NetScaler 14.1

Machine translated content

Disclaimer

Contents

NetScaler-Versionshinweise

June 19, 2023

Versionshinweise beschreiben, wie sich die Software in einem bestimmten Build geändert hat und welche Probleme im Build bekannt sind.

Das Dokument mit den Versionshinweisen enthält alle oder einige der folgenden Abschnitte:

- **Was ist neu**: Die Verbesserungen und anderen Änderungen, die im Build veröffentlicht wurden.
- **Behobene Probleme**: Die Probleme, die im Build behoben wurden.
- **Bekannte Probleme**: Die Probleme, die im Build bestehen.
- **Zu beachtenswerte Punkte**: Die wichtigen Aspekte, die bei der Verwendung des Builds zu beachten sind.
- **Einschränkungen**: Die Einschränkungen, die im Build bestehen.

> **Hinweis**
>
> - Die [# XXXXXX]-Kennungen unter den Problembeschreibungen sind interne Tracking-IDs, die vom NetScaler-Team verwendet werden.
> - Diese Versionshinweise dokumentieren keine sicherheitsrelevanten Korrekturen. Eine Liste sicherheitsbezogener Fixes und Empfehlungen finden Sie im Security Bulletin.

Versionshinweise für NetScaler 14.1—4.42

September 1, 2023

In diesem Dokument mit den Versionshinweisen werden die Verbesserungen und Änderungen sowie die behobenen und bekannten Probleme beschrieben, die für die NetScaler-Version Build 14.1—4.42 bestehen.

Hinweise

- Dieses Dokument mit Versionshinweisen enthält keine sicherheitsbezogenen Fixes. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Was ist neu

Die Verbesserungen und Änderungen, die in Build 14.1—4.42 verfügbar sind.

Analytics-Infrastruktur

- **Unterstützung für den direkten Export von NetScaler-Ereignissen nach Splunk**

  Sie können die auf NetScaler generierten Ereignisse jetzt direkt nach Splunk exportieren. Mithilfe von Splunk-Dashboards können Sie die exportierten Daten visualisieren und aussagekräftige Einblicke erhalten.

  Weitere Informationen finden Sie unter Exportieren von Audit-Logs und Ereignissen direkt von NetScaler nach Splunk.

  [NSANINFRA-3892]

Authentifizierung, Autorisierung und Auditing

- **Referenzwerte für Authentifizierungskontextklassen speichern**

  NetScaler, der als on-premises IdP konfiguriert ist, kann ACR-Werte (Authentication Context Class Reference) speichern, die von Citrix Workspace zur Unterstützung der Multidomänen-Anmeldefunktion der Citrix Workspace-Plattform bereitgestellt werden. Wenn Citrix Workspace die ACR-Werte an den OAuth-Autorisierungsendpunkt des NetScaler-IdP sendet, speichert NetScaler die ACR-Werte.

  Die Richtlinienausdrücke `aaa.user.wsp.eq("URL")` und `aaa.user.acr_values.value("wsp").eq("URL")` werden im Rahmen dieser Unterstützung eingeführt. Sie können die ACR-Werte verwenden, um den nächsten Faktor im nFactor-Flow zu bestimmen. Weitere Informationen finden Sie unter Referenzwerte der Store Authentication Context Class.

  [NSAUTH-12981]

NetScaler Anwendungsbereitstellung und Sicherheitsanalyse

- **Unterstützung für einen erweiterten StoreFront-Monitor**

  NetScaler führt einen erweiterten StoreFront-Monitor ein, der die Authentifizierung und App-Enumeration im Citrix StoreFront-Store im Namen eines Testbenutzerkontos simulieren kann. Sie müssen dieses Konto in StoreFront für die Überwachung vorkonfigurieren und aktivieren. Geben Sie die Anmeldeinformationen des Testbenutzers, den Speichernamen und das `nssf_extend.pl` Skript an, um die Funktionen dieses Monitors nutzen zu können. Weitere Informationen finden Sie unter Erweiterte StoreFront-Überwachung.

  [NSADSA-805]

NetScaler Gateway

- **Verbesserungen am Gateway Insights-Dashboard**
  Die Seite Gateway > Gateway Insight Overview der NetScaler ADM GUI wurde unter EPA (End Point Analysis) um die folgenden Funktionen erweitert:
  - EPA-Fehler werden auch für fortgeschrittenes EPA angezeigt. Die Fehler können gemeldet werden, wenn EPA als Faktor in einem nFactor-Authentifizierungsablauf konfiguriert ist.
  - Fehlerbeschreibung: Im Feld Fehlerbeschreibung wird die Meldung “Fehler bei der EPA-Pre-Auth-Prüfung” angezeigt, wenn eine EPA-Prüfung fehlschlägt.
  - Fall-ID: Im Feld Benutzername wird die Fall-ID bei Einträgen angezeigt, denen kein Benutzername zugewiesen wurde, wenn EPA als Faktor in einem nFactor-Flow verwendet wird.

  Weitere Informationen finden Sie unter Gateway Insight.

  [CGOP-17730]

NetScaler SDX-Appliance

- **Informationen zum Ablauf der Abonnementlizenz anzeigen**

  Sie können jetzt Informationen zum Ablauf der NetScaler SDX-Abonnementlizenz im Management Service anzeigen, indem Sie zu System > Lizenzen navigieren.

  [NSSVM-5629]

- **Höhere Lizenzlimits für NetScaler SDX 9100 Appliance**

  Das Lizenzlimit für die NetScaler SDX 9100 Appliance wurde von 30 G auf 95 G erhöht.

  [NSSVM-5609]

- **Aktivieren, Deaktivieren und Bearbeiten von BMC-Einstellungen (LOM) mithilfe der Management Service-Benutzeroberfläche**

  Sie können jetzt BMC-Einstellungen (LOM) mithilfe der Management Service-Benutzeroberfläche aktivieren, deaktivieren und bearbeiten. Navigieren Sie zu **Konfiguration > System > Systemeinstellungen > BMC-Einstellungen konfigurieren**. Die folgenden Einstellungen werden für alle Plattformen angezeigt.
  - IP-Adresse
  - Subnetzmaske
  - Standard-Gateway

  Auf den Plattformen SDX 9100 und SDX 16000 wird auch die LOM Access-Einstellung angezeigt. Der LOM-Zugriff muss entsperrt sein, um die anderen Einstellungen bearbeiten zu können.

  [NSSVM-5558]

- **Wechseln Sie zur Häufigkeit der XenServer-Statusüberwachung und zu Ping-Fehlerwarnungen**

  Die Häufigkeit der Überwachung der Integritätseigenschaften für einen XenServer wurde von 14 Sekunden auf 1 Minute geändert. Wenn ein Ping an den XenServer fehlschlägt, wird außerdem erst nach 10 ununterbrochenen Ausfällen eine Warnung ausgelöst. Zuvor wurde für jeden Fehler eine Warnung ausgelöst.

  [NSSVM-5510]

- **Sichern Sie VPX-Partitionen während der Backup einer SDX-Appliance**

  Eine NetScaler SDX-Appliance sichert und stellt jetzt die folgenden Eigenschaften von VPX-Partitionen während der Backup und Wiederherstellung der SDX-Appliance wieder her.

  - Responder-Datei
  - MACs partitionieren

  [NSSVM-5230]

NetScaler Secure Web Gateway

- **Veraltete URL-Kategorisierung in der URL-Filterfunktion**

  Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

  Hinweis: Veraltete Funktionen werden nicht sofort entfernt. NetScaler behält die veraltete Funktion weiterhin bei, bis sie in einer zukünftigen Version entfernt wird.

  [NSSWG-1370]

Netzwerke

- **Komprimierte Core-Dumps für die NetScaler BLX-Appliance**
  Jetzt generiert die NetScaler BLX-Appliance komprimierte Core-Dumps, wenn der Parameter **core-dumps in der NetScaler BLX-Konfigurationsdatei (blx.conf)** aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren komprimierter Core-Dumps für NetScalerBLX.

  [NSNET-28478]

- **Konfigurierbarer interner HTTPS-Dienst**

  Sie können den internen HTTPS-Dienst jetzt mithilfe von GUI-, CLI- NITRO-APIs konfigurieren. Sie können beispielsweise die NetScaler CLI verwenden, um die maximale Anzahl von Clients zu ändern, die gleichzeitig eine Verbindung zum internen HTTPS-Dienst herstellen können.

  Der interne HTTPS-Dienst hat das folgende Namensformat: `nshttps-<loop back IP address>-443`

Verwenden Sie die NetScaler-Dienstbefehlsoperationen, um den internen HTTPS-Dienst zu konfigurieren.

[NSNET-15878, NSHELP-22575]

- **Die Befehlsweiterleitung ist während der HA-Synchronisierung deaktiviert Bei** Hochverfügbarkeits-Setups ist die Befehlsweiterleitung während der HA-Synchronisierung deaktiviert, um Fehler bei der Befehlsverbreitung während der HA-Synchronisierung zu verhindern. Weitere Informationen finden Sie unter Konfiguration der Befehlsweiterleitung.

  [NSHELP-34253]

- **Large Scale NAT-Funktion ist veraltet**

  Die Large Scale NAT (LSN) -Funktion, die LSN44, Dual-Stack Lite und LSN64 umfasst, ist in dieser Version veraltet. Weitere Informationen finden Sie unter Large Scale NAT.

  Hinweis: Veraltete Funktionen werden nicht sofort entfernt. Die NetScaler Appliance unterstützt die veraltete Funktion weiterhin, bis sie in einer zukünftigen Version entfernt wird.

  [NSNET-27990]

Plattform

- **Entfernung der Unterstützung für NetScaler MPX 5500, MPX 7500 und MPX 17500**

  NetScaler MPX 5500, MPX 7500/9500 und MPX 17500/19500/21500 werden mit NetScaler Firmware 14.1 nicht unterstützt.

  [NSPLAT-25839]

SSL

- **Ratenbegrenzende SSL-Neuverhandlungen**

  Wenn die SSL-Neuverhandlung aktiviert ist, gibt es keine Begrenzung für die Anzahl der Neuverhandlungsanfragen an einen NetScaler. Infolgedessen stoppt NetScaler möglicherweise die Verarbeitung von SSL-Verkehr, wenn es eine große Anzahl von Neuverhandlungsanfragen erhält. Diese Funktion begrenzt die Anzahl der Neuverhandlungsanfragen, die innerhalb einer Sekunde auf einer SSL-Entität eingehen.

  In den folgenden Befehlen ist „MaxRenegrate“ beispielsweise auf 100 gesetzt. Infolgedessen sind maximal 100 Anfragen pro Sekunde an alle Entitäten zulässig, an die das Profil gebunden ist. Sie können diesen Parameter festlegen, indem Sie den `add ssl profile` Befehl verwenden, wenn Sie ein SSL-Profil hinzufügen. Verwenden Sie den `set ssl profile` Befehl, um diesen Parameter festzulegen, nachdem Sie ein SSL-Profil hinzugefügt haben.


```
set ssl profile pf1 -denySSLReneg (NO | FRONTEND_CLIENT | FRONTEND_CLIENTSERVER
 | NONSECURE)-maxRenegRate 100

add ssl profile pf1 -denySSLReneg (NO | FRONTEND_CLIENT | FRONTEND_CLIENTSERVER
 | NONSECURE)-maxRenegRate 100
```

Weitere Informationen finden Sie unter SSL-Neuverhandlungen mit Ratenbegrenzung.

[NSSSL-12186]

- **Unterstützung für das TLS 1.3-Protokoll auf Backend-Diensten, Servicegruppen und Monitoren**

  Back-End-Dienste, Dienstgruppen und Monitore unterstützen jetzt das TLS 1.3-Protokoll bei der Verbindung mit Backend-Servern. Weitere Informationen finden Sie unter Unterstützung für das TLS 1.3-Protokoll.

  [NSSSL-5970]

System

- **Verbesserter Schutz vor TCP-Spoofing-Angriffen**

  Ab der NetScaler ADC 14.1-4.x-Version ist NetScaler mit RFC5961 kompatibel, was einen verbesserten Schutz vor TCP-Spoofing-Angriffen bietet. Mit der RFC 5961-Konformität bietet NetScaler zusätzlich zur RST-Fensterdämpfung und dem SYN-Spoof-Schutz die folgenden Funktionen:

  - Reduziert die Wahrscheinlichkeit einer ungültigen Dateneinspeisung.
  - Ermöglicht die Begrenzung der Anzahl der vom NetScaler gesendeten Challenge-ACK-Antworten pro Sekunde.

  Wenn Sie die RFC 5961-Konformität aktivieren, antwortet NetScaler mit einer Challenge-Bestätigung (ACK), wenn inakzeptable RST, SYN oder ACK gemäß RFC 5961-Konformität empfangen werden. Sie können die RFC 5961-Konformität sowohl mit der CLI als auch mit der GUI aktivieren. Weitere Informationen finden Sie unter TCP-Konfigurationen.

  [NSBASE - 17086]

Benutzeroberfläche

- **Beschränken Sie gleichzeitige Sitzungen für Benutzer auf Systemebene**

  Sie können jetzt die Anzahl der gleichzeitigen Sitzungen begrenzen, die für alle Benutzer auf Systemebene zulässig sind. Mit dem Parameter `maxsessionperuser` im Befehl `set system parameter` können Sie dieses Limit festlegen.

  ```
  set system parameter maxsessionperuser <positive integer>
  ```


Wenn der Systembenutzer auf dem NetScaler erstellt wurde und das `maxsession` Limit für den Systembenutzer festgelegt ist, `maxsession` hat es Vorrang vor diesem Limit auf Systemebene ().`maxsessionperuser`

[NSCONFIG -6546]

Behobene Probleme

Die Probleme, die nach der Feature-Version 13.1-48.x behoben wurden.

Analytics-Infrastruktur

- Wenn ein Netzprofil in einer nicht standardmäßigen Verkehrsdomäne konfiguriert und in der AppFlow-Konfiguration verwendet wird, sind die Systemports erschöpft und der Datenverkehr wird beeinträchtigt.

  [NSHELP-34544]

- Die Datei `ns.log` generiert die Debug-Protokolle auch dann, wenn die Audit-Protokollebene auf “Keine” gesetzt ist und daher die konfigurierte Dateigrößenbeschränkung überschreitet. Das Problem tritt auf, weil die erweiterte Richtlinie an die lokale Protokollierung gebunden ist, obwohl sie nicht erforderlich ist.

  [NSHELP-32404]

Authentifizierung, Autorisierung und Auditing

- Ein mit einer OAuth-Authentifizierungsrichtlinie konfigurierter NetScaler stürzt möglicherweise ab, wenn ein Zertifikat mit elliptischer Kurve global an das VPN gebunden ist.

  [NSHELP-34795]

- Ein HTTP 404-Fehler tritt auf, wenn ein Benutzer versucht, sich nach Ablauf der Sitzung mit einem GSLB-konfigurierten NetScaler zu authentifizieren.

  [NSHELP-34336]

- Die NetScaler-Appliance kann abstürzen, wenn der virtuelle Authentifizierungsserver in einer nicht standardmäßigen Partition verwendet wird.

  [NSHELP-32054, NSCXLCM-640]

- Nach einem Upgrade von Citrix SSO für iOS werden die Pushbenachrichtigungen, die Sie zur Authentifizierung erhalten, möglicherweise nicht mit einem Ton angezeigt.

  [NSHELP-27525]

Bot-Verwaltung

- Die NetScaler-Appliance kann abstürzen, wenn die BOT-Richtlinie eine Protokollaktion mit komplexen Richtlinienregeln verwendet.

  [NHELP - 34999]

- Angriffe zur Wiederholung von Bot-Gerätefingerabdrucksitzungen werden verworfen, wenn die Aktion für den Gerätefingerabdruck auf LOG, RESET oder REDIRECT gesetzt ist.

  [NSBOT-1117]

CallHome

- Call Home sendet Telemetriedaten an den NetScaler Technical Support Server, obwohl die Funktion deaktiviert ist.

  [NSHELP-33240]

Lastausgleich

- In seltenen Fällen kann eine NetScaler-Appliance abstürzen und einen Core-Dump generieren, wenn die folgenden Bedingungen erfüllt sind:
  - Die TCP-basierte DNS-Monitor-Sonde wird verwendet, um einen Back-End-Dienst zu überwachen.
  - Der Appliance geht der Arbeitsspeicher zur Neige.

  [NHELP - 35289]

- In einer Clusterkonfiguration mit acht oder mehr Knoten funktioniert das Feature für die Ratenlimit-ID möglicherweise nicht wie vorgesehen.

  [NSHELP-34555]

- Der sekundäre NetScaler kann abstürzen, wenn die folgenden Bedingungen erfüllt sind:
  - In einem Hochverfügbarkeits-Setup wird eine große Anzahl von Load Balancing-Servern mit Lastausgleichsgruppen konfiguriert.
  - Während der Synchronisation wird der festgelegte Vorgang auf einem der Load Balancing-Server in der Load Balancing-Gruppe ausgeführt.

  [NHELP - 34225]

- Der NetScaler stürzt möglicherweise aufgrund eines Zeitproblems zwischen dem Abrufen von ratenbegrenzenden Datensätzen und dem Alterungsprozess der Datensätze ab.

  [NSHELP-33349]

- In einigen Fällen wird ein Speicherverlust in einer NetScaler-Appliance beobachtet, wenn die DNS-Rewrite-Richtlinie mit der DROP-Aktion konfiguriert ist.

  [NSHELP-33077]

Sonstiges

- Wenn ein Cluster-Setup inaktiv ist, kann Node-zu-Node-Messaging (NNM) eine Verzögerung von 20 Millisekunden für Ping-Pakete mit einer bestimmten sndbuf-Größe hinzufügen (Ping-Befehl mit Option -S).

  [NHELP - 34774]

NetScaler Gateway

- Manchmal stürzt ein NetScaler mit konfiguriertem VPN und AppFlow ab, was zu einem HA-Failover führt.

  [NSHELP-35734, NSCXLCM-1247]

- Die NetScaler Gateway-Homepage listet die Apps möglicherweise nicht auf, wenn Sie versuchen, mit einem mobilen Browser im clientlosen VPN-Modus darauf zuzugreifen.

  [NSHELP-35541, NSCXLCM-1132, NSCXLCM-1212, NSCXLCM-1248]

- Wenn der erweiterte clientlose VPN-Zugriff auf NetScaler Gateway konfiguriert ist, können die Seiten möglicherweise nicht von den mit Lesezeichen versehenen URLs geladen werden.

  [NSHELP-33771]

- Wenn Sie eine VPN-Verbindung über NetScaler Gateway herstellen, werden Sie manchmal mit falschem Text in der URL zur Startseite weitergeleitet. Dieses Problem tritt auf, wenn NetScaler mit dem RfWebUI Portaldesign konfiguriert ist.

  [NSHELP-30097, NSCXLCM-481]

- Wenn Sie eine EULA-Entität erstellen, wird der Text als einzelne Zeile im RfWebUI Portaldesign von NetScaler Gateway angezeigt. Dieses Problem tritt aufgrund des HTML-Zeilenumbruchtags `<br>` auf. Alle HTML-Tags zusammen mit `<br>` sind im EULA-Text vorübergehend deaktiviert. Sie können versuchen, Zeilenumbrüche hinzuzufügen, indem Sie verwenden `\n`.

  [CGOP-24534]

NetScaler SDX-Appliance

- Auf NetScaler SDX FIPS wird der folgende Fehler angezeigt, wenn Sie einen Vorgang zum Hinzufügen oder Bearbeiten auf VPX ausführen:

„is_fips_enabled ist nicht definiert“

[NSSVM-5786]

NetScaler Web App Firewall

- Der NetScaler stürzt möglicherweise ab, wenn **VerboseLogLevel** im Web App Firewall-Profil auf **patternPayloadHeader** gesetzt ist.

  [NSHELP-35915]

- Die IP-Reputationsdatenbank wird möglicherweise nicht von Webroot aktualisiert, wenn Sie die unbefristete Lizenz auf dem NetScaler verwenden.

  [NSHELP-33965]

Netzwerke

- NetScaler BLX-NIC-Einstellungen sind möglicherweise noch auf dem Linux-Host vorhanden, wenn Sie die NetScaler BLX-Appliance deinstallieren, während sie läuft.

  Workaround. Stoppen Sie die NetScaler BLX-Appliance, bevor Sie die Appliance deinstallieren.

  [NSNET-29109]

- Die NetScaler-Appliance reagiert möglicherweise nicht auf “SNMP GETBULK”-Anfragen.

  [NSHELP-35902]

- In einem Hochverfügbarkeits-Setup stürzt der sekundäre Knoten ab, wenn eine Route im Rahmen der HA-Synchronisierung vom Knoten entfernt wird, während Sie sie ändern.

  [NSHELP-34927]

- In einem Hochverfügbarkeits-Setup zeigt der Knoten show ha möglicherweise eine falsche Ausgabe an, wenn die beiden folgenden Bedingungen erfüllt sind:

  - HA-Heartbeats werden nur über eine einzige Schnittstelle oder einen einzelnen Kanal ausgetauscht.
  - Die Schnittstelle oder der Kanal ist deaktiviert.

  [NSHELP-34193]

- Die NetScaler-Appliance protokolliert die Meldungen zum SNMPv3-Authentifizierungsfehler nicht in der NetScaler-Protokolldatei (“/var/log/ns.log”).

  [NSHELP-33909]

- In einem Hochverfügbarkeits-Setup dauert es mindestens 60 Sekunden, bis der Status eines Knotens aktiv wird, wenn alle folgenden Bedingungen erfüllt sind:

- Fail-safe ist für das HA-Setup aktiviert
- Die HA-Überwachung ist auf mehr als einer Schnittstelle aktiviert
- Eine der für die HA-Überwachung aktivierten Schnittstellen wird nicht mehr erreichbar
- Mindestens eine der HA-Überwachungsschnittstellen ist erreichbar

Mit diesem Fix wird der Status des Knotens sofort auf UP gesetzt, wenn alle diese Bedingungen erfüllt sind.

[NSHELP-32157]

Plattform

- In einer HA-Paarkonfiguration auf der AWS-Plattform wurden NetScaler VPX-Schnittstellen während eines Failovers für die folgende Konfiguration nicht ordnungsgemäß migriert:
  - Die HA-Bereitstellung erfolgt in derselben Zone.
  - Mehrere Schnittstellen verwenden dasselbe Subnetz.

  [NSHELP-35369]
- Sie können nicht mehr auf einen Citrix Hypervisor zugreifen, der auf NetScaler SDX gehostet wird, indem Sie ältere SSL-Protokolle wie SSLv3, TLS 1.0 und TLS 1.1 verwenden.

  [NSHELP-33196]
- Nach einem Firmware-Upgrade kann die Verwaltungsschnittstelle einer NetScaler MPX 5900/8900-Appliance ausfallen. Daher ist das Gerät nicht zugänglich.

  [NSHELP-31587]

SSL

- Auf einem NetScaler MPX/SDX 14000 FIPS, der im Hybridmodus betrieben wird, wird der Schlüsselspeicher möglicherweise zurückgesetzt, nachdem beschädigte Daten im Rahmen eines Schlüsselaustauschs empfangen wurden.

  [NSHELP-35020]
- Bei hohem Datenverkehr kann es zu vorübergehenden Leistungseinbußen kommen, wenn die Gesamtgröße der in einem SSL-Handshake ausgetauschten Client-, Server- und CA-Zertifikate das 16K-Limit überschreitet.

  [NSHELP-33905]

System

- Wenn der Backend-Server einen 464-Fehler für eine HTTP-Anfrage sendet, leitet der NetScaler diesen Fehler nicht an den Client weiter und daher ist die Verbindung auf der Clientseite blockiert.

  [NSHELP-33571, NSCXLCM-1098]

Benutzeroberfläche

- Wenn Sie eine Responder-Richtlinie oder eine Rewrite-Richtlinie auf der NetScaler-GUI konfigurieren, ohne Werte in den Feldern **Log Action** und **AppFlow Action** hinzuzufügen, die nicht obligatorisch sind, wird der folgende Fehler angezeigt:

  “Invalid name; names must begin with an alphanumeric character or underscore and must contain only alphanumerics, ‘_’, ‘%23’, ‘.’, ‘ ‘, ‘:’, ‘@’, ‘=’ or ‘-‘ [logAction,]”

  [NSHELP-35726]

- Benutzersitzungen werden falsch berechnet, wenn derselbe Benutzer an zwei verschiedene Partitionen gebunden ist. Bei den beiden Partitionen kann es sich um Standardpartitionen, Nichtstandardpartitionen oder beides handeln.

  [NSHELP-34971]

- Wenn Sie einen Autorisierungsrichtlinienausdruck auf der NetScaler Gateway-Benutzeroberfläche ändern, wird die AAA-Option nicht in der Dropdownliste “Ausdrucksеditor” angezeigt.

  [NSHELP-33509]

- Einige integrierte Konfigurationen sind nicht verfügbar, wenn eine NetScaler ADC-Instanz erstellt wird.

  [NSHELP-33451, NSCXLCM-502]

- In der NetScaler-GUI schlägt die nFactor-Authentifizierung fehl und der Fehler „Keine aktive Richtlinie während der Authentifizierung“ wird angezeigt. Dieses Problem tritt auf, wenn eine Zuweisungsaktion konfiguriert, aber nicht an eine Authentifizierungsrichtlinie gebunden ist.

  [NSHELP-33339]

- Wenn ein Benutzer die Bindung in einer Content Switching-Richtlinie betrachtet, werden die Details des virtuellen Content Switching-Servers nicht in derselben Zeile unter **Bindungen anzeigen** angezeigt.

  [NSHELP-33149]

- Die NetScaler GUI zeigt im Vergleich zur Befehlsschnittstelle weniger zwischengespeicherte Objekte an.

[NSHELP-24337]

Bekannte Probleme

Die Probleme, die in Version 14.1—4.42 bestehen.

Analytics-Infrastruktur

- Wenn Sie in einer Cluster-Bereitstellung den Befehl “Force Cluster Sync” auf einem Nicht-CCO-Knoten ausführen, enthält die Datei ns.log doppelte Protokolleinträge.

  [NSANINFRA-2850, NSGI-1293]

- Wenn Sie NetScaler ADM auf einem Kubernetes-Cluster installieren, funktioniert es nicht wie erwartet, da die erforderlichen Prozesse möglicherweise nicht ausgeführt werden.

  Problemumgehung: Starten Sie den Management-Pod neu.

  [NSANINFRA-1504]

Authentifizierung, Autorisierung und Auditing

- Ein NetScaler stürzt ab, wenn die folgenden Bedingungen erfüllt sind:
  - Die 401-basierte Zertifikatsauthentifizierung erfolgt über einen virtuellen Lastausgleichsserver.
  - Es gibt keine Authentifizierungsrichtlinie, die an einen virtuellen Authentifizierungsserver gebunden ist.
  - Die Debug-Protokollierung ist aktiviert.

  [NSAUTH-13259]

- Administratoren können keine benutzerdefinierte Protokollierung für Authentifizierungsfehler durchführen, die auf ungültige Anmeldeinformationen zurückzuführen sind. Dieses Problem tritt auf, weil die NetScaler-Responder-Richtlinien Fehler für Anmeldefehler nicht erkennen können.

  [NSAUTH-11151]

- Das ADFS-Proxy-Profil kann in einer Clusterbereitstellung konfiguriert werden. Der Status für ein Proxy-Profil wird fälschlicherweise als leer angezeigt, wenn der folgende Befehl ausgegeben wird.
  `show adfsproxyprofile <profile name>`

  Problemumgehung: Stellen Sie eine Verbindung zum primären aktiven NetScaler im Cluster her und führen Sie den Befehl `show adfsproxyprofile <profile name>` aus. Er zeigt den Status des Proxyprofils an.

[NSAUTH-5916]

- Die Seite Authentifizierung LDAP-Server konfigurieren auf der NetScaler-GUI reagiert nicht mehr, wenn Sie die folgenden Schritte ausführen:
  - Die Option LDAP-Erreichbarkeit testen wird geöffnet.
  - Ungültige Anmeldeinformationen werden ausgefüllt und übermittelt.
  - Gültige Anmeldeinformationen werden ausgefüllt und übermittelt.

  Problemumgehung: Schließen Sie die Option LDAP Reachability testen und öffnen Sie sie.

  [NSAUTH-2147]

Lastausgleich

- In einem Hochverfügbarkeitssetup werden Teilnehmersitzungen des primären Knotens möglicherweise nicht mit dem sekundären Knoten synchronisiert. Dies ist ein seltener Fall.

  [NSLB-7679]

Sonstiges

- Wenn die EDT Insight-Funktion aktiviert ist, können Audiokanäle manchmal während einer Netzwerkabweichung ausfallen.

  [GOPHDX-1055]

- In einem Hochverfügbarkeitssetup wird während des NetScaler-Failovers die SR-Anzahl anstelle der Failover-Anzahl in NetScaler ADM erhöht.

  [GOPHDX-1050]

NetScaler Gateway

- Manchmal erscheint beim Durchsuchen von Schemas die Fehlermeldung “Cannot read property ‘type’ of undefined”.

  [NSHELP-21897]

- Die Windows-Betriebssystemoption ist in der Dropdownliste des Expression Editors für Vorauthentifizierungsrichtlinien und Authentifizierungsaktionen auf der NetScaler GUI nicht aufgeführt. Wenn Sie den Windows-Betriebssystemscan jedoch bereits in einem früheren NetScaler-Build mithilfe der GUI oder der CLI konfiguriert haben, hat das Upgrade keine Auswirkungen auf die Funktionalität. Sie können die CLI verwenden, um bei Bedarf Änderungen vorzunehmen.

  Workaround:

Verwenden Sie die CLI-Befehle für die Konfiguration.

- Verwenden Sie den folgenden Befehl, um die erweiterte EPA-Aktion in der nFactor-Authentifizierung zu konfigurieren.
  add authentication epaAction adv_win_scan -csecexpr “sys.client_expr(“sys_0_WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]”)”
- Verwenden Sie die folgenden Befehle, um eine klassische Vorauthentifizierungsaktion zu konfigurieren.
  add aaa preauthenticationaction win_scan_action ALLOW
  add aaa preauthenticationpolicy win_scan_policy “CLIENT.SYSTEM(‘WIN-OS_NAME_anyof_WIN-10[COMMENT: Windows OS]’) EXISTS” win_scan_action

[CGOP-22966]

- Um die Always-On-VPN-Funktion vor der Windows-Anmeldung zu verwenden, wird empfohlen, Ihr NetScaler Gateway auf 13.0 oder höher zu aktualisieren. Auf diese Weise können Sie die zusätzlichen Verbesserungen nutzen, die in Version 13.0 eingeführt wurden und die in Version 12.1 nicht verfügbar sind.

  [CGOP-19355]

- Eine Fehlermeldung wird angezeigt, wenn Sie eine Sitzungsrichtlinie über die NetScaler-GUI hinzufügen oder bearbeiten.

  [CGOP-11830]

- Wenn Sie in Outlook Web App (OWA) 2013 im Menü Einstellungen auf **Optionen** klicken, wird ein Dialogfeld mit **kritischem Fehler** angezeigt. Außerdem reagiert die Seite nicht mehr.

  [CGOP-7269]

NetScaler Secure Web Gateway

- Wenn in einem Hochverfügbarkeits-Setup eine erzwungene Synchronisation stattfindet, führt die Appliance den Befehl “set urlfiltering parameter” im sekundären Knoten aus.
  Daher überspringt der sekundäre Knoten jedes geplante Update bis zur nächsten geplanten Zeit, die im Parameter “TimeOfDayToUpdateDB” angegeben ist.

  [NSSWG-849]

- Eine NetScaler-Appliance wird möglicherweise aufgrund einer Stagnation der Verwaltungs-CPU neu gestartet, wenn ein Verbindungsproblem mit dem Drittanbieter der URL-Filterung auftritt.

  [NSHELP-22409]

Netzwerke

- Die folgenden Schnittstellenvorgänge werden für Intel `X710 10G (i40e)`-Schnittstellen auf einer NetScaler BLX-Appliance mit DPDK nicht unterstützt:
  - Deaktivieren
  - Aktivieren
  - Reset

  [NSNET-16559]

- Die Installation einer NetScaler BLX-Appliance schlägt möglicherweise auf einem Debian-basierten Linux-Host (Ubuntu Version 18 und höher) mit dem folgenden Abhängigkeitsfehler fehl:

  "The following packages have unmet dependencies: blx-core-libs:i386 : PreDepends: libc6:i386 (>= 2.19) but it is not installable"

  Problemumgehung: Führen Sie die folgenden Befehle in der Linux-Host-CLI aus, bevor Sie eine NetScaler BLX-Appliance installieren:
  - dpkg — Architektur hinzufügen i386
  - apt-get update
  - apt-get install libc6:i386

  [NSNET-14602]

- In einigen Fällen von FTP-Datenverbindungen führt die NetScaler-Appliance nur NAT-Operationen und keine TCP-Verarbeitung für die Pakete für die TCP-MSS-Aushandlung aus. Infolgedessen ist die optimale Schnittstellen-MTU nicht für die Verbindung eingestellt. Diese falsche MTU-Einstellung führt zu einer Fragmentierung von Paketen und beeinträchtigt die CPU-Leistung.

  [NSNET-5233]

- Wenn ein Speicherlimit für die Administratorpartition in der NetScaler-Appliance geändert wird, wird das TCP-Pufferspeicherlimit automatisch auf das neue Speicherlimit der Administratorpartition festgelegt.

  [NSHELP-21082]

Plattform

- Einige Python-Pakete werden nicht installiert, wenn Sie die NetScaler-Appliance von Version 13.1-4.x und höheren Versionen auf eine der folgenden Versionen herabstufen:
  - Jeder 11.1-Build
  - 12.1-62,21 und früher

- 13.0-81.x und früher

[NSPLAT-21691]

- Wenn Sie eine Autoscale-Einstellung oder einen VM-Skalierungssatz aus einer Azure-Ressourcengruppe löschen, löschen Sie die entsprechende Cloud-Profilkonfiguration aus der NetScaler-Instanz. Verwenden Sie den Befehl "rm cloudprofile", um das Profil zu löschen.

  [NSPLAT-4520]

- In einem Hochverfügbarkeitssetup auf Azure wird bei der Anmeldung am sekundären Knoten über die GUI der Bildschirm für den Erstbenutzer (FTU) für die automatische Skalierung der Cloud-Profilkonfiguration angezeigt.
  Workaround: Überspringen Sie den Bildschirm und melden Sie sich beim primären Knoten an, um das Cloud-Profil zu erstellen. Das Cloud-Profil sollte immer auf dem primären Knoten konfiguriert werden.

  [NSPLAT-4451]

Policies

- Verbindungen können hängen, wenn die Größe der Verarbeitungsdaten größer ist als die konfigurierte Standard-TCP-Puffergröße.

  Problemumgehung: Stellen Sie die TCP-Puffergröße auf die maximale Größe der Daten ein, die verarbeitet werden müssen.

  [NSPOLICY-1267]

SSL

- Auf einem heterogenen Cluster von NetScaler SDX 22000 und NetScaler SDX 26000 Appliances kommt es zu einem Konfigurationsverlust von SSL-Entitäten, wenn die SDX 26000-Appliance neu gestartet wird.

  Workaround:

  1. Deaktivieren Sie auf dem CLIP SSLv3 für alle vorhandenen und neuen SSL-Entitäten wie virtuellen Server, Dienst, Dienstgruppe und interne Dienste. Beispiel: `set ssl vserver <name> -SSL3 DISABLED`.
  2. Speichern Sie die Konfiguration.

  [NSSSL-9572]

- Sie können kein Azure Key Vault-Objekt hinzufügen, wenn bereits ein Azure Key Vault-Authentifizierungsobjekt hinzugefügt wurde.

  [NSSSL-6478]

- Sie können mehrere Azure Application Entitäten mit derselben Client-ID und demselben Clientgeheimnis erstellen. Die NetScaler-Appliance gibt keinen Fehler zurück.

  [NSSSL-6213]

- Die folgende falsche Fehlermeldung wird angezeigt, wenn Sie einen HSM-Schlüssel entfernen, ohne KEYVAULT als HSM-Typ anzugeben.
  FEHLER: CRL-Aktualisierung deaktiviert

  [NSSSL-6106]

- Die automatische Aktualisierung des Sitzungsschlüssels wird fälschlicherweise auf einer Cluster-IP-Adresse als deaktiviert angezeigt. (Diese Option kann nicht deaktiviert werden.)

  [NSSSL-4427]

- Wenn Sie versuchen, das SSL-Protokoll oder die Verschlüsselung im SSL-Profil zu ändern, wird eine falsche Warnmeldung mit dem Titel “Warnung: Keine verwendbaren Verschlüsselungen konfiguriert auf dem SSL vserver/service” angezeigt.

  [NSSSL-4001]

- Ein abgelaufenes Sitzungsticket wird nach einem HA-Failover auf einem Nicht-CCO-Knoten und auf einem HA-Knoten berücksichtigt.

  [NSSSL-3184, NSSSL-1379, NSSSL-1394]

System

- Die mit einem SSL-Dienst konfigurierte NetScaler-Appliance stürzt ab, wenn die Appliance ein TCP-FIN-Steuerpaket empfängt, gefolgt von einem TCP-RESET-Steuerpaket.

  [NSHELP-31656]

- Ein hoher RTT wird für eine TCP-Verbindung beobachtet, wenn die folgende Bedingung erfüllt ist:

  - ein hohes maximales Überlastungsfenster (>4 MB) ist eingestellt
  - Der TCP-NILE-Algorithmus ist aktiviert

  Damit eine NetScaler-Appliance den NILE-Algorithmus zur Überlastungskontrolle verwenden kann, müssen die Bedingungen den Schwellenwert für den langsamen Start überschreiten, der mit dem Fenster für maximale Überlastung gekoppelt ist.

  Bis das maximal konfigurierte Überlastungsfenster erreicht ist, akzeptiert der NetScaler weiterhin Daten und endet mit einem hohen RTT.

  [NSHELP-31548]

- Die mptcp_cur_session_without_subflow-Zähler verringern fälschlicherweise auf einen negativen Wert statt auf Null.

  [NSBASE - 18295]

- Client-IP und Server-IP werden im HDX Insight SkipFlow-Datensatz invertiert, wenn der LogStream-Transporttyp für Insight konfiguriert ist.

  [NSBASE-8506]

Benutzeroberfläche

- In der NetScaler-GUI ist der Link “Hilfe” auf der Registerkarte “Dashboard” defekt.

  [NSUI-14752]

- Der Assistent zum Erstellen/Überwachen von CloudBridge Connector reagiert möglicherweise nicht oder konfiguriert keinen Cloudbridge-Konnektor.

  Problemumgehung: Konfigurieren Sie Cloudbridge-Connectors, indem Sie IPSec-Profile, IP-Tunnel und PBR-Regeln mithilfe der NetScaler GUI oder CLI hinzufügen.

  [NSUI-13024]

- Wenn Sie über die GUI einen ECDSA-Schlüssel erstellen, wird der Kurventyp nicht angezeigt.

  [NSUI-6838]

Erste Schritte mit NetScaler

August 4, 2023

In diesem Thema werden die grundlegenden Funktionen und Konfigurationsdetails einer NetScaler-Appliance beschrieben. System- und Netzwerkadministratoren, die Netzwerkgeräte installieren und konfigurieren, können auf den Inhalt verweisen.

NetScaler verstehen

Die NetScaler-Appliance ist ein Anwendungs-Switch, der anwendungsspezifische Verkehrsanalysen durchführt, um Layer 4-Layer 7 (L4—L7) -Netzwerkverkehr für Webanwendungen intelligent zu verteilen, zu optimieren und zu sichern. Beispielsweise gleicht eine NetScaler-Appliance Lastausgleichsentscheidungen für einzelne HTTP-Anforderungen anstelle von langlebigen TCP-Verbindungen aus. Die Lastausgleichsfunktion hilft dabei, den Ausfall eines Servers zu verlangsamen und die Clients weniger zu unterbrechen. Die ADC-Funktionen können grob klassifiziert werden als:

1. Daten-Switching
2. Firewall-Sicherheit
3. Optimierung
4. Politische Infrastruktur
5. Paketfluss

Daten-Switching

Bei der Bereitstellung vor Anwendungsservern sorgt ein NetScaler für eine optimale Verteilung des Datenverkehrs, indem er Clientanfragen leitet. Administratoren können den Anwendungsverkehr nach Informationen im Text einer HTTP- oder TCP-Anfrage und basierend auf L4-L7-Header-Informationen wie URL, Anwendungsdatentyp oder Cookie segmentieren. Zahlreiche Lastausgleichsalgorithmen und umfangreiche Serverzustandsprüfungen verbessern die Anwendungsverfügbarkeit, indem sichergestellt wird, dass Clientanfragen an die entsprechenden Server geleitet werden.

Firewall-Sicherheit

Die Sicherheit und der Schutz von NetScaler schützen Webanwendungen vor Angriffen auf Application Layer. Eine ADC-Appliance ermöglicht legitime Clientanfragen und kann böswillige Anfragen blockieren. Es bietet integrierte Abwehrmaßnahmen gegen Denial-of-Service (DoS) -Angriffe und unterstützt Funktionen, die vor legitimen Überspannungen im Anwendungsverkehr schützen, die sonst die Server überfordern würden. Eine verfügbare integrierte Firewall schützt Webanwendungen vor Angriffen auf Application Layer, einschließlich Pufferüberlauf-Exploits, SQL-Einschleusungsversuchen, Cross-Site-Scripting-Angriffen und vielem mehr. Darüber hinaus bietet die Firewall Schutz vor Identitätsdiebstahl, indem sie vertrauliche Unternehmensinformationen und sensible Kundendaten schützt.

Optimierung

Durch die Optimierung werden ressourcenintensive Vorgänge wie Secure Sockets Layer (SSL) -Verarbeitung, Datenkomprimierung, Client-Keep-Alive, TCP-Pufferung und das Zwischenspeichern statischer und dynamischer Inhalte von Servern entlastet. Dies verbessert die Leistung der Server in der Serverfarm und beschleunigt daher Anwendungen. Eine ADC-Appliance unterstützt mehrere transparente TCP-Optimierungen, die Probleme reduzieren, die durch hohe Latenz und überlastete Netzwerkverbindungen verursacht werden. Dadurch wird die Bereitstellung von Anwendungen beschleunigt, ohne dass Konfigurationsänderungen an Clients oder Servern erforderlich sind.

Politische Infrastruktur

Eine Richtlinie definiert spezifische Details der Verkehrsfilterung und -verwaltung auf einem NetScaler. Es besteht aus zwei Teilen: dem Ausdruck und der Handlung. Der Ausdruck definiert die Arten von Anforderungen, mit denen die Richtlinie übereinstimmt. Die Aktion teilt der ADC-Appliance mit, was zu tun ist, wenn eine Anforderung mit dem Ausdruck übereinstimmt. Beispielsweise könnte der Ausdruck darin bestehen, ein bestimmtes URL-Muster für einen Sicherheitsangriff mit dem zu löschenden oder zurückzusetzen konfigurierten URL-Muster abzugleichen. Jede Richtlinie hat eine Priorität, und die Prioritäten bestimmen die Reihenfolge, in der die Richtlinien bewertet werden.

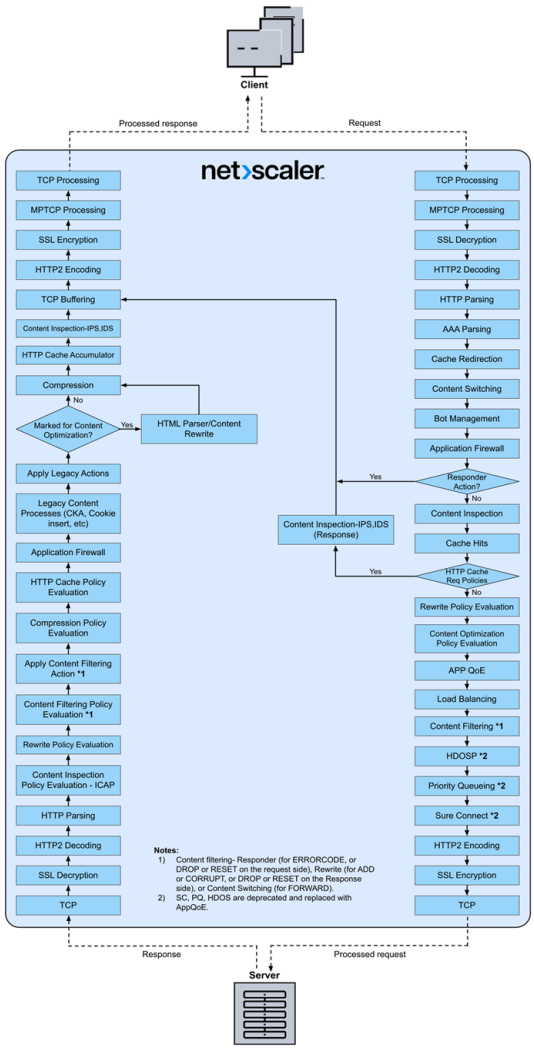
Wenn eine ADC-Appliance Datenverkehr empfängt, bestimmt die entsprechende Richtlinienliste, wie der Datenverkehr verarbeitet werden soll. Jede Richtlinie in der Liste enthält einen oder mehrere Ausdrücke, die zusammen die Kriterien definieren, die eine Verbindung erfüllen muss, um der Richtlinie zu entsprechen.

Für alle Richtlinientypen außer Umschreiben implementiert die Appliance nur die erste Richtlinie, die eine Anforderungsübereinstimmung aufweist. Bei Rewrite-Richtlinien wertet die ADC-Appliance die Richtlinien der Reihenfolge nach aus und führt die zugehörigen Aktionen in derselben Reihenfolge aus. Die Priorität der Richtlinien ist wichtig, um die gewünschten Ergebnisse zu erzielen.

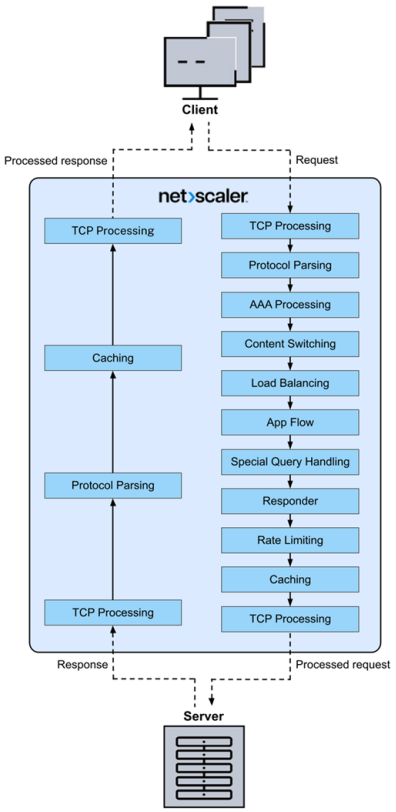
Paketfluss

Je nach Anforderung können Sie mehrere Funktionen konfigurieren. Sie können beispielsweise sowohl die Kompression als auch den SSL-Offload konfigurieren. Infolgedessen kann ein ausgehendes Paket komprimiert und dann verschlüsselt werden, bevor es an den Client gesendet wird.

Die folgende Abbildung zeigt den HTTP2-Paketfluss in der NetScaler-Appliance.



Die folgende Abbildung zeigt den Ablauf der Datenstream-Abfrageverarbeitung in der NetScaler-Appliance. DataStream wird für MySQL- und MS SQL-Datenbanken unterstützt. Informationen zur DataStream-Funktion finden Sie unter DataStream.



> **Hinweis:** Wenn der Datenverkehr für einen virtuellen Content Switching-Server ist, wertet die Appliance die Richtlinien in der folgenden Reihenfolge aus:
>
> 1. an globale Überschreibung gebunden.
> 2. an den virtuellen Lastausgleichsserver gebunden.
> 3. an den virtuellen Content Switching-Server gebunden.
> 4. an den globalen Standard gebunden.
>
> Auf diese Weise beenden wir die weitere Richtlinienbewertung, wenn eine Richtlinienregel wahr ist und gotoprioritytexpression END ist.
> Wenn Content Switching kein virtueller Lastausgleichsserver ausgewählt oder an den virtuellen Content-Switch-Server gebunden ist, bewerten wir die Responderrichtlinien, die nur an den virtuellen Content-Switch-Server gebunden sind.

Beschränkung des Systems

Bei der Installation von NetScaler Software 9.2 oder höher gibt es Systemeinschränkungen für jede NetScaler Funktion. Weitere Informationen finden Sie im Citrix-Artikel, CTX118716.

Wo passt eine NetScaler Appliance in das Netzwerk?

September 11, 2023

NetScaler befindet sich zwischen den Clients und Servern im Netzwerk. Es spielt die Rolle eines Vermittlers und verarbeitet den Verkehr zwischen Client und Server. Für den von den Clients kommenden Datenverkehr fungiert NetScaler als Server und empfängt die Anfragen. Nach Erhalt der Client-Anfrage sendet NetScaler im Namen des Clients eine neue Anfrage an den Server. Beim Senden der Anfrage an den Server fungiert NetScaler als Client.

Im Folgenden sind einige gängige Netzwerkbereitstellungen aufgeführt, für die NetScaler geeignet ist:

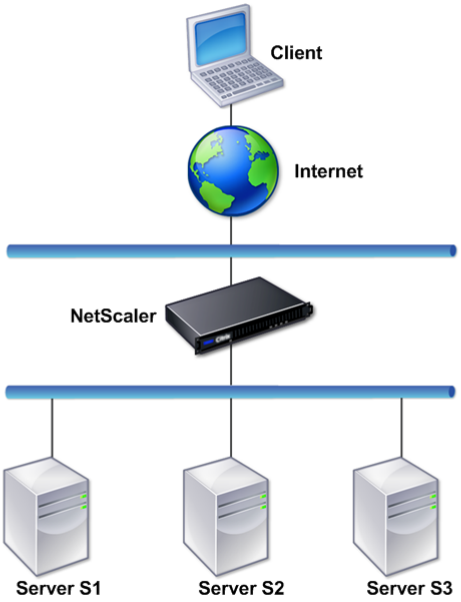
- **Gateway** — Sie können NetScaler als Gateway am Perimeter des internen Netzwerks (oder Intranets) Ihres Unternehmens verwenden, um einen sicheren zentralen Zugriffspunkt auf die Server, Anwendungen und andere Netzwerkressourcen bereitzustellen, die sich im internen Netzwerk befinden.
- **Anwendungsfirewall** — Sie können NetScaler als Anwendungsfirewall verwenden, um Sicherheitsverletzungen, Datenverlust und mögliche unbefugte Änderungen an Websites zu verhindern, die auf vertrauliche Geschäfts- oder Kundeninformationen zugreifen. Dazu filtert es sowohl Anfragen als auch Antworten, untersucht sie auf Hinweise auf böswillige Aktivitäten und blockiert Anfragen, die solche Aktivitäten aufweisen.
- **Load Balancer** — Sie können den NetScaler als Load Balancer verwenden, bei dem er Client-Anfragen auf mehrere Server verteilt, um die Ressourcennutzung zu optimieren. In einem realen Szenario mit einer begrenzten Anzahl von Servern, die Dienste für viele Clients bereitstellen, kann ein Server überlastet werden und die Leistung der Serverfarm beeinträchtigen. Eine NetScaler Appliance verwendet Lastausgleichskriterien, um Engpässe zu vermeiden, indem sie jede Client-Anfrage an den Server weiterleitet, der am besten für die Bearbeitung der Anfrage geeignet ist, wenn sie eingeht.
- **Globaler Server Load Balancer** — Sie können NetScaler als Global Server Load Balancer (GSLB) konfigurieren, um Disaster Recovery bereitzustellen und die kontinuierliche Verfügbarkeit von Anwendungen gegen Fehlerquellen in einem WAN sicherzustellen. GSLB verteilt die Last auf die Rechenzentren, indem es Kundenanfragen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder an überlebende Rechenzentren weiterleitet, falls es zu einem Ausfall kommt.
- **Paketweiterleitung —** Sie können NetScaler als Paketweiterleitung verwenden, um Pakete an eine IP weiterzuleiten, die ihm nicht gehört. NetScaler verhält sich wie ein Router und betrachtet die Routen, die er gelernt hat oder die für die Weiterleitung von Paketen konfiguriert wurden.

Physische Bereitstellungsmodi

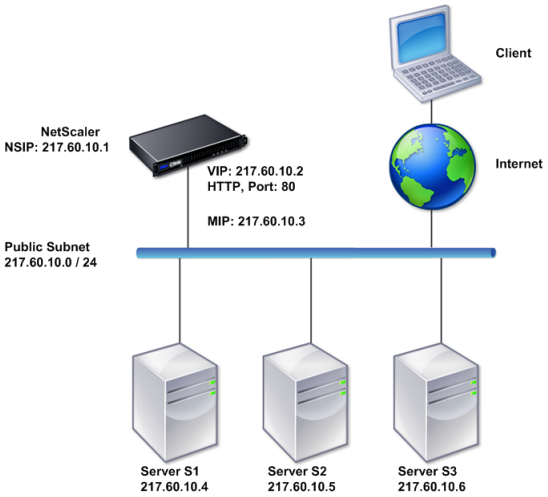
Eine NetScaler Appliance, die sich logisch zwischen Clients und Servern befindet, kann in einem von zwei physischen Modi bereitgestellt werden:

- Inline- oder Zweiarm-Modus
- Einarmiger Modus

Im Inline-Modus verwendet die Appliance mehrere Netzwerkschnittstellen, um eine Verbindung zu verschiedenen Ethernet-Segmenten herzustellen und positioniert sich so zwischen Clients und Servern. Es kann über eine oder mehrere redundante Schnittstellen eine Verbindung zum Servernetzwerk herstellen, und sowohl die Appliance als auch die Server können sich in separaten Subnetzen befinden. Es ist möglich, dass sich die Server in einem öffentlichen Netzwerk befinden und die Clients über die Appliance direkt auf die Server zugreifen können, wobei die Appliance die L4-L7-Funktionen transparent anwendet. Normalerweise werden virtuelle Server (später beschrieben) so konfiguriert, dass sie eine Abstraktion der realen Server bereitstellen. Die folgende Abbildung zeigt eine typische Inline-Bereitstellung.



Im Einarmmodus ist nur eine Netzwerkschnittstelle der Appliance mit einem Ethernet-Segment verbunden. Die Appliance isoliert in diesem Fall nicht die Client- und Serverseite des Netzwerks, sondern bietet Zugriff auf Anwendungen über konfigurierte virtuelle Server. Der Einarmmodus kann Netzwerkänderungen vereinfachen, die für die NetScaler-Installation in einigen Umgebungen erforderlich sind.



Beispiele für den Inline-Einsatz (zweiarmig) und einarmigen Einsatz finden Sie unter Grundlegendes zu gängigen Netzwerktopologien.

How a NetScaler appliance communicates with clients and servers

August 15, 2023

Eine NetScaler-Appliance wird normalerweise vor einer Serverfarm bereitgestellt und fungiert als transparenter TCP-Proxy zwischen Clients und Servern, ohne dass eine clientseitige Konfiguration erforderlich ist. Dieser grundlegende Betriebsmodus wird als Request Switching-Technologie bezeichnet und ist das Herzstück der NetScaler-Funktionalität. Request Switching ermöglicht es einer Appliance, die TCP-Verbindungen zu multiplexen und auszulagern, persistente Verbindungen aufrechtzuerhalten und den Datenverkehr auf Anforderungsebene (Andwendungslayer) zu verwalten. Dies ist möglich, weil die Appliance die HTTP-Anfrage von der TCP-Verbindung trennen kann, über die die Anfrage zugestellt wird.

Abhängig von der Konfiguration verarbeitet eine Appliance möglicherweise den Datenverkehr, bevor die Anfrage an einen Server weitergeleitet wird. Wenn der Client beispielsweise versucht, auf eine sichere Anwendung auf dem Server zuzugreifen, führt die Appliance möglicherweise die erforderliche SSL-Verarbeitung durch, bevor der Datenverkehr an den Server gesendet wird.

Um einen effizienten und sicheren Zugriff auf Serverressourcen zu ermöglichen, verwendet eine Appliance eine Reihe von IP-Adressen, die zusammen als Netscaler-eigene IP-Adressen bezeichnet werden. Um Ihren Netzwerkverkehr zu verwalten, weisen Sie NetScaler-eigene IP-Adressen virtuellen Entitäten zu, die zu den Bausteinen Ihrer Konfiguration werden. Um beispielsweise den Lastenausgleich

zu konfigurieren, erstellen Sie virtuelle Server, um Clientanfragen zu empfangen und sie an Dienste zu verteilen, bei denen es sich um Entitäten handelt, die die Anwendungen auf Ihren Servern repräsentieren.

Grundlegendes zu Netscaler-eigenen IP-Adressen

Um als Proxy zu fungieren, verwendet eine NetScaler-Appliance eine Vielzahl von IP-Adressen. Die wichtigsten Netscaler-eigenen IP-Adressen sind:

- NetScaler IP-Adresse (NSIP)

  Die NSIP-Adresse ist die IP-Adresse für die Verwaltung und den allgemeinen Systemzugriff auf die Appliance selbst sowie für die Kommunikation zwischen Appliances in einer Hochverfügbarkeitskonfiguration.

- IP-Adresse des virtuellen Servers (VIP)

  Eine VIP-Adresse ist die IP-Adresse, die einem virtuellen Server zugeordnet ist. Es ist die öffentliche IP-Adresse, mit der sich Clients verbinden. Auf einer Appliance, die ein breites Spektrum an Datenverkehr verwaltet, sind möglicherweise viele VIPs konfiguriert.

- Subnetz-IP-Adresse (SNIP)

  Eine SNIP-Adresse wird für die Verbindungsverwaltung und Serverüberwachung verwendet. Sie können mehrere SNIP-Adressen für jedes Subnetz angeben. SNIP-Adressen können an ein VLAN gebunden werden.

- IP-Satz

  Ein IP-Set ist ein Satz von IP-Adressen, die auf der Appliance als SNIP konfiguriert sind. Ein IP-Satz wird mit einem aussagekräftigen Namen identifiziert, der bei der Identifizierung der Verwendung der darin enthaltenen IP-Adressen hilft.

- Net-Profil

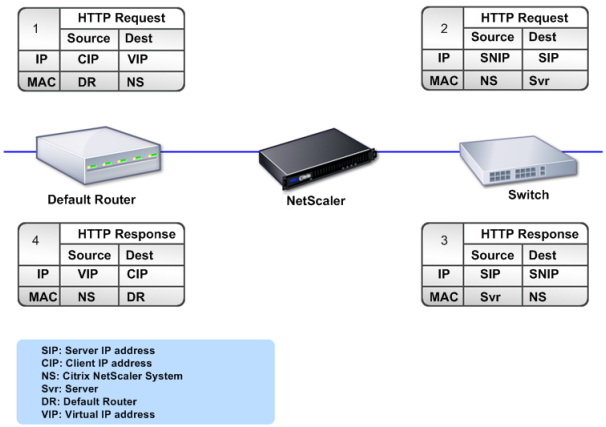
  Ein Netzprofil (oder Netzwerkprofil) enthält eine IP-Adresse oder einen IP-Satz. Ein Netzprofil kann an virtuelle Server, Dienste, Dienstgruppen oder Monitore mit Lastausgleich oder Content Switching gebunden werden. Während der Kommunikation mit physischen Servern oder Peers verwendet die Appliance die im Profil angegebenen Adressen als Quell-IP-Adressen.

Wie Verkehrsflüsse verwaltet werden

Da eine NetScaler-Appliance als TCP-Proxy fungiert, übersetzt sie IP-Adressen, bevor sie Pakete an einen Server sendet. Wenn Sie einen virtuellen Server konfigurieren, stellen Clients eine Verbindung zu einer VIP-Adresse auf der NetScaler-Appliance her, anstatt sich direkt mit einem Server zu verbinden. Wie durch die Einstellungen auf dem virtuellen Server bestimmt, wählt die Appliance

einen geeigneten Server aus und sendet die Anfrage des Clients an diesen Server. Standardmäßig verwendet die Appliance eine SNIP-Adresse, um Verbindungen mit dem Server herzustellen, wie in der folgenden Abbildung dargestellt.

Abbildung 1. Auf virtuellen Servern basierende Verbindungen



Wenn kein virtueller Server vorhanden ist, leitet eine Appliance, wenn sie eine Anfrage empfängt, die Anfrage transparent an den Server weiter. Dies wird als transparenter Betriebsmodus bezeichnet. Im transparenten Modus übersetzt eine Appliance die Quell-IP-Adressen eingehender Clientanforderungen in die SNIP-Adresse, ändert jedoch nicht die Ziel-IP-Adresse. Damit dieser Modus funktioniert, muss der L2- oder L3-Modus entsprechend konfiguriert werden.

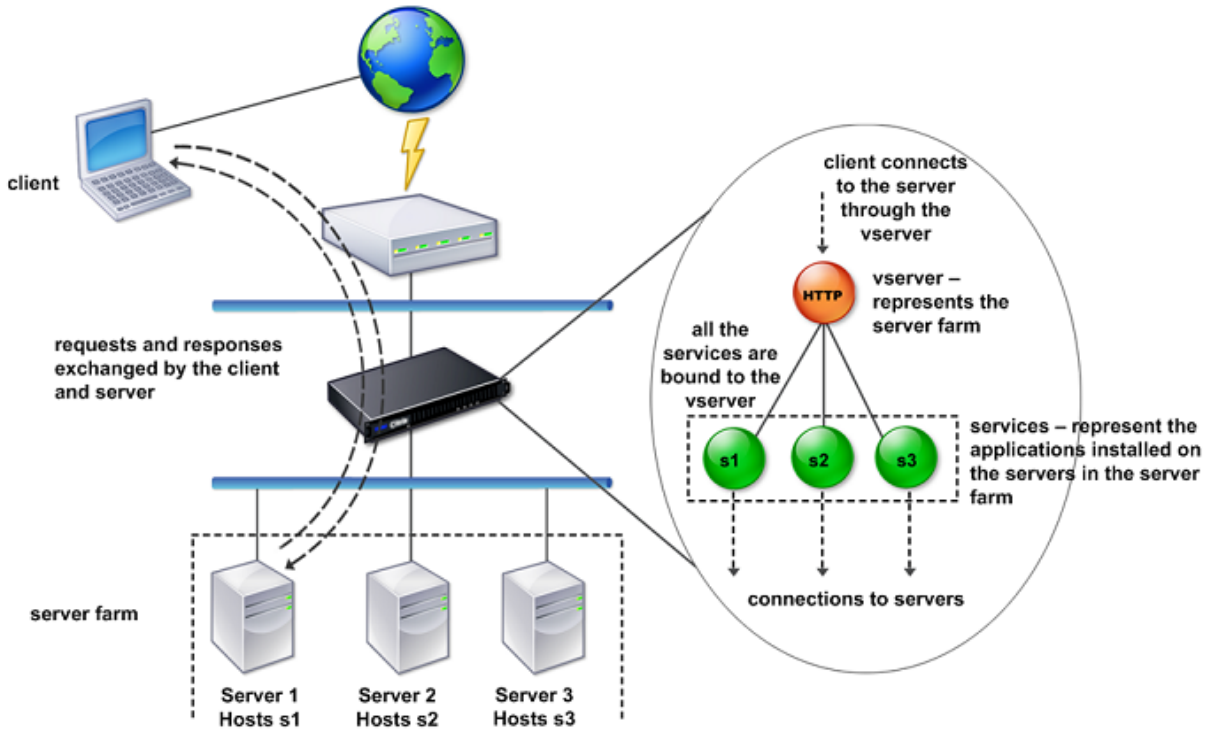
In Fällen, in denen die Server die tatsächliche Client-IP-Adresse benötigen, kann die Appliance so konfiguriert werden, dass sie den HTTP-Header ändert, indem die Client-IP-Adresse als zusätzliches Feld eingefügt wird, oder so konfiguriert werden, dass die Client-IP-Adresse anstelle einer SNIP-Adresse für Verbindungen zu den Servern verwendet wird.

Bausteine des Verkehrsmanagements

Die Konfiguration einer NetScaler-Appliance besteht in der Regel aus einer Reihe virtueller Entitäten, die als Bausteine für das Verkehrsmanagement dienen. Der Bausteinansatz hilft dabei, Verkehrsflüsse voneinander zu trennen. Virtuelle Entitäten sind Abstraktionen, die in der Regel IP-Adressen, Ports und Protokollhandler für die Verarbeitung des Datenverkehrs darstellen. Kunden greifen über diese virtuellen Entitäten auf Anwendungen und Ressourcen zu. Die am häufigsten verwendeten Entitäten sind virtuelle Server und Dienste. Virtuelle Server stellen Servergruppen in einer Serverfarm oder einem Remote-Netzwerk dar, und Dienste stellen spezifische Anwendungen auf jedem Server dar.

Die meisten Funktionen und Verkehrseinstellungen werden über virtuelle Entitäten aktiviert. Sie können beispielsweise eine Appliance so konfigurieren, dass sie alle Serverantworten an einen Client komprimiert, der über einen bestimmten virtuellen Server mit der Serverfarm verbunden ist. Um die Appliance für eine bestimmte Umgebung zu konfigurieren, müssen Sie die entsprechenden Funktionen identifizieren und dann die richtige Mischung virtueller Entitäten auswählen, um sie bereitzustellen. Die meisten Funktionen werden über eine Kaskade von virtuellen Entitäten bereitgestellt, die miteinander verbunden sind. In diesem Fall sind die virtuellen Entitäten wie Blöcke, die zur endgültigen Struktur einer bereitgestellten Anwendung zusammengesetzt werden. Sie können die virtuellen Entitäten hinzufügen, entfernen, ändern, binden, aktivieren und deaktivieren, um die Funktionen zu konfigurieren. Die folgende Abbildung zeigt die in diesem Abschnitt behandelten Konzepte.

Abbildung 2. So funktionieren die Bausteine des Verkehrsmanagements



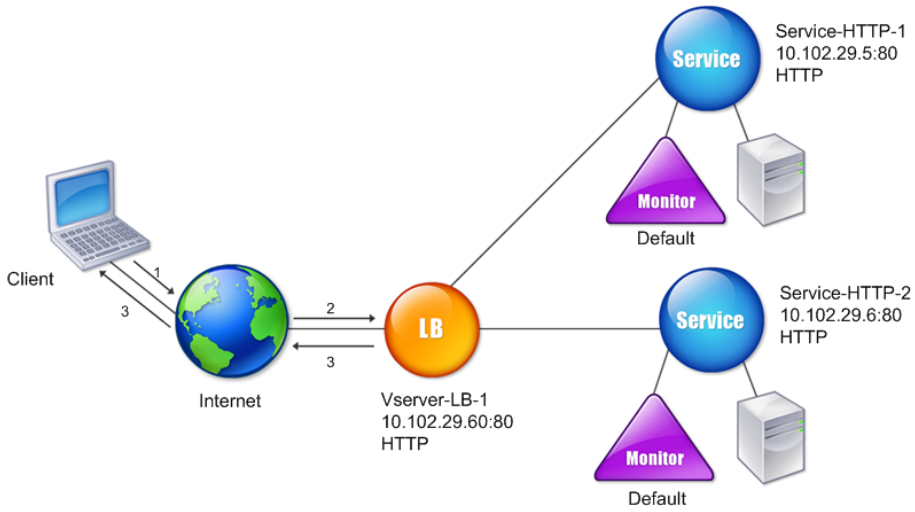
Eine einfache Load-Balancing-Konfiguration

In dem in der folgenden Abbildung gezeigten Beispiel ist die NetScaler-Appliance so konfiguriert, dass sie als Load Balancer fungiert. Für diese Konfiguration müssen Sie virtuelle Entitäten konfigurieren, die für den Lastenausgleich spezifisch sind, und sie in einer bestimmten Reihenfolge binden. Als Load Balancer verteilt eine Appliance Client-Anfragen auf mehrere Server und optimiert so die Auslastung der Ressourcen.

Die grundlegenden Bausteine einer typischen Load-Balancing-Konfiguration sind Dienste und

virtuelle Lastausgleichsserver. Die Dienste stellen die Anwendungen auf den Servern dar. Die virtuellen Server abstrahieren die Server, indem sie eine einzige IP-Adresse bereitstellen, zu der sich die Clients verbinden. Um sicherzustellen, dass Clientanfragen an einen Server gesendet werden, müssen Sie jeden Dienst an einen virtuellen Server binden. Das heißt, Sie müssen Dienste für jeden Server erstellen und die Dienste an einen virtuellen Server binden. Clients verwenden die VIP-Adresse, um eine Verbindung zu einer NetScaler-Appliance herzustellen. Wenn die Appliance an die VIP-Adresse gesendete Client-Anforderungen empfängt, sendet sie diese an einen Server, der durch den Load-Balancing-Algorithmus bestimmt wird. Load Balancing verwendet eine virtuelle Entität, die als Monitor bezeichnet wird, um zu verfolgen, ob ein bestimmter konfigurierter Dienst (Server plus Anwendung) für den Empfang von Anfragen verfügbar ist.

Abbildung 3. Lastausgleich für virtuelle Server, Dienste und Monitore



Neben der Konfiguration des Load Balancing-Algorithmus können Sie mehrere Parameter konfigurieren, die sich auf das Verhalten und die Leistung der Load-Balancing-Konfiguration auswirken. Sie können den virtuellen Server beispielsweise so konfigurieren, dass die Persistenz auf der Grundlage der Quell-IP-Adresse aufrechterhalten wird. Die Appliance leitet dann alle Anfragen von einer bestimmten IP-Adresse an denselben Server weiter.

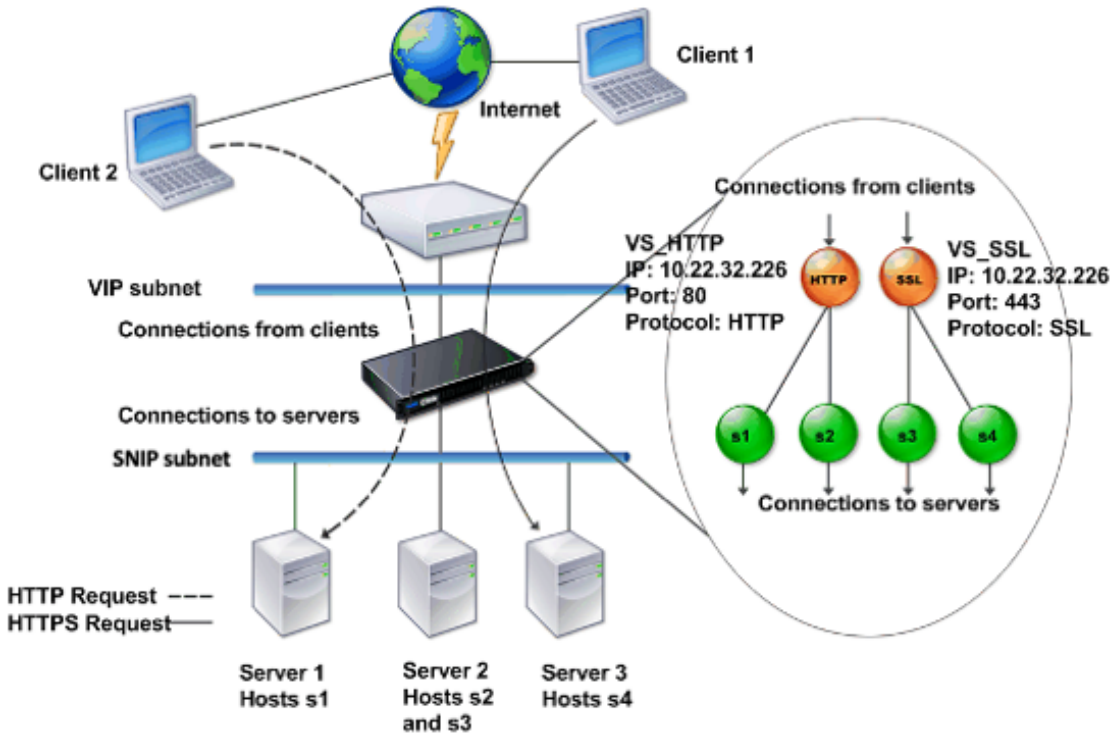
Grundlegendes zu virtuellen Servern

Ein virtueller Server ist eine benannte NetScaler-Entität, mit der externe Clients auf Anwendungen zugreifen können, die auf den Servern gehostet werden. Es wird durch einen alphanumerischen Namen, eine virtuelle IP-Adresse (VIP), einen Port und ein Protokoll dargestellt. Der Name des virtuellen Servers ist nur von lokaler Bedeutung und soll die Identifizierung des virtuellen Servers erleichtern. Wenn ein Client versucht, auf Anwendungen auf einem Server zuzugreifen, sendet er eine Anfrage an den VIP und nicht an die IP-Adresse des physischen Servers. Wenn die Appliance eine Anfrage an der VIP-Adresse empfängt, beendet sie die Verbindung auf dem virtuellen Server und verwendet im Namen des Clients ihre eigene Verbindung mit dem Server. Die Port- und Protokolleinstellungen des virtuellen Servers bestimmen die Anwendungen, die der virtuelle Server repräsentiert. Ein Webserver kann beispielsweise durch einen virtuellen Server und einen Dienst dargestellt werden, dessen Port und Protokoll auf 80 bzw. HTTP gesetzt sind. Mehrere virtuelle Server können dieselbe VIP-Adresse, aber unterschiedliche Protokolle und Ports verwenden.

Virtuelle Server sind Punkte für die Bereitstellung von Funktionen. Die meisten Funktionen wie Komprimierung, Caching und SSL-Offload sind normalerweise auf einem virtuellen Server aktiviert. Wenn die Appliance eine Anfrage an einer VIP-Adresse empfängt, wählt sie den entsprechenden virtuellen Server anhand des Port, an dem die Anfrage empfangen wurde, und des Protokolls aus. Die Appliance verarbeitet die Anfrage dann entsprechend den auf dem virtuellen Server konfigurierten Funktionen.

In den meisten Fällen arbeiten virtuelle Server mit Diensten zusammen. Sie können mehrere Dienste an einen virtuellen Server binden. Diese Dienste stellen die Anwendungen dar, die auf physischen Servern in einer Serverfarm ausgeführt werden. Nachdem die Appliance an einer VIP-Adresse eingegangene Anfragen verarbeitet hat, leitet sie diese an die Server weiter, wie durch den auf dem virtuellen Server konfigurierten Load-Balancing-Algorithmus festgelegt. Die folgende Abbildung veranschaulicht diese Konzepte.

Abbildung 4. Mehrere virtuelle Server mit einer einzigen VIP-Adresse



Die obige Abbildung zeigt eine Konfiguration, die aus zwei virtuellen Servern mit einer gemeinsamen VIP-Adresse, aber unterschiedlichen Ports und Protokollen besteht. An jeden der virtuellen Server sind zwei Dienste gebunden. Die Dienste s1 und s2 sind an VS_HTTP gebunden und repräsentieren die HTTP-Anwendungen auf Server 1 und Server 2. Die Dienste s3 und s4 sind an VS_SSL gebunden und repräsentieren die SSL-Anwendungen auf Server 2 und Server 3 (Server 2 stellt sowohl HTTP- als auch SSL-Anwendungen bereit). Wenn die Appliance eine HTTP-Anfrage an der VIP-Adresse empfängt, verarbeitet sie die Anfrage gemäß den Einstellungen von VS_HTTP und sendet sie entweder an Server 1 oder Server 2. In ähnlicher Weise verarbeitet die Appliance, wenn sie eine HTTPS-Anfrage an der VIP-Adresse empfängt, diese gemäß den Einstellungen von VS_SSL und sendet sie entweder an Server 2 oder Server 3.

Virtuelle Server werden nicht immer durch bestimmte IP-Adressen, Portnummern oder Protokolle repräsentiert. Sie können durch Platzhalter dargestellt werden. In diesem Fall werden sie als virtuelle Wildcard-Server bezeichnet. Wenn Sie beispielsweise einen virtuellen Server mit einem Platzhalter anstelle eines VIP, aber mit einer bestimmten Portnummer konfigurieren, fängt die Appliance den gesamten Datenverkehr ab und verarbeitet ihn, der diesem Protokoll entspricht und für den vordefinierten Port bestimmt ist. Bei virtuellen Servern mit Platzhaltern anstelle von VIPs und Portnummern fängt die Appliance den gesamten Datenverkehr ab und verarbeitet ihn protokollkonform.

Virtuelle Server können in die folgenden Kategorien eingeteilt werden:

- Lastenausgleich virtueller Server

  Empfängt Anfragen und leitet sie an einen geeigneten Server weiter. Die Auswahl des geeigneten Servers hängt davon ab, welche der verschiedenen Load-Balancing-Methoden der Benutzer konfiguriert.

- Virtueller Server für die Cache-Umleitung

  Leitet Clientanfragen für dynamischen Inhalt an Ursprungsserver und Anfragen für statischen Inhalt an Cache-Server weiter. Virtuelle Server für die Cache-Umleitung funktionieren häufig in Verbindung mit virtuellen Servern für den Lastenausgleich.

- Virtuelle Content Switching-Server

  Leitet den Datenverkehr auf der Grundlage des vom Client angeforderten Inhalts an einen Server weiter. Sie können beispielsweise einen virtuellen Content Switching-Server erstellen, der alle Client-Anforderungen für Bilder an einen Server weiterleitet, der nur Bilder bereitstellt. Virtuelle Content Switching-Server funktionieren häufig in Verbindung mit virtuellen Servern für den Lastenausgleich.

- Virtueller Server für virtuelles privates Netzwerk (VPN)

  Entschlüsselt getunnelten Datenverkehr und sendet ihn an Intranetanwendungen.

- Virtueller SSL-Server

  Empfängt und entschlüsselt SSL-Verkehr und leitet ihn dann an einen geeigneten Server weiter. Die Auswahl des geeigneten Servers ähnelt der Auswahl eines virtuellen Lastausgleichsservers.

Dienste verstehen

Dienste stellen Anwendungen auf einem Server dar. Während Dienste normalerweise mit virtuellen Servern kombiniert werden, kann ein Dienst in Ermangelung eines virtuellen Servers dennoch den anwendungsspezifischen Datenverkehr verwalten. Sie können beispielsweise einen HTTP-Dienst auf einer NetScaler-Appliance erstellen, um eine Webserveranwendung darzustellen. Wenn der Client versucht, auf eine auf dem Webserver gehostete Website zuzugreifen, fängt die Appliance die HTTP-Anfragen ab und stellt eine transparente Verbindung mit dem Webserver her.

Im Nur-Servicemodus fungiert eine Appliance als Proxy. Es beendet Clientverbindungen, verwendet eine SNIP-Adresse, um eine Verbindung zum Server herzustellen, und übersetzt die Quell-IP-Adressen eingehender Clientanfragen in eine SNIP-Adresse. Obwohl die Clients Anfragen direkt an die IP-Adresse des Servers senden, geht der Server davon aus, dass sie von der SNIP-Adresse stammen. Die Appliance übersetzt die IP-Adressen, Portnummern und Sequenznummern.

Ein Service ist auch ein Punkt, an dem Funktionen angewendet werden können. Betrachten Sie das Beispiel der SSL-Beschleunigung. Um diese Funktion verwenden zu können, müssen Sie einen SSL-Dienst erstellen und ein SSL-Zertifikat an den Dienst binden. Wenn die Appliance eine HTTPS-Anfrage

empfängt, entschlüsselt sie den Datenverkehr und sendet ihn im Klartext an den Server. Im Fall, in dem nur der Service verfügbar ist, kann nur ein begrenzter Funktionsumfang konfiguriert werden.

Dienste verwenden Entitäten, die als Monitore bezeichnet werden, um den Zustand von Anwendungen zu verfolgen. Jeder Dienst hat einen Standardmonitor, der auf dem Servicetyp basiert und an ihn gebunden ist. Wie in den auf dem Monitor konfigurierten Einstellungen angegeben, sendet die Appliance in regelmäßigen Abständen Sonden an die Anwendung, um deren Status zu ermitteln. Wenn die Sonden ausfallen, markiert die Appliance den Dienst als inaktiv. In solchen Fällen reagiert die Appliance auf Clientanfragen mit einer entsprechenden Fehlermeldung oder leitet die Anfrage entsprechend den konfigurierten Load-Balancing-Richtlinien weiter.

Weitere Informationen zur Konfiguration von virtuellen Servern, Diensten und Monitoren für den Lastenausgleich finden Sie unter NetScaler LoadBalancing.

Einführung in die NetScaler-Produktlinie

September 1, 2023

Die NetScaler-Produktlinie optimiert die Bereitstellung von Anwendungen über das Internet und private Netzwerke und kombiniert Sicherheit, Optimierung und Verkehrsmanagement auf Anwendungsebene in einer einzigen, integrierten Appliance. Sie können eine NetScaler Appliance in Ihrem Serverraum installieren und alle Verbindungen zu Ihren verwalteten Servern darüber weiterleiten. Die NetScaler-Funktionen, die Sie aktivieren, und die von Ihnen festgelegten Richtlinien werden dann auf eingehenden und ausgehenden Datenverkehr angewendet.

Eine NetScaler Appliance kann als Ergänzung zu vorhandenen Load Balancern, Servern, Caches und Firewalls in jedes Netzwerk integriert werden. Es erfordert keine zusätzliche client- oder serverseitige Software und kann mit den webbasierten GUI- und CLI-Konfigurationsdienstprogrammen von NetScaler konfiguriert werden.

Dieses Artikel enthält die folgenden Abschnitte:

- NetScaler-Hardwareplattformen
- NetScaler-Editionen
- Unterstützte Versionen auf ADC-Hardware
- Unterstützte Browser

NetScaler-Hardwareplattformen

NetScaler-Hardware ist auf einer Vielzahl von Plattformen mit einer Reihe von Hardwarespezifikationen verfügbar:

NetScaler MPX-Hardwareplattform

NetScaler SDX-Hardwareplattform

NetScaler-Editionen

Das NetScaler-Betriebssystem ist in zwei Editionen erhältlich:

- Advanced
- Premium

Funktionen werden auf der Grundlage der Lizenz aktiviert.

Weitere Informationen zu NetScaler-Softwareversionen finden Sie im Datenblatt der NetScaler Editions.

Unterstützte Versionen auf NetScaler Hardware

In den folgenden Kompatibilitätsmatrixtabellen finden Sie alle NetScaler-Hardwareplattformen und die auf diesen Plattformen unterstützten Softwareversionen:

NetScaler MPX Hardwaresoftware-Kompatibilitätsmatrix

NetScaler SDX Hardware-Software-Kompatibilitätsmatrix

Kompatible Browser

Um auf die NetScaler GUI zuzugreifen, muss Ihre Arbeitsstation über einen kompatiblen Webbrowser verfügen.

In der folgenden Tabelle sind die kompatiblen Browser für NetScaler GUI Version 12.0, 12.1 und 13.0 aufgeführt:

Betriebssystem	Browser	Versionen
Windows 7 und höher	Internet Explorer	11, Edge und später
Windows 7 und höher	Mozilla Firefox	45 und später
Windows 7 und höher	Chrome	60 und später
MAC	Mozilla Firefox	45 und später
MAC	Safari	10.1.1 und später

Die kompatiblen Browserversionen für NetScaler 11.1 lauten wie folgt:

Betriebssystem	Browser	Versionen
Windows 7 und höher	Internet Explorer	8, 9, 10, 11, Rand
Windows 7 und höher	Mozilla Firefox	45 und später
Windows 7 und höher	Chrome	60 und später
MAC	Mozilla Firefox	45 und später
MAC	Safari	10.1.1 und später

Hardware installieren

May 11, 2023

Bevor Sie eine NetScaler-Appliance installieren, lesen Sie die Checkliste vor der Installation.

Um die SDX-Appliance zu verwenden, müssen Sie die folgenden Aufgaben ausführen, indem Sie den Anweisungen in den Ressourcen in der Tabelle folgen. Erledigen Sie die Aufgaben in der angegebenen Reihenfolge.

Aufgabe

Beschreibung

1. Lesen Sie Sicherheitsinformationen, Vorsichtsmaßnahmen, Warnungen und andere Informationen

   Lesen Sie die Warnhinweise und Gefahreninformationen, die Sie kennen müssen, bevor Sie das Produkt installieren.

2. Vorbereitung für die Installation

   Packen Sie Ihr Gerät aus und stellen Sie sicher, dass alle Teile geliefert wurden, bereiten Sie den Standort und das Rack vor und befolgen Sie die grundlegenden elektrischen Sicherheitsvorkehrungen, bevor Sie Ihr neues Gerät installieren.

3. Hardware installieren

   Montieren Sie die Appliance im Rack, installieren Sie Transceiver (falls verfügbar) und verbinden Sie die Appliance mit dem Netzwerk und einer Stromquelle.

4. Konfigurieren Sie die Appliance.

   Konfigurieren Sie die Anfangseinstellungen der NetScaler-Appliance mithilfe der GUI oder der seriellen Konsole.

   Folgen Sie den Schritten in den folgenden Dokumentationen, um diese Aufgaben abzuschließen:

- NetScaler MPX-Hardwaredokumentation
- NetScaler SDX-Hardwaredokumentation

Greifen Sie auf eine NetScaler-Appliance zu

May 11, 2023

Eine NetScaler Appliance verfügt sowohl über eine Befehlszeilenschnittstelle (CLI) als auch über eine GUI. Die GUI enthält ein Konfigurationsprogramm für die Konfiguration der Appliance und ein statistisches Hilfsprogramm namens Dashboard. Für den ersten Zugriff werden alle Appliances mit der standardmäßigen NetScaler IP-Adresse (NSIP) 192.168.100.1 und der Standardsubnetzmaske von 255.255.0.0 geliefert. Sie können bei der Erstkonfiguration ein neues NSIP und eine zugehörige Subnetzmaske zuweisen.

Wenn bei der Bereitstellung mehrerer NetScaler-Einheiten ein IP-Adresskonflikt auftritt, überprüfen Sie die folgenden möglichen Ursachen:

- Haben Sie ein NSIP ausgewählt, bei dem es sich um eine IP-Adresse handelt, die bereits einem anderen Gerät in Ihrem Netzwerk zugewiesen wurde?
- Haben Sie dasselbe NSIP mehreren NetScaler Appliances zugewiesen?
- Das NSIP ist an allen physischen Ports erreichbar. Die Ports auf einem NetScaler sind Host-Ports, keine Switch-Ports.

In der folgenden Tabelle sind die verfügbaren Zugriffsmethoden zusammengefasst.

Access-Methode	Port	Standard-IP-Adresse erforderlich? (JA/N)
CLI	Konsole	N
CLI und GUI	Ethernet	J

Befehlszeilenschnittstelle

Greifen Sie lokal auf die CLI zu, indem Sie eine Workstation mit dem Konsolenport verbinden, oder remote, indem Sie eine Verbindung über die Secure Shell (SSH) von einer beliebigen Workstation im selben Netzwerk aus herstellen.

Melden Sie sich über den Konsolenport an der Befehlszeilenschnittstelle an

Die Appliance verfügt über einen Konsolenanschluss für den Anschluss an eine Computerarbeitsstation. Um sich an der Appliance anzumelden, benötigen Sie ein serielles Crossover-Kabel und eine Workstation mit einem Terminal-Emulationsprogramm.

Gehen Sie wie folgt vor, um sich über den Konsolenport bei der CLI anzumelden:

1. Schließen Sie den Konsolenanschluss an einen seriellen Anschluss an der Workstation an. Weitere Informationen finden Sie unter Verbinden des Konsolenkabels.
2. Starten Sie HyperTerminal oder ein anderes Terminal-Emulationsprogramm auf der Workstation. Wenn die Anmeldeaufforderung nicht angezeigt wird, müssen Sie möglicherweise ein- oder mehrmals die EINGABETASTE drücken, um sie anzuzeigen.
3. Geben Sie im Feld Benutzername den Wert ein `nsroot`. Geben Sie unter Kennwort `nsroot` ein und falls das Kennwort nicht funktioniert, versuchen Sie, die Seriennummer der Appliance einzugeben. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar.

Melden Sie sich mit SSH an der Befehlszeilenschnittstelle an

Das SSH-Protokoll ist die bevorzugte Remotezugriffsmethode für den Remotezugriff auf eine Appliance von jeder Workstation im selben Netzwerk aus. Sie können entweder SSH Version 1 (SSH1) oder SSH Version 2 (SSH2) verwenden.

Wenn Sie keinen funktionierenden SSH-Client haben, können Sie eines der folgenden SSH-Client-Programme herunterladen und installieren:

- PuTTY

  Open-Source-Software, die auf mehreren Plattformen unterstützt wird. Erhältlich bei:

  http://www.chiark.greenend.org.uk/~sgtatham/putty/

- `Vandyke` Software SecureCRT

  Kommerzielle Software, die auf der Windows-Plattform unterstützt wird. Erhältlich bei:

  http://www.vandyke.com/products/securecrt/

Diese Programme werden vom NetScaler-Team getestet, das überprüft hat, dass sie mit einer NetScaler-Appliance ordnungsgemäß funktionieren. Andere Programme funktionieren möglicherweise ebenfalls korrekt, wurden jedoch nicht getestet.

Um zu überprüfen, ob der SSH-Client ordnungsgemäß installiert ist, verwenden Sie ihn, um eine Verbindung zu einem beliebigen Gerät in Ihrem Netzwerk herzustellen, das SSH-Verbindungen akzeptiert.

Gehen Sie wie folgt vor, um sich mit einem SSH-Client bei einer NetScaler Appliance anzumelden:

1. Starten Sie auf Ihrer Workstation den SSH-Client.

2. Verwenden Sie für die Erstkonfiguration die Standard-IP-Adresse (NSIP), die 192.168.100.1 lautet. Verwenden Sie für den nachfolgenden Zugriff das NSIP, das bei der Erstkonfiguration zugewiesen wurde. Wählen Sie entweder SSH1 oder SSH2 als Protokoll aus.
3. Geben Sie im Feld Benutzername den Wert ein `nsroot`. Geben Sie unter Kennwort `nsroot` ein und falls das Kennwort nicht funktioniert, versuchen Sie, die Seriennummer der Appliance einzugeben. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar. Zum Beispiel.

```
login as: nsroot


Using keyboard-interactive authentication.


Password:


Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9




Done


>

<!--NeedCopy-->
```

NetScaler-Benutzeroberfläche

> **Wichtig:**
>
> Für den HTTPS-Zugriff auf die Citric ADC GUI ist ein Zertifikatsschlüsselpaar erforderlich. Auf dem ADC wird ein Zertifikatsschlüsselpaar automatisch an die internen Dienste gebunden. Auf einer MPX- oder SDX-Appliance beträgt die Standardschlüsselgröße 1024 Byte, und bei einer VPX-Instanz beträgt die Standardschlüsselgröße 512 Byte. Die meisten Browser akzeptieren heute jedoch keinen Schlüssel mit weniger als 1024 Bytes. Infolgedessen wird der HTTPS-Zugriff auf das VPX-Konfigurationsdienstprogramm blockiert.

Wenn auf einer MPX-Appliance beim Start keine Lizenz vorhanden ist und Sie später eine Lizenz hinzufügen und die Appliance neu starten, verlieren Sie möglicherweise die Zertifikatsbindung.

Citrix empfiehlt, dass Sie für den HTTPS-Zugriff auf die GUI ein Zertifikatsschlüsselpaar von mindestens 1024 Byte auf der Appliance installieren. Installieren Sie außerdem eine entsprechende Lizenz, bevor Sie die Appliance starten.

Die GUI umfasst ein Konfigurations- und ein Statistikprogramm namens Dashboard, auf die Sie jeweils über eine Workstation zugreifen können, die mit einem Ethernet-Port der Appliance verbunden ist.

Die Systemanforderungen für die Workstation, auf der die GUI ausgeführt wird, lauten wie folgt:

- Für Windows-basierte Workstations ein Pentium-Prozessor mit 166 MHz oder schneller.
- Für Linux-basierte Workstations eine Pentium-Plattform mit Linux-Kernel v2.2.12 oder höher und `glibc` Version 2.12—11 oder höher. Es sind mindestens 32 MB RAM erforderlich, und 48 MB RAM werden empfohlen. Die Workstation muss den 16-Bit-Farbmodus sowie die zusammen verwendeten KDE- und KWM-Fenstermanager unterstützen, wobei die Displays auf lokale Hosts eingestellt sind.
- Für Solaris-basierte Workstations eine Sun, auf der entweder Solaris 2.6, Solaris 7 oder Solaris 8 ausgeführt wird.

Ihre Workstation muss über einen unterstützten Webbrowser verfügen, um auf das Konfigurationsprogramm und das Dashboard zugreifen zu können.

In der folgenden Tabelle sind die kompatiblen Browser für NetScaler GUI Version 12.1, 13.0 und 13.1 aufgeführt:

Betriebssystem	Browser	Versionen
Windows 10 und später	Edge	110.1587.63 und später
Windows 10 und später	Mozilla Firefox	102 und später
Windows 10 und später	Chrome	108 und später
MAC	Mozilla Firefox	110.0.1 und später
MAC	Safari	15.5 und später

Verwenden der NetScaler GUI

Sobald Sie sich beim Konfigurationsprogramm angemeldet haben, können Sie die Appliance über eine grafische Oberfläche konfigurieren, die kontextsensitive Hilfe enthält.

Gehen Sie wie folgt vor, um sich an der GUI anzumelden:

1. Öffnen Sie Ihren Webbrowser und geben Sie die NetScaler IP (NSIP) als HTTP-Adresse ein. Wenn Sie die Erstkonfiguration noch nicht eingerichtet haben, geben Sie das Standard-NSIP (http://192.168.100.1) ein. Die NetScaler-Anmeldeseite wird angezeigt.

Hinweis: Wenn Sie zwei NetScaler-Appliances in einem Hochverfügbarkeits-Setup haben, greifen Sie nicht auf die GUI zu, indem Sie die IP-Adresse der sekundären NetScaler-Appliance eingeben. Wenn Sie dies tun und die GUI verwenden, um die sekundäre Appliance zu konfigurieren, werden Ihre Konfigurationsänderungen nicht auf die primäre NetScaler Appliance angewendet.

2. Geben Sie in das Textfeld Benutzername Folgendes ein `nsroot`.
3. Geben Sie in das Textfeld Kennwort das Administratorkennwort ein, das Sie dem `nsroot` Konto bei der Erstkonfiguration zugewiesen haben, und klicken Sie auf **Anmelden**. Wenn das Passwort nicht funktioniert, versuchen Sie, die Seriennummer der Appliance einzugeben. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar.

   Um auf die Online-Hilfe zuzugreifen, wählen Sie im Hilfemenü oben rechts die Option Hilfe aus.

Verwenden Sie das Statistische Hilfsprogramm

Dashboard, das statistische Hilfsprogramm, ist eine browserbasierte Anwendung, die Diagramme und Tabellen anzeigt, auf denen Sie die Leistung einer NetScaler Appliance überwachen können.

Gehen Sie wie folgt vor, um sich im Dashboard anzumelden:

1. Öffnen Sie Ihren Webbrowser und geben Sie das NSIP als HTTP-Adresse ein. Die NetScaler-Anmeldeseite wird angezeigt.
2. Geben Sie in das Textfeld Benutzername Folgendes ein `nsroot`.
3. Geben Sie in das Textfeld Kennwort das Administratorkennwort ein, das Sie dem `nsroot` Konto bei der Erstkonfiguration zugewiesen haben. Wenn das Passwort nicht funktioniert, versuchen Sie, die Seriennummer der Appliance einzugeben. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar.

Erstkonfiguration von ADC

June 2, 2023

Informationen zur Erstkonfiguration einer NetScaler MPX-Appliance finden Sie unter Erstkonfiguration einer NetScaler MPX-Appliance.

Informationen zur Erstkonfiguration einer NetScaler SDX-Appliance finden Sie unter Erstkonfiguration einer NetScaler SDX-Appliance.

NITRO API

Sie können die NITRO-API verwenden, um die NetScaler-Appliance zu konfigurieren. NITRO stellt seine Funktionalität durch Representational State Transfer (REST) -Schnittstellen zur Verfügung. Daher können NITRO-Anwendungen in jeder Programmiersprache entwickelt werden. Für Anwendungen, die in Java oder .NET oder Python entwickelt werden müssen, werden NITRO-APIs über relevante Bibliotheken bereitgestellt, die als separate Software Development Kits (SDKs) verpackt sind. Weitere Informationen finden Sie unter NITRO-API.

Sichern der NetScaler-Bereitstellung

May 11, 2023

Um die Sicherheit während des gesamten Bereitstellungszyklus der NetScaler-Appliance zu gewährleisten, empfiehlt Citrix, die folgenden Sicherheitsaspekte zu berücksichtigen:

- Physische Sicherheit
- Gerätesicherheit
- Netzwerksicherheit
- Verwaltung und Verwaltung

Verschiedene Bereitstellungen können unterschiedliche Sicherheitsüberlegungen erfordern. Die Richtlinien zur sicheren Bereitstellung von NetScaler bieten allgemeine Sicherheitshinweise, die Ihnen bei der Entscheidung für eine geeignete sichere Bereitstellung basierend auf Ihren speziellen Sicherheitsanforderungen helfen.

Weitere Informationen zu Richtlinien für die sichere Bereitstellung der NetScaler Appliance finden Sie unter Richtlinien für sichere Bereitstellung von NetScaler.

Konfigurieren der Hochverfügbarkeit

May 11, 2023

Sie können zwei NetScaler-Appliances in einer Hochverfügbarkeitskonfiguration bereitstellen, bei der eine Einheit aktiv Verbindungen akzeptiert und Server verwaltet, während die sekundäre Einheit die erste überwacht. Die NetScaler-Appliance, die aktiv Verbindungen akzeptiert und die Server verwaltet, wird in einer Hochverfügbarkeitskonfiguration als primäre Einheit und die andere als sekundäre Einheit bezeichnet. Tritt in der Primäreinheit ein Fehler auf, wird die Sekundäreinheit zur primären Einheit und beginnt, Verbindungen aktiv anzunehmen.

Jede NetScaler-Appliance in einem Hochverfügbarkeitspaar überwacht die andere, indem sie in regelmäßigen Abständen Nachrichten, sogenannte Heartbeat-Meldungen oder Integritätsprüfungen, sendet, um den Zustand oder Status des Peer-Knotens zu ermitteln. Wenn eine Zustandsprüfung für eine primäre Einheit fehlschlägt, versucht die sekundäre Einheit die Verbindung für einen bestimmten Zeitraum erneut. Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Wenn ein Wiederholungsversuch bis zum Ende des angegebenen Zeitraums nicht erfolgreich ist, übernimmt die sekundäre Einheit für die primäre Einheit in einem Prozess namens Failover. Die folgende Abbildung zeigt zwei Hochverfügbarkeitskonfigurationen, eine im einarmigen Modus und die andere im zweiarmigen Modus.

Abbildung 1. Hohe Verfügbarkeit im Einarm-Modus

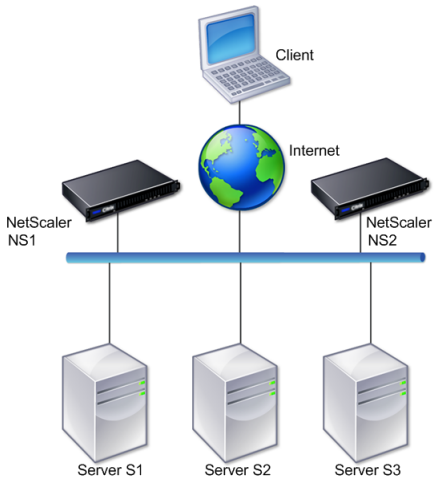
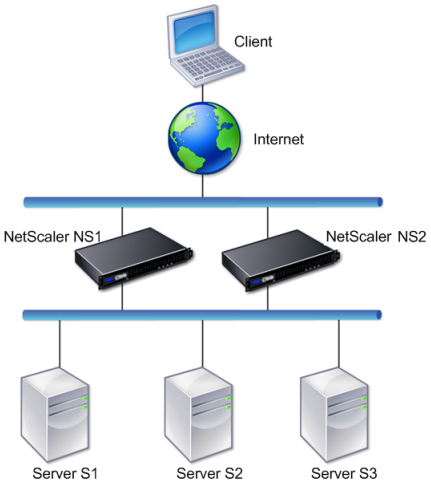


Abbildung 2. Hohe Verfügbarkeit im Zweiarm-Modus



In der einarmigen Konfiguration sind sowohl NS1 als auch NS2 und die Server S1, S2 und S3 mit dem Switch verbunden.

In einer Konfiguration mit zwei Armen sind sowohl NS1 als auch NS2 mit zwei Switches verbunden. Die Server S1, S2 und S3 sind mit dem zweiten Switch verbunden. Der Datenverkehr zwischen dem Client und den Servern wird entweder über NS1 oder NS2 geleitet.

Um eine Hochverfügbarkeitsumgebung einzurichten, konfigurieren Sie eine ADC-Appliance als primäres und ein anderes als sekundäres Gerät. Führen Sie die folgenden Aufgaben auf jeder ADC-Appliance aus:

- Fügen Sie einen Knoten hinzu.
- Deaktivieren Sie die Hochverfügbarkeitsüberwachung für ungenutzte Schnittstellen.

Einen Knoten hinzufügen

Ein Knoten ist eine logische Darstellung einer Peer-NetScaler-Appliance. Es identifiziert die Peer-Einheit anhand von ID und NSIP. Eine Appliance verwendet diese Parameter, um mit dem Peer zu kommunizieren und seinen Status zu verfolgen. Wenn Sie einen Knoten hinzufügen, tauschen die Primär- und Sekundäreinheiten asynchron Heartbeat-Nachrichten aus. Die Knoten-ID ist eine Ganzzahl, die nicht größer als 64 sein darf.

Über CLI

Gehen Sie folgendermaßen vor, um mithilfe der Befehlszeilenschnittstelle einen Knoten hinzuzufügen:

Geben Sie in der Befehlszeile die folgenden Befehle ein, um einen Knoten hinzuzufügen, und überprüfen Sie, ob der Knoten hinzugefügt wurde:

- add HA node <id> <IPAddress>
- show HA node <id>

  Beispiel

```
add HA node 0 10.102.29.170
 Done
> show HA node 0
1)      Node ID:      0
        IP:   10.102.29.200 (NS200)
        Node State: UP
        Master State: Primary
        SSL Card Status: UP
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 1:0:41:50 (days:hrs:min:
           sec)
<!--NeedCopy-->
```

Über die GUI

Gehen Sie folgendermaßen vor, um mithilfe der GUI einen Knoten hinzuzufügen:

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Klicken Sie auf der Registerkarte **Knoten** auf **Hinzufügen** .
3. Geben Sie auf der Seite **HA-Knoten erstellen** in das Textfeld **IP-Adresse des Remote-Knotens** die NSIP-Adresse (z. B. 10.102.29.170) des Remote-Knotens ein.
4. Vergewissern Sie sich, dass das Kontrollkästchen **Remotesystem für die Teilnahme am Hochverfügbarkeits-Setup konfigurieren** aktiviert ist. Geben Sie die Anmeldeinformationen des Remote-Knotens in die Textfelder unter **Anmeldeinformationen für das Remotesystem ein**.
5. Markieren Sie das Kontrollkästchen **HA-Monitor auf inaktiven Schnittstellen/Kanälen ausschalten, um den HA-Monitor auf ausgefallen** Schnittstellen zu deaktivieren.

Stellen Sie sicher, dass der von Ihnen hinzugefügte Knoten in der Liste der Knoten auf der Registerkarte Knoten erscheint.

Deaktivieren Sie die Hochverfügbarkeitsüberwachung für ungenutzte Schnittstellen

Der High Availability Monitor ist eine virtuelle Entität, die eine Schnittstelle überwacht. Sie müssen den Monitor für Schnittstellen deaktivieren, die nicht angeschlossen sind oder nicht für den Daten-

verkehr verwendet werden. Wenn der Monitor auf einer Schnittstelle aktiviert ist, deren Status DOWN ist, wird der Status des Knotens NICHT AKTIV. In einer Hochverfügbarkeitskonfiguration kann ein primärer Knoten, der in den Status NOT UP wechselt, zu einem Hochverfügbarkeits-Failover führen. Eine Schnittstelle wird unter den folgenden Bedingungen als DOWN markiert:

- Die Schnittstelle ist nicht angeschlossen
- Die Schnittstelle funktioniert nicht richtig
- Das Kabel, das die Schnittstelle verbindet, funktioniert nicht richtig

Über CLI

Gehen Sie folgendermaßen vor, um den Hochverfügbarkeitsmonitor für eine ungenutzte Schnittstelle mithilfe der Befehlszeilenschnittstelle zu deaktivieren:

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den Hochverfügbarkeitsmonitor für eine ungenutzte Schnittstelle zu deaktivieren und zu überprüfen, ob er deaktiviert ist:

- set interface <id> -haMonitor OFF
- show interface <id>

  Beispiel

```
> set interface 1/8 -haMonitor OFF
 Done
> show interface 1/8
        Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
        flags=0x4000 <ENABLED, DOWN, down, autoneg, 802.1q>
        MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d, downtime
           238h55m44s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
                 throughput 0

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
           Muted(0)
        Bandwidth thresholds are not set.
<!--NeedCopy-->
```

  Wenn der Hochverfügbarkeitsmonitor für eine ungenutzte Schnittstelle deaktiviert ist, enthält die Ausgabe des Befehls show interface für diese Schnittstelle nicht „HAMON“. „

Über die GUI

Gehen Sie folgendermaßen vor, um den Hochverfügbarkeitsmonitor für ungenutzte Schnittstellen mithilfe der GUI zu deaktivieren:

1. Navigieren Sie zu System > Netzwerk > Schnittstellen.
2. Wählen Sie die Schnittstelle aus, für die der Monitor deaktiviert werden muss.
3. Klicken Sie auf Öffnen. Das Dialogfeld „Schnittstelle ändern“ wird angezeigt.
4. Wählen Sie in HA Monitoring die Option AUS.
5. Klicken Sie auf OK.
6. Stellen Sie sicher, dass bei Auswahl der Schnittstelle in den Details unten auf der Seite „HA-Überwachung: AUS“ angezeigt wird.

Ändern eines RPC-Knotenkennworts

May 11, 2023

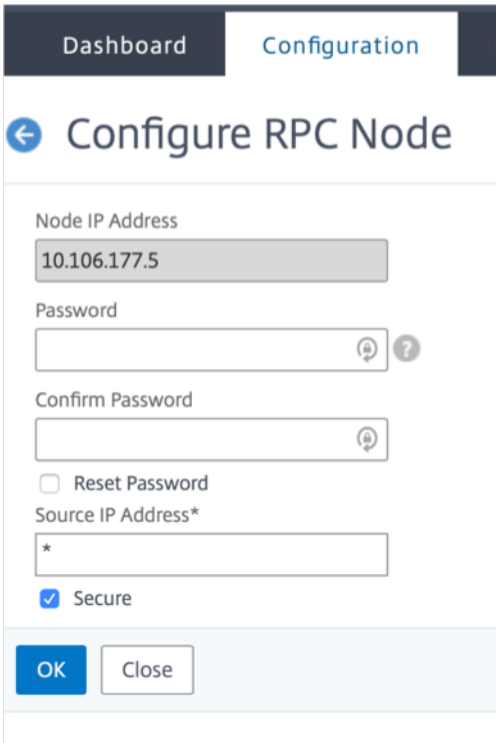
Für die Kommunikation mit anderen NetScaler Appliances erfordert jede Appliance Kenntnisse der anderen Appliances, einschließlich der Authentifizierung auf der NetScaler Appliance. RPC-Knoten sind interne Systementitäten, die für die System-zu-System-Kommunikation von Konfigurations- und Sitzungsinformationen verwendet werden. Auf jeder NetScaler Appliance ist ein RPC-Knoten vorhanden, in dem Informationen gespeichert werden, z. B. die IP-Adressen der anderen NetScaler Appliance und die für die Authentifizierung verwendeten Kennwörter. Die NetScaler Appliance, die die andere NetScaler Appliance kontaktiert, überprüft das Kennwort im RPC-Knoten.

> **Hinweis:**
>
> Nachdem Sie eine NetScaler-Appliance von einem der folgenden Builds auf Version 13.1 Build 33.x oder höher aktualisiert haben, wird die `secure` Option für den RPC-Knoten auf der Grundlage der TLS 1.2-Einstellung (aktiviert oder deaktiviert) aktiviert oder deaktiviert, die für die internen RPCS- und KRPCS-Dienste vorhanden ist.
>
> - Version 13.0 Build 64.35 oder früher
> - Version 12.1 Build 61.18 oder früher
>
> Die RPC-Kommunikation wird zwischen den NetScaler-Knoten der folgenden Setups verschlüsselt, wenn die Option `Secure` aktiviert ist:
>
> - Hohe Verfügbarkeit
> - Cluster
> - GSLB
>
> Die Option `secure` verwendet das sichere Protokoll TLS1.2 und die Portnummern 3008 und 3009

> für die RPC-Verbindung zwischen den NetScaler-Knoten.
>
> Um eine sichere RPC-Kommunikation zu gewährleisten, empfiehlt Citrix, vor dem Upgrade dieser Setups die folgenden Vorgänge durchzuführen:
>
> - TLS 1.2 muss für die internen RPCS - und KRPCS-Dienste aktiviert sein:
>   - `nsrpcs-127.0.0.1-3008`
>   - `nskrpcs-127.0.0.1-3009`
>   - `nsrpcs-::1l-3008`
> - 3008 und 3009 müssen in Firewalls zwischen den NetScaler-Knoten entsperrt werden.
>
> Sie können die Option `secure` mit der NetScaler CLI oder der GUI aktivieren oder deaktivieren.

So ändern Sie ein RPC-Knotenkennwort über die GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **RPC.**
2. Wählen Sie im **RPC-Bereich** den Knoten aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben **Sie unter RPC-Knoten konfigurieren**das neue Kennwort ein.
4. Geben Sie im **Feld Quell-IP-Adresse**die IP-Adresse des vorhandenen Knotens ein, die für die Kommunikation mit dem Peer-Systemknoten verwendet werden soll.



5. Wählen Sie **Sicher** und klicken Sie dann auf **OK**.

> **Hinweis**
>
> Zur Erhöhung der Sicherheit empfiehlt Citrix, die Option **Sicher** auf RPC-Knoten zu aktivieren. Wenn Sie die Option **Sicher** aktivieren, verschlüsselt die Appliance die gesamte RPC-Kommunikation, die von einem ADC-Knoten an andere ADC-Knoten gesendet wird, und sichert so die RPC-Kommunikation. Diese sichere Kommunikation verwendet die Portnummer 3008. Wenn die Firewall zwischen den ADC-Knoten die Portnummer 3008 blockiert, entsperren Sie sie und fahren Sie fort. Andernfalls schlägt die Konfigurationssynchronisierung und die Konfigurationspropagierung möglicherweise fehl.

So ändern Sie ein RPC-Knotenkennwort über die CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein:

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]
show ns rpcNode
<!--NeedCopy-->
```

Beispiel:

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>

<!--NeedCopy-->
```

Konfigurieren Sie zum ersten Mal eine FIPS-Appliance

May 11, 2023

> **Hinweis**
>
> - FIPS FAQ finden Sie hier: FIPS FAQ.

Für den HTTPS-Zugriff auf das Konfigurationsdienstprogramm und für sichere Remoteprozeduraufrufe ist ein Zertifikatsschlüsselpaar erforderlich. RPC-Knoten sind interne Systementitäten, die für die System-zu-System-Kommunikation von Konfigurations- und Sitzungsinformationen verwendet werden. Auf jeder Appliance ist ein RPC-Knoten vorhanden. Dieser Knoten speichert das Kennwort, das mit dem vom kontaktierenden Gerät bereitgestellten abgeglichen wird. Für die Kommunikation mit anderen NetScaler Appliances benötigt jede Appliance Kenntnisse der anderen Appliances, einschließlich der Authentifizierung auf der anderen Appliance. RPC-Knoten verwalten diese Informationen, einschließlich der IP-Adressen der anderen NetScaler Appliances und der Kennwörter, die für die Authentifizierung auf den einzelnen Geräten verwendet werden.

Auf einer virtuellen Appliance der NetScaler MPX-Appliance ist ein Zertifikatsschlüsselpaar automatisch an die internen Dienste gebunden. Auf einer FIPS-Appliance muss ein Zertifikatsschlüsselpaar in das Hardwaresicherheitsmodul (HSM) einer FIPS-Karte importiert werden. Dazu müssen Sie die FIPS-Karte konfigurieren, ein Zertifikatsschlüsselpaar erstellen und es an die internen Dienste binden.

Konfigurieren Sie sicheres HTTPS mithilfe der CLI

Gehen Sie folgendermaßen vor, um sicheres HTTPS mithilfe der CLI zu konfigurieren

1. Initialisieren Sie das Hardwaresicherheitsmodul (HSM) auf der FIPS-Karte der Appliance. Informationen zur Initialisierung des HSM finden Sie unter einem der folgenden Links:
   - Für MPX: Konfigurieren Sie das HSM.
   - Für SDX: Konfigurieren Sie das HSM für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Appliance.
2. Wenn die Appliance Teil eines Hochverfügbarkeitssetups ist, aktivieren Sie die SIM. Informationen zum Aktivieren der SIM auf den primären und sekundären Appliances finden Sie unter Konfigurieren von FIPS-Appliances in einem Hochverfügbarkeits-Setup.
3. Importieren Sie den FIPS-Schlüssel in das HSM der FIPS-Karte der Appliance. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. Fügen Sie ein Zertifikatsschlüsselpaar hinzu. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Binden Sie den im vorherigen Schritt erstellten Zertifikatsschlüssel an die folgenden internen Dienste. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   bind ssl service nshttps-127.0.0.1-443 -certkeyname server
   ```



```
bind ssl service nshttps-::1l-443 -certkeyname server
```

Konfigurieren Sie sicheres HTTPS mithilfe der GUI

Gehen Sie folgendermaßen vor, um sicheres HTTPS mithilfe der GUI zu konfigurieren:

1. Initialisieren Sie das Hardwaresicherheitsmodul (HSM) auf der FIPS-Karte der Appliance. Informationen zur Initialisierung des HSM finden Sie unter einem der folgenden Links:
   - Für MPX: Konfigurieren Sie das HSM.
   - Für SDX: Konfigurieren Sie das HSM für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Appliance.
2. Wenn die Appliance Teil eines Hochverfügbarkeitssetups ist, aktivieren Sie das Secure Information System (SIM). Informationen zum Aktivieren der SIM auf den primären und sekundären Appliances finden Sie unter Konfigurieren von FIPS-Appliances in einem Hochverfügbarkeits-Setup.
3. Importieren Sie den FIPS-Schlüssel in das HSM der FIPS-Karte der Appliance. Weitere Informationen zum Importieren eines FIPS-Schlüssels finden Sie im Abschnitt Importieren eines vorhandenen FIPS-Schlüssels .
4. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**.
5. Klicken Sie im Detailbereich auf Installieren.
6. Geben Sie im Dialogfeld Zertifikat installieren die Zertifikatsdetails ein.
7. Klicken Sie auf Erstellenund dann auf Schließen.
8. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
9. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf Interne Dienste.
10. Wählen Sie `nshttps-127.0.0.1-443` aus der Liste aus, und klicken Sie dann auf Öffnen.
11. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
12. Wählen Sie `nshttps-::1l-443` aus der Liste aus, und klicken Sie dann auf Öffnen.
13. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
14. Klicken Sie auf OK.

Konfigurieren von sicherem RPC mithilfe der CLI

Gehen Sie folgendermaßen vor, um sicheres RPC mithilfe der CLI zu konfigurieren:

1. Initialisieren Sie das Hardwaresicherheitsmodul (HSM) auf der FIPS-Karte der Appliance. Informationen zur Initialisierung des HSM finden Sie unter einem der folgenden Links:
   - Für MPX: Konfigurieren Sie das HSM.
   - Für SDX: Konfigurieren Sie das HSM für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Appliance.

2. Aktivieren Sie das sichere Informationssystem (SIM). Informationen zum Aktivieren der SIM auf den primären und sekundären Appliances finden Sie unter Konfigurieren von FIPS-Appliances in einem Hochverfügbarkeits-Setup.
3. Importieren Sie den FIPS-Schlüssel in das HSM der FIPS-Karte der Appliance. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. Fügen Sie ein Zertifikatsschlüsselpaar hinzu. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. Binden Sie das Zertifikatsschlüsselpaar an die folgenden internen Dienste. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   bind ssl service nsrpcs-127.0.0.1-3008 -certkeyname server

   bind ssl service nskrpcs-127.0.0.1-3009 -certkeyname server

   bind ssl service nsrpcs-::1l-3008 -certkeyname server
   ```

6. Aktivieren Sie den sicheren RPC-Modus. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   set ns rpcnode \<IP address\> -secure YES
   ```

   Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

Konfigurieren Sie sicheren RPC über die GUI

Gehen Sie folgendermaßen vor, um sicheren RPC mithilfe der GUI zu konfigurieren:

1. Initialisieren Sie das Hardwaresicherheitsmodul (HSM) auf der FIPS-Karte der Appliance. Informationen zur Initialisierung des HSM finden Sie unter einem der folgenden Links:
   - Für MPX: Konfigurieren Sie das HSM.
   - Für SDX: Konfigurieren Sie das HSM für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Appliance.
2. Aktivieren Sie das sichere Informationssystem (SIM). Informationen zum Aktivieren der SIM auf den primären und sekundären Appliances finden Sie unter Konfigurieren Sie FIPS-Appliances in einem Hochverfügbarkeits-Setup.
3. Importieren Sie den FIPS-Schlüssel in das HSM der FIPS-Karte der Appliance. Weitere Informationen zum Importieren eines FIPS-Schlüssels finden Sie im Abschnitt Bestehenden FIPS-Schlüssel importieren .
4. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**.
5. Klicken Sie im Detailbereich auf Installieren.
6. Geben Sie im Dialogfeld Zertifikat installieren die Zertifikatsdetails ein.

7. Klicken Sie auf Erstellenund dann auf Schließen.
8. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
9. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf Interne Dienste.
10. Wählen Sie in der Liste nsrpcs-127.0.0.1-3008 aus der Liste aus, und klicken Sie dann auf Öffnen.
11. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
12. Wählen Sie in der Liste nskrpcs-127.0.0.1-3009 aus, und klicken Sie dann auf Öffnen.
13. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
14. Wählen Sie `nsrpcs-::11-3008` aus der Liste aus, und klicken Sie dann auf Öffnen.
15. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
16. Klicken Sie auf OK.
17. Navigieren Sie zu **System > Netzwerk > RPC.**
18. Wählen Sie im Detailbereich die IP-Adresse aus, und klicken Sie auf Öffnen.
19. Wählen Sie im Dialogfeld RPC-Knoten konfigurieren die Option Sicher aus.
20. Klicken Sie auf OK.

Gemeinsame Netzwerktopologien

May 11, 2023

Wie im Abschnitt “Physischer Bereitstellungsmodus” unter Wo passt eine NetScaler Appliance in das Netzwerk?können Sie die NetScaler Appliance entweder inline zwischen den Clients und Servern oder im Einarmmodus bereitstellen. Im Inline-Modus wird eine Zweiarm-Topologie verwendet, bei der es sich um den gebräuchlichsten Bereitstellungstyp handelt.

Richten Sie eine gemeinsame zweiarmige Topologie ein

In einer zweiarmigen Topologie ist eine Netzwerkschnittstelle mit dem Client-Netzwerk und eine andere Netzwerkschnittstelle mit dem Servernetzwerk verbunden, wodurch sichergestellt wird, dass der gesamte Datenverkehr durch die Appliance fließt. Bei dieser Topologie müssen Sie möglicherweise Ihre Hardware erneut anschließen, was auch zu vorübergehenden Ausfallzeiten führen kann. Die grundlegenden Varianten der zweiarmigen Topologie sind mehrere Subnetze, in der Regel mit der Appliance in einem öffentlichen Subnetz und die Server in einem privaten Subnetz, und ein transparenter Modus, bei dem sich sowohl die Appliance als auch die Server im öffentlichen Netzwerk befinden.

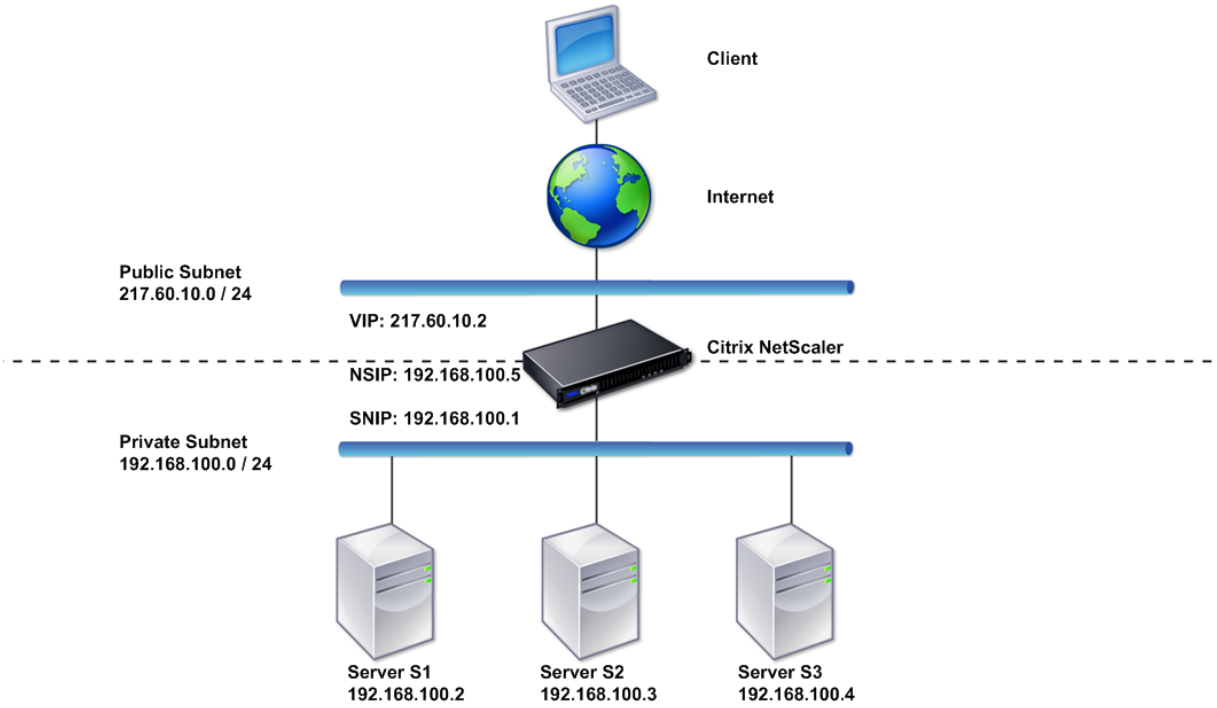
Richten Sie eine einfache Topologie mit zwei Armen und mehreren Subnetzen ein

Bei einer der am häufigsten verwendeten Topologien ist die NetScaler-Appliance zwischen den Clients und den Servern integriert, wobei ein virtueller Server für die Bearbeitung der Clientanforderungen konfiguriert ist. Diese Konfiguration wird verwendet, wenn sich die Clients und Server in verschiedenen Subnetzen befinden. In den meisten Fällen befinden sich die Clients und Server in öffentlichen bzw. privaten Subnetzen.

Stellen Sie sich beispielsweise eine Appliance vor, die im zweiarmigen Modus für die Verwaltung der Server S1, S2 und S3 bereitgestellt wird, wobei auf der Appliance ein virtueller Server vom Typ HTTP konfiguriert ist und auf den Servern HTTP-Dienste ausgeführt werden. Die Server befinden sich in einem privaten Subnetz und auf der Appliance ist ein SNIP für die Kommunikation mit den Servern konfiguriert. Die Option SNIP verwenden (USNIP) muss auf der Appliance aktiviert sein, damit sie das SNIP anstelle des MIP verwendet.

Wie in der folgenden Abbildung dargestellt, befindet sich das VIP im öffentlichen Subnetz 217.60.10.0 und das NSIP, die Server und das SNIP befinden sich im privaten Subnetz 192.168.100.0/24.

Abbildung 1. Topologiediagramm für den Zweiarmmodus, mehrere Subnetze



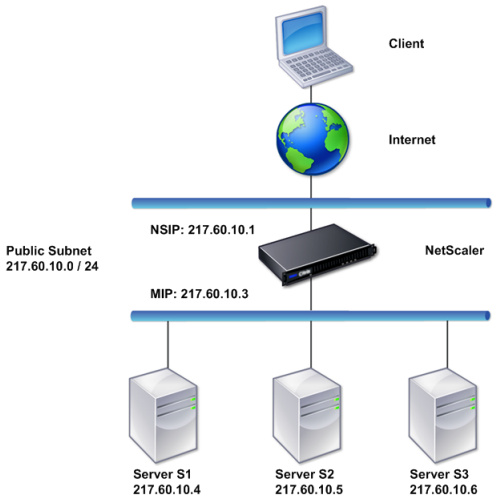
Gehen Sie folgendermaßen vor, um eine NetScaler Appliance im Zweiarmmodus mit mehreren Subnetzen bereitzustellen:

1. Konfigurieren Sie den NSIP und das Standardgateway, wie unter Konfigurieren der NetScaler IP-Adresse (NSIP)beschrieben.
2. Konfigurieren Sie den SNIP, wie unter Subnetz-IP-Adressen konfigurierenbeschrieben.
3. Aktivieren Sie die USNIP-Option, wie im Abschnitt So aktivieren oder deaktivieren Sie den USNIP-Modus beschrieben.
4. Konfigurieren Sie den virtuellen Server und die Dienste, wie im Abschnitt Erstellen eines virtuellen Servers und im Abschnitt Dienste konfigurieren beschrieben.
5. Verbinden Sie eine der Netzwerkschnittstellen mit einem privaten Subnetz und die andere Schnittstelle mit einem öffentlichen Subnetz.

Richten Sie eine einfache transparente Topologie mit zwei Armen ein

Verwenden Sie den transparenten Modus, wenn die Clients direkt auf die Server zugreifen müssen, ohne dass ein virtueller Server dazwischengeschaltet wird. Die Server-IP-Adressen müssen öffentlich sein, da die Clients auf sie zugreifen können müssen. In dem in der folgenden Abbildung gezeigten Beispiel wird eine NetScaler-Appliance zwischen dem Client und dem Server platziert, sodass der Datenverkehr die Appliance passieren muss. Sie müssen den L2-Modus aktivieren, um die Pakete zu überbrücken. NSIP und MIP befinden sich im selben öffentlichen Subnetz, 217.60.10.0/24.

Abbildung 2. Topologiediagramm für den zweiarmigen, transparenten Modus



Gehen Sie folgendermaßen vor, um eine NetScaler Appliance im transparenten Zweiarmmodus bereitzustellen:

1. Konfigurieren Sie den NSIP und das Standardgateway, wie unter Konfigurieren der NetScaler IP-Adresse (NSIP)beschrieben.
2. Aktivieren Sie den L2-Modus, wie im Layer-2-Modus aktivieren unddeaktivieren beschrieben.

3. Konfigurieren Sie das Standard-Gateway der verwalteten Server als MIP.
4. Verbinden Sie die Netzwerkschnittstellen mit den entsprechenden Ports des Switches.

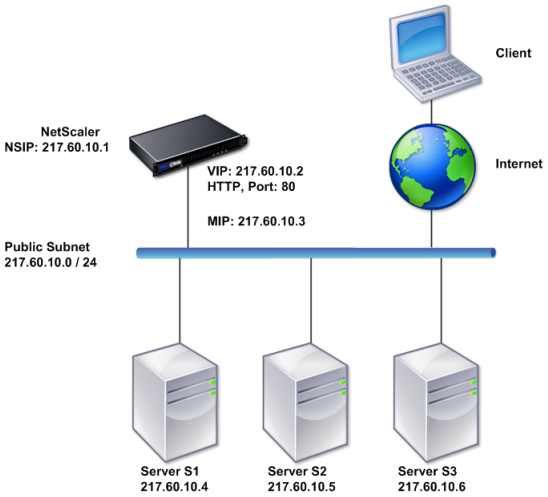
Richten Sie gemeinsame einarmige Topologien ein

Die beiden grundlegenden Varianten der Einarm-Topologie bestehen aus einem einzelnen Subnetz und aus mehreren Subnetzen.

Richten Sie eine einfache einarmige Subnetztopologie ein

Sie können eine einarmige Topologie mit einem einzigen Subnetz verwenden, wenn sich die Clients und Server im selben Subnetz befinden. Stellen Sie sich beispielsweise eine NetScaler-Appliance vor, die im einarmigen Modus für die Verwaltung der Server S1, S2 und S3 bereitgestellt wird. Ein virtueller Server vom Typ HTTP ist auf einer ADC-Appliance konfiguriert, und HTTP-Dienste werden auf den Servern ausgeführt. Wie in der folgenden Abbildung dargestellt, befinden sich die NetScaler-IP-Adresse (NSIP), die zugeordnete IP-Adresse (MIP) und die Server-IP-Adressen im selben öffentlichen Subnetz, 217.60.10.0/24.

Abbildung 3. Topologiediagramm für den Einarmmodus, Einzelsubnetz



Gehen Sie folgendermaßen vor, um eine NetScaler Appliance im Einarmmodus mit einem einzelnen Subnetz bereitzustellen:

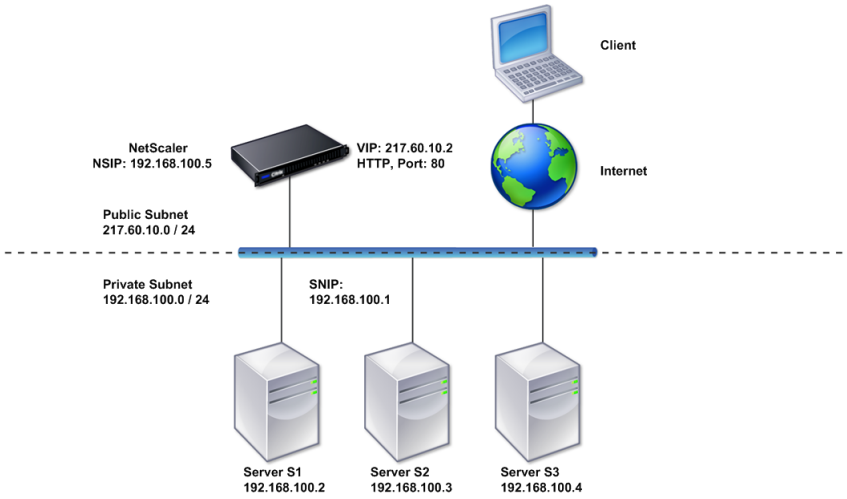
1. Konfigurieren Sie den NSIP und das Standardgateway wie unter Konfigurieren der NetScaler IP-Adresse (NSIP)beschrieben.
2. Konfigurieren Sie den virtuellen Server und die Dienste, wie im Abschnitt Erstellen eines virtuellen Servers und im Abschnitt Dienste konfigurieren beschrieben.

3. Verbinden Sie eine der Netzwerkschnittstellen mit dem Switch.

Richten Sie eine einfache einarmige Topologie mit mehreren Subnetzen ein

Sie können eine einarmige Topologie mit mehreren Subnetzen verwenden, wenn sich die Clients und Server in den verschiedenen Subnetzen befinden. Stellen Sie sich zum Beispiel eine NetScaler-Appliance vor, die im einarmigen Modus für die Verwaltung der Server S1, S2 und S3 bereitgestellt wird, wobei die Server an den Switch SW1 im Netzwerk angeschlossen sind. Ein virtueller Server vom Typ HTTP ist auf der Appliance konfiguriert, und HTTP-Dienste werden auf den Servern ausgeführt. Diese drei Server befinden sich im privaten Subnetz, sodass eine Subnetz-IP-Adresse (SNIP) für die Kommunikation mit ihnen konfiguriert ist. Die Option Subnetz-IP-Adresse (USNIP) verwenden muss aktiviert sein, damit die Appliance das SNIP anstelle eines MIP verwendet. Wie in der folgenden Abbildung dargestellt, befindet sich die virtuelle IP-Adresse (VIP) im öffentlichen Subnetz 217.60.10.0/24; die NSIP-, SNIP- und Server-IP-Adressen befinden sich im privaten Subnetz 192.168.100.0/24.

Abbildung 4. Topologiediagramm für den einarmigen Modus, mehrere Subnetze



Gehen Sie folgendermaßen vor, um eine NetScaler Appliance im Einarmmodus mit mehreren Subnetzen bereitzustellen:

1. Konfigurieren Sie den NSIP und das Standardgateway, wie unter Konfigurieren der NetScaler IP-Adresse (NSIP)beschrieben.
2. Konfigurieren Sie das SNIP und aktivieren Sie die USNIP-Option, wie unter Subnetz-IP-Adressen konfigurierenbeschrieben.
3. Konfigurieren Sie den virtuellen Server und die Dienste, wie im Abschnitt Erstellen eines virtuellen Servers und im Abschnitt Dienste konfigurieren beschrieben.
4. Verbinden Sie eine der Netzwerkschnittstellen mit dem Switch.

Einstellungen für die Systemverwaltung

May 11, 2023

Sobald Ihre Erstkonfiguration abgeschlossen ist, können Sie Einstellungen konfigurieren, um das Verhalten der NetScaler-Appliance zu definieren und die Verbindungsverwaltung zu vereinfachen. Sie haben eine Reihe von Optionen für den Umgang mit HTTP-Anfragen und -Antworten. Für die Verarbeitung von Paketen, die nicht an die NetScaler-Appliance adressiert sind, stehen Routing-, Bridging- und MAC-basierte Weiterleitungsmodi zur Verfügung. Sie können die Eigenschaften Ihrer Netzwerkschnittstellen definieren und die Schnittstellen aggregieren. Um Zeitprobleme zu vermeiden, können Sie die Citrix-Uhr mit einem NTP-Server (Network Time Protocol) synchronisieren. Die NetScaler-Appliance kann in verschiedenen DNS-Modi betrieben werden, unter anderem als autorisierender Domainnamenserver (ADNS). Sie können SNMP für die Systemverwaltung einrichten und die Syslog-Protokollierung von Systemereignissen anpassen. Stellen Sie vor der Bereitstellung sicher, dass Ihre Konfiguration vollständig und korrekt ist.

Systemeinstellungen

May 11, 2023

Die Konfiguration der Systemeinstellungen umfasst grundlegende Aufgaben wie die Konfiguration von HTTP-Ports, um die Aufrechterhaltung der Verbindung und den Server-Offload zu ermöglichen, das Festlegen der maximalen Anzahl von Verbindungen für jeden Server und das Festlegen der maximalen Anzahl von Anfragen pro Verbindung. Sie können das Einfügen von Client-IP-Adressen für Situationen aktivieren, in denen eine Proxy-IP-Adresse nicht geeignet ist, und Sie können die Version des HTTP-Cookies ändern.

Sie können eine NetScaler-Appliance auch so konfigurieren, dass FTP-Verbindungen auf einem kontrollierten Portbereich statt auf kurzlebigen Ports für Datenverbindungen geöffnet werden. Dies verbessert die Sicherheit, da das Öffnen aller Ports auf der Firewall unsicher ist. Sie können den Bereich zwischen 1.024 und 64.000 festlegen.

Gehen Sie vor der Bereitstellung die Überprüfungschecklisten durch, um Ihre Konfiguration zu überprüfen. Verwenden Sie die NetScaler-GUI, um HTTP-Parameter und den FTP-Portbereich zu konfigurieren.

Sie können die in der folgenden Tabelle beschriebenen Typen von HTTP-Parametern ändern.

Parametertyp: HTTP-Portinformationen

Gibt an: Die HTTP-Ports des Webservers, die von Ihren verwalteten Servern verwendet werden. Wenn Sie die Ports angeben, führt die Appliance Anforderungswechsel für jede Client-Anfrage durch, deren

Zielport mit einem angegebenen Port übereinstimmt.

> Hinweis: Wenn eine eingehende Clientanforderung nicht für einen Dienst oder einen virtuellen Server bestimmt ist, der speziell auf der Appliance konfiguriert ist, muss der Zielport in der Anfrage mit einem der global konfigurierten HTTP-Ports übereinstimmen. Dadurch kann die Appliance die Verbindung aufrechterhalten und den Server entladen.

Parametertyp: Grenzwerte

Gibt an: Die maximale Anzahl von Verbindungen zu jedem verwalteten Server und die maximale Anzahl von Anfragen, die über jede Verbindung gesendet werden. Wenn Sie beispielsweise Max. Verbindungen auf 500 setzen und die Appliance drei Server verwaltet, kann sie maximal 500 Verbindungen zu jedem der drei Server öffnen. Standardmäßig kann die Appliance eine unbegrenzte Anzahl von Verbindungen zu jedem der von ihr verwalteten Server herstellen. Um eine unbegrenzte Anzahl von Anfragen pro Verbindung anzugeben, setzen Sie Max. Anfragen auf 0.

> Hinweis: Wenn Sie den Apache HTTP-Server verwenden, müssen Sie Max Connections auf den Wert des MaxClient-Parameters in der Apache httpd.conf-Datei setzen. Das Festlegen dieses Parameters ist für andere Webserver optional.

Parametertyp: Client-IP-Einfügung

Spezifiziert: Aktiviert/deaktiviert das Einfügen der IP-Adresse des Clients in den HTTP-Anforderungsheader. Sie können im angrenzenden Textfeld einen Namen für das Header-Feld angeben. Wenn ein von einer Appliance verwalteter Webserver eine Subnetz-IP-Adresse erhält, identifiziert der Server sie als die IP-Adresse des Clients. Einige Anwendungen benötigen die IP-Adresse des Clients zu Protokollierungszwecken oder um dynamisch zu bestimmen, welche Inhalte vom Webserver bereitgestellt werden sollen.

Sie können das Einfügen der tatsächlichen Client-IP-Adresse in die HTTP-Header-Anfrage aktivieren, die vom Client an einen, einige oder alle von der Appliance verwalteten Server gesendet wird. Sie können dann auf die eingefügte Adresse zugreifen, indem Sie eine geringfügige Änderung am Server vornehmen (mithilfe eines Apache-Moduls, einer ISAPI-Schnittstelle oder einer NSAPI-Schnittstelle).

Parametertyp: Cookie-Version

Gibt an: Die HTTP-Cookie-Version, die verwendet werden soll, wenn die COOKIEINSERT-Persistenz auf einem virtuellen Server konfiguriert wird. Die Standardversion, Version 0, ist der gebräuchlichste Typ im Internet. Alternativ können Sie Version 1 angeben.

Parametertyp: Anfragen/Antworten

Spezifiziert: Optionen für die Behandlung bestimmter Arten von Anfragen und zum Aktivieren/Deaktivieren der Protokollierung von HTTP-Fehlerantworten.

Parametertyp: Einfügen des Server-Headers

Spezifiziert: Fügt einen Server-Header in von NetScaler generierte HTTP-Antworten ein.

Gehen Sie folgendermaßen vor, um HTTP-Parameter mithilfe der GUI zu konfigurieren:

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **HTTP-Parameter ändern**.
3. Geben **Sie im Dialogfeld „HTTP-Parameter konfigurieren** “ Werte für einige oder alle Parameter an, die unter den in der obigen Tabelle aufgeführten Überschriften angezeigt werden.
4. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um den FTP-Portbereich mithilfe der GUI festzulegen:

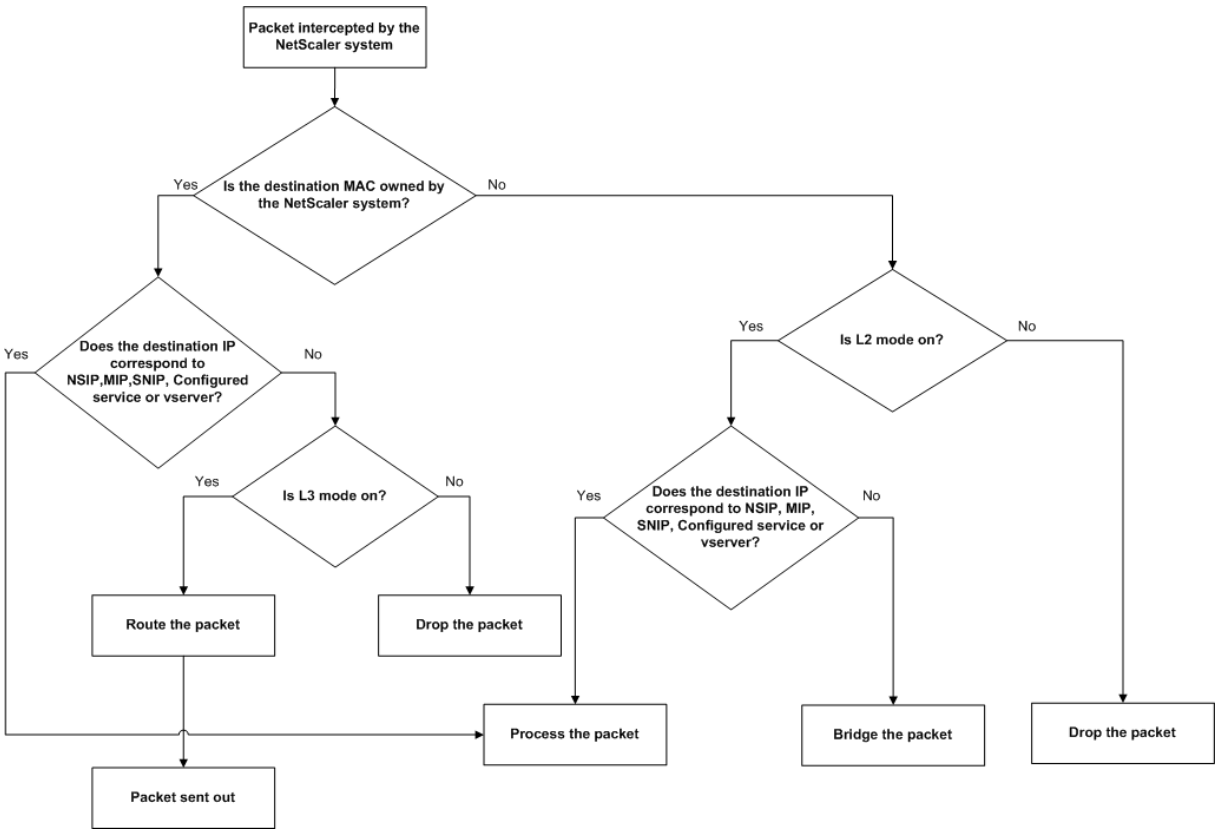
1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Systemeinstellungen ändern**.
3. Geben Sie unter **FTP-Portbereich** in den Textfeldern **Startportund Endport** die niedrigste bzw. höchste Portnummer für den Bereich ein, den Sie angeben möchten (z. B. 5000 und 6000).
4. Klicken Sie auf **OK**.

Paketweiterleitungsmodi

May 11, 2023

Die NetScaler Appliance kann Pakete entweder weiterleiten oder überbrücken, die nicht für eine IP-Adresse bestimmt sind, die der Appliance gehört (das heißt, die IP-Adresse ist nicht das NSIP, ein MIP, ein SNIP, ein konfigurierter Dienst oder ein konfigurierter virtueller Server). Standardmäßig ist der L3-Modus (Routing) aktiviert und der L2-Modus (Bridging) ist deaktiviert, aber Sie können die Konfiguration ändern. Das folgende Flussdiagramm zeigt, wie die Appliance Pakete auswertet und sie entweder verarbeitet, weiterleitet, überbrückt oder verwirft.

Abbildung 1. Interaktion zwischen Layer-2- und Layer-3-Modi



Eine Appliance kann die folgenden Modi verwenden, um die empfangenen Pakete weiterzuleiten:

- Layer 2 (L2) -Modus
- Layer 3 (L3) -Modus
- MAC-basierten Weiterleitungsmodus

Layer-2-Modus aktivieren und deaktivieren

Der Layer-2-Modus steuert die Layer-2-Weiterleitungsfunktion (Bridging). Sie können diesen Modus verwenden, um eine NetScaler Appliance so zu konfigurieren, dass sie sich wie ein Layer-2-Gerät verhält und die Pakete überbrücken, die nicht dafür bestimmt sind. Wenn dieser Modus aktiviert ist, werden Pakete nicht an eine der MAC-Adressen weitergeleitet, da die Pakete auf jeder Schnittstelle der Appliance ankommen können und jede Schnittstelle ihre eigene MAC-Adresse hat.

Wenn der Layer-2-Modus deaktiviert ist (was der Standard ist), verwirft die Appliance Pakete, die nicht für eine ihrer MAC-Adressen bestimmt sind. Wenn ein anderes Layer-2-Gerät parallel zur Appliance installiert ist, muss der Layer-2-Modus deaktiviert werden, um eine Überbrückung (Layer 2) -Schleifen zu verhindern. Sie können das Konfigurationsdienstprogramm oder die Befehlszeile verwenden, um den Layer-2-Modus zu aktivieren.

Hinweis: Die Appliance unterstützt das Spanning Tree Protocol nicht. Um Schleifen zu vermeiden, verbinden Sie nicht zwei Schnittstellen der Appliance mit derselben Broadcast-Domäne, wenn Sie den

L2-Modus aktivieren.

So aktivieren oder deaktivieren Sie den Layer-2-Modus mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Layer-2-Modus zu aktivieren/zu deaktivieren und sicherzustellen, dass er aktiviert/deaktiviert wurde:

- enable ns mode <Mode>
- disable ns mode <Mode>
- show ns mode

Beispiele

```
    > enable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 ON
    .
    .
    .
    Done
    >

    > disable ns mode l2
    Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 OFF
    .
    .
    .
    Done
    >
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie den Layer-2-Modus über die grafische Benutzeroberfläche

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.

2. Klicken Sie im Detailbereich unter **Modi** und **Funktionen**auf **Modi konfigurieren**.
3. Um im Dialogfeld “ **Modi konfigurieren** “ den Layer-2-Modus zu aktivieren, aktivieren Sie das Kontrollkästchen **Layer-2-Modus** . Deaktivieren Sie das Kontrollkästchen, um den Layer-2-Modus zu deaktivieren.
4. Klicken Sie auf **OK**. Der **Aktivieren-/Deaktivierenmodus?** wird im Detailbereich angezeigt.
5. Klicken Sie auf **Ja**.

Layer-3-Modus aktivieren und deaktivieren

Der Layer-3-Modus steuert die Layer-3-Weiterleitungsfunktion. Sie können diesen Modus verwenden, um eine NetScaler Appliance so zu konfigurieren, dass sie ihre Routingtabelle anzeigt und Pakete weiterleitet, die nicht dafür bestimmt sind. Wenn der Layer-3-Modus aktiviert ist (was der Standard ist), führt die Appliance Routing-Tabellen-Suchen durch und leitet alle Pakete weiter, die nicht für eine Appliance-eigene IP-Adresse bestimmt sind. Wenn Sie den Layer-3-Modus deaktivieren, verwirft die Appliance diese Pakete.

Aktivieren oder Deaktivieren des Layer-3-Modus mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Layer-3-Modus zu aktivieren/zu deaktivieren und zu überprüfen, ob er aktiviert/deaktiviert wurde:

- enable ns mode <Mode>
- disable ns mode <Mode>
- show ns mode

Beispiele

```
> enable ns mode l3
Done
> show ns mode

Mode Acronym Status
------- ------- ------
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
9) Layer 3 mode (ip forwarding) L3 ON
.
.
.
Done
```



```
17      >
18
19      > disable ns mode l3
20      Done
21      > show ns mode
22
23      Mode Acronym Status
24      ------- ------- ------
25      1) Fast Ramp FR ON
26      2) Layer 2 mode L2 OFF
27      .
28      .
29      .
30      9) Layer 3 mode (ip forwarding) L3 OFF
31      .
32      .
33      .
34      Done
35      >
36  <!--NeedCopy-->
```

Layer-3-Modus über die grafische Benutzeroberfläche aktivieren oder deaktivieren

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter **Modes and Features**auf **Configure Modes**.
3. Um den Layer-3-Modus zu aktivieren, aktivieren Sie im Dialogfeld " **Modi konfigurieren** " das Kontrollkästchen **Layer-3-Modus (IP-Weiterleitung)** . Deaktivieren Sie das Kontrollkästchen, um den Layer-3-Modus zu deaktivieren.
4. Klicken Sie auf **OK**. Der **Aktivieren-/Deaktivierenmodus?** wird im Detailbereich angezeigt.
5. Klicken Sie auf **Ja**.

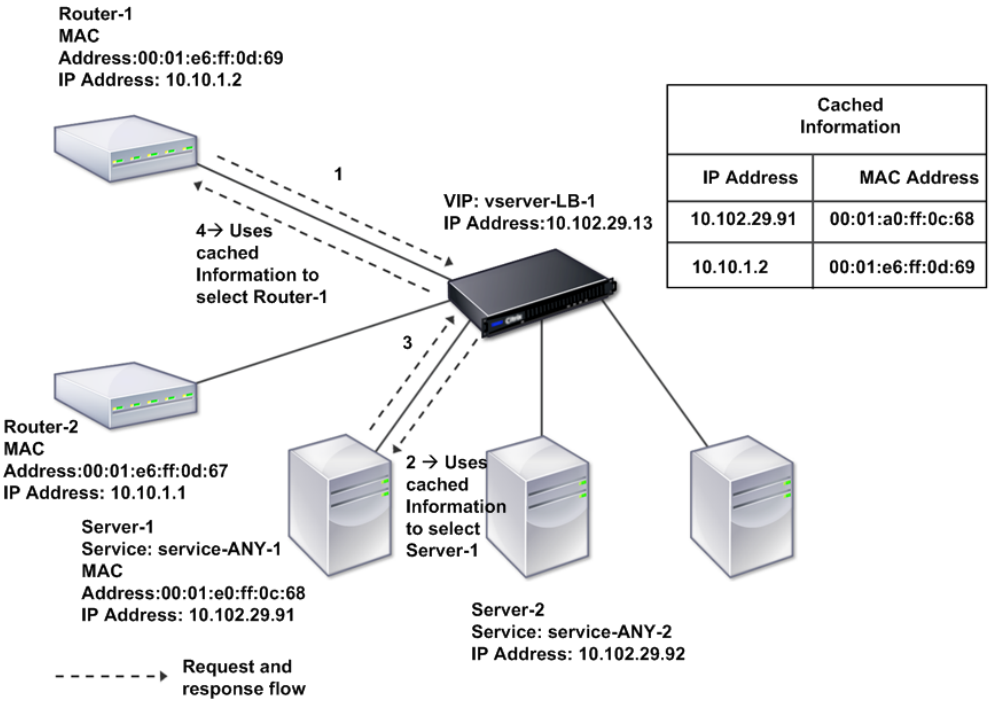
Mac-basierten Weiterleitungsmodus aktivieren und deaktivieren

Sie können die MAC-basierte Weiterleitung verwenden, um den Datenverkehr effizienter zu verarbeiten und beim Weiterleiten von Paketen Mehrfachroute- oder ARP-Suchen zu vermeiden, da sich die NetScaler Appliance die MAC-Adresse der Quelle merkt. Um mehrfache Suchvorgänge zu vermeiden, speichert die Appliance die Quell-MAC-Adresse jeder Verbindung, für die sie eine ARP-Suche durchführt, zwischen und gibt die Daten an dieselbe MAC-Adresse zurück.

Mac-basierte Weiterleitung ist nützlich, wenn Sie VPN-Geräte verwenden, da die Appliance sicherstellt, dass der gesamte Datenverkehr, der durch ein bestimmtes VPN fließt, dasselbe VPN-Gerät durchläuft

Die folgende Abbildung zeigt den Vorgang der MAC-basierten Weiterleitung.

Abbildung 2. Mac-basierter Weiterleitungsprozess



Wenn die MAC-basierte Weiterleitung aktiviert ist, speichert die Appliance die MAC-Adresse von:

- Die Quelle (ein übertragendes Gerät wie Router, Firewall oder VPN-Gerät) der eingehenden Verbindung.
- Der Server, der auf die Anfragen reagiert.

Wenn ein Server über eine Appliance antwortet, legt die Appliance die Ziel-MAC-Adresse des Antwortpakets auf die zwischengespeicherte Adresse fest, um sicherzustellen, dass der Datenverkehr symmetrisch fließt, und leitet die Antwort dann an den Client weiter. Der Prozess umgeht die Routentabellensuche und die ARP-Suchfunktionen. Wenn eine Appliance jedoch eine Verbindung initiiert, verwendet sie die Route- und ARP-Tabellen für die Suchfunktion. Um die MAC-basierte Weiterleitung zu aktivieren, verwenden Sie das Konfigurationsdienstprogramm oder die Befehlszeile.

Bei einigen Bereitstellungen müssen die eingehenden und ausgehenden Pfade durch verschiedene Router fließen. In diesen Situationen bricht die MAC-basierte Weiterleitung das Topologiedesign. Für einen Global Server Load Balancing (GSLB) -Site, bei dem die eingehenden und ausgehenden Pfade durch verschiedene Router fließen müssen, müssen Sie die MAC-basierte Weiterleitung deaktivieren und den Standardrouter der Appliance als ausgehenden Router verwenden.

Bei deaktivierter MAC-basierter Weiterleitung und aktivierter Layer-2- oder Layer-3-Konnektivität kann eine Routing-Tabelle separate Router für ausgehende und eingehende Verbindungen angeben. Um die MAC-basierte Weiterleitung zu deaktivieren, verwenden Sie das Konfigurationsdienstprogramm oder die Befehlszeile.

Mac-basierte Weiterleitung mit der CLI aktivieren oder deaktivieren

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den MAC-basierten Weiterleitungsmodus zu aktivieren/zu deaktivieren und zu überprüfen, ob er aktiviert/deaktiviert wurde:

- <enable ns mode <Mode>
- <disable ns mode <Mode>
- <show ns mode
  Example

  “‘ pre codeblock

  ```
  enable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               ON   .   .   .
        Done  >
  ```

  ```
  disable ns mode mbf
  Done
  show ns mode
  ```

  ```
  1   Mode                          Acronym           Status
  2   -------                       -------           ------   1)  Fast
      Ramp                     FR                ON   2)  Layer 2
      mode                  L2                OFF   .   .   .   6)
      MAC-based forwarding        MBF               OFF   .   .   .
         Done  >  <!--NeedCopy--> ```
  ```

So aktivieren oder deaktivieren Sie die MAC-basierte Weiterleitung mit der GUI

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter der Gruppe **Modi und Funktionen** auf **Modi konfigurieren**.

3. Um den MAC-basierten Weiterleitungsmodus zu aktivieren, aktivieren Sie im Dialogfeld **Modi konfigurieren** das Kontrollkästchen **MAC-basierte Weiterleitung**. Deaktivieren Sie das Kontrollkästchen, um den MAC-basierten Weiterleitungsmodus zu deaktivieren
4. Klicken Sie auf **OK**. Der **Aktivieren-/Deaktivierenmodus?** wird im Detailbereich angezeigt.
5. Klicken Sie auf **Ja**.

Netzwerkschnittstellen

May 11, 2023

Die NetScaler-Schnittstellen sind in der Steckplatz-/Port-Schreibweise nummeriert. Sie können nicht nur die Eigenschaften einzelner Schnittstellen ändern, sondern auch virtuelle LANs konfigurieren, um den Datenverkehr auf bestimmte Hostgruppen zu beschränken. Sie können Links auch zu Hochgeschwindigkeitskanälen zusammenfassen.

Virtuelle LANs

Die NetScaler-Appliance unterstützt (Layer 2) Port und IEEE802.1Q-markierte virtuelle LANs (VLANs). VLAN-Konfigurationen sind nützlich, wenn Sie den Verkehr auf bestimmte Stationsgruppen beschränken müssen. Sie können eine Netzwerkschnittstelle so konfigurieren, dass sie zu mehreren VLANs gehört, indem Sie IEEE 802.1q-Tagging verwenden.

Sie können Ihre konfigurierten VLANs an IP-Subnetze binden. Die ADC-Appliance (falls sie als Standardrouter für die Hosts in den Subnetzen konfiguriert ist) führt dann die IP-Weiterleitung zwischen diesen VLANs durch.

Die NetScaler-Appliance unterstützt die folgenden Arten von VLANs.

- Standard-VLAN

  Standardmäßig sind die Netzwerkschnittstellen einer NetScaler-Appliance in einem einzigen, portbasierten VLAN als ungetaggte Netzwerkschnittstellen enthalten. Dieses Standard-VLAN hat eine VID von 1 und ist dauerhaft vorhanden. Sie kann nicht gelöscht werden und ihre VID kann nicht geändert werden.

- Portbasierte VLANs

  Eine Reihe von Netzwerkschnittstellen, die sich eine gemeinsame, exklusive Layer-2-Broadcast-Domäne teilen, definieren die Mitgliedschaft eines portbasierten VLANs. Sie können mehrere portbasierte VLANs konfigurieren. Wenn Sie einem neuen VLAN als Mitglied ohne Tagged eine Schnittstelle hinzufügen, wird sie automatisch aus dem Standard-VLAN entfernt.

- Getaggtes VLAN

Eine Netzwerkschnittstelle kann ein markiertes oder ein ungetaggtes Mitglied eines VLAN sein. Jede Netzwerkschnittstelle ist ein unmarkiertes Mitglied nur eines VLANs (seines nativen VLAN). Die ungetaggte Netzwerkschnittstelle leitet die Frames für das native VLAN als ungetaggte Frames weiter. Eine markierte Netzwerkschnittstelle kann Teil von mehr als einem VLAN sein. Wenn Sie das Tagging konfigurieren, stellen Sie sicher, dass beide Enden der Verbindung über die passenden VLAN-Einstellungen verfügen. Sie können das Konfigurationsprogramm verwenden, um ein markiertes VLAN (nsvlan) zu definieren, an das alle Ports als markierte Mitglieder des VLAN gebunden werden können. Die Konfiguration dieses VLAN erfordert einen Neustart der ADC-Appliance und muss daher während der ersten Netzwerkkonfiguration erfolgen.

Aggregierte Kanäle verknüpfen

Die Link-Aggregation kombiniert eingehende Daten von mehreren Ports zu einer einzigen Hochgeschwindigkeitsverbindung. Die Konfiguration des Link-Aggregat-Kanals erhöht die Kapazität und Verfügbarkeit des Kommunikationskanals zwischen einer NetScaler-Appliance und anderen angeschlossenen Geräten. Ein aggregierter Link wird auch als Kanal bezeichnet.

Wenn eine Netzwerkschnittstelle an einen Kanal gebunden ist, haben die Kanalparameter Vorrang vor den Netzwerkschnittstellenparametern. Eine Netzwerkschnittstelle kann nur an einen Kanal gebunden werden. Das Binden einer Netzwerkschnittstelle an einen Link-Aggregatkanal ändert die VLAN-Konfiguration. Das heißt, wenn Netzwerkschnittstellen an einen Kanal gebunden werden, werden sie aus den VLANs entfernt, zu denen sie ursprünglich gehörten, und sie werden dem Standard-VLAN hinzugefügt. Sie können den Kanal jedoch wieder an das alte oder an ein neues VLAN binden. Wenn Sie beispielsweise die Netzwerkschnittstellen 1/2 und 1/3 an ein VLAN mit der ID 2 gebunden haben und sie dann an den Link-Aggregatkanal LA/1 binden, werden die Netzwerkschnittstellen in das Standard-VLAN verschoben, Sie können sie jedoch an VLAN 2 binden.

Hinweis: Sie können auch das Link Aggregation Control Protocol (LACP) verwenden, um die Linkaggregation zu konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Link-Aggregation mithilfe des Link Aggregation Control Protocol.

Uhrsynchronisierung

May 11, 2023

Sie können Ihre NetScaler-Appliance so konfigurieren, dass ihre lokale Uhr mit einem Network Time Protocol (NTP) -Server synchronisiert wird. Dadurch wird sichergestellt, dass die Uhr dieselben Datums- und Uhrzeiteinstellungen hat wie die anderen Server in Ihrem Netzwerk. NTP verwendet

den User Datagram Protocol (UDP) Port 123 als Transportschicht. Fügen Sie NTP-Server in der NTP-Konfigurationsdatei hinzu, damit die Appliance regelmäßig Updates von diesen Servern erhält.

Wenn Sie keinen lokalen NTP-Server haben, finden Sie eine Liste der öffentlichen Open-Access-NTP-Server auf der offiziellen NTP-Site unter http://www.ntp.org.

Gehen Sie folgendermaßen vor, um die Uhrsynchronisierung auf Ihrer Appliance zu konfigurieren:

1. Melden Sie sich an der Befehlszeile an und geben Sie den Shell-Befehl ein.
2. Kopieren Sie an der Shell-Eingabeaufforderung die Datei ntp.conf aus dem Verzeichnis /etc in das Verzeichnis /nsconfig. Falls die Datei bereits im Verzeichnis /nsconfig existiert, entfernen Sie die folgenden Einträge aus der Datei ntp.conf:

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

   Diese Einträge sind nur erforderlich, wenn Sie das Gerät als Zeitserver ausführen möchten. Diese Funktion wird jedoch auf der NetScaler Appliance nicht unterstützt.
3. Bearbeiten Sie /nsconfig/ntp.conf, indem Sie die IP-Adresse für den gewünschten NTP-Server unter dem Server der Datei eingeben und Einträge einschränken.
4. Erstellen Sie eine Datei mit dem Namen rc.netscaler im Verzeichnis /nsconfig, falls die Datei nicht bereits im Verzeichnis existiert.
5. Bearbeiten Sie /nsconfig/rc.netscaler, indem Sie den folgenden Eintrag hinzufügen: `/bin/sh /etc/ntpd_ctl full_start`.

   Dieser Eintrag startet den ntpd-Dienst und prüft die ntp.conf-Datei.

   Wenn Sie die Uhrzeit, zu der ein großer Unterschied besteht, nicht zwangsweise synchronisieren möchten, können Sie das Datum manuell einstellen und dann ntpd erneut starten. Sie können den Zeitunterschied zwischen der Appliance und dem Zeitserver überprüfen, indem Sie den folgenden Befehl in der Shell ausführen:

   ```
   ntpdate -q <IP address or domain name of the NTP server>
   <!--NeedCopy-->
   ```

6. Starten Sie die Appliance neu, um die Uhrsynchronisierung

   Hinweis: Wenn Sie die Zeitsynchronisierung starten möchten, ohne die Appliance neu zu starten, geben Sie an der Shell-Eingabeaufforderung einen der folgenden Befehle ein:

   ```
   /usr/sbin/ntpd -c /nsconfig/ntp.conf -g -p /var/run/ntpd.pid -l /
      var/log/ntpd.log &

   or

   ```



```
/bin/sh /etc/ntpd_ctl full_start

<!--NeedCopy-->
```

DNS-Konfiguration

May 11, 2023

Sie können eine NetScaler-Appliance so konfigurieren, dass sie als autorisierender Domänennamenserver (ADNS), DNS-Proxyserver, End Resolver oder Forwarder fungiert. Sie können DNS-Ressourceneinträge wie SRV Records, AAAA Records, A Records, MX Records, NS Records, CNAME Records, PTR Records und SOA Records hinzufügen. Außerdem kann die Appliance die Last auf externen DNS-Servern ausgleichen.

Eine gängige Praxis besteht darin, eine Appliance als Forwarder zu konfigurieren. Für diese Konfiguration müssen Sie externe Nameserver hinzufügen. Nachdem Sie die externen Server hinzugefügt haben, sollten Sie überprüfen, ob Ihre Konfiguration korrekt ist.

Sie können externe Nameserver hinzufügen, entfernen, aktivieren und deaktivieren. Sie können einen Namenserver erstellen, indem Sie seine IP-Adresse angeben, oder Sie können einen vorhandenen virtuellen Server als Namenserver konfigurieren.

Beim Hinzufügen von Nameservern können Sie IP-Adressen oder virtuelle IP-Adressen (VIPs) angeben. Wenn Sie IP-Adressen verwenden, gleicht die Appliance Anfragen an die konfigurierten Nameserver auf Roundrobin-Weise aus. Wenn Sie VIPs verwenden, können Sie eine beliebige Load-Balancing-Methode angeben.

Fügen Sie einen Namenserver mithilfe der CLI hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Namenserver hinzuzufügen und die Konfiguration zu überprüfen:

- `<add dns nameServer \<IP\>`
- `<show dns nameServer \<IP\>`

Beispiel

```
> add dns nameServer 10.102.29.10
 Done
> show dns nameServer 10.102.29.10
1)       10.102.29.10  -  State: DOWN
 Done
```



```
6
7   <!--NeedCopy-->
```

Namenserver über die GUI hinzufügen

1. Navigieren Sie zu **Traffic Management** > **DNS** > **Nameserver**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Wählen **Sie im Dialogfeld Namenserver erstellen** die Option **IP-Adresse**aus.
4. Geben Sie im Textfeld **IP-Adresse** die IP-Adresse des Namenservers ein (z. B. 10.102.29.10). Wenn Sie einen externen Nameserver hinzufügen, deaktivieren Sie das Kontrollkästchen **Lokal** .
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Stellen Sie sicher, dass der hinzugefügte Namenserver im Bereich **Namensserver** angezeigt wird.

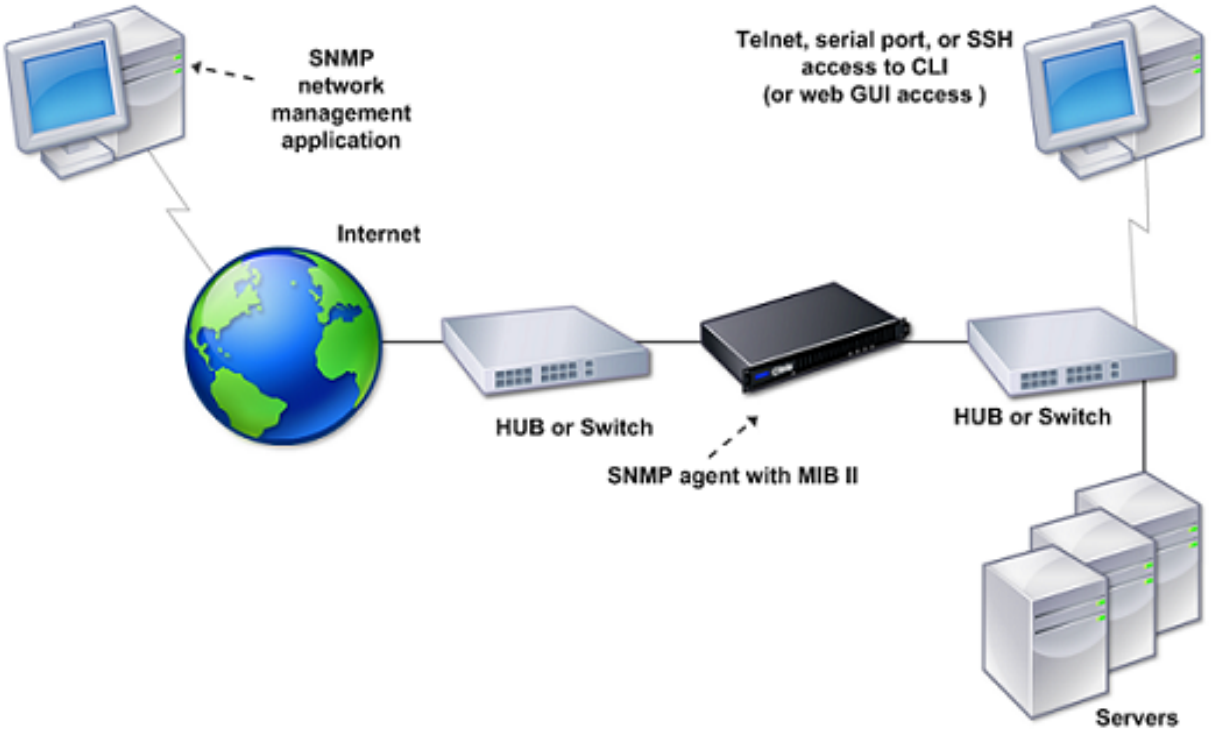
SNMP-Konfiguration

May 11, 2023

Die Netzwerkverwaltungsanwendung Simple Network Management Protocol (SNMP), die auf einem externen Computer ausgeführt wird, fragt den SNMP-Agenten auf der NetScaler-Appliance ab. Der Agent durchsucht die Management Information Base (MIB) nach Daten, die von der Netzwerkverwaltungsanwendung angefordert werden, und sendet die Daten an die Anwendung.

Die SNMP-Überwachung verwendet Trap-Meldungen und Alarme. SNMP-Trap-Meldungen sind asynchrone Ereignisse, die der Agent generiert, um ungewöhnliche Bedingungen zu signalisieren, die durch Alarme angezeigt werden. Wenn Sie beispielsweise informiert werden möchten, wenn die CPU-Auslastung über 90 Prozent liegt, können Sie für diesen Zustand einen Alarm einrichten. Die folgende Abbildung zeigt ein Netzwerk mit einer NetScaler-Appliance, für die SNMP aktiviert und konfiguriert ist.

Abbildung 1. SNMP auf der NetScaler-Appliance



Der SNMP-Agent auf einer NetScaler-Appliance unterstützt SNMP Version 1 (SNMPv1), SNMP Version 2 (SNMPv2) und SNMP Version 3 (SNMPv3). Da der Agent im zweisprachigen Modus arbeitet, kann er SNMPv2-Abfragen wie Get-Bulk- und SNMPv1-Abfragen verarbeiten. Der SNMP-Agent sendet außerdem SNMPv2-konforme Traps und unterstützt SNMPv2-Datentypen wie Counter64. SNMPv1-Manager (Programme auf anderen Servern, die SNMP-Informationen von der ADC-Appliance anfordern) verwenden bei der Verarbeitung von SNMP-Abfragen die Datei NS-MIB-SMIv1.mib. SNMPv2-Manager verwenden die Datei NS-MIB-SMIV2.mib.

Die NetScaler Appliance unterstützt die folgenden unternehmensspezifischen MIBs:

- Eine Teilmenge von Standard-MIB-2-Gruppen. Stellt die MIB-2-Gruppen SYSTEM, IF, ICMP, UDP und SNMP bereit.
- Ein Systemunternehmen MIB. Bietet systemspezifische Konfiguration und Statistiken.

Um SNMP zu konfigurieren, geben Sie an, welche Manager den SNMP-Agenten abfragen können, fügen SNMP-Trap-Listener hinzu, die die SNMP-Trap-Meldungen empfangen, und SNMP-Alarme konfigurieren.

Fügen Sie SNMP-Manager hinzu

Sie können eine Workstation, auf der eine Verwaltungsanwendung ausgeführt wird, die der SNMP-Version 1, 2 oder 3 entspricht, für den Zugriff auf eine Appliance konfigurieren. Eine solche Workstation wird als SNMP-Manager bezeichnet. Wenn Sie keinen SNMP-Manager auf der Appliance angeben, akzeptiert und beantwortet die Appliance SNMP-Abfragen von allen IP-Adressen im Net-

zwerk. Wenn Sie einen oder mehrere SNMP-Manager konfigurieren, akzeptiert und beantwortet die Appliance SNMP-Abfragen nur von diesen spezifischen IP-Adressen. Wenn Sie die IP-Adresse eines SNMP-Managers angeben, können Sie den Parameter netmask verwenden, um Zugriff von ganzen Subnetzen aus zu gewähren. Sie können maximal 100 SNMP-Manager oder Netzwerke hinzufügen. So fügen Sie einen SNMP-Manager mithilfe der CLI hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen SNMP-Manager hinzuzufügen und die Konfiguration zu überprüfen:

```
add snmp manager <IPAddress> ... [-netmask <netmask>]
show snmp manager <IPAddress>
```

Beispiel:

```
1 add snmp manager 10.102.29.5 -netmask 255.255.255.255
2 Done
3 show snmp manager 10.102.29.5
4 10.102.29.5 255.255.255.255
5 Done
6 <!--NeedCopy-->
```

Um einen SNMP-Manager mithilfe der GUI hinzuzufügen:

1. Erweitern Sie im Navigationsbereich **System**, erweitern Sie **SNMP**und klicken Sie dann auf **Manager**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Geben Sie im Dialogfeld SNMP-Manager hinzufügen** in das Textfeld **IP-Adresse die IP-Adresse** der Arbeitsstation ein, auf der die Verwaltungsanwendung ausgeführt wird (z. B. 10.102.29.5).
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
5. Stellen Sie sicher, dass der von Ihnen hinzugefügte SNMP-Manager im Abschnitt **Details** unten im Bereich angezeigt wird.

Fügen Sie SNMP-Trap-Listener hinzu

Nach der Konfiguration der Alarme müssen Sie den Trap-Listener angeben, an den die Appliance die Trap-Meldungen sendet. Neben der Angabe von Parametern wie der IP-Adresse und dem Zielport des Trap-Listeners können Sie auch den Trap-Typ (entweder generisch oder spezifisch) und die SNMP-Version angeben.

Sie können maximal 20 Trap-Listener für den Empfang von generischen oder spezifischen Traps konfigurieren.

So fügen Sie mit der CLI einen SNMP-Trap-Listener hinzu

Geben Sie an der Befehlszeile den folgenden Befehl ein, um einen SNMP-Trap hinzuzufügen, und überprüfen Sie, ob er hinzugefügt wurde:

- `add snmp trap specific <IP>`
- `show snmp trap`

Beispiel:

```
Trap type: SPECIFIC
Destination IP: 10.102.29.3
TD: 0
Destination Port: 162
Source IP: NetScaler IP
Version: V2
Min-Severity: -
AllPartition: DISABLED
Community: public
<!--NeedCopy-->
```

So fügen Sie mithilfe der GUI einen SNMP-Trap-Listener hinzu

1. Erweitern Sie im Navigationsbereich System, erweitern Sie **SNMP**, und klicken Sie dann auf **Traps**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld „SNMP-Trap-Ziel erstellen** “ in das Textfeld **Ziel-IP-Adresse** die IP-Adresse ein (z. B. 10.102.29.3).
4. Klicken Sie auf **Create** und dann auf **Close**.
5. Stellen Sie sicher, dass der von Ihnen hinzugefügte SNMP-Trap im Abschnitt **Details** unten im Bereich angezeigt wird.

SNMP-Alarme konfigurieren

Sie konfigurieren Alarme so, dass die Appliance eine Trap-Meldung generiert, wenn ein Ereignis eintritt, das einem der Alarme entspricht. Die Konfiguration eines Alarms besteht darin, den Alarm zu aktivieren und den Schweregrad festzulegen, ab dem eine Falle generiert wird. Es gibt fünf Schweregrade: Kritisch, schwerwiegend, gering, Warnung und informativ. Ein Trap wird nur gesendet, wenn der Schweregrad des Alarms dem für den Trap angegebenen Schweregrad entspricht.

Einige Alarme sind standardmäßig aktiviert. Wenn Sie einen SNMP-Alarm deaktivieren, generiert die Appliance keine Trap-Meldungen, wenn entsprechende Ereignisse eintreten. Wenn Sie beispielsweise

den SNMP-Alarm bei Anmeldefehler deaktivieren, generiert die Appliance keine Trap-Meldung, wenn ein Anmeldefehler auftritt.

So aktivieren oder deaktivieren Sie einen Alarm mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen Alarm zu aktivieren oder zu deaktivieren, und überprüfen Sie, ob er aktiviert oder deaktiviert wurde:

- set snmp alarm <trapName> [-state ENABLED | DISABLED]
- show snmp alarm <trapName>

Beispiel

```
set snmp alarm LOGIN-FAILURE -state ENABLED
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- --------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED - ENABLED
Done
<!--NeedCopy-->
```

So legen Sie den Schweregrad des Alarms mithilfe der CLI fest

Geben Sie in der Befehlszeile die folgenden Befehle ein, um den Schweregrad des Alarms festzulegen und zu überprüfen, ob der Schweregrad richtig eingestellt wurde:

- set snmp alarm <trapName> [-severity <severity>]
- show snmp alarm <trapName>

Beispiel:

```
set snmp alarm LOGIN-FAILURE -severity Major
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
----- --------------- ---------------- ---- -------- --------- --------
LOGIN-FAILURE N/A N/A N/A ENABLED Major ENABLED
Done
<!--NeedCopy-->
```


So konfigurieren Sie Alarme mithilfe der GUI

1. Erweitern Sie im Navigationsbereich **System**, erweitern Sie SNMP, und klicken Sie dann auf **Alarme**.
2. **Wählen Sie im Detailbereich einen Alarm aus (z. B. LOGIN-FAILURE), und klicken Sie dann auf Öffnen.**
3. Um den Alarm zu aktivieren, wählen Sie im Dialogfeld **SNMP-Alarm konfigurieren** in der Dropdownliste **Status** die Option "Aktiviert" aus. Um den Alarm zu deaktivieren, wählen Sie Deaktiviert.
4. Wählen Sie in der Dropdownliste **Schweregrad** eine Option für den Schweregrad aus (z. B. Major)
5. Klicken Sie auf **OK**und dann auf **Schließen**.
6. Vergewissern Sie sich, dass die Parameter für den von Ihnen konfigurierten SNMP-Alarm korrekt konfiguriert sind, indem Sie sich den Abschnitt **Details** unten im Bereich ansehen.

Konfiguration verifizieren

May 11, 2023

Nachdem Sie die Konfiguration Ihres Systems abgeschlossen haben, füllen Sie die folgenden Checklisten aus, um Ihre Konfiguration zu überprüfen.

Checkliste für die Konfiguration

- Der Build läuft wie folgt:
- Es gibt keine Inkompatibilitätsprobleme. (Inkompatibilitätsprobleme sind in den Versionshinweisen des Builds dokumentiert.)
- Die Porteinstellungen (Geschwindigkeit, Duplex, Flusskontrolle, Überwachung) entsprechen denen des Switch-Ports.
- Es wurden genügend SNIP-IP-Adressen konfiguriert, um alle serverseitigen Verbindungen in Spitzenzeiten zu unterstützen.
  - Die Anzahl der konfigurierten SNIP-IP-Adressen ist: __
  - Die erwartete Anzahl gleichzeitiger Serververbindungen ist:
    [] 62.000 [] 124.000 [] Andere____

Checkliste für die Topologiekonfiguration

Die Routen wurden verwendet, um Server in anderen Subnetzen aufzulösen.

Die eingegebenen Routen sind:

_____

- Wenn sich die NetScaler-Appliance in einer öffentlich-privaten Topologie befindet, wurde Reverse-NAT konfiguriert.
- Die auf der ADC-Appliance konfigurierten Failover-Einstellungen (Hochverfügbarkeit) werden in einer einarmigen oder zweiarmigen Konfiguration aufgelöst. Alle ungenutzten Netzwerkschnittstellen wurden deaktiviert:

_____

- Wenn sich die ADC-Appliance hinter einem externen Load Balancer befindet, lautet die Load-Balancing-Richtlinie auf dem externen Load Balancer nicht „Least Connection“.

  Die auf dem externen Load Balancer konfigurierte Load Balancing-Richtlinie lautet:

_____

- Wenn die ADC-Appliance vor einer Firewall platziert wird, wird das Sitzungs-Timeout an der Firewall auf einen Wert von mindestens 300 Sekunden festgelegt.

  Hinweis: Das TCP-Verbindungs-Timeout im Leerlauf auf einer NetScaler-Appliance beträgt 360 Sekunden. Wenn das Timeout an der Firewall ebenfalls auf 300 Sekunden oder mehr eingestellt ist, kann die Appliance TCP-Verbindungsmultiplexe effektiv durchführen, da Verbindungen nicht früher geschlossen werden.

  Der für das Sitzungs-Timeout konfigurierte Wert ist: _____

Checkliste für die Serverkonfiguration

- „Keep-Alive“ wurde auf allen Servern aktiviert.

  Der für das Keep-Alive-Timeout konfigurierte Wert ist: _____
- Das Standard-Gateway wurde auf den richtigen Wert gesetzt. (Das Standard-Gateway sollte entweder eine NetScaler-Appliance oder ein Upstream-Router sein.) Das Standard-Gateway ist:

_____

- Die Serverporteinstellungen (Geschwindigkeit, Duplex, Flusskontrolle, Überwachung) entsprechen den Switch-Port-Einstellungen.

_____

- Wenn der Microsoft® Internet Information Server verwendet wird, ist die Pufferung auf dem Server aktiviert.
- Wenn ein Apache Server verwendet wird, wird der Parameter MaxConn (maximale Anzahl von Verbindungen) auf dem Server und auf der NetScaler-Appliance konfiguriert.

  Der Wert MaxConn (maximale Anzahl von Verbindungen), der gesetzt wurde, ist:

- Wenn ein Netscape Enterprise Server verwendet wird, wird die maximale Anzahl von Anfragen pro Verbindungsparameter auf der NetScaler-Appliance festgelegt. Der maximale Wert für Anfragen pro Verbindung, der festgelegt wurde, ist:

Checkliste für die Konfiguration der Softwarefunktionen

- Muss die Layer-2-Modus-Funktion deaktiviert werden? (Deaktivieren Sie diese Option, wenn ein anderes Layer-2-Gerät parallel zu einer NetScaler-Appliance arbeitet.)

  Grund für die Aktivierung oder Deaktivierung:

- Muss die MAC-basierte Weiterleitungsfunktion deaktiviert werden? (Wenn die für den Rückverkehr verwendete MAC-Adresse unterschiedlich ist, sollte sie deaktiviert werden.)

  Grund für die Aktivierung oder Deaktivierung:

- Muss die hostbasierte Wiederverwendung deaktiviert werden? (Gibt es virtuelles Hosting auf den Servern?)

  Grund für die Aktivierung oder Deaktivierung:

- Müssen die Standardeinstellungen der Überspannungsschutzfunktion geändert werden?

  Grund für die Änderung oder Nichtänderung:

Checkliste aufrufen

- Die System-IPs können vom clientseitigen Netzwerk aus angepingt werden.
- Die System-IPs können vom serverseitigen Netzwerk aus angepingt werden.
- Die verwalteten Server können über den NetScaler angepingt werden.
- Internet-Hosts können von den verwalteten Servern aus angepingt werden.
- Auf die verwalteten Server kann über den Browser zugegriffen werden.
- Über den Browser kann von verwalteten Servern aus auf das Internet zugegriffen werden.
- Auf das System kann über SSH zugegriffen werden.
- Der Administratorzugriff auf alle verwalteten Server funktioniert.

> Hinweis: Wenn Sie das Ping-Hilfsprogramm verwenden, stellen Sie sicher, dass auf dem angepingten Server ICMP ECHO aktiviert ist, da Ihr Ping sonst nicht erfolgreich ist.

Firewall-Checkliste

Die folgenden Firewall-Anforderungen wurden erfüllt:

- UDP 161 (SNMP)
- UDP 162 (SNMP-Trap)
- TCP/UDP 3010 (GUI)
- HTTP 80 (GUI)
- TCP 22 (SSH)

Lastausgleichs-Datenverkehr auf einer NetScaler-Appliance

May 11, 2023

Die Load-Balancing-Funktion verteilt Clientanfragen auf mehrere Server, um die Ressourcennutzung zu optimieren. In einem realen Szenario mit einer begrenzten Anzahl von Servern, die Dienste für eine große Anzahl von Clients bereitstellen, kann ein Server überlastet werden und die Leistung der Serverfarm beeinträchtigt werden. Eine NetScaler-Appliance verwendet Lastausgleichskriterien, um Engpässe zu vermeiden, indem jede Client-Anfrage an den Server weitergeleitet wird, der für die Bearbeitung der Anfrage am besten geeignet ist, wenn sie eintrifft.

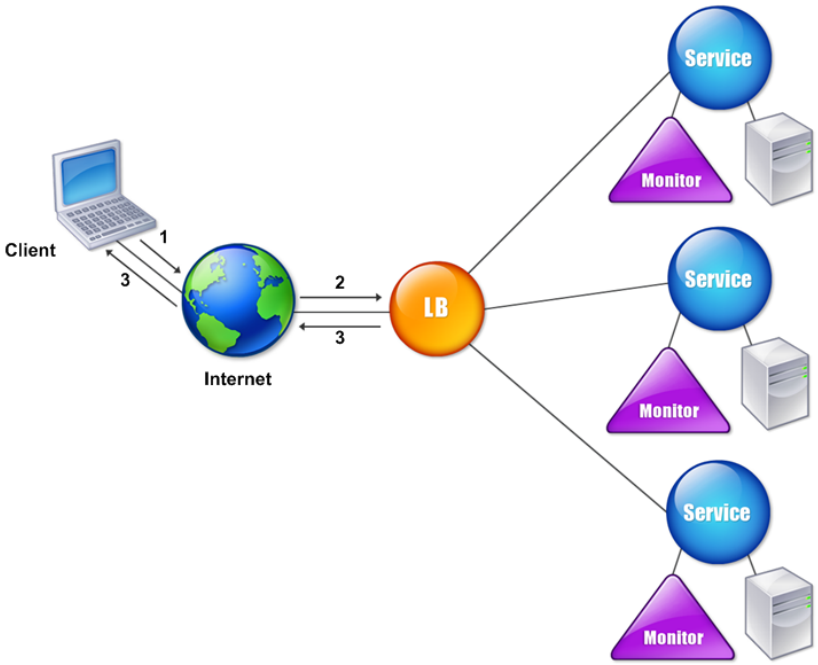
Um den Lastenausgleich zu konfigurieren, definieren Sie einen virtuellen Server, der mehrere Server in einer Serverfarm als Proxy leitet und die Last zwischen ihnen verteilt.

Wenn ein Client eine Verbindung zum Server initiiert, beendet ein virtueller Server die Clientverbindung und initiiert eine neue Verbindung mit dem ausgewählten Server oder verwendet eine bestehende Verbindung mit dem Server wieder, um den Lastenausgleich durchzuführen. Die Load-Balancing-Funktion ermöglicht das Verkehrsmanagement von Layer 4 (TCP und UDP) bis Layer 7 (FTP, HTTP und HTTPS).

Die NetScaler-Appliance verwendet eine Reihe von Algorithmen, sogenannte Load Balancing-Methoden, um zu bestimmen, wie die Last auf die Server verteilt wird. Die Standardmethode für den Lastenausgleich ist die Methode mit den wenigsten Verbindungen.

Eine typische Load-Balancing-Bereitstellung besteht aus den in der folgenden Abbildung beschriebenen Entitäten.

Abbildung 1. Lastenausgleich-Architektur



Die Entitäten funktionieren wie folgt:

- **Virtueller Server**. Eine Entität, die durch eine IP-Adresse, einen Port und ein Protokoll repräsentiert wird. Die IP-Adresse des virtuellen Servers (VIP) ist normalerweise eine öffentliche IP-Adresse. Der Client sendet Verbindungsanfragen an diese IP-Adresse. Der virtuelle Server stellt eine Bank von Servern dar.
- **Bedienung**. Eine logische Darstellung eines Servers oder einer Anwendung, die auf einem Server ausgeführt wird. Identifiziert die IP-Adresse des Servers, einen Port und ein Protokoll. Die Dienste sind an die virtuellen Server gebunden.
- **Serverobjekt**. Eine Entität, die durch eine IP-Adresse repräsentiert wird. Das Serverobjekt wird erstellt, wenn Sie einen Dienst erstellen. Die IP-Adresse des Dienstes wird als Name des Serverobjekts verwendet. Sie können auch ein Serverobjekt erstellen und dann Dienste erstellen, indem Sie das Serverobjekt verwenden.
- **Überwachen**. Eine Entität, die den Zustand der Dienste verfolgt. Die Appliance überprüft regelmäßig die Server mithilfe des Monitors, der an jeden Dienst gebunden ist. Wenn ein Server innerhalb eines bestimmten Antwort-Timeouts nicht reagiert und die angegebene Anzahl von Tests fehlschlägt, wird der Dienst als DOWN markiert. Anschließend führt die Appliance den Lastausgleich unter den verbleibenden Diensten durch.

Lastausgleich

May 11, 2023

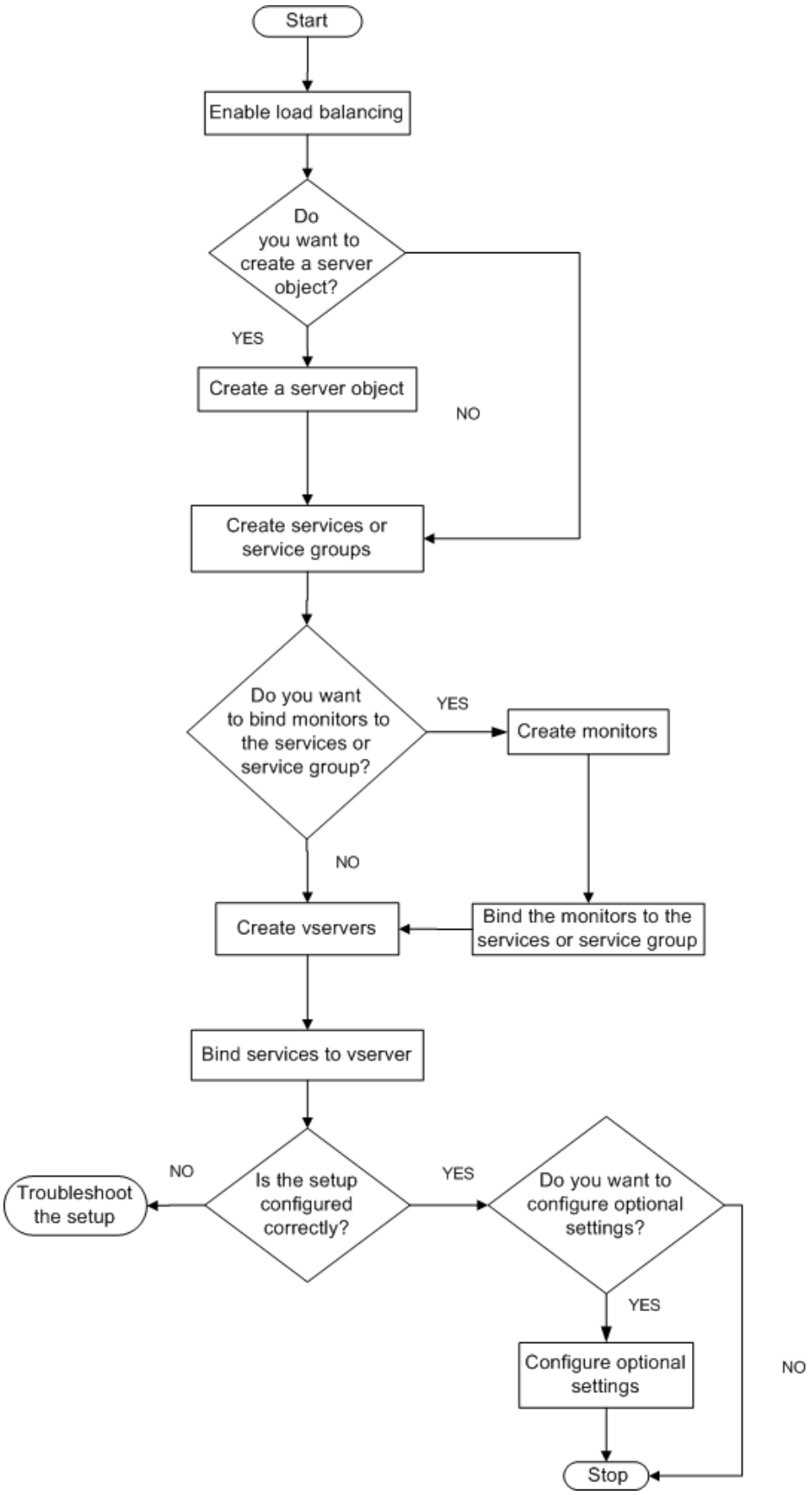
Um Load Balancing zu konfigurieren, müssen Sie zunächst Dienste erstellen. Anschließend erstellen Sie virtuelle Server und binden die Dienste an die virtuellen Server. Standardmäßig bindet die NetScaler-Appliance einen Monitor an jeden Dienst. Nachdem Sie die Dienste gebunden haben, überprüfen Sie Ihre Konfiguration, indem Sie sicherstellen, dass alle Einstellungen korrekt sind.

> Hinweis: Nachdem Sie die Konfiguration bereitgestellt haben, können Sie Statistiken anzeigen, die zeigen, wie die Entitäten in der Konfiguration abschneiden. Verwenden Sie das Statistikprogramm oder den Befehl
> stat lb vserver <vserverName>.

Optional können Sie einem Service Gewichte zuweisen. Die Load-Balancing-Methode verwendet dann das zugewiesene Gewicht, um einen Dienst auszuwählen. Für den Einstieg können Sie optionale Aufgaben jedoch auf die Konfiguration einiger grundlegender Persistenzeinstellungen, für Sitzungen, die eine Verbindung zu einem bestimmten Server aufrechterhalten müssen, und auf einige grundlegende Konfigurationsschutzeinstellungen beschränken.

Das folgende Flussdiagramm veranschaulicht die Reihenfolge der Konfigurationsaufgaben.

Abbildung 1. Reihenfolge der Aufgaben zur Konfiguration des Load Balancings



Lastenausgleich aktivieren

Stellen Sie vor der Konfiguration des Lastenausgleichs sicher, dass die Load-Balancing-Funktion aktiviert ist.

So aktivieren Sie den Lastenausgleich mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den Load Balancing zu aktivieren, und überprüfen Sie, ob er aktiviert ist:

- Feature Lab aktivieren
- show feature

  Beispiel

  “‘ pre codeblock

  ```
  enable feature lb
  Done
  show feature
  ```

  ```
  1   Feature                  Acronym          Status
  2   -------                  -------          ------   1)  Web
      Logging                WL               OFF   2)  Surge
      Protection           SP               OFF   3)  Load Balancing
                LB               ON   .   .   .   9)  SSL
      Offloading             SSL              ON   .   .   .  Done
      <!--NeedCopy--> ```
  ```

So aktivieren Sie den Lastenausgleich mithilfe der GUI

1. Erweitern Sie im Navigationsbereich System, und klicken Sie dann auf Einstellungen.
2. Klicken Sie im Detailbereich unter Modi und Funktionenauf Grundfunktionen ändern.
3. Aktivieren Sie im Dialogfeld „Grundfunktionen konfigurieren“ das Kontrollkästchen Load Balancing, und klicken Sie dann auf OK.
4. In den Funktionen zum Aktivieren/Deaktivieren? Nachricht, klicken Sie auf Ja.

Dienste und einen virtuellen Server konfigurieren

Wenn Sie die Dienste identifiziert haben, die Sie lastenausgleichen möchten, können Sie Ihre anfängliche Load-Balancing-Konfiguration implementieren, indem Sie die Dienstobjekte erstellen, einen virtuellen Lastausgleichsserver erstellen und die Dienstobjekte an den virtuellen Server binden.

So implementieren Sie die anfängliche Load-Balancing-Konfiguration mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Erstkonfiguration zu implementieren und zu überprüfen:

- <add service <name> <IPaddress> <serviceType> <port>
- <add lb vserver <vServerName> <serviceType> [<IPaddress> <port>]
- <bind lb vserver <name> <serviceName>
- <show service bindings <serviceName>

Beispiel

```
> add service service-HTTP-1 10.102.29.5 HTTP 80
 Done
> add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
 Done
> bind lb vserver vserver-LB-1 service-HTTP-1
 Done
> show service bindings service-HTTP-1
    service-HTTP-1 (10.102.29.5:80) - State : DOWN

      1)      vserver-LB-1 (10.102.29.60:80) - State : DOWN
 Done
<!--NeedCopy-->
```

Um die anfängliche Load-Balancing-Konfiguration mithilfe der GUI zu implementieren

1. Navigieren Sie zu Traffic Management > Load Balancing.
2. Klicken Sie im Detailbereich unter Erste Schritte auf Load Balancing Wizard und folgen Sie den Anweisungen, um ein grundlegendes Load Balancing-Setup zu erstellen.
3. Kehren Sie zum Navigationsbereich zurück, erweitern Sie Load Balancing, und klicken Sie dann auf Virtuelle Server.
4. Wählen Sie den virtuellen Server aus, den Sie konfiguriert haben, und stellen Sie sicher, dass die unten auf der Seite angezeigten Parameter korrekt konfiguriert sind.
5. Klicken Sie auf Öffnen.
6. Stellen Sie sicher, dass jeder Dienst an den virtuellen Server gebunden ist, indem Sie bestätigen, dass das Kontrollkästchen Aktiv für jeden Dienst auf der Registerkarte Dienste aktiviert ist.

Persistenzeinstellungen

May 11, 2023

Sie müssen die Persistenz auf einem virtuellen Server konfigurieren, wenn Sie den Status der Verbindungen auf den Servern beibehalten möchten, die durch diesen virtuellen Server dargestellt werden (z. B. Verbindungen, die im E-Commerce verwendet werden). Die Appliance verwendet dann die konfigurierte Load-Balancing-Methode für die anfängliche Auswahl eines Servers, leitet jedoch alle nachfolgenden Anforderungen von demselben Client an denselben Server weiter.

Wenn Persistenz konfiguriert ist, überschreibt sie die Lastausgleichsmethoden, sobald der Server ausgewählt wurde. Wenn die konfigurierte Persistenz für einen Dienst gilt, der nicht verfügbar ist, verwendet die Appliance die Lastausgleichsmethoden, um einen neuen Dienst auszuwählen, und der neue Dienst wird für nachfolgende Anforderungen vom Client persistent. Wenn sich der ausgewählte Dienst im Status "Nicht in Betrieb" befindet, bedient er weiterhin die ausstehenden Anforderungen, akzeptiert jedoch keine neuen Anforderungen oder Verbindungen. Nach Ablauf der Shutdown-Phase werden die bestehenden Verbindungen geschlossen. In der folgenden Tabelle sind die Persistenztypen aufgeführt, die Sie konfigurieren können.

Persistenz-Typ	Persistente Verbindungen
Quell-IP, SSL-Sitzungs-ID, Regel, DESTIP, SRCIPDESTIP	250K*
CookieInsert, URL passiv, benutzerdefinierte Server-ID	Speicherbegrenzung. Wenn im Falle von CookieInsert das Timeout nicht 0 ist, ist eine beliebige Anzahl von Verbindungen zulässig, bis es durch den Speicher begrenzt ist.

* in der obigen Tabelle angegebene bezieht sich auf Folgendes:

250.000 Sitzungen pro Core ist die Standardeinstellung pro Paket-Engine. Führen Sie den folgenden Befehl aus, um 1 Million Sitzungseinträge pro Packet Engine zu konfigurieren:

```
set lb parameter -sessionsthreshold <1000000*number of PE>
```

Führen Sie für ein 3-PE-System den folgenden Befehl aus:

```
set lb parameter -sessionsthreshold 3000000
```

Tabelle 1. Einschränkungen bei der Anzahl gleichzeitiger persistenter Verbindungen

Wenn die konfigurierte Persistenz aufgrund fehlender Ressourcen auf einer Appliance nicht aufrechterhalten werden kann, werden die Lastausgleichsmethoden für die Serverauswahl verwendet. Die Persistenz wird für einen konfigurierten Zeitraum aufrechterhalten, abhängig vom

Persistenztyp. Einige Persistenztypen sind spezifisch für bestimmte virtuelle Server. Die folgende Tabelle zeigt die Beziehung.

Persistence TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
Quell-IP	JA	JA	JA	JA	JA
CookieInsert	JA	JA	NEIN	NEIN	NEIN
SSL-Sitzung ID	NEIN	JA	NEIN	NEIN	JA
URL Passive	JA	JA	NEIN	NEIN	NEIN
Benutzerdefinie Server-ID	JA	JA	NEIN	NEIN	NEIN
Regel	JA	JA	NEIN	NEIN	NEIN
SRCIPDESTIP	–	–	JA	JA	–
DESTIP	–	–	JA	JA	–

Tabelle 2. Persistenztypen, die für jeden Typ von virtuellem Server verfügbar sind

Sie können auch Persistenz für eine Gruppe virtueller Server angeben. Wenn Sie die Persistenz für die Gruppe aktivieren, werden die Clientanforderungen an denselben ausgewählten Server weitergeleitet, unabhängig davon, welcher virtuelle Server in der Gruppe die Clientanforderung empfängt. Wenn die konfigurierte Zeit für die Persistenz abgelaufen ist, kann jeder virtuelle Server in der Gruppe für eingehende Clientanforderungen ausgewählt werden.

Zwei häufig verwendete Persistenztypen sind Persistenz basierend auf Cookies und Persistenz basierend auf Server-IDs in URLs.

Konfigurieren Sie die Persistenz basierend auf Cookies

Wenn Sie die auf Cookies basierende Persistenz aktivieren, fügt die NetScaler-Appliance dem **Set-Cookie-Header-Feld der HTTP-Antwort ein HTTP-Cookie** hinzu. Das Cookie enthält Informationen über den Dienst, an den die HTTP-Anfragen gesendet werden müssen. Der Kunde speichert das Cookie und schließt es in alle nachfolgenden Anfragen ein, und der ADC verwendet es, um den Dienst für diese Anfragen auszuwählen. Sie können diese Art der Persistenz auf virtuellen Servern vom Typ HTTP oder HTTPS verwenden.

Die NetScaler Appliance fügt das Cookie <NSC_XXXX>= <ServiceIP> <ServicePort> ein

Wobei:

- <NSC_XXXX> ist die virtuelle Server-ID, die vom Namen des virtuellen Servers abgeleitet wird.
- <ServiceIP> ist der hexadezimale Wert der Service-IP-Adresse.
- <ServicePort> ist der hexadezimale Wert des Serviceports.

Wenn die Option `useEncryptedPersistenceCookie` aktiviert ist, verschlüsselt der ADC ServiceIP und ServicePort über den SHA2-Hash-Algorithmus, wenn er ein Cookie einfügt, und entschlüsselt, wenn er ein Cookie empfängt.

Hinweis: Wenn der Client das HTTP-Cookie nicht speichern darf, haben die nachfolgenden Anforderungen nicht das HTTP-Cookie, und die Persistenz wird nicht berücksichtigt.

Standardmäßig sendet die ADC-Appliance das HTTP-Cookie Version 0 gemäß der Netscape-Spezifikation. Es kann auch Version 1 senden, in Übereinstimmung mit RFC 2109.

Sie können einen Timeoutwert für Persistenz konfigurieren, der auf HTTP-Cookies basiert. Beachten Sie Folgendes:

- Wenn die HTTP-Cookie-Version 0 verwendet wird, fügt die NetScaler-Appliance die absolute koordinierte Weltzeit (GMT) des Ablaufs des Cookie (das Expires-Attribut des HTTP-Cookies) ein, berechnet als Summe der aktuellen GMT-Zeit auf einer ADC-Appliance und des Timeout-Werts.
- Wenn ein HTTP-Cookie Version 1 verwendet wird, fügt die ADC-Appliance eine relative Ablaufzeit ein (Max-Age-Attribut des HTTP-Cookies). In diesem Fall berechnet die Clientsoftware die tatsächliche Ablaufzeit.

Hinweis: Die meisten derzeit installierten Clientsoftware (Microsoft Internet Explorer und Netscape-Browser) verstehen die HTTP-Cookie-Version 0. Einige HTTP-Proxys verstehen jedoch die HTTP-Cookie-Version 1.

Wenn Sie den Timeout-Wert auf 0 festlegen, gibt die ADC Appliance unabhängig von der verwendeten HTTP-Cookie-Version keine Ablaufzeit an. Die Ablaufzeit hängt dann von der Client-Software ab, und solche Cookies sind nicht gültig, wenn diese Software heruntergefahren wird. Dieser Persistenztyp verbraucht keine Systemressourcen. Daher kann es eine unbegrenzte Anzahl von persistenten Clients aufnehmen.

Ein Administrator kann die HTTP-Cookie-Version ändern.

So ändern Sie die HTTP-Cookie-Version über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns param [-cookieversion ( 0 | 1 )]
<!--NeedCopy-->
```

Beispiel:

```
set ns param -cookieversion 1
```



```
<!--NeedCopy-->
```

So ändern Sie die HTTP-Cookie-Version über die GUI

1. Navigieren Sie zu **System > Einstellungen**.
2. Klicken Sie im Detailbereich auf HTTP-Parameter ändern.
3. Wählen Sie im Dialogfeld HTTP-Parameter konfigurieren unter Cookie die Option Version 0 oder Version 1.

Hinweis: Informationen zu den Parametern finden Sie unter Konfigurieren der Persistenz basierend auf Cookies.

So konfigurieren Sie die Persistenz basierend auf Cookies über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die auf Cookies basierende Persistenz zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -persistenceType COOKIEINSERT

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: COOKIEINSERT (version 0)
    Persistence Timeout: 2 min
    .
    .
    .
 Done
<!--NeedCopy-->
```

So konfigurieren Sie Persistenz basierend auf Cookies über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.

2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die Persistenz konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld “Virtuellen Server konfigurieren (Load Balancing)” auf der Registerkarte “Methode und Persistenz” in der Liste “Persistenz” die Option COOKIEINSERT aus.
4. Geben Sie im Textfeld Timeout (min) den Timeoutwert ein (z. B. 2).
5. Klicken Sie auf OK.
6. Stellen Sie sicher, dass der virtuelle Server, für den Sie die Persistenz konfiguriert haben, korrekt konfiguriert ist, indem Sie den virtuellen Server auswählen und den Abschnitt Details unten im Bereich anzeigen.

Konfigurieren der Persistenz basierend auf Server-IDs in URLs

Die NetScaler-Appliance kann die Persistenz auf der Grundlage der Server-IDs in den URLs aufrechterhalten. In einer Technik, die als passive URL-Persistenz bezeichnet wird, extrahiert der ADC die Server-ID aus der Serverantwort und bettet sie in die URL-Abfrage der Clientanforderung ein. Die Server-ID ist eine IP-Adresse und der als Hexadezimalzahl angegebene Port. Der ADC extrahiert die Server-ID aus nachfolgenden Clientanforderungen und verwendet sie, um den Server auszuwählen.

Die passive URL-Persistenz erfordert die Konfiguration eines Payload-Ausdrucks oder eines Richtlinieninfrastrukturausdrucks, der den Speicherort der Server-ID in den Clientanforderungen angibt. Weitere Informationen zu Ausdrücken finden Sie unter Richtlinienkonfiguration und Referenz.

Hinweis: Wenn die Server-ID nicht aus den Clientanforderungen extrahiert werden kann, basiert die Serverauswahl auf der Load Balancing-Methode.

Beispiel: Payload Expression

Der Ausdruck URLQUERY enthält sid= konfiguriert das System, um die Server-ID aus der URL-Abfrage einer Clientanforderung zu extrahieren, nachdem das Token sid= abgeglichen wurde. Somit wird eine Anfrage mit der URL `http://www.citrix.com/index.asp?\\&sid;=c0a864100050` an den Server mit der IP-Adresse 10.102.29.10 und Port 80 gerichtet.

Der Timeoutwert wirkt sich nicht auf diese Art der Persistenz aus, die beibehalten wird, solange die Server-ID aus den Clientanforderungen extrahiert werden kann. Dieser Persistenztyp verbraucht keine Systemressourcen, so dass er eine unbegrenzte Anzahl von persistenten Clients aufnehmen kann.

> Hinweis: Informationen zu den Parametern finden Sie unter Load Balancing.

So konfigurieren Sie die Persistenz basierend auf Server-IDs in URLs über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Persistenz basierend auf Server-IDs in URLs zu konfigurieren und die Konfiguration zu überprüfen:


```
set lb vserver <name> -persistenceType URLPASSIVE

<show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: URLPASSIVE
    Persistence Timeout: 2 min
    .
    .
    .
Done
<!--NeedCopy-->
```

So konfigurieren Sie Persistenz basierend auf Server-IDs in URLs über die GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die Persistenz konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld “Virtuellen Server konfigurieren (Load Balancing)” auf der Registerkarte “Methode und Persistenz” in der Liste “Persistenz” die Option URLPASSIVE aus.
4. Geben Sie im Textfeld Timeout (min) den Timeoutwert ein (z. B. 2).
5. Geben Sie im Textfeld Regel einen gültigen Ausdruck ein. Klicken Sie alternativ neben dem Textfeld Regel auf Konfigurieren und verwenden Sie das Dialogfeld “Ausdruck erstellen”, um einen Ausdruck zu erstellen.
6. Klicken Sie auf OK.
7. Stellen Sie sicher, dass der virtuelle Server, für den Sie die Persistenz konfiguriert haben, korrekt konfiguriert ist, indem Sie den virtuellen Server auswählen und den Abschnitt Details unten im Bereich anzeigen.

Konfigurieren von Features zum Schutz der Lastausgleichskonfiguration

January 19, 2021

Sie können die URL-Umleitung so konfigurieren, dass Benachrichtigungen über Fehlfunktionen des virtuellen Servers bereitgestellt werden, und Sie können virtuelle Backupserver so konfigurieren, dass sie übernommen werden, wenn ein primärer virtueller Server nicht verfügbar ist.

URL-Umleitung konfigurieren

Sie können eine Umleitungs-URL konfigurieren, um den Status der Appliance zu kommunizieren, falls ein virtueller Server vom Typ HTTP oder HTTPS heruntergefahren oder deaktiviert ist. Diese URL kann ein lokaler oder Remote-Link sein. Die Appliance verwendet HTTP 302-Umleitung.

Weiterleitungen können absolute URLs oder relative URLs sein. Wenn die konfigurierte Umleitungs-URL eine absolute URL enthält, wird die HTTP-Umleitung unabhängig von der in der eingehenden HTTP-Anforderung angegebenen URL an den konfigurierten Speicherort gesendet. Wenn die konfigurierte Umleitungs-URL nur den Domänennamen (relative URL) enthält, wird die HTTP-Umleitung an einen Speicherort gesendet, nachdem die eingehende URL an die in der Umleitungs-URL konfigurierte Domäne angehängt wurde.

Hinweis: Wenn ein virtueller Lastausgleichsserver sowohl mit einem virtuellen Backupserver als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backupserver Vorrang vor der Weiterleitungs-URL. In diesem Fall wird eine Umleitung verwendet, wenn sowohl der primäre als auch der virtuelle Backupserver ausgefallen sind.

So konfigurieren Sie einen virtuellen Server für die Umleitung von Clientanforderungen an eine URL über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Server zu konfigurieren, um Clientanforderungen an eine URL umzuleiten und die Konfiguration zu überprüfen:

```
set lb vserver <name> -redirectURL <URL>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
    > set lb vserver vserver-LB-1 -redirectURL <http://www.newdomain.
       com/mysite/maintenance>
```



```
2       Done
3     > show lb vserver vserver-LB-1
4         vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
5         State: DOWN
6         Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)
7         .
8         .
9         .
10        Redirect URL: <http://www.newdomain.com/mysite/maintenance>
11        .
12        .
13        .
14      Done
15    >
16 <!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Server für die Umleitung von Clientanforderungen an eine URL über die GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die URL-Umleitung konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Geben Sie im Dialogfeld Virtuellen Server konfigurieren (Lastenausgleich) auf der Registerkarte Erweitert im Textfeld Umleitungs-URL den URL ein (z. B.`http://www.newdomain.com/mysite/maintenance`), und klicken Sie dann auf OK.
4. Stellen Sie sicher, dass die für den Server konfigurierte Umleitungs-URL im Abschnitt Details am unteren Rand des Bereichs angezeigt wird.

Konfigurieren von virtuellen Backup-Servern

Wenn der primäre virtuelle Server heruntergefahren oder deaktiviert ist, kann die Appliance die Verbindungen oder Clientanforderungen an einen virtuellen Backupserver weiterleiten, der den Clientdatenverkehr an die Dienste weiterleitet. Die Appliance kann auch eine Benachrichtigung über den Standortausfall oder die Wartung an den Client senden. Der virtuelle Backup-Server ist ein Proxy und ist für den Client transparent.

Sie können einen virtuellen Backupserver konfigurieren, wenn Sie einen virtuellen Server erstellen oder die optionalen Parameter eines vorhandenen virtuellen Servers ändern. Sie können auch einen virtuellen Backup-Server für einen vorhandenen virtuellen Backup-Server konfigurieren und so einen kaskadierten virtuellen Backup-Server erstellen. Die maximale Tiefe der Kaskadierung virtueller Backup-Server beträgt 10. Die Appliance sucht nach einem virtuellen Backupserver, der aktiviert ist, und greift auf diesen virtuellen Server zu, um den Inhalt bereitzustellen.

Sie können die URL-Umleitung auf dem primären Server für die Verwendung konfigurieren, wenn der primäre und die virtuellen Backup-Server ausgefallen sind oder deren Schwellenwerte für die Verarbeitung von Anforderungen erreicht haben.

Hinweis: Wenn kein virtueller Backup-Server vorhanden ist, wird eine Fehlermeldung angezeigt, es sei denn, der virtuelle Server ist mit einer Umleitungs-URL konfiguriert. Wenn sowohl ein virtueller Backupserver als auch eine Umleitungs-URL konfiguriert sind, hat der virtuelle Backupserver Vorrang.

So konfigurieren Sie einen virtuellen Backupserver über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Backupserver zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> [-backupVserver <string>]

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
    > set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
     Done
    > show lb vserver vserver-LB-1
        vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jun 17 08:56:34 2009 (+661 ms)
        .
        .
        .
        Backup: vserver-LB-2
        .
        .
        .
     Done
    >
<!--NeedCopy-->
```

So richten Sie einen virtuellen Backupserver über die GUI ein

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den virtuellen Backupserver konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.

3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) auf der Registerkarte Erweitert in der Liste Virtueller Server sichern den virtuellen Backupserver aus (z. B. vServer-LB-2, und klicken Sie dann auf OK.
4. Stellen Sie sicher, dass der konfigurierte virtuelle Backupserver im Abschnitt Details am unteren Rand des Bereichs angezeigt wird.

   Hinweis: Wenn der primäre Server ausfällt und dann wieder hochgefahren wird und Sie möchten, dass der virtuelle Backupserver als primärer Server fungiert, bis Sie den primären virtuellen Server explizit wiederherstellen, aktivieren Sie das Kontrollkästchen Primäre bei Heruntergefahren deaktivieren.

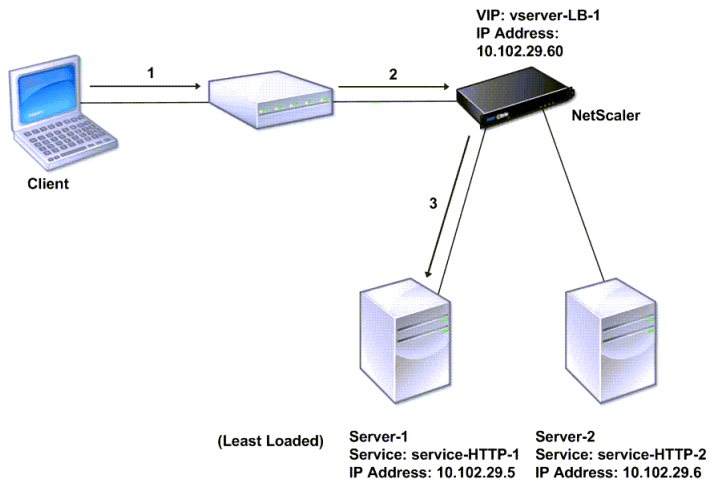
Ein typisches Lastausgleichszenario

May 11, 2023

In einem Load-Balancing-Setup befinden sich die NetScaler-Appliances logisch zwischen dem Client und der Serverfarm und verwalten den Datenverkehr zu den Servern.

Die folgende Abbildung zeigt die Topologie einer grundlegenden Load-Balancing-Konfiguration.

Abbildung 1. Grundlegende Load Balancing-Topologie



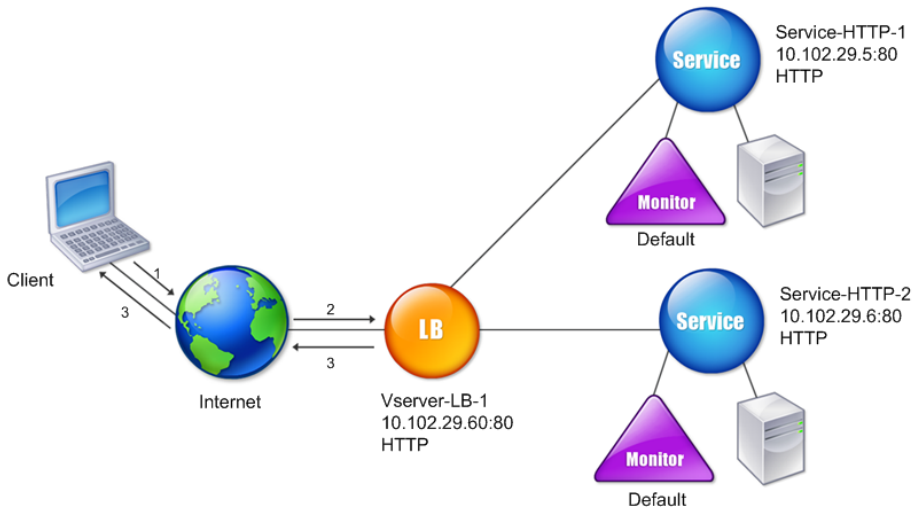
Der virtuelle Server wählt den Dienst aus und weist ihn der Bearbeitung von Clientanforderungen zu. Stellen Sie sich das Szenario in der vorherigen Abbildung vor, in dem die Dienste Service-HTTP-1 und Service-HTTP-2 erstellt und an den virtuellen Server mit dem Namen virtual Server-LB-1 gebunden werden. Virtual Server-LB-1 leitet die Client-Anfrage entweder an Service-HTTP-1 oder Service-HTTP-

2 weiter. Das System wählt den Dienst für jede Anfrage aus, indem es die Load-Balancing-Methode für die wenigsten Verbindungen verwendet. In der folgenden Tabelle sind die Namen und Werte der grundlegenden Entitäten aufgeführt, die auf dem System konfiguriert werden müssen.

Tabelle 1. LB-Konfigurationsparameterwerte

Die folgende Abbildung zeigt die Beispielwerte für den Load Balancing und die erforderlichen Parameter, die in der vorherigen Tabelle beschrieben sind.

Abbildung 2. Load Balancing Entity Modell



In den folgenden Tabellen sind die Befehle aufgeführt, die verwendet werden, um dieses Load Balancing-Setup mithilfe der Befehlszeilenschnittstelle zu konfigurieren.

Aufgabe	Befehl
Um den Lastenausgleich zu aktivieren	Feature Lab aktivieren
Um einen Dienst mit dem Namen Service-HTTP-1 zu erstellen	Dienst hinzufügen Service-HTTP-1 10.102.29.5 HTTP 80
Um einen Dienst mit dem Namen Service-HTTP-2 zu erstellen	Dienst hinzufügen Service-HTTP-2 10.102.29.6 HTTP 80

Aufgabe	Befehl
Um einen virtuellen Server mit dem Namen vServer-LB-1 zu erstellen	add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
Um einen Dienst namens Service-HTTP-1 an einen virtuellen Server mit dem Namen vServer-LB-1 zu binden	bind lb vserver vServer-LB-1 Service-HTTP-1
Um einen Dienst namens Service-HTTP-2 an einen virtuellen Server mit dem Namen vServer-LB-1 zu binden	bind lb vserver vServer-LB-1 Service-HTTP-2

Tabelle 2. Aufgaben zur Erstkonfiguration

Weitere Informationen zu den Aufgaben zur Erstkonfiguration finden Sie unter Einrichten des Basic Load Balancing.

Aufgabe	Befehl
Um die Eigenschaften eines virtuellen Servers mit dem Namen vServer-LB-1 anzuzeigen	show lb vserver vserver-LB-1
Um die Statistiken eines virtuellen Servers mit dem Namen vServer-LB-1 anzuzeigen	stat lb vserver vserver-LB-1
Um die Eigenschaften eines Dienstes mit dem Namen service-HTTP-1 anzuzeigen	show service service-HTTP-1
Um die Statistiken eines Dienstes mit dem Namen service-HTTP-1 anzuzeigen	stat service service-HTTP-1
Um die Bindungen eines Dienstes namens service-HTTP-1 anzuzeigen	show service bindings service-HTTP-1

Tabelle 3. Überprüfungsaufgaben

Aufgabe	Befehl
So konfigurieren Sie die Persistenz auf einem virtuellen Server mit dem Namen vServer-LB-1	set lb vserver vserver-LB-1 -persistenceType SOURCEIP -persistenceMask 255.255.255.255 -timeout 2

Aufgabe	Befehl
Um die COOKIEINSERT-Persistenz auf einem virtuellen Server mit dem Namen vServer-LB-1 zu konfigurieren	set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
So konfigurieren Sie die URLPassive-Persistenz auf einem virtuellen Server mit dem Namen vServer-LB-1	set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
Um einen virtuellen Server so zu konfigurieren, dass er die Clientanfrage an eine URL auf einem virtuellen Server mit dem Namen vServer-LB-1 umleitet	set lb vserver vserver-LB-1 -redirectURL `http://www.newdomain.com/mysite/maintenance`
Um einen virtuellen Backup-Server auf einem virtuellen Server mit dem Namen vServer-LB-1 einzurichten	set lb vserver vserver-LB-1 -backupVserver vserver-LB-2

Tabelle 4. Anpassungsaufgaben

Weitere Informationen zum Konfigurieren von Persistenz finden Sie unter Auswählen und Konfigurieren von Persistenzeinstellungen. Informationen zum Konfigurieren eines virtuellen Servers zum Umleiten einer Clientanforderung an eine URL und zum Einrichten eines virtuellen Sicherungsservers finden Sie unter Konfigurieren von Funktionen zum Schutz der Load Balancing-Konfiguration.

Anwendungsfall: So erzwingen Sie sichere und HttpOnly-Cookie-Optionen für Websites, die die NetScaler-Appliance verwenden

May 11, 2023

Die Webadministratoren können Secure oder HttpOnly oder sowohl die Flags auf der Session-ID als auch die Authentifizierungscookies erzwingen, die von den Webanwendungen generiert werden. Sie können die Set-Cookie-Header so ändern, dass sie diese beiden Optionen enthalten, indem Sie einen virtuellen HTTP-Lastenausgleichsserver und Rewriterichtlinien auf einer NetScaler-Appliance verwenden.

- **HttpOnly** - Diese Option in einem Cookie bewirkt, dass die Webbrowser das Cookie nur über das HTTP- oder HTTPS-Protokoll zurückgeben. Die Nicht-HTTP-Methoden wie JavaScript-Document.cookie Verweise können nicht auf das Cookie zugreifen. Diese Option hilft,

Cookie-Diebstahl aufgrund von Cross-Site Scripting zu verhindern.

> HINWEIS:
>
> Sie können die Option HttpOnly nicht verwenden, wenn eine Webanwendung Zugriff auf Cookie-Inhalte benötigt, indem Sie ein clientseitiges Skript wie JavaScript oder ein clientseitiges Java-Applet verwenden. Sie können die in diesem Dokument erwähnte Methode verwenden, um nur die servergenerierten Cookies und nicht die von der NetScaler-Appliance generierten Cookies neu zu schreiben. Zum Beispiel AppFirewall, Persistenz, VPN-Sitzungscookies und so weiter.

- **Sicher** - Diese Option in einem Cookie bewirkt, dass die Webbrowser nur den Cookie-Wert zurückgeben, wenn die Übertragung durch SSL verschlüsselt wird. Diese Option kann verwendet werden, um Cookie-Diebstahl durch Verbindungsabhörung zu verhindern.

> HINWEIS:
>
> Das folgende Verfahren gilt nicht für virtuelle VPN-Server.

So konfigurieren Sie die NetScaler-Appliance so, dass die Secure- und HttpOnly-Flags für einen vorhandenen virtuellen HTTP-Server mithilfe von CLI erzwingen

1. Erstellen Sie eine Rewrite-Aktion.

   Dieses Beispiel ist so konfiguriert, dass sowohl Secure- als auch HttpOnly-Flags festgelegt werden. Wenn einer fehlt, ändern Sie es nach Bedarf für andere Kombinationen.

   ```
   1 add rewrite action act_cookie_Secure replace_all http.RES.
       full_Header ""Secure; HttpOnly; path=/"" -search "regex(re!(
       path=/\\; Secure; HttpOnly)|(path=/\\; Secure)|(path=/\\;
       HttpOnly)|(path=/)!)"
   2 <!--NeedCopy-->
   ```

   Diese Richtlinie ersetzt alle Instanzen von “path=/”, “path=/; Secure”, “path=/; Secure; HttpOnly” und “path=/; HttpOnly” durch “Secure; HttpOnly; path=/”. Dieser reguläre Ausdruck (Regex) schlägt fehl, wenn der Fall nicht übereinstimmt.

2. Erstellen Sie eine Rewriterichtlinie, um die Aktion auszulösen.

   ```
   1 add rewrite policy rw_force_secure_cookie "http.RES.HEADER("Set-
       Cookie").EXISTS" act_cookie_Secure
   2 <!--NeedCopy-->
   ```

3. Binden Sie die Rewriterichtlinie an den zu sichernden virtuellen Server. Wenn `Secure` Option verwendet wird, muss ein virtueller SSL-Server verwendet werden.


```
bind lb vserver mySSLVServer -policyName rw_force_secure_cookie -
    priority 100 -gotoPriorityExpression NEXT -type RESPONSE
<!--NeedCopy-->
```

Beispiele:

Das folgende Beispiel zeigt das Cookie, bevor das HttpOnly-Flag gesetzt wird

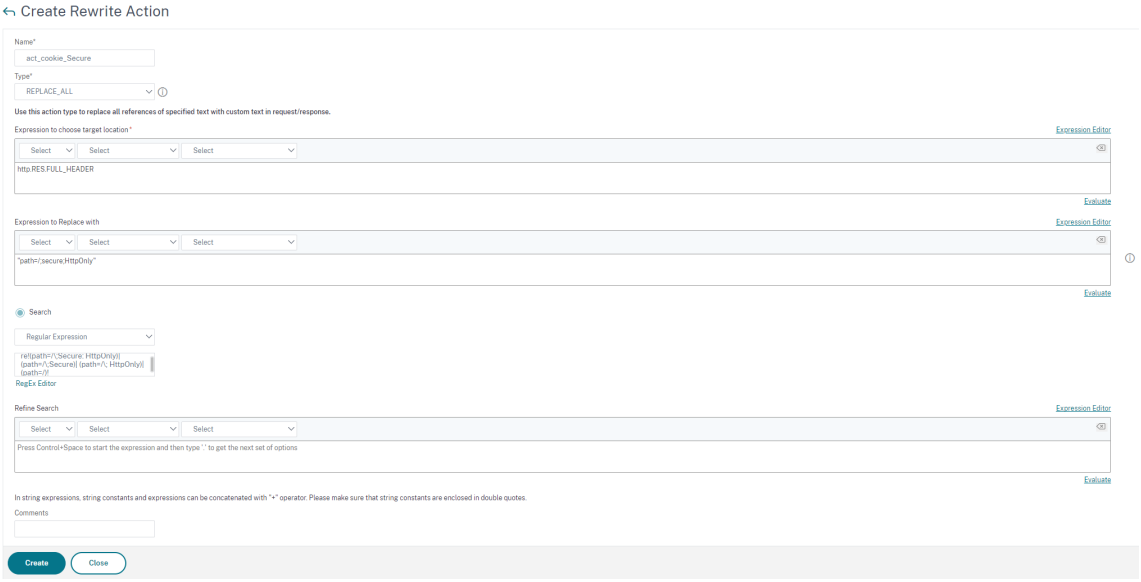
```
Set-Cookie: CtxsAuthId=C5614491; path=/Citrix/ProdWeb
<!--NeedCopy-->
```

Das folgende Beispiel zeigt das Cookie nach dem Setzen des Flag HttpOnly

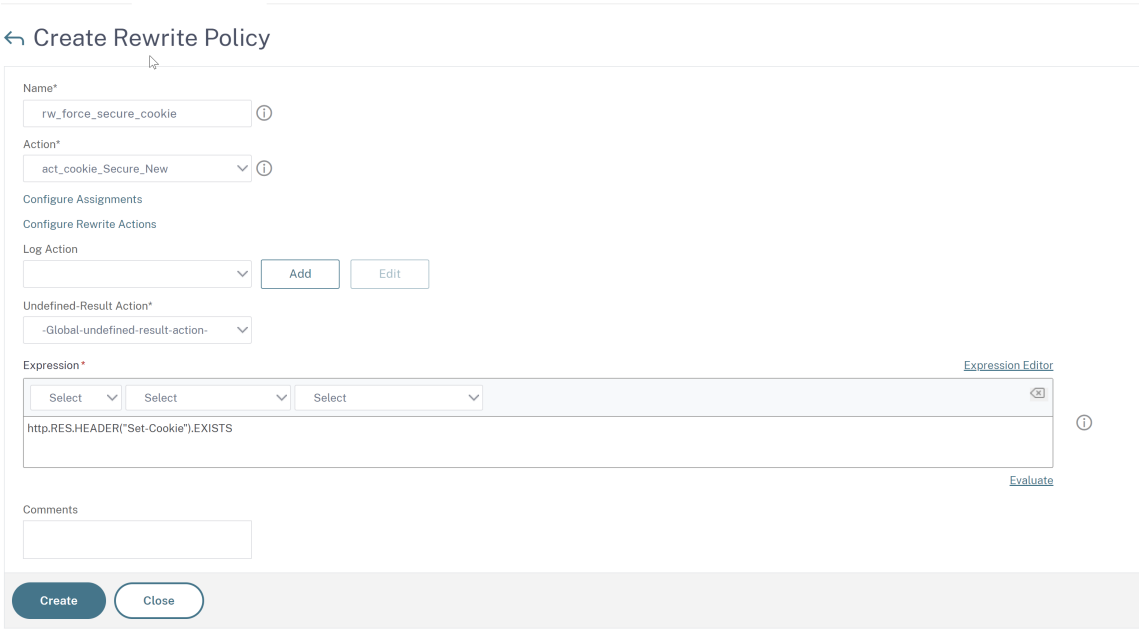
```
Set-Cookie: CtxsAuthId=C5614491; Secure; HttpOnly; path=/Citrix/ProdWeb
    /
<!--NeedCopy-->
```

So konfigurieren Sie die NetScaler-Appliance so, dass die Secure- und HttpOnly-Flags für einen vorhandenen virtuellen HTTP-Server über die grafische Benutzeroberfläche erzwingen

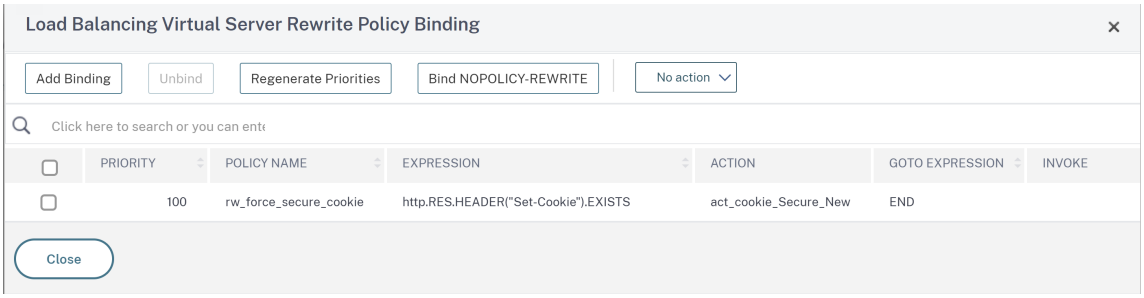
1. Navigieren Sie zu **AppExpert > Rewrite > Aktionen**und klicken Sie auf **Hinzufügen**, um eine neue Neuschreibaktion hinzuzufügen.



2. Navigieren Sie zu **AppExpert > Rewrite > Richtlinien**und klicken Sie auf **Hinzufügen**, um eine neue Rewriterichtlinie hinzuzufügen.



3. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und binden Sie dann die Rewriterichtlinie (Antwort) an den entsprechenden virtuellen SSL-Server.



Beschleunigen des Lastausgleichsverkehrs durch Verwendung von Komprimierung

May 11, 2023

Die Komprimierung ist ein beliebtes Mittel zur Optimierung der Bandbreitennutzung, und die meisten Webbrowser unterstützen komprimierte Daten. Wenn Sie die Komprimierungsfunktion aktivieren, fängt die NetScaler-Appliance Anfragen von Clients ab und bestimmt, ob der Client komprimierte Inhalte akzeptieren kann. Nach Erhalt der HTTP-Antwort vom Server untersucht die Appliance den Inhalt, um festzustellen, ob er komprimierbar ist. Wenn der Inhalt komprimierbar ist, komprimiert die Appliance ihn, ändert den Antwortheader, um die Art der durchgeführten Komprimierung anzugeben, und leitet den komprimierten Inhalt an den Client weiter.

Die NetScaler-Komprimierung ist eine richtlinienbasierte Funktion. Eine Richtlinie filtert Anfragen

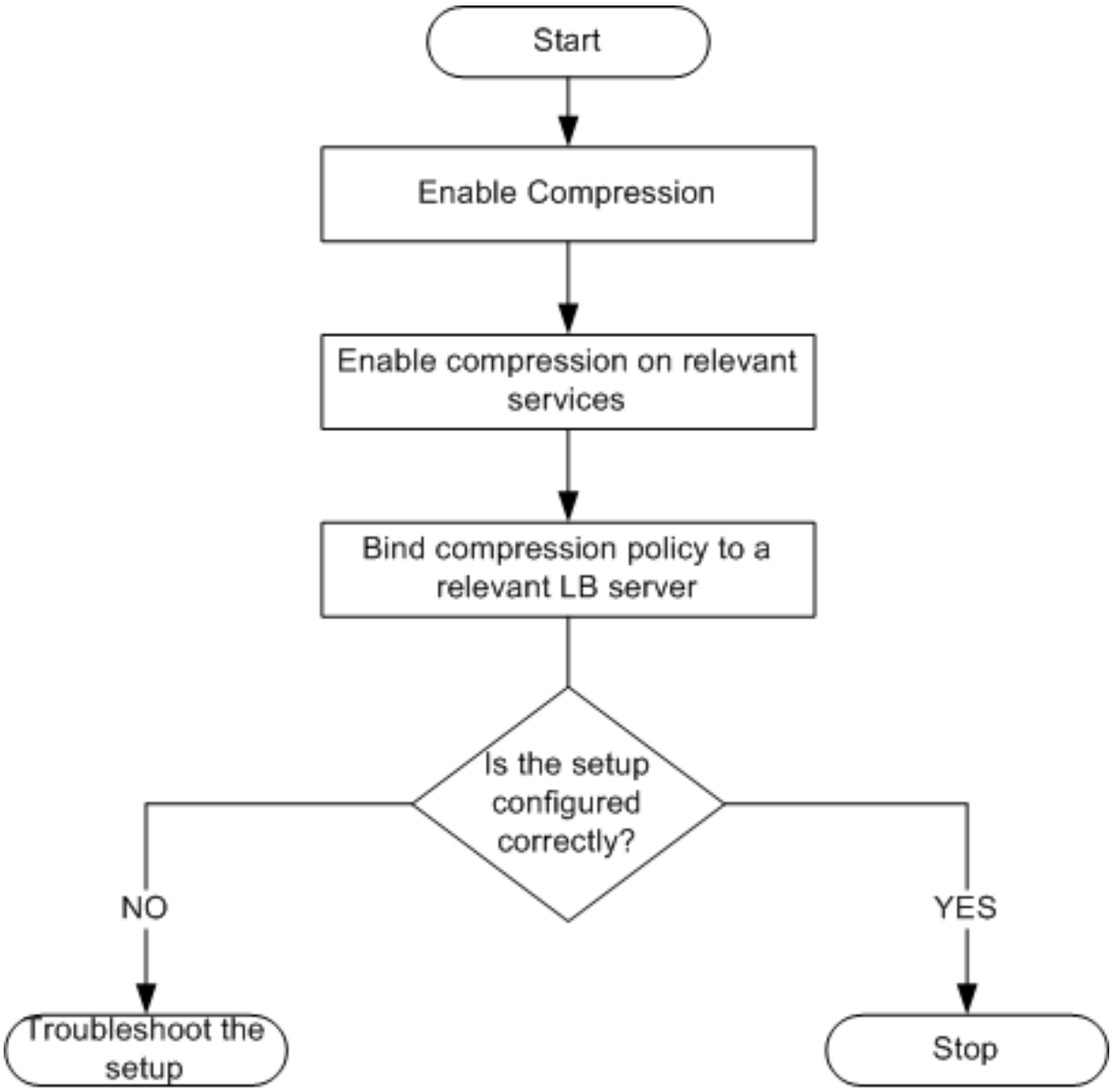
und Antworten, um zu komprimierende Antworten zu identifizieren, und gibt die Art der Komprimierung an, die auf jede Antwort angewendet werden soll. Die Appliance bietet mehrere integrierte Richtlinien zum Komprimieren gängiger MIME-Typen wie Text/HTML, Text/Plain, Text/XML, Text/CSS, Text/RTF, Anwendung/MSWord, Anwendung/VND.MS-Excel und Anwendung/VND.MS-Powerpoint. Sie können auch benutzerdefinierte Richtlinien erstellen. Die Appliance komprimiert keine komprimierten MIME-Typen wie Anwendungs-/Oktettstrom-, Binär-, Byte- und komprimierte Bildformate wie GIF und JPEG.

Um die Komprimierung zu konfigurieren, müssen Sie sie global und für jeden Dienst aktivieren, der Antworten liefert, die komprimiert werden sollen. Wenn Sie virtuelle Server für den Lastenausgleich oder das Content Switching konfiguriert haben, sollten Sie die Richtlinien an die virtuellen Server binden. Andernfalls gelten die Richtlinien für den gesamten Datenverkehr, der durch die Appliance fließt.

Tasksequenz für die Komprimierungs

Das folgende Flussdiagramm zeigt die Reihenfolge der Aufgaben zum Konfigurieren der Basiskomprimierung in einem Lastausgleichs-Setup.

Abbildung 1. Abfolge von Aufgaben zur Konfiguration der Kompression



> Hinweis: Bei den Schritten in der obigen Abbildung wird davon ausgegangen, dass der Lastenausgleich bereits konfiguriert wurde.

Komprimierung aktivieren

Standardmäßig ist die Komprimierung nicht aktiviert. Sie müssen die Komprimierungsfunktion aktivieren, um die Komprimierung von HTTP-Antworten zu ermöglichen, die an den Client gesendet werden.

So aktivieren Sie die Komprimierung über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Komprimierung zu aktivieren und die Konfiguration zu überprüfen:

- enable ns feature CMP
- show ns feature

```
    > enable ns feature CMP



    Done

    > show ns feature



            Feature                         Acronym             Status

            -------                         -------             ------

    1)      Web Logging                     WL                  ON

    2)      Surge Protection                SP                  OFF

    .

    7) Compression Control CMP ON

       .

    Done
<!--NeedCopy-->
```


So aktivieren Sie die Komprimierung über die GUI

1. Erweitern Sie im Navigationsbereich System, und klicken Sie dann auf Einstellungen.
2. Klicken Sie im Detailbereich unter Modi und Funktionenauf Grundfunktionen ändern.
3. Aktivieren Sie im Dialogfeld Grundfunktionen konfigurieren das Kontrollkästchen Komprimierung, und klicken Sie dann auf OK.
4. In den Funktion (en) aktivieren/deaktivieren? klicken Sie auf Ja.

Konfigurieren von Diensten zum Komprimieren von Daten

Zusätzlich zur globalen Aktivierung der Komprimierung müssen Sie sie für jeden Dienst aktivieren, der zu komprimierende Dateien liefert.

So aktivieren Sie die Komprimierung für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Komprimierung eines Dienstes zu aktivieren und die Konfiguration zu überprüfen:

- set service <name> -CMP YES
- show service <name>

```
> show service SVC_HTTP1

SVC_HTTP1 (10.102.29.18:80) - HTTP

State: UP

Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)

Time since last state change: 0 days, 03:03:37.200

Server Name: 10.102.29.18

Server ID : 0   Monitor Threshold : 0

Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits

```



```
24
25 Use Source IP: NO
26
27
28 Client Keepalive(CKA): NO
29
30
31 Access Down Service: NO
32
33
34 TCP Buffering(TCPB): NO
35
36
37 HTTP Compression(CMP): YES
38
39
40 Idle timeout: Client: 180 sec   Server: 360 sec
41
42
43 Client IP: DISABLED
44
45
46 Cacheable: NO
47
48
49 SC: OFF
50
51
52 SP: OFF
53
54
55 Down state flush: ENABLED
56
57 1)      Monitor Name: tcp-default
58
59
60 State: DOWN     Weight: 1
61
62
63 Probes: 1095    Failed [Total: 1095 Current: 1095]
64
65
66 Last response: Failure - TCP syn sent, reset received.
67
68
```



```
Response Time: N/A


Done

<!--NeedCopy-->
```

So aktivieren Sie die Komprimierung eines Dienstes über die GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Wählen Sie im Detailbereich den Dienst aus, für den Sie die Komprimierung konfigurieren möchten (z. B. Service-HTTP-1), und klicken Sie dann auf Öffnen.
3. Aktivieren Sie auf der Registerkarte Erweitert unter Einstellungen das Kontrollkästchen Komprimierung, und klicken Sie dann auf OK.
4. Stellen Sie sicher, dass bei Auswahl des Dienstes HTTP Compression (CMP): ON im Abschnitt **Details** unten im Bereich des Bereichs angezeigt wird.

Binden einer Komprimierungsrichtlinie an einen virtuellen Server

Wenn Sie eine Richtlinie an einen virtuellen Server binden, wird die Richtlinie nur von den Diensten ausgewertet, die diesem virtuellen Server zugeordnet sind. Sie können Komprimierungsrichtlinien entweder über das Dialogfeld Virtuellen Server konfigurieren (Load Balancing) oder über das Dialogfeld Komprimierungsrichtlinien-Manager an einen virtuellen Server binden. Dieses Thema enthält Anweisungen zum Binden von Komprimierungsrichtlinien an einen virtuellen Lastausgleichsserver mithilfe des Dialogfelds Virtuellen Server konfigurieren (Load Balancing).

So binden oder lösen Sie eine Komprimierungsrichtlinie mithilfe der Befehlszeile an einen virtuellen Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Komprimierungsrichtlinie an einen virtuellen Lastausgleichsserver zu binden oder aufzuheben und die Konfiguration zu überprüfen:

- (bind|unbind) lb vserver <name> -policyName <string>
- show lb vserver <name>

Beispiel:

```
> bind lb vserver lbvip -policyName ns_cmp_msapp
Done
> showlbserverlbvip

```



```
lbvip(8.7.6.6:80)-HTTPType:ADDRESS
State:UP
LaststatechangewasatThuMay2805:37:212009(+685ms)
Timesincelaststatechange:19days,04:26:50.470
EffectiveState:UP
ClientIdleTimeout:180sec
Downstateflush:ENABLED
DisablePrimaryVserverOnDown:DISABLED
PortRewrite:DISABLED
No.ofBoundServices:1(Total)1(Active)
ConfiguredMethod:LEASTCONNECTION
CurrentMethod:RoundRobin,Reason:Boundservice'sstatechangedtoUP
Mode:IP
Persistence:NONE
VserverIPandPortinsertion:OFF
Push:DISABLEDPushVServer:
PushMultiClients:NO
PushLabelRule:

BoundServiceGroups:
1)GroupName:Service-Group-1

1)Service-Group-1(10.102.29.252:80)-HTTPState:UPWeight:1

1)Policy:ns_cmp_msappPriority:0

Done

<!--NeedCopy-->
```

So binden oder lösen Sie eine Komprimierungsrichtlinie über die GUI an einen virtuellen Lastausgleichsserver

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, an den Sie eine Komprimierungsrichtlinie binden oder aufheben möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) auf der Registerkarte Richtlinien auf Komprimierung.
4. Führen Sie einen der folgenden Schritte aus:
   - Um eine Komprimierungsrichtlinie zu binden, klicken Sie auf Richtlinie einfügen, und wählen Sie dann die Richtlinie aus, die Sie an den virtuellen Server binden möchten.
   - Um die Bindung einer Komprimierungsrichtlinie aufzuheben, klicken Sie auf den Namen

der Richtlinie, die Sie vom virtuellen Server trennen möchten, und klicken Sie dann auf Richtlinie aufheben.

5. Klicken Sie auf OK.

Sicherer Lastausgleichsverkehr durch Verwendung von SSL

May 11, 2023

Die NetScaler SSL-Offload-Funktion verbessert transparent die Leistung von Websites, die SSL-Transaktionen durchführen. Durch die Übertragung von CPU-intensiven SSL-Verschlüsselungs- und Entschlüsselungsaufgaben vom lokalen Webserver auf die Appliance gewährleistet die SSL-Abladung die sichere Bereitstellung von Webanwendungen ohne die Leistungseinbußen, die bei der Verarbeitung der SSL-Daten durch den Server entstehen. Sobald der SSL-Verkehr entschlüsselt wurde, kann er von allen Standarddiensten verarbeitet werden. Das SSL-Protokoll arbeitet nahtlos mit verschiedenen Arten von HTTP- und TCP-Daten zusammen und bietet einen sicheren Kanal für Transaktionen, die solche Daten verwenden.

Um SSL zu konfigurieren, müssen Sie es zuerst aktivieren. Dann konfigurieren Sie HTTP- oder TCP-Dienste und einen virtuellen SSL-Server auf der Appliance und binden die Dienste an den virtuellen Server. Sie müssen auch ein Zertifikatschlüsselpaar hinzufügen und an den virtuellen SSL-Server binden. Wenn Sie Outlook Web Access-Server verwenden, müssen Sie eine Aktion erstellen, um die SSL-Unterstützung zu aktivieren, und eine Richtlinie zum Anwenden der Aktion. Ein virtueller SSL-Server fängt eingehenden verschlüsselten Datenverkehr ab und entschlüsselt ihn mithilfe eines ausgehandelten Algorithmus. Der virtuelle SSL-Server leitet dann die entschlüsselten Daten zur entsprechenden Verarbeitung an die anderen Entitäten auf der Appliance weiter.

Ausführliche Informationen zum SSL-Offloading finden Sie unter SSL-Offload und Beschleunigung.

SSL-Konfigurations-Tasksequenz

Um SSL zu konfigurieren, müssen Sie es zuerst aktivieren. Dann müssen Sie einen virtuellen SSL-Server und HTTP- oder TCP-Dienste auf der NetScaler-Appliance erstellen. Schließlich müssen Sie ein gültiges SSL-Zertifikat und die konfigurierten Dienste an den virtuellen SSL-Server binden.

Ein virtueller SSL-Server fängt eingehenden verschlüsselten Datenverkehr ab und entschlüsselt ihn mithilfe eines ausgehandelten Algorithmus. Der virtuelle SSL-Server leitet die entschlüsselten Daten dann zur entsprechenden Verarbeitung an die anderen Entitäten auf der NetScaler-Appliance weiter.

Das folgende Flussdiagramm zeigt die Reihenfolge der Aufgaben zum Konfigurieren eines grundlegenden SSL-Offload-Setups.

Abbildung 1. Abfolge von Aufgaben zum Konfigurieren von SSL-Ladung

SSL-Offload aktivieren

Aktivieren Sie zuerst die SSL-Funktion. Sie können SSL-basierte Entitäten auf der Appliance konfigurieren, ohne die SSL-Funktion zu aktivieren, aber sie funktionieren erst, wenn Sie SSL aktivieren.

Aktivieren Sie SSL über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um SSL-Offload zu aktivieren und die Konfiguration zu überprüfen:

```
-  enable ns feature SSL
-  show ns feature
<!--NeedCopy-->
```

Beispiel:

```
> enable ns feature ssl

Done


> show ns feature


Feature Acronym Status


------- ------- ------


1) Web Logging WL ON


2) SurgeProtection SP OFF


3) Load Balancing LB ON . . .


 9) SSL Offloading SSL ON


10) Global Server Load Balancing GSLB ON . .


```



```
30 Done >
31 <!--NeedCopy-->
```

Aktivieren Sie SSL über die GUI

Führen Sie die folgenden Schritte aus:

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter **Modi und Funktionen**auf **Grundfunktionen ändern**.
3. Aktivieren Sie das **Kontrollkästchen SSL-Ladung**, und klicken Sie dann auf **OK**.
4. In den **Funktion (en) aktivieren/deaktivieren?** klicken Sie auf **Ja**.

Erstellen von HTTP-Diensten

Ein Dienst auf der Appliance repräsentiert eine Anwendung auf einem Server. Nach der Konfiguration befinden sich die Dienste im Status Deaktiviert, bis die Appliance den Server im Netzwerk erreichen und seinen Status überwachen kann. In diesem Thema werden die Schritte zum Erstellen eines HTTP-Dienstes behandelt.

Hinweis: Führen Sie für TCP-Verkehr die folgenden Verfahren aus, erstellen Sie jedoch TCP-Dienste anstelle von HTTP-Diensten.

Fügen Sie über die CLI einen HTTP-Dienst hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen HTTP-Dienst hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add service <name> (<IP> | <serverName>) <serviceType> <port>
2 -  show service <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add service SVC_HTTP1 10.102.29.18 HTTP 80
2
3
4  Done
5
6
7 > show service SVC_HTTP1
8
9
10         SVC_HTTP1 (10.102.29.18:80) - HTTP
```



```
11
12
13          State: UP
14
15
16          Last state change was at Wed Jul 15 06:13:05 2009
17
18
19          Time since last state change: 0 days, 00:00:15.350
20
21
22          Server Name: 10.102.29.18
23
24
25          Server ID : 0   Monitor Threshold : 0
26
27
28          Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
29
30
31          Use Source IP: NO
32
33
34          Client Keepalive(CKA): NO
35
36
37          Access Down Service: NO
38
39
40          TCP Buffering(TCPB): NO
41
42
43          HTTP Compression(CMP): YES
44
45
46          Idle timeout: Client: 180 sec   Server: 360 sec
47
48
49          Client IP: DISABLED
50
51
52          Cacheable: NO
53
54
55          SC: OFF
```



```
56
57
58          SP: OFF
59
60
61          Down state flush: ENABLED
62
63
64
65
66
67  1)      Monitor Name: tcp-default
68
69
70                  State: UP       Weight: 1
71
72
73                  Probes: 4       Failed [Total: 0 Current: 0]
74
75
76                  Last response: Success - TCP syn+ack received.
77
78
79                  Response Time: N/A
80
81
82   Done
83  <!--NeedCopy-->
```

Fügen Sie über die GUI einen HTTP-Dienst hinzu

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL Offload > Dienste**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Dienst erstellen** den Namen des Dienstes, die IP-Adresse und den Port ein (z. B. SVC_HTTP1, 10.102.29.18 und 80).
4. Wählen Sie in der Liste **Protokoll** den Typ des Dienstes aus (z. B. HTTP).
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Der von Ihnen konfigurierte HTTP-Dienst wird auf der Seite Dienste angezeigt.
6. Stellen Sie sicher, dass die von Ihnen konfigurierten Parameter korrekt konfiguriert sind, indem Sie den Dienst auswählen und den Abschnitt Details unten im Bereich anzeigen.

Fügen Sie einen SSL-basierten virtuellen Server hinzu

In einem einfachen SSL-Offloading-Setup fängt der virtuelle SSL-Server verschlüsselten Datenverkehr ab, entschlüsselt ihn und sendet die Klartextnachrichten an die Dienste, die an den virtuellen Server gebunden sind. Durch das Ausladen der CPU-intensiven SSL-Verarbeitung auf die Appliance können die Back-End-Server eine größere Anzahl von Anfragen verarbeiten.

Fügen Sie über die CLI einen SSL-basierten virtuellen Server hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen SSL-basierten virtuellen Server zu erstellen und die Konfiguration zu überprüfen:

```
-  add lb vserver <name> <serviceType> [<IPAddress> <port>]
-  show lb vserver <name>
<!--NeedCopy-->
```

> **Vorsicht:** Um sichere Verbindungen zu gewährleisten, müssen Sie ein gültiges SSL-Zertifikat an den SSL-basierten virtuellen Server binden, bevor Sie es aktivieren.

Beispiel:

```
> add lb vserver vserver-SSL-1 SSL 10.102.29.50 443
  Done


  > show lb vserver vserver-SSL-1


  vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS


  State: DOWN[Certkey not bound] Last state change was at Tue Jun 16
     06:33:08 2009 (+176 ms)


  Time since last state change: 0 days, 00:03:44.120


  Effective State: DOWN Client Idle Timeout: 180 sec


  Down state flush: ENABLED


  Disable Primary Vserver On Down : DISABLED
```



```
24
25
26    No. of Bound Services : 0 (Total) 0 (Active)
27
28
29    Configured Method: LEASTCONNECTION Mode: IP
30
31
32    Persistence: NONE
33
34
35    Vserver IP and Port insertion: OFF
36
37
38    Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:
          Done
39  <!--NeedCopy-->
```

Fügen Sie über die GUI einen SSL-basierten virtuellen Server hinzu

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL-Offload > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Virtuellen Server erstellen (SSL-Offload)** den Namen des virtuellen Servers, die IP-Adresse und den Port ein.
4. Wählen Sie in der Liste **Protokoll** den Typ des virtuellen Servers aus, z. B.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Stellen Sie sicher, dass die von Ihnen konfigurierten Parameter korrekt konfiguriert sind, indem Sie den virtuellen Server auswählen und den Abschnitt Details unten im Bereich anzeigen. Der virtuelle Server ist als DOWN gekennzeichnet, da ein Zertifikatschlüsselpaar und Dienste nicht an ihn gebunden waren.

> **Vorsicht:** Um sichere Verbindungen zu gewährleisten, müssen Sie ein gültiges SSL-Zertifikat an den SSL-basierten virtuellen Server binden, bevor Sie es aktivieren.

Binden Sie Dienste an den virtuellen SSL-Server

Nach dem Entschlüsseln der eingehenden Daten leitet der virtuelle SSL-Server die Daten an die Dienste weiter, die Sie an den virtuellen Server gebunden haben.

Die Datenübertragung zwischen der Appliance und den Servern kann verschlüsselt oder im Klartext erfolgen. Wenn die Datenübertragung zwischen der Appliance und den Servern verschlüsselt ist, ist

die gesamte Transaktion von Ende zu Ende sicher. Weitere Informationen zum Konfigurieren des Systems für End-to-End-Sicherheit finden Sie unter SSL-Offload and Acceleration.

Binden eines Dienstes an einen virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Dienst an den virtuellen SSL-Server zu binden und die Konfiguration zu überprüfen:

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> bind lb vserver vserver-SSL-1 SVC_HTTP1



  Done


  > show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) -
     SSL Type:


  ADDRESS State: DOWN[Certkey not bound]


  Last state change was at Tue Jun 16 06:33:08 2009 (+174 ms)


  Time since last state change: 0 days, 00:31:53.70


  Effective State: DOWN Client Idle


  Timeout: 180 sec


  Down state flush: ENABLED Disable Primary Vserver On Down :


  DISABLED No. of Bound Services : 1 (Total) 0 (Active)
```



```
31
32
33    Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver
          IP and
34
35
36    Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients:
          NO Push Label Rule:
37
38
39
40
41
42    1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
43
44
45    State: DOWN Weight: 1
46
47
48    Done
49  <!--NeedCopy-->
```

Binden Sie einen Dienst über die GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management > SSL-Offload > Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus, und klicken Sie dann auf **Öffnen**.
3. Aktivieren Sie auf der Registerkarte **Dienste** in der Spalte **Aktiv** die Kontrollkästchen neben den Diensten, die Sie an den ausgewählten virtuellen Server binden möchten.
4. Klicken Sie auf **OK**.
5. Stellen Sie sicher, dass der Zähler Anzahl gebundener Dienste im Abschnitt Details am unteren Rand des Bereichs um die Anzahl der Dienste erhöht wird, die Sie an den virtuellen Server gebunden haben.

Fügen Sie ein Zertifikatschlüsselpaar hinzu

Ein SSL-Zertifikat ist ein integraler Bestandteil des SSL Key-Exchange- und Verschlüsselungs-/Entschlüsselungsprozesses. Das Zertifikat wird während eines SSL-Handshakes verwendet, um die Identität des SSL-Servers festzustellen. Sie können ein gültiges, vorhandenes SSL-Zertifikat verwenden, das Sie auf der NetScaler-Appliance haben, oder Sie können ein eigenes SSL-Zertifikat erstellen. Die Appliance unterstützt RSA-Zertifikate mit bis zu 4096 Bit.

ECDSA-Zertifikate mit nur den folgenden Kurven werden unterstützt:

- prime256v1 (P_256 im ADC)
- secp384r1 (P_384 im ADC)
- secp521r1 (P_521 im ADC; nur auf VPX unterstützt)
- secp224r1 (P_224 im ADC; nur auf VPX unterstützt)

> **Hinweis:** Citrix empfiehlt, dass Sie ein gültiges SSL-Zertifikat verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde. Ungültige Zertifikate und selbst erstellte Zertifikate sind nicht mit allen SSL-Clients kompatibel.

Bevor ein Zertifikat für die SSL-Verarbeitung verwendet werden kann, müssen Sie es mit dem entsprechenden Schlüssel koppeln. Das Zertifikatschlüsselpaar wird dann an den virtuellen Server gebunden und für die SSL-Verarbeitung verwendet.

Hinzufügen eines Zertifikatsschlüsselpaars über die CLI

> **Hinweis:** Informationen zum Erstellen eines ECDSA-Zertifikatschlüsselpaars finden Sie unter Erstellen eines ECDSA-Zertifikatschlüsselpaars.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein Zertifikatschlüsselpaar zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add ssl certKey <certkeyName> -cert <string> [-key <string>]
2 -  show sslcertkey <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1  > add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key
2
3   Done
4
5
6  > show sslcertkey CertKey-SSL-1
7
8
9     Name: CertKey-SSL-1 Status: Valid,
10
11
12    Days to expiration:4811 Version: 3
13
14
15    Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer:
         C=US,ST=California,L=San
16
17
```



```
18     Jose,O=Citrix ANG,OU=NS Internal,CN=de fault
19
20
21     Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17
           21:26:47 2022 GMT
22
23
24     Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,
           CN=d efault Public Key
25
26
27     Algorithm: rsaEncryption Public Key
28
29
30     size: 1024
31
32
33   Done
34 <!--NeedCopy-->
```

Fügen Sie über die GUI ein Zertifikatschlüsselpaar hinzu

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Zertifikat installieren** im Textfeld Name des Zertifikatschlüsselpaars einen Namen für das Zertifikatschlüsselpaar ein, das Sie hinzufügen möchten, z. B. CertKey-SSL-1.
4. Klicken Sie unter **Details**unter Certificate File Name auf **Durchsuchen (Appliance)**, um das Zertifikat zu suchen. Sowohl das Zertifikat als auch der Schlüssel werden im Ordner /nsconfig/ssl/ auf der Appliance gespeichert. Um ein auf dem lokalen System vorhandenes Zertifikat zu verwenden, wählen Sie Lokal aus.
5. Wählen Sie das Zertifikat aus, das Sie verwenden möchten, und klicken Sie dann auf **Auswählen**.
6. Klicken Sie unter Private Key File Name auf **Durchsuchen (Appliance)**, um die Datei mit dem privaten Schlüssel zu suchen. Um einen privaten Schlüssel auf dem lokalen System zu verwenden, wählen Sie Lokal aus.
7. Wählen Sie den Schlüssel aus, den Sie verwenden möchten, und klicken Sie auf **Auswählen**. Um den im Zertifikatschlüsselpaar verwendeten Schlüssel zu verschlüsseln, geben Sie das für die Verschlüsselung zu verwendende Kennwort in das Textfeld Kennwort ein.
8. Klicken Sie auf **Installieren**.

9. Doppelklicken Sie auf das Zertifikatschlüsselpaar und überprüfen Sie im Fenster Zertifikatsdetails, ob die Parameter korrekt konfiguriert und gespeichert wurden.

Binden Sie ein SSL-Zertifikatschlüsselpaar an den virtuellen Server

Nachdem Sie ein SSL-Zertifikat mit dem entsprechenden Schlüssel gekoppelt haben, binden Sie das Zertifikatschlüsselpaar an den virtuellen SSL-Server, damit es für die SSL-Verarbeitung verwendet werden kann. Sichere Sitzungen erfordern das Herstellen einer Verbindung zwischen dem Clientcomputer und einem SSL-basierten virtuellen Server auf der Appliance. Die SSL-Verarbeitung wird dann für den eingehenden Datenverkehr auf dem virtuellen Server durchgeführt. Bevor Sie den virtuellen SSL-Server auf der Appliance aktivieren, müssen Sie daher ein gültiges SSL-Zertifikat an den virtuellen SSL-Server binden.

Binden Sie ein SSL-Zertifikatschlüsselpaar über die CLI an einen virtuellen Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein SSL-Zertifikatschlüsselpaar an einen virtuellen Server zu binden und die Konfiguration zu überprüfen:

```
-  bind ssl vserver <vServerName> -certkeyName <string>
-  show ssl vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1

Done


> show ssl vserver Vserver-SSL-1




     Advanced SSL configuration for VServer Vserver-SSL-1:


     DH: DISABLED


     Ephemeral RSA: ENABLED Refresh Count: 0

```



```
20
21       Session Reuse: ENABLED Timeout: 120 seconds
22
23
24       Cipher Redirect: ENABLED
25
26
27       SSLv2 Redirect: ENABLED
28
29
30       ClearText Port: 0
31
32
33       Client Auth: DISABLED
34
35
36       SSL Redirect: DISABLED
37
38
39       Non FIPS Ciphers: DISABLED
40
41
42       SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
43
44
45
46
47
48  1) CertKey Name: CertKey-SSL-1 Server Certificate
49
50
51  1) Cipher Name: DEFAULT
52
53
54     Description: Predefined Cipher Alias
55
56
57  Done
58  <!--NeedCopy-->
```

Binden Sie ein SSL-Zertifikatschlüsselpaar über die GUI an einen virtuellen Server

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL-Offload > Virtuelle Server**.
2. Wählen Sie den virtuellen Server aus, an den Sie das Zertifikatschlüsselpaar binden möchten, z. B. vServer-SSL-1, und klicken Sie auf Öffnen.
3. Wählen **Sie im Dialogfeld Virtuellen Server konfigurieren (SSL-Offload)** auf der Registerkarte **SSL-Einstellungen** unter **Verfügbar**das Zertifikatschlüsselpaar aus, das Sie an den virtuellen Server binden möchten. Klicken Sie dann auf **Hinzufügen**.
4. Klicken Sie auf **OK**.
5. Stellen Sie sicher, dass das von Ihnen ausgewählte Zertifikatschlüsselpaar im Bereich Konfiguriert angezeigt wird.

Konfigurieren der Unterstützung für Outlook Web Access

Wenn Sie Outlook Web Access (OWA) -Server auf Ihrer NetScaler-Appliance verwenden, müssen Sie die Appliance so konfigurieren, dass ein spezielles Header-Feld, FRONT-END-HTTPS: ON, in HTTP-Anforderungen an die OWA-Server eingefügt wird, damit die Server `https://` anstelle von URL-Links generieren `http://`.

Hinweis: Sie können die OWA-Unterstützung nur für HTTP-basierte virtuelle SSL-Server und -Dienste aktivieren. Sie können es nicht für TCP-basierte virtuelle SSL-Server und -Dienste anwenden.

Gehen Sie wie folgt vor, um die OWA-Unterstützung zu konfigurieren:

- Erstellen Sie eine SSL-Aktion, um die OWA-Unterstützung zu aktivieren.
- Erstellen Sie eine SSL-Richtlinie.
- Binden Sie die Richtlinie an den virtuellen SSL-Server.

Erstellen Sie eine SSL-Aktion, um OWA-Unterstützung zu aktivieren

Bevor Sie die Unterstützung von Outlook Web Access (OWA) aktivieren können, müssen Sie eine SSL-Aktion erstellen. SSL-Aktionen sind an SSL-Richtlinien gebunden und werden ausgelöst, wenn eingehende Daten der in der Richtlinie angegebenen Regel entsprechen.

Erstellen Sie eine SSL-Aktion, um die OWA-Unterstützung über die CLI zu aktivieren

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine SSL-Aktion zu erstellen, um die OWA-Unterstützung zu aktivieren und die Konfiguration zu überprüfen:

```
1 -  add ssl action <name> -OWASupport ENABLED
2 -  show SSL action <name>
3 <!--NeedCopy-->
```

Beispiel:


```
    > add ssl action Action-SSL-OWA -OWASupport enabled



    Done

    > show SSL action Action-SSL-OWA

    Name: Action-SSL-OWA

    Data Insertion Action: OWA

    Support: ENABLED

    Done
<!--NeedCopy-->
```

Erstellen Sie eine SSL-Aktion, um die OWA-Unterstützung über die GUI zu aktivieren

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.
2. Klicken Sie im Detailbereich auf der Registerkarte **Aktionen** auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld SSL-Aktion erstellen** im Textfeld Name Action-SSL-OWA ein.
4. Wählen Sie unter Outlook Web Access die Option **Aktiviert**.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Stellen Sie sicher, dass Action-SSL-OWA auf der Seite **SSL-Aktionen** angezeigt wird.

Erstellen von SSL-Richtlinien

SSL-Richtlinien werden mithilfe der Richtlinieninfrastruktur erstellt. An jede SSL-Richtlinie ist eine SSL-Aktion gebunden, und die Aktion wird ausgeführt, wenn eingehender Datenverkehr mit der in der Richtlinie konfigurierten Regel übereinstimmt.

Erstellen einer SSL-Richtlinie über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine SSL-Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
-  add ssl policy <name> -rule <expression> -reqAction <string>
-  show ssl policy <name>
<!--NeedCopy-->
```

Beispiel:

```
> add ssl policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA

Done

> show ssl policy-SSL-1

Name: Policy-SSL-1 Rule: ns_true

Action: Action-SSL-OWA Hits: 0

Policy is bound to following entities

1) PRIORITY : 0

Done
<!--NeedCopy-->
```

Erstellen einer SSL-Richtlinie über die GUI

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **SSL-Richtlinie erstellen** im Textfeld Name den Namen der SSL-Richtlinie ein (z. B. Policy-SSL-1).
4. Wählen Sie unter der Aktion **Request** die konfigurierte SSL-Aktion aus, die Sie dieser Richtlinie zuordnen möchten (z. B. Action-SSL-OWA). Der allgemeine Ausdruck ns_true wendet die Richtlinie auf den gesamten erfolgreichen SSL-Handshake-Verkehr an. Um bestimmte Antworten zu filtern, können Sie jedoch Richtlinien mit einer höheren Detailgenauigkeit erstellen. Weitere Informationen zum Konfigurieren granularer Richtlinienausdrücke finden Sie unter SSL-Aktionen und Richtlinien.
5. Wählen Sie in **Benannte Ausdrücke**den integrierten allgemeinen Ausdruck ns_true aus und

klicken Sie auf **Ausdruck hinzufügen**. Der Ausdruck ns_true wird jetzt im Textfeld Ausdruck angezeigt.

6. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
7. Stellen Sie sicher, dass die Richtlinie korrekt konfiguriert ist, indem Sie die Richtlinie auswählen und den Abschnitt Details unten im Bereich anzeigen.

Binden Sie die SSL-Richtlinie an den virtuellen SSL-Server

Nachdem Sie eine SSL-Richtlinie für Outlook Web Access konfiguriert haben, binden Sie die Richtlinie an einen virtuellen Server, der eingehenden Outlook-Datenverkehr abfängt. Wenn die eingehenden Daten mit einer der in der SSL-Richtlinie konfigurierten Regeln übereinstimmen, wird die Richtlinie ausgelöst und die damit verbundene Aktion wird ausgeführt.

Binden Sie eine SSL-Richtlinie über die CLI an einen virtuellen SSL-Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine SSL-Richtlinie an einen virtuellen SSL-Server zu binden und die Konfiguration zu überprüfen:

```
-  bind ssl vserver <vServerName> -policyName <string>
-  show ssl vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1

 Done

> show ssl vserver Vserver-SSL-1

Advanced SSL configuration for VServer Vserver-SSL-1:

DH: DISABLED

Ephemeral RSA: ENABLED

Refresh Count: 0

Session Reuse: ENABLED

Timeout: 120 seconds

Cipher Redirect: ENABLED
```



```
20
21 SSLv2 Redirect: ENABLED
22
23 ClearText Port: 0
24
25 Client Auth: DISABLED
26
27 SSL Redirect: DISABLED
28
29 Non FIPS Ciphers: DISABLED
30
31 SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
32
33 1) CertKey Name: CertKey-SSL-1 Server Certificate
34
35 1) Policy Name: Policy-SSL-1 Priority: 0
36
37 1) Cipher Name: DEFAULT Description: Predefined Cipher Alias
38
39 Done
40 <!--NeedCopy-->
```

Binden Sie eine SSL-Richtlinie über die GUI an einen virtuellen SSL-Server

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL-Offload > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus (z. B. vServer-SSL-1), und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Virtuellen Server konfigurieren (SSL-Offload)** auf **Richtlinie einfügen**, und wählen Sie dann die Richtlinie aus, die Sie an den virtuellen SSL-Server binden möchten. Optional können Sie auf das Feld Priorität doppelklicken und eine neue Prioritätsstufe eingeben.
4. Klicken Sie auf **OK**.

Funktionen auf einen Blick

May 11, 2023

Die NetScaler-Funktionen können unabhängig oder in Kombinationen konfiguriert werden, um spezifische Anforderungen zu erfüllen. Obwohl einige Features in mehr als einer Kategorie passen, können

die zahlreichen NetScaler Funktionen im Allgemeinen als Anwendungswechsel und Verkehrsverwaltungsfunktionen, Anwendungsbeschleunigungsfunktionen sowie Anwendungssicherheits- und Firewallfunktionen sowie Anwendungssichtbarkeitsfunktion kategorisiert werden.

Informationen zur Reihenfolge, in der die Features ihre Verarbeitung durchführen, finden Sie im Abschnitt Verarbeitungsreihenfolge der Funktionen .

Funktionen für Anwendungs-Switching und Verkehrsmanagement

May 11, 2023

Nachfolgend finden Sie die Funktionen für Anwendungswechsel und Verkehrsmanagement.

SSL Offloading

Lädt die SSL-Verschlüsselung und -Entschlüsselung transparent von Webservern aus, wodurch Serverressourcen für Serviceanfragen freigegeben werden. SSL belastet die Leistung einer Anwendung stark und kann viele Optimierungsmaßnahmen unwirksam machen. SSL-Offload und -Beschleunigung ermöglichen die Anwendung aller Vorteile der Citrix Request Switching-Technologie auf den SSL-Datenverkehr, wodurch eine sichere Bereitstellung von Webanwendungen gewährleistet wird, ohne dass die Endbenutzerleistung beeinträchtigt wird.

Weitere Informationen finden Sie unter SSL-Offload und Beschleunigung.

Zugriffssteuerungslisten

Vergleicht eingehende Pakete mit Zugriffssteuerungslisten (ACLs). Wenn ein Paket mit einer ACL-Regel übereinstimmt, wird die in der Regel angegebene Aktion auf das Paket angewendet. Andernfalls wird die Standardaktion (ALLOW) angewendet und das Paket wird normal verarbeitet. Damit die Appliance eingehende Pakete mit den ACLs vergleichen kann, müssen Sie die ACLs anwenden. Alle ACLs sind standardmäßig aktiviert, aber Sie müssen sie anwenden, damit die NetScaler-Appliance eingehende Pakete mit ihnen vergleichen kann. Wenn eine ACL nicht Teil der Nachschlagetabelle sein muss, aber dennoch in der Konfiguration beibehalten werden muss, sollte sie deaktiviert werden, bevor die ACLs angewendet werden. Eine ADC-Appliance vergleicht eingehende Pakete nicht mit deaktivierten ACLs.

Weitere Informationen finden Sie unter Zugriffssteuerungsliste.

Lastausgleich

Load Balancing-Entscheidungen basieren auf einer Vielzahl von Algorithmen, darunter Round-Robin, geringste Verbindungen, gewichtete geringste Bandbreite, gewichtete geringste Pakete, minimale

Reaktionszeit und Hashing basierend auf URL, Domänenquell-IP oder Ziel-IP. Sowohl das TCP- als auch das UDP-Protokoll werden unterstützt, sodass die NetScaler-Appliance den gesamten Datenverkehr ausgleichen kann, der diese Protokolle als zugrunde liegenden Träger verwendet (z. B. HTTP, HTTPS, UDP, DNS, NNTP und allgemeiner Firewall-Verkehr). Darüber hinaus kann die ADC-Appliance die Sitzungspersistenz basierend auf Quell-IP, Cookie, Server, Gruppe oder SSL-Sitzung aufrechterhalten. Es ermöglicht Benutzern, benutzerdefinierte Extended Content Verification (ECV) auf Server, Caches, Firewalls und andere Infrastrukturgeräte anzuwenden, um sicherzustellen, dass diese Systeme ordnungsgemäß funktionieren und den Benutzern die richtigen Inhalte bereitstellen. Es kann auch Zustandsprüfungen mithilfe von Ping-, TCP- oder HTTP-URL durchführen, und der Benutzer kann Monitore basierend auf Perl-Skripten erstellen.
Um eine hochwertige WAN-Optimierung zu ermöglichen, können die in Rechenzentren bereitgestellten CloudBridge-Appliances über NetScaler-Appliances einen Lastausgleich durchführen. Die Bandbreite und Anzahl gleichzeitiger Sitzungen lassen sich erheblich verbessern.

Weitere Informationen finden Sie unter Load Balancing.

Traffic-Domänen

Verkehrsdomänen bieten eine Möglichkeit, logische ADC-Partitionen in einer einzelnen NetScaler-Appliance zu erstellen. Sie ermöglichen es Ihnen, den Netzwerkverkehr für verschiedene Anwendungen zu segmentieren. Sie können Traffic-Domänen verwenden, um mehrere isolierte Umgebungen zu erstellen, deren Ressourcen nicht miteinander interagieren. Eine Anwendung, die zu einer bestimmten Verkehrsdomäne gehört, kommuniziert nur mit Entitäten und verarbeitet Datenverkehr innerhalb dieser Domäne. Verkehr, der zu einer Verkehrsdomäne gehört, kann die Grenze einer anderen Verkehrsdomäne nicht überschreiten. Daher können Sie doppelte IP-Adressen auf der Appliance verwenden, solange eine Adresse nicht innerhalb derselben Domäne dupliziert wird.

Weitere Informationen finden Sie unter Traffic-Domains.

Netzwerkadressübersetzung

Die Netzwerkadressübersetzung (NAT) beinhaltet die Änderung der Quell- und/oder Ziel-IP-Adressen und/oder der TCP/UDP-Portnummern von IP-Paketen, die die NetScaler-Appliance passieren. Das Aktivieren von NAT auf der Appliance erhöht die Sicherheit Ihres privaten Netzwerks und schützt es vor einem öffentlichen Netzwerk wie dem Internet, indem die Quell-IP-Adressen Ihres Netzwerks geändert werden, wenn Daten die NetScaler-Appliance passieren.

Die NetScaler-Appliance unterstützt die folgenden Arten der Netzwerkadressübersetzung:

INAT: In Inbound NAT (INAT) hört eine auf der NetScaler-Appliance konfigurierte IP-Adresse (normalerweise öffentlich) im Namen eines Servers Verbindungsanforderungen ab. Für ein Anforderungspaket, das von der Appliance auf einer öffentlichen IP-Adresse empfangen wird, ersetzt der ADC die Ziel-IP-Adresse durch die private IP-Adresse des Servers. Mit anderen Worten, die Appliance fungiert

als Proxy zwischen Clients und dem Server. Die INAT-Konfiguration umfasst INAT-Regeln, die eine 1:1 -Beziehung zwischen der IP-Adresse auf der NetScaler-Appliance und der IP-Adresse des Servers definieren.

RNAT: Bei Reverse Network Address Translation (RNAT) ersetzt die NetScaler-Appliance für eine von einem Server initiierte Sitzung die Quell-IP-Adresse in den vom Server generierten Paketen durch eine auf der Appliance konfigurierte IP-Adresse (Typ SNIP). Die Appliance verhindert dadurch, dass die IP-Adresse des Servers in einem der vom Server generierten Pakete verfügbar gemacht wird. Eine RNAT Konfiguration beinhaltet eine RNAT Regel, die eine Bedingung angibt. Die Appliance führt eine RNAT-Verarbeitung für die Pakete durch, die der Bedingung entsprechen.

Zustandslose NAT46-Übersetzung: Stateless NAT46 ermöglicht die Kommunikation zwischen IPv4- und IPv6-Netzwerken über die IPv4-zu-IPv6-Paketübersetzung und umgekehrt, ohne Sitzungsinformationen auf der NetScaler-Appliance beizubehalten. Eine zustandslose NAT46-Konfiguration beinhaltet eine IPv4-IPv6-INAT-Regel und ein NAT46-IPv6-Präfix.

Stateful NAT64-Übersetzung: Die stateful NAT64-Funktion ermöglicht die Kommunikation zwischen IPv4-Clients und IPv6-Servern über die IPv6-zu-IPv4-Paketübersetzung und umgekehrt, während Sitzungsinformationen auf der NetScaler-Appliance verwaltet werden. Eine statusbehaftete NAT64-Konfiguration beinhaltet eine NAT64-Regel und ein NAT64-IPv6-Präfix.

Weitere Informationen finden Sie unter Konfigurieren der Netzwerkadressübersetzung.

Multipath-TCP-Unterstützung

NetScaler-Appliances unterstützen Multipath TCP (MPTCP). MPTCP ist eine TCP/IP-Protokollerweiterung, die mehrere zwischen Hosts verfügbare Pfade identifiziert und verwendet, um die TCP-Sitzung aufrechtzuerhalten. Sie müssen MPTCP für ein TCP-Profil aktivieren und an einen virtuellen Server binden. Wenn MPTCP aktiviert ist, fungiert der virtuelle Server als MPTCP-Gateway und konvertiert MPTCP-Verbindungen mit den Clients in TCP-Verbindungen, die er mit den Servern verwaltet.

Weitere Informationen finden Sie unter MPTCP (Multi-Path TCP).

Content Switching

Bestimmt den Server, an den die Anforderung gesendet werden soll, auf der Grundlage konfigurierter Content Switching-Richtlinien. Richtlinienregeln können auf der IP-Adresse, der URL und den HTTP-Headern basieren. Auf diese Weise können die Switching-Entscheidungen auf Benutzer- und Geräteeigenschaften basieren, z. B. wer der Benutzer ist, welcher Art von Agent verwendet wird und welche Inhalte der Benutzer angefordert hat.

Weitere Informationen finden Sie unter Content Switching.

Globaler Serverlastenausgleich (GSLB)

Erweitert die Traffic-Management-Funktionen eines NetScaler um verteilte Internetseiten und globale Unternehmen. Unabhängig davon, ob die Installationen über mehrere Netzwerkstandorte oder mehrere Cluster an einem einzigen Standort verteilt sind, behält der NetScaler die Verfügbarkeit bei und verteilt den Datenverkehr auf diese. Es trifft intelligente DNS-Entscheidungen, um zu verhindern, dass Benutzer zu einer ausgefallenen oder überlasteten Website gesendet werden. Wenn die Proximity-basierte GSLB-Methode aktiviert ist, kann NetScaler Lastausgleichsentscheidungen basierend auf der Nähe des lokalen DNS-Servers (LDNS) des Clients in Bezug auf verschiedene Standorte treffen. Der Hauptvorteil der proximitätsbasierten GSLB-Methode ist eine schnellere Reaktionszeit, die sich aus der Auswahl des nächstgelegenen verfügbaren Standorts ergibt.

Weitere Informationen finden Sie unter Globaler Server-Lastenausgleich.

Dynamisches Routing

Ermöglicht Routern das automatische Abrufen von Topologieinformationen, Routen und IP-Adressen von benachbarten Routern. Wenn dynamisches Routing aktiviert ist, hört der entsprechende Routing-Prozess auf Routenaktualisierungen und kündigt Routen an. Die Routing-Prozesse können auch in den passiven Modus versetzt werden. Routingprotokolle ermöglichen es einem Upstream-Router, Datenverkehr auf identische virtuelle Server auszugleichen, die auf zwei eigenständigen NetScaler Einheiten gehostet werden, mit der Equal Cost Multipath Technik.

Weitere Informationen finden Sie unter Konfigurieren dynamischer Routen.

Link-Lastausgleich

Load gleicht mehrere WAN-Verbindungen aus und bietet Link-Failover, wodurch die Netzwerkleistung weiter optimiert und die Geschäftskontinuität sichergestellt wird. Stellt sicher, dass Netzwerkverbindungen hochverfügbar bleiben, indem intelligente Verkehrssteuerung und Zustandsprüfungen angewendet werden, um den Datenverkehr effizient auf Upstream-Router zu verteilen. Identifiziert die beste WAN-Verbindung, um eingehenden und ausgehenden Datenverkehr basierend auf Richtlinien und Netzwerkbedingungen zu leiten, und schützt Anwendungen vor WAN- oder Internetverbindungsausfällen durch schnelle Fehlererkennung und Failover.

Weitere Informationen finden Sie unter Link Load Balancing.

TCP-Optimierung

Sie können TCP-Profile verwenden, um den TCP-Verkehr zu optimieren. TCP-Profile definieren die Art und Weise, wie virtuelle NetScaler-Server TCP-Verkehr verarbeiten. Administratoren können die integrierten TCP-Profile verwenden oder benutzerdefinierte Profile konfigurieren. Nachdem Sie ein TCP-

Profil definiert haben, können Sie es an einen einzelnen virtuellen Server oder an mehrere virtuelle Server binden.

Einige der wichtigsten Optimierungsfunktionen, die durch TCP-Profile aktiviert werden können, sind:

- TCP Keep-Alive — Überprüft den Betriebsstatus der Peers in bestimmten Zeitintervallen, um zu verhindern, dass die Verbindung unterbrochen wird.
- Selektive Bestätigung (SACK) — Verbessert die Leistung der Datenübertragung, insbesondere in Long Fat Networks (LFNs).
- TCP-Fensterskalierung — Ermöglicht eine effiziente Übertragung von Daten über lange Fat-Netzwerke (LFNs).

Weitere Informationen zu TCP-Profilen finden Sie unter Konfigurieren von TCP-Profilen.

CloudBridge-Connector

Die NetScaler CloudBridge Connector-Funktion, ein grundlegender Bestandteil des Citrix OpenCloud-Frameworks, ist ein Tool, das zum Aufbau eines Cloud-erweiterten Rechenzentrums verwendet wird. Mit der OpenCloud Bridge können Sie eine oder mehrere NetScaler-Appliances oder virtuelle NetScaler Appliances in der Cloud mit Ihrem Netzwerk verbinden, ohne Ihr Netzwerk neu zu konfigurieren. In der Cloud gehostete Anwendungen sehen aus, als würden sie in einem zusammenhängenden Unternehmensnetzwerk ausgeführt. Der Hauptzweck der OpenCloud Bridge besteht darin, Unternehmen die Möglichkeit zu geben, ihre Anwendungen in die Cloud zu verlagern und gleichzeitig die Kosten und das Risiko eines Anwendungsausfalls zu senken. Darüber hinaus erhöht die OpenCloud Bridge die Netzwerksicherheit in Cloud-Umgebungen. Eine OpenCloud Bridge ist eine Layer-2-Netzwerkbrücke, die eine NetScaler-Appliance oder eine virtuelle NetScaler-Appliance auf einer Cloud-Instanz mit einer NetScaler-Appliance oder einer virtuellen NetScaler-Appliance in Ihrem LAN verbindet. Die Verbindung wird über einen Tunnel hergestellt, der das Generic Routing Encapsulation (GRE) -Protokoll verwendet. Das GRE-Protokoll bietet einen Mechanismus zum Kapseln von Paketen aus einer Vielzahl von Netzwerkprotokollen, die über ein anderes Protokoll weitergeleitet werden sollen. Dann wird IPsec (Internet Protocol Security) Protokollsuite verwendet, um die Kommunikation zwischen den Peers in der OpenCloud Bridge zu sichern.

Weitere Informationen finden Sie unter CloudBridge.

DataStream

Die NetScaler DataStream-Funktion bietet einen intelligenten Mechanismus für den Anforderungswechsel auf Datenbankebene, indem Anfragen auf der Grundlage der gesendeten SQL-Abfrage verteilt werden.

Bei der Bereitstellung vor Datenbankservern sorgt ein NetScaler für eine optimale Verteilung des Datenverkehrs von den Anwendungsservern und Webservern. Administratoren können den

Datenverkehr nach Informationen in der SQL-Abfrage und auf der Grundlage von Datenbanknamen, Benutzernamen, Zeichensätzen und Paketgröße segmentieren.

Sie können den Lastenausgleich so konfigurieren, dass Anforderungen gemäß Lastausgleichsalgorithmen umgestellt werden, oder Sie können die Switching-Kriterien festlegen, indem Sie Content Switching so konfigurieren, dass eine Entscheidung basierend auf SQL-Abfrageparametern wie Benutzernamen, Datenbanknamen und Befehlsparametern getroffen wird. Sie können Monitore weiter konfigurieren, um den Status von Datenbankservern zu verfolgen.

Die erweiterte Richtlinieninfrastruktur auf der NetScaler-Appliance enthält Ausdrücke, mit denen Sie die Anforderungen auswerten und verarbeiten können. Die erweiterten Ausdrücke werten den Verkehr aus, der mit MySQL-Datenbankservern verbunden ist. Sie können anforderungsbasierte Ausdrücke (Ausdrücke, die mit MYSQL.CLIENT und MYSQL.REQ beginnen) in erweiterten Richtlinien verwenden, um Anforderungswechselentscheidungen am Bindepunkt des virtuellen Servers für Content Switching und antwortbasierte Ausdrücke (Ausdrücke, die mit MYSQL.RES beginnen) zu treffen, um Serverantworten auf Benutzer- konfigurierte Gesundheitsmonitore.

> Hinweis: DataStream wird für MySQL L- und MS SQL-Datenbanken unterstützt.

Weitere Informationen finden Sie unter DataStream.

Funktionen zur Anwendungsbeschleunigung

May 11, 2023

- AppCompress

  Verwendet das gzip-Komprimierungsprotokoll, um eine transparente Komprimierung für HTML- und Textdateien bereitzustellen. Das typische Kompressionsverhältnis von 4:1 führt zu einer Reduzierung der Bandbreitenanforderungen des Rechenzentrums um bis zu 50% Dies führt auch zu einer deutlich verbesserten Reaktionszeit des Endbenutzers, da die Datenmenge reduziert wird, die an den Browser des Benutzers übermittelt werden muss.

- Cacheumleitung

  Verwaltet den Datenverkehr zu einer Reverse-Proxy-, Transparent Proxy- oder Forward-Proxy-Cache-Farm. Prüft alle Anfragen und identifiziert Anfragen, die nicht zwischengespeichert werden können, und sendet sie über persistente Verbindungen direkt an die Ursprungsserver. Indem die NetScaler-Appliance nicht zwischenspeicherbare Anforderungen intelligent an die Ursprungs-Webserver umgeleitet wird, gibt die NetScaler Appliance Cache-Ressourcen frei und erhöht die Cache-Trefferraten und reduziert gleichzeitig den gesamten Bandbreitenverbrauch und die Antwortverzögerungen für diese Anforderungen.

  Weitere Informationen finden Sie unter Cache-Umleitung.

- AppCache

  Hilft bei der Optimierung der Bereitstellung von Webinhalten und Anwendungsdaten, indem ein schnelles, HTTP/1.1- und HTTP/1.0-konformes Web-Caching im Arbeitsspeicher sowohl für statische als auch für dynamische Inhalte bereitgestellt wird. Dieser integrierte Cache speichert die Ergebnisse eingehender Anwendungsanforderungen, auch wenn eine eingehende Anfrage gesichert oder die Daten komprimiert sind, und verwendet die Daten dann erneut, um nachfolgende Anfragen für dieselben Informationen zu erfüllen. Durch die direkte Bereitstellung von Daten aus dem integrierten Cache kann die Appliance die Regenerierungszeiten von Seiten reduzieren, da keine statischen und dynamischen Inhaltsanforderungen an den Server übertragen werden müssen.

  Weitere Informationen finden Sie unter Integriertes Caching.

- TCP-Pufferung

  Puffert die Antwort des Servers und liefert sie an den Client mit der Geschwindigkeit des Clients, wodurch der Server schneller entlastet und dadurch die Leistung von Websites verbessert wird.

Anwendungssicherheit und Firewall-Funktionen

May 11, 2023

Nachfolgend sind die Sicherheits- und Firewall-Funktionen aufgeführt.

Denial-of-Service (DoS) -Angriffsabwehr

Erkennt und stoppt böswillige Distributed-Denial-of-Service-Angriffe (DDoS) und andere Arten von böswilligen Angriffen, bevor sie Ihre Server erreichen, und verhindert, dass sie die Netzwerk- und Anwendungsleistung beeinträchtigen. Die NetScaler-Appliance identifiziert legitime Clients und erhöht ihre Priorität, sodass verdächtige Clients keinen unverhältnismäßigen Prozentsatz an Ressourcen verbrauchen und Ihre Site lähmen können. Die Appliance bietet Schutz auf Anwendungsebene vor den folgenden Arten böswilliger Angriffe:

- SYN-Flood-Angriffe
- Pipeline-Angriffe
- Teardrop-Angriffe
- Landangriffe
- Fraggle-Angriffe
- Angriffe auf Zombie-Verbindungen

Die Appliance verteidigt sich aggressiv gegen diese Art von Angriffen, indem sie die Zuweisung von Serverressourcen für diese Verbindungen verhindert. Dies isoliert Server vor der überwältigenden Flut von Paketen, die mit diesen Ereignissen verbunden sind.

Die Appliance schützt außerdem Netzwerkressourcen vor ICMP-basierten Angriffen, indem sie ICMP-Ratenbegrenzung und aggressive ICMP-Paketinspektion verwendet. Es führt eine starke IP-Neuzusammenstellung durch, löscht eine Vielzahl von verdächtigen und fehlerhaften Paketen und wendet Zugriffssteuerungslisten (Access Control Lists, ACLs) auf den Sitedatenverkehr an, um weiteren Schutz zu gewährleisten.

Weitere Informationen finden Sie unter AppQOE.

Inhaltsfilterung

Bietet Schutz vor böswilligen Angriffen für Websites auf Layer 7-Ebene. Die Appliance prüft jede eingehende Anforderung gemäß vom Benutzer konfigurierten Regeln basierend auf HTTP-Headern und führt die vom Benutzer konfigurierte Aktion aus. Zu den Aktionen können das Zurücksetzen der Verbindung, das Ablegen der Anfrage oder das Senden einer Fehlermeldung an den Browser des Benutzers gehören. Auf diese Weise kann die Appliance unerwünschte Anfragen überprüfen und die Gefahr Ihrer Server gegenüber Angriffen verringern.

Diese Funktion kann auch HTTP-GET- und POST-Anfragen analysieren und bekannte fehlerhafte Signaturen herausfiltern, so dass Ihre Server vor HTTP-basierten Angriffen geschützt werden können.

Weitere Informationen finden Sie unter Inhaltsfilterung.

Responder

Funktionen wie ein erweiterter Filter und können verwendet werden, um Antworten von der Appliance an den Client zu generieren. Einige häufige Verwendungszwecke dieser Funktion sind die Generierung von Umleitungsantworten, benutzerdefinierten Antworten und Zurücksetzen.

Weitere Informationen finden Sie unter Responder.

Rewrite

Ändert HTTP-Header und Textkörper. Sie können die Rewrite-Funktion verwenden, um einer HTTP-Anforderung oder -Antwort HTTP-Header hinzuzufügen, Änderungen an einzelnen HTTP-Headern vorzunehmen oder HTTP-Header zu löschen. Sie können damit auch den HTTP-Hauptteil in Anfragen und Antworten ändern.

Wenn die Appliance eine Anforderung empfängt oder eine Antwort sendet, prüft sie auf Rewrite-Regeln. Falls zutreffende Regeln vorhanden sind, wendet sie diese auf die Anforderung oder Antwort an, bevor sie an den Webserver oder den Clientcomputer weitergeleitet wird.

Weitere Informationen finden Sie unter Rewrite.

Überlastungsschutz

Reguliert den Fluss von Benutzeranforderungen an Server und steuert die Anzahl der Benutzer, die gleichzeitig auf die Ressourcen auf den Servern zugreifen können, und stellt alle zusätzlichen Anforderungen in die Warteschlange, sobald Ihre Server ihre Kapazität erreicht haben. Durch die Steuerung der Geschwindigkeit, mit der Verbindungen hergestellt werden können, blockiert die Appliance die Überlastung von Anfragen an Ihre Server und verhindert so eine Überlastung des Standorts.

Weitere Informationen finden Sie unter Überlastungsschutz.

NetScaler Gateway

NetScaler Gateway ist eine sichere Anwendungszugriffslösung, die Administratoren granulare Richtlinien- und Aktionskontrollen auf Anwendungsebene bietet, um den Zugriff auf Anwendungen und Daten zu sichern und Benutzern gleichzeitig die Möglichkeit zu geben, von überall aus zu arbeiten. Es bietet IT-Administratoren einen einzigen Kontrollpunkt und Tools, mit denen die Einhaltung von Vorschriften und ein Höchstmaß an Informationssicherheit innerhalb und außerhalb des Unternehmens gewährleistet werden können. Gleichzeitig ermöglicht es Benutzern einen einzigen Zugriffspunkt — optimiert für Rollen, Geräte und Netzwerke — auf die Unternehmensanwendungen und Daten, die sie benötigen. Diese einzigartige Kombination von Funktionen trägt dazu bei, die Produktivität der mobilen Mitarbeiter von heute zu maximieren.

Weitere Informationen finden Sie unter NetScaler Gateway.

Anwendungs-Firewall

Schützt Anwendungen vor Missbrauch durch Hacker und Malware, wie Cross-Site-Scripting-Angriffe, Pufferüberlauf-Angriffe, SQL-Injection-Angriffe und kraftvolles Surfen, indem der Datenverkehr zwischen jedem geschützten Webserver und Benutzern gefiltert wird, die eine Verbindung zu einer beliebigen Website auf diesem Webserver herstellen. Die Anwendungsfirewall untersucht den gesamten Datenverkehr auf Hinweise auf Angriffe auf Webserversicherheit oder Missbrauch von Webserverressourcen und ergreift geeignete Maßnahmen, um den Erfolg dieser Angriffe zu verhindern.

Weitere Informationen finden Sie unter Anwendungs-Firewall.

Funktion zur Sichtbarkeit von Anwendungen

May 11, 2023

- NetScaler Application Delivery Management

  NetScaler Application Delivery Management (ADM) ist ein leistungsstarker Collector, der einen umfassenden Überblick über die Benutzererfahrung im Web- und HDX- (ICA) -Traffic bietet. Es sammelt HTTP- und ICA-AppFlow-Datensätze, die von NetScaler-Appliances generiert wurden, und füllt Analyseberichte aus, die Statistiken der Ebenen 3 bis 7 abdecken. NetScaler ADM bietet eine eingehende Analyse der Echtzeitdaten der letzten fünf Minuten sowie der historischen Daten, die in den letzten einer Stunde, einem Tag, einer Woche und einem Monat gesammelt wurden.

  Mit dem HDX (ICA) -Analyse-Dashboard können Sie anhand von HDX-Benutzern, -Anwendungen, -Desktops und sogar anhand von Informationen auf Gateway-Ebene detaillierte Analysen durchführen. In ähnlicher Weise bieten HTTP-Analysen eine Vogelperspektive über Webanwendungen, aufgerufene URLs, Client-IP-Adressen und Server-IP-Adressen sowie andere Dashboards. Der Administrator kann in jedem dieser Dashboards die Schwachstellen aufschlüsseln und diese identifizieren, je nachdem, wie es für den Anwendungsfall angemessen ist.

- Verbesserte Anwendungstransparenz mit AppFlow

  Die NetScaler-Appliance ist ein zentraler Steuerungspunkt für den gesamten Anwendungsverkehr im Rechenzentrum. Es sammelt Informationen auf Fluss- und Benutzersitzungsebene, die für die Überwachung der Anwendungsleistung, Analyse und Business Intelligence-Anwendungen wertvoll sind. AppFlow überträgt diese Informationen mithilfe des IPFIX-Formats (Internet Protocol Flow Information eXport), einem offenen Standard der Internet Engineering Task Force (IETF), der in RFC 5101 definiert ist. IPFIX (die standardisierte Version von NetFlow von Cisco) wird häufig zur Überwachung von Netzwerkflussinformationen verwendet. AppFlow definiert neue Informationselemente zur Darstellung von Informationen auf Anwendungsebene.

  Unter Verwendung von UDP als Transportprotokoll überträgt AppFlow die gesammelten Daten, die als *Flow-Datensätze*bezeichnet werden, an einen oder mehrere IPv4-Sammler. Die Kollektoren aggregieren die Flow-Datensätze und generieren Echtzeit- oder historische Berichte.

  AppFlow bietet Transparenz auf Transaktionsebene für HTTP-, SSL-, TCP- und SSL_TCP-Flows. Sie können die Flow-Typen, die Sie überwachen möchten, testen und filtern.

  Um die zu überwachenden Flow-Typen einzuschränken, indem Sie den Anwendungsdatenverkehr abtasten und filtern, können Sie AppFlow für einen virtuellen Server aktivieren. AppFlow kann auch Statistiken für den virtuellen Server bereitstellen.

  Sie können AppFlow auch für einen bestimmten Dienst aktivieren, der einen Anwendungsserver darstellt, und den Datenverkehr zu diesem Anwendungsserver überwachen.

  Weitere Informationen finden Sie unter AppFlow.

- Stream-Analysen

Die Leistung Ihrer Website oder Anwendung hängt davon ab, wie gut Sie die Bereitstellung der am häufigsten angeforderten Inhalte optimieren. Techniken wie Caching und Komprimierung beschleunigen die Bereitstellung von Diensten für Kunden. Sie müssen jedoch in der Lage sein, die am häufigsten angeforderten Ressourcen zu identifizieren und diese Ressourcen dann zwischenzuspeichern oder zu komprimieren. Sie können die am häufigsten verwendeten Ressourcen identifizieren, indem Sie Echtzeitstatistiken über den Website- oder Anwendungsverkehr aggregieren. Mithilfe von Statistiken wie der Häufigkeit, mit der auf eine Ressource im Verhältnis zu anderen Ressourcen zugegriffen wird und wie viel Bandbreite von diesen Ressourcen verbraucht wird, können Sie feststellen, ob diese Ressourcen zwischengespeichert oder komprimiert werden müssen, um die Serverleistung und die Netzwerkauslastung zu verbessern. Statistiken wie Reaktionszeiten und die Anzahl gleichzeitiger Verbindungen zur Anwendung helfen Ihnen festzustellen, ob Sie serverseitige Ressourcen erweitern müssen.

Wenn sich die Website oder Anwendung nicht häufig ändert, können Sie Produkte verwenden, die statistische Daten sammeln, die Statistiken manuell analysieren und die Bereitstellung von Inhalten optimieren. Wenn Sie jedoch keine manuellen Optimierungen vornehmen möchten oder wenn Ihre Website oder Anwendung dynamischer Natur ist, benötigen Sie eine Infrastruktur, die nicht nur statistische Daten sammeln kann, sondern auch die Bereitstellung von Ressourcen auf der Grundlage der Statistiken automatisch optimieren kann. Auf der NetScaler-Appliance wird diese Funktion durch die Stream Analytics-Funktion bereitgestellt. Die Funktion läuft auf einer einzelnen NetScaler-Appliance und erfasst Laufzeitstatistiken auf der Grundlage der von Ihnen definierten Kriterien. Bei Verwendung mit NetScaler Richtlinien bietet das Feature auch die Infrastruktur, die Sie für die automatische Optimierung des Datenverkehrs in Echtzeit benötigen.

Weitere Informationen finden Sie unter Aktionsanalysen.

NetScaler Lösungen

May 11, 2023

NetScaler-Lösungen vereinfachen die Einrichtung häufig bereitgestellter Konfigurationen. Schauen Sie von Zeit zu Zeit in diesem Bereich nach weiteren Lösungen.

Dieser Abschnitt enthält die folgenden Lösungen.

- Einrichten von NetScaler für Citrix Virtual Apps and Desktops
- Voreinstellung für den globalen Serverlastausgleich (GSLB)
- Anycast-Unterstützung in NetScaler
- Bereitstellung einer digitalen Werbeplattform auf AWS mit NetScaler

- Verbesserung der Clickstream-Analyse in AWS mit NetScaler
- NetScaler in einer privaten Cloud - verwaltet von Microsoft Windows Azure Pack und Cisco ACI

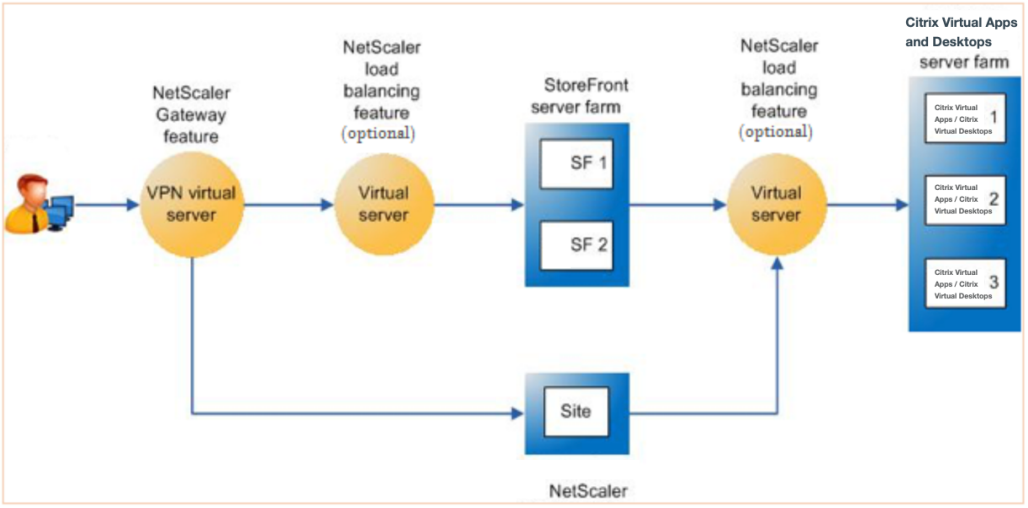
Einrichten von NetScaler für Citrix Virtual Apps and Desktops

May 11, 2023

Eine NetScaler-Appliance kann einen sicheren Remotezugriff auf Ihre Citrix Virtual Apps and Desktops-Anwendungen mit Lastausgleich bieten. Sie können die NetScaler Load Balancing-Funktion verwenden, um den Datenverkehr auf den Citrix Virtual Apps and Desktops-Server zu verteilen. Sie können die NetScaler Gateway-Funktion verwenden, um einen sicheren Remotezugriff auf die Server bereitzustellen.

NetScaler kann auch den Verkehrsfluss beschleunigen und optimieren und bietet Sichtbarkeitsfunktionen, die für Citrix Virtual Apps and Desktopsbereitstellungen nützlich sind.

Abbildung 1. NetScaler-Appliance im Setup von Citrix Virtual Apps and Desktops



Die vorherige Abbildung zeigt die an dieser Bereitstellung beteiligten Komponenten:

- **NetScaler Gateway.** Stellt die URL für den Benutzerzugriff bereit und sorgt für Sicherheit, indem die Benutzer authentifiziert werden.
- **Virtueller NetScaler-Lastausgleichsserver.** Lastausgleich des Datenverkehrs für die StoreFront-Server. Sie können auch einen virtuellen Lastausgleichsserver vor den Citrix Virtual

Apps and Desktop-Servern bereitstellen, um den Lastausgleich für wichtige Komponenten wie den XML-Broker und den Desktop Delivery Controller (DDC) -Server zu gewährleisten.

- **Citrix Virtual Apps and Desktops.** Stellt die Anwendungen bereit, auf die Ihre Benutzer zugreifen möchten.

So richten Sie den NetScaler für Citrix Virtual Apps and Desktops über die NetScaler-GUI ein

Voraussetzungen

- Citrix Virtual Apps und Desktop-Server sind konfiguriert und verfügbar.
- Sie verfügen über praktische Kenntnisse in NetScaler Gateway, NetScaler, Citrix Virtual Apps and Desktops und StoreFront
- Stellen Sie sicher, dass Sie einen virtuellen Server und einen Dienst konfiguriert und den Dienst an den virtuellen Server gebunden haben. Weitere Informationen:
  - Lastausgleich für Citrix Virtual Apps and Desktops
  - Lastausgleich für Citrix Virtual Apps and Desktops

Vorgehensweise:

1. Melden Sie sich bei der NetScaler-Appliance an und klicken Sie auf der Registerkarte **Konfiguration** auf **XenApp und XenDesktop**.
2. Klicken Sie im **Detailbereich** auf **Get Started**. Wenn das Setup auf dem NetScaler vorhanden ist, klicken Sie auf den Link **Bearbeiten**, der jedem Abschnitt entspricht, den Sie ändern möchten.
3. Wählen Sie das Produkt (StoreFront) aus, das in Ihrer Bereitstellung die Schnittstelle für den Zugriff auf die Citrix Virtual Apps and Desktops-Anwendungen bereitstellt.
4. Richten Sie einen sicheren Fernzugriff ein.
   a) Geben Sie im Abschnitt **NetScaler Gateway-Einstellungen** die Details für den virtuellen VPN-Server an und klicken Sie auf **Weiter**.
   b) Wählen Sie im Abschnitt **Serverzertifikat** ein vorhandenes Zertifikat aus oder installieren Sie ein neues Zertifikat und klicken Sie auf **Weiter**.
   c) Konfigurieren Sie im Abschnitt **Authentifizierung** den zu verwendenden primären Authentifizierungsmechanismus und geben Sie die Serverdetails an, oder verwenden Sie einen vorhandenen Server und klicken Sie auf **Weiter**.
   d) Geben Sie im Abschnitt **StoreFront** die Details des Servers an, der die Schnittstelle für den Zugriff auf die Anwendungen bereitstellt, und klicken Sie auf **Weiter**.
   e) Sie können den virtuellen LB-Server, der auf mehrere SF-Server verweist, als Ihren StoreFront-Server verwenden.
5. Klicken Sie auf **Fertig**, um die Konfiguration abzuschließen.

Voreinstellung für den globalen Serverlastausgleich (GSLB)

May 11, 2023

Die GSLB-gestützte Zonenpräferenz ist eine Funktion, die Citrix Virtual Apps and Desktops, StoreFront und NetScaler integriert, um Kunden Zugriff auf das am besten optimierte Rechenzentrum zu bieten, das auf dem Client-Standort basiert.

In einer verteilten Bereitstellung von Citrix Virtual Apps and Desktops wählt StoreFront möglicherweise kein optimales Rechenzentrum aus, wenn mehrere gleichwertige Ressourcen aus mehreren Rechenzentren verfügbar sind. In solchen Fällen wählt StoreFront nach dem Zufallsprinzip ein Rechenzentrum aus. Es kann die Anfrage an jeden Citrix Virtual Apps and Desktops-Server in jedem Rechenzentrum senden, unabhängig von der Nähe zu dem Client, der die Anfrage stellt.

Die Client-IP-Adresse wird überprüft, wenn eine HTTP-Anfrage an der NetScaler Gateway-Appliance eingeht. Die echte Client-IP-Adresse wird verwendet, um die Liste der Rechenzentrumspräferenzen zu erstellen, die an StoreFront weitergeleitet wird. Wenn die NetScaler Appliance so konfiguriert ist, dass sie den Zonenpräferenz-Header einfügt, kann StoreFront 3.5 oder höher die von der Appliance bereitgestellten Informationen verwenden, um die Liste der Delivery Controller neu anzuordnen und eine Verbindung zu einem optimalen Delivery Controller in derselben Zone wie der Client herzustellen. StoreFront wählt den optimalen virtuellen Gateway-VPN-Server für die ausgewählte Rechenzentrumszone aus, fügt diese Informationen der ICA-Datei mit den entsprechenden IP-Adressen hinzu und sendet sie an den Client. StoreFront versucht dann, Anwendungen zu starten, die auf den Delivery Controllern des bevorzugten Rechenzentrums gehostet werden, bevor versucht wird, gleichwertige Controller in anderen Rechenzentren zu kontaktieren.

Weitere Informationen zum Konfigurieren dieser Lösung finden Sie hier.

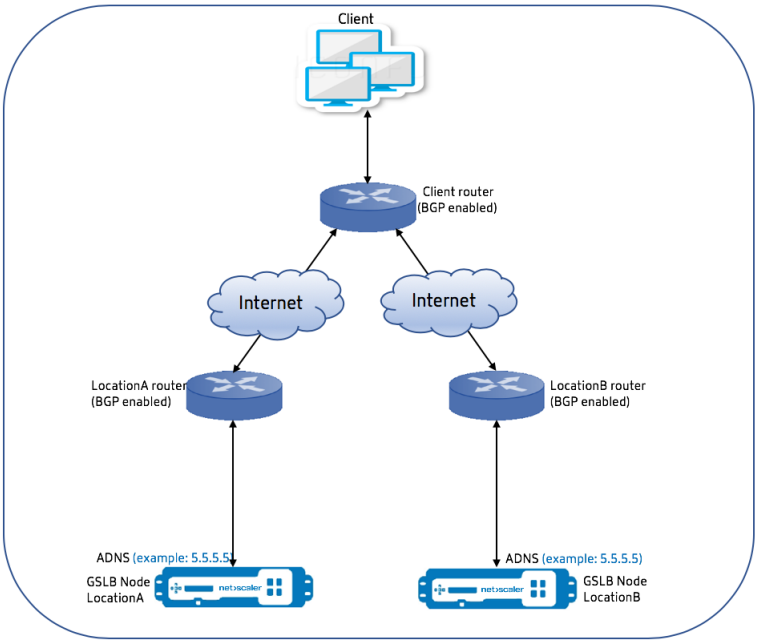
Anycast-Unterstützung in NetScaler

May 11, 2023

Anycast ist ein Netzwerktyp, in dem sich mehrere Server eine IP-Adresse teilen. Die Client-Anfrage wird anhand der Routing-Tabellen an den topografisch nächstgelegenen Server weitergeleitet. Dieses Routing reduziert Latenzprobleme, gewährleistet eine hohe Verfügbarkeit und minimiert Ausfallzeiten.

NetScaler unterstützt Anycast-Netzwerke mit Global Server Load Balancing (GSLB) und DNS-Funktionen.

Das folgende Diagramm zeigt ein Topologiediagramm von Anycast in NetScaler.



Anycast GSLB

Die NetScaler GSLB-Funktion bietet einen Lastenausgleich zwischen global verteilten Standorten sowie eine Notfallwiederherstellung und gewährleistet die kontinuierliche Verfügbarkeit von Anwendungen.

Während eines Ausfalls sorgt GSLB für eine sofortige Notfallwiederherstellung, indem der Datenverkehr an das nächstgelegene oder das leistungsstärkste Rechenzentrum weitergeleitet wird. GSLB kann jedoch Folgendes nicht kontrollieren:

- Wie der DNS-Verkehr an GSLB-Knoten an verschiedenen geografischen Standorten weitergeleitet wird.
- Wie viel Latenz wird hinzugefügt, während DNS-Abfragen an GSLB-Knoten weitergeleitet werden.

In einem typischen GSLB-Setup verfügt jedes Rechenzentrum über einen GSLB-Knoten, der mit dem standortspezifischen Authoritative Domain Name Server (ADNS) für den Empfang von DNS-Abfragen konfiguriert ist. Das ADNS jeder Site ist als Nameserver im DNS-Resolver konfiguriert. Mit zunehmender Anzahl der GSLB-Knoten steigt auch die Anzahl der Nameserver-Einträge. In solchen Fällen muss LDNS bei einem Ausfall eines Rechenzentrums die Lösung mit einem anderen Nameserver erneut versuchen. Dieser Wiederholungsversuch erhöht die Latenz bei der DNS-Auflösung. Außerdem müssen jedes Mal, wenn ein GSLB-Knoten hinzugefügt wird, die Nameserver-Einträge aktualisiert werden.

Um diese Nachteile zu überwinden, können Sie Anycast ADNS verwenden. In Anycast ADNS wird eine

einzige ADNS-IP-Adresse für alle GSLB-Knoten verwendet und der DNS-Verkehr wird mithilfe von dynamischem Routing an GSLB-Knoten weitergeleitet.

Wenn beispielsweise eine GSLB-Site NICHT verfügbar ist, wird die Routingtabelle aktualisiert und die Route zu dieser Site wird entfernt. Daher werden die DNS-Abfragen nicht an die Websites gesendet, die nicht verfügbar sind. Daher gibt es keine Wiederholungsversuche.

Wenn ein neuer GSLB-Knoten hinzugefügt wird, wird dem neuen Knoten dieselbe ADNS-IP-Adresse zugewiesen. Das dynamische Routing aktualisiert die Routing-Tabellen automatisch mit Routen zu neuen Standorten, die auf den Routing-Algorithmen basieren. Daher müssen Sie die DNS-Nameserver-Einträge nicht aktualisieren. Die Einführung neuer GSLB-Sites wird mit Anycast einfacher und schneller gemacht.

So konfigurieren Sie eine ADNS-IP-Adresse in einem Anycast-Modus

Aktivieren Sie das Host-Routing auf der ADNS-IP in einer NetScaler-Appliance und stellen Sie die entsprechende Route Health Injection (RHI) -Stufe ein. In den meisten Fällen gäbe es keine virtuellen Server auf der ADNS-IP und daher muss die RHI-Ebene als NONE ausgewählt werden. Die Aktivierung der Host-Route auf der ADNS-IP macht sie zu einer Kernel-Route. Sie können dann das dynamische Routing Ihrer Wahl aktivieren und das Routing-Protokoll so konfigurieren, dass die Kernel-Routen neu verteilt werden.

ADNS-IP-Konfiguration — Beispiel

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service adns_public 5.5.5.5 ADNS 53

set ip 5.5.5.5 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

BGP-Konfiguration auf der GSLB-Site — Beispiel

```
Site1#sh run
!
hostname Site1
!
log syslog
log record-priority
!
ns route-install bgp
!
```



```
interface lo0
 ip address 127.0.0.1/8
 ipv6 address fe80::1/64
 ipv6 address ::1/128
!
interface vlan0
 ip address 10.102.148.94/25
 ipv6 address fe80::e84c:f4ff:fe74:4588/64
!
interface vlan2
 ip address 172.18.30.15/24
!
router bgp 5
 redistribute kernel -----> redistributing the kernel routes
 neighbor 172.18.30.30 remote-as 4
 neighbor 172.18.30.30 advertisement-interval 1
 neighbor 172.18.30.30 timers 4 16
!
End

Site1#
<!--NeedCopy-->
```

GSLB-Site-Routing-Tabelle — Beispiel

```
Site1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, I - Intranet
       * - candidate default

K       5.5.5.5/32 via 0.0.0.0 ---------------------------------------->
    Kernel Route for ADNS
C       10.102.148.0/25 is directly connected, vlan0
C       127.0.0.0/8 is directly connected, lo0
B       172.18.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       172.18.20.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
C       172.18.30.0/24 is directly connected, vlan2
B       192.168.3.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.5.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
```



```
19
20 Gateway of last resort is not set
21 Site1#
22 <!--NeedCopy-->
```

Anycast-DNS

Sie können Anycast DNS für virtuelle DNS-Proxyserver auf NetScaler verwenden. Wenn mehrere DNS-Nameserver konfiguriert sind, reagiert der DNS-Resolver auf der Grundlage der Round-Robin-Methode. Wenn der Resolver beispielsweise keine Antwort vom ersten Server erhält, wechselt er nach Ablauf des konfigurierten Timeout-Werts zum zweiten Server. Der Wechsel vom ersten Server zum zweiten Server erhöht die Latenz bei der DNS-Auflösung. Wenn die DNS-Resolver mit Anycast konfiguriert sind, kann diese Latenz beseitigt werden.

DNS-Konfiguration — Beispiel

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver dns DNS 5.5.5.50 53
2
3 set ip 5.5.5.50 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
4 <!--NeedCopy-->
```

Bereitstellung einer digitalen Werbeplattform auf AWS mit NetScaler

May 11, 2023

Angesichts der sich weiterentwickelnden Natur digitaler Plattformen steht eine Vielzahl von Werbeanwendungen zur Verfügung. Zum Beispiel soziale Medien, Direktwerbung, Videos, Banner, Pops, Interstitials, Rich Media und so weiter. Werbetreibende nutzen Videowerbenetzwerke in rasantem Tempo, auf die fast 40% des Werbeverkehrs entfallen. Angesichts der zunehmenden Nutzung von Mobiltelefonen durch moderne Nutzer hat die Schaltung von Videoanzeigen auf der mobilen Plattform jedoch erheblich zugenommen.

Die digitalen Werbeplattformen stehen vor mehreren Herausforderungen. Einige der Herausforderungen sind:

- Sicherheitsbedrohungen
- Hohe Betriebskosten

- Es steht eine Vielzahl von Geräten zur Verfügung, um Datenverkehr über das Internet zu senden. Die verschiedenen Protokolle für die Echtzeitkommunikation stellen folgende Herausforderungen dar:
  - WebRTC
  - Adaptives Streaming
  - UDP für Video, wobei WebRTC UDP über HTTP verwendet

Um dem komplexen Verhalten von Werbeplattformen gerecht zu werden, bietet die NetScaler-Lösung mit ihrer gesamten Palette von Funktionen und Funktionen, die gut in AWS integriert sind, überall und jederzeit einen sofortigen, sicheren und zuverlässigen Zugriff auf digitales Werbeinventar. NetScaler spielt eine entscheidende Rolle bei der Bereitstellung von SaaS- und Web-Apps für digitale Plattformen.

Integration digitaler Werbeplattformen mit NetScaler

Überblick über die digitale Werbeplattform

Die digitale Werbeplattform besteht aus den folgenden Schlüsselkomponenten:

- Austausch von Anzeigen
- Werbenetzwerk
- Demand-Side-Plattform (DSP)
- Plattform auf der Angebotsseite (SSP)
- Systeme für Echtzeit-Bidding (RTB)

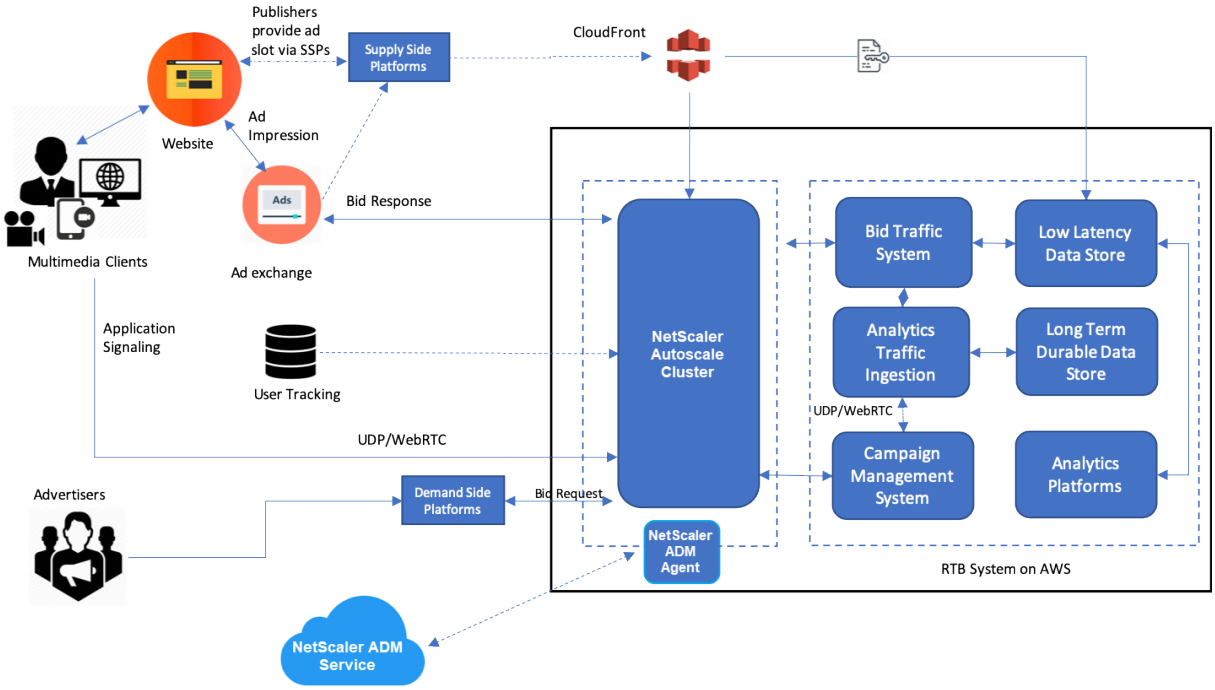
Ein Überblick über den Prozess, der in einem Werbesystem angewendet wird, lautet wie folgt.

- Die erste Transaktion findet statt, wenn der Benutzer die Website besucht.
- Dadurch wird eine Gebots-/Werbeanfrage (einschließlich der demografischen Informationen des Nutzers) ausgelöst, die an den Anzeigenserver oder an den Publisher gesendet wird, der eine Anzeigenbörse kontaktiert.
- Die Anzeigen-Publisher senden die Werbeanfrage über SSPs an einen Ad Exchange.
- Die Ad Exchange übermittelt diese Anfrage und die zugehörigen Daten an DSP und teilt ihnen mit, dass eine Impression oder Werbeanfrage verfügbar ist. Daher können mehrere Werbetreibende automatisch in Echtzeit Gebote abgeben, um ihre Anzeigen zu platzieren.
- In der Zwischenzeit müssen die Werbetreibenden ihre Kampagnen in DSP einrichten. Verwenden Sie die Informationen über den Benutzer aus der Data Management Platform (DMP), um zu ermitteln, welchen Betrag er bereit ist, für die Bereitstellung einer Werbung an den Nutzer zu zahlen.
- DSPs geben diese Angebote in Echtzeit für jede Werbeimpression ab, da sie der Anzeigenbörse zugestellt werden.
- Der Bieter, der innerhalb eines von der Ad Exchange oder den SSP festgelegten Zeitraums am meisten bietet, erhält von den Publishern einen Anzeigenplatz für die Schaltung seiner

Anzeigen. Andernfalls verlieren sie die Gelegenheit, die richtige Werbung für ihre wichtigste Zielgruppe zu erhalten.

Wie die digitale Werbeplattform in NetScaler integriert ist

Das folgende Diagramm zeigt, wie die verschiedenen Komponenten der Werbeplattform mit NetScaler und NetScaler Application Delivery Management (ADM) kommunizieren, um Online-Werbung zu schalten.



Wie NetScaler dazu beiträgt

Bei der Veröffentlichung von Werbung hilft die NetScaler-Lösung dabei, den inkonsistenten Zustrom von Gebotszugriffen zu bewältigen und zu verarbeiten. Es dient als Einstiegspunkt für den gesamten Datenverkehr, um Skalierbarkeit und Verfügbarkeit in den Availability Zones sicherzustellen. Um dem elastischen Charakter des Werbe-Traffics Rechnung zu tragen, wird dieser in einer Autoscaling-Gruppe vor Webanwendungen und Datenbankservern eingesetzt.

Die Werbeplattform auf AWS mit der NetScaler-Lösung bietet Ihnen Echtzeitleistung, hohe Skalierbarkeit und hohe Verfügbarkeit auf der ganzen Welt. Sie können Rich Media-, Video-, Mobile- und native Werbung in Echtzeit kaufen und verkaufen. Es reduziert die Gesamtbetriebskosten und die Latenz, die mit dem Betrieb einer Werbeplattform verbunden sind. Es ist der leistungsstärkste Proxy mit den umfassenden Funktionen, die Backend-Server bei Autoscale problemlos zu entfernen, Verbindungsmultiplexing durchzuführen und sicherzustellen, dass der Endbenutzer-Traffic nicht

beeinträchtigt wird. NetScaler unterstützt den Lastenausgleich der HTTP-, UDP-, WebRTC- und RTSP-Protokolle, die in den Werbeplattformen verwendet werden.

NetScaler fügt sich mit den folgenden Hauptmerkmalen kohärent in die AWS-Umgebung ein:

- Inhaltswechsel — Wechseln Sie anhand des Hostnamens zur richtigen Plattform.
- Sicherheitsschutz — Nutzen Sie WAF-Funktionen (Web Application Firewall), Ratenbegrenzung (über Client-IP) und Schutz vor DDoS-Angriffen.
- Automatische Skalierung von Front-End- und Back-End-Verkehr.
- Durchgängige Transparenz und Erkennung von Anomalien auf allen ADC-Appliances mithilfe von ADM.
- Niedrige Latenz.

Wie NetScaler ADM dazu beiträgt

NetScaler verwendet NetScaler ADM, um die folgenden Herausforderungen zu bewältigen, mit denen digitale Werbeplattformen konfrontiert sind:

- Identifizieren Sie die Trendabweichungen von der erwarteten Leistung
- Analyse der Anwendungsleistung in Echtzeit
- Kapazitätsüberwachung

Vorteile der Integration von Werbeplattformen mit NetScaler und ADM

Die NetScaler-Lösung bietet einem Anbieter digitaler Werbeplattformen die folgenden Funktionen und Vorteile.

Niedrige Kosten

- Die NetScaler VPX-Instance ist in den AWS Autoscaling-Service integriert und kann Ihre Front-End- und Back-End-Ressourcen automatisch nach oben oder unten skalieren. Dies bietet eine Zero-Touch-Konfiguration, die der Elastizität von Werbeplattformen Rechnung trägt.
- Konsolidierung der Bereitstellung aller Arten von Verkehr von einem einzigen Punkt aus.

Weitere Informationen zur Autoscaling von AWS finden Sie unter Hinzufügen von Back-End-AWS Autoscaling-Service.

Hohe Verfügbarkeit

- Wenn eine Availability Zone nicht mehr verfügbar ist, wendet NetScaler seine Fehlertoleranzfähigkeit an, um die Server in einer anderen Availability Zone automatisch zu erkennen, ohne dass der Datenverkehr unterbrochen wird.

- Außerdem werden Server ordnungsgemäß beendet, wodurch der Verlust von Clientverbindungen vermieden wird.

Weitere Informationen finden Sie unter Funktionsweise von Hochverfügbarkeit in AWS.

Analyse der Anwendungsleistung

Die intelligenten Analysen und Analysen der Anwendungsleistung von NetScaler ADM stellen Folgendes sicher:

- Verschaffen Sie sich einen Überblick über die Probleme (Anomalien bei der Serverreaktion, 5XX-Fehler usw.), die das Endbenutzererlebnis beeinträchtigen.
- Informieren Sie den Administrator, sofort Korrekturmaßnahmen zu ergreifen.

Weitere Informationen finden Sie unter Leistungsindikatoren für Anwendungsanalysen.

Reichhaltige Firewall-Sicherheit

Die häufigsten Sicherheitslücken treten in Webanwendungen und nicht in Netzwerken auf. Es ist wichtig, Ihre Webanwendungen vor unbefugtem Zugriff wie Bots, Datendiebstahl und Angriffen auf Andwendungslayer zu schützen.

NetScaler bietet umfassende und integrierte Layer-4- bis Layer-7-Sicherheit, die Folgendes beinhaltet:

- Web App Firewall (WAF) zum Schutz Ihrer Webanwendungen, zur Identifizierung und Abwehr bösartiger Bots mit regelmäßig aktualisierten Bot-Signaturen und verhaltensbasierter Erkennung.
- Ratenbegrenzung, um zu verhindern, dass eine Werbeplattform überfordert wird.

Weitere Informationen finden Sie unter NetScaler Web App Firewall.

Wählen Sie den richtigen AWS-Instanztyp für die Werbeplattform

Wählen Sie den richtigen AWS-Instance-Typ für ADC, abhängig von den folgenden zwei Faktoren:

- Anzahl der Benutzer, die gleichzeitig auf die Werbeplattform zugreifen.
- Durchschnittliche Anzahl der Benutzer auf der Plattform.

Der NetScaler kann in verschiedenen EC2-Instances eingesetzt werden, zu denen c5, c5n, m5 usw. gehören. Verwenden Sie für Werbeplattformen die folgenden AWS-Instance-Typen:

- c5 oder c5n eignen sich für den Umgang mit hohem SSL-Verkehr.
- c5.large kann bis zu 1000 SSL TPS verarbeiten.

Weitere Informationen finden Sie unter VPX-AWS-Unterstützungsmatrix.

Verbesserung der Clickstream-Analyse in AWS mit NetScaler

May 11, 2023

Kunden greifen zunehmend über verschiedene Anwendungen wie mobile Apps, SaaS-Apps usw. auf die Unternehmensprodukte zu. Daher können Anwendungen zu einer Landmine von Kundenerlebnisdaten werden. Um das Kundenverhalten online zu verfolgen, bilden kundenorientierte Unternehmen datengesteuerte Profile für jeden ihrer Kunden, die diese Kundenverhaltensdaten verwenden.

Ein Clickstream ist eine Sequenz oder ein Stream von Ereignissen, die Benutzeraktionen (Klicks) auf einer Website oder einer mobilen Anwendung darstellen. Der Umfang von Clickstream reicht jedoch über Klicks hinaus. Es umfasst Produktsuchen, Impressionen, Käufe und solche Ereignisse, die für das Unternehmen von Relevanz sein könnten. Das bloße Sammeln und Speichern der Kundenerlebnisdaten ist nicht von großem Wert. Es ist notwendig, die hochkomplexen Daten zur richtigen Zeit nahtlos an die richtigen Anbieter zu verteilen. Unternehmen können Wert aus den Daten ableiten und schnell bewusste Entscheidungen treffen, um ihre Strategien zu verbessern. Daher nutzen Unternehmen zunehmend Clickstream Analytics, um Einblicke in die Customer Experience Journey der Apps zu erhalten.

Dieses Dokument vermittelt Ihnen ein gutes Verständnis darüber, warum Clickstream-Daten von größter Bedeutung sind, wie sie gesammelt, gespeichert, verteilt und in aussagekräftige und umsetzbare Analysen umgewandelt werden.

NetScaler lässt sich in NetScaler ADM integrieren und bietet AWS-Services wie Amazon Kinesis Data Firehose einen Mehrwert, um Unternehmen mit der erstklassigen Analyselösung auszustatten, die sich auf die Clickstreams der Benutzer konzentriert.

Diese NetScaler-Lösung hilft Ihnen, komplexe Geschäftsprobleme effizient und extrem einfach zu lösen. NetScaler und AWS Kinesis helfen dabei, die Probleme mit dem schlecht konzipierten Workflow zu erfassen. NetScaler ADM hilft dabei, Probleme im Zusammenhang mit der Webanwendung und der Netzwerkleistung zu erfassen, indem entsprechende Filter angewendet werden. Die Kombination von NetScaler mit NetScaler ADM und AWS Kinesis hilft Ihnen, den riesigen Zustrom von Clickstream-Daten in jeder Phase zu verwalten und zu analysieren. Diese Lösung ist hochverfügbar, skalierbar, robust und stellt sicher, dass die Lieferung kontinuierlich und sicher ist. So können Sie umsetzbare Erkenntnisse ableiten.

Warum entscheiden sich Unternehmen für Clickstream-Analytics?

Unternehmen entscheiden sich für Clickstream in erster Linie, um zu verstehen, wie Benutzer mit der Anwendung interagieren, und um Einblicke in die Verbesserung der Ziele der Anwendung zu erhalten. Clickstream Analytics ist ein Anwendungsfall zum Abrufen von Informationen, der das Verhalten, die

Navigationsgewohnheiten Ihres Benutzers usw. verfolgt. Clickstream-Analytics gibt Ihnen Informationen zu:

- Auf welchen Link klicken Ihre Kunden öfter und zu welchem Zeitpunkt.
- Wo war der Besucher, bevor er meine Website erreichte?
- Wie viel Zeit hat der Besucher auf jeder Seite verbracht?
- Wann und wo hat der Besucher im Webbrowser auf die Schaltfläche “Zurück” geklickt?
- Welche Artikel hat der Besucher zu seinem Warenkorb hinzugefügt (oder daraus entfernt)?
- Von welcher Seite hat der Besucher meine Website verlassen?

Analysedienst zur Verwaltung von Clickstream-Daten mit Amazon Kinesis

Sie können Amazon Kinesis verwenden, um Clickstream Analytics durchzuführen. Amazon Kinesis ermöglicht Clickstream-Analysen mit den folgenden Services:

- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Analytics
- Amazon Kinesis-Datenströme

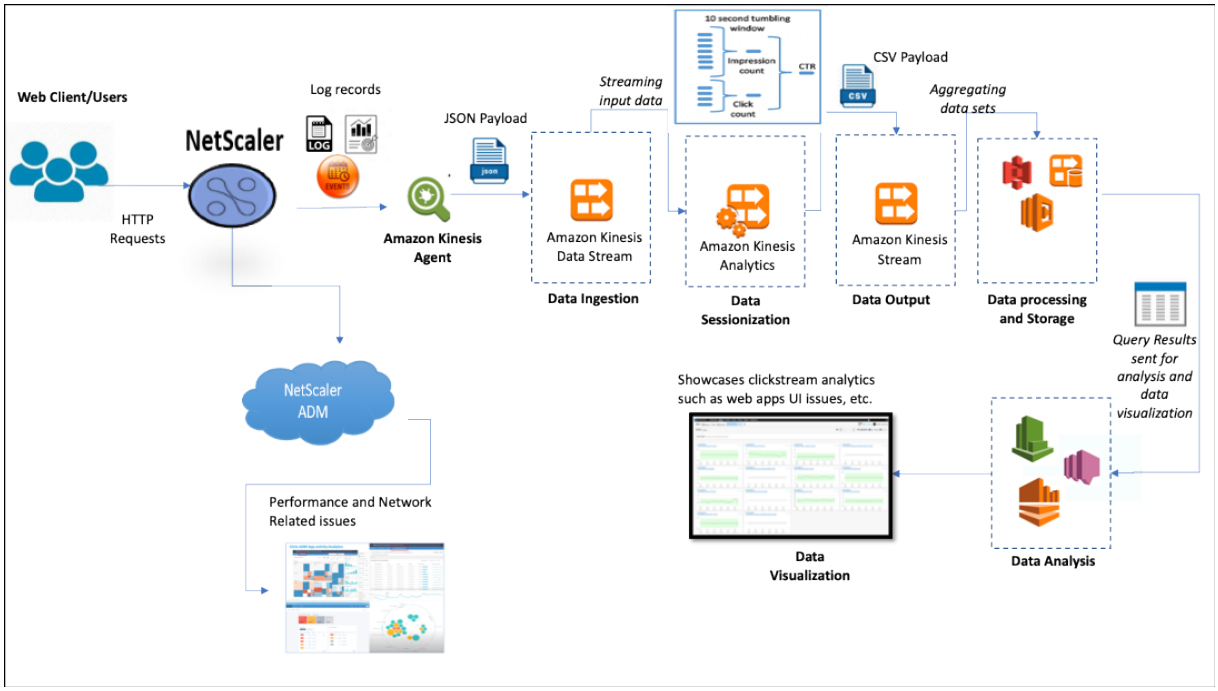
Mit Amazon Kinesis können Sie Ihre riesigen Datensätze in jedem Maßstab sammeln und analysieren. AWS Kinesis kann Daten aus verschiedenen Quellen verarbeiten, wie zum Beispiel:

- Mobile und Webanwendungen (z. B. Gaming, E-Commerce)
- IoT-Geräte
- Anwendungen für soziale Netzwerke
- Dienstleistungen des Finanzhandels
- Geospatiale Dienste

Wie NetScaler Clickstream-Analysen ermöglicht

Die NetScaler-Lösung sammelt und liefert Informationen über die Aktivitäten der Benutzer, wie z. B. besuchte Websites, verbrauchte Bandbreite und Navigationsfluss, auf sichere Weise. Unternehmen analysieren diesen hohen Durchsatz und die kontinuierlichen Clickstream-Daten, um die Wirksamkeit der folgenden Punkte zu bestätigen:

- Site-Layout
- Marketingkampagnen
- Neue Anwendungsfunktionen



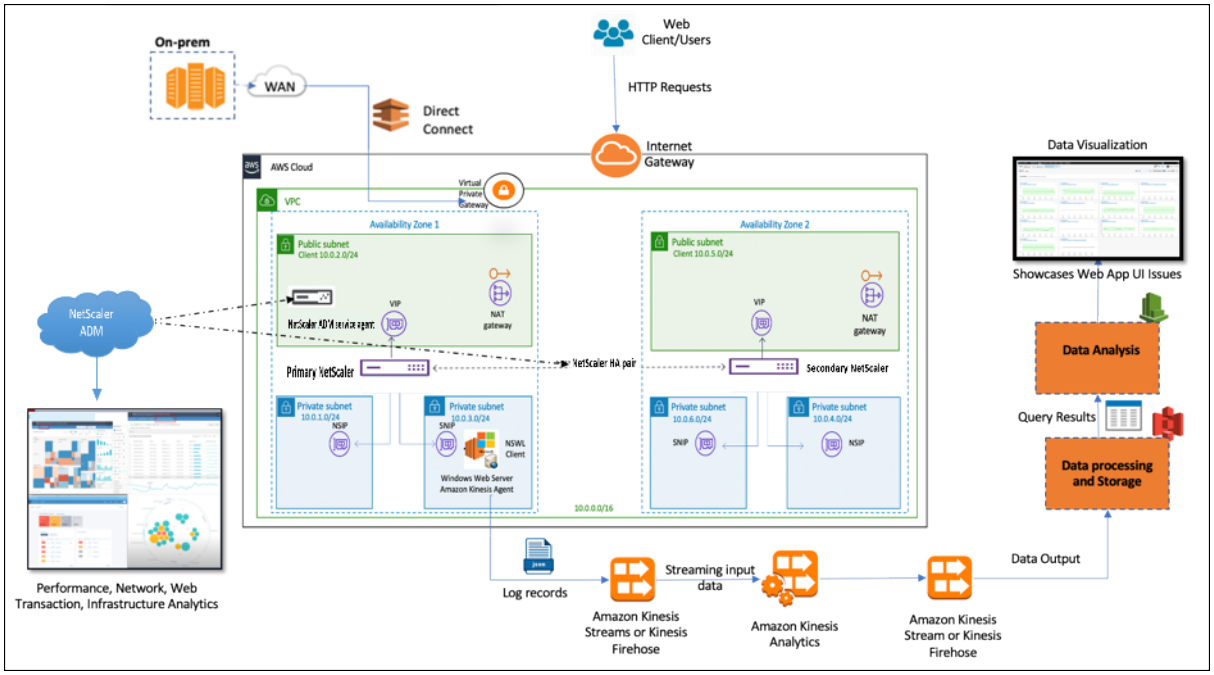
Da NetScaler in der Lage ist, einen robusten Netzwerkschutz für Unternehmensumgebungen bereitzustellen, werden die Serverkosten um ein Vielfaches reduziert, indem rechenintensive Aufgaben ausgelagert und Sitzungen mit diesen Daten ausgeführt werden. Dadurch können Unternehmen Ereignisse in Echtzeit mit hoher Verfügbarkeit, Sicherheit und geringer Latenz immer identifizieren.

Informationen zur Konfiguration finden Sie unter Konfigurieren der NetScaler-Lösung für Clickstream Analytics.

Wie NetScaler und NetScaler ADM die AWS-Umgebung ergänzen

Das folgende Diagramm veranschaulicht den End-to-End-Benutzerworkflow zur Durchführung von Clickstream-Analysen in der AWS-Infrastruktur. Dieses Diagramm hilft Ihnen, die folgenden Prozesse zu verstehen:

- Wie der Benutzer mit NetScaler interagiert
- Wie NetScaler Benutzeraktionen erfasst und Clickstream-Daten generiert
- Wie die Clickstream-Daten an AWS-Services geliefert werden (Amazon Kinesis)
- Wie Amazon Kinesis die Datenprotokolle verarbeitet und speichert, um aussagekräftige Clickstream Analytics zu erstellen



Der NetScaler lässt sich nahtlos in die AWS-Umgebung und NetScaler ADM integrieren, sodass Unternehmen mit variablem Volumen und unterschiedlicher Natur der Clickstream-Daten kompatibel sind. Es bietet Dienste zum einfachen Laden und Analysieren von Streaming-Wissen. Sie können auch benutzerdefinierte Streaming-Wissensanwendungen für spezielle Wünsche erstellen.

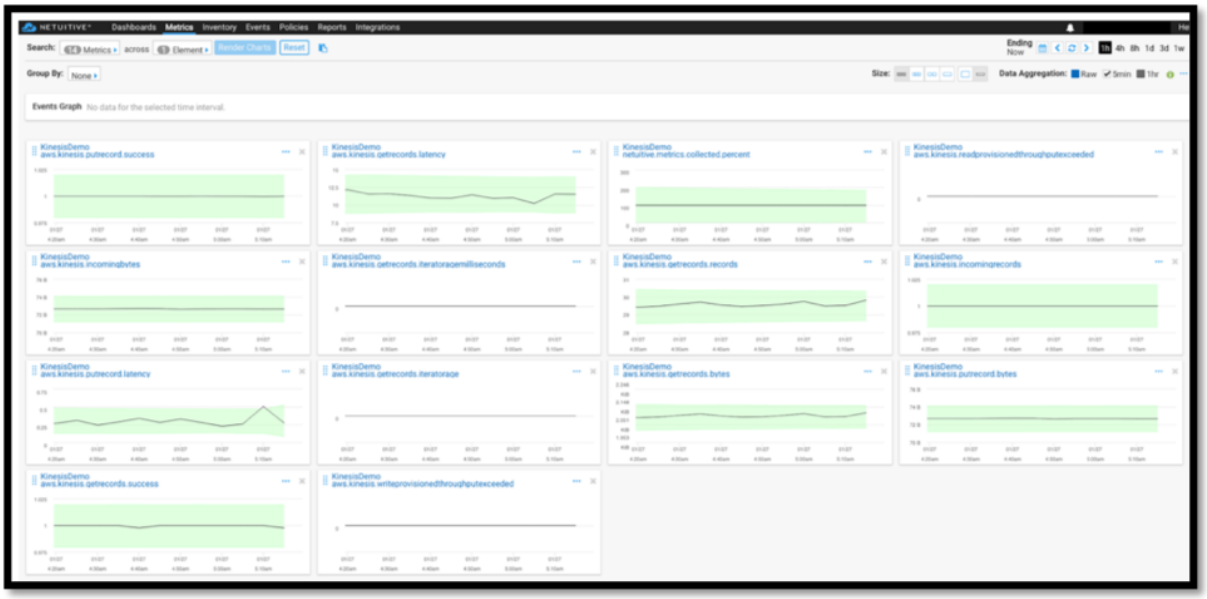
Amazon Kinesis

Die AWS-Umgebung verfügt über verschiedene Services, die Analysen der von NetScaler erfassten Benutzerereignisse, Protokolle und Metriken durchführen. Die Daten können Website-Clickstreams, Finanztransaktionen, Social-Media-Feeds, IT-Protokolle und Ereignisse zur Standortverfolgung sein.

- Amazon Kinesis Data Streams führen Analysen in Szenarien durch, die skalierbares und dauerhaftes Echtzeit-Datenstreaming beinhalten, das kontinuierlich GB an Daten pro Sekunde aus mehreren Quellen erfassen kann.
- Amazon Kinesis Data Analytics kann für Szenarien mit geringerer Latenz zwischen der Sitzungsgenerierung verwendet werden, da das Aggregieren verschiedener Datensätze weniger Zeit benötigt.
- Amazon Kinesis Agent für Microsoft Windows sammelt, analysiert, filtert und streamt Eingabedaten in Kinesis-Datenströme.
- Sobald die Daten in der Cloud verfügbar sind, können Sie die genaue Datenpipeline implementieren, um die gewünschten Ergebnisse zu erhalten. Sie können diese Informationen beispielsweise in Amazon Quick Sight verwenden, einem Visualisierungstool, das zum Erstellen von Dashboards verwendet wird.

Das AWS Kinesis-Dashboard bietet folgende Angebote:

- Zeigt Probleme mit der Benutzeroberfläche von Web-Apps
- Visualisierungen von Metriken zur Webnutzung, wie Ereignisse pro Stunde, Besucherzahl und Referenzen in nahezu Echtzeit.
- Sitzungsweise Analyse



NetScaler ADM-Analytik

Durch die Verwendung von NetScaler ADM mit NetScaler erhalten Sie eine zentrale Ansicht aller Geschäftsumgebungen. Die von NetScaler erfassten Protokolle werden in NetScaler ADM eingespeist, das Ihre einzelnen Anwendungen als eine Einheit behandelt. Sie können wertvolle Erkenntnisse gewinnen und Probleme mit den folgenden ADM-Funktionen effektiv beheben:

- Intelligente Analytik
- Web-Transaktionsanalyse
- Erkennung von Anomalien
- Leistungs- und Netzwerkprobleme

Das folgende ADM-Service-Dashboard hilft Ihnen dabei, wertvolle Erkenntnisse zu gewinnen, um die Probleme effektiv zu beheben.

Wie NetScaler ADM mit Clickstream-Analysen korreliert

Clickstream-Analysedaten können mit ADM-Analysen korreliert werden, um die Anwendungsleistung zu beschreiben, vorherzusagen und zu verbessern.

Weitere Informationen zu NetScaler ADM finden Sie unter NetScaler ADM%20is%20A%20Centralised%20Managem &text=you%20CAN%20USE%20Adm%20TO, von%20A%20Single%2C%20Unified%20Console.)

Zum Beispiel bemerkt eine Organisation, die ihre Protokolle analysiert, dass die meisten Benutzer ihre Websites verlassen. Um jedoch die Ursache für dieses Benutzerverhalten zu finden, müssen sie herausfinden, welcher Teil ihrer Anwendung schlecht funktioniert. Mit Clickstream-Analysedaten und ADM-Analysen können Sie die folgenden Erkenntnisse ableiten, um den Grund für das Verlassen einer Website durch Benutzer zu analysieren:

- Wird der Benutzer aufgrund von Latenzzeiten, 5xx-Fehlern abgebrochen?
- Gibt es SSL-Handshake-Fehler?
- Gibt es einen Teil der Anwendung, der Leistungs- oder Netzwerkprobleme aufweist?
- Gibt es einen 404-Fehler oder die Ladezeit der Seite dauert ewig, um zu antworten, und so weiter.
- Stehen Kunden vor Anomalien der Serverantwort?

Der NetScaler ADM Service bietet Web Insights, mit denen IT-Administratoren Probleme mithilfe der folgenden Funktionen schneller lösen können:

- Bietet eine integrierte Überwachung aller Webanwendungen in Echtzeit, die vom NetScaler bereitgestellt werden.
- Verschaffen Sie sich einen ganzheitlichen Überblick über die Anwendungsleistung zu Zeit, Latenz und das Verhalten des üblichen Benutzers durch Observability-Tools (z. B. globales Service-Graph).
- Führen Sie intelligente Analysen durch, um Anomalien der Serverantwort zu verstehen.
- SSL-Erkenntnisse tragen zur Behebung von 5xx- und 4xx-Fehlern bei.
- So führen Sie Aufzeichnungen aller Websitzungen, die Folgendes beinhalten:
  - Detaillierte Protokolle jeder Web-Transaktion
  - Suchfunktion, um relevante Logs zu finden
  - Möglichkeit, einen ADC-zu-Endbenutzer im Vergleich zu isolieren ADC-zu-Server-Problem

Arten von Daten, die von ADC für Clickstream-Analytics exportiert werden

NetScaler erfasst die verschiedenen Quellen, aus denen verschiedene Datenformen generiert werden. Diese lauten wie folgt:

- Webserver-Protokolle

  Die Webserver-Protokollierungsfunktion sendet Protokolle von HTTP- und HTTPS-Anfragen zum Speichern und Abrufen an ein Clientsystem. Diese Protokolle enthalten eine große Menge an Daten, die schwer zu verstehen und daraus sinnvoll sind. Analytische Tools helfen dabei, sie zu verstehen und daraus einen Mehrwert zu schaffen. Weitere Informationen zur Konfiguration finden Sie im **Abschnitt Konfiguration der Webprotokollierung** in diesem Dokument.

- Syslogs

  Die primäre Verwendung von Syslogs ist für das Systemmanagement. Die proaktive Syslog-Überwachung zahlt sich aus, da die Ausfallzeiten von Servern und anderen Geräten in Ihrer Infrastruktur erheblich reduziert werden. Syslog identifiziert kritische Netzwerkprobleme und meldet sie proaktiv.

- Zugriff auf Protokolle

  Die Zugriffsprotokolle speichern Informationen über Ereignisse, die auf Ihrem Webserver aufgetreten sind. Wenn beispielsweise jemand Ihre Website besucht, wird ein Protokoll aufgezeichnet und gespeichert, um dem Webserver-Administrator Informationen wie die IP-Adresse des Besuchers, welche Seiten er angeschaut hat, Statuscodes und verwendeten Browser zur Verfügung zu stellen. Der Zugriff auf Protokolle kann überwältigend sein, wenn es an angemessenen Kenntnissen mangelt, um sie zu verstehen.
  Sie können Ihr System so programmieren, dass es integriert ist mit:

  - NetScaler für eine nahtlose Bereitstellung
  - Kinesis für umsetzbare Erkenntnisse, die für Unternehmen nützlich sind

- Auditprotokolle

  Mit der Audit-Logging-Funktion können Sie die NetScaler-Status und Statusinformationen protokollieren, die von verschiedenen Modulen im Kernel und in den Daemons auf Benutzerebene gesammelt wurden.

- Fehler-Logs

  Die Fehlerprotokolldatei ist eine Hilfe für Administratoren, um weitere Informationen zu einem bestimmten Fehler bereitzustellen, der auf dem Webserver aufgetreten ist.

Konfigurieren Sie die NetScaler-Lösung für Clickstream Analytics

Die Webserver-Protokollierungsfunktion ermöglicht es Ihnen, Protokolle von HTTP- und HTTPS-Anfragen zur Speicherung und Abruf an ein Clientsystem zu senden.

Um den NetScaler für die Webserver-Protokollierung zu konfigurieren, müssen Sie:

- Web-Logging-Funktion aktivieren
- Konfigurieren Sie die Größe des Puffers, um die Protokolleinträge vorübergehend zu speichern, da der Web-Log-Server auf dem NetScaler läuft.

So konfigurieren Sie die Webserver-Protokollierung mit der CLI:

1. Aktivieren Sie die Webserver-Protokollierungsfunktion.

```
enable ns feature WL
<!--NeedCopy-->
```

2. [Optional] Ändern/konfigurieren Sie die Puffergröße zum Speichern der protokollierten Informationen.

```
set ns weblogparam -bufferSizeMB 60
<!--NeedCopy-->
```

3. Installieren Sie den NetScaler Web Logging (NSWL) Client. Weitere Informationen finden Sie unter Installieren des NetScaler Web Logging (NSWL) -Clients

4. Installieren Sie den NSWL-Client unter Windows, indem Sie die folgenden Vorgänge auf dem System ausführen, auf das Sie das Paket heruntergeladen haben.

   a) Extrahieren und kopieren Sie die< release number > Datei nswl_win–.zip< build number > aus dem Paket auf ein Windows-System, auf dem Sie den NSWL-Client installieren möchten.

b) Entpacken Sie die Datei auf dem Windows-System in einem Verzeichnis (genannt < NSWL-HOME>). Bin, Samples und andere Verzeichnisse werden extrahiert.

c) Führen Sie an der Eingabeaufforderung den folgenden Befehl aus dem < NSWL-HOME > Verzeichnis\ bin aus:

```
nswl -install -f < path of the log.conf file >\log.conf
<!--NeedCopy-->
```

> **Hinweis:**
>
> Um den NSWL-Client zu deinstallieren, führen Sie an der Eingabeaufforderung den folgenden Befehl aus dem < NSWL-HOME > Verzeichnis\ bin aus:

```
nswl -remove
<!--NeedCopy-->
```

5. Konfigurieren Sie nach der Installation des NSWL-Clients den NSWL-Client mit der ausführbaren NSWL-Datei. Diese Konfigurationen werden in der NSWL-Client-Konfigurationsdatei (log.conf) gespeichert.

   Führen Sie die folgenden Befehle aus dem Verzeichnis aus, in dem sich die ausführbare NSWL-Datei befindet:

```
\ns\bin
<!--NeedCopy-->
```

6. Fügen Sie in der NSWL-Client-Konfigurationsdatei (log.conf) die NetScaler-IP-Adresse (NSIP) hinzu, von der der NSWL-Client Protokolle sammelt, indem Sie in der Befehlszeile des Clientsystems Folgendes ausführen:

```
nswl -addns -f < Path to the configuration(log.conf) file >\log.
   conf
<!--NeedCopy-->
```

7. Geben Sie den NSIP (IP-Adresse), den Benutzernamen als `nsroot` und das Kennwort der NetScaler-Appliance als “Instanz-ID/Ihr eingestelltes Kennwort” ein, damit:

   - NSWL-Client stellt eine Verbindung zum ADC her, nachdem Sie die NetScaler-IP-Adresse (NSIP) zur NSWL-Konfigurationsdatei hinzugefügt haben
   - ADC puffert die HTTP- und HTTPS-Anforderungsprotokolleinträge, bevor er sie an den Client sendet.
   - Der Client kann die Einträge filtern (indem er die log.conf-Datei ändert), bevor er sie speichert.

> Hinweis
>
> Ändern Sie das Standardkennwort für NetScaler und fahren Sie dann mit der Konfiguration fort. Geben Sie den folgenden Befehl ein, um das Kennwort zu ändern:

```
set system user nsroot -password <your password>
<!--NeedCopy-->
```

Konfigurieren des Amazon Kinesis-Agenten

Führen Sie die folgenden Schritte in der AWS-Webkonsole aus, um den Amazon Kinesis-Agent zu konfigurieren:

1. Erstellen Sie eine Konfigurationsdatei (appsettings.json) und stellen Sie sie bereit. Konfigurationsdateien definieren Gruppen von Quellen, Senken und Pipes, die Quellen mit Senken verbinden, zusammen mit optionalen Transformationen.

   Das folgende Beispiel ist eine vollständige `appsettings.json` Konfigurationsdatei, die den Kinesis Agent so konfiguriert, dass Windows-Anwendungsprotokollereignisse an Kinesis Data Firehose streamen.

```
{

"Sources": [
    {

        "Id": "NSWLog",
        "SourceType": "DirectorySource",
        "Directory": "C:\Users\Administrator\Downloads\nswl_win
           -13.0-52.24\bin",
        "FileNameFilter": "*.log"
        "RecordParser": "TimeStamp",
        "TimestampFormat": "yyyy-MM-dddd HH:mm:ss.ffff", //
           Optional parameter required only by the timestamp
           record parser
        "TimeZoneKind": "UTC", //Local or UTC
        "SkipLines": 0 //Skip a number of lines at the beginning
           of each file
     }

    ],
"Sinks": [
    {

        "Id": "ApplicationLogKinesisFirehoseSink",
```



```
21          "SinkType": "KinesisFirehose",
22          "StreamName": "Delivery-ik-logs",
23          "AccessKey": "Your Access Key",
24          "SecretKey": "YourSecretKey",
25          "Region": "ap-south-1"
26       }
27
28     ],
29 "Pipes": [
30     {
31
32     "Id": "ApplicationLogSourceToApplicationLogKinesisFirehoseSink
          ",
33     "SourceRef": "ApplicationLogSource",
34     "SinkRef": "ApplicationLogKinesisFirehoseSink"
35       }
36
37     ],
38 "Telemetrics":
39     {
40
41     "off": "true"
42       }
43
44  }
45
46 <!--NeedCopy-->
```

2. Richten Sie einen Kinesis Agent für Datenquellen ein, um Daten zu sammeln und diese kontinuierlich an Amazon Kinesis Firehose/Kinesis Data Analytics zu senden. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Kinesis Agent für Microsoft Windows.
3. Erstellen Sie mit Amazon Kinesis Firehoseeinen End-to-End-Daten-Delivery-Stream. Der Lieferdatenstrom überträgt Ihre Daten vom Agenten an das Ziel. Das Ziel umfasst Amazon Kinesis Analytics, Amazon Redshift, Amazon Elasticsearch-Service und Amazon S3. Wählen Sie für die Quelle **Direct PUT oder andere Quellen** aus, um einen Kinesis Data Firehose-Bereitstellungsstream zu erstellen.
4. Verarbeiten Sie die eingehenden Protokolldaten mithilfe von SQL-Abfragen in Amazon Kinesis Analytics.
5. Laden Sie verarbeitete Daten von Kinesis Analytics in Amazon Elasticsearch Service, um die Daten zu indizieren.
6. Analysieren und visualisieren Sie die verarbeiteten Daten mit Visualisierungstools wie Kibana

und AWS QuickInsight Services.

Referenzen

- Syslog-Meldungen anzeigen und exportieren
- Citrix Networking für Hybrid Multi Cloud
- Schreiben in AWK Kinesis Data Streams mit Kinesis Agent

NetScaler in einer privaten Cloud - verwaltet von Microsoft Windows Azure Pack und Cisco ACI

May 11, 2023

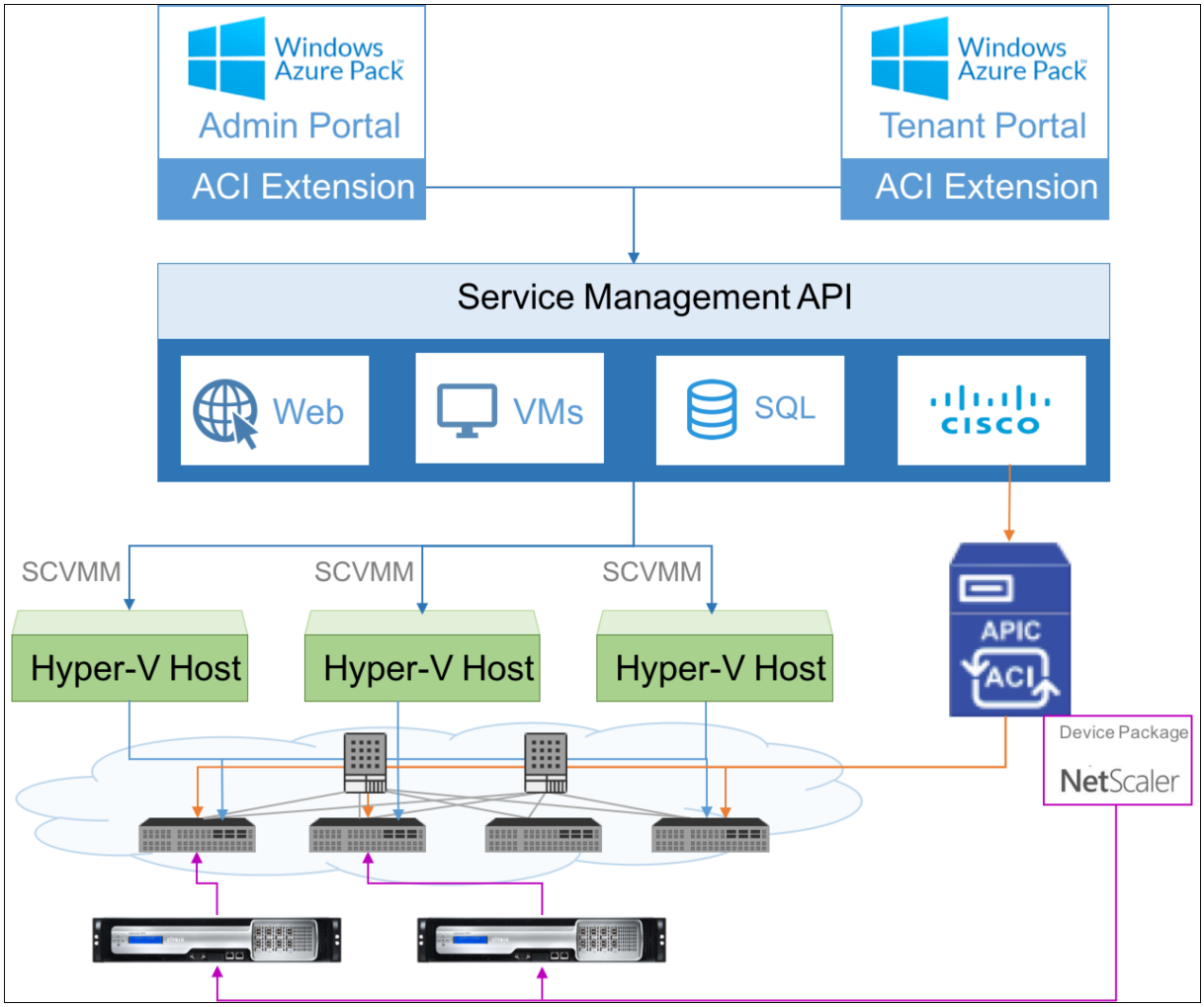
Sie können eine NetScaler-Appliance für den Lastenausgleich in einer privaten Cloud verwenden, die über Microsoft Windows Azure Pack verwaltet wird. Das Netzwerk für die Private Cloud wird mithilfe von Cisco ACI und NetScaler automatisiert.

Diese Lösung umfasst viele Integrationspunkte, wie z. B. Windows Azure Pack (WAP) zu Cisco APIC, Cisco APIC zu System Center Virtual Machine Manager (SCVMM) und Cisco APIC zu NetScaler. Als Mandant in der privaten Cloud können Sie NAT aktivieren, Netzwerkdienste bereitstellen und einen Load Balancer hinzufügen.

WAP unterstützt Mandanten- und Administratorportale, auf denen ein Administrator administrative Aufgaben wie die ACI-Registrierung, den VIP-Bereich, die Verknüpfung von NetScaler-Geräten mit der Cloud für virtuelle Maschinen und die Erstellung von Mandantenbenutzerkonten ausführen kann. Mandanten können sich am WAP Tenant Portal anmelden und das Netzwerk, die Bridge-Domänen und Virtual Routing and Forwarding (VRFs) konfigurieren und die NetScaler-Load-Balancing- und RNAT-Funktionen nutzen.

> **Wichtig**
>
> - In dieser Lösung bietet die NetScaler-Appliance nur einen grundlegenden Lastenausgleich.
> - Mandanten können mehrere VIP-Adressen mit unterschiedlichen Ports für dasselbe Netzwerk bereitstellen, müssen jedoch sicherstellen, dass die Kombination aus IP und Port eindeutig ist.
> - Das NetScaler-Gerätepaket unterstützt nur die Bereitstellung mit einem Kontext. Jeder Tenant erhält eine dedizierte NetScaler-Instanz.
> - WAP unterstützt NetScaler MPX-Appliances und virtuelle NetScaler VPX-Appliances, einschließlich NetScaler VPX-Instanzen, die auf der NetScaler SDX-Plattform bereitgestellt werden.

Die folgende Abbildung gibt einen Überblick über die Lösung:



Voraussetzungen

Stellen Sie Folgendes sicher:

- Sie verfügen über konzeptionelle Kenntnisse der Cisco ACI-Komponenten und NetScaler.
  - Weitere Informationen zu Cisco ACI und seinen Komponenten finden Sie in der Produktdokumentation unter: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Weitere Informationen zu den NetScalers finden Sie in der NetScaler-Produktdokumentation unter. http://docs.citrix.com/
- Alle erforderlichen Komponenten von Cisco ACI, einschließlich Cisco APIC im Rechenzentrum, sind eingerichtet und konfiguriert. Weitere Informationen zu Cisco ACI und seinen Komponenten finden Sie in der Produktdokumentation unter: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

- Sie wissen, wie Sie Cisco ACI in Microsoft Windows Azure Pack integrieren. Die Produktdokumentation finden Sie unter: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/virtualization/b_ACI_Virtualization_Guide_2_2_1.html.
- Sie verfügen über konzeptionelle Kenntnisse von Microsoft Windows Azure Pack. Die Produktdokumentation finden Sie unter: https://www.microsoft.com/en-in/cloud-platform/windows-azure-pack.
- Sie haben die NetScaler-Softwareversion 11.1 oder höher installiert.
- Sie konfigurieren NetScaler in Cisco ACI, sodass sie mithilfe von Cisco APIC verwaltet werden können.
- Stellen Sie von Cisco APIC aus sicher, dass:
  - Die Verwaltungskonnektivität von Cisco APIC zu NetScaler ist eingerichtet.
  - Sie laden das NetScaler-Gerätepaket Version *11.1—52.3* hoch und registrieren das NetScaler-Gerät mithilfe des Cisco APIC in Cisco ACI.
  - Sie konfigurieren die NetScaler-Appliance im Common Tenant von Cisco APIC und stellen sicher, dass der Cisco APIC keine Fehler enthält.
  - Sie haben alle APIC-spezifischen Konfigurationen wie VLAN-Pool, L3OutServicesDOM, L3ExtOut, Ressourcenpool konfiguriert. Weitere Informationen finden Sie in der *Cisco-Dokumentation*.

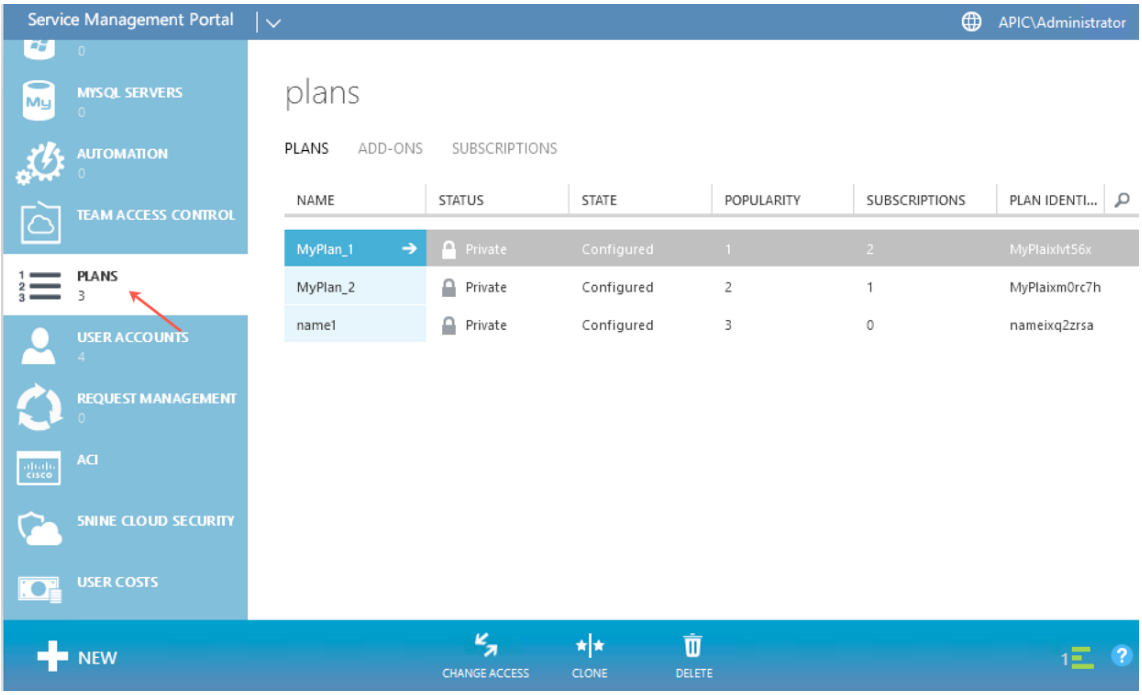
NetScaler Load Balancer in einem Plan im Service Management Portal (Admin Portal) erstellen

May 11, 2023

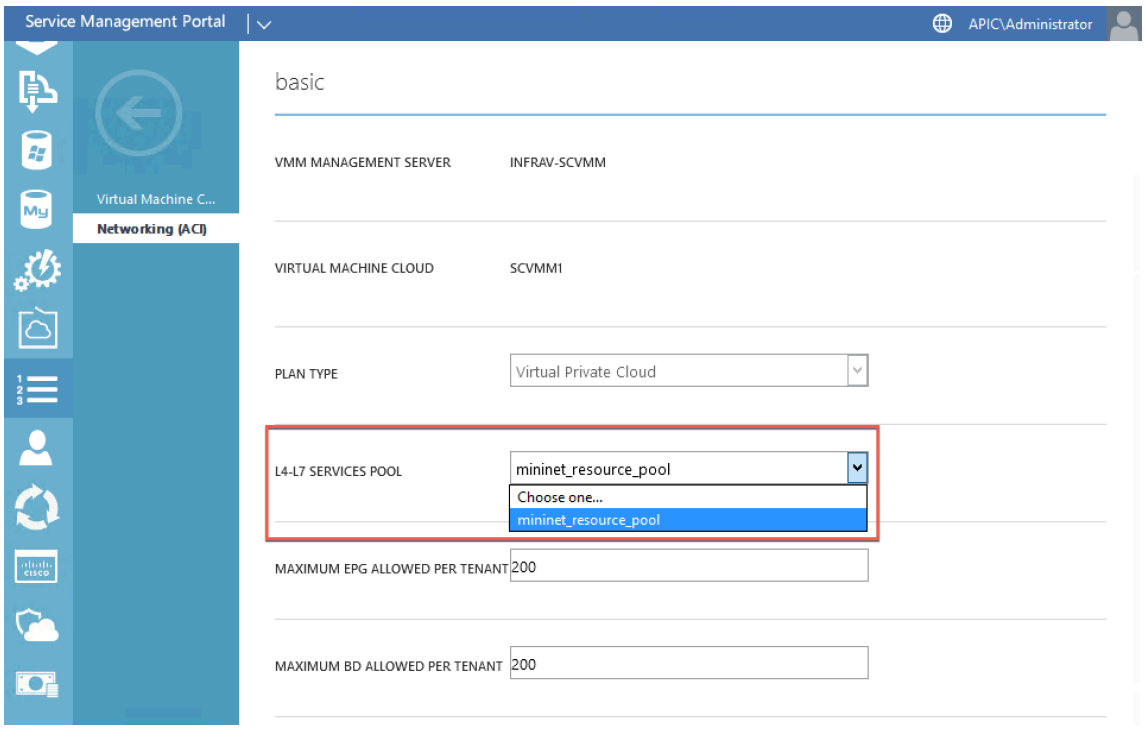
Das Service Management Portal in WAP ermöglicht es einem Administrator, Cisco APIC bei WAP zu registrieren und auch einen Hosting-Plan zu erstellen. Im Rahmen des Plans können Sie den VIP-Bereich angeben, den NetScaler Load Balancer mit dem Plan verknüpfen und Mandantenbenutzerkonten erstellen.

So erstellen Sie einen NetScaler Load Balancer in einem Plan im Admin-Portal:

1. Melden Sie sich beim Service Management Portal (Admin Portal) an.
2. Wählen Sie im Navigationsbereich **PLÄNE**aus.



3. Wählen Sie im Bereich Pläne den Plan aus, dem Sie einen Load Balancer hinzufügen möchten.
4. Wählen Sie im Bereich des ausgewählten Tarifs die Option **Networking (ACI)**aus.
5. Wählen Sie im Bereich **Networking (ACI)** in der Dropdownliste **L4-L7 SERVICE POOL** den L4-L7-Ressourcenpool aus, den Sie in Cisco APIC erstellt haben.



6. Erstellen Sie ein Mandantenbenutzerkonto, und ordnen Sie den Benutzer mit dem von Ihnen

erstellten Plan zu.

NetScaler Load Balancer über Service Management Portals (Tenant Portal) konfigurieren

May 11, 2023

Sobald der Tenant in WAP die Bridge Domain (BD), VRF und ein Netzwerk erstellt hat, kann er über das Service Management Portal (Tenant Portal) einen NetScaler Load Balancer konfigurieren.

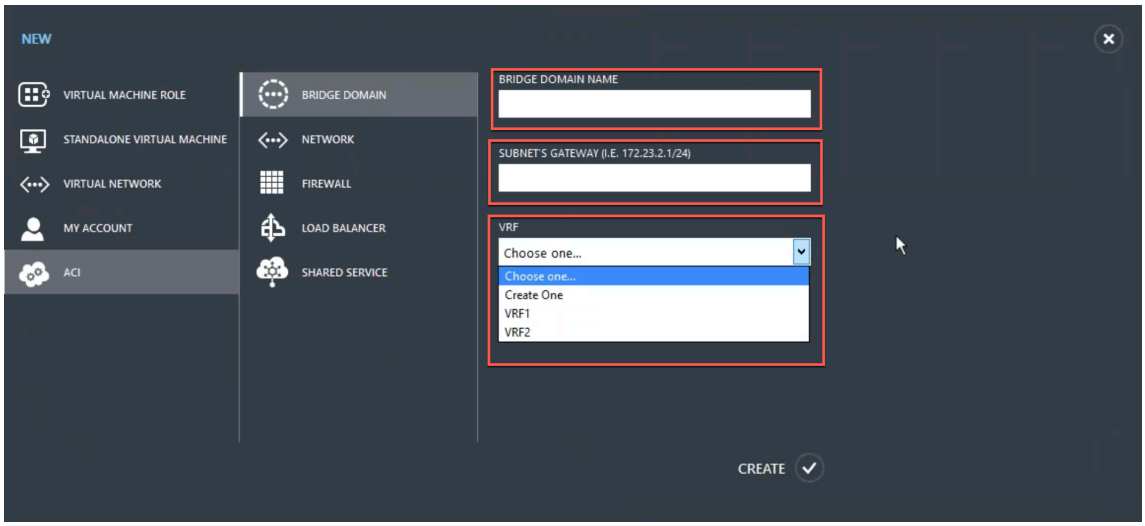
So konfigurieren Sie NetScaler Load Balancer im Service Management Portal (Tenant Portal)

1. Melden Sie sich beim Service Management Portal (Tenant Portal) an.
2. Erstellen Sie eine Bridge-Domäne und VRF wie folgt:

   a. Wählen Sie im Navigationsbereich **ACI**aus.

   b. Klicken Sie auf **NEU**.

   c. Wählen Sie im Bereich **NEU** die Option **BRIDGE DOMAIN**aus.



   d. Geben Sie in das Feld **BRIDGE-DOMAIN** den Bridge-Domainnamen ein (z. B. BD01).

   e. (Optional) Geben Sie in das Feld **SUBNETZ-GATEWAY das Gateway des** Subnetzes ein (z. B. 192.168.1.1/24).

   f. Wählen Sie im Feld **VRF** ein VRF aus, das bereits Teil des Abonnements ist, oder wählen Sie **Create One** aus, um ein VRF zu erstellen.

   g. Klicken Sie auf **CREATE**.

3. Erstellen Sie ein Netzwerk und verknüpfen Sie es mit der Bridge-Domäne, die Sie erstellt haben. Führen Sie folgende Schritte aus:

   a. Wählen Sie im Navigationsbereich **ACI**aus.

   b. Klicken Sie auf **NEU**.

   c. Wählen Sie im Bereich **NEU** die Option **NETZWERK**aus.

   d. Geben Sie in das Feld **NETZWERKNAME** den Netzwerknamen ein (z. B. S01).

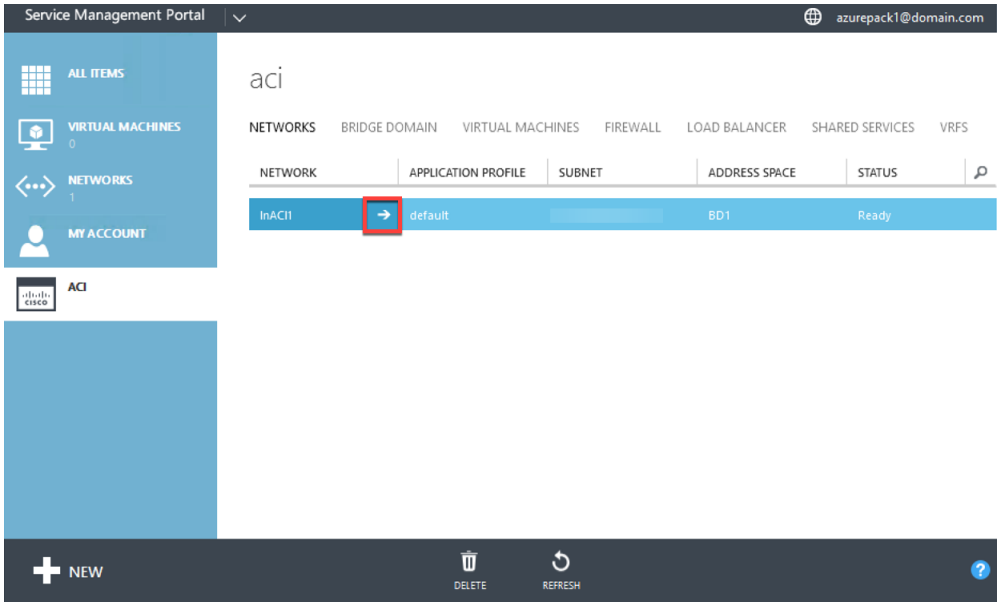
   e. Wählen Sie in der Dropdownliste **BRIDGE-DOMAIN** die Bridge-Domain aus, die Sie erstellt haben. (zum Beispiel BD01).

   f. Geben Sie in das **GATEWAY-Feld des Subnetzes die Gateway-Adresse** des Subnetzes ein (z. B. 172.23.2.1/24).

   g. (Optional) Geben Sie in das Feld **DNS-SERVER-IP/IPS** die DNS-Serverdetails ein.

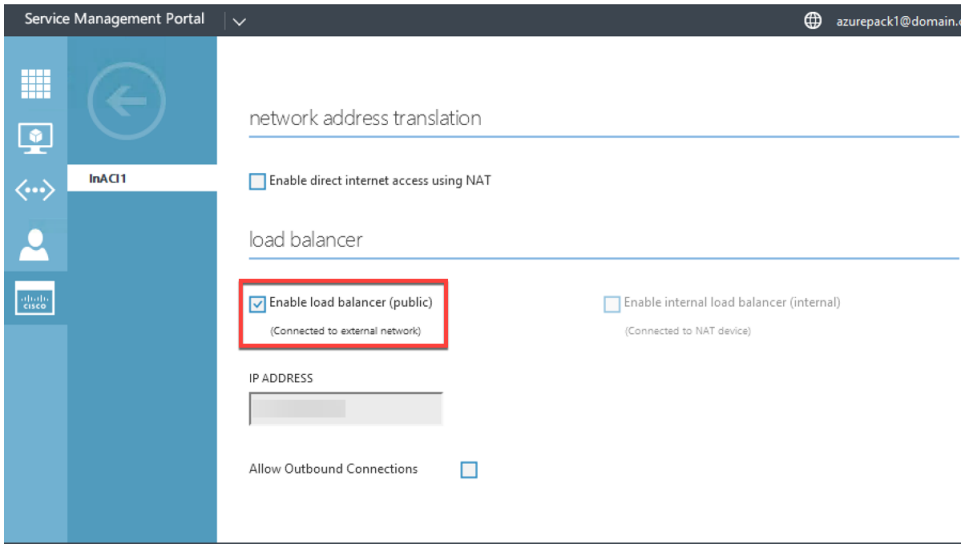
   h. Klicken Sie auf **CREATE**.

4. Wählen Sie im **ACI-BereichNETWORKS**aus.



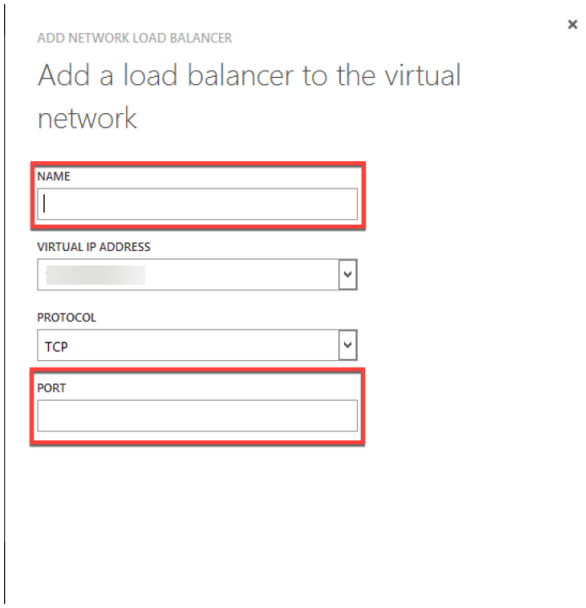
5. Doppelklicken Sie auf das Netzwerk, das Sie erstellt haben. Wählen Sie dann im Netzwerkbereich die Option **Load Balancer aktivieren (öffentlich)**aus. Im Feld **IP-Adresse** wird automatisch ein VIP aus dem VIP-Bereich zugewiesen, den der Administrator im Admin-Portal konfiguriert hat. Weitere Informationen finden Sie unter Erstellen eines NetScaler Load Balancer in einem Plan im Service Management Portal (Admin-Portal).

6. Doppelklicken Sie auf das Netzwerk, das Sie erstellt haben. Wählen Sie dann im Netzwerkbereich die Option **Load Balancer aktivieren (öffentlich)**aus. Im Feld **IP-Adresse** wird automatisch ein VIP aus dem VIP-Bereich zugewiesen, den der Administrator im Admin-Portal konfiguriert hat. Weitere Informationen finden Sie unter Erstellen eines NetScaler Load Balancer in einem Plan im Service Management Portal (Admin-Portal).



7. Wählen Sie im Netzwerkbereich die Registerkarte **Load Balancers** aus und klicken Sie auf

HINZUFÜGEN.



8. Gehen **Sie im Bereich NETWORK LOAD BALANCER HINZUFÜGEN** wie folgt vor:

   a. Geben Sie im Feld **NAME** den Namen für den Load Balancer ein.

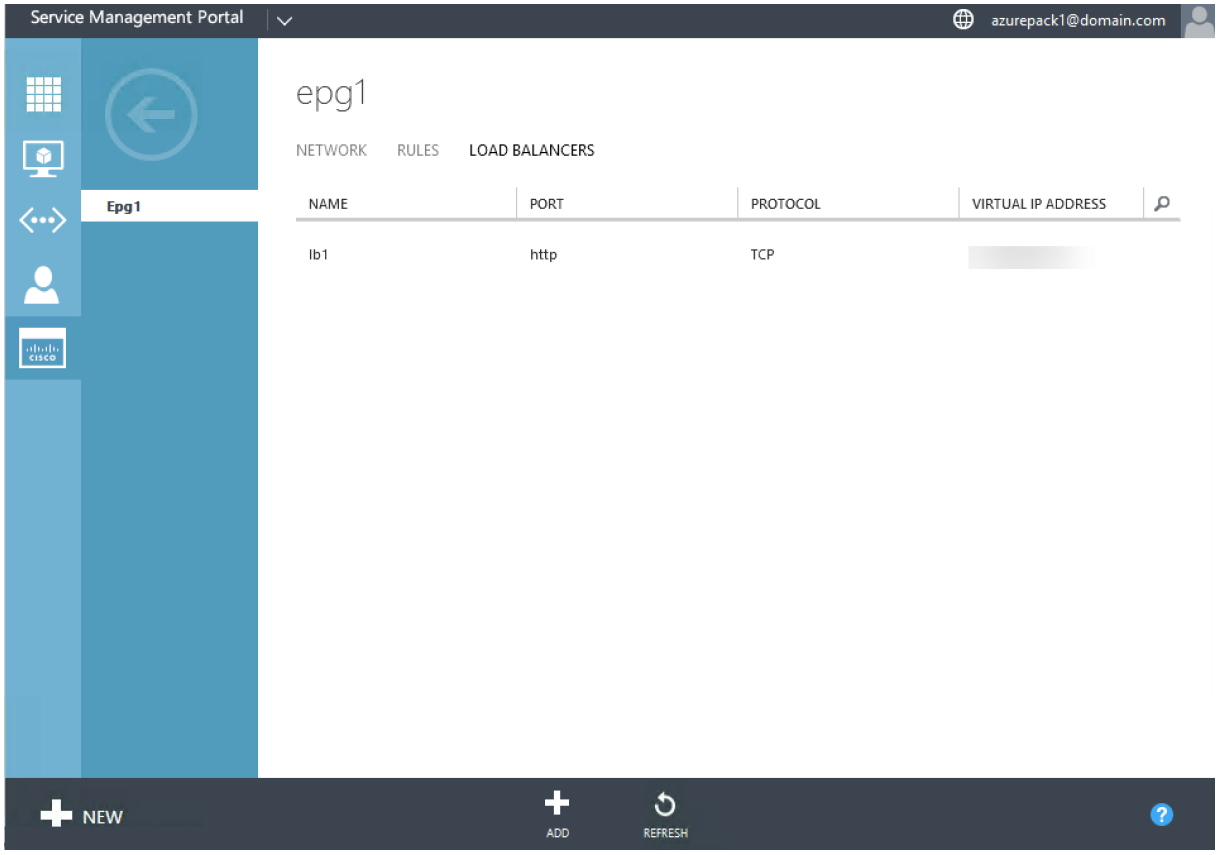
   b. Weisen Sie dem Load Balancer optional im Feld **VIRTUELLE IP-ADRESSE** eine VIP-Adresse aus dem VIP-Bereich zu, den Sie zuvor definiert haben.

   c. Wählen Sie optional im Feld **PROTOKOLL** die Option **TCP**aus.

   d. Geben Sie in das Feld **PORT** die Portnummer ein.

9. Klicken Sie auf **CREATE**.

   Der NetScaler Load Balancer wird auf der Registerkarte **LOAD BALANCERS** angezeigt und der NetScaler Load Balancer ist bereit für den Datenpfad.



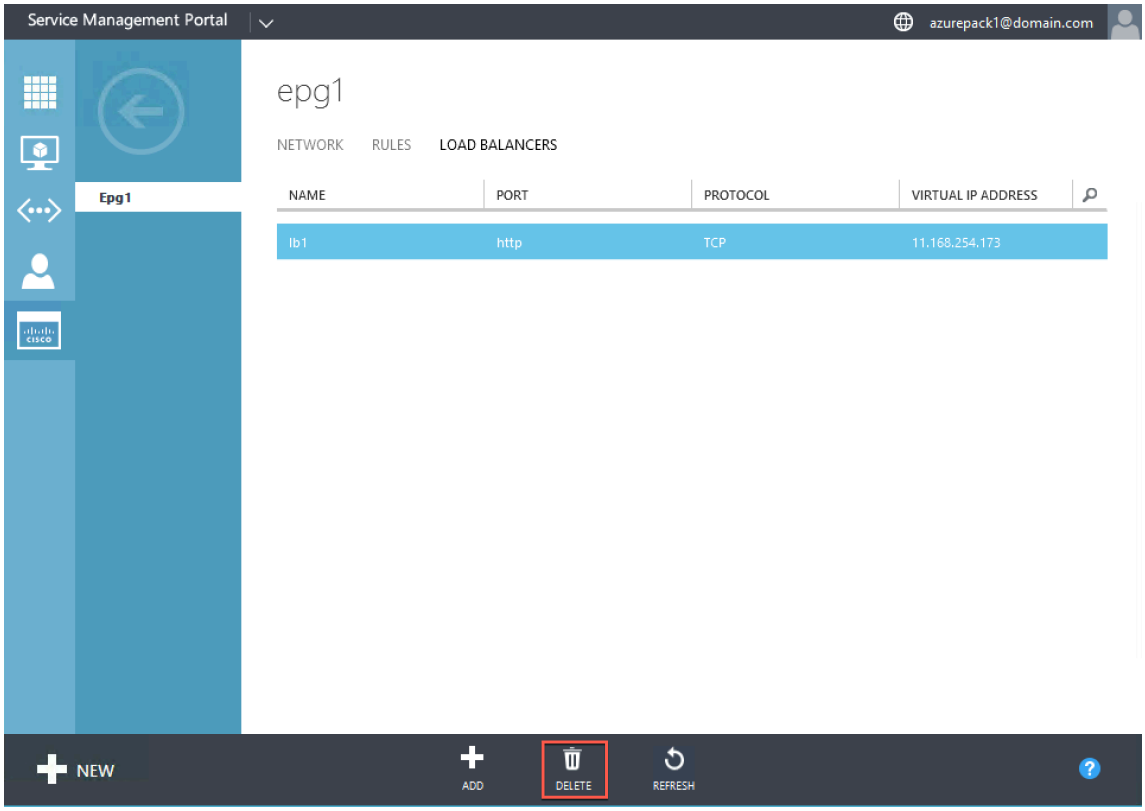
NetScaler Load Balancer aus dem Netzwerk löschen

May 11, 2023

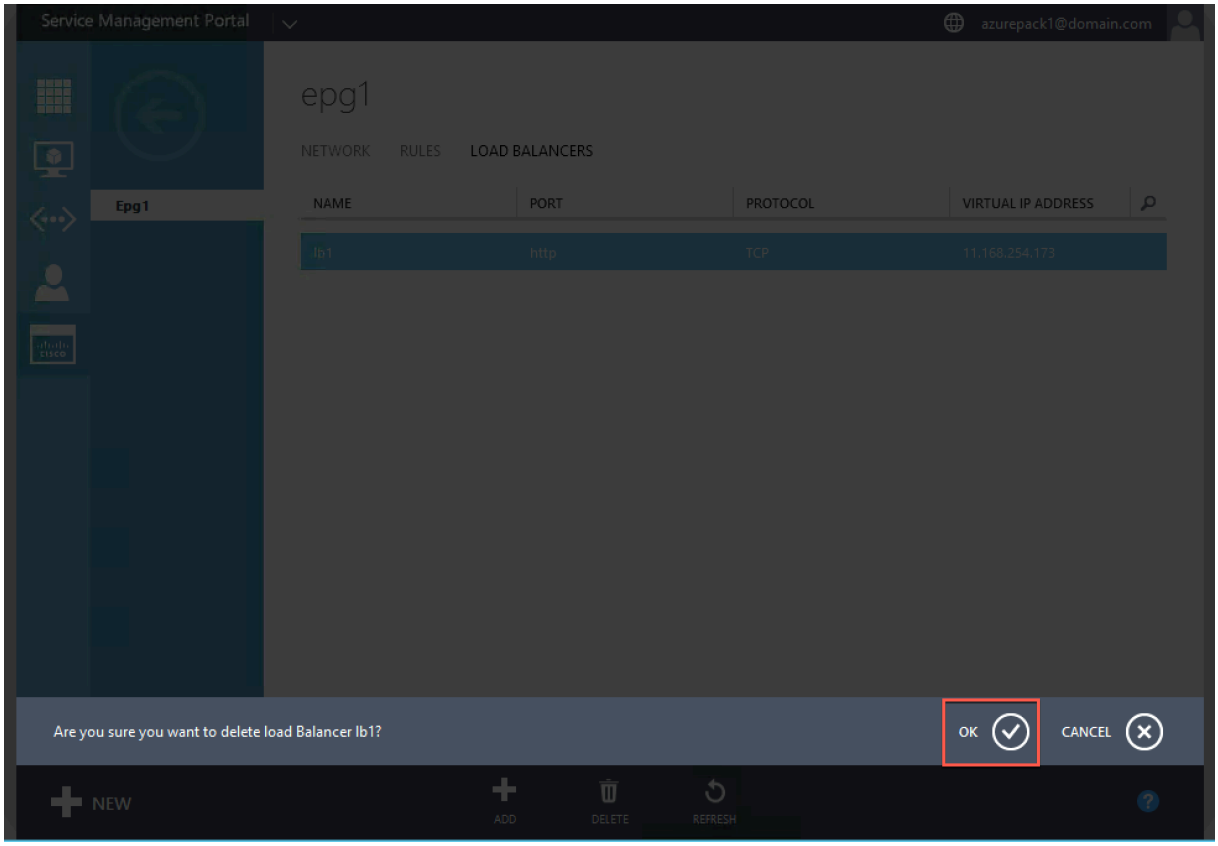
Mithilfe des Service Management Portals (Tenant Portal) können Sie den NetScaler Load Balancer, den Sie erstellt haben, aus dem Netzwerk löschen.

So löschen Sie einen NetScaler Load Balancer aus dem Netzwerk:

1. Melden Sie sich beim Service Management Portal (Tenant Portal) an.
2. Wählen Sie im Navigationsbereich **ACI**aus.
3. Klicken **Sie im ACI-Bereich** auf der Registerkarte **NETZWERKE** auf das Netzwerk, das Sie erstellt haben.
4. **Wählen Sie im Bereich des ausgewählten Netzwerks den NetScaler Load Balancer aus und klicken Sie auf LÖSCHEN.**



5. Klicken Sie auf **OK**, um den NetScaler Load Balancer zu löschen.



NetScaler Cloud-native Lösung für Microservices auf Basis von Kubernetes

May 11, 2023

Während sich Unternehmen transformieren, um schneller Innovationen zu entwickeln und näher an ihre Kunden heranzukommen, gestalten sie ihre internen Prozesse neu und überwinden Grenzen innerhalb ihrer Organisation. Sie bauen Silos auf, um die richtigen Fähigkeiten im selben Team zusammenzuführen. Eines der Ziele ist es, Softwareanwendungen schnell, agil und effizient zu erstellen und bereitzustellen. In dieser Hinsicht werden moderne Anwendungsarchitekturen, die auf Microservices basieren, von einer wachsenden Zahl von Unternehmen übernommen.
Mithilfe einer Microservices-Architektur können Sie Anwendungen als Gruppen von lose gekoppelten Diensten erstellen, die unabhängig voneinander bereitgestellt, aktualisiert und skaliert werden können.

Cloud Native ist ein Ansatz, der auf der Microservices-Architektur für die Erstellung und Bereitstellung von Anwendungen mit den folgenden Schlüsselattributen basiert:

- Stellt Anwendungen als lose gekoppelte Microservices oder Container bereit
- Beinhaltet einen sehr hohen Automatisierungsgrad
- Implementiert agile DevOps-Prozesse und Continuous-Delivery-Workflows
- Im Mittelpunkt stehen APIs für Interaktion und Zusammenarbeit

Wie hilft Kubernetes auf dem Weg zur Cloud-Native?

Um das gewünschte Maß an Agilität und Stabilität zu bieten, erfordern Cloud-native Anwendungen ein hohes Maß an Infrastrukturautomatisierung, Sicherheit, Netzwerk und Überwachung. Sie benötigen ein Container-Orchestrierungssystem, das Container in großem Maßstab effizient verwalten kann. Kubernetes hat sich als die beliebteste Plattform für die Bereitstellung und Orchestrierung von Containern entwickelt. Kubernetes abstrahiert die komplexe Aufgabe der Ausführung, Bereitstellung und Verwaltung von Containern von Entwicklern und Operatoren und plant automatisch Container zwischen einem Cluster von Knoten. Kubernetes und das Ökosystem der Cloud Native Computing Foundation (CNCF) helfen Ihnen beim Aufbau einer Plattform für Cloud-native Lösungen.

Einige der wichtigsten Vorteile der Verwendung von Kubernetes:

- Vereinfacht die Anwendungsbereitstellung, unabhängig davon, ob es sich um eine lokale, hybride oder öffentliche Cloud-Infrastruktur handelt
- Beschleunigt die Anwendungsentwicklung und -bereitstellung
- Erhöht die Agilität, Flexibilität und Skalierbarkeit von Anwendungen

Was ist die native Cloud-Lösung von NetScaler?

Um die Vorteile des Einsatzes von Kubernetes in der Produktion zu maximieren, müssen Sie Kubernetes in verschiedene Tools sowie Komponenten von Anbietern und Open-Source-Komponenten integrieren. Die Sicherstellung der Zuverlässigkeit und Sicherheit ihrer Cloud-nativen Anwendungen auf Produktionsniveau ist für viele Unternehmen eine Herausforderung.
Als Anbieter branchenführender NetScaler bietet NetScaler eine native NetScaler-Cloud-Lösung, um die Herausforderungen in einer Kubernetes-Produktionsumgebung zu bewältigen.

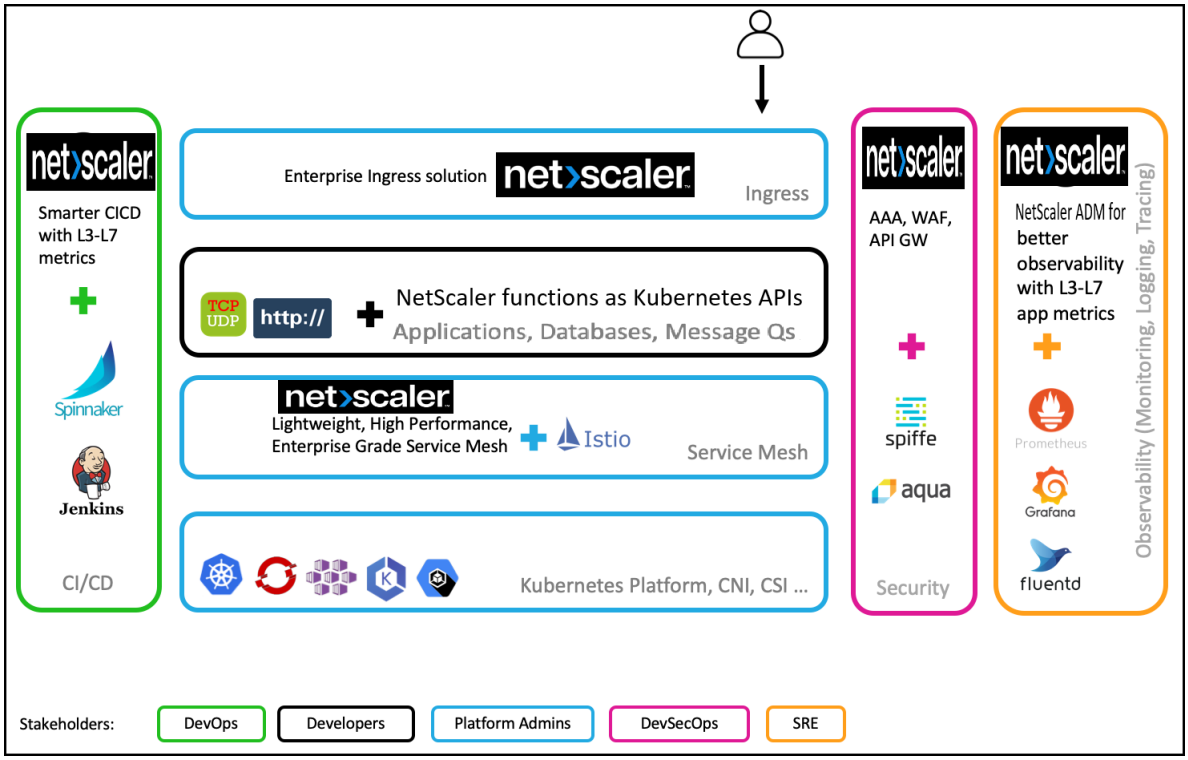
Die native Cloud-Lösung von NetScaler nutzt das fortschrittliche Verkehrsmanagement, die Beobachtbarkeit und die umfassenden Sicherheitsfunktionen von NetScalers, um Zuverlässigkeit und Sicherheit auf Unternehmensebene zu gewährleisten. Es kann einen vollständigen Überblick über den Anwendungsverkehr in Ihrer Kubernetes-Umgebung bieten, sofortiges Feedback geben und dabei helfen, aussagekräftige Einblicke in die Anwendungsleistung zu gewinnen.

In der folgenden Tabelle sind die wichtigsten Anforderungen der verschiedenen Stakeholder bei der Implementierung einer Ingress-Lösung aufgeführt.

Interessenvertreter	Funktion des Jobs	Bedürfnisse
Plattformadministratoren	Stellen Sie die Verfügbarkeit von Kubernetes-Clustern sicher	Einfachere Methoden zur Verwaltung von Anwendungen, die in mehreren Clustern eingesetzt werden, sowie Betriebs- und Plattformlebenszyklusmanagement
DevOps	Beschleunigen Sie die Bereitstellung von Anwendungen für die Produktion	Integration mit der CI/CD-Pipeline, Unterstützung von Bereitstellungstechniken wie Canary und Blue-Green für eine schnellere Bereitstellung
Entwickler	Entwickeln und testen Sie Microservices	Möglichkeiten, Traffic in den Kubernetes-Cluster zu bringen, Tracing und Debugging, Ratenbegrenzung für Anwendungen und Authentifizierung für Anwendungen

Interessenvertreter	Funktion des Jobs	Bedürfnisse
SREs	Stellen Sie die Verfügbarkeit von Anwendungen sicher, um Service Level Agreements einzuhalten	Fortschrittliche Telemetrie für Anwendungen und Infrastruktur
SecOps	Stellen Sie die Einhaltung der Sicherheitsbestimmungen	Sicherer Ingress-Traffic, API-Schutz, Service Mesh für sichere Kommunikation zwischen Microservices innerhalb des Kubernetes-Clusters

In der folgenden Abbildung wird die native Cloud-Lösung von NetScaler erläutert und erklärt, wie sie die verschiedenen Herausforderungen bewältigt, mit denen die Beteiligten auf ihrem Weg zur Cloud-nativen Nutzung konfrontiert sind.



Die native Cloud-Lösung von NetScaler bietet die folgenden Hauptvorteile:

- Bietet eine fortschrittliche Kubernetes Ingress-Lösung, die auf die Bedürfnisse von Entwicklern, SREs, DevOps sowie Netzwerk- oder Clusteradministratoren zugeschnitten ist.
- Macht es überflüssig, ältere Anwendungen auf der Grundlage von TCP- oder UDP-Verkehr neu

zu schreiben und sie gleichzeitig in eine Kubernetes-Umgebung zu verschieben.
- Sichert Anwendungen mit NetScaler-Richtlinien, die als Kubernetes-APIs verfügbar sind.
- Hilft bei der Bereitstellung leistungsstarker Microservices für den Nord-Süd-Verkehr und den Ost-West-Verkehr.
- Bietet eine Komplettansicht aller Microservices mithilfe des NetScaler ADM Service Graph.
- Ermöglicht eine schnellere Fehlerbehebung von Microservices für verschiedene Arten von Datenverkehr, einschließlich TCP, UDP, HTTP, HTTPS und SSL.
- Sichert APIs.
- Automatisiert die CI/CD-Pipeline für Canary-Bereitstellungen.
- Bietet sofort einsatzbereite Integrationen mit CNCF-Open-Source-Tools.

Weitere Informationen zu den verschiedenen Cloud-nativen Lösungen von Citrix finden Sie unter den folgenden Links:

- Kubernetes Ingress-Lösung
- Service-Mesh
- Lösungen für die Beobachtbarkeit
- API-Gateway für Kubernetes

Komponenten der nativen Cloud-Lösung von NetScaler

In der folgenden Tabelle werden die Hauptkomponenten der nativen Cloud-Lösung von NetScaler erläutert:

Komponente	Beschreibung
NetScaler Ingress Controller	Dieser Container ist eine Implementierung des Kubernetes Ingress Controllers zur Verwaltung und Weiterleitung von Datenverkehr in Ihren Kubernetes-Cluster mithilfe von NetScalern (NetScaler CPX, VPX oder MPX). Mit dem NetScaler Ingress Controller können Sie NetScaler CPX, VPX oder MPX gemäß den Ingress-Regeln konfigurieren und Ihre NetScaler in die Kubernetes-Umgebung integrieren.

Komponente	Beschreibung
NetScaler Observability Exporteur	NetScaler Observability Exporter ist ein Container, der Metriken und Transaktionen von NetScalern sammelt und sie in geeignete Formate (wie JSON, AVRO) für unterstützte Endgeräte umwandelt. Sie können die von NetScaler Observability Exporter gesammelten Daten zum gewünschten Endpunkt exportieren. Durch die Analyse der an den Endpunkt exportierten Daten können Sie wertvolle Erkenntnisse auf Microservices-Ebene für Anwendungen gewinnen, die von NetScalern als Proxy bereitgestellt werden.
NetScaler xDS-Adapter	Der NetScaler xDS-Adapter ist ein Container für die Integration von NetScaler in Implementierungen der Service-Mesh-Steuerungsebene, die auf xDS-APIs (Istio, Consul usw.) basieren. Es kommuniziert mit der Service-Mesh-Steuerungsebene und wartet auf Aktualisierungen, indem es als gRPC-Client für den API-Server der Steuerungsebene fungiert. Basierend auf den Updates von der Steuerungsebene generiert der NetScaler xDS-Adaptor die entsprechende NetScaler-Konfiguration.

Komponente	Beschreibung
NetScaler CPX	NetScaler CPX ist ein Container-basierter Anwendungsbereitstellungscontroller, der auf einem Docker-Host bereitgestellt werden kann. NetScaler CPX ermöglicht es Kunden, die Docker-Engine-Funktionen zu nutzen und NetScaler Load Balancing- und Traffic-Management-Funktionen für Container-basierte Anwendungen zu nutzen. Sie können eine oder mehrere NetScaler CPX-Instanzen als eigenständige Instanzen auf einem Docker-Host bereitstellen.

Kubernetes Ingress-Lösung

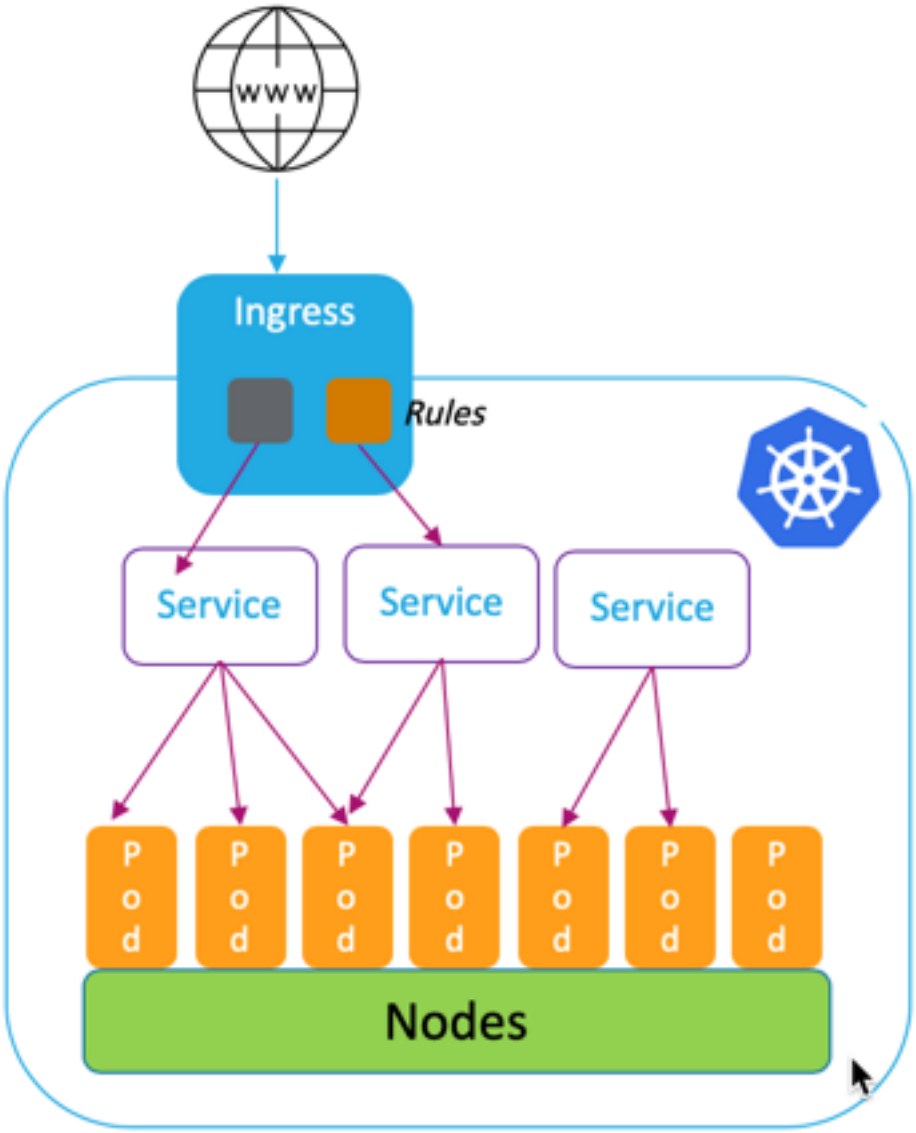
May 11, 2023

Dieses Thema bietet einen Überblick über die von NetScaler bereitgestellte Kubernetes Ingress-Lösung und erklärt die Vorteile.

Was ist Kubernetes Ingress?

Wenn Sie eine Anwendung in einem Kubernetes-Cluster ausführen, müssen Sie externen Benutzern die Möglichkeit bieten, von außerhalb des Kubernetes-Clusters auf die Anwendungen zuzugreifen. Kubernetes bietet ein Objekt namens Ingress, das die effektivste Methode bietet, mehrere Dienste mithilfe einer stabilen IP-Adresse verfügbar zu machen. Ein Kubernetes-Ingress-Objekt ist immer mit einem oder mehreren Diensten verknüpft und dient als zentraler Einstiegspunkt für externe Benutzer, um auf Dienste zuzugreifen, die innerhalb des Clusters ausgeführt werden.

Das folgende Diagramm erklärt, wie Kubernetes Ingress funktioniert.



Die Kubernetes Ingress-Implementierung besteht aus den folgenden Komponenten:

- **Eingangsressource**. Mit einer Ingress-Ressource können Sie Regeln für den Zugriff auf die Anwendungen von außerhalb des Clusters definieren.
- **Eingangskontrolle**. Ein Ingress-Controller ist eine Anwendung, die innerhalb des Clusters bereitgestellt wird, die Regeln interpretiert, die im Ingress definiert sind. Ingress-Controller wandelt die Ingress-Regeln in Konfigurationsanweisungen für eine in den Cluster integrierte Load Balancing-Anwendung um. Der Load Balancer kann eine Softwareanwendung sein, die innerhalb Ihres Kubernetes-Clusters ausgeführt wird, oder eine Hardware-Appliance, die außerhalb des Clusters ausgeführt wird.

- **Gerät eingeben**. Ein Ingress-Gerät ist eine Lastausgleichsanwendung wie NetScaler CPX, VPX oder MPX, die den Lastausgleich gemäß den Konfigurationsanweisungen des Ingress-Controller durchführt.

Was ist die Kubernetes Ingress-Lösung von Citrix?

In dieser Lösung bietet NetScaler eine Implementierung des Kubernetes Ingress Controllers zur Verwaltung und Weiterleitung des Datenverkehrs an Ihren Kubernetes-Cluster mithilfe von NetScalern (NetScaler CPX, VPX oder MPX). Der NetScaler Ingress Controller integriert NetScalers in Ihre Kubernetes-Umgebung und konfiguriert NetScaler CPX, VPX oder MPX gemäß den Ingress-Regeln.

Standardlösungen von Kubernetes Ingress bieten Load Balancing nur auf Layer 7 (HTTP- oder HTTPS-Datenverkehr). Manchmal müssen Sie viele Legacy-Anwendungen verfügbar machen, die auf TCP oder UDP oder Anwendungen angewiesen sind und eine Möglichkeit benötigen, diese Anwendungen auszugleichen. Die NetScaler Ingress Controller-Lösung bietet neben dem standardmäßigen HTTP- oder HTTPS-Ingress Unterstützung für TCP-, TCP-SSL- und UDP-Verkehr. Außerdem funktioniert es nahtlos über mehrere Clouds oder on-premises Rechenzentren hinweg.

NetScaler bietet Verkehrsverwaltungsrichtlinien für Unternehmen wie Rewrite- und Responder-Richtlinien für einen effizienten Lastenausgleich des Datenverkehrs auf Layer 7. Kubernetes Ingress fehlen jedoch solche Traffic-Management-Richtlinien für Unternehmen. Mit der Kubernetes Ingress-Lösung von Citrix können Sie mithilfe von CRDs von NetScaler Rewrite- und Responder-Richtlinien für den Anwendungsverkehr in einer Kubernetes-Umgebung anwenden.

Die Kubernetes Ingress-Lösung von Citrix unterstützt auch die automatisierte Canary-Bereitstellung für Ihre CI/CD-Anwendungspipeline. In dieser Lösung ist NetScaler in die Spinnaker-Plattform integriert und dient als Quelle für die Bereitstellung präziser Metriken für die Analyse der Canary-Bereitstellung mit Kayenta. Nach der Analyse der Metriken generiert Kayenta einen Aggregatwert für den Kanarienvogel und beschließt, die kanarische Version zu bewerben oder zu scheitern. Sie können auch die Verteilung des Datenverkehrs auf die Canary-Version mithilfe der NetScaler Richtlinieninfrastruktur regeln.

In der folgenden Tabelle sind die Vorteile zusammengefasst, die die Ingress-Lösung von Citrix gegenüber Kubernetes Ingress bietet.

Features	Kubernetes Ingress	Ingress-Lösung von Citrix
HTTP- und HTTPS-Unterstützung	Ja	Ja
URL-Routing	Ja	Ja
TLS	Ja	Ja
Lastausgleich	Ja	Ja

Features	Kubernetes Ingress	Ingress-Lösung von Citrix
TCP, TCP-SSL	Nein	Ja
UDP	Nein	Ja
HTTP/2	Ja	Ja
Automatisierter Canary-Deployment-Support mit CI/CD-Tools	Nein	Ja
Unterstützung für die Anwendung der NetScaler Rewrite- und Responder-Richtlinien	Nein	Ja
Authentifizierung (Open Authorization (OAuth), gegenseitiges TLS (mTLS))	Nein	Ja
Unterstützung für die Anwendung der Citrix-Richtlinien zur Ratenbegrenzung	Nein	Ja

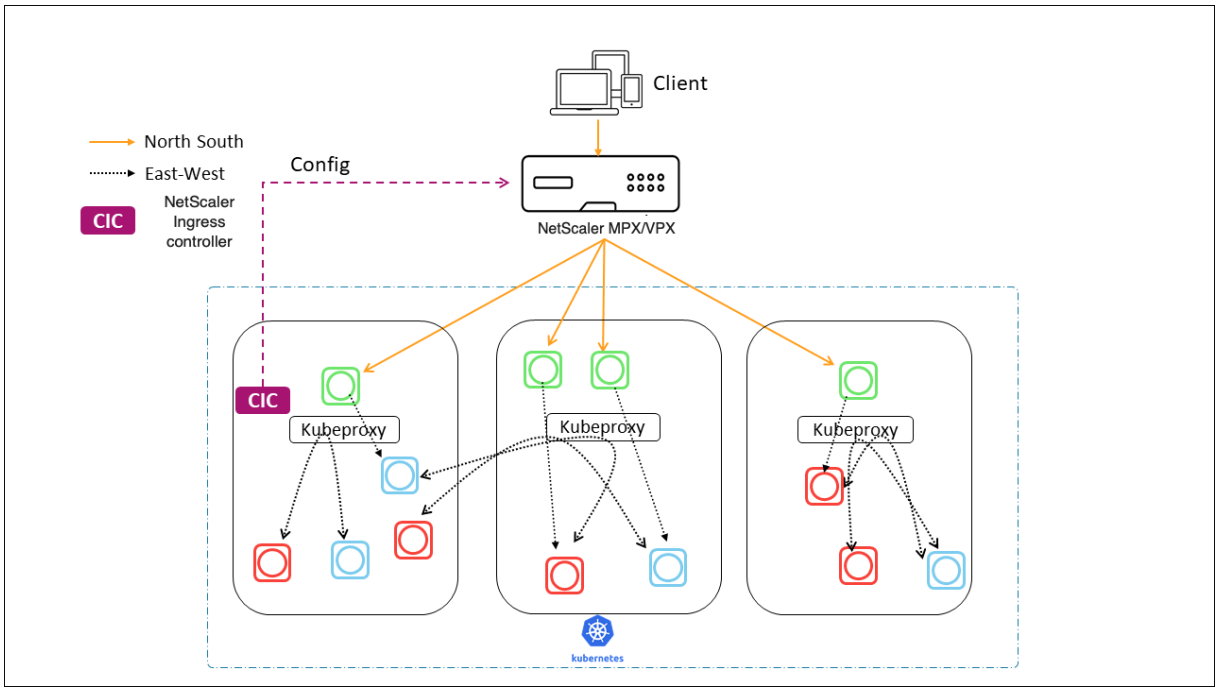
Bereitstellungsoptionen für die Kubernetes Ingress-Lösung

Die Kubernetes Ingress-Lösung von NetScaler bietet Ihnen eine flexible Architektur, je nachdem, wie Sie Ihre NetScalers- und Kubernetes-Umgebung verwalten möchten.

Einheitliches Ingress (einstufig)

In einer einheitlichen Ingress-Architektur (Single-Tier) wird ein NetScaler MPX- oder VPX-Gerät, das außerhalb des Kubernetes-Clusters bereitgestellt wird, mithilfe des NetScaler Ingress Controller in die Kubernetes-Umgebung integriert. Der NetScaler Ingress Controller wird als Pod im Kubernetes-Cluster bereitgestellt und automatisiert die Konfiguration von NetScalern auf der Grundlage von Änderungen an den Microservices oder den Ingress-Ressourcen. Das NetScaler Gerät führt Funktionen wie Lastenausgleich, TLS-Beendigung und HTTP- oder TCP-Protokolloptimierungen für eingehenden Datenverkehr aus und leitet den Datenverkehr dann an den richtigen Microservice innerhalb eines Kubernetes-Clusters weiter. Diese Architektur eignet sich am besten für Szenarien, in denen dasselbe Team die Kubernetes-Plattform und andere Netzwerkinfrastrukturen einschließlich Application Delivery Controllers (ADCs) verwaltet.

Das folgende Diagramm zeigt eine Bereitstellung mit der einheitlichen Ingress-Architektur.



Eine einheitliche Ingress-Lösung bietet die folgenden Hauptvorteile:

- Bietet eine Möglichkeit, die Funktionen Ihrer vorhandenen NetScaler-Infrastruktur auf die Kubernetes-Umgebung zu erweitern
- Ermöglicht die Anwendung von Verkehrsmanagementrichtlinien für eingehenden Datenverkehr
- Bietet eine vereinfachte Architektur, die für netzwerkaffine DevOps-Teams geeignet ist
- Unterstützt Mehrmandantenfähigkeit

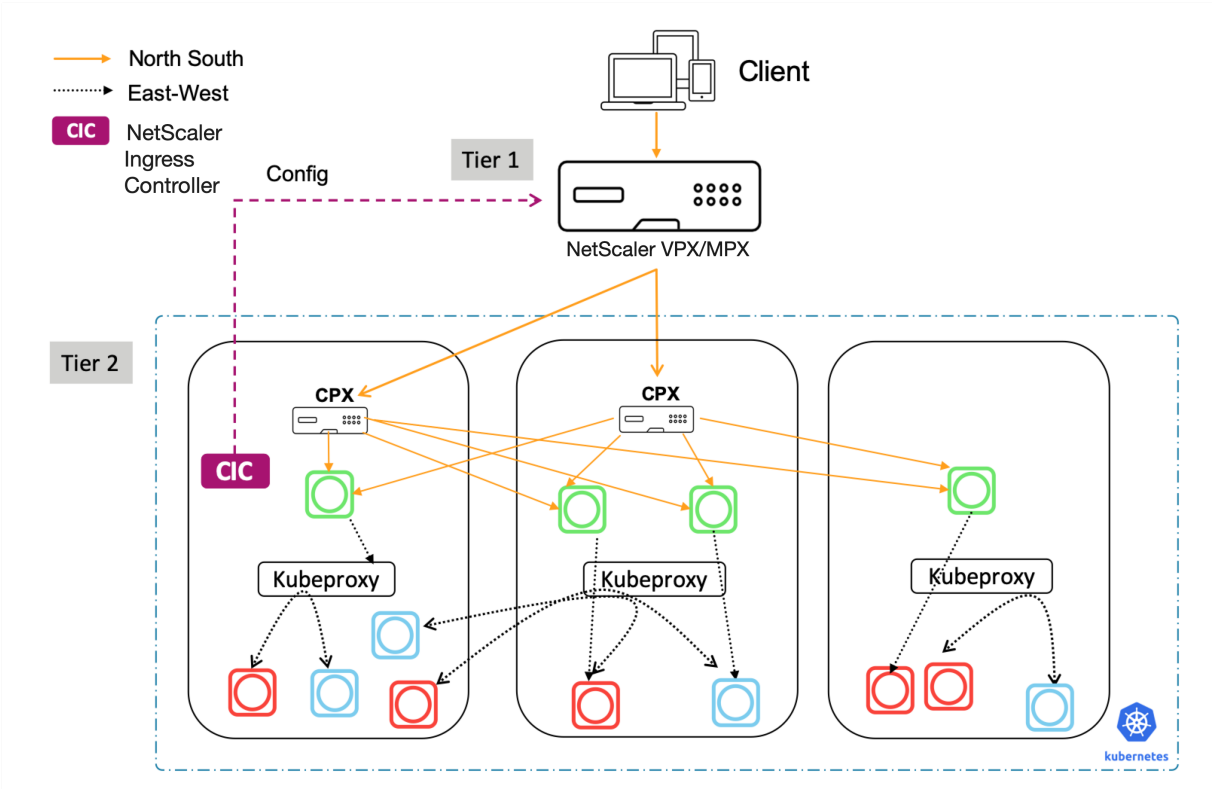
Zweistufiger Ingress

In einer dualen Architektur agiert NetScaler (MPX oder VPX), das außerhalb des Kubernetes-Clusters bereitgestellt wird, auf Ebene 1 und verteilt den Nord-Süd-Verkehr auf NetScaler CPXs, die innerhalb des Clusters laufen. NetScaler CPX fungiert auf Stufe 2 und führt Load Balancing für Microservices innerhalb des Kubernetes-Clusters durch.

In Szenarien, in denen separate Teams die Kubernetes-Plattform und die Netzwerkinfrastruktur verwalten, ist die Dual-Tier-Architektur am besten geeignet.

Netzwerkteams verwenden NetScaler Tier 1 für Anwendungsfälle wie GSLB, TLS-Beendigung auf der Hardwareplattform und TCP-Lastenausgleich. Kubernetes-Plattformteams können Tier 2 NetScaler (CPX) für Layer-7-Lastenausgleich (HTTP/HTTPS), gegenseitiges TLS sowie Observability oder Überwachung von Microservices verwenden. Der Tier-2-NetScaler (CPX) kann eine andere Softwareversion als der Tier-1-NetScaler haben, um neu verfügbare Funktionen zu berücksichtigen.

Das folgende Diagramm zeigt eine Bereitstellung mit Dual-Tier-Architektur.



Ein zweistufiges Ingress bietet die folgenden Hauptvorteile:

- Sorgt für eine hohe Geschwindigkeit der Anwendungsentwicklung für Entwickler oder Plattformteams
- Ermöglicht die Anwendung von entwicklergesteuerten Traffic-Management-Richtlinien für Microservices innerhalb des Kubernetes-Clusters
- Ermöglicht Cloud-Skalierung und Mandantenfähigkeit

Weitere Informationen finden Sie in der NetScaler IngressController-Dokumentation.

Erste Schritte

Um mit der Kubernetes Ingress-Lösung von Citrix zu beginnen, können Sie die folgenden Beispiele ausprobieren:

- Lastausgleich für eingehenden Datenverkehr mit NetScaler CPX in Minikube
- Lastausgleich zwischen Nord-Süd und eingehenden Datenverkehr mithilfe des NetScaler CPX-Proxys
- Lastenausgleich des Ost-West-Microservice-Datenverkehrs mithilfe des NetScaler CPX-Proxys

Service-Mesh

May 11, 2023

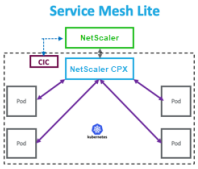
Ein Service Mesh ist eine Infrastrukturebene für die Verwaltung der Service-to-Service-Kommunikation für cloudnative Anwendungen mithilfe von APIs. Es bietet eine Möglichkeit, Ihre Microservices zu verbinden, zu sichern und zu überwachen. NetScaler bietet zwei Lösungen, um Ihre Service-Mesh-Anforderungen zu erfüllen:

- Service Mesh Lite
- Service-Mesh (NetScaler Integration mit Istio)

Service Mesh Lite

Eine vollwertige Service-Mesh-Implementierung ist komplex und erfordert eine steile Lernkurve. Wenn Sie nach einer vereinfachten Implementierung eines Service Mesh mit ähnlichen Vorteilen suchen, bietet NetScaler eine Lösung namens Service Mesh Lite mit geringerer Komplexität. In dieser Lösung wird ein NetScaler CPX als zentralisierter Lastausgleichsdienst im Kubernetes-Cluster ausgeführt und der Lastenausgleich zwischen den Mikrodiensten erfolgt. NetScaler CPX setzt Richtlinien für eingehenden Datenverkehr und Datenverkehr zwischen Containern durch.

Das folgende Diagramm zeigt eine Service Mesh Lite-Architektur.



Weitere Informationen finden Sie in der Service Mesh Lite-Dokumentation.

Service-Mesh (NetScaler Integration mit Istio)

NetScaler bietet eine Service-Mesh-Lösung durch die Integration von NetScaler in Istio. Istio, ein plattformunabhängiges Open-Source-Service-Mesh, ist eine der beliebtesten Service-Mesh-Implementierungen. Durch die Integration von NetScaler in Istio können Sie die NetScaler-Funktionen nutzen, um den Datenverkehr für Anwendungen im Service Mesh zu sichern und zu optimieren.

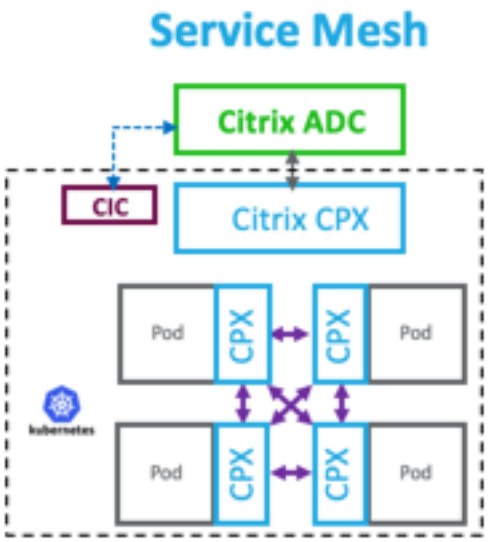
NetScaler kann auf folgende Weise in Istio integriert werden:

- NetScaler MPX, VPX oder CPX als Istio Ingress Gateway zum Service Mesh, um den Datenverkehr für den Kubernetes-Cluster verfügbar zu machen.

- NetScaler CPX als Sidecar-Proxy mit Anwendungscontainern im Service Mesh zur Steuerung der Kommunikation zwischen Anwendungen.

Sie können entweder die Integration unabhängig verwenden oder beide Methoden kombinieren, um eine einheitliche Datenebenenlösung zu erhalten.

Das folgende Diagramm zeigt eine Service Mesh-Architektur.



Service Mesh ist ideal für hochsichere Anwendungen und bietet außerdem die folgenden Vorteile.

- Bietet ein feinkörniges (modularisiertes) Verkehrsmanagement pro Container
- Sorgt dank Sidecar-Implementierung für umfassendere Beobachtbarkeit, Analytik und Sicherheit (Mutual TLS)
- Ermöglicht die automatische Bereitstellung von Canary für jeden Container mit eingebettetem NetScaler CPX
- Unterstützt Cloud-Portabilität
- Ermöglicht das Auslagern einiger der von Anwendungen ausgeführten Funktionen auf den Beiwagen
- Bietet geringere Seitenwagen Latenz
- Bietet Integrationen mit Open-Source-Tools
- Bietet Skalierbarkeit

Weitere Informationen finden Sie in der Dokumentation zu NetScaler Integration mit Istio.

Lösungen für die Beobachtbarkeit

May 11, 2023

In einer auf Microservices basierenden Architektur ist die Transparenz der Service-to-Service-Kommunikation entscheidend für den Aufbau einer effizienten und belastbaren Architektur. Herkömmliche Methoden zur Protokollierung und Überwachung sind nicht in der Lage, die Herausforderungen einer Microservice-Architektur zu bewältigen. Observability-Lösungen von Citrix bieten Ihnen die Möglichkeit, zu sehen, was passiert, wenn Ihre Dienste miteinander interagieren, und aussagekräftige Einblicke in Ihr System zu erhalten.

NetScaler bietet die folgenden Lösungen, um die Observability-Anforderungen Ihrer Microservices-Architektur zu erfüllen:

- NetScaler ADM Service Graph und Analytics
- NetScaler Observability Exporteur

NetScaler ADM Service Graph und Analytics

NetScaler Application Delivery Management (ADM) ist eine zentrale Verwaltungslösung, die unternehmensweite Transparenz und Automatisierung von Verwaltungsaufgaben bietet, die auf mehreren Instanzen ausgeführt werden müssen.

In einer Microservice-Architektur stellt die Fehlerbehebung eine Herausforderung dar, da sich eine einzelne Endbenutzeranforderung über mehrere Microservices erstrecken kann.

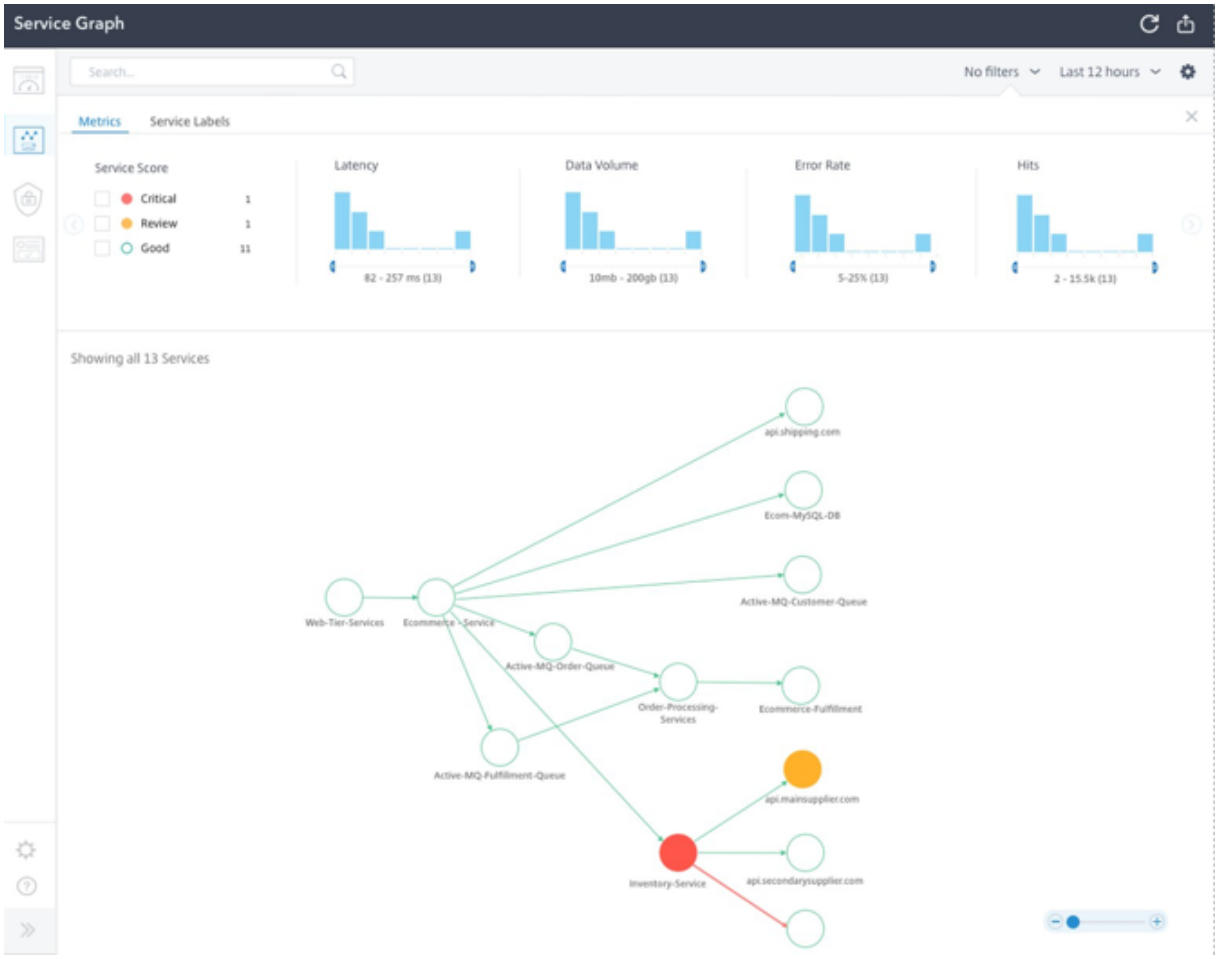
NetScaler ADM Service Graph and Analytics bieten Einblicke in Interaktionen zwischen Microservices und helfen bei der Identifizierung und Behebung von Problemen auf der Grundlage verschiedener Metriken wie Latenz und HTTP-Fehlern.

NetScaler ADM bietet auch erweiterte Analysen basierend auf Metriken und Transaktionsprotokollen, die von NetScaler erfasst wurden.

Die NetScaler ADM-Lösung bietet die folgenden Vorteile:

- Bietet eine zentrale Oberfläche für Anwendungen in Containern, on-premises oder in der Cloud
- Sorgt für bessere Beobachtbarkeit und schnellere Fehlerbehebung für Microservices
- Unterstützt Canary-Bereitstellungen

Das folgende Diagramm zeigt ein Beispiel für ein Servicediagramm für eine Anwendung, die mehrere Microservices enthält.



Weitere Informationen zum Einrichten von NetScaler ADM Service Graph and Analytics finden Sie in der Service Graph-Dokumentation .

NetScaler Observability Exporteur

NetScaler Observability Exporter ist ein Container, der Metriken und Transaktionen von NetScalern sammelt und sie in geeignete Formate (wie JSON, AVRO) für unterstützte Endgeräte umwandelt. Sie können die von NetScaler Observability Exporter gesammelten Daten zum gewünschten Endpunkt exportieren. Durch die Analyse der Daten können Sie wertvolle Erkenntnisse auf Microservices-Ebene für Anwendungen gewinnen, die von NetScalern als Proxy bereitgestellt werden.

Unterstützung für verteilte Verfolgung

Verteilte Tracer ermöglichen es Ihnen, den Datenfluss zwischen Ihren Microservices zu visualisieren und helfen, Engpässe in Ihrer Microservices-Architektur zu identifizieren. OpenTracing ist eine Spezifikation und ein Standardsatz von APIs zum Entwerfen und Implementieren von verteiltem Tracing.

NetScaler Observability Exporter implementiert die verteilte Ablaufverfolgung für NetScaler und unterstützt derzeit Zipkin als verteilten Tracer.

Sie können die Trace-Analyse verbessern, indem Sie Elasticsearch und Kibana mit Zipkin verwenden. Elasticsearch ermöglicht eine langfristige Aufbewahrung der Trace-Daten. Kibana ermöglicht Ihnen einen viel tieferen Einblick in die Daten, indem es ein Tool zur Untersuchung und Visualisierung von Protokollnachrichten bereitstellt.

Unterstützung für Transaktionssammlung und Streaming-Unterstützung

NetScaler Observability Exporter unterstützt das Sammeln von Transaktionen und das Streaming an Endpunkte. Derzeit unterstützt NetScaler Observability Exporter Elasticsearch und Kafka als Transaktionsendpunkte.

Weitere Informationen finden Sie in der NetScaler ObservabilityExporter-Dokumentation.

Aktivieren Sie Analysen mithilfe von Anmerkungen in der NetScaler Ingress Controller-YAML-Datei

Sie können Analysen mithilfe des Analyseprofils aktivieren, das in Ingress oder Service vom Typ LoadBalancer-Konfiguration als intelligente Annotation definiert ist. Sie können die spezifischen Parameter definieren, die Sie überwachen müssen, indem Sie sie in der Ingress- oder Dienstkonfiguration der Anwendung angeben. Weitere Informationen zum Aktivieren von Analysen mit Anmerkungen finden Sie unter Analytics mit Anmerkungen.

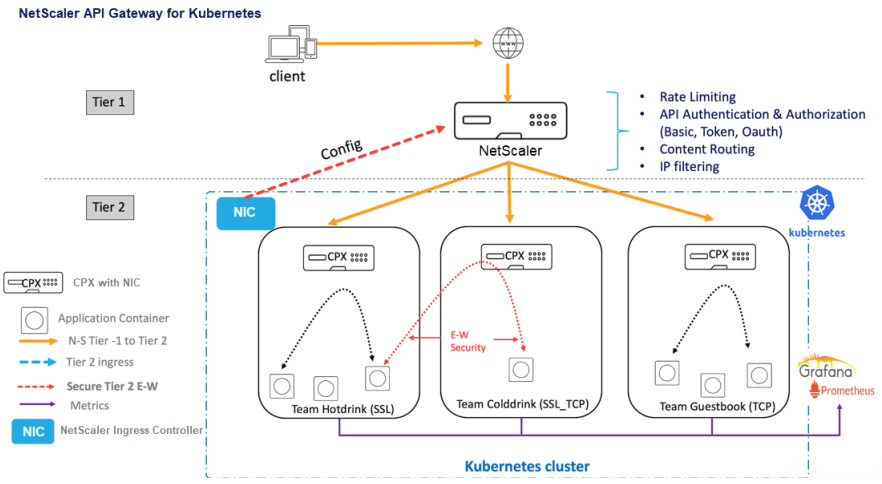
API-Gateway für Kubernetes

May 11, 2023

Ein API-Gateway dient als einziger Einstiegspunkt für Ihre APIs und gewährleistet einen sicheren und zuverlässigen Zugriff auf mehrere APIs und Microservices in Ihrem System.

NetScaler bietet ein API-Gateway der Enterprise-Klasse für den Nord-Süd-API-Traffic in den Kubernetes-Cluster. Das
API-Gateway lässt sich über den NetScaler Ingress Controller und den NetScaler (NetScaler MPX, VPX oder CPX), der als Ingress-Gateway für on-premises oder Cloud-Bereitstellungen eingesetzt wird, in Kubernetes integrieren.

Das folgende Diagramm zeigt eine Dual-Tier-Topologie für das API-Gateway.



Mit dem von Citrix angebotenen API-Gateway können Sie die folgenden Funktionen ausführen:

- Durchsetzung von Authentifizierungsrichtlinien
- Ratenlimit für Zugriff auf Dienste
- Erweitertes Inhaltsrouting
- Flexible und umfassende Transformation von HTTP-Transaktionen mithilfe der Rewrite- und Responder-Richtlinien
- Durchsetzung von Firewall-Richtlinien für Web

Wie funktioniert das API-Gateway?

Das API-Gateway basiert auf dem NetScaler Ingress Gateway und verwendet Kubernetes-API-Erweiterungen wie benutzerdefinierte Ressourcendefinitionen (CRDs). Mithilfe von CRDs können Sie das NetScaler und das API-Gateway automatisch in derselben Instanz konfigurieren.

NetScaler stellt die folgenden CRDs für das API-Gateway bereit:

- Auth CRD
- Ratenlimit CRD
- CRD für Inhaltsrouting
- Rewrite- und Responder-CRD
- WAF CRD

Hauptvorteile der Verwendung des API-Gateways

Im Folgenden werden die wichtigsten Vorteile des von Citrix angebotenen API-Gateway aufgeführt:

- Verwendet das erweiterte Verkehrsmanagement und die umfassenden Sicherheitsfunktionen von NetScaler.
- Optimiert Ihre Bereitstellungen, indem Sie mehrere Netzwerkfunktionen in einer einzigen Komponente des NetScaler Ingress Gateway konsolidieren.

- Reduziert die betriebliche Komplexität und die Kosten, die mit dem Einsatz mehrerer Komponenten verbunden sind.
- Sorgt für eine bessere Leistung Ihres Anwendungsdatenverkehrs, indem mehrere TCP- oder TLS-Entschlüsselungssprünge reduziert und gleichzeitig separate Komponenten verwendet werden.
- Vereinfacht die Bereitstellung und Integration in Ihre Kubernetes-Umgebungen, indem Sie entweder direkt YAMLs oder Helm-Charts verwenden.

Bereitstellung des API-Gateways

Weitere Informationen zur Konfiguration der API-Gateway-Funktionen mithilfe von CRDs finden Sie in der NetScaler Ingress Controller-Dokumentation:

- Authentifizierung
- Ratenlimit
- Erweitertes Inhaltsrouting
- Rewrite- und Responder-Richtlinien
- Firewallrichtlinien für Webanwendungen

Verwenden Sie NetScaler ADM, um Probleme mit NetScaler Cloud Native Networking zu beheben

May 11, 2023

Übersicht

Dieses Dokument enthält Informationen darüber, wie Sie NetScaler ADM verwenden können, um Kubernetes-Microservice-Anwendungen bereitzustellen und zu überwachen. Sie beschäftigen sich auch mit der Verwendung der CLI, der Dienstdiagramme und der Ablaufverfolgung, damit die Plattform- und SRE-Teams Probleme beheben können.

Überblick über Anwendungsleistung und Latenz

TLS-Verschlüsselung

TLS ist ein Verschlüsselungsprotokoll zur Sicherung der Internetkommunikation. Ein TLS-Handshake ist der Prozess, der eine Kommunikationssitzung startet, die TLS-Verschlüsselung verwendet. Während eines TLS-Handshakes tauschen die beiden kommunizierenden Seiten Nachrichten aus, um sich gegenseitig zu bestätigen, sich gegenseitig zu verifizieren, die von ihnen verwendeten

Verschlüsselungsalgorithmen festzulegen und Sitzungsschlüssel zu vereinbaren. TLS-Handshakes sind ein grundlegender Bestandteil der Funktionsweise von HTTPS.

TLS im Vergleich zu SSL-Handshakes

SSL (Secure Sockets Layer) war das ursprüngliche Verschlüsselungsprotokoll, das für HTTP entwickelt wurde. TLS (Transport Layer Security) hat SSL vor einiger Zeit ersetzt. SSL-Handshakes werden jetzt TLS-Handshakes genannt, obwohl der Name "SSL" immer noch weit verbreitet ist.

Wann findet ein TLS-Handshake statt?

Ein TLS-Handshake findet immer dann statt, wenn ein Benutzer über HTTPS zu einer Website navigiert und der Browser zuerst den Original-Server der Website abfragt. Ein TLS-Handshake findet auch dann statt, wenn andere Kommunikationen HTTPS verwenden, einschließlich API-Aufrufe und DNS-über-HTTPS-Abfragen.

TLS-Handshakes treten auf, nachdem eine TCP-Verbindung über einen TCP-Handshake geöffnet wurde.

Was passiert während eines TLS-Handshakes?

- Während eines TLS-Handshakes führen der Client und der Server zusammen Folgendes aus:
  - Geben Sie an, welche Version von TLS (TLS 1.0, 1.2, 1.3 usw.) sie verwenden.
  - Entscheiden Sie, welche Verschlüsselungssammlungen (siehe folgenden Abschnitt) sie verwenden.
  - Authentifizieren Sie die Identität des Servers über den öffentlichen Schlüssel des Servers und die digitale Signatur der SSL-Zertifizierungsstelle.
  - Generieren Sie Sitzungsschlüssel, um die symmetrische Verschlüsselung zu verwenden, nachdem der Handshake abgeschlossen ist.

Was sind die Schritte eines TLS-Handshakes?

- TLS-Handshakes sind eine Reihe von Datagrammen oder Nachrichten, die von einem Client und einem Server ausgetauscht werden. Ein TLS-Handshake umfasst mehrere Schritte, da der Client und der Server die Informationen austauschen, die für den Abschluss des Handshakes und die Ermöglichung weiterer Konversationen erforderlich sind.

Die genauen Schritte innerhalb eines TLS-Handshakes variieren je nach Art des verwendeten Schlüsselaustauschalgorithmus und den von beiden Seiten unterstützten Verschlüsselungssammlungen. Der RSA-Schlüsselaustauschalgorithmus wird am häufigsten verwendet. Es geht wie folgt:

1. Die 'Client-Hallo'-Nachricht: Der Client initiiert den Handshake, indem er eine "Hallo" -Nachricht an den Server sendet. Die Meldung enthält, welche TLS-Version der Client unterstützt, welche Verschlüsselungssammlungen unterstützt werden und eine Reihe von zufälligen Bytes, die als "client random" bezeichnet werden.
2. Die "Server-Hallo" -Meldung: Als Antwort auf die Hello-Nachricht des Clients sendet der Server eine Nachricht mit dem SSL-Zertifikat des Servers, der vom Server ausgewählten Verschlüs-

selungssammlung und dem “zufälligen Server”, einer weiteren zufälligen Bytefolge, die vom Server generiert wird.

3. Authentifizierung: Der Client überprüft das SSL-Zertifikat des Servers bei der Zertifizierungsstelle, die es ausgestellt hat. Dies bestätigt, dass der Server der ist, für den er sich ausgibt, und dass der Client mit dem tatsächlichen Eigentümer der Domäne interagiert.
4. Das Premaster-Secret: Der Client sendet eine weitere zufällige Bytefolge, das “premaster secret”. Das Premaster-Secret ist mit dem öffentlichen Schlüssel verschlüsselt und kann nur mit dem privaten Schlüssel vom Server entschlüsselt werden. (Der Client erhält den öffentlichen Schlüssel aus dem SSL-Zertifikat des Servers.)
5. Verwendeter privater Schlüssel: Der Server entschlüsselt das Premaster-Secret.
6. Sitzungsschlüssel erstellt: Sowohl der Client als auch der Server generieren Sitzungsschlüssel aus dem zufälligen Client, dem zufälligen Server und dem Premaster-Secret. Sie sollten zu den gleichen Ergebnissen kommen.
7. Der Client ist bereit: Der Client sendet eine “fertige” Nachricht, die mit einem Sitzungsschlüssel verschlüsselt ist.
8. Server ist bereit: Der Server sendet eine “fertige” Nachricht, die mit einem Sitzungsschlüssel verschlüsselt ist.
9. Sichere symmetrische Verschlüsselung erreicht: Der Handshake ist abgeschlossen und die Kommunikation wird unter Verwendung der Sitzungsschlüssel fortgesetzt.

Alle TLS-Handshakes verwenden eine asymmetrische Verschlüsselung (den öffentlichen und privaten Schlüssel), aber nicht alle verwenden den privaten Schlüssel beim Generieren von Sitzungsschlüsseln. Ein kurzlebiger Diffie-Hellman-Handschlag läuft beispielsweise wie folgt ab:

1. Client-Hallo: Der Client sendet eine Client-Hello-Nachricht mit der Protokollversion, dem zufälligen Client und einer Liste von Verschlüsselungssammlungen.
2. Server-Hallo: Der Server antwortet mit seinem SSL-Zertifikat, seiner ausgewählten Verschlüsselungssammlung und dem Server zufällig. Im Gegensatz zu dem im vorherigen Abschnitt beschriebenen RSA-Handshake enthält der Server in dieser Nachricht auch Folgendes (Schritt 3).
3. Digitale Signatur des Servers: Der Server verwendet seinen privaten Schlüssel, um den Client zufällig, den Server zufällig und seinen DH-Parameter* zu verschlüsseln. Diese verschlüsselten Daten fungieren als digitale Signatur des Servers und stellen fest, dass der Server über den privaten Schlüssel verfügt, der mit dem öffentlichen Schlüssel aus dem SSL-Zertifikat übereinstimmt.
4. Digitale Signatur bestätigt: Der Client entschlüsselt die digitale Signatur des Servers mit dem öffentlichen Schlüssel und überprüft, ob der Server den privaten Schlüssel kontrolliert und wer er vorgibt zu sein. Client-DH-Parameter: Der Client sendet seinen DH-Parameter an den Server.
5. Client und Server berechnen das Premaster-Secret: Anstatt dass der Client das Premaster-Secret generiert und an den Server sendet, wie bei einem RSA-Handshake, verwenden der

Client und der Server die ausgetauschten DH-Parameter, um ein passendes Premaster-Secret separat zu berechnen.

6. Sitzungsschlüssel erstellt: Jetzt berechnen der Client und der Server Sitzungsschlüssel aus dem Premaster-Secret, dem Client zufällig und dem Server zufällig, genau wie bei einem RSA-Handshake.

    - **Der Kunde ist bereit** Wie ein RSA-Handshake
    - Server ist bereit
    - Sichere symmetrische Verschlüsselung erreicht

    *DH-Parameter: DH steht für Diffie-Hellman. Der Diffie-Hellman-Algorithmus verwendet Exponentialberechnungen, um zum selben Premaster-Secret zu gelangen. Der Server und der Client stellen jeweils einen Parameter für die Berechnung bereit, und wenn sie kombiniert werden, führen sie zu einer anderen Berechnung auf jeder Seite, wobei die Ergebnisse gleich sind.

Weitere Informationen zum Kontrast zwischen kurzlebigen Diffie-Hellman-Handshakes und anderen Arten von Handshakes und wie sie eine Vorwärtsgeheimnis erreichen, finden Sie in dieser TLS-Protokolldokumentation.

Was ist eine Verschlüsselungssammlung?

- Eine Verschlüsselungssuite ist eine Reihe von Verschlüsselungsalgorithmen, die beim Aufbau einer sicheren Kommunikationsverbindung verwendet werden. (Ein Verschlüsselungsalgorithmus ist eine Reihe mathematischer Operationen, die an Daten ausgeführt werden, um die Daten zufällig erscheinen zu lassen.) Es gibt verschiedene Verschlüsselungssammlungen, die weit verbreitet sind, und ein wesentlicher Bestandteil des TLS-Handshakes ist die Vereinbarung, welche Verschlüsselungssammlung für diesen Handshake verwendet wird.

Für die ersten Schritte siehe Referenz: TLS-Protokolldokumentation.

NetScaler Application Delivery Management SSL-Dashboard

NetScaler Application Delivery Management (ADM) optimiert jetzt jeden Aspekt der Zertifikatsverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und korrekte Algorithmen sicherzustellen, während Sie nicht verwendete oder bald ablaufende Zertifikate im Auge behalten. Um mit der Verwendung des NetScaler ADM SSL-Dashboards und seiner Funktionen beginnen zu können, müssen Sie wissen, was ein SSL-Zertifikat ist und wie Sie NetScaler ADM verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Ein SSL-Zertifikat (Secure Socket Layer), das Teil einer SSL-Transaktion ist, ist ein digitales Eingabeformular (X509), das ein Unternehmen (Domain) oder eine Person identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit

dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der Citrix Application Delivery Controller (ADC) -Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung des asymmetrischen Schlüssels (oder des öffentlichen Schlüssels) abzuschließen.

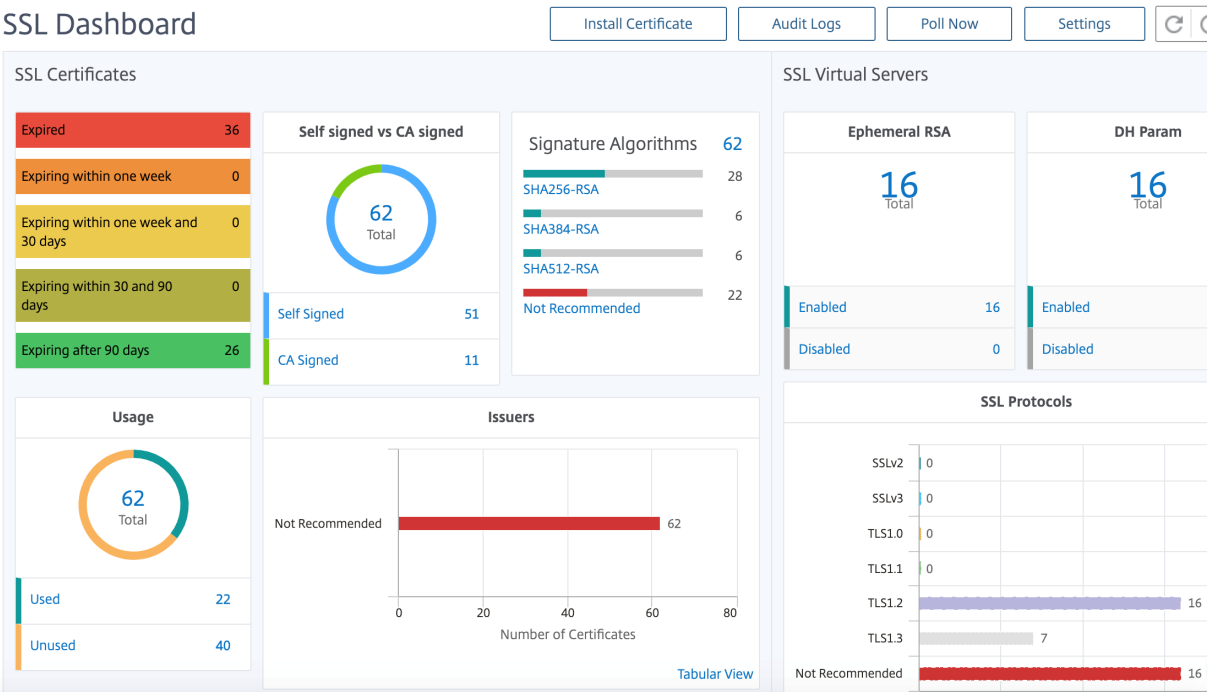
Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

- Von einer autorisierten Zertifizierungsstelle (CA)
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der NetScaler-Appliance

NetScaler ADM bietet eine zentrale Ansicht der in allen verwalteten NetScaler-Instanzen installierten SSL-Zertifikate. Im SSL-Dashboard können Sie Diagramme anzeigen, mit denen Sie Zertifikataussteller, wichtige Stärken, Signaturalgorithmen, abgelaufene oder nicht verwendete Zertifikate usw. nachverfolgen können. Sie können auch die Verteilung der SSL-Protokolle sehen, die auf Ihren virtuellen Servern ausgeführt werden, und die Schlüssel, die auf ihnen aktiviert sind.

Sie können auch Benachrichtigungen einrichten, um Sie darüber zu informieren, wann Zertifikate ablaufen werden, und Informationen darüber enthalten, welche NetScaler-Instanzen diese Zertifikate verwenden.

Sie können die Zertifikate einer NetScaler Instanz mit einem Zertifizierungsstellenzertifikat verknüpfen. Stellen Sie jedoch sicher, dass die Zertifikate, die Sie mit demselben CA-Zertifikat verknüpfen, dieselbe Quelle und denselben Aussteller haben. Nachdem Sie die Zertifikate mit einem CA-Zertifikat verknüpft haben, können Sie die Verknüpfung aufheben.



Um loszulegen, lesen Sie die SSL-Dashboard-Dokumentation.

Integrationen von Drittanbietern

Die Anwendungslatenz wird in Millisekunden gemessen und kann je nach verwendeter Metrik eines von zwei Dingen anzeigen. Die gebräuchlichere Methode zur Messung der Latenz wird als “Round-Trip-Zeit” (oder RTT) bezeichnet. RTT berechnet die Zeit, die ein Datenpaket benötigt, um im Netzwerk von einem Punkt zum anderen zu gelangen und eine Antwort an die Quelle zurückzusenden. Die andere Messung wird als “Time to First Byte” (oder TTFB) bezeichnet und zeichnet die Zeit auf, die vom Zeitpunkt, an dem ein Paket einen Punkt im Netzwerk verlässt, bis zu dem Moment, zu dem es an seinem Ziel ankommt, benötigt wird. RTT wird häufiger zur Messung der Latenz verwendet, da es von einem einzigen Punkt im Netzwerk aus ausgeführt werden kann und keine Datenerfassungssoftware auf dem Zielpunkt installiert werden muss (wie dies bei TTFB der Fall ist).

Durch die Überwachung der Bandbreitennutzung und -leistung Ihrer Anwendung in Echtzeit erleichtert der ADM-Dienst die Identifizierung von Problemen und die vorbeugende Behandlung potenzieller Probleme, bevor sie sich manifestieren und Benutzer in Ihrem Netzwerk betreffen. Diese Flow-basierte Lösung verfolgt die Nutzung nach Schnittstelle, Anwendung und Konversation und liefert Ihnen detaillierte Informationen zu Aktivitäten in Ihrem Netzwerk.

Verwenden von Splunk-Tools

Infrastruktur und Anwendungsleistung sind voneinander abhängig. Um das vollständige Bild zu sehen, bietet SignalFX eine nahtlose Korrelation zwischen der Cloud-Infrastruktur und den darauf laufenden Microservices. Wenn Ihre Anwendung aufgrund von Speicherverlust, einem verrauschten Nachbarcontainer oder einem anderen infrastrukturbezogenen Problem auftritt, informiert SignalFX Sie darüber. Um das Bild zu vervollständigen, ermöglicht der kontextbezogene Zugriff auf Splunk-Protokolle und -Ereignisse eine tiefere Fehlerbehebung und Ursachenanalyse.

Weitere Informationen zu SignalFX Microservices APM und zur Fehlerbehebung mit Splunk finden Sie unter Splunk für DevOps-Informationen .

MongoDB-Unterstützung

MongoDB speichert Daten in flexiblen, JSON-ähnlichen Dokumenten. Bedeutungsfelder können von Dokument zu Dokument variieren und die Datenstruktur kann im Laufe der Zeit geändert werden.

Das Dokumentmodell wird den Objekten in Ihrem Anwendungscode zugeordnet, sodass Sie problemlos mit Daten arbeiten können.

On-Demand-Abfragen, Indizierung und Echtzeitaggregation bieten leistungsstarke Möglichkeiten, auf Ihre Daten zuzugreifen und sie zu analysieren.

MongoDB ist im Kern eine verteilte Datenbank, sodass Hochverfügbarkeit, horizontale Skalierung und geografische Verteilung integriert und einfach zu bedienen sind.

MongoDB wurde entwickelt, um die Anforderungen moderner Apps mit einer technologischen Grundlage zu erfüllen, die Ihnen Folgendes ermöglicht:

- Das Dokumentdatenmodell — das Ihnen die beste Art bietet, mit Daten zu arbeiten.
- Ein Design verteilter Systeme, mit dem Sie Daten intelligent dort ablegen können, wo Sie sie haben möchten.
- Ein einheitliches Erlebnis, das Ihnen die Freiheit gibt, überall zu arbeiten, sodass Sie Ihre Arbeit zukunftssicher machen und die Anbieterbindung vermeiden können.

Mit diesen Funktionen können Sie eine Intelligent Operational Data Platform aufbauen, die von MongoDB unterstützt wird. Weitere Informationen finden Sie in der MongoDB-Dokumentation.

Lastenausgleich für eingehenden Datenverkehr zu TCP- oder UDP-basierten Anwendungen

In einer Kubernetes-Umgebung ist ein Ingress ein Objekt, das den Zugriff auf die Kubernetes-Dienste von außerhalb des Kubernetes-Clusters ermöglicht. Bei Standard-Kubernetes Ingress-Ressourcen wird davon ausgegangen, dass der gesamte Datenverkehr HTTP-basiert ist und keine nicht-HTTP-basierten Protokolle wie TCP, TCP-SSL und UDP unterstützt. Daher können kritische Anwendungen, die auf L7-Protokollen wie DNS, FTP, LDAP basieren, nicht mit Standard-Kubernetes Ingress verfügbar gemacht werden.

Die Kubernetes-Standardlösung besteht darin, einen Dienst vom Typ LoadBalancer zu erstellen. Weitere Informationen finden Sie unter Service Type LoadBalancer in NetScaler .

Die zweite Option besteht darin, das Eingangsobjekt mit Anmerkungen zu versehen. Mit dem NetScaler Ingress Controller können Sie den Lastausgleich von TCP- oder UDP-basiertem Ingress-Verkehr durchführen. Es enthält die folgenden Anmerkungen, die Sie in Ihrer Kubernetes Ingress-Ressourcendefinition verwenden können, um den TCP- oder UDP-basierten Ingress-Datenverkehr zu belasten:

- ingress.citrix.com/insecure-service-type: Die Annotation ermöglicht den L4-Lastausgleich mit TCP, UDP oder ANY als Protokoll für NetScaler.
- ingress.citrix.com/insecure-port: Die Annotation konfiguriert den TCP-Port. Die Anmerkung ist hilfreich, wenn Micro-Service-Zugriff an einem nicht standardmäßigen Port erforderlich ist. Standardmäßig ist Port 80 konfiguriert.

Weitere Informationen finden Sie unter Load Balancing von eingehendem Datenverkehr zu TCP- oder UDP-basierten Anwendungen.

Überwachen und verbessern Sie die Leistung Ihrer TCP- oder UDP-basierten Anwendungen

Anwendungsentwickler können den Zustand von TCP- oder UDP-basierten Anwendungen über umfangreiche Monitore (wie TCP-ECV, UDP-ECV) in NetScaler genau überwachen. Die ECV-Monitore (Extended Content Validation) helfen bei der Überprüfung, ob die Anwendung erwarteten Inhalt zurückgibt oder nicht.

Die Anwendungsleistung kann auch verbessert werden, indem Persistenzmethoden wie Quell-IP verwendet werden. Sie können diese NetScaler-Funktionen über Smart Annotations in Kubernetes verwenden. Das Folgende ist ein Beispiel:

```
1 apiVersion: extensions/v1beta1
2 kind: Ingress
3 metadata:
4     name: mongodb
```



```
5     annotations:
6         ingress.citrix.com/insecure-port:  “80”
7         ingress.citrix.com/frontend-ip:  “192.168.1.1”
8         ingress.citrix.com/csvserver:  ‘{
9   “l2conn” :” on”  }
10  ’
11        ingress.citrix.com/lbvserver:  ‘{
12  “mongodb-svc” :{
13  “lbmethod” :” SRCIPDESTIPHASH”  }
14  }
15  ’
16        ingress.citrix.com/monitor:  ‘{
17  “mongodbsvc” :{
18  “type” :” tcp-ecv”  }
19  }
20  ’
21 Spec:
22     rules:
23     - host: mongodb.beverages.com
24       http:
25         paths:
26         - path: /
27           backend:
28             serviceName: mongodb-svc
29             servicePort: 80
30 <!--NeedCopy-->
```

NetScaler Application Delivery Management (ADM) -Dienst

Der NetScaler ADM-Dienst bietet die folgenden Vorteile:

- **Agilität** — Einfach zu bedienen, zu aktualisieren und zu verwenden. Das Servicemodell des NetScaler ADM Service ist über die Cloud verfügbar, sodass die bereitgestellten Funktionen einfach zu bedienen, zu aktualisieren und zu verwenden sind. Die Häufigkeit von Updates in Kombination mit der automatischen Update-Funktion verbessert die NetScaler Bereitstellung schnell.
- **Schnellere Wertschöpfung** — Schnellere Erreichung der Geschäftsziele. Im Gegensatz zur herkömmlichen on-premises Bereitstellung können Sie Ihren NetScaler ADM-Dienst mit wenigen Klicks verwenden. Sie sparen nicht nur Installations- und Konfigurationszeit, sondern verschwenden auch Zeit und Ressourcen für potenzielle Fehler.
- **Verwaltung mehrerer Standorte** — Single Pane of Glass für Instanzen in Rechenzentren mit mehreren Standorten. Mit dem NetScaler ADM Service können Sie NetScaler verwalten und überwachen, die sich in verschiedenen Bereitstellungstypen befinden. Sie haben eine zentrale Verwaltung für NetScaler, die on-premises und in der Cloud bereitgestellt werden.

- **Betriebseffizienz** — Optimierte und automatisierte Methode zur Erzielung höherer Betriebsproduktivität. Mit dem NetScaler ADM Service werden Ihre Betriebskosten reduziert, indem Sie Zeit, Geld und Ressourcen bei der Wartung und Aktualisierung der herkömmlichen Hardwarebereitstellungen sparen.

Service-Diagramm für Kubernetes-Anwendungen

Mit dem Service-Diagramm für die Cloud-native Anwendungsfunktion in NetScaler ADM können Sie:

- Sicherstellung der Gesamtleistung der Anwendung durch End-to-End-Anwendung
- Identifizieren Sie Engpässe, die durch die gegenseitige Abhängigkeit verschiedener Komponenten Ihrer Anwendungen entstehen
- Sammeln Sie Einblicke in die Abhängigkeiten der verschiedenen Komponenten Ihrer Anwendungen
- Überwachen Sie Dienste innerhalb des Kubernetes-Clusters
- Überwachen Sie, welcher Dienst Probleme hat
- Prüfen Sie die Faktoren, die zu Leistungsproblemen beitragen
- Detaillierte Sichtbarkeit der HTTP-Transaktionen des Dienstes anzeigen
- Analysieren der HTTP-, TCP- und SSL-Metriken

Durch die Visualisierung dieser Metriken in NetScaler ADM können Sie die Ursache von Problemen analysieren und die erforderlichen Fehlerbehebungsaktionen schneller durchführen. Service Graph zeigt Ihre Anwendungen in verschiedenen Komponentendiensten an. Diese Dienste, die innerhalb des Kubernetes-Clusters ausgeführt werden, können mit verschiedenen Komponenten innerhalb und außerhalb der Anwendung kommunizieren.

Informationen zu den ersten Schritten finden Sie unter Service Graph einrichten.

Service-Diagramm für dreistufige Webanwendungen

Mit der Service Graph-Funktion aus dem Anwendungs-Dashboard können Sie Folgendes anzeigen:

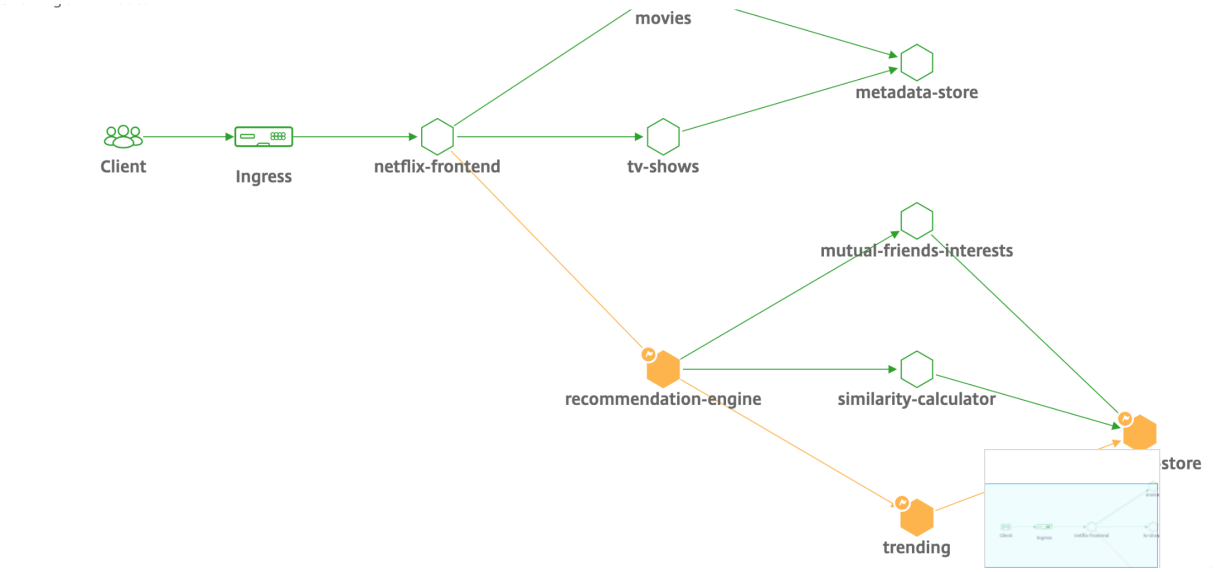
- Details zur Konfiguration der Anwendung (mit dem virtueller Content Switching-Server und dem virtuellen Load Balancing-Server)
  - Für GSLB-Anwendungen können Sie Rechenzentrum, ADC-Instanz, virtuelle CS- und LB-Server anzeigen
- Ende-zu-Ende-Transaktionen vom Kunden zum Service
- Der Ort, von dem aus der Client auf die Anwendung zugreift
- Der Name des Rechenzentrums, in dem die Clientanforderungen verarbeitet werden, und die zugehörigen NetScaler-Metriken des Rechenzentrums (nur für GSLB-Anwendungen)
- Metrikdetails für Client, Service und virtuelle Server
- Wenn die Fehler vom Kunden oder vom Dienst stammen

- Der Dienststatus wie “ **Kritisch**”, “ **Überprüfung**” und “ **Gut**”. NetScaler ADM zeigt den Dienststatus basierend auf der Reaktionszeit des Dienstes und der Fehleranzahl an.
  - **Kritisch (rot)** — Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms UND Fehlerzähler > 0
  - **Überprüfung (orange)** — Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** — Zeigt keinen Fehler an und durchschnittliche Reaktionszeit < 200 ms
- Der Kundenstatus wie “ **Kritisch**”, “ **Überprüfung**” und “ **Gut**”. NetScaler ADM zeigt den Clientstatus basierend auf der Latenz des Clientnetzwerks und der Fehleranzahl an.
  - **Kritisch (rot)**— Zeigt an, wenn die durchschnittliche Netzwerklatenz des Clients > 200 ms UND Fehleranzahl > 0
  - **Überprüfung (orange)** — Zeigt an, wenn die durchschnittliche Clientnetzwerklatenz > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** — Zeigt keinen Fehler an und durchschnittliche Latenz des Client-Netzwerks < 200 ms
- Der Status des virtuellen Servers wie “ **Kritisch**”, “ **Überprüfung**” und “ **Gut**”. NetScaler ADM zeigt den Status des virtuellen Servers basierend auf dem App-Score an.
  - **Kritisch (rot)** — Zeigt an, wenn der App-Wert < 40 ist
  - **Überprüfung (orange)** — Zeigt an, wenn der App-Score zwischen 40 und 75 liegt
  - **Gut (grün)** — Zeigt an, wenn der App-Score > 75 ist

Zu beachtende Punkte:

- Im Service-Diagramm werden nur Load Balancing, Content Switching und virtuelle GSLB-Server angezeigt.
- Wenn kein virtueller Server an eine benutzerdefinierte Anwendung gebunden ist, sind die Details im Service-Diagramm für die Anwendung nicht sichtbar.
- Sie können Metriken für Clients und Services im Service-Diagramm nur anzeigen, wenn aktive Transaktionen zwischen virtuellen Servern und Webanwendung stattfinden.
- Wenn keine aktiven Transaktionen zwischen virtuellen Servern und der Webanwendung verfügbar sind, können Sie Details im Service-Diagramm nur basierend auf den Konfigurationsdaten wie Load Balancing, Content Switching, virtuelle GSLB-Server und Dienste anzeigen.
- Es kann 10 Minuten dauern, bis Aktualisierungen in der Anwendungskonfiguration im Service-Diagramm angezeigt werden.

Weitere Informationen finden Sie unter Service-Diagramm für Anwendungen.



Informationen zum Einstieg finden Sie in der Service Graph-Dokumentation.

Fehlerbehebung für NetScaler-Teams

Lassen Sie uns einige der häufigsten Attribute für die Fehlerbehebung bei der NetScaler-Plattform besprechen und wie diese Techniken zur Fehlerbehebung auf die Tier-1-Bereitstellungen für Microservices-Topologien angewendet werden.

Der NetScaler verfügt über eine Befehlszeilenschnittstelle (CLI), die Befehle in Echtzeit anzeigt und zum Bestimmen von Laufzeitkonfigurationen, Statik und Richtlinienkonfiguration nützlich ist. Dies wird über den Befehl **“SHOW”** erleichtert.

SHOW - ADC-CLI-Operationen ausführen:

```
>Show running config (-summary -fullValues)

 Ability to search (grep command)
> “sh running config | -i grep vserver”

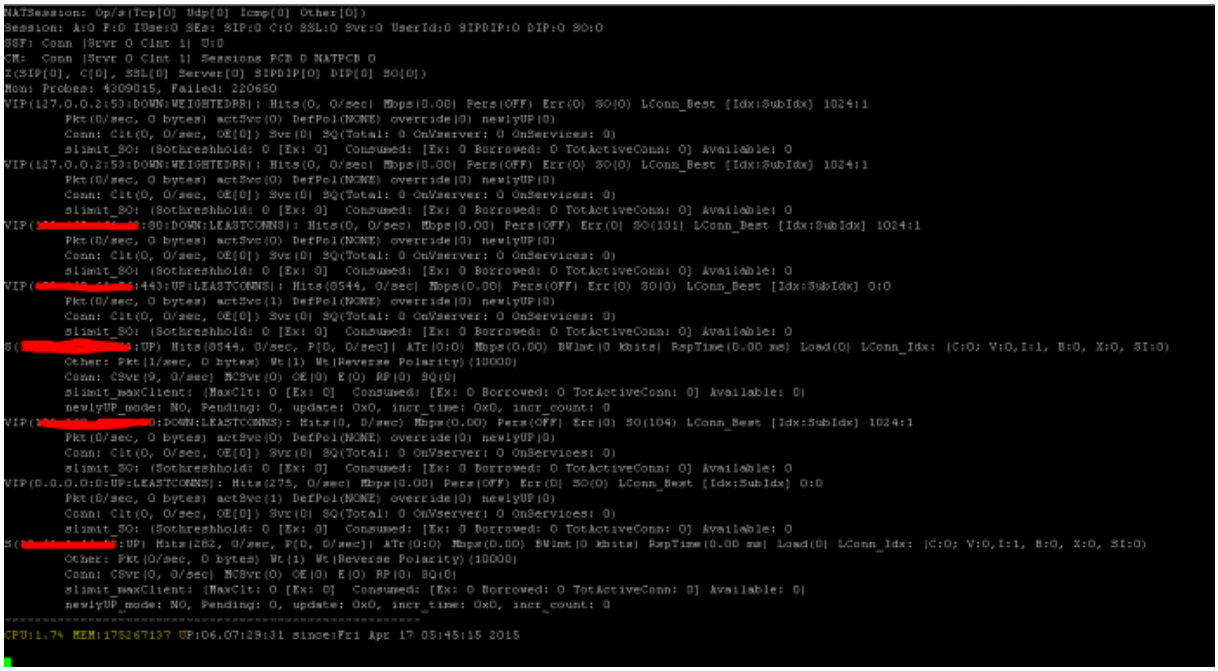
Check the version.
>Show license
   “sh license"
<!--NeedCopy-->
```

SSL Statistiken anzeigen

```
>Sh ssl
        System
        Frontend
        Backend
```



```
5           Encryption
6  <!--NeedCopy-->
```



Der NetScaler verfügt über einen Befehl zum Aufzählen von Statistiken für alle Objekte basierend auf einem Zählerintervall von sieben (7) Sekunden. Dies wird über den Befehl **“STAT”** erleichtert.

Hochgranulare L3-L7-Telemetrie von NetScaler

- Systemebene: CPU- und Speicherauslastung von ADC.
- HTTP-Protokoll: #Requests /Responses, GET/POST Split, HTTP-Fehler für N-S und E-W (nur für Service Mesh Lite, Sidecar bald).
- SSL: #Sessions und #Handshakes nur für N-S- und E-W-Verkehr für Service Mesh Lite.
- IP-Protokoll: #Packets empfangen/gesendet, #Bytes empfangen/gesendet, #Truncated -Pakete und #IP Adresssuche.
- NetScaler AAA: #Active -Sitzungen
- Schnittstelle: #Total Multicast-Pakete, #Total übertragene Bytes und #Jumbo -Pakete empfangen/gesendet.
- Virtueller Lastenausgleichsserver und virtueller Content Switching-Server: #Packets, #Hits und #Bytes empfangen/gesendet.

STAT - ADC-CLI-Operationen ausführen:

```
1  >Statistics
2   “stat ssl”
3  <!--NeedCopy-->
```



```
> stat ns

System overview

Up since        Thu Apr 16 19:45:15 2015
Packet CPU usage (%)                1.60
Management CPU usage (%)            0.80
Memory usage (MB)                    165
InUse Memory (%)                   17.03
Last Transition time Th...015
System state                         UP
Master state                    Primary
# SSL cards UP                         0
# SSL cards present                    0

System Disks                   Used (%) Available
/flash Used (%)                       17      1168
/var Used (%)                         13     11246

Throughput Statistics                    Rate (/s)               Total
Megabits received                                2                288237
Megabits transmitted                             3                345685

TCP Connections                  Client   Server
All client connections              158      272
Established client connections      158      145

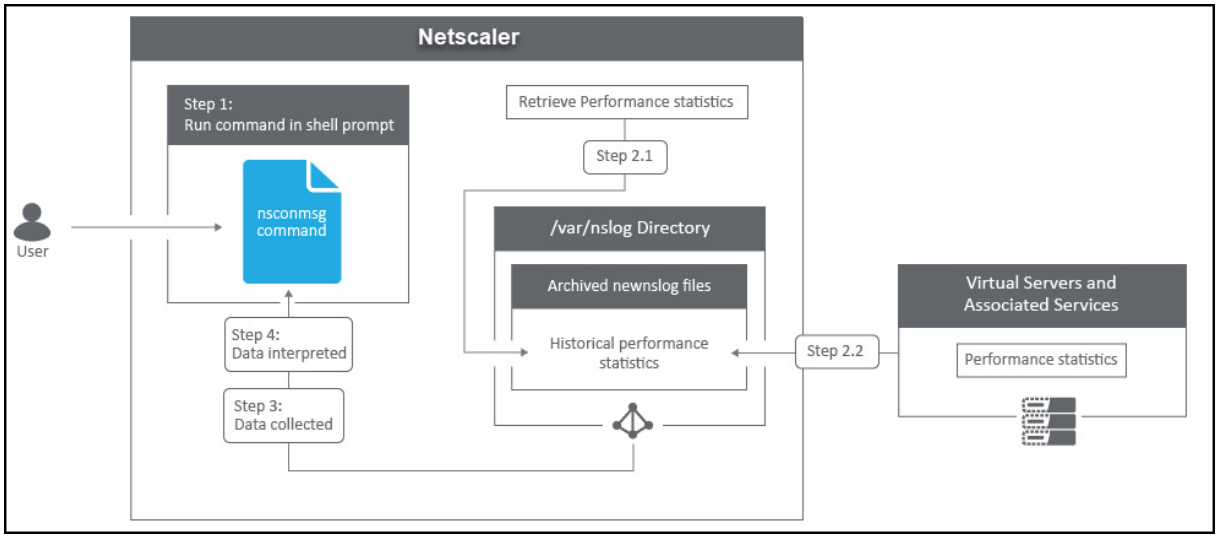
HTTP                                     Rate (/s)               Total
Total requests                                   0                191529
Total responses                                  0                263011
Request bytes received                        7007           1178810535
Response bytes received                     164477          12348432171

SSL                                      Rate (/s)               Total
```

Der NetScaler verfügt über eine Protokollarchivstruktur, die das Durchsuchen von Statistiken und Leistungsindikatoren bei der Behandlung bestimmter Fehler über den Befehl **“NSCONMSG”** ermöglicht.

NSCONMSG - Haupt-Protokolldatei (NS-Datenformat)

```
1      Cd/var/nslog
2
3       “Mac Moves”
4      nsconmsg -d current -g nic_err
5  <!--NeedCopy-->
```

Nstcpdump

Sie können `nstcpdump` für die Fehlerbehebung auf niedriger Ebene verwenden. `nstcpdump` sammelt weniger detaillierte Informationen als `nstrace`. Öffnen Sie die ADC-CLI und geben Sie ein `shell`. Sie können Filter mit verwenden `nstcpdump`, aber keine für ADC-Ressourcen spezifischen Filter verwenden. Die Dump-Ausgabe kann direkt im CLI-Bildschirm angezeigt werden.

CTRL + C — Drücken Sie diese Tasten gleichzeitig, um eine zu stoppen `nstcpdump`.

`nstcpdump.sh dst host x.x.x.x` — Zeigt den an den Zielhost gesendeten Datenverkehr an.

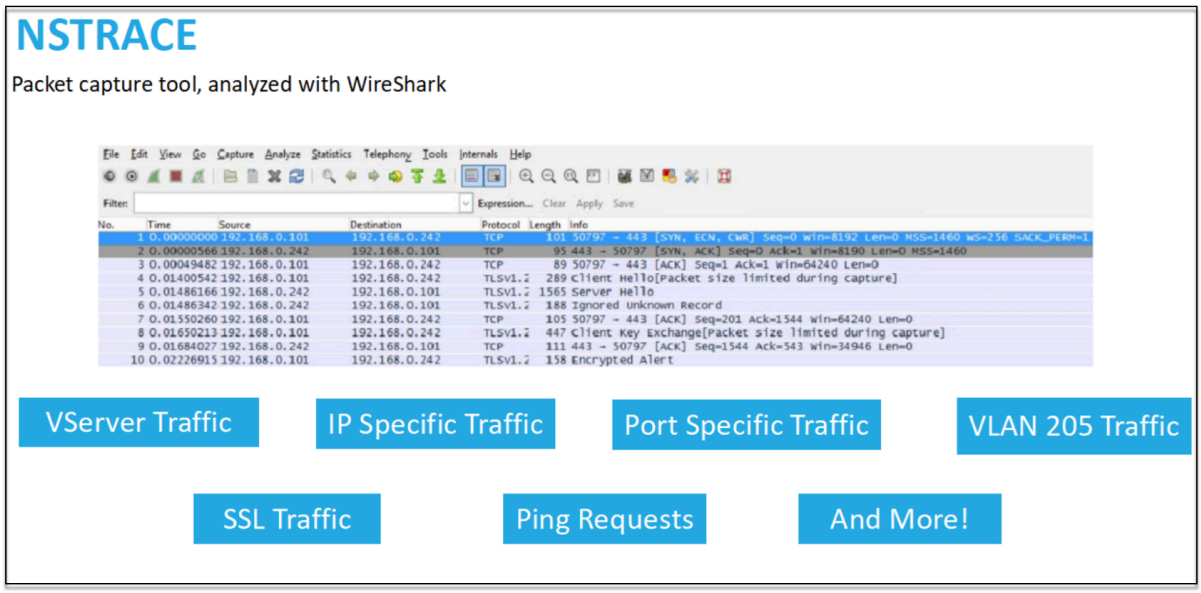
`nstcpdump.sh -n src host x.x.x.x` — Zeigt den Datenverkehr vom angegebenen Host an und wandelt keine IP-Adressen in Namen um (-n).

`nstcpdump.sh host x.x.x.x` — Zeigt den Datenverkehr zu und von der angegebenen Host-IP an.


```
root@Netscaler1# nstcpdump.sh -c 10 dst host 192.168.0.242
reading from file -, link-type EN10MB (Ethernet)
21:45:45.834700 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [S], seq 1702255264, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK],
length 0
21:45:45.836702 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 748367253, win 64240, length 0
21:45:45.837202 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 1, win 64240, length 232
21:45:45.839203 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 1544, win 64240, length 0
21:45:45.840244 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 1544, win 64240, length 342
21:45:45.847709 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 1619, win 64165, length 469
21:45:45.994744 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [P.], ack 2712, win 63072, length 581
21:45:46.002746 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 7092, win 64240, length 0
21:45:46.003250 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 15853, win 64240, length 0
21:45:46.009748 IP 192.168.0.11.62477 > citrixstore.citrixpro.co.uk.https: Flags
 [.], ack 30455, win 64240, length 0
```

NSTRACE - Paket-Trace-Datei

NSTRACE ist ein Paket-Debugging-Tool auf niedriger Ebene zur Fehlerbehebung bei Netzwerken. Es ermöglicht Ihnen, Capture-Dateien zu speichern, die Sie mit den Analysewerkzeugen weiter analysieren können. Zwei gängige Tools sind Network Analyzer und Wireshark.




```
> start nstrace -size 0
 Done
> stop nstrace
 Done
```


Sobald die NSTRACE-Capture-Datei in /var/nstrace auf dem ADC erstellt wurde, können Sie die Capture-Datei zur Paketerfassung und Netzwerkanalyse in Wireshark importieren.

SYSCTL - Ausführliche ADC-Informationen: Beschreibung, Modell, Plattform, CPUs usw

```
    sysctl -a grep hw.physmem

    hw.physmem: 862306304
    netscaler.hw_physmem_mb: 822
<!--NeedCopy-->
```

aaad.debug - Open Pipe für Debug-Informationen zur Authentifizierung

```
process_radius Got RADIUS event
process_radius Received BAD_ACCESS_REJECT for: <username>
process_radius Sending reject.
send_reject_with_code Rejecting with error code 4001.
```

Weitere Informationen zur Behebung von Authentifizierungsproblemen über ADC oder ADC Gateway mit dem Modul aaad.debug finden Sie im aaad.debug-Supportartikel.

Es besteht auch die Möglichkeit, Leistungsstatistiken und Ereignisprotokolle direkt für den ADC abzurufen. Weitere Informationen dazu finden Sie im ADC-Supportdokument.

Fehlerbehebung für SRE und Plattformteams

Kubernetes-Verkehrsströme

Norden/Süden:

- Nord/Süd-Verkehr ist der Datenverkehr, der vom Benutzer über den Ingress in den Cluster fließt.

Ost/West:

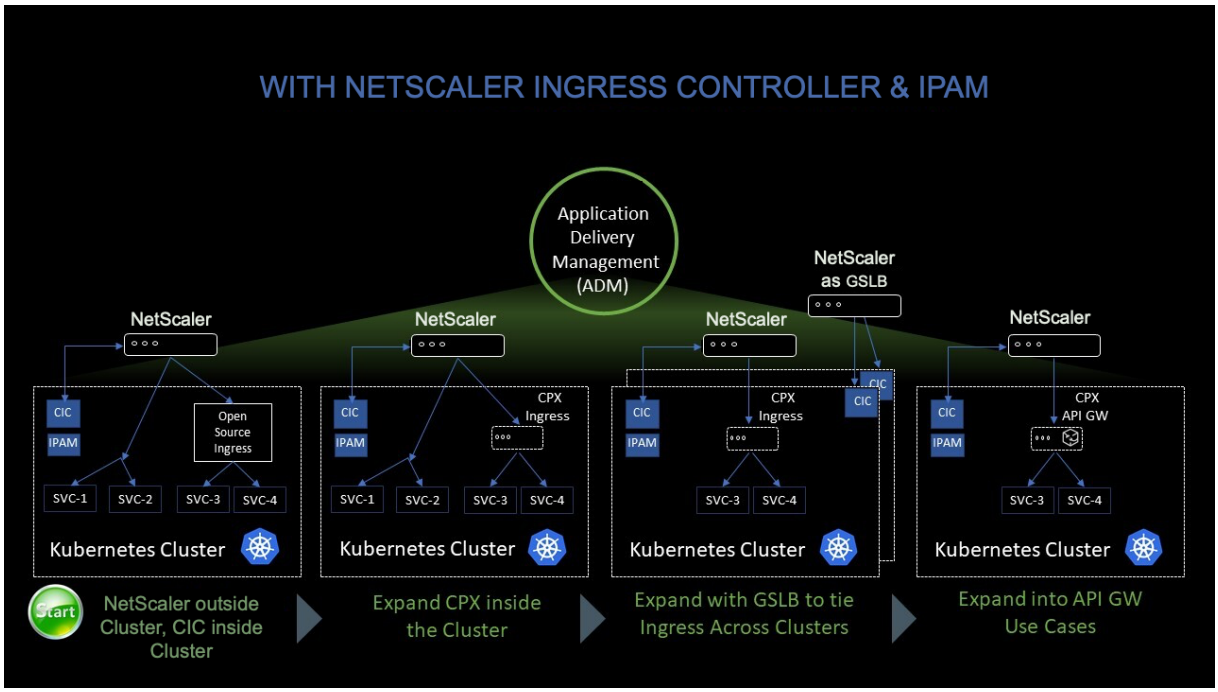
- Der Ost/West-Verkehr ist der Verkehr, der um den Kubernetes-Cluster fließt: Service-to-Service oder Service-zu-Datenspeicher.

Wie NetScaler CPX-Last den Ost-West-Verkehrsfluss in einer Kubernetes-Umgebung ausgleicht

Nachdem Sie den Kubernetes-Cluster bereitgestellt haben, müssen Sie den Cluster in ADM integrieren, indem Sie die Details der Kubernetes-Umgebung in ADM angeben. ADM überwacht die Änderungen der Kubernetes-Ressourcen wie Dienste, Endpunkte und Ingress-Regeln.

Wenn Sie eine NetScaler CPX-Instanz im Kubernetes-Cluster bereitstellen, registriert sie sich automatisch bei ADM. Im Rahmen des Registrierungsprozesses erfährt ADM mehr über die IP-Adresse der CPX-Instanz und den Port, über den es die Instanz erreichen kann, um sie mithilfe von NITRO REST-APIs zu konfigurieren.

Die folgende Abbildung zeigt, wie NetScaler CPX den Ost-West-Traffic-Flow in einem Kubernetes-Cluster ausgleicht.



In diesem Beispiel wird

Knoten 1 und Knoten 2 der Kubernetes-Cluster enthalten Instanzen eines Front-End-Dienstes und eines Back-End-Dienstes. Wenn die NetScaler CPX-Instanzen in Knoten 1 und Knoten 2 bereitgestellt werden, werden die NetScaler CPX-Instanzen automatisch bei ADM registriert. Sie müssen den Kubernetes-Cluster manuell in ADM integrieren, indem Sie die Kubernetes-Clusterdetails in ADM konfigurieren.

Wenn ein Client den Front-End-Dienst anfordert, gleicht die eingehende Ressourcenlast die Anforderung zwischen den Instanzen des Front-End-Dienstes auf den beiden Knoten aus. Wenn eine Instanz des Front-End-Dienstes Informationen von den Back-End-Diensten im Cluster benötigt, leitet sie die Anfragen an die NetScaler CPX-Instanz in ihrem Knoten weiter. Diese NetScaler CPX-Instanz verteilt die Anforderungen zwischen den Back-End-Diensten im Cluster und sorgt so für einen Ost-West-Traffic.

ADM Service Graph für Anwendungen

Mit der Service Graph-Funktion in NetScaler ADM können Sie alle Dienste in einer grafischen Darstellung überwachen. Diese Funktion bietet auch eine detaillierte Analyse und nützliche Metriken. Sie können Service-Diagramme anzeigen für:

- Für alle NetScaler-Instanzen konfigurierte Anwendungen
- Kubernetes-Anwendungen
- 3-stufige Webanwendungen

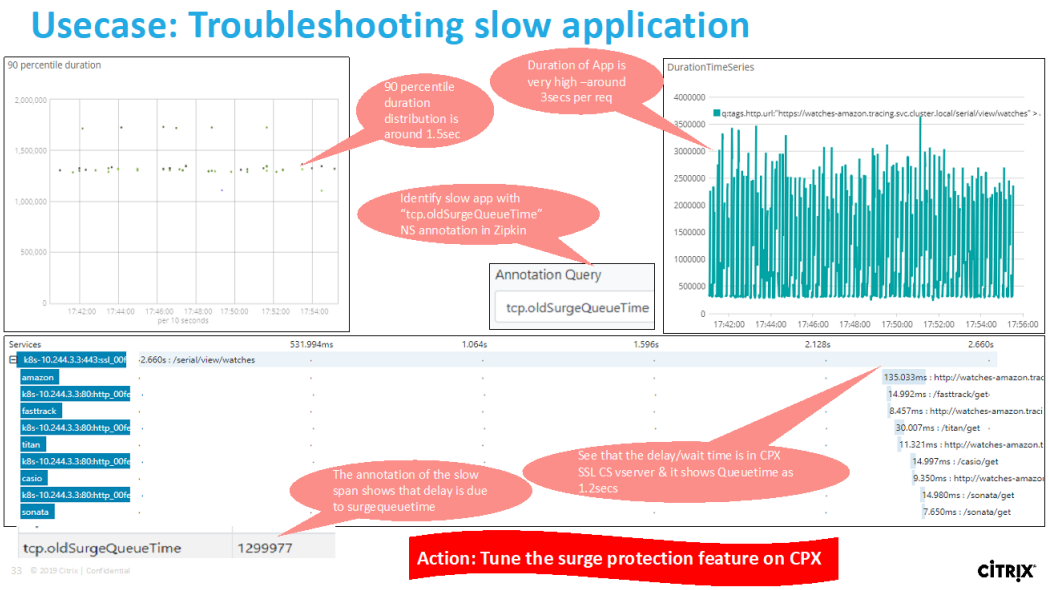
Um loszulegen, sehen Sie sich die Details im Service Graphan.

Zähler für Microservice-Anwendungen anzeigen

Das Service-Diagramm zeigt auch alle Microservice-Anwendungen an, die zu den Kubernetes-Clustern gehören. Der Mauszeiger auf einem Service, um die Metrik-Details anzuzeigen.

Sie können Folgendes anzeigen:

- Der Dienstname
- Das vom Dienst verwendete Protokoll wie SSL, HTTP, TCP, SSL über HTTP
- **Treffer** — Die Gesamtzahl der vom Dienst erhaltenen Treffer
- **Reaktionszeit des Service** — Die durchschnittliche Reaktionszeit, die vom Service in Anspruch genommen wurde.
  (Reaktionszeit = Client-RTT+ letztes Byte anfordern - erstes Byte anfordern)
- **Errors** — Die Gesamtzahl der Fehler wie 4xx, 5xx usw.
- **Datenvolumen** — Das Gesamtvolumen der vom Dienst verarbeiteten Daten
- **Namespace** — Der Namensraum des Service
- **Clustername** — Der Clustername, in dem der Dienst gehostet wird
- **SSL-Serverfehler** — Die gesamten SSL-Fehler vom Dienst



Diese spezifischen Zähler und Transaktionsprotokolle können über den NetScaler Observability Exporter (COE) mithilfe einer Reihe unterstützter Endpunkte extrahiert werden. Weitere Informationen zu COE finden Sie in den folgenden Abschnitten.

Exporteur für NetScaler-Statistiken

Dies ist ein einfacher Server, der NetScaler-Statistiken kratzt und sie über HTTP nach Prometheus exportiert. Prometheus kann dann als Datenquelle zu Grafana hinzugefügt werden, um die NetScaler-Statistiken grafisch anzuzeigen.

Um die Statistiken und Zähler von NetScaler-Instanzen zu überwachen, `citrix-adc-metric-exporter` kann als Container oder Skript ausgeführt werden. Das Exportprogramm sammelt NetScaler-Statistiken wie die Gesamtzahl der Treffer auf einen virtuellen Server, die HTTP-Anforderungsrate, die SSL-Verschlüsselungs-Entschlüsselungsrate usw. von den NetScaler-Instanzen und hält sie so lange, bis der Prometheus-Server die Statistiken abruft und sie mit einem Zeitstempel speichert. Grafana kann dann auf den Prometheus-Server verwiesen werden, um die Statistiken abzurufen, sie zu zeichnen, Alarme einzustellen, Heatmaps zu erstellen, Tabellen zu generieren usw. nach Bedarf, um die NetScaler-Statistiken zu analysieren.

Einzelheiten zum Einrichten des Exportprogramms für die Arbeit in einer Umgebung, wie in der Abbildung dargestellt, finden Sie in den folgenden Abschnitten. Ein Hinweis, auf welchen NetScaler-Entitäten/Metriken der Exporteur standardmäßig kratzt und wie er geändert werden kann, wird ebenfalls erläutert.

Weitere Informationen zu Exporter for NetScaler finden Sie im Metrics Exporter GitHub.

ADM-Dienst verteilte Ablaufverfolgung

Im Service-Diagramm können Sie die Ansicht für die verteilte Ablaufverfolgung verwenden, um:

- Analysieren Sie die gesamte Leistung des Dienstes.
- Visualisieren Sie den Kommunikationsfluss zwischen dem ausgewählten Dienst und seinen voneinander abhängigen Diensten.
- Identifizieren Sie, welcher Dienst auf Fehler hinweist, und beheben Sie den fehlerhaften Dienst
- Zeigen Sie Transaktionsdetails zwischen dem ausgewählten Dienst und jedem voneinander abhängigen Dienst an.

Voraussetzungen für die verteilte ADM-Ablaufverfolgung

Um die Trace-Informationen für den Dienst anzuzeigen, müssen Sie:

- Stellen Sie sicher, dass eine Anwendung die folgenden Trace-Header verwaltet, während sie Ost-West-Verkehr sendet:

- `x-request-id`
- `x-b3-traceid`
- `x-b3-spanid`
- `x-b3-parentspanid`
- `x-b3-sampled`
- `x-b3-flags`
- `x-ot-span-context`

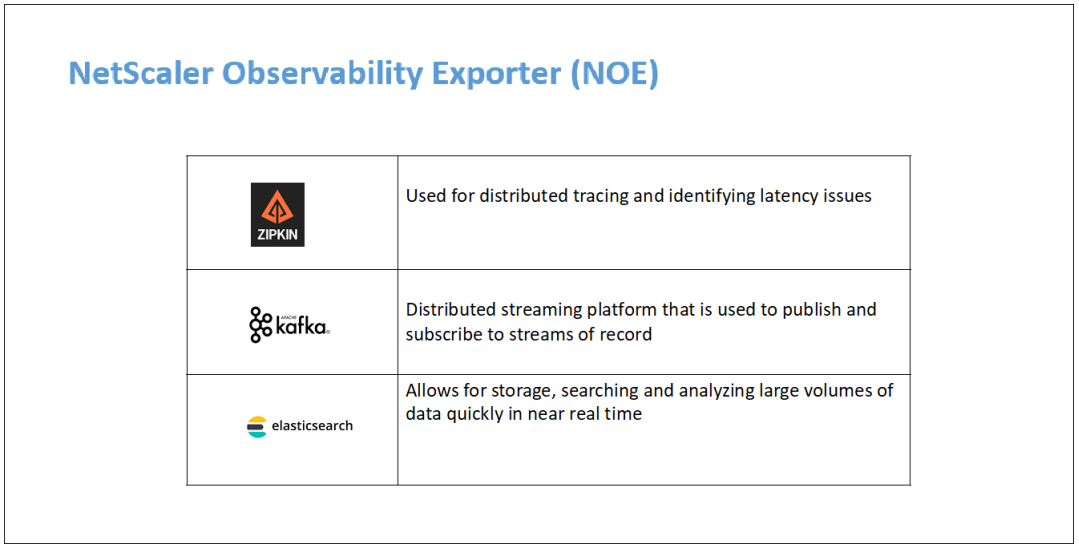
- Aktualisieren Sie die CPX-YAML-Datei mit NS_DISTRIBUTED_TRACING und den Wert auf YES. Informationen zu den ersten Schritten finden Sie unter Verteilte Ablaufverfolgung.

Parsen des NetScaler Observability Exporter (COE)

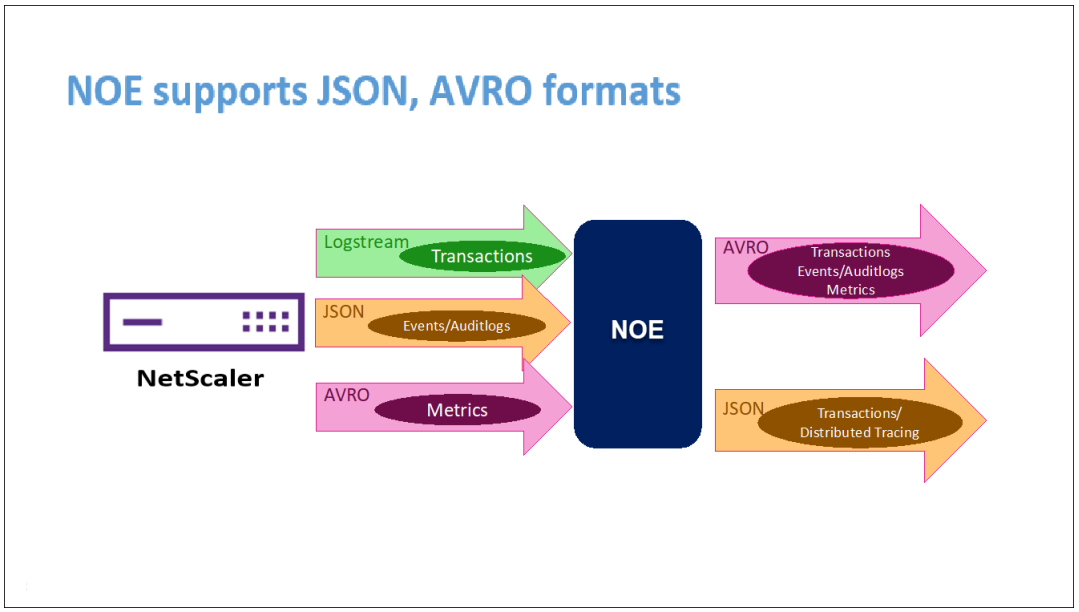
NetScaler Observability Exporter ist ein Container, der Metriken und Transaktionen von NetScalern sammelt und sie in geeignete Formate (wie JSON, AVRO) für unterstützte Endgeräte umwandelt. Sie können die vom NetScaler Observability Exporter gesammelten Daten auf den gewünschten Endpunkt exportieren. Durch die Analyse der an den Endpunkt exportierten Daten können Sie wertvolle Erkenntnisse auf Microservices-Ebene für Anwendungen gewinnen, die von NetScalern als Proxy bereitgestellt werden.

Weitere Informationen zu COE finden Sie im COE GitHub.

COE mit Elasticsearch als Transaktionsendpunkt



Wenn Elasticsearch als Transaktionsendpunkt angegeben ist, konvertiert NetScaler Observability Exporter die Daten in das JSON-Format. Auf dem Elasticsearch-Server erstellt NetScaler Observability Exporter stündlich Elasticsearch-Indizes für jeden ADC. Diese Indizes basieren auf Daten, Stunde, UUID des ADC und dem Typ der HTTP-Daten (http_event oder http_error). Anschließend lädt der NetScaler Observability Exporter die Daten im JSON-Format unter Elastic-Suchindizes für jeden ADC hoch. Alle regulären Transaktionen werden in den http_event-Index aufgenommen und alle Anomalien werden in den http_error-Index aufgenommen.



Unterstützung für verteilte Ablaufverfolgung mit Zipkin

In einer Microservice-Architektur kann sich eine einzelne Endbenutzeranfrage über mehrere Microservices erstrecken, was die Verfolgung einer Transaktion und das Beheben von Fehlerquellen schwierig macht. In solchen Fällen können herkömmliche Methoden der Leistungsüberwachung nicht genau bestimmen, wo Fehler auftreten und was der Grund für eine schlechte Leistung ist. Sie müssen Datenpunkte erfassen, die für jeden Microservice spezifisch sind, der eine Anfrage bearbeitet, und diese analysieren, um aussagekräftige Erkenntnisse zu erhalten.

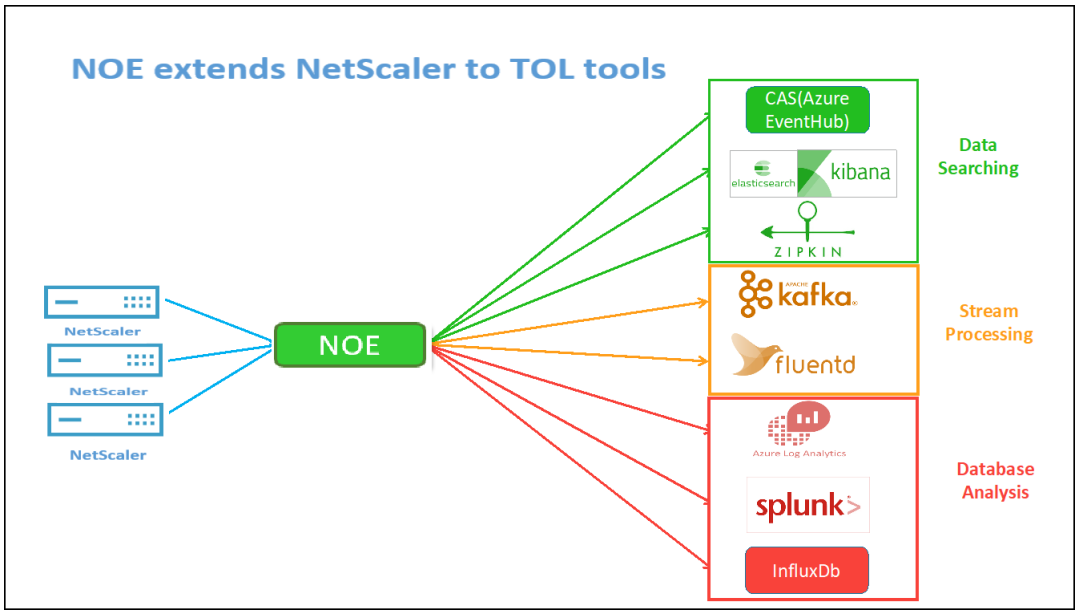
Das verteilte Tracing begegnet dieser Herausforderung, indem es eine Möglichkeit bietet, eine Transaktion durchgängig zu verfolgen und zu verstehen, wie sie über mehrere Microservices hinweg gehandhabt wird.

OpenTracing ist eine Spezifikation und ein Standardsatz von APIs zum Entwerfen und Implementieren von verteiltem Tracing. Verteilte Tracer ermöglichen es Ihnen, den Datenfluss zwischen Ihren Microservices zu visualisieren und helfen, Engpässe in Ihrer Microservices-Architektur zu identifizieren.

NetScaler Observability Exporter implementiert die verteilte Ablaufverfolgung für NetScaler und unterstützt derzeit Zipkin als verteilten Tracer.

Derzeit können Sie die Leistung auf Anwendungsebene mit NetScaler überwachen. Mit NetScaler Observability Exporter mit NetScaler können Sie Protokollierungsdaten für Microservices jeder Anwendung abrufen, die von Ihrem NetScaler CPX, MPX oder VPX als Proxy bereitgestellt werden.

Um loszulegen, lesen Sie den GitHub Observability Exporter.

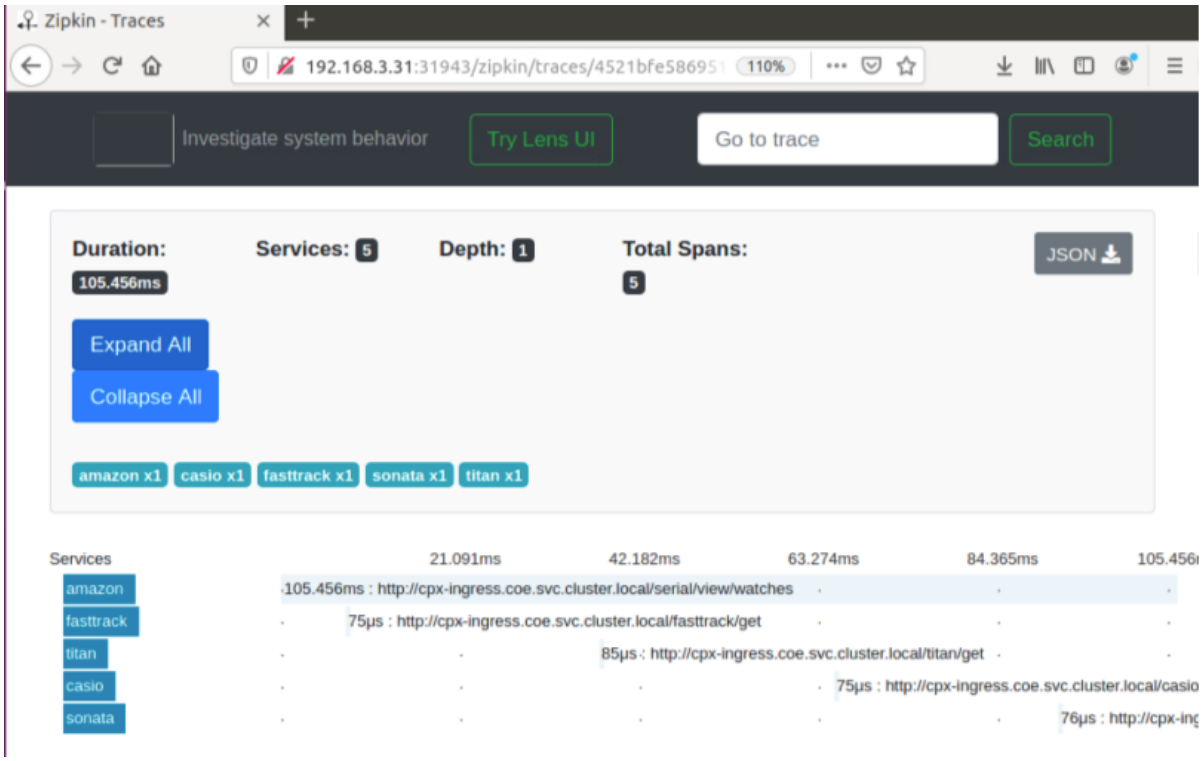


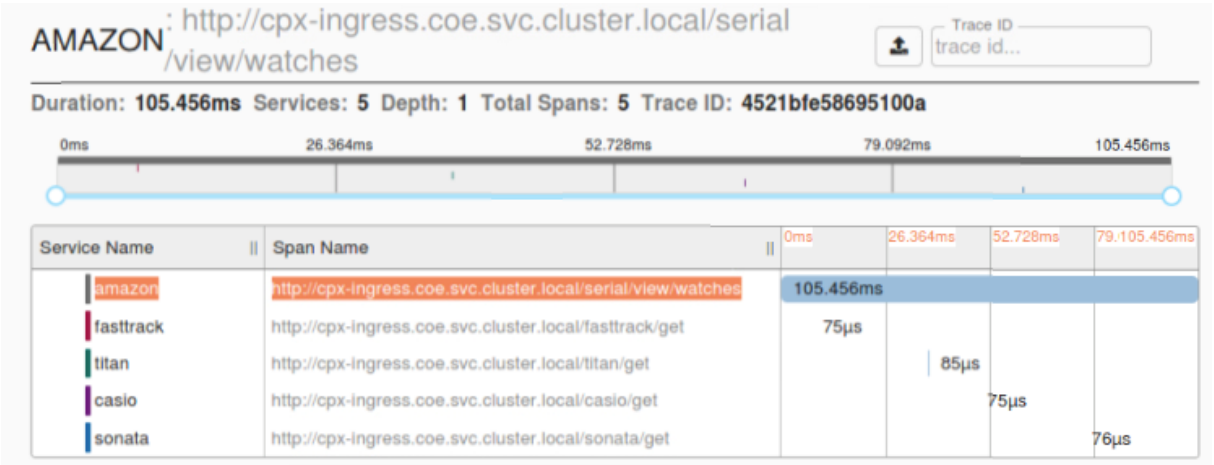
Zipkin für das Debugging von Anwendungen

Zipkin ist ein verteiltes Open Source-Verfolgungssystem, das auf Dappers Papier von Googlebasiert. Dapper ist Googles System für die systemverteilte Rückverfolgung in der Produktion. Google erklärt dies in seinem Artikel: “Wir haben Dapper entwickelt, um den Entwicklern von Google mehr Informationen über das Verhalten komplexer verteilter Systeme zu liefern”. Die Beobachtung des Systems aus verschiedenen Blickwinkeln ist bei der Fehlersuche von entscheidender Bedeutung, insbesondere wenn ein System komplex und verteilt ist.

Die folgenden Zipkin-Verfolgungsdaten identifizieren insgesamt 5 Bereiche und 5 Dienste im Zusammenhang mit der Watches-Beispielanwendung. Die Trace-Daten zeigen die spezifischen Span-Daten über die 5 Microservices hinweg.

Um loszulegen, siehe Zipkin.





Beispiel für einen Zipkin-Zeitraum, der die Anwendungslatenz für die erste Anforderung zum Laden

Services: amazon

Date Time	Relative Time	Annotation	Address
7/15/2020, 2:14:24 PM		Server Start	10.10.235.179:1719 (amazon)
7/15/2020, 2:14:24 PM	105.456ms	Server Finish	10.10.235.179:1719 (amazon)

Key	Value
component	py_zipkin
http.host	amazon:1719
http.method	GET
http.path	/serial/view/watches
http.url	http://cpx-ingress.coe.svc.cluster.local/serial/view/watches
Local Component	amazon
peer.address	10.10.235.190

Kibana zum Anzeigen von Daten

Kibana ist eine offene Benutzeroberfläche, mit der Sie Ihre Elasticsearch-Daten visualisieren und im Elastic Stack navigieren können. Erledigen Sie alles, von der Verfolgung der Abfrageladung bis hin zum Verständnis des Ablaufs von Anfragen

Egal, ob Sie Analyst oder Administrator sind, Kibana macht Ihre Daten umsetzbar, indem es die folgenden drei Schlüsselfunktionen bereitstellt:

- **Eine Open Source Analyse- und Visualisierungsplattform.** Erkunden Sie mit Kibana Ihre Elasticsearch-Daten und erstellen Sie anschließend wunderschöne Visualisierungen und Dashboards.
- **Eine Benutzeroberfläche für die Verwaltung des Elastic Stack.** Verwalten Sie Ihre Sicherheitseinstellungen, weisen Sie Benutzerrollen zu, erstellen Sie Snapshots, rollen Sie Ihre Daten zusammen und vieles mehr — alles bequem über eine Kibana-Benutzeroberfläche.
- **Ein zentraler Knotenpunkt für die Lösungen von Elastic.** Von der Protokollanalyse über die Dokumentenerkennung bis hin zum SIEM ist Kibana das Portal für den Zugriff auf diese und andere Funktionen.

Kibana wurde entwickelt, um Elasticsearch als Datenquelle zu verwenden. Stellen Sie sich Elasticsearch als die Engine vor, die die Daten speichert und verarbeitet, wobei Kibana an der Spitze sitzt.

Auf der Homepage bietet Kibana die folgenden Optionen zum Hinzufügen von Daten:

- Importieren Sie Daten mit dem Dateidaten-Visualizer.
- Richten Sie mithilfe unserer integrierten Tutorials einen Datenfluss zu Elasticsearch ein. Wenn es für deine Daten kein Tutorial gibt, gehe zur Beats Übersicht, um mehr über andere Datenversender in der Beats-Familie zu erfahren.
- Fügen Sie einen Beispieldatensatz hinzu und testen Sie Kibana, ohne selbst Daten zu laden.
- Indizieren Sie Ihre Daten mit REST-APIs oder Clientbibliothekenin Elasticsearch.

Kibana verwendet ein Indexmuster, um anzugeben, welche Elasticsearch-Indizes untersucht werden sollen. Wenn Sie eine Datei hochladen, ein integriertes Tutorial ausführen oder Beispieldaten hinzufügen, erhalten Sie ein kostenloses Indexmuster und können mit der Erkundung beginnen. Wenn Sie Ihre eigenen Daten laden, können Sie in Stack Managementein Indexmuster erstellen.

Schritt 1: Index-Pattern für Logstash konfigurieren

Schritt 2: Wählen Sie den Index aus und generieren Sie den zu füllenden Datenverkehr.

Schritt 3: Generieren Sie eine Anwendung aus den unstrukturierten Daten aus Protokoll-Feeds.

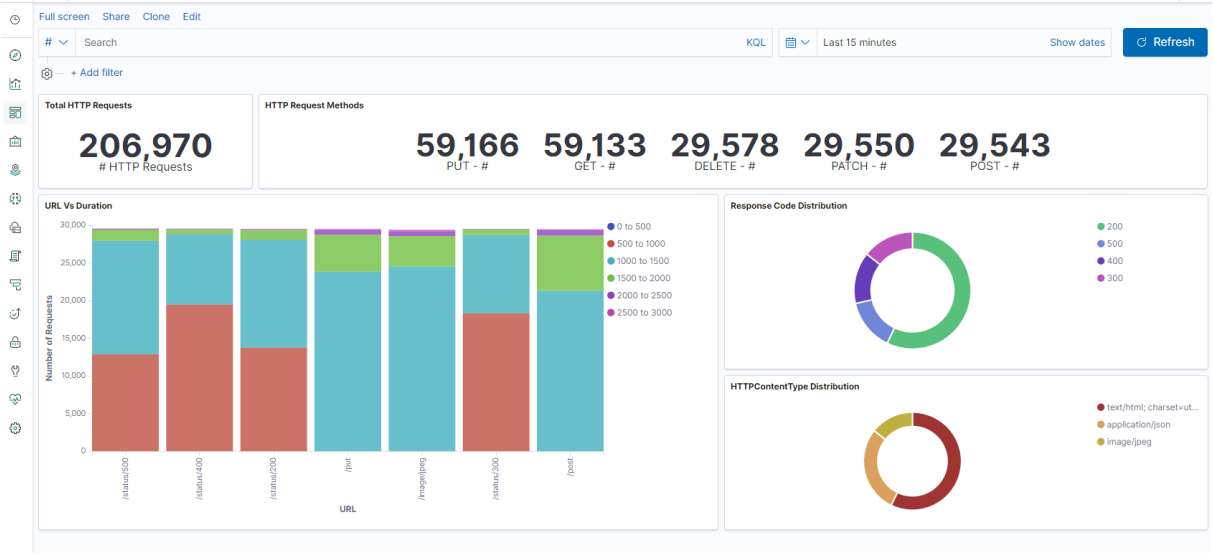
Schritt 4: Kibana formatiert die Logstash-Eingabe, um Berichte und Dashboards zu erstellen.

- Zeitbereich
- Tabellarische Ansicht
- Trefferzahlen basierend auf der Anwendung.

- Zeit-IP, Agent, Maschine.OS, Antwortcode (200), URL
- Filtern nach Werten

Schritt 5: Visualisieren Sie die Daten in einem Aggregationsbericht.

- Ergebnisaggregation in einem Diagrammbericht (Torte, Grafik usw.)



Bereitstellen einer NetScaler VPX- Instanz

May 11, 2023

> **Hinweis**
>
> NetScaler ADM Service Connect ist standardmäßig aktiviert, nachdem Sie NetScaler oder NetScaler Gateway installiert oder aktualisiert haben, um 13.0 Build 61.xx und höher freizugeben. Weitere Informationen finden Sie unter Data Governance und NetScaler ADM Service verbinden.

Das NetScaler VPX Produkt ist eine virtuelle Appliance, die auf einer Vielzahl von Virtualisierungs- und Cloud-Plattformen gehostet werden kann:

- Citrix Hypervisor
- VMware ESX
- Microsoft Hyper-V
- Linux KVM
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Weitere Informationen finden Sie im Datenblatt zu NetScaler VPX.

Weitere Informationen zum Provisionieren einer NetScaler VPX-Instanz auf einer SDX-Appliance finden Sie unter Provisioning von NetScaler-Instanzen.

NetScaler Application Delivery Management für NetScaler VPX

Die NetScaler Application Delivery Management-Software ist eine zentrale Verwaltungslösung, die den Betrieb vereinfacht, indem sie Administratoren unternehmensweite Transparenz bietet und Verwaltungsaufgaben automatisiert, die auf mehreren Instanzen ausgeführt werden müssen.

Sie können NetScaler VPX-Instanzen zusätzlich zu anderen NetScaler-Produkten wie NetScaler Gateway, NetScaler SDX, NetScaler CPX und Citrix SD-WAN verwalten und überwachen. Mit der Application Delivery Management-Software können Sie die gesamte globale Anwendungsbereitstellungsinfrastruktur über eine einzige einheitliche Konsole verwalten, überwachen und beheben.

Weitere Informationen finden Sie in der NetScaler Application Delivery Management-Dokumentation.

Support-Matrix und Nutzungsrichtlinien

September 18, 2023

In diesem Dokument werden die verschiedenen Hypervisoren und Funktionen aufgeführt, die auf einer NetScaler VPX-Instanz unterstützt werden. Das Dokument beschreibt auch ihre Nutzungsrichtlinien und bekannten Einschränkungen.

VPX-Instanz auf Citrix Hypervisor

Citrix Hypervisor Version	SysID	VPX Modelle
8.2 unterstützt ab 13.0 64.x, 8.0, 7.6, 7.1	450000	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G

VPX-Instanz auf dem VMware ESX-Hypervisor

Die folgenden VPX-Modelle mit 450010 (Sys ID) unterstützen die in der Tabelle aufgeführten VMware ESX-Versionen.

VPX-Modelle: VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G und VPX 100G.

ESX-Version	ESX-Veröffentlichungsdatum (JJJJ/MM/TT)	ESX-Build-Nummer	NetScaler VPX Version
ESXi 8.0u1	2023/04/18	21495797	13.1-45.x und höher
ESXi 8.0c	2023/03/30	21493926	13.1-45.x und höher
ESXi 8.0	2022/10/11	20513097	13.1-42.x und höher
ESXi 7.0 Update 3m	2023/05/03	21686933	14.1-4.x und höher
ESXi 7.0 Update 3i	2022/12/08	20842708	13.1-37.x und höher
ESXi 7.0-Update 3f	2022/07/12	20036589	Ab 13.1-33.x
ESXi 7.0-Update 3d	2022/03/29	19482537	Ab 13.1-27.x
ESXi 7.0 3c aktualisieren	2022/01/27	19193900	ab 13,1-21.x
ESXi 6.7 P04	2020/11/19	17167734	Ab 13.0-67.x
ESXi 6.7 P03	2020/08/20	16713306	Ab 13.0-67.x
ESXi 6.5 GA	2016/11/15	4564106	Ab 13.0-47.x
ESXi 6.5 U1g	2018/3/20	7967591	Ab 13.0 47.x

ESX-Version	ESX-Veröffentlichungsdatum (JJJJ/MM/TT)	ESX-Build-Nummer	NetScaler VPX Version
ESXi 6.0 Update 3	2017/2/24	5050593	Ab 12.0-51.x

VPX-Instanz auf Microsoft Hyper-V

Hyper-V-Version	SysID	VPX Modelle
2012, 2012 R2, 2016, 2019	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000

VPX-Instanz auf generischem KVM

Generische KVM-Version	SysID	VPX Modelle
RHEL 7.4, RHEL 7.5 (ab NetScaler Version 12.1 50.x), RHEL 7.6, RHEL 8.0, Ubuntu 16.04, Ubuntu 18.04, RHV 4.2	450070	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G. VPX 25G, VPX 40G, VPX 100G

Zu beachtende Punkte:

Berücksichtigen Sie bei der Verwendung von KVM-Hypervisoren die folgenden Punkte.

- Die VPX-Instanz ist für Hypervisor Releaseversionen in Tabelle 1—4 und nicht für Patch-Releases innerhalb einer Version qualifiziert. Es wird jedoch erwartet, dass die VPX-Instanz nahtlos mit Patch-Versionen einer unterstützten Version funktioniert. Wenn dies nicht der Fall ist, öffnen Sie einen Supportfall für die Fehlerbehebung und das Debuggen.
- Bevor Sie RHEL 7.6 verwenden, führen Sie die folgenden Schritte auf dem KVM-Host aus:
  1. Bearbeiten Sie /etc/default/grub und hängen Sie `"kvm_intel.preemption_timer=0"` an die Variable `GRUB_CMDLINE_LINUX` an.
  2. Generieren Sie grub.cfg mit dem Befehl `"## grub2-mkconfig -o /boot/grub2/grub.cfg"` neu.
  3. Starten Sie den Hostcomputer neu.
- Bevor Sie Ubuntu 18.04 verwenden, führen Sie die folgenden Schritte auf dem KVM-Host aus:

1. Bearbeiten Sie /etc/default/grub und hängen Sie `"kvm_intel.preemption_timer=0"` an die Variable `GRUB_CMDLINE_LINUX` an.
2. Generieren Sie grub.cfg mit dem Befehl `"## grub-mkconfig -o /boot/grub/grub.cfg "` neu.
3. Starten Sie den Hostcomputer neu.

VPX-Instanz auf AWS

AWS-Version	SysID	VPX Modelle
–	450040	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX BYOL, VPX 8000, VPX 10G, VPX 15G und VPX 25G sind nur mit BYOL mit EC2-Instanztypen (C5, M5 und C5n) verfügbar

> **Hinweis:**
>
> Das VPX 25G-Angebot bietet nicht den 25G-Durchsatz in AWS, kann jedoch im Vergleich zum VPX 15G-Angebot eine höhere SSL-Transaktionsrate bieten.

VPX-Instanz auf Azure

Azure-Version	SysID	VPX Modelle
–	450020	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX BYOL

VPX-Funktionsmatrix

	VPX on XenServer		VPX on VMware ESX				VPX on Microsoft Hyper-V	VPX on generic KVM			VPX on AWS	VPX on Azure	VPX on GCP
Features	**PV**	**SR-IOV**	**PV**	**SR-IOV**	**Emulated**	**PCI Passthrough**	**PV**	**PV**	**SR-IOV**	**PCI Passthrough**			
Multi-PE Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clustering Support	Yes	Yes[1]	Yes	Yes[1]	Yes	Yes	Yes	Yes	Yes[1]	Yes	No	No	No
VLAN Tagging	Yes	Yes	Yes	Yes	Yes	Yes	Yes (only on 2012R2)	Yes	Yes	Yes	No	No	No
Detecting Link Events	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	No[2]	Yes[3]	Yes[3]	No[2]	No[2]	No[2]
Interface Parameter Configuration	No	No	No	No	No	Yes	No	No	No	Yes	No	No	No
Static LA	Yes[2]	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	Yes[2]	Yes[2]	Yes[3]	Yes[3]	No	No	No
LACP	No	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Static CLAG	No	No	No	No	No	No	No	No	No	No	No	No	No
LACP CLAG	No	No	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Hot-plug	No	No	No	No	No	No	No	No	No	No	Yes	No	No

Die in der vorstehenden Tabelle verwendeten hochgestellten Zahlen (1, 2, 3) beziehen sich auf die folgenden Punkte mit entsprechender Nummerierung:

1. Clustering-Unterstützung ist auf SRIOV für clientseitige und serverseitige Schnittstellen und nicht für die Rückwandplatine verfügbar.
2. Interface DOWN Ereignisse werden in NetScaler VPX-Instanzen nicht aufgezeichnet.
3. Für statische LA wird möglicherweise weiterhin Datenverkehr auf der Schnittstelle gesendet, deren physischer Status DOWN ist.
4. Für LACP kennt das Peer-Gerät das Interface DOWN-Ereignis basierend auf dem LACP-Timeout-Mechanismus.
    - Kurzes Timeout: 3 Sekunden
    - Langes Timeout: 90 Sekunden
5. Teilen Sie für LACP keine Schnittstellen zwischen VMs.
6. Bei dynamischem Routing hängt die Konvergenzzeit vom Routingprotokoll ab, da Linkereignisse nicht erkannt werden.
7. Die überwachte statische Route-Funktionalität schlägt fehl, wenn Sie keine Monitore an statische Routen binden, da der Routenstatus vom VLAN-Status abhängt. Der VLAN-Status hängt vom Verbindungsstatus ab.
8. Eine teilweise Fehlererkennung erfolgt bei hoher Verfügbarkeit nicht, wenn ein Verbindungsfehler vorliegt. Eine Hohe-Verfügbarkeit-Split-Brain-Bedingung kann auftreten, wenn ein Verbindungsfehler vorliegt.

- Wenn ein Linkereignis (Deaktivieren/Aktivieren, Zurücksetzen) von einer VPX-Instanz generiert wird, ändert sich der physische Status des Links nicht. Bei statischer LA wird jeder vom Peer initiierte Datenverkehr auf der Instanz gelöscht.
- Damit die VLAN-Tagging-Funktion funktioniert, gehen Sie folgendermaßen vor:

Legen Sie auf VMware ESX die VLAN-ID der Portgruppe auf dem vSwitch des VMware ESX-Servers auf 1-4095 fest. Weitere Informationen zum Festlegen einer VLAN-ID auf dem vSwitch des VMware ESX-Servers finden Sie unter VMware ESX Server 3 802.1Q VLAN Solutions.

Unterstützte Browser

Betriebssystem	Browser und Versionen
Windows 7	Internet Explorer-8, 9, 10 und 11; Mozilla Firefox 3.6.25 und höher; Google Chrome-15 und höher
Windows 64-Bit	Internet Explorer — 8, 9; Google Chrome — 15 und höher
MAC	Mozilla Firefox - 12 und höher; Safari - 5.1.3; Google Chrome - 15 und höher

AMD-Prozessorunterstützung für VPX-Instanzen

Ab NetScaler Version 13.1 unterstützt die VPX-Instanz sowohl die Intel- als auch die AMD-Prozessoren. Virtuelle VPX-Appliances können auf jedem Instanztyp bereitgestellt werden, der über zwei oder mehr virtualisierte Kerne und mehr als 2 GB Arbeitsspeicher verfügt. Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu NetScaler VPX.

VPX-Plattformen im Vergleich zu NIC-Matrixtabelle

In der folgenden Tabelle sind die Netzwerkkarten aufgeführt, die auf einer VPX-Plattform oder Cloud unterstützt werden.

	Mellanox CX-3	Mellanox CX-4	Mellanox CX-5	Intel 82599 SRIOV VF	Intel X710/X722/XL710 SRIOV VF	Intel X710/XL710 PCI-Passthrough-Modus
VPX (ESXi)	Nein	Ja	Nein	Ja	Nein	Ja
VPX (Citrix Hypervisor)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Ja	Ja	Nein
VPX (KVM)	Nein	Ja	Ja	Ja	Ja	Ja
VPX (Hyper-V)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nein	Nein	Nein
VPX (AWS)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Ja	Nicht verfügbar	Nicht verfügbar
VPX (Azure)	Ja	Ja	Ja	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
VPX (GCP)	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar

Richtlinien für die Verwendung

Folgen Sie diesen Nutzungsrichtlinien:

- Wir empfehlen Ihnen, eine VPX-Instanz auf lokalen Datenträgern des Servers oder auf SAN-basierten Speichervolumes bereitzustellen.

Weitere Informationen finden Sie im Abschnitt **VMware ESXi CPU Considerations** im Dokument Performance Best Practices for VMware vSphere 6.5. Hier ist ein Auszug:

- Es wird nicht empfohlen, virtuelle Maschinen mit hohem CPU-/Speicherbedarf auf einem Host oder Cluster zu lagern, der überfordert ist.
- In den meisten Umgebungen ermöglicht ESXi eine erhebliche CPU-Überbelegung, ohne die Leistung der virtuellen Maschine zu beeinträchtigen. Auf einem Host können Sie mehr vCPUs ausführen als die Gesamtzahl der physischen Prozessorkerne in diesem Host.
- Wenn ein ESXi-Host CPU-gesättigt wird, d.h. die virtuellen Maschinen und andere Lasten auf dem Host alle CPU-Ressourcen verlangen, die der Host hat, funktionieren latenzsensitive Workloads möglicherweise nicht gut. In diesem Fall können Sie die CPU-Last reduzieren, z. B. indem Sie einige virtuelle Maschinen ausschalten oder sie auf einen anderen Host migrieren (oder DRS die automatische Migration durchführen lassen).

- Citrix empfiehlt die neueste Hardwarekompatibilitätsversion, um die neuesten Funktionen des ESXi-Hypervisors für die virtuelle Maschine nutzen zu können. Weitere Informationen zur Hardware- und ESXi-Versionskompatibilität finden Sie in der VMware-Dokumentation.
- Der NetScaler VPX ist eine latenzempfindliche, leistungsstarke virtuelle Appliance. Um die erwartete Leistung zu erzielen, benötigt die Appliance eine vCPU-Reservierung, Speicherreservierung und vCPU-Pinning auf dem Host. Außerdem muss Hyper-Threading auf dem Host deaktiviert werden. Wenn der Host diese Anforderungen nicht erfüllt, treten Probleme wie Hochverfügbarkeitsfailover, CPU-Anstieg innerhalb der VPX-Instanz, Trägheit beim Zugriff auf die VPX CLI, Absturz des Pitboss-Daemons, Paketausfälle und ein niedriger Durchsatz auf.

Ein Hypervisor gilt als übermäßig bereitgestellt, wenn eine der folgenden beiden Bedingungen erfüllt ist:

- Die Gesamtzahl der auf dem Host bereitgestellten virtuellen Kerne (vCPU) ist größer als die Gesamtzahl der physischen Kerne (pCPUs).
- Die Gesamtzahl der bereitgestellten VMs verbrauchen mehr vCPUs als die Gesamtzahl der pCPUs.

  Wenn eine Instanz übermäßig bereitgestellt wird, garantiert der Hypervisor möglicherweise nicht die für die Instanz reservierten Ressourcen (wie CPU, Speicher und andere) aufgrund von Hypervisor-Planungs-Overheads, Fehlern oder Einschränkungen mit dem Hypervisor. Dieses Verhalten kann zu einem Mangel an CPU-Ressource für NetScaler führen und zu den im ersten Punkt unter den **Nutzungsrichtlinien** genannten Problemen führen. Als Administratoren wird empfohlen, die Mandanten auf dem Host zu reduzieren, sodass die Gesamtanzahl der auf dem Host bereitgestellten vCPUs kleiner oder gleich der Gesamtzahl der pCPUs ist.

  Beispiel

  Wenn für ESX-Hypervisor der Parameter `%RDY%` einer VPX-vCPU in der Befehlsausgabe von `esxtop` größer als 0 ist, wird für den ESX-Host Zeitplanungsoverhead angegeben, was zu Latenzproblemen für die VPX-Instanz führen kann.

  Reduzieren Sie in einer solchen Situation die Mandanten auf dem Host, sodass `%RDY%` immer auf 0 zurückkehrt. Wenden Sie sich alternativ an den Hypervisor-Anbieter, um den Grund für die Nichteinhalten der durchgeführten Ressourcenreservierung zu prüfen.
- Hot Adding wird nur für PV- und SRIOV-Schnittstellen mit NetScaler auf AWS unterstützt. VPX-Instanzen mit ENA-Schnittstellen unterstützen kein Hot-Plug, und das Verhalten der Instanzen kann unvorhersehbar sein, wenn Hot-Plugging versucht wird.
- Hot-Removal über die AWS-Webkonsole oder die AWS CLI-Schnittstelle wird mit den PV-, SRIOV- und ENA-Schnittstellen für NetScaler nicht unterstützt. Das Verhalten der Instanzen kann unvorhersehbar sein, wenn versucht wird, Hot-Removal durchzuführen.

Befehle zur Steuerung der CPU-Auslastung der Paket-Engine

Sie können zwei Befehle (`set ns vpxparam` und `show ns vpxparam`) verwenden, um das CPU-Auslastungsverhalten von VPX-Instanzen in Hypervisor- und Cloud-Umgebungen zu steuern:

- `set ns vpxparam [-cpuyield (YES | NO | DEFAULT)] [-masterclockcpu1 (YES | NO)]`

  Erlauben Sie jeder VM, CPU-Ressourcen zu verwenden, die einer anderen VM zugewiesen wurden, aber nicht verwendet werden.

  Parameter für `Set ns vpxparam`:

  -cpuyield: Freigabe von zugewiesenen, aber nicht genutzten CPU-Ressourcen.

  - **YES**: Erlauben Sie, dass zugewiesene, aber ungenutzte CPU-Ressourcen von einer anderen VM verwendet werden.
  - **NO**: Reservieren Sie alle CPU-Ressourcen für die VM, der sie zugewiesen wurden. Diese Option zeigt einen höheren Prozentsatz in Hypervisor- und Cloud-Umgebungen für die VPX-CPU-Auslastung.
  - **DEFAULT**: Nein.

  > **Hinweis:**
  >
  > Auf allen NetScaler VPX-Plattformen beträgt die vCPU-Auslastung auf dem Hostsystem 100 Prozent. Geben Sie den Befehl `set ns vpxparam -cpuyield YES` ein, um diese Verwendung zu überschreiben.

  Wenn Sie die Clusterknoten auf “yield” setzen möchten, müssen Sie die folgenden zusätzlichen Konfigurationen für CCO durchführen:

  - Wenn ein Cluster gebildet wird, erhalten alle Knoten “yield=DEFAULT”.
  - Wenn ein Cluster unter Verwendung der Knoten gebildet wird, die bereits auf “yield=YES” eingestellt sind, werden die Knoten mit “yield=DEFAULT” zum Cluster hinzugefügt.

  > **Hinweis:**
  >
  > Wenn Sie die Clusterknoten auf “yield=YES” setzen möchten, können Sie erst nach der Bildung des Clusters konfigurieren, aber nicht bevor der Cluster gebildet wurde.

  -masterclockcpu1: Sie können die Haupttaktquelle von CPU0 (Management-CPU) auf CPU1 verschieben. Dieser Parameter hat die folgenden Optionen:

  - **YES**: Erlauben Sie der VM, die Haupttaktquelle von CPU0 auf CPU1 zu verschieben.
  - **NO**: VM verwendet CPU0 für die Haupttaktquelle. Standardmäßig ist CPU0 die Haupttaktquelle.

- `show ns vpxparam`

  Zeigt die aktuellen `vpxparam`-Einstellungen an.

Andere Referenzen

- Für Citrix Ready-Produkte besuchen Sie Citrix Ready Marketplace.
- Informationen zum Citrix Ready-Produktsupport finden Sie auf der FAQ-Seite.
- Informationen zu VMware ESX-Hardwareversionen finden Sie unter Upgrade von VMware Tools.

Optimieren der Leistung von NetScaler VPX auf VMware ESX, Linux KVM und Citrix Hypervisors

September 1, 2023

Die Leistung von NetScaler VPX hängt stark vom Hypervisor, den zugewiesenen Systemressourcen und den Hostkonfigurationen ab. Um die gewünschte Leistung zu erzielen, befolgen Sie zunächst die Empfehlungen im VPX-Datenblatt und optimieren Sie es dann mithilfe der in diesem Dokument enthaltenen Best Practices weiter.

NetScaler VPX-Instanz auf VMware ESX-Hypervisoren

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie andere Vorschläge, mit denen Sie eine optimale Leistung der NetScaler VPX-Instanz auf VMware ESX-Hypervisoren erzielen können.

- Empfohlene Konfiguration auf ESX-Hosts
- NetScaler VPX mit E1000-Netzwerkschnittstellen
- NetScaler VPX mit VMXNET3-Netzwerkschnittstellen
- NetScaler VPX mit SR-IOV- und PCI Passthrough-Netzwerkschnittstellen

Empfohlene Konfiguration auf ESX-Hosts

Befolgen Sie diese Empfehlungen, um eine hohe Leistung für VPX mit E1000-, VMXNET3-, SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen zu erzielen:

- Die Gesamtzahl der auf dem ESX-Host bereitgestellten virtuellen CPUs (vCPUs) muss kleiner oder gleich der Gesamtzahl der physischen CPUs (PCPUs) auf dem ESX-Host sein.

- Affinität und CPU-Affinität für ungleichmäßigen Speicherzugriff (NUMA) müssen festgelegt werden, damit der ESX-Host gute Ergebnisse erzielt.

  — Um die NUMA-Affinität eines Vmnic zu ermitteln, melden Sie sich lokal oder remote beim Host an und geben Sie Folgendes ein:

```
#vsish -e get /net/pNics/vmnic7/properties | grep NUMA
Device NUMA Node: 0
<!--NeedCopy-->
```

  - Informationen zum Festlegen der NUMA- und vCPU-Affinität für eine VM finden Sie in der VMware-Dokumentation

NetScaler VPX mit E1000-Netzwerkschnittstellen

Nehmen Sie die folgenden Einstellungen auf dem VMware ESX-Host vor:

- Erstellen Sie auf dem VMware ESX-Host zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Empfangsthreads (Rx) auf dem ESX-Host. Dies erhöht den Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede von Ihnen erstellte vNIC.
- Um den vNIC-Übertragungsdurchsatz (Tx) zu erhöhen, verwenden Sie einen separaten Tx-Thread im ESX-Host pro vNIC. Verwenden Sie den folgenden ESX-Befehl:
  - Für ESX Version 5.5:

```
esxcli system settings advanced set -o /Net/NetTxWorldlet -
   i
<!--NeedCopy-->
```

  - Für ESX ab Version 6.0:

```
esxcli system settings advanced set -o /Net/NetVMTxType -i 1
<!--NeedCopy-->
```

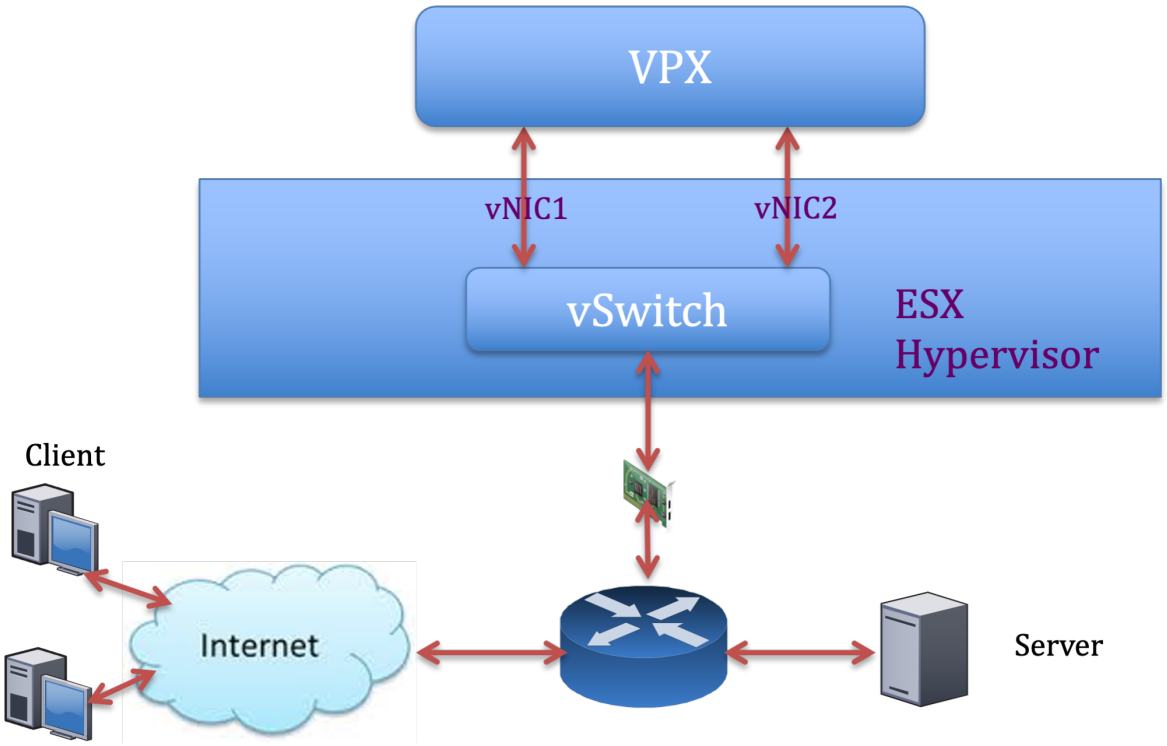
- Um den vNIC Tx-Durchsatz weiter zu erhöhen, verwenden Sie einen separaten Tx-Vervollständigungs-Thread und Rx-Threads pro Gerät (NIC) -Warteschlange. Verwenden Sie den folgenden ESX-Befehl:

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```


> Hinweis:
>
> Stellen Sie sicher, dass Sie den VMware ESX-Host neu starten, um die aktualisierten Einstellungen zu übernehmen.

Zwei vNICs pro pNIC-Bereitstellung

Im Folgenden finden Sie ein Beispiel für Topologie und Konfigurationsbefehle für das Bereitstellungsmodell mit **zwei vNICs pro pNIC**, das eine bessere Netzwerkleistung bietet.



NetScaler VPX Beispielkonfiguration:

Um die in der vorherigen Beispieltopologie gezeigte Bereitstellung zu erreichen, führen Sie die folgende Konfiguration auf der NetScaler VPX-Instanz durch:

- Binden Sie auf Clientseite das SNIP (1.1.1.2) an die Netzwerkschnittstelle 1/1 und aktivieren Sie den VLAN-Tag-Modus.

```
bind vlan 2 -ifnum 1/1 - tagged
bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
<!--NeedCopy-->
```

- Binden Sie auf der Serverseite das SNIP (2.2.2.2) an die Netzwerkschnittstelle 1/1 und aktivieren Sie den VLAN-Tag-Modus.

```
bind vlan 3 -ifnum 1/2 - tagged
```



```
bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
<!--NeedCopy-->
```

- Fügen Sie einen virtuellen HTTP-Server (1.1.1.100) hinzu und binden Sie ihn an einen Dienst (2.2.2.100).

```
add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -
   Listenpolicy None -cltTimeout 180
add service s1 2.2.2.100 HTTP 80 -gslb NONE -maxClient 0 -maxReq
   0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
   180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
bind lb vserver v1 s1
<!--NeedCopy-->
```

> Hinweis:
>
> Stellen Sie sicher, dass Sie die folgenden beiden Einträge in die Routentabelle aufnehmen:
>
> - 1.1.1.0/24 Subnetz mit Gateway, das auf SNIP zeigt 1.1.1.2
> - 2.2.2.0/24 Subnetz mit Gateway, das auf SNIP zeigt 2.2.2.2

NetScaler VPX mit VMXNET3-Netzwerkschnittstellen

Um eine hohe Leistung für VPX mit VMXNET3-Netzwerkschnittstellen zu erzielen, nehmen Sie die folgenden Einstellungen auf dem VMware ESX-Host vor:

- Erstellen Sie zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Rx-Threads im ESX-Host. Dies erhöht den Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede von Ihnen erstellte vNIC.
- Um den vNIC-Übertragungsdurchsatz (Tx) zu erhöhen, verwenden Sie einen separaten Tx-Thread im ESX-Host pro vNIC. Verwenden Sie die folgenden ESX-Befehle:
  - Für ESX Version 5.5:

```
esxcli system settings advanced set  -o /Net/NetTxWorldlet  -i
<!--NeedCopy-->
```

  - Für ESX ab Version 6.0:

```
 esxcli system settings advanced set -o /Net/NetVMTxType  -i 1
 <!--NeedCopy-->
```

Führen Sie auf dem VMware ESX-Host die folgende Konfiguration durch:

- Erstellen Sie auf dem VMware ESX-Host zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Tx- und Rx-Threads im ESX-Host. Dies erhöht den Tx- und Rx-Durchsatz der pNIC-Schnittstelle.

- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede von Ihnen erstellte vNIC.
- Um den Tx-Durchsatz einer vNIC zu erhöhen, verwenden Sie einen separaten Tx-Vervollständigungs-Thread und Rx-Threads pro Gerät (NIC) -Warteschlange. Verwenden Sie den folgenden Befehl:

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```

- Konfigurieren Sie eine VM für die Verwendung eines Übertragungs-Threads pro vNIC, indem Sie der Konfiguration der VM die folgende Einstellung hinzufügen:

```
ethernetX.ctxPerDev = "1"
<!--NeedCopy-->
```

- Konfigurieren Sie eine VM so, dass sie bis zu 8 Übertragungs-Threads pro vNIC verwendet, indem Sie der Konfiguration der VM die folgende Einstellung hinzufügen:

```
ethernetX.ctxPerDev = "3"
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine Erhöhung der Übertragungs-Threads pro vNIC erfordert mehr CPU-Ressourcen (bis zu 8) auf dem ESX-Host. Stellen Sie sicher, dass genügend CPU-Ressourcen verfügbar sind, bevor Sie die obigen Einstellungen vornehmen.

Weitere Informationen finden Sie unter Best Practices für die Leistungsoptimierung von Telekommunikations- und NFV-Workloads
in vSphere

> Hinweis:
>
> Stellen Sie sicher, dass Sie den VMware ESX-Host neu starten, um die aktualisierten Einstellungen zu übernehmen.

Sie können VMXNET3 als Bereitstellung mit **zwei vNICs pro pNIC** konfigurieren. Weitere Informationen finden Sie unter Zwei vNICs pro pNIC-Bereitstellung.

Konfiguration der Multi-Queue- und RSS-Unterstützung auf VMware ESX für VMXNET3-Geräte

Standardmäßig unterstützt das VMXNET3-Gerät nur 8 Rx- und Tx-Warteschlangen. Wenn die Anzahl der vCPUs auf dem VPX 8 überschreitet, wird die Anzahl der für eine VMXNET3-Schnittstelle konfigurierten Rx- und Tx-Warteschlangen standardmäßig auf 1 gesetzt. Sie können bis zu 19 Rx- und Tx-Warteschlangen für VMXNET3-Geräte konfigurieren, indem Sie bestimmte Konfigurationen auf ESX

ändern. Diese Option erhöht die Leistung und die gleichmäßige Verteilung der Pakete über die vCPUs der VPX-Instanz.

> **Hinweis:**
>
> Ab NetScaler Version 13.1 Build 48.x unterstützt NetScaler VPX bis zu 19 Rx- und Tx-Warteschlangen auf ESX für VMXNET3-Geräte.

Voraussetzungen:

Um bis zu 19 Rx- und Tx-Warteschlangen auf ESX für VMXNET3-Geräten zu konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die NetScaler VPX-Version ist 13.1 Build 48.X und höher.
- NetScaler VPX ist mit einer virtuellen Maschine der Hardwareversion 17 und höher konfiguriert, die von VMware ESX 7.0 und höher unterstützt wird.

Konfigurieren Sie VMXNET3-Schnittstellen für die Unterstützung von mehr als 8 Rx- und Tx-Warteschlangen:

1. Öffnen Sie die Konfigurationsdatei der virtuellen Maschine (.vmx).
2. Geben Sie die Anzahl der Rx- und TX-Warteschlangen an, indem Sie die `ethernetX.maxRxQueues` Werte `ethernetX.maxTxQueues` und konfigurieren (wobei X die Anzahl der zu konfigurierenden virtuellen NICs ist). Die maximale Anzahl der konfigurierten Warteschlangen darf nicht größer als die Anzahl der vCPUs in der virtuellen Maschine sein.

   > **Hinweis:**
   >
   > Eine Erhöhung der Anzahl der Warteschlangen erhöht auch den Prozessor-Overhead auf dem ESX-Host. Stellen Sie daher sicher, dass ausreichend CPU-Ressourcen auf dem ESX-Host verfügbar sind, bevor Sie die Warteschlangen erhöhen. Sie können die maximale Anzahl der unterstützten Warteschlangen in Szenarien erhöhen, in denen die Anzahl der Warteschlangen als Leistungsengpass identifiziert wird. In diesen Situationen empfehlen wir, die Anzahl der Warteschlangen schrittweise zu erhöhen. Zum Beispiel von 8 bis 12, dann bis 16, dann bis 20 und so weiter. Bewerten Sie die Leistung bei jeder Einstellung, anstatt sie direkt bis zur Höchstgrenze zu erhöhen.

NetScaler VPX mit SR-IOV- und PCI Passthrough-Netzwerkschnittstellen

Um eine hohe Leistung für VPX mit SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen zu erzielen, siehe Empfohlene Konfiguration auf ESX-Hosts.

NetScaler VPX-Instanz auf Linux-KVM-Plattform

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie andere Vorschläge, mit denen Sie eine optimale Leistung der NetScaler VPX-Instanz auf der Linux-KVM-Plattform erzielen können.

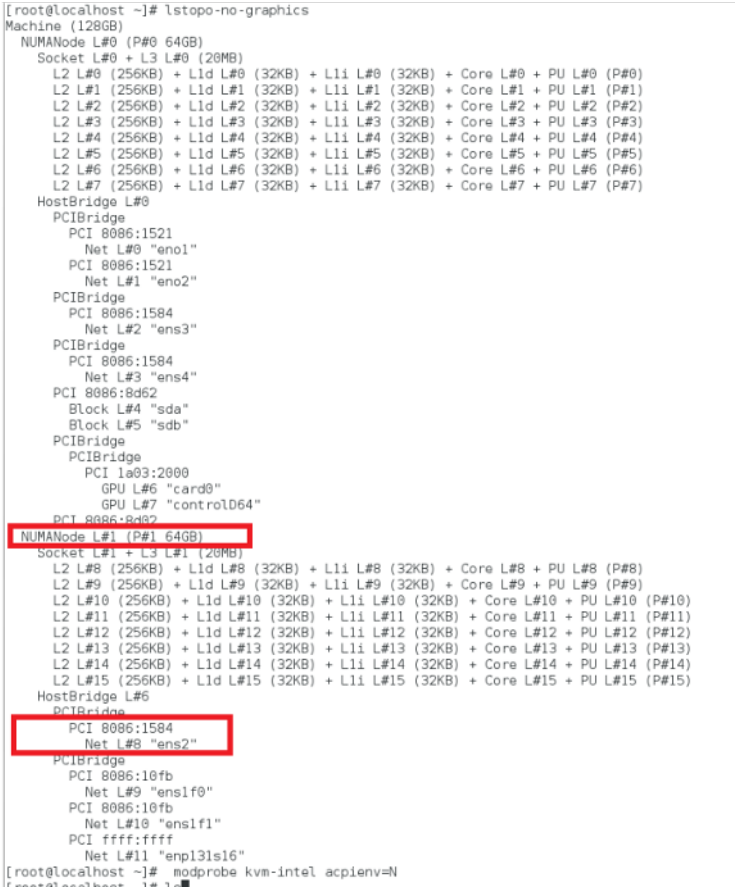
- Leistungseinstellungen für KVM
- NetScaler VPX mit PV-Netzwerkschnittstellen
- NetScaler VPX mit SR-IOV und Fortville PCIe Passthrough-Netzwerkschnittstellen

Leistungseinstellungen für KVM

Nehmen Sie die folgenden Einstellungen auf dem KVM-Host vor:

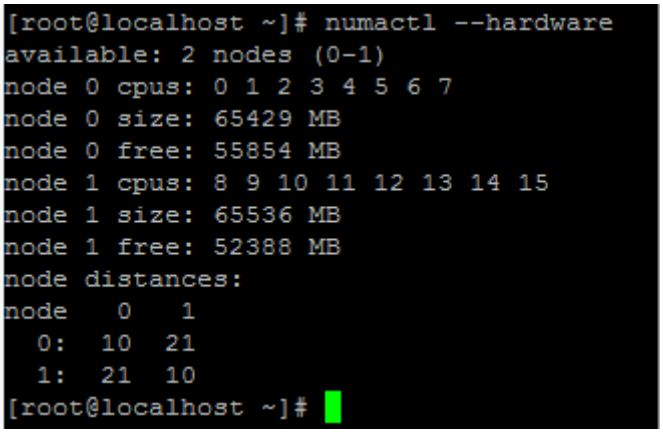
Finden Sie die NUMA-Domäne der NIC mit dem `lstopo` Befehl:

Stellen Sie sicher, dass der Speicher für den VPX und die CPU an derselben Stelle angeheftet ist.
In der folgenden Ausgabe ist die 10G-NIC “ens2” an die NUMA-Domäne #1 gebunden.



Weisen Sie den VPX-Speicher aus der NUMA-Domäne zu.

Der `numactl` Befehl gibt die NUMA-Domäne an, von der der Speicher zugewiesen wird. In der folgenden Ausgabe werden etwa 10 GB RAM vom NUMA-Knoten #0 zugewiesen.



Gehen Sie folgendermaßen vor, um die NUMA-Knotenzuordnung zu ändern.

1. Bearbeiten Sie die XML des VPX auf dem Host.

```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

2. Fügen Sie das folgende Tag hinzu:

```
<numatune>
<memory mode="strict" nodeset="1"/>   This is the NUMA domain name
</numatune>
<!--NeedCopy-->
```

3. Fahren Sie den VPX herunter.
4. Führen Sie den folgenden Befehl aus:

```
virsh define /etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

   Dieser Befehl aktualisiert die Konfigurationsinformationen für die VM mit den NUMA-Knotenzuordnungen.

5. Schalten Sie den VPX ein. Überprüfen Sie dann die `numactl -hardware` Befehlsausgabe auf dem Host, um die aktualisierten Speicherzuweisungen für den VPX zu sehen.


```
[root@localhost ~]# numactl --hardware
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 6 7
node 0 size: 65429 MB
node 0 free: 65429 MB
node 1 cpus: 8 9 10 11 12 13 14 15
node 1 size: 65536 MB
node 1 free: 55854 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
[root@localhost ~]#
```

Pin vCPUs von VPX an physische Kerne.

- Um die vCPU zu pCPU-Zuordnungen einer VPX anzuzeigen, geben Sie den folgenden Befehl ein

```
virsh vcpupin <VPX name>
<!--NeedCopy-->
```

```
root@localhost qemu]#  virsh vcpupin NS-VPX-DVR
CPU: CPU Affinity
----------------------------------
 0: 8
 1: 9
 2: 10
 3: 11
```

Die vCPUs 0—4 werden physikalischen Kernen 8—11 zugeordnet.

- Um die aktuelle pCPU-Nutzung anzuzeigen, geben Sie den folgenden Befehl ein:

```
mpstat -P ALL 5
<!--NeedCopy-->
```

```
[root@localhost qemu]# mpstat -P ALL 5
Linux 3.10.0-123.el7.x86_64 (localhost.localdomain)     05/17/2016      _x86_64_        (16 CPU)

02:26:20 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
02:26:25 PM  all    0.24    0.00    1.67    0.00    0.00    0.00    0.00   17.32    0.00   80.78
02:26:25 PM    0    0.20    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00   98.80
02:26:25 PM    1    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    2    0.20    0.00    0.40    0.00    0.00    0.00    0.00    0.00    0.00   99.40
02:26:25 PM    3    0.00    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.80
02:26:25 PM    4    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    5    0.60    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.20
02:26:25 PM    6    0.40    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    7    1.62    0.00    1.42    0.00    0.00    0.00    0.00    0.00    0.00   96.96
02:26:25 PM    8    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM    9    0.00    0.00    7.60    0.00    0.00    0.00    0.00   92.40    0.00    0.00
02:26:25 PM   10    0.20    0.00    7.00    0.00    0.00    0.00    0.00   92.80    0.00    0.00
02:26:25 PM   11    0.00    0.00    8.60    0.00    0.00    0.00    0.00   91.40    0.00    0.00
02:26:25 PM   12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   13    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   14    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   15    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
```


In dieser Ausgabe ist 8 Management-CPU und 9—11 Paket-Engines.

- Um die vCPU auf pCPU-Pinning zu ändern, gibt es zwei Möglichkeiten.
  - Ändern Sie es zur Laufzeit, nachdem der VPX mit dem folgenden Befehl hochgefahren wurde:

```
virsh vcpupin <VPX name> <vCPU id>  <pCPU number>
virsh vcpupin NetScaler-VPX-XML 0 8
virsh vcpupin NetScaler-VPX-XML 1 9
virsh vcpupin NetScaler-VPX-XML 2 10
virsh vcpupin NetScaler-VPX-XML 3 11
<!--NeedCopy-->
```

  - Um statische Änderungen an der VPX vorzunehmen, bearbeiten Sie die `.xml` Datei wie zuvor mit den folgenden Tags:

    1. Bearbeiten Sie die XML-Datei des VPX auf dem Host

```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

    2. Fügen Sie das folgende Tag hinzu:

```
<vcpu placement='static' cpuset='8-11'>4</vcpu>
    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>
<!--NeedCopy-->
```

    3. Fahren Sie den VPX herunter.
    4. Aktualisieren Sie die Konfigurationsinformationen für die VM mit den NUMA-Knotenzuordnungen mithilfe des folgenden Befehls:

```
virsh define /etc/libvirt/qemu/ <VPX_name>.xml
<!--NeedCopy-->
```

    5. Schalten Sie den VPX ein. Überprüfen Sie dann die `virsh vcpupin <VPX name>` Befehlsausgabe auf dem Host, um das aktualisierte CPU-Pinning zu sehen.

Eliminieren Sie Host-Interrupt-Overhead.

- Erkennt VM_EXITS mithilfe des `kvm_stat` Befehls.

Auf Hypervisor-Ebene werden Host-Interrupts denselben PCPUs zugeordnet, auf denen die vCPUs des VPX angeheftet sind. Dies kann dazu führen, dass vCPUs auf dem VPX regelmäßig rausgeschmissen werden.

Verwenden Sie den `kvm_stat` Befehl, um die VM-Exits zu finden, die von VMs durchgeführt wurden, auf denen der Host ausgeführt wird

```
[root@localhost ~]# kvm_stat -1  | grep EXTERNAL
kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738
[root@localhost ~]#
<!--NeedCopy-->
```

Ein höherer Wert in der Größenordnung von 1+M weist auf ein Problem hin.

Wenn eine einzelne VM vorhanden ist, beträgt der erwartete Wert 30—100 K. Alles andere kann darauf hinweisen, dass ein oder mehrere Host-Interrupt-Vektoren derselben pCPU zugeordnet sind.

- Erkennen Sie Host-Interrupts und migrieren Sie Host-Interrupts.

  Wenn Sie den `concatenate` Befehl für die Datei "/proc/interrupts" ausführen, werden alle Host-Interrupt-Zuordnungen angezeigt. Wenn ein oder mehrere aktive IRQs derselben pCPU zugeordnet werden, erhöht sich der entsprechende Zähler.

  Verschieben Sie alle Interrupts, die sich mit den PCPUs Ihres NetScaler VPX überschneiden, auf ungenutzte PCPUs:

```
echo 0000000f > /proc/irq/55/smp_affinity
0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can
   only be scheduled on pCPUs 0 - 3
<!--NeedCopy-->
```

- Deaktivieren Sie das IRQ Guthaben

  Deaktivieren Sie den IRQ-Balance-Daemon, damit im laufenden Betrieb keine Umschuldung erfolgt.

```
service irqbalance stop
service irqbalance show - To check the status
service irqbalance start - Enable if needed
<!--NeedCopy-->
```

  Stellen Sie sicher, dass Sie den `kvm_stat` Befehl ausführen, um sicherzustellen, dass es nicht viele Zähler gibt.

NetScaler VPX mit PV-Netzwerkschnittstellen

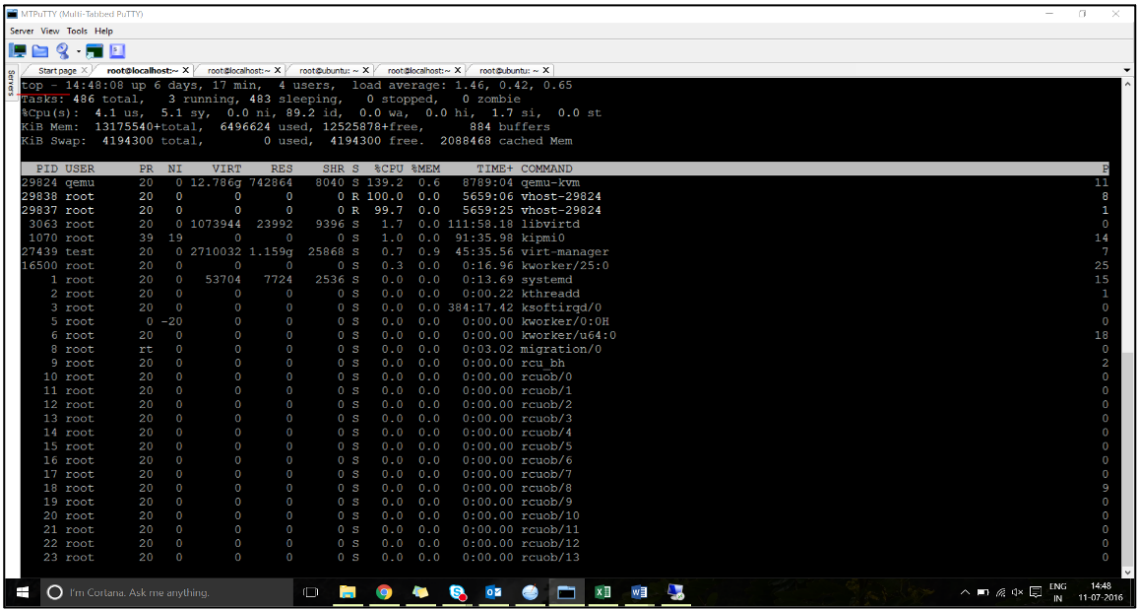
Sie können Para-Virtualization (PV), SR-IOV und PCIe-Passthrough-Netzwerkschnittstellen als **Zwei vNICs pro pNIC-Bereitstellung** konfigurieren. Weitere Informationen finden Sie unter Zwei vNICs pro pNIC-Bereitstellung.

Gehen Sie folgendermaßen vor, um eine optimale Leistung von PV (virtio) -Schnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz/die NIC gehört.
- Der Speicher und die vCPU für den VPX müssen an dieselbe NUMA-Domäne angeheftet sein.
- Der Vhost-Thread muss an die CPUs in derselben NUMA-Domäne gebunden sein.

Binden Sie die virtuellen Host-Threads an die entsprechenden CPUs:

1. Sobald der Verkehr gestartet wurde, führen Sie den `top` Befehl auf dem Host aus.



2. Identifizieren Sie die Affinität des virtuellen Host-Prozesses (benannt als `vhost-<pid-of-qemu>`).
3. Binden Sie die vHost-Prozesse mit dem folgenden Befehl an die zuvor identifizierten physischen Kerne in der NUMA-Domäne:

```
taskset -pc <core-id> <process-id>
<!--NeedCopy-->
```

Beispiel:

```
taskset -pc 12 29838
<!--NeedCopy-->
```


4. Die Prozessorkerne, die der NUMA-Domäne entsprechen, können mit dem folgenden Befehl identifiziert werden:

```
[root@localhost ~]# virsh capabilities | grep cpu
<cpu>
    </cpu>
        <cpus num='8'>
            <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
            <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
            <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
            <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
            <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
            <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
            <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
            <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
        </cpus>

        <cpus num='8'>
        <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
        <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
        <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
        <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
        <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
        <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
        <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
        <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
        </cpus>

    <cpuselection/>
    <cpuselection/>

<!--NeedCopy-->
```

Binden Sie den QEMU-Prozess an den entsprechenden physikalischen Kern:

1. Identifizieren Sie die physikalischen Kerne, auf denen der QEMU-Prozess läuft. Weitere Informationen finden Sie in der vorhergehenden Ausgabe.
2. Binden Sie den QEMU-Prozess mit dem folgenden Befehl an dieselben physikalischen Kerne, an die Sie die vCPUs binden:

```
taskset -pc 8-11 29824
<!--NeedCopy-->
```


NetScaler VPX mit SR-IOV und Fortville PCIe Passthrough-Netzwerkschnittstellen

Gehen Sie folgendermaßen vor, um eine optimale Leistung der SR-IOV- und Fortville PCIe-Passthrough-Netzwerkschnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz/die NIC gehört.
- Der Speicher und die vCPU für den VPX müssen an dieselbe NUMA-Domäne angeheftet sein.

Beispiel für eine VPX-XML-Datei für vCPU und Speicher-Pinning für Linux KVM:

```
    <domain type='kvm'>
        <name>NetScaler-VPX</name>
        <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
        <memory unit='KiB'>8097152</memory>
        <currentMemory unit='KiB'>8097152</currentMemory>
        <vcpu placement='static'>4</vcpu>

    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>

    <numatune>
    <memory mode='strict' nodeset='1'/>
    </numatune>

    </domain>
<!--NeedCopy-->
```

NetScaler VPX-Instanz auf Citrix Hypervisors

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie andere Vorschläge, mit denen Sie eine optimale Leistung der NetScaler VPX-Instanz auf Citrix Hypervisors erzielen können.

- Leistungseinstellungen für Citrix Hypervisors
- NetScaler VPX mit SR-IOV-Netzwerkschnittstellen
- NetScaler VPX mit paravirtualisierten Schnittstellen

Leistungseinstellungen für Citrix Hypervisors

Finden Sie die NUMA-Domäne der NIC mit dem Befehl “xl”:


```
xl info -n
<!--NeedCopy-->
```

Pin vCPUs von VPX an physische Kerne.

```
xl vcpu-pin <Netsclaer VM Name>  <vCPU id>  <physical CPU id>
<!--NeedCopy-->
```

Überprüfen Sie die Bindung von vCPUs.

```
xl vcpu-list
<!--NeedCopy-->
```

Weisen Sie NetScaler VMs mehr als 8 vCPUs zu.

Führen Sie zum Konfigurieren von mehr als 8 vCPUs die folgenden Befehle von der Citrix Hypervisor-Konsole aus:

```
xe vm-param-set uuid=your_vms_uuid VCPUs-max=16
xe vm-param-set uuid=your_vms_uuid VCPUs-at-startup=16
<!--NeedCopy-->
```

NetScaler VPX mit SR-IOV-Netzwerkschnittstellen

Gehen Sie folgendermaßen vor, um eine optimale Leistung der SR-IOV-Netzwerkschnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, an die der PCIe-Steckplatz oder die NIC gebunden ist.
- Stecken Sie den Speicher und die vCPU für den VPX an dieselbe NUMA-Domäne an.
- Binden Sie die Domain-0 vCPU an die verbleibende CPU.

NetScaler VPX mit paravirtualisierten Schnittstellen

Für eine optimale Leistung werden zwei vNICs pro pNIC und eine vNIC pro pNIC-Konfiguration empfohlen, wie in anderen PV-Umgebungen.

Gehen Sie folgendermaßen vor, um eine optimale Leistung paravirtualisierter (Netfront) Schnittstellen zu erzielen:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz oder die NIC gehört.
- Stecken Sie den Speicher und die vCPU für den VPX an dieselbe NUMA-Domäne an.
- Binden Sie die Domain-0 vCPU an die verbleibende CPU derselben NUMA-Domäne.
- Pin Host Rx/Tx-Threads von vNIC an Domain-0 vCPUs.

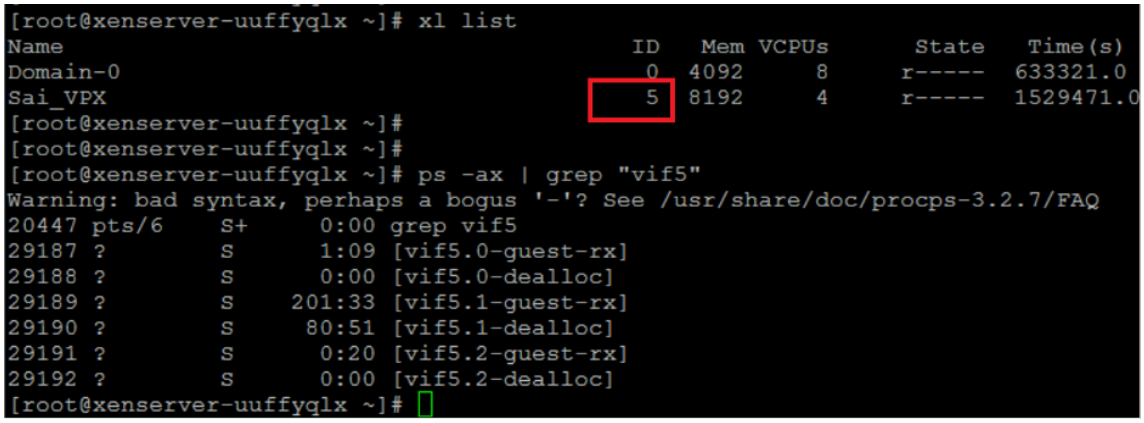
Host-Threads an Domain-0 vCPUs anheften:

1. Suchen Sie die Xen-ID des VPX mithilfe des `xl list` Befehls auf der Citrix Hypervisor Hostshell.
2. Identifizieren Sie Host-Threads mithilfe des folgenden Befehls:

```
ps -ax | grep vif <Xen-ID>
<!--NeedCopy-->
```

Im folgenden Beispiel zeigen diese Werte an:

- **vif5.0** — Die Threads für die erste Schnittstelle, die VPX in XenCenter (Verwaltungsschnittstelle) zugewiesen ist.
- **vif5.1** — Die Threads für die zweite Schnittstelle, die VPX usw. zugewiesen ist.



3. Stecken Sie die Threads mit dem folgenden Befehl an Domain-0 vCPUs an:

```
taskset -pc <core-id> <process-id>
<!--NeedCopy-->
```

Beispiel:

```
taskset -pc 1 29189
<!--NeedCopy-->
```

NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance in der Cloud anwenden

June 19, 2023

Sie können die NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance in einer Cloud-Umgebung anwenden. Diese Phase wird in diesem Dokument als **Preboot-Phase** behandelt.

Daher wird in bestimmten Fällen wie der ADC-gepoolten Lizenzierung eine bestimmte VPX-Instanz in viel geringerer Zeit aufgebracht. Diese Funktion ist in Microsoft Azure, Google Cloud-Plattform und AWS-Clouds verfügbar.

Was sind Benutzerdaten

Wenn Sie eine VPX-Instanz in einer Cloud-Umgebung bereitstellen, haben Sie die Möglichkeit, Benutzerdaten an die Instanz zu übergeben. Mit den Benutzerdaten können Sie allgemeine automatisierte Konfigurationsaufgaben ausführen, das Startverhalten von Instanzen anpassen und Skripts ausführen, nachdem die Instanz gestartet wurde. Beim ersten Start führt die NetScaler VPX-Instanz die folgenden Aufgaben aus:

- Liest die Benutzerdaten.
- Interpretiert die in Benutzerdaten bereitgestellte Konfiguration.
- Wendet die neu hinzugefügte Konfiguration beim Booten an.

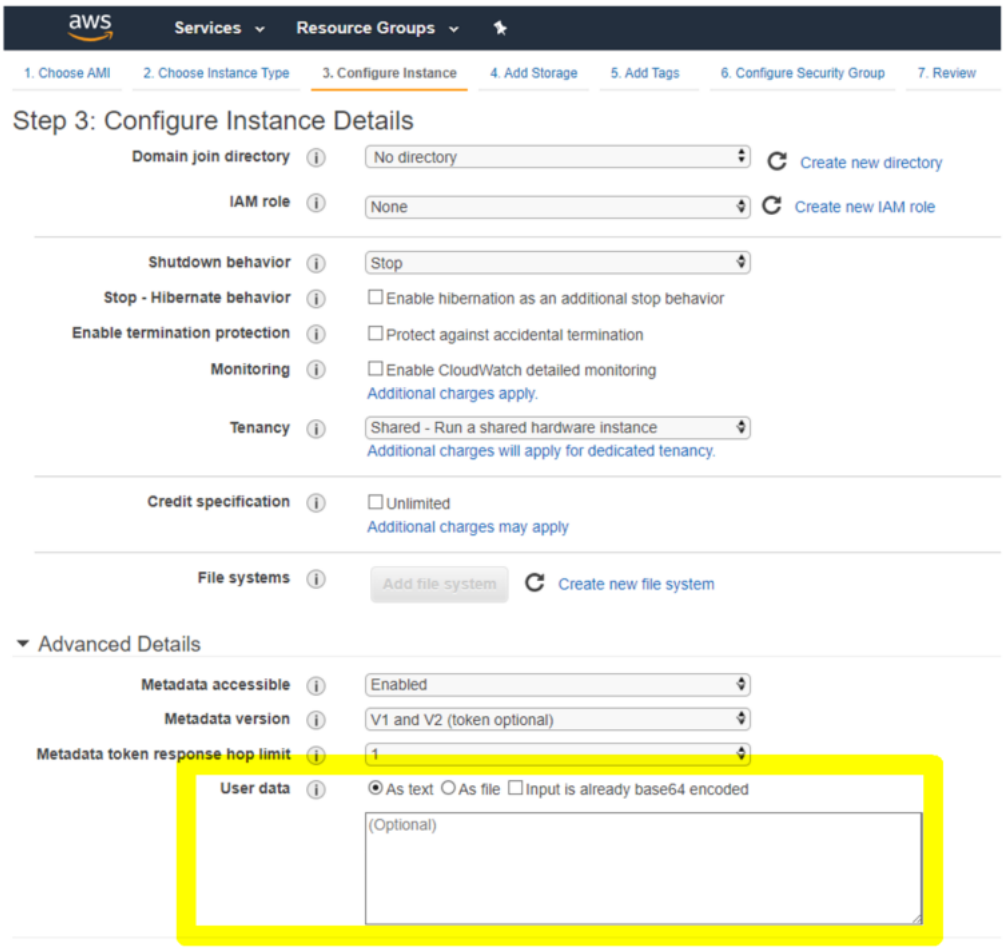
So stellen Sie Preboot-Benutzerdaten in Cloud-Instanz zur Verfügung

Sie können der Cloud-Instanz Preboot-Benutzerdaten im XML-Format zur Verfügung stellen. Verschiedene Clouds haben unterschiedliche Schnittstellen zur Bereitstellung von Benutzerdaten.

Bereitstellung von Preboot-Benutzerdaten über die AWS-Konsole

Wenn Sie eine NetScaler VPX-Instanz über die AWS-Konsole bereitstellen, navigieren **Sie zu Instanzdetails konfigurieren > Erweiterte Details**und geben Sie die Preboot-Benutzerdatenkonfiguration im Feld **Benutzerdaten** an.

Ausführliche Anweisungen zu jedem der Schritte finden Sie unter Bereitstellen einer NetScaler VPX-Instanz in AWS mithilfe der AWS-Webkonsole.
Weitere Informationen finden Sie in der AWS-Dokumentation zum Starten einer Instanz.



> **Hinweis:**
>
> Der reine AWS-IMDSv2-Modus für die Preboot-Benutzerdatenfunktion wird ab NetScaler VPX Version 13.1.48.x und späteren Versionen unterstützt.

Bereitstellung von Preboot-Benutzerdaten mit AWS CLI

Geben Sie den folgenden Befehl in die AWS CLI ein:

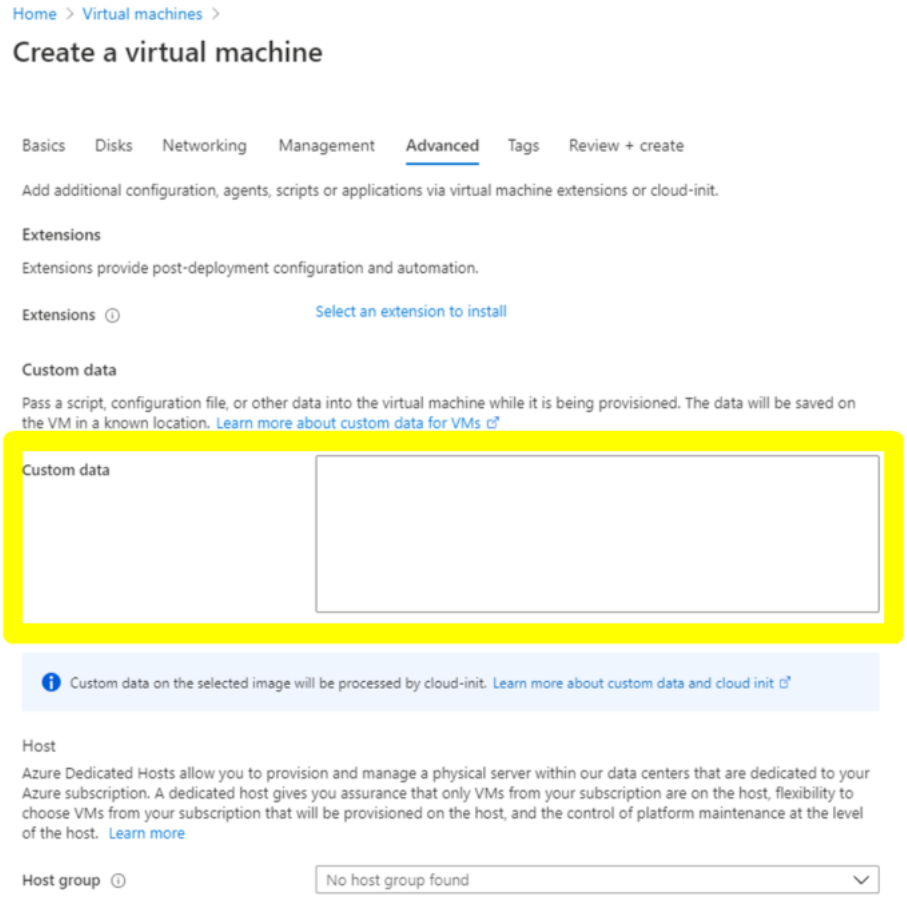
```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
<!--NeedCopy-->
```


Weitere Informationen finden Sie in der AWS-Dokumentation zu Running Instances.

Weitere Informationen finden Sie in der AWS-Dokumentation zur Verwendung von Instanz-Benutzerdaten

Stellen Sie Preboot-Benutzerdaten mit der Azure-Konsole bereit

Wenn Sie eine NetScaler VPX-Instanz mit der Azure-Konsole bereitstellen, navigieren **Sie zu Virtuelle Maschine erstellen > Erweitert** . Geben Sie im Feld **Benutzerdefinierte Daten** eine Preboot-Benutzerdatenkonfiguration an.



Bereitstellen von Preboot-Benutzerdaten mit der Azure CLI

Geben Sie den folgenden Befehl in die Azure CLI ein:

```
az vm create \
  --resource-group myResourceGroup \
  --name MyVm \
  --image debian \
  --custom-data MyCloudInitScript.txt \
```



```
<!--NeedCopy-->
```

Beispiel:

```
az vm create --resource-group MyResourceGroup -name MyVm --image debian
    --custom-data MyCloudInitScript.txt
<!--NeedCopy-->
```

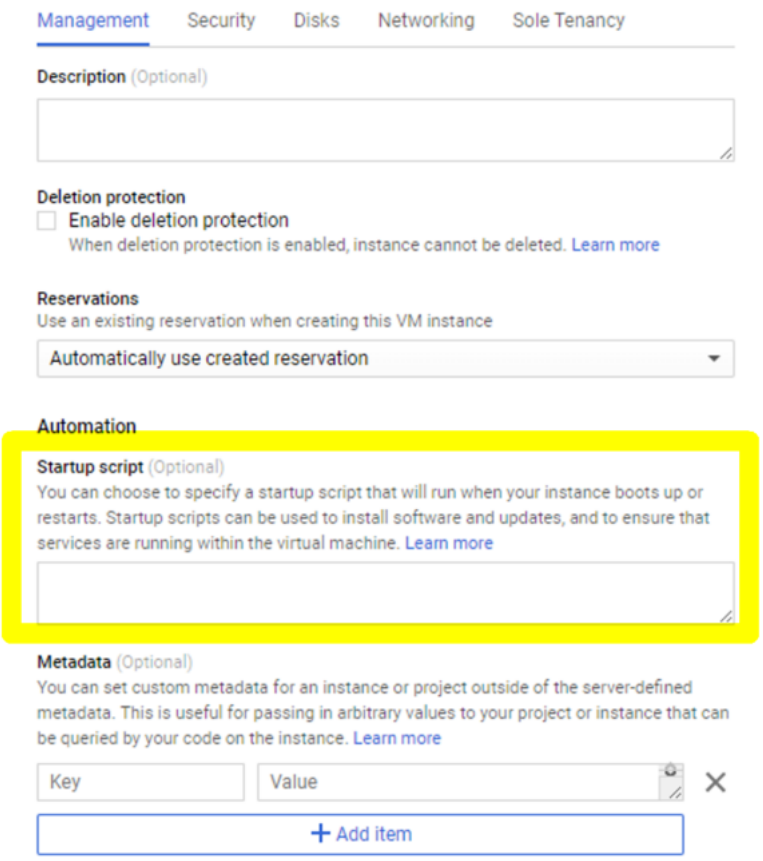
Sie können Ihre benutzerdefinierten Daten oder Preboot-Konfiguration als Datei an den Parameter "—custom-data" übergeben. In diesem Beispiel lautet der Dateiname **MyCloudInitScript.txt**.

Weitere Informationen finden Sie in der Azure CLI-Dokumentation.

Stellen Sie Preboot-Benutzerdaten mit der GCP-Konsole bereit

Wenn Sie eine NetScaler VPX-Instanz mit der GCP-Konsole bereitstellen, füllen Sie die Eigenschaften der Instanz aus. Erweitern Sie **Management, Sicherheit, Datenträger, Netzwerke, Einzelmandanten**. Navigieren Sie zur Registerkarte **Verwaltung**. Geben Sie im Abschnitt **Automatisierung** die Konfiguration der Preboot-Benutzerdaten im Feld **Startskript** ein.

Ausführliche Informationen zum Erstellen der VPX-Instanz mit GCP finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform.



Stellen Sie Preboot-Benutzerdaten mit der gcloud CLI bereit

Geben Sie den folgenden Befehl in die GCP CLI ein:

```
1 gcloud compute instances create INSTANCE_NAMES --metadata-from-file=
     startup-script=LOCAL_FILE_PATH
2 <!--NeedCopy-->
```

metadata-from-file - Liest den Wert oder die Benutzerdaten aus einer Datei, die im .

Weitere Informationen finden Sie in der gcloud CLI-Dokumentation

Preboot-Benutzerdatenformat

Die Preboot-Benutzerdaten müssen der Cloud-Instanz im XML-Format zur Verfügung gestellt werden. Die NetScaler Preboot-Benutzerdaten, die Sie während des Bootens über die Cloud-Infrastruktur bereitstellen, können die folgenden vier Abschnitte umfassen:

- NetScaler-Konfiguration wird mit dem <NS-CONFIG> Tag dargestellt.

- Benutzerdefiniertes Bootstrapping des NetScaler, der mit dem <NS-BOOTSTRAP> Tag dargestellt wird.
- Speichern von Benutzerskripten in NetScaler, dargestellt mit dem <NS-SCRIPTS> Tag.
- Gepoolte Lizenzierungskonfiguration, die mit dem <NS-LICENSE-CONFIG> Tag dargestellt wird.

Sie können die vorangegangenen vier Abschnitte in beliebiger Reihenfolge innerhalb der ADC-Preboot-Konfiguration angeben.
Stellen Sie sicher, dass Sie die in den folgenden Abschnitten gezeigten Formatierung genau befolgen, während Sie die Preboot-Benutzerdaten bereitstellen.

> Hinweis:
>
> Die gesamte Preboot-Benutzerdatenkonfiguration muss in das <NS-PRE-BOOT-CONFIG> Tag eingeschlossen sein, wie in den folgenden Beispielen gezeigt.

Beispiel 1:

```
<NS-PRE-BOOT-CONFIG>
      <NS-CONFIG>           </NS-CONFIG>
      <NS-BOOTSTRAP>        </NS-BOOTSTRAP>
      <NS-SCRIPTS>          </NS-SCRIPTS>
      <NS-LICENSE-CONFIG>   </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Beispiel 2:

```
<NS-PRE-BOOT-CONFIG>
    <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
    <NS-SCRIPTS>        </NS-SCRIPTS>
    <NS-BOOTSTRAP>      </NS-BOOTSTRAP>
    <NS-CONFIG>         </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Verwenden Sie das <NS-CONFIG> Tag, um die spezifischen NetScaler VPX-Konfigurationen bereitzustellen, die im Preboot-Stadium auf die VPX-Instanz angewendet werden müssen.

> HINWEIS:
>
> Der <NS-CONFIG> Abschnitt muss über gültige ADC CLI-Befehle verfügen. Die CLIs werden nicht auf die syntaktischen Fehler oder das Format überprüft.

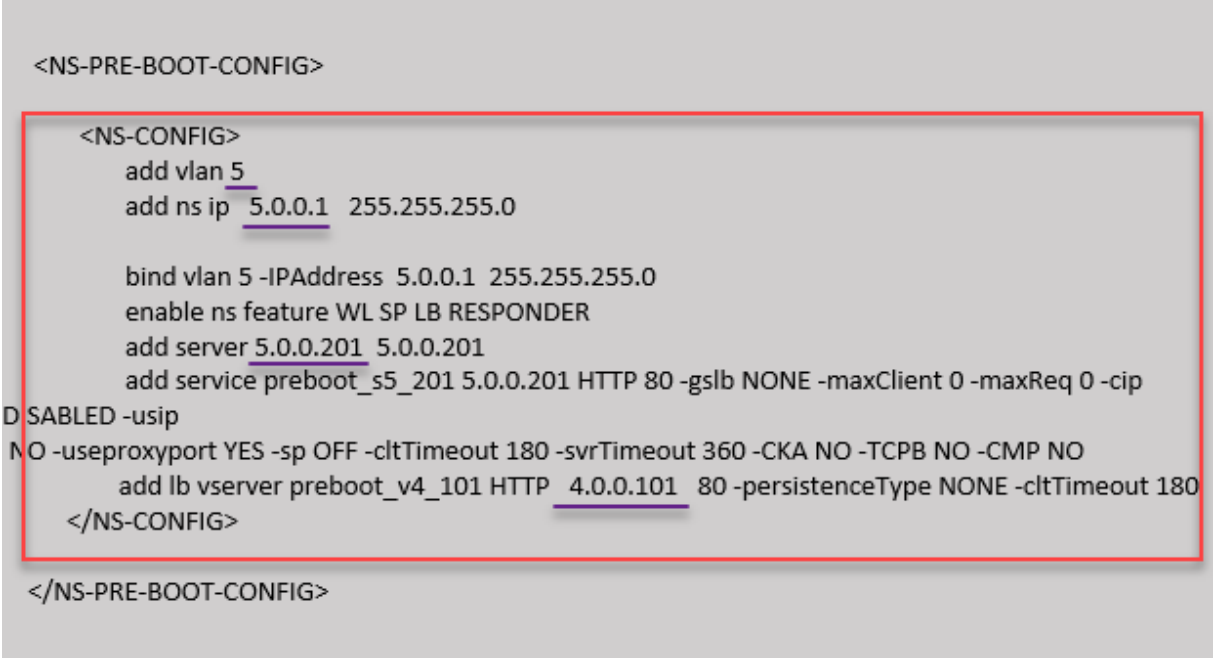
NetScaler-Konfigurationen

Verwenden Sie das <NS-CONFIG> Tag, um die spezifischen NetScaler VPX-Konfigurationen bereitzustellen, die im Preboot-Stadium auf die VPX-Instanz angewendet werden müssen.

> HINWEIS:
>
> Der <NS-CONFIG> Abschnitt muss über gültige ADC CLI-Befehle verfügen. Die CLIs werden nicht auf die syntaktischen Fehler oder das Format überprüft.

Beispiel:

Im folgenden Beispiel enthält der <NS-CONFIG> Abschnitt die Details der Konfigurationen. Ein VLAN der ID '5' ist konfiguriert und an das SNIP gebunden (5.0.0.1). Ein virtueller Lastenausgleichsserver (4.0.0.101) ist ebenfalls konfiguriert.



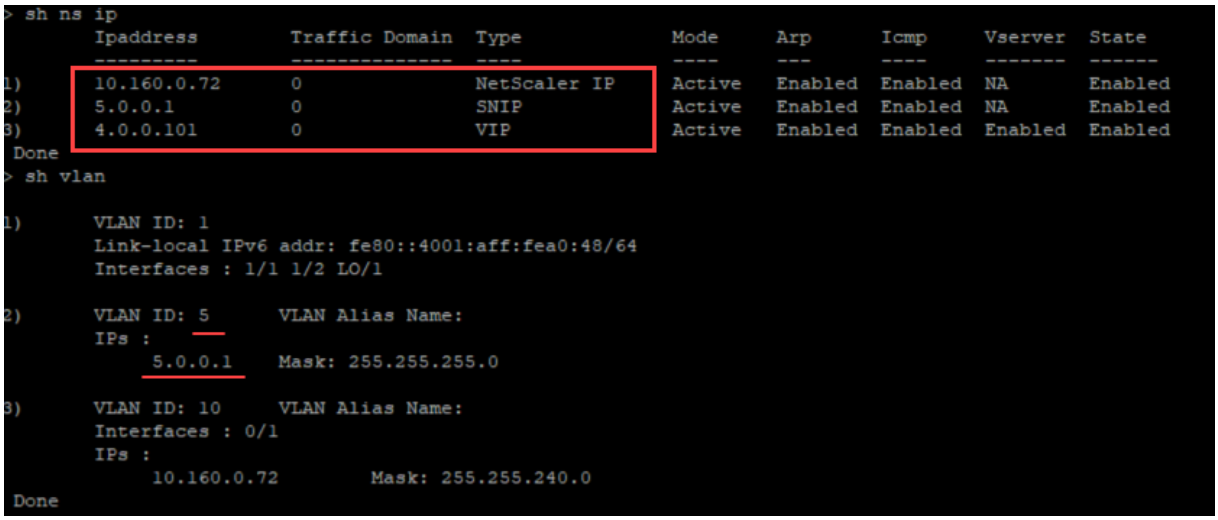
Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

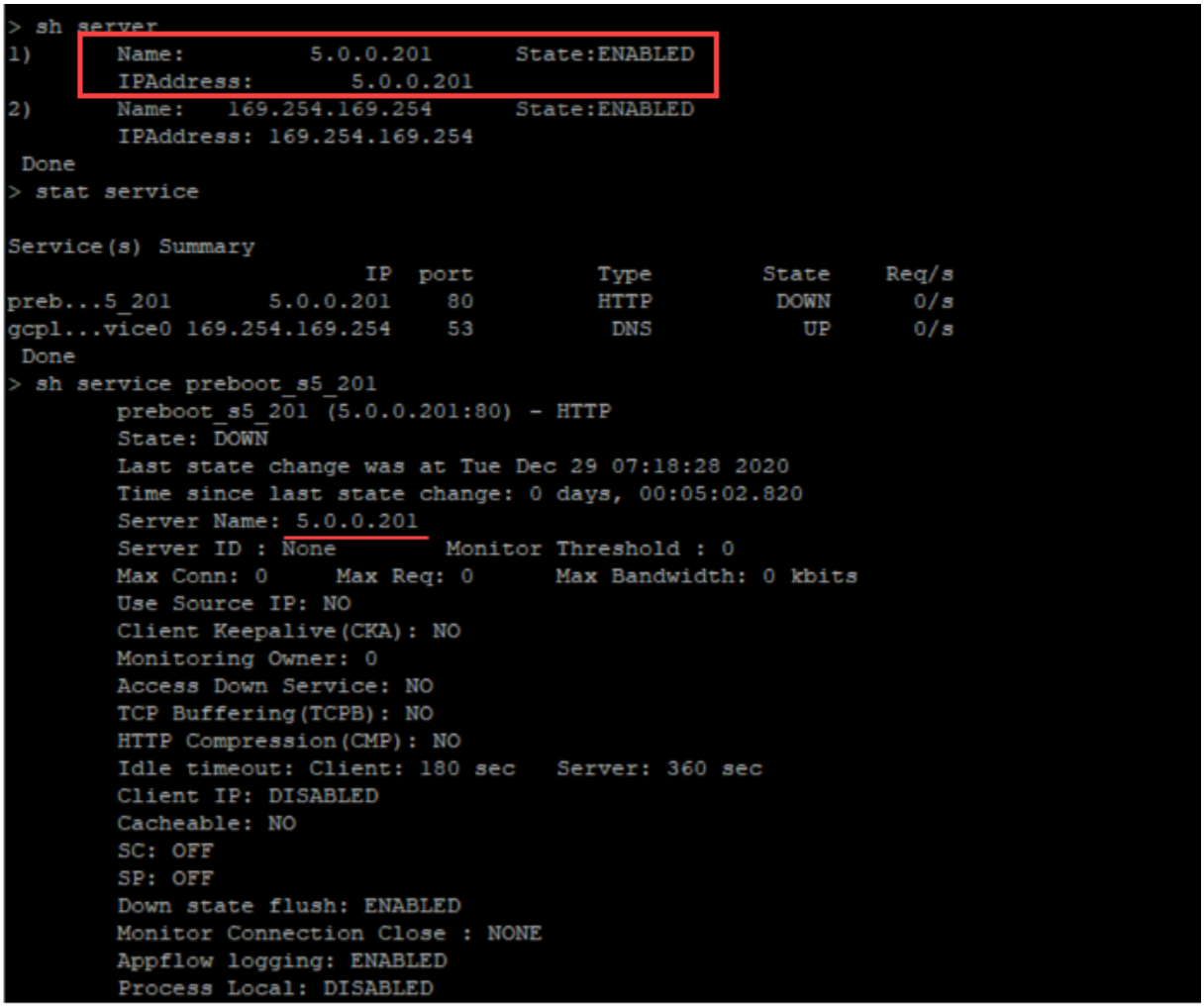
```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>
         add vlan 5
         add ns ip 5.0.0.1 255.255.255.0
         bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
         enable ns feature WL SP LB RESPONDER
         add server 5.0.0.201 5.0.0.201
         add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip
 NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -
    TCPB NO -CMP NO
```



```
10          add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
               persistenceType NONE -cltTimeout 180
11       </NS-CONFIG>
12  </NS-PRE-BOOT-CONFIG>
13  <!--NeedCopy-->
```

Die NetScaler VPX-Instanz enthält die im <NS-CONFIG> Abschnitt angewendete Konfiguration, wie in den folgenden Abbildungen gezeigt.





Benutzer-Skripts

Verwenden Sie das <NS-SCRIPTS> Tag, um jedes Skript bereitzustellen, das in der NetScaler VPX-Instanz gespeichert und ausgeführt werden muss.

Sie können viele Skripts in das <NS-SCRIPTS> Tag aufnehmen. Jedes Skript muss in das <SCRIPT> Tag aufgenommen sein.
Jeder <SCRIPT> Abschnitt entspricht einem Skript und enthält alle Details des Skripts unter Verwendung der folgenden Sub-Tags.

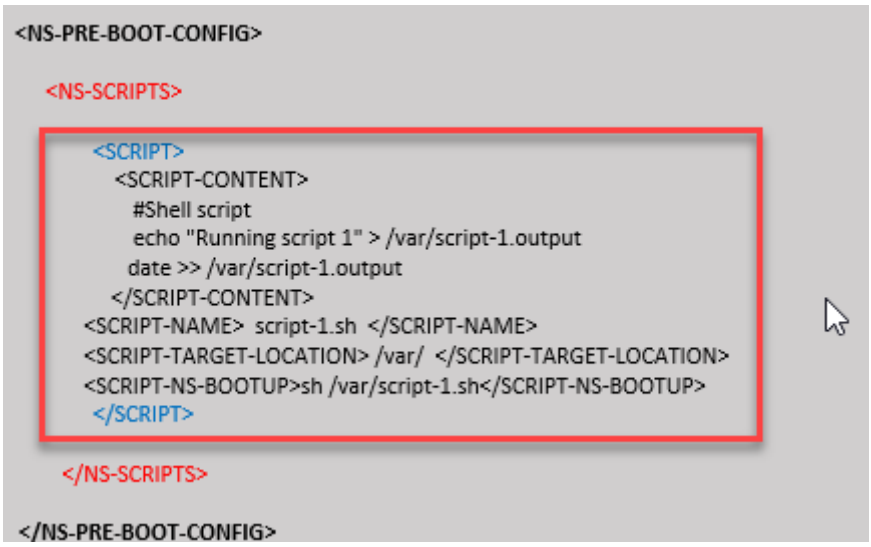
- **<SCRIPT-NAME>:** Gibt den Namen der Skriptdatei an, die gespeichert werden muss.
- **<SCRIPT-CONTENT>:** Gibt den Inhalt der Datei an, die gespeichert werden muss.
- **<SCRIPT-TARGET-LOCATION>:** Gibt den angegebenen Zielspeicherort an, an dem diese Datei gespeichert werden muss. Wenn der Zielspeicherort nicht angegeben wird, wird die Datei oder das Skript standardmäßig im Verzeichnis "/nsconfig" gespeichert.
- **<SCRIPT-NS-BOOTUP>:** Geben Sie die Befehle an, die Sie zum Ausführen des Skripts verwen-

den.

- Wenn Sie den <SCRIPT-NS-BOOTUP> Abschnitt verwenden, werden die in diesem Abschnitt bereitgestellten Befehle in “/nsconfig/nsafter.sh” gespeichert, und die Befehle werden ausgeführt, nachdem die Paket-Engine im Rahmen der Ausführung “nsafter.sh” hochgefahren ist.
- Wenn Sie den <SCRIPT-NS-BOOTUP> Abschnitt nicht verwenden, wird die Skriptdatei an dem von Ihnen angegebenen Zielspeicherort gespeichert.

Beispiel 1:

In diesem Beispiel enthält das <NS-SCRIPTS> Tag Details zu nur einem Skript: script-1.sh. Das “script-1.sh” -Skript wird im Verzeichnis “/var” gespeichert. Das Skript wird mit dem angegebenen Inhalt gefüllt und nach dem Hochfahren der Paket-Engine mit dem Befehl “sh /var/script-1.sh” ausgeführt.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

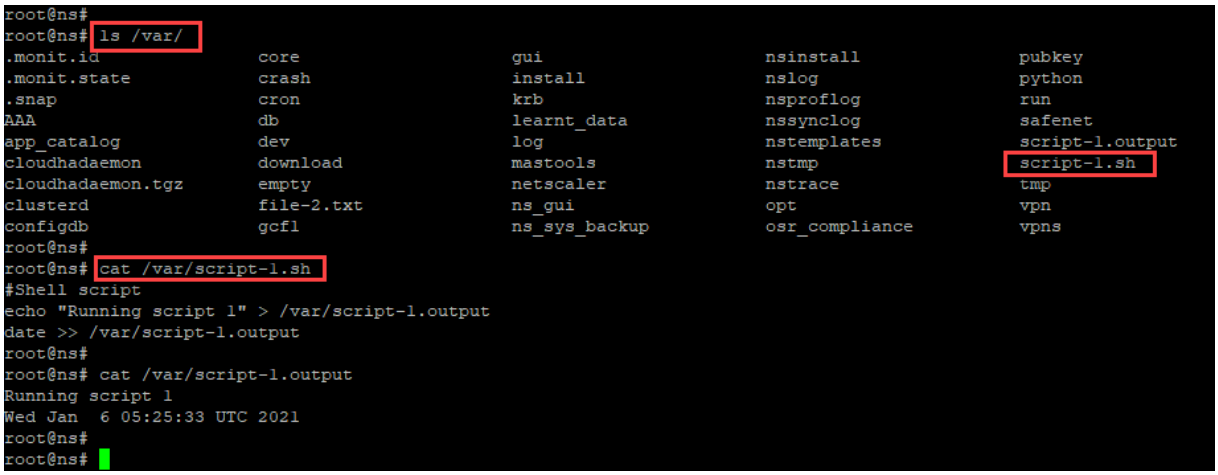
```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
    <SCRIPT>
            <SCRIPT-CONTENT>
                #Shell script
                echo "Running script 1" > /var/script-1.output
                date >> /var/script-1.output
            </SCRIPT-CONTENT>

                <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>
                <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-LOCATION
                    >
                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP
                    >
        </SCRIPT>
```



```
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

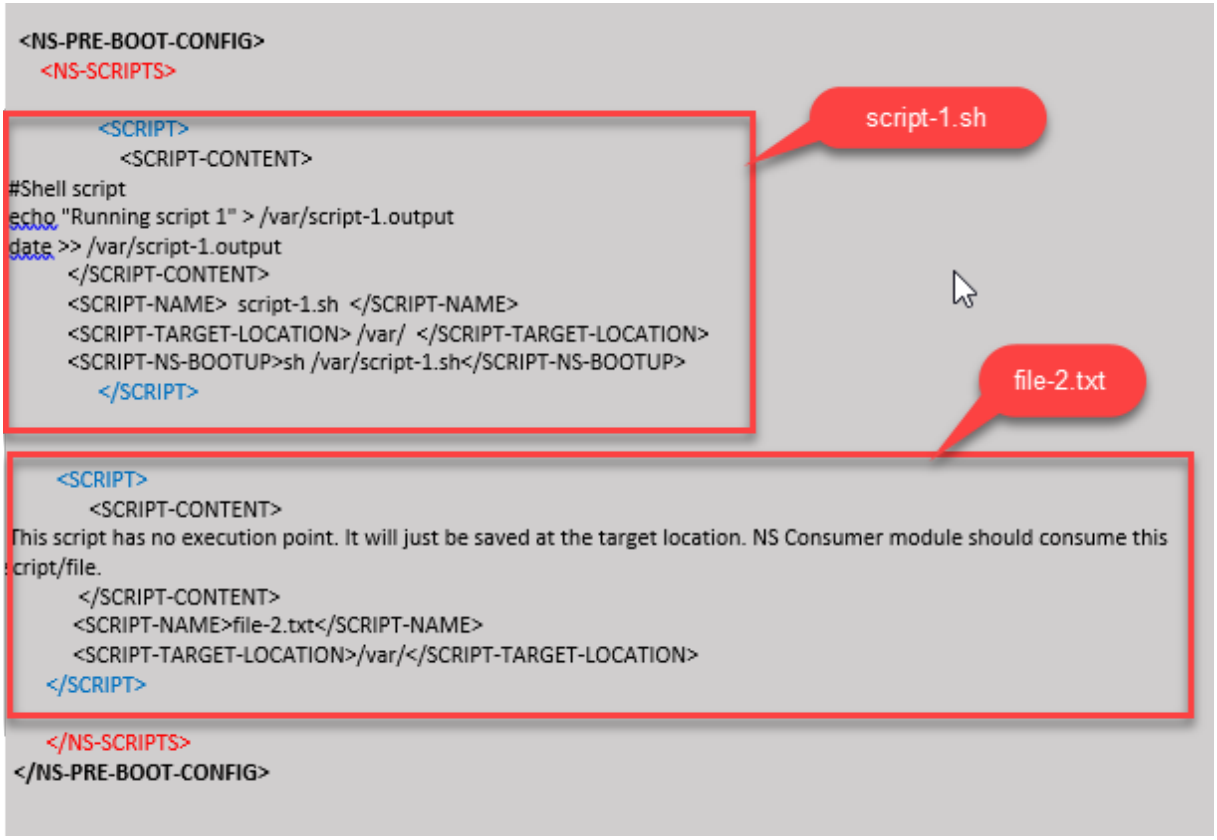
Im folgenden Snapshot können Sie überprüfen, ob das “script-1.sh” -Skript im Verzeichnis “/var/” gespeichert ist. Das “Script-1.sh” -Skript wird ausgeführt und die Ausgabedatei wird entsprechend erstellt.



Beispiel 2:

Im folgenden Beispiel enthält das <NS-SCRIPTS> Tag Details zu zwei Skripten.

- Das erste Script wird als “script-1.sh” im Verzeichnis “/var” gespeichert. Das Skript wird mit dem angegebenen Inhalt gefüllt und nach dem Hochfahren der Paket-Engine mit dem Befehl “sh /var/script-1.sh” ausgeführt.
- Das zweite Script wird als “file-2.txt” im Verzeichnis “/var” gespeichert. Diese Datei wird mit dem angegebenen Inhalt gefüllt. Es wird jedoch nicht ausgeführt, da der Bootup-Ausführungsbefehl nicht bereitgestellt <SCRIPT-NS-BOOTUP> wird.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
        <SCRIPT>
            <SCRIPT-CONTENT>
               #Shell script
               echo "Running script 1" > /var/script-1.output
               date >> /var/script-1.output
            </SCRIPT-CONTENT>

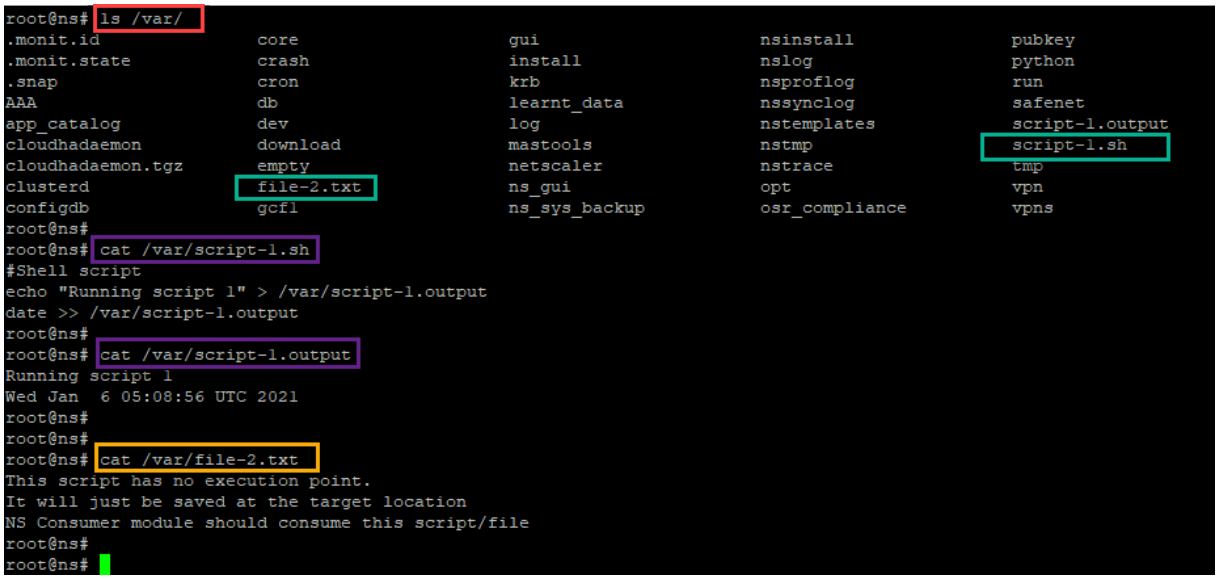
            <SCRIPT-NAME>  script-1.sh  </SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION> /var/  </SCRIPT-TARGET-LOCATION>
            <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
            </SCRIPT>

        <SCRIPT>
            <SCRIPT-CONTENT>
                This script has no execution point.
                It will just be saved at the target location
                NS Consumer module should consume this script/file
            </SCRIPT-CONTENT>
```



```
            <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Im folgenden Snapshot können Sie überprüfen, ob script-1.sh und file-2.txt im Verzeichnis "/var/" erstellt wurden. Die Script-1.sh wird ausgeführt und die Ausgabedatei wird entsprechend erstellt.



Lizenzierung

Verwenden Sie das <NS-LICENSE-CONFIG> Tag, um die gepoolte NetScaler-Lizenzierung anzuwenden, während Sie die VPX-Instanz hochfahren. Verwenden Sie das <LICENSE-COMMANDS> Tag im <NS-LICENSE-CONFIG> Abschnitt, um die gepoolten Lizenzbefehle bereitzustellen. Diese Befehle müssen syntaktisch gültig sein.

Sie können die gepoolten Lizenzierungsdetails wie Lizenztyp, Kapazität und Lizenzserver im <LICENSE-COMMANDS> Abschnitt mit den standardmäßigen gepoolten Lizenzbefehlen angeben. Weitere Informationen finden Sie unter Konfigurieren der Lizenzierung der gepoolten Kapazität von NetScaler.

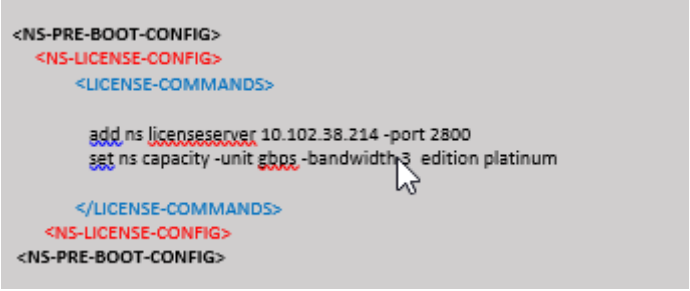
Nach dem <NS-LICENSE-CONFIG>Anwenden des wird der VPX beim Booten mit der angeforderten Edition geliefert, und VPX versucht, die konfigurierten Lizenzen vom Lizenzserver auszuchecken.

- Wenn das Auschecken der Lizenz erfolgreich ist, wird die konfigurierte Bandbreite auf VPX angewendet.
- Wenn das Auschecken der Lizenz fehlschlägt, wird die Lizenz nicht innerhalb von 10 bis 12 Minuten vom Lizenzserver abgerufen. Infolgedessen wird das System neu gestartet und

wechselt in einen nicht lizenzierten Zustand.

Beispiel:

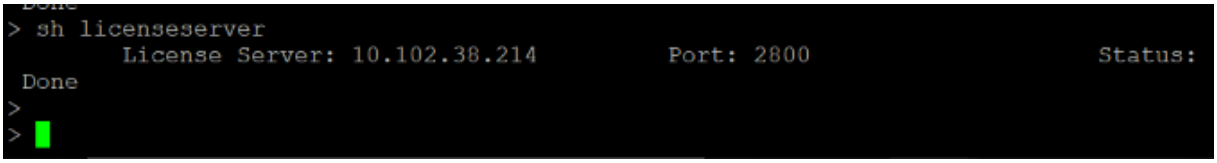
Im folgenden Beispiel wird der VPX nach dem <NS-LICENSE-CONFIG>Anwenden des beim Booten die Premium Edition bereitgestellt, und VPX versucht, die konfigurierten Lizenzen vom Lizenzserver auszuchecken (10.102.38.214).



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>
   <NS-LICENSE-CONFIG>
        <LICENSE-COMMANDS>
            add ns licenseserver 10.102.38.214 -port 2800
            set ns capacity -unit gbps -bandwidth 3  edition platinum
        </LICENSE-COMMANDS>
    </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Wie in der folgenden Abbildung gezeigt, können Sie den Befehl “show license server” ausführen und überprüfen, ob der Lizenzserver (10.102.38.214) zum VPX hinzugefügt wurde.



Bootstrapping

Verwenden Sie das <NS-BOOTSTRAP> Tag, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können die <NEW-BOOTSTRAP-SEQUENCE> Tags <SKIP-DEFAULT-BOOTSTRAP > und innerhalb des <NS-BOOTSTRAP> Abschnitts verwenden. In diesem Abschnitt wird NetScaler-Appliance darüber informiert, ob der Standard-Bootstrap vermieden werden soll oder nicht. Wenn das Standard-Bootstrapping vermieden wird, bietet Ihnen dieser Abschnitt die Möglichkeit, eine neue Bootstrapping-Sequenz bereitzustellen.

Standardmäßige Bootstrap-Konfiguration

Die Standard-Bootstrap-Konfiguration in der NetScaler-Appliance folgt diesen Schnittstellenzuweisungen:

- **Eth0** - Verwaltungsschnittstelle mit einer bestimmten NSIP-Adresse.
- **Eth1** - Clientorientierte Schnittstelle mit einer bestimmten VIP-Adresse.
- **Eth2** - Server-Schnittstelle mit einer bestimmten SNIP-Adresse.

Anpassen der Bootstrap-Konfiguration

Sie können die standardmäßige Bootstrap-Sequenz überspringen und eine neue Bootstrap-Sequenz für die NetScaler VPX-Instanz bereitstellen. Verwenden Sie das <NS-BOOTSTRAP> Tag, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können beispielsweise das Standard-Bootstrapping ändern, bei dem die Verwaltungsschnittstelle (NSIP), die clientseitige Schnittstelle (VIP) und die Serverschnittstelle (SNIP) immer in einer bestimmten Reihenfolge bereitgestellt werden.

Die folgende Tabelle zeigt das Bootstrapping-Verhalten mit den verschiedenen zulässigen Werten <SKIP-DEFAULT-BOOTSTRAP> und <NEW-BOOTSTRAP-SEQUENCE> Tags an.

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	Bootstrap-Verhalten
JA	JA	Das standardmäßige Bootstrapping-Verhalten wird übersprungen, und eine neue benutzerdefinierte Bootstrap-Sequenz im <NS-BOOTSTRAP> Abschnitt wird ausgeführt.
JA	NEIN	Das standardmäßige Bootstrapping-Verhalten wird übersprungen. Die im <NS-CONFIG> Abschnitt bereitgestellten Bootstrap-Befehle werden ausgeführt.

Sie können die Bootstrap-Konfiguration mit den folgenden drei Methoden anpassen:

- Geben Sie nur die Schnittstellendetails
- Geben Sie die Schnittstellendetails zusammen mit IP-Adressen und Subnetzmaske an

- Geben Sie Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt

Methode 1: Benutzerdefinierter Bootstrap durch Angabe nur der Schnittstellendetails

Sie geben die verwaltungs-, clientorientierten und serverorientierten Schnittstellen an, nicht jedoch deren IP-Adressen und Subnetzmasken. Die IP-Adressen und Subnetzmasken werden durch Abfragen der Cloud-Infrastruktur ausgefüllt.

Benutzerdefiniertes Bootstrap-Beispiel für AWS

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth0-Schnittstelle als Client-Schnittstelle (VIP) und Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.

```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

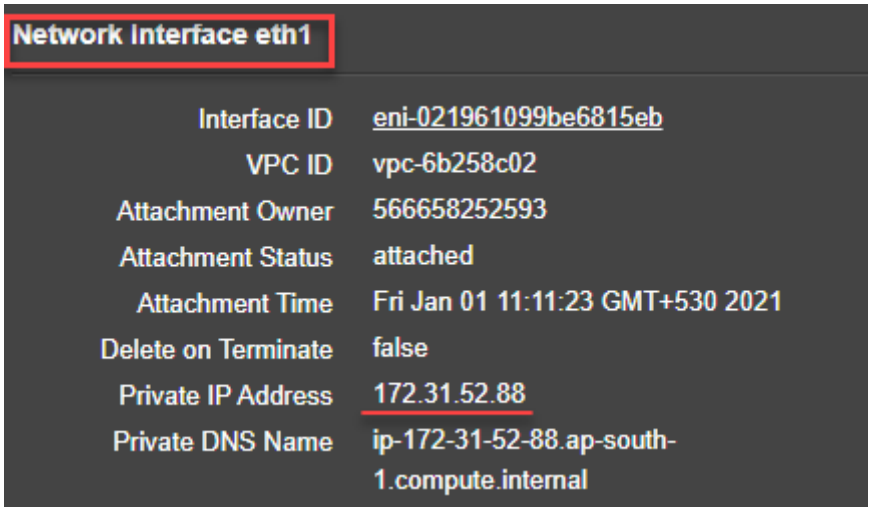
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

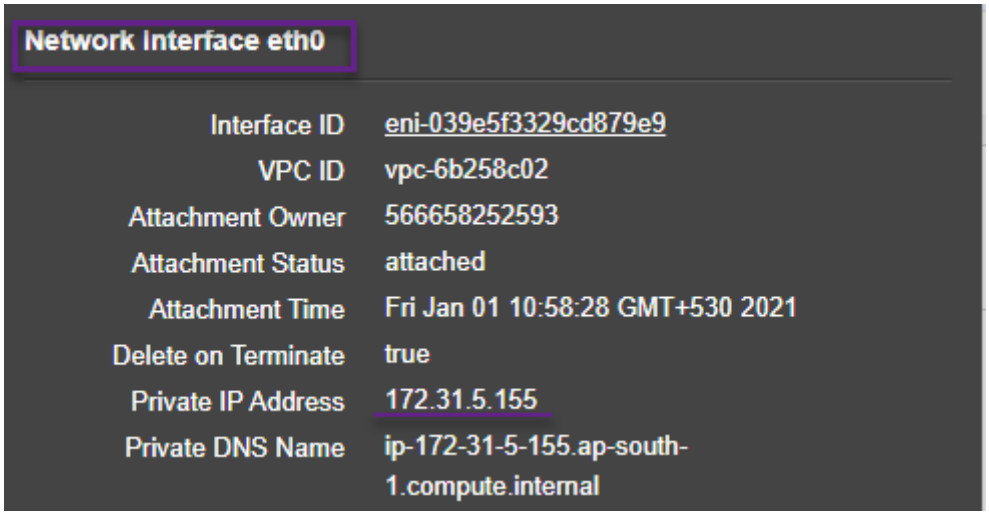
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

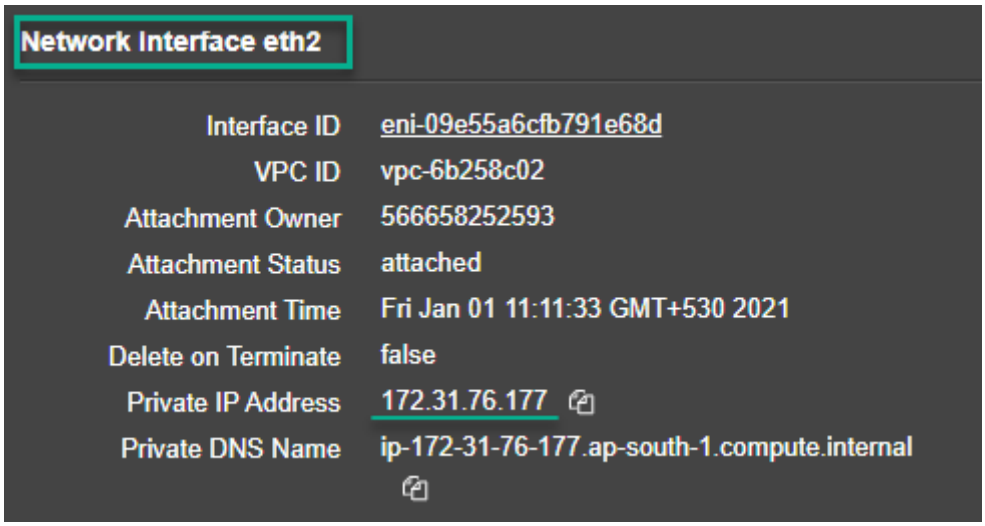
    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

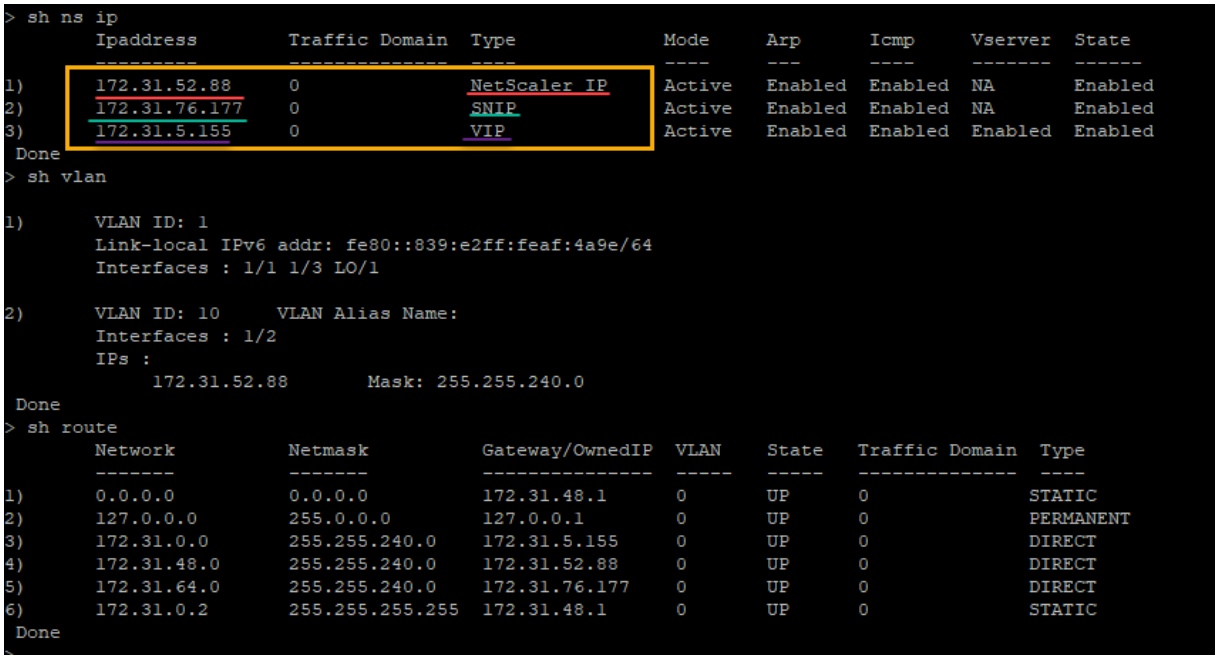
1. Navigieren Sie zum **AWS Portal > EC2-Instanzen**und wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.







Sie können den Befehl `show nsip` in der **ADC-CLI** ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
```

Benutzerdefiniertes Bootstrap-Beispiel für Azure

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Die Eth2-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth1-Schnittstelle als Client-Schnittstelle (VIP) und Eth0-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

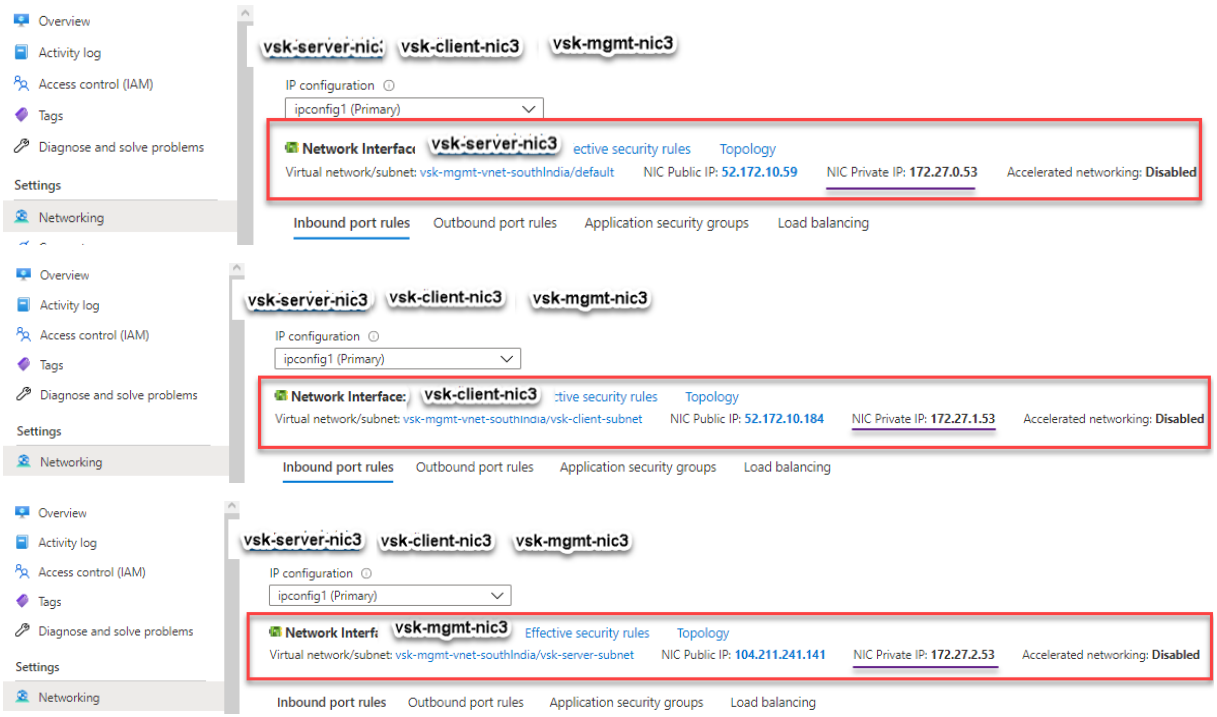
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

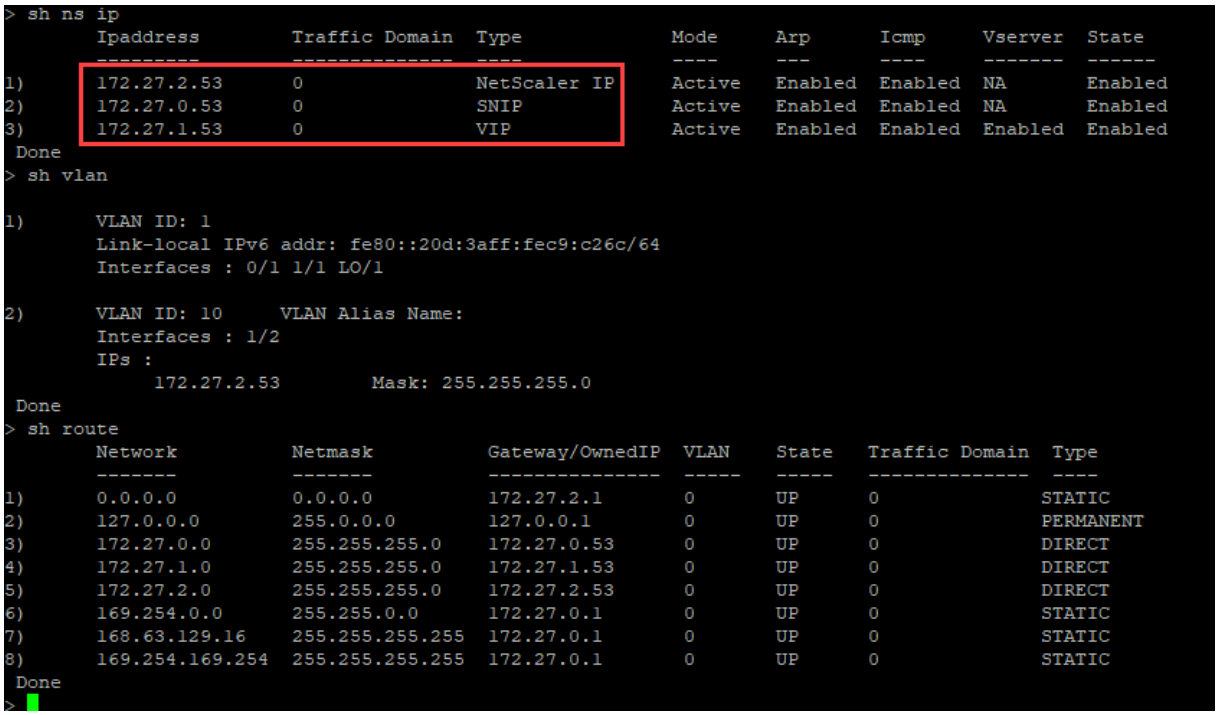
</NS-PRE-BOOT-CONFIG>
```

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.



Sie können den Befehl “show nsip” in der ADC CLI ausführen und überprüfen, ob die im <NS-

BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.



Benutzerdefinierte Bootstrap-Beispiele für GCP

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth0-Schnittstelle als Client-Schnittstelle (VIP) und Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Nachdem die VM-Instanz im GCP-Portal erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

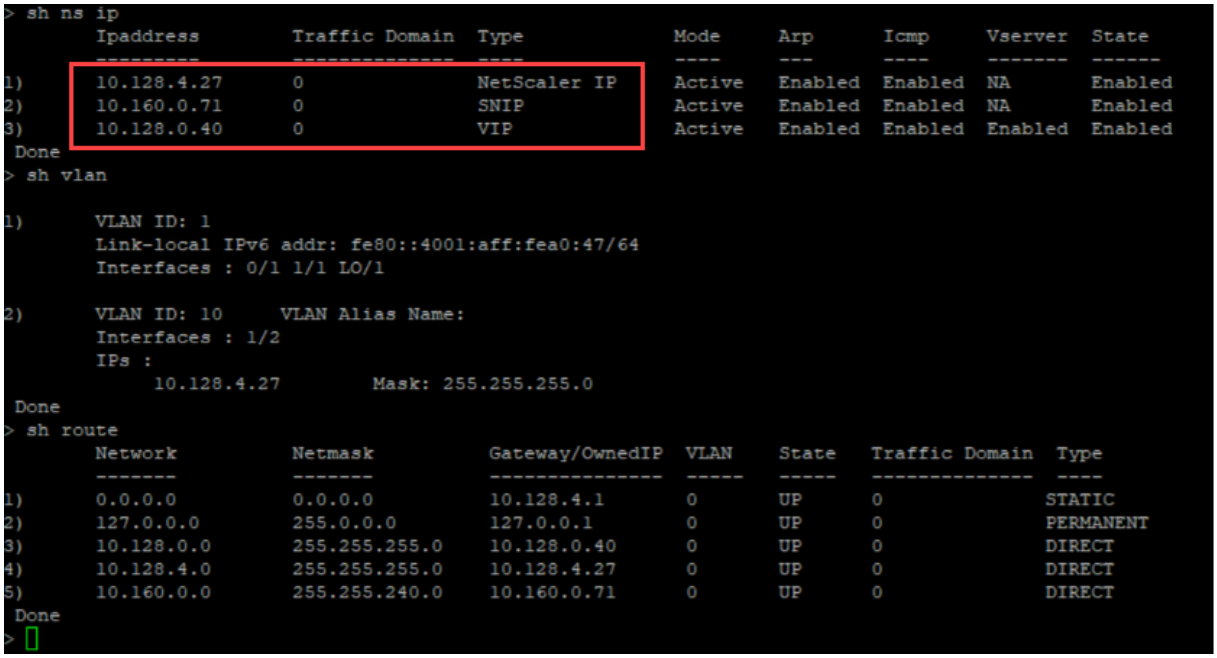
1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die NIC-Details wie folgt:

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	10.160.0.71	–	35.244.56.180 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	10.128.0.40	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.27	–	34.93.241.147 (ephemeral)	Premium		View details

Public DNS PTR Record
None

Sie können den Befehl `show nsip` in der **ADC-CLI** ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.



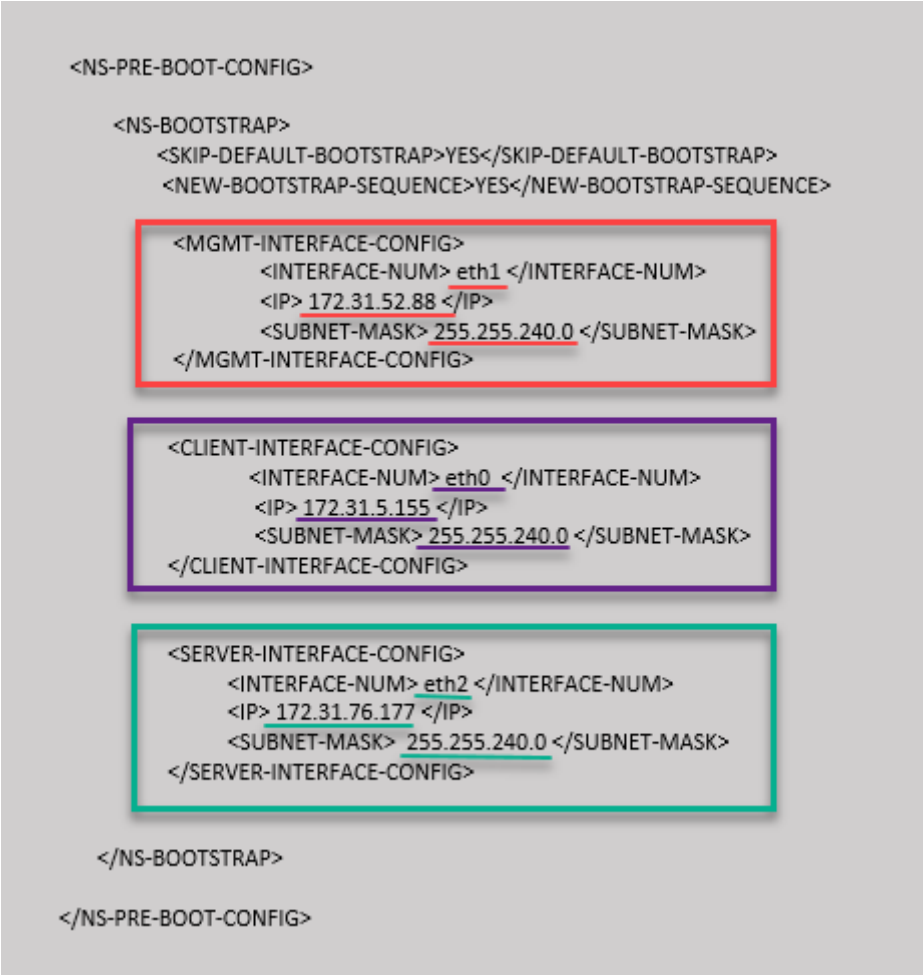
Methode 2: Benutzerdefiniertes Bootstrap durch Angabe der Schnittstellen, IP-Adressen und Subnetzmasken

Sie geben die verwaltungs-, clientorientierten und serverorientierten Schnittstellen zusammen mit ihren IP-Adressen und der Subnetzmaske an.

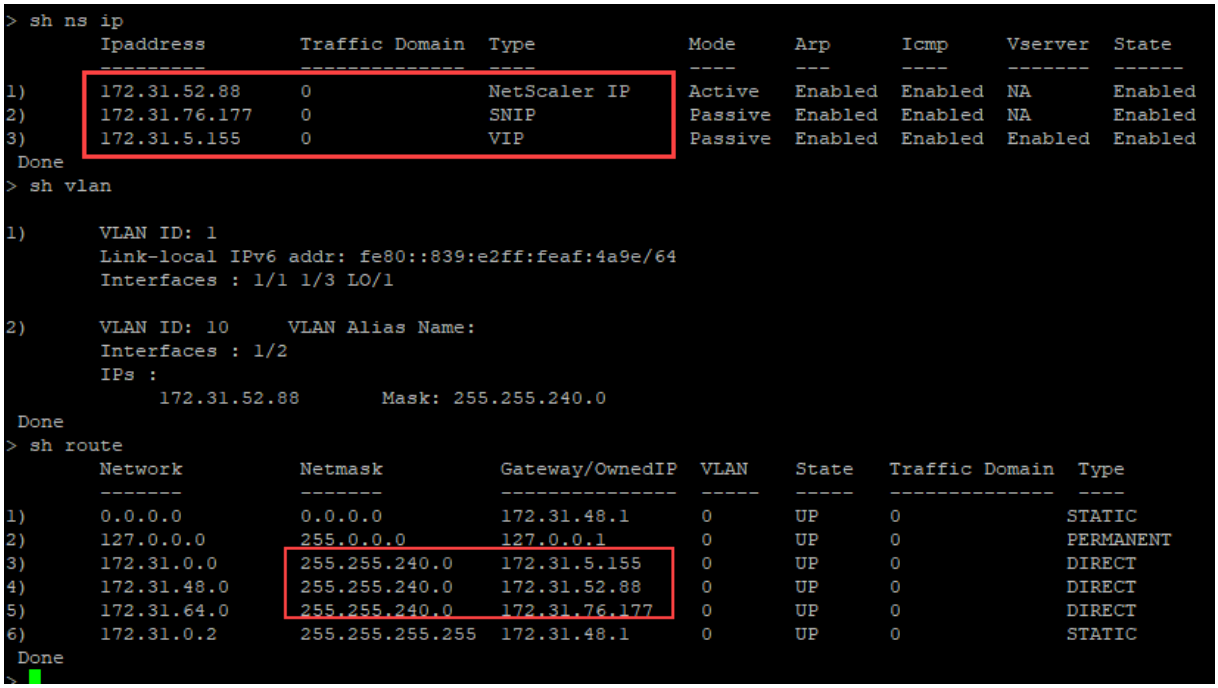
Benutzerdefinierte Bootstrap-Beispiele für AWS

Im folgenden Beispiel überspringen Sie den Standard-Bootstrap und führen eine neue Bootstrap-Sequenz für die NetScaler-Appliance aus. Für die neue Bootstrap-Sequenz geben Sie folgende Details an:

- **Verwaltungsschnittstelle:** Interface - Eth1, NSIP - 172.31.52.88 und Subnetzmaske - 255.255.240.0
- **Clientorientierte Schnittstelle:** Schnittstelle - Eth0, VIP - 172.31.5.155 und Subnetzmaske - 255.255.240.0.
- **Server-zugewandte Schnittstelle:** Schnittstelle - Eth2, SNIP - 172.31.76.177 und Subnetzmaske - 255.255.240.0.



Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im `<NS-BOOTSTRAP>` Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  -----
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Passive  Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Passive  Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Benutzerdefiniertes Bootstrap-Beispiel für Azure

Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Verwaltungsschnittstelle (eth2), NSIP (172.27.2.53) und Subnetzmaske (255.255.255.0)
- Clientorientierte Schnittstelle (eth1), VIP (172.27.1.53) und Subnetzmaske (255.255.255.0)
- Server-zugewandte Schnittstelle (eth0), SNIP (172.27.0.53) und Subnetzmaske (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 172.27.2.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>

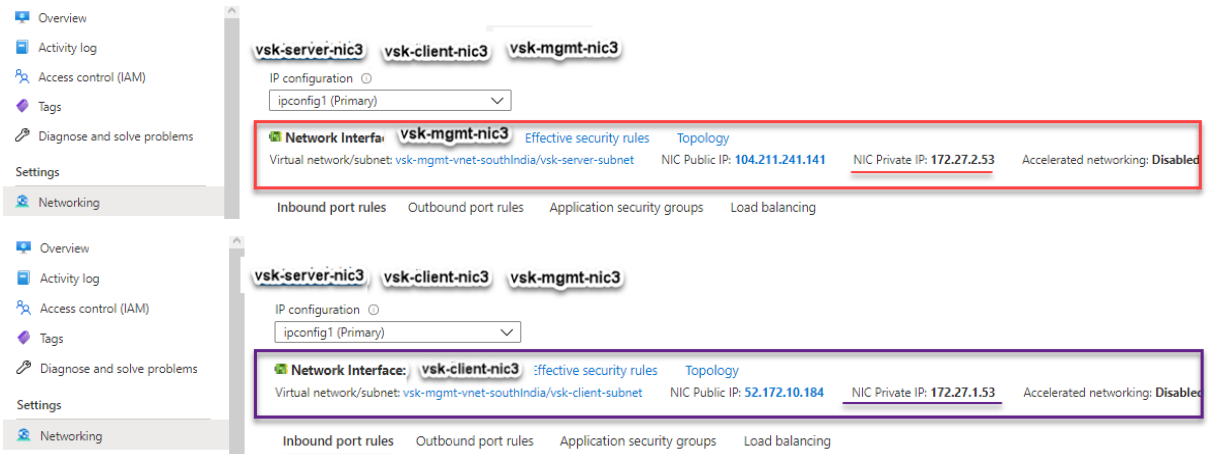
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 172.27.1.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
            </CLIENT-INTERFACE-CONFIG>

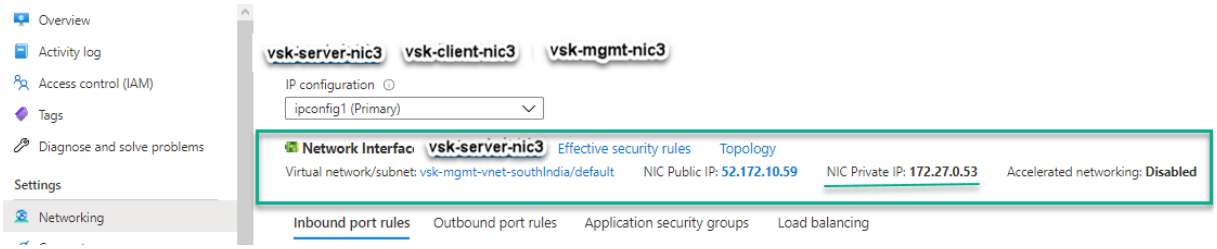
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 172.27.0.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.





Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im <NS-BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl "Route anzeigen" ausführen, um die Subnetzmaske zu überprüfen.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Benutzerdefiniertes Bootstrap-Beispiel für GCP

Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Verwaltungsschnittstelle (eth2), NSIP (10.128.4.31) und Subnetzmaske (255.255.255.0)
- Clientorientierte Schnittstelle (eth1), VIP (10.128.0.43) und Subnetzmaske (255.255.255.0)
- Server-zugewandte Schnittstelle (eth0), SNIP (10.160.0.75) und Subnetzmaske (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 10.128.4.31 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 10.128.0.43 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </CLIENT-INTERFACE-CONFIG>
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 10.160.0.75 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

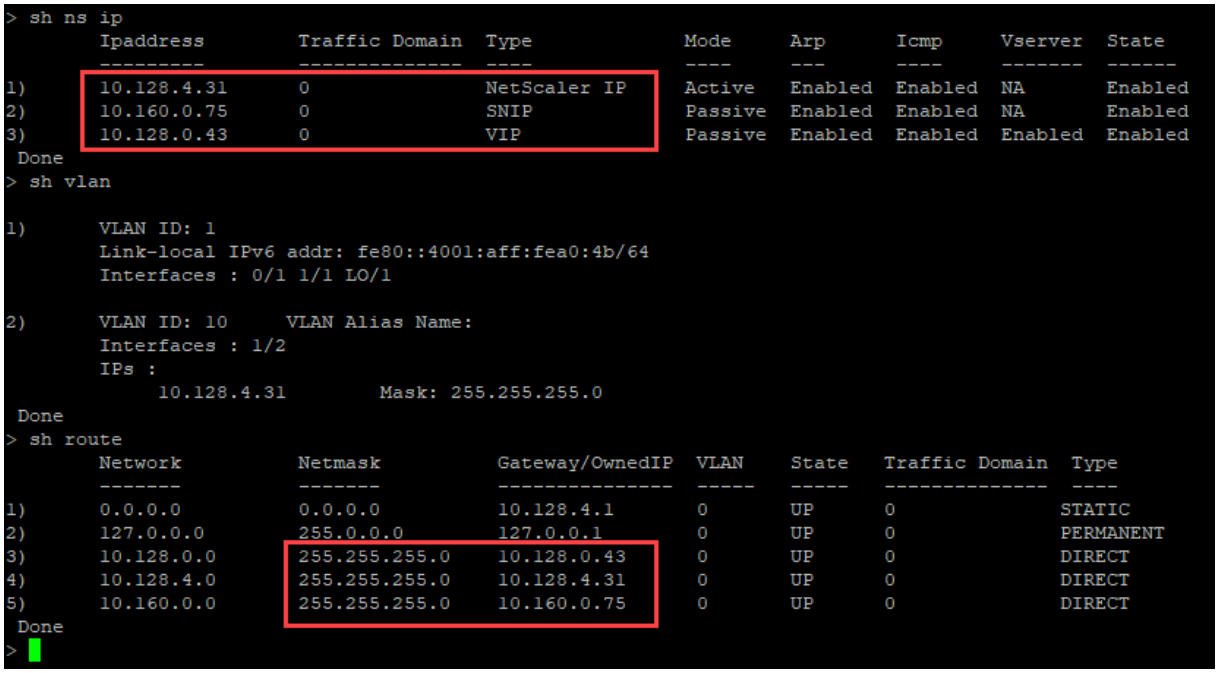
Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die Netzwerkdetails wie folgt.

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	vsk-defnw-st-ip1 (10.160.0.75)	–	34.93.216.90 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	vsk-vpc-nw1-st-ip1 (10.128.0.43)	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	vsk-nw2-st-ip-1 (10.128.4.31)	–	34.93.202.214 (ephemeral)	Premium		View details

Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im `<NS-BOOTSTRAP>` Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.



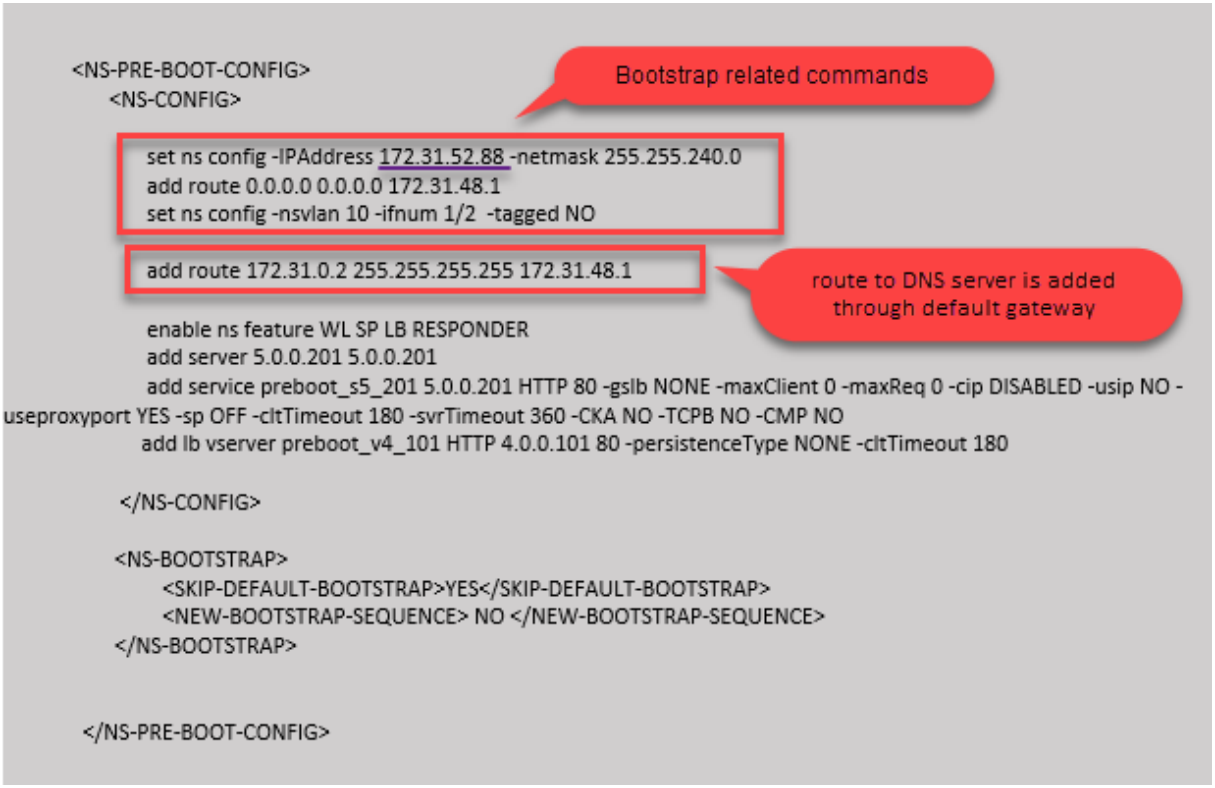
Methode 3: Benutzerdefiniertes Bootstrap durch Bereitstellung von Bootstrap-bezogenen Befehlen im <NS-CONFIG> Abschnitt

Sie können die Bootstrap-bezogenen Befehle im <NS-CONFIG> Abschnitt angeben. In <NS-BOOTSTRAP> diesem Abschnitt müssen Sie das <NEW-BOOTSTRAP-SEQUENCE> als “Nein” angeben, um die Bootstrapping-Befehle im <NS-CONFIG> Abschnitt auszuführen. Sie müssen auch die Befehle angeben, um NSIP, Standardroute und NSVLAN zuzuweisen. Geben Sie außerdem die Befehle ein, die für die von Ihnen verwendete Cloud relevant sind.

Stellen Sie vor der Bereitstellung eines benutzerdefinierten Bootstrap sicher, dass Ihre Cloud-Infrastruktur eine bestimmte Schnittstellenkonfiguration unterstützt.

Benutzerdefiniertes Bootstrap-Beispiel für AWS

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen ausgeführt werden. Sie müssen auch die Befehle zum Erstellen von NSIP, zum Hinzufügen einer Standardroute und zum Hinzufügen von NSVLAN angeben.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
        add route 0.0.0.0 0.0.0.0 172.31.48.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add route 172.31.0.2 255.255.255.255 172.31.48.1

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO - useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

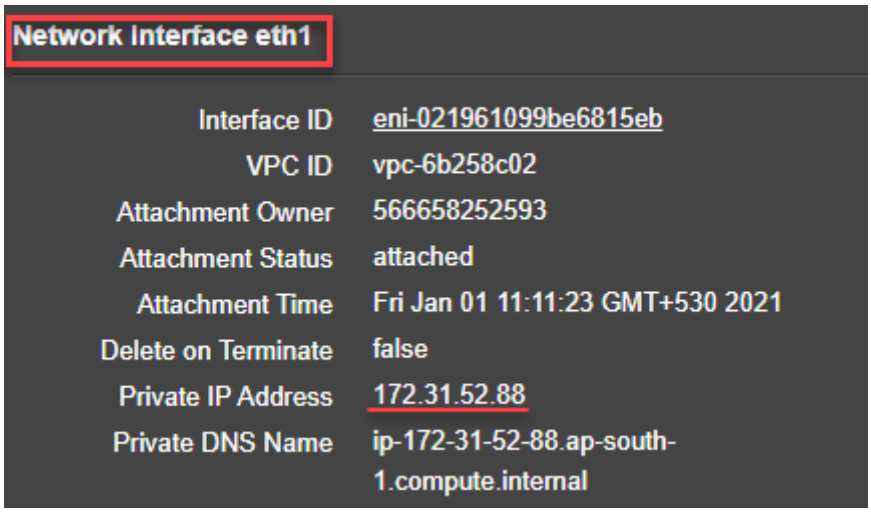
    <NS-BOOTSTRAP>
     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
```

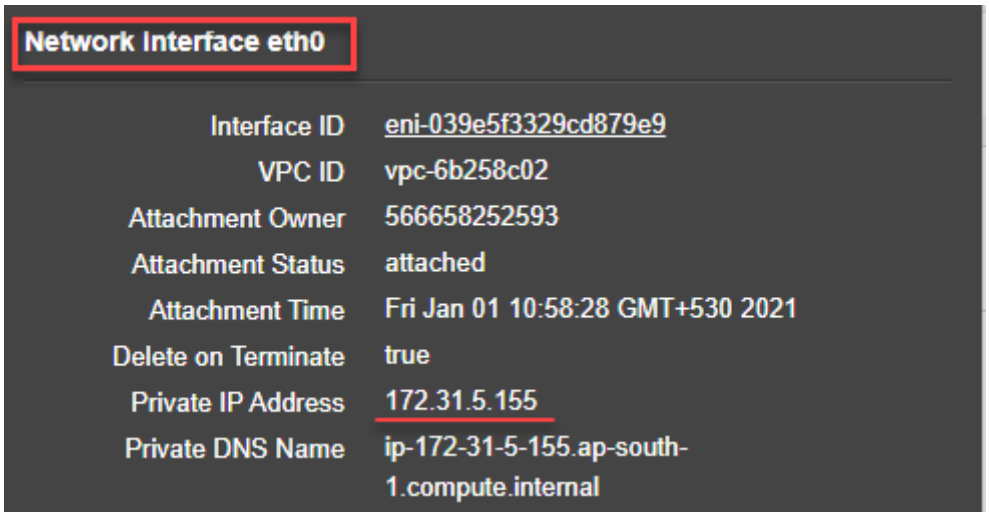


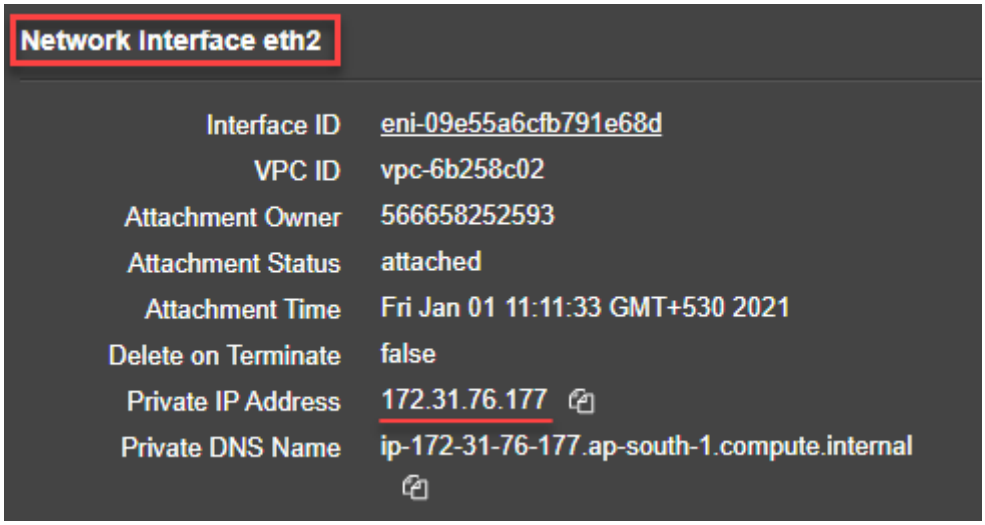
```
19      </NS-BOOTSTRAP>
20
21
22  </NS-PRE-BOOT-CONFIG>
23  <!--NeedCopy-->
```

Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Navigieren Sie zum **AWS Portal > EC2-Instanzen**und wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.







Sie können den Befehl `show nsip` in der **ADC-CLI** ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

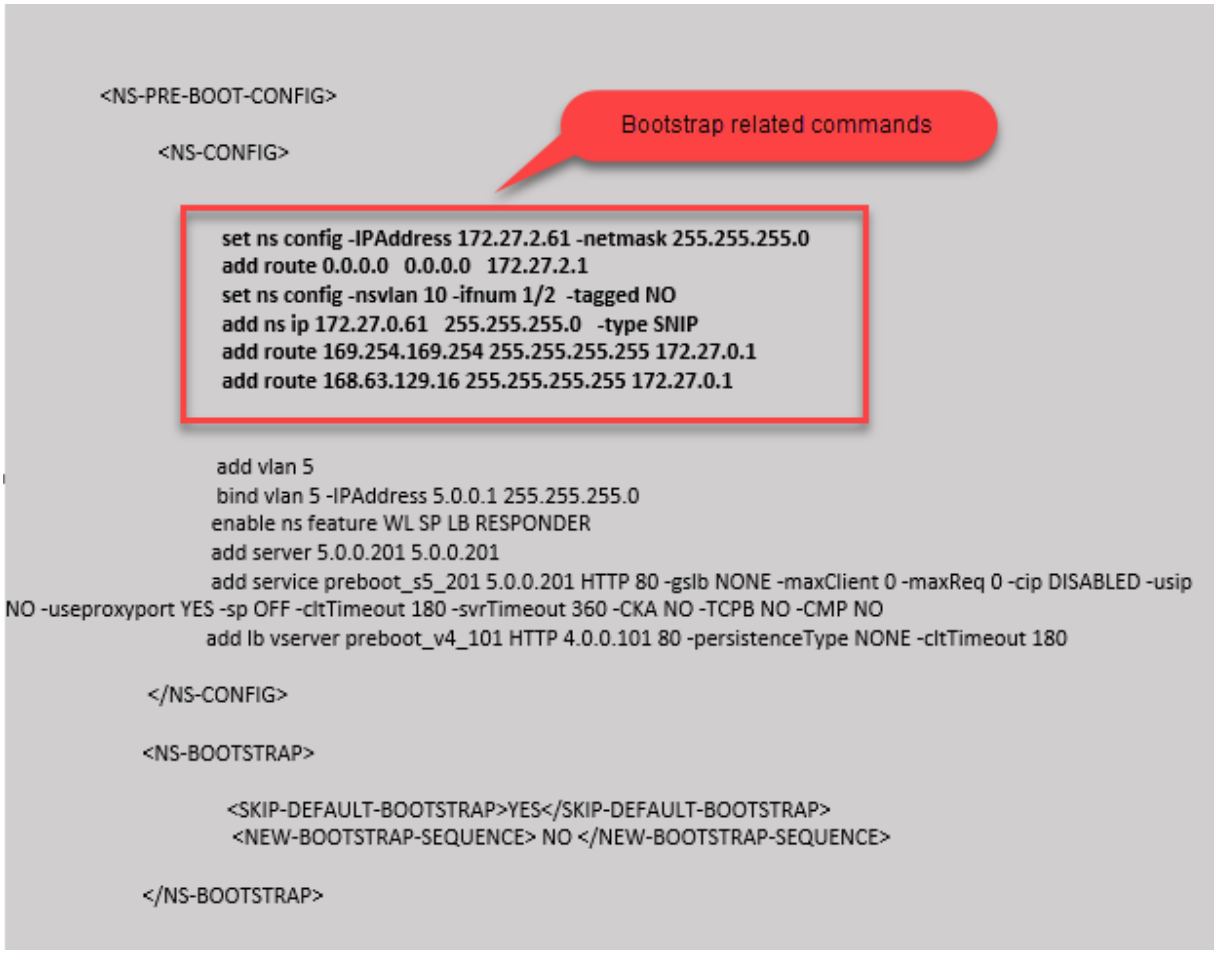
2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
4)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Benutzerdefiniertes Bootstrap-Beispiel für Azure

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen ausgeführt werden.

> Hinweis:
>
> Für Azure Cloud sind Instance Metadata Server (IMDS) und DNS-Server nur über die primäre

> Schnittstelle (Eth0) zugänglich. Wenn die Eth0-Schnittstelle nicht als Verwaltungsschnittstelle (NSIP) verwendet wird, muss die Eth0-Schnittstelle daher zumindest als SNIP für IMDS- oder DNS-Zugriff auf die Arbeit konfiguriert werden. Die Route zum IMDS-Endpunkt (169.254.169.254) und zum DNS-Endpunkt (168.63.129.16) über das Gateway von Eth0 muss ebenfalls hinzugefügt werden.




```
<NS-PRE-BOOT-CONFIG>

   <NS-CONFIG>

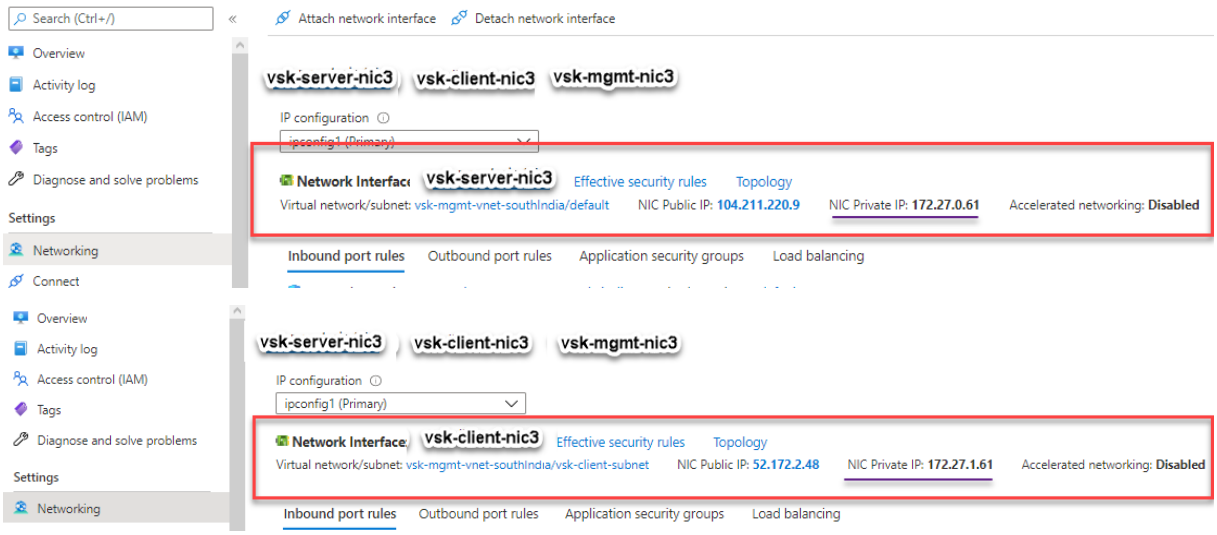
        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
        add route 0.0.0.0   0.0.0.0   172.27.2.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add ns ip 172.27.0.61   255.255.255.0   -type SNIP
        add route 169.254.169.254 255.255.255.255 172.27.0.1
        add route 168.63.129.16 255.255.255.255 172.27.0.1

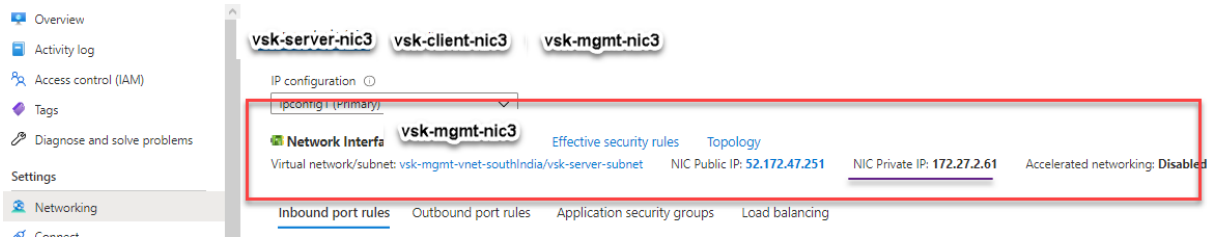
        add vlan 5
        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
```



```
14          enable ns feature WL SP LB RESPONDER
15          add server 5.0.0.201 5.0.0.201
16          add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
               maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
               YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
                -CMP NO
17          add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
               persistenceType NONE -cltTimeout 180
18
19      </NS-CONFIG>
20
21      <NS-BOOTSTRAP>
22
23      <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
24      <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
25
26      </NS-BOOTSTRAP>
27
28  </NS-PRE-BOOT-CONFIG>
29  <!--NeedCopy-->
```

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.





Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im <NS-BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.61      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.61      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

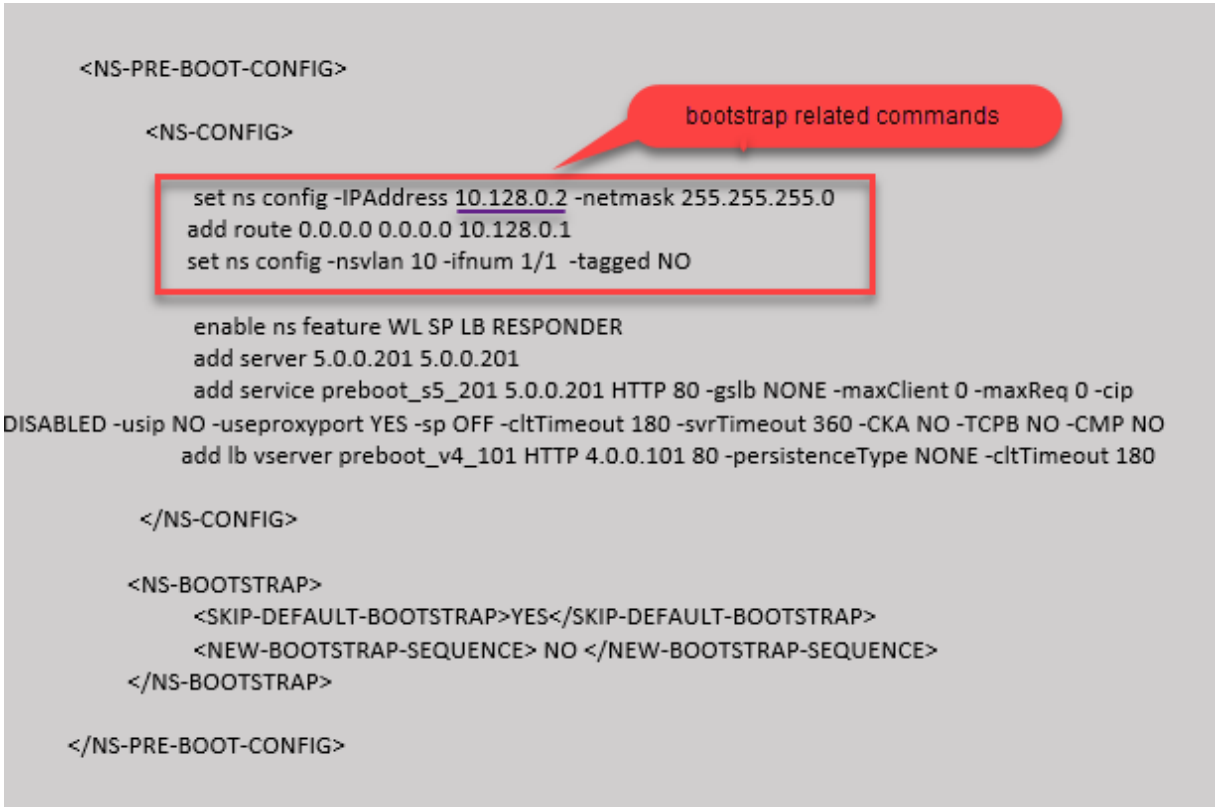
1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:9076/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 5      VLAN Alias Name:

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.61        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.61      0       UP      0               DIRECT
4)      172.27.2.0       255.255.255.0    172.27.2.61      0       UP      0               DIRECT
5)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
6)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
7)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Benutzerdefiniertes Bootstrap-Beispiel für GCP

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen angewendet werden.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>

        set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
        add route 0.0.0.0 0.0.0.0 10.128.0.1
        set ns config -nsvlan 10 -ifnum 1/1  -tagged NO

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
```

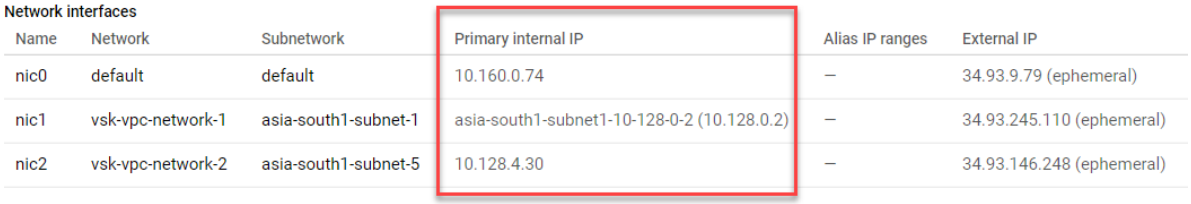


```
        <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

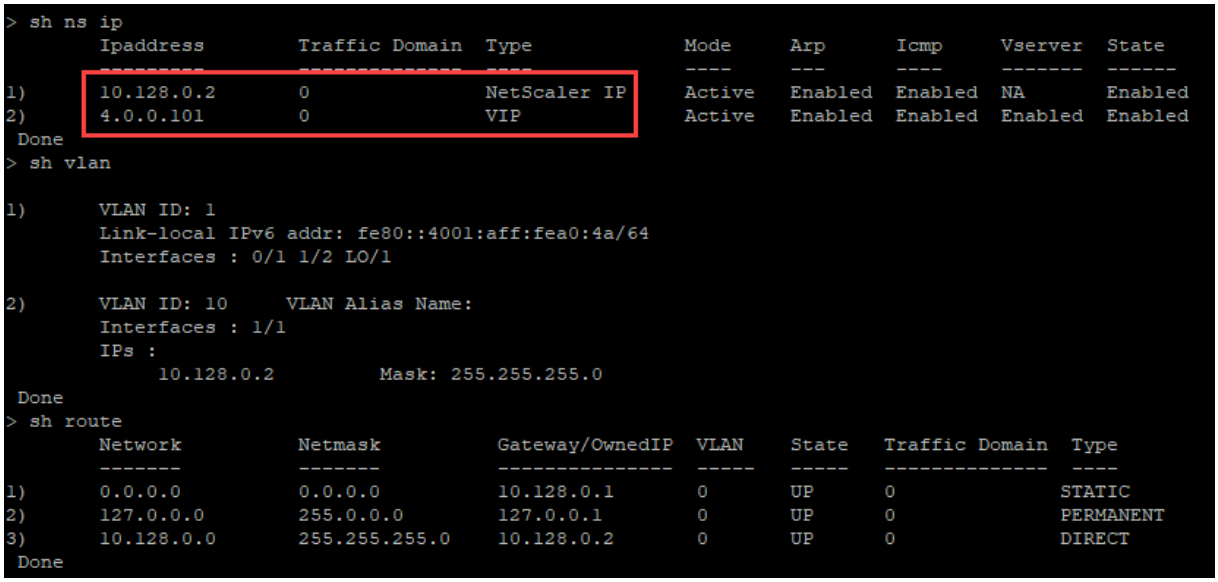
1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die Netzwerkdetails wie in der Abbildung gezeigt.



Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	default	default	10.160.0.74	–	34.93.9.79 (ephemeral)
nic1	vsk-vpc-network-1	asia-south1-subnet-1	asia-south1-subnet1-10-128-0-2 (10.128.0.2)	–	34.93.245.110 (ephemeral)
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.30	–	34.93.146.248 (ephemeral)

Sie können den `show nsip` Befehl in **ADC CLI**ausführen und sicherstellen, dass die im vorherigen <NS-CONFIG> Abschnitt bereitgestellten Konfigurationen beim ersten Start der ADC-Appliance angewendet werden.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.128.0.2       0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:4a/64
        Interfaces : 0/1 1/2 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/1
        IPs :
             10.128.0.2         Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.0.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.2       0       UP      0               DIRECT
 Done
```

Auswirkungen des Anhängen und Trennen von NICs in AWS und Azure

AWS und Azure bieten die Möglichkeit, eine Netzwerkschnittstelle an eine Instanz anzuschließen und eine Netzwerkschnittstelle von einer Instanz zu trennen. Das Anhängen oder Trennen von

Schnittstellen kann die Positionen der Schnittstelle verändern. Daher empfiehlt Citrix, Schnittstellen nicht von der NetScaler VPX-Instanz zu trennen. Wenn Sie eine Schnittstelle trennen oder anhängen, wenn benutzerdefiniertes Bootstrapping konfiguriert ist, weist die NetScaler VPX-Instanz die primäre IP der neu verfügbaren Schnittstelle in der Position der Verwaltungsschnittstelle als NSIP zu. Wenn nach der von Ihnen getrennten Schnittstelle keine weiteren Schnittstellen verfügbar sind, wird die erste Schnittstelle zur Verwaltungsschnittstelle für die NetScaler VPX-Instanz gemacht.

Zum Beispiel wird eine NetScaler VPX-Instanz mit 3 Schnittstellen aufgebracht: Eth0 (SNIP), Eth1 (NSIP) und Eth2 (VIP). Wenn Sie die Eth1-Schnittstelle von der Instanz trennen, bei der es sich um eine Verwaltungsschnittstelle handelt, konfiguriert ADC die nächste verfügbare Schnittstelle (Eth2) als Verwaltungsschnittstelle. Dadurch wird auf die NetScaler VPX-Instanz weiterhin über die primäre IP der Eth2-Schnittstelle zugegriffen. Wenn Eth2 ebenfalls nicht verfügbar ist, wird die verbleibende Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht. Daher besteht der Zugriff auf die NetScaler VPX-Instanz weiterhin.

Betrachten wir eine andere Zuweisung von Schnittstellen wie folgt: Eth0 (SNIP), Eth1 (VIP) und Eth2 (NSIP). Wenn Sie Eth2 (NSIP) trennen, da nach Eth2 keine neue Schnittstelle verfügbar ist, wird die erste Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht.

Verbessern der SSL-TPS-Leistung auf Public-Cloud-Plattformen

May 11, 2023

Sie können eine bessere SSL-TPS-Leistung in AWS- und GCP-Clouds erzielen, indem Sie die Gewichte der Paket-Engine (PE) gleichmäßig verteilen. Die Aktivierung dieser Funktion kann zu einem leichten Rückgang des HTTP-Durchsatzes um etwa 10—12% führen.

In AWS- und GCP-Clouds zeigen die NetScaler VPX-Instanzen mit 10—16 vCPUs keine Leistungsverbesserung, da die PE-Gewichte standardmäßig gleichmäßig verteilt sind.

> Hinweis:
>
> In der Azure-Cloud sind die PE-Gewichte standardmäßig gleichmäßig verteilt. Diese Funktion verbessert nicht die Leistung der Azure-Instanzen.

Konfigurieren des PE-Modus mithilfe der NetScaler CLI

Nachdem Sie den PE-Modus eingestellt haben, müssen Sie das System neu starten, damit die Konfigurationsänderungen wirksam werden.

Geben Sie in der Befehlszeile Folgendes ein:

```
set cpuparam pemode [CPUBOUND | Default]
```



```
<!--NeedCopy-->
```

Wenn der PE-Modus auf CPUBOUND eingestellt ist, sind die PE-Gewichte gleichmäßig verteilt.
Wenn der PE-Modus auf DEFAULT eingestellt ist, werden die PE-Gewichte auf Standardwerte eingestellt.

> Hinweis:
>
> Dieser Befehl ist knotenspezifisch. In einem Hochverfügbarkeits- oder Cluster-Setup müssen Sie den Befehl auf jedem Knoten ausführen. Wenn Sie den Befehl auf CLIP ausführen, tritt der folgende Fehler auf:
> `Operation not permitted on CLIP`

Führen Sie den folgenden Befehl aus, um den Status des konfigurierten PE-Modus anzuzeigen:

```
show cpuparam
<!--NeedCopy-->
```

Beispiel:

```
> show cpuparam
    Pemode:  CPUBOUND
 Done
<!--NeedCopy-->
```

Wenden Sie die PE-Modus-Konfiguration beim ersten Start der NetScaler Appliance in der Cloud an

Um die PE-Modus-Konfiguration beim ersten Start der NetScaler Appliance in der Cloud anzuwenden, müssen Sie eine Datei `/nsconfig/.cpubound.conf` mit dem benutzerdefinierten Skript erstellen. Weitere Informationen finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance in der Cloud.

Installieren einer NetScaler VPX Instanz auf einem Bare-Metal-Server

May 11, 2023

Ein Bare-Metal-Server ist ein vollständig dedizierter physischer Server, der physische Isolierung bietet und vollständig in die Cloud-Umgebung integriert ist. Er wird auch als Single-Tenant-Server bezeichnet. Single Tenancy ermöglicht es Ihnen, den Noisy-Neighbor-Effekt zu vermeiden. Bei blankem Metall treten Sie nicht auf, da Sie der alleinige Benutzer sind, den Noise-Neighbor-Effekt.

Ein Bare-Metal-Server, auf dem ein Hypervisor installiert ist, bietet Ihnen eine Management-Suite zum Erstellen virtueller Maschinen auf dem Server. Der Hypervisor führt keine Anwendungen nativ aus. Ziel ist es, Ihre Workloads in separaten virtuellen Maschinen zu virtualisieren, um die Flexibilität und Zuverlässigkeit der Virtualisierung zu erreichen.

Voraussetzungen für die Installation der NetScaler VPX-Instanz auf Bare-Metal-Servern

Ein Bare-Metal-Server muss von einem Cloud-Anbieter bezogen werden, der alle Systemanforderungen für den jeweiligen Hypervisor erfüllt.

Installieren Sie die NetScaler VPX-Instanz auf Bare-Metal-Servern

Um NetScaler VPX-Instances auf einem Bare-Metal-Server zu installieren, müssen Sie zunächst einen Bare-Metal-Server mit ausreichenden Systemressourcen von einem Cloud-Anbieter erwerben. Auf diesem Bare-Metal-Server muss jeder der unterstützten Hypervisoren wie Linux KVM, VMware ESX, Citrix Hypervisor oder Microsoft Hyper-V installiert und konfiguriert werden, bevor die NetScaler VPX-Instanz bereitgestellt wird.

Weitere Informationen zur Liste der verschiedenen Hypervisoren und Funktionen, die von einer NetScaler VPX-Instanz unterstützt werden, finden Sie unter Unterstützungsmatrix und Nutzungsrichtlinien.

Weitere Informationen zur Installation von NetScaler VPX Instanzen auf verschiedenen Hypervisoren finden Sie in der entsprechenden Dokumentation.

- **Citrix Hypervisor:** Siehe Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor.
- **VMware ESX:** Siehe Installieren einer NetScaler VPX-Instanz unter VMware ESX.
- **Microsoft Hyper-V:** Siehe Installieren einer NetScaler VPX-Instanz auf Microsoft Hyper-V-Server.
- **Linux KVM-Plattform:** Siehe Installieren einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform.

Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor

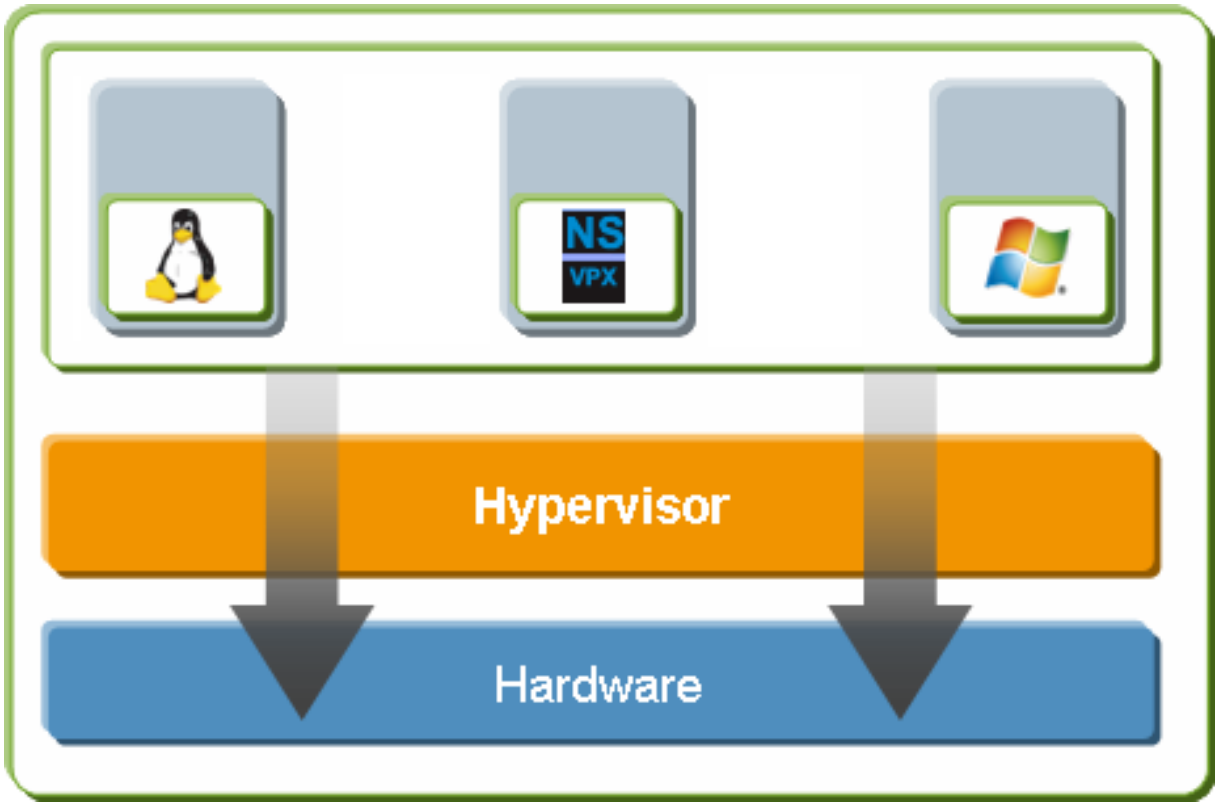
August 4, 2023

Um VPX-Instanzen auf dem Citrix Hypervisor zu installieren, müssen Sie zuerst den Hypervisor auf einem Computer mit ausreichenden Systemressourcen installieren. Um die NetScaler VPX-Instanzinstallation durchzuführen, verwenden Sie Citrix XenCenter, das auf einem Remotecomputer installiert sein muss, der über das Netzwerk eine Verbindung zum Hypervisor-Host herstellen kann.

Weitere Informationen zu Hypervisor finden Sie in der Dokumentation zu Citrix Hypervisor.

Die folgende Abbildung zeigt die Bare-Metal-Lösungsarchitektur der NetScaler VPX-Instanz auf Hypervisor.

Abbildung. Eine NetScaler VPX-Instanz auf Citrix Hypervisor



Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf Hypervisor

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Installieren Sie Hypervisor Version 6.0 oder höher auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie XenCenter auf einer Verwaltungsarbeitsstation, die die Mindestsystemanforderungen erfüllt.
- Beziehen Sie Lizenzdateien für virtuelle Appliances Weitere Informationen zu virtuellen Appliance-Lizenzen finden Sie im NetScaler Licensing Guide.

Hypervisor-Hardwareanforderungen

In der folgenden Tabelle werden die Mindestanforderungen an die Hardware für eine Hypervisor-Plattform beschrieben, auf der eine NetScaler VPX-Instanz ausgeführt wird.

Tabelle 1. Mindestsystemanforderungen für Hypervisor, der eine NCore VPX-Instanz ausführt

Komponente	Voraussetzung
CPU	2 oder mehr 64-Bit-x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT). Um die NetScaler VPX-Instanz auszuführen, muss die Hardwareunterstützung für die Virtualisierung auf dem Hypervisor-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für die Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Einzelheiten finden Sie in der BIOS-Dokumentation.
RAM	3 GB
Speicherplatz	Lokal angeschlossener Speicher (PATA, SATA, SCSI) mit 40 GB Speicherplatz. Hinweis: Die Hypervisor-Installation erstellt eine 4-GB-Partition für die Hypervisor-Host-Steuerdomäne. Der verbleibende Speicherplatz ist für die NetScaler VPX-Instanz und andere virtuelle Maschinen verfügbar.
Netzwerkkarte	Eine 1-Gbit/s-NIC; empfohlen: zwei 1-Gbit/s-NICs

Informationen zur Installation von Hypervisor finden Sie in der Hypervisor-Dokumentation unter http://support.citrix.com/product/xens/.

In der folgenden Tabelle sind die virtuellen Rechenressourcen aufgeführt, die Hypervisor für jede virtuelle NCore VPX-Appliance bereitstellen muss.

Tabelle 2. Minimale virtuelle Computing-Ressourcen, die zum Ausführen einer NCore VPX-Instanz erforderlich sind

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	2

> **Hinweis:**
>
> Für den Produktionseinsatz der NetScaler VPX-Instanz empfiehlt Citrix, die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf die höchste Stufe einzustellen, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

XenCenter Systemanforderungen

XenCenter ist eine Windows-Clientanwendung. Es kann nicht auf demselben Computer wie der Hypervisor-Host ausgeführt werden. Weitere Informationen zu Mindestsystemanforderungen und zur Installation von XenCenter finden Sie in den folgenden Hypervisor-Dokumenten:

- Systemanforderungen
- Installieren

Installieren Sie NetScaler VPX-Instanzen auf Hypervisor mithilfe von XenCenter

Nachdem Sie Hypervisor und XenCenter installiert und konfiguriert haben, können Sie XenCenter verwenden, um virtuelle Appliances auf Hypervisor zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge an Speicher ab, die auf der Hardware verfügbar ist, auf der Hypervisor ausgeführt wird.

Gehen Sie folgendermaßen vor, um NetScaler VPX-Instanzen auf Hypervisor mithilfe von XenCenter zu installieren:

1. Starten Sie **XenCenter** auf Ihrer Workstation.
2. Klicken Sie im Menü **Server** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Neuen Server hinzufügen** in das Textfeld Hostname die IP-Adresse oder den DNS-Namen des Hypervisors ein, zu dem Sie eine Verbindung herstellen möchten.
4. Geben Sie in den Textfeldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Verbinden**. Der Hypervisor-Name wird im Navigationsbereich mit einem grünen Kreis angezeigt, der angibt, dass der Hypervisor verbunden ist.
5. Klicken Sie im Navigationsbereich auf den Namen des Hypervisor, auf dem Sie die NetScaler VPX-Instanz installieren möchten.
6. Klicken Sie im Menü **VM** auf **Importieren**.
7. Navigieren Sie im Dialogfeld **Import** im Namen der Importdatei zu dem Speicherort, an dem Sie die NetScaler VPX `.xva` VPX-Instanzbilddatei gespeichert haben. Stellen Sie sicher, dass die Option Exportierte VM ausgewählt ist, und klicken Sie dann auf **Weiter**.
8. Wählen Sie den Hypervisor aus, auf dem Sie die virtuelle Appliance installieren möchten, und klicken Sie dann auf **Weiter**.

9. Wählen Sie das lokale Speicher-Repository aus, in dem die virtuelle Appliance gespeichert werden soll, und klicken Sie dann auf Importieren, um mit dem Importvorgang zu beginnen.
10. Sie können die virtuellen Netzwerkschnittstellen nach Bedarf hinzufügen, ändern oder löschen. Wenn Sie fertig sind, klicken Sie auf Weiter.
11. Klicken Sie auf **Fertig stellen**, um den Importvorgang abzuschließen.

    Hinweis: Um den Status des Importvorgangs anzuzeigen, klicken Sie auf die Registerkarte **Protokoll** .
12. Wenn Sie eine weitere virtuelle Appliance installieren möchten, wiederholen Sie die Schritte 5 bis 11.

> **Hinweis:**
>
> Wenn Sie nach der Erstkonfiguration der VPX-Instanz die Appliance auf die neueste Softwareversion aktualisieren möchten, lesen Sie Upgraden oder Downgrade der Systemsoftware.

Konfigurieren von VPX-Instanzen für die Verwendung von Single-Root-I/O-Virtualisierungs-Netzwerkschnittstellen (SR-IOV)

May 11, 2023

Nachdem Sie eine NetScaler VPX-Instanz auf Citrix Hypervisor installiert und konfiguriert haben, können Sie die virtuelle Appliance für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren.

Die folgenden NICs werden unterstützt:

- Intel 82599 10 G
- Intel X710 10 G
- Intel XL710 40 G

Einschränkungen

Citrix Hypervisor unterstützt einige Funktionen auf SR-IOV-Schnittstellen nicht. Die Einschränkungen bei Intel 82599, Intel X710 und Intel XL710 NICs sind in den folgenden Abschnitten aufgeführt.

Einschränkungen für Intel 82599 NIC

Intel 82599 NIC unterstützt die folgenden Funktionen nicht:

- L2-Modus Umschaltung
- Clustering

- Admin-Partitionierung [Shared VLAN-Modus]
- Hochverfügbarkeit [Aktiv - Aktiver Modus]
- Jumbo-Rahmen
- IPv6-Protokoll in Cluster-Umgebung

Einschränkungen für Intel X710 10G und Intel XL710 40G NICs

Intel X710 10G und Intel XL710 40G NICs weisen die folgenden Einschränkungen auf:

- Die Umschaltung im L2-Modus wird nicht unterstützt.
- Admin-Partitionierung (Shared VLAN-Modus) wird nicht unterstützt.
- In einem Cluster werden Jumbo-Frames nicht unterstützt, wenn die XL710-NIC als Datenschnittstelle verwendet wird.
- Die Schnittstellenliste ordnet neu an, wenn Schnittstellen getrennt und wieder verbunden werden.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und automatische Absprache werden nicht unterstützt.
- Sowohl für Intel X710 10G- als auch für Intel XL710 40G-NICs ist die Schnittstelle als 40/x-Schnittstelle verfügbar.
- Bis zu nur 16 Intel X710/XL710 SR-IOV-Schnittstellen können auf einer VPX-Instanz unterstützt werden.

> **Hinweis:**
>
> Damit Intel X710 10G- und Intel XL710 40G-NICs IPv6 unterstützen, aktivieren Sie den Vertrauensmodus für die virtuellen Funktionen (VFs), indem Sie den folgenden Befehl auf dem Citrix Hypervisor-Host eingeben:
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> **Beispiel:**
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Voraussetzungen für Intel 82599 NIC

Stellen Sie auf dem Citrix Hypervisor-Host sicher, dass Sie:

- Fügen Sie die Intel 82599 NIC (NIC) zum Host hinzu.
- Blockieren Sie den Treiber `ixgbevf`, indem Sie der Datei **/etc/modprobe.d/blacklist.conf** den folgenden Eintrag hinzufügen:

  blacklist ixgbevf

- Aktivieren Sie SR-IOV Virtual Functions (VFs), indem Sie der Datei **/etc/modprobe.d/ixgbe** den folgenden Eintrag hinzufügen:

  optionen ixgbe max_vfs=* <number_of_VFs>*

  Dabei ist <*number_VFs*> die Anzahl der SR-IOV-VFs, die Sie erstellen möchten.

- Stellen Sie sicher, dass SR-IOV im BIOS aktiviert ist.

> Hinweis:
>
> IXGBE-Treiberversion 3.22.3 wird empfohlen.

Weisen Sie der NetScaler VPX-Instanz Intel 82599 SR-IOV VFs zu, indem Sie den Citrix Hypervisor-Host verwenden

Gehen Sie folgendermaßen vor, um der NetScaler VPX-Instanz einen Intel 82599 SR-IOV-VFs zuzuweisen:

1. Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die SR-IOV-VFs der NetScaler VPX-Instanz zuzuweisen:

   xe host-call-plugin plugin=iovirt host-uuid=<*Xen host UUID*> **fn=assign_free_vf args:uuid**=<*NetScaler VM UUID*> **args:ethdev**=<*interface name*> **args:mac=***<Mac addr>*

   Es gilt:

   - ** <Xen host UUID>ist die UUID des Citrix Hypervisor-Hosts.
   - <*NetScaler VM UUID*> ist die UUID der NetScaler VPX-Instanz.
   - <*interface name*> ist die Schnittstelle für die SR-IOV-VFs.
   - <*MAC address* > ist die MAC-Adresse des SR-IOV VF.

   > **Hinweis**
   >
   > Geben Sie die MAC-Adresse an, die Sie im Parameter args:mac= verwenden möchten. Wenn nicht angegeben, generiert das Skript `iovirt` zufällig eine MAC-Adresse und weist sie zu. Wenn Sie die SR-IOV-VFs im Link-Aggregationsmodus verwenden möchten, stellen Sie sicher, dass Sie die MAC-Adresse als 00:00:00:00:00:00 angeben.

2. Starten Sie die NetScaler VPX-Instanz.

Aufheben der Zuweisung von Intel 82599 SR-IOV-VFs zur NetScaler VPX-Instanz mithilfe des Citrix Hypervisor-Hosts

Wenn Sie ein falsches SR-IOV-VFs zugewiesen haben oder wenn Sie ein zugewiesenes SR-IOV-VFs ändern möchten, müssen Sie die Zuweisung der SR-IOV-VFs aufheben und der NetScaler VPX-Instanz neu zuweisen.

Gehen Sie folgendermaßen vor, um die Zuweisung der SR-IOV-Netzwerkschnittstelle aufzuheben, die einer NetScaler VPX-Instanz zugewiesen ist:

1. Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die SR-IOV-VFs der NetScaler VPX-Instanz zuzuweisen und die NetScaler VPX-Instanz neu zu starten:

   xe host-call-plugin plugin=iovirt **host-uuid**=*<Xen_host_UUID>* **fn**=unassign_all **args:uuid**=*<Netscaler_VM_U*

   Es gilt:

   - *<Xen_host_UUID>* - Die UUID des Citrix Hypervisor-Hosts.
   - *<Netscaler_VM_UUID>* - Die UUID der NetScaler VPX-Instanz ist.

2. Starten Sie die NetScaler VPX-Instanz.

Weisen Sie der NetScaler VPX-Instanz Intel X710/XL710 SR-IOV VFs zu, indem Sie den Citrix Hypervisor-Host verwenden

Gehen Sie folgendermaßen vor, um der NetScaler VPX-Instanz einen Intel X710/XL710 SR-IOV VF zuzuweisen:

1. Führen Sie den folgenden Befehl auf dem Citrix Hypervisor-Host aus, um ein Netzwerk zu erstellen.

```
xe network-create name-label=<network-name>
<!--NeedCopy-->
```

   Beispiel:

```
xe network-create name-label=SR-IOV-NIC-18 8ee59b73-7319-6998-cd69
   -b9fa3e8d7503
<!--NeedCopy-->
```

2. Ermitteln Sie den PIF Universal Unique Identifier (UUID) der NIC, auf der das SR-IOV-Netzwerk konfiguriert werden soll.

```
xe pif-list

            uuid ( RO)  : e2874343-f1de-1fa7-8fef-98547c348783
            device ( RO): eth18
currently-attached ( RO): true
              VLAN ( RO): -1
      network-uuid ( RO): f865bd85-44dd-b865-ab65-dcd6ae28c16e
<!--NeedCopy-->
```


3. Konfigurieren Sie das Netzwerk als SR-IOV-Netzwerk. Der folgende Befehl gibt auch die UUID des neu erstellten SR-IOV-Netzwerks zurück:

```
xe network-sriov-create network-uuid=<network-uuid> pif-uuid=<
    physical-pif-uuid>
<!--NeedCopy-->
```

Beispiel:

```
xe network-sriov-create network-uuid=8ee59b73-7319-6998-cd69-
    b9fa3e8d7503 pif-uuid=e2874343-f1de-1fa7-8fef-98547
    c3487831629b44f-832a-084e-d67d-5d6d314d5e0f
<!--NeedCopy-->
```

Um weitere Informationen zu den SR-IOV-Netzwerkparametern zu erhalten, führen Sie den folgenden Befehl aus:

```
[root@citrix-XS82-TOPO ~]# xe network-sriov-param-list uuid=1629
    b44f-832a-084e-d67d-5d6d314d5e0f

               uuid ( RO): 1629b44f-832a-084e-d67d-5d6d314d5e0f
      physical-PIF ( RO): e2874343-f1de-1fa7-8fef-98547c348783
       logical-PIF ( RO): 85d52771-5814-c62d-45fa-f37b536144ff
   requires-reboot ( RO): false
remaining-capacity ( RO): 32
<!--NeedCopy-->
```

4. Erstellen Sie eine virtuelle Schnittstelle (VIF) und hängen Sie sie an die Ziel-VM an.

```
xe vif-create device=0 mac=b2:61:fc:ae:00:1d network-uuid=8ee59b73
    -7319-6998-cd69-b9fa3e8d7503 vm-uuid=b507e8a6-f5ca-18eb-561d
    -308218a9dd68
3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
<!--NeedCopy-->
```

> HINWEIS: Die NIC-Indexnummer der VM muss mit 0 beginnen.

Verwenden Sie den folgenden Befehl, um die VM-UUID zu finden:

```
[root@citrix-XS82-TOPO ~]# xe vm-list
uuid ( RO): b507e8a6-f5ca-18eb-561d-308218a9dd68
 name-label ( RW): sai-vpx-1
power-state ( RO): halted
<!--NeedCopy-->
```


Entfernen Sie Intel X710/XL710 SR-IOV VFs aus der NetScaler-Instanz, indem Sie den Citrix Hypervisor-Host verwenden

Gehen Sie folgendermaßen vor, um einen Intel X710/XL710 SR-IOV VF aus einer NetScaler VPX-Instanz zu entfernen:

1. Kopieren Sie die UUID für das VIF, das Sie löschen möchten.
2. Führen Sie den folgenden Befehl auf dem Citrix Hypervisor-Host aus, um die VIF zu zerstören.

```
xe vif-destroy uuid=<vif-uuid>
<!--NeedCopy-->
```

Beispiel:

```
[root@citrix-XS82-TOPO ~]# xe vif-destroy uuid=3e1e2e58-b2ad-6dc0
   -61d4-1d149c9c6466
<!--NeedCopy-->
```

Konfigurieren Sie die Link-Aggregation auf der SR-IOV-Schnittstelle

Um die virtuellen SR-IOV-Funktionen (VFs) im Link-Aggregationsmodus verwenden zu können, müssen Sie die Spoof-Prüfung für virtuelle Funktionen, die Sie erstellt haben, deaktivieren.

Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die Spoof-Prüfung zu deaktivieren:

ip link set <*interface_name*> **vf** <*VF_id*> **spoofchk** off

Es gilt:

- <interface_name>ist der Schnittstellenname.
- <VF_id>ist die virtuelle Funktions-ID.

Nachdem Sie die Spoof-Prüfung für alle von Ihnen erstellten virtuellen Funktionen deaktiviert haben, starten Sie die NetScaler VPX-Instanz neu und konfigurieren Sie die Linkaggregation. Anweisungen finden Sie unter Konfigurieren der Link-Aggregation.

> **Wichtig**
>
> Stellen Sie beim Zuweisen der SR-IOV-VFs zur NetScaler VPX-Instanz sicher, dass Sie die MAC-Adresse 00:00:00:00:00:00 für die VFs angeben.

Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

Sie können VLAN für die virtuellen SR-IOV-Funktionen konfigurieren. Anweisungen finden Sie unter Konfiguration eines VLAN.

> **Wichtig**
>
> Stellen Sie sicher, dass der Citrix Hypervisor-Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

Installieren einer NetScaler VPX-Instanz auf VMware ESX

May 11, 2023

Stellen Sie vor der Installation von NetScaler VPX-Instanzen auf VMware ESX sicher, dass der VMware ESX Server auf einem Computer mit ausreichenden Systemressourcen installiert ist. Um eine NetScaler VPX-Instanz auf VMware ESXi zu installieren, verwenden Sie den VMware vSphere-Client. Der Client oder das Tool muss auf einem Remote-Computer installiert sein, der über das Netzwerk eine Verbindung zu VMware ESX herstellen kann.

Dieser Abschnitt enthält die folgenden Themen:

- Voraussetzungen
- Installieren einer NetScaler VPX-Instanz auf VMware ESX

> **Wichtig:**
>
> Sie können keine standardmäßigen VMware Tools installieren oder die auf einer NetScaler VPX-Instanz verfügbare Version von VMware Tools aktualisieren. VMware Tools für eine NetScaler VPX-Instanz werden im Rahmen der NetScaler-Softwareversion bereitgestellt.

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Installieren Sie VMware ESX auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Laden Sie die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie einen virtuellen Switch und verbinden Sie die physische Netzwerkkarte mit dem virtuellen Switch.
- Fügen Sie eine Portgruppe hinzu und verbinden Sie sie mit dem virtuellen Switch.
- Hängen Sie die Portgruppe an die VM an.
- VPX-Lizenzdateien abrufen. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie unter Lizenzierungsübersicht.

VMware ESX-Hardwareanforderungen

In der folgenden Tabelle werden die Mindestsystemanforderungen für VMware ESX-Server beschrieben, auf denen die virtuelle NetScaler VPX nCore Appliance ausgeführt wird.

Tabelle 1. Mindestsystemanforderungen für einen VMware ESX-Server, auf dem eine NetScaler VPX-Instanz ausgeführt wird

Komponente	Voraussetzung
CPU	2 oder mehr 64-Bit-x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT). Um eine NetScaler VPX-Instanz ausführen zu können, muss Hardwareunterstützung für die Virtualisierung auf dem VMware ESX-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Informationen finden Sie in Ihrer BIOS-Dokumentation. Ab der NetScaler 13.1 Version unterstützt die NetScaler VPX-Instanz auf dem VMware ESXi Hypervisor AMD-Prozessoren.
RAM	2 GB VPX. Für kritische Bereitstellungen empfehlen wir 2 GB RAM für VPX nicht, da das System in einer Umgebung mit begrenztem Arbeitsspeicher betrieben wird. Dies kann zu Skalierungs-, Leistungs- oder Stabilitätsproblemen führen. Empfohlen werden 4 GB RAM oder 8 GB RAM.
Speicherplatz	20 GB mehr als die minimalen Serveranforderungen von VMware für die Einrichtung von ESXi. Die Mindestanforderungen an den Server finden Sie in der VMware-Dokumentation.
Netzwerk	Eine 1-Gbit/s-NIC (NIC); Zwei 1-Gbit/s-NICs empfohlen

Hinweise zur Installation von VMware ESX finden Sie unterhttp://www.vmware.com/.

Stellen Sie für die SR-IOV-Netzwerkschnittstelle oder die PCI-Passthrough-Unterstützung sicher, dass die folgenden Prozessoren und Einstellungen aktiviert sind:

- Intel-Prozessoren, die Intel-VT unterstützen
- AMD-Prozessoren, die AMD-V unterstützen
- Die I/O Memory Management Unit (IOMMU) oder SR-IOV ist im BIOS aktiviert

Die folgenden Netzwerkkarten werden im SR-IOV-Modus unterstützt:

- Mellanox ConnectX-4 NIC, ab NetScaler Release 13.1-42.x
- Intel 82599 NIC

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die der VMware ESX-Server für jede virtuelle VPX nCore Appliance bereitstellen muss.

Tabelle 2. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	4 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In ESX können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> **Hinweis:**
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktionsnutzung der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden. CPU-Zyklen (in MHz), die mindestens der Geschwindigkeit eines CPU-Kerns des ESX entsprechen, müssen reserviert werden.

Systemanforderungen für VMware vSphere-Clients

VMware vSphere ist eine Clientanwendung, die auf Windows- und Linux-Betriebssystemen ausgeführt werden kann. Es kann nicht auf demselben Computer wie der VMware ESX-Server ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 3. Mindestsystemanforderungen für die Installation des VMware vSphere-Clients

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware, suchen Sie nach der PDF-Datei “vSphere Compatibility Matrixes” unter http://kb.vmware.com/.
CPU	750 MHz; 1 Gigahertz (GHz) oder schneller empfohlen
RAM	1 GB. 2 GB empfohlen
NIC (NIC)	Netzwerkkarte mit 100 Mbit/s oder schneller

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. Es kann nicht auf demselben Computer wie der VMware ESX-Server ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 4. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
NIC (NIC)	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix Konto haben, rufen Sie die Homepage unter http://www.citrix.comauf, klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen

zum Erstellen eines Citrix Kontos.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (for example, NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (for example, NSVPX-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (for example, NSVPX-ESX-13.0-71.44_nc_64.mf)

Installieren einer NetScaler VPX-Instanz auf VMware ESX

Nachdem Sie VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere-Client verwenden, um virtuelle Appliances auf dem VMware ESX-Server zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge an Speicher ab, die auf der Hardware verfügbar ist, auf der VMware ESX ausgeführt wird.

Gehen Sie folgendermaßen vor, um NetScaler VPX-Instanzen auf VMware ESX mithilfe von VMware vSphere Client zu installieren:

1. Starten Sie den VMware vSphere Client auf Ihrer Workstation.
2. Geben Sie im Textfeld **IP-Adresse/Name** die IP-Adresse des VMware ESX-Servers ein, mit dem Sie eine Verbindung herstellen möchten.
3. Geben Sie in den Textfeldern **User Name** und **Password** die Administratoranmeldeinformationen ein, und klicken Sie dann auf Anmelden.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Deploy from file** zu dem Speicherort, an dem Sie die NetScaler VPX-Instanz-Setupdateien gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf **Weiter**.
6. Ordnen Sie die in der OVF-Vorlage für virtuelle Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem ESX-Host konfiguriert haben. Klicken Sie auf **Weiter**, um mit der Installation einer virtuellen Appliance auf VMware ESX zu beginnen. Wenn die Installation abgeschlossen ist, informiert Sie ein Popup-Fenster über die erfolgreiche Installation.
7. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Rechtsklickmenü die Option **Power On**aus.
8. Nachdem die VM gestartet wurde, konfigurieren Sie von der Konsole aus die NetScaler IP-, Netmask- und Gateway-Adressen. Wenn Sie die Konfiguration abgeschlossen haben, wählen Sie in der Konsole die Option **Speichern und beenden** .
9. Um eine weitere virtuelle Appliance zu installieren, wiederholen Sie die Schritte 6 bis Schritt 8.

> **Hinweis:**
>
> Standardmäßig verwendet die NetScaler VPX-Instanz E1000 Netzwerkschnittstellen.
>
> Nach der Installation können Sie den vSphere Client oder vSphere Web Client verwenden, um virtuelle Appliances auf VMware ESX zu verwalten.
>
> Damit die VLAN-Tagging-Funktion funktioniert, legen Sie auf dem VMware ESX die VLAN-ID der Portgruppe auf Alle (4095) auf dem vSwitch des VMware ESX-Servers fest. Weitere Informationen zum Festlegen einer VLAN-ID auf dem vSwitch des VMware ESX-Servers finden Sie unter http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

Migrieren Sie eine NetScaler VPX-Instanz mithilfe von VMware VMotion

Sie können eine NetScaler VPX-Instanz mithilfe von VMware vSphere vMotion migrieren.

Folgen Sie diesen Nutzungsrichtlinien:

- VMware unterstützt die VMotion-Funktion auf virtuellen Maschinen, die mit PCI-Passthrough- und SR-IOV-Schnittstellen konfiguriert sind, nicht.
- Unterstützte Schnittstellen sind E1000 und VMXNET3. Um vMotion auf Ihrer VPX-Instanz zu verwenden, stellen Sie sicher, dass die Instanz mit einer unterstützten Schnittstelle konfiguriert ist.
- Weitere Informationen zur Migration einer Instanz mithilfe von VMware VMotion finden Sie in der VMware-Dokumentation.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der VMXNET3-Netzwerkschnittstelle

May 11, 2023

Nachdem Sie die NetScaler VPX-Instanz auf dem VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere-Webclient verwenden, um die virtuelle Appliance für die Verwendung von VMXNET3-Netzwerkschnittstellen zu konfigurieren.

Gehen Sie wie folgt vor, um NetScaler VPX-Instanzen für die Verwendung von VMXNET3-Netzwerkschnittstellen mithilfe des VMware vSphere Web Client zu konfigurieren:

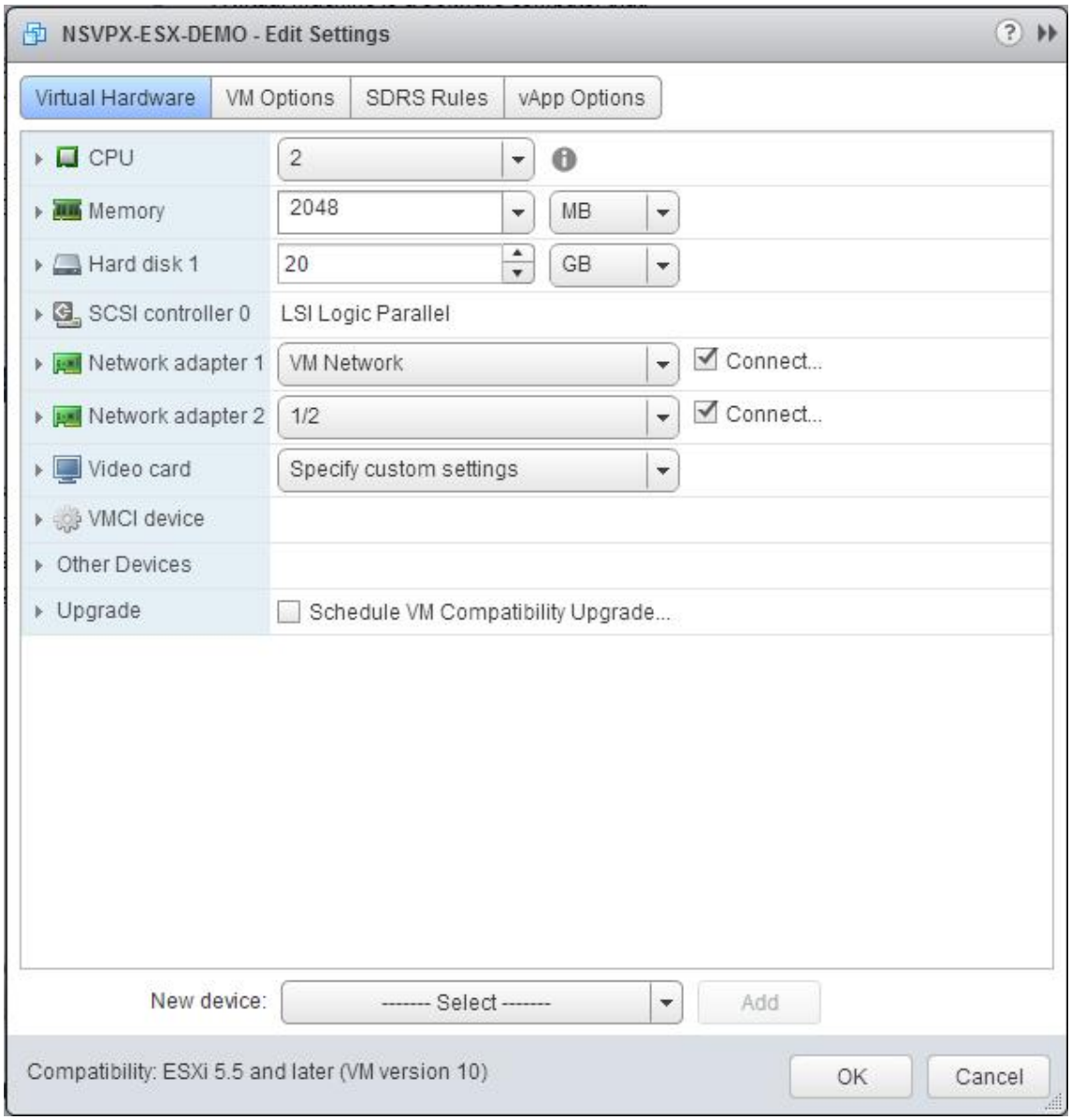
1. Wählen Sie im vSphere Web Client Hosts and Clustersaus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der NetScaler VPX-Instanz wie folgt auf ESX:

   a. Schalten Sie die NetScaler VPX-Instanz aus.

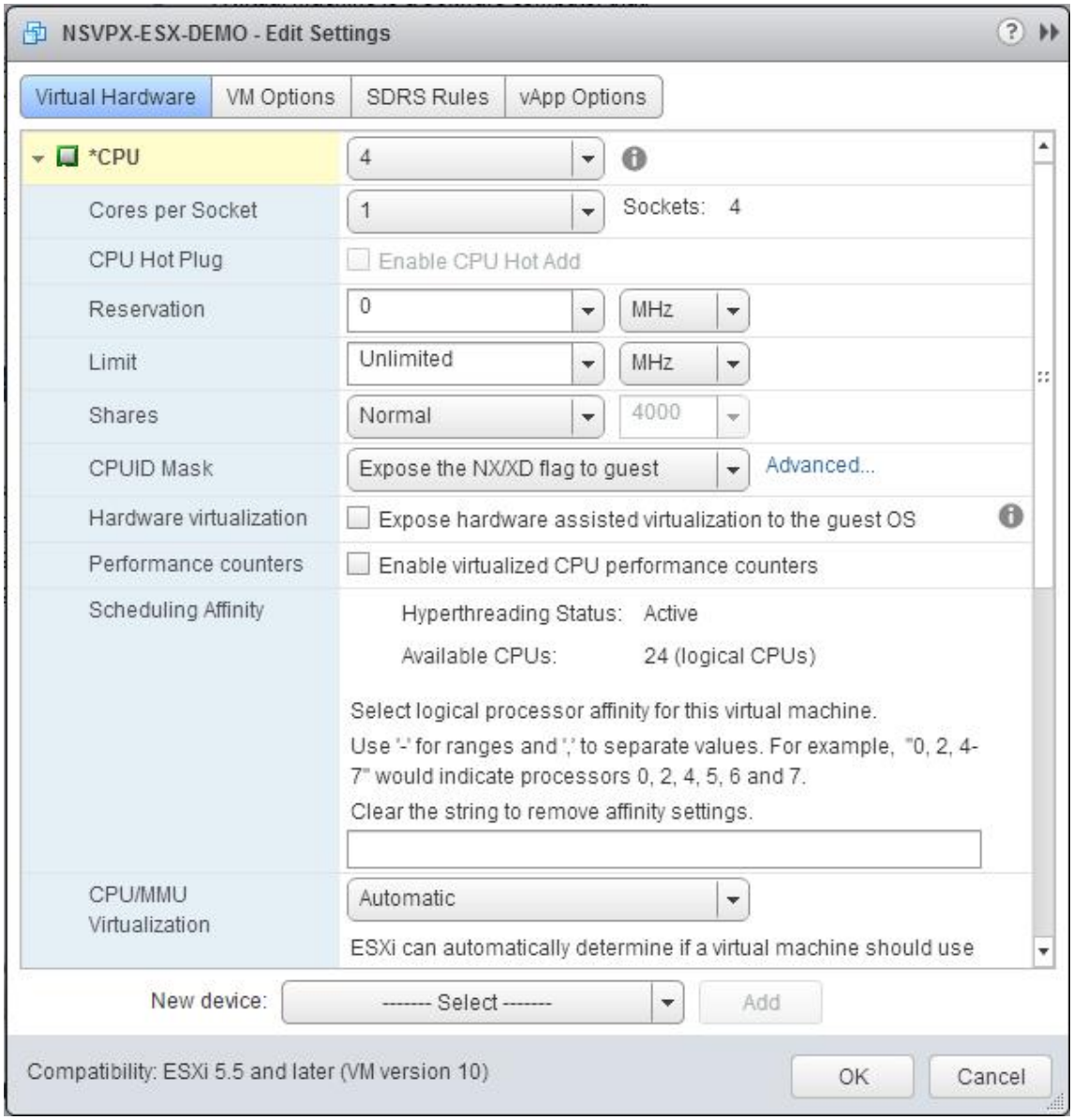
b. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und wählen Sie Kompatibilität > VM-Kompatibilität aktualisieren.

c. Wählen Sie im Dialogfeld VM-Kompatibilität konfigurieren die Option ESXi 5.5 und höher aus der Dropdown-Liste Kompatibel mit aus, und klicken Sie auf OK.

3. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX Instanz, und klicken Sie auf Einstellungen bearbeiten.



4. Klicken Sie im Dialogfeld <virtual_appliance> - Einstellungen bearbeiten auf den Abschnitt CPU.



5. Aktualisieren Sie im Abschnitt CPU Folgendes:

   - CPU-Anzahl
   - Anzahl der Buchsen
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

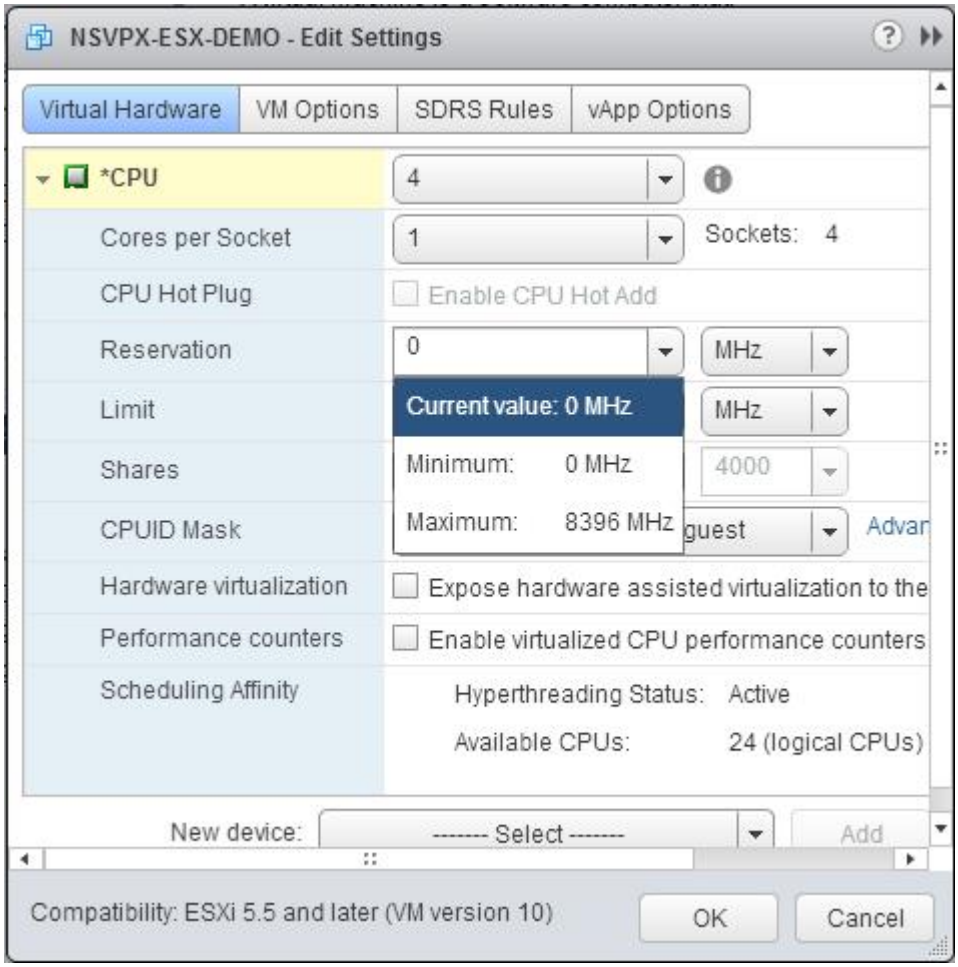
   a. Wählen Sie in der Dropdownliste CPU die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

   b. Wählen Sie in der Dropdownliste Kerne pro Socket die Anzahl der Sockets aus.

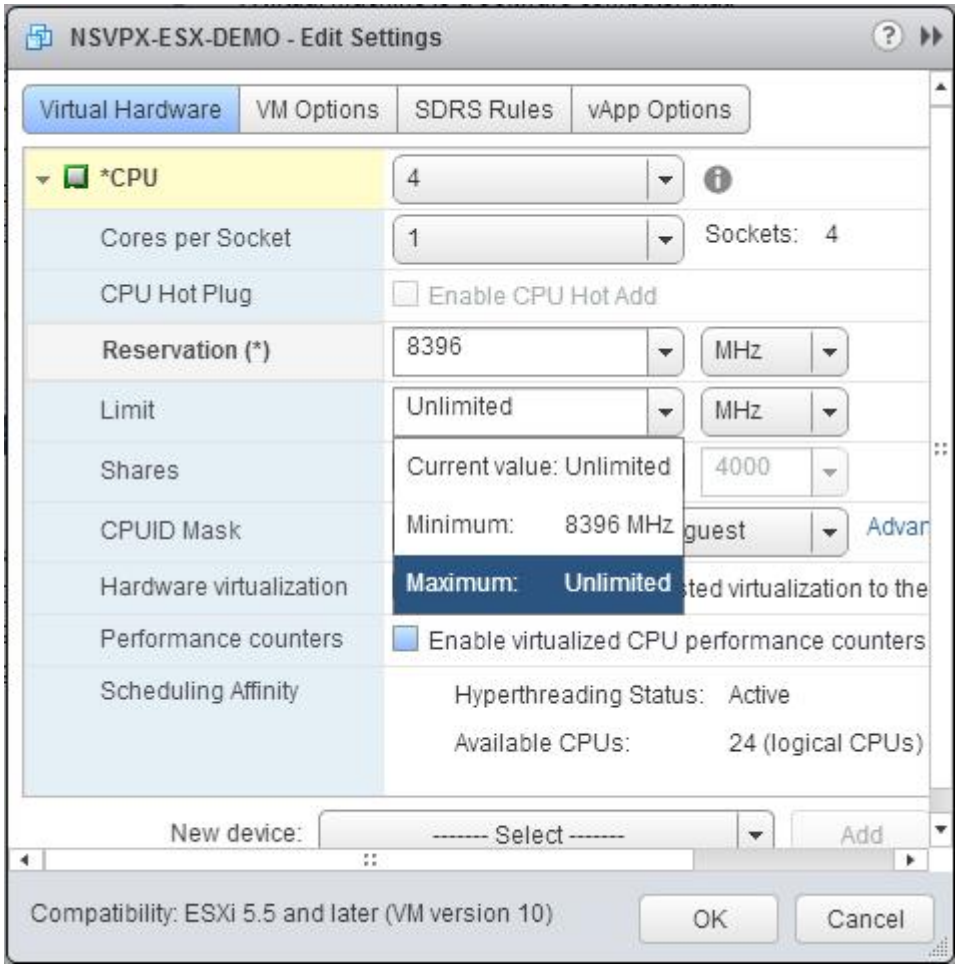
c. (Optional) Aktivieren oder deaktivieren Sie im Feld CPU-Hotplug das Kontrollkästchen CPU-Hotadd aktivieren.

Hinweis: Citrix empfiehlt, die Standardeinstellung zu akzeptieren (deaktiviert).

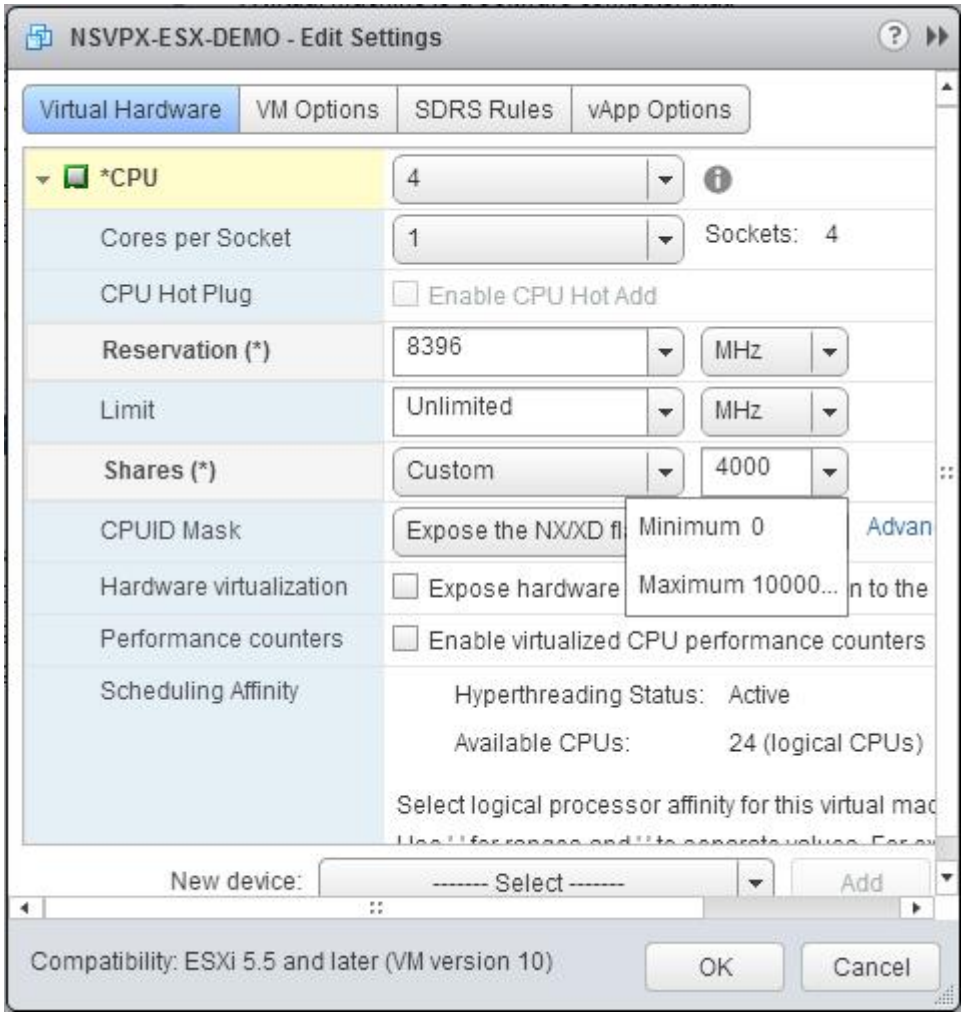
d. Wählen Sie in der Dropdownliste Reservierung die Zahl aus, die als Maximalwert angezeigt wird.



e. Wählen Sie in der Dropdownliste Limit die Zahl aus, die als Maximalwert angezeigt wird.



f. Wählen Sie in den Dropdownlisten Anteile die Option Benutzerdefiniert und die Zahl aus, die als Maximalwert angezeigt wird.



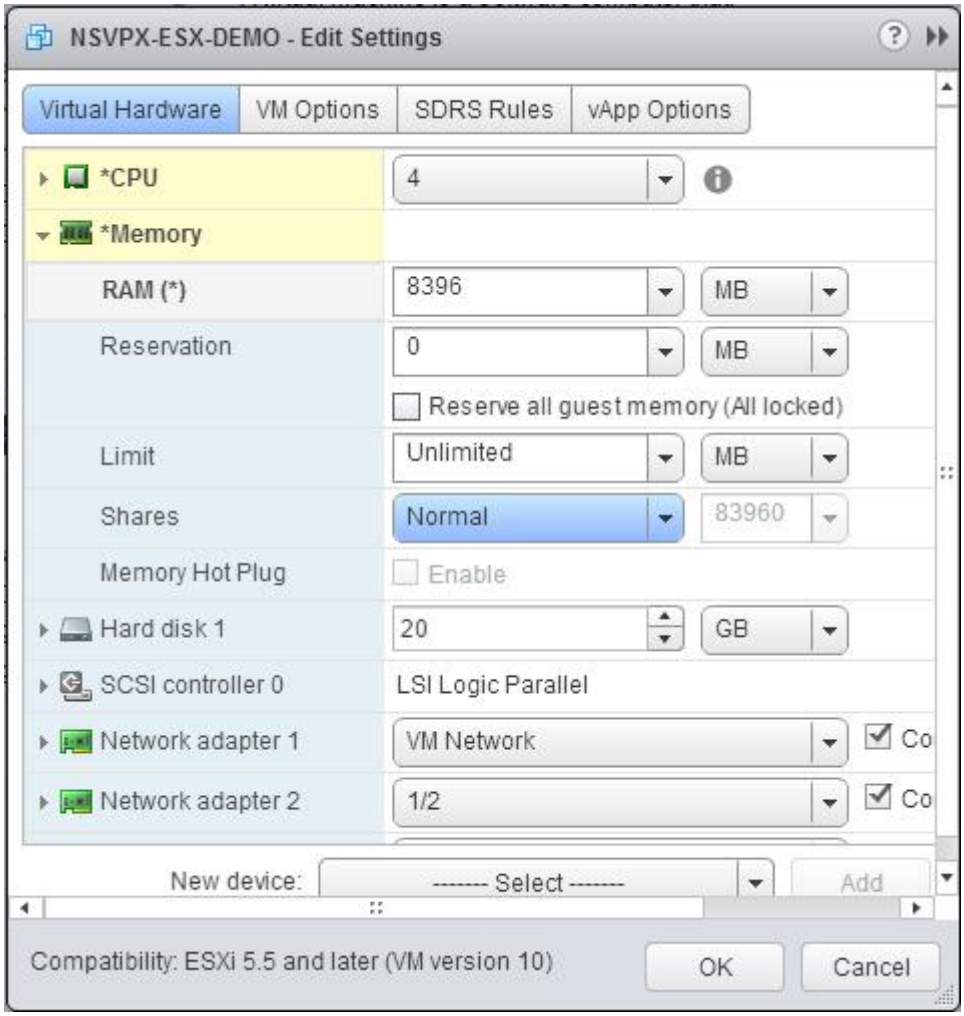
6. Aktualisieren Sie im Abschnitt Speicher Folgendes:

   - Größe des RAM
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

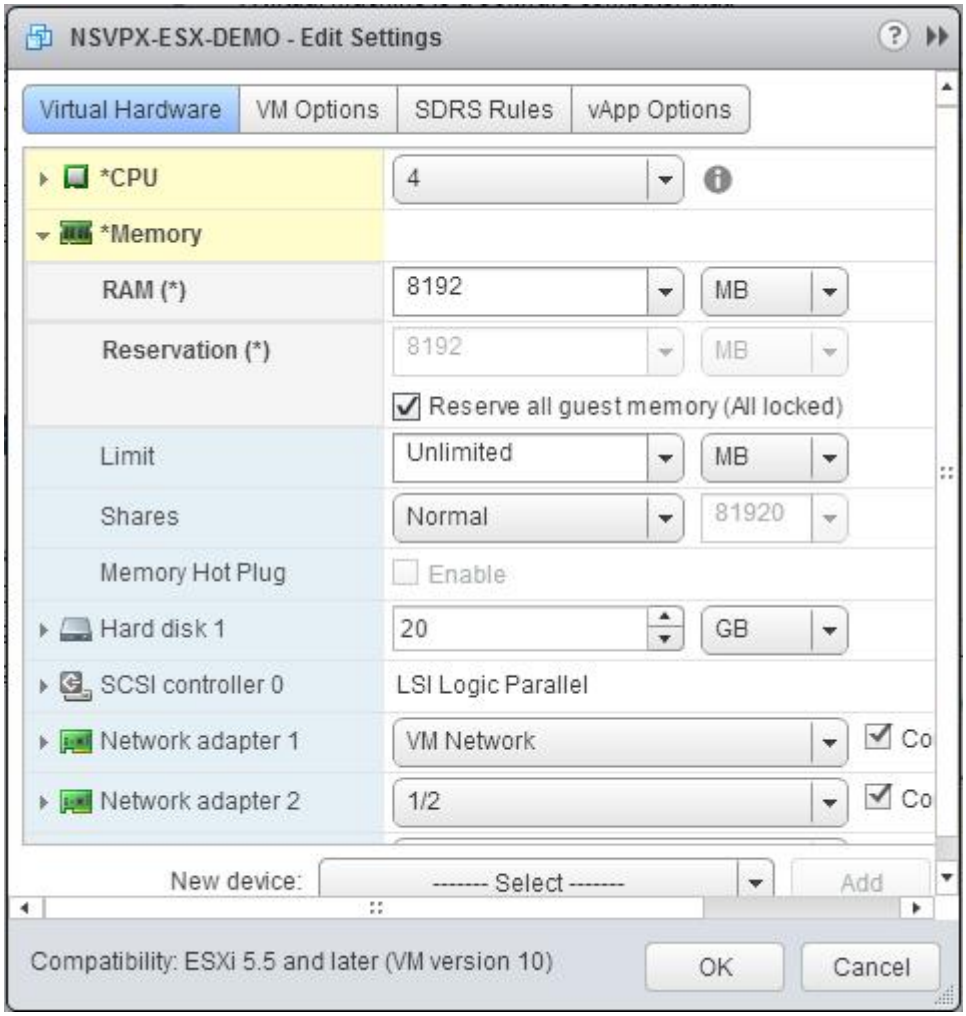
   a. Wählen Sie in der RAM-Dropdownliste die Größe des RAM aus. Es muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss der Arbeitsspeicher 4 x 2 GB = 8 GB betragen.

   Hinweis: Stellen Sie bei einer Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.

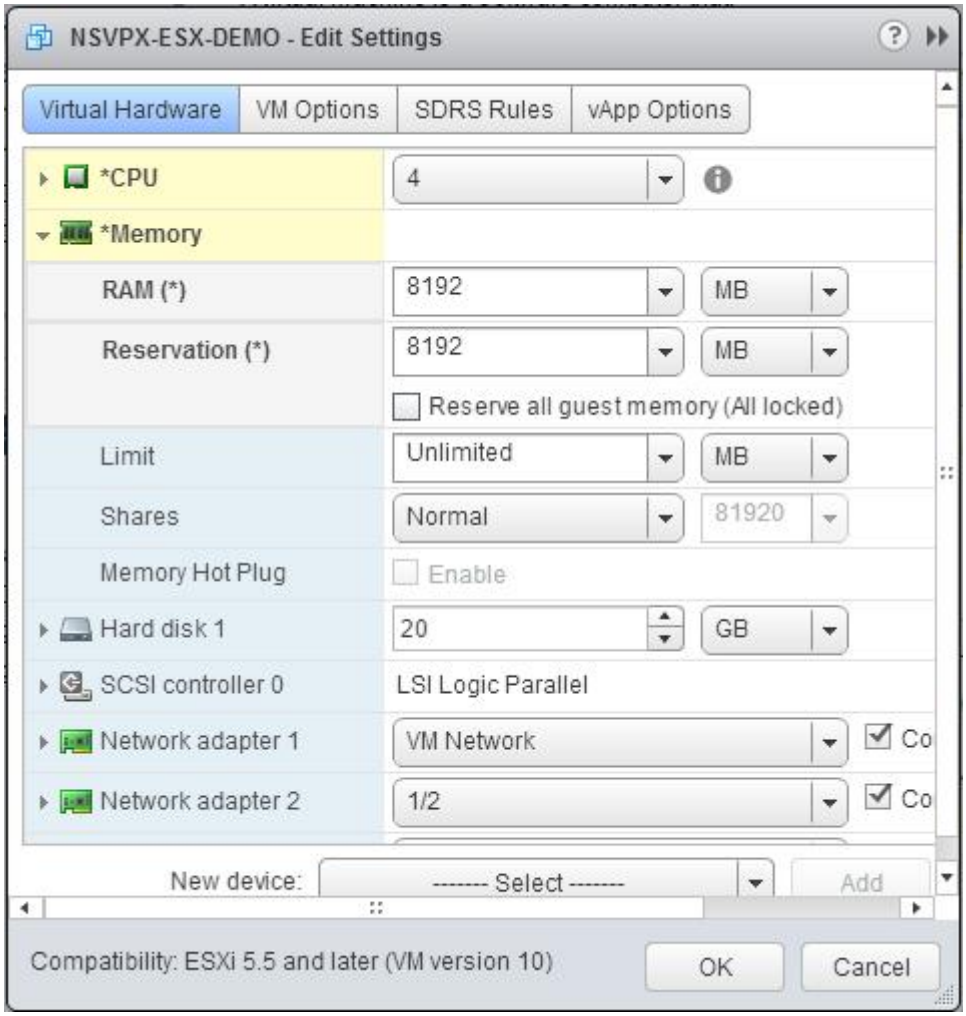


b. Geben Sie in der Dropdownliste Reservierung den Wert für die Speicherreservierung ein und aktivieren Sie das Kontrollkästchen Gesamten Gastspeicher reservieren (Alles gesperrt) . Die Speicherreservierung muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

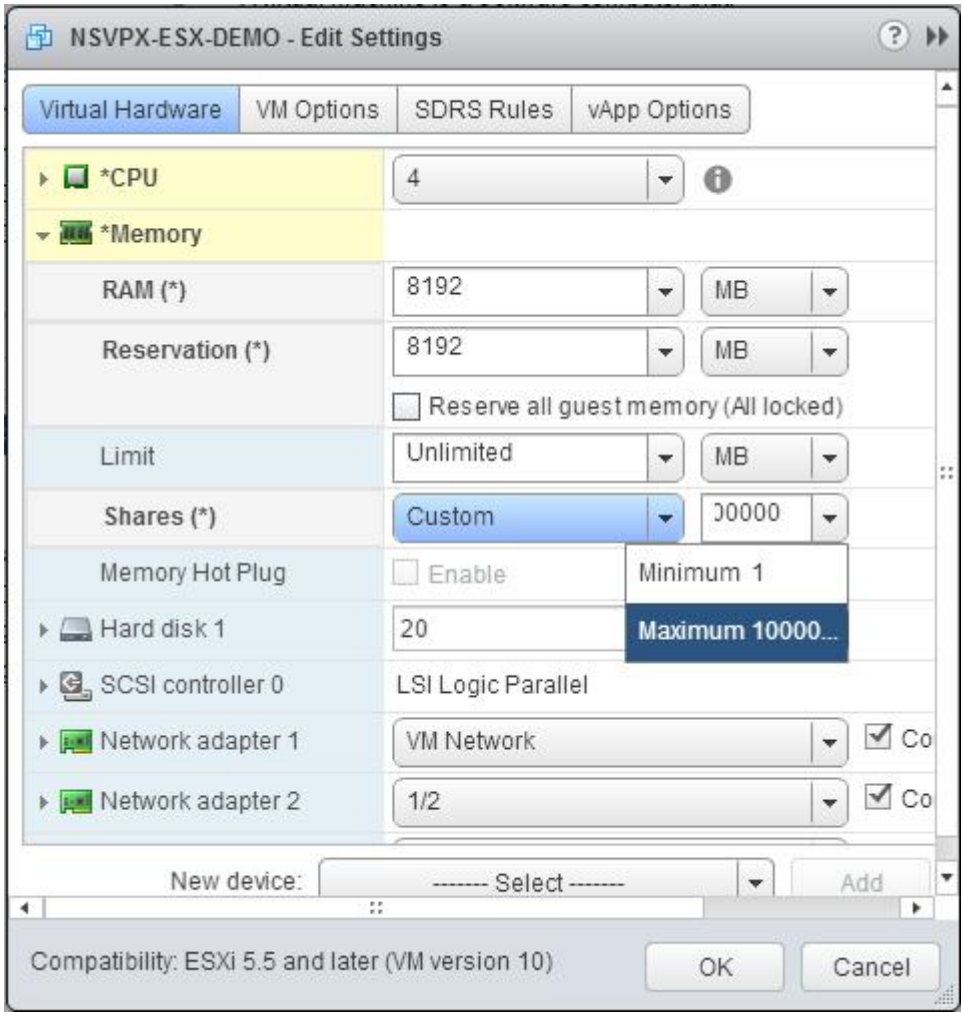
Hinweis: Stellen Sie bei einer Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.



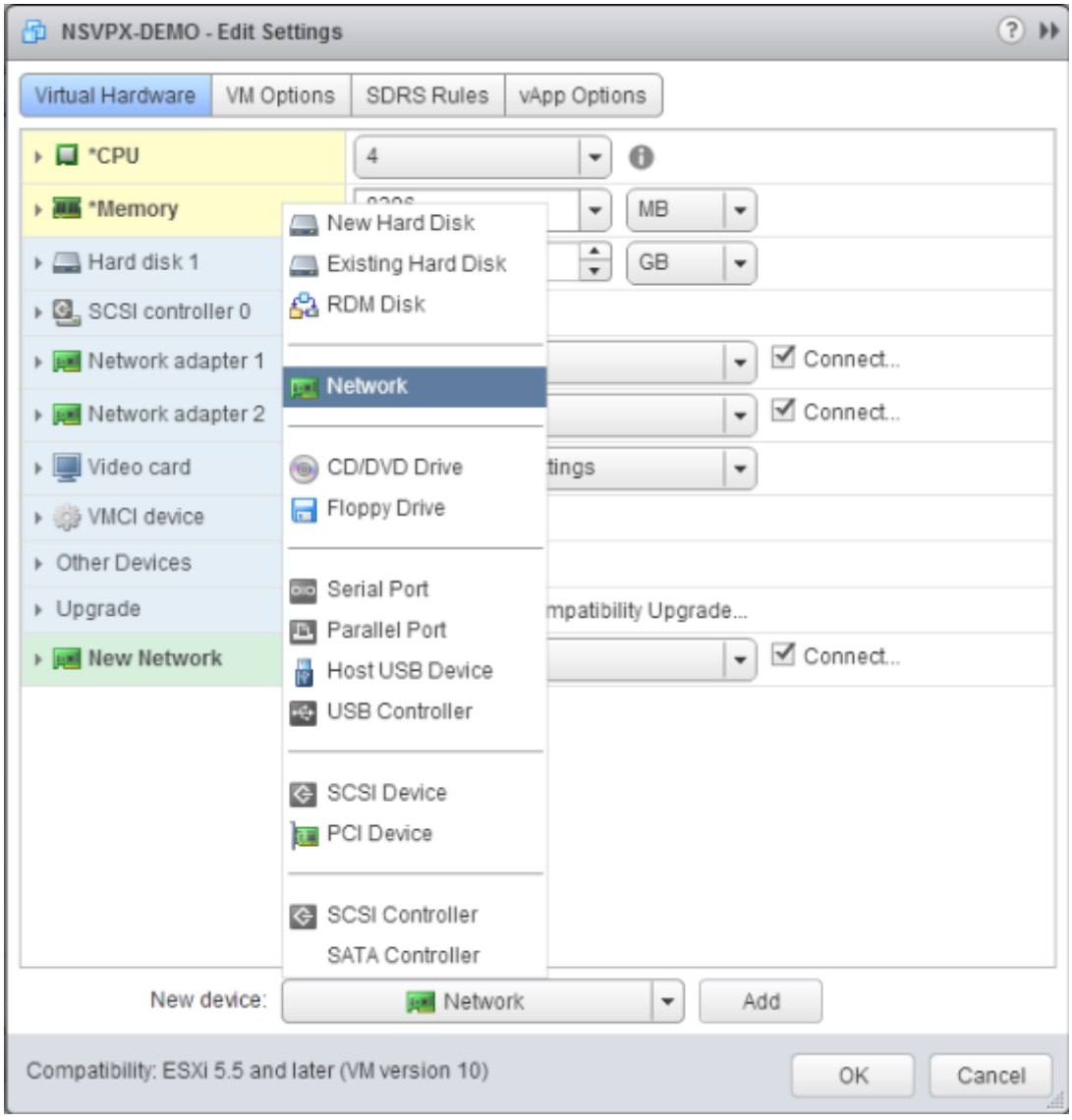
c. Wählen Sie in der Dropdownliste Limit die Zahl aus, die als Maximalwert angezeigt wird.



d. Wählen Sie in den Dropdownlisten Freigaben die Option Benutzerdefiniert und die Zahl, die als Maximalwert angezeigt wird.



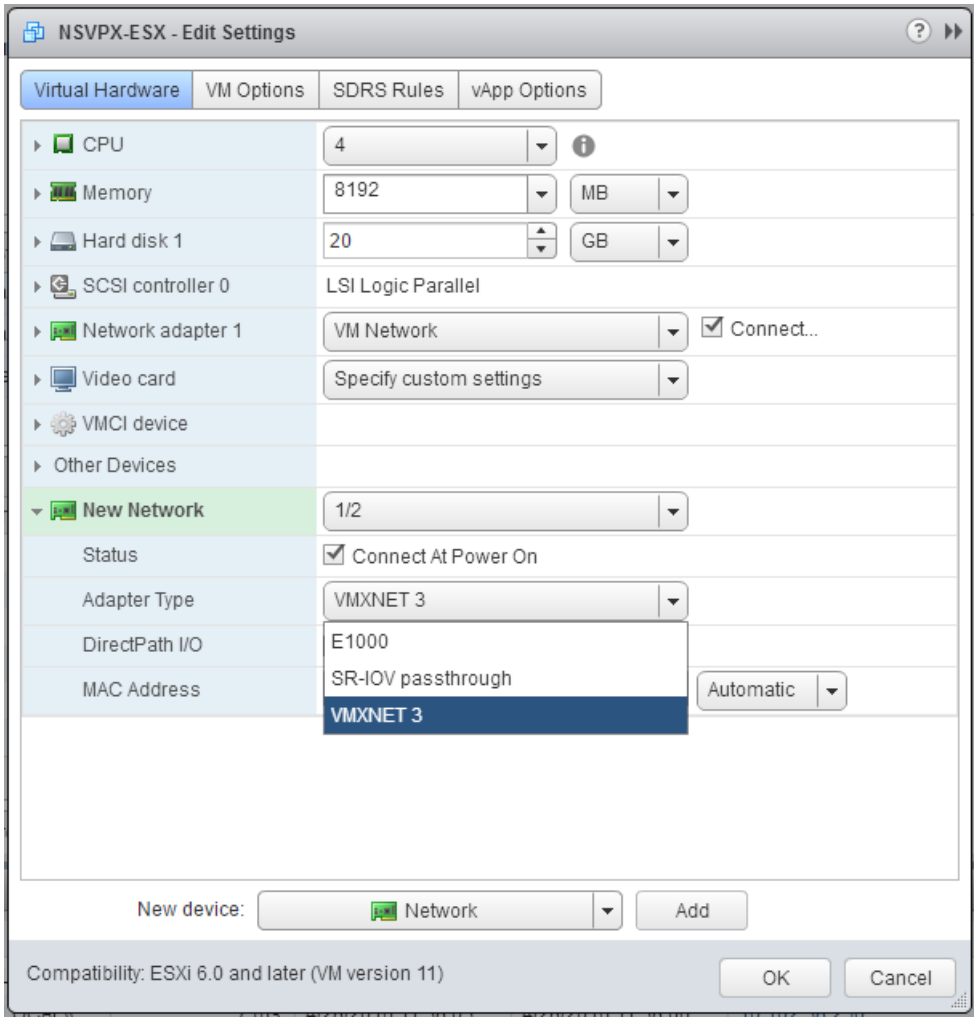
7. Fügen Sie eine VMXNET3-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdownliste Neues Gerät die Option Netzwerk aus und klicken Sie auf Hinzufügen.



8. Wählen Sie im Abschnitt Neues Netzwerk aus der Dropdownliste die Netzwerkschnittstelle aus, und führen Sie die folgenden Schritte aus:

   a. Wählen Sie in der Dropdownliste Adaptertyp die Option VMXNET3 aus.

> **Wichtig**
>
> Die standardmäßige E1000-Netzwerkschnittstelle und VMXNET3 können nicht koexistieren. Stellen Sie sicher, dass Sie die E1000-Netzwerkschnittstelle entfernen und VMXNET3 (0/1) als Verwaltungsschnittstelle verwenden.



9. Klicken Sie auf OK.
10. Schalten Sie die NetScaler VPX-Instanz ein.
11. Sobald die NetScaler VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

    > show interface summary

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

```
1 > show interface summary
2 ---------------------------------------------------------------------------

3       Interface  MTU        MAC                Suffix
4 ---------------------------------------------------------------------------

5 1     0/1        1500       00:0c:29:89:1d:0e  NetScaler Vir...rface,
      VMXNET3
```



```
6 2     1/1         9000        00:0c:29:89:1d:18    NetScaler Vir...rface,
      VMXNET3
7 3     1/2         9000        00:0c:29:89:1d:22    NetScaler Vir...rface,
      VMXNET3
8 4     LO/1        9000        00:0c:29:89:1d:0e    Netscaler Loopback
    interface
```

> **Hinweis**
>
> Nachdem Sie eine VMXNET3-Schnittstelle hinzugefügt und die NetScaler VPX Appliance neu gestartet haben, ändert der VMware ESX-Hypervisor möglicherweise die Reihenfolge, in der die NIC der VPX-Appliance angezeigt wird. Daher bleibt der Netzwerkadapter 1 möglicherweise nicht immer 0/1, was zu einem Verlust der Verwaltungskonnektivität mit der VPX-Appliance führt. Um dieses Problem zu vermeiden, ändern Sie das virtuelle Netzwerk des Netzwerkadapters entsprechend.
>
> Dies ist eine Einschränkung des VMware ESX Hypervisors.

Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

May 11, 2023

Nachdem Sie die NetScaler VPX-Instanz auf VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere Webclient verwenden, um die virtuelle Appliance für die Verwendung von Single-Root-I/O-V-Virtualisierungs-Netzwerkschnittstellen (SR-IOV) zu konfigurieren.

Einschränkungen

Für NetScaler VPX, die mit SR-IOV-Netzwerkschnittstelle konfiguriert ist, gelten folgende Einschränkungen:

- Die folgenden Funktionen werden auf SR-IOV-Schnittstellen, die die Intel 82599 10G-NIC auf ESX VPX verwenden, nicht unterstützt:
  - L2-Modus Umschaltung
  - Statische Link-Aggregation und LACP
  - Clustering
  - Admin-Partitionierung [Shared VLAN-Modus]
  - Hochverfügbarkeit [Aktiv - Aktiver Modus]
  - Jumbo-Rahmen
  - IPv6

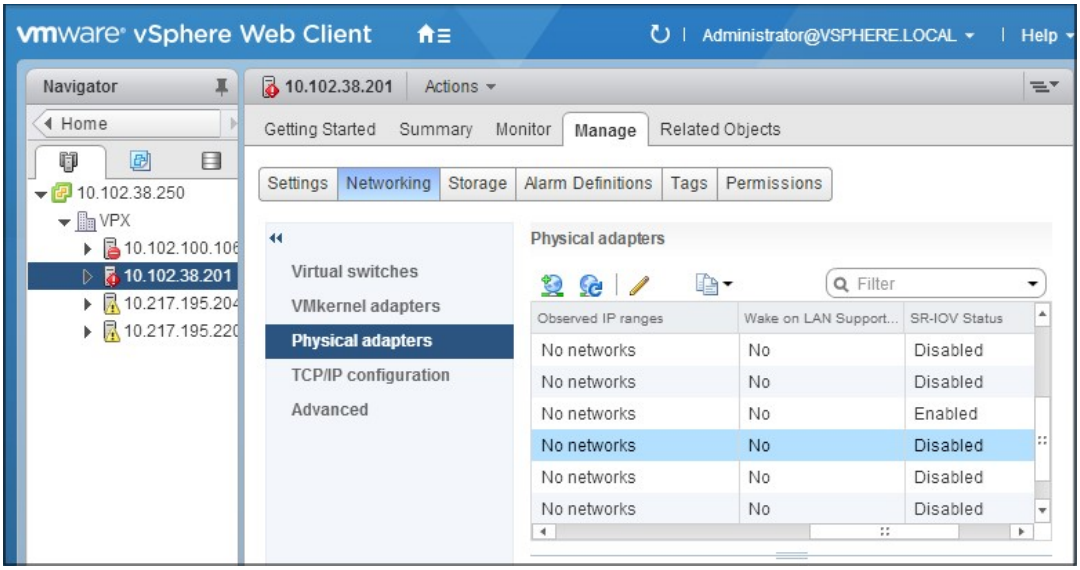
- Die folgenden Funktionen werden auf der SR-IOV-Schnittstelle mit einer Intel 82599 10G-NIC auf KVM VPX nicht unterstützt:
  - Statische Link-Aggregation und LACP
  - L2-Modus Umschaltung
  - Clustering
  - Admin-Partitionierung [Shared VLAN-Modus]
  - Hohe Verfügbarkeit [Aktiv — Aktiver Modus]
  - Jumbo-Rahmen
  - IPv6
  - Die VLAN-Konfiguration auf Hypervisor für SR-IOV VF-Schnittstelle über `ip link` Befehl wird nicht unterstützt

Voraussetzung

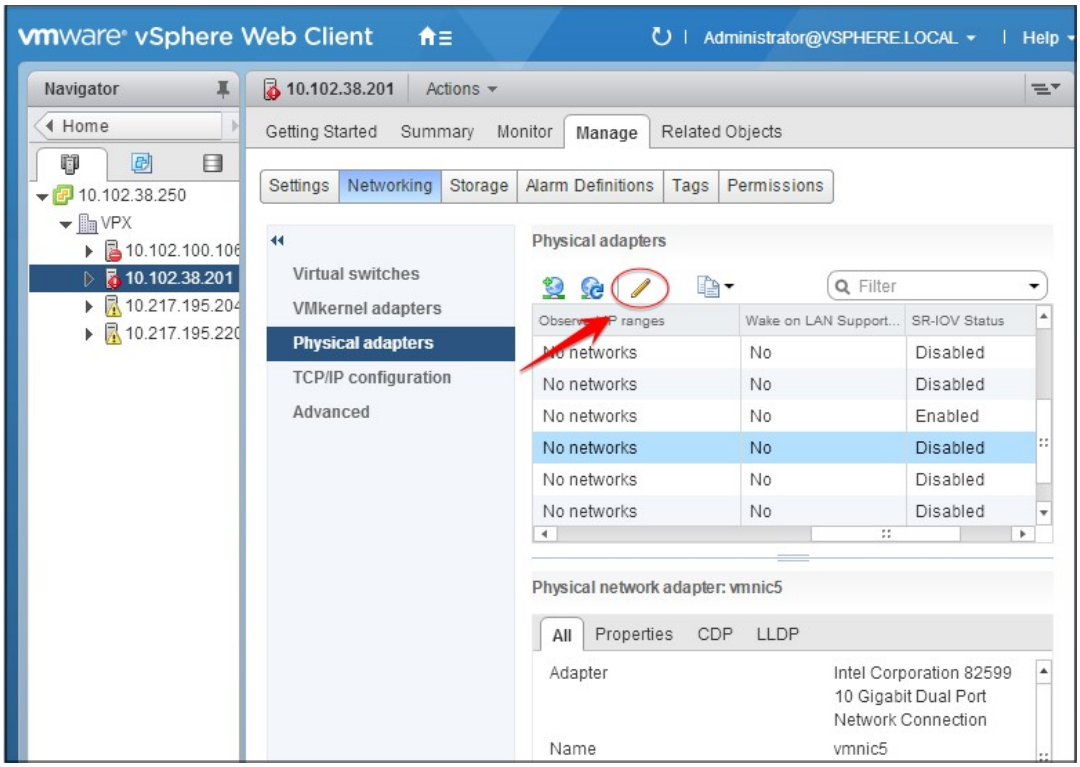
- Stellen Sie sicher, dass Sie dem ESX-Host eine der folgenden Netzwerkkarten hinzufügen:
  - Intel 82599 NIC, IXGBE-Treiberversion 3.7.13.7.14iov oder höher wird empfohlen.
  - Mellanox ConnectX-4 NIC
- Aktivieren Sie SR-IOV auf dem physischen Hostadapter.

  Gehen Sie wie folgt vor, um SR-IOV auf dem physischen Hostadapter zu aktivieren:

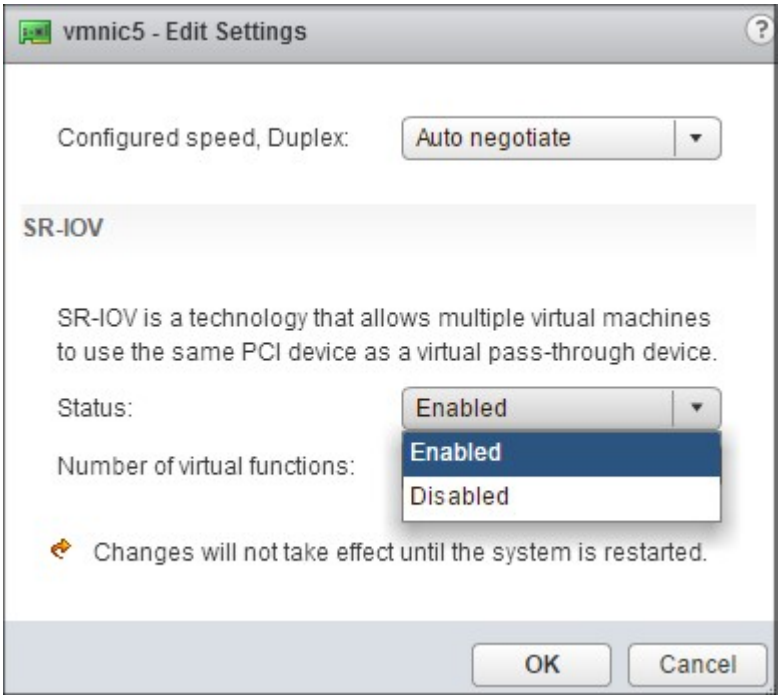
  1. Navigieren Sie im vSphere Web Client zum Host.
  2. Wählen Sie auf der Registerkarte **Verwalten > Netzwerk** die Option **Physikalische Adapter**aus. Das Feld SR-IOV Status zeigt an, ob ein physischer Adapter SR-IOV unterstützt.



3. Wählen Sie den physischen Adapter aus, und klicken Sie dann auf das Stiftsymbol, um das Dialogfeld **Einstellungen bearbeiten** zu öffnen.

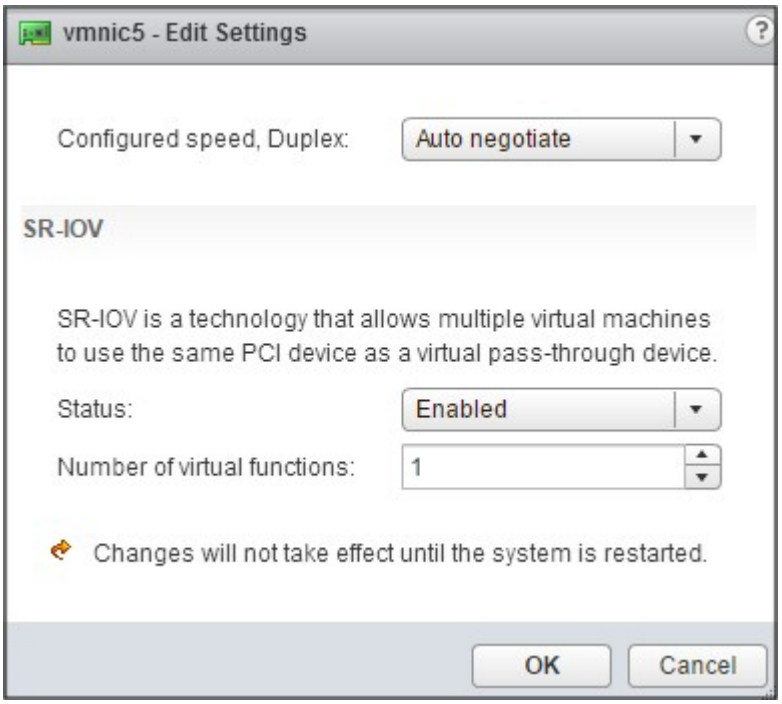


4. Wählen Sie unter SR-IOV in der Dropdownliste **Status** die Option **Aktiviert** aus.



5. Geben Sie im Feld **Anzahl der virtuellen Funktionen** die Anzahl der virtuellen Funktionen

ein, die Sie für den Adapter konfigurieren möchten.



6. Klicken Sie auf **OK**.
7. Starten Sie den Host neu.

- Erstellen Sie einen Distributed Virtual Switch (DVS) und `Portgroups`. Anweisungen finden Sie in der VMware Dokumentation.

  > **Hinweis**
  >
  > Citrix hat die SR-IOV-Konfiguration `Portgroups` nur auf DVS qualifiziert.

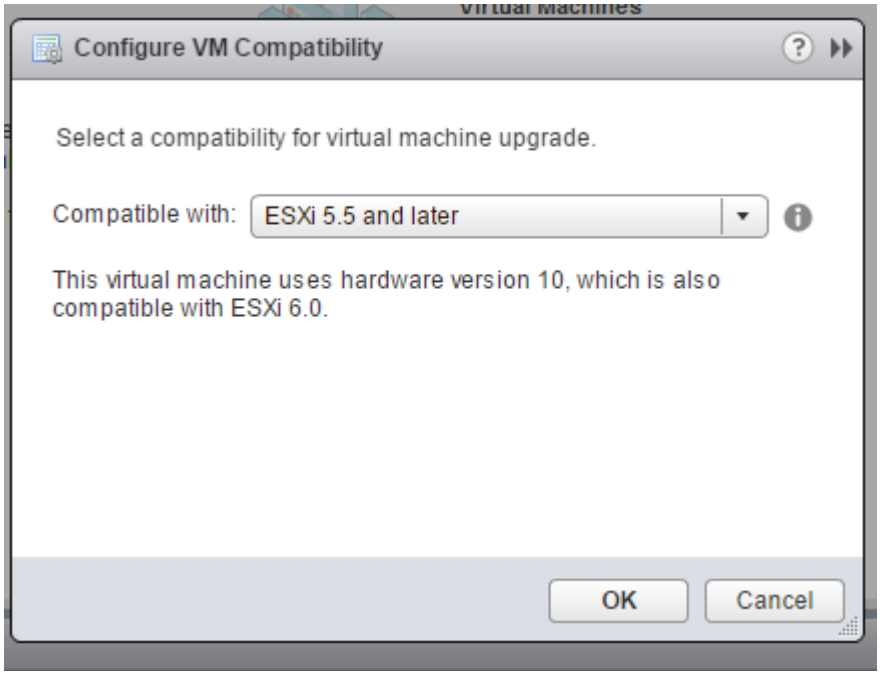
So konfigurieren Sie NetScaler VPX-Instanzen für die Verwendung der SR-IOV-Netzwerkschnittstelle mithilfe von VMware vSphere Web Client:

1. Wählen Sie im vSphere Web Client **Hosts und Cluster**aus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der NetScaler VPX-Instanz wie folgt auf ESX 5.5 oder höher:

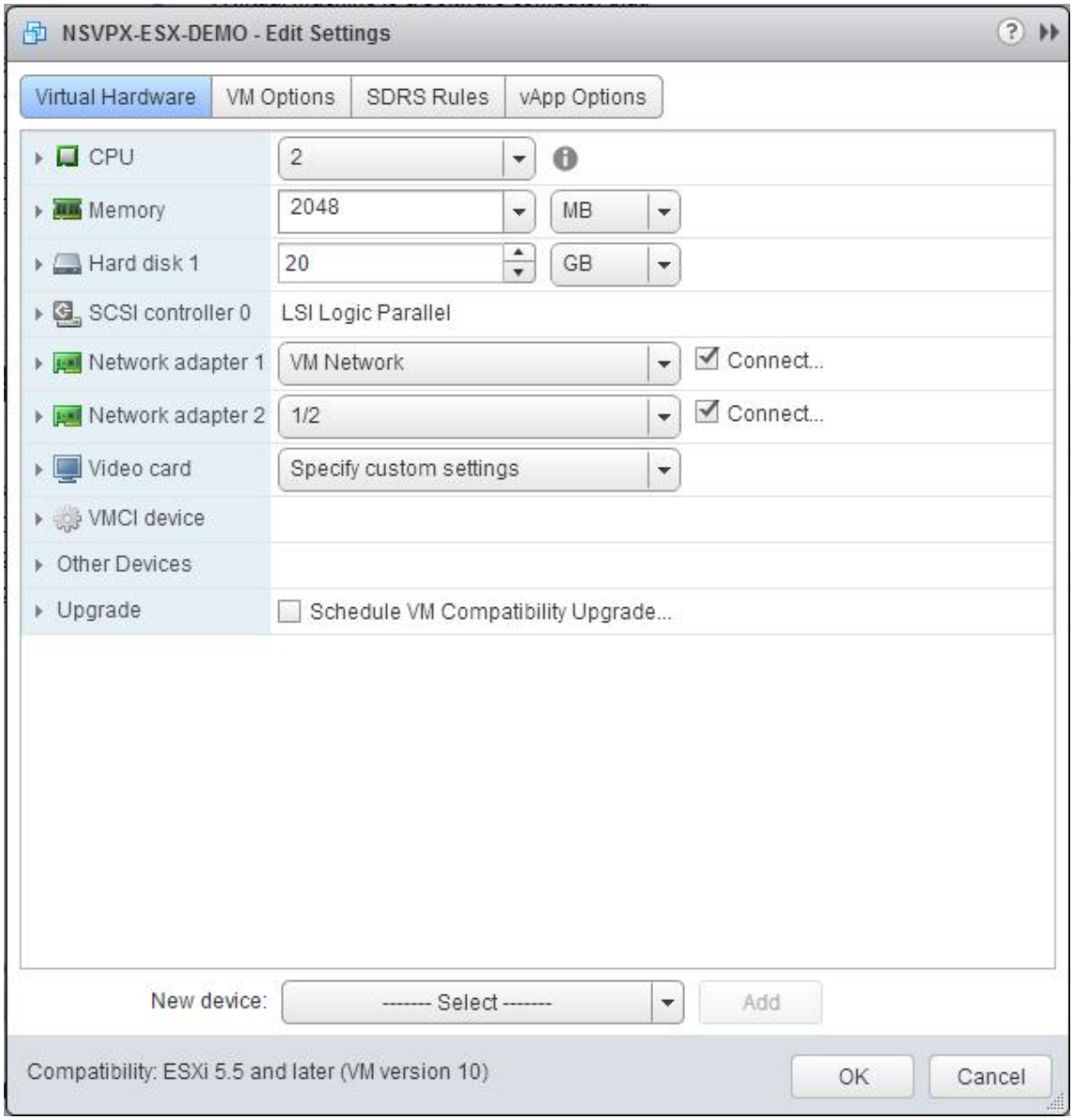
   a. Schalten Sie die NetScaler VPX-Instanz aus.

   b. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und wählen Sie **Kompatibilität > VM-Kompatibilität aktualisieren**.

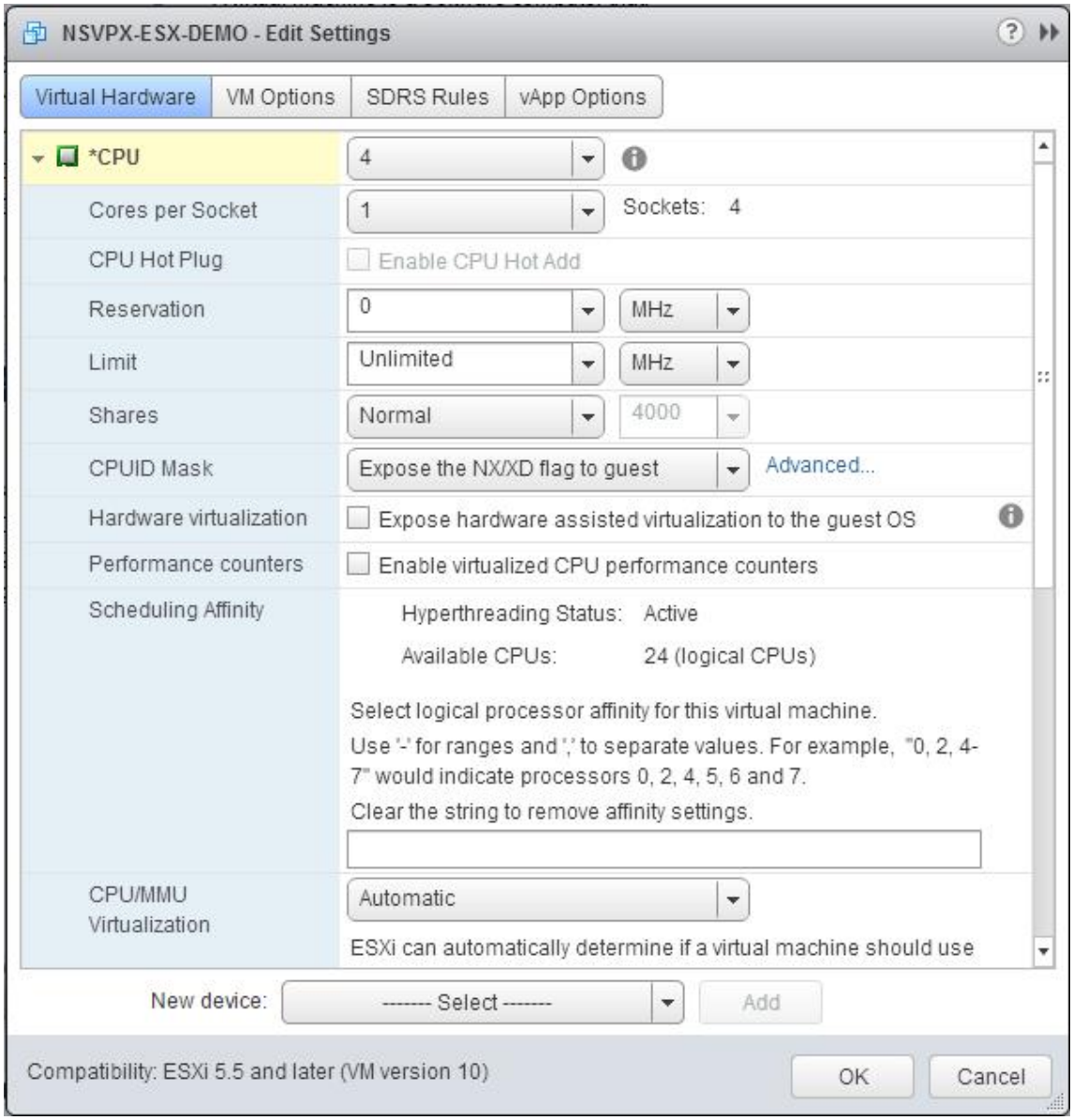
   c. Wählen **Sie im Dialogfeld „VM-Kompatibilität konfigurieren** “ in der Dropdownliste „ **Kompatibel mit** “ die Option **ESXi 5.5 und höher** aus und klicken Sie auf „ **OK“**.



3. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX Instanz, und klicken Sie auf **Einstellungen bearbeiten**.



4. Klicken Sie im Dialogfeld **<virtual_appliance> - Einstellungen bearbeiten** auf den Abschnitt **CPU**.



5. Aktualisieren Sie im Abschnitt **CPU** die folgenden Einstellungen:

   - CPU-Anzahl
   - Anzahl der Buchsen
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

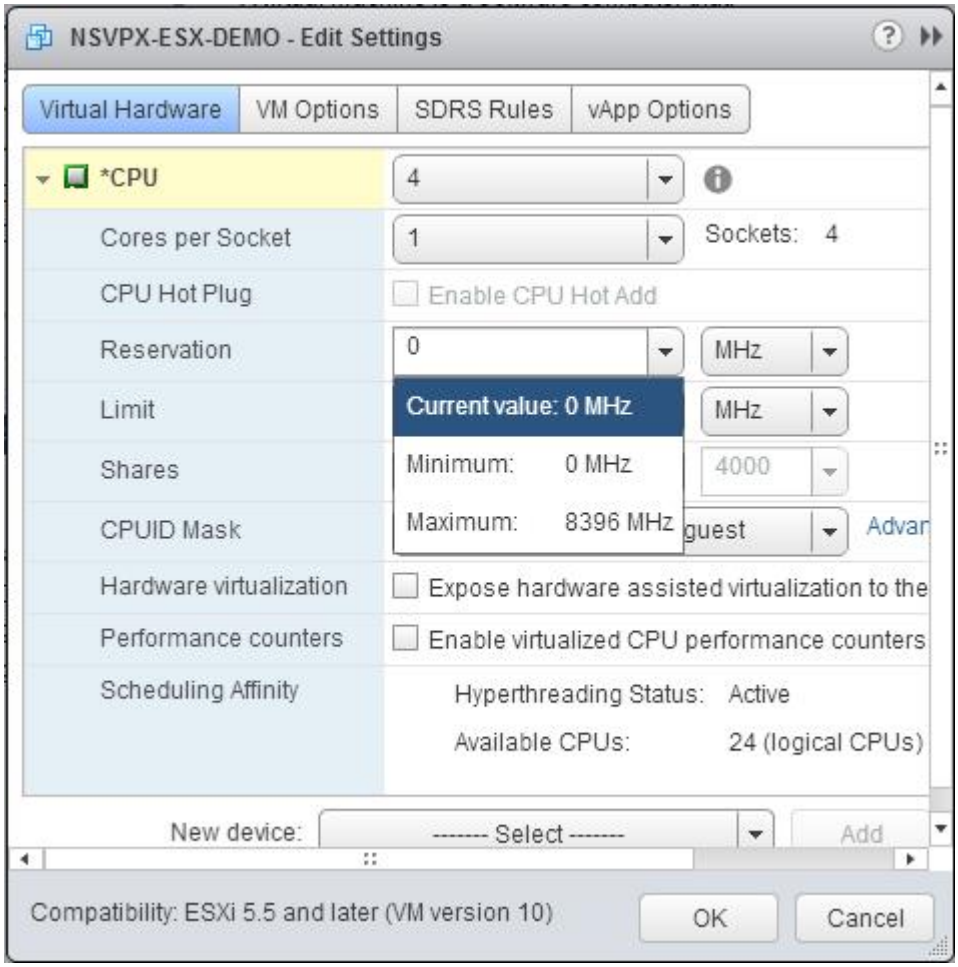
   a. Wählen Sie in der Dropdownliste **CPU** die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

   b. Wählen Sie in der Dropdownliste **Kerne pro Socket** die Anzahl der Sockets aus.

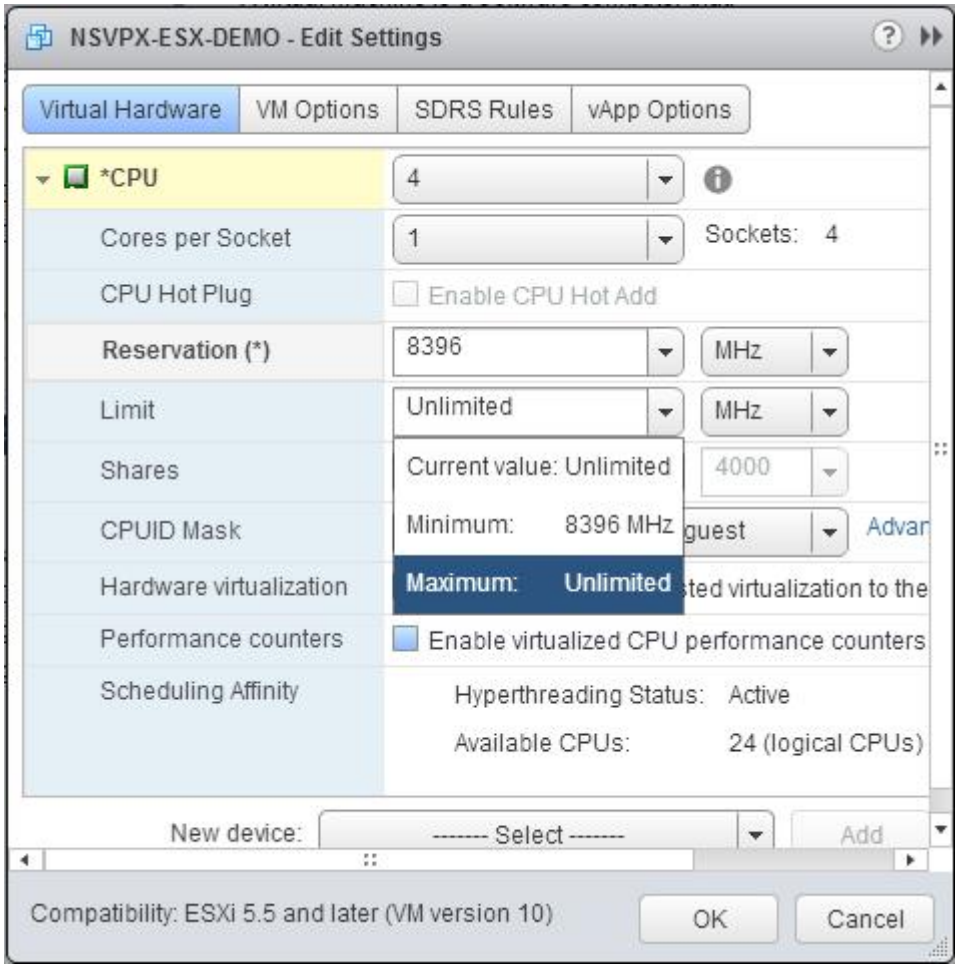
c. (Optional) Aktivieren oder deaktivieren Sie im Feld **CPU Hot Plug** das Kontrollkästchen **Enable CPU Hot Add** .

Hinweis: Citrix empfiehlt, die Standardeinstellung zu akzeptieren (deaktiviert).

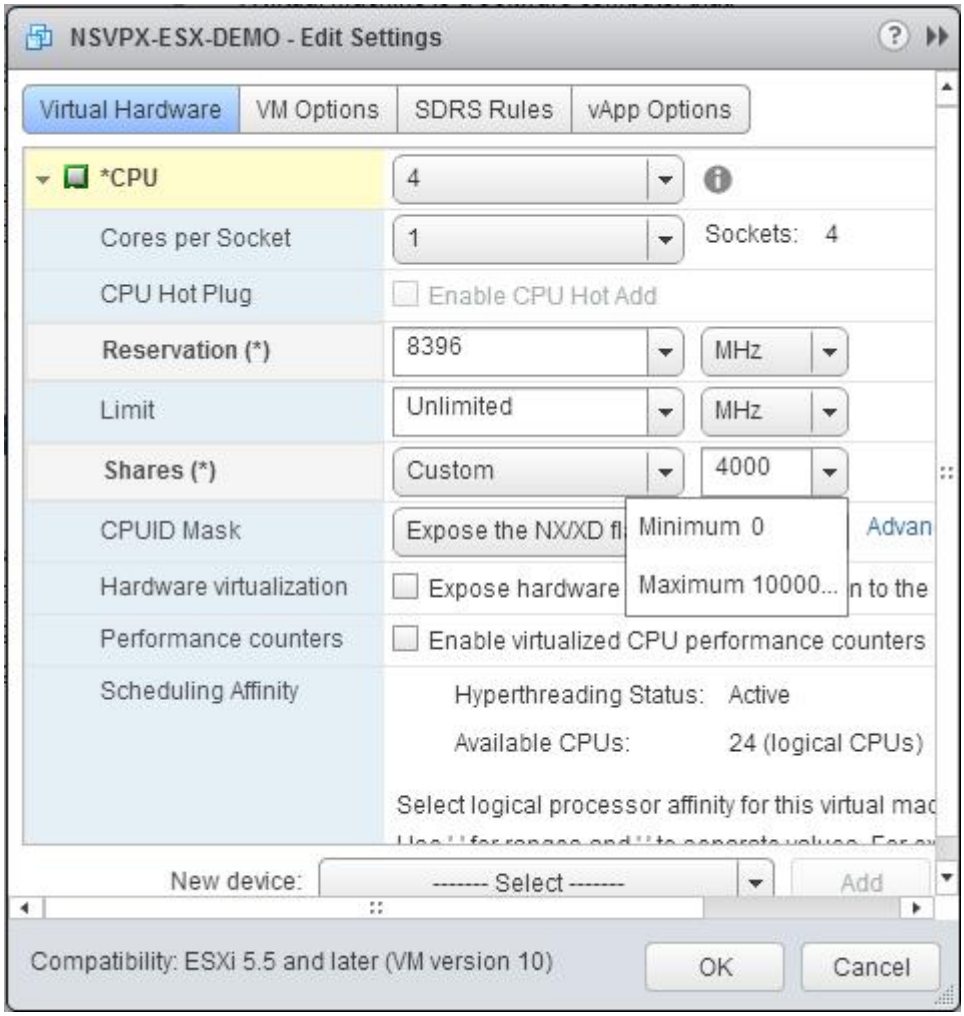
d. Wählen Sie in der Dropdownliste **Reservierung** die Zahl aus, die als Maximalwert angezeigt wird.



e. Wählen Sie in der Dropdownliste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.



f. Wählen Sie in den Dropdownlisten **Anteile** die Option **Benutzerdefiniert** und die Zahl aus, die als Maximalwert angezeigt wird.



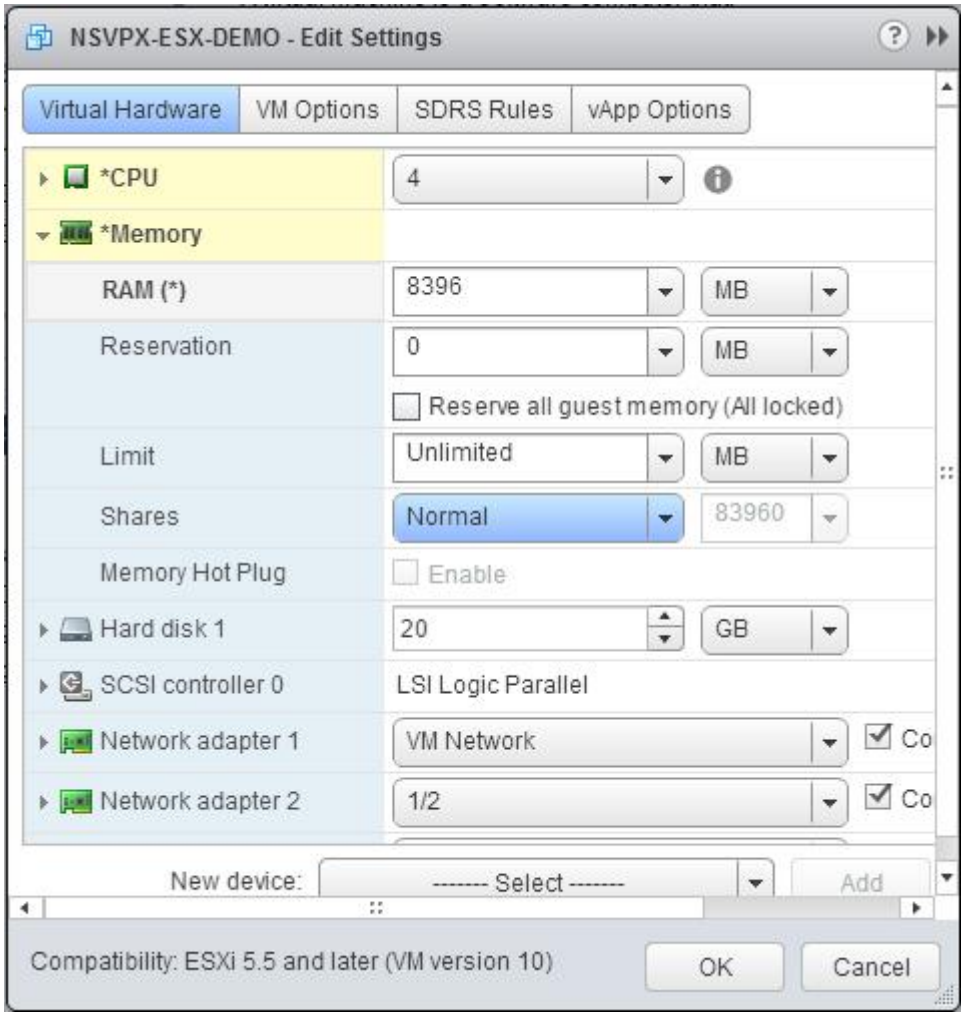
6. Aktualisieren Sie im Abschnitt **Speicher** die folgenden Einstellungen:

   - Größe des RAM
   - Reservierungen
   - Limit
   - Aktien

   Legen Sie die Werte wie folgt fest:

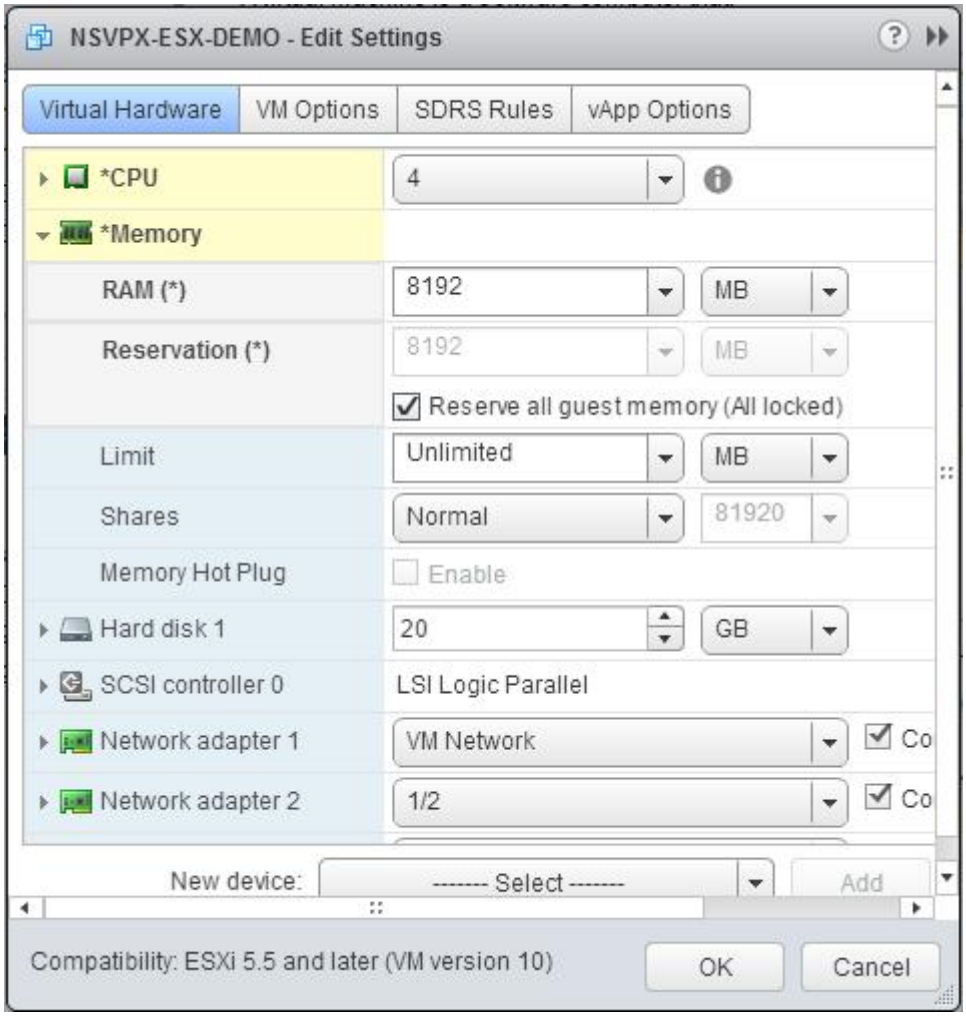
   a. Wählen Sie in der **RAM-Dropdownliste** die Größe des RAM aus. Es muss die Anzahl der vCPUs x 2 GB sein. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 2 GB = 8 GB.

   Hinweis: Stellen Sie für die Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.

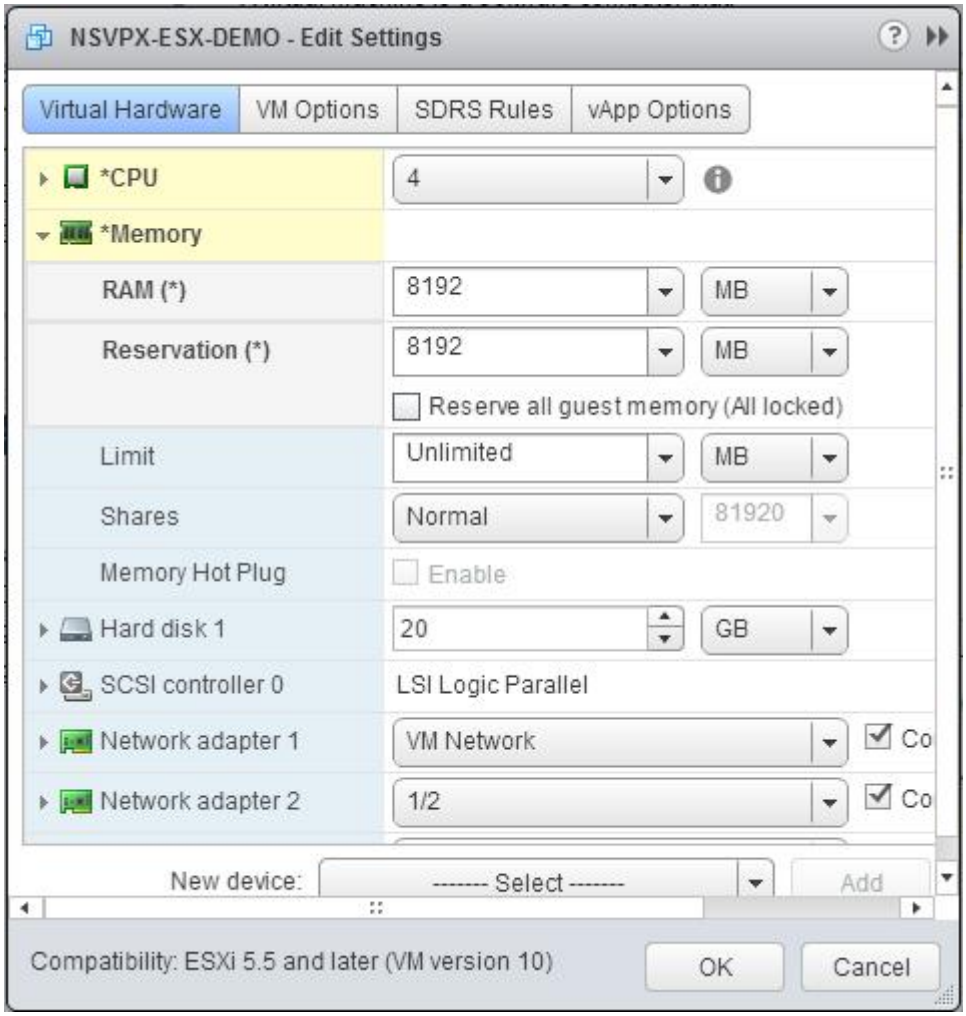


b. Geben Sie in der Dropdownliste **Reservierung** den Wert für die Speicherreservierung ein und aktivieren Sie das Kontrollkästchen **Gesamten Gastspeicher reservieren (Alles gesperrt)** . Die Speicherreservierung muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

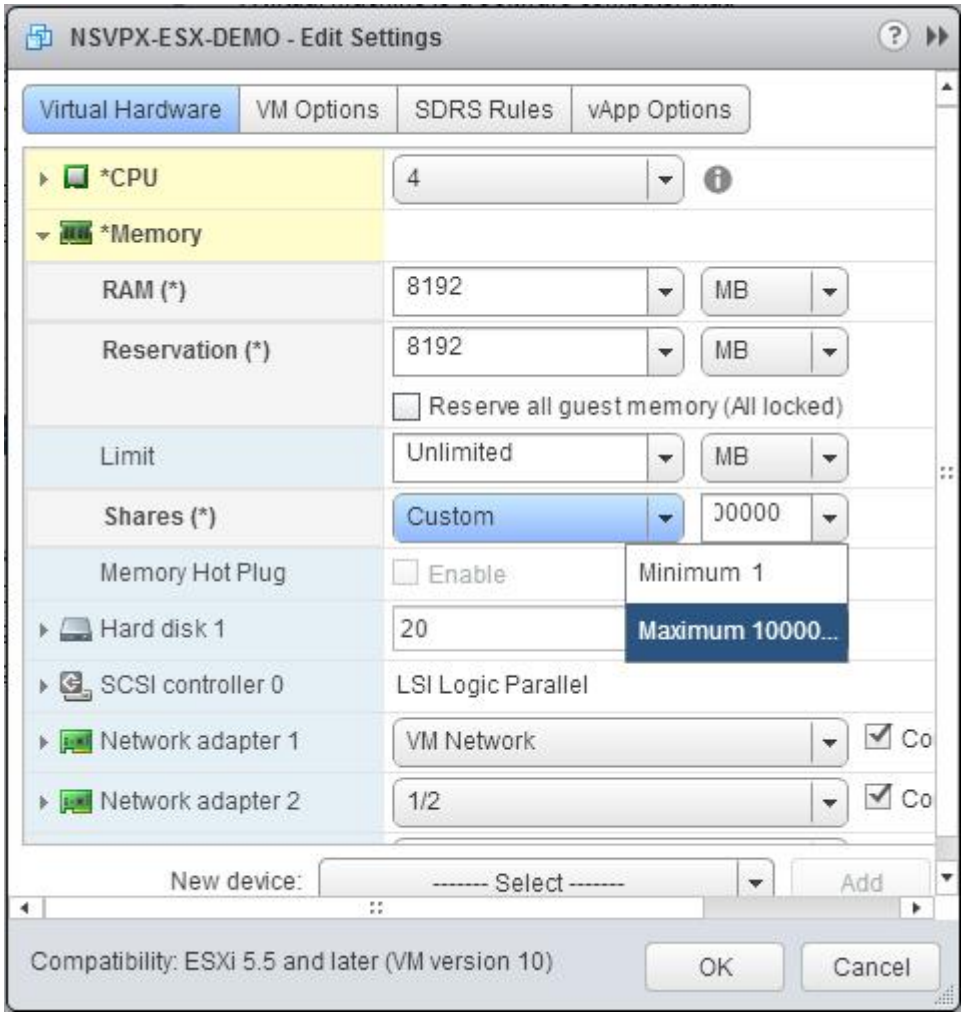
Hinweis: Stellen Sie für die Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.



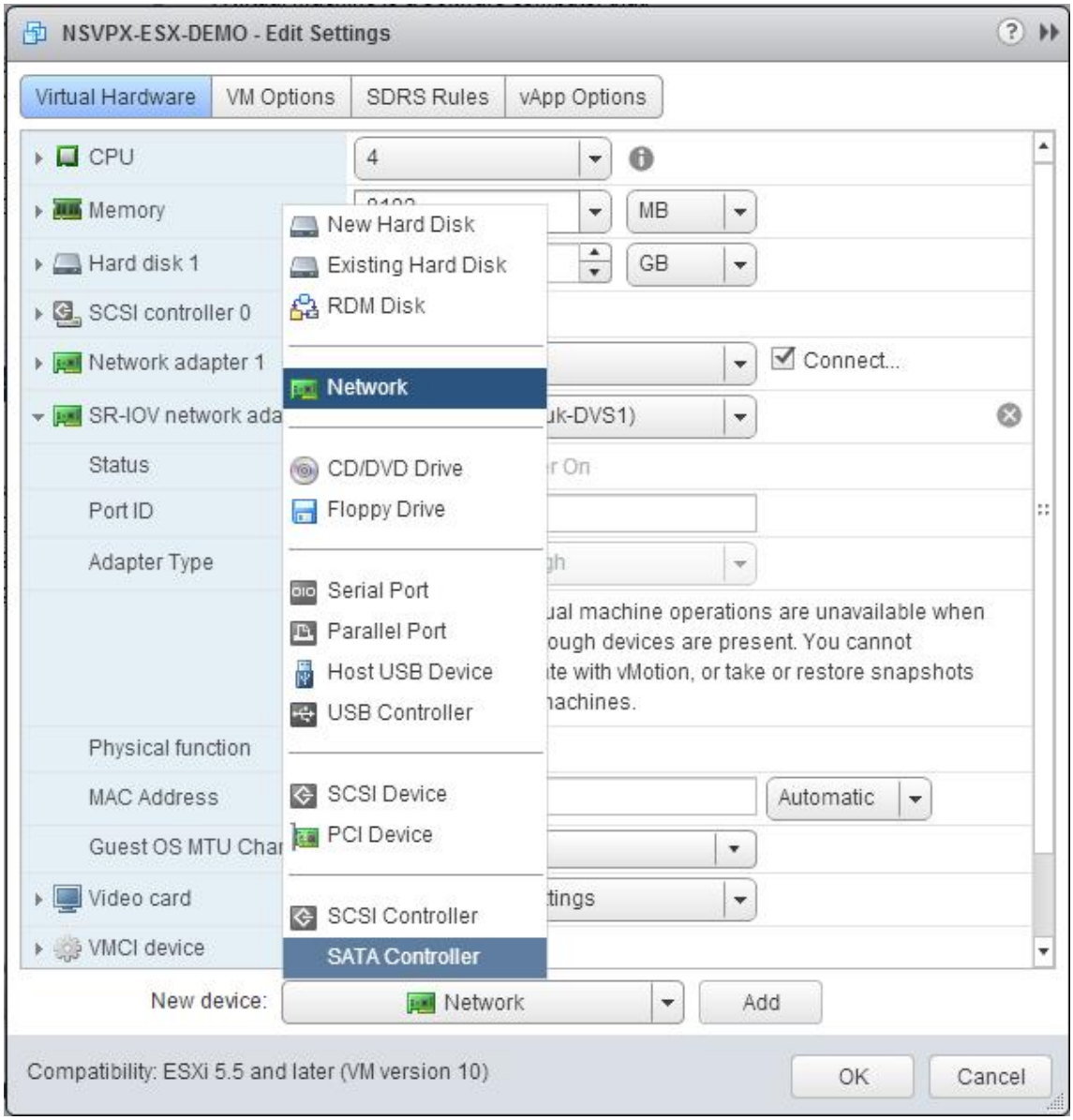
c. Wählen Sie in der Dropdownliste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.



d. Wählen Sie in den Dropdownlisten **Freigaben** die Option **Benutzerdefiniert** aus, und wählen Sie die Zahl aus, die als Maximalwert angezeigt wird.

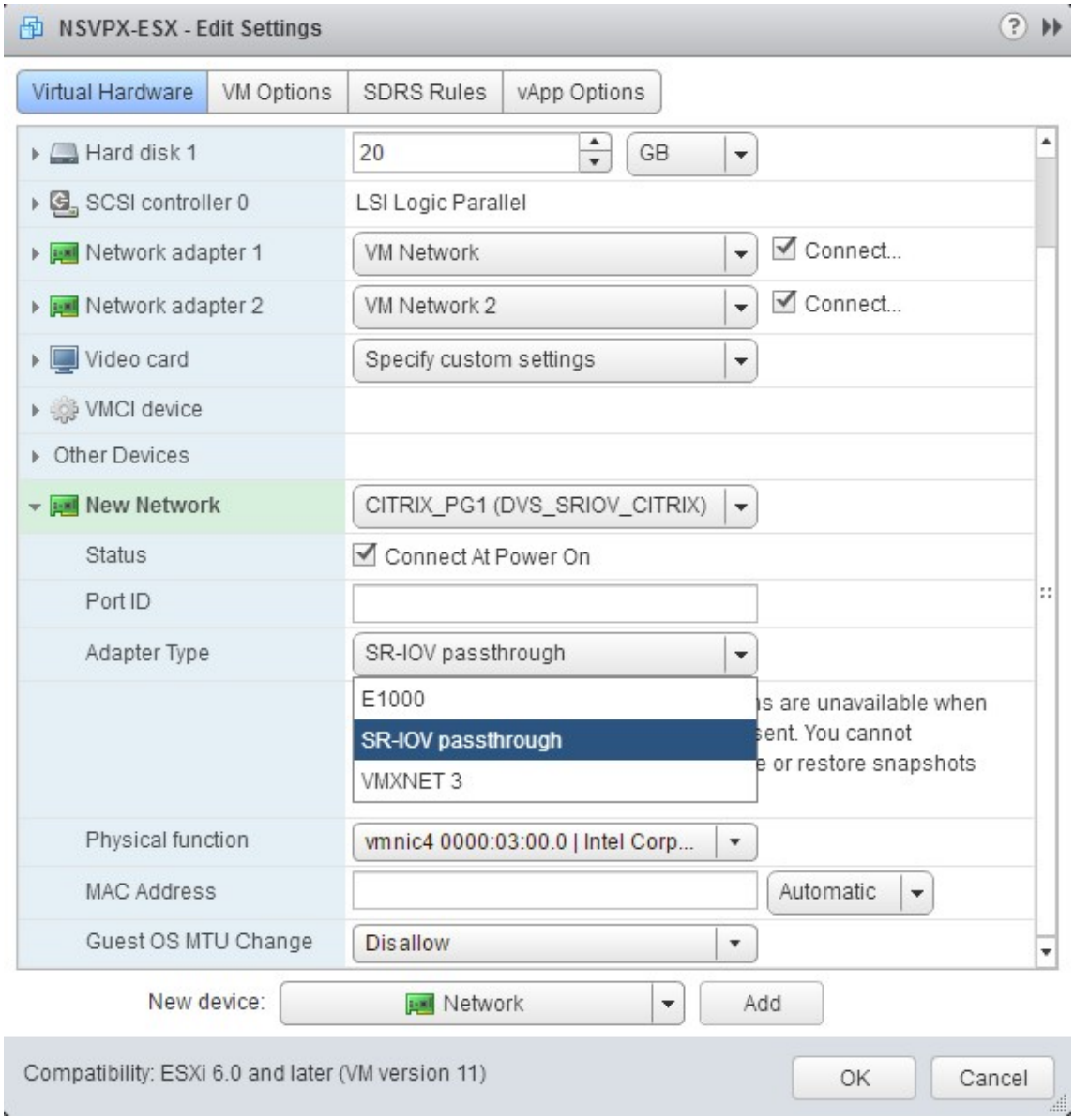


7. Fügen Sie eine SR-IOV-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdownliste **Neues Gerät** die Option **Netzwerk** aus und klicken Sie auf **Hinzufügen**.

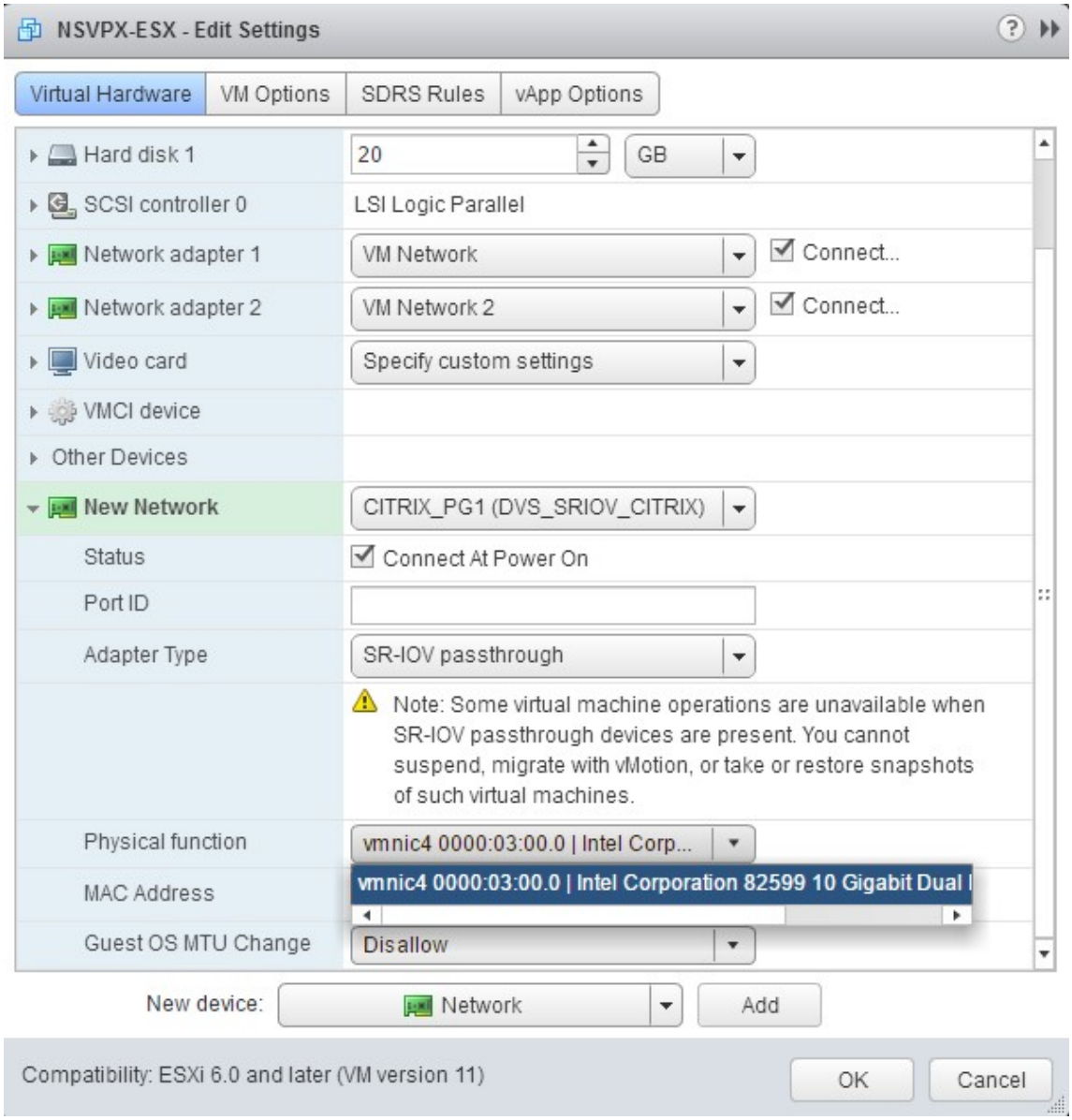


8. Im Abschnitt **Neues Netzwerk**. Wählen Sie in der Dropdownliste `Portgroup` das von Ihnen erstellte aus, und gehen Sie wie folgt vor:

   a. Wählen Sie in der Dropdownliste **Adaptertyp** die Option **SR-IOV-Passthrough** aus.

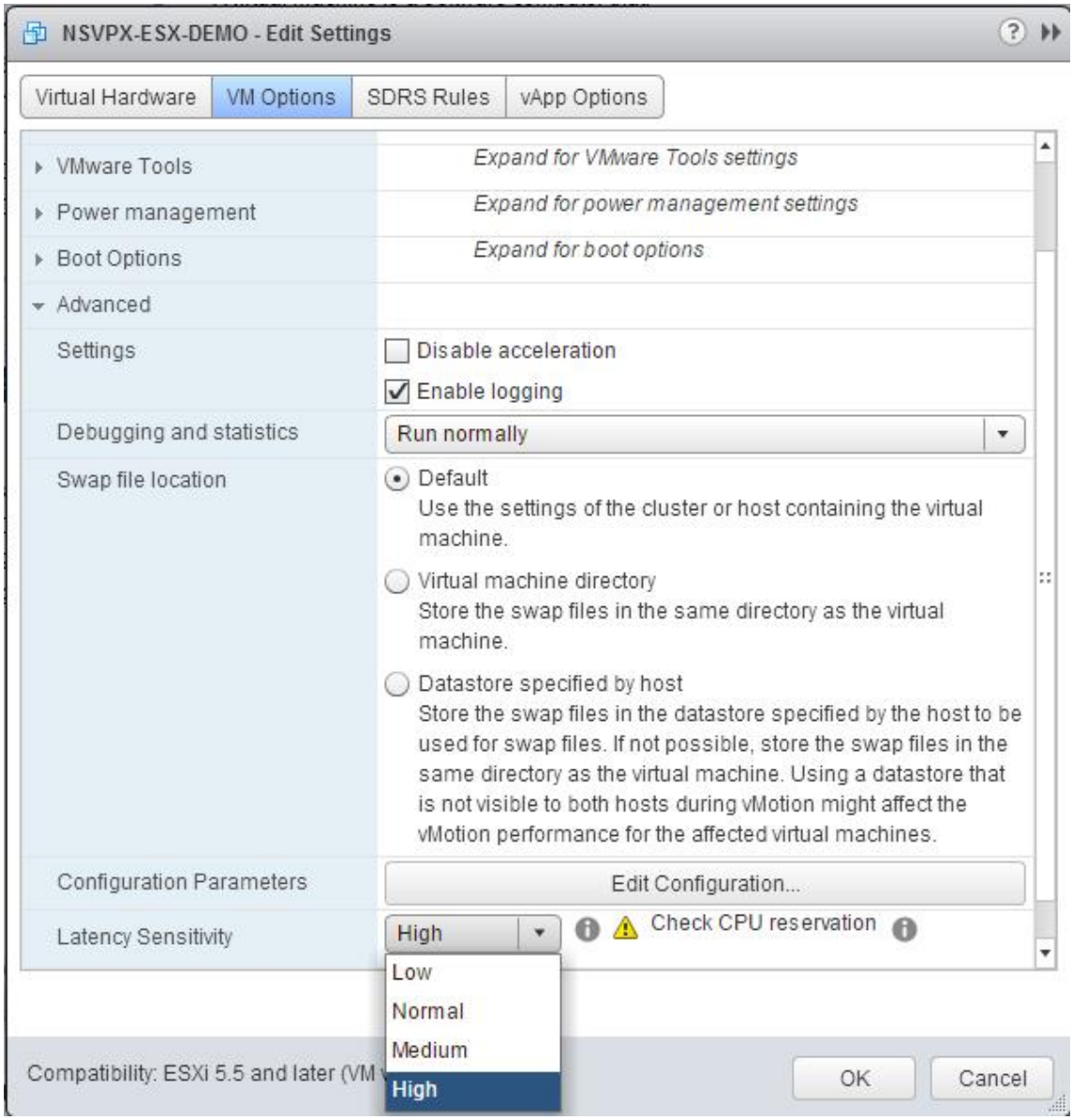


b. Wählen Sie in der Dropdownliste **Physische Funktion** den physischen Adapter aus, der dem zugeordnet ist `Portgroup`.



c. Wählen Sie in der Dropdownliste **MTU-Änderung des Gastbetriebssystems** die Option **Nicht zulassen**aus.

9. Klicken Sie im <virtual_appliance>Dialogfeld **— Einstellungen bearbeiten** auf die Registerkarte **VM-Optionen** .
10. Wählen Sie auf der Registerkarte **VM-Optionen** den Abschnitt **Erweitert** aus. Wählen Sie in der Dropdownliste **Latenzempfindlichkeit** die Option **Hoch** aus.



11. Klicken Sie auf **OK**.
12. Schalten Sie die NetScaler VPX-Instanz ein.
13. Sobald die NetScaler VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

    ```
    show interface summary
    ```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

```
1 > show interface summary
2 ---------------------------------------------------------------------------

3       Interface  MTU        MAC                Suffix
```



```
4  ----------------------------------------------------------------------------

5  1     0/1        1500       00:0c:29:1b:81:0b    NetScaler Virtual
       Interface
6  2     10/1       1500       00:50:56:9f:0c:6f    Intel 82599 10G VF
       Interface
7  3     10/2       1500       00:50:56:9f:5c:1e    Intel 82599 10G VF
       Interface
8  4     10/3       1500       00:50:56:9f:02:1b    Intel 82599 10G VF
       Interface
9  5     10/4       1500       00:50:56:9f:5a:1d    Intel 82599 10G VF
       Interface
10 6     10/5       1500       00:50:56:9f:4e:0b    Intel 82599 10G VF
       Interface
11 7     LO/1       1500       00:0c:29:1b:81:0b    Netscaler Loopback
       interface
12  Done
13 > show inter 10/1
14 1)      Interface 10/1 (Intel 82599 10G VF Interface) #1
15         flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
16         MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
               h21m53s
17         Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
               throughput 10000
18         LLDP Mode: NONE,                LR Priority: 1024
19
20         RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
               Stalls(0)
21         TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0) Stalls
               (0)
22         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
23         Bandwidth thresholds are not set.
24  Done
```

Migration des NetScaler VPX von E1000 auf SR-IOV- oder VMXNET3-Netzwerkschnittstellen

May 11, 2023

24. Mai 2018

Sie können Ihre beendenden NetScaler VPX-Instanzen, die E1000 Netzwerkschnittstellen verwenden,

so konfigurieren, dass SR-IOV- oder VMXNET3-Netzwerkschnittstellen verwendet werden.

Informationen zum Konfigurieren einer vorhandenen NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen finden Sie unter Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle.

Informationen zum Konfigurieren einer vorhandenen NetScaler VPX-Instanz für die Verwendung von VMXNET3-Netzwerkschnittstellen finden Sie unter Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der VMXNET3-Netzwerkschnittstelle.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der PCI-Passthrough-Netzwerkschnittstelle

May 11, 2023

Übersicht

Nachdem Sie eine NetScaler VPX-Instanz auf VMware ESX Server installiert und konfiguriert haben, können Sie den vSphere Web Client verwenden, um die virtuelle Appliance für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

Die PCI-Passthrough-Funktion ermöglicht es einer virtuellen Gastmaschine, direkt auf physische PCI- und PCIe-Geräte zuzugreifen, die mit einem Host verbunden sind.

Voraussetzungen

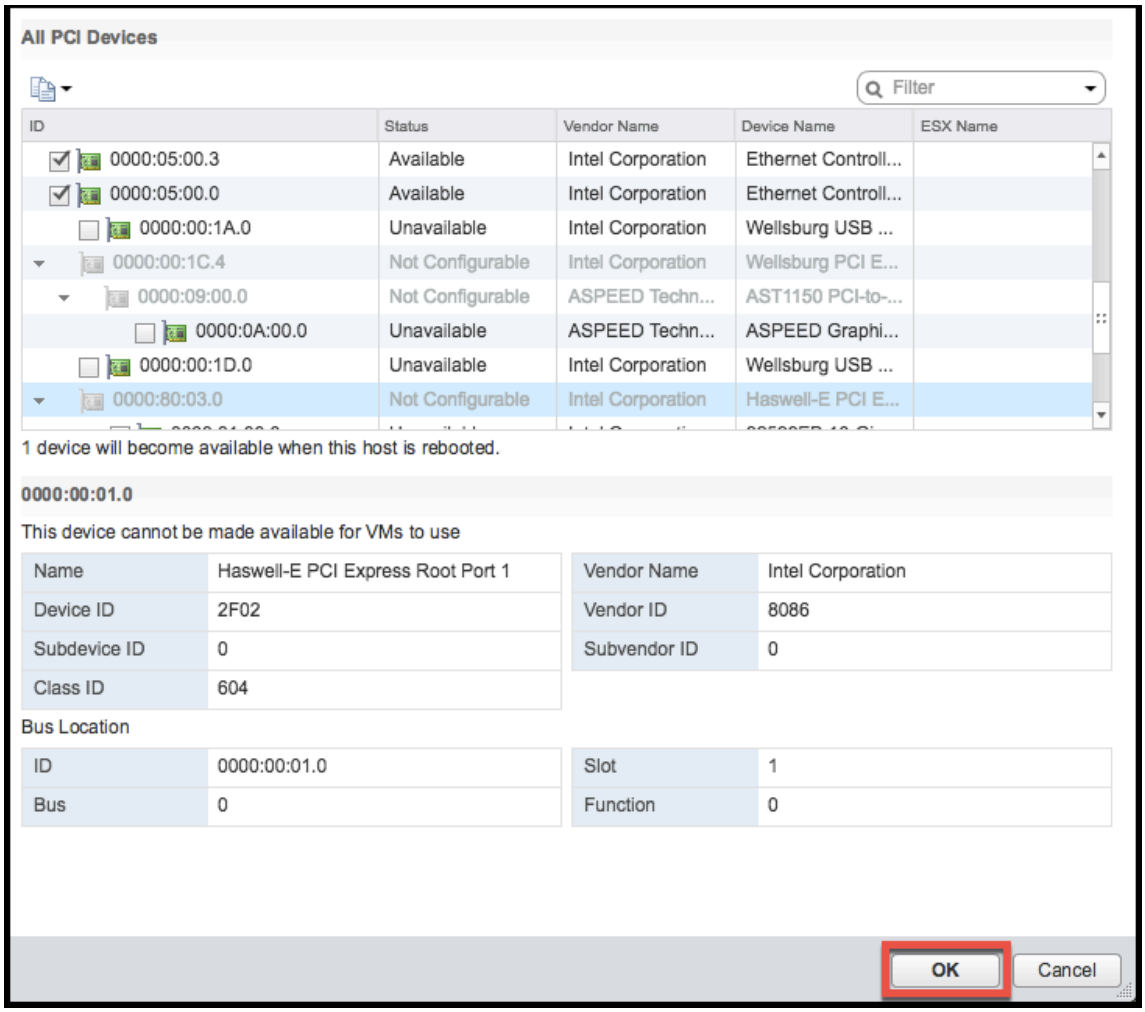
- Die Firmware-Version der Intel XL710-NIC auf dem Host ist 5.04.
- Ein PCI-Passthrough-Gerät, das mit dem Host verbunden und auf dem Host konfiguriert ist
- Unterstützte NICs:
  - Intel X710 10G-Netzwerkkarte
  - Intel XL710 40G-NIC mit zwei Anschlüssen
  - Intel XL710 40G-NIC mit einem Port

Konfigurieren von Passthrough-Geräten auf einem Host

Bevor Sie ein Passthrough-PCI-Gerät auf einer virtuellen Maschine konfigurieren, müssen Sie es auf dem Host-Computer konfigurieren. Gehen Sie folgendermaßen vor, um Passthrough-Geräte auf einem Host zu konfigurieren.

1. Wählen Sie den Host im Navigator-Bereich des vSphere Web Client aus.

2. Klicken Sie auf **Verwalten** > **Einstellungen** > **PCI-Geräte.** Alle verfügbaren Passthrough-Geräte werden angezeigt.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.
4. Das Fenster **PCI-Geräteverfügbarkeit bearbeiten** wird angezeigt.
5. Wählen Sie die Geräte aus, die für den Passthrough verwendet werden sollen, und klicken Sie auf **OK**.



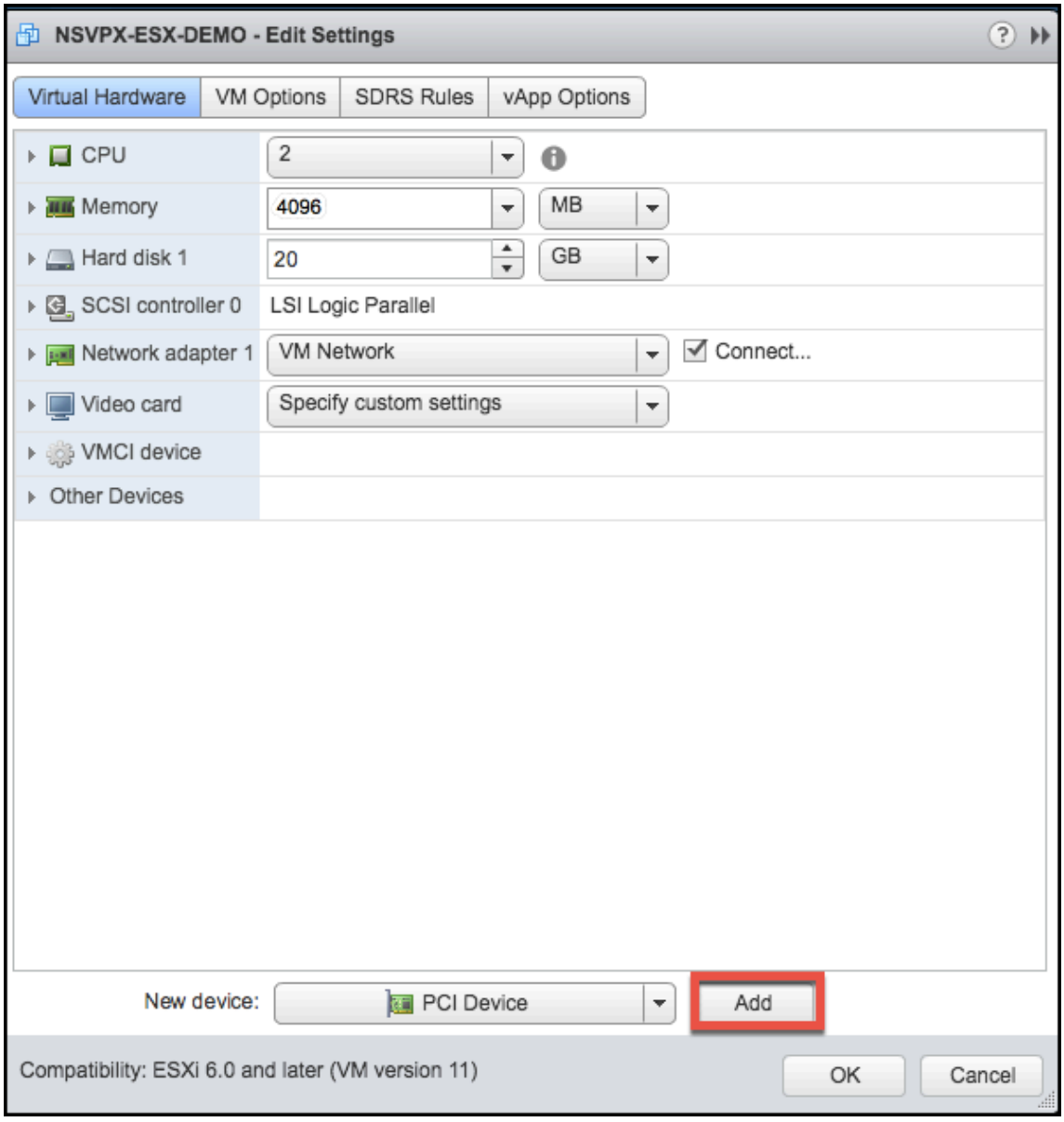
6. Starten Sie den Hostcomputer neu.

Passthrough-Geräte auf einer NetScaler VPX-Instanz konfigurieren

Gehen Sie wie folgt vor, um ein Passthrough-PCI-Gerät auf einer NetScaler VPX-Instanz zu konfigurieren.

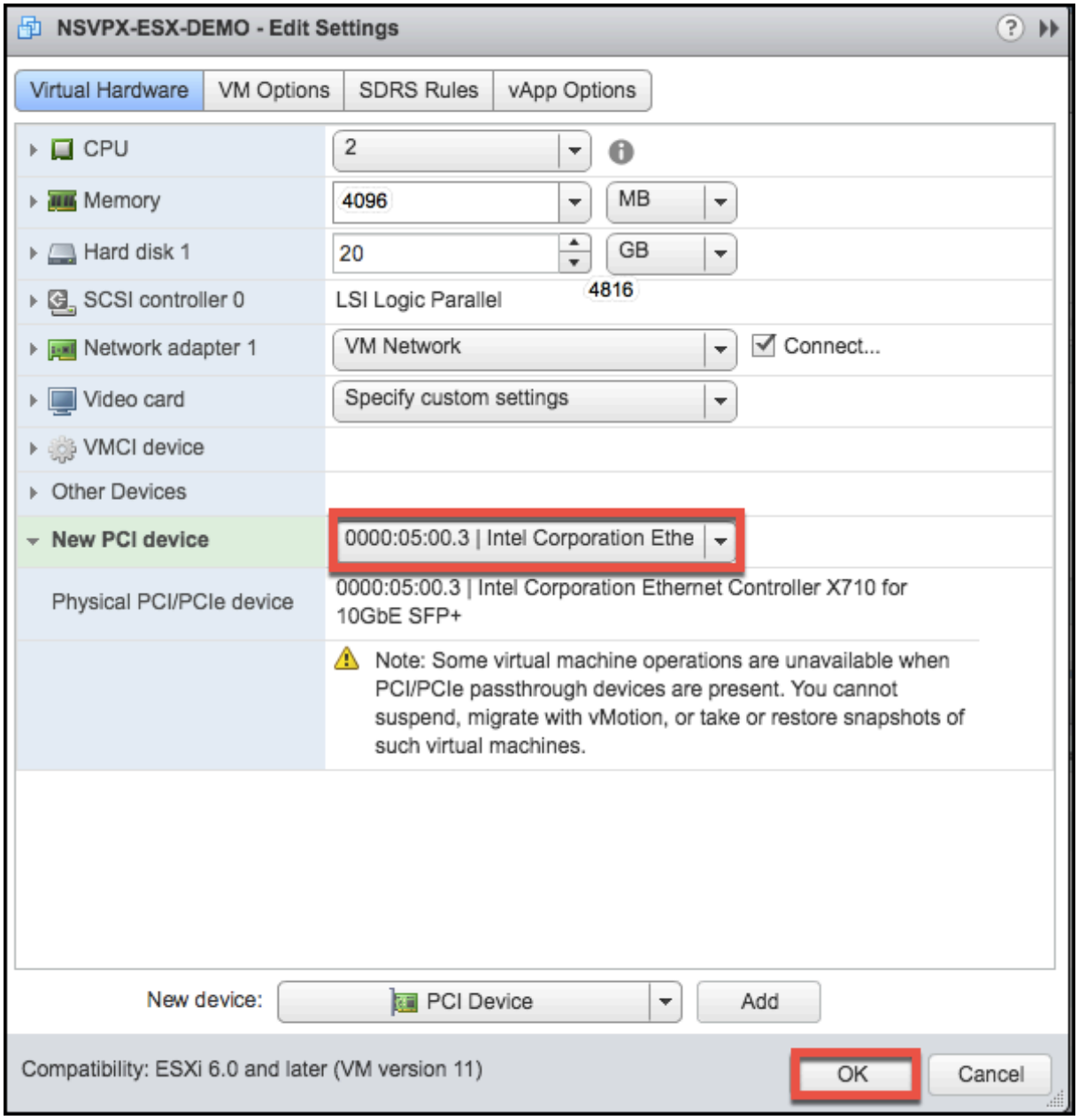
1. Schalten Sie die virtuelle Maschine aus.

2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** im Dropdownmenü **Neues Gerät** die Option **PCI-Gerät** aus, und klicken Sie auf **Hinzufügen**.



4. Erweitern Sie **Neues PCI-Gerät**, und wählen Sie das Passthrough-Gerät aus, das mit der virtuellen Maschine verbunden werden soll, aus der Dropdownliste aus, und klicken Sie auf **OK**.

> **Hinweis**
>
> VMXNET3-Netzwerkschnittstelle und PCI-Passthrough-Netzwerkschnittstelle können nicht koexistieren.



1. Schalten Sie den virtuellen Gastcomputer ein.

Sie haben die Schritte zur Konfiguration von NetScaler VPX für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen abgeschlossen.

Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance auf dem VMware ESX Hypervisor

May 11, 2023

Sie können die NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance auf dem VMware ESX-Hypervisor anwenden. Daher wird in bestimmten Fällen eine bestimmte Setup- oder VPX-Instanz in viel kürzer Zeit angezeigt.

Weitere Informationen zu Preboot-Benutzerdaten und ihrem Format finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance in der Cloud.

> **Hinweis:**
>
> Um mit Preboot-Benutzerdaten in ESX zu booten, muss die Standard-Gateway-Konfiguration in <NS-CONFIG> Abschnitt übergeben werden. Weitere Informationen zum Inhalt des <NS-CONFIG> Tags finden Sie unter [Sample-<NS-CONFIG>-section] (apply-preboot-userdata-on-esx-vpx.html #sample -<ns-config>-section).

Beispiel <NS-CONFIG> Abschnitt:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP> 10.102.38.216 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

So stellen Sie Preboot-Benutzerdaten auf dem ESX-Hypervisor bereit

Sie können Preboot-Benutzerdaten auf dem ESX Hypervisor vom Webclient oder vSphere-Client aus auf die folgenden zwei Arten bereitstellen:

- CD/DVD-ISO verwenden
- OVF-Eigenschaft verwenden

Benutzerdaten mit CD/DVD-ISO bereitstellen

Sie können den VMware vSphere-Client verwenden, um Benutzerdaten mithilfe des CD/DVD-Laufwerks als ISO-Image in die VM einzufügen.

Gehen Sie wie folgt vor, um Benutzerdaten mithilfe der CD/DVD-ISO bereitzustellen:

1. Erstellen Sie eine Datei mit einem Dateinamen `userdata`, die den Inhalt der Preboot-Benutzerdaten enthält. Weitere Informationen zum Inhalt des <NS-CONFIG>-Tags finden Sie im Beispielabschnitt <NS-CONFIG>.

   > Hinweis: Der Dateiname muss ausschließlich als `userdata` verwendet werden.

2. Speichern Sie die `userdata`-Datei in einem Ordner und erstellen Sie mithilfe des Ordners ein ISO-Image.

   Sie können ein ISO-Image mit einer `userdata`-Datei mit den folgenden zwei Methoden erstellen:

   - Verwenden eines beliebigen Imageverarbeitungstools wie PowerISO.
   - Befehl `mkisofs` unter Linux verwenden.

   Die folgende Beispielkonfiguration zeigt, wie ein ISO-Image über den Befehl `mkisofs` in Linux generiert wird.

```
root@ubuntu:~/sai/14jul2021# ls -l total 4
drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
root@ubuntu:~/sai/14jul2021#
root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
-rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso
    ./esx_preboot_userdata
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
root@ubuntu:~/sai/14jul2021# ls -lh
total 356K
drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata
-rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.iso

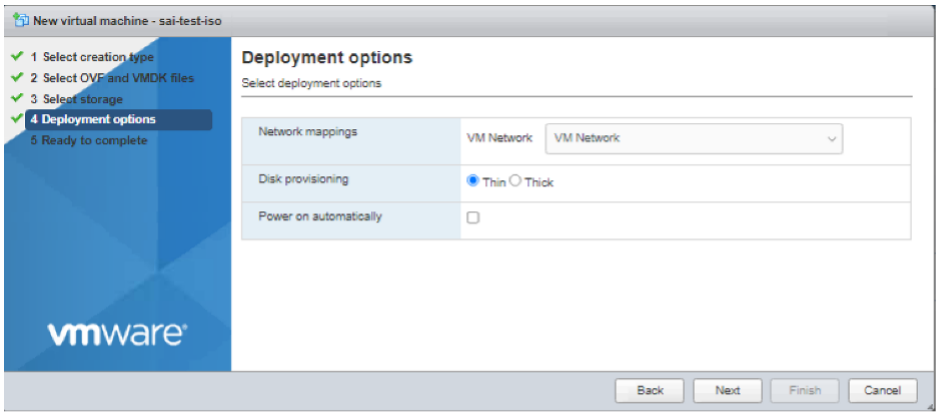
root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata
root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
    preboot_userdata_155_193
```



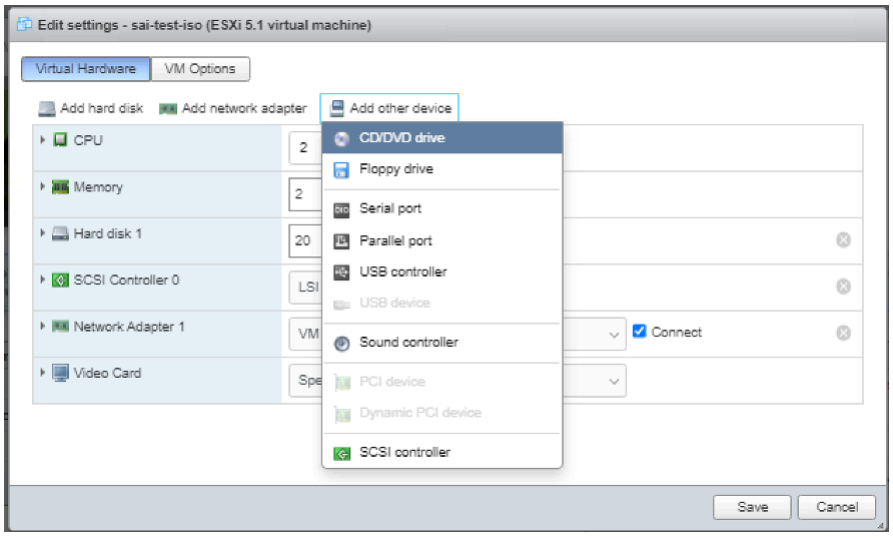
```
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)

<!--NeedCopy-->
```

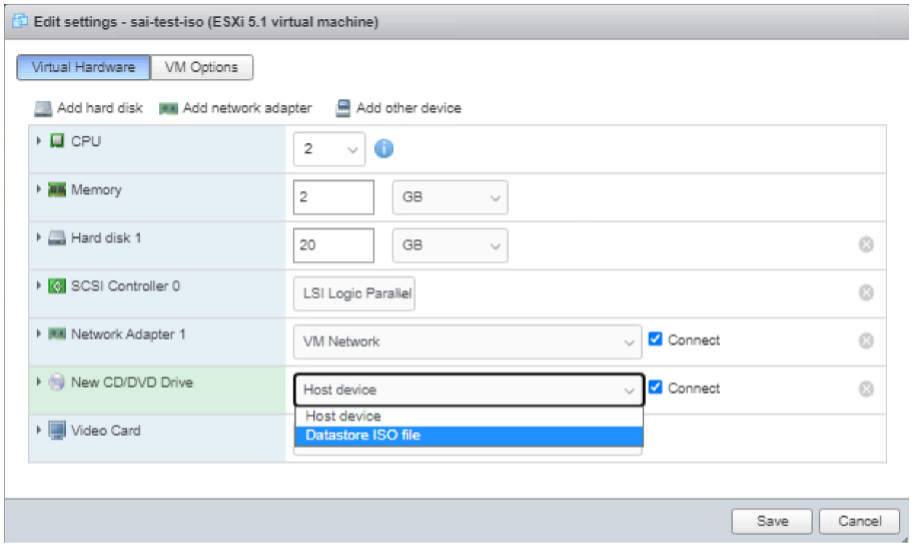
3. Stellen Sie die NetScaler VPX-Instanz über den Standardbereitstellungsprozess zum Erstellen der VM bereit. Schalten Sie die VM jedoch nicht automatisch ein.



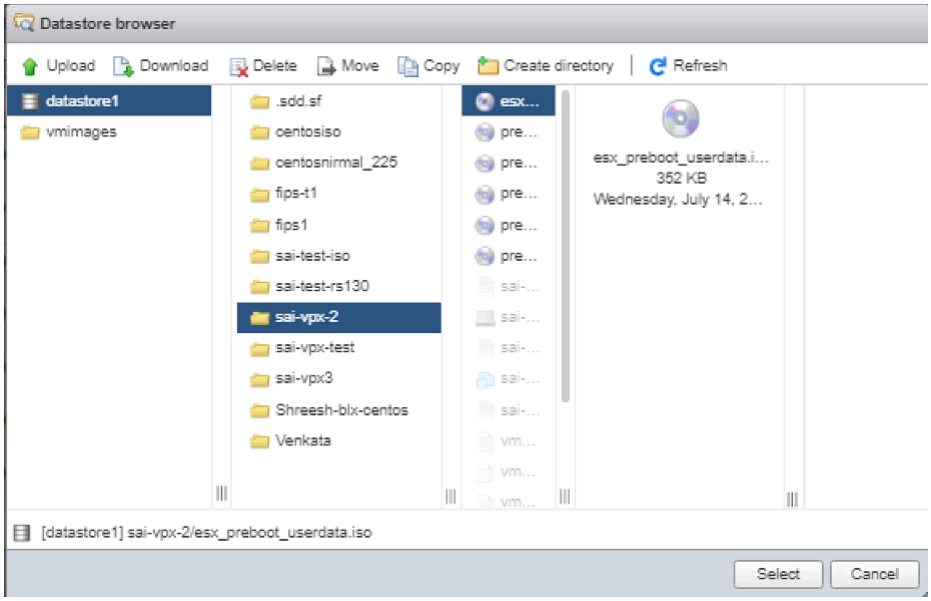
4. Nachdem die VM erfolgreich erstellt wurde, hängen Sie die ISO-Datei als CD/DVD-Laufwerk an die VM an.



5. Navigieren Sie zu **Neues CD/DVD-Laufwerk** und wählen Sie **Datenspeicher-ISO-Datei** aus dem Dropdown-Menü.



6. Wählen Sie im vSphere Client einen Datenspeicher aus.



7. Schalten Sie die VM ein.

Stellen Sie Benutzerdaten mithilfe der OVF-Eigenschaft vom ESX-Webclient bereit

Befolgen Sie diese Schritte, um Benutzerdaten mithilfe der OVF-Eigenschaft bereitzustellen.

1. Erstellen Sie eine Datei mit Benutzerdateninhalten.


```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

2. Codieren Sie den Inhalt der Benutzerdaten mit der Base64-Codierung. Sie können die Base64-Kodierung mit den folgenden zwei Methoden durchführen:

   - Verwenden Sie unter Linux den folgenden Befehl:

     ```
     base64 <userdata-filename>  >   <outuput-file>
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     base64 esx_userdata.xml  > esx_userdata_b64
     <!--NeedCopy-->
     ```

     ```
     root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
     root@ubuntu:~/sai/14jul2021#
     root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
     PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQPgog
     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
     U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
     RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
     ```

   - Verwenden Sie Online-Tools, um Inhalte von Benutzerdaten zu codieren, z. B. Base64 Encode and Decode.

3. Nehmen Sie einen **Produktabschnitt** in die OVF-Vorlage einer NetScaler VPX-Instanz auf dem ESX-Hypervisor auf.

   Beispiel Produkt Abschnitt:

   ```
   <ProductSection>

   ```



```
3    <Info>Information about the installed software</Info>
4    <Product>NSVPX-VSK Template</Product>
5    <Vendor>Citrix</Vendor>
6    <VendorUrl>www.citrix.com</VendorUrl>
7    <Category> Preboot Userdata </Category>
8
9    <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
        userConfigurable="true" ovf:value="">
10
11     <Label>Userdata</Label>
12     <Description> Userdata for ESX VPX </Description>
13   </Property>
14
15 </ProductSection>
16 <!--NeedCopy-->
```

4. Geben Sie die base64-codierten Benutzerdaten als die `ovf:value` for `guestinfo.userdata` -Eigenschaft im Abschnitt Produkt an.

```
1  <ProductSection>
2
3    <Info>Information about the installed software</Info>
4    <Product>NSVPX-VSK Template</Product>
5    <Vendor>Citrix</Vendor>
6    <VendorUrl>www.citrix.com</VendorUrl>
7    <Category> Preboot Userdata </Category>
8    <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
        userConfigurable="true"
9      ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
          CglhZGQgcm91dGUgMC4wLjAuMCAw
10     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQ

11     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1C

12     U1RSQVA+
          CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT

13     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAg

14     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAg

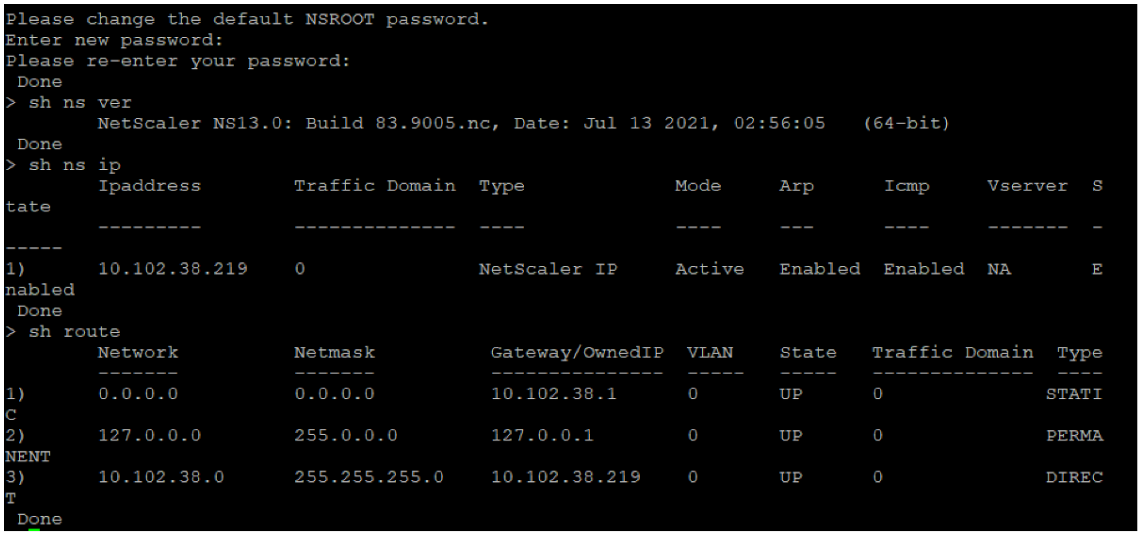
15     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5F

16     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
          CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
```



```
17      RS1DT05GSUc+
            CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg
            ==">
18
19      <Label>Userdata</Label>
20      <Description> Userdata for ESX VPX </Description>
21    </Property>
22
23  </ProductSection>
24  <!--NeedCopy-->
```

5. Verwenden Sie die geänderte OVF-Vorlage mit dem Abschnitt Produkt für die VM-Bereitstellung.



Stellen Sie Benutzerdaten mithilfe der OVF-Eigenschaft vom ESX vSphere-Client bereit

Gehen Sie wie folgt vor, um Benutzerdaten mithilfe der OVF-Eigenschaft vom ESX vSphere Client bereitzustellen.

1. Erstellen Sie eine Datei mit Benutzerdateninhalten.


```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

2. Codieren Sie den Inhalt der Benutzerdaten mit der Base64-Codierung. Sie können die Base64-Kodierung mit den folgenden zwei Methoden durchführen:

   - Verwenden Sie unter Linux den folgenden Befehl:

     ```
     base64 <userdata-filename>  >   <outuput-file>
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     base64 esx_userdata.xml  > esx_userdata_b64
     <!--NeedCopy-->
     ```

     ```
     root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
     root@ubuntu:~/sai/14jul2021#
     root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
     PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
     LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQPgog
     ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
     U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
     VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
     ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
     ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
     QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
     RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
     ```

   - Verwenden Sie Online-Tools, um Inhalte von Benutzerdaten zu codieren, z. B. Base64 Encode and Decode.

3. Nehmen Sie einen **Produktabschnitt** in die OVF-Vorlage einer NetScaler VPX-Instanz auf dem ESX-Hypervisor auf.

   Beispiel Produkt Abschnitt:

   ```
   <ProductSection>

   ```



```
  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>

  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true" ovf:value="">

    <Label>Userdata</Label>
    <Description> Userdata for ESX VPX </Description>
  </Property>

</ProductSection>
<!--NeedCopy-->
```

4. Geben Sie die base64-codierten Benutzerdaten als die `ovf:value` for `guestinfo.userdata` -Eigenschaft im Abschnitt Produkt an.

```
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.Citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>
  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true"
    ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
       CglhZGQgcm91dGUgMC4wLjAuMCAw
    LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQ

    ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1C

    U1RSQVA+
       CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT

    VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAg

    ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg

    ICAgICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgICAgICAgPFNVQk5F

    QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
       CiAgICAgICAgICAgPC9NR01ULUlOVEVSRkFD
```



```
      RS1DT05GSUc+
          CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg
          ==">

      <Label>Userdata</Label>
      <Description> Userdata for ESX VPX </Description>
    </Property>

</ProductSection>
<!--NeedCopy-->
```

5. Fügen Sie die Eigenschaft wie folgt `ovf:transport="com.vmware.guestInfo"` zu Virtual-HardwareSection hinzu:

```
<VirtualHardwareSection  ovf:transport="com.vmware.guestInfo">
<!--NeedCopy-->
```

6. Verwenden Sie die geänderte OVF-Vorlage mit dem Abschnitt Produkt für die VM-Bereitstellung.

```
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
 Done
> sh ns ver
        NetScaler NS13.0: Build 83.9005.nc, Date: Jul 13 2021, 02:56:05   (64-bit)
 Done
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  S
tate
        ---------        --------------  ----             ----     ---      ----     -------  -
-----
1)      10.102.38.219    0               NetScaler IP     Active   Enabled  Enabled  NA       E
nabled
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.102.38.1      0       UP      0               STATI
C
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMA
NENT
3)      10.102.38.0      255.255.255.0    10.102.38.219    0       UP      0               DIREC
T
 Done
```

Installieren einer NetScaler VPX-Instanz in der VMware Cloud auf AWS

May 11, 2023

Mit der VMware Cloud (VMC) auf AWS können Sie softwaredefinierte Cloud-Rechenzentren (SDDC) auf AWS mit der gewünschten Anzahl von ESX-Hosts erstellen. Das VMC auf AWS unterstützt NetScaler VPX-Bereitstellungen. VMC stellt eine Benutzeroberfläche bereit, die gleiche wie bei vCenter vor Ort ist. Es funktioniert identisch mit den ESX-basierten NetScaler VPX-Bereitstellungen.

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Ein VMware SDDC muss mit mindestens einem Host vorhanden sein.
- Laden Sie die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie geeignete Netzwerksegmente auf VMware SDDC, mit denen die virtuellen Maschinen eine Verbindung herstellen.
- VPX-Lizenzdateien abrufen. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie im *NetScaler VPX Licensing Guide* unter http://support.citrix.com/article/ctx131110.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX nCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> Hinweis
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 2. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
Netzwerkkarte	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-<Releasenummer>-<Buildnummer>-disk1.vmdk (z. B. NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-<Releasenummer>-<Buildnummer>.ovf (z. B. NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<Releasenummer>-<Buildnummer>.mf (z. B. NSVPX-ESX-13.0-79.64.mf)

Installieren einer NetScaler VPX Instanz in VMware Cloud

Nachdem Sie VMware SDDC installiert und konfiguriert haben, können Sie das SDDC verwenden, um virtuelle Appliances in der VMware-Cloud zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des auf dem SDDC verfügbaren Speichers ab.

Gehen Sie folgendermaßen vor, um NetScaler VPX-Instanzen in der VMware-Cloud zu installieren:

1. Öffnen Sie VMware SDDC auf Ihrer Workstation.

2. Geben Sie in den Textfeldern **User Name** und **Password** die Administratoranmeldeinformationen ein, und klicken Sie dann auf Anmelden.
3. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
4. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Deploy from file** zu dem Speicherort, an dem Sie die NetScaler VPX-Instanz-Setupdateien gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf **Weiter**.

   > **Hinweis:** Standardmäßig verwendet die NetScaler VPX Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird.

5. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem VMware SDDC konfiguriert haben. Klicken Sie auf **Weiter**, um mit der Installation einer virtuellen Appliance auf VMware SDDC zu beginnen.
6. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.
7. Wenn Sie eine weitere virtuelle Appliance installieren möchten, wiederholen Sie Schritt 6.
8. Geben Sie die Verwaltungs-IP-Adresse aus demselben Segment an, das als Verwaltungsnetzwerk ausgewählt wurde. Das gleiche Subnetz wird für das Gateway verwendet.
9. VMware SDDC erfordert, dass NAT- und Firewall-Regeln explizit für alle privaten IP-Adressen erstellt werden, die zu Netzwerksegmenten gehören.

Installieren Sie eine NetScaler VPX-Instanz auf einem Microsoft Hyper-V-Server

May 11, 2023

Um NetScaler VPX-Instanzen auf Microsoft Windows Server zu installieren, müssen Sie zuerst Windows Server mit aktivierter Hyper-V-Rolle auf einem Computer mit ausreichenden Systemressourcen installieren. Beim Installieren der Hyper-V-Rolle müssen Sie die Netzwerkkarten auf dem Server angeben, den Hyper-V zum Erstellen von virtuellen Netzwerken verwenden soll. Sie können einige NICs für den Host reservieren. Verwenden Sie Hyper-V Manager, um die Installation der NetScaler VPX-Instanz durchzuführen.

Die NetScaler VPX-Instanz für Hyper-V wird im Format der virtuellen Festplatte (VHD) bereitgestellt. Es enthält die Standardkonfiguration für Elemente wie CPU, Netzwerkschnittstellen sowie Festplattengröße und -format. Nach der Installation der NetScaler VPX-Instanz können Sie die Netzwerkadapter

auf einer virtuellen Appliance konfigurieren, virtuelle Netzwerkkarten hinzufügen und dann die NetScaler IP-Adresse, Subnetzmaske und Gateway zuweisen und die Grundkonfiguration der virtuellen Appliance abschließen.

Wenn Sie nach der Erstkonfiguration der VPX-Instanz die Appliance auf die neueste Softwareversion aktualisieren möchten, finden Sie weitere Informationen unter Aufrüsten einer eigenständigen NetScalerVPX-Appliance

> **Hinweis**
>
> Das ISIS-Protokoll (Intermediate System-to-Intermediate System) wird auf der virtuellen NetScaler VPX-Appliance, die auf der HyperV-2012-Plattform gehostet wird, nicht unterstützt.

Voraussetzungen für die Installation der NetScaler VPX-Instanz auf Microsoft-Servern

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Aktivieren Sie die Hyper-V-Rolle auf Windows-Servern. Weitere Informationen finden Sie unter http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Laden Sie die Setupdateien der virtuellen Appliance
- Holen Sie sich NetScaler VPX-Instanzlizenzdateien. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie im *NetScaler VPX Licensing Guide* unter http://support.citrix.com/article/ctx131110.

Hardwareanforderungen für Microsoft-Server

In der folgenden Tabelle werden die Mindestsystemanforderungen für Microsoft-Server beschrieben.

Tabelle 1. Mindestsystemanforderungen für Microsoft-Server

Komponente	Voraussetzung
CPU	1,4 GHz 64-Bit-Prozessor
RAM	8 GB
Speicherplatz	32 GB oder mehr

In der folgenden Tabelle sind die virtuellen Computerressourcen für jede NetScaler VPX-Instanz aufgeführt.

Tabelle 2. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
RAM	4 GB
Virtuelle CPU	2
Speicherplatz	20 GB
Virtuelle Netzwerkschnittstellen	1

Laden Sie die NetScaler VPX-Setup-Dateien herunter

Die NetScaler VPX-Instanz für Hyper-V wird im Format der virtuellen Festplatte (VHD) bereitgestellt. Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf, klicken Sie auf **Anmelden > Mein Konto > Citrix Account erstellen** und folgen Sie den Anweisungen zum Erstellen eines Citrix-Kontos.

Gehen Sie folgendermaßen vor, um die Setup-Dateien der NetScaler VPX Instanz herunterzuladen:

1. Navigieren Sie in einem Webbrowser zu http://www.citrix.com/.
2. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
3. Klicken Sie auf **Downloads**.
4. Wählen Sie im Dropdownmenü **Produkt auswählen** die Option **NetScaler (NetScaler ADC)** aus.
5. Klicken Sie unter **NetScaler Release X.X > Virtual Appliances**auf **NetScaler**VPX Release X.X.
6. Laden Sie die komprimierte Datei auf Ihren Server herunter.

Installieren Sie die NetScaler VPX-Instanz auf Microsoft-Servern

Nachdem Sie die Hyper-V-Rolle auf Microsoft Server aktiviert und die Dateien der virtuellen Appliance extrahiert haben, können Sie Hyper-V Manager verwenden, um die NetScaler VPX-Instanz zu installieren. Nachdem Sie die virtuelle Maschine importiert haben, müssen Sie die virtuellen Netzwerkkarten konfigurieren, indem Sie sie den von Hyper-V erstellten virtuellen Netzwerken zuordnen.

Sie können maximal acht virtuelle Netzwerkkarten konfigurieren. Selbst wenn die physische Netzwerkkarte DOWN ist, geht die virtuelle Appliance davon aus, dass die virtuelle Netzwerkkarte AKTIV ist, da sie weiterhin mit den anderen virtuellen Appliances auf demselben Host (Server) kommunizieren kann.

> **Hinweis**
>
> Sie können keine Einstellungen ändern, während die virtuelle Appliance ausgeführt wird. Fahren Sie die virtuelle Appliance herunter und nehmen Sie dann Änderungen vor.

So installieren Sie die NetScaler VPX-Instanz mit Hyper-V Manager auf Microsoft Server:

1. Klicken Sie zum Starten von Hyper-V Manager auf **Start**, zeigen Sie auf **Verwaltung**, und klicken Sie dann auf **Hyper-V-Manager**.
2. Wählen Sie im Navigationsbereich unter **Hyper-V Manage**r den Server aus, auf dem Sie die NetScaler VPX-Instanz installieren möchten.
3. Klicken Sie im Menü **Aktion** auf **Virtuelle Maschine importieren**e.
4. Geben Sie im Dialogfeld **Virtuelle Maschine importieren** unter **Speicherort**den Pfad des Ordners an, der die NetScaler VPX-Instanzsoftwaredateien enthält, und wählen Sie dann **Die virtuelle Maschine kopieren (neue eindeutige ID erstellen)**aus. Dieser Ordner ist der übergeordnete Ordner, der die Ordner Snapshots, Virtuelle Festplatten und Virtuelle Maschinen enthält.
5. Hinweis: Wenn Sie eine komprimierte Datei erhalten haben, stellen Sie sicher, dass Sie die Dateien in einen Ordner extrahieren, bevor Sie den Pfad zum Ordner angeben.
6. Klicken Sie auf **Importieren**.
7. Stellen Sie sicher, dass die von Ihnen importierte virtuelle Appliance unter **Virtuelle Maschinen**aufgeführt ist.
8. Um eine weitere virtuelle Appliance zu installieren, wiederholen Sie die Schritte **2** bis **6.**

> **Wichtig**
>
> Stellen Sie sicher, dass Sie die Dateien in Schritt **4**in einen anderen Ordner extrahieren.

Automatische Bereitstellung einer NetScaler VPX-Instanz auf Hyper-V

Die automatische Bereitstellung der NetScaler VPX-Instanz ist optional. Wenn die automatische Bereitstellung nicht erfolgt, bietet die virtuelle Appliance eine Option zum Konfigurieren der IP-Adresse usw.

Führen Sie die folgenden Schritte aus, um die NetScaler VPX-Instanz auf Hyper-V automatisch bereitzustellen.

1. Erstellen Sie ein ISO9660-konformes ISO-Image mit der xml-Datei, wie im Beispiel dargestellt. Stellen Sie sicher, dass der Name der xml-Datei **userdata**lautet.

   Sie können eine ISO-Datei aus einer XML-Datei erstellen, indem Sie Folgendes verwenden:

   • Jedes Imageverarbeitungstool wie PowerISO.

   • `mkisofs` Befehl unter Linux.


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment/1`
    "

xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"

oe:id=""

xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">

<PlatformSection>

<Kind>HYPER-V</Kind>

<Version>2013.1</Version>

<Vendor>CITRIX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
    />

<Property oe:key="com.citrix.netscaler.platform" oe:value="NS1000V
    "/>

<Property oe:key="com.citrix.netscaler.orch_env" oe:value="cisco-
    orch-env"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="
    10.102.100.122"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
    255.255.255.128"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="
    10.102.100.67"/></PropertySection>

</Environment>
```



```
38 <!--NeedCopy-->
```

2. Kopieren Sie das ISO-Image auf den Hyper-V-Server.
3. Wählen Sie die virtuelle Appliance aus, die Sie importiert haben, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen**aus. Sie können auch die virtuelle Appliance auswählen und dann mit der rechten Maustaste klicken und **Einstellungen**auswählen. Das Fenster **Einstellungen** für die ausgewählte virtuelle Appliance wird angezeigt.
4. Klicken **Sie im Fenster Einstellungen** unter dem Abschnitt Hardware auf **IDE Controller**.
5. Wählen Sie im rechten Fensterbereich **DVD-Laufwerk** und klicken Sie auf **Hinzufügen**. Das DVD-Laufwerk wird im Abschnitt **IDE Controller** im linken Fensterbereich hinzugefügt.
6. Wählen Sie das in Schritt 5 hinzugefügte **DVD-Laufwerk** aus. Aktivieren Sie im rechten Fensterbereich das **Optionsfeld Image-Datei**, klicken Sie auf **Durchsuchen** und wählen Sie das ISO-Image aus, das Sie in Schritt 2 auf den Hyper-V-Server kopiert haben.
7. Klicken Sie auf **Anwenden**.

> **Hinweis**
>
> Die Instanz der virtuellen Appliance wird in folgenden Fällen mit der Standard-IP-Adresse angezeigt:
>
> - Das DVD-Laufwerk ist angeschlossen und die ISO-Datei wird nicht bereitgestellt.
> - Die ISO-Datei enthält nicht die Benutzerdatendatei.
> - Der Name oder das Format der Benutzerdatendatei ist nicht korrekt.

Gehen Sie folgendermaßen vor, um virtuelle Netzwerkkarten auf der NetScaler VPX-Instanz zu konfigurieren:

1. Wählen Sie die virtuelle Appliance aus, die Sie importiert haben, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen**aus.
2. <virtual appliance name>Klicken **Sie im Dialogfeld Einstellungen für** im linken Bereich auf **Hardware hinzufügen** .
3. Wählen Sie im rechten Bereich aus der Geräteliste die Option **Netzwerkadapter**aus.
4. Klicken Sie auf **Hinzufügen**.
5. Stellen Sie sicher, dass **Netzwerkadapter (nicht verbunden)** im linken Bereich angezeigt wird.
6. Wählen Sie im linken Bereich den Netzwerkadapter aus.
7. Wählen Sie im rechten Bereich im Menü **Netzwerk** das virtuelle Netzwerk aus, mit dem der Adapter verbunden werden soll.
8. Wiederholen Sie die Schritte **6** und **7**, um das virtuelle Netzwerk für andere Netzwerkadapter auszuwählen, die Sie verwenden möchten.
9. Klicken Sie auf **Übernehmen** und dann auf **OK**.

So konfigurieren Sie die NetScaler VPX-Instanz:

1. Klicken Sie mit der rechten Maustaste auf die zuvor installierte virtuelle Appliance, und wählen Sie dann **Starten**.
2. Rufen Sie die Konsole auf, indem Sie auf die virtuelle Appliance doppelklicken.
3. Geben Sie die NetScaler-IP-Adresse, die Subnetzmaske und das Gateway für Ihre virtuelle Appliance ein.

Sie haben die Grundkonfiguration Ihrer virtuellen Appliance abgeschlossen. Geben Sie die IP-Adresse in einen Webbrowser ein, um auf die virtuelle Appliance zuzugreifen.

> **Hinweis**
>
> Sie können auch die Vorlage für virtuelle Maschinen (VM) verwenden, um die NetScaler VPX-Instanz mithilfe von SCVMM bereitzustellen.
>
> Wenn Sie die Microsoft Hyper-V NIC-Teaming-Lösung mit NetScaler VPX-Instanzen verwenden, finden Sie im Artikel CTX224494 weitere Informationen.

Installieren einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform

May 11, 2023

Um einen NetScaler VPX für die Linux-KVM-Plattform einzurichten, können Sie die grafische Virtual Machine Manager (Virtual Manager) -Anwendung verwenden. Wenn Sie die Linux-KVM-Befehlszeile bevorzugen, können Sie das `virsh` Programm verwenden.

Das Host-Linux-Betriebssystem muss mit Virtualisierungstools wie KVM Module und QEMU auf geeigneter Hardware installiert werden. Die Anzahl der virtuellen Maschinen (VMs), die auf dem Hypervisor bereitgestellt werden können, hängt von der Anwendungsanforderung und der ausgewählten Hardware ab.

Nachdem Sie eine NetScaler VPX-Instanz bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

Einschränkungen und Nutzungsrichtlinien

Allgemeine Empfehlungen

Um unvorhersehbares Verhalten zu vermeiden, wenden Sie die folgenden Empfehlungen an:

- Ändern Sie nicht die MTU der VNet-Schnittstelle, die mit der VPX-VM verknüpft ist. Fahren Sie die VPX-VM herunter, bevor Sie Konfigurationsparameter wie Schnittstellenmodi oder CPU ändern.
- Erzwingen Sie kein Herunterfahren der VPX-VM. Verwenden Sie also nicht den Befehl **Force off** .

- Alle Konfigurationen, die auf dem Host-Linux vorgenommen werden, sind je nach den Einstellungen Ihrer Linux-Distribution möglicherweise persistent oder auch nicht. Sie können sich dafür entscheiden, diese Konfigurationen persistent zu machen, um ein konsistentes Verhalten bei Neustarts des Linux-Host-Betriebssystems zu gewährleisten.
- Das NetScaler-Paket muss für jede bereitgestellte NetScaler VPX-Instanz einzigartig sein.

Einschränkungen

- Die Live-Migration einer VPX-Instanz, die auf KVM ausgeführt wird, wird nicht unterstützt.

Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform

May 11, 2023

Überprüfen Sie die Mindestsystemanforderungen für einen Linux-KVM-Server, der auf einer NetScaler VPX-Instanz ausgeführt wird.

CPU-Anforderung:

- 64-Bit-x86-Prozessoren mit der Hardwarevirtualisierungsfunktion, die in Intel VT-X-Prozessoren enthalten ist.

Um zu testen, ob Ihre CPU den Linux-Host unterstützt, geben Sie den folgenden Befehl an der Linux-Shell-Eingabeaufforderung

```
1 \*.egrep '^flags.\*(vmx|svm)' /proc/cpuinfo*
2 <!--NeedCopy-->
```

Wenn die **BIOS-Einstellungen** für die vorhergehende Erweiterung deaktiviert sind, müssen Sie sie im BIOS aktivieren.

- Stellen Sie mindestens 2 CPU-Kerne für Host Linux bereit.
- Es gibt keine spezifische Empfehlung für die Prozessorgeschwindigkeit, aber je höher die Geschwindigkeit, desto besser ist die Leistung der VM-Anwendung.

Speicherbedarf (RAM):

Mindestens 4 GB für den Host-Linux-Kernel. Fügen Sie mehr Arbeitsspeicher hinzu, wie es von den VMs benötigt wird.

Festplattenanforderung:

Berechnen Sie den Speicherplatz für den Host-Linux-Kernel und die VM-Anforderungen. Eine einzelne NetScaler VPX-VM benötigt 20 GB Festplattenspeicher.

Softwareanforderungen

Der verwendete Host-Kernel muss ein 64-Bit-Linux-Kernel, Version 2.6.20 oder höher, mit allen Virtualisierungstools sein. Citrix empfiehlt neuere Kernel wie 3.6.11-4 und höher.

Viele Linux-Distributionen wie Red Hat, CentOS und Fedora haben Kernelversionen und zugehörige Virtualisierungstools getestet.

Hardwareanforderungen für Gast-VM

NetScaler VPX unterstützt IDE- und VirtIO-Festplattentypen. Der Festplattentyp wurde in der XML-Datei konfiguriert, die Teil des NetScaler-Pakets ist.

Netzwerkanforderungen

NetScaler VPX unterstützt paravirtualisierte VirtIO-, SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen.

Weitere Informationen zu den unterstützten Netzwerkschnittstellen finden Sie unter:

- Stellen Sie die NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereit
- Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen
- Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen

Quellschnittstelle und Modi

Der Quellgerätetyp kann entweder Bridge oder MacVTap sein. In MacVTap sind vier Modi möglich - VEPA, Bridge, Private und Pass-Through. Überprüfen Sie die Arten von Schnittstellen, die Sie verwenden können, und die unterstützten Datenverkehrstypen wie folgt:

Brücke:

- Linux-Brücke.
- `Ebtables` und `iptables` Einstellungen auf Host Linux filtern möglicherweise den Datenverkehr auf der Bridge, wenn Sie nicht die richtige Einstellung auswählen oder `IPtable` Dienste deaktivieren.

MacVTap (VEPA-Modus):

- Bessere Leistung als eine Brücke.
- Schnittstellen desselben niedrigeren Geräts können von allen VMs gemeinsam genutzt werden.
- Inter-VM-Kommunikation mit derselben
- niedrigeres Gerät ist nur möglich, wenn der Upstream- oder Downstream-Switch den VEPA-Modus unterstützt.

MacVTap (privater Modus):

- Bessere Leistung als eine Brücke.
- Schnittstellen desselben niedrigeren Geräts können von allen VMs gemeinsam genutzt werden.
- Eine VM-Kommunikation mit demselben niedrigeren Gerät ist nicht möglich.

MacVTAP (Bridge-Modus):

- Besser im Vergleich zu Bridge.
- Schnittstellen von demselben niedrigeren Gerät können für die VMs gemeinsam genutzt werden.
- Die Kommunikation zwischen VM mit demselben niedrigeren Gerät ist möglich, wenn die untere Geräteverbindung UP ist.

MacVTap (Pass-Through-Modus):

- Besser im Vergleich zu Bridge.
- Schnittstellen von demselben niedrigeren Gerät können nicht für die VMs freigegeben werden.
- Nur eine VM kann das untere Gerät verwenden.

> Hinweis: Um die beste Leistung durch die VPX-Instanz zu erzielen, stellen Sie sicher, dass die `lro` Funktionen `gro` und auf den Quellschnittstellen ausgeschaltet sind.

Eigenschaften von Quellschnittstellen

Stellen Sie sicher, dass Sie die Funktionen generic-Receive-offload (`gro`) und Large-Receive-Offload (`lro`) der Quellschnittstellen ausschalten. Um die `lro` Funktionen `gro` und auszuschalten, führen Sie die folgenden Befehle an der Linux-Shell des Hosts aus.

```
ethtool -K eth6 gro off
ethool -K eth6 lro off
```

Beispiel:

```
[root@localhost ~]# ethtool -K eth6

                    Offload parameters for eth6:

                                        rx-checksumming: on

                                        tx-checksumming: on

                    scatter-gather: on

                    tcp-segmentation-offload: on

                    udp-fragmentation-offload: off

```



```
                    generic-segmentation-offload: on

                    generic-receive-offload: off

                    large-receive-offload: off

                    rx-vlan-offload: on

                    tx-vlan-offload: on

                    ntuple-filters: off

                    receive-hashing: on

    [root@localhost ~]#
<!--NeedCopy-->
```

Beispiel:

Wenn die Linux-Brücke des Hosts wie im folgenden Beispiel als Quellgerät verwendet wird, müssen die `lro` Funktionen an den VNet-Schnittstellen ausgeschaltet werden, bei denen es sich um die virtuellen Schnittstellen handelt, die den Host mit den Gast-VMs verbinden.

```
    [root@localhost ~]# brctl show eth6_br

    bridge name     bridge  id               STP enabled interfaces

    eth6_br         8000.00e0ed1861ae          no         eth6

                                                          vnet0

                                                          vnet2

    [root@localhost ~]#
<!--NeedCopy-->
```

Im vorhergehenden Beispiel werden die beiden virtuellen Schnittstellen von eth6_br abgeleitet und werden als vnet0 und vnet2 dargestellt. Führen Sie die folgenden Befehle aus, um auszuschalten `gro` und `lro` Funktionen für diese Schnittstellen.

```
    ethtool -K vnet0 gro off
            ethtool -K vnet2 gro off
            ethtool -K vnet0 lro off
                    ethtool -K vnet2 lro off
<!--NeedCopy-->
```


Promiscuous-Modus

Der Promiscuous-Modus muss aktiviert sein, damit die folgenden Funktionen funktionieren:

- L2-Modus
- Verarbeitung des Multicast-Datenverkehrs
- Übertragung
- IPv6-Verkehr
- virtueller MAC
- Dynamisches Routing

Verwenden Sie den folgenden Befehl, um den Promiscuous-Modus zu aktivieren.

```
[root@localhost ~]# ifconfig eth6 promisc
[root@localhost ~]# ifconfig eth6
eth6       Link encap:Ethernet  HWaddr 78:2b:cb:51:54:a3
            inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
            UP BROADCAST RUNNING PROMISC MULTICAST  MTU:9000  Metric:1
            RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2895843 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)

[root@localhost ~]#
<!--NeedCopy-->
```

Modul erforderlich

Stellen Sie für eine bessere Netzwerkleistung sicher, dass das Modul vhost_net auf dem Linux-Host vorhanden ist. Um zu überprüfen, ob das Modul vhost_net vorhanden ist, führen Sie den folgenden Befehl auf dem Linux-Host aus:

```
lsmod | grep "vhost_net"
<!--NeedCopy-->
```

Wenn vhost_net noch nicht läuft, geben Sie den folgenden Befehl ein, um es auszuführen:

```
modprobe vhost_net
<!--NeedCopy-->
```


Bereitstellen der NetScaler VPX Instanz mithilfe von OpenStack

May 11, 2023

Sie können eine NetScaler VPX-Instanz in einer OpenStack-Umgebung bereitstellen, indem Sie entweder den **Nova-Boot-Befehl** (OpenStack CLI) oder Horizon (OpenStack-Dashboard) verwenden.

Das Provisioning einer VPX-Instanz umfasst optional die Verwendung von Daten aus dem Konfigurationslaufwerk. Das Konfigurationslaufwerk ist ein spezielles Konfigurationslaufwerk, das beim Booten als CD-ROM-Gerät an die Instanz angeschlossen wird. Dieses Konfigurationslaufwerk kann verwendet werden, um Netzwerkkonfigurationen wie die Management-IP-Adresse, die Netzwerkmaske und das Standard-Gateway zu übergeben und Kundenskripte einzufügen.

In einer NetScaler Appliance ist der Standardauthentifizierungsmechanismus kennwortbasiert. Jetzt wird der SSH-Schlüsselpaar-Authentifizierungsmechanismus für NetScaler VPX-Instanzen in der OpenStack-Umgebung unterstützt.

Das Schlüsselpaar (öffentlicher Schlüssel und privater Schlüssel) wird generiert, bevor der Public Key Cryptographie-Mechanismus verwendet wird. Sie können verschiedene Mechanismen wie Horizon, Puttygen.exe für Windows und `ssh-keygen` für die Linux-Umgebung verwenden, um das Schlüsselpaar zu generieren. Weitere Informationen zum Generieren von Schlüsselpaaren finden Sie in der Online-Dokumentation der jeweiligen Mechanismen.

Sobald ein Schlüsselpaar verfügbar ist, kopieren Sie den privaten Schlüssel an einen sicheren Ort, auf den autorisierte Personen Zugriff haben. In OpenStack kann Public Key mit dem Boot-Befehl Horizon oder Nova auf einer VPX-Instanz bereitgestellt werden. Wenn eine VPX-Instanz mithilfe von OpenStack bereitgestellt wird, erkennt sie zuerst, dass die Instanz in einer OpenStack-Umgebung gestartet wird, indem sie eine bestimmte BIOS-Zeichenfolge liest. Diese Zeichenfolge ist OpenStack Foundation und für Red Hat Linux-Distributionen wird sie in /etc/nova/release gespeichert. Dies ist ein Standardmechanismus, der in allen OpenStack-Implementierungen verfügbar ist, die auf der KVM-Hypervisor-Plattform basieren. Das Laufwerk muss ein bestimmtes OpenStack-Label haben.

Wenn das Konfigurationslaufwerk erkannt wird, versucht die Instanz, die Netzwerkkonfiguration, die benutzerdefinierten Skripts und das SSH-Schlüsselpaar zu lesen, falls vorhanden.

Benutzer-Datendatei

Die NetScaler VPX-Instanz verwendet eine benutzerdefinierte OVF-Datei, auch Benutzerdatendatei genannt, um Netzwerkkonfiguration, benutzerdefinierte Skripts zu injizieren. Diese Datei wird als Teil des Konfigurationslaufwerks bereitgestellt. Hier ist ein Beispiel für eine benutzerdefinierte OVF-Datei.

```
1 ```
2 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
3 <Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
```



```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1"
xmlns:cs="http://schemas.citrix.com/openstack">
<PlatformSection>
<Kind></Kind>
<Version>2016.1</Version>
<Vendor>VPX</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>
<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>
<Property oe:key="com.citrix.netscaler.orch_env" oe:value="openstack-
   orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
   "/>
</PropertySection>
 <cs:ScriptSection>
   <cs:Version>1.0</cs:Version>
     <ScriptSettingSection xmlns="http://schemas.citrix.com/openstack"
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
         <Scripts>
           <Script>
                 <Type>shell</Type>
                 <Parameter>X Y</Parameter>
                <Parameter>Z</Parameter>
                <BootScript>before</BootScript>
                  <Text>
                        #!/bin/bash
                        echo "Hi, how are you" $1 $2 >> /var/sample.txt
                  </Text>
           </Script>
           <Script>
                 <Type>python</Type>
                 <BootScript>after</BootScript>
                  <Text>
                       #!/bin/python
 print("Hello");
                  </Text>
           </Script>
   <Script>
```



```
45                   <Type>perl</Type>
46                   <BootScript>before</BootScript>
47                    <Text>
48                         !/usr/bin/perl
49   my $name = "VPX";
50   print "Hello, World $name !\n" ;
51                    </Text>
52              </Script>
53              <Script>
54                   <Type>nscli</Type>
55                   <BootScript>after</BootScript>
56                   <Text>
57                    add vlan 33
58   bind vlan 33 -ifnum 1/2
59                   </Text>
60              </Script>
61            </Scripts>
62        </ScriptSettingSection>
63    </cs:ScriptSection>
64  </Environment>
65  <!--NeedCopy--> ```
```

In der OVF-Datei wird “PropertySection” für die NetScaler-Netzwerkkonfiguration verwendet, während <cs:ScriptSection> zum Umschließen aller Skripts verwendet wird. Die Tags <Scripts></Scripts> werden verwendet, um alle Skripts zu bündeln. Jedes Skript ist zwischen den Tags <Script> </Script> definiert. Jedes Skript-Tag hat folgende Felder/Tags:

a) <Type>: Gibt den Wert für den Skripttyp an. Mögliche Werte: Shell/Perl/Python/NSLCI (für NetScaler CLI-Skripts)

b) <Parameter>: Stellt Parameter für das Skript bereit. Jedes Skript kann mehrere <Parameter>-Tags haben.

c) <BootScript>: Gibt den Ausführungspunkt des Skripts an. Mögliche Werte für dieses Tag: vorher/-nachher. “before” gibt an, dass das Skript ausgeführt wird, bevor PE auftaucht. “after” gibt an, dass das Skript ausgeführt wird, nachdem PE angezeigt wird.

d) <Text>: Fügt den Inhalt eines Skripts ein.

> **Hinweis**
>
> Derzeit kümmert sich die VPX-Instanz nicht um die Bereinigung von Skripten. Als Administrator müssen Sie die Gültigkeit des Skripts überprüfen.
>
> Nicht alle Abschnitte müssen vorhanden sein. Verwenden Sie eine leere “PropertySection”, um nur Skripts zu definieren, die beim ersten Start oder einer leeren Ausführung ausgeführt werden

> sollen, um nur die Netzwerkkonfiguration zu definieren.
>
> Nachdem die erforderlichen Abschnitte der OVF-Datei (Benutzerdatendatei) ausgefüllt wurden, verwenden Sie diese Datei, um die VPX-Instanz bereitzustellen.

Netzwerkkonfiguration

Im Rahmen der Netzwerkkonfiguration lautet die VPX-Instanz:

- Verwaltungs-IP-Adresse
- Netzwerkmaske
- Standard-Gateway

Nachdem die Parameter erfolgreich gelesen wurden, werden sie in die NetScaler-Konfiguration eingetragen, um die Instanz remote verwalten zu können. Wenn die Parameter nicht erfolgreich gelesen werden oder das Konfigurationslaufwerk nicht verfügbar ist, wechselt die Instanz zum Standardverhalten, das wie folgt lautet:

- Die Instanz versucht, die IP-Adressinformationen von DHCP abzurufen.
- Wenn DHCP ausfällt oder Times-Out ausfällt, wird die Instanz mit der Standardnetzwerkkonfiguration (192.168.100.1/16) erstellt.

Kundenskript

Die VPX-Instanz erlaubt es, während der ersten Bereitstellung ein benutzerdefiniertes Skript auszuführen. Die Appliance unterstützt Skripts vom Typ Shell, Perl, Python und NetScaler CLI-Befehle.

SSH-Schlüsselpaar-Authentifizierung

Die VPX-Instanz kopiert den öffentlichen Schlüssel, der im Konfigurationslaufwerk als Teil der Instanzmetadaten verfügbar ist, in ihre Datei „authorized_keys“. Dadurch kann der Benutzer mit einem privaten Schlüssel auf die Instanz zugreifen.

> **Hinweis**
>
> Wenn ein SSH-Schlüssel angegeben wird, funktionieren die Standardanmeldeinformationen (nsroot/nsroot) nicht mehr. Wenn ein kennwortbasierter Zugriff erforderlich ist, melden Sie sich mit dem entsprechenden privaten SSH-Schlüssel an und legen Sie manuell ein Kennwort fest.

Voraussetzungen

Bevor Sie eine VPX-Instanz in der OpenStack-Umgebung bereitstellen, extrahieren Sie die Datei `.qcow2` aus der TGZ-Datei und bauen Sie

Ein OpenStack-Bild aus dem qcow2-Image. Führen Sie die folgenden Schritte aus:

1. Extrahieren Sie die `.qcow2` Datei aus der `.tqz` Datei, indem Sie den folgenden Befehl eingeben

```
tar xvzf <TAR file>
tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. Erstellen Sie ein OpenStack-Image mit der in Schritt 1 extrahierten `.qcoz2` Datei, indem Sie den folgenden Befehl eingeben.

```
openstack image create --container-format bare --property
    hw_disk_bus=ide --disk-format qcow2 --file <path to qcow2 file>
     --public <name of the OpenStack image>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --ispublic=
true --container-format=bare --disk-format=qcow2< NSVPX-KVM
    -12.0-26.2_nc.qcow2
```

Abbildung 1: Die folgende Abbildung enthält eine Beispielausgabe für den Befehl glance image-create.

```
+------------------+--------------------------------------------------------+
| Field            | Value                                                  |
+------------------+--------------------------------------------------------+
| checksum         | 154ade3fc7dca7d1706b1d03d7d97552                       |
| container_format | bare                                                   |
| created_at       | 2017-03-13T08:52:31Z                                   |
| disk_format      | qcow2                                                  |
| file             | /v2/images/322c1e0f-cce8-4b7b-b53e-bd8152c388ed/file   |
| id               | 322c1e0f-cce8-4b7b-b53e-bd8152c388ed                   |
| min_disk         | 0                                                      |
| min_ram          | 0                                                      |
| name             | VPX-KVM-12.0-26.2
| owner            | 58d17d81df5d4406afbb4fdab3a58d79                       |
| properties       | hw_disk_bus='ide'                                      |
| protected        | False                                                  |
| schema           | /v2/schemas/image                                      |
| size             | 784338944                                              |
| status           | active                                                 |
| updated_at       | 2017-03-13T08:52:43Z                                   |
| virtual_size     | None                                                   |
| visibility       | public                                                 |
+------------------+--------------------------------------------------------+
```

Provisioning einer VPX-Instanz

Sie können eine VPX-Instanz auf zwei Arten bereitstellen, indem Sie eine der Optionen verwenden:

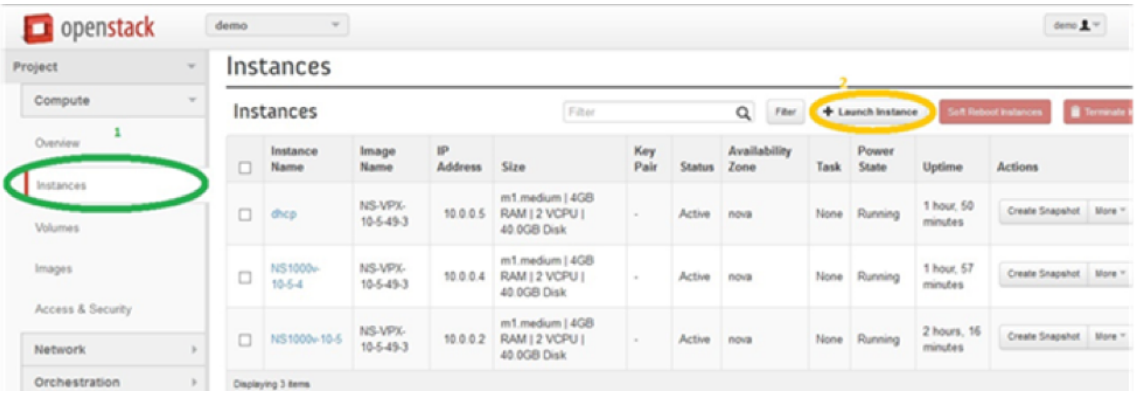
- Horizon (OpenStack-Dashboard)

- Nova-Startbefehl (OpenStack CLI)

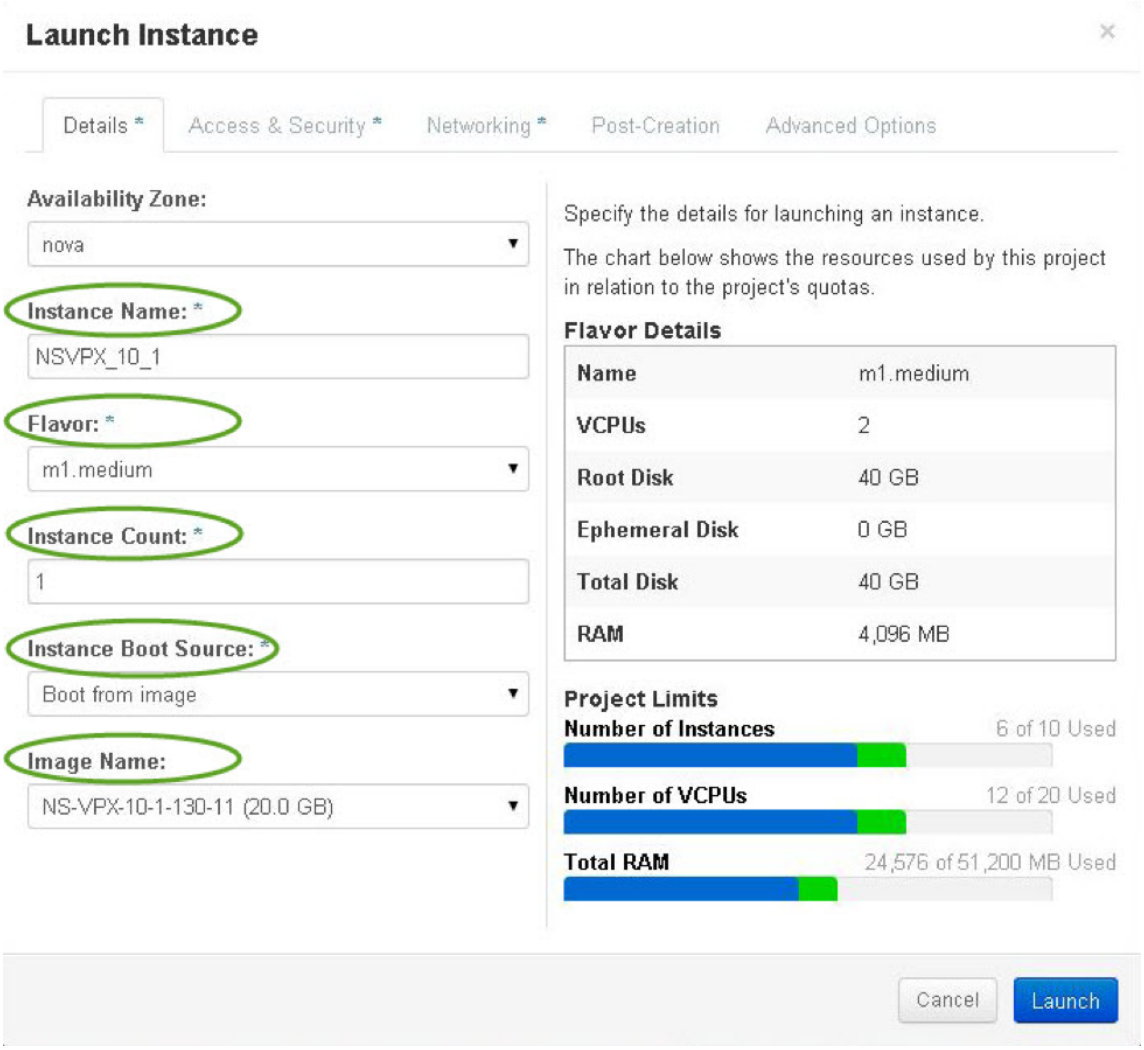
Stellen Sie eine VPX-Instanz mithilfe des OpenStack-Dashboards bereit

Gehen Sie wie folgt vor, um die VPX-Instanz mithilfe von Horizon bereitzustellen:

1. Melden Sie sich im OpenStack-Dashboard an.
2. Wählen Sie im Projektfenster auf der linken Seite des Dashboards die Option **Instanzen**aus.
3. Klicken Sie im Instanzen Bedienfeld auf **Instanz starten**, um den Instanzentart-Assistenten zu öffnen.



4. Geben Sie im Assistenten zum Starten von Instanz die folgenden Details ein:
   a) Instanzname
   b) Instanzgeschmack
   c) Anzahl der Instanzen
   d) Instance-Startquelle
   e) Imagename



5. Stellen Sie ein neues Schlüsselpaar oder ein vorhandenes Schlüsselpaar über Horizon bereit, indem Sie die folgenden Schritte ausführen:

   a) Wenn Sie kein bestehendes Schlüsselpaar haben, erstellen Sie den Schlüssel, indem Sie alle vorhandenen Mechanismen verwenden. Wenn Sie einen vorhandenen Schlüssel haben, überspringen Sie diesen Schritt.

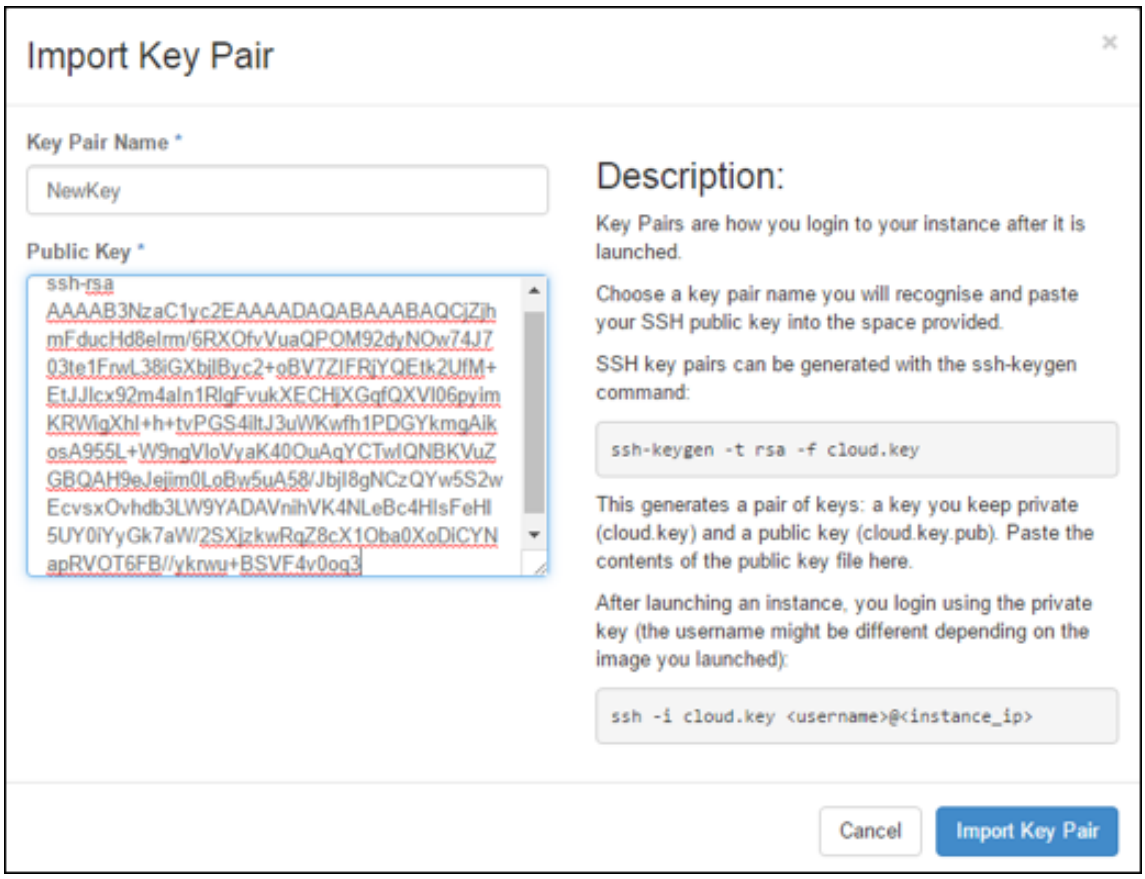
   b) Kopieren Sie den Inhalt des öffentlichen Schlüssels.

   c) Gehen Sie zu **Horizon > Instances > Create New Instances**.

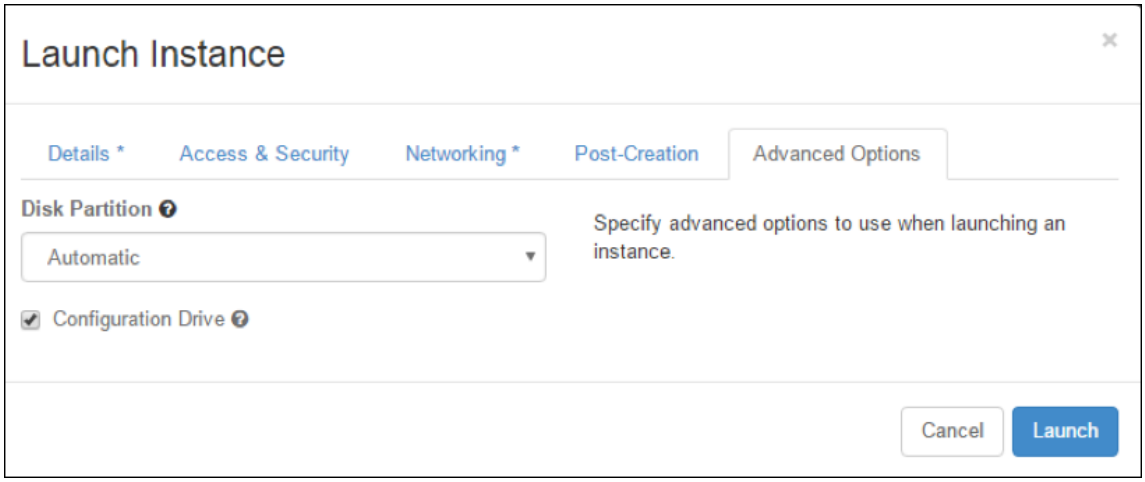
   d) Klicken Sie **auf Access & Security**.

   e) Klicken Sie auf das Pluszeichen neben dem Dropdownmenü **Schlüsselpaar** und geben Sie Werte für die angezeigten Parameter ein.

   f) Fügen Sie den Inhalt des öffentlichen Schlüssels in das Feld *Öffentlicher Schlüssel* ein, geben Sie dem Schlüssel einen Namen und klicken Sie auf **Schlüsselpaar importieren**.



6. Klicken Sie im Assistenten auf die Registerkarte **Post-Creation**. Fügen Sie im Anpassungsskript den Inhalt der Benutzerdatendatei hinzu. Die Benutzerdatendatei enthält die IP-Adresse, Netmask- und Gateway-Details sowie Kundenskripte der VPX-Instanz.
7. Nachdem ein Schlüsselpaar ausgewählt oder importiert wurde, aktivieren Sie die Option config-drive und klicken Sie auf **Starten**.



Provisioning der VPX-Instanz mi OpenStack CLI

Gehen Sie wie folgt vor, um mithilfe der OpenStack-CLI eine VPX-Instanz bereitzustellen.

1. Um ein Image aus qcow2 zu erstellen, geben Sie den folgenden Befehl ein:

   ```
   openstack image create --container-format bare --property hw_disk_bus=
   ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX-ToT-
   Image
   ```

2. Um ein Image für die Erstellung einer Instanz auszuwählen, geben Sie den folgenden Befehl ein:

   ```
   openstack image list | more
   ```

3. Um eine Instanz einer bestimmten Variante zu erstellen, geben Sie den folgenden Befehl ein, um eine Flavour-ID/einen Namen von aus einer Liste auszuwählen:

   ```
   openstack flavor list
   ```

4. Um eine Netzwerkkarte an ein bestimmtes Netzwerk anzuschließen, geben Sie den folgenden Befehl ein, um eine Netzwerk-ID aus einer Netzwerkliste auszuwählen:

   ```
   openstack network list
   ```

5. Um eine Instanz zu erstellen, geben Sie den folgenden Befehl ein:

   ```
   1 openstack server create --flavor FLAVOR_ID --image IMAGE_ID --key-
       name KEY_NAME
   2 --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id=
       net-uuid
   3 INSTANCE_NAME
   4 openstack server create --image VPX-ToT-Image --flavor m1.medium
       --user-data
   5 ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6-3
       efd44b761b9
   6 VPX-ToT
   ```

Abbildung 2: Die folgende Abbildung zeigt eine Beispielausgabe.

Field	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	None
OS-EXT-SRV-ATTR:hypervisor_hostname	None
OS-EXT-SRV-ATTR:instance_name	instance-000001c2
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	None
OS-SRV-USG:terminated_at	None
accessIPv4	
accessIPv6	
addresses	
adminPass	pFVvMtq7N8Z6
config_drive	True
created	2017-03-13T10:32:59Z
flavor	m1.medium (3)
hostId	
id	a1fe991e-3604-43a0-9dd6-59fa0f3749df
image	VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)
key_name	None
name	VPX-ToT
os-extended-volumes:volumes_attached	[]
progress	0
project_id	58d17d81df5d4406afbb4fdab3a58d79
properties	
security_groups	[{u'name': u'default'}]
status	BUILD
updated	2017-03-13T10:33:00Z
user_id	a6347b33916b4eb1b1f76360a9c8f935

NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereitstellen

May 11, 2023

Der Virtual Machine Manager ist ein Desktop-Tool zur Verwaltung von VM-Gästen. Es ermöglicht Ihnen, neue VM-Gäste und verschiedene Speichertypen zu erstellen und virtuelle Netzwerke zu verwalten. Sie können mit dem integrierten VNC-Viewer auf die grafische Konsole der VM-Gäste zugreifen und Leistungsstatistiken entweder lokal oder remote einsehen.

Nachdem Sie Ihre bevorzugte Linux-Distribution mit aktivierter KVM-Virtualisierung installiert haben, können Sie mit der Bereitstellung virtueller Maschinen fortfahren.

Wenn Sie den Virtual Machine Manager zur Bereitstellung einer NetScaler VPX-Instanz verwenden, haben Sie zwei Möglichkeiten:

- Geben Sie die IP-Adresse, das Gateway und die Netzmaske manuell ein
- Automatische Zuweisung der IP-Adresse, des Gateway und der Netzmaske (automatische Bereitstellung)

Sie können zwei Arten von Images verwenden, um eine NetScaler VPX-Instanz bereitzustellen:

- ROH
- QCOW2

Sie können ein NetScaler VPX-RAW-Image in ein QCOW2-Image konvertieren und die NetScaler VPX-Instanz bereitstellen. Um das RAW-Bild in ein QCOW2-Bild zu konvertieren, geben Sie den folgenden Befehl ein:

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Zum Beispiel:

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5_nc
.qcow
```

Eine typische NetScaler VPX-Bereitstellung auf KVM umfasst die folgenden Schritte:

- Überprüfung der Voraussetzungen für die automatische Provisioning einer NetScaler VPX-Instance
- Provisioning der NetScaler VPX-Instanz mithilfe eines RAW-Images
- Provisioning der NetScaler VPX-Instanz mithilfe eines QCOW2-Images
- Hinzufügen zusätzlicher Schnittstellen zu einer VPX-Instanz mithilfe von Virtual Machine Manager

Überprüfen Sie die Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz

Die automatische Bereitstellung ist eine optionale Funktion, bei der Daten vom CD-ROM-Laufwerk verwendet werden. Wenn diese Funktion aktiviert ist, müssen Sie die Management-IP-Adresse, die Netzwerkmaske und das Standard-Gateway der NetScaler VPX-Instanz bei der Ersteinrichtung nicht eingeben.

Sie müssen die folgenden Aufgaben ausführen, bevor Sie eine VPX-Instanz automatisch bereitstellen können:

1. Erstellen Sie eine benutzerdefinierte XML-Datei oder Benutzerdatendatei (Open Virtualization Format) (OVF).
2. Konvertieren Sie die OVF-Datei in ein ISO-Image mit einer Online-Anwendung (z. B. PowerISO).
3. Hängen Sie das ISO-Image auf dem KVM-Host mit beliebigen Secure Copy (SCP) -basierten Tools ein.

Beispiel für OVF-XML-Datei:

Hier ist ein Beispiel für den Inhalt einer OVF-XML-Datei, die Sie als Beispiel verwenden können, um Ihre Datei zu erstellen.

```
1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2
3 <Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`
4
```



```
xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`

oe:id=""

xmlns="`http://schemas.dmtf.org/ovf/environment/1"`

xmlns:cs="`http://schemas.citrix.com/openstack">`

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>

<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>

<Property oe:key="com.citrix.netscaler.orch_env" oe:value="KVM"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="
   255.255.255.0"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1
   "/>

</PropertySection>

</Environment>
<!--NeedCopy-->
```

In der vorangehenden OVF-XML-Datei wird “PropertySection” für die NetScaler-Netzwerkkonfiguration verwendet. Wenn Sie die Datei erstellen, geben Sie Werte für die Parameter an, die am Ende des Beispiels hervorgehoben werden:

- Verwaltungs-IP-Adresse
- Netzmaske
- Gateway

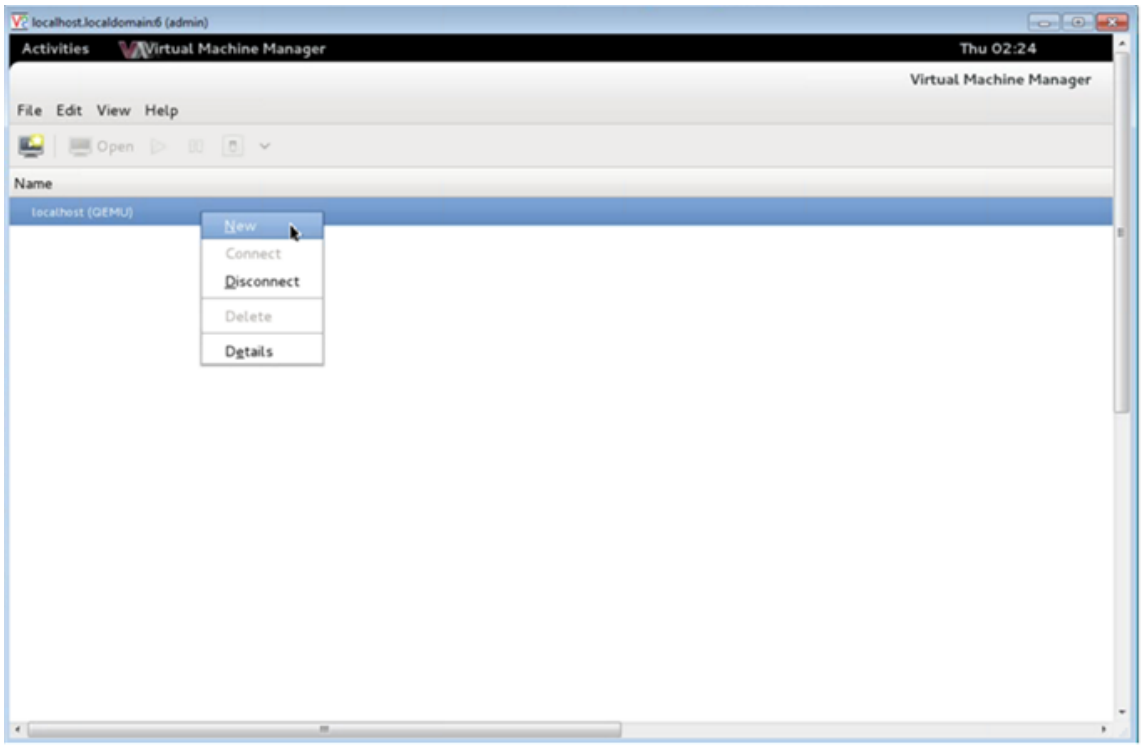
> **Wichtig**
>
> Wenn die OVF-Datei nicht richtig XML-formatiert ist, wird der VPX-Instanz die Standard-Netzwerkkonfiguration zugewiesen, nicht die in der Datei angegebenen Werte.

Stellen Sie die NetScaler VPX-Instanz mithilfe eines RAW-Images bereit

Mit dem Virtual Machine Manager können Sie eine NetScaler VPX-Instanz mithilfe eines RAW-Images bereitstellen.

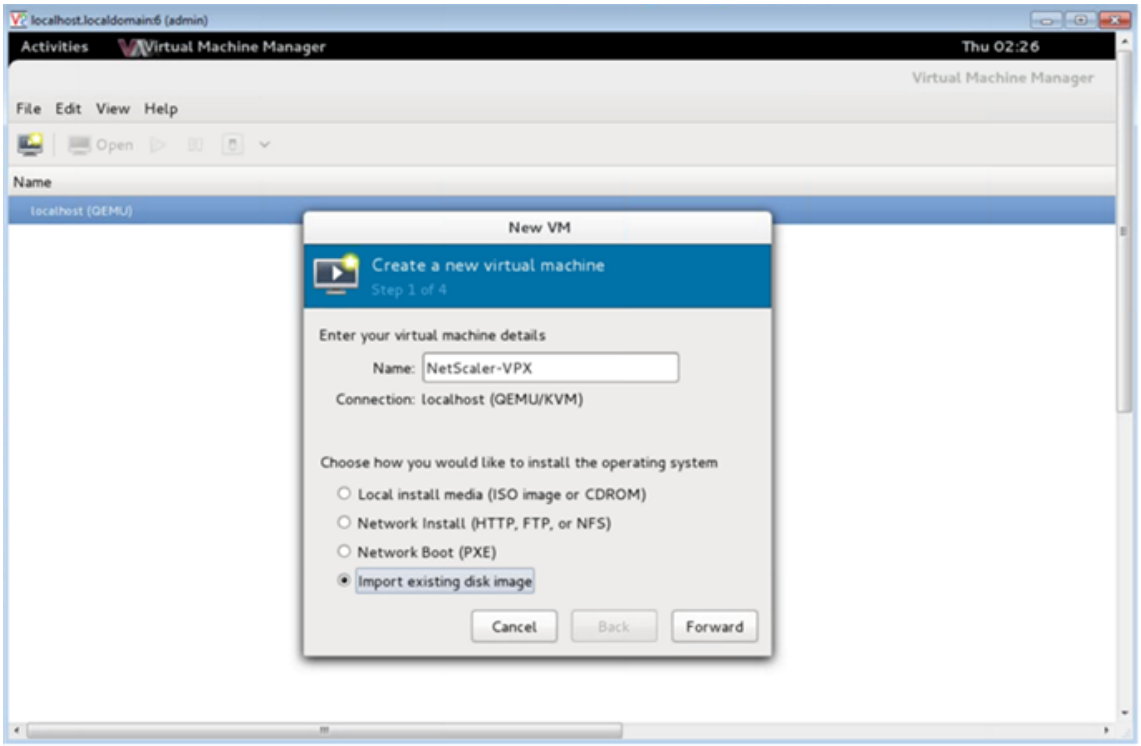
Gehen Sie folgendermaßen vor, um eine NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereitzustellen:

1. Öffnen Sie den Virtual Machine Manager (**Anwendung** > **Systemprogramme** > **Virtual Machine Manager**), und geben Sie die Anmeldeinformationen im Fenster **Authentifizieren** ein.
2. Klicken Sie auf das  oder klicken Sie mit der rechten Maustaste auf **localhost (QEMU)**, um eine neue NetScaler VPX-Instanz zu erstellen.

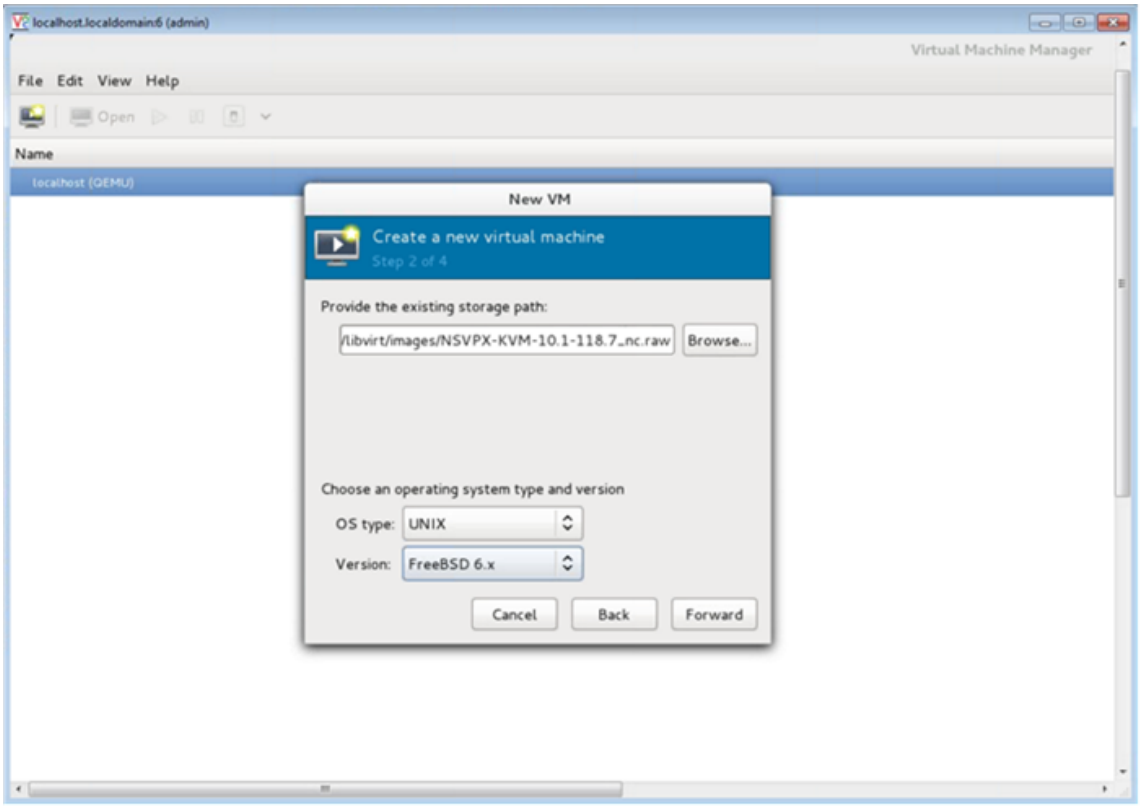


3. Geben Sie im Textfeld **Name** einen Namen für die neue VM ein (z. B. NetScaler-VPX).

4. Wählen Sie im Fenster **Neue virtuelle Maschine** unter „Wählen Sie aus, wie Sie das Betriebssystem installieren möchten“ die Option **Vorhandenes Festplatten-Image importieren**und klicken Sie dann auf **Weiterleiten**.

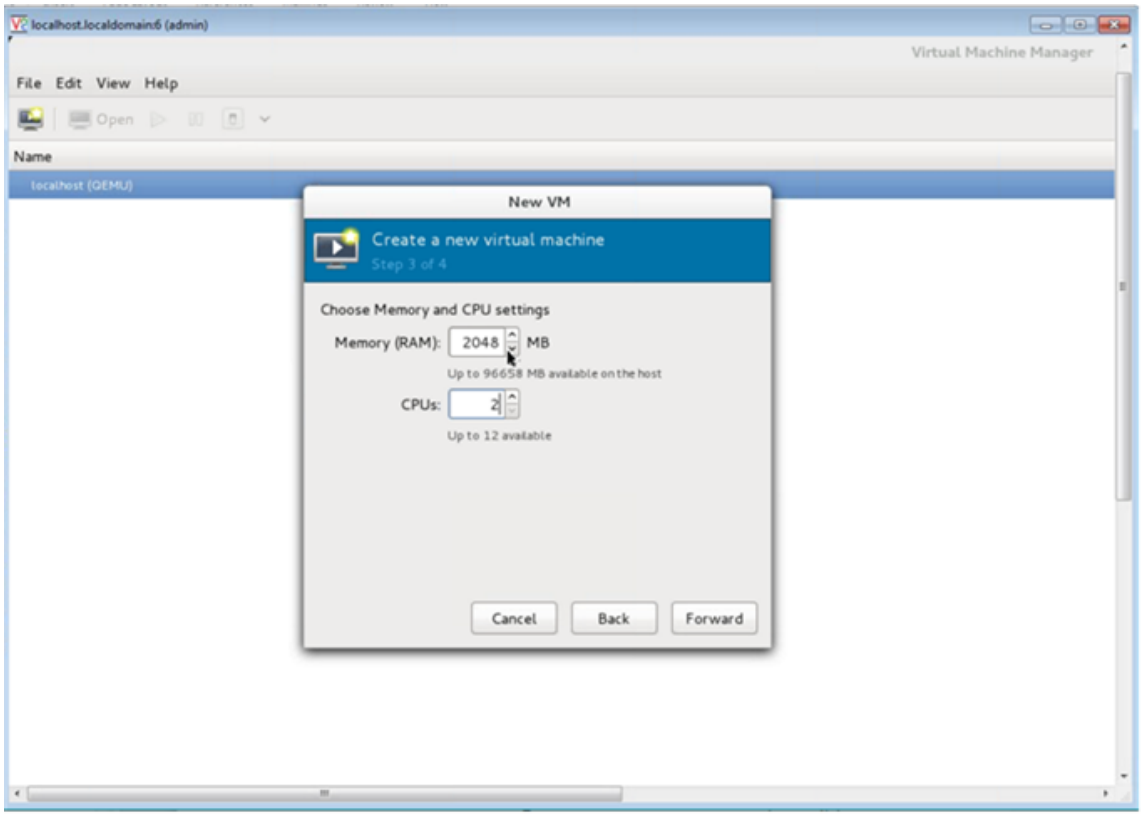


5. Navigieren **Sie im Feld Vorhandenen Speicherpfad angeben** zum Pfad zum Image. Wählen Sie den Betriebssystemtyp UNIX und die Version FreeBSD 6.x. Klicken Sie dann auf **Weiterleiten**.

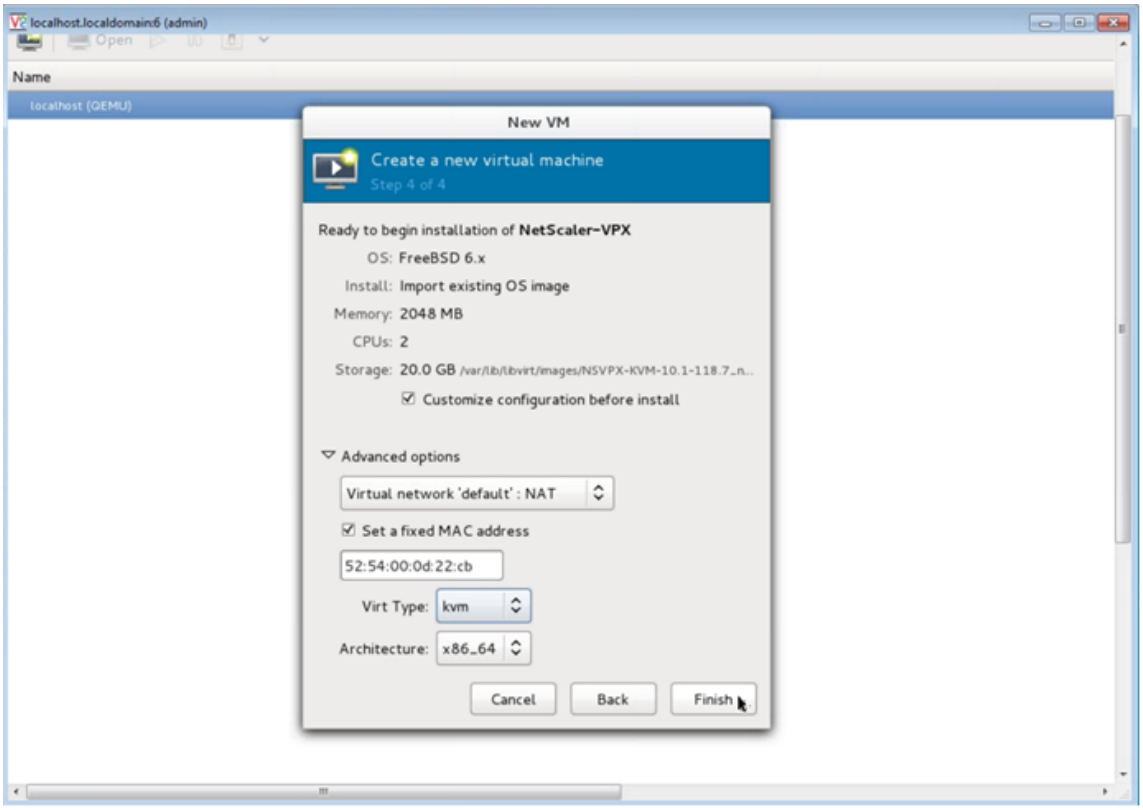


6. **Wählen Sie unter Speicher- und CPU-Einstellungen** auswählen die folgenden Einstellungen aus, und klicken Sie dann auf **Weiterleiten**:

    - Speicher (RAM) — 2048 MB
    - CPUs — 2

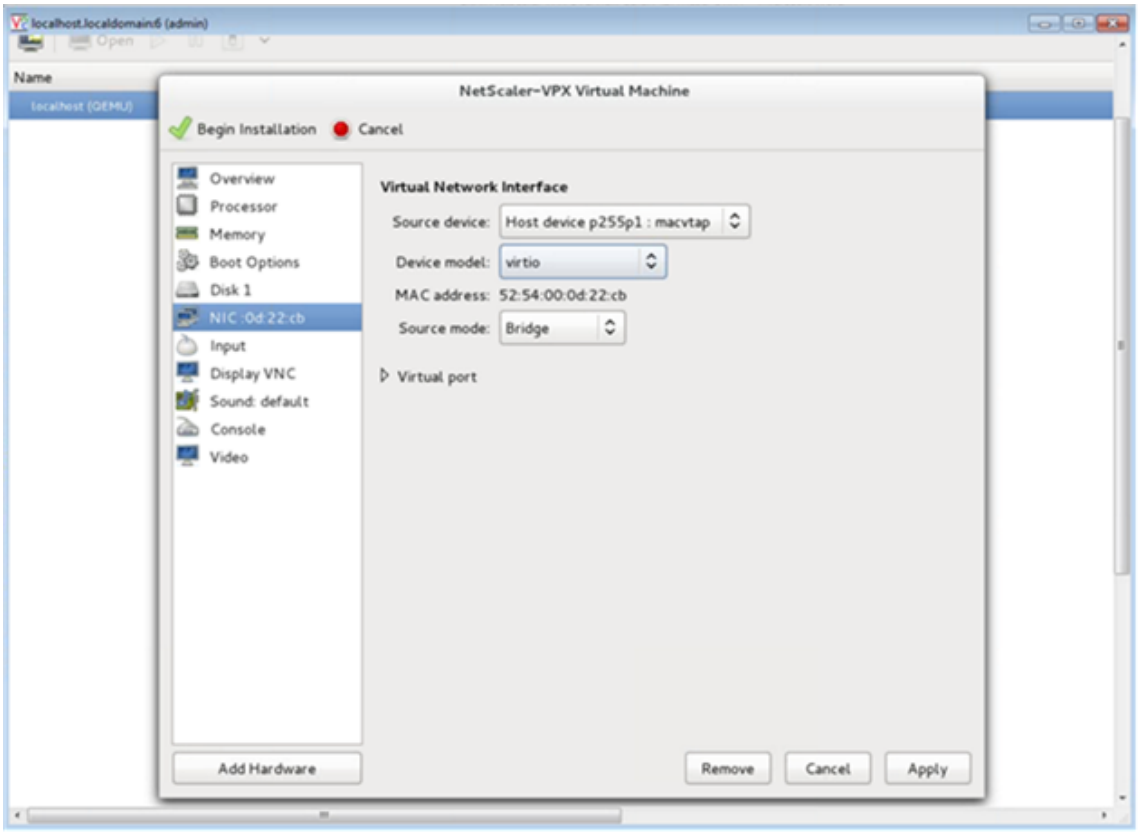


7. Aktivieren Sie das Kontrollkästchen **Konfiguration vor der Installation anpassen** . Optional können Sie unter **Erweiterte Optionen** die MAC-Adresse anpassen. Stellen Sie sicher, dass der ausgewählte **Virt-Typ** KVM ist und die ausgewählte Architektur x86_64 ist. Klicken Sie auf **Fertig stellen**.



8. Wählen Sie eine Netzwerkkarte aus, und stellen Sie die folgende Konfiguration bereit:

   - Quellgerät- `ethX macvtap` oder Bridge
   - Geräte-Modell— `virtio`
   - Quellmodus— Brücke



9. Klicken Sie auf **Anwenden**.
10. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, lesen Sie den Abschnitt **Aktivieren der automatischen Provisioning durch Anhängen eines CD-ROM-Laufwerks** in diesem Dokument. Klicken Sie andernfalls auf **Installation beginnen**. Nachdem Sie den NetScaler VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

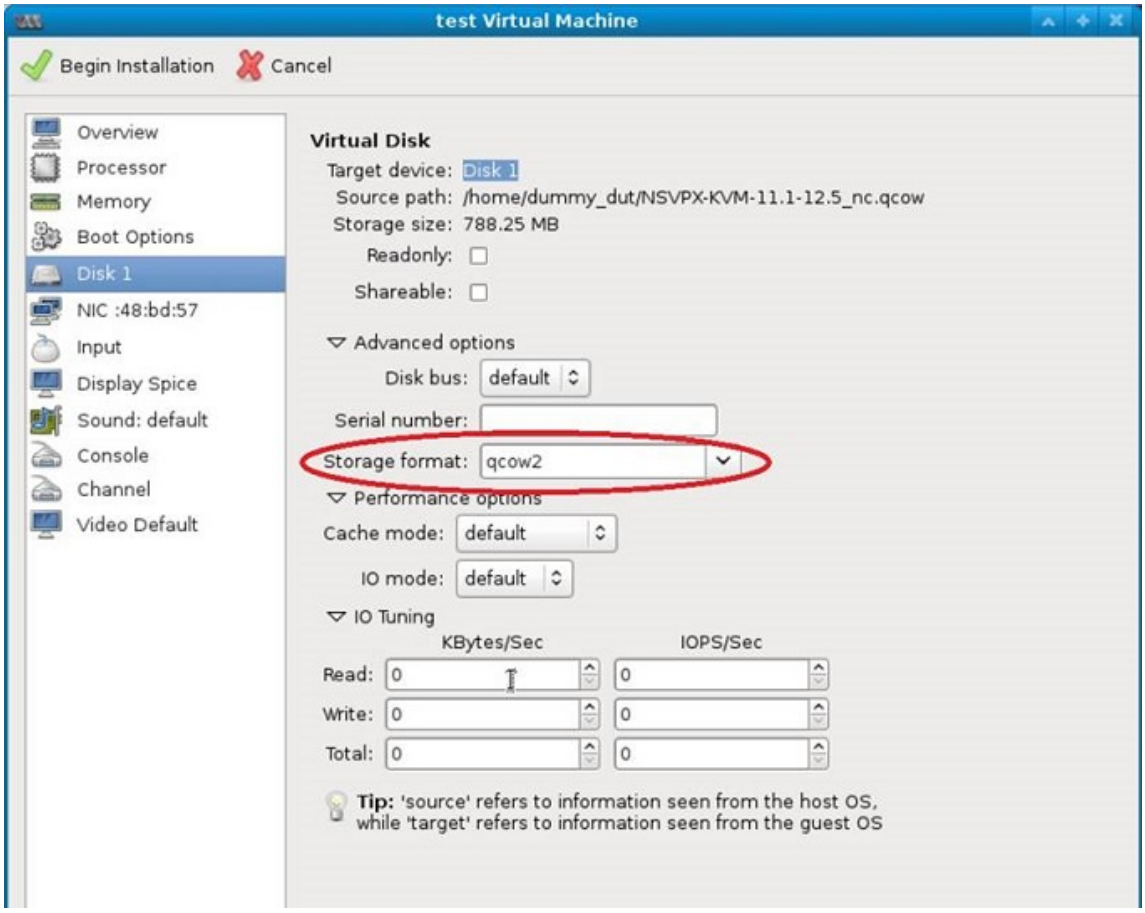
Bereitstellen der NetScaler VPX Instanz mithilfe eines QCOW2-Images

Mit dem Virtual Machine Manager können Sie die NetScaler VPX-Instanz mithilfe eines QCOW2-Images bereitstellen.

Gehen Sie folgendermaßen vor, um eine NetScaler VPX-Instanz mit einem QCOW2-Image bereitzustellen:

1. Folgen Sie **Schritt 1** bis **Schritt 8** unter Bereitstellen der NetScaler VPX-Instanz mithilfe eines RAW-Images.

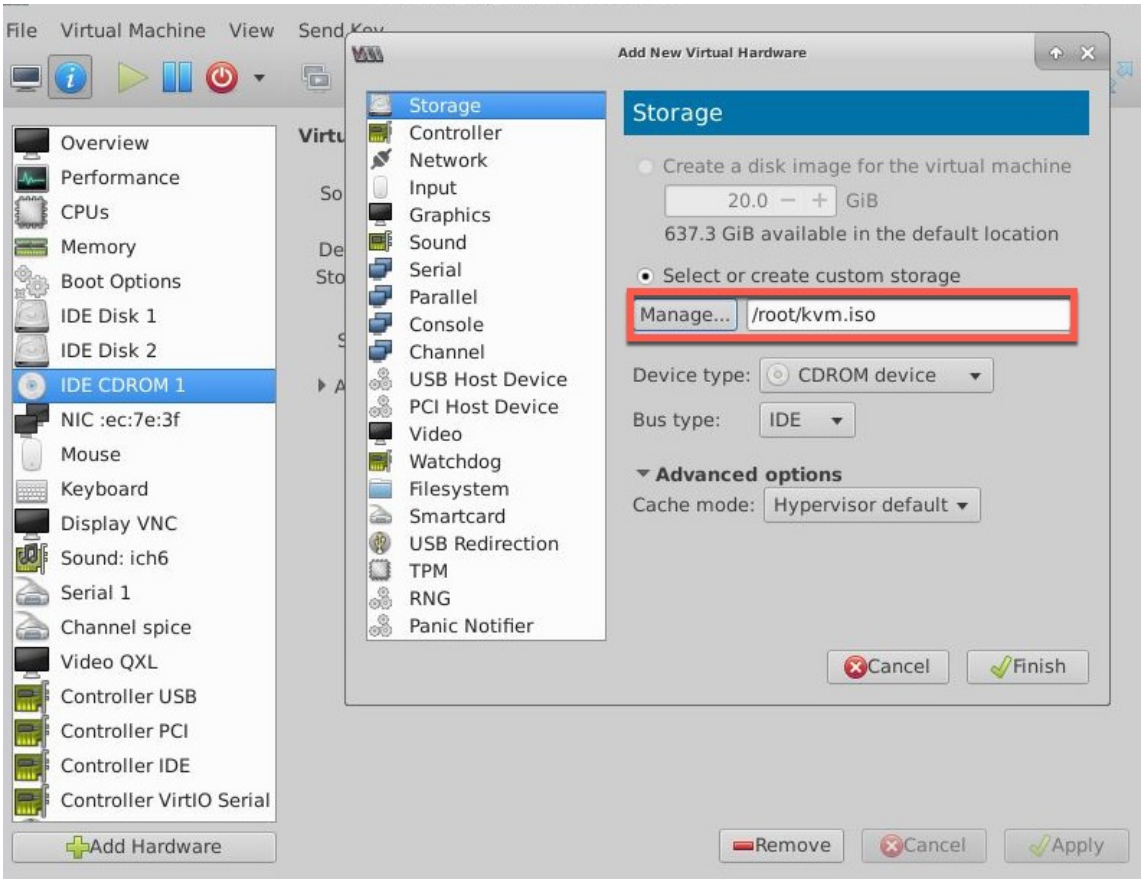
   Hinweis: Stellen Sie sicher, dass Sie **qcow2**image in **Schritt 5**auswählen.
2. Wählen Sie **Disk 1** und klicken Sie auf **Erweiterte Optionen**.
3. Wählen Sie **qcow2** aus der Dropdownliste Speicherformat aus.



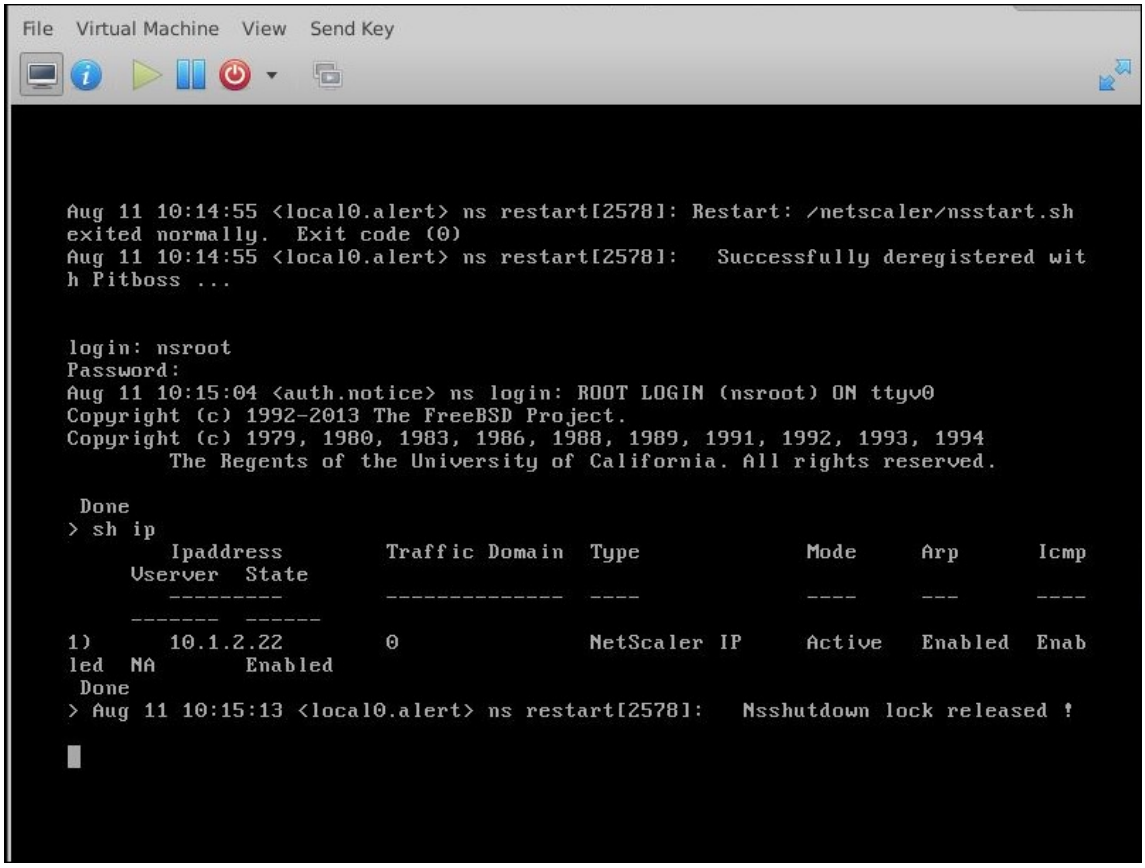
4. Klicken Sie auf **Übernehmen**, und klicken Sie dann auf **Installation beginnen**. Nachdem Sie den NetScaler VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

Aktivieren der automatischen Bereitstellung durch Anfügen eines CD-ROM-Laufwerks

1. Klicken Sie auf **Hardware hinzufügen > Speicher > Gerätetyp > CD-ROM-Gerät**.
2. Klicken Sie auf **Verwalten**, wählen Sie die richtige ISO-Datei aus, die Sie im Abschnitt “Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz” bereitgestellt haben, und klicken Sie auf **Fertig stellen**. Eine neue CD-ROM unter Resources auf Ihrer NetScaler VPX-Instanz wird erstellt.



3. Schalten Sie die VPX-Instanz ein und stellt automatisch die in der OVF-Datei bereitgestellte Netzwerkkonfiguration bereit, wie in der Beispielbildaufnahme gezeigt.



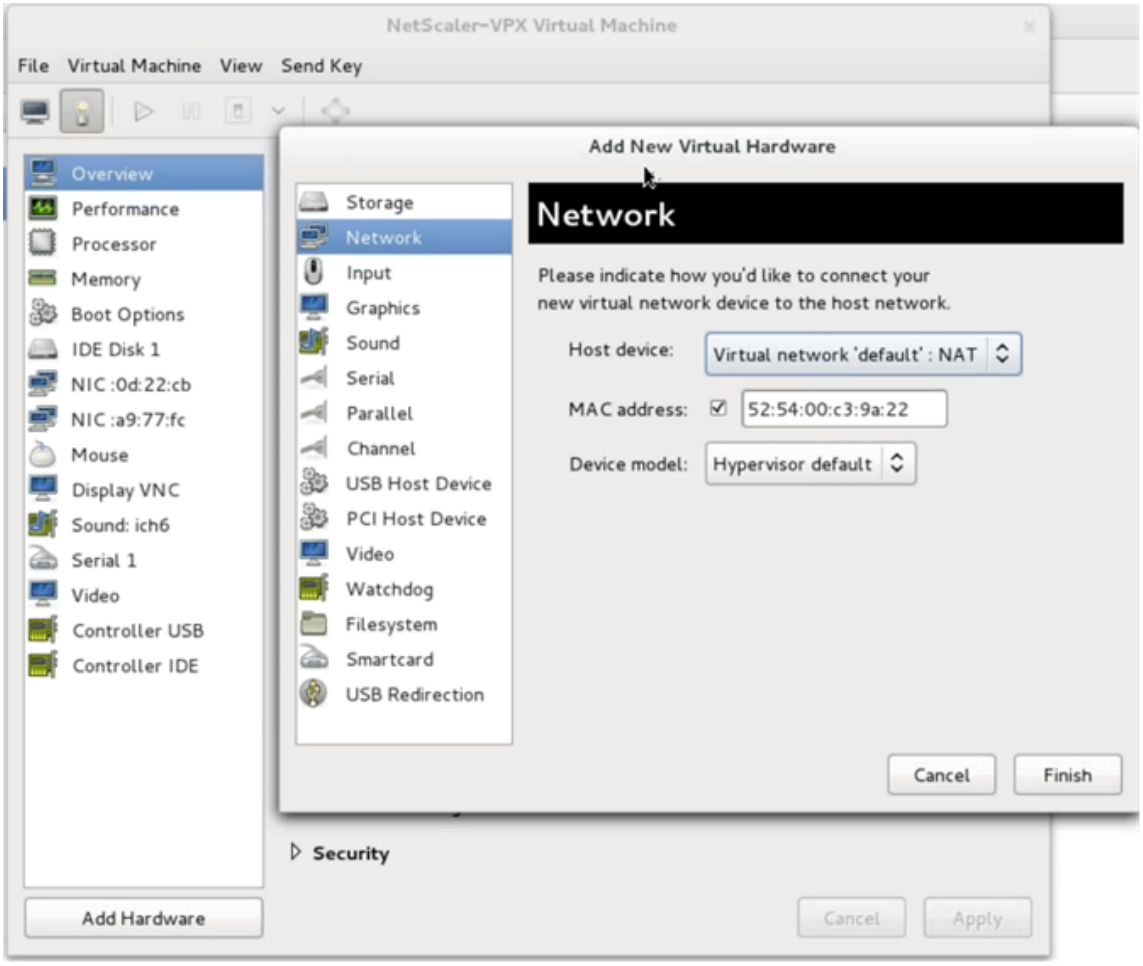
4. Wenn die automatische Bereitstellung fehlschlägt, wird die Instanz die Standard-IP-Adresse (192.168.100.1) angezeigt. In diesem Fall müssen Sie die Erstkonfiguration manuell abschließen. Weitere Informationen finden Sie unter Konfigurieren des ADC zum ersten Mal.

Fügen Sie der NetScaler VPX-Instanz weitere Schnittstellen hinzu, indem Sie den Virtual Machine Manager verwenden

Nachdem Sie die NetScaler VPX-Instanz auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

Gehen Sie folgendermaßen vor, um weitere Schnittstellen hinzuzufügen.

1. Fahren Sie die NetScaler VPX-Instanz herunter, die auf der KVM ausgeführt wird.
2. Klicken Sie mit der rechten Maustaste auf die VPX-Instanz und wählen Sie **Öffnen** aus dem Popup-Menü.
3. Klicken Sie auf das  in der Kopfzeile, um die Details der virtuellen Hardware anzuzeigen.
4. Klicken Sie auf **Hardware hinzufügen**. Wählen **Sie im Fenster Neue virtuelle Hardware hinzufügen**im Navigationsmenü die Option **Netzwerk** aus.



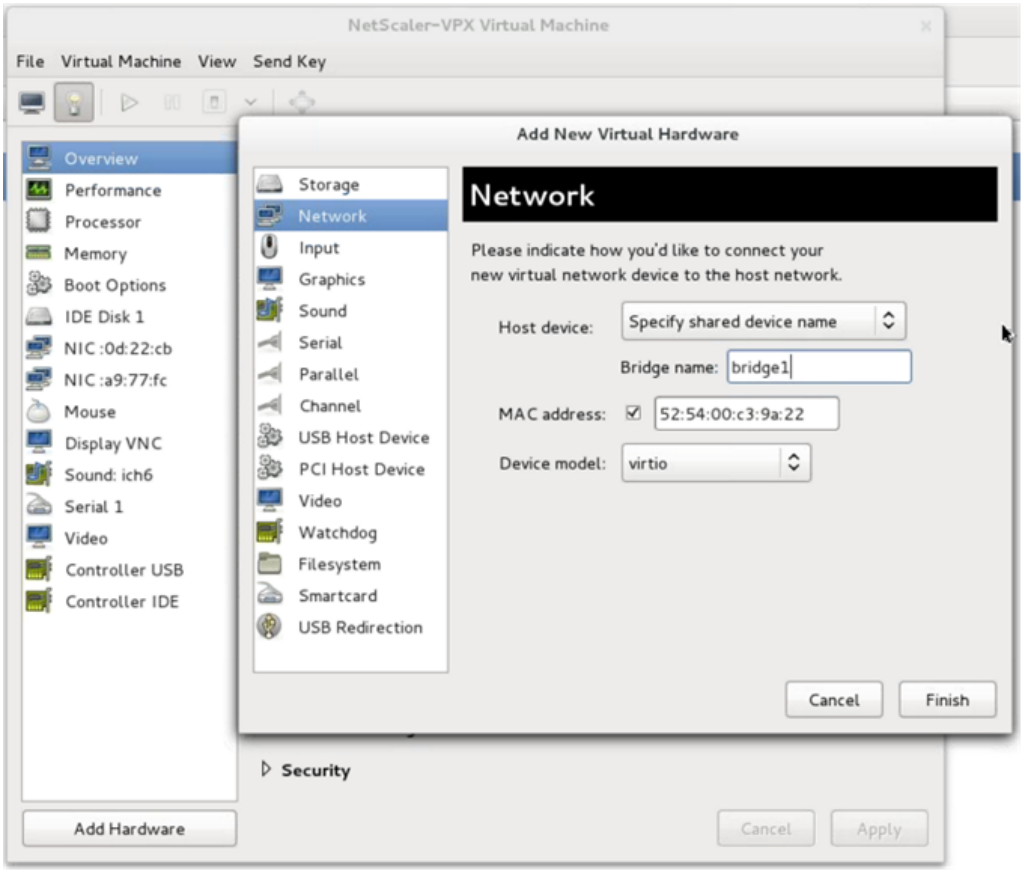
5. Wählen Sie im Feld **Host-Gerät** den physischen Schnittstellentyp aus. Der Hostgerätetyp kann entweder Bridge oder MacVTap sein. Im Falle von MacVTap sind VEPA, Bridge, Private und Pass-Through vier Modi möglich.

    a) Für Brücke

        i. Host-Gerät — Wählen Sie die Option „Namen des gemeinsam genutzten Geräts angeben“.

        ii. Geben Sie den Bridge-Namen ein, der auf dem KVM-Host konfiguriert ist.

        Hinweis: Stellen Sie sicher, dass Sie eine Linux-Bridge auf dem KVM-Host konfiguriert, die physische Schnittstelle an die Bridge gebunden und die Bridge in den Status UP versetzt haben.



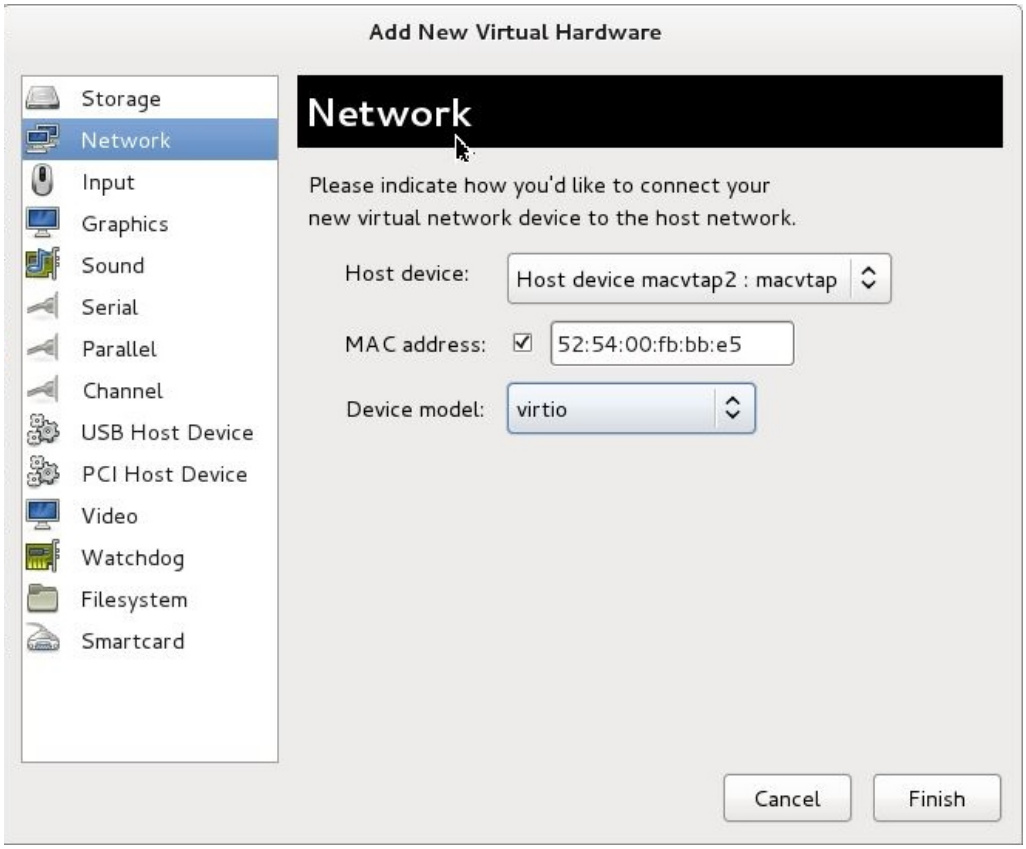
iii. Gerätemodell—`virtio`.

iv. Klicken Sie auf Fertig stellen.

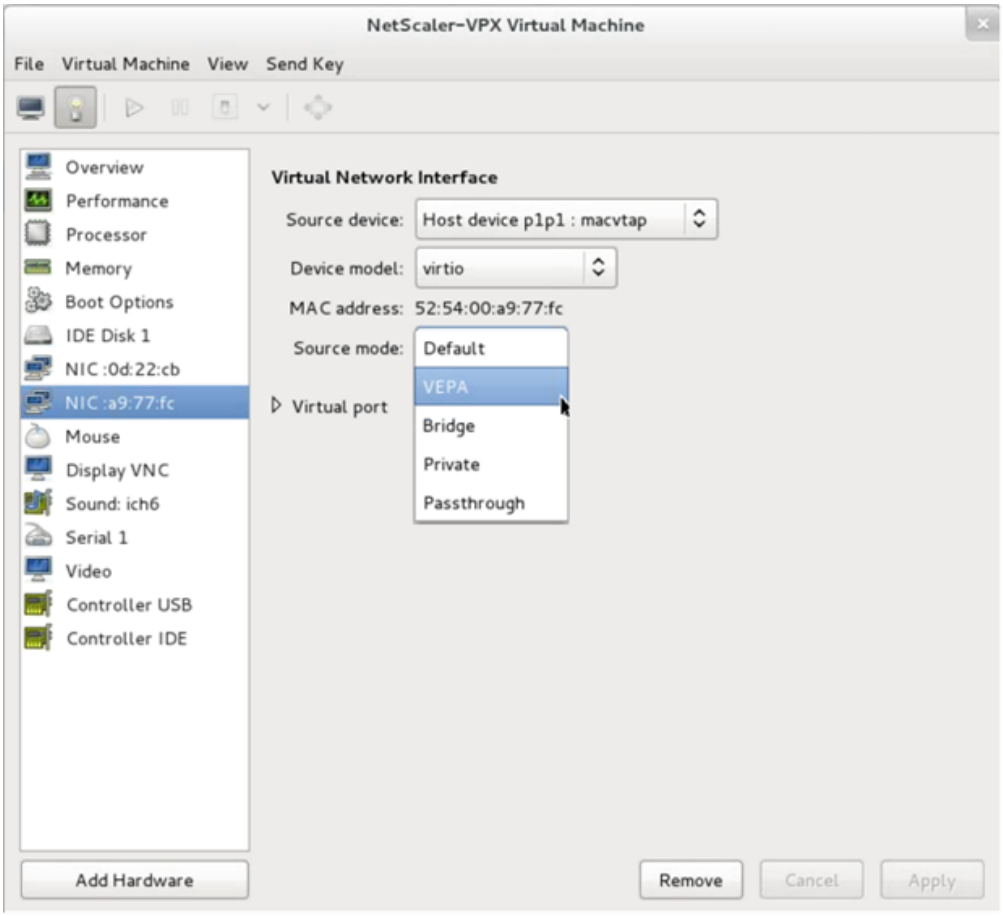
b) Für MacVTAP

i. Hostgerät — Wählen Sie die physische Schnittstelle aus dem Menü aus.

ii. Gerätemodell—`virtio`.



iii. Klicken Sie auf Fertig stellen. Sie können die neu hinzugefügte NIC im Navigationsbereich anzeigen.



iv. Wählen Sie die neu hinzugefügte NIC und wählen Sie den Quellmodus für diese NIC. Die verfügbaren Modi sind VEPA, Bridge, Private und Passthrough. Weitere Informationen zur Benutzeroberfläche und den Modi finden Sie unter Quellschnittstelle und Modi.

v. Klicken Sie auf Anwenden.

6. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, lesen Sie den Abschnitt „Hinzufügen eines Konfigurationslaufwerks zur Aktivierung der automatischen Provisioning“ in diesem Dokument. Andernfalls schalten Sie die VPX-Instanz ein, um die Erstkonfiguration manuell abzuschließen.

> **Wichtig**
>
> Konfigurationen von Schnittstellenparametern wie Geschwindigkeit, Duplex und Autonegotiation werden nicht unterstützt.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen

May 11, 2023

Sie können eine NetScaler VPX-Instanz konfigurieren, die auf einer Linux-KVM-Plattform ausgeführt wird, mithilfe der Single-Root-I/O-Virtualisierung (SR-IOV) mit den folgenden Netzwerkkarten:

- Intel 82599 10 G
- Intel X710 10 G
- Intel XL710 40 G
- Intel X722 10G

In diesem Abschnitt wird beschrieben, wie Sie:

- Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle
- Statisches LA/LACP auf der SR-IOV-Schnittstelle konfigurieren
- VLAN auf der SR-IOV-Schnittstelle konfigurieren

Einschränkungen

Beachten Sie die Einschränkungen bei der Verwendung von Intel 82599-, X710-, XL710- und X722-NICs. Die folgenden Funktionen werden nicht unterstützt.

Einschränkungen für Intel 82599 NIC:

- L2-Moduswechsel.
- Admin-Partitionierung (gemeinsam genutzter VLAN-Modus).
- Hohe Verfügbarkeit (aktiv-aktiver Modus).
- Jumbo-Rahmen.
- IPv6: Sie können nur bis zu 30 eindeutige IPv6-Adressen in einer VPX-Instanz konfigurieren, wenn Sie mindestens eine SR-IOV-Schnittstelle haben.
- Die VLAN-Konfiguration auf Hypervisor für SRIOV VF-Schnittstelle über `ip link` Befehl wird nicht unterstützt.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Autonegotiationen werden nicht unterstützt.

Einschränkungen für Intel X710 10G-, Intel XL710 40G- und Intel X722 10G-NICs:

- L2-Moduswechsel.
- Admin-Partitionierung (gemeinsam genutzter VLAN-Modus).
- In einem Cluster werden Jumbo-Frames nicht unterstützt, wenn die XL710-NIC als Datenschnittstelle verwendet wird.

- Die Schnittstellenliste ordnet neu an, wenn Schnittstellen getrennt und wieder verbunden werden.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und automatische Absprache werden nicht unterstützt.
- Der Schnittstellenname ist 40/X für Intel X710 10G-, Intel XL710 40G- und Intel X722 10G-NICs
- Bis zu 16 Intel XL710/X710/X722 SRIOV- oder PCI-Passthrough-Schnittstellen können auf einer VPX-Instance unterstützt werden.

> **Hinweis:** Damit Intel X710 10G-, Intel XL710 40G- und Intel X722 10G-NICs IPv6 unterstützen, müssen Sie den Vertrauensmodus auf den Virtual Functions (VFS) aktivieren, indem Sie den folgenden Befehl auf dem KVM-Host eingeben:
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> Beispiel:
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Voraussetzungen

Bevor Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren, müssen Sie die folgenden erforderlichen Aufgaben ausführen. Einzelheiten zur Ausführung der entsprechenden Aufgaben finden Sie in der Spalte NIC.

Aufgabe	Intel 82599 NIC	Intel X710-, XL710- und X722-Netzwerkkarten
1. Fügen Sie die Netzwerkkarte zum KVM-Host hinzu.	-	-
2. Laden Sie den neuesten Intel-Treiber herunter und installieren Sie ihn.	IXGBE-Treiber	I40E-Treiber
3. Listet den Treiber auf dem KVM-Host auf.	Fügen Sie den folgenden Eintrag in der Datei /etc/modprobe.d/blacklist.conf hinzu: `blacklist ixgbevf`. Verwenden Sie die IXGBE-Treiberversion 4.3.15 (empfohlen).	Fügen Sie den folgenden Eintrag in der Datei /etc/modprobe.d/blacklist.conf hinzu: `blacklist i40evf`. Verwenden Sie die i40e-Treiberversion 2.0.26 (empfohlen).

Aufgabe	Intel 82599 NIC	Intel X710-, XL710- und X722-Netzwerkkarten
4.Aktivieren Sie virtuelle SR-IOV-Funktionen (VFs) auf dem KVM-Host. In beiden Befehlen in den nächsten beiden Spalten: `number_of_VFs` = die Anzahl der virtuellen VFs, die Sie erstellen möchten. `device_name` = der Name der Schnittstelle.	Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/ixgbe den folgenden Eintrag hinzu und starten Sie den KVM-Host neu: `options ixgbe max_vfs =<number_of_VFs>` Wenn Sie Kernel 3.8 Version oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo < number_of_VFs> > /sys/class/net/<device_name >/device/sriov_numvfs`. Siehe Beispiel in Abbildung 1.	Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/i40e.conf den folgenden Eintrag hinzu und starten Sie den KVM-Host neu:. `options i40e max_vfs=< number_of_VFs>` Wenn Sie Kernel 3.8 Version oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo<number_of_VFs> > /sys/class/net/< device_name>/device/ sriov_numvfs`. Siehe Beispiel in Abbildung 2.
5. Machen Sie die VFs persistent, indem Sie die Befehle, die Sie zum Erstellen von VFs verwendet haben, zur Datei rc.local hinzufügen.	Siehe Beispiel in Abbildung 3.	Siehe Beispiel in Abbildung 3.

> **Wichtig**
>
> Stellen Sie beim Erstellen der SR-IOV-VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

Abbildung 1: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für die Intel 82599 10G-NIC.

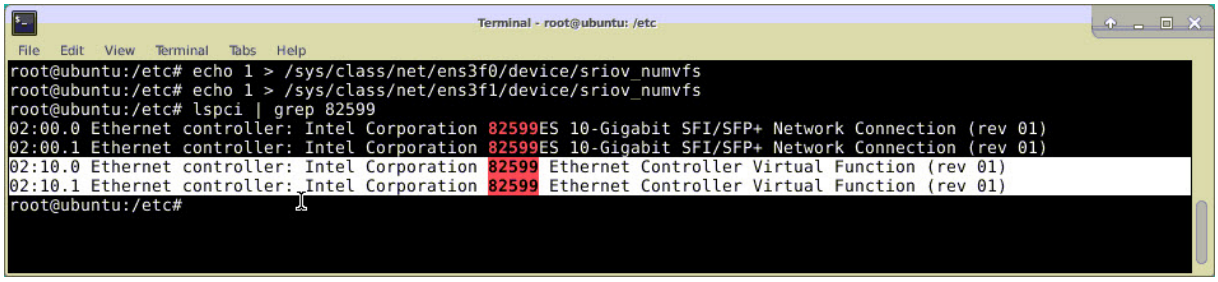


Abbildung 2: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für Intel X710 10G- und XL710 40G-NICs.

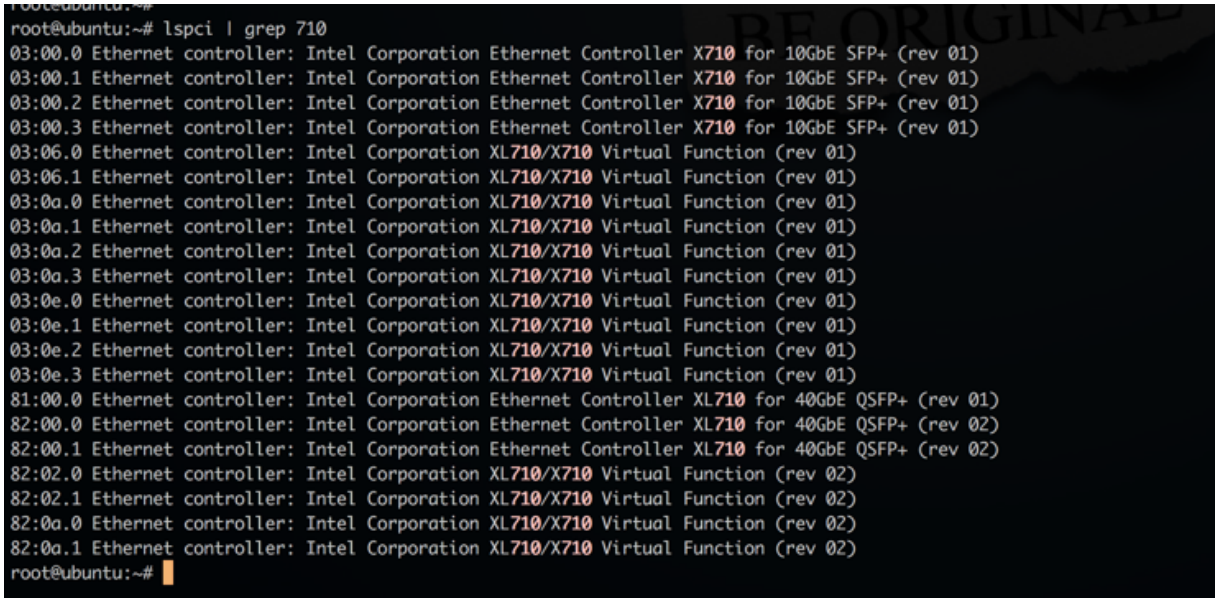


Abbildung 3: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für die Intel X722 10G-NIC.

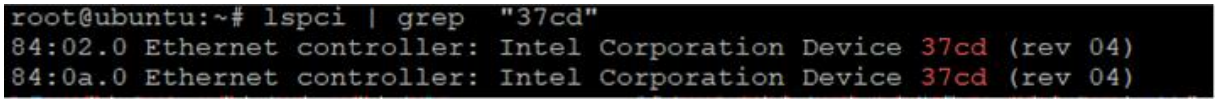
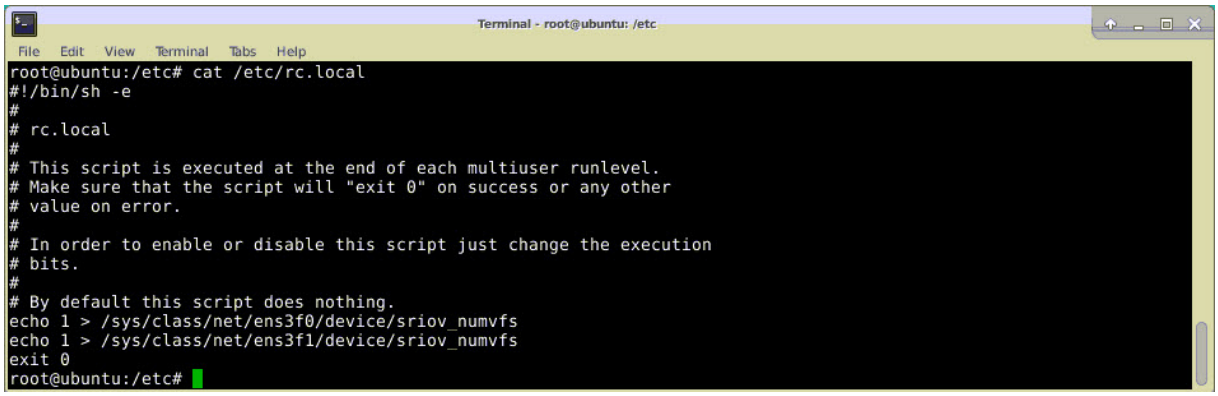


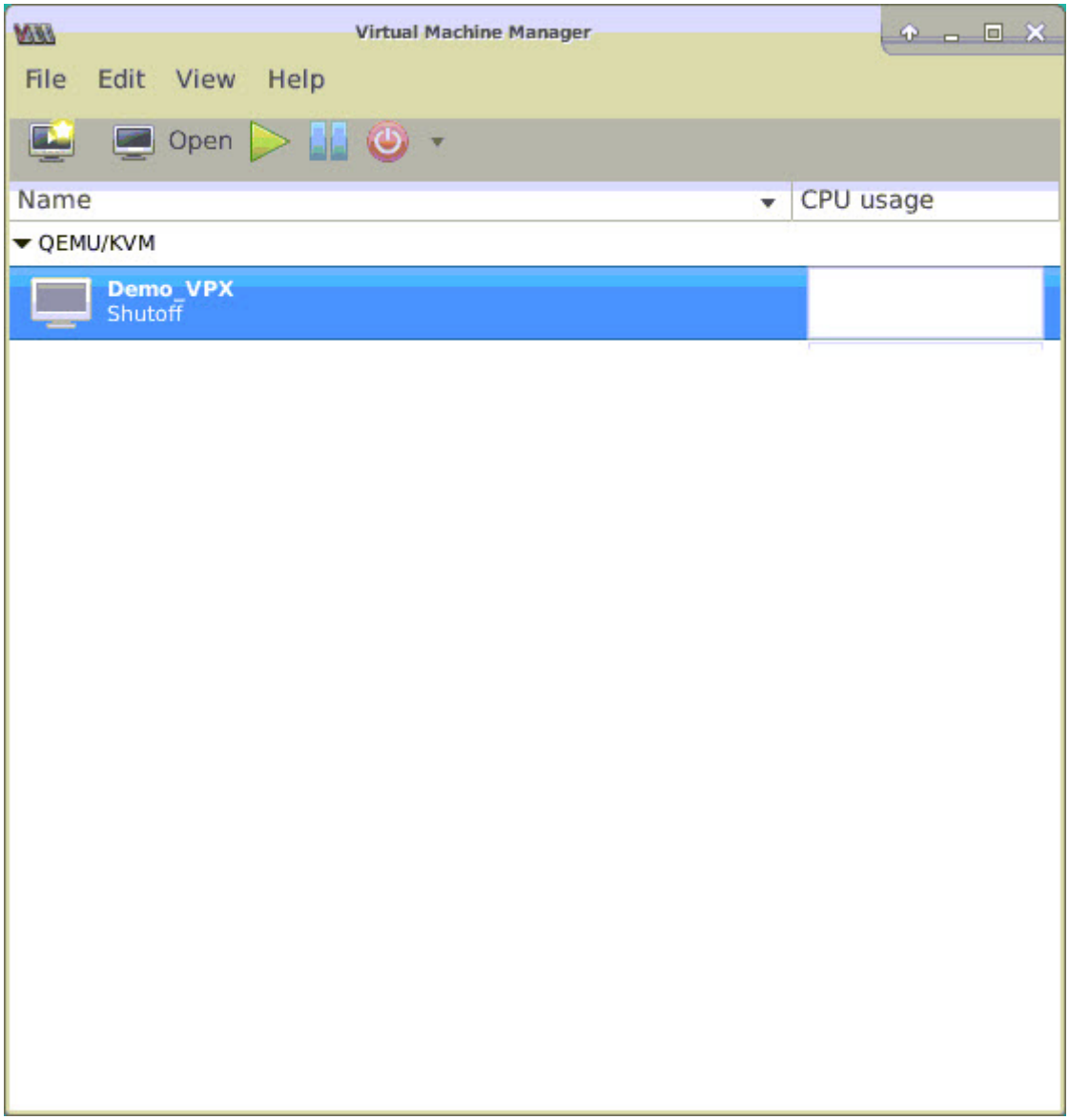
Abbildung 4: Machen Sie die VFs persistent.



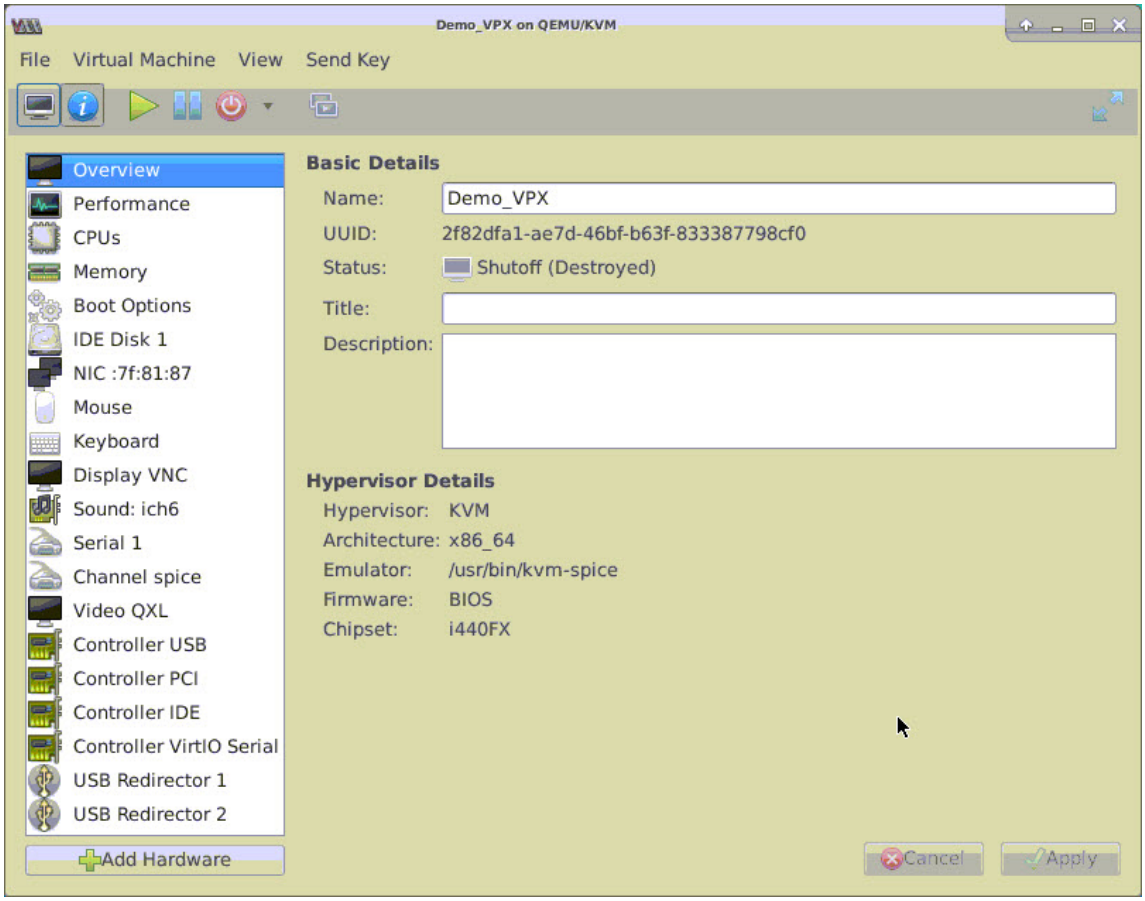
Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

Führen Sie die folgenden Schritte aus, um die NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle mit Virtual Machine Manager zu konfigurieren:

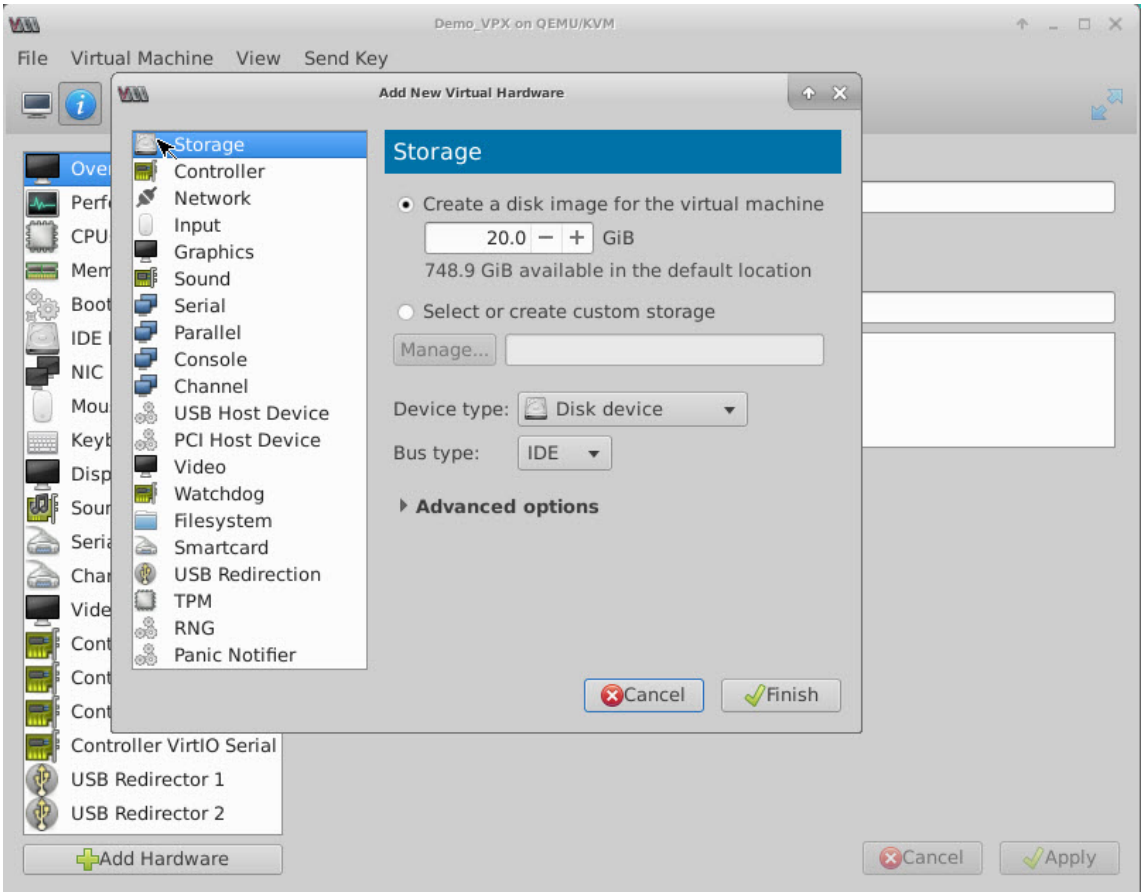
1. Schalten Sie die NetScaler VPX-Instanz aus.
2. Wählen Sie die NetScaler VPX-Instanz und dann Öffnen aus.



3. <virtual machine on KVM>Wählen Sie im Fenster das **I-Symbol** aus.



4. Wählen Sie **Hardware hinzufügen**aus.



5. Führen **Sie im Dialogfeld Neue virtuelle Hardware hinzufügen** die folgenden Schritte aus:

   a) Wählen Sie PCI-Host-Gerät aus.
   b) Wählen Sie im Abschnitt Host-Gerät das VF aus, das Sie erstellt haben, und klicken Sie auf Fertig stellen.

Abbildung 4: VF für Intel 82599 10G-NIC

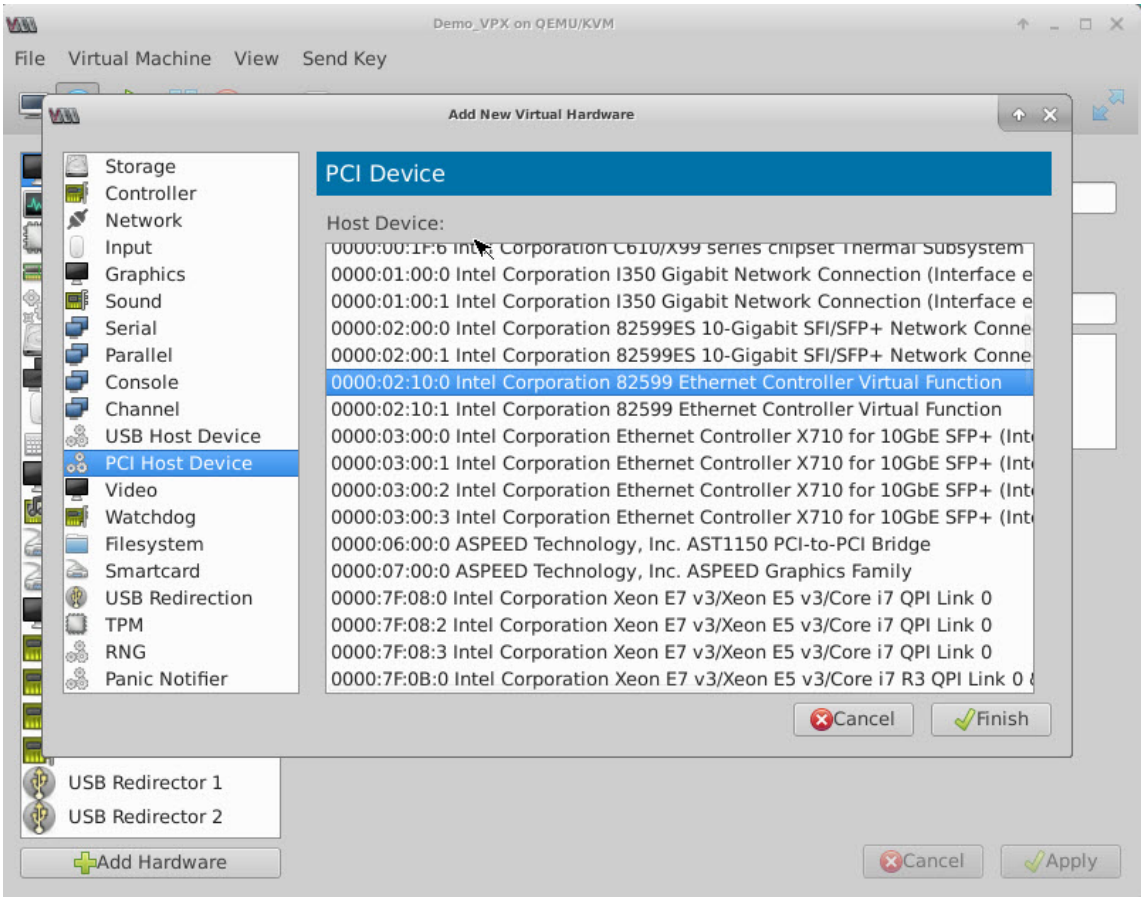


Abbildung 5: VF für Intel XL710 40G NIC

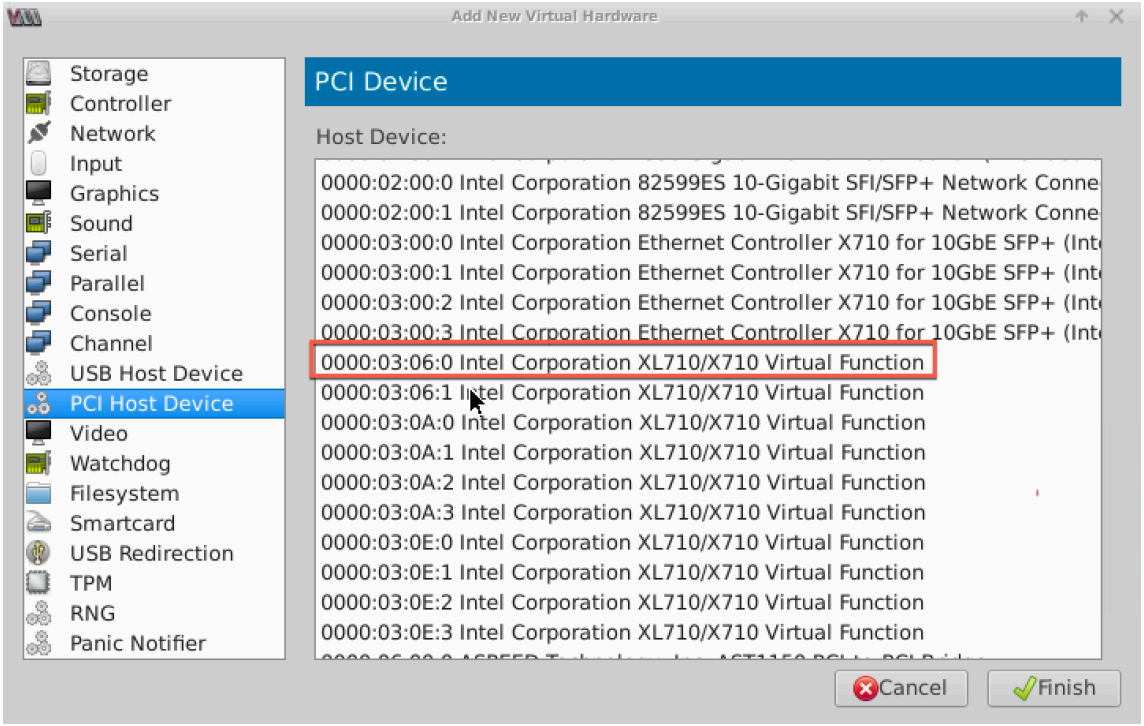
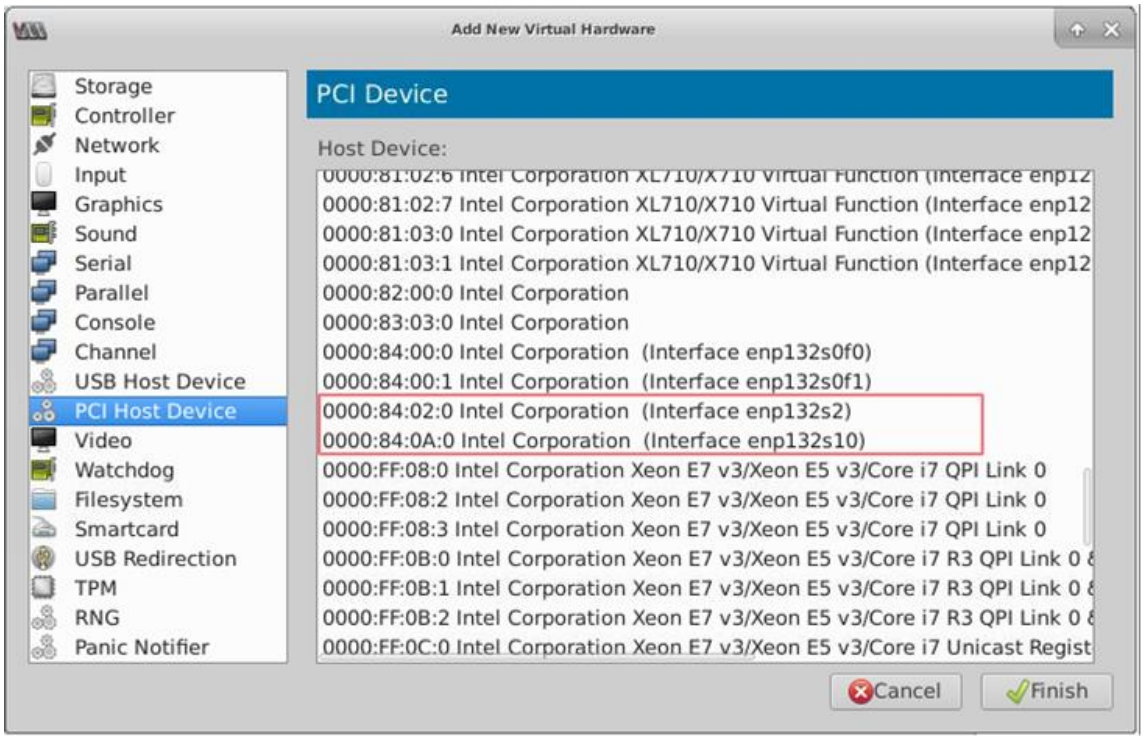


Abbildung 6: VF für Intel X722 10G-NIC



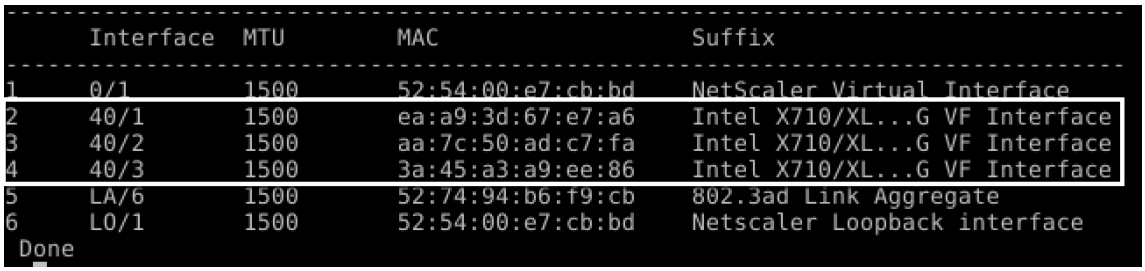
6. Wiederholen Sie die Schritte 4 und 5, um die von Ihnen erstellten VFs hinzuzufügen.
7. Schalten Sie die NetScaler VPX-Instanz ein.
8. Verwenden Sie nach dem Einschalten der NetScaler VPX-Instanz den folgenden Befehl, um die Konfiguration zu überprüfen:

```
show interface summary
<!--NeedCopy-->
```

Die Ausgabe zeigt alle Schnittstellen, die Sie konfiguriert haben.

Abbildung 6: Zusammenfassung der Ausgabe für Intel 82599 NIC.

Abbildung 7. Zusammenfassung der Ausgangsdaten für Intel X710- und XL710-NICs.



Konfigurieren Sie statisches LA/LACP auf der SR-IOV-Schnittstelle

> **Wichtig**
>
> Stellen Sie beim Erstellen der SR-IOV-VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

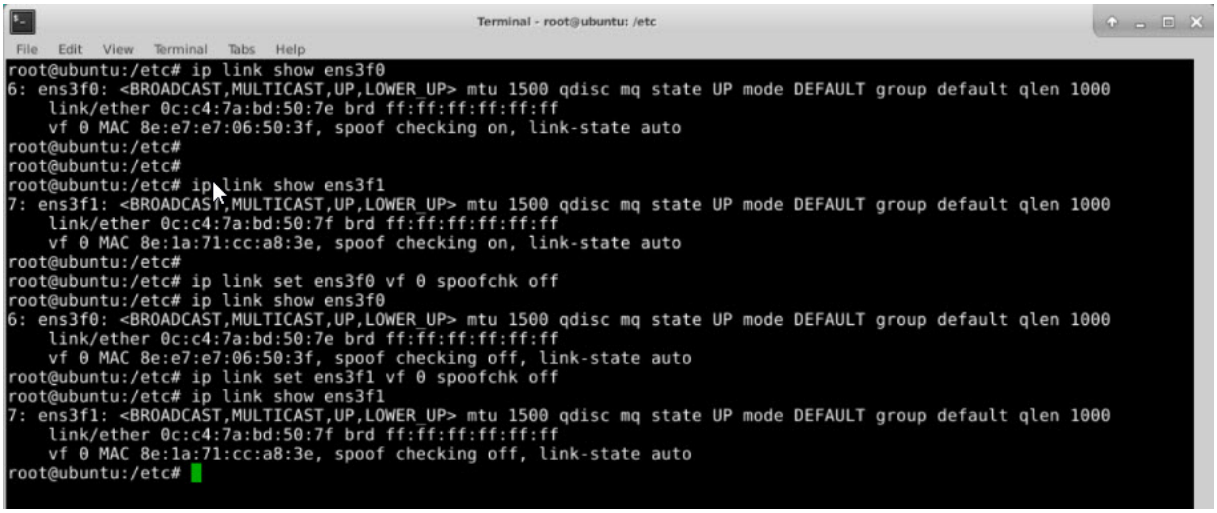
Um die SR-IOV-VFs im Link-Aggregationsmodus zu verwenden, deaktivieren Sie die Spoof-Prüfung für von Ihnen erstellte VFs. Verwenden Sie auf dem KVM-Host den folgenden Befehl, um die Spoof-Prüfung zu deaktivieren:

```
*ip link set \<interface\\_name\> vf \<VF\\_id\> spoofchk off*
```

Es gilt:

- interface_name — ist der Schnittstellenname.
- vf_ID — ist die virtuelle Funktions-ID.

Beispiel:



Nachdem Sie die Spoof-Prüfung für alle von Ihnen erstellten VFs deaktiviert haben. Starten Sie die NetScaler VPX-Instanz neu, und konfigurieren Sie die Linkaggregation. Ausführliche Anweisungen finden Sie unter Konfigurieren der Link-Aggregation.

Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

Sie können VLAN auf SR-IOV-VFs konfigurieren. Ausführliche Anweisungen finden Sie unter Konfigurieren eines VLANs.

> **Wichtig**
>
> Stellen Sie sicher, dass der KVM-Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen

May 11, 2023

Nachdem Sie eine NetScaler VPX-Instanz auf der Linux-KVM-Plattform installiert und konfiguriert haben, können Sie den Virtual Machine Manager verwenden, um die virtuelle Appliance für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

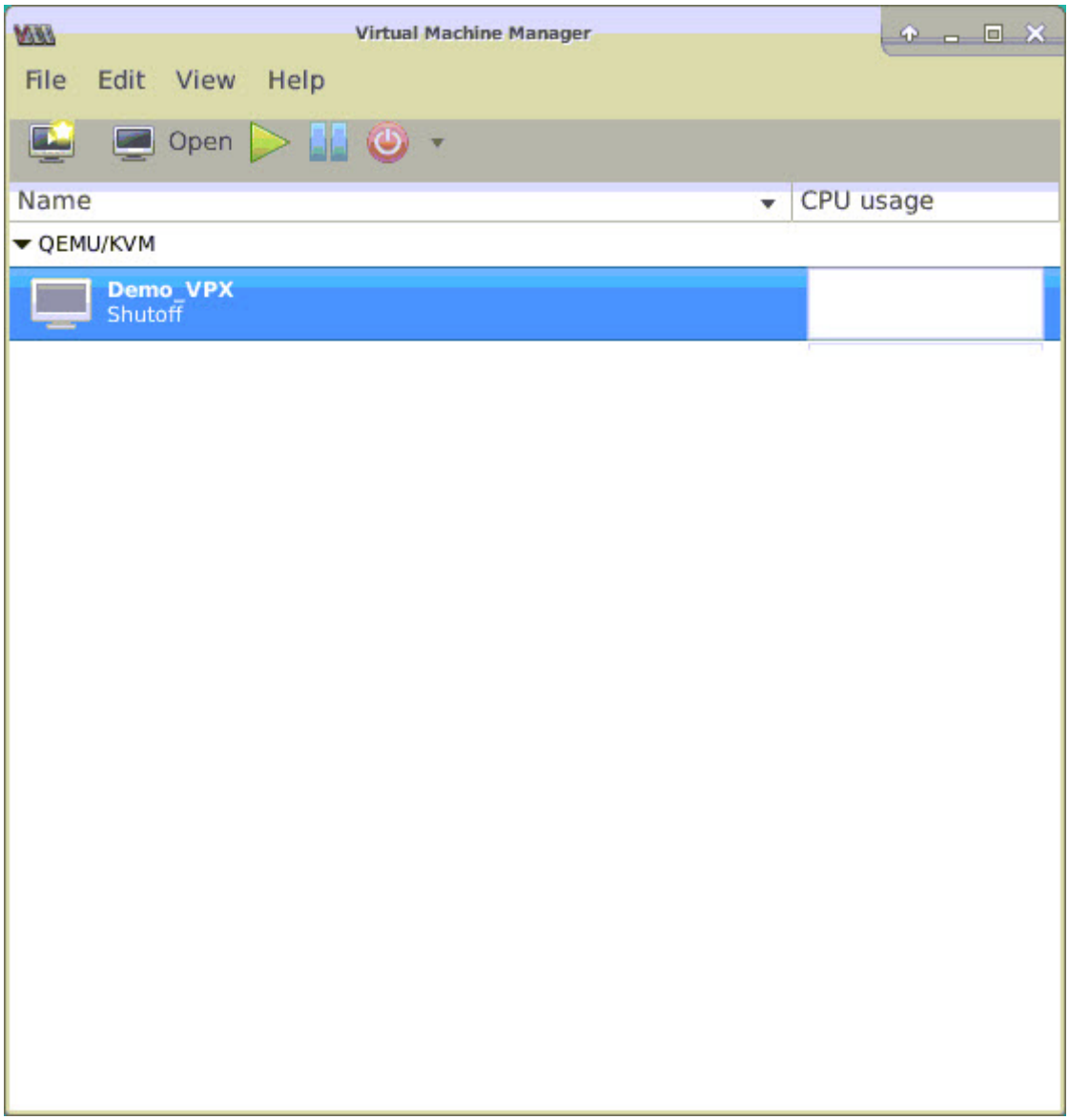
Voraussetzungen

- Die Firmware-Version der Intel XL710-NIC (NIC) auf dem KVM-Host ist 5.04.
- Der KVM-Host unterstützt Eingabe-Output-Speicherverwaltungseinheit (IOMMU) und Intel VT-d und ist im BIOS des KVM-Hosts aktiviert. Fügen Sie auf dem KVM-Host den folgenden Eintrag zur Datei **/boot/grub2/grub.cfg** hinzu, um IOMMU zu aktivieren:**intel_iommu=1**

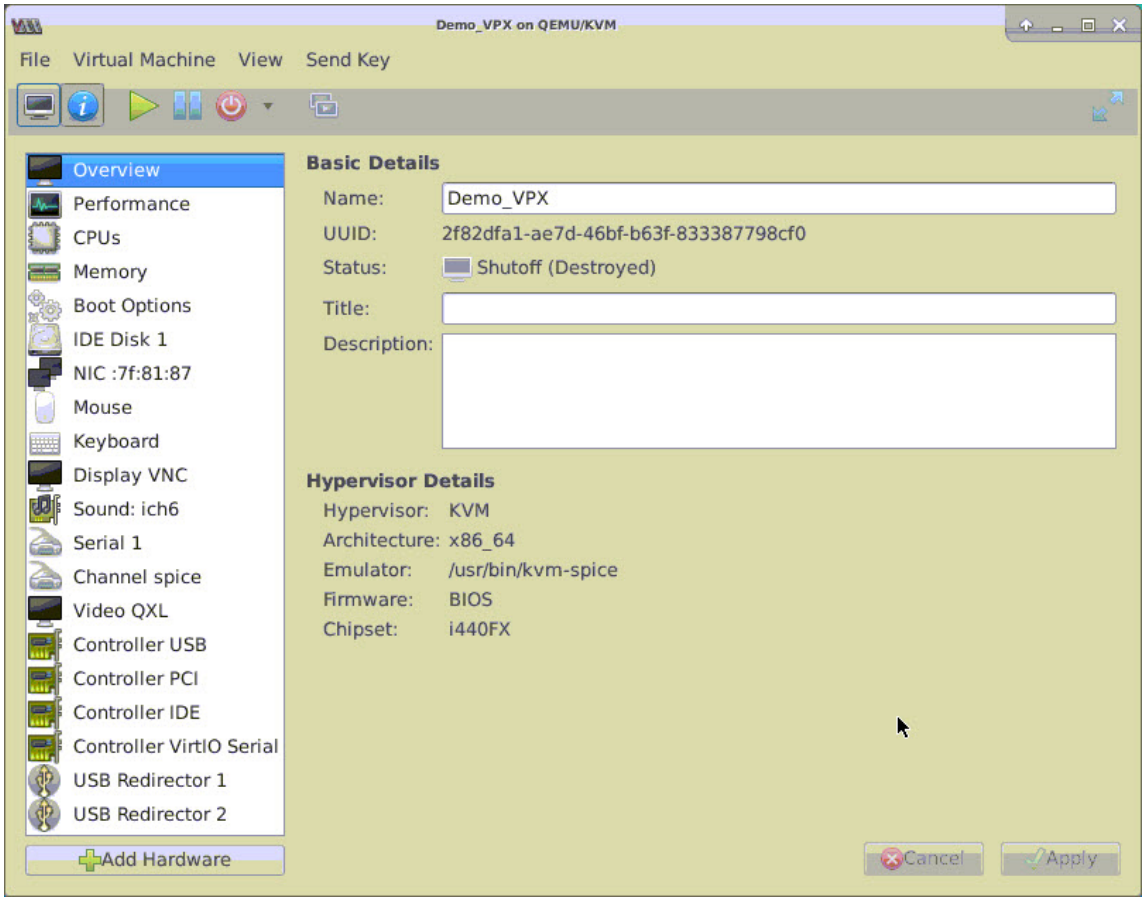
- Führen Sie den folgenden Befehl aus und starten Sie den KVM-Host neu: **Grub2-mkConfig —o /boot/grub2/grub.cfg**

So konfigurieren Sie NetScaler VPX-Instanzen für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen mithilfe des Virtual Machine Manager:

1. Schalten Sie die NetScaler VPX-Instanz aus.
2. Wählen Sie die NetScaler VPX-Instanz aus, und klicken Sie auf **Öffnen**.



3. Klicken Sie im Fenster **virtual_machine im KVM** -Fenster auf das **I-Symbol** .

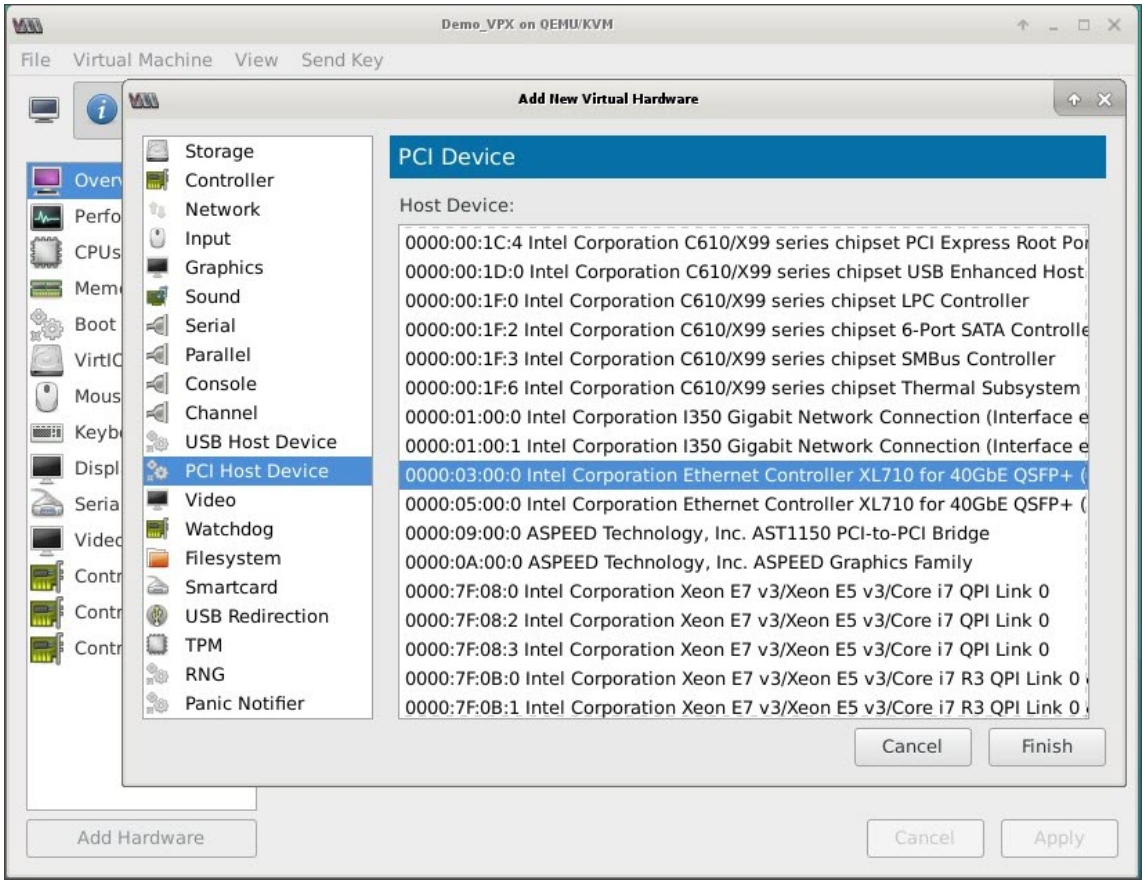


4. Klicken Sie auf **Hardware hinzufügen**.
5. Führen **Sie im Dialogfeld Neue virtuelle Hardware hinzufügen** die folgenden Schritte aus:

   a. Wählen Sie **PCI-Host-Gerät**aus.

   b. Wählen Sie im Bereich **Host-Gerät** die physische Funktion Intel XL710 aus.

   c. Klicken Sie auf **Fertig stellen**.

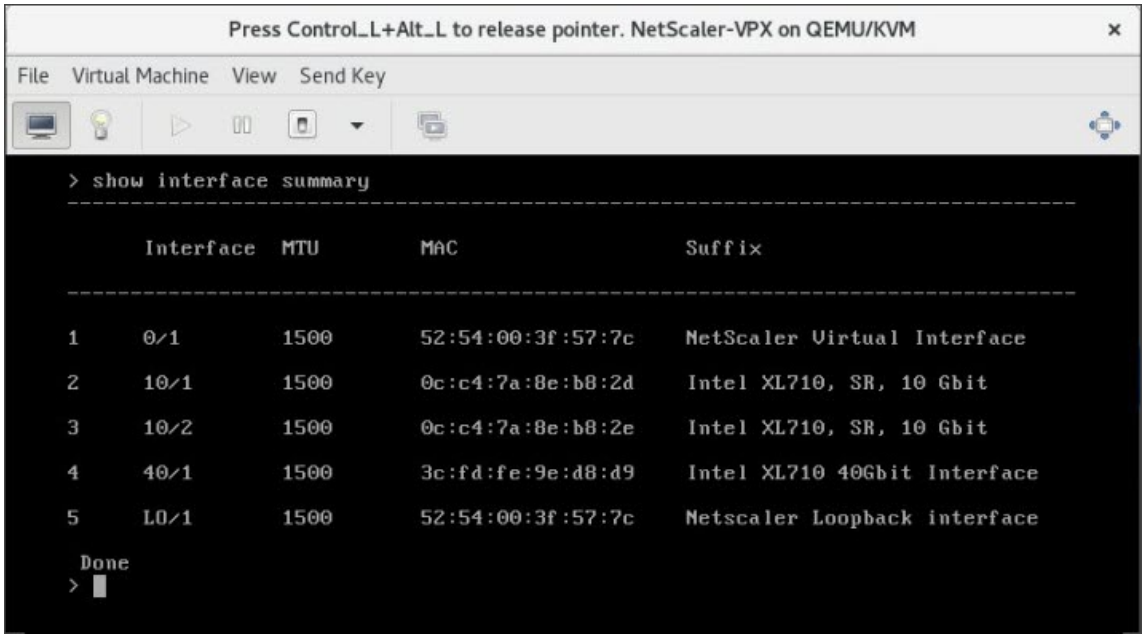


6. Wiederholen Sie die Schritte **4** und **5**, um zusätzliche physische Funktionen des Intel XL710 hinzuzufügen.
7. Schalten Sie die NetScaler VPX-Instanz ein.
8. Sobald die NetScaler VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

```
COMMAND

> show interface summary
```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:



Stellen Sie die NetScaler VPX-Instanz mithilfe des virsh Programms bereit

May 11, 2023

Das `virsh` Programm ist ein Befehlszeilentool zur Verwaltung von VM-Gästen. Seine Funktionalität ähnelt der von Virtual Machine Manager. Es ermöglicht Ihnen, den Status eines VM-Gastes (Start, Stopp, Pause usw.) zu ändern, neue Gäste und Geräte einzurichten und vorhandene Konfigurationen zu bearbeiten. Das `virsh` Programm ist auch nützlich für das Skripten von VM-Gastverwaltungsvorgängen.

Gehen Sie folgendermaßen vor, um NetScaler VPX mithilfe des `virsh` Programms bereitzustellen:

1. Verwenden Sie den Befehl tar, um das NetScaler VPX-Paket aufzuheben. Das Paket NSVPX-KVM-*_nc.tgz enthält die folgenden Komponenten:

   - Die Domänen-XML-Datei mit VPX-Attributen [NSVPX-KVM-*_nc.xml]
   - Prüfen Sie die Summe des NS-VM-Datenträgerimages [CheckSum.txt]
   - NS-VM-Festplattenabbild [NSVPX-KVM-*_NC.raw]

   Beispiel:

   ```
   tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
   NSVPX-KVM-10.1-117_nc.xml
   NSVPX-KVM-10.1-117_nc.raw
   checksum.txt
   ```



```
<!--NeedCopy-->
```

2. Kopieren Sie die XML-Datei NSVPX-KVM-*_nc.xml in eine Datei mit dem Namen <DomainName>-NSVPX-KVM-*_nc.xml. <DomainName> ist auch der Name der virtuellen Maschine. Beispiel:

```
cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.xml
<!--NeedCopy-->
```

3. Bearbeiten Sie die Datei <DomainName>-NSVPX-KVM-*_nc.xml, um die folgenden Parameter anzugeben:

   - name— Geben Sie den Namen an.
   - Mac - Geben Sie die MAC-Adresse an.
     Hinweis: Der Domänenname und die MAC-Adresse müssen eindeutig sein.
   - Quelldatei - Geben Sie den absoluten Quellpfad für das Datenträgerimage an. Der Dateipfad muss absolut sein. Sie können den Pfad der RAW-Bilddatei oder einer QCOW2-Bilddatei angeben.

     Wenn Sie eine RAW-Image-Datei angeben möchten, geben Sie den Pfad der Datenträgerimagequelle an, wie im folgenden Beispiel gezeigt:

     Beispiel:

     ```
     <name>NetScaler-VPX</name>
     <mac address='52:54:00:29:74:b3'/>
     <source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
     <!--NeedCopy-->
     ```

     Geben Sie den absoluten QCOW2-Datenträgerimagequellpfad an, und definieren Sie den Treibertyp als **qcow2**, wie im folgenden Beispiel gezeigt:

     Beispiel:

     ```
     <name>NetScaler-VPX</name>
     <mac address='52:54:00:29:74:b3'/>
     <driver name ='qemu' type='qcow2'/>
     <source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
     <!--NeedCopy-->
     ```

4. Bearbeiten Sie die Datei <DomainName>-NSVPX-KVM-*_nc.xml, um die Netzwerkdetails zu konfigurieren:

   - source dev — gibt die Schnittstelle an.
   - Modus — gibt den Modus an. Die Standardschnittstelle ist **Macvtap Bridge**.

Beispiel: Modus: MacVTap Bridge Setzen Sie Zielschnittstelle als `ethx` und Modus als Bridge-Modelltyp als `virtio`

```
  <interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth0' mode='bridge'/>
      <target dev='macvtap0'/>
      <model type='virtio'/>
      <alias name='net0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
         function='0x0'/>
    </interface>
<!--NeedCopy-->
```

Hier ist eth0 die physische Schnittstelle, die an die VM angeschlossen ist.

5. Definieren Sie die VM-Attribute in der Datei <DomainName>-NSVPX-KVM-*_nc.xml, indem Sie den folgenden Befehl verwenden: define `virsh` define <DomainName>-NSVPX-KVM-*_nc.xml Beispiel:

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
<!--NeedCopy-->
```

6. Starten Sie die VM, indem Sie den folgenden Befehl eingeben: `virsh` start [<DomainName> | <DomainUUID>] Beispiel:

```
virsh start NetScaler-VPX
<!--NeedCopy-->
```

7. Verbinden Sie die Gast-VM über die Konsole `virsh` console [<DomainName> | <DomainUUID> |<DomainID>] Beispiel:

```
virsh console NetScaler-VPX
<!--NeedCopy-->
```

Fügen Sie NetScaler VPX-Instanz mithilfe `virsh` des Programms weitere Schnittstellen hinzu

Nachdem Sie NetScaler VPX auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

Gehen Sie folgendermaßen vor, um weitere Schnittstellen hinzuzufügen:

1. Fahren Sie die NetScaler VPX-Instanz herunter, die auf der KVM ausgeführt wird.

2. Bearbeiten Sie die Datei <DomainName>-NSVPX-KVM-*_nc.xml mit folgendem Befehl: `virsh edit [<DomainName> | <DomainUUID>]`
3. Fügen Sie in der Datei <DomainName>-NSVPX-KVM-*_nc.xml die folgenden Parameter an:

   a) **Für MacVTAP**

   - Schnittstellentyp — Geben Sie den Schnittstellentyp als ‘direct’ an.
   - MAC-Adresse— Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über die Schnittstellen eindeutig ist.
   - source dev— Geben Sie den Schnittstellennamen an.
   - mode - Geben Sie den Modus an. Die unterstützten Modi sind Bridge, VEPA, Private und Pass-Through
   - Modelltyp— Geben Sie den Modelltyp an als `virtio`

   Beispiel:

   Modus: MacVTap Pass-Through

   Setzen Sie die Zielschnittstelle als
   `ethx`, Modus als
   Bridge und Modelltyp als
   `virtio`

   ```
   <interface type='direct'>
         <mac address='52:54:00:29:74:b3'/>
         <source dev='eth1' mode='passthrough'/>
         <model type='virtio'/>
    </interface>
   <!--NeedCopy-->
   ```

   Hier eth1 ist die physische Schnittstelle, die an die VM angeschlossen ist.

   b) **Für den Bridge-Modus**

   Hinweis: Stellen Sie sicher, dass Sie eine Linux-Bridge auf dem KVM-Host konfiguriert, die physische Schnittstelle an die Bridge gebunden und die Bridge in den Status UP versetzt haben.

   - Schnittstellentyp — Geben Sie den Schnittstellentyp als ‘Bridge’ an.
   - MAC-Adresse— Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über die Schnittstellen eindeutig ist.
   - Quellbrücke — Geben Sie den Bridge-Namen an.
   - Modelltyp— Geben Sie den Modelltyp an als `virtio`

   Beispiel: Bridge-Modus

   ```
   <interface type='bridge'>
   ```



```
        <mac address='52:54:00:2d:43:a4'/>
        <source bridge='br0'/>
        <model type='virtio'/>
    </interface>
<!--NeedCopy-->
```

Verwalten der NetScaler VPX Gast-VMs

May 11, 2023

Sie können den Virtual Machine Manager und das `virsh` Programm verwenden, um Verwaltungsaufgaben wie das Starten oder Stoppen eines VM-Gastes, das Einrichten neuer Gäste und Geräte, das Bearbeiten vorhandener Konfigurationen und die Verbindung mit der grafischen Konsole über Virtual Network Computing (VNC) auszuführen.

Verwalten der VPX-Gast-VMs mithilfe von Virtual Machine Manager

- Liste der VM-Gäste

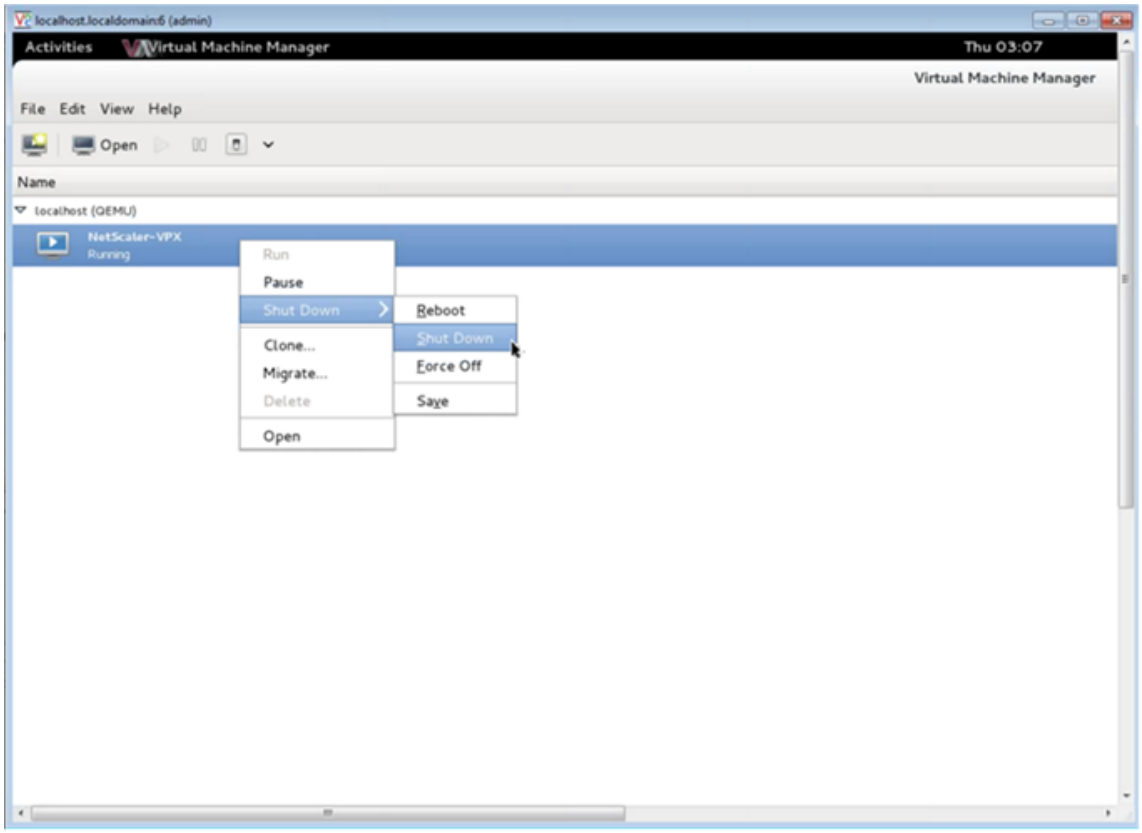
  Im Hauptfenster des Virtual Machine Manager wird eine Liste aller VM-Gäste für jeden VM-Hostserver angezeigt, mit dem er verbunden ist. Jeder VM-Gasteintrag enthält den Namen der virtuellen Maschine zusammen mit seinem Status (Ausführen, Pausiert oder Shutoff), der wie im Symbol angezeigt wird.

- Öffnen einer grafischen Konsole

  Wenn Sie einem VM-Gast eine grafische Konsole öffnen, können Sie mit dem Computer wie mit einem physischen Host über eine VNC-Verbindung interagieren. Um die grafische Konsole im Virtual Machine Manager zu öffnen, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie im Popup-Menü die Option Öffnen.

- Einen Gast starten und herunterfahren

  Sie können einen VM-Gast vom Virtual Machine Manager aus starten oder beenden. Um den Status der VM zu ändern, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie Ausführen oder eine der Optionen zum Herunterfahren aus dem Popupmenü.



- Einen Gast neu starten

  Sie können einen VM-Gast über den Virtual Machine Manager neu starten. Um die VM neu zu starten, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie dann im Popupmenü die Option Herunterfahren > Neustarten aus.

- Löschen eines Gastes

  Beim Löschen eines VM-Gastes wird standardmäßig dessen XML-Konfiguration entfernt. Sie können auch die Speicherdateien eines Gastes löschen. Dadurch wird der Gast vollständig gelöscht.

  1. Klicken Sie im Virtual Machine Manager mit der rechten Maustaste auf den VM-Gasteintrag.
  2. Wählen Sie im Popup-Menü die Option Löschen aus. Ein Bestätigungsfenster öffnet sich. Hinweis: Die Option Löschen ist nur aktiviert, wenn der VM-Gast heruntergefahren ist.
  3. Klicken Sie auf Löschen.
  4. Um den Gast vollständig zu löschen, löschen Sie die zugehörige RAW-Datei, indem Sie das Kontrollkästchen Zugehörige Speicherdateien löschen aktivieren.

Verwalten Sie die NetScaler VPX-Gast-VMs mit dem `virsh` Programm

- Listen Sie die VM-Gäste und ihre aktuellen Status auf.

So zeigen `virsh` Sie Informationen über die Gäste an

```
virsh list --all
```

Die Befehlsausgabe zeigt alle Domänen mit ihrem Status an. Beispiel-Ausgabe:

```
1  Id Name                 State
2  ----------------------------------
3    0 Domain-0            running
4    1 Domain-1            paused
5    2 Domain-2            inactive
6    3 Domain-3            crashed
7  <!--NeedCopy-->
```

- Öffne eine `virsh` Konsole.

  Verbinden der Gast-VM über die Konsole

  ```
  virsh console [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh console NetScaler-VPX
  ```

- Startet und schaltet einen Gast aus.

  Gäste können mit dem DomainNamen oder der Domain-UUID gestartet werden.

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh start NetScaler-VPX
  ```

  Um einen Gast herunterzufahren:

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh shutdown NetScaler-VPX
  ```

- Einen Gast neu starten

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh reboot NetScaler-VPX
  ```

  Löschen eines Gastes

  Um eine Gast-VM zu löschen, müssen Sie die Gast-VM herunterfahren und die Definition von <DomainName>-NSVPX-KVM-*_nc.xml aufheben, bevor Sie den Löschbefehl ausführen.


```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
<!--NeedCopy-->
```

Beispiel:

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
<!--NeedCopy-->
```

> Hinweis: Der Befehl delete entfernt keine Datenträgerimage-Datei, die manuell entfernt werden muss.

Stellen Sie die NetScaler VPX-Instanz mit SR-IOV auf OpenStack bereit

May 11, 2023

Sie können leistungsstarke NetScaler VPX-Instances auf OpenStack bereitstellen, die die Single-Root-I/O-Virtualisierungstechnologie (SR-IOV) verwenden.

Sie können eine NetScaler VPX-Instanz, die die SR-IOV-Technologie verwendet, auf OpenStack in drei Schritten bereitstellen:

- Aktivieren Sie virtuelle SR-IOV-Funktionen (VFs) auf dem Host.
- Konfigurieren Sie die vFS und stellen Sie sie OpenStack zur Verfügung.
- Stellen Sie den NetScaler VPX auf OpenStack bereit.

Voraussetzungen

Stellen Sie sicher, dass Sie:

- Fügen Sie die Intel 82599 NIC (NIC) zum Host hinzu.
- Laden Sie den neuesten IXGBE Treiber von Intel herunter und installieren Sie ihn.
- Blockieren Sie den IXGBEVF-Treiber auf dem Host auf. Fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/blacklist.conf hinzu: Sperrliste `ixgbevf`

> **Hinweis**
>
> Die `ixgbe` Treiberversion muss mindestens 5.0.4 sein.

Aktivieren von SR-IOV-VFs auf dem Host

Führen Sie einen der folgenden Schritte aus, um SR-IOV-VFs zu aktivieren:

- Wenn Sie eine ältere Kernelversion als 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/ixgbe den folgenden Eintrag hinzu und starten Sie den Host neu: options ixgbe max_vfs= <number_of_VFs>
- Wenn Sie die Kernel-Version 3.8 oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl:

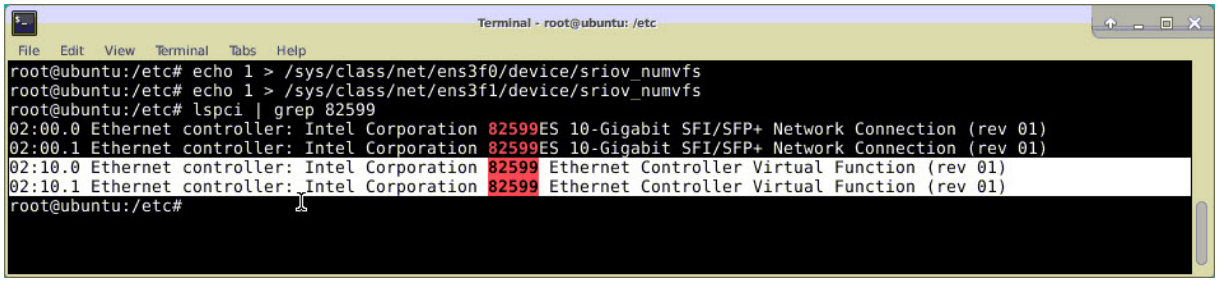
```
1     echo <number_of_VFs> > /sys/class/net/<device_name>/device/
         sriov_numvfs
2 <!--NeedCopy-->
```

Es gilt:

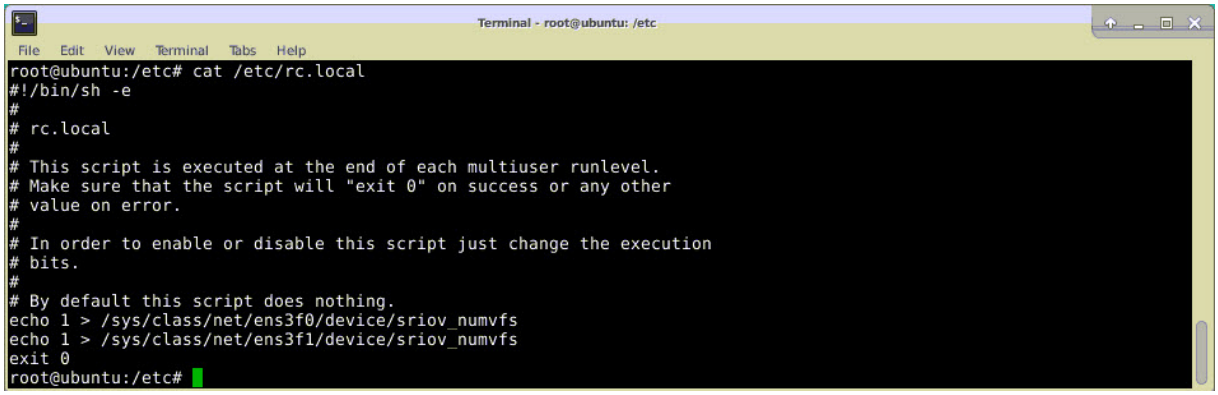
- Number_of_VFS ist die Anzahl der virtuellen Funktionen, die Sie erstellen möchten.
- device_name ist der Schnittstellenname.

> **Wichtig**
>
> Achten Sie beim Erstellen der SR-IOV-VFs darauf, dass Sie den VFs keine MAC-Adressen zuweisen.

Hier ist ein Beispiel für vier VFs, die erstellt werden.



Machen Sie die VFs persistent, fügen Sie die Befehle, die Sie zum Erstellen von VFs verwendet haben, zur Datei **rc.local** hinzu. Hier ist ein Beispiel, das den Inhalt der rc.local-Datei zeigt.



Weitere Informationen finden Sie in diesem Intel SR-IOV-Konfigurationshandbuch.

Konfigurieren und stellen Sie die VFs für OpenStack zur Verfügung

Folgen Sie den Schritten unter dem folgenden Link, um SR-IOV auf OpenStack zu konfigurieren:. https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking

Bereitstellen der NetScaler VPX Instanz auf OpenStack

Sie können eine NetScaler VPX-Instanz in einer OpenStack-Umgebung bereitstellen, indem Sie die OpenStack-CLI verwenden.

Das Provisioning einer VPX-Instanz umfasst optional die Verwendung von Daten aus dem Konfigurationslaufwerk. Das Konfigurationslaufwerk ist ein spezielles Konfigurationslaufwerk, das beim Booten an die Instanz anhängt. Dieses Konfigurationslaufwerk kann verwendet werden, um Netzwerkkonfigurationsinformationen wie Management-IP-Adresse, Netzwerkmaske und Standardgateway usw. an die Instanz zu übergeben, bevor Sie die Netzwerkeinstellungen für die Instanz konfigurieren.

Wenn OpenStack eine VPX-Instanz zur Verfügung stellt, erkennt sie zuerst, dass die Instanz in einer OpenStack-Umgebung gestartet wird, indem sie eine bestimmte BIOS-Zeichenfolge (OpenStack Foundation) liest, die OpenStack angibt. Für Red Hat Linux-Distributionen wird die Zeichenfolge in /etc/nova/release gespeichert. Dies ist ein Standardmechanismus, der in allen OpenStack-Implementierungen verfügbar ist, die auf der KVM-Hypervisor-Plattform basieren. Das Laufwerk muss ein bestimmtes OpenStack-Label haben. Wenn das Konfigurationslaufwerk erkannt wird, versucht die Instanz, die folgenden Informationen aus dem im `nova` Boot-Befehl angegebenen Dateinamen zu lesen. In den folgenden Verfahren heißt die Datei userdata.txt.

- Verwaltungs-IP-Adresse
- Netzwerkmaske
- Standard-Gateway

Sobald die Parameter erfolgreich gelesen wurden, werden sie in den NetScaler-Stack gefüllt. Dies hilft bei der Remote-Verwaltung der Instanz. Wenn die Parameter nicht erfolgreich gelesen werden oder das Konfigurationslaufwerk nicht verfügbar ist, wechselt die Instanz zum Standardverhalten, das wie folgt lautet:

- Die Instanz versucht, die IP-Adressinformationen von DHCP abzurufen.
- Wenn DHCP ausfällt oder ein Timeout auftritt, erstellt die Instance die Standard-Netzwerkkonfiguration (192.168.100.1/16).

Stellen Sie die NetScaler VPX-Instanz auf OpenStack über CLI bereit

Sie können eine VPX-Instanz in einer OpenStack-Umgebung mithilfe der OpenStack-CLI bereitstellen. Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen einer NetScaler VPX-Instanz auf OpenStack:

1. Extrahieren der `.qcow2` Datei aus der TGZ-Datei
2. Erstellen eines OpenStack-Images aus dem qcow2-Image
3. Provisioning einer VPX-Instanz

Führen Sie die folgenden Schritte aus, um eine VPX-Instanz in einer OpenStack-Umgebung bereitzustellen.

1. Extrahiere das. `qcow2` Datei aus der `.tqz` Datei, indem Sie den Befehl eingeben:

```
tar xvzf <TAR file>
tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

2. Erstellen Sie ein OpenStack-Image mit der in Schritt 1 extrahierten `.qcoz2` Datei, indem Sie den folgenden Befehl eingeben:

```
glance image-create --name="<name of the OpenStack image>" --
    property hw_disk_bus=ide --is-public=true --container-format=
    bare --disk-format=qcow2< <name of the qcow2 file>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --is-public= true --container-format=bare --
    disk-format=qcow2< NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

   Die folgende Abbildung enthält eine Beispielausgabe für den Befehl glance image-create.

Property	Value
checksum	735dae4ea6e46e39ed3f0acfba02e755
container_format	bare
created_at	2017-02-16T10:03:29Z
disk_format	qcow2
hw_disk_bus	ide
id	aeaa13e9-b49b-411c-ab54-c61820a8e2f3
min_disk	0
min_ram	0
name	NSVPX-KVM-12.0-26.2
owner	06c41a73b32f4b48af55359fd7d3502c
protected	False
size	717946880
status	active
tags	[]
updated_at	2017-02-16T10:03:38Z
virtual_size	None
visibility	private

3. Nachdem ein OpenStack-Image erstellt wurde, stellen Sie die NetScaler VPX-Instanz bereit.

```
nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true --
   userdata
./userdata.txt --flavor m1. medium --nic net-id=3b258725-eaae-
455e-a5de-371d6d1f349f --nic port-id=218ba819-9f55-4991-adb6-
02086a6bdee2 NSVPX-10
<!--NeedCopy-->
```

Im vorherigen Befehl ist userdata.txt die Datei, die Details wie IP-Adresse, Netzmaske und Standardgateway für die VPX-Instanz enthält. Die Benutzerdatendatei ist eine vom Benutzer anpassbare Datei. NSVPX-KVM-12.0-26.2 ist der Name der virtuellen Appliance, die Sie bereitstellen möchten. —NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 ist der OpenStack ss.

Die folgende Abbildung zeigt eine Beispielausgabe des `nova` Boot-Befehls.

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

Die folgende Abbildung zeigt ein Beispiel der Datei userdata.txt. Die Werte innerhalb der Tags <PropertySection></PropertySection> sind die vom Benutzer konfigurierbaren Werte und enthalten Informationen wie IP-Adresse, Netzmaske und Standardgateway.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
   />
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"/>
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
oe:value="openstack-orch-env"/>
<Property oe:key="com.citrix.netscaler.mgmt.ip"
```



```
oe:value="10.1.0.100"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.0.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway"
oe:value="10.1.0.1"/>
</PropertySection>
</Environment>
<!--NeedCopy-->
```

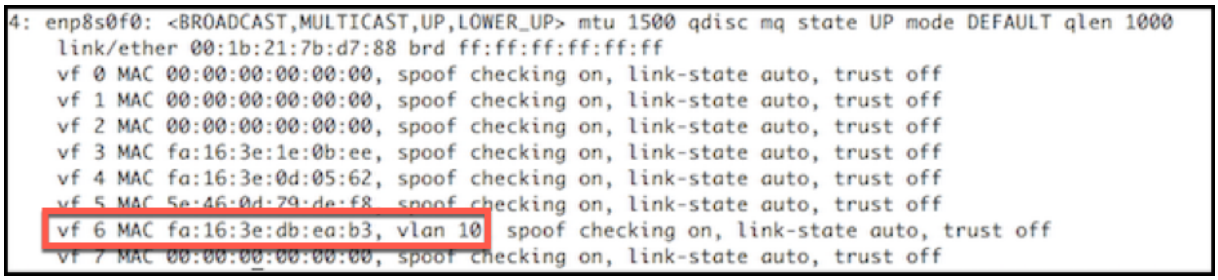
Zusätzliche unterstützte Konfigurationen: Erstellen und Löschen von VLANs auf SR-IOV-VFs vom Host

Geben Sie den folgenden Befehl ein, um ein VLAN auf dem SR-IOV VF zu erstellen:

```
ip link show enp8s0f0 vf 6 vlan 10
```

Im vorherigen Befehl “enp8s0f0” ist der Name der physikalischen Funktion.

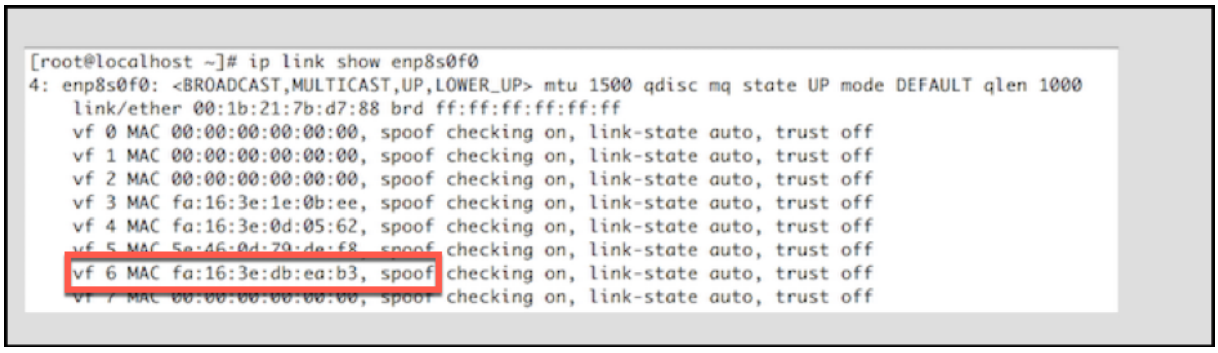
Beispiel: VLAN 10, erstellt auf vf 6



Geben Sie den folgenden Befehl ein, um ein VLAN auf dem SR-IOV VF zu löschen:

```
ip link show enp8s0f0 vf 6 vlan 0
```

Beispiel: VLAN 10, aus vf 6 entfernt



Mit diesen Schritten wird das Verfahren zum Bereitstellen einer NetScaler VPX-Instanz, die die SRIOV-Technologie verwendet, auf OpenStack abgeschlossen.

Konfigurieren Sie eine NetScaler VPX-Instanz auf KVM für die Verwendung von OVS-DPDK-basierten Hostschnittstellen

May 11, 2023

Sie können eine NetScaler VPX-Instanz konfigurieren, die auf KVM (Fedora und RHOS) ausgeführt wird, um Open vSwitch (OVS) mit Data Plane Development Kit (DPDK) für eine bessere Netzwerkleistung zu verwenden. In diesem Dokument wird beschrieben, wie die NetScaler VPX-Instanz so konfiguriert wird, dass sie an den `vhost-user` Ports arbeitet, die von OVS-DPDK auf dem KVM-Host bereitgestellt werden.

OVS ist ein Multilayer-Virtual Switch, der unter der Open-Source-Apache 2.0-Lizenz lizenziert DPDK ist eine Reihe von Bibliotheken und Treibern für die schnelle Paketverarbeitung.

Die folgenden Versionen von Fedora, RHOS, OVS und DPDK sind für die Konfiguration einer NetScaler VPX-Instanz qualifiziert:

Fedora	RHOS
Fedora 25	RHOS 7,4
OVS 2.7.0	VERSION 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Voraussetzungen

Stellen Sie vor der Installation von DPDK sicher, dass der Host über 1 GB große Seiten verfügt.

Weitere Informationen finden Sie in dieser Dokumentation zu den DPDK-Systemanforderungen. Es folgt eine Zusammenfassung der Schritte, die erforderlich sind, um eine NetScaler VPX-Instanz auf KVM für die Verwendung von OVS DPDK-basierten Host-Interfaces zu konfigurieren:

- Installieren Sie DPDK.
- Erstellen und installieren Sie OVS.
- Erstellen Sie eine OVS-Brücke.
- Schließen Sie eine physikalische Schnittstelle an die OVS-Brücke an.
- Hängen Sie `vhost-user` Ports an den OVS-Datenpfad an.
- Stellen Sie einen KVM-VPX mit OVS-DPDK-basierten `vhost-user` Ports bereit.

DPDK installieren

Um DPDK zu installieren, folgen Sie den Anweisungen in diesem Open vSwitch mit DPDK-Dokument .

Erstellen und Installieren von OVS

Laden Sie OVS von der OVS-Downloadseite herunter. Erstellen und installieren Sie als Nächstes OVS mit einem DPDK-Datapath. Folgen Sie den Anweisungen im Dokument Installieren von Open vSwitch .

Ausführlichere Informationen finden Sie im DPDK Getting Started Guide für Linux.

Erstellen einer OVS-Brücke

Geben Sie je nach Bedarf den Befehl Fedora oder RHOS ein, um eine OVS-Bridge zu erstellen:

Fedora-Befehl:

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
    datapath_type=netdev
<!--NeedCopy-->
```

RHOS-Befehl:

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
<!--NeedCopy-->
```

Verbinden Sie die physische Schnittstelle mit der OVS-Brücke

Binden Sie die Ports an DPDK und verbinden Sie sie dann mit der OVS-Bridge, indem Sie die folgenden Fedora- oder RHOS-Befehle eingeben:

Fedora-Befehl:

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface
    dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface
    dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```

RHOS-Befehl:

```
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
    options:dpdk-devargs=0000:03:00.0


ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
    options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```


Die als Teil der Optionen `dpdk-devargs` gezeigte gibt den PCI-BDF der jeweiligen physikalischen NIC an.

Anhängen von `vhost-user` Ports an den OVS-Datenpfad

Geben Sie die folgenden Fedora- oder RHOS-Befehle ein, um `vhost-user` Ports an den OVS-Datenpfad anzuhängen:

Fedora-Befehl:

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set
    Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-
    user1  mtu_request=9000

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set
    Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-
    user2  mtu_request=9000

chmod g+w  /usr/local/var/run/openvswitch/vhost*
<!--NeedCopy-->
```

RHOS-Befehl:

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
    type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
    type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w /var/run/openvswitch/vhost*
<!--NeedCopy-->
```

Stellen Sie einen KVM-VPX mit OVS-DPDK-basierten `vhost-user` Ports bereit

Sie können eine VPX-Instanz auf Fedora KVM mit OVS-DPDK-basierten `vhost-user` Ports nur von der CLI aus bereitstellen, indem Sie die folgenden QEMU-Befehle verwenden:
Fedora Befehl:

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \

-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages,
    share=on -numa node,memdev=mem \

```



```
-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc-image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \

-device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,bootindex=1 \

-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \

-device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,bus=pci.0,addr=0x3 \

-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-user1> \

-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \

-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-user2> \

-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device virtio-net

pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \

--nographic
<!--NeedCopy-->
```

Verwenden Sie für RHOS die folgende XML-Beispieldatei, um die NetScaler VPX-Instanz mithilfe von bereitzustellen `virsh`.

```
<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>

    <hugepages>

```



```
15        <page size='1048576' unit='KiB'/>
16
17      </hugepages>
18
19    </memoryBacking>
20
21    <vcpu placement='static'>6</vcpu>
22
23    <cputune>
24
25      <shares>4096</shares>
26
27      <vcpupin vcpu='0' cpuset='0'/>
28
29      <vcpupin vcpu='1' cpuset='2'/>
30
31      <vcpupin vcpu='2' cpuset='4'/>
32
33      <vcpupin vcpu='3' cpuset='6'/>
34
35      <emulatorpin cpuset='0,2,4,6'/>
36
37    </cputune>
38
39    <numatune>
40
41      <memory mode='strict' nodeset='0'/>
42
43    </numatune>
44
45    <resource>
46
47      <partition>/machine</partition>
48
49    </resource>
50
51    <os>
52
53      <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55      <boot dev='hd'/>
56
57    </os>
58
59    <features>
```



```
60
61      <acpi/>
62
63      <apic/>
64
65    </features>
66
67    <cpu mode='custom' match='minimum' check='full'>
68
69      <model fallback='allow'>Haswell-noTSX</model>
70
71      <vendor>Intel</vendor>
72
73      <topology sockets='1' cores='6' threads='1'/>
74
75      <feature policy='require' name='ss'/>
76
77      <feature policy='require' name='pcid'/>
78
79      <feature policy='require' name='hypervisor'/>
80
81      <feature policy='require' name='arat'/>
82
83  <domain type='kvm'>
84
85    <name>dpdk-vpx1</name>
86
87    <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88
89    <memory unit='KiB'>16777216</memory>
90
91    <currentMemory unit='KiB'>16777216</currentMemory>
92
93    <memoryBacking>
94
95      <hugepages>
96
97        <page size='1048576' unit='KiB'/>
98
99      </hugepages>
100
101   </memoryBacking>
102
103   <vcpu placement='static'>6</vcpu>
104
```



```
<cputune>

  <shares>4096</shares>

  <vcpupin vcpu='0' cpuset='0'/>

  <vcpupin vcpu='1' cpuset='2'/>

  <vcpupin vcpu='2' cpuset='4'/>

  <vcpupin vcpu='3' cpuset='6'/>

  <emulatorpin cpuset='0,2,4,6'/>

</cputune>

<numatune>

  <memory mode='strict' nodeset='0'/>

</numatune>

<resource>

  <partition>/machine</partition>

</resource>

<os>

  <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>

  <boot dev='hd'/>

</os>

<features>

  <acpi/>

  <apic/>

</features>

<cpu mode='custom' match='minimum' check='full'>
```



```
150
151     <model fallback='allow'>Haswell-noTSX</model>
152
153     <vendor>Intel</vendor>
154
155     <topology sockets='1' cores='6' threads='1'/>
156
157     <feature policy='require' name='ss'/>
158
159     <feature policy='require' name='pcid'/>
160
161     <feature policy='require' name='hypervisor'/>
162
163     <feature policy='require' name='arat'/>
164
165     <feature policy='require' name='tsc_adjust'/>
166
167     <feature policy='require' name='xsaveopt'/>
168
169     <feature policy='require' name='pdpe1gb'/>
170
171     <numa>
172
173       <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess='
             shared'/>
174
175     </numa>
176
177   </cpu>
178
179   <clock offset='utc'/>
180
181   <on_poweroff>destroy</on_poweroff>
182
183   <on_reboot>restart</on_reboot>
184
185   <on_crash>destroy</on_crash>
186
187   <devices>
188
189     <emulator>/usr/libexec/qemu-kvm</emulator>
190
191     <disk type='file' device='disk'>
192
193       <driver name='qemu' type='qcow2' cache='none'/>
```



```
194
195         <source file='/home/NSVPX-KVM-12.0-52.18_nc.qcow2'/>
196
197         <target dev='vda' bus='virtio'/>
198
199         <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
               function='0x0'/>
200
201       </disk>
202
203       <controller type='ide' index='0'>
204
205         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
               function='0x1'/>
206
207       </controller>
208
209       <controller type='usb' index='0' model='piix3-uhci'>
210
211         <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
               function='0x2'/>
212
213       </controller>
214
215       <controller type='pci' index='0' model='pci-root'/>
216
217       <interface type='direct'>
218
219         <mac address='52:54:00:bb:ac:05'/>
220
221         <source dev='enp129s0f0' mode='bridge'/>
222
223         <model type='virtio'/>
224
225         <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
               function='0x0'/>
226
227       </interface>
228
229       <interface type='vhostuser'>
230
231         <mac address='52:54:00:55:55:56'/>
232
233         <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
               'client'/>
```



```
234
235         <model type='virtio'/>
236
237         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
               function='0x0'/>
238
239       </interface>
240
241       <interface type='vhostuser'>
242
243         <mac address='52:54:00:2a:32:64'/>
244
245         <source type='unix' path='/var/run/openvswitch/vhost-user2' mode=
               'client'/>
246
247         <model type='virtio'/>
248
249         <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
               function='0x0'/>
250
251       </interface>
252
253       <interface type='vhostuser'>
254
255         <mac address='52:54:00:2a:32:74'/>
256
257         <source type='unix' path='/var/run/openvswitch/vhost-user3' mode=
               'client'/>
258
259         <model type='virtio'/>
260
261         <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
               function='0x0'/>
262
263       </interface>
264
265       <interface type='vhostuser'>
266
267         <mac address='52:54:00:2a:32:84'/>
268
269         <source type='unix' path='/var/run/openvswitch/vhost-user4' mode=
               'client'/>
270
271        <model type='virtio'/>
272
```



```
273         <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
               function='0x0'/>
274
275       </interface>
276
277       <serial type='pty'>
278
279         <target port='0'/>
280
281       </serial>
282
283       <console type='pty'>
284
285         <target type='serial' port='0'/>
286
287       </console>
288
289       <input type='mouse' bus='ps2'/>
290
291       <input type='keyboard' bus='ps2'/>
292
293       <graphics type='vnc' port='-1' autoport='yes'>
294
295         <listen type='address'/>
296
297       </graphics>
298
299       <video>
300
301         <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
303         <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
               function='0x0'/>
304
305       </video>
306
307       <memballoon model='virtio'>
308
309         <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
               function='0x0'/>
310
311       </memballoon>
312
313     </devices>
314
```



```
</domain
<!--NeedCopy-->
```

Wichtige Hinweise

In der XML-Datei muss die hugepage Größe 1 GB betragen, wie in der Beispieldatei gezeigt.

```
<memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>
<!--NeedCopy-->
```

In der Beispieldatei ist vhost-user1 auch der vhost Benutzerport, der an ovs-br0 gebunden ist.

```
<interface type='vhostuser'>

      <mac address='52:54:00:55:55:56'/>

      <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
         'client'/>

      <model type='virtio'/>

      <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
         function='0x0'/>

    </interface>
<!--NeedCopy-->
```

Um die NetScaler VPX-Instanz aufzurufen, verwenden Sie den virsh Befehl.

Anwenden der NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance auf dem KVM-Hypervisor

May 11, 2023

Sie können die NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance auf dem

KVM-Hypervisor anwenden. Daher kann ein Kunden-Setup auf einer VPX-Instanz in viel kürzerer Zeit konfiguriert werden.

Weitere Informationen zu Preboot-Benutzerdaten und deren Format finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance in der Cloud.

> Hinweis:
>
> Um mithilfe von Preboot-Benutzerdaten im KVM-Hypervisor bootstrappen zu können, muss die Standard-Gateway-Konfiguration im <NS-CONFIG> Abschnitt übergeben werden. Weitere Informationen zum Inhalt des <NS-CONFIG> Transponders finden Sie im folgenden <NS-CONFIG> Abschnitt “Beispiel”.

Beispiel <NS-CONFIG> Abschnitt:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP> 10.102.38.216 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

So stellen Sie Preboot-Benutzerdaten auf dem KVM-Hypervisor bereit

Sie können Preboot-Benutzerdaten auf dem KVM-Hypervisor über eine ISO-Datei bereitstellen, die mit einem CD-ROM-Gerät angehängt wird.

Benutzerdaten mit CD-ROM-ISO-Datei bereitstellen

Sie können Virtual Machine Manager (VMM) verwenden, um Benutzerdaten mit dem CD-ROM-Gerät als ISO-Image in die virtuelle Maschine (VM) zu injizieren. KVM unterstützt CD-ROMs in VM Guest entweder

durch direkten Zugriff auf ein physisches Laufwerk auf dem VM-Hostserver oder durch Zugriff auf ISO-Images.

Mit den folgenden Schritten können Sie Benutzerdaten mithilfe der CD-ROM-ISO-Datei bereitstellen:

1. Erstellen Sie eine Datei mit dem Dateinamen `userdata`, die den Inhalt der Preboot-Benutzerdaten enthält.

   > Hinweis: Der Dateiname muss ausschließlich als `userdata` verwendet werden.

2. Speichern Sie die `userdata`-Datei in einem Ordner und erstellen Sie mithilfe des Ordners ein ISO-Image.

   Sie können ein ISO-Image mit einer `userdata`-Datei mit den folgenden zwei Methoden erstellen:

   - Verwenden eines beliebigen Imageverarbeitungstools wie PowerISO.
   - Befehl `mkisofs` unter Linux verwenden.

   Die folgende Beispielkonfiguration zeigt, wie ein ISO-Image über den Befehl `mkisofs` in Linux generiert wird.

```
root@ubuntu:~/sai/19oct# ls -lh
total 4.0K
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata
I: -input-charset not specified, using utf-8 (detected in locale
   settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
175 extents written (0 MB)
root@ubuntu:~/sai/19oct#
root@ubuntu:~/sai/19oct# ls -lh
total 356K
-rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
<!--NeedCopy-->
```

3. Stellen Sie die NetScaler VPX-Instanz mithilfe des Standardbereitstellungsprozesses bereit, um die VM zu erstellen. Schalten Sie die VM jedoch nicht automatisch ein.

4. Fügen Sie mit Virtual Machine Manager ein CD-ROM-Gerät hinzu, indem Sie die folgenden Schritte ausführen:

a) Doppelklicken Sie im Virtual Machine Manager auf einen VM-Gasteintrag, um dessen Konsole zu öffnen, und wechseln Sie mit Ansicht **> Details zur Ansicht Details**.
b) Klicken Sie auf **Hardware hinzufügen > Speicher > Gerätetyp > CD-ROM-Gerät**.
c) Klicken Sie auf **Verwalten**, wählen Sie die richtige ISO-Datei aus und klicken Sie auf **Fertig stellen**. Eine neue CD-ROM unter **Resources** auf Ihrer NetScaler VPX-Instanz wird erstellt.

5. Schalten Sie die VM ein.

NetScaler VPX auf AWS

July 4, 2023

Sie können eine NetScaler VPX-Instanz auf Amazon Web Services (AWS) starten. Die NetScaler VPX-Appliance ist als Amazon Machine Image (AMI) im AWS Marketplace verfügbar. Mit einer NetScaler VPX-Instanz auf AWS können Sie AWS-Cloud-Computing-Funktionen nutzen und NetScaler Load Balancing- und Traffic-Management-Funktionen für ihre Geschäftsanforderungen verwenden. Die VPX-Instanz unterstützt alle Funktionen der Datenverkehrsverwaltung einer physischen NetScaler Appliance und kann als eigenständige Instanzen oder in HA-Paaren bereitgestellt werden. Weitere Informationen zu VPX-Funktionen finden Sie im VPX-Datenblatt.

Erste Schritte

Bevor Sie mit Ihrer VPX-Bereitstellung beginnen, müssen Sie mit den folgenden Informationen vertraut sein:

- AWS-Terminologie
- AWS-VPX-Unterstützungsmatrix
- Einschränkungen und Nutzungsrichtlinien
- Voraussetzungen
- So funktioniert eine NetScaler VPX-Instanz auf AWS

Bereitstellen einer NetScaler VPX-Instanz auf AWS

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Eigenständig
- Hochverfügbarkeit (aktiv-Passiv)
  - Hochverfügbarkeit innerhalb derselben Zone
  - Hochverfügbarkeit über verschiedene Zonen hinweg mit Elastic IP
  - Hochverfügbarkeit über verschiedene Zonen hinweg mit Private IP
- Aktiv-Aktiv GSLB

- Autoscaling (Active-Active) mit ADM

Hybrid-Bereitstellungen

- Bereitstellen von NetScaler in AWS Outpost
- Bereitstellen von NetScaler in VMC in AWS

Lizenzierung

Für eine NetScaler VPX-Instanz auf AWS ist eine Lizenz erforderlich. Die folgenden Lizenzoptionen sind für NetScaler VPX-Instanzen verfügbar, die auf AWS ausgeführt werden:

- Kostenlos (unbegrenzt)
- Stündlich
- jährlich
- BYOL
- Kostenlose Testversion (alle NetScaler VPX-AWS-Abonnementangebote für 21 Tage kostenlos im AWS Marketplace.)

Automatisierung

- NetScaler ADM: Intelligente Bereitstellung
- AWS-Schnellstarts: NetScaler VPX für Webanwendungen auf AWS
- GitHub CFTs: NetScaler Vorlagen und Skripts für die AWS-Bereitstellung
- GitHub Ansible: NetScaler Vorlagen und Skripts für die AWS-Bereitstellung
- GitHub Terraform: NetScaler Vorlagen und Skripts für die AWS-Bereitstellung
- AWS-Pattern-Bibliothek (PL): NetScaler VPX

Blogs

- Wie NetScaler auf AWS Kunden hilft, Anwendungen sicher bereitzustellen
- Anwendungsbereitstellung in Hybrid Cloud mit NetScaler und AWS
- Citrix ist ein AWS-Netzwerkkompetenzpartner
- NetScaler: Immer bereit für Public Clouds
- Einfache Skalierung oder Skalierung in öffentlichen Clouds mit NetScaler
- Citrix erweitert die Auswahl an ADC-Bereitstellungen mit AWS Outposts

- Verwenden von NetScaler mit Amazon VPC-Ingress-Routing
- Citrix bietet Auswahl, Leistung und vereinfachte Bereitstellung in AWS
- Die Sicherheit der NetScaler Web App Firewall — jetzt auf dem AWS Marketplace
- Wie Aria Systems die NetScaler Web App Firewall auf AWS verwendet

Videos

- Vereinfachung der Public Cloud NetScaler-Bereitstellungen durch ADM
- Provisioning und Konfiguration von NetScaler VPX in AWS mit sofort einsatzbereiten Terraform-Skripten
- Bereitstellen von NetScaler HA in AWS mithilfe der CloudFormation-Vorlage
- Bereitstellen von NetScaler HA über Availability Zones hinweg mit AWS QuickStart
- So stellen Sie NetScaler in AWS bereit
- NetScaler Autoscale mit ADM
- NetScaler unterstützt automatische Backend-Serverskalierung in AWS oder AWS Autoscaling-Gruppe

Fallstudien von Kunden

- Technologielösung — Xenit AB
- Ein besserer Weg, um mit Citrix und AWS Cloud Geschäfte zu machen — Aria
- Entdecken Sie den Vorteil von NetScaler und AWS
- Regen zu vermieten - Kundenbericht

Lösungen

- Bereitstellung einer digitalen Werbeplattform auf AWS mit NetScaler
- Verbesserung der Clickstream-Analyse in AWS mit NetScaler

Support

- Öffnen eines Support-Falls
- Informationen zum Angebot von NetScaler-Abonnements finden Sie unter Problembehandlung bei einer VPX-Instanz in AWS. Um eine Support-Anfrage einzureichen, suchen Sie nach Ihrer AWS-Kontonummer und Ihrem Support-PIN-Code und wenden Sie sich an den NetScaler-Support.

- Stellen Sie für NetScaler Customer Licensed Offering oder BYOL sicher, dass Sie über den gültigen Support- und Wartungsvertrag verfügen. Wenn Sie keine Vereinbarung haben, wenden Sie sich an Ihren NetScaler-Ansprechpartner.

Zusätzliche Referenzen

- AWS-Webinar auf Abruf — NetScaler auf AWS
- Bereitstellungshandbücher für NetScaler VPX auf AWS
- Erstellen eines VPX Amazon Machine Image (AMI) in SC2S/geheimer Region
- NetScaler auf AWS
- NetScaler VPX — Datenblatt
- NetScaler im AWS Marketplace
- NetScaler ist Teil der AWS-Netzwerkpartnerlösungen (Load Balancer)
- NetScaler für VMware Cloud auf AWS
- AWS FAQs

AWS-Terminologie

August 19, 2021

In diesem Abschnitt wird die Liste der häufig verwendeten AWS-Begriffe und -Ausdrücke beschrieben. Weitere Informationen finden Sie unter AWS Glossar.

Begriff	Definition
Amazon Machine Image (AMI)	Ein Maschinenimage, das die Informationen bereitstellt, die zum Starten einer Instanz erforderlich sind, bei der es sich um einen virtuellen Server in der Cloud handelt.
Elastic Block Store	Bietet persistente Blockspeicher-Volumes für die Verwendung mit Amazon EC2-Instanzen in der AWS-Cloud.
Simple Storage Service (S3)	Speicher für das Internet. Es wurde entwickelt, um Web-Scale-Computing für Entwickler einfacher zu machen.

Begriff	Definition
Elastic Compute Cloud (EC2)	Ein Webdienst, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Es wurde entwickelt, um Web-basierte Cloud Computing für Entwickler einfacher zu machen.
Elastischer Lastenausgleich (ELB)	Verteilt eingehenden Anwendungsdatenverkehr auf mehrere EC2-Instanzen in mehreren Availability Zones. Dies erhöht die Fehlertoleranz Ihrer Anwendungen.
Elastische Netzwerkschnittstelle (ENI)	Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer Virtual Private Cloud (VPC) anfügen können.
Elastic IP (EIP) Adresse	Eine statische, öffentliche IPv4-Adresse, die Sie in Amazon EC2 oder Amazon VPC zugewiesen und dann einer Instanz zugeordnet haben. Elastic IP-Adressen sind Ihrem Konto zugeordnet, nicht einer bestimmten Instanz. Sie sind elastisch, weil Sie sie leicht zuordnen, befestigen, lösen und befreien können, wenn sich Ihre Bedürfnisse ändern.
Instanztyp	Amazon EC2 bietet eine große Auswahl an Instanztypen, die für verschiedene Anwendungsfälle optimiert sind. Instanztypen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität und bieten Ihnen die Flexibilität, den geeigneten Ressourcenmix für Ihre Anwendungen auszuwählen.

Begriff	Definition
Identity and Access Management (IAM)	Eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht. Sie können eine IAM-Rolle verwenden, um Anwendungen, die auf einer EC2-Instanz ausgeführt werden, den sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen. Die IAM-Rolle ist erforderlich, um VPX-Instanzen in einem Hochverfügbarkeits-Setup bereitzustellen.
Internet-Gateway	Verbindet ein Netzwerk mit dem Internet. Sie können Datenverkehr für IP-Adressen außerhalb Ihrer VPC an das Internet-Gateway weiterleiten.
Schlüsselpaar	Eine Reihe von Sicherheitsanmeldeinformationen, die Sie zum elektronischen Nachweis Ihrer Identität verwenden. Ein Schlüsselpaar besteht aus einem privaten Schlüssel und einem öffentlichen Schlüssel.
Routentabellen	Eine Reihe von Routingregeln, die den Datenverkehr steuert, der ein Subnetz verlässt, das der Routingtabelle zugeordnet ist. Sie können einer einzelnen Routingtabelle mehrere Subnetze zuordnen, aber ein Subnetz kann jeweils nur einer Routingtabelle zugeordnet werden.
Sicherheitsgruppen	Eine benannte Gruppe zulässiger eingehender Netzwerkverbindungen für eine Instanz.
Subnetze	Ein Segment des IP-Adressbereichs einer VPC, an die EC2-Instanzen angeschlossen werden können. Sie können Subnetze erstellen, um Instanzen entsprechend den Sicherheits- und betrieblichen Anforderungen zu gruppieren.

Begriff	Definition
Virtuelle Private Cloud (VPC)	Ein Webservice zum Provisioning eines logisch isolierten Abschnitts der AWS-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.
Auto Scaling	Ein Webservice zum automatischen Starten oder Beenden von Amazon EC2-Instanzen basierend auf benutzerdefinierten Richtlinien, Zeitplänen und Zustandsprüfungen.
CloudFormation	Ein Service zum Schreiben oder Ändern von Vorlagen, die zugehörige AWS-Ressourcen zusammen als Einheit erstellen und löschen.

AWS-VPX-Unterstützungsmatrix

May 11, 2023

In den folgenden Tabellen sind das unterstützte VPX-Modell und die AWS-Regionen, Instanztypen und Dienste aufgeführt.

Tabelle 1: Unterstützte VPX-Modelle auf AWS

Unterstütztes VPX-Modell
NetScaler VPX Standard/Erweiterte/Premium Edition — 200 Mbit/s
NetScaler VPX Standard/Erweiterte/Premium Edition — 1000 Mbit/s
NetScaler VPX Standard/Erweiterte/Premium Edition — 3 Gbit/s
NetScaler VPX Standard/Erweitert/Premium Edition — 5 Gbit/s
NetScaler VPX Standard/Erweitert/Premium — 10 Mbit/s
NetScaler VPX Express — 20 Mbit/s
NetScaler VPX — vom Kunden lizenziert
NetScaler (ehemals NetScaler) VPX FIPS — vom Kunden lizenziert

Tabelle: 2 Unterstützte AWS-Regionen

Unterstützte AWS Regionen
USA West (Oregon)
USA West (Nordkalifornien)
USA Ost (Ohio)
USA Ost (Nord-Virginia)
Asien-Pazifik (Mumbai)
Asien-Pazifik (Seoul)
Asien-Pazifik (Singapur)
Asien-Pazifik (Sydney)
Asien-Pazifik (Tokio)
Asien-Pazifik (Hongkong)
Asien-Pazifik (Osaka)
Kanada (Central)
China (Peking)
China (Ningxia)
EU (Frankfurt)
EU (Irland)
EU (London)
EU (Paris)
EU (Mailand)
Südamerika (São Paulo)
AWS GovCloud (USA-Ost)
AWS GovCloud (USA, West)
AWS Streng geheim (C2S)
Naher Osten (Bahrain)
Afrika (Kapstadt)
C2S

Tabelle 3: Unterstützte AWS-Instanztypen

Unterstützte AWS-Instanztypen
t2.medium, t2.large, t2.xlarge, t2.2xlarge
m3.large, m3.xlarge, m3.2xlarge
c4.large, c4.xlarge, c4.2xlarge, c4.4xlarge, c4.8xlarge
m4.large, m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16xlarge
m5.large, m5.xlarge, m5.2xlarge, m5.4xlarge, m5.12xlarge, m5.24xlarge
c5.large, c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.18xlarge, c5.24xlarge
c5n.large, c5n.xlarge, c5n.2xlarge, c5n.4xlarge, c5n.9xlarge, c5n.18xlarge
D2.xlarge, D2.2xlarge, D2.4xlarge, D2.8xlarge
m5a.large, m5a.xlarge, m5a.2xlarge, m5a.8xlarge, m5a.12xlarge, m5a.16xlarge, m5a.24xlarge
t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge

Tabelle 4: Unterstützte AWS-Services

Unterstützte AWS Services
EC2: Startet ADC-Instanzen.
Lambda: Ruft NetScaler VPX NITRO-APIs während der Bereitstellung von NetScaler VPX-Instanzen über CFT auf.
VPC- und VPC-Ingress-Routing: VPC erstellt isolierte Netzwerke, in denen ADC gestartet werden kann. Das VPC Ingress Routing wird in der Firewall Load Balancing-Lösung verwendet.
Route53: Verteilt den Datenverkehr auf alle NetScaler VPX-Knoten in der NetScaler Autoscale-Lösung.
ELB: Verteilt den Datenverkehr auf alle NetScaler VPX-Knoten in der NetScaler Autoscale-Lösung.
Cloudwatch: Überwacht Leistung und Systemparameter für die NetScaler VPX Instanz.
AWS Autoscaling: Wird für die automatische Skalierung von Backend-Servern verwendet.
Cloud-Bildung: CloudFormation-Vorlagen werden verwendet, um NetScaler VPX-Instanzen bereitzustellen.
Simple Queue Service (SQS): Überwacht Skalierungs- und Herunterskalierungsereignisse beim Back-End-Autoscaling.
Simple Notification Service (SNS): Überwacht Skalierungs- und Herunterskalierungsereignisse beim Back-End-Autoscaling.
Identitäts- und Zugriffsmanagement (IAM): Bietet Zugriff auf AWS-Services und -Ressourcen.

Unterstützte AWS Services
AWS-Außenposten: Bereitstellung von NetScaler VPX-Instanzen in AWS Outposts.

Citrix empfiehlt die folgenden AWS-Instanztypen:

- M5- und C5n-Serien für Marketplace-Editionen oder bandbreitenbasierte Poollizenzierung.
- C5n-Serie für vCPU-basierte Pool-Lizenzierung.

VPX-Angebot auf dem AWS-Marktplatz	AWS-Instanzempfehlung
VPX 10, VPX Express 20, VPX 200	M5.xLarge
VPX 1000, VPX 3 G, VPX 5 G	M5.2xLarge

Citrix empfiehlt die folgenden AWS-Instanztypen basierend auf dem Durchsatz.

VPX mit gepoolter Lizenzierung (Bandbreitenlizenzen)	AWS-Instanzempfehlung
VPX 8G	C5n.4xLarge
VPX 10G, VPX 15G, VPX 25G	C5n.9xLarge

> Hinweis:
>
> Das VPX 25G-Angebot bietet nicht den gewünschten 25G-Durchsatz in AWS, kann jedoch zu einer höheren SSL-Transaktionsrate führen.

Gehen Sie wie folgt vor, um einen Durchsatz von mehr als 5G zu erreichen:

- Wählen Sie **NetScaler VPX — Customer Licensed (BYOL)-Angebot** im AWS Marketplace.
- Wählen Sie **Pooled Licensing (Bandbreitenlizenzen)** in der NetScaler GUI oder CLI aus.

Um Ihre Instanz basierend auf verschiedenen Metriken wie Paketen pro Sekunde und SSL-Transaktionsrate zu ermitteln, wenden Sie sich an Ihren Citrix Kontakt, um Unterstützung zu erhalten. Hinweise zur Lizenzierung und Dimensionierung von vCPU-basierten Pools erhalten Sie beim NetScaler-Support.

Einschränkungen und Nutzungsrichtlinien

May 11, 2023

Bei der Bereitstellung einer NetScaler VPX-Instanz in AWS gelten die folgenden Einschränkungen und Verwendungsrichtlinien:

- Bevor Sie beginnen, lesen Sie den Abschnitt AWS-Terminologie unter Bereitstellen einer NetScaler VPX-Instanz auf AWS.
- Das Clustering-Feature wird für VPX nicht unterstützt.
- Damit das Hochverfügbarkeitssetup effektiv funktioniert, verknüpfen Sie ein dediziertes NAT-Gerät der Verwaltungsschnittstelle oder verknüpfen Sie EIP mit NSIP. Weitere Informationen zu NAT finden Sie in der AWS-Dokumentation unter NAT-Instances.
- Datenverkehr und Verwaltungsverkehr müssen durch ENIs getrennt werden, die zu verschiedenen Subnetzen gehören.
- Nur die NSIP-Adresse muss auf der Management-ENI vorhanden sein.
- Wenn eine NAT-Instanz zur Sicherheit verwendet wird, anstatt dem NSIP einen EIP zuzuweisen, sind entsprechende Änderungen beim Routing auf VPC-Ebene erforderlich. Anweisungen zum Vornehmen von Routingänderungen auf VPC-Ebene finden Sie in der AWS-Dokumentation unter Szenario 2: VPC mit öffentlichen und privaten Subnetzen.
- Eine VPX-Instanz kann von einem EC2-Instanz-Typ zu einem anderen verschoben werden (z. B. von m3.large auf m3.xlarge).
- Für Speicheroptionen für VPX in AWS empfiehlt Citrix EBS, da es dauerhaft ist und die Daten auch verfügbar sind, nachdem sie von der Instanz getrennt wurden.
- Das dynamische Hinzufügen von ENIs zu VPX wird nicht unterstützt. Starten Sie die VPX-Instanz neu, um das Update anzuwenden. Citrix empfiehlt, die Standalone- oder HA-Instanz zu beenden, die neue ENI anzufügen und die Instanz dann neu zu starten.
- Sie können einem ENI mehrere IP-Adressen zuweisen. Die maximale Anzahl von IP-Adressen pro ENI wird durch den EC2-Instanztyp bestimmt, siehe Abschnitt “IP-Adressen pro Netzwerkschnittstelle pro Instanztyp” in Elastic Network Interfaces. Sie müssen die IP-Adressen in AWS zuweisen, bevor Sie sie ENIs zuweisen. Weitere Informationen finden Sie unter Elastic Network Interfaces.
- Citrix empfiehlt, die Interface-Befehle zum Aktivieren und Deaktivieren von NetScaler VPX Schnittstellen zu vermeiden.
- Die NetScaler Befehle `set ha node \<NODE\_ID\> -haStatus STAYPRIMARY` und `set ha node \<NODE\_ID\> -haStatus STAYSECONDARY` sind standardmäßig deaktiviert.
- IPv6 wird für VPX nicht unterstützt.
- Aufgrund von AWS-Einschränkungen werden diese Funktionen nicht unterstützt:
  - Gratuitous ARP(GARP)

  - L2-Modus
  - Getaggtes VLAN
  - Dynamisches Routing
  - virtueller MAC

- Damit RNAT funktioniert, stellen Sie sicher, dass die **Quelle/Destination Check** deaktiviert ist. Weitere Informationen finden Sie unter "Ändern der Quelle/Zielüberprüfung" in Elastic Network Interfaces.

- In einer NetScaler VPX Bereitstellung auf AWS in einigen AWS-Regionen kann die AWS-Infrastruktur möglicherweise keine AWS-API-Aufrufe auflösen. Dies passiert, wenn die API-Aufrufe über eine Nicht-Verwaltungsschnittstelle auf der NetScaler VPX-Instanz ausgegeben werden.
  Beschränken Sie zur Problemumgehung die API-Aufrufe nur auf die Verwaltungsschnittstelle. Erstellen Sie dazu ein NSVLAN auf der VPX-Instanz und binden Sie die Verwaltungsschnittstelle mit dem entsprechenden Befehl an das NSVLAN.
  Beispiel:
  ```
  set ns config -nsvlan <vlan id> -ifnum 1/1 -tagged NO
  save config
  ```
  Starten Sie die VPX-Instanz an der Eingabeaufforderung neu. Weitere Informationen zum Konfigurieren `nsvlan`finden Sie unter Konfigurieren von NSVLAN.

- In der AWS-Konsole kann die vCPU-Auslastung, die für eine VPX-Instance auf der Registerkarte **Monitoring** angezeigt wird, hoch sein (bis zu 100 Prozent), selbst wenn die tatsächliche Nutzung viel niedriger ist. Um die tatsächliche vCPU-Auslastung zu sehen, navigieren Sie zu **Alle CloudWatch-Metriken anzeigen**. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instanzen mit Amazon CloudWatch.

Voraussetzungen

September 1, 2023

Bevor Sie versuchen, eine VPX-Instanz in AWS zu erstellen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- **Ein AWS-Konto**: zum Starten eines NetScaler VPX AMI in einer AWS Virtual Private Cloud (VPC). Unter www.aws.amazon.com können Sie kostenlos ein AWS-Konto erstellen.

- **Ein AWS Identity and Access Management (IAM) -Benutzerkonto**: zum sicheren Steuern des Zugriffs auf AWS-Services und -Ressourcen für Ihre Benutzer. Weitere Informationen zum Erstellen eines IAM-Benutzerkontos finden Sie unter Erstellen von IAM-Benutzern (Konsole). Eine

IAM-Rolle ist sowohl für eigenständige als auch für Hochverfügbarkeitsbereitstellungen obligatorisch.

Die mit Ihrem AWS-Konto verknüpfte IAM-Rolle muss für verschiedene Szenarien über die folgenden IAM-Berechtigungen verfügen.

HA-Paar mit IPv4-Adressen in derselben AWS-Zone:

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
<!--NeedCopy-->
```

HA-Paar mit IPv6-Adressen in derselben AWS-Zone:

```
"ec2:DescribeInstances",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
<!--NeedCopy-->
```

HA-Paar mit IPv4- und IPv6-Adressen in derselben AWS-Zone:

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
<!--NeedCopy-->
```

HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
<!--NeedCopy-->
```


HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
<!--NeedCopy-->
```

HA-Paar mit privaten IP- und Elastic IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
<!--NeedCopy-->
```

Autoscaling des AWS-Backends:

```
"ec2:DescribeInstances",
"autoscaling:*",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:ListTopics",
"sns:Subscribe",
"sqs:CreateQueue",
"sqs:ListQueues",
"sqs:DeleteMessage",
"sqs:GetQueueAttributes",
"sqs:SetQueueAttributes",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"ec2:CreateTags"
<!--NeedCopy-->
```


> Hinweis:
>
> - Wenn Sie eine Kombination der vorhergehenden Funktionen verwenden, verwenden Sie die Kombination von IAM-Berechtigungen für jede der Funktionen.
> - Wenn Sie die Citrix CloudFormation-Vorlage verwenden, wird die IAM-Rolle automatisch erstellt. Die Vorlage erlaubt es nicht, eine bereits erstellte IAM-Rolle auszuwählen.
> - Wenn Sie sich über die GUI bei der VPX-Instanz anmelden, wird eine Aufforderung zur Konfiguration der erforderlichen Berechtigungen für die IAM-Rolle angezeigt. Ignorieren Sie die Aufforderung, wenn Sie die Berechtigungen bereits konfiguriert haben.

- **AWS CLI**: So verwenden Sie alle Funktionen, die von der AWS Management Console aus Ihrem Terminalprogramm bereitgestellt werden. Weitere Informationen finden Sie im AWS CLI-Benutzerhandbuch. Sie benötigen auch die AWS CLI, um den Netzwerkschnittstellentyp in SR-IOV zu ändern.
- **Elastic Network Adapter (ENA)**: Für den treiberfähigen ENA-Instanz-Typ, z. B. M5-, C5-Instanzen, muss die Firmware-Version 13.0 und höher sein.
- Sie müssen den Instance Metadata Service (IMDS) auf der EC2-Instance für NetScaler VPX konfigurieren. IMDSv1 und IMDSv2 sind zwei Modi, die für den Zugriff auf Instance-Metadaten von einer laufenden AWS EC2-Instance verfügbar sind. IMDSv2 ist sicherer als IMDSv1. Sie können die Instanz so konfigurieren, dass sie entweder beide Methoden (die Standardoption) oder nur den IMDSv2-Modus verwendet (indem Sie IMDSv1 deaktivieren). Citrix ADC VPX unterstützt ab NetScaler VPX Version 13.1.48.x nur den IMDSv2-Modus.

AWS IAM-Rollen auf der NetScaler VPX-Instanz konfigurieren

May 11, 2023

Anwendungen, die auf einer Amazon EC2-Instanz ausgeführt werden, müssen AWS-Anmeldeinformationen in den AWS-API-Anfragen enthalten. Sie können AWS-Anmeldeinformationen direkt in der Amazon EC2-Instanz speichern und Anwendungen in dieser Instanz erlauben, diese Anmeldeinformationen zu verwenden. Dann müssen Sie jedoch die Anmeldeinformationen verwalten und sicherstellen, dass sie die Anmeldeinformationen sicher an jede Instanz weitergeben, und jede Amazon EC2-Instanz aktualisieren, wenn es Zeit ist, die Anmeldeinformationen zu wechseln. Das ist eine Menge zusätzlicher Arbeit.

Stattdessen können und müssen Sie eine Identity and Access Management (IAM) -Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2-Instanz ausgeführt werden. Wenn Sie eine Rolle verwenden, müssen Sie keine langfristigen Anmeldeinformationen (wie Benutzername und Kennwort oder Zugriffsschlüssel) an eine Amazon EC2-Instanz

verteilen. Stattdessen bietet die Rolle temporäre Berechtigungen, die Anwendungen verwenden können, wenn sie andere AWS-Ressourcen aufrufen. Wenn Sie eine Amazon EC2-Instanz starten, geben Sie eine IAM-Rolle an, die der Instanz zugeordnet werden soll. Anwendungen, die auf der Instanz ausgeführt werden, können dann die von der Rolle bereitgestellten temporären Anmeldeinformationen verwenden, um API-Anfragen zu signieren.

Die mit Ihrem AWS-Konto verknüpfte IAM-Rolle muss für verschiedene Szenarien über die folgenden IAM-Berechtigungen verfügen.

HA-Paar mit IPv4-Adressen in derselben AWS-Zone:

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

HA-Paar mit IPv6-Adressen in derselben AWS-Zone:

```
"ec2:DescribeInstances",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

HA-Paar mit IPv4- und IPv6-Adressen in derselben AWS-Zone:

```
"ec2:DescribeInstances",
"ec2:AssignPrivateIpAddresses",
"ec2:AssignIpv6Addresses",
"ec2:UnassignIpv6Addresses",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```


HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

HA-Paar mit privaten IP- und Elastic IP-Adressen über verschiedene AWS-Zonen hinweg:

```
"ec2:DescribeInstances",
"ec2:DescribeAddresses",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:DescribeRouteTables",
"ec2:DeleteRoute",
"ec2:CreateRoute",
"ec2:ModifyNetworkInterfaceAttribute",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Autoscaling des AWS-Backends:

```
"ec2:DescribeInstances",
"autoscaling:*",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:ListTopics",
"sns:Subscribe",
"sqs:CreateQueue",
"sqs:ListQueues",
"sqs:DeleteMessage",
"sqs:GetQueueAttributes",
"sqs:SetQueueAttributes",
"iam:SimulatePrincipalPolicy",
"iam:GetRole"
<!--NeedCopy-->
```

Zu beachtende Punkte:

- Wenn Sie eine Kombination der vorhergehenden Funktionen verwenden, verwenden Sie die Kombination von IAM-Berechtigungen für jede der Funktionen.

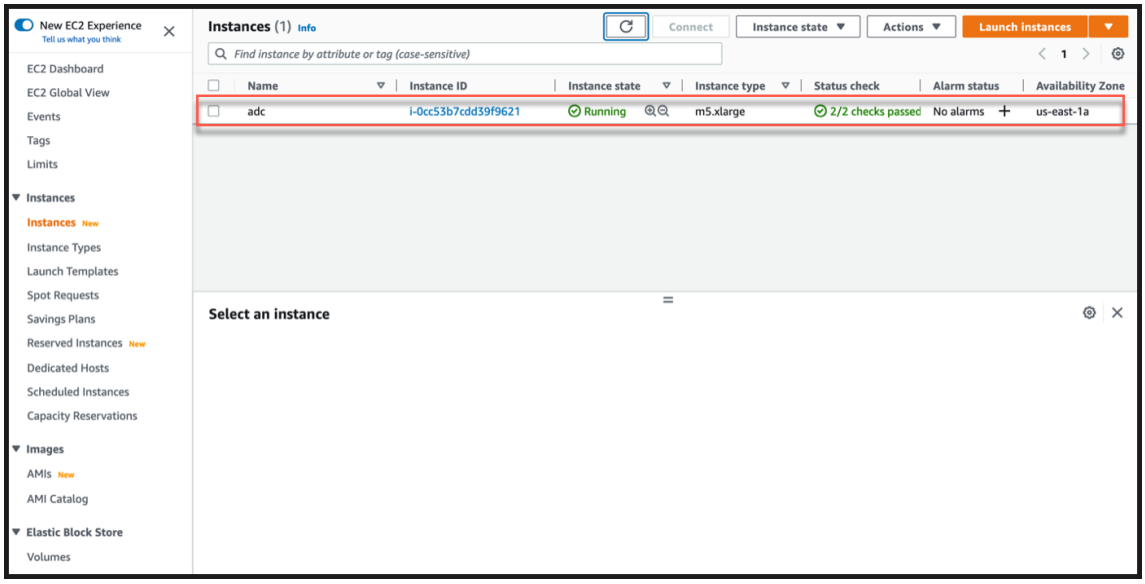
- Wenn Sie die Citrix CloudFormation-Vorlage verwenden, wird die IAM-Rolle automatisch erstellt. Die Vorlage erlaubt es nicht, eine bereits erstellte IAM-Rolle auszuwählen.
- Wenn Sie sich über die GUI bei der VPX-Instanz anmelden, wird eine Aufforderung zur Konfiguration der erforderlichen Berechtigungen für die IAM-Rolle angezeigt. Ignorieren Sie die Aufforderung, wenn Sie die Berechtigungen bereits konfiguriert haben.
- Eine IAM-Rolle ist sowohl für eigenständige als auch für Hochverfügbarkeitsbereitstellungen obligatorisch.

Erstellen einer IAM-Rolle

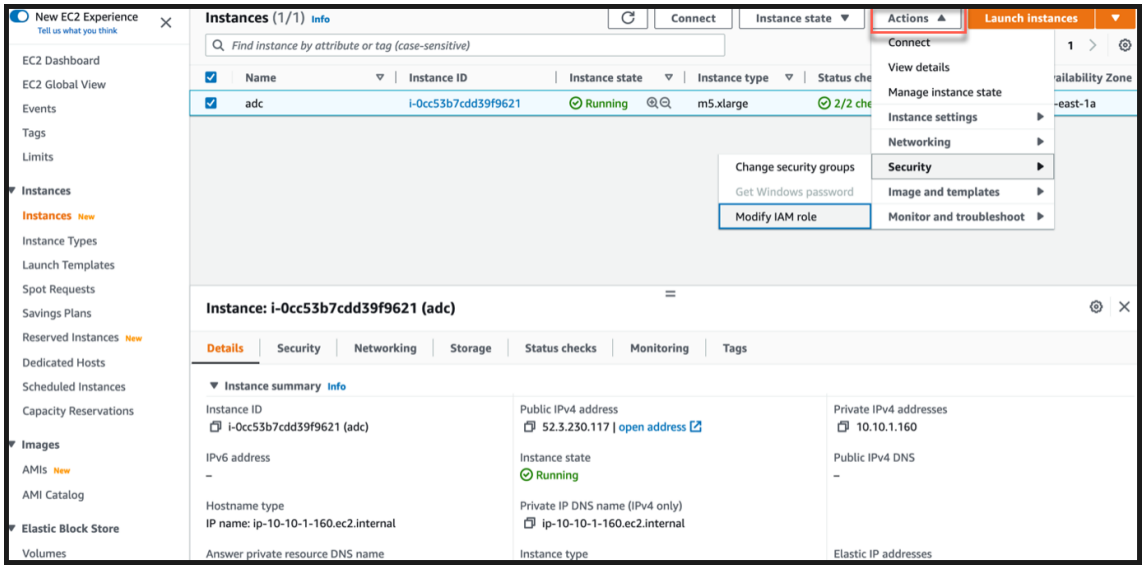
Dieses Verfahren beschreibt, wie Sie eine IAM-Rolle für die AWS-Back-End-Autoscaling-Funktion erstellen.

> **Hinweis:**
>
> Sie können dasselbe Verfahren anwenden, um alle IAM-Rollen zu erstellen, die anderen Funktionen entsprechen.

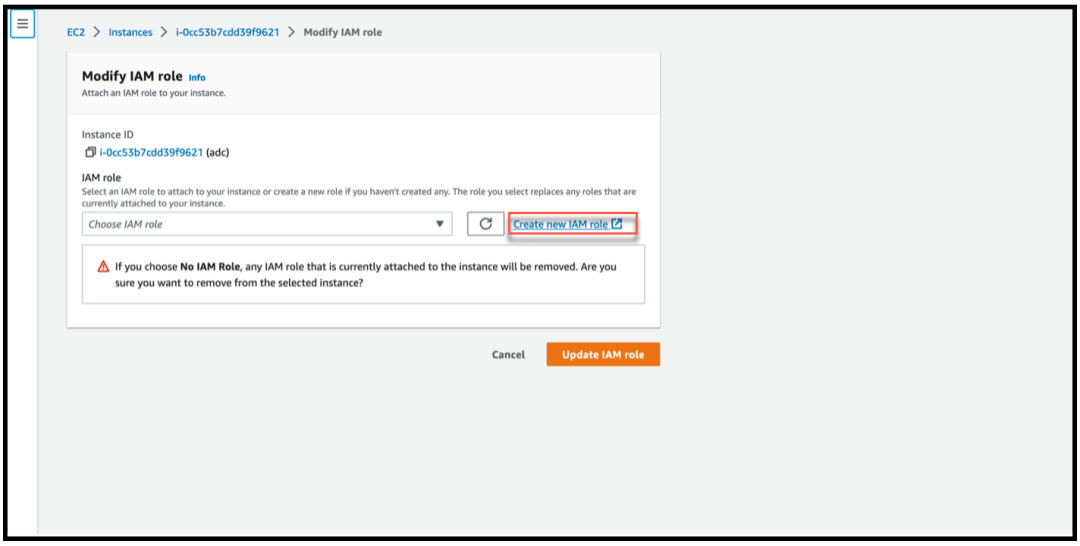
1. Melden Sie sich an der AWS-Managementkonsole für EC2an.
2. Gehen Sie zur EC2-Instanz-Seite und wählen Sie Ihre ADC-Instanz aus.



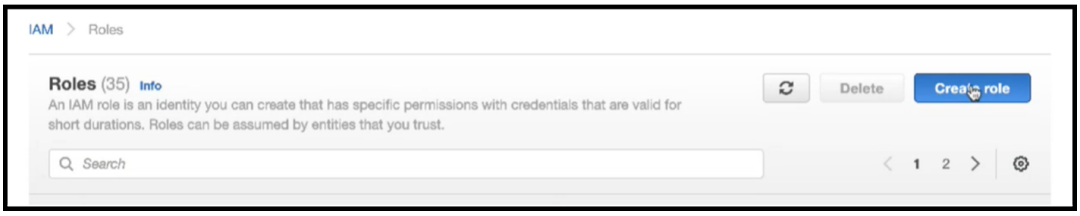
3. Navigieren Sie zu **Aktionen > Sicherheit > IAM-Rolle ändern**.



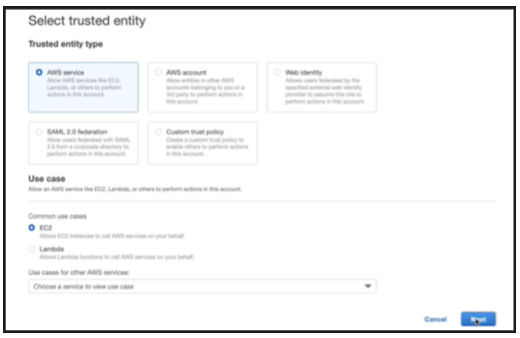
4. Auf der Seite “ **IAM-Rolle ändern** “ können Sie entweder eine bestehende IAM-Rolle auswählen oder eine IAM-Rolle erstellen.
5. Gehen Sie wie folgt vor, um eine IAM-Rolle zu erstellen:
   a) Klicken Sie auf der Seite “ **IAM-Rolle ändern** “ auf **Neue IAM-Rolle erstellen**.



   b) Klicken Sie auf der Seite **Rollen** auf **Rolle erstellen**.



   c) Wählen Sie **AWS-Service** unter **Trusted Entity Type** und **EC2** unter **Common Use Cases** aus und klicken Sie dann auf **Weiter**.



d) Klicken Sie auf der Seite " **Berechtigungen hinzufügen** " auf **Richtlinie erstellen**.

e) Klicken Sie auf den **JSON-Tab**, um den JSON-Editor zu öffnen.

f) Löschen Sie im JSON-Editor alles und fügen Sie die IAM-Berechtigungen für die Funktion ein, die Sie verwenden möchten.

Fügen Sie beispielsweise die folgenden IAM-Berechtigungen für die AWS-Back-End-Autoscaling-Funktion ein:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
```



```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "autoscaling:\*",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListTopics",
                "sns:Subscribe",
                "sqs:CreateQueue",
                "sqs:ListQueues",
                "sqs:DeleteMessage",
                "sqs:GetQueueAttributes",
                "sqs:SetQueueAttributes",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "\*"
        }

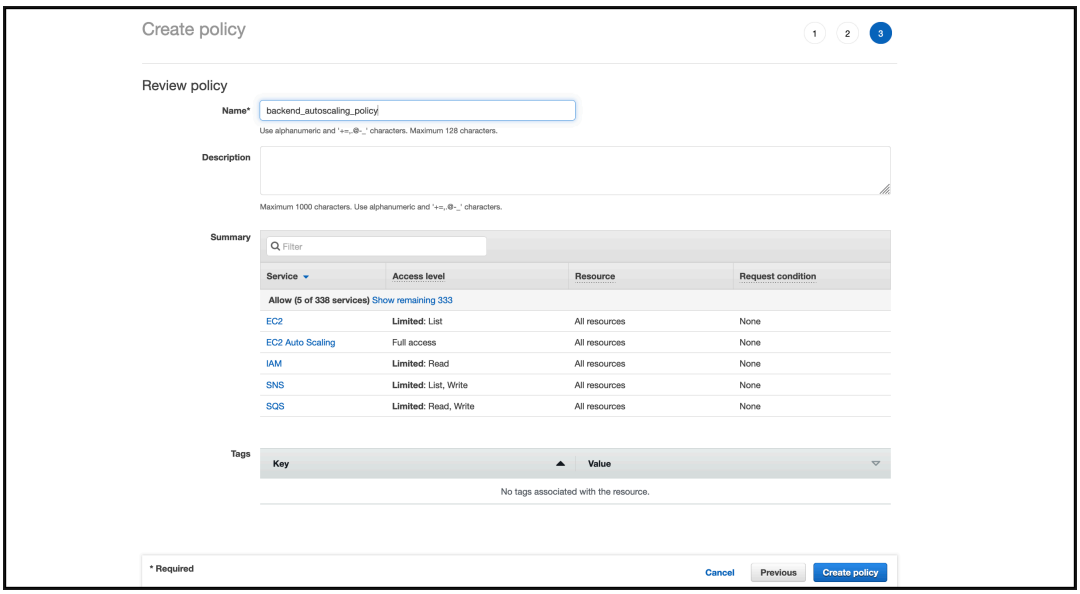
    ]
}


<!--NeedCopy-->
```

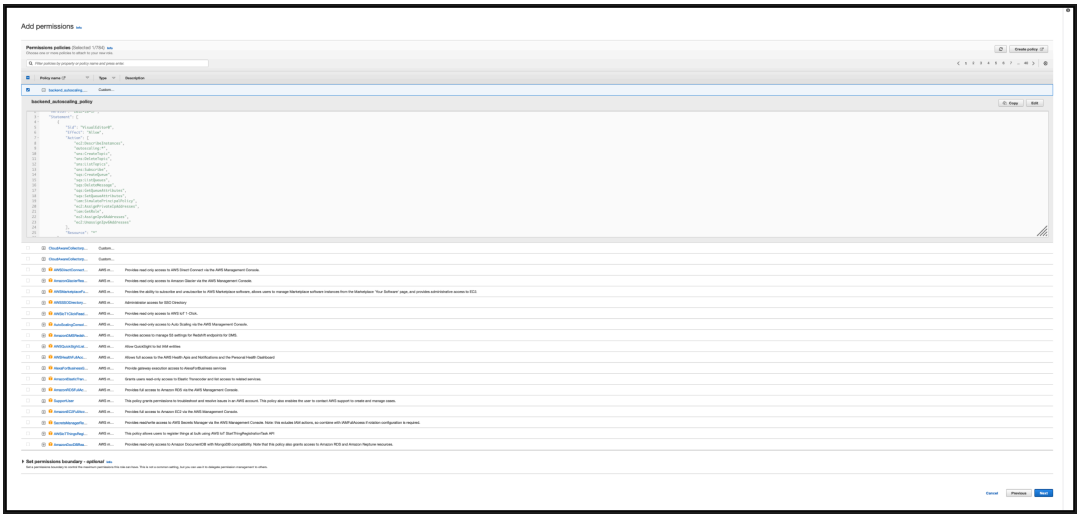
Stellen Sie sicher, dass das Schlüsselwertpaar “Version”, das Sie angeben, mit dem identisch ist, das automatisch von AWS generiert wird.

g) Klicken Sie auf **Weiter: Überprüfen**.

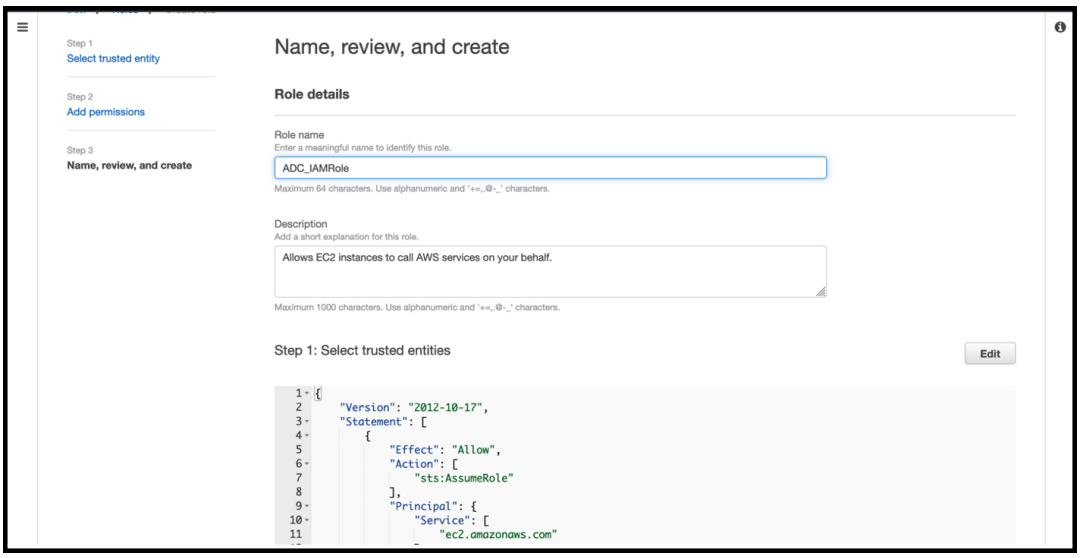
h) Geben Sie auf der Registerkarte **Richtlinie überprüfen** der Richtlinie einen gültigen Namen und klicken Sie auf **Richtlinie erstellen**.



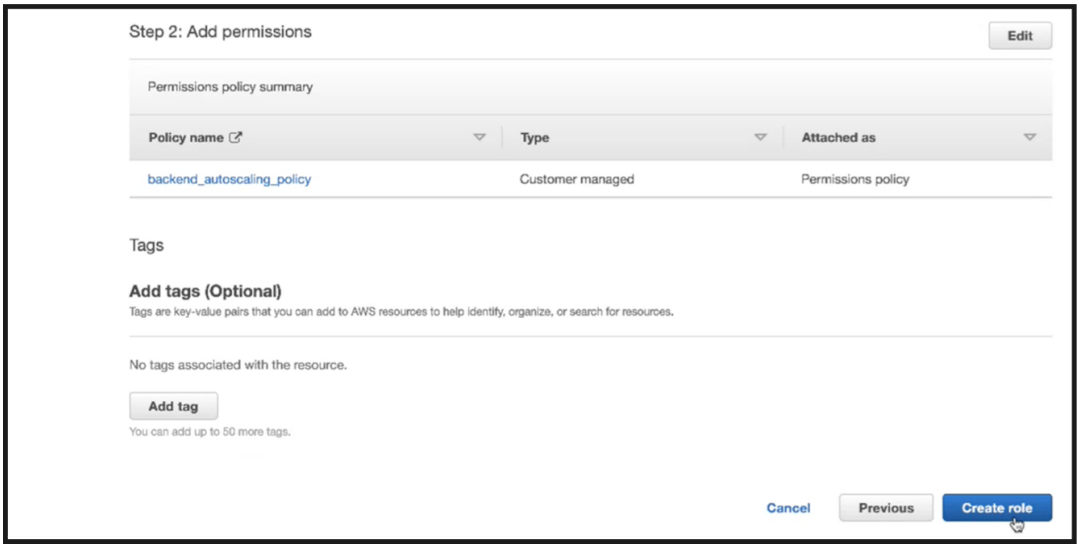
i) Klicken Sie auf der Seite **Identity Access Management** auf den Richtliniennamen, den Sie erstellt haben. Erweitern Sie die Richtlinie, um den gesamten JSON-Code zu überprüfen, und klicken Sie auf **Weiter**.



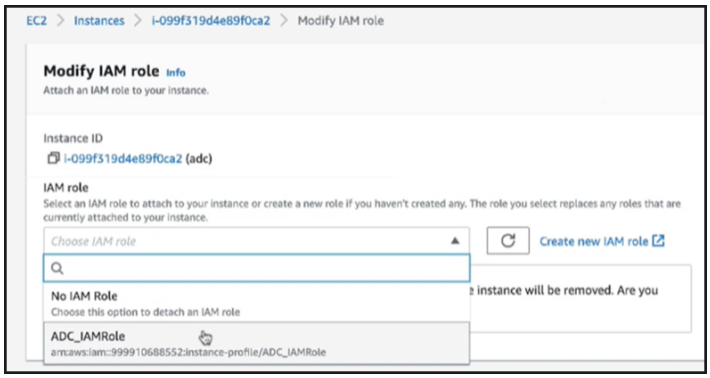
j) Geben Sie der Rolle auf der Seite **Name, Überprüfung und Erstellen** einen gültigen Namen.



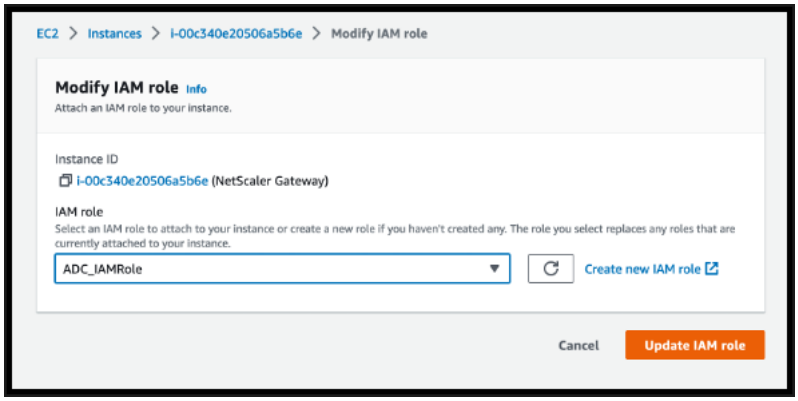
k) Klicken Sie auf **Rolle erstellen**.



6. Wiederholen Sie die Schritte 1, 2 und 3. Wählen Sie die Schaltfläche **Aktualisieren** und dann das Dropdownmenü aus, um die von Ihnen erstellte Rolle zu sehen.



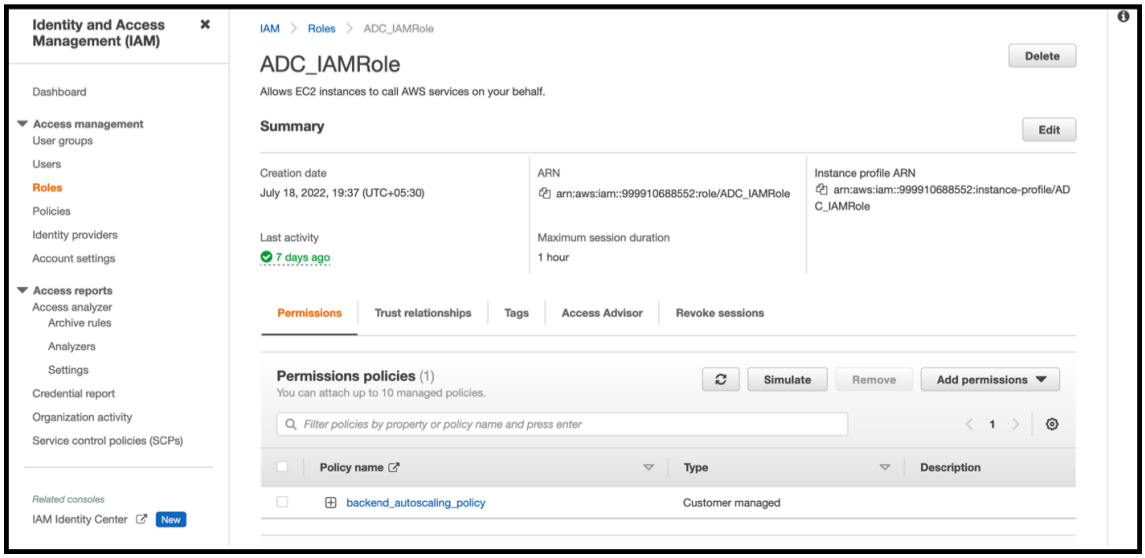
7. Klicken Sie auf **IAM-Rolle aktualisieren**.



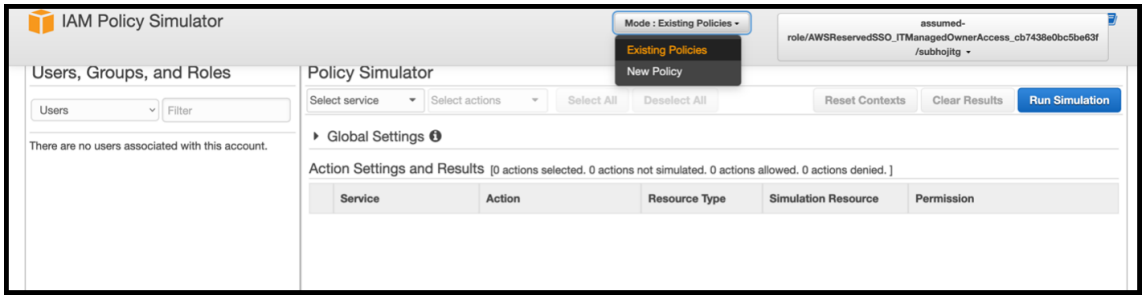
Testen Sie IAM-Richtlinien mit dem IAM-Richtliniensimulator

Der IAM-Richtliniensimulator ist ein Tool, mit dem Sie die Auswirkungen von IAM-Zugriffskontrollrichtlinien testen können, bevor Sie sie in die Produktion übernehmen. Es ist einfacher, Berechtigungen zu überprüfen und Fehler zu beheben.

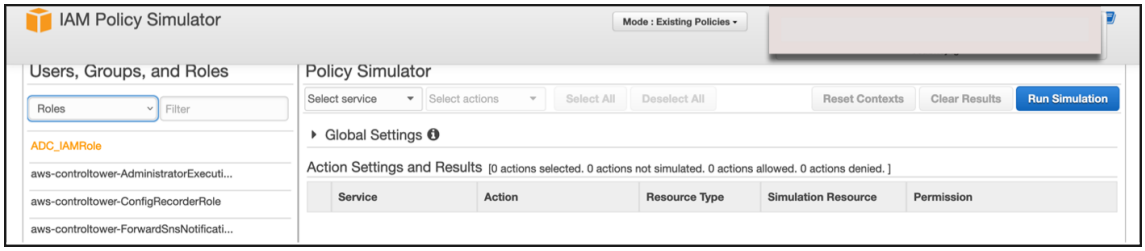
1. Wählen Sie auf der **IAM-Seite** die IAM-Rolle aus, die Sie testen möchten, und klicken Sie auf **Simulieren**. Im folgenden Beispiel ist “ADC_IAMRole” die IAM-Rolle.



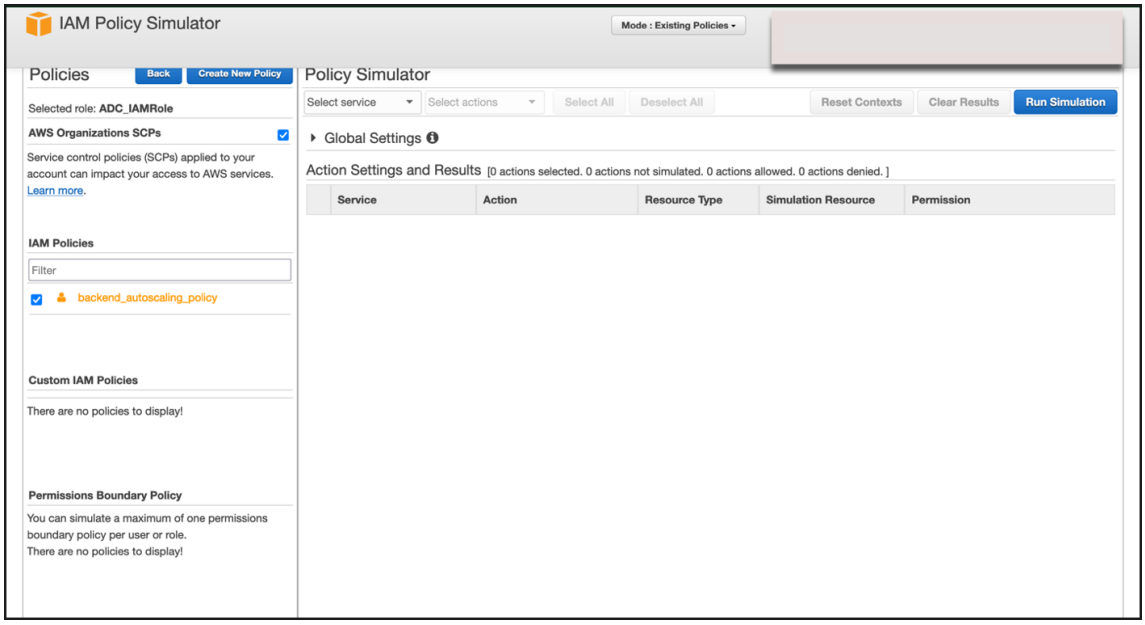
2. Wählen Sie in der **IAM-Policy Simulator-KonsoleExisting Policies**als**Modus** aus.



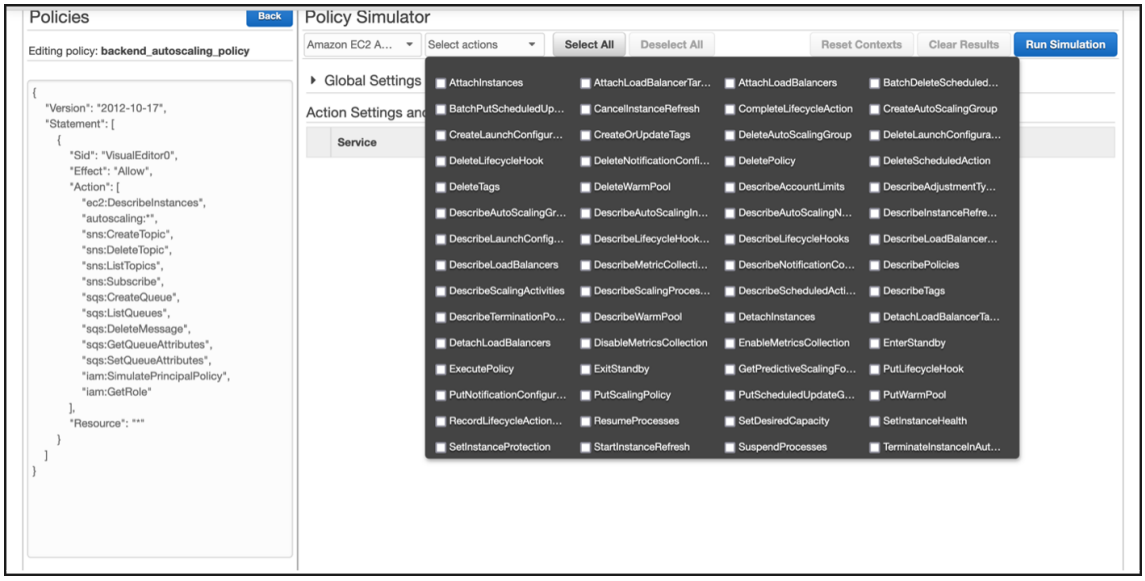
3. Wählen Sie auf der Registerkarte **Benutzer, Gruppen und Rollen** die Option **Rollen** aus dem Dropdownmenü aus und wählen Sie eine vorhandene Rolle aus.



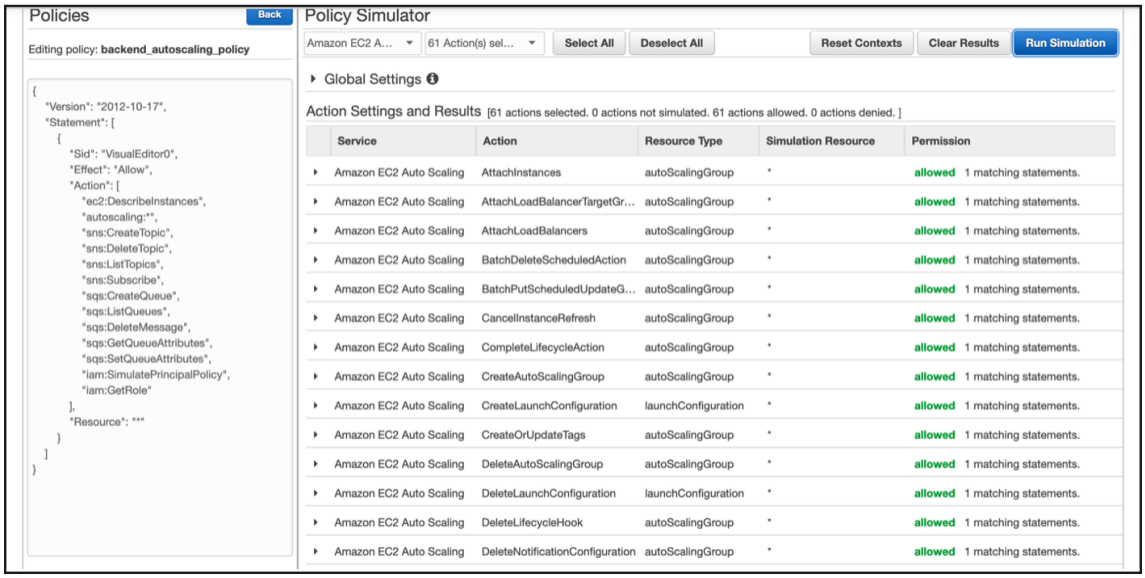
4. Nachdem Sie die vorhandene Rolle ausgewählt haben, wählen Sie die darunter befindliche Richtlinie aus.



5. Nachdem Sie die Richtlinie ausgewählt haben, können Sie den genauen JSON-Code auf der linken Seite des Bildschirms sehen. Wählen Sie die gewünschten Aktionen im Dropdownmenü **Aktionen auswählen** aus.



6. Klicken Sie auf **Simulation ausführen**.



Detaillierte Informationen finden Sie in der AWS IAM-Dokumentation.

Andere Referenzen

Verwenden einer IAM-Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf Amazon EC2-Instanzen ausgeführt werden

So funktioniert eine NetScaler VPX-Instanz auf AWS

May 11, 2023

Die NetScaler VPX-Instance ist als AMI im AWS-Marketplace verfügbar und kann als EC2-Instance innerhalb einer AWS-VPC gestartet werden. Die NetScaler VPX AMI-Instanz benötigt mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher. Eine EC2-Instanz, die in einer AWS VPC gestartet wird, kann auch die für die VPX-Konfiguration erforderlichen Schnittstellen, mehrere IP-Adressen pro Schnittstelle sowie öffentliche und private IP-Adressen bereitstellen. Jede VPX-Instanz benötigt mindestens drei IP-Subnetze:

- Ein Management-Subnetz
- Ein Client-Subnetz (VIP)
- Ein Subnetz mit Back-End-Ausrichtung (SNIP, MIP usw.)

Citrix empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz in der AWS-Installation.

AWS stellt derzeit Multi-IP-Funktionen nur für Instances zur Verfügung, die in einer AWS-VPC ausgeführt werden. Eine VPX-Instanz in einer VPC kann zum Lastausgleich von Servern verwendet werden, die in EC2-Instanzen ausgeführt werden. Mit einer Amazon VPC können Sie eine virtuelle Netzwerkumgebung erstellen und steuern, einschließlich Ihres eigenen IP-Adressbereichs, Subnetze, Routing-Tabellen und Netzwerk-Gateways.

Hinweis: Standardmäßig können Sie bis zu 5 VPC-Instances pro AWS-Region für jedes AWS-Konto erstellen. Sie können höhere VPC-Limits beantragen, indem Sie das Antragsformular http://aws.amazon.com/contact-us/vpc-requestvon Amazon einreichen.

Abbildung 1. Ein Beispiel für die Bereitstellung einer NetScaler VPX-Instance auf der AWS-Architektur

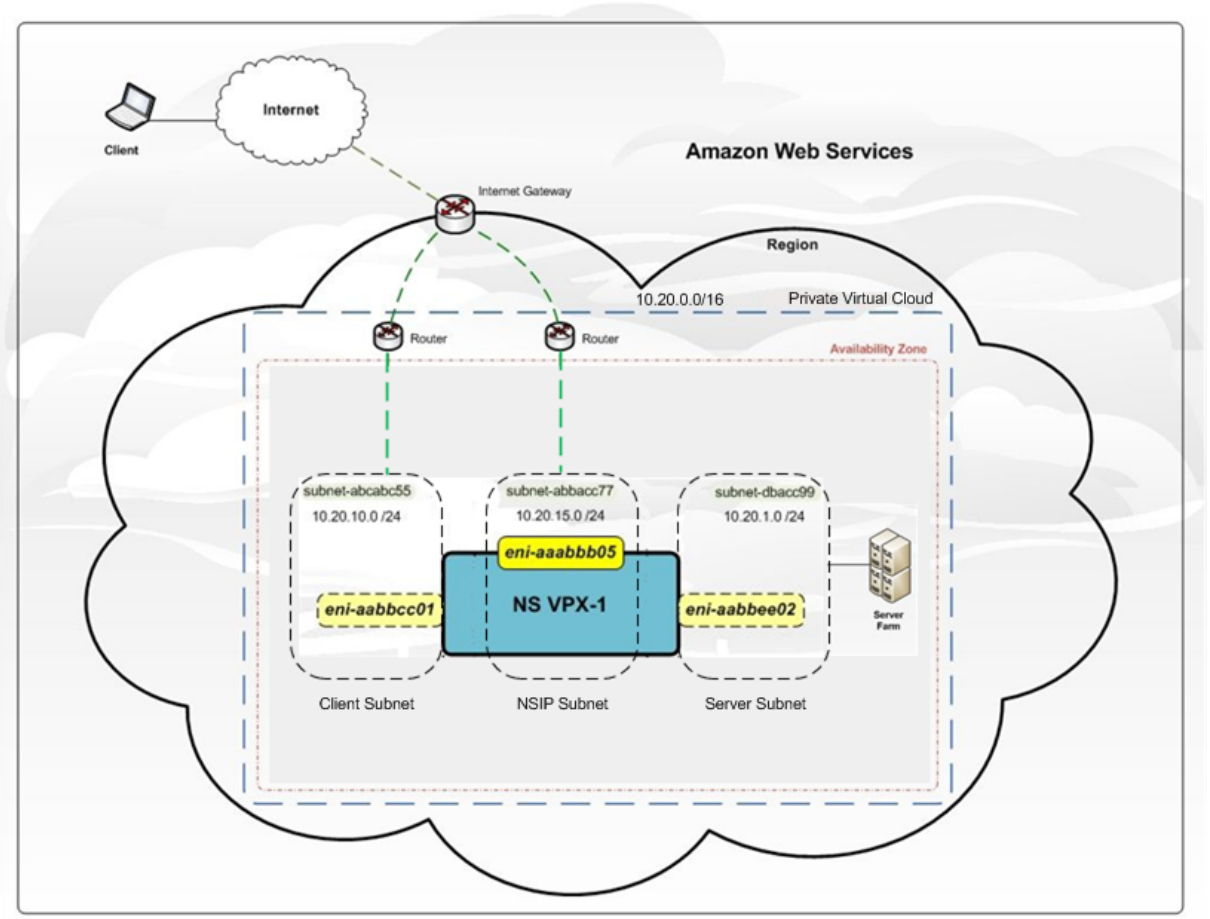


Abbildung 1 zeigt eine einfache Topologie einer AWS-VPC mit einer NetScaler VPX-Bereitstellung. Die AWS-VPC hat:

1. Ein einzelnes Internet-Gateway zum Weiterleiten des Datenverkehrs in und aus der VPC.
2. Netzwerkkonnektivität zwischen dem Internet-Gateway und dem Internet.
3. Drei Subnetze, jeweils eines für Management, Client und Server.
4. Netzwerkkonnektivität zwischen dem Internet-Gateway und den beiden Subnetzen (Management und Client).
5. Eine eigenständige NetScaler VPX-Instanz, die innerhalb der VPC bereitgestellt wird. Die VPX-Instanz verfügt über drei ENIs, eine mit jedem Subnetz verbunden.

Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS

May 11, 2023

Sie können eine eigenständige NetScaler VPX-Instance auf AWS bereitstellen, indem Sie die folgenden Optionen verwenden:

- AWS-Webkonsole
- Von Citrix verfasste CloudFormation-Vorlage
- AWS CLI

In diesem Thema wird das Verfahren zur Bereitstellung einer NetScaler VPX-Instance auf AWS beschrieben.

Lesen Sie die folgenden Themen, bevor Sie mit der Bereitstellung beginnen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Stellen Sie mithilfe der AWS-Webkonsole eine NetScaler VPX-Instance auf AWS bereit

Sie können eine NetScaler VPX-Instance auf AWS über die AWS-Webkonsole bereitstellen. Der Bereitstellungsprozess umfasst die folgenden Schritte:

1. Erstellen eines Schlüsselpaars
2. Erstellen einer Virtual Private Cloud (VPC)
3. Weitere Subnetze hinzufügen
4. Erstellen von Sicherheitsgruppen und Sicherheitsregeln
5. Routentabellen hinzufügen
6. Erstellen Sie ein Internet-Gateway
7. Erstellen Sie eine NetScaler VPX-Instanz
8. Weitere Netzwerkschnittstellen erstellen und anhängen
9. Elastische IPs an die Management-NIC anhängen
10. Herstellen einer Verbindung mit der VPX-Instanz

Schritt 1: Erstellen Sie ein Schlüsselpaar.

Amazon EC2 verwendet ein Schlüsselpaar, um Anmeldeinformationen zu verschlüsseln und zu entschlüsseln. Um sich bei Ihrer Instance anzumelden, müssen Sie ein Schlüsselpaar erstellen, den Namen des Schlüsselpaars angeben, wenn Sie die Instance starten, und den privaten Schlüssel angeben, wenn Sie eine Verbindung zur Instance herstellen.

Wenn Sie eine Instanz mit dem AWS Launch Instance Wizard überprüfen und starten, werden Sie aufgefordert, ein vorhandenes Schlüsselpaar zu verwenden oder ein neues Schlüsselpaar zu erstellen. Weitere Informationen zum Erstellen eines Schlüsselpaars finden Sie unter Amazon EC2-Schlüsselpaare.

Schritt 2: Erstellen einer VPC.

Eine NetScaler VPC-Instanz wird in einer AWS VPC bereitgestellt. Mit einer VPC können Sie das virtuelle Netzwerk definieren, das Ihrem AWS-Konto gewidmet ist. Weitere Informationen zu AWS VPC finden Sie unter Erste Schritte mit Amazon VPC.

Beachten Sie beim Erstellen einer VPC für Ihre NetScaler VPX-Instanz die folgenden Punkte:

- Verwenden Sie die Option VPC with a Single Public Subnet, um eine AWS-VPC in einer AWS-Availability Zone zu erstellen.
- Citrix empfiehlt, mindestens **drei Subnetze**der folgenden Typen zu erstellen:
  - Ein Subnetz für den Verwaltungsdatenverkehr. Sie platzieren die Management-IP (NSIP) in diesem Subnetz. Standardmäßig wird das Elastic Network Interface (ENI) eth0 für die Management-IP verwendet.
  - Ein oder mehrere Subnetze für den Clientzugriffsverkehr (User-to-NetScaler VPX), über die Clients eine Verbindung zu einer oder mehreren virtuellen IP (VIP) -Adressen herstellen, die den virtuellen Servern des NetScaler Load Balancing zugewiesen sind.
  - Ein oder mehrere Subnetze für den Serverzugriffsverkehr (VPX-to-Server), über den Ihre Server eine Verbindung zu VPX-eigenen Subnetz-IP-Adressen (SNIP) herstellen. Weitere Informationen zum NetScaler-Lastenausgleich und zu virtuellen Servern, virtuellen IP-Adressen (VIPs) und Subnetz-IP-Adressen (SNIPs) finden Sie unter:
  - Alle Subnetze müssen sich in derselben Availability Zone befinden.

Schritt 3: Fügen Sie Subnetzehinzu.

Als Sie den VPC-Assistenten verwendet haben, wurde nur ein Subnetz erstellt. Je nach Anforderung möchten Sie möglicherweise weitere Subnetze erstellen. Weitere Informationen zum Erstellen weiterer Subnetze finden Sie unter Hinzufügen eines Subnetzes zu Ihrer VPC.

Schritt 4: Erstellen von Sicherheitsgruppen und Sicherheitsregeln.

Um eingehenden und ausgehenden Datenverkehr zu steuern, erstellen Sie Sicherheitsgruppen und fügen Sie den Gruppen Regeln hinzu. Weitere Informationen zum Erstellen von Gruppen und zum Hinzufügen von Regeln finden Sie unter Sicherheitsgruppen für Ihre VPC.

Für NetScaler VPX -Instanzen stellt der EC2-Assistent Standardsicherheitsgruppen bereit, die von AWS Marketplace generiert werden und auf empfohlenen Einstellungen von Citrix basieren. Sie können jedoch je nach Ihren Anforderungen weitere Sicherheitsgruppen erstellen.

> **Hinweis**
>
> Port 22, 80, 443, der in der Sicherheitsgruppe jeweils für den SSH-, HTTP- und HTTPS-Zugriff geöffnet wird.

Schritt 5: Fügen Sie Routentabellenhinzu.

Die Routentabelle enthält eine Reihe von Regeln, die als Routen bezeichnet werden und anhand derer bestimmt wird, wohin der Netzwerkverkehr geleitet wird. Jedes Subnetz in Ihrer VPC muss einer Routentabelle zugeordnet sein. Weitere Informationen zum Erstellen einer Routentabelle finden Sie unter Routentabellen.

Schritt 6: Erstellen Sie ein Internet-Gateway.

Ein Internet-Gateway dient zwei Zwecken: der Bereitstellung eines Ziels in Ihren VPC-Routing-Tabellen für internetfähigen Datenverkehr und der Durchführung von Netzwerkadressübersetzungen

(NAT) für Instanzen, denen öffentliche IPv4-Adressen zugewiesen wurden.

Erstellen Sie ein Internet-Gateway für den Internetverkehr. Weitere Informationen zum Erstellen eines Internet-Gateways finden Sie im Abschnitt Anhängen eines Internet-Gateways.

Schritt 7: Erstellen Sie eine NetScaler VPX-Instanz mithilfe des AWS EC2-Dienstes.

Gehen Sie wie folgt vor, um mithilfe des AWS EC2-Service eine NetScaler VPX-Instance zu erstellen.

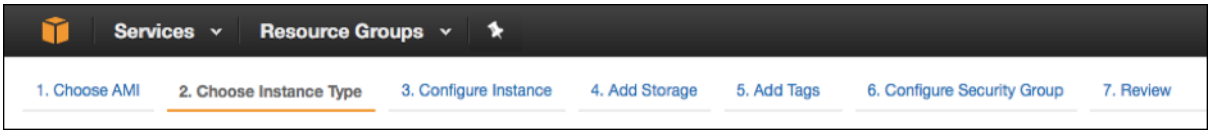
1. Gehen Sie im AWS-Dashboard zu **Compute > EC2 > Launch Instance > AWS Marketplace**.

   Bevor Sie auf **Launch Instance**klicken, stellen Sie sicher, dass Ihre Region korrekt ist, indem Sie den Hinweis überprüfen, der unter **Launch Instance**erscheint.

2. Suchen Sie in der Leiste Search AWS Marketplace nach dem Schlüsselwort NetScaler VPX.
3. Wählen Sie die Version aus, die Sie bereitstellen möchten, und klicken Sie dann auf **Auswählen**. Für die NetScaler VPX-Version haben Sie folgende Optionen:
   - Eine lizenzierte Version
   - NetScaler VPX Express Appliance (Dies ist eine kostenlose virtuelle Appliance, die ab NetScaler 12.0 56.20 verfügbar ist.)
   - Bringen Sie Ihr eigenes Gerät

Der Assistent Instance starten wird gestartet. Folgen Sie dem Assistenten, um eine Instanz zu erstellen. Der Assistent fordert Sie auf:

- Instanztyp auswählen
- Instanz konfigurieren
- Speicher hinzufügen
- Tags hinzufügen
- Sicherheitsgruppe konfigurieren
- Bewertung



Schritt 8: Weitere Netzwerkschnittstellen erstellen und anhängen.

Erstellen Sie zwei weitere Netzwerkschnittstellen für VIP und SNIP. Weitere Informationen zum Erstellen weiterer Netzwerkschnittstellen finden Sie im Abschnitt Erstellen einer Netzwerkschnittstelle .

Nachdem Sie die Netzwerkschnittstellen erstellt haben, müssen Sie sie an die VPX-Instanz anhängen. Fahren Sie vor dem Anfügen der Schnittstelle die VPX-Instanz herunter, schließen Sie die Schnittstelle an und schalten Sie die Instanz ein. Weitere Informationen zum Anhängen von Netzwerkschnittstellen finden Sie im Abschnitt Anhängen einer Netzwerkschnittstelle beim Starten einer Instanz .

Schritt 9: Zuweisen und Zuordnen von elastischen IPs.

Wenn Sie einer EC2-Instance eine öffentliche IP-Adresse zuweisen, bleibt diese nur so lange zugewiesen, bis die Instance gestoppt wird. Danach wird die Adresse wieder in den Pool freigegeben. Wenn Sie die Instance neu starten, wird eine neue öffentliche IP-Adresse zugewiesen.

Im Gegensatz dazu bleibt eine elastische IP-Adresse (EIP) zugewiesen, bis die Adresse von einer Instanz getrennt wird.

Weisen Sie eine elastische IP für die Management-NIC zu und ordnen Sie sie zu. Weitere Informationen zur Zuweisung und Zuordnung von elastischen IP-Adressen finden Sie in den folgenden Themen:

- Zuweisen einer elastischen IP-Adresse
- Eine Elastic IP-Adresse mit einer laufenden Instance verknüpfen

Diese Schritte vervollständigen das Verfahren zur Erstellung einer NetScaler VPX-Instance auf AWS. Es kann einige Minuten dauern, bis die Instanz fertig ist. Vergewissern Sie sich, dass Ihre Instance ihre Statusprüfungen bestanden hat. Sie können diese Informationen in der Spalte **Status Checks** auf der Seite Instances einsehen.

Schritt 10: Stellen Sie eine Verbindung zur VPX-Instanzher.

Nachdem Sie die VPX-Instanz erstellt haben, verbinden Sie die Instanz mithilfe der GUI und eines SSH-Clients.

- Grafische Benutzeroberfläche (GUI)

Im Folgenden finden Sie die standardmäßigen Administratoranmeldeinformationen für den Zugriff auf eine NetScaler VPX-Instanz.

Benutzername: `nsroot`

Passwort: Das Standardkennwort für das ns-Root-Konto ist auf die AWS-Instance-ID der NetScaler VPX-Instance festgelegt. Bei Ihrer ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Passwort zu ändern. Nachdem Sie das Kennwort geändert haben, müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu gestartet wird, müssen Sie sich mit dem Standardkennwort anmelden. Ändern Sie das Passwort erneut, wenn Sie dazu aufgefordert werden.

- SSH-Client

Wählen Sie in der AWS-Managementkonsole die NetScaler VPX-Instance aus und klicken Sie auf Verbinden. Folgen Sie den Anweisungen auf der Seite **Mit Ihrer Instance verbinden** .

Weitere Informationen zum Bereitstellen einer eigenständigen NetScaler VPX-Instanz in AWS mithilfe der AWS-Webkonsole finden Sie unter:

- Szenario: Standalone-Instanz
- So konfigurieren Sie eine NetScaler VPX-Instanz auf AWS mithilfe der Citrix CloudFormation-Vorlage

Konfigurieren Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage

Sie können die von Citrix bereitgestellte CloudFormation-Vorlage verwenden, um den Start der VPX-Instance zu automatisieren. Die Vorlage bietet Funktionen zum Starten einer einzelnen NetScaler VPX-Instance oder zum Erstellen einer Hochverfügbarkeitsumgebung mit zwei NetScaler VPX-Instances.

Sie können die Vorlage über AWS Marketplace oder GitHub starten.

Die CloudFormation-Vorlage erfordert eine bestehende VPC-Umgebung und startet eine VPX-Instance mit drei elastischen Netzwerkschnittstellen (ENIs). Bevor Sie mit der CloudFormation-Vorlage beginnen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Eine virtuelle Private Cloud (VPC) von AWS
- Drei Subnetze innerhalb der VPC: eines für die Verwaltung, eines für den Client-Verkehr und eines für Back-End-Server
- Ein EC2-Schlüsselpaar, um den SSH-Zugriff auf die Instance zu ermöglichen
- Eine Sicherheitsgruppe mit UDP 3003, TCP 3009—3010, HTTP, SSH-Ports geöffnet

Weitere Informationen zum Vervollständigen der Voraussetzungen finden Sie im Abschnitt Bereitstellen einer NetScaler VPX-Instanz auf AWS mit der AWS Web Console oder in der AWS-Dokumentation.

In diesem Video erfahren Sie, wie Sie eine eigenständige NetScaler VPX-Instanz mithilfe der im AWS Marketplace verfügbaren Citrix CloudFormation-Vorlage konfigurieren und starten können.

Darüber hinaus konfigurieren und starten Sie eine eigenständige NetScaler VPX Express-Instanz mithilfe der in GitHub verfügbaren Citrix CloudFormation-Vorlage:

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

Eine IAM-Rolle ist für eine eigenständige Bereitstellung nicht zwingend erforderlich. Citrix empfiehlt jedoch, dass Sie eine IAM-Rolle mit den erforderlichen Rechten erstellen und der Instanz zuordnen, um sie in Zukunft benötigen zu können. Die IAM-Rolle stellt sicher, dass die eigenständige Instanz bei Bedarf problemlos mit SR-IOV in einen Hochverfügbarkeitsknoten konvertiert wird.

Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Konfigurieren von NetScaler VPX-Instanzen für die Verwendung der SR-IOV-Netzwerkschnittstelle.

> Hinweis
> Wenn Sie eine NetScaler VPX-Instanz unter AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert. Wenn Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, ist die Standardoption Ja. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie Nein. Weitere Informationen finden Sie unter Überwachen Ihrer Instanzen mit Amazon CloudWatch

Konfigurieren einer NetScaler VPX-Instanz mithilfe der AWS CLI

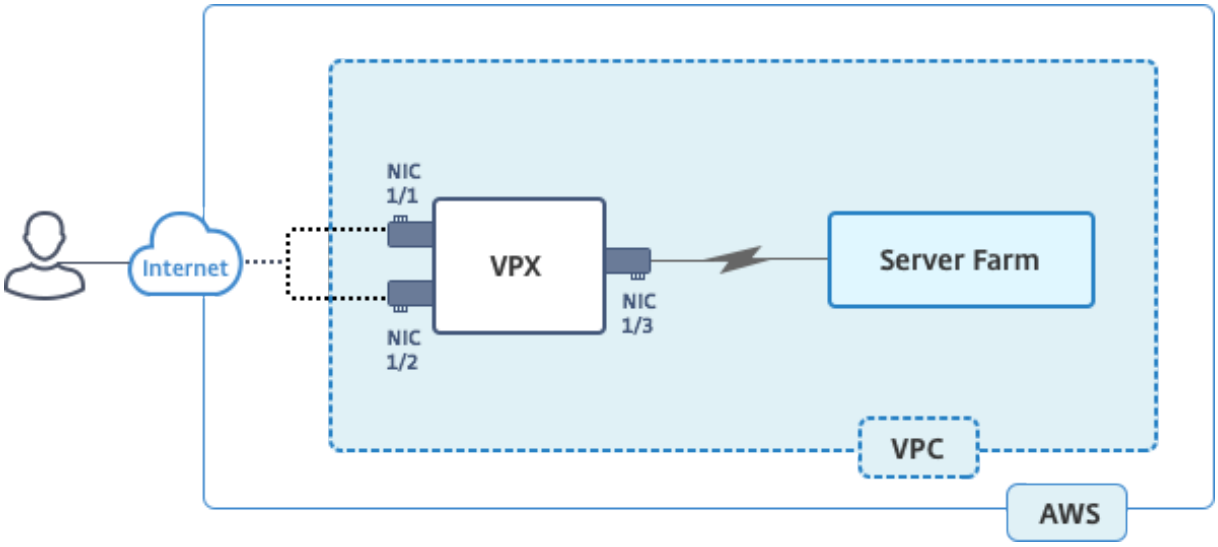
Sie können die AWS CLI zum Starten von Instanzen verwenden. Weitere Informationen finden Sie in der Dokumentation zur AWS-Befehlszeilenschnittstelle.

Szenario: Standalone-Instanz

May 11, 2023

Dieses Szenario zeigt, wie eine eigenständige NetScaler VPX-EC2-Instance in AWS mithilfe der AWS-GUI bereitgestellt wird. Erstellen Sie eine eigenständige VPX-Instanz mit drei NICs. Die Instanz, die als virtueller Lastausgleichsserver konfiguriert ist, kommuniziert mit Backend-Servern (der Serverfarm). Richten Sie für diese Konfiguration die erforderlichen Kommunikationswege zwischen der Instanz und den Back-End-Servern sowie zwischen der Instanz und den externen Hosts im öffentlichen Internet ein.

Weitere Informationen zum Verfahren zum Bereitstellen einer VPX-Instanz finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS.

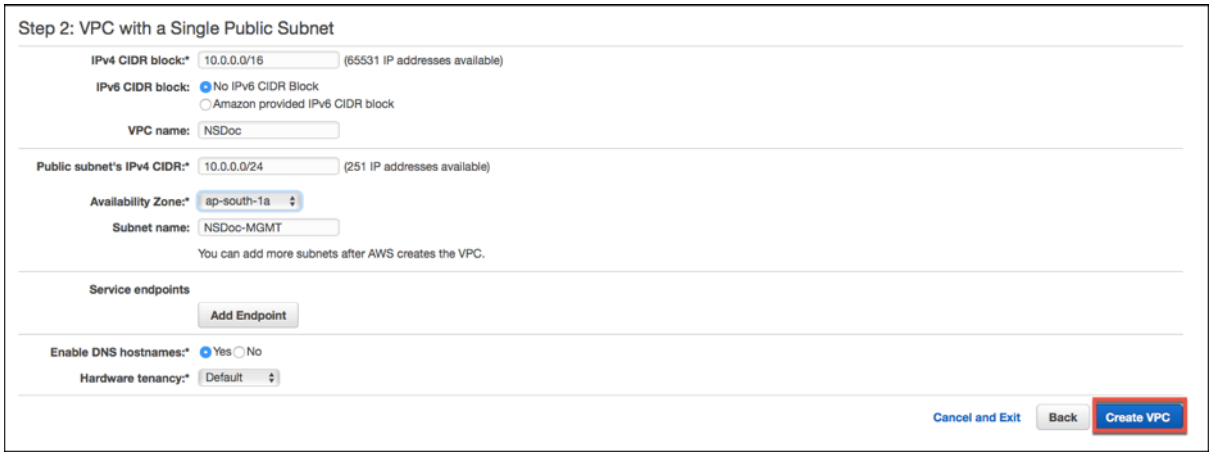


Erstellen Sie drei Netzwerkkarten. Jede NIC kann mit einem Paar von IP-Adressen (öffentlich und privat) konfiguriert werden. Die NICs dienen den folgenden Zwecken.

Netzwerkkarte	Zweck	Verbunden mit
eth0	Dient dem Verwaltungsverkehr (NSIP)	Eine öffentliche IP-Adresse und eine private IP-Adresse
eth1	Dient clientseitigem Datenverkehr (VIP)	Eine öffentliche IP-Adresse und eine private IP-Adresse
eth2	Kommuniziert mit Back-End-Servern (SNIP)	Eine öffentliche IP-Adresse (private IP-Adresse ist nicht erforderlich)

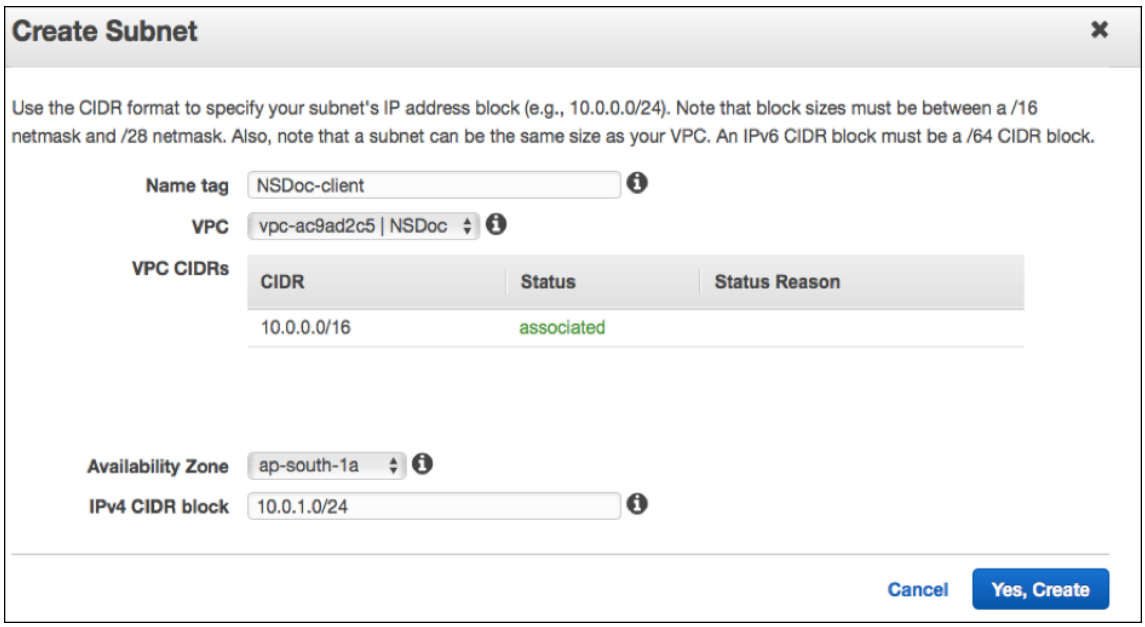
Schritt 1: Erstellen einer VPC.

1. Melden Sie sich an der AWS-Webkonsole an und navigieren Sie zu **Networking & Content Delivery** > **VPC**. Klicken Sie auf **VPC Wizard starten**.
2. **Wählen Sie**VPC mit einem einzigen öffentlichen Subnetz**aus und klicken Sie auf Auswählen.**
3. Stellen Sie den IP-CIDR-Block für dieses Szenario auf 10.0.0.0/16 ein.
4. Geben Sie einen Namen für die VPC ein.
5. Stellen Sie das öffentliche Subnetz auf 10.0.0.0/24 ein. (Dies ist das Verwaltungsnetzwerk).
6. Wählen Sie eine Verfügbarkeitszone aus.
7. Geben Sie einen Namen für das Subnetz an.
8. Klicken Sie auf **VPC**erstellen.

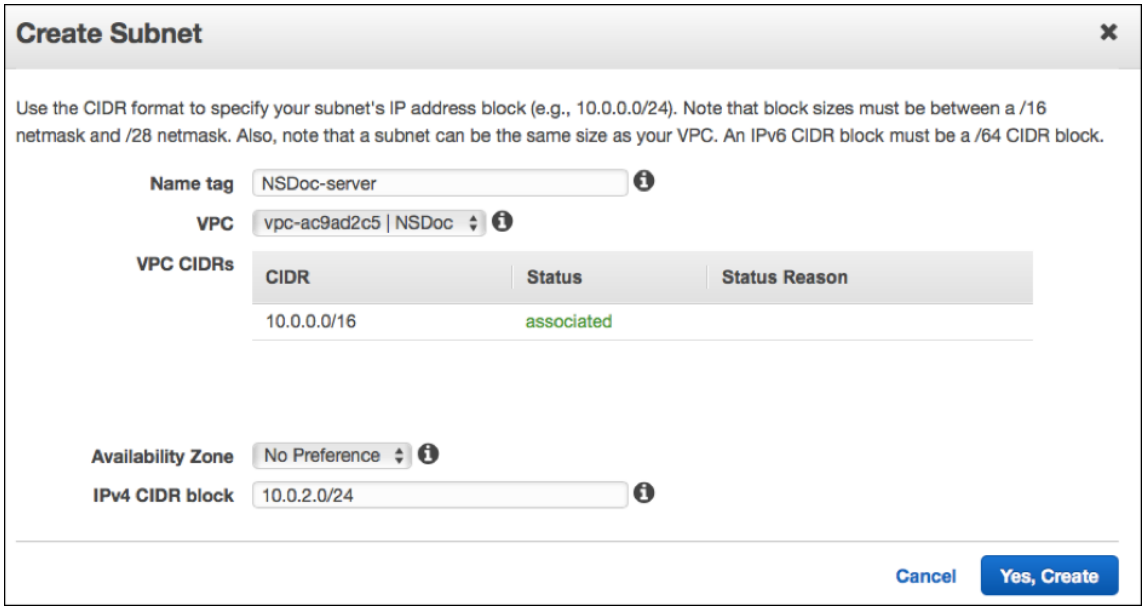


Schritt 2: Erstellen Sie zusätzliche Subnetze.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets, Create Subnet aus, nachdem Sie die folgenden Details eingegeben haben.
   - Namensschild: Geben Sie einen Namen für Ihr Subnetz ein.
   - VPC: Wählen Sie die VPC aus, für die Sie das Subnetz erstellen.
   - Availability Zone: Wählen Sie die Availability Zone aus, in der Sie die VPC in Schritt 1 erstellt haben.
   - IPv4-CIDR-Block: Geben Sie einen IPv4-CIDR-Block für Ihr Subnetz an. Wählen Sie für dieses Szenario 10.0.1.0/24.

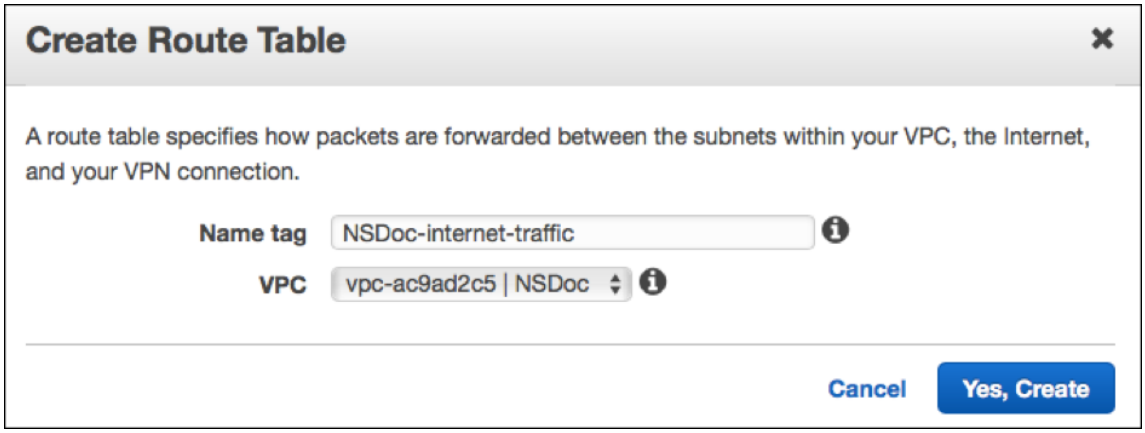


3. Wiederholen Sie die Schritte, um ein weiteres Subnetz für Back-End-Server zu erstellen.



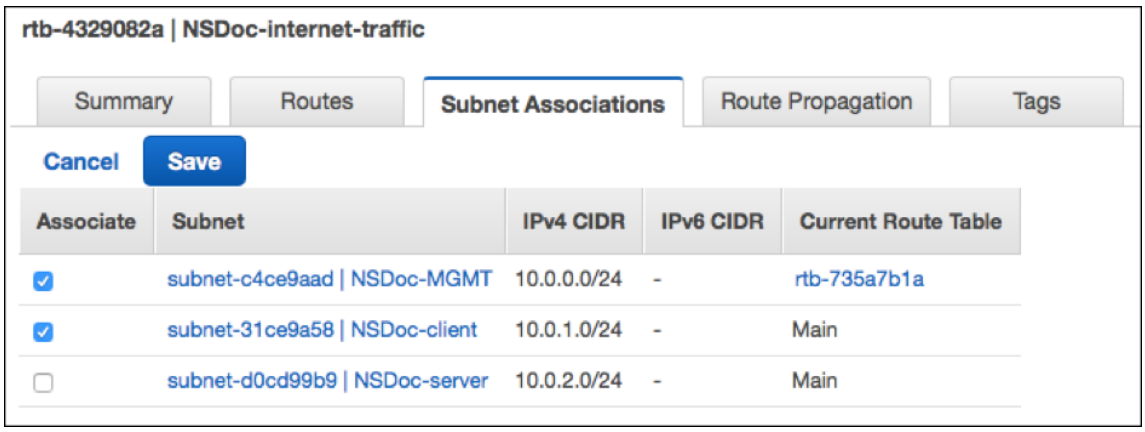
Schritt 3: Erstellen Sie eine Routentabelle.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich **Routing Tables** > **Create Routing Table.**
3. Fügen Sie im Fenster Create Route Table einen Namen hinzu und wählen Sie die VPC aus, die Sie in Schritt 1 erstellt haben.
4. Klicken Sie auf **Yes, Create**.



   Die Routing-Tabelle wird allen Subnetzen zugewiesen, die Sie für diese VPC erstellt haben, so dass das Routing von Datenverkehr von einer Instanz in einem Subnetz eine Instanz in einem anderen Subnetz erreichen kann.

5. Klicken Sie auf Subnetzzuordnungen, und klicken Sie dann auf Bearbeiten.
6. Klicken Sie auf das Management- und Client-Subnetz und dann auf Speichern. Dadurch wird eine Routentabelle nur für den Internetverkehr erstellt.



7. Klicken Sie auf **Routen > Bearbeiten > Weitere Route hinzufügen**.
8. Fügen Sie im Feld Ziel 0.0.0.0/0 hinzu und klicken Sie auf das Zielfeld, um das Internetgateway igw-<xxxx> auszuwählen, das der VPC-Assistent automatisch erstellt hat.
9. Klicken Sie auf Speichern.

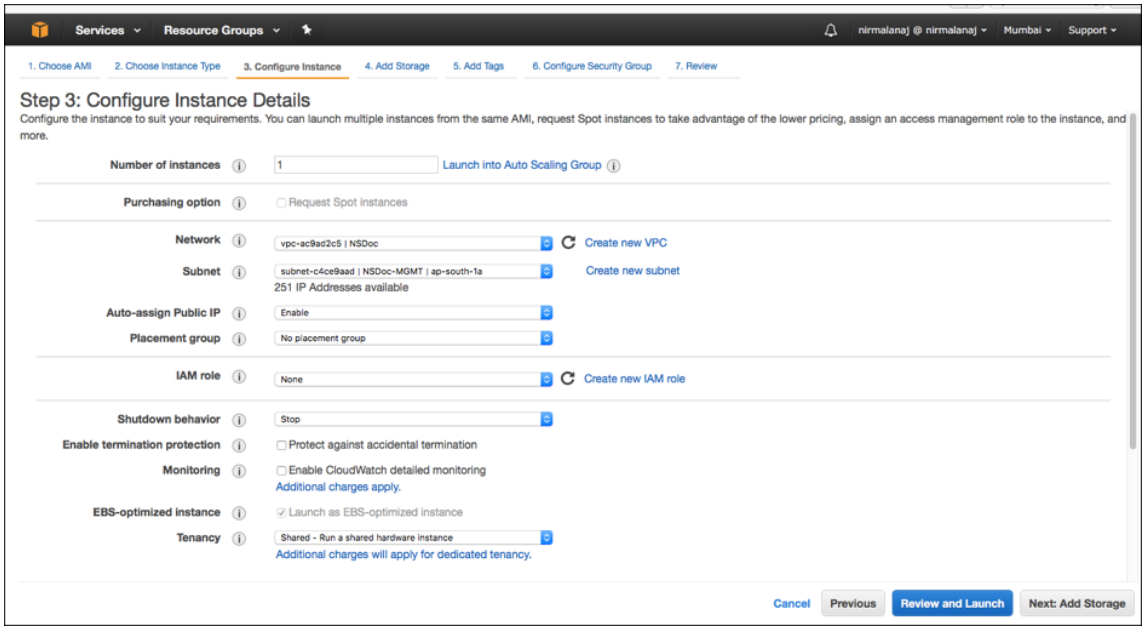
10. Folgen Sie den Schritten, um eine Routentabelle für serverseitigen Verkehr zu erstellen.

Schritt 4: Erstellen Sie eine NetScaler VPX-Instanz.

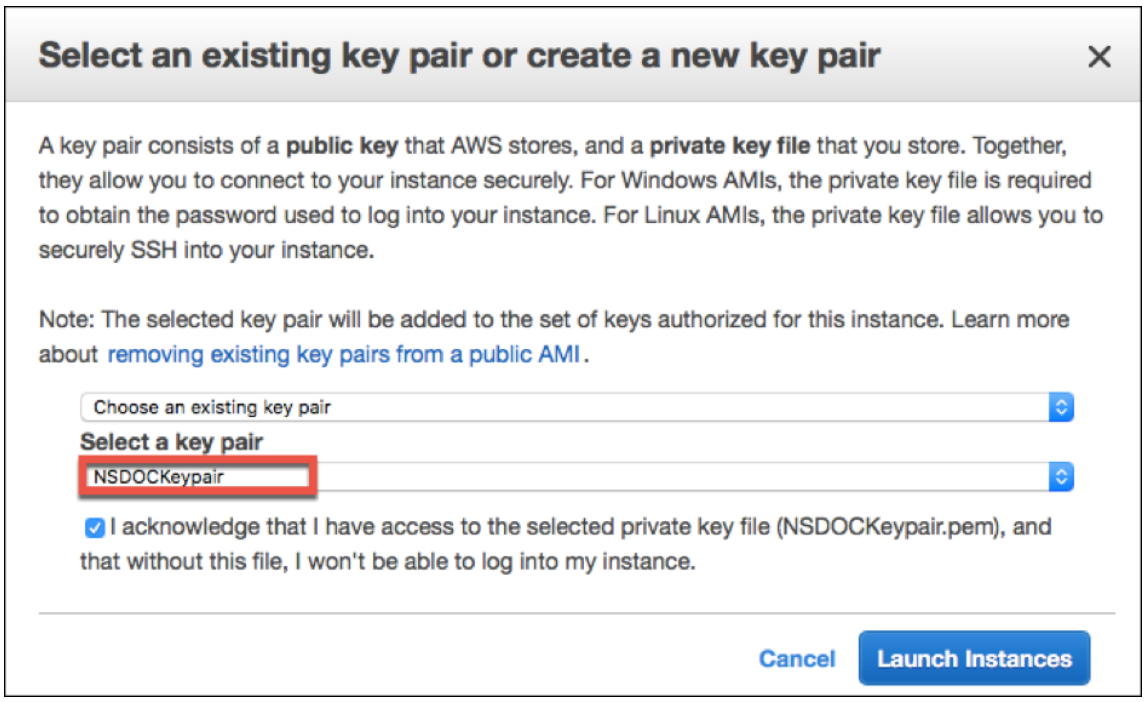
1. Melden Sie sich an der AWS-Managementkonsole an und klicken Sie unter **Compute** auf **EC2**.
2. Klicken Sie auf AWS Marketplace. Geben Sie in der Suchleiste von AWS Marketplace NetScaler VPX ein und drücken Sie die Eingabetaste. Die verfügbaren NetScaler VPX-Editionen werden angezeigt.
3. Klicken Sie auf **Auswählen**, um die gewünschte NetScaler VPX-Edition auszuwählen. Der EC2-Instance-Assistent wird gestartet.
4. **Wählen Sie auf der Seite Choose Instance Type** die Option **m4 aus. Vergrößern Sie die** Größe (empfohlen) und klicken Sie auf **Weiter: Instanzdetails konfigurieren**.

5. Wählen Sie auf der Seite „Instanzdetails konfigurieren“ Folgendes aus, und klicken Sie dann auf Weiter: Speicher hinzufügen.

    - Anzahl der Instanzen: 1
    - Netzwerk: Die VPC, die in Schritt 1 erstellt wurde
    - Subnetz: das Management-Subnetz
    - Öffentliche IP automatisch zuweisen: Aktivieren



6. Wählen Sie auf der Seite „Speicher hinzufügen“ die Standardoption aus und klicken Sie auf Weiter: Tags hinzufügen.
7. Fügen Sie auf der Seite „Tags hinzufügen“ einen Namen für die Instance hinzu und klicken Sie auf Weiter: Sicherheitsgruppe konfigurieren.
8. Wählen Sie auf der Seite „Sicherheitsgruppe konfigurieren“ die Standardoption aus (die vom AWS Marketplace generiert wird und auf den empfohlenen Einstellungen von Citrix Systems basiert) und klicken Sie dann auf **Überprüfen und starten > Starten**.
9. Sie werden aufgefordert, ein vorhandenes Schlüsselpaar auszuwählen oder ein neues Schlüsselpaar zu erstellen. Wählen Sie in der Dropdownliste Wählen Sie ein Schlüsselpaar das Schlüsselpaar aus, das Sie als Voraussetzung erstellt haben (siehe Abschnitt Voraussetzung).
10. Markieren Sie das Kontrollkästchen, um das Schlüsselpaar zu bestätigen, und klicken Sie auf Launch Instances.



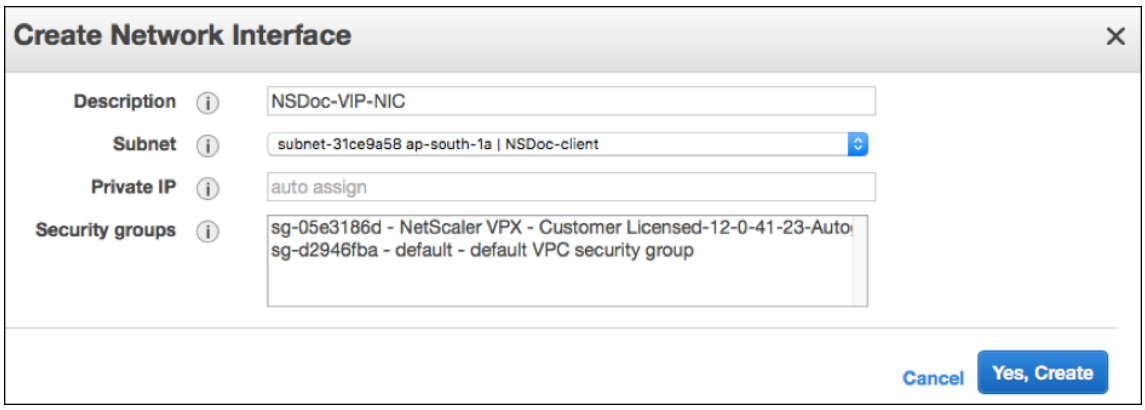
Der Launch Instance Wizard zeigt den Startstatus an und die Instance erscheint in der Liste der Instances, wenn sie vollständig gestartet ist.

Rufen Sie die Check-Instance auf, klicken Sie in der AWS-Konsole auf EC2 > Running Instances. Wählen Sie die Instanz aus und fügen Sie einen Namen hinzu. Stellen Sie sicher, dass der Instanzstatus läuft und die Statusprüfungen abgeschlossen sind.

Schritt 5: Weitere Netzwerkschnittstellen erstellen und anhängen.

Als Sie die VPC erstellt haben, war ihr nur eine Netzwerkschnittstelle zugeordnet. Fügen Sie der VPC nun zwei weitere Netzwerkschnittstellen hinzu, für VIP und SNIP.

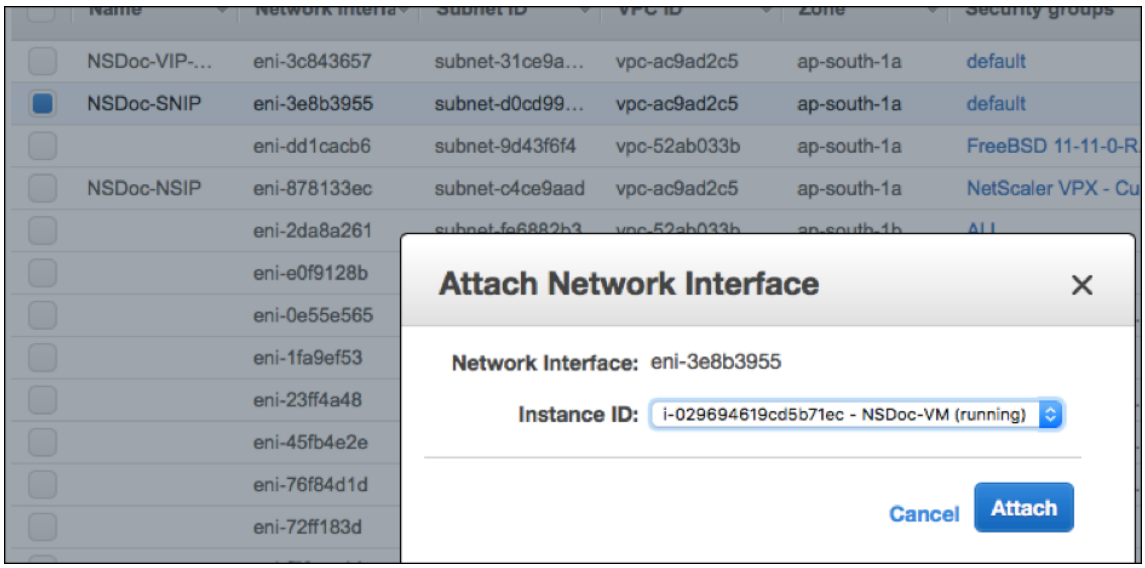
1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfacesaus.
3. Wählen Sie Create Network Interface.
4. Geben Sie für Beschreibung einen aussagekräftigen Namen ein.
5. Wählen Sie für Subnetz das Subnetz aus, das Sie zuvor für den VIP erstellt haben.
6. Belassen Sie für Private IP die Standardoption.
7. Wählen Sie für Sicherheitsgruppen die Gruppe aus.
8. Klicken Sie auf **Yes, Create**.



9. Nachdem die Netzwerkschnittstelle erstellt wurde, fügen Sie der Schnittstelle einen Namen hinzu.
10. Wiederholen Sie die Schritte, um eine Netzwerkschnittstelle für serverseitigen Datenverkehr zu erstellen.

Schließen Sie die Netzwerkschnittstellenan:

1. Wählen Sie im Navigationsbereich Network Interfacesaus.
2. Wählen Sie die Netzwerkschnittstelle aus und wählen Sie Attach.
3. Wählen Sie im Dialogfeld Netzwerkschnittstelle anhängen die Instanz aus und klicken Sie auf Attach.



Schritt 6: Verbinden Sie das NSIP mit einer elastischen IP.

1. Gehen Sie in der AWS-Managementkonsole zu **NETWORK & SECURITY > Elastic IPs**.
2. Suchen Sie nach verfügbaren kostenlosen EIPs zum Anhängen. Wenn keine vorhanden ist, klicken Sie auf **Neue Adresse zuweisen**.

3. Wählen Sie die neu zugewiesene IP-Adresse aus und wählen Sie **Aktionen > Adresse zuordnen**.
4. Klicken Sie auf das Optionsfeld **Netzwerkschnittstelle** .
5. Wählen Sie in der Dropdownliste Netzwerkschnittstelle die Management-NIC aus.
6. Wählen Sie im Dropdownmenü **Private IP** die von AWS generierte IP-Adresse aus.
7. Markieren Sie das Kontrollkästchen **Neuzuordnung** .
8. Klicken Sie auf **Zuordnen**.

Greifen Sie auf die VPX-Instanzzu:

Nachdem Sie eine eigenständige NetScaler VPX-Instanz mit drei NICs konfiguriert haben, melden Sie sich bei der VPX-Instanz an, um die NetScaler-seitige Konfiguration abzuschließen. Verwendung der folgenden Optionen:

- GUI: Geben Sie die öffentliche IP der Management-NIC im Browser ein. Melden Sie sich an, indem Sie `nsroot` als Benutzernamen und die Instanz-ID (i-0c1ffe1d987817522) als Kennwort verwenden.

> Hinweis
>
> Bei Ihrer ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Passwort zu ändern. Nachdem Sie das Kennwort geändert haben, müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu gestartet wird, müssen Sie sich mit dem Standardkennwort anmelden. Ändern Sie das Kennwort an der Eingabeaufforderung erneut und speichern Sie die Konfiguration.

- SSH: Öffnen Sie einen SSH-Client und geben Sie Folgendes ein:

```
ssh -i \<location of your private key\> ns root@\<public DNS of the instance
\>
```

Um das öffentliche DNS zu finden, klicken Sie auf die Instance und dann auf **Verbinden**.

Weitere Informationen:

- Informationen zum Konfigurieren der IP-Adressen im Besitz von NetScaler (NSIP, VIP und SNIP) finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.
- Sie haben eine BYOL-Version der NetScaler VPX Appliance konfiguriert. Weitere Informationen finden Sie im VPX-Lizenzierungshandbuch unterhttp://support.citrix.com/article/CTX122426

Download einer NetScaler VPX-Lizenz

August 4, 2023

Nach dem Start der NetScaler VPX-kundenlizenzierten Instanz vom AWS-Marktplatz ist eine Lizenz erforderlich. Weitere Informationen zur VPX-Lizenzierung finden Sie unter Übersicht über die Lizenzierung.

Sie müssen:

1. Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
2. Laden Sie die Lizenz auf die Instanz hoch.

Wenn es sich um eine **kostenpflichtige** Marketplace-Instanz handelt, müssen Sie keine Lizenz installieren. Der richtige Funktionsumfang und die richtige Leistung werden automatisch aktiviert.

Wenn Sie eine NetScaler VPX-Instanz mit einer Modellnummer über VPX 5000 verwenden, ist der Netzwerkdurchsatz möglicherweise nicht der gleiche wie in der Lizenz der Instanz angegeben. Andere Funktionen wie SSL-Durchsatz und SSL-Transaktionen pro Sekunde können jedoch verbessert werden.

Im `c4.8xlarge` Instanztyp wird eine 5-Gbit/s-Netzwerkbandbreite beobachtet.

So migrieren Sie das AWS-Abonnement auf BYOL

In diesem Abschnitt wird das Verfahren zur Migration vom AWS-Abonnement auf Bring your own License (BYOL) beschrieben, und umgekehrt.

Führen Sie die folgenden Schritte aus, um ein AWS-Abonnement auf BYOL zu migrieren:

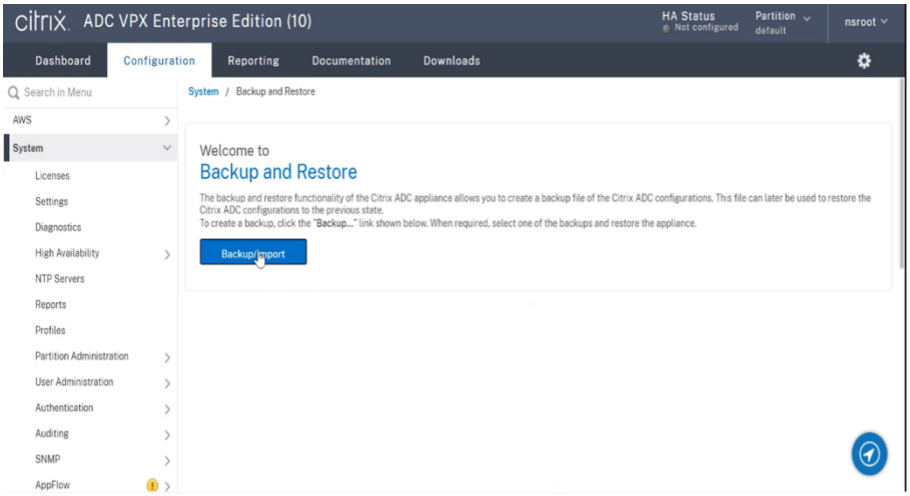
> Hinweis
>
> Der **Schritt 2** und der **Schritt 3** werden auf der NetScaler VPX-Instanz ausgeführt, und alle anderen Schritte werden im AWS-Portal ausgeführt.

1. Erstellen Sie eine BYOL EC2-Instanz mit NetScaler VPX - Kundenlizenziert in derselben Availability Zone wie die alte EC2-Instanz, die dieselbe Sicherheitsgruppe, IAM-Rolle und das gleiche Subnetz hat. Die neue EC2-Instanz muss nur eine ENI-Schnittstelle haben.

2. Gehen Sie folgendermaßen vor, um die Daten auf der alten EC2-Instanz mit der NetScaler GUI zu sichern.

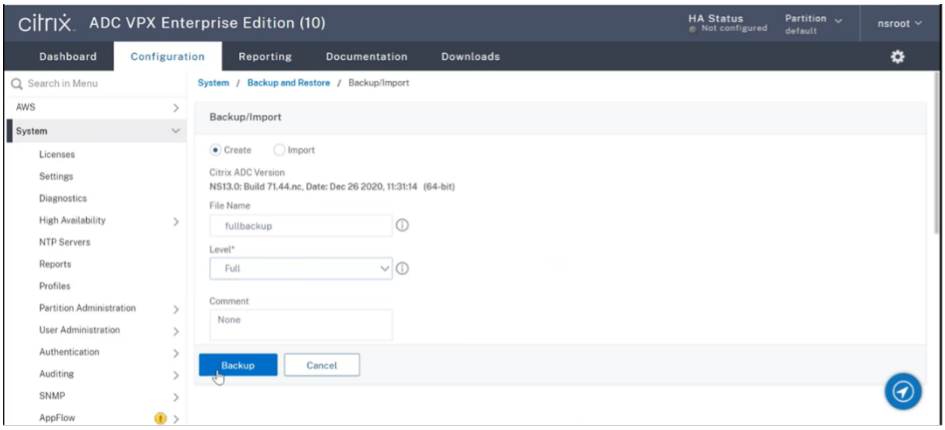
   a) Navigieren Sie zu **System > Sichern und Wiederherstellen**.

   b) Klicken Sie auf der **Begrüßungsseite** auf **Backup/Importieren**, um den Vorgang zu starten.

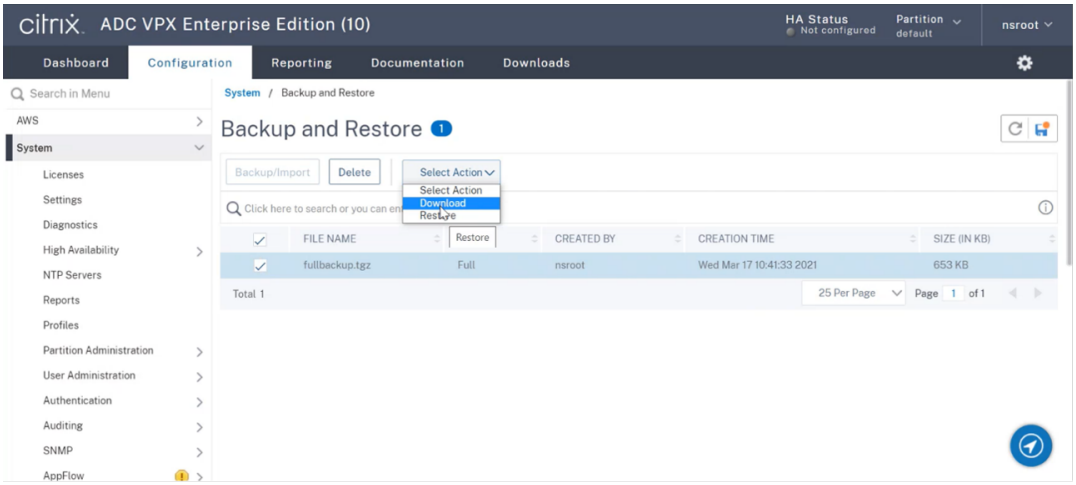


   c) Geben Sie auf der Seite **“Backup/Import** “ die folgenden Details ein:

   - **Name** — Name der Sicherungsdatei.
   - **Level** — Wählen Sie die Backup-Level als **Full**aus.
   - **Kommentar** — Geben Sie eine kurze Beschreibung des Backup an.



   d) Klicken Sie auf **Backup**. Sobald die Backup abgeschlossen ist, können Sie die Datei auswählen und auf Ihren lokalen Computer herunterladen.

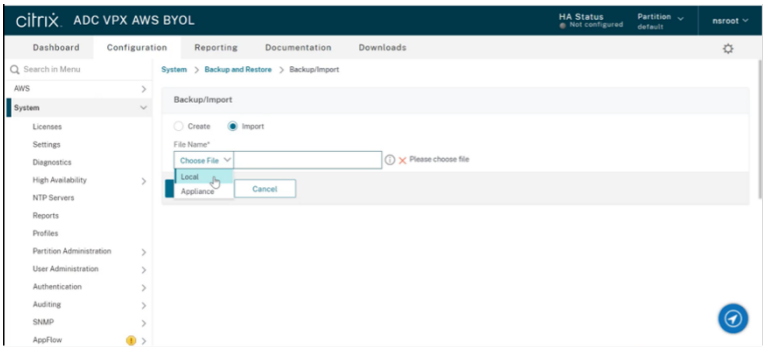


3. Gehen Sie folgendermaßen vor, um die Daten auf der neuen EC2-Instanz mit der NetScaler GUI wiederherzustellen:

   a) Navigieren Sie zu **System > Sichern und Wiederherstellen**.

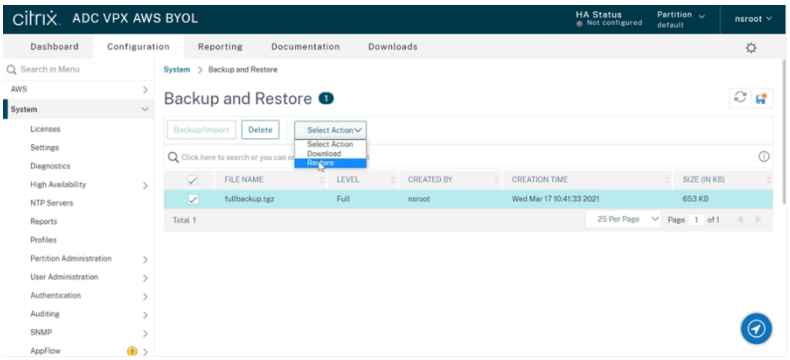
   b) Klicken Sie auf **Backup/Import**, um den Vorgang zu starten.

   c) Wählen Sie die Option **Importieren** aus und laden Sie die Sicherungsdatei hoch.

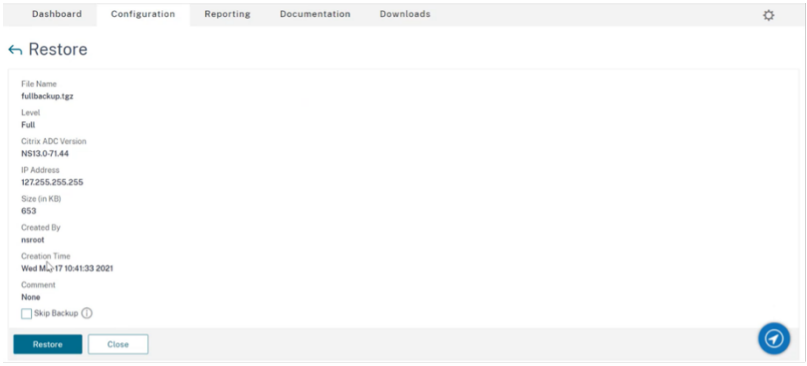


   d) Wählen Sie die Datei aus.

   e) **Wählen Sie im Dropdownmenü Aktion** auswählen die Option **Wiederherstellen**aus.



   f) Überprüfen Sie auf der Seite **Wiederherstellen** die Dateidetails und klicken Sie auf **Wiederherstellen**.



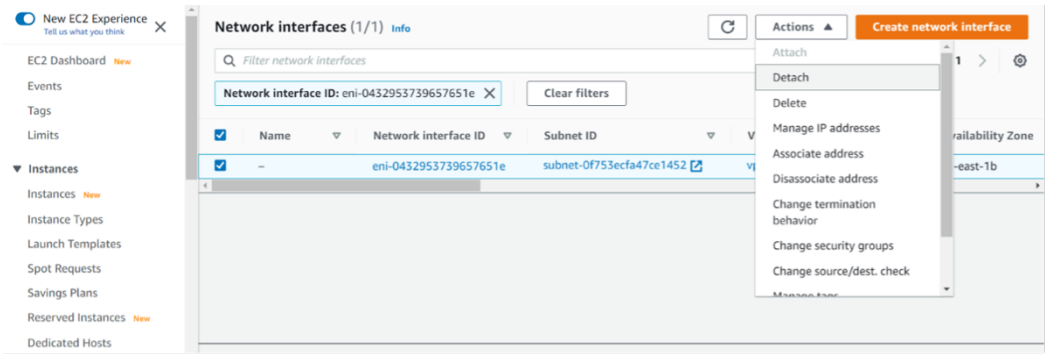
g) Starten Sie nach der Wiederherstellung die EC2-Instanz neu.

4. Verschieben Sie alle Schnittstellen (mit Ausnahme der Verwaltungsschnittstelle, an die die NSIP-Adresse gebunden ist) von der alten EC2-Instanz zur neuen EC2-Instanz. Gehen Sie folgendermaßen vor, um eine Netzwerkschnittstelle von einer EC2-Instanz in eine andere zu verschieben:

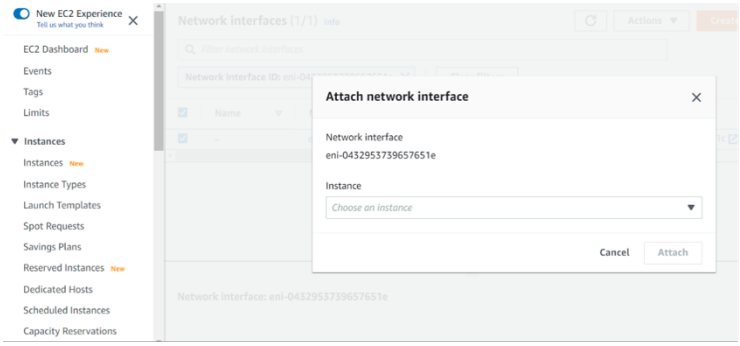
   a) Stoppen Sie im **AWS-Portal**sowohl die alte als auch die neue EC2-Instanz.

   b) Navigieren Sie zu **Netzwerkschnittstellen**und wählen Sie die Netzwerkschnittstelle aus, die an die alte EC2-Instanz angeschlossen ist.

   c) Trennen Sie die EC2-Instanz, indem Sie auf **Aktionen > Trennen**klicken.



   d) Schließen Sie die Netzwerkschnittstelle an die neue EC2-Instanz an, indem Sie auf **Aktionen > Anhängen**klicken. Geben Sie den Namen der EC2-Instanz ein, an den die Netzwerkschnittstelle angeschlossen werden muss.



e) Führen Sie den **Schritt 1** bis **Schritt 4** für alle anderen angehängten Schnittstellen aus. Vergewissern Sie sich, dass Sie die Reihenfolge befolgen und die Reihenfolge der Schnittstelle beibehalten. Das heißt, trennen Sie zuerst Schnittstelle 2 und schließen Sie es an, trennen Sie dann Schnittstelle 3 und schließen Sie es an und so weiter.

5. Sie können die Verwaltungsschnittstelle nicht von einer alten EC2-Instanz trennen. Verschieben Sie also alle sekundären IP-Adressen (falls vorhanden) auf der Verwaltungsschnittstelle (primäre Netzwerkschnittstelle) der alten EC2-Instanz auf die neue EC2-Instanz. Gehen Sie folgendermaßen vor, um eine IP-Adresse von einer Schnittstelle in eine andere zu verschieben:

   a) Stellen Sie im **AWS-Portal**sicher, dass sich sowohl die alten als auch die neue EC2-Instanzen im Status " **Stop** " befinden.

   b) Navigieren Sie zu **Netzwerkschnittstellen**und wählen Sie die Verwaltungsnetzwerkschnittstelle aus, die an die alte EC2-Instanz angeschlossen ist.

   c) Klicken Sie auf **Aktionen > IP-Adresse verwalten**und notieren Sie sich alle sekundären IP-Adressen (falls vorhanden).

   d) Navigieren Sie zur Verwaltungsnetzwerkschnittstelle oder zur primären Schnittstelle der neuen EC2-Instanz.

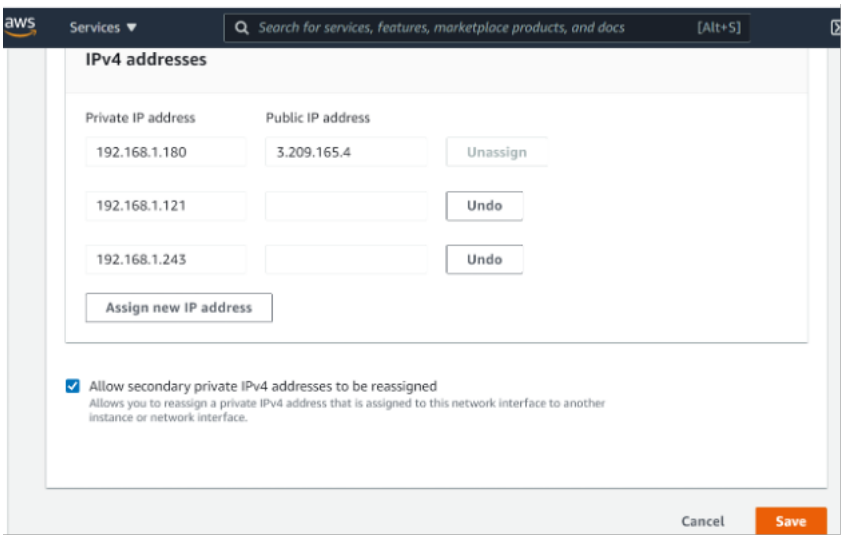
   e) Klicken Sie auf **Aktionen > IP-Adressen verwalten**.

   f) Klicken Sie unter **IPv4-Adressen**auf **Neue IP-Adresse zuweisen**.

   g) Geben Sie die IP-Adressen ein, die im **Schritt 3**vermerkt sind.

   h) Aktivieren **Sie das Kontrollkästchen Neuzuweisung sekundärer privater IP-Adressen** zulassen.

   i) Klicken Sie auf **Speichern**.



6. Starten Sie die neue EC2-Instanz und überprüfen Sie die Konfiguration. Nachdem die gesamte Konfiguration verschoben wurde, können Sie die alte EC2-Instanz gemäß Ihren Anforderungen löschen oder behalten.
7. Wenn eine EIP-Adresse an die NSIP-Adresse der alten EC2-Instanz angehängt ist, verschieben Sie die alte Instanz-NSIP-Adresse an die NSIP-Adresse der neuen Instanz.
8. Wenn Sie zur alten Instanz zurückkehren möchten, führen Sie die gleichen Schritte in entgegengesetzter Weise zwischen der alten und der neuen Instanz aus.
9. Nachdem Sie von der Abonnementinstanz zur BYOL-Instanz umgezogen sind, ist eine Lizenz erforderlich. Gehen Sie folgendermaßen vor, um eine Lizenz zu installieren:
    - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
    - Laden Sie die Lizenz auf die Instanz hoch. Weitere Informationen finden Sie unter VPX ADC - Installieren einer neuen Lizenz.

> Hinweis
>
> Wenn Sie die BYOL-Instanz auf eine Abonnementinstanz (kostenpflichtige Marketplace-Instanz) verschieben, müssen Sie die Lizenz nicht installieren. Der richtige Funktionsumfang und die richtige Leistung werden automatisch aktiviert.

Einschränkungen

Die Verwaltungsschnittstelle kann nicht auf die neue EC2-Instanz verschoben werden. Citrix empfiehlt daher, die Verwaltungsschnittstelle manuell zu konfigurieren. Weitere Informationen finden Sie unter **Schritt 5** des vorherigen Verfahrens. Eine neue EC2-Instanz wird mit dem genauen Replikat der alten EC2-Instanz erstellt, aber nur die NSIP-Adresse hat eine neue IP-Adresse.

Load Balancing-Server in verschiedenen Availability Zones

May 11, 2023

Eine VPX-Instanz kann für den Lastenausgleich von Servern verwendet werden, die in derselben Availability Zone laufen, oder in:

- Eine andere Availability Zone (AZ) in derselben AWS-VPC
- Eine andere AWS-Region
- AWS EC2 in einer VPC

Um einer VPX-Instance den Lastenausgleich von Servern zu ermöglichen, die außerhalb der AWS-VPC laufen, in der sich die

VPX-Instance befindet, konfigurieren Sie die Instance so, dass sie EIPs verwendet, um den Datenverkehr über das Internet-Gateway weiterzuleiten, wie folgt:

1. Konfigurieren Sie ein SNIP auf der NetScaler VPX-Instanz mithilfe der NetScaler-CLI oder der GUI.
2. Ermöglichen Sie das Weiterleiten des Datenverkehrs aus der AZ, indem Sie ein öffentlich zugängliches Subnetz für den serverseitigen Verkehr erstellen.
3. Fügen Sie der Routingtabelle mithilfe der AWS GUI-Konsole eine Internet-Gateway -Route hinzu.
4. Ordnen Sie die Routingtabelle, die Sie aktualisiert haben, dem serverseitigen Subnetz zu.
5. Ordnen Sie eine EIP der serverseitigen privaten IP-Adresse zu, die einer NetScaler SNIP-Adresse zugeordnet ist.

So funktioniert Hochverfügbarkeit auf AWS

May 11, 2023

Sie können zwei NetScaler VPX-Instanzen auf AWS als aktives und passives Paar mit hoher Verfügbarkeit (HA) konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären Knoten. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Übernahme.

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Hochverfügbarkeit innerhalb derselben Zone
- Hohe Verfügbarkeit über verschiedene Zonen hinweg

> **Hinweis**
>
> Damit die Hochverfügbarkeit funktioniert, stellen Sie sicher, dass beide NetScaler VPX-Instanzen mit IAM-Rollen verknüpft und dem NSIP die Elastic IP (EIP)-Adresse zugewiesen sind. Sie müssen NSIP keine EIP zuweisen, wenn das NSIP über die NAT-Instanz das Internet erreichen kann.

Hohe Verfügbarkeit innerhalb derselben Zonen

In einer Hochverfügbarkeitsbereitstellung innerhalb derselben Zonen müssen beide VPX-Instanzen ähnliche Netzwerkkonfigurationen haben.

Folgen Sie diesen beiden Regeln:

Regel 1. Jede Netzwerkkarte auf einer VPX-Instanz muss sich im selben Subnetz befinden wie die entsprechende Netzwerkkarte in der anderen VPX. Beide Instanzen müssen Folgendes haben:

- Verwaltungsschnittstelle im selben Subnetz (als Management-Subnetz bezeichnet)

- Client-Schnittstelle im selben Subnetz (als Client-Subnetz bezeichnet)
- Serverschnittstelle im selben Subnetz (als Serversubnetz bezeichnet)

Regel 2. Die Reihenfolge der Mgmt-NIC, der Client-NIC und der Server-NIC auf beiden Instanzen muss identisch sein.
Beispielsweise wird das folgende Szenario nicht unterstützt.

VPX-Instanz 1

NIC 0: Verwaltung
NIC 1: Client
NIC 2: Server

VPX-Instanz 2

NIC 0: Verwaltung

NIC 1: Server

NIC 2: Client

In diesem Szenario befindet sich NIC 1 von Instanz 1 im Clientsubnetz, während NIC 1 von Instanz 2 im Serversubnetz ist. Damit HA funktioniert, muss sich NIC 1 der beiden Instanzen entweder im Client-Subnetz oder im Serversubnetz befinden.

Ab 13.0 41.xx kann eine hohe Verfügbarkeit erreicht werden, indem sekundäre private IP-Adressen migriert werden, die an die Netzwerkkarten (Client- und serverseitige Netzwerkkarten) des primären HA-Knotens nach dem Failover angeschlossen sind. In dieser Bereitstellung gilt:

- Beide VPX-Instanzen haben die gleiche Anzahl von Netzwerkkarten und Subnetzzuordnung gemäß der NIC-Aufzählung.
- Jede VPX-NIC hat eine zusätzliche private IP-Adresse, mit Ausnahme der ersten NIC - die der Verwaltungs-IP-Adresse entspricht. Die zusätzliche private IP-Adresse wird als primäre private IP-Adresse in der AWS-Webkonsole angezeigt. In unserem Dokument bezeichnen wir diese zusätzliche IP-Adresse als Dummy-IP-Adresse).
- Die Dummy-IP-Adressen dürfen auf der NetScaler-Instanz nicht als VIP und SNIP konfiguriert werden.
- Andere sekundäre private IP-Adressen müssen bei Bedarf erstellt und als VIP und SNIP konfiguriert werden.
- Bei Failover sucht der neue Primärknoten nach konfigurierten SNIPs und VIPs und verschiebt sie von NICs, die an den vorherigen primären Knoten angeschlossen sind, auf die entsprechenden Netzwerkkarten auf dem neuen Primärbereich.
- NetScaler Instanzen erfordern IAM-Berechtigungen, damit HA funktioniert. Fügen Sie der IAM-Richtlinie, die jeder Instanz hinzugefügt wurde, die folgenden IAM-Berechtigungen hinzu.


```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeNetworkInterfaces"
"ec2:AssignPrivateIpAddresses"
```

> Hinweis:`unassignPrivateIpAddress` ist nicht erforderlich.

Diese Methode ist schneller als die Legacy-Methode. Bei der älteren Methode hängt HA von der Migration elastischer AWS-Netzwerkschnittstellen des primären Knotens zum sekundären Knoten ab.

Für eine Legacy-Methode sind die folgenden Richtlinien erforderlich:

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Weitere Informationen finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares in AWS.

Hohe Verfügbarkeit über verschiedene Zonen hinweg

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen als aktiv-passives Paar mit hoher Verfügbarkeit im Modus Independent Network Configuration (INC) konfigurieren. Beim Failover migriert die EIP (Elastic IP) des VIP der primären Instanz auf die sekundäre, die als neue primäre Instanz übernommen wird. Im Failover-Prozess wird die AWS-API:

- Überprüft die virtuellen Server, an die `IPSets` angeschlossen sind.
- Sucht die IP-Adresse mit einer zugeordneten öffentlichen IP-Adresse aus den beiden IP-Adressen, die der virtuelle Server überwacht. Eine, die direkt an den virtuellen Server angeschlossen ist, und eine, die über den IP-Satz angeschlossen ist.
- Ordnet die öffentliche IP (EIP) der privaten IP zu, die zum neuen primären VIP gehört.

Für HA über verschiedene Zonen hinweg sind folgende Richtlinien erforderlich:

```
"iam:GetRole"
"ec2:DescribeInstances"
"ec2:DescribeAddresses"
"ec2:AssociateAddress"
"ec2:DisassociateAddress"
```

Weitere Informationen finden Sie unter Hochverfügbarkeit in AWS Availability Zones.

Bevor Sie mit der Bereitstellung beginnen

Bevor Sie mit einer HA-Bereitstellung auf AWS beginnen, lesen Sie das folgende Dokument:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- Hohe Verfügbarkeit

Problembehandlung

Um Fehler während eines HA-Failovers der NetScaler VPX-Instanz in der AWS-Cloud zu beheben, überprüfen Sie die am Speicherort `/var/log/` gespeicherte Datei `cloud-ha-daemon.log`.

Bereitstellen eines VPX-HA-Paar in derselben AWS-Verfügbarkeitszone

May 11, 2023

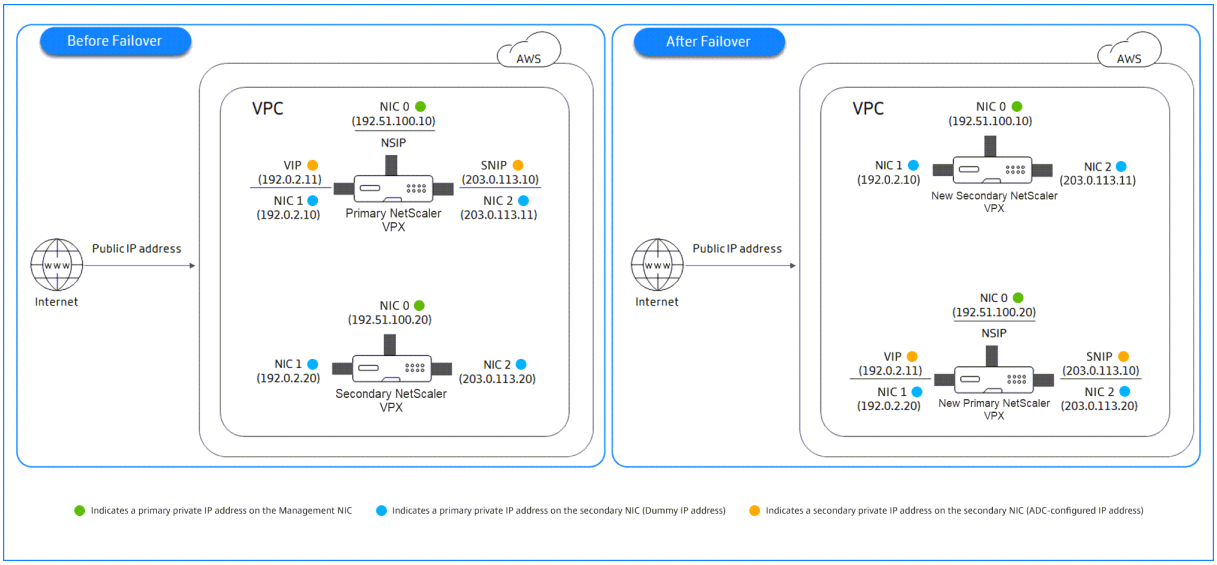
> **Hinweis:**
>
> Ab NetScaler Version 13.1 Build 27.x unterstützt das VPX HA-Paar in derselben AWS-Verfügbarkeitszone IPv6-Adressen.

Sie können zwei NetScaler VPX-Instanzen in AWS als HA-Paar in derselben AWS-Zone konfigurieren, in der sich beide VPX-Instanzen im selben Subnetz befinden. HA wird erreicht, indem sekundäre private IP-Adressen, die an die NICs (client- und serverseitige NICs) des primären HA-Knotens angeschlossen sind, nach einem Failover zum sekundären HA-Knoten migriert. Alle Elastic IP-Adressen, die mit den sekundären privaten IP-Adressen verknüpft sind, werden ebenfalls migriert.

Das NetScaler VPX HA-Paar unterstützt sowohl IPv4- als auch IPv6-Adressen in derselben AWS-Verfügbarkeitszone.

Die folgende Abbildung zeigt ein HA-Failoverszenario durch Migration sekundärer privater IP-Adressen.

Abbildung 1. Ein NetScaler VPX HA-Paar auf AWS mit privater IP-Migration



Bevor Sie mit Ihrem Dokument beginnen, lesen Sie die folgenden Dokumente:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- Hohe Verfügbarkeit

So stellen Sie ein VPX-HA-Paar in derselben Zone bereit

Hier ist eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-HA-Paars in derselben Zone:

1. Erstellen Sie zwei VPX-Instanzen auf AWS mit jeweils drei Netzwerkkarten
2. Weisen Sie VIP und SNIP des primären Knotens eine sekundäre private AWS IP-Adresse zu
3. Konfigurieren von VIP und SNIP auf dem primären Knoten mit sekundären privaten IP-Adressen von AWS
4. Konfigurieren der HA auf beiden Knoten

Schritt 1. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) mit derselben VPC mit jeweils drei NICs (Ethernet 0, Ethernet 1, Ethernet 2)

Befolgen Sie die Schritte unter Bereitstellen einer NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole.

Schritt 2. Weisen Sie auf dem primären Knoten private IP-Adressen für Ethernet 1 (Client-IP oder VIP) und Ethernet 2 (Backend-Server-IP oder SNIP) zu

Die AWS-Konsole weist den konfigurierten NICs automatisch primäre private IP-Adressen zu. Weisen Sie VIP und SNIP mehr private IP-Adressen zu, die als sekundäre private IP-Adressen bekannt sind.

Gehen Sie folgendermaßen vor, um einer Netzwerkschnittstelle eine private IP-Adresse zuzuweisen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich **Netzwerkschnittstellen** und dann die Netzwerkschnittstelle aus, die mit der Instanz verbunden ist.
3. Wählen Sie **Aktionen > IP-Adressen verwalten**.
4. Wählen Sie je nach Anforderung **IPv4-Adressenoder IPv6-Adressen** aus.
5. Für IPv4-Adressen:
   a) Wählen Sie **Neue IP zuweisen**.
   b) Geben Sie eine bestimmte IPv4-Adresse ein, die innerhalb des Subnetzbereichs der Instanz liegt, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse für Sie auswählen kann.
   c) (Optional) Wählen Sie **Neuzuweisung** zulassen, damit die sekundäre private IP-Adresse neu zugewiesen werden kann, wenn sie bereits einer anderen Netzwerkschnittstelle zugewiesen ist.
6. Für IPv6-Adressen:
   a) Wählen Sie **Neue IP zuweisen**.
   b) Geben Sie eine bestimmte IPv6-Adresse ein, die innerhalb des Subnetzbereichs für die Instanz liegt, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse für Sie auswählen kann.
   c) (Optional) Wählen Sie **Neuzuweisung** zulassen, damit die primäre oder sekundäre private IP-Adresse neu zugewiesen werden kann, wenn sie bereits einer anderen Netzwerkschnittstelle zugewiesen ist.
7. Wählen Sie **Ja > Aktualisieren**.

Unter der **Instanzbeschreibung**werden die zugewiesenen privaten IP-Adressen angezeigt.

> **Hinweis:**
>
> In einer IPv4-HA-Paarbereitstellung können Sie nur die sekundären IPv4-Adressen auf der Schnittstelle zuweisen und sie als VIP- und SNIP-Adressen verwenden. In einer IPv6-HA-Pair-Bereitstellung können Sie jedoch entweder die primären IPv6- oder sekundären IPv6-Adressen auf der Schnittstelle zuweisen und sie als VIP- und SNIP-Adressen verwenden.

Schritt 3. Konfigurieren von VIP und SNIP auf dem primären Knoten mit sekundären privaten IP-Adressen

Greifen Sie mit SSH auf den primären Knoten zu. Öffnen Sie einen SSH-Client und geben Sie ein:

```
1 ssh -i <location of your private key> nsroot@<public DNS of the
     instance>
2 <!--NeedCopy-->
```

Konfigurieren Sie als Nächstes VIP und SNIP.

Geben Sie für VIP Folgendes ein:

```
1 add ns ip <IPAddress> <netmask> -type <type>
2 <!--NeedCopy-->
```

Geben Sie für SNIP Folgendes ein:

```
1 add ns ip <IPAddress> <netmask> -type SNIP
2 <!--NeedCopy-->
```

Tippen Sie `save config` zum Speichern ein.

Um die konfigurierten IP-Adressen anzuzeigen, geben Sie den folgenden Befehl ein:

```
1 show ns ip
2 <!--NeedCopy-->
```

Weitere Informationen finden Sie in den folgenden Artikeln:

- Virtuelle IP-Adressen (VIP) konfigurieren und verwalten
- Konfigurieren der NSIP-Adresse

Schritt 4: Konfigurieren von HA auf beiden Instanzen

Öffnen Sie auf dem primären Knoten einen Shell-Client und geben Sie den folgenden Befehl ein:

```
1 add ha node <id> <private IP address of the management NIC of the
     secondary node>
2 <!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

```
1 add ha node <id> < private IP address of the management NIC of the
     primary node >
2 <!--NeedCopy-->
```

Geben Sie `save config` ein, um die Konfiguration zu speichern.

Um die konfigurierten HA-Knoten anzuzeigen, geben Sie ein `show ha node`.

Nach dem Failover werden die sekundären privaten IP-Adressen, die auf dem vorherigen primären Knoten als VIP und SNIP konfiguriert sind, auf den neuen primären Knoten migriert.

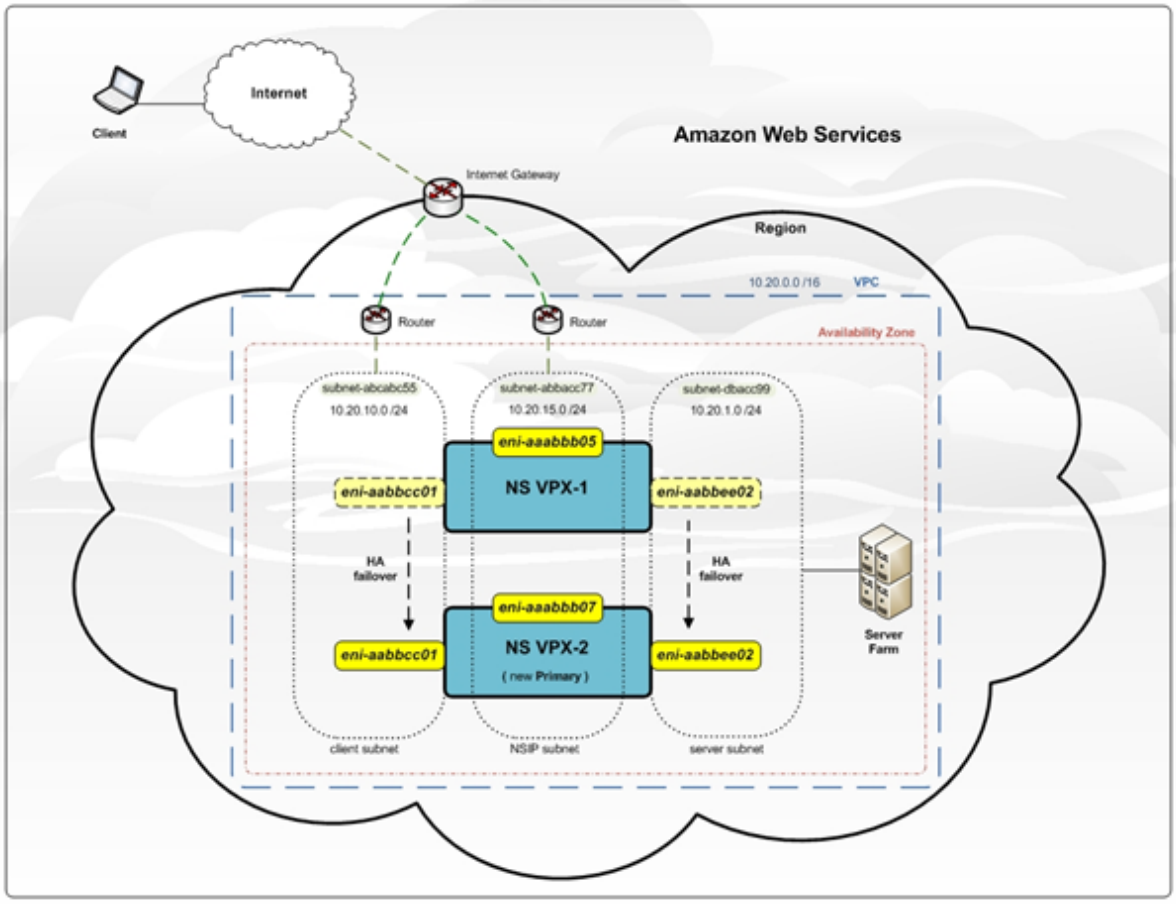
Um ein Failover auf einem Knoten zu erzwingen, geben Sie `force HA`Failover ein.

Legacy-Methode für die Bereitstellung eines VPX-HA-Paars

Vor der Veröffentlichung von 13.0 41.x wurde die HA innerhalb derselben Zone durch die AWS Elastic Network Interface (ENI) -Migration erreicht. Diese Methode ist jedoch langsam veraltet.

Die folgende Abbildung zeigt ein Beispiel für die HA-Bereitstellungsarchitektur für NetScaler VPX-Instanzen auf AWS.

Abbildung 1. Ein NetScaler VPX HA-Paar in AWS mit ENI-Migration



Sie können zwei VPX-Instanzen in AWS als HA-Paar bereitstellen, indem Sie eine der folgenden Optionen verwenden:

- Erstellen Sie die Instanzen mit IAM-Rolle manuell mithilfe der AWS Management Console und konfigurieren Sie anschließend HA darauf.
- Oder automatisieren Sie die Hochverfügbarkeitsbereitstellung mithilfe der Citrix CloudFormation-Vorlage.

Die CloudFormation-Vorlage reduziert die Anzahl der Schritte zum Erstellen eines HA-Paars erheblich und erstellt automatisch eine IAM-Rolle. In diesem Abschnitt wird beschrieben, wie ein NetScaler VPX HA-Paar (aktiv-passiv) mithilfe der Citrix CloudFormation-Vorlage bereitgestellt wird.

Beachten Sie die folgenden Punkte, wenn Sie zwei NetScaler VPX-Instanzen als HA-Paar bereitstellen.

Wichtige Hinweise

- HA in AWS erfordert, dass der primäre Knoten über mindestens zwei ENIs verfügt (eine für die Verwaltung und die andere für den Datenverkehr), und der sekundäre Knoten muss über eine Management-ENI verfügen. Erstellen Sie aus Sicherheitsgründen jedoch drei ENIs auf dem primären Knoten, da Sie mit diesem Setup das private und öffentliche Netzwerk trennen können (empfohlen).
- Der sekundäre Knoten hat immer eine ENI-Schnittstelle (für die Verwaltung) und der primäre Knoten kann bis zu vier ENIs haben.
- Die NSIP-Adressen für jede VPX-Instanz in einem Hochverfügbarkeitspaar müssen auf der Standard-ENI der Instanz konfiguriert werden.
- Amazon erlaubt keine Broadcast-/Multicast-Pakete in AWS. Infolgedessen werden in einem HA-Setup ENIs auf Datenebene von der primären zur sekundären VPX-Instanz migriert, wenn die primäre VPX-Instanz ausfällt.
- Da die standardmäßige (Verwaltungs-) ENI nicht auf eine andere VPX-Instanz verschoben werden kann, verwenden Sie nicht die Standard-ENI für Client- und Serververkehr (Datenebenenverkehr).
- Die Meldung AWSCONFIG IOCTL NSAPI_HOTPLUG_INTF Erfolgsausgabe 0 in der /var/log/ns.log zeigt an, dass die beiden Daten-ENIs erfolgreich an die sekundäre Instanz (die neue primäre) angehängt wurden.
- Ein Failover kann aufgrund des AWS Detach/Attach ENI Mechanismus bis zu 20 Sekunden dauern.
- Nach einem Failover wird die ausgefallene Instanz immer neu gestartet.
- Die Heartbeat-Pakete werden nur über die Verwaltungsschnittstelle empfangen.
- Die Konfigurationsdatei der primären und sekundären VPX-Instanz wird synchronisiert, einschließlich des `nsroot`-Kennworts. Das`nsroot` Kennwort des sekundären Knotens wird nach der HA-Konfigurationssynchronisierung auf das des primären Knotens festgelegt.
- Um Zugriff auf die AWS-API-Server zu haben, muss der VPX-Instanz entweder eine öffentliche IP-Adresse zugewiesen sein oder das Routing muss auf VPC-Subnetzebene korrekt eingerichtet sein, was auf das Internet-Gateway der VPC verweist.
- Nameservers/DNS-Server werden auf VPC-Ebene mit DHCP-Optionen konfiguriert.
- Die Citrix CloudFormation-Vorlage erstellt kein HA-Setup zwischen verschiedenen Availability Zones.
- Die Citrix CloudFormation-Vorlage erstellt keinen INC-Modus.
- Die AWS-Debug-Meldungen sind in der Protokolldatei /var/log/ns.log auf der VPX-Instanz verfügbar.

Stellen Sie mithilfe der Citrix CloudFormation-Vorlage ein Hochverfügbarkeitspaar bereit

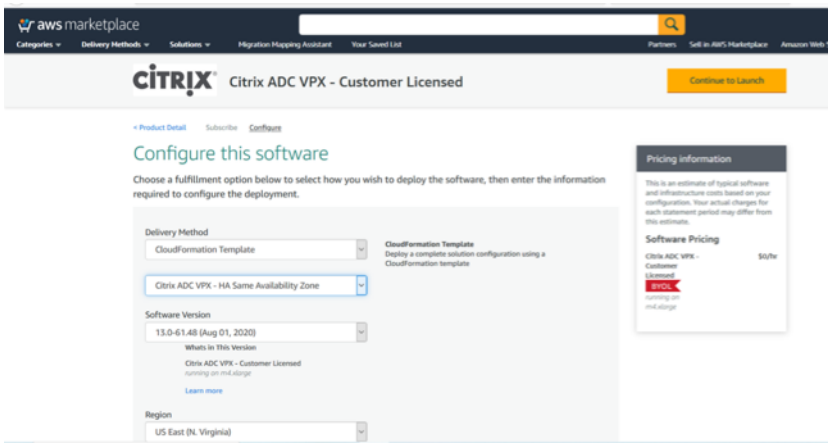
Bevor Sie die CloudFormation-Vorlage starten, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Eine VPC
- Drei Subnetze innerhalb der VPC
- Eine Sicherheitsgruppe mit UDP 3003, TCP 3009—3010, HTTP, SSH-Ports geöffnet
- Ein Schlüsselpaar
- Erstellen Sie ein Internet-Gateway
- Bearbeiten von Routinetabellen für Client- und Verwaltungsnetzwerke, um auf das Gateway

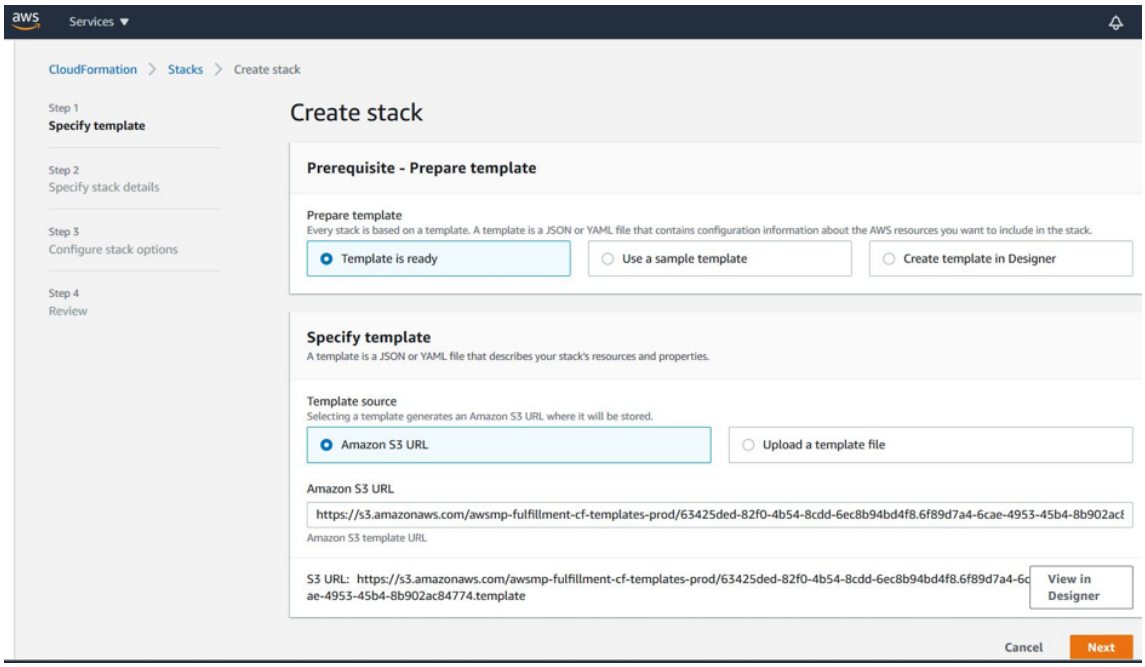
> **Hinweis**
>
> Die Citrix CloudFormation-Vorlage erstellt automatisch eine IAM-Rolle. Bestehende IAM-Rollen werden nicht in der Vorlage angezeigt.

So starten Sie die Citrix CloudFormation-Vorlage:

1. Melden Sie sich mit Ihren AWS-Anmeldeinformationen am AWS-Marketplace an .
2. Geben Sie im Suchfeld **NetScaler VPX** ein, um nach dem NetScaler AMI zu suchen, und klicken Sie auf **Los**.
3. Klicken Sie auf der Suchergebnisseite auf das gewünschte NetScaler VPX Angebot.
4. Klicken Sie auf die Registerkarte **Preise**, um zu **Preisinformationen** zu gelangen.
5. Wählen Sie die Region und die **Fulfillment-Option** als **NetScaler VPX — Kundenlizenziert**aus.
6. Klicken Sie auf **Weiter, um zu abonnieren**.
7. Überprüfen Sie die Details auf der Seite **Abonnieren** und klicken Sie **auf Configuration fortsetzen**.
8. Wählen Sie **Bereitstellungsmethode** als **CloudFormation-Vorlage** aus.
9. Wählen Sie die erforderliche CloudFormation-Vorlage aus.
10. Wählen Sie **Softwareversion** und **Region** aus und klicken Sie auf **Weiter zu Launch**.



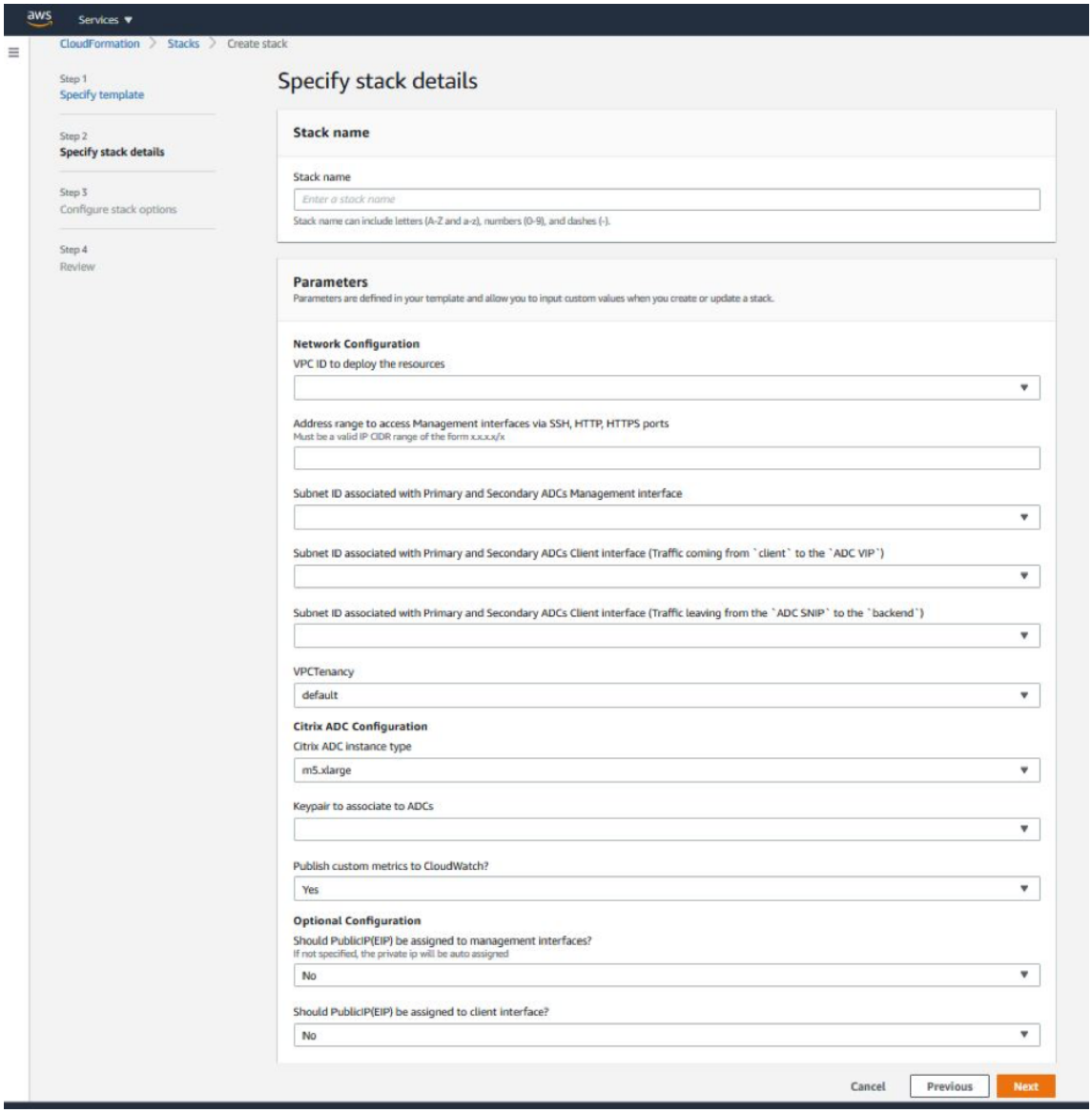
11. Wählen Sie unter **Aktion auswählen** die Option **CloudFormation starten** aus, und klicken Sie auf **Starten**.
    Die Seite **Stapel erstellen** wird angezeigt.
12. Klicken Sie auf **Weiter**.



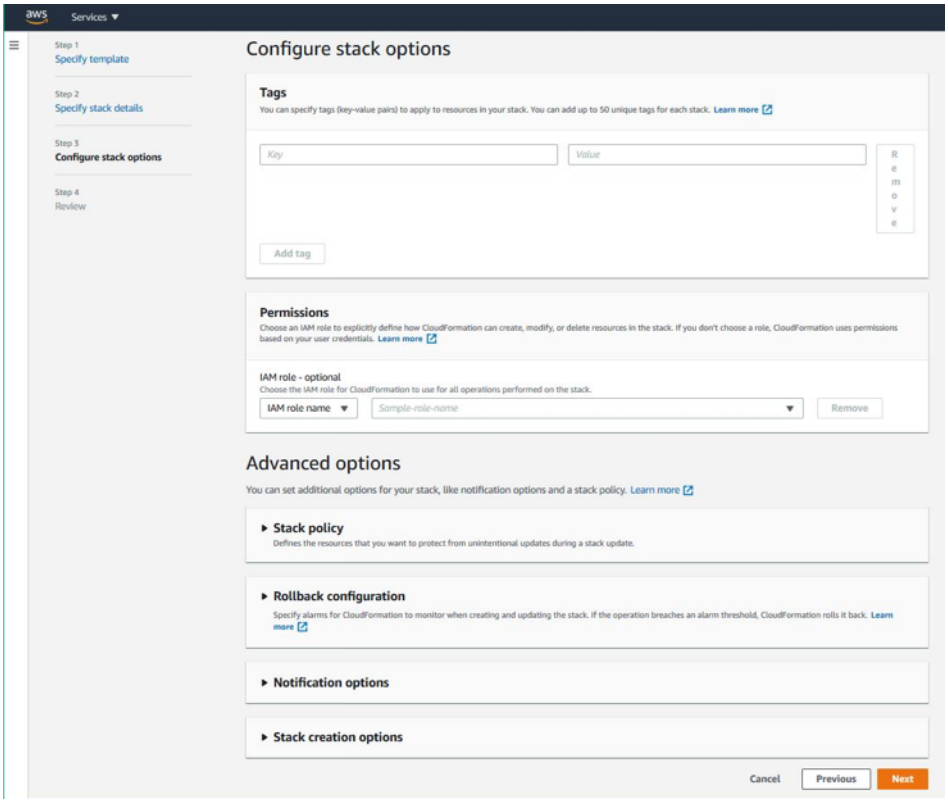
13. Die Seite **Stapeldetails angeben** wird angezeigt. Geben Sie die folgenden Details ein.
    - Geben Sie einen **Stack-Namen**ein. Der Name muss innerhalb von 25 Zeichen sein.
    - Führen Sie unter **Netzwerkkonfiguration**die folgenden Schritte aus:
      - Wählen Sie **Verwaltungsteilnetz**, **Client-Subnetz** und **Server-Subnetz** aus. Stellen Sie sicher, dass Sie die richtigen Teilnetze auswählen, die Sie in der VPC erstellt haben, die Sie unter VPC-ID ausgewählt haben.
      - Fügen Sie **primäre Verwaltungs-IP**, **sekundäre Verwaltungs-IP, Client-IPund Server-** Die IP-Adressen müssen zu denselben Subnetzen der jeweiligen Teilnetze

gehören. Alternativ können Sie die Vorlage die IP-Adressen automatisch zuweisen lassen.
  - Wählen Sie **Standard** für **vpcTenancy**aus.
- Führen Sie unter **NetScaler Configuration**die folgenden Schritte aus:
  - Wählen Sie **m5.xlarge** als **Instanztyp**aus.
  - Wählen Sie im Menü für Schlüsselpaar das **Schlüsselpaar**aus, das Sie bereits erstellt haben.
  - Standardmäßig sind die **Benutzerdefinierte Metriken in CloudWatch veröffentlichen?** Option ist auf **Ja**eingestellt. Wenn Sie diese Option deaktivieren möchten, wählen Sie **Nein**aus.

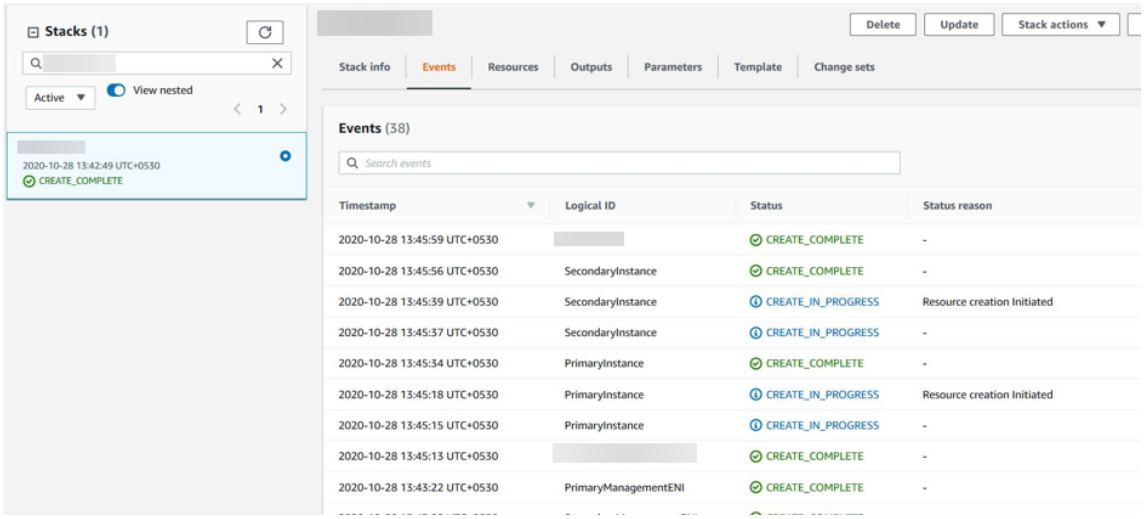
    Weitere Informationen zu CloudWatch-Metriken finden Sie unter Überwachen Ihrer Instanzen mit Amazon CloudWatch.
- Führen Sie unter **Optionale Konfiguration**Folgendes aus:
  - Standardmäßig **sollte PublicIp (EIP) Management-Interfaces zugewiesen werden?** Option ist auf **Nein**eingestellt.
  - Standardmäßig **sollte PublicIp (EIP) der Clientschnittstelle zugewiesen werden?** Option ist auf **Nein**eingestellt.



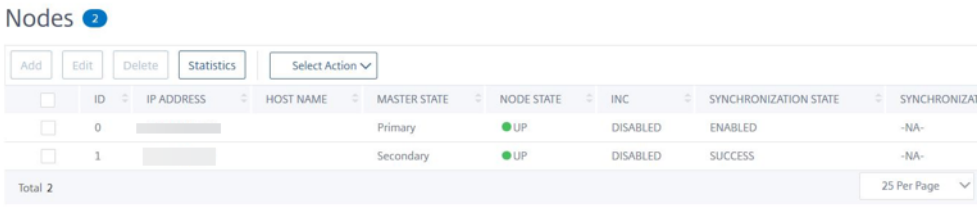
14. Klicken Sie auf **Weiter**.
15. Die Seite **Stack-Optionen konfigurieren** wird angezeigt. Dies ist eine optionale Seite.



16. Klicken Sie auf **Weiter**.
17. Die Seite **Optionen** wird angezeigt. (Dies ist eine optionale Seite.). Klicken Sie auf **Weiter**.
18. Die Seite **Überprüfen** wird angezeigt. Nehmen Sie sich einen Moment Zeit, um die Einstellungen zu überprüfen und gegebenenfalls Änderungen vorzunehmen.
19. Wählen Sie die Option **Ich bestätige, dass AWS CloudFormation IAM-Ressourcen erstellt**. , und klicken Sie dann auf **Stapel erstellen**.
20. Der Status **CREATE-IN-PROGRESS** wird angezeigt. Warten Sie bis der Status **CREATE-COMPLETE**ist. Wenn sich der Status nicht in **COMPLETE**ändert, überprüfen Sie die Registerkarte **Ereignisse** auf den Grund des Fehlers und erstellen Sie die Instanz mit den richtigen Konfigurationen neu.



21. Navigieren Sie nach dem Erstellen einer IAM-Ressource zu **EC2 Management Console > Instanzen**. Sie finden zwei VPX-Instanzen, die mit IAM-Rolle erstellt wurden. Die primären und sekundären Knoten werden jeweils mit drei privaten IP-Adressen und drei Netzwerkschnittstellen erstellt.
22. Melden Sie sich am primären Knoten mit dem Benutzernamen`nsroot` und der Instanz-ID als Kennwort an. Navigieren Sie in der GUI zu **System > Hochverfügbarkeit > Knoten**. Der NetScaler VPX ist bereits von der CloudFormation-Vorlage als HA-Paar konfiguriert.
23. Das NetScaler VPX HA-Paar wird angezeigt.



Überwachen Sie Ihre Instanzen mit Amazon CloudWatch

Sie können den Amazon CloudWatch-Dienst verwenden, um eine Reihe von NetScaler VPX-Metriken wie CPU- und Speicherauslastung und Durchsatz zu überwachen. CloudWatch überwacht Ressourcen und Anwendungen, die auf AWS ausgeführt werden, in Echtzeit. Sie können über die AWS Management Console auf das Amazon CloudWatch-Dashboard zugreifen. Weitere Informationen finden Sie unter Amazon CloudWatch.

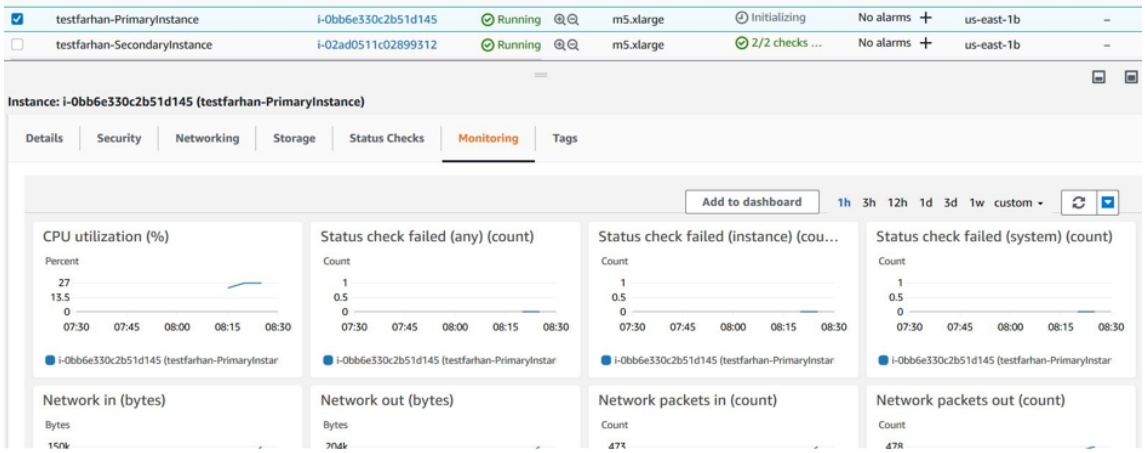
Wichtige Hinweise

- Wenn Sie eine NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert.
- Wenn Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, lautet die Standardoption “Ja”. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie “Nein”.
- Metriken sind für CPU (Verwaltung und Paket-CPU-Auslastung), Arbeitsspeicher und Durchsatz (eingehend und ausgehend) verfügbar.

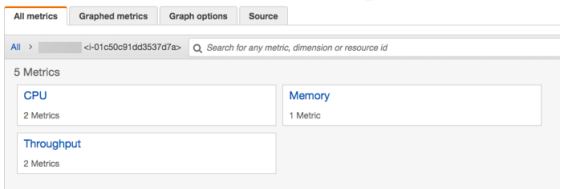
So zeigen Sie CloudWatch-Metriken an

Gehen Sie folgendermaßen vor, um CloudWatch-Metriken für Ihre Instanz anzuzeigen:

1. Melden Sie sich bei **AWS Management Console > EC2 > Instanzen** an.
2. Wählen Sie die Instanz aus.
3. Klicken Sie auf **Überwachung**.
4. Klicken Sie auf **Alle CloudWatch-Metriken anzeigen**.

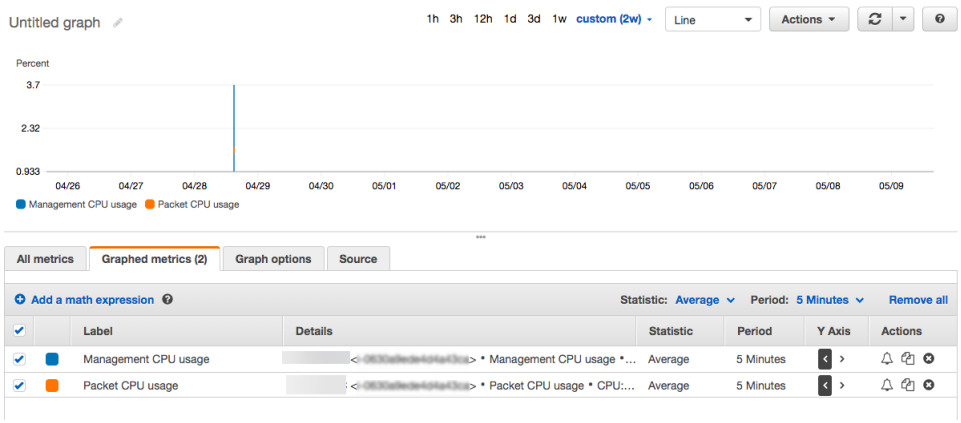


5. Klicken Sie unter Alle Metriken auf Ihre Instanz-ID.



6. Klicken Sie auf die Metriken, die Sie anzeigen möchten, und legen Sie die Dauer fest (nach Minuten, Stunden, Tagen, Wochen, Monaten).
7. Klicken Sie auf **Befehlseinschleusung**, um die Nutzungsstatistiken anzuzeigen. Verwenden Sie die **Graph options**, um Ihr Diagramm anzupassen.

Abbildung. Graphische Metriken für die CPU-



Konfigurieren von SR-IOV auf einem Hochverfügbarkeitssetup

Unterstützung für SR-IOV-Schnittstellen in einem Hochverfügbarkeitssetup ist ab NetScaler Version 12.0 57.19 verfügbar. Weitere Informationen zur Konfiguration von SR-IOV finden Sie unter Konfigurieren von NetScaler VPX-Instanzen für die Verwendung der SR-IOV-Netzwerkschnittstelle.

Zugehörige Ressourcen

So funktioniert Hochverfügbarkeit auf AWS

Hochverfügbarkeit über verschiedene AWS-Verfügbarkeitszonen

May 11, 2023

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen als aktiv-passives Paar mit hoher Verfügbarkeit im Modus Independent Network Configuration (INC) konfigurieren. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Übernahme.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

Wichtige Hinweise

- Lesen Sie die folgenden Dokumente, bevor Sie mit der Bereitstellung beginnen:
  - AWS-Terminologie

  - Voraussetzungen
  - Einschränkungen und Nutzungsrichtlinien
- Das VPX-Hochverfügbarkeitspaar kann sich entweder in derselben Availability Zone in einem anderen Subnetz oder in zwei verschiedenen AWS-Verfügbarkeitszonen befinden.
- Citrix empfiehlt, dass Sie verschiedene Subnetze für die Verwaltung (NSIP), den Clientverkehr (VIP) und den Back-End-Server (SNIP) verwenden.
- Hochverfügbarkeit muss im Modus Independent Network Configuration (INC) festgelegt werden, damit ein Failover funktioniert.
- Für die beiden Instanzen muss Port 3003 für UDP-Verkehr geöffnet sein, da dieser für Heartbeats verwendet wird.
- Die Management-Subnetze beider Knoten müssen über interne NAT Zugriff auf das Internet oder auf den AWS-API-Server haben, damit die restlichen APIs funktionsfähig sind.
- Die IAM-Rolle muss über eine E2-Berechtigung für die öffentliche IP- oder Elastic IP (EIP) -Migration und EC2-Routentabellen-Berechtigungen für die private IP-Migration verfügen.

Sie können Hochverfügbarkeit in AWS Availability Zones auf folgende Weise bereitstellen:

- Verwenden von elastischen IP-Adressen
- Verwenden privater IP-Adressen

Zusätzliche Referenzen

Weitere Informationen zu NetScaler Application Delivery Management (ADM) für AWS finden Sie unter Installieren des NetScalerADM-Agenten auf AWS.

Bereitstellen eines VPX Hochverfügbarkeitspaars mit elastischen IP-Adressen in verschiedenen AWS-Zonen

May 11, 2023

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen mithilfe von elastischen IP-Adressen (EIP) im INC-Modus konfigurieren.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

So funktioniert HA mit EIP-Adressen in verschiedenen AWS-Zonen

Bei einem Failover migriert das EIP des VIP der primären Instanz zur sekundären Instanz, die als neue primäre Instanz übernimmt. Im Failover-Prozess führt die AWS-API:

1. Überprüft die virtuellen Server, an die `IPSets` angeschlossen sind.
2. Sucht die IP-Adresse mit einer zugeordneten öffentlichen IP-Adresse aus den beiden IP-Adressen, die der virtuelle Server überwacht. Eine, die direkt an den virtuellen Server angeschlossen ist, und derjenige, der über den IP-Satz angeschlossen ist.
3. Ordnet die öffentliche IP (EIP) der privaten IP zu, die zum neuen primären VIP gehört.

> **Hinweis**
>
> Um Ihr Netzwerk vor Angriffen wie Denial-of-Service (DoS) zu schützen, können Sie bei der Verwendung eines EIP Sicherheitsgruppen in AWS erstellen, um den IP-Zugriff einzuschränken. Zur Hochverfügbarkeit können Sie gemäß Ihren Bereitstellungen von EIP zu einer privaten IP-Verlagungslösung wechseln.

So stellen Sie ein VPX-Paar mit hoher Verfügbarkeit und elastischen IP-Adressen in verschiedenen AWS-Zonen bereit

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen.

1. Erstellen Sie eine virtuelle Private Cloud von Amazon.
2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones oder in derselben Zone, aber in verschiedenen Subnetzen bereit.
3. Konfigurieren der Hochverfügbarkeit
   a) Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.
   b) Fügen Sie in beiden Instanzen einen IP-Satz hinzu.
   c) Binden Sie die in beiden Instanzen festgelegte IP an den VIP.
   d) Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

Verwenden Sie für die Schritte 1 und 2 die AWS-Konsole. Verwenden Sie für Schritte 3 die NetScaler VPX GUI oder die CLI.

Schritt 1. Erstellen Sie eine Amazon Virtual Private Cloud (VPC).

Schritt 2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones oder in derselben Zone, aber in verschiedenen Subnetzen bereit. Schließen Sie eine EIP an die VIP des primären VPX an.

Weitere Informationen zum Erstellen einer VPC und zum Bereitstellen einer VPX-Instanz auf AWS finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX Instanz auf AWS und Scenario: Standalone-Instanz

Schritt 3. Konfigurieren Sie Hochverfügbarkeit. Sie können die NetScaler VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

Konfigurieren Sie Hochverfügbarkeit über die CLI

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

   Auf dem primären Knoten:

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   ```

   Auf dem sekundären Knoten:

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   ```

   <sec_ip> bezieht sich auf die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens

   <prim_ip> bezieht sich auf die private IP-Adresse der Verwaltungs-NIC des primären Knotens

2. Fügen Sie das IP-Set in beiden Instanzen hinzu.

   Geben Sie in beiden Instanzen den folgenden Befehl ein.

   ```
   add ipset <ipsetname>
   ```

3. Binden Sie den IP-Satz an den VIP-Satz auf beiden Instanzen.

   Geben Sie in beiden Instanzen den folgenden Befehl ein:

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   ```

   ```
   bind ipset <ipsetname> <secondary VIP>
   ```

   > **Hinweis**
   >
   > Sie können den IP-Satz an den primären VIP oder an den sekundären VIP binden. Wenn Sie den IP-Satz jedoch an den primären VIP binden, verwenden Sie den sekundären VIP, um ihn dem virtuellen Server hinzuzufügen, und umgekehrt.

4. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Geben Sie den folgenden Befehl ein:

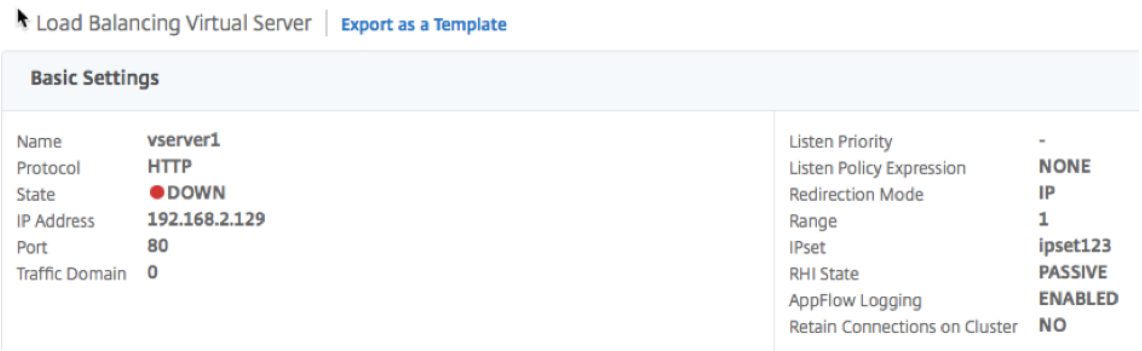
   ```
   add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
   > -ipset \<ipset_name>
   ```

Konfigurieren der Hochverfügbarkeit mit der GUI

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein
2. Melden Sie sich mit dem Benutzernamen `nsroot` und der Instanz-ID als Kennwort am primären Knoten an.
3. Gehen Sie in der GUI zu **Konfiguration** > **System** > **Hochverfügbarkeit**. Klicken Sie auf **Hinzufügen**.

4. Fügen Sie im Feld **IP-Adresse des Remote-Nodes** die private IP-Adresse der Management-NIC des sekundären Knotens hinzu.
5. Wählen Sie **den Modus NIC (Unabhängige Netzwerkkonfiguration) auf Selbstknoten einschalten** .
6. Fügen Sie unter **Remote System Login Credential**den Benutzernamen und das Kennwort für den sekundären Knoten hinzu und klicken Sie auf **Erstellen**.
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie den IP-Satz hinzu und binden Sie den IP-Satz an den VIP-Satz beider Instanzen
9. Navigieren Sie in der GUI zu **System** > **Netzwerk** > **IPs** > **Hinzufügen**.
10. Fügen Sie die erforderlichen Werte für IP-Adresse, Netzwerkmaske, IP-Typ (virtuelle IP) hinzu und klicken Sie auf **Erstellen**.
11. Navigieren Sie zu **System** > **Netzwerk** > **IP-Sets** > **Hinzufügen**. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
12. Wählen Sie auf der Seite IPv4s die virtuelle IP aus und klicken Sie auf **Einfügen**. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.
13. Fügen Sie einen virtuellen Server in der primären Instanz hinzu

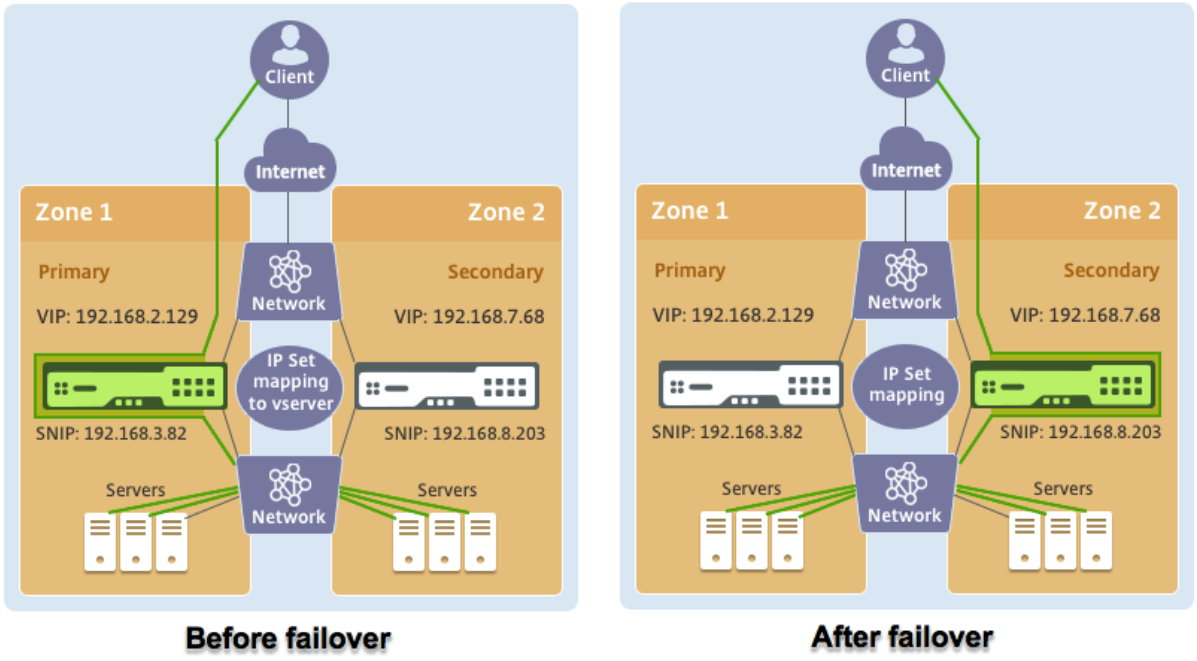
    Gehen Sie in der GUI zu **Konfiguration** > **Traffic Management** > **Virtuelle Server** > **Hinzufügen**.



Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Availability Zones erstellt. Jede Instanz hat drei Subnetze - eines für die Verwaltung, eines für den Client und eines für den Backend-Server. Ein EIP ist an den VIP des primären Knotens angeschlossen.

Diagramm: Dieses Diagramm veranschaulicht das NetScaler VPX Hochverfügbarkeits-Setup im INC-Modus in AWS



Verwenden Sie für dieses Szenario CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

   Geben Sie die folgenden Befehle auf dem primären und sekundären Knoten ein.

   Auf Primär:

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   Hier bezieht sich 192.168.6.82 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   In der Sekundarstufe:

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   Hier bezieht sich 192.168.1.108 auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen IP-Satz hinzu und binden Sie den IP-Satz auf beiden Instanzen an den VIP

   In der Primarschule:

   ```
   add ipset ipset123
   ```

   ```
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   ```

   ```
   bindipset ipset123 192.168.7.68
   ```

   In der Sekundarstufe:

   ```
   add ipset ipset123
   ```



```
add ns ip 192.168.7.68 255.255.255.0 -type VIP

bind ipset ipset123 192.168.7.68
```

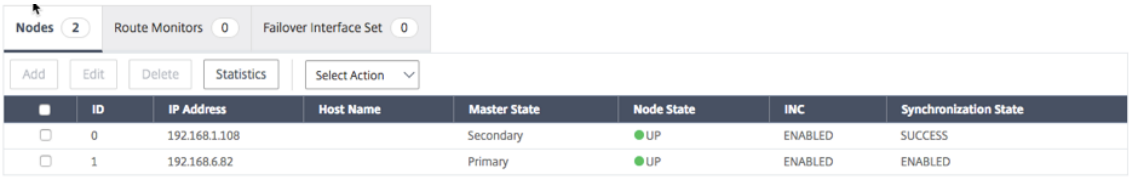
3. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Der folgende Befehl:

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Speichern Sie die Konfiguration.

5. Nach einem erzwungenen Failover wird der sekundäre zum neuen primären.



Bereitstellen eines VPX Hochverfügbarkeitspaars mit privaten IP-Adressen in verschiedenen AWS-Zonen

May 11, 2023

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen mit privaten IP-Adressen im INC-Modus konfigurieren. Diese Lösung kann einfach in das vorhandene Multizonen-VPX-Hochverfügbarkeitspaar mit elastischen IP-Adressenintegriert werden. Daher können Sie beide Lösungen zusammen verwenden.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

> **Hinweis:**
>
> Diese Bereitstellung wird ab NetScaler Release 13.0 Build 67.39 unterstützt. Diese Bereitstellung ist mit AWS Transit Gateway kompatibel.

Hochverfügbarkeits-Paar mit privaten IP-Adressen unter Verwendung von AWS nicht gemeinsam genutzter VPC

Voraussetzungen

Stellen Sie sicher, dass die mit Ihrem AWS-Konto verknüpfte IAM-Rolle über die folgenden IAM-Berechtigungen verfügt:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
         }

    ]
 }


<!--NeedCopy-->
```

Bereitstellen eines VPX-HA-Paars mit privaten IP-Adressen mithilfe der nicht gemeinsam genutzten AWS VPC

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen unter Verwendung privater IP-Adressen.

1. Erstellen Sie eine virtuelle Private Cloud von Amazon.

2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones bereit.
3. Konfigurieren der Hochverfügbarkeit
    a) Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.
    b) Fügen Sie die entsprechenden Routentabellen in der VPC hinzu, die auf die Clientschnittstelle verweist.
    c) Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

Verwenden Sie für die Schritte 1, 2 und 3b die AWS-Konsole. Verwenden Sie für Schritt 3a und 3c die NetScaler VPX GUI oder die CLI.

Schritt 1. Erstellen Sie eine Amazon Virtual Private Cloud (VPC).

Schritt 2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones mit der gleichen Anzahl von ENI (Network Interface) bereit.

Weitere Informationen zum Erstellen einer VPC und zum Bereitstellen einer VPX-Instanz auf AWS finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX Instanz auf AWS und Scenario: Standalone-Instanz

Schritt 3. Konfigurieren Sie die ADC-VIP-Adressen, indem Sie ein Subnetz auswählen, das sich nicht mit den Amazon VPC-Subnetzen überschneidet. Wenn Ihre VPC 192.168.0.0/16 ist, können Sie zur Konfiguration von ADC-VIP-Adressen ein beliebiges Subnetz aus diesen IP-Adressbereichen auswählen:

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

In diesem Beispiel wurde das ausgewählte 10.10.10.0/24-Subnetz und VIPs in diesem Subnetz erstellt. Sie können ein beliebiges Subnetz außer dem VPC-Subnetz (192.168.0.0/16) wählen.

Schritt 4. Fügen Sie aus der VPC-Routingtabelle eine Route hinzu, die auf die Clientschnittstelle (VIP) des primären Knotens verweist.

Geben Sie in der AWS CLI den folgenden Befehl ein:

```
1 aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-
     block 10.10.10.0/24 --gateway-id <eni-client-primary>
2 <!--NeedCopy-->
```

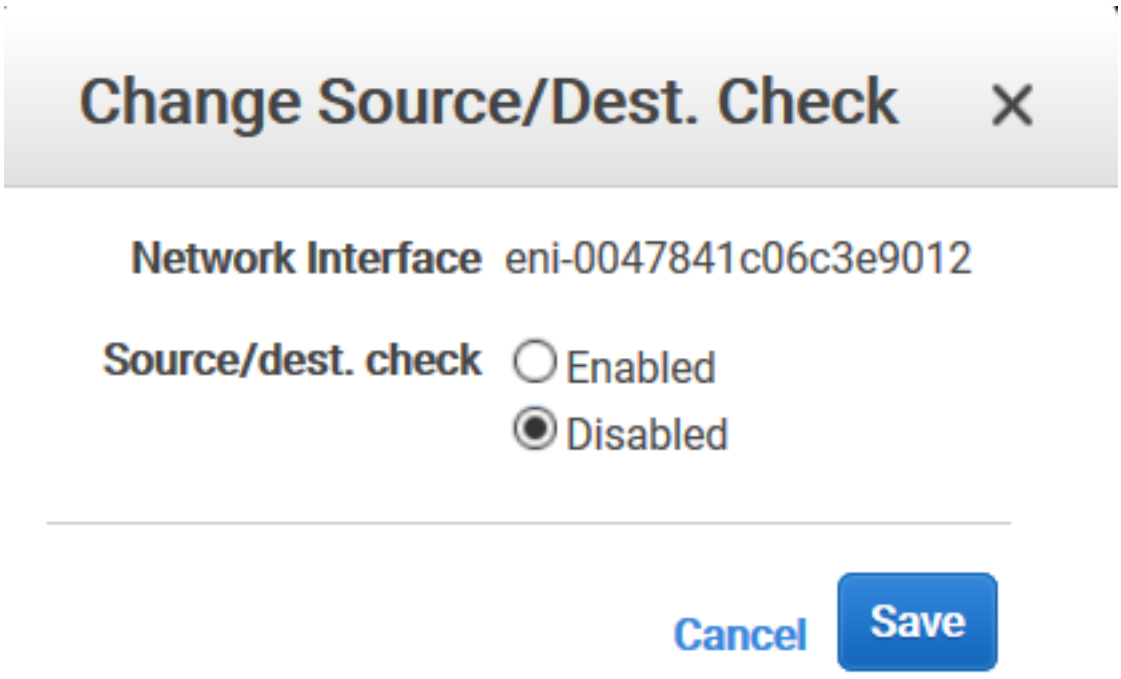
Führen Sie in der AWS-GUI die folgenden Schritte aus, um eine Route hinzuzufügen:

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Route Tables**und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie **Aktionen**und klicken Sie auf **Routen bearbeiten**.
4. Um eine Route hinzuzufügen, wählen Sie **Route hinzufügen**. Geben Sie für **Destination**den Ziel-CIDR-Block, eine einzelne IP-Adresse oder die ID einer Präfixliste ein. Wählen Sie für Gateway-ID das ENI einer Client-Schnittstelle des primären Knotens aus.

> **Hinweis:**
>
> Sie müssen **Source/Dest-Check** auf dem Client-ENI der primären Instanz deaktivieren.

Um die Quell-/Zielüberprüfung für eine Netzwerkschnittstelle mithilfe der Konsole zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Network Interfaces**aus.
3. Wählen Sie die Netzwerkschnittstelle einer primären Clientschnittstelle aus, wählen Sie **Aktionen**aus und klicken Sie auf Quelle/Dest **ändern. Überprüfe**.
4. Wählen Sie im Dialogfeld **Deaktiviert**und klicken Sie auf **Speichern**.



Schritt 5. Konfigurieren Sie Hochverfügbarkeit. Sie können die NetScaler VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

Konfigurieren Sie Hochverfügbarkeit über die CLI

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

   Auf dem primären Knoten:

   ```
   1 add ha node 1 <sec_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   Auf dem sekundären Knoten:

   ```
   1 add ha node 1 <prim_ip> -inc ENABLED
   2 <!--NeedCopy-->
   ```

   <sec_ip>bezieht sich auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   <prim_ip>bezieht sich auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu. Sie müssen es aus dem ausgewählten Subnetz hinzufügen, z. B. 10.10.10.0/24.

   Geben Sie den folgenden Befehl ein:

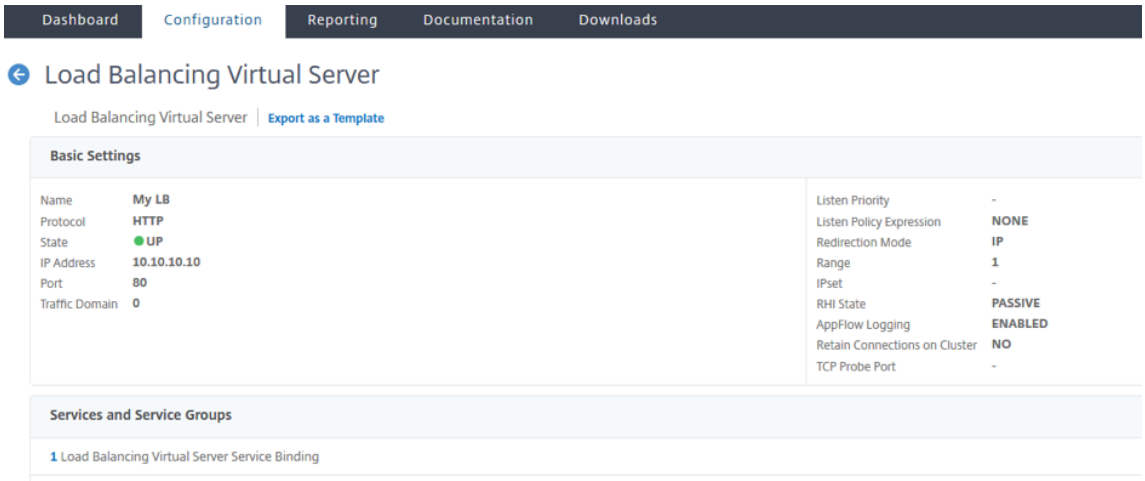
   ```
   1 add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<
       primary\_vip\> \<port\>
   2 <!--NeedCopy-->
   ```

Konfigurieren der Hochverfügbarkeit mit der GUI

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein
2. Melden Sie sich mit dem Benutzernamen `nsroot` und der Instanz-ID als Kennwort am primären Knoten an.
3. Navigieren Sie zu **Konfiguration** > **System** > **Hochverfügbarkeit**und klicken Sie auf **Hinzufügen**.
4. Fügen Sie im Feld **IP-Adresse des Remote-Nodes** die private IP-Adresse der Management-NIC des sekundären Knotens hinzu.
5. Wählen Sie **den Modus NIC (Unabhängige Netzwerkkonfiguration) auf Selbstknoten einschalten** .

6. Fügen Sie unter **Remote System Login Credential**den Benutzernamen und das Kennwort für den sekundären Knoten hinzu und klicken Sie auf **Erstellen**.
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie einen virtuellen Server in der primären Instanz hinzu

   Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Virtuelle Server** > **Hinzufügen**.



Bereitstellen eines VPX-HA-Paars mit privaten IP-Adressen mithilfe von AWS Shared VPC

In einem gemeinsam genutzten AWS-VPC-Modell teilt sich das Konto, dem die VPC (Eigentümer) gehört, ein oder mehrere Subnetze mit anderen Konten (Teilnehmern). Daher haben Sie ein VPC-Besitzerkonto und ein Teilnehmerkonto. Nachdem ein Subnetz freigegeben wurde, können die Teilnehmer ihre Anwendungsressourcen in den für sie freigegebenen Subnetzen anzeigen, erstellen, ändern und löschen. Teilnehmer können keine Ressourcen anzeigen, ändern oder löschen, die anderen Teilnehmern oder dem VPC-Besitzer gehören.

Informationen zur gemeinsam genutzten AWS-VPC finden Sie in der AWS-Dokumentation.

> **Hinweis:**
>
> Die Konfigurationsschritte für die Bereitstellung eines VPX-HA-Paars mit privaten IP-Adressen unter Verwendung der gemeinsam genutzten AWS-VPC entsprechen denen der Bereitstellung eines VPX-HA-Paars mit privaten IP-Adressen unter Verwendung der nicht gemeinsam genutzten AWS VPC mit der folgenden Ausnahme:
>
> - Die Routing-Tabellen in der VPC, die auf die Clientschnittstelle verweisen, müssen aus dem *VPC-Besitzerkonto*hinzugefügt werden.

Voraussetzungen

- Stellen Sie sicher, dass die IAM-Rolle, die der NetScaler VPX-Instance im AWS-Teilnehmerkonto zugeordnet ist, über die folgenden IAM-Berechtigungen verfügt:

```
"Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DisassociateAddress",
                "iam:GetRole",
                "iam:SimulatePrincipalPolicy",
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                 “ec2:AssociateAddress” ,
                "sts:AssumeRole"
        ],
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> Hinweis:
>
> Mit der **AssumeRole** kann die NetScaler VPX-Instanz die kontenübergreifende IAM-Rolle übernehmen, die vom VPC-Besitzerkonto erstellt wird.

- Stellen Sie sicher, dass das VPC-Besitzerkonto dem Teilnehmerkonto mithilfe der kontenübergreifenden IAM-Rolle die folgenden IAM-Berechtigungen bereitstellt:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
```



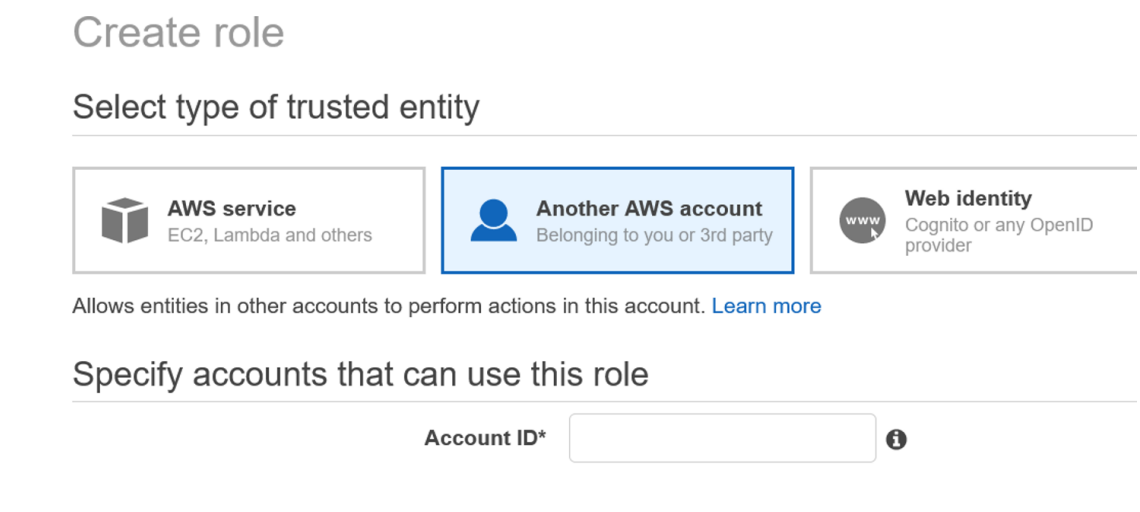
```
                    "ec2:CreateRoute",
                    "ec2:DeleteRoute",
                    "ec2:DescribeRouteTables"
                ],
                "Resource": "*"
            }

        ]
    }

<!--NeedCopy-->
```

Erstellen einer kontenübergreifenden IAM-Rolle

1. Melden Sie sich bei der AWS-Webkonsole an.
2. Navigieren Sie auf der Registerkarte **IAM** zu **Roles**, und wählen Sie dann **Create Role**aus.
3. Wählen Sie **ein anderes AWS-Konto**.



4. Geben Sie die 12-stellige Konto-ID des Teilnehmerkontos ein, auf das Sie Administratorzugriff gewähren möchten.

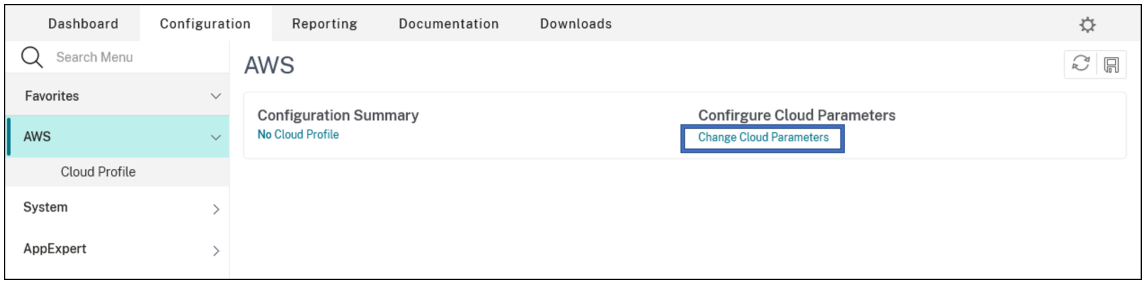
Festlegen der kontenübergreifenden IAM-Rolle mithilfe der NetScaler CLI

Mit dem folgenden Befehl kann die NetScaler VPX-Instanz die kontoübergreifende IAM-Rolle übernehmen, die im VPC-Besitzerkonto vorhanden ist.

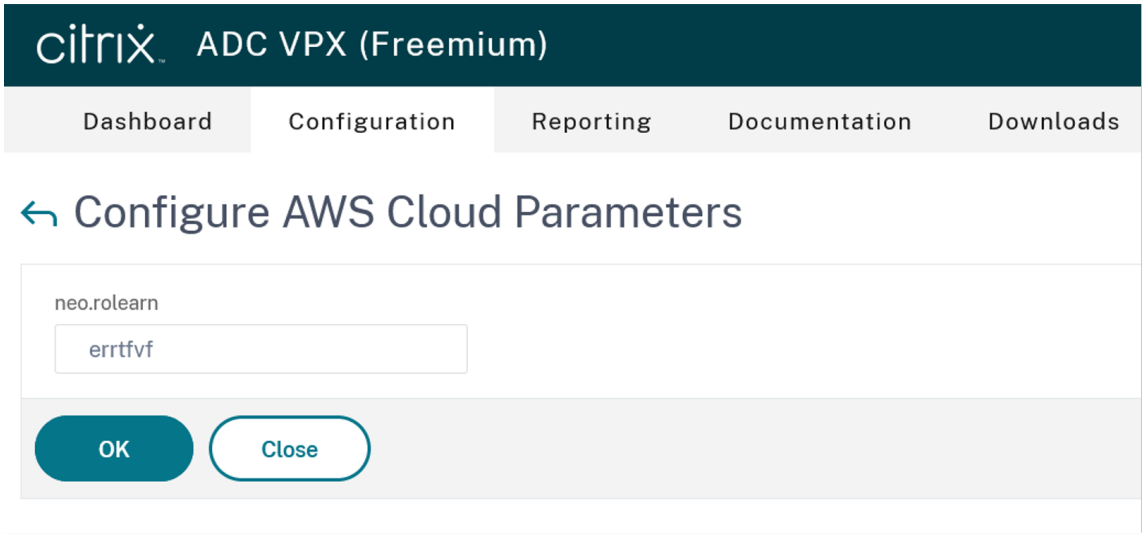
```
set cloud awsParam -roleARN <string>
<!--NeedCopy-->
```


Festlegen der kontenübergreifenden IAM-Rolle mithilfe der NetScaler GUI

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration > AWS > Cloud-Parameter ändern**.



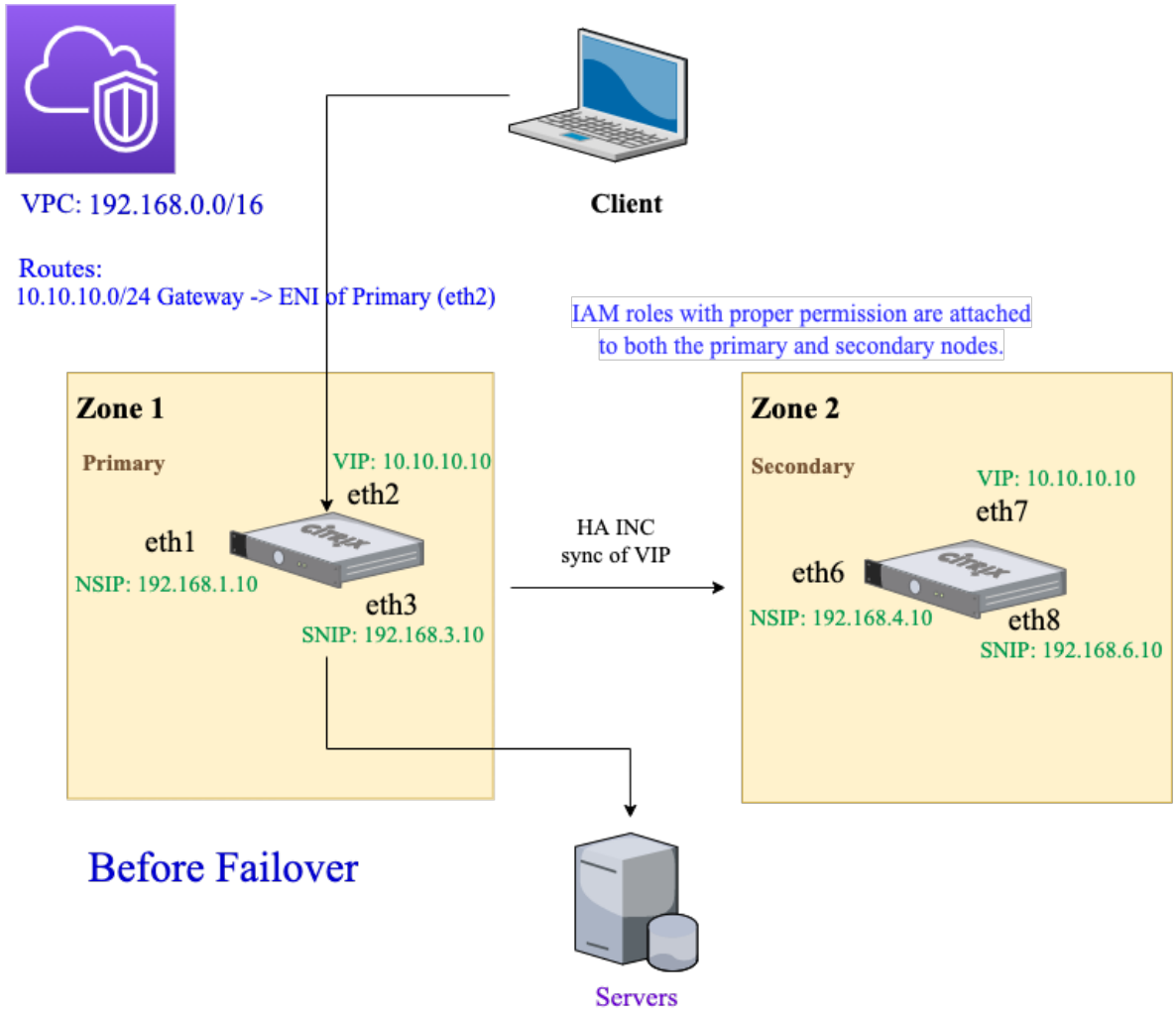
2. Geben **Sie auf der Seite "AWS Cloud-Parameter konfigurieren** " einen Wert für das Feld **Rolearn** ein.

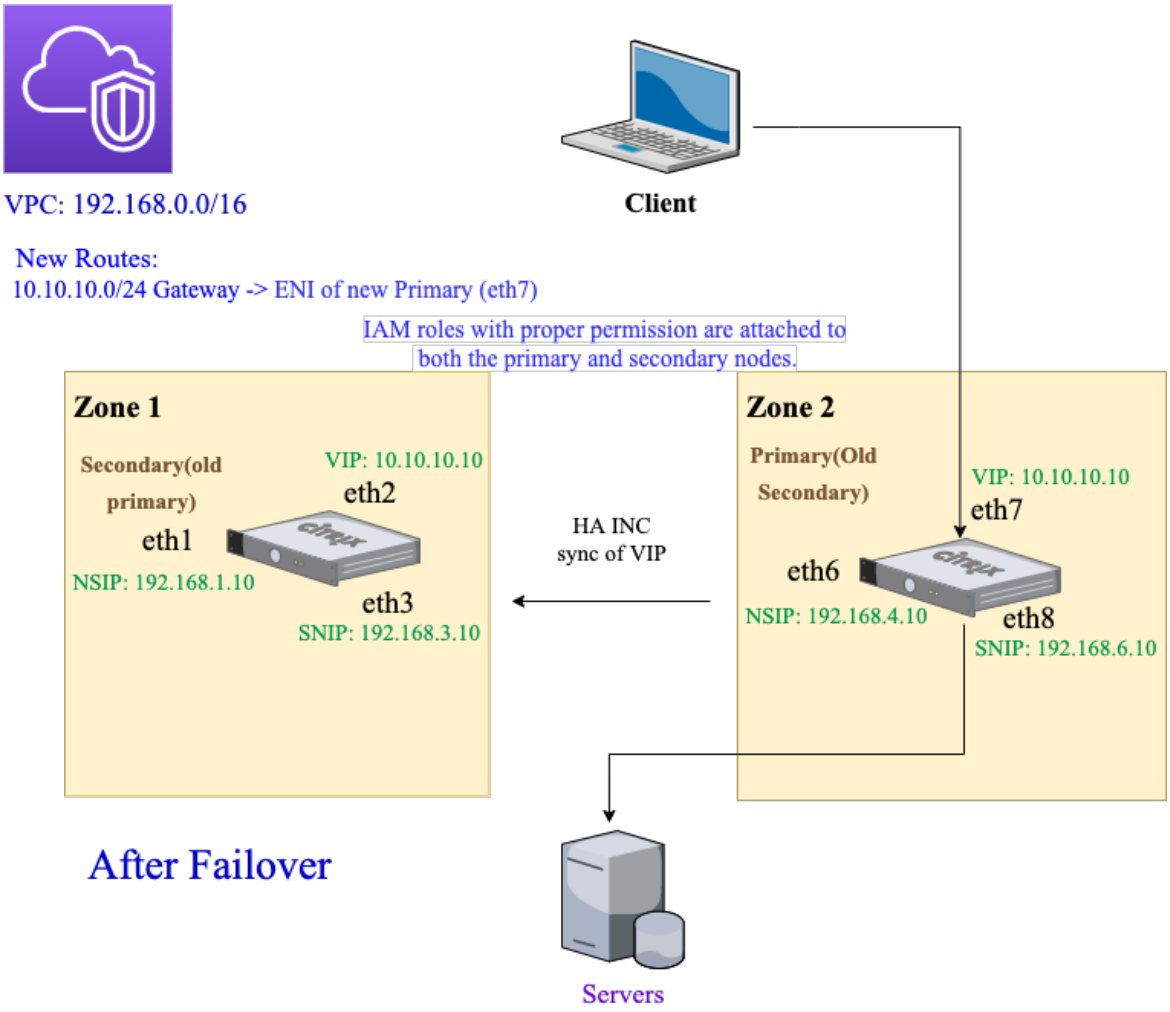


Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Availability Zones erstellt. Jede Instanz hat drei Subnetze - eines für die Verwaltung, eines für den Client und eines für den Backend-Server.

Die folgenden Diagramme veranschaulichen das NetScaler VPX Hochverfügbarkeitssetup im INC-Modus auf AWS. Das benutzerdefinierte Subnetz 10.10.10.10, das nicht Teil der VPC ist, wird als VIP verwendet. Daher kann das Subnetz 10.10.10.10 über Availability Zones hinweg verwendet werden.





Verwenden Sie für dieses Szenario CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

   Geben Sie die folgenden Befehle auf dem primären und sekundären Knoten ein.

   Auf dem primären Knoten:

   ```
   add ha node 1 192.168.4.10 -inc enabled
   <!--NeedCopy-->
   ```

   Hier bezieht sich 192.168.4.10 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   Auf dem sekundären Knoten:

   ```
   add ha node 1 192.168.1.10 -inc enabled
   <!--NeedCopy-->
   ```


Hier bezieht sich 192.168.1.10 auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

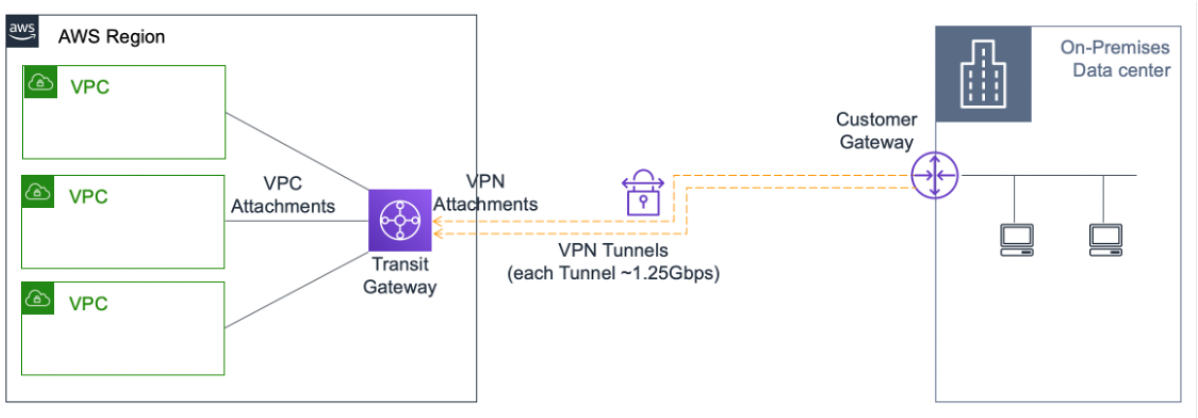
   Geben Sie den folgenden Befehl ein:

```
add lbvserver vserver1 http 10.10.10.10 80
<!--NeedCopy-->
```

3. Speichern Sie die Konfiguration.
4. Nach einem erzwungenen Failover:
   - Die sekundäre Instanz wird zur neuen primären Instanz.
   - Die VPC-Route, die auf die primäre ENI zeigt, migriert zum sekundären Client-ENI.
   - Der Clientverkehr wird auf die neue primäre Instanz fortgesetzt.

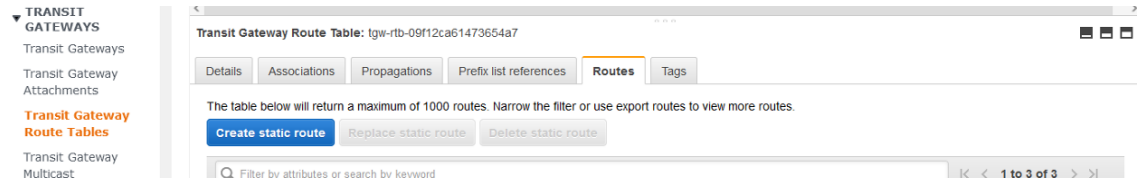
AWS Transit Gateway-Konfiguration für eine private HA-IP-Lösung

Sie benötigen AWS Transit Gateway, um das private VIP-Subnetz innerhalb des internen Netzwerks über AWS-VPCs, Regionen und lokale Netzwerke hinweg routbar zu machen. Die VPC muss eine Verbindung zu AWS Transit Gateway herstellen. Eine statische Route für das VIP-Subnetz oder den IP-Pool in der AWS Transit Gateway-Routingtabelle wird erstellt und auf die VPC gerichtet.

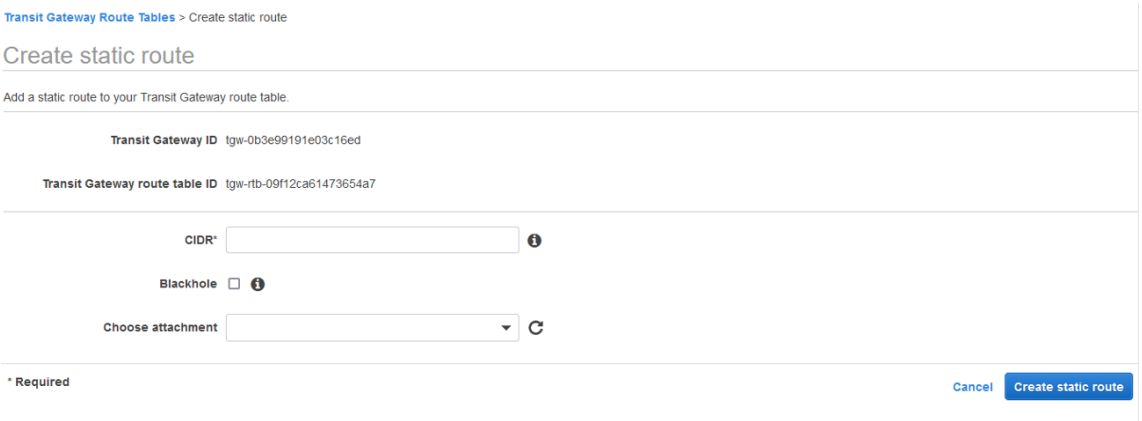


Gehen Sie folgendermaßen vor, um AWS Transit Gateway zu konfigurieren:

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich **Transit Gateway Route Table** aus.
3. Wählen Sie die Registerkarte **Routen** und klicken Sie auf **Statische Route erstellen**.



4. Erstellen Sie eine statische Route, bei der CIDR auf Ihr privates VIPS-Subnetz und die Anschlusspunkte auf die VPC mit NetScaler VPX verweist.



5. Klicken Sie auf **Statische Route erstellen**und wählen Sie dann **Schließen**.

Problembehandlung

Wenn Sie bei der Konfiguration der privaten HA-IP-Lösung für Multizonen-HA auf Probleme stoßen, überprüfen Sie die folgenden wichtigen Punkte zur Fehlerbehebung:

- Sowohl der primäre als auch der sekundäre Knoten haben dieselben IAM-Berechtigungen.
- Der INC-Modus ist sowohl auf dem primären als auch auf dem sekundären Knoten aktiviert.
- Sowohl der primäre als auch der sekundäre Knoten haben die gleiche Anzahl von Schnittstellen.
- Folgen Sie beim Erstellen einer Instanz derselben Reihenfolge beim Anhängen von Schnittstellen an beiden Knoten. Auf einem primären Knoten, wenn zuerst die Client-Schnittstelle und dann die Serverschnittstelle angeschlossen wird. Folgen Sie dann der gleichen Reihenfolge auch auf dem sekundären Knoten. Wenn es eine Diskrepanz gibt, trennen Sie die Schnittstellen und fügen Sie sie in der richtigen Reihenfolge wieder an.
- Wenn kein Verkehr fließt, vergewissern Sie sich, dass die “Source/dest. Check” ist auf der Client-Oberfläche des primären Knotens beim ersten Mal deaktiviert.
- Stellen Sie sicher, dass der Befehl cloudhadaemon (`ps -aux | grep cloudha`) in der Shell ausgeführt wird.
- Stellen Sie sicher, dass die NetScaler-Firmware-Version 13.0 Build 70.x oder höher ist.
- Bei Problemen mit dem Failover-Prozess überprüfen Sie die Protokolldatei unter: /var/log/cloud-ha-daemon.log

Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts

May 11, 2023

AWS Outposts ist ein Pool von AWS-Rechen- und Speicherkapazität, der an Ihrem Standort bereitgestellt wird. Outposts stellt AWS-Infrastruktur und -Services an Ihrem On-Premises-Standort bereit. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS-Region. Sie können dieselben NetScaler VPX-Instanzen, AWS-APIs, Tools und Infrastrukturen on-premises und in der AWS-Cloud verwenden, um ein konsistentes Hybriderlebnis zu erzielen.

Sie können Subnetze auf Ihren Outposts erstellen und diese angeben, wenn Sie AWS-Ressourcen wie EC2-Instanzen, EBS-Volumes, ECS-Cluster und RDS-Instanzen erstellen. Instanzen in den Außenposten-Subnetzen kommunizieren mit anderen Instanzen in der AWS-Region über private IP-Adressen, alle innerhalb derselben Amazon Virtual Private Cloud (VPC).

Weitere Informationen finden Sie im Benutzerhandbuch für AWS Outposts.

Funktionsweise von AWS Outposts

AWS Outposts ist für den Betrieb mit einer ständigen und konsistenten Verbindung zwischen Ihren Outposts und einer AWS-Region konzipiert. Um diese Verbindung zur Region und zu den lokalen Workloads in Ihrer on-premises Umgebung herzustellen, müssen Sie Ihren Outpost mit Ihrem on-premises Netzwerk verbinden. Ihr on-premises Netzwerk muss einen WAN-Zugriff zurück zur Region und zum Internet bieten. Das Internet muss auch einen LAN- oder WAN-Zugriff auf das lokale Netzwerk bieten, in dem sich Ihre on-premises Workloads oder Anwendungen befinden.

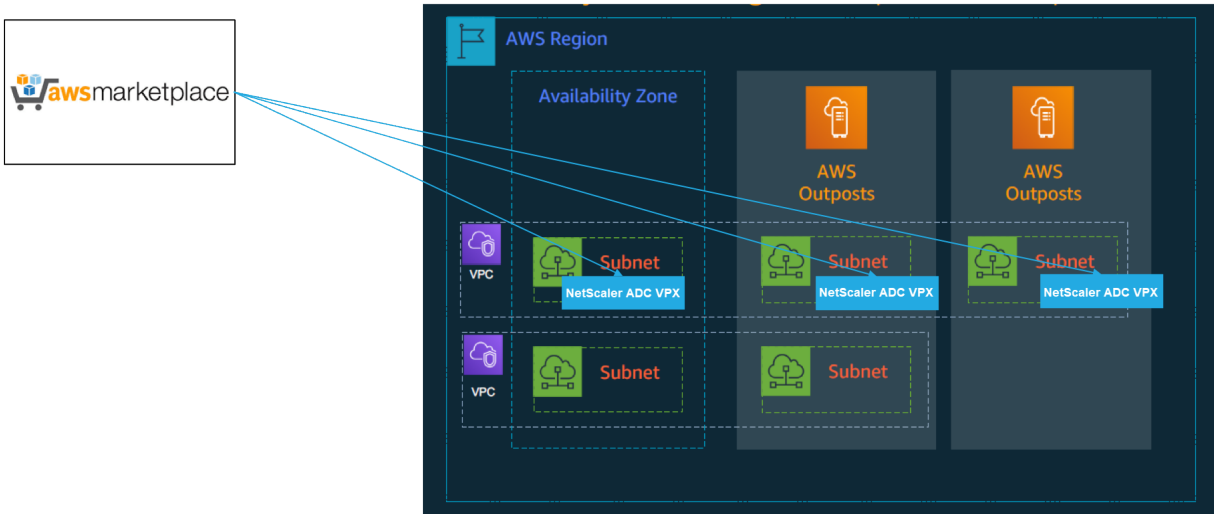
Voraussetzung

- Sie müssen einen AWS Outposts in Ihrer Site installieren.
- Die Rechen- und Speicherkapazität der AWS Outposts muss zur Nutzung verfügbar sein.

Weitere Informationen zur Bestellung von AWS Outposts finden Sie in der folgenden AWS-Dokumentation:
https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

NetScaler VPX-Instanz auf AWS Outposts mit der AWS-Webkonsole bereitstellen

Die folgende Abbildung zeigt eine einfache Bereitstellung von NetScaler VPX-Instanzen auf den Outposts. Das im AWS Marketplace vorhandene NetScaler AMI wird auch in den Outposts bereitgestellt.



Melden Sie sich bei der AWS-Webkonsole an und führen Sie die folgenden Schritte aus, um NetScaler VPX EC2-Instances auf Ihren AWS-Outposts bereitzustellen.

1. Erstellen Sie ein Schlüsselpaar.
2. Erstellen Sie eine Virtual Private Cloud (VPC).
3. Fügen Sie weitere Subnetze hinzu.
4. Erstellen Sie Sicherheitsgruppen und Sicherheitsregeln.
5. Fügen Sie Routingtabellen hinzu.
6. Erstellen Sie ein Internet-Gateway.
7. Erstellen Sie eine NetScaler VPX-Instance mithilfe des AWS EC2-Service.
   Navigieren Sie im AWS-Dashboard zu **Compute > EC2 > Launch Instanz > AWS Marketplace**.
8. Erstellen Sie mehr Netzwerkschnittstellen und fügen Sie sie hinzu.
9. Hängen Sie elastische IPs an die Management-NIC an.
10. Stellen Sie eine Verbindung mit der VPX-Instanz her.

Ausführliche Anweisungen zu jedem der Schritte finden Sie unter Bereitstellen einer NetScaler VPX-Instanz in AWS mithilfe der AWS-Webkonsole.

Informationen zur Hochverfügbarkeit innerhalb derselben Availability Zone-Bereitstellung finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

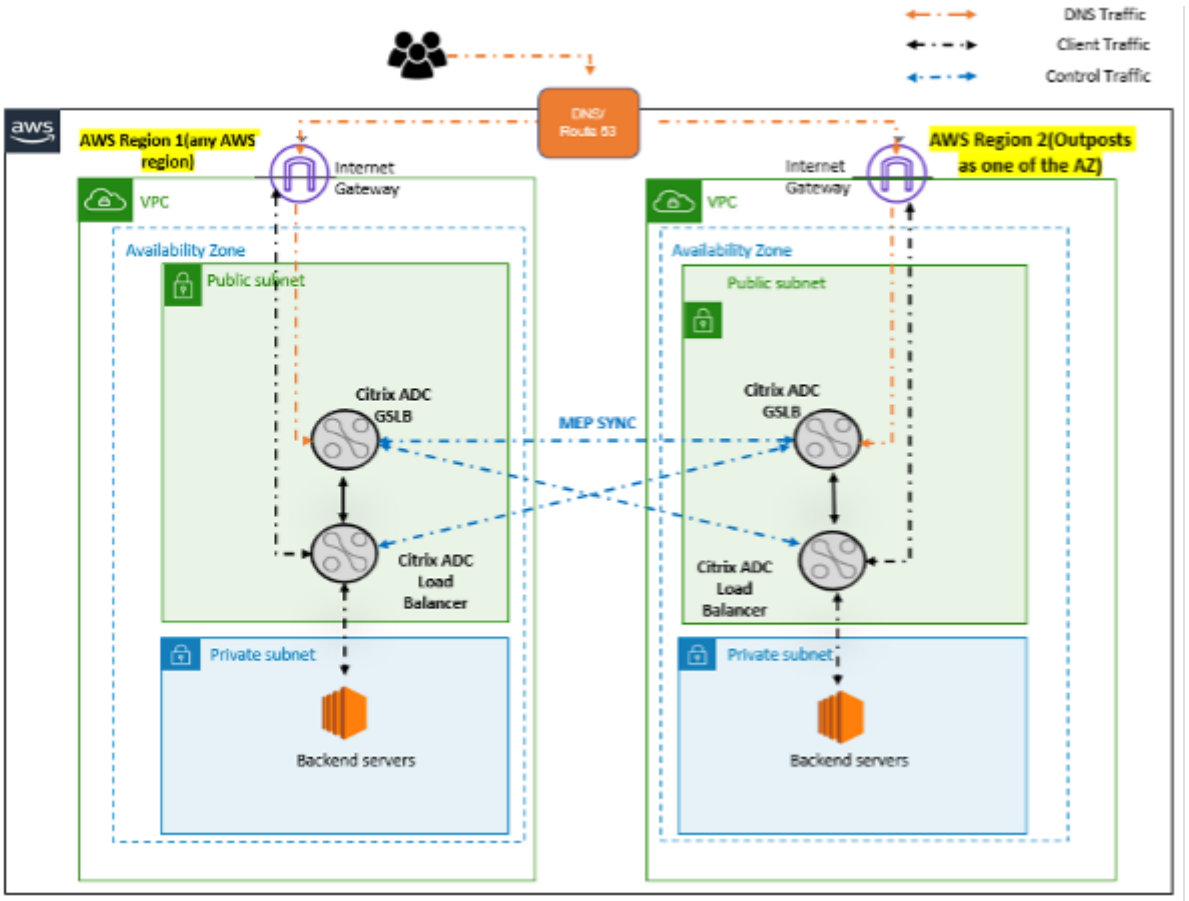
Eine NetScaler VPX-Instanz in der Hybrid Cloud mit AWS Outposts bereitstellen

Sie können eine NetScaler VPX-Instanz in einer Hybrid Cloud in einer AWS-Umgebung bereitstellen, die AWS-Outposts enthält. Sie können den Mechanismus zur Bereitstellung von Apps mithilfe der NetScaler Global Server Load Balancing (GSLB) -Lösung vereinfachen. Die GSLB-Lösung verteilt den Anwendungsdatenverkehr auf mehrere Rechenzentren in Hybrid-Clouds, die auf der Grundlage der AWS-Regionen und der Infrastruktur von AWS Outpost erstellt wurden.

NetScaler GSLB unterstützt sowohl die aktiv-aktiven als auch die aktiv-passiven Bereitstellungstypen,

um verschiedene Anwendungsfälle zu adressieren. Zusammen mit diesen flexiblen Bereitstellungsoptionen und Mechanismen zur Anwendungsbereitstellung sichert NetScaler das gesamte Netzwerk- und Anwendungsportfolio, unabhängig davon, ob Anwendungen nativ in der AWS Cloud oder in AWS Outposts bereitgestellt werden.

Das folgende Diagramm zeigt eine Anwendungsbereitstellung mit der NetScaler Appliance in der Hybrid Cloud mit AWS.



In einer aktiven und aktiven Bereitstellung steuert der NetScaler den Datenverkehr global über eine verteilte Umgebung. Alle Standorte in der Umgebung tauschen über das Metrics Exchange Protocol (MEP) Kennzahlen über ihre Verfügbarkeit und den Zustand der Ressourcen aus. Die NetScaler-Appliance verwendet diese Informationen, um den Datenverkehr zwischen den Standorten zu verteilen, und sendet Clientanforderungen an die am besten geeigneten GSLB-Site, die durch die in der GSLB-Konfiguration angegebene definierte Methode (Round Robin, kleinste Verbindung und statische Nähe) bestimmt wird.

Sie können das aktiv-aktive GSLB-Deployment verwenden, um:

- Optimieren Sie die Ressourcenauslastung, wenn alle Knoten aktiv sind.
- Verbessern Sie die Benutzererfahrung, indem Sie Anfragen an die Website weiterleiten, die jedem einzelnen Benutzer am nächsten ist.

- Migrieren Sie Anwendungen in einem benutzerdefinierten Tempo in die Cloud.

Sie können das aktiv-passive GSLB-Deployment verwenden für:

- Notfallwiederherstellung
- Cloudburst

Referenzen

- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- NetScaler VPX-Instanz auf AWS Outposts mit der AWS-Webkonsole bereitstellen
- Konfigurieren von GSLB auf NetScaler VPX-Instanzen

Schützen Sie das AWS API Gateway mithilfe der NetScaler Web App Firewall

May 11, 2023

Sie können eine NetScaler Appliance vor Ihrem AWS API Gateway bereitstellen und das API-Gateway vor externen Bedrohungen schützen. NetScaler Web App Firewall (WAF) kann Ihre API vor den 10 wichtigsten OWASP-Bedrohungen und Zero-Day-Angriffen schützen. NetScaler Web App Firewall verwendet eine einzige Codebasis für alle ADC-Formfaktoren. Daher können Sie Sicherheitsrichtlinien in jeder Umgebung konsequent anwenden und durchsetzen. NetScaler Web App Firewall ist einfach zu implementieren und als Einzellizenz erhältlich. Die NetScaler Web App Firewall bietet Ihnen die folgenden Funktionen:

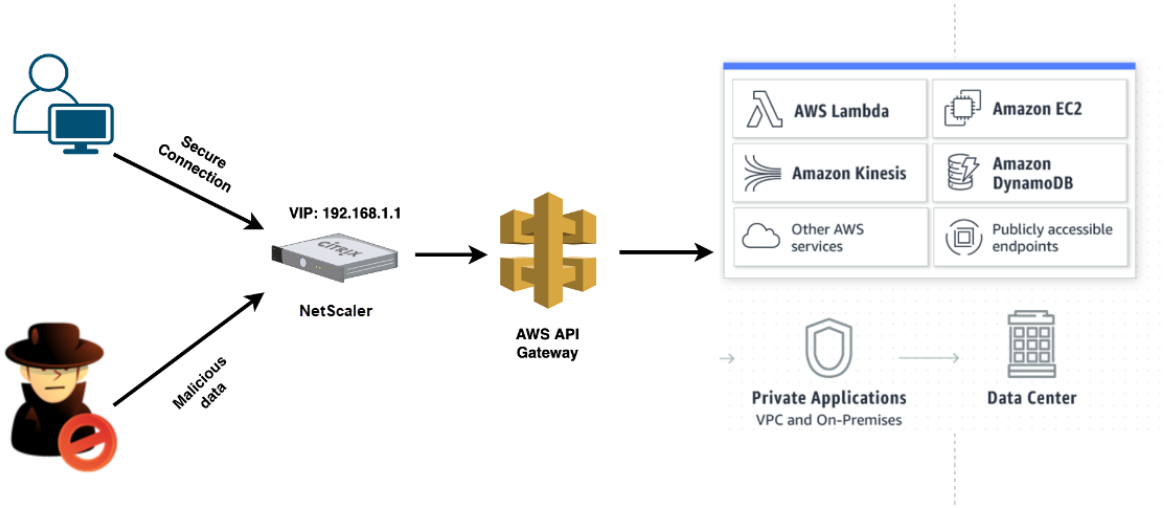
- Vereinfachte Konfiguration
- Bot-Verwaltung
- Ganzheitliche Sichtbarkeit
- Sammeln Sie Daten aus mehreren Quellen und zeigen Sie die Daten in einem einheitlichen Bildschirm an

Zusätzlich zum API-Gateway-Schutz können Sie auch die anderen NetScaler-Funktionen verwenden. Weitere Informationen finden Sie in der NetScaler-Dokumentation. Um Ausfallzeiten von Rechenzentren zu vermeiden und die Herunterfahrzeit zu minimieren, können Sie ADC in oder über Availability Zones hinweg in Hochverfügbarkeit versetzen. Sie können auch Clustering mit der Autoscale-Funktion verwenden oder konfigurieren.

Zuvor unterstützte AWS API Gateway den erforderlichen Schutz nicht, um die dahinter stehenden Anwendungen zu sichern. Ohne den Schutz der Web Application Firewall (WAF) waren APIs anfällig für Sicherheitsbedrohungen.

Stellen Sie die NetScaler Appliance vor dem AWS API-Gateway bereit

Im folgenden Beispiel wird eine NetScaler Appliance vor dem AWS-API-Gateway bereitgestellt.



Nehmen wir an, es gibt eine echte API-Anforderung für den AWS Lambda-Service. Diese Anforderung kann für jeden der API-Dienste gelten, wie in der Amazon API Gateway-Dokumentationerwähnt. Wie im vorhergehenden Diagramm gezeigt, ist der Verkehrsfluss wie folgt:

1. Der Client sendet eine Anfrage an die AWS Lambda-Funktion (XYZ). Diese Clientanforderung wird an den virtuellen NetScaler-Server (192.168.1.1) gesendet.
2. Der virtuelle Server prüft das Paket und prüft auf schädliche Inhalte.
3. Die NetScaler Appliance löst eine Rewrite-Richtlinie aus, um den Hostnamen und die URL in einer Clientanforderung zu ändern. Zum Beispiel möchten Sie `https://restapi.citrix.com/default/LamdaFunctionXYZ` zu `https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ` ändern.
4. Die NetScaler Appliance leitet diese Anforderung an das AWS-API-Gateway weiter.
5. Das AWS API Gateway sendet die Anforderung weiter an den Lambda-Dienst und ruft die Lambda-Funktion “XYZ” auf.
6. Wenn ein Angreifer gleichzeitig eine API-Anfrage mit schädlichem Inhalt sendet, landet die böswillige Anfrage auf der NetScaler Appliance.
7. Die NetScaler Appliance untersucht die Pakete und verwirft die Pakete basierend auf der konfigurierten Aktion.

Konfigurieren der NetScaler Appliance mit aktivierter WAF

Führen Sie die folgenden Schritte aus, um WAF auf einer NetScaler Appliance zu aktivieren:

1. Fügen Sie einen Content Switching oder einen virtuellen Lastausgleichsserver hinzu. Nehmen wir an, die IP-Adresse des virtuellen Servers ist 192.168.1.1, was zu einem Domainnamen (restapi.citrix.com) aufgelöst wird.

2. Aktivieren Sie die WAF-Richtlinie auf dem virtuellen NetScaler-Server. Weitere Informationen finden Sie unter Konfigurieren der Web App Firewall.
3. Aktivieren Sie Rewrite-Richtlinie, um den Domainnamen zu ändern. Nehmen wir an, Sie möchten die eingehende Anforderung für den Load Balancer unter “restapi.citrix.com” -Domänennamen ändern, um in das Back-End-AWS-API-Gateway unter “citrix.execute-api” neu geschrieben zu werden.<region>.amazonaws” Domänenname.
4. Aktivieren Sie den L3-Modus auf der NetScaler Appliance, damit sie als Proxy fungiert. Verwenden Sie den folgenden Befehl:

```
enable ns mode L3
<!--NeedCopy-->
```

Nehmen wir in Schritt 3 des vorherigen Beispiels an, der Website-Administrator möchte, dass die NetScaler Appliance den Domänennamen “restapi.citrix.com” durch “citrix.execute-api” ersetzt.<region>.amazonaws.com” und die URL mit “Default/Lambda/XYZ”.

Das folgende Verfahren beschreibt, wie Sie den Hostnamen und die URL in einer Clientanforderung mithilfe der Rewrite-Funktion ändern:

1. Melden Sie sich mit SSH bei der NetScaler Appliance an.
2. Aktionen zum Umschreiben hinzufügen.

```
add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER("
    Host")" ""citrix.execute-api.<region>.amazonaws.com""

add rewrite action rewrite_url_act replace HTTP.REQ.URL.
    PATH_AND_QUERY ""/default/lambda/XYZ""
<!--NeedCopy-->
```

3. Fügen Sie Richtlinien zum Umschreiben für die Umschreibaktionen hinzu.

```
add rewrite policy rewrite_host_hdr_pol "HTTP.REQ.HEADER("Host").
    CONTAINS("restapi.citrix.com") "rewrite_host_hdr_act

add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER("Host").
    CONTAINS("restapi.citrix.com") "rewrite_url_act
<!--NeedCopy-->
```

4. Binden Sie die Umschreibungsrichtlinien an einen virtuellen Server.

```
bind lb vserver LB_API_Gateway -policyName rewrite_host_hdr_pol -
    priority 10 -gotoPriorityExpression 20 -type REQUEST

```



```
bind lb vserver LB_API_Gateway -policyName rewrite_url_pol -
    priority 20 -gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Weitere Informationen finden Sie unter Konfigurieren des Umschreibens, um den Hostnamen und die URL in der Clientanforderung auf der NetScaler Appliance zu ändern.

NetScaler Funktionen und Funktionen

Die NetScaler Appliance kann neben der Sicherung der Bereitstellung auch die Anforderung basierend auf den Benutzeranforderungen verbessern. Die NetScaler Appliance bietet die folgenden Hauptfunktionen.

- **Lastausgleich für das API-Gateway:** Wenn Sie über mehr als ein API-Gateway verfügen, können Sie mithilfe der NetScaler Appliance mehrere API-Gateways ausgleichen und das Verhalten der API-Anforderung definieren.
  - Es sind verschiedene Lastausgleichsmethoden verfügbar. Beispielsweise verhindert die Methode Least Connection eine Überlastung des API-Gateway-Limits, die benutzerdefinierte Lademethode behält eine bestimmte Last auf einem bestimmten API-Gateway bei und so weiter. Weitere Informationen finden Sie unter Load-Balancing-Algorithmen.
  - SSL-Offloading ist konfiguriert, ohne den Verkehr zu unterbrechen.
  - Der Modus Quell-IP (USIP) verwenden ist aktiviert, um die Client-IP-Adresse beizubehalten.
  - Benutzerdefinierte SSL-Einstellungen: Sie können Ihren eigenen virtuellen SSL-Server mit Ihren eigenen signierten Zertifikaten und Algorithmen haben.
  - Virtueller Backup-Server: Wenn das API-Gateway nicht erreichbar ist, können Sie die Anforderung für weitere Aktionen an einen virtuellen Sicherungsserver senden.
  - Viele andere Lastausgleichsfunktionen sind verfügbar. Weitere Informationen finden Sie unter Lastausgleich des Datenverkehrs auf einer NetScaler Appliance.
- **Authentifizierung, Autorisierung und Überwachung:** Sie können Ihre eigenen Authentifizierungsmethoden wie LDAP, SAML, RADIUS definieren und die API-Anforderungen autorisieren und überwachen.
- **Responder:** Sie können API-Anforderungen während des Herunterfahrens an ein anderes API-Gateway umleiten.
- **Ratenbegrenzung:** Sie können die Ratenbegrenzungsfunktion konfigurieren, um eine Überlastung eines API-Gateways zu vermeiden.

- **Bessere Verfügbarkeit:** Sie können eine NetScaler Appliance in einem Hochverfügbarkeits-Setup oder einem Cluster-Setup konfigurieren, um Ihren AWS-API-Datenverkehr besser verfügbar zu machen.
- **REST-API:** Unterstützt die REST-API, die zur Automatisierung der Arbeit in Cloud-Produktionsumgebungen verwendet werden kann.
- **Daten überwachen:** Überwacht und protokolliert die Daten als Referenz.

Die NetScaler Appliance bietet viel mehr Funktionen, die in das AWS-API-Gateway integriert werden können. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

Fügen Sie den Back-End-Dienst AWS Autoscaling hinzu

May 11, 2023

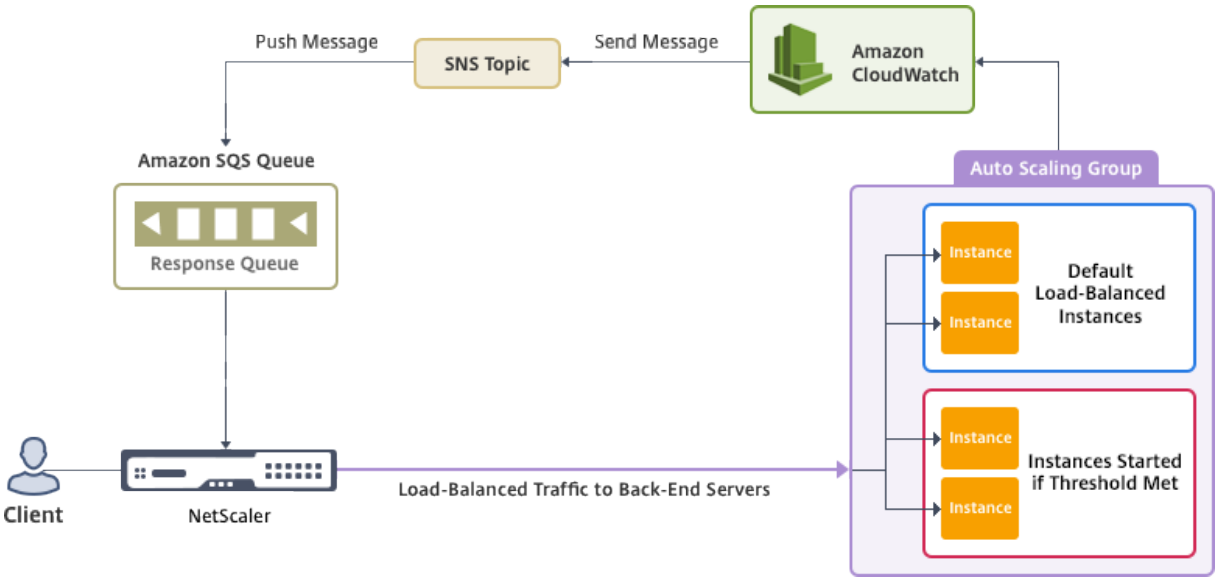
Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen je nach Anwendungsbedarf. Um der steigenden Nachfrage gerecht zu werden, müssen Sie die Netzwerkressourcen nach oben skalieren. Unabhängig davon, ob die Nachfrage nachlässt, müssen Sie eine Reduzierung vornehmen, um unnötige Kosten durch ungenutzte Ressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, indem Sie nur so viele Instanzen bereitstellen, wie zu einem bestimmten Zeitpunkt erforderlich sind, müssen Sie den Datenverkehr, die Speicher- und CPU-Auslastung usw. ständig überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Die NetScaler VPX-Instanz ist in den AWS Auto Scaling-Service integriert und bietet folgende Vorteile:

- **Lastverteilung und Verwaltung**: Server werden automatisch so konfiguriert, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die VPX-Instanz erkennt Autoscale-Gruppen im Back-End-Subnetz automatisch und ermöglicht es einem Benutzer, die Autoscale-Gruppen auszuwählen, um die Last auszugleichen. All dies erfolgt durch die automatische Konfiguration der virtuellen IP-Adressen und der Subnetz-IP-Adressen auf der VPX-Instanz.
- **Hochverfügbarkeit**: Erkennt Autoscale-Gruppen, die sich über mehrere Availability Zones erstrecken, und verteilt die Serverlast.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:
  - Backend-Server auf verschiedenen VPCs mithilfe von VPC-Peering
  - Backend-Server auf denselben Platzierungsgruppen
  - Backend-Server in verschiedenen Verfügbarkeitszonen
- **Sorgfältiger Verbindungsabbruch:** **Mithilfe der Funktion Graceful**Timeout werden Autoscale-Server ordnungsgemäß entfernt und so der Verlust von Client-Verbindungen

vermieden, wenn eine Scale-Down-Aktivität auftritt.

Diagramm: AWS Autoscaling-Service mit einer NetScaler VPX-Instanz



Dieses Diagramm zeigt, wie der AWS Autoscaling-Service mit einer NetScaler VPX-Instanz (Load Balancing Virtual Server) kompatibel ist. Weitere Informationen finden Sie in den folgenden AWS-Themen.

- Gruppen automatisch skalieren
- Cloud-Uhr
- Einfacher Benachrichtigungsdienst (SNS)
- Einfacher Warteschlangendienst (Amazon SQS)

Voraussetzungen

Bevor Sie Autoscaling mit Ihrer NetScaler VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben ausführen.

1. Lesen Sie die folgenden Themen:
   - Voraussetzungen
   - Einschränkungen und Nutzungsrichtlinien
2. Erstellen Sie eine NetScaler VPX-Instanz auf AWS entsprechend Ihren Anforderungen.
   - Weitere Informationen zum Erstellen einer eigenständigen NetScaler VPX Instanz finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS und Scenario: Standalone-Instanz
   - Weitere Informationen zur Bereitstellung von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

> **Hinweis:**
>
> Citrix empfiehlt die CloudFormation-Vorlage für die Erstellung von NetScaler VPX-Instanzen auf AWS.
>
> Citrix empfiehlt, drei Schnittstellen zu erstellen: eine für das Management (NSIP), eine für den Client zugewandten virtuellen LB-Server (VIP) und eine für Subnetz-IP (NSIP).

3. Erstellen Sie eine AWS Autoscale-Gruppe. Wenn Sie keine bestehende Autoscaling-Konfiguration haben, müssen Sie:

   a) Erstellen Sie eine Startkonfiguration

   b) Erstellen Sie eine Autoscaling-Gruppe

   c) Überprüfen Sie die Autoscaling-Gruppe

   Weitere Informationen finden Sie unter http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html.

4. In der AWS Autoscale-Gruppe müssen Sie mindestens eine Scale-Down-Richtlinie angeben. Die NetScaler VPX-Instanz unterstützt nur die Step Scaling-Richtlinie. Die einfache Skalierungsrichtlinie und die Skalierungsrichtlinie Target Tracking werden für die Autoscale-Gruppe nicht unterstützt.

Fügen Sie den AWS Autoscaling-Service zu einer NetScaler VPX-Instance hinzu

Sie können den Autoscaling-Dienst mit einem einzigen Klick zu einer VPX-Instanz hinzufügen, indem Sie die GUI verwenden. Gehen Sie wie folgt vor, um den Autoscaling-Dienst zur VPX-Instanz hinzuzufügen:

1. Melden Sie sich mit Ihren Anmeldeinformationen für bei der VPX-Instanz an `nsroot`.
2. Wenn Sie sich zum ersten Mal bei der NetScaler VPX-Instanz anmelden, wird die standardmäßige Cloud-Profilseite angezeigt. Wählen Sie die AWS Autoscaling-Gruppe aus dem Drop-down-Menü aus und klicken Sie auf **Erstellen**, um ein Cloud-Profil zu erstellen. Klicken Sie auf **Überspringen**, wenn Sie das Cloud-Profil später erstellen möchten.

   Punkte, die beim Erstellen eines Cloud-Profils berücksichtigtwerden müssen: Standardmäßig erstellt und fügt die CloudFormation-Vorlage die folgende IAM-Rolle an.

```
{


    "Version": "2012-10-17",
    "Statement": [

     {
```



```
8
9
10              "Action": [
11
12                  "ec2:DescribeInstances",
13                  "ec2:DescribeNetworkInterfaces",
14                  "ec2:DetachNetworkInterface",
15                  "ec2:AttachNetworkInterface",
16                  "ec2:StartInstances",
17                  "ec2:StopInstances",
18                  "ec2:RebootInstances",
19                  "autoscaling:\*",
20                  "sns:\*",
21                  "sqs:*"
22
23                 “iam: SimulatePrincipalPolicy”
24                 “iam: GetRole”
25
26              ],
27
28              "Resource": "*",
29              "Effect": "Allow"
30
31          }
32
33
34      ]
35
36   }
37
38 <!--NeedCopy-->
```

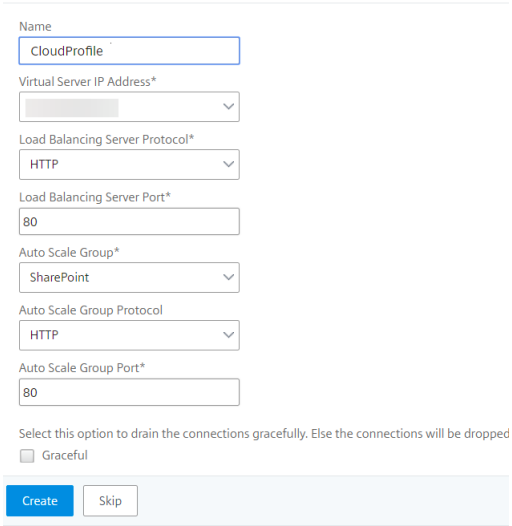
Stellen Sie sicher, dass die IAM-Rolle einer Instanz über die richtigen Berechtigungen verfügt.

- Die IP-Adresse des virtuellen Servers wird automatisch von der für die VPX-Instanz verfügbaren freien IP-Adresse abgeleitet. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP
- Die Autoscale-Gruppe wird aus der Autoscale-Gruppe, die in Ihrem AWS-Konto konfiguriert ist, vorab aufgefüllt. http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html.
- Stellen Sie bei der Auswahl des Autoscaling-Group-Protokolls und -Ports sicher, dass Ihre Server diese Protokolle und Ports abhören und dass Sie den richtigen Monitor in der Servicegruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
- Für den SSL-Protokolltyp Autoscaling ist der virtuelle Lastausgleichsserver oder die Ser-

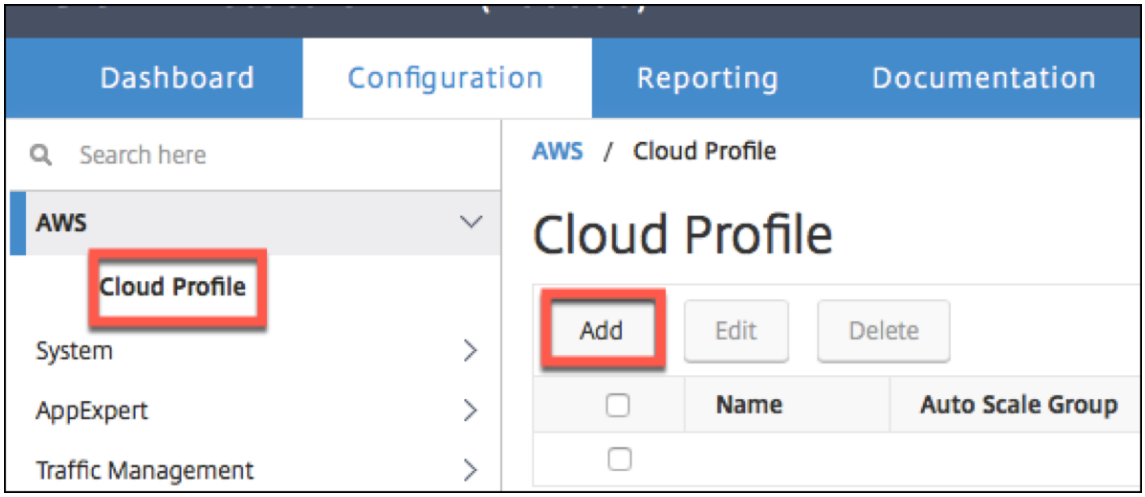
vicegruppe nach der Erstellung des Cloud-Profils aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

- Wählen Sie die Option Graceful Timeout, um Autoscale-Server ordnungsgemäß zu entfernen. Wenn diese Option nicht ausgewählt ist, wird die Gruppe Server in der Autoscale-Gruppe sofort entfernt, nachdem die Last gesunken ist, was zu einer Betriebsunterbrechung für die vorhandenen verbundenen Clients führen kann. Wählen Sie Graceful aus und geben Sie ein Timeout-Mittel für den Fall einer Reduzierung. Die VPX-Instanz entfernt den Server nicht sofort, sondern markiert einen der Server für das geordnete Löschen. Während dieses Zeitraums lässt die Instanz keine neuen Verbindungen zu diesem Server zu. Bestehende Verbindung wird bereitgestellt, bis das Timeout eintritt, und nach einem Timeout entfernt die VPX-Instanz den Server.

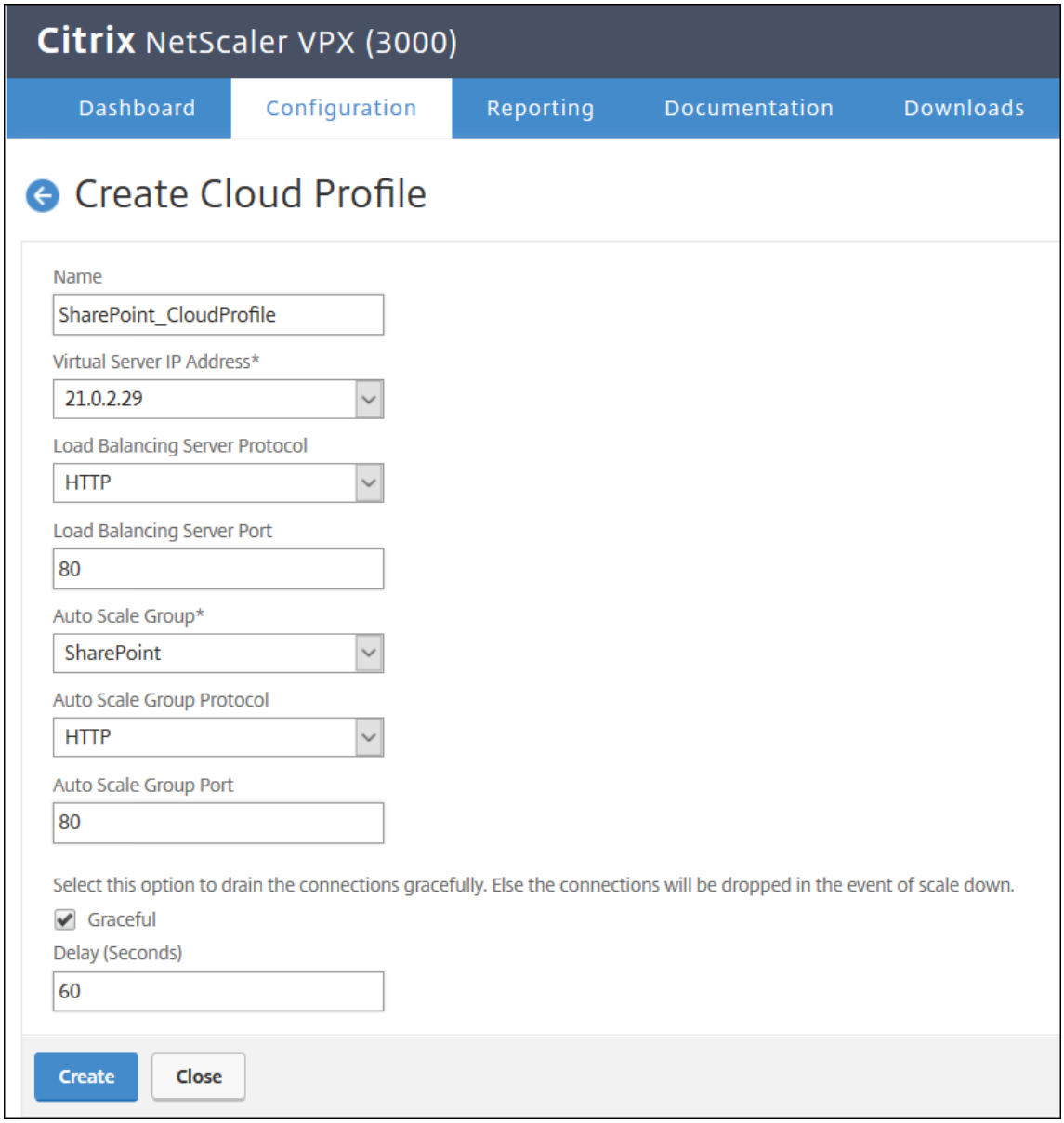
Abbildung: Seite Standard-Cloud-Profil



3. Wenn Sie nach der ersten Anmeldung ein Cloud-Profil erstellen möchten, gehen Sie in der GUI zu **System > AWS > Cloud-Profil** und klicken Sie auf **Hinzufügen**.

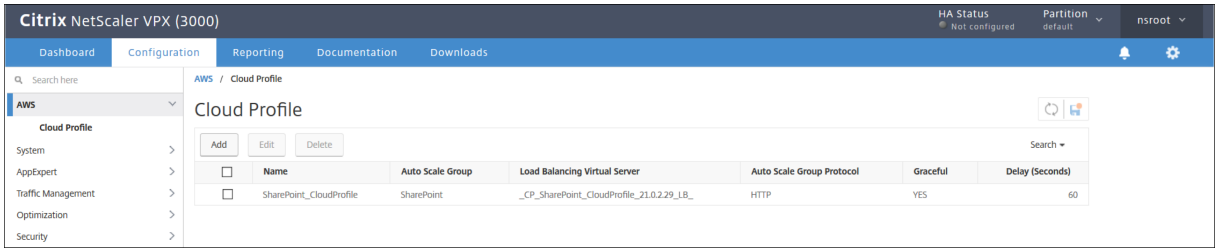


Die Konfigurationsseite „ **Cloud-Profil erstellen** “ wird angezeigt.



Cloud Profile erstellt einen virtuellen NetScaler-Lastenausgleichsserver und eine Dienstgruppe mit Mitgliedern als Server der Autoscaling-Gruppe. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

> **Hinweis:**
>
> Ab NetScaler Version 13.1-42.x können Sie verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung verschiedener Ports) mit derselben Autoscaling Group (ASG) in AWS erstellen. Somit unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.



> **Hinweis**
>
> **Informationen zu AutoScale finden Sie in der AWS-Konsole unter**EC2**>**Dashboard**> Auto Scaling >**Auto Scaling Group**.**

Konfigurieren einer NetScaler VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

May 11, 2023

> **Hinweis**
>
> Unterstützung für SR-IOV-Schnittstellen in einem Hochverfügbarkeitssetup ist ab NetScaler Version 12.0 57.19 verfügbar.

Nachdem Sie eine NetScaler VPX-Instanz in AWS erstellt haben, können Sie die virtuelle Appliance mithilfe der AWS CLI für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren.

In allen NetScaler VPX-Modellen, außer NetScaler VPX AWS Marketplace Editions von 3G und 5G, ist SR-IOV in der Standardkonfiguration einer Netzwerkschnittstelle nicht aktiviert.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Dieser Abschnitt enthält die folgenden Themen:

- Ändern Sie den Schnittstellentyp auf SR-IOV
- Konfiguration von SR-IOV in einem Hochverfügbarkeits-Setup

Ändern Sie den Schnittstellentyp auf SR-IOV

Sie können den Befehl show interface summary ausführen, um die Standardkonfiguration einer Netzwerkschnittstelle zu überprüfen.

Beispiel 1: Die folgende CLI-Bildschirmaufnahme zeigt die Konfiguration einer Netzwerkschnittstelle, bei der SR-IOV standardmäßig in NetScaler VPX AWS Marketplace Editions von 3G und 5G aktiviert ist.


```
> show interface summary
-------------------------------------------------------------------------------
     Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------------
1      1/1      1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2      LO/1     1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```

Beispiel 2: Die folgende CLI-Bildschirmaufnahme zeigt die Standardkonfiguration einer Netzwerkschnittstelle, bei der SR-IOV nicht aktiviert ist.

```
 Done
> sh int s
-------------------------------------------------------------------------------
     Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------------
1      1/1      1500      12:fc:04:c5:d0:12  NetScaler Virtual Interface
2      LO/1     1500      12:fc:04:c5:d0:12  Netscaler Loopback interface
 Done
>
```

Weitere Informationen zum Ändern des Schnittstellentyps in SR-IOV finden Sie unterhttp://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

Um den Schnittstellentyp auf SR-IOV zu ändern

1. Fahren Sie die NetScaler VPX-Instance herunter, die auf AWS ausgeführt wird.
2. Um SR-IOV auf der Netzwerkschnittstelle zu aktivieren, geben Sie den folgenden Befehl in die AWS-CLI ein.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \<instance\\_id\> --sriov-net-support simple
   ```

3. Um zu überprüfen, ob SR-IOV aktiviert wurde, geben Sie den folgenden Befehl in der AWS CLI ein.

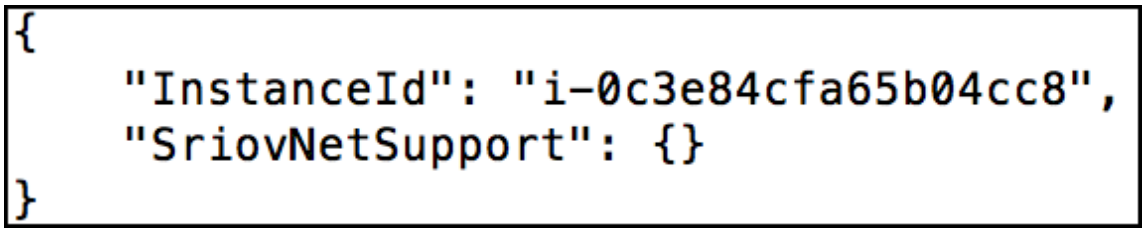
   ```
   $ aws ec2 describe-instance-attribute --instance-id \<instance\\_id\> --attribute sriovNetSupport
   ```

   Beispiel 3: Der Netzwerkschnittstellentyp wurde unter Verwendung der AWS CLI in SR-IOV geändert.

   ```
   aws ec2 modify-instance-attribute --instance-id i-008c1230aaf303bee --sriov-net-support simple
   aws ec2 describe-instance-attribute --instance-id   i-008c1230aaf303bee  --attribute sriovNetSupport
   {
       "InstanceId": "i-008c1230aaf303bee",
       "SriovNetSupport": {
           "Value": "simple"
       }
   }
   ```

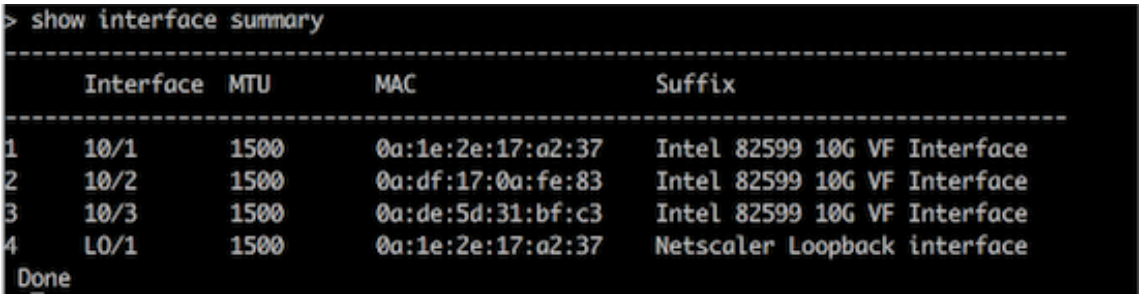
   Wenn SR-IOV nicht aktiviert ist, ist der Wert für SRIOVNetSupport nicht vorhanden.

Beispiel 4: Im folgenden Beispiel ist die SR-IOV-Unterstützung nicht aktiviert.



4. Schalten Sie die VPX-Instanz ein. Um den geänderten Status der Netzwerkschnittstelle anzuzeigen, geben Sie “Interface-Zusammenfassung anzeigen” in die CLI ein.

   Beispiel 5: Die folgende Bildschirmaufnahme zeigt die Netzwerkschnittstellen mit aktiviertem SR-IOV. Die Schnittstellen 10/1, 10/2, 10/3 sind SR-IOV aktiviert.



Mit diesen Schritten wird das Verfahren zum Konfigurieren von VPX-Instanzen für die Verwendung von SR-IOV-Netzwerkschnittstellen abgeschlossen.

Konfiguration von SR-IOV in einem Hochverfügbarkeits-Setup

Hochverfügbarkeit wird mit SR-IOV-Schnittstellen ab NetScaler Version 12.0 Build 57.19 unterstützt.

Wenn das Hochverfügbarkeits-Setup manuell oder mithilfe der Citrix CloudFormation-Vorlage für NetScaler Version 12.0 56.20 und niedriger bereitgestellt wurde, muss die dem Hochverfügbarkeits-Setup zugeordnete IAM-Rolle über die folgenden Rechte verfügen:

- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- autoscaling:*
- Söhne: *
- sqs:*
- iam:SimulatePrincipalPolicy

- iam:GetRole

Standardmäßig fügt die Citrix CloudFormation-Vorlage für NetScaler Version 12.0 57.19 automatisch die erforderlichen Berechtigungen zur IAM-Rolle hinzu.

> **Hinweis**
>
> Ein Hochverfügbarkeits-Setup mit SR-IOV-Schnittstellen benötigt etwa 100 Sekunden Ausfallzeiten.

Verwandte Ressourcen:

Weitere Informationen zu IAM-Rollen finden Sie in der AWS-Dokumentation.

Konfigurieren einer NetScaler VPX-Instanz für die Verwendung von Enhanced Networking mit AWS ENA

May 11, 2023

Nachdem Sie eine NetScaler VPX-Instanz in AWS erstellt haben, können Sie die virtuelle Appliance mithilfe von [AWS CLI für die Verwendung von Enhanced Networking with AWS Elastic Network Adapter (ENA)](https://aws.amazon.com/about-aws/whats-new/2016/06/introducing-elastic-network-adapter-ena-the-next-generation-network-interface-for-ec2-instances/)konfigurieren.

In Verbindung mit AWS ENA bietet das erweiterte Netzwerk eine höhere Bandbreite, eine höhere Paketper-Sekunden-Leistung (PPS) und konstant niedrigere Instanz-Latenzen.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Die folgenden HA-Konfigurationen werden für ENA-fähige Instances unterstützt:

- Private IP-Adressen können innerhalb derselben Verfügbarkeitszone verschoben werden.
- Elastische IP-Adressen können über Availability Zones verschoben werden.

Aktualisieren einer NetScaler VPX-Instanz auf AWS

May 11, 2023

Sie können den EC2-Instance-Typ, den Durchsatz, die Software-Edition und die Systemsoftware eines NetScaler VPX, das auf AWS ausgeführt wird, aktualisieren. Für bestimmte Arten von Upgrades emp-

fiehlt Citrix, die Hochverfügbarkeitskonfigurationsmethode zu verwenden, um Ausfallzeiten zu minimieren.

> Hinweis:
>
> - Die NetScaler-Softwareversion 10.1.e-124.1308.e oder höher für ein NetScaler VPX-AMI (einschließlich Utility-Lizenz und Kundenlizenz) unterstützt die Instance-Familien M1 und M2 nicht.
> - Aufgrund von Änderungen bei der VPX-Instance-Unterstützung wird ein Downgrade von 10.1.e-124 oder einer späteren Version auf 10.1.123.x oder eine frühere Version nicht unterstützt.
> - Für die meisten Upgrades ist kein neues AMI erforderlich, und das Upgrade kann auf der aktuellen NetScaler-AMI-Instance durchgeführt werden. Wenn Sie ein Upgrade auf eine neue NetScaler-AMI-Instance durchführen möchten, verwenden Sie die Hochverfügbarkeitskonfigurationsmethode.

Ändern Sie den EC2-Instance-Typ einer NetScaler VPX-Instance auf AWS

Wenn auf Ihren NetScaler VPX-Instances Version 10.1.e-124.1308.e oder höher ausgeführt wird, können Sie den EC2-Instance-Typ von der AWS-Konsole aus wie folgt ändern:

1. Stoppen Sie die VPX-Instanz.
2. Ändern Sie den EC2-Instance-Typ in der AWS-Konsole.
3. Starten Sie die Instanz.

Sie können das obige Verfahren auch verwenden, um den EC2-Instanztyp für eine Version vor 10.1.e-124.1308.e zu ändern, es sei denn, Sie möchten den Instanztyp in M3 ändern. In diesem Fall müssen Sie zuerst das standardmäßige NetScaler-Upgradeverfahren befolgen, um die NetScaler-Software auf 10.1.e-124 oder eine spätere Version zu aktualisieren, und dann die obigen Schritte ausführen.

Aktualisieren des Durchsatzes oder der Software-Edition einer NetScaler VPX-Instanz auf AWS

Um die Software-Edition (z. B. um von Standard auf Premium Edition zu aktualisieren) oder den Durchsatz (z. B. um von 200 Mbit/s auf 1000 Mbit/s zu aktualisieren), hängt die Methode von der Lizenz der Instanz ab.

Verwendung einer Kundenlizenz (Bring-Your-Own-Lizenz)

Wenn Sie eine Kundenlizenz verwenden, können Sie die neue Lizenz von der Citrix-Website kaufen und herunterladen und dann die Lizenz auf der VPX-Instanz installieren. Weitere Informationen zum Herunterladen und Installieren einer Lizenz von der Citrix-Website finden Sie im VPX-Lizenzleitfaden.

Verwendung einer Versorgungslizenz (Versorgungslizenz mit Stundengebühr)

AWS unterstützt keine direkten Upgrades für kostenpflichtige Instances. Um die Software-Edition oder den Durchsatz einer gebührenbasierten NetScaler VPX-Instanz zu aktualisieren, starten Sie ein neues AMI mit der gewünschten Lizenz und Kapazität und migrieren Sie die ältere Instanzkonfiguration auf die neue Instanz. Dies kann erreicht werden, indem eine NetScaler-Hochverfügbarkeitskonfiguration verwendet wird, wie unter Upgrade auf eine neue NetScaler AMI-Instanz unter Verwendung eines NetScaler-Unterabschnitts für hohe Verfügbarkeit auf dieser Seite beschrieben.

Aktualisieren der Systemsoftware einer NetScaler VPX-Instanz auf AWS

Wenn Sie eine VPX-Instanz mit 10.1.e-124.1308.e oder einer späteren Version aktualisieren müssen, befolgen Sie das standardmäßige NetScaler-Upgradeverfahren beim Upgrade und Downgrade einer NetScaler Appliance.

Wenn Sie eine VPX-Instanz mit einer älteren Version als 10.1.e-124.1308.e auf 10.1.e-124.1308.e oder höher aktualisieren müssen, aktualisieren Sie zuerst die Systemsoftware, und ändern Sie dann den Instanztyp wie folgt auf M3:

1. Stoppen Sie die VPX-Instanz.
2. Ändern Sie den EC2-Instance-Typ in der AWS-Konsole.
3. Starten Sie die Instanz.

Führen Sie ein Upgrade auf eine neue NetScaler AMI-Instance mithilfe einer NetScaler-Hochverfügbarkeitskonfiguration durch

Gehen Sie wie folgt vor, um die Hochverfügbarkeitsmethode für ein Upgrade auf eine neue NetScaler AMI-Instance zu verwenden:

- Erstellen Sie eine neue Instance mit dem gewünschten EC2-Instance-Typ, der gewünschten Software-Edition, dem gewünschten Durchsatz oder der gewünschten Softwareversion aus dem AWS-Marketplace.
- Konfigurieren Sie die Hochverfügbarkeit zwischen der alten Instance (die aktualisiert werden soll) und der neuen Instance. Nachdem die Hochverfügbarkeit zwischen der alten und der neuen Instanz konfiguriert wurde, wird die Konfiguration der alten Instanz mit der neuen Instanz synchronisiert.
- Erzwingen Sie einen HA-Failover von der alten Instance zur neuen Instance. Infolgedessen wird die neue Instance zur primären Instanz und beginnt, Traffic zu empfangen.
- Stoppen Sie die alte Instance und konfigurieren Sie sie neu oder entfernen Sie sie aus AWS.

Voraussetzungen und zu beachtende Punkte

- Stellen Sie sicher, dass Sie verstehen, wie hohe Verfügbarkeit zwischen zwei NetScaler VPX -Instanzen in AWS funktioniert. Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei NetScaler VPX-Instanzen in AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.
- Sie müssen die neue Instanz in derselben Availability Zone wie die alte Instanz erstellen, wobei genau dieselbe Sicherheitsgruppe und dasselbe Subnetz vorhanden sind.
- Für die Einrichtung einer hohen Verfügbarkeit sind für beide Instanzen Zugriff und geheime Schlüssel erforderlich, die mit dem AWS Identity and Access Management (IAM) -Konto des Benutzers verknüpft sind. Wenn beim Erstellen von VPX-Instanzen die richtigen Schlüsselinformationen nicht verwendet werden, schlägt das HA-Setup fehl. Weitere Informationen zum Erstellen eines IAM-Kontos für eine VPX-Instanz finden Sie unter Voraussetzungen.
  - Sie müssen die EC2-Konsole verwenden, um die neue Instanz zu erstellen. Sie können den AWS-1-Click-Start nicht verwenden, da er die Zugriffs- und geheimen Schlüssel nicht als Eingabe akzeptiert.
  - Die neue Instanz muss nur eine ENI-Schnittstelle haben.

Gehen Sie folgendermaßen vor, um eine NetScaler VPX-Instanz mithilfe einer Hochverfügbarkeitskonfiguration zu aktualisieren:

1. Konfigurieren Sie die hohe Verfügbarkeit zwischen der alten und der neuen Instanz. Um die Hochverfügbarkeit zwischen zwei NetScaler VPX-Instanzen zu konfigurieren, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   Beispiel:

   Geben Sie in der Befehlszeile der alten Instanz Folgendes ein:

   ```
   1 add ha node 30 192.0.2.30
   2 Done
   3 <!--NeedCopy-->
   ```

   Geben Sie in der Befehlszeile der neuen Instanz Folgendes ein:

   ```
   1 add ha node 10 192.0.2.10
   2 Done
   3 <!--NeedCopy-->
   ```

   Beachten Sie Folgendes:

   - Im HA-Setup ist die alte Instanz der primäre Knoten und die neue Instanz ist der sekundäre Knoten.

- Die NSIP-IP-Adresse wird nicht von der alten Instanz auf die neue Instanz kopiert. Daher hat Ihre neue Instanz nach dem Upgrade eine andere Verwaltungs-IP-Adresse als die vorherige.
- Das `nsroot` Kontokennwort der neuen Instanz wird nach der HA-Synchronisierung auf das der alten Instanz festgelegt.

Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei NetScaler VPX-Instanzen in AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

2. Erzwingen Sie ein HA-Failover. Um ein Failover in einer Hochverfügbarkeitskonfiguration zu erzwingen, geben Sie an der Befehlszeile einer der Instanzen Folgendes ein:

```
1 force HA failover
2 <!--NeedCopy-->
```

Wenn ein Failover erzwungen wird, werden die ENIs der alten Instance auf die neue Instance migriert und der Datenverkehr fließt durch die neue Instance (den neuen primären Knoten). Die alte Instanz (der neue sekundäre Knoten) wird neu gestartet.

Wenn die folgende Warnmeldung angezeigt wird, geben Sie N ein, um den Vorgang abzubrechen:

```
1 [WARNING]:Force Failover may cause configuration loss, peer health
      not optimum. Reason(s):
2 HA version mismatch
3 HA heartbeats not seen on some interfaces
4 Please confirm whether you want force-failover (Y/N)?
5 <!--NeedCopy-->
```

Die Warnmeldung wird angezeigt, weil die Systemsoftware der beiden VPX-Instanzen nicht HA-kompatibel ist. Daher kann die Konfiguration der alten Instanz bei einem erzwungenen Failover nicht automatisch mit der neuen Instanz synchronisiert werden.

Im Folgenden finden Sie die Problemumgehung für dieses Problem:

a) Geben Sie an der NetScaler-Shell-Eingabeaufforderung der alten Instanz den folgenden Befehl ein, um eine Backup der Konfigurationsdatei (ns.conf) zu erstellen:

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

b) Entfernen Sie die folgende Zeile aus der Sicherungskonfigurationsdatei (ns.conf.bkp):

- `set ns config -IPAddress <IP> -netmask <MASK>`

Zum Beispiel `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c) Kopieren Sie die Backup-Konfigurationsdatei der alten Instanz (ns.conf.bkp) in das Verzeichnis /nsconfig der neuen Instanz.

d) Geben Sie an der NetScaler -Shell Eingabeaufforderung der neuen Instanz den folgenden Befehl ein, um die Konfigurationsdatei der alten Instanz (ns.conf.bkp) auf die neue Instanz zu laden:

- `batch -f /nsconfig/ns.conf.bkp`

e) Speichern Sie die Konfiguration auf der neuen Instanz.

- `save conifg`

f) Geben Sie an der Eingabeaufforderung eines der Knoten den folgenden Befehl ein, um ein Failover zu erzwingen, und geben Sie dann Y für die Warnmeldung ein, um den Failover-Vorgang zu bestätigen:

- `force ha failover`

Beispiel:

```
1         > force ha failover
2
3 WARNING]:Force Failover may cause configuration loss, peer health
     not optimum.
4         Reason(s):
5         HA version mismatch
6         HA heartbeats not seen on some interfaces
7         Please confirm whether you want force-failover (Y/N)? Y
8 <!--NeedCopy-->
```

3. Entfernen Sie die HA-Konfiguration, sodass sich die beiden Instanzen nicht mehr in einer HA-Konfiguration befinden. Entfernen Sie zuerst die HA-Konfiguration vom sekundären Knoten und dann die HA-Konfiguration vom primären Knoten.

   Um eine HA-Konfiguration zwischen zwei NetScaler VPX-Instanzen zu entfernen, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

```
1     > remove ha node \<nodeID\>
2     >  save config
3 <!--NeedCopy-->
```

   Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei VPX-Instanzen in AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

   Beispiel:

Geben Sie in der Befehlszeile der alten Instanz (neuer sekundärer Knoten) Folgendes ein:


```
          > remove ha node 30
            Done
          > save config
            Done
<!--NeedCopy-->
```

Geben Sie in der Befehlszeile der neuen Instanz (neuer primärer Knoten) Folgendes ein:

```
          > remove ha node 10
            Done
          > save config
            Done
<!--NeedCopy-->
```

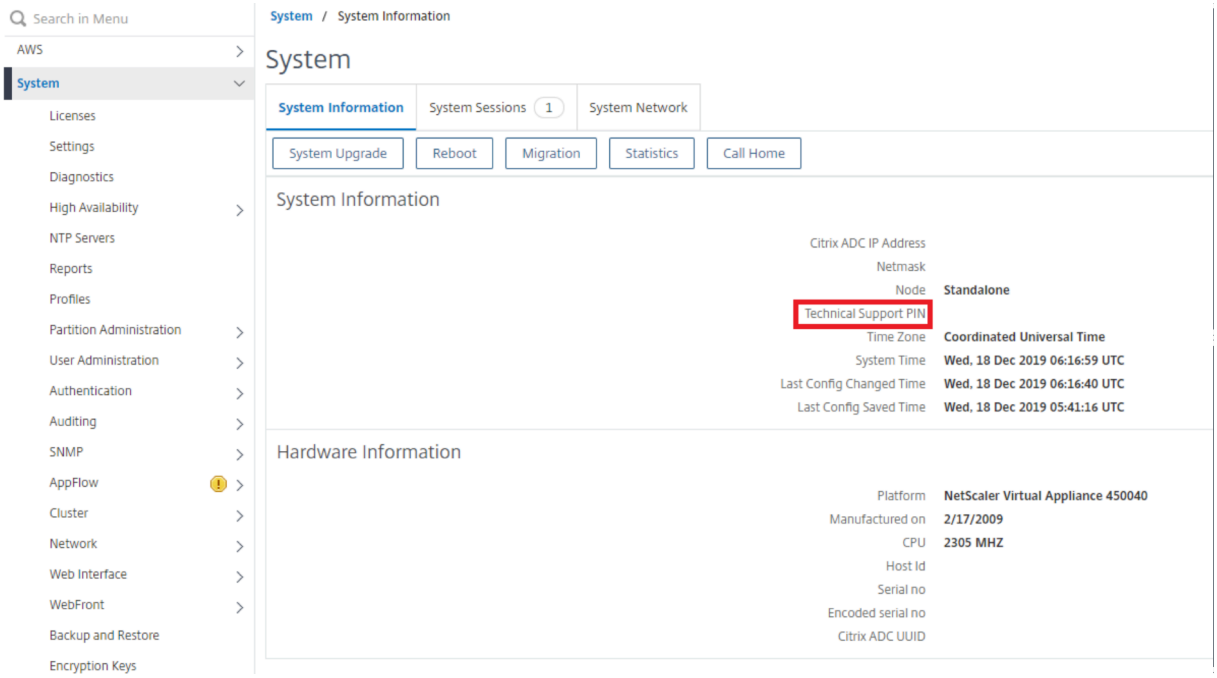
Problembehandlung bei einer VPX-Instanz in AWS

May 11, 2023

Amazon bietet keinen Konsolenzugriff auf eine NetScaler VPX-Instance. Zur Fehlerbehebung müssen Sie die AWS-GUI verwenden, um das Aktivitätsprotokoll einzusehen. Sie können nur debuggen, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz anzuzeigen, klicken Sie mit der rechten Maustaste auf die Instanz und wählen Sie Systemprotokoll

NetScaler bietet Support für von AWS Marketplace lizenzierte NetScaler VPX-Instances (Utility-Lizenz mit Stundengebühr) auf AWS. Um eine Support-Anfrage einzureichen, suchen Sie nach Ihrer AWS-Kontonummer und Ihrem Support-PIN-Code und wenden Sie sich an den NetScaler-Support. Sie werden auch nach Ihrem Namen und Ihrer E-Mail-Adresse gefragt. Um die Support-PIN zu finden, melden Sie sich an der VPX-GUI an und navigieren Sie zur Systemseite.

Hier ist ein Beispiel für eine Systemseite, die die Support-PIN zeigt.



AWS FAQs

May 11, 2023

- **Unterstützt eine NetScaler VPX-Instance die verschlüsselten Volumes in AWS?**

  Die Verschlüsselung und Entschlüsselung erfolgt auf Hypervisor-Ebene und funktioniert daher problemlos mit jeder Instanz. Weitere Informationen zu den verschlüsselten Volumes finden Sie im folgenden AWS-Dokument:

  https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- **Was ist der beste Weg, um eine NetScaler VPX-Instanz auf AWS bereitzustellen?**

  Sie können eine NetScaler VPX-Instance auf AWS auf eine der folgenden Arten bereitstellen:

  - AWS CloudFormation-Vorlage (CFT) auf dem AWS-Marktplatz
  - NetScaler ADM
  - AWS Quick Starts
  - Citrix AWS CFTs in GitHub
  - Citrix Terraform-Skripts in GitHub
  - Citrix Ansible Playbooks in GitHub
  - AWS EC2-Start-Workflow

  Sie können eine der aufgelisteten Optionen basierend auf dem von Ihnen verwendeten Automatisierungswerkzeug auswählen.

Weitere Informationen zu den Optionen finden Sie unter NetScaler VPX on AWS.

- **Wie aktualisiere ich die NetScaler VPX Instanz in AWS?**

  Um die NetScaler VPX-Instanz in AWS zu aktualisieren, können Sie die Systemsoftware aktualisieren oder auf ein neues NetScaler VPX Amazon Machine Image (AMI) aktualisieren, indem Sie das Verfahren unter Upgrade einer NetScaler VPX-Instanz auf AWSbefolgen.

  Die empfohlene Möglichkeit, eine NetScaler VPX-Instanz zu aktualisieren, besteht darin, den ADM-Dienst zu verwenden, indem Sie das Verfahren unter Verwenden von Jobs zum Upgrade von NetScaler-Instanzenbefolgen.

- **Wie hoch ist die HA-Failover-Zeit für NetScaler VPX in AWS?**

  - Das HA-Failover von NetScaler VPX innerhalb der AWS Availability Zone dauert etwa 3 Sekunden.
  - Das HA-Failover von NetScaler VPX in AWS-Verfügbarkeitszonen dauert etwa 5 Sekunden.

- **Welchen Support erhalten Kunden des NetScaler VPX Marketplace-Abonnements, die die PIN für den technischen Support bereitstellen?**

  Standardmäßig wird der Dienst “Für Software auswählen” Kunden zur Verfügung gestellt, die die PIN für den technischen Support bereitstellen.

- **Müssen wir bei Hochverfügbarkeit in verschiedenen Zonen mithilfe der Elastic IP-Bereitstellung mehrere IPSets für jede Anwendung erstellen?**

  Ja. Wenn es mehrere Anwendungen mit mehreren VIPs gibt, die mehreren EIPs zugeordnet sind, sind mehrere IPSets erforderlich. Daher werden während des HA-Failovers alle primären VIP-Zuordnungen von EIPs in sekundäre (neue primäre) VIPs geändert.

- **Warum ist der INC-Modus bei hoher Verfügbarkeit für verschiedene Zonenbereitstellungen aktiviert?**

  HA-Paare in allen Availability Zones befinden sich in verschiedenen Netzwerken. Für die HA-Synchronisation darf die Netzwerkkonfiguration nicht synchronisiert werden. Dies wird erreicht, indem der INC-Modus für ein HA-Paar aktiviert wird.

- **Kann der HA-Knoten in einer Availability Zone mit Back-End-Servern in einer anderen Availability Zone kommunizieren, vorausgesetzt, diese Verfügbarkeitszonen befinden sich in derselben VPC?**

  Ja, Subnetze in verschiedenen Availability Zones derselben VPC sind erreichbar, indem eine zusätzliche Route hinzugefügt wird, die über SNIP auf das Backend-Server-Subnetz verweist. Wenn das SNIP-Subnetz von ADC in AZ1 beispielsweise 192.168.3.0/24 ist und das Backend-Server-Subnetz in AZ2 192.168.6.0/24 ist, muss eine Route in der NetScaler Appliance hinzugefügt werden, die in AZ1 als 192.168.6.0 255.255.255.0 192.168.3.1 vorhanden ist.

- **Kann Hochverfügbarkeit über verschiedene Zonen mit Elastic IP und High Availability in verschiedenen Zonen über private IP-Bereitstellungen hinweg zusammenarbeiten?**

  Ja, beide Konfigurationen können auf dasselbe HA-Paar angewendet werden.

- **Wie weiß ein sekundärer Knoten im HA-Paar bei Hochverfügbarkeit in verschiedenen Zonen mit privaten IP-Bereitstellung, wenn mehrere Subnetze mit mehreren Routentabellen in einer VPC vorhanden sind, von der Routing-Tabelle Bescheid, die während des HA-Failovers überprüft werden soll?**

  Der sekundäre Knoten kennt die primären NICs und sucht in allen Routing-Tabellen in einer VPC.

- **Wie groß ist die Partition `/var`, wenn das Standardimage für VPX in AWS verwendet wird? Wie erhöht man den Speicherplatz?**

  Die Größe des Rootdatenträgers ist auf 20 GB begrenzt, um das Datenträgerimage klein zu halten.

  Wenn Sie den Verzeichnisspeicher für `/var/core/` oder `/var/crash/` vergrößern möchten, hängen Sie einen zusätzlichen Datenträger an. Um die Größe von `/var` zu erhöhen, müssen Sie derzeit einen zusätzlichen Datenträger anhängen und einen symbolischen Link zu `/var` erstellen, nachdem Sie den kritischen Inhalt auf den neuen Datenträger kopiert haben.

- **Wie viele Paket-Engines werden aktiviert und vCPUs zugewiesen?**

  Die Paket-Engines (PEs) sind durch die Anzahl der lizenzierten vCPUs begrenzt. Die NetScaler Daemons sind nicht an eine bestimmte vCPU angeheftet und werden möglicherweise auf einem der vCPUs ohne PE ausgeführt. Laut AWS ist der C5.9XLarge eine 36VCPU-Instanz mit 72 GB Speicher. Bei der gepoolten Lizenzierung wird die NetScaler VPX-Instanz mit der maximalen Anzahl von PEs bereitgestellt. In diesem Fall laufen 19 PEs auf Kernen 1 bis 19. ADC-Managementprozesse laufen jedoch von CPUs 20 bis 31 aus.

- **Wie entscheide ich die richtige AWS-Instanz für ADC?**

  1. Verstehen Sie Ihren Anwendungsfall und Ihre Anforderungen wie Durchsatz, PPS, SSL-Anforderungen und durchschnittliche Paketgröße.
  2. Wählen Sie das richtige ADC-Angebot und die richtige Lizenzierung für ADC, die Ihren Anforderungen entspricht, wie VPX-Bandbreitenangebote oder vCPU-basierte Lizenzierung.
  3. Entscheiden Sie sich basierend auf dem gewählten Angebot für die AWS-Instanz.

  Beispiel:

  Eine 5-Gbit/s-Lizenz ermöglicht 5 Datenpaket-Engines. Daher ist die vCPU-Anforderung 6 (5+1 für die Verwaltung). 6 vCPU-Instanz ist jedoch nicht verfügbar. Eine 8 vCPU ist also gut genug, um diesen Durchsatz zu erreichen, vorausgesetzt, Sie wählen ein Netzwerk, das 5 Gbit/s Bandbreite unterstützt. Zum Beispiel müssen Sie m5.2xlarge für eine 5-Gbit/s-Bandbreitenlizenz wählen, um die maximale PE-Zuweisung für eine 5-Gbit/s-Lizenz zu ermöglichen. Wenn Sie

jedoch eine vCPU-Lizenz verwenden, die nicht durch den Durchsatz begrenzt ist, erhalten Sie möglicherweise einen Durchsatz von 5 Gbit/s mithilfe der m5.xlarge-Instanz selbst.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750

- **Ist die Bereitstellung von drei NICs-drei Subnetzen für ADC in AWS obligatorisch**?

  `Three NICs-three subnets` ist die empfohlene Bereitstellung, bei der jede für Management-, Client- und Server-Netzwerk verwendet wird. Diese Bereitstellung bietet eine bessere Verkehrsisolation und VPX-Leistung. Zwei NICS-zwei Subnetze und ein NIC-One-Subnetz sind die anderen verfügbaren Optionen. Citrix empfiehlt nicht, dass mehrere Netzwerkkarten ein Subnetz in AWS teilen, z. B. zwei NICs - eine Subnetzbereitstellung. Weil dies zu Netzwerkproblemen wie asymmetrischem Routing führen kann. Weitere Informationen finden Sie unter Best Practices zum Konfigurieren von Netzwerkschnittstellen in AWS.

Bereitstellen einer NetScaler VPX-Instanz auf Microsoft Azure

May 11, 2023

Wenn Sie eine NetScaler VPX-Instanz in Microsoft Azure Resource Manager (ARM) bereitstellen, können Sie beide der folgenden Feature-Sets verwenden, um Ihre Geschäftsanforderungen zu erfüllen:

- Azure Cloud Computing-Funktionen
- Funktionen für NetScaler Load Balancing und Traffic Management

Sie können NetScaler VPX-Instanzen auf ARM entweder als eigenständige Instanzen oder als Hochverfügbarkeitspaare im aktiven Standby-Modus bereitstellen.

Sie können eine NetScaler VPX-Instanz auf Microsoft Azure auf zwei Arten bereitstellen:

- Über Azure Marketplace. NetScaler VPX ist eine virtuelle Appliance, die als Image in Microsoft Azure Marketplace zur Verfügung steht.
- Verwenden der auf GitHub verfügbaren JSON-Vorlage NetScaler Azure Resource Manager (ARM). Weitere Informationen finden Sie im GitHub-Repository für NetScaler-Lösungsvorlagen.

Der Microsoft Azure-Stack ist eine integrierte Plattform für Hardware und Software, die die Public Cloud-Dienste von Microsoft Azure in einem lokalen Rechenzentrum bereitstellt, damit Unternehmen

Hybrid-Clouds erstellen können. Sie können jetzt die NetScaler VPX-Instanzen auf dem Microsoft Azure-Stack bereitstellen.

Voraussetzung

Sie benötigen einige Vorkenntnisse, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen können.

- Vertrautheit mit Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Kenntnisse einer NetScaler-Appliance. Ausführliche Informationen zur NetScaler-Appliance finden Sie unter NetScaler
- Kenntnisse über NetScaler Netzwerke. Weitere Informationen finden Sie im Thema Netzwerk .

Funktionsweise einer NetScaler VPX-Instanz in Azure

In einer on-premises Bereitstellung benötigt eine NetScaler VPX-Instanz mindestens drei IP-Adressen:

- Verwaltungs-IP-Adresse, NSIP-Adresse genannt
- Subnetz-IP (SNIP) -Adresse für die Kommunikation mit der Serverfarm
- Virtual Server IP (VIP) Adresse für die Annahme von Clientanforderungen

Weitere Informationen finden Sie unter Netzwerkarchitektur für NetScaler VPX-Instanzen auf Microsoft Azure.

> **Hinweis**
>
> NetScaler VPX-Instanz unterstützt sowohl Intel- als auch AMD-Prozessoren. Virtuelle VPX-Appliances können auf jedem Instanztyp bereitgestellt werden, der über zwei oder mehr virtualisierte Kerne und mehr als 2 GB Arbeitsspeicher verfügt. Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu NetScaler VPX.

In einer Azure-Bereitstellung können Sie eine NetScaler VPX-Instanz in Azure auf drei Arten bereitstellen:

- Multi-NIC-Multi-IP-Architektur
- Multi-IP-Architektur mit einer NIC
- Einzelne NIC-Einzel-IP

Je nach Bedarf können Sie jeden dieser unterstützten Architekturtypen verwenden.

Multi-NIC-Multi-IP-Architektur

Bei diesem Bereitstellungstyp können Sie mehrere Netzwerkschnittstellen (NICs) an eine VPX-Instanz anschließen. Jede NIC kann eine oder mehrere IP-Konfigurationen haben - statische oder dynamische

öffentliche und private IP-Adressen, die ihr zugewiesen sind.

Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs konfigurieren
- Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs über PowerShell-Befehle konfigurieren

> Hinweis
>
> Um MAC-Verschiebungen und Schnittstellenstummschaltung in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, ein VLAN pro Datenschnittstelle (ohne Tag) der NetScaler VPX-Instanz zu erstellen und die primäre IP der NIC in Azure zu binden. Weitere Informationen finden Sie im Artikel CTX224626 .

Multi-IP-Architektur mit einer NIC

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstellen (NIC) mit mehreren IP-Konfigurationen verknüpft - statische oder dynamische öffentliche und private IP-Adressen, die ihr zugewiesen sind. Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz konfigurieren
- Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz über PowerShell-Befehle konfigurieren

Einzelne NIC-Einzel-IP

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstellen (NIC) mit einer einzigen IP-Adresse verknüpft, die zur Ausführung der Funktionen von NSIP, SNIP und VIP verwendet wird.

Weitere Informationen finden Sie im folgenden Anwendungsfall:

- Eigenständige NetScaler VPX-Instanz konfigurieren

> **Hinweis**
>
> Der einzelne IP-Modus ist nur in Azure-Bereitstellungen verfügbar. Dieser Modus ist für eine NetScaler VPX-Instanz in Ihren Räumlichkeiten, in AWS oder in einer anderen Art von Bereitstellung nicht verfügbar.

NetScaler VPX-Lizenzierung

Eine NetScaler VPX-Instanz auf Azure benötigt eine Lizenz. Die folgenden Lizenzierungsoptionen sind für NetScaler VPX-Instanzen verfügbar, die auf Azure ausgeführt werden.

- **Abonnementbasierte Lizenzierung**: NetScaler VPX Appliances sind als kostenpflichtige Instanzen auf Azure Marketplace verfügbar. Abonnementbasierte Lizenzierung ist eine Pay-as-you-go-Option. Benutzer werden stündlich berechnet.

  > **Hinweis**
  >
  > Bei Abonnementlizenzinstanzen gilt Ihre Abonnementabrechnung für den gesamten Lizenzzeitraum für ein bestimmtes Lizenzmodell. Aufgrund von Cloud-Einschränkungen unterstützt Azure das Ändern oder Entfernen des für Ihr Abonnement geltenden Lizenzmodells nicht. Um eine Abonnementlizenz zu ändern oder zu entfernen, löschen Sie die vorhandene ADC-VM und erstellen Sie eine neue ADC-VM mit der gewünschten Lizenz neu.

  NetScaler bietet technischen Support für Abonnementlizenzinstanzen. Informationen zum Einreichen eines Supportfalls finden Sie unter Unterstützung für NetScaler auf Azure — Abonnementlizenz mit Stundenpreis.

- **Bringen Sie Ihre eigene Lizenz (BYOL) mit:** Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, finden Sie weitere Informationen im VPX-Lizenzierungsleitfaden unter http://support.citrix.com/article/CTX122426. Sie müssen:

  - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
  - Laden Sie die Lizenz auf die Instanz hoch.

  > **Hinweis**
  >
  > In einer Azure-Stack-Umgebung ist **BYOL** die einzig verfügbare Lizenzierungsoption.

- **NetScaler VPX Check-In/Auschecken Lizenzierung**: Weitere Informationen finden Sie unter NetScaler VPX Check-In/Auschecken Lizenzierung.

  Ab NetScaler Version 12.0 56.20 benötigt NetScaler VPX Express für on-premises und Cloud-Bereitstellungen keine Lizenzdatei. Weitere Informationen zu NetScaler VPX Express finden Sie im Abschnitt “NetScaler VPX Express-Lizenz” in der Übersicht über die NetScaler Lizenzierung.

Die folgenden VPX-Modelle und Lizenztypen sind auf Azure Marketplace verfügbar.

VPX-Modell	Lizenztyp	Die empfohlene Instanz		
		VPX 1 NIC/2 NIC	**VPX 3 NIC**	**VPX bis zu 8 NIC**
VPX10	Standard, Fortgeschritten, Premium	Standard_D2s_v4	Standard_DS3_v2	Standard_DS4_v2

VPX-Modell	Lizenztyp	Die empfohlene Instanz		
VPX200	Standard, Fortgeschritten, Premium	Standard_D2s_v4	Standard_DS3_v2	Standard_DS4_v2
VPX1000	Standard, Fortgeschritten, Premium	Standard_D4s_v4	Standard_DS3_v2	Standard_DS4_v2
VPX3000	Standard, Fortgeschritten, Premium	Standard_D4s_v4	Standard_D8s_v4	Standard_DS4_v2
VPX5000	Standard, Fortgeschritten, Premium	Standard_D8s_v4	Standard_D8s_v4	Standard_DS4_v2
VPX8000	Standard, Fortgeschritten, Premium	Standard_D8s_v4	Standard_D8s_v4	Standard_DS4_v2
VPX10000	Standard, Fortgeschritten, Premium	Standard_D16s_v4	Standard_D16s_v4	Standard_D16s_v4

Zu beachtende Punkte:

- Sie müssen das beschleunigte Azure-Netzwerk auf NetScaler VPX-Instanzen aktivieren, um die optimale Leistung für die folgenden VPX-Modelle zu erzielen:
  - VPX1000
  - VPX3000
  - VPX5000
  - VPX8000
  - VPX10000

  Weitere Informationen zum Konfigurieren des beschleunigten Netzwerks finden Sie unter Konfigurieren einer NetScaler VPX-Instanz für die Verwendung des beschleunigten Azure-Netzwerks.
- Die VPX8000- und VPX10000-Lizenzen sind nur als BYOL verfügbar.
- Unabhängig von der abonnementbasierten Stundenlizenz, die von Azure Marketplace gekauft wurde, wird in seltenen Fällen die NetScaler VPX Instanz, die in Azure bereitgestellt wird,

möglicherweise mit einer standardmäßigen NetScaler-Lizenz geliefert. Dies geschieht aufgrund von Problemen mit dem Azure Instance Metadata Service (IMDS).

- Führen Sie einen Warmstart durch, bevor Sie eine Konfigurationsänderung an der NetScaler VPX-Instanz vornehmen, um die richtige NetScaler VPX-Lizenz zu aktivieren.

IPv6-Unterstützung für die NetScaler VPX-Instanz in Azure

Ab Version 13.1-21.x unterstützt die eigenständige NetScaler VPX-Instanz IPv6-Adressen in Azure. Sie können die IPv6-Adressen als VIP- und SNIP-Adressen auf der eigenständigen NetScaler VPX-Instanz in der Azure Cloud konfigurieren.

Informationen zum Aktivieren von IPv6 in Azure finden Sie in der folgenden Azure-Dokumentation:

- Was ist IPv6 für Azure Virtual Network?
- IPv6 zu einer IPv4-Anwendung im virtuellen Azure-Netzwerk hinzufügen — Azure CLI
- Typen von Adressen

Informationen darüber, wie die NetScaler-Appliance IPv6 unterstützt, finden Sie unter Internet Protocol Version 6.

IPv6-Einschränkungen:

- IPv6-Bereitstellungen in NetScaler unterstützen derzeit kein Azure-Backend-Autoscaling.
- IPv6 wird für die NetScaler VPX HA-Bereitstellung nicht unterstützt.

Einschränkungen

Die Ausführung der NetScaler VPX Load Balancing-Lösung auf ARM erlegt die folgenden Einschränkungen auf:

- Die Azure-Architektur unterstützt die folgenden NetScaler-Funktionen nicht:
  - Unentgeltliches ARP (GARP)
  - L2-Modus
  - Getaggtes VLAN
  - Dynamisches Routing
  - virtueller MAC
  - USIP
  - Clustering

> **Hinweis:**
>
> Mit der Autoscale-Funktion (Cloud-Bereitstellung) von NetScaler Application Delivery Management (ADM) unterstützen die ADC-Instanzen das Clustering auf allen Lizenzen. Weit-

> ere Informationen finden Sie unter Autoscaling von NetScaler VPX in Microsoft Azure mit NetScaler ADM.

- Wenn Sie erwarten, dass Sie die virtuelle NetScaler VPX-Maschine jederzeit herunterfahren und vorübergehend freigeben müssen, weisen Sie beim Erstellen der virtuellen Maschine eine statische interne IP-Adresse zu. Wenn Sie keine statische interne IP-Adresse zuweisen, weist Azure der virtuellen Maschine bei jedem Neustart möglicherweise eine andere IP-Adresse zu, und auf die virtuelle Maschine kann nicht zugegriffen werden.
- In einer Azure-Bereitstellung werden nur die folgenden NetScaler VPX-Modelle unterstützt: VPX 10, VPX 200, VPX 1000, VPX 3000 und VPX 5000. Weitere Informationen finden Sie im NetScaler VPX-Datenblatt.

  Wenn Sie eine NetScaler VPX-Instanz mit einer Modellnummer über VPX 3000 verwenden, ist der Netzwerkdurchsatz möglicherweise nicht der gleiche wie in der Lizenz der Instanz angegeben. Andere Funktionen wie SSL-Durchsatz und SSL-Transaktionen pro Sekunde könnten sich jedoch verbessern.
- Die Bereitstellungs-ID, die von Azure während der Bereitstellung virtueller Maschinen generiert wird, ist für den Benutzer in ARM nicht sichtbar. Sie können die Bereitstellungs-ID nicht verwenden, um NetScaler VPX Appliance auf ARM bereitzustellen.
- Die NetScaler VPX-Instanz unterstützt einen Durchsatz von 20 Mbit/s und Funktionen der Standard Edition, wenn sie initialisiert wird.
- Die NetScaler VPX-Instanzen auf Azure mit aktiviertem beschleunigtem Netzwerk bieten eine bessere Leistung. Azure-beschleunigtes Netzwerk wird ab Version 13.0 Build 76.x auf NetScaler VPX-Instanzen unterstützt. Um beschleunigtes Netzwerken auf NetScaler VPX zu aktivieren, empfiehlt Citrix, einen Azure-Instanztyp zu verwenden, der beschleunigte Netzwerke unterstützt.
- Für die Bereitstellung von Citrix Virtual Apps and Desktops kann ein virtueller VPN-Server auf einer VPX-Instanz in den folgenden Modi konfiguriert werden:
  - Basismodus, in dem der Parameter `ICAOnly` des virtuellen VPN-Servers auf ON eingestellt ist. Der Basismodus funktioniert vollständig auf einer nicht lizenzierten NetScaler VPX-Instanz.
  - SmartAccess-Modus, in dem der Parameter `ICAOnly` des virtuellen VPN-Servers auf OFF eingestellt ist. Der SmartAccess Modus funktioniert nur für fünf NetScaler AAA-Sitzungsbenutzer auf einer nicht lizenzierten NetScaler VPX Instanz.

> **Hinweis:**
>
> Um das SmartControl-Feature zu konfigurieren, müssen Sie eine Premium-Lizenz auf die NetScaler VPX Instanz anwenden.

Azure-Terminologie

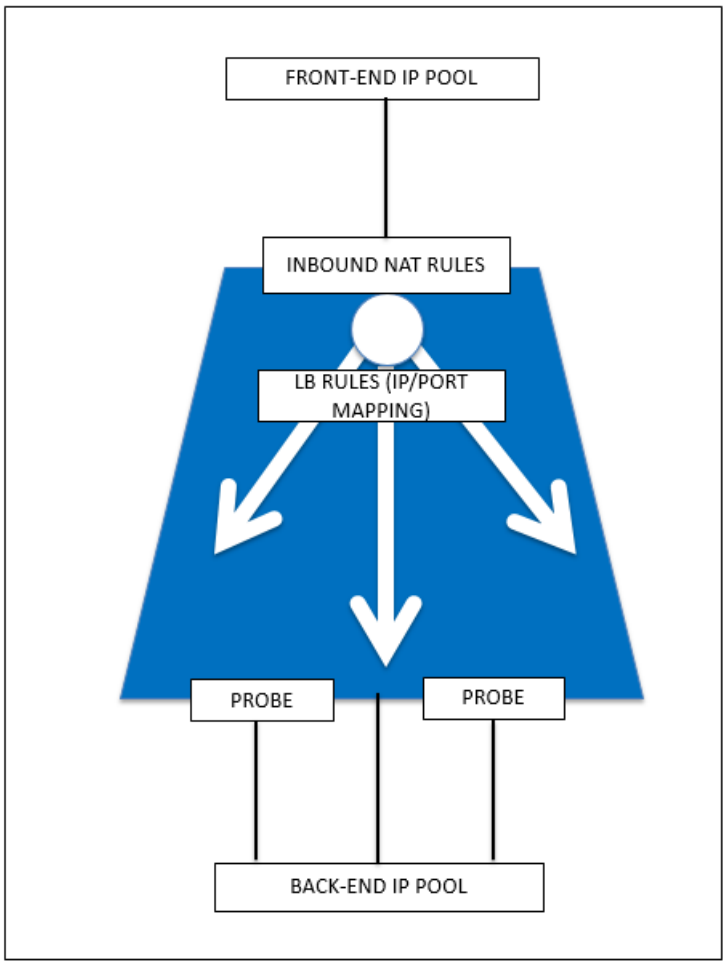
May 11, 2023

Einige der Azure-Begriffe, die in der NetScaler VPX Azure-Dokumentation verwendet werden, sind unten aufgeführt.

1. Azure Load Balancer — Azure Load Balancer ist eine Ressource, die eingehenden Datenverkehr auf Computer in einem Netzwerk verteilt. Der Datenverkehr wird auf virtuelle Maschinen verteilt, die in einem Load Balancer-Set definiert sind. Ein Load Balancer kann extern oder mit dem Internet verbunden sein, oder er kann intern sein.
2. Azure Resource Manager (ARM) — ARM ist das neue Verwaltungsframework für Dienste in Azure. Azure Load Balancer wird mit ARM-basierten APIs und Tools verwaltet.
3. Back-End-Adresspool — Dies sind IP-Adressen, die mit der NIC (NIC) der virtuellen Maschine verknüpft sind, auf die die Last verteilt wird.
4. BLOB - Binary Large Object — Jedes binäre Objekt wie eine Datei oder ein Image, das im Azure-Speicher gespeichert werden kann.
5. Front-End-IP-Konfiguration — Ein Azure Load Balancer kann eine oder mehrere Front-End-IP-Adressen enthalten, die auch als virtuelle IPs (VIPs) bezeichnet werden. Diese IP-Adressen dienen als Eindringen für den Datenverkehr.
6. Instance Level Public IP (ILPIP) — Eine ILPIP ist eine öffentliche IP-Adresse, die Sie direkt Ihrer virtuellen Maschine oder Rolleninstanz zuweisen können, anstatt dem Cloud-Dienst, in dem sich Ihre virtuelle Maschine oder Rolleninstanz befindet. Dies tritt nicht an die Stelle der VIP (virtuelle IP), die Ihrem Cloud-Dienst zugewiesen ist. Vielmehr handelt es sich um eine zusätzliche IP-Adresse, die Sie verwenden können, um eine direkte Verbindung mit Ihrer virtuellen Maschine oder Rolleninstanz herzustellen.

   Hinweis: In der Vergangenheit wurde ein ILPIP als PIP bezeichnet, was für öffentliches IP steht.
7. NAT-Regeln für eingehenden Datenverkehr — Diese Regeln enthalten Regeln, die einen öffentlichen Port auf dem Load Balancer einem Port für eine bestimmte virtuelle Maschine im Back-End-Adresspool zuordnen.
8. IP-config - Es kann als ein IP-Adresspaar (öffentliche IP und private IP) definiert werden, das mit einer einzelnen NIC verknüpft ist. In einer IP-Konfiguration kann die öffentliche IP-Adresse NULL sein. Jeder NIC kann mehrere IP-Konfig zugeordnet sein, was bis zu 255 betragen kann.
9. Lastenausgleichsregeln — Eine Regeleigenschaft, die eine gegebene Front-End-IP- und Port-Kombination einer Reihe von Back-End-IP-Adressen und einer Portkombination zuordnet. Mit einer einzigen Definition einer Load Balancer-Ressource können Sie mehrere Lastenausgleichsregeln definieren, wobei jede Regel eine Kombination aus einer Front-End-IP und einem Port

sowie einer Back-End-IP und einem Port für virtuelle Maschinen widerspiegelt.

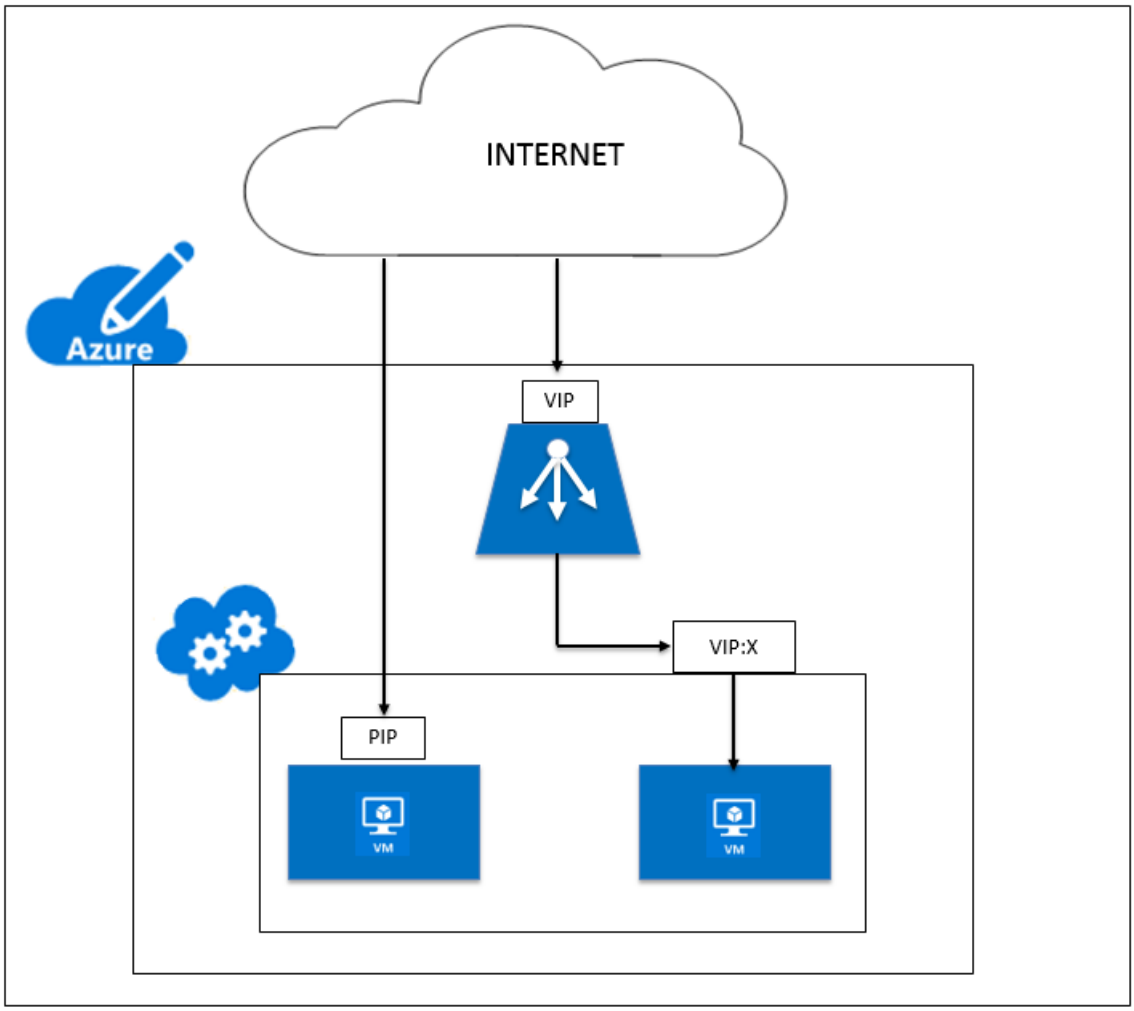


10. Netzwerksicherheitsgruppe — Enthält eine Liste von Zugriffssteuerungslisten (ACL) -Regeln, die den Netzwerkverkehr für Ihre Instanzen der virtuellen Maschine in einem virtuellen Netzwerk zulassen oder verweigern. NSGs können entweder Subnetzen oder einzelnen Instanzen virtueller Maschinen innerhalb dieses Subnetzes zugeordnet werden. Wenn eine Netzwerksicherheitsgruppe mit einem Subnetz verknüpft ist, gelten die ACL-Regeln für alle Instanzen der virtuellen Maschine in diesem Subnetz. Darüber hinaus kann der Datenverkehr zu einer einzelnen virtuellen Maschine weiter eingeschränkt werden, indem eine Netzwerksicherheitsgruppe direkt mit dieser virtuellen Maschine verknüpft wird.

11. Private IP-Adressen — Wird für die Kommunikation innerhalb eines virtuellen Azure-Netzwerks und Ihres lokalen Netzwerks verwendet, wenn Sie ein VPN-Gateway verwenden, um Ihr Netzwerk auf Azure zu erweitern. Private IP-Adressen ermöglichen es Azure-Ressourcen, mit anderen Ressourcen in einem virtuellen Netzwerk oder einem lokalen Netzwerk über ein VPN-Gateway oder eine ExpressRoute-Schaltung zu kommunizieren, ohne eine vom Internet erreichbare IP-Adresse zu verwenden. Im Azure Resource Manager Bereitstellungsmodell ist eine private IP-Adresse den folgenden Arten von Azure-Ressourcen zugeordnet: virtuelle Maschinen, interne

Lastausgleichsdienste (ILBs) und Anwendungsgateways.

12. Tests — Dies enthält Integritätstests, mit denen die Verfügbarkeit von Instanzen virtueller Maschinen im Back-End-Adresspool überprüft wird. Wenn eine bestimmte virtuelle Maschine für einige Zeit nicht auf Health Probes reagiert, wird sie aus dem Datenverkehr genommen. Mithilfe von Sonden können Sie den Zustand virtueller Instanzen verfolgen. Wenn eine Integritätsprüfung fehlschlägt, wird die virtuelle Instanz automatisch aus der Rotation genommen.
13. Öffentliche IP-Adressen (PIP) — PIP wird für die Kommunikation mit dem Internet verwendet, einschließlich öffentlicher Azure-Dienste und ist mit virtuellen Maschinen, mit Internetzugang verbundenen Lastausgleichsdiensten, VPN-Gateways und Anwendungsgateways verknüpft.
14. Region - Ein Gebiet innerhalb einer Geographie, das keine nationalen Grenzen überschreitet und ein oder mehrere Rechenzentren enthält. Preise, regionale Dienstleistungen und Angebotsarten werden auf regionaler Ebene angezeigt. Eine Region wird in der Regel mit einer anderen Region, die bis zu mehreren hundert Meilen entfernt sein kann, gepaart, um ein regionales Paar zu bilden. Regionale Paare können als Mechanismus für Disaster Recovery und Hochverfügbarkeitsszenarien verwendet werden. Auch allgemein als Standort bezeichnet.
15. Ressourcengruppe — Ein Container in Resource Manager enthält zugehörige Ressourcen für eine Anwendung. Die Ressourcengruppe kann alle Ressourcen für eine Anwendung oder nur die Ressourcen enthalten, die logisch gruppiert sind.
16. Speicherkonto — Mit einem Azure-Speicherkonto haben Sie Zugriff auf die Azure-Blob-, Warteschlangen-, Tabellen- und Dateidienste in Azure Storage. Ihr Speicherkonto stellt den eindeutigen Namespace für Ihre Azure-Speicherdatenobjekte bereit.
17. Virtuelle Maschine — Die Software-Implementierung eines physischen Computers, auf dem ein Betriebssystem ausgeführt wird. Mehrere virtuelle Maschinen können gleichzeitig auf derselben Hardware ausgeführt werden. In Azure sind virtuelle Maschinen in verschiedenen Größen verfügbar.
18. Virtuelles Netzwerk — Ein virtuelles Azure-Netzwerk ist eine Darstellung Ihres eigenen Netzwerks in der Cloud. Es handelt sich um eine logische Isolierung der Azure-Cloud, die Ihrem Abonnement gewidmet ist. Sie können die IP-Adressblöcke, DNS-Einstellungen, Sicherheitsrichtlinien und Routing-Tabellen in diesem Netzwerk vollständig kontrollieren. Sie können Ihr VNet auch weiter in Subnetze unterteilen und virtuelle Azure-IaaS-Maschinen und -Cloud-Dienste (PaaS-Rolleninstanzen) starten. Darüber hinaus können Sie das virtuelle Netzwerk mithilfe einer der in Azure verfügbaren Konnektivitätsoptionen mit Ihrem on-premises Netzwerk verbinden. Im Wesentlichen können Sie Ihr Netzwerk auf Azure erweitern, mit vollständiger Kontrolle über IP-Adressblöcke mit dem Vorteil, dass Azure Enterprise Scale bietet.



Netzwerkarchitektur für NetScaler VPX-Instanzen auf Microsoft Azure

May 11, 2023

In Azure Resource Manager (ARM) befindet sich eine virtuelle NetScaler VPX-Maschine (VM) in einem virtuellen Netzwerk. Eine einzelne Netzwerkschnittstelle kann in einem bestimmten Subnetz des virtuellen Netzwerks erstellt und an die VPX-Instanz angehängt werden. Sie können den Netzwerkverkehr zu und von einer VPX-Instanz in einem virtuellen Azure-Netzwerk mit einer Netzwerksicherheitsgruppe filtern. Eine Netzwerksicherheitsgruppe enthält Sicherheitsregeln, die eingehenden Netzwerkverkehr zu oder ausgehenden Netzwerkverkehr von einer VPX-Instanz zulassen oder ablehnen. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Die Netzwerksicherheitsgruppe filtert die Anforderungen an die NetScaler VPX-Instanz, und die VPX-Instanz sendet sie an die Server. Die Antwort von einem Server folgt dem gleichen Pfad in

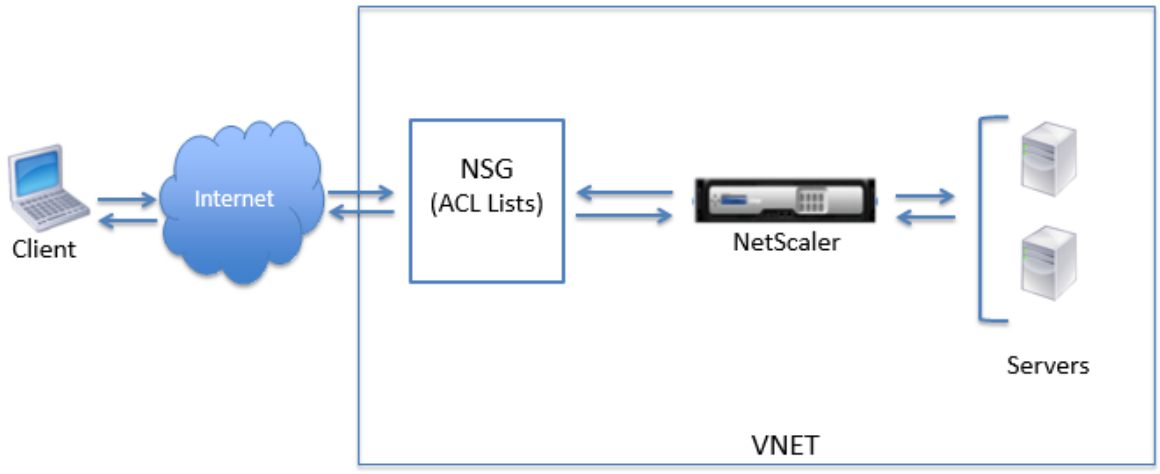
umgekehrter Richtung. Die Netzwerksicherheitsgruppe kann so konfiguriert werden, dass sie eine einzelne VPX-VM filtert, oder, mit Subnetzen und virtuellen Netzwerken, kann sie den Datenverkehr bei der Bereitstellung mehrerer VPX-Instanzen filtern.

Die NIC enthält Netzwerkkonfigurationsdetails wie das virtuelle Netzwerk, Subnetze, interne IP-Adresse und öffentliche IP-Adresse.

Bei ARM sollten Sie die folgenden IP-Adressen kennen, die für den Zugriff auf die VMs verwendet werden, die mit einer einzelnen Netzwerkkarte und einer einzelnen IP-Adresse bereitgestellt werden:

- Die öffentliche IP-Adresse (PIP) ist die IP-Adresse, die direkt auf der virtuellen Netzwerkkarte der NetScaler-VM konfiguriert wurde. Auf diese Weise können Sie direkt über das externe Netzwerk auf eine VM zugreifen.
- Die NetScaler IP (auch NSIP genannt) Adresse ist die interne IP-Adresse, die auf der VM konfiguriert ist. Es ist nicht routingfähig.
- Die virtuelle IP-Adresse (VIP) wird mithilfe des NSIP und einer Portnummer konfiguriert. Clients greifen über die PIP-Datei auf NetScaler-Dienste zu. Wenn die Anfrage die NIC der NetScaler VPX-VM oder des Azure Load Balancers erreicht, wird die VIP in interne IP (NSIP) und interne Portnummer übersetzt.
- Die interne IP-Adresse ist die private interne IP-Adresse der VM aus dem Adressraumpool des virtuellen Netzwerks. Diese IP-Adresse kann nicht vom externen Netzwerk aus erreicht werden. Diese IP-Adresse ist standardmäßig dynamisch, sofern Sie sie nicht auf statisch setzen. Der Datenverkehr aus dem Internet wird gemäß den Regeln, die in der Netzwerksicherheitsgruppe erstellt wurden, an diese Adresse weitergeleitet. Die Netzwerksicherheitsgruppe lässt sich in die Netzwerkkarte integrieren, um selektiv den richtigen Datenverkehr an den richtigen Port der NIC zu senden, was von den auf der VM konfigurierten Diensten abhängt.

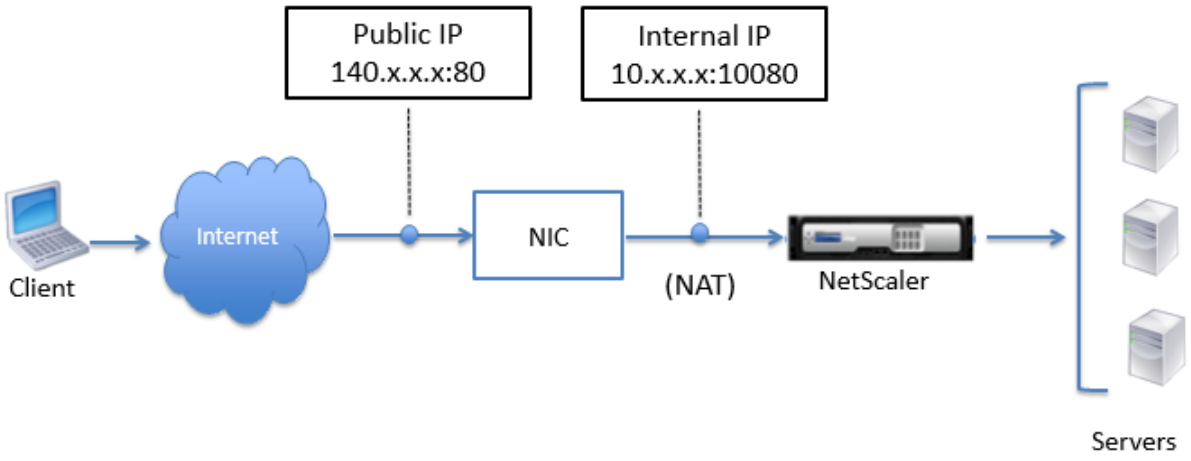
Die folgende Abbildung zeigt, wie der Datenverkehr von einem Client zu einem Server über eine in ARM bereitgestellte NetScaler VPX-Instanz fließt.



Verkehrsfluss durch Netzwerkadressübersetzung

Sie können auch eine öffentliche IP-Adresse (PIP) für Ihre NetScaler VPX-Instanz (Instanzebene) anfordern. Wenn Sie dieses direkte PIP auf VM-Ebene verwenden, müssen Sie keine eingehenden und ausgehenden Regeln definieren, um den Netzwerkverkehr abzufangen. Die eingehende Anfrage aus dem Internet wird direkt auf der VM empfangen. Azure führt die Netzwerkadressübersetzung (NAT) durch und leitet den Datenverkehr an die interne IP-Adresse der VPX-Instanz weiter.

Die folgende Abbildung zeigt, wie Azure die Netzwerkadressübersetzung durchführt, um die interne NetScaler-IP-Adresse zuzuordnen.



In diesem Beispiel lautet die der Netzwerksicherheitsgruppe zugewiesene öffentliche IP 140.x.x.x und die interne IP-Adresse 10.x.x.x. Wenn die eingehenden und ausgehenden Regeln definiert sind, wird der öffentliche HTTP-Port 80 als Port definiert, auf dem die Clientanforderungen empfangen werden, und ein entsprechender privater Port, 10080, wird als Port definiert, auf dem die NetScaler VPX-Instanz wartet. Die Client-Anfrage wird auf der öffentlichen IP-Adresse (140.x.x.x) empfangen. Azure führt eine Netzwerkadressübersetzung durch, um die PIP der internen IP-Adresse 10.x.x.x auf Port 10080 zuzuordnen, und leitet die Clientanfrage weiter.

> **Hinweis**
>
> NetScaler VPX-VMs mit hoher Verfügbarkeit werden von externen oder internen Load Balancern gesteuert, auf denen eingehende Regeln zur Steuerung des Load-Balancing-Datenverkehrs definiert sind. Der externe Datenverkehr wird zuerst von diesen Load Balancern abgefangen und der Verkehr wird gemäß den konfigurierten Load-Balancing-Regeln umgeleitet, für die Back-End-Pools, NAT-Regeln und Integritätstests auf den Load Balancern definiert sind.

Richtlinien zur Port-Nutzung

Sie können weitere eingehende und ausgehende Regeln n Netzwerksicherheitsgruppen konfigurieren, während Sie die NetScaler VPX-Instanz erstellen oder nachdem die virtuelle Maschine bereitgestellt wurde. Jede eingehende und ausgehende Regel ist einem öffentlichen und einem privaten Port zugeordnet.

Beachten Sie vor der Konfiguration der Regeln für Netzwerksicherheitsgruppen die folgenden Richtlinien bezüglich der Portnummern, die Sie verwenden können:

1. Die NetScaler VPX-Instanz reserviert die folgenden Ports. Sie können diese nicht als private Ports definieren, wenn Sie die öffentliche IP-Adresse für Anfragen aus dem Internet verwenden.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Wenn Sie jedoch möchten, dass Internetdienste wie der VIP einen Standardport verwenden (z. B. Port 443), müssen Sie mithilfe der Netzwerksicherheitsgruppe eine Portzuordnung erstellen. Der Standardport wird dann einem anderen Port zugeordnet, der auf dem NetScaler für diesen VIP-Dienst konfiguriert ist.

   Beispielsweise kann ein VIP-Dienst auf Port 8443 der VPX-Instanz ausgeführt werden, wird aber dem öffentlichen Port 443 zugeordnet. Wenn der Benutzer also über die Public IP auf Port 443 zugreift, wird die Anforderung an den privaten Port 8443 weitergeleitet.
2. Die öffentliche IP-Adresse unterstützt keine Protokolle, in denen die Portzuordnung dynamisch geöffnet wird, wie passives FTP oder ALG.
3. Hochverfügbarkeit funktioniert nicht für Datenverkehr, der eine öffentliche IP-Adresse (PIP) verwendet, die einer VPX-Instanz zugeordnet ist, anstelle eines auf dem Azure-Load Balancer konfigurierten PIP.

> **Hinweis**
>
> In Azure Resource Manager ist eine NetScaler VPX-Instanz zwei IP-Adressen zugeordnet - eine öffentliche IP-Adresse (PIP) und eine interne IP-Adresse. Während der externe Datenverkehr mit dem PIP verbunden ist, ist die interne IP-Adresse oder der NSIP nicht routingfähig. Um VIP in VPX zu konfigurieren, verwenden Sie die interne IP-Adresse und einen der verfügbaren freien Ports. Verwenden Sie nicht die PIP, um VIP zu konfigurieren.

Eigenständige NetScaler VPX-Instanz konfigurieren

May 11, 2023

Sie können eine einzelne NetScaler VPX-Instanz im Azure Resource Manager (ARM) -Portal in einem eigenständigen Modus bereitstellen, indem Sie die virtuelle Maschine erstellen und andere Ressourcen konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein Microsoft Azure-Benutzerkonto
- Zugriff auf Microsoft Azure Resource Manager
- Microsoft Azure-SDK
- Microsoft Azure PowerShell

Melden Sie sich auf der Seite Microsoft Azure-Portal beim Azure Resource Manager-Portal an, indem Sie Ihren Benutzernamen und Ihr Kennwort angeben.

> **Hinweis**
>
> Wenn Sie im ARM-Portal auf eine Option in einem Bereich klicken, wird rechts ein neuer Bereich geöffnet. Navigieren Sie von einem Bereich zum anderen, um Ihr Gerät zu konfigurieren.

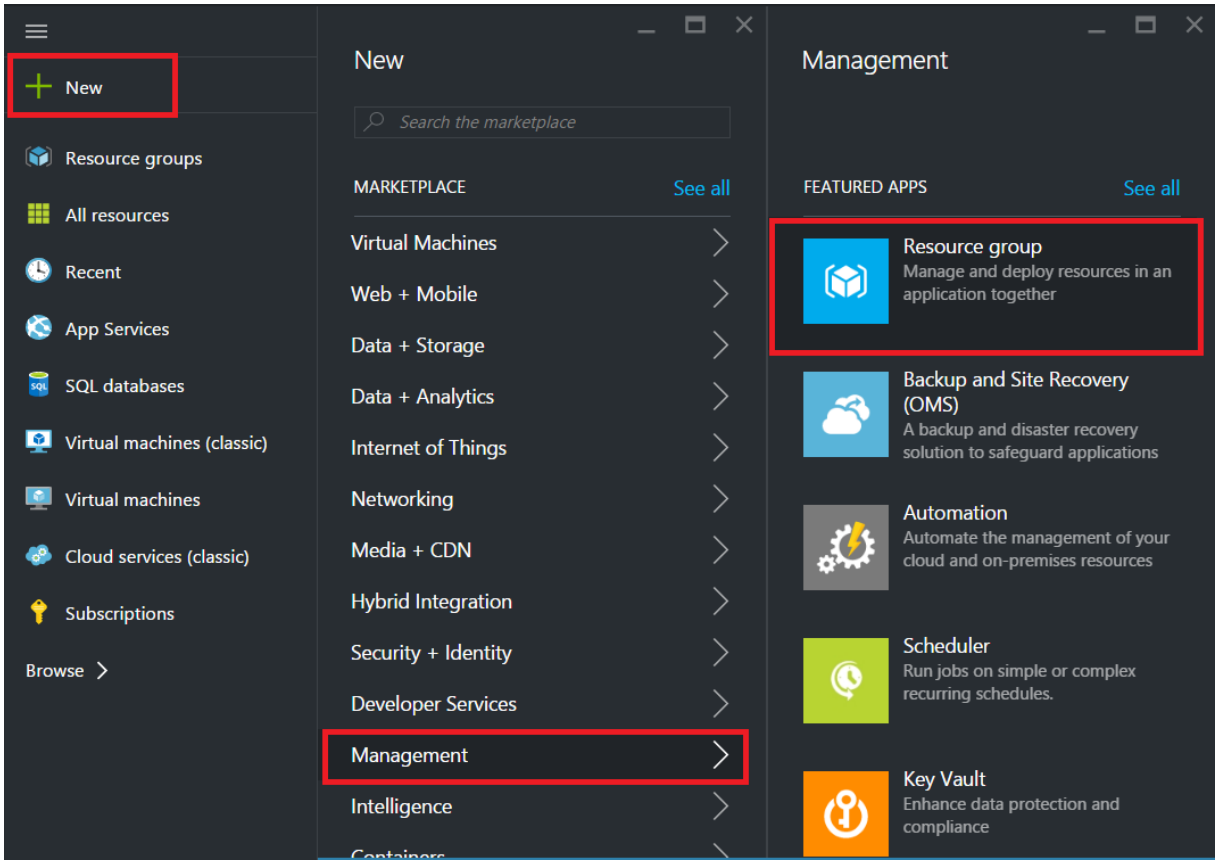
Zusammenfassung der Konfigurationsschritte

1. Eine Ressourcengruppe konfigurieren
2. Konfigurieren einer Netzwerksicherheitsgruppe
3. Virtuelles Netzwerk und seine Subnetze konfigurieren
4. Konfigurieren eines Speicherkontos
5. Konfigurieren eines Verfügbarkeitssatzes
6. Konfigurieren Sie eine NetScaler VPX-Instanz.

Eine Ressourcengruppe konfigurieren

Erstellen Sie eine neue Ressourcengruppe, die ein Container für all Ihre Ressourcen ist. Verwenden Sie die Ressourcengruppe, um Ihre Ressourcen als Gruppe bereitzustellen, zu verwalten und zu überwachen.

1. Klicken Sie auf **Neu** > **Verwaltung** > **Ressourcengruppe**.
2. Geben Sie im Bereich **Ressourcengruppe** die folgenden Details ein:
   - Ressourcengruppenname
   - Standort der Ressourcengruppe
3. Klicken Sie auf **Erstellen**.

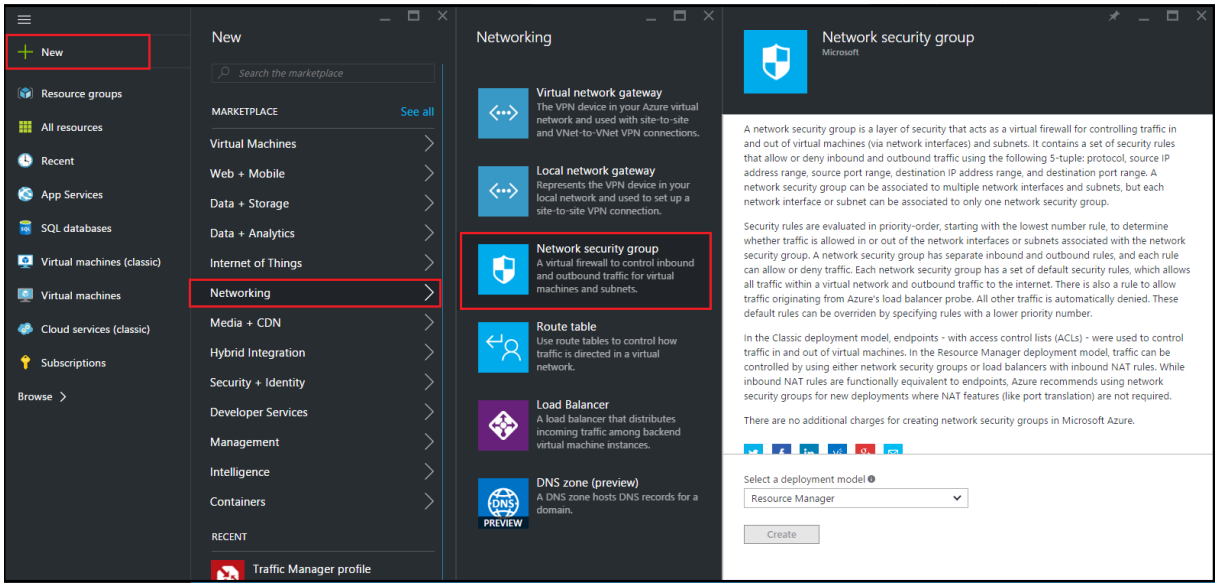


Konfigurieren einer Netzwerksicherheitsgruppe

Erstellen Sie eine Netzwerksicherheitsgruppe, um eingehende und ausgehende Regeln zuzuweisen, um den eingehenden und ausgehenden Datenverkehr innerhalb des virtuellen Netzwerks zu steuern. Mit der Netzwerksicherheitsgruppe können Sie Sicherheitsregeln für eine einzelne virtuelle Maschine definieren und Sicherheitsregeln für ein virtuelles Netzwerksubnetz definieren.

1. Klicken Sie auf **Neu** > **Netzwerk** > **Netzwerksicherheitsgruppe**.
2. Geben **Sie im Bereich Netzwerksicherheitsgruppe erstellen** die folgenden Details ein, und klicken Sie dann auf **Erstellen**.
    - Name — geben Sie einen Namen für die Sicherheitsgruppe ein
    - Ressourcengruppe — wählen Sie die Ressourcengruppe aus der Dropdownliste aus

> **Hinweis**
>
> Stellen Sie sicher, dass Sie den richtigen Standort ausgewählt haben. Die Liste der Ressourcen, die in der Dropdownliste angezeigt werden, unterscheidet sich für verschiedene Speicherorte.

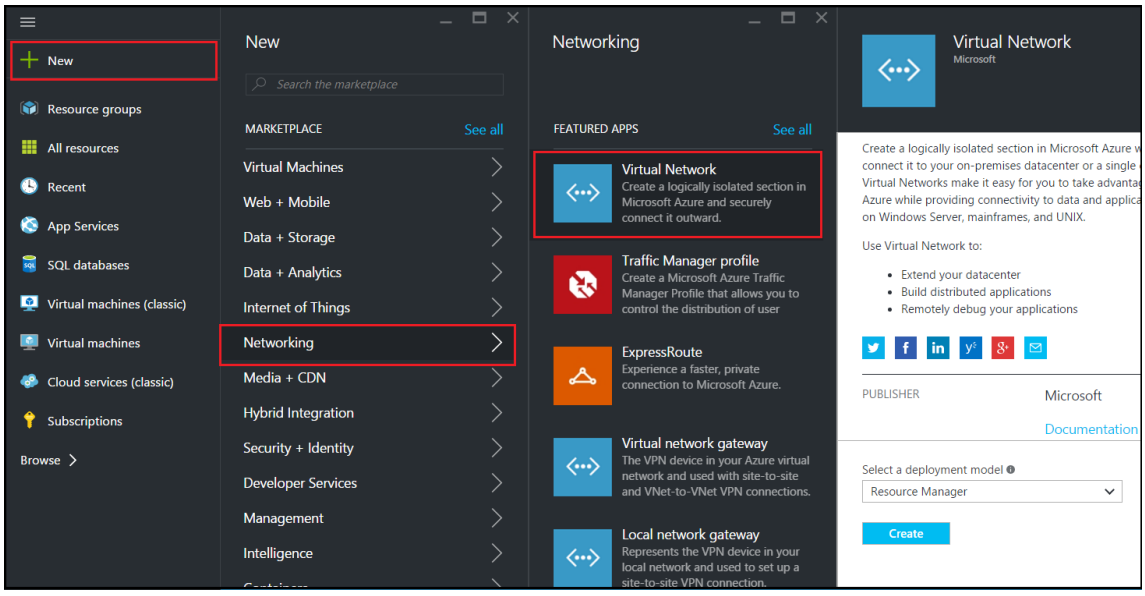


Konfigurieren eines virtuellen Netzwerks und der Subnetze

Virtuelle Netzwerke in ARM bieten eine Sicherheits- und Isolationsebene für Ihre Dienste. VMs und Dienste, die Teil desselben virtuellen Netzwerks sind, können aufeinander zugreifen.

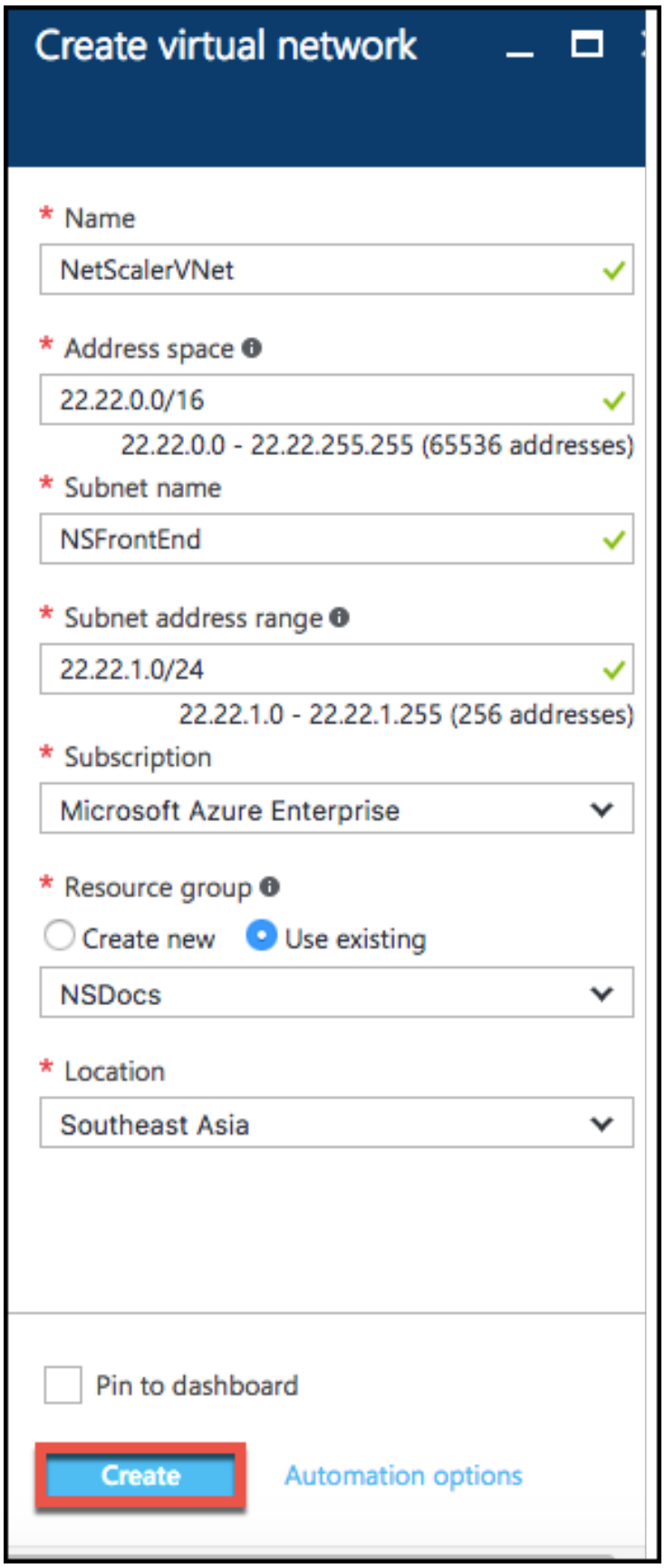
Für diese Schritte, um ein virtuelles Netzwerk und Subnetze zu erstellen.

1. Klicken Sie auf **Neu** > **Netzwerk** > **Virtuelles Netzwerk**.
2. Stellen Sie im Bereich **Virtuelles Netzwerk** sicher, dass der Bereitstellungsmodus **Ressourcenmanager** ist, und klicken Sie auf **Erstellen**.



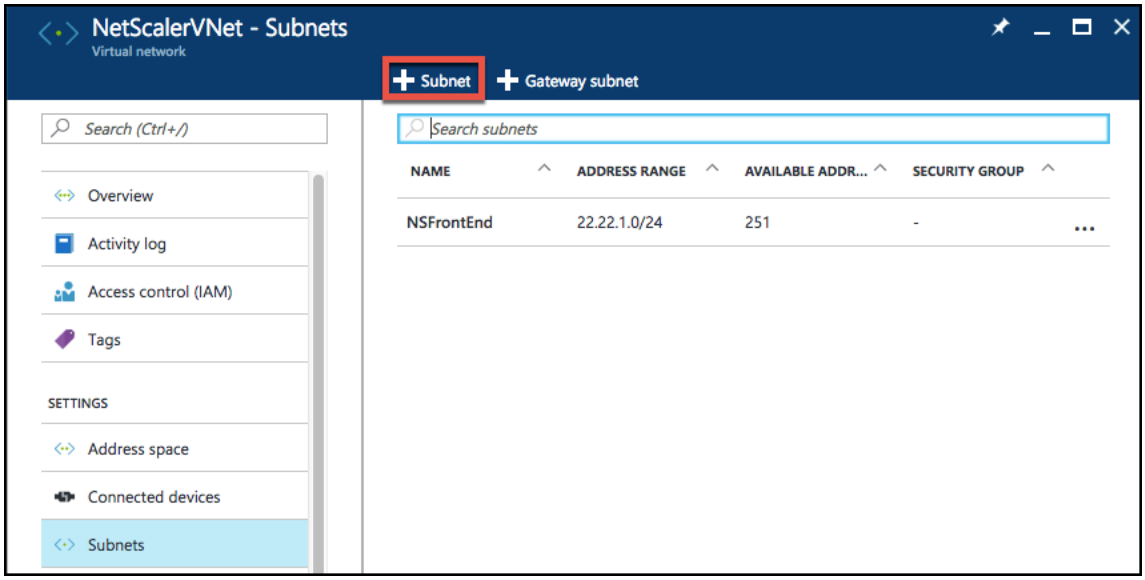
3. Geben Sie im Bereich **Virtuelles Netzwerk erstellen** die folgenden Werte ein, und klicken Sie dann auf **Erstellen**.

- Name des virtuellen Netzwerks
- Adressraum — geben Sie den reservierten IP-Adressblock für das virtuelle Netzwerk ein
- Subnetz — geben Sie den Namen des ersten Subnetzes ein (das zweite Subnetz erstellen Sie später in diesem Schritt)
- Subnetz-Adressbereich — Geben Sie den reservierten IP-Adressblock des Subnetzes ein
- Ressourcengruppe: Wählen Sie die zuvor erstellte Ressourcengruppe aus der Dropdownliste aus

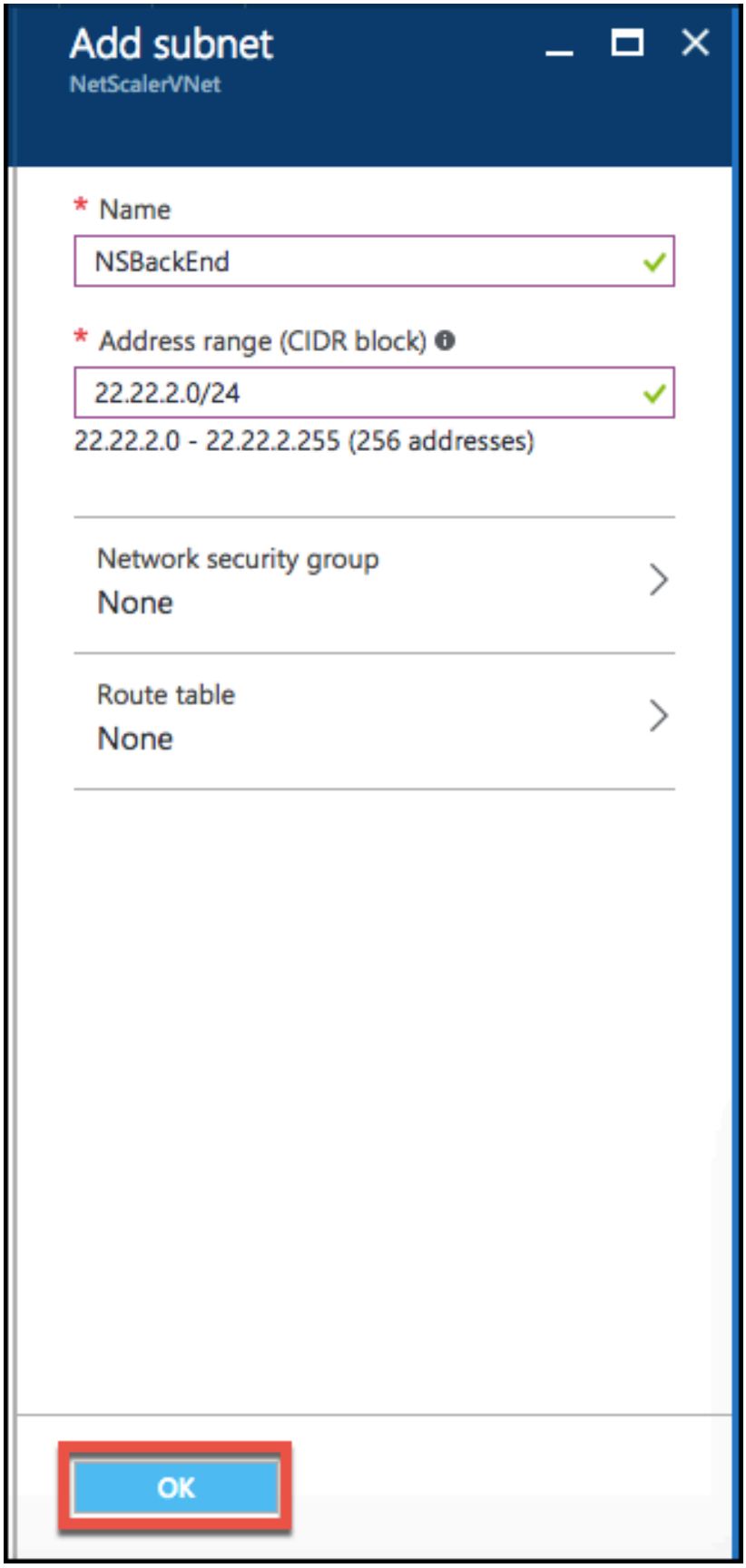


Konfigurieren des zweiten Subnetzes

1. Wählen Sie im Bereich **Alle Ressourcen** das neu erstellte virtuelle Netzwerk aus, und klicken Sie im Bereich **Einstellungen** auf **Subnetze**.



2. Klicken Sie auf **+ Subnetz**, und erstellen Sie das zweite Subnetz, indem Sie die folgenden Details eingeben.
   - Name des zweiten Subnetzes
   - Adressbereich - Geben Sie den reservierten IP-Adressblock des zweiten Subnetzes ein
   - Netzwerksicherheitsgruppe - wählen Sie die Netzwerksicherheitsgruppe aus der Dropdownliste
3. Klicken Sie auf **Erstellen**.

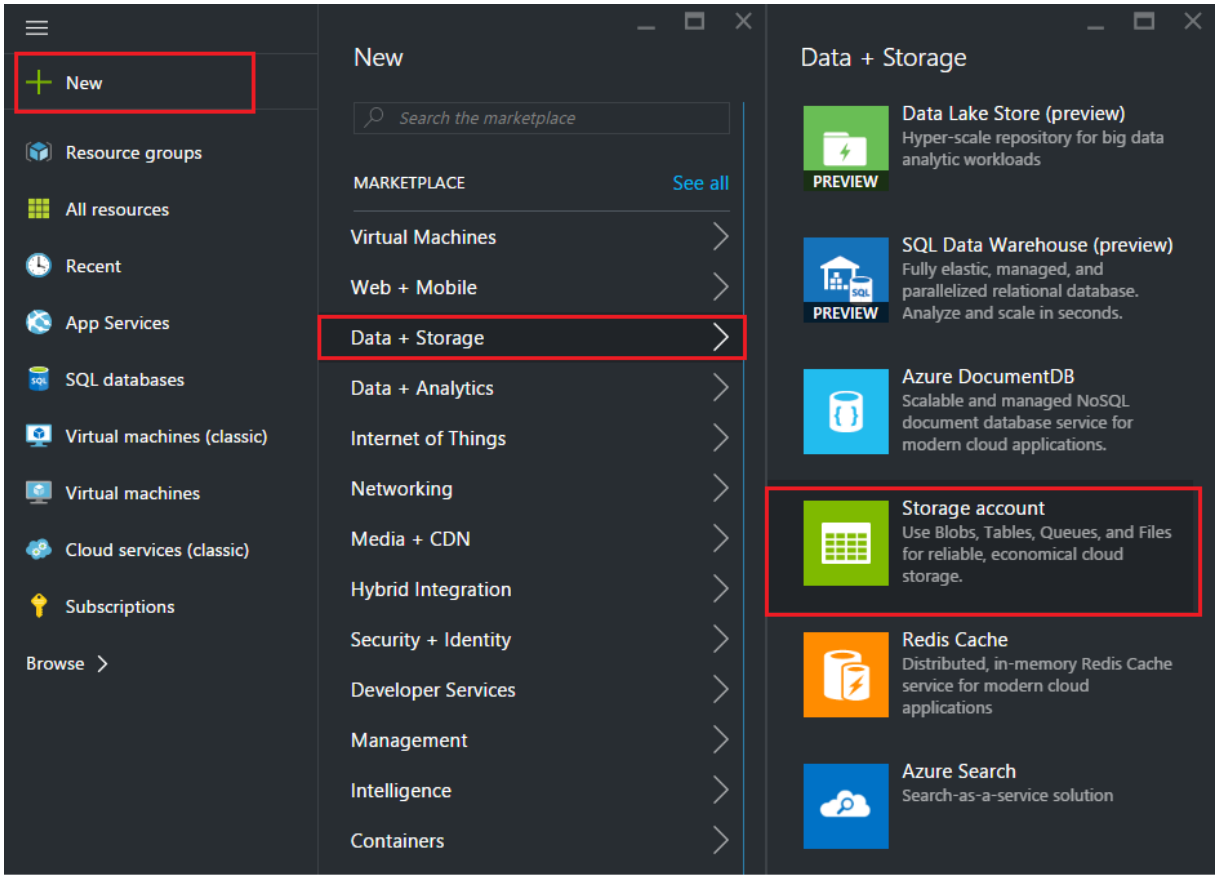


Konfigurieren eines Speicherkontos

Der ARM-IaaS-Infrastrukturspeicher umfasst alle Dienste, in denen wir Daten in Form von Blobs, Tabellen, Warteschlangen und Dateien speichern können. Sie können auch Anwendungen erstellen, die diese Formen von Speicherdaten in ARM verwenden.

Erstellen Sie ein Speicherkonto, um all Ihre Daten zu speichern.

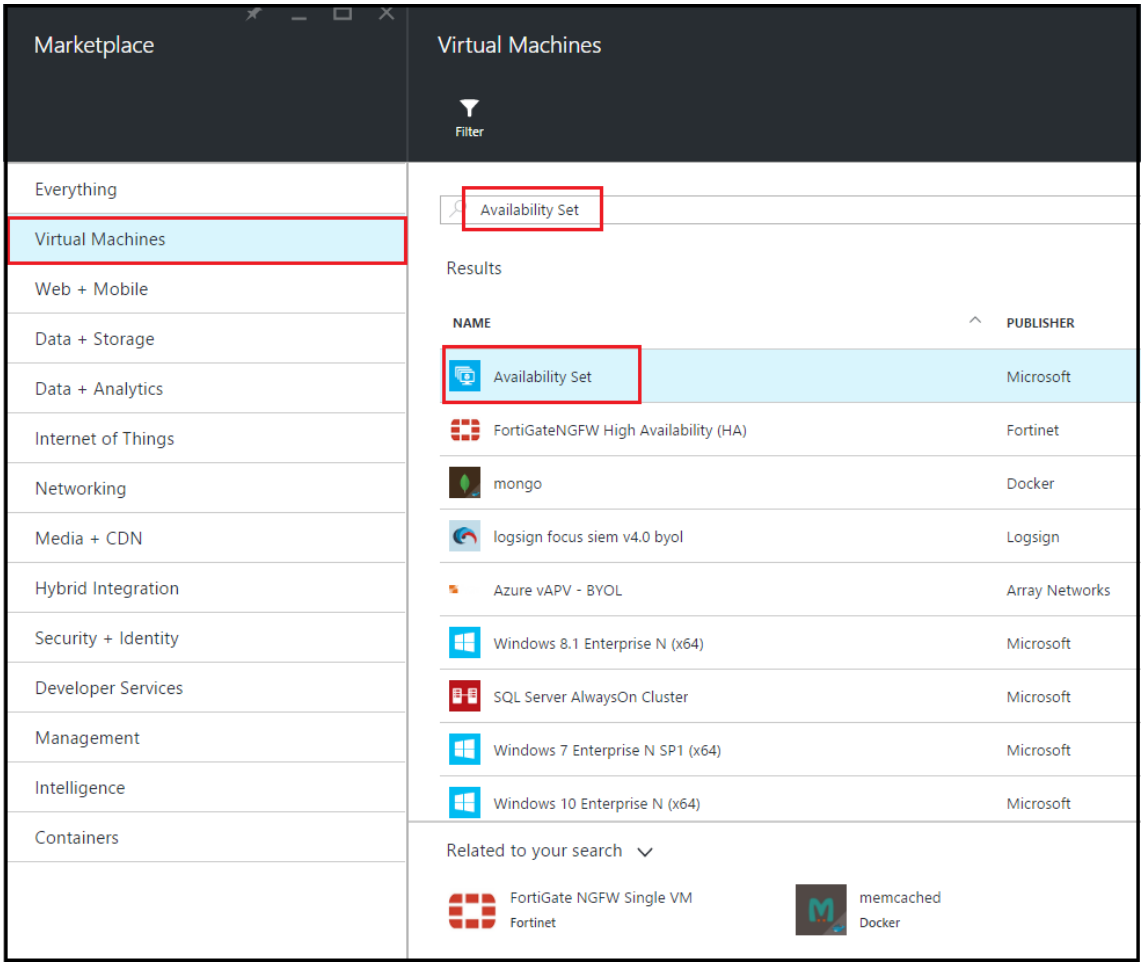
1. Klicken Sie auf **+Neu** > **Daten + Speicher** > **Speicherkonto**.
2. Geben **Sie im Bereich Speicherkonto erstellen** die folgenden Details ein:
    - Name des Accounts
    - Bereitstellungsmodus — stellen Sie sicher, dass Sie **Resource Manager**auswählen
    - Kontoart - wählen Sie **Allzweck** aus der Dropdownliste
    - Replikation — Wählen Sie **Lokal redundanter Speicher** aus der Dropdownliste aus
    - Ressourcengruppe — wählen Sie die neu erstellte Ressourcengruppe aus der Dropdown-liste aus
3. Klicken Sie auf **Erstellen**.



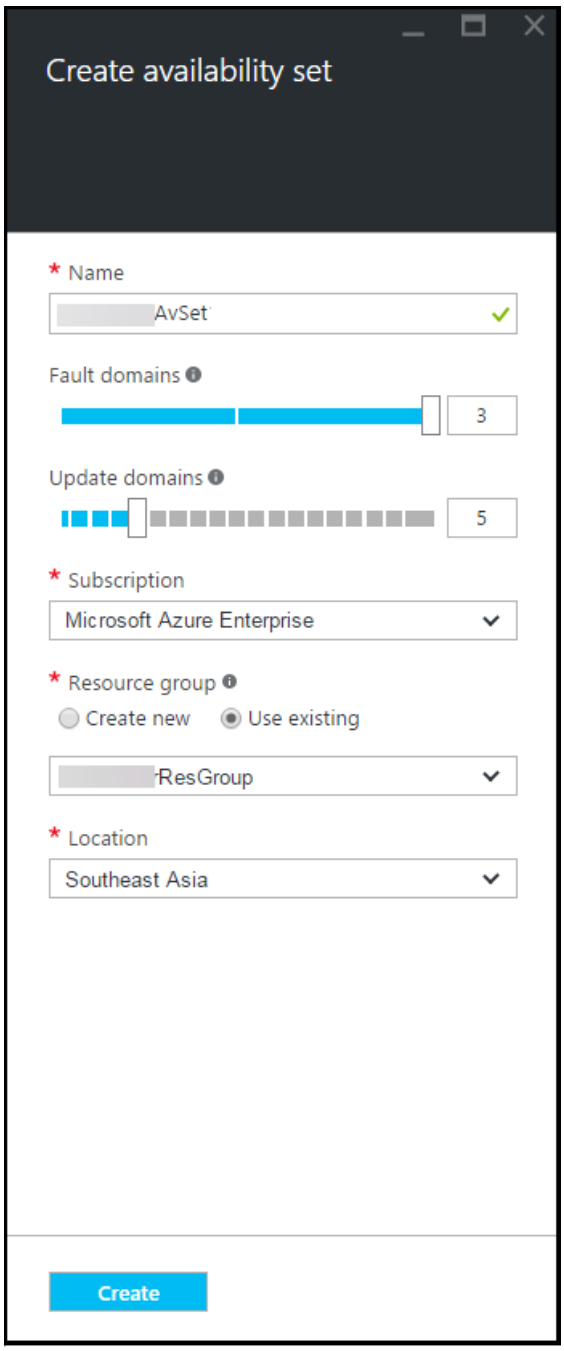
Konfigurieren eines Verfügbarkeitssatzes

Ein Verfügbarkeitsset garantiert, dass mindestens eine VM im Falle einer geplanten oder ungeplanten Wartung betriebsbereit bleibt. Zwei oder mehr VMs unter derselben „Verfügbarkeitsgruppe“ werden in verschiedenen Fehlerdomänen platziert, um redundante Dienste bereitzustellen.

1. Klicken Sie auf **+Neu**.
2. Klicken **Sie im Bereich MARKETPLACE auf Alle anzeigen** und dann auf **Virtuelle Maschinen**.
3. Suchen Sie nach Verfügbarkeitssatz, und wählen Sie dann **Verfügbarkeitssatzentität** aus der angezeigten Liste aus.



4. Klicken Sie auf **Erstellen,** und geben **Sie im Bereich Verfügbarkeitssatz** erstellen die folgenden Details ein:
   - Name des Sets
   - Ressourcengruppe — wählen Sie die neu erstellte Ressourcengruppe aus der Dropdownliste aus
5. Klicken Sie auf **Erstellen**.



Konfigurieren einer NetScaler VPX-Instanz

Erstellen Sie eine Instanz von NetScaler VPX im virtuellen Netzwerk. Besorgen Sie sich das NetScaler VPX-Image vom Azure Marketplace und verwenden Sie dann das Azure Resource Manager-Portal, um eine NetScaler VPX-Instanz zu erstellen.

Bevor Sie mit der Erstellung der NetScaler VPX-Instanz beginnen, stellen Sie sicher, dass Sie ein virtuelles Netzwerk mit den erforderlichen Subnetzen erstellt haben, in denen sich die Instanz

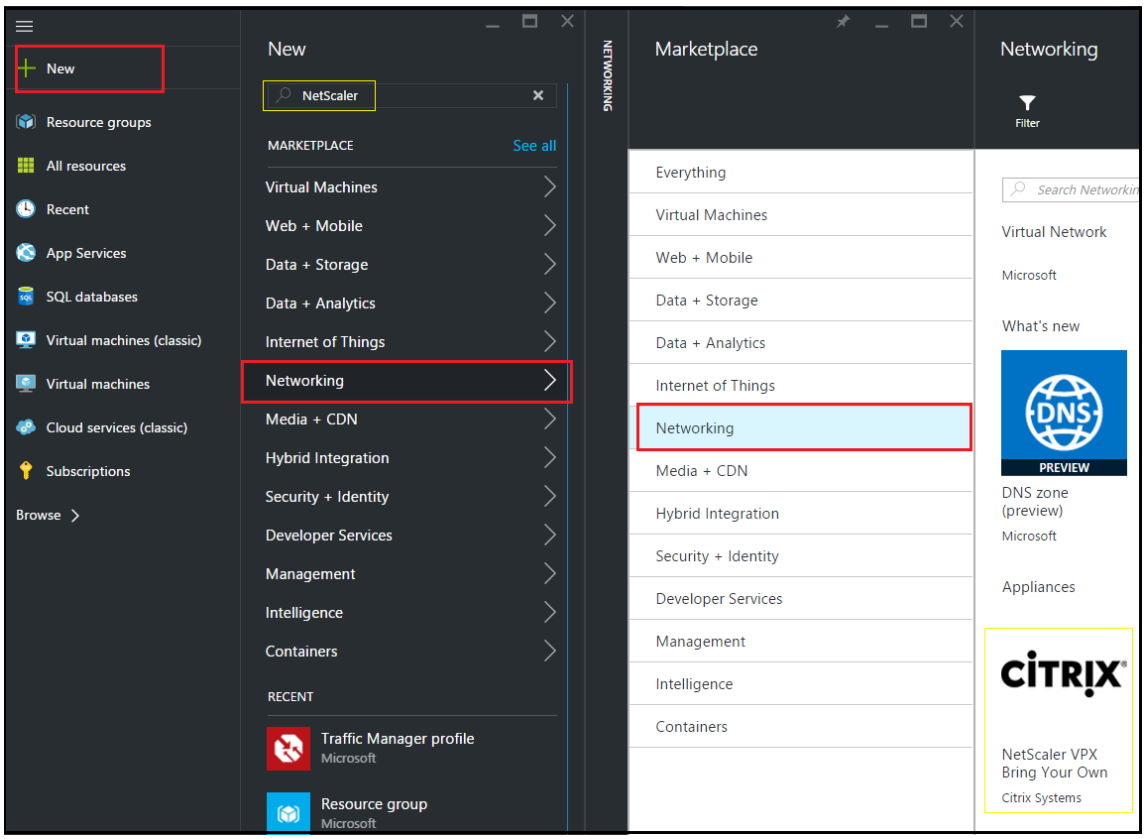
befindet. Sie können während des VM-Provisionings virtuelle Netzwerke erstellen, jedoch ohne die Flexibilität, verschiedene Subnetze einzurichten. Hinweise zum Erstellen virtueller Netzwerke finden Sie unter http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/.

Konfigurieren Sie optional den DNS-Server und die VPN-Konnektivität, die es einer virtuellen Maschine ermöglichen, auf Internetressourcen zuzugreifen.

> **Hinweis**
>
> Citrix empfiehlt, dass Sie vor der Bereitstellung der NetScaler VPX-VM eine Ressourcengruppe, eine Netzwerksicherheitsgruppe, ein virtuelles Netzwerk und andere Entitäten erstellen, damit die Netzwerkinformationen während der Bereitstellung verfügbar sind.

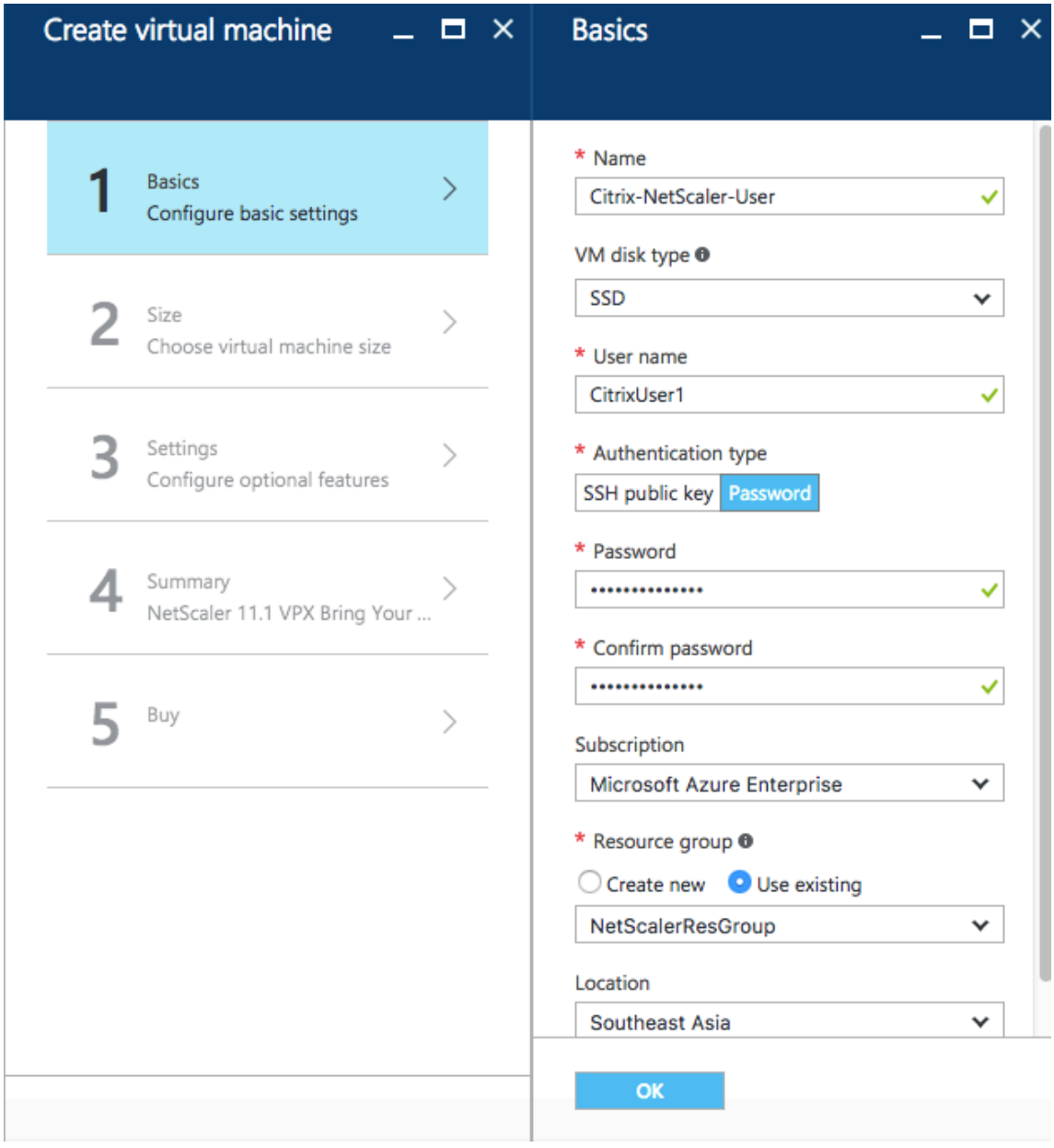
1. Klicken Sie auf **+Neu** > **Netzwerk**.
2. Klicken Sie auf **Alle anzeigen** und klicken Sie im Bereich Netzwerk auf **NetScaler 13.0**.
3. Wählen Sie **NetScaler 13.0 VPX Bring Your Own License** aus der Liste der Softwarepläne aus.

   Um schnell eine Entität im ARM-Portal zu finden, können Sie auch den Namen der Entität in das Azure Marketplace-Suchfeld eingeben und auf <Enter> drücken. Geben Sie NetScaler in das Suchfeld ein, um die NetScaler ADC-Images zu finden.



> **Hinweis**
>
> Stellen Sie sicher, dass Sie das neueste Image auswählen. Ihr NetScaler-Image hat möglicherweise die Versionsnummer im Namen.

4. Wählen Sie auf der Seite **NetScaler VPX Bring Your Own License** aus der Dropdownliste die Option **Resource Manager** aus, und klicken Sie auf **Create**.



5. Geben Sie im Bereich **Virtuelle Maschine erstellen** in jedem Abschnitt die erforderlichen Werte an, um eine virtuelle Maschine zu erstellen. Klicken Sie in jedem Abschnitt auf **OK**, um Ihre Konfiguration zu speichern.

Grundlegend:

- Name — geben Sie einen Namen für die NetScaler VPX-Instanz an
- VM-Festplattentyp — wählen Sie SSD (Standardwert) oder HDD aus dem Drop-down-Menü
- Benutzername und Passwort — Geben Sie einen Benutzernamen und ein Passwort für den Zugriff auf die Ressourcen in der Ressourcengruppe an, die Sie erstellt haben
- Authentifizierungstyp — wählen Sie den öffentlichen SSH-Schlüssel oder das Passwort
- Ressourcengruppe — wählen Sie die von Ihnen erstellte Ressourcengruppe aus der Dropdownliste aus

Sie können hier eine Ressourcengruppe erstellen, Citrix empfiehlt jedoch, eine Ressourcengruppe aus Ressourcengruppen in Azure Resource Manager zu erstellen und die Gruppe dann aus der Dropdownliste auszuwählen.

> **Hinweis**
>
> Geben Sie in einer Azure-Stack-Umgebung zusätzlich zu den grundlegenden Parametern die folgenden Parameter an:
>
> - Azure-Stack-Domäne
> - Azure-Stack-Mandant (optional)
> - Azure-Client (optional)
> - Azure-Clientgeheimnis (optional)

Größe:

Abhängig vom VM-Festplattentyp, SDD oder HDD, den Sie in den Grundeinstellungen ausgewählt haben, werden die Festplattengrößen angezeigt.

- Wählen Sie eine Festplattengröße entsprechend Ihren Anforderungen aus und klicken Sie auf **Auswählen**.

Einstellungen:

- Wählen Sie den Standardfestplattentyp (Standard)
- Speicherkonto — wählen Sie das Speicherkonto aus
- Virtuelles Netzwerk — wählen Sie das virtuelle Netzwerk
- Subnetz — legt die Subnetzadresse fest
- Öffentliche IP-Adresse — wählen Sie die Art der IP-Adresszuweisung aus
- Netzwerksicherheitsgruppe — Wählen Sie die Sicherheitsgruppe aus, die Sie erstellt haben. Stellen Sie sicher, dass Regeln für eingehenden und ausgehenden Datenverkehr in der Sicherheitsgruppe konfiguriert sind.
- Verfügbarkeitsset — wählen Sie das Verfügbarkeitsset aus dem Drop-down-Menüfeld aus

Zusammenfassung:

Die Konfigurationseinstellungen werden überprüft und auf der Übersichtsseite wird das Ergebnis der Überprüfung angezeigt. Schlägt die Überprüfung fehl, wird auf der Übersichtsseite die Ursache des

Fehlers angezeigt. Gehen Sie zurück zum jeweiligen Abschnitt und nehmen Sie ggf. Änderungen vor. Wenn die Überprüfung erfolgreich ist, klicken Sie auf **OK**.

Kaufen:

Lesen Sie die Angebotsdetails und rechtlichen Bedingungen auf der Kaufseite und klicken Sie auf **Kaufen**.

Erstellen Sie für Hochverfügbarkeitsbereitstellungen zwei unabhängige Instanzen von NetScaler VPX in demselben Verfügbarkeitssatz und in derselben Ressourcengruppe, um sie in der aktiven Standby-Konfiguration bereitzustellen.

Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz konfigurieren

May 11, 2023

In diesem Abschnitt wird erläutert, wie Sie eine eigenständige NetScaler VPX-Instanz mit mehreren IP-Adressen im Azure Resource Manager (ARM) konfigurieren. An die VPX-Instanz können eine oder mehrere NICs angeschlossen sein, und jeder NIC können eine oder mehrere statische oder dynamische öffentliche und private IP-Adressen zugewiesen werden. Sie können mehrere IP-Adressen als NSIP, VIP, SNIP usw. zuweisen.

Weitere Informationen finden Sie in der Azure-Dokumentation Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.

Informationen zur Verwendung von PowerShell-Befehlen finden Sie unter Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

Anwendungsfall

In diesem Anwendungsfall wird eine eigenständige NetScaler VPX Appliance mit einer einzelnen Netzwerkkarte konfiguriert, die mit einem virtuellen Netzwerk (VNET) verbunden ist. Die Netzwerkkarte ist mit drei IP-Konfigurationen (ipconfig) verknüpft, wobei jeder Server einen anderen Zweck hat - wie in der Tabelle dargestellt.

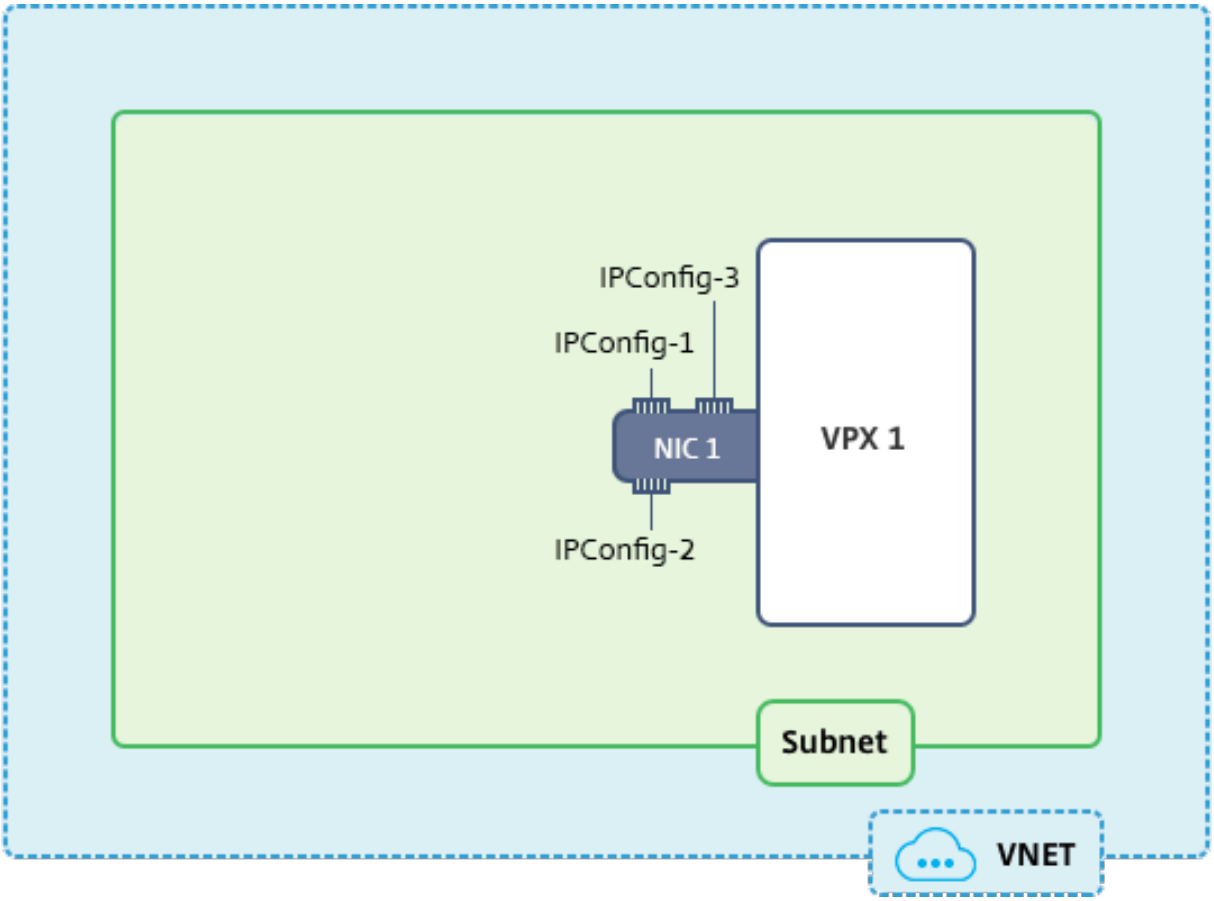
IP-Konfiguration	Verbunden mit	Zweck
ipconfig1	Statische öffentliche IP-Adresse; statische private IP-Adresse	Dient zum Verwalten von Datenverkehr

IP-Konfiguration	Verbunden mit	Zweck
ipconfig2	Statische öffentliche IP-Adresse; statische Privatadresse	Dient dem clientseitigen Datenverkehr
ipconfig3	Statische private IP-Adresse	Kommuniziert mit Back-End-Servern

> **Hinweis**
>
> `IPConfig-3` ist mit keiner öffentlichen IP-Adresse verknüpft.

Diagramm: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.



> **Hinweis**
>
> In einer Multi-Nic, Multi-IP Azure NetScaler VPX-Bereitstellung wird die private IP, die mit der primären (ersten) `IPConfig` der primären (ersten) Netzwerkkarte verknüpft ist, automatisch als

> Verwaltungs-NSIP der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die mit verknüpft sind, `IPConfigs` müssen in der VPX-Instanz als VIP oder SNIP mithilfe des `add ns ip` Befehls entsprechend Ihrer Anforderung hinzugefügt werden.

Voraussetzungen

Bevor Sie beginnen, erstellen Sie eine VPX-Instanz, indem Sie die unter diesem Link angegebenen Schritte ausführen:

Eigenständige NetScaler VPX-Instanz konfigurieren

Für diesen Anwendungsfall wird die NSDoc0330VM VPX-Instanz erstellt.

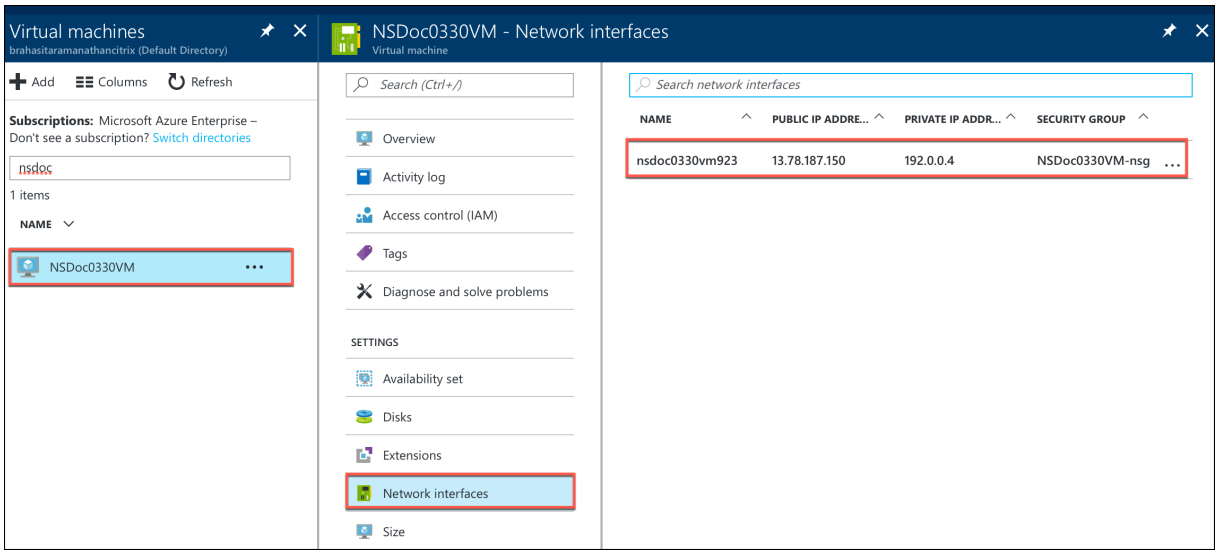
Verfahren zur Konfiguration mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus.

Um mehrere IP-Adressen für eine NetScaler VPX-Appliance im Standalone-Modus zu konfigurieren:

1. Hinzufügen von IP-Adressen zur VM
2. Konfigurieren von NetScaler eigenen IP-Adressen

Schritt 1: Fügen Sie der VM IP-Adressen hinzu

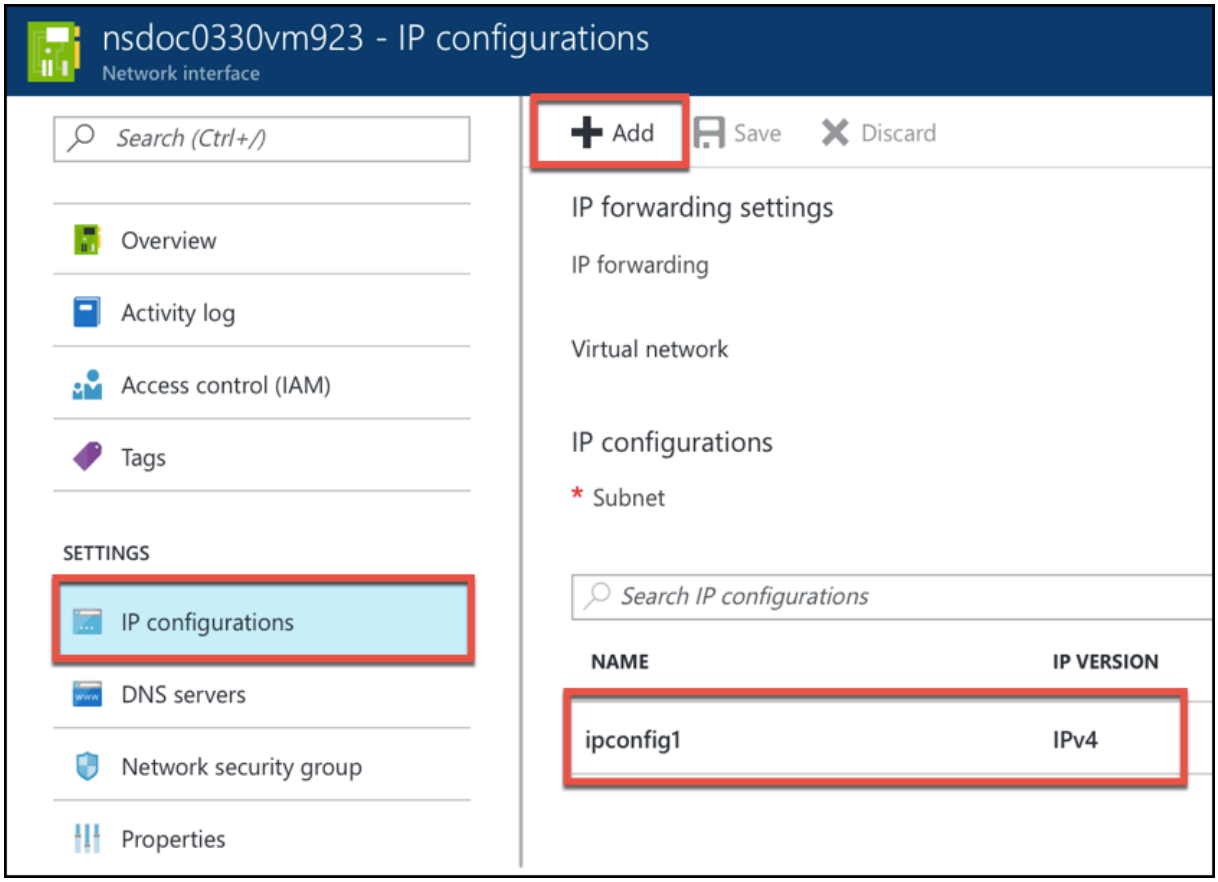
1. Klicken Sie im Portal auf **Weitere Dienste > geben Sie virtuelle Maschinen** in das Filterfeld ein, und klicken Sie dann auf **Virtuelle Maschinen**.
2. Klicken Sie im Blade **Virtuelle Maschinen** auf die VM, zu der Sie IP-Adressen hinzufügen möchten. Klicken Sie auf **Netzwerkschnittstellen** im Blade der virtuellen Maschine, das angezeigt wird, und wählen Sie dann die Netzwerkschnittstelle aus.



Klicken Sie im Blade, das für die ausgewählte NIC angezeigt wird, auf **IP-Konfigurationen**. Die vorhandene IP-Konfiguration, die bei der Erstellung der VM zugewiesen wurde, **ipconfig1**, wird angezeigt.

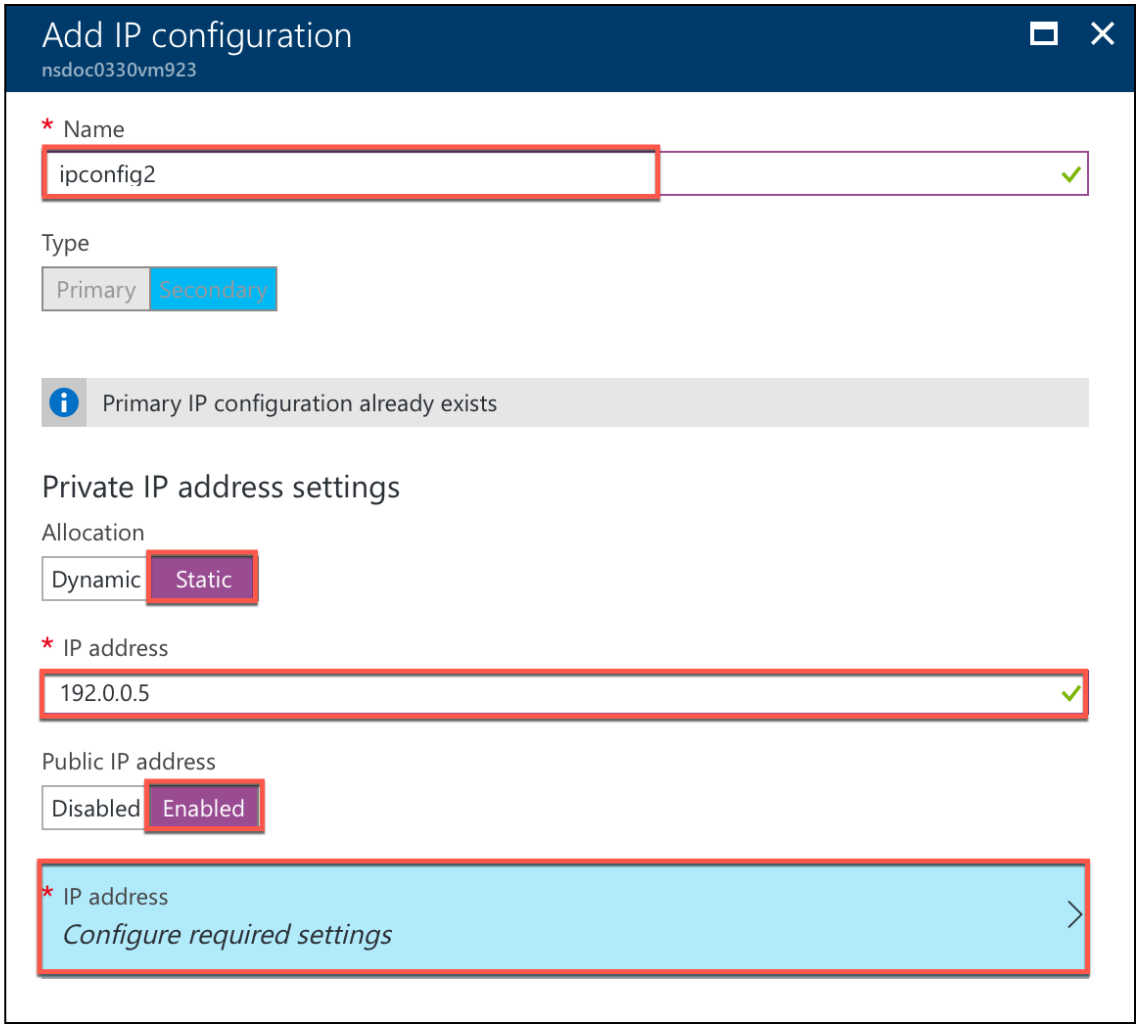
Stellen Sie für diesen Anwendungsfall sicher, dass die IP-Adressen, die mit ipconfig1 verknüpft sind, statisch sind. Als nächstes erstellen Sie zwei weitere IP-Konfigurationen: ipconfig2 (VIP) und ipconfig3 (SNIP).

Um mehr zu erstellen `ipconfigs`, erstellen **Sie Hinzufügen**.



Geben **Sie im Fenster IP-Konfiguration hinzufügen** einen **Namen** ein, geben Sie die Zuweisungsmethode als **Statisch** an, geben Sie eine IP-Adresse ein (192.0.0.5 für diesen Anwendungsfall) und aktivieren Sie die **öffentliche IP-Adresse** .

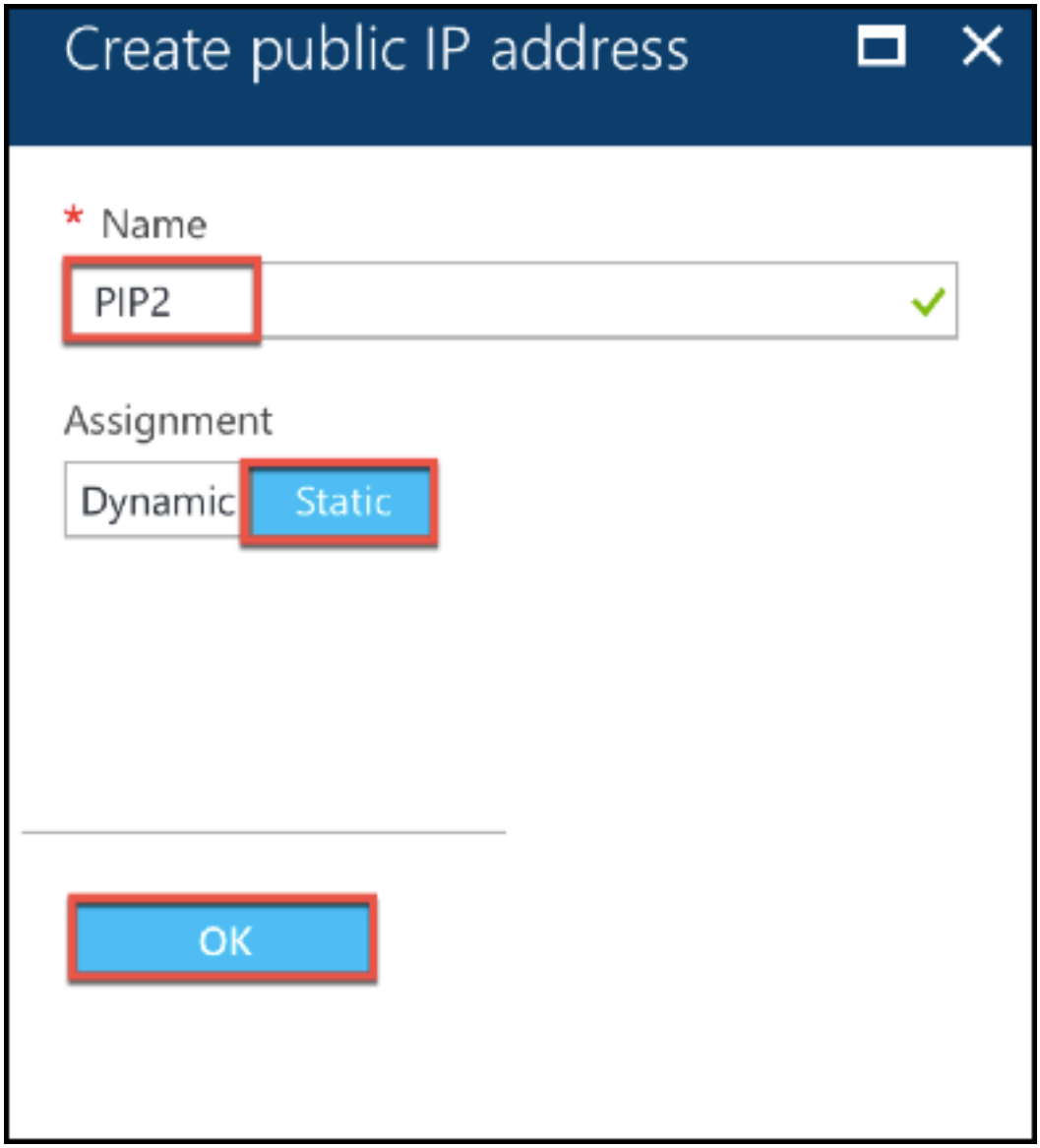
> **Hinweis**
>
> Bevor Sie eine statische private IP-Adresse hinzufügen, überprüfen Sie die Verfügbarkeit der IP-Adresse und stellen Sie sicher, dass die IP-Adresse zu demselben Subnetz gehört, an das die Netzwerkkarte angeschlossen ist.



Klicken Sie als Nächstes auf **Erforderliche Einstellungen konfigurieren**, um eine statische öffentliche IP-Adresse für ipconfig2 zu erstellen.

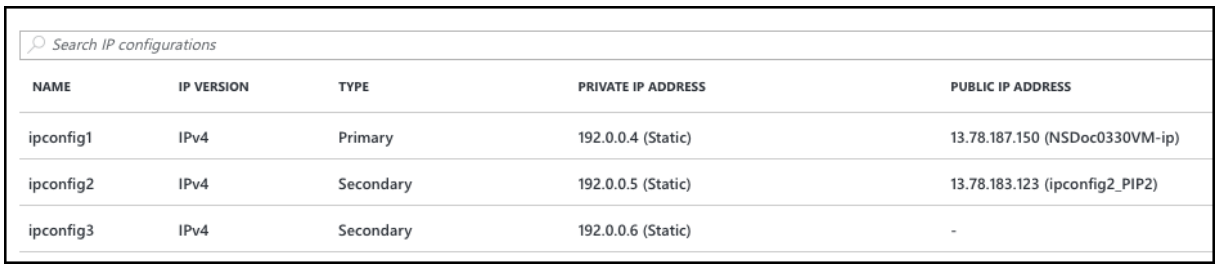
Standardmäßig sind öffentliche IPs dynamisch. Um sicherzustellen, dass die VM immer dieselbe öffentliche IP-Adresse verwendet, erstellen Sie eine statische öffentliche IP-Adresse.

Fügen Sie im Blade Create public ip address einen Namen hinzu und klicken Sie unter Zuweisung auf **Statisch**. Klicken Sie dann auf **OK**.



> **Hinweis**
>
> Selbst wenn Sie die Zuweisungsmethode auf statisch setzen, können Sie die tatsächliche IP-Adresse, die der öffentlichen IP-Ressource zugewiesen ist, nicht angeben. Stattdessen wird es aus einem Pool verfügbarer IP-Adressen an dem Azure-Standort zugewiesen, an dem die Ressource erstellt wurde.

Führen Sie die Schritte aus, um eine weitere IP-Konfiguration für ipconfig3 hinzuzufügen. Öffentliche IP ist nicht obligatorisch.



Schritt 2: Konfigurieren von NetScaler-eigenen IP-Adressen

Konfigurieren Sie die NetScaler-eigenen IP-Adressen mit der GUI oder des Befehls`add ns ip`. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs konfigurieren

May 11, 2023

In einer Microsoft Azure-Bereitstellung wird eine Hochverfügbarkeitskonfiguration von zwei NetScaler VPX-Instanzen mit Azure Load Balancer (ALB) erreicht. Dies wird durch die Konfiguration einer Integritätsprobe auf ALB erreicht, die jede VPX-Instanz überwacht, indem alle 5 Sekunden eine Integritätsprobe an primäre und sekundäre Instanzen gesendet wird.

In diesem Setup reagiert nur der primäre Knoten auf Integritätssonden und der sekundäre nicht. Sobald der Primärserver die Antwort an den Integritätstest sendet, beginnt die ALB den Datenverkehr an die Instanz zu senden. Wenn die primäre Instance zwei aufeinanderfolgende Integritätstests verpasst, leitet ALB den Datenverkehr nicht an diese Instance weiter. Beim Failover reagiert die neue primäre Instanz auf Integritätstests und der ALB leitet den Datenverkehr an ihn weiter. Die standardmäßige VPX-Hochverfügbarkeits-Failover-Zeit beträgt drei Sekunden. Die gesamte Failover-Zeit, die für den Wechsel des Datenverkehrs dauern kann, kann maximal 13 Sekunden betragen.

Sie können ein Paar von NetScaler VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

Die folgenden Optionen sind für eine Bereitstellung mit mehreren NICs mit hoher Verfügbarkeit verfügbar:

- Hohe Verfügbarkeit mit dem Azure-Verfügbarkeitssatz
- Hochverfügbarkeit mit Azure Availability Zones

Weitere Informationen zu Azure Availability Set und Availability Zones finden Sie in der Azure-Dokumentation Verwalten der Verfügbarkeit virtueller Linux-Maschinen.

Hochverfügbarkeit mit Verfügbarkeitssatz

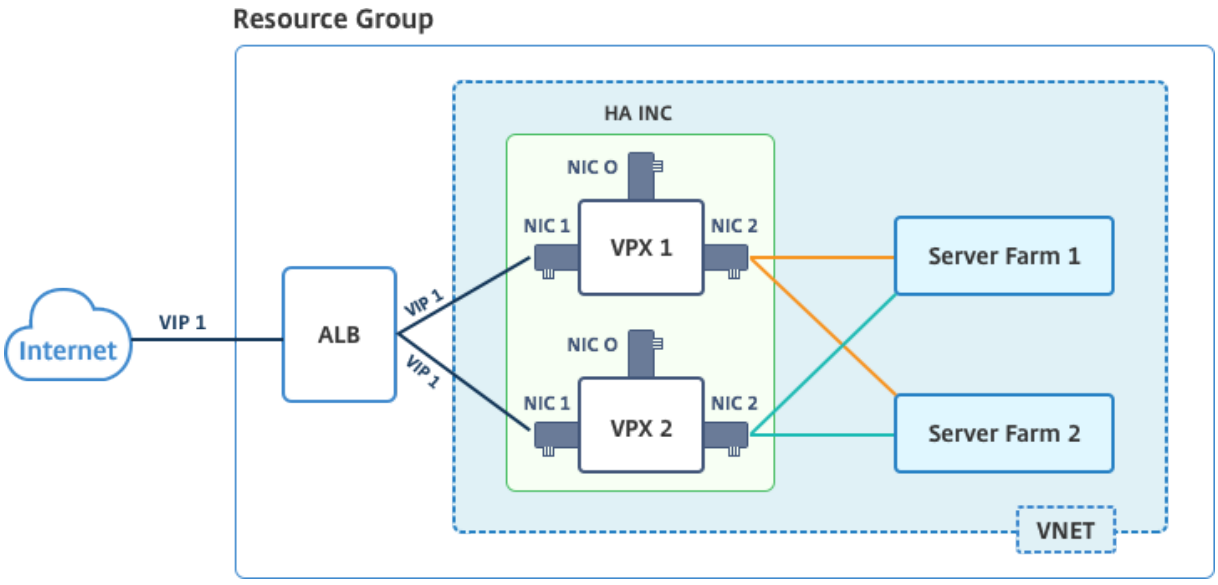
Ein Hochverfügbarkeits-Setup, das ein Verfügbarkeitsset verwendet, muss die folgenden Anforderungen erfüllen:

- Eine HA Independent Network Configuration (INC) Konfiguration
- Der Azure Load Balancer (ALB) im Direct Server Return (DSR) -Modus

Der gesamte Verkehr läuft über den primären Knoten. Der sekundäre Knoten bleibt im Standbymodus, bis der primäre Knoten ausfällt.

> **Hinweis**
>
> Damit eine NetScaler VPX-Hochverfügbarkeitsbereitstellung in der Azure-Cloud funktioniert, benötigen Sie eine Floating Public IP (PIP), die zwischen den beiden VPX-Knoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt dieses schwebende PIP bereit, das im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

Abbildung: Beispiel für eine Bereitstellungsarchitektur mit hoher Verfügbarkeit unter Verwendung von Azure Availability Set



In einer aktiv-passiven Bereitstellung werden die öffentlichen IP-Adressen (PIP) von ALB Frontend als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen unverankert und SNIP-Adressen sind Instanzenpezifisch.

Sie können ein VPX-Paar im aktiv-passiven Hochverfügbarkeitsmodus auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

- **NetScaler VPX-Standardvorlage für hohe Verfügbarkeit**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs NICs zu konfigurieren.
- **Windows PowerShell-Befehle**: Verwenden Sie diese Option, um ein HA-Paar entsprechend Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

In diesem Thema wird beschrieben, wie ein VPX-Paar im aktiv-passiven HA-Setup mithilfe der Citrix Vorlage bereitgestellt wird. Informationen zur Verwendung von PowerShell-Befehlen finden Sie unter Konfigurieren eines HA-Setups mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen.

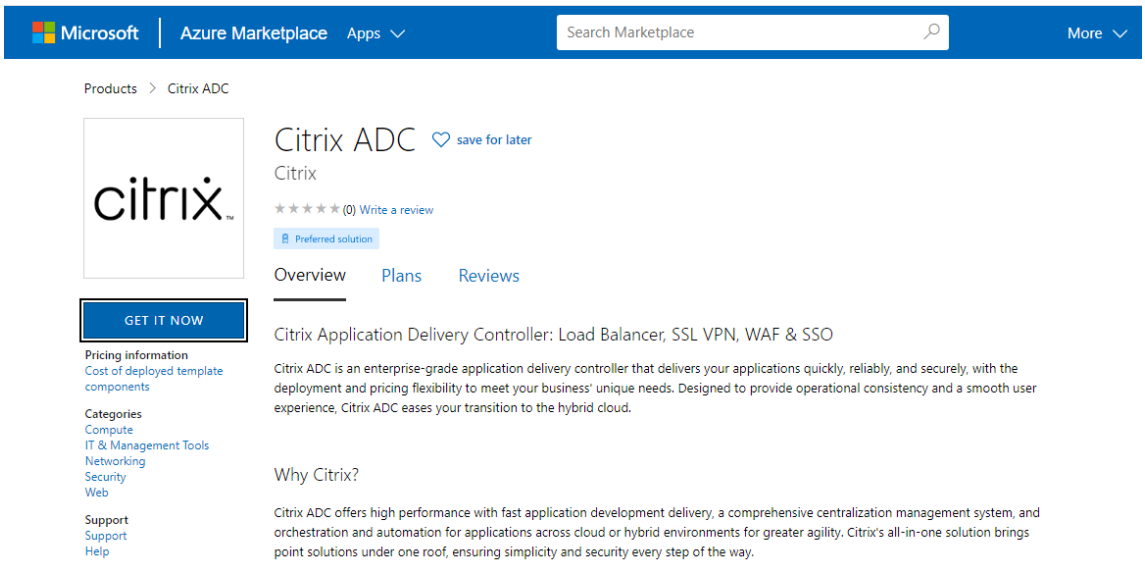
Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage

Mithilfe der Standardvorlage können Sie schnell und effizient ein Paar VPX-Instances im HA-INC-Modus bereitstellen. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze sind für Verwaltungs-, Client- und serverseitigen Datenverkehr, und jedes Subnetz verfügt über zwei Netzwerkkarten für beide VPX-Instanzen.

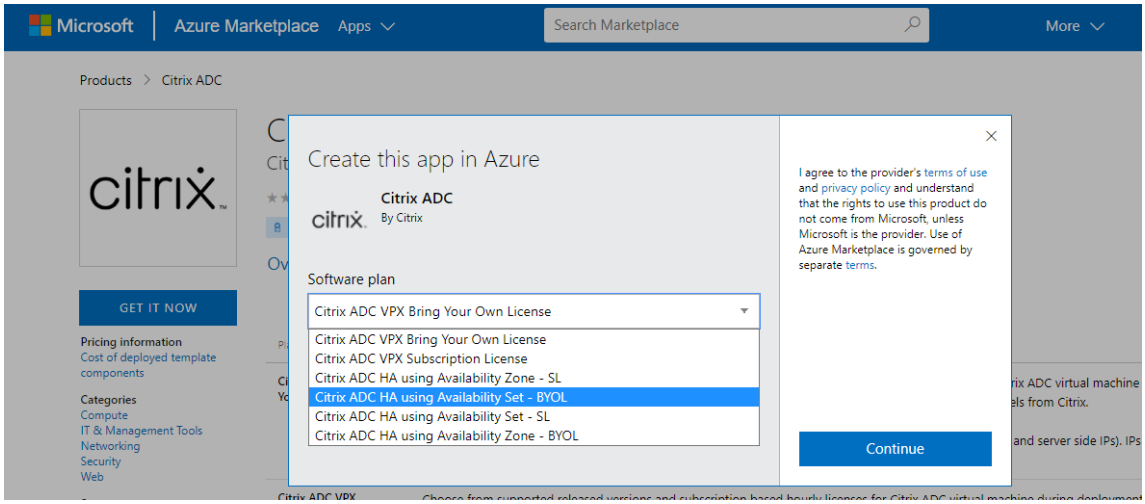
Sie können die NetScaler HA Pair Vorlage im Azure Marketplaceabrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein VPX-Paar mit hoher Verfügbarkeit bereitzustellen, indem Sie Azure-Verfügbarkeitssätze verwenden.

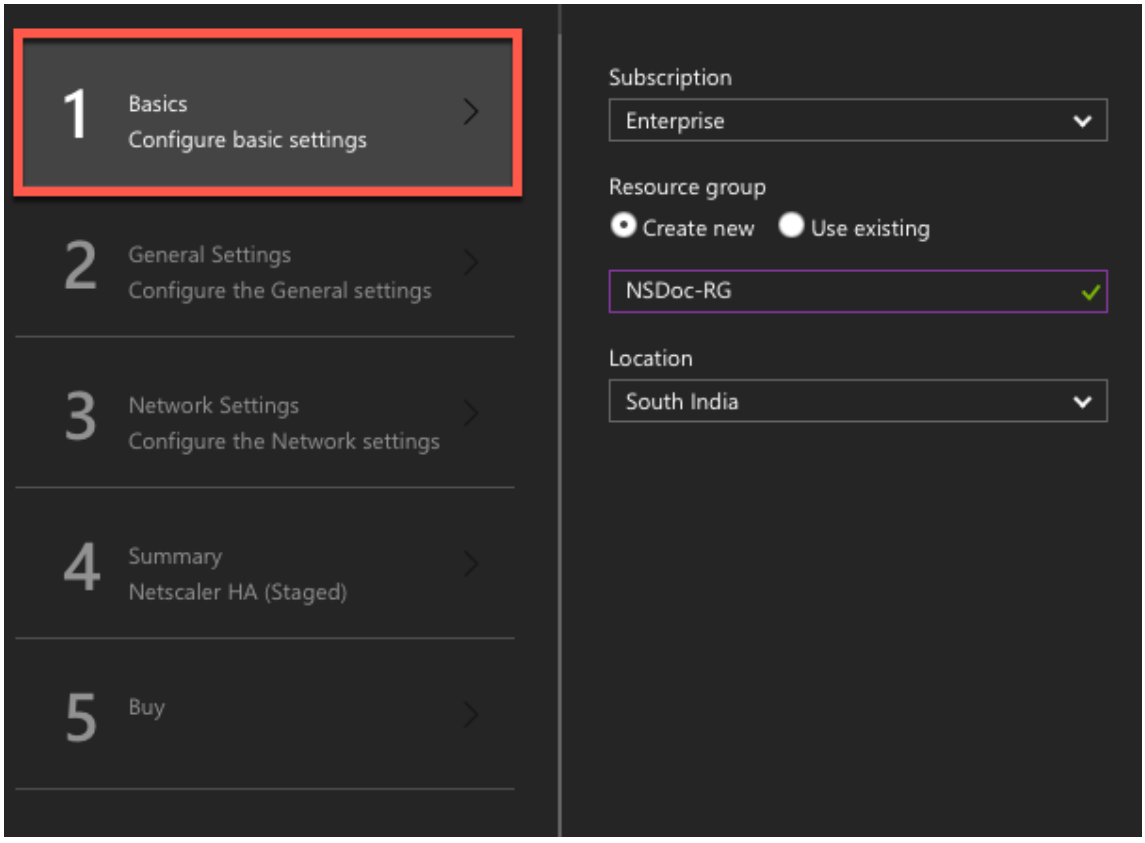
1. Suchen Sie in Azure Marketplace nach **NetScaler**.



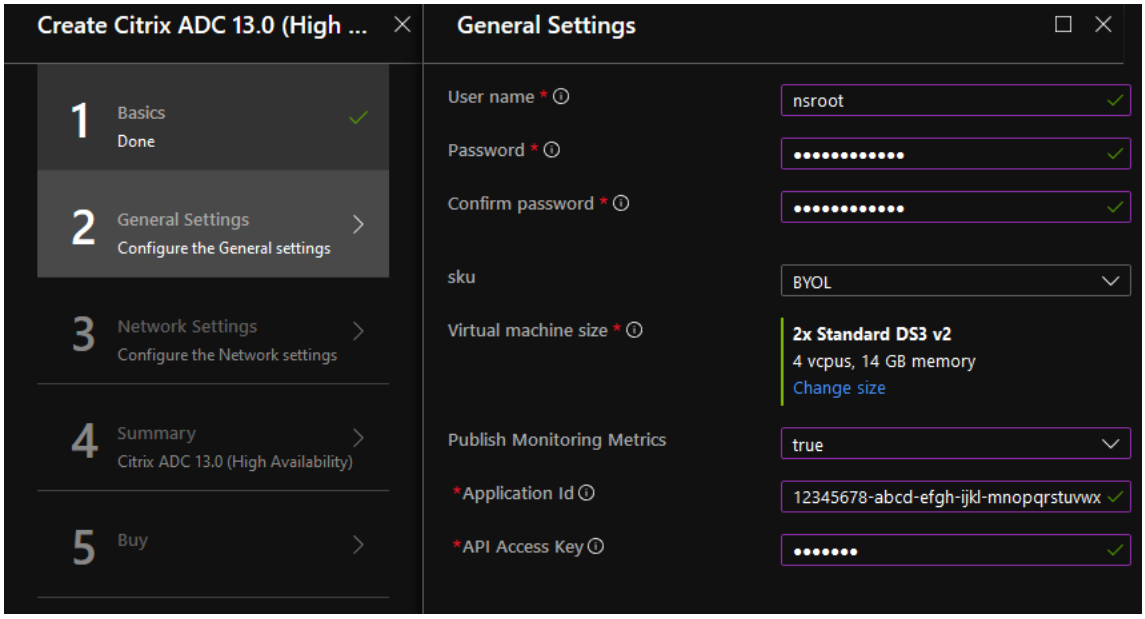
2. Klicken Sie auf **JETZT HOLEN**.
3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.



4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe und wählen Sie **OK**.

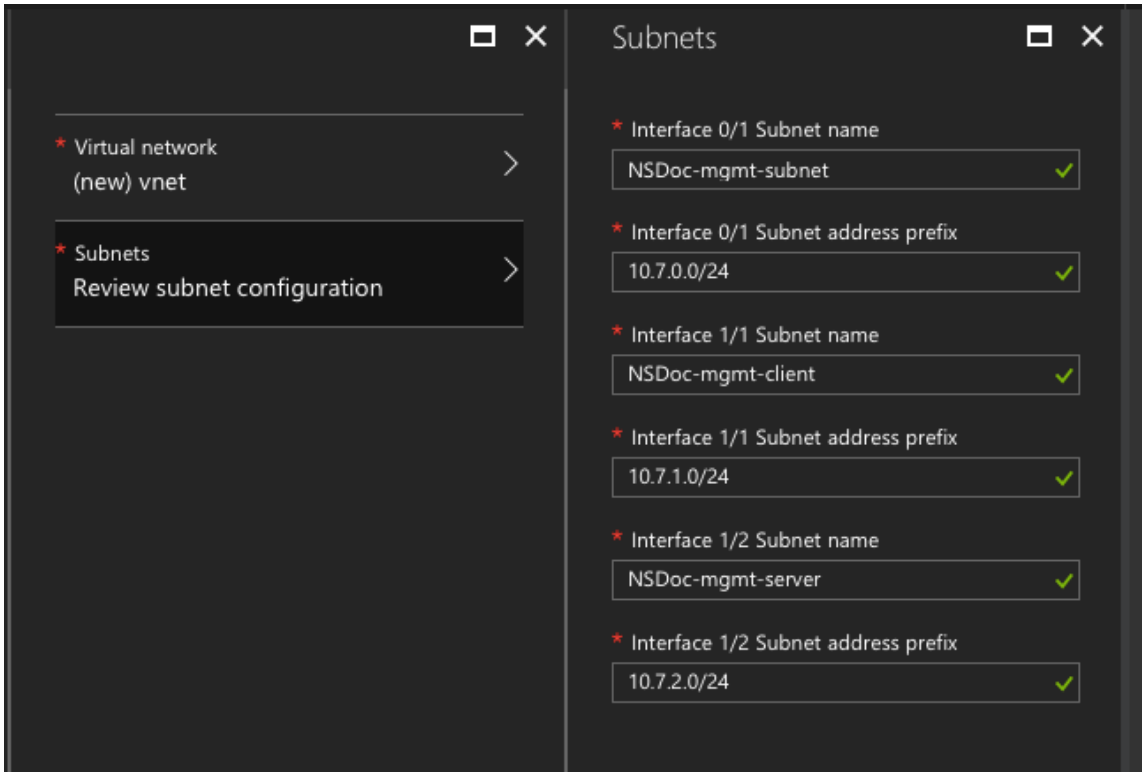


5. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein und wählen Sie **OK**.



> Hinweis:
>
> Die Option „ **Monitoring-Metriken veröffentlichen** “ ist standardmäßig auf **„False“**gesetzt. Wenn Sie diese Option aktivieren möchten, wählen Sie **True**aus.
> Erstellen Sie eine Azure Active Directory (ADD) -Anwendung und Dienstprinzipal, die auf Ressourcen zugreifen können. Weisen Sie der neu erstellten AAD-Anwendung die Rolle der Mitwirkenden zu. Weitere Informationen finden Sie unter Verwenden des Portals zum Erstellen einer Azure Active Directory-Anwendung und eines Dienstprinzipals, die auf Ressourcen zugreifen können.

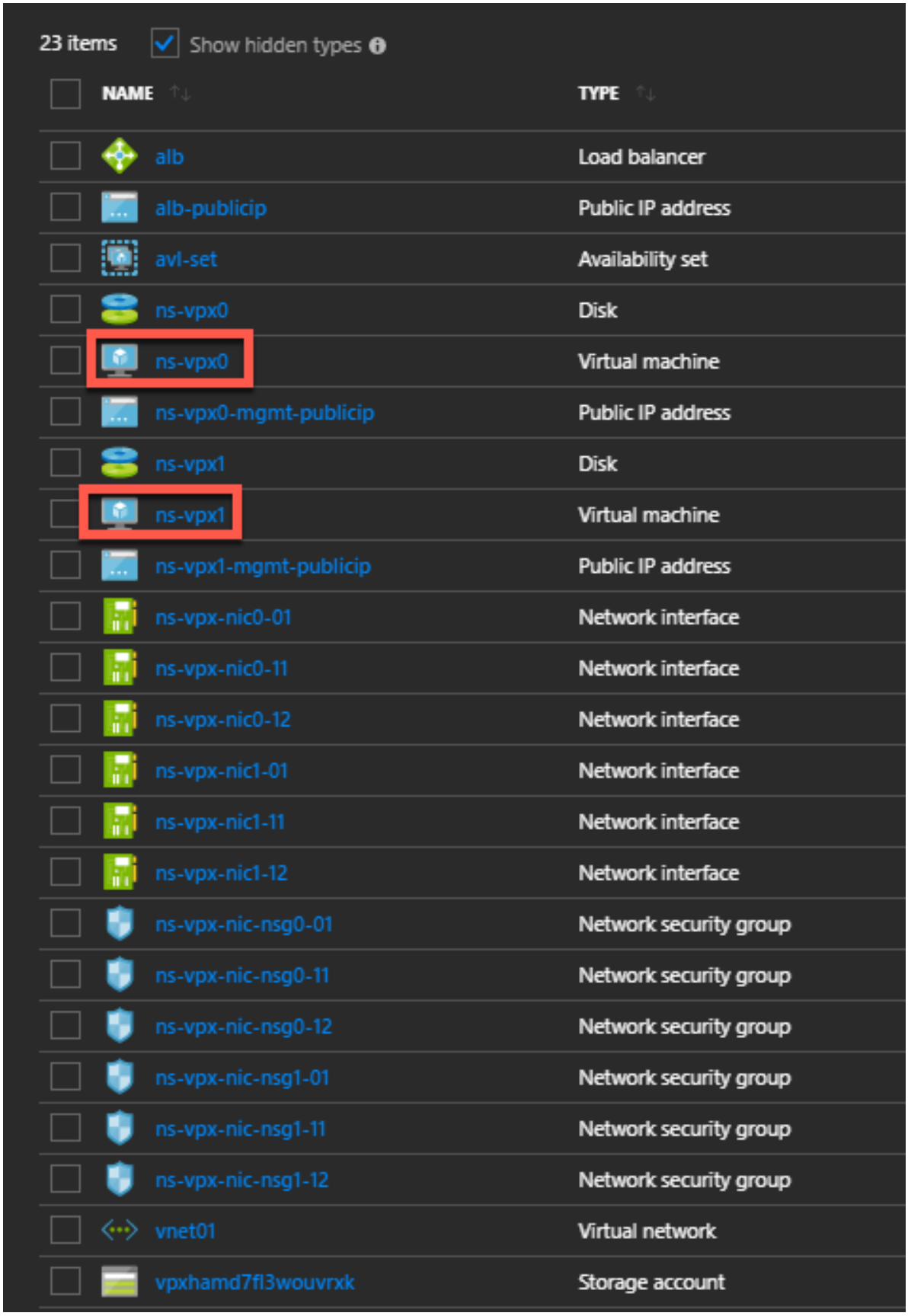
6. Die Seite **“Netzwerkeinstellungen** “ wird angezeigt. Überprüfen Sie die VNet- und Subnetz-Konfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK**aus.



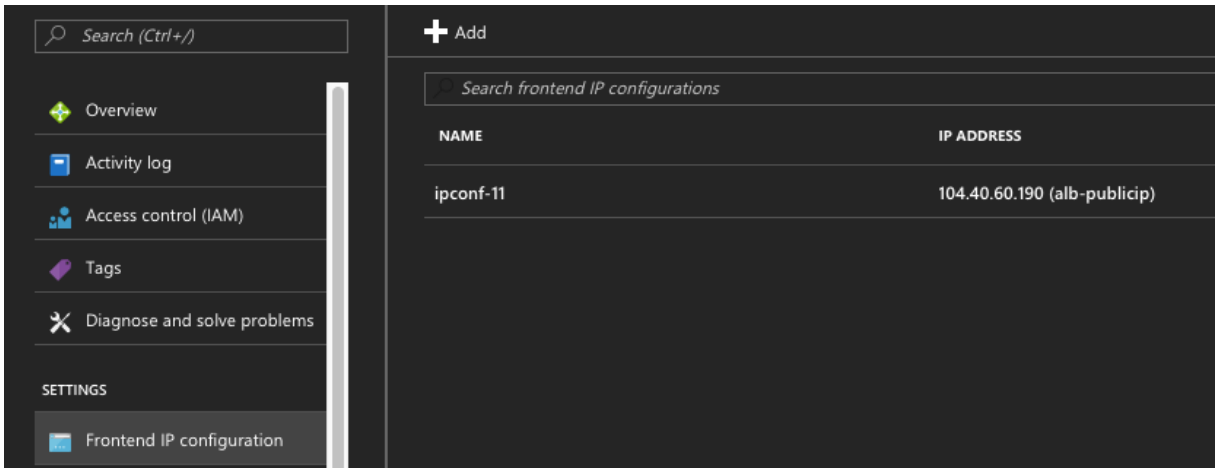
7. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie sie entsprechend. Wählen Sie zur Bestätigung **OK** .
8. Die Seite „ **Kaufen** “ wird angezeigt. Wählen Sie **Kaufen** aus, um die Bereitstellung abzuschließen.

Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die **Ressourcengruppe** im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritäts-Sonden anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.



Als Nächstes müssen Sie den virtuellen Lastenausgleichsserver mit der **öffentlichen IP-Adresse (PIP) des ALB mit der Frontend-IP-Adresse (PIP)**auf dem primären Knoten konfigurieren. Um das ALB PIP zu finden, wählen Sie ALB > **Frontend-IP-Konfiguration**.



Weitere Informationen zur Konfiguration des virtuellen Load-Balancing-Servers finden Sie im Abschnitt **Ressourcen** .

Ressourcen:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Konfiguration virtueller Server:

- Konfigurieren von Knoten mit hoher Verfügbarkeit in verschiedenen Subnetzen
- Einrichten des grundlegenden Lastenausgleichs

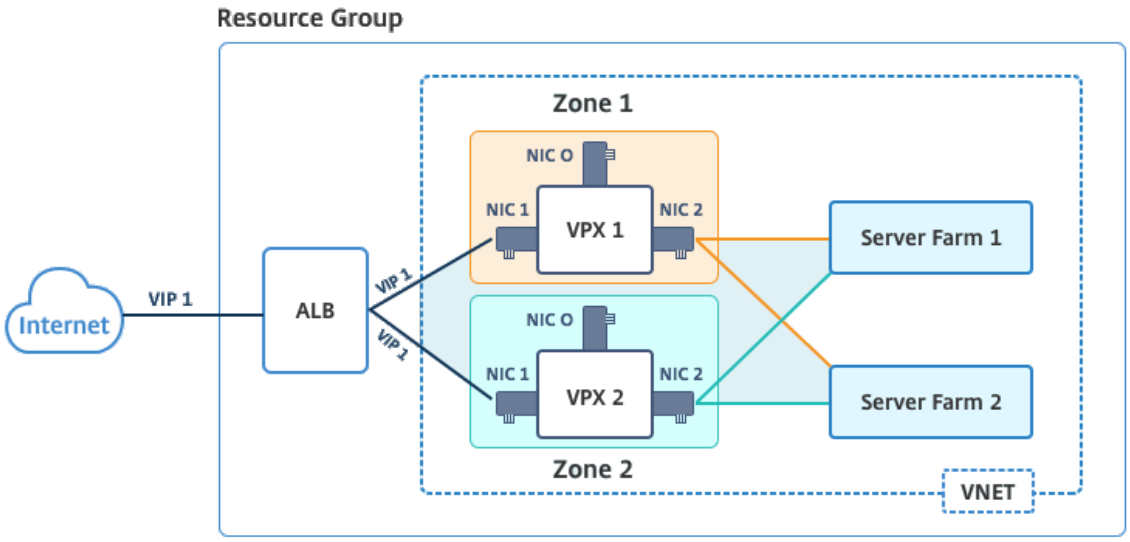
Verwandte Ressourcen:

- Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs über PowerShell-Befehle konfigurieren
- Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

Hohe Verfügbarkeit mithilfe von Availability Zones

Azure Availability Zones sind fehlerisolierte Standorte in einer Azure-Region, die redundante Stromversorgung, Kühlung und Netzwerke bieten und die Ausfallsicherheit erhöhen. Nur bestimmte Azure-Regionen unterstützen Availability Zones. Weitere Informationen finden Sie in der Azure-Dokumentation [Was sind Availability Zones in Azure.

Diagramm: Beispiel für eine Hochverfügbarkeitsbereitstellungsarchitektur mit Azure Availability Zones



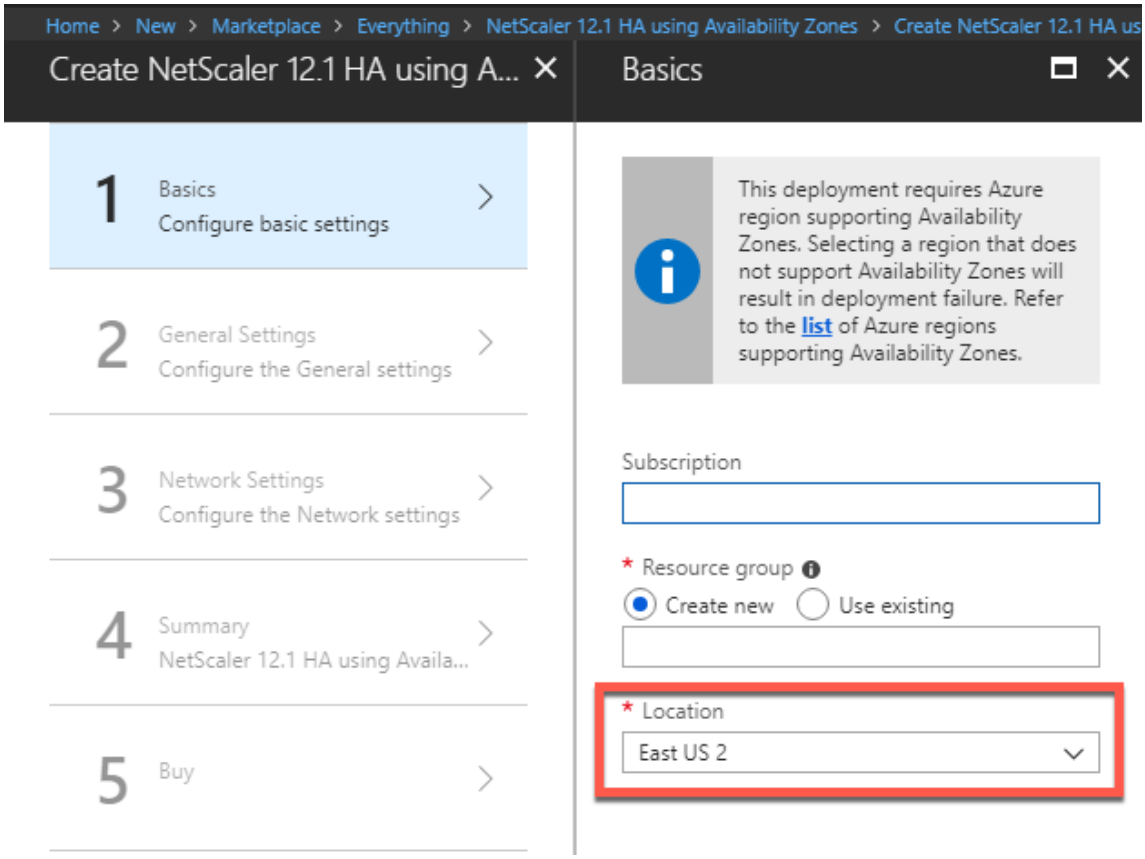
Sie können ein VPX-Paar im Hochverfügbarkeitsmodus bereitstellen, indem Sie die Vorlage „NetScaler 13.0 HA using Availability Zones“ verwenden, die im Azure Marketplace verfügbar ist.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein hochverfügbarkeitsfähiges VPX-Paar mithilfe von Azure Availability Zones bereitzustellen.

1. Wählen Sie in Azure Marketplace die Citrix Lösungsvorlage aus, und starten Sie sie.

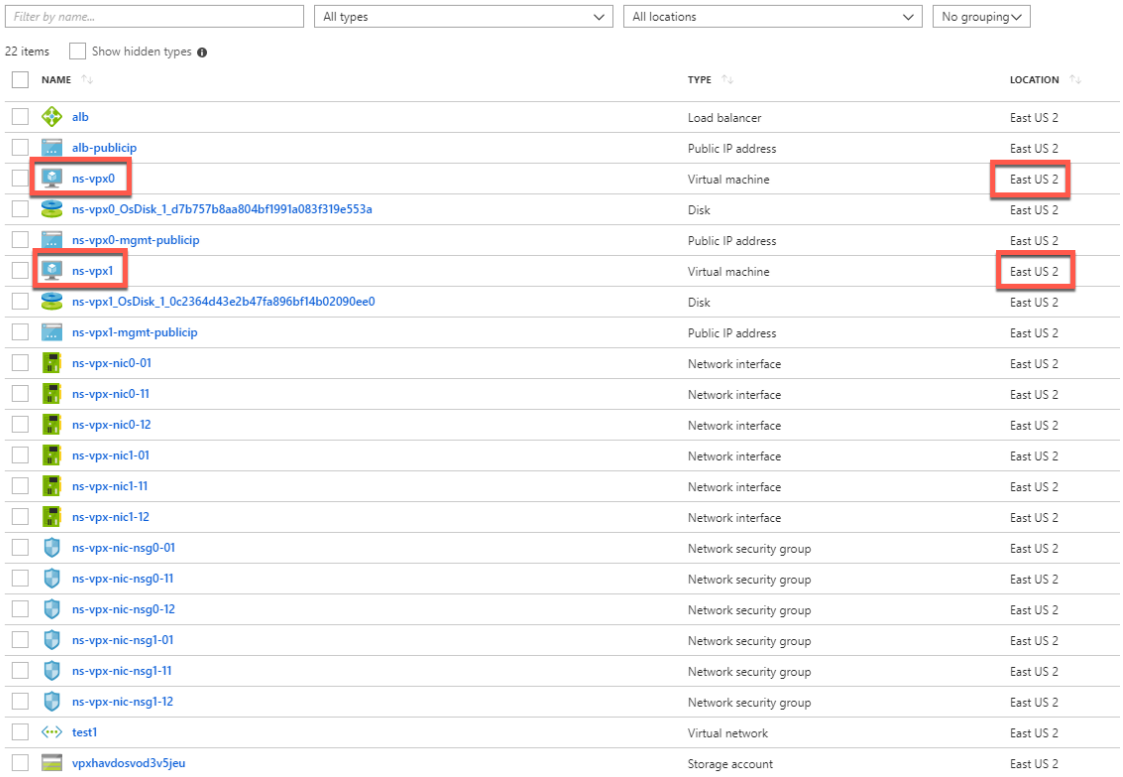
2. Stellen Sie sicher, dass der Bereitstellungstyp Resource Manager ist, und wählen Sie **Erstellen**aus.
3. Die Seite **Grundlagen** wird angezeigt. Geben Sie die Details ein und klicken Sie auf **OK**.

> Hinweis: Stellen Sie sicher, dass Sie eine Azure-Region auswählen, die Availability Zones unterstützt. Weitere Informationen zu Regionen, die Availability Zones unterstützen, finden Sie in der Azure-Dokumentation Was sind Availability Zones in Azure?



4. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein und wählen Sie **OK**.
5. Die Seite mit den **Netzwerkeinstellungen** wird angezeigt. Überprüfen Sie die VNet- und Subnetz-Konfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK**aus.
6. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie sie entsprechend. Wählen Sie zur Bestätigung **OK** .
7. Die Seite „ **Kaufen** “ wird angezeigt. Wählen Sie **Kaufen** aus, um die Bereitstellung abzuschließen.

   Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die **Ressourcengruppe** aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools, Integritätstests usw. im Azure-Portal anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt. Sie können den Standort auch in der Spalte **Standort** sehen.



Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Überwachen Sie Ihre Instanz mit Metriken in Azure Monitor

Sie können Metriken auf der Azure Monitor-Datenplattform verwenden, um eine Reihe von NetScaler VPX-Ressourcen wie CPU, Speicherauslastung und Durchsatz zu überwachen. Der Metrics-Dienst überwacht NetScaler VPX-Ressourcen, die auf Azure ausgeführt werden, in Echtzeit. Sie können den **Metrics Explorer** verwenden, um auf die gesammelten Daten zuzugreifen. Weitere Informationen finden Sie unter Übersicht über Azure Monitor-Metriken.

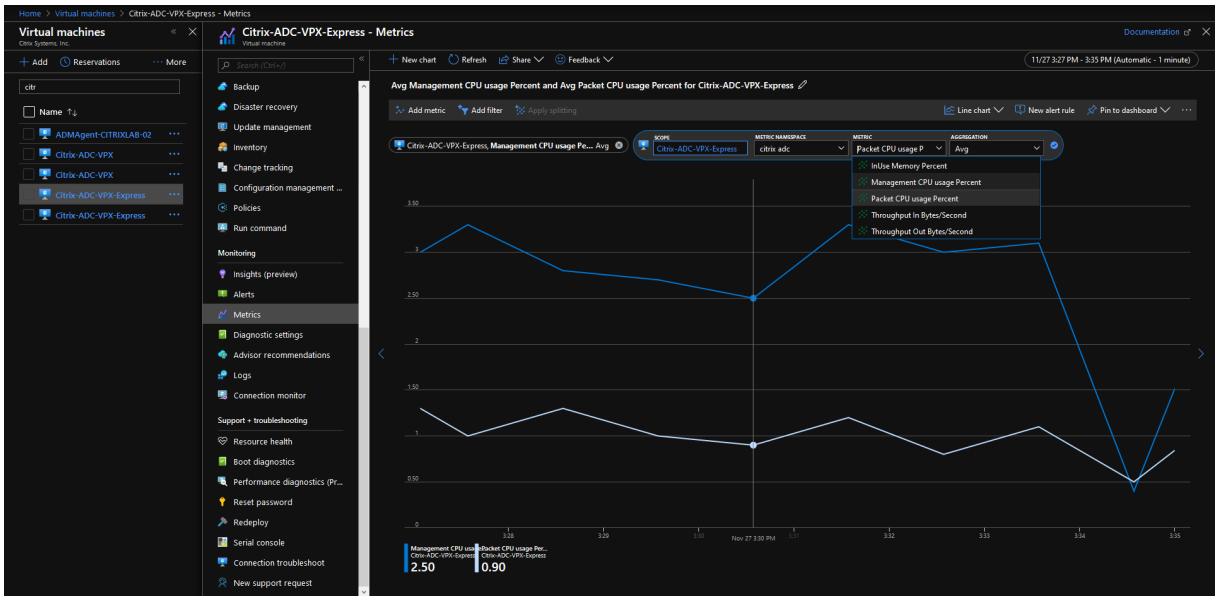
Wichtige Hinweise

- Wenn Sie mithilfe des Azure Marketplace-Angebots eine NetScaler VPX-Instanz in Azure bereitstellen, ist der Metrics-Dienst standardmäßig deaktiviert.
- Der Metrics-Dienst wird in Azure CLI nicht unterstützt.
- Metriken sind für CPU (Verwaltung und Paket-CPU-Auslastung), Arbeitsspeicher und Durchsatz (eingehend und ausgehend) verfügbar.

So zeigen Sie Metriken im Azure-Monitor an

Gehen Sie folgendermaßen vor, um Metriken im Azure-Monitor für Ihre Instanz anzuzeigen:

1. Melden Sie sich bei **Azure Portal > Virtuelle Maschinen**an.
2. Wählen Sie die virtuelle Maschine aus, die der primäre Knoten ist.
3. Klicken Sie im Abschnitt **Überwachung** auf **Metriken**.
4. Klicken Sie im Dropdownmenü **Metric Namespace** auf **NetScaler**.
5. Klicken Sie im Dropdownmenü **Alle Metrikenin Metriken** auf die Metriken, die Sie anzeigen möchten.
6. Klicken Sie auf **Metrik hinzufügen**, um eine weitere Metrik im selben Diagramm anzuzeigen. Verwenden Sie die Diagrammoptionen, um Ihr Diagramm anzupassen.



Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs über PowerShell-Befehle konfigurieren

May 11, 2023

Sie können ein Paar von NetScaler VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

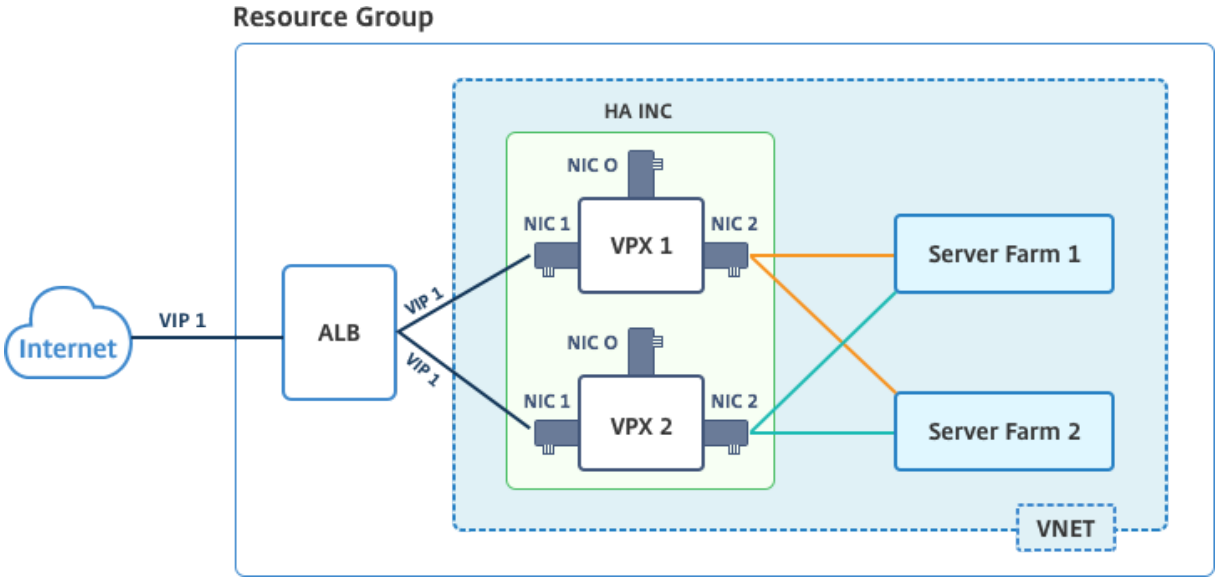
Eine Aktiv-Passiv-Bereitstellung erfordert:

- Eine HA Independent Network Configuration (INC) Konfiguration
- Der Azure Load Balancer (ALB) im Direct Server Return (DSR) -Modus

Der gesamte Verkehr läuft über den primären Knoten. Der sekundäre Knoten bleibt im Standbymodus, bis der primäre Knoten ausfällt.

> **Hinweis**
>
> Damit eine NetScaler VPX Hochverfügbarkeitsbereitstellung in einer Azure-Cloud funktioniert, benötigen Sie eine Floating Public IP (PIP), die zwischen den beiden Hochverfügbarkeitsknoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt dieses schwebende PIP bereit, das im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

Diagramm: Beispiel einer aktiv-passiven Bereitstellungsarchitektur



In einer aktiven und passiven Bereitstellung werden die ALB Floating Public IP (PIP) Adressen als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen unverankert und SNIP-Adressen sind Instanzenpezifisch.

ALB überwacht jede VPX-Instanz, indem es alle 5 Sekunden den Integritäts-Sonde sendet, und leitet den Datenverkehr nur an diese Instanz um, die die Reaktion der Integritätssonden in regelmäßigen Intervallen sendet. In einem HA-Setup reagiert der primäre Knoten auf Gesundheitssonden und sekundäre nicht. Wenn die primären Instanzen zwei aufeinanderfolgende Gesundheitssonden verpassen, leitet ALB den Datenverkehr nicht zu dieser Instanz um. Beim Failover reagiert die neue primäre Instanz auf Integritätstests und der ALB leitet den Datenverkehr an ihn weiter. Die standardmäßige VPX-Hochverfügbarkeits-Failover-Zeit beträgt drei Sekunden. Die gesamte Failover-Zeit, die für den Traffic Switching in Anspruch nehmen kann, kann maximal 13 Sekunden betragen.

Sie können ein VPX-Paar in einem aktiv/passiven HA-Setup auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

- **NetScaler VPX Standard-Vorlage für hohe Verfügbarkeit**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs NICs zu konfigurieren.

- **Windows PowerShell-Befehle**: Verwenden Sie diese Option, um ein HA-Paar entsprechend Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

In diesem Thema wird beschrieben, wie ein VPX-Paar in aktiv-passiven HA-Setup mithilfe von PowerShell Befehlen bereitgestellt wird. Informationen zur Verwendung der NetScaler VPX Standard HA-Vorlage finden Sie unter Konfigurieren eines HA-Setups mit mehreren IP-Adressen und NICs.

Konfigurieren Sie HA-INC-Knoten mit PowerShell-Befehlen

Szenario: HA-INC PowerShell Bereitstellung

In diesem Szenario stellen Sie ein NetScaler VPX-Paar bereit, indem Sie die in der Tabelle angegebene Topologie verwenden. Jede VPX-Instanz enthält drei NICs, wobei jede NIC in einem anderen Subnetz bereitgestellt wird. Jeder NIC ist eine IP-Konfiguration zugewiesen.

ALB	VPX1	VPX2
ALB ist mit öffentlicher IP 3 (pip3) verknüpft	Die Management-IP ist mit ipConfig1 konfiguriert, was eine öffentliche IP (pip1) und eine private IP (12.5.2.24) beinhaltet; nic1; Mgmtsubnet=12.5.2.0/24	Die Management-IP ist mit IPConfig5 konfiguriert, was eine öffentliche IP (pip3) und eine private IP (12.5.2.26) beinhaltet; nic4; Mgmtsubnet=12.5.2.0/24
LB-Regeln und der konfigurierte Port sind HTTP (80), SSL (443), Health Probe (9000)	Die clientseitige IP wird mit IPConfig3 konfiguriert, was eine private IP beinhaltet (12.5.1.27); nic2; FrontendSubT=12.5.1.0/24	Die clientseitige IP wird mit IPConfig7 konfiguriert, was eine private IP beinhaltet (12.5.1.28); nic5; FrontendSubT=12.5.1.0/24
-	Die serverseitige IP wird mit IPConfig4 konfiguriert, was eine private IP beinhaltet (12.5.3.24); nic3; BackendSubnet=12.5.3.0/24	Die serverseitige IP wird mit IPConfig8 konfiguriert, was eine private IP beinhaltet (12.5.3.28); nic6; BackendSubnet=12.5.3.0/24
-	Regeln und Ports für NSG sind SSH (22), HTTP (80), HTTPS (443)	-

Parameter-Einstellungen

Die folgenden Parametereinstellungen werden in diesem Szenario verwendet.

$locName= „Südostasien“

$rgName = „Mehrstufiges Multi-RG“

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = „Azure-MultiIP-Alben-VNET“

$vNetAddressRange= „12.5.0.0/16”

$frontendSubnetName = „Frontend-Subnetz“

$frontendSubnetRange= „12.5.1.0/24”

$mgmtSubnetName = „MGMT-Subnetz“

$mgmtSubnetRange= „12.5.2.0/24”

$backendSubnetName = „BackendSubnetz“

$backendSubnetRange = „12.5.3.0/24”

$prmStorageAccountName = „multiipmultinicbstorage“

$avSetName = „Mehrere AVSets“

$vmSize= “Standard_DS4_V2”

$Publisher = “Citrix”

$offer = “netscalervpx-120”

$sku = „netscalerbyl“

$version=”latest”

$pubIPName1=”VPX1MGMT”

$pubIPName2=”VPX2MGMT”

$pubIPName3=”ALBPIP”

$domName1=”vpx1dns”

$domName2=”vpx2dns”

$domName3=”vpxalbdns”

$vmNamePrefix=”vpxMultiIPAlb“

$osDiskSuffix1=”osmultiipalbdiskdb1”

$osDiskSuffix2=”osmultiipalbdiskdb2”

$lbName = „Mehrere IPAlb“

$frontendConfigName1 = „Frontend-IP“

$backendPoolName1 = „BackendpoolHTTP“

$lbRuleName1 = „LbRuleHttp“

$healthProbename = „HealthProbe“

$nsgName=”NSG-MultiIP-Alb“

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

Führen Sie die folgenden Schritte mithilfe von PowerShell-Befehlen durch, um die Bereitstellung abzuschließen:

1. Erstellen Sie eine Ressourcengruppe, ein Speicherkonto und einen Verfügbarkeitssatz
2. Erstellen Sie eine Netzwerksicherheitsgruppe und fügen Sie Regeln hinzu
3. Erstellen Sie ein virtuelles Netzwerk und drei Subnetze
4. Öffentliche IP-Adressen erstellen
5. IP-Konfigurationen für VPX1 erstellen
6. IP-Konfigurationen für VPX2 erstellen
7. Netzwerkkarten für VPX1 erstellen
8. Netzwerkkarten für VPX2 erstellen
9. VPX1 erstellen
10. VPX2 erstellen
11. ALB erstellen

Erstellen Sie eine Ressourcengruppe, ein Speicherkonto und ein Verfügbarkeitsset.

```
1 New-AzureRmResourceGroup -Name $rgName -Location $locName
2
3
4 $prmStorageAccount=New-AzureRMStorageAccount -Name
     $prmStorageAccountName -ResourceGroupName $rgName -Type Standard_LRS
      -Location $locName
5
6
```



```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $rgName -Location $locName
```

Erstellen Sie eine Netzwerksicherheitsgruppe und fügen Sie Regeln hinzu.

```
$rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
    Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 101


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 80


$rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
    Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 110


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 443


$rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
    Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 120


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 22


$nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
    Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

Erstellen Sie ein virtuelles Netzwerk und drei Subnetze.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
    parameter value should be as per your requirement)


$mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $mgmtSubnetName
     -AddressPrefix $mgmtSubnetRange

```



```
6
7  $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       $backEndSubnetName -AddressPrefix $backEndSubnetRange
8
9
10 $vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
       $rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
       $frontendSubnet,$backendSubnet, $mgmtSubnet
11
12
13 $subnetName ="frontEndSubnet"
14
15
16 $subnet1=$vnet.Subnets|?{
17  $_.Name -eq $subnetName }
18
19
20
21 $subnetName="backEndSubnet"
22
23
24 $subnet2=$vnet.Subnets|?{
25  $_.Name -eq $subnetName }
26
27
28
29 $subnetName="mgmtSubnet"
30
31
32 $subnet3=$vnet.Subnets|?{
33  $_.Name -eq $subnetName }
```

Erstellen Sie öffentliche IP-Adressen.

```
1  $pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
       $rgName -DomainNameLabel $domName1 -Location $locName -
       AllocationMethod Dynamic
2
3  $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
       $rgName -DomainNameLabel $domName2 -Location $locName -
       AllocationMethod Dynamic
4
5  $pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
       $rgName -DomainNameLabel $domName3 -Location $locName -
       AllocationMethod Dynamic
```


Erstellen Sie IP-Konfigurationen für VPX1.

```
$IpConfigName1 = "IPConfig1"


$IPAddress = "12.5.2.24"


$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip1
    -Primary


$IPConfigName3="IPConfig-3"


$IPAddress="12.5.1.27"


$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName4 = "IPConfig-4"


$IPAddress = "12.5.3.24"


$IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Erstellen Sie IP-Konfigurationen für VPX2.

```
$IpConfigName5 = "IPConfig5"


$IPAddress="12.5.2.26"


$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip2
    -Primary


```



```
$IPConfigName7="IPConfig-7"


$IPAddress="12.5.1.28"


$IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName8="IPConfig-8"


$IPAddress="12.5.3.28"


$IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Erstellen Sie Netzwerkkarten für VPX1.

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig1 -
    NetworkSecurityGroupId $nsg.Id


$nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig3 -
    NetworkSecurityGroupId $nsg.Id


$nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig4 -
    NetworkSecurityGroupId $nsg.Id
```

Erstellen Sie Netzwerkkarten für VPX2.

```
$nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig5 -
    NetworkSecurityGroupId $nsg.Id


$nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig7 -
    NetworkSecurityGroupId $nsg.Id
```



```
5
6
7 $nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig8 -
      NetworkSecurityGroupId $nsg.Id
```

Erstellen Sie VPX1.

Dieser Schritt umfasst die folgenden Teilschritte:

- VM-Konfigurationsobjekt erstellen
- Anmeldeinformationen, Betriebssystem und Image festlegen
- Netzwerkkarten hinzufügen
- Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

```
1  $suffixNumber = 1
2
3  $vmName=$vmNamePrefix + $suffixNumber
4
5  $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avSet.Id
6
7  $cred=Get-Credential -Message "Type the name and password for VPX
        login."
8
9  $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
       ComputerName $vmName -Credential $cred
10
11 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
       $publisher -Offer $offer -Skus $sku -Version $version
12
13 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.
       Id -Primary
14
15 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.
       Id
16
17 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.
       Id
18
19 $osDiskName=$vmName + "-" + $osDiskSuffix1
20
21 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "
       vhds/" + $osDiskName + ".vhd"
```



```
22
23  $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -
        VhdUri $osVhdUri -CreateOption fromImage
24
25  Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product
        $offer -Name $sku
26
27  New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
        $locName
```

Erstellen Sie VPX2.

```
1  ```
2  $suffixNumber=2
3
4
5  $vmName=$vmNamePrefix + $suffixNumber
6
7
8  $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avSet.Id
9
10
11 $cred=Get-Credential -Message "Type the name and password for VPX login
       ."
12
13
14 $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
       ComputerName $vmName -Credential $cred
15
16
17 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
       $publisher -Offer $offer -Skus $sku -Version $version
18
19
20 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
       Primary
21
22
23 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
24
25
26 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
27
28
```



```
$osDiskName=$vmName + "-" + $osDiskSuffix2


$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
    + $osDiskName + ".vhd"


$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
   $osVhdUri -CreateOption fromImage


Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
   Name $sku


New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
   $locName
<!--NeedCopy--> ```
```

Geben Sie die folgenden Befehle ein, um private und öffentliche IP-Adressen anzuzeigen, die den Netzwerkkarten zugewiesen sind:

```
```
$nic1.IPConfig

$nic2.IPConfig

$nic3.IPConfig

$nic4.IPConfig

$nic5.IPConfig

$nic6.IPConfig
<!--NeedCopy--> ```
```

**Erstellen Sie Azure-Lastenausgleich (ALB)**.

Dieser Schritt umfasst die folgenden Teilschritte:

- Frontend-IP-Konfiguration erstellen

 
```

- Integritätstest erstellen
- Back-End-Adresspool erstellen
- Erstellen von Lastenausgleichsregeln (HTTP und SSL)
- Erstellen Sie ALB mit Front-End-IP-Konfiguration, Back-End-Adresspool und LB-Regel
- Verknüpfen Sie IP-Konfiguration mit Back-End-Pools

```
$frontEndIP1=New-AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName1
 -PublicIpAddress $pip3

$healthProbe=New-AzureRmLoadBalancerProbeConfig -Name $healthProbeName
-Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2

$beAddressPool1=New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$backendPoolName1

$lbRule1=New-AzureRmLoadBalancerRuleConfig -Name $lbRuleName1 -FrontendIpConfigur
 $frontEndIP1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe -
Protocol Tcp -FrontendPort 80 -BackendPort 80 -EnableFloatingIP

$lb=New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name $lbName -
Location $locName -FrontendIpConfiguration $frontEndIP1 -LoadBalancingRule
 $lbRule1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe

$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$nic5.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$lb=$lb |Set-AzureRmLoadBalancer

$nic2=$nic2 | Set-AzureRmNetworkInterface

$nic5=$nic5 | Set-AzureRmNetworkInterface
```

Nachdem Sie das NetScaler VPX-Paar erfolgreich bereitgestellt haben, melden Sie sich bei jeder VPX-Instanz an, um HA-INC- sowie SNIP- und VIP-Adressen zu konfigurieren.

1. Geben Sie den folgenden Befehl ein, um HA-Knoten hinzuzufügen.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Fügen Sie private IP-Adressen von clientseitigen Netzwerkkarten als SNIPs für VPX1 (NIC2) und VPX2 (NIC5) hinzu

   ```
   add nsip privateIPofNIC2 255.255.255.0 -type SNIP
   add nsip privateIPofNIC5 255.255.255.0 -type SNIP
   ```


3. Fügen Sie einen virtuellen Lastenausgleichsserver auf dem primären Knoten mit Front-End-IP-Adresse (öffentliche IP) von ALB hinzu.

   ```
   add lb virtual server v1 HTTP FrontEndIPofALB 80
   ```

Verwandte Ressourcen:

Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

NetScaler-Hochverfügbarkeitspaar auf Azure mit ALB im Floating IP-Deaktiviert-Modus bereitstellen

May 11, 2023

Sie können ein Paar von NetScaler VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede Netzwerkkarte kann viele IP-Adressen enthalten.

Eine Aktiv-Passiv-Bereitstellung erfordert:

- Eine HA Independent Network Configuration (INC) Konfiguration
- Der Azure Load Balancer (ALB) mit:
  - Floating IP-fähiger Modus oder Direct Server Return (DSR) -Modus
  - Floating-IP-Modus deaktiviert

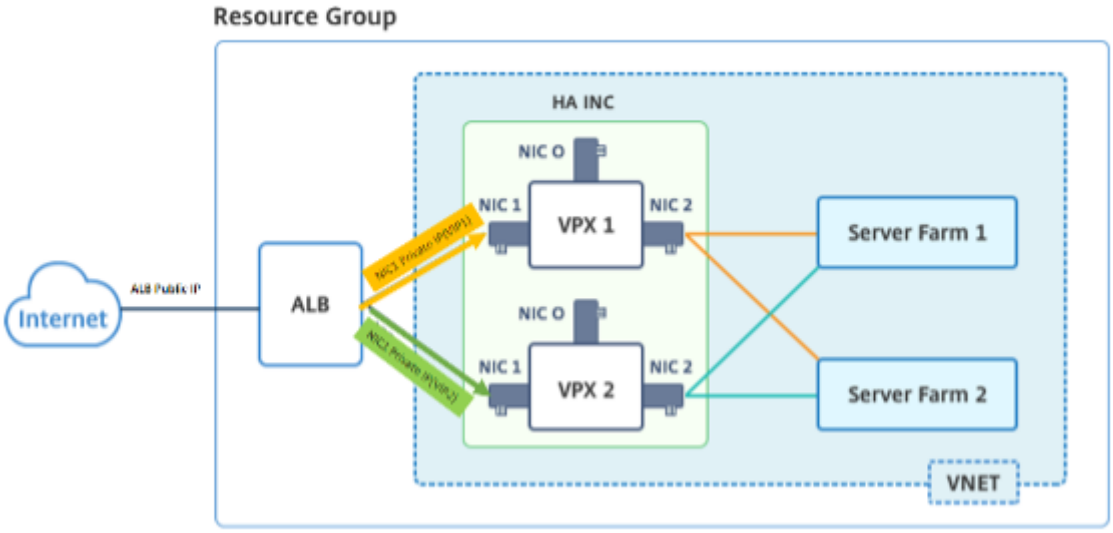
Weitere Informationen zu ALB Floating-IP-Optionen finden Sie in der Azure-Dokumentation.

Wenn Sie ein VPX-Paar im Aktiv-Passiv-HA-Setup auf Azure mit aktivierter ALB-Floating-IP bereitstellen möchten, finden Sie weitere Informationen unter Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und Netzwerkkarten mithilfe von PowerShell-Befehlen.

HA-Bereitstellungsarchitektur mit ALB im Floating-IP-deaktivierten Modus

Bei einer Aktiv-Passiv-Bereitstellung werden die privaten IP-Adressen der Client-Schnittstelle jeder Instanz als VIP-Adressen in jeder VPX-Instanz hinzugefügt. Konfiguration im HA-INC-Modus mit VIP-Adressen, die über IPset geteilt werden und SNIP-Adressen instanzspezifisch sind. Der gesamte Datenverkehr durchläuft die primäre Instanz. Die sekundäre Instanz befindet sich im Standby-Modus, bis die primäre Instanz ausfällt.

Diagramm: Beispiel einer aktiv-passiven Bereitstellungsarchitektur



Voraussetzungen

Sie müssen mit den folgenden Informationen vertraut sein, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen.

- Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Arbeiten einer NetScaler-Appliance. Weitere Informationen finden Sie in der NetScaler-Dokumentation.
- NetScaler-Netzwerk. Weitere Informationen finden Sie im ADC-Netzwerk.
- Konfiguration von Azure Load Balancer und Load Balancing-Regeln Weitere Informationen finden Sie in der Azure ALB-Dokumentation.

So stellen Sie ein VPX HA-Paar auf Azure mit deaktivierter ALB Floating-IP bereit

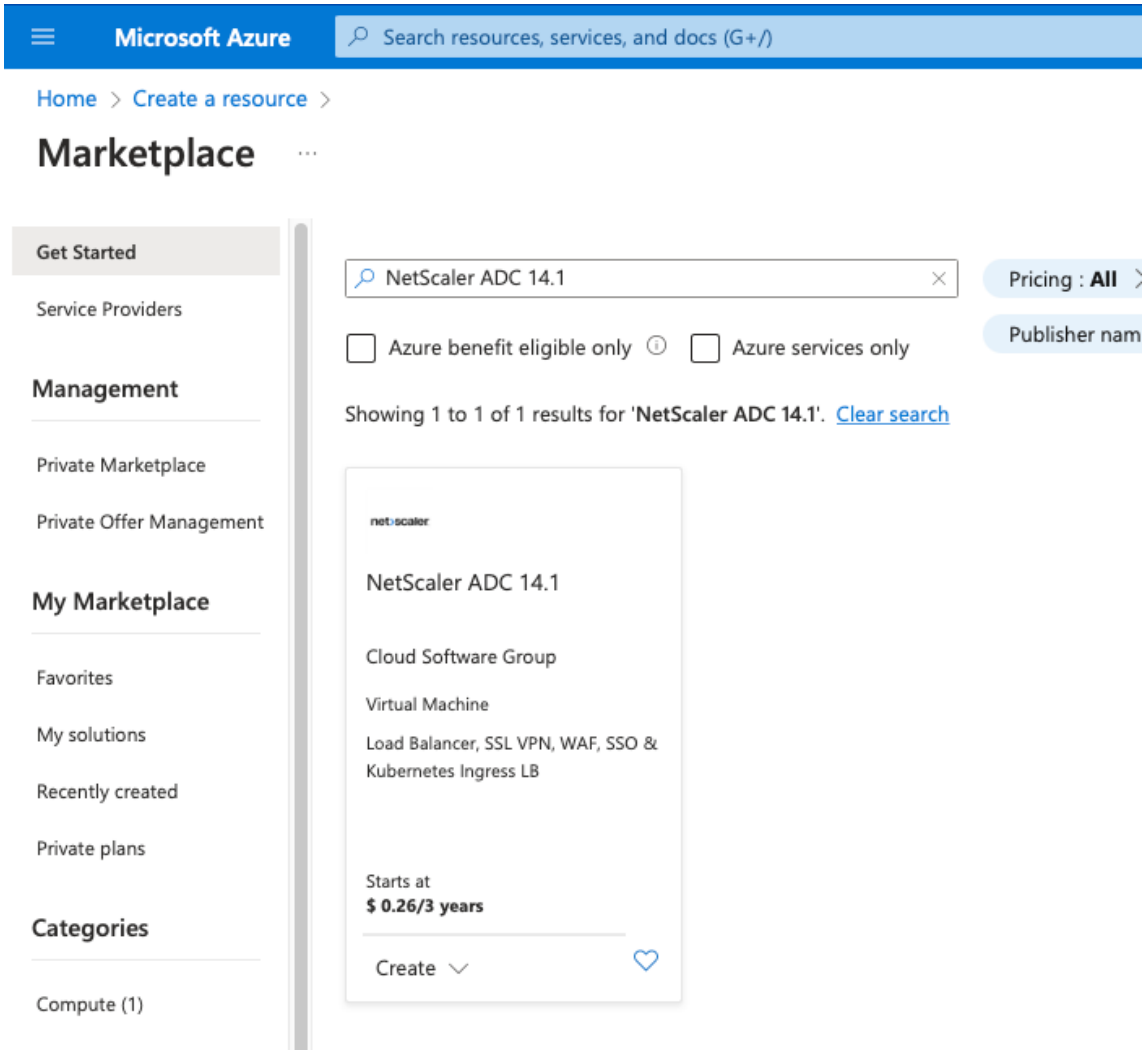
Hier finden Sie eine Zusammenfassung der Schritte zur HA- und ALB-Bereitstellung:

1. Stellen Sie zwei VPX-Instanzen (primäre und sekundäre Instanzen) in Azure bereit.
2. Fügen Sie auf beiden Instanzen eine Client- und Server-Netzwerkkarte hinzu.
3. Stellen Sie eine ALB mit Load Balancing-Regel bereit, deren Floating-IP-Modus deaktiviert ist.
4. Konfigurieren Sie HA-Einstellungen auf beiden Instanzen mithilfe der NetScaler GUI.

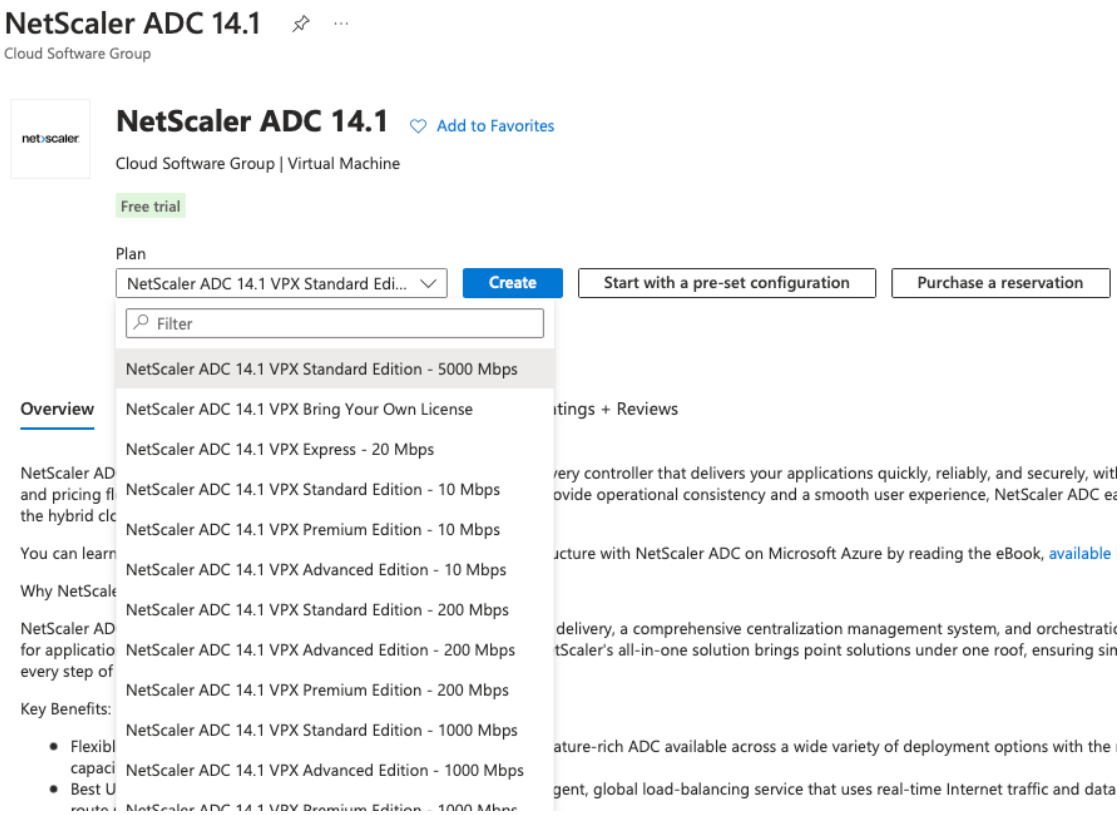
Schritt 1. Stellen Sie zwei VPX-Instanzen auf Azure bereit.

Erstellen Sie zwei VPX-Instanzen, indem Sie die folgenden Schritte ausführen:

1. Wählen Sie die NetScaler-Version aus Azure Marketplace aus (in diesem Beispiel wird NetScaler Version 13.1 verwendet).

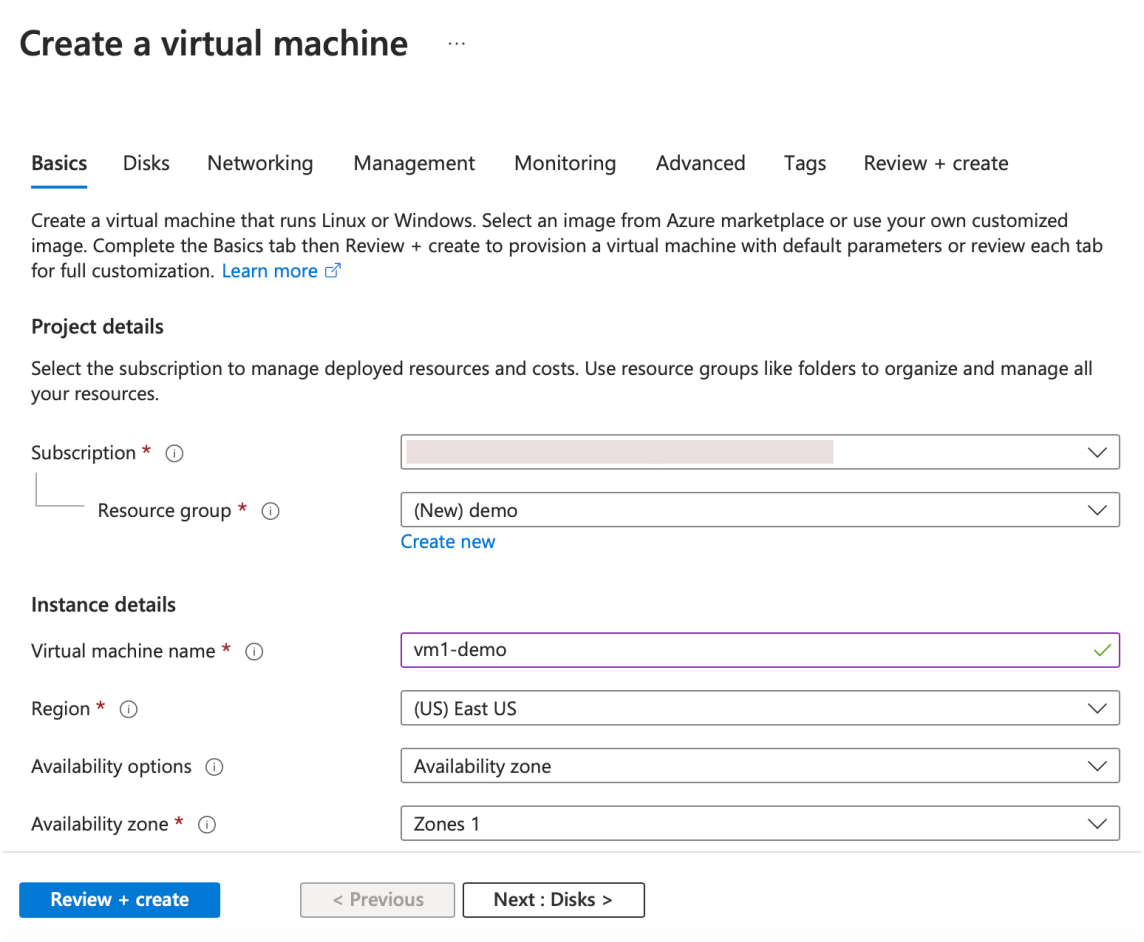


2. Wählen Sie den erforderlichen ADC-Lizenzierungsmodus aus und klicken Sie auf **Erstellen**.



Die Seite **Virtuelle Maschine erstellen** wird geöffnet.

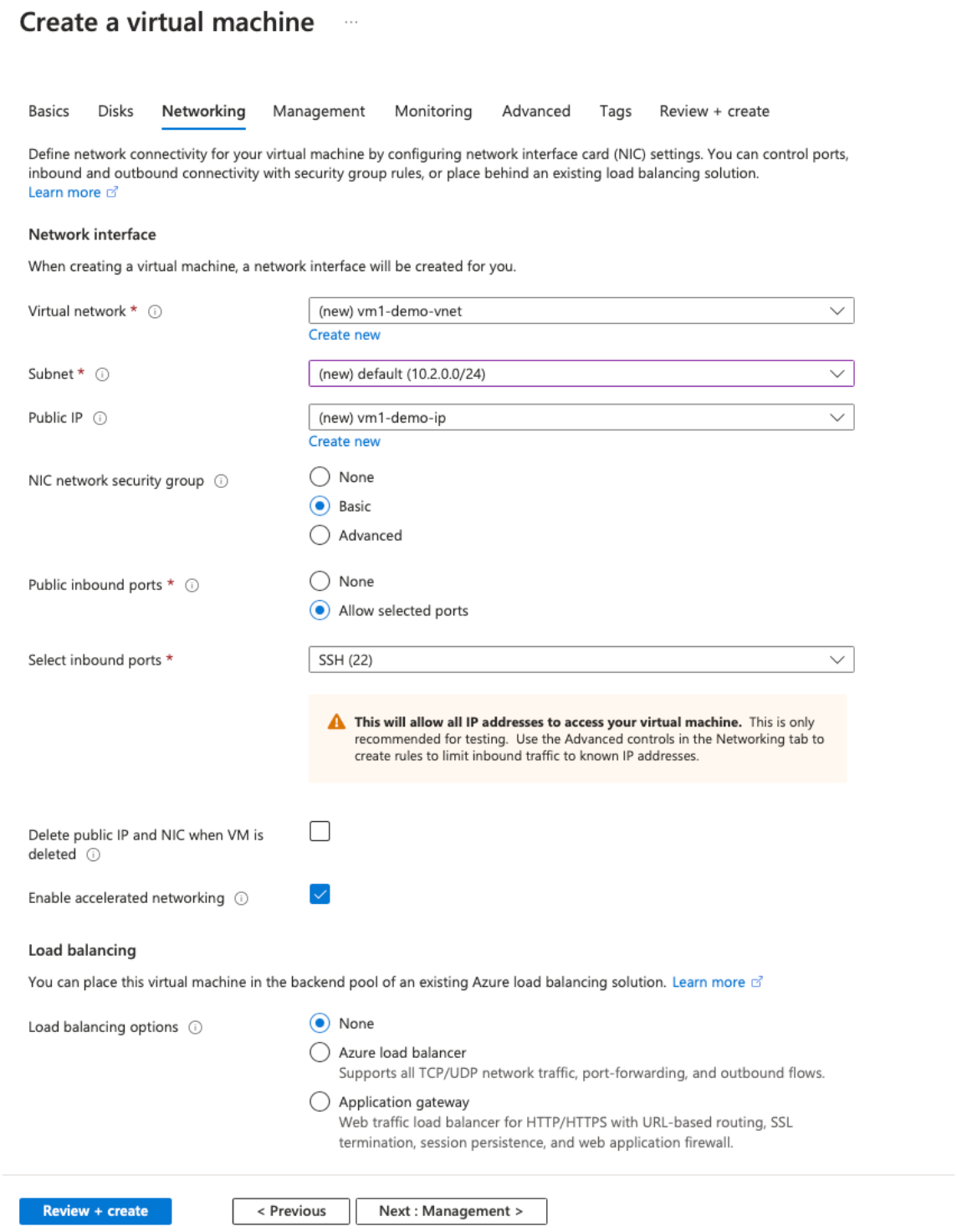
3. Füllen Sie auf jeder Registerkarte die erforderlichen Details für eine erfolgreiche Bereitstellung aus.



4. Erstellen Sie auf der Registerkarte **Netzwerk** ein neues virtuelles Netzwerk mit 3 Subnetzen, jeweils eines für: Verwaltungs-, Client- und Server-Netzwerkkarten. Andernfalls können Sie auch ein vorhandenes virtuelles Netzwerk verwenden. Die Management-NIC wird während der VM-Bereitstellung erstellt. Client- und Server-Netzwerkkarten werden erstellt und angehängt, nachdem die VM erstellt wurde. Für die Netzwerksicherheitsgruppe NIC können Sie eine der folgenden Aktionen ausführen:

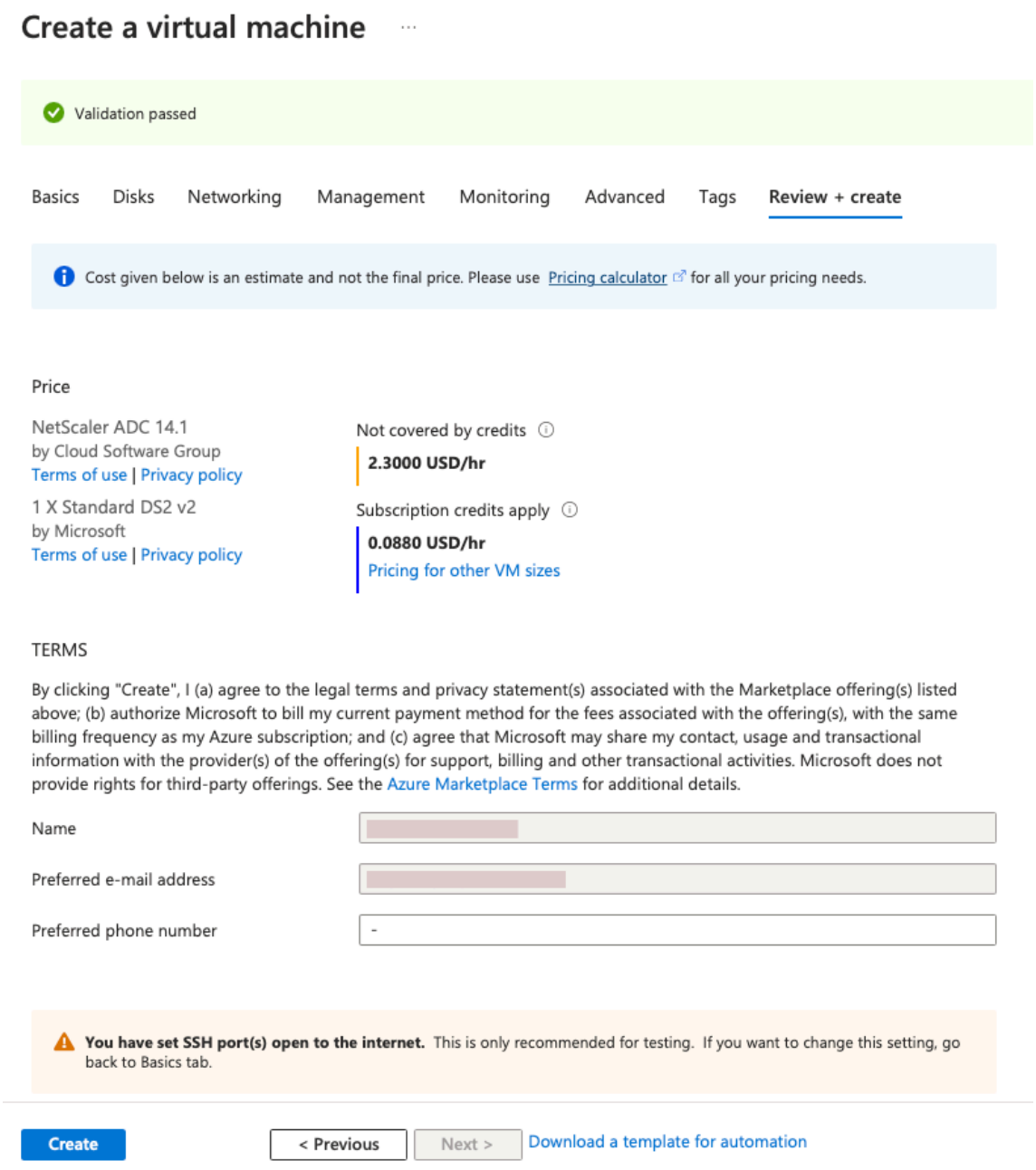
   - Wählen Sie **Erweitert** aus und verwenden Sie eine vorhandene Netzwerksicherheitsgruppe, die Ihren Anforderungen entspricht.
   - Wählen Sie **Basic** und dann die erforderlichen Ports aus.

   > **Hinweis:**
   >
   > Sie können die Einstellungen der Netzwerksicherheitsgruppe auch ändern, nachdem die VM-Bereitstellung abgeschlossen ist.

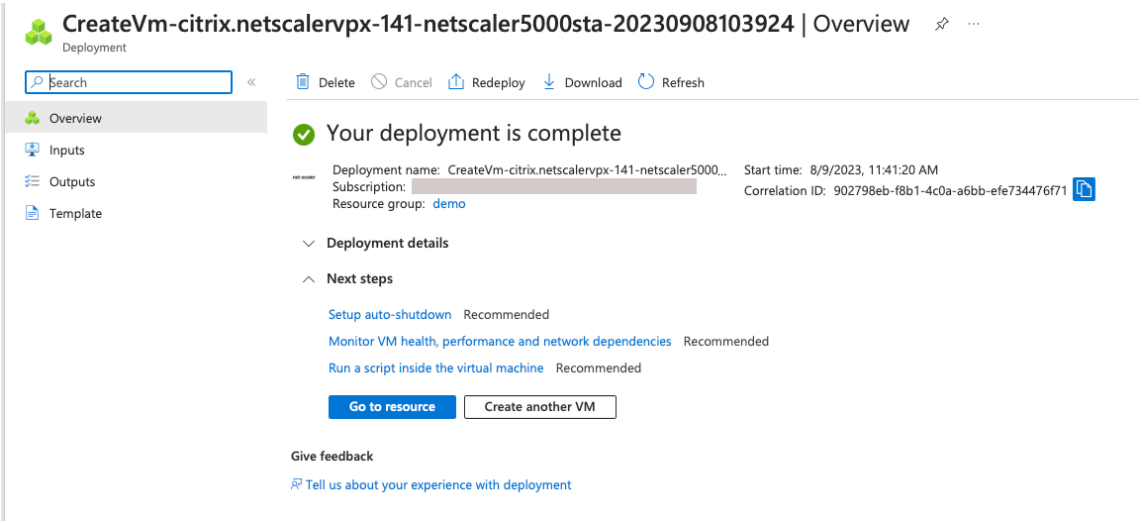


5. Klicken Sie auf Weiter: **Überprüfen + erstellen**.

   Überprüfen Sie nach erfolgreicher Validierung die Grundeinstellungen, VM-Konfigurationen, das Netzwerk und zusätzliche Einstellungen und klicken Sie auf **Erstellen**.



6. Klicken Sie nach Abschluss der Bereitstellung auf **Gehe zu Ressource**, um die Konfigurationsdetails anzuzeigen.



Stellen Sie auf ähnliche Weise eine zweite NetScaler VPX-Instanz bereit.

Schritt 2. Fügen Sie auf beiden Instanzen Client- und Server-Netzwerkkarten hinzu.

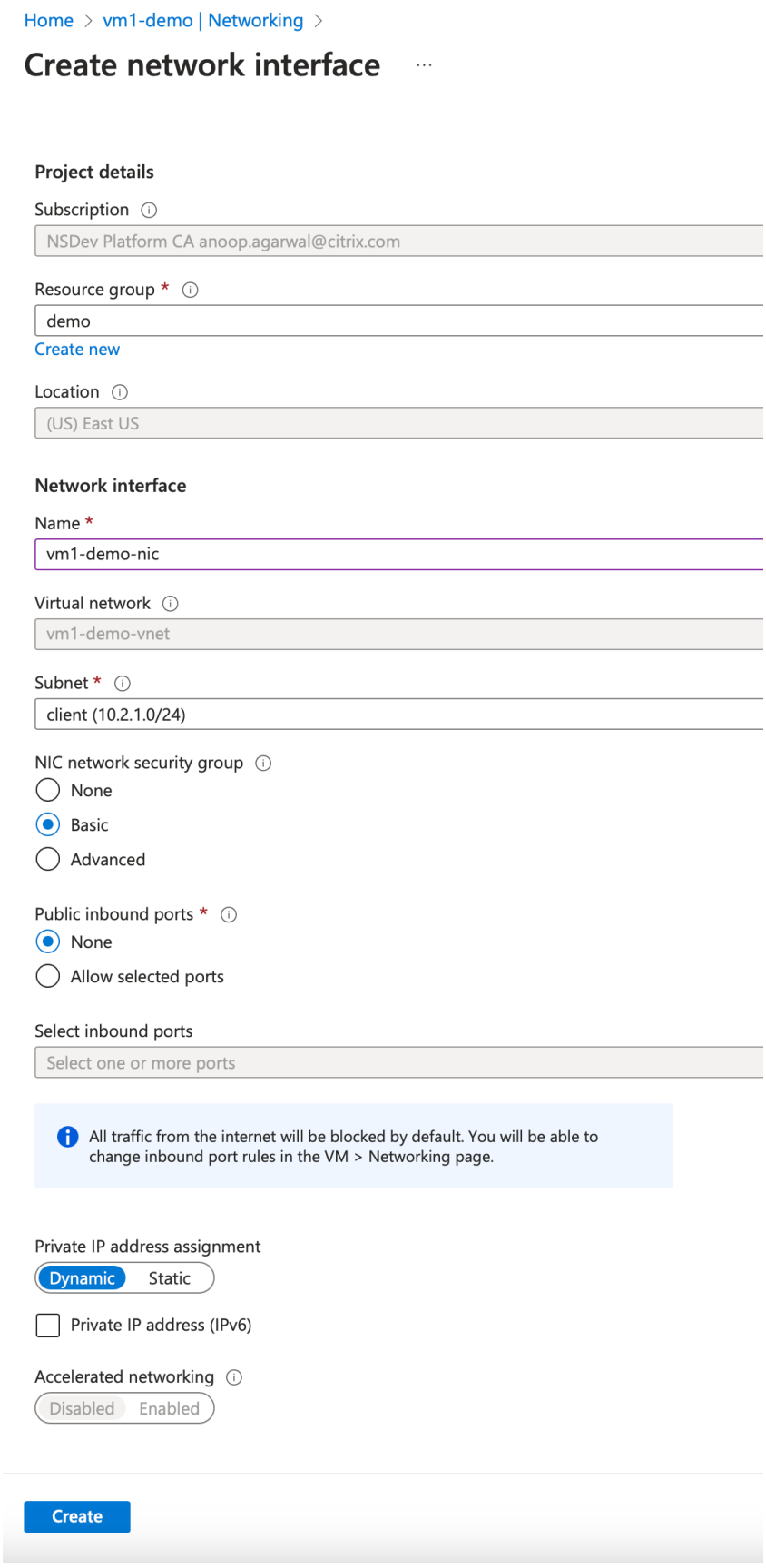
> **Hinweis:**
>
> Um weitere Netzwerkkarten anzuhängen, müssen Sie zuerst die VM beenden. Wählen Sie im Azure-Portal die VM aus, die Sie beenden möchten. Klicken Sie auf der Registerkarte **Overview** auf **Stop**. Warten Sie, bis der Status als **Gestoppt angezeigt wird**.

Gehen Sie folgendermaßen vor, um eine Client-Netzwerkkarte zur primären Instanz hinzuzufügen:

1. Navigieren Sie zu **Netzwerk > Netzwerkschnittstelle anhängen**.

   Sie können eine vorhandene Netzwerkkarte auswählen oder eine neue Schnittstelle erstellen und anfügen.

2. Für die Netzwerksicherheitsgruppe NIC können Sie eine vorhandene Netzwerksicherheitsgruppe verwenden, indem Sie **Erweitert** auswählen, oder eine erstellen, indem Sie **Basic**auswählen.



Um eine Server-Netzwerkkarte hinzuzufügen, führen Sie dieselben Schritte wie beim Hinzufügen einer Client-Netzwerkkarte aus.

An die NetScaler VPX-Instanz sind alle drei Netzwerkkarten (Management-NIC, Client-NIC und Server-NIC) angeschlossen.

Wiederholen Sie die vorherigen Schritte zum Hinzufügen von Netzwerkkarten auf der sekundären Instanz.

Nachdem Sie die Netzwerkkarten auf beiden Instanzen erstellt und angehängt haben, starten Sie beide Instanzen neu, indem Sie zu **Übersicht > Start**gehen.

> **Hinweis:**
>
> Sie müssen den Datenverkehr durch den Port in der eingehenden Client-NIC-Regel zulassen, die später verwendet wird, um einen virtuellen Lastausgleichsserver beim Konfigurieren der NetScaler VPX-Instanz zu erstellen.

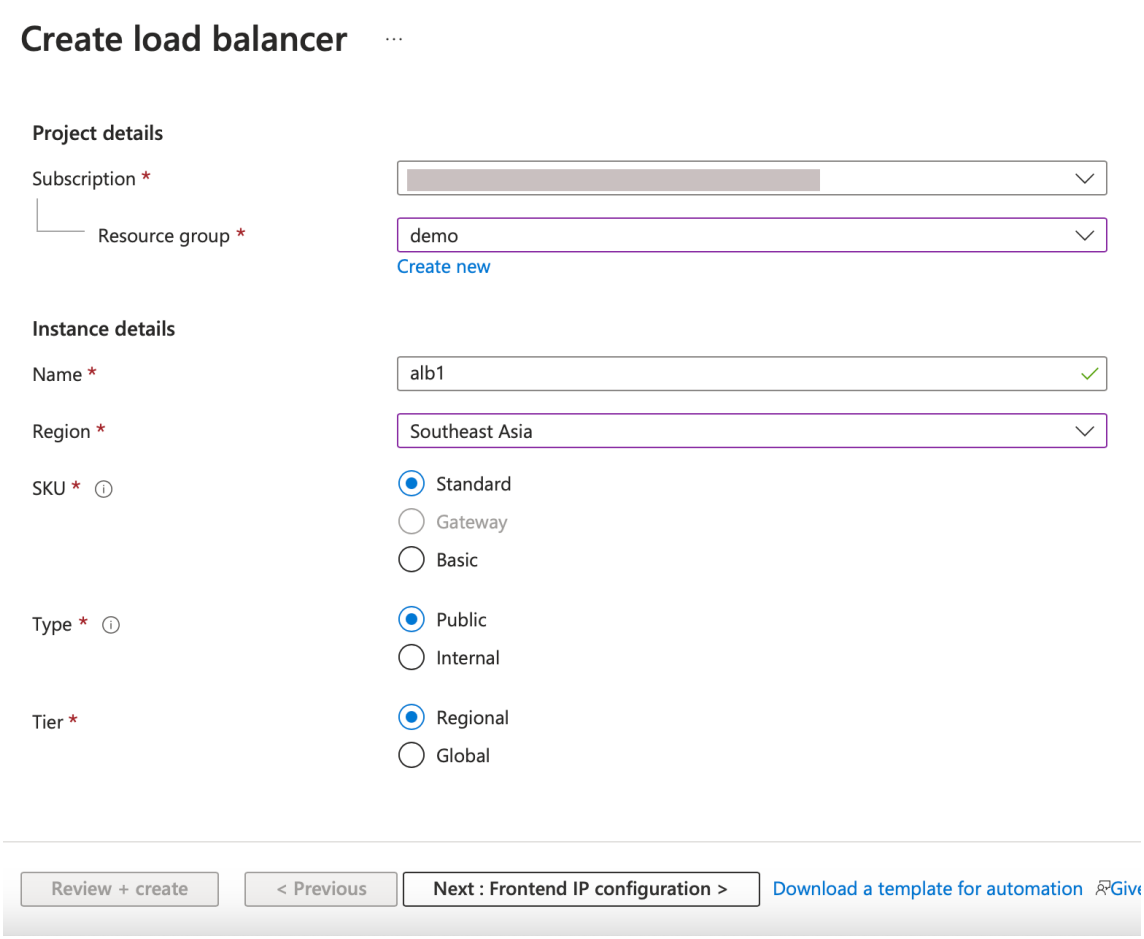
Im folgenden Beispiel wird der Sicherheitsregel für eingehenden Datenverkehr ein HTTP-Port 80 hinzugefügt.

Schritt 3. Stellen Sie eine ALB mit Load Balancing-Regel bereit, deren Floating-IP-Modus deaktiviert ist.

Gehen Sie folgendermaßen vor, um die Konfiguration von ALB zu starten:

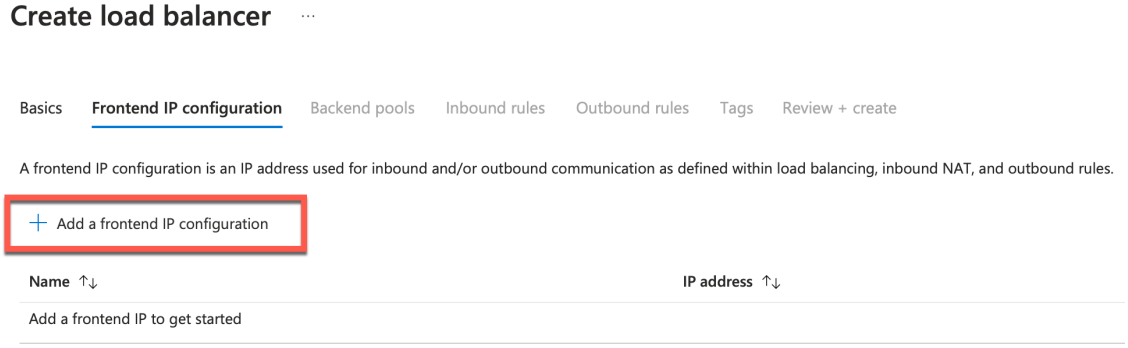
1. Gehen Sie zur Seite **Load Balancers** und klicken Sie auf **Erstellen**.
2. Geben **Sie auf der Seite Load Balancer erstellen** die Details nach Bedarf ein.

   Im folgenden Beispiel stellen wir einen regionalen öffentlichen Load Balancer der Standard-SKU bereit.



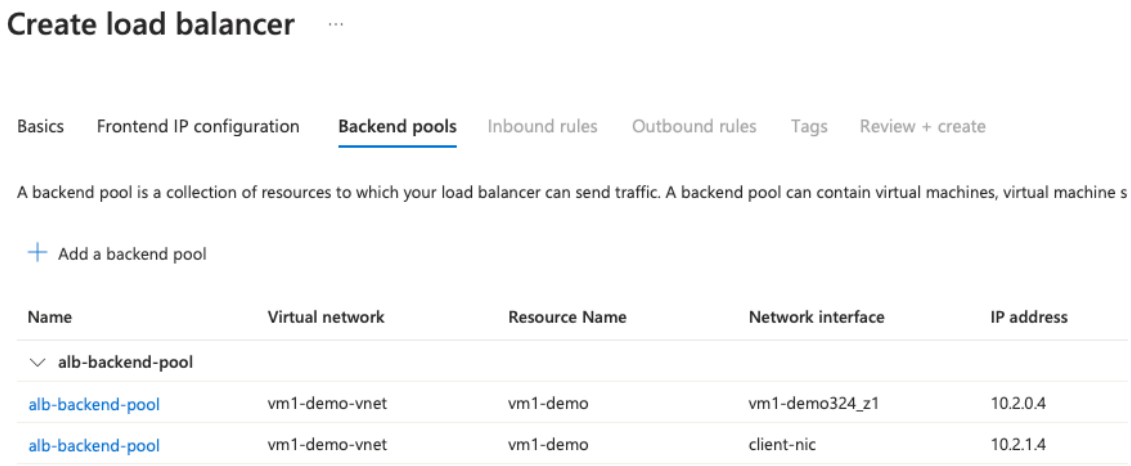
> **Hinweis:**
>
> Alle öffentlichen IPs, die an die NetScaler VMs angeschlossen sind, müssen dieselbe SKU wie die von ALB haben. Weitere Informationen zu ALB-SKUs finden Sie in der Dokumentation der Azure Load Balancer-SKUs.

3. Erstellen Sie auf der Registerkarte **Frontend-IP-Konfiguration** entweder eine IP-Adresse oder verwenden Sie eine vorhandene IP-Adresse.

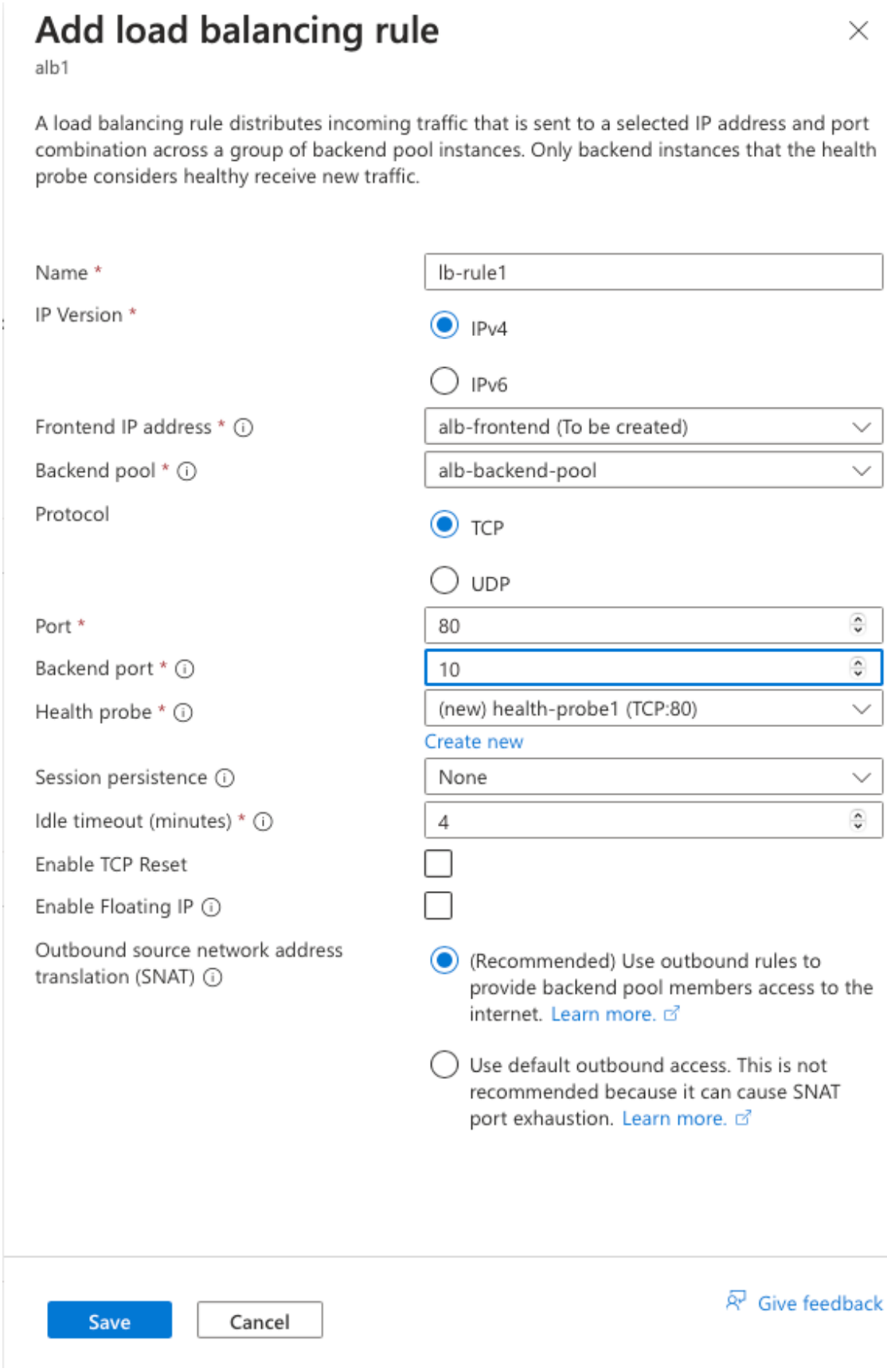


4. Wählen Sie auf der Registerkarte **Backend-Pools** die NIC-basierte Backend-Poolkonfiguration

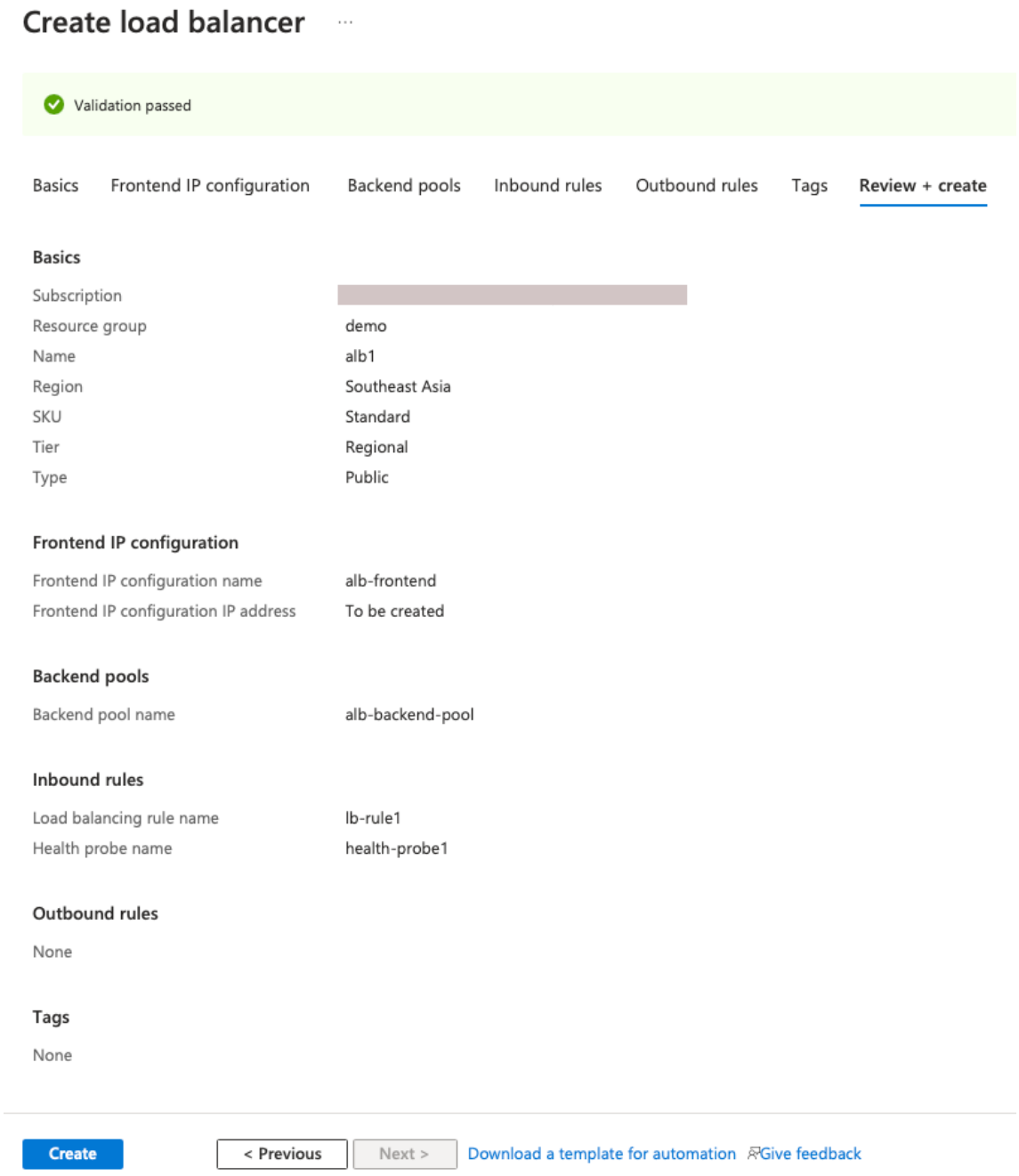
aus und fügen Sie die Client-NICs der beiden NetScaler VMs hinzu.



5. Klicken Sie auf der Registerkarte **Eingehende Regeln** auf **Load Balancing-Regel hinzufügen**und geben Sie die Frontend-IP-Adresse und den Backend-Pool an, die in den vorherigen Schritten erstellt wurden. Wählen Sie das Protokoll und den Port basierend auf Ihren Anforderungen aus. Erstellen oder verwenden Sie eine vorhandene Gesundheitssonde. Die Floating-IP-Option muss auf **Deaktiviert**gesetzt sein.



6. Klicken Sie auf **Review + Erstellen**. Nachdem die Überprüfung erfolgreich war, klicken Sie auf **Erstellen**.



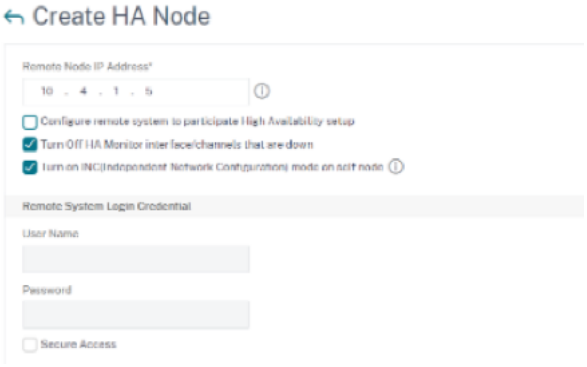
Schritt 4. Konfigurieren Sie HA-Einstellungen auf beiden NetScaler VPX-Instanzen mithilfe der NetScaler GUI.

Nachdem Sie die NetScaler VPX-Instanzen in Azure erstellt haben, können Sie HA mithilfe der NetScaler GUI konfigurieren.

Schritt 1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

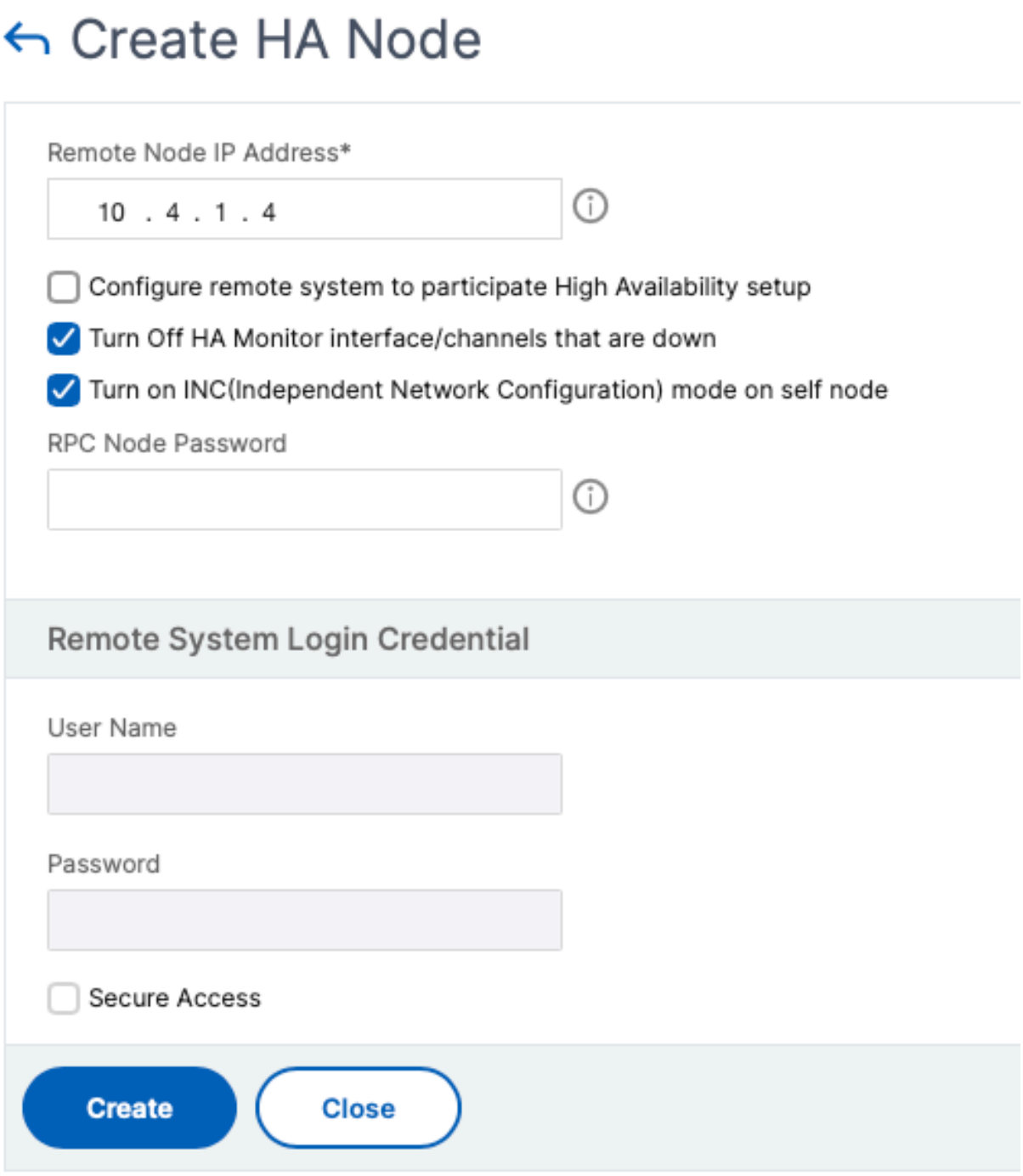
Führen Sie auf der primären Instanz die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem bei der Bereitstellung der Instanz angegebenen Benutzernamen und Kennwort von `nsroot` an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Remote Node-IP-Adresse** die private IP-Adresse der Management-NIC der sekundären Instanz ein, z. B.: 10.4.1.5.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.



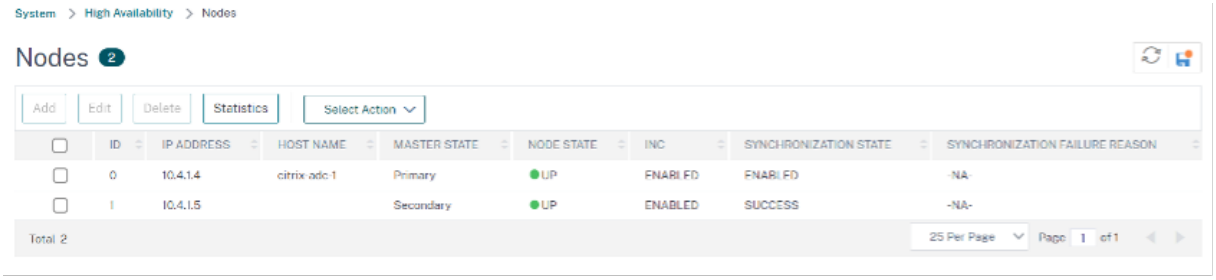
Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem bei der Bereitstellung der Instanz angegebenen Benutzernamen und Kennwort von `nsroot` an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Remote Node-IP-Adresse** die private IP-Adresse der Management-NIC der primären Instanz ein, z. B.: 10.4.1.4.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.



Bevor Sie fortfahren, stellen Sie sicher, dass der **Synchronisierungsstatus** der sekundären Instanz auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

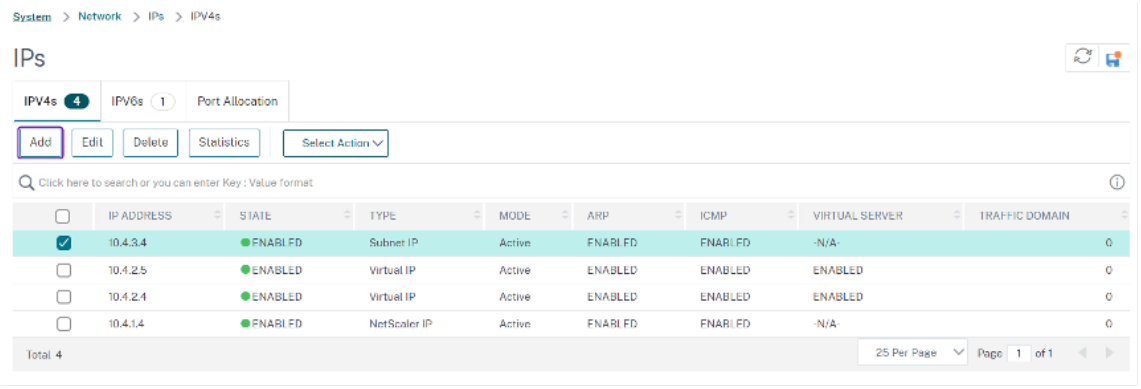
> **Hinweis:**
>
> Jetzt hat die sekundäre Instanz dieselben Anmeldeinformationen wie die primäre Instanz.



Schritt 2. Fügen Sie auf beiden Instanzen virtuelle IP-Adresse und Subnetz-IP-Adresse hinzu.

Führen Sie auf der primären Instanz die folgenden Schritte aus:

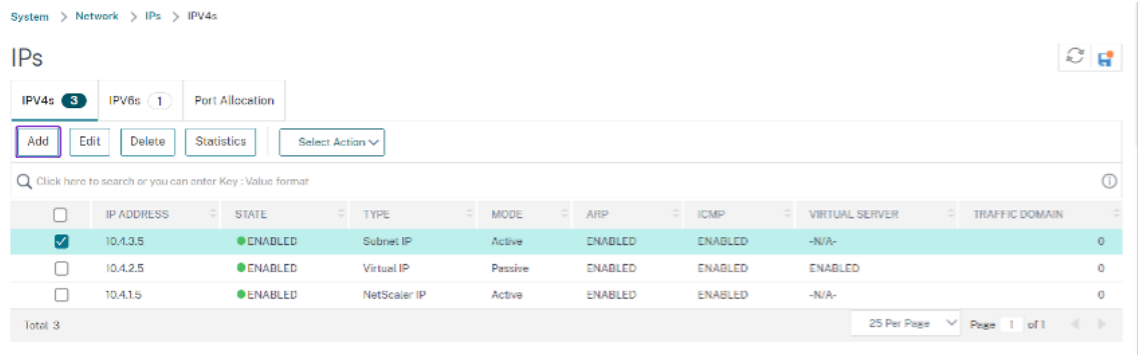
1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine primäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die private IP-Adresse der Client-NIC der primären Instanz und die für das Client-Subnetz konfigurierte Netzmaske in der VM-Instanz ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. Fügen Sie eine primäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Server-Netzwerkkarte der primären Instanz und die für das Serversubnetz in der primären Instanz konfigurierte Netzmaske ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
4. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Client-NIC der sekundären Instanz und die für das Client-Subnetz konfigurierte Netzmaske in der VM-Instanz ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.

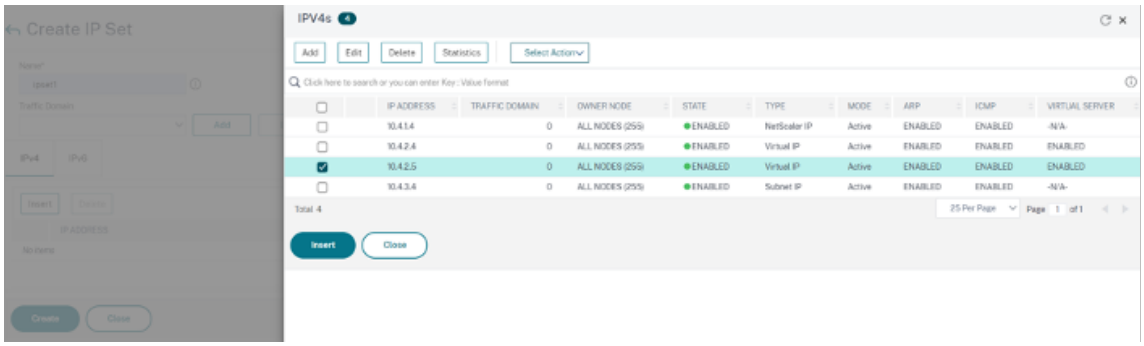
2. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Client-NIC der sekundären Instanz und die für das Client-Subnetz konfigurierte Netzmaske in der VM-Instanz ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
3. Fügen Sie eine sekundäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der Server-Netzwerkkarte der sekundären Instanz und die für das Serversubnetz in der sekundären Instanz konfigurierte Netzmaske ein.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie IP-Set hinzu und binden Sie die IP, die an den sekundären VIP auf beiden Instanzen festgelegt ist.

Führen Sie auf der primären Instanz die folgenden Schritte aus:

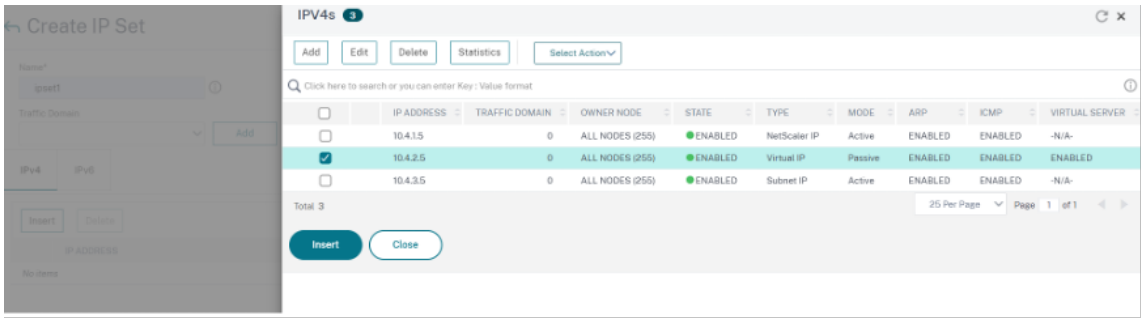
1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.

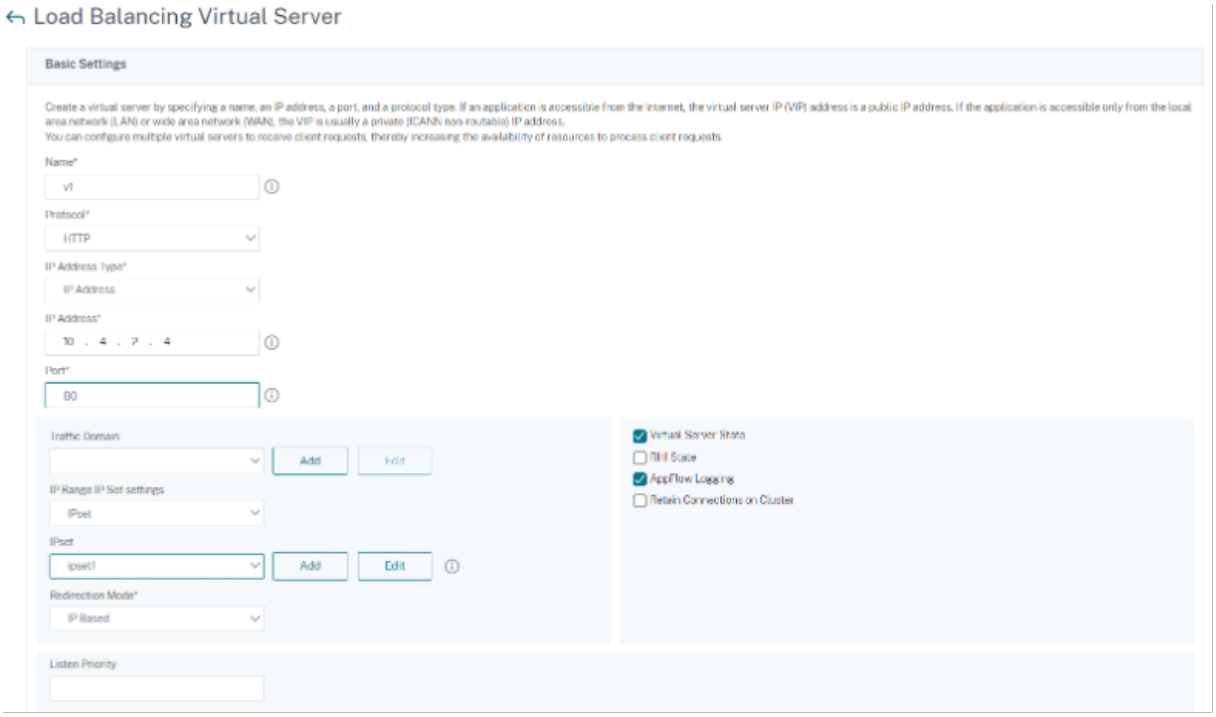
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der Seite **IPv4s** die virtuelle IP (sekundäre VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



> **Hinweis:**
>
> Der Name des IP-Sets muss sowohl auf der primären als auch auf der sekundären Instanz identisch sein.

Schritt 4. Fügen Sie der primären Instanz einen virtuellen Lastausgleichsserver hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäres VIP) und Port hinzu.
3. Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen**, wählen Sie im Dropdownmenü **IPset** aus und geben Sie das in **Schritt 3** erstellte IPset ein.
4. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.

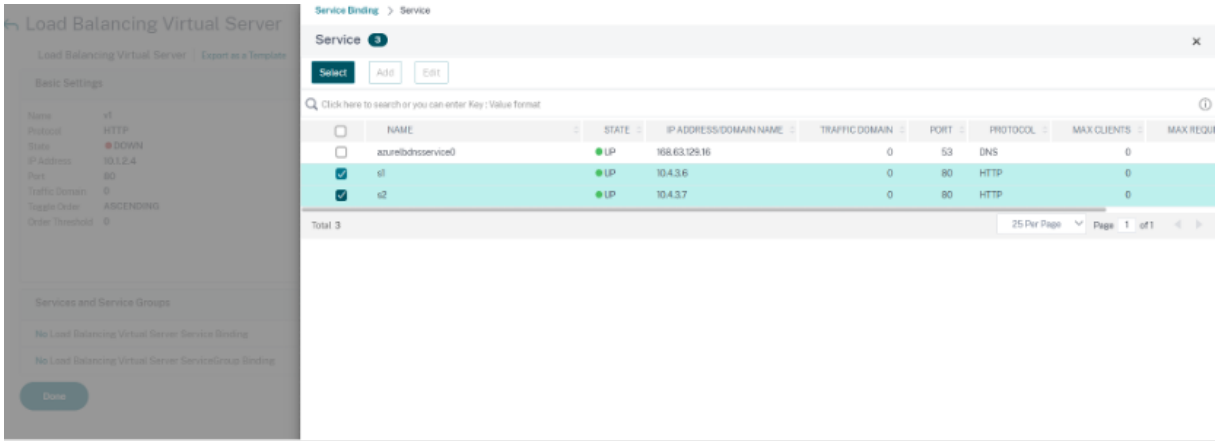


Schritt 5. Fügen Sie der primären Instanz einen Dienst oder eine Servicegruppe hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 6. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf der primären Instanz.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 4**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 5**konfigurierten Dienst aus und klicken Sie auf “ **Binden**”.



Schritt 7. Speichern Sie die Konfiguration.

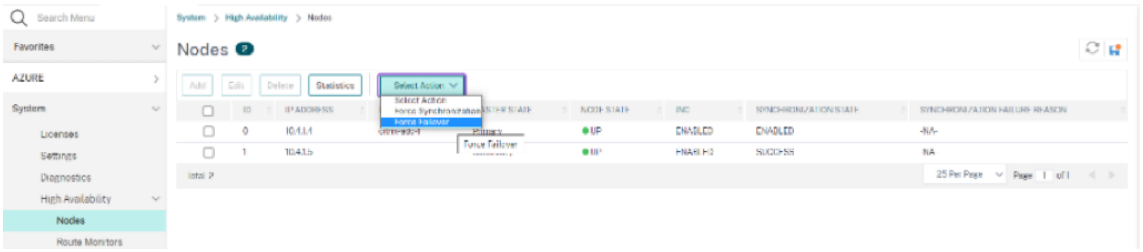
Andernfalls geht die gesamte Konfiguration nach einem Neustart oder einem sofortigen Neustart verloren.

Schritt 8. Überprüfen Sie die Konfiguration.

Stellen Sie sicher, dass die ALB-Frontend-IP-Adresse nach einem Failover erreichbar ist.

1. Kopieren Sie die ALB-Frontend-IP-Adresse.
2. Fügen Sie die IP-Adresse in den Browser ein und stellen Sie sicher, dass die Backend-Server erreichbar sind.
3. Führen Sie auf der primären Instanz Failover durch:

   Navigieren Sie in der NetScaler GUI zu **Konfiguration > System > Hochverfügbarkeit > Aktion > Failover erzwingen**.



4. Stellen Sie sicher, dass Backend-Server nach einem Failover über die zuvor verwendete ALB-Frontend-IP erreichbar sind.

Stellen Sie eine private NetScaler for Azure DNS-Zone bereit

September 1, 2023

Azure DNS ist ein Dienst in der Microsoft Azure-Infrastruktur zum Hosten von DNS-Domänen und zur Bereitstellung von Namensauflösung.

Private Azure DNS-Zonen sind ein Dienst, der sich auf die Auflösung von Domainnamen in einem privaten Netzwerk konzentriert. Mit privaten Zonen können Kunden ihre eigenen benutzerdefinierten Domainnamen anstelle der derzeit von Azure bereitgestellten Namen verwenden.

NetScaler, die führende Lösung für die Anwendungsbereitstellung, eignet sich am besten für die Bereitstellung von Lastenausgleichs- und GSLB-Funktionen für eine private Azure DNS-Zone. Durch das Abonnement der Azure DNS Private Zone kann sich das Unternehmen auf die Leistung und Intelligenz von NetScaler Global Server Load Balancing (GSLB) verlassen, um den Intranetverkehr auf Workloads in mehreren Regionen und über Rechenzentren zu verteilen, die über sichere VPN-Tunnel verbunden sind. Diese Zusammenarbeit garantiert Unternehmen den nahtlosen Zugriff auf einen Teil ihrer Arbeitslast, den sie in die Azure Public Cloud verlagern möchten.

Überblick über Azure DNS

Das Domain Name System (DNS) ist für die Übersetzung oder Auflösung eines Dienstnamens in seine IP-Adresse verantwortlich. Azure DNS ist ein Hosting-Service für DNS-Domänen und bietet Namensauflösung mithilfe der Microsoft Azure-Infrastruktur. Azure DNS unterstützt nicht nur mit dem Internet verbundene DNS-Domänen, sondern jetzt auch private DNS-Domänen.

Azure DNS bietet einen zuverlässigen, sicheren DNS-Dienst zur Verwaltung und Auflösung von Domainnamen in einem virtuellen Netzwerk, ohne dass eine benutzerdefinierte DNS-Lösung erforderlich ist. Durch die Verwendung von privaten DNS-Zonen können Sie anstelle der von Azure bereitgestellten Namen Ihre eigenen benutzerdefinierten Domainnamen verwenden. Mithilfe benutzerdefinierter Domainnamen können Sie Ihre virtuelle Netzwerkarchitektur optimal an die Bedürfnisse Ihres Unternehmens anpassen. Es bietet die Namensauflösung für virtuelle Maschinen (VMs) innerhalb eines virtuellen Netzwerks und zwischen virtuellen Netzwerken. Außerdem können Kunden Zonennamen mit einer Split-Horizon-Ansicht konfigurieren, sodass eine private und eine öffentliche DNS-Zone einen gemeinsamen Namen haben können.

Warum NetScaler GSLB für Azure DNS Private Zone?

In der heutigen Welt möchten Unternehmen ihre Workloads von lokalen Workloads auf die Azure-Cloud verlagern. Der Übergang zur Cloud ermöglicht es ihnen, die Markteinführungszeit, die Kapitalaufwand/den Preis, die einfache Implementierung und die Sicherheit zu nutzen. Der Azure DNS Private Zone Service bietet ein einzigartiges Angebot für Unternehmen, die einen Teil ihrer Workloads in die Azure Cloud verlagern. Diese Unternehmen können ihren privaten DNS-Namen, den sie jahrelang in lokalen Bereitstellungen hatten, erstellen, wenn sie den Private Zone Service nutzen. Bei diesem Hybridmodell von Intranet-Anwendungsservern, die sich lokal und in der Azure-Cloud befinden und über sichere VPN-Tunnel verbunden sind, besteht die einzige Herausforderung darin, einen nahtlosen

Zugriff auf diese Intranetanwendungen zu haben. NetScaler löst diesen einzigartigen Anwendungsfall mit seiner globalen Lastenausgleichsfunktion, die den Anwendungsdatenverkehr an die optimalsten verteilten Workloads/Server entweder vor Ort oder in der Azure-Cloud weiterleitet und den Integritätsstatus des Anwendungsservers bereitstellt.

Anwendungsfall

Benutzer in einem lokalen Netzwerk und in verschiedenen Azure-VNets können eine Verbindung zu den optimalsten Servern in einem internen Netzwerk herstellen, um auf die erforderlichen Inhalte zuzugreifen. Dadurch wird sichergestellt, dass die Anwendung immer verfügbar ist, die Kosten optimiert werden und die Benutzererfahrung gut ist. Azure Private Traffic Management (PTM) ist hier die Hauptanforderung. Azure PTM stellt sicher, dass die DNS-Abfragen der Benutzer zu einer geeigneten privaten IP-Adresse des Anwendungsservers aufgelöst werden.

Lösung für Anwendungsfälle

NetScaler enthält die GSLB-Funktion (Global Server Load Balancing), um die Azure PTM-Anforderungen zu erfüllen. GSLB verhält sich wie ein DNS-Server, der die DNS-Anfragen empfängt und die DNS-Anfrage in eine geeignete IP-Adresse auflöst, um Folgendes bereitzustellen:

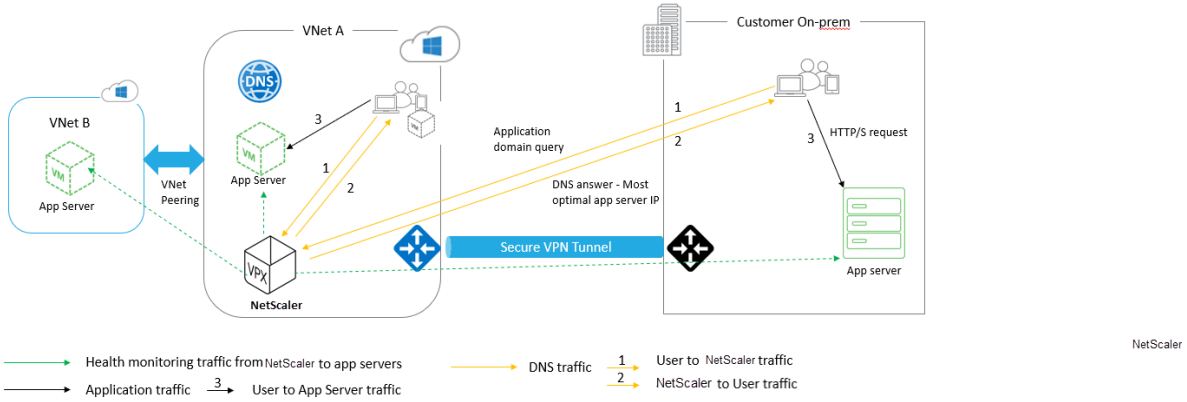
- Reibungsloser DNS-basierter Failover.
- Schrittweise Migration von On-Premise zur Cloud.
- A/B-Tests einer neuen Funktion.

Unter den vielen unterstützten Lastausgleichsmethoden können die folgenden Methoden in dieser Lösung nützlich sein:

1. Runde Robin
2. Statische Nähe (standortbasierte Serverauswahl). Es kann auf zwei Arten eingesetzt werden:
    a) Auf EDNS Client Subnet (ECS) basierendes GSLB auf NetScaler.
    b) Stellen Sie für jedes virtuelle Netzwerk einen DNS-Forwarder bereit.

Topologie

Die folgende Abbildung zeigt die NetScaler GSLB-Bereitstellung für eine private Azure-DNS-Zone.



Ein Benutzer kann auf jeden Anwendungsserver entweder in Azure oder vor Ort zugreifen, der auf der NetScaler GSLB-Methode in einer privaten Azure-DNS-Zone basiert. Der gesamte Datenverkehr zwischen dem lokalen und dem virtuellen Azure-Netzwerk erfolgt ausschließlich über einen sicheren VPN-Tunnel. Anwendungsverkehr, DNS-Verkehr und Überwachungsverkehr werden in der vorherigen Topologie angezeigt. Abhängig von der erforderlichen Redundanz können NetScaler und DNS-Forwarder in den virtuellen Netzwerken und Rechenzentren eingesetzt werden. Der Einfachheit halber wird hier nur ein NetScaler angezeigt, aber wir empfehlen mindestens einen Satz NetScaler und DNS-Forwarder für die Azure-Region. Alle Benutzer-DNS-Abfragen werden zunächst an den DNS-Forwarder weitergeleitet, für den Regeln für die Weiterleitung der Anfragen an einen geeigneten DNS-Server definiert sind.

Konfiguration von NetScaler für die private Azure DNS-Zone

Getestete Produkte und Versionen:

Produkt	Version
Azure	Cloud-Abonnement
NetScaler VPX	BYOL (Bringen Sie Ihre eigene Lizenz mit)

> **Hinweis:**
>
> Die Bereitstellung wurde getestet und bleibt mit NetScaler Version 12.0 und höher unverändert.

Voraussetzungen

Im Folgenden sind allgemeine Voraussetzungen aufgeführt.

- Microsoft Azure-Portalkonto mit einem gültigen Abonnement.
- Stellen Sie die Konnektivität (Secure VPN Tunnel) zwischen On-Prem und Azure Cloud sicher.

Informationen zum Einrichten eines sicheren VPN-Tunnels in Azure finden Sie unter Schritt für Schritt: Konfiguration eines Site-to-Site-VPN-Gateways zwischen Azure und on-premises.

Lösungsbeschreibung

Wenn Sie eine Anwendung hosten möchten, die private Azure-DNS-Zone (rr.ptm.mysite.net), die auf HTTPs läuft und in Azure und lokal mit Intranetzugriff bereitgestellt wird, der auf der Round-Robin-GSLB-Lastenausgleichsmethode basiert. Um diese Bereitstellung zu erreichen, aktivieren Sie GSLB für die private Azure-DNS-Zone mit NetScaler, die aus den folgenden Konfigurationen besteht:

1. Konfigurieren Sie das Azure- und On-Premises-Setup.
2. NetScaler-Appliance im virtuellen Azure-Netzwerk.

Azure- und On-Premises-Setup konfigurieren

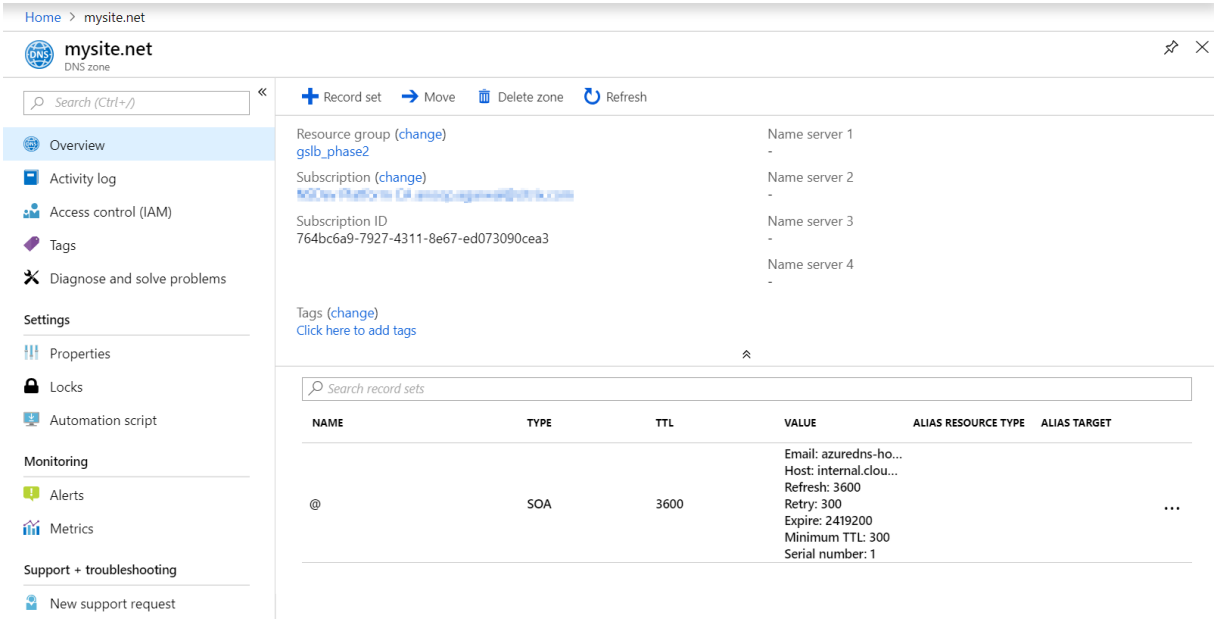
Richten Sie, wie in der Topologie gezeigt, das virtuelle Azure-Netzwerk (in diesem Fall VNet A, VNet B) und das lokale Setup ein.

1. Erstellen Sie eine private Azure-DNS-Zone mit dem Domainnamen (mysite.net).
2. Erstellen Sie zwei virtuelle Netzwerke (VNet A, VNet B) in einem Hub-and-Spoke-Modell in einer Azure-Region.
3. Stellen Sie App Server, DNS-Forwarder, Windows 10 Pro-Client und NetScaler in VNet A bereit.
4. Stellen Sie einen App Server bereit und stellen Sie einen DNS-Forwarder bereit, falls sich Clients in VNet B befinden.
5. Stellen Sie einen App-Server, eine DNS-Weiterleitung und einen Windows 10 Pro-Client vor Ort bereit.

Private Azure-DNS-Zone

Erstellen Sie eine private Azure-DNS-Zone mit einem Domainnamen.

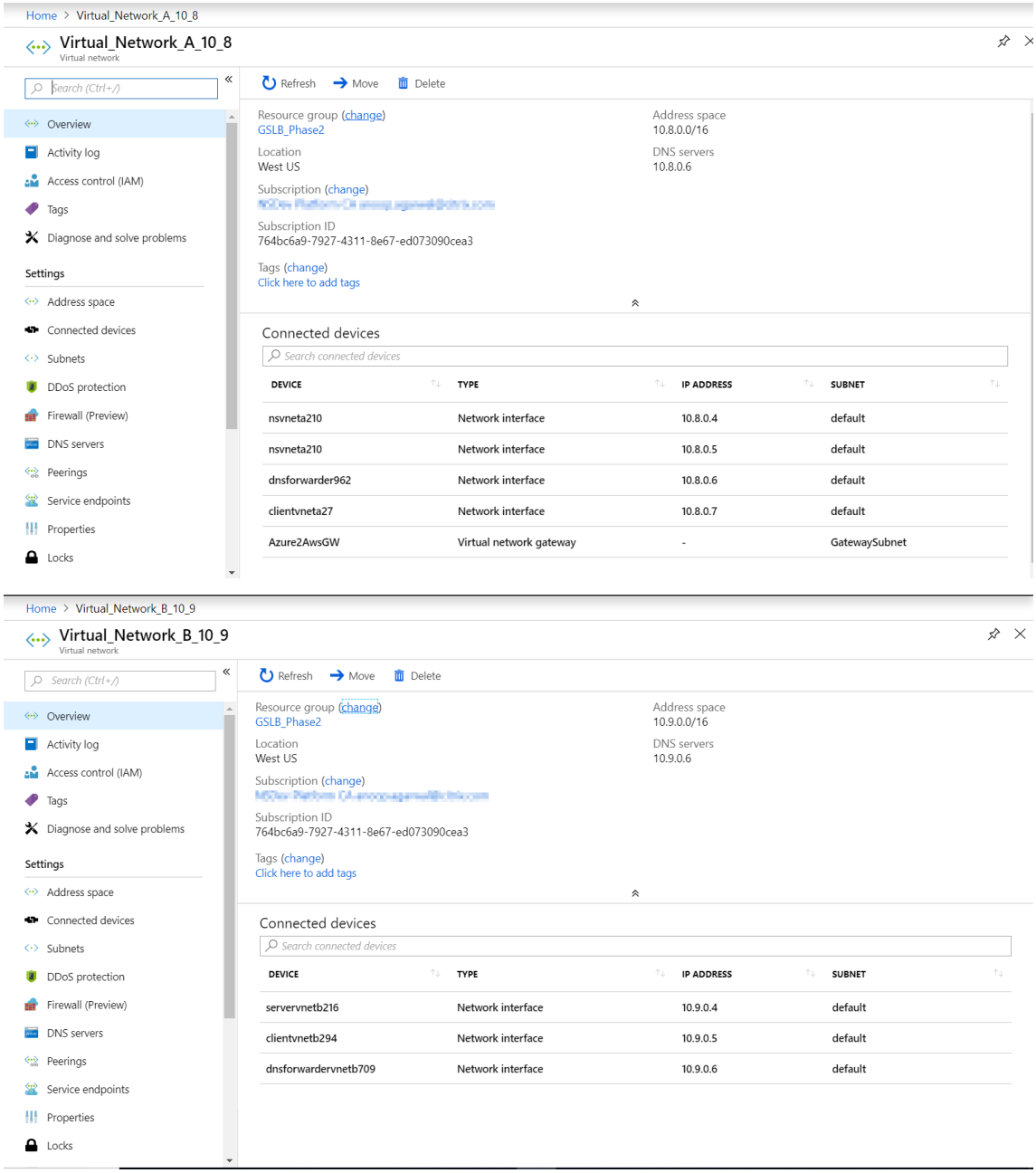
1. Melden Sie sich im Azure-Portal an und wählen Sie ein Dashboard aus oder erstellen Sie es.
2. Klicken Sie auf **Ressource erstellen und suchen Sie nach der DNS-Zone, um eine** private Azure-DNS-Zone mit dem Domänennamen (mysite.net) zu erstellen (in diesem Fall mysite.net).



Virtuelle Azure-Netzwerke (VNet A, VNet B) im Hub-and-Spoke-Modell

Erstellen Sie zwei virtuelle Netzwerke (VNet A, VNet B) in einem Hub-and-Spoke-Modell in einer Azure-Region.

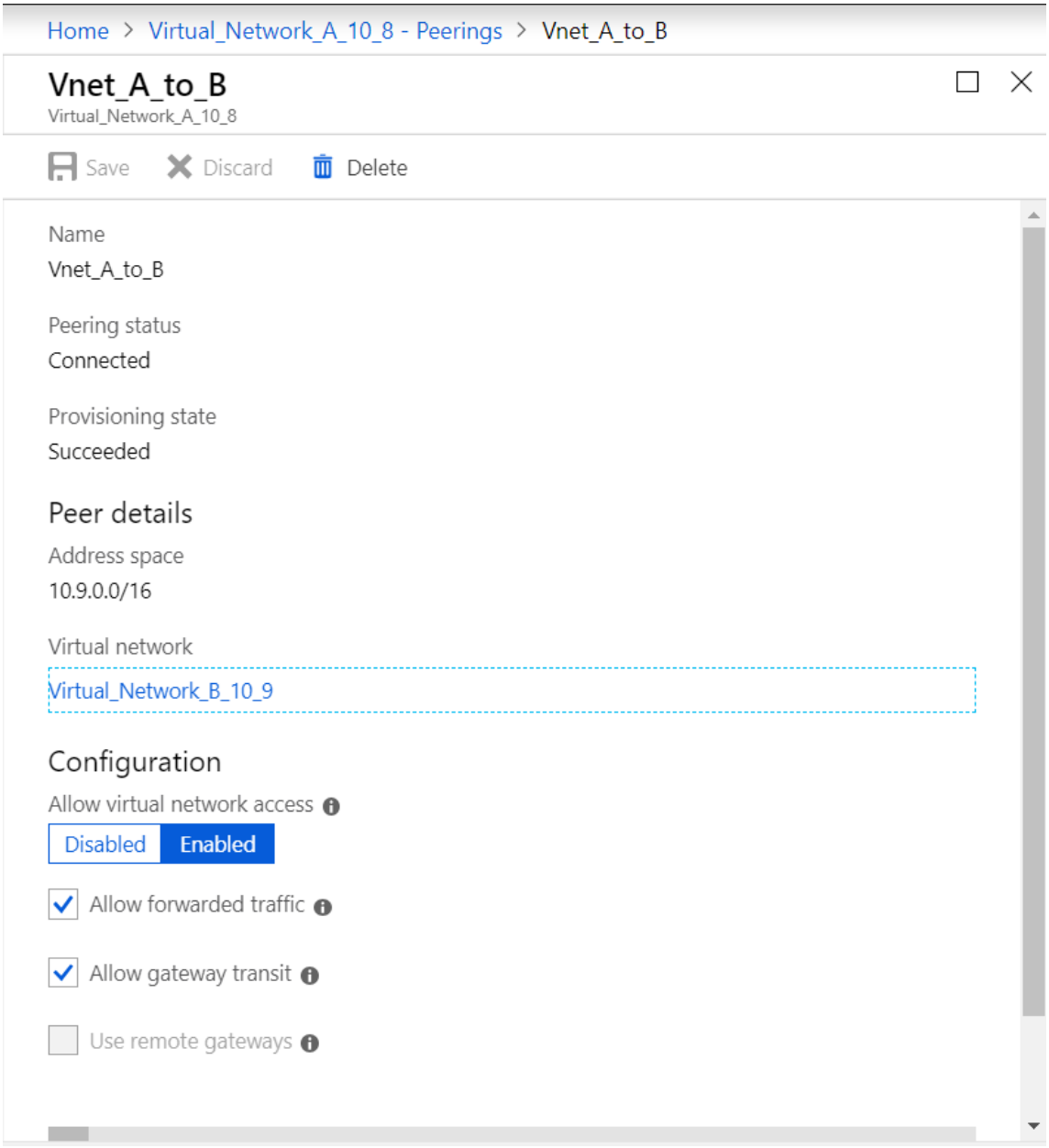
1. Erstellen Sie zwei virtuelle Netzwerke.
2. Wählen Sie dasselbe Dashboard aus, klicken Sie auf **Ressource erstellen** und suchen Sie nach virtuellen Netzwerken, um zwei virtuelle Netzwerke, nämlich VNet A und VNet B, in derselben Region zu erstellen und sie miteinander zu verbinden, um ein Hub-and-Spoke-Modell zu bilden, wie in der folgenden Abbildung gezeigt.
   Weitere Informationen zum Einrichten einer Hub-and-Spoke-Topologie finden Sie unter Implementieren einer Hub-Spoke-Netzwerktopologiein Azure.



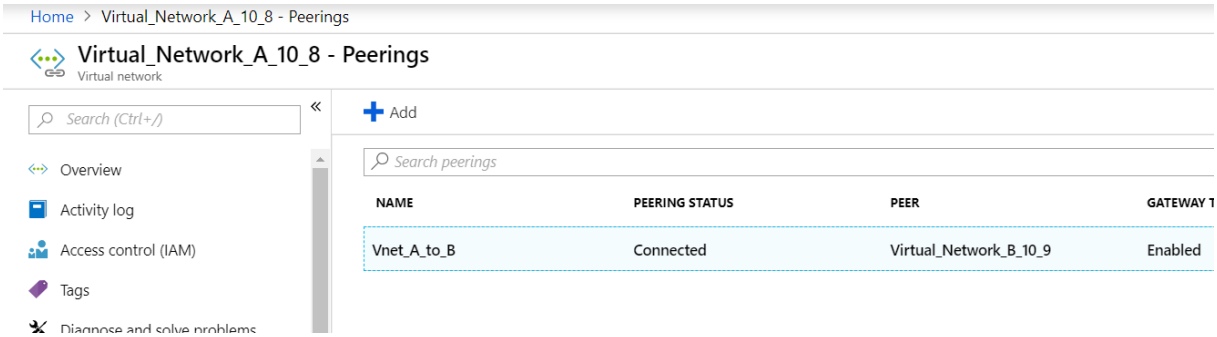
Peering von VNet A zu VNet B

Um VNet A und VNet B miteinander zu verbinden:

1. Klicken Sie im **Einstellungsmenü** von VNet A und **Peer-VNet B auf Peerings** .
2. Aktivieren **Sie Weitergeleiteten Verkehrzulassen und Gateway-Transit** zulassen, wie in der folgenden Abbildung gezeigt.



Die folgende Abbildung zeigt das erfolgreiche Peering von VNet A zu VNet B.



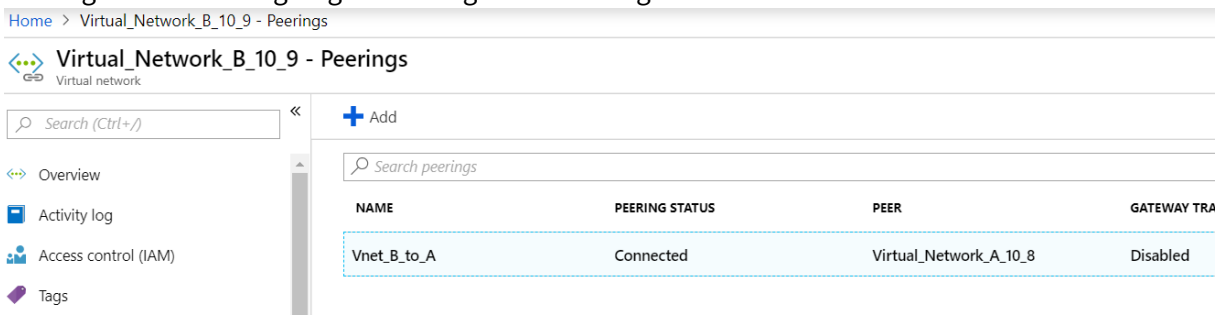
Peering von VNet B zu VNet A

Zum Peering von VNet B und VNet A:

1. Klicken Sie im **Einstellungsmenü** von VNet B und **Peer-VNet A auf Peerings** .
2. Aktivieren **Sie Weitergeleiteten Verkehr zulassen** und verwenden Sie Remote-Gateways, wie in der folgenden Abbildung gezeigt.

```
1 ![VNet B to A](/en-us/citrix-adc/media/image-07.png)
```

Die folgende Abbildung zeigt das erfolgreiche Peering von VNet B zu VNet A.



App-Server, DNS-Forwarder, Windows 10 Pro-Client und NetScaler in VNet A bereitstellen

Wir besprechen kurz den App-Server, den DNS-Forwarder, den Windows 10 Pro-Client und NetScaler auf VNet A.

1. Wählen Sie dasselbe Dashboard aus und klicken Sie **auf Ressource erstellen**.
2. Suchen Sie nach den entsprechenden Instanzen und weisen Sie eine IP aus dem VNet A-Subnetz zu.

App-Server

App-Server ist nichts anderes als der Webserver (HTTP-Server), auf dem ein Ubuntu-Server 16.04 als Instanz auf der Azure- oder lokalen VM bereitgestellt wird. Um ihn als Webserver einzurichten, geben Sie an der Befehlszeile Folgendes ein:

```
sudo apt install apache2
```

Windows 10 Pro-Client

Starten Sie die Windows 10 Pro-Instanz als Client-Computer auf VNet A und lokal.

NetScaler

NetScaler ergänzt die private Zone von Azure DNA durch Health Check und Analytics von NetScaler MAS. Starten Sie je nach Ihren Anforderungen einen NetScaler vom Azure Marketplace aus. Hier haben wir NetScaler (BYOL) für diese Bereitstellung verwendet.

Für die detaillierten Schritte zur Bereitstellung von NetScaler auf Microsoft Azure. Siehe Bereitstellen einer NetScaler VPX-Instanz auf Microsoft Azure.

Verwenden Sie nach der Bereitstellung NetScaler IP, um NetScaler GSLB zu konfigurieren.

DNS-Weiterleitung

Es wird verwendet, um die Client-Anfragen von gehosteten Domänen weiterzuleiten, die an NetScaler GSLB (ADNS IP) gebunden sind. Starten Sie einen Ubuntu-Server 16.04 als Linux-Instanz (Ubuntu-Server 16.04) und finden Sie unter der folgenden URL, wie Sie ihn als DNS-Forwarder einrichten.

> **Hinweis:**
>
> Für die Round Robin GSLB-Lastausgleichsmethode ist ein DNS-Forwarder für die Azure-Region ausreichend, aber für Static Proximity benötigen wir einen DNS-Forwarder pro virtuellem Netzwerk.

1. Ändern Sie nach der Bereitstellung der Forwarder die DNS-Servereinstellungen des virtuellen Netzwerks A von Standard auf Benutzerdefiniert mit VNet A-DNS-Forwarder-IP, wie in der folgenden Abbildung gezeigt.
2. Ändern Sie die `named.conf.options` Datei in VNet A DNS-Forwarder, um Weiterleitungsregeln für Domain (mysite.net) und Subdomain (ptm.mysite.net) zur ADNS-IP von NetScaler GSLB hinzuzufügen.
3. Starten Sie den DNS-Forwarder neu, um die in der Datei `named.conf.options`vorgenommenen Änderungen widerzuspiegeln.

DNS-Forwarder-Einstellungen für VNet A

```
    zone "mysite.net" {

                type forward;
    forwarders {
 168.63.129.16;  }
;
     }
;
    zone "ptm.mysite.net" {

        type forward;
        forwarders {
```



```
13    10.8.0.5;  }
14   ;
15       }
16   ;
17   <!--NeedCopy-->
```

> **Hinweis:**
>
> Verwenden Sie für die Zonen-IP-Adresse der Domäne („mysite.net“) die DNS-IP-Adresse Ihrer Azure-Region. Verwenden Sie für die IP-Adresse der Subdomain (“ptm.mysite.net”) Zone alle ADNS-IP-Adressen Ihrer GSLB-Instanzen.

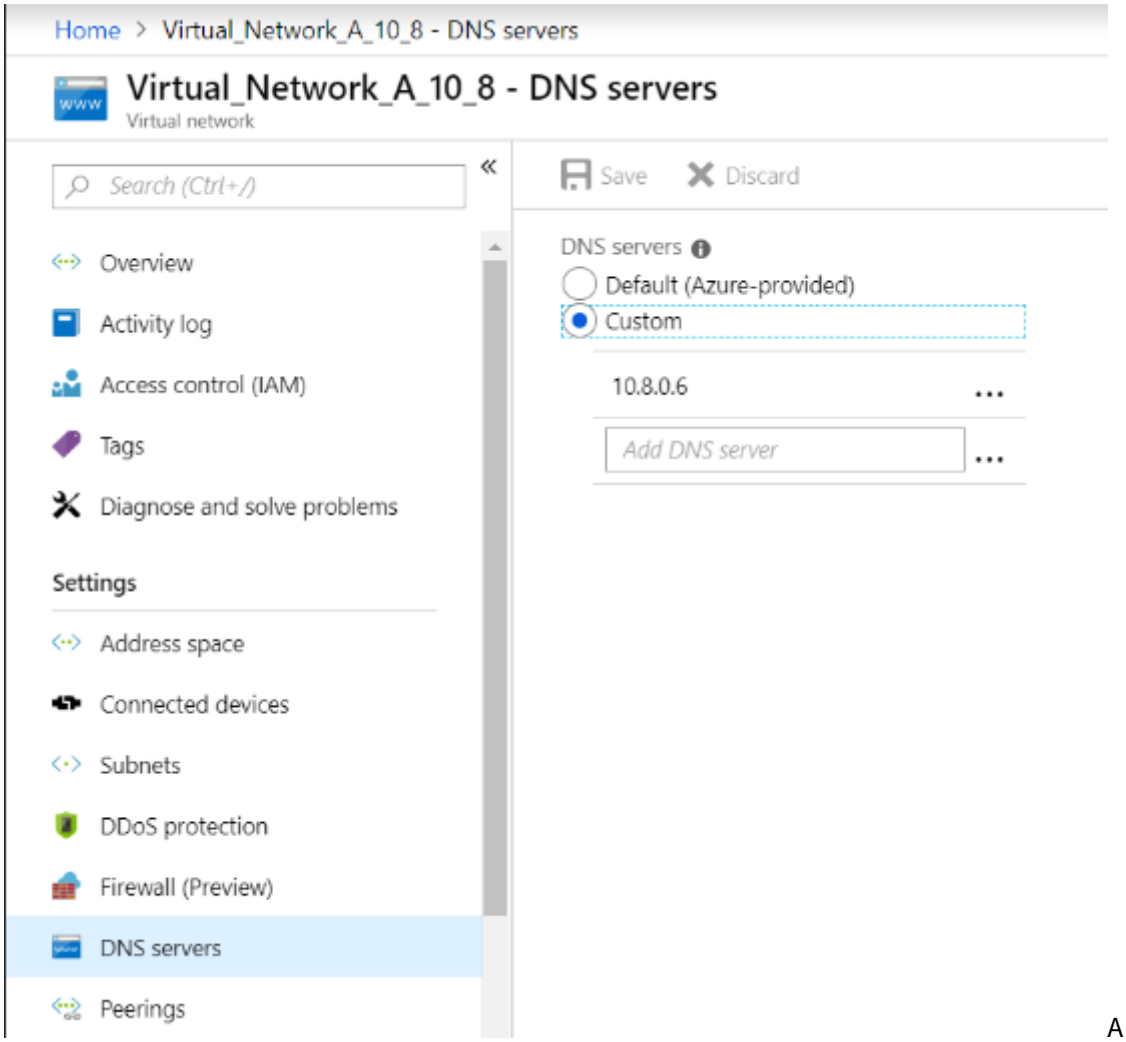
Stellen Sie einen App-Server und einen DNS-Forwarder bereit, wenn sich Clients in VNet B befinden

1. Wählen Sie für das virtuelle Netzwerk B dasselbe Dashboard aus und klicken Sie auf **Ressource erstellen**.
2. Suchen Sie nach den entsprechenden Instanzen und weisen Sie eine IP aus dem VNet B-Subnetz zu.
3. Starten Sie den App-Server und den DNS-Forwarder, wenn ein statischer Proximity-GSLB-Lastenausgleich ähnlich wie bei VNet A besteht.
4. Bearbeiten Sie die DNS-Forwarder-Einstellungen von VNet B `named.conf.options` wie in der folgenden Einstellung gezeigt:

   DNS-Forwarder-Einstellungen für VNet B:

```
1     zone "ptm.mysite.net" {
2
3         type forward;
4         forwarders {
5   10.8.0.5;  }
6   ;
7       }
8   ;
9   <!--NeedCopy-->
```

Die folgende Abbildung zeigt die DNS-Forwarder-Einstellungen von VNet B:



A DNS-Server

App-Server, DNS-Forwarder und Windows 10 Pro-Client lokal bereitstellen

1. Starten Sie für lokale Umgebungen die VMs auf Bare Metal und verwenden Sie den App-Server, den DNS-Forwarder und den Windows 10 Pro-Client, der VNet A ähnelt.
2. Bearbeiten Sie die lokalen DNS-Forwarder-Einstellungen `named.conf.options` wie im folgenden Beispiel gezeigt.

Lokale DNS-Forwarder-Einstellungen

```
1     zone "mysite.net" {
2
3                 type forward;
4                 forwarders {
5   10.8.0.6;  }
```



```
6   ;
7       }
8   ;
9      zone "ptm.mysite.net" {
10
11          type forward;
12          forwarders {
13    10.8.0.5;  }
14  ;
15      }
16  ;
17  <!--NeedCopy-->
```

Denn `mysite.net`wir haben die DNS-Forwarder-IP von VNet A anstelle der IP des privaten DNS-Zonenservers von Azure angegeben, da es sich um eine spezielle IP-Adresse handelt, die von lokal aus nicht erreichbar ist. Daher ist diese Änderung in der DNS-Forwarder-Einstellung von On-premises erforderlich.

Konfigurieren Sie den NetScaler im virtuellen Azure-Netzwerk

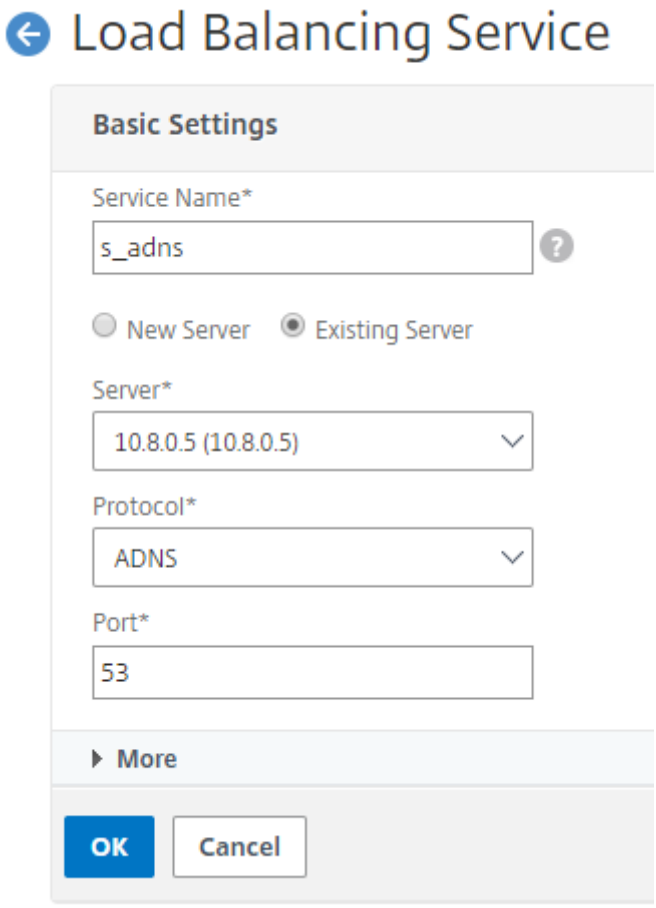
Wie in der Topologie gezeigt, stellen Sie NetScaler im virtuellen Azure-Netzwerk (in diesem Fall VNet A) bereit und greifen Sie über die NetScaler-GUI darauf zu.

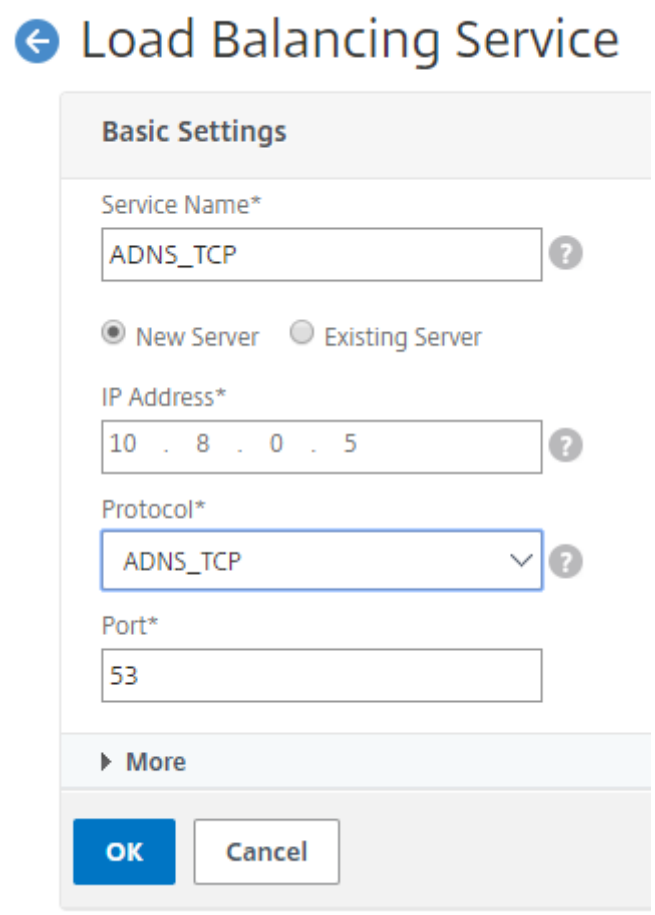
Konfiguration von NetScaler GSLB

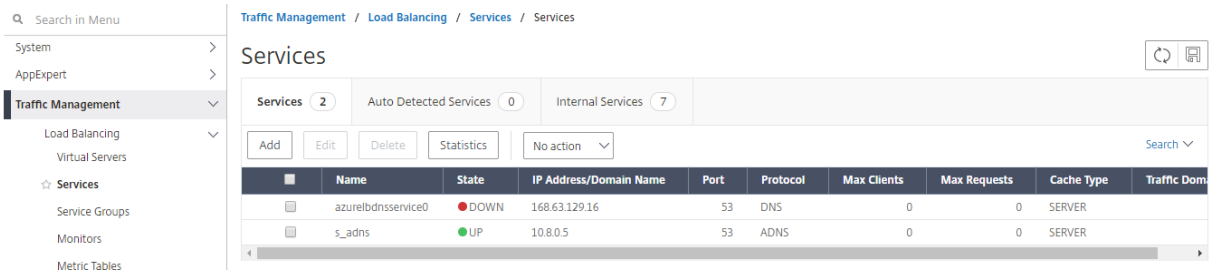
1. Erstellen Sie einen ADNS-Dienst.
2. Erstellen Sie lokale und Remote-Sites.
3. Erstellen Sie Dienste für die lokalen virtuellen Server.
4. Erstellen Sie virtuelle Server für die GSLB-Dienste.

ADNS-Dienst hinzufügen

1. Melden Sie sich bei der NetScaler-GUI an.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > Load Balancing > Services**.
3. Fügen Sie einen Dienst hinzu.
   Wir empfehlen Ihnen, den ADNS-Dienst sowohl in TCP als auch in UDP zu konfigurieren, wie in der folgenden Abbildung gezeigt:

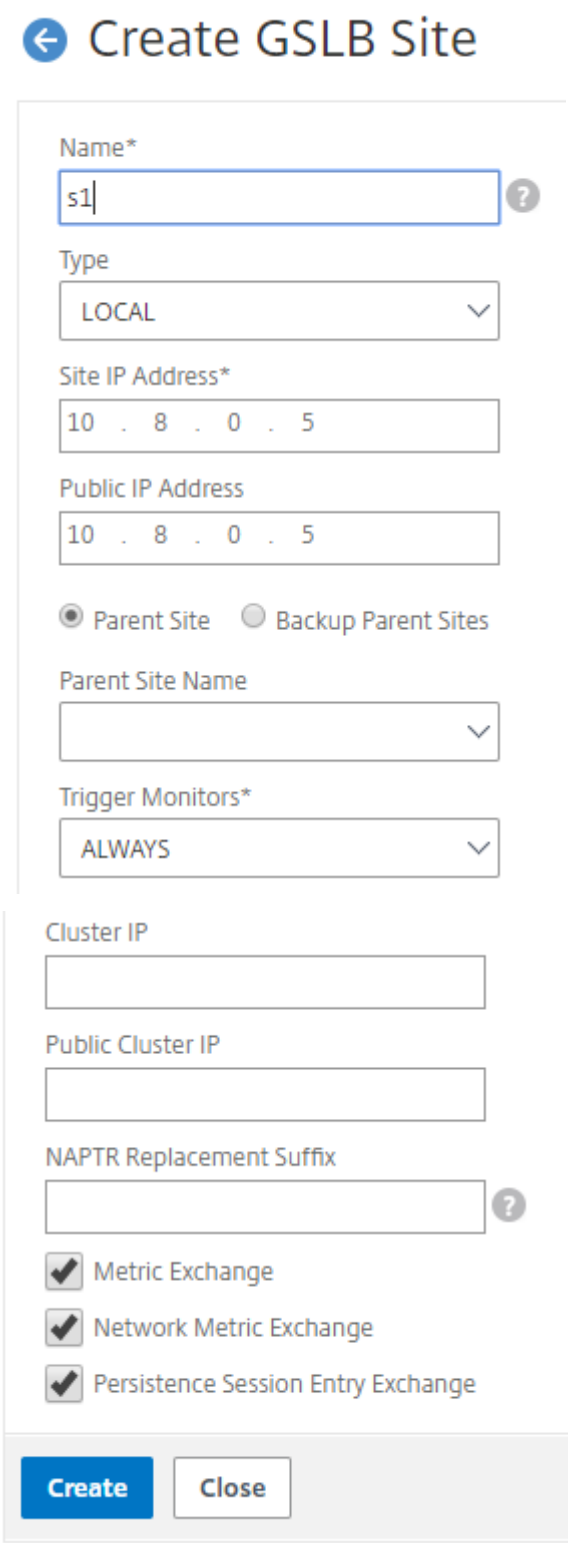


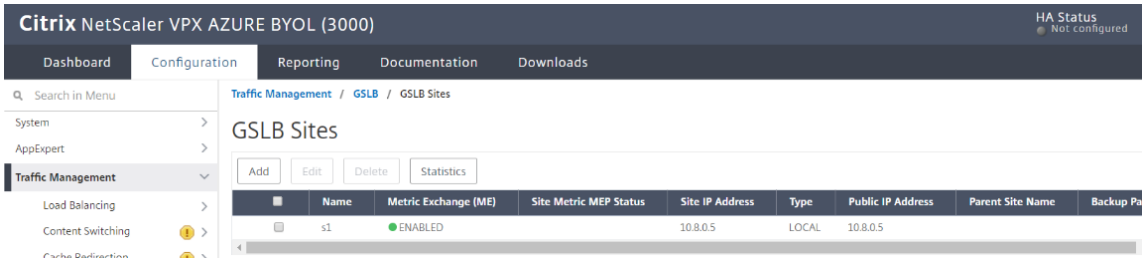




GSLB-Sites hinzufügen

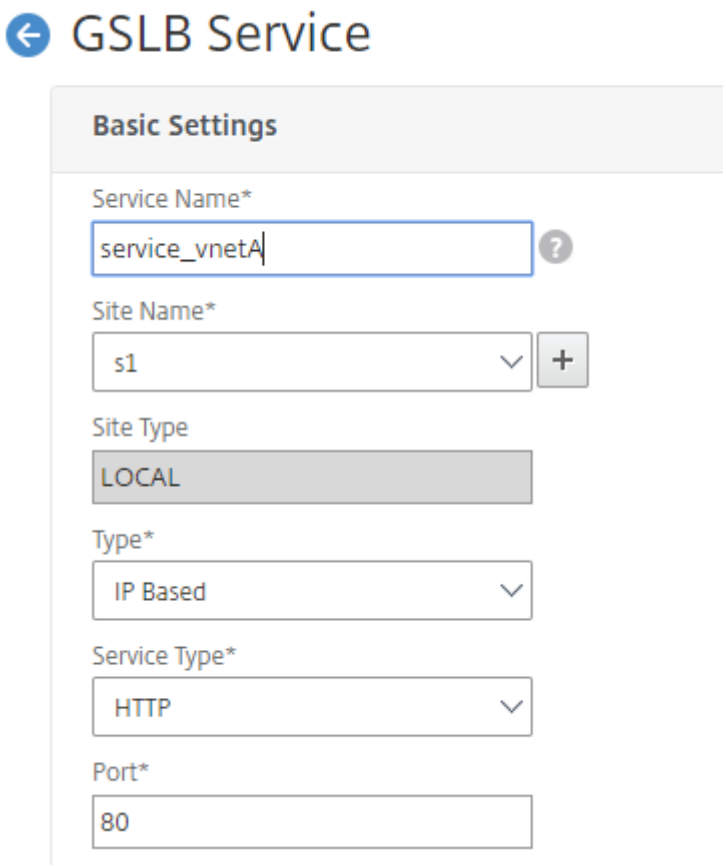
1. Fügen Sie lokale und Remote-Sites hinzu, zwischen denen GSLB konfiguriert wird.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Datenverkehrsverwaltung > GSLB > GSLB-Sites** .
   Fügen Sie eine Site hinzu, wie im folgenden Beispiel gezeigt, und wiederholen Sie das gleiche Verfahren für andere Sites.

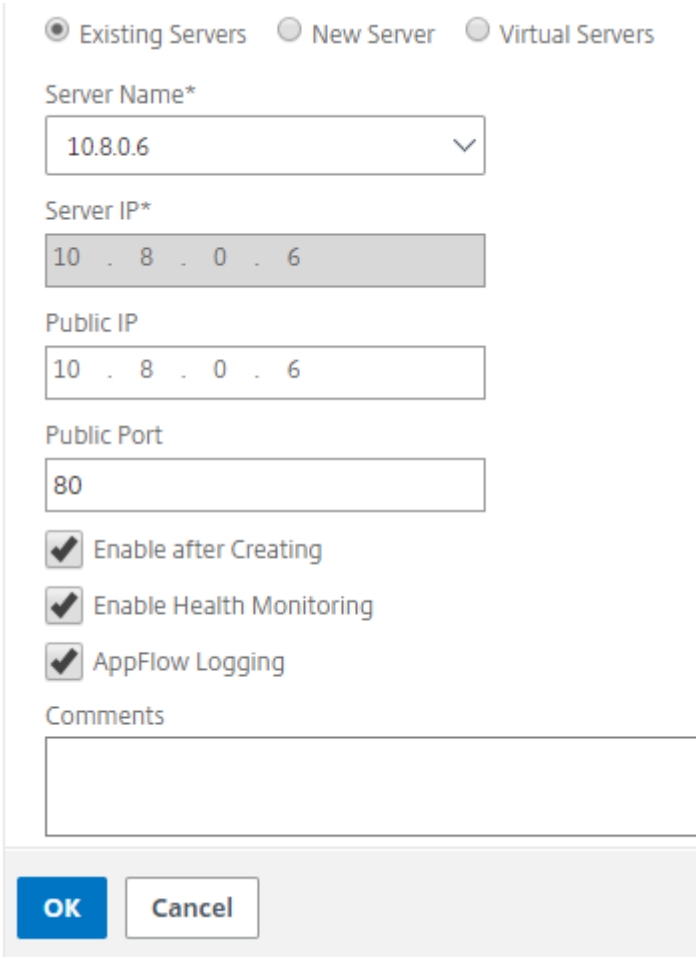




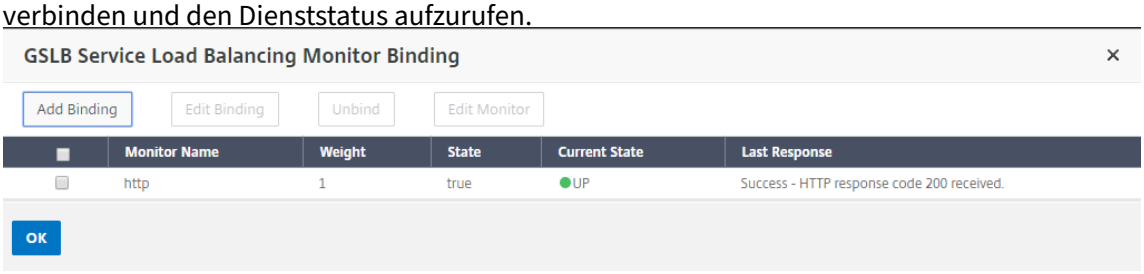
GSLB-Dienste hinzufügen

1. Fügen Sie GSLB-Dienste für die lokalen und virtuellen Remote-Server hinzu, die den Lastenausgleich für App-Server ermöglichen.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > GSLB > GSLB Services**.
3. Fügen Sie die Dienste wie in den folgenden Beispielen gezeigt hinzu.
4. Binden Sie den HTTP-Monitor, um den Serverstatus zu überprüfen.





5. Nachdem Sie den Dienst erstellt haben, wechseln Sie im GSLB-Dienst zur Registerkarte **Erweiterte Einstellungen** .
6. Klicken Sie auf **Monitor hinzufügen**, um den GSLB-Dienst mit einem HTTP-Monitor zu verbinden und den Dienststatus aufzurufen.

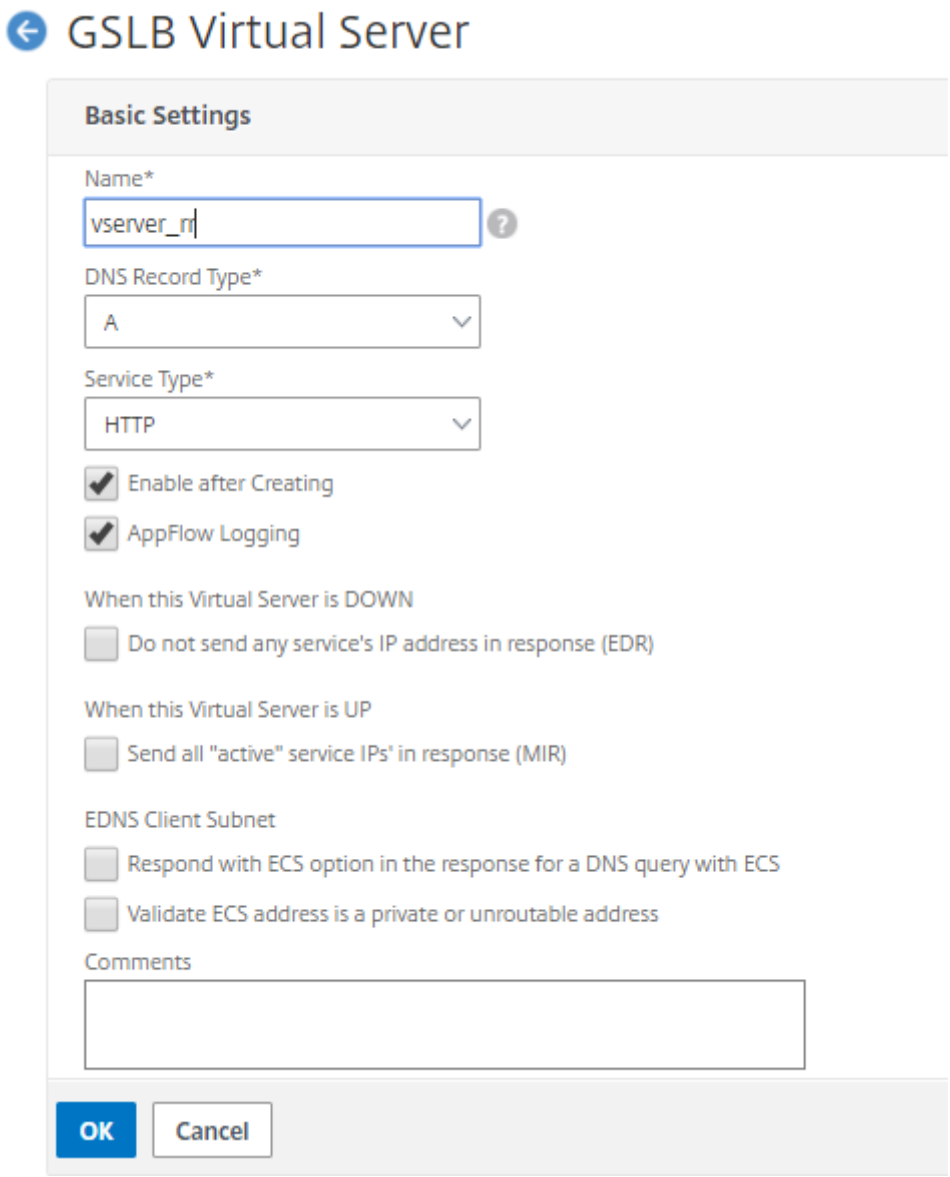


7. Sobald Sie sich mit dem HTTP-Monitor verbinden, wird der Status der Dienste als UP markiert, wie in der folgenden Abbildung gezeigt:

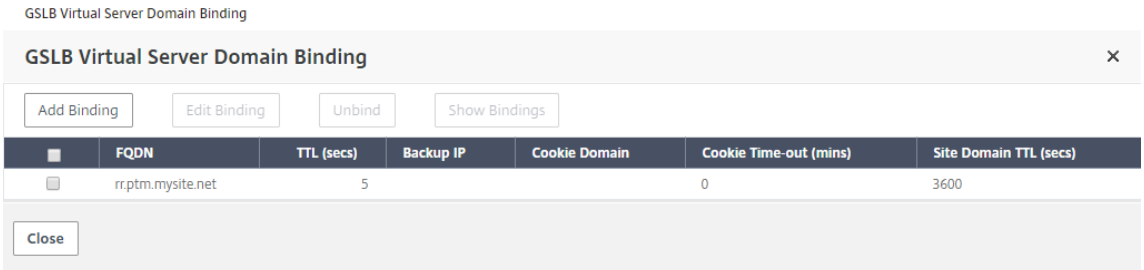
Virtuellen GSLB-Server hinzufügen

Fügen Sie einen virtuellen GSLB-Server hinzu, über den auf die Alias-GSLB-Dienste der App-Server zugegriffen werden kann.

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > GSLB > GSLB Virtual Servers**.
2. Fügen Sie die virtuellen Server hinzu, wie im folgenden Beispiel gezeigt.
3. Binden Sie GSLB-Dienste und den Domainnamen daran.



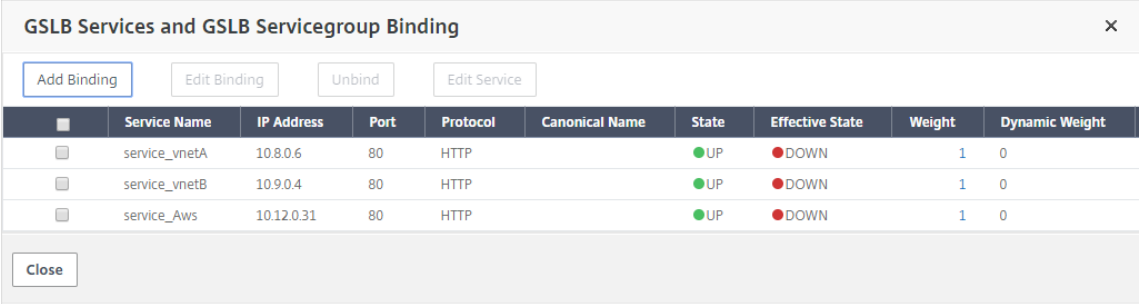
4. Nachdem Sie den virtuellen GSLB-Server erstellt und die entsprechende Lastausgleichsmethode ausgewählt haben (in diesem Fall Round Robin), binden Sie GSLB-Dienste und -Domänen, um den Schritt abzuschließen.



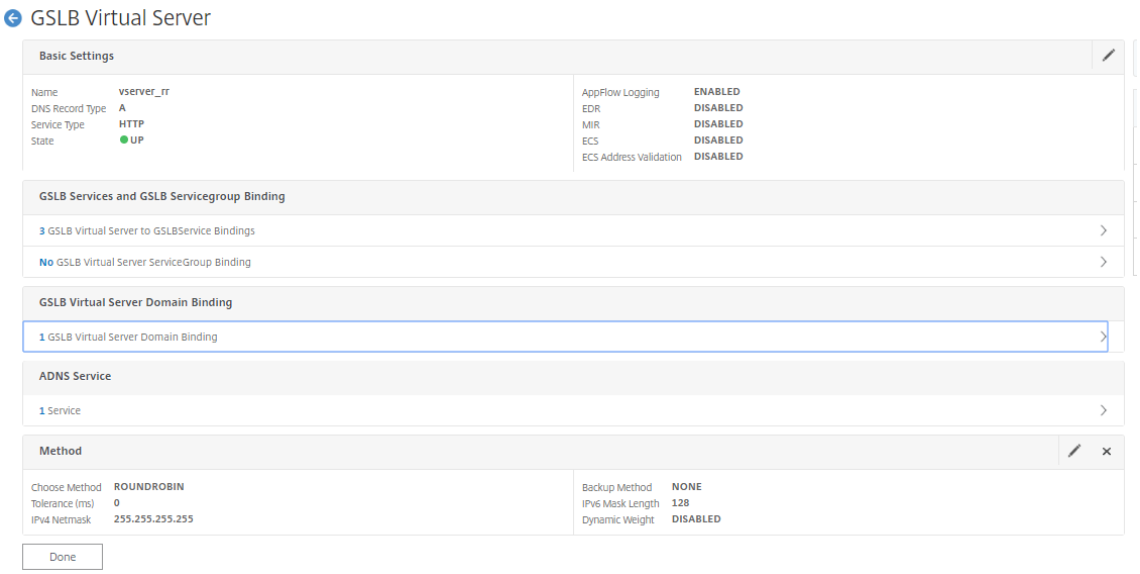
5. Gehen Sie auf dem virtuellen Server zur Registerkarte **Erweiterte Einstellungen** und klicken

Sie auf die Registerkarte **Domänen hinzufügen**, um eine Domain zu binden.

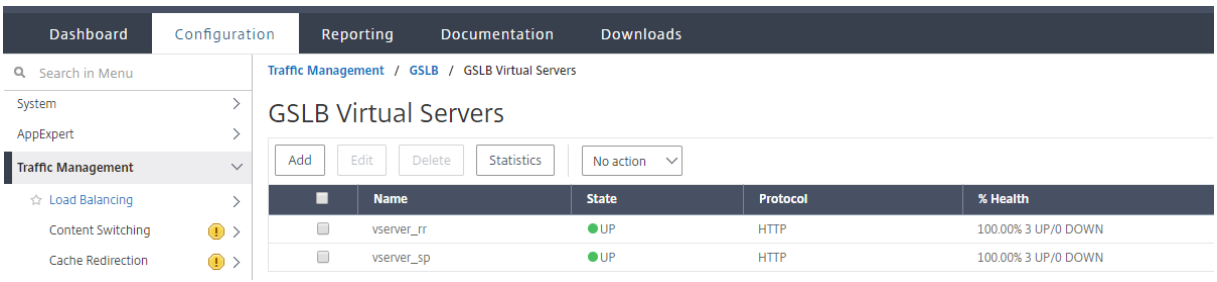
6. Gehen Sie zu **Advanced > Services** und klicken Sie auf den Pfeil, um einen GSLB-Dienst zu binden und alle drei Dienste (VNet A, VNet B, On-Premise) an den virtuellen Server zu binden.



Nach dem Binden der GSLB-Dienste und der Domäne an den virtuellen Server wird es wie in der folgenden Abbildung dargestellt angezeigt:



Überprüfen Sie, ob der virtuelle GSLB-Server aktiv und zu 100% fehlerfrei ist. Wenn der Monitor anzeigt, dass der Server aktiv und fehlerfrei ist, bedeutet dies, dass die Websites synchronisiert sind und Back-End-Dienste verfügbar sind.



Um die Bereitstellung zu testen, greifen Sie entweder `rr.ptm.mysite.net` vom Cloud-Client-Computer oder vom lokalen Client-Computer auf die Domain-URL zu. Wenn Sie über einen

Cloud-Windows-Client-Computer darauf zugreifen, stellen Sie sicher, dass auf den on-premises App-Server in einer privaten DNS-Zone zugegriffen wird, ohne dass DNS-Lösungen von Drittanbietern oder benutzerdefinierte DNS-Lösungen erforderlich sind.

Konfigurieren Sie eine NetScaler VPX-Instanz für die Verwendung von Azure Accelerated Networking

September 11, 2023

Accelerated Networking ermöglicht die virtuelle Funktions- (VF) -Netzwerkkarte (Single Root I/O Virtualization, SR-IOV) für eine virtuelle Maschine, wodurch die Netzwerkleistung verbessert wird. Sie können diese Funktion bei hohen Workloads verwenden, bei denen Daten mit höherem Durchsatz bei zuverlässigem Streaming und geringerer CPU-Auslastung gesendet oder empfangen werden müssen.
Wenn eine NIC mit beschleunigter Vernetzung aktiviert ist, bündelt Azure die vorhandene para-virtualisierte (PV) -Schnittstelle der NIC mit einer SR-IOV VF-Schnittstelle. Die Unterstützung der SR-IOV VF-Schnittstelle ermöglicht und verbessert den Durchsatz der NetScaler VPX-Instanz.

Accelerated Networking bietet die folgenden Vorteile:

- Niedrigere Latenz
- Höhere Leistung von Paketen pro Sekunde (pps)
- Verbesserter Durchsatz
- Reduzierter Jitter
- Verminderte CPU-Auslastung

> Hinweis
>
> Azure Accelerated Networking wird auf NetScaler VPX-Instanzen ab Version 13.0 Build 76.29 unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass Ihre VM-Größe den Anforderungen für Azure Accelerated Networking entspricht.
- Stoppen Sie VMs (einzeln oder in einem Verfügbarkeitssatz), bevor Sie beschleunigtes Netzwerk auf einer beliebigen Netzwerkkarte aktivieren.

Einschränkungen

Accelerated Networking kann nur für einige Instance-Typen aktiviert werden. Weitere Informationen finden Sie unter Unterstützte Instance-Typen.

Unterstützte NICs für beschleunigtes Networking

Azure bietet Mellanox ConnectX3-, ConnectX4- und ConnectX5-NICs im SR-IOV-Modus für beschleunigte Netzwerke.

Wenn Accelerated Networking auf einer NetScaler VPX-Schnittstelle aktiviert ist, bündelt Azure entweder die ConnectX3-, ConnectX4- oder ConnectX5-Schnittstelle mit der vorhandenen PV-Schnittstelle einer NetScaler VPX-Appliance.

Weitere Informationen zum Aktivieren von Accelerated Networking vor dem Anfügen einer Schnittstelle an eine VM finden Sie unter Erstellen einer Netzwerkschnittstelle mit beschleunigtem Netzwerk.

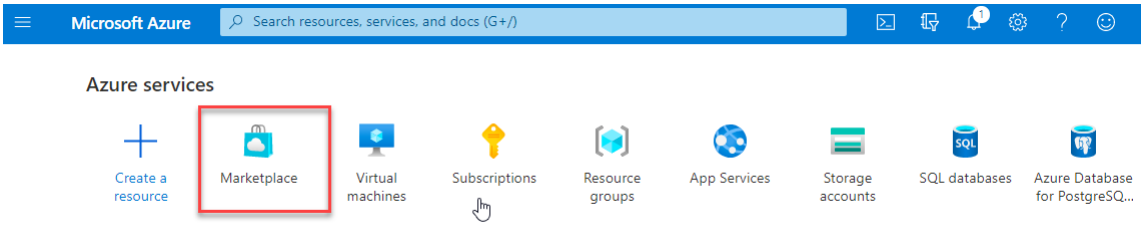
Weitere Informationen zum Aktivieren von beschleunigten Netzwerken auf einer vorhandenen Schnittstelle auf einer VM finden Sie unter Aktivieren vorhandener Schnittstellen auf einer VM.

So aktivieren Sie beschleunigtes Networking auf einer NetScaler VPX-Instanz mithilfe der Azure-Konsole

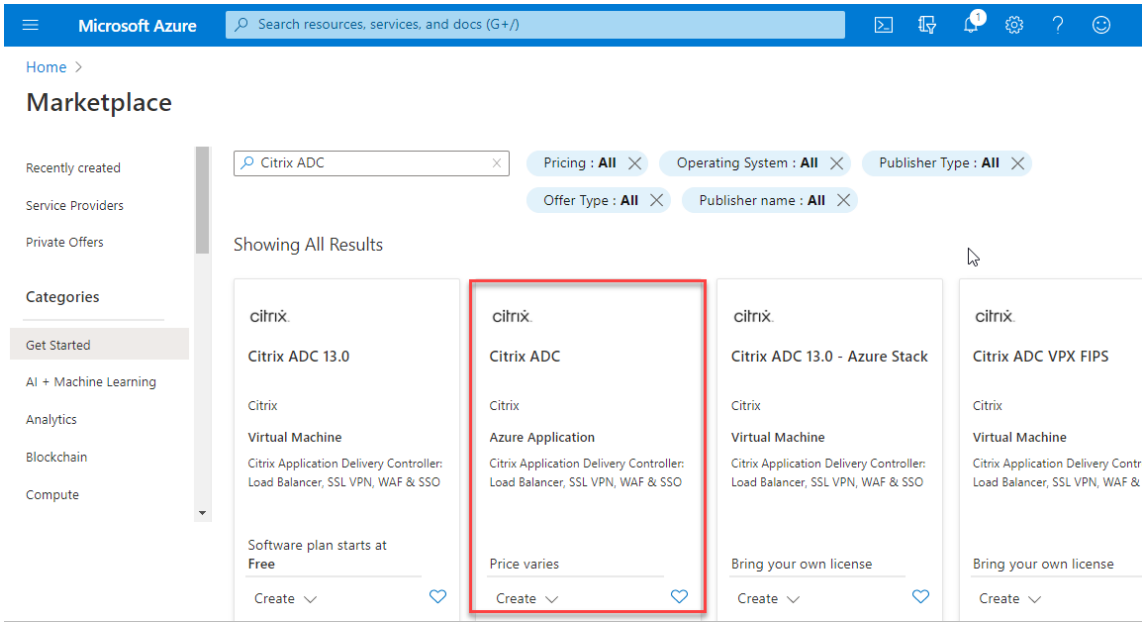
Sie können beschleunigte Netzwerke auf einer bestimmten Schnittstelle mithilfe der Azure-Konsole oder der Azure PowerShell aktivieren.

Gehen Sie wie folgt vor, um beschleunigtes Networking mithilfe von Azure-Verfügbarkeitssätzen oder Availability Zones zu aktivieren.

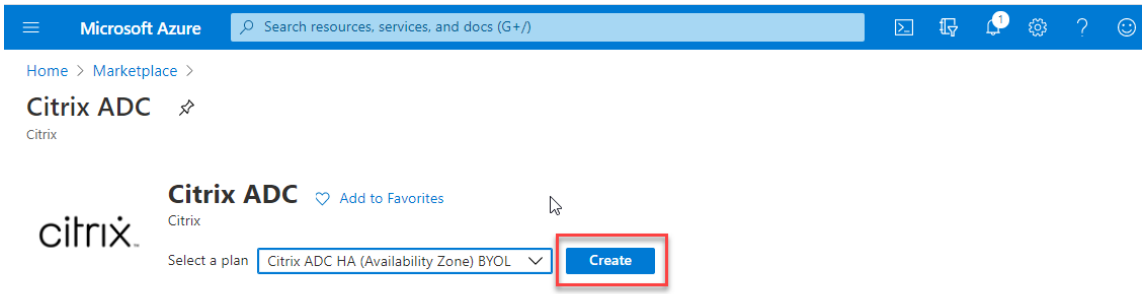
1. Melden Sie sich beim Azure-Portalan und navigieren Sie zu **Azure Marketplace**.



2. Suchen Sie im **Azure Marketplace** nach **NetScaler**.

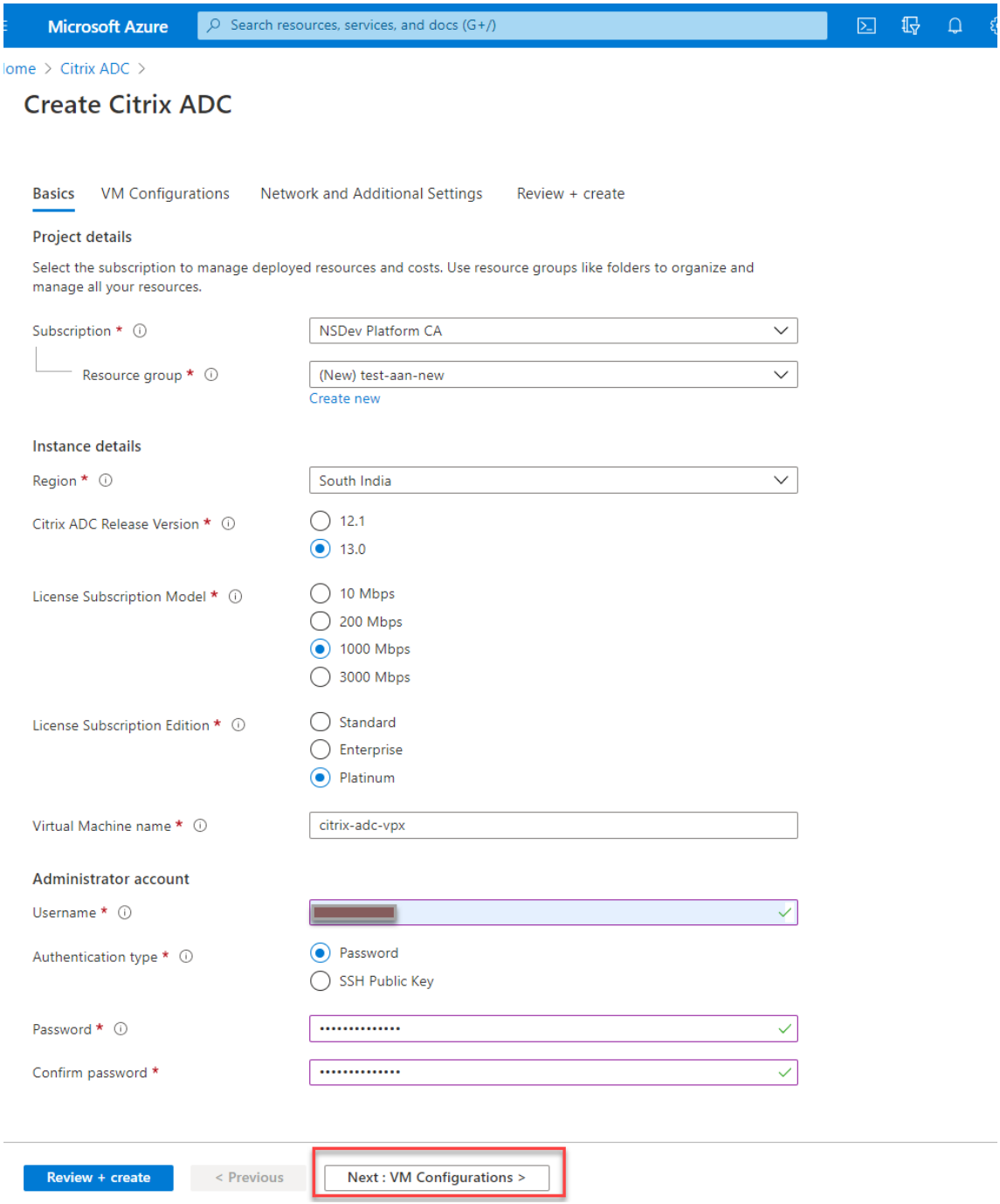


3. Wählen Sie einen NetScaler-Plan ohne FIPS zusammen mit der Lizenz aus und klicken Sie auf **Erstellen**.



Die Seite **NetScaler erstellen** wird angezeigt.

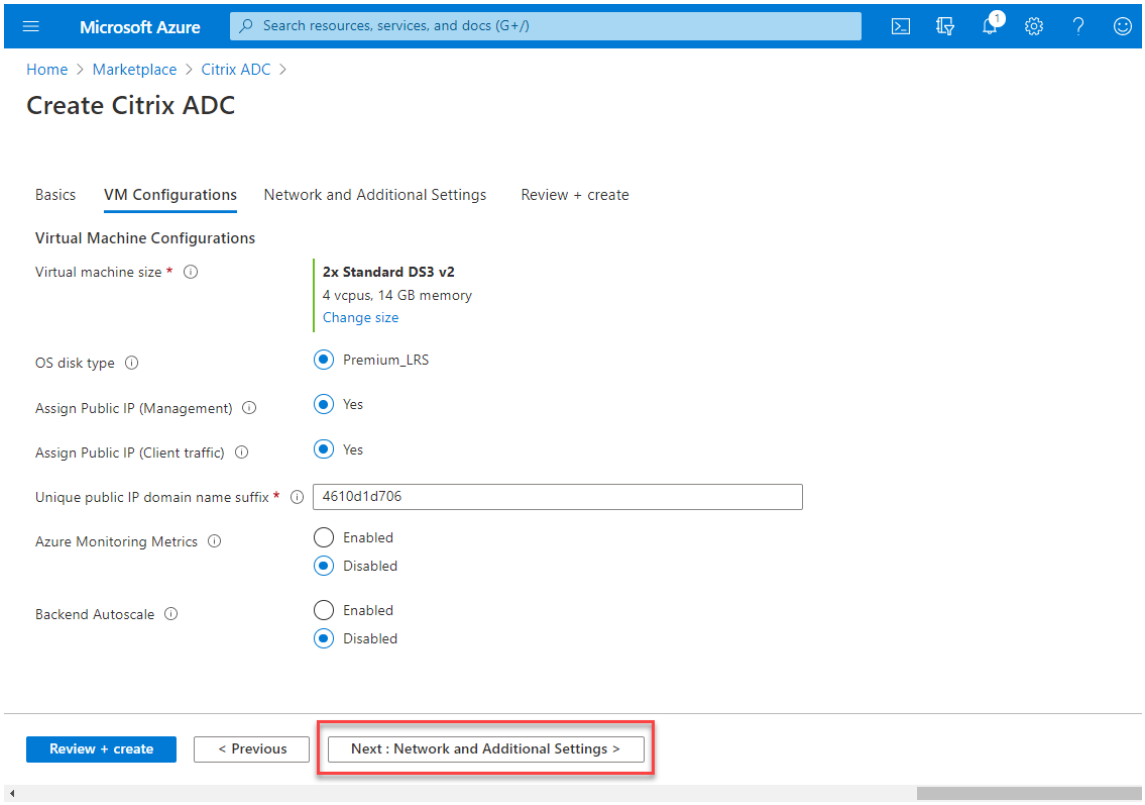
4. Erstellen Sie auf der Registerkarte **Grundlagen** eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Felder Region, Admin-Benutzername, Admin-Kennwort, Lizenztyp (VM SKU) und andere ein.



5. Klicken Sie auf **Weiter: VM-Konfigurationen**.

   Führen Sie auf der Seite **VM-Konfigurationen** die folgenden Schritte aus:

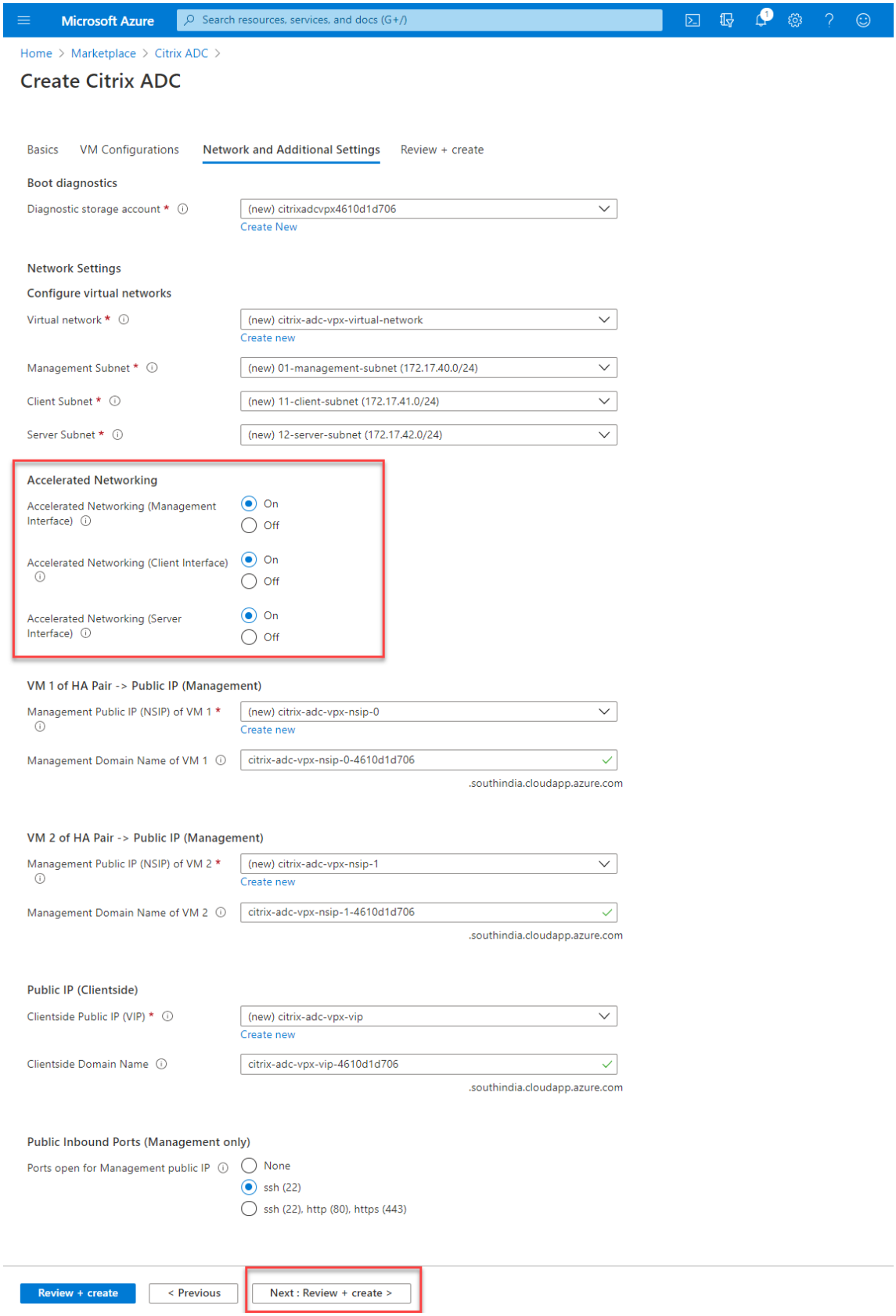
   a) Konfigurieren Sie ein öffentliches IP-Domänennamensuffix.
   b) Aktivieren oder deaktivieren Sie **Azure Monitoring-Metriken**.
   c) Aktivieren oder deaktivieren Sie **Backend Autoscale**.



6. Klicken Sie auf **Weiter: Netzwerk und Zusätzliche Einstellungen**.

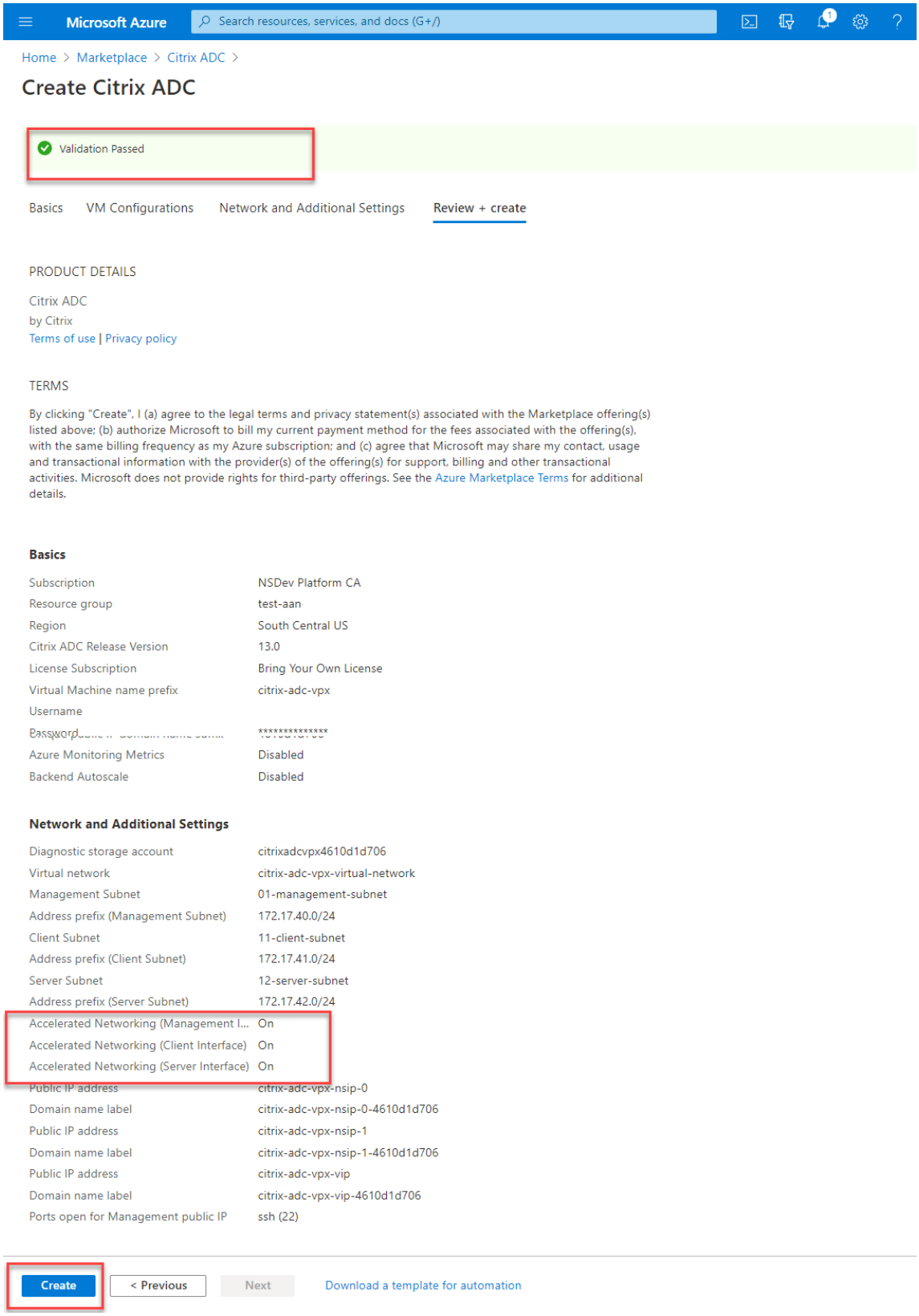
   Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Boot-Diagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.

   Im Abschnitt **Accelerated Networking** haben Sie die Möglichkeit, das beschleunigte Netzwerk separat für die Verwaltungsschnittstelle, die Client-Schnittstelle und die Serverschnittstelle zu aktivieren oder zu deaktivieren.



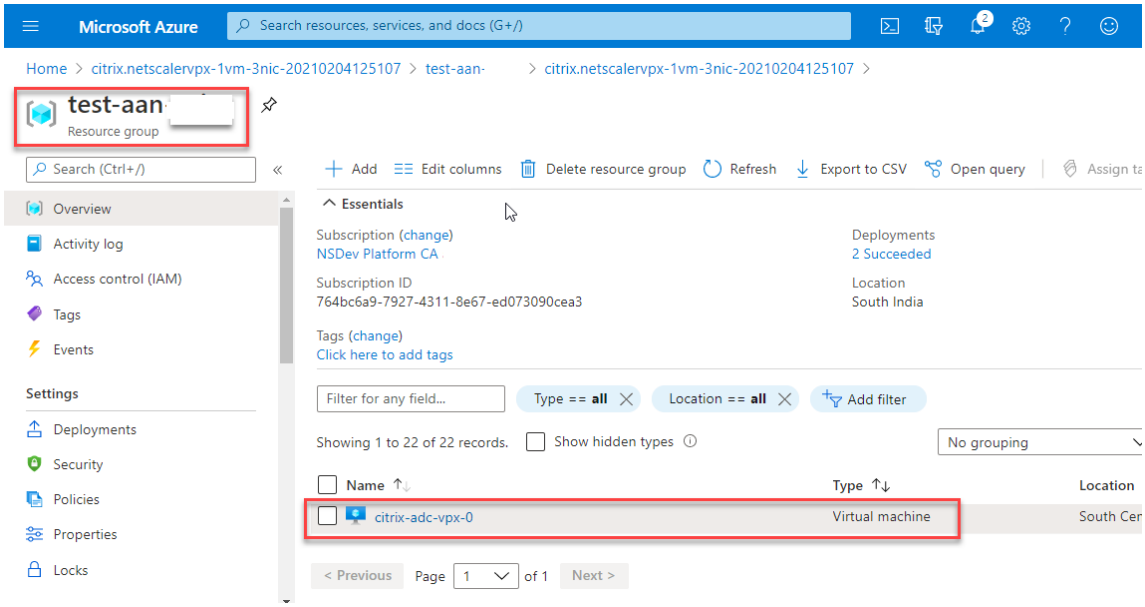
7. Klicken Sie auf **Weiter: Überprüfen + erstellen**.

   Überprüfen Sie nach erfolgreicher Validierung die Grundeinstellungen, VM-Konfigurationen, das Netzwerk und zusätzliche Einstellungen und klicken Sie auf **Erstellen**. Es kann einige Zeit dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt ist.

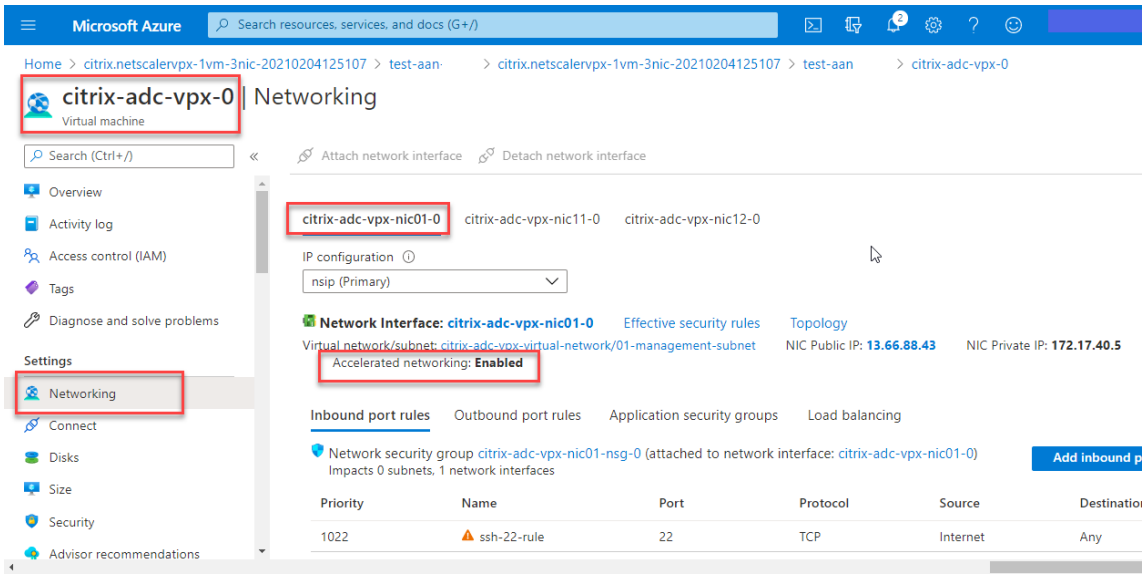


8. Wählen Sie nach Abschluss der Bereitstellung die **Ressourcengruppe** aus, um die Konfigura-

tionsdetails zu sehen.



9. Um die Konfigurationen für beschleunigte Netzwerke zu überprüfen, wählen Sie **Virtuelle Maschine > Netzwerk**aus. Der Status “Beschleunigtes Netzwerk” wird für jede Netzwerkkarte als **Aktiviert oder**Deaktiviert** angezeigt.



Aktivieren Sie beschleunigtes Networking mit Azure PowerShell

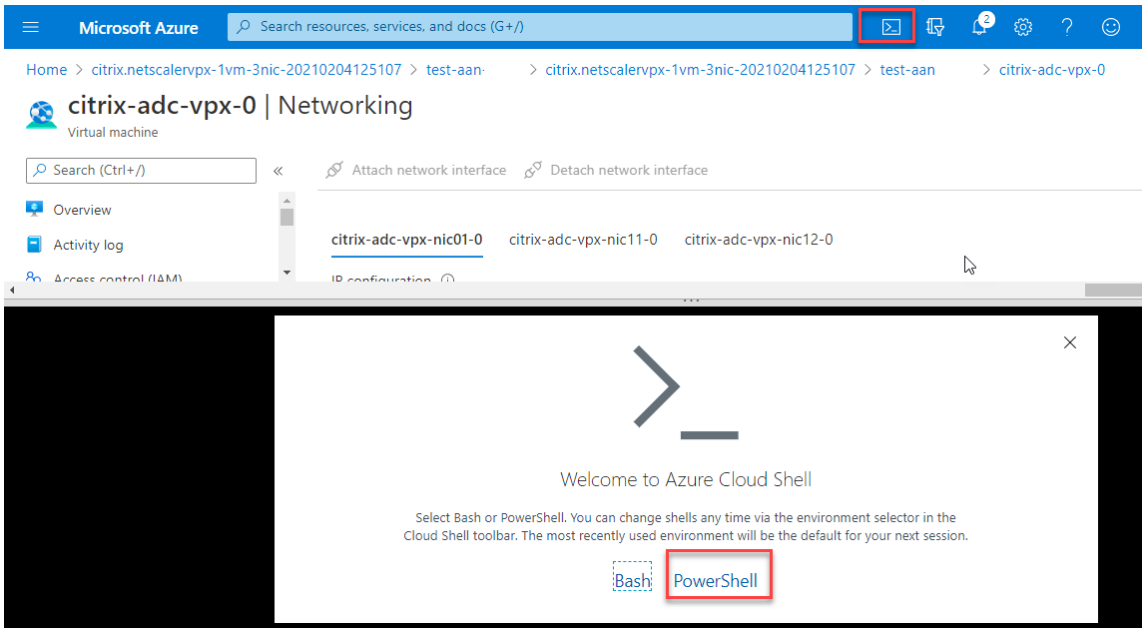
Wenn Sie nach der VM-Erstellung beschleunigte Netzwerke aktivieren müssen, können Sie dies mit Azure PowerShell tun.

> Hinweis:
>
> Stellen Sie sicher, dass Sie die VM beenden, bevor Sie Accelerated Networking mit Azure PowerShell aktivieren.

Führen Sie die folgenden Schritte aus, um beschleunigtes Networking mithilfe von Azure PowerShell zu aktivieren.

1. Navigieren Sie zum **Azure-Portal**und klicken Sie auf das **PowerShell-Symbol** in der rechten oberen Ecke.

   > Hinweis:
   >
   > Wenn Sie sich im Bash-Modus befinden, wechseln Sie in den PowerShell-Modus.



2. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
az network nic update --name <nic-name> --accelerated-networking [true | false] --resource-group <resourcegroup-name>
<!--NeedCopy-->
```

   Der Parameter Accelerated Networking akzeptiert einen der folgenden Werte:

   - **True:** Aktiviert beschleunigtes Netzwerk auf der angegebenen NIC.
   - **False:** Deaktiviert das beschleunigte Netzwerk auf der angegebenen Netzwerkkarte.

   So aktivieren Sie beschleunigtes Netzwerk auf einer bestimmten NIC:

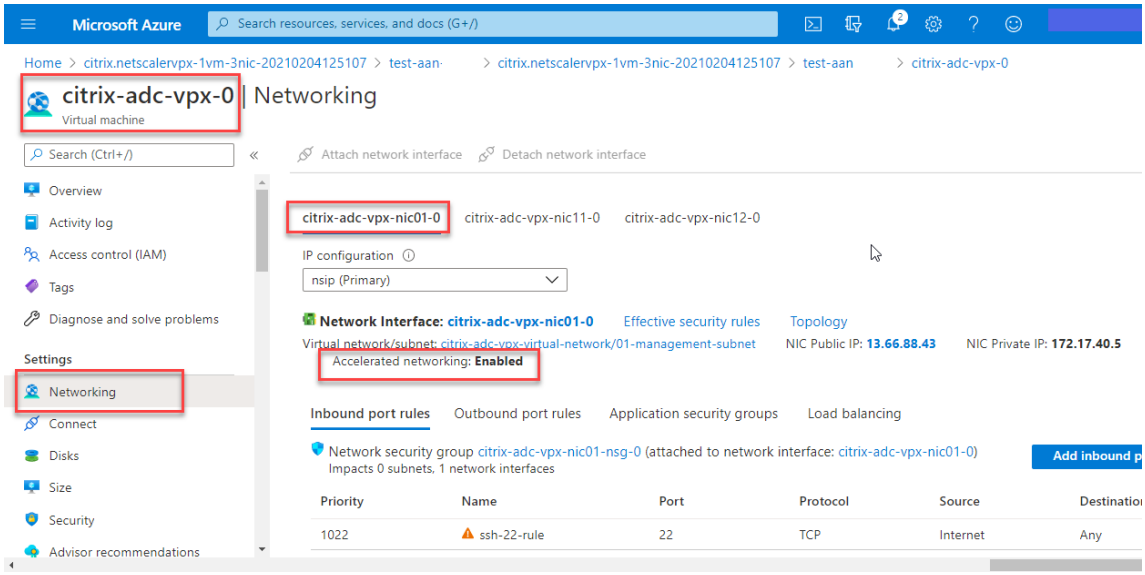
```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking true --resource-group rsgp1-aan
<!--NeedCopy-->
```


So deaktivieren Sie das beschleunigte Netzwerk auf einer bestimmten NIC:

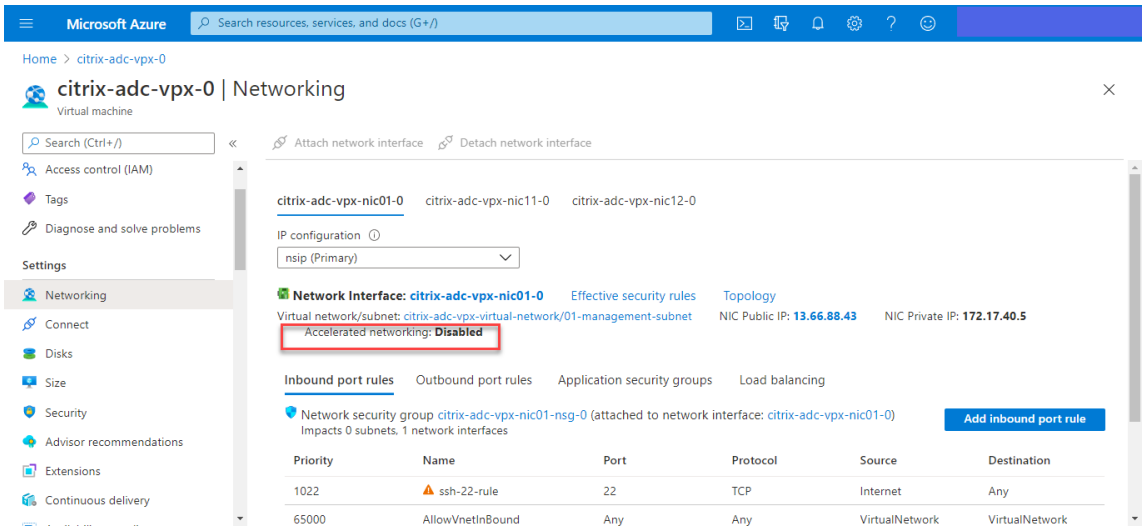
```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking false --resource-group rsgp1-aan
<!--NeedCopy-->
```

3. Um zu überprüfen, ob der Status Beschleunigtes Netzwerk nach Abschluss der Bereitstellung angezeigt wird, navigieren Sie zu **VM > Netzwerk**.

   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **aktiviert**ist.



   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **deaktiviert**ist.



Um beschleunigte Netzwerke auf einer Schnittstelle mithilfe der FreeBSD-Shell von NetScaler zu überprüfen

Sie können sich bei der FreeBSD-Shell von NetScaler anmelden und die folgenden Befehle ausführen, um den Status des beschleunigten Netzwerks zu überprüfen.

Beispiel für ConnectX3 NIC:

Das folgende Beispiel zeigt die Befehlsausgabe „ifconfig“ der Mellanox ConnectX3-NIC. Das „50/n“ steht für die VF-Schnittstellen der Mellanox ConnectX3-NICs. 0/1 und 1/1 stehen für die PV-Schnittstellen der NetScaler VPX-Instanz. Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX3-VF-Schnittstelle (50/1) dieselben MAC-Adressen haben (00:22:48:1 c: 99:3 e). Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind.


```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

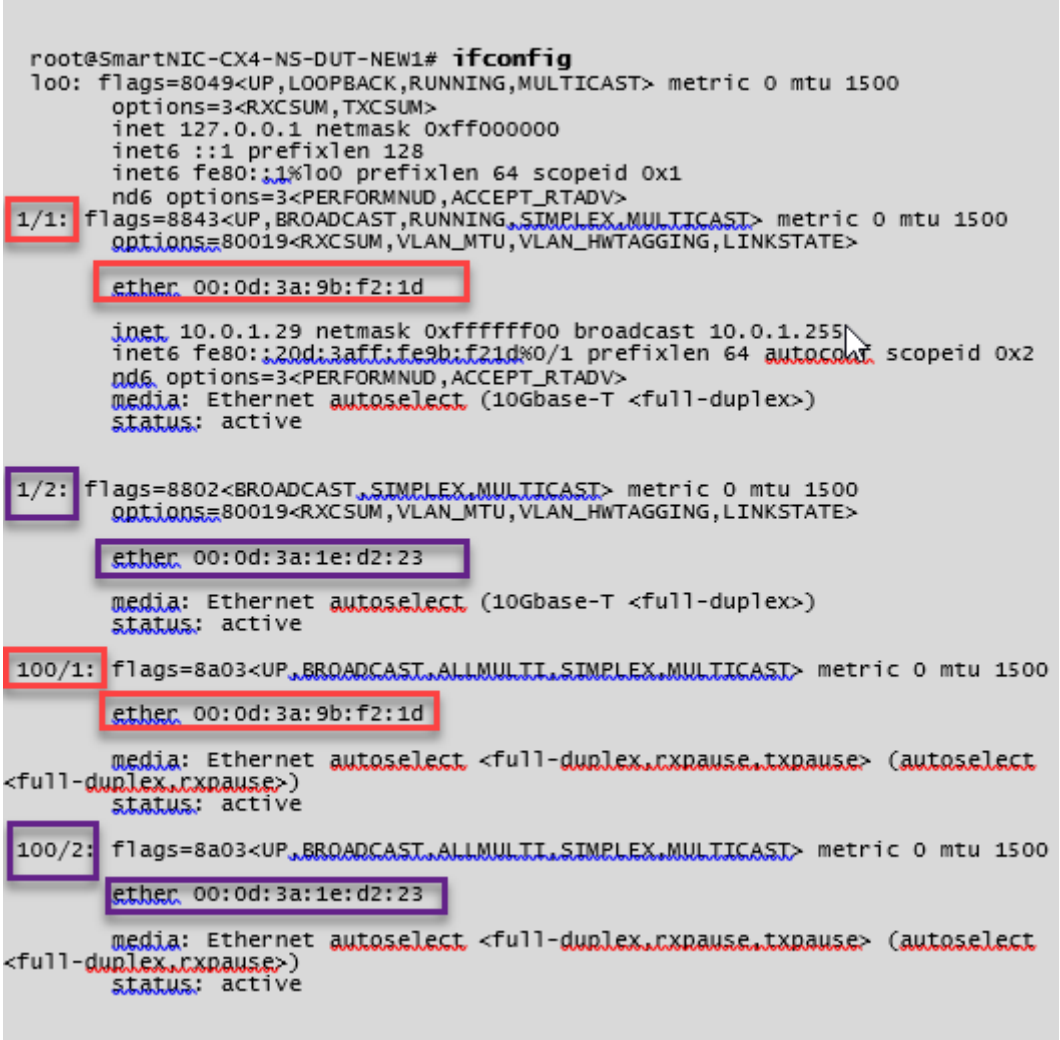
options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

Beispiel für ConnectX4 NIC:

Das folgende Beispiel zeigt die Befehlsausgabe „ifconfig“ der Mellanox ConnectX4-NIC. Das „100/n“ steht für die VF-Schnittstellen der Mellanox ConnectX4-NICs. 0/1, 1/1 und 1/2 stehen für die PV-Schnittstellen der NetScaler VPX-Instanz.

Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX4-VF-Schnittstelle (100/1) dieselben MAC-Adressen haben (00:0d:3a:9b:f2:1d). Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind. In ähnlicher Weise haben die PV-Schnittstelle (1/2) und die

CX4-VF-Schnittstelle (100/2) dieselben MAC-Adressen (00:0 d:3a:1e:d 2:23).



Um beschleunigte Netzwerke auf einer Schnittstelle mithilfe von ADC CLI zu überprüfen

Beispiel für ConnectX3 NIC:

Die folgende Befehlsausgabe zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 50/1 gebündelt ist, bei der es sich um eine SR-IOV-VF-NIC handelt. Die MAC-Adressen der 1/1- und 50/1-NICs sind identisch. Nachdem das beschleunigte Netzwerk aktiviert wurde, werden die Daten der 1/1-Schnittstelle über den Datenpfad der 50/1-Schnittstelle gesendet, bei der es sich um eine ConnectX3-Schnittstelle handelt. Sie können sehen, dass der Ausgang „Show Interface“ der PV-Schnittstelle (1/1) auf den VF (50/1) zeigt. In ähnlicher Weise zeigt die Ausgabe „Show Interface“ der VF-Schnittstelle (50/1) auf die PV-Schnittstelle (1/1).


```
> show interface 1/1

        Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1 Datapath 50/1) #1
        flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.

Done

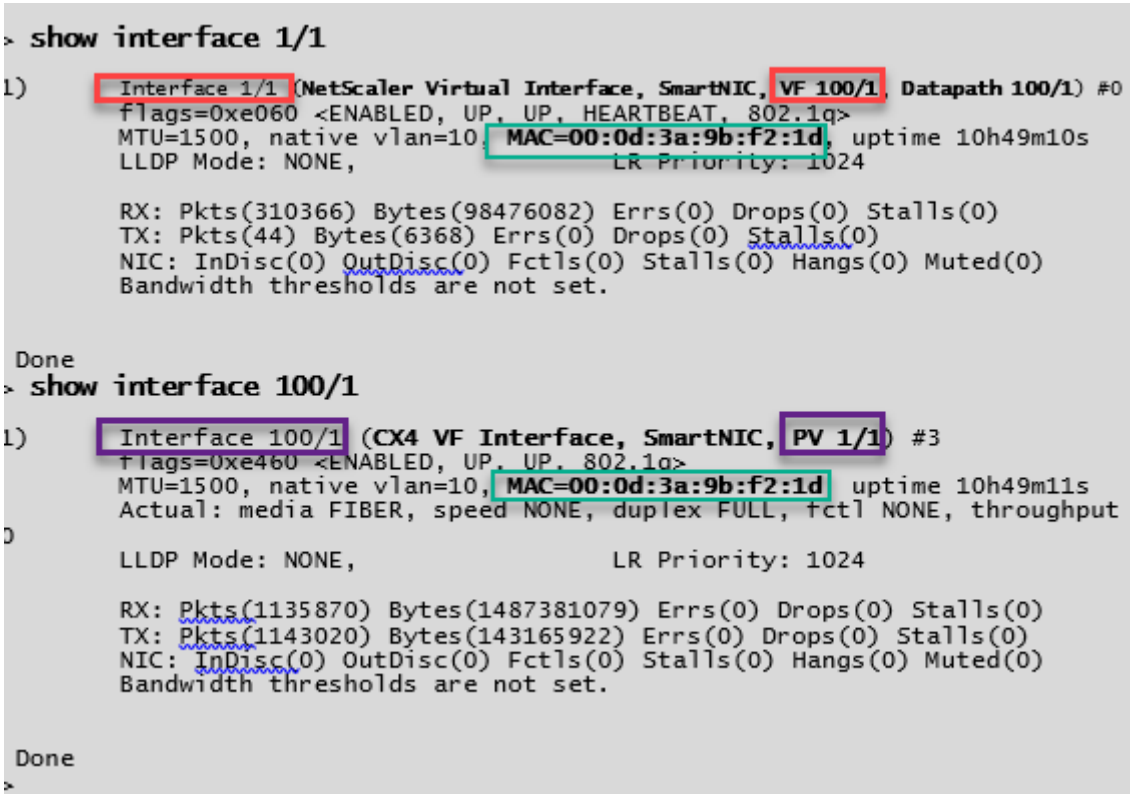
> show interface 50/1

      Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2
        flags=0xe460 <ENABLED, UP, UP, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m08s
        Actual: media NONE, speed 50000, duplex FULL, fctl NONE, throughput 50000
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
```

Beispiel für ConnectX4 NIC:

Die folgende Befehlsausgabe zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 100/1 gebündelt ist, bei der es sich um eine SR-IOV-VF-NIC handelt. Die MAC-Adressen der 1/1- und 100/1-NICs sind identisch. Nachdem das beschleunigte Netzwerk aktiviert wurde, werden die Daten der 1/1-Schnittstelle über den Datenpfad der 100/1-Schnittstelle gesendet, bei der es sich um eine ConnectX4-Schnittstelle handelt. Sie können sehen, dass der Ausgang „Show Interface“ der PV-Schnittstelle (1/1) auf den VF (100/1) zeigt. In ähnlicher Weise zeigt die Ausgabe „Show Interface“ der VF-Schnittstelle (100/1) auf die PV-Schnittstelle (1/1).



Zu beachtende Punkte in NetScaler

- Die PV-Schnittstelle wird als primäre oder Hauptschnittstelle für alle erforderlichen Operationen betrachtet. Konfigurationen dürfen nur an PV-Schnittstellen durchgeführt werden.
- Alle „Set“ -Operationen auf einer VF-Schnittstelle sind blockiert, mit Ausnahme der folgenden:
  - Schnittstelle aktivieren
  - Schnittstelle deaktivieren
  - Schnittstelle zurücksetzen
  - Statistiken löschen

  > Hinweis:
  >
  > Citrix empfiehlt, dass Sie keine Operationen auf der VF-Schnittstelle ausführen.
- Sie können die Bindung der PV-Schnittstelle an die VF-Schnittstelle mit dem `show interface` Befehl überprüfen.
- Ab NetScaler Version 13.1-33.x kann eine NetScaler VPX-Instanz dynamische NIC-Entfernungen und das erneute Anhängen der entfernten NICs in Azure Accelerated Networking nahtlos verarbeiten. Azure kann die SR-IOV VF-NIC von Accelerated Networking für ihre Host-Wartungsaktivitäten entfernen. Immer wenn eine Netzwerkkarte aus der Azure-VM entfernt wird, zeigt die NetScaler VPX-Instanz den Schnittstellenstatus als „Link Down“ an und der

Datenverkehr fließt nur über die virtuelle Schnittstelle. Nachdem die entfernte Netzwerkkarte wieder angeschlossen wurde, verwenden die VPX-Instanzen die erneut verbundene SR-IOV-VF-Netzwerkkarte. Dieser Vorgang erfolgt nahtlos und erfordert keine Konfiguration.

Konfigurieren Sie ein VLAN zu einer PV-Schnittstelle

Wenn eine PV-Schnittstelle an ein VLAN gebunden ist, ist die zugehörige beschleunigte VF-Schnittstelle auch an dasselbe VLAN wie die PV-Schnittstelle gebunden. In diesem Beispiel ist die PV-Schnittstelle (1/1) an VLAN (20) gebunden. Die VF-Schnittstelle (100/1), die mit der PV-Schnittstelle (1/1) gebündelt ist, ist ebenfalls an VLAN 20 gebunden.

Beispiel:

1. Erstellen Sie ein VLAN.

```
add vlan 20
<!--NeedCopy-->
```

2. Binden Sie ein VLAN an die PV-Schnittstelle.

```
bind vlan 20  -ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2

<!--NeedCopy-->
```

> Hinweis
>
> VLAN-Bindungsvorgänge sind auf einer beschleunigten VF-Schnittstelle nicht zulässig.

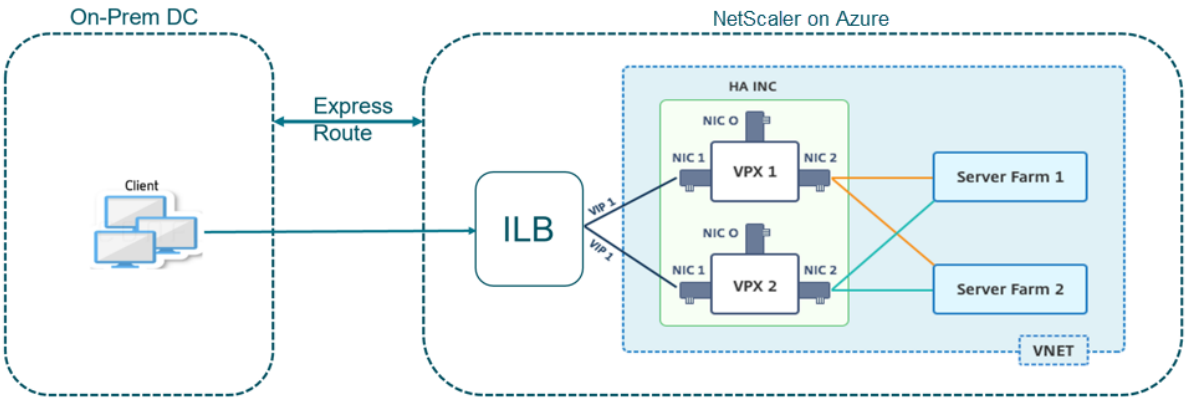
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
<!--NeedCopy-->
```


Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage mit Azure ILB

May 11, 2023

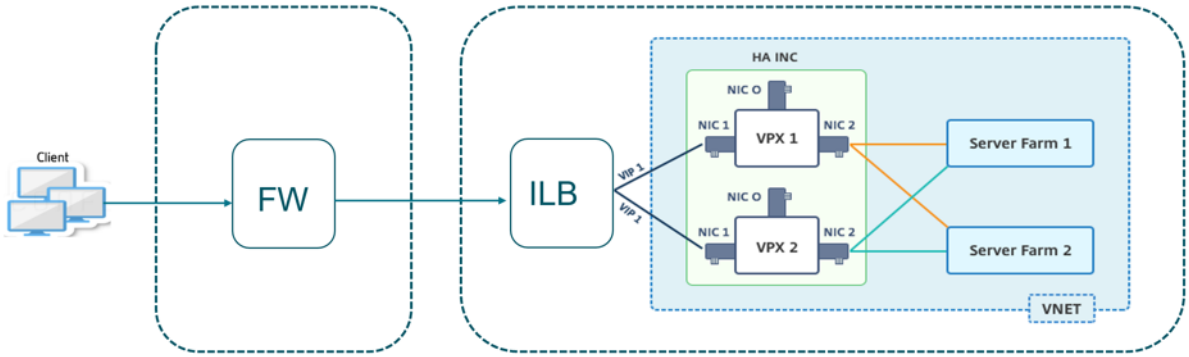
Sie können schnell und effizient ein Paar VPX-Instanzen im HA-INC-Modus bereitstellen, indem Sie die Standardvorlage für Intranetanwendungen verwenden. Der Azure Internal Load Balancer (ILB) verwendet eine interne oder private IP-Adresse für das Frontend, wie in Abbildung 1 dargestellt. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze dienen der Verwaltung, des Clients und des serverseitigen Datenverkehrs, wobei jedes Subnetz zu einer anderen Netzwerkkarte auf jedem Gerät gehört.

Abbildung 1: NetScaler HA-Paar für Clients in einem internen Netzwerk



Sie können diese Bereitstellung auch verwenden, wenn sich das NetScaler HA-Paar hinter einer Firewall befindet, wie in Abbildung 2 dargestellt. Die öffentliche IP-Adresse gehört zur Firewall und ist mit NAT der Front-End-IP-Adresse der ILB verbunden.

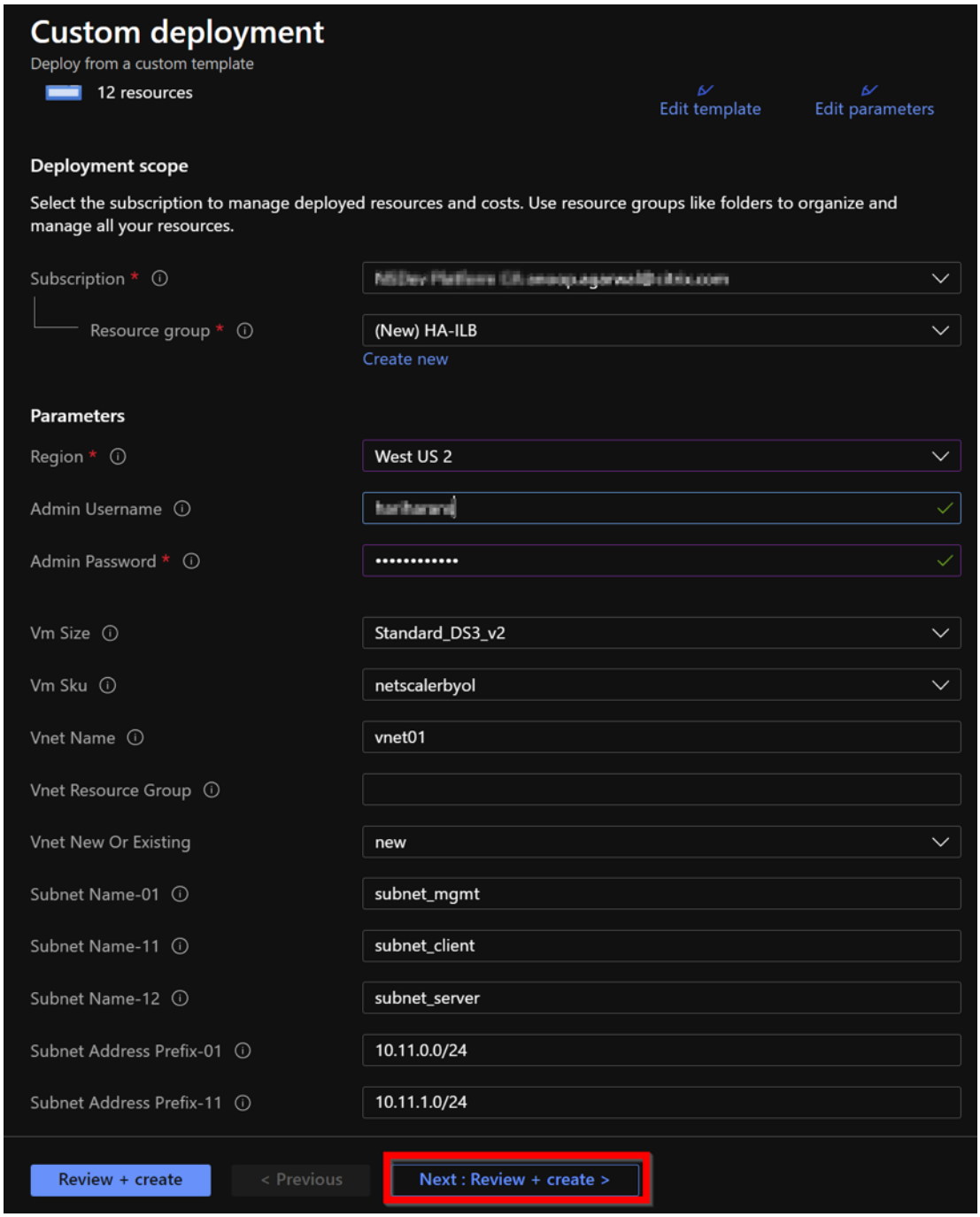
Abbildung 2: NetScaler HA-Paar mit Firewall mit öffentlicher IP-Adresse



Sie können die NetScaler HA-Paarvorlage für Intranetanwendungen im Azure-Portalabrufen

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure Availability Sets bereitzustellen.

1. Navigieren Sie im Azure-Portal zur Seite **Benutzerdefinierte Bereitstellung** .
2. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Region, den Admin-Benutzernamen, das Admin-Kennwort, den Lizenztyp (`VM sku`) und andere Felder ein.

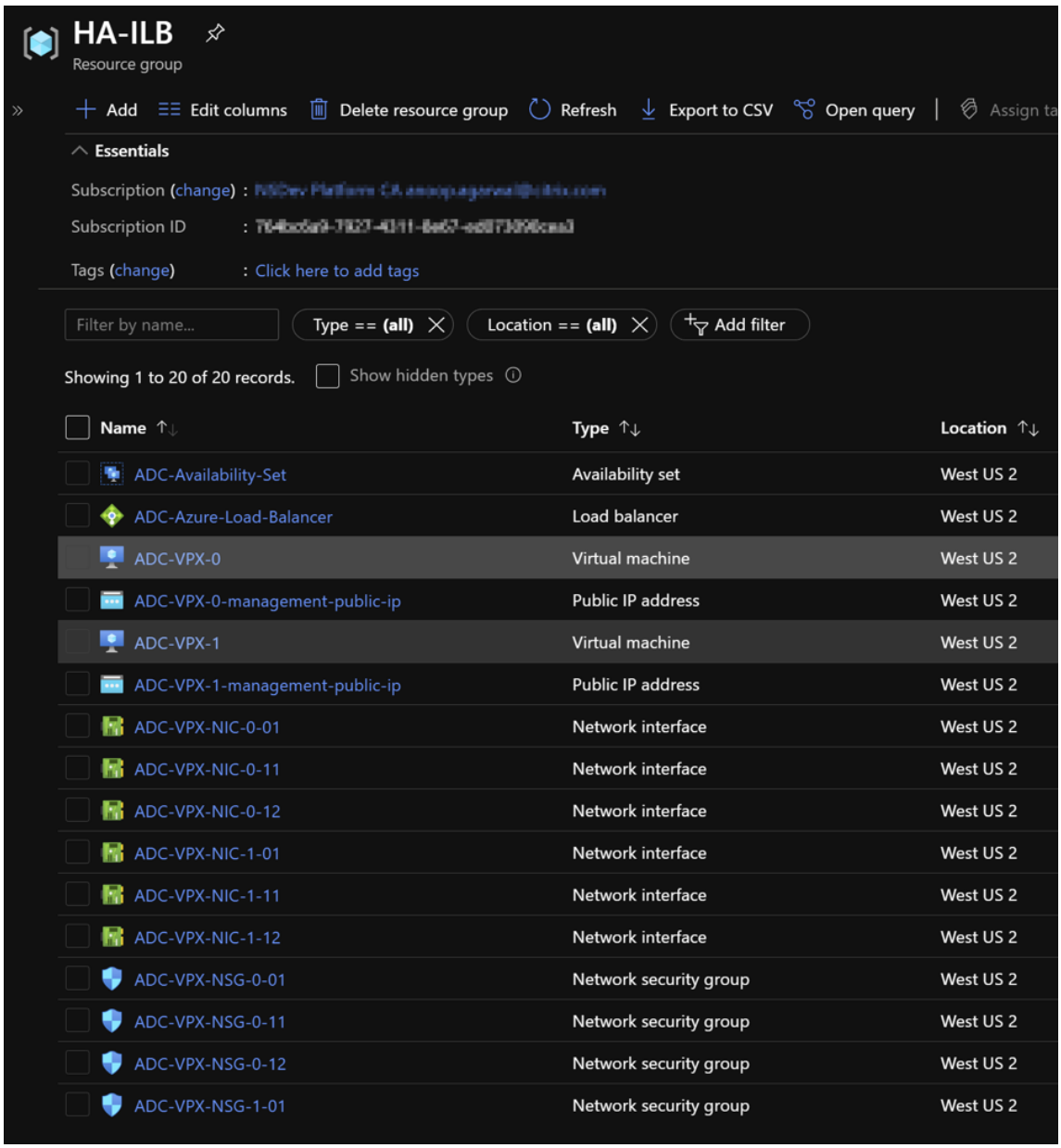


3. Klicken Sie auf **Weiter: Überprüfen + erstellen**.

Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritäts-Sonden anzuzeigen. Das Hochverfügbarkeitspaar erscheint als ADC-VPX-0 und ADC-VPX-1.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.

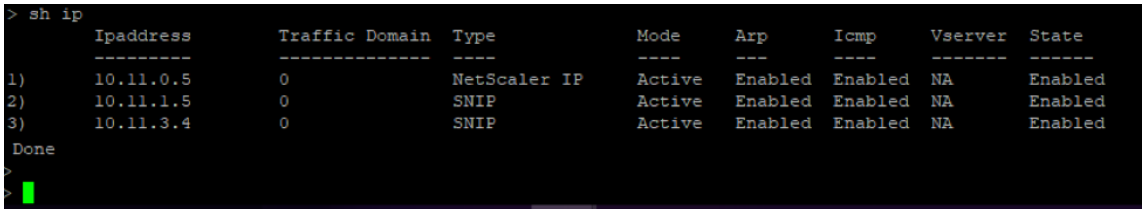


4. Melden Sie sich bei den Knoten **ADC-VPX-0** und **ADC-VPX-1** an, um die folgende Konfiguration zu überprüfen:

- NSIP-Adressen für beide Knoten müssen sich im Management-Subnetz befinden.
- Auf den primären (ADC-VPX-0) und sekundären (ADC-VPX-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Ein SNIP (Client-Subnetz) wird für die Reaktion auf ILB-Prüfpunkte verwendet und das andere SNIP (Serversubnetz) wird für die Back-End-Server-Kommunikation verwendet.

> Hinweis
>
> Im HA-INC-Modus unterscheiden sich die SNIP-Adresse der ADC-VPX-0- und ADC-VPX-1-VMs im selben Subnetz, im Gegensatz zu der klassischen lokalen ADC HA-Bereitstellung, bei der beide gleich sind.
> Um Bereitstellungen zu unterstützen, wenn sich das VPX-Paar SNIP in verschiedenen Subnetzen befindet oder wenn sich der VIP nicht im selben Subnetz wie ein SNIP befindet, müssen Sie entweder Mac-Based Forwarding (MBF) aktivieren oder jedem VPX-Knoten eine statische Host-Route für jeden VIP hinzufügen.

Auf dem primären Knoten (ADC-VPX-0)




```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.4
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

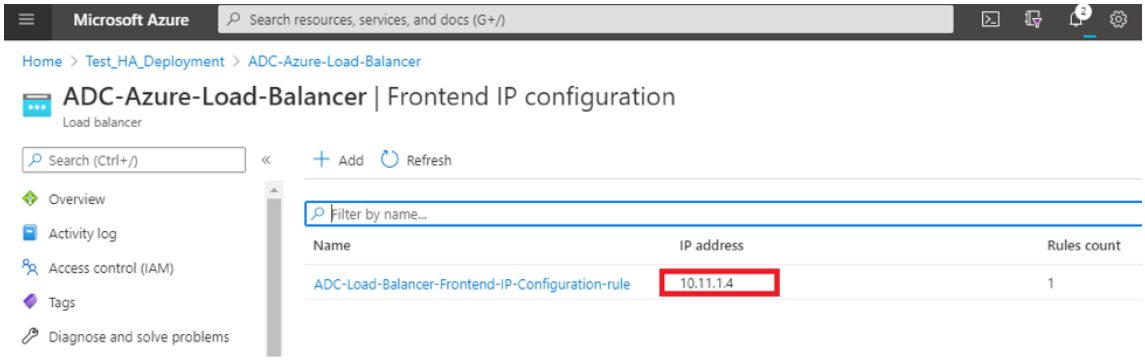
Auf dem sekundären Knoten (ADC-VPX-1)

```
> sh ip
        Ipaddress       Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------       --------------  ----            ----     ---      ----     -------  ------
1)      10.11.0.4       0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.11.1.6       0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.11.3.5       0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

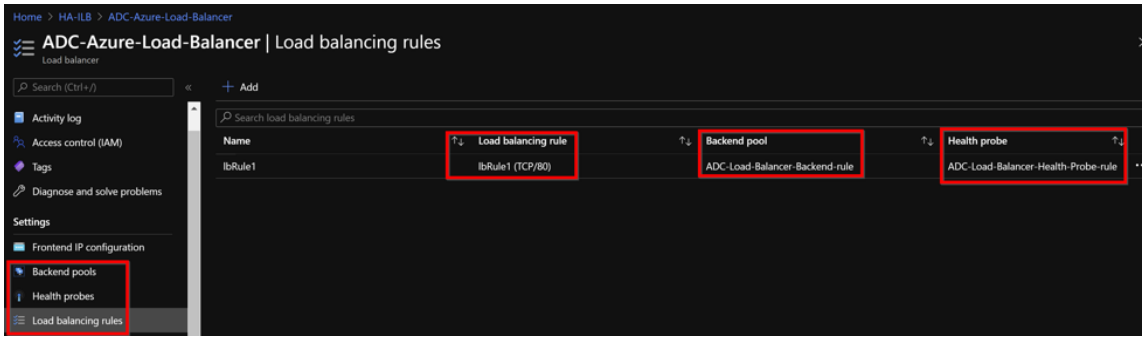


```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

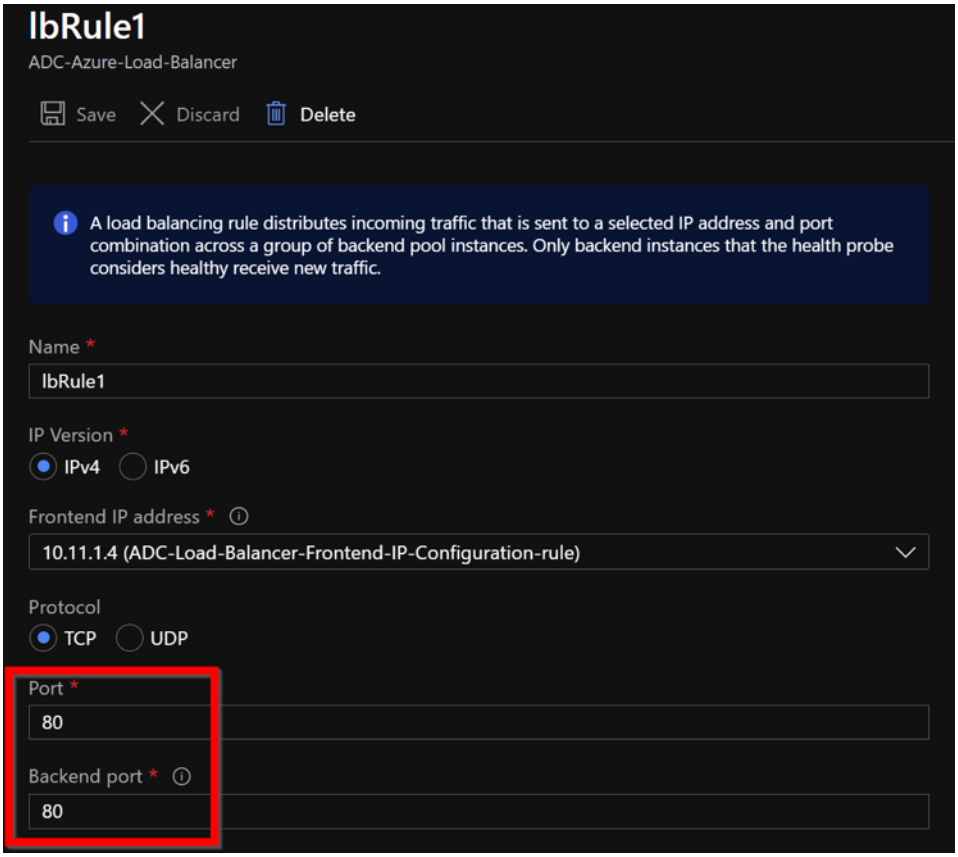
5. Nachdem die primären und sekundären Knoten aktiv sind und der Synchronisierungsstatus **ERFOLGREICH**ist, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem Primärknoten (ADC-VPX-0) mit der privaten Floating IP (FIP) -Adresse des ADC Azure Load Balancers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration .
6. Um die private IP-Adresse des ADC Azure Load Balancers zu finden, navigieren Sie zum **Azure-Portal > ADC Azure Load Balancer > Frontend IP-Konfiguration**.



7. Auf der **Azure Load Balancer-Konfigurationsseite** hilft die ARM-Vorlagenbereitstellung beim Erstellen der LB-Regel, Back-End-Pools und Gesundheitsproben.

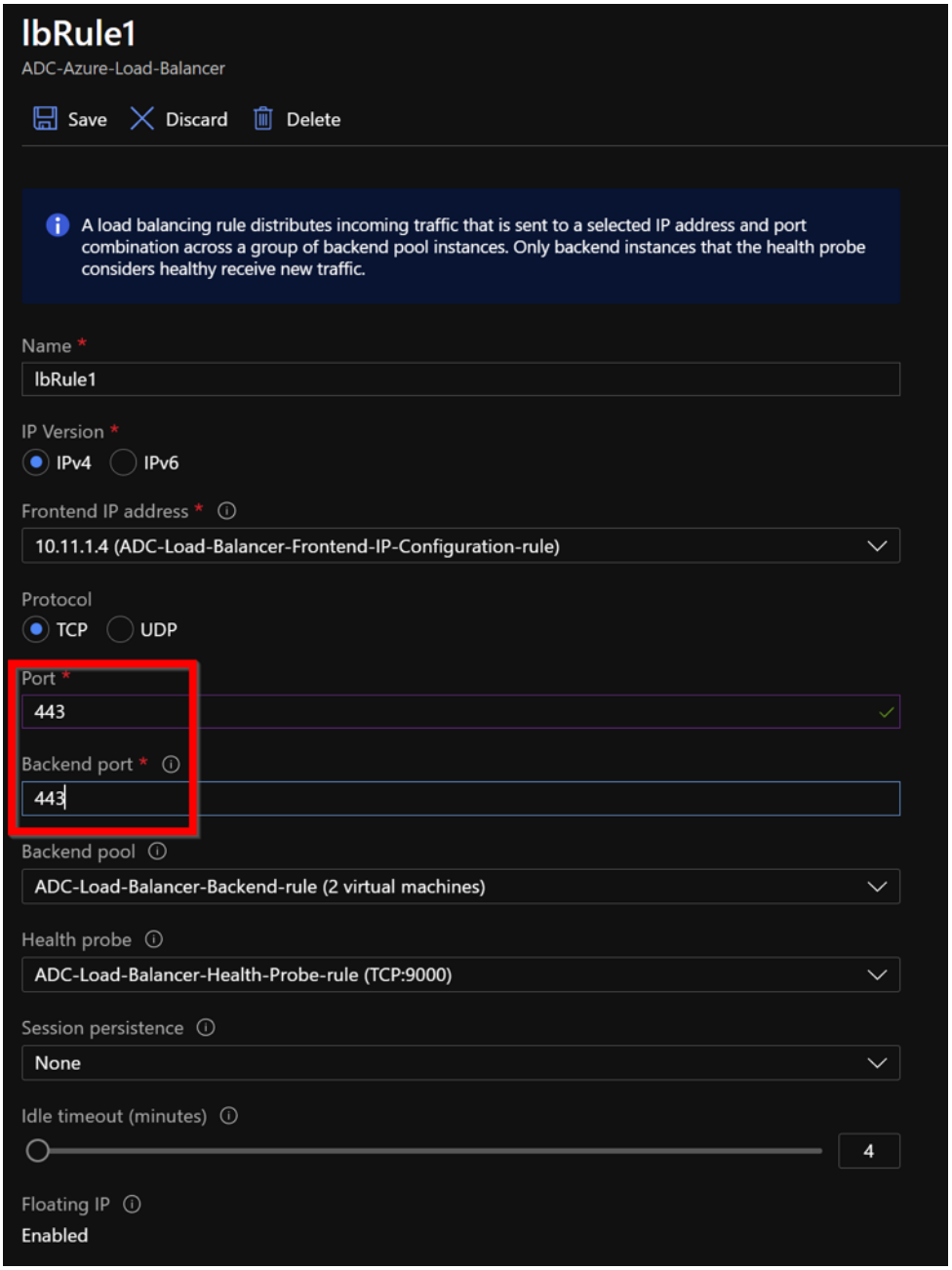


   - Die LB-Regel (LBrule1) verwendet standardmäßig Port 80.



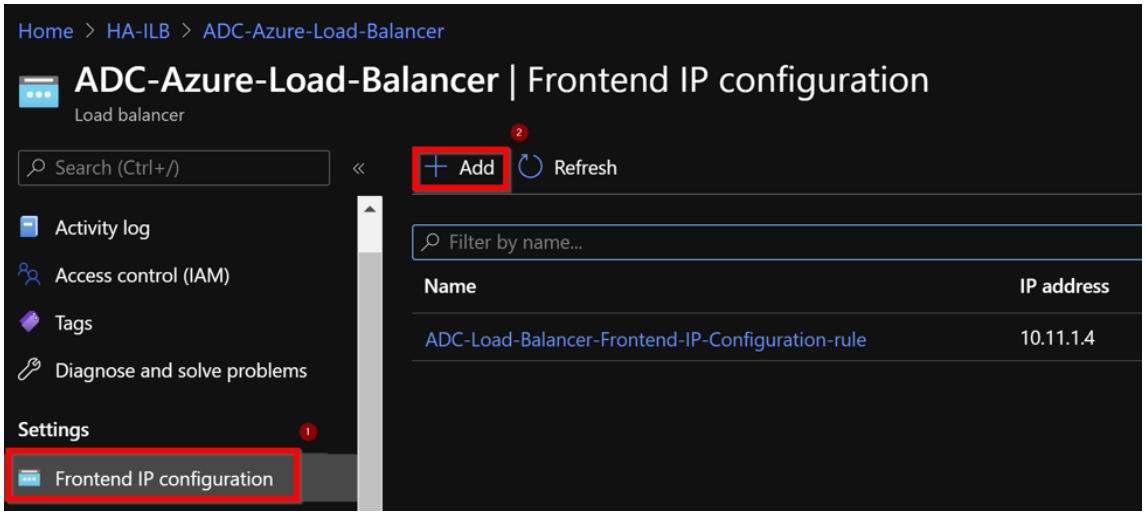
- Bearbeiten Sie die Regel, um Port 443 zu verwenden, und speichern Sie die Änderungen.

  > Hinweis
  >
  > Für eine verbesserte Sicherheit empfiehlt Citrix, den SSL-Port 443 für den virtuellen LB-Server oder den virtuellen Gateway-Server zu verwenden.

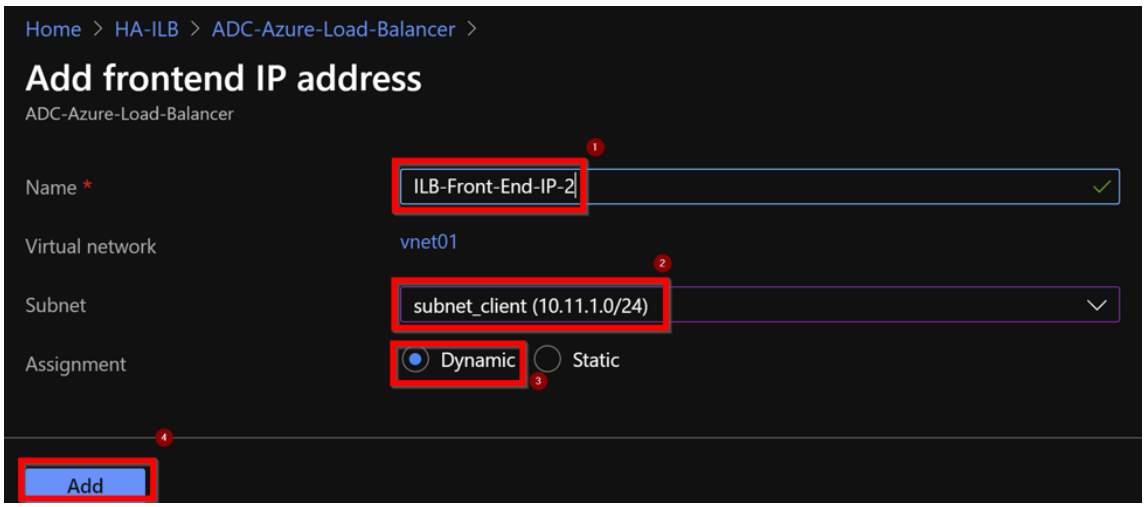


Gehen Sie wie folgt vor, um weitere VIP-Adressen zum ADC hinzuzufügen:

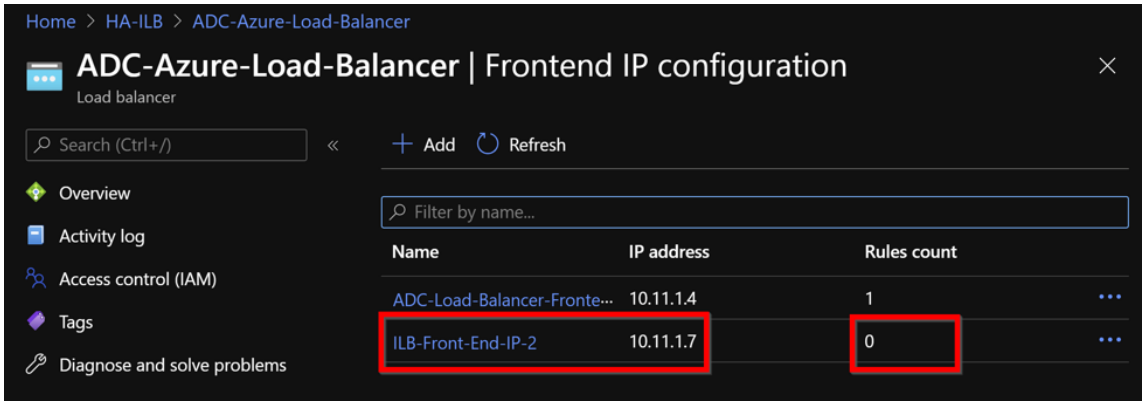
1. Navigieren Sie zu **Azure Load Balancer > Frontend-IP-Konfiguration**, und klicken Sie auf **Hinzufügen**, um eine neue interne Load Balancer-IP-Adresse zu erstellen.



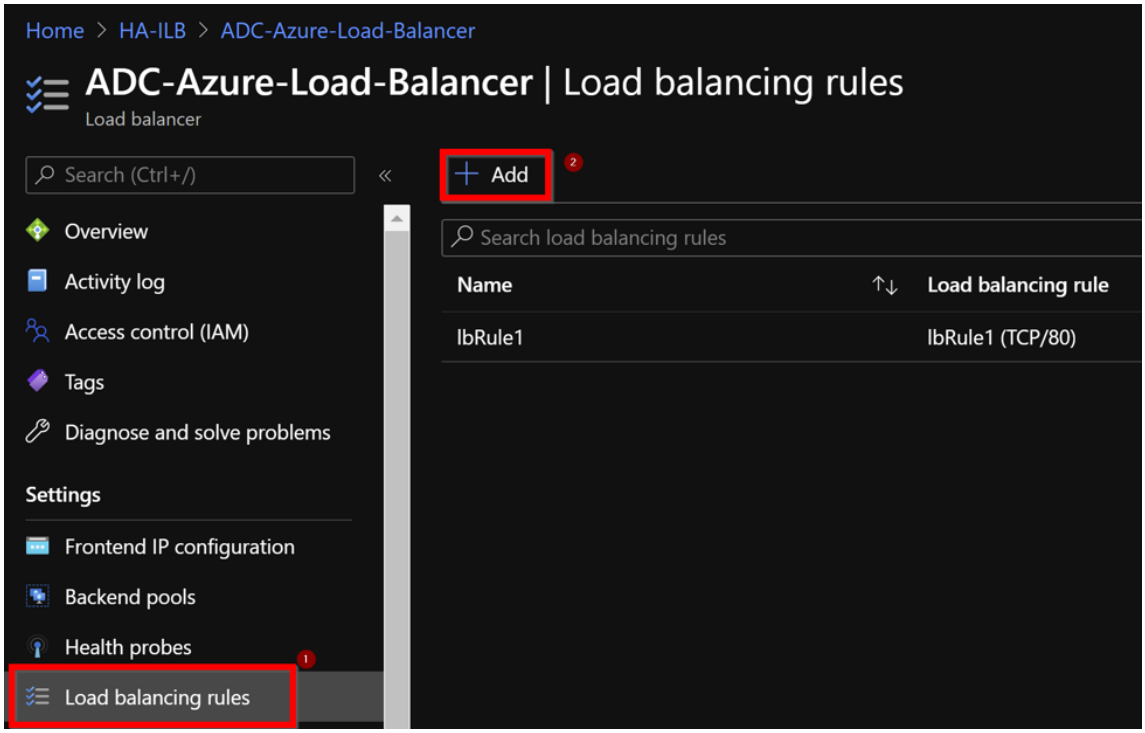
2. Geben Sie auf der Seite **Frontend-IP-Adresse hinzufügen** einen Namen ein, wählen Sie das Client-Subnetz aus, weisen Sie entweder dynamische oder statische IP-Adresse zu und klicken Sie auf **Hinzufügen**.



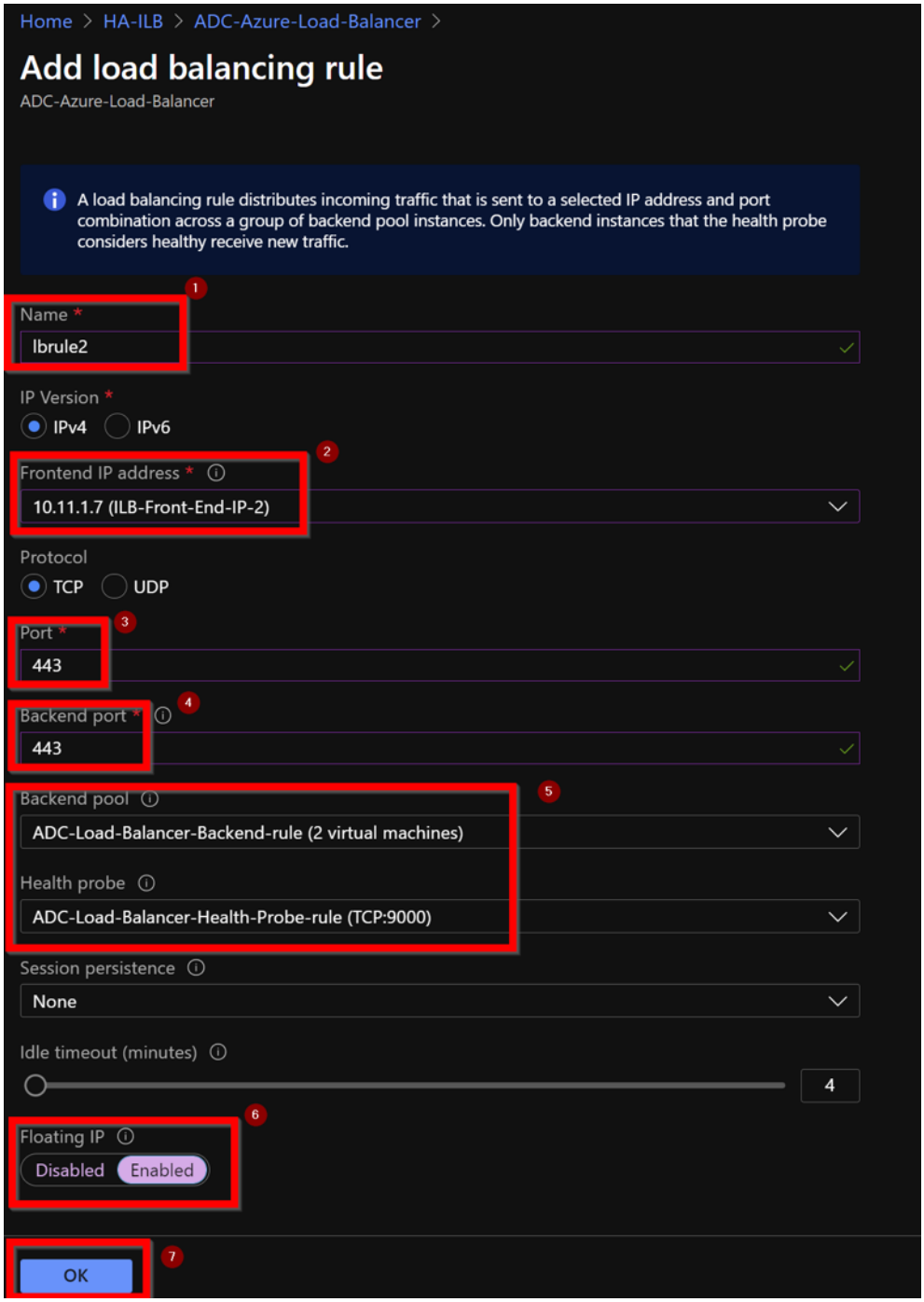
3. Die Front-End-IP-Adresse wird erstellt, aber eine LB-Regel ist nicht zugeordnet. Erstellen Sie eine neue Lastausgleichsregel, und verknüpfen Sie sie mit der Front-End-IP-Adresse.



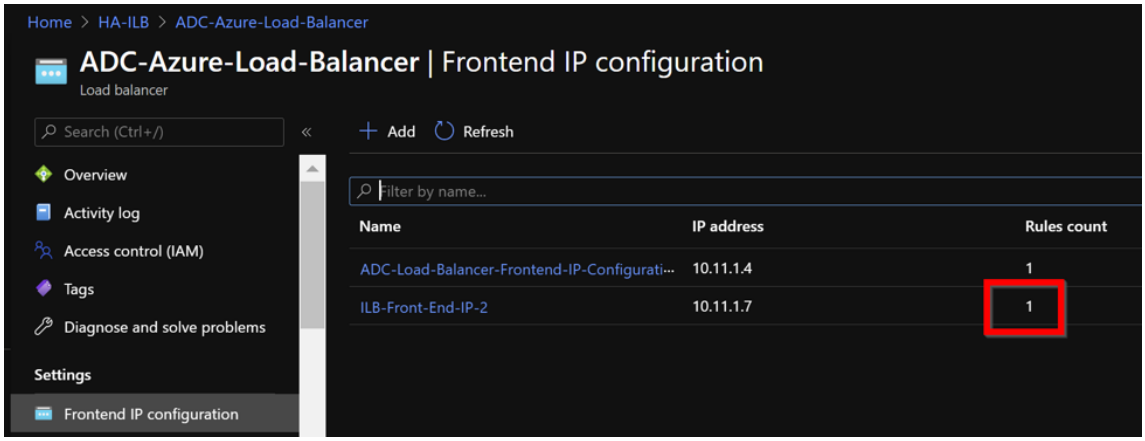
4. Wählen Sie auf der Seite **Azure Load Balancer** die Option **Load Balancing-Regeln**aus, und klicken Sie dann auf **Hinzufügen**.



5. Erstellen Sie eine neue LB-Regel, indem Sie die neue Front-End-IP-Adresse und den Port auswählen. Das**Floating-IP-Feld** muss auf **Enabled**gesetzt sein.



6. Jetzt zeigt die **Frontend-IP-Konfiguration** die angewendete LB-Regel an.



Beispiel-Konfiguration

Führen Sie zum Konfigurieren eines virtuellen Gateway-VPN-Servers und eines virtuellen Lastausgleichsservers die folgenden Befehle auf dem primären Knoten aus (ADC-VPX-0). Die Konfiguration synchronisiert sich automatisch mit dem sekundären Knoten (ADC-VPX-1).

Gateway Beispielkonfiguration

```
enable feature aaa LB SSL SSLVPN
enable ns mode MBF
add vpn vserver vpn_ssl SSL 10.11.1.4 443
add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Beispielkonfiguration für den Lastausgleich

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 10.11.1.7 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Sie können jetzt mit dem vollqualifizierten Domänennamen (FQDN), der mit der internen IP-Adresse von ILB verknüpft ist, auf den Lastausgleich- oder virtuellen VPN-Server zugreifen.

Weitere Informationen zur Konfiguration des virtuellen Load-Balancing-Servers finden Sie im Abschnitt **Ressourcen** .

Ressourcen:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Konfiguration virtueller Server:

- Konfigurieren von Knoten mit hoher Verfügbarkeit in verschiedenen Subnetzen
- Einrichten des grundlegenden Lastenausgleichs

Verwandte Ressourcen:

- Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs über PowerShell-Befehle konfigurieren
- Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

Konfigurieren Sie HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage für mit dem Internet verbundene Anwendungen

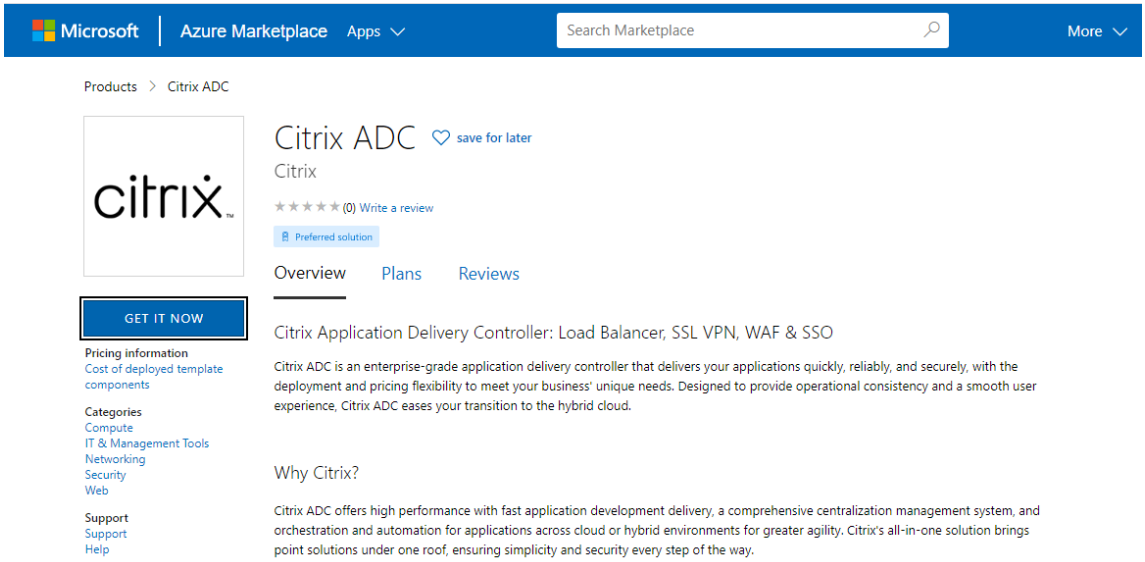
May 11, 2023

Sie können schnell und effizient ein Paar von VPX-Instanzen im HA-INC-Modus bereitstellen, indem Sie die Standardvorlage für internetfähige Anwendungen verwenden. Der Azure Load Balancer (ALB) verwendet eine öffentliche IP-Adresse für das Frontend. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze sind für den Management-, Client- und serverseitigen Verkehr bestimmt. Jedes Subnetz hat zwei Netzwerkkarten für beide VPX-Instanzen.

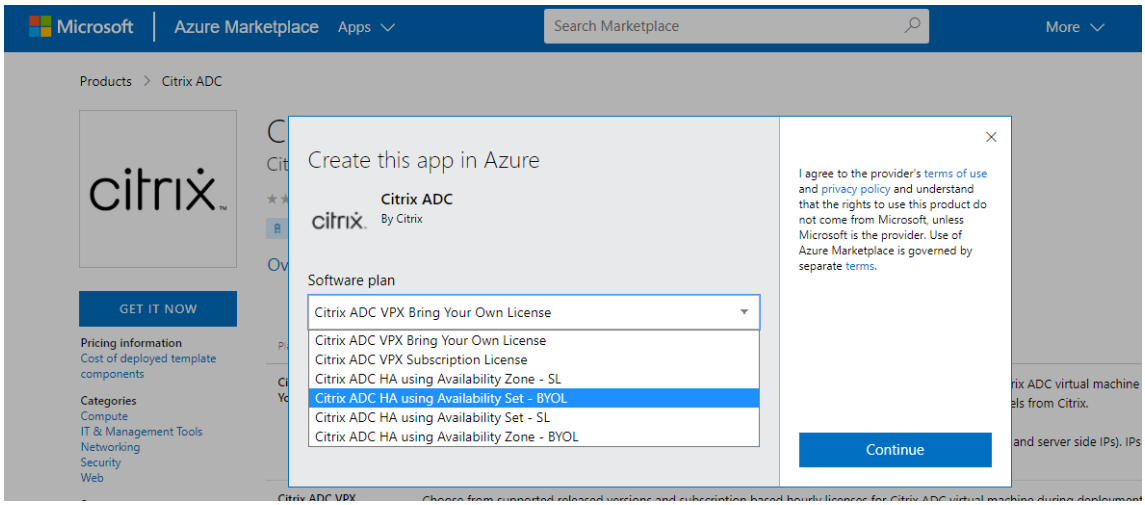
Sie können die NetScaler HA-Paar-Vorlage für internetorientierte Anwendungen im Azure Marketplaceabrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure Availability Sets oder Availability Zone bereitzustellen.

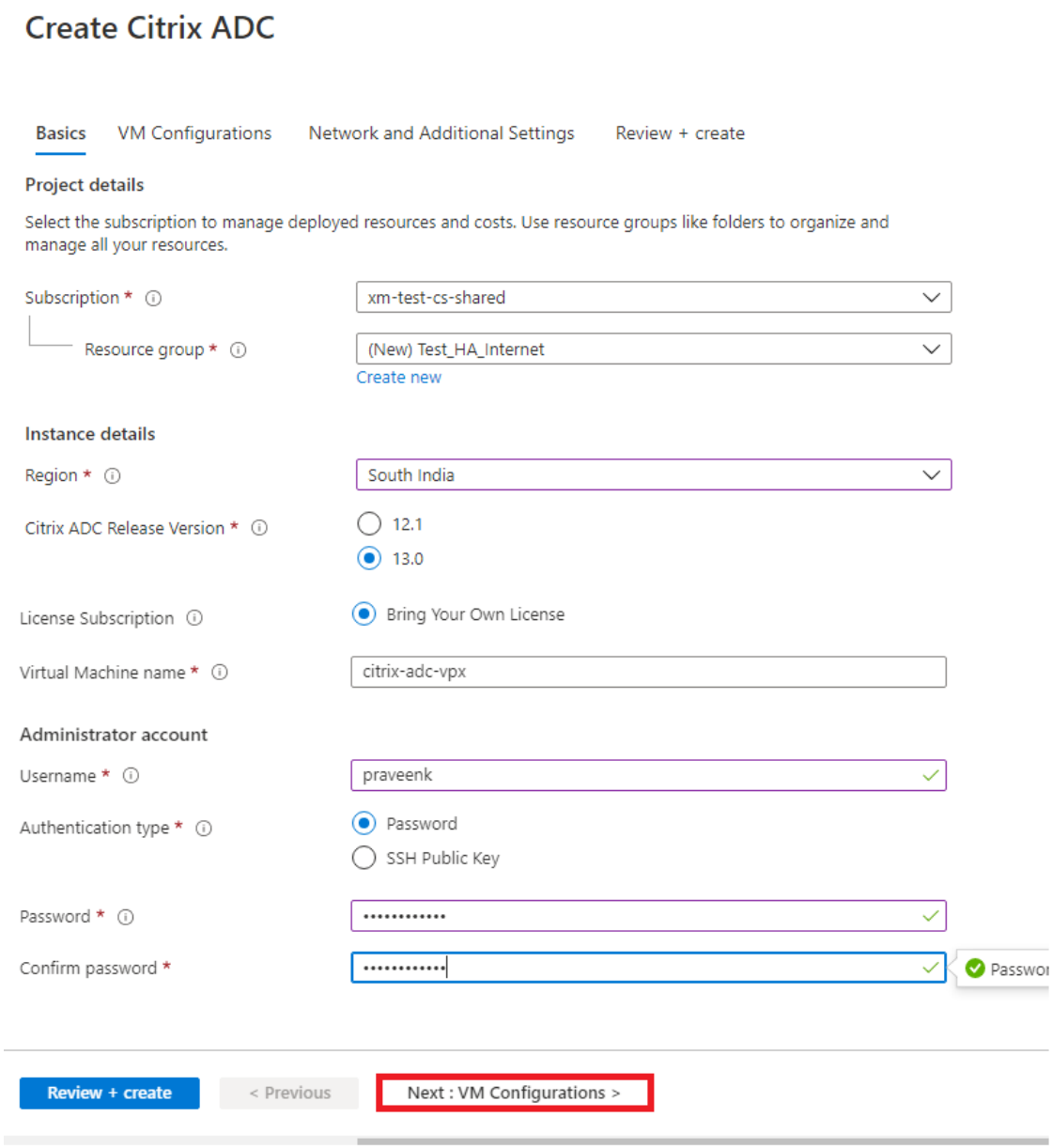
1. Suchen Sie im Azure Marketplace nach **NetScaler**.
2. Klicken Sie auf **JETZT HOLEN**.



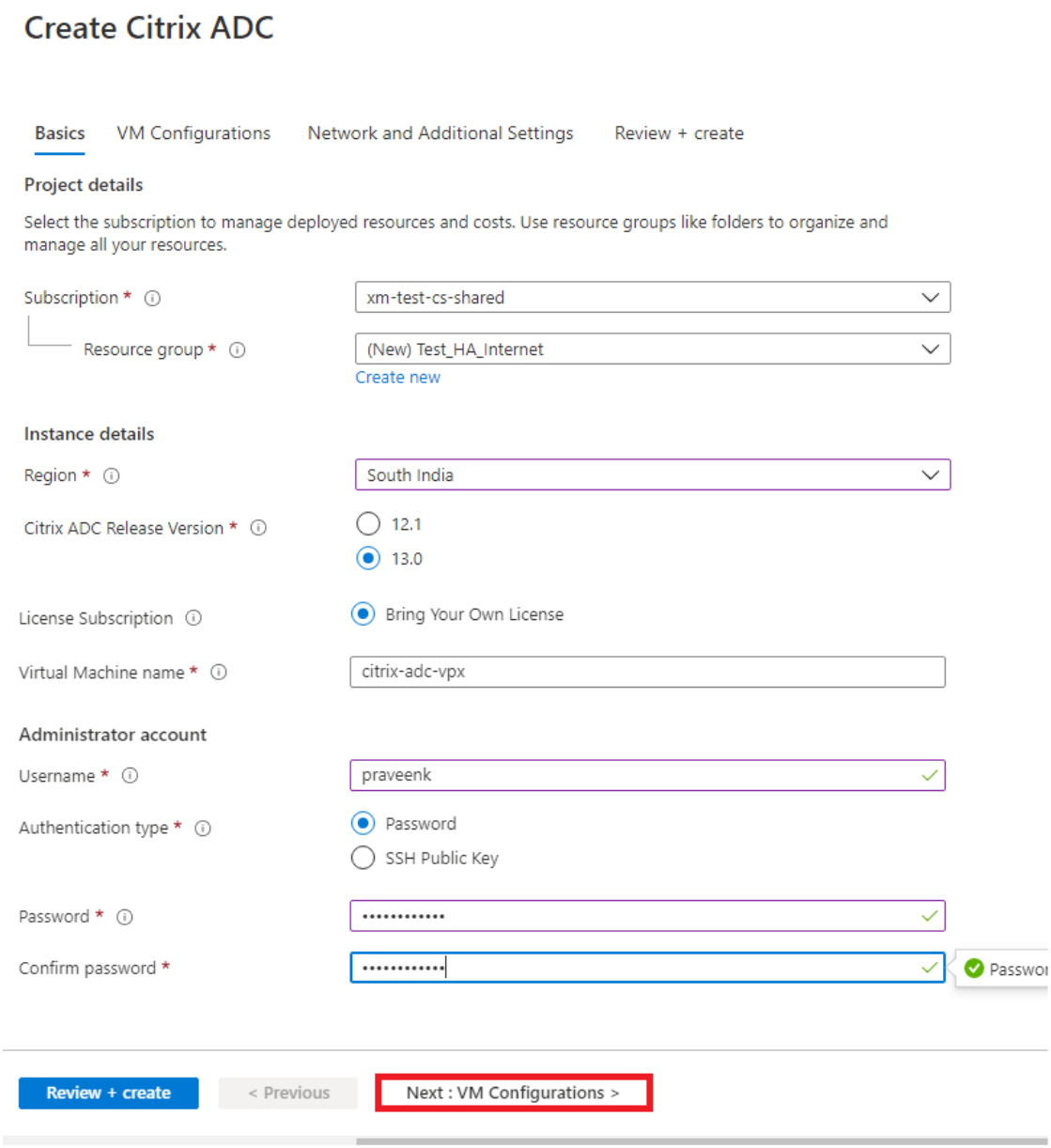
3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.



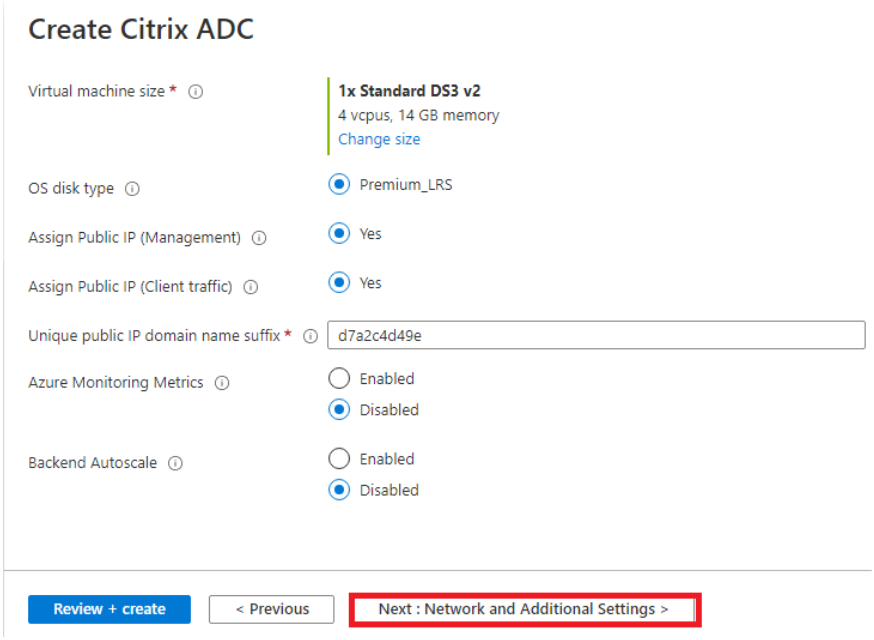
4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Felder Region, Admin-Benutzername, Admin-Kennwort, Lizenztyp (VM SKU) und andere ein.



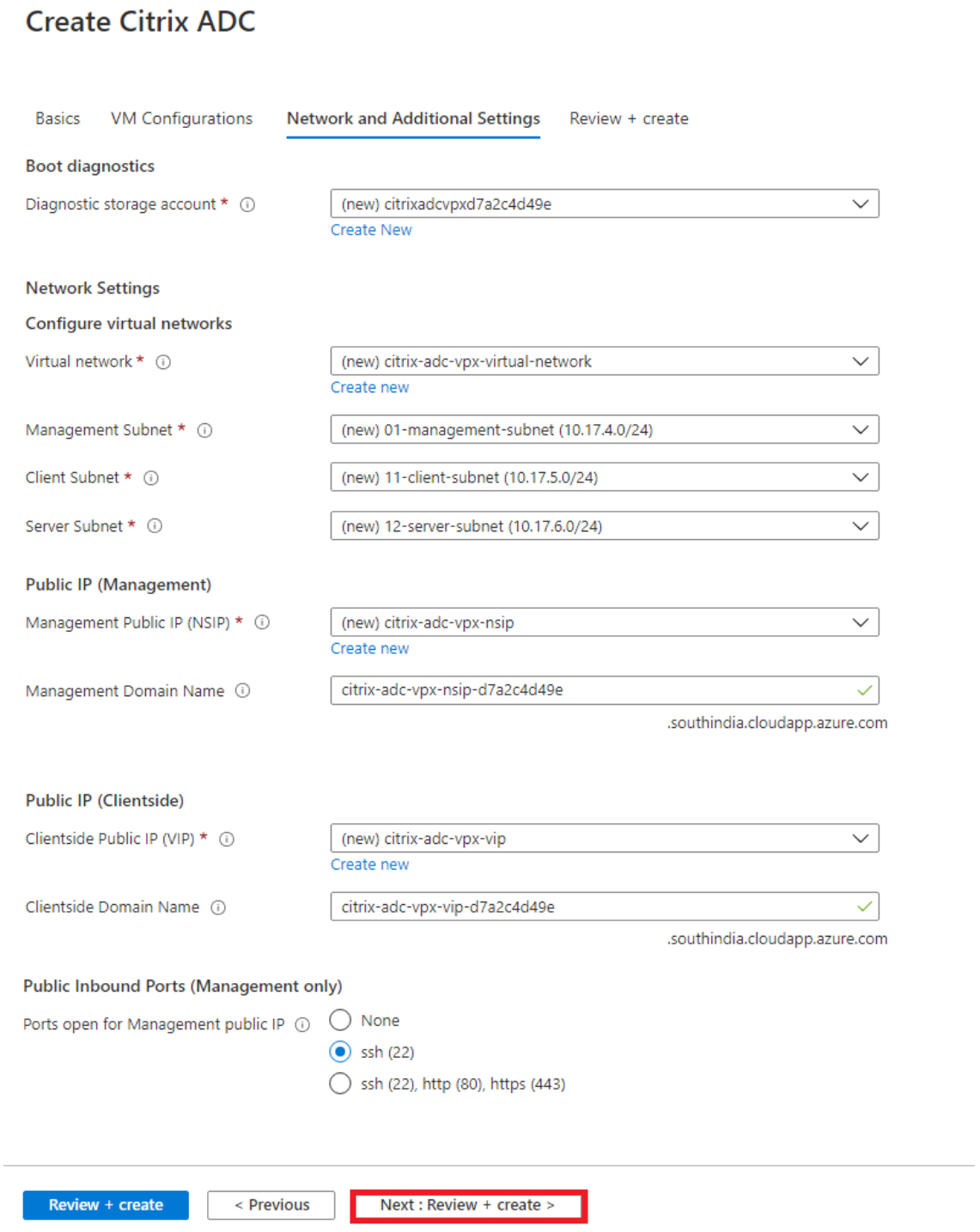
5. Klicken Sie auf **Weiter: VM-Konfigurationen**.



6. Führen Sie auf der Seite **VM-Konfigurationen** die folgenden Schritte aus:
   - Konfigurieren Sie das Suffix für den öffentlichen IP-Domainnamen
   - **Azure Monitoring Metrics**aktivieren oder deaktivieren
   - **Backend**Autoscale aktivieren oder deaktivieren
7. Klicken Sie auf **Weiter: Netzwerk- und Zusatzeinstellungen**



8. Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Startdiagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.

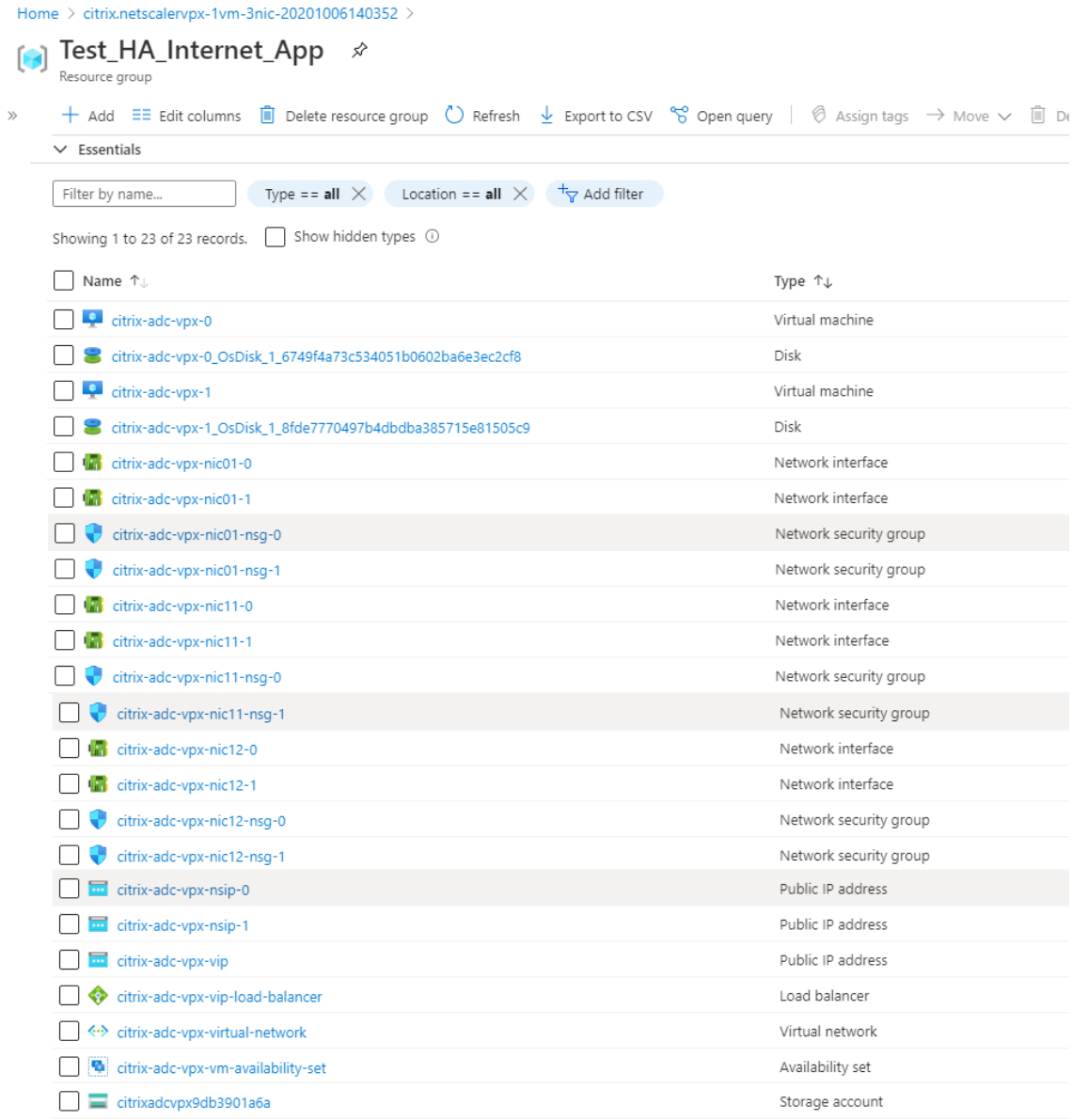


9. Klicken Sie auf **Weiter: Überprüfen + Erstellen**.
10. Überprüfen Sie die Grundeinstellungen, die VM-Konfiguration, das Netzwerk und die zusätzlichen Einstellungen und klicken Sie auf **Erstellen**.

Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Health Probes anzuzeigen. Das Hochverfügbarkeitspaar wird als **citrix-adc-vpx-0** und **citrix-adc-vpx-1**angezeigt.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.



11. Sie müssen sich an den Knoten **citrix-adc-vpx-0** und **citrix-adc-vpx-1** anmelden, um die folgende Konfiguration zu validieren:

- NSIP-Adressen für beide Knoten müssen sich im Management-Subnetz befinden.
- Auf den primären (citrix-adc-vpx-0) und sekundären (citrix-adc-vpx-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Ein SNIP (Client-Subnetz) wird für die Beantwortung der ALB-Sonden verwendet und das andere SNIP (Serversubnetz) wird für die Backend-Serverkommunikation verwendet.

> Hinweis
>
> Im HA-INC-Modus unterscheiden sich die SNIP-Adressen der VMs citrix-adc-vpx-0 und citrix-adc-vpx-1, im Gegensatz zur klassischen on-premises ADC-Hochverfügbarkeitsbereitstellung, bei der beide gleich sind.

Auf dem primären Knoten (citrix-adc-vpx-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.18.0.4        0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP             Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

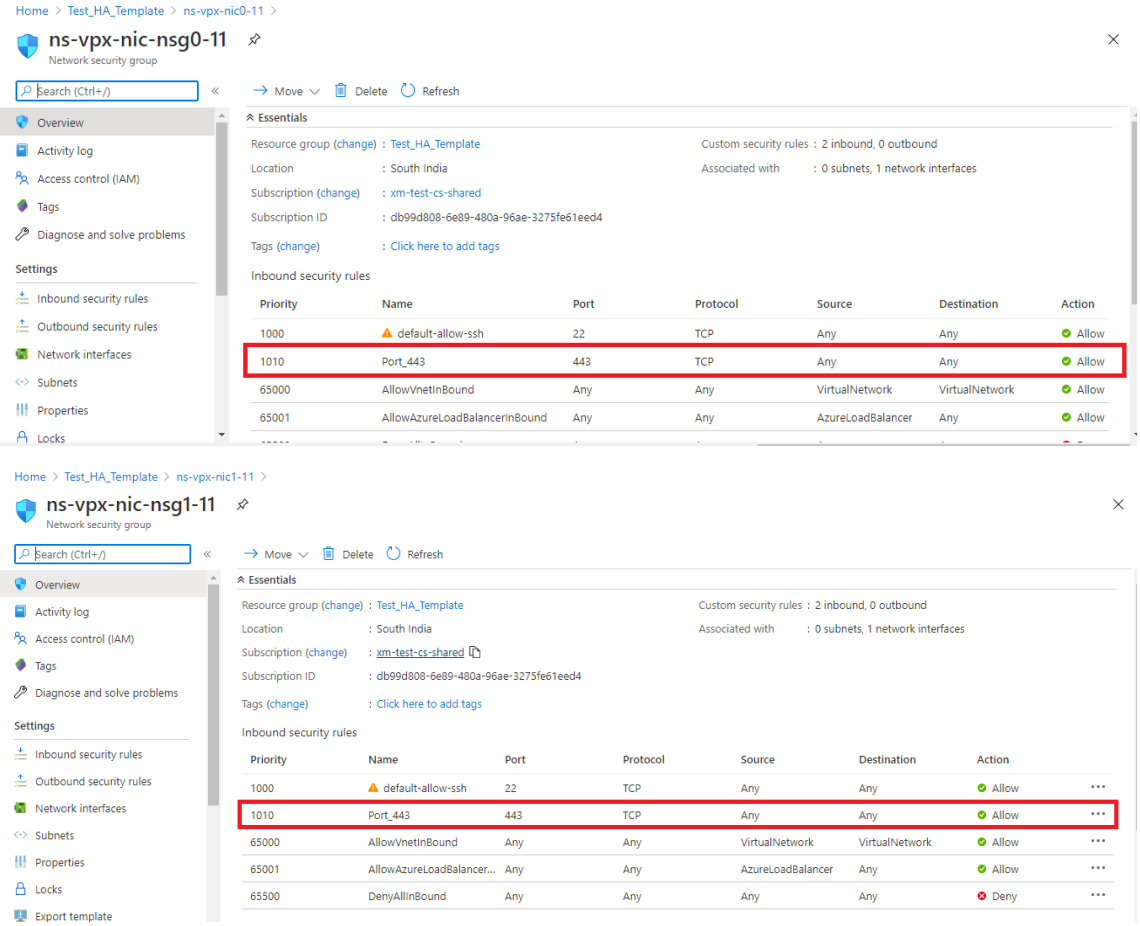
Auf dem sekundären Knoten (citrix-adc-vpx-1)


```
> show ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.5        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
```

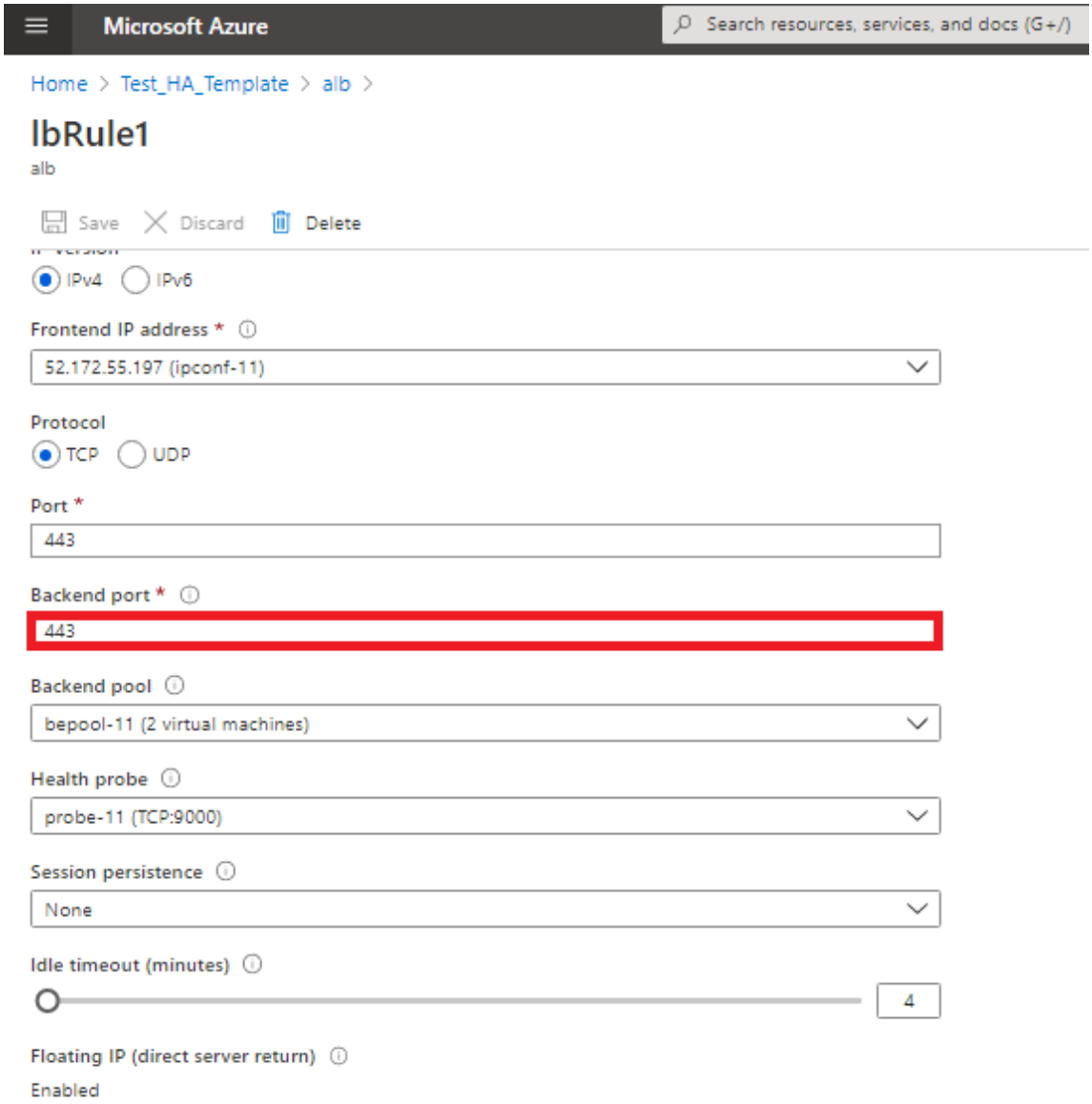
```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

12. Nachdem der primäre und sekundäre Knoten UP sind und der Synchronisierungsstatus **ERFOLG**ist, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem primären Knoten (citrix-adc-vpx-0) mit der öffentlichen IP-Adresse des virtuellen ALB-Servers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration .
13. Um die öffentliche IP-Adresse des virtuellen ALB-Servers zu finden, navigieren Sie zum **Azure-Portal > Azure Load Balancer > Frontend IP-Konfiguration**.

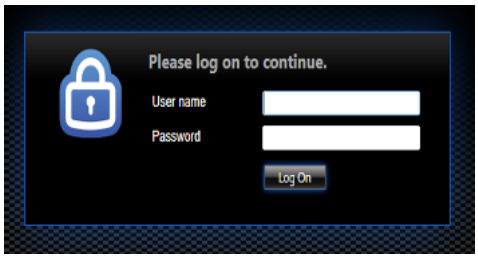
14. Fügen Sie die eingehende Sicherheitsregel für den virtuellen Serverport 443 in der Netzwerksicherheitsgruppe der beiden Client-Schnittstellen hinzu.



15. Konfigurieren Sie den ALB-Port, auf den Sie zugreifen möchten, und erstellen Sie eine Sicherheitsregel für eingehenden Datenverkehr für den angegebenen Port. Der Backend-Port ist Ihr virtueller Load-Balancing-Serverport oder der virtuelle VPN-Serverport.



16. Jetzt können Sie über den vollqualifizierten Domänennamen (FQDN), der der öffentlichen ALB-IP-Adresse zugeordnet ist, auf den virtuellen Lastausgleichsserver oder den virtuellen VPN-Server zugreifen.



Beispiel-Konfiguration

Führen Sie zum Konfigurieren eines virtuellen Gateway-VPN-Servers und eines virtuellen Lastausgleichsservers die folgenden Befehle auf dem primären Knoten aus (ADC-VPX-0). Die Konfiguration synchronisiert sich automatisch mit dem sekundären Knoten (ADC-VPX-1).

Gateway Beispielkonfiguration

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Beispielkonfiguration für den Lastausgleich

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 52.172.55.197 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Sie können jetzt über den FQDN, der der öffentlichen IP-Adresse von ALB zugeordnet ist, auf den virtuellen Loadbalancing- oder VPN-Server zugreifen.

Im Abschnitt **Ressourcen** finden Sie weitere Informationen zur Konfiguration des virtuellen Lastausgleichsservers.

Ressourcen:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Konfiguration virtueller Server:

- Virtuelle Server erstellen
- Einrichten des grundlegenden Lastenausgleichs

Hochverfügbarkeitssetup mit externen und internen Load Balancern von Azure gleichzeitig konfigurieren

May 11, 2023

Das Hochverfügbarkeitspaar auf Azure unterstützt sowohl externe als auch interne Load Balancer gleichzeitig.

Sie haben die folgenden zwei Möglichkeiten, ein Hochverfügbarkeitspaar mit externen und internen Load Balancern von Azure zu konfigurieren:

- Verwenden von zwei virtuellen LB-Servern auf der NetScaler Appliance.
- Verwenden eines virtuellen LB-Servers und eines IP-Sets. Der einzelne virtuelle LB-Server dient Datenverkehr zu mehreren IPs, die durch das IPSet definiert sind.

Führen Sie die folgenden Schritte aus, um ein Hochverfügbarkeitspaar in Azure zu konfigurieren, wobei sowohl externe als auch interne Load Balancer gleichzeitig verwendet werden:

Verwenden Sie für die Schritte 1 und 2 das Azure-Portal. Verwenden Sie für die Schritte 3 und 4 die NetScaler VPX GUI oder die CLI.

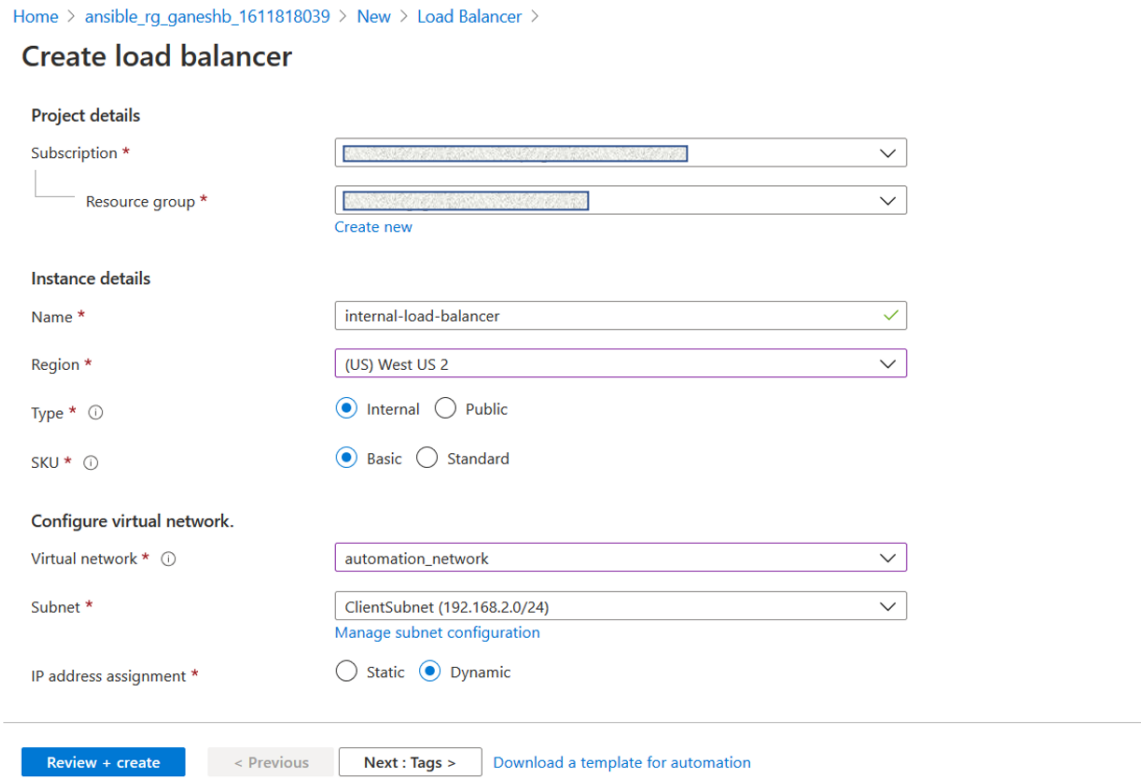
Schritt 1. Konfigurieren Sie einen Azure-Load Balancer, entweder einen externen Load Balancer oder einen internen Load Balancer.

Weitere Informationen zum Konfigurieren von Hochverfügbarkeits-Setups mit externen Azure Load Balancern finden Sie unter Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und NIC.

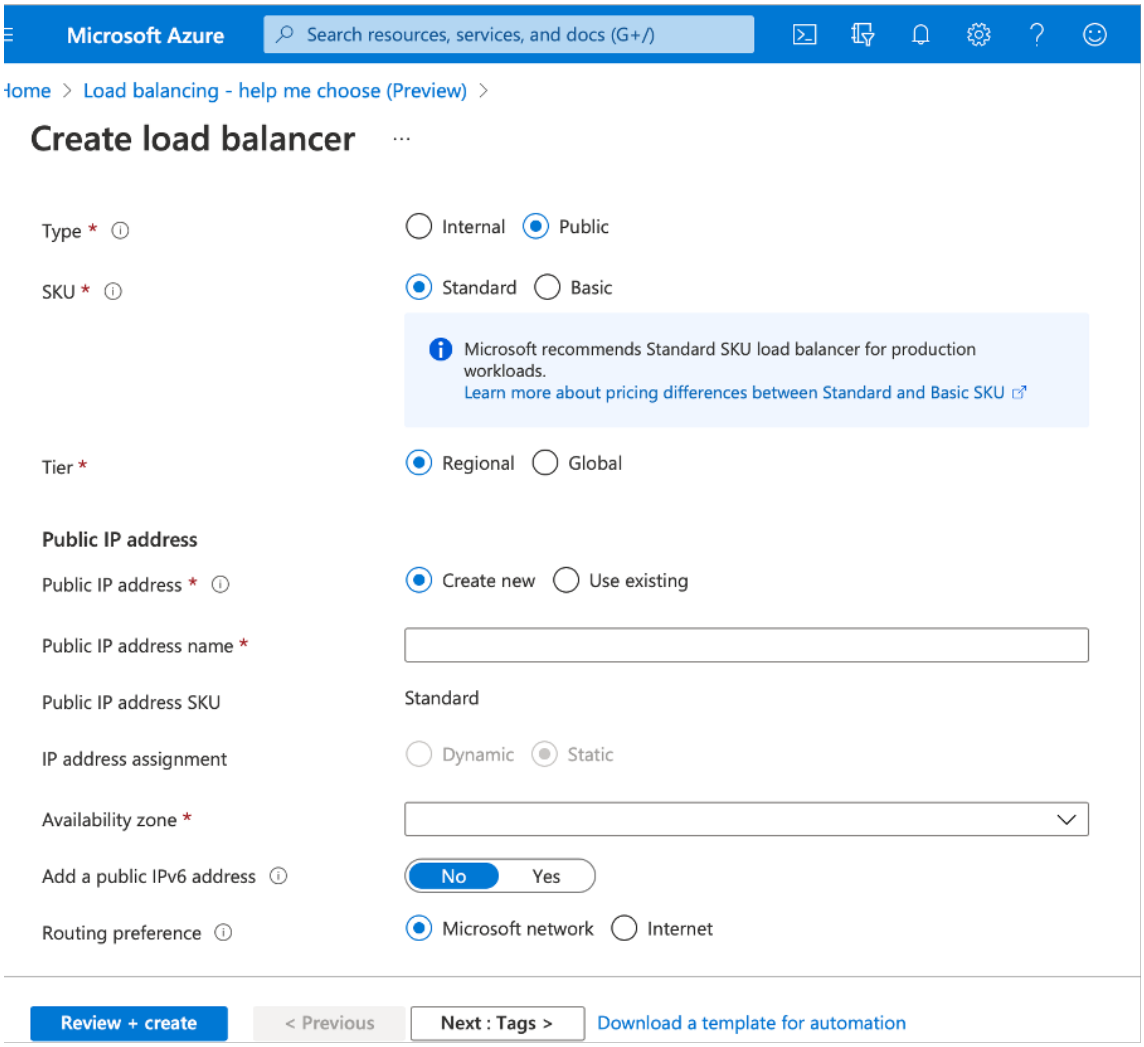
Weitere Informationen zur Konfiguration von Hochverfügbarkeits-Setups mit internen Azure-Load Balancern finden Sie unter Konfigurieren von HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlagemit Azure ILB.

Schritt 2. Erstellen Sie einen zusätzlichen Load Balancer (ILB) in Ihrer Ressourcengruppe. Wenn Sie in Schritt 1 einen externen Load Balancer erstellt haben, erstellen Sie jetzt einen internen Load Balancer und umgekehrt.

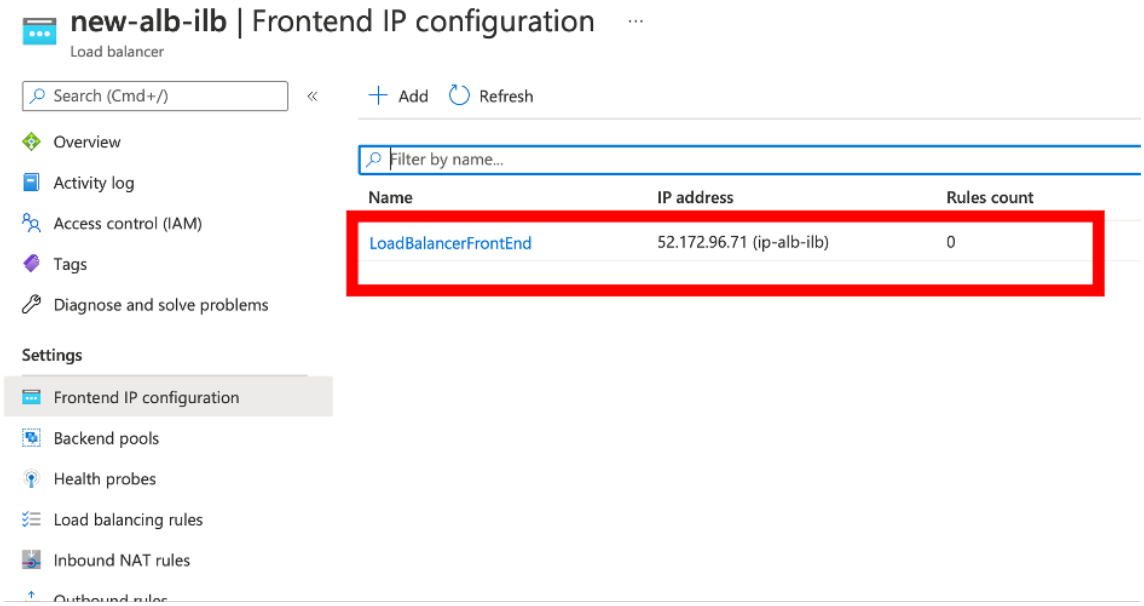
- Um einen internen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Intern**aus. Für das Feld **Subnet** müssen Sie Ihr NetScaler Client-Subnetz auswählen. Sie können eine statische IP-Adresse in diesem Subnetz angeben, vorausgesetzt, es gibt keine Konflikte. Wählen Sie andernfalls die dynamische IP-Adresse aus.



- Um einen externen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Public** und erstellen Sie hier die öffentliche IP-Adresse.



1. Nachdem Sie den Azure Load Balancer erstellt haben, navigieren Sie zur **Frontend-IP-Konfiguration** und notieren Sie sich die hier angezeigte IP-Adresse. Sie müssen diese IP-Adresse verwenden, während Sie den virtuellen ADC Load Balancing Server wie in Schritt 3 erstellen.



2. Auf der **Azure Load Balancer-Konfigurationsseite** hilft die ARM-Vorlagenbereitstellung bei der Erstellung der LB-Regel, Back-End-Pools und Integritätstests.
3. Fügen Sie die Client-NICs mit hoher Verfügbarkeit zum Backend-Pool für die ILB hinzu.
4. Erstellen Sie eine Gesundheitssonde (TCP, 9000-Port)
5. Erstellen Sie zwei Load Balancing-Regeln:
    - Eine LB-Regel für HTTP-Datenverkehr (Webapp-Anwendungsfall) auf Port 80. Die Regel muss auch den Backend-Port 80 verwenden. Wählen Sie den erstellten Backend-Pool und die Integritätsprobe aus. Floating IP muss aktiviert sein.
    - Eine weitere LB-Regel für HTTPS- oder CVAD-Datenverkehr auf Port 443. Der Prozess ist der gleiche wie der HTTP-Datenverkehr.

Schritt 3. Erstellen Sie auf dem primären Knoten der NetScaler Appliance einen virtuellen Lastausgleichsserver für ILB.

1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

```
add lb vserver <name> <serviceType> [<ILB Frontend IP address>] [<
    port>]
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vserver_name HTTP 52.172.96.71 80
<!--NeedCopy-->
```


> Hinweis:
>
> Verwenden Sie die Frontend-IP-Adresse des Load Balancers, die mit dem zusätzlichen Load Balancer verknüpft ist, den Sie in Schritt 2 erstellen.

2. Binden Sie einen Dienst an einen virtuellen Lastenausgleichsserver.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Weitere Informationen finden Sie unter Einrichten des grundlegenden Lastenausgleichs

Schritt 4: Alternativ zu Schritt 3 können Sie mit IPSets einen virtuellen Lastausgleichsserver für ILB erstellen.

1. Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu.

```
add nsip <ILB Frontend IP address> -type <type>
<!--NeedCopy-->
```

Beispiel:

```
add nsip 52.172.96.71 -type vip
<!--NeedCopy-->
```

2. Fügen Sie ein IPSet sowohl auf primären als auch auf sekundären Knoten hinzu.

```
add ipset <name>
<!--NeedCopy-->
```

Beispiel:

```
add ipset ipset1
<!--NeedCopy-->
```

3. Binden Sie IP-Adressen an den IP-Satz.

```
bind ipset <name> <ILB Frontend IP address>
<!--NeedCopy-->
```

Beispiel:


```
bind ipset ipset1 52.172.96.71
<!--NeedCopy-->
```

4. Stellen Sie den vorhandenen virtuellen LB-Server so ein, dass er das IPSet verwendet.

```
set lb vserver <vserver name> -ipset <ipset name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vserver_name -ipset ipset1
<!--NeedCopy-->
```

Weitere Informationen finden Sie unter Konfigurieren eines virtuellen Multi-IP-Servers.

Installieren Sie eine NetScaler VPX-Instanz auf Azure VMware Solution

May 11, 2023

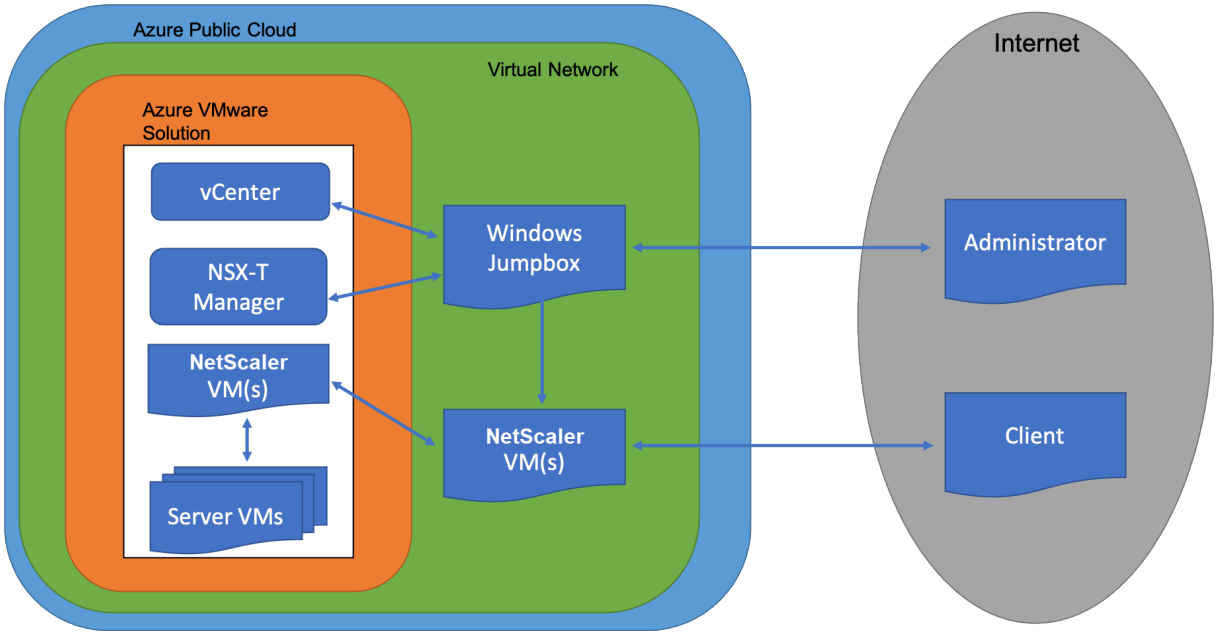
Azure VMware Solution (AVS) bietet Ihnen private Clouds, die vSphere-Cluster enthalten, die aus einer dedizierten Bare-Metal-Azure-Infrastruktur basieren. Die minimale Erstbereitstellung beträgt drei Hosts, aber zusätzliche Hosts können einzeln hinzugefügt werden, bis zu maximal 16 Hosts pro Cluster. Alle bereitgestellten Private Clouds verfügen über vCenter Server, vSAN, vSphere und NSX-T.

Mit der VMware Cloud (VMC) auf Azure können Sie Cloud-softwaredefinierte Rechenzentren (SDDC) auf Azure mit der Anzahl der gewünschten ESX-Hosts erstellen. Der VMC auf Azure unterstützt NetScaler VPX-Bereitstellungen. VMC stellt eine Benutzeroberfläche bereit, die gleiche wie bei vCenter vor Ort ist. Es funktioniert ähnlich wie die ESX-basierten NetScaler VPX-Bereitstellungen.

Das folgende Diagramm zeigt die Azure VMware-Lösung in der Azure Public Cloud, auf die ein Administrator oder ein Client über das Internet zugreifen kann. Ein Administrator kann Workload- oder Server-VMs mit der Azure VMware-Lösung erstellen, verwalten und konfigurieren. Der Administrator kann von einer Windows Jumpbox aus auf das webbasierte vCenter und den NSX-T Manager des AVS zugreifen. Sie können die NetScaler VPX-Instanzen (eigenständige oder Hochverfügbarkeitspaar) und Server-VMs in Azure VMware Solution mit vCenter erstellen und das entsprechende Netzwerk mit NSX-T Manager verwalten. Die NetScaler VPX-Instanz auf AVS funktioniert ähnlich dem lokalen VMware-Host-Cluster. AVS wird von einer Windows Jumpbox aus verwaltet, die im selben virtuellen Netzwerk erstellt wird.

Ein Client kann nur auf den AVS-Dienst zugreifen, indem er sich mit dem VIP von ADC verbindet. Eine andere NetScaler VPX-Instanz außerhalb von Azure VMware Solution, aber im selben virtuellen

Azure-Netzwerk, hilft dabei, den VIP der NetScaler VPX-Instanz in Azure VMware Solution als Dienst hinzuzufügen. Je nach Anforderung können Sie die NetScaler VPX-Instanz so konfigurieren, dass sie Dienste über das Internet bereitstellt.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Dokumentation zu Azure VMware Solution.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer Azure VMware Solution Private Cloud.
- Weitere Informationen zum Erstellen einer Windows Jump Box-VM für den Zugriff und die Verwaltung der Azure VMware-Lösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware Solution
- Laden Sie in der Windows Jump Box VM die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution
- VPX-Lizenzdateien abrufen.
- Virtuelle Maschinen (VMs), die in die Azure VMware Solution Private Cloud erstellt oder migriert wurden, müssen an ein Netzwerksegment angeschlossen sein.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX nCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> Hinweis
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Systemvoraussetzungen für die Installation des OVF-Tools beschrieben.

Tabelle 2. Systemvoraussetzungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen

Komponente	Voraussetzung
Netzwerkkarte	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

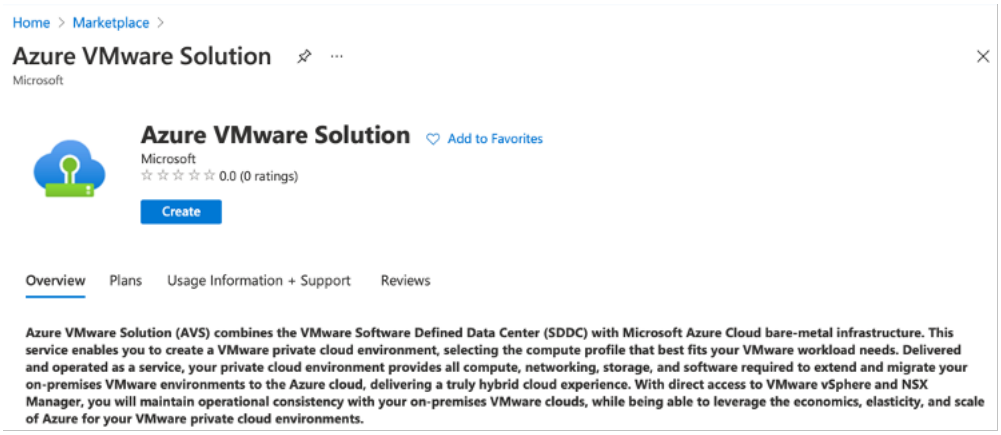
Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-<Releasenummer>-<Buildnummer>-disk1.vmdk (z. B. NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-<Releasenummer>-<Buildnummer>.ovf (z. B. NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<Releasenummer>-<Buildnummer>.mf (z. B. NSVPX-ESX-13.0-79.64.mf)

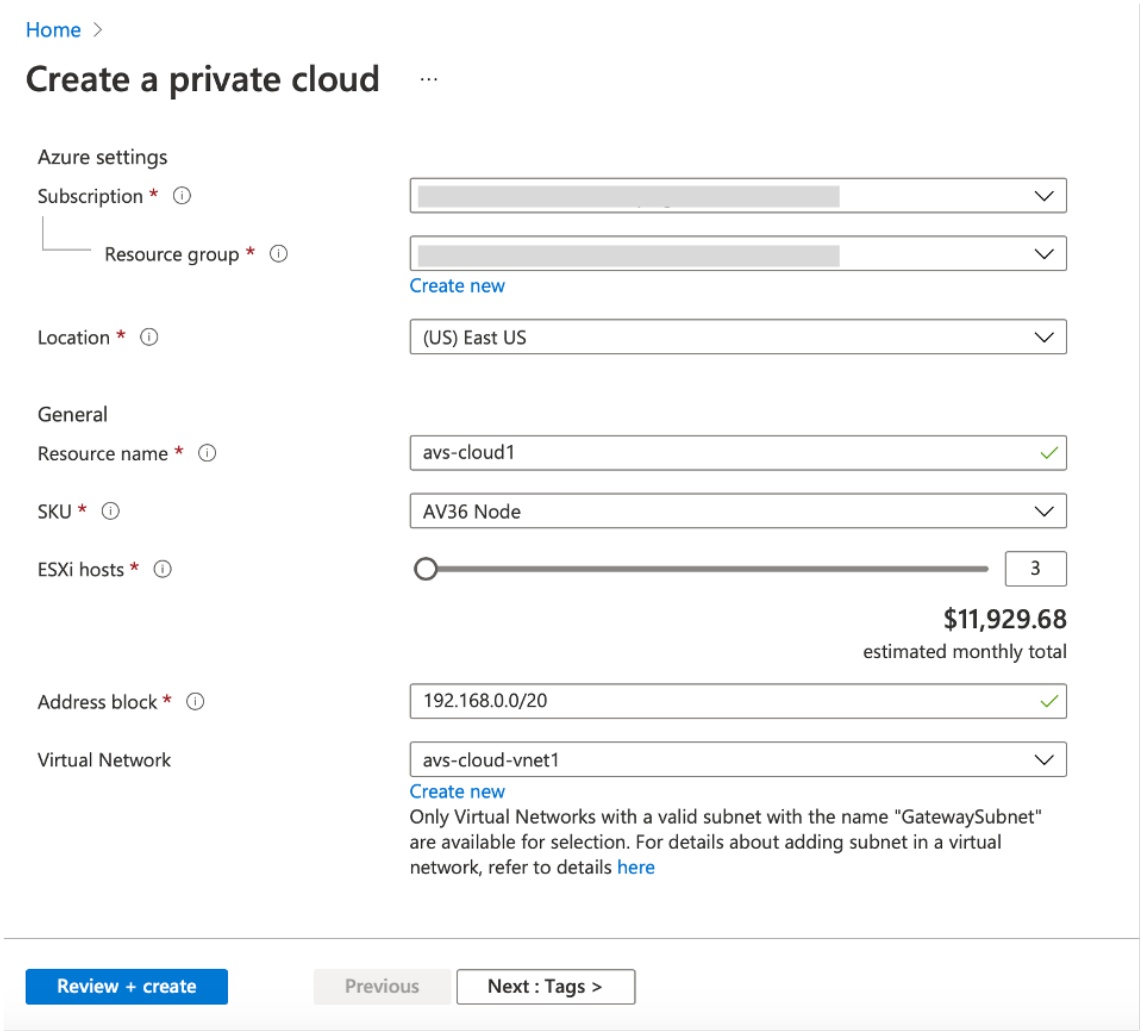
Bereitstellen von Azure VMware-Lösung

1. Melden Sie sich bei Ihrem Microsoft Azure-Portalan und navigieren Sie zu **Azure Marketplace**.
2. Suchen Sie im **Azure Marketplace**nach **Azure VMware Solution** und klicken Sie auf **Erstellen**.

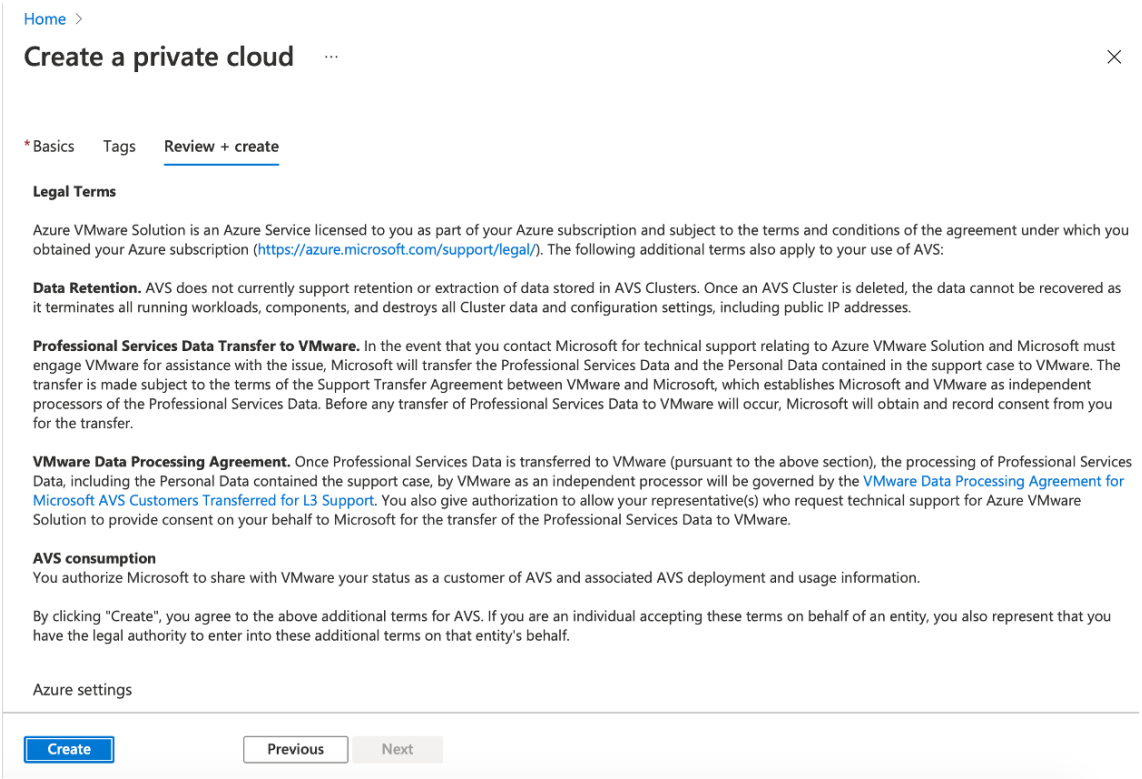


3. Geben **Sie auf der Seite Private Cloud erstellen** die folgenden Details ein:

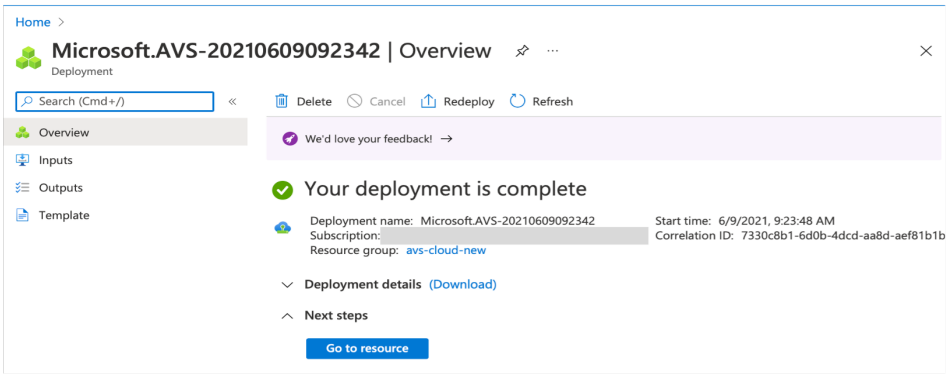
   - Wählen Sie mindestens 3 ESXi-Hosts aus, um den Standardcluster Ihrer Private Cloud zu erstellen.
   - Verwenden Sie für das Feld **Adressblock/22** Adressraum.
   - Stellen Sie für das **virtuelle Netzwerk**sicher, dass sich der CIDR-Bereich nicht mit einem Ihrer on-premises oder anderen Azure-Subnetze (virtuelle Netzwerke) oder mit dem Gateway-Subnetz überschneidet.
   - Das Gateway-Subnetz wird verwendet, um die Verbindung mit Private Cloud weiterzuleiten.



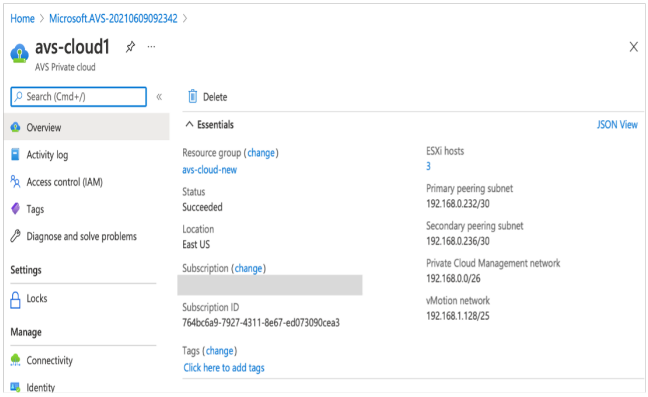
4. Klicken Sie auf **Review + Erstellen**.
5. Prüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.



6. Klicken Sie auf **Erstellen**. Der Provisioning-Prozess der Private Cloud beginnt. Es kann bis zu zwei Stunden dauern, bis die Private Cloud bereitgestellt wird.



7. Klicken Sie auf **Gehe zu Ressource**, um die erstellte Private Cloud zu überprüfen.



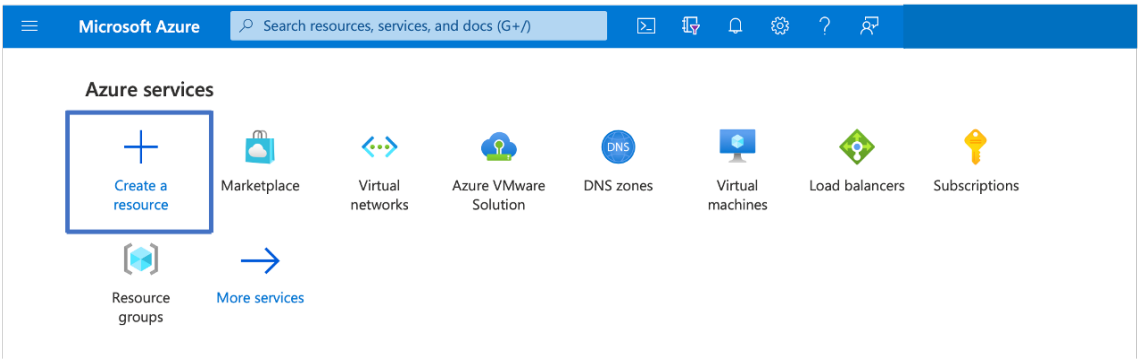
> Hinweis
>
> Um auf diese Ressource zugreifen zu können, benötigen Sie eine VM in Windows, die als Sprungbox fungiert.

Verbinden Sie sich mit einer virtuellen Azure-Maschine unter Windows

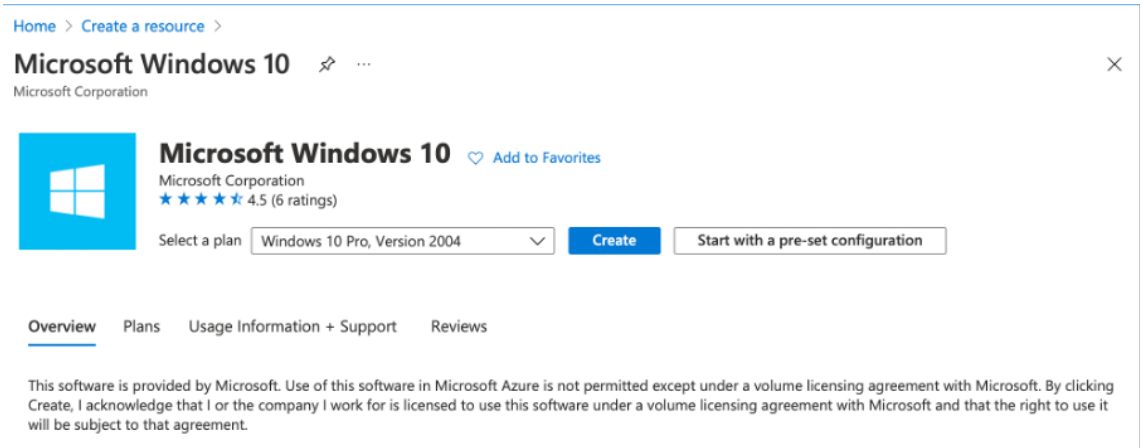
Dieses Verfahren zeigt Ihnen, wie Sie das Azure-Portal verwenden, um eine virtuelle Maschine (VM) in Azure bereitzustellen, auf der Windows Server 2019 ausgeführt wird. Um Ihre VM in Aktion zu sehen, rdp dann auf die VM und installieren den IIS-Webserver.

Um auf die von Ihnen erstellte Private Cloud zugreifen zu können, müssen Sie eine Windows Jump-Box innerhalb desselben virtuellen Netzwerks erstellen.

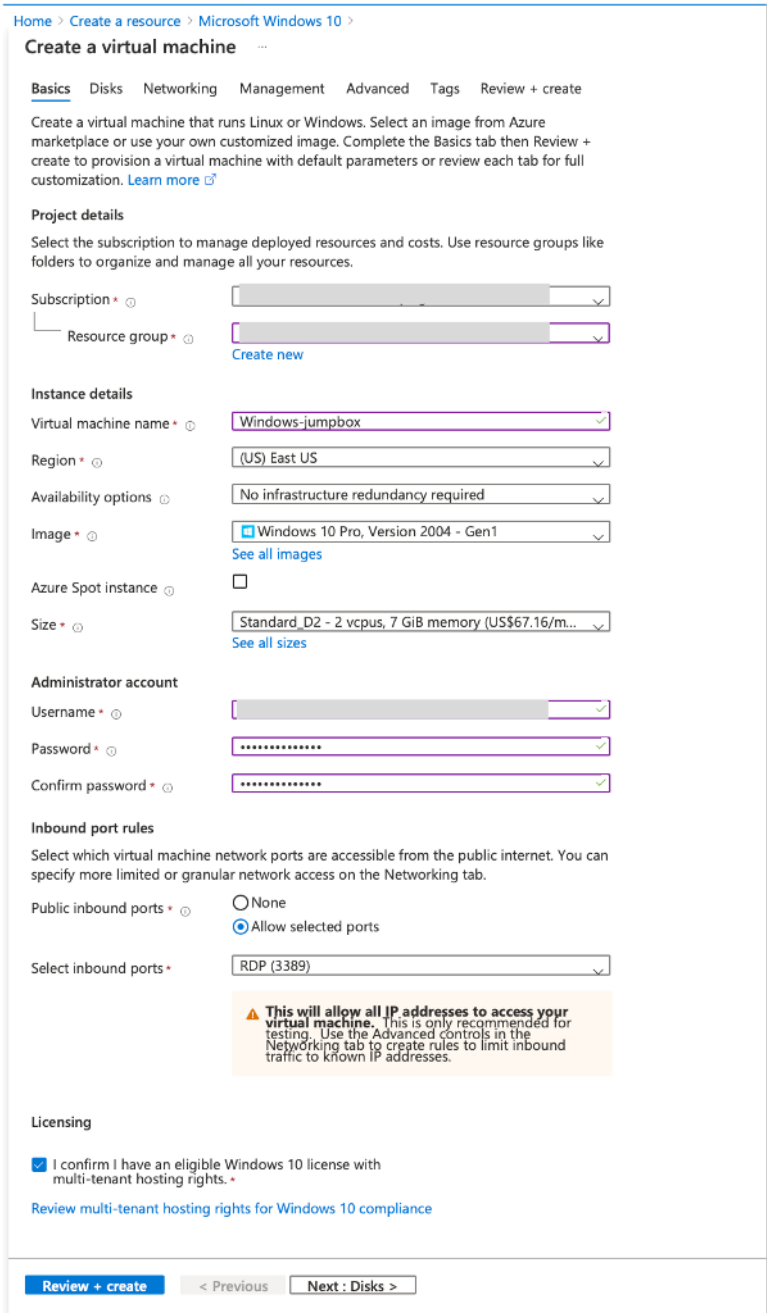
1. Wechseln Sie zum **Azure-Portal**und klicken Sie auf **Ressource erstellen**.



2. Suchen Sie nach **Microsoft Windows 10**und klicken Sie auf **Erstellen**.



3. Erstellen Sie eine virtuelle Maschine (VM), auf der Windows Server 2019 ausgeführt wird. Die Seite " **Virtuelle Maschine erstellen** " wird angezeigt. Geben Sie alle Details auf der Registerkarte **Grundlagen** ein und aktivieren Sie das Kontrollkästchen **Lizenzierung** . Belassen Sie die verbleibenden Standardeinstellungen und wählen Sie dann unten auf der Seite die Schaltfläche **Review + erstellen** .



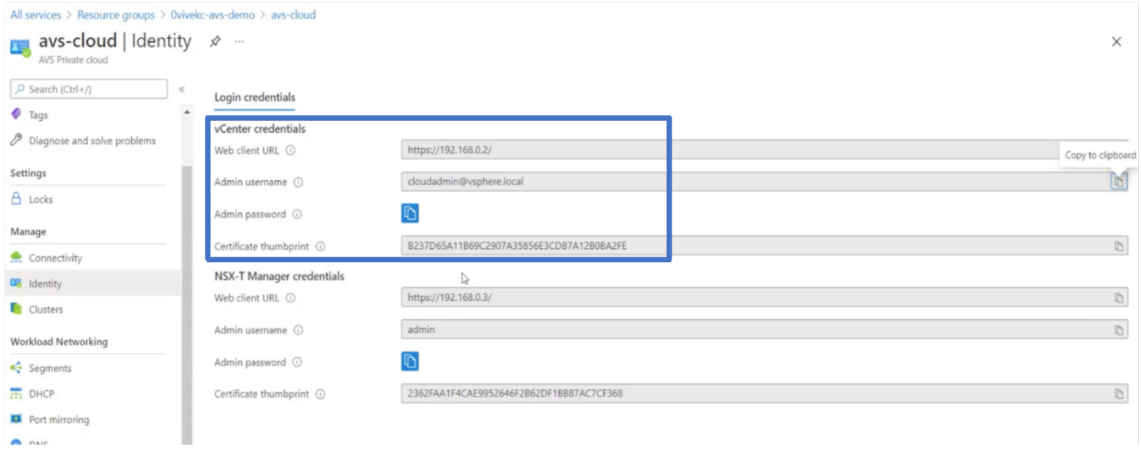
4. Nachdem die Validierung ausgeführt wurde, klicken Sie unten auf der Seite auf die Schaltfläche **Erstellen** .
5. Wählen Sie nach Abschluss der Bereitstellung **Gehe zu Ressource**aus.
6. Wechseln Sie zu der von Ihnen erstellten Windows-VM. Verwenden Sie die öffentliche IP-Adresse der Windows-VM und stellen Sie eine Verbindung mit RDP her.

   Verwenden Sie die Schaltfläche **Verbinden** im Azure-Portal, um eine Remotedesktop-Sitzung (RDP) von einem Windows-Desktop aus zu starten. Zuerst stellen Sie eine Verbindung mit der virtuellen Maschine her und melden sich dann an.

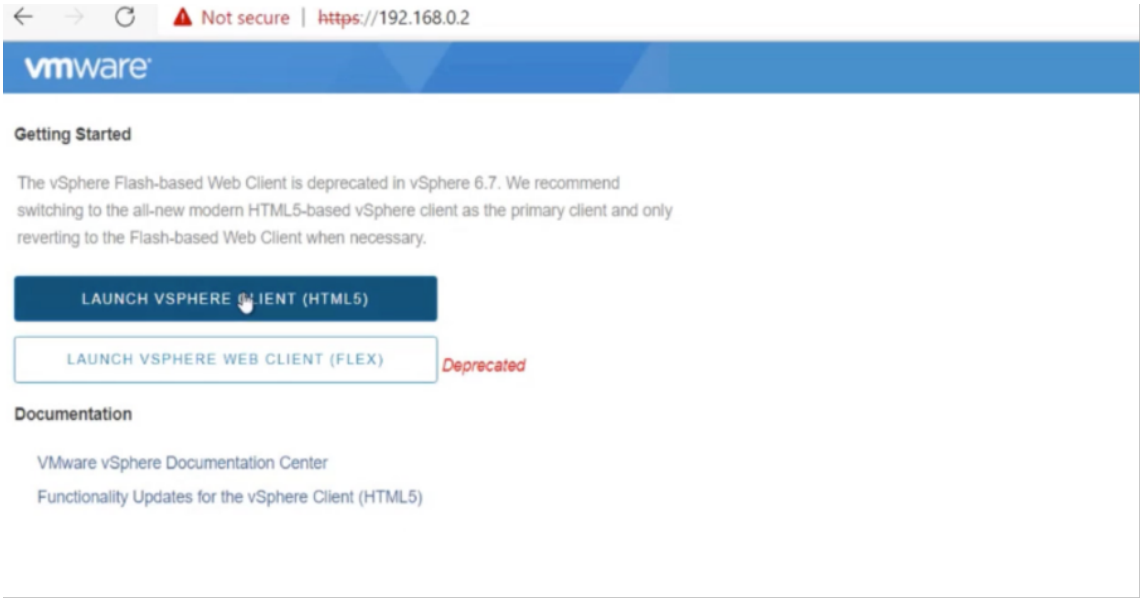
Um eine Verbindung mit einer Windows-VM von einem Mac aus herzustellen, müssen Sie einen RDP-Client für Mac wie Microsoft Remote Desktop installieren. Weitere Informationen finden Sie unter Herstellen und Melden Sie sich bei einer virtuellen Azure-Maschine unter Windowsan.

Greifen Sie auf Ihr Private Cloud vCenter Portal zu

1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten**die Option **Identität**aus. Notieren Sie sich die vCenter-Anmeldeinformationen.

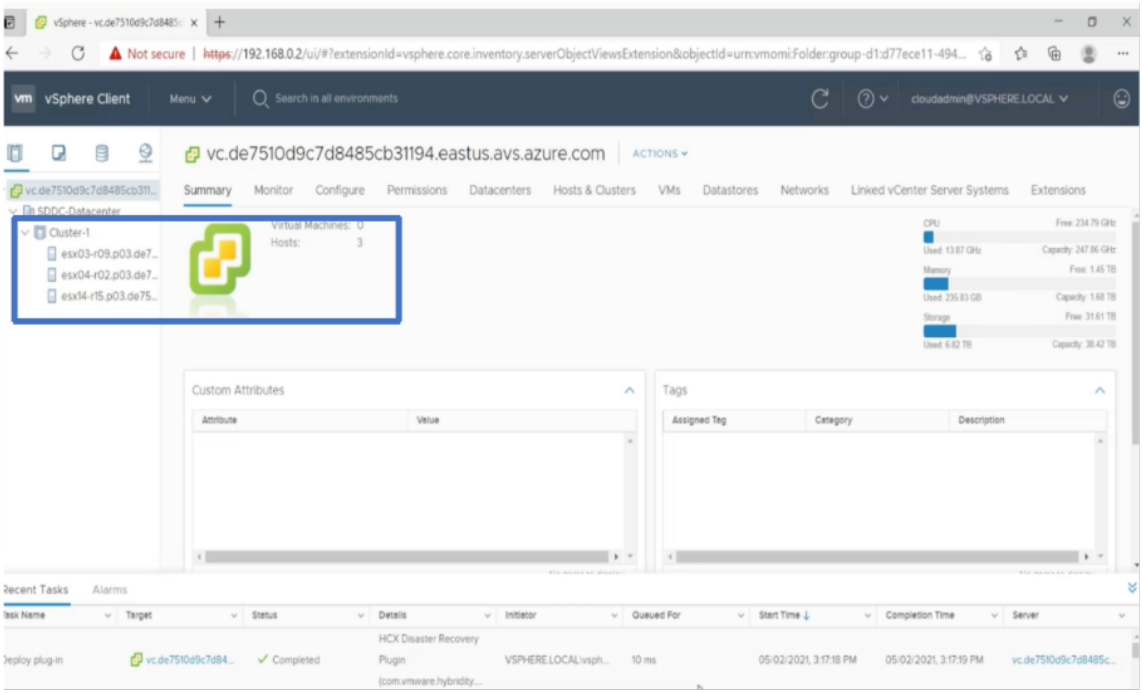


2. Starten Sie den vSphere-Client, indem Sie die vCenter-Webclient-URL eingeben.



3. Melden Sie sich mit den vCenter-Anmeldeinformationen Ihrer Azure VMware Solution Private Cloud bei VMware vSphere an.

4. Im vSphere-Client können Sie die ESXi-Hosts überprüfen, die Sie im Azure-Portal erstellt haben.



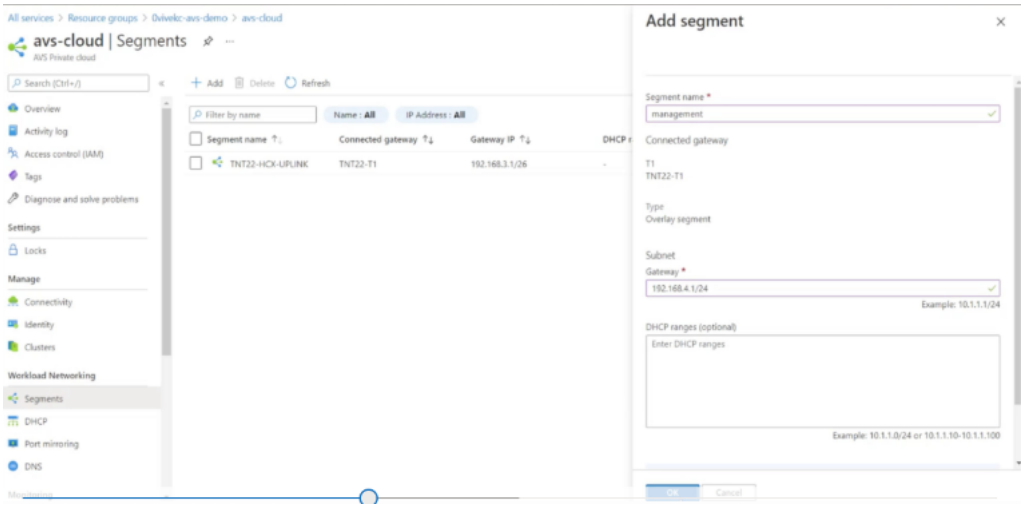
Weitere Informationen finden Sie unter Zugriff auf Ihr Private Cloud vCenter-Portal.

Erstellen Sie ein NSX-T-Segment im Azure-Portal

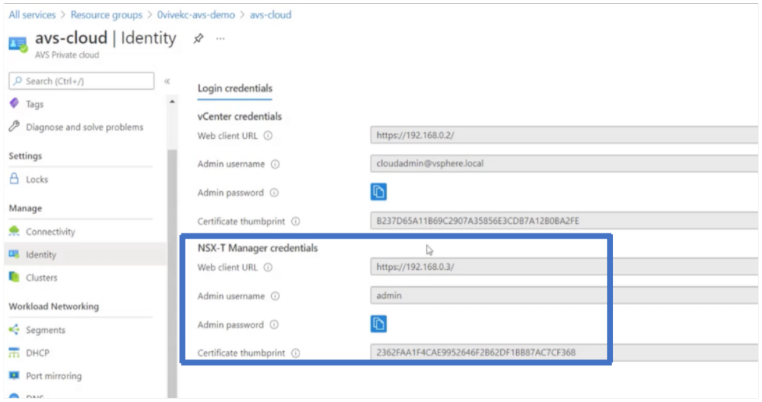
Sie können ein NSX-T-Segment über die Azure VMware Solution Console im Azure-Portal erstellen und konfigurieren. Diese Segmente sind mit dem Standard-Tier-1-Gateway verbunden, und die Workloads in diesen Segmenten erhalten Ost-West- und Nord-Süd-Konnektivität. Sobald Sie das Segment er-

stellt haben, wird es in NSX-T Manager und vCenter angezeigt.

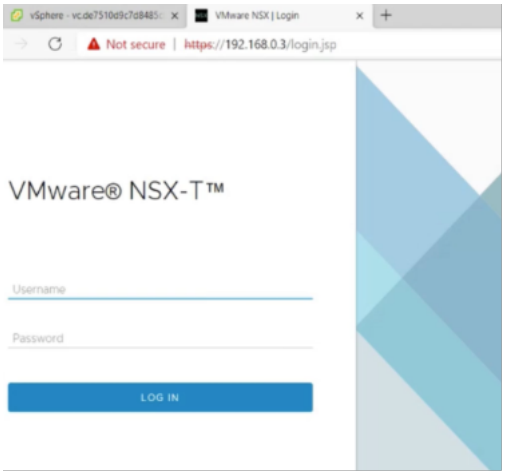
1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Workload-NetzwerkSegmente > Hinzufügen**aus. Geben Sie die Details für das neue logische Segment ein und wählen Sie**OK**aus. Sie können drei separate Segmente für Client-, Management- und Server-Schnittstellen erstellen.



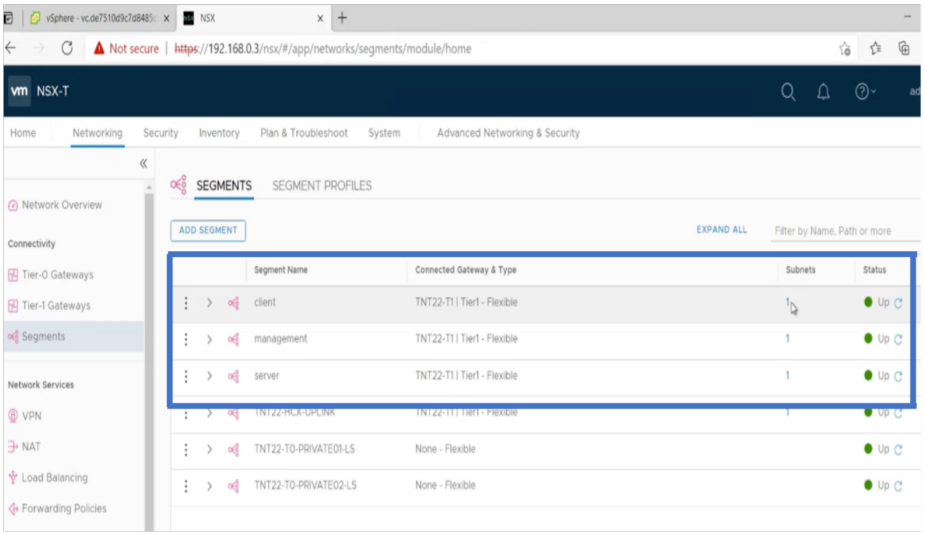
2. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten**die Option **Identität**aus. Notieren Sie sich die Anmeldeinformationen von NSX-T Manager.



3. Starten Sie den VMware NSX-T Manager, indem Sie die URL des NSX-T-Webclients eingeben.



4. Im NSX-T-Manager unter **Netzwerk > Segmente**sehen Sie alle Segmente, die Sie erstellt haben. Sie können die Subnetze auch überprüfen.



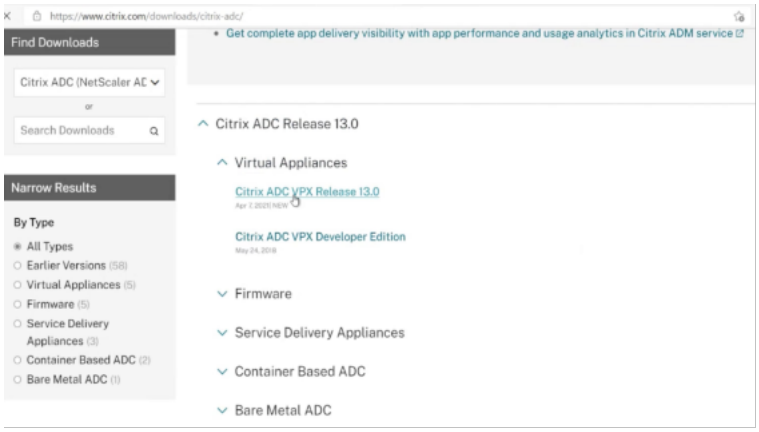
Weitere Informationen finden Sie unter Erstellen eines NSX-T-Segments im Azure-Portal.

Installieren einer NetScaler VPX Instanz in VMware Cloud

Nachdem Sie VMware Software-Defined Data Center (SDDC) installiert und konfiguriert haben, können Sie das SDDC verwenden, um virtuelle Appliances in der VMware-Cloud zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des auf dem SDDC verfügbaren Speichers ab.

Um NetScaler VPX-Instanzen in der VMware Cloud zu installieren, führen Sie die folgenden Schritte in Windows Jumpbox VM aus:

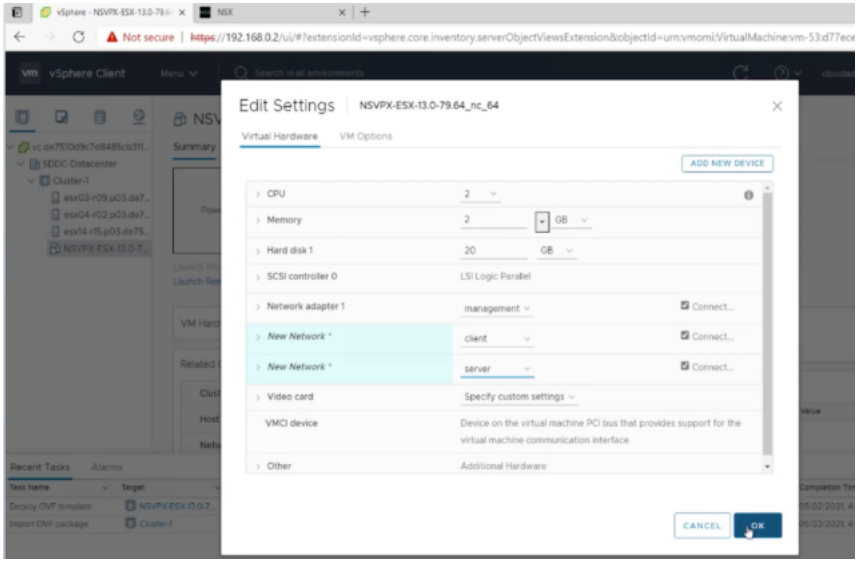
1. Laden Sie die Setup-Dateien der NetScaler VPX-Instanz für den ESXi-Host von der NetScaler-Downloadseite herunter.



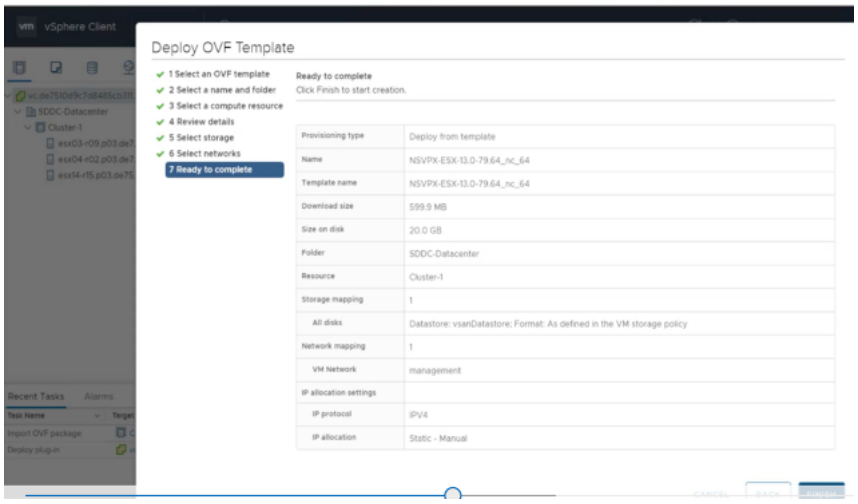
2. Öffnen Sie VMware SDDC in der Windows Jumpbox.
3. Geben Sie in die Felder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlagebereitstellen im Feld Aus Datei bereitstellen**zu dem Speicherort, an dem Sie die Setupdateien der NetScaler VPX-Instanz gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf**Weiter**.

   > HINWEIS:
   >
   > Standardmäßig verwendet die NetScaler VPX-Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird. Die Verfügbarkeit der VMXNET3-Schnittstelle ist durch die Azure-Infrastruktur begrenzt und ist möglicherweise in Azure VMware Solution nicht verfügbar.

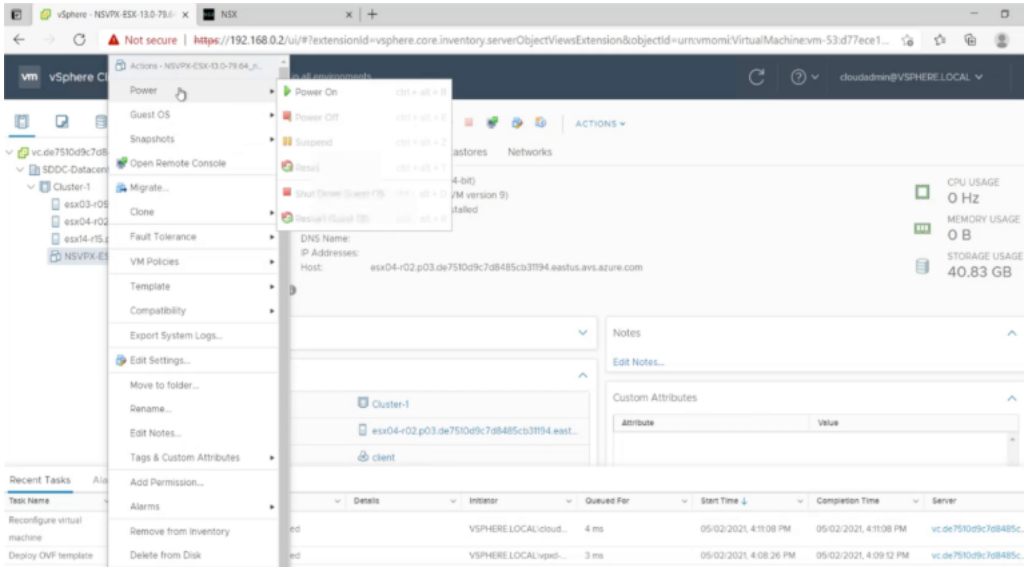
6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem VMware SDDC konfiguriert haben. Klicken Sie auf **OK**.



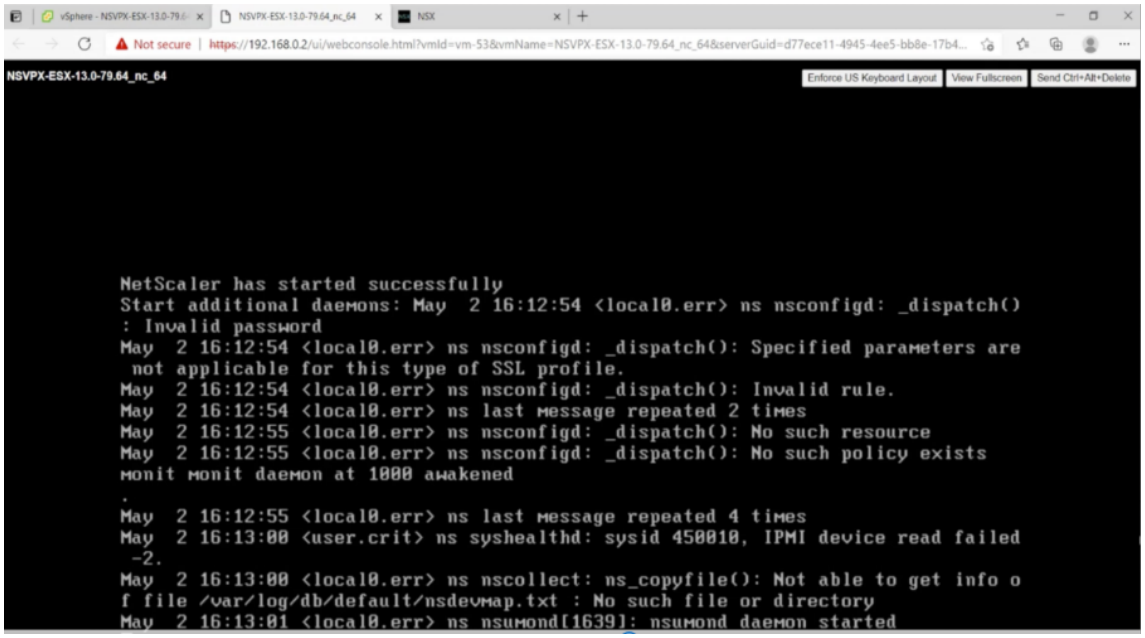
7. Klicken Sie auf **Fertig stellen**, um mit der Installation einer virtuellen Appliance auf VMware SDDC zu beginnen.



8. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.



9. Sie sind jetzt vom vSphere-Client aus mit der NetScaler VM verbunden.



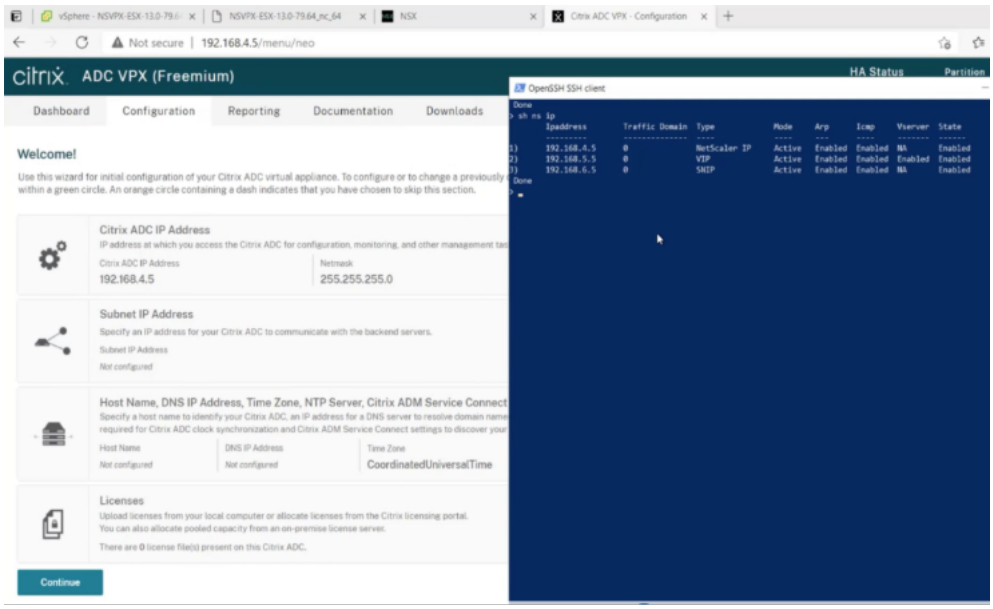
10. Um mit den SSH-Schlüsseln auf die NetScaler-Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

```
ssh nsroot@<management IP address>
<!--NeedCopy-->
```

Beispiel:

```
ssh nsroot@192.168.4.5
<!--NeedCopy-->
```


11. Sie können die ADC-Konfiguration mit dem Befehl `show ns ip` überprüfen.

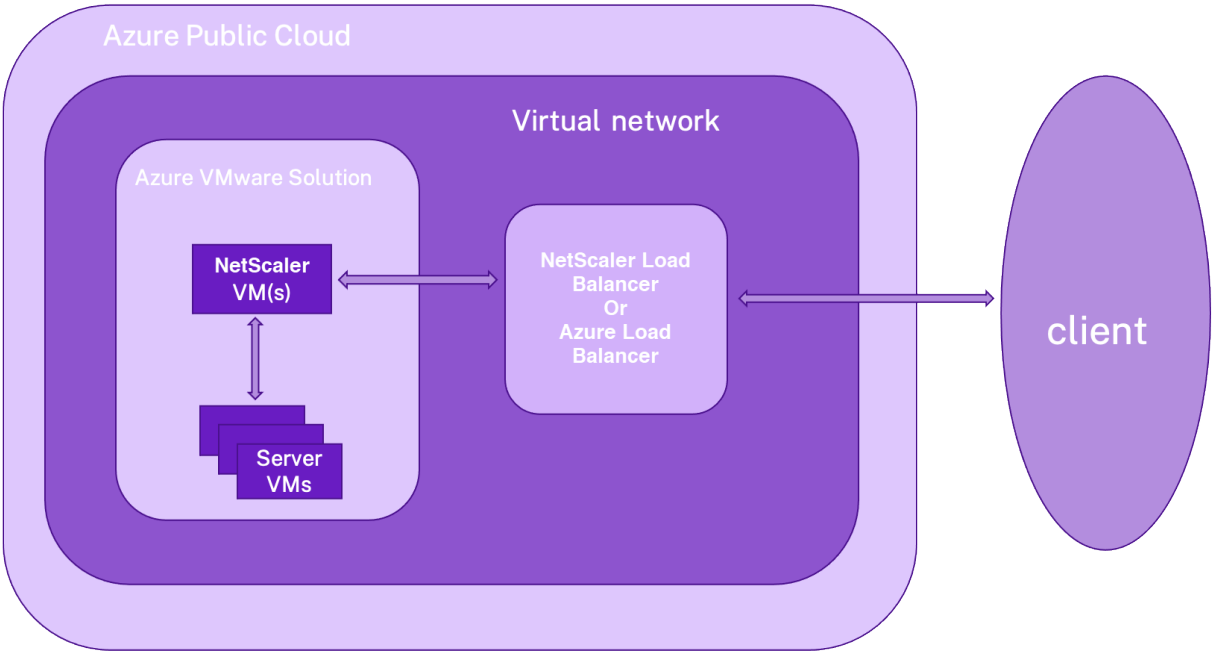


Eigenständige NetScaler VPX-Instanz auf der Azure VMware-Lösung konfigurieren

May 11, 2023

Sie können eine eigenständige NetScaler VPX-Instanz auf der Azure VMware-Lösung (AVS) für internetfähige Anwendungen konfigurieren.

Das folgende Diagramm zeigt die eigenständige NetScaler VPX-Instanz auf Azure VMware Solution. Ein Client kann auf den AVS-Dienst zugreifen, indem er eine Verbindung zur virtuellen IP-Adresse (VIP) von NetScaler innerhalb des AVS herstellt. Sie können dies erreichen, indem Sie einen NetScaler Load Balancer oder die Azure Load Balancer-Instanz außerhalb von AVS, jedoch im selben virtuellen Azure-Netzwerk bereitstellen. Konfigurieren Sie den Load Balancer für den Zugriff auf den VIP der NetScaler VPX-Instanz innerhalb des AVS-Dienstes.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, lesen Sie die folgenden Azure-Voraussetzungen:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Dokumentation zu Azure VMware Solution.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer Azure VMware Solution Private Cloud.
- Weitere Informationen zum Erstellen einer Windows Jumpbox-VM für den Zugriff auf und die Verwaltung der Azure VMware-Lösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware-Lösung.
- Laden Sie in der Windows Jump Box VM die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution
- Weitere Informationen zum Installieren einer NetScaler VPX-Instanz in der VMware Cloud finden Sie unter Installieren einer NetScaler VPX-Instanz in der VMware-Cloud.

Konfigurieren einer eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des NetScaler Load Balancer

Befolgen Sie diese Schritte, um die eigenständige NetScaler VPX-Instanz auf AVS für internetorientierte Anwendungen mithilfe des NetScaler Load Balancer zu konfigurieren.

1. Stellen Sie eine NetScaler VPX-Instanz in der Azure Cloud bereit. Weitere Informationen finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz.

   > Hinweis:
   >
   > Stellen Sie sicher, dass es im selben virtuellen Netzwerk wie die Azure VMware Cloud bereitgestellt wird.

2. Konfigurieren Sie die NetScaler VPX-Instanz für den Zugriff auf die VIP-Adresse von NetScaler VPX, das auf AVS bereitgestellt wird.

   a) Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

   ```
   add lb vserver <name> <serviceType> [<vip>] [<port>]
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   add lb vserver lb1 HTTPS 172.31.0.6 443
   <!--NeedCopy-->
   ```

   b) Fügen Sie einen Dienst hinzu, der eine Verbindung zum VIP von NetScaler VPX herstellt, der auf AVS bereitgestellt wird.

   ```
   add service <name> <ip> <serviceType> <port>
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   add service webserver1 192.168.4.10 HTTP 80
   <!--NeedCopy-->
   ```

   c) Binden Sie einen Dienst an den virtuellen Lastausgleichsserver.

   ```
   bind lb vserver <name> <serviceName>
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   bind lb vserver lb1 webserver1
   <!--NeedCopy-->
   ```


Konfigurieren der eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des Azure Load Balancer

Befolgen Sie diese Schritte, um die eigenständige NetScaler VPX-Instanz auf AVS für internetorientierte Anwendungen mithilfe des Azure Load Balancer zu konfigurieren.

1. Konfigurieren Sie eine Azure Load Balancer-Instanz in Azure Cloud Weitere Informationen finden Sie in der Azure-Dokumentation zum Erstellen des Load Balancers.
2. Fügen Sie die VIP-Adresse der NetScaler VPX-Instanz, die auf AVS bereitgestellt wird, zum Backend-Pool hinzu.

   Der folgende Azure-Befehl fügt eine Back-End-IP-Adresse zum Back-End-Adresspool des Lastenausgleichs hinzu.

```
az network lb address-pool address add
                                    --resource-group <Azure VMC
                                       Resource Group>
                                    --lb-name <LB Name>
                                    --pool-name <Backend pool name
                                       >
                                    --vnet <Azure VMC Vnet>
                                    --name <IP Address name>
                                    --ip-address <VIP of ADC in
                                       VMC>
<!--NeedCopy-->
```

   > Hinweis:
   >
   > Stellen Sie sicher, dass der Azure Load Balancer im selben virtuellen Netzwerk wie die Azure VMware-Cloud bereitgestellt wird.

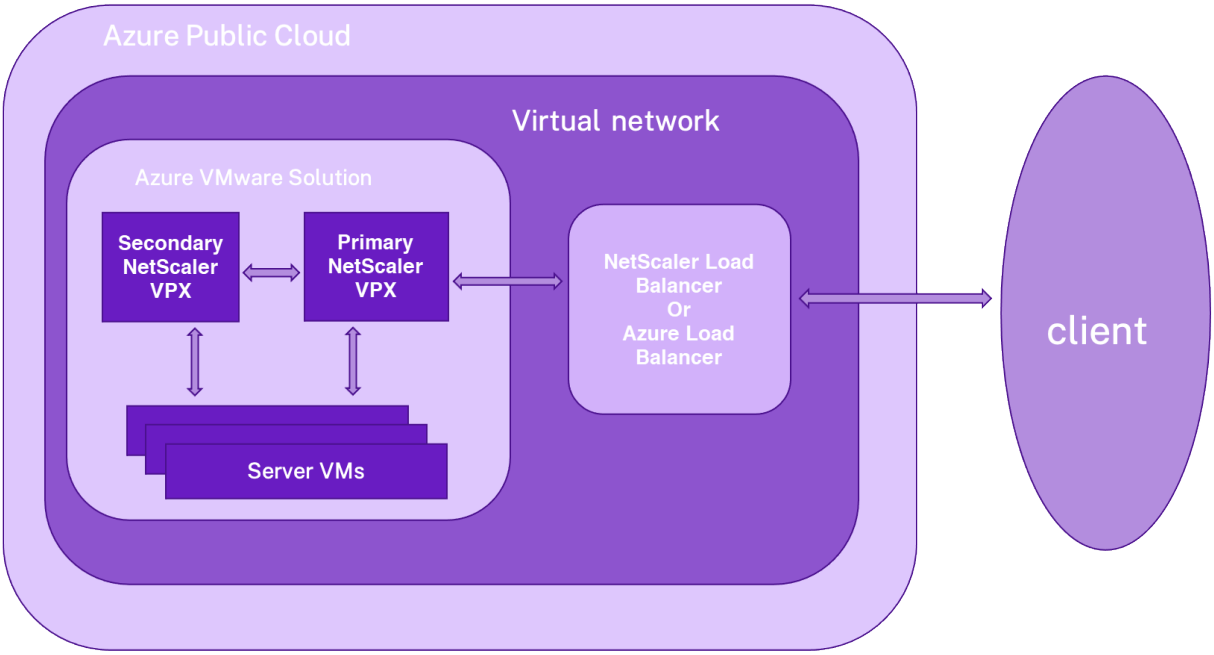
NetScaler VPX-Hochverfügbarkeitssetups auf Azure VMware-Lösung konfigurieren

May 11, 2023

Sie können ein NetScaler VPX HA-Setup auf Azure VMware-Lösung (AVS) für internetfähige Anwendungen konfigurieren.

Das folgende Diagramm zeigt das NetScaler VPX HA-Paar auf AVS. Ein Client kann auf den AVS-Dienst zugreifen, indem er sich mit dem VIP des primären ADC-Knotens innerhalb des AVS verbindet. Sie können dies erreichen, indem Sie einen NetScaler Load Balancer oder die Azure Load Balancer-Instanz

außerhalb von AVS, jedoch im selben virtuellen Azure-Netzwerk bereitstellen. Konfigurieren Sie den Load Balancer für den Zugriff auf den VIP des primären ADC-Knotens innerhalb des AVS-Dienstes.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, lesen Sie die folgenden Azure-Voraussetzungen:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Dokumentation zu Azure VMware Solution.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer Azure VMware Solution Private Cloud.
- Weitere Informationen zum Erstellen einer Windows Jumpbox-VM für den Zugriff auf und die Verwaltung der Azure VMware-Lösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware-Lösung.
- Laden Sie in der Windows Jump Box VM die Setupdateien der NetScaler VPX Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware-Lösung.

Konfigurationsschritte

Befolgen Sie diese Schritte, um das NetScaler VPX Hochverfügbarkeitssetup in AVS für internetfähige Anwendungen zu konfigurieren.

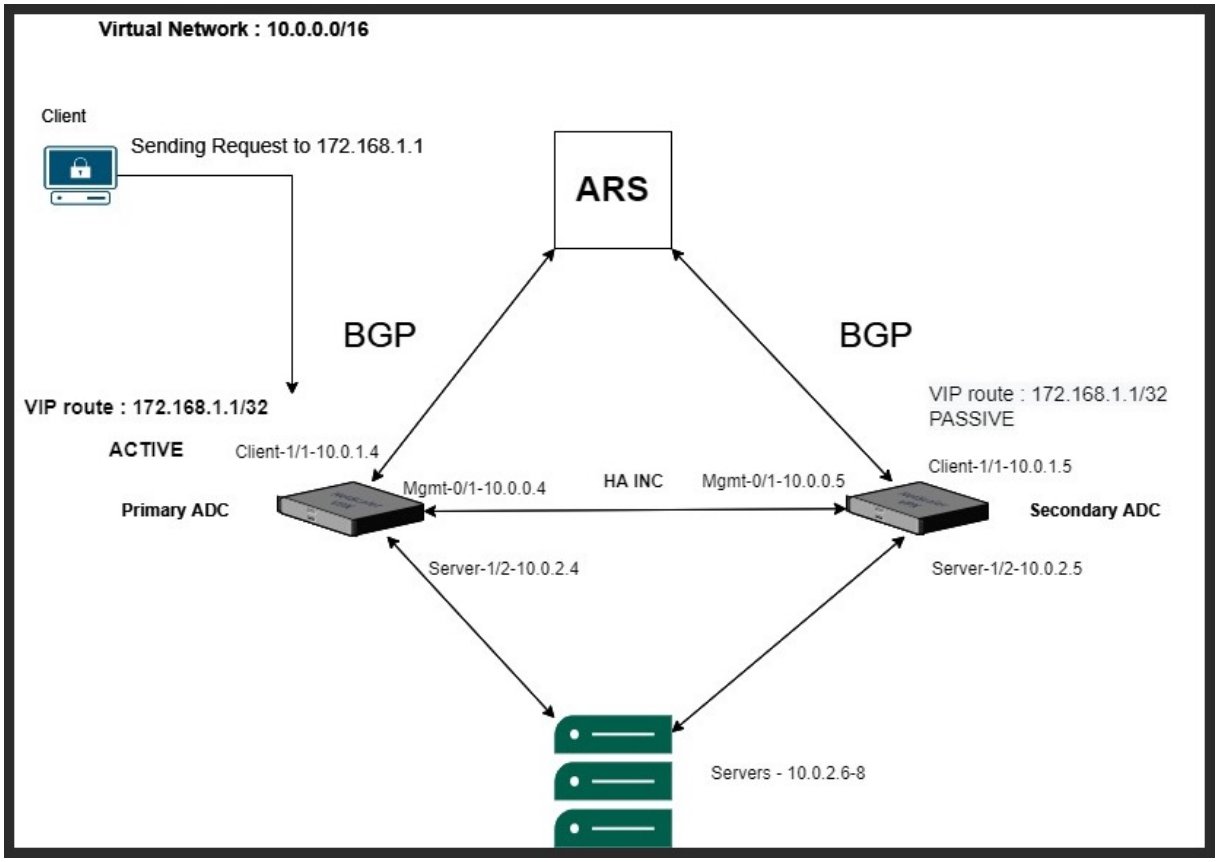
1. Erstellen Sie zwei NetScaler VPX-Instanzen in der VMware Cloud. Weitere Informationen finden Sie unter Installieren einer NetScaler VPX-Instanz in der VMware-Cloud.
2. Konfigurieren Sie das NetScaler HA-Setup. Weitere Informationen finden Sie unter Konfigurieren von Hochverfügbarkeit.
3. Konfigurieren Sie das NetScaler HA-Setup so, dass es für internetorientierte Anwendungen zugänglich ist.
    - Informationen zum Konfigurieren der NetScaler VPX-Instanz mit dem NetScaler Load Balancer finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des NetScaler Load Balancer.
    - Informationen zum Konfigurieren der NetScaler VPX-Instanz mithilfe des Azure-Lastausgleichsdiensts finden Sie unter Konfigurieren der eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des Azure Load Balancer.

Azure-Routenserver mit NetScaler VPX HA-Paar konfigurieren

May 11, 2023

Sie können den Azure-Routenserver mit der NetScaler VPX-Instanz konfigurieren, um die mit dem virtuellen Netzwerk konfigurierten VIP-Routen mit dem BGP-Protokoll auszutauschen. Der NetScaler kann im Standalone- oder HA-INC-Modus bereitgestellt und dann mit BGP konfiguriert werden. Für diese Bereitstellung ist kein Azure Load Balancer (ALB) vor dem ADC HA-Paar erforderlich.

Das folgende Diagramm zeigt, wie eine VPX HA-Topologie in den Azure-Routenserver integriert ist. Jede der ADC-Instanzen verfügt über 3 Schnittstellen: eine für die Verwaltung, eine für den Client-Datenverkehr und eine für den Serververkehr.



Das Topologiediagramm verwendet die folgenden IP-Adressen.

Beispiel-IP-Konfiguration für die primäre ADC-Instanz:

```
NSIP: 10.0.0.4/24
SNIP on 1/1: 10.0.1.4/24
SNIP on 1/2: 10.0.2.4/24
VIP: 172.168.1.1/32
<!--NeedCopy-->
```

Beispiel-IP-Konfiguration für die sekundäre ADC-Instanz:

```
NSIP: 10.0.0.5/24
SNIP on 1/1: 10.0.1.5/24
SNIP on 1/2: 10.0.2.5/24
VIP: 172.168.1.1/32
<!--NeedCopy-->
```

Voraussetzungen

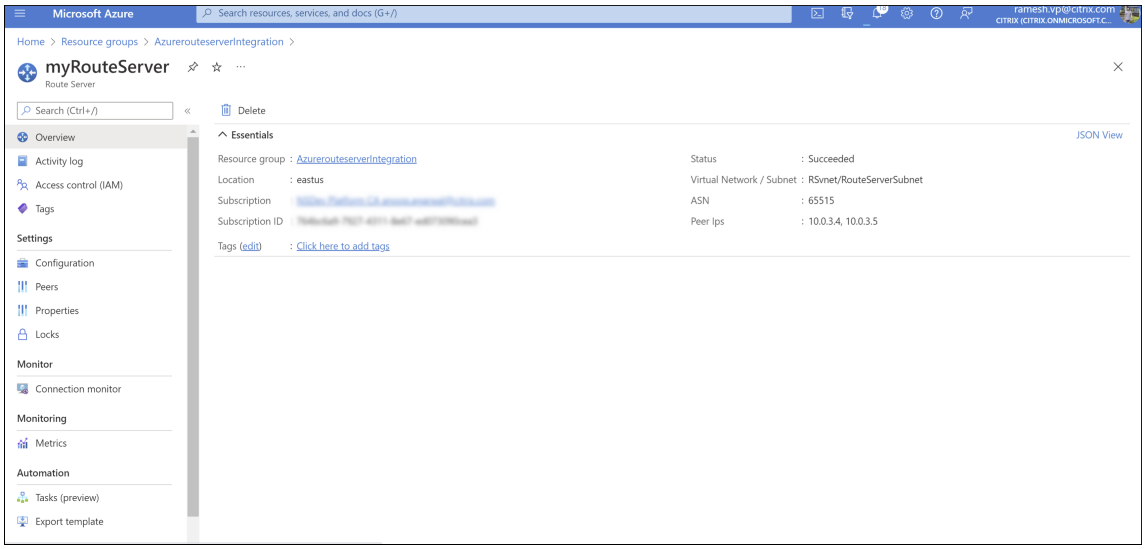
Sie müssen mit den folgenden Informationen vertraut sein, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen.

- Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Überblick über Azure Route Server. Weitere Informationen finden Sie unter Was ist Azure Route Server?.
- Arbeiten einer NetScaler-Appliance. Weitere Informationen finden Sie in der NetScaler-Dokumentation.
- NetScaler-Netzwerk. Weitere Informationen finden Sie im ADC-Netzwerk.

So konfigurieren Sie einen Azure-Routenserver mit einem NetScaler VPX HA-Paar

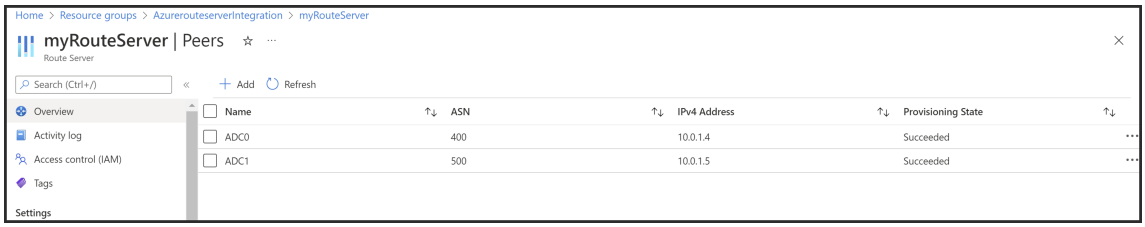
1. Erstellen Sie einen Routenserver im Azure-Portal. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines Routenservers mithilfe des Azure-Portals.

   Im folgenden Beispiel wird das Subnetz 10.0.3.0/24 für die Bereitstellung des Azure-Servers verwendet. Sobald der Routenserver erstellt wurde, rufen Sie die IP-Adressen des Routenservers ab, zum Beispiel: 10.0.3.4, 10.0.3.5.



2. Richten Sie Peering mit einer virtuellen Netzwerkanwendung (NVA) im Azure-Portal ein. Fügen Sie Ihre NetScaler VPX-Instanz als NVA hinzu. Weitere Informationen finden Sie unter Einrichten von Peering mit NVA.

   Im folgenden Beispiel werden das ADC-SNIP auf 1/1-Schnittstellen 10.0.1.4 und 10.0.1.5 und die ASN: 400 und 500 beim Hinzufügen des Peers verwendet.



3. Fügen Sie zwei NetScaler VPX-Instanzen für die HA-Konfiguration hinzu.

   Führen Sie hierzu die folgenden Schritte aus:

   a) Stellen Sie zwei VPX-Instanzen (primäre und sekundäre Instanzen) in Azure bereit.
   b) Fügen Sie auf beiden Instanzen eine Client- und Server-Netzwerkkarte hinzu.
   c) Konfigurieren Sie HA-Einstellungen auf beiden Instanzen mithilfe der NetScaler GUI.

4. Konfigurieren Sie das dynamische Routing in der primären ADC-Instanz.

   Beispielkonfiguration:

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -dynamicRouting
    ENABLED
VTYSH
configure terminal
router BGP 400
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
<!--NeedCopy-->
```

5. Konfigurieren Sie das dynamische Routing in der sekundären ADC-Instanz.

   Beispielkonfiguration:

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD
enable ns feature LB BGP
add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -dynamicRouting
    ENABLED
VTYSH
configure terminal
router BGP 500
timers bgp 1 3
neighbor 10.0.3.4 remote-as 65515
neighbor 10.0.3.4 advertisement-interval 3
neighbor 10.0.3.4 fall-over  bfd
neighbor 10.0.3.5 remote-as 65515
```



```
neighbor 10.0.3.5 advertisement-interval 3
neighbor 10.0.3.5 fall-over  bfd
address-family ipv4
redistribute kernel
redistribute static
<!--NeedCopy-->
```

6. Überprüfen Sie die BGP-Peers, die mithilfe der BGP-Befehle in der VTY-Shell-Schnittstelle eingerichtet wurden. Weitere Informationen finden Sie unter Überprüfen der BGP-Konfiguration.

```
show ip bgp neighbors
<!--NeedCopy-->
```

7. Konfigurieren Sie den virtuellen LB-Server in der primären ADC-Instanz.

   Beispielkonfiguration:

```
add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute ENABLED
add lbvserver v1 HTTP 172.16.1.1 80
add service s1 10.0.2.6 HTTP 80
bind lbvserver v1 s1
enable ns feature lb
<!--NeedCopy-->
```

   Ein Client im selben virtuellen Netzwerk wie die NetScaler VPX-Instanz kann jetzt auf den virtuellen LB-Server zugreifen. In diesem Fall kündigt die NetScaler VPX-Instanz die VIP-Route an den Azure-Routenserver an.

Fügen Sie Azure Autoscale-Einstellungen hinzu

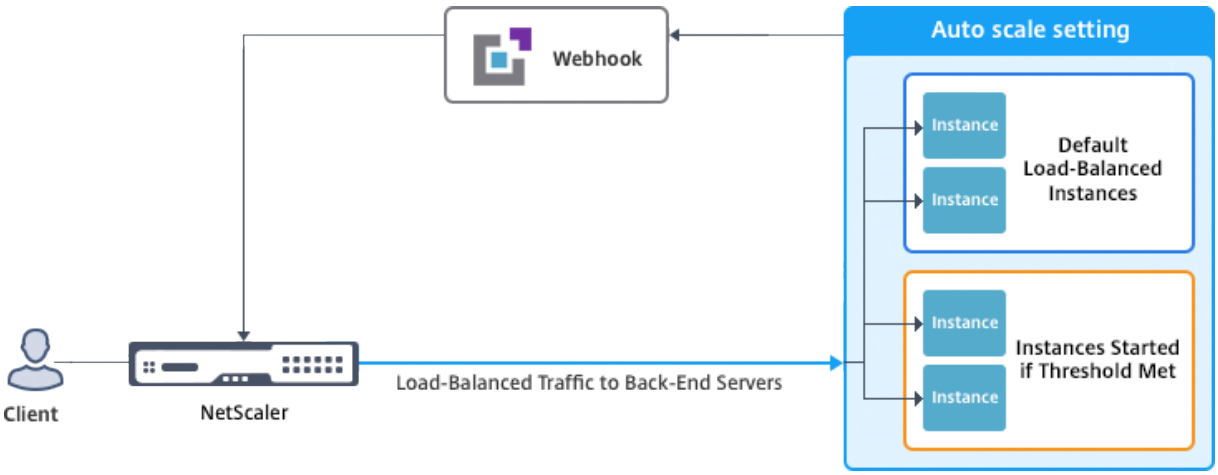
September 1, 2023

Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen je nach Anwendungsbedarf. Um der steigenden Nachfrage gerecht zu werden, müssen Sie die Netzwerkressourcen nach oben skalieren. Unabhängig davon, ob die Nachfrage nachlässt, müssen Sie herunterfahren, um die unnötigen Kosten ungenutzter Ressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, müssen Sie den Datenverkehr, die Speicher- und CPU-Auslastung usw. ständig überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Sie können Autoscale mit Azure VM Scale Sets (VMSS) für die eigenständige VPX Multi-IP-Bereitstellung und Hochverfügbarkeitsbereitstellung auf Azure verwenden.

Die NetScaler VPX-Instanz ist in die Azure VMSS- und Autoscale-Funktion integriert und bietet die folgenden Vorteile:

- Lastverteilung und Verwaltung: Server werden automatisch so konfiguriert, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die NetScaler VPX-Instanz erkennt automatisch die Einstellung VMSS Autoscale in demselben virtuellen Netzwerk, in dem die VPX-Instanz bereitgestellt wird, oder in den virtuellen Peered-Netzwerken, die sich im selben Azure-Abonnement befinden. Sie können die Einstellung VMSS Autoscale auswählen, um die Last auszugleichen. Dies geschieht durch die automatische Konfiguration der virtuellen NetScaler-IP-Adresse und Subnetz-IP-Adresse auf der VPX-Instanz.
- Hochverfügbarkeit: Erkennt Autoscale-Gruppen und gleicht Server aus.
- Bessere Netzwerkverfügbarkeit: Die VPX-Instanz unterstützt Back-End-Server in verschiedenen virtuellen Netzwerken (VNETs).



Weitere Informationen finden Sie im folgenden Azure-Thema

- Dokumentation zu Skalierungssätzen für virtuelle Maschinen
- Überblick über Autoscale in virtuellen Maschinen, Cloud-Diensten und Web-Apps von Microsoft Azure

Voraussetzungen

1. Lesen Sie die Azure-bezogenen Nutzungsrichtlinien. Weitere Informationen finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf Microsoft Azure.
2. Erstellen Sie je nach Anforderung eine oder mehrere NetScaler VPX -Instanzen mit drei Netzwerkschnittstellen in Azure (eigenständige oder hochverfügbare Bereitstellung).
3. Öffnen Sie den TCP 9001-Port in der Netzwerksicherheitsgruppe der 0/1-Schnittstelle

der VPX-Instanz. Die VPX-Instanz verwendet diesen Port, um die Scale-Out- und Scale-In-Benachrichtigung zu empfangen.

4. Erstellen Sie eine Azure-VMSS im selben virtuellen Netzwerk, in dem die NetScaler VPX-Instanz bereitgestellt wird. Wenn die VMSS- und NetScaler VPX-Instanz in verschiedenen virtuellen Azure-Netzwerken bereitgestellt werden, müssen die folgenden Bedingungen erfüllt sein:

   - Beide virtuellen Netzwerke müssen im selben Azure-Abonnement enthalten sein.
   - Die beiden virtuellen Netzwerke müssen mithilfe der Peering-Funktion für virtuelle Netzwerke von Azure verbunden werden.

   Wenn Sie keine vorhandene VMSS-Konfiguration haben, führen Sie die folgenden Aufgaben aus:

   a) Erstellen eines VMSS

   b) Autoscale auf VMSS aktivieren

   c) Erstellen Sie eine Scale-In- und Scale-Out-Richtlinie in der VMSS-Autoscale-Einstellung

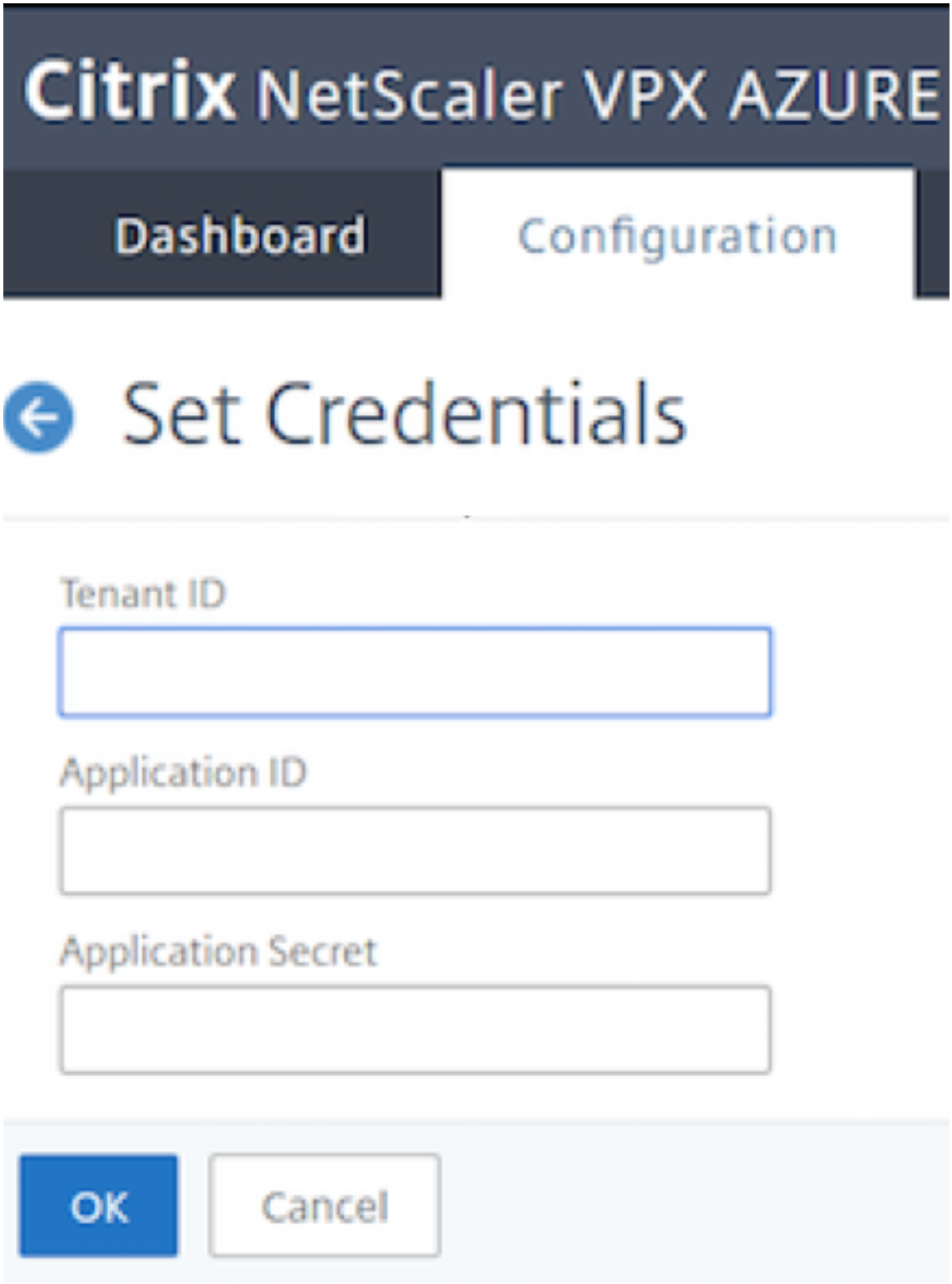
   Weitere Informationen finden Sie unter Überblick über Autoscale with Azure Skalierungssätze für virtuelle Maschinen.

5. Erstellen Sie eine Azure Active Directory (ADD) -Anwendung und Dienstprinzipal, die auf Ressourcen zugreifen können. Weisen Sie der neu erstellten AAD-Anwendung die Rolle der Mitwirkenden zu. Weitere Informationen finden Sie unter Verwenden des Portals zum Erstellen einer Azure Active Directory-Anwendung und eines Dienstprinzipals, die auf Ressourcen zugreifen können.

Hinzufügen von VMSS zu einer NetScaler VPX-Instanz

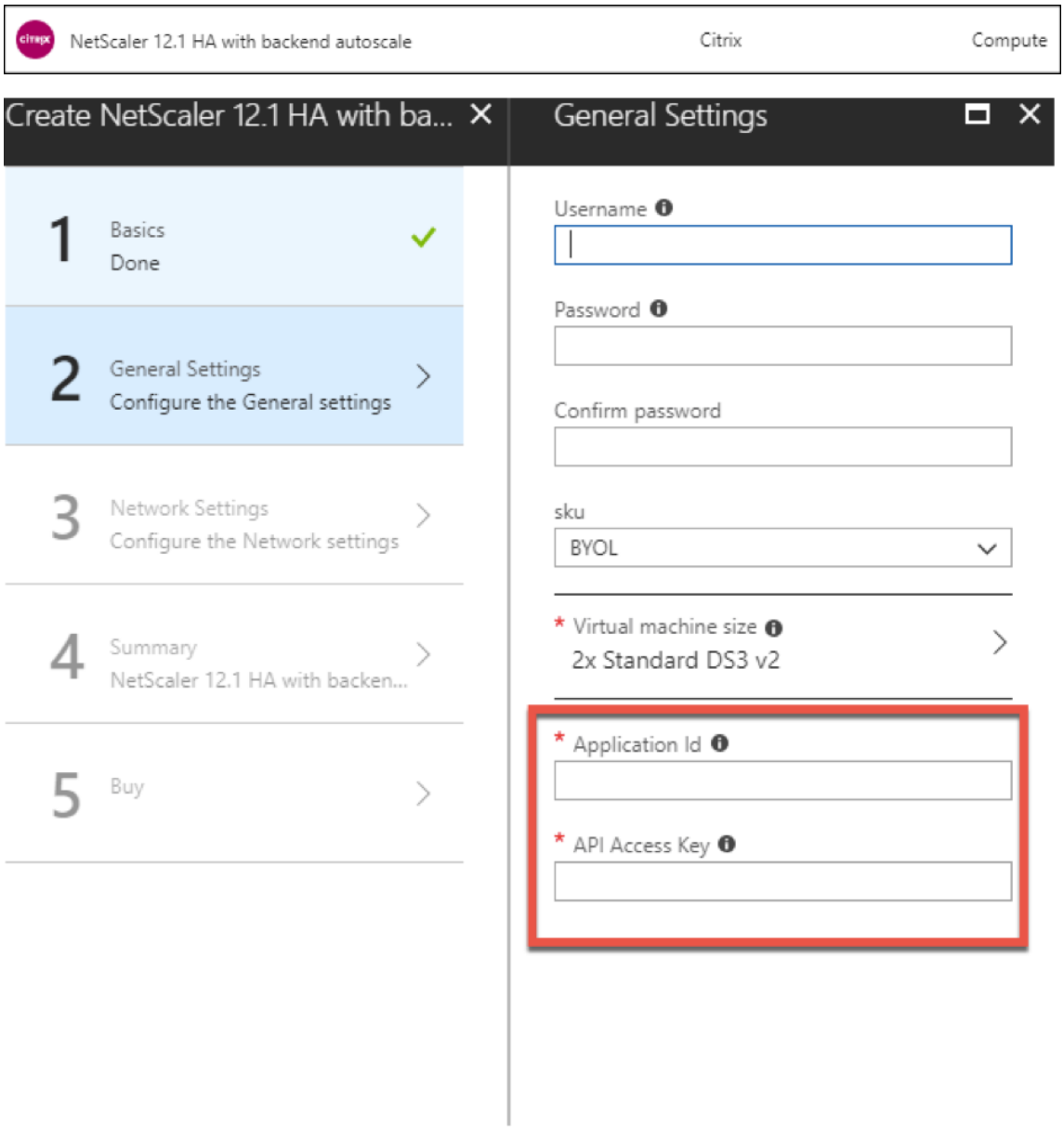
Sie können die Autoscale-Einstellung mit einem einzigen Klick zu einer VPX-Instanz hinzufügen, indem Sie die GUI verwenden. Führen Sie diese Schritte aus, um der VPX-Instanz die Autoscale-Einstellung hinzuzufügen:

1. Melden Sie sich bei der VPX-Instanz an.
2. Wenn Sie sich zum ersten Mal bei der NetScaler VPX-Instanz anmelden, wird die Seite Anmeldeinformationen festlegen angezeigt. Fügen Sie die erforderlichen Azure-Anmeldeinformationen hinzu, damit die Autoscale-Funktion funktioniert.



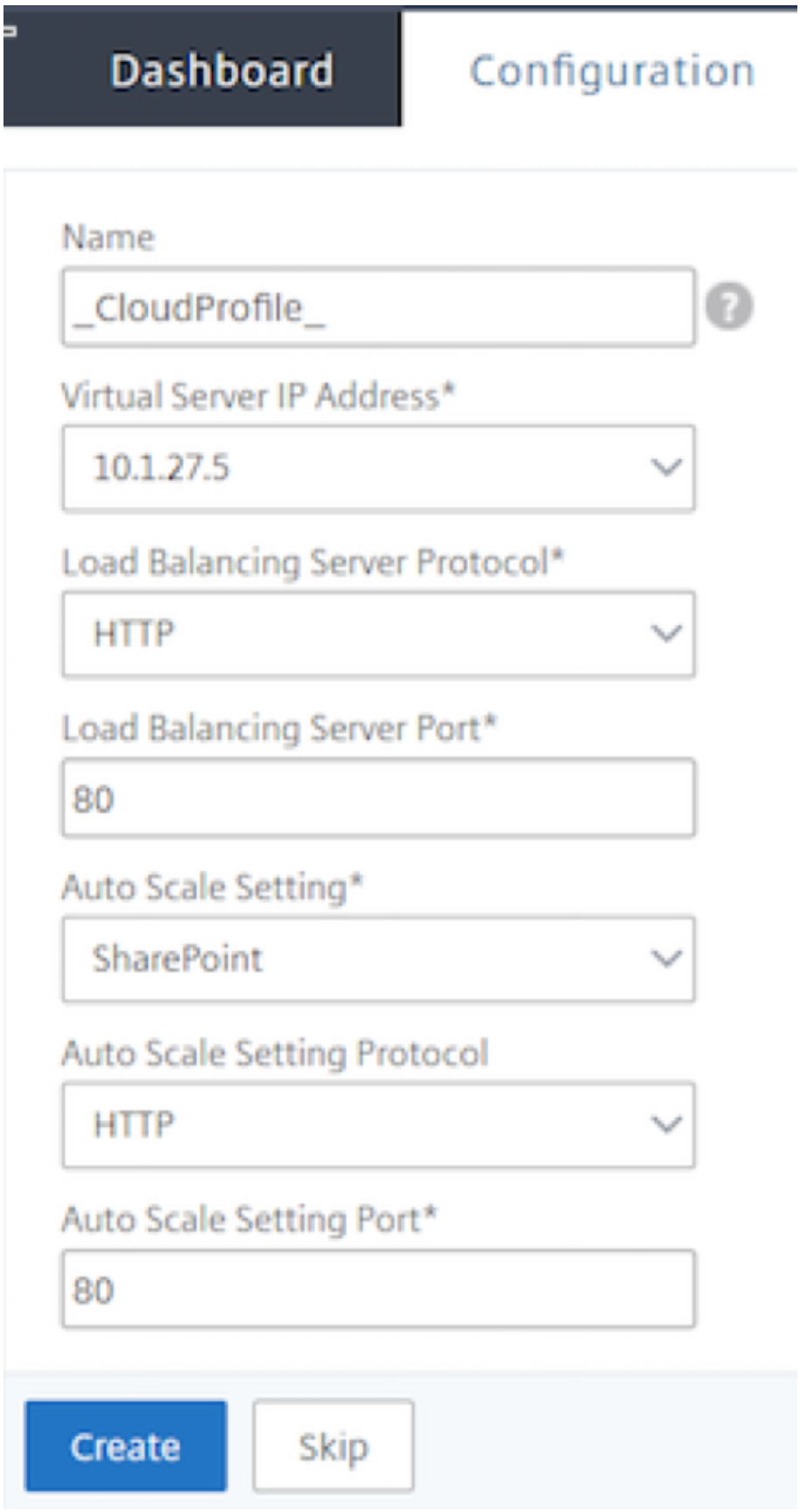
Die Seite “Anmeldeinformationen festlegen” wird nur angezeigt, wenn die Anwendungs-ID und der API-Zugriffsschlüssel nicht festgelegt sind oder die richtigen Anwendungs-ID und API-Zugriffsschlüssel (wie Application Secret) im Azure-Portal nicht festgelegt sind.

Wenn Sie das Angebot “NetScaler 12.1 HA mit Back-End-Autoscale” vom Azure Marketplace bereitstellen, fordert das Azure-Portal zur Eingabe der Hauptanmeldeinformationen des Azure-Dienstes (Anwendungs-ID und API-Zugriffsschlüssel) auf.



Informationen zum Erstellen einer Anwendungs-ID finden Sie unter Anwendung hinzufügen und Erstellen eines Zugriffsschlüssels oder eines Anwendungsgeheimnisses finden Sie unter Konfigurieren einer Clientanwendung für den Zugriff auf Web-APIs.

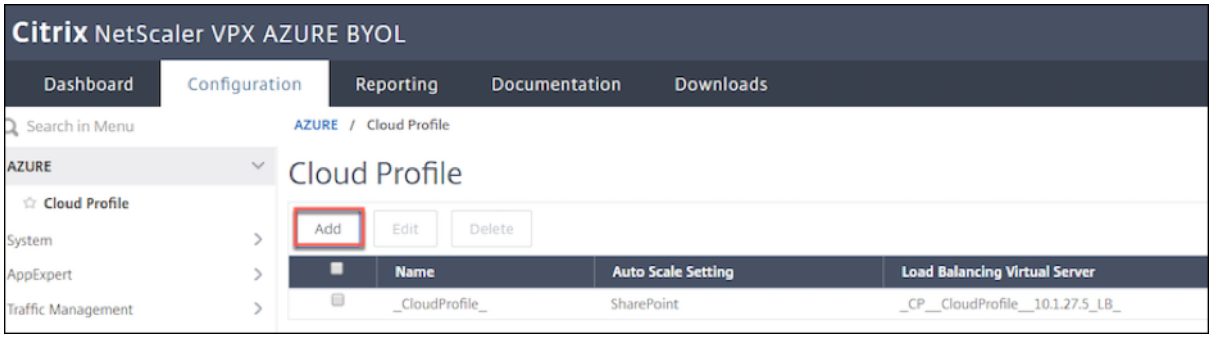
3. Geben Sie auf der Standard-Cloud-Profilseite die Details ein, wie im folgenden Beispiel gezeigt, und klicken Sie auf Erstellen.



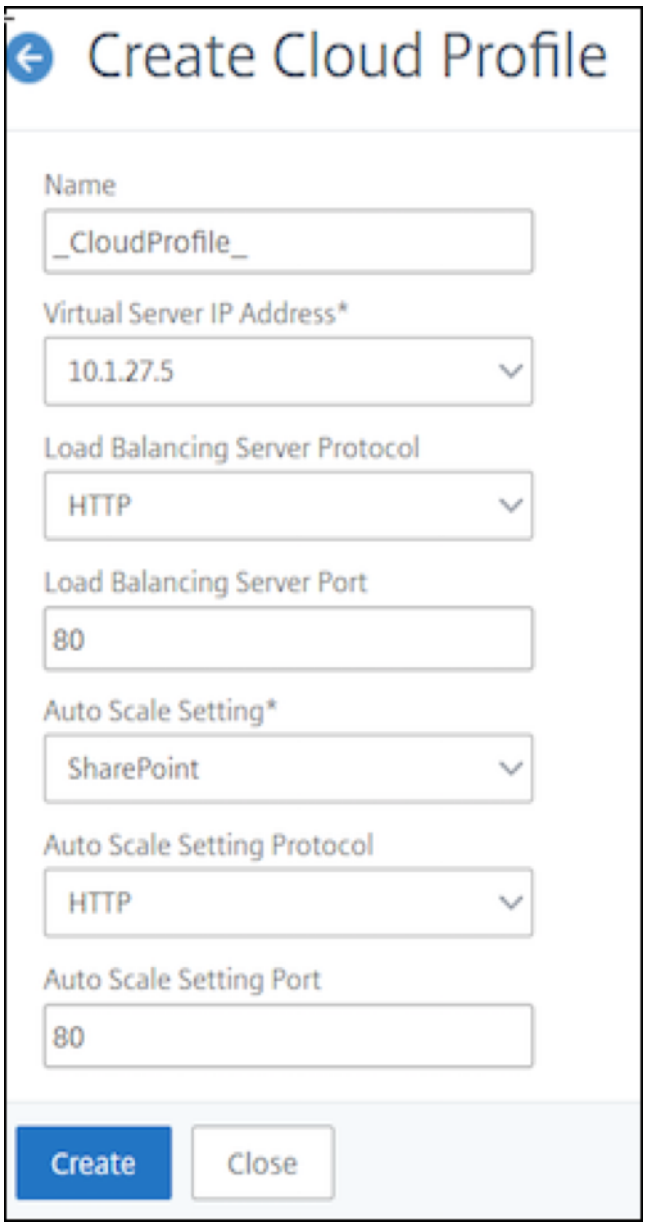
Punkte, die beim Erstellen eines Cloud-Profils berücksichtigt werden müssen

- Die IP-Adresse des virtuellen Servers wird automatisch von der freien IP-Adresse ausgefüllt, die für die VPX-Instanz verfügbar ist. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
- Die Autoscale-Einstellung wird von der VMSS-Instanz vorausgefüllt, die mit der NetScaler VPX-Instanz entweder im selben virtuellen Netzwerk oder in virtuellen Peering-Netzwerken verbunden ist. Weitere Informationen finden Sie unter Überblick über Autoscale with Azure Skalierungssätze für virtuelle Maschinen.
- Stellen Sie bei der Auswahl des Auto Scaling Group-Protokolls und des Port sicher, dass Ihre Server die Protokolle und Ports überwachen und Sie den richtigen Monitor in der Servicegruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
- Bei Autos Scaling vom Typ SSL Protocol ist der virtuelle Load Balancing-Server oder die Dienstgruppe nach dem Erstellen des Cloud-Profils aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

Wenn Sie nach der ersten Anmeldung ein Cloud-Profil erstellen möchten, gehen Sie auf der GUI zu **System > Azure > Cloud-Profil** und klicken Sie auf **Hinzufügen**.



Die Konfigurationsseite „ Cloud-Profil erstellen “ wird angezeigt.



Cloud Profile erstellt einen virtuellen NetScaler Load Balancing-Server und eine Dienstgruppe mit Mitgliedern (Servern) als Server der Auto Scaling Group. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

> **Hinweis:**
>
> Ab NetScaler Version 13.1-42.x können Sie verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung verschiedener Ports) mit demselben VMSS in Azure erstellen. Somit unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.

Um Informationen zu Autoscale im Azure-Portal anzuzeigen, gehen Sie zu **Alle Dienste > Maßstab für virtuelle Maschinen > Scale Set für virtuelle Maschinen auswählen > Skalierung**.

Referenzen

Informationen zur automatischen Skalierung von NetScaler VPX in Microsoft Azure mithilfe von NetScaler Application Delivery and Management finden Sie unter Azure Autoscale mit NetScaler ADM.

Azure-Tags für NetScaler VPX Bereitstellung

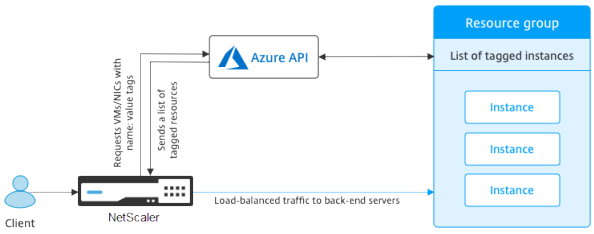
May 11, 2023

Im Azure-Cloud-Portal können Sie Ressourcen mit einem Namen: Wertepaar (wie Abt: Finance) kennzeichnen, um Ressourcen zwischen Ressourcengruppen und innerhalb des Portals über Abonnements hinweg zu kategorisieren und anzuzeigen. Tagging ist hilfreich, wenn Sie Ressourcen für die Abrechnung, Verwaltung oder Automatisierung organisieren müssen.

So funktioniert das Azure-Tag für die VPX-Bereitstellung

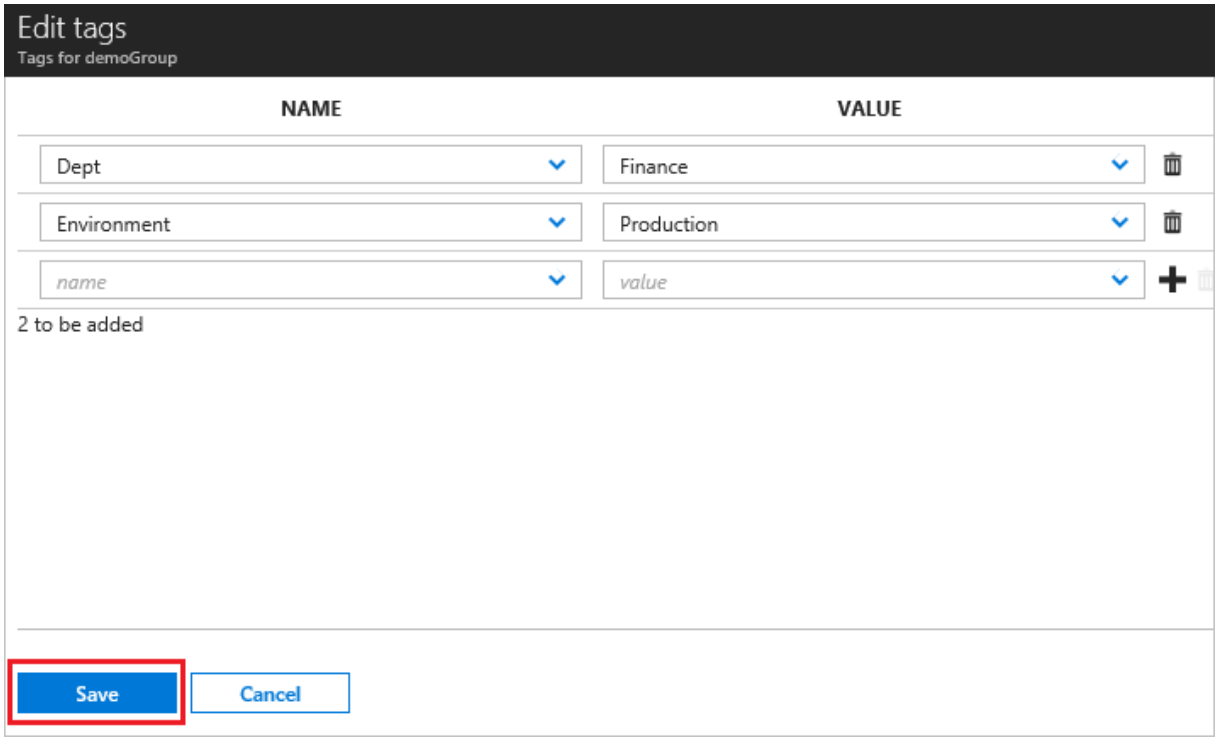
Für eigenständige NetScaler VPX-Instanzen und Hochverfügbarkeitsinstanzen, die in Azure Cloud bereitgestellt werden, können Sie jetzt Lastausgleichsdienstgruppen erstellen, die einem Azure-Tag zugeordnet sind. Die VPX-Instanz überwacht ständig virtuelle Azure-Computer (Back-End-Server) und Netzwerkschnittstellen (NICs) oder beides mit dem entsprechenden Tag und aktualisiert die Servicegruppe entsprechend.

Die VPX-Instanz erstellt die Dienstgruppe, die die Back-End-Server mit Tags ausgleicht. Die Instanz fragt die Azure-API nach allen Ressourcen ab, die mit einem bestimmten Tagnamen und Tag-Wert gekennzeichnet sind. Abhängig vom zugewiesenen Abfragezeitraum (standardmäßig 60 Sekunden) fragt die VPX-Instanz regelmäßig die Azure-API ab und ruft die verfügbaren Ressourcen mit dem in der VPX-GUI zugewiesenen Tag-Namen und den Tag-Werten ab. Immer wenn eine VM oder NIC mit dem entsprechenden Tag hinzugefügt oder gelöscht wird, erkennt der ADC die entsprechende Änderung und fügt die VM- oder NIC-IP-Adresse automatisch zur Dienstgruppe hinzu oder löscht sie aus der Dienstgruppe.



Voraussetzungen

Bevor Sie NetScaler Load Balancing-Dienstgruppen erstellen, fügen Sie den Servern in Azure ein Tag hinzu. Sie können das Tag entweder der virtuellen Maschine oder der Netzwerkkarte zuweisen.



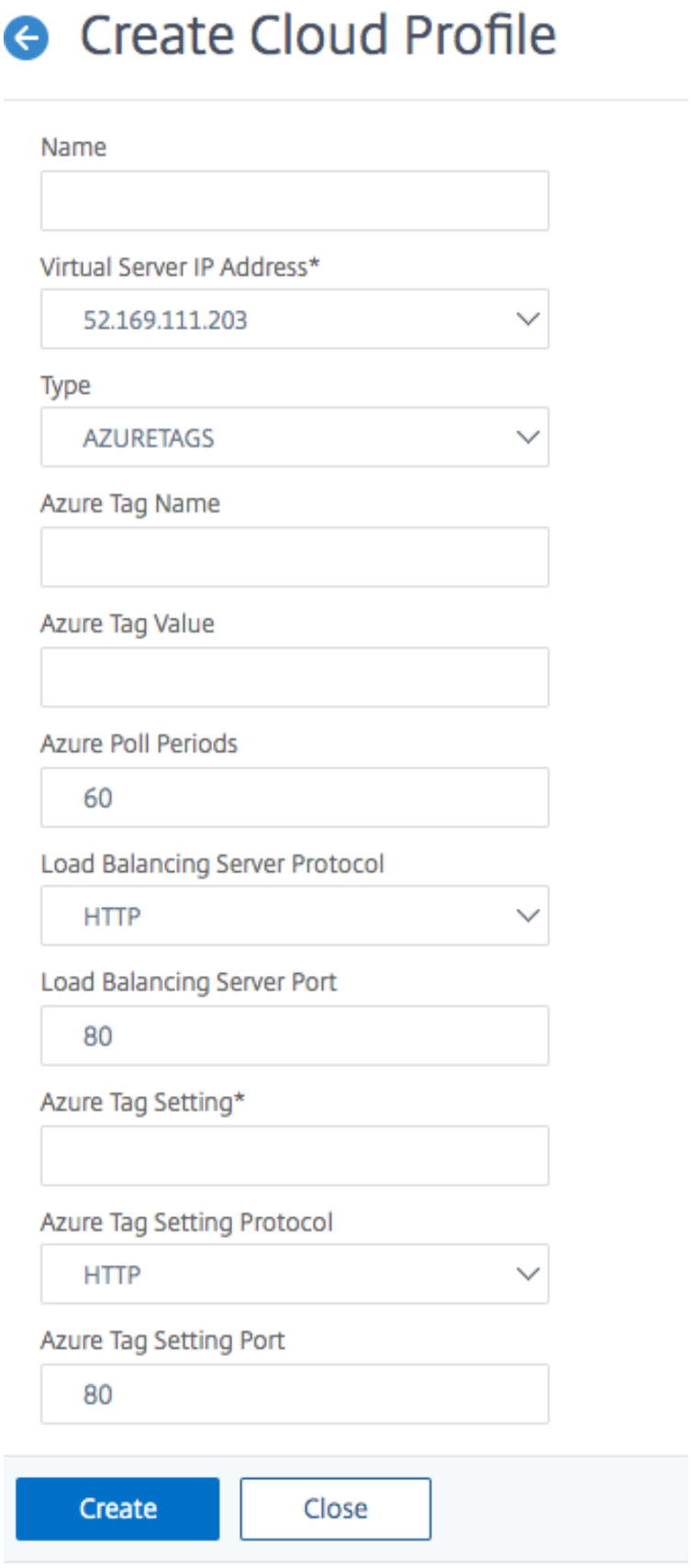
Weitere Informationen zum Hinzufügen von Azure-Tags finden Sie unter Microsoft-Dokument Verwenden Sie Tags zum Organisieren Ihrer Azure-Ressourcen.

> Hinweis
> ADC-CLI-Befehle zum Hinzufügen von Azure-Tag-Einstellungen unterstützen Tagnamen und Tag-Werte, die nur mit Ziffern oder Alphabeten und nicht mit anderen Tastaturzeichen beginnen.

So fügen Sie Azure-Tag-Einstellungen mithilfe der VPX-GUI hinzu

Sie können das Azure-Tag-Cloud-Profil zu einer VPX-Instanz hinzufügen, indem Sie die VPX-GUI verwenden, sodass die Instanz die Back-End-Server mithilfe des angegebenen Tags ausgleichen kann. Führen Sie die folgenden Schritte aus:

1. Gehen Sie in der VPX-GUI zu **Konfiguration > Azure > Cloud-Profil**.
2. Klicken Sie auf Hinzufügen, um ein Cloud-Profil zu erstellen. Das Cloud-Profilfenster wird geöffnet.



1. Geben Sie Werte für die folgenden Felder ein:
   - Name: Füge einen Namen für dein Profil hinzu
   - IP-Adresse des virtuellen Servers: Die IP-Adresse des virtuellen Servers wird automatisch von der freien IP-Adresse ausgefüllt, die für die VPX-Instanz verfügbar ist. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
   - Typ: Wählen Sie im Menü AZURETAGS.
   - Azure-Tag-Name: Geben Sie den Namen ein, den Sie den VMs oder NICs im Azure-Portal zugewiesen haben.
   - Azure-Tag-Wert: Geben Sie den Wert ein, den Sie den VMs oder Netzwerkkarten im Azure-Portal zugewiesen haben.
   - Azure-Abfragezeiträume: Standardmäßig beträgt der Abfragezeitraum 60 Sekunden, was dem Mindestwert entspricht. Sie können es entsprechend Ihren Anforderungen ändern.
   - Load Balancing Server Protocol: Wählen Sie das Protokoll aus, das Ihr Load Balancer überwacht.
   - Load Balancing-Server-Port: Wählen Sie den Port aus, auf dem Ihr Load Balancer lauscht.
   - Azure-Tag-Einstellung: Der Name der Dienstgruppe, die für dieses Cloud-Profil erstellt wird.
   - Azure Tag Setting Protocol: Wählen Sie das Protokoll aus, das Ihre Backend-Server abhören.
   - Azure Tag Setting Port: Wählen Sie den Port aus, den Ihre Back-End-Server abhören.
2. Klicken Sie auf **Erstellen**.

Ein virtueller Load-Balancer-Server und eine Dienstgruppe werden für die markierten VMs oder NICs erstellt. Um den virtuellen Load Balancer-Server zu sehen, navigieren Sie in der VPX-GUI zu **Traffic Management > Load Balancing > Virtual**Servers.

So fügen Sie Azure-Tag-Einstellungen mithilfe der VPX CLI hinzu

Geben Sie den folgenden Befehl in der NetScaler CLI ein, um ein Cloud-Profil für Azure-Tags zu erstellen.

```
1 add cloud profile `<profile name>` -type azuretags -vServerName `<
    vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>` -
    port 80 -serviceGroupName `<service group name>` -
    boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
    Azure tag specified on Azure portal>` -azureTagValue `<Azure value
    specified on the Azure portal>` -azurePollPeriod 60
2
3 <!--NeedCopy-->
```


> Wichtig
> Sie müssen alle Konfigurationen speichern. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanz neu gestartet haben. Geben Sie `save config` ein.

Beispiel 1: Hier ist ein Beispielbefehl für ein Cloud-Profil für den HTTP-Verkehr aller Azure-VMs/NICs, die mit dem Paar „myTagName/myTagValue“ gekennzeichnet sind:

```
add cloud profile MyTagCloudProfile -type azuretags -vServerName
    MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
    serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP -
    vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue myTagValue
     -azurePollPeriod 60
Done
<!--NeedCopy-->
```

Um das Cloud-Profil anzuzeigen, geben Sie ein `show cloudprofile`.

Beispiel 2: Der folgende CLI-Befehl druckt Informationen über das neu hinzugefügte Cloud-Profil in Beispiel 1.

```
show cloudprofile
1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
    MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133
    Port:  80               ServiceGroupName:  MyTagsServiceGroup
    BoundServiceGroupSvcType:  HTTP
       Vsvrbindsvcport:  80     AzureTagName:  myTagName AzureTagValue:
           myTagValue AzurePollPeriod:  60     GraceFul:  NO
          Delay:  60
<!--NeedCopy-->
```

Um ein Cloud-Profil zu entfernen, geben Sie rm Cloud-Profil ein `<cloud profile name>`

Beispiel 3: Mit dem folgenden Befehl wird das in Beispiel 1 erstellte Cloud-Profil entfernt.

```
> rm cloudprofile MyTagCloudProfile
  Done
<!--NeedCopy-->
```

Problembehandlung

Problem: In sehr seltenen Fällen kann der CLI-Befehl “rm cloud profile” die Dienstgruppe und Server, die mit dem gelöschten Cloud-Profil verknüpft sind, möglicherweise nicht entfernen. Dies geschieht, wenn der Befehl Sekunden vor Ablauf des Abfragezeitraums des gelöschten Cloud-Profils ausgegeben wird.

Lösung: Löschen Sie die verbleibenden Dienstgruppen manuell, indem Sie den folgenden CLI-Befehl für jede der verbleibenden Dienstgruppen eingeben:

```
#> rm servicegroup <serviceGroupName>

<!--NeedCopy-->
```

Entfernen Sie auch jeden der verbleibenden Server, indem Sie den folgenden CLI-Befehl für jeden der verbleibenden Server eingeben:

```
#> rm server <name>
<!--NeedCopy-->
```

Problem: Wenn Sie einer VPX-Instanz über die Befehlszeilenschnittstelle eine Azure-Tag-Einstellung hinzufügen, wird der rain_tags-Prozess nach einem Warmneustart weiterhin auf einem HA-Paar-Node ausgeführt.

Lösung: Beenden Sie den Prozess auf dem sekundären Knoten nach einem warmen Neustart manuell. Von der CLI des sekundären HA-Knotens beenden Sie die Shell-Eingabeaufforderung

```
#> shell

<!--NeedCopy-->
```

Verwenden Sie den folgenden Befehl, um den rain_tags-Prozess zu beenden:

```
# PID=`ps -aux | grep rain_tags | awk '{
 print $2 }
 '`; kill -9 $PID

<!--NeedCopy-->
```

Problem: Back-End-Server sind möglicherweise nicht erreichbar und werden von der VPX-Instanz als DOWN gemeldet, obwohl sie gesund sind.
Lösung: Stellen Sie sicher, dass die VPX-Instanz die getaggte IP-Adresse erreichen kann, die dem Back-End-Server entspricht. Bei einer getaggten NIC handelt es sich hierbei um die NIC-IP-Adresse. Bei einer getaggten VM handelt es sich dabei um die primäre IP-Adresse der VM. Wenn sich die VM/NIC in einem anderen Azure VNet befindet, stellen Sie sicher, dass VNet-Peering aktiviert ist.

Konfigurieren von GSLB auf NetScaler VPX-Instanzen

May 11, 2023

NetScaler Appliances, die für den Global Server Load Balancing (GSLB) konfiguriert sind, bieten Disaster Recovery und kontinuierliche Verfügbarkeit von Anwendungen, indem sie vor Fehlerpunkten in einem WAN schützen. GSLB kann die Last über Rechenzentren hinweg ausgleichen, indem sie Kundenanfragen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder an überlebende Rechenzentren bei einem Ausfall weiterleitet.

In diesem Abschnitt wird beschrieben, wie Sie GSLB auf VPX-Instanzen auf zwei Standorten in einer Microsoft Azure-Umgebung mithilfe von Windows PowerShell Befehlen aktivieren.

> **Hinweis**
>
> Weitere Informationen zu GSLB finden Sie unter Globaler Server-Lastenausgleich.

Sie können GSLB für eine NetScaler VPX-Instanz in Azure in zwei Schritten konfigurieren:

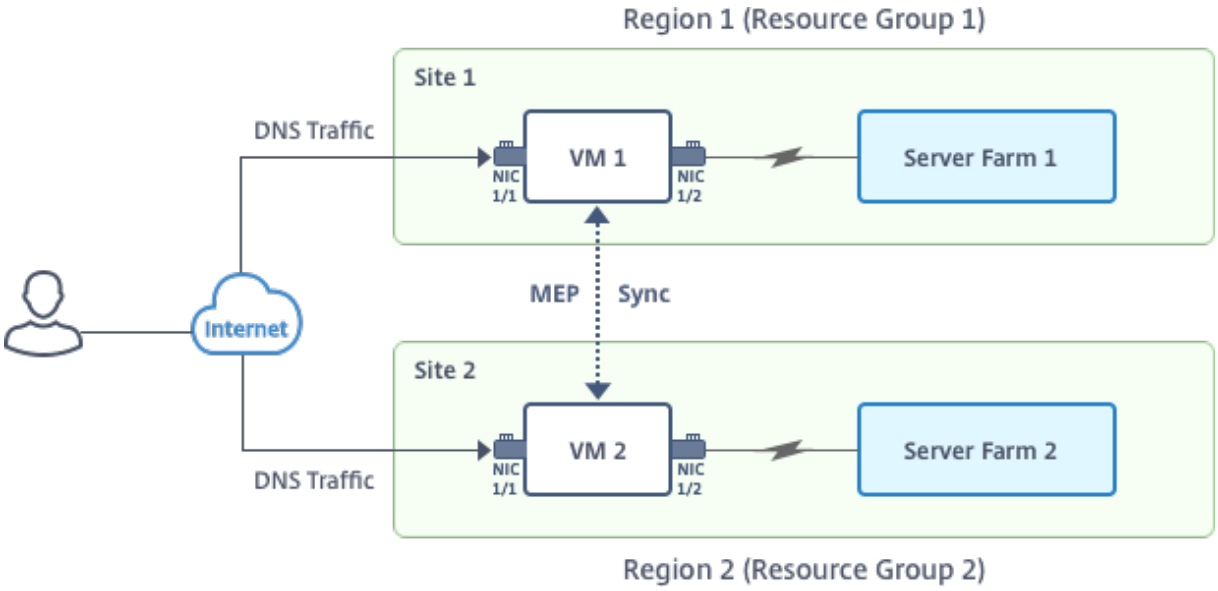
1. Erstellen Sie auf jeder Site eine VPX-Instanz mit mehreren Netzwerkkarten und mehreren IP-Adressen.
2. Aktivieren Sie GSLB für die VPX-Instanzen.

> **Hinweis**
>
> Weitere Informationen zum Konfigurieren mehrerer Netzwerkkarten und IP-Adressen finden Sie unter: Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen

Szenario

Dieses Szenario umfasst zwei Standorte — Standort 1 und Standort 2. Jeder Standort verfügt über eine VM (VM1 und VM2), die mit mehreren NICs, mehreren IP-Adressen und GSLB konfiguriert ist.

Abbildung. GSLB-Setup implementiert an zwei Standorten - Standort 1 und Standort 2.



In diesem Szenario hat jede VM drei Netzwerkkarten - NIC 0/1, 1/1 und 1/2. Jede NIC kann mehrere private und öffentliche IP-Adressen haben. Die Netzwerkkarten sind für die folgenden Zwecke konfiguriert.

- NIC 0/1: zur Bedienung des Management-Datenverkehrs
- NIC 1/1: zur Bedienung des clientseitigen Datenverkehrs
- NIC 1/2: Kommunikation mit Back-End-Servern

Informationen zu den IP-Adressen, die in diesem Szenario auf jeder Netzwerkkarte konfiguriert sind, finden Sie im Abschnitt Details zur IP-Konfiguration .

Parameter

Im Folgenden finden Sie Beispielparametereinstellungen für dieses Szenario in diesem Dokument. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard_DS3_V2"

<!--NeedCopy-->
```

Hinweis: Die Mindestanforderung für eine VPX-Instanz ist 2 vCPUs und 2 GB RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"
```



```
14
15 $numberOfVMs=1
16
17 $ipAddressPrefix="10.0.0."
18
19 $ipAddressPrefix1="10.0.1."
20
21 $ipAddressPrefix2="10.0.2."
22
23 $pubIPName1="MultiIP-pip1"
24
25 $pubIPName2="MultiIP-pip2"
26
27 $IpConfigName1="IPConfig1"
28
29 $IPConfigName2="IPConfig-2"
30
31 $IPConfigName3="IPConfig-3"
32
33 $IPConfigName4="IPConfig-4"
34
35 $frontendSubnetName="default"
36
37 $backendSubnetName1="subnet_1"
38
39 $backendSubnetName2="subnet_2"
40
41 $suffixNumber=10
42 <!--NeedCopy-->
```

Erstellen einer virtuellen Maschine

Führen Sie die Schritte 1 bis 10 aus, um VM1 mit mehreren Netzwerkkarten und mehreren IP-Adressen zu erstellen, indem Sie PowerShell-Befehle verwenden:

1. Ressourcengruppe erstellen
2. Erstellen eines Speicherkontos
3. Verfügbarkeitssatz erstellen
4. Virtuelles Netzwerk erstellen
5. Öffentliche IP-Adresse erstellen
6. NICs erstellen

7. VM-Konfigurationsobjekt erstellen
8. Anmeldeinformationen abrufen und Betriebssystemeigenschaften für die VM festlegen
9. Netzwerkkarten hinzufügen
10. Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

Nachdem Sie alle Schritte und Befehle zum Erstellen von VM1 abgeschlossen haben, wiederholen Sie diese Schritte, um VM2 mit spezifischen Parametern zu erstellen.

Ressourcengruppe erstellen

```
New-AzureRMResourceGroup -Name $RGName -Location $location
<!--NeedCopy-->
```

Erstellen eines Speicherkontos

```
$prmStorageAccount=New-AzureRMStorageAccount -Name
    $prmStorageAccountName -ResourceGroupName $RGName -Type Standard_LRS
     -Location $location
<!--NeedCopy-->
```

Verfügbarkeitssatz erstellen

```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $RGName -Location $location
<!--NeedCopy-->
```

Virtuelles Netzwerk erstellen

1. Fügen Sie Subnetze hinzu.

   ```
   $subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
       $frontendSubnetName -AddressPrefix "10.0.0.0/24"
   $subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
       $backendSubnetName1 -AddressPrefix "10.0.1.0/24"
   $subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
       $backendSubnetName2 -AddressPrefix "10.0.2.0/24"
   <!--NeedCopy-->
   ```

2. Fügen Sie ein virtuelles Netzwerkobjekt hinzu.


```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
    $RGName -Location $location -AddressPrefix 10.0.0.0/16 -Subnet
    $subnet1, $subnet2, $subnet3
<!--NeedCopy-->
```

3. Rufen Sie Subnetze ab.

```
$frontendSubnet=$vnet.Subnets|?{
 $\_.Name -eq $frontendSubnetName }

$backendSubnet1=$vnet.Subnets|?{
 $\_.Name -eq $backendSubnetName1 }

$backendSubnet2=$vnet.Subnets|?{
 $_.Name -eq $backendSubnetName2 }

<!--NeedCopy-->
```

Öffentliche IP-Adresse erstellen

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
<!--NeedCopy-->
```

NICs erstellen

NIC 0/1 erstellen

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$ipAddressPrefix + $suffixNumber
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -PrivateIpAddress
     $ipAddress1 -Primary
$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig1
<!--NeedCopy-->
```

NIC 1/1 erstellen

```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"
```



```
$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)
$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -
    PrivateIpAddress $ipAddress2  -Primary
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3
nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig2, $IpConfig3
<!--NeedCopy-->
```

NIC 1/2 erstellen

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"
$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)
$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary
$nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig4
<!--NeedCopy-->
```

VM-Konfigurationsobjekt erstellen

```
$vmName=$vmNamePrefix
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
<!--NeedCopy-->
```

Anmeldeinformationen abrufen und Betriebssystemeigenschaften festlegen

```
$cred=Get-Credential -Message "Type the name and password for VPX login
    ."
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
<!--NeedCopy-->
```

Netzwerkkarten hinzufügen


```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
<!--NeedCopy-->
```

Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

```
$osDiskName=$vmName + "-" + $osDiskSuffix
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
     +$osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
    Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
<!--NeedCopy-->
```

> **Hinweis**
>
> Wiederholen Sie die Schritte 1 bis 10, die unter “Erstellen von VMs mit PowerShell-Befehlen erstellen” aufgeführt sind, um VM2 mit Parametern zu erstellen, die für VM2 spezifisch sind.

IP-Konfigurationsdetails

Die folgenden IP-Adressen werden verwendet.

Tabelle 1. In VM1 verwendete IP-Adressen

Netzwerkkarte	Private IP	Öffentliche IP (PIP)	Beschreibung
0/1	10.0.0.10	PIP1	Als NSIP (Management-IP) konfiguriert
1/1	10.0.1.10	PIP2	Als SNIP/GSLB Site IP konfiguriert
-	10.0.1.11	-	Als LB-Server-IP konfiguriert. Öffentliche IP ist nicht verpflichtend

Netzwerkkarte	Private IP	Öffentliche IP (PIP)	Beschreibung
1/2	10.0.2.10	-	Konfiguriert als SNIP für das Senden von Monitorprobes an Dienste; öffentliche IP ist nicht obligatorisch

Tabelle 2. In VM2 verwendete IP-Adressen

Netzwerkkarte	Interne IP	Öffentliche IP (PIP)	Beschreibung
0/1	20.0.0.10	PIP4	Als NSIP (Management-IP) konfiguriert
1/1	20.0.1.10	PIP5	Als SNIP/GSLB Site IP konfiguriert
-	20.0.1.11	-	Als LB-Server-IP konfiguriert. Öffentliche IP ist nicht verpflichtend
1/2	20.0.2.10	-	Konfiguriert als SNIP für das Senden von Monitorprobes an Dienste; öffentliche IP ist nicht obligatorisch

Hier finden Sie Beispielkonfigurationen für dieses Szenario, die die IP-Adressen und anfänglichen LB-Konfigurationen zeigen, die über die NetScaler VPX CLI für VM1 und VM2 erstellt wurden.

Hier ist eine Beispielkonfiguration auf VM1.

```
add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
Add nsip 10.0.2.10 255.255.255.0
add service svc1 10.0.1.10 ADNS 53
add lb vserver v1 HTTP 10.0.1.11 80
add service s1 10.0.2.120 http 80
Add service s2 10.0.2.121 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```


Hier ist eine Beispielkonfiguration auf VM2.

```
add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED
Add nsip 20.0.2.10 255.255.255.0
add service svc1 20.0.1.10 ADNS 53
add lb vserver v1 HTTP 20.0.1.11 80
Add service s1 20.0.2.90 http 80
Add service s2 20.0.2.91 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```

Konfigurieren von GSLB-Sites und anderen Einstellungen

Führen Sie die im folgenden Thema beschriebenen Aufgaben aus, um die beiden GSLB-Sites und andere erforderliche Einstellungen zu konfigurieren:

Globaler Serverlastausgleich

Weitere Informationen finden Sie in diesem Support-Artikel:https://support.citrix.com/article/CTX110348

Hier ist ein Beispiel für eine GSLB-Konfiguration auf VM1 und VM2.

```
enable ns feature LB GSLB
add gslb site site1 10.0.1.10 -publicIP PIP2
add gslb site site2 20.0.1.10 -publicIP PIP5
add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP PIP3
    -publicPort 80 -siteName site1
add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP PIP6
    -publicPort 80 -siteName site2
add gslb vserver gslb_http_vip1 HTTP
bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
<!--NeedCopy-->
```

Sie haben GSLB auf NetScaler VPX-Instanzen konfiguriert, die in Azure ausgeführt werden.

Notfallwiederherstellung

Katastrophe ist eine plötzliche Störung der Geschäftsfunktionen, die durch Naturkatastrophen oder durch Menschen verursachte Ereignisse verursacht werden. Katastrophen wirken sich auf den Betrieb des Rechenzentrums aus. Danach müssen die am Katastrophenort verlorenen Ressourcen und Daten vollständig neu aufgebaut und wiederhergestellt werden. Der Verlust von Daten oder Ausfallzeiten im Rechenzentrum ist entscheidend und reduziert die Business Continuity.

Eine der Herausforderungen, vor denen Kunden heute stehen, besteht darin, zu entscheiden, wo sie ihren DR-Standort platzieren möchten. Unternehmen suchen nach Konsistenz und Leistung, unabhängig von zugrunde liegenden Infrastruktur- oder Netzwerkfehlern.

Mögliche Gründe, warum sich viele Unternehmen für eine Migration in die Cloud entscheiden, sind:

- Ein Rechenzentrum vor Ort ist sehr teuer. Durch die Nutzung der Cloud können die Unternehmen Zeit und Ressourcen für die Erweiterung ihrer eigenen Systeme sparen.
- Viele der automatisierten Orchestrierungen ermöglichen eine schnellere Wiederherstellung
- Replizieren Sie Daten, indem Sie kontinuierlichen Datenschutz oder kontinuierliche Snapshots bereitstellen, um sich vor Ausfällen oder Angriffen zu schützen.
- Unterstützen Sie Anwendungsfälle, in denen Kunden viele verschiedene Arten von Compliance- und Sicherheitskontrollen benötigen, die bereits in den Public Clouds vorhanden sind. Diese machen es einfacher, die von ihnen benötigte Compliance zu erreichen, als ihre eigenen zu erstellen.

Ein für GSLB konfigurierter NetScaler leitet den Datenverkehr an das am wenigsten ausgelastete oder leistungsstärkste Rechenzentrum weiter. Diese Konfiguration, die als aktiv-aktives Setup bezeichnet wird, verbessert nicht nur die Leistung, sondern bietet auch eine sofortige Notfallwiederherstellung, indem Datenverkehr an andere Rechenzentren weitergeleitet wird, wenn ein Rechenzentrum, das Teil des Setups ist, ausfällt. NetScaler spart Kunden dadurch wertvolle Zeit und Geld.

Bereitstellung mehrerer Netzwerkkarten (drei Netzwerkkarten) für die Notfallwiederherstellung

Kunden würden möglicherweise eine Bereitstellung mit drei Netzwerkkarten bereitstellen, wenn sie in einer Produktionsumgebung eingesetzt werden, in der Sicherheit, Redundanz, Verfügbarkeit, Kapazität und Skalierbarkeit entscheidend sind. Bei dieser Bereitstellungsmethode sind Komplexität und einfache Verwaltung für die Benutzer kein kritisches Problem.

Multi-IP-Bereitstellung mit einer Netzwerkkarte für die Notfallwiederherstellung

Kunden stellen die Bereitstellung möglicherweise mithilfe einer einzigen Netzwerkkarte bereit, wenn sie die Bereitstellung in einer Umgebung außerhalb der Produktionsumgebung vornehmen, und zwar aus den folgenden Gründen:

- Sie richten die Umgebung für Tests ein, oder sie stellen eine neue Umgebung vor der Bereitstellung in der Produktion bereit.
- Schnelle und effiziente Bereitstellung direkt in der Cloud.
- Sie sind auf der Suche nach der Einfachheit einer einzelnen Subnetzkonfiguration.

Konfigurieren Sie GSLB in einem aktiven Standby-Hochverfügbarkeits-Setup

May 11, 2023

Sie können den globalen Serverlastenausgleich (GSLB) bei der HA-Bereitstellung im aktiven Standby in Azure in drei Schritten konfigurieren:

1. Erstellen Sie ein VPX HA-Paar auf jeder GSLB-Site. Weitere Informationen zum Erstellen eines HA-Paares finden Sie unter Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und NICs .
2. Konfigurieren Sie den Azure Load Balancer (ALB) mit der Front-End-IP-Adresse und -Regeln, um GSLB- und DNS-Datenverkehr zuzulassen.

   Dieser Schritt beinhaltet die folgenden Teilschritte. Das Szenario in diesem Abschnitt enthält die PowerShell-Befehle, die zum Ausführen dieser Teilschritte verwendet werden.

   a. Erstellen Sie ein Front-End-`IPconfig` für die GSLB-Site.

   b. Erstellen Sie einen Back-End-Adresspool mit der IP-Adresse der NIC 1/1 der Knoten in HA.

   c. Erstellen Sie Lastenausgleichsregeln für Folgendes:

   ```
   TCP/3009 - gslb communication
   TCP/3008 - gslb communication
   UDP/53 - DNS communication
   ```

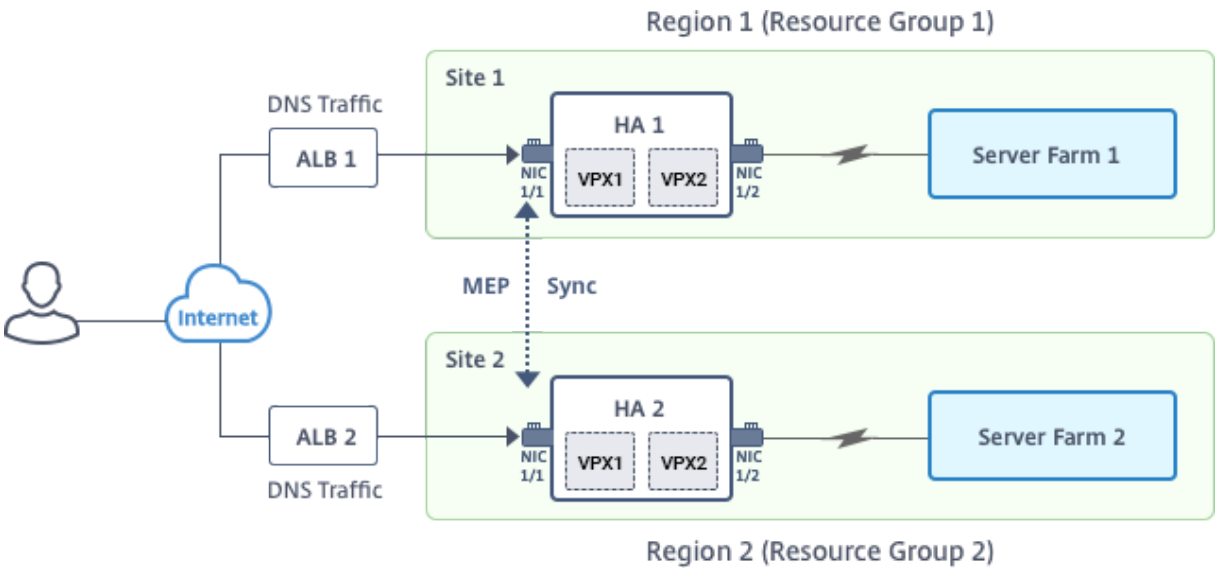
   d. Ordnen Sie den Back-End-Adresspool mit den in Schritt c erstellten LB-Regeln zu.

   e. Aktualisieren Sie die Netzwerksicherheitsgruppe von NIC 1/1 der Knoten in beiden HA-Paaren, um den Datenverkehr für TCP 3008-, TCP 3009- und UDP 53-Ports zuzulassen.
3. Aktivieren Sie GSLB auf jedem HA-Paar.

Szenario

Dieses Szenario umfasst zwei Standorte — Standort 1 und Standort 2. Jeder Standort verfügt über ein HA-Paar (HA1 und HA2), das mit mehreren Netzwerkkarten, mehreren IP-Adressen und GSLB konfiguriert ist.

Abbildung: GLSB auf Active-Standy HA-Bereitstellung in Azure



In diesem Szenario hat jede VM drei Netzwerkkarten - NIC 0/1, 1/1 und 1/2. Die Netzwerkkarten sind für die folgenden Zwecke konfiguriert.

NIC 0/1: zur Bedienung des Management-Datenverkehrs

NIC 1/1: zur Bedienung des clientseitigen Datenverkehrs

NIC 1/2: Kommunikation mit Back-End-Servern

Parameter-Einstellungen

Im Folgenden finden Sie Beispielparametereinstellungen für den ALB. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"

$domName4="vpxgslbdns"

$lbName="MultiIPALB"

$frontEndConfigName2="FrontEndIP2"

$backendPoolName1="BackendPoolHttp"

$lbRuleName2="LBRuleGSLB1"

```



```
$lbRuleName3="LBRuleGSLB2"

$lbRuleName4="LBRuleDNS"

$healthProbeName="HealthProbe"
```

Konfiguration von ALB mit der Front-End-IP-Adresse und Regeln, um GSLB- und DNS-Verkehr zuzulassen

Schritt 1. **Erstellen einer öffentlichen IP für GSLB-Site-IP**

```
$pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
    $rgName -DomainNameLabel $domName4 -Location $locName -
    AllocationMethod Dynamic


Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName | Add-
    AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName2 -
    PublicIpAddress $pip4 | Set-AzureRmLoadBalancer
```

Schritt 2. **Erstellen Sie LB-Regeln und aktualisieren Sie die vorhandene ALB**.

```
$alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName


$frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
    LoadBalancer $alb -Name $frontEndConfigName2


$backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
    LoadBalancer $alb -Name $backendPoolName1


$healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
    Name $healthProbeName


$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName2 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3009 -BackendPort
    3009 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer


```



```
$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName3 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3008 -BackendPort
    3008 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer


$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName4 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Udp" -FrontendPort 53 -BackendPort 53
    -Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer
```

Aktivieren von GSLB für jedes Hochverfügbarkeitspaar

Jetzt haben Sie zwei Front-End-IP-Adressen für jedes ALB: ALB 1 und ALB 2. Eine IP-Adresse ist für den virtuellen LB-Server und die andere für die GSLB-Site-IP.

HA 1 hat die folgenden Front-End-IP-Adressen:

- FrontEndIPofALB1 (für virtuellen LB-Server)
- PIPFORGSLB1 (GSLB IP)

HA 2 hat die folgenden Front-End-IP-Adressen:

- FrontEndIPofALB2 (für virtuellen LB-Server)
- PIPFORGSLB2 (GSLB IP)

Die folgenden Befehle werden für dieses Szenario verwendet.

```
enable ns feature LB GSLB

add service dnssvc PIPFORGSLB1 ADNS 53

add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1

add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2

add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
    publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1

add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
    publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
```



```
16
17 bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
18
19 bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Verwandte Ressourcen:

Konfigurieren von GSLB auf NetScaler VPX-Instanzen

Globaler Serverlastausgleich

NetScaler GSLB und Back-End-Autoscale für domänenbasierte Dienste mit Cloud Load Balancer bereitstellen

September 1, 2023

Angesichts der steigenden Nachfrage möchten Unternehmen, die ein lokales Rechenzentrum für regionale Kunden betreiben, mithilfe der Azure-Cloud weltweit skalieren und bereitstellen. Mit NetScaler auf der Seite des Netzwerkadministrators können Sie das GSLB StyleBook verwenden, um Anwendungen sowohl vor Ort als auch in der Cloud zu konfigurieren. Sie können dieselbe Konfiguration mit NetScaler ADM in die Cloud übertragen. Je nach Nähe zu GSLB können Sie entweder lokale oder Cloud-Ressourcen erreichen. Dies ermöglicht Ihnen ein nahtloses Erlebnis, egal wo Sie sich auf der Welt befinden.

DBS-Übersicht

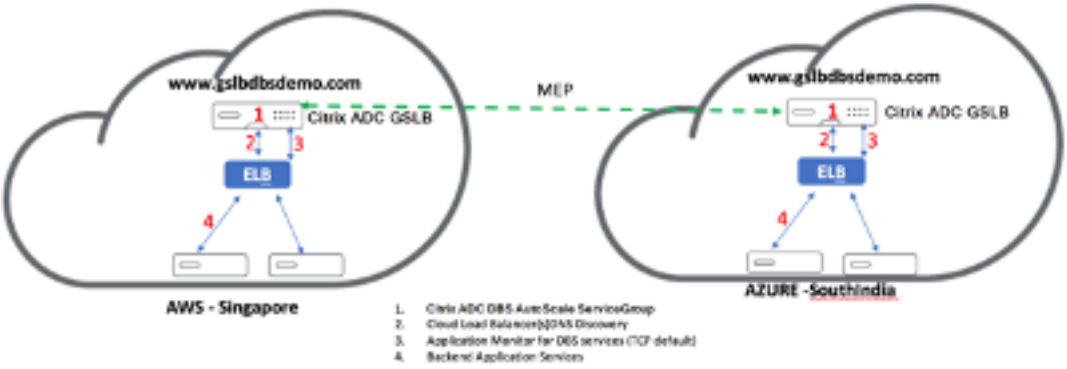
NetScaler GSLB unterstützt die Verwendung von Domain-Based Services (DBS) für Cloud-Load Balancer. Dies ermöglicht die automatische Erkennung dynamischer Cloud-Dienste mithilfe einer Cloud-Load-Balancer-Lösung. Diese Konfiguration ermöglicht es dem NetScaler, GSLB DBS in einer Active-Active-Umgebung zu implementieren. DBS ermöglicht die Skalierung von Back-End-Ressourcen in Microsoft Azure-Umgebungen ab der DNS-Erkennung. Dieser Abschnitt behandelt die Integration zwischen NetScalers in der Azure Autoscale-Umgebung.

Domänennamenbasierte Dienste mit Azure Load Balancer (ALB)

GLSB DBS verwendet den FQDN des ALB des Benutzers, um die GSLB-Dienstgruppen dynamisch zu aktualisieren, sodass sie die Backend-Server einschließen, die in Azure erstellt und gelöscht werden. Um diese Funktion zu konfigurieren, verweist der Benutzer den NetScaler ADC auf seinen ALB, um ihn dynamisch an verschiedene Server in Azure weiterzuleiten. Sie können dies tun, ohne den NetScaler ADC jedes Mal manuell aktualisieren zu müssen, wenn eine Instanz in Azure erstellt und gelöscht wird. Die

NetScaler ADC DBS-Funktion für GSLB-Dienstgruppen verwendet die DNS-fähige Diensterkennung, um die Mitgliedsdienstressourcen des DBS-Namespaces zu ermitteln, der in der Autoscale-Gruppe identifiziert wurde.

Das folgende Bild zeigt die Autoscale-Komponenten von NetScaler GSLB DBS mit Cloud-Loadbalancern:



Voraussetzungen für Azure GSLB

Zu den Voraussetzungen für die NetScaler GSLB-Servicegruppen gehört eine funktionierende Microsoft Azure-Umgebung mit dem Wissen und der Fähigkeit, Sicherheitsgruppen, Linux-Webserver, NetScaler-Appliances innerhalb von AWS, Elastic IPs und Elastic Load Balancers (ELB) zu konfigurieren.

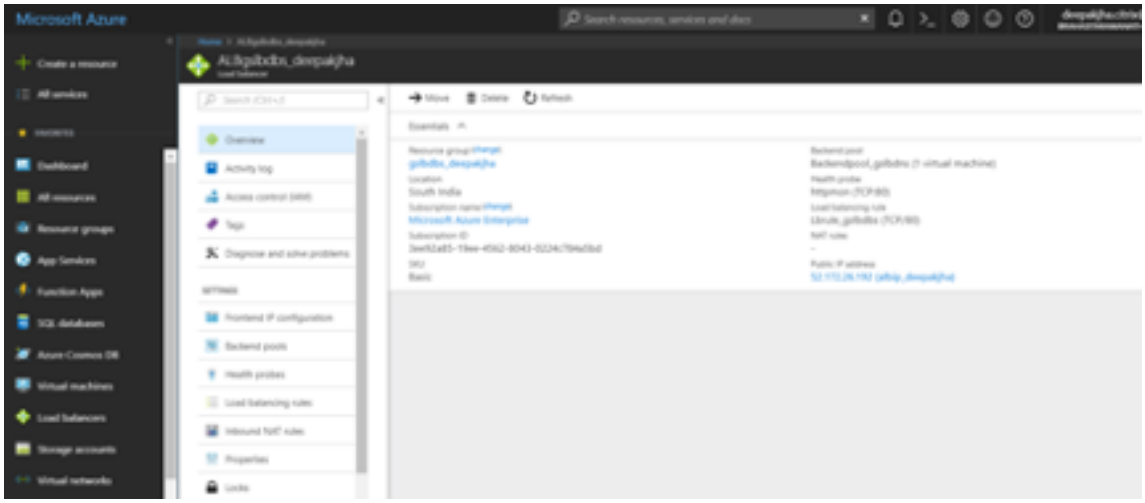
- Die GSLB DBS Service-Integration erfordert NetScaler Version 12.0.57 für Microsoft Azure-Loadbalancer-Instanzen.
- GSLB-Dienstgruppenentität: NetScaler Version 12.0.57.
- Die GSLB-Servicegruppe wird eingeführt, die die automatische Skalierung mithilfe von DBS Dynamic Discovery unterstützt.
- DBS-Feature-Komponenten (domänenbasierter Dienst) müssen an die GSLB-Dienstgruppe gebunden sein.

Beispiel:

```
1 ```
2  > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
     amazonaws.com
3  > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName sydney
4  > bind gslb serviceGroup sydney_sg sydney_server 80
5 <!--NeedCopy--> ```
```


Azure-Komponenten konfigurieren

1. Melden Sie sich beim Benutzer Azure Portal an und erstellen Sie eine neue virtuelle Maschine aus einer NetScaler-Vorlage.
2. Erstellen Sie einen Azure Load Balancer.

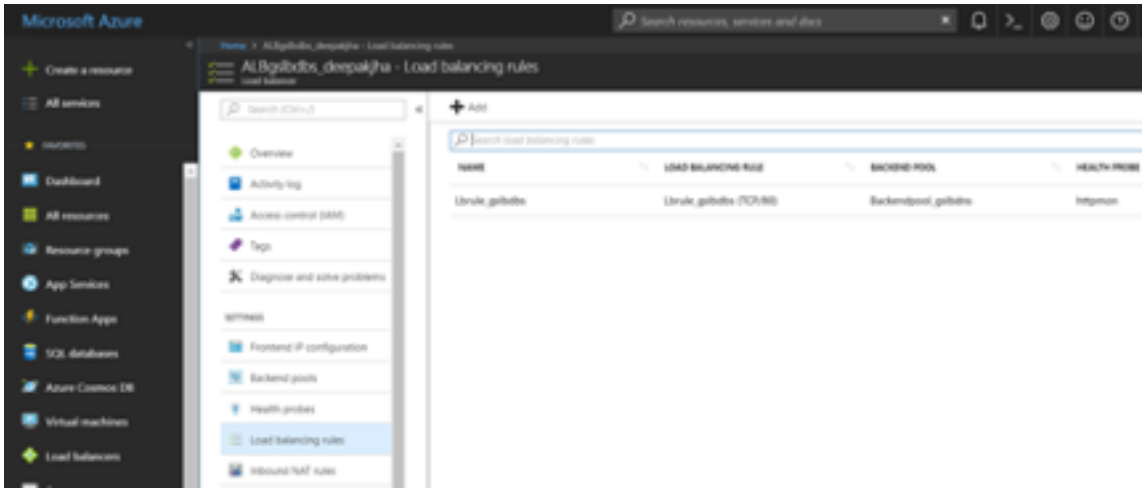


3. Fügen Sie die erstellten NetScaler-Back-End-Pools hinzu.

4. Erstellen Sie eine Integritätsprüfung für Port 80.

   Erstellen Sie eine Load-Balancing-Regel unter Verwendung der vom Load Balancer erstellten Front-End-IP.

   - Protokoll: TCP
   - Back-End-Port: 80
   - Back-End-Pool: NetScaler wurde in Schritt 1 erstellt
   - Health Probe: In Schritt 4 erstellt
   - Sitzungsbeständigkeit: Keine



Konfigurieren Sie den domänenbasierten Dienst NetScaler GSLB

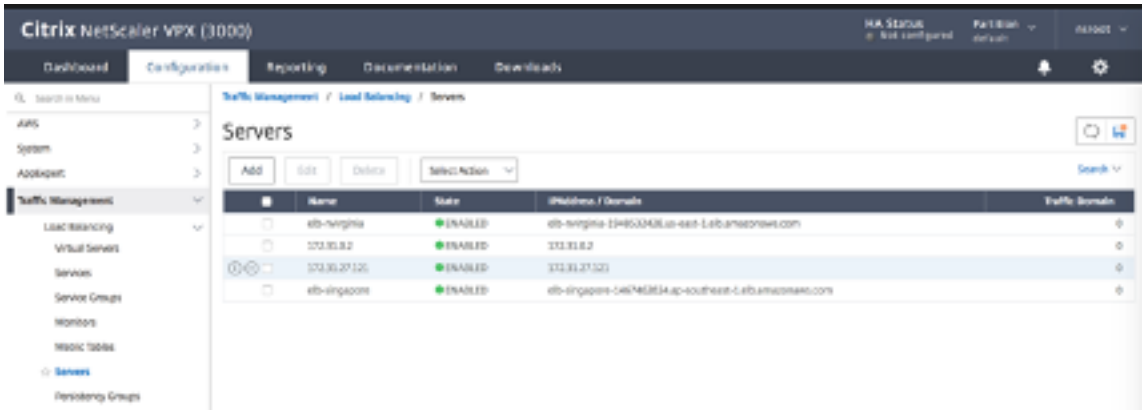
Die folgenden Konfigurationen fassen zusammen, was erforderlich ist, um domänenbasierte Dienste für die automatische Skalierung von ADCs in einer GSLB-fähigen Umgebung zu aktivieren.

- Konfigurationen für die Datenverkehrsverwaltung
- GSLB-Konfigurationen

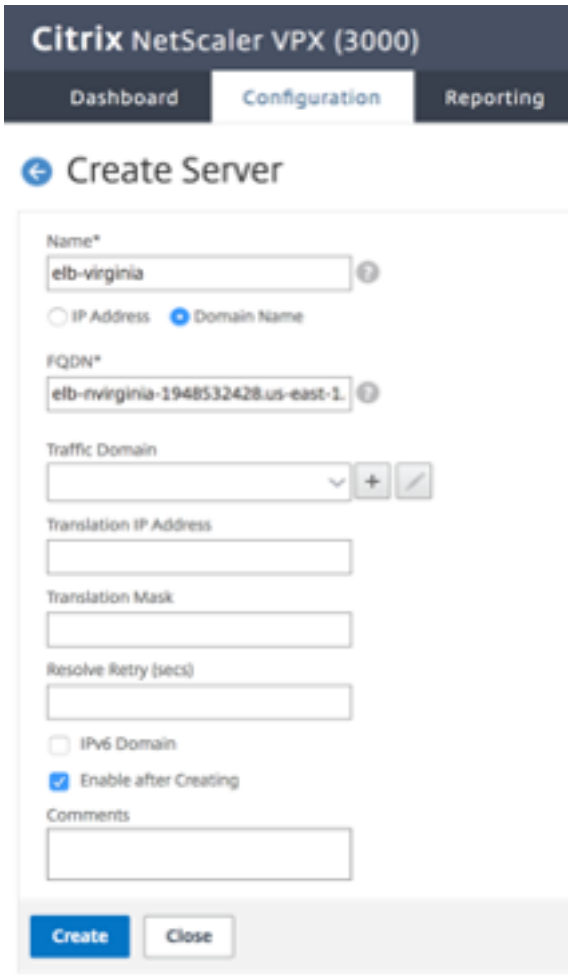
Konfigurationen für die Datenverkehrsverwaltung

> **Hinweis:**
>
> Es ist erforderlich, den NetScaler entweder mit einem Nameserver oder einem virtuellen DNS-Server zu konfigurieren, über den die ELB /ALB-Domänen für die DBS-Servicegruppen aufgelöst werden. Weitere Informationen zu Nameservern oder virtuellen DNS-Servern finden Sie unter: DNS-Nameserver

1. Navigieren Sie zu**Traffic Management > Load Balancing > Server**.



2. Klicken Sie auf**Hinzufügen**, um einen Server zu erstellen, und geben Sie einen Namen und einen FQDN an, die dem A-Eintrag (Domänenname) in Azure für die ALB entsprechen.



3. Wiederholen Sie Schritt 2, um die zweite ALB aus der zweiten Ressource in Azure hinzuzufügen.

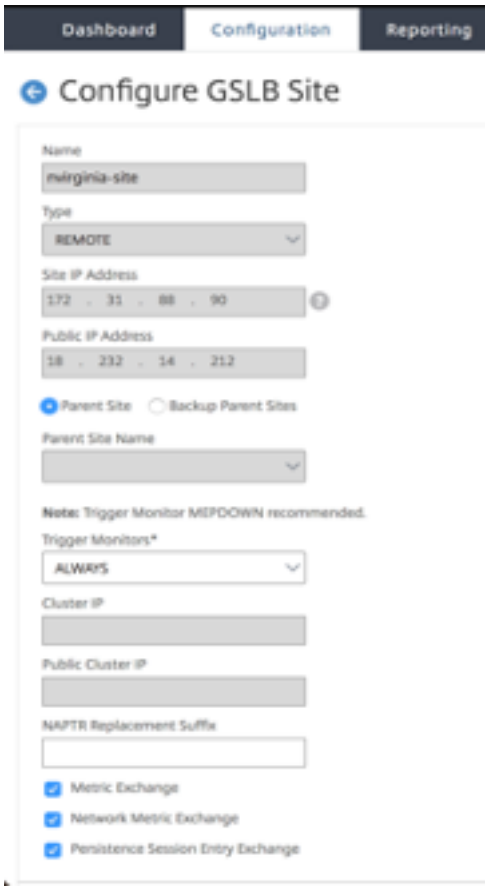
GSLB-Konfigurationen

1. Klicken Sie auf die Schaltfläche**Hinzufügen**, um eine GSLB-Site zu konfigurieren.
2. Geben Sie die Details für die Konfiguration der GSLB-Site an

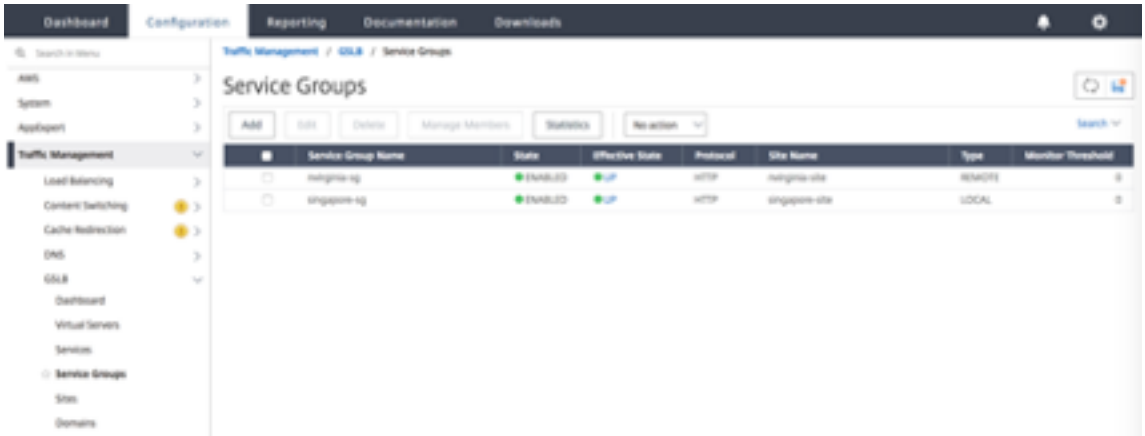
   Benennen Sie die Site. Der Typ wird als remote oder lokal konfiguriert, je nachdem, auf welchem NetScaler Sie die Site konfigurieren. Die Site-IP-Adresse ist die IP-Adresse für die GSLB-Site. Die GSLB-Site verwendet diese IP-Adresse, um mit den anderen GSLB-Sites zu kommunizieren. Die öffentliche IP-Adresse ist erforderlich, wenn Sie einen Cloud-Dienst verwenden, bei dem eine bestimmte IP-Adresse auf einer externen Firewall oder einem NAT-Gerät gehostet wird. Die Site sollte als übergeordneter Standort konfiguriert werden. Stellen Sie sicher, dass die **Trigger-Monitore** auf **ALWAYS**eingestellt sind. Stellen Sie außerdem

sicher, dass Sie die drei Kästchen unten für **Metric Exchange**, **Network Metric Exchange**und **Persistence Session Entry Exchange**aktivieren.

Wir empfehlen Ihnen, den **Trigger-Monitor** auf **MEPDOWN**einzustellen. Weitere Informationen findenSie unter Konfiguration einer GSLB-Dienstgruppe.



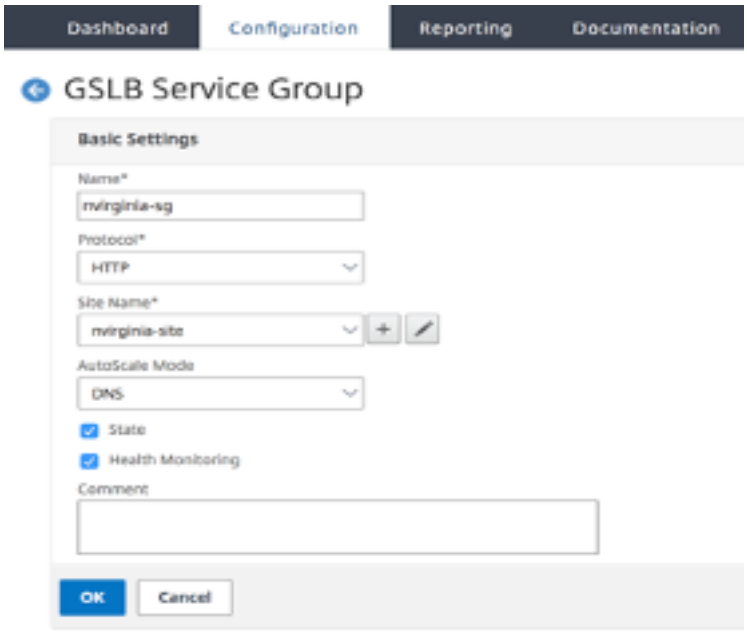
3. Klicken Sie auf **Erstellen**.
4. Navigieren Sie zu **Traffic Management > GSLB > Dienstgruppen**.



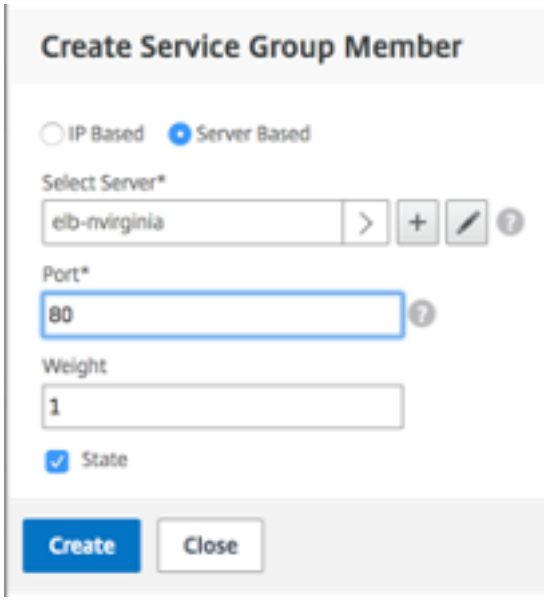
5. Klicken Sie auf **Hinzufügen**, um eine Dienstgruppe hinzuzufügen.

6. Geben Sie die Details zur Konfiguration der Dienstgruppe an

   Benennen Sie die Dienstgruppe und verwenden Sie das HTTP-Protokoll. Wählen Sie unter **Site-Name** die entsprechende Site aus, die Sie erstellt haben. Stellen Sie sicher, dass Sie den automatischen Skalierungsmodus als DNS konfigurieren und die Kontrollkästchen für die Status- und Integritätsüberwachung aktivieren. Klicken Sie auf**OK**, um die Dienstgruppe zu erstellen.



7. Klicken Sie auf**Service Group Members**und wählen Sie**Serverbasiert**aus. Wählen Sie den jeweiligen ELB aus, der zu Beginn der Run-Anleitung konfiguriert wurde. Konfigurieren Sie den Datenverkehr so, dass er über Port 80 geht. Klicken Sie auf **Erstellen**.

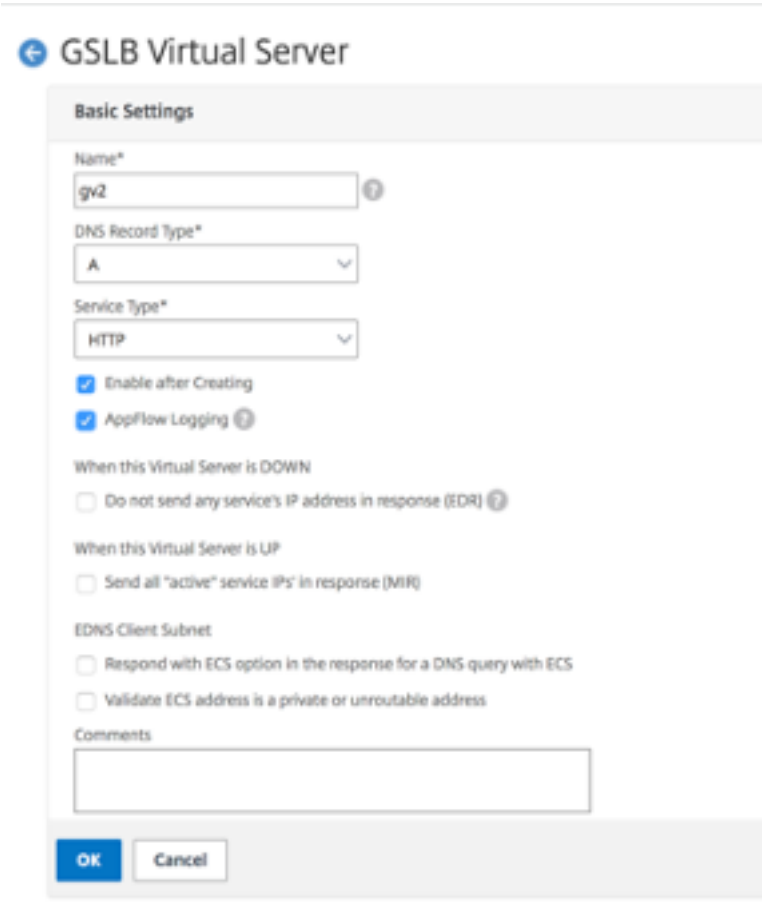


   Die Dienstgruppenmitgliederbindung sollte mit 2 Instanzen aufgefüllt werden, die sie vom ELB

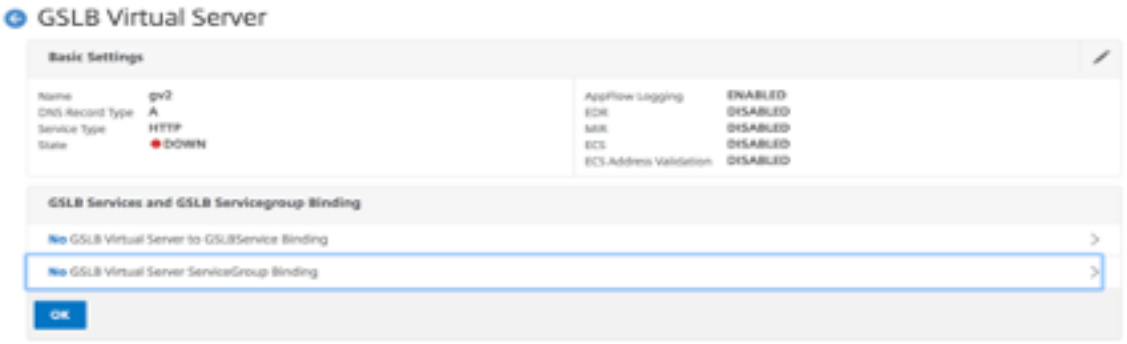
empfängt.

8. Wiederholen Sie die Schritte 5 und 6, um die Dienstgruppe für den zweiten Ressourcenstandort in Azure zu konfigurieren. (Dies kann über dieselbe NetScaler GUI erfolgen).
9. Um einen virtuellen GSLB-Server einzurichten. Navigieren Sie zu **Traffic Management > GSLB > Virtuelle Server**.
10. Klicken Sie auf**Hinzufügen**, um den virtuellen Server zu erstellen.
11. Geben Sie die Details zur Konfiguration des virtuellen GSLB-Servers an.

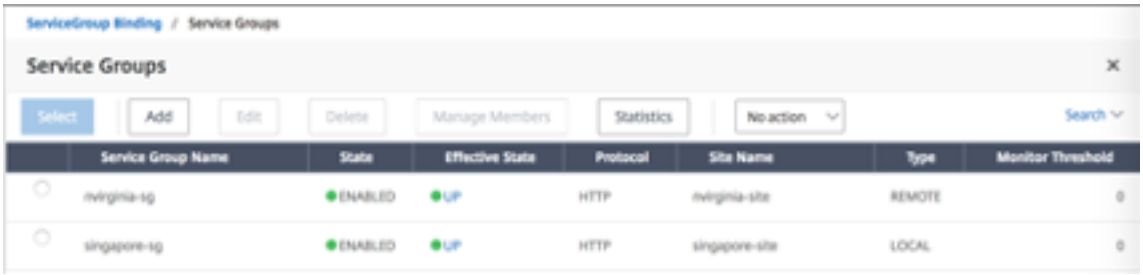
    Nennen Sie den Server, DNS-Datensatztyp ist als A, Diensttyp als HTTP festgelegt, und aktivieren Sie die Kontrollkästchen Nach dem Erstellen aktivieren und AppFlow-Protokollierung. Klicken Sie auf**OK**, um den virtuellen GSLB Server zu erstellen.



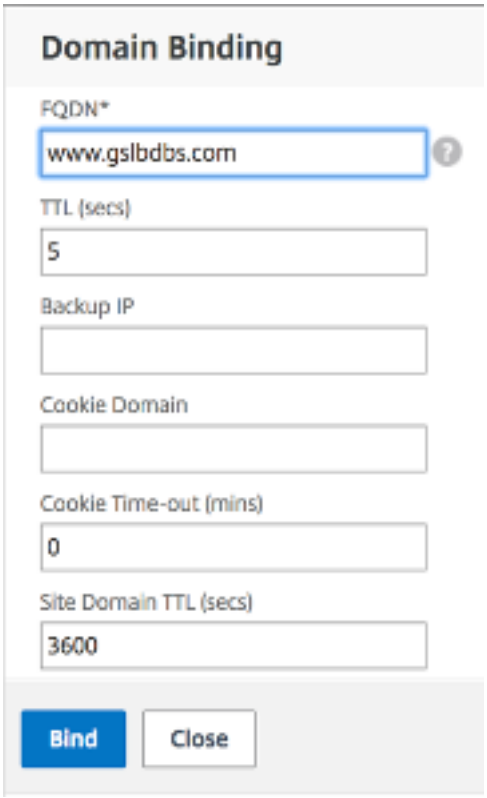
12. Sobald der virtuelle GSLB-Server erstellt wurde, klicken Sie auf**No GSLB Virtual Server ServiceGroup Binding**.



13. Verwenden**Sie unter**ServiceGroup Binding**die Option Select Service Group Name** , um die Dienstgruppen auszuwählen und hinzuzufügen, die in den vorherigen Schritten erstellt wurden.

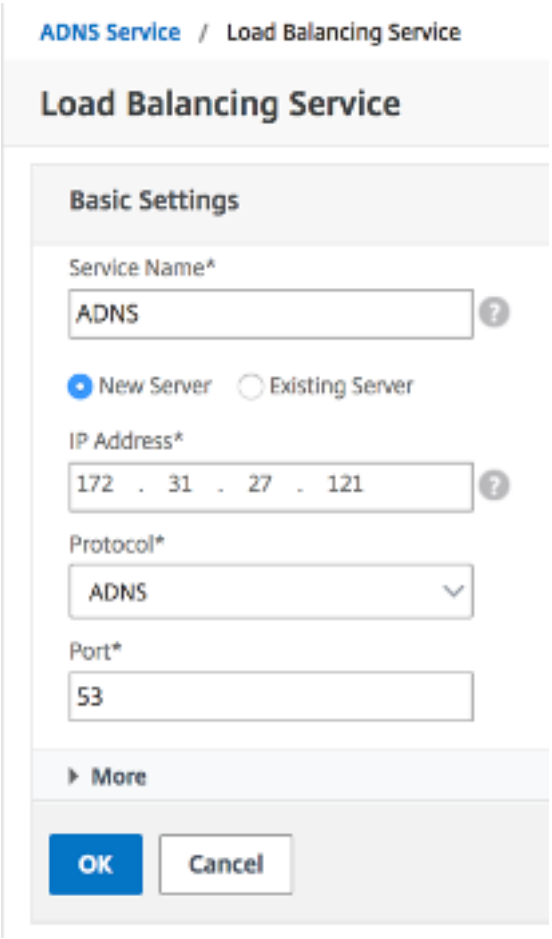


14. Konfigurieren Sie die Domänenbindung für virtuelle GSLB-Server, indem Sie auf**Keine GSLB-Domainbindung für virtuelle Server**klicken. Konfigurieren Sie den FQDN und binden Sie ihn. Behalten Sie die Standardeinstellung für andere Parameter bei.



15. Konfigurieren Sie den ADNS-Dienst, indem Sie auf**Kein Dienst**klicken.
16. Geben Sie die Details an, um den Load Balancing-Dienst zu konfigurieren.

    Fügen Sie einen **Dienstnamen**hinzu, klicken Sie auf**Neuer Server**und geben Sie die **IP-Adresse** des ADNS-Servers ein. Wenn der Benutzer ADNS bereits konfiguriert ist, können Benutzer**Existing Server**und dann den Benutzer ADNS aus dem Drop-down-Menü auswählen. Stellen Sie sicher, dass das Protokoll ADNS ist und der Datenverkehr so konfiguriert ist, dass er über Port 53 fließt.



17. Konfigurieren Sie die **Methode** als **Least Connection** und die Backup-Methode als **Round Robin**.
18. Klicken Sie auf**Fertig**und stellen Sie sicher, dass der virtuelle GSLB-Server des Benutzers als Up angezeigt wird.

Andere Ressourcen

Globaler NetScaler Lastenausgleich für Hybrid- und Multi-Cloud-Bereitstellungen

Konfigurieren der Intranet-IP für Adresspools für eine NetScaler Gateway-App

May 11, 2023

In einigen Situationen benötigen Benutzer, die eine Verbindung mit dem NetScaler Gateway -Plug-In herstellen, eine eindeutige IP-Adresse für eine NetScaler Gateway-Appliance. Wenn Sie Adresspools (auch als IP-Pooling bezeichnet) für eine Gruppe aktivieren, kann die NetScaler Gateway-Appliance jedem Benutzer einen eindeutigen IP-Adressalias zuweisen. Sie konfigurieren Adresspools mithilfe von Intranet-IP (IIP) -Adressen.

Sie können Adresspools auf einer in Azure bereitgestellten NetScaler Gateway -Appliance konfigurieren, indem Sie diese zweistufige Vorgehensweise ausführen:

- Registrieren der privaten IP-Adressen, die im Adresspool verwendet werden, in Azure
- Konfigurieren von Adresspools in der NetScaler Gateway Appliance

Registrieren Sie eine private IP-Adresse im Azure-Portal

In Azure können Sie eine NetScaler VPX-Instanz mit mehreren IP-Adressen bereitstellen. Sie können einer VPX-Instanz auf zwei Arten IP-Adressen hinzufügen:

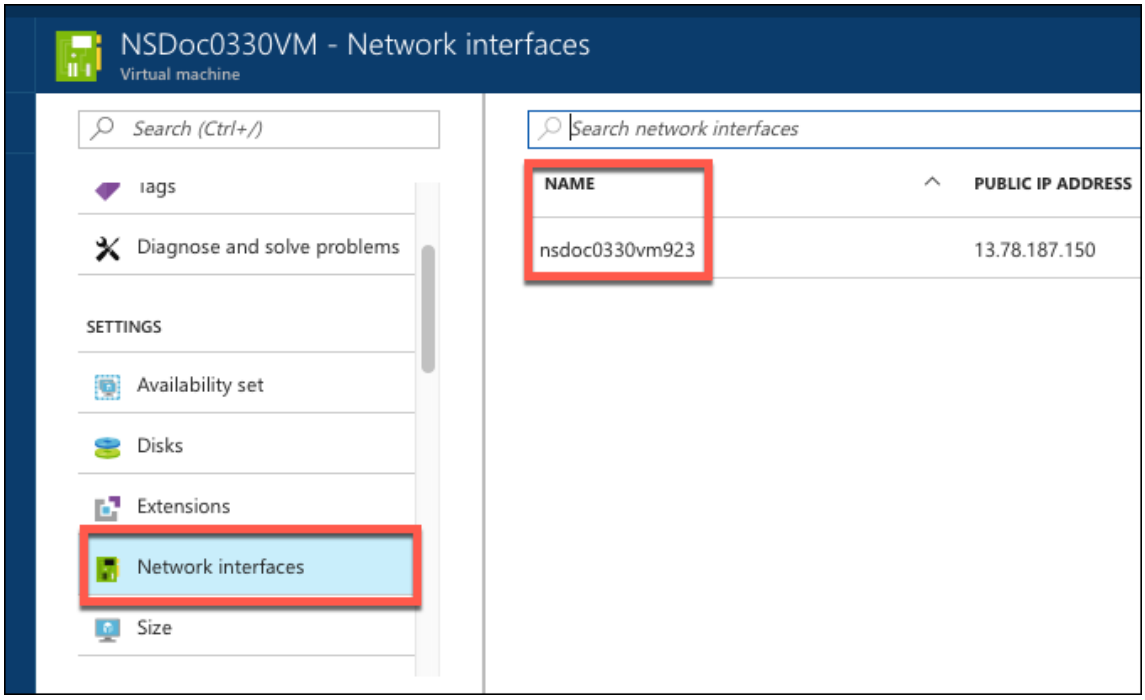
a. Beim Provisioning einer VPX-Instanz

Weitere Informationen zum Hinzufügen mehrerer IP-Adressen während der Bereitstellung einer VPX-Instanz finden Sie unter Konfigurieren mehrerer IP-Adressen für eine eigenständige NetScaler-Instanz. Informationen zum Hinzufügen von IP-Adressen mithilfe von PowerShell-Befehlen während der Bereitstellung einer VPX-Instanz finden Sie unter Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

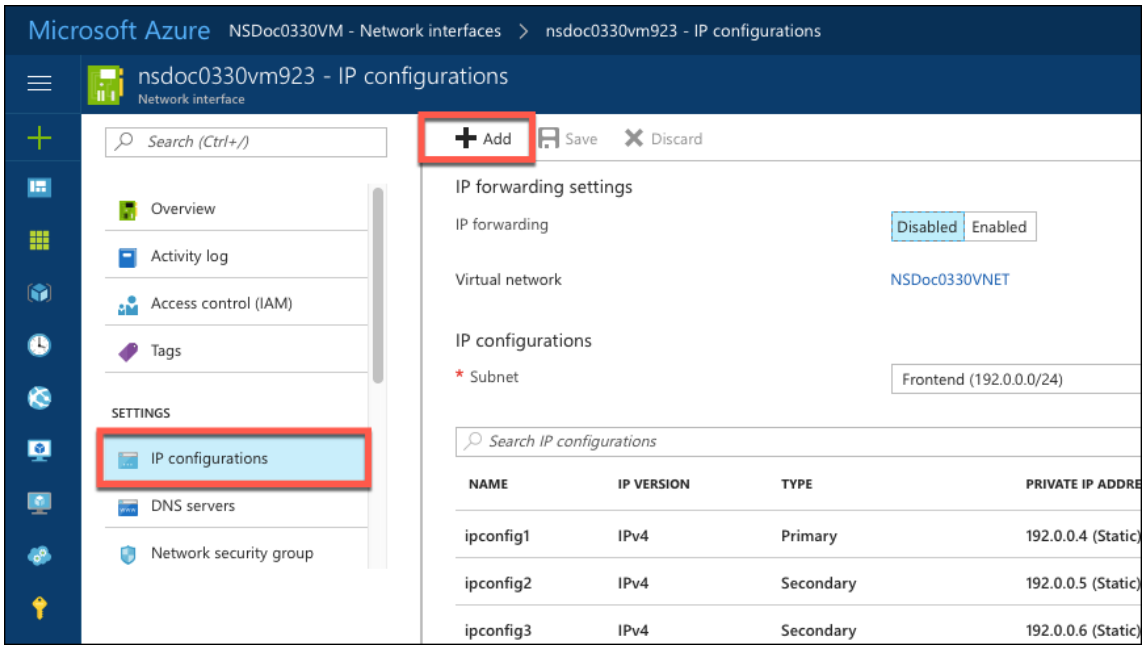
b. Nach der Provisioning einer VPX-Instanz

Nachdem Sie eine VPX-Instanz bereitgestellt haben, führen Sie diese Schritte aus, um eine private IP-Adresse im Azure-Portal zu registrieren, das Sie als Adresspool in der NetScaler Gateway-Appliance konfigurieren.

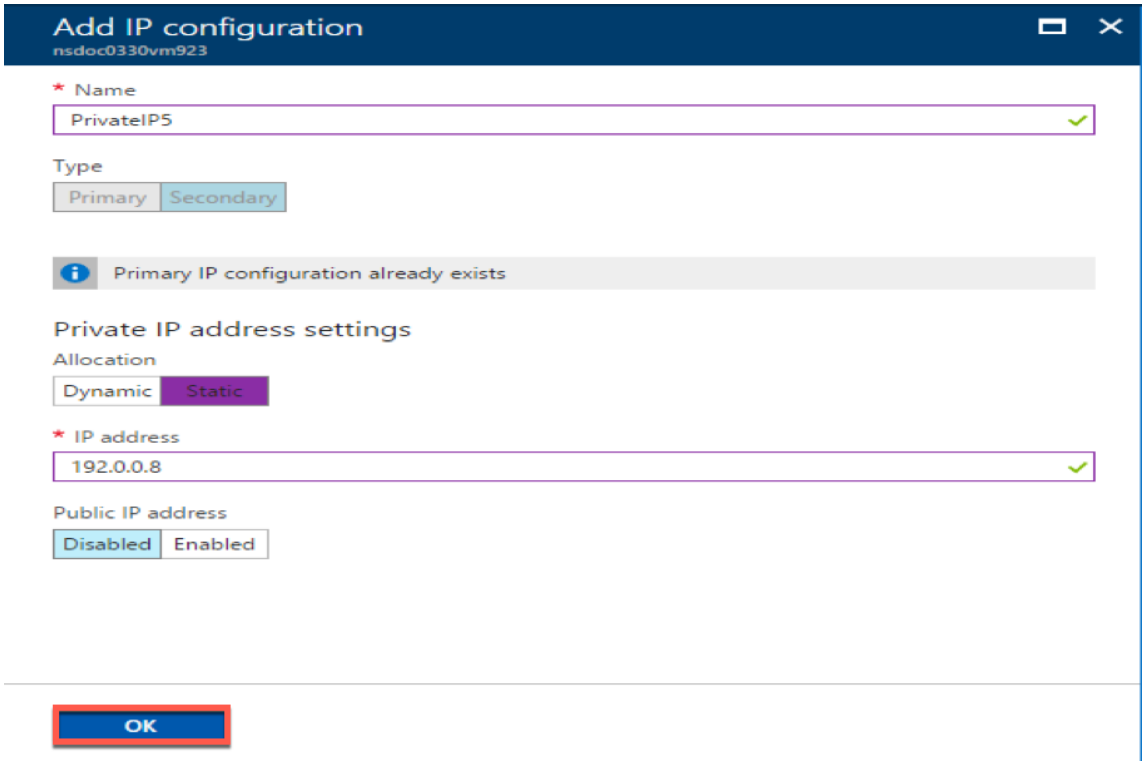
1. Wechseln Sie in Azure Resource Manager (ARM) zur bereits erstellten NetScaler VPX-Instanz > **Netzwerkschnittstellen**. Wählen Sie die Netzwerkschnittstelle, die an ein Subnetz gebunden ist, zu dem das IIP gehört, das Sie registrieren möchten.



2. Klicken Sie auf **IP-Konfigurationen**, und klicken Sie dann auf **Hinzufügen**.



3. Geben Sie die erforderlichen Details ein, wie im folgenden Beispiel gezeigt, und klicken Sie auf **OK**.



Konfigurieren von Adresspools in der NetScaler Gateway Appliance

Weitere Informationen zum Konfigurieren von Adresspools auf dem NetScaler Gateway finden Sie unter Konfigurieren von Adresspools.

Einschränkung: Sie können eine Reihe von IIP-Adressen nicht an Benutzer binden. Jede IIP-Adresse, die in einem Adresspool verwendet wird, muss registriert sein.

Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz über PowerShell-Befehle konfigurieren

May 11, 2023

In einer Azure-Umgebung kann eine virtuelle NetScaler VPX-Appliance mit mehreren NICs bereitgestellt werden. Jede Netzwerkkarte kann mehrere IP-Adressen haben. In diesem Abschnitt wird beschrieben, wie Sie eine NetScaler VPX-Instanz mit einer einzelnen Netzwerkkarte und mehreren IP-Adressen mithilfe von PowerShell-Befehlen bereitstellen. Sie können dasselbe Skript für die Multi-NIC- und Multi-IP-Bereitstellung verwenden.

> **Hinweis**
>
> In diesem Dokument bezieht sich IP-Config auf ein Paar von IP-Adressen, öffentliche IP und private IP, die mit einer einzelnen Netzwerkkarte verknüpft sind. Weitere Informationen finden Sie im Abschnitt Azure-Terminologie .

Anwendungsfall

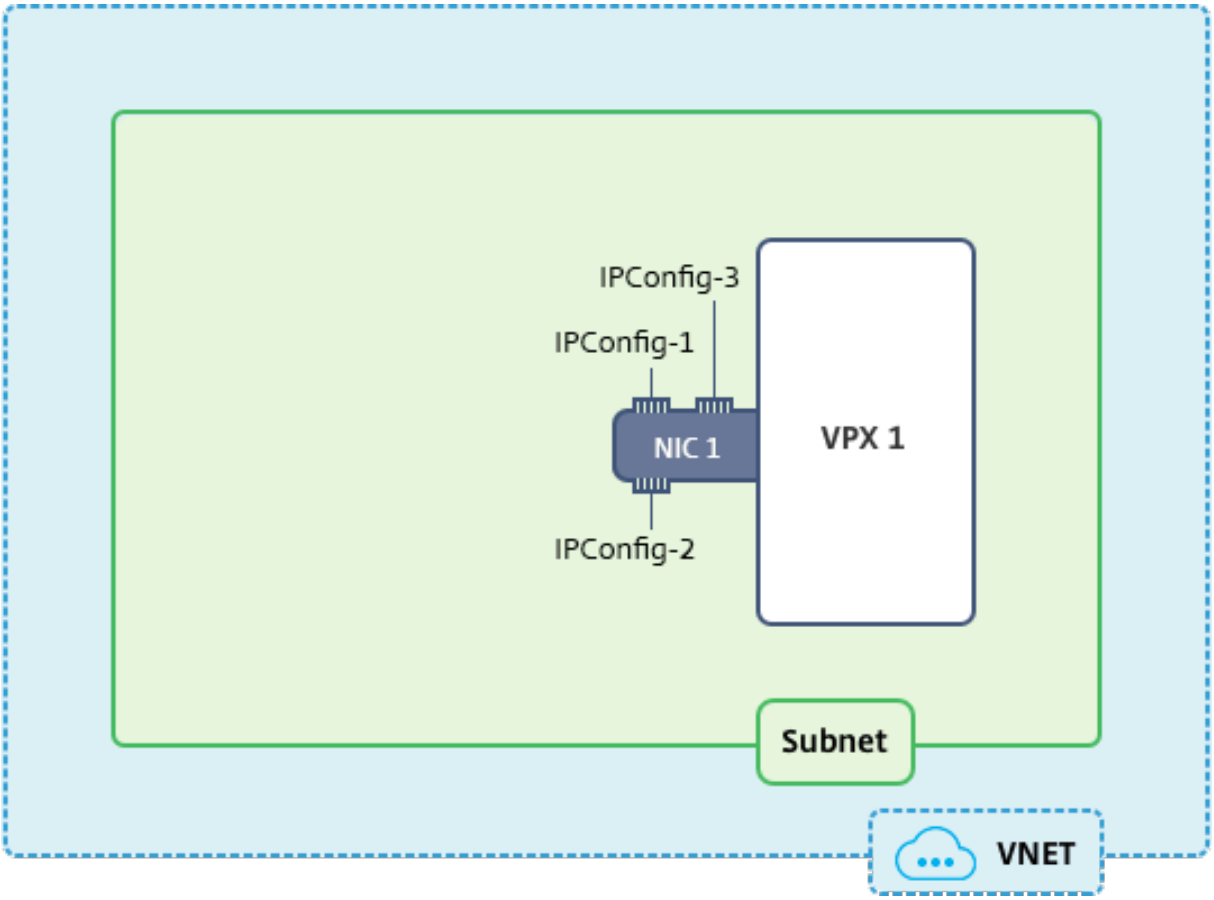
In diesem Anwendungsfall ist eine einzelne Netzwerkkarte mit einem virtuellen Netzwerk (VNET) verbunden. Die Netzwerkkarte ist drei IP-Konfigurationen zugeordnet, wie in der folgenden Tabelle dargestellt.

IP-Konfiguration	Verbunden mit
IPConfig-1	Statische öffentliche IP-Adresse; statische private IP-Adresse
IPConfig-2	Statische öffentliche IP-Adresse; statische Privatadresse
IPConfig-3	Statische private IP-Adresse

> **Hinweis**
>
> ipConfig-3 ist mit keiner öffentlichen IP-Adresse verknüpft.

Diagramm: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.



> **Hinweis**
>
> In einer Multi-Nic, Multi-IP Azure NetScaler VPX-Bereitstellung wird die private IP-Adresse, die mit der primären (ersten) `IPConfig` der primären (ersten) Netzwerkkarte verknüpft ist, automatisch als Verwaltungs-NSIP-Adresse der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die mit verknüpft sind, `IPConfigs` müssen in der VPX-Instanz als VIPs oder SNIPs mit dem `add ns ip` Befehl hinzugefügt werden, wie von Ihren Anforderungen festgelegt.

Im Folgenden finden Sie die Schritte, die zum Konfigurieren mehrerer IP-Adressen für eine virtuelle NetScaler VPX Appliance im Standalone-Modus erforderlich sind:

1. Ressourcengruppe erstellen
2. Speicherkonto erstellen
3. Verfügbarkeitsset erstellen
4. Netzwerkdienstgruppe erstellen
5. Virtuelles Netzwerk erstellen
6. Öffentliche IP-Adresse erstellen
7. IP-Konfiguration zuweisen
8. NIC erstellen
9. Erstellen Sie NetScaler VPX-Instanz

10. NIC-Konfigurationen überprüfen
11. VPX-seitige Konfigurationen überprüfen

Skript

Parameter

Im Folgenden finden Sie Beispielparametereinstellungen für den Anwendungsfall in diesem Dokument. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

$locName=”westcentralus”

$rgName=”Azure-MultiIP”

$nicName1=”VM1-NIC1”

$vNetName=”Azure-MultiIP-vnet”

$vNetAddressRange=”11.6.0.0/16”

$frontEndSubnetName=”frontEndSubnet”

$frontEndSubnetRange=”11.6.1.0/24”

$prmStorageAccountName=”multiipstorage”

$avSetName=”multiip-avSet”

$vmSize=”Standard_DS4_v2” (Dieser Parameter erstellt eine VM mit bis zu vier NICs.)

Hinweis: Die Mindestanforderung für eine VPX-Instanz ist 2 vCPUs und 2 GB RAM.

$Publisher = “Citrix”

$offer=”netscalervpx110-6531” (Sie können andere Angebote verwenden.)

$sku=”netscalerbyol” (Je nach Ihrem Angebot kann die SKU unterschiedlich sein.)

$version=”latest”

$pubIPName1=”PIP1”

$pubIPName2=”PIP2”

$domName1=”multiipvpx1”

$domName2=”multiipvpx2”

$vmNamePrefix=”VPXMultiIP”

$osDiskSuffix=”osmultiipalbdiskdb1”

Informationen zur Netzwerksicherheitsgruppe (NSG):

$nsgName=”NSG-MultiIP”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=”IPConfig1”

$IPConfigName2=”IPConfig-2”

$IPConfigName3=”IPConfig-3”

1. Ressourcengruppe erstellen

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Speicherkonto erstellen

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Verfügbarkeitsset erstellen

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$rgName -Location $locName
```

4. Netzwerksicherheitsgruppe erstellen

1. Fügen Sie Regeln hinzu. Sie müssen der Netzwerksicherheitsgruppe eine Regel für jeden Port hinzufügen, der Datenverkehr bedient.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -Description
    "Allow HTTP"-Access Allow -Protocol Tcp -Direction Inbound -Priority
   101 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 80
   $rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -Description
    "Allow HTTPS"-Access Allow -Protocol Tcp -Direction Inbound -Priority
   110 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 443
   $rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -Description
    "Allow SSH"-Access Allow -Protocol Tcp -Direction Inbound -Priority
   120 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 22
   ```


2. Erstellen Sie ein Netzwerksicherheitsgruppenobjekt.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

5. Virtuelles Netzwerk erstellen

1. Fügen Sie Subnetze hinzu.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $frontEndSubnetName
 -AddressPrefix $frontEndSubnetRange
```

2. Fügen Sie ein virtuelles Netzwerkobjekt hinzu.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
$frontendSubnet
```

3. Rufen Sie Subnetze ab.

```
$subnetName="frontEndSubnet"
$subnet1=$vnet.Subnets|?{ $_.Name -eq $subnetName }
```

6. Öffentliche IP-Adresse erstellen

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod
Static
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod
Static
```

> **Hinweis**
>
> Prüfen Sie vor der Verwendung die Verfügbarkeit von Domainnamen.
>
> Die Zuordnungsmethode für IP-Adressen kann dynamisch oder statisch sein.

7. IP-Konfiguration zuweisen

Berücksichtigen Sie in diesem Anwendungsfall die folgenden Punkte, bevor Sie IP-Adressen zuweisen:

- ipConfig-1 gehört zum Subnetz1 von VPX1.
- ipConfig-2 gehört zum Subnetz 1 von VPX1.
- ipConfig-3 gehört zum Subnetz 1 von VPX1.

> **Hinweis**
>
> Wenn Sie einer NIC mehrere IP-Konfigurationen zuweisen, muss eine Konfiguration als primäre zugewiesen werden.

```
$IPAddress1="11.6.1.27"
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress $pip1
     -Primary
$IPAddress2="11.6.1.28"
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress $pip2
$IPAddress3="11.6.1.29"
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

Verwenden Sie eine gültige IP-Adresse, die Ihren Subnetzanforderungen entspricht, und überprüfen Sie deren Verfügbarkeit.

8. NIC erstellen

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,$IPConfig3
 -NetworkSecurityGroupId $nsg.Id
```

9. Erstellen Sie NetScaler VPX-Instanz

1. Initialisieren Sie Variablen.

   ```
   $suffixNumber = 1
   $vmName = $vmNamePrefix + $suffixNumber
   ```

2. Erstellen Sie ein VM-Konfigurationsobjekt.

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
    $avSet.Id
   ```

3. Legen Sie Anmeldeinformationen, Betriebssystem und Image fest.

   ```
   $cred=Get-Credential -Message "Type the name and password for VPX login
   ."
   $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
    $vmName -Credential $cred
   $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher
    -Offer $offer -Skus $sku -Version $version
   ```


4. Fügen Sie NIC hinzu.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
Primary
```

> **Hinweis**
>
> In einer VPX-Bereitstellung mit mehreren Nic muss eine NIC primär sein. Daher muss "-Primary" angehängt werden, während diese NIC zur VPX-Instanz hinzugefügt wird.

5. Geben Sie den Betriebssystemdatenträger an und erstellen Sie VM.

```
$osDiskName=$vmName + "-"+ $osDiskSuffix1
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString()+ "vhds/"+
 $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

10. NIC-Konfigurationen überprüfen

Nachdem die VPX-Instanz gestartet wurde, können Sie die IP-Adressen, die `IPConfigs` der VPX-NIC zugewiesen sind, mit dem folgenden Befehl überprüfen.

```
$nic.IPConfig
```

11. VPX-seitige Konfigurationen überprüfen

Wenn die NetScaler VPX-Instanz gestartet wird, wird eine private IP-Adresse, die mit `IPconfig` der primären Netzwerkkarte verknüpft ist, als NSIP-Adresse hinzugefügt. Die verbleibenden privaten IP-Adressen müssen gemäß Ihren Anforderungen als VIP- oder SNIP-Adressen hinzugefügt werden. Verwenden Sie den folgenden Befehl.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Sie haben jetzt mehrere IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus konfiguriert.

Zusätzliche PowerShell-Skripts für die Azure-Bereitstellung

June 2, 2023

Dieser Abschnitt enthält die PowerShell-Cmdlets, mit denen Sie die folgenden Konfigurationen in Azure PowerShell durchführen können:

- Bereitstellung einer eigenständigen NetScaler VPX-Instanz
- Bereitstellung eines NetScaler VPX-Paars in einem Hochverfügbarkeits-Setup mit einem externen Azure-Load Balancer
- Stellen Sie ein NetScaler VPX-Paar in einem Hochverfügbarkeits-Setup mit dem internen Azure-Load Balancer bereit

In den folgenden Themen finden Sie auch Konfigurationen, die Sie mithilfe von PowerShell-Befehlen durchführen können:

- Hochverfügbarkeitssetup mit mehreren IP-Adressen und NICs über PowerShell-Befehle konfigurieren
- Konfigurieren von GSLB auf NetScaler VPX-Instanzen
- Konfigurieren Sie GSLB auf einem NetScaler Active-Standby-Hochverfügbarkeits-Setup
- Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalonemodus über PowerShell-Befehle
- Konfigurieren mehrerer Azure-VIPs für eine eigenständige VPX-Instanz

Bereitstellung einer eigenständigen NetScaler VPX-Instanz

1. **Eine Ressourcengruppe erstellen**

   Die Ressourcengruppe kann alle Ressourcen für die Lösung oder nur die Ressourcen enthalten, die Sie als Gruppe verwalten möchten. Der hier angegebene Standort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Load Balancers dieselbe Ressourcengruppe verwenden.

   ```
   $rgName="<resource group name>"
   $locName="<location name, such as West US>
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Zum Beispiel:

   ```
   $rgName = "ARM-VPX"
   $locName = "West US"
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.


```
$saName="<storage account name>"
$saType="<storage account type>"
```
, geben Sie eine an: `Standard_LRSStandard_GRS`, `Standard_RAGRS`, oder `Premium_LRS`

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -
Type $saType -Location $locName
```

Zum Beispiel:

```
$saName="vpxstorage"
$saType="Standard_LRS"
New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
    -Type $saType -Location $locName
<!--NeedCopy-->
```

3. **Verfügbarkeitssatz erstellen**

   Das Verfügbarkeitsset hilft dabei, Ihre virtuellen Maschinen während Ausfallzeiten, z. B. während Wartungsarbeiten, verfügbar zu halten. Ein mit einem Verfügbarkeitssatz konfigurierter Load Balancer stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, falls das Subnetz nicht zuvor erstellt wurde.

   ```
   $FrontendAddressPrefix="10.0.1.0/24"
   $BackendAddressPrefix="10.0.2.0/24"
   $vnetAddressPrefix="10.0.0.0/16"
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet
    -AddressPrefix $FrontendAddressPrefix
   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet
    -AddressPrefix $BackendAddressPrefix
   New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName -
   Location $locName -AddressPrefix $vnetAddressPrefix -Subnet $frontendSubnet
   ,$backendSubnet
   ```

   Zum Beispiel:

   ```
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       frontendSubnet -AddressPrefix $FrontendAddressPrefix

   ```



```
3 $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
     backendSubnet -AddressPrefix $BackendAddressPrefix
4
5 New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
      -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
     $frontendSubnet,$backendSubnet
6 <!--NeedCopy-->
```

5. **Erstellen Sie eine NIC**

   Erstellen Sie eine NIC und verknüpfen Sie die NIC mit der NetScaler VPX-Instanz. Das im obigen Verfahren erstellte Front-End-Subnetz wird mit 0 und das Back-End-Subnetz mit 1 indexiert. Erstellen Sie nun eine NIC auf eine der drei folgenden Arten:

   a) *NIC mit öffentlicher IP-Adresse*

   ```
   $nicName="<name of the NIC of the VM>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -Location $locName -AllocationMethod Dynamic

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   b) *NIC mit öffentlicher IP und DNS-Label*

   ```
   $nicName="<name of the NIC of the VM>"

   $domName="<domain name label>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -DomainNameLabel $domName -Location $locName -AllocationMethod
   Dynamic
   ```

   Bevor Sie $domName zuweisen, überprüfen Sie mit dem folgenden Befehl, ob er verfügbar ist oder nicht:

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -Location
   $locName

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   Zum Beispiel:

   ```
   1 $nicName="frontendNIC"
   2
   ```



```
$domName="vpxazure"

$pip = New-AzureRmPublicIpAddress -Name $nicName -
    ResourceGroupName $rgName -DomainNameLabel $domName -Location
    $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
    Subnets[0].Id -PublicIpAddressId $pip.Id
<!--NeedCopy-->
```

c) *NIC mit dynamischer öffentlicher Adresse und statischer privater IP-Adresse*

Stellen Sie sicher, dass die private (statische) IP-Adresse, die Sie der VM hinzufügen, den gleichen Bereich haben muss wie die des angegebenen Subnetzes.

```
$nicName="<name of the NIC of the VM>"

$staticIP="<available static IP address on the subnet>"

$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
$rgName -Location $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
```

6. **Erstellen eines virtuellen Objekts**

```
$vmName="<VM name>"

$vmSize="<VM size string>"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName

$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
 $avset.Id
```

7. **Holen Sie sich das NetScaler VPX-Image**

```
$pubName="<Image publisher name>"

$offerName="<Image offer name>"

$skuName="<Image SKU name>"

$cred=Get-Credential -Message "Type the name and password of the local
administrator account."
```

Geben Sie Ihre Anmeldeinformationen ein, die für die Anmeldung bei VPX verwendet werden


```
$vm=Set-AzureRmVMOperatingSystem -VM $vm -Linux -ComputerName $vmName -
Credential $cred -Verbose

$vm=Set-AzureRmVMSourceImage -VM $vm -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"

$vm=Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
```

Zum Beispiel:

```
$pubName="citrix"
```

Mit dem folgenden Befehl werden alle Angebote von Citrix angezeigt:

```
1 Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
     Select Offer
2
3 $offerName="netscalervpx110-6531"
4 <!--NeedCopy-->
```

Der folgende Befehl wird verwendet, um die vom Herausgeber angebotene SKU für einen bestimmten Angebotsnamen zu kennen:

```
Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -Offer
$offerName | Select Skus
```

8. **Erstellen einer virtuellen Maschine**

```
$diskName="<name identifier for the disk in Azure storage, such as
OSDisk>"
```

Zum Beispiel:

```
1  $diskName="dynamic"
2
3  $pubName="citrix"
4
5  $offerName="netscalervpx110-6531"
6
7  $skuName="netscalerbyol"
8
9  $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
       Name $saName
10
11 $osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/"
       + $diskName  + ".vhd"
12
13 $vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri
        -CreateOption fromImage
```



```
<!--NeedCopy-->
```

Wenn Sie eine VM aus Images erstellen, die auf dem Marketplace vorhanden sind, verwenden Sie den folgenden Befehl, um den VM-Plan anzugeben:

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName -Name
 $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Bereitstellung eines NetScaler VPX-Paars in einem Hochverfügbarkeits-Setup mit einem externen Azure-Load Balancer

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei Azure-Konto an.

1. **Eine Ressourcengruppe erstellen**

   Der hier angegebene Standort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle, die zum Erstellen eines Load Balancers verwendet werden, dieselbe Ressourcengruppe verwenden.

   ```
   $rgName="<resource group name>"

   $locName="<location name, such as West US>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Zum Beispiel:

   ```
   $rgName = "ARM-LB-NS"

   $locName = "West US"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   ```
   $saName="<storage account name>"

   $saType="<storage account type>"
   ```

   , geben Sie eine an: `Standard_LRSStandard_GRS`, `Standard_RAGRS`, oder `Premium_LRS`

   ```
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -
   Type $saType -Location $locName
   ```

   Zum Beispiel:


```
$saName="vpxstorage"

$saType="Standard_LRS"

New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
    -Type $saType -Location $locName
<!--NeedCopy-->
```

3. **Verfügbarkeitssatz erstellen**

   Ein mit einem Verfügbarkeitssatz konfigurierter Load Balancer stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   ```
   $avName="<availability set name>"
   ```

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, falls das Subnetz nicht zuvor erstellt wurde.

   ```
   $vnetName = "LBVnet"

   $FrontendAddressPrefix="10.0.1.0/24"

   $BackendAddressPrefix="10.0.2.0/24"

   $vnetAddressPrefix="10.0.0.0/16"

   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       frontendSubnet -AddressPrefix $FrontendAddressPrefix

   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
       backendSubnet -AddressPrefix $BackendAddressPrefix

   $vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
       $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
       Subnet $frontendSubnet,$backendSubnet
   <!--NeedCopy-->
   ```

   Hinweis: Wählen Sie den AddressPrefix-Parameterwert gemäß Ihren Anforderungen.

   Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, Front-End- und Back-End-Subnetz zu.

Wenn das Front-End-Subnetz das erste Element von Array VNet ist, muss subnetId $vNet.Subnets [0] .Id sein.

Wenn das Front-End-Subnetz das zweite Element im Array ist, muss die subnetID $vNet.Subnets [1] .Id und so weiter sein.

5. **Konfigurieren der Front-End-IP-Adresse und Erstellen eines Back-End-Adress-Pools**

   Konfigurieren Sie eine Front-End-IP-Adresse für den eingehenden Load Balancer-Netzwerkverkehr und erstellen Sie einen Back-End-Adresspool, um den Load Balancer-Verkehr zu empfangen.

```
$pubName="PublicIp1"

$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -AllocationMethod
    Static -DomainNameLabel nsvpx
<!--NeedCopy-->
```

   Hinweis: Prüfen Sie, ob der Wert für DomainNameLabel verfügbar ist.

```
$FIPName = "ELBFIP"

$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -Name
    $FIPName -PublicIpAddress $publicIP1

$BEPool = "LB-backend-Pool"

$beaddresspool1= New-AzureRmLoadBalancerBackendAddressPoolConfig -
    Name $BEPool
<!--NeedCopy-->
```

6. **Erstellen Sie eine Gesundheitssonde**

   Erstellen Sie einen TCP-Integritätstest mit Port 9000 und einem Intervall von 5 Sekunden.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
    HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```

7. **Eine Load-Balancing-Regel erstellen**

   Erstellen Sie eine LB-Regel für jeden Dienst, den Sie Load Balancing durchführen.

   Zum Beispiel:

   Sie können das folgende Beispiel verwenden, um den HTTP-Dienst auszubalancieren.


```
$lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
    FrontendIpConfiguration $frontendIP1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe -Protocol Tcp -FrontendPort
     80 -BackendPort 80
<!--NeedCopy-->
```

8. **NAT-Regeln für eingehenden Datenverkehr erstellen**

   Erstellen Sie NAT-Regeln für Dienste, für die Sie keinen Lastenausgleich durchführen.

   Zum Beispiel beim Erstellen eines SSH-Zugriffs auf eine NetScaler VPX Instanz.

   Hinweis: Protocol-FrontendPort-BackendPort-Triplet darf für zwei NAT-Regeln nicht identisch sein.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH1     -FrontendIpConfiguration $frontendIP1 -Protocol
    TCP -FrontendPort 22 -BackendPort 22

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH2 -FrontendIpConfiguration $frontendIP1 -Protocol TCP -
    FrontendPort 10022 -BackendPort 22
<!--NeedCopy-->
```

9. **Erstellen einer Load Balancer-Entität**

   Erstellen Sie den Load Balancer, indem Sie alle Objekte (NAT-Regeln, Load Balancer-Regeln, Testkonfigurationen) zusammenfügen.

```
$lbName="ELB"

$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
    $lbName -Location $locName -InboundNatRule $inboundNATRule1,
    $inboundNATRule2 -FrontendIpConfiguration $frontendIP1 -
    LoadBalancingRule $lbrule1 -BackendAddressPool $beAddressPool1
    -Probe $healthProbe
<!--NeedCopy-->
```

10. **Erstellen Sie eine NIC**

    Erstellen Sie zwei NICs und ordnen Sie jede NIC jeder VPX-Instanz zu

    a) NIC1 mit VPX1

    Zum Beispiel:

```
$nicName="NIC1"
```



```
2
3  $lbName="ELB"
4
5  $bePoolIndex=0
6
7  * Rule indexes starts from 0.
8
9  $natRuleIndex=0
10
11 $subnetIndex=0
12
13 * Frontend subnet index
14
15 $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
       $rgName
16
17 $nic1=New-AzureRmNetworkInterface -Name $nicName -
       ResourceGroupName $rgName -Location $locName -Subnet $vnet.
       Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
       BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
       $lb.InboundNatRules[$natRuleIndex]
18 <!--NeedCopy-->
```

b) NIC2 mit VPX2

Zum Beispiel:

```
1  $nicName="NIC2"
2
3  $lbName="ELB"
4
5  $bePoolIndex=0
6
7  $natRuleIndex=1
8
9  * Second Inbound NAT (SSH) rule we need to use
10
11 `$subnetIndex=0
12
13 * Frontend subnet index
14
15 $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
       $rgName
16
17 $nic2=New-AzureRmNetworkInterface -Name $nicName -
```



```
    ResourceGroupName $rgName -Location $locName -Subnet $vnet.
    Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
    BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
    $lb.InboundNatRules[$natRuleIndex]
<!--NeedCopy-->
```

11. **Erstellen von NetScaler VPX-Instanzen**

    Erstellen Sie zwei NetScaler VPX-Instanzen als Teil derselben Ressourcengruppe und derselben Verfügbarkeitsgruppe und hängen Sie sie an den externen Load Balancer an.

    a) NetScaler VPX-Instanz 1

    Zum Beispiel:

```
$vmName="VPX1"

$vmSize="Standard_A3"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
    $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
    to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName
```



```
26
27 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
      " + $diskName  + ".vhd"
28
29 $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
      $osDiskUri1 -CreateOption fromImage
30
31 Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
       -Name $skuName
32
33 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
      $vm1
34 <!--NeedCopy-->
```

b) NetScaler VPX-Instanz 2

Zum Beispiel:

```
1  $vmName="VPX2"
2
3  $vmSize="Standard_A3"
4
5  $avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
       $rgName
6
7  $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
      AvailabilitySetId $avset.Id
8
9  $cred=Get-Credential -Message " Type Credentials which will be
      used to login to VPX instance "
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
      $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
      Offer $offerName -Skus $skuName -Version "latest"
14
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
      Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
```



```
      " + $diskName  + ".vhd"
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
      $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
       -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
      $vm2
28 <!--NeedCopy-->
```

12. **Konfiguration der virtuellen Maschinen**

    Wenn beide NetScaler VPX-Instanzen gestartet werden, stellen Sie mithilfe des SSH-Protokolls eine Verbindung zu beiden NetScaler VPX-Instanzen her, um die virtuellen Maschinen zu konfigurieren.

    a) Active-Active: Führen Sie dieselben Konfigurationsbefehle auf der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    b) Active-Passive: Führen Sie diesen Befehl in der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    ```
    add ha node ##nodeID <nsip of other NetScaler VPX>
    ```

    Führen Sie im Active-Passive-Modus Konfigurationsbefehle nur auf dem primären Knoten aus.

Stellen Sie ein NetScaler VPX-Paar in einem Hochverfügbarkeits-Setup mit dem internen Azure-Load Balancer bereit

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei Azure-Konto an.

1. **Eine Ressourcengruppe erstellen**

   Der hier angegebene Standort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Load Balancers dieselbe Ressourcengruppe verwenden.

   ```
   $rgName="\<resource group name\>"

   $locName="\<location name, such as West US\>"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Zum Beispiel:

   ```
   1 $rgName = "ARM-LB-NS"
   2
   ```



```
$locName = "West US"

New-AzureRmResourceGroup -Name $rgName -Location $locName
<!--NeedCopy-->
```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, geben Sie eine an: `Standard_LRSStandard_GRS`, `Standard_RAGRS`, oder `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   Zum Beispiel:

   ```
   $saName="vpxstorage"

   $saType="Standard_LRS"

   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
       -Type $saType -Location $locName
   <!--NeedCopy-->
   ```

3. **Verfügbarkeitssatz erstellen**

   Ein mit einem Verfügbarkeitssatz konfigurierter Load Balancer stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, falls das Subnetz nicht zuvor erstellt wurde.

   ```
   $vnetName = "LBVnet"

   $vnetAddressPrefix="10.0.0.0/16"

   $FrontendAddressPrefix="10.0.1.0/24"

   ```



```
$BackendAddressPrefix="10.0.2.0/24"

$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
    Subnet $frontendSubnet,$backendSubnet`

$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix
<!--NeedCopy-->
```

Hinweis: Wählen Sie den AddressPrefix-Parameterwert gemäß Ihren Anforderungen.

Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, Front-End- und Back-End-Subnetz zu.

Wenn das Front-End-Subnetz das erste Element von Array VNet ist, muss subnetId $vNet.Subnets [0] .Id sein.

Wenn das Front-End-Subnetz das zweite Element im Array ist, muss die subnetID $vNet.Subnets [1] .Id und so weiter sein.

5. **Erstellen eines Backend-Adresspool**

```
$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name "
LB-backend"
```

6. **NAT-Regeln erstellen**

   Erstellen Sie NAT-Regeln für Dienste, für die Sie keinen Lastenausgleich durchführen.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -
    Protocol TCP -FrontendPort 3441 -BackendPort 3389

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name "RDP2" -FrontendIpConfiguration $frontendIP -Protocol TCP
    -FrontendPort 3442 -BackendPort 3389
<!--NeedCopy-->
```

   Verwenden Sie Front-End- und Back-End-Ports gemäß Ihren Anforderungen.

7. **Erstellen Sie eine Gesundheitssonde**

   Erstellen Sie einen TCP-Integritätstest mit Port 9000 und einem Intervall von 5 Sekunden.


```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "
    HealthProbe"  " -Protocol tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```

8. **Eine Load-Balancing-Regel erstellen**

   Erstellen Sie eine LB-Regel für jeden Dienst, den Sie Load Balancing durchführen.

   Zum Beispiel:

   Sie können das folgende Beispiel verwenden, um den HTTP-Dienst auszubalancieren.

```
$lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1" -
    FrontendIpConfiguration $frontendIP -BackendAddressPool
    $beAddressPool -Probe $healthProbe -Protocol Tcp -FrontendPort
    80 -BackendPort 80
<!--NeedCopy-->
```

   Verwenden Sie Front-End- und Back-End-Ports gemäß Ihren Anforderungen.

9. **Erstellen einer Load Balancer-Entität**

   Erstellen Sie den Load Balancer, indem Sie alle Objekte (NAT-Regeln, Load Balancer-Regeln, Testkonfigurationen) zusammenfügen.

```
$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -Name
    "InternalLB" -Location $locName -FrontendIpConfiguration
    $frontendIP -InboundNatRule $inboundNATRule1,$inboundNatRule2 -
    LoadBalancingRule $lbrule -BackendAddressPool $beAddressPool -
    Probe $healthProbe
<!--NeedCopy-->
```

10. **Erstellen Sie eine NIC**

    Erstellen Sie zwei Netzwerkkarten und ordnen Sie jede Netzwerkkarte jeder NetScaler VPX-Instanz zu

```
$backendnic1= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic1-be -Location $locName -PrivateIpAddress
    10.0.2.6 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[0]
<!--NeedCopy-->
```

    Diese Netzwerkkarte ist für NetScaler VPX 1. Die Private IP muss sich im selben Subnetz befinden wie die des hinzugefügten Subnetzes.


```
$backendnic2= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic2-be -Location $locName -PrivateIpAddress
    10.0.2.7 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
     $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules[1].
<!--NeedCopy-->
```

Diese NIC ist für NetScaler VPX 2. Der Parameter `Private IPAddress` kann jede private IP gemäß Ihrer Anforderung haben.

11. **Erstellen von NetScaler VPX-Instanzen**

    Erstellen Sie zwei VPX-Instanzen, die Teil derselben Ressourcengruppe und derselben Verfügbarkeitsgruppe sind, und hängen Sie sie an den internen Load Balancer an.

    a) NetScaler VPX-Instanz 1

    Zum Beispiel:

```
$vmName="VPX1"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
     $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
     to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

```



```
$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
    " + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
    $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
     -Name $skuName

New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
    $vm1
<!--NeedCopy-->
```

b) NetScaler VPX-Instanz 2

Zum Beispiel:

```
$vmName="VPX2"

$vmSize="Standard_A3"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
     $rgName

$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avset.Id

$cred=Get-Credential -Message " Type Credentials which will be
    used to login to VPX instance "

$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
    $vmName -Credential $cred -Verbose

$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
    Offer $offerName -Skus $skuName -Version "latest"

$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
    " + $diskName  + ".vhd"
```



```
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
       $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
        -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
       $vm2
28 <!--NeedCopy-->
```

12. **Konfiguration der virtuellen Maschinen**

    Wenn beide NetScaler VPX-Instanzen gestartet werden, stellen Sie mithilfe des SSH-Protokolls eine Verbindung zu beiden NetScaler VPX-Instanzen her, um die virtuellen Maschinen zu konfigurieren.

    a) Active-Active: Führen Sie dieselben Konfigurationsbefehle auf der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    b) Active-Passive: Führen Sie diesen Befehl in der Befehlszeile der beiden NetScaler VPX-Instanzen aus.

    ```
    add ha node ##nodeID <nsip of other NetScaler VPX>
    ```

    Führen Sie im Active-Passive-Modus Konfigurationsbefehle nur auf dem primären Knoten aus.

Häufig gestellte Fragen zu Azure

May 11, 2023

- **Unterscheidet sich das Upgrade-Verfahren der im Azure Marketplace installierten NetScaler VPX-Instanz vom on-premises Upgrade-Verfahren?**

  Nein. Sie können Ihre NetScaler VPX-Instanz in der Microsoft Azure-Cloud mithilfe der standardmäßigen NetScaler VPX-Upgrade-Verfahren auf NetScaler VPX Version 11.1 oder höher aktualisieren. Sie können das Upgrade entweder mithilfe von GUI- oder CLI-Verfahren durchführen. Verwenden Sie für neue Installationen das NetScaler VPX Image für die Microsoft Azure-Cloud.

  Um die NetScaler VPX-Upgrade-Builds herunterzuladen, gehen Sie zu **NetScaler Downloads > NetScaler Firmware.**

- **Wie korrigiert man MAC-Bewegungen und Interface-Stummutes, die auf NetScaler VPX-Instanzen auf Azure gehostet werden?**

In der Azure Multi-NIC-Umgebung zeigen alle Datenschnittstellen standardmäßig MAC-Bewegungen und Schnittstellenstummschaltung an. Um MAC-Verschiebungen und Schnittstellen-Stummschaltung in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, ein VLAN pro Datenschnittstelle (ohne Tag) der NetScaler VPX-Instanz zu erstellen und die primäre IP der NIC in Azure zu binden.

Weitere Informationen finden Sie im Artikel CTX224626 .

Bereitstellen einer NetScaler VPX Instanz auf der Google Cloud Platform

May 11, 2023

Sie können eine NetScaler VPX-Instanz auf der Google Cloud Platform (GCP) bereitstellen. Mit einer VPX-Instanz in GCP können Sie die Vorteile der GCP-Cloud-Computing-Funktionen nutzen und Citrix Load Balancing und Traffic-Management-Funktionen für Ihre geschäftlichen Anforderungen nutzen. Sie können VPX-Instanzen in GCP als eigenständige Instanzen bereitstellen. Sowohl einzelne NIC- als auch Multi-NIC-Konfigurationen werden unterstützt.

Unterstützte Features

Alle Premium-, Advanced- und Standardfunktionen werden auf der GCP basierend auf dem verwendeten Lizenz-/Versionstyp unterstützt.

Einschränkung

- IPv6 wird nicht unterstützt.

Hardwareanforderungen

Die VPX-Instanz in GCP muss mindestens 2 vCPUs und 4 GB RAM haben.

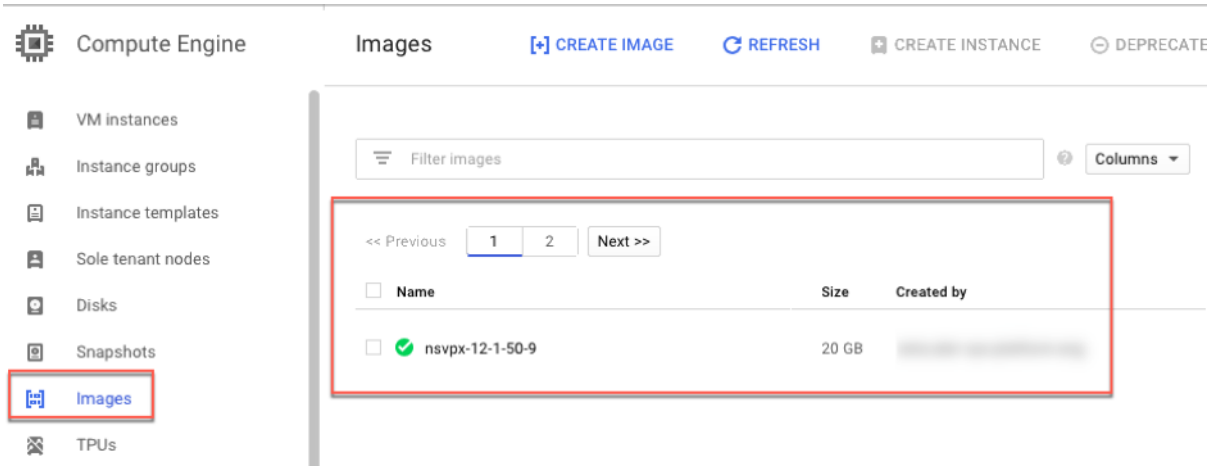
Voraussetzungen

1. Installieren Sie das Dienstprogramm “gcloud” auf Ihrem Gerät. Das Dienstprogramm finden Sie unter diesem Link: https://cloud.google.com/sdk/install
2. Laden Sie das NSVPX-GCP-Image von der NetScaler-Website herunter.
3. Laden Sie die Datei (z. B. NSVPX-GCP-12.1-50.9_NC_64.tar.gz) in einen Speicher-Bucket bei Google hoch, indem Sie die unter angegebenen Schritte ausführen https://cloud.google.com/storage/docs/uploading-objects.

4. Führen Sie den folgenden Befehl im gcloud-Dienstprogramm aus, um ein Image zu erstellen.

```
gcloud compute images create <IMAGE_NAME> --source-uri=gs://<
    STORAGE_BUCKET_NAME>/<FILE_NAME>.tar.gz --guest-os-features=
    MULTI_IP_SUBNET
<!--NeedCopy-->
```

Es kann einen Moment dauern, bis das Image erstellt wurde. Nachdem das Image erstellt wurde, wird es in der GCP-Konsole unter **Compute** > **Compute Engine** angezeigt.



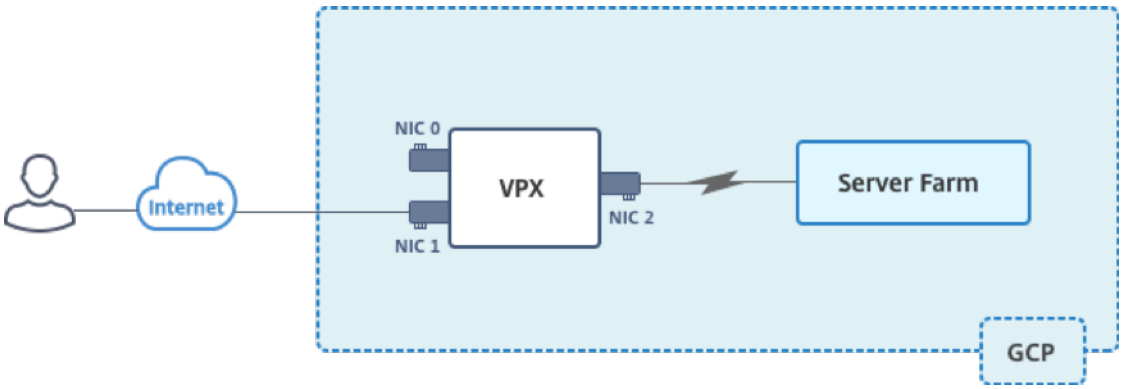
Wichtige Hinweise

Berücksichtigen Sie die folgenden GCP-spezifischen Punkte, bevor Sie mit der Bereitstellung beginnen.

- Nach dem Erstellen der Instanz können Sie keine Netzwerkschnittstellen hinzufügen oder entfernen.
- Erstellen Sie für eine Multi-NIC-Bereitstellung separate VPC-Netzwerke für jede Netzwerkkarte. Eine Netzwerkkarte kann nur mit einem Netzwerk verknüpft werden.
- Für eine Single-NIC-Instanz erstellt die GCP-Konsole standardmäßig ein Netzwerk.
- Für eine Instanz mit mehr als zwei Netzwerkschnittstellen sind mindestens 4 vCPUs erforderlich.
- Wenn IP-Weiterleitung erforderlich ist, müssen Sie die IP-Weiterleitung aktivieren, während Sie die Instanz erstellen und die Netzwerkkarte konfigurieren.

Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit mehreren NICs und mehreren IPs

Dieses Szenario zeigt, wie eine eigenständige NetScaler VPX-Instanz in GCP bereitgestellt wird. In diesem Szenario erstellen Sie eine eigenständige VPX-Instanz mit vielen NICs. Die Instanz kommuniziert mit Back-End-Servern (der Serverfarm).



Erstellen Sie drei NICs, um den folgenden Zwecken zu dienen.

Netzwerkkarte	Zweck	Verbunden mit VPC-Netzwerk
NIC 0	Dient Verwaltungsdatenverkehr (NetScaler IP)	Management-Netzwerk
NIC 1	Dient clientseitigem Datenverkehr (VIP)	Kunden-Netzwerk
NIC 2	Kommuniziert mit Back-End-Servern (SNIP)	Back-End-Server-Netzwerk

Richten Sie die erforderlichen Kommunikationswege zwischen den folgenden ein:

- VPX-Instanz und die Back-End-Server.
- VPX-Instanz und die externen Hosts im öffentlichen Internet.

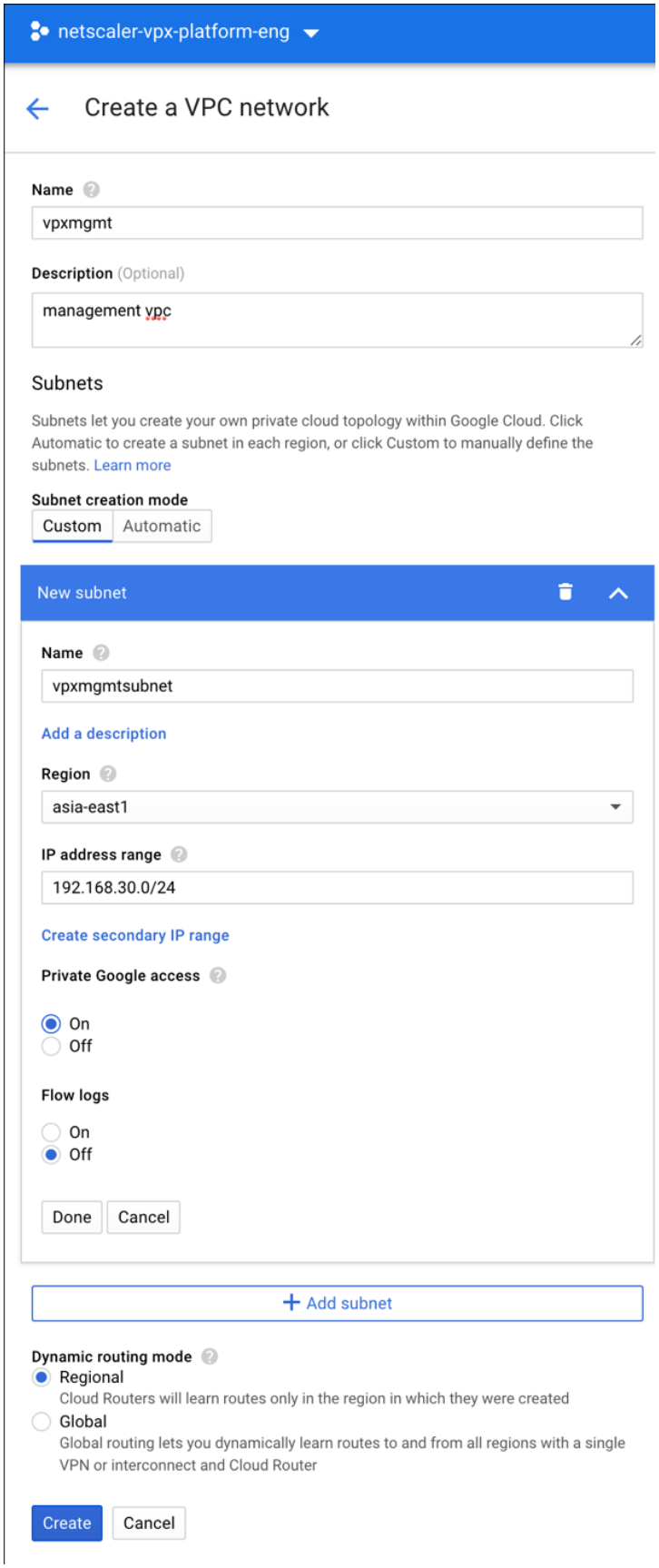
Zusammenfassung der Bereitstellungsschritte

1. Erstellen Sie drei VPC-Netzwerke für drei verschiedene NICs.
2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443
3. Erstellen einer Instanz mit drei NICs

> **Hinweis:**
>
> Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

Schritt 1. Erstellen Sie VPC-Netzwerke.

Erstellen Sie drei VPC-Netzwerke, die mit Verwaltungs-NIC, Client-NIC und Server-NIC verknüpft sind. Um ein VPC-Netzwerk zu erstellen, melden Sie sich bei **Google-Konsole > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**an. Füllen Sie die erforderlichen Felder aus, wie in der Bildschirmaufnahme gezeigt, und klicken Sie auf **Erstellen**.

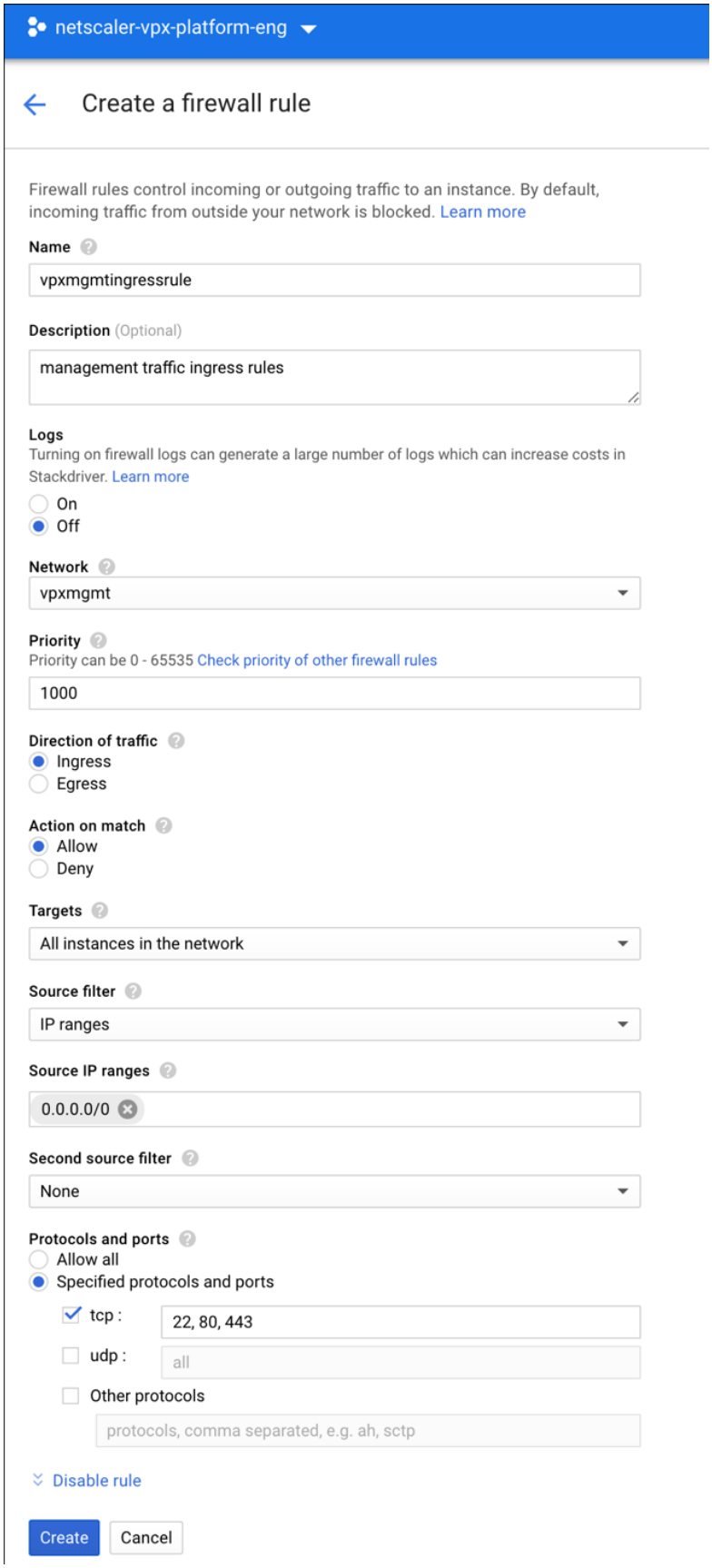


Erstellen Sie in ähnlicher Weise VPC-Netzwerke für client- und serverseitige Netzwerkkarten.

> **Hinweis:**
>
> Alle drei VPC-Netzwerke müssen sich in derselben Region befinden, die in diesem Szenario asia-east1 ist.

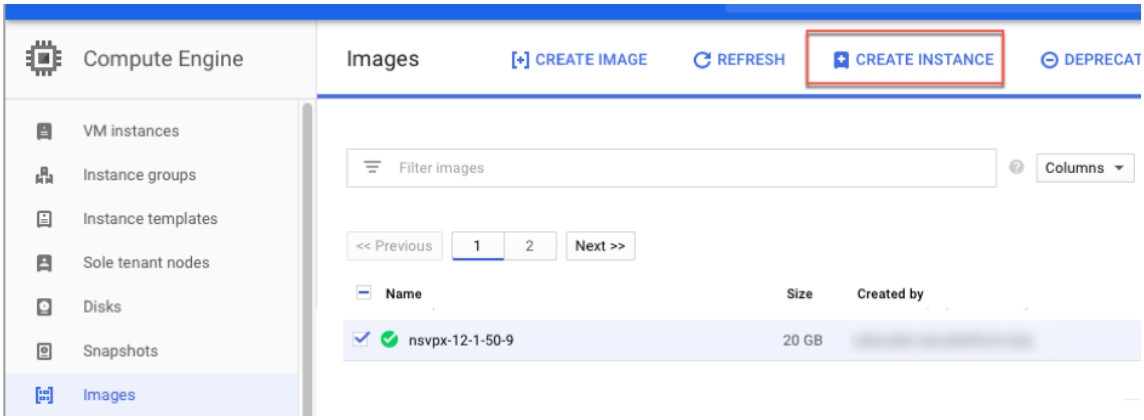
Schritt 2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für jedes VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Übersicht über Firewall-Regeln.



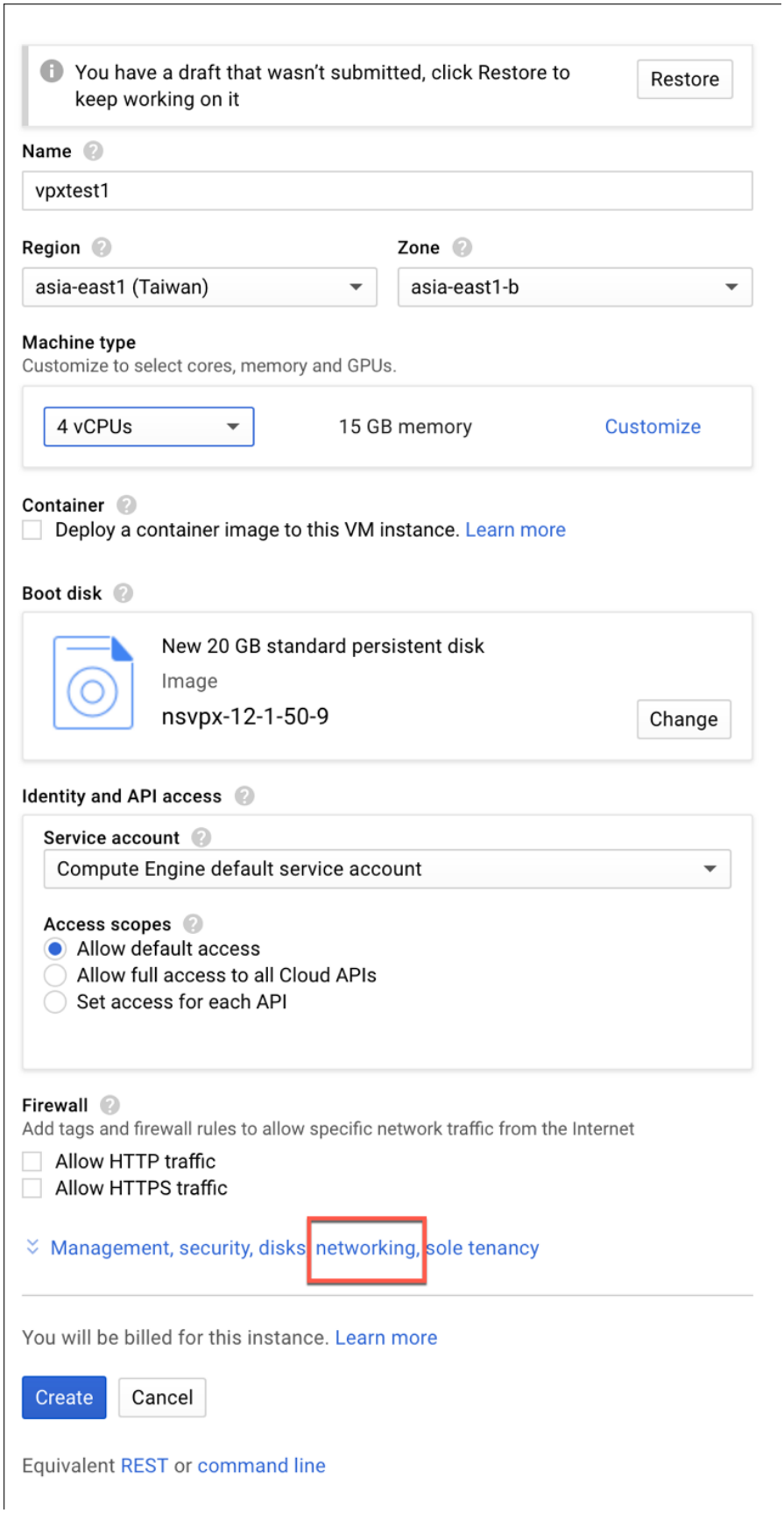
Schritt 3. Erstellen Sie die VPX-Instanz.

1. Melden Sie sich bei der GCP-Konsole an.
2. **Zeigen Sie unter**Compute**mit der Maus auf Compute Engine und wählen Sie Images aus.**
3. Wählen Sie das Image aus und klicken Sie auf **Instanz erstellen**.

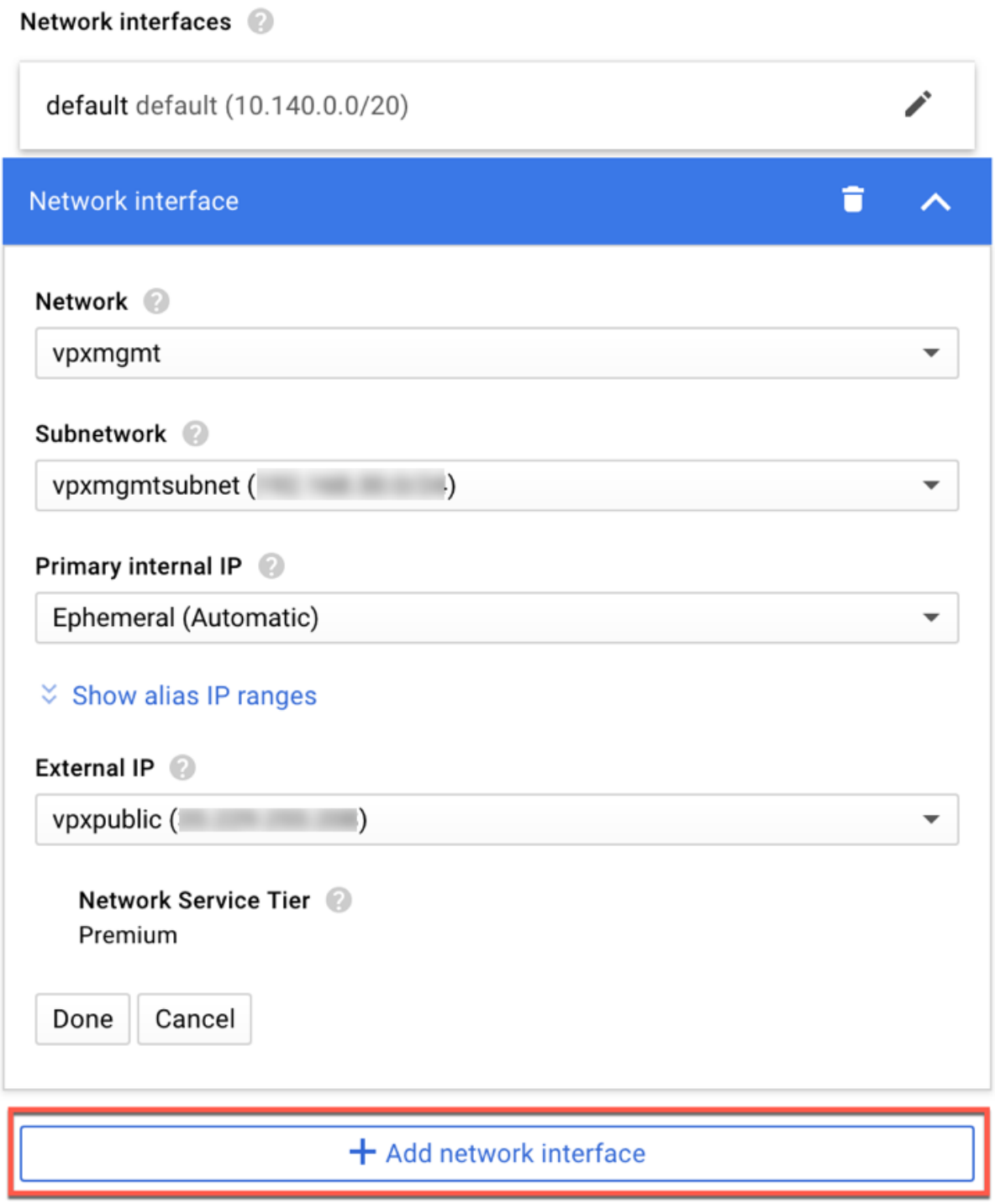


4. Wählen Sie eine Instanz mit 4 vCPUs aus, um mehrere Netzwerkkarten zu unterstützen.
5. Klicken Sie auf die Netzwerkoption unter Verwaltung, Sicherheit, Datenträger, Netzwerk, Einzelmandanten, um die zusätzlichen NICs hinzuzufügen.

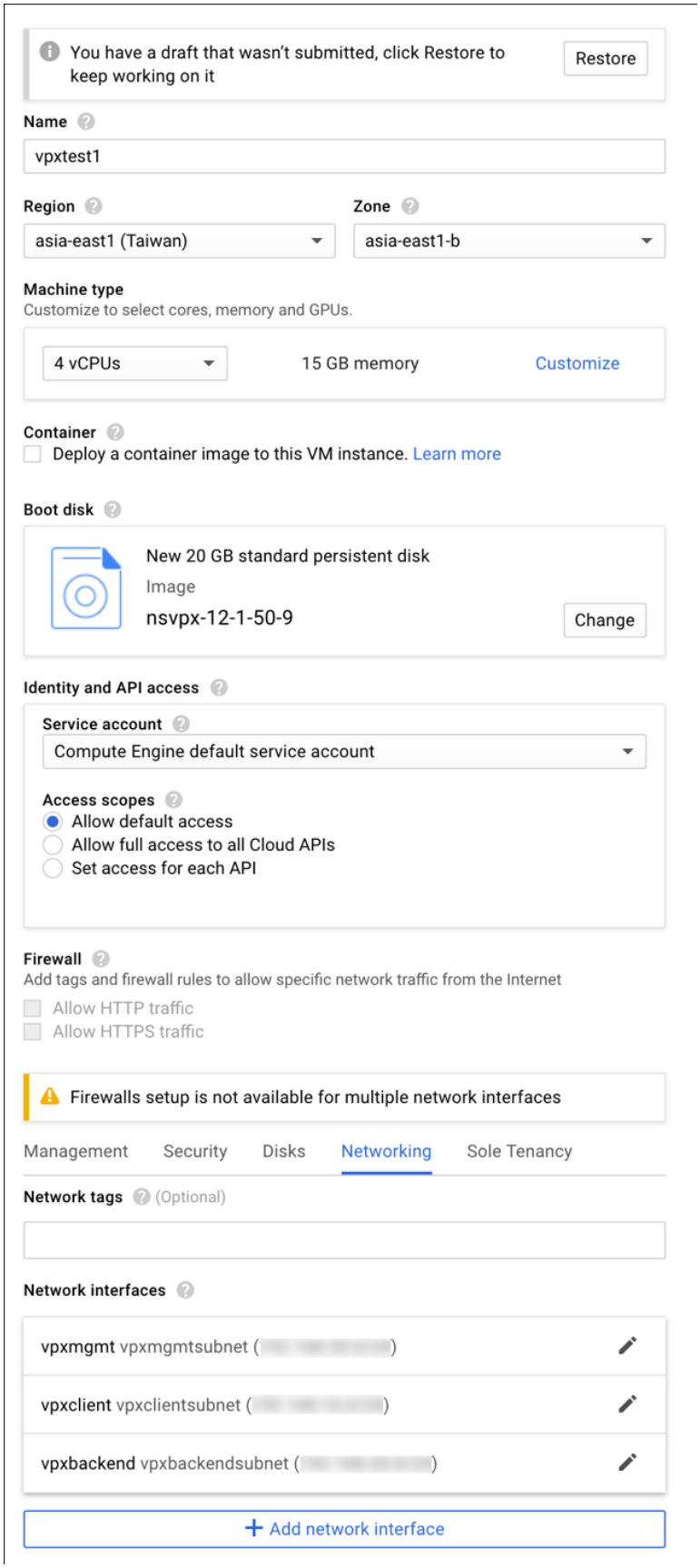
> **Hinweis:**
>
> Das Container-Image wird auf VPX-Instanzen auf GCP nicht unterstützt.



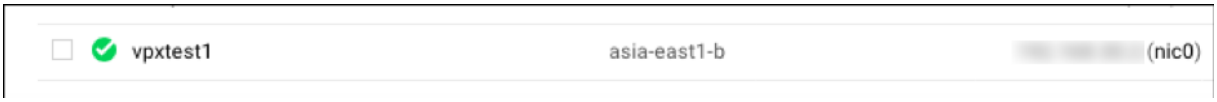
6. Klicken Sie unter **Netzwerkschnittstellen**auf das Bearbeitungssymbol, um die Standard-Netzwerkkarte zu bearbeiten. Diese NIC ist die Verwaltungs-NIC.
7. Wählen Sie im Fenster **Netzwerkschnittstellen** unter **Netzwerk**das VPC-Netzwerk aus, das Sie für die Verwaltungs-NIC erstellt haben.
8. Erstellen Sie für die Verwaltungs-NIC eine statische externe IP-Adresse. Klicken Sie unter der Liste Externe IP auf **IP-Adresse erstellen**.
9. Fügen Sie im Fenster **Neue statische IP-Adresse reservieren einen** Namen und eine Beschreibung hinzu und klicken Sie auf **Reservieren**.
10. Klicken Sie auf **Netzwerkschnittstelle hinzufügen**, um Netzwerkkarten für einen Client- und serverseitigen Datenverkehr zu erstellen.



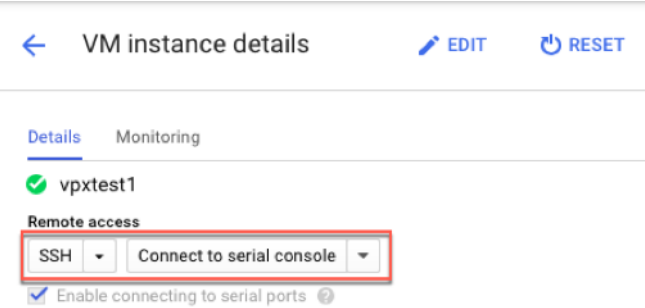
Nachdem Sie alle NICs erstellt haben, klicken Sie auf **Erstellen**, um die VPX-Instanz zu erstellen.



Die Instanz wird unter **VM-Instanzen**angezeigt.

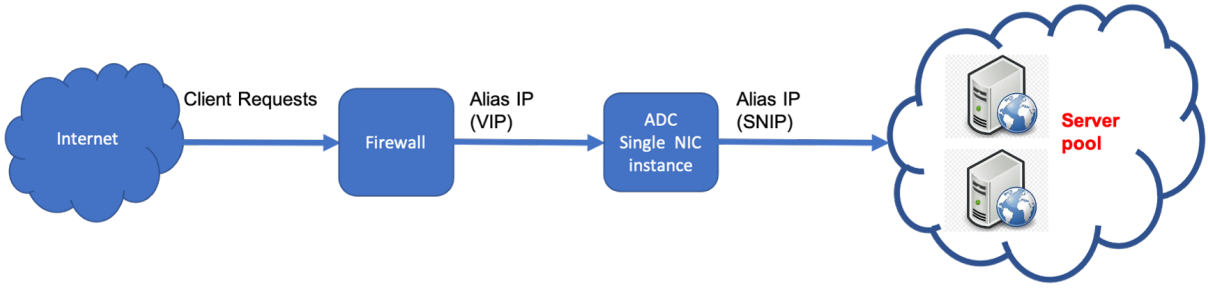


Verwenden Sie die GCP SSH oder die serielle Konsole, um die VPX-Instanz zu konfigurieren und zu verwalten.



Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit einer einzigen NIC

Dieses Szenario zeigt, wie eine eigenständige NetScaler VPX-Instanz mit einer einzigen Netzwerkkarte in GCP bereitgestellt wird. Die Alias-IP-Adressen werden verwendet, um diese Bereitstellung zu erreichen.



Erstellen Sie eine einzelne NIC (NIC0) für folgende Zwecke:

- Behandeln Sie den Verwaltungsdatenverkehr (NetScaler IP) im Verwaltungsnetzwerk.
- Behandeln Sie clientseitigen Datenverkehr (VIP) im Clientnetzwerk.
- Kommunizieren Sie mit Back-End-Servern (SNIP) im Back-End-Server-Netzwerk.

Richten Sie die erforderlichen Kommunikationswege zwischen den folgenden ein:

- Instanz und die Back-End-Server.
- Instanz und die externen Hosts im öffentlichen Internet.

Zusammenfassung der Bereitstellungsschritte

1. Erstellen Sie ein VPC-Netzwerk für NIC0.

2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.
3. Erstellen Sie eine Instanz mit einer einzigen NIC.
4. Fügen Sie Alias-IP-Adressen zu VPX hinzu.
5. Fügen Sie VIP und SNIP auf VPX hinzu.
6. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.
7. Fügen Sie der Instanz einen Dienst oder eine Servicegruppe hinzu.
8. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver der Instanz.

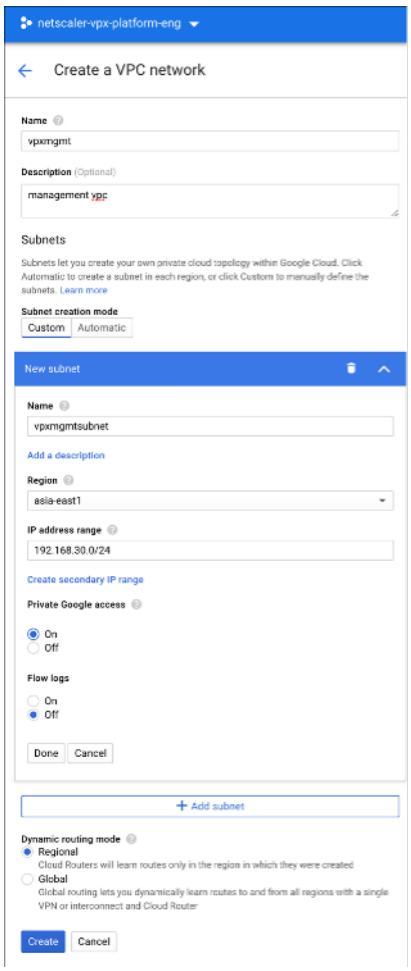
> **Hinweis**:
>
> Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

Schritt 1. Erstellen Sie ein VPC-Netzwerk.

Erstellen Sie ein VPC-Netzwerk, das Sie mit NIC0 verknüpfen möchten.

Gehen Sie folgendermaßen vor, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich bei **GCP Console an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.



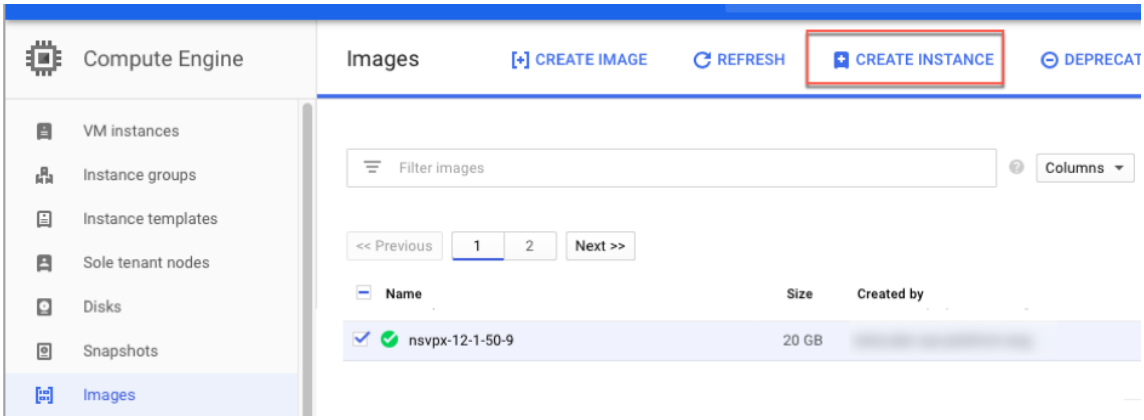
Schritt 2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für das VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Übersicht über Firewall-Regeln.

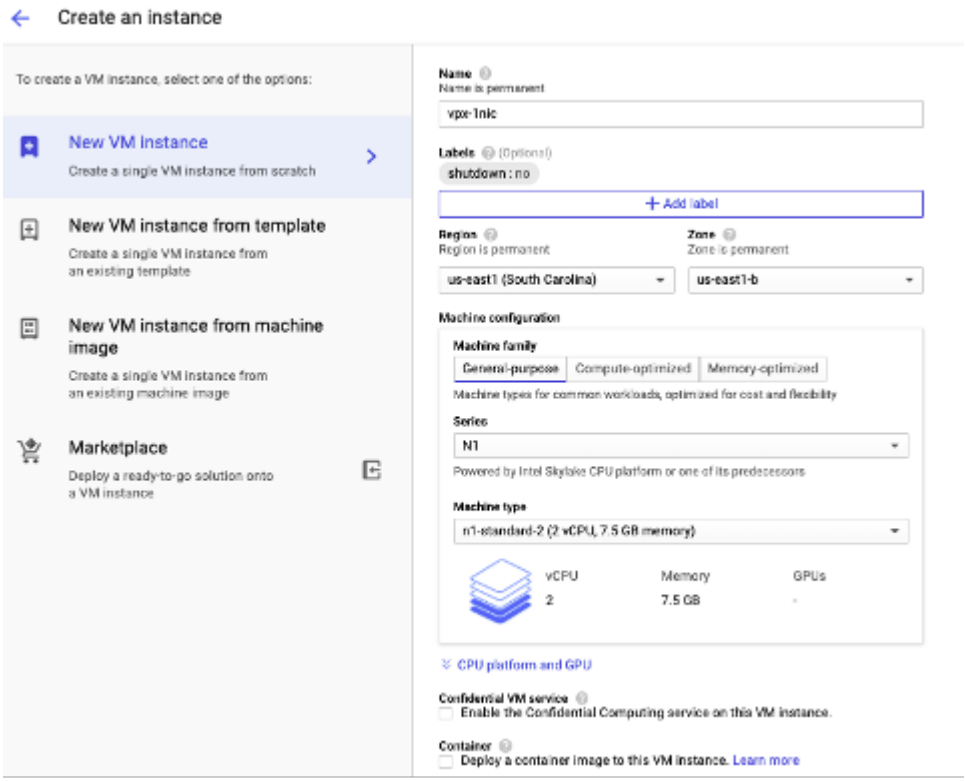
Schritt 3. Erstellen Sie eine Instanz mit einer einzelnen NIC.

Gehen Sie folgendermaßen vor, um eine Instanz mit einer einzelnen NIC zu erstellen:

1. Melden Sie sich bei der **GCP-Konsole** an.
2. Zeigen Sie unter **Compute** mit der Maus auf **Compute Engine** und wählen Sie **Images** aus.
3. Wählen Sie das Image aus und klicken Sie auf **Instanz erstellen**.



4. Wählen Sie einen Instanztyp mit zwei vCPUs aus (Mindestanforderung für ADC).



5. Klicken Sie im Fenster **Verwaltung, Sicherheit, Datenträger, Netzwerk** auf die Registerkarte **Netzwerk**.
6. Klicken Sie unter **Netzwerkschnittstellen** auf das Symbol **Bearbeiten**, um die Standard-Netzwerkkarte zu bearbeiten.
7. Wählen Sie im Fenster **Netzwerkschnittstellen** unter **Netzwerk** das VPC-Netzwerk aus, das Sie erstellt haben.
8. Sie können eine statische externe IP-Adresse erstellen. Klicken Sie unter den **Externen IP-Adressen** auf **IP-Adresse erstellen**.

9. Fügen Sie im Fenster **Statische Adresse reservieren** einen Namen und eine Beschreibung hinzu und klicken Sie auf **Reservieren**.
10. Klicken Sie auf **Erstellen**, um die VPX-Instanz zu erstellen.
    Die neue Instanz wird unter VM-Instanzen angezeigt.

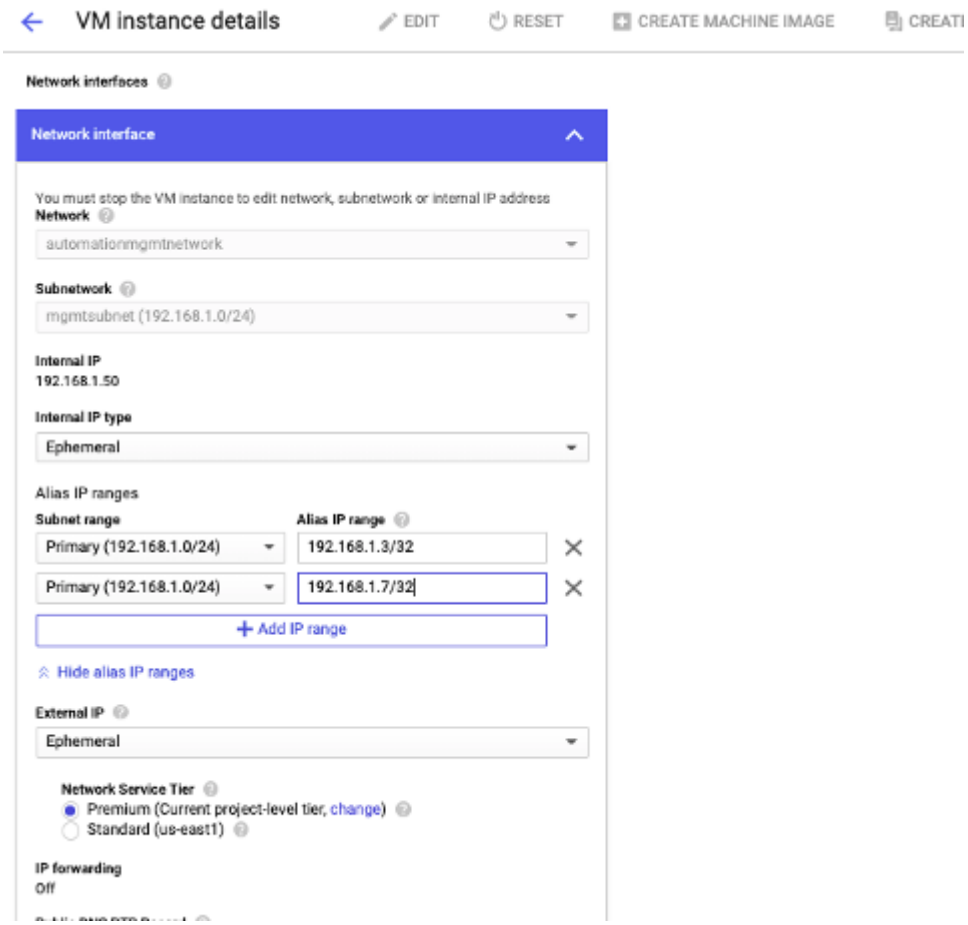
Schritt 4. Fügen Sie der VPX-Instanz Alias-IP-Adressen hinzu.

Weisen Sie der VPX-Instanz zwei Alias-IP-Adressen zu, die als VIP- und SNIP-Adressen verwendet werden sollen.

> **Hinweis:**
>
> Verwenden Sie nicht die primäre interne IP-Adresse der VPX-Instanz, um den VIP oder SNIP zu konfigurieren.

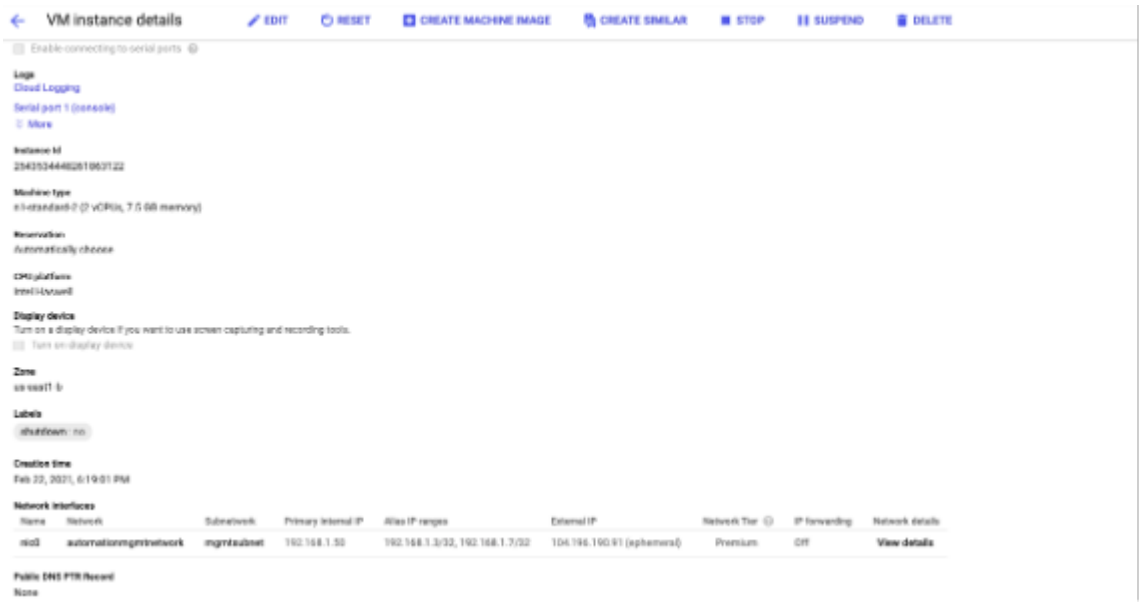
Gehen Sie folgendermaßen vor, um eine Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster der **Netzwerkschnittstelle** die NIC0-Schnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die Alias-IP-Adressen ein.



4. Klicken Sie auf **Fertig**und dann auf **Speichern**.

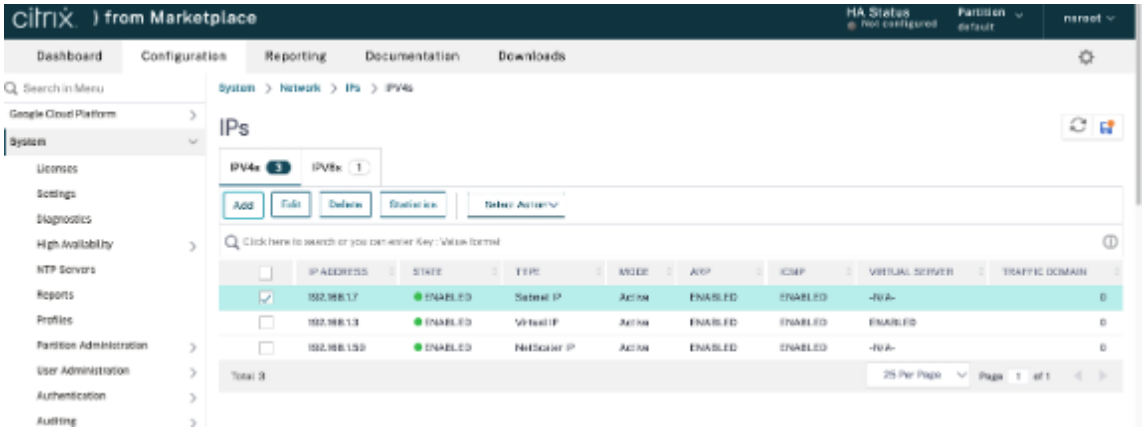
5. Überprüfen Sie die Alias-IP-Adressen auf der **Detailseite der VM-Instanz** .



Schritt 5. Fügen Sie VIP und SNIP in der VPX-Instanz hinzu.

Fügen Sie in der VPX-Instanz die IP-Adresse des Client-Alias und die IP-Adresse des Serveralias hinzu.

1. Navigieren Sie in der NetScaler-GUI zu **System > Netzwerk > IPs > IPv4s**und klicken Sie auf **Hinzufügen**.

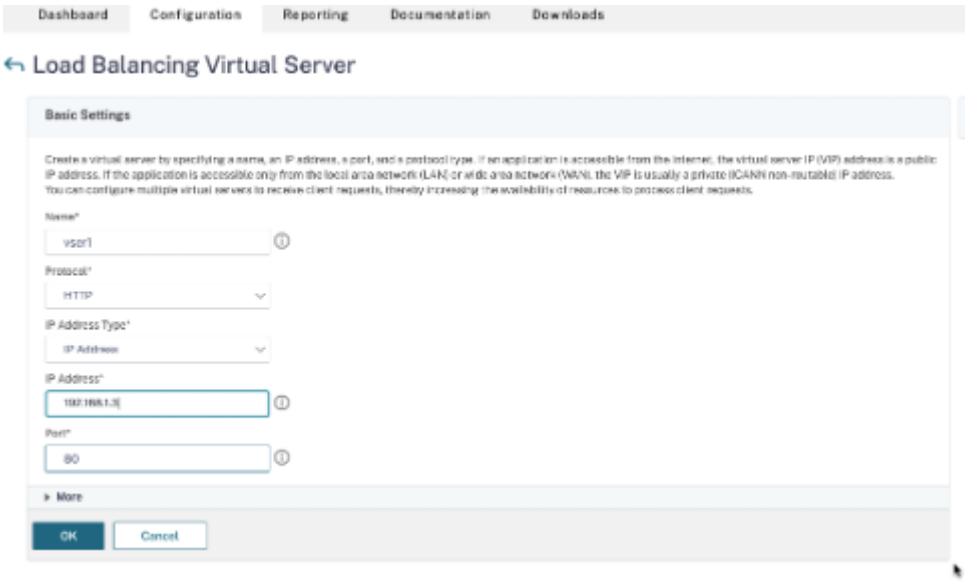


2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   - Geben Sie die Client-Alias-IP-Adresse und Netzmaske ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.
   - Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   - Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine IP-Adresse (SNIP) des Server-Alias:
   - Geben Sie die IP-Adresse und Netzmaske des Server-Alias ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.

- Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
- Klicken Sie auf **Erstellen**.

Schritt 6. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

1. Navigieren Sie in der NetScaler-GUI zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Clientalias-IP) und Port hinzu.
3. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.



Schritt 7. Fügen Sie der VPX-Instanz einen Dienst oder eine Dienstgruppe hinzu.

1. Navigieren Sie in der NetScaler-GUI zu **Konfiguration > Traffic Management > Load Balancing > Services**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu, und klicken Sie auf **OK**.

Schritt 8. Binden Sie die Service/Dienstgruppe an den virtuellen Load Balancing Server in der Instanz.

1. Navigieren Sie in der GUI zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 6**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Fenster **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 7**konfigurierten Dienst aus und klicken Sie auf **Binden**.

Hinweise zu beachten, nachdem Sie die VPX-Instanz auf GCP bereitgestellt haben

- Melden Sie sich beim VPX mit Benutzernamen `nsroot` und Instanz-ID als Kennwort an. Ändern Sie an der Eingabeaufforderung das Kennwort und speichern Sie die Konfiguration.
- Um ein Paket für den technischen Support zu sammeln, führen Sie den Befehl `shell /netscaler/showtech_cloud.pl` anstelle des üblichen `show techsupport` aus.
- Löschen Sie nach dem Löschen einer NetScaler VM von der GCP-Konsole auch die zugehörige interne Zielinstanz von NetScaler. Gehen Sie dazu zur gcloud CLI und geben Sie den folgenden Befehl ein:

```
gcloud compute -q  target-instances delete <instance-name>-
   adcinternal --zone <zone>
<!--NeedCopy-->
```

> **Hinweis:**
>
> `<instance-name>-adcinternal` ist der Name der Zielinstanz, die gelöscht werden muss.

NetScaler VPX-Lizenzierung

Eine NetScaler VPX-Instanz auf GCP benötigt eine Lizenz. Die folgenden Lizenzierungsoptionen sind für NetScaler VPX-Instanzen verfügbar, die auf GCP ausgeführt werden.

- **Abonnementbasierte Lizenzierung**: NetScaler VPX Appliances sind als kostenpflichtige Instanzen auf dem GCP-Marktplatz verfügbar. Abonnementbasierte Lizenzierung ist eine Pay-as-you-go-Option. Benutzer werden stündlich berechnet. Die folgenden VPX-Modelle und Lizenz-Editionen sind auf dem GCP-Marktplatz verfügbar.

VPX-Modell	Lizenz-Editionen
VPX10, VPX200, VPX1000, VPX3000, VPX5000	Standard, Fortgeschritten, Premium

- **Bringen Sie Ihre eigene Lizenz (BYOL) mit:** Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, finden Sie weitere Informationen im VPX-Lizenzierungsleitfaden unter http://support.citrix.com/article/CTX122426. Sie müssen:
  - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
  - Laden Sie die Lizenz auf die Instanz hoch.
- **NetScaler VPX Check-In/Auschecken Lizenzierung**: Weitere Informationen finden Sie unter NetScaler VPX Check-In/Auschecken Lizenzierung.

VPX Express für lokale und Cloud-Bereitstellungen erfordert keine Lizenzdatei. Weitere Informationen zu NetScaler VPX Express finden Sie im Abschnitt “NetScaler VPX Express-Lizenz” in der Übersicht über die NetScaler Lizenzierung.

GDM-Vorlagen zur Bereitstellung einer NetScaler VPX-Instanz

Sie können eine NetScaler VPX Google Deployment Manager (GDM) -Vorlage verwenden, um eine VPX-Instanz auf GCP bereitzustellen. Weitere Informationen finden Sie unter NetScaler GDM Templates.

NetScaler Marketplace-Images

Sie können die Images in GDM-Vorlagen verwenden, um die NetScaler-Appliance aufzurufen.

In der folgenden Tabelle sind die Images aufgeführt, die auf dem GCP Marketplace verfügbar sind.

Release	Imagename	Imageort
13.0	citrix-adc-vpx-10-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-0-83-29
13.0	citrix-adc-vpx-10-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-0-83-29
13.0	citrix-adc-vpx-10-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-standard-13-0-83-29
13.0	citrix-adc-vpx-200-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-0-83-29
13.0	citrix-adc-vpx-200-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-0-83-29

Release	Imagename	Imageort
13.0	citrix-adc-vpx-200-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-0-83-29
13.0	citrix-adc-vpx-1000-advanced-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-0-83-29
13.0	citrix-adc-vpx-1000-premium-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-0-83-29
13.0	citrix-adc-vpx-1000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-0-83-29
13.0	citrix-adc-vpx-3000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-3000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-0-83-29
13.0	citrix-adc-vpx-3000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-0-83-29
13.0	citrix-adc-vpx-5000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-5000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-0-83-29

Release	Imagename	Imageort
13.0	citrix-adc-vpx-5000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-0-83-29
13.0	citrix-adc-vpx-byol-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-0-83-29
13.0	citrix-adc-vpx-express-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-0-83-29
13.0	citrix-adc-vpx-waf-1000-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-waf-1000-13-0-83-29
13.1	citrix-adc-vpx-10-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-1-9-60
13.1	citrix-adc-vpx-10-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-1-9-60
13.1	citrix-adc-vpx-10-standard-13-1-9-60	projects/citrix-master-project/global/imagescitrix-adc-vpx-10-standard-13-1-9-60
13.1	citrix-adc-vpx-200-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-1-9-60
13.1	citrix-adc-vpx-200-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-1-9-60

Release	Imagename	Imageort
13.1	citrix-adc-vpx-200-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-1-9-60
13.1	citrix-adc-vpx-1000-advanced-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-1-9-60
13.1	citrix-adc-vpx-1000-premium-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-1-9-60
13.1	citrix-adc-vpx-1000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-1-9-60
13.1	citrix-adc-vpx-3000-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-1-9-60
13.1	citrix-adc-vpx-3000-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-1-9-60
13.1	citrix-adc-vpx-3000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-1-9-60
13.1	citrix-adc-vpx-5000-enterprise-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-1-9-60
13.1	citrix-adc-vpx-5000-platinum-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-1-9-60

Release	Imagename	Imageort
13.1	citrix-adc-vpx-5000-standard-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-1-9-60
13.1	citrix-adc-vpx-byol-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-1-9-60
13.1	citrix-adc-vpx-express-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-1-9-60
13.1	citrix-adc-vpx-waf-1000-13-1-9-60	projects/citrix-master-project/global/images/citrix-adc-vpx-waf-1000-13-1-9-60

Ressourcen

- Erstellen von Instanzen mit mehreren Netzwerkschnittstellen
- Erstellen und Starten einer VM-Instanz

Verwandte Informationen

- VPX-Hochverfügbarkeitspaars auf der Google Cloud Platform bereitstellen

VPX-Hochverfügbarkeitspaars auf der Google Cloud Platform bereitstellen

May 11, 2023

Sie können zwei NetScaler VPX-Instanzen auf der Google Cloud Platform (GCP) als aktives und passives Paar mit hoher Verfügbarkeit (HA) konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären Knoten. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Die Knoten müssen sich in derselben Region befinden; sie können sich jedoch entweder in derselben Zone oder in verschiedenen Zonen befinden. Weitere Informationen finden Sie unter Regionen und Zonen.

Jede VPX-Instanz benötigt mindestens drei IP-Subnetze (Google VPC-Netzwerke):

- Ein Management-Subnetz
- Ein Client-Subnetz (VIP)
- Ein Subnetz mit Back-End-Ausrichtung (SNIP, MIP usw.)

Citrix empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz.

Sie können ein VPX-Hochverfügbarkeitspaar mit den folgenden Methoden bereitstellen:

- Verwendung einer externen statischen IP-Adresse
- Verwendung einer privaten IP-Adresse
- Verwendung von Single-NIC-VMs mit privater IP-Adresse

GDM-Vorlagen zur Bereitstellung eines VPX-Hochverfügbarkeitspaars auf GCP

Sie können eine NetScaler Google Deployment Manager (GDM) -Vorlage verwenden, um ein VPX-Hochverfügbarkeitspaar auf GCP bereitzustellen. Weitere Informationen finden Sie unter NetScaler GDM Templates.

Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP

Sie können ein VPX Hochverfügbarkeitspaar auf dem GCP mithilfe von Weiterleitungsregeln bereitstellen.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

Voraussetzungen

- Die Weiterleitungsregeln müssen sich in derselben Region wie die VPX-Instanzen befinden.
- Zielinstanzen müssen sich in derselben Zone wie die VPX-Instanz befinden.
- Die Anzahl der Zielinstanzen für den primären und den sekundären Knoten muss übereinstimmen.

Beispiel:

Sie haben ein Hochverfügbarkeitspaar in der Region `us-east1` mit primärem VPX in der Zone `us-east1-b` und sekundärem VPX in der Zone `us-east1-c`. Eine Weiterleitungsregel wird für die primäre VPX mit der Zielinstanz in der Zone `us-east1-b` konfiguriert. Konfigurieren Sie eine Zielinstanz für sekundäres VPX in der Zone `us-east1-c`, um die Weiterleitungsregel bei einem Failover zu aktualisieren.

Einschränkungen

Bei der VPX-Bereitstellung mit hoher Verfügbarkeit werden nur Weiterleitungsregeln unterstützt, die mit Zielinstanzen im Backend konfiguriert sind.

Stellen Sie ein VPX-Hochverfügbarkeitspaar mit externer statischer IP-Adresse auf der Google Cloud Platform bereit

May 11, 2023

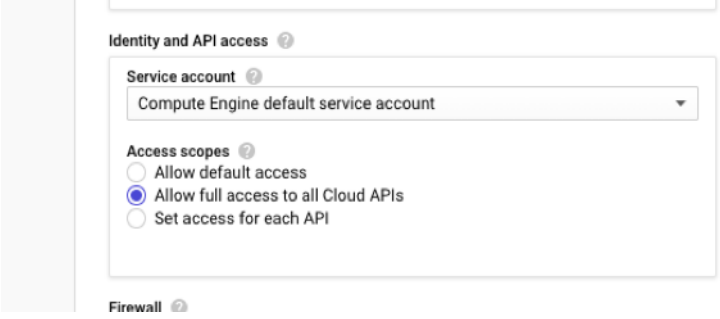
Sie können ein VPX-Paar mit hoher Verfügbarkeit auf GCP mit einer externen statischen IP-Adresse bereitstellen. Die Client-IP-Adresse des primären Knotens muss an eine externe statische IP-Adresse gebunden sein. Beim Failover wird die externe statische IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann.

Eine statische externe IP-Adresse ist eine externe IP-Adresse, die für Ihr Projekt reserviert ist, bis Sie sich entscheiden, sie freizugeben. Wenn Sie eine IP-Adresse für den Zugriff auf einen Dienst verwenden, können Sie diese IP-Adresse so reservieren, dass nur Ihr Projekt sie verwenden kann. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Vorbereitung

- Lesen Sie die Beschränkung, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platformerwähnt werden. Diese Informationen gelten auch für HA-Bereitstellungen.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



- Stellen Sie sicher, dass die mit Ihrem GCP-Dienstkonto verknüpfte IAM-Rolle die folgenden IAM-Berechtigungen besitzt:


```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.instances.get",
"Compute.instances.list",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
<!--NeedCopy-->
```

- Wenn Sie Alias-IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden zusätzlichen IAM-Berechtigungen verfügt:

```
"compute.instances.updateNetworkInterface"
<!--NeedCopy-->
```

- Wenn Sie GCP-Weiterleitungsregeln für den primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP aufgeführt sind, um sie beim Failover auf neue primäre Daten zu aktualisieren.

So stellen Sie ein VPX HA-Paar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der HA-Bereitstellungsschritte:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder in verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie HA-Einstellungen auf beiden Instanzen über die NetScaler GUI- oder ADC-CLI-Befehle.

Schritt 1. Erstellen von VPC-Netzwerken

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix empfiehlt Ihnen, drei VPC-Netzwerke für die Verknüpfung mit Verwaltungs-NIC, Client-NIC und Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

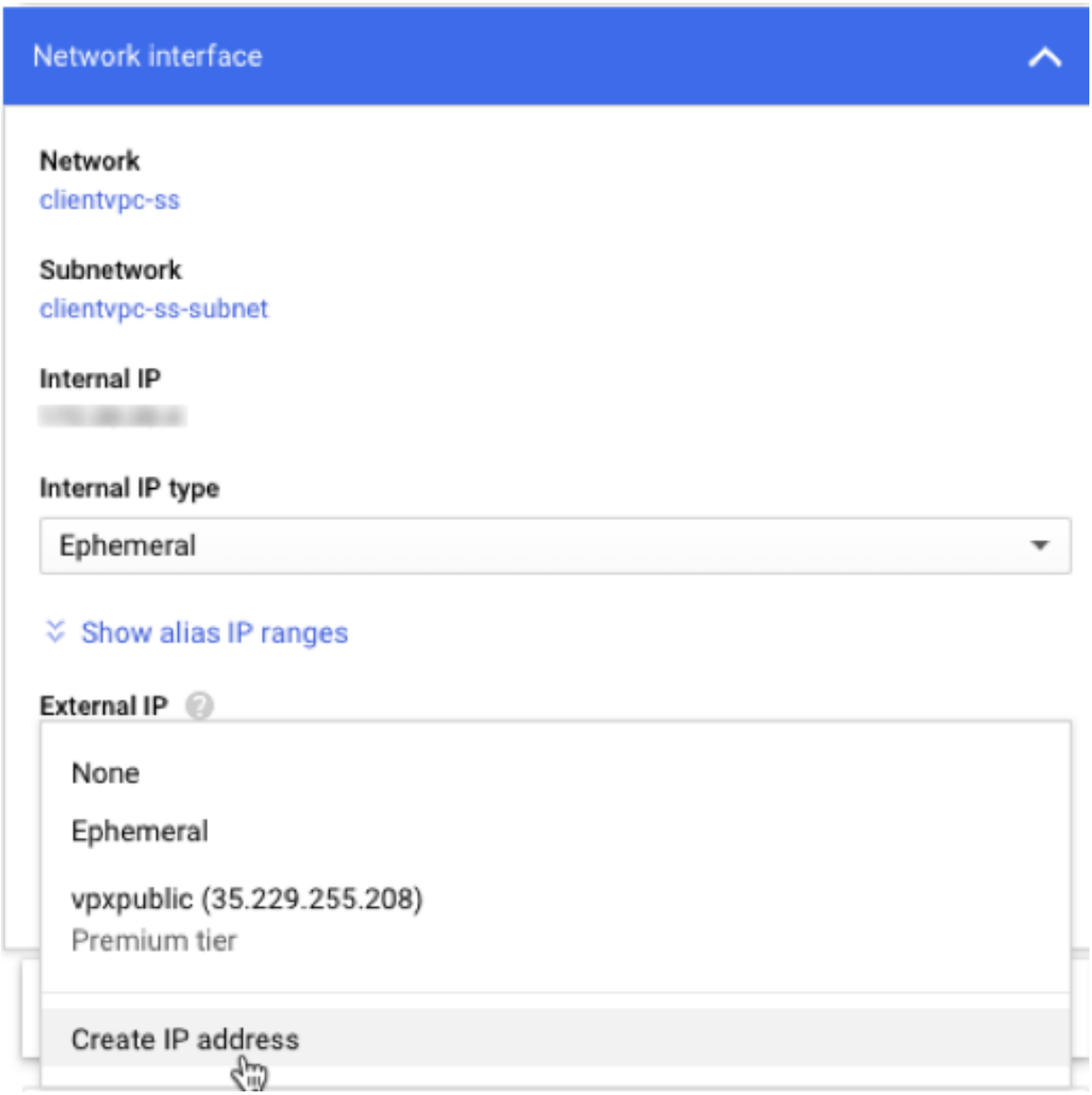
1. Melden Sie sich auf der **Google-Konsole an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **Erstellen von VPC-Netzwerken** unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platform.

Schritt 2. Erstellen Sie zwei VPX-Instanzen

Erstellen Sie zwei VPX-Instanzen, indem Sie die in Szenario angegebenen Schritte ausführen: Stellen Sie eine eigenständige VPX-Instanz mit mehreren NIC, Multi-IPbereit.

> **Wichtig**
>
> Weisen Sie der Client-IP-Adresse (VIP) des primären Knotens eine statische externe IP-Adresse zu. Sie können eine vorhandene reservierte IP-Adresse verwenden oder eine neue erstellen. Um eine statische externe IP-Adresse zu erstellen, navigieren Sie zu **Netzwerkschnittstelle > Externe IP**und klicken Sie auf **IP-Adresse erstellen**.



Wenn nach dem Failover der alte primäre neue sekundäre wird, wird die statische externe IP-Adresse von der alten primären IP-Adresse verschoben und an den neuen primären Server angeschlossen. Weitere Informationen finden Sie im Google Cloud-Dokument Reservieren einer statischen externen IP-Adresse.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die VIP- und SNIP-Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie HA über die NetScaler GUI für CLI konfigurieren.

Konfigurieren von HA mit der GUI

Schritt 1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

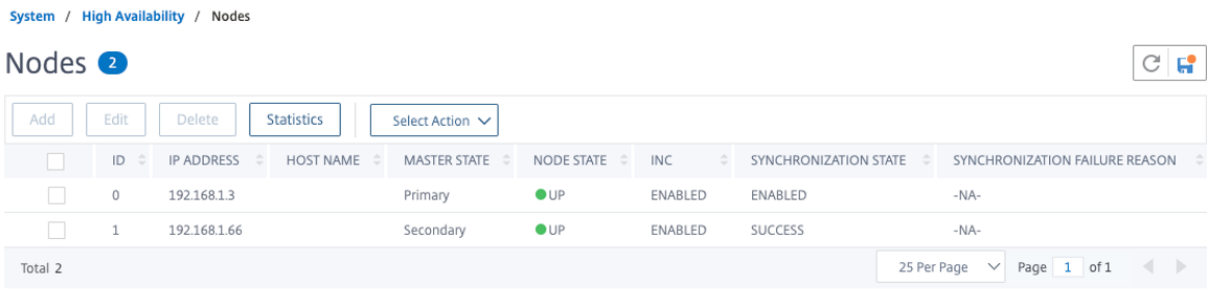
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

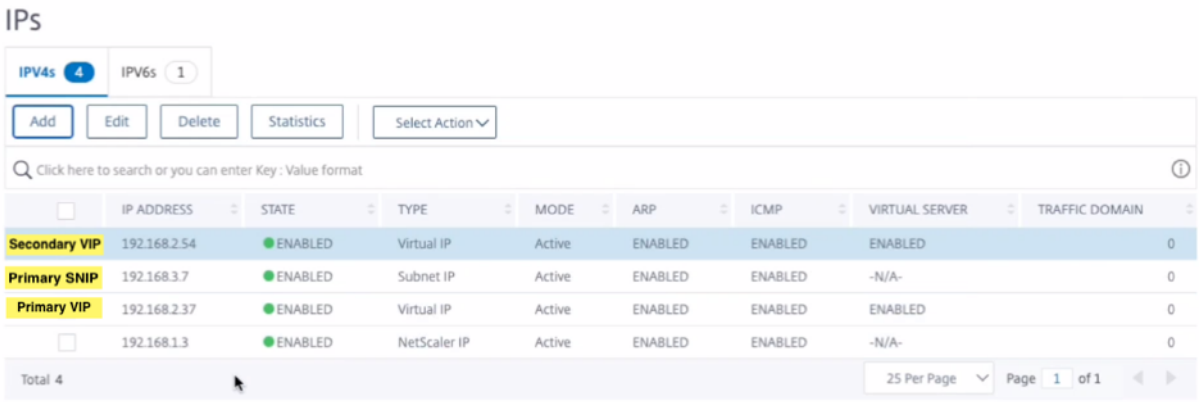


> **Hinweis**
>
> Jetzt hat der sekundäre Knoten die gleichen Anmeldeinformationen wie der primäre Knoten.

Schritt 2. Fügen Sie auf beiden Knoten virtuelle IP-Adresse und Subnet-IP-Adresse hinzu.

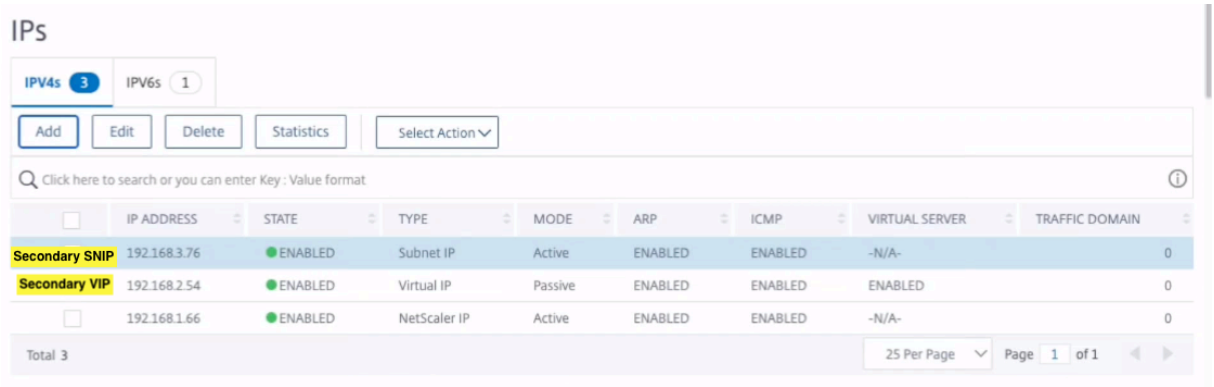
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine primäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der primären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. Fügen Sie eine primäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz und Netzmaske ein, die für das Serversubnetz in der primären Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
4. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

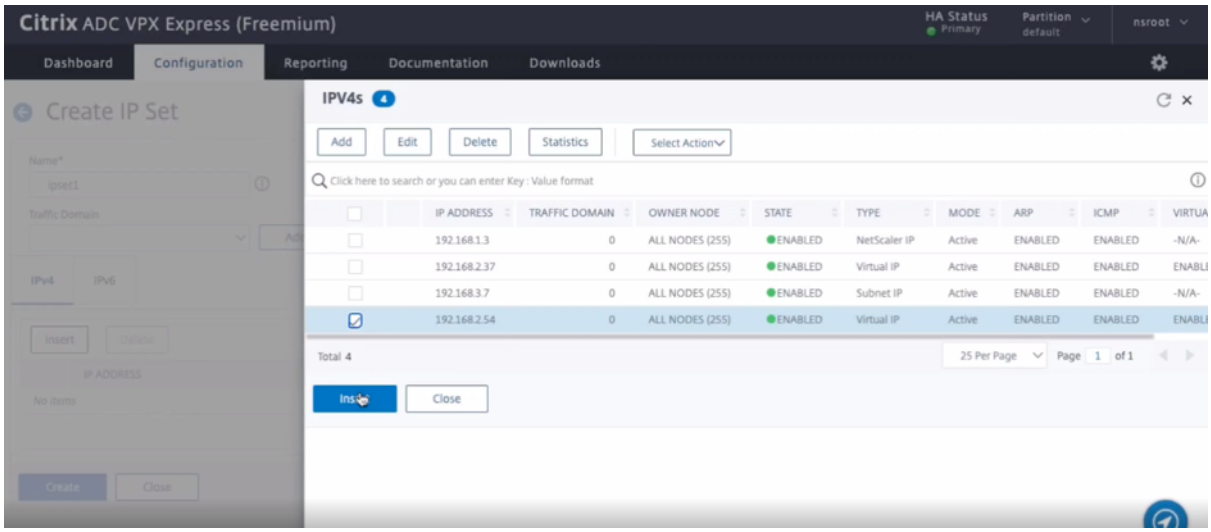
1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
3. Fügen Sie eine sekundäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Serversubnetz in der sekundären Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie IP-Set hinzu und binden Sie die IP, die an den sekundären VIP auf beiden Instanzen festgelegt ist.

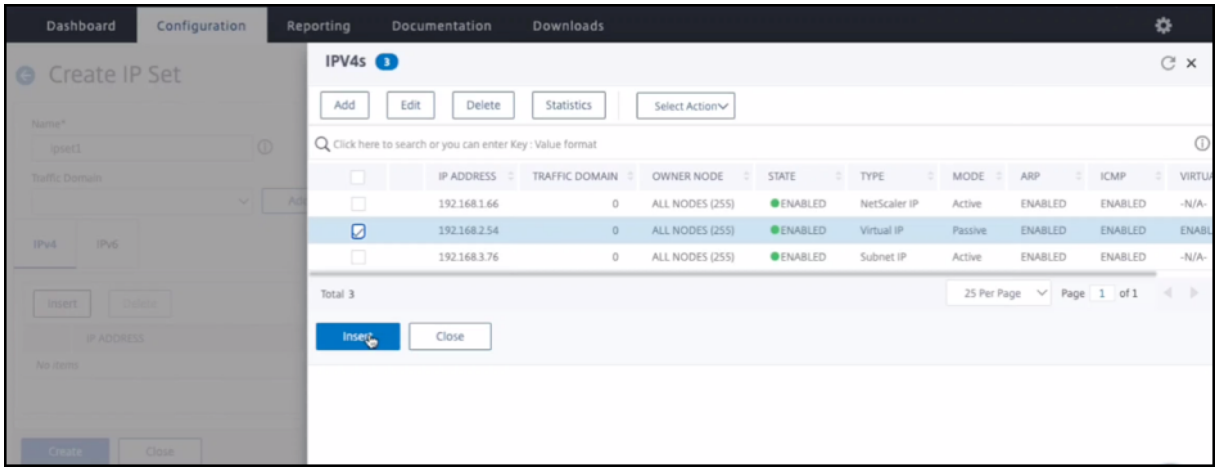
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

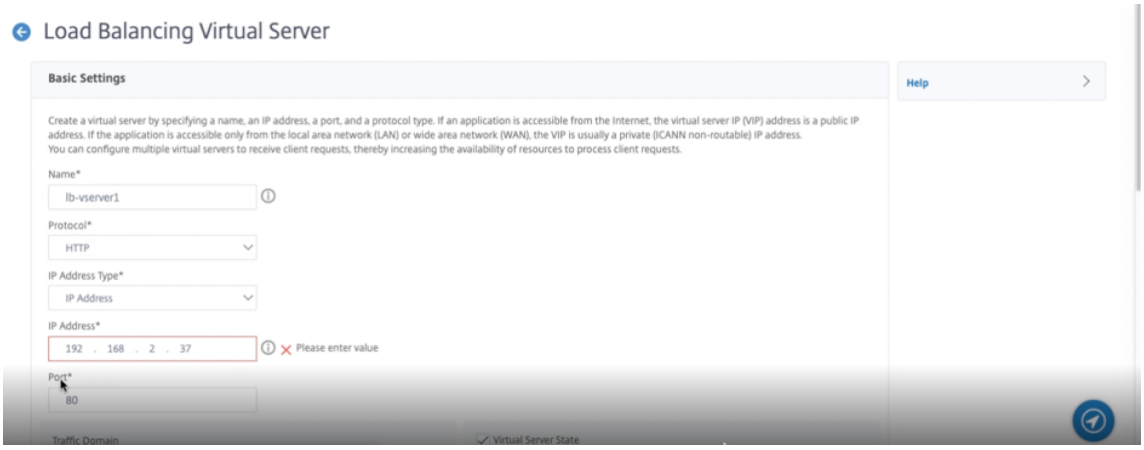
1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



> **Hinweis**
>
> Der Name des IP-Sets muss auf beiden Instanzen identisch sein.

Schritt 4. Fügen Sie der primären Instanz einen virtuellen Lastausgleichsserver hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäres VIP) und Port hinzu.



3. Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen**, wählen Sie im Dropdownmenü **IPset** aus und geben Sie das in **Schritt 3** erstellte IPset ein.
4. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.

Schritt 5. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 6. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 4**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 5**konfigurierten Dienst aus und klicken Sie auf " **Binden**".

Speichern Sie die Konfiguration. Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die externe statische IP des alten primären VIP wechselt zum neuen sekundären VIP.

Konfigurieren Sie Hochverfügbarkeit mithilfe von CLI

Schritt 1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

`sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

`prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Schritt 2. Fügen Sie auf beiden Knoten virtuelle und Subnet-IPs hinzu.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <primary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

`primary_vip` bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der primären Instanz.

`secondary_vip` bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz.

`primary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz.

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ns ip <secondary_vip> <subnet> -type VIP

add ns ip <secondary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

`secondary_vip` bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz.

`secondary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz.

Schritt 3. Fügen Sie IP-Set hinzu und binden Sie IP, die auf beiden Instanzen an sekundären VIP eingestellt ist.

Geben Sie auf dem primären Knoten den folgenden Befehl ein:

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
<!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

```
add ipset <ipsetname>
bind ipset <ipsetname> <secondary VIP>
<!--NeedCopy-->
```

> **Hinweis**
>
> Der Name des IP-Sets muss auf beiden Instanzen identisch sein.

Schritt 4. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
    > -ipset <ipset_name>
<!--NeedCopy-->
```

Schritt 5. Fügen Sie der primären Instanz einen Dienst oder eine Servicegruppe hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```


Schritt 6. Binden Sie die Service/Dienstgruppe an den virtuellen Lastenausgleichsserver auf der primären Instanz.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> *Hinweis*:
>
> Um Ihre Konfiguration zu speichern, geben Sie den Befehl ein `save config`. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

Schritt 7. Überprüfen Sie die Konfiguration.

Stellen Sie sicher, dass die an die primäre Client-NIC angehängte externe IP-Adresse bei einem Failover zur sekundären IP-Adresse wechselt.

1. Stellen Sie eine cURL-Anfrage an die externe IP-Adresse und stellen Sie sicher, dass sie erreichbar ist.
2. Führen Sie auf der primären Instanz Failover durch:

   Navigieren Sie in der GUI zu **Konfiguration > System > Hochverfügbarkeit > Aktion > Failover erzwingen**.

   Geben Sie in der CLI den folgenden Befehl ein:

   ```
   force ha failover -f
   <!--NeedCopy-->
   ```

   Navigieren Sie auf der GCP-Konsole zur sekundären Instanz. Die externe IP-Adresse muss nach dem Failover auf die sekundäre Client-NIC verschoben worden sein.
3. Stellen Sie eine cURL-Anforderung an die externe IP aus und stellen Sie sicher, dass sie wieder erreichbar ist.

Einzelnes NIC-VPX-Hochverfügbarkeitspaar mit privater IP-Adresse auf der Google Cloud Platform bereitstellen

May 11, 2023

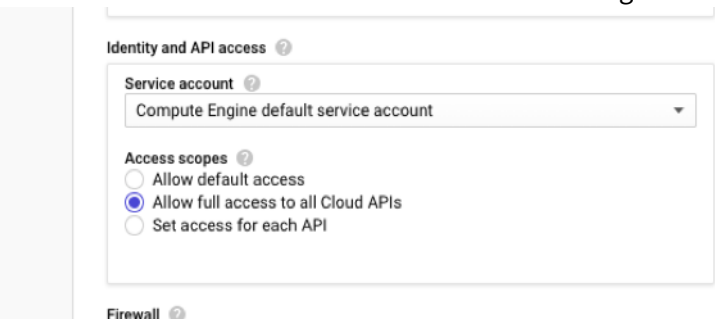
Sie können ein einzelnes NIC-VPX-Hochverfügbarkeitspaar auf GCP mithilfe einer privaten IP-Adresse bereitstellen. Die Client-IP-Adresse (VIP) muss als Alias-IP-Adresse auf dem Primärknoten konfiguriert werden. Beim Failover wird die Client-IP-Adresse auf den sekundären Knoten verschoben, damit der

Datenverkehr wieder aufgenommen werden kann. Die Subnetz-IP-Adressen (SNiPs) für jeden Knoten müssen ebenfalls als Alias-IP-Bereich konfiguriert werden.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

Vorbereitung

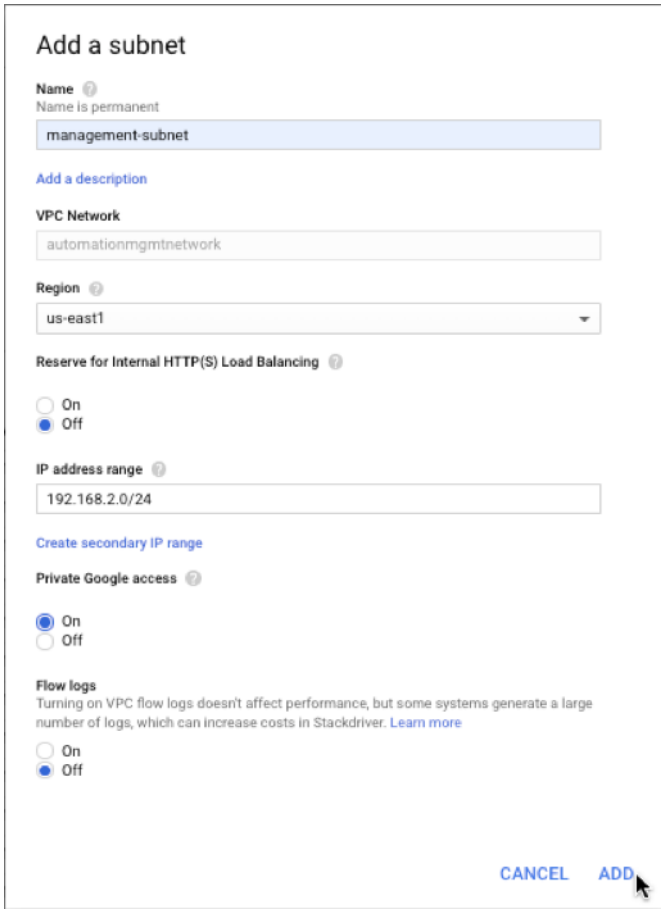
- Lesen Sie die Beschränkung, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platformerwähnt werden. Diese Informationen gelten auch für Bereitstellungen mit hoher Verfügbarkeit.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
<!--NeedCopy-->
```

- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie **Private Google Access** im VPC-Subnetz aktivieren.



- Wenn Sie GCP-Weiterleitungsregeln für den primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP aufgeführt sind, um sie beim Failover auf neue primäre Daten zu aktualisieren.

So stellen Sie ein VPX Hochverfügbarkeitspaar auf der Google Cloud Platform bereit

Hier finden Sie eine Zusammenfassung der Schritte zur Bereitstellung eines HA-Paars mit einer einzelnen Netzwerkkarte:

1. Erstellen Sie ein VPC-Netzwerk.
2. Erstellen Sie zwei VPX-Instanzen (primärer und sekundärer Knoten) in derselben Region. Sie können sich in derselben Zone oder in verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie HA-Einstellungen auf beiden Instanzen über die NetScaler GUI- oder ADC-CLI-Befehle.

Schritt 1. Erstellen Sie ein VPC-Netzwerk

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich an der **Google-Konsole an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **Erstellen von VPC-Netzwerken** unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platform.

Schritt 2. Erstellen Sie zwei VPX-Instanzen

Erstellen Sie zwei VPX-Instanzen, indem Sie den Schritten 1 bis 3 unter Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit einer einzelnen Netzwerkkarte folgen.

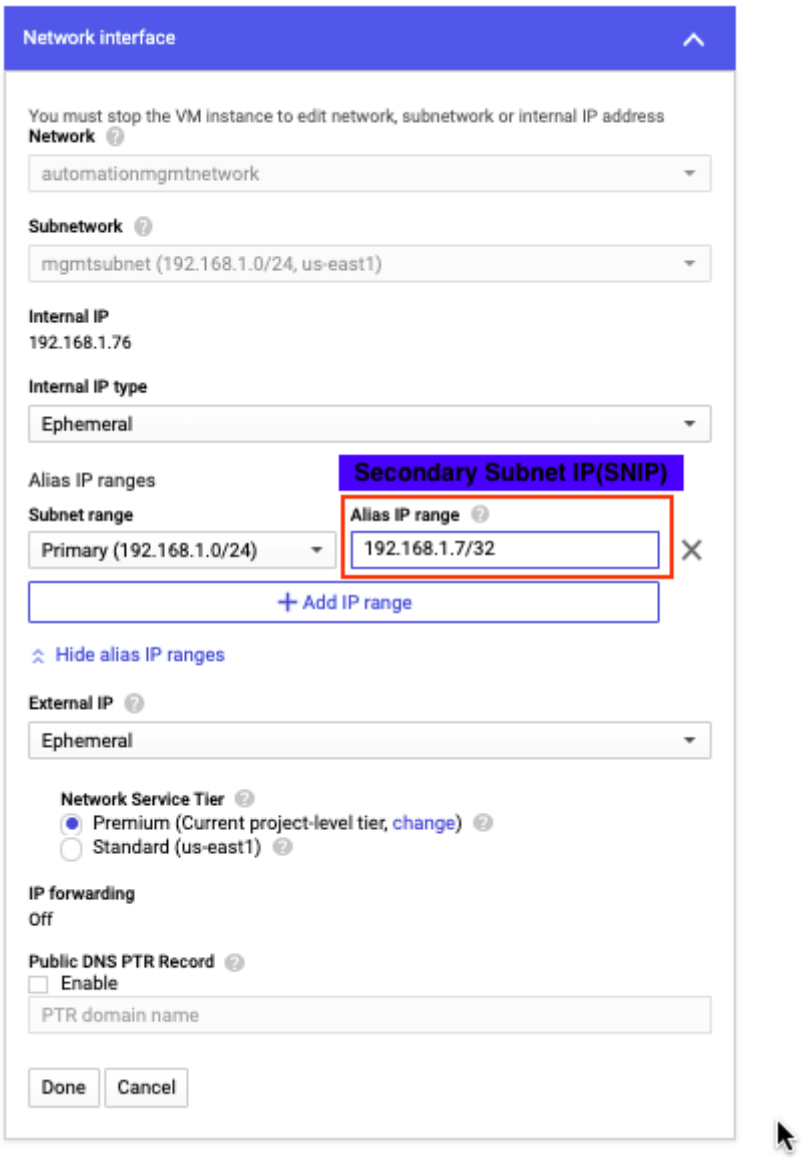
> **Wichtig:**
>
> Weisen Sie nur dem primären Knoten eine Client-Alias-IP-Adresse und primären und sekundären Knoten Server-Alias-IP-Adressen zu. Verwenden Sie nicht die interne IP-Adresse der VPX-Instanz, um VIP oder SNIP zu konfigurieren.

Gehen Sie auf dem primären Knoten wie folgt vor, um Client- und Server-Alias-IP-Adressen zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Client-Schnittstelle (NIC0).
3. Geben Sie im Feld **Alias-IP-Bereich** die IP-Adresse des Client-Alias ein.
4. Klicken Sie auf **IP-Bereich hinzufügen** und geben Sie die Server-Alias-IP-Adresse ein.

Gehen Sie auf dem sekundären Knoten wie folgt vor, um eine Serveralias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Client-Schnittstelle (NIC0).
3. Geben Sie im Feld **Alias-IP-Bereich** die Serveralias-IP-Adresse ein.



Nach dem Failover, wenn der alte primäre zum neuen sekundären wird, wird die Client-Alias-IP-Adresse vom alten primären verschoben und an den neuen primären angehängt.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die Virtual (VIP) und Subnet IP (SNIP) -Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie die Hochverfügbarkeit über die NetScaler-GUI oder CLI konfigurieren.

Konfigurieren der Hochverfügbarkeit mit der GUI

Schritt 1. Richten Sie die Hochverfügbarkeit im Modus INC Enabled auf beiden Knoten ein.

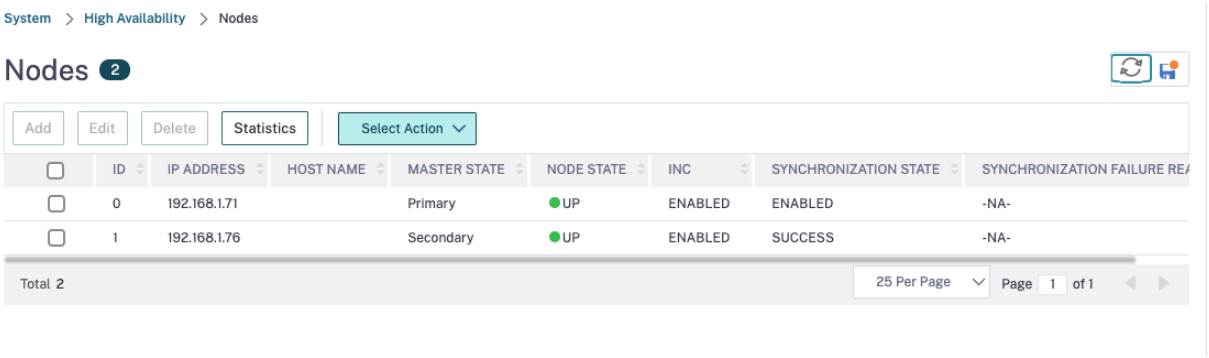
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

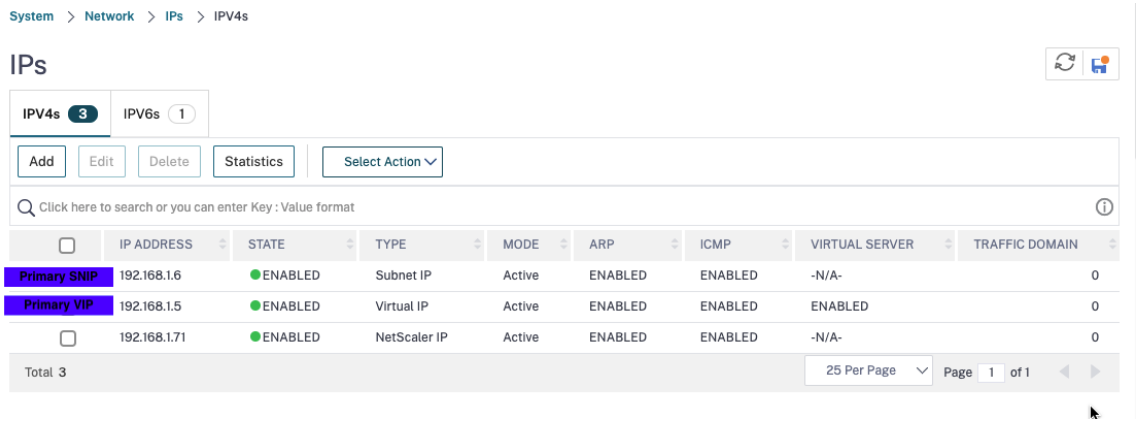


> **Hinweis:**
>
> Nachdem der sekundäre Knoten mit dem primären Knoten synchronisiert wurde, hat der sekundäre Knoten dieselben Anmeldeinformationen wie der primäre Knoten.

Schritt 2. Fügen Sie auf beiden Knoten virtuelle IP-Adresse und Subnet-IP-Adresse hinzu.

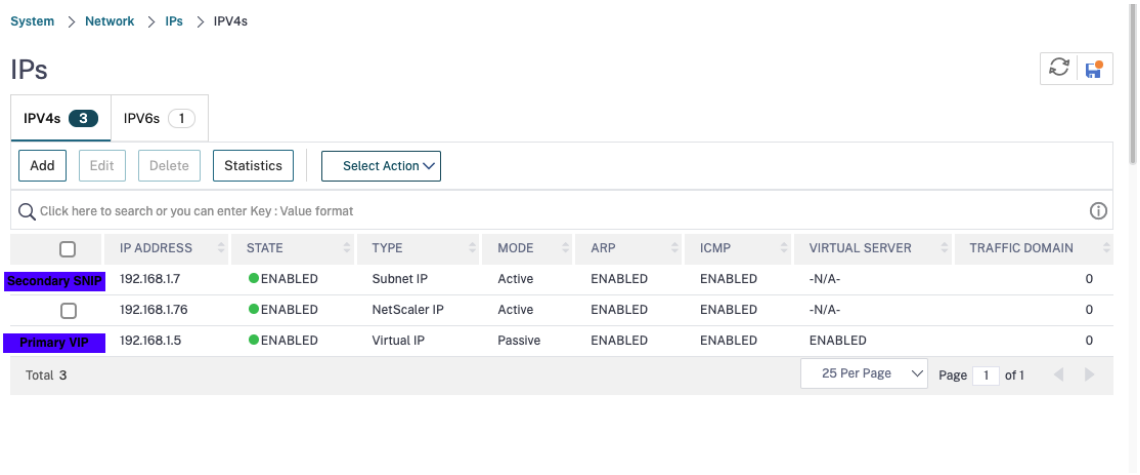
Führen Sie auf dem primären Knotendie folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Client-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine IP-Adresse (SNIP) des Server-Alias:
   a) Geben Sie die Serveralias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



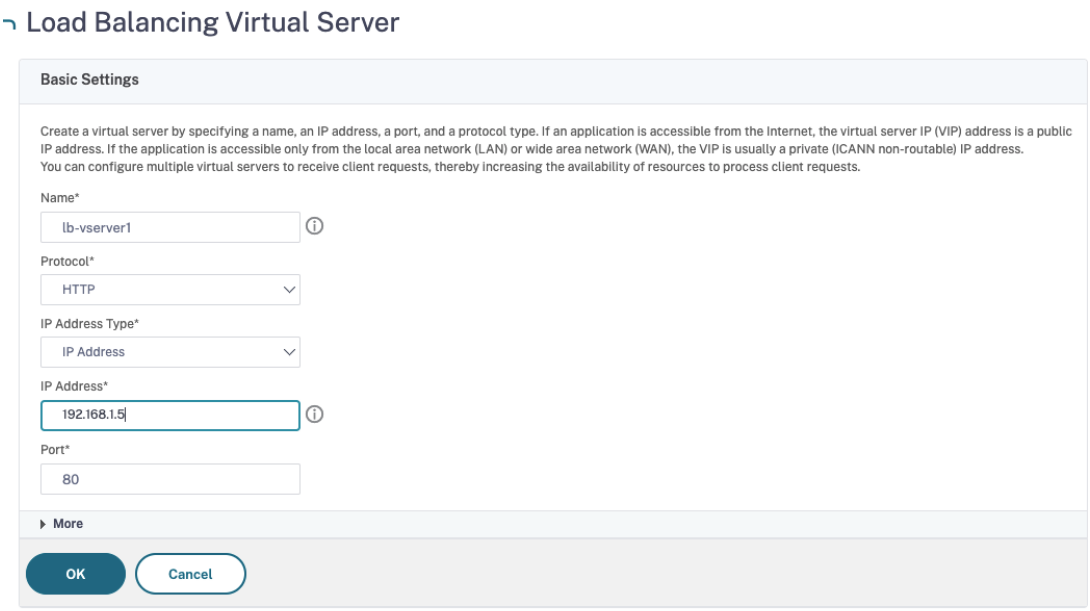
Führen Sie auf dem sekundären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Client-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine IP-Adresse (SNIP) des Server-Alias:
   a) Geben Sie die Serveralias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz der sekundären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie einen virtuellen Lastausgleichsserver auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre Clientalias-IP-Adresse) und Port hinzu, und klicken Sie auf **OK**.



Schritt 4. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 5. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf

dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 3**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 4**konfigurierten Dienst aus und klicken Sie auf " **Binden**".

Schritt 6. Speichern Sie die Konfiguration.

Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die Client-Alias-IP (VIP) vom alten Primärknoten wird auf den neuen Primärknoten verschoben.

Konfigurieren Sie Hochverfügbarkeit über die CLI

Schritt 1. Richten Sie in beiden Instanzen die Hochverfügbarkeit im **INC-aktivierten** Modus mithilfe der NetScaler CLI ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

Der `sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

Der `prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Schritt 2. Fügen Sie VIP und SNIP sowohl auf dem primären als auch auf dem sekundären Knoten hinzu.

Geben Sie die folgenden Befehle auf den primären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP

<!--NeedCopy-->
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.


```
add ns ip <primary_server_alias_ip> <subnet> -type SNIP
<!--NeedCopy-->
```

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
<!--NeedCopy-->
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

```
add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
<!--NeedCopy-->
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Serversubnetz in der VM-Instanz konfiguriert sind.

Schritt 3. Fügen Sie einen virtuellen Server auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
<!--NeedCopy-->
```

Schritt 4. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Schritt 5. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```


> **Hinweis:**
>
> Um Ihre Konfiguration zu speichern, geben Sie den Befehl ein `save config`. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

Stellen Sie ein VPX-Hochverfügbarkeitspaar mit privater IP-Adresse auf der Google Cloud Platform bereit

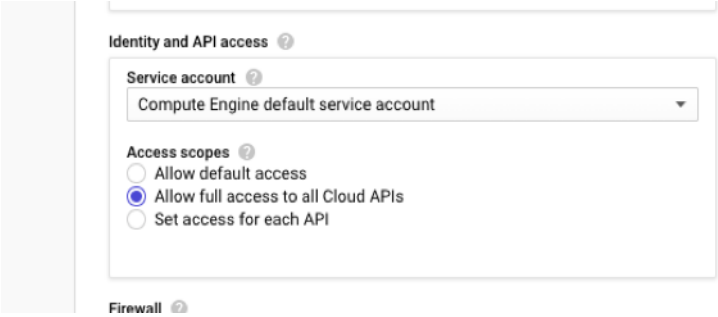
May 11, 2023

Sie können ein VPX-Hochverfügbarkeitspaar auf GCP mithilfe einer privaten IP-Adresse bereitstellen. Die Client-IP (VIP) muss als Alias-IP-Adresse auf dem primären Knoten konfiguriert sein. Beim Failover wird die Client-IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

Vorbereitung

- Lesen Sie die Beschränkung, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platformerwähnt werden. Diese Informationen gelten auch für Bereitstellungen mit hoher Verfügbarkeit.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.setMetadata",
"compute.instances.get",
"compute.instances.list",
```

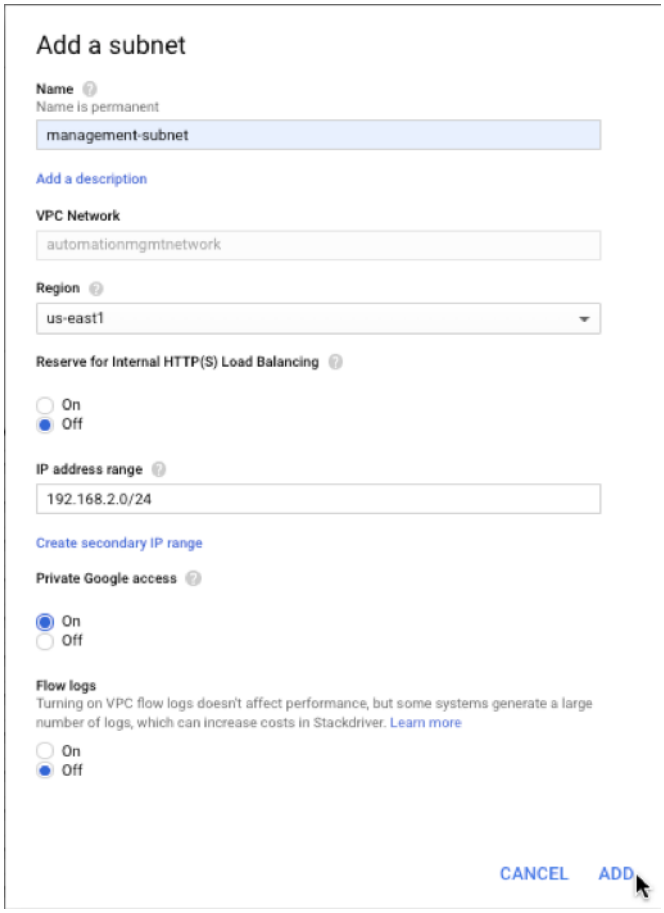


```
"compute.instances.updateNetworkInterface",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.targetInstances.create",
"compute.zones.list",
"compute.zoneOperations.get",
]
<!--NeedCopy-->
```

- Wenn Sie externe IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden zusätzlichen IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.addresses.use"
"compute.instances.addAccessConfig",
"compute.instances.deleteAccessConfig",
"compute.networks.useExternalIp",
"compute.subnetworks.useExternalIp",
]
<!--NeedCopy-->
```

- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie **Private Google Access** im Verwaltungssubnetz aktivieren.



- Wenn Sie GCP-Weiterleitungsregeln für den primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP aufgeführt sind, um sie beim Failover auf neue primäre Daten zu aktualisieren.

So stellen Sie ein VPX Hochverfügbarkeitspaar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der Bereitstellungsschritte für hohe Verfügbarkeit:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder in verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie Hochverfügbarkeitseinstellungen für beide Instanzen mit den Befehlen NetScaler-GUI oder ADC CLI-Befehle.

Schritt 1. Erstellen von VPC-Netzwerken

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix empfiehlt Ihnen, drei VPC-Netzwerke für die Verknüpfung mit Verwaltungs-NIC, Client-NIC und Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich auf der **Google-Konsole an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **Erstellen von VPC-Netzwerken** unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platform.

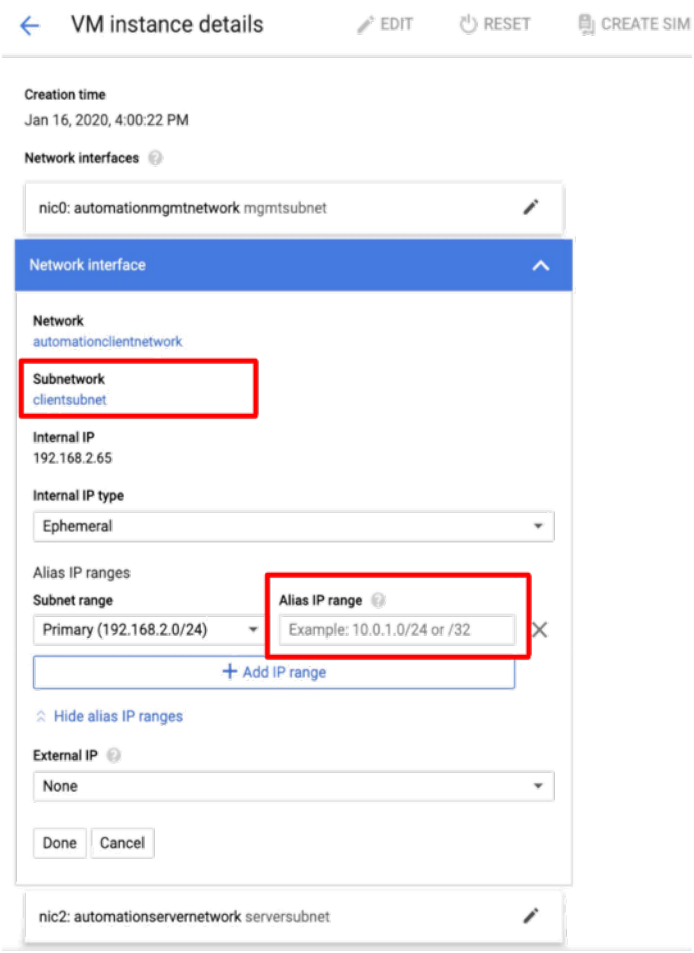
Schritt 2. Erstellen Sie zwei VPX-Instanzen

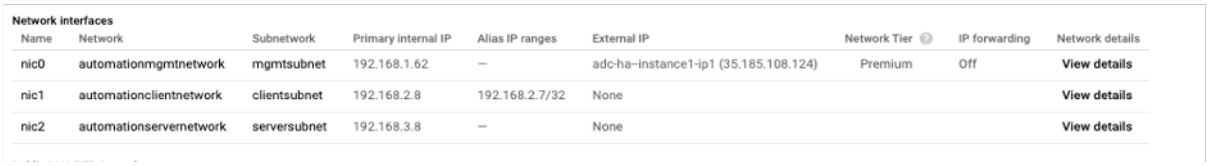
Erstellen Sie zwei VPX-Instanzen, indem Sie die in Szenario angegebenen Schritte ausführen: Stellen Sie eine eigenständige VPX-Instanz mit mehreren NIC, Multi-IPbereit.

> **Wichtig:**
>
> Weisen Sie dem primären Knoten eine Client-Alias-IP-Adresse zu. Verwenden Sie nicht die interne IP-Adresse der VPX-Instanz, um den VIP zu konfigurieren.

Führen Sie die folgenden Schritte aus, um eine Client-Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Clientschnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die IP-Adresse des Client-Alias ein.





Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	automationmgmtnetwork	mgmtsubnet	192.168.1.62	–	adc-ha--instance1-ip1 (35.185.108.124)	Premium	Off	View details
nic1	automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details
nic2	automationservernetwork	serversubnet	192.168.3.8	–	None			View details

Nach dem Failover, wenn der alte Primär zur neuen Sekundärgruppe wird, wechseln die Alias-IP-Adressen von der alten primären und sind an den neuen Primärbereich angehängt.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die Virtual (VIP) und Subnet IP (SNIP) -Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von NetScaler.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie die Hochverfügbarkeit über die NetScaler-GUI oder CLI konfigurieren.

Konfigurieren der Hochverfügbarkeit mit der GUI

Schritt 1. Richten Sie die Hochverfügbarkeit im Modus INC Enabled auf beiden Knoten ein.

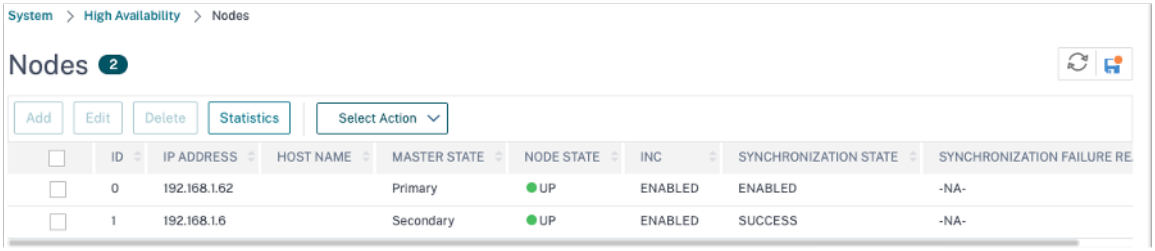
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

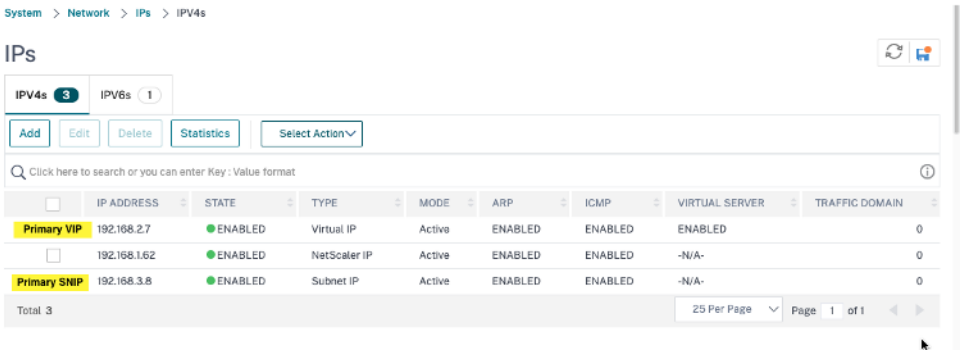


> **Hinweis**
>
> Nachdem der sekundäre Knoten mit dem primären Knoten synchronisiert wurde, hat der sekundäre Knoten dieselben Anmeldeinformationen wie der primäre Knoten.

Schritt 2. Fügen Sie auf beiden Knoten virtuelle IP-Adresse und Subnet-IP-Adresse hinzu.

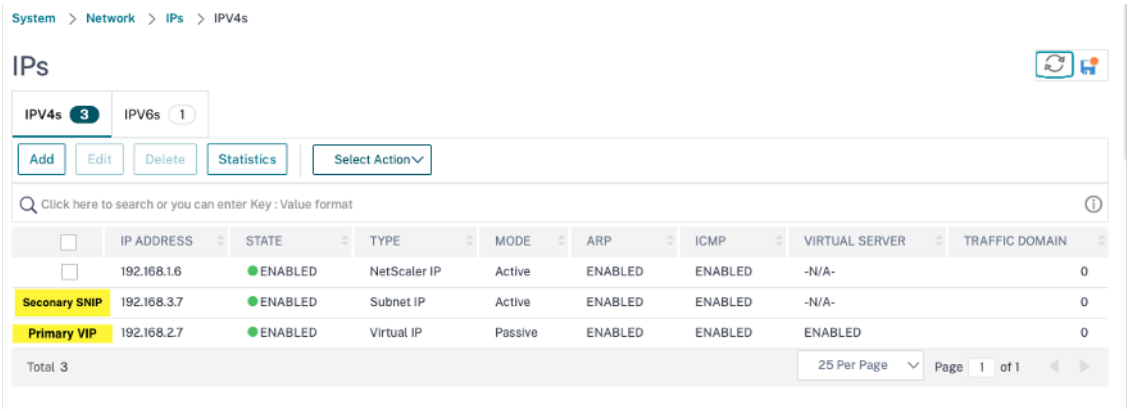
Führen Sie auf dem primären Knotendie folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-IP-Adresse (SNIP):
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz und Netzmaske ein, die für das Serversubnetz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



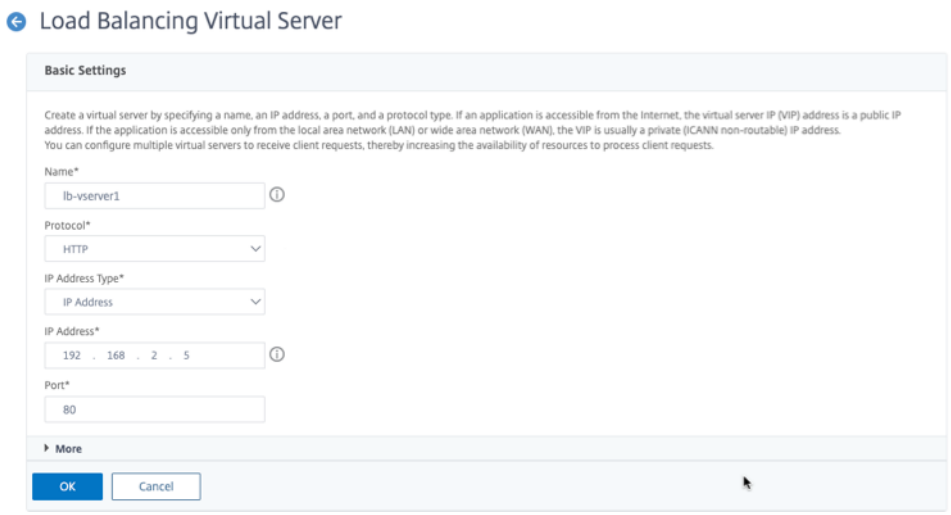
Führen Sie auf dem sekundären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a) Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der primären VM-Instanz konfiguriert sind.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-IP-Adresse (SNIP):
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Serversubnetz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie einen virtuellen Lastausgleichsserver auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre Clientalias-IP-Adresse) und Port hinzu, und klicken Sie auf **OK**.



Schritt 4. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 5. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 3**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.

3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 4**konfigurierten Dienst aus und klicken Sie auf “ **Binden**”.

Schritt 5. Speichern Sie die Konfiguration.

Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die Client-Alias-IP (VIP) und die Server-Alias-IP (SNIP) von der alten primären wechselt zur neuen primären.

Konfigurieren Sie Hochverfügbarkeit über die CLI

Schritt 1. Richten Sie in beiden Instanzen die Hochverfügbarkeit im **INC-aktivierten** Modus mithilfe der NetScaler CLI ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
1 add ha node 1 <sec_ip> -inc ENABLED
2 <!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
1 add ha node 1 <prim_ip> -inc ENABLED
2 <!--NeedCopy-->
```

Der `sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

Der `prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Schritt 2. Fügen Sie VIP und SNIP auf beiden Knoten hinzu.

Geben Sie die folgenden Befehle auf den primären Knoten ein:

```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
2
3 <!--NeedCopy-->
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

```
1 add ns ip <primary_snip> <subnet> -type SNIP
2 <!--NeedCopy-->
```

Der `primary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz.

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:


```
1 add ns ip <primary_client_alias_ip> <subnet> -type VIP
2 <!--NeedCopy-->
```

> Hinweis
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der primären VM-Instanz konfiguriert sind.

```
1 add ns ip <secondary_snip> <subnet> -type SNIP
2 <!--NeedCopy-->
```

Der `secondary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz.

> **Hinweis:**
>
> Geben Sie die IP-Adresse und Netzmaske ein, die für das Serversubnetz in der VM-Instanz konfiguriert sind.

Schritt 3. Fügen Sie einen virtuellen Server auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
1 add <server_type> vserver <vserver_name> <protocol> <
     primary_client_alias_ip> <port>
2 <!--NeedCopy-->
```

Schritt 4. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
1 add service <service_name> <service_ip_address> <protocol> <port>
2 <!--NeedCopy-->
```

Schritt 5. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

Geben Sie den folgenden Befehl ein:

```
1 bind <server_type> vserver <vserver_name> <service_name>
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Um Ihre Konfiguration zu speichern, geben Sie den Befehl ein `save config`. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

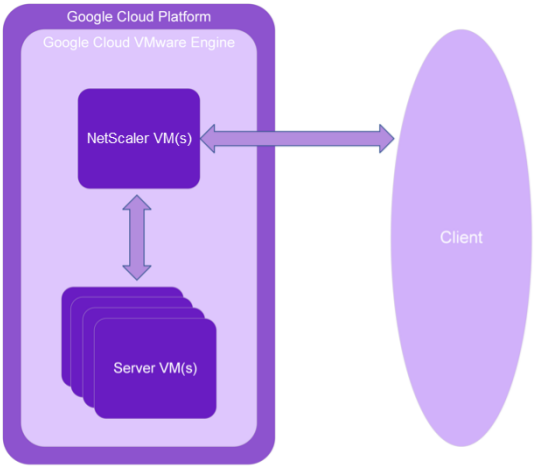
NetScaler VPX-Instanz auf Google Cloud VMware Engine bereitstellen

May 11, 2023

Google Cloud VMware Engine (GCVE) bietet Ihnen Private Clouds, die vSphere-Cluster enthalten, die aus einer dedizierten Bare-Metal-Infrastruktur der Google Cloud Platform erstellt wurden. Die minimale anfängliche Bereitstellung beträgt drei Hosts, es können jedoch nacheinander zusätzliche Hosts hinzugefügt werden. Alle bereitgestellten Private Clouds verfügen über vCenter Server, vSAN, vSphere und NSX-T.

GCVE ermöglicht es Ihnen, Cloud Software Defined Data Center (SDDC) auf der Google Cloud Platform mit der gewünschten Anzahl von ESX-Hosts zu erstellen. GCVE unterstützt NetScaler VPX-Bereitstellungen. GCVE bietet eine gleiche Benutzeroberfläche wie das lokale vCenter. Es funktioniert identisch mit den ESX-basierten NetScaler VPX-Bereitstellungen.

Das folgende Diagramm zeigt den GCVE auf der Google Cloud Platform, auf den ein Administrator oder ein Client über das Internet zugreifen kann. Ein Administrator kann Workload- oder Server-VMs mithilfe von GCVE erstellen, verwalten und konfigurieren. Der Administrator kann über eine OpenVPN-Verbindung auf das webbasierte vCenter und NSX-T Manager des GCVE zugreifen. Sie können die NetScaler VPX-Instanzen (eigenständig oder HA-Paar) und Server-VMs innerhalb von GCVE mithilfe von vCenter erstellen und das entsprechende Netzwerk mit NSX-T Manager verwalten. Die NetScaler VPX-Instanz auf GCVE funktioniert ähnlich wie der lokale VMware-Hostcluster. GCVE kann über eine OpenVPN-Verbindung zur Verwaltungsinfrastruktur verwaltet werden.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Weitere Informationen zu Google Cloud VMware Engine und ihren Voraussetzungen finden Sie in der Dokumentation zu Google Cloud VMware Engine.

- Weitere Informationen zum Bereitstellen von Google Cloud VMware Engine finden Sie unter Bereitstellen einer privaten Cloud VMware Engine Cloud.
- Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Private Cloud über ein Point-to-Site-VPN-Gateway für den Zugriff auf und die Verwaltung von Google Cloud VMware Engine finden Sie unter Zugriff auf eine private Cloud VMware Engine-Cloud.
- Laden Sie auf dem VPN-Clientcomputer die Setupdateien der NetScaler VPX-Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Google Cloud VMware Engine.
- VPX-Lizenzdateien abrufen. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie unter Lizenzierungsübersicht.
- Virtuelle Maschinen (VMs), die in die GCVE Private Cloud erstellt oder in diese migriert wurden, müssen mit einem Netzwerksegment verbunden sein.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX nCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer NetScaler VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> Hinweis
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Mindestsystemanforderungen für die Installation des OVF-Tools beschrieben.

Tabelle 2. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
Netzwerkkarte	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.

Herunterladen der Setup-Dateien für NetScaler VPX

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

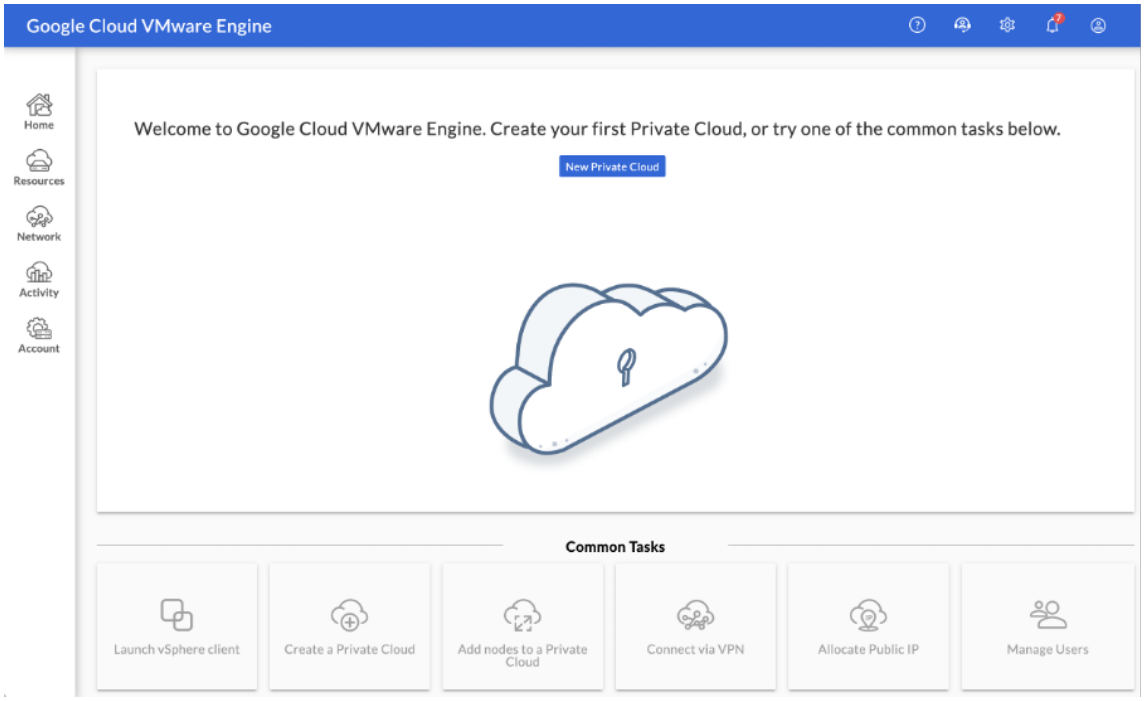
Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-<Releasenummer>-<Buildnummer>-disk1.vmdk (z. B. NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-<Releasenummer>-<Buildnummer>.ovf (z. B. NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-<Releasenummer>-<Buildnummer>.mf (z. B. NSVPX-ESX-13.0-79.64.mf)

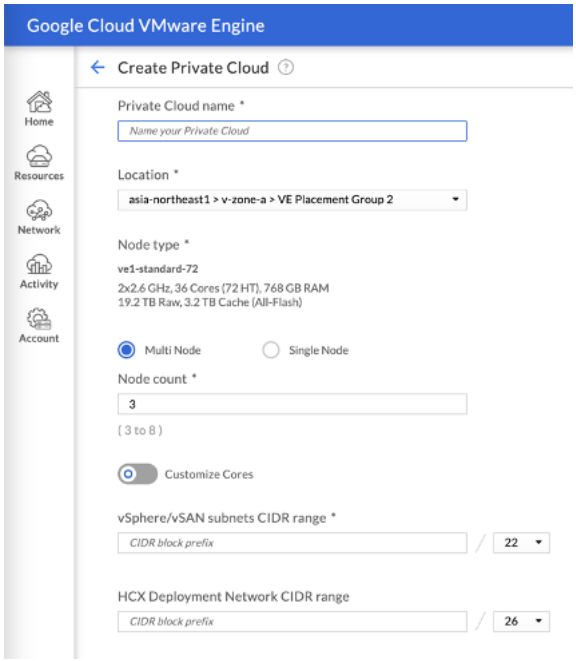
Google Cloud VMware Engine bereitstellen

1. Melden Sie sich bei Ihrem GCVE-Portal an und navigieren Sie zu **Home**.

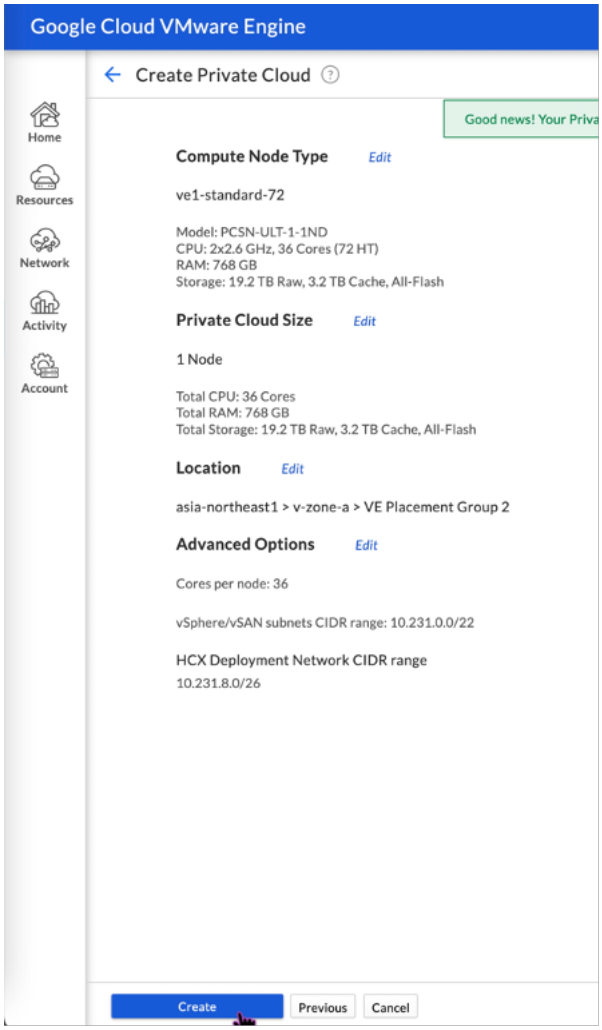


2. Geben Sie auf der Seite **Neue Private Cloud** die folgenden Details ein:

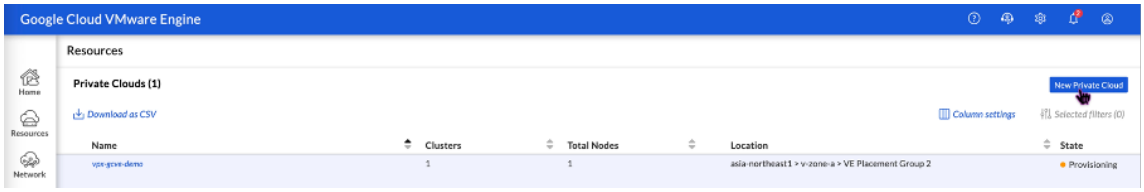
   - Wählen Sie mindestens 3 ESXi-Hosts aus, um den Standardcluster Ihrer Private Cloud zu erstellen.
   - Verwenden Sie für das Feld **CIDR-Bereich des vSphere/vSAN-Subnetzes** den Adressraum /22.
   - Verwenden Sie für das Feld **CIDR-Bereich des HCX Deployment Network** den Adressraum /26.
   - Stellen Sie für das virtuelle Netzwerk sicher, dass sich der CIDR-Bereich nicht mit Ihren on-premises oder anderen GCP-Subnetzen (virtuellen Netzwerken) überschneidet.



3. Klicken Sie auf **Überprüfen und erstellen**.
4. Prüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.



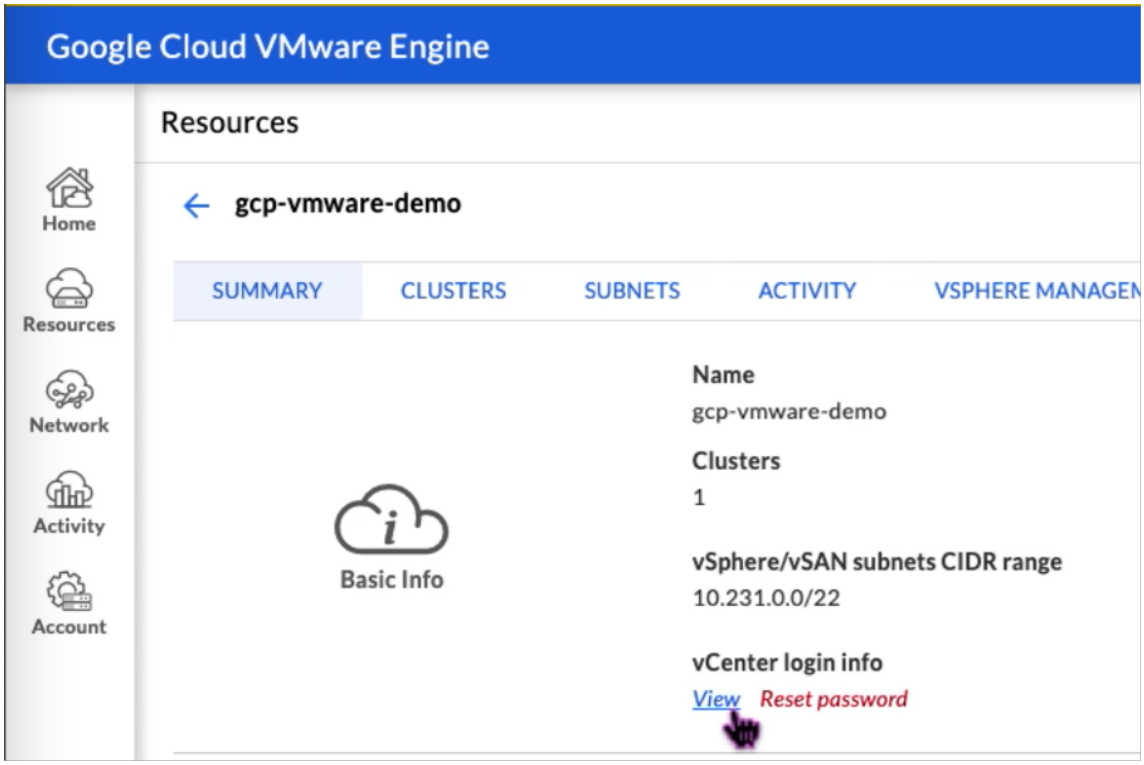
5. Klicken Sie auf **Erstellen**. Der Private Cloud-Bereitstellungsprozess wird gestartet. Es kann bis zu zwei Stunden dauern, bis die Private Cloud bereitgestellt ist.
6. Gehen Sie zu **Ressourcen**, um die erstellte Private Cloud zu überprüfen.



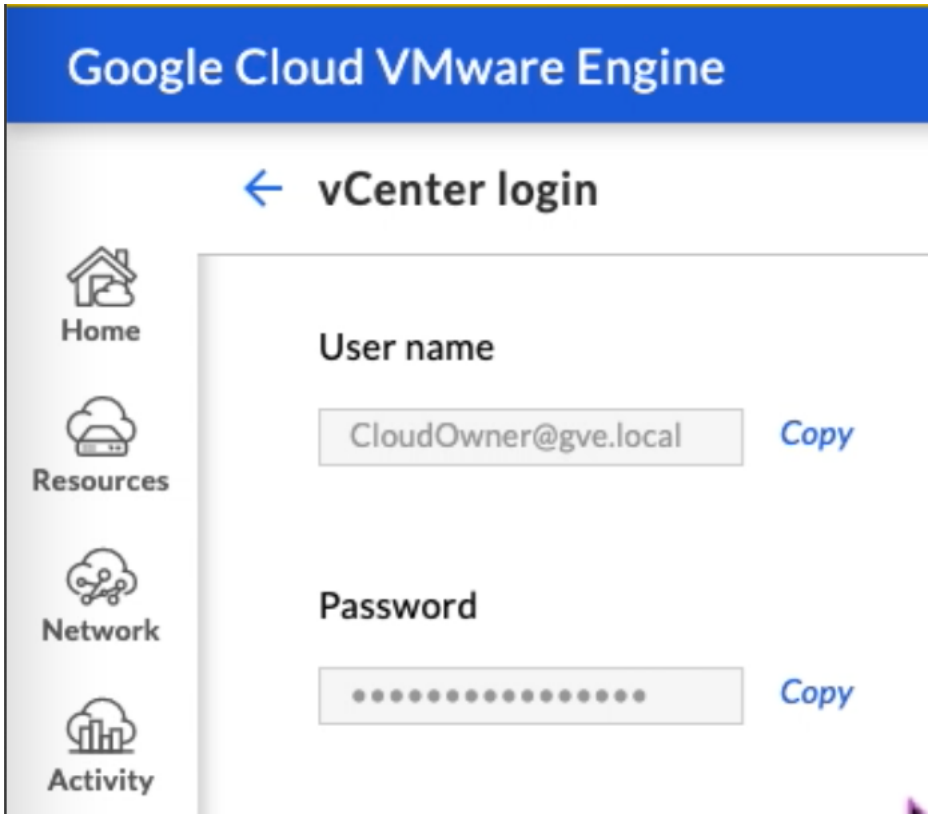
7. Um auf diese Ressource zugreifen zu können, müssen Sie über Point-to-Site-VPN eine Verbindung zu GCVE herstellen. Weitere Informationen finden Sie in der folgenden Dokumentation:
   - VPN-Gateways
   - Verbindung über VPN herstellen

Greifen Sie auf Ihr Private Cloud vCenter Portal zu

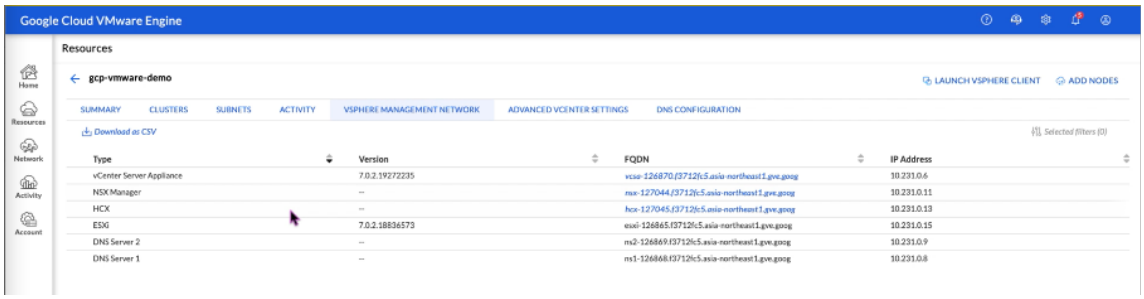
1. Navigieren Sie zu Ihrer privaten Cloud VMware Engine Cloud. Klicken Sie auf der Registerkarte **ZUSAMMENFASSUNG** unter **vCenter-Anmeldeinformationen**auf **Anzeigen**.



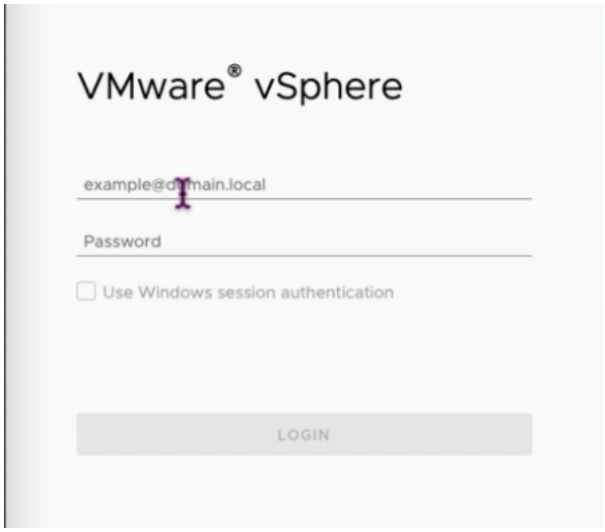
2. Notieren Sie sich die vCenter-Anmeldeinformationen.



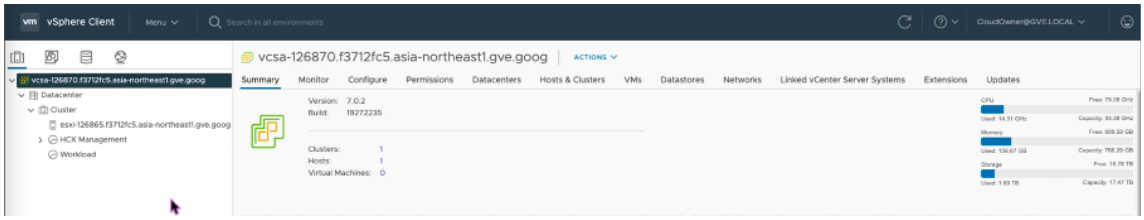
3. Starten Sie den vSphere Client, indem Sie auf **LAUNCH VSPHERE CLIENT** klicken, oder navigieren Sie zu **VSPHERE MANAGEMENT NETWORK** und klicken Sie auf den **vCenter Server Appliance**-FQDN.



4. Melden Sie sich mit den in Schritt 2 dieses Verfahrens vCenter-Anmeldeinformationen bei VMware vSphere an.



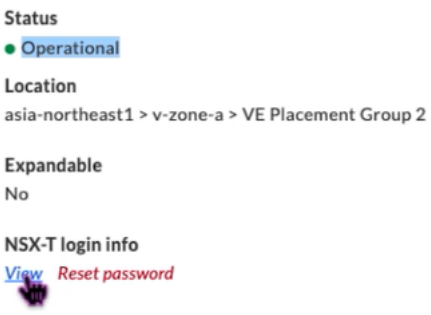
5. Im vSphere Client können Sie die ESXi-Hosts überprüfen, die Sie im GCVE Portal erstellt haben.



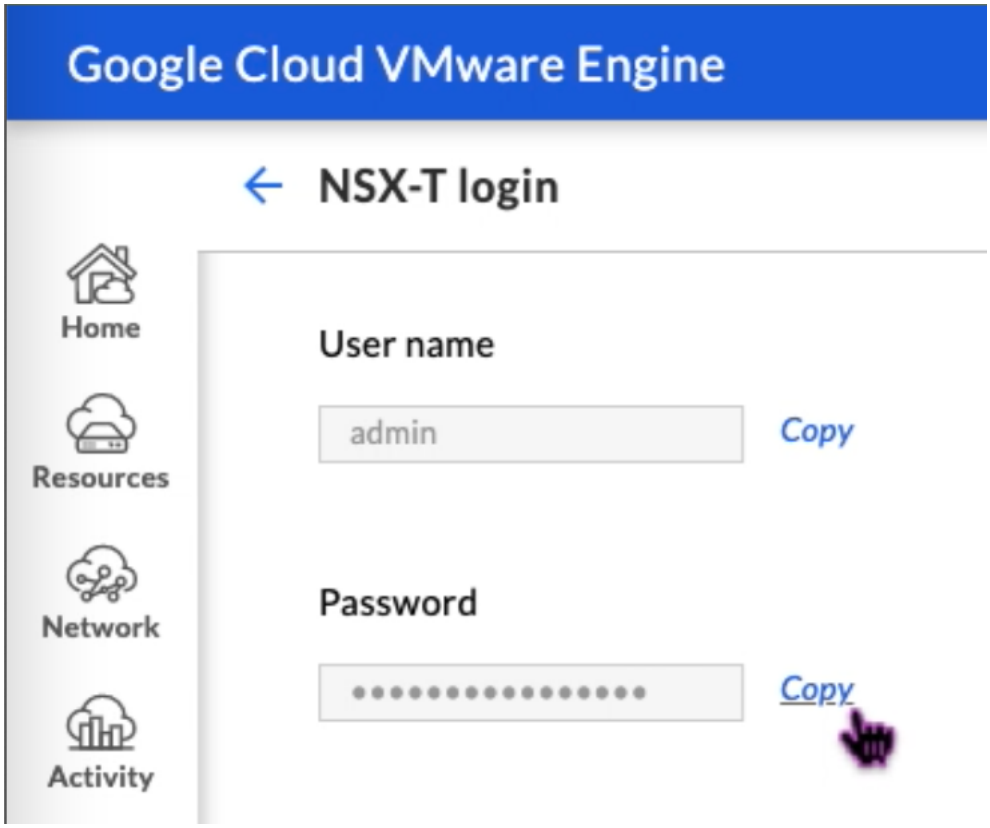
Erstellen eines NSX-T-Segments im GCVE NSX-T-Portal

Sie können ein NSX-T-Segment über NSX Manager in der Google Cloud VMware Engine-Konsole erstellen und konfigurieren. Diese Segmente sind mit dem Standard-Tier-1-Gateway verbunden, und die Workloads in diesen Segmenten erhalten Ost-West- und Nord-Süd-Konnektivität. Sobald Sie das Segment erstellt haben, wird es in vCenter angezeigt.

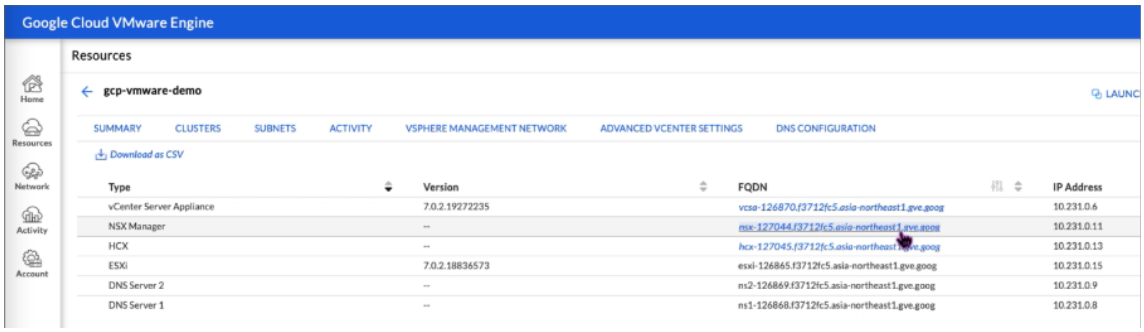
1. Wählen Sie in Ihrer GCVE Private Cloud unter **Zusammenfassung -> NSX-T-Anmeldeinformationen**die Option **Anzeigen**aus.



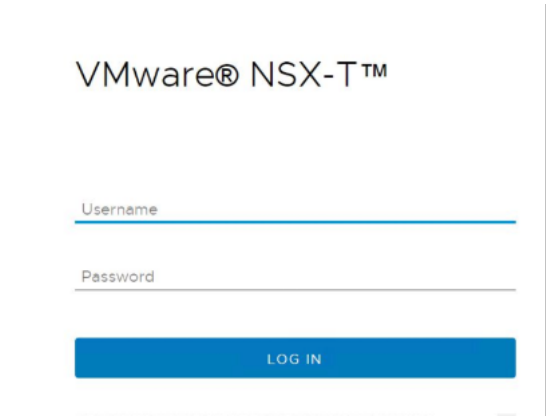
2. Notieren Sie sich die NSX-T-Anmeldeinformationen.



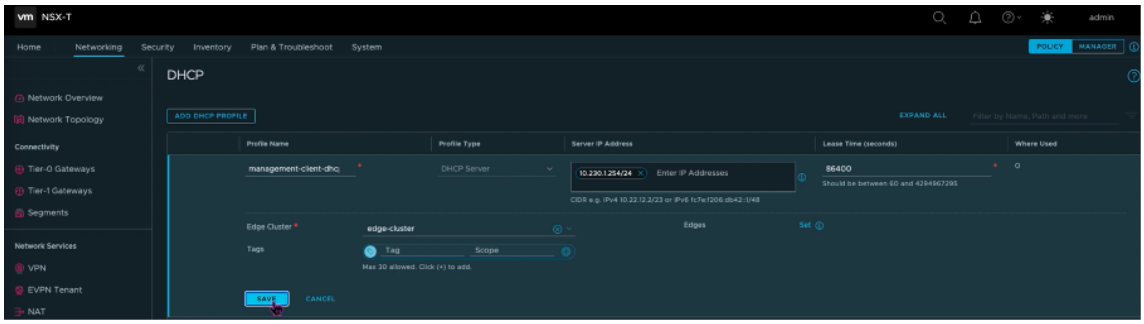
3. Starten Sie NSX Manager, indem Sie zu **VSPHERE MANAGEMENT NETWORK** navigieren und auf den **NSX Manager-FQDN** klicken.



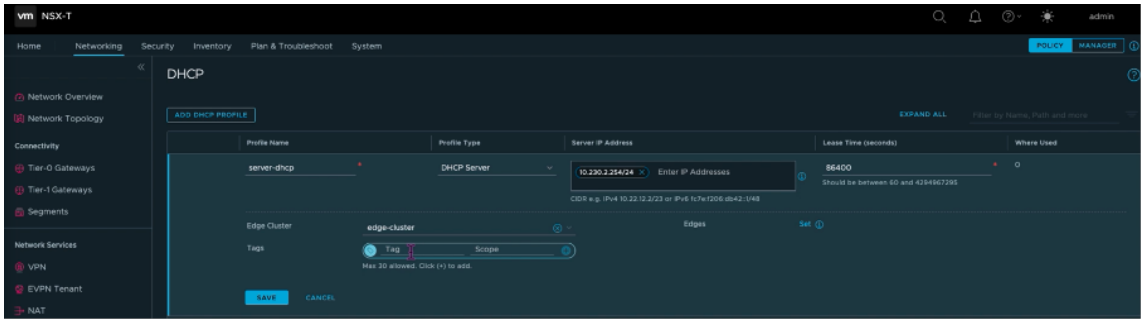
4. Melden Sie sich mit den in Schritt 2 dieses Verfahrens angegebenen Anmeldeinformationen beim NSX Manager an.



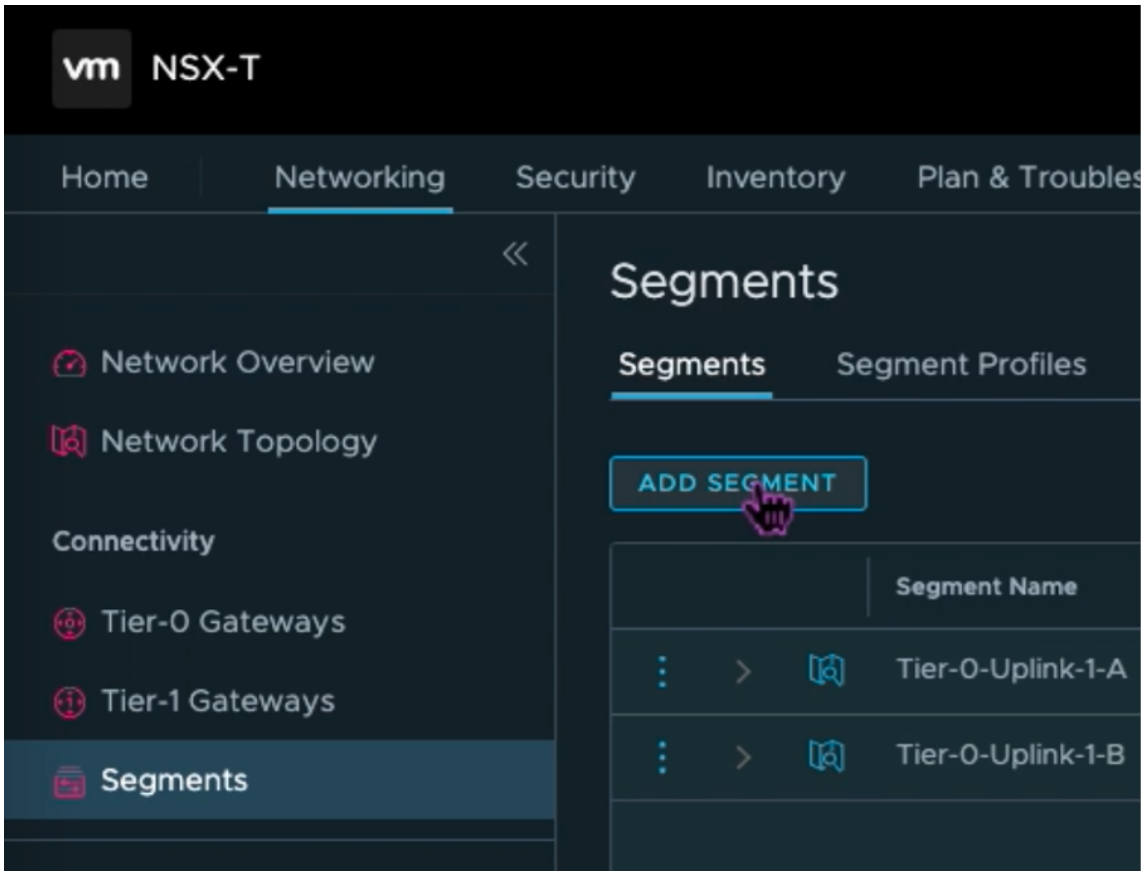
5. Richten Sie den DHCP-Service für die neuen Segmente oder Subnetze ein.
6. Bevor Sie ein Subnetz erstellen können, richten Sie einen DHCP-Dienst ein.
7. Gehen Sie in NSX-T zu **Netzwerk > DHCP**. Das Netzwerk-Dashboard zeigt an, dass der Dienst ein Tier-0- und ein Tier-1-Gateway erstellt.
8. Um mit der Bereitstellung eines DHCP-Servers zu beginnen, klicken Sie auf **DHCP-Profil hinzufügen**.
9. Geben Sie im Feld DHCP-Name einen Namen für das **Client-Management-Profil** ein.
10. Wählen Sie **DHCP-Server** als Profiltyp aus.
11. Geben Sie in der Spalte **Server-IP-Adresse** einen IP-Adressbereich für den DHCP-Dienst an.
12. Wählen Sie Ihren **Edge Cluster aus**.
13. Klicken Sie auf **Save**, um den DHCP-Dienst zu erstellen.



14. Wiederholen Sie die Schritte 6 bis 13 für den Server-DHCP-Bereich.

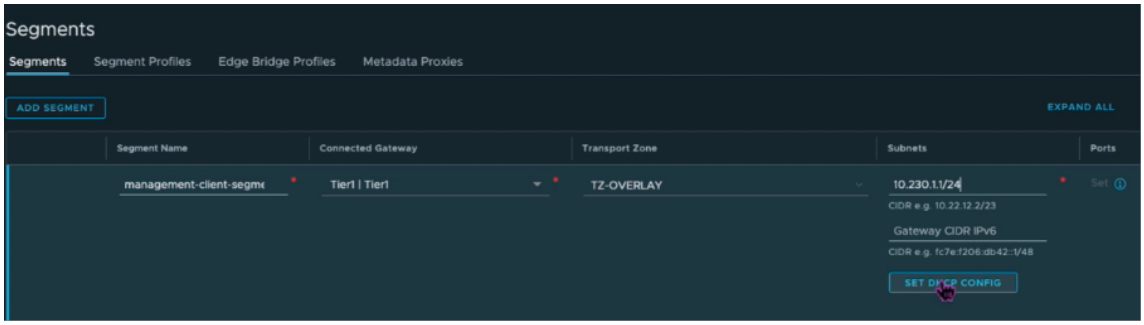


15. Erstellen Sie zwei separate Segmente: eines für Client- und Management-Schnittstellen und eines für Serverschnittstellen.
16. Gehen Sie in NSX-T zu **Netzwerk > Segmente**.
17. Klicken Sie auf **Add Segment**.

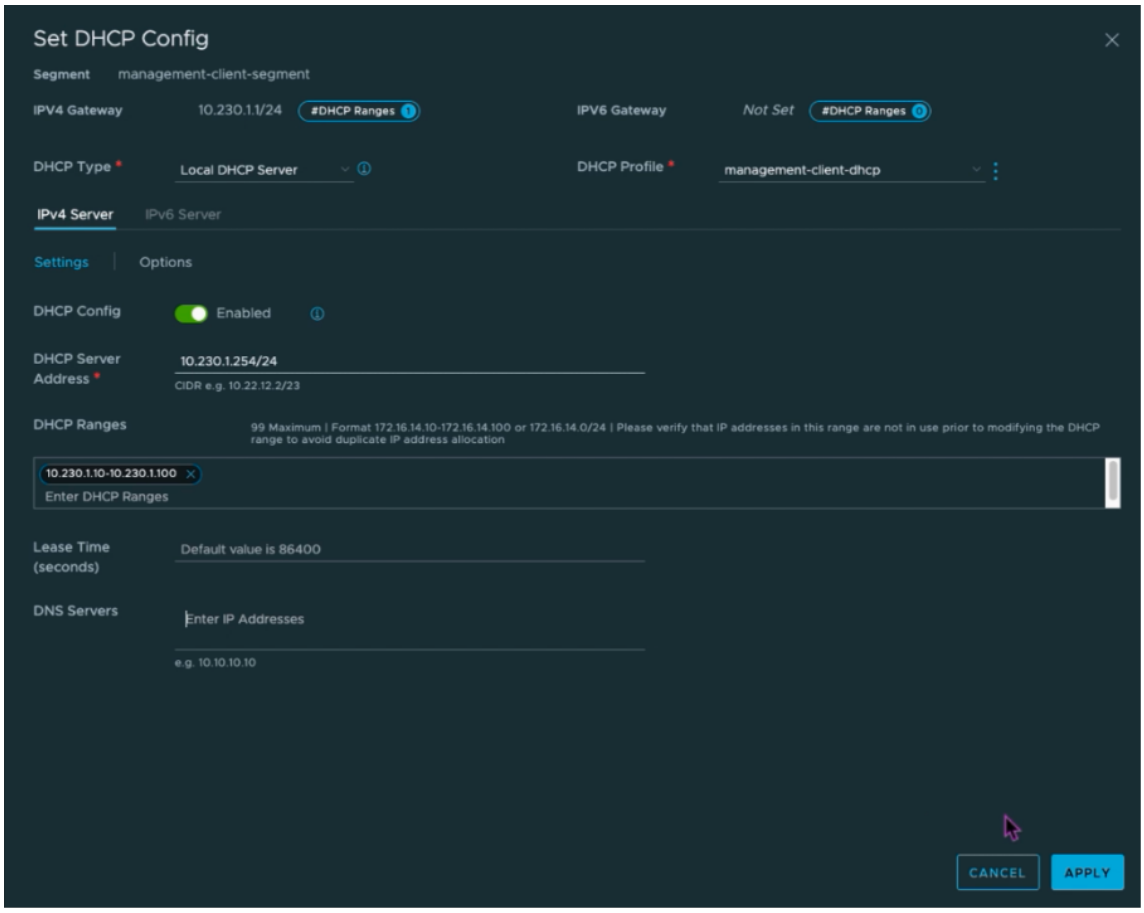


18. Geben Sie im Feld **Segmentname** einen Namen für Ihr **Kundenmanagement-Segment** ein.
19. Wählen Sie in der Liste **Verbundenes GatewayTier1** aus, um eine Verbindung zum Tier-1-Gateway herzustellen.
20. Wählen Sie in der Liste **TransportzoneTZ-OVERLAY | Overlay**aus.
21. Geben Sie in der Spalte **Subnetze** den Subnetzbereich ein. Geben Sie den Subnetzbereich mit

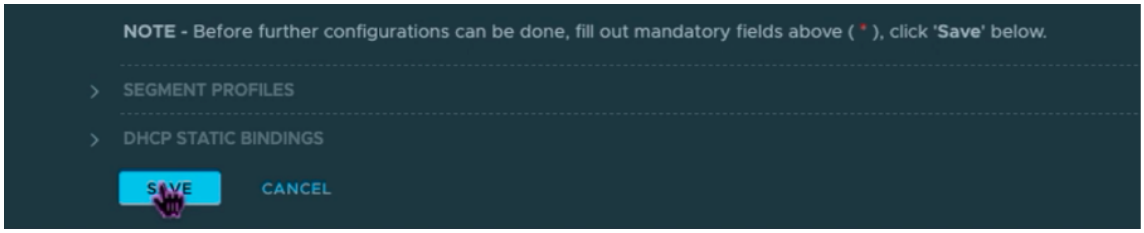
. 1 als letztes Oktett an. Beispiel: 10.12.2.1/24.

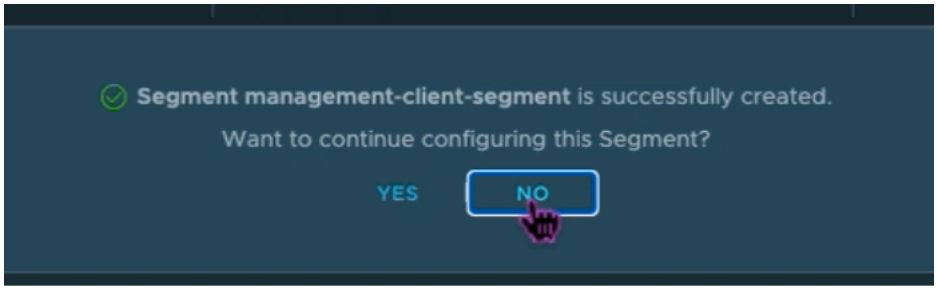


22. Klicken Sie auf **DHCP-Konfiguration festlegen**und geben Sie Werte für das Feld **DHCP-Bereiche** an.



23. Klicken Sie auf **Übernehmen**, um Ihre DHCP-Konfiguration zu
24. Klicken Sie auf **Speichern**.





25. Wiederholen Sie die Schritte 17 bis 24 auch für das Serversegment.
26. Sie können diese Netzwerksegmente jetzt in vCenter auswählen, wenn Sie eine VM erstellen.

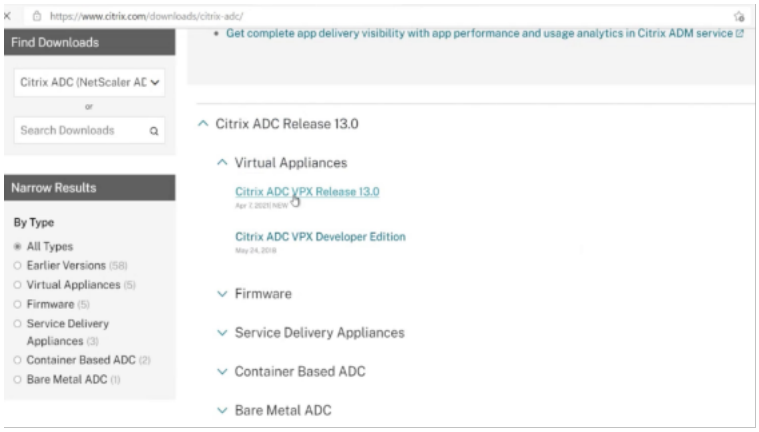
Weitere Informationen finden Sie unter Erstellen Ihres ersten Subnetzes.

Installieren einer NetScaler VPX Instanz in VMware Cloud

Nachdem Sie Private Cloud auf GCVE installiert und konfiguriert haben, können Sie das vCenter verwenden, um virtuelle Appliances auf der VMware Engine zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge der in der Private Cloud verfügbaren Ressourcen ab.

Um NetScaler VPX-Instanzen in Private Cloud zu installieren, führen Sie die folgenden Schritte auf einem Desktop aus, der mit dem Point-to-Site-VPN der Private Cloud verbunden ist:

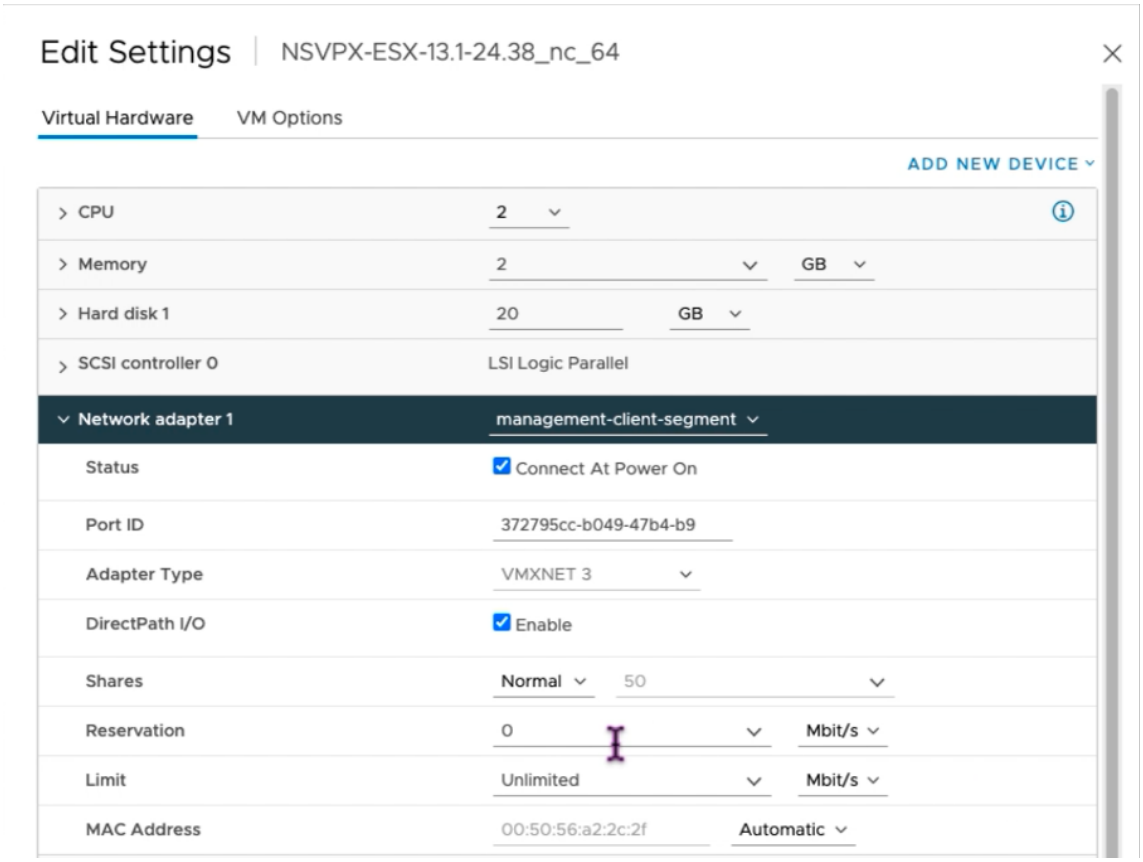
1. Laden Sie die Setup-Dateien der NetScaler VPX-Instanz für den ESXi-Host von der NetScaler-Downloadseite herunter.

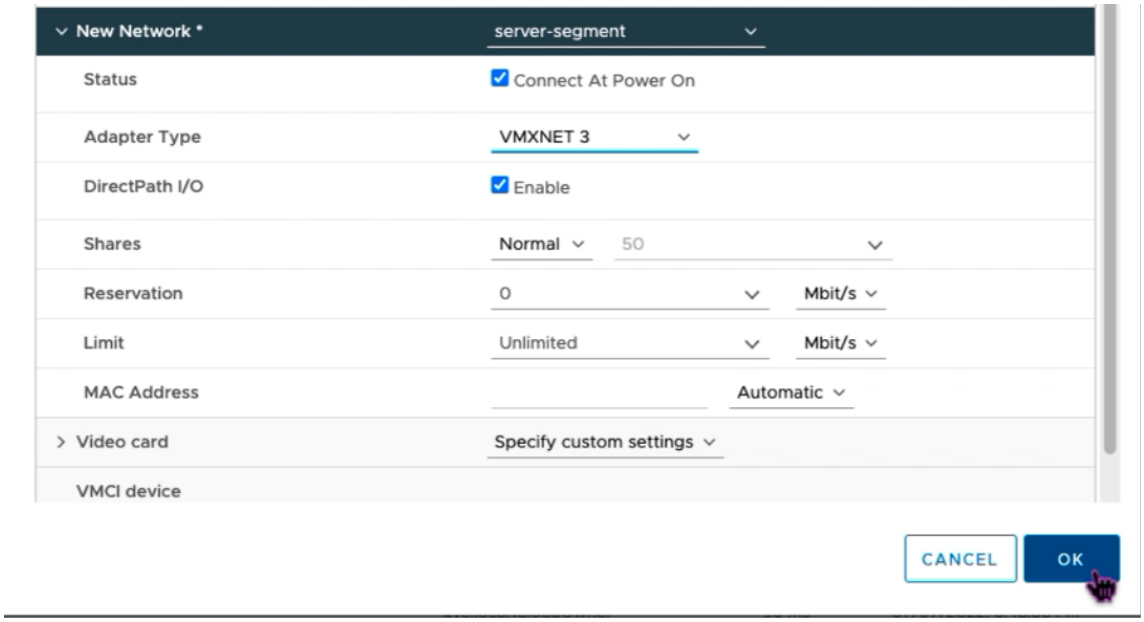


2. Öffnen Sie VMware vCenter in einem Browser, der mit Ihrem Point-to-Site-VPN der Private Cloud verbunden ist.
3. Geben Sie in die Felder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlagebereitstellen im Feld Aus Datei bereitstellen**zu dem Speicherort, an dem Sie die Setupdateien der NetScaler VPX-Instanz gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf**Weiter**.

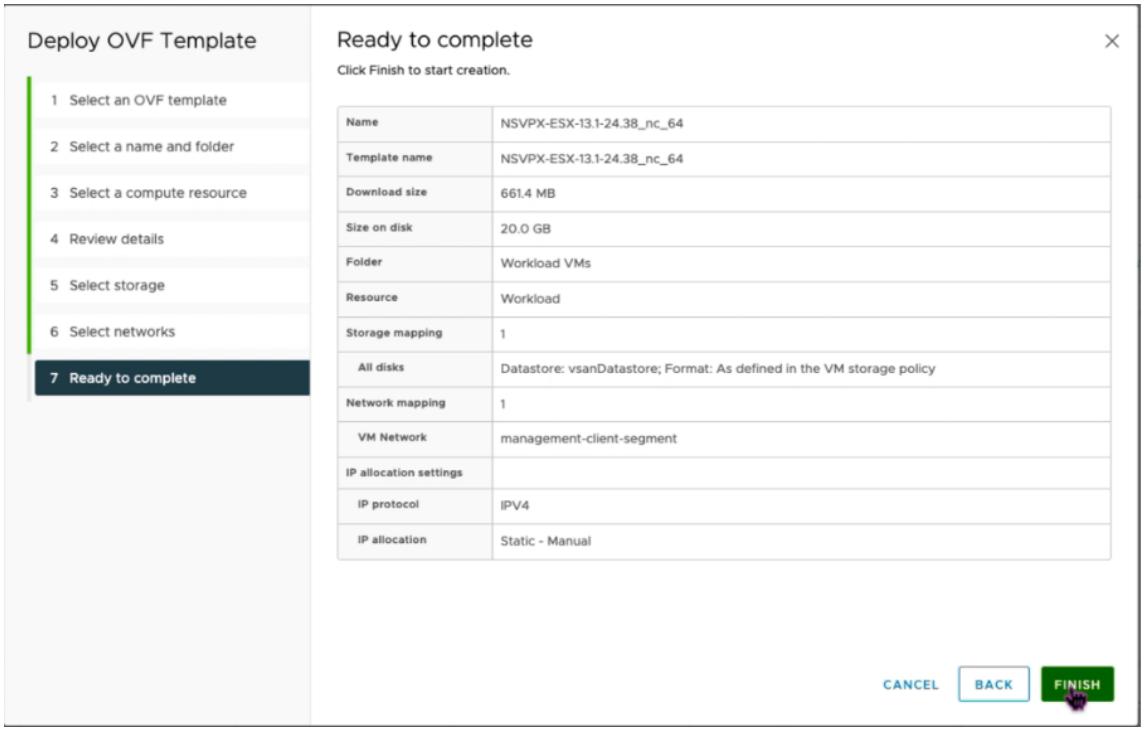
   > HINWEIS:
   >
   > Standardmäßig verwendet die NetScaler VPX-Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird. Die Verfügbarkeit der VMXNET3-Schnittstelle ist durch die GCP-Infrastruktur begrenzt und in Google Cloud VMware Engine möglicherweise nicht verfügbar.

6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf NSX-T Manager konfiguriert haben. Klicken Sie auf **OK**.

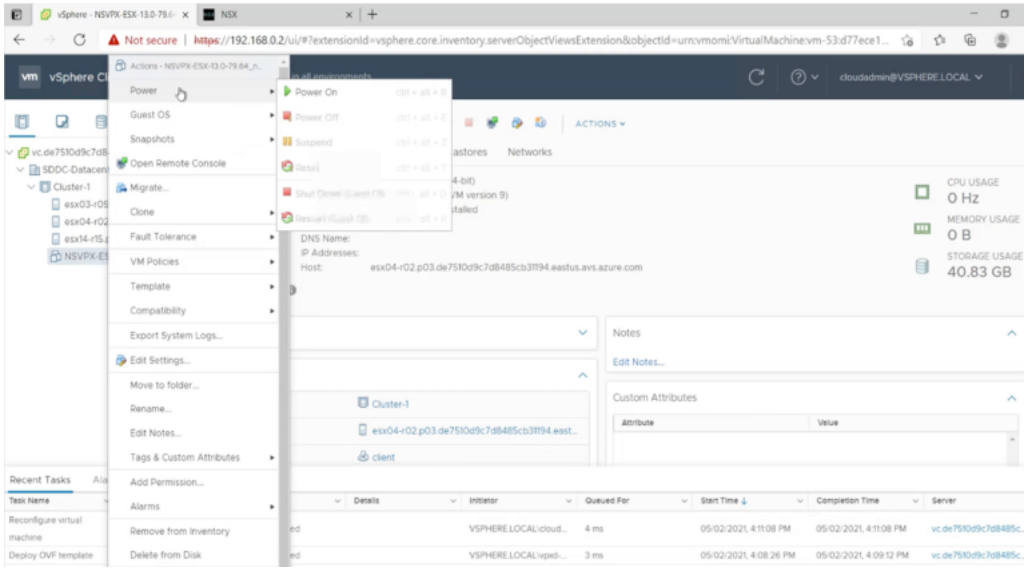




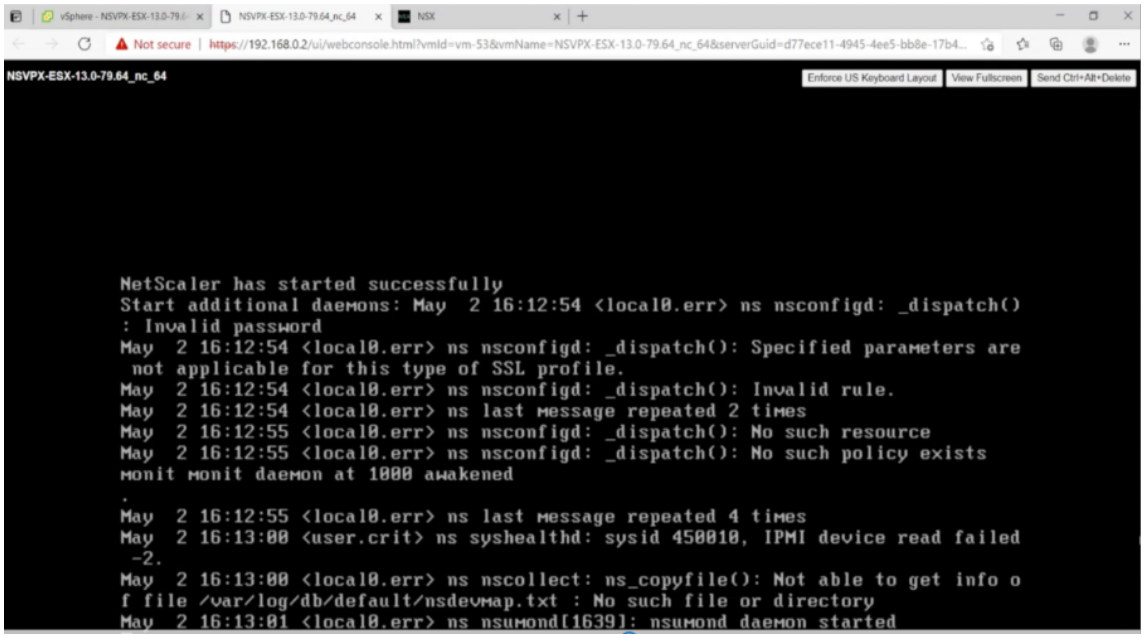
7. Klicken Sie auf **Fertig stellen**, um mit der Installation einer virtuellen Appliance in der VMware Cloud zu beginnen.



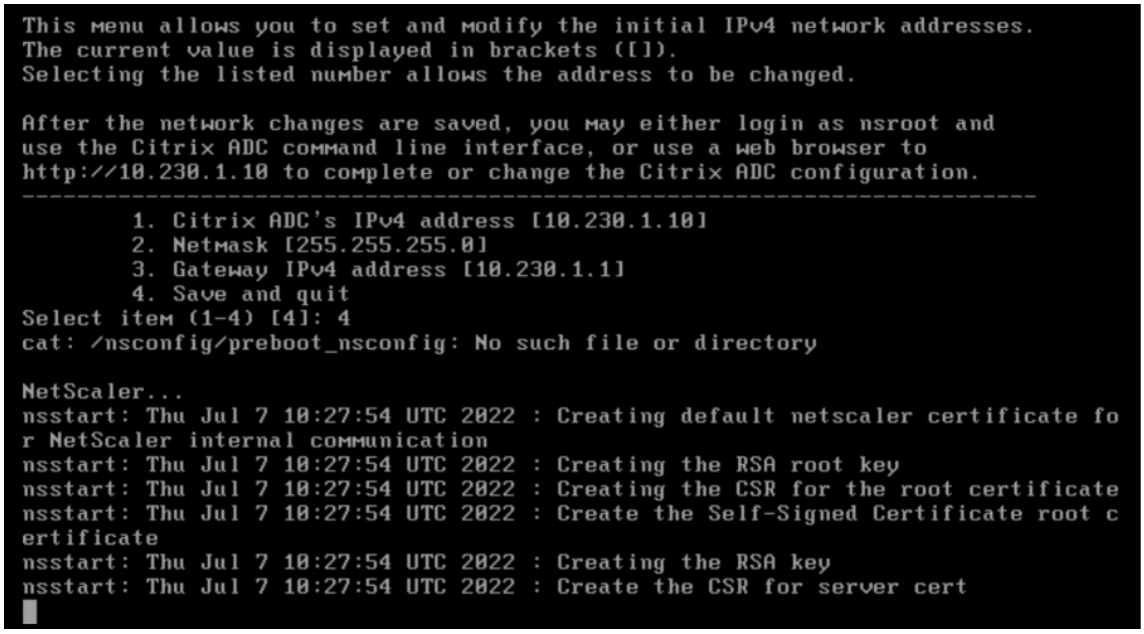
8. Sie können nun die NetScaler VPX-Instanz starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Web-Konsole starten**, um einen Konsolenport zu emulieren.



9. Sie sind jetzt vom vSphere-Client aus mit der NetScaler VM verbunden.



10. Legen Sie beim ersten Start die Verwaltungs-IP und das Gateway für die ADC-Instanz fest.



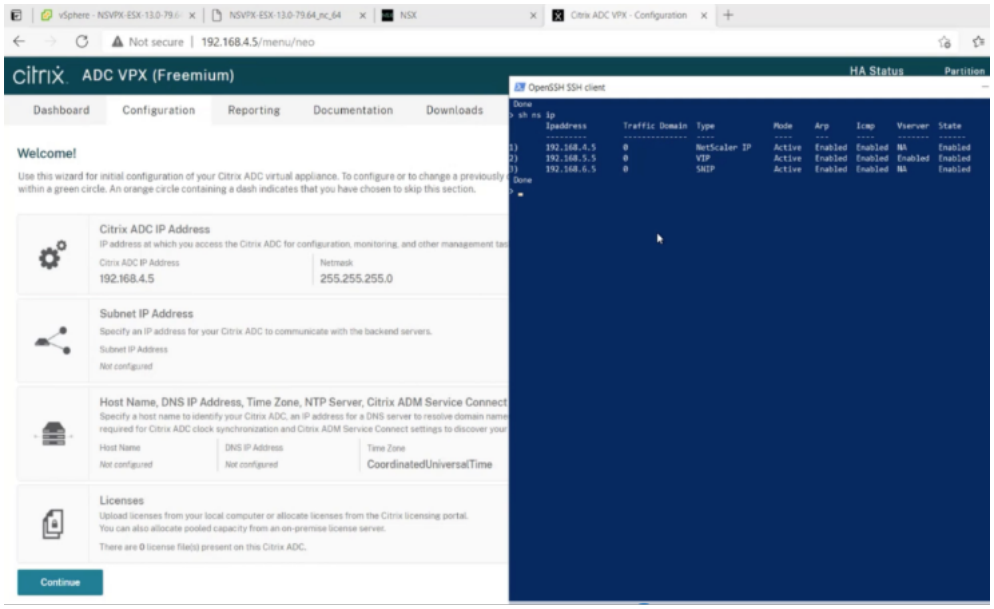
11. Um mit den SSH-Schlüsseln auf die NetScaler-Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

```
ssh nsroot@<management IP address>
<!--NeedCopy-->
```

Beispiel:

```
ssh nsroot@10.230.1.10
<!--NeedCopy-->
```

12. Sie können die ADC-Konfiguration mit dem Befehl `show ns ip` überprüfen.

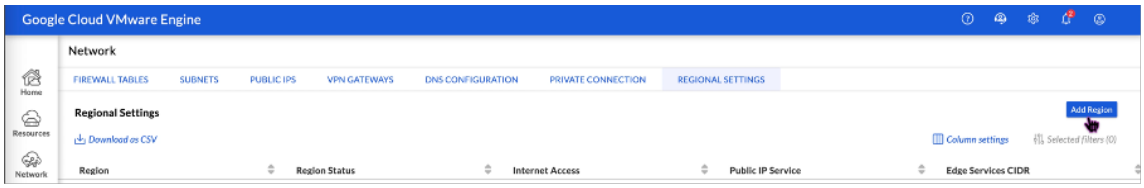


Weisen Sie einer NetScaler VPX-Instanz in der VMware-Cloud eine öffentliche IP-Adresse zu

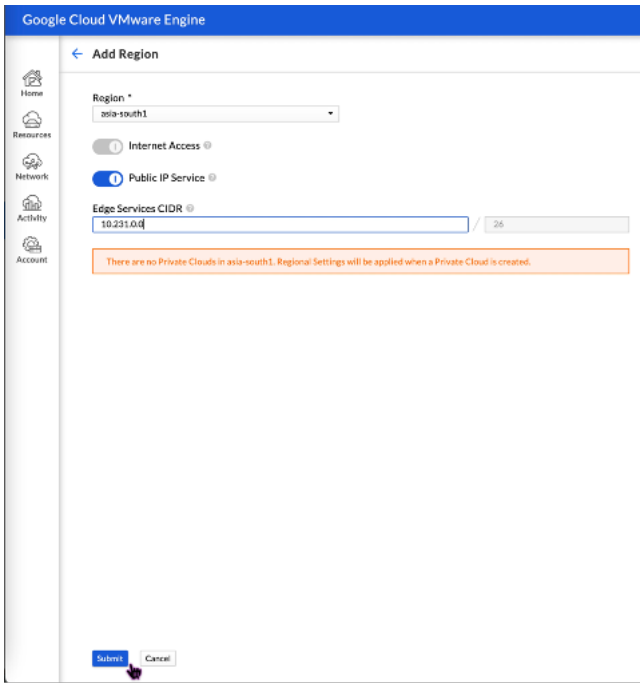
Nachdem Sie die NetScaler VPX-Instanz auf GCVE installiert und konfiguriert haben, müssen Sie der Clientschnittstelle eine öffentliche IP-Adresse zuweisen. Stellen Sie vor dem Zuweisen öffentlicher IP-Adressen zu Ihren VMs sicher, dass der öffentliche IP-Dienst für Ihre Google Cloud-Region aktiviert ist.

Gehen Sie folgendermaßen vor, um den öffentlichen IP-Dienst für eine neue Region zu aktivieren:

1. Navigieren Sie in der GCVE Console zu **Netzwerk > REGIONALE EINSTELLUNGEN > Region hinzufügen**.



2. Wählen Sie Ihre Region aus und aktivieren Sie **den Internetzugriff und denöffentlichen IP-Dienst**.
3. Weisen Sie einen Edge-Services-CIDR zu und stellen Sie sicher, dass sich der CIDR-Bereich nicht mit Ihren on-premises oder anderen GCP/GCVE-Subnetzen (virtuellen Netzwerken) überschneidet.

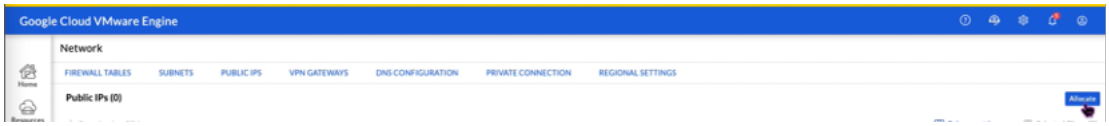


4. Der öffentliche IP-Dienst wird in wenigen Minuten für die ausgewählte Region aktiviert.

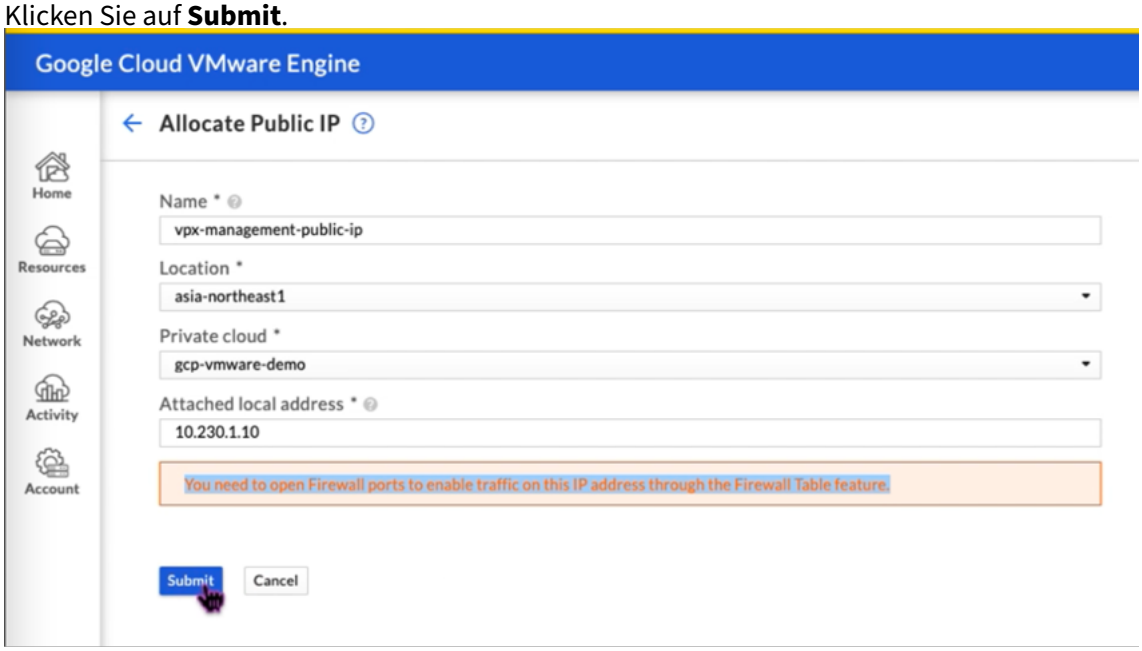
Um der Clientschnittstelle auf der NetScaler VPX-Instanz auf GCVE eine öffentliche IP zuzuweisen,

führen Sie die folgenden Schritte im GCVE Portal aus:

1. Navigieren Sie in der GCVE Console zu **Netzwerk > PUBLIC IPS > Allocate**.



2. Geben Sie einen Namen für die öffentliche IP ein. Wählen Sie Ihre Region und wählen Sie die Private Cloud aus, in der die IP verwendet werden soll.
3. Geben Sie die private IP für die Schnittstelle an, der die öffentliche IP zugeordnet werden soll. Dies ist die **private IP** für Ihre **Client-Schnittstelle** .
4. Klicken Sie auf **Submit**.



5. Public IP ist in wenigen Minuten einsatzbereit.
6. Sie müssen Firewallregeln hinzufügen, um den Zugriff auf die öffentliche IP zu ermöglichen, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter Firewallregeln.

Back-End-GCP-Autoscaling-Dienst hinzufügen

September 11, 2023

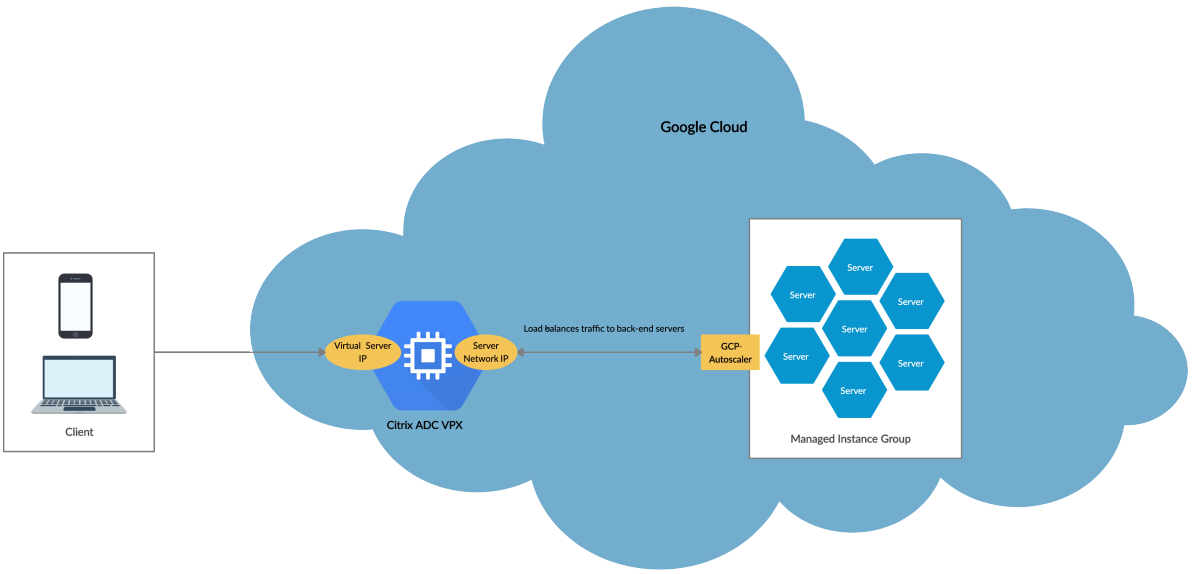
Ein effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen, abhängig von den Anwendungsanforderungen. Um der steigenden Nachfrage gerecht zu werden, müssen Sie die Netzwerkressourcen nach oben skalieren. Wenn die Nachfrage nachlässt, müssen Sie herunterfahren, um unnötige Kosten durch nicht ausgelastete

Ressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, müssen Sie den Datenverkehr, die Speicher- und CPU-Auslastung usw. ständig überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Die NetScaler VPX-Instanz ist in den GCP Autoscaling-Dienst integriert und bietet die folgenden Vorteile:

- **Lastverteilung und Verwaltung**: Server werden automatisch so konfiguriert, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die VPX-Instanz erkennt automatisch verwaltete Instanzgruppen im Back-End-Subnetz und ermöglicht es Ihnen, die verwalteten Instanzgruppen auszuwählen, um die Last auszugleichen. Die virtuellen IP-Adressen und Subnetz-IP-Adressen werden auf der VPX-Instanz automatisch konfiguriert.
- **Hochverfügbarkeit**: Erkennt verwaltete Instanzgruppen, die sich über mehrere Zonen erstrecken, und verteilt die Serverlast.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:
  - Backend-Server auf denselben Platzierungsgruppen
  - Backend-Server in verschiedenen Zonen

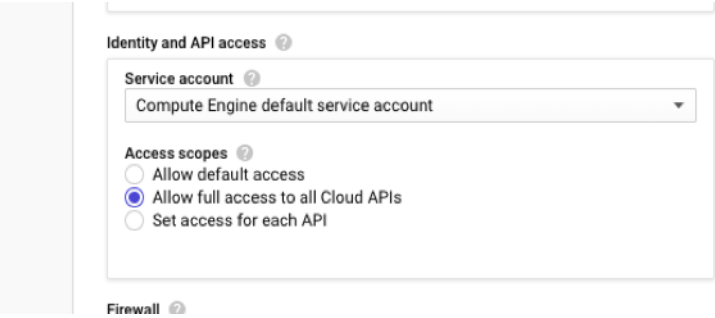
Dieses Diagramm zeigt, wie der GCP Autoscaling-Dienst in einer NetScaler VPX-Instanz funktioniert, die als virtueller Lastausgleichsserver fungiert.



Voraussetzungen

Bevor Sie Autoscaling mit Ihrer NetScaler VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben ausführen.

- Erstellen Sie eine NetScaler VPX Instanz auf GCP entsprechend Ihren Anforderungen.
  - Weitere Informationen zum Erstellen einer NetScaler VPX-Instanz finden Sie unter Bereitstellen einer NetScaler VPX-Instanzauf der Google Cloud Platform.
  - Weitere Informationen zur Bereitstellung von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines VPX-Hochverfügbarkeitspaars auf der GoogleCloud Platform.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
"compute.instances.get",
"compute.instanceGroupManagers.get",
"compute.instanceGroupManagers.list",
"compute.zones.list",
"logging.sinks.create",
"logging.sinks.delete",
"logging.sinks.get",
"logging.sinks.list",
"logging.sinks.update",
"pubsub.subscriptions.consume",
"pubsub.subscriptions.create",
"pubsub.subscriptions.delete",
"pubsub.subscriptions.get",
"pubsub.topics.attachSubscription",
"pubsub.topics.create",
"pubsub.topics.delete",
"pubsub.topics.get",
"pubsub.topics.getIamPolicy",
"pubsub.topics.setIamPolicy",
]
<!--NeedCopy-->
```

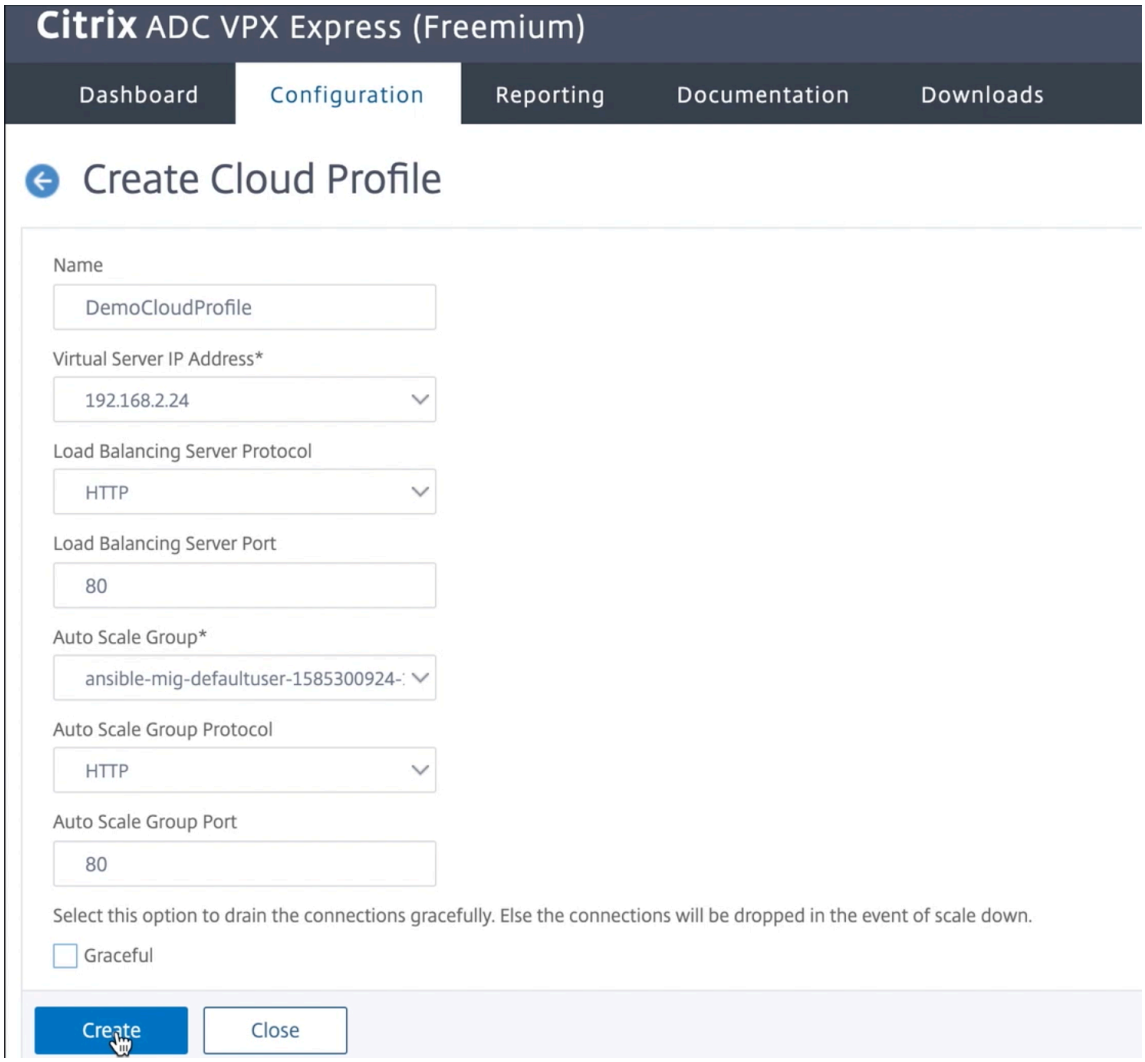
- Um Autoscaling einzurichten, stellen Sie sicher, dass Folgendes konfiguriert ist:
  - Instanzvorlage

- Gruppe „Verwaltete Instanzen“
- Richtlinie zur automatischen Skalierung

Fügen Sie den GCP Autoscaling-Dienst zu einer NetScaler VPX-Instanz hinzu

Sie können den Autoscaling-Dienst mit einem einzigen Klick zu einer VPX-Instanz hinzufügen, indem Sie die GUI verwenden. Gehen Sie wie folgt vor, um den Autoscaling-Dienst zur VPX-Instanz hinzuzufügen:

1. Melden Sie sich mit Ihren Anmeldeinformationen für `nsroot`bei der VPX-Instanz an.
2. Wenn Sie sich zum ersten Mal bei der NetScaler VPX-Instanz anmelden, wird die standardmäßige Cloud-Profilseite angezeigt. Wählen Sie im Dropdownmenü die von GCP verwaltete Instanzgruppe aus und klicken Sie auf **Erstellen**, um ein Cloud-Profil zu erstellen.

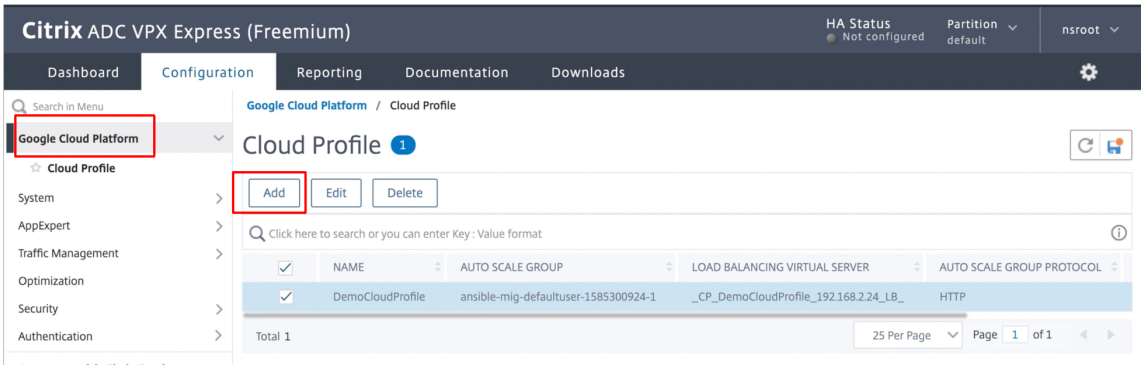


- Das Feld **IP-Adresse des virtuellen Servers** wird automatisch von allen IP-Adressen ausgefüllt, die den Instanzen zugeordnet sind.

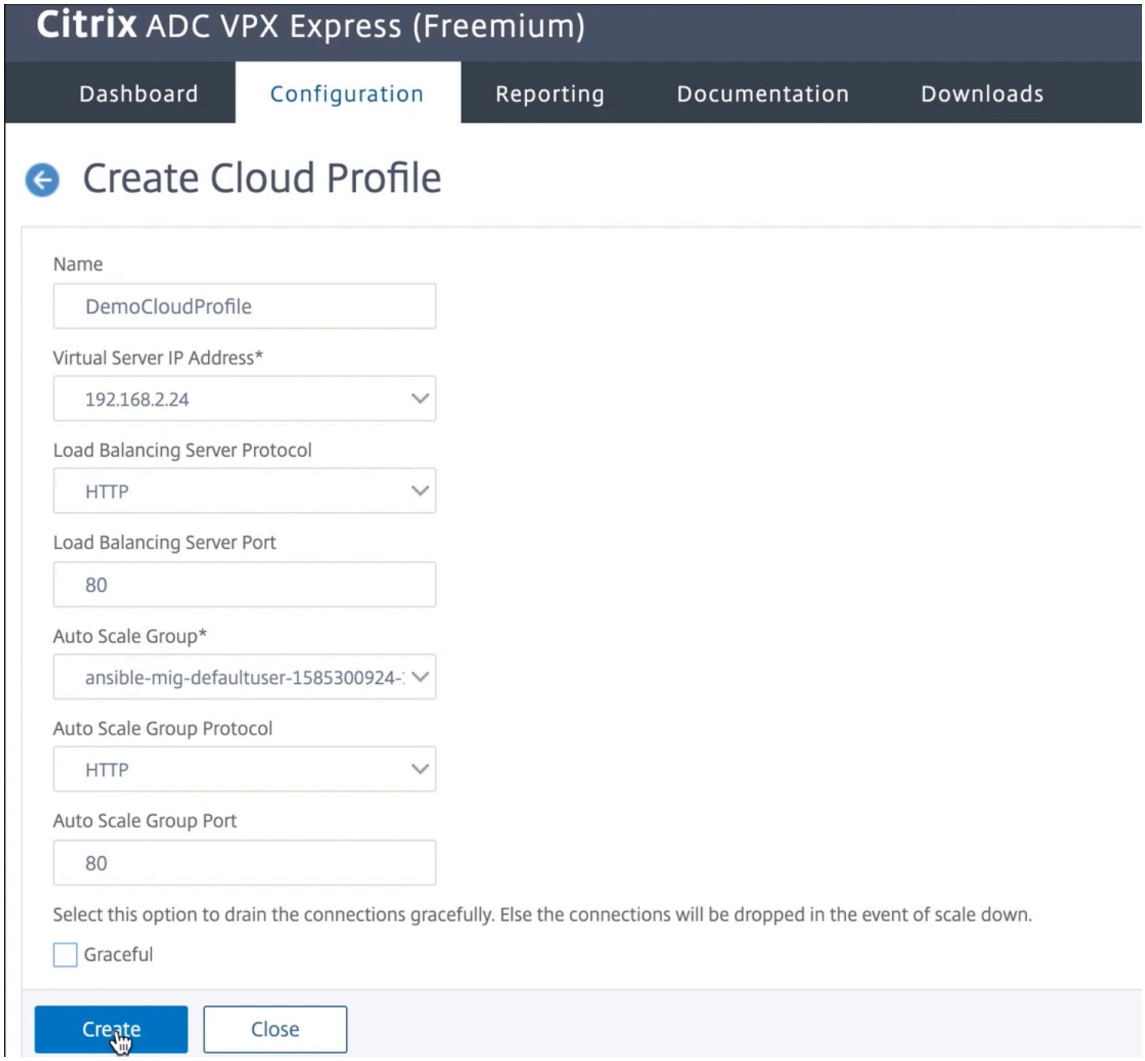
- Die **Autoscale Group** wird aus der verwalteten Instanzgruppe vorausgefüllt, die für Ihr GCP-Konto konfiguriert ist.
- Stellen Sie bei der Auswahl von **Autoscale Group Protocol** und **Autoscale Group Port**sicher, dass die Server das konfigurierte Protokoll und die konfigurierten Ports überwachen. Binden Sie den richtigen Monitor in der Servicegruppe. Standardmäßig wird der TCP-Monitor verwendet.
- Deaktivieren Sie das Kontrollkästchen **Graceful**, da es nicht unterstützt wird.

> Hinweis:
>
> Bei Autoscaling des SSL-Protokolltyps ist der virtuelle Lastausgleichsserver oder die Servicegruppe nach der Erstellung des Cloud-Profils aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

3. Wenn Sie nach der ersten Anmeldung ein Cloud-Profil erstellen möchten, gehen Sie in der GUI zu **System > Google Cloud Platform > Cloud-Profil** und klicken Sie auf **Hinzufügen**.

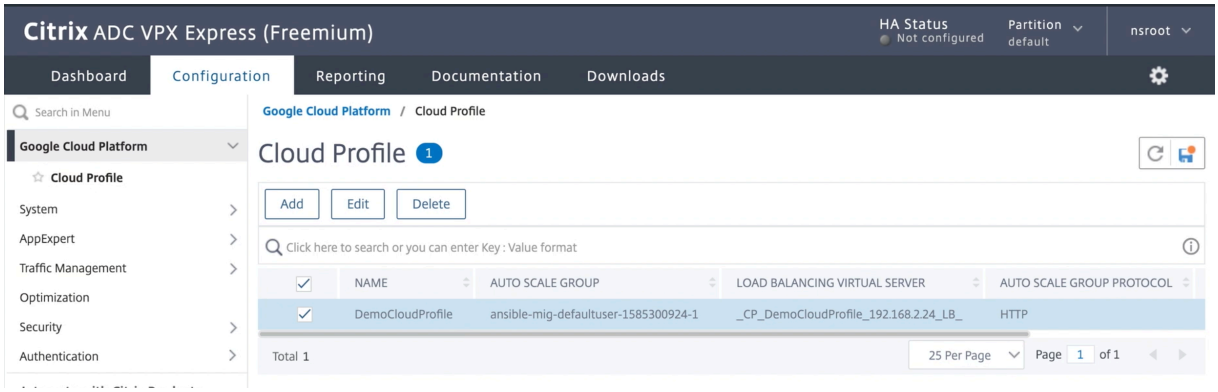


Die Konfigurationsseite „ **Cloud-Profil erstellen** “ wird angezeigt.



Cloud Profile erstellt einen virtuellen NetScaler Loadbalancing-Server und eine Dienstgruppe mit Mitgliedern als Servern der verwalteten Instanzgruppe. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

> **Hinweis:**
>
> Ab NetScaler Version 13.1-42.x können Sie verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung verschiedener Ports) mit derselben verwalteten Instanzgruppe in GCP erstellen. Somit unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.



Unterstützung für VIP-Skalierung für NetScaler VPX-Instanz auf GCP

May 11, 2023

Eine NetScaler-Appliance befindet sich zwischen den Clients und den Servern, sodass Clientanfragen und Serverantworten sie durchlaufen. In einer typischen Installation stellen virtuelle Server, die auf der Appliance konfiguriert sind, Verbindungspunkte bereit, mit denen Clients auf die Anwendungen hinter der Appliance zugreifen. Die Anzahl der öffentlichen virtuellen IP-Adressen (VIP), die für eine Bereitstellung benötigt werden, variiert von Fall zu Fall.

Die GCP-Architektur schränkt jede Schnittstelle der Instanz ein, die mit einer anderen VPC verbunden werden soll. Eine VPC auf GCP ist eine Sammlung von Subnetzen, und jedes Subnetz kann sich über Zonen einer Region erstrecken. Darüber hinaus legt GCP die folgende Einschränkung vor:

- Es gibt eine 1:1 -Zuordnung der Anzahl öffentlicher IP-Adressen zur Anzahl der NICs. Einer NIC kann nur eine öffentliche IP-Adresse zugewiesen werden.
- An einem Instanztyp mit höherer Kapazität können maximal 8 NICs angeschlossen werden.

Zum Beispiel kann eine n1-Standard-2-Instanz nur 2 NICs haben, und die öffentlichen VIPs, die hinzugefügt werden können, sind auf 2 beschränkt. Weitere Informationen finden Sie unter VPC-Ressourcenkontingente.

Um höhere Maßstäbe öffentlicher virtueller IP-Adressen auf einer NetScaler VPX-Instanz zu erreichen, können Sie die VIP-Adressen als Teil der Metadaten der Instanz konfigurieren. Die NetScaler VPX-Instanz verwendet intern Weiterleitungsregeln, die von der GCP bereitgestellt werden, um eine VIP-Skalierung zu erreichen. Die NetScaler VPX-Instanz bietet auch Hochverfügbarkeit für die konfigurierten VIPs.
Nachdem Sie VIP-Adressen als Teil der Metadaten konfiguriert haben, können Sie einen virtuellen LB-Server mit derselben IP konfigurieren, die zum Erstellen der Weiterleitungsregeln verwendet wird. Daher können wir Weiterleitungsregeln verwenden, um die Einschränkungen zu mildern, die wir bei der Skalierung bei der Verwendung öffentlicher VIP-Adressen auf einer NetScaler VPX-Instance auf GCP

haben.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Wichtige Hinweise

- Google berechnet einige zusätzliche Kosten für jede virtuelle IP-Weiterleitungsregel. Die tatsächlichen Kosten hängen von der Anzahl der erstellten Einträge ab. Die damit verbundenen Kosten entnehmen Sie den Google-Preisdokumenten.
- Die Weiterleitungsregeln gelten nur für öffentliche VIPs. Sie können Alias-IP-Adressen verwenden, wenn die Bereitstellung private IP-Adressen als VIPs benötigt.
- Sie können Weiterleitungsregeln nur für die Protokolle erstellen, die den virtuellen LB-Server benötigen. VIPs können im laufenden Betrieb erstellt, aktualisiert oder gelöscht werden. Sie können auch einen neuen virtuellen Lastausgleichsserver mit derselben VIP-Adresse, jedoch mit einem anderen Protokoll hinzufügen.

Vorbereitung

- Die NetScaler VPX-Instanz muss auf GCP bereitgestellt werden.
- Die externe IP-Adresse muss reserviert werden. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create"
"compute.targetInstances.get"
"compute.targetInstances.use",
]

<!--NeedCopy-->
```

- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.

- Wenn Sie VIP-Skalierung auf einer eigenständigen VPX-Instanz verwenden, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [
"compute.addresses.list",
"compute.addresses.get",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.instances.use",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
]
<!--NeedCopy-->
```

- Wenn Sie die VIP-Skalierung in einem Hochverfügbarkeitsmodus verwenden, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [
"compute.addresses.get",
"compute.addresses.list",
"compute.addresses.use",
"compute.forwardingRules.create",
"compute.forwardingRules.delete",
"compute.forwardingRules.get",
"compute.forwardingRules.list",
"compute.forwardingRules.setTarget",
"compute.instances.use",
"compute.instances.get",
"compute.instances.list",
"compute.instances.setMetadata",
"compute.subnetworks.use",
"compute.targetInstances.create",
"compute.targetInstances.list",
"compute.targetInstances.use",
"compute.zones.list",
]
<!--NeedCopy-->
```


> Hinweis:
>
> Wenn Ihr Dienstkonto in einem Hochverfügbarkeitsmodus keine Eigentümer- oder Bearbeiterrollen hat, müssen Sie die **Rolle Dienstkontobenutzer** zu Ihrem Dienstkonto hinzufügen.

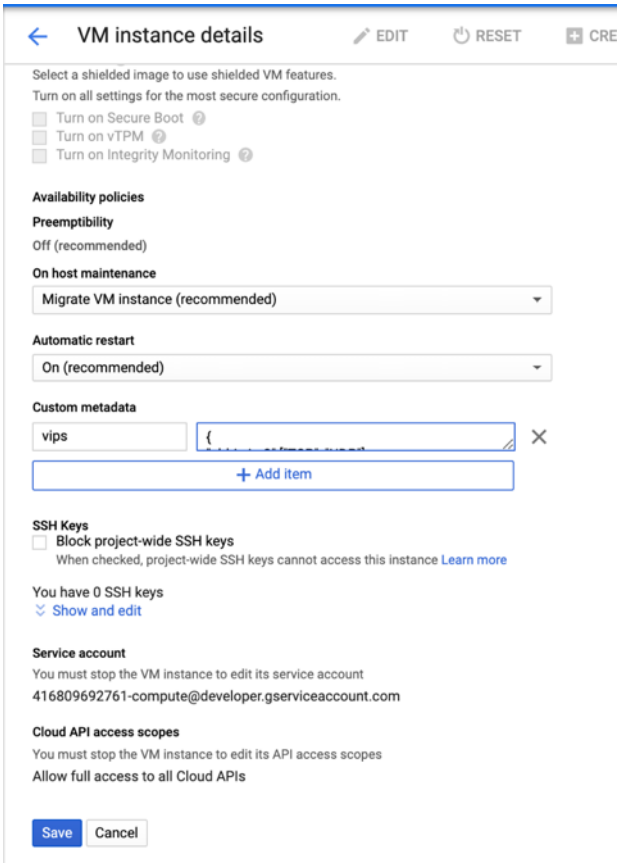
Konfigurieren externer IP-Adressen für die VIP-Skalierung auf der NetScaler VPX-Instanz

1. Navigieren Sie in der Google Cloud Console zur Seite **VM-Instanzen** .
2. Erstellen Sie eine neue VM-Instanz oder verwenden Sie eine vorhandene Instanz.
3. Klicken Sie auf den Instanznamen. Klicken Sie auf der **Detailseite der VM-Instanz** auf **Bearbeiten**.
4. Aktualisieren Sie die **benutzerdefinierten Metadaten**, indem Sie Folgendes eingeben:
   - Schlüssel = vips
   - Value = Geben Sie einen Wert im folgenden JSON-Format an:

     {
     „Name der externen reservierten IP“: [Liste der Protokolle],
     }

   GCP unterstützt die folgenden Protokolle:

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP



Weitere Informationen finden Sie unter Benutzerdefinierte Metadaten.

Beispiel für benutzerdefinierte Metadaten:

{
“external-ip1-name”:[“TCP”, “UDP”],
“external-ip2-name”:[“ICMP”, “AH”]
}

In diesem Beispiel erstellt die NetScaler VPX-Instanz intern eine Weiterleitungsregel für jedes IP-Protokollpaar. Die Metadateneinträge werden den Weiterleitungsregeln zugeordnet. Dieses Beispiel hilft Ihnen zu verstehen, wie viele Weiterleitungsregeln für einen Metadateneintrag erstellt werden.

Vier Weiterleitungsregeln werden wie folgt erstellt:

a) external-ip1-Name und TCP
b) external-ip1-Name und UDP
c) external-ip2-name und ICMP
d) external-ip2-name und AH

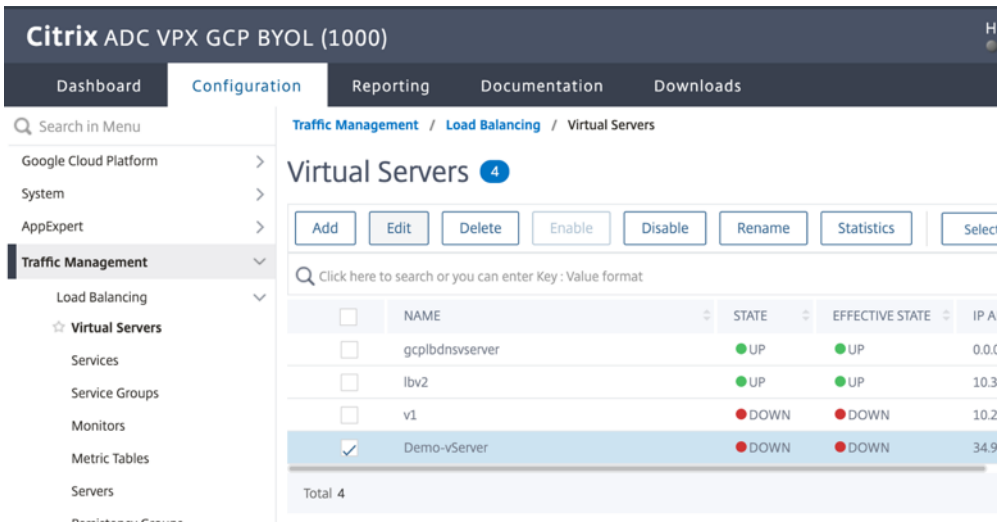
> Hinweis:
>
> Im HA-Modus müssen Sie benutzerdefinierte Metadaten nur für die primäre Instanz hinzufügen. Beim Failover werden die benutzerdefinierten Metadaten mit dem neuen Primärgerät synchronisiert.

5. Klicken Sie auf **Speichern**.

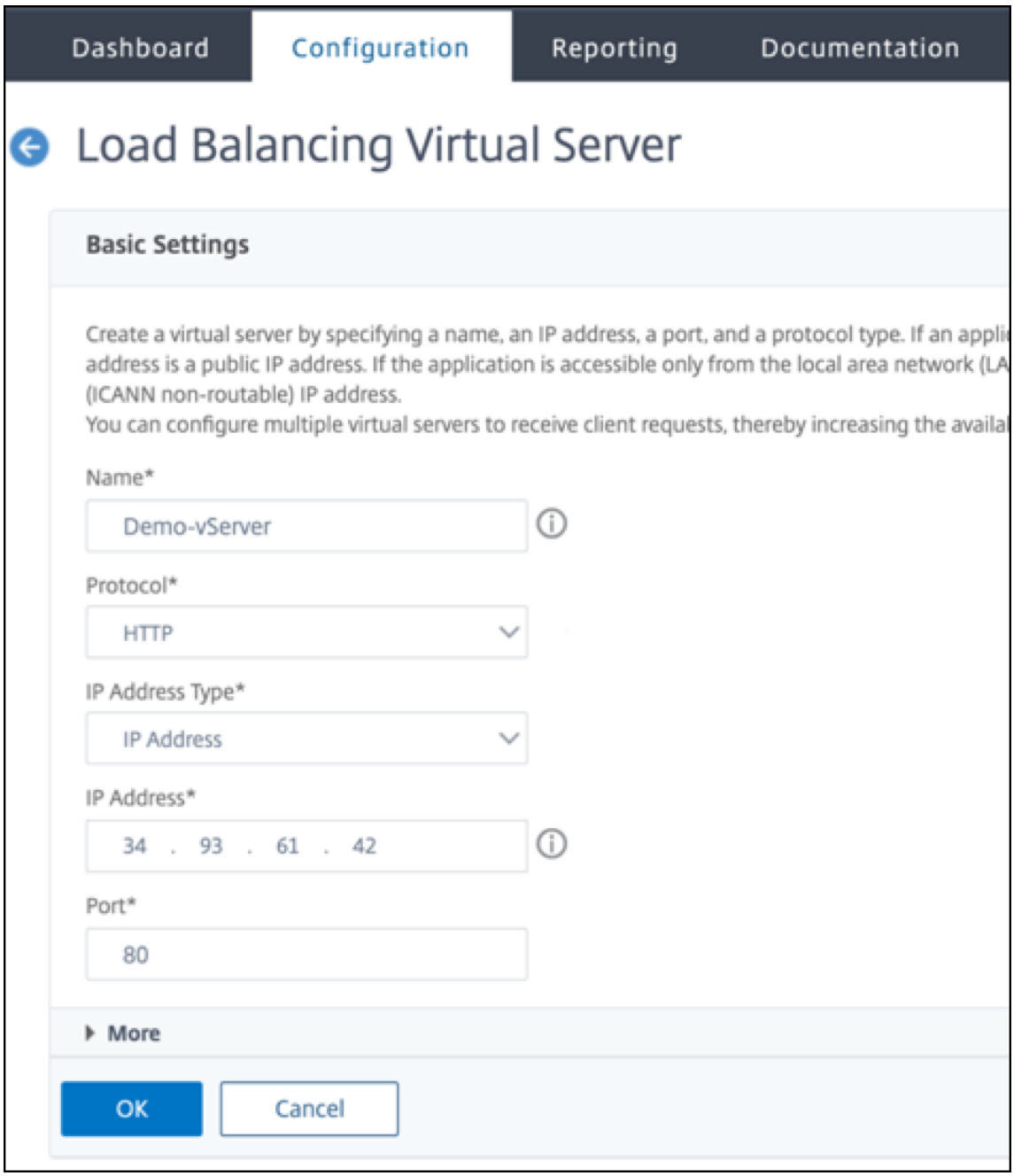
Einrichten eines virtuellen Lastausgleichsservers mit externer IP-Adresse auf einer NetScaler VPX-Instanz

Schritt 1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.

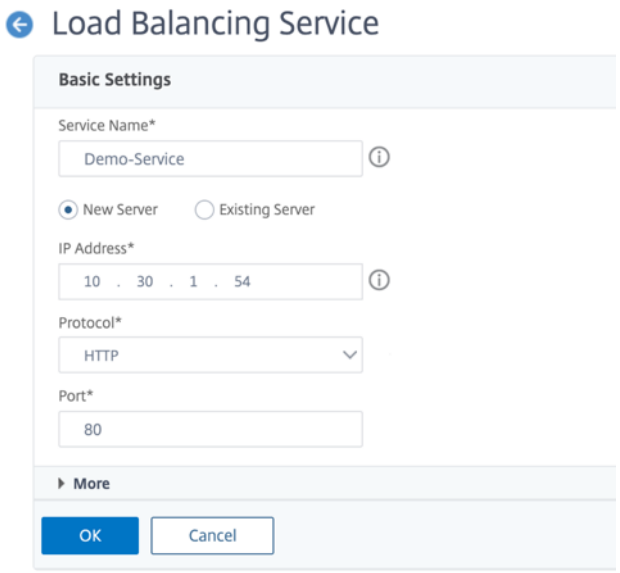


2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Externe IP-Adresse der Weiterleitungsregel, die als VIP auf ADC hinzugefügt wird) und Port hinzu, und klicken Sie auf **OK**.



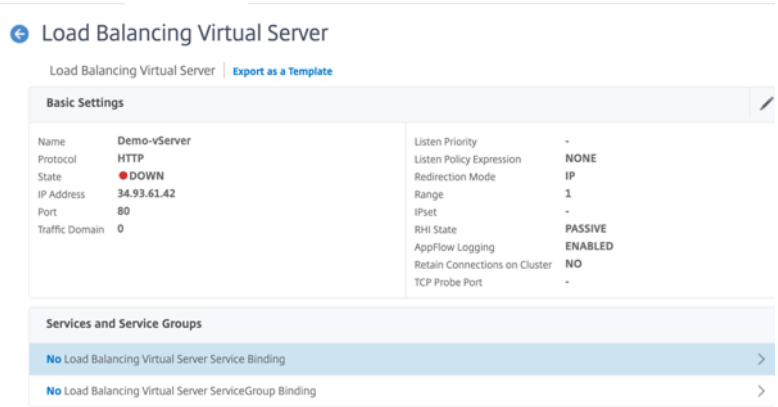
Schritt 2. Fügen Sie einen Dienst oder eine Dienstgruppe hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

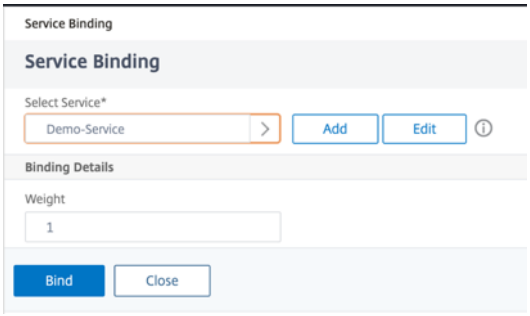


Schritt 3. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastenausgleichsserver.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 1**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.



4. Wählen Sie den in **Schritt 3**konfigurierten Dienst aus und klicken Sie auf “ **Binden**”.



5. Speichern Sie die Konfiguration.

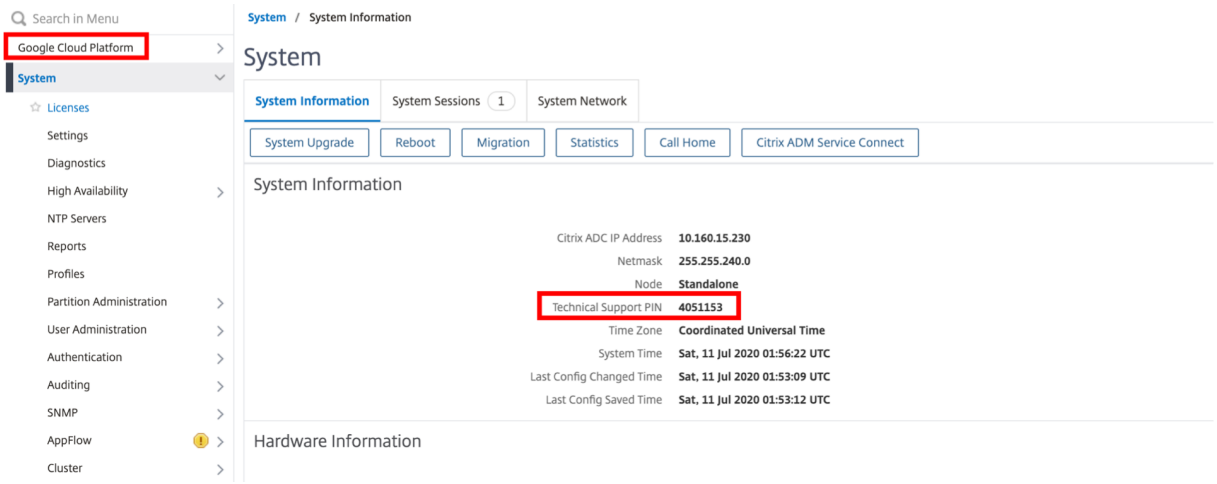
Problembehandlung bei einer VPX-Instanz auf GCP

May 11, 2023

Die Google Cloud Platform (GCP) bietet Konsolenzugriff auf eine NetScaler VPX-Instanz. Sie können nur debuggen, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz einzusehen, greifen Sie auf die Konsole zu und überprüfen Sie die **Systemprotokolldateien**.

NetScaler unterstützt gebührenpflichtige NetScaler VPX-Instances (Utility-Lizenz mit Stundengebühr) auf GCP. Um eine Support-Anfrage einzureichen, suchen Sie nach Ihrer GCP-Kontonummer und Ihrem Support-PIN-Code und wenden Sie sich an den NetScaler-Support. Sie werden gebeten, Ihren Namen und Ihre E-Mail-Adresse anzugeben. Um die Support-PIN zu finden, melden Sie sich an der VPX-GUI an und navigieren Sie zur **Systemseite** .

Hier ist ein Beispiel für eine Systemseite, die die Support-PIN zeigt.



Jumbo-Frames auf NetScaler VPX-Instanzen

May 11, 2023

NetScaler VPX-Appliances unterstützen das Empfangen und Senden von Jumbo-Frames mit bis zu 9216 Byte an IP-Daten. Jumbo-Frames können große Dateien effizienter übertragen als dies mit der standardmäßigen IP-MTU-Größe von 1500 Byte möglich ist.

Eine NetScaler-Appliance kann Jumbo-Frames in den folgenden Bereitstellungsszenarien verwenden:

- Jumbo zu Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Jumbo-Frames.
- Von Non-Jumbo zu Jumbo. Die Appliance empfängt Daten als reguläre Frames und sendet sie als Jumbo-Frames.
- Jumbo bis Non-Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als reguläre Frames.

Weitere Informationen finden Sie unterKonfigurieren der Unterstützung von Jumbo Frames auf einer NetScaler Appliance.

Unterstützung für Jumbo Frames ist auf NetScaler VPX -Appliances verfügbar, die auf den folgenden Virtualisierungsplattformen ausgeführt werden:

- VMware ESX
- Linux-KVM-Plattform
- Citrix XenServer
- Amazon Web Services (AWS)

Jumbo-Frames auf VPX-Appliances funktionieren ähnlich wie Jumbo-Frames auf MPX-Appliances. Weitere Informationen zu Jumbo Frames und ihren Anwendungsfällen finden Sie unter Konfiguration von Jumbo Frames auf MPX-Appliances. Die Anwendungsfälle von Jumbo-Frames auf MPX-Appliances gelten auch für VPX-Appliances.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die auf VMware ESX ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf dem VMware ESX-Server ausgeführt wird:

1. Stellen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich von 1501-9000 ein. Verwenden Sie die CLI oder GUI, um die MTU-Größe festzulegen. Die NetScaler VPX-Appliances, die auf VMware ESX laufen, unterstützen das Empfangen und Senden von Jumbo-Frames, die nur bis zu 9000 Byte an IP-Daten enthalten.

2. Legen Sie die gleiche MTU-Größe auf den entsprechenden physischen Schnittstellen des VMware ESX-Servers mithilfe der Verwaltungsanwendungen fest. Weitere Informationen zum Festlegen der MTU-Größe auf den physischen Schnittstellen von VMware ESX finden Sie unter http://vmware.com/.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die auf dem Linux-KVM-Server ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf einem Linux-KVM-Server ausgeführt wird:

1. Stellen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich 1501—9216 ein. Verwenden Sie die NetScaler VPX CLI oder GUI, um die MTU-Größe festzulegen.
2. Stellen Sie dieselbe MTU-Größe auf den entsprechenden physischen Schnittstellen eines Linux-KVM-Servers ein, indem Sie dessen Verwaltungsanwendungen verwenden. Weitere Hinweise zum Festlegen der MTU-Größe auf den physischen Schnittstellen von Linux-KVM finden Sie unter. http://www.linux-kvm.org/

Konfigurieren Sie Jumbo-Frames für eine VPX-Instanz, die auf Citrix XenServer ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf Citrix XenServer ausgeführt wird:

1. Stellen Sie mithilfe von XenCenter eine Verbindung zum XenServer her.
2. Fahren Sie alle VPX-Instanzen herunter, die die Netzwerke verwenden, für die die MTU geändert werden muss.
3. Wählen Sie auf der Registerkarte **Netzwerk** das Netzwerk — Netzwerk 0/1/2 aus.
4. Wählen Sie **Eigenschaften** und bearbeiten Sie MTU.

Nachdem Sie die Jumbo-Frames auf dem XenServer konfiguriert haben, können Sie die Jumbo-Frames auf der ADC-Appliance konfigurieren. Weitere Informationen finden Sie unterKonfigurieren der Unterstützung von Jumbo Frames auf einer NetScaler Appliance.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die in AWS ausgeführt wird

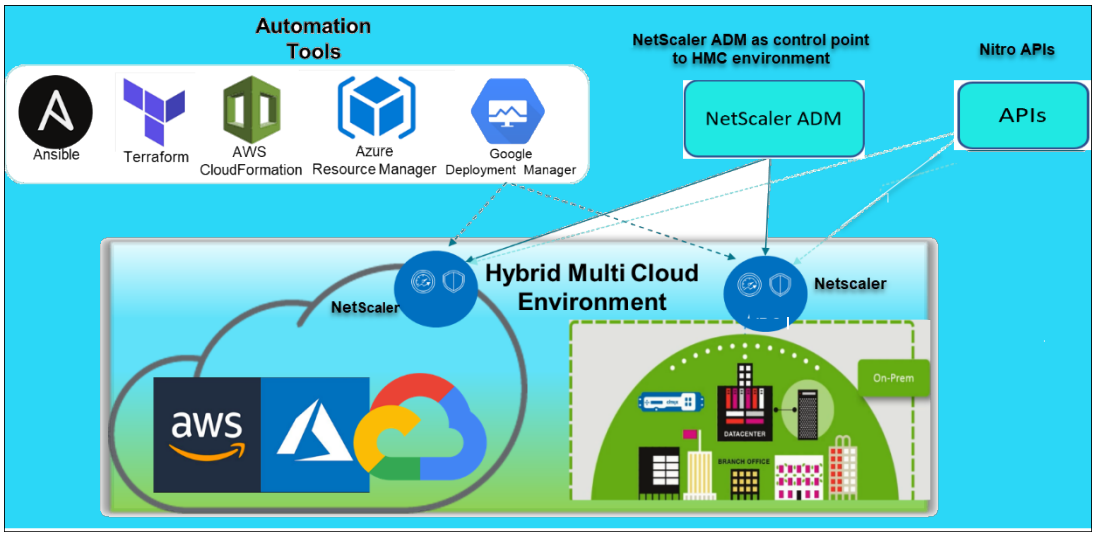
Konfiguration auf Hostebene ist für VPX unter Azure nicht erforderlich. Um Jumbo Frames auf VPX zu konfigurieren, befolgen Sie die Schritte unter Konfigurieren von Jumbo Frames Support auf einer NetScaler Appliance.

Bereitstellung und Konfigurationen von NetScaler automatisieren

June 19, 2023

NetScaler bietet mehrere Tools zur Automatisierung Ihrer ADC-Bereitstellungen und Konfigurationen. Dieses Dokument enthält eine kurze Zusammenfassung verschiedener Automatisierungstools und Verweise auf verschiedene Automatisierungsressourcen, mit denen Sie ADC-Konfigurationen verwalten können.

Die folgende Abbildung bietet einen Überblick über die NetScaler-Automatisierung in einer Hybrid-Multi-Cloud-Umgebung (HMC).



Automatisieren Sie NetScaler mit NetScaler ADM

NetScaler ADM fungiert als Kontrollpunkt für die Automatisierung Ihrer verteilten ADC-Infrastruktur. Das NetScaler ADM bietet umfassende Automatisierungsfunktionen von der Bereitstellung von ADC-Appliances bis hin zum Upgrade. Im Folgenden sind die wichtigsten Automatisierungsfunktionen von ADM aufgeführt:

- Provisioning von NetScaler VPX-Instanzen auf AWS
- Provisioning von NetScaler VPX-Instanzen auf Azure
- StyleBooks
- Konfigurationsaufträge
- Konfigurationsaudit
- ADC-Aktualisierungen
- SSL Zertifikatsverwaltung
- Integrationen - GitHub, ServiceNow, Integrationen von Ereignisbenachrichtigungen

NetScaler ADM Blogs und Videos zur Automatisierung

- Anwendungsmigrationen mit StyleBooks
- Integrieren Sie ADC-Konfigurationen mit CI/CD mithilfe von ADM StyleBooks
- Vereinfachung der Public Cloud NetScaler-Bereitstellungen durch ADM
- 10 Möglichkeiten, wie NetScaler ADM Service einfachere NetScaler-Upgrades unterstützt

NetScaler ADM bietet auch APIs für seine verschiedenen Funktionen, die NetScaler ADM und NetScaler als Teil der gesamten IT-Automatisierung integrieren. Weitere Informationen finden Sie unter NetScaler ADM Service-APIs.

Automatisieren Sie NetScaler mit Terraform

Terraform ist ein Tool, das Infrastruktur als Code-Ansatz zur Bereitstellung und Verwaltung von Cloud, Infrastruktur oder Service verwendet. NetScaler-Terraform-Ressourcen sind in GitHub zur Verwendung verfügbar. Lesen Sie GitHub für eine ausführliche Dokumentation und Verwendung.

- NetScaler Terraform-Module zur Konfiguration von ADC für verschiedene Anwendungsfälle wie Load Balancing und GSLB
- Terraform Cloud-Skripts zur Bereitstellung von ADC in AWS
- Terraform-Cloud-Skripts zur Bereitstellung von ADC in Azure
- Terraform-Cloud-Skripte zur Bereitstellung von ADC in GCP
- Blau-grüne Bereitstellung mit NetScaler VPX und Azure-Pipelines

Blogs und Videos auf Terraform für die ADC-Automatisierung

- Automatisieren Sie Ihre NetScaler-Bereitstellungen mit Terraform
- Bereitstellung und Konfiguration von ADC im HA-Setup in AWS mithilfe von Terraform

Automatisieren Sie NetScaler mit Consul-Terraform-Sync

Mit dem NetScaler Consul-Terraform-Sync (CTS) -Modul können Anwendungsteams automatisch neue Instanzen von Diensten zu NetScaler hinzufügen oder entfernen. Es ist nicht erforderlich, manuelle Tickets für IT-Administratoren oder Netzwerkteams zu erheben, um die erforderlichen Änderungen der ADC-Konfiguration vorzunehmen.

- NetScaler Consul-Terraform-Sync-Modul für die Automatisierung der Netzwerkinfrastruktur
- Gemeinsames Webinar von Citrix-HashiCorp: Dynamisches Networking mit Consul-Terraform-Sync für Terraform Enterprise und NetScaler

Automatisieren Sie NetScaler mit Ansible

Ansible ist ein Open-Source-Tool zur Softwarebereitstellung, Konfigurationsverwaltung und Anwendungsbereitstellung, das die Infrastruktur als Code ermöglicht. NetScaler Ansible-Module und Beispiel-Playbooks können in GitHub zur Verwendung gefunden werden. Lesen Sie GitHub für eine ausführliche Dokumentation und Verwendung.

- Ansible-Module zur Konfiguration von ADC
- Dokumentation/Referenzhandbuch zu ADC Ansible-Modulen
- Ansible-Module für ADM

Citrix ist ein zertifizierter Ansible Automation Partner. Benutzer mit einem Red Hat Ansible Automation Platform-Abonnement können von Red Hat Automation Hubaus auf NetScaler Collections zugreifen.

Automatisierungsblogs von Terraform und Ansible

- Citrix wurde zum HashiCorp-Integrationspartner des Jahres ernannt
- Citrix ist jetzt zertifizierter Red Hat Ansible Automation Platform Partner
- Terraform und Ansible Automation für App-Bereitstellung und Sicherheit

Public-Cloud-Vorlagen für ADC-Bereitstellungen

Öffentliche Cloudvorlagen vereinfachen die Bereitstellung Ihrer Bereitstellungen in Public Clouds. Für verschiedene Umgebungen stehen verschiedene NetScaler-Vorlagen zur Verfügung. Einzelheiten zur Verwendung finden Sie in den jeweiligen GitHub-Repositorys.

AWS-CFTs:

- CFTs zur Bereitstellung von NetScaler VPX auf AWS

Azure Resource Manager (ARM)-Vorlagen:

- ARM-Vorlagen zur Bereitstellung von NetScaler VPX auf Azure

Google Cloud-Bereitstellungsmanager (GDM) -Vorlagen:

- GDM-Vorlagen zur Bereitstellung von NetScaler VPX bei Google

Videos auf Vorlagen

- Bereitstellen von NetScaler HA in AWS mithilfe der CloudFormation-Vorlage
- Bereitstellen von NetScaler HA über Availability Zones hinweg mit AWS QuickStart
- NetScaler HA-Bereitstellung in GCP mit GDM-Vorlagen

AWS Quick Starts

- NetScaler Web App Firewall — Schnellstart
- AWS Quick Start für NetScaler VPX für Webanwendungen auf AWS

NITRO-APIs

Mit dem NetScaler NITRO-Protokoll können Sie die NetScaler-Appliance programmgesteuert konfigurieren und überwachen, indem Sie Schnittstellen für den Representational State Transfer (REST) verwenden. Daher können NITRO-Anwendungen in jeder Programmiersprache entwickelt werden. Für Anwendungen, die in Java oder .NET oder Python entwickelt werden müssen, werden NITRO-APIs durch relevante Bibliotheken bereitgestellt, die als separate Software Development Kits (SDKs) gepackt sind.

- NITRO-API-Dokumentation
- NetScaler-API-Referenz
- Beispiel einer ADC-Anwendungsfallkonfiguration mit NITRO API

Häufig gestellte Fragen

August 4, 2023

Der folgende Abschnitt hilft Ihnen bei der Kategorisierung der FAQs basierend auf Citrix Application Delivery Controller (ADC) VPX.

- Feature und Funktionalität
- Verschlüsselung
- Preisgestaltung und Verpackung
- NetScaler VPX Express
- Hypervisor
- Kapazitätsplanung oder -größe
- Systemanforderungen
- Weitere technische FAQs

Feature und Funktionalität

Was ist NetScaler VPX?

NetScaler VPX ist eine virtuelle ADC-Appliance, die auf einem Hypervisor gehostet werden kann, der auf Industriestandard-Servern installiert ist.

Enthalten NetScaler VPX alle Funktionen zur Optimierung von Webanwendungen als ADC-Appliances?

Ja. NetScaler VPX umfasst alle Lastenausgleich, Datenverkehrsverwaltung, Anwendungsbeschleunigung, Anwendungssicherheit (einschließlich NetScaler Gateway und Citrix Application Firewall) und Offload-Funktionen. Einen vollständigen Überblick über die Funktion und Funktionalität von NetScaler finden Sie unter Anwendungsbereitstellung auf Ihre Weise.

Gibt es Einschränkungen bei der Citrix Application Firewall bei der Verwendung auf NetScaler VPX?

Citrix Application Firewall auf NetScaler VPX bietet denselben Sicherheitsschutz wie auf NetScaler-Appliances. Die Leistung oder der Durchsatz der Citrix Application Firewall variiert je nach Plattform.

Gibt es Unterschiede zwischen NetScaler Gateway auf NetScaler VPX und NetScaler Gateway auf NetScaler-Appliances?

Funktional sind sie identisch. NetScaler Gateway auf NetScaler VPX unterstützt alle NetScaler Gateway-Funktionen, die in NetScaler Softwareversion 9.1 verfügbar sind. Da NetScaler-Appliances jedoch dedizierte SSL-Beschleunigungshardware bieten, bietet sie eine größere SSL-VPN-Skalierbarkeit als eine NetScaler VPX-Instanz.

Abgesehen von dem offensichtlichen Unterschied, auf einem Hypervisor laufen zu können, wie unterscheidet sich NetScaler VPX von physischen NetScaler-Appliances?

Es gibt zwei Hauptbereiche, in denen Kunden Verhaltensunterschiede feststellen. Das erste ist, dass NetScaler VPX nicht die gleiche Leistung bieten kann wie viele NetScaler-Appliances. Das zweite ist, dass NetScaler-Appliances zwar über eine eigene L2-Netzwerkfunktionalität verfügen, NetScaler VPX jedoch für seine L2-Netzwerkdienste auf den Hypervisor angewiesen ist. Im Allgemeinen schränkt dies nicht ein, wie der NetScaler VPX bereitgestellt werden kann. Es kann bestimmte L2-Funktionen geben, die auf einer physischen NetScaler-Appliance konfiguriert sind und auf dem zugrunde liegenden Hypervisor konfiguriert werden müssen.

Wie spielt NetScaler VPX eine Rolle auf dem Markt für Anwendungsbereitstellung?

NetScaler VPX ändert das Spiel auf dem Markt für Anwendungsbereitstellung auf folgende Weise:

- Indem eine NetScaler-Appliance noch erschwinglicher wird, ermöglicht NetScaler VPX jeder IT-Organisation, eine NetScaler-Appliance bereitzustellen. Dies ist nicht nur für ihre geschäftskritischsten Webanwendungen gedacht, sondern für alle ihre Webanwendungen.
- NetScaler VPX ermöglicht es Kunden, Netzwerk und Virtualisierung in ihren Rechenzentren weiter zu konvergieren. NetScaler VPX kann nicht nur zur Optimierung von Webanwendungen verwendet werden, die auf virtualisierten Servern gehostet werden. Darüber hinaus kann die Bereitstellung von Webanwendungen selbst zu einem virtualisierten Service werden, der einfach und schnell überall bereitgestellt werden kann. IT-Organisationen verwenden die Standard-Rechenzentrumsprozesse für Aufgaben wie Bereitstellung, Automatisierung und Rückladung für die Infrastruktur zur Bereitstellung von Webanwendungen.
- NetScaler VPX eröffnet neue Bereitstellungsarchitekturen, die nicht praktisch sind, wenn nur physische Appliances verwendet werden. NetScaler VPX und NetScaler MPX Appliances können als Basis verwendet werden, die auf die individuellen Bedürfnisse der jeweiligen Anwendung zugeschnitten sind, um prozessorintensive Aktionen wie Komprimierung und Anwendungsfirewall zu verarbeiten. Am Rechenzentrumsrand übernehmen NetScaler MPX-Appliances netzwerkweite Aufgaben mit hohem Volumen wie die anfängliche Datenverkehrsverteilung, SSL-Verschlüsselung oder Entschlüsselung, Denial-of-Service-Angriffsprävention (DoS) und den globalen Lastenausgleich. Die Kopplung von leistungsstarken NetScaler MPX-Appliances mit der einfach bereitzustellenden virtuellen NetScaler VPX Appliance bringt beispiellose Flexibilität und Anpassungsfunktionen für moderne, große Rechenzentrumsumgebungen und reduziert gleichzeitig die Gesamtkosten für Rechenzentren.

Wie passt NetScaler VPX in unsere Citrix Delivery Center-Strategie?

Mit der Verfügbarkeit von NetScaler VPX ist das gesamte Citrix Delivery Center-Angebot als virtualisiertes Angebot verfügbar. Das gesamte Citrix Delivery Center profitiert von den leistungsstarken Verwaltungs-, Bereitstellungs-, Überwachungs- und Berichtsfunktionen, die in Citrix XenCenter verfügbar sind. Dies kann schnell in fast jeder Umgebung eingesetzt und von überall aus zentral verwaltet werden. Mit einer integrierten, virtualisierten Anwendungsbereitstellungsinfrastruktur können Unternehmen Desktops, Client-Server-Anwendungen und Webanwendungen bereitstellen.

Verschlüsselung

Unterstützt NetScaler VPX SSL-Offload?

Ja. NetScaler VPX führt jedoch die gesamte SSL-Verarbeitung in Software durch, sodass NetScaler VPX nicht die gleiche SSL-Leistung wie NetScaler-Appliances bietet. NetScaler VPX kann bis zu 750 neue

SSL-Transaktionen pro Sekunde unterstützen.

Beschleunigen SSL-Karten von Drittanbietern, die auf dem Server installiert sind, auf dem NetScaler VPX gehostet wird, die SSL-Verschlüsselung oder -Entschlüsselung?

Nein. Die Unterstützung von SSL-Karten von Drittanbietern kann den NetScaler VPX nicht bestimmten Hardwareimplementierungen zuordnen. Dies verringert die Fähigkeit eines Unternehmens, NetScaler VPX flexibel überall im Rechenzentrum zu hosten. NetScaler MPX-Appliances müssen verwendet werden, wenn mehr SSL-Durchsatz erforderlich ist, als NetScaler VPX bietet.

Unterstützt NetScaler VPX dieselben Verschlüsselungsverschlüsselungen wie physische NetScaler-Appliances?

VPX unterstützt alle Verschlüsselungsverschlüsselungen als physische NetScaler-Appliances, mit Ausnahme der ECDSA.

Was ist der SSL-Transaktionsdurchsatz von NetScaler VPX?

Informationen zum Durchsatz von SSL-Transaktionen finden Sie im NetScaler VPX Datenblatt .

Preisgestaltung und Verpackung

Wie ist NetScaler VPX verpackt?

Die Auswahl von NetScaler VPX ähnelt der Auswahl von NetScaler-Appliances. Zunächst wählt der Kunde die NetScaler Edition basierend auf seinen Funktionsanforderungen aus. Anschließend wählt der Kunde die spezifische NetScaler VPX -Bandbreitenstufe basierend auf den Durchsatzanforderungen aus. NetScaler VPX ist in Standard-, Advanced- und Premium-Editionen verfügbar. NetScaler VPX bietet von 10 Mbit/s (VPX 10) bis 100 Gbit/s (VPX 100G). Weitere Details finden Sie im NetScaler VPX Datenblatt.

Ist der Preis für NetScaler VPX für alle Hypervisoren gleich?

Ja.

Werden dieselben NetScaler-SKUs für VPX auf allen Hypervisoren verwendet?

Ja.

Kann eine NetScaler VPX-Lizenz von einem Hypervisor auf einen anderen verschoben werden (z. B. von VMware auf Hyper-V)?

Ja. NetScaler VPX-Lizenzen sind unabhängig vom zugrunde liegenden Hypervisor. Wenn Sie sich entscheiden, die virtuelle NetScaler VPX-Maschine von einem Hypervisor auf einen anderen zu verschieben, müssen Sie keine neue Lizenz erwerben. Möglicherweise müssen Sie jedoch die vorhandene NetScaler VPX-Lizenz neu hosten.

Können NetScaler VPX-Instanzen aktualisiert werden?

Ja. Sowohl die Durchsatzbeschränkungen als auch die NetScaler Family Edition können aktualisiert werden. Upgrade-SKUs für beide Upgrade-Typen sind verfügbar.

Wie viele Lizenzen benötige ich, wenn ich NetScaler VPX in einem Hochverfügbarkeitspaar bereitstellen möchte?

Wie bei physischen NetScaler-Appliances erfordert eine NetScaler-Hochverfügbarkeitskonfiguration zwei aktive Instanzen. Daher muss der Kunde zwei Lizenzen erwerben.

NetScaler VPX Express und kostenlose 90-Tage-Testversion

Enthalten NetScaler VPX Express alle NetScaler-Standardfunktionen? Umfasst es NetScaler Gateway und Load Balancing für Citrix Virtual Apps (ehemals XenApp), Webinterface und XML-Broker?

Ja. NetScaler VPX Express enthält die volle NetScaler Standardfunktionalität. Ab NetScaler Version 12.0—56.20 änderte Citrix das VPX Express-Verhalten.

Enthalten NetScaler VPX Express alle NetScaler-Standardfunktionen? Umfasst es NetScaler Gateway und Lastausgleich für Citrix Virtual Apps Webinterface und XML-Broker?

Ab NetScaler Version 12.0—56.20 bietet VPX Express das Featureset NetScaler Standard Edition mit Ausnahme der Gateway-Funktionalität. Vor der Version 12.0—56.20 enthält VPX alle Funktionen der Standardausgabe.

Benötigt NetScaler VPX Express eine Lizenz?

Mit der neuen NetScaler VPX Express-Version (12.0—56.20 und neuer) ist VPX Express kostenlos und benötigt keine Lizenzdateien für die Installation und wird unverbindlich geliefert. Wenn Sie bereits über eine VPX Express-Lizenz verfügen, bleibt das vorherige VPX Express-Verhalten erhalten. Wenn

die VPX *Express-Lizenzdatei* entfernt und die Version 12.0—56.20 verwendet wird, wird das neue VPX-Express-Verhalten wirksam.

Lauf die NetScaler VPX Express-Lizenz ab?

Mit dem neuen VPX Express nein. Es gibt keine Lizenz und kein Ablaufdatum. Wenn Sie bereits eine VPX Express-Lizenz besitzen, läuft die Lizenz ein Jahr nach dem Download ab.

Enthalten NetScaler VPX Express die fünf kostenlosen NetScaler Gateway Concurrent-Lizenzen?

Ja, wenn Sie eine VPX-Express-Lizenz besitzen.

Gibt es ein Limit, wie viele NetScaler VPX Expresses ein Kunde herunterladen kann?

Fünf.

Unterstützt NetScaler VPX Express dieselben Verschlüsselungsverschlüsselungen wie NetScaler MPX-Appliances?

Für die allgemeine Verfügbarkeit sind dieselben starken Verschlüsselungsverschlüsselungen, die auf NetScaler-Appliances unterstützt werden, für NetScaler VPX und NetScaler VPX Express verfügbar. Es unterliegt denselben Import- oder Exportvorschriften.

Kann ich technische Supportfälle für NetScaler VPX Express einreichen?

Nein. Eine NetScaler VPX-Lizenz für den Einzelhandel wie VPX-10, VPX-200, VPX-1000, VPX-3000 ist erforderlich, um technische Supportfälle einzureichen. NetScaler VPX Express-Benutzer können jedoch sowohl das NetScaler VPX Knowledge Center verwenden als auch über die Z-Diskussionsforen Hilfe von der Community anfordern.

Kann NetScaler VPX Express auf eine Einzelhandelsversion aktualisiert werden?

Ja. Erwerben Sie einfach die NetScaler VPX-Lizenz für den Einzelhandel, die Sie benötigen, und wenden Sie dann die entsprechende Lizenz auf die NetScaler VPX Express-Instanz an.

Hypervisor

Welche VMware-Versionen unterstützt NetScaler VPX?

NetScaler VPX unterstützt VMware ESX und ESXi für Versionen 3.5 oder höher. Weitere Informationen finden Sie unter Supportmatrix und Nutzungsrichtlinien

Wie viele virtuelle Netzwerkschnittstellen können Sie für VMware einem VPX zuweisen?

Sie können einem NetScaler VPX bis zu 10 virtuelle Netzwerkschnittstellen zuweisen.

Wie können wir von vSphere auf die NetScaler VPX-Befehlszeile zugreifen?

Der VMware vSphere-Client bietet über eine Konsolenregisterkarte integrierten Zugriff auf die NetScaler VPX-Befehlszeile. Sie können auch jeden SSH- oder Telnet-Client verwenden, um auf die Befehlszeile zuzugreifen. Sie können die NSIP-Adresse des NetScaler VPX im SSH- oder Telnet-Client verwenden.

Wie können Sie auf die NetScaler VPX GUI zugreifen?

Um auf die NetScaler VPX GUI zuzugreifen, geben Sie die NSIP des NetScaler VPX, beispielsweise `http://NSIP address`, in das Adressfeld eines beliebigen Browsers ein.

Können zwei NetScaler VPX-Instanzen, die auf demselben VMware ESX installiert sind, in einem Hochverfügbarkeits-Setup konfiguriert werden?

Ja, aber es wird nicht empfohlen. Ein Hardwarefehler würde sich auf beide NetScaler VPX-Instanzen auswirken.

Können zwei NetScaler VPX-Instanzen, die auf zwei verschiedenen VMware ESX-Systemen ausgeführt werden, in einem Hochverfügbarkeits-Setup konfiguriert werden?

Ja. Es wird in einem Hochverfügbarkeits-Setup empfohlen.

Werden für die VMware interface-bezogene Ereignisse auf NetScaler VPX unterstützt?

Nein. Interface-bezogene Ereignisse werden nicht unterstützt.

Werden für die VMware getaggte VLANs auf NetScaler VPX unterstützt?

Ja. NetScaler-markierte VLANs werden ab Version 11.0 und höher von NetScaler VPX unterstützt. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

Werden Link-Aggregation und LACP für VMware auf NetScaler VPX unterstützt?

Nein. Link Aggregation und LACP werden für NetScaler VPX nicht unterstützt. Die Link-Aggregation muss auf VMware-Ebene konfiguriert werden.

Wie greifen wir auf die NetScaler VPX-Dokumentation zu?

Die Dokumentation ist über die NetScaler VPX GUI verfügbar. Nachdem Sie sich angemeldet haben, wählen Sie die Registerkarte **Dokumentation** .

Kapazitätsplanung oder -größe

Welche Leistung kann ich mit NetScaler VPX erwarten?

NetScaler VPX bietet eine gute Leistung. Ein bestimmtes Leistungsniveau, das mit NetScaler VPX erreicht werden kann, finden Sie im NetScaler VPX Datenblatt .

Wie können wir die maximale Leistung einer NetScaler Instanz schätzen, da die CPU-Leistung des Servers variiert?

Die Verwendung einer schnelleren CPU kann zu einer höheren Leistung führen (bis zu dem von der Lizenz zulässigen Maximum), während die Verwendung einer langsameren CPU die Leistung sicherlich einschränken kann.

Sind NetScaler VPX Bandbreiten- oder Durchsatzbeschränkungen für eingehenden Datenverkehr oder sowohl eingehenden als auch ausgehenden Datenverkehr?

NetScaler VPX-Bandbreitenbeschränkungen werden nur für den Datenverkehr durchgesetzt, der an den NetScaler eingeht, unabhängig davon, ob der Anforderungsverkehr oder der Antwortverkehr erfolgt. Dies zeigt an, dass ein NetScaler VPX-1000 (zum Beispiel) sowohl 1 Gbit/s eingehenden Datenverkehr als auch 1 Gbit/s ausgehenden Datenverkehr gleichzeitig verarbeiten kann. Eingehender und ausgehender Datenverkehr ist nicht identisch mit Anforderungs- und Antwortdatenverkehr. Für den NetScaler ist sowohl der Datenverkehr, der von Endpunkten (Anforderungsverkehr) kommt, als auch Datenverkehr von Ursprungsservern (Antwortverkehr) “eingehend” (d. h. in den NetScaler).

Können mehrere Instanzen von NetScaler VPX auf demselben Server ausgeführt werden?

Ja. Stellen Sie jedoch sicher, dass der physische Server über genügend CPU- und E/A-Kapazität verfügt, um die gesamte auf dem Host ausgeführte Arbeitslast zu unterstützen, da sonst die Leistung von NetScaler VPX beeinträchtigt werden kann.

Wenn mehr als eine Instanz von NetScaler VPX auf einem physischen Server ausgeführt wird, was ist die Mindestanforderungen für die Hardware pro NetScaler VPX-Instanz?

Jeder NetScaler VPX Instanz muss 2 GB physischen RAM, 20 GB Speicherplatz und 2 vCPUs zugewiesen werden.

> **Hinweis:**
>
> Der NetScaler VPX ist eine latenzempfindliche, leistungsstarke virtuelle Appliance. Um die erwartete Leistung zu erzielen, benötigt die Appliance eine vCPU-Reservierung, Speicherreservierung und vCPU-Pinning auf dem Host. Außerdem muss Hyper-Threading auf dem Host deaktiviert werden. Wenn der Host diese Anforderungen nicht erfüllt, treten Probleme wie Hochverfügbarkeitsfailover, CPU-Anstieg innerhalb der VPX-Instanz, Trägheit beim Zugriff auf die VPX CLI, Absturz des Pitboss-Daemons, Paketausfälle und ein niedriger Durchsatz auf.
>
> Stellen Sie sicher, dass jede VPX-Instanz die vordefinierten Bedingungen erfüllt.

Kann ich NetScaler VPX und andere Anwendungen auf demselben Server hosten?

Ja. Beispielsweise können NetScaler VPX, Citrix Virtual Apps Webinterface und Citrix Virtual Apps XML Broker alle virtualisiert werden und auf demselben Server ausgeführt werden. Stellen Sie für eine optimale Leistung sicher, dass der physische Host über genügend CPU- und E/A-Kapazität verfügt, um alle laufenden Workloads zu unterstützen.

Wird das Hinzufügen von CPU-Kernen zu einer einzelnen NetScaler VPX-Instanz die Leistung dieser Instanz erhöhen?

Abhängig von der Lizenz kann eine NetScaler VPX Instanz heute bis zu 4 vCPU verwenden. Das Hinzufügen einer zusätzlichen CPU zu einer NetScaler VPX-Instanz, die mehr CPUs verwenden kann, erhöht die Leistung.

Warum sieht NetScaler VPX so aus, als würde er mehr als 90% der CPU verbraucht, obwohl er im Leerlauf ist?

Es ist normales Verhalten und NetScaler-Appliances zeigen das gleiche Verhalten. Um die tatsächliche Ausdehnung der NetScaler VPX CPU-Auslastung anzuzeigen, verwenden Sie den Befehl stat CPU in der NetScaler CLI oder zeigen Sie die NetScaler VPX CPU-Auslastung von der NetScaler GUI an. Die NetScaler Paketverarbeitungs-Engine ist immer “auf der Suche nach Arbeit”, auch wenn keine Arbeit zu tun ist. Daher tut es alles, um die Kontrolle über die CPU zu übernehmen und sie nicht freizugeben. Auf einem Server, der mit NetScaler VPX und sonst nichts installiert ist, ergibt sich (aus der Sicht des Hypervisors), dass NetScaler VPX die gesamte CPU verbraucht. Ein Blick auf die CPU-Auslastung von

“innerhalb von NetScaler” (über die Befehlszeilenschnittstelle oder der GUI) liefert ein Bild der verwendeten NetScaler VPX CPU-Kapazität.

Systemanforderungen

Was sind die Mindestanforderungen an die Hardware für NetScaler VPX?

In der folgenden Tabelle werden die Mindestanforderungen an die Hardware für NetScaler VPX erläutert.

Typ	Anforderungen
Prozessor	Dual-Core-Server mit Intel Xeon oder AMD EPYC.
Speicher	Mindestens 2 GB. Es werden jedoch 4 GB empfohlen.
Datenträger	Mindestens 20 GB Festplatte.
Hypervisor	Citrix Hypervisor 5.6 oder höher, VMware ESX/ESXi 3.5 oder höher oder Windows Server 2008 R2 mit Hyper-V
Netzwerk-Konnek	Mindestens 100 Mbit/s, aber 1 Gbit/s wird empfohlen.
Netzwerkkarte	Eine NIC, die mit dem von Ihnen verwendeten Hypervisor kompatibel ist.

> **Hinweis:**
>
> Für kritische Bereitstellungen werden 4 GB Arbeitsspeicher für NetScaler VPX bevorzugt. Mit 2 GB Arbeitsspeicher arbeitet NetScaler VPX in einer Umgebung mit sehr eingeschränktem Arbeitsspeicher. Dies kann zu Skalierungs-, Leistungs- oder Stabilitätsproblemen führen.

Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu NetScaler VPX.

> **Hinweis:**
>
> Ab Version NetScaler 13.1 unterstützt die NetScaler VPX-Instanz auf dem VMware ESXi-Hypervisor AMD EPYC-Prozessoren.

Was ist Intel VT-x?

Diese Funktionen, die manchmal als “Hardware-Assist” oder “Virtualisierungsassistent” bezeichnet werden, erfassen sensible oder privilegierte CPU-Anweisungen, die vom Gastbetriebssystem an den

Hypervisor ausgeführt werden. Dies vereinfacht das Hosten von Gastbetriebssystemen (BSD für einen NetScaler VPX) auf dem Hypervisor.

Wie üblich sind VT-x?

Praktisch können alle Server, die innerhalb der letzten zwei Jahre ausgeliefert wurden, VT-x unterstützen. Viele Server werden mit deaktivierter Virtualisierungsunterstützung im BIOS ausgeliefert. Bevor Sie davon ausgehen, dass Sie NetScaler VPX nicht ausführen können, prüfen Sie, ob Sie diese Einstellung auf dem Server ändern müssen.

Gibt es eine Hardwarekompatibilitätsliste (HCL) für NetScaler VPX?

Solange der Server Intel VT-x unterstützt, muss NetScaler VPX auf jedem Server laufen, der mit dem zugrunde liegenden Hypervisor kompatibel ist. Eine umfassende Liste der unterstützten Plattformen finden Sie in der Hypervisor-HCL.

Auf welcher Version von NetScaler OS basiert NetScaler VPX?

NetScaler VPX basiert auf NetScaler 9.1 oder höheren Versionen.

Da NetScaler VPX auf BSD läuft, kann es nativ auf einem Server mit installiertem BSD Unix ausgeführt werden?

Nein. NetScaler VPX erfordert die Ausführung des Hypervisors. Detaillierte Hypervisor-Unterstützungen finden Sie im Datenblatt von NetScaler VPX.

Weitere technische FAQs

Funktioniert die Link-Aggregation auf einem physischen Server mit mehreren Netzwerkkarten?

LACP wird nicht unterstützt. Für den Citrix Hypervisor wird die statische Link-Aggregation unterstützt und hat Grenzen von vier Kanälen und sieben virtuellen Schnittstellen. Für VMware wird die statische Link-Aggregation in NetScaler VPX nicht unterstützt, kann aber auf VMware-Ebene konfiguriert werden.

Wird MAC-basierte Weiterleitung (MBF) auf VPX unterstützt? Gibt es Änderungen gegenüber der Implementierung der NetScaler-Appliance?

MBF wird unterstützt und verhält sich genauso wie bei der NetScaler-Appliance. Der Hypervisor schaltet grundsätzlich alle von NetScaler VPX empfangenen Pakete nach außen und umgekehrt.

Wie wird der NetScaler VPX-Upgrade-Prozess durchgeführt?

Upgrades werden genauso ausgeführt wie für NetScaler-Appliances: Laden Sie eine Kerneldatei herunter und verwenden Sie install ns oder das Upgrade-Dienstprogramm in der Benutzeroberfläche.

Wie werden Flash- und Datenträgerspeicher zugewiesen? Können wir es ändern?

/flash = 965M
/var = 14G
Jeder NetScaler VPX-Instanz müssen mindestens 2 GB Speicher zugewiesen werden. Das NetScaler VPX Disk-Image hatte eine Größe von 20 GB für Wartungszwecke, z. B. Platz für die Aufnahme und Speicherung von bis zu 4 GB Core-Dumps sowie Protokoll- und Trace-Dateien. Obwohl es möglich wäre, ein kleineres Datenträgerimage zu generieren, ist dies derzeit nicht geplant. `/flash` und `/var` sind beide im selben Datenträgerimage. Sie werden aus Kompatibilitätsgründen als separate Dateisysteme aufbewahrt.
Ausführliche Empfehlungen zur Speicherzuweisung finden Sie im NetScaler VPX-Datenblatt.

Können wir eine neue Festplatte hinzufügen, um den Speicherplatz auf der NetScaler VPX-Instanz zu erhöhen?

Ja. Ab NetScaler Release 13.1 Build 21.x haben Sie die Möglichkeit, den Speicherplatz auf der NetScaler VPX-Instanz zu vergrößern, indem Sie einen zweiten Datenträger hinzufügen. Wenn Sie den zweiten Datenträger bereitstellen, wird das Verzeichnis "/var/crash" automatisch auf diesem Datenträger bereitgestellt. Der zweite Datenträger wird zum Speichern von Kerndateien und zum Protokollieren verwendet. Bestehende Verzeichnisse, die zum Speichern von Kern- und Protokolldateien verwendet werden, funktionieren weiterhin wie zuvor.

> **Hinweis:**
>
> Nehmen Sie beim Downgrade der NetScaler-Appliance ein externes Backup vor, um Datenverlust zu vermeiden.

Informationen zum Anschließen eines neuen Festplattenlaufwerks (HDD) an eine NetScaler VPX-Instanz in einer Cloud finden Sie in den folgenden Abschnitten:

- Azure-Dokumentation

  > **Hinweis:**
  >
  > Um eine sekundäre Festplatte an VPX-Instanzen anzuhängen, die auf Azure bereitgestellt werden, stellen Sie sicher, dass die Azure-VM-Größen über eine lokale temporäre Festplatte verfügen. Weitere Informationen finden Sie unter Azure-VM-Größen ohne lokale temporäre Festplatte.

- AWS-Dokumentation

- GCP-Dokumentation

> **Warnung:**
>
> Nachdem Sie eine neue Festplatte zu VPX hinzugefügt haben, können einige der Skripts, die mit Dateien arbeiten, die auf die neue Festplatte verschoben wurden, unter den folgenden Bedingungen fehlschlagen:
>
> Wenn Sie den Shell-Befehl “Link” verwenden, um feste Links zu den Dateien zu erstellen, die auf eine neue Festplatte verschoben wurden.
>
> Alle diese Befehle müssen durch “ln -s” ersetzt werden, um einen symbolischen Link zu verwenden. Ändern Sie auch die fehlgeschlagenen Skripte entsprechend.

Was können wir erwarten, dass die NetScaler VPX Build-Nummerierung und die Interoperabilität mit anderen Builds berücksichtigt werden?

NetScaler VPX hat eine ähnliche Build-Nummerierung wie die 9.1. Cl (klassisch) und 9.1. Nc (nCore) Release, zum Beispiel 9.1_97.3.vpx, 9.1_97.3.nc und 9.1_97.3.cl.

Kann der NetScaler VPX Teil eines Hochverfügbarkeitssetups mit einer NetScaler-Appliance sein?

Keine unterstützte Konfiguration.

Befinden sich alle in NetScaler VPX sichtbaren Schnittstellen in direktem Zusammenhang mit der Anzahl der Schnittstellen auf dem Hypervisor?

Nein. Sie können bis zu sieben Schnittstellen (10 für VMware) über das NetScaler VPX Konfigurationsprogramm mit nur einer physischen Netzwerkkarte auf dem Hypervisor hinzufügen.

Kann Citrix Hypervisor XenMotion oder VMware VMotion oder Hyper-V Live-Migration verwendet werden, um aktive Instanzen von NetScaler VPX zu verschieben?

NetScaler VPX unterstützt keine XenMotion- oder Hyper-V-Live-Migration. vMotion wird ab Version NetScaler 12.1 unterstützt. Weitere Informationen finden Sie unter Versionshinweise.

Lizenzierungsübersicht

September 11, 2023

NetScaler bietet eine breite Palette von Produkteditionen und Lizenzmodellen für MPX- und VPX-Appliances, um den Anforderungen Ihres Unternehmens gerecht zu werden.

Für den ordnungsgemäßen Betrieb einer NetScaler-Appliance muss sie über eine der NetScaler Family Edition-Lizenzen verfügen. Die ADC-Produktlinie umfasst drei Familienausgaben:

- Standard Edition

  > **Hinweis**
  >
  > Die Standard Edition hat das Verkaufsende (EOS) erreicht und kann nur noch verlängert werden.

- Advanced Edition
- Premium Edition

Weitere Informationen finden Sie im Datenblatt. Das Datenblatt ist auf www.netscaler.comverfügbar.

Wählen Sie eine NetScaler-Edition aus. Wählen Sie dann ein MPX- oder VPX-Lizenzangebot basierend auf den folgenden Kriterien aus:

- Unbefristet und Abonnement (Jahres- und Stundenabonnement)
- vCPU und Bandbreite
- lokal und in der Cloud

NetScaler VPX Express-Lizenz

VPX Express für on-premises und Cloud-Bereitstellungen erfordert keine Lizenzdatei und bietet die folgenden Funktionen:

- 20 Mbit/s Bandbreite
- Webprotokollierung, Load Balancing, Content Switching, Cache-Umleitung, SSL-Offloading, Inhaltsfilterung, Umschreiben, IPv6-Protokollübersetzung, Responder, AppFlow, Clustering und CallHome
- Maximal 250 SSL-Sitzungen
- 20 Mbit/s SSL-Durchsatz

Sie können die VPX Express-Lizenz auf die folgenden zwei Optionen aktualisieren:

1. Eine eigenständige NetScaler VPX-Lizenz.
2. NetScaler Pooled Capacity Lizenz für VPX-Instanzen. Weitere Informationen finden Sie unter NetScaler PooledCapacity.

NetScaler Pooled Capacity-Lizenz

Verwenden Sie NetScaler Application Delivery Management (ADM), um ein Lizenzierungsframework zu erstellen, das eine gemeinsame Bandbreite und einen Instanzpool umfasst. Weitere Informationen

finden Sie unter NetScaler PooledCapacity.

> **Hinweis:**
>
> NetScaler ADM kann sowohl Pool-Lizenzen als auch Self Managed Pool-Lizenzen hosten. Um die erforderliche Lizenz zu verwenden, konfigurieren Sie den Lizenzserver auf NetScaler und überprüfen Sie die Kapazität aus dem entsprechenden Pool. Die ADC-CLI- und GUI-Konfigurationsschritte für die Pooled- und Self Managed Pool-Lizenz sind identisch.

NetScaler Self Managed Pool-Lizenz

Ab NetScaler Version 13.1 Build 30.x unterstützen NetScaler-Instances die Self Managed Pool-Lizenz. Mit dieser Lizenz können Sie das Hochladen von Lizenzdateien auf einen Lizenzserver vereinfachen und automatisieren. Verwenden Sie NetScaler ADM, um ein Lizenzierungsframework zu erstellen, das eine gemeinsame Bandbreite oder einen gemeinsamen vCPU- und Instanzpool umfasst.

Um die Self Managed Pool-Lizenz zu verwenden, konfigurieren Sie den Lizenzserver auf NetScaler für den `SelfManagedPool` Lizenzmodus und überprüfen Sie die erforderliche Kapazität. Verwenden Sie den `show ns license` Befehl nach dem Neustart der NetScaler Appliance, um die konfigurierte Lizenz zu ermitteln.

> **Wichtig**
>
> Wenn Ihr System mit einer Pooled Capacity-Lizenz konfiguriert ist, Sie jedoch zur Lizenz für selbstverwalteten Pool migrieren möchten, ohne den Datenverkehrsfluss zu beeinträchtigen, stellen Sie sicher, dass der Zielserver über die erforderliche Lizenz für den selbstverwalteten Pool verfügt.
>
> Sie können nur zwischen den folgenden kompatiblen Lizenzen migrieren:
>
> - Gebündelte Kapazität zum selbstverwalteten Pool und umgekehrt.
> - vCPU zu selbstverwalteter vCPU und umgekehrt.
>
> Führen Sie den folgenden Befehl aus, um die Lizenz zu migrieren:
>
> ```
> add ns licenseserver (<licenseServerIP> | <serverName>)-forceUpdateIP -licensemode [CICO | Pooled | SelfManagedPool | VCPU | SelfManagedvCPU]
> ```
>
> **Beispiel:**
>
> ```
> add licenseserver 192.0.2.246 -forceUpdateIP -licensemode selfManagedvcPU
> ```

Konfigurieren der Self Managed Pool-Lizenz mit der CLI

Führen Sie den folgenden Befehl aus, um die Lizenzserverkonfiguration zur NetScaler-Appliance hinzuzufügen:


```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    positive_integer>] -licensemode [CICO | Pooled | SelfManagedPool |
    VCPU | SelfManagedvCPU]
<!--NeedCopy-->
```

Beispiel:

```
add ns licenseserver 192.0.2.246 -port 27000 -licensemode
    SelfManagedPool
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der `show ns licenseserverpool` Befehl zeigt nur Lizenzen an, die auf dem angegebenen Lizenzmodus basieren. Daher werden die Lizenzen schneller abgerufen. Führen Sie den `show ns licenseserverpool -getallLicenses` Befehl aus, um eine Bestandsaufnahme aller Lizenzen zu erhalten. Wenn der Lizenzmodus nicht angegeben ist, werden die Pooled Capacity-Lizenzen standardmäßig angezeigt.

Führen Sie den folgenden Befehl aus, um die Systemkapazität zu ändern:

```
set ns capacity ((-bandwidth <positive_integer> -unit ( Gbps | Mbps ))
    | -platform <platform>) [-Edition <Edition>]
<!--NeedCopy-->
```

Beispiel:

```
set ns capacity -bandwidth 3 -unit gbps -edition enterprise
<!--NeedCopy-->
```

> Hinweis:
>
> Die Kapazität wurde aus dem Lizenzpool des Lizenzservers ausgecheckt.

Führen Sie den folgenden Befehl aus, um die NetScaler-Appliance neu zu starten:

```
reboot [-warm]
<!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um den Status aller lizenzierten Funktionen und den konfigurierten Lizenzmodus anzuzeigen:

```
show ns license
<!--NeedCopy-->
```

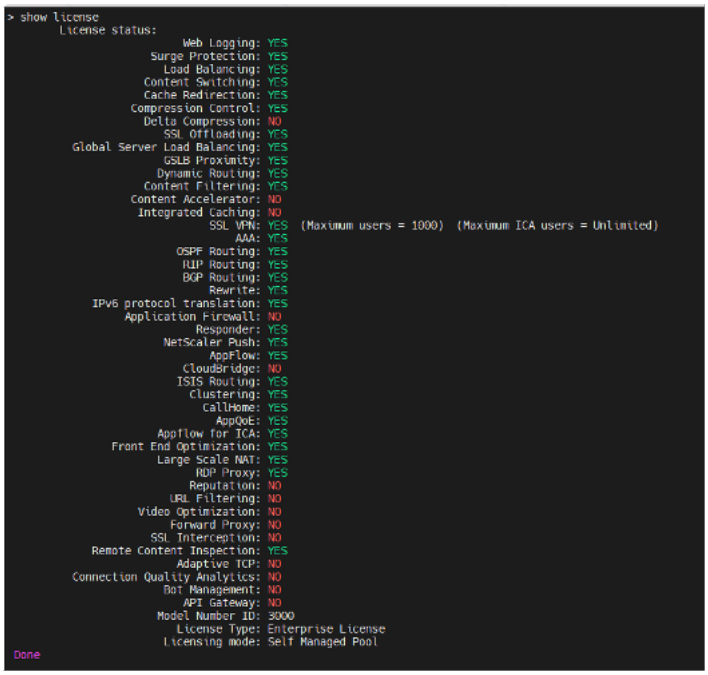

Beispielausgabe des Befehls `show ns licenseserverpool`:

```
> add licenseserver                -licensemode SelfManagedPool
 Done
> sh licenseserverpool
        Instance Total                      : 200
        Instance Available                  : 199
        Standard Bandwidth Total            : 10.00 Gbps
        Standard Bandwidth Available        : 10.00 Gbps
        Enterprise Bandwidth Total          : 10.00 Gbps
        Enterprise Bandwidth Available      : 7.00 Gbps
        Platinum Bandwidth Total            : 0 Mbps
        Platinum Bandwidth Available        : 0 Mbps
```

Beispielausgabe des Befehls `show ns licenseserverpool -getallLicenses`:

```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

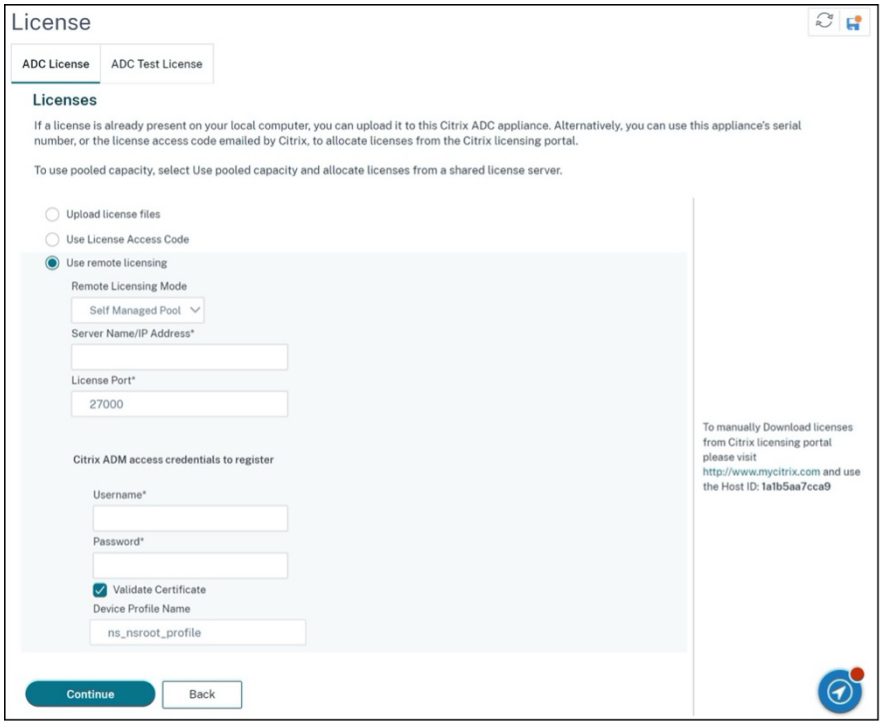
Beispielausgabe des Befehls `show license`:



Konfigurieren der Lizenz für den Self Managed Pool über die GUI

Führen Sie folgende Schritte aus, um die Self Managed Pool-Lizenz zu konfigurieren

1. Navigieren Sie zu **System > Lizenzen > ADC-Lizenz > Lizenzen verwalten > Neue Lizenz hinzufügen**.
2. Wählen Sie auf der Seite **Lizenzen** das Optionsfeld **Remote-Lizenzierung verwenden** und wählen Sie Ihren Lizenzmodus unter **Remote-Lizenzierungsmodus**aus.
3. Geben Sie die IP-Adresse des Servers und die Details zum Lizenzport ein.
4. Geben Sie die Anmeldeinformationen für den NetScaler ADM-Zugriff an.
5. Klicken Sie auf **Weiter**.



Zugehörige Ressourcen

Das Citrix Lizenzierungssystem

VPX-Lizenzierung in Cloud

Die VPX-Bereitstellung wird von Public Cloud-Anbietern wie Azure, AWS und Google unterstützt. Weitere Informationen finden Sie in den folgenden Dokumenten:

- VPX-Azure-Lizenz
- VPX-AWS-Lizenz
- VPX-GCP-Lizenz

Zuweisen und Anwenden einer Lizenz

August 4, 2023

In der NetScaler MPX- und VPX ADC-GUI können Sie Ihre Hardware-Seriennummer (HSN) oder Ihren Lizenzzugangscode verwenden, um Ihre Lizenzen zuzuweisen. Wenn auf Ihrem lokalen Computer bereits eine Lizenz vorhanden ist, können Sie sie alternativ auf die Appliance hochladen.

Für alle anderen Funktionen, wie die Rückgabe oder Neuzuweisung Ihrer Lizenz, müssen Sie das Lizenzportal verwenden. Optional können Sie weiterhin das Lizenzportal für die Lizenzzuweisung verwenden. Weitere Informationen finden Sie unter Verwenden von Verwalten von Lizenzen in My Account auf citrix.com.

Leitfaden zur Citrix Lizenzierung

Das Citrix Lizenzierungsleitfaden enthält auch Informationen zur Installation von Lizenzen in einer NetScaler-Appliance und zur Installation von Lizenzen in anderen NetScaler-Produkten. Weitere Informationen finden Sie im Citrix Licensing Guide.

Voraussetzungen

> **Hinweis**
>
> Erwerben Sie separate Lizenzen für jede Appliance in einem Hochverfügbarkeitspaar. Stellen Sie sicher, dass auf beiden Appliances dieselben Lizenzen installiert sind. Wenn Sie beispielsweise eine Premium-Lizenz für eine Appliance erwerben, müssen Sie eine andere Premium-Lizenz für die andere Appliance erwerben.

So verwenden Sie die Hardwareseriennummer oder den Lizenzzugriffscode, um Ihre Lizenzen zuzuweisen:

- Sie müssen über die Appliance auf öffentliche Domains zugreifen können. Das Gerät muss beispielsweise auf www.citrix.comzugreifen können. Die Lizenzzuweisungssoftware greift intern auf das Citrix Lizenzierungsportal für Ihre Lizenz zu. Um auf eine gemeinfreie Domain zuzugreifen:
  - Verwenden Sie einen Proxyserver oder richten Sie einen DNS-Server ein.
  - Konfigurieren Sie eine NetScaler IP (NSIP) -Adresse oder eine Subnetz-IP-Adresse (SNIP) auf Ihrer NetScaler-Appliance.
- Ihre Lizenz muss mit Ihrer Hardware verknüpft sein, oder Sie müssen über einen gültigen Lizenzzugangscode verfügen. Citrix sendet Ihren Lizenzzugangscode per E-Mail, wenn Sie eine Lizenz erwerben.

Weisen Sie über die GUI eine Lizenz zu

Wenn Ihre Lizenz bereits mit Ihrer Hardware verknüpft ist, kann der Lizenzzuweisungsprozess die Hardware-Seriennummer verwenden. Andernfalls müssen Sie den Lizenzzugangscode eingeben.

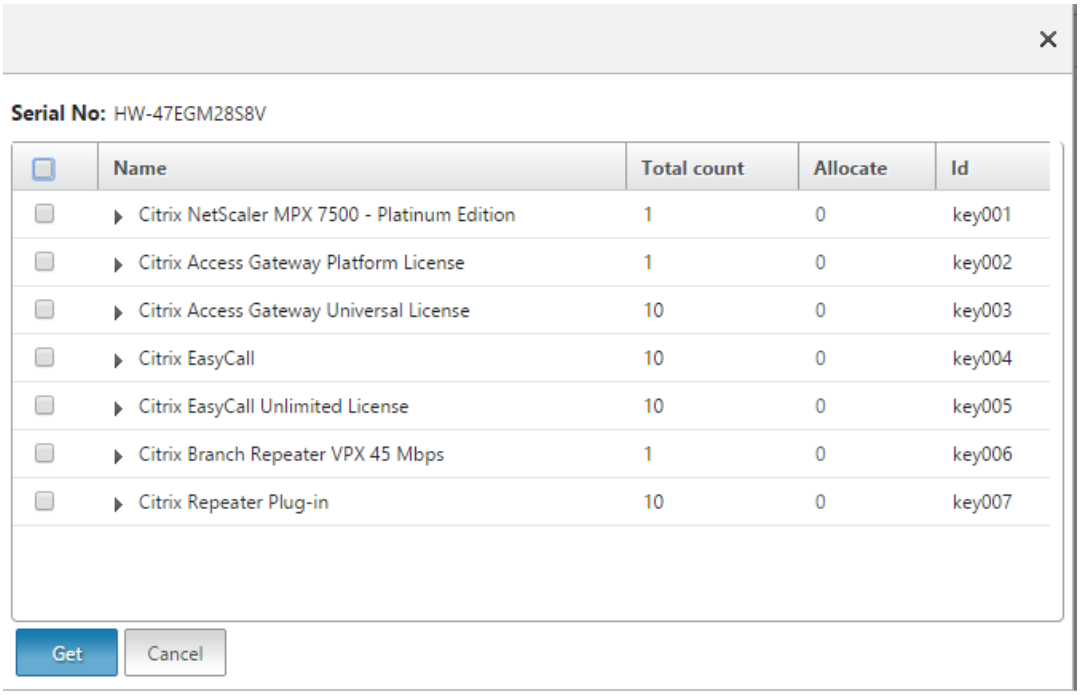
Sie können nach Bedarf für Ihre Bereitstellung teilweise Lizenzen zuweisen. Wenn Ihre Lizenzdatei beispielsweise 10 Lizenzen enthält, Ihre aktuelle Anforderung jedoch nur sechs Lizenzen umfasst, kön-

nen Sie jetzt sechs Lizenzen zuweisen und später weitere Lizenzen zuweisen. Sie können nicht mehr als die Gesamtzahl der in Ihrer Lizenzdatei enthaltenen Lizenzen zuweisen.

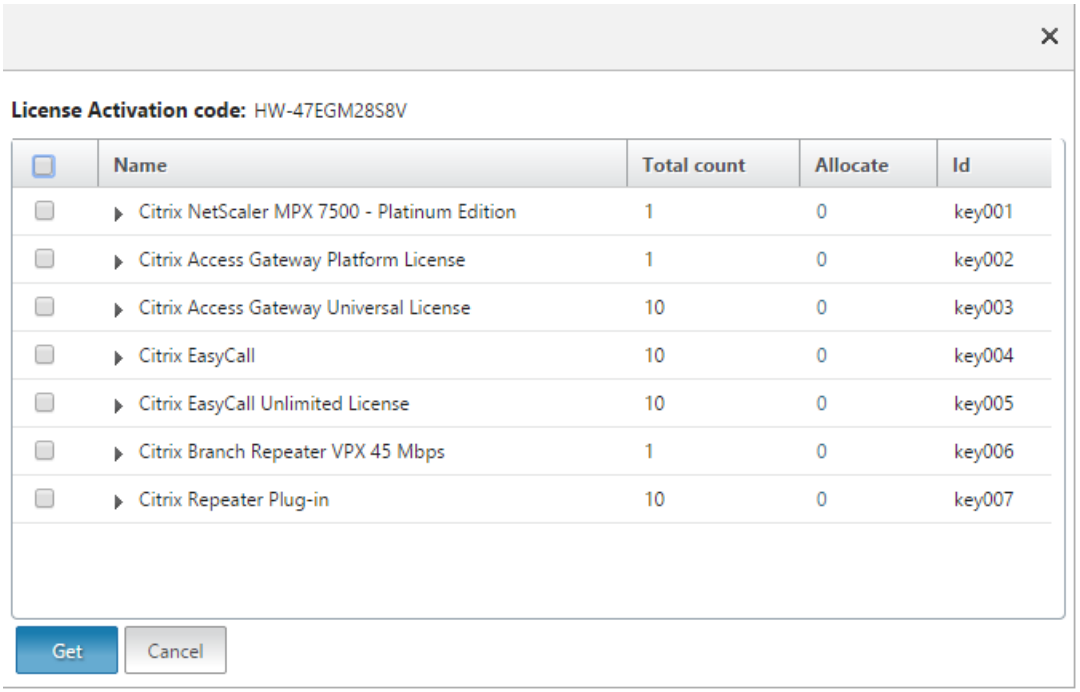
So weisen Sie Ihre Lizenz zu

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler-Appliance ein (z. B. `http://192.168.100.1`).
2. Geben Sie im Feld User Name und Password die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Configuration** zu **System > Licenses**.
4. Klicken Sie im Detailbereich auf **Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen**, und wählen Sie dann eine der folgenden Optionen aus:
   - **Seriennummer verwenden**: Die Software ruft intern die Seriennummer Ihres Geräts ab und verwendet diese Nummer, um Ihre Lizenzen anzuzeigen.
   - **Verwenden Sie den Lizenzzugangscode**: Citrix sendet den Lizenzzugangscode für die von Ihnen erworbene Lizenz per E-Mail. Geben Sie den Lizenzzugangscode in das Textfeld ein.

     Wenn Sie die Internetkonnektivität auf der NetScaler-Appliance nicht konfigurieren möchten, können Sie einen Proxyserver verwenden. Aktivieren Sie das Kontrollkästchen **Connect through Proxy Server** und geben Sie die IP-Adresse und den Port des Proxyservers an.
5. Klicken Sie auf **Get Licenses**. Abhängig von der ausgewählten Option wird eines der folgenden Dialogfelder angezeigt.
   - Das folgende Dialogfeld wird angezeigt, wenn Sie Hardware-Seriennummerausgewählt haben.

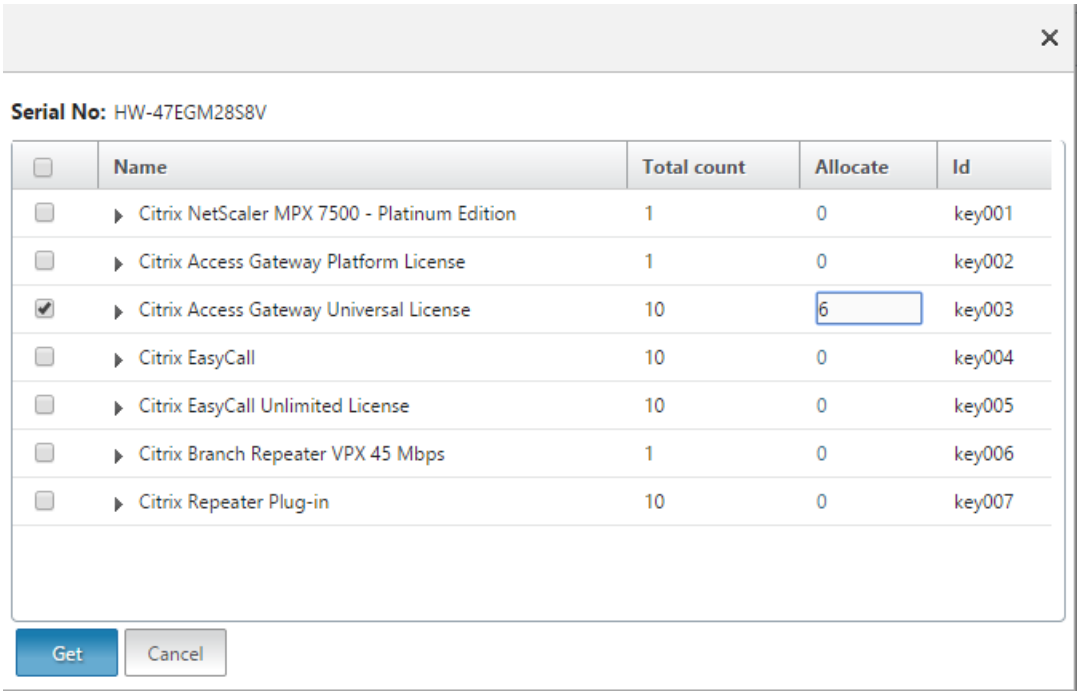


- Das folgende Dialogfeld wird angezeigt, wenn Sie den Lizenzzugangscode ausgewählt haben.

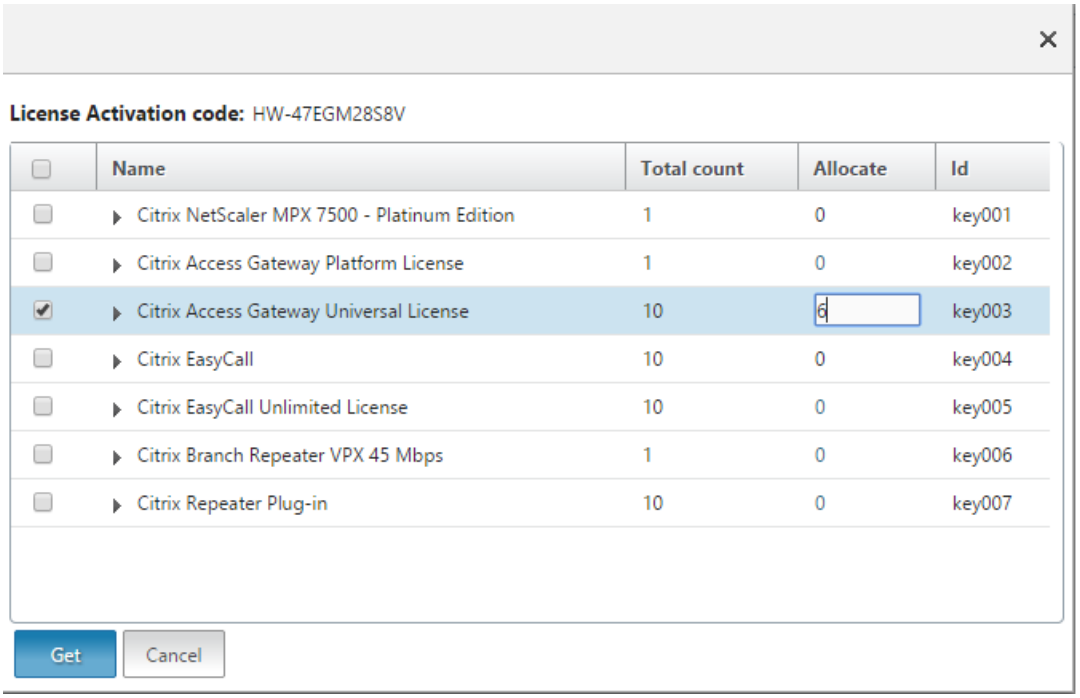


6. Wählen Sie die Lizenzdatei aus, mithilfe derer Sie Lizenzen zuteilen möchten.
7. Geben Sie in der Spalte **Zuweisen** die Anzahl der zuzuordnenden Lizenzen ein. Dann klick **Abrufen**.
    - Wenn Sie **Hardware-Seriennummer**ausgewählt haben, geben Sie die Anzahl der Lizen-

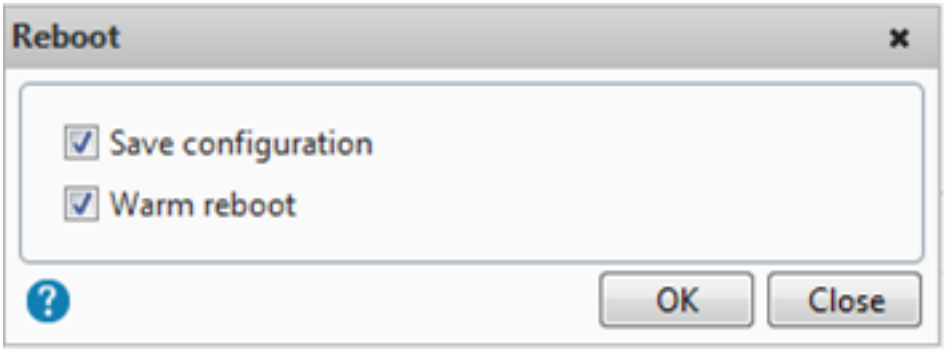
zen ein, wie im folgenden Screenshot gezeigt.



- Wenn Sie den **Lizenzzugangscode**ausgewählt haben, geben Sie die Anzahl der Lizenzen ein, wie im folgenden Screenshot gezeigt.



8. Klicken Sie auf “Restart”, damit die Lizenz in Kraft tritt.
9. Klicken Sie im Neustartdialogfeld auf **OK**, um mit den Änderungen fortzufahren, oder klicken Sie auf **Schließen**, um die Änderungen abzubrechen.



Installieren Sie eine Lizenz

Wenn Sie Ihre Lizenzdatei durch Zugriff auf das Lizenzportal auf Ihren lokalen Computer heruntergeladen haben, müssen Sie die Lizenz auf die Appliance hochladen.

So installieren Sie eine Lizenzdatei über die GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler-Appliance ein (z. B. `http://192.168.100.1`).
2. Geben Sie im Feld User Name und Password die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu Systemlizenzen.
4. Klicken Sie im Detailbereich auf **Manage Licenses**.
5. Klicken Sie auf **Add New License** und wählen Sie dann **Upload license files from a local computer**.
6. Klicken Sie auf **Durchsuchen**. Navigieren Sie zum Speicherort der Lizenzdateien, wählen Sie die Lizenzdatei aus und klicken Sie auf **Open**.
7. Klicken Sie auf "Restart", um die Lizenz anzuwenden.
8. Klicken Sie im Neustartdialogfeld auf **OK**, um mit den Änderungen fortzufahren, oder klicken Sie auf **Schließen**, um die Änderungen abzubrechen.

So installieren Sie die Lizenzen über die CLI

1. Öffnen Sie mithilfe eines **SSH-Clients wie PuTTY eine SSH-Verbindung** zur ADC-Appliance.
2. Melden Sie sich mithilfe der Administratoranmeldeinformationen bei der ADC-Appliance an.
3. Wechseln Sie zur Shell-Eingabeaufforderung, erstellen Sie ein Lizenzunterverzeichnis im Verzeichnis `nsconfig`, falls es nicht existiert, und kopieren Sie eine oder mehrere neue Lizenzdateien in dieses Verzeichnis.

   Beispiel

   ```
   1 login: nsroot
   ```



```
Password: nsroot
Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9
Done
> shell
Last login: Mon Aug  4 03:51:42 from 10.103.25.64
root@ns# mkdir /nsconfig/license
root@ns# cd /nsconfig/license
<!--NeedCopy-->
```

Kopieren Sie eine oder mehrere neue Lizenzdateien in dieses Verzeichnis.

> **Hinweis**
>
> Die NetScaler-Appliance fordert keine Neustartoption auf, wenn Sie die Befehlszeilenschnittstelle zum Installieren der Lizenzen verwenden. Führen Sie den Befehl reboot -w aus, um das System neu zu starten, oder führen Sie den Neustartbefehl aus, um das System normal neu zu starten.

Überprüfen Sie lizenzierte Funktionen

Stellen Sie vor der Verwendung einer Funktion sicher, dass Ihre Lizenz die Funktion unterstützt.

So überprüfen Sie die lizenzierten Funktionen über die CLI

1. Öffnen Sie mithilfe eines **SSH-Clients wie PuTTY eine SSH-Verbindung** zur ADC-Appliance.
2. Melden Sie sich mithilfe der Administratoranmeldeinformationen bei der ADC-Appliance an.
3. Geben Sie an der Eingabeaufforderung den Befehl sh ns license ein, um die von der Lizenz unterstützten Funktionen anzuzeigen.

   Beispiel

```
sh ns license
        License status:
                            Web Logging: YES
                        Surge Protection: YES
                          .......

                          Responder: YES
 Done
<!--NeedCopy-->
```


So überprüfen Sie die lizenzierten Funktionen über die GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der ADC-Appliance ein, z. B. `http://192.168.100.1`.
2. Geben Sie im Feld User Name und Password die Administratoranmeldeinformationen ein.
3. Geben Sie den Benutzernamen und das Kennwort ein und klicken Sie auf **Anmelden**.
4. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Lizenzen**. Neben den lizenzierten Funktionen sehen Sie ein grünes Häkchen.

Aktivieren oder Deaktivieren einer Funktion

Wenn Sie die NetScaler-Appliance zum ersten Mal verwenden, müssen Sie eine Funktion aktivieren, bevor Sie ihre Funktionalität verwenden können. Wenn Sie ein Feature konfigurieren, bevor es aktiviert wird, wird eine Warnmeldung angezeigt. Die Konfiguration wird gespeichert, gilt jedoch erst, nachdem die Funktion aktiviert wurde.

So aktivieren Sie eine Funktion über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Funktion zu aktivieren und die Konfiguration zu überprüfen:

- enable feature <FeatureName>
- show feature

Beispiel

```
enable feature lb cs
done
 >show feature

        Feature                         Acronym
           Status
        -------                         -------
           ------
 1)     Web Logging                     WL                      OFF
 2)     Surge Protection                SP                      ON
 3)     Load Balancing                  LB                      ON
 4)     Content Switching               CS                      ON
 5)     Cache Redirection               CR                      ON
 .
 .
 .
 24)    NetScaler Push                  push                    OFF
 Done
```



```
<!--NeedCopy-->
```

Das Beispiel zeigt, wie Load Balancing (lb) und Content Switching (cs) aktiviert werden.

Wenn der Lizenzschlüssel für eine bestimmte Funktion nicht verfügbar ist, wird für diese Funktion die folgende Fehlermeldung angezeigt:

FEHLER: Funktionen nicht lizenziert

Hinweis: Um eine optionale Funktion zu aktivieren, benötigen Sie eine funktionsspezifische Lizenz. Sie haben beispielsweise die NetScaler Advanced Edition-Lizenz gekauft und installiert. Um die Funktion Integrated Caching zu aktivieren, müssen Sie jedoch die AppCache-Lizenz erwerben und installieren.

So deaktivieren Sie eine Funktion über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Funktion zu deaktivieren und die Konfiguration zu überprüfen:

- disable feature <FeatureName>
- show feature

Beispiel

Das folgende Beispiel zeigt, wie der Lastenausgleich (LB) deaktiviert wird.

```
> disable feature lb
 Done
> show feature

        Feature                        Acronym
           Status
        -------                        -------
           ------
 1)     Web Logging                    WL                     OFF
 2)     Surge Protection               SP                     ON
 3)     Load Balancing                 LB                     OFF
 4)     Content Switching              CS                     ON
 .
 .
 .
 24)    NetScaler Push                 push                   OFF
 Done
>
<!--NeedCopy-->
```


Konfigurieren von Warnungen zum Ablauf der NetScaler Lizenz

Standardmäßig wird eine GUI-Warnung angezeigt, wenn das Ablaufdatum der ADC-Lizenz weniger als oder gleich 30 Tage ist.

Sie können die NetScaler-Appliance so konfigurieren, dass sie die folgenden Warnvorgänge ab einer bestimmten Anzahl von Tagen vor Ablauf einer NetScaler Lizenz ausführt:

- Zeigen Sie auf der NetScaler GUI ein Warnungsbanner für den Lizenzablauf an.
- Senden Sie in regelmäßigen Abständen SNMP-Traps mit den Informationen zum Lizenzablauf an die konfigurierten Trap-Listener, wenn der SNMP-Alarm “NS_LICENSE_EXPIRY” aktiviert ist.

Nach Ablauf der Lizenz wird die NetScaler-Appliance automatisch neu gestartet, um die Lizenz zu widerrufen. Wenn eine NetScaler-Appliance Citrix Service Provider (CSP) -Lizenzen verwendet, startet die Appliance nicht automatisch neu, um die Lizenz zu widerrufen. Wenn der Benutzer die Appliance jedoch neu startet, wird sie als nicht lizenziert neu gestartet.

Um mithilfe der CLI eine Anzahl von Tagen für Benachrichtigungen zum Ablauf der NetScaler-Lizenz anzugeben, gehen Sie wie folgt vor:

Geben Sie in der Befehlszeile Folgendes ein:

- **set license parameter** [-**licenseexpiryalerttime**]
- **sh Lizenzparameter**

Beispiel:

```
> set licenseparameters -licenseexpiryalerttime 200
Done

> sh licenseparameters
...
    Licenseexpiryalerttime:  200
<!--NeedCopy-->
```

So geben Sie mit der NetScaler GUI eine Anzahl von Tagen für NetScaler Lizenzablaufwarnungen an:

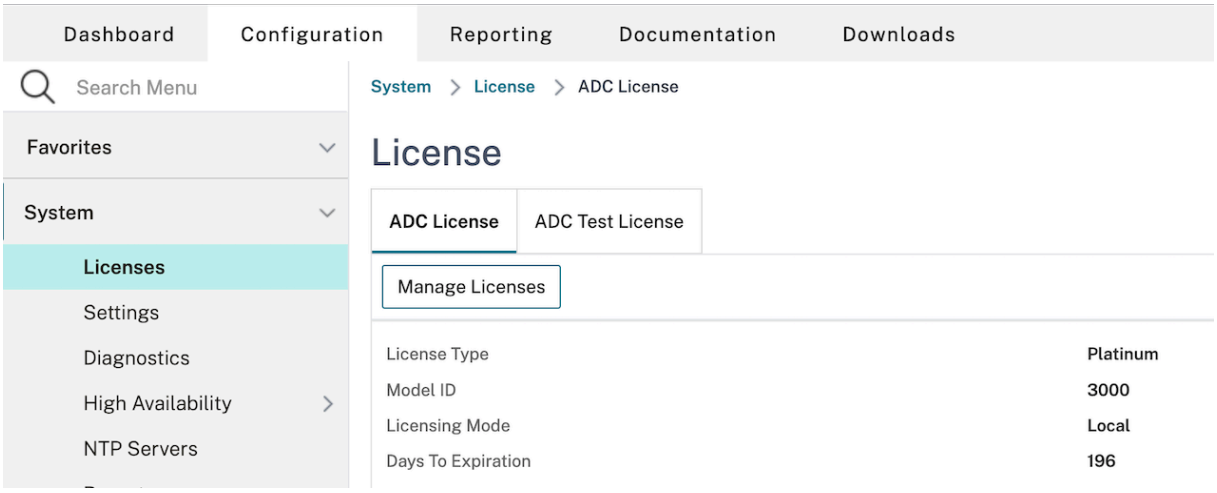
1. Navigieren Sie zu **Konfiguration** > **System** > **Lizenzen** > **Lizenzen verwalten**.
2. Klicken Sie in den **Benachrichtigungseinstellungen**auf die Schaltfläche Bearbeiten, um eine Anzahl von Tagen für die Warnungen zum Ablauf der NetScaler Lizenz anzugeben.

Überprüfen Sie die Informationen zum Ablauf der Lizenz

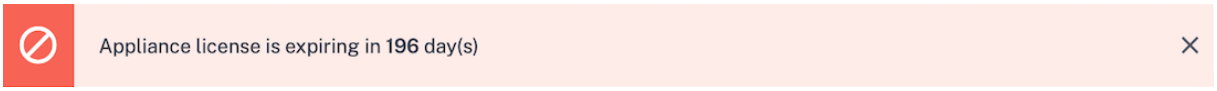
Sie können die Informationen zum Ablauf der NetScaler-Lizenz über die GUI oder CLI überprüfen.

So überprüfen Sie die Informationen zum Ablauf der NetScaler-Lizenz über die GUI:

Wechseln Sie zu **Konfiguration > System > Lizenzen**.



Eine GUI-Warnung wird angezeigt, wenn das Ablaufdatum der ADC-Lizenz weniger als oder gleich der angegebenen Anzahl von Tagen für die NetScaler Lizenzablaufwarnung ist.



So überprüfen Sie die Informationen zum Ablauf der Lizenz über CLI:

Geben Sie den Befehl “show ns license” ein.

```
> sh license
    License status:

    Web Logging: YES
    Surge Protection: YES

    Web Logging: YES
    Surge Protection: YES

    ...

Days to expiry: 196

Done
>
<!--NeedCopy-->
```

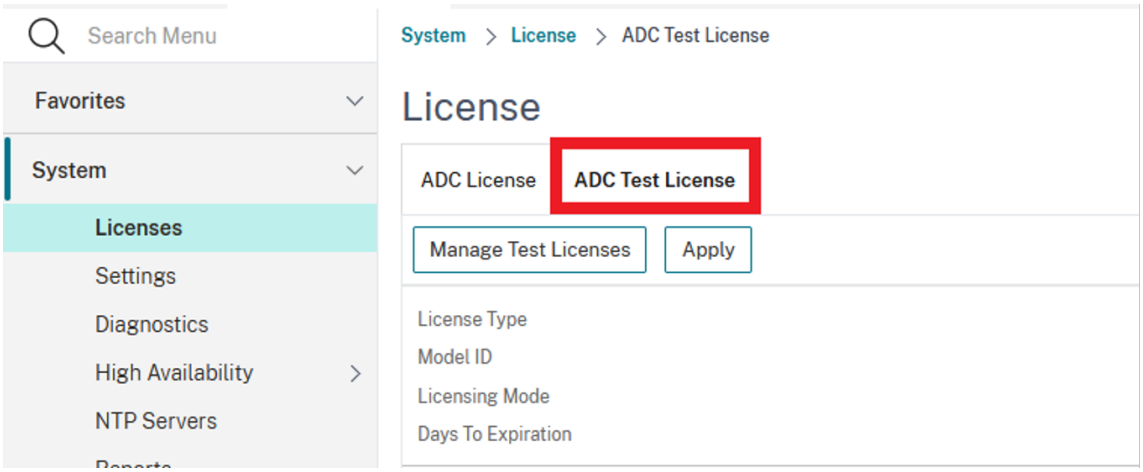

Validieren Sie Lizenzdateien, ohne die NetScaler-Appliance neu zu starten

Mit dieser Funktion können Sie Lizenzen testen und alle in der jeweiligen Lizenz verfügbaren Funktionen sehen, ohne sie auf der NetScaler-Appliance anwenden zu müssen. Mit dieser Option können Sie neue Lizenzen testen, ohne die NetScaler-Appliance neu starten zu müssen.

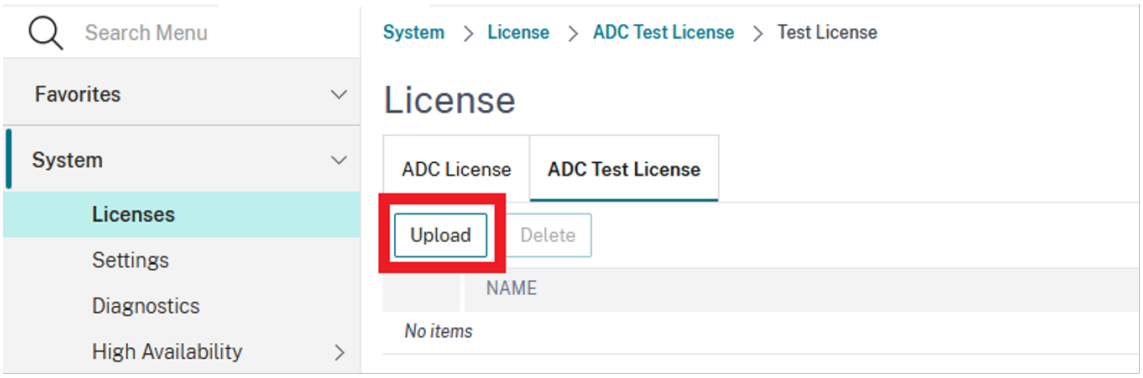
Sie können diese Funktion sowohl über die GUI als auch über die CLI verwenden.

Validieren Sie Lizenzdateien mithilfe der GUI

1. Gehen Sie zu **System -> Lizenzen**.
2. Klicken Sie auf der Registerkarte **ADC-Testlizenz** auf **Testlizenzen verwalten**.

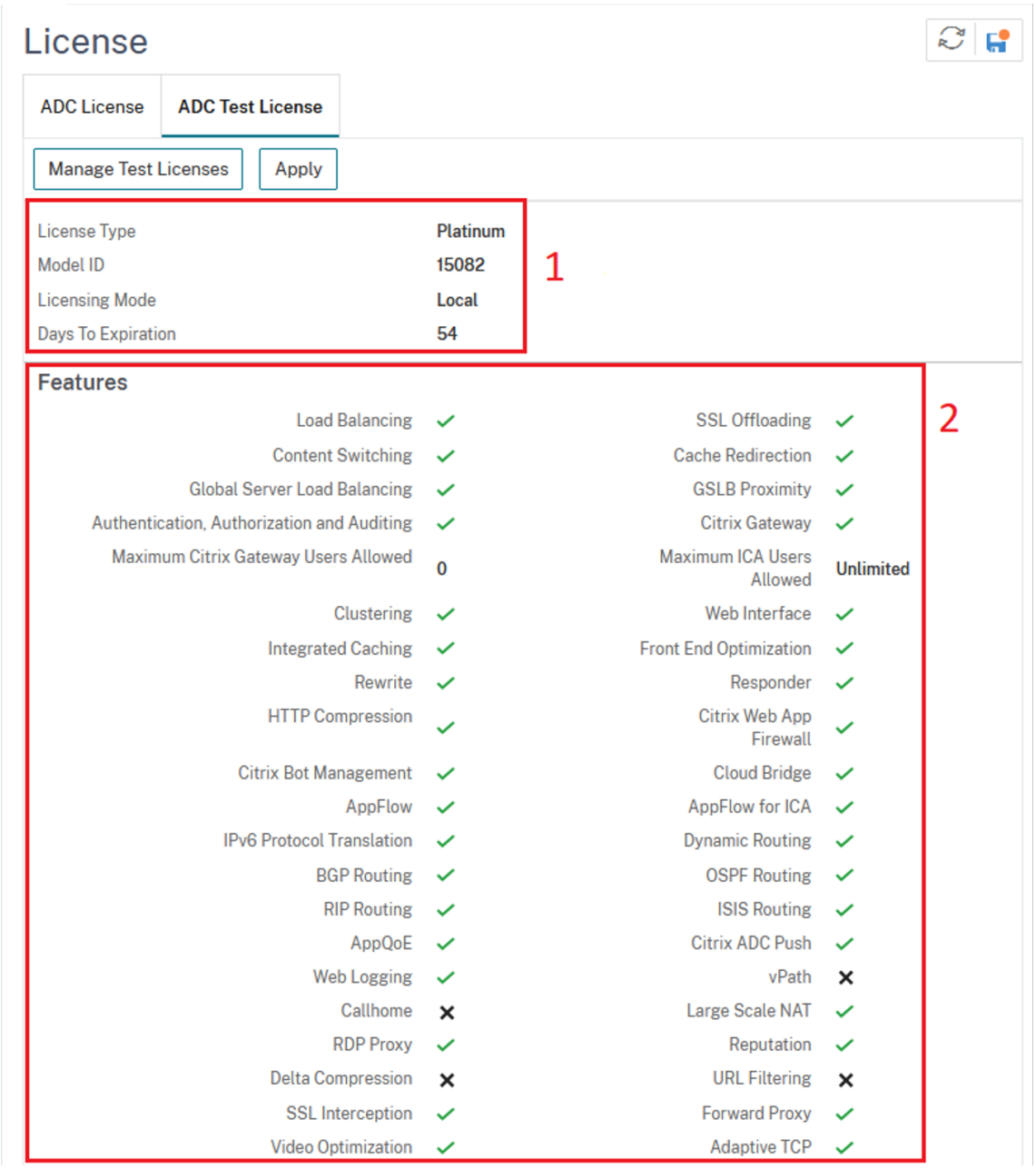


3. Klicken Sie auf **Hochladen**und laden Sie eine oder mehrere Lizenzdateien hoch. Wenn mehrere Lizenzdateien hochgeladen werden, wird die Vereinigung aller Lizenzdateien berechnet.



4. Nachdem der Upload der Lizenzdatei abgeschlossen ist, klicken Sie erneut auf **ADC Test License**, um die lizenzierten Funktionen der hochgeladenen Lizenz anzuzeigen.

   Abschnitt 1 enthält Lizenzinformationen und Abschnitt 2 zeigt alle Funktionen, die die Lizenz beinhaltet.



5. Überprüfen Sie die angezeigten Informationen und klicken Sie auf **Anwenden**, um die Lizenz zu verwenden. Starten Sie die NetScaler-Appliance neu (warmlaufen), damit die Lizenz wirksam wird. Ein sofortiger Neustart ist nicht erforderlich, und die aktuelle Lizenz gilt bis zum nächsten Neustart.

Validieren Sie Lizenzdateien mithilfe der CLI

1. Kopieren Sie die Testlizenzdatei auf die ADC-Appliance unter dem Pfad: `/nsconfig/testlicense`.

Beispiel:

```
scp CNS_15082_SERVER_PLT_Retail.lic nsroot@<ns_ip>:/nsconfig/
   testlicense/
<!--NeedCopy-->
```

2. Überprüfen Sie, ob die Lizenzdatei an den richtigen Speicherort kopiert wurde.

   Beispiel:

```
ls /nsconfig/testlicense/  CNS_15082_SERVER_PLT_Retail.lic
<!--NeedCopy-->
```

3. Führen Sie den `show ns testlicense` Befehl aus, um die Lizenzinformationen einzusehen.

```
> sh ns testlicense
    License status:
                        Web Logging: YES
                  Surge Protection: YES
                    Load Balancing: YES
                 Content Switching: YES
                 Cache Redirection: YES
               Compression Control: YES
                 Delta Compression: NO
                    SSL Offloading: YES
      Global Server Load Balancing: YES
                               .....
                       API Gateway: YES
                  Model Number ID: 15082
                     License Type: Platinum License
                  Licensing mode: Local
                Days to expiration: 54
<!--NeedCopy-->
```

4. Überprüfen Sie die angezeigten Informationen und führen Sie den `apply ns testlicense` Befehl aus, um die Lizenz anzuwenden. Starten Sie die NetScaler-Appliance neu (warmlaufen), damit die Lizenz wirksam wird.

```
> apply ns testlicense

Warning: The configuration changes will not take effect until the
   system is rebooted
Done
> reboot -w
Are you sure you want to restart NetScaler (Y/N)? [N]:Y
Done
```



```
<!--NeedCopy-->
```

Aktualisieren Sie eine Lizenz

Sie können eine NetScaler-Appliance von einer Familienedition auf eine andere und von einem Kapazitätsbereich auf einen anderen aktualisieren, indem Sie eine Lizenz mit höherer Kapazität erwerben.

Upgrades sind von zwei Arten:

- Editions-Upgrades: Standard auf Advanced, Standard zu Premium und Advanced to Premium. Edition-Upgrades müssen innerhalb derselben Bandbreite liegen.
- Kapazitätsupgrades: Sie können sowohl für vCPU als auch für Bandbreite von niedrigerer auf höherer Kapazität upgraden. Kapazitätsupgrades können nur für dieselbe Edition (Standard, Advanced oder Premium) durchgeführt werden.

Wenn Sie sowohl die Kapazität als auch die Edition aktualisieren möchten, aktualisieren Sie zuerst die Kapazität, starten Sie die Appliance neu und aktualisieren Sie dann die Edition.

Beispiel: Um eine VPX 10 Mbit/s Standard Edition-Lizenz auf die VPX 200 Mbit/s Premium Edition zu aktualisieren, muss das Upgrade in zwei Schritten erfolgen.

- VPX-Upgrade von 10 Mbit/s Standard Edition auf 200 Mbit/s Standard Edition.
- VPX-Upgrade von 200 Mbit/s Standard Edition auf 200 Mbit/s Premium Edition.

> Hinweis
>
> Sie können NetScaler Application Delivery Management (ADM) verwenden, um ein Lizenzierungsframework zu erstellen, das eine gemeinsame Bandbreite und einen gemeinsamen Instanzpool umfasst. Vollständige Informationen finden Sie unter Gepoolte Kapazität von NetScaler.

Zugehörige Ressourcen

- Citrix Lizenzierungssystem
- So weisen Sie NetScaler VPX-Lizenzen zu

Data Governance

May 11, 2023

Was ist NetScaler ADM Service Connect?

NetScaler Application Delivery Management (ADM) Service Connect ist eine Funktion, die das nahtlose Onboarding von NetScaler MPX-, SDX- und VPX-Instanzen sowie NetScaler Gateway-Appliances in den NetScaler ADM Service ermöglicht. Mit dieser Funktion können die NetScaler-Instanz oder die NetScaler Gateway-Appliance automatisch eine sichere Verbindung mit dem NetScaler ADM Service herstellen und System-, Nutzungs- und Telemetriedaten an sie senden. Basierend auf diesen Daten erhalten Sie Erkenntnisse und Empfehlungen für Ihre NetScaler-Infrastruktur auf dem NetScaler ADM Service.

Verwenden Sie die Verbindungsfunktion des NetScaler ADM Service ADM Servicees und Onboarding Ihrer NetScaler-Instanzen oder NetScaler Gateway-Appliances in den NetScaler ADM Service. Sie können auch alle Ihre NetScaler und NetScaler Gateway -Assets verwalten, ob lokal oder in der Cloud. Außerdem profitieren Sie vom Zugriff auf eine Vielzahl von Sichtbarkeitsfunktionen, die bei der schnellen Identifizierung von Leistungsproblemen, hoher Ressourcennutzung, kritischen Fehlern usw. helfen. Der NetScaler ADM Service bietet eine Vielzahl von Funktionen für Ihre NetScaler-Instanzen und -Anwendungen. Weitere Informationen zum NetScaler ADM Service finden Sie unter NetScalerApplication Delivery Management Service

> **Wichtig**
>
> - Die NetScaler Gateway -Appliance unterstützt auch die Funktion “NetScaler ADM Service Connect”. Zur besseren Vereinfachung wird die NetScaler Gateway-Appliance in den aufeinanderfolgenden Abschnitten nicht explizit aufgerufen.

Was ist der NetScaler ADM Service?

Der NetScaler ADM Service ist eine Cloud-basierte Lösung, mit der Sie Ihre NetScaler-Instanzen verwalten, überwachen, orchestrieren, automatisieren und Fehler beheben können. Es bietet Ihnen auch analytische Einblicke und kuratierte, auf maschinellem Lernen basierende Empfehlungen zu NetScaler Instanzen sowie zu Anwendungsstatus, Leistung und Sicherheit. Weitere Informationen finden Sie unter Überblick über den NetScaler ADM Service

Wie ist der NetScaler ADM Service Connect aktiviert?

NetScaler ADM Service Connect ist standardmäßig aktiviert, nachdem Sie NetScaler oder Gateway auf Version 13.0 Build 61.xx und höher installiert oder aktualisiert haben.

Welche Daten werden mit NetScaler ADM Service Connect erfasst?

Die folgenden Details werden mithilfe von NetScaler ADM Service Connect erfasst:

- **NetScaler Einzelheiten**

  - Seriennummer
  - Codierte Seriennummer
  - Host-ID
  - UUID
  - Verwaltungs-IP-Adresse
  - Hostname
  - Version
  - Buildtyp
  - Build
  - Lizenztyp
  - Hypervisor
  - Bereitstellungstyp (Standalone/HA)
  - Plattformtyp
  - Beschreibung der Plattform
  - System-ID
  - Modi aktiviert auf ADC
  - Auf ADC aktivierte Funktionen

- **Informationen zur Lizenz**
  - Auf NetScaler lizenzierte Funktionen
  - Nummer der Lizenz

- **Wichtige Nutzungsmetriken**
  - Datum und Uhrzeit des Systems
  - CPU-Nutzung in Prozent
  - Prozentsatz der Verwaltungs-C
  - Durchsatz
  - SSL neue Sessions
  - Durchsatz der SSL-Verschlüsselung
  - Durchsatz bei SSL-Entschlüsselung
  - Systembetriebszeit

- **Konfiguration**
  - ns.conf

> **Hinweis**
>
> Bevor der NetScaler ADM Service Connect die `ns.conf` Datei von der NetScaler Appliance an den NetScaler ADM Service sendet, anonymisiert er die verschlüsselten oder gehashten Kennwörter. Der NetScaler ADM Service Connect prüft nach `-encrypted` oder `-passcrypt` Parametern und ersetzt den zugehörigen verschlüsselten oder gehashten

> Wert durch `XXXX`. Der NetScaler ADM Service Connect kodiert und komprimiert die `ns.conf` Datei dann und sendet sie an den Endpunkt des NetScaler ADM-Service.

- **Details zum kritischen Fehler**
  - Festplattenausfälle
  - Ausfälle der SSL-Karte
  - Ausfälle der Stromversorgungseinheit (PSU)
  - Ausfall des Flashlaufwerks
  - Warmer Neustart
  - Anhaltende Speichernutzung über 90% oder ein Speicherleck
  - Anhaltende Zinsgrenze sinkt
- **Einsatz von NITRO-Automatisierungstools**
  - Verwendung von Automatisierungstools wie Ansible, Terraform oder NITRO SDKs.
- **Einzelheiten zur Diagnostik**

  > Hinweis:
  >
  > Das ADM-Diagnosetool verwendet die folgenden Diagnosedetails. Weitere Informationen finden Sie im Thema Diagnosetool in NetScaler ADM.

  - ADC-CLI-Status
  - ADC-DNS-Status
  - Netzwerkverbindungsstatus zum ADM-Endpunkt “adm.cloud.com”
  - Netzwerkverbindungsstatus zum ADM-Endpunkt “agent.adm.cloud.com”
  - Netzwerkverbindungsstatus zum ADM-Vertrauensdienst “trust.citrixnetworkapi.net”
  - Netzwerkverbindungsstatus zur ADM-Download-Site “download.citrixnetworkapi.net”

Wie werden die Daten verwendet?

Durch die Erfassung der Daten kann NetScaler Ihnen zeitnahe und detaillierte Einblicke in Ihre NetScaler-Installationen bieten, die Folgendes beinhalten:

- **Die wichtigsten Kennzahlen**. Details zu wichtigen Metriken zu CPU, Arbeitsspeicher, Durchsatz, SSL-Durchsatz und heben anomales Verhalten auf NetScaler-Instanzen hervor.
- **Kritische Fehler**. Alle kritischen Fehler, die möglicherweise in Ihren NetScaler-Instanzen aufgetreten sind.
- **Beratung zur Bereitstellung**. Identifizieren Sie NetScaler-Instanzen, die im Standalone-Modus bereitgestellt werden, aber einen hohen Durchsatz aufweisen und anfällig für einen einzigen Fehlerpunkt sind.
- **Diagnose-Tool**. Wenn Sie eine ADC-Instanz in NetScaler ADM integrieren, treten möglicherweise einige Probleme auf, die das erfolgreiche Onboarding der ADC-Instanz verhindern. Um

die Probleme zu beheben, können Sie das Diagnosetool entweder manuell verwenden oder die Diagnoseinformationen in der ADM-GUI einsehen. Weitere Informationen finden Sie unter Diagnosetool.

Wie lange werden die gesammelten Daten aufbewahrt?

Alle gesammelten Daten werden nicht länger als 13 Monate aufbewahrt.

Wenn Sie sich dazu entschließen, die Nutzung des Dienstes zu beenden, indem Sie die NetScaler ADM Service Connect-Funktion vom NetScaler deaktivieren, werden alle zuvor gesammelten Daten nach einem Zeitraum von 30 Tagen gelöscht.

Wo werden die Daten gespeichert und wie sicher sind sie?

Alle vom NetScaler ADM Service Connect gesammelten Daten werden in einer der drei Regionen gespeichert — USA, Europäische Union und Australien und Neuseeland (ANZ). Weitere Informationen finden Sie unter Geografische Überlegungen.

Die Daten werden sicher mit strenger Tenant-Isolation auf der Datenbankschicht gespeichert.

Wie deaktiviere ich NetScaler ADM Service Connect?

Wenn Sie die Datenerfassung über den NetScaler ADM Service Connect deaktivieren möchten, finden Sie unter So aktivieren und deaktivieren Sie den NetScaler ADM Service Connect.

Einführung in NetScaler ADM Service Connect für NetScaler Appliances

May 11, 2023

Der NetScaler ADM Service ist eine Cloud-basierte Lösung, mit der Sie Ihre NetScaler-Instanzen verwalten, überwachen, orchestrieren, automatisieren und Fehler beheben können. Es bietet auch analytische Erkenntnisse und kuratierte auf maschinellem Lernen basierende Empfehlungen für den Zustand, die Leistung und die Sicherheit Ihrer Anwendungen. Weitere Informationen finden Sie unter NetScaler Application Delivery Management Service.

NetScaler Application Delivery Management (ADM) Service Connect ist eine Funktion, die das nahtlose Onboarding von NetScaler Instances in den NetScaler ADM Service ermöglicht. Diese Funktion hilft NetScaler Instanzen und dem NetScaler ADM Service, als ganzheitliche Lösung zu fungieren, die Kunden mehrfache Vorteile bietet.

Mit der NetScaler ADM Service Connect-Funktion kann die NetScaler Instanz automatisch eine Verbindung mit dem NetScaler ADM Dienst herstellen und System-, Nutzungs- und Telemetriedaten

an sie senden. Basierend auf diesen Daten gibt Ihnen der NetScaler ADM Service einige Einblicke und Empfehlungen zu Ihrer NetScaler- und Gateway-Infrastruktur wie folgt:

- Einblicke in Sicherheitsberatung, die Ihre gefährdeten ADC-Appliances hervorheben.
- Aktualisieren Sie die beratenden Erkenntnisse, in denen ADC-Geräte hervorgehoben werden, die das Ende der Wartung und das Ende der Lebensdauer erreicht haben oder gerade erreicht haben.
- Schnelle Identifizierung von Leistungsproblemen, hoher Ressourcennutzung und kritischen Fehlern.

Um die Leistungsfähigkeit des NetScaler ADM Dienstes zu nutzen, können Sie Ihre NetScaler Instanzen für den NetScaler ADM Dienst einbinden. Der Onboarding-Prozess nutzt ADM Service Connect und macht das Erlebnis für Sie reibungslos und schneller.

> **Wichtige Hinweise**
>
> - NetScaler ADM Service Connect ist jetzt auf NetScaler MPX-, SDX- und VPX-Instanzen und NetScaler Gateway -Appliances verfügbar.
> - Die Initiative im NetScaler ADM Service, die diese Funktion für NetScaler ADM Service Connect verwendet, ist das auf ADM Service Connect basierendes Low-Touch-Onboarding. Weitere Informationen finden Sie unter Berührungsarmes Onboarding von NetScaler-Instanzen mit NetScaler ADM Service Connect.
> - Wenn ADM Service Connect auf einer ADC-Instanz aktiviert ist, werden bestimmte Diagnosedetails automatisch an den ADM Service gesendet.

Weitere Informationen finden Sie unter Data Governance.

> **Wichtig**
>
> NetScaler ADM Service Connect erfasst die Prüfdaten nicht und kann nicht beim Einsteigen der ADC Appliance in den ADM Service helfen, wenn die folgenden Bedingungen erfüllt sind:
>
> - `NSinternal` das Benutzerkonto ist deaktiviert.
> - Der öffentliche SSH-Schlüssel ist nicht eingerichtet.
>
> Um das vorhergehende Szenario zu überwinden, empfiehlt Citrix, eine der folgenden Aktionen zu befolgen:
>
> - Aktivieren Sie das `internaluser` Benutzerkonto mithilfe des `set ns param -internaluserlogin ENABLED`.
> - Konfigurieren Sie die öffentliche Schlüsselauthentifizierung. Weitere Informationen finden Sie unter Zugriff auf eine NetScaler-Appliance mit SSH-Schlüsseln und ohne Kennwort.

Wie verbindet der NetScaler ADM Service den Support mit dem NetScaler ADM Service?

Im Folgenden finden Sie einen allgemeinen Arbeitsablauf, der zeigt, wie die NetScaler ADM Service Connect-Funktion auf NetScaler mit dem NetScaler ADM Service interagiert.

1. NetScaler ADM Service Connects auf der NetScaler Appliance stellt mithilfe einer regelmäßigen Sondenanforderung automatisch eine Verbindung mit dem NetScaler ADM Service her.
2. Diese Anforderung enthält System-, Nutzungs- und Telemetriedaten, mit denen der NetScaler ADM Service Ihnen einige Einblicke und Empfehlungen zu Ihrer NetScaler-Infrastruktur gibt. Wie; schnelle Identifizierung von Leistungsproblemen, hohem Ressourcenverbrauch und kritischen Fehlern.
3. Sie können die Erkenntnisse und Empfehlungen anzeigen und beschließen, Ihre ADC-Instanzen in den NetScaler ADM Service einzubinden, um mit der Verwaltung Ihrer NetScaler-Instanzen zu beginnen.
4. Wenn Sie sich für das Onboarding entscheiden, hilft NetScaler ADM Service Connect dabei, das Onboarding nahtlos abzuschließen.

Auf welchen Versionen von NetScaler wird NetScaler ADM Service Connect unterstützt?

NetScaler ADM Service Connect wird auf allen NetScaler-Plattformen und allen Appliance-Modellen (MPX, VPX und SDX) unterstützt. Ab NetScaler Release 13.0 Build 61.xx ist NetScaler ADM Service Connect standardmäßig für NetScaler Appliances aktiviert.

Wie aktiviere ich NetScaler ADM Service Connect?

Wenn Sie ein bestehender NetScaler-Kunde sind und ein Upgrade auf NetScaler Release 13.0 Build 61.xx durchführen, ist NetScaler ADM Service Connect im Rahmen des Upgrade-Vorgangs standardmäßig aktiviert.

Wenn Sie ein neuer NetScaler-Kunde sind und NetScaler Release 13.0 Build 61.xx installieren, ist NetScaler ADM Service Connect standardmäßig als Teil des Installationsvorgangs aktiviert.

> **Hinweis**
>
> Im Gegensatz zu den neuen NetScaler Appliances finden vorhandene NetScaler Appliances die Route über den Citrix Insight Service (CIS) oder Call Home.

Wie aktiviere und deaktiviere ich NetScaler ADM Service Connect?

Sie können die NetScaler ADM Service Connect über CLI-, GUI- oder NITRO-API-Methoden aktivieren und deaktivieren.

CLI verwenden

Um den NetScaler ADM Service zu aktivieren, stellen Sie eine Verbindung mit der CLI her

Geben Sie in der Befehlszeile Folgendes ein:

```
set adm parameter -admserviceconnect ENABLED
```

So deaktivieren Sie NetScaler ADM Service Connect mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set adm parameter -admserviceconnect DISABLED
```

> **Wichtig**
>
> Wenn sich Ihr NetScaler in Release 13.0 Build 61.xx befindet, lautet der Parametername zum Aktivieren oder Deaktivieren des NetScaler Service Connect “Autoconnect. “ Verwenden Sie zum Beispiel den `set adm parameter -autoconnect ENABLED` Befehl, um Service Connect zu aktivieren.

Verwenden der GUI

Um den NetScaler ADM Service zu deaktivieren, stellen Sie eine Verbindung mit der NetScaler-GUI her.

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler-Appliance ein (z. B. http://192.0.2.10).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **System > Einstellungen > ADM-Parameter konfigurieren**.
4. Deaktivieren Sie auf der Seite **ADM-Parameter konfigurieren** das Dialogfeld **NetScaler ADM Service Connect aktivieren**, und klicken Sie auf **OK**.

Verwenden der NITRO-API

Sie können NetScaler ADM Service Connect mit dem Befehl **NITRO** deaktivieren.

- In NetScaler Release 13.0 Build 61.xx können Sie NetScaler ADM Service Connect mit dem folgenden Befehl aktivieren oder deaktivieren:


```
- curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/
  nitro/v1/config/admparameter> -d '{ "admparameter":{ "autoconnect
  ":"enabled" } } ' -u nsroot:Test@1
```

- Ab NetScaler Release 13.0 Build 64.xx wird der Parametername “autoconnect” in umbenannt `admserviceconnect`. Sie können NetScaler ADM Service Connect mit dem folgenden Befehl deaktivieren:

```
- curl -X PUT -H “Content-Type:application/json” http://192.0.2.10/
  nitro/v1/config/admparameter -d '{ "admparameter":{ "admserviceconnect
  ":"disabled" } } ' -u nsroot:Test@1
```

Diagnosetool

Wenn Sie eine ADC-Instanz in NetScaler ADM integrieren, treten möglicherweise einige Probleme auf, die das erfolgreiche Onboarding der ADC-Instanz verhindern. Um die Probleme zu beheben, können Sie das Diagnosetool entweder manuell verwenden oder die Diagnoseinformationen in der ADM-GUI einsehen.

- Weitere Informationen zu den Details, die mit ADM Service Connect erfasst wurden, finden Sie unter Datenverwaltung.
- Weitere Informationen zum Diagnose-Tool finden Sie unter Diagnosetool.

Verhalten des integrierten NetScaler ADM-Agenten

Ab NetScaler Release 13.0 Build 61.xx und höher kommuniziert der in NetScaler-Instanzen verfügbare NetScaler ADM-Agent mit dem ADM Service. Es kommuniziert ohne die Notwendigkeit einer manuellen Initialisierung auf der jeweiligen ADC-Instanz. Nachdem die Kommunikation mit dem ADM Service hergestellt wurde, bleibt der integrierte Agent immergrün, indem er sich regelmäßig automatisch auf die neueste Softwareversion aktualisiert.

Zuvor mussten Sie den integrierten Agenten auf den ADC-Instanzen mit `mastools` Befehlen initialisieren, um die Kommunikation mit dem ADM Service herzustellen und regelmäßige automatische Upgrades zu erstellen.
Weitere Informationen finden Sie unter Konfigurieren des integrierten ADC-Agenten für die Verwaltung von Instanzen.

Referenzen

Weitere Informationen zu NetScaler ADM Service Connect finden Sie in den folgenden Themen:

- Data Governance: Data Governance.
- NetScaler ADM Service: NetScaler Application Delivery ManagementService.

Aktualisieren und Downgrade einer NetScaler-Appliance

August 15, 2023

NetScaler 14.1 bietet neue und aktualisierte Funktionen mit erweiterter Funktionalität. Eine umfassende Liste von Verbesserungen ist in den Versionshinweisen aufgeführt, die der Release-Ankündigung beigefügt sind. Lesen Sie das Dokument mit den Versionshinweisen, bevor Sie Ihre Software aktualisieren.

Dieser Abschnitt enthält Informationen zum **Aktualisieren und Herunterstufen einer NetScaler-Appliance** (MPX und VPX) -Firmware **über die NetScaler GUI oder CLI**.

Sie können **NetScaler ADM auch verwenden, um eine NetScaler-Appliance zu aktualisieren**. Weitere Informationen:

- 10 Möglichkeiten, wie NetScaler ADM Service einfachere NetScaler-Upgrades unterstützt
- Verwenden Sie den NetScaler ADM Service, um NetScaler-Instanzen zu aktualisieren
- Verwenden Sie NetScaler ADM-Software, um NetScaler Instanzen zu aktualisieren

Informationen zum **Upgrade einer NetScaler SDX-Appliance**finden Sie unter Single Bundle Upgrade.

Voraussetzungen

September 11, 2023

Bevor Sie mit dem Upgrade- oder Downgrade-Prozess beginnen, überprüfen Sie Folgendes:

- Bewerten Sie die Supportvereinbarung Ihres Unternehmens. Dokumentieren Sie die Seriennummer der Appliance, den Supportvertrag und die Kontaktdaten für den Support durch den technischen Support von Citrix oder den autorisierten Citrix Partner.
- Zeit für das Upgrade von NetScaler-Appliances. Beachten Sie das Änderungskontrollverfahren Ihres Unternehmens. Weisen Sie doppelt so viel Zeit zu, um die Upgrades durchzuführen. Weisen Sie genügend Zeit zu, um jede der NetScaler-Appliance zu aktualisieren.
- Das NetScaler-Lizenzsystem erzwingt die Validierung der Customer Success Services (CSS) -Mitgliedschaftslizenz für NetScaler VPX-Appliances. Stellen Sie vor dem Upgrade einer NetScaler VPX-Appliance sicher, dass die aktuelle CSS-Mitgliedschaft der Appliance gültig und nicht abgelaufen ist.

  Stellen Sie sicher, dass das aktuelle Ablaufdatum der CSS-Mitgliedschaft dem CSS-Zulassungsdatum der zu aktualisierenden NetScaler-Produktversion entspricht oder neuer ist.

Wenn das Ablaufdatum der CSS-Mitgliedschaft vor dem CSS-Zulassungsdatum liegt, funktioniert die vorhandene Lizenz nicht auf der aktualisierten Version der NetScaler VPX-Appliance. Diese Funktion kann die unbefugte Verwendung der Lizenzen verhindern. Sie müssen die CSS-Mitgliedschaft erneuern, bevor Sie die NetScaler VPX-Appliance aktualisieren können.

Eine Liste der NetScaler VPX-Versionen und ihrer CSS-Zulassungsdaten finden Sie unter Gültigkeitsdaten für NetScaler-Produktefür Customer Success Services.

Weitere Informationen zu CSS finden Sie unter Customer Success Services.

- Citrix empfiehlt ein Upgrade von jeweils einer Hauptversion. Wenn sich die NetScaler-Appliance beispielsweise auf Version 13.0 befindet und Sie ein Upgrade auf Version 14.1 durchführen möchten, aktualisieren Sie die Appliance zuerst auf Version 13.1 und dann auf Version 14.1.
- Das Lizenzierungs-Framework und die Arten von Lizenzen. Ein Software-Edition-Upgrade erfordert möglicherweise neue Lizenzen, wie zum Beispiel:
  - ein Upgrade von der Standard Edition auf die Advanced Edition oder
  - die Standardausgabe zur Premium Edition oder
  - die Advanced Edition zur Premium Edition.

  Bestehende NetScaler-Lizenzen funktionieren weiterhin, wenn Sie ein Upgrade auf Version 14.1 durchführen. Weitere Informationen finden Sie unter Lizenzierung
- Suchen Sie nach neuen und veralteten Befehlen, Parametern und SNMP-OIDs.
- Suchen Sie nach der Hardware- und Softwarekompatibilitätsmatrix für NetScaler MPX.
- Wenn die Anmeldeseite NetScaler Gateway angepasst ist, stellen Sie sicher, dass das Benutzeroberflächendesign auf Standard festgelegt ist.
- Wenn Sie LOM aktualisieren, lesen Sie die Seite LOM-Firmware-Upgrade.
- Laden Sie die NetScaler-Firmware von den NetScaler-Downloadsherunter. Die detaillierten Schritte zum Herunterladen der NetScaler-Firmware finden Sie im NetScaler-Release-Paket herunterladen.
- Sichern Sie die Dateien. Führen Sie eine Sicherungskopie der Konfigurationsdatei, der Anpassungsdatei, der Zertifikate, Monitorskripts, Lizenzdateien usw. entweder manuell durch oder beziehen Sie sich auf die folgende Dokumentation zur Sicherung mit NetScaler CLI oder GUI — Backupand restore.
  - In der folgenden Liste finden Sie zusätzliche gebräuchliche benutzerdefinierte Dateien für die Backup.
    * `/nsconfig/monitors/*.pl`
    * `/nsconfig/rc.netscaler`
  - Erstellen Sie eine Sicherungskopie und löschen Sie den Anpassungsordner. Dies ist normalerweise unter `/var/customizations`. Ein Beispiel für die Anpassung ist eine An-

meldeseite mit einem Logo. Nachdem Sie den Anpassungsordner kopiert haben, müssen Sie ihn von der NetScaler-Appliance löschen, bevor Sie die Appliance aktualisieren. Ein Upgrade mit der Anpassung kann einige Probleme verursachen.

> **Wichtig:**
>
> Citrix empfiehlt dringend, die oben genannten Backup-Verfahren zu überprüfen. Haben Sie einen Aktionsplan für den Fall, dass das Update auf der NetScaler-Appliance nicht abgeschlossen wird.

- Stellen Sie sicher, dass im Verzeichnis /var und /flash ausreichend Platz für die NetScaler-Appliance vorhanden ist, bevor Sie ein Upgrade durchführen. Der /var benötigt 5 GB freien Speicherplatz (1 GB für das Upgrade-Paket + 4 GB für den Upgrade-Prozess)
  Der /flash benötigt genügend Speicherplatz, um über den neuen Kernel zu kopieren, der sich zwischen 140 MB und 160 MB unterscheidet, um sicherzustellen, dass mindestens 250 MB freier Speicherplatz verfügbar ist.
  Weitere Informationen zum Löschen des Festplattenspeichers in /var finden Sie unter So geben Sie Speicherplatz im Verzeichnis /var für die Protokollierung von Problemen mit einer NetScaler Appliance frei.
  Weitere Informationen zum Löschen des Speicherplatzes in /flash finden Sie unter https://support.citrix.com/article/CTX133587.

- Stellen Sie sicher, dass keine ungültigen Konfigurationen vorliegen, bevor Sie ein Upgrade mit dem Tool zur Überprüfung der Vorkonfiguration durchführen. Dieses Tool wird standardmäßig auch während des Upgrade-Vorgangs und als Teil des `installns` Skripts ausgeführt. Um Upgrade-Fehler aufgrund einer ungültigen Konfiguration zu vermeiden, wird empfohlen, vor dem Upgrade das Tool zur Überprüfung der Vorkonfiguration auszuführen. Weitere Informationen finden Sie unter Tool zur Überprüfung der Vorkonfiguration.

  Wenn es Konfigurationen gibt, die sich auf klassische Richtlinien beziehen, finden Sie weitere Informationen unter Überlegungen zum Upgrade für Konfigurationen mit klassischen Richtlinien und Häufig gestellte Fragen zu Classic Policy Deprecation.

  Wenn ungültige Konfigurationen vorhanden sind, verwenden Sie das `nspepi` Tool, um die ungültigen Konfigurationen in gültige Konfigurationen umzuwandeln. Informationen zum `nspepi` Tool finden Sie unter Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool.

  > **Hinweis:**
  >
  > Wenn Sie `Y` im `installns` Skript eine Option für das Upgrade des Builds auswählen, wird die Vorkonfigurationsprüfung nicht durchgeführt.

- Überprüfen Sie die Integrität der NetScaler-Appliance. Wenn Sie über eine NetScaler-Hardware-Appliance verfügen, empfiehlt Citrix dringend, diese auszuführen, `fsck` um eine Festplattenprüfung durchzuführen und die Integrität der NetScaler-Festplatte zu überprüfen. Im Falle eines

Fehlers setzen Sie das Festplattenlaufwerk zurück und wiederholen Sie den Befehl Disk check. Wenn die Fehlermeldung erneut angezeigt wird, wenden Sie sich an den NetScaler-Support, um das Problem weiter zu untersuchen.

- Validieren Sie die Datenträgerintegrität der Festplatte über den fsck-Befehl. Weitere Informationen finden Sie unter CTX122845.
- Überprüfen Sie die Integrität einer NetScaler-Appliance mit Diagnosepaketdateien und durch Hochladen der Protokolle zur Analyse in den Citrix Insight Service. Weitere Informationen finden Sie unter So erhalten Sie ein Paket für technischen Support.

- Sehen Sie sich die NetScaler VPX Support Matrix unddie Nutzungsrichtlinien an.
- Schauen Sie im FAQ-Bereich nach.
- Überprüfen Sie die Upgrade-Verfahren mit einer Testumgebung.

Weitere Informationen zu den Voraussetzungen für das Upgrade oder Downgrade der NetScaler-Appliance finden Sie in diesen Supportartikeln:

- CTX220371: Artikel müssen vor und nach dem Upgrade von NetScaler gelesenwerden

Überlegungen zum Upgrade für Konfigurationen mit klassischen Richtlinien

September 11, 2023

Klassische Richtlinien sind ab NetScaler Version 12.0 Build 56.20 veraltet. Ab Version 13.1 wird die klassische Richtlinienunterstützung aus einigen Funktionen entfernt. Eine vollständige Liste der Funktionen oder Befehle, die ab Version 13.1 nicht unterstützt werden, finden Sie in **Tabelle 2** in der Ankündigung einer Statusänderung für richtlinienbasierte Funktionen und Funktionen von NetScaler Classic.

Als Voraussetzung für das Upgrade auf Version 13.1 oder höher empfehlen wir Ihnen, die klassischen Richtlinien für die Funktionen, die klassische Richtlinien nicht unterstützen, in erweiterte Richtlinien umzuwandeln. Wenn Sie vor dem Upgrade nicht auf erweiterte Richtlinien umstellen, schlägt das Upgrade aufgrund einer ungültigen Konfiguration fehl.

> **Wichtig:**
>
> Bevor Sie auf Version 13.1 oder höher aktualisieren, empfehlen wir Ihnen, das Tool zur Überprüfung der Vorkonfiguration auszuführen. Dieses Tool stellt sicher, dass Ihre Konfiguration keine Befehle enthält, die sich auf veraltete oder entfernte Funktionen beziehen. Wenn es Befehle gibt, die sich auf die veralteten oder entfernten Funktionen beziehen, gibt das Tool einen Fehler aus und die Konfiguration geht möglicherweise verloren. Wir empfehlen Ihnen, die neueste Ver-

> sion des Tools zur Überprüfung der Voreinstellung über den öffentlichen GitHub-Link herunterzuladen - https://github.com/citrix/ADC-scripts/tree/master/nspepi.
>
> Weitere Informationen finden Sie im Tool zur Überprüfung der Vorkonfiguration vor dem Upgrade.

Wenn bei der Vorkonfigurationsprüfung Fehler auftreten, empfehlen wir Ihnen, das `nspepi` Tool zu verwenden, um die ungültigen Konfigurationen in gültige Konfigurationen umzuwandeln. Laden Sie die neueste Version des `nspepi` Tools über den öffentlichen GitHub-Link herunter - https://github.com/citrix/ADC-scripts/tree/master/nspepi. Weitere Informationen zum Konvertieren von Richtlinienausdrücken mit dem `nspepi` Tool finden Sie unter Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool.

Das `nspepi` Tool übernimmt die Konvertierung einiger Befehle oder Funktionen nicht. Eine vollständige Liste finden Sie unter Befehle oder Funktionen, die nicht vom nspepi-Konvertierungstool verarbeitet werden.

Führen Sie die folgenden Schritte für jede unterschiedliche Konfiguration aus, die Sie konvertieren müssen:

1. Führen Sie das `nspepi` Tool auf Citrix ADC Version 12.1 oder 13.0 aus, um die Datei zu konvertieren. `ns.conf` Das NSPEPI-Tool generiert zwei Dateien mit Präfixen und. `new_warn_` Die Datei mit dem `new_` Präfix enthält die konvertierte Konfiguration und die Datei mit dem `warn_` Präfix enthält die Warnungen und Fehler.
2. Überprüfen Sie die Datei mit dem `warn_` Präfix und beheben Sie Fehler (falls vorhanden).
3. Testen Sie die konvertierte Konfiguration. Wenden Sie die konvertierte Konfiguration mit einer der folgenden Optionen an:
   a) Führen Sie den `clear config -f basic` Befehl aus und beziehen Sie dann die konvertierte Konfiguration, indem `source /nsconfig/new_ns.conf` Sie den Befehl ausführen.
   b) Entfernen Sie die klassischen Befehle manuell (indem Sie die Bindung aufheben und Richtlinien entfernen) und beziehen Sie dann die konvertierte Konfiguration, indem Sie den `source /nsconfig/new_ns.conf` Befehl ausführen.

      > **Hinweis:**
      > Möglicherweise werden für die Konfigurationen, die nicht mit dem `clear config -f basic`Befehl gelöscht wurden, die Fehlermeldung „Ressource ist bereits vorhanden“ angezeigt. Sie können diese Fehler ignorieren.
4. Speichern Sie die Konfiguration.

Nachdem Sie ungültige Konfigurationen erfolgreich in gültige Konfigurationen konvertiert haben, überprüfen Sie, ob weitere Voraussetzungen erfüllt sind, und fahren Sie dann mit dem Upgrade fort. Weitere Informationen finden Sie unter Upgrade und Downgrade einer NetScaler-Appliance.

Überlegungen zum Upgrade für benutzerdefinierte Konfigurationsdateien im Verzeichnis /etc

May 11, 2023

Es wird unterstützt, dass die folgenden Konfigurationsdateien im Verzeichnis `/etc` geändert werden:

- `inetd.conf`
- `syslog.conf`
- `newsyslog.conf`
- `ntp.conf`
- `crontab`
- `host.conf`
- `hosts`
- `ttys`
- `sshd_config`
- `httpd.conf`
- `monitrc`
- `rc.conf`
- `ssh_config`
- `localtime`
- `issue`
- `issue.net`
- `ldap.conf`
- `motd`

> **Hinweis:**
>
> Je nachdem, welcher NetScaler-Build auf der Appliance ausgeführt wird, können der obigen Liste neue Dateien hinzugefügt werden. Sie können eine aktualisierte Dateiliste anzeigen, indem Sie den folgenden Shell-Befehl in der NetScaler-Befehlszeilenschnittstelle ausführen:
>
> ```
> grep NSETC= /etc/rc
> ```

Wenn Sie eine der Konfigurationsdateien im Verzeichnis `/etc` geändert und in das Verzeichnis `/nsconfig` kopiert haben, erstellt die NetScaler-Appliance aus Gründen der Persistenz einen Symlink in `/etc`, der auf die Datei `/nsconfig` verweist.

Beispiel: `/etc/httpd.conf -> /nsconfig /httpd.conf`

Ein Release-Paket kann eine eigene Version der Konfigurationsdateien im Verzeichnis `/etc` enthalten. Diese Konfigurationsdateien enthalten wichtige Updates, die für die ordnungsgemäße Funktion der NetScaler-Appliance erforderlich sind. Beim Upgrade einer NetScaler-Appliance auf eine Version werden die Konfigurationsdateien im Verzeichnis `/etc` durch die Konfigurationsdateien ersetzt, die die

Release-Updates enthalten.

Betrachten Sie ein Beispiel für eine angepasste Konfigurationsdatei `example.conf`, die im Verzeichnis `/etc` vorhanden ist. Die Datei `example.conf` wird in das Verzeichnis `/nsconfig` kopiert, um die Persistenz aufrechtzuerhalten. Die NetScaler-Appliance erstellt einen Symlink in `/etc` durch einen Verweis auf die Datei in `/nsconfig`: `/etc/example.conf -> / nsconfig /example.conf`

Außerdem enthält ein Release-Paket eine eigene Version von `example.conf`, die wichtige Updates enthält. Das folgende Verhalten wird beobachtet, wenn Sie die NetScaler-Appliance auf die Version aktualisieren:

Da der Symlink `/etc/example.conf` bereits vorhanden ist, legt die NetScaler-Appliance die Releasepaketkopie von `example.conf` während des Upgradevorgangs nicht im Verzeichnis `/etc` ab.

Da die Releasepaketkopie von `example.conf` wichtige Updates enthält, kann das Fehlen im Verzeichnis `/etc` dazu führen, dass die NetScaler-Appliance fehlschlägt oder nicht ordnungsgemäß funktioniert.

Schritte zum Beibehalten von Änderungen und Anpassungen bei Upgrades

Um sicherzustellen, dass sowohl Versionsupdates als auch Ihre Anpassungen nicht verloren gehen, führen Sie die folgenden Schritte aus:

- Schritte vor dem Upgrade:
  - Benutzerdefinierte Datei vor dem Upgrade sichern
  - Entfernen Sie die Persistenz der angepassten Datei vor dem Upgrade
- Schritte nach dem Upgrade:
  - Wenden Sie Anpassungen auf die aktualisierte Datei an und fügen Sie nach dem Upgrade Persistenz hinzu

    > **Wichtig:**
    > Ersetzen Sie Ihre angepasste Datei NICHT direkt im Ordner `/etc`. Durch direktes Ersetzen einer Datei `/etc` durch die benutzerdefinierte Backupdatei werden alle Release-Updates entfernt, die der Datei während des Upgradeprozesses hinzugefügt wurden.

Benutzerdefinierte Datei vor dem Upgrade sichern

Erstellen Sie eine Backup der im Verzeichnis `/nsconfig` vorhandenen benutzerdefinierten Dateien, bevor Sie die Appliance aktualisieren.

Erstellen Sie ein Verzeichnis `/var/nsconfig_backup` und verschieben Sie die angepassten Dateien in dieses Verzeichnis. Verschieben Sie also alle Dateien, die Sie im Verzeichnis `/etc` geändert und in

/nsconfig kopiert haben, indem Sie den folgenden Befehl an der Shell-Eingabeaufforderung ausführen:

```
mv /nsconfig/<filename> /var/nsconfig_backup/
<!--NeedCopy-->
```

Beispiel:

```
mv /nsconfig/httpd.conf /var/nsconfig_backup/
<!--NeedCopy-->
```

Entfernen Sie die Persistenz der angepassten Datei vor dem Upgrade

Löschen Sie die Symlinks /etc, die auf die Dateien /nsconfig verweisen, bevor Sie die Appliance aktualisieren.

1. Überprüfen Sie die vorhandenen Symlinks im Verzeichnis /etc, indem Sie den folgenden Befehl an der Shell-Eingabeaufforderung ausführen:

   ```
   ls -la /etc
   <!--NeedCopy-->
   ```

2. Löschen Sie einen Symlink /etc, der auf eine Datei /nsconfig zeigt, indem Sie den folgenden Befehl an der Shell-Eingabeaufforderung ausführen:

   ```
   unlink /etc/<filename>
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   unlink /etc/httpd.conf
   <!--NeedCopy-->
   ```

3. Überprüfen Sie, ob der Symlink entfernt wurde, indem Sie den folgenden Befehl an der Shell-Eingabeaufforderung ausführen:

   ```
   cat /etc/<filename>
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   cat /etc/httpd.conf
   <!--NeedCopy-->
   ```

   Dieser Befehl zeigt keinen Inhalt an, wenn der Symlink entfernt wird.

Wenden Sie Anpassungen auf die aktualisierte Datei an und fügen Sie nach dem Upgrade Persistenz hinzu

Wenn Sie eine Backup einer geänderten Konfigurationsdatei /nsconfig in /var/nsconfig_backup erstellt haben, gehen Sie nach dem Upgrade der Appliance wie folgt vor:

1. Vergleichen Sie die in den Verzeichnissen /var/nsconfig_backup und /etc vorhandene Datei. Fügen Sie der Datei /etc, die bereits die Release-Updates enthält, manuell die entsprechenden Änderungen hinzu.

   > **Wichtig:**
   >
   > Durch direktes Ersetzen der Datei /etc durch die Datei /var/nsconfig_backup werden alle Release-Updates entfernt, die der Datei während des Upgradeprozesses hinzugefügt wurden. Dieses Entfernen von Updates kann dazu führen, dass die zugehörigen NetScaler-Funktionen fehlschlagen oder nicht ordnungsgemäß funktionieren.

2. Um die Persistenz aufrechtzuerhalten, kopieren Sie die im Verzeichnis /etc vorhandene aktualisierte Datei in das Verzeichnis /nsconfig, indem Sie den folgenden Befehl an der Shell-Eingabeaufforderung ausführen:

   ```
   cp /etc/<filename> /nsconfig/
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   cp /etc/httpd.conf /nsconfig/
   <!--NeedCopy-->
   ```

3. Wiederholen Sie die beiden obigen Schritte für jede angepasste Datei, die im Verzeichnis /var/nsconfig_backup ist.
4. Starten Sie das Gerät neu, um die Änderungen in Kraft zu setzen.

Überlegungen zum Upgrade - SNMP-Konfiguration

May 11, 2023

Der Timeout-Parameter für einen SNMP-Alarm ist eine interne Option, die keinen Einfluss auf die Alarmkonfiguration hat.

Der Timeout-Parameter kann in den SNMP-Alarmkonfigurationen in der laufenden Konfiguration (sh läuft) und der gespeicherten Konfiguration (ns.conf) erscheinen, auch wenn Sie keine Änderungen an diesen SNMP-Alarmkonfigurationen vorgenommen haben.

Beim Upgrade auf einen Release-Build mit der Behebung des Timeout-Einstellungsproblems werden die SNMP-Konfigurationen fälschlicherweise auf die Standardwerte zurückgesetzt.

Die folgenden SNMP-Alarme (falls konfiguriert) sind während eines Upgrades betroffen:

- APPFW-PUFFERÜBERLAUF
- APPFW-COOKIE
- APPFW-CSRF-TAG
- APPFW-DENY-URL
- APPFW-FELDKONSISTENZ
- APPFW-FELDFORMAT
- APPFW-POLICY-HIT
- APPFW-REFERER-HEADER
- APPFW-SAFE E-COMMERCE
- APPFW-SAFE-OBJEKT
- APPFW-SQL
- APPFW-STARTURL
- TYP APPFW-VIOLATIONS-TYPE
- APPFW-XML-ANHANG
- APPFW-XML-DOS
- APPFW-XML-SCHEMA-KOMPILIEREN
- APPFW-XML-SOAP-FEHLER
- APPFW-XML-SQL
- APPFW-XML-VALIDIERUNG
- APPFW-XML-WSI
- APPFW-XML-XSS
- APPFW-XSS
- CLUSTER-BACKPLANE-HB-FEHLT
- ZUSTAND DES CLUSTERKNOTENS
- CLUSTERKNOTEN-QUORUM
- CLUSTER-VERSIONSKONFLIKT
- COMPACT-FLASH-ERRORS
- KONFIGURATIONSÄNDERUNG
- KONFIGURATION SPEICHERN
- HA-BAD-SEKUNDÄRSTAAT
- HAT KEINEN HERZSCHLAG
- HA-SYNC-FEHLER
- HA-VERSIONSKONFLIKT
- HARD-DISK-DRIVE-ERRORS
- HA-STATE-CHANGE
- HA-STICKY-PRIMARY

- PORT-ALLOC-FEHLER
- SYNFLUT

Diese SNMP-Alarmkonfigurationen sind betroffen, wenn Sie den NetScaler auf die folgenden Release-Builds aktualisieren:

- Version 11.1 Build 61.2 oder höher
- Version 12.0 Build 61.0 oder höher
- Version 12.1 Build 30.1 oder höher
- Version 13.0 Build 51.4 oder höher

Beispiel

Betrachten wir ein Beispiel für einen CLUSTER-NODE-HEALTH SNMP-Alarm.

```
1 CLUSTER-NODE-HEALTH SNMP alarm is set up by using the NetScaler command
      line:
2
3 > set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -
     severity Major
4
5 > save config
6 <!--NeedCopy-->
```

Diese SNMP-Alarmkonfiguration erscheint in der gespeicherten Konfigurationsdatei (`ns.conf`) als:

```
1 set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -severity
     Major -timeout 86400
2
3 <!--NeedCopy-->
```

Während eines Upgrades auf einen der oben genannten Release-Builds erscheint der folgende Fehler in der Datei ns.log:

```
1 May 23 09:14:46 <local0.err> ns nsconfigd: __init_config_filter(): (
     null) line 0: No such argument [-timeout]>> set snmp alarm CLUSTER-
     NODE-HEALTH -time 111 -state DISABLED -severity Major -timeout
     86400.
2 <!--NeedCopy-->
```

Nach dem Upgrade werden die SNMP-Alarmkonfigurationen auf die Standardwerte zurückgesetzt.

Workaround

Verwenden Sie einen der folgenden Workarounds:

- Entfernen Sie vor dem Upgrade die Timeout-Einstellung aus den SNMP-Konfigurationen in der gespeicherten Konfigurationsdatei (ns.conf).
- Nach dem Upgrade konfigurieren Sie die SNMP-Alarme ohne den Timeout-Parameter neu.

Download eines NetScaler Release-Pakets

May 11, 2023

Führen Sie die folgenden Schritte aus, um ein NetScaler Releasepaket herunterzuladen:

1. Öffnen Sie die Seite NetScaler Downloads in einem Webbrowser.
2. Erweitern Sie auf der Seite NetScaler Downloads die **NetScaler Version**, auf die Sie aktualisieren möchten.
3. Erweitern Sie eine der entsprechenden Kategorien und klicken Sie auf den NetScaler-Build-Link. **Um beispielsweise eine Version der NetScaler-Firmware herunterzuladen, erweitern Sie Firmware und klicken Sie auf den NetScaler-Build, den Sie herunterladen möchten.**
4. Erweitern Sie auf der ausgewählten NetScaler-Buildseite den Abschnitt **Build** und klicken Sie auf **Datei herunterladen**, um das NetScaler-Build-Paket herunterzuladen.

> **Hinweis:**
> Die Prüfsumme wird bereitgestellt, um sicherzustellen, dass Sie das heruntergeladene Build-Paket dem tatsächlichen Paket zuordnen, das auf der Website gehostet wird. Die Prüfsumme ist eine wichtige Prüfung, um sicherzustellen, dass Sie die richtigen Bits haben.

Upgrade einer eigenständigen NetScaler-Appliance

August 15, 2023

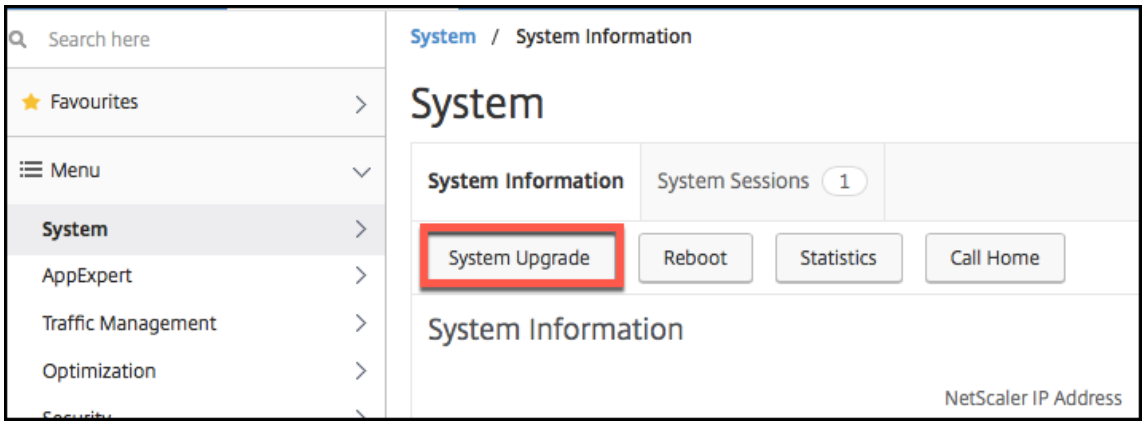
Bevor Sie die Systemsoftware aktualisieren, lesen Sie den Abschnitt Bevor Sie beginnen, und erfüllen Sie die Voraussetzungen wie das Sichern der erforderlichen Dateien und das Herunterladen der NetScaler-Firmware.

Upgrade einer eigenständigen NetScaler-Appliance über die GUI

Gehen Sie wie folgt vor, um einen eigenständigen NetScaler mithilfe der GUI auf Version 14.1 zu aktualisieren.

1. Geben Sie beispielsweise in einem Webbrowser die IP-Adresse des NetScaler ein `http://10.102.29.50`.

2. Geben Sie unter Benutzername und Kennwort die Administratoranmeldeinformationen (nsroot/nsroot) ein und klicken Sie dann **auf Anmelden**.
3. Klicken Sie auf der GUI auf **System Upgrade**.



4. Wählen Sie im Menü **Datei wählen** die entsprechende Option: **Lokal** oder **Gerät**. Wenn Sie die Option Appliance verwenden möchten, muss die Firmware zuerst auf den NetScaler hochgeladen werden. Sie können jede Dateiübertragungsmethode wie WinSCP verwenden, um die NetScaler-Firmware auf die Appliance hochzuladen.
5. Wählen Sie die richtige Datei aus und klicken Sie auf **Upgrade**.
6. Folgen Sie den Anweisungen, um die Software zu aktualisieren.
7. Wenn Sie dazu aufgefordert werden, wählen Sie **Neustart** aus.

Schließen Sie nach dem Upgrade alle Browserinstanzen und löschen Sie den Cache Ihres Computers, bevor Sie auf die Appliance zugreifen.

Aktualisieren einer NetScaler Standalone-Appliance über die CLI

Befolgen Sie diese Schritte, um einen eigenständigen NetScaler über die CLI auf Version 14.1 zu aktualisieren:

Im folgenden Verfahren sind `<release>` und `<releasenumber>` die Releaseversion, auf die Sie ein Upgrade durchführen, und `<targetbuildnumber>` ist die Buildnummer, auf die Sie aktualisieren. Das Verfahren beinhaltet optionale Schritte, um zu vermeiden, dass Aktualisierungen verloren gehen, die während des Upgrades in das Verzeichnis /etc übertragen werden.

1. Verwenden Sie einen SSH-Client wie PuTTY, um eine SSH-Verbindung zur Appliance herzustellen.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an. Speichern Sie die laufende Konfiguration. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   save config
   ```


3. Wechseln Sie zur Shell-Eingabeaufforderung, indem Sie folgenden Befehl ausführen:

   ```
   shell
   ```

4. Erstellen Sie eine Kopie der Datei ns.conf. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   - `cd /nsconfig`
   - `cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber>`

   Sie sollten die Konfigurationsdatei auf einem anderen Computer Backup.

5. **WICHTIG:**

   Es ist wichtig, dass sowohl die Upgrade-Änderungen als auch Ihre Anpassungen auf eine aktualisierte NetScaler-Appliance angewendet werden. Wenn Sie benutzerdefinierte Konfigurationsdateien im Verzeichnis `/etc` haben, führen Sie die **Schritte vor dem Upgrade** unter Überlegungen zum Upgrade für benutzerdefinierte Konfigurationsdateien aus.

6. Erstellen Sie einen Speicherort für das Installationspaket. An der Shell-Eingabeaufforderung geben

   - `cd /var/nsinstall`
   - `cd <releasenumber>`

     Hinweis:

     Wenn das gewünschte Versionsnummernverzeichnis nicht vorhanden ist, erstellen Sie eines mit dem folgenden Befehl:

     `mkdir <releasenumber>`

     Beispiel:

     `mkdir 14.1`

   - `mkdir build_<targetbuildnumber>`
   - `cd build_<targetbuildnumber>`

7. Kopieren Sie die bereits heruntergeladene NetScaler-Firmware in das Build-Verzeichnis, das Sie im obigen Schritt erstellt haben, indem Sie eine beliebige Dateiübertragungsmethode wie WinSCP verwenden. Weitere Informationen zum Herunterladen der NetScaler-Firmware finden Sie im Abschnitt Bevor Sie beginnen .

8. Extrahieren Sie den Inhalt des Installationspakets. Beispiel:

   ```
   tar -xvzf build-14.1-37.2_nc_64.tgz
   ```

9. Führen Sie das Installationsskript aus, um die neue Version der Systemsoftware zu installieren.

   ```
   ./installns
   ```


10. Starten Sie den NetScaler neu, wenn Sie dazu aufgefordert werden.
11. **WICHTIG:**

    Es ist wichtig, dass sowohl die Upgrade-Änderungen als auch Ihre Anpassungen auf eine aktualisierte NetScaler-Appliance angewendet werden. Wenn Sie benutzerdefinierte Konfigurationsdateien im Verzeichnis `/etc` haben, führen Sie die **Schritte nach dem Upgrade** unter Überlegungen zum Upgrade für benutzerdefinierte Konfigurationsdateien aus.

Im Folgenden finden Sie ein Beispiel für das NetScaler Firmware-Upgrade.

```
login: nsroot

Password: nsroot

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

Done

> save config

> shell

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

root@NSnnn# cd /var/nsinstall

root@NSnnn# cd 14.1

root@NSnnn# mkdir build_43.1

root@NSnnn# cd build_43.1

root@NSnnn# ftp <FTP server IP address>

ftp> mget build-14.1-41.1_nc.tgz

ftp> bye

root@NSnnn# tar xzvf build-14.1-41.1_nc.tgz

root@NSnnn# ./installns

installns version (14.1-41.1) kernel (ns-14.1-41.1_nc.gz)

...
```



```
36
37 Copying ns-14.1-41.1_nc.gz to /flash/ns-14.1-41.1_nc.gz ...
38
39 ...
40
41 Installation has completed.
42
43 Reboot NOW? [Y/N] Y
```

So aktualisieren Sie eine eigenständige NetScaler-Appliance mithilfe der CLI

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Upgrade einer eigenständigen NetScaler-Appliance mit der NITRO-API

Informationen zur Verwendung der NITRO-API zum Upgrade oder Downgrade eines NetScaler finden Sie unter Automatisieren von NetScaler Upgrade und Downgrade mit einer einzigen API.

Überprüfen des Entitätsstatus auf der NetScaler-Appliance nach dem Upgrade

Überprüfen Sie nach dem Upgrade der NetScaler-Appliance den Status der folgenden Entitäten:

- Virtuelle Server befinden sich im Status UP
- Monitore befinden sich im UP-Zustand
- GSLB-Sites synchronisieren sich ohne Probleme
- Alle Zertifikate sind auf dem Gerät vorhanden
- Alle Lizenzen sind auf der Appliance vorhanden

Überprüfen und installieren Sie NetScaler 14.1 Softwareupdate

Aktualisieren Sie die NetScaler-Software, wenn ein Update verfügbar ist, um eine bessere Leistung zu erzielen. Ein NetScaler-Update kann Funktionsverbesserungen, Leistungskorrekturen oder Verbesserungen enthalten. Lesen Sie unbedingt die Versionshinweise, um zu sehen, welche Korrekturen und Verbesserungen im Update verfügbar sind. Gehen Sie wie folgt vor, um ein Software-Update zu überprüfen und zu installieren.

1. Klicken Sie auf der NetScaler-Homepage im **nsroot-Menü** oben rechts auf **Nach Update suchen**.
2. Überprüfen Sie auf der Seite **Neueste Systemsoftwareupdates verfügbar** das verfügbare Softwareupdate, das Sie installieren können.
3. Klicken Sie auf **Herunterladen**, um das Installationspaket von der NetScaler-Download-Website herunterzuladen .

4. Nachdem Sie das Softwarepaket heruntergeladen haben, installieren Sie das Update entweder über CLI- oder GUI-Prozedur.

> **Hinweis**
>
> **Auf den Link "Nach Update suchen** " kann nur zugegriffen werden, wenn Sie sich über das HTTP-Protokoll und nicht über das HTTPS-Protokoll bei der GUI anmelden.

Zugehörige Ressourcen

Die folgenden Ressourcen enthalten verwandte Informationen zum Upgrade oder Herabstufung einer NetScaler-Appliance:

- Video-Tutorial - So aktualisieren Sie Ihren NetScaler mit CLI

Downgrade einer eigenständigen NetScaler-Appliance

August 15, 2023

Sie können über die CLI oder GUI auf eine frühere Version auf einem eigenständigen NetScaler downgraden.

> **Hinweis:**
>
> Bei einem Downgrade kann es zu Konfigurationsverlusten kommen. Vergleichen Sie die Konfigurationen vor und nach dem Downgrade und geben Sie dann alle fehlenden Einträge manuell erneut ein.

Downgrade einer NetScaler-Appliance über die CLI

Befolgen Sie die unten angegebenen Schritte, um eine NetScaler Standalone-Appliance mit Version 14.1 auf eine frühere Version herunterzustufen.

Stellen Sie in diesem Verfahren die Release-Version `<releasenumber>` dar, `<release>` auf die Sie ein Downgrade durchführen, und `<targetbuildnumber>` stellt die Build-Nummer dar, auf die Sie ein Downgrade durchführen.

1. Öffnen Sie mithilfe eines SSH-Clients wie PuTTY eine SSH-Verbindung zum NetScaler.
2. Melden Sie sich mithilfe der Administratoranmeldeinformationen beim NetScaler an. Speichern Sie die laufende Konfiguration. Geben Sie an der Eingabeaufforderung Folgendes ein:

   Konfiguration speichern
3. Erstellen Sie eine Kopie der Datei ns.conf. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

a) `cd /nsconfig`
b) `cp ns.conf ns.conf.NS<currentbuildnumber>`

Sie sollten eine Backup der Konfigurationsdatei auf einem anderen Computer sichern.

4. Kopieren Sie die Konfigurationsdatei für <releasenumber> (ns.conf.NS<releasenumber>) nach ns.conf. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cp ns.conf.NS<releasenumber> ns.conf
<!--NeedCopy-->
```

> **Hinweis:**
>
> `ns.conf.NS<releasenumber>` ist die Backup-Konfigurationsdatei, die automatisch erstellt wird, wenn die Systemsoftware von der Release-Version `<releasenumber>` auf die aktuelle Release-Version aktualisiert wird.
>
> Beim Downgrade kann es zu einem gewissen Konfigurationsverlust kommen. Vergleichen Sie nach dem Neustart der Appliance die in Schritt 3 gespeicherte Konfiguration mit der laufenden Konfiguration und nehmen Sie alle Anpassungen für Funktionen und Entitäten vor, die vor dem Downgrade konfiguriert wurden. Speichern Sie die laufende Konfiguration, nachdem Sie die Änderungen vorgenommen haben.
>
> **Wichtig:**
>
> Wenn Routing aktiviert ist, führen Sie Schritt 5 aus. Fahren Sie ansonsten mit Schritt 6 fort.

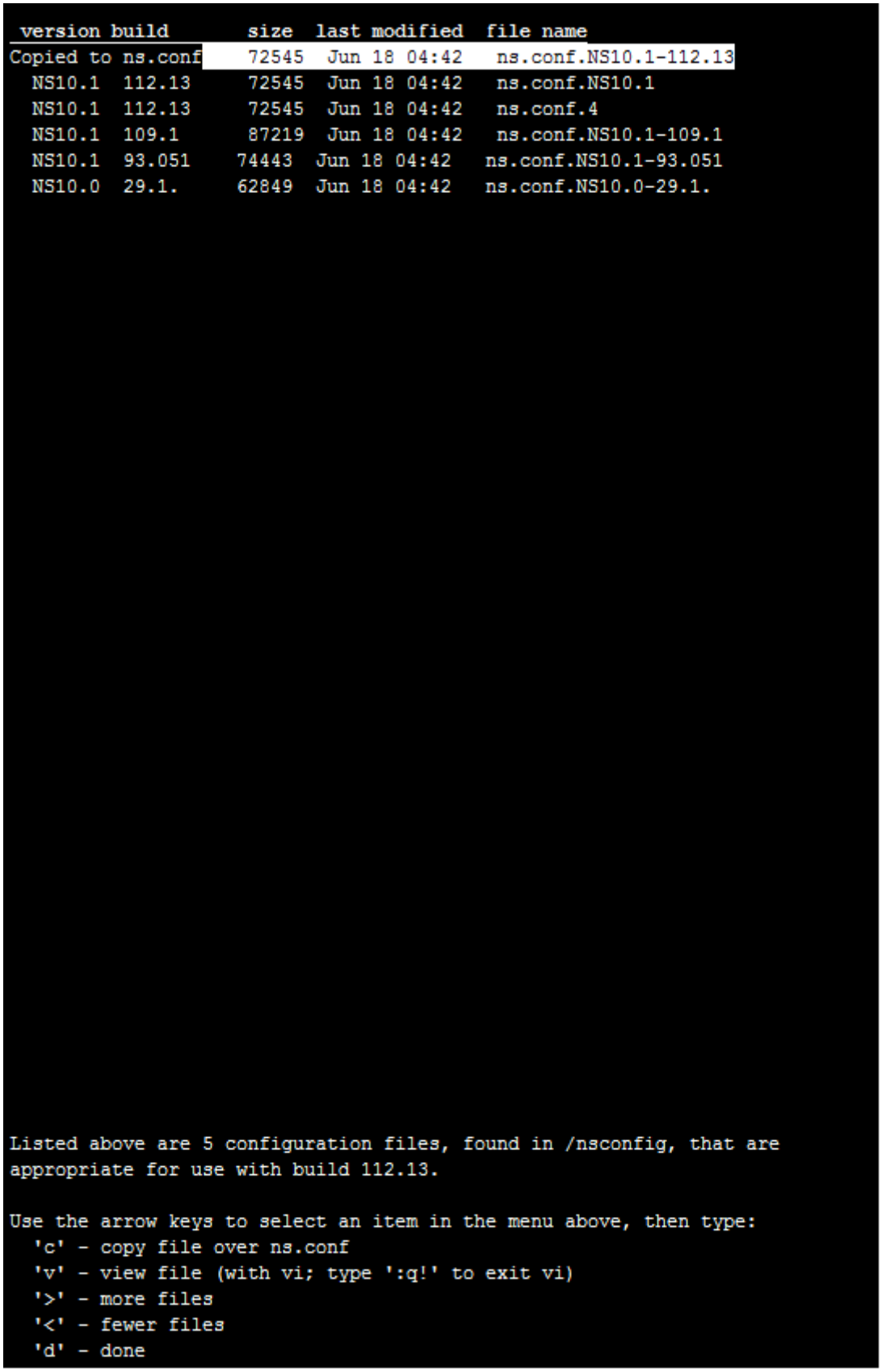
5. Wenn Routing aktiviert ist, enthält die Datei Zebos.conf die Konfiguration. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cd /nsconfig
cp ZebOS.conf ZebOS.conf.NS
cp ZebOS.conf.NS<targetreleasenumber> ZebOS.conf
<!--NeedCopy-->
```

6. Wechseln Sie in das Verzeichnis oder erstellen Sie eines `/var/nsinstall/<releasenumber>nsinstall`, falls es nicht existiert.
7. Wechseln Sie in das Verzeichnis oder erstellen Sie eines `build_<targetbuildnumber>`, falls es nicht existiert.
8. Laden Sie das Installationspaket (`build-<release>-<targetbuildnumber>.tgz`) herunter oder kopieren Sie es in dieses Verzeichnis und extrahieren Sie den Inhalt des Installationspakets.
9. Führen Sie das `installns` Skript aus, um die neue Version der Systemsoftware zu installieren. Das Skript aktualisiert das `/etc` Verzeichnis.

Wenn die Konfigurationsdatei für den Build, auf den Sie ein Downgrade durchführen, auf der Appliance vorhanden ist, werden Sie aufgefordert, diese Konfiguration zu laden:

Abbildung 1. Downgrade-Menü, falls eine Konfigurationsdatei existiert



Wenn der auf dem Flash-Laufwerk verfügbare freie Speicherplatz nicht ausreicht, um den neuen Build zu installieren, bricht NetScaler die Installation ab. Bereinigen Sie das Flash-Laufwerk manuell und starten Sie die Installation neu.

Beispiel:

```
login: nsroot

Password: nsroot

Last login: Mon Apr 24 02:06:52 2017 from 10.102.29.9

Done

> save config

> shell

root@NSnnn# cp ns.conf.NS10.5 ns.conf

root@NSnnn# cd /var/nsinstall

root@NSnnn# mkdir 10.5nsinstall

root@NSnnn# cd 10.5nsinstall

root@NSnnn# mkdir build_57

root@NSnnn# cd build_57

root@NSnnn# ftp 10.102.1.1

ftp> mget build-10.5-57_nc.tgz

ftp> bye

root@NSnnn# tar -xzvf build-10.1-125_nc.tgz

root@NSnnn# ./installns

installns version (10.5-57) kernel (ns-10.5-57.gz)

...

...
```



```
40
41 ...
42
43 Copying ns-10.5-57.gz to /flash/ns-10.5-57_nc.gz ...
44
45 Changing /flash/boot/loader.conf for ns-10.5-57 ...
46
47
48
49 Installation has completed.
50
51
52
53 Reboot NOW? [Y/N] Y
54 <!--NeedCopy-->
```

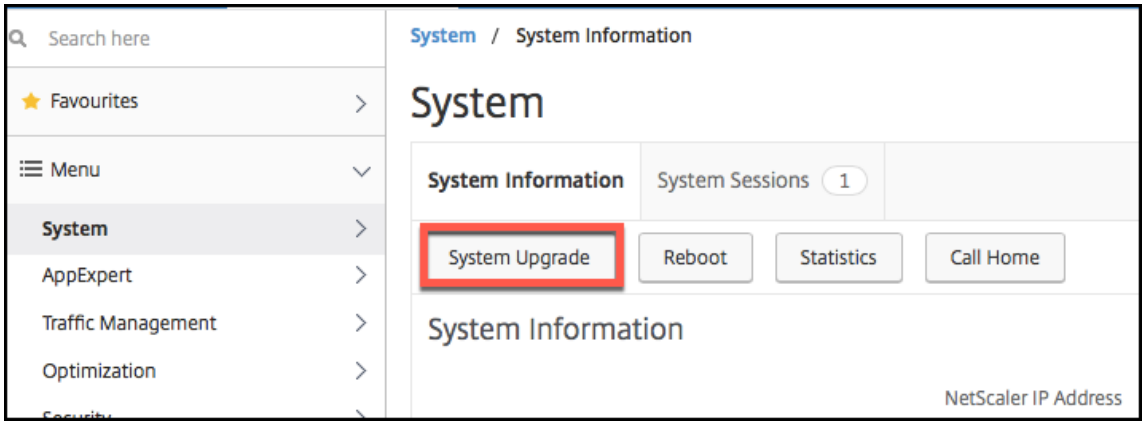
Downgrade einer NetScaler-Appliance über die GUI

Sie können den Upgrade-Assistenten der GUI verwenden, um eine NetScaler-Appliance mit Version 14.1 auf eine frühere Version herunterzustufen.

> **Hinweise:**
>
> Sie können eine NetScaler-Appliance, auf der Version 14.1 ausgeführt wird, mithilfe der GUI nicht direkt auf Version 10.5 oder früher herunterstufen. Citrix empfiehlt, die CLI zum Herunterstufen zu verwenden.
>
> Weitere Informationen zum NetScaler Release-Lebenszyklus finden Sie auf der Produktmatrix-Website .
>
> Es ist eine bewährte Methode, auf jeweils eine Hauptversion herabzusetzen.
>
> Wenn sich die NetScaler-Appliance beispielsweise auf Version 14.1 befindet und Sie ein Downgrade auf Version 13.0 durchführen möchten, müssen Sie die Appliance zuerst auf Version 13.1 und dann auf Version 13.0 herunterstufen.

Befolgen Sie die unten angegebenen Schritte, um eine NetScaler-Appliance mit Version 14.1 über die GUI auf eine frühere Version herunterzustufen.

1. Geben Sie beispielsweise in einem Webbrowser die IP-Adresse des NetScaler ein `http://10.102.29.50`.
2. Geben Sie unter Benutzername und Kennwort die Administratoranmeldeinformationen ein und klicken Sie dann **auf Anmelden**.
3. Klicken Sie auf der GUI auf **System Upgrade**.



4. Wählen Sie im Menü **Datei wählen** die entsprechende Option: **Lokal** oder **Gerät**. Wenn Sie die Option Appliance verwenden möchten, muss die Firmware zuerst auf den NetScaler hochgeladen werden. Sie können jede Dateiübertragungsmethode wie WinSCP verwenden, um die NetScaler-Firmware auf die Appliance hochzuladen.
5. Wählen Sie die richtige Datei aus und klicken Sie auf **Upgrade**.
6. Folgen Sie den Anweisungen zum Downgrade der Software.
7. Wenn Sie dazu aufgefordert werden, wählen Sie **Neustart** aus.

Schließen Sie nach dem Downgrade alle Browserinstanzen und löschen Sie den Cache Ihres Computers, bevor Sie auf die Appliance zugreifen.

Zugehörige Ressourcen

Die folgenden Ressourcen enthalten verwandte Informationen zum Upgrade oder Herabstufung einer NetScaler-Appliance:

- Video-Tutorial - So aktualisieren Sie Ihren NetScaler mit CLI

Ein Hochverfügbarkeitspaar aktualisieren

September 11, 2023

Eine der Anforderungen von NetScaler Appliances in einem Hochverfügbarkeits-Setup besteht darin, dieselbe NetScaler-Softwareversion auf beiden Appliances des Setups zu installieren. Wenn die Software auf einer Appliance aktualisiert wird, stellen Sie daher sicher, dass die Software auf beiden Appliances aktualisiert wird.

Sie können dasselbe Verfahren anwenden, um eine eigenständige Appliance oder jede Appliance in einem Hochverfügbarkeitspaar zu aktualisieren, obwohl für das Upgrade eines Hochverfügbarkeitspaars andere Überlegungen gelten.

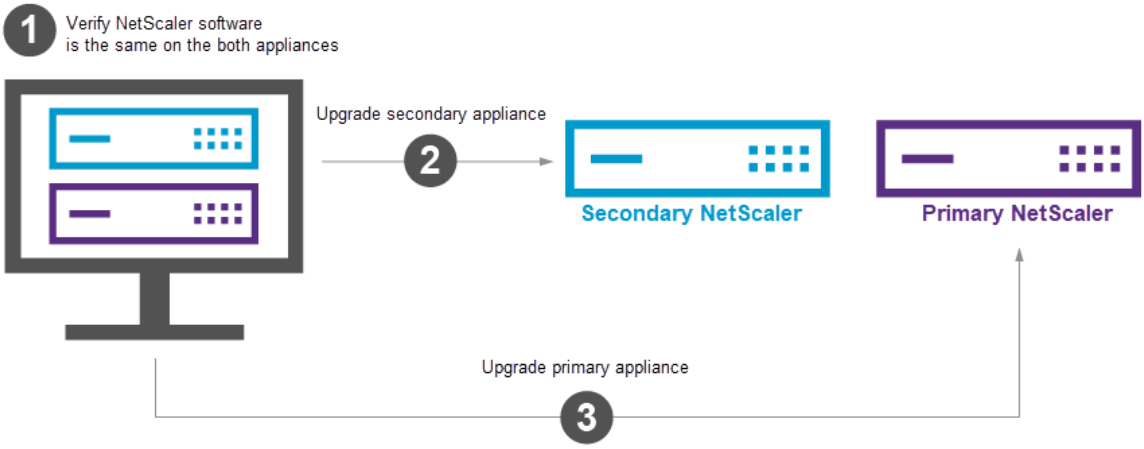
Bevor Sie ein NetScaler-Firmware-Upgrade auf einem HA-Paar starten, lesen Sie die im Abschnitt Bevor Sie beginnen genannten Voraussetzungen. Außerdem müssen Sie einige HA-spezifische Punkte berücksichtigen.

Wichtige Hinweise

> - **WICHTIG:**
>
> Es ist wichtig, dass sowohl die Upgrade-Änderungen als auch Ihre Anpassungen auf eine aktualisierte NetScaler-Appliance angewendet werden. Wenn Sie also benutzerdefinierte Konfigurationsdateien in dem `/etc` Verzeichnis haben, lesen Sie den Abschnitt Überlegungen zum Upgrade für benutzerdefinierte Konfigurationsdateien, bevor Sie mit dem Upgrade fortfahren.

- Aktualisieren Sie zuerst den sekundären Knoten und dann den primären Knoten. Durch das Aktualisieren der Software auf der sekundären Appliance vor der primären Appliance wird sichergestellt, dass der Upgrade-Vorgang problemlos abgeschlossen wird.

  Sie können das Upgrade mit der NetScaler CLI oder GUI durchführen.



- Wenn auf beiden Knoten in einem Hochverfügbarkeits-Setup (HA) unterschiedliche NetScaler-Softwareversionen ausgeführt werden, sind die folgenden Funktionen deaktiviert:
  - HA-Konfigurationssynchronisierung
  - Weitergabe von HA-Befehlen
  - HA-Synchronisierung von States-Dienste-Informationen
  - Verbindungsspiegelung (Verbindungsfailover) von Sitzungen
  - HA-Synchronisierung von Informationen zu Persistenzsitzungen
- Die oben genannten Funktionen sind deaktiviert, wenn auf beiden Knoten in einem Hochverfügbarkeits- (HA) -Setup unterschiedliche Builds derselben Version ausgeführt werden, beide Builds jedoch unterschiedliche interne HA-Versionen haben. Die oben genannten

Funktionen funktionieren einwandfrei, wenn auf beiden Knoten in einem Hochverfügbarkeits-setup (HA) unterschiedliche Builds derselben Version ausgeführt werden, beide Builds jedoch dieselben internen HA-Versionen haben.

Im Abschnitt Neue interne HA-Version in NetScaler-Builds können Sie überprüfen, ob sich die interne HA-Version in einem NetScaler-Build geändert hat.

- Die Synchronisation der Dateien im Modus „Alle“ des Befehls „HA-Dateien synchronisieren“ funktioniert erfolgreich, wenn auf den beiden Knoten in einer HA-Konfiguration unterschiedliche NetScaler-Softwareversionen ausgeführt werden oder auf den beiden Knoten unterschiedliche Builds derselben Version ausgeführt werden. Weitere Informationen finden Sie unter Synchronisieren von Konfigurationsdateien im Hochverfügbarkeits-Setup.

Neue interne HA-Version in NetScaler-Builds

In der folgenden Tabelle sind die NetScaler Builds aufgeführt, die eine neue interne HA-Version haben:

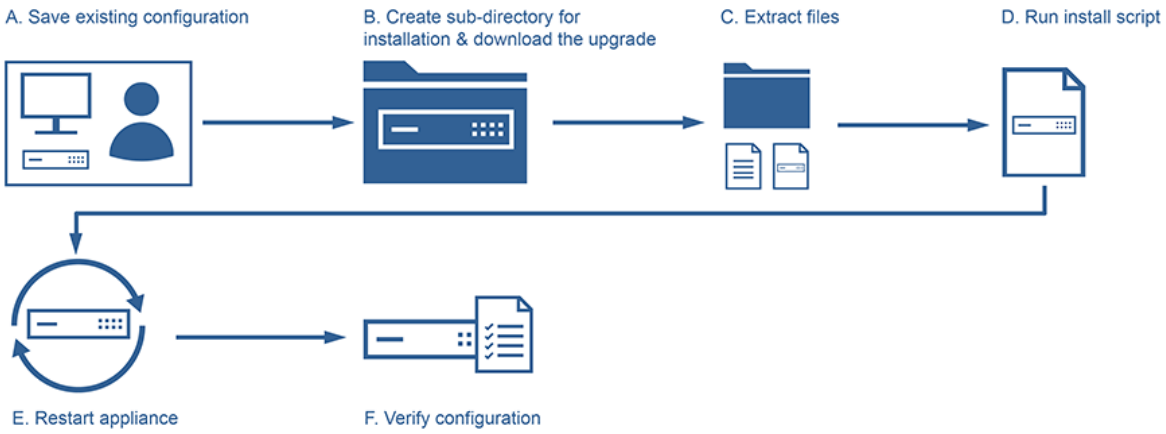
Version 14.1	Version 13.1	Release 13	Version 12.1
Build 4.42	Build 37.38	Build 87.9	Version 65.21
	Build 33.54	Build 86.17	Build 62.27
	Build 30.52	Build 85.19	Build 61.19
	Build 27.59	Build 84.11	Build 60.19
	Build 24.38	Build 82.45	Build 59.16
	Build 21.50	Build 79.64	Build 58.15
	Build 17.42	Build 76.31	Build 57.18
	Build 12.51	Build 71.44	Build 56.22
	Build 9.60	Build 67.43	Build 55.24
	Build 4.44	Build 64.35	Build 50.31
		Build 61.48	Build 49.37
		Build 58.32	
		Build 52.24	
		Build 41.28	

Upgrade eines Hochverfügbarkeitspaars mit der CLI

Der Upgrade-Prozess umfasst die folgenden Schritte:

1. Aktualisieren Sie die Software auf der sekundären Appliance
2. Software auf der primären Appliance aktualisieren

Die folgende Abbildung zeigt das Verfahren zum Aktualisieren der Software auf der Appliance:



Aktualisieren Sie die Software auf der sekundären Appliance

1. Melden Sie sich mit einem SSH-Hilfsprogramm wie PuTTY an der sekundären Appliance an und geben Sie die NetScaler IP (NSIP) an. Verwenden Sie die `nsroot` Anmeldeinformationen, um sich an der Appliance anzumelden.
2. Geben Sie über die Befehlszeilenschnittstelle der Appliance den folgenden Befehl ein, um die vorhandene Konfiguration zu speichern:

```
save config
<!--NeedCopy-->
```

3. Wechseln Sie zur Shell-Eingabeaufforderung:

```
shell
<!--NeedCopy-->
```

4. Führen Sie den folgenden Befehl aus, um zum Standardinstallationsverzeichnis zu wechseln:

```
cd /var/nsinstall
<!--NeedCopy-->
```

5. Führen Sie den folgenden Befehl aus, um ein temporäres Unterverzeichnis im `nsinstall` Verzeichnis zu erstellen:

```
mkdir x_xnsinstall
<!--NeedCopy-->
```


> **Hinweis:**
>
> Der Text x_x wird verwendet, um die NetScaler-Version für zukünftige Konfigurationen zu benennen. Das Verzeichnis für die Installationsdateien von NetScaler 14.1 heißt beispielsweise 13_1nsinstall. Verwenden Sie keinen Punkt (.) im Ordnernamen, da dies zu fehlgeschlagenen Upgrades führen kann.

6. Wechseln Sie in das Verzeichnis **x_xnsinstall** .
7. Laden Sie das erforderliche Installationspaket und das Dokumentationspaket, z. B. ns-x.0-xx.x-doc.tgz, in das in Schritt 4 erstellte temporäre Verzeichnis herunter.

   > **Hinweis:**
   >
   > Einige Builds haben kein Dokumentationspaket, da es nicht installiert werden muss.
   >
   > Klicken Sie in der GUI auf die Registerkarte **Dokumentation**, um auf die Dokumentation zuzugreifen.

8. Bevor Sie das Installationsskript ausführen, müssen die Dateien extrahiert und auf der Appliance platziert werden. Verwenden Sie den folgenden Befehl, um das von der Citrix-Website heruntergeladene Paket zu dekomprimieren: `tar -zxvf ns-x.0-xx.x-doc.tgz`. Im Folgenden finden Sie eine kurze Erklärung der verwendeten Parameter.

   - x - Extrahieren Sie Dateien.
   - v - Druckt die Dateinamen so, wie sie nacheinander extrahiert werden.
   - z - Die Datei ist eine `gzipped` Datei.
   - f - Verwenden Sie das folgende TAR-Archiv für die Operation.

9. Führen Sie den folgenden Befehl aus, um die heruntergeladene Software zu installieren:

   ```
   ./installns
   <!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > Wenn die Appliance nicht über genügend Festplattenspeicher verfügt, um die neuen Kerneldateien zu installieren, führt der Installationsvorgang eine automatische Bereinigung des Flash-Laufwerks durch.

10. Nach Abschluss des Installationsvorgangs werden Sie aufgefordert, die Appliance neu zu starten. Drücken Sie `y`, um das Gerät neu zu starten.
11. Melden Sie sich mit den `nsroot` Anmeldeinformationen bei der Befehlszeilenschnittstelle der Appliance an.
12. Führen Sie den folgenden Befehl von aus, um den Status der NetScaler Appliance anzuzeigen. Die Ausgabe des vorherigen Befehls muss angeben, dass es sich bei der Appliance um einen

sekundären Knoten handelt und die Synchronisation deaktiviert ist.

```
show ha node
<!--NeedCopy-->
```

13. Führen Sie den folgenden Befehl aus, um einen Failover und eine Übernahme als primäres Gerät zu erzwingen:

```
force failover
<!--NeedCopy-->
```

14. Stellen Sie sicher, dass die Appliance jetzt eine primäre Appliance ist.

    Hier ist eine Beispielkonfiguration im neuen Primärknoten.

```
login: nsroot
Password: nsroot
Last login: Monday Apr  17 08:37:26 2017 from 10.102.29.9
Done
show ha node
        2 nodes:
1)      Node ID:      0
        IP:        10.0.4.2
        Node State: UP
        Master State: Primary
        ...
        Sync State: AUTO DISABLED
        Propagation: AUTO DISABLED
        ...
Done
<!--NeedCopy-->
```

Software auf der primären Appliance aktualisieren

> **Hinweis:**
>
> Nach Abschluss des Verfahrens „Software auf der sekundären Appliance aktualisieren“ ist die ursprüngliche primäre Appliance jetzt eine sekundäre Appliance.

1. Melden Sie sich mit einem SSH-Hilfsprogramm wie PuTTY bei der sekundären Appliance an. Verwenden Sie die `nsroot` Anmeldeinformationen, um sich an der Appliance anzumelden. Folgen Sie den gleichen Schritten wie im vorherigen Abschnitt beschrieben, um den Installationsvorgang abzuschließen. Wir müssen dieselben Schritte ausführen, die in Schritt 2 bis Schritt 9 im vorherigen Abschnitt (Upgrade-Software der sekundären Appliance) erwähnt wurden.

2. Nach Abschluss des Installationsvorgangs werden Sie aufgefordert, die Appliance neu zu starten. Drücken Sie `y`, um das Gerät neu zu starten.
3. Melden Sie sich mit den `nsroot` Anmeldeinformationen bei der Befehlszeilenschnittstelle der Appliance an.
4. Führen Sie den folgenden Befehl aus, um den Status der NetScaler Appliance anzuzeigen. Die Ausgabe des vorherigen Befehls muss angeben, dass es sich bei der Appliance um einen sekundären Knoten handelt und der Status des Knotenstatus als UP markiert ist.

```
show ha node
<!--NeedCopy-->
```

5. Führen Sie den folgenden Befehl aus, um einen Failover zu erzwingen und sicherzustellen, dass es sich bei der Appliance um eine primäre Appliance handelt:

```
force failover
<!--NeedCopy-->
```

6. Stellen Sie sicher, dass es sich bei der Appliance um eine primäre Appliance handelt.

   Hier ist eine Beispielkonfiguration des neuen Primärknotens und des neuen Sekundärknotens.

```
show ha node
    Node ID:      0
    IP:   10.0.4.11
    Node State: UP
    Master State: Primary
    ...
    ...
    INC State: DISABLED
    Sync State: ENABLED
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    ...
    ...
    Local node information
    Critical Interfaces: 1/1
Done

Show ha node
    Node ID:      0
    IP:   10.0.4.2
    Node State: UP
```



```
    Master State: Secondary
    ..
    ..
    INC State: DISABLED
    Sync State: SUCCESS
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    . .
    . .
    Local node information:
    Critical Interfaces: 1/1
Done
<!--NeedCopy-->
```

Aktualisieren eines Hochverfügbarkeitspaars über die GUI

Gehen Sie wie folgt vor, um ein NetScaler-Paar in einem Hochverfügbarkeits-Setup mithilfe der ADC-GUI zu aktualisieren. Stellen Sie sich ein Beispiel für ein Hochverfügbarkeits-Setup der NetScaler Appliances CITRIX-ADC-A (primär) und CITRIX-ADC-B (sekundär) vor.

1. **Aktualisieren Sie den sekundären Knoten**. Melden Sie sich mit Administratoranmeldedaten bei der GUI des sekundären Knotens an, und aktualisieren Sie den Knoten, wie unter Aktualisieren einer eigenständigen NetScaler-Appliance mithilfe derGUI beschrieben.
2. **Failover erzwingen**. Führen Sie mithilfe der GUI ein erzwungenes Failover auf dem sekundären Knoten durch, wie unter Einen Knoten zum Failover erzwingenbeschrieben.

   Nach dem Failover-Vorgang übernimmt der sekundäre Knoten die Position des primären Knotens und der primäre Knoten wird der neue sekundäre Knoten. Nach dem Failover-Vorgang im HA-Beispiel-Setup:

   - CITRIX-ADC-B wird der neue Primärserver
   - CITRIX-ADC-A wird die neue Sekundärseite
3. **Aktualisieren Sie den ursprünglichen primären Knoten (neuer sekundärer Knoten)**. Melden Sie sich bei der neuen GUI für den sekundären Knoten (CITRIX-ADC-A) an und aktualisieren Sie den Knoten, wie unter Aktualisieren einer eigenständigen NetScaler-Appliance mithilfeder GUI beschrieben.
4. **Failover erzwingen**. Führen Sie mithilfe der GUI ein erzwungenes Failover auf dem neuen sekundären Knoten (CITRIX-ADC-A) durch, wie unter Einen Knoten zum Failover erzwingenbeschrieben.

Nach diesem zweiten Failover-Vorgang kehrt der Zustand beider Knoten in den Zustand vor dem Start des HA-Upgrade-Vorgangs zurück. Nach dem Failover-Vorgang im HA-Beispiel-Setup:

- CITRIX-ADC-A wird primär
- CITRIX-ADC-B wird zweitrangig

5. **Überprüfen Sie den Upgrade-Vorgang**. Melden Sie sich an der GUI beider Knoten an. Navigieren Sie zu **System > Hochverfügbarkeit**, überprüfen Sie auf der Detailseite den HA-Status beider Knoten. Überprüfen Sie außerdem die aktualisierten Versionsdetails, die im oberen Bereich der GUI angezeigt werden.

So aktualisieren Sie ein Hochverfügbarkeits-Setup mithilfe der GUI

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Support für Software-Upgrades im Dienst für Hochverfügbarkeit bei Upgrades ohne Ausfallzeiten

May 11, 2023

Während eines regulären Upgrade-Prozesses in einem Hochverfügbarkeitssetup führen beide Knoten irgendwann unterschiedliche Software-Builds aus. Diese beiden Builds können dieselbe oder unterschiedliche interne Versionsnummern für hohe Verfügbarkeit haben.

Wenn beide Builds unterschiedliche Versionsnummern für hohe Verfügbarkeit haben, wird ein Verbindungsfailover (auch wenn es aktiviert ist) für vorhandene Datenverbindungen nicht unterstützt. Mit anderen Worten, alle vorhandenen Datenverbindungen gehen verloren, was zu Ausfallzeiten führt.

Um dieses Problem zu beheben, kann in Service Software Upgrade (ISSU) für Hochverfügbarkeitssetups verwendet werden. ISSU führt eine Migrationsfunktion ein, die den Schritt des Force-Failover-Vorgangs im Aktualisierungsprozess ersetzt. Die Migrationsfunktion berücksichtigt die vorhandenen Verbindungen und umfasst den Force-Failover-Vorgang.

Nachdem ein Migrationsvorgang durchgeführt wurde, erhält der neue primäre Knoten immer Datenverkehr (Anfrage und Antwort) in Bezug auf die vorhandenen Verbindungen, leitet sie jedoch zum alten primären Knoten. Der alte primäre Knoten verarbeitet den Datenverkehr und sendet ihn dann direkt an das Ziel.

So funktioniert das erweiterte ISSU

Der reguläre Upgradeprozess in einem Hochverfügbarkeitssetup umfasst die folgenden Schritte:

1. **Aktualisieren Sie den sekundären Knoten**. Dieser Schritt umfasst ein Software-Upgrade des sekundären Knotens und einen Neustart des Knotens.
2. **Failover erzwingen**. Durch Ausführen des Force-Failovers wird der aktualisierte sekundäre Knoten zum primären Knoten und der primäre Knoten zum sekundären Knoten.
3. **Aktualisieren Sie den neuen sekundären Knoten**. Dieser Schritt umfasst ein Software-Upgrade des neuen sekundären Knotens und einen Neustart des Knotens.

Während des Zeitraums zwischen Schritt 1 und Schritt 3 führen beide Knoten unterschiedliche Software-Builds aus. Diese beiden Builds können dieselbe oder verschiedene interne Hochverfügbarkeitsversionen haben.

Wenn beide Builds unterschiedliche Versionsnummern für hohe Verfügbarkeit haben, wird ein Verbindungsfailover (auch wenn es aktiviert ist) für vorhandene Datenverbindungen nicht unterstützt. Mit anderen Worten, alle vorhandenen Datenverbindungen gehen verloren, was zu Ausfallzeiten führt.

Der ISSU-Upgrade-Prozess in einem Hochverfügbarkeitssetup umfasst die folgenden Schritte:

1. **Aktualisieren Sie den sekundären Knoten**. Dieser Schritt umfasst ein Software-Upgrade des sekundären Knotens und einen Neustart des Knotens.
2. **ISSU-Migrationsvorgang**. Der Schritt umfasst den Force-Failover-Vorgang und kümmert sich um die vorhandenen Verbindungen. Nachdem Sie den Migrationsvorgang ausgeführt haben, erhält der neue primäre Knoten immer Datenverkehr (Anforderung und Antwort) in Bezug auf die vorhandenen Verbindungen, leitet sie jedoch über das konfigurierte SYNC-VLAN im GRE-Tunnel zum alten primären Knoten. Der alte primäre Knoten verarbeitet den Datenverkehr und sendet ihn dann direkt an das Ziel. Der ISSU-Migrationsvorgang ist abgeschlossen, wenn alle vorhandenen Verbindungen geschlossen sind.
3. **Aktualisieren Sie den neuen sekundären Knoten**. Dieser Schritt umfasst ein Software-Upgrade des neuen sekundären Knotens und einen Neustart des Knotens.

Voraussetzungen

Bevor Sie mit der Durchführung des ISSU-Prozesses in einem Hochverfügbarkeits-Setup beginnen, sollten Sie die folgenden Voraussetzungen, Einschränkungen und Punkte beachten:

- Stellen Sie sicher, dass `SYNC VLAN` auf beiden Knoten des Hochverfügbarkeitssetups konfiguriert ist. Weitere Informationen finden Sie unter Beschränken des Synchronisationsdatenverkehrs für hohe Verfügbarkeit auf ein VLAN.
- ISSU wird in der Microsoft Azure-Cloud nicht unterstützt, da Microsoft Azure kein GRE-Tunneling unterstützt.

- Konfigurations-Propagierung und Synchronisierung mit hoher Verfügbarkeit funktionieren während der ISSU nicht.
- ISSU wird für IPv6-Hochverfügbarkeitssetup nicht unterstützt.
- ISSU wird in den folgenden Sitzungen nicht unterstützt:
  - Jumbo-Rahmen
  - IPv6-Sitzungen
  - NAT (LSN) in großem Maßstab
- In einem HA-Setup im INC-Modus migriert der ISSU-Migrationsvorgang nur die clientseitigen Verbindungen. Die Migration serverseitiger Verbindungen ist nicht erforderlich, da beide HA-Knoten über unabhängige SNIP-Konfigurationen verfügen.

Konfigurationsschritte

ISSU umfasst eine Migrationsfunktion, die den Force-Failover-Vorgang im regulären Upgrade-Prozess eines Hochverfügbarkeitssetups ersetzt. Die Migrationsfunktion berücksichtigt die vorhandenen Verbindungen und umfasst den Force-Failover-Vorgang.

Während des ISSU-Prozesses eines Hochverfügbarkeitssetups führen Sie den Migrationsvorgang unmittelbar nach dem Upgrade des sekundären Knotens aus. Sie können den Migrationsvorgang von einem der beiden Knoten aus ausführen.

CLI-Verfahren

So führen Sie den Migrationsvorgang für hohe Verfügbarkeit über die CLI durch:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
start ns migration
<!--NeedCopy-->
```

GUI-Verfahren

So führen Sie den Migrationsvorgang für hohe Verfügbarkeit über die GUI durch:

Navigieren Sie zu **System**, klicken Sie auf die Registerkarte **Systeminformationen**, klicken Sie auf **Registerkarte Migration**, und klicken Sie dann auf **Migration starten**.

ISSU Statistiken anzeigen

Sie können die ISSU-Statistiken zur Überwachung des aktuellen ISSU-Prozesses in einem Hochverfügbarkeitssetup anzeigen. In der ISSU-Statistik werden folgende Informationen angezeigt:

- Aktueller Stand des ISSU-Migrationsvorgangs
- Startzeit des ISSU-Migrationsvorgangs
- Endzeit des ISSU-Migrationsvorgangs
- Startzeit des ISSU Rollback-Vorgangs
- Gesamtzahl der Verbindungen, die im Rahmen des ISSU-Migrationsvorgangs verarbeitet werden
- Anzahl der verbleibenden Verbindungen, die im Rahmen des ISSU-Migrationsvorgangs verarbeitet werden

Sie können die ISSU-Statistiken auf einem der Hochverfügbarkeitsknoten mithilfe von CLI oder GUI anzeigen.

CLI-Verfahren

So zeigen Sie die ISSU-Statistiken über die CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 show ns migration
2 <!--NeedCopy-->
```

GUI-Verfahren

So zeigen Sie die ISSU-Statistiken mit der GUI an:

Navigieren Sie zu **System**, klicken Sie auf die Registerkarte **Systeminformationen**, klicken Sie auf **Registerkarte Migration**, und klicken Sie dann **auf Klicken, um Migrationsdetails anzuzeigen**

ISSU-Statistiken anzeigen — die Liste der vorhandenen Verbindungen, die der alte primäre Knoten verarbeitet

Sie können die Liste der vorhandenen Verbindungen anzeigen, die der alte primäre Knoten derzeit im Rahmen des ISSU-Migrationsvorgangs bedient, indem Sie die Option `dumpsession`(`Dump Session`) des Vorgangs `show migration` verwenden.

Der Showmigrationsvorgang mit der Option `dumpsession` darf während des ISSU-Vorgangs nur auf dem neuen primären Knoten ausgeführt werden.

CLI-Verfahren

So zeigen Sie die Liste der vorhandenen Verbindungen an, die der alte primäre Knoten derzeit mit der CLI verarbeitet:

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show ns migration  - dumpsession YES
<!--NeedCopy-->
```

```
> sh migration -dumpsession yes

Index   remote-IP-port          local-IP-port           idle-time(x 10
    ms)

1       192.0.2.10      22      192.0.2.1       15998       703
2       198.51.100.20   7375    98.51.100.2     22          687
3       203.0.113.30    5506    203.0.113.3     22          687


<!--NeedCopy-->
```

GUI-Verfahren

So zeigen Sie die Liste der vorhandenen Verbindungen an, die der alte Primärknoten derzeit mit der GUI verarbeitet:

Navigieren Sie zu **System**, klicken Sie auf die Registerkarte **Systeminformationen**, klicken Sie auf **Registerkarte Migration**, und klicken Sie dann **auf Klicken, um Migrationsverbindungen anzuzeigen**

Rollback des ISSU-Prozesses

Hochverfügbarkeitssetups (HA) unterstützen jetzt das Rollback des In Service Software Upgrade (ISSU) -Prozesses. Die ISSU-Rollback-Funktion ist hilfreich, wenn Sie feststellen, dass das HA-Setup während des ISSU-Migrationsvorgangs nicht stabil ist oder nicht wie erwartet auf einem optimalen Niveau funktioniert.

Das ISSU-Rollback ist anwendbar, wenn der ISSU-Migrationsvorgang im Gange ist. Das ISSU-Rollback funktioniert nicht, wenn der ISSU-Migrationsvorgang bereits abgeschlossen ist. Mit anderen Worten, Sie müssen den ISSU-Rollback-Vorgang ausführen, wenn der ISSU-Migrationsvorgang ausgeführt wird.

Das ISSU-Rollback funktioniert je nach Status des ISSU-Migrationsvorgangs unterschiedlich, wenn der ISSU-Rollback-Vorgang ausgelöst wird:

- Während des**ISSU-Migrationsvorgangs ist noch kein erzwungenes Failover aufgetreten**. Das ISSU-Rollback stoppt den ISSU-Migrationsvorgang und entfernt alle internen Daten im Zusammenhang mit der ISSU-Migration, die auf beiden Knoten gespeichert sind. Der aktuelle

primäre Knoten bleibt als primärer Knoten und verarbeitet weiterhin den Datenverkehr in Bezug auf bestehende und neue Verbindungen.

- **Während der ISSU-Migration ist ein erzwungenes Failover**aufgetreten Wenn das Hochverfügbarkeits-Failover während des ISSU-Migrationsvorgangs stattgefunden hat, verarbeitet der neue primäre Knoten (z. B. N1) den Datenverkehr in Bezug auf die neuen Verbindungen. Der alte primäre Knoten (neuer sekundärer Knoten, z. B. N2) verarbeitet den Datenverkehr im Zusammenhang mit den alten Verbindungen (vorhandene Verbindungen vor dem ISSU-Migrationsvorgang).

  Das ISSU Rollback stoppt den ISSU-Migrationsvorgang und löst ein erzwungenes Failover aus. Der neue primäre Knoten (N2) beginnt nun mit der Verarbeitung des Datenverkehrs im Zusammenhang mit den neuen Verbindungen. Der neue primäre Knoten (N2) verarbeitet auch weiterhin den Datenverkehr im Zusammenhang mit alten Verbindungen (bestehende Verbindungen, die vor dem ISSU-Migrationsvorgang hergestellt wurden). Mit anderen Worten, die vorhandenen Verbindungen, die vor dem ISSU-Migrationsvorgang hergestellt wurden, gehen nicht verloren.

  Der neue sekundäre Knoten (N1) entfernt alle vorhandenen Verbindungen (neue Verbindungen, die während des ISSU-Migrationsvorgangs erstellt wurden) und verarbeitet keinen Datenverkehr. Mit anderen Worten, alle vorhandenen Verbindungen, die nach dem erzwungenen Failover des ISSU-Migrationsvorgangs hergestellt wurden, gehen für immer verloren.

Konfigurationsschritte

Sie können die NetScaler CLI oder die GUI verwenden, um den ISSU-Rollback-Vorgang durchzuführen.

CLI-Verfahren

So führen Sie den ISSU-Rollback-Vorgang mit der CLI durch:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stop ns migration
<!--NeedCopy-->
```

GUI-Verfahren

So führen Sie den ISSU-Rollback-Vorgang mit der GUI durch:

Navigieren Sie zu **System**, klicken Sie auf die Registerkarte **Systeminformationen**, klicken Sie auf **Registerkarte Migration**, und klicken Sie dann auf **Migration beenden**.

SNMP-Traps für den Software-Upgrade-Prozess im Dienst

Der In Service Software Upgrade (ISSU) -Prozess für ein Hochverfügbarkeitssetup unterstützt die folgenden SNMP-Trap-Nachrichten zu Beginn und am Ende des ISSU-Migrationsvorgangs.

SNMP-Trap	Beschreibung
migrationStarted	Dieser SNMP-Trap wird generiert und an die konfigurierten SNMP-Trap-Listener gesendet, wenn der ISSU-Migrationsvorgang gestartet wird.
migrationComplete	Dieser SNMP-Trap wird generiert und an die konfigurierten SNMP-Trap-Listener gesendet, wenn der ISSU-Migrationsvorgang abgeschlossen ist.

Der primäre Knoten (vor dem Start des ISSU-Prozesses) generiert immer diese beiden SNMP-Traps und sendet sie an die konfigurierten SNMP-Trap-Listener.

Mit den ISSU SNMP-Traps sind keine SNMP-Alarme verknüpft. Mit anderen Worten, diese Traps werden unabhängig von einem SNMP-Alarm generiert. Sie müssen nur die Trap SNMP Listener konfigurieren.

Weitere Informationen zum Konfigurieren von SNMP-Trap-Listener finden Sie unter SNMP-Traps auf NetScaler.

Downgrade eines Hochverfügbarkeitspaares

May 11, 2023

Sie können ein Downgrade auf eine beliebige Version eines Hochverfügbarkeitspaars durchführen, indem Sie die Befehlszeilenschnittstelle verwenden. Die GUI unterstützt den Downgrade-Prozess nicht.

Um die Systemsoftware auf einem NetScaler Paar in einem Hochverfügbarkeitspaar herunterzustufen, müssen Sie die Software zuerst auf dem sekundären Knoten und dann auf dem primären Knoten herunterstufen. Anweisungen zum separaten Downgrade jedes Knotens finden Sie unter Downgrade einer eigenständigen NetScaler Appliance.

> **Wichtig**
>
> Bei einem Downgrade kann es zu Konfigurationsverlusten kommen. Sie sollten die Konfiguratio-

> nen vor und nach dem Downgrade vergleichen und dann alle fehlenden Einträge manuell erneut eingeben.

Behebung von Problemen im Zusammenhang mit den Installations-, Upgrade- und Downgrade-Prozessen

May 11, 2023

Wenn die Appliance nach Abschluss des Installations-, Upgrade- oder Downgrade-Vorgangs nicht wie erwartet funktioniert, müssen Sie zunächst nach den häufigsten Ursachen des Problems suchen.

Ressourcen für die Fehlerbehebung

Verwenden Sie für beste Ergebnisse die folgenden Ressourcen, um ein Problem im Zusammenhang mit der Installation, dem Upgrade oder dem Downgrade eines NetScaler zu beheben:

- Die Konfigurationsdateien von der Appliance. Im Falle eines Hochverfügbarkeitspaars die Konfigurationsdateien von beiden Appliances.
- Die folgenden Dateien von den Appliance (s):
  - Die relevanten Newslog-Dateien.
  - Die Datei ns.log.
  - Die Nachrichtendatei.
- Ein Netzwerktopologie-Diagramm.

Probleme und Lösungen

Im Folgenden finden Sie die häufigsten Installations-, Upgrade- und Downgrade-Probleme sowie Tipps zur Behebung dieser Probleme:

1. **Problem**

   Das Aktualisieren einer NetScaler MPX-Appliance schlägt aufgrund von Hardware- und Softwareinkompatibilität fehl.

   Auflösung

   Sehen Sie sich die NetScaler MPX Hardware-Software-Kompatibilitätsmatrix an und prüfen Sie, ob das Software-Release auf der NetScaler MPX-Hardware unterstützt wird.

2. **Problem**

   Das Aktualisieren einer NetScaler VPX-Appliance schlägt aufgrund der Inkompatibilität von NetScaler VPX Appliance und Hypervisor fehl.

Auflösung

Sehen Sie sich die NetScaler VPX Appliance und die Hypervisor-Kompatibilitätsmatrix an, und prüfen Sie, ob das NetScaler VPX Appliance-Modell auf dem Hypervisor unterstützt wird.

3. **Problem**

   Das Aktualisieren einer NetScaler-Appliance schlägt aufgrund von Hardwarefehlern fehl.

   Auflösung

   Überprüfen Sie die Integrität der NetScaler-Appliance. Wenn Sie über eine NetScaler Hardware-Appliance verfügen, empfiehlt Citrix, eine Festplattenprüfung durchzuführen und die Integrität der NetScaler -Festplatte zu überprüfen. `fsck`

   Weitere Informationen finden Sie unter Überprüfen der Dateisystemintegrität einer NetScaler-Appliance.

4. **Problem**

   Aktualisieren einer NetScaler-Appliance über die GUI-Stalls.

   Auflösung

   Aktualisieren Sie den Browser, um zu überprüfen, ob das Upgrade voranschreitet oder nicht.

5. **Problem**

   Das Aktualisieren einer NetScaler-Appliance schlägt aufgrund des geringen Speicherplatzes im Verzeichnis /var fehl

   Auflösung

   Geben Sie Speicherplatz im /var-Verzeichnis frei. Weitere Informationen finden Sie unter So geben Sie Speicherplatz im /var-Verzeichnis frei.

6. **Problem**

   Auf den NetScaler kann nach dem Software-Downgrade nicht zugegriffen werden

   Ursache

   Wenn während des Software-Downgrade-Prozesses die Konfigurationsdatei der vorhandenen Version und des Builds nicht mit der Konfigurationsdatei der früheren Version und des früheren Builds übereinstimmt, kann die Appliance die Konfiguration nicht laden, und die Standard-IP-Adresse wird der Appliance zugewiesen.

   Auflösung

   - Stellen Sie sicher, dass die Appliance von der Konsole aus zugänglich ist.
   - Überprüfen Sie die NSIP-Adresse und die Routen auf der Appliance.
     - Wenn sich die IP-Adresse auf die standardmäßige 192.168.100.1-IP-Adresse geändert hat, ändern Sie die IP-Adresse nach Bedarf.

- Stellen Sie sicher, dass die Appliance zugänglich ist.

7. **Problem**

   Wenn ich während eines Upgrades den Befehl zur Synchronisierung ausführe, wird die folgende Meldung angezeigt:

   Der Befehl ist auf dem sekundären Knoten fehlgeschlagen, aber auf dem primären Knoten erfolgreich.

   Auflösung

   Führen Sie keine abhängigen Befehle aus (set /unset /bind /unbind), wenn die Synchronisierung mit hoher Verfügbarkeit (HA) läuft.

8. **Problem**

   Während eines Upgrade-Vorgangs durchläuft der Datenverkehr den neuen primären Knoten nicht, wenn Sie den Befehl Force Failover ausführen.

   Auflösung

   - Prüfen Sie auf Probleme mit der Netzwerktopologie und den Switch-Konfigurationen.
   - Führen Sie den Befehl set L2Param -garpreply ENABLED aus, um die GARP-Antwort zu aktivieren.
   - Versuchen Sie es mit virtuellem MAC, falls nicht bereits verwendet.
   - Führen Sie den Befehl sendarp —a vom primären Knoten aus.

9. **Problem**

   Nach dem Upgrade oder Downgrade einer NetScaler-Appliance schlägt die Verbindung zur Appliance über SSH fehl.

   Auflösung

   Führen Sie die folgenden Vorgänge in der NetScaler-Appliance aus:

   - Entfernen Sie alte oder unsichere Host-Schlüssel bei `/nsconfig/ssh/ssh_host_*`.
   - Überprüfen Sie die benutzerdefinierte SSHD-Konfiguration unter `/nsconfig/sshd_config` und prüfen Sie, ob sie immer noch relevant und kompatibel ist. Benennen Sie die benutzerdefinierte SSHD-Konfiguration entsprechend um oder entfernen Sie sie.
   - Kaltstart der NetScaler-Appliance

10. **Problem**

    In einem HA-Paar starten die Geräte nach dem Ausführen des Befehls Force HA-Failover weiter neu. Das sekundäre Gerät wird nach einem Upgrade nicht hochgestellt.

    Auflösung

    Prüfen Sie, ob das Verzeichnis /var voll ist. Wenn ja, entfernen Sie die alten Installationsdateien. Führen Sie den Befehl df —h aus, um den verfügbaren Speicherplatz anzuzeigen.

11. **Problem**

    Nach dem Upgrade eines HA-Paares wird einer der Knoten als Status UNKNOWN aufgeführt.

    Auflösung

    - Prüfen Sie, ob beide Knoten denselben Build ausführen. Wenn die Builds nicht identisch sind und HA-Knoten eine Versionsübereinstimmung aufweisen, werden einige der Felder als UNKNOWN angezeigt, wenn Sie den Befehl show ha node ausführen.
    - Prüfen Sie, ob das sekundäre Gerät erreichbar ist.

12. **Problem**

    Nach dem Upgrade des NetScaler zeigt die Schnittstelle an, dass die meisten virtuellen Lastausgleichsserver und -dienste DOWN sind.

    Auflösung

    Stellen Sie sicher, dass die SNIP-Adresse auf der sekundären Appliance aktiv ist. Geben Sie außerdem den Befehl show service ein, um zu sehen, ob der Dienst ausgeführt wird.

13. **Problem**

    Nach dem Durchführen eines Upgrades sind alle virtuellen Server auf der sekundären Appliance ausgefallen.

    Auflösung

    Aktivieren Sie den HA-Status und die HA-Synchronisierung, indem Sie die folgenden Befehle ausführen:

    - set node hastate enable
    - set node hasync enable

    Das Deaktivieren von HA wird nicht empfohlen.

14. **Problem**

    Nach dem Durchführen eines Downgrades startet der NetScaler nicht ordnungsgemäß.

    Auflösung

    Prüfen Sie, ob die richtige Lizenz installiert wurde.

15. **Problem**

    In einem HA-Paar werden einige Funktionen nicht synchronisiert, nachdem ein Upgrade durchgeführt wurde.

    Auflösung

    Führen Sie den Befehl sync ha file misc aus, um die Konfigurationsdateien vom primären Knoten zum sekundären Knoten zu synchronisieren.

16. **Problem**

    Während des Neustarts wird die folgende Fehlermeldung angezeigt:

    Ein oder mehrere Befehle in ns.conf sind fehlgeschlagen Was soll ich tun?

    Auflösung

    Stellen Sie sicher, dass kein Befehl in der Datei ns.conf das 255-Byte-Limit überschreitet. In Befehlen, die Richtlinien erstellen, die für das 255-Byte-Limit zu lang sind, können Sie Mustersätze verwenden, um die Richtlinien zu verkürzen.

    Beispiel:

    ```
    add cs policy p11 -rule 'HTTP.REQ.URL.ENDSWITH_ANY("
        ctx_file_extensions")'
    Done
    <!--NeedCopy-->
    ```

    ctx_file_extensions ist ein Standard-Patset, das eine große Anzahl von Erweiterungen abdeckt. Zusätzlich zu den Standardmustersätzen können Sie benutzerdefinierte Mustersätze erstellen. Fügen Sie ein Patset hinzu, indem Sie den folgenden Befehl ausführen:

    ```
    add patset <name>
    <!--NeedCopy-->
    ```

    Hinweis: Patsets werden nur in Version 9.3 oder höher unterstützt.

17. **Problem**

    Beim Upgrade einer NetScaler VPX-Appliance werde ich aufgefordert, Speicherplatz in /var freizugeben. Welche Dateien entferne ich?

    Auflösung

    Entfernt die alten Installationsdateien aus dem Verzeichnis /var/tmp/. Entferne auch unerwünschte Dateien aus /flash.

18. **Problem**

    Es besteht keine Verbindung zur grafischen Benutzeroberfläche (GUI), wenn Sie den Befehl force HA-Failover auf der sekundären Appliance ausführen.

    Auflösung

    Melden Sie sich über die Befehlszeilenschnittstelle an der sekundären Appliance an und aktivieren Sie den Zugriff auf die GUI, indem Sie den Befehl set ns ip <IP> -gui enabled ausführen.

19. **Problem**

Nach dem Durchführen eines Upgrades und wenn ich auf einen Link auf der GUI klicke, der ein Java-Applet laden muss (Upgrade-Assistent oder Lizenzassistent), wird die folgende Fehlermeldung angezeigt: Die **GUI-Version stimmt nicht mit der Kernelversion überein. Bitte schließen Sie diese Instanz, löschen Sie den Java-Plug-In-Cache und öffnen Sie erneut**.

Auflösung

- Melden Sie sich mit der GUI beim NetScaler an.
- Navigieren Sie zu NetScaler Gateway > Globale Einstellungen.
- Klicken Sie unter Einstellungen auf Globale Einstellungen ändern.
- Wählen Sie im Detailbereich unter Client Experience in der Liste des UI-Themas die Option Standard aus.
- Klicken Sie auf OK.

20. **Problem**

    Wenn das Upgrade einer NetScaler-Appliance aus irgendeinem Grund fehlgeschlagen ist, wie kann die Appliance mithilfe der gesicherten Dateien wiederhergestellt werden?

    Auflösung

    Wenn das Upgrade nicht erfolgreich ist, stellen Sie die Appliance mithilfe der gesicherten Dateien auf die vorherige Version der NetScaler-Appliance wieder her. Weitere Informationen finden Sie unter Backup und Wiederherstellen einer NetScaler-Appliance.

    Weitere Informationen zum Backup und Wiederherstellen eines NetScaler Clustersetups finden Sie unter Backup und Wiederherstellen eines Clustersetups.

21. **Problem**

    Wie kann das Problem behoben werden, wenn nach einem fehlgeschlagenen Upgrade einer NetScaler-Appliance Lizenzen fehlen?

    Auflösung

    Wenn eine Lizenz fehlt oder Sie die Lizenzen neu zuweisen möchten, lesen Sie das folgende Thema Übersicht über die Lizenzierung.

> **Hinweis**
>
> Diese Schritte zur Fehlerbehebung gelten auch für Probleme mit Konfigurationsverlust beim Downgrade der Software über mehrere Versionen hinweg.
>
> Für jedes andere Problem lesen Sie die Versionshinweise, Artikel des Knowledge Center und FAQs.

FAQ

May 11, 2023

Antworten auf die Fragen, die Sie möglicherweise zum Upgrade der NetScaler-Firmware haben, finden Sie unter Häufig gestellte Fragen zum Installieren, Aktualisieren und Downgraden .

Lösungen für Telekommunikationsdienstleister

May 11, 2023

Bei der Informations- und Kommunikationstechnologie (IKT) geht es darum, den Internetnutzer den Apps und Daten näher zu bringen. Die neuesten Rechenzentrumstechnologien haben es ermöglicht, dass Benutzer, Apps und Daten überall lokalisiert werden können. Ein Benutzer kann vom Büro oder von zu Hause aus oder von einem Ort wie einem Flughafen aus auf Apps und Daten zugreifen. Die Apps und Daten können sich entweder in den Räumlichkeiten des Unternehmens, in einer öffentlichen oder privaten Cloud oder auf einem Hybrid-Host befinden. Das Ergebnis war nur eine höhere Produktivität, aber auch geringere Betriebs- und Wartungskosten.

Dienstanbieter bieten die Kerninfrastruktur, die für die Übertragung der Apps und Daten des Benutzers über das Netzwerk erforderlich ist. Da die Kerninfrastruktur Millionen von Abonnenten und eine Vielzahl von Apps und Daten bedient, sind die Anforderungen an Skalierung und Protokollunterstützung sehr hoch. Die Kerninfrastruktur verarbeitet zwei Hauptarten von Verkehr: Datenebene und Steuerungsebene. Jedes dieser Flugzeuge hat seine eigenen Anforderungen an die Skalierung und die Protokollunterstützung.

Die Datenebene ist der Teil der Kerninfrastruktur, der Benutzeranwendungen und -daten von Ende zu Ende überträgt, d. h. zwischen den Geräten des Endbenutzers und dem Anwendungsserver. Die Anzahl der Benutzer, die auf Apps und Daten zugreifen, geht in die Tausende von Millionen, sodass die Anforderungen an Durchsatz und IP-Adressierung sehr hoch sind. Jeder Benutzer im Netzwerk muss eindeutig identifizierbar sein. Nur dann kann der Dienstanbieter den Datenverkehr kontrollieren, die Netzwerknutzung überwachen, benutzerspezifische Dienste bereitstellen und Informationen korrekt protokollieren. Viele der heutigen Client-Geräte und Anwendungsserver unterstützen IPv6 nativ. Die Kerninfrastruktur muss nicht nur eine Mischung aus IPv4- und IPv6-Clients und -Servern unterstützen, sondern auch die Technologien für die Querkommunikation zwischen IPv4 und IPv6 bereitstellen. Schließlich wird ein Dienstanbieter an der Servicequalität (die in direktem Zusammenhang mit der Erfahrung der Endnutzer steht) und der Verfügbarkeit des Dienstes ohne Unterbrechungen gemessen. Die Datenebene sollte robust genug sein, um gleichzeitig Qualität und Verfügbarkeit zu gewährleisten.

Die Infrastruktur auf der Steuerungsebene verwaltet den Benutzerverkehr und verwaltet die Geschäfts- und Netzwerkbetriebsdienste. Die wichtigsten der vielen Protokolle, die in dieser Ebene

laufen, sind Diameter, Radius und SMPP. Diameter ist ein Basisprotokoll, auf dessen Grundlage mehrere andere funktionsspezifische Protokolle entwickelt wurden. Zum Beispiel:

- Gx-Schnittstelle zwischen der Policy and Charging Enforcement Function (PCEF) und der Policy and Charging Rules Function (PCRF)
- Gy-Schnittstelle zwischen dem Online Charging System (OCS) und dem Cisco Packet Data Network Gateway (PGW) /Policy and Charging Enforcement Function (PCEF)

Das Volumen des Verkehrs auf der Kontrollebene steht in direktem Verhältnis zur Benutzeraktivität. Um den Verkehr auf der Steuerungsebene zu verwalten, verwenden Dienstanbieter verschiedene ADC-Funktionen wie Load Balancing und Content Switching. Sie benötigen eine detaillierte Kontrolle des Verkehrs auf der Steuerungsebene, was in seiner Komplexität dem Datenebenenverkehr entspricht.

Dienstanbieter müssen anspruchsvolle Service Level Agreements (SLAs) einhalten und werden von den Aufsichtsbehörden eingehend auf ihre Einhaltung überprüft. Die Einhaltung der Anforderungen bei der Verwaltung des Daten- und Steuerungsebenenverkehrs erfordert von einem Dienstanbieter, seine Infrastruktur agil, budgetgerecht, leicht erweiterbar und flexibel zu halten. Als die leistungsstärksten und fortschrittlichsten ADCs, die derzeit auf dem Markt erhältlich sind, eignen sich NetScaler-Produkte hervorragend für Service Provider-Umgebungen.

NAT im großen Maßstab

September 1, 2023

> **Hinweis:**
>
> Die Large Scale NAT (LSN) -Funktion ist ab Version NetScaler 14.1 veraltet.
>
> Veraltete Funktionen werden nicht sofort entfernt. Die NetScaler Appliance unterstützt die veraltete Funktion weiterhin, bis sie in einer zukünftigen Version entfernt wird.

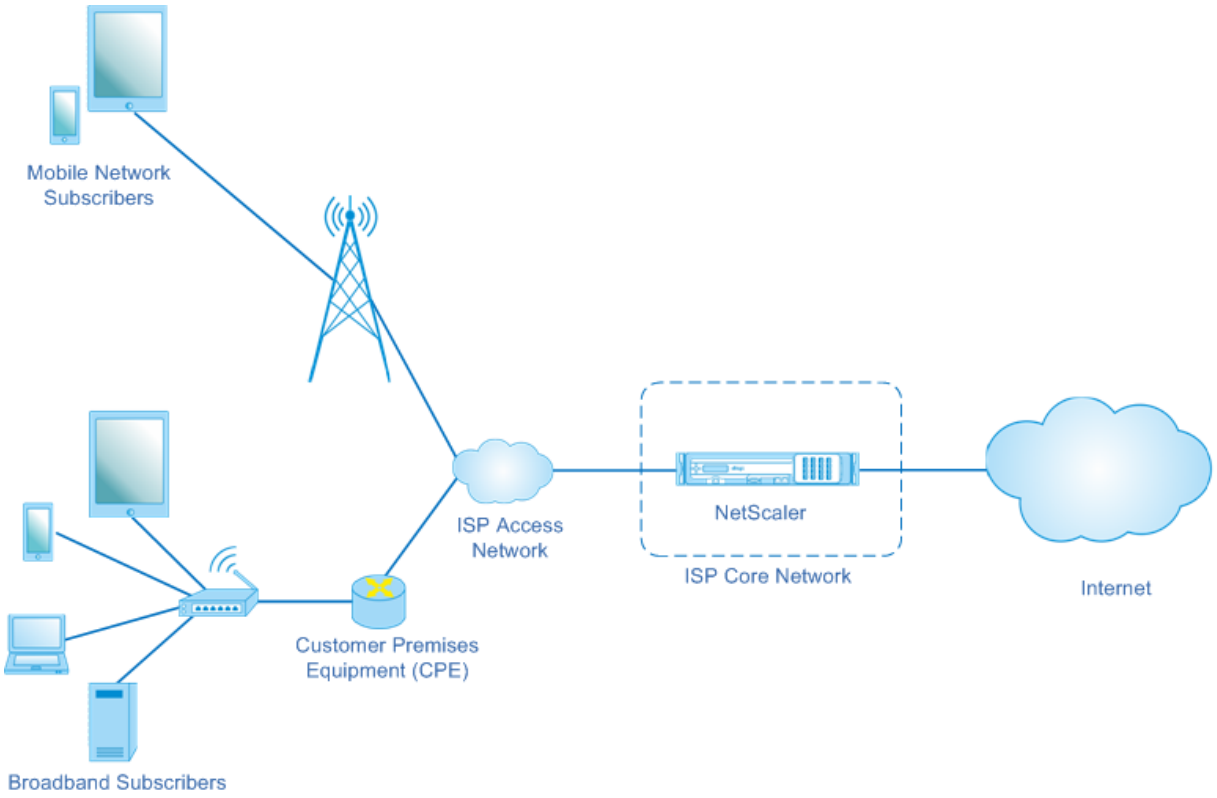
Das phänomenale Wachstum des Internets hat zu einem Mangel an öffentlichen IPv4-Adressen geführt. Large Scale NAT (LSN/CGNAT) bietet eine Lösung für dieses Problem und maximiert die Nutzung verfügbarer öffentlicher IPv4-Adressen, indem einige öffentliche IPv4-Adressen von einem großen Pool von Internetbenutzern gemeinsam genutzt werden.

LSN übersetzt private IPv4-Adressen in öffentliche IPv4-Adressen. Es umfasst Methoden zur Netzwerkadressen- und Portübersetzung, um viele private IP-Adressen zu weniger öffentlichen IPv4-Adressen zusammenzufassen. LSN ist darauf ausgelegt, NAT in großem Maßstab zu handhaben. Die NetScaler LSN-Funktion ist sehr nützlich für Internetdienstanbieter (ISPs) und Netzbetreiber, die Millionen von Übersetzungen zur Unterstützung einer großen Anzahl von Benutzern (Abonnenten) und bei sehr hohem Durchsatz bereitstellen.

LSN-Architektur

Die LSN-Architektur eines ISP, der NetScaler-Produkte verwendet, besteht aus Abonnenten (Internetbenutzern) in privaten Adressräumen, die über eine NetScaler-Appliance, die im Kernnetzwerk des ISP bereitgestellt wird, auf das Internet zugreifen. Abonnenten sind über das Zugangsnetz des ISP mit dem ISP verbunden. Normalerweise sind Abonnenten für die kommerzielle Nutzung des Internets direkt mit dem Zugangsnetz des ISP verbunden. Für die Betreuung dieser Abonnenten ist nur ein NAT-Level (NAT44) erforderlich.

Nichtkommerzielle Abonnenten stehen jedoch in der Regel hinter kundeneigenen Geräten (CPE) wie Routern und Modems, die auch NAT implementieren. Diese beiden NAT-Ebenen bilden das NAT444-Modell. Die Bereitstellung einer NetScaler-Appliance im Kernnetzwerk eines ISP für die LSN-Funktionalität ist für die Abonnenten transparent und erfordert keine Konfigurationsänderungen für die Abonnenten oder die CPEs.



Large Scale NAT

Die NetScaler-Appliance empfängt alle Abonnentenpakete, die für das Internet bestimmt sind. Die Appliance ist mit einem Pool vordefinierter NAT-IP-Adressen konfiguriert, die für LSN verwendet werden. Die NetScaler-Appliance verwendet ihre LSN-Funktion, um die Quell-IP-Adresse (privat) und den Port des Pakets in die NAT-IP-Adresse (öffentlich) und den NAT-Port zu übersetzen und das Paket dann an sein Ziel im Internet zu senden. Die Appliance zeichnet alle aktiven Sitzungen auf, die die LSN-Funktion verwenden. Diese Sitzungen werden als LSN-Sitzungen bezeichnet. Die NetScaler-Appliance verwaltet auch die Zuordnungen zwischen der IP-Adresse und dem Port des

Abonnenten sowie der NAT-IP-Adresse und dem Port für jede Sitzung. Diese Zuordnungen werden als LSN-Mappings bezeichnet. Anhand von LSN-Sitzungen und LSN-Zuordnungen erkennt die NetScaler-Appliance ein Antwortpaket (aus dem Internet empfangen), das zu einer bestimmten Sitzung gehört. Die Appliance übersetzt die Ziel-IP-Adresse und den Port des Antwortpakets von NAT-IP-Adresse:Port in die Abonnenten-IP-Adresse:Port und sendet das übersetzte Paket an den Abonnenten.

Von der NetScaler-Appliance unterstützte LSN-Funktionen

Im Folgenden werden einige der LSN-Funktionen beschrieben, die auf der NetScaler-Appliance unterstützt werden:

NAT-Ressourcenzuweisung

Die NetScaler-Appliance weist Abonnenten NAT-IP-Adressen und -Ports aus ihrem vordefinierten NAT-Ressourcenpool zu, um ihre Pakete für die Übertragung an externe Hosts (Internet) zu übersetzen. Die NetScaler-Appliance unterstützt die folgenden Arten von NAT-IP-Adressen und Portzuweisungen für Abonnenten:

- **Deterministisch.** Die NetScaler-Appliance weist jedem Abonnenten eine NAT-IP-Adresse und einen Block von Ports zu. Die Appliance weist diesen Abonnenten sequentiell NAT-Ressourcen zu. Es weist den ersten Portblock auf der ersten NAT-IP-Adresse der ersten Abonnenten-IP-Adresse zu. Der nächste Portbereich wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht mehr über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock an der nächsten NAT-Adresse dem Abonnenten zugewiesen usw.

  Die NetScaler-Appliance protokolliert die zugewiesene NAT-IP-Adresse und den Portblock für einen Abonnenten. Bei einer Verbindung kann ein Abonnent nur anhand seiner zugeordneten NAT-IP-Adresse und seines Portblocks identifiziert werden. Aus diesem Grund protokolliert die NetScaler-Appliance keine erstellten oder gelöschten LSN-Sitzungen. Wenn der gesamte Portblock verwendet wird, unterbricht die NetScaler-Appliance jede neue Verbindung des Abonnenten.

- **Dynamisch.** Die NetScaler-Appliance weist der Verbindung eines Abonnenten eine zufällige NAT-IP-Adresse und einen Port aus dem LSN-NAT-Pool zu. Wenn die Portblockzuweisung in der Konfiguration aktiviert ist, weist die Appliance einem Abonnenten eine zufällige NAT-IP-Adresse und einen Block von Ports zu, wenn sie zum ersten Mal eine Verbindung initiiert. Die NetScaler-Appliance weist dann jeder nachfolgenden Verbindung von diesem Abonnenten diese NAT-IP-Adresse und einen der Ports aus dem zugewiesenen Block zu. Wenn der gesamte Portblock verwendet wird, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu, wenn sie eine neue Verbindung initiiert. Einer der Port im neuen Portblock ist für die neue Verbindung zugewiesen.

IP-Pooling

Die folgenden NAT-Ressourcenzuweisungsoptionen sind für nachfolgende Sitzungen eines Abonnenten verfügbar, dem eine zufällige NAT-IP-Adresse und ein Port für eine bestehende Sitzung zugewiesen wurden.

- **Gepaart.** Die NetScaler-Appliance weist allen Sitzungen, die demselben Abonnenten zugeordnet sind, dieselbe NAT-IP-Adresse zu. Wenn für diese Adresse keine Ports mehr verfügbar sind, unterbricht die Appliance alle neuen Verbindungen des Abonnenten. Diese Option ist für das reibungslose Funktionieren bestimmter Anwendungen erforderlich, die die Erstellung mehrerer Sitzungen an derselben Quell-IP-Adresse erfordern (z. B. in Peer-to-Peer-Anwendungen, die das RTP- oder RTCP-Protokoll verwenden).
- **Zufällig.** Die NetScaler-Appliance weist zufällige NAT-IP-Adressen aus dem Pool für verschiedene Sitzungen zu, die demselben Abonnenten zugeordnet sind.

LSN-Zuordnungen wiederverwenden

Die NetScaler-Appliance kann eine vorhandene LSN-Map für neue Verbindungen wiederverwenden, die von derselben Abonnenten-IP-Adresse und demselben Port ausgehen. Die NetScaler LSN-Funktion unterstützt die folgenden Arten der Wiederverwendung von LSN-Mappings:

1. **Endgeräteunabhängig.** Die NetScaler-Appliance verwendet die LSN-Zuordnung für nachfolgende Pakete, die von derselben Abonnenten-IP-Adresse und demselben Port (x:X) an jede externe IP-Adresse und jeden Port gesendet werden. Diese Art der Wiederverwendung von LSN-Karten ist nützlich für das reibungslose Funktionieren von VOIP- und Peer-to-Peer-Anwendungen.
2. **Adressabhängig.** Die NetScaler-Appliance verwendet die LSN-Zuordnung für nachfolgende Pakete, die von derselben Abonnenten-IP-Adresse und demselben Port (x:X) an dieselbe externe IP-Adresse (Y) gesendet werden, unabhängig vom externen Port.
3. **Abhängig vom Adressport.** Die NetScaler-Appliance verwendet das LSN-Mapping für nachfolgende Pakete, die von derselben internen IP-Adresse und demselben Port (x:X) an dieselbe externe IP-Adresse und denselben Port (y:Y) gesendet werden, solange das Mapping noch aktiv ist.

LSN-Filterung

Die NetScaler-Appliance kann Pakete von externen Hosts auf der Grundlage der aktiven LSN-Sitzungen und LSN-Zuordnungen filtern. Stellen Sie sich ein Beispiel für eine LSN-Zuordnung vor, die die Zuordnung von Abonnenten-IP:Port (x:X), NAT-IP:Port (n:N) und externem Host-IP:Port (y:Y) umfasst. Die NetScaler LSN-Funktion unterstützt die folgenden Filtertypen:

1. **Endgeräteunabhängig.** Die NetScaler-Appliance filtert nur die Pakete heraus, die nicht für den

NAT-IP:Port (n:N) bestimmt sind, der Abonnenten-IP:Port (x:X) darstellt, unabhängig von der externen Host-IP-Adresse und der Portquelle (z:Z). Die NetScaler-Appliance leitet alle Pakete weiter, die für x:x bestimmt sind. Mit anderen Worten, das Senden von Paketen vom Abonnenten an eine beliebige externe IP-Adresse reicht aus, um Pakete von einem beliebigen externen Host an den Abonnenten zuzulassen. Diese Art der Filterung ist nützlich für das reibungslose Funktionieren von VOIP- und Peer-to-Peer-Anwendungen.

2. **Adressabhängig.** Die NetScaler-Appliance filtert Pakete heraus, die nicht für NAT IP:Port (n:N) bestimmt sind, was Abonnenten-IP:Port (x:X) darstellt. Darüber hinaus filtert die Appliance Pakete von der externen Host-IP-Adresse und dem Port (Y:Y) heraus, die für N:n bestimmt sind, wenn der Abonnent zuvor keine Pakete an y:AnyPort gesendet hat (unabhängig vom externen Port). Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an die IP-Adresse dieses bestimmten externen Hosts sendet.
3. **Abhängig vom Adressport.** Die NetScaler-Appliance filtert Pakete heraus, die nicht für NAT IP:Port (n:N) bestimmt sind, was Abonnenten-IP:Port (x:X) darstellt. Darüber hinaus filtert die Appliance Pakete von der externen Host-IP-Adresse und dem Port (Y:y) heraus, die für N:n bestimmt sind, falls der Abonnent zuvor keine Pakete an Y:y gesendet hat. Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an diese bestimmte externe IP-Adresse und diesen Port sendet.

Kontingente

Die NetScaler-Appliance kann die Anzahl der NAT-Ports und -Sitzungen für jeden Abonnenten begrenzen, um eine faire Verteilung der Ressourcen unter den Abonnenten zu gewährleisten. Die NetScaler-Appliance kann auch die Anzahl der Sitzungen für eine Abonnentengruppe begrenzen, um eine faire Verteilung der Ressourcen auf verschiedene Abonnentengruppen zu gewährleisten.

- **Hafenkontingent.** Die NetScaler-Appliance kann die LSN-NAT-Ports einschränken, die jeweils von jedem Abonnenten für ein bestimmtes Protokoll verwendet werden. Sie könnten beispielsweise jeden Abonnenten auf maximal 500 TCP-NAT-Ports beschränken. Wenn die LSN-NAT-Zuordnungen für einen Abonnenten das Limit erreichen, weist die NetScaler-Appliance diesem Abonnenten keine zusätzlichen NAT-Ports des angegebenen Protokolls zu.
- **Sitzungslimit für Abonnenten.** Die Anzahl gleichzeitiger Sitzungen für einen Abonnenten kann das Portkontingent überschreiten. Die NetScaler-Appliance kann die LSN-Sitzungen einschränken, die für jeden Abonnenten für ein bestimmtes Protokoll zulässig sind. Wenn die Anzahl der LSN-Sitzungen das Limit für einen Abonnenten erreicht, erlaubt die NetScaler-Appliance dem Abonnenten nicht, weitere Sitzungen des angegebenen Protokolls zu öffnen.
- **Limit für Gruppensitzungen.** Die NetScaler-Appliance kann die Gesamtzahl der LSN-Sitzungen begrenzen, die für eine Abonnentengruppe für ein bestimmtes Protokoll zulässig sind. Wenn die Gesamtzahl der LSN-Sitzungen das Limit für eine Gruppe für ein bestimmtes

Protokoll erreicht, erlaubt die NetScaler-Appliance keinem Abonnenten der Gruppe, zusätzliche Sitzungen des angegebenen Protokolls zu öffnen. Sie beschränken beispielsweise eine Gruppe auf maximal 10000 UDP-Sitzungen. Wenn die Gesamtzahl der UDP-Sitzungen für diese Gruppe 10000 erreicht, erlaubt die NetScaler-Appliance keinem Abonnenten der Gruppe, weitere UDP-Sitzungen zu öffnen.

Gateways auf Anwendungsebene

Bei einigen Protokollen auf Anwendungsebene werden die IP-Adressen und Protokollportnummern auch in der Payload des Pakets übermittelt. Das Application Layer Gateway für ein Protokoll analysiert die Nutzdaten des Pakets und nimmt die erforderlichen Änderungen vor, um sicherzustellen, dass das Protokoll weiterhin über LSN funktioniert.

Die NetScaler-Appliance unterstützt ALG für die folgenden Protokolle:

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Haarnadelstütze

Die NetScaler-Appliance unterstützt die Kommunikation zwischen Abonnenten oder internen Hosts mithilfe von NAT-IP-Adressen. Diese Art der Kommunikation zwischen zwei Teilnehmern unter Verwendung von NAT-IP-Adressen wird als Hairpin Flow bezeichnet. Der Haarnadelfluss ist standardmäßig aktiviert und kann nicht deaktiviert werden.

Vor dem Konfigurieren von LSN zu berücksichtigende Punkte

May 11, 2023

Beachten Sie die folgenden Punkte, bevor Sie LSN auf einer NetScaler-Appliance konfigurieren:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten von Large Scale NAT verstehen, die in den RFCs 6888, 5382, 5508 und 4787 beschrieben werden.
- Endpoint Independent Mapping (EIM) und Endpoint Independent Filterung (EIF) sind standardmäßig deaktiviert. Diese Optionen müssen aktiviert sein, damit VoIP- und Peer-to-Peer-Anwendungen (P2P) ordnungsgemäß funktionieren.

- **LSN protokollieren**: Im Folgenden sind die wichtigsten Punkte für die Protokollierung von LSN-Informationen aufgeführt:
  - Citrix empfiehlt, die LSN-Informationen auf externen Protokollservern statt auf der NetScaler-Appliance zu protokollieren. Die Protokollierung auf externen Servern ermöglicht eine optimale Leistung, wenn die Appliance eine große Anzahl von LSN-Protokolleinträgen erstellt (in der Größenordnung von Millionen).
  - Citrix empfiehlt die Verwendung von SYSLOG über TCP oder NSLOG. Standardmäßig verwendet SYSLOG UDP und NSLOG verwendet nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist für die Übertragung vollständiger Daten zuverlässiger als UDP.
  - Die folgenden Einschränkungen gelten für SYSLOG über TCP:
    * Die Syslog-over-TCP-Lösung bietet keine Authentifizierung, Integritätsprüfung und Datenschutz.
    * Die NetScaler-Appliance stützt sich auf das TCP-Protokoll, um die Übermittlung von SYSLOG-Nachrichten an externe Protokollserver zu bestätigen.
- **Hohe Verfügbarkeit**: Im Folgenden sind die wichtigsten Punkte für die Hochverfügbarkeit von NetScaler-Appliances für LSN aufgeführt:
  - Citrix empfiehlt, die LSN-Funktion in einer Hochverfügbarkeitsbereitstellung von zwei NetScaler-Appliances zu konfigurieren, um einen unterbrechungsfreien und reibungslosen Betrieb aller LSN-Sitzungen zu gewährleisten.
  - Für eine Bereitstellung mit hoher Verfügbarkeit empfiehlt Citrix:
    * Einstellung des SYNC-VLAN-Parameters für die Dedizierung eines VLANs für die gesamte HA-bezogene Kommunikation.
    * Synchronisierung des symmetrischen RSS-Schlüssels des primären Knotens mit dem sekundären Knoten zur statusmäßigen Synchronisation einer großen Anzahl von LSN-Zuordnungen und -Sitzungen.
    * Binden Sie das Subnetz der LSN-IP-Adressen an ein VLAN, um eine Flut von GARP-Broadcasts auf allen VLANs nach einem Failover zu vermeiden.
  - Bei einer Bereitstellung von NetScaler-Appliances mit hoher Verfügbarkeit werden ALG-bezogene Sitzungen nicht auf die sekundäre Appliance übertragen.
- **Application Layer Gateways (ALGs)**: Im Folgenden finden Sie die wichtigsten Punkte im Zusammenhang mit ALGs auf einer NetScaler-Appliance:
  - Folgendes wird für SIP ALG nicht unterstützt:
    * Multicast-IP-Adressen
    * Verschlüsseltes SDP
    * SIP-Nachrichten über TLS
    * FQDN-Übersetzung in SIP-Nachrichten
    * Authentifizierung von SIP-Nachrichten
    * Verkehrsdomänen, Admin-Partitionen und NetScaler-Cluster.

        * SIP-Nachrichten mit mehrteiligen Textteilen.
    - Folgendes wird für RTSP ALG nicht unterstützt:
        * Multicast-RTSP-Sitzungen
        * RTSP-Sitzung über UDP
        * NetScaler-Verkehrsdomänen, Admin-Partitionen und NetScaler-Cluster
    - Die NetScaler-Appliance unterstützt ALG für das IPSec-Protokoll nicht.
- Wenn Sie die LSN-Funktion deaktivieren, obwohl einige LSN-Sitzungen auf der NetScaler-Appliance vorhanden sind, bestehen diese Sitzungen für die Dauer des konfigurierten Timeout-Intervalls weiter.
- LSN hat Vorrang vor RNAT. Wenn ein Paket von einem angegebenen LSN-Abonnenten auch einer RNAT-Regel entspricht, wird das Paket gemäß der LSN-Konfiguration übersetzt.
- Die Weiterleitung von Paketen, die sich nur auf die LSN-Sitzungen beziehen, basiert auf der Routingtabelle der NetScaler-Appliance.
- Im Gegensatz zu Subnetz-IP-Adressen basiert die Auswahl einer LSN-NAT-IP-Adresse für die Verbindung eines Abonnenten nicht auf dem Routing-Eintrag für die Ziel-IP-Adresse.
- Bei eingehenden Paketen haben statische LSN-Zuordnungen Vorrang vor dynamischen LSN-Zuordnungen.
- Bei ausgehenden Paketen haben LSN-Anwendungsprofile Vorrang vor statischer Zuordnung.
- Wenn auf der NetScaler-Appliance eine große Anzahl von LSN-Sitzungen (> 1 Million) vorhanden ist, empfiehlt Citrix, ausgewählte LSN-Sitzungen statt aller anzuzeigen. Verwenden Sie in der Befehlszeilenschnittstelle oder im Konfigurationsprogramm die Auswahlparameter, um den LSN-Sitzungsbetrieb anzuzeigen.
- Um die Menge an aktivem Speicher zu reduzieren, die der LSN-Funktion zugewiesen ist, müssen Sie die NetScaler-Appliance warmstarten, nachdem Sie die konfigurierte Speichereinstellung geändert haben. Ohne einen warmen Neustart können Sie nur die Menge des aktiven Speichers erhöhen.

Konfigurationsschritte für LSN

May 11, 2023

Die Konfiguration von LSN auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

1. **Stellen Sie die globalen LSN-Parameterein.** Zu den globalen Parametern gehören die Menge des NetScaler-Speichers, der für die LSN-Funktion reserviert ist, und die Synchronisation von LSN-Sitzungen in einem Hochverfügbarkeits-Setup.
2. **Erstellen Sie eine LSN-Client-Entität und binden Sie Abonnenten daran.** Eine LSN-Client-Entität ist eine Gruppe von Abonnenten, für deren Datenverkehr die NetScaler-Appliance LSN ausführen soll. Die Client-Entität enthält IPv4-Adressen und erweiterte ACL-Regeln zur Identi-

fizierung von Abonnenten. Ein LSN-Client kann nur an eine LSN-Gruppe gebunden werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen einer LSN-Client-Entität und zum Binden eines Abonnenten an die LSN-Client-Entität. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.

3. **Erstellen Sie einen LSN-Pool und binden Sie NAT-IP-Adressen daran.** Ein LSN-Pool definiert einen Pool von NAT-IP-Adressen, die von der NetScaler-Appliance zur Ausführung von LSN verwendet werden. Dem Pool werden Parameter wie Portblockzuweisung und NAT-Typ (Deterministisch oder Dynamisch) zugewiesen. Ein an eine LSN-Gruppe gebundener LSN-Pool gilt für alle Abonnenten einer LSN-Client-Entität, die an dieselbe Gruppe gebunden ist. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Für dynamisches NAT kann ein LSN-Pool an mehrere LSN-Gruppen gebunden werden. Für deterministisches NAT können Pools, die an eine LSN-Gruppe gebunden sind, nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen eines LSN-Pool und zum Binden von NAT-IP-Adressen an den LSN-Pool. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.
4. **(Optional) Erstellen Sie ein LSN-Transportprofil für ein bestimmtes Protokoll.** Ein LSN-Transportprofil definiert verschiedene Timeouts und Limits, wie z. B. maximale LSN-Sitzungen und maximale Portauslastung, die ein Abonnent für ein bestimmtes Protokoll haben kann. Sie binden ein LSN-Transportprofil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes Profil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für die Protokolle TCP, UDP und ICMP bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standard-Transportprofil bezeichnet. Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das Standard-LSN-Transportprofil für dieses Protokoll.
5. **(Optional) Erstellen Sie ein LSN-Anwendungsprofil für ein bestimmtes Protokoll und binden Sie eine Reihe von Zielports daran.** Ein LSN-Anwendungsprofil definiert die LSN-Zuordnung und die LSN-Filterung einer Gruppe für ein bestimmtes Protokoll und für eine Reihe von Zielports. Für eine Reihe von Zielports binden Sie ein LSN-Profil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes LSN-Anwendungsprofil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für die TCP-, UDP- und ICMP-Protokolle für alle Zielports bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardanwendungsprofil bezeichnet. Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen eines LSN-

Anwendungsprofils und zum Binden einer Reihe von Zielports an das LSN-Anwendungsprofil. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.

6. **Erstellen Sie eine LSN-Gruppe und binden Sie LSN-Pools, (optional) LSN-Transportprofile und (optional) LSN-Anwendungsprofile an die LSN-Gruppe.** Eine LSN-Gruppe ist eine Entität, die aus einem LSN-Client, einem oder mehreren LSN-Pool (en), LSN-Transportprofilen und LSN-Anwendungsprofilen besteht. Einer Gruppe werden Parameter wie die Portblockgröße und die Protokollierung von LSN-Sitzungen zugewiesen. Die Parametereinstellungen gelten für alle Abonnenten eines LSN-Clients, der an die LSN-Gruppe gebunden ist. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Für dynamisches NAT kann ein LSN-Pool an mehrere LSN-Gruppen gebunden werden. Für deterministisches NAT können Pools, die an eine LSN-Gruppe gebunden sind, nicht an andere LSN-Gruppen gebunden werden. Nur eine LSN-Client-Entität kann an eine LSN-Gruppe gebunden werden, und eine LSN-Client-Entität, die an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen einer LSN-Gruppe und zum Binden von LSN-Pools, LSN-Transportprofilen und LSN-Anwendungsprofilen an die LSN-Gruppe. Das Konfigurationsprogramm kombiniert diese beiden Operationen in einem einzigen Bildschirm.

In der folgenden Tabelle ist die maximale Anzahl verschiedener LSN-Entitäten und Bindungen aufgeführt, die auf einer NetScaler-Appliance erstellt werden können. Diese Grenzwerte hängen auch vom verfügbaren Speicher auf der NetScaler-Appliance ab.

LSN-Entitäten und -Bindungen	Limit
LSN-Kunden	1024
LSN-Pools	128
LSN-Gruppen	1024
Abonnentennetzwerke, die an einen LSN-Client gebunden werden können	64
Erweiterte ACLs, die an einen LSN-Client gebunden werden können	1024
NAT-IP-Adressen in einem Pool	4096
LSN-Pools, die an eine LSN-Gruppe gebunden werden können	8
LSN-Gruppen, die denselben LSN-Pool verwenden können	16

LSN-Entitäten und -Bindungen	Limit
LSN-Transportprofile, die an eine LSN-Gruppe gebunden werden können	3 (jeweils eins für TCP-, UDP- und ICMP-Protokolle)
LSN-Gruppen, die dasselbe LSN-Transportprofil verwenden können	8
LSN-Anwendungsprofile, die an eine LSN-Gruppe gebunden werden können	64
LSN-Gruppen, die dasselbe LSN-Anwendungsprofil verwenden können	8
Portbereiche, die an ein LSN-Anwendungsprofil gebunden werden können	8

Konfiguration über die Befehlszeilenschnittstelle

So erstellen Sie einen LSN-Client mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

So binden Sie mithilfe der Befehlszeilenschnittstelle eine Netzwerkadresse oder eine ACL-Regel an einen LSN-Client

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn client <clientname> ((-network <ip_addr> [-netmask <netmask>]
    [-td<positive_integer>]) | -aclname <string>)

show lsn client
<!--NeedCopy-->
```

So erstellen Sie einen LSN-Pool mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
add lsn pool <poolname> [-nattype ( DYNAMIC | DETERMINISTIC )] [-
    portblockallocation ( ENABLED | DISABLED )] [-portrealloctimeout <
    secs>] [-maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

So binden Sie einen IP-Adressbereich mithilfe der Befehlszeilenschnittstelle an einen LSN-Pool

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Hinweis: Verwenden Sie den Befehl unbind lsn pool, um LSN-IP-Adressen aus einem LSN-Pool zu entfernen.

So erstellen Sie ein LSN-Transportprofil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Anwendungsprofil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```


So binden Sie einen Portbereich eines Anwendungsprotokolls mithilfe der Befehlszeilenschnittstelle an ein LSN-Anwendungsprofil

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

So erstellen Sie eine LSN-Gruppe mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging (
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync (ENABLED | DISABLED )] [-snmptraplimit <positive_integer
    >] [-ftp ( ENABLED | DISABLED )]

show lsn group
<!--NeedCopy-->
```

So binden Sie LSN-Profile und LSN-Pools mithilfe der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -appsprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Konfiguration mit dem Configuration Utility

So konfigurieren Sie einen LSN-Client und binden eine IPv4-Netzwerkadresse oder eine ACL-Regel mithilfe des Konfigurationsprogramms

Navigieren Sie zu **System** > **Large Scale NAT** > **Clients**, fügen Sie einen Client hinzu und binden Sie dann eine IPv4-Netzwerkadresse oder eine ACL-Regel an den Client.

So konfigurieren Sie einen LSN-Pool und binden NAT-IP-Adressen mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **System > Large Scale NAT** > **Pools**, fügen Sie einen Pool hinzu und binden Sie dann eine NAT-IP-Adresse oder einen Bereich von NAT-IP-Adressen an den Pool.

So konfigurieren Sie ein LSN-Transportprofil mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **System > Large Scale NAT > Profile**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Transport**, und fügen Sie dann ein Transportprofil hinzu.

So konfigurieren Sie ein LSN-Anwendungsprofil mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **System > Large Scale NAT > Profile**.
2. Klicken Sie im Detailbereich auf die Registerkarte **Anwendung** und fügen Sie dann ein Anwendungsprofil hinzu.

So konfigurieren Sie eine LSN-Gruppe und binden einen LSN-Client, Pools, Transportprofile und Anwendungsprofile mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **System > Large Scale NAT > Groups**, fügen Sie eine Gruppe hinzu und binden Sie dann einen LSN-Client, Pools, Transportprofile und Anwendungsprofile an die Gruppe.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- LSN-Client hinzufügen
  - clientname

    Name für die LSN-Client-Entität. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Client erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn client1" oder 'lsn client1').

    Dies ist ein zwingendes Argument. Maximale Länge: 127

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- LSN-Client binden
  - clientname

    Name für die LSN-Client-Entität. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash

(#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Client erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn client1" oder 'lsn client1').

Dies ist ein zwingendes Argument. Maximale Länge: 127

- network

  IPv4-Adresse (n) der LSN-Abonnenten oder Abonnentennetzwerke, auf deren Datenverkehr die NetScaler-Appliance Large Scale NAT ausführen soll.

- Netzmaske

  Subnetzmaske für die im Netzwerkparameter angegebene IPv4-Adresse.

  Standardwert: 255.255.255.255

- td

  ID der Verkehrsdomäne, zu der dieser Teilnehmer oder das Abonnentennetzwerk (wie im Netzwerkparameter angegeben) gehört.

  Wenn Sie keine ID angeben, wird der Abonnent oder das Abonnentennetzwerk Teil der Standard-Verkehrsdomäne.

  Standardwert: 0

  Mindestwert: 0

  maximaler Wert: 4094

- ACL-Name

  Name (n) aller konfigurierten erweiterten ACL (s), deren Aktion ALLOW ist. Die in der erweiterten ACL-Regel angegebene Bedingung identifiziert den Datenverkehr von einem LSN-Abonnenten, für den die NetScaler-Appliance NAT in großem Umfang ausführen soll. Maximale Länge: 127

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- LSN-Pool hinzufügen

  - Poolname

    Name für den LSN-Pool. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Pool erstellt wurde. Die folgende

Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn pool1" oder 'lsn pool1').

Dies ist ein zwingendes Argument. Maximale Länge: 127

- Nat-Typ

  Art der NAT-IP-Adresse und Portzuweisung (aus den an eine LSN-Gruppe gebundenen LSN-Pools) für Abonnenten (der an die LSN-Gruppe gebundenen LSN-Client-Entität):

  Die verfügbaren Optionen funktionieren wie folgt:

  * **Deterministisch**— Weisen Sie jedem Abonnenten (des an die LSN-Gruppe gebundenen LSN-Clients) eine NAT-IP-Adresse und einen Block von Ports zu. Die NetScaler-Appliance weist diesen Abonnenten sequentiell NAT-Ressourcen zu. Die NetScaler-Appliance weist der ersten Abonnenten-IP-Adresse den ersten Portblock (die Blockgröße wird durch den Portblockgrößenparameter der LSN-Gruppe bestimmt) auf der ersten NAT-IP-Adresse zu. Der nächste Portbereich wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht mehr über genügend Ports für den nächsten Abonnenten verfügt. In diesem Fall wird der erste Portblock an der nächsten NAT-Adresse für den Abonnenten verwendet usw. Da jeder Abonnent jetzt eine deterministische NAT-IP-Adresse und einen Block von Ports erhält, kann ein Abonnent identifiziert werden, ohne dass eine Protokollierung erforderlich ist. Bei einer Verbindung kann ein Abonnent nur anhand der NAT-IP-Adresse und des Port sowie der Ziel-IP-Adresse und des Port identifiziert werden.
  * **Dynamisch**— Weisen Sie einer Abonnentenverbindung eine zufällige NAT-IP-Adresse und einen Port aus dem LSN-NAT-Pool zu. Wenn die Portblockzuweisung aktiviert ist (im LSN-Pool) und eine Portblockgröße angegeben ist (in der LSN-Gruppe), weist die NetScaler-Appliance einem Abonnenten eine zufällige NAT-IP-Adresse und einen Portblock zu, wenn sie zum ersten Mal eine Verbindung initiiert. Die Appliance weist diese NAT-IP-Adresse und einen Port (aus dem zugewiesenen Portblock) für verschiedene Verbindungen dieses Abonnenten zu. Wenn alle Ports (für verschiedene Abonnentenverbindungen) aus dem dem Abonnenten zugewiesenen Portblock zugewiesen sind, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden.

    Mögliche Werte: DYNAMIC, DETERMINISTIC

    Standardwert: DYNAMIC

- Zuweisung von Portblöcken

Weisen Sie jedem Abonnenten einen zufälligen NAT-Portblock aus dem verfügbaren NAT-Portpool einer NAT-IP-Adresse zu, wenn die NAT-Zuweisung auf Dynamic NAT festgelegt ist. Für jede von einem Abonnenten initiierte Verbindung weist die NetScaler-Appliance einen NAT-Port aus dem dem Abonnenten zugewiesenen NAT-Portblock zu, um die LSN-Sitzung zu erstellen.

Sie müssen die Portblockgröße in der gebundenen LSN-Gruppe festlegen. Wenn für einen Abonnenten alle Ports aus dem dem Abonnenten zugewiesenen Portblock zugewiesen sind, weist die NetScaler-Appliance dem Abonnenten einen neuen zufälligen Portblock zu.

Für Deterministisches NAT ist dieser Parameter standardmäßig aktiviert und kann nicht deaktiviert werden.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

- Timeout für Portrealloc-Timeout

  Die Wartezeit in Sekunden zwischen der Freigabe von LSN-NAT-Ports (wenn eine LSN-Zuordnung entfernt wird) und deren Neuzuweisung für eine neue LSN-Sitzung. Dieser Parameter ist erforderlich, um Kollisionen zwischen alten und neuen Mappings und Sessions zu verhindern. Es stellt sicher, dass alle eingerichteten Sitzungen unterbrochen werden, anstatt an einen anderen Abonnenten umgeleitet zu werden. Dies gilt nicht für Ports, die verwendet werden in:

  * Deterministisches NAT
  * Adressabhängige Filterung und adressportabhängige Filterung
  * Dynamisches NAT mit Portblockzuweisung

  In diesen Fällen werden die Ports sofort neu zugewiesen.

  Standardwert: 0

  Maximalwert: 600

- MaxPort Realloctmq

  Maximale Anzahl von Ports, für die das Timeout für die Port-Neuzuweisung gilt, für jede NAT-IP-Adresse. Mit anderen Worten, die maximale Größe der Warteschlange für freigegebene Port, für die das Zeitlimit für die Neuzuweisung gilt, für jede NAT-IP-Adresse.

  Wenn die Warteschlangengröße voll ist, wird die nächste Portfreigabe sofort für eine neue LSN-Sitzung neu zugewiesen.

  Standardwert: 65536

  Maximaler Wert: 65536

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- Lindenpool binden
  - Poolname

    Name für den LSN-Pool. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Pool erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn pool1" oder 'lsn pool1').

    Dies ist ein zwingendes Argument. Maximale Länge: 127
  - Lsnip

    IPv4-Adresse oder ein Bereich von IPv4-Adressen, die als NAT-IP-Adressen für LSN verwendet werden sollen.

    Nachdem der Pool erstellt wurde, werden diese IPv4-Adressen der NetScaler-Appliance als NetScaler-eigene IP-Adresse vom Typ LSN hinzugefügt. Eine LSN-IP-Adresse, die einem LSN-Pool zugeordnet ist, kann nicht mit anderen LSN-Pools geteilt werden. Die für diesen Parameter angegebenen IP-Adressen dürfen nicht bereits auf der NetScaler-Appliance vorhanden sein, ebenso wie NetScaler-eigene IP-Adressen. Trennen Sie den Bereich in der Befehlszeilenschnittstelle durch einen Bindestrich. Zum Beispiel: 10.102.29.30-10.102.29.189. Später können Sie einige oder alle LSN-IP-Adressen aus dem Pool entfernen und dem LSN-Pool IP-Adressen hinzufügen.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- lsn transportprofile hinzufügen
  - Name des Transportprofils

    Name für das LSN-Transportprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem das LSN-Transportprofil erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn transport profile1" oder 'lsn transport profile1').

    Dies ist ein zwingendes Argument. Maximale Länge: 127

- Transportprotokoll

  Protokoll, für das die LSN-Transportprofilparameter festgelegt werden sollen.

  Dies ist ein zwingendes Argument.

  Mögliche Werte: TCP, UDP, ICMP

- Sitzungs-Timeout

  Timeout in Sekunden für eine inaktive LSN-Sitzung. Wenn eine LSN-Sitzung für eine Zeit inaktiv ist, die diesen Wert überschreitet, entfernt die NetScaler-Appliance die Sitzung.

  Dieses Timeout gilt nicht für eine TCP-LSN-Sitzung, wenn eine FIN- oder RST-Nachricht von einem der Endpunkte empfangen wird.

  Standardwert: 120

  Mindestwert: 60

- feinstes Timeout

  Timeout in Sekunden für eine TCP-LSN-Sitzung, nachdem eine FIN- oder RST-Nachricht von einem der Endpunkte empfangen wurde.

  Wenn eine TCP-LSN-Sitzung für eine Zeit, die diesen Wert überschreitet, inaktiv ist (nachdem die NetScaler-Appliance eine FIN- oder RST-Nachricht empfangen hat), entfernt die NetScaler-Appliance die Sitzung.

  Da die LSN-Funktion der NetScaler-Appliance keine Statusinformationen von TCP-LSN-Sitzungen verwaltet, ermöglicht dieser Timeout die Übertragung der FIN- oder RST- und ACK-Nachrichten vom anderen Endpunkt, sodass beide Endpunkte die Verbindung ordnungsgemäß schließen können.

  Standardwert: 30

- Hafenkontingent

  Maximale Anzahl von LSN-NAT-Ports, die von jedem Abonnenten gleichzeitig für das angegebene Protokoll verwendet werden. Beispielsweise kann jeder Abonnent auf maximal 500 TCP-NAT-Ports beschränkt werden. Wenn die LSN-NAT-Zuordnungen für einen Abonnenten das Limit erreichen, weist die NetScaler-Appliance diesem Abonnenten keine zusätzlichen NAT-Ports zu.

  Standardwert: 0

  Mindestwert: 0

  Maximaler Wert: 65535

- Sitzungskontingent

Maximale Anzahl gleichzeitiger LSN-Sitzungen, die für jeden Abonnenten für das angegebene Protokoll zulässig sind. Wenn die Anzahl der LSN-Sitzungen das Limit für einen Abonnenten erreicht, erlaubt die NetScaler-Appliance dem Abonnenten nicht, weitere Sitzungen zu öffnen.

Standardwert: 0

Mindestwert: 0

Maximaler Wert: 65535

- Portpreserve-Parität

  Aktivieren Sie die Portparität zwischen einem Abonnentenport und seinem zugeordneten LSN-NAT-Port. Wenn ein Abonnent beispielsweise eine Verbindung von einem Port mit einer ungeraden Nummer initiiert, weist die NetScaler-Appliance dieser Verbindung einen LSN-NAT-Port mit ungerader Nummer zu. Sie müssen diesen Parameter festlegen, damit Protokolle ordnungsgemäß funktionieren, bei denen der Quellport gerade oder ungerade Zahlen haben muss, z. B. in Peer-to-Peer-Anwendungen, die das RTP- oder RTCP-Protokoll verwenden.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: DISABLED

- Portpreserverrange

  Wenn ein Abonnent eine Verbindung von einem bekannten Port (0-1023) initiiert, weisen Sie dieser Verbindung einen NAT-Port aus dem bekannten Portbereich (0-1023) zu. Wenn ein Abonnent beispielsweise eine Verbindung von Port 80 aus initiiert, kann die NetScaler-Appliance Port 100 als NAT-Port für diese Verbindung zuweisen.

  Dieser Parameter gilt für dynamisches NAT ohne Portblockzuweisung. Dies gilt auch für Deterministic NAT, wenn der Bereich der zugewiesenen Ports bekannte Ports umfasst.

  Wenn alle bekannten Ports aller verfügbaren NAT-IP-Adressen in verschiedenen Abonnentenverbindungen (LSN-Sitzungen) verwendet werden und ein Abonnent eine Verbindung von einem bekannten Port initiiert, unterbricht die NetScaler-Appliance diese Verbindung.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: DISABLED

- Syncheck

  Löschen Sie im Hintergrund alle Nicht-SYN-Pakete für Verbindungen, für die keine LSN-NAT-Sitzung auf der NetScaler-Appliance vorhanden ist.

  Wenn Sie diesen Parameter deaktivieren, akzeptiert die NetScaler-Appliance alle Nicht-SYN-Pakete und erstellt einen neuen LSN-Sitzungseintrag für diese Verbindung.

Im Folgenden sind einige Gründe aufgeführt, aus denen die NetScaler-Appliance solche Pakete empfängt:

* Eine LSN-Sitzung für eine Verbindung existierte, aber die NetScaler-Appliance hat diese Sitzung entfernt, weil die LSN-Sitzung für eine Zeit inaktiv war, die das konfigurierte Sitzungs-Timeout überschritten hat.
* Solche Pakete können Teil eines DoS-Angriffs sein.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- lsn apps-profil hinzufügen
  - appsprofil-Dateiname

    Name für das LSN-Anwendungsprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem das LSN-Anwendungsprofil erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn application profile1" oder 'lsn application profile1').

    Dies ist ein zwingendes Argument. Maximale Länge: 127
  - Transportprotokoll

    Name des Protokolls, für das die Parameter dieses LSN-Anwendungsprofils gelten.

    Dies ist ein zwingendes Argument.

    Mögliche Werte: TCP, UDP, ICMP
  - IPpooling

    Optionen für die NAT-IP-Adresszuweisung für Sitzungen, die demselben Abonnenten zugeordnet sind.

    Die verfügbaren Optionen funktionieren wie folgt:

    * **Gepaart**— Die NetScaler-Appliance weist allen Sitzungen, die demselben Abonnenten zugeordnet sind, dieselbe NAT-IP-Adresse zu. Wenn alle Ports einer NAT-IP-Adresse in LSN-Sitzungen verwendet werden (für denselben oder mehrere Abonnenten), unterbricht die NetScaler-Appliance jede neue Verbindung des Abonnenten.

* **Zufällig**— Die NetScaler-Appliance weist zufällige NAT-IP-Adressen aus dem Pool für verschiedene Sitzungen zu, die demselben Abonnenten zugeordnet sind.

Dieser Parameter gilt nur für die dynamische NAT-Zuweisung.

Mögliche Werte: PAIRD, RANDOM

Standardwert: RANDOM

– kartierend

Art der LSN-Zuordnung, die auf nachfolgende Pakete angewendet werden soll, die von derselben Abonnenten-IP-Adresse und demselben Port stammen.

Stellen Sie sich ein Beispiel für ein LSN-Mapping vor, das die Zuordnung der Abonnenten-IP:Port (x:X), NAT-IP:Port (n:N) und der externen Host-IP:Port (y:Y) umfasst.

Die verfügbaren Optionen funktionieren wie folgt:

* **ENDPUNKTUNABHÄNGIG**— Verwenden Sie die LSN-Zuordnung für nachfolgende Pakete, die von derselben Abonnenten-IP-Adresse und demselben Port (x:X) an eine beliebige externe IP-Adresse und einen Port gesendet werden.
* **ADRESSABHÄNGIG**— Verwenden Sie die LSN-Zuordnung für nachfolgende Pakete, die von derselben Abonnenten-IP-Adresse und demselben Port (x:X) an dieselbe externe IP-Adresse (Y) gesendet werden, unabhängig vom externen Port.
* **ADDRESS-PORT-DEPENDENT**— Verwenden Sie die LSN-Zuordnung für nachfolgende Pakete, die von derselben internen IP-Adresse und demselben Port (x:X) an dieselbe externe IP-Adresse und denselben Port (y:Y) gesendet werden, solange die Zuordnung noch aktiv ist.

Mögliche Werte: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

Standardwert: ADDRESS-PORT-DEPENDENT

– filtern

Art des Filters, der auf Pakete angewendet werden soll, die von externen Hosts stammen.

Stellen Sie sich ein Beispiel für eine LSN-Zuordnung vor, die die Zuordnung von Abonnenten-IP:Port (x:X), NAT-IP:Port (n:N) und externem Host-IP:Port (y:Y) umfasst.

Die verfügbaren Optionen funktionieren wie folgt:

* **ENDPOINT INDEPENDENT**— Filtert nur Pakete heraus, die nicht für die Abonnenten-IP-Adresse und den Port x:X bestimmt sind, unabhängig von der externen Host-IP-Adresse und der Portquelle (z:Z). Die NetScaler-Appliance leitet alle Pakete weiter, die für x:x bestimmt sind. Mit anderen Worten, das Senden von Paketen vom Abonnenten an eine beliebige externe IP-Adresse reicht aus, um Pakete von beliebigen externen Hosts an den Abonnenten zuzulassen.

* **ADRESSABHÄNGIG**— Filtert Pakete heraus, die nicht für die IP-Adresse und den Port x:X des Abonnenten bestimmt sind. Darüber hinaus filtert die Appliance Pakete aus Y:y heraus, die für den Abonnenten bestimmt sind (x:x), wenn der Client zuvor keine Pakete an y:AnyPort gesendet hat (unabhängig vom externen Port). Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an die IP-Adresse dieses bestimmten externen Hosts sendet.
* **ADDRESS PORT DEPENDENT** (Standard) — Filtert Pakete heraus, die nicht für die IP-Adresse und den Port des Abonnenten bestimmt sind (x:X). Darüber hinaus filtert die NetScaler-Appliance Pakete aus Y:y heraus, die für den Abonnenten (x:x) bestimmt sind, wenn der Abonnent zuvor keine Pakete an Y:y gesendet hat. Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an diese externe IP-Adresse und diesen Port sendet.

Mögliche Werte: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

Standardwert: ADDRESS-PORT-DEPENDENT

- tcp-Proxy

  Aktivieren Sie den TCP-Proxy, der es der NetScaler-Appliance ermöglicht, den TCP-Verkehr mithilfe von Layer-4-Funktionen zu optimieren.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: DISABLED

- td

  ID der Verkehrsdomäne, über die die NetScaler-Appliance den ausgehenden Datenverkehr sendet, nachdem sie LSN ausgeführt hat.

  Wenn Sie keine ID angeben, sendet die Appliance den ausgehenden Datenverkehr über die Standardverkehrsdomäne, die eine ID von 0 hat.

  Standardwert: 65535

  Maximaler Wert: 65535

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- Binden Sie das LSN Apps-Profil
  - appsprofil-Dateiname

    Name für das LSN-Anwendungsprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche,

Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem das LSN-Anwendungsprofil erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn application profile1" oder 'lsn application profile1').

Dies ist ein zwingendes Argument. Maximale Länge: 127

- Lsnport

  Portnummern oder Bereich von Portnummern, die mit dem Zielport des von einem Abonnenten eingehenden Pakets abgeglichen werden sollen. Wenn der Zielport übereinstimmt, wird das LSN-Anwendungsprofil für die LSN-Sitzung angewendet. Trennen Sie eine Reihe von Ports durch einen Bindestrich. Zum Beispiel 40-90.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- LSN-Gruppe hinzufügen
  - Gruppenname

    Name für die LSN-Gruppe. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn group1" oder 'lsn group1').

    Dies ist ein zwingendes Argument. Maximale Länge: 127

  - clientname

    Name der LSN-Client-Entität, die der LSN-Gruppe zugeordnet werden soll. Sie können einer LSN-Gruppe nur eine LSN-Client-Entität zuordnen. Sie können diese Zuordnung nicht entfernen oder durch eine andere LSN-Client-Entität ersetzen, sobald die LSN-Gruppe erstellt wurde.

    Dies ist ein zwingendes Argument. Maximale Länge: 127

  - Nat-Typ

    Art der NAT-IP-Adresse und Portzuweisung (aus den gebundenen LSN-Pools) für Abonnenten:

    Die verfügbaren Optionen funktionieren wie folgt:

* **Deterministisch**— Weisen Sie jedem Abonnenten (des an die LSN-Gruppe gebundenen LSN-Clients) eine NAT-IP-Adresse und einen Block von Ports zu. Die NetScaler-Appliance weist diesen Abonnenten sequentiell NAT-Ressourcen zu. Die NetScaler-Appliance weist der ersten Abonnenten-IP-Adresse den ersten Portblock (die Blockgröße wird durch den Portblockgrößenparameter der LSN-Gruppe bestimmt) auf der ersten NAT-IP-Adresse zu. Der nächste Portbereich wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht mehr über genügend Ports für den nächsten Abonnenten verfügt. In diesem Fall wird der erste Portblock an der nächsten NAT-Adresse für den Abonnenten verwendet usw. Da jeder Abonnent jetzt eine deterministische NAT-IP-Adresse und einen Block von Ports erhält, kann ein Abonnent identifiziert werden, ohne dass eine Protokollierung erforderlich ist. Bei einer Verbindung kann ein Abonnent nur anhand der NAT-IP-Adresse und des Port sowie der Ziel-IP-Adresse und des Port identifiziert werden.
* **Dynamisch**— Weisen Sie der Verbindung eines Abonnenten eine zufällige NAT-IP-Adresse und einen Port aus dem LSN-NAT-Pool zu. Wenn die Portblockzuweisung aktiviert ist (im LSN-Pool) und eine Portblockgröße angegeben ist (in der LSN-Gruppe), weist die NetScaler-Appliance einem Abonnenten eine zufällige NAT-IP-Adresse und einen Portblock zu, wenn sie zum ersten Mal eine Verbindung initiiert. Die Appliance weist diese NAT-IP-Adresse und einen Port (aus dem zugewiesenen Portblock) für verschiedene Verbindungen dieses Abonnenten zu. Wenn alle Ports (für verschiedene Abonnentenverbindungen) aus dem dem Abonnenten zugewiesenen Portblock zugewiesen sind, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu.

Mögliche Werte: DYNAMIC, DETERMINISTIC

Standardwert: DYNAMIC

– Portblockgröße

Größe des NAT-Portblocks, der jedem Abonnenten zugewiesen werden soll.

Um diesen Parameter für Dynamic NAT festzulegen, müssen Sie den Parameter für die Portblockzuweisung im gebundenen LSN-Pool aktivieren. Für deterministisches NAT ist der Parameter für die Portblockzuweisung immer aktiviert und kann nicht deaktiviert werden.

In Dynamic NAT weist die NetScaler-Appliance jedem Abonnenten einen zufälligen NAT-Portblock aus dem verfügbaren NAT-Portpool einer NAT-IP-Adresse zu. Wenn für einen Abonnenten alle Ports aus dem dem Abonnenten zugewiesenen Portblock zugewiesen sind, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu.

– Protokollierung

Protokollzuordnungseinträge und Sitzungen, die für diese LSN-Gruppe erstellt oder gelöscht wurden. Die NetScaler-Appliance protokolliert LSN-Sitzungen für diese

LSN-Gruppe nur, wenn sowohl die Protokollierungs- als auch die Sitzungsprotokollierungsparameter aktiviert sind.

Die Appliance verwendet ihr vorhandenes Syslog- und Audit-Log-Framework, um LSN-Informationen zu protokollieren. Sie müssen die LSN-Protokollierung auf globaler Ebene aktivieren, indem Sie den LSN-Parameter in den zugehörigen Entitäten der NSLOG-Aktion und der SYLOG-Aktion aktivieren. Wenn der Logging-Parameter aktiviert ist, generiert die NetScaler-Appliance Protokollmeldungen, die sich auf LSN-Zuordnungen und LSN-Sitzungen dieser LSN-Gruppe beziehen. Die Appliance sendet diese Protokollmeldungen dann an Server, die den Entitäten NSLOG-Aktion und SYSLOG-Aktionen zugeordnet sind.

Eine Protokollnachricht für einen LSN-Zuordnungseintrag besteht aus den folgenden Informationen:

* NSIP-Adresse der NetScaler-Appliance
* Zeitstempel
* Art des Eintrags (MAPPING oder SESSION)
* Ob der LSN-Mapping-Eintrag erstellt oder gelöscht wurde
* IP-Adresse, Port und Domain-ID des Abonnenten
* NAT-IP-Adresse und Port
* Name des Protokolls
* Abhängig von den folgenden Bedingungen können Ziel-IP-Adresse, Port und Verkehrsdomänen-ID vorhanden sein:
  - Ziel-IP-Adresse und Port werden für die endpunktunabhängige Zuordnung nicht protokolliert
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse (und nicht der Port) protokolliert
  - Ziel-IP-Adresse und Port werden für die adressportabhängige Zuordnung protokolliert

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

– Sitzungsprotokollierung

Protokollsitzungen, die für die LSN-Gruppe erstellt oder gelöscht wurden. Die NetScaler-Appliance protokolliert LSN-Sitzungen für diese LSN-Gruppe nur, wenn sowohl die Protokollierungs- als auch die Sitzungsprotokollierungsparameter aktiviert sind.

Eine Protokollnachricht für eine LSN-Sitzung besteht aus den folgenden Informationen:

* NSIP-Adresse der NetScaler-Appliance
* Zeitstempel
* Art des Eintrags (MAPPING oder SESSION)

* Ob die LSN-Sitzung erstellt oder entfernt wurde
* IP-Adresse, Port und Domain-ID des Abonnenten
* NAT-IP-Adresse und Port
* Name des Protokolls
* Ziel-IP-Adresse, Port und Traffic-Domain-ID

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

- Sitzungssynchronisierung

  Synchronisieren Sie in einer Bereitstellung mit hoher Verfügbarkeit (HA) die Informationen aller LSN-Sitzungen, die sich auf diese LSN-Gruppe beziehen, mit dem sekundären Knoten. Nach einem Failover werden hergestellte TCP-Verbindungen und UDP-Paketflüsse aktiv gehalten und auf dem sekundären Knoten (neuer primärer Knoten) wieder aufgenommen.

  Damit diese Einstellung funktioniert, müssen Sie den globalen Sitzungssynchronisationsparameter aktivieren.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: ENABLED

- snmp-Trap-Limit

  Maximale Anzahl von SNMP-Trap-Meldungen, die in einer Minute für die LSN-Gruppe generiert werden können.

  Standardwert: 100

  Mindestwert: 0

  Maximalwert: 10000

- ftp

  Aktivieren Sie Application Layer Gateway (ALG) für das FTP-Protokoll. Bei einigen Protokollen auf Anwendungsebene werden die IP-Adressen und Protokollportnummern normalerweise in der Payload der Pakete übermittelt. Wenn die Appliance als ALG fungiert, ändert sie die Payload der Pakete, um sicherzustellen, dass das Protokoll weiterhin über LSN funktioniert.

  Hinweis: Die NetScaler-Appliance enthält auch ALG für ICMP- und TFTP-Protokolle. ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es ist nicht vorgesehen, es zu deaktivieren. ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. ALG wird automatisch für eine LSN-Gruppe aktiviert, wenn Sie ein UDP-LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- Lsn-Gruppe binden
  - Gruppenname

    Name für die LSN-Gruppe. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn group1" oder 'lsn group1').

    Dies ist ein zwingendes Argument. Maximale Länge: 127
  - Poolname

    Name des LSN-Pools, der an die angegebene LSN-Gruppe gebunden werden soll. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden.

    Für deterministisches NAT können Pools, die an eine LSN-Gruppe gebunden sind, nicht an andere LSN-Gruppen gebunden werden. Für dynamisches NAT können Pools, die an eine LSN-Gruppe gebunden sind, an mehrere LSN-Gruppen gebunden werden. Maximale Länge: 127
  - Name des Transportprofils

    Name des LSN-Transportprofils, das an die angegebene LSN-Gruppe gebunden werden soll. Binden Sie ein Profil für jedes Protokoll, für das Sie Einstellungen angeben möchten.

    Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für die Protokolle TCP, UDP und ICMP bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardtransport bezeichnet.

    Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das Standard-LSN-Transportprofil für dieses Protokoll. Maximale Länge: 127
  - appsprofil-Dateiname

    Name des LSN-Anwendungsprofils, das an die angegebene LSN-Gruppe gebunden werden soll. Binden Sie für jeden Satz von Zielports ein Profil für jedes Protokoll, für das Sie Einstellungen angeben möchten.

Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für die TCP-, UDP- und ICMP-Protokolle für alle Zielports bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardanwendungsprofil bezeichnet.

Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Maximale Länge: 127

Beispiel-LSN-Konfigurationen

January 19, 2021

Im Folgenden finden Sie Beispiele für die Konfiguration von LSN über die Befehlszeilenschnittstelle.

Erstellen Sie eine einfache LSN-Konfiguration mit einem einzelnen Teilnehmernetzwerk, einer einzelnen LSN-NAT-IP-Adresse und Standardeinstellungen:

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done
<!--NeedCopy-->
```


Erstellen Sie eine LSN-Konfiguration mit einer erweiterten ACL zur Identifizierung von LSN-Abonnenten:

```
add ns acl LSN-ACL-2 ALLOW -srcIP 192.0.2.10-192.0.2.20

Done

apply acls

Done

add lsn client LSN-CLIENT-2

Done

bind lsn client LSN-CLIENT-2  -aclname LSN-ACL-2

Done

add lsn pool LSN-POOL-2

Done

bind lsn pool LSN-POOL-2 203.0.113.5-203.0.113.10

Done

add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2

Done

bind lsn group LSN-GROUP-2 -poolname LSN-POOL-2

Done
<!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration mit endpunktunabhängiger Zuordnung für HTTP-Protokoll (Port 80) und adressenport-abhängige Zuordnung für das SSH-Protokoll (Port 22). Beschränken Sie außerdem jeden Abonnenten auf maximal 1000 NAT-Ports für das TCP-Protokoll und 100 NAT-Ports für das UDP-Protokoll. Beschränken Sie jeden Abonnenten auf maximal 2000 gleichzeitige Sitzungen für das TCP-Protokoll. Beschränken Sie die Gruppe auf maximal 30000 gleichzeitige Sitzungen für das TCP-Protokoll:

```
add lsn client LSN-CLIENT-3
```



```
2
3  Done
4
5  bind lsn client LSN-CLIENT-3 -network 192.0.3.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-3
10
11 Done
12
13 bind lsn pool LSN-POOL-3 203.0.113.11
14
15 Done
16
17 add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-3
18
19 Done
20
21 bind lsn group LSN-GROUP-3 -poolname LSN-POOL-3
22
23 Done
24
25 add lsn appsprofile LSN-APPS-HTTPPROFILE-3 TCP -mapping ENDPOINT-
      INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile LSN-APPS-HTTPPROFILE-3 80
30
31 Done
32
33 bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-HTTPPROFILE
      -3
34
35 Done
36
37 add lsn appsprofile LSN-APPS-SSHPROFILE-3 TCP -mapping ADDRESS-PORT-
      DEPENDENT
38
39 Done
40
41 bind lsn appsprofile LSN-APPS-SSHPROFILE-3 22
42
43 Done
```



```
44
45 bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-SSHPROFILE
       -3
46
47 Done
48
49 add lsn transportprofile LSN-TRANS-PROFILE-TCP-3 TCP -portquota 1000 -
       sessionquota 2000 -groupSessionLimit 30000
50
51 Done
52
53 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-TCP
       -3
54
55 Done
56
57 add lsn transportprofile LSN-TRANS-PROFILE-UDP-3 UDP -portquota 100
58
59 Done
60
61 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-UDP
       -3
62
63 Done
64 <!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration für einen großen Satz von Abonnenten:

```
1  add lsn client LSN-CLIENT-4
2
3  Done
4
5  bind lsn client LSN-CLIENT-4 -network 192.0.4.0 -netmask 255.255.255.0
6
7  Done
8
9  bind lsn client LSN-CLIENT-4 -network 192.0.5.0 -netmask 255.255.255.0
10
11 Done
12
13 bind lsn client LSN-CLIENT-4 -network 192.0.6.0 -netmask 255.255.255.0
14
15 Done
16
17 bind lsn client LSN-CLIENT-4 -network 192.0.7.0 -netmask 255.255.255.0
```



```
18
19 Done
20
21 bind lsn client LSN-CLIENT-4 -network 192.0.8.0 -netmask 255.255.255.0
22
23 Done
24
25 add lsn pool LSN-POOL-4
26
27 Done
28
29 bind lsn pool LSN-POOL-4 203.0.113.30-203.0.113.40
30
31 Done
32
33 bind lsn pool LSN-POOL-4 203.0.113.45-203.0.113.50
34
35 Done
36
37 bind lsn pool LSN-POOL-4 203.0.113.55-203.0.113.60
38
39 Done
40
41 add lsn group LSN-GROUP-4 -clientname LSN-CLIENT-4
42
43 Done
44
45 bind lsn group LSN-GROUP-4 -poolname LSN-POOL-4
46
47 Done
48
49 add lsn appsprofile LSN-APPS-WELLKNOWNPROFILE-4 TCP -mapping ENDPOINT-
      INDEPENDENT
50
51 Done
52
53 bind lsn appsprofile LSN-APPS-WELLKNOWN-PORTS-PROFILE-4 1- 1023
54
55 Done
56
57 bind lsn group LSN-GROUP-4 -applicationprofilename LSN-APPS-WELLKNOWN-
      PORTS-PROFILE-4
58
59 Done
60 <!--NeedCopy-->
```


Erstellen Sie eine LSN-Konfiguration mit Freigabe von NAT-Ressourcen für mehrere LSN-Gruppen. In diesem Beispiel wird LSN-Pool LSN-POOL-5 für die LSN-Gruppen LSN-GROUP-5 und LSN-GROUP-6 freigegeben:

```
add lsn client LSN-CLIENT-5

Done

bind lsn client LSN-CLIENT-5 -network 192.0.15.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-5

Done

bind lsn pool LSN-POOL-5 203.0.113.12-203.0.113.14

Done

add lsn group LSN-GROUP-5 -clientname LSN-CLIENT-5

Done

bind lsn group LSN-GROUP-5 -poolname LSN-POOL-5

Done

add lsn client LSN-CLIENT-6

Done

bind lsn client LSN-CLIENT-6 -network 192.0.16.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-6

Done

bind lsn pool LSN-POOL-6 203.0.113.15-203.0.113.18

Done
```



```
40
41 add lsn group LSN-GROUP-6 -clientname LSN-CLIENT-6
42
43 Done
44
45 bind lsn group LSN-GROUP-6 -poolname LSN-POOL-6
46
47 Done
48
49 bind lsn group LSN-GROUP-6 -poolname LSN-POOL-5
50
51 Done
52 <!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration mit deterministischer NAT-Ressourcenzuweisung:

```
1  add lsn client LSN-CLIENT-7
2
3  Done
4
5  bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-7 -nattype DETERMINISTIC
10
11 Done
12
13 bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23
14
15 Done
16
17 add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
      DETERMINISTIC -portblocksize 1024
18
19 Done
20
21 bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
22
23 Done
24 <!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration mit mehreren Teilnehmernetzen, die dieselbe Netzwerkadresse haben, aber jedes Netzwerk, das zu einer anderen Verkehrsdomäne gehört. Beschränken Sie außerdem den ausgehenden Datenverkehr im Zusammenhang mit dem

HTTP-Protokoll (Port 80) und senden Sie ihn über eine bestimmte Datenverkehrsdomäne (td 5):

```
add lsn client LSN-CLIENT-8

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 1

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 2

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 3

Done

add lsn pool LSN-POOL-8

Done

bind lsn pool LSN-POOL-8 203.0.113.80-203.0.113.86

Done

add lsn group LSN-GROUP-8 -clientname LSN-CLIENT-8

Done

bind lsn group LSN-GROUP-8 -poolname LSN-POOL-8

Done

add lsn appsprofile LSN-APPS-HTTP-PROFILE-8 TCP -td 5

Done

bind lsn appsprofile LSN-APPS-HTTP-PROFILE-8 80

Done
```



```
40
41 bind lsn group LSN-GROUP-8 -applicationprofilename LSN-APPS-HTTP-
      PROFILE-8
42
43 Done
44 <!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration, die den ausgehenden Datenverkehr eines bestimmten Protokolls (TCP) einschränkt und über eine bestimmte Datenverkehrsdomäne (td 5) sendet. Mit der endpunktunabhängigen Filterung empfangen Sie eingehenden Datenverkehr im Zusammenhang mit diesem Protokoll (TCP) in einer beliebigen Datenverkehrsdomäne:

```
1  add lsn client LSN-CLIENT-9
2
3  Done
4
5  bind lsn client LSN-CLIENT-9 -network 192.0.9.0 -netmask 255.255.255.0
      -td 1
6
7  Done
8
9  add lsn pool LSN-POOL-9
10
11 Done
12
13 bind lsn pool LSN-POOL-9 203.0.113.90
14
15 Done
16
17 add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
18
19 Done
20
21 bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
22
23 Done
24
25 add lsn appsprofile LSN-APPS-PROFILE-9 TCP -filtering ENDPOINT-
      INDEPENDENT -td 5
26
27 Done
28
29 bind lsn group LSN-GROUP-9 -approfile LSN-APPS-PROFILE-9
30
```



```
Done
<!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration, die den ausgehenden HTTP-Datenverkehr (Port 80) einschränkt und über eine bestimmte Datenverkehrsdomäne (td 10) sendet. Bei adressabhängiger Filterung empfangen Sie eingehenden Datenverkehr im Zusammenhang mit diesem Protokoll (HTTP) in der angegebenen Datenverkehrsdomäne (td 10):

```
add lsn client LSN-CLIENT-10

Done

bind lsn client LSN-CLIENT-10 -network 192.0.10.0 -netmask
   255.255.255.0 -td 1

Done

add lsn pool LSN-POOL-10

Done

bind lsn pool LSN-POOL-10 203.0.113.100

Done

add lsn group LSN-GROUP-10 -clientname LSN-CLIENT-10

Done

bind lsn group LSN-GROUP-10 -poolname LSN-POOL-10

Done

add lsn appsprofile LSN-APPS-PROFILE-10 TCP -mapping ENDPOINT -
   INDEPENDENT -filtering ADDRESS-DEPENDENT -td 10

Done

bind lsn appsprofile LSN-APPS-PROFILE-10 80

Done

bind lsn group LSN-GROUP-10 -approfile LSN-APPS-PROFILE-10

```



```
Done
<!--NeedCopy-->
```

Konfigurieren von statischen LSN-Maps

May 11, 2023

Die NetScaler-Appliance unterstützt die manuelle Erstellung einer Eins-zu-Eins-LSN-Zuordnung zwischen einer Abonnenten-IP-Adresse:Port und einer NAT-IP-Adresse:Port. Statische LSN-Zuordnungen sind nützlich, wenn Sie sicherstellen möchten, dass die zu einem NAT-IP:Port initiierten Verbindungen der Abonnenten-IP-Adresse: Port zugeordnet werden. Zum Beispiel Webserver, die sich im internen Netzwerk befinden.

So erstellen Sie ein statisches LSN-Mapping mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [<natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd
     <positive_integer>]]
-  show lsn static
<!--NeedCopy-->
```

So erstellen Sie ein statisches LSN-Mapping mithilfe des Konfigurationsprogramms

Navigieren Sie zu System > Large Scale NAT > Static und fügen Sie ein neues statisches Mapping hinzu.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

statischen LSN-Namen hinzufügen

Name für den statischen LSN-Mapping-Eintrag. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „lsn static1" oder 'lsn static1'). Dies ist ein zwingendes Argument. Maximale Länge: 127

Transportprotokoll

Protokoll für den LSN-Mapping-Eintrag. Dies ist ein zwingendes Argument. Mögliche Werte: TCP, UDP, ICMP

Abonniere

IPv4-Adresse eines LSN-Abonnenten für den LSN-Mapping-Eintrag. Dies ist ein zwingendes Argument.

Abonnieren

Port des LSN-Abonnenten für den LSN-Mapping-Eintrag. Dies ist ein zwingendes Argument. Maximaler Wert: 65535

td

ID der Verkehrsdomäne, zu der der Abonnent gehört. Wenn Sie keine ID angeben, wird davon ausgegangen, dass der Abonnent Teil der Standard-Verkehrsdomäne ist. Standardwert: 0, Mindestwert: 0, Maximalwert: 4094

Antip

IPv4-Adresse, die bereits auf der NetScaler-Appliance als Typ LSN vorhanden ist und als NAT-IP-Adresse für diesen Zuordnungseintrag verwendet werden soll.

NAT-Anschluss

NAT-Port für diesen LSN-Mapping-Eintrag.

DE Tip

Ziel-IP-Adresse für den LSN-Zuordnungseintrag.

dsttd

ID der Verkehrsdomäne, über die die Ziel-IP-Adresse für diesen LSN-Mapping-Eintrag von der NetScaler-Appliance aus erreichbar ist. Wenn Sie keine ID angeben, wird davon ausgegangen, dass die Ziel-IP-Adresse über die Standard-Verkehrsdomäne erreichbar ist, die eine ID von 0 hat. Standardwert: 0, Mindestwert: 0, Maximalwert: 4094

Statische Wildcard-Portkarten

Ein statischer Zuordnungseintrag ist normalerweise eine Eins-zu-Eins-LSN-Zuordnung zwischen einer Abonnenten-IP-Adresse:Port und einer NAT-IP-Adresse:Port. Ein statischer LSN-Mapping-Eintrag im Eins-zu-Eins-Format macht nur einen Port des Abonnenten für das Internet verfügbar.

In einigen Situationen müssen möglicherweise alle Ports (64 KB) eines Abonnenten dem Internet zugänglich gemacht werden (z. B. ein Server, der in einem internen Netzwerk gehostet wird und an jedem Port ein anderer Dienst ausgeführt wird). Um diese internen Dienste über das Internet zugänglich zu machen, müssen Sie alle Ports des Servers dem Internet zugänglich machen.

Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, 64.000 statische Eins-zu-Eins-Zuordnungseinträge hinzuzufügen, einen Zuordnungseintrag für jeden Port. Das Erstellen von 64.000 Einträgen ist sehr umständlich und eine große Aufgabe. Außerdem kann diese große Anzahl von Konfigurationseinträgen zu Leistungsproblemen in der NetScaler-Appliance führen.

Eine weitere einfache Methode besteht darin, Platzhalterports in einem statischen Zuordnungseintrag zu verwenden. Sie müssen nur einen statischen Mapping-Eintrag erstellen, bei dem die Parameter NAT-Port und Subscriber-Port auf das Platzhalterzeichen (*) gesetzt sind und der Protokollparameter auf ALL gesetzt ist, um alle Ports eines Abonnenten für das Internet verfügbar zu machen. Bei eingehenden oder ausgehenden Verbindungen eines Abonnenten, die einem statischen Platzhalterzuordnungseintrag entsprechen, ändert sich der Port des Abonnenten nach dem NAT-Vorgang nicht.

Wenn eine vom Abonnenten initiierte Verbindung zum Internet mit einem statischen Platzhaltereintrag übereinstimmt, weist die NetScaler-Appliance einen NAT-Port zu, der dieselbe Nummer wie der Abonnentenport hat, von dem aus die Verbindung initiiert wird. In ähnlicher Weise wird ein Internet-Host mit dem Port eines Abonnenten verbunden, indem er sich mit dem NAT-Port verbindet, der dieselbe Nummer wie der Port des Abonnenten hat.

Konfiguration der NetScaler-Appliance für den Zugriff auf alle Ports eines IPv4-Abonnenten

Um die NetScaler-Appliance so zu konfigurieren, dass sie Zugriff auf alle Ports eines IPv4-Abonnenten gewährt, erstellen Sie eine statische Wildcard-Map mit den folgenden obligatorischen Parametereinstellungen:

- protocol=Alle
- Abonnenten-Port = *
- NAT-Anschluss = *

In einer statischen Wildcard-Map ist im Gegensatz zu einer statischen Eins-zu-Eins-Map das Festlegen des NAT-IP-Parameters obligatorisch. Außerdem kann die einer statischen Wildcard-Map zugewiesene NAT-IP-Adresse nicht für andere Abonnenten verwendet werden.

So erstellen Sie mithilfe der Befehlszeilenschnittstelle eine statische Wildcard-Map

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
    positive_integer>] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Beispielkonfiguration

In der folgenden Beispielkonfiguration einer statischen Wildcard-Map werden alle Ports eines Abonnenten, dessen IP-Adresse 192.0.2.10 lautet, über die NAT-IP 203.0.11.33 zugänglich gemacht.

Beispielkonfiguration:

```
add lsn static NAT44-WILDCARD-STATIC-1 ALL  192.0.2.10 * 203.0.113.33 *

Done
<!--NeedCopy-->
```

Konfigurieren von Application Layer-Gateways

May 11, 2023

Bei einigen Protokollen auf Anwendungsebene werden die IP-Adressen und Protokollportnummern auch in der Payload des Pakets übermittelt. Das Application Layer Gateway für ein Protokoll analysiert die Nutzdaten des Pakets und nimmt die erforderlichen Änderungen vor, um sicherzustellen, dass das Protokoll weiterhin über LSN funktioniert.

Die NetScaler-Appliance unterstützt ALG für die folgenden Protokolle:

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Application Layer Gateway für FTP-, ICMP- und TFTP-Protokolle

May 11, 2023

Sie können ALG für das FTP-Protokoll für eine LSN-Konfiguration aktivieren oder deaktivieren, indem Sie die FTP-Option der LSN-Gruppe der LSN-Konfiguration aktivieren oder deaktivieren.

ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es ist nicht vorgesehen, es zu deaktivieren.

ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. TFTP-ALG wird automatisch für eine LSN-Konfiguration aktiviert, wenn Sie ein UDP-LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

LSN-Beispielkonfiguration für FTP-ALG:
In der folgenden LSN-Beispielkonfiguration ist FTP-ALG für Abonnenten aktiviert, deren IP-Adresse im Bereich 192.0.2.30-192.0.2.100 liegt.

```
add ns acl LSN-ACL-1 ALLOW -srcIP 192.0.2.30-192.0.2.100

Done

apply acls

Done

add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1  -aclname LSN-ACL

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.10

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -FTP ENABLED

Done
```



```
28
29 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
30
31 Done
32 <!--NeedCopy-->
```

Beispiel für eine LSN-Konfiguration für TFTP ALG:

In der folgenden LSN-Beispielkonfiguration sind die endpunktunabhängige Zuordnung und die endpunktunabhängige Filterung für das TFTP-Protokoll (UDP-Port 69) aktiviert. Die NetScaler Appliance aktiviert automatisch TFTP ALG für diese LSN-Konfiguration.

```
1  add lsn client LSN-CLIENT-2
2
3  Done
4
5  bind lsn client LSN-CLIENT-2 -network 198.51.100.0 -netmask
       255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-2
10
11 Done
12
13 bind lsn pool LSN-POOL-2 203.0.113.10-203.0.113.11
14
15 Done
16
17 add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2
18
19 Done
20
21 bind lsn group LSN-GROUP-2 -poolname pool1 LSN-POOL-2
22
23 Done
24
25 add lsn appsprofile LSNAPPSPROFILE-TFTP-2 UDP -mapping ENDPOINT-
       INDEPENDENT  - filtering  ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile LSNAPPSPROFILE-TFTP-2 69
30
31 Done
```



```
32
33 bind lsn group LSN-GROUP-1 -applicationprofilename LSNAPPSPROFILE-TFTP
       -2
34
35 Done
36 <!--NeedCopy-->
```

Application Layer Gateway für das PPTP-Protokoll

May 11, 2023

Die NetScaler-Appliance unterstützt Application Layer Gateways (ALGs) für das Point-to-Point Tunneling Protocol (PPTP).

PPTP ist ein Netzwerkprotokoll, das die sichere Übertragung von Daten von einem Remote-Client zu einem Unternehmensserver ermöglicht, indem ein Tunnel über TCP/IP-basierte Datennetzwerke erstellt wird. PPTP kapselt PPP-Pakete in IP-Pakete für die Übertragung über das Internet ein. PPTP richtet einen Tunnel für jedes kommunizierende PPTP-Netzwerkserver (PNS) -PPTP Access Concentrator (PAC) -PPTP Access Concentrator (PAC) -Paar ein. Nachdem der Tunnel eingerichtet ist, wird Enhanced Generic Routing Encapsulation (GRE) verwendet, um PPP-Pakete auszutauschen. Eine Anruf-ID im GRE-Header gibt die Sitzung an, zu der ein bestimmtes PPP-Paket gehört.

Die NetScaler-Appliance erkennt PPTP-Pakete, die am Standard-TCP-Port 1723 ankommen. Die Appliance analysiert PPTP-Steuerpakete, übersetzt die Anruf-ID und weist eine NAT-IP-Adresse zu. Für die bidirektionale Datenkommunikation zwischen Client und Server erstellt die NetScaler-Appliance einen LSN-Sitzungseintrag auf der Grundlage der Serveraufruf-ID und eine LSN-Sitzung auf der Grundlage der Client-Anruf-ID. Die Appliance analysiert dann die GRE-Datenpakete und übersetzt Anruf-IDs auf der Grundlage der beiden LSN-Sitzungseinträge.

Für das PPTP-Protokoll enthält die NetScaler-Appliance auch eine Timeout-Einstellung für alle inaktiven PPTP-LSN-Sitzungen. Wenn eine PPTP-LSN-Sitzung für eine Zeit inaktiv ist, die die Timeout-Einstellung überschreitet, entfernt die NetScaler-Appliance die Sitzung.

Einschränkungen:

Im Folgenden sind die Einschränkungen von PPTP ALG auf einer NetScaler-Appliance aufgeführt:

- PPTP ALG wird für Hairpin LSN Flow nicht unterstützt.
- PPTP ALG wird nicht unterstützt, um mit einer RNAT-Konfiguration zu arbeiten.
- PPTP ALG wird in NetScaler-Clustern nicht unterstützt.

PPTP ALG konfigurieren

Die Konfiguration von PPTP ALG auf der NetScaler-Appliance umfasst die folgenden Aufgaben:

- Erstellen Sie eine LSN-Konfiguration und aktivieren Sie PPTP ALG darauf. In einer LSN-Konfiguration enthält die LSN-Gruppe die PPTP-ALG-Einstellung. Anweisungen zum Erstellen einer LSN-Konfiguration finden Sie unter Konfigurationsschritte für LSN.
- (Optional) Legen Sie das globale Timeout für unzulässige PPTP-LSN-Sitzungen fest.

So aktivieren Sie PPTP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-pptp ( ENABLED |
   DISABLED )]

show lsn group
<!--NeedCopy-->
```

So legen Sie das globale Timeout für inaktive PPTP-LSN-Sitzungen mithilfe der CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set appAlgParam -pptpGreIdleTimeout <positive_integer>

show appAlgParam
<!--NeedCopy-->
```

Beispiel:

In der folgenden LSN-Beispielkonfiguration ist PPTP ALG für Abonnenten im 192.0.2.0/24-Netzwerk aktiviert.

Außerdem ist das Timeout für PPTP-LSN-Sitzungen im Leerlauf auf 200 Sekunden festgelegt.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

```



```
Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -pptp ENABLED

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done

set appAlgParam -pptpGreIdleTimeout 200

Done
<!--NeedCopy-->
```

Application Layer Gateway für SIP-Protokoll

May 11, 2023

Die Verwendung von Large Scale NAT (LSN) mit Session Initiation Protocol (SIP) ist kompliziert, da SIP-Nachrichten IP-Adressen sowohl in den SIP-Headern als auch im SIP-Body enthalten. Wenn LSN mit SIP verwendet wird, enthalten die SIP-Header Informationen über den Anrufer und den Empfänger, und das Gerät übersetzt diese Informationen, um sie vor dem externen Netzwerk zu verbergen. Der SIP-Text enthält die SDP-Informationen (Session Description Protocol), zu denen IP-Adressen und Portnummern für die Übertragung der Medien gehören.

SIP ALG hält sich an die folgenden RFCs:

- RFC 3261
- RFC 3581
- RFC 456
- RFC 475

> **Hinweis**
>
> SIP ALG wird in einer eigenständigen NetScaler-Appliance, in einem NetScaler-Hochverfügbarkeits-Setup sowie in einem NetScaler-Cluster-Setup unterstützt.

So funktioniert SIP ALG

Wie die IP-Adressübersetzung durchgeführt wird, hängt vom Typ und der Richtung der Nachricht ab. Eine Nachricht kann eine der folgenden sein:

- Eingehende Anfrage
- Ausgehende Antwort
- Ausgehende Anfrage
- Eingehende Antwort

Bei einer ausgehenden Nachricht werden die private IP-Adresse und die Portnummer des SIP-Clients durch die NetScaler-eigene öffentliche IP-Adresse und Portnummer ersetzt, die als *LSN-Pool-IP-Adresse und Portnummer bezeichnet werden und*während der LSN-Konfiguration angegeben wurden. Bei einer eingehenden Nachricht werden die LSN-Pool-IP-Adresse und die Portnummer durch die private Adresse des Clients ersetzt. Wenn die Nachricht öffentliche IP-Adressen enthält, behält das NetScaler SIP ALG diese. Außerdem entsteht eine Lochblende auf der:

- LSN pool-IP-Adresse und Port im Namen des privaten Clients, sodass die Nachrichten, die aus dem öffentlichen Netzwerk an dieser IP-Adresse und diesem Port ankommen, als SIP-Nachrichten behandelt werden.
- Öffentliche IP-Adresse und Port im Namen der öffentlichen Clients, sodass die Nachrichten, die vom privaten Netzwerk an dieser IP-Adresse und diesem Port ankommen, als SIP-Nachrichten behandelt werden.

Wenn eine SIP-Nachricht über das Netzwerk gesendet wird, sammelt das SIP Application Layer Gateway (ALG) Informationen aus der Nachricht und übersetzt die IP-Adressen in den folgenden Headern in LSN-Pool-IP-Adressen:

- Über
- Kontakt
- Route
- Route aufzeichnen

In der folgenden Beispiel-SIP-Anforderungsnachricht ersetzt LSN die IP-Adressen in den Header-Feldern, um sie vor dem externen Netzwerk zu verbergen.

```
1 INVITE adam@10.102.185.156 SIP/2.0 Via: SIP/2.0/UDP 192.170.1.161:62914
      From: eve@10.120.210.3 To: adam@10.102.185.156 Call-ID: a12abcde@10
     .120.210.3 Contact: adam@10.102.185.156 Route: <sip:netscreen@10
     .150.20.3:5060> Record-Route: <sip:netscreen@10.150.20.3:5060>
2 <!--NeedCopy-->
```

Wenn eine Nachricht mit SDP-Informationen eingeht, sammelt das SIP-ALG Informationen aus der Nachricht und übersetzt die IP-Adressen in den folgenden Feldern in LSN-Pool-IP-Adressen und Portnummern:

- c= (Verbindungsinformationen)

  Dieses Feld kann auf Sitzungs- oder Medienebene angezeigt werden. Es wird im folgenden Format angezeigt:

  c=<network-type><address-type><connection-address>

  Wenn die Ziel-IP-Adresse eine Unicast-IP-Adresse ist, erstellt das SIP-ALG Pinholes, indem es die im Feld m= angegebene IP-Adresse und Portnummern verwendet.

- m= (Medienmitteilung)

  Dieses Feld wird auf Medienebene angezeigt und enthält die Beschreibung des Mediums. Es wird im folgenden Format angezeigt:

  m=<media><port><transport><fmt list>

- a= (information about the media field)

  Dieses Feld kann auf Sitzungs- oder Medienebene im folgenden Format angezeigt werden:

  a=<attribute>

  a=<attribute>:<value>

Der folgende Auszug aus einem SDP-Beispielabschnitt zeigt die Felder, die für die Ressourcenzuweisung übersetzt wurden.

o=Benutzer 2344234 55234434 DIN IP4 10.150.20.3

C=in IP4 10.150.20.3

m=audio 43249 RTP/AVP 0

Die folgende Tabelle zeigt, wie SIP-Payload übersetzt wird.

Eingehende Anfrage (von öffentlich nach privat)	In:	Ohne
	Von:	Ohne
	Anruf-ID:	Ohne
	Über:	Ohne
	Anfrage-URI:	Ersetzen Sie die LSN-Pool-IP-Adresse durch eine private IP-Adresse
	Kontakt:	Ohne
	Route aufzeichnen	Ohne

	Reiseroute:	Ohne
Ausgehende Antwort (von privat nach öffentlich)	In:	Ohne
	Von:	Ohne
	Anruf-ID:	Ohne
	Über:	Ohne
	Anfrage-URI:	Ersetzen Sie die private IP-Adresse durch die LSN-Pool-IP-Adresse
	Kontakt:	Ersetzen Sie die private IP-Adresse durch die LSN-Pool-IP-Adresse
	Route aufzeichnen	Ohne
	Reiseroute:	Ohne
Ausgehende Anfrage (von privat nach öffentlich)	In:	Ohne
	Von:	Ohne
	Anruf-ID:	Ohne
	Über:	Ersetzen Sie die private IP-Adresse durch die LSN-Pool-IP-Adresse
	Anfrage-URI:	Ohne
	Kontakt:	Ersetzen Sie die private IP-Adresse durch die LSN-Pool-IP-Adresse
	Route aufzeichnen	Ohne
	Reiseroute:	Ohne
Eingehende Antwort (von öffentlich nach privat)	In:	Ohne
	Von:	Ohne
	Anruf-ID:	Ohne

	Über:	Ersetzen Sie die LSN-Pool-IP-Adresse durch eine private IP-Adresse
	Anfrage-URI:	Ohne
	Kontakt:	Behalte die öffentliche IP-Adresse, falls vorhanden
	Route aufzeichnen	Ohne
	Reiseroute:	Ohne

Einschränkungen von SIP ALG

Ein SIP-ALG hat die folgenden Einschränkungen:

- Nur SDP-Payload wird unterstützt.
- Folgende Komponenten werden nicht unterstützt:
  - Multicast-IP-Adressen
  - Verschlüsseltes SDP
  - SCHIFF BIS
  - FQDN-Übersetzung
  - SIP-Layer-Authentifizierung
  - TD/Partitionierung
  - Mehrteiliger Körper
  - SIP-Nachrichten über IPv6-Netzwerk
  - Faltung der Leitung

Getestete SIP-Clients und Proxyserver

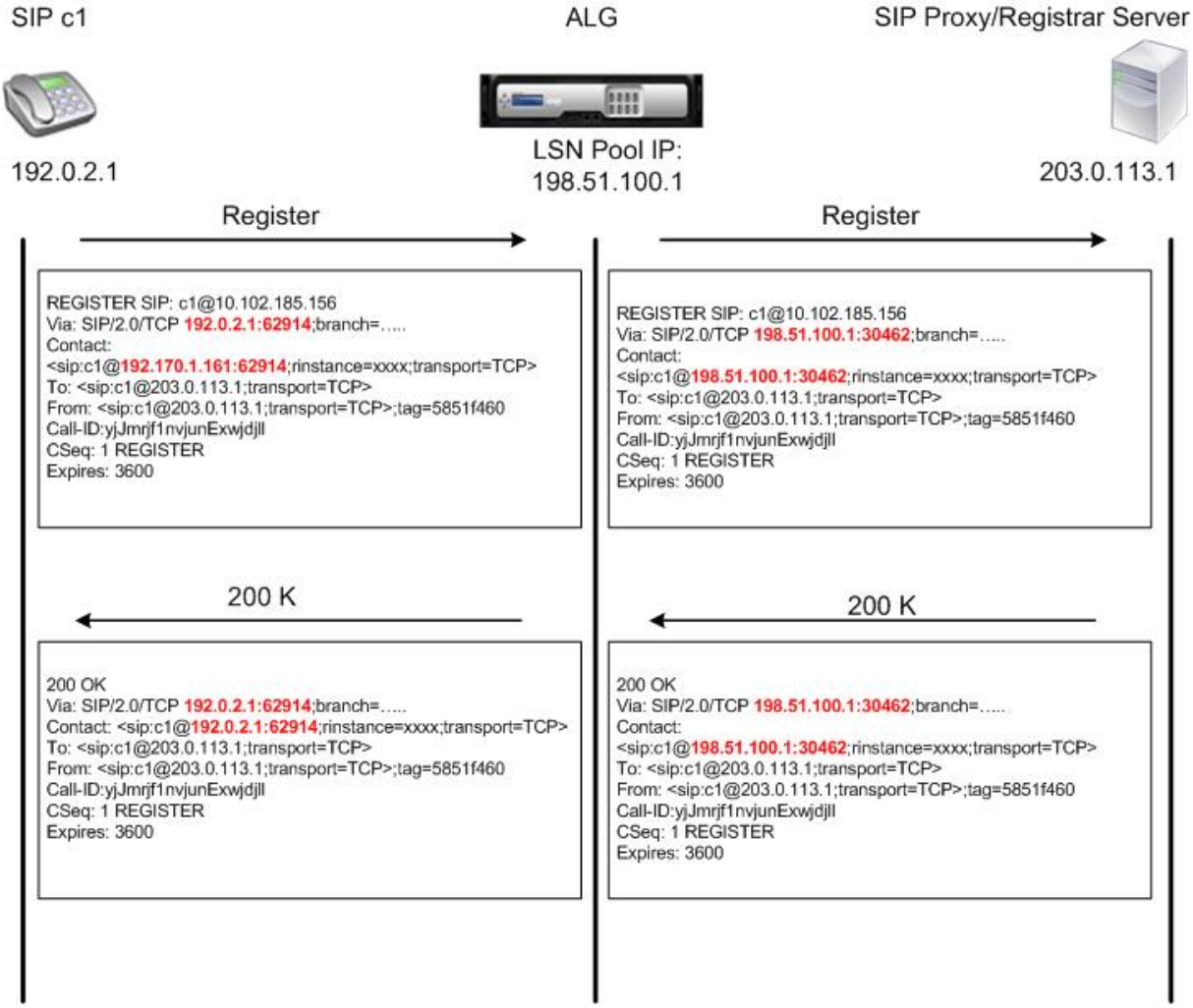
Die folgenden SIP-Clients und Proxyserver wurden mit SIP ALG getestet:

- **SIP-Kunden:** X-Lite, Zoiper, Ekiga. Avaya
- **Proxyserver: OpenSIPS**

LSN SIP-Szenario: SIP-Proxy außerhalb des privaten Netzwerks (öffentliches Netzwerk)

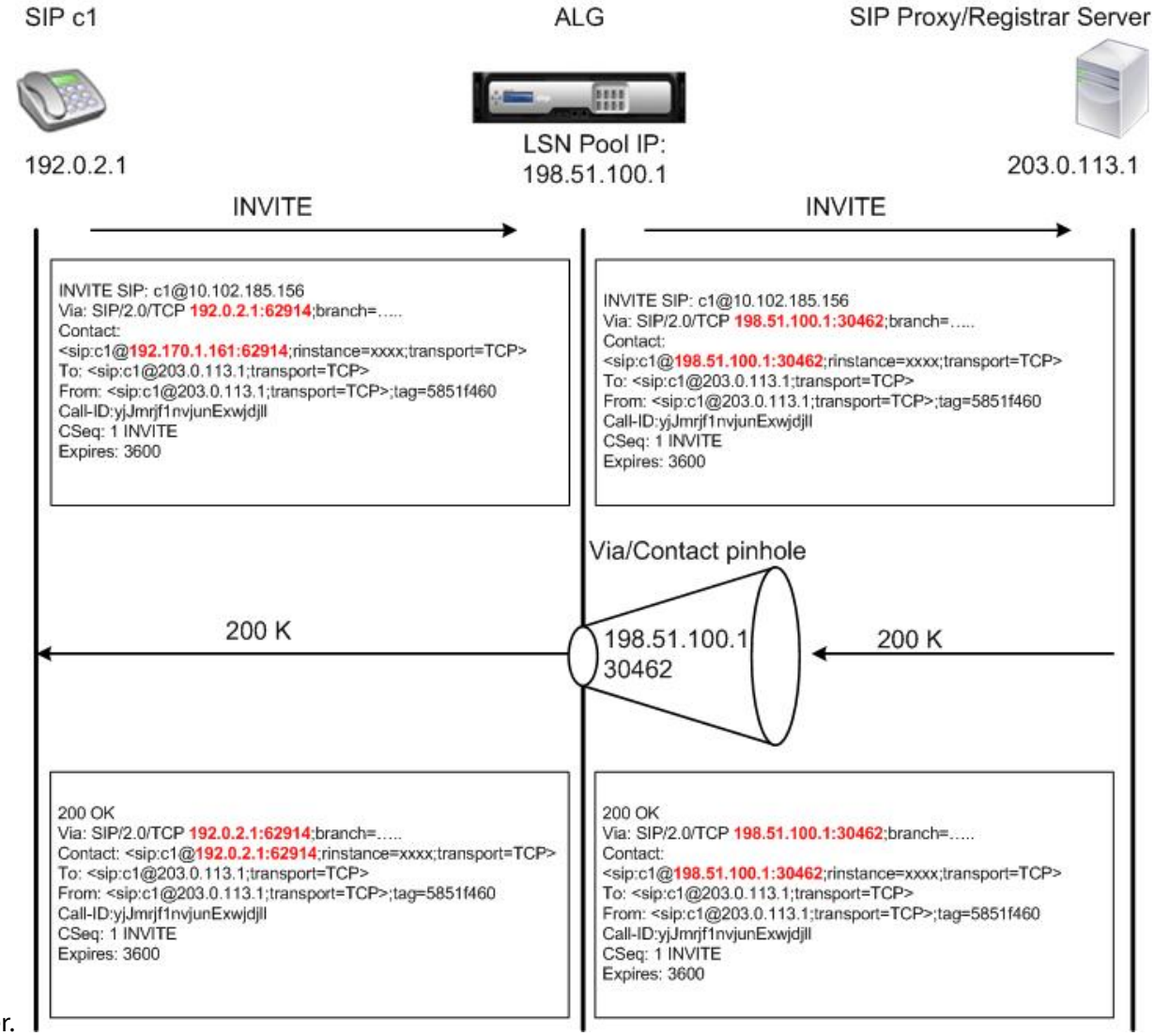
SIP-Client-Registrierung

Für einen typischen SIP-Anruf muss sich der SIP-Client beim SIP-Registrar registrieren, indem er eine REGISTER-Anfrage verfasst und an den SIP-Registrar sendet. Das SIP-ALG der NetScaler-Appliance fängt die Anfrage ab, ersetzt die IP-Adresse und Portnummer in der Anfrage durch die LSN-Pool-IP-Adresse und Portnummer, die in der LSN-Konfiguration angegeben sind, und leitet die Anfrage an den SIP-Registrar weiter. Das SIP-ALG öffnet dann ein Loch in der NetScaler-Konfiguration, um die weitere SIP-Kommunikation zwischen dem SIP-Client und dem SIP-Registrar zu ermöglichen. Der SIP-Registrar sendet über die IP-Adresse und Portnummer des LSN-Pools eine 200-OK-Antwort an den SIP-Client. Die NetScaler-Appliance erfasst diese Antwort im Pinhole, und das SIP-ALG ersetzt den SIP-Header und fügt die ursprünglichen SIP-Felder Contact, Via, Route und Record-Route wieder in die Nachricht ein. Das SIP-ALG leitet die Nachricht dann an den SIP-Client weiter. Die folgende Abbildung zeigt, wie SIP ALG LSN in einem Ablauf zur SIP-Anrufregistrierung verwendet.



Ausgehende Anrufe

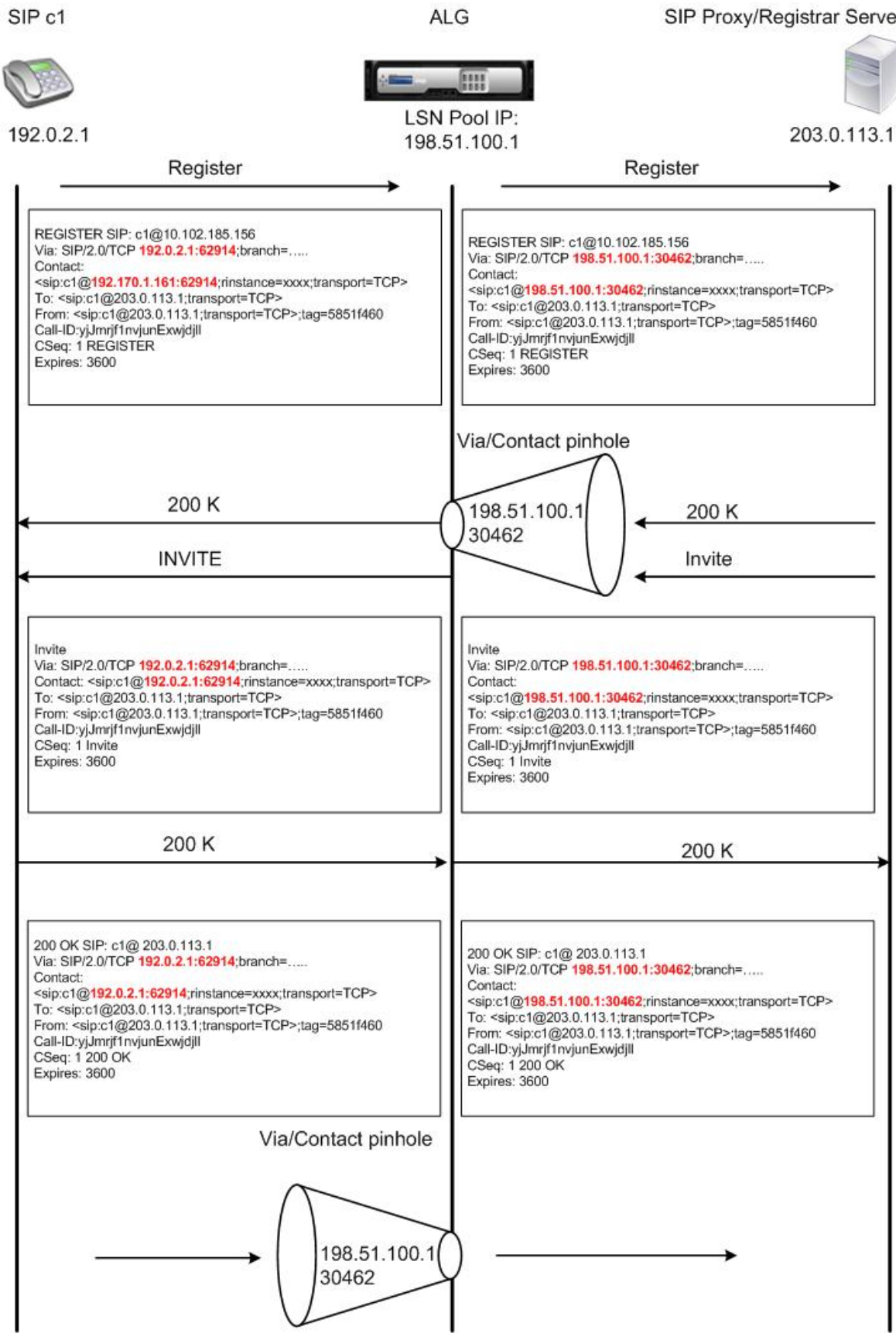
Ein SIP-Anruf wird mit einer SIP INVITE-Nachricht initiiert, die vom internen an das externe Netzwerk gesendet wird. Das SIP-ALG führt NAT für die IP-Adressen und Portnummern in den SIP-Headerfeldern Via, Contact, Route und Record-Route durch und ersetzt sie durch die IP-Adresse und Portnummer des LSN-Pools. LSN speichert diese Zuordnungen für nachfolgende SIP-Nachrichten im SIP-Anruf. Das SIP-ALG öffnet dann separate Pinholes in der NetScaler-Konfiguration, sodass SIP und Medien über die NetScaler-Appliance an den dynamisch zugewiesenen Ports, die in den SDP- und SIP-Headern angegeben sind, übertragen werden können. Wenn eine 200 OK-Meldung beim NetScaler eingeht, wird sie von einer der erstellten Pinholes erfasst. Das SIP-ALG ersetzt den SIP-Header, stellt die ursprünglichen SIP-Felder Contact, Via, Route und Record-Route wieder her und leitet die Nachricht dann an den internen SIP-Client weiter.



Eingehende Anrufe

Ein eingehender SIP-Anruf wird mit einer SIP INVITE-Nachricht vom externen Client an das interne Netzwerk initiiert. Der SIP-Registrar leitet die INVITE-Nachricht an den SIP-Client im internen Netzwerk weiter und verwendet dabei die Pinhole, die erstellt wurde, als sich der interne SIP-Client beim SIP-Registrar registriert hat.

Das SIP-ALG führt NAT für die LSN-IP-Adressen und Portnummern in den SIP-Headerfeldern Via, Contact, Route und Record-Route durch, übersetzt sie in die IP-Adresse und Portnummer des internen SIP-Clients und leitet die Anfrage an den SIP-Client weiter. Wenn die vom internen SIP-Client gesendete 200-OK-Antwortnachricht an der NetScaler-Appliance ankommt, führt das SIP-ALG NAT für die IP-Adressen und Portnummern in den SIP-Headerfeldern Via, Contact, Route und Record-Route durch, übersetzt sie in die IP-Adresse und Portnummer des LSN-Pools, leitet die Antwortnachricht an den SIP-Registrar weiter und öffnet dann eine Lochblende in ausgehender Richtung für die weitere SIP-



Kommunikation.

Beendigung des Anrufs

Die BYE-Nachricht beendet einen Anruf. Wenn das Gerät eine BYE-Nachricht empfängt, übersetzt es die Header-Felder in der Nachricht genauso wie bei jeder anderen Nachricht. Da jedoch eine BYE-Nachricht vom Empfänger mit 200 OK bestätigt werden muss, verzögert das ALG den Anruf-Teardown um 15 Sekunden, um Zeit für die Übertragung der 200 OK zu haben.

Telefonieren zwischen Clients im selben Netzwerk

Wenn sowohl Client A als auch Client B im selben Netzwerk einen Anruf initiieren, werden die SIP-Nachrichten über den SIP-Proxy im externen Netzwerk weitergeleitet. Das SIP-ALG verarbeitet die INVITE von Client A als normalen ausgehenden Anruf. Da sich Client B im selben Netzwerk befindet, sendet der SIP-Proxy das INIVITE zurück an die NetScaler-Appliance. Das SIP-ALG untersucht die INIVITE-Nachricht, stellt fest, dass sie die NAT-IP-Adresse von Client A enthält, und ersetzt diese Adresse durch die private IP-Adresse von Client A, bevor die Nachricht an Client B gesendet wird. Sobald der Anruf zwischen den Clients hergestellt ist, ist der NetScaler nicht an der Medienübertragung zwischen den Clients beteiligt.

Weitere LSN-SIP-Szenarien: SIP-Proxy im privaten Netzwerk

Wenn Sie den SIP-Proxyserver im privaten Netzwerk hosten möchten, empfiehlt Citrix, dass Sie einen der folgenden Schritte ausführen:

- Konfigurieren Sie eine statische LSN-Zuordnung für den privaten SIP-Proxy. Weitere Informationen finden Sie unter Konfigurieren von statischen LSN-Maps. Stellen Sie sicher, dass der NAT-Port mit dem Port identisch ist, der im SIP-ALG-Profil konfiguriert ist.
- Konfigurieren Sie den SIP-Proxyserver in einer entmilitarisierten Zone (DMZ).

Abbildung 1. SIP-Anrufregistrierung

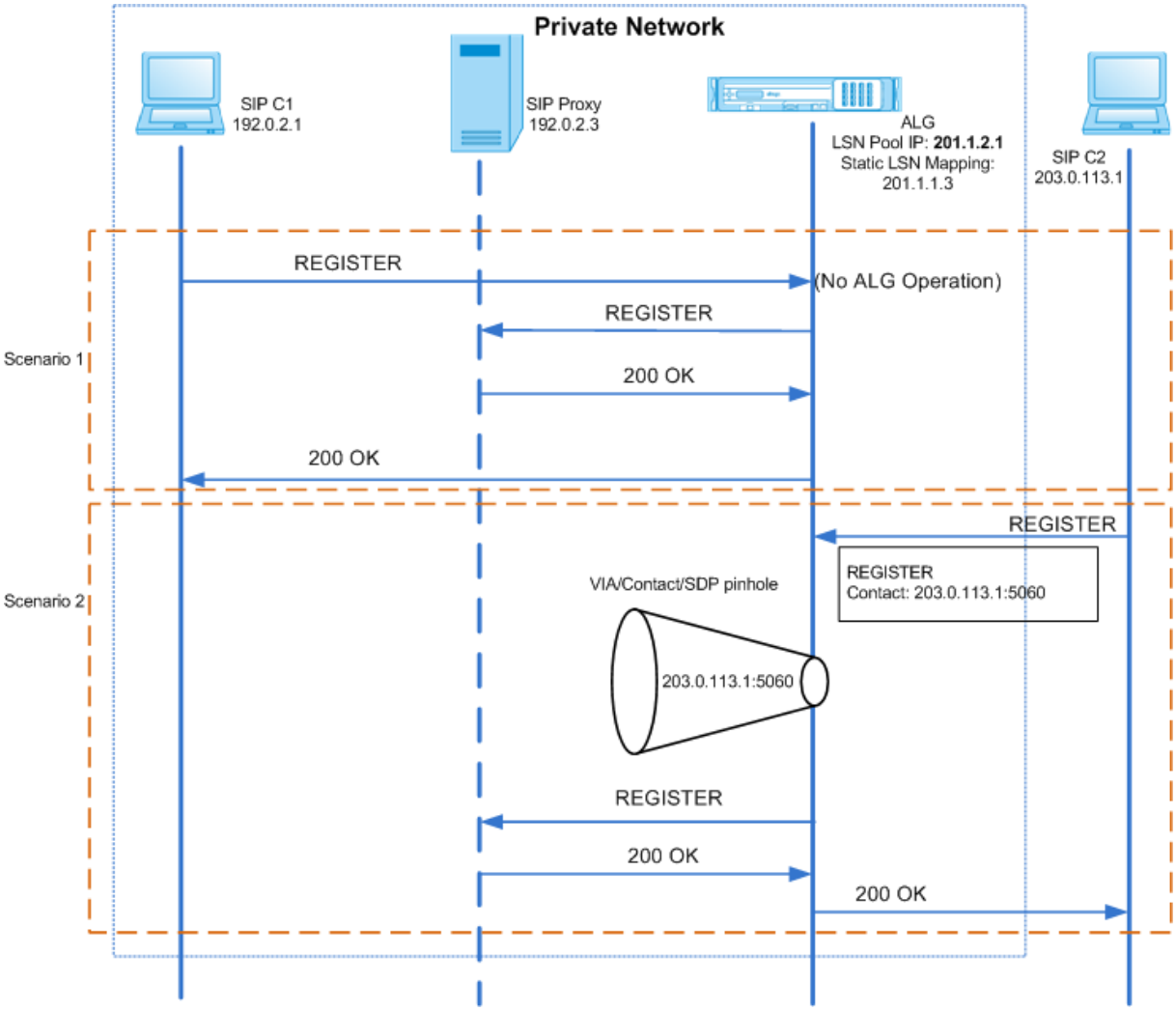
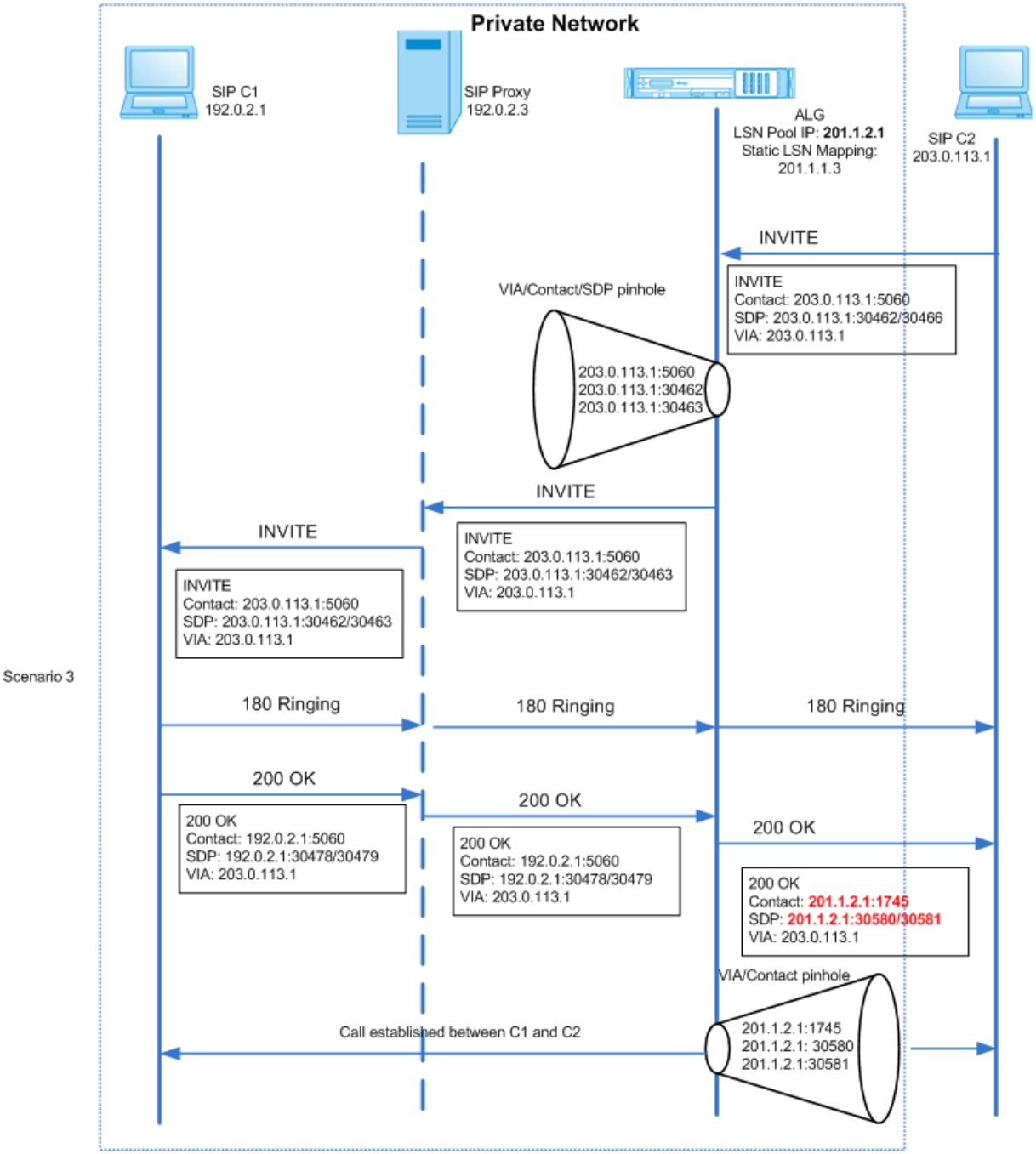


Abbildung 2. Ablauf eingehender SIP-Anrufe



Die Abbildungen 1 und 2 zeigen die folgenden Szenarien:

- Szenario 1: Der SIP-Client im privaten Netzwerk registriert sich beim SIP-Proxyserver im selben Netzwerk. ALG-Operationen werden nicht ausgeführt, da sich der SIP-Client und der SIP-Proxyserver im selben Netzwerk befinden.
- Szenario 2: Der SIP-Client im öffentlichen Netzwerk registriert sich beim SIP-Proxyserver im privaten Netzwerk. Die REGISTER-Nachricht vom öffentlichen SIP-Client wird mithilfe der auf der Appliance konfigurierten statischen LSN-Zuordnung an die NetScaler-Appliance gesendet, und

die Appliance erstellt eine Pinhole für weitere SIP-Operationen.

- Szenario 3 — Ablauf eingehender SIP-Anrufe. Ein eingehender SIP-Anruf wird mit einer SIP INVITE-Nachricht vom externen zum internen Netzwerk initiiert. Die NetScaler-Appliance empfängt die INVITE-Nachricht vom SIP-Client C2, der sich im externen Netzwerk befindet, über die auf der NetScaler-Appliance konfigurierten statischen LSN-Maps.
  Die Appliance erstellt eine Pinhole und leitet die INVITE-Nachricht an den SIP-Proxy weiter. Der SIP-Proxy leitet dann die INVITE-Nachricht an den SIP-Client C1 im internen Netzwerk weiter. Der SIP-Client C1 sendet dann 180 und 200 OK-Nachrichten an den SIP-Proxy, der die Nachricht wiederum über die NetScaler-Appliance an den SIP-Client C2 weiterleitet.
  Wenn die vom internen SIP-Client C1 gesendete 200-OK-Antwortnachricht beim NetScaler eingeht, führt das SIP-ALG NAT für die IP-Adressen und Portnummern in den SIP-Headerfeldern Via, Contact, Route und Record-Route sowie in den SDP-Feldern durch und ersetzt sie durch die IP-Adresse und Portnummer des LSN-Pools. Das SIP-ALG leitet die Antwortnachricht dann an den SIP-Client C2 weiter und öffnet in ausgehender Richtung eine Pinhole für die weitere SIP-Kommunikation.

Unterstützung für Audit-Logs

Sie können ALG-Informationen als Teil der LSN-Protokollierung protokollieren, indem Sie ALG in der LSN-Überwachungsprotokollierungskonfiguration aktivieren. Weitere Informationen zur LSN-Protokollierung finden Sie unter LSN protokollieren und überwachen. Eine Protokollmeldung für einen ALG-Eintrag im LSN-Protokoll besteht aus folgenden Informationen:

- Zeitstempel
- Art der SIP-Nachricht (z. B. SIP-Anfrage)
- Quell-IP-Adresse und Port des SIP-Clients
- Ziel-IP-Adresse und Port des SIP-Proxys
- NAT-IP-Adresse und Port
- SIP-Methode
- Sequenznummer
- Ob der SIP-Client registriert ist oder nicht
- Benutzername und Domain des Anrufers
- Benutzername und Domäne des Empfängers

Beispiel für ein Audit-Protokoll:

Anfrage:

```
07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 169 0 : Infomsg: "SIP request" - Group: g2
     - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. - Transport
    : TCP - Source_IP: 192.169.1.165 - Source_port: 57952 -
    Destination_IP: 10.102.185.156 - Destination_port: 5060 - Natted_IP:
```



```
        10.102.185.191 - Natted_port: 10313 - Method: REGISTER -
       Sequence_Number: 3060 - Register: YES - Content_Type: -
       Caller_user_name: 156_pvt_1 - Callee_user_name: 156_pvt_1 -
       Caller_domain_name: - Callee_domain_name: -
<!--NeedCopy-->
```

Antwort:

```
07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 170 0 : Infomsg: "SIP response" - Group:
    g2 - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. -
    Transport: TCP - Response_code 200 - Source_IP: 10.102.185.156 -
    Source_port: 5060 - Destination_IP: 192.169.1.165 - Destination_port
    : 57952 - Natted_IP: 10.102.185.191 - Natted_port: 10313 -
    Sequence_Number: 3060 - Content_Type: - Caller_user_name: 156_pvt_1
    - Callee_user_name: 156_pvt_1 - Caller_domain_name: -
    Callee_domain_name: -
<!--NeedCopy-->
```

Konfiguration von SIP ALG

Sie müssen die SIP ALG als Teil der LSN-Konfiguration konfigurieren. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurationsschritte für LSN. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Stellen Sie beim Hinzufügen des LSN-Anwendungsprofils die folgenden Parameter ein:
  - IP-Pooling = GEPAART
  - Adress- und Portzuordnung = ENDPUNKTUNABHÄNGIG
  - Filterung = ENDPUNKTUNABHÄNGIG

Wichtig: Damit das SIP-ALG funktioniert, ist eine vollständige Cone NAT-Konfiguration erforderlich.

Beispiel:

```
add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT
<!--NeedCopy-->
```

- Erstellen Sie ein SIP-ALG-Profil und stellen Sie sicher, dass Sie entweder den Quellportbereich oder den Zielportbereich definieren.

Beispiel:

```
add lsn sipalgprofile sipalgprofile_tcp -sipsrcportrange 1-65535 -
    sipdstportrange 5060 -openViaPinhole ENABLED -openRecordRoutePinhole
     ENABLED  - sipTransportProtocol TCP
```



```
<!--NeedCopy-->
```

- Stellen Sie SIP ALG = ENABLED ein, während Sie die LSN-Gruppe erstellen.

Beispiel:

```
add lsn group g1 -clientname c1 -sipalg ENABLED
<!--NeedCopy-->
```

- Binden Sie das SIP-ALG-Profil an die LSN-Gruppe.

Beispiel für eine SIP-ALG-Konfiguration:

Die folgende Beispielkonfiguration zeigt, wie Sie eine einfache LSN-Konfiguration mit einem einzelnen Teilnehmernetzwerk, einer einzelnen LSN-NAT-IP-Adresse, einer SIP-ALG-spezifischen Einstellung erstellen und SIP-ALG konfigurieren:

```
add lsn pool p1

Done

bind lsn pool p1 10.102.185.190

Done

add lsn client c1

Done

bind lsn client c1 -network 192.170.1.0 -netmask 255.255.255.0

Done

add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

add lsn appsprofile app_udp UDP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

bind lsn appsprofile app_tcp 1-65535

Done
```



```
28
29 bind lsn appsprofile app_udp 1-65535
30
31 Done
32
33 add lsn sipalgprofile sipalgprofile_tcp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED  -
      sipTransportProtocol TCP
34
35 Done
36
37 add lsn sipalgprofile sipalgprofile_udp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED -
      sipTransportProtocol UDP
38
39 Done
40
41 add lsn group g1 -clientname c1 -sipalg ENABLED
42
43 Done
44
45 bind lsn group g1 -poolname p1
46
47 Done
48
49 bind lsn group g1 -appsprofilename app_tcp
50
51 Done
52
53 bind lsn group g1 -appsprofilename app_udp
54
55 Done
56
57 bind lsn group g1 -sipalgprofilename sipalgprofile_tcp
58
59 Done
60
61 bind lsn group g1 -sipalgprofilename sipalgprofile_udp
62
63 Done
64 <!--NeedCopy-->
```


Application Layer Gateway für das RTSP-Protokoll

July 24, 2023

Das Real Time Streaming Protocol (RTSP) ist ein Protokoll auf Anwendungsebene für die Übertragung von Mediendaten in Echtzeit. RTSP ist ein Kontrollkanalprotokoll zwischen dem Medienclient und dem Medienserver, das für die Einrichtung und Steuerung von Mediensitzungen zwischen Endpunkten verwendet wird. Die typische Kommunikation findet zwischen einem Client und einem Streaming-Media-Server statt.

Um Medien von einem privaten Netzwerk in ein öffentliches Netzwerk zu streamen, müssen IP-Adressen und Portnummern über das Netzwerk übersetzt werden. Die NetScaler-Funktionalität umfasst ein Application Layer Gateway (ALG) für RTSP, das zusammen mit Large Scale NAT (LSN) verwendet werden kann, um den Medienstream zu analysieren und alle erforderlichen Änderungen vorzunehmen, um sicherzustellen, dass das Protokoll weiterhin über das Netzwerk funktioniert.

Wie die IP-Adressübersetzung durchgeführt wird, hängt vom Typ und der Richtung der Nachricht sowie von der Art der Medien ab, die von der Client-Server-Bereitstellung unterstützt werden. Nachrichten werden wie folgt übersetzt:

- Ausgehende Anfrage — Private IP-Adresse für eine öffentliche IP-Adresse im Besitz von NetScaler, die als LSN-Pool-IP-Adresse bezeichnet wird.
- Eingehende Antwort — LSN-Pool-IP-Adresse zur privaten IP-Adresse.
- Eingehende Anfrage — keine Übersetzung.
- Ausgehende Antwort — Private IP-Adresse zur LSN-Pool-IP-Adresse.

> **Hinweis**
>
> RTSP ALG wird in einer eigenständigen NetScaler-Appliance, in einem NetScaler-Hochverfügbarkeits-Setup sowie in einem NetScaler-Cluster-Setup unterstützt.

Einschränkungen von RTSP ALG

Das RTSP-ALG unterstützt Folgendes nicht:

- Multicast-RTSP-Sitzungen
- RTSP-Sitzung über UDP
- TD/Admin-Partitionierung
- RSTP-Authentifizierung
- HTTP-Tunneling

RTSP- und LSN-Szenario

In der Regel gibt eine RTSP-SETUP-Anfrage an, wie ein einzelner Medienstream transportiert werden muss. Die Anfrage enthält die URL des Medienstreams und einen Transportspezifizierer. Dieser Spezifizierer umfasst in der Regel einen lokalen Port für den Empfang von RTP-Daten (Audio oder Video) und einen weiteren für den Empfang von RTCP-Daten (Metainformationen). Die Serverantwort bestätigt normalerweise die ausgewählten Parameter und füllt die fehlenden Teile aus, z. B. die vom Server ausgewählten Ports. Jeder Medienstream muss mithilfe des SETUP-Befehls konfiguriert werden, bevor eine aggregierte Wiedergabeanforderung gesendet werden kann.

Bei einer typischen RTSP-Kommunikation sendet der Medienclient im öffentlichen Netzwerk eine SETUP-Anfrage an den Medienserver im privaten Netzwerk. RSTP ALG fängt die Anfrage ab und ersetzt im Medienstream die öffentliche IP-Adresse und Portnummer durch die LSN-Pool-IP-Adresse und die LSN-Portnummer.

Der Medienserver im privaten Netzwerk verwendet die LSN-Pool-IP-Adresse und die LSN-Portnummer, um eine 200-OK-Antwort an den Medienclient im öffentlichen Netzwerk zu senden. Das NetScaler RTSP ALG fängt die Antwort ab und ersetzt die LSN-Pool-IP-Adresse und die LSN-Portnummer durch die öffentliche IP-Adresse und Portnummer des Media Clients.

Konfiguration von RTSP ALG

Konfigurieren Sie RTSP ALG als Teil der LSN-Konfiguration. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurationsschritte für LSN. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Stellen Sie den **NAT-Typ** auf DETERMINSTIC oder DYNAMIC ein, während Sie den LSN-Pool hinzufügen.
- Stellen Sie beim Hinzufügen des LSN-Anwendungsprofils die folgenden Parameter ein:
  - IP-Pooling = GEPAART
  - Adress- und Portzuordnung = ENDPUNKTUNABHÄNGIG
  - Filterung = ENDPUNKTUNABHÄNGIG
- Erstellen Sie ein RTSP-ALG-Profil und binden Sie das RTSP-ALG-Profil an die LSN-Gruppe.

Beispiel-RTSP-ALG-Konfiguration:

Die folgende Beispielkonfiguration zeigt, wie Sie eine einfache LSN-Konfiguration mit einem einzelnen Abonnentennetzwerk, einer einzelnen LSN-NAT-IP-Adresse und RTSP-ALG-Einstellungen erstellen:

```
enable ns feature WL SP LB CS LSN

Done

add lsn pool pool1 -nattype DETERMINISTIC
```



```
6
7  Done
8
9  bind lsn pool pool1 10.102.218.246
10
11 Done
12
13 add lsn client client1
14
15 Done
16
17 bind lsn client client1 -network 200.200.200.11 -netmask 255.255.255.0
18
19 Done
20
21 add lsn appsprofile app1 TCP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
22
23 Done
24
25 add lsn appsprofile app2 UDP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile app1 1-65535
30
31 Done
32
33 bind lsn appsprofile app2 1-65535
34
35 Done
36
37 add lsn rtspalgprofile rtspalgprofiledefault -rtspIdleTimeout 1000 -
      rtspportrange 554
38
39 Done
40
41 add lsn group group1 -clientname client1 -nattype DETERMINISTIC -
      portblocksize 512 -rtspalg ENABLED
42
43 Done
44
45 bind lsn group group1 -poolname pool1
46
```



```
Done

bind lsn group group1 -appsprofilename app1

Done

bind lsn group group1 -appsprofilename app2

Done

bind lsn group group1 -rtspalgprofilename rtspalgprofiledefault

Done
<!--NeedCopy-->
```

Application Layer Gateway für IPSec-Protokoll

May 11, 2023

Wenn die Kommunikation zwischen zwei Netzwerkgeräten (z. B. Client und Server) das IPSec-Protokoll verwendet, verwendet der IKE-Verkehr (der über UDP erfolgt) Portfelder, der ESP-Verkehr (Encapsulating Security Payload) jedoch nicht. Wenn ein NAT-Gerät auf dem Pfad zwei oder mehr Clients am selben Ziel dieselbe NAT-IP-Adresse (aber unterschiedliche Ports) zuweist, kann das NAT-Gerät den zurückgegebenen ESP-Verkehr nicht unterscheiden und ordnungsgemäß weiterleiten. Er enthält keine Portinformationen. Daher schlägt der IPSec-ESP-Verkehr am NAT-Gerät fehl.

NAT-Traversal (NAT-T) fähige IPSec-Endpunkte erkennen während der IKE-Phase 1 das Vorhandensein eines NAT-Zwischengeräts und wechseln für den gesamten nachfolgenden IKE- und ESP-Verkehr auf den UDP-Port 4500 (ESP wird in UDP gekapselt). Ohne NAT-T-Unterstützung auf den Peer-IPSec-Endpunkten wird IPsec-geschützter ESP-Verkehr ohne UDP-Kapselung übertragen. Daher schlägt der IPSec-ESP-Verkehr am NAT-Gerät fehl.

Die NetScaler-Appliance unterstützt IPSec Application Andwendungslayer Gateway (ALG) - Funktionalität für umfangreiche NAT-Konfigurationen. Das IPSec-ALG verarbeitet IPSec-ESP-Verkehr und verwaltet die Sitzungsinformationen, sodass der Datenverkehr nicht ausfällt, wenn die IPSec-Endpunkte NAT-T (UDP-Kapselung des ESP-Datenverkehrs) nicht unterstützen.

So funktioniert IPSec ALG

Ein IPSec-ALG überwacht den IKE-Verkehr zwischen einem Client und dem Server und erlaubt zu einem bestimmten Zeitpunkt nur einen IKE-Phase-2-Nachrichtenaustausch zwischen dem Client

und dem Server.

Sobald die bidirektionalen ESP-Pakete für einen bestimmten Fluss empfangen wurden, erstellt das IPSec-ALG eine NAT-Sitzung für diesen bestimmten Fluss, sodass der nachfolgende ESP-Verkehr reibungslos fließen kann. Der ESP-Verkehr wird durch Sicherheitsparameterindizes (SPIs) identifiziert, die für einen Fluss und für jede Richtung einzigartig sind. Ein IPSec-ALG verwendet ESP-SPIs anstelle von Quell- und Zielports, um NAT in großem Maßstab durchzuführen.

Wenn ein Gate keinen Verkehr empfängt, wird es zu einem Timeout. Nach dem Timeout beider Gates ist ein weiterer IKE-Phase-2-Austausch zulässig.

IPSec-ALG-Timeouts

IPSec ALG auf einer NetScaler-Appliance hat drei Timeout-Parameter:

- **ESP-Gate-Timeout**. Maximale Zeit, in der die NetScaler-Appliance ein IPSec-ALG-Gate für einen bestimmten Client auf einer bestimmten NAT-IP-Adresse für einen bestimmten Server blockiert, wenn kein bidirektionaler ESP-Verkehr zwischen dem Client und dem Server ausgetauscht wird.
- **Timeout für die IKE-Sitzung.** Maximale Zeit, in der die NetScaler-Appliance die IKE-Sitzungsinformationen speichert, bevor sie entfernt werden, wenn für diese Sitzung kein IKE-Verkehr vorhanden ist.
- **Zeitlimit für ESP-Sitzung**. Maximale Zeit, für die die NetScaler-Appliance die ESP-Sitzungsinformationen speichert, bevor sie entfernt werden, falls für diese Sitzung kein ESP-Verkehr vorhanden ist.

Punkte, die vor der Konfiguration von IPSec ALG zu beachten sind

Bevor Sie mit der Konfiguration von IPSec ALG beginnen, sollten Sie die folgenden Punkte berücksichtigen:

- Sie müssen die verschiedenen Komponenten des IPSec-Protokolls verstehen.
- IPSec ALG wird für DS-Lite- und Large-Scale-NAT64-Konfigurationen nicht unterstützt.
- IPSec ALG wird für Hairpin LSN Flow nicht unterstützt.
- IPSec ALG funktioniert nicht mit RNAT-Konfigurationen.
- IPSec ALG wird in NetScaler-Clustern nicht unterstützt.

Konfigurationsschritte

Die Konfiguration von IPSec ALG für NAT44 in großem Maßstab auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- **Erstellen Sie ein LSN-Anwendungsprofil und binden Sie es an die LSN-Konfiguration.** Stellen Sie bei der Konfiguration eines Anwendungsprofils die folgenden Parameter ein:

- Protokoll=UDP
- IP-Pooling = GEPAART
- Port=500

Binden Sie das Anwendungsprofil an die LSN-Gruppe einer LSN-Konfiguration. Anweisungen zum Erstellen einer LSN-Konfiguration finden Sie unter Konfigurationsschritte für LSN.

- **Erstellen Sie ein IPsec-ALG-Profil**. Ein IPSec-Profil umfasst verschiedene IPSec-Timeouts, z. B. das IKE-Sitzungs-Timeout, das ESP-Sitzungs-Timeout und das ESP-Gate-Timeout. Sie binden ein IPSec-ALG-Profil an eine LSN-Gruppe. Ein IPSec-ALG-Profil hat die folgenden Standardeinstellungen:
  - IKE-Sitzungs-Timeout = 60 Minuten
  - ESP-Sitzungs-Timeout = 60 Minuten
  - ESP-Gate-Timeout = 30 Sekunden
- **Binden Sie das IPSec-ALG-Profil an die LSN-Konfiguration**. IPSec ALG wird für eine LSN-Konfiguration aktiviert, wenn Sie ein IPSec-ALG-Profil an die LSN-Konfiguration binden. Binden Sie das IPSec-ALG-Profil an die LSN-Konfiguration, indem Sie den IPSec-ALG-Profilparameter auf den Namen des erstellten Profils in der LSN-Gruppe festlegen. Ein IPSec-ALG-Profil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein IPSec-ALG-Profil haben.

So erstellen Sie ein LSN-Anwendungsprofil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lsn appsprofile <appsprofilename> UDP -ippooling PAIRED
2
3 show lsn appsprofile
4 <!--NeedCopy-->
```

So binden Sie den Zielport mithilfe der Befehlszeilenschnittstelle an das LSN-Anwendungsprofil

Geben Sie in der Befehlszeile Folgendes ein:

```
1 bind lsn appsprofile <appsprofilename> <lsnport>
2
3 show lsn appsprofile
4 <!--NeedCopy-->
```


So binden Sie ein LSN-Anwendungsprofil mithilfe der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> -appsprofilename <string>

show lsn group
<!--NeedCopy-->
```

So erstellen Sie ein IPSec-ALG-Profil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add ipsecalg profile <name> [-ikeSessionTimeout <positive_integer>] [-
    espSessionTimeout <positive_integer>] [-espGateTimeout <
    positive_integer>] [-connfailover ( ENABLED | DISABLED)

show ipsecalg profile <name>
<!--NeedCopy-->
```

So binden Sie ein IPSec-ALG-Profil mithilfe der CLI an eine LSN-Konfiguration

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> -poolname <string> - ipsecAlgProfile <string
    >

show lsn group <name>
<!--NeedCopy-->
```

Um ein LSN-Anwendungsprofil zu erstellen und es mithilfe der GUI an eine LSN-Konfiguration zu binden

Navigieren Sie zu **System** > **Large Scale NAT** > **Profiles**, klicken Sie auf die Registerkarte **Anwendung**, fügen Sie ein LSN-Anwendungsprofil hinzu und binden Sie es an eine LSN-Gruppe.

So erstellen Sie ein IPSec-ALG-Profil mithilfe der GUI

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf die Registerkarte **IPSEC ALG** und fügen Sie dann ein IPSec-ALG-Profil hinzu.

So binden Sie ein IPSec-ALG-Profil mithilfe der GUI an eine LSN-Konfiguration**

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group**, öffnen Sie die LSN-Gruppe.
2. Klicken Sie in **den Erweiterten Einstellungen**auf **+ IPSEC-ALG-Profil**, um das erstellte IPSec-ALG-Profil an die LSN-Gruppe zu binden.

Beispielkonfiguration

In der folgenden NAT44-Beispielkonfiguration im großen Maßstab ist IPSec ALG für Abonnenten im 192.0.2.0/24-Netzwerk aktiviert. Das IPSec-ALG-Profil IPSECALGPROFILE-1 mit verschiedenen IPSec-Timeout-Einstellungen wird erstellt und ist an die LSN-Gruppe LSN Group -1 gebunden.

Beispielkonfiguration:

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.9

Done

add lsn appsprofile LSN-APPSPROFILE-1 UDP -ippooling PAIRED

Done

bind lsn appsprofile LSN-APPSPROFILE-1 500

Done

add ipsecalg profile  IPSECALGPROFILE-1 -ikeSessionTimeout 45  -
   espSessionTimeout 40  - espGateTimeout 20 -connfailover ENABLED

Done

bind lsn group LSN-GROUP-1 -appsprofilename LSN-APPSPROFILE-1

```



```
Done

bind lsn group LSN-GROUP-1 -poolname LSN-POOL-1

Done

bind lsn group LSN-GROUP-1 - ipsecAlgProfile IPSECALGPROFILE-1

Done
<!--NeedCopy-->
```

Protokollieren und Überwachen von LSN

May 11, 2023

Sie können LSN-Informationen protokollieren, um Probleme zu diagnostizieren, zu beheben und gesetzliche Anforderungen zu erfüllen. Sie können die Leistung der LSN-Funktion überwachen, indem Sie die statistischen LSN-Zähler verwenden und aktuelle LSN-Sitzungen anzeigen.

LSN protokollieren

Die Protokollierung von LSN-Informationen ist eine der wichtigen Funktionen, die die ISPs benötigen, um die gesetzlichen Anforderungen zu erfüllen und die Quelle des Datenverkehrs zu einem bestimmten Zeitpunkt zu identifizieren.

Eine NetScaler-Appliance protokolliert LSN-Zuordnungseinträge und die LSN-Sitzungen, die für jede LSN-Gruppe erstellt oder gelöscht wurden. Sie können die Protokollierung von LSN-Informationen für eine LSN-Gruppe steuern, indem Sie die Protokollierungs- und Sitzungsprotokollierungsparameter der LSN-Gruppe verwenden. Dies sind Parameter auf Gruppenebene und sind standardmäßig deaktiviert. Die NetScaler-Appliance protokolliert LSN-Sitzungen für eine LSN-Gruppe nur, wenn sowohl die Protokollierungs- als auch die Sitzungsprotokollierungsparameter aktiviert sind.

Die folgende Tabelle zeigt das Protokollierungsverhalten für eine LSN-Gruppe für verschiedene Einstellungen der Protokollierungs- und Sitzungsprotokollparameter.

Protokollierung	Sitzungsprotokollierung	Verhalten protokollieren
Aktiviert	Aktiviert	Protokolliert LSN-Zuordnungseinträge sowie LSN-Sitzungen.

Protokollierung	Sitzungsprotokollierung	Verhalten protokollieren
Aktiviert	Deaktiviert	Protokolliert LSN-Zuordnungseinträge, aber keine LSN-Sitzungen.
Deaktiviert	Aktiviert	Protokolliert weder Zuordnungseinträge noch LSN-Sitzungen.

Eine Protokollnachricht für einen LSN-Zuordnungseintrag besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt.
- Zeitstempel
- Art des Eintrags (MAPPING)
- Ob der LSN-Zuordnungseintrag erstellt oder gelöscht wurde
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Abhängig von den folgenden Bedingungen können Ziel-IP-Adresse, Port und Verkehrsdomänen-ID vorhanden sein:
  - Ziel-IP-Adresse und Port werden für die endpunktunabhängige Zuordnung nicht protokolliert.
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Die Ziel-IP-Adresse und der Port werden für die adressportabhängige Zuordnung protokolliert.

Eine Protokollnachricht für eine LSN-Sitzung besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt.
- Zeitstempel
- Art des Eintrags (SESSION)
- Ob die LSN-Sitzung erstellt oder entfernt wurde
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Ziel-IP-Adresse, Port und Traffic-Domain-ID

Die Appliance verwendet ihr vorhandenes Syslog- und Audit-Log-Framework, um LSN-Informationen zu protokollieren. Sie müssen die LSN-Protokollierung auf globaler Ebene aktivieren, indem Sie den

LSN-Parameter in den zugehörigen Entitäten der NSLOG-Aktion und der SYLOG-Aktion aktivieren. Wenn der Logging-Parameter aktiviert ist, generiert die NetScaler-Appliance Protokollmeldungen, die sich auf LSN-Zuordnungen und LSN-Sitzungen dieser LSN-Gruppe beziehen. Die Appliance sendet diese Protokollmeldungen dann an Server, die mit den Entitäten NSLOG-Aktion und SYSLOG-Aktion verknüpft sind.

Für die Protokollierung von LSN-Informationen empfiehlt Citrix:

- Protokollierung der LSN-Informationen auf externen Protokollservern statt auf der NetScaler-Appliance. Die Protokollierung auf externen Servern ermöglicht eine optimale Leistung, wenn die Appliance große Mengen an LSN-Protokolleinträgen erstellt (in der Größenordnung von Millionen).
- Verwenden von SYSLOG über TCP oder NSLOG. Standardmäßig verwendet SYSLOG UDP und NSLOG verwendet nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist für die Übertragung vollständiger Daten zuverlässiger als UDP.

  Hinweis:

  - Die auf der NetScaler-Appliance generierten SYSLOG werden dynamisch an die externen Protokollserver gesendet.
  - Wenn Sie SYSLOG über TCP verwenden, wenn die TCP-Verbindung ausgefallen ist oder der SYSLOG-Server ausgelastet ist, speichern die NetScaler Appliances die Protokolle im Puffer und senden die Daten, sobald die Verbindung aktiv ist.

Weitere Informationen zum Konfigurieren der Protokollierung finden Sie unter Audit-Protokollierung.

Die Konfiguration der LSN-Protokollierung umfasst die folgenden Aufgaben:

- **Konfiguration der NetScaler-Appliance für die Protokollierung.** Diese Aufgabe beinhaltet das Erstellen und Festlegen verschiedener Entitäten und Parameter der NetScaler-Appliance:
  - **Erstellen Sie eine SYSLOG- oder NSLOG-Audit-Logging-Konfiguration**. Das Erstellen einer Audit-Logging-Konfiguration umfasst die folgenden Aufgaben:
    * Erstellen Sie eine NSLOG- oder SYSLOG-Audit-Aktion und aktivieren Sie den LSN-Parameter. Prüfaktionen geben die IP-Adressen der Protokollserver an.
    * Erstellen Sie eine SYSLOG- oder NSLOG-Auditrichtlinie und binden Sie die Prüfungsaktion an die Prüfungsrichtlinie. Prüfaktionen geben die IP-Adressen der Protokollserver an. Optional können Sie die Transportmethode für Protokollnachrichten festlegen, die an die externen Protokollserver gesendet werden. Standardmäßig ist UDP ausgewählt. Sie können die Transportmethode als TCP festlegen, um einen zuverlässigen Transportmechanismus zu gewährleisten. Binden Sie die Überwachungsrichtlinie an das globale System.
    * Erstellen Sie eine SYSLOG- oder NSLOG-Auditrichtlinie und binden Sie die Prüfungsaktion an die Prüfungsrichtlinie.

    * Binden Sie die Prüfungsrichtlinie an das globale System.
      Hinweis: Für eine bestehende Audit-Logging-Konfiguration aktivieren Sie einfach den LSN-Parameter für die Protokollierung von LSN-Informationen auf dem Server, der durch die Audit-Aktion angegeben wurde.
  - **Aktivieren Sie die Protokollierungs- und Sitzungsprotokollparameter.** Aktivieren Sie die Protokollierungs- und Sitzungsprotokollparameter entweder beim Hinzufügen von LSN-Gruppen oder nachdem Sie die Gruppen erstellt haben. Die NetScaler-Appliance generiert Protokollmeldungen, die sich auf diese LSN-Gruppen beziehen, und sendet sie an den Server der Prüfaktionen, für die der LSN-Parameter aktiviert ist.
- **Konfiguration von Protokollservern.** Diese Aufgabe beinhaltet die Installation von SYSLOG- oder NSLOG-Paketen auf den gewünschten Servern. Zu dieser Aufgabe gehört auch die Angabe der NSIP-Adresse der NetScaler-Appliance in der Konfigurationsdatei von SYSLOG oder NSLOG. Durch die Angabe der NSIP-Adresse kann der Server die Protokollinformationen identifizieren, die von der NetScaler Appliance zum Speichern in einer Protokolldatei gesendet werden.

Weitere Informationen zum Konfigurieren der Protokollierung finden Sie unter Audit-Protokollierung.

SYSLOG-Konfiguration über die Befehlszeilenschnittstelle

So erstellen Sie eine SYSLOG-Serveraktion für die LSN-Protokollierung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
      <logLevel>... [-transport (TCP)] [-lsn ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

So erstellen Sie eine SYSLOG-Serverrichtlinie für die LSN-Protokollierung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add audit syslogPolicy <name> <rule> <action>
2 <!--NeedCopy-->
```

Um eine SYSLOG-Serverrichtlinie für die LSN-Protokollierung mithilfe der Befehlszeilenschnittstelle an das globale System zu binden

Geben Sie in der Befehlszeile Folgendes ein:

```
1 bind system global [<policyName> [-priority <positive_integer>]]
```



```
<!--NeedCopy-->
```

SYSLOG-Konfiguration mit dem Configuration Utility

So konfigurieren Sie eine SYSLOG-Serveraktion für die LSN-Protokollierung mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Systems** > **Auditing** > **Syslog** und fügen Sie auf der Registerkarte Server einen neuen Auditing-Server hinzu oder bearbeiten Sie einen vorhandenen Server.
2. Um die LSN-Protokollierung zu aktivieren, wählen Sie die Option **Large Scale NAT Logging** .
3. (Optional) Um SYSLOG über TCP zu aktivieren, wählen Sie die Option **TCP-Protokollierung** .

So konfigurieren Sie eine SYSLOG-Serverrichtlinie für die LSN-Protokollierung mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Systeme** > **Auditing** > **Syslog** und fügen Sie auf der Registerkarte **Richtlinien** eine neue Richtlinie hinzu oder bearbeiten Sie eine bestehende Richtlinie.

So binden Sie mithilfe des Konfigurationsdienstprogramms eine SYSLOG-Serverrichtlinie für die LSN-Protokollierung an das globale System

1. Navigieren Sie zu **Systeme** > **Auditing >**Syslog**.
2. Klicken Sie auf der Registerkarte **Richtlinien** in der Liste **Aktionen** auf **Globale Bindungen**, um die globalen Audit-Richtlinien zu binden.

NSLOG-Konfiguration über die Befehlszeilenschnittstelle

So erstellen Sie eine NSLOG-Serveraktion für die LSN-Protokollierung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel> ... [-lsn ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

So erstellen Sie eine NSLOG-Serverrichtlinie für die LSN-Protokollierung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
add audit nslogPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Um eine NSLOG-Serverrichtlinie für die LSN-Protokollierung mithilfe der Befehlszeilenschnittstelle an das globale System zu binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind system global [<policyName>]
<!--NeedCopy-->
```

NSLOG-Konfiguration mit dem Configuration Utility

So konfigurieren Sie eine NSLOG-Serveraktion für die LSN-Protokollierung mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Systems** > **Auditing** > **Nslog** und fügen Sie auf der Registerkarte **Server** einen neuen Auditing-Server hinzu oder bearbeiten Sie einen vorhandenen Server.
2. Um die LSN-Protokollierung zu aktivieren, wählen Sie die Option **Large Scale NAT Logging** .

So konfigurieren Sie eine NSLOG-Serverrichtlinie für die LSN-Protokollierung mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Systeme** > **Auditing** > **Nslog** und fügen Sie auf der Registerkarte **Richtlinien** eine neue Richtlinie hinzu oder bearbeiten Sie eine bestehende Richtlinie.

So binden Sie eine NSLOG-Serverrichtlinie für die LSN-Protokollierung mithilfe des Konfigurationsdienstprogramms an das globale System

1. Navigieren Sie zu **Systeme** > **Auditing >**Nslog**.
2. Klicken Sie auf der Registerkarte **Richtlinien** in der Liste **Aktionen** auf **Globale Bindungen**, um die globalen Audit-Richtlinien zu binden.

Beispiel

Die folgende Konfiguration spezifiziert zwei SYSLOG- und zwei NSLOG-Server zum Speichern von Protokolleinträgen einschließlich LSN-Protokollen. LSN Logging ist für die LSN-Gruppen LSN-GROUP-2 und LSN-GROUP-3 konfiguriert.

Die NetScaler-Appliance generiert Protokollmeldungen, die sich auf LSN-Zuordnungen und LSN-Sitzungen dieser LSN-Gruppen beziehen, und sendet sie an die angegebenen Protokollserver.


```
add audit syslogAction SYS-ACTION-1 198.51.101.10 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
Done
bind system global SYSLOG-POLICY-1
Done

add audit syslogAction SYS-ACTION-2 198.51.101.20 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-2 ns_true SYS-ACTION-2
Done
bind system global SYSLOG-POLICY-2
Done

add audit nslogAction NSLOG-ACTION-1 198.51.101.30 -logLevel ALL -lsn
    ENABLED
Done
add audit nslogPolicy NSLOG-POLICY-1 ns_true NSLOG-ACTION-1
Done
bind system global NSLOG-POLICY-1
Done
add audit nslogAction NSLOG-ACTION-2 198.51.101.40 -logLevel ALL -lsn
    ENABLED
Done
add audit nslogPolicy NSLOG-POLICY-2 ns_true NSLOG-ACTION-2
Done
bind system global NSLOG-POLICY-2
Done

add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-2 -logging ENABLED -
    sessionLogging ENABLED
Done
set lsn group LSN-GROUP-2  -logging ENABLED -sessionLogging ENABLED
Done
<!--NeedCopy-->
```

Die folgende Konfiguration spezifiziert die SYSLOG-Konfiguration für das Senden von Protokollnachrichten an
den externen SYSLOG-Server 192.0.2.10 mithilfe von TCP.

```
add audit syslogAction SYS-ACTION-1 192.0.2.10 -logLevel ALL -transport
    TCP
```



```
Done

add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
Done

bind system global SYSLOG-POLICY-1
Done
<!--NeedCopy-->
```

In der folgenden Tabelle werden Beispiele für LSN-Protokolleinträge der einzelnen Typen angezeigt, die auf den konfigurierten Protokollservern gespeichert sind. Diese LSN-Logeinträge werden von einer NetScaler-Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet.

Typ des LSN-Protokolleintrags	Beispiel für einen Logeintrag
Erstellung von LSN-Sitzungen	Local4.Informational 10.102.37.115 08/05/2014:09:59:48 GMT 0-PPE-0 : LSN LSN_SESSION 2581750 : SESSION CREATED Client IP:Port:TD 192.0.2.10: 15136:0, NatIP:NatPort 203.0.113.6: 6234, Destination IP:Port:TD 198.51.100.9: 80:0, Protocol: TCP
Löschen einer LSN-Sitzung	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0 : LSN LSN_SESSION 3871790 : SESSION DELETED Client IP:Port:TD 192.0.2.11: 15130:0, NatIP:NatPort 203.0.113.6: 7887, Destination IP:Port:TD 198.51.101.2:80:0, Protocol: TCP
Erstellung von LSN-Mappings	Local4.Informational 10.102.37.115 08/05/2014:09:59:47 GMT 0-PPE-0 : LSN LSN_MAPPING 2581580 : EIM CREATED Client IP:Port 192.0.2.15: 14567, NatIP:NatPort 203.0.113.5: 8214, Protocol: TCP
Löschen der LSN-Zuordnung	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0 : LSN LSN_MAPPING 3871700 : EIM DELETED Client IP:Port 192.0.3.15: 14565, NatIP:NatPort 203.0.113.11: 8217, Protocol: TCP

Minimale Protokollierung

Deterministische LSN-Konfigurationen und dynamische LSN-Konfigurationen mit Portblock reduzieren das LSN-Protokollvolumen erheblich. Für diese beiden Konfigurationstypen weist die NetScaler-Appliance einem Abonnenten eine NAT-IP-Adresse und einen Block von Ports zu. Die NetScaler-Appliance generiert zum Zeitpunkt der Zuweisung an einen Abonnenten eine Protokollnachricht für einen Portblock. Die NetScaler-Appliance generiert außerdem eine Protokollmeldung, wenn eine NAT-IP-Adresse und ein Portblock freigegeben werden. Bei einer Verbindung kann ein Abonnent nur anhand seiner zugeordneten NAT-IP-Adresse und seines Portblocks identifiziert werden. Aus diesem Grund protokolliert die NetScaler-Appliance keine erstellten oder gelöschten LSN-Sitzungen. Die Appliance protokolliert auch weder einen Zuordnungseintrag, der für eine Sitzung erstellt wurde, noch wenn der Zuordnungseintrag entfernt wird.

Die minimale Protokollierungsfunktion für deterministische LSN-Konfigurationen und dynamische LSN-Konfigurationen mit Portblock ist standardmäßig aktiviert und es ist nicht vorgesehen, sie zu deaktivieren. Mit anderen Worten, die NetScaler-Appliance führt automatisch eine minimale Protokollierung für deterministische LSN-Konfigurationen und dynamische LSN-Konfigurationen mit Portblock durch. Es ist keine Option verfügbar, um diese Funktion zu deaktivieren. Die Appliance sendet die Protokollmeldungen an alle konfigurierten Protokollserver.

Eine Lognachricht für jeden Portblock besteht aus den folgenden Informationen:

- NSIP-Adresse der NetScaler-Appliance
- Zeitstempel
- Eintragstyp als DETERMINISTIC oder PORTBLOCK
- Ob ein Portblock zugewiesen oder freigegeben ist
- Die IP-Adresse des Abonnenten und die zugewiesene NAT-IP-Adresse und der Portblock
- Name des Protokolls

Minimale Protokollierung für die deterministische LSN-Konfiguration

Stellen Sie sich ein Beispiel für eine einfache deterministische LSN-Konfiguration für vier Abonnenten mit den IP-Adressen 192.0.17.1, 192.0.17.2, 192.0.17.3 und 192.0.17.4 vor.

In dieser LSN-Konfiguration ist die Portblockgröße auf 32768 festgelegt und der LSN-NAT-IP-Adresspool hat IP-Adressen im Bereich 203.0.113.19-203.0.113.23.

```
1 add lsn client LSN-CLIENT-7
2 Done
3 bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask
     255.255.255.253
4 Done
5 add lsn pool LSN-POOL-7 -nattype DETERMINISTIC
6 Done
```



```
bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23
Done
add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
   DETERMINISTIC -portblocksize 32768
Done
bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
Done
<!--NeedCopy-->
```

Die NetScaler-Appliance weist jedem Abonnenten sequentiell aus dem LSN-NAT-IP-Pool und auf der Grundlage der festgelegten Portblockgröße eine LSN-NAT-IP-Adresse und einen Block von Ports zu. Es weist der ersten Abonnenten-IP-Adresse (192.0.17.1) der ersten NAT-IP-Adresse (203.0.113.19) den ersten Portblock (1024-33791) zu. Der nächste Portbereich wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht mehr über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock auf der nächsten NAT-IP-Adresse dem Abonnenten zugewiesen usw. Die Appliance protokolliert die NAT-IP-Adresse und den Portblock, der jedem Abonnenten zugewiesen ist.

Die NetScaler-Appliance protokolliert keine LSN-Sitzung, die für diese Abonnenten erstellt oder gelöscht wurde. Die Appliance generiert die folgenden Protokollmeldungen für die LSN-Konfiguration.

```
1) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201453 0 :  Dtrstc ALLOC Client 12.0.0.241,
   NatInfo 50.0.0.2:59904 to 60415
2) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201454 0 :  Dtrstc ALLOC Client 12.0.0.242,
   NatInfo 50.0.0.2:60416 to 60927
3) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
4) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
<!--NeedCopy-->
```

Wenn Sie die LSN-Konfiguration entfernen, werden die zugewiesene NAT-IP-Adresse und der Portblock für jeden Abonnenten freigegeben. Die Appliance protokolliert die NAT-IP-Adresse und den Block von Ports, die von jedem Abonnenten freigegeben wurden. Die Appliance generiert die folgenden Protokollmeldungen für jeden Abonnenten, wenn Sie die LSN-Konfiguration entfernen.

```
1) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201706 0 :  Dtrstc FREE Client 12.0.0.238,
   NatInfo 50.0.0.2:58368 to 58879
```



```
2) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201707 0 :  Dtrstc FREE Client 12.0.0.239,
   NatInfo 50.0.0.2:58880 to 59391
3) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201708 0 :  Dtrstc FREE Client 12.0.0.240,
   NatInfo 50.0.0.2:59392 to 59903
<!--NeedCopy-->
```

Minimale Protokollierung für dynamische LSN-Konfiguration mit Portblock

Stellen Sie sich ein Beispiel für eine einfache dynamische LSN-Konfiguration mit Portblock für jeden Teilnehmer im Netzwerk 192.0.2.0/24 vor. In dieser LSN-Konfiguration ist die Portblockgröße auf 1024 festgelegt und der LSN-NAT-IP-Adresspool hat IP-Adressen im Bereich 203.0.113.3-203.0.113.4.

```
set lsn parameter -memLimit 4000
Done
add lsn client LSN-CLIENT-1
Done
bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-1
Done
bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done
bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done
<!--NeedCopy-->
```

Die NetScaler-Appliance weist einem Abonnenten eine zufällige NAT-IP-Adresse und einen Block von Ports aus dem LSN-NAT-IP-Pool und auf der Grundlage der eingestellten Portblockgröße zu, wenn dieser zum ersten Mal eine Sitzung initiiert. Der NetScaler protokolliert die NAT-IP-Adresse und den Portblock, die diesem Abonnenten zugewiesen sind. Die Appliance protokolliert keine LSN-Sitzung, die für diesen Abonnenten erstellt oder gelöscht wurde. Wenn alle Ports (für Sitzungen verschiedener Abonnenten) aus dem dem Abonnenten zugewiesenen Portblock zugewiesen sind, weist die Appliance dem Abonnenten eine neue zufällige NAT-IP-Adresse und einen Portblock für weitere Sitzungen zu. Der NetScaler protokolliert jede NAT-IP-Adresse und jeden Portblock, die einem Abonnenten zugewiesen sind.

Die Appliance generiert die folgende Protokollmeldung, wenn der Abonnent mit der IP-Adresse 192.0.2.1 eine Sitzung initiiert. Die Protokollmeldung zeigt, dass die Appliance dem Abonnenten die NAT-IP-Adresse 203.0.113.3 und den Portblock 1024-2047 zugewiesen hat.


```
03/23/2015:00:07:12 GMT  Informational 0-PPE-3 : default LSN
   LSN_PORTBLOCK 106725793 0 :  Portblock ALLOC Client 12.0.2.72,
   NatInfo 203.0.113.3:1024 to 2047, Proto:TCP
<!--NeedCopy-->
```

Sobald keine Sitzungen mehr übrig sind, die die zugewiesene NAT-IP-Adresse und einen der Ports im zugewiesenen Portblock verwenden, werden die zugewiesene NAT-IP-Adresse und der Portblock für den Abonnenten freigegeben. Der NetScaler protokolliert, dass die NAT-IP-Adresse und der Portblock für den Abonnenten freigegeben wurden. Die Appliance generiert die folgenden Protokollmeldungen für den Abonnenten mit der IP-Adresse 192.0.2.1, wenn keine Sitzungen mehr übrig sind, die die zugewiesene NAT-IP-Adresse (203.0.113.3) und einen Port aus dem zugewiesenen Portblock (1024-2047) verwenden. Die Protokollmeldung zeigt, dass die NAT-IP-Adresse und der Portblock vom Abonnenten freigegeben wurden.

```
03/23/2015:00:11:09 GMT Informational 0-PPE-3 : default LSN
   LSN_PORTBLOCK 106814342 0 :  Portblock FREE Client 12.0.3.122,
   NatInfo 203.0.113.3: 1024 to 2047, Proto:TC
<!--NeedCopy-->
```

Load Balancing SYSLOG-Server

Die NetScaler-Appliance sendet ihre SYSLOG-Ereignisse und -Meldungen an alle konfigurierten externen Protokollserver. Dies führt zur Speicherung redundanter Nachrichten und erschwert die Überwachung für Systemadministratoren. Um dieses Problem zu beheben, bietet die NetScaler-Appliance Lastausgleichsalgorithmen, mit denen die SYSLOG-Meldungen für eine bessere Wartung und Leistung zwischen den externen Protokollservern ausgeglichen werden können. Zu den unterstützten Lastausgleichsalgorithmen gehören RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets und AuditlogHash.

Load-Balancing von SYSLOG-Servern über die Befehlszeilenschnittstelle

Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

```
add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
   SYSLOGUDP)> <port>
<!--NeedCopy-->
```

Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP und die Lastausgleichsmethode als AUDITLOGHASH an.


```
add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
    <AUDITLOGHASH>]
<!--NeedCopy-->
```

Bringen Sie den Dienst auf den virtuellen Load-Balancing-Server.

```
Bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
     <logLevel>]
<!--NeedCopy-->
```

Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

```
bind system global <policyName>
<!--NeedCopy-->
```

Lastenausgleich von SYSLOG-Servern mithilfe des Konfigurationsprogramms

1. Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   Navigieren Sie zu Traffic Management > Services, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP und die Lastausgleichsmethode als AUDITLOGHASH an.

   Navigieren Sie zu Traffic Management > Virtuelle Server, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver an den Dienst.

   Bringen Sie den Dienst auf den virtuellen Load-Balancing-Server.

   Navigieren Sie zu Traffic Management > Virtuelle Server, wählen Sie einen virtuellen Server aus und wählen Sie dann AUDITLOGHASH in der Load Balancing-Methode aus.

4. Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

   Navigieren Sie zu System > Auditing, klicken Sie auf Server und fügen Sie einen Server hinzu, indem Sie die Option LB vserver in Servers auswählen.

5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

   Navigieren Sie zu System > Syslog, klicken Sie auf Richtlinien, und fügen Sie eine SYSLOG-Richtlinie hinzu.

6. Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

   Navigieren Sie zu System > Syslog, wählen Sie eine SYSLOG-Richtlinie aus, und klicken Sie auf Aktion. Klicken Sie dann auf Globale Bindungen, und binden Sie die Richtlinie an System Global.

Beispiel:

Die folgende Konfiguration legt den Lastausgleich von SYSLOG-Meldungen zwischen den externen Protokollservern fest, wobei AUDITLOGHASH als Load-Balancing-Methode verwendet wird. Die NetScaler-Appliance generiert SYSLOG-Ereignisse und -Meldungen, die einen Lastausgleich zwischen den Diensten Service1, Service2 und Dienst 3 aufweisen.

```
add service service1 192.0.2.10 SYSLOGUDP 514
Done

add service service2 192.0.2.11 SYSLOGUDP 514
Done

add service service3 192.0.2.11 SYSLOGUDP 514
Done

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
Done

bind lb vserver lbvserver1 service1
Done

bind lb vserver lbvserver1 service2
Done

bind lb vserver lbvserver1 service3
Done

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
Done

```



```
add syslogpolicy syspol1 ns_true sysaction1
Done

bind system global syspol1
Done
<!--NeedCopy-->
```

Loggen von HTTP-Header-Informationen

Die NetScaler-Appliance kann jetzt Anforderungsheaderinformationen einer HTTP-Verbindung protokollieren, die die LSN-Funktionalität von NetScaler verwendet. Die folgenden Header-Informationen eines HTTP-Anforderungspakets können protokolliert werden:

- URL, für die die HTTP-Anfrage bestimmt ist.
- In der HTTP-Anfrage angegebene HTTP-Methode.
- In der HTTP-Anfrage verwendete HTTP-Version.
- IP-Adresse des Abonnenten, der die HTTP-Anfrage gesendet hat.

Die HTTP-Header-Logs können von ISPs verwendet werden, um die Trends im Zusammenhang mit dem HTTP-Protokoll bei einer Gruppe von Abonnenten zu verfolgen. Ein ISP kann diese Funktion beispielsweise verwenden, um die beliebtesten Websites unter einer Gruppe von Abonnenten herauszufinden.

Ein HTTP-Header-Logprofil ist eine Sammlung von HTTP-Header-Attributen (z. B. URL und HTTP-Methode), die für die Protokollierung aktiviert oder deaktiviert werden können. Das HTTP-Header-Logprofil ist dann an eine LSN-Gruppe gebunden. Die NetScaler-Appliance protokolliert dann HTTP-Header-Attribute, die im gebundenen HTTP-Header-Logprofil für die Protokollierung aktiviert sind, aller HTTP-Anfragen, die sich auf die LSN-Gruppe beziehen. Die Appliance sendet dann die Protokollmeldungen an die konfigurierten Protokollserver.

Ein HTTP-Header-Logprofil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein HTTP-Header-Logprofil haben.

HTTP-Header-Logprofil mithilfe der Befehlszeilenschnittstelle erstellen

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```


HTTP-Header-Logprofil mithilfe der Befehlszeilenschnittstelle an eine LSN-Gruppe binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Beispiel

Im folgenden Beispiel einer LSN-Konfiguration ist das HTTP-Header-Logprofil HTTP-Header-Log-1 an die LSN-Gruppe LSN-GROUP-1 gebunden. Im Protokollprofil sind alle HTTP-Attribute (URL, HTTP-Methode, HTTP-Version und HOST-IP-Adresse) für die Protokollierung aktiviert, sodass all diese Attribute für alle HTTP-Anfragen von Abonnenten (im Netzwerk 192.0.2.0/24) protokolliert werden, die sich auf die LSN-Gruppe beziehen.

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done

set lsn parameter -memLimit 4000
Done

add lsn client LSN-CLIENT-1
Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done

add lsn pool LSN-POOL-1
Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done

bind lsn group  LSN-GROUP-1  -httphdrlogprofilename HTTP-HEADER-LOG-1
Done
<!--NeedCopy-->
```


Der NetScaler generiert die folgende HTTP-Header-Lognachricht, wenn einer der Abonnenten, die zum LSN-Konfigurationsbeispiel gehören, eine HTTP-Anfrage sendet.

Die Lognachricht teilt uns mit, dass ein Client mit der IP-Adresse 192.0.2.33 eine HTTP-Anfrage an die URL example.com sendet, indem er die HTTP-Methode GET und die HTTP-Version 1.1 verwendet.

```
1 03/19/2015:16:24:04 GMT  Informational 0-PPE-1 : default LSN Message 59
      0 :  "LSN Client IP:TD 10.102.37.118:0 URL: example.com Host:
     192.0.2.33 Version: HTTP1.1 Method: GET"
2 <!--NeedCopy-->
```

Protokollieren von MSISDN-Informationen

Eine Mobile Station Integrated Subscriber Directory Number (MSISDN) ist eine Telefonnummer, die einen Teilnehmer in mehreren Mobilfunknetzen eindeutig identifiziert. Die MSISDN ist mit einer Landesvorwahl und einer nationalen Zielvorwahl verknüpft, die den Betreiber des Abonnenten identifizieren.

Sie können eine NetScaler-Appliance so konfigurieren, dass MSISDNS in die LSN-Protokolleinträge für Abonnenten in Mobilfunknetzen aufgenommen wird. Das Vorhandensein von MSISDNS in den LSN-Protokollen hilft dem Administrator bei der schnelleren und genaueren Rückverfolgung eines Mobilfunkabonnenten, der gegen eine Richtlinie oder ein Gesetz verstoßen hat oder dessen Informationen von rechtmäßigen Abhörbehörden benötigt werden.

Die folgenden LSN-Beispielprotokolleinträge enthalten MSISDN-Informationen für eine Verbindung von einem mobilen Abonnenten in einer LSN-Konfiguration. Die Protokolleinträge zeigen, dass ein Mobilfunkteilnehmer, dessen MSISDN E 164:5556543210 ist, über die NAT-IP:Port 203.0.113. 3:45195 mit Ziel-IP:Port 23.0.0. 1:80 verbunden war.

Art des Protokolleintrags	Beispiel für einen Logeintrag
Erstellung von LSN-Sitzungen	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : default LSN LSN_SESSION 25012 0 : SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP

Art des Protokolleintrags	Beispiel für einen Logeintrag
Erstellung von LSN-Mappings	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
Löschen einer LSN-Sitzung	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : default LSN LSN_SESSION 25012 0 : SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
LSN-Zuordnung	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP

Führen Sie die folgenden Aufgaben aus, um MSISDN-Informationen in die LSN-Protokolle aufzunehmen

- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den Log-Abonnenten-ID-Parameter, der angibt, ob die MSISDN-Informationen in die LSN-Protokolle einer LSN-Konfiguration aufgenommen werden sollen oder nicht. Aktivieren Sie den Parameter Log-Abonnenten-ID, wenn Sie das LSN-Protokollprofil erstellen.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter Protokollprofilname auf den erstellten LSN-Protokollprofilnamen festlegen. Anweisungen zum Konfigurieren von Large Scale NAT finden Sie unter Konfigurationsschritte für LSN.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn logprofile <logprofilename -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

LSN-Protokollprofil mithilfe der CLI an eine LSN-Gruppe einer LSN-Konfiguration binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Beispielkonfiguration:

In diesem Beispiel einer LSN-Konfiguration ist für das LSN-Protokollprofil der Parameter Log-Abonnenten-ID aktiviert. Das Profil ist an die LSN-Gruppe LSN-GROUP-9 gebunden. MSISDN-Informationen sind in den LSN-Sitzungs- und LSN-Zuordnungsprotokollen für Verbindungen von Mobilfunkteilnehmern enthalten (im Netzwerk 192.0.2.0/24).

```
add lsn logprofile  LOG-PROFILE-MSISDN-9   -logSubscriberID ENABLED

Done
add lsn client LSN-CLIENT-9

Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done
add lsn pool LSN-POOL-9

Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done
```



```
bind lsn group  LSN-GROUP-9  -logprofilename LOG-PROFILE-MSISDN-9

Done
<!--NeedCopy-->
```

Aktuelle LSN-Sitzungen anzeigen

Sie können die aktuellen LSN-Sitzungen anzeigen, um unerwünschte oder ineffiziente LSN-Sitzungen auf der NetScaler-Appliance zu erkennen. Sie können alle oder einige LSN-Sitzungen auf der Grundlage von Auswahlparametern anzeigen.

Hinweis: Wenn auf der NetScaler-Appliance mehr als eine Million LSN-Sitzungen vorhanden sind, empfiehlt Citrix, mithilfe der Auswahlparameter ausgewählte LSN-Sitzungen anzuzeigen und nicht alle.

Konfiguration über die Befehlszeilenschnittstelle

Um alle LSN-Sitzungen mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
show lsn session
<!--NeedCopy-->
```

So zeigen Sie ausgewählte LSN-Sitzungen mithilfe der Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:

```
show lsn session [-clientname <string>] [-network <ip_addr> [-netmask <
    netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]
<!--NeedCopy-->
```

Beispiel

Um alle auf einem NetScaler vorhandenen LSN-Sitzungen anzuzeigen


```
> show lsn session
          SubscrIP             SubscrPort      SubscrTD              DstIP                      DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10               15136           0               198.51.100.9            80              0       203.0.113.6     6234            TCP     OUT
2.      192.0.2.11               15130           0               198.51.101.2            80              0       203.0.113.6     7887            TCP     OUT
3.      192.0.2.12               16136           0               198.51.100.3            80              0       203.0.113.6     9807            TCP     OUT
4.      192.0.2.13               18148           0               198.51.101.6            80              0       203.0.113.6     4657            TCP     OUT
5.      192.0.2.14               13560           0               198.51.101.7            80              0       203.0.113.7     9341            TCP     OUT
6.      192.0.2.15               14567           0               198.51.100.8            80              0       203.0.113.5     8214            TCP     OUT
7.      192.0.2.15               16890           0               198.51.101.1            80              0       203.0.113.5     8214            TCP     OUT
8.      192.0.2.16               12345           0               198.51.102.9            80              0       203.0.113.5     1678            TCP     OUT
9.      192.0.2.19               19876           0               198.51.103.8            80              0       203.0.113.5     1567            TCP     OUT
10.     192.0.2.20               10989           0               198.51.104.19           80              0       203.0.113.11    1343            TCP     OUT
11.     192.0.3.13               18149           0               198.51.101.61           80              0       203.0.113.11    4653            TCP     OUT
12.     192.0.3.14               13510           0               198.51.101.74           80              0       203.0.113.11    9344            TCP     OUT
13.     192.0.3.15               14565           0               198.51.100.82           80              0       203.0.113.11    8217            TCP     OUT
14.     192.0.3.15               16899           0               198.51.101.12           80              0       203.0.113.11    8219            TCP     OUT
15.     192.0.3.16               12343           0               198.51.102.99           80              0       203.0.113.11    1673            TCP     OUT

Done
```

Um alle LSN-Sitzungen anzuzeigen, die sich auf eine LSN-Client-Entität beziehen LSN-CLIENT-2

```
> show lsn session -clientname LSN-CLIENT-2
        SubscrIP               SubscrPort      SubscrTD              DstIP                    DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10               15136           0               198.51.100.9            80              0       203.0.113.6     68234           TCP     OUT
2.      192.0.2.11               15130           0               198.51.101.2            80              0       203.0.113.6     7887            TCP     OUT
3.      192.0.2.12               16136           0               198.51.100.3            80              0       203.0.113.6     9807            TCP     OUT
4.      192.0.2.13               18148           0               198.51.101.6            80              0       203.0.113.6     4657            TCP     OUT
5.      192.0.2.14               13560           0               198.51.101.7            80              0       203.0.113.7     9341            TCP     OUT
6.      192.0.2.15               14567           0               198.51.100.8            80              0       203.0.113.5     8214            TCP     OUT
7.      192.0.2.15               16890           0               198.51.101.1            80              0       203.0.113.5     8214            TCP     OUT
8.      192.0.2.16               12345           0               198.51.102.9            80              0       203.0.113.5     1678            TCP     OUT
9.      192.0.2.19               19876           0               198.51.103.8            80              0       203.0.113.5     1567            TCP     OUT
10.     192.0.2.20               10989           0               198.51.104.19           80              0       203.0.113.11    1343            TCP     OUT

Done
```

Um alle LSN-Sitzungen anzuzeigen, die 203.0.113.5 als NAT-IP-Adresse verwenden

```
> show lsn session –natIP 203.0.113.5
SubscrIP               SubscrPort      SubscrTD        DstIP                   DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.15               14567           0               198.51.100.8            80              0       203.0.113.5     8214            TCP     OUT
2.      192.0.2.15               16890           0               198.51.101.1            80              0       203.0.113.5     8214            TCP     OUT
3.      192.0.2.16               12345           0               198.51.102.9            80              0       203.0.113.5     1678            TCP     OUT
4.      192.0.2.19               19876           0               198.51.103.8            80              0       203.0.113.5     1567            TCP     OUT
Done
```

Konfiguration mit dem Configuration Utility

So zeigen Sie alle oder ausgewählte LSN-Sitzungen mithilfe des Konfigurationsdienstprogramms an

1. Navigieren Sie zu System > Large Scale NAT > Sessions und klicken Sie auf die Registerkarte NAT44.
2. Um LSN-Sitzungen auf der Grundlage von Auswahlparametern anzuzeigen, klicken Sie auf Suchen.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- LSN-Sitzung anzeigen
  - clientname

    Name der LSN-Client-Entität. Maximale Länge: 127

- network

  IP-Adresse oder Netzwerkadresse des/der Abonnenten.

- Netzmaske

  Subnetzmaske für die im Netzwerkparameter angegebene IP-Adresse.

  Standardwert: 255.255.255.255

- td

  Verkehrsdomänen-ID der LSN-Client-Entität.

  Standardwert: 0

  Mindestwert: 0

  maximaler Wert: 4094

- Antip

  Zugeordnete NAT-IP-Adresse, die in LSN-Sitzungen verwendet wird.

LSN-Statistiken anzeigen

Sie können Statistiken zur LSN-Funktion anzeigen, um die Leistung der LSN-Funktion zu bewerten oder Probleme zu beheben. Sie können eine Zusammenfassung der Statistiken der LSN-Funktion oder einer bestimmten LSN-Gruppe anzeigen. Die statistischen Zähler geben Ereignisse seit dem letzten Neustart der NetScaler-Appliance wieder. Alle diese Zähler werden auf 0 zurückgesetzt, wenn die NetScaler-Appliance neu gestartet wird.

Um alle LSN-Statistiken mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat lsn
<!--NeedCopy-->
```

Um Statistiken für eine angegebene LSN-Gruppe mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat lsn group [<groupname>]
<!--NeedCopy-->
```


Beispiel

```
> stat lsn

Large Scale NAT statistics
                                                    Rate(/s)
                                                       Total
LSN TCP Received Packets                                 0
    40
LSN TCP Received Bytes                                   0
    3026
LSN TCP Transmitted Packets                              0
    40
LSN TCP Transmitted Bytes                                0
    3026
LSN TCP Dropped Packets                                  0
                        0
LSN TCP Current Sessions                                 0
                        0
LSN UDP Received Packets                                 0
                        0
LSN UDP Received Bytes                                   0
                        0
LSN UDP Transmitted Packets                              0
                        0
LSN UDP Transmitted Bytes                                0
                        0
LSN UDP Dropped Packets                                  0
                        0
LSN UDP Current Sessions                                 0
                        0
LSN ICMP Received Packets                                0
    982
LSN ICMP Received Bytes                                  0
    96236
LSN ICMP Transmitted Packets                             0
                        0
LSN ICMP Transmitted Bytes                               0
                        0
LSN ICMP Dropped Packets                                 0
    982
LSN ICMP Current Sessions                                0
                        0
LSN Subscribers                                          0
                        1
```



```
24
25 Done
26
27 > stat lsn group LSN-GROUP-1
28
29 LSN Group Statistics
30                                                  Rate (/s)
                                                       Total
31 TCP Translated Pkts                                0
       40
32 TCP Translated Bytes                               0
       3026
33 TCP Dropped Pkts                                   0
                          0
34 TCP Current Sessions                               0
                          0
35 UDP Translated Pkts                                0
                          0
36 UDP Translated Bytes                               0
                          0
37 UDP Dropped Pkts                                   0
                          0
38 UDP Current Sessions                               0
                          0
39 ICMP Translated Pkts                               0
                          0
40 ICMP Translated Bytes                              0
                          0
41 ICMP Dropped Pkts                                  0
                          0
42 ICMP Current Sessions                              0
                          0
43 Current Subscribers                                0
                          1
44
45 Done
46 <!--NeedCopy-->
```

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- starte lsn group
  - Gruppenname

    Name der LSN-Gruppe. Maximale Länge: 127

- Detail

  Gibt eine detaillierte Ausgabe an (einschließlich weiterer Statistiken). Die Ausgabe kann sehr umfangreich sein. Ohne dieses Argument wird in der Ausgabe nur eine Zusammenfassung angezeigt.

- Vollständige Werte

  Gibt an, dass Zahlen und Zeichenketten in ihrer vollen Form angezeigt werden sollen. Ohne diese Option werden lange Zeichenketten gekürzt und große Zahlen abgekürzt.

- n-mal

  Gibt an, wie oft die Statistik in Intervallen von sieben Sekunden angezeigt werden soll.

  Standardwert: 1

- Log-Datei

  Der Name der Logdatei, die als Eingabe verwendet werden soll.

- Statistiken löschen

  Löschen Sie die Statistiken/Zähler

  Mögliche Werte: basic, full

Kompaktes Logging

Die Protokollierung von LSN-Informationen ist eine der wichtigen Funktionen, die ISPs benötigen, um die gesetzlichen Anforderungen zu erfüllen und die Quelle des Datenverkehrs jederzeit identifizieren zu können. Dies führt letztendlich zu einer riesigen Menge an Protokolldaten, sodass die ISPs große Investitionen tätigen müssen, um die Protokollierungsinfrastruktur aufrechtzuerhalten.

Compact Logging ist eine Technik zur Reduzierung der Protokollgröße, indem eine Notationsänderung verwendet wird, bei der Kurzcodes für Ereignis- und Protokollnamen verwendet werden. Zum Beispiel C für Client, SC für Sitzung erstellt und T für TCP. Die kompakte Protokollierung führt zu einer durchschnittlichen Reduzierung der Protokollgröße um 40 Prozent.

Die folgenden Beispiele für Logeinträge zur Erstellung von NAT44-Mappings zeigen den Vorteil der kompakten Protokollierung.

|-|-|
|Default logging format|02/02/2016:01:13:01 GMT Informational 0-PPE-2 : default LSN LSN_ADDRPORT_MAPPING 85 0 : A&PDM CREATED ClientIP:Port:TD1.1.1.1:6500:0,NatIP:NatPort8.8.8.8:47902, DestinationIP:Port:TD2.2.2.2:80:0, Protocol: TCP|
|Compact logging format|02/02/2016:01:14:57 GMT Info 0-PE2:default LSN 87 0:A&PDMC|C-1.1.1.1:6500:0|N-8.8.8.9:51066|D-2.2.2.2:80:0|T|

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um LSN-Informationen im Kompaktformat zu protokollieren:

- **Erstellen Sie ein LSN-Protokollprofil.** Ein LSN-Protokollprofil enthält den Parameter Log Compact, der angibt, ob Informationen für eine LSN-Konfiguration im kompakten Format protokolliert werden sollen oder nicht.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration.** Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter Log-Profilname auf den Namen des erstellten LSN-Protokollprofils setzen. Alle Sitzungen und Zuordnungen für diese LSN-Gruppe werden im kompakten Format protokolliert.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

LSN-Protokollprofil mithilfe der CLI an eine LSN-Gruppe einer LSN-Konfiguration binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Beispielkonfiguration:

```
add lsn logprofile  LOG-PROFILE-COMPACT-9 -logCompact ENABLED

Done
add lsn client LSN-CLIENT-9
Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-9
Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
```



```
Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
Done
bind lsn group  LSN-GROUP-9  - logProfileName LOG-PROFILE-COMPACT-9
Done
<!--NeedCopy-->
```

IPFIX-Protokollierung

Die NetScaler-Appliance unterstützt das Senden von Informationen über LSN-Ereignisse im IPFIX-Format (Internet Protocol Flow Information Export) an den konfigurierten Satz von IPFIX Collector (s). Die Appliance verwendet die vorhandene AppFlow-Funktion, um LSN-Ereignisse im IPFIX-Format an die IPFIX-Collectors zu senden.

IPFIX-basierte Protokollierung ist für die folgenden groß angelegten NAT44-Ereignisse verfügbar:

- Erstellen oder Löschen einer LSN-Sitzung.
- Erstellung oder Löschung eines LSN-Mapping-Eintrags.
- Zuweisung oder Entzuweisung von Portblöcken im Kontext von deterministischem NAT.
- Zuweisung oder Entzuweisung von Portblöcken im Kontext von dynamischem NAT.
- Immer wenn das Kontingent für Abonnentensitzungen überschritten wird.

Punkte, die Sie beachten sollten, bevor Sie die IPFIX-Protokollierung konfigurieren

Bevor Sie mit der Konfiguration von IPSec ALG beginnen, sollten Sie die folgenden Punkte berücksichtigen:

- Sie müssen die AppFlow Funktion und die IPFIX-Kollektoren auf der NetScaler Appliance konfigurieren. Anweisungen finden Sie im Thema Konfiguration der AppFlow-Funktion.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um LSN-Informationen im IPFIX-Format zu protokollieren:

- **Aktivieren Sie die LSN-Protokollierung in der AppFlow-Konfiguration**. Aktivieren Sie den LSN-Logging-Parameter als Teil der AppFlow-Konfiguration.
- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den IPFIX-Parameter, der die Protokollinformationen im IPFIX-Format aktiviert oder deaktiviert.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das LSN-Protokollprofil an eine oder mehrere LSN-Gruppe (n). Ereignisse, die sich auf die gebundene LSN-Gruppe beziehen, werden im IPFIX-Format protokolliert.

So aktivieren Sie die LSN-Protokollierung in der AppFlow-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Protokollprofil mithilfe der CLI in der Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie das LSN-Protokollprofil mithilfe der CLI an eine LSN-Gruppe einer LSN-Konfiguration

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Protokollprofil mithilfe der GUI

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf die Registerkarte **Protokoll** und fügen Sie dann ein Protokollprofil hinzu.

So binden Sie das LSN-Protokollprofil mithilfe der GUI an eine LSN-Gruppe einer LSN-Konfiguration

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group und** öffnen Sie die **LSN-Gruppe** .
2. Klicken Sie **unter Erweiterte Einstellungen** auf **+ Protokollprofil**, um das erstellte Protokollprofil an die LSN-Gruppe zu binden.

TCP-SYN Leerlauf-Timeout

May 11, 2023

Das SYN-Idle-Timeout ist das Timeout für den Aufbau von TCP-Verbindungen, die LSN auf der NetScaler-Appliance verwenden. Wenn innerhalb des konfigurierten Timeout-Zeitraums keine TCP-Sitzung eingerichtet wird, entfernt der NetScaler die Sitzung. Der SYN-Idle-Timeout ist nützlich, um Schutz vor SYN-Flood-Angriffen zu bieten. In einer LSN-Konfiguration enthält die LSN-Gruppenentität die SYN-Einstellung für das Leerlaufzeitlimit.

Beispiel:

In der folgenden LSN-Beispielkonfiguration ist das SYN-Idle-Timeout für TCP-Verbindungen, die sich auf Abonnenten aus dem 192.0.2.0/24-Netzwerk beziehen, auf 30 Sekunden festgelegt.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  - synidletimeout 30

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done
<!--NeedCopy-->
```


Überschreiben der LSN-Konfiguration mit Load Balancing-Konfiguration

May 11, 2023

Eine LSN-Konfiguration hat standardmäßig Vorrang vor jeder Load-Balancing-Konfiguration. Um die LSN-Konfiguration (Large Scale Networking) durch die Load-Balancing-Konfiguration für den Datenverkehr zu überschreiben, der beiden Konfigurationen entspricht, erstellen Sie ein Netzprofil, bei dem der Parameter LSN überschreiben aktiviert ist, und binden Sie dieses Profil an den virtuellen Server der Load-Balancing-Konfiguration. Die USNIP- oder USIP-Einstellungen der Load-Balancing-Konfiguration werden auf den Datenverkehr angewendet, anstatt die LSN-IP-Adresse der LSN-Konfiguration anzuwenden.

Diese Option ist nützlich in einer LSN-Bereitstellung, die NetScaler-Appliances und Mehrwertdienste wie Firewall- und Optimierungsgeräte umfasst. Bei dieser Art der Bereitstellung muss der eingehende Datenverkehr auf der NetScaler-Appliance diese Mehrwertdienste durchlaufen, bevor eine LSN-Konfiguration auf der Appliance auf den Datenverkehr angewendet wird. Damit die NetScaler-Appliance den eingehenden Datenverkehr an einen Mehrwertdienst senden kann, wird eine Load-Balancing-Konfiguration erstellt und das Override-LSN auf der Appliance aktiviert. Die Load-Balancing-Konfiguration umfasst Mehrwertdienste, die als Load Balancing-Dienste dargestellt werden und an einen virtuellen Server vom Typ ANY gebunden sind. Der virtuelle Server ist mit Listening-Richtlinien konfiguriert, um den Datenverkehr zu identifizieren, der an den Mehrwertdienst gesendet werden soll.

Um das Überschreiben von lsn in einem Netzprofil mithilfe der CLI zu aktivieren

Um Override lsn beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie in der Befehlszeile Folgendes ein

```
add netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Um Override lsn beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie in der Befehlszeile Folgendes ein

```
set netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
```



```
<!--NeedCopy-->
```

Um das Überschreiben von lsn in einem Netzprofil mithilfe der GUI zu aktivieren

1. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile**.
2. Stellen Sie den Parameter **Override LSN ein**, während Sie Netzprofile hinzufügen oder ändern.

In der folgenden Beispielkonfiguration ist für das Netzprofil NETPROFILE-OVERRIDELSN-1 die Option zum Überschreiben von LSN aktiviert und es ist an den virtuellen Lastausgleichsserver LBVS-1 gebunden.

Beispielkonfiguration:

```
add netprofile NETPROFILE-OVERRIDELSN-1 -overrideLsn ENABLED

Done

set lb vserver LBVS-1 -netprofile NETPROFILE-OVERRIDELSN-1

Done
<!--NeedCopy-->
```

LSN-Sitzungen löschen

May 11, 2023

Sie können alle unerwünschten oder ineffizienten LSN-Sitzungen aus der NetScaler-Appliance entfernen. Die Appliance gibt sofort die für diese Sitzungen zugewiesenen Ressourcen (wie NAT-IP-Adresse, Port und Speicher) frei, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance verwirft auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte LSN-Sitzungen von der NetScaler-Appliance entfernen.

So löschen Sie alle LSN-Sitzungen mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session

show lsn session
<!--NeedCopy-->
```


So löschen Sie ausgewählte LSN-Sitzungen mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session [-clientname <string>] [-network <ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <port>]]

show lsn session
<!--NeedCopy-->
```

Beispiel

Löschen Sie alle auf einem NetScaler vorhandenen LSN-Sitzungen

```
flush lsn session

Done
<!--NeedCopy-->
```

Löscht alle LSN-Sitzungen, die sich auf die LSN-Client-Entität LSN-CLIENT-1 beziehen

```
flush lsn session -clientname LSN-CLIENT-1

Done
<!--NeedCopy-->
```

Löscht alle LSN-Sitzungen, die sich auf ein Abonnentennetzwerk (192.0.2.0) der LSN-Client-Entität LSN-CLIENT-2 beziehen, die zur Verkehrsdomäne 100 gehört

```
flush lsn session -clientname LSN-CLIENT-2 -network 192.0.2.0 -netmask 255.255.255.0 -td 100

Done
<!--NeedCopy-->
```

So löschen Sie alle LSN-Sitzungen mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu System > Large Scale NAT > Sessions und klicken Sie auf Flush Sessions.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- Linsenspülung

- clientname

  Name der LSN-Client-Entität. Maximale Länge: 127

- network

  IP-Adresse oder Netzwerkadresse des/der Abonnenten.

- Netzmaske

  Subnetzmaske für die im Netzwerkparameter angegebene IP-Adresse.

  Standardwert: 255.255.255.255

- td

  Verkehrsdomänen-ID der LSN-Client-Entität.

  Standardwert: 0

  Mindestwert: 0

  maximaler Wert: 4094

- Antip

  Zugeordnete NAT-IP-Adresse, die in LSN-Sitzungen verwendet wird.

- NAT-Anschluss

  Zugeordneter NAT-Port, der in den LSN-Sitzungen verwendet wird.

Load Balancing SYSLOG-Server

May 11, 2023

Die NetScaler-Appliance sendet ihre SYSLOG-Ereignisse und -Meldungen an alle konfigurierten externen Protokollserver. Dies führt zur Speicherung redundanter Nachrichten und erschwert die Überwachung für Systemadministratoren. Um dieses Problem zu beheben, bietet die NetScaler-Appliance Lastausgleichsalgorithmen, mit denen die SYSLOG-Meldungen für eine bessere Wartung und Leistung zwischen den externen Protokollservern ausgeglichen werden können. Zu den unterstützten Lastausgleichsalgorithmen gehören RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets und AuditlogHash.

Load-Balancing von SYSLOG-Servern über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.


```
add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
    SYSLOGUDP)> <port>
<!--NeedCopy-->
```

Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP und die Lastausgleichsmethode als AUDITLOGHASH an.

```
add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
    <AUDITLOGHASH>]
<!--NeedCopy-->
```

Binden Sie den Dienst an den virtuellen Lastausgleichsserver.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

1. Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
<!--NeedCopy-->
```

Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

```
bind system global <policyName>
<!--NeedCopy-->
```

Lastenausgleich von SYSLOG-Servern mithilfe des Konfigurationsprogramms

1. Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   Navigieren Sie zu Traffic Management > Services, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP und die Lastausgleichsmethode als AUDITLOGHASH an.

   Navigieren Sie zu Traffic Management > Virtuelle Server, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver an den Dienst.

   Bringen Sie den Dienst auf den virtuellen Load-Balancing-Server.

   Navigieren Sie zu Traffic Management > Virtuelle Server, wählen Sie einen virtuellen Server aus und wählen Sie dann AUDITLOGHASH in der Load Balancing-Methode aus.

4. Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

   Navigieren Sie zu System > Auditing, klicken Sie auf Server und fügen Sie einen Server hinzu, indem Sie die Option LB vserver in Servers auswählen.

5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

   Navigieren Sie zu System > Syslog, klicken Sie auf Richtlinien, und fügen Sie eine SYSLOG-Richtlinie hinzu.

6. Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

   Navigieren Sie zu System > Syslog, wählen Sie eine SYSLOG-Richtlinie aus, und klicken Sie auf Aktion. Klicken Sie dann auf Globale Bindungen, und binden Sie die Richtlinie an System Global.

Beispiel:

Die folgende Konfiguration legt den Lastausgleich von SYSLOG-Meldungen zwischen den externen Protokollservern fest, wobei AUDITLOGHASH als Load-Balancing-Methode verwendet wird. Die NetScaler-Appliance generiert SYSLOG-Ereignisse und -Meldungen, die einen Lastausgleich zwischen den Diensten Service1, Service2 und Dienst 3 aufweisen.

```
add service service1 192.0.2.10 SYSLOGUDP 514

add service service2 192.0.2.11 SYSLOGUDP 514

add service service3 192.0.2.11 SYSLOGUDP 514

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH

bind lb vserver lbvserver1 service1

bind lb vserver lbvserver1 service2

bind lb vserver lbvserver1 service3

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All

add syslogpolicy syspol1 ns_true sysaction1

bind system global syspol1
```



```
<!--NeedCopy-->
```

Einschränkungen:

Die NetScaler-Appliance unterstützt keinen externen Lastenausgleich des virtuellen Servers, der die SYSLOG-Nachrichten zwischen den Protokollservern ausgleicht.

Port Control Protocol

May 11, 2023

NetScaler-Appliances unterstützen jetzt das Port Control Protocol (PCP) für Large Scale NAT (LSN). Viele der Abonnentenanwendungen eines Internetdienstanbieters müssen über das Internet zugänglich sein (z. B. IoT-Geräte (Internet of Things), wie z. B. eine IP-Kamera, die die Überwachung über das Internet ermöglicht). Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, statische großskalige NAT-Karten (LSN) zu erstellen. Für eine sehr große Anzahl von Abonnenten ist die Erstellung statischer LSN-NAT-Maps jedoch keine praktikable Lösung.

Das Port Control Protocol (PCP) ermöglicht es einem Abonnenten, spezifische LSN-NAT-Zuordnungen für sich selbst und/oder für andere Geräte von Drittanbietern anzufordern. Das große NAT-Gerät erstellt eine LSN-Map und sendet sie an den Abonnenten. Der Abonnent sendet den Remote-Geräten im Internet die NAT-IP-Adresse: NAT-Port, an dem sie sich mit dem Abonnenten verbinden können.

Anwendungen senden in der Regel häufig Keep-Alive-Nachrichten an das große NAT-Gerät, damit ihre LSN-Zuordnungen nicht zu einem Timeout führen. PCP trägt dazu bei, die Häufigkeit solcher Keep-Alive-Nachrichten zu reduzieren, indem es den Anwendungen ermöglicht, die Timeout-Einstellungen der LSN-Zuordnungen zu erlernen. Dies trägt dazu bei, den Bandbreitenverbrauch im Zugangsnetz des ISP und den Batterieverbrauch auf Mobilgeräten zu reduzieren.

PCP ist ein Client-Server-Modell und läuft über das UDP-Transportprotokoll. Eine NetScaler-Appliance implementiert die PCP-Serverkomponente und entspricht RFC 6887.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben zur Konfiguration von PCP aus:

- (Optional) Erstellen Sie ein PCP-Profil. Ein PCP-Profil enthält Einstellungen für PCP-bezogene Parameter (z. B. um auf Mapping- und Peer-PCP-Anfragen zu warten). Ein PCP-Profil kann an einen PCP-Server gebunden werden. Ein an einen PCP-Server gebundenes PCP-Profil wendet alle seine Einstellungen auf den PCP-Server an. Ein PCP-Profil kann an mehrere PCP-Server gebunden werden. Standardmäßig ist ein PCP-Profil mit Standardparametereinstellungen an alle PCP-Server gebunden. Ein PCP-Profil, das Sie an einen PCP-Server binden, überschreibt

die standardmäßigen PCP-Profileinstellungen für diesen Server. Ein Standard-PCP-Profil hat die folgenden Parametereinstellungen:
  - Zuordnung: Aktiviert
  - Peer: Aktiviert
  - Minimale Lebensdauer der Karte: 120 Sekunden
  - Maximale Lebensdauer: 86400 Sekunden
  - Anzahl ankündigen: 10
  - Drittanbieter: Deaktiviert
- Erstellen Sie einen PCP-Server und binden Sie ein PCP-Profil daran. Erstellen Sie einen PCP-Server auf der NetScaler-Appliance, um auf PCP-bezogene Anfragen und Nachrichten der Abonnenten zu warten. Um darauf zugreifen zu können, muss einem PCP-Server eine Subnetz-IP-Adresse (SNIP) zugewiesen werden. Standardmäßig überwacht ein PCP-Server Port 5351.
- Binden Sie den PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration. Binden Sie den erstellten PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den PCP-Serverparameter so festlegen, dass der erstellte PCP-Server angegeben wird. Auf den erstellten PCP-Server können nur die Abonnenten dieser LSN-Gruppe zugreifen.

> **Hinweis**
>
> Ein PCP-Server für eine umfangreiche NAT-Konfiguration bedient keine Anfragen von Abonnenten, die anhand der ACL-Regeln identifiziert werden.

So erstellen Sie ein PCP-Profil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

So erstellen Sie einen PCP-Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
```



```
<!--NeedCopy-->
```

Beispielkonfiguration für NAT44

In der folgenden Beispielkonfiguration ist der PCP-Server PCP-SERVER-9 mit Standard-PCP-Einstellungen an die LSN-Gruppe LSN-GROUP-9 gebunden. PCP-SERVER-9 bedient PCP-Anfragen von Abonnenten im Netzwerk 192.0.2.0/24.

Beispielkonfiguration:

```
add pcp server PCP-SERVER-9 192.0.3.9

Done

add lsn client LSN-CLIENT-9

Done

bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-9

Done

bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done

add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done

bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done

bind lsn group  LSN-GROUP-9  -pcpServer PCP-SERVER-9

Done
<!--NeedCopy-->
```


LSN44 in einem Cluster-Setup

May 11, 2023

Große NAT44-Konfigurationen werden in einem NetScaler-Cluster-Setup unterstützt.

Ein NetScaler-Cluster ist eine Gruppe von NetScaler-Appliances, die als ein einzelnes System konfiguriert und verwaltet werden. Ein NetScaler-Cluster bietet Skalierbarkeit und Verfügbarkeit. Jede NetScaler-Appliance in einem Cluster-Setup fungiert als unabhängige LSN-Entität und wird als einzelnes System verwaltet.

Die LSN-Konfiguration in einem Cluster-Setup ist dieselbe wie in einer eigenständigen Appliance, außer dass ein bestimmter Pool von LSN-IP-Adressen jeweils nur einem Knoten gehört. Mit anderen Worten, eine LSN-IP-Pool-Entität ist als Spott-Entität in einem bestimmten Knoten konfiguriert. Alle Knoten eines Cluster-Setups können eine bestimmte LSN-IP-Pool-Entität haben. Um sicherzustellen, dass die Pakete, die sich auf eine LSN-Sitzung beziehen, auf demselben Clusterknoten empfangen werden, der den NAT-Vorgang ausgeführt hat, ist Policy Based Backplane (PBS) Steering konfiguriert. PBS leitet die empfangenen zugehörigen Pakete einer LSN-Sitzung an denselben Clusterknoten weiter.

Beispielkonfiguration:

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 -ownerNode 1 203.0.113.3

Done

bind lsn pool LSN-POOL-1 -ownerNode 2 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done
```



```
24
25 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
26
27 Done
28
29 add ns acl b1 ALLOW -srcIP = 192.0.2.0-192.0.2.255 -type DFD -dfdhash
      SIP
30
31
32 Done
33
34 apply ns acls -type DFD
35
36 Done
37 <!--NeedCopy-->
```

Dual-Stack Lite

September 1, 2023

> **Hinweis:**
>
> Die Dual-Stack Lite-Funktion ist ab Version NetScaler 14.1 veraltet.
>
> Veraltete Funktionen werden nicht sofort entfernt. Die NetScaler Appliance unterstützt die veraltete Funktion weiterhin, bis sie in einer zukünftigen Version entfernt wird.

Aufgrund des Mangels an IPv4-Adressen und der Vorteile von IPv6 gegenüber IPv4 haben viele ISPs begonnen, auf eine IPv6-Infrastruktur umzustellen. Während der Umstellung müssen ISPs jedoch weiterhin IPv4 zusammen mit IPv6 unterstützen, da der Großteil des öffentlichen Internets immer noch nur IPv4 verwendet und viele Abonnenten IPv6 nicht unterstützen.

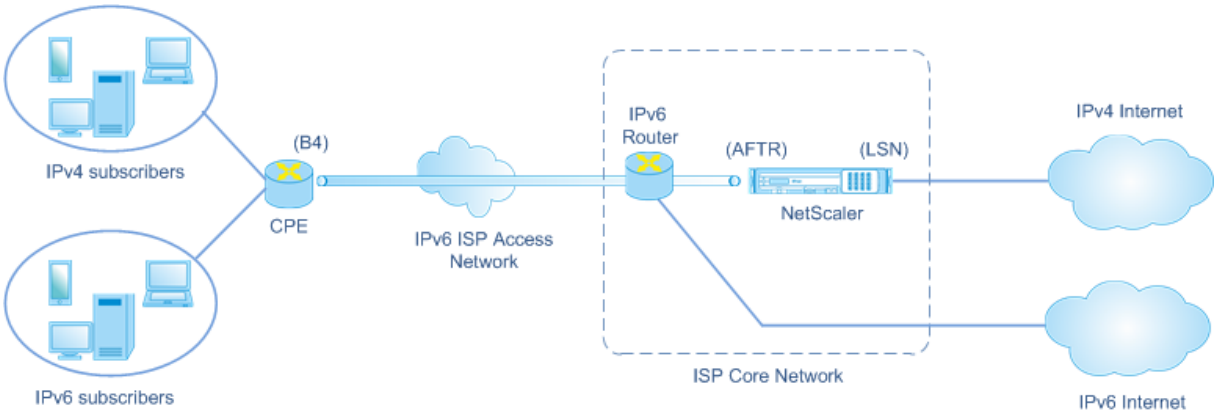
Dual Stack Lite (DS-Lite) ist eine IPv6-Übergangslösung für ISPs mit IPv6-Infrastruktur, um ihre IPv4-Abonnenten mit dem Internet zu verbinden. DS-Lite verwendet IPv4-in-IPv6-Tunneling, um das IPv4-Paket eines Abonnenten durch einen Tunnel im IPv6-Zugangsnetzwerk an den ISP zu senden. Das IPv6-Paket wird entkapselt, um das IPv4-Paket des Abonnenten wiederherzustellen, und wird dann nach der NAT-Adress- und Portübersetzung und anderer LSN-bezogener Verarbeitung an das Internet gesendet. Die Antwortpakete durchqueren denselben Pfad zum Abonnenten.

Die NetScaler-Appliance implementiert die AFTR-Komponente einer DS-Lite-Bereitstellung und entspricht RFC 6333.

Architektur

Die Dual-Stack Lite-Architektur für einen ISP besteht aus den folgenden Komponenten:

- **Basic Bridging-Breitband (B4).** Basic Bridging Broadband (B4) ist ein Gerät oder eine Komponente, die sich in den Räumlichkeiten des Abonnenten befindet. In der Regel ist B4 eine Komponente der CPE-Geräte in den Räumlichkeiten des Abonnenten. IPv4-Abonnenten sind über das CPE-Gerät, das die B4-Komponente enthält, mit dem reinen IPv6-ISP-Zugangsnetzwerk verbunden. Die Hauptfunktion des B4 besteht darin, einen IPv6-Tunnel zwischen B4 und einem Address Family Transition Router (AFTR) zu initiieren, um IPv4-Anfrage- oder Antwortpakete von Abonnenten über den Tunnel zu senden oder zu empfangen. B4 enthält eine IPv6-Adresse, die als B4-Tunnel-Endpunktadresse bekannt ist. B4 verwendet diese Adresse, um IPv6-Pakete an AFTR zu beziehen und Pakete von AFTR zu empfangen.
- **Adressiere den Family Transition Router (AFTR).** AFTR ist ein Gerät oder eine Komponente, die sich im Kernnetzwerk des ISP befindet. AFTR beendet den IPv6-Tunnel vom B4-Gerät aus. Mit anderen Worten, der IPv6-Tunnel wird zwischen B4 im Teilnehmergebäude und AFTR im ISP-Kernnetz gebildet. AFTR entkapselt von B4 empfangene IPv6-Pakete, um die ursprünglichen IPv4-Pakete der Abonnenten wiederherzustellen. AFTR sendet die IPv4-Pakete an das LSN-Gerät oder die LSN-Komponente. LSN leitet die IPv4-Pakete an ihr Ziel weiter, nachdem es die NAT-Adresse- und Portübersetzung (NAT 44) und andere LSN-bezogene Verarbeitungen durchgeführt hat. AFTR enthält eine IPv6-Adresse, die als AFTR-Tunnel-Endpunktadresse bekannt ist. AFTR verwendet diese Adresse, um IPv6-Pakete an B4 zu senden und IPv6-Pakete von B4 zu empfangen. Die NetScaler-Appliance implementiert die AFTR-Komponente.
- **Softwire.** Der zwischen B4 und AFTR erstellte IPv6-Tunnel wird als Softwire bezeichnet.



Die DS-Lite-Architektur eines ISP, der eine NetScaler-Appliance verwendet, besteht aus Abonnenten in privaten Adressräumen, die über eine NetScaler-Appliance, die im Kernnetzwerk des ISP bereitgestellt wird, auf das Internet zugreifen. IPv4-Abonnenten sind mit einem CPE-Gerät verbunden, das die DS-Lite B4-Funktionalität enthält. Das CPE-Gerät ist über das reine IPv6-Zugangsnetzwerk des ISP mit dem ISP-Kernnetzwerk verbunden. Die NetScaler-Appliance enthält die DS-Lite AFTR- und LSN-Funktionalität.

IPv4-Abonnenten, die mit dem CPE-Gerät verbunden sind, erhalten private IPv4-Adressen entweder manuell oder über einen DHCP-Server, der auf dem CPE-Gerät ausgeführt wird. Auf dem CPE-Gerät wird die AFTR-Tunnel-Endpunktadresse manuell oder über DHCPv6 angegeben. Die Konfiguration von CPE-Geräten ist herstellerspezifisch und fällt daher nicht in den Rahmen dieser Dokumentation.

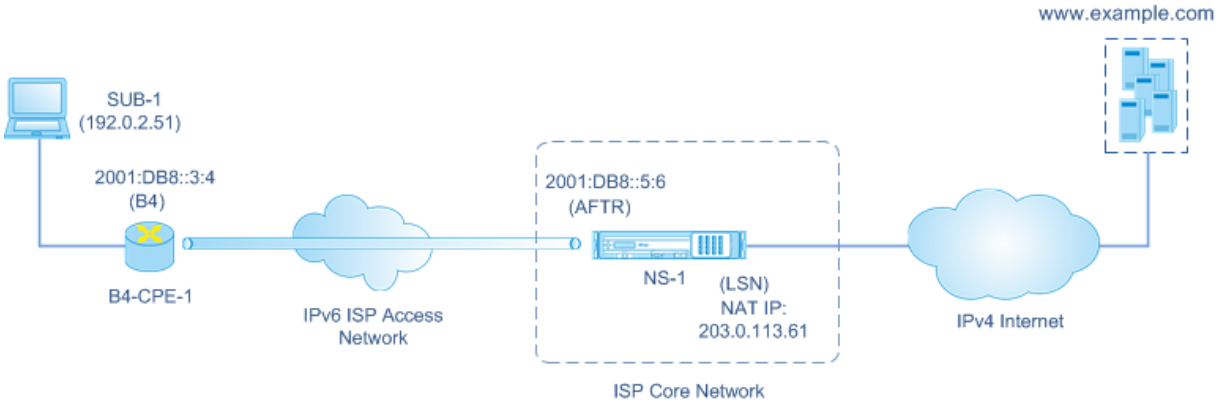
Beim Empfang eines Anforderungspakets, das von einem IPv4-Abonnenten stammt und für einen Standort im Internet bestimmt ist, kapselt die B4-Komponente des CPE-Geräts das IPv4-Paket in ein IPv6-Paket und sendet es an die NetScaler-Appliance im ISP-Kernnetzwerk. Die AFTR-Funktionalität der NetScaler-Appliance entkapselt das IPv6-Paket, um das ursprüngliche IPv4-Paket des Abonnenten wiederherzustellen. Die LSN-Funktionalität der NetScaler-Appliance übersetzt die Quell-IP-Adresse und den Port des IPv4-Pakets in eine NAT-IP-Adresse und einen NAT-Port, die aus dem konfigurierten NAT-Pool ausgewählt wurden, und sendet das Paket dann an sein Ziel im Internet.

Die Appliance zeichnet alle aktiven Sitzungen auf, die die AFTR- und LSN-Funktionen verwenden. Diese Sitzungen werden DS-Lite-Sitzungen genannt. Die NetScaler-Appliance verwaltet auch die Zuordnungen zwischen B4-IPv6-Adresse, Abonnenten-IPv4-Adresse und Port sowie NAT-IPv4-Adresse und Port für jede DS-Lite-Sitzung. Diese Zuordnungen werden als DS-Lite-LSN-Mappings bezeichnet. Anhand von DS-Lite-Sitzungseinträgen und DS-Lite-LSN-Zuordnungseinträgen erkennt die NetScaler-Appliance ein (aus dem Internet empfangenes) Antwortpaket als Teil einer bestimmten DS-Lite-Sitzung.

Wenn die NetScaler-Appliance ein Antwortpaket empfängt, das zu einer bestimmten DS-Lite-Sitzung gehört, übersetzt die LSN-Funktionalität der Appliance die Ziel-IP-Adresse und den Port des Antwortpakets von der NAT-IP-Adresse und dem Port in die IP-Adresse und den Port des Abonnenten. Die AFTR-Funktion kapselt das resultierende Paket in ein IPv6-Paket und sendet es an das CPE-Gerät. Die B4-Funktionalität des CPE-Geräts entkapselt das IPv6-Paket, um das IPv4-Antwortpaket wiederherzustellen, und sendet dann das IPv4-Paket an den Abonnenten.

Beispiel

Stellen Sie sich ein Beispiel für eine DS-Lite-Bereitstellung vor, die aus NetScaler NS-1 im Kernnetzwerk eines ISP, dem CPE-Gerät B4-CPE-1 in einem Abonnentengebäude und einem einzelnen IPv4-Abonnenten SUB-1 besteht. B4-CPE-1 unterstützt die B4-Funktionalität der DS-Lite-Funktion.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
IPv4-Adresse des Abonnenten SUB-1		192.0.2.51
IPv6-Adresse des Softwire-Endpunkts auf dem B4-Gerät (B4-CPE-1)		2001:DB8::3:4
IPv6-Adresse des Softwire-Endpunkts auf dem AFTR-Gerät (NS-1)		2001:DB8::5:6

Einstellungen auf der NetScaler-Appliance NS-1:

Entität	Name	Details
LSN-Client	LSN-DSLITE-CLIENT-1	Network6 (Identifizierung von Datenverkehr von B4-Geräten) = 2001:DB8:: 3:0 /100
LSN-Pool	LSN-DSLITE-POOL-1	LSN-IP-Adressen (NAT-IP) = 203.0.113.61 - 203.0.113.70
IPv6-Profil	LSN-DSLITE-PROFILE-1	Typ = DS-LITE; IPv6-Adresse (AFTR-IPv6-Adresse) = Eine der NetScaler-eigenen IPv6-Adressen vom Typ SNIP6 = 2001:DB8:: 5:6

Entität	Name	Details
LSN-Gruppe	LSN-DSLITE-GROUP-1	LSN-Client = LSN-DSLITE-CLIENT-1; LSN-Pool = LSN-DSLITE-POOL-1; IPv6-Profil = LSN-DSLITE-PROFILE-1

Es folgt der Verkehrsfluss in diesem Beispiel:

1. Der IPv4-Abonnent SUB-1 sendet eine Anfrage an ()http://www.example.com/. Das IPv4-Paket hat:
    - Quell-IP-Adresse = 192.0.2.51
    - Quellport = 2552
    - Ziel-IP-Adresse = 198.51.100.250
    - Zielport = 80
2. Nach Empfang des IPv4-Anforderungspakets kapselt B4-CPE-1 es in die Payload eines IPv6-Pakets ein und sendet das IPv6-Paket dann an NS-1. Das IPv6-Paket hat:
    - Quell-IP-Adresse = 2001:DB8:: 3:4
    - Ziel-IP-Adresse = 2001:DB8:: 5:6
3. Wenn NS-1 das IPv6-Paket empfängt, entkapselt das AFTR-Modul das Paket, indem es die IPv6-Header entfernt. Das resultierende Paket ist das ursprüngliche IPv4-Anforderungspaket von SUB-1.
4. Das LSN-Modul von NS-1 übersetzt die Quell-IP-Adresse und den Port des Pakets in eine NAT-IP-Adresse und einen NAT-Port, die aus dem konfigurierten NAT-Pool ausgewählt wurden. Das übersetzte IPv4-Paket hat:
    - Quell-IP-Adresse = 203.0.113.61
    - Quellport = 3002
    - Ziel-IP-Adresse = 198.51.100.250
    - Zielport = 80
5. Das LSN-Modul erstellt auch eine LSN-Zuordnung und einen Sitzungseintrag für diese DS Lite-Sitzung. Das Mapping enthält die folgenden Informationen:
    - Quell-IP-Adresse des IPv6-Pakets (IPv6-Adresse von B4-CPE-1) = 2001:DB8:: 3:4
    - Quell-IP-Adresse des IPv4-Pakets (IPv4-Adresse von SUB-1) = 192.0.2.51
    - Quellport des IPv4-Pakets = 2552
    - NAT-IP-Adresse = 203.0.113.61

- NAT-Anschluss = 3002

6. NS-1 sendet das resultierende IPv4-Paket an sein Ziel im Internet.
7. Der Server für www.example.com verarbeitet das Anforderungspaket und sendet ein Antwortpaket. Das IPv4-Antwortpaket enthält:
   - Quell-IP-Adresse = 198.51.100.250
   - Quellport = 80
   - Ziel-IP-Adresse = 203.0.113.61
   - Zielport = 3002
8. Nach Empfang des IPv4-Pakets untersucht NS-1 die LSN-Zuordnung und die Sitzungseinträge und stellt fest, dass das IPv4-Antwortpaket zu einer DS Lite-Sitzung gehört. Das LSN-Modul von NS-1 übersetzt die Ziel-IP-Adresse und den Port. Das IPv4-Paket hat jetzt:
   - Quell-IP-Adresse = 198.51.100.250
   - Quellport = 80
   - Ziel-IP-Adresse = 192.0.2.51
   - Zielport = 2552
9. Das AFTR-Modul von NS-1 kapselt das IPv4-Paket in ein IPv6-Paket und sendet das IPv6-Paket dann an B4-CPE-1. Das IPv6-Paket hat:
   - Quell-IP-Adresse = 2001:DB8: :5:6
   - Ziel-IP-Adresse = 2001:DB8:: 3:4
10. Nach Erhalt des Pakets entkapselt B4-CPE-1 das IPv6-Paket, indem die IPv6-Header entfernt werden, und sendet dann das resultierende IPv4-Paket an CL-1.

Punkte, die vor der Konfiguration von DS-Lite zu beachten sind

May 11, 2023

Beachten Sie die folgenden Punkte, bevor Sie DS-Lite auf einer NetScaler-Appliance konfigurieren:

1. Sie müssen die verschiedenen Komponenten von DS-Lite verstehen, die in RFC 6333 beschrieben werden.
2. Eine DS-Lite-Konfiguration auf einer NetScaler-Appliance verwendet die LSN-Befehlssätze. In einer DS-Lite-Konfiguration gibt die LSN-Client-Entität die IPv6-Adresse oder IPv6-Netzwerkadresse oder ACL6-Regeln für die Identifizierung des Datenverkehrs vom B4-Gerät an. Eine DS-Lite-Konfiguration enthält auch ein IPv6-Profil, das die IPv6-Adressen-AFTR-Komponente auf einer NetScaler Appliance angibt. Weitere Informationen zur NetScaler LSN-Funktion finden Sie unter Large Scale NAT.

3. Bei einer DS-Lite-Konfiguration unterstützt die NetScaler Appliance LSN für IPv4-Pakete, die nur zu einem der folgenden Protokolle gehören. Die NetScaler-Appliance löscht IPv4-Pakete, die zu anderen Protokollen gehören:
    - TCP
    - UDP
    - ICMP
4. Die NetScaler-Appliance unterstützt die folgenden ALGs DS-Lite:
    - ICMP
    - FTP
    - TFTP
    - Sitzungsinitiierungsprotokoll (SIP)
    - Echtzeit-Streaming-Protokoll (RTSP)

Konfigurieren von DS-Lite

May 11, 2023

Eine DS-Lite-Konfiguration auf einer NetScaler-Appliance verwendet die LSN-Befehlssätze. In einer DS-Lite-Konfiguration gibt die LSN-Client-Entität die IPv6-Adresse oder IPv6-Netzwerkadresse oder ACL6-Regeln für die Identifizierung des Datenverkehrs vom B4-Gerät an. Weitere Informationen zur NetScaler LSN-Funktion finden Sie unter Large Scale NAT. Eine DS-Lite-Konfiguration enthält auch ein IPv6-Profil, das die IPv6-Adresse (vom Typ SNIP6) der DS-Lite-AFTR-Komponente auf einer NetScaler Appliance angibt.

Die Konfiguration von DS-Lite auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- **Stellen Sie die globalen LSN-Parameter ein.** Zu den globalen Parametern gehören die Menge des NetScaler-Speichers, der für die LSN-Funktion reserviert ist, und die Synchronisation von LSN-Sitzungen in einem Hochverfügbarkeits-Setup.
- **Erstellen Sie eine LSN-Client-Entität zur Identifizierung des Datenverkehrs von B4-CPE-Geräten**. Die LSN-Client-Entität bezieht sich auf eine Reihe von DS-Lite B4-Geräten. Die Client-Entität enthält IPv6-Adressen oder IPv6-Netzwerkadressen oder ACL6-Regeln zur Identifizierung des Datenverkehrs von diesen B4-Geräten. Ein LSN-Client kann nur an eine LSN-Gruppe gebunden werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen einer LSN-Client-Entität und zum Binden eines Abonnenten an die LSN-Client-Entität. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.
- **Erstellen Sie einen LSN-Pool und binden Sie NAT-IP-Adressen daran**. Ein LSN-Pool definiert einen Pool von NAT-IP-Adressen, die von der NetScaler-Appliance zur Ausführung von LSN

verwendet werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen eines LSN-Pool und zum Binden von NAT-IP-Adressen an den LSN-Pool. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.

- **Erstellen Sie ein LSN IP6-Profil.** Ein LSN-IP6-Profil definiert die IPv6-Adresse der DS-Lite AFTR-Komponente auf der NetScaler-Appliance. Die IPv6-Adresse muss eine der NetScaler-eigenen IPv6-Adressen des Typs SNIP6 sein.
- **(Optional) Erstellen Sie ein LSN-Transportprofil für ein bestimmtes Protokoll**. Ein LSN-Transportprofil definiert verschiedene Timeouts und Limits, z. B. die maximale LSN-Sitzung und die maximale Portauslastung, die ein Abonnent für ein bestimmtes Protokoll haben kann. Sie binden ein LSN-Transportprofil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes Profil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für die Protokolle TCP, UDP und ICMP bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standard-Transportprofil bezeichnet. Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das Standard-LSN-Transportprofil für dieses Protokoll.
- **(Optional) Erstellen Sie ein LSN-Anwendungsprofil für ein bestimmtes Protokoll und binden Sie eine Reihe von Zielports daran**. Ein LSN-Anwendungsprofil definiert die LSN-Zuordnung und die LSN-Filterung einer Gruppe für ein bestimmtes Protokoll und für eine Reihe von Zielports. Für eine Reihe von Zielports binden Sie ein LSN-Profil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes LSN-Anwendungsprofil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für die TCP-, UDP- und ICMP-Protokolle für alle Zielports bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardanwendungsprofil bezeichnet. Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen eines LSN-Anwendungsprofils und zum Binden einer Reihe von Zielports an das LSN-Anwendungsprofil. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.
- **Erstellen Sie eine LSN-Gruppe und binden Sie LSN-Pools, LSN-IPv6-Profile, (optional) LSN-Transportprofile und (optional) LSN-Anwendungsprofile an die LSN-Gruppe**. Eine LSN-Gruppe ist eine Entität, die aus einem LSN-Client, einem LSN-IPv6-Profil, LSN-Pool (n), LSN-Transportprofilen und LSN-Anwendungsprofilen (en) besteht. Einer Gruppe werden Parameter wie die Portblockgröße und die Protokollierung von LSN-Sitzungen zugewiesen. Die Parametereinstellungen gelten für alle Abonnenten eines LSN-Clients, der an die LSN-Gruppe

gebunden ist. Nur ein LSN-IPv6-Profil kann an eine LSN-Gruppe gebunden werden, und ein an eine LSN-Gruppe gebundenes LSN-IPv6-Profil kann nicht an andere LSN-Gruppen gebunden werden. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Nur eine LSN-Client-Entität kann an eine LSN-Gruppe gebunden werden, und eine LSN-Client-Entität, die an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen einer LSN-Gruppe und zum Binden von LSN-Pools, LSN-Transportprofilen und LSN-Anwendungsprofilen an die LSN-Gruppe. Das Konfigurationsprogramm kombiniert diese beiden Operationen in einem einzigen Bildschirm.

Konfiguration über die Befehlszeile

Um einen LSN-Client mithilfe der Befehlszeilenschnittstelle zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

Um ein IPv6-Netzwerk oder eine ACL6-Regel mithilfe der Befehlszeilenschnittstelle an einen LSN-Client zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
    string>)

show lsn client
<!--NeedCopy-->
```

Um einen LSN-Pool mithilfe der Befehlszeilenschnittstelle zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn pool <poolname> [-nattype ( DYNAMIC )] [-portblockallocation (
    ENABLED | DISABLED )] [-portrealloctimeout <secs>] [-
    maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

Um einen IP-Adressbereich mithilfe der Befehlszeilenschnittstelle an einen LSN-Pool zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Hinweis: Verwenden Sie zum Entfernen von LSN-IP-Adressen aus einem LSN-Pool den Befehl unbind lsn pool.

So konfigurieren Sie ein LSN-IPv6-Profil mithilfe der Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn ip6profile <name>  -type DS-Lite  -network6 < ipv6_addr|*s >

show lsn ip6profile
<!--NeedCopy-->
```

Um ein LSN-Transportprofil mithilfe der Befehlszeilenschnittstelle zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

Um ein LSN-Anwendungsprofil mithilfe der Befehlszeilenschnittstelle zu erstellen, gehen Sie wie folgt vor:

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```

Um einen Portbereich für das Anwendungsprotokoll mithilfe der Befehlszeilenschnittstelle an ein LSN-Anwendungsprofil zu binden:

Geben Sie in der Befehlszeile Folgendes ein:


```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

So erstellen Sie eine LSN-Gruppe mithilfe der Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC )]
    [-portblocksize <positive_integer>] [-logging (ENABLED | DISABLED )]
     [-sessionLogging ( ENABLED | DISABLED )][-sessionSync ( ENABLED |
    DISABLED )] [-snmptraplimit<positive_integer>] [-ftp ( ENABLED |
    DISABLED )] [-pptp ( ENABLED |DISABLED )] [-sipalg ( ENABLED |
    DISABLED )] [-rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

show lsn group
<!--NeedCopy-->
```

So binden Sie LSN-Protokollprofile und LSN-Pools mithilfe der Befehlszeilenschnittstelle an eine LSN-Gruppe:

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Konfiguration mit dem Configuration Utility

Um einen LSN-Client zu konfigurieren und eine IPv6-Netzwerkadresse oder eine ACL6-Regel zu binden, verwenden Sie das Konfigurationsprogramm:

Navigieren Sie zu **System** > **Large Scale NAT** > **Clients**, fügen Sie einen Client hinzu und binden Sie dann eine IPv6-Netzwerkadresse oder eine ACL6-Regel an den Client.

So konfigurieren Sie einen LSN-Pool und binden NAT-IP-Adressen mithilfe des Konfigurations-dienstprogramms:

Navigieren Sie zu **System** > **Large Scale NAT** > **Pools**, fügen Sie einen Pool hinzu und binden Sie dann eine NAT-IP-Adresse oder einen Bereich von NAT-IP-Adressen an den Pool.

So konfigurieren Sie ein LSN-IPv6-Profil mithilfe des Konfigurationsdienstprogramms:

Navigieren Sie zu **System** > **Large Scale NAT** > **Profiles**, klicken Sie auf die Registerkarte **IPv6** und weisen Sie DS-Lite AFTR eine IPv6-Adresse zu.

So konfigurieren Sie ein LSN-Transportprofil mithilfe des Konfigurationsdienstprogramms:

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**.
2. Klicken Sie im Detailbereich auf **Transport**, und fügen Sie dann ein Transportprofil hinzu.

So konfigurieren Sie ein LSN-Anwendungsprofil mithilfe des Konfigurationsdienstprogramms:

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**.
2. Klicken Sie im Detailbereich auf **Anwendung**und fügen Sie dann ein Anwendungsprofil hinzu.

Um eine LSN-Gruppe zu konfigurieren und einen LSN-Client, ein LSN-IPv6-Profil, Pools, Transportprofile und Anwendungsprofile zu binden, verwenden Sie das Konfigurationsdienstprogramm:

Navigieren Sie zu **System** > **Large Scale NAT** > **Groups**, fügen Sie eine Gruppe hinzu und binden Sie dann einen LSN-Client, ein LSN-IPv6-Profil, Pools, Transportprofile und Anwendungsprofile an die Gruppe.

```
> add lsn client LSN-DSLITE-CLIENT-1
Done
> bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
> add lsn pool LSN-DSLITE-POOL-1
Done
> bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
> add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6
Done
> add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1
Done
> add lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
Done
```

Protokollierung und Überwachung DS-Lite

Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die NetScaler Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie

zum Konfigurieren der DS-Lite-Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (MAPPING)
- Ob der DS-Lite LSN-Mapping-Eintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Abhängig von den folgenden Bedingungen können Ziel-IP-Adresse, Port und Verkehrsdomänen-ID vorhanden sein:
  - Ziel-IP-Adresse und Port werden für die endpunktunabhängige Zuordnung nicht protokolliert.
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Die Ziel-IP-Adresse und der Port werden für die adressportabhängige Zuordnung protokolliert.

Eine Lognachricht für eine DS-Lite-Sitzung besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Ziel-IP-Adresse, Port und Traffic-Domain-ID

Die folgende Tabelle zeigt Beispiele für DS-Lite-Protokolleinträge der einzelnen Typen, die auf den konfigurierten Protokollservern gespeichert sind. Diese Protokolleinträge werden von einer NetScaler-Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet. Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die NetScaler Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie zum Konfigurieren der DS-Lite-

Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (MAPPING)
- Ob der DS-Lite LSN-Mapping-Eintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Abhängig von den folgenden Bedingungen können Ziel-IP-Adresse, Port und Verkehrsdomänen-ID vorhanden sein:
  - Ziel-IP-Adresse und Port werden für die endpunktunabhängige Zuordnung nicht protokolliert.
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Die Ziel-IP-Adresse und der Port werden für die adressportabhängige Zuordnung protokolliert.

Eine Lognachricht für eine DS-Lite-Sitzung besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Ziel-IP-Adresse, Port und Traffic-Domain-ID

Die folgende Tabelle zeigt Beispiele für DS-Lite-Protokolleinträge der einzelnen Typen, die auf den konfigurierten Protokollservern gespeichert sind. Diese Protokolleinträge werden von einer NetScaler-Appliance generiert, deren NSIP-Adresse 10.102.37.115 ist.

Typ des LSN-Protokolleintrags	Beispiel für einen Logeintrag
DS-Lite-Sitzungserstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1 : default LSN LSN_SESSION 37647607 0 : SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP
Löschen einer DS-Lite-Sitzung	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1 : default LSN LSN_SESSION 37647617 0 : SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP
DS-Lite LSN-Mapping-Erstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647610 0 : EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP
Löschen der DS-Lite-LSN-Zuordnung	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647618 0 : EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Aktuelle DS-Lite-Sessions anzeigen

Sie können die aktuellen DS-Lite-Sitzungen anzeigen, um unerwünschte oder ineffiziente Sitzungen auf der NetScaler-Appliance zu erkennen. Sie können alle oder einige DS-Lite-Sitzungen auf der Grundlage von Auswahlparametern anzeigen.

Konfiguration mithilfe der Befehlszeilenschnittstelle

Um alle DS-Lite-Sessions mithilfe der Befehlszeilenschnittstelle anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

```
show lsn session  -nattype DS-Lite
<!--NeedCopy-->
```

Um ausgewählte DS-Lite-Sitzungen mithilfe der Befehlszeilenschnittstelle anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

```
show lsn session  -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Beispiel:

In der folgenden Beispielausgabe werden alle DS-Lite-Sitzungen angezeigt, die auf einer NetScaler-Appliance vorhanden sind:

```
show lsn session  -nattype DS-Lite
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1.  2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2.  2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3.  2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4.  2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT

Done
<!--NeedCopy-->
```

Konfiguration mit dem Configuration Utility

Um alle oder ausgewählte DS-Lite-Sessions mithilfe des Konfigurationsdienstprogramms anzuzeigen

1. **Navigieren Sie zu System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die Registerkarte **DS-Lite** .
2. **Um DS-Lite-Sitzungen auf der Grundlage von Auswahlparametern anzuzeigen, klicken Sie auf Suchen.**

DS-Lite-Sitzungen löschen

Sie können alle unerwünschten oder ineffizienten DS-Lite-Sitzungen aus der NetScaler-Appliance entfernen. Die Appliance gibt sofort die für diese Sitzungen zugewiesenen Ressourcen (wie NAT-IP-Adresse, Port und Speicher) frei, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance verwirft auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte DS-Lite-Sitzungen von der NetScaler-Appliance entfernen.

Um alle DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle zu löschen:

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session -nattype DS-Lite
show lsn session -nattype DS-Lite
```

Um ausgewählte DS-Lite-Sitzungen mithilfe der Befehlszeilenschnittstelle zu löschen:

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session  - nattype DS-Lite
<!--NeedCopy-->
```

Um alle oder ausgewählte DS-Lite-Sitzungen mit dem Konfigurationsprogramm zu löschen:

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die **Registerkarte DS-Lite** .
2. Klicken Sie auf **Sitzungen leeren**.

Konfigurieren statischer DS-Lite Maps

May 11, 2023

Die NetScaler-Appliance unterstützt die manuelle Erstellung von DS-Lite-LSN-Zuordnungen, die die Zuordnung zwischen den folgenden Informationen enthalten:

- IP-Adresse und Port des Abonnenten sowie IPv6-Adresse des B4-Geräts oder der B4-Komponente
- NAT-IP-Adresse und Port

Statische DS-Lite-LSN-Zuordnungen sind nützlich, wenn Sie sicherstellen möchten, dass die zu einer NAT-IP-Adresse und einem Port initiierten Verbindungen der IP-Adresse und dem Port des Abonnenten über das angegebene B4-Gerät zugeordnet werden (z. B. Webserver im internen Netzwerk).

Hinweis: Diese Funktion wird in Version 11.0 Build 64.x und höher unterstützt.

So erstellen Sie ein statisches DS-Lite-LSN-Mapping mithilfe der Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [-network6 <B4_ADDR>] [<natIP> [<natPort>]] [-
    destIP<ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Parameterbeschreibungen

lsn static hinzufügen

- name

Name für den statischen LSN-Mapping-Eintrag. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „ds-lite lsn static1" oder 'ds-lite lsn static1'). Dies ist ein zwingendes Argument. Maximale Länge: 127

- Transportprotokoll

Protokoll für den DS-Lite LSN-Mapping-Eintrag.

- Abonniere

IPv4-Adresse eines Abonnenten für den DS-Lite LSN-Mapping-Eintrag.

- Abonnieren

Port des Abonnenten für den DS-Lite LSN-Mapping-Eintrag.

- Network6

IPv6-Adresse des B4-Geräts oder der B4-Komponente.

- td

ID der Verkehrsdomäne, zu der das B4-Gerät gehört. Die IPv6-Adresse des B4-Geräts ist im Parameter network6 angegeben. Wenn Sie keine ID angeben, wird davon ausgegangen, dass das B4-Gerät Teil der Standard-Verkehrsdomäne ist.

- Antip

IPv4-Adresse, die bereits auf der NetScaler-Appliance als Typ LSN vorhanden ist und als NAT-IP-Adresse für diesen Zuordnungseintrag verwendet werden soll.

- NAT-Anschluss

NAT-Port für diesen DS-Lite-LSN-Mapping-Eintrag.

- DE Tip

Ziel-IP-Adresse für den DS-Lite LSN-Zuordnungseintrag.

- dsttd

ID der Verkehrsdomäne, über die die Ziel-IP-Adresse für diesen DS-Lite-LSN-Mapping-Eintrag von der NetScaler-Appliance aus erreichbar ist. Wenn Sie keine ID angeben, wird davon ausgegangen, dass die Ziel-IP-Adresse über die Standard-Verkehrsdomäne erreichbar ist, die eine ID von 0 hat.

So erstellen Sie ein statisches DS-Lite-LSN-Mapping mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu System > Large Scale NAT > Statisch, und fügen Sie eine neue statische DS-Lite-LSN-Zuordnung hinzu.

Konfigurieren der deterministischen NAT-Allokation für DS-Lite

May 11, 2023

Die deterministische NAT-Zuweisung für DS-Lite-LSN-Bereitstellungen ist eine Art der NAT-Ressourcenzuweisung, bei der die NetScaler-Appliance jedem Abonnenten (Abonnent hinter dem B4-Gerät) aus dem LSN-NAT-IP-Pool und auf der Grundlage der angegebenen Portblockgröße vorab eine LSN-NAT-IP-Adresse und einen Block von Ports zuweist.

Hinweis: Diese Funktion wird in Version 11.0 Build 64.x und höher unterstützt.

Die Appliance weist diesen Abonnenten sequentiell NAT-Ressourcen zu. Es weist den ersten Portblock auf der ersten NAT-IP-Adresse der ersten Abonnenten-IP-Adresse zu. Der nächste Portbereich wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht mehr über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock an der nächsten NAT-Adresse dem Abonnenten zugewiesen usw.

Die NetScaler-Appliance protokolliert die zugewiesene NAT-IP-Adresse und den Portblock für einen Abonnenten. Bei einer Verbindung kann ein Abonnent nur anhand seiner zugeordneten NAT-IP-Adresse und seines Portblocks identifiziert werden. Aus diesem Grund protokolliert die NetScaler-Appliance die Erstellung oder Löschung einer LSN-Sitzung nicht.

Ein DS-Lite-Abonnent kann nur einen deterministischen Portblock haben. Wenn der gesamte Portblock verwendet wird, unterbricht die NetScaler-Appliance jede neue Verbindung des Abonnenten.

Beispiel: Deterministisches DS-Lite

In diesem Beispiel umfasst eine deterministische DS-Lite-Konfiguration vier Abonnenten mit den IP-Adressen 192.0.17.5, 192.0.17.6, 192.0.17.7 und 192.0.17.8. Diese IPv4-Abonnenten stehen hinter einem B4-Gerät mit der IPv6-Adresse 2001:DB8:: 3:4 In dieser Konfiguration ist die Portblockgröße auf 20480 festgelegt und der LSN NAT-IP-Adresspool hat IP-Adressen im Bereich 203.0.113.41-203.0.113.42.

Die NetScaler-Appliance weist jedem Abonnenten sequentiell aus dem LSN-NAT-IP-Pool und auf der Grundlage der festgelegten Portblockgröße eine LSN-NAT-IP-Adresse und einen Block von Ports zu. Es weist der ersten Abonnenten-IP-Adresse (192.0.17.5) der ersten NAT-IP-Adresse (203.0.113.41) den ersten Portblock (1024-21503) zu. Der nächste Portbereich wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht mehr über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock auf der nächsten NAT-IP-Adresse dem Abonnenten zugewiesen usw. Der NetScaler protokolliert die NAT-IP-Adresse und den Portblock, der jedem Abonnenten zugewiesen ist.

Die NetScaler-Appliance protokolliert keine LSN-Sitzung, die für diese Abonnenten erstellt oder gelöscht wurde.

In der folgenden Tabelle sind die NAT-IP-Adresse und die Portblöcke aufgeführt, die jedem Abonnenten in diesem Beispiel zugewiesen wurden:

IP-Adresse des Abonnenten	Zugewiesene NAT-IP-Adresse	Zugewiesener Block von Ports	IPv6-Adresse von B4
192.0.17.5	203.0.113.41	1024 - 21503	2001:DB8::3:4
192.0.17.6	203.0.113.41	21504 - 41983	2001:DB8::3:4

192.0.17.7	203.0.113.41	41984 - 62463	2001:DB8::3:4
192.0.17.8	203.0.113.42	1024 - 21503	2001:DB8::3:4

Konfigurationsschritte

Sie müssen deterministische NAT als Teil der DS-Lite-Konfiguration konfigurieren. Anweisungen zum Konfigurieren von DS-Lite finden Sie unter Konfigurieren von DS-Lite.

Stellen Sie bei der Konfiguration von DS-Lite sicher, dass Sie:

- Stellen Sie den Parameter NAT Type auf Deterministic ein, wenn Sie den LSN-Pool und die LSN-Gruppe hinzufügen.
- Stellen Sie den gewünschten Portblockgrößenparameter ein, wenn Sie die LSN-Gruppe hinzufügen, es sei denn, Sie können den Standardwert akzeptieren.

Punkte, die vor der Konfiguration von Deterministic DS-Lite zu beachten sind

Beachten Sie die folgenden Punkte, bevor Sie deterministisches DS-Lite konfigurieren:

- Die vollständige IP-Adresse jedes Abonnenten muss in einem separaten Befehl add lsn client angegeben werden, indem die Parameter Network und Netmask festgelegt werden. (Setzen Sie Netmask auf 255.255.255.255.) Außerdem muss die im Network6-Parameter angegebene IPv4-Adresse des B4-Geräts vollständig sein (/128-Präfix). Mit anderen Worten, die Parameter Network und Network6 akzeptieren keine anderen Adressen als die /32-Bit-Maske bzw. das /128-Präfix.
- Die NetScaler-Appliance unterbricht Verbindungen von Abonnenten, die in keiner deterministischen DS-Lite-Konfiguration angegeben sind, sondern sich hinter B4-Geräten befinden, die in einer deterministischen DS-Lite-Konfiguration spezifiziert sind.
- Die NetScaler-Appliance erkennt Abonnenten mit derselben IPv4-Adresse wie verschiedene Abonnenten, wenn sie sich hinter verschiedenen B4-Geräten befinden. Eine Kombination aus Abonnenten-IPv4-Adresse und B4-Gerät definiert einen eindeutigen Abonnenten in der LSN-Client-Entität einer DS-Lite-Konfiguration.

Beispiel für eine deterministische DS-Lite-Konfiguration:

Die folgende Konfiguration verwendet die im Abschnitt Beispiel: Deterministisches DS-Lite aufgeführten Einstellungen.

```
1 add lsn client LSN-DSLITE-CLIENT-10
2
3 Done
```



```
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.5 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.6 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.7 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.8 -netmask
    255.255.255.255 -network6 2001:DB8::3:4/128

Done
add lsn pool LSN-DSLITE-POOL-10 -nattype DETERMINISTIC

Done
bind lsn pool LSN-DSLITE-POOL-10  203.0.113.41-203.0.113.42

Done
add lsn ip6profile LSN-DSLITE-PROFILE-10 -type DS-Lite -network6 2001:
    DB8::5:6

Done
add lsn group LSN-DSLITE-GROUP-10 -clientname LSN-DSLITE-CLIENT-10 -
    nattype DETERMINISTIC -portblocksize 20480 -ip6profile LSN-DSLITE-
    PROFILE-10

Done
bind lsn group LSN-DSLITE-GROUP-10 -poolname LSN-DSLITE-POOL-10

Done
<!--NeedCopy-->
```

Konfigurieren von Application Layer-Gateways für DS-Lite

May 11, 2023

Bei einigen Protokollen auf Andwendungslayer werden die IP-Adressen und Protokollportnummern auch in der Payload des Pakets übermittelt. Application Layer Gateway (AGL) für ein Protokoll

analysiert die Paket-Payload und nimmt die erforderlichen Änderungen vor, um sicherzustellen, dass das Protokoll weiterhin über DS-Lite funktioniert.

Die NetScaler-Appliance unterstützt ALG für die folgenden Protokolle für DS-Lite:

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Application Layer Gateway für FTP-, ICMP- und TFTP-Protokolle

January 19, 2021

Sie können ALG für das FTP-Protokoll für eine DS-Lite-Konfiguration aktivieren oder deaktivieren, indem Sie die Option FTP ALG der LSN-Gruppe der Konfiguration aktivieren oder deaktivieren.

ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es gibt keine Möglichkeit, es zu deaktivieren.

ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. TFTP ALG wird automatisch für eine DS-Lite-Konfiguration aktiviert, wenn Sie ein UDP LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport als 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

Application Layer Gateway für SIP-Protokoll

May 11, 2023

Die Verwendung von DS-Lite mit dem Session Initiation Protocol (SIP) ist kompliziert, da SIP-Nachrichten IP-Adressen sowohl in den SIP-Headern als auch im SIP-Body enthalten. Wenn LSN mit SIP verwendet wird, enthalten die SIP-Header Informationen über den Anrufer und den Empfänger, und das Gerät übersetzt diese Informationen, um sie vor dem externen Netzwerk zu verbergen. Der SIP-Text enthält die SDP-Informationen (Session Description Protocol), zu denen IP-Adressen und Portnummern für die Übertragung der Medien gehören. SIP ALG für DS-Lite entspricht RFC 3261, RFC 3581, RFC 4566 und RFC 4475.

> **Hinweis**
>
> SIP ALG wird in einer eigenständigen NetScaler-Appliance, in einem NetScaler-Hochverfügbarkeits-

> Setup sowie in einem NetScaler-Cluster-Setup unterstützt.

Einschränkungen von SIP ALG

SIP ALG für DS-Lite weist die folgenden Einschränkungen auf:

- Nur SDP-Payload wird unterstützt.
- Folgende Komponenten werden nicht unterstützt:
  - Multicast-IP-Adressen
  - Verschlüsseltes SDP
  - SCHIFF BIS
  - FQDN-Übersetzung
  - SIP-Layer-Authentifizierung
  - Admin-Partitionen
  - Mehrteiliger Körper
  - Faltung der Leitung

Konfiguration von SIP ALG

Sie müssen die SIP ALG als Teil der LSN-Konfiguration konfigurieren. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurieren von DS-Lite. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Stellen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter ein:
  - IP-Pooling = GEPAART
  - Adress- und Portzuordnung = ENDPUNKTUNABHÄNGIG
  - Filterung = ENDPUNKTUNABHÄNGIG
- Erstellen Sie ein SIP-ALG-Profil und stellen Sie sicher, dass Sie entweder den Quellportbereich oder den Zielportbereich definieren. Binden Sie das SIP-ALG-Profil an die LSN-Gruppe
- Aktivieren Sie SIP ALG in der LSN-Gruppe

So aktivieren Sie SIP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lsn group <groupname> -clientname <string>[-sipalg ( ENABLED |
     DISABLED )]
2
3 show lsn group<groupname>
4 <!--NeedCopy-->
```


So aktivieren Sie SIP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn sipalgprofile<sipalgprofilename>[-dataSessionIdleTimeout<
    positive_integer>][-sipSessionTimeout<positive_integer>][-
    registrationTimeout<positive_integer>][-sipsrcportrange<port[-port
    ]>][-sipdstportrange<port[-port]>][-openRegisterPinhole ( ENABLED |
    DISABLED )][-openContactPinhole ( ENABLED | DISABLED )][-
    openViaPinhole ( ENABLED | DISABLED )][-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP )[-
    openRoutePinhole ( ENABLED | DISABLED )][-rport ( ENABLED | DISABLED
     )]

show lsn sipalgprofile<sipalgprofilename>
<!--NeedCopy-->
```

Beispielkonfiguration

In der folgenden DS-Lite-Beispielkonfiguration ist SIP ALG für TCP-Verkehr von B4-Geräten im Netzwerk aktiviert 2001:DB8:: 3:0 /96.

```
add lsn client LSN-DSLITE-CLIENT-1
Done
bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/96
Done
add lsn pool LSN-DSLITE-POOL-1
Done
bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
    DB8::5:6
Done
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-1 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn sipalgprofile SIPALGPROFILE-1  -sipdstportrange 5060 -
    sipTransportProtocol TCP
Done
add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
    portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1 -sipalg ENABLED
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
Done
```



```
bind lsn group LSN-DSLITE-GROUP-1 -appsprofilename LSN-DSLITE-APPS-
    PROFILE-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -sipalgprofilename SIPALGPROFILE-1
Done
<!--NeedCopy-->
```

Application Layer Gateway für das RTSP-Protokoll

May 11, 2023

Das Real Time Streaming Protocol (RTSP) ist ein Protokoll auf Anwendungsebene für die Übertragung von Mediendaten in Echtzeit. RTSP ist ein Kontrollkanalprotokoll zwischen dem Medienclient und dem Medienserver, das für die Einrichtung und Steuerung von Mediensitzungen zwischen Endpunkten verwendet wird. Die typische Kommunikation findet zwischen einem Client und einem Streaming-Media-Server statt.

Um Medien von einem privaten Netzwerk in ein öffentliches Netzwerk zu streamen, müssen IP-Adressen und Portnummern über das Netzwerk übersetzt werden. Die NetScaler-Funktionalität umfasst ein Application Layer Gateway (ALG) für RTSP, das zusammen mit Large Scale NAT (LSN) verwendet werden kann, um den Medienstream zu analysieren und alle erforderlichen Änderungen vorzunehmen, um sicherzustellen, dass das Protokoll weiterhin über das Netzwerk funktioniert.

Wie die IP-Adressübersetzung durchgeführt wird, hängt vom Typ und der Richtung der Nachricht sowie von der Art der Medien ab, die von der Client-Server-Bereitstellung unterstützt werden. Nachrichten werden wie folgt übersetzt:

- Ausgehende Anfrage — Private IP-Adresse für eine öffentliche IP-Adresse im Besitz von NetScaler, die als LSN-IP-Adresse bezeichnet wird.
- Eingehende Antwort — LSN-IP-Adresse an private IP-Adresse.
- Eingehende Anfrage — keine Übersetzung.
- Ausgehende Antwort — Private IP-Adresse zur LSN-Pool-IP-Adresse.

> **Hinweis**
>
> RTSP ALG wird in einer eigenständigen NetScaler-Appliance, in einem NetScaler-Hochverfügbarkeits-Setup sowie in einem NetScaler-Cluster-Setup unterstützt.

Einschränkungen von RTSP ALG

Das RTSP-ALG unterstützt Folgendes nicht:

- Multicast-RTSP-Sitzungen

- RTSP-Sitzung über UDP
- Admin-Partitionen
- RTSP-Authentifizierung
- HTTP-Tunneling

Konfiguration von RTSP ALG

Konfigurieren Sie RTSP ALG als Teil der LSN-Konfiguration. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurieren von DS-Lite. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Stellen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter ein:
  - IP-Pooling = GEPAART
  - Adress- und Portzuordnung = ENDPUNKTUNABHÄNGIG
  - Filterung = ENDPUNKTUNABHÄNGIG
- Aktivieren Sie RTSP ALG in der LSN-Gruppe
- Erstellen Sie ein RTSP-ALG-Profil und binden Sie das RTSP-ALG-Profil an die LSN-Gruppe.

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Beispiel für eine RTSP-ALG-Konfiguration

Die folgende DS-Lite-Beispielkonfiguration, RTSP ALG, ist für TCP-Verkehr von B4-Geräten im Netzwerk aktiviert 2001:DB8:: 4:0 /96.

Beispiel-RTSP-ALG-Konfiguration:

```
add lsn client LSN-DSLITE-CLIENT-5
Done
bind lsn client LSN-DSLITE-CLIENT-5 -network6 2001:DB8::4:0/96
Done
add lsn pool LSN-DSLITE-POOL-5
Done
bind lsn pool LSN-DSLITE-POOL-5 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-5 -type DS-Lite -network6 2001:
   DB8::5:6
Done
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-5 TCP -ippooling PAIRED -
   mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-5 -rtspIdleTimeout 1000 -
   rtspportrange 554
Done
add lsn group LSN-DSLITE-GROUP-5 -clientname LSN-DSLITE-CLIENT-5 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-5 -rtspalg ENABLED
Done
bind lsn group LSN-DSLITE-GROUP-5 -poolname LSN-DSLITE-POOL-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -appsprofilename LSN-DSLITE-APPS-
   PROFILE-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -rtspalgprofilename RTSPALGPROFILE-5
Done
<!--NeedCopy-->
```

Protokollierung und Überwachung DS-Lite

May 11, 2023

Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die NetScaler Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie zum Konfigurieren der DS-Lite-Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (MAPPING)
- Ob der DS-Lite LSN-Mapping-Eintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Abhängig von den folgenden Bedingungen können Ziel-IP-Adresse, Port und Verkehrsdomänen-ID vorhanden sein:
  - Ziel-IP-Adresse und Port werden für die endpunktunabhängige Zuordnung nicht protokolliert.
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Die Ziel-IP-Adresse und der Port werden für die adressportabhängige Zuordnung protokolliert.

Eine Lognachricht für eine DS-Lite-Sitzung besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Ziel-IP-Adresse, Port und Traffic-Domain-ID

Die folgende Tabelle zeigt Beispiele für DS-Lite-Protokolleinträge der einzelnen Typen, die auf den konfigurierten Protokollservern gespeichert sind. Diese Protokolleinträge werden von einer NetScaler-Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet. Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die NetScaler Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie zum Konfigurieren der DS-Lite-Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (MAPPING)
- Ob der DS-Lite LSN-Mapping-Eintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Abhängig von den folgenden Bedingungen können Ziel-IP-Adresse, Port und Verkehrsdomänen-ID vorhanden sein:
  - Ziel-IP-Adresse und Port werden für die endpunktunabhängige Zuordnung nicht protokolliert.
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Die Ziel-IP-Adresse und der Port werden für die adressportabhängige Zuordnung protokolliert.

Eine Lognachricht für eine DS-Lite-Sitzung besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Ziel-IP-Adresse, Port und Traffic-Domain-ID

Die folgende Tabelle zeigt Beispiele für DS-Lite-Protokolleinträge der einzelnen Typen, die auf den konfigurierten Protokollservern gespeichert sind. Diese Protokolleinträge werden von einer NetScaler-Appliance generiert, deren NSIP-Adresse 10.102.37.115 ist.

Typ des LSN-Protokolleintrags	Beispiel für einen Logeintrag

DS-Lite-Sitzungserstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1 : default LSN LSN_SESSION 37647607 0 : SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP
Löschen einer DS-Lite-Sitzung	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1 : default LSN LSN_SESSION 37647617 0 : SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP
DS-Lite LSN-Mapping-Erstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647610 0 : EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP
Löschen der DS-Lite-LSN-Zuordnung	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647618 0 : EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Aktuelle DS-Lite-Sessions anzeigen

Sie können die aktuellen DS-Lite-Sitzungen anzeigen, um unerwünschte oder ineffiziente Sitzungen auf der NetScaler-Appliance zu erkennen. Sie können alle oder einige DS-Lite-Sitzungen auf der Grundlage von Auswahlparametern anzeigen.

Um alle DS-Lite-Sessions mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:


```
show lsn session  - nattype DS-Lite
<!--NeedCopy-->
```

Um ausgewählte DS-Lite-Sitzungen mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
show lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

In der folgenden Beispielausgabe werden alle DS-Lite-Sitzungen angezeigt, die auf einer NetScaler-Appliance vorhanden sind:

> lsn-Sitzung anzeigen —nattype DS-Lite

```
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1. 2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2. 2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3. 2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4. 2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT
Done
<!--NeedCopy-->
```

Konfiguration mit dem Configuration Utility

Um alle oder ausgewählte DS-Lite-Sessions mithilfe des Konfigurationsdienstprogramms anzuzeigen

1. **Navigieren Sie zu System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die Registerkarte **DS-Lite** .
2. **Um DS-Lite-Sitzungen auf der Grundlage von Auswahlparametern anzuzeigen, klicken Sie auf Suchen.**

DS-Lite-Sitzungen löschen

Sie können alle unerwünschten oder ineffizienten DS-Lite-Sitzungen aus der NetScaler-Appliance entfernen. Die Appliance gibt sofort die für diese Sitzungen zugewiesenen Ressourcen (wie NAT-IP-Adresse, Port und Speicher) frei, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance verwirft auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte DS-Lite-Sitzungen von der NetScaler-Appliance entfernen.

So löschen Sie alle DS-Lite-Sitzungen mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session -nattype DS-Lite

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

So löschen Sie ausgewählte DS-Lite-Sitzungen mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

So löschen Sie alle oder ausgewählte DS-Lite-Sitzungen mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die **Registerkarte DS-Lite** .
2. Klicken Sie auf **Sitzungen leeren**.

Loggen von HTTP-Header-Informationen

Die NetScaler-Appliance kann Anforderungsheaderinformationen einer HTTP-Verbindung protokollieren, die die DS-Lite-Funktionalität verwendet. Die folgenden Header-Informationen eines HTTP-Anforderungspakets können protokolliert werden:

- URL, für die die HTTP-Anfrage bestimmt ist

- In der HTTP-Anfrage angegebene HTTP-Methode
- In der HTTP-Anfrage verwendete HTTP-Version
- IPv4-Adresse des Abonnenten, der die HTTP-Anfrage gesendet hat

Die HTTP-Header-Logs können von ISPs verwendet werden, um die Trends im Zusammenhang mit dem HTTP-Protokoll bei einer Gruppe von Abonnenten zu ermitteln. Ein ISP kann diese Funktion beispielsweise verwenden, um die beliebteste Website unter einer Gruppe von Abonnenten herauszufinden.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um die NetScaler-Appliance für die Protokollierung von HTTP-Header-Informationen zu konfigurieren:

- **Erstellen Sie ein HTTP-Header-Logprofil**. Ein HTTP-Header-Logprofil ist eine Sammlung von HTTP-Header-Attributen (z. B. URL und HTTP-Methode), die für die Protokollierung aktiviert oder deaktiviert werden können.
- **Binden Sie den HTTP-Header an eine LSN-Gruppe einer DS-Lite-LSN-Konfiguration**. Binden Sie das HTTP-Header-Logprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter für den Namen des HTTP-Header-Logprofils auf den Namen des erstellten HTTP-Header-Logprofils setzen. Die NetScaler-Appliance protokolliert dann die HTTP-Header-Informationen aller HTTP-Anfragen, die sich auf die LSN-Gruppe beziehen. Ein HTTP-Header-Logprofil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein HTTP-Header-Logprofil haben.

So erstellen Sie ein HTTP-Header-Logprofil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

So binden Sie ein HTTP-Header-Logprofil mithilfe der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

```



```
show lsn group <groupname>
<!--NeedCopy-->
```

Beispielkonfiguration

In der folgenden DS-Lite-LSN-Konfiguration ist das HTTP-Header-Logprofil HTTP-Header-Log-1 an die LSN-Gruppe LSN-DSLITE-GROUP-1 gebunden. Im Protokollprofil sind alle HTTP-Attribute (URL, HTTP-Methode, HTTP-Version und HOST-IP-Adresse) für die Protokollierung aktiviert, sodass all diese Attribute für alle HTTP-Anfragen von B4-Geräten (im Netzwerk 2001:DB 8:5001: :/96) protokolliert werden.

Beispielkonfiguration:

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1

Done

add lsn client LSN-DSLITE-CLIENT-1

Done

bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100

Done

add lsn pool LSN-DSLITE-POOL-1

Done

bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70

Done

add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6

Done

add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1

Done

bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
```



```
30
31 Done
32
33 bind lsn group LSN-DSLITE-GROUP-1 -httphdrlogprofilename HTTP-HEADER-
       LOG-1
34
35 Done
36 <!--NeedCopy-->
```

IPFIX-Protokollierung

Die NetScaler-Appliance unterstützt das Senden von Informationen über LSN-Ereignisse im IPFIX-Format (Internet Protocol Flow Information Export) an den konfigurierten Satz von IPFIX Collector (s). Die Appliance verwendet die vorhandene AppFlow-Funktion, um LSN-Ereignisse im IPFIX-Format an die IPFIX-Collectors zu senden.

IPFIX-basiertes Logging ist für die folgenden DS_Lite-bezogenen Ereignisse verfügbar:

- Erstellen oder Löschen einer LSN-Sitzung.
- Erstellung oder Löschung eines LSN-Mapping-Eintrags.
- Zuweisung oder Entzuweisung von Portblöcken im Kontext von deterministischem NAT.
- Zuweisung oder Entzuweisung von Portblöcken im Kontext von dynamischem NAT.
- Immer wenn das Kontingent für Abonnentensitzungen überschritten wird.

Punkte, die Sie beachten sollten, bevor Sie die IPFIX-Protokollierung konfigurieren

Bevor Sie mit der Konfiguration von IPSec ALG beginnen, sollten Sie die folgenden Punkte berücksichtigen:

- Sie müssen die AppFlow Funktion und die IPFIX-Kollektoren auf der NetScaler Appliance konfigurieren. Anweisungen finden Sie unter Konfigurieren der AppFlow-Funktion.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um LSN-Informationen im IPFIX-Format zu protokollieren:

- **Aktivieren Sie die LSN-Protokollierung in der AppFlow-Konfiguration**. Aktivieren Sie den LSN-Logging-Parameter als Teil der AppFlow-Konfiguration.
- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den IPFIX-Parameter, der die Protokollinformationen im IPFIX-Format aktiviert oder deaktiviert.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das LSN-Protokollprofil an eine oder mehrere LSN-Gruppe (n). Ereignisse, die sich auf die gebundene LSN-Gruppe beziehen, werden im IPFIX-Format protokolliert.

So aktivieren Sie die LSN-Protokollierung in der AppFlow-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set appflow param -lsnLogging (ENABLED |DISABLED )

show appflow param
<!--NeedCopy-->
```

Um mithilfe der CLI ein LSN-Protokollprofil zu erstellen, geben Sie in der Befehlszeile Folgendes ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie das LSN-Protokollprofil mithilfe der CLI an eine LSN-Gruppe einer LSN-Konfiguration

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Protokollprofil mithilfe der GUI

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf die Registerkarte **Protokoll** und fügen Sie dann ein Protokollprofil hinzu.

So binden Sie das LSN-Protokollprofil mithilfe der GUI an eine LSN-Gruppe einer LSN-Konfiguration

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group und** öffnen Sie die **LSN-Gruppe** .
2. Klicken Sie **unter Erweiterte Einstellungen** auf **+ Protokollprofil**, um das erstellte Protokollprofil an die LSN-Gruppe zu binden.

Port Control Protocol für DS-Lite

May 11, 2023

NetScaler-Appliances unterstützen jetzt das Port Control Protocol (PCP) für Large Scale NAT (LSN). Viele der Abonnentenanwendungen eines Internetdienstanbieters müssen über das Internet zugänglich sein (z. B. IoT-Geräte (Internet of Things), wie z. B. eine IP-Kamera, die die Überwachung über das Internet ermöglicht). Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, statische großskalige NAT-Karten (LSN) zu erstellen. Für eine sehr große Anzahl von Abonnenten ist die Erstellung statischer LSN-NAT-Maps jedoch keine praktikable Lösung.

Das Port Control Protocol (PCP) ermöglicht es einem Abonnenten, spezifische LSN-NAT-Zuordnungen für sich selbst und/oder für andere Geräte von Drittanbietern anzufordern. Das große NAT-Gerät erstellt eine LSN-Map und sendet sie an den Abonnenten. Der Abonnent sendet den Remote-Geräten im Internet die NAT-IP-Adresse: NAT-Port, an dem sie sich mit dem Abonnenten verbinden können.

Anwendungen senden in der Regel häufig Keep-Alive-Nachrichten an das große NAT-Gerät, damit ihre LSN-Zuordnungen nicht zu einem Timeout führen. PCP trägt dazu bei, die Häufigkeit solcher Keep-Alive-Nachrichten zu reduzieren, indem es den Anwendungen ermöglicht, die Timeout-Einstellungen der LSN-Zuordnungen zu erlernen. Dies trägt dazu bei, den Bandbreitenverbrauch im Zugangsnetz des ISP und den Batterieverbrauch auf Mobilgeräten zu reduzieren.

PCP ist ein Client-Server-Modell und läuft über das UDP-Transportprotokoll. Eine NetScaler-Appliance implementiert die PCP-Serverkomponente und entspricht RFC 6887.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben zur Konfiguration von PCP aus:

- (Optional) Erstellen Sie ein PCP-Profil. Ein PCP-Profil enthält Einstellungen für PCP-bezogene Parameter (z. B. um auf Mapping- und Peer-PCP-Anfragen zu warten). Ein PCP-Profil kann an einen PCP-Server gebunden werden. Ein an einen PCP-Server gebundenes PCP-Profil wendet alle seine Einstellungen auf den PCP-Server an. Ein PCP-Profil kann an mehrere PCP-Server gebunden werden. Standardmäßig ist ein PCP-Profil mit Standardparametereinstellungen an alle PCP-Server gebunden. Ein PCP-Profil, das Sie an einen PCP-Server binden, überschreibt die standardmäßigen PCP-Profileinstellungen für diesen Server. Ein Standard-PCP-Profil hat die folgenden Parametereinstellungen:
  - Zuordnung: Aktiviert
  - Peer: Aktiviert
  - Minimale Lebensdauer der Karte: 120 Sekunden
  - Maximale Lebensdauer: 86400 Sekunden
  - Anzahl ankündigen: 10

- Drittanbieter: Deaktiviert

- Erstellen Sie einen PCP-Server und binden Sie ein PCP-Profil daran. Erstellen Sie einen PCP-Server auf der NetScaler-Appliance, um auf PCP-bezogene Anfragen und Nachrichten der Abonnenten zu warten. Um darauf zugreifen zu können, muss einem PCP-Server eine Subnetz-IP-Adresse (SNIP) zugewiesen werden. Standardmäßig überwacht ein PCP-Server Port 5351.
- Binden Sie den PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration. Binden Sie den erstellten PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den PCP-Serverparameter so festlegen, dass der erstellte PCP-Server angegeben wird. Auf den erstellten PCP-Server können nur die Abonnenten dieser LSN-Gruppe zugreifen.
  Hinweis: Ein PCP-Server für eine große NAT-Konfiguration erfüllt keine Anfragen von Abonnenten, die anhand von ACL-Regeln identifiziert wurden.

So erstellen Sie ein PCP-Profil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
     ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
     announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
     DISABLED )]
2
3 show pcp profile <name>
4 <!--NeedCopy-->
```

So erstellen Sie einen PCP-Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
     string>]
2
3 show pcp server <name>
4 <!--NeedCopy-->
```

Beispielkonfiguration für DS-LITE

In der folgenden Beispielkonfiguration ist der PCP-Server PCP-SERVER-1 mit den PCP-Einstellungen von PCP-DSLITE-PROFILE-1 an die LSN-Gruppe LSN-DSLITE-GROUP-1 gebunden. PCP-SERVER-9 bedient PCP-Anfragen von IPv4-Abonnenten hinter B4-Geräten aus dem Netzwerk 2001:DB8:: 3:0 /100.

Beispielkonfiguration:


```
add pcp profile PCP-DSLITE-PROFILE-1 -minMapLife 300
Done
add pcp server PCP-DSLITE-SERVER-1 192.0.3.10  -pcpProfile PCP-DSLITE-PROFILE-1
Done
add lsn client LSN-DSLITE-CLIENT-1
Done
bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
add lsn pool LSN-DSLITE-POOL-1
Done
bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:DB8::5:6
Done
add lsn group LSN-DSLITE-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname  PCP-NAT64-SERVER-1
Done
<!--NeedCopy-->
```

Large Scale NAT64

September 1, 2023

> **Hinweis:**
>
> Die Large Scale NAT64 (LSN64) -Funktion ist ab Version NetScaler 14.1 veraltet.
>
> Veraltete Funktionen werden nicht sofort entfernt. Die NetScaler Appliance unterstützt die veraltete Funktion weiterhin, bis sie in einer zukünftigen Version entfernt wird.

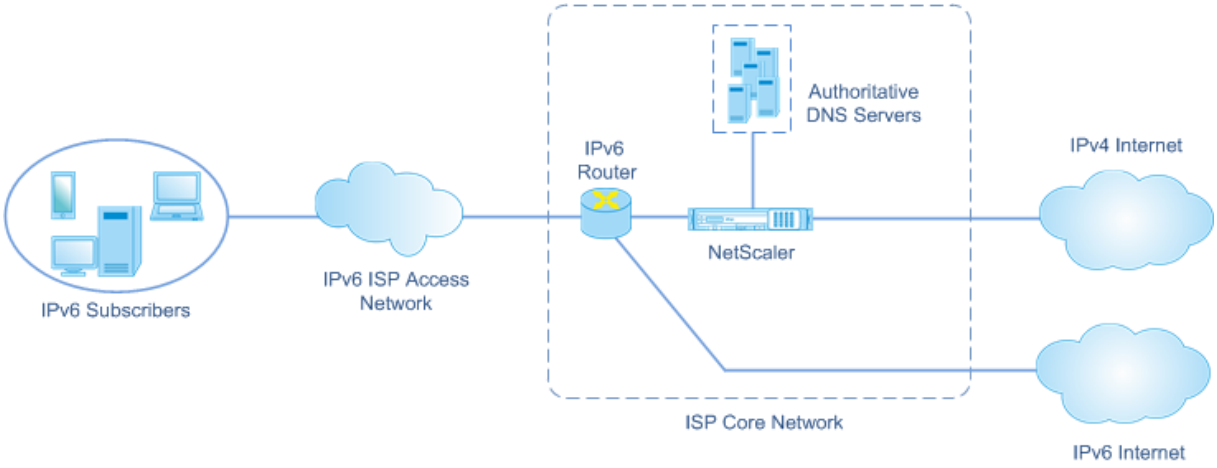
Aufgrund der bevorstehenden Erschöpfung der IPv4-Adressen haben ISPs mit der Umstellung auf die IPv6-Infrastruktur begonnen. Während der Umstellung müssen ISPs jedoch weiterhin IPv4 zusammen mit IPv6 unterstützen, da der Großteil des öffentlichen Internets immer noch IPv4 verwendet. Large Scale NAT64 ist eine IPv6-Übergangslösung für ISPs mit IPv6-Infrastruktur, um ihre reinen IPv6-Abonnenten mit dem IPv4-Internet zu verbinden. DNS64 ist eine Lösung, um die Erkennung von reinen IPv4-Domänen durch reine IPv6-Clients zu ermöglichen. DNS64 wird mit NAT64 in großem

Maßstab verwendet, um eine nahtlose Kommunikation zwischen reinen IPv6-Clients und reinen IPv4-Servern zu ermöglichen.

Eine NetScaler-Appliance implementiert NAT64 und DNS64 in großem Maßstab und ist mit den RFCs 6145, 6146, 6147, 6052, 3022, 2373, 2765 und 2464 kompatibel.

Architektur

Die NAT64-Architektur eines ISP, der eine NetScaler-Appliance verwendet, besteht aus IPv6-Abonnenten, die über eine NetScaler-Appliance, die im Kernnetzwerk des ISP bereitgestellt wird, auf das IPv4-Internet zugreifen. IPv6-Abonnenten sind über das reine IPv6-Zugangsnetzwerk des ISP mit dem ISP-Kernnetzwerk verbunden.



Die umfangreiche NAT64-Funktionalität einer NetScaler-Appliance ermöglicht die Kommunikation zwischen IPv6-Clients und IPv4-Servern durch IPv6-zu-IPv4-Paketübersetzung und umgekehrt, wobei die Sitzungsinformationen auf der NetScaler Appliance erhalten bleiben. Die NetScaler DNS64-Funktionalität stellt IPv4-reine IPv4-Domänen für IPv6-Abonnenten dar, indem DNS-AAAAA-Einträge für reine IPv4-Domänen synthetisiert und an die Abonnenten gesendet werden.

Large Scale NAT64 besteht aus zwei Hauptkomponenten: dem NAT64-Präfix und dem NAT-IPv4-Pool. DNS64 hat eine Hauptkomponente, das DNS64-Präfix, das den gleichen Wert wie das NAT64-Präfix hat.

Beim Empfang einer AAAA-Anfrage von einem reinen IPv6-Abonnenten für einen Domainnamen, der auf einem reinen IPv4-Webserver im Internet gehostet wird, synthetisiert die NetScaler DNS64-Funktionalität einen AAAA-Datensatz für den Domainnamen und sendet ihn an den Abonnenten. Der AAAA-Datensatz wird synthetisiert, indem das DNS64-Präfix (das auf das NAT64-Präfix gesetzt ist) und die tatsächliche IPv4-Adresse des Domainnamens verkettet werden.

Der Abonnent hat jetzt eine IPv6-Zieladresse, die dem gewünschten Domainnamen entspricht. Der Abonnent sendet die Anfrage an die synthetisierte IPv6-Adresse. Nach Empfang der IPv6-Anfrage

übersetzt die umfangreiche NetScaler NAT64-Funktionalität das IPv6-Anforderungspaket in ein IPv4-Anforderungspaket. In großem Maßstab setzt NAT64 die Zieladresse der IPv4-Anfrage auf die IPv4-Adresse, die aus der Zieladresse der IPv6-Anfrage extrahiert wird, indem das NAT64-Präfix von der IPv6-Adresse entfernt wird. Der Zielport wird aus der IPv6-Anfrage beibehalten. Large Scale NAT64 setzt außerdem die Quell-IP-Adresse: Quellport des IPv4-Pakets auf den NAT-IP-Adresse:NAT-Port, der aus dem konfigurierten NAT-Pool ausgewählt wurde.

Die Appliance zeichnet alle aktiven Sitzungen auf, die die umfangreiche NAT64-Funktionalität verwenden. Diese Sitzungen werden als groß angelegte NAT64-Sitzungen bezeichnet. Die Appliance verwaltet auch die Zuordnungen zwischen der IPv6-Adresse und dem Port für Abonnenten sowie der NAT-IPv4-Adresse und dem Port für jede groß angelegte NAT64-Sitzung. Diese Zuordnungen werden als groß angelegte NAT64-Mappings bezeichnet. Anhand von umfangreichen NAT64-Sitzungseinträgen und umfangreichen NAT64-Mapping-Einträgen erkennt die NetScaler-Appliance ein (aus dem Internet empfangenes) Antwortpaket als Teil einer bestimmten NAT64-Sitzung.

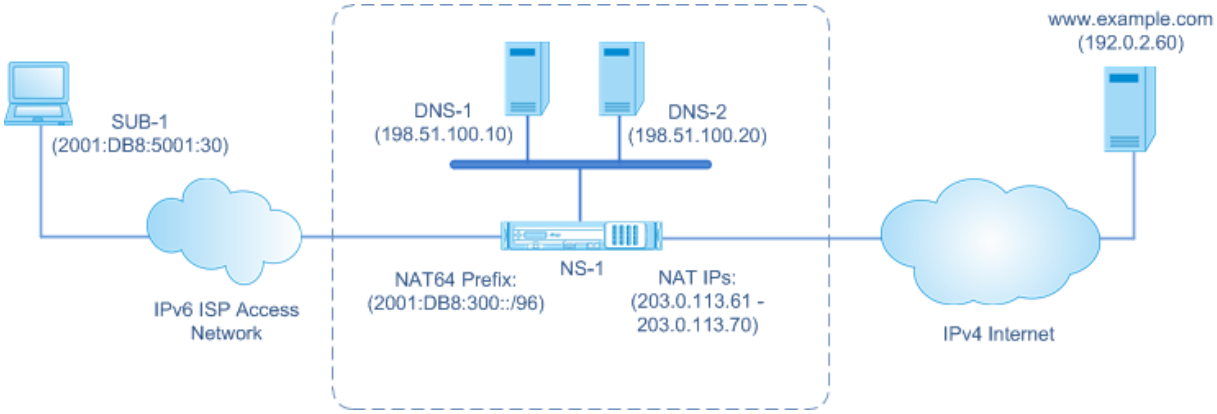
Wenn die Appliance ein IPv4-Antwortpaket empfängt, das zu einer bestimmten NAT64-Sitzung gehört, verwendet sie die in der NAT64-Sitzung gespeicherten Informationen, um das IPv4-Paket in ein IPv6-Paket zu übersetzen, und sendet dann das IPv6-Antwortpaket an den Abonnenten.

Beispiel: Verkehrsfluss bei der NAT64- und DNS64-Bereitstellung

Stellen Sie sich ein Beispiel für eine groß angelegte NAT64- und DNS64-Bereitstellung vor, die aus der NetScaler-Appliance NS-1 und zwei lokalen DNS-Servern, DNS-1 und DNS-2, im Kernnetzwerk eines ISP und einem IPv6-Abonnenten SUB-1 besteht. SUB-1 ist über das IPv6-Zugangsnetzwerk des ISP mit NS-1 verbunden. NS-1 umfasst umfangreiche NAT64- und DNS64-Konfigurationen, um die Kommunikation zwischen IPv6-Abonnenten-SUB-1 und IPv4-Hosts (intern und extern) zu ermöglichen.

Eine groß angelegte NAT64-Konfiguration umfasst ein NAT64-Präfix (2001:DB 8:300: :/96) und einen NAT-IPv4-Pool für die Übersetzung von IPv6-Anfragen in IPv4-Anfragen und IPv4-Antworten auf IPv6-Antworten.

Die DNS64-Konfiguration umfasst einen virtuellen DNS-Lastausgleichsserver LBVS-DNS64-1 (2001:DB 8:9999: :99) und ein DNS64-Präfix (2001:DB 8:300: :/96). LBVS-DNS64-1 stellt die lokalen DNS-Server DNS-1 und DNS-2 für die Abonnenten des ISP dar. Das DNS64-Präfix, das den gleichen Wert wie das NAT64-Präfix hat, wird für die Synthese von DNS-AAAA-Einträgen aus DNS-A-Einträgen verwendet, die von den DNS-Servern DNS-1 und DNS-2 empfangen wurden. NS-1 antwortet mit einem synthetisierten AAAA-Eintrag an SUB-1 auf eine DNS-Anfrage zur Auflösung eines IPv4-Hosts.



DNS64-Verkehrsfluss

Der Datenverkehr zwischen dem IPv6-Abonnenten SUB-1 und der Site `www.example.com`, die sich auf einem reinen IPv4-Webserver im Internet befindet, fließt wie folgt:

1. Der IPv6-Abonnent SUB-1 sendet eine DNS-AAAA-Anfrage für `www.example.com` an seinen angegebenen DNS-Server (2001:DB 8:9999: :99).
2. Der virtuelle DNS-Lastausgleichsserver LBVS-DNS64-1 (2001:DB 8:9999: :99) auf der NetScaler Appliance NS1 empfängt die AAAA-Anfrage. Der Load-Balancing-Algorithmus von LBVS-DNS64-1 wählt den DNS-Server DNS-1 aus und leitet die AAAA-Anfrage an ihn weiter.
3. DNS-1 gibt einen leeren Datensatz oder eine Fehlermeldung zurück, da kein AAAA-Datensatz für verfügbar ist. `www.example.com`
4. Da die DNS64-Option auf LBVS-DNS64-1 aktiviert ist und die AAAA-Anfrage von CL1 der in DNS64-Policy-1 angegebenen Bedingung entspricht, sendet NS1 eine DNS-A-Anfrage an DNS-1 für die IPv4-Adresse von. `www.example.com`
5. DNS-1 antwortet mit dem A-Record von 192.0.2.60 für. `www.example.com`
6. Das DNS64-Modul auf NS1 synthetisiert einen AAAA-Datensatz für `www.example.com`, indem es das DNS64-Präfix (2001:DB8:300::/96), das mit LBVS-DNS64-1 verknüpft ist, und die IPv4-Adresse (192.0.2.60) für `www.example.com` wie folgt verkettet: 2001:DB8:300::192.0.2.60
7. NS1 sendet den synthetisierten AAAA-Datensatz an den IPv6-Client CL1. NS1 speichert auch den A-Datensatz in seinem Speicher. NS1 verwendet den zwischengespeicherten A-Datensatz, um AAAA-Datensätze für nachfolgende AAAA-Anfragen zu synthetisieren.

NAT64-Verkehrsfluss

1. Der IPv6-Abonnent SUB-1 sendet eine Anfrage an 2001:DB 8:5001:30. `www.example.com` Das IPv6-Paket hat:
   - Quell-IP-Adresse = 2001:DB 8:5001:30
   - Quellport = 2552

- Ziel-IP-Adresse = 2001:DB 8:300: :192.0.2.60
- Zielport = 80

2. Der IPv6-Abonnent SUB-1 sendet eine Anfrage an 2001:DB 8:5001:30. `www.example.com` Das IPv6-Paket hat:
   - Quell-IP-Adresse = 2001:DB 8:5001:30
   - Quellport = 2552
   - Ziel-IP-Adresse = 2001:DB 8:300: :192.0.2.60
   - Zielport = 80
3. Wenn NS-1 das IPv6-Paket empfängt, erstellt das umfangreiche NAT64-Modul ein übersetztes IPv4-Anforderungspaket mit:
   - Quell-IP-Adresse = Eine der im konfigurierten NAT-Pool verfügbaren IPv4-Adressen (203.0.113.61)
   - Quellport = Einer der Ports, die mit der zugewiesenen NAT-IPv4-Adresse (3002) verfügbar sind
   - Ziel-IP-Adresse = IPv4-Adresse, die aus der Zieladresse der IPv6-Anfrage extrahiert wurde, indem das NAT64-Präfix (2001:DB 8:300: :/96) von der IPv6-Adresse entfernt wurde (192.0.2.60)
   - Zielport = Zielport der IPv6-Anfrage (80)
4. Das groß angelegte NAT64-Modul erstellt auch Mappings- und Sitzungseinträge für diesen groß angelegten NAT64-Fluss. Die Sitzungs- und Zuordnungseinträge enthalten die folgenden Informationen:
   - Quell-IP-Adresse des IPv6-Pakets = 2001:DB 8:5001:30
   - Quellport des IPv6-Pakets = 2552
   - NAT-IP-Adresse = 203.0.113.61
   - NAT-Anschluss = 3002
   - NS-1 sendet das resultierende IPv4-Paket an sein Ziel im Internet.
5. Nach Empfang des Anforderungspakets `www.example.com` verarbeitet der Server das Paket und sendet ein Antwortpaket an NS-1. Das IPv4-Antwortpaket enthält:
   - Quell-IP-Adresse = 192.0.2.60
   - Quellport = 80
   - Ziel-IP-Adresse = 203.0.113.61
   - Zielport = 3002
6. Nach Empfang des IPv4-Antwortpakets untersucht NS-1 die umfangreiche NAT64-Zuordnung und die Sitzungseinträge und stellt fest, dass das IPv4-Antwortpaket zu einer großen NAT64-Sitzung gehört. Das groß angelegte NAT64-Modul erstellt ein übersetztes IPv6-Antwortpaket:
   - Quell-IP-Adresse = 2001:DB 8:300: :192.0.2.60

- Quellport = 80
- Ziel-IP-Adresse = 2001:DB 8:5001:30
- Zielport = 2552

7. NS-1 sendet die übersetzte IPv6-Antwort an den Client SUB-1.

Große NAT64-Funktionen, die auf NetScaler-Appliances unterstützt werden

Der große NAT64 auf einer NetScaler Appliance unterstützt den standardmäßigen LSN-Funktionsumfang. Weitere Informationen zu diesen LSN-Funktionen finden Sie unter LSN Architecture.

Im Folgenden finden Sie einige der großen NAT64-Funktionen, die von NetScaler Appliances unterstützt werden:

- ALGs. Unterstützung von Application Layer Gateway (ALG) für SIP-, RTSP-, FTP-, ICMP- und TFTP-Protokolle.
- Deterministisches/Festes NAT. Unterstützung für die vorherige Zuweisung von Portblöcken an Abonnenten, um die Protokollierung zu minimieren.
- Kartierung. Unterstützung von endpunktunabhängiger Zuordnung (EIM), adressabhängiger Zuordnung (ADM) und adressportabhängiger Zuordnung (APDM).
- Filterung. Unterstützung von Endpunktunabhängiger Filterung (EIF), adressabhängiger Filterung (ADF) und adressportabhängiger Filterung (APDF).
- Kontingente. Konfigurierbare Grenzwerte für die Anzahl der Ports, Sitzungen pro Abonnent und Sitzungen pro LSN-Gruppe.
- Statische Kartierung. Unterstützung für die manuelle Definition eines groß angelegten NAT64-Mappings.
- Hairpin Flow. Unterstützung für die Kommunikation zwischen Abonnenten oder internen Hosts mithilfe von NAT-IP-Adressen.
- 464XLAT-Verbindungen. Unterstützung für die Kommunikation zwischen reinen IPv4-Anwendungen auf IPv6-Abonnenten-Hosts und IPv4-Hosts im Internet über ein IPv6-Netzwerk.
- NAT64- und DNS64-Präfixe variabler Länge. Die NetScaler-Appliance unterstützt die Definition von NAT64- und DNS64-Präfixen mit den Längen 32, 40, 48, 56, 64 und 96.
- Mehrfaches NAT64- und DNS64-Präfix. Die NetScaler-Appliance unterstützt mehrere NAT64- und DNS64-Präfixe.
- LSN-Kunden. Unterstützung für die Spezifizierung oder Identifizierung von Abonnenten für NAT64 in großem Maßstab mithilfe von IPv6-Präfixen und erweiterten ACL6-Regeln.
- Protokollierung. Unterstützung für die Protokollierung von NAT64-Sitzungen für Strafverfolgungsbehörden. Darüber hinaus wird Folgendes für die Protokollierung unterstützt.
  - **Zuverlässiges SYSLOG**. Unterstützung für das Senden von SYSLOG-Nachrichten über TCP an externe Protokollserver für einen zuverlässigeren Transportmechanismus.
  - **Lastenausgleich von Protokollservern**. Unterstützung für den Lastenausgleich externer Protokollserver, um die Speicherung redundanter Protokollmeldungen zu verhindern.

- **Minimale Protokollierung**. Deterministische LSN-Konfigurationen oder dynamische LSN-Konfigurationen mit Portblock reduzieren das große NAT64-Protokollvolumen erheblich.
- **Protokollierung von MSISDN-Informationen**. Unterstützung für die Einbeziehung der MSISDN-Informationen von Abonnenten in große NAT64-Protokolle, um Abonnentenaktivitäten über das Internet zu identifizieren und zu verfolgen.

Punkte, die bei der Konfiguration des Großmaßes NAT64 zu beachten sind

May 11, 2023

Bevor Sie mit der Konfiguration von NAT64 und DNS64 in großem Maßstab beginnen, sollten Sie die folgenden Punkte berücksichtigen:

1. Stellen Sie sicher, dass Sie die verschiedenen Komponenten von Large Scale NAT64 verstehen, die in den RFCs beschrieben werden.
2. Die NetScaler-Appliance unterstützt nur die folgenden ALGs für Large Scale NAT64:
   - FTP
   - TFTP
   - ICMP
   - SIP
   - RTSP
3. In einem Hochverfügbarkeits-Setup mit zwei NetScaler-Appliances wird die Synchronisation großer NAT64-Sitzungen (Verbindungsspiegelung) nicht unterstützt.

Konfigurieren von DNS64

May 11, 2023

Das Erstellen der erforderlichen Entitäten für die statusmäßige NAT64-Konfiguration auf der NetScaler-Appliance umfasst die folgenden Verfahren:

- Fügen Sie DNS-Dienste hinzu. DNS-Dienste sind logische Darstellungen von DNS-Servern, für die die NetScaler Appliance als DNS-Proxyserver fungiert. Weitere Informationen zum Festlegen optionaler Parameter eines Dienstes finden Sie unter Load Balancing.
- Fügen Sie DNS64-Aktion und DNS64-Richtlinie hinzu, und binden Sie dann die DNS64-Aktion an die DNS64-Richtlinie. Eine DNS64-Richtlinie legt die Bedingungen fest, die gemäß den Einstellungen in der zugehörigen DNS64-Aktion mit dem Datenverkehr für die DNS64-Verarbeitung

abgeglichen werden. Die DNS64-Aktion gibt das obligatorische DNS64-Präfix und die optionalen Einstellungen für Ausschlussregeln und zugeordnete Regeln an.

- Erstellen Sie einen virtuellen DNS-Lastausgleichsserver und binden Sie die DNS-Dienste und die DNS64-Richtlinie daran. Der virtuelle DNS-Lastenausgleichsserver fungiert als DNS-Proxyserver für DNS-Server, die durch die gebundenen DNS-Dienste repräsentiert werden. Datenverkehr, der auf dem virtuellen Server eintrifft, wird mit der gebundenen DNS64-Richtlinie für die DNS64-Verarbeitung abgeglichen. Weitere Informationen zum Festlegen optionaler Parameter eines virtuellen Lastausgleichsservers finden Sie unter Load Balancing.

> **Hinweis**
>
> Die Befehlszeilenschnittstelle hat separate Befehle für diese beiden Aufgaben, aber die GUI kombiniert sie in einem einzigen Dialogfeld.

- Aktivieren Sie das Zwischenspeichern von DNS-Einträgen. Aktivieren Sie den globalen Parameter für die NetScaler Appliance, um DNS-Einträge zwischenzuspeichern, die über DNS-Proxyvorgänge abgerufen werden. Weitere Informationen zum Aktivieren des Zwischenspeichers von DNS-Datensätzen finden Sie unter Aktivieren des Zwischenspeichers von DNS-Datensätzen.

So erstellen Sie einen Dienst vom Typ DNS mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add service <name> <IP> <serviceType> <port> …
2 <!--NeedCopy-->
```

So erstellen Sie eine DNS64-Aktion mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add dns action64 <actionName> -Prefix <ipv6_addr|*> [-mappedRule <
     expression>] [-excludeRule <expression>]
2 <!--NeedCopy-->
```

So erstellen Sie eine DNS64-Richtlinie mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add dns policy64 <name> -rule <expression> -action <string>
2 <!--NeedCopy-->
```


So erstellen Sie einen virtuellen DNS-Lastausgleichsserver mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> DNS <IPAddress> <port> -dns64 (ENABLED | DISABLED ) [-bypassAAAA ( YES | NO)] …
<!--NeedCopy-->
```

Um die DNS-Dienste und die DNS64-Richtlinie mithilfe der Befehlszeilenschnittstelle an den virtuellen DNS-Lastenausgleichsserver zu binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName> ...

bind lb vserver <name> -policyName <string> -priority <positive_integer> ...
<!--NeedCopy-->
```

Beispielkonfiguration:

```
add service SVC-DNS-1 203.0.113.50 DNS 53
Done
add service SVC-DNS-2 203.0.113.60 DNS 53
Done
add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
Done
add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET(2001:DB8:5001::/64)" -action DNS64-Action-1
Done
add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
Done
bind lb vserver LBVS-DNS64-1 SVC-DNS-1
Done
bind lb vserver LBVS-DNS64-1 SVC-DNS-2
Done
bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
Done
<!--NeedCopy-->
```


Konfigurieren des Large Scaler NAT64

May 11, 2023

Eine groß angelegte NAT64-Konfiguration auf einer NetScaler-Appliance verwendet die LSN-Befehlssätze. In einer groß angelegten NAT64-Konfiguration gibt die LSN-Client-Entität die IPv6-Adresse oder IPv6-Netzwerkadresse oder die ACL6-Regeln zur Identifizierung von IPv6-Abonnenten an. Eine NAT64-Konfiguration umfasst auch ein IPv6-Profil, das ein NAT64-Präfix spezifiziert.

Die Konfiguration von NAT64 auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- Stellen Sie die globalen LSN-Parameterein. Zu den globalen Parametern gehören die Menge des NetScaler-Speichers, der für die LSN-Funktion reserviert ist, und die Synchronisation von LSN-Sitzungen in einem Hochverfügbarkeits-Setup.
- Erstellen Sie eine LSN-Client-Entität zur Identifizierung des Datenverkehrs von IPv6-Abonnenten. Die LSN-Client-Entität bezieht sich auf eine Gruppe von IPv6-Abonnenten. Die Client-Entität enthält IPv6-Adressen oder IPv6-Netzwerkpräfixe oder ACL6-Regeln, um den Datenverkehr dieser Abonnenten zu identifizieren. Ein LSN-Client kann nur an eine LSN-Gruppe gebunden werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen einer LSN-Client-Entität und zum Binden eines Abonnenten an die LSN-Client-Entität. Die GUI kombiniert diese beiden Operationen auf einem einzigen Bildschirm.
- Erstellen Sie einen LSN-Pool und binden Sie NAT-IP-Adressen daran. Ein LSN-Pool definiert einen Pool von NAT-IP-Adressen, die von der NetScaler-Appliance verwendet werden, um NAT64 im großen Maßstab auszuführen. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen eines LSN-Pool und zum Binden von NAT-IP-Adressen an den LSN-Pool. Die GUI kombiniert diese beiden Operationen auf einem einzigen Bildschirm.
- Erstellen Sie ein LSN IP6-Profil. Ein LSN-IP6-Profil definiert das NAT64-Präfix für eine groß angelegte NAT64-Konfiguration.
- (Optional) Erstellen Sie ein LSN-Transportprofil für ein bestimmtes Protokoll. Ein LSN-Transportprofil definiert verschiedene Timeouts und Limits, wie z. B. die maximalen Large Scale NAT64-Sitzungen und die maximale Portauslastung, die ein Abonnent für ein bestimmtes Protokoll haben kann. Sie binden ein LSN-Transportprofil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes Profil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für die Protokolle TCP, UDP und ICMP bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standard-Transportprofil bezeichnet. Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das Standard-LSN-Transportprofil für dieses Protokoll.
- (Optional) Erstellen Sie ein LSN-Anwendungsprofil für ein bestimmtes Protokoll und binden Sie eine Reihe von Zielports daran. Ein LSN-Anwendungsprofil definiert die LSN-Zuordnung und die LSN-Filterung einer Gruppe für ein bestimmtes Protokoll und für eine Reihe von Zielports.

Für eine Reihe von Zielports binden Sie ein LSN-Profil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes LSN-Anwendungsprofil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für die TCP-, UDP- und ICMP-Protokolle für alle Zielports bei seiner Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardanwendungsprofil bezeichnet. Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen eines LSN-Anwendungsprofils und zum Binden einer Reihe von Zielports an das LSN-Anwendungsprofil. Die GUI kombiniert diese beiden Operationen auf einem einzigen Bildschirm.

- Erstellen Sie eine LSN-Gruppe und binden Sie LSN-Pools, LSN-IPv6-Profile, (optional) LSN-Transportprofile und (optional) LSN-Anwendungsprofile an die LSN-Gruppe. Eine LSN-Gruppe ist eine Entität, die aus einem LSN-Client, einem LSN-IPv6-Profil, LSN-Pool (n), LSN-Transportprofilen und LSN-Anwendungsprofilen (en) besteht. Einer Gruppe werden Parameter wie die Portblockgröße und die Protokollierung von LSN-Sitzungen zugewiesen. Die Parametereinstellungen gelten für alle Abonnenten eines LSN-Clients, der an die LSN-Gruppe gebunden ist. Nur ein LSN-IPv6-Profil kann an eine LSN-Gruppe gebunden werden, und ein an eine LSN-Gruppe gebundenes LSN-IPv6-Profil kann nicht an andere LSN-Gruppen gebunden werden. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Nur eine LSN-Client-Entität kann an eine LSN-Gruppe gebunden werden, und eine LSN-Client-Entität, die an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle enthält zwei Befehle zum Erstellen einer LSN-Gruppe und zum Binden von LSN-Pools, LSN-Transportprofilen und LSN-Anwendungsprofilen an die LSN-Gruppe. Die GUI kombiniert diese beiden Operationen in einem einzigen Bildschirm.

Konfiguration über die Befehlszeile

Mit der Befehlszeilenschnittstelle können Sie verschiedene Konfigurationen erstellen. Folgen Sie den unten angegebenen Schritten.

So erstellen Sie einen LSN-Client mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn client <clientname
```



```
show lsn client
<!--NeedCopy-->
```

So binden Sie ein IPv6-Netzwerk oder eine ACL6-Regel mithilfe der Befehlszeilenschnittstelle an einen LSN-Client

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
   string>)

show lsn client
<!--NeedCopy-->
```

So erstellen Sie einen LAN-Pool mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn pool <poolname>

show lsn pool <poolname>
<!--NeedCopy-->
```

So binden Sie NAT-IP-Adressen mithilfe der Befehlszeilenschnittstelle an einen LSN-Pool

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

> **Hinweis**
>
> Verwenden Sie den Befehl unbind lsn pool, um NAT-IP-Adressen (LSN-IP-Adressen) aus einem LSN-Pool zu entfernen.

So konfigurieren Sie ein LSN-IPv6-Profil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
add lsn ip6profile <name>  - type NAT64 -natprefix <ipv6_addr|*>

show lsn ip6profile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Transportprofil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Anwendungsprofil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )]

show lsn appsprofile
<!--NeedCopy-->
```

So binden Sie einen Portbereich eines Anwendungsprotokolls mithilfe der Befehlszeilenschnittstelle an ein LSN-Anwendungsprofil

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```


So erstellen Sie eine LSN-Gruppe mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging(
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync ( ENABLED | DISABLED )] [-snmptraplimit<positive_integer
    >] [-ftp ( ENABLED | DISABLED )] [-sipalg ( ENABLED | DISABLED )] [-
    rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

show lsn group
<!--NeedCopy-->
```

So binden Sie LSN-Protokollprofile und LSN-Pools mithilfe der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Beispiele für groß angelegte NAT64-Konfigurationen

Hier sind einige Beispielkonfigurationen von NAT64 im großen Maßstab:

Einfache groß angelegte NAT64-Konfiguration mit Standardeinstellungen:

```
add lsn client LSN-NAT64-CLIENT-1

bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96

add lsn pool LSN-NAT64-POOL-1

bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70

add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96

```



```
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1

bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1

<!--NeedCopy-->
```

Einfache groß angelegte NAT64-Konfiguration mit einer erweiterten ACL6-Regel zur Identifizierung von Abonnenten:

```
add ns acl6 LSN-NAT64-ACL-2 ALLOW  - srcIPv6 = 2001:DB8:5002::20 - 2001:
    DB8:5002::200

apply acl6s

add lsn client LSN-NAT64-CLIENT-2

bind lsn client LSN-NAT64-CLIENT-2  - acl6name LSN-NAT64-ACL-2

add lsn pool LSN-NAT64-POOL-2

bind lsn pool LSN-NAT64-POOL-2 203.0.113.5-203.0.113.10

add lsn ip6profile LSN-NAT64-PROFILE-2 -type NAT64 -natprefix 2001:DB8
    :302::/96

add lsn group LSN-NAT64-GROUP-2 -clientname LSN-NAT64-CLIENT-2 -
    ip6profile LSN-NAT64-PROFILE-2

bind lsn group LSN-NAT64-GROUP-2 -poolname LSN-NAT64-POOL-2

<!--NeedCopy-->
```

Große NAT64-Konfiguration mit deterministischer NAT-Ressourcenzuweisung:

```
add lsn client LSN-NAT64-CLIENT-7

bind lsn client LSN-NAT64-CLIENT-7 -network6 2001:DB8:1002::7/128

add lsn pool LSN-NAT64-POOL-7 -nattype DETERMINISTIC

bind lsn pool LSN-NAT64-POOL-7 203.0.113.24-203.0.113.27

add lsn ip6profile LSN-NAT64-PROFILE-7 -type NAT64 -natprefix 2001:DB8
    :307::/96
```



```
10
11 add lsn group LSN-NAT64-GROUP-7 -clientname LSN-NAT64-CLIENT-7 -
       ip6profile LSN-NAT64-PROFILE-7 -nattype DETERMINISTIC -portblocksize
        256
12
13 bind lsn group LSN-NAT64-GROUP-7 -poolname LSN-POOL-7
14
15 <!--NeedCopy-->
```

Konfigurieren von Application Layer Gateways für Large Scale NAT64

May 11, 2023

Bei einigen Protokollen auf Anwendungsebene werden die IP-Adressen und Protokollportnummern auch in der Paket-Payload übermittelt. Das Application Layer Gateway für ein Protokoll analysiert die Payload des Pakets und nimmt die erforderlichen Änderungen vor, um sicherzustellen, dass das Protokoll auch über NAT64 in großem Maßstab funktioniert.

Die NetScaler-Appliance unterstützt ALG für die folgenden Protokolle für NAT64 in großem Maßstab:

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Application Layer Gateway für FTP-, ICMP- und TFTP-Protokolle

January 19, 2021

Sie können ALG für das FTP-Protokoll für eine große NAT64-Konfiguration aktivieren oder deaktivieren, indem Sie die Option FTP ALG der LSN-Gruppe der Konfiguration aktivieren oder deaktivieren.

ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es gibt keine Möglichkeit, es zu deaktivieren.

ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. TFTP ALG wird automatisch für eine groß angelegte NAT64-Konfiguration aktiviert, wenn Sie ein UDP LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport als 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

Application Layer Gateway für SIP-Protokoll

May 11, 2023

Die Verwendung von Large Scale NAT64 mit Session Initiation Protocol (SIP) ist kompliziert, da SIP-Nachrichten IP-Adressen sowohl in den SIP-Headern als auch im SIP-Body enthalten. Wenn LSN mit SIP verwendet wird, enthalten die SIP-Header Informationen über den Anrufer und den Empfänger, und das Gerät übersetzt diese Informationen, um sie vor dem externen Netzwerk zu verbergen. Der SIP-Text enthält die SDP-Informationen (Session Description Protocol), zu denen IP-Adressen und Portnummern für die Übertragung der Medien gehören. SIP ALG für NAT64 in großem Maßstab entspricht RFC 3261, RFC 3581, RFC 4566 und RFC 4475.

> **Hinweis**
>
> SIP ALG wird in einer eigenständigen NetScaler-Appliance, in einem NetScaler-Hochverfügbarkeits-Setup sowie in einem NetScaler-Cluster-Setup unterstützt.

Einschränkungen von SIP ALG

SIP-ALG für NAT64 in großem Maßstab weist die folgenden Einschränkungen auf:

- Nur SDP-Payload wird unterstützt.
- Folgende Komponenten werden nicht unterstützt:
  - Multicast-IP-Adressen
  - Verschlüsseltes SDP
  - SCHIFF BIS
  - FQDN-Übersetzung
  - SIP-Layer-Authentifizierung
  - Traffic-Domänen
  - Admin-Partitionen
  - Mehrteiliger Körper
  - Faltung der Leitung

Konfiguration von SIP ALG

Sie müssen die SIP ALG als Teil der LSN-Konfiguration konfigurieren. Anweisungen zur Konfiguration von LSN finden Sie unter Configuration Large Scale NAT64. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Stellen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter ein:
  - IP-Pooling = GEPAART
  - Adress- und Portzuordnung = ENDPUNKTUNABHÄNGIG

  - Filterung = ENDPUNKTUNABHÄNGIG
- Erstellen Sie ein SIP-ALG-Profil und stellen Sie sicher, dass Sie entweder den Quellportbereich oder den Zielportbereich definieren. Binden Sie das SIP-ALG-Profil an die LSN-Gruppe.
- Aktivieren Sie SIP ALG in der LSN-Gruppe.

So aktivieren Sie SIP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-sipalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

So aktivieren Sie SIP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn sipalgprofile <sipalgprofilename>[-dataSessionIdleTimeout <
    positive_integer>][-sipSessionTimeout <positive_integer>] [-
    registrationTimeout <positive_integer>] [-sipsrcportrange <port[-
    port]>] [-sipdstportrange <port[-port]>] [-openRegisterPinhole (
    ENABLED | DISABLED )] [-openContactPinhole ( ENABLED | DISABLED )]
    [-openViaPinhole ( ENABLED | DISABLED )] [-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP ) [-
    openRoutePinhole ( ENABLED | DISABLED )] [-rport ( ENABLED |
    DISABLED )]

show lsn sipalgprofile <sipalgprofilename
<!--NeedCopy-->
```

Beispielkonfiguration

Die folgende große NAT64-Beispielkonfiguration, SIP ALG, ist für TCP-Datenverkehr von Teilnehmergeräten im Netzwerk 2001 aktiviert: DB 8:1003: :/96.

```
add lsn client LSN-NAT64-CLIENT-9

Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96

Done
```



```
add lsn pool LSN-NAT64-POOL-9

Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90

Done
add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
   :309::/96

Done
add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
   mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done
add lsn sipalgprofile SIPALGPROFILE-9  -sipdstportrange 5060  -
   sipTransportProtocol TCP

Done
add lsn group LSN-NAT64-GROUP-9 -clientnameLSN-NAT64-CLIENT-9 -
   ip6profile LSN-NAT64-PROFILE-7 -sipalg ENABLED

Done
bind lsn group LSN-NAT64-GROUP-9 -poolnameLSN-NAT64-POOL-9
Done
bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
   PROFILE-9
Done
bind lsn group LSN-NAT64-GROUP-9 -sipalgprofilename SIPALGPROFILE-9
Done
<!--NeedCopy-->
```

Application Layer Gateway für das RTSP-Protokoll

May 11, 2023

Das Real Time Streaming Protocol (RTSP) ist ein Protokoll auf Anwendungsebene für die Übertragung von Mediendaten in Echtzeit. RTSP ist ein Kontrollkanalprotokoll zwischen dem Medienclient und dem Medienserver, das für die Einrichtung und Steuerung von Mediensitzungen zwischen Endpunkten verwendet wird. Die typische Kommunikation findet zwischen einem Client und einem Streaming-Media-Server statt.

Um Medien von einem privaten Netzwerk in ein öffentliches Netzwerk zu streamen, müssen IP-

Adressen und Portnummern über das Netzwerk übersetzt werden. Die NetScaler-Funktionalität umfasst ein Application Layer Gateway (ALG) für RTSP, das zusammen mit Large Scale NAT (LSN) verwendet werden kann, um den Medienstream zu analysieren und alle erforderlichen Änderungen vorzunehmen, um sicherzustellen, dass das Protokoll weiterhin über das Netzwerk funktioniert.

Wie die IP-Adressübersetzung durchgeführt wird, hängt vom Typ und der Richtung der Nachricht sowie von der Art der Medien ab, die von der Client-Server-Bereitstellung unterstützt werden. Nachrichten werden wie folgt übersetzt:

- Ausgehende Anfrage — Private IP-Adresse für eine öffentliche IP-Adresse im Besitz von NetScaler, die als LSN-IP-Adresse bezeichnet wird.
- Eingehende Antwort — LSN-IP-Adresse an private IP-Adresse.
- Eingehende Anfrage — keine Übersetzung.
- Ausgehende Antwort — Private IP-Adresse zur LSN-Pool-IP-Adresse.

> **Hinweis**
>
> RTSP ALG wird in einer eigenständigen NetScaler-Appliance, in einem NetScaler-Hochverfügbarkeits-Setup sowie in einem NetScaler-Cluster-Setup unterstützt.

Einschränkungen von RTSP ALG

Das RTSP-ALG unterstützt Folgendes nicht:

- Multicast-RTSP-Sitzungen
- RTSP-Sitzung über UDP
- Admin-Partitionen
- RTSP-Authentifizierung
- HTTP-Tunneling

Konfiguration von RTSP ALG

Konfigurieren Sie RTSP ALG als Teil der LSN-Konfiguration. Anweisungen zur Konfiguration von LSN finden Sie unter Configuring Large Scale NAT64. Achten Sie bei der Konfiguration darauf, dass Sie:

- Stellen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter ein:
  - IP-Pooling = GEPAART
  - Adress- und Portzuordnung = ENDPUNKTUNABHÄNGIG
  - Filterung = ENDPUNKTUNABHÄNGIG
- Aktivieren Sie RTSP ALG in der LSN-Gruppe
- Erstellen Sie ein RTSP-ALG-Profil und binden Sie das RTSP-ALG-Profil an die LSN-Gruppe.

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]

show lsn rtspalgprofile <rtspalgprofilename>
<!--NeedCopy-->
```

Beispiel für eine RTSP-ALG-Konfiguration

Die folgende groß angelegte NAT64-Beispielkonfiguration, RTSP ALG, ist für TCP-Verkehr von Abonnentengeräten im Netzwerk aktiviert 2001:DB 8:1002: :/96.

```
add lsn client LSN-NAT64-CLIENT-9
Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96
Done
add lsn pool LSN-NAT64-POOL-9
Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90
Done
add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
    :309::/96
Done
add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-9 -rtspIdleTimeout 1000 -
    rtspportrange 554
Done
```



```
add lsn group LSN-NAT64-GROUP-9 -clientname LSN-NAT64-CLIENT-9 -
   ip6profile LSN-NAT64-PROFILE-7 -rtspalg ENABLED
Done
bind lsn group LSN-NAT64-GROUP-9 -poolname LSN-NAT64-POOL-9
Done
bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
   PROFILE-9
Done
bind lsn group LSN-NAT64-GROUP-9  -rtspalgprofilename RTSPALGPROFILE-9
Done
<!--NeedCopy-->
```

Konfigurieren von statischen Large Scale NAT64-Maps

May 11, 2023

Die NetScaler-Appliance unterstützt die manuelle Erstellung von NAT64-Mappings, die die Zuordnung zwischen den folgenden Informationen enthalten:

- IP-Adresse und Port des Abonnenten
- NAT-IP-Adresse und Port

Statische, groß angelegte NAT64-Zuordnungen sind nützlich, wenn Sie sicherstellen möchten, dass die IPv4-Verbindungen, die zu einer NAT-IP-Adresse:Port initiiert wurden, IPv6-übersetzt und der Abonnenten-IP-Adresse:Port zugeordnet sind (z. B. Webserver im internen Netzwerk).

So erstellen Sie ein groß angelegtes NAT64-Mapping mithilfe der Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort>  [<
   natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Wildcard-Port Statische NAT64-Karten in großem Maßstab

Ein statischer großer NAT64-Zuordnungseintrag ist normalerweise eine Eins-zu-Eins-Zuordnung zwischen einem Abonnenten IPv6-Adresse:Port und einer NAT-IPv4-Adresse:Port. Ein statischer, groß angelegter NAT64-Mapping-Eintrag im Eins-zu-Eins-Format macht nur einen Port der Abonnenten-IP-Adresse für das Internet verfügbar.

In einigen Situationen kann es erforderlich sein, alle Ports (64 KB — begrenzt auf die maximale Anzahl von Ports einer NAT-IPv4-Adresse) einer Abonnenten-IP-Adresse für das Internet verfügbar zu machen (z. B. ein Server, der in einem internen Netzwerk gehostet wird und an jedem Port einen anderen Dienst ausführt). Um diese internen Dienste über das Internet zugänglich zu machen, müssen Sie alle Ports des Servers dem Internet zugänglich machen.

Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, 64.000 statische Eins-zu-Eins-Zuordnungseinträge hinzuzufügen, einen Zuordnungseintrag für jeden Port. Das Erstellen dieser Einträge ist sehr umständlich und eine große Aufgabe. Außerdem kann diese große Anzahl von Konfigurationseinträgen zu Leistungsproblemen in der NetScaler-Appliance führen.

Eine einfachere Methode besteht darin, Platzhalterports in einem statischen Zuordnungseintrag zu verwenden. Sie müssen nur einen statischen Mapping-Eintrag erstellen, bei dem die Parameter NAT-Port und Subscriber-Port auf das Platzhalterzeichen (*) gesetzt sind und der Protokollparameter auf ALL gesetzt ist, um alle Ports einer Abonnenten-IP-Adresse für alle Protokolle für das Internet verfügbar zu machen.

Bei eingehenden oder ausgehenden Verbindungen eines Abonnenten, die einem statischen Platzhalterzuordnungseintrag entsprechen, ändert sich der Port des Abonnenten nach dem NAT-Vorgang nicht. Wenn eine vom Abonnenten initiierte Verbindung zum Internet mit einem statischen Platzhaltereintrag übereinstimmt, weist die NetScaler-Appliance einen NAT-Port zu, der dieselbe Nummer wie der Abonnentenport hat, von dem aus die Verbindung initiiert wird. In ähnlicher Weise wird ein Internet-Host mit dem Port eines Abonnenten verbunden, indem er sich mit dem NAT-Port verbindet, der dieselbe Nummer wie der Port des Abonnenten hat.

Um die NetScaler-Appliance so zu konfigurieren, dass sie Zugriff auf alle Ports einer Abonnenten-IPv6-Adresse bietet, erstellen Sie eine statische Wildcard-Map mit den folgenden obligatorischen Parametereinstellungen:

- protocol=Alle
- Abonnenten-Port = *
- NAT-Anschluss = *

In einer statischen Wildcard-Map ist im Gegensatz zu einer statischen Eins-zu-Eins-Map das Festlegen des NAT-IP-Parameters obligatorisch. Außerdem kann die einer statischen Wildcard-Map zugewiesene NAT-IP-Adresse nicht für andere Abonnenten verwendet werden.

So erstellen Sie mithilfe der Befehlszeilenschnittstelle eine statische Wildcard-Map

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
     positive_integer>] [-destIP <ip_addr>
2
3 show lsn static
4 <!--NeedCopy-->
```


In der folgenden Beispielkonfiguration einer statischen Wildcard-Map werden alle Ports eines Abonnenten, dessen IP-Adresse 2001:DB 8:5001: :3 lautet, über NAT-IP 203.0.11.33 zugänglich gemacht.

```
1 add lsn static NAT64-WILDCARD-STATIC-1 ALL 2001:DB8:5001::3 *
     203.0.113.33 *
2 Done
3 <!--NeedCopy-->
```

Protokollieren und Überwachen von Large Scale NAT64

May 11, 2023

Sie können umfangreiche NAT64-Informationen protokollieren, um Probleme zu diagnostizieren und zu beheben und gesetzliche Anforderungen zu erfüllen. Sie können die Leistung der groß angelegten NAT64-Bereitstellung überwachen, indem Sie statistische Zähler verwenden und die entsprechenden aktuellen Sitzungen anzeigen.

NAT64 im großen Maßstab protokollieren

Die Protokollierung umfangreicher NAT64-Informationen ist für ISPs erforderlich, um die gesetzlichen Anforderungen zu erfüllen und die Quelle des Datenverkehrs zu einem bestimmten Zeitpunkt zu identifizieren.

Eine Protokollnachricht für einen umfangreichen NAT64-Mapping-Eintrag besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt.
- Zeitstempel.
- Eintragstyp (MAPPING).
- Ob der Zuordnungseintrag erstellt oder gelöscht wurde.
- IP-Adresse, Port und Domain-ID des Abonnenten.
- NAT-IP-Adresse und Port.
- Name des Protokolls.
- Abhängig von den folgenden Bedingungen können Ziel-IP-Adresse, Port und Verkehrsdomänen-ID vorhanden sein:
  - Ziel-IP-Adresse und Port werden für die endpunktunabhängige Zuordnung nicht protokolliert.
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.

- Die Ziel-IP-Adresse und der Port werden für die adressportabhängige Zuordnung protokolliert.

Eine Protokollnachricht für eine groß angelegte NAT64-Sitzung besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Art des Eintrags (SESSION)
- Ob die Sitzung erstellt oder entfernt wurde
- IP-Adresse, Port und Domain-ID des Abonnenten
- NAT-IP-Adresse und Port
- Name des Protokolls
- Ziel-IP-Adresse, Port und Traffic-Domain-ID

In der folgenden Tabelle werden Beispiele für umfangreiche NAT64-Protokolleinträge der einzelnen Typen angezeigt, die auf den konfigurierten Protokollservern gespeichert sind. Die Protokolleinträge zeigen, dass ein Abonnent, dessen IPv6-Adresse 2001:db 8:5001: :9 ist, am 7. April 2016 von 14:07:57 GMT bis 14:10:59 GMT über NAT-IP:Port 203.0.113. 63:45195 mit dem Ziel-IP:Port 23.0.0. 1:80 verbunden war.

Art des Protokolleintrags	Beispiel für einen Logeintrag
Erstellung einer Sitzung	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_SESSION 5532 0 : SESSION CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Erstellung von Kartografie	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_ADDR_MAPPING 5533 0 : ADM CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Löschen einer Sitzung	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_SESSION 25012 0 : SESSION DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Art des Protokolleintrags	Beispiel für einen Logeintrag
Löschen von Zuordnungen	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Konfigurationsschritte

Sie können die Protokollierung umfangreicher NAT64-Informationen für eine umfangreiche NAT64-Konfiguration konfigurieren, indem Sie die Protokollierungs- und Sitzungsprotokollierungsparameter der LSN-Gruppen festlegen. Dies sind Parameter auf Gruppenebene und sind standardmäßig deaktiviert. Die NetScaler-Appliance protokolliert große NAT64-Sitzungen für eine LSN-Gruppe nur, wenn sowohl die Protokollierungs- als auch die Sitzungsprotokollierungsparameter aktiviert sind.

Die folgende Tabelle zeigt das Protokollierungsverhalten für eine LSN-Gruppe für verschiedene Einstellungen der Protokollierungs- und Sitzungsprotokollparameter.

Protokollierung	Sitzungsprotokollierung	Verhalten protokollieren
Aktiviert	Aktiviert	Protokolliert LSN-Zuordnungseinträge sowie LSN-Sitzungen
Aktiviert	Deaktiviert	Protokolliert LSN-Zuordnungseinträge, aber keine LSN-Sitzungen
Deaktiviert	Aktiviert	Protokolliert weder Mapping-Einträge noch LSN-Sitzungen

Um umfangreiche NAT64-Informationen mit der CLI zu protokollieren

Um die Protokollierungs- und Sitzungsprotokollierungsparameter beim Hinzufügen einer LSN-Gruppe festzulegen, geben Sie an der Befehlszeile Folgendes ein:

```
1 add lsn group <groupname> -clientname <string> [-logging (ENABLED|
      DISABLED)] [-sessionLogging (ENABLED|DISABLED)]
2
```



```
3 show lsn group
4 <!--NeedCopy-->
```

Um die Protokollierungs- und Sitzungsprotokollparameter für eine bestehende LSN-Gruppe festzulegen, geben Sie an der Befehlszeile Folgendes ein:

```
1 set lsn group <groupname> [-logging (ENABLED|DISABLED)] [-
     sessionLogging (ENABLED|DISABLED)]
2
3 show lsn group
4 <!--NeedCopy-->
```

Beispielkonfiguration

In diesem Beispiel einer groß angelegten NAT64-Konfiguration sind die Protokollierungs- und Sitzungsprotokollierungsparameter für die LSN-Gruppe LSN-NAT64-GROUP-1 aktiviert.

Die NetScaler-Appliance protokolliert umfangreiche NAT64-Sitzungs- und Zuordnungsinformationen für Verbindungen von Abonnenten (im Netzwerk 2001:DB 8:5001: :/96).

Beispielkonfiguration:

```
1  add lsn client LSN-NAT64-CLIENT-1 Done
2  Done
3  bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
4  Done
5  add lsn pool LSN-NAT64-POOL-1
6  Done
7  bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
8  Done
9  add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
10 Done
11 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1  -logging ENABLED -sessionLogging
      ENABLED
12 Done
13 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
14 Done
15 <!--NeedCopy-->
```


Protokollierung von MSISDN-Informationen für NAT64 im großen Maßstab

Eine Mobile Station Integrated Subscriber Directory Number (MSISDN) ist eine Telefonnummer, die einen Teilnehmer in mehreren Mobilfunknetzen eindeutig identifiziert. Die MSISDN ist mit einer Landesvorwahl und einer nationalen Zielvorwahl verknüpft, die den Betreiber des Abonnenten identifizieren.

Sie können eine NetScaler-Appliance so konfigurieren, dass MSISDNS in großen NAT64-LSN-Protokolleinträgen für Abonnenten in Mobilfunknetzen enthalten ist. Das Vorhandensein von MSISDNS in den LSN-Protokollen ermöglicht eine schnellere und genauere Rückverfolgung eines Mobilfunkabonnenten, der gegen eine Richtlinie oder ein Gesetz verstoßen hat oder dessen Informationen von rechtmäßigen Abhörbehörden angefordert werden.

Die folgenden LSN-Beispielprotokolleinträge enthalten MSISDN-Informationen für eine Verbindung von einem mobilen Abonnenten in einer LSN-Konfiguration. Die Protokolleinträge zeigen, dass ein Mobilfunkabonnent, dessen MSISDN E 164:5556543210 ist und dessen IPv6-Adresse 2001:db 8:5001: :9 lautet, am 7. April 2016 von 14:07:57 GMT bis 14:10:59 GMT über den NAT-IP:Port 203.0.113. 63:45195 mit dem Ziel-IP:Port 23.0.0. 1:80 verbunden war.

Art des Protokolleintrags	Beispiel für einen Logeintrag
Erstellung einer Sitzung	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_SESSION 5532 0 : SESSION CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Erstellung von Kartografie	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_ADDR_MAPPING 5533 0 : ADM CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Löschen einer Sitzung	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_SESSION 25012 0 : SESSION DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Art des Protokolleintrags	Beispiel für einen Logeintrag
Löschen von Zuordnungen	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um MSISDN-Informationen in die LSN-Protokolle aufzunehmen:

- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den Log-Abonnenten-ID-Parameter, der angibt, ob die MSISDN-Informationen in die LSN-Protokolle einer LSN-Konfiguration aufgenommen werden sollen oder nicht.
- Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration. Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter für den Protokollprofilnamen auf den Namen des erstellten LSN-Protokollprofils festlegen. MSISDN-Informationen sind in allen LSN-Protokollen enthalten, die sich auf Mobilfunkabonnenten dieser LSN-Gruppe beziehen.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn logprofile <logprofilename> -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie ein LSN-Protokollprofil mit der CLI an eine LSN-Gruppe einer NAT64-LSN-Konfiguration

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
```



```
<!--NeedCopy-->
```

Beispielkonfiguration

In diesem Beispiel einer NAT64-LSN-Konfiguration ist für das LSN-Protokollprofil LOG-PROFILE-MSISDN-1 der Log-Abonnenten-ID-Parameter aktiviert. LOG-PROFILE-MSISDN-1 ist an die LSN-Gruppe LSN-NAT64-GROUP-1 gebunden. MSISDN-Informationen sind in den LSN-Sitzungs- und LSN-Zuordnungsprotokollen für Verbindungen von Mobilfunkteilnehmern enthalten (im Netzwerk 2001:DB8:5001::/96).

```
add lsn logprofile  LOG-PROFILE-MSISDN-1  -logSubscriberID ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1 -logprofilename  LOG-PROFILE-MSISDN-1
Done
<!--NeedCopy-->
```

Kompaktes Logging für NAT in großem Maßstab

Die Protokollierung von LSN-Informationen ist eine der wichtigen Funktionen, die ISPs benötigen, um die gesetzlichen Anforderungen zu erfüllen und die Quelle des Datenverkehrs jederzeit identifizieren zu können. Dies führt letztendlich zu einer riesigen Menge an Protokolldaten, sodass die ISPs große Investitionen tätigen müssen, um die Protokollierungsinfrastruktur aufrechtzuerhalten.

Compact Logging ist eine Technik zur Reduzierung der Protokollgröße, indem eine Notationsänderung verwendet wird, bei der Kurzcodes für Ereignis- und Protokollnamen verwendet werden.

Zum Beispiel C für Client, SC für Sitzung erstellt und T für TCP. Die kompakte Protokollierung führt zu einer durchschnittlichen Reduzierung der Protokollgröße um 40 Prozent.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um LSN-Informationen im Kompaktformat zu protokollieren:

1. Erstellen Sie ein LSN-Protokollprofil. Ein LSN-Protokollprofil enthält den Parameter Log Compact, der angibt, ob Informationen für eine LSN-Konfiguration im kompakten Format protokolliert werden sollen oder nicht.
2. Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration. Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter Log-Profilname auf den Namen des erstellten LSN-Protokollprofils setzen. Alle Sitzungen und Zuordnungen für diese LSN-Gruppe werden im kompakten Format protokolliert.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

LSN-Protokollprofil mithilfe der CLI an eine LSN-Gruppe einer LSN-Konfiguration binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Beispielkonfiguration für NAT64:

```
add lsn logprofile  LOG-PROFILE-COMPACT-1 -logCompact ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
```



```
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - logProfileName LOG-PROFILE-COMPACT-1
Done
<!--NeedCopy-->
```

Loggen von HTTP-Header-Informationen

Die NetScaler-Appliance kann Anforderungsheaderinformationen einer HTTP-Verbindung protokollieren, die die NetScaler Large Scale NAT64-Funktionalität verwendet. Die folgenden Header-Informationen eines HTTP-Anforderungspakets können protokolliert werden:

- URL, für die die HTTP-Anfrage bestimmt ist
- In der HTTP-Anfrage angegebene HTTP-Methode
- In der HTTP-Anfrage verwendete HTTP-Version
- IPv6-Adresse des Abonnenten, der die HTTP-Anfrage gesendet hat

Die HTTP-Header-Logs können von ISPs verwendet werden, um die Trends im Zusammenhang mit dem HTTP-Protokoll bei einer Gruppe von Abonnenten zu ermitteln. Ein ISP kann diese Funktion beispielsweise verwenden, um die beliebteste Website unter einer Gruppe von Abonnenten herauszufinden.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um die NetScaler-Appliance für die Protokollierung von HTTP-Header-Informationen zu konfigurieren:

- Erstellen Sie ein HTTP-Header-Logprofil. Ein HTTP-Header-Logprofil ist eine Sammlung von HTTP-Header-Attributen (z. B. URL und HTTP-Methode), die für die Protokollierung aktiviert oder deaktiviert werden können.
- Binden Sie den HTTP-Header an eine LSN-Gruppe einer groß angelegten NAT64-Konfiguration. Binden Sie das HTTP-Header-Logprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter für den Namen des HTTP-Header-Logprofils auf den Namen des erstellten HTTP-Header-Logprofils setzen. Die NetScaler-Appliance protokolliert dann die HTTP-Header-Informationen aller HTTP-Anfragen, die sich auf die LSN-Gruppe beziehen.

Ein HTTP-Header-Logprofil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein HTTP-Header-Logprofil haben.

HTTP-Header-Logprofil mithilfe der Befehlszeilenschnittstelle erstellen

Geben Sie in der Befehlszeile Folgendes ein:

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED | DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion ( ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

show lsn httphdrlogprofile
<!--NeedCopy-->
```

HTTP-Header-Logprofil mithilfe der Befehlszeilenschnittstelle an eine LSN-Gruppe binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Beispielkonfiguration

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done
add lsn client LSN-NAT64-CLIENT-1 Done
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8:300::/96
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
```



```
bind lsn group LSN-NAT64-GROUP-1 -httphdrlogprofilename HTTP-HEADER-LOG
    -1
Done
<!--NeedCopy-->
```

Aktuelle NAT64-Sitzungen im großen Maßstab anzeigen

Sie können die aktuellen großen NAT64-Sitzungen anzeigen, um unerwünschte oder ineffiziente Sitzungen auf der NetScaler-Appliance zu erkennen. Sie können alle oder einige große NAT64-Sitzungen auf der Grundlage von Auswahlparametern anzeigen.

> **Hinweis**
>
> Wenn mehr als eine Million Large Scale NAT64-Sitzungen auf der NetScaler-Appliance vorhanden sind, empfiehlt Citrix, die Auswahlparameter zu verwenden, um ausgewählte Large Scale NAT64-Sitzungen anzuzeigen, anstatt sie alle anzuzeigen.

Um alle Large Scale NAT64-Sitzungen mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
show lsn session  -nattype NAT64
<!--NeedCopy-->
```

Ausgewählte Large Scale NAT64-Sitzungen mit der Befehlszeilenschnittstelle anzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
show lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

NAT64-Statistiken in großem Maßstab anzeigen

Sie können Statistiken zu einem großen NAT64-Modul anzeigen und dessen Leistung bewerten oder Probleme beheben. Sie können eine Zusammenfassung der Statistiken aller großen NAT64-Konfigurationen oder einer bestimmten großen NAT64-Konfiguration anzeigen. Die statistischen Zähler geben Ereignisse seit dem letzten Neustart der NetScaler-Appliance wieder. Alle diese Zähler werden auf 0 zurückgesetzt, wenn die NetScaler-Appliance neu gestartet wird.

Large Scale NAT64-Gesamtstatistiken mithilfe der Befehlszeilenschnittstelle anzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat lsn nat64
<!--NeedCopy-->
```

Statistiken für eine angegebene Large Scale NAT64-Konfiguration mithilfe der Befehlszeilenschnittstelle anzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat lsn group <groupname>
<!--NeedCopy-->
```

Löschen großer NAT64-Sitzungen

Sie können alle unerwünschten oder ineffizienten NAT64-Sitzungen in großem Maßstab von der NetScaler-Appliance entfernen. Die Appliance gibt sofort die für diese Sitzungen zugewiesenen Ressourcen (wie NAT-IP-Adresse, Port und Speicher) frei, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance verwirft auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte Large Scale NAT64-Sitzungen von der NetScaler-Appliance entfernen.

So löschen Sie alle Large Scale NAT64-Sitzungen mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session -nattype NAT64

show lsn session -nattype NAT64
<!--NeedCopy-->
```

Ausgewählte Large Scale NAT64-Sitzungen mithilfe der Befehlszeilenschnittstelle löschen

Geben Sie in der Befehlszeile Folgendes ein:

```
flush lsn session -nattype NAT64 [-network6 <ipv6_addr|*>] [-
    clientname <string>] [-natIP <ip_addr> [-natPort <port>]]

show lsn session -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
     <string>] [-natIP <ip_addr> [-natPort <port>]]
```



```
<!--NeedCopy-->
```

Beispielkonfiguration:

Löschen Sie alle großen NAT64-Sitzungen, die auf einer NetScaler-Appliance vorhanden sind

```
flush lsn session  -nattype NAT64
Done
<!--NeedCopy-->
```

Löscht alle großen NAT64-Sitzungen, die sich auf die Client-Entität LSN-NAT64-CLIENT-1 beziehen

```
flush lsn session -nattype NAT64 -clientname LSN-NAT64-CLIENT-1
Done
<!--NeedCopy-->
```

Löschen Sie alle großen NAT64-Sitzungen, die sich auf ein Abonnentennetzwerk (2001:DB 8:5001::/96) der LSN-Client-Entität LSN-NAT64-CLIENT-2 beziehen

```
flush lsn session -nattype NAT64 -network6 2001:DB8:5001::/96 -
   clientname LSN-NAT64-CLIENT-2
Done
<!--NeedCopy-->
```

IPFIX-Protokollierung

Die NetScaler-Appliance unterstützt das Senden von Informationen über LSN-Ereignisse im IPFIX-Format (Internet Protocol Flow Information Export) an den konfigurierten Satz von IPFIX Collector (s). Die Appliance verwendet die vorhandene AppFlow-Funktion, um LSN-Ereignisse im IPFIX-Format an die IPFIX-Collectors zu senden.

IPFIX-basiertes Logging ist für die folgenden NAT64-bezogenen Ereignisse verfügbar:

- Erstellen oder Löschen einer LSN-Sitzung.
- Erstellung oder Löschung eines LSN-Mapping-Eintrags.
- Zuweisung oder Entzuweisung von Portblöcken im Kontext von deterministischem NAT.
- Zuweisung oder Entzuweisung von Portblöcken im Kontext von dynamischem NAT.
- Immer wenn das Kontingent für Abonnentensitzungen überschritten wird.

Punkte, die Sie beachten sollten, bevor Sie die IPFIX-Protokollierung konfigurieren

Bevor Sie mit der Konfiguration von IPSec ALG beginnen, sollten Sie die folgenden Punkte berücksichtigen:

- Sie müssen die AppFlow Funktion und die IPFIX-Kollektoren auf der NetScaler Appliance konfigurieren. Anweisungen finden Sie unter Konfigurieren der AppFlow-Funktion.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um LSN-Informationen im IPFIX-Format zu protokollieren:

- **Aktivieren Sie die LSN-Protokollierung in der AppFlow-Konfiguration**. Aktivieren Sie den LSN-Logging-Parameter als Teil der AppFlow-Konfiguration.
- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den IPFIX-Parameter, der die Protokollinformationen im IPFIX-Format aktiviert oder deaktiviert.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das LSN-Protokollprofil an eine oder mehrere LSN-Gruppe (n). Ereignisse, die sich auf die gebundene LSN-Gruppe beziehen, werden im IPFIX-Format protokolliert.

So aktivieren Sie die LSN-Protokollierung in der AppFlow-Konfiguration mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Um mithilfe der CLI ein LSN-Protokollprofil zu erstellen, geben Sie in der Befehlszeile Folgendes ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie das LSN-Protokollprofil mithilfe der CLI an eine LSN-Gruppe einer LSN-Konfiguration

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```


So erstellen Sie ein LSN-Protokollprofil mithilfe der GUI

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf die Registerkarte **Protokoll** und fügen Sie dann ein Protokollprofil hinzu.

So binden Sie das LSN-Protokollprofil mithilfe der GUI an eine LSN-Gruppe einer LSN-Konfiguration

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group und** öffnen Sie die **LSN-Gruppe** .
2. Klicken Sie **unter Erweiterte Einstellungen** auf **+ Protokollprofil**, um das erstellte Protokollprofil an die LSN-Gruppe zu binden.

Portsteuerungsprotokoll für Large Scale NAT64

May 11, 2023

NetScaler-Appliances unterstützen jetzt das Port Control Protocol (PCP) für Large Scale NAT (LSN). Viele der Abonnentenanwendungen eines Internetdienstanbieters müssen über das Internet zugänglich sein (z. B. IoT-Geräte (Internet of Things), wie z. B. eine IP-Kamera, die die Überwachung über das Internet ermöglicht). Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, statische großskalige NAT-Karten (LSN) zu erstellen. Für eine sehr große Anzahl von Abonnenten ist die Erstellung statischer LSN-NAT-Maps jedoch keine praktikable Lösung.

Das Port Control Protocol (PCP) ermöglicht es einem Abonnenten, spezifische LSN-NAT-Zuordnungen für sich selbst und/oder für andere Geräte von Drittanbietern anzufordern. Das große NAT-Gerät erstellt eine LSN-Map und sendet sie an den Abonnenten. Der Abonnent sendet den Remote-Geräten im Internet die NAT-IP-Adresse: NAT-Port, an dem sie sich mit dem Abonnenten verbinden können.

Anwendungen senden in der Regel häufig Keep-Alive-Nachrichten an das große NAT-Gerät, damit ihre LSN-Zuordnungen nicht zu einem Timeout führen. PCP trägt dazu bei, die Häufigkeit solcher Keep-Alive-Nachrichten zu reduzieren, indem es den Anwendungen ermöglicht, die Timeout-Einstellungen der LSN-Zuordnungen zu erlernen. Dies trägt dazu bei, den Bandbreitenverbrauch im Zugangsnetz des ISP und den Batterieverbrauch auf Mobilgeräten zu reduzieren.

PCP ist ein Client-Server-Modell und läuft über das UDP-Transportprotokoll. Eine NetScaler-Appliance implementiert die PCP-Serverkomponente und entspricht RFC 6887.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben zur Konfiguration von PCP aus:

- **(Optional) Erstellen Sie ein PCP-Profil**. Ein PCP-Profil enthält Einstellungen für PCP-bezogene Parameter (z. B. um auf Mapping- und Peer-PCP-Anfragen zu warten). Ein PCP-Profil kann an einen PCP-Server gebunden werden. Ein an einen PCP-Server gebundenes PCP-Profil wendet alle seine Einstellungen auf den PCP-Server an. Ein PCP-Profil kann an mehrere PCP-Server gebunden werden. Standardmäßig ist ein PCP-Profil mit Standardparametereinstellungen an alle PCP-Server gebunden. Ein PCP-Profil, das Sie an einen PCP-Server binden, überschreibt die standardmäßigen PCP-Profileinstellungen für diesen Server. Ein Standard-PCP-Profil hat die folgenden Parametereinstellungen:
  - Zuordnung: Aktiviert
  - Peer: Aktiviert
  - Minimale Lebensdauer der Karte: 120 Sekunden
  - Maximale Lebensdauer: 86400 Sekunden
  - Anzahl ankündigen: 10
  - Drittanbieter: Deaktiviert
- **Erstellen Sie einen PCP-Server und binden Sie ein PCP-Profil daran**. Erstellen Sie einen PCP-Server auf der NetScaler-Appliance, um auf PCP-bezogene Anfragen und Nachrichten der Abonnenten zu warten. Einem PCP-Server muss eine Subnetz-IP-Adresse (SNIP) oder (SNIP6) zugewiesen werden, um darauf zugreifen zu können. Standardmäßig überwacht ein PCP-Server Port 5351.
- **Binden Sie den PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie den erstellten PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den PCP-Serverparameter so festlegen, dass der erstellte PCP-Server angegeben wird. Auf den erstellten PCP-Server können nur die Abonnenten dieser LSN-Gruppe zugreifen.

> **Hinweis**
>
> Ein PCP-Server für eine umfangreiche NAT-Konfiguration bedient keine Anfragen von Abonnenten, die anhand der ACL-Regeln identifiziert werden.

So erstellen Sie ein PCP-Profil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```


So erstellen Sie einen PCP-Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Beispielkonfiguration für NAT64

In der folgenden Beispielkonfiguration ist der PCP-Server PCP-SERVER-1 mit den PCP-Einstellungen von PCP-PROFILE-1 an die LSN-Gruppe LSN-NAT64-GROUP-1 gebunden. PCP-SERVER-1 bedient PCP-Anfragen von IPv6-Abonnenten im Netzwerk 2001:DB 8:5001: :/96.

Beispielkonfiguration:

```
add pcp profile PCP-PROFILE-1 -minMapLife 400
Done
add pcp server PCP-SERVER-1 2001:DB8:6001::90  -pcpProfile PCP-PROFILE
    -1
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - pcpServer PCP-NAT64-SERVER-1
Done
<!--NeedCopy-->
```


LSN64 in einem Cluster-Setup

May 11, 2023

Große NAT64-Konfigurationen werden in einem NetScaler-Cluster-Setup unterstützt.

Ein NetScaler-Cluster ist eine Gruppe von NetScaler-Appliances, die als ein einzelnes System konfiguriert und verwaltet werden. Ein NetScaler-Cluster bietet Skalierbarkeit und Verfügbarkeit. Jede NetScaler-Appliance in einem Cluster-Setup fungiert als unabhängige LSN-Entität und wird als einzelnes System verwaltet.

Die LSN-Konfiguration in einem Cluster-Setup ist dieselbe wie in einer eigenständigen Appliance, mit der Ausnahme, dass ein bestimmter Pool von LSN-IP-Adressen jeweils nur einem Knoten gehört. Mit anderen Worten, eine LSN-IP-Pool-Entität ist als Spott-Entität in einem bestimmten Knoten konfiguriert. Alle Knoten eines Cluster-Setups können eine bestimmte LSN-IP-Pool-Entität haben. Um sicherzustellen, dass die Pakete, die sich auf eine LSN-Sitzung beziehen, auf demselben Clusterknoten empfangen werden, der den NAT-Vorgang ausgeführt hat, ist Policy Based Backplane (PBS) Steering konfiguriert. PBS leitet die empfangenen zugehörigen Pakete einer LSN-Sitzung an denselben Clusterknoten weiter.

Beispielkonfiguration:

```
add lsn client LSN-NAT64-CLIENT-1

Done

bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96

Done

add lsn pool LSN-NAT64-POOL-1

Done

bind lsn pool LSN-NAT64-POOL-1 -ownerNode 1  203.0.113.61 -
    203.0.113.70

Done

bind lsn pool LSN-NAT64-POOL-1 -ownerNode 2  203.0.113.101 -
    203.0.113.110

Done

```



```
21 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
22
23 Done
24
25 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
26
27 Done
28
29 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
30
31 Done
32
33 add ns acl6 NAT64-DFD ALLOW -srcIPv6 = 2001:DB8:5001:: -type DFD -
      dfdhash SIP -dfdprefix 64
34
35 Done
36
37 apply ns acls6 -type DFD
38
39 Done
40 <!--NeedCopy-->
```

Zuordnung von Adresse und Port mit Übersetzung

May 11, 2023

Mapping Address and Port using Translation (MAP-T) ist eine IPv6-Übergangslösung für ISPs mit IPv6-Infrastruktur, um ihre IPv4-Abonnenten mit dem IPv4-Internet zu verbinden. Sie_.MAP-T basiert auf zustandslosen IPv4- und IPv6-Adressübersetzungstechnologien. MAP-T ist ein Mechanismus, der eine doppelte Übersetzung (IPv4 zu IPv6 und umgekehrt) auf Kundenendgeräten (CE) und Grenzroutern (im ISP-Kernnetzwerk) durchführt.

In einer MAP-T-Bereitstellung implementiert das CE-Gerät eine Kombination aus statusfähiger NAPT44-Übersetzung und statusloser NAT46-Übersetzung. Das CE-Gerät erhält NAT-IP und den Portblock, der für die Übersetzung über DHCPv6 oder eine andere Methode verwendet werden soll.

Wenn ein IPv4-Paket von einem Abonnentengerät auf dem CE-Gerät ankommt, führt das CE-Gerät NAPT44 durch und speichert die NAPT44-Bindungsinformationen. Nach der NAT44-Übersetzung wird das Paket einer NAT46-Übersetzung unterzogen und dann an das Border Router (BR) -Gerät weitergeleitet, das sich im Kernnetzwerk des ISP befindet. Das BR-Gerät empfängt die IPv6-Pakete

vom CE-Gerät, extrahiert und validiert die im IPv6-Header eingebettete NAT-IP und den Portblock und leitet das IPv4-Paket an das IPv4-Internet weiter. Wenn der BR das IPv4-Paket aus dem Internet empfängt, übersetzt er das IPv4-Paket in ein IPv6-Paket und sendet das IPv6-Paket an das CE-Gerät.

MAP-T ist auf einem BR-Gerät statuslos, sodass das BR-Gerät nicht NAT für den Datenverkehr ausführt. Stattdessen wird die NAT-Funktionalität an die CE-Geräte delegiert. Dank dieser Delegierungs- und Statusfunktion in BR-Geräten kann die BR-Bereitstellung proportional zum Verkehrsaufkommen skaliert werden.

Die NetScaler-Appliance implementiert die BR-Funktionalität einer MAP-T-Lösung, wie in RFC 7599 beschrieben.

Konfiguration von MAP-T

Die Konfiguration von MAP-T auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- Fügen Sie eine Standard-Zuordnungsregel hinzu
- Fügen Sie eine grundlegende Zuordnungsregel hinzu
- Binden Sie einen IPv4-NAT-Adressbereich von CE-Geräten an eine grundlegende Zuordnungsregel
- Fügen Sie eine Zuordnungsdomäne hinzu und binden Sie eine grundlegende Zuordnungsregel und eine Standardzuordnungsregel an die Domäne

So fügen Sie mithilfe der CLI eine Standard-Zuordnungsregel hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add MapDmr <name> -BRIpv6Prefix ( <ipv6_addr> | <*> )

show MapDmr <name>
<!--NeedCopy-->
```

So fügen Sie mithilfe der CLI eine grundlegende Zuordnungsregel hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add MapBmr <name> -RuleIpv6Prefix <ipv6_addr> | <*>  [-psidoffset <
    positive_integer>] [-EAbitLength <positive_integer>]  [-psidlength <
    positive_integer>]

show MapBmr <name>
<!--NeedCopy-->
```


So binden Sie den IPv4-NAT-Adressbereich von CE-Geräten mithilfe der CLI an eine grundlegende Zuordnungsregel

Geben Sie in der Befehlszeile Folgendes ein:

```
bind MapBmr <name> (-network <ip_addr>  [-netmask <netmask>])

show MapBmr <name>
<!--NeedCopy-->
```

So fügen Sie eine Map-Domain mithilfe der CLI hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add MapDomain <name> -MapDmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

So binden Sie eine grundlegende Zuordnungsregel mithilfe der CLI an eine Kartendomäne

Geben Sie in der Befehlszeile Folgendes ein:

```
bind MapDomain <name> -MapBmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

Beispiel-Konfiguration

```
add mapdmr DMR-1 -BRIpv6Prefix 2002:db8::/64

Done

add mapbmr BMR-1 -ruleIpv6Prefix 2002:db8:89ab::/48 -eAbitLength 16 -
    psidlength 8 -psidoffset 6

Done

bind mapbmr BMR-1 -network 192.0.1.0 -netmask 255.255.255.0

Done

```



```
13 add MapDomain MAP-DOMAIN-1 -mapdmrname DMR-1
14
15 Done
16
17 bind MapDomain MAP-DOMAIN-1 -mapbmrname BMR-1
18 Done
19 <!--NeedCopy-->
```

Telekommunikations-Abonnentenmanagement

May 11, 2023

Die Anzahl der Abonnenten in einem Telekommunikationsnetz nimmt in einem beispiellosen Tempo zu, und ihre Verwaltung wird für Dienstanbieter zu einer Herausforderung. Neuere, schnellere und intelligentere Geräte stellen hohe Anforderungen an das Netzwerk und die Abonnentenverwaltungssysteme. Es ist nicht mehr möglich, jedem Abonnenten den gleichen Servicestandard zu bieten, und die Notwendigkeit einer Verarbeitung des Datenverkehrs für jeden Abonnenten ist unerlässlich.

Die NetScaler-Appliance stellt die Informationen bereit, um Abonnenten auf der Grundlage ihrer in der Policy and Charging Rules Function (PCRF) gespeicherten Informationen zu profilieren. Wenn ein mobiler Abonnent eine Verbindung zum Internet herstellt, ordnet das Paket-Gateway dem Abonnenten eine IP-Adresse zu und leitet das Datenpaket an das Gerät weiter. Die Appliance empfängt die Abonnenteninformationen dynamisch, oder Sie können statische Abonnenten konfigurieren. Diese Informationen ermöglichen es der Appliance, ihre umfassenden Traffic-Management-Funktionen wie Content Switching, integriertes Caching, Rewrite und Responder auf Abonnentenbasis anzuwenden, um den Datenverkehr zu verwalten.

Bevor Sie die NetScaler-Appliance für die Verwaltung von Abonnenten konfigurieren, müssen Sie dem Modul, das Abonnentensitzungen speichert, Speicher zuweisen. Für dynamische Abonnenten müssen Sie eine Schnittstelle konfigurieren, über die die Appliance Sitzungsinformationen empfängt. Statischen Abonnenten müssen IDs zugewiesen werden, und Sie können sie mit Richtlinien verknüpfen.

Sie können auch Folgendes tun:

- Durchsetzung und Verwaltung der Abonnentenrichtlinien.
- Konfigurieren Sie die Appliance so, dass sie einen Abonnenten eindeutig identifiziert, indem Sie nur das IPv6-Präfix anstelle der vollständigen IPv6-Adresse verwenden.
- Verwenden Sie Richtlinien, um den TCP-Verkehr sowohl für dynamische als auch für statische Abonnenten zu optimieren. Diese Richtlinien verknüpfen verschiedene TCP-Profile mit verschiedenen Benutzertypen.

- Verwalten Sie inaktive Sitzungen auf einer NetScaler-Appliance.
- Aktivieren Sie die Protokollierung auf einem Protokollserver.
- Entfernen Sie LSN-Sitzungen für gelöschte Abonnentensitzungen.

Zuweisung von Speicher für das Modul „Subscriber Session Store“

Jeder Abonnentensitzungseintrag verbraucht 1 KB Speicher. Das Speichern von 500.000 Abonnentensitzungen zu einem beliebigen Zeitpunkt erfordert 500 MB Speicher. Dieser Wert muss zur Mindestspeicheranforderung hinzugefügt werden, die als Teil der Ausgabe des Befehls „show extendedmemoryparam“ angezeigt wird. Im folgenden Beispiel bezieht sich die Ausgabe auf eine NetScaler VPX-Instanz mit 3 Paket-Engines und 8 GB Arbeitsspeicher.

Um 500.000 Abonnentensitzungen auf dieser Appliance zu speichern, muss der konfigurierte Speicher 2058+500 MB (500.000 x 1 KB = 500 MB) betragen.

> **Hinweis**
>
> Der konfigurierte Speicher muss ein Vielfaches von 2 MB sein und darf die maximale Speicherauslastung nicht überschreiten. Die Appliance muss neu gestartet werden, damit die Änderungen wirksam werden.

Beispiel

```
show extendedmemoryparam
        Extended Memory Global Configuration. This memory is utilized by
            LSN and Subscriber Session Store Modules:
         Active Memory Usage: 0 MBytes
         Configured Memory Limit: 0 MBytes
         Minimum Memory Required: 2058 MBytes
         Maximum Memory Usage Limit: 2606 MBytes
     Done
     set extendedmemoryparam -memLimit 2558
     Done
     show extendedmemoryparam
             Extended Memory Global Configuration. This memory is
                utilized by LSN and Subscriber Session Store Modules:

             Active Memory Usage: 2558 MBytes
             Configured Memory Limit: 2558 MBytes
             Minimum Memory Required: 2058 MBytes
             Maximum Memory Usage Limit: 2606 MBytes
     Done
<!--NeedCopy-->
```


Konfiguration einer Schnittstelle für dynamische Abonnenten

Die NetScaler-Appliance empfängt die Abonnenteninformationen dynamisch über einen der folgenden Schnittstellentypen:

- Gx-Schnittstelle
- RADIUS-Schnittstelle
- RADIUS- und Gx-Schnittstelle

> **Hinweis**
>
> - Ab NetScaler Version 12.0 Build 57.19 wird die Gx-Schnittstelle für eine Clusterbereitstellung unterstützt. Weitere Informationen finden Sie unter Gx-Schnittstelle in einer Cluster-Topologie.
> - In einem HA-Setup werden die Teilnehmersitzungen kontinuierlich auf dem sekundären Knoten synchronisiert. Im Falle eines Failovers sind die Abonnenteninformationen weiterhin auf dem sekundären Knoten verfügbar.

Gx-Schnittstelle

Eine Gx-Schnittstelle (wie in 3GPP 29.212 spezifiziert) ist eine Standardschnittstelle, die auf dem Diameter-Protokoll basiert und den Austausch von Richtlinien- und Gebührenregeln zwischen einem PCRF und einer Policy and Charging Enforcement Function (PCEF) -Einheit in einem Telekommunikationsnetz ermöglicht.

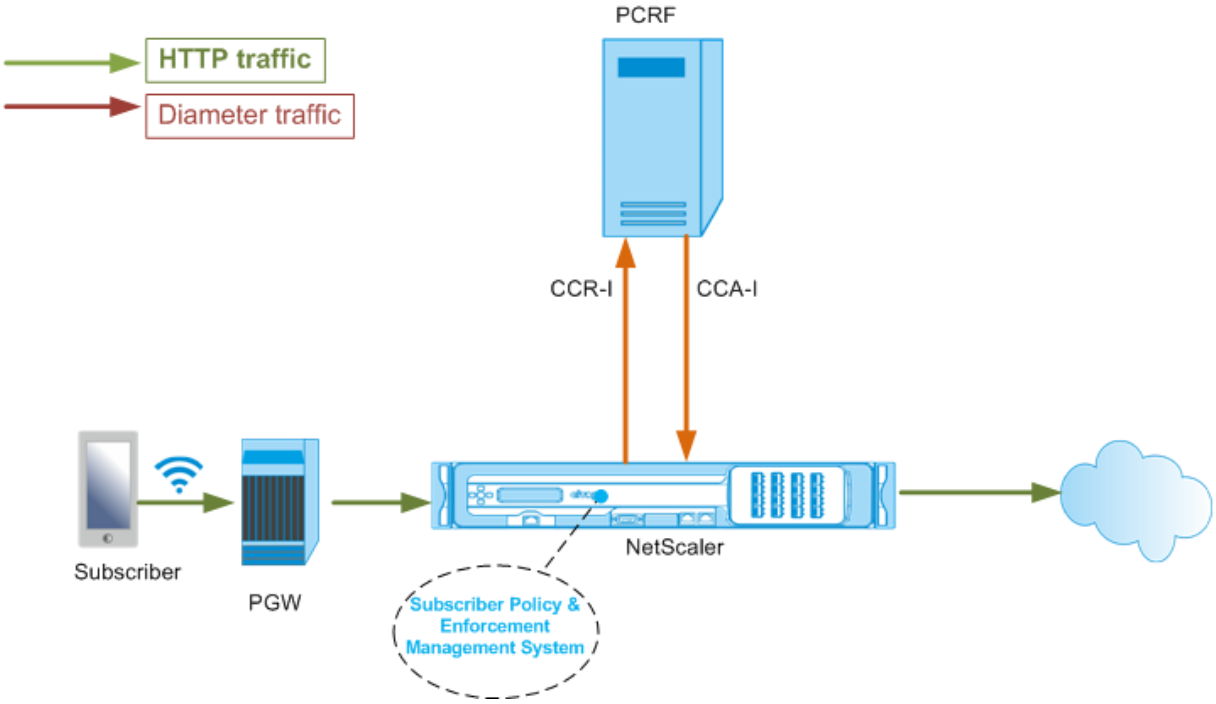
Wenn eine IP-CAN-Sitzung eingerichtet ist, leitet das Paket-Gateway die Abonnenten-ID, z. B. die MSISDN, und die Frame-IP-Adressinformationen über den Abonnenten als Diameter-Nachricht an das PCRF weiter. Wenn das Datenpaket vom Packet Gateway (PGW) bei der Appliance ankommt, verwendet die Appliance die Abonnenten-IP-Adresse, um den PCRF abzufragen, um die Abonnenteninformationen abzurufen. Dies wird auch als sekundäre PCEF-Funktionalität bezeichnet.

Die Policy and Charging Control (PCC) -Regeln, die von der Appliance über die Gx-Schnittstelle empfangen werden, werden während der Abonnentensitzung auf der Appliance gespeichert, d. h. bis das PCRF eine Re-Auth-Request (RAR) -Nachricht mit einer Session-Release-Cause AVP sendet oder die Abonnentensitzung über die CLI oder das Konfigurationsprogramm beendet wird. Wenn es Aktualisierungen für einen bestehenden Abonnenten gibt, sendet das PCRF die Updates in einer RAR-Nachricht. Eine Abonnentensitzung wird initiiert, wenn sich ein Abonnent am Netzwerk anmeldet, und beendet, wenn sich der Abonnent abmeldet.

> **Hinweis**: Wenn der PCRF-Server ausgefallen ist, erstellt die NetScaler-Appliance negative Sitzungen für die ausstehenden oder eingehenden Gx-Abonnentenanfragen. Wenn der PCRF-Server wieder verfügbar ist, verhindert die NetScaler-Appliance einen Sturm von Anfragen, indem sie wartet, bis die negativen Sitzungen abgelaufen sind, bevor die spezifischen Abonnentenanfra-

> gen ausgeführt werden.

Die folgende Abbildung zeigt den Verkehrsfluss auf hoher Ebene. Es wird davon ausgegangen, dass der Datenebenenverkehr HTTP ist. Die Appliance sendet eine Credit Control Request (CCR) über eine Gx-Schnittstelle an den PCRF-Server und empfängt in der Credit Control Answer (CCA) die PCC-Regeln und optional weitere Informationen, wie den Typ der Radio Access Technology (RAT), die für den jeweiligen Abonnenten gelten. PCC-Regeln enthalten einen oder mehrere Richtliniennamen (Regelnamen) und andere Parameter. Die Appliance verwendet diese Informationen, um die auf der Appliance gespeicherten vordefinierten Regeln abzurufen und den Verkehrsfluss zu steuern. Diese Informationen werden während der Abonnentensitzung auch in den Richtlinien- und Durchsetzungsmanagementsystemen für Abonnenten gespeichert. Nachdem eine Abonnentensitzung beendet wurde, verwirft die Appliance alle Informationen über den Abonnenten.



Das folgende Beispiel zeigt die Befehle zur Konfiguration einer Gx-Schnittstelle. Die Befehle sind fett gedruckt.

Führen Sie die folgenden Aufgaben aus, um eine Gx-Schnittstelle einzurichten

Fügen Sie für jede Gx-Schnittstelle einen DIAMETER-Service hinzu. Zum Beispiel:

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868

add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```


Fügen Sie einen nicht adressierbaren virtuellen DIAMETER-Ladausgleichsserver hinzu und binden Sie die in Schritt 1 erstellten Dienste an diesen virtuellen Server. Geben Sie für mehr als einen Dienst einen PersistenceType und den persistaVpNo an, damit bestimmte Sitzungen vom gleichen PCRF-Server verarbeitet werden. Zum Beispiel:

```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```

Konfigurieren Sie die NetScaler-Diameter, die Identität und den Bereich. Identität und Realm werden als Origin-Host- und Origin-Realm-AVPs in Durchmessernachrichten verwendet, die vom Gx-Client gesendet werden. Zum Beispiel:

```
set ns diameter  - identity netscaler.com  - realm com
<!--NeedCopy-->
```

Konfigurieren Sie die Gx-Schnittstelle, um den in Schritt 2 erstellten virtuellen Server als virtuellen PCRF-Server zu verwenden. Geben Sie den PCRF-Realm an, der als Zielbereichs-AVP in Durchmessernachrichten verwendet werden soll, die vom Gx-Client gesendet werden. Zum Beispiel:

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com
<!--NeedCopy-->
```

Stellen Sie den Subscriber-Schnittstellentyp auf GXOnly ein. Zum Beispiel:

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Um die Konfiguration und den Status der Gx-Schnittstelle zu sehen, geben Sie Folgendes ein:

```
show subscriber gxinterface
<!--NeedCopy-->
```

Beispiel

```
show subscriber gxinterface
    Gx Interface parameters:
        PCRF Vserver: vdiam (DOWN)
        Gx Client Identity...:  netscaler1.com
```



```
        Gx Client Realm ..........:  com
        PCRF Realm: epc.mnc030.mcc234.3gppnetwork.org
        Hold Packets On Subscriber Absence: YES
        CCR Request Timeout: 4 Seconds
        CCR Request Retry Attempts: 1
        Gx HealthCheck enabled: NO
        Gx HealthCheck TTL : 30 Seconds
        CER Request Timeout: 10 Seconds
        RevalidationTimeout: 30 Seconds
        NegativeTTL: 60 Seconds
        NegativeTTL Limited Success: NO
        Purge SDB on Gx Failure: YES
        ServicePath AVP code: 262099    ServicePath AVP VendorID: 3845
        PCRF Connection State: PCRF is not ready
    Done

<!--NeedCopy-->
```

ARGUMENTE

vServer

Name des virtuellen Load-Balancing- oder Content-Switching-Servers, zu dem die Gx-Verbindungen hergestellt werden. Der Diensttyp des virtuellen Servers muss DIAMETER oder SSL_DIAMETER sein. Dieser Parameter schließt sich gegenseitig mit dem Serviceparameter aus. Daher können Sie nicht sowohl den Dienst als auch den virtuellen Server in der Gx-Schnittstelle einrichten.

Service

Name des DIAMETER- oder SSL_DIAMETER-Dienstes, der dem PCRF entspricht, zu dem die Gx-Verbindung hergestellt wird. Dieser Parameter schließt sich gegenseitig mit dem Parameter vserver aus. Daher können Sie nicht sowohl den Dienst als auch den virtuellen Server in der Gx-Schnittstelle einrichten.

PCRF Realm

Der Bereich von PCRF, an den die Nachricht weitergeleitet werden soll. Dies ist der Realm, der in Destination-Realm AVP vom NetScaler Gx-Client (als Diameter-Knoten) verwendet wird.

Bei Abwesenheit des Abonnenten festhalten

Auf Ja setzen, um Pakete zu speichern, bis die Sitzungsinformationen des Abonnenten vom PCRF-Server abgerufen werden. Wenn diese Option auf Nein gesetzt ist, wird das Standardabonnentenprofil angewendet, bis die Abonnentensitzungsinformationen vom PCRF-Server abgerufen werden. Wenn kein Standard-Abonnentenprofil konfiguriert ist, wird ein UNDEF für Ausdrücke ausgelöst, die Abonnentenattribute verwenden.

Timeout anfragen

Zeit in Sekunden, innerhalb derer die Gx-CCR-Anforderung abgeschlossen sein muss. Wenn die Anforderung nicht innerhalb dieser Zeit abgeschlossen wird, wird die Anforderung so oft erneut übertragen, wie im Parameter RequestRetryAttempts angegeben. Wenn die Anfrage auch nach der erneuten Übertragung nicht abgeschlossen ist, wird das Standard-Abonnentenprofil auf diesen Abonnenten angewendet. Wenn kein Standard-Abonnentenprofil konfiguriert ist, wird ein UNDEF für Ausdrücke ausgelöst, die Abonnentenattribute verwenden. Null deaktiviert den Timeout. Standardwert: 10

Wiederholungsversuche anfordern

Geben Sie an, wie oft eine Anfrage erneut übertragen werden muss, wenn die Anforderung nicht innerhalb des im RequestTimeout-Parameter angegebenen Werts abgeschlossen wird. Standardwert: 3.

Gesundheitscheck

Auf Ja setzen, um die Inline-Integritätsprüfung des Gx-Peers zu aktivieren. Wenn diese Option aktiviert ist, sendet NetScaler DWR-Pakete an den PCRF-Server. Wenn die Gx-Sitzung inaktiv ist, läuft der HealthCheck-Timer ab und DWR-Pakete werden initiiert, um zu überprüfen, ob der PCRF-Server aktiv ist. Standardwert: Nein.
Hinweis: Dieser Parameter wird in NetScaler 12.1 Build 51.xx und höher unterstützt.

Gesundheitscheck TTL

Zeit in Sekunden, die für die Watchdog-Überwachung definiert wurde. Nach Ablauf der TTL-Zeit für die Integritätsprüfung wird DWR gesendet, um den Status des PCRF-Servers zu überprüfen. Jede CCR-, CCA-, RAR- oder RAA-Nachricht setzt den Timer zurück.
Mindestwert: 6 Sekunden. Standardwert: 30 Sekunden.
Hinweis: Dieser Parameter wird in NetScaler 12.1 Build 51.xx und höher unterstützt.

Zeitlimit für CER-Anfragen

Definierte Zeit in Sekunden für die erneute Übertragung der Anfrage zum Austausch von Fähigkeiten. NetScaler initiiert eine neue CER-Nachricht, wenn es innerhalb dieser konfigurierten Zeit keine CEA

vom PCRF erhält.
Wenn keine Antwort vom PCRF-Server empfangen wird, versucht die Appliance fünfmal, die CER-Nachricht zu senden. Wenn auch nach 5 CER-Meldungen keine Antwort erfolgt, schließt die Appliance die TCP-Verbindung und meldet einen Fehler. Wenn der Timeout-Wert auf 0 gesetzt ist, ist die Funktion zur Überprüfung der Anwendungsintegrität deaktiviert.
Mindestwert: 0 Sekunden. Standardwert: 0 Sekunden.
Hinweis: Dieser Parameter wird in NetScaler 12.1 Build 51.xx und höher unterstützt.

Timeout für die erneute Validierung

Zeit in Sekunden, nach deren Ablauf die Gx-CCR-U-Anforderung nach jeder PCRF-Aktivität in einer Sitzung gesendet wird. Jede RAR- oder CCA-Nachricht setzt den Timer zurück. Der Wert Null deaktiviert das Leerlauf-Timeout.

Negatives TTL

Zeit in Sekunden, nach der die Gx CCR-I-Anfrage für Sitzungen, die von PCRF nicht aufgelöst wurden, erneut gesendet wird, weil der Server ausgefallen ist oder keine Antwort eingeht oder eine fehlgeschlagene Antwort empfangen wurde. Anstatt den PCRF-Server ständig abzufragen, sorgt eine negative TTL dafür, dass die Appliance an einer ungelösten Sitzung festhält. Bei negativen Sitzungen erbt die Appliance die Attribute aus dem Standard-Abonnentenprofil, sofern eines konfiguriert ist, und aus der RADIUS-Kontonachricht, falls eine empfangen wird. Der Wert Null deaktiviert die negativen Sitzungen. Die Appliance installiert keine negativen Sitzungen, auch wenn eine Abonnentensitzung nicht abgerufen werden konnte. Standardwert: 600

Negativer TTL Eingeschränkter Erfolg

Auf Ja setzen, um einen negativen Antwortcode für eine Sitzung bei teilweisem Erfolg zu erstellen (2002). Wenn auf Nein gesetzt, wird eine reguläre Sitzung erstellt. Standardwert: Nein.

Dieser Parameter wird in NetScaler 12.1 Build 49.xx und höher unterstützt.

Löscht den DBONGX-Fehler

Auf Ja setzen, um die Abonnentendatenbank zu leeren, wenn die Gx-Schnittstelle ausfällt. Der Ausfall der Gx-Schnittstelle umfasst sowohl die DWR-Überwachung (falls aktiviert) als auch den Netzwerk-Integritätscheck (falls aktiviert). Wenn diese Option auf Ja gesetzt ist, werden alle Abonnentensitzungen gelöscht.
Standardwert: Nein.
Hinweis: Dieser Parameter wird in NetScaler 12.1 Build 51.xx und höher unterstützt.

ServicePfad AVP

Der AVP-Code, in dem PCRF den für einen Abonnenten geltenden Dienstpfad sendet.

Servicepath-Anbieter-ID

Die Anbieter-ID des AVP, in dem PCRF den für einen Abonnenten geltenden Dienstpfad sendet.

So konfigurieren Sie die Gx-Schnittstelle mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter Interface-Typ **GxOnly**aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Klicken Sie auf **OK**.

Erkennen Sie Transportfehler über etablierte Gx-Verbindungen

Hinweis: Diese Funktion wird in NetScaler 12.1 Build 51.xx und höher unterstützt.

Eine NetScaler-Appliance kann so konfiguriert werden, dass sie Transportfehler über etablierte Gx-Verbindungen erkennt, indem sie DWR-Meldungen (Device Watchdog Request) und DWA-Meldungen (Device Watchdog Answer) verwendet.

Nachdem eine Gx-Sitzung eingerichtet wurde, wird ein vordefinierter Timer ausgelöst, um zu erkennen, ob eine Sitzung inaktiv ist. Eine DWR-Nachricht wird gesendet, nachdem der Timer für die Leerlaufzeit abgelaufen ist. Der Timer für die Leerlaufzeit wird jedes Mal zurückgesetzt, wenn die NetScaler-Appliance eine Nachricht über eine etablierte Gx-Sitzung empfängt. Die Verfügbarkeit des Peers wird anhand der DWA-Nachricht bestätigt, nachdem eine DWR-Nachricht gesendet wurde.

- Wenn der DWA empfangen wird, wird die Verfügbarkeit eines Peers bestätigt und der Watchdog-Timer wird zurückgesetzt.
- Wenn der DWA nicht empfangen wird und der Watchdog-Timer zweimal hintereinander abläuft, gilt die Sitzung als ausgefallen und der Peer ist nicht verfügbar. Die Appliance schließt die Sitzung und versucht, eine neue Sitzung mit dem Gx-Peer einzurichten.

Wenn der Watchdog-Timer zweimal abläuft, ohne dass eine Reaktion erfolgt, betrachtet die NetScaler-Appliance die Gx-Verbindung als fehlerhaft und leitet eine Verbindungsunterbrechung ein. Sobald die Verbindung geschlossen ist, wird keine weitere Watchdog-Anfrage an den Gx-Peer gesendet. Die NetScaler-Appliance verwendet die nächste verfügbare Gx-Sitzung für alle PCRF-Anfragen.

Um Transportfehler über etablierte Gx-Verbindungen mithilfe der CLI zu erkennen

Geben Sie in der Befehlszeile Folgendes ein:


```
set subscriber gxInterface [-vServer <string>] [-service <string>] [-
    healthCheck ( YES | NO )] [-healthCheckTTL<positive_integer>][-
    cerRequestTimeout <positive_integer>] [-purgeSDBonGxFailure ( YES |
    NO )]
<!--NeedCopy-->
```

Beispiel:

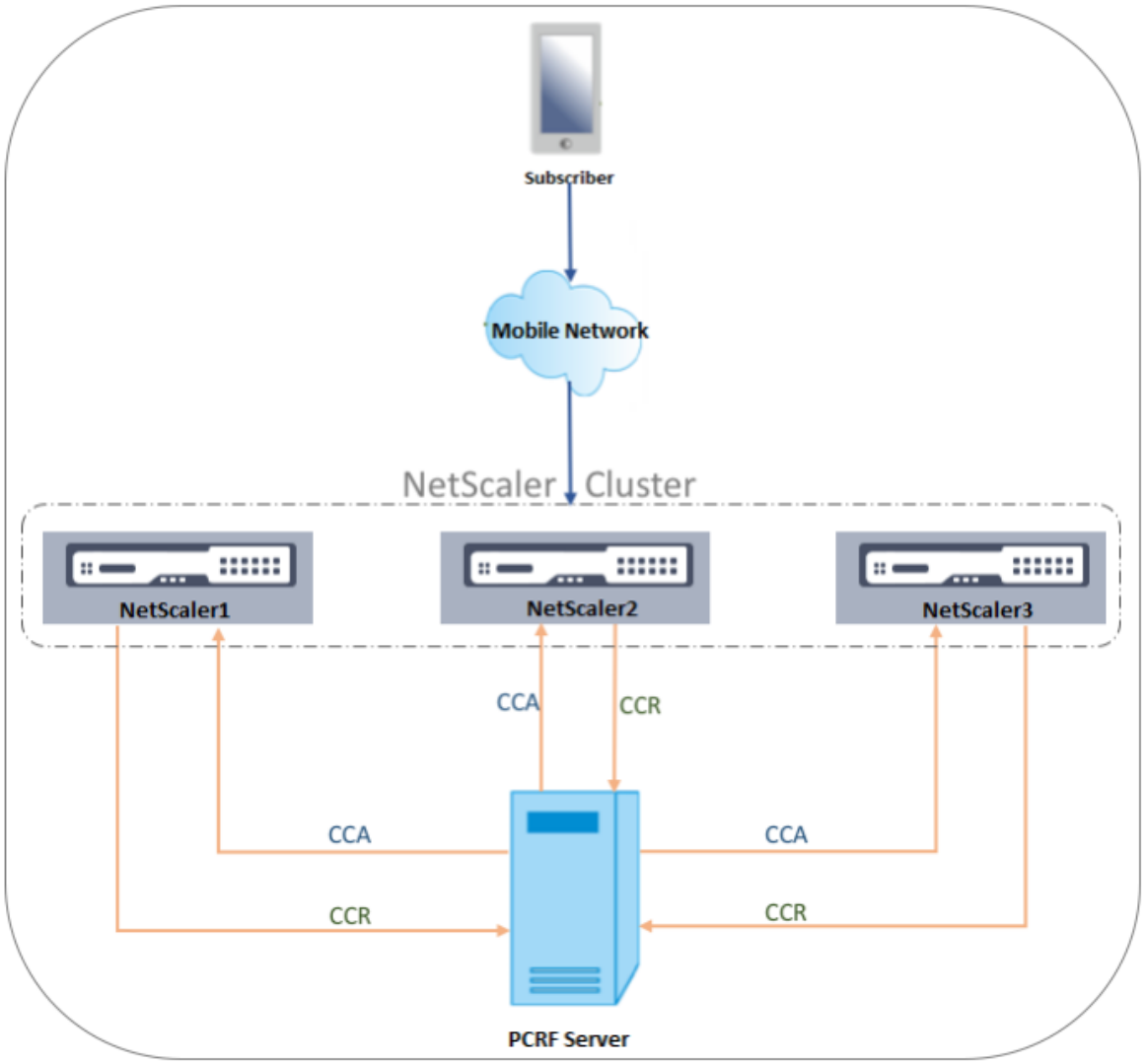
```
set subscriber gxInterface set subscriber gxInterface -vServer vdiam -
    healthCheck YES -healthCheckTTL 31 -cerRequestTimeout 15
    purgeSDBonGxFailure  YES
<!--NeedCopy-->
```

Um Transportfehler über etablierte Gx-Verbindungen mithilfe der GUI zu erkennen

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter **Schnittstellentyp**die Option **GxOnly**aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Wählen Sie **Health Check** und geben Sie Werte für **Health Check TTL** und **CER Request Timeout an**.
6. Klicken Sie auf **OK**.

Gx-Schnittstelle in einer Cluster-Topologie

Die NetScaler-Appliance unterstützt die Gx-Schnittstelle in einer Cluster-Topologie.



Die NetScaler-Knoten im Cluster kommunizieren über die Gx-Schnittstelle mit einem externen PCRF-Server. Wenn ein Knoten Client-Verkehr empfängt, führt die Appliance Folgendes aus:

- Sendet eine CCR-I-Anfrage an den PCRF-Server, um Abonnenteninformationen abzurufen.
- Der PCRF-Server antwortet mit einem CCR-A.
- Der NetScaler-Knoten speichert dann die empfangenen Abonnenteninformationen in seinem Abonnentenspeicher und wendet die Regeln auf den Client-Verkehr an.

Jeder Knoten unterhält einen unabhängigen Abonnentenspeicher und Abonnentensitzungen werden nicht mit anderen Knoten synchronisiert.

Gemäß dem Diameter Base Protocol RFC 6733 muss jeder Peer mit einer eindeutigen Durchmesseridentität konfiguriert werden, um über das Diameter-Protokoll mit anderen Peers kommunizieren zu können. Daher wird bei einer Cluster-Bereitstellung die Konfiguration der Durchmesseridentität erkannt. Die Durchmesserparameter (Identität, Realm, Server Close Propagation) für jeden Knoten können mithilfe der GUI oder der CLI individuell konfiguriert werden.

Wenn ein Knoten zu einem Cluster hinzugefügt wird, verwendet er die Standardparameter für den Durchmesser (identity=netscaler.com, realm=com, serverClosePropogation=no). Nachdem die Knoten hinzugefügt wurden, müssen die Durchmesserparameter für jeden Knoten konfiguriert werden.

So konfigurieren Sie die Durchmesserparameter mithilfe der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Durchmesserparameter ändern**.
3. **Wählen Sie auf der Seite „Durchmesserparameter“ den NetScaler-Knoten aus, für den Sie die Durchmesserparameter konfigurieren möchten, und klicken Sie dann auf Konfigurieren.**
4. Konfigurieren Sie auf der Seite „Durchmesserparameter konfigurieren“ die Durchmesseridentität, den Durchmesserbereich und die Server-Close Propagation für den ausgewählten Knoten.
5. Klicken Sie auf **OK**.

So konfigurieren Sie die Durchmesserparameter mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns diameter [-identity <string>] [-ownerNode <positive_integer>]
<!--NeedCopy-->
```

ARGUMENTE

Identität

Diameter Identity wird verwendet, um einen Durchmesserknoten eindeutig zu identifizieren. Vor der Einrichtung der Durchmesserkonfiguration muss der NetScaler-Appliance (als Diameter-Knoten) eine eindeutige Durchmesseridentität zugewiesen werden.

Geben Sie beispielsweise ns diameter -identity netscaler.com -OwnerNode 1 ein. Wann immer das NetScaler-System also Identity in Diameter Messages verwenden muss, verwendet es ‘netscaler.com’ als Origin-Host AVP, wie in RFC3588 definiert.

Maximale Länge: 255

InhaberNode

OwnerNode stellt die ID des Clusterknotens dar, für den die Durchmesser-ID festgelegt ist. OwnerNode kann nur über CLIP konfiguriert werden.

Mindestwert: 0

Höchstwert: 31

Beispiel:

set ns diameter -identity netscaler1.com -ownerNode 1

Hinweis:

Die Option ownerNode wurde auch zum Befehl show ns diameter hinzugefügt.

Beispiel:

```
show diameter -ownerNode <0-31>
<!--NeedCopy-->
```

Wenn der Befehl show ns diameter ausgeführt wird, werden die Durchmesserparameter für einen bestimmten Knoten angezeigt.

So konfigurieren Sie eine Gx-Schnittstelle für die Cluster-Bereitstellung

Gehen Sie wie folgt vor, um eine Gx-Schnittstelle einzurichten:

Fügen Sie für jede Gx-Schnittstelle einen DIAMETER-Service hinzu.

Beispiel:

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868
add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

Fügen Sie einen virtuellen DIAMETER-Load-Balancing-Server hinzu und binden Sie die in Schritt 1 erstellten Dienste an diesen virtuellen Server.

Beispiel:

```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```

Konfigurieren Sie die NetScaler-Durchmesseridentität und den Realm auf allen Clusterknoten. Identität und Realm werden als Origin-Host- und Origin-Realm-AVPs in Durchmessernachrichten verwendet, die vom Gx-Client gesendet werden.

Beispiel:


```
set ns diameter -identity node0.netscaler.com -realm netscaler.com -
    ownerNode 0

set ns diameter -identity node1.netscaler.com -realm netscaler.com -
    ownerNode 1
<!--NeedCopy-->
```

Konfigurieren Sie die Gx-Schnittstelle so, dass der in Schritt 2 erstellte virtuelle Server als virtuellen PCRF-Server verwendet wird, und legen Sie auch den PCRF-Realm fest.

Beispiel:

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com

Set the subscriber interface type to GxOnly.
<!--NeedCopy-->
```

Beispiel:

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Um die Konfiguration und den Status der Gx-Schnittstelle zu sehen, geben Sie Folgendes ein:

```
show subscriber gxinterface
<!--NeedCopy-->
```

RADIUS-Schnittstelle

Bei einer RADIUS-Schnittstelle leitet das Paket-Gateway die Abonnenteninformationen in einer RADIUS Accounting Start-Nachricht über die RADIUS-Schnittstelle an die Appliance weiter, wenn eine IP-CAN-Sitzung eingerichtet wird. Ein Dienst vom Typ RadiusListener verarbeitet RADIUS Accounting-Nachrichten. Fügen Sie einen gemeinsamen geheimen Schlüssel für den RADIUS-Client hinzu. Wenn kein Shared Secret konfiguriert ist, wird die RADIUS-Nachricht stillschweigend gelöscht. Das folgende Beispiel zeigt die Befehle zur Konfiguration einer RADIUS-Schnittstelle. Die Befehle sind fett gedruckt.

Gehen Sie wie folgt vor, um eine RADIUS-Schnittstelle einzurichten:

Erstellen Sie einen RADIUS-Listener-Dienst an der SNIP-Adresse, an der die RADIUS-Nachrichten empfangen werden. Zum Beispiel:

```
add service srad1 192.0.0.206 RADIUSLISTENER 1813
<!--NeedCopy-->
```


Konfigurieren Sie die RADIUS-Schnittstelle für Abonnenten, um diesen Dienst zu verwenden. Zum Beispiel:

```
set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Legen Sie den Schnittstellentyp für Abonnenten auf RadiusOnly fest. Zum Beispiel:

```
set subscriber param -interfaceType RadiusOnly
<!--NeedCopy-->
```

Fügen Sie einen RADIUS-Client hinzu, der ein Subnetz und einen gemeinsamen Schlüssel angibt. Zum Beispiel:

```
add radius client 192.0.2.0/24 -radkey client123
<!--NeedCopy-->
```

Ein Subnetz von 0.0.0.0/0 bedeutet, dass es der standardmäßige gemeinsame geheime Schlüssel für alle Clients ist. Um die Konfiguration und den Status der RADIUS-Schnittstelle zu sehen, geben Sie Folgendes ein:

```
show subscriber radiusInterface
<!--NeedCopy-->
```

RADIUS-Schnittstellenparameter:

Radius-Listener-Dienst: srad1 (UP)

Fertig

Beispiel:

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868

add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

ARGUMENTE

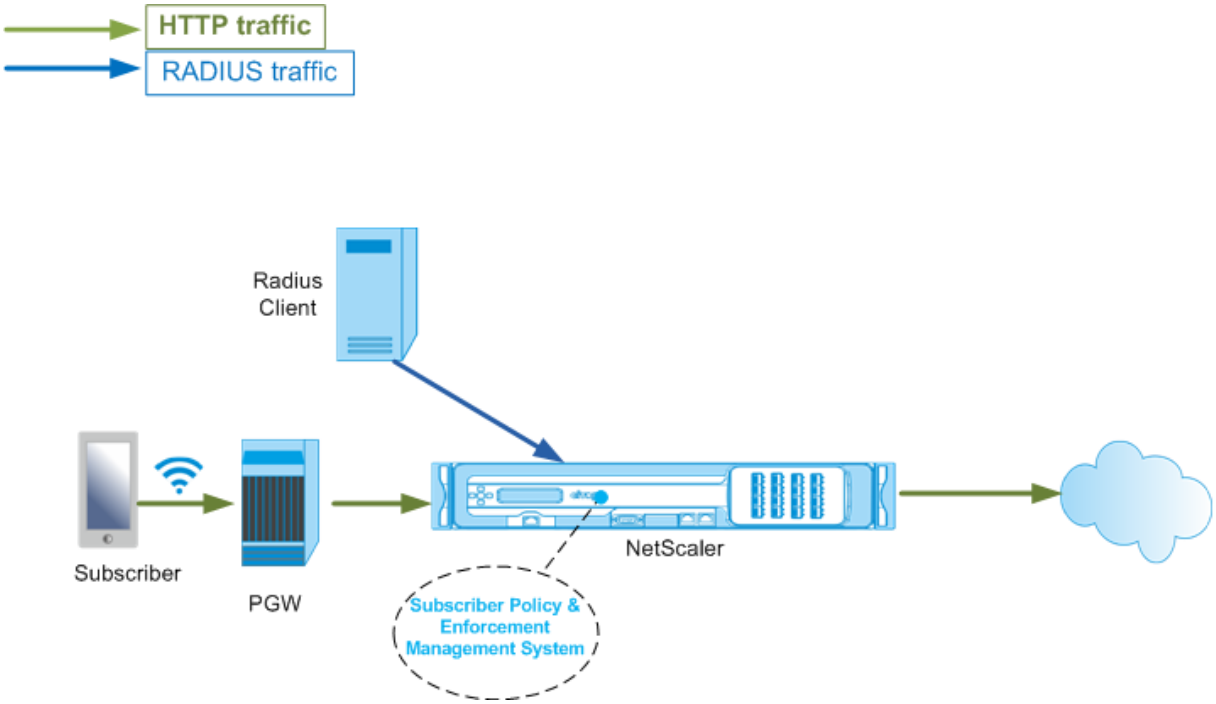
Service zum Zuhören

Name des RADIUS-Listening-Dienstes, der die RADIUS-Abrechnungsanfragen verarbeitet.

SVR-Staat

Der Status des RADIUS-Abhördienstes.

Die folgende Abbildung zeigt den Verkehrsfluss auf hoher Ebene.



So konfigurieren Sie die RadiusOnly-Schnittstelle mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter Schnittstellentyp die Option **RadiusOnly**aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Klicken Sie auf **OK**.

RADIUS- und Gx-Schnittstelle

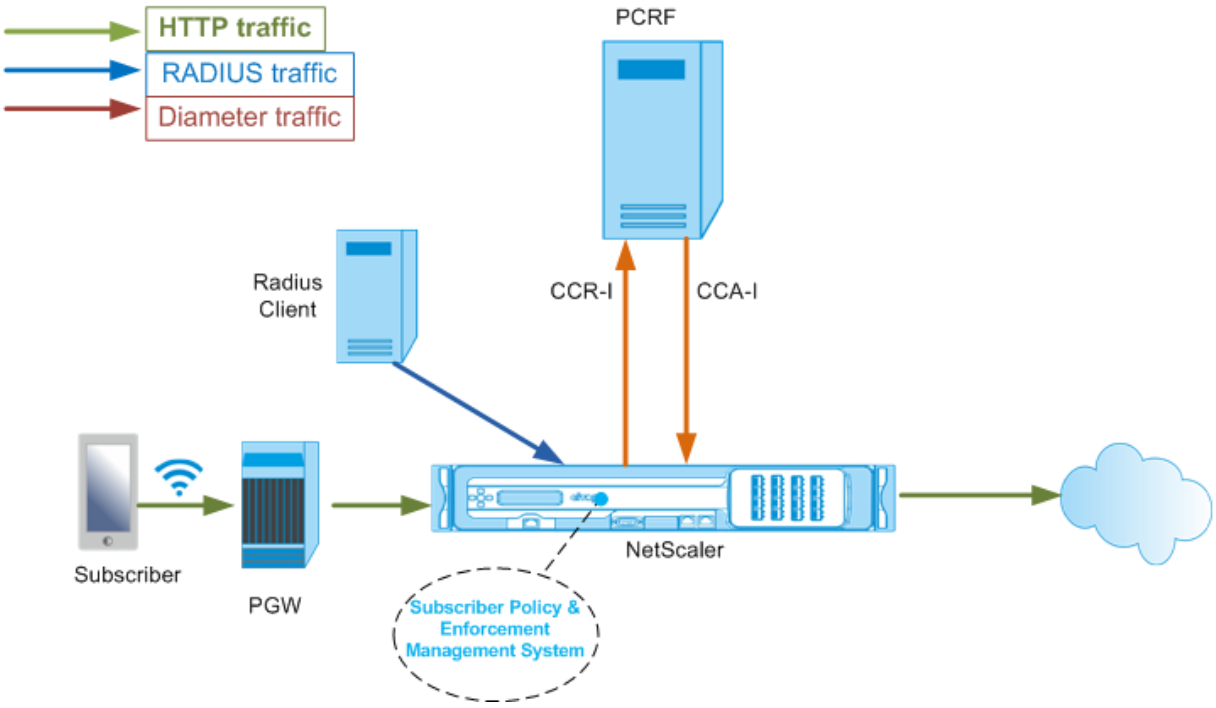
Bei einer RADIUS- und Gx-Schnittstelle leitet das Paket-Gateway beim Einrichten einer IP-CAN-Sitzung die Abonnenten-ID, z. B. die MSISDN, und die Frame-IP-Adressinformationen über den Abonnenten über die RADIUS-Schnittstelle an die Appliance weiter. Die Appliance verwendet diese Abonnenten-ID, um den PCRF auf der Gx-Schnittstelle abzufragen, um die Abonnenteninformationen abzurufen. Dies wird als primäre PCEF-Funktionalität bezeichnet. Das folgende Beispiel zeigt die Befehle zur Konfiguration einer RADIUS- und Gx-Schnittstelle.

```
set subscriber param -interfaceType RadiusandGx
add service pcrf-svc 203.0.113.1 DIAMETER 3868
```



```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263
bind lb vserver vdiam pcrf-svc
set subscriber gxInterface -vServer vdiam -pcrfRealm testrealm1.net -
    holdOnSubscriberAbsence YES -revalidationTimeout 60 -negativeTTL 120
add service srad1 192.0.0.206 RADIUSLISTENER 1813    set subscriber
    radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Die folgende Abbildung zeigt den Verkehrsfluss auf hoher Ebene.



So konfigurieren Sie die RadiusandGX-Schnittstelle mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter Schnittstellentyp die Option **RadiusandGX**aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Klicken Sie auf **OK**.

Statische Abonnenten konfigurieren

Sie können die Abonnenten manuell auf der NetScaler-Appliance konfigurieren, indem Sie die Befehlszeile oder das Konfigurationsprogramm verwenden. Sie erstellen statische Abonnenten, indem Sie jedem Abonnenten eine eindeutige Abonnenten-ID zuweisen und optional jedem Abonnenten

eine Richtlinie zuordnen. Die folgenden Beispiele zeigen die Befehle zur Konfiguration eines statischen Abonnenten.

In den folgenden Beispielen gibt **SubscriptionIDValue** die internationale Telefonnummer an, und **SubscriptionIdType** (E164 in diesem Beispiel) gibt das allgemeine Format für internationale Telefonnummern an.

```
1     add subscriber profile 203.0.113.6 -subscriberRules policy1 policy2
          -subscriptionIdType E164 -subscriptionIdvalue 98767543211
2     add subscriber profile 2002::a66:e8d3/64 -subscriberRules policy1
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543212
3     add subscriber profile 203.0.24.2 10 -subscriberRules policy2
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543213
4 <!--NeedCopy-->
```

Um die konfigurierten Abonnentenprofile anzuzeigen, geben Sie Folgendes ein:

> Abonnentenprofil anzeigen

```
1     > show subscriber profile
2
3     1)  Subscriber IP: 203.0.24.2 VLAN:10
4         Profile Attributes:
5                 Active Rules: policy2, policy3
6                 Subscriber Id Type: E164
7                 Subscriber Id Value: 98767543213
8     2)  Subscriber IP: 2002::/64
9         Profile Attributes:
10                Active Rules: policy1, policy3
11                Subscriber Id Type: E164
12                Subscriber Id Value: 98767543212
13    3)  Subscriber IP: 203.0.113.6
14        Profile Attributes:
15                Active Rules: policy1, policy2
16                Subscriber Id Type: E164
17                Subscriber Id Value: 98767543211
18
19     Done
20 <!--NeedCopy-->
```


Standard-Abonnentenprofil

Ein Standard-Abonnentenprofil wird verwendet, wenn die Abonnenten-IP-Adresse nicht im Abonnenten-Sitzungsspeicher auf der Appliance gefunden wird. Im folgenden Beispiel wird ein Standard-Abonnentenprofil mit der Abonnentenregel policy1 hinzugefügt.

```
    > add subscriber profile * -subscriberRules policy1
<!--NeedCopy-->
```

Abonnentensitzungen anzeigen und löschen

Verwenden Sie den folgenden Befehl, um alle statischen und dynamischen Abonnentensitzungen anzuzeigen.

> Abonnentensitzungen anzeigen

```
    > show subscriber sessions
    1)  Subscriber IP: 2002::/64
        Session Attributes:
                Active Rules: policy1, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543212
    2)  Subscriber IP: *
        Session Attributes:
                Active Rules: policy1
    3)  Subscriber IP: 203.0.24.2 VLAN:10
        Session Attributes:
                Active Rules: policy2, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543213
    4)  Subscriber IP: 203.0.113.6
        Session Attributes:
                Active Rules: policy1, policy2
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543211
    5)  Subscriber IP: 192.168.0.11
        Session Attributes:
                Idle TTL remaining: 361 Seconds
                Active Rules: policy1
                Subscriber Id Type: E164
                Subscriber Id Value: 1234567811
                Service Path: policy1
                AVP(44): 34 44 32 42 42 38 41 43  2D 30 30 30 30 30 30
                   31 31
                AVP(257): 00 01 C0 A8 0A 02
```



```
29                  PCRF-Host: host.pcrf.com
30                  AVP(280): 74 65 73 74 2E 63 6F 6D
31
32      Done
33  <!--NeedCopy-->
```

Verwenden Sie den folgenden Befehl, um eine einzelne Sitzung oder den gesamten Sitzungsspeicher zu löschen. Wenn Sie keine IP-Adresse angeben, wird der gesamte Abonnenten-Sitzungsspeicher gelöscht.

```
1  clear subscriber sessions <ip>
2  <!--NeedCopy-->
```

System zur Durchsetzung und Verwaltung der Abonnentenrichtlinien

Die NetScaler-Appliance verwendet die IP-Adresse des Abonnenten als Schlüssel für das System zur Durchsetzung und Verwaltung der Abonnentenrichtlinien.

Sie können Abonnentenausdrücke hinzufügen, um die Abonnenteninformationen zu lesen, die im Subscriber Policy Enforcement & Management System verfügbar sind. Diese Ausdrücke können mit Richtlinienregeln und Aktionen verwendet werden, die für NetScaler-Funktionen wie integriertes Caching, Rewrite, Responder und Content Switching konfiguriert sind.

Die folgenden Befehle sind ein Beispiel für das Hinzufügen einer auf Abonnenten basierenden Responder-Aktion und -Richtlinie. Die Richtlinie wird als wahr ausgewertet, wenn der Wert der Abonnentenregel „pol1“ ist.

```
1      add responder action error_msg respondwith '"HTTP/1.1 403 OKrnrn" +
           " You are  not authorized to access Internet"'
2      add responder policy no_internet_access "SUBSCRIBER.RULE_ACTIVE("
          pol1")" error_msg
3  <!--NeedCopy-->
```

Das folgende Beispiel zeigt die Befehle zum Hinzufügen einer auf Abonnenten basierenden Umschreibeaktion und -richtlinie. Die Aktion fügt einen HTTP-Header „x-Nokia-MSISDN“ ein, indem der Wert von AVP (45) in der Abonnentensitzung verwendet wird.

```
1      > add rewrite action AddHDR-act insert_http_header X-Nokia-MSISDN "
          SUBSCRIBER.AVP(45).VALUE"
2      > add rewrite policy AddHDR-pol "HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.
          URL).EQUALS_ANY("patset-test")" AddHDR-act
3  <!--NeedCopy-->
```


Im folgenden Beispiel werden zwei Richtlinien auf der Appliance konfiguriert. Wenn die Appliance die Abonnenteninformationen überprüft und die Abonnentenregel cache_enable lautet, führt sie das Caching durch. Wenn die Abonnentenregel cache_disable lautet, führt die Appliance kein Caching durch.

```
1      > add cache policy nocachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_disable")" - action NOCACHE
2      > add cache policy cachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_enable")" - action CACHE -storeInGroup cg1
3  <!--NeedCopy-->
```

Eine vollständige Liste der Ausdrücke, die mit „SUBSCRIBER“ beginnen, finden Sie im Leitfaden zur Richtlinienkonfiguration.

> **Wichtige**
>
> NetScaler-Softwareversion 12.1 unterstützt die IPANDVLAN-Schlüsselsuchmethode, wenn die Abonnentenschnittstelle auf GXOnly festgelegt ist. Weitere Informationen finden Sie unter Nachschlagmethode für IP-Adresse und VLAN-ID-Schlüssel.

IPv6-Präfix-basierte Teilnehmersitzungen

Ein Telco-Benutzer wird durch das IPv6-Präfix und nicht durch die vollständige IPv6-Adresse identifiziert. Die NetScaler-Appliance verwendet jetzt das Präfix anstelle der vollständigen IPv6-Adresse (/128), um einen Abonnenten in der Datenbank (Abonnentenspeicher) zu identifizieren. Für die Kommunikation mit dem PCRF-Server (z. B. in einer CCR-I-Nachricht) verwendet die Appliance jetzt das gerahmte IPv6-Präfix AVP anstelle der vollständigen IPv6-Adresse. Die Standardlänge des Präfixes ist /64, aber Sie können die Appliance so konfigurieren, dass sie einen anderen Wert verwendet.

So konfigurieren Sie das IPv6-Präfix mithilfe der Befehlszeile

```
set subscriber param [-ipv6PrefixLookupList <positive_integer> ...]
```

Der erste Beispielbefehl unten legt ein einzelnes Präfix fest und der zweite Beispielbefehl legt mehrere Präfixe fest.

```
1      set subscriber param -ipv6PrefixLookupList 64
2      set subscriber param -ipv6PrefixLookupList 64 72 96
3  <!--NeedCopy-->
```

So konfigurieren Sie das IPv6-Präfix mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.

2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Abonnentenparameter konfigurieren** und geben Sie in der **IPv6-Präfix-Suchliste**ein oder mehrere Präfixe an.

Suchmethode für IP-Adresse und VLAN-ID-Schlüssel

Die NetScaler-Appliance verwendet die IP-Adresse des Abonnenten als zentrale Suchmethode für das Durchsetzungs- und Verwaltungssystem der Abonnentenrichtlinien. Diese Methode ist nicht wirksam, wenn sich die IP-Adressen überschneiden. In solchen Fällen können Sie die VLAN-ID als zusätzlichen Abonnenten-Suchtyp verwenden. Die IPANDVLAN-Schlüsselsuchmethode wird nur unterstützt, wenn die Abonnentenschnittstelle auf GXOnly eingestellt ist. Wenn IPANDVLAN als Suchmethode konfiguriert ist, führt die NetScaler-Appliance Folgendes aus:

- Schließt die ursprüngliche VLAN-ID in die Gx-Abfrage für IPv4-Abonnenten ein.
- Schließt das Gx-VLAN-AVP in alle Gx-Antworten ein. Wenn jedoch eine VLAN-ID nicht übereinstimmt, ignoriert die Appliance die Antworten.

Wenn die Appliance beispielsweise ein CCR-I mit GxSessionID-a:IPv4-b:VLAN-C sendet und die Antwort GxSessionid-A:IPv4-B:VLAN-D enthält, wird die Antwort gelöscht und ein Standard-Abonnenteneintrag wird erstellt.

> **Hinweis**
>
> - Die Schnittstellentypen RadiusandGX und RadiusOnly können nicht zusammen mit dem Schlüsseltyp IPANDVLAN konfiguriert werden.
> - Wenn der Datenverkehr von einer IPv6-Adresse stammt, verwendet die NetScaler-Appliance die IP-Suchmethode.

So konfigurieren Sie IP oder IPANDVLAN als Schlüsselsuchmethode mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set subscriber param [-keytype ( IP | IPANDVLAN )] [-interfaceType <
   interfaceType>]
<!--NeedCopy-->
```

Beispiel:

```
set subscriber param -keytype IPANDVLAN -interfaceType GxOnly

set subscriber param -keytype IP -interfaceType GxOnly
<!--NeedCopy-->
```


> **Hinweis**
>
> Wenn Sie den Schlüsseltypparameter von IP in IPANDVLAN ändern und umgekehrt alle Abonnentendaten löschen.

VLAN-Parameter

Der VLAN-Parameter wurde auch für die folgenden Befehle hinzugefügt.

```
add subscriber profile <ip>@ [-vlan]

set subscriber profile <ip>@ [-vlan] [-subscriptionIdType  <
   subscriptionIdType>]

show subscriber profile [<ip>@] [-vlan]

rm subscriber profile <ip>@ [-vlan <positive_integer>]
<!--NeedCopy-->
```

Argumente

ip

Stellt die IP-Adresse des Abonnenten dar. Dies ist ein obligatorisches Argument und kann nicht geändert werden, nachdem das Abonnentenprofil hinzugefügt wurde.

vlan

Stellt die VLAN-Nummer dar, auf der sich der Abonnent befindet. Die VLAN-Nummer kann nicht geändert werden, nachdem das Abonnentenprofil hinzugefügt wurde.

Mindestwert: 1

Höchstwert: 4096

```
add subscriber profile 192.0.2.23 10

set subscriber profile 192.0.2.23 10 -subscriptionIdtype E164

show subscriber profile 192.0.2.23 10

rm subscriber profile 192.0.2.23 10

<!--NeedCopy-->
```


So konfigurieren Sie IP oder IPANDVLAN als Schlüsselsuchmethode mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter.**
2. Klicken Sie auf **Abonnentenparameter konfigurieren.**
3. Wählen Sie **unter SchlüsseltypIP**oder**IPANDVLAN gemäß Ihren Anforderungen** aus.
4. Schließen Sie die Konfiguration ab und klicken Sie auf **OK**.

Verwaltung von Inaktivsitzungen von Abonnentensitzungen in einem Telekommunikationsnetz

Die Bereinigung von Abonnentensitzungen auf einer NetScaler-Appliance basiert auf Ereignissen auf der Steuerungsebene, wie z. B. einer Meldung zum Stoppen der RADIUS-Abrechnung, einer Diameter RAR-Meldung (Sitzungsfreigabe) oder einem Befehl zum Löschen der Abonnentensitzung. In einigen Bereitstellungen erreichen die Nachrichten von einem RADIUS-Client oder einem PCRF-Server die Appliance möglicherweise nicht. Außerdem können die Nachrichten bei starkem Verkehr verloren gehen. Eine Abonnentensitzung, die lange Zeit inaktiv ist, verbraucht weiterhin Speicher- und IP-Ressourcen auf der NetScaler-Appliance. Die Funktion zur Verwaltung von Leerlaufsitzungen bietet konfigurierbare Timer zur Identifizierung inaktiver Sitzungen und bereinigt diese Sitzungen auf der Grundlage der angegebenen Aktion.

Eine Sitzung gilt als inaktiv, wenn kein Datenverkehr von diesem Teilnehmer auf der Datenebene oder der Steuerungsebene empfangen wird. Sie können eine Aktion angeben, beenden (PCRF informieren und dann die Sitzung löschen) oder löschen (ohne PCRF darüber zu informieren). Die Aktion wird erst ausgeführt, wenn die Sitzung für die im Leerlauf-Timeout-Parameter angegebene Zeit inaktiv war.

So konfigurieren Sie das Timeout für die Leerlaufsitzung und die zugehörige Aktion mithilfe der Befehlszeile

```
set subscriber param [-idleTTL <positive_integer>] [-idleAction <
    idleAction>]
<!--NeedCopy-->
```

Beispiele:

```
set subscriber param -idleTTL 3600 -idleAction ccrTerminate

set subscriber param -idleTTL 3600 -idleAction ccrUpdate

set subscriber param -idleTTL 3600 -idleAction delete
<!--NeedCopy-->
```

Um das Idle-Sitzungs-Timeout zu deaktivieren, setzen Sie das Leerlauf-Timeout auf Null.

setze den Abonnentenparameter —idletTL 0

So konfigurieren Sie das Timeout für die Leerlaufsitzung und die zugehörige Aktion mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Abonnentenparameter konfigurieren** und geben Sie eine **Leerlaufzeit und eine**Inaktivitätsaktion**an.

Protokollierung von Abonnentensitzungen

Wenn Sie die Abonnentenprotokollierung aktivieren, können Sie die Nachrichten der RADIUS- und Gx-Kontrollebene für einen Abonnenten verfolgen und die historischen Daten verwenden, um die Abonnentenaktivitäten zu analysieren. Einige der wichtigsten Attribute sind MSISDN und Zeitstempel. Die folgenden Attribute werden ebenfalls protokolliert:

- Sitzungsereignis (Installieren, Aktualisieren, Löschen, Fehler)
- Gx-Nachrichtentyp (CCR-I, CCR-U, CCR-T, RAR)
- Radius-Nachrichtentyp (Start, Stopp)
- Abonnenten-IP
- Abonnenten-ID-Typ (MSI, ISDN (E164), IMSI)
- Abonnenten-ID-Wert

Mithilfe dieser Protokolle können Sie Benutzer anhand der IP-Adresse und, falls verfügbar, nach MSISDN verfolgen.

Sie können die Protokollierung von Abonnentensitzungen auf einem lokalen oder entfernten Syslog- oder NSLog-Server aktivieren. Das folgende Beispiel zeigt, wie die Abonnentenprotokollierung auf einem Remote-Syslog-Server aktiviert wird.

```
1      > add syslogAction sysact1 192.0.2.0 -loglevel EMERGENCY ALERT
          CRITICAL ERROR WARNING NOTICE INFORMATIONAL -subscriberlog
          enabled
2  <!--NeedCopy-->
```

Aus diesen Protokollen können Sie sich über alle Aktivitäten im Zusammenhang mit einem Benutzer informieren, z. B. die Uhrzeit, zu der eine Sitzung aktualisiert, gelöscht oder erstellt (installiert) wurde. Zusätzlich werden auch Fehlermeldungen protokolliert.

Beispiele:

1. Die folgenden Protokolleinträge sind Beispiele für die Erstellung, Aktualisierung und Löschung von RadiusandGX-Sitzungen.

> 09/30/ 2015:16:29:18 GMT Informatives 0-PPE-0: Standard SUBSCRIBER SESSION_EVENT 147 0: Sitzungsinstallation, GX-Meldungstyp: CCR-I, RADIUS-Nachrichtentyp: Start, IP: 100.10.1.1, ID: E164 - 30000000001
>
> 09/30/ 2015:16:30:18 GMT Informatives 0-PPE-0: Standard SUBSCRIBER SESSION_EVENT 148 0: Sitzungsaktualisierung, GX-Nachrichtentyp: CCR-U, IP: 100.10.1.1, ID: E164 - 30000000001
>
> 09/30/ 2015:17:27:56 GMT Informatives 0-PPE-0: Standard SUBSCRIBER SESSION_EVENT 185 0: Sitzung löschen, GX-Meldungstyp: CCR-T, RADIUS-Nachrichtentyp: Stop, IP: 100.10.1.1, ID: E164 - 30000000001

2. Die folgenden Protokolleinträge sind Beispiele für Fehlermeldungen, z. B. wenn kein Abonnent auf dem PCRF-Server gefunden wird und wenn die Appliance keine Verbindung zum PCRF-Server herstellen kann.

   > 09/30/ 2015:16:44:15 GMT Fehler 0-PPE-0: Standard SUBSCRIBER SESSION_FAILURE 169 0: Fehlerursache: PCRF-Fehlerreaktion, GX-Nachrichtentyp: CCR-I, IP: 100.10.1.1
   >
   > 30. September 13:03:01 09/30/ 2015:16:49:08 GMT 0-PPE-0: default SUBSCRIBER SESSION_FAILURE 176 0: Fehlergrund: Verbindung zu PCRF, GX MsgType: CCR-I, RADIUS MsgType: Start, IP: 100.10.1.1, ID: E164 - 30000000001 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000 #000

Beendigung der LSN-Sitzung durch Abonnenten

In früheren Versionen wurden die entsprechenden LSN-Sitzungen des Abonnenten erst nach Ablauf des konfigurierten LSN-Timeouts entfernt, wenn eine Abonnentensitzung gelöscht wird, wenn eine RADIUS Accounting STOP- oder PCRF-RAR-Nachricht empfangen wird oder wenn ein anderes Ereignis wie TTL-Ablauf oder Flush eingetreten ist. LSN-Sitzungen, die bis zum Ablauf dieses Timeouts geöffnet bleiben, verbrauchen weiterhin Ressourcen auf der Appliance.

Ab Version 11.1 wird ein neuer Parameter (subscrSessionRemoval) hinzugefügt. Wenn dieser Parameter aktiviert ist und die Abonnenteninformationen aus der Abonnentendatenbank gelöscht werden, werden LSN-Sitzungen, die diesem Abonnenten entsprechen, ebenfalls entfernt. Wenn dieser Parameter deaktiviert ist, wird für die Abonnentensitzungen ein Timeout ausgelöst, wie in den LSN-Timeout-Einstellungen angegeben.

So konfigurieren Sie die abonnentenorientierte Beendigung von LSN-Sitzungen mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

setze den LSN-Parameter -SubscrSessionRemoval (AKTIVIERT)	DEAKTIVIERT)

```
1      > set lsn parameter -subscrSessionRemoval ENABLED
2      Done
3      > sh lsn parameter
4                  LSN Global Configuration:
5
6                  Active Memory Usage: 0 MBytes
7                  Configured Memory Limit: 0 MBytes
8                  Maximum Memory Usage Limit: 912 MBytes
9                  Session synchronization: ENABLED
10                 Subscriber aware session removal: ENABLED
11 <!--NeedCopy-->
```

So konfigurieren Sie die abonnentenorientierte Beendigung von LSN-Sitzungen mithilfe der GUI

1. Navigieren Sie zu **System** > **Large Scale NAT**.
2. Klicken Sie unter **Erste Schritte**auf **LSN-Parameter festlegen**.
3. Stellen Sie den **Parameter Abonnentensensitive Sitzungsentfernung**ein.

Problembehandlung

Wenn Ihr Deployment nicht wie erwartet funktioniert, verwenden Sie die folgenden Befehle zur Fehlerbehebung:

- show subscriber gxinterface Die Ausgabe
  dieses Befehls kann die folgenden Fehlermeldungen enthalten (hier mit vorgeschlagenen Antworten):
  - Gx-Schnittstelle nicht konfiguriert — Verwenden Sie den Befehl set subscriber param, um den richtigen Schnittstellentyp zu konfigurieren.
  - PCRF nicht konfiguriert — Konfigurieren Sie einen virtuellen Diameter-vServer oder -Dienst auf einer GXSchnittstelle. Verwenden Sie den Befehl set subscriber gx interface, um dieser Schnittstelle einen virtuellen Diameter-Server oder -Dienst zuzuweisen.
  - PCRF ist nicht bereit. Überprüfen Sie den entsprechenden vServer/Service auf weitere Details. Verwenden Sie den Befehl show LB vserver oder show service, um den Status des Dienstes zu überprüfen.
  - NetScaler wartet auf CEA von PCRF-Fähigkeit. Die Verhandlungen zwischen dem PCRF und NetScaler schlagen möglicherweise fehl. Dies könnte ein intermittierender Zustand sein.

Wenn es weiterhin auftritt, überprüfen Sie die DIAMETER-Einstellungen auf Ihrem PCRF-Server.

- Der Speicher ist nicht zum Speichern von Abonnentensitzungen konfiguriert. Bitte verwenden Sie 'set extendedmemoryparam -memlimit <>'-Verwenden Sie den Befehl set extendedmemoryparam, um den erweiterten Speicher zu konfigurieren.

- show subscriber radiusinterface
  Wenn „Nicht konfiguriert" die Ausgabe dieses Befehls ist, verwenden Sie den Befehl set subscriber radiusinterface, um einen RadiusListener-Dienst anzugeben.

Wenn die Abonnentenprotokollierung aktiviert ist, können Sie detailliertere Informationen aus den Protokolldateien abrufen.

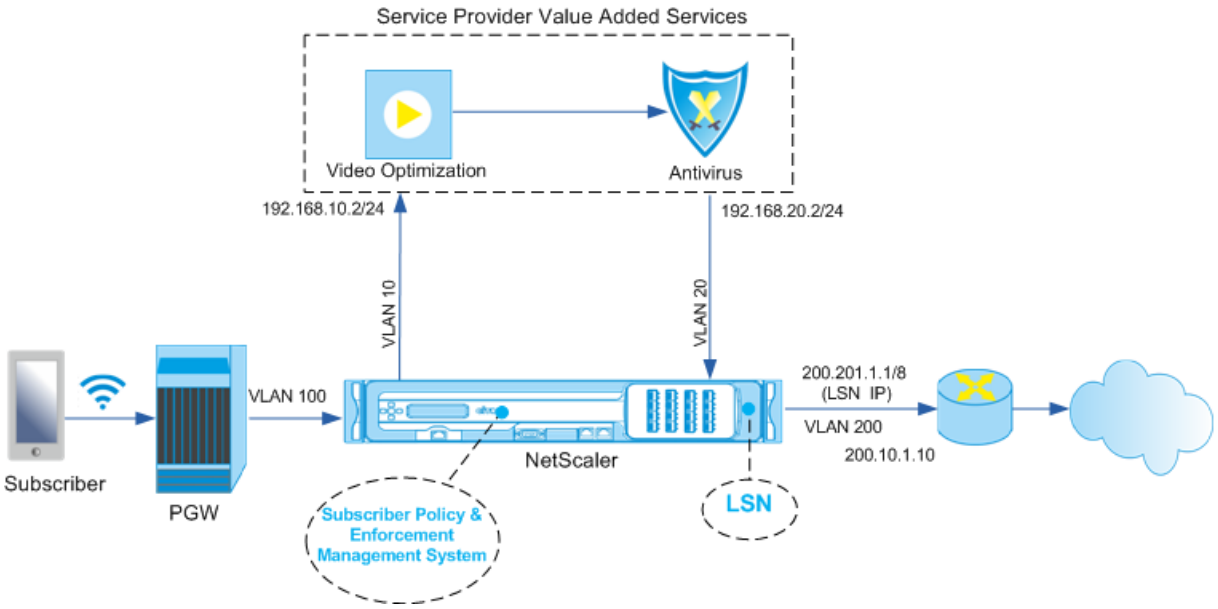
Abonnentenbewusste Verkehrssteuerung

May 11, 2023

Traffic Steering leitet den Abonnentenverkehr von einem Punkt zum anderen. Wenn ein Abonnent eine Verbindung zum Netzwerk herstellt, ordnet das Paket-Gateway dem Abonnenten eine IP-Adresse zu und leitet das Datenpaket an die NetScaler-Appliance weiter. Die Appliance kommuniziert über die Gx-Schnittstelle mit dem PCRF-Server, um die Richtlinieninformationen abzurufen. Abhängig von den Richtlinieninformationen führt die Appliance eine der folgenden Aktionen aus:

- Leiten Sie das Datenpaket an eine andere Gruppe von Diensten weiter (wie in der folgenden Abbildung dargestellt).
- Lass das Paket fallen.
- Führen Sie nur Large Scale NAT (LSN) durch, wenn LSN auf der Appliance konfiguriert ist.

Die in der folgenden Abbildung gezeigten Werte werden in der CLI-Prozedur konfiguriert, die der Abbildung folgt. Ein virtueller Content-Switching-Server auf der NetScaler-Appliance leitet Anfragen an die Mehrwertdienste weiter oder überspringt sie, je nach der definierten Regel, und sendet das Paket dann an das Internet, nachdem LSN ausgeführt wurde.



So konfigurieren Sie Traffic Steering für die obige Bereitstellung mithilfe der CLI

Fügen Sie die Subnetz-IP-Adressen (SNIP) der Appliance hinzu.

Beispiel:

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 100.100.100.1 255.0.0.0 -type snip

add ns ip 200.200.200.1 255.0.0.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Fügen Sie die VLANs hinzu. VLANs helfen der Appliance dabei, die Quelle des Datenverkehrs zu identifizieren. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.

Beispiel:

```
add vlan 10

add vlan 20

add vlan 100
```



```
6
7  add vlan 200
8
9  bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0
10
11 bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0
12
13 bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0
14
15 bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.1.1.1 255.0.0.0
16 <!--NeedCopy-->
```

Geben Sie das VLAN an, über das der Abonnentenverkehr auf der Appliance ankommt. Geben Sie den Dienstpfad AVP an, der der Appliance mitteilt, wo in der Abonnentensitzung nach dem Dienstpfadnamen gesucht werden soll. Geben Sie für die primäre PCEF-Funktionalität den Schnittstellentyp als RadiusandGX an.

Beispiel:

```
1 set ns param -servicePathIngressVLAN 100
2
3 set subscriber gxinterface -servicepathAVP 1001 1005 -
     servicepathVendorid 10415
4
5 set subscriber param -interfaceType RadiusAndGx
6 <!--NeedCopy-->
```

Konfigurieren Sie einen Dienst und einen virtuellen Server vom Typ Diameter und binden Sie den Dienst an den virtuellen Server. Geben Sie dann die Parameter der PCRF-Realm- und Abonnenten-Gx-Schnittstelle an. Für die primäre PCEF-Funktionalität konfigurieren Sie einen RADIUS-Listener-Dienst und eine RADIUS-Schnittstelle.

Beispiel:

```
1 add service sd1 10.102.232.200 DIAMETER 3868
2
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4
5 bind lb vserver vdiam sd1
6
7 set ns diameter -identity netscaler.sc1.net -realm pcrf1.net
8
9 set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
     holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120
```



```
10
11 add service srad1 10.102.232.236 RADIUSListener 1813
12
13 set subscriber radiusInterface -listeningService srad1
14 <!--NeedCopy-->
```

Fügen Sie Dienstfunktionen hinzu, um ein VAS mit einem Eingangs-VLAN zu verknüpfen. Fügen Sie einen Dienstpfad hinzu, um die Kette zu definieren, d. h. geben Sie das VAS an, an das das Paket gesendet werden muss, und die Reihenfolge, in der es an dieses VAS gesendet werden muss. Der Dienstpfadname wird normalerweise vom PCRF gesendet. Der Dienstpfad des Standard-Abonnentenprofils (*) gilt jedoch, wenn einer der folgenden Punkte zutrifft:

- PCRF hat keine Abonnenteninformationen.
- Die Abonnenteninformationen beinhalten diesen AVP nicht.
- Die Appliance kann den PCRF nicht abfragen. Beispielsweise ist der Dienst, der den PCRF repräsentiert, DOWN.

Der Dienstpfad AVP, der diesen Namen enthält, muss bereits als Teil der globalen Konfiguration konfiguriert sein. Binden Sie die Servicefunktion an den Dienstpfad. Der Serviceindex gibt die Reihenfolge an, in der das VAS zur Kette hinzugefügt wird. Die höchste Zahl (255) gibt den Anfang der Kette an.

Beispiel:

```
1 add ns servicefunction SF1 -ingressVLAN 20
2
3 add ns servicepath pol1
4
5 bind ns servicepath pol1 -servicefunction SF1 -index 255
6
7 add subscriber profile * -subscriberrules default_path
8 <!--NeedCopy-->
```

Fügen Sie die LSN-Konfiguration hinzu. Definieren Sie also den NAT-Pool und identifizieren Sie die Clients, für die die Appliance LSN ausführen muss.

```
1 add lsn pool pool1
2
3 bind lsn pool pool1 200.201.1.1
4
5 add lsn client client1
6
7 bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0
8
9 add lsn group group1 -clientname client1
10
```



```
bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

Die Appliance führt standardmäßig LSN aus. Um LSN zu überschreiben, müssen Sie ein Netzprofil mit aktiviertem OverrideLSN-Parameter erstellen und dieses Profil an alle virtuellen Lastausgleichsserver binden, die für Value Added Services (VASS) konfiguriert sind.

Beispiel:

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Konfigurieren Sie das VAS auf der Appliance. Dazu gehört das Erstellen der Dienste und virtuellen Server und das anschließende Binden der Dienste an die virtuellen Server.

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vint sint
<!--NeedCopy-->
```

Fügen Sie die Content Switching (CS) -Konfiguration hinzu. Dazu gehören virtuelle Server, Richtlinien und die zugehörigen Aktionen. Der Datenverkehr kommt auf dem virtuellen CS-Server an und wird dann an den entsprechenden virtuellen Load-Balancing-Server umgeleitet. Definieren Sie Ausdrücke, die einen virtuellen Server mit einer Servicefunktion verknüpfen.

Beispiel:

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csactint -targetLBVserver vint

```



```
add cs policy cspol1 -rule  SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
    SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```

So konfigurieren Sie die Verkehrssteuerung auf der Appliance mithilfe der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** und fügen Sie die Subnetz-IP-Adressen hinzu.
2. Navigieren Sie zu System > Netzwerk > **VLANs und fügen Sie VLANs** hinzu. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.
3. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Configure Service Path Ingress VLAN und geben Sie ein Eingangs-VLAN** an.
4. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter** > **Abonnentenparameter konfigurieren** und geben Sie Folgendes an:
   - Schnittstellentyp: Geben Sie **Radius**und GX an.
   - Konfigurieren Sie einen virtuellen Diameterserver, einen PCRF-Realm und die GX-Schnittstellenparameter für Abonnenten.
   - Geben Sie die RADIUS-Schnittstellenparameter an.
5. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Function** und fügen Sie Dienstfunktionen hinzu, um einem Eingangs-VLAN einen Mehrwertdienst zuzuordnen.
6. Navigieren Sie zu **System** > **Netzwerk** > **Large Scale NAT**. Klicken Sie auf **Pools** und fügen Sie einen Pool hinzu. Klicken Sie auf **Kunden** und fügen Sie einen Kunden hinzu. Klicken Sie auf **Gruppen**, fügen Sie eine Gruppe hinzu und geben Sie den Client an. Bearbeiten Sie die Gruppe und binden Sie den Pool an diese Gruppe.
7. Navigieren Sie zu **System** > **Netzwerk >**Netzprofile**** und fügen Sie ein Netzprofil hinzu. Wählen Sie **LSN überschreiben**aus. Navigieren Sie optional zu **System** > **Netzwerk** > **Einstellungen** > **Layer-3-Parameter konfigurieren** und stellen Sie sicher, dass **LSN überschreiben nicht ausgewählt** ist.
8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server** und konfigurieren Sie die virtuellen Server und Mehrwertdienste auf der Appliance. Binden Sie die Dienste und das Netzprofil an den virtuellen Server.
9. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server** und konfigurieren Sie einen virtuellen Server, eine Richtlinie und eine Aktion. Geben Sie den virtuellen Zielserver für Lastenausgleich an.

So konfigurieren Sie Service Chaining auf der Appliance mithilfe der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** und fügen Sie die Subnetz-IP-Adressen hinzu.
2. Navigieren Sie zu System > Netzwerk > **VLANs und fügen Sie VLANs** hinzu. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.
3. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Configure Service Path Ingress VLAN und geben Sie ein Eingangs-VLAN** an.
4. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter** > **Abonnentenparameter konfigurieren** und geben Sie Folgendes an:
   - Schnittstellentyp: Geben Sie **Radius**und GX an.
   - Konfigurieren Sie einen virtuellen Diameterserver, einen PCRF-Realm und die GX-Schnittstellenparameter für Abonnenten.
   - Geben Sie die RADIUS-Schnittstellenparameter an.
5. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Function** und fügen Sie Dienstfunktionen hinzu, um einem Eingangs-VLAN einen Mehrwertdienst zuzuordnen.
6. Navigieren Sie zu **System** > **Netzwerk** > **Large Scale NAT**. Klicken Sie auf **Pools** und fügen Sie einen Pool hinzu. Klicken Sie auf **Kunden** und fügen Sie einen Kunden hinzu. Klicken Sie auf **Gruppen**, fügen Sie eine Gruppe hinzu und geben Sie den Client an. Bearbeiten Sie die Gruppe und binden Sie den Pool an diese Gruppe.
7. Navigieren Sie zu **System** > **Netzwerk >**Netzprofile**** und fügen Sie ein Netzprofil hinzu. Wählen Sie **LSN überschreiben**aus. Navigieren Sie optional zu **System** > **Netzwerk** > **Einstellungen** > **Layer-3-Parameter konfigurieren** und stellen Sie sicher, dass **LSN überschreiben nicht ausgewählt** ist.
8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server** und konfigurieren Sie die virtuellen Server und Mehrwertdienste auf der Appliance. Binden Sie die Dienste und das Netzprofil an den virtuellen Server.
9. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server** und konfigurieren Sie einen virtuellen Server, eine Richtlinie und eine Aktion. Geben Sie den virtuellen Zielserver für Lastenausgleich an.

Abonnentenbewusste Service-Verkettung

May 11, 2023

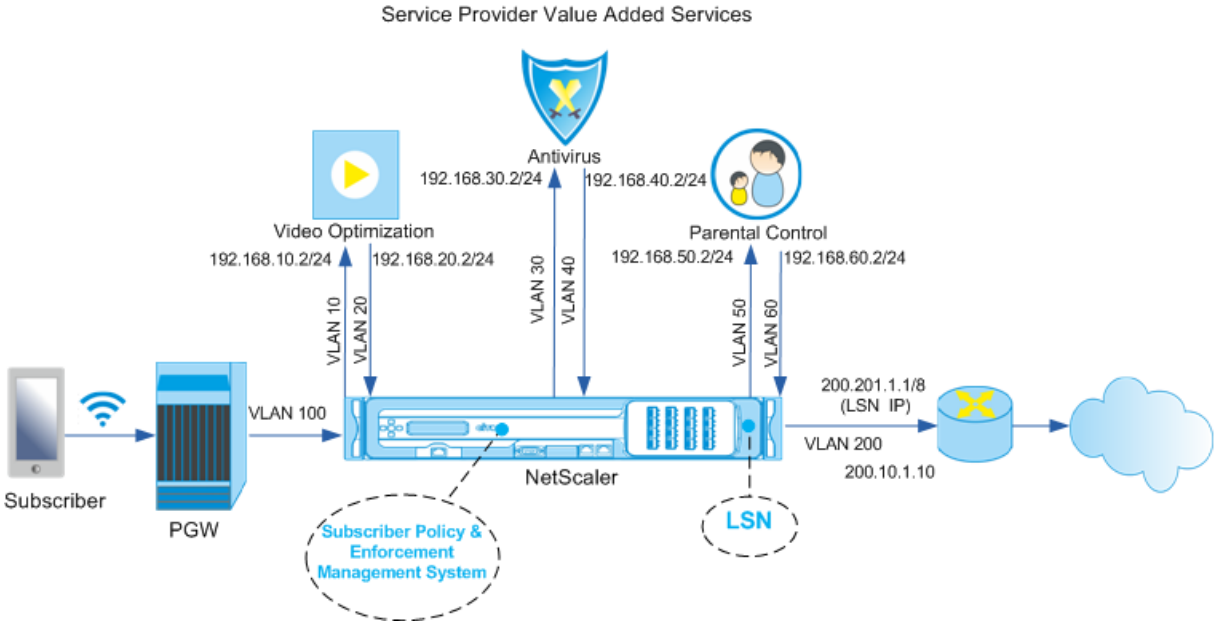
Angesichts des enormen Anstiegs des Datenverkehrs über Telekommunikationsnetze ist es für Dienstanbieter nicht mehr möglich, den gesamten Datenverkehr über alle Mehrwertdienste (VAS) zu steuern. Ein Dienstanbieter sollte in der Lage sein, die Nutzung von VAS zu optimieren und den Traffic intelligent zu steuern, um das Benutzererlebnis zu verbessern. Beispielsweise ist keine Videooptimierung für Traffic erforderlich, der kein Video enthält. Wenn ein Abonnent mit einem

4G-Netzwerk verbunden ist, können Inhalte außerdem in High Definition (HD) gestreamt werden, und eine Videooptimierung ist möglicherweise nicht erforderlich. Die Videooptimierung verbessert jedoch die Benutzererfahrung in einem 3G-Netzwerk. In ähnlicher Weise bietet Caching eine schnellere und bessere Benutzererfahrung und kann je nach Abonnentenplan aktiviert werden. Ein weiteres Beispiel für VAS ist die elterliche Kontrolle. Wenn Eltern einem minderjährigen Kind ein Handy zur Verfügung stellen, möchten sie eine gewisse Kontrolle über die Websites haben, die ihr Kind besucht.

Um dies und mehr zu tun, müssen Dienstanbieter in der Lage sein, Mehrwertdienste pro Abonnent anzubieten. Mit anderen Worten, die Entitäten im Netzwerk des Dienstanbieters müssen in der Lage sein, die Teilnehmerinformationen zu extrahieren und das Paket auf der Grundlage dieser Informationen intelligent zu steuern.

Die Servicekette bestimmt die Reihe von Diensten, über die der Datenverkehr eines Abonnenten geleitet werden muss, bevor er ins Internet geht. Anstatt den gesamten Datenverkehr an alle Dienste zu senden, leitet der NetScaler alle Anfragen von einem Abonnenten auf der Grundlage der für diesen Abonnenten definierten Richtlinie intelligent an eine bestimmte Gruppe von Diensten weiter.

Die folgende Abbildung zeigt die Entitäten, die an Service Chaining beteiligt sind. Die angezeigten Werte werden in dem Verfahren konfiguriert, das der Abbildung folgt. Ein virtueller Content-Switching-Server auf der NetScaler-Appliance leitet Anfragen an die Mehrwertdienste weiter oder überspringt sie, je nach der definierten Regel, und sendet das Paket dann an das Internet, nachdem LSN ausgeführt wurde.



So konfigurieren Sie Service Chaining für die obige Bereitstellung mithilfe der CLI

Fügen Sie die Subnetz-IP-Adressen (SNIP) der Appliance hinzu.

Beispiel:


```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.30.1 255.255.255.0 -type snip

add ns ip 192.168.40.1 255.255.255.0 -type snip

add ns ip 192.168.50.1 255.255.255.0 -type snip

add ns ip 192.168.60.1 255.255.255.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Fügen Sie die VLANs hinzu. VLANs helfen der Appliance dabei, die Quelle des Datenverkehrs zu identifizieren. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen. Fügen Sie für jedes VAS ein Eingangs- und ein Ausgangs-VLAN hinzu.

Beispiel:

```
add vlan 10

add vlan 20

add vlan 30

add vlan 40

add vlan 50

add vlan 60

add vlan 100

add vlan 200

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.30.1 255.255.255.0
```



```
22
23 bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.40.1 255.255.255.0
24
25 bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.50.1 255.255.255.0
26
27 bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.60.1 255.255.255.0
28
29 bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0
30
31 bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.201.1.1 255.0.0.0
32 <!--NeedCopy-->
```

Geben Sie das VLAN an, über das der Abonnentenverkehr auf der Appliance ankommt. Geben Sie den Dienstpfad AVP an, der der Appliance mitteilt, wo in der Abonnentensitzung nach dem Dienstpfadnamen gesucht werden soll. Geben Sie für die primäre PCEF-Funktionalität den Schnittstellentyp als RadiusandGX an.

Beispiel:

```
1 set ns param -servicePathIngressVLAN 100
2
3 set subscriber gxinterface -servicepathAVP 1001 1005 -
     servicepathVendorid 10415
4
5 set subscriber param -interfaceType RadiusAndGx
6 <!--NeedCopy-->
```

Konfigurieren Sie einen Dienst und einen virtuellen Server vom Typ Diameter und binden Sie den Dienst an den virtuellen Server. Geben Sie dann die Parameter der PCRF-Realm- und Abonnenten-Gx-Schnittstelle an. Für die primäre PCEF-Funktionalität konfigurieren Sie einen RADIUS-Listener-Dienst und eine RADIUS-Schnittstelle.

Beispiel:

```
1 add service sd1 10.102.232.200 DIAMETER 3868
2
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4
5 bind lb vserver vdiam sd1
6
7 set ns diameter -identity netscaler.sc1.net -realm pcrf1.net
8
9 set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
     holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120
```



```
10
11 add service srad1 10.102.232.236 RADIUSListener 1813
12
13 set subscriber radiusInterface -listeningService srad1
14 <!--NeedCopy-->
```

Fügen Sie Dienstfunktionen hinzu, um ein VAS mit einem Eingangs-VLAN zu verknüpfen. Fügen Sie einen Dienstpfad hinzu, um die Kette zu definieren, d. h. geben Sie das VAS an, an das das Paket gesendet werden muss, und die Reihenfolge, in der es an dieses VAS gesendet werden muss. Der Dienstpfadname wird normalerweise vom PCRF gesendet. Der Dienstpfad des Standard-Abonnentenprofils (*) gilt jedoch, wenn einer der folgenden Punkte zutrifft:

- PCRF hat keine Abonnenteninformationen.
- Die Abonnenteninformationen beinhalten diesen AVP nicht.
- Die Appliance kann den PCRF nicht abfragen. Beispielsweise ist der Dienst, der den PCRF repräsentiert, DOWN.

Der Dienstpfad AVP, der diesen Namen enthält, muss zuvor als Teil der globalen Konfiguration konfiguriert werden. Binden Sie die Servicefunktion an den Dienstpfad. Der Serviceindex gibt die Reihenfolge an, in der das VAS zur Kette hinzugefügt wird. Die höchste Zahl (255) gibt den Anfang der Kette an.

Beispiel:

```
1  add ns servicefunction SF1 -ingressVLAN 20
2
3  add ns servicefunction SF2 -ingressVLAN 40
4
5  add ns servicefunction SF3 -ingressVLAN 60
6
7  add ns servicepath pol1
8
9  bind ns servicepath pol1 -servicefunction SF1 -index 255
10
11 bind ns servicepath pol1 -servicefunction SF2 -index 254
12
13 bind ns servicepath pol1 -servicefunction SF3 -index 253
14
15 add ns servicepath pol2
16
17 bind ns servicepath pol2 -servicefunction SF2 -index 255
18
19 add ns servicepath pol3
20
21 bind ns servicepath pol3 -servicefunction SF1 -index 255
```



```
22
23 add subscriber profile * -subscriberrules default_path
24 <!--NeedCopy-->
```

Fügen Sie die LSN-Konfiguration hinzu. Definieren Sie also den NAT-Pool und identifizieren Sie die Clients, für die die Appliance LSN ausführen muss.

Beispiel:

```
1 add lsn pool pool1
2
3 bind lsn pool pool1 200.201.1.1
4
5 add lsn client client1
6
7 bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0
8
9 add lsn group group1 -clientname client1
10
11 bind lsn group group1 -poolname pool1
12 <!--NeedCopy-->
```

Die Appliance führt standardmäßig LSN aus. Um LSN zu überschreiben, müssen Sie ein Netzprofil mit aktiviertem OverrideLSN-Parameter erstellen und dieses Profil an alle virtuellen Lastausgleichsserver binden, die für Value Added Services (VASS) konfiguriert sind.

Beispiel:

```
1 add netprofile np1
2
3 set netprofile np1 -overrideLsn ENABLED
4
5 set lb vserver vs1 -netprofile np1
6 <!--NeedCopy-->
```

Konfigurieren Sie das VAS auf der Appliance. Dazu gehört das Erstellen der Dienste und virtuellen Server und das anschließende Binden der Dienste an die virtuellen Server.

Beispiel:

```
1 add service vas1 192.168.10.2 ANY 80 -usip YES
2
3 add service vas2 192.168.30.2 ANY 80 -usip YES
4
5 add service vas3 192.168.50.2 ANY 80 -usip YES
6
```



```
add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vs2 ANY -m MAC -l2Conn ON

add lb vserver vs3 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vs2 vas2

bind lb vserver vs3 vas3

bind lb vserver vint sint
<!--NeedCopy-->
```

Fügen Sie die Content Switching (CS) -Konfiguration hinzu. Dazu gehören virtuelle Server, Richtlinien und die zugehörigen Aktionen. Der Datenverkehr kommt auf dem virtuellen CS-Server an und wird dann an den entsprechenden virtuellen Load-Balancing-Server umgeleitet. Definieren Sie Ausdrücke, die einen virtuellen Server mit einer Servicefunktion verknüpfen.

Beispiel:

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csact2 -targetLBVserver vs2

add cs action csact3 -targetLBVserver vs3

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

add cs policy cspol2 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF2") &&
   SYS.VSERVER("vs2").STATE.EQ(UP)" -action csact2

add cs policy cspol3 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF3") &&
   SYS.VSERVER("vs3").STATE.EQ(UP)" -action csact3

```



```
bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -policyName cspol2 -priority 120

bind cs vserver cs1 -policyName cspol3 -priority 130

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```

So konfigurieren Sie Service Chaining auf der Appliance mithilfe der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** und fügen Sie die Subnetz-IP-Adressen hinzu.
2. Navigieren Sie zu **System** > **Netzwerk** > **VLANs und fügen Sie VLANs** hinzu. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.
3. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Configure Service Path Ingress VLAN und geben Sie ein Eingangs-VLAN** an.
4. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter** > **Abonnentenparameter konfigurieren** und geben Sie Folgendes an:
   - Schnittstellentyp: Geben Sie **Radius**und GX an.
   - Konfigurieren Sie einen virtuellen Diameterserver, einen PCRF-Realm und die GX-Schnittstellenparameter für Abonnenten.
   - Geben Sie die RADIUS-Schnittstellenparameter an.
5. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Function** und fügen Sie Dienstfunktionen hinzu, um einem Eingangs-VLAN einen Mehrwertdienst zuzuordnen.
6. Navigieren Sie zu **System** > **Netzwerk** > **Large Scale NAT**. Klicken Sie auf **Pools** und fügen Sie einen Pool hinzu. Klicken Sie auf **Kunden** und fügen Sie einen Kunden hinzu. Klicken Sie auf **Gruppen**, fügen Sie eine Gruppe hinzu und geben Sie den Client an. Bearbeiten Sie die Gruppe und binden Sie den Pool an diese Gruppe.
7. Navigieren Sie zu **System** > **Netzwerk >**Netzprofile**** und fügen Sie ein Netzprofil hinzu. Wählen Sie **LSN überschreiben**aus. Navigieren Sie optional zu **System** > **Netzwerk** > **Einstellungen** > **Layer-3-Parameter konfigurieren** und stellen Sie sicher, dass **LSN überschreiben nicht ausgewählt** ist.
8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server** und konfigurieren Sie die virtuellen Server und Mehrwertdienste auf der Appliance. Binden Sie die Dienste und das Netzprofil an den virtuellen Server.
9. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server** und konfigurieren Sie einen virtuellen Server, eine Richtlinie und eine Aktion. Geben Sie den virtuellen Zielserver für Lastenausgleich an.

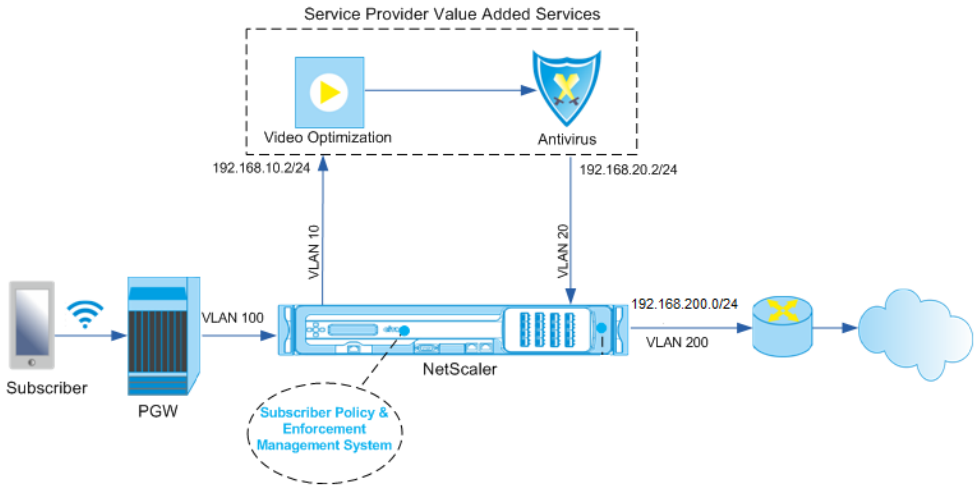
Abonnentenbewusste Verkehrssteuerung mit TCP-Optimierung

May 11, 2023

Traffic Steering leitet den Abonnentenverkehr von einem Punkt zum anderen. Wenn ein Abonnent eine Verbindung zum Netzwerk herstellt, ordnet das Paket-Gateway dem Abonnenten eine IP-Adresse zu und leitet das Datenpaket an die NetScaler-Appliance weiter. Die Appliance kommuniziert über die Gx-Schnittstelle mit dem PCRF-Server, um die Informationen zur Abonnentenrichtlinie abzurufen. Abhängig von den Richtlinieninformationen führt die Appliance eine der folgenden Aktionen aus:

- Leiten Sie das Datenpaket an eine andere Gruppe von Diensten weiter (wie in der folgenden Abbildung dargestellt).
- Führen Sie nur eine TCP-Optimierung durch.

Die in der folgenden Abbildung gezeigten Werte werden in der CLI-Prozedur konfiguriert, die der Abbildung folgt. Ein virtueller Content Switching-Server auf der NetScaler-Appliance leitet Anfragen an die Mehrwertdienste weiter oder überspringt sie und führt je nach definierter Regel eine TCP-Optimierung durch und sendet das Paket dann an das Internet.



> **Hinweis**
>
> Die Unterstützung für die unten abgebildete Konfiguration wurde in Version 11.1 Build 50.10 eingeführt.

Gehen Sie wie folgt vor, um Traffic Steering für die obige Bereitstellung mithilfe der CLI zu konfigurieren:

1. Fügen Sie die Subnetz-IP-Adressen (SNIP) der Appliance hinzu.

```
1 add ns ip 192.168.10.1 255.255.255.0 -type snip
```



```
2
3 add ns ip 192.168.20.1 255.255.255.0 -type snip
4
5 add ns ip 192.168.100.1 255.255.255.0 -type snip
6
7 add ns ip 192.168.200.1 255.255.255.0 -type snip
8
9 add ns ip 10.102.232.236 255.255.255.0  - type snip
10 <!--NeedCopy-->
```

2. Fügen Sie die VLANs hinzu. VLANs helfen der Appliance dabei, die Quelle des Datenverkehrs zu identifizieren. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.

```
1 add vlan 10
2
3 add vlan 20
4
5 add vlan 100
6
7 add vlan 200
8
9 add vlan 102
10
11 bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1
      255.255.255.0
12
13 bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1
      255.255.255.0
14
15 bind vlan 100 -ifnum 1/2 -tagged -IPAddress 192.168.100.1
      255.255.255.0
16
17 bind vlan 200 -ifnum 1/2 -tagged -IPAddress 192.168.200.1
      255.255.255.0
18
19 bind vlan 102  - ifnum 1/1  - tagged  - IPAddress 10.102.232.236
      255.255.255.0
20 <!--NeedCopy-->
```

3. Konfigurieren Sie einen Dienst und einen virtuellen Server vom Typ Diameter und binden Sie den Dienst an den virtuellen Server. Geben Sie den PCRF-Bereich und die Werte für die Gx-Schnittstellenparameter des Abonnenten an. Geben Sie auch den Dienstpfad AVP an, der angibt, wo die Appliance den Dienstpfadnamen innerhalb der Abonnentensitzung finden kann. Für die primäre PCEF-Funktionalität konfigurieren Sie einen RADIUS-Listener-Dienst und eine

RADIUS-Schnittstelle und geben Sie den Schnittstellentyp als „RadiusAndGX“ an.

```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER
   -persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set extendedmemoryparam -memLimit 2558

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net

set subscriber gxinterface -servicepathAVP 1001 1005 -
   servicepathVendorid 10415

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1

set subscriber param -interfaceType RadiusAndGx
<!--NeedCopy-->
```

4. Geben Sie ein standardmäßiges Abonnentenprofil (*) an, das angewendet werden soll, wenn einer der folgenden Punkte zutrifft:

   - PCRF hat keine Abonnenteninformationen.
   - Die Abonnenteninformationen enthalten nicht den Dienstpfad AVP.
   - Die Appliance kann den PCRF nicht abfragen. Beispielsweise ist der Dienst, der den PCRF repräsentiert, DOWN.

```
add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

5. Erstellen Sie TCP-Profile für den VAS- bzw. TCP-Optimierungspfad. Der an VAS gelenkte Verkehr wird vor oder nach dem Verlassen des VAS keiner TCP-Optimierung unterzogen. Daher sollte der TCP-Modus des VAS-Profils auf TRANSPARENT gesetzt werden, während der TCP-Modus des TcpOpt-Profils auf ENDPOINT gesetzt werden sollte.

   füge ns tcpProfile VAS —tcpMode TRANSPARENT hinzu

   fügen Sie ns TCPProfile tcpOpt -WS AKTIVIERT -SACK AKTIVIERT -WSval 8 -mss 1460 -MaxBurst 30 -InitialCwnd 16 -oooqGröße 15000 -minRTO 800 -bufferSize 4000000 -flavor BIC -DynamicReceiveBuffering AKTIVIERT -KA AKTIVIERT -SendBuffSize 4000000 -RSTWindowAttenuate

AKTIVIERT -SpoofSyndrop AKTIVIERT -ecn AKTIVIERT -frto -aktiviert maxcwnd 1000000 -fack AKTIVIERT -RSTMaxAck aktiviert -tcpmode ENDPUNKT

6. Konfigurieren Sie den Lastenausgleich für die VAS-Server. Erstellen Sie einen nicht adressierbaren virtuellen Server vom Typ TCP. Erstellen Sie TCP-Dienste mit den IP-Adressen der VAS-Server und binden Sie die Dienste an den virtuellen Server. Der virtuelle Server und die Dienste verwenden das transparente TCP-Profil, das für den VAS-Pfad erstellt wurde:

```
add service vas1 192.168.10.2 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS

add service vas2 192.168.10.3 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS

add lb vserver vs1 TCP -m MAC -l2Conn ON  - tcpProfileName VAS

bind lb vserver vs1 vas1

bind lb vserver vs1 vas2
<!--NeedCopy-->
```

7. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, um ausgehenden VAS-Verkehr zu erfassen. Dieser vServer überwacht das VAS-Ausgangs-VLAN und verwendet das transparente TCP-Profil:

```
add lb vserver vsint TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ(20)"
     - Listenpriority 30  - l2Conn ON  - tcpProfileName VAS
<!--NeedCopy-->
```

8. Fügen Sie einen virtuellen TCP-Optimierungsserver hinzu, der auf jeglichen Datenverkehr im drahtlosen VLAN wartet und das für den TCP-Optimierungspfad erstellte Endpunkt-TCP-Profil verwendet:

```
add lb vserver vs-TcpOpt TCP * * -Listenpolicy "client.vlan.id.eq
    (100)"  - Listenpriority 20 -l2Conn ON -tcpProfileName TCPOpt
<!--NeedCopy-->
```

9. Fügen Sie die Content Switching (CS) -Konfiguration hinzu. Dazu gehören virtuelle Server, Richtlinien und die zugehörigen Aktionen. Der virtuelle CS-Server empfängt den Datenverkehr und leitet ihn gemäß den definierten CS-Richtlinien an den entsprechenden virtuellen Load-Balancing-Server weiter. Erstellen Sie einen virtuellen CS TCP-Server, der auf jeglichen Datenverkehr im drahtlosen VLAN mit der höchsten Priorität wartet und das TCP-Profil für Endgeräte verwendet. Erstellen Sie eine CS-Richtlinie, die als TRUE ausgewertet wird, wenn „vas“ die Abonnentenregel ist, und geben Sie eine CS-Aktion an, die den Datenverkehr zu VAS

leitet. Machen Sie den virtuellen TCP-Optimierungsserver zum Standard-LB-vserver. Jeglicher Abonnentenverkehr mit einer anderen Regel als „vas“ wird über den standardmäßigen LB-vserver geleitet.

```
add cs vserver cs1 TCP * * -Listenpolicy "client.vlan.id.eq(100)" - Listenpriority 10 -l2Conn ON  - tcpProfileName TCPOpt

add cs action csact1 -targetLBVserver vs1

add cs policy cspol1 -rule  SUBSCRIBER.RULE_ACTIVE("vas") && SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1

bind cs vserver cs1 -lbvserver vs-TcpOpt
<!--NeedCopy-->
```

10. Fügen Sie statische oder richtlinienbasierte Routen zum Internet hinzu. Dynamisches Routing wird in dieser Konfiguration ebenfalls unterstützt. Im folgenden Beispiel werden richtlinienbasierte Routen verwendet:

```
add ns pbr pbr-vlan100-to-vlan200 ALLOW -nextHop 192.168.200.10 -vlan 100 -priority 10

add ns pbr pbr-vlan20-to-vlan200 ALLOW -nextHop 192.168.200.10 -vlan 20 -priority 11

apply ns pbrs
<!--NeedCopy-->
```

Hinweis

- Die CS-Richtlinien können zusätzlich zu den Abonnentenausdrücken IP-Adressen und Portnummern enthalten, zum Beispiel SUBSCRIBER.RULE_ACTIVE („vas“) && (CLIENT.TCP.DSTPORT.EQ (80) || CLIENT.TCP.DSTPORT.EQ (443). Sie können auch HTTP-basierte Ausdrücke enthalten, zum Beispiel HTTP.REQ.HOSTNAME.DOMAIN.EQ („somedomain.com“). Ersetzen Sie in diesem Fall TCP-Entitäten (vserver, service usw.) durch HTTP. Die TCP-Profilkonfiguration bleibt dieselbe.
- Fügen Sie eine IPv6-Konfiguration (Adressen, Routen, PBRs) hinzu, um IPv6-Abonnenten zu unterstützen. Die Client-Anwendungen von Happy Eyeballs funktionieren sowohl für VAS- als auch für TCP-Optimierungspfade reibungslos.
- Fügen Sie VLANs, IP-Adressen, PBRs und virtuelle LB-Server vor VAS (vs1, vs2 usw.) hinzu, um mehrere Abonnentenflüsse zu unterstützen. Ändern Sie die Listen-Richtlinien von CS

> vserver „cs1" und LB vserver „vsint", um die zusätzlichen VLANs einzubeziehen.

Richtlinienbasierte TCP-Profilauswahl

May 11, 2023

Sie können die NetScaler Appliance so konfigurieren, dass sie die TCP-Optimierung basierend auf Abonnentenattributen durchführt. Beispielsweise kann die Appliance zur Laufzeit verschiedene TCP-Profile auswählen, basierend auf dem Netzwerk, mit dem das Benutzergerät (UE) verbunden ist. Auf diese Weise können Sie die Benutzererfahrung eines mobilen Benutzers verbessern, indem Sie einige Parameter in den TCP-Profilen festlegen und dann eine Richtlinie verwenden, um das entsprechende Profil auszuwählen.

Erstellen Sie separate TCP-Profile für Abonnenten, die sich über ein 4G-Netzwerk verbinden, und für Benutzer, die sich über ein anderes Netzwerk verbinden. Definieren Sie eine Richtlinienregel, die basierend auf einem Teilnehmerparameter wie dem Typ der Funkzugriffstechnologie (RAT-Typ) ausgewählt wird. Wenn in den folgenden Beispielen der RAT-Typ EUTRAN ist, wird ein TCP-Profil ausgewählt, das eine schnellere Verbindung unterstützt (Beispiel 1). Für alle anderen Werte vom Typ RAT wird ein anderes TCP-Profil ausgewählt (Beispiel 2).

Weitere Informationen zur Funkzugriffstechnologie und ihrer Richtlinienkonfiguration finden Sie in RFC 29.212.

> **Hinweis**
>
> Der AVP vom Typ RAT (AVP-Code 1032) ist vom Typ "Enumerated" und dient zur Identifizierung der Funkzugangstechnologie, die das UE bedient.
>
> Der Wert "1004" zeigt an, dass RAT EUTRAN ist.

Beispiel 1:

```
add ns tcpProfile tcp2 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 1000000 -flavor BIC
     - dynamicReceiveBuffering DISABLED -sendBuffsize 1000000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 500 -maxburst 15

add appqoe action appact2 -priority HIGH -tcpprofile tcp2

add appqoe policy apppol2 -rule "SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).EQ(1004)" -action appact2

bind cs vserver <name>  -policyname apppol2 -priority 20 -type request
<!--NeedCopy-->
```


Beispiel 2:

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 150000 -flavor BIC
    - dynamicReceiveBuffering DISABLED -sendBuffsize 150000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 200 -maxburst 15

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).NE(1004)" -action appact1

bind cs vserver <name>  -policyname apppol1 -priority 10 -type request
<!--NeedCopy-->
```

Lastausgleichs-Datenverkehr für Steuerungsebene, der auf Diameter-, SIP- und SMPP-Protokollen basiert

May 11, 2023

Mit der Zunahme des Datenverkehrs auf der Steuerungsebene können die Server zu einem Engpass werden, da der Datenverkehr nicht optimal auf die Server verteilt wird. Daher müssen Nachrichten über einen Lastenausgleich verfügen. Die NetScaler-Appliance unterstützt Diameter-, SIP- und SMPP-Lastenausgleich.

SIP

NetScaler ermöglicht Ihnen den Lastenausgleich von SIP-Nachrichten über UDP oder über TCP (einschließlich TLS) an eine Gruppe von Proxyservern. NetScaler bietet auch eine auf Call-ID basierende Persistenz- und Call-ID-Hash-Load-Balancing-Methode, mit der Sie Pakete für eine bestimmte SIP-Sitzung an denselben SIP-Server mit Lastausgleich weiterleiten.
Die NetScaler-Standardausdruckssprache enthält eine Reihe von Ausdrücken, die für SIP-Verbindungen (Session Initiation Protocol) verwendet werden. Diese Ausdrücke sind für die Verwendung in Richtlinien für das SIP-Protokoll vorgesehen, das auf Anforderungs-/Antwortbasis arbeitet. Diese Ausdrücke können für Content Switching, Ratenbegrenzung, Responder und Umschreibrichtlinien verwendet werden.

Weitere Informationen finden Sie unter Load Balancing einer Gruppe von SIP-Servern.

SMPP

Millionen von Kurznachrichten werden täglich zwischen Einzelpersonen und Mehrwertdienstanbietern wie Banken, Werbetreibenden und Verzeichnisdiensten ausgetauscht, indem das Short Message Peer-to-Peer (SMPP) -Protokoll verwendet wird. Oft verzögert sich die Nachrichtenzustellung, weil die Server überlastet sind und der Datenverkehr nicht optimal auf die Server verteilt wird. Die NetScaler Appliance sorgt für eine optimale Verteilung von Nachrichten auf Ihren Servern und verhindert so Leistungseinbußen und Ausfälle. Die NetScaler-Appliance:

- Load gleicht Nachrichten aus, die vom Server und vom Client stammen
- Überwacht den Zustand der Nachrichtenzentren
- Bietet Unterstützung für das Content Switching für die Nachrichtenzentren
- Behandelt verkettete Nachrichten

Einschränkung: Nachrichten-IDs aus dem Message Center, die länger als 59 Byte sind, werden nicht unterstützt. Wenn die vom Nachrichtencenter zurückgegebene Nachrichtenkennungslänge mehr als 59 Byte beträgt, schlagen Nebenvorgänge fehl, und die NetScaler Appliance antwortet mit einer Fehlermeldung.

Weitere Informationen finden Sie unter SMPP Load Balancing

Diameter

Diameter ist ein Basisprotokoll, auf dem mehr als 50 Protokolle (auch Anwendungen genannt) basieren. Daher ist der in einem Telekommunikationsnetz generierte Datendurchmesserverkehr hoch. Um diesen Datenverkehr optimal aufrechtzuerhalten, führt die NetScaler-Appliance Load Balancing und Content Switching durch und fungiert als Relay-Agent. Darüber hinaus bietet die Appliance Rewrite- und Responder-Funktionen. Die Appliance unterstützt die Begrenzung der Durchmessermeldungen.

Weitere Informationen finden Sie unter Konfigurieren des Durchmesser-Lastenausgleichs.

Bereitstellung von DNS-Infrastruktur-/Verkehrsdiensten wie Load Balancing, Caching und Protokollierung für Telekommunikationsdienstanbieter

May 11, 2023

Telekommunikationsdienstanbieter können die NetScaler-Appliance so konfigurieren, dass sie als DNS-Proxy fungiert. Das Zwischenspeichern von DNS-Datensätzen, was eine wichtige Funktion eines DNS-Proxys ist, ist standardmäßig auf der NetScaler-Appliance aktiviert. Dadurch kann die

NetScaler-Appliance bei wiederholten Übersetzungen schnell reagieren, was das Kundenerlebnis verbessert und außerdem Bandbreite spart. Der speichert Antworten von DNS-Nameservern im Cache. Wenn die Appliance eine DNS-Anfrage empfängt, sucht sie in ihrem Cache nach der abgefragten Domain. Wenn die Adresse der abgefragten Domäne in ihrem Cache vorhanden ist, gibt die NetScaler-Appliance die entsprechende Adresse an den Client zurück. Andernfalls leitet es die Anfrage an einen DNS-Nameserver weiter, der die Verfügbarkeit der Adresse überprüft und sie an die NetScaler-Appliance zurückgibt. Die NetScaler-Appliance gibt dann die Adresse an den Client zurück.

Bei Anfragen für eine Domain, die zuvor zwischengespeichert wurde, stellt die NetScaler-Appliance den Adressdatensatz der Domäne aus dem Cache bereit, ohne den konfigurierten DNS-Server abzufragen, und spart somit die Bandbreite.

Ab Version 11.0 protokolliert NetScaler auch die DNS-Anfragen, die es empfängt, sowie die Antworten, die es an den Client sendet. Telekommunikationsdienstleister können dieses Protokoll verwenden, um:

- Prüfen Sie die DNS-Antworten an den Kunden
- Prüfung von DNS-Clients
- Erkennen und verhindern Sie DNS-Angriffe
- Problembehandlung

Weitere Informationen finden Sie unter Domänennamensystem.

Bereitstellung der Lastverteilung von Abonnenten mit GSLB über Kernnetze eines Telekommunikationsdienstanbieters

May 11, 2023

Skalierbarkeit, Hochverfügbarkeit und Leistung sind für den Einsatz von Service Providern von entscheidender Bedeutung. Obwohl viele Dienstanbieter ihre Infrastruktur an einem einzelnen Standort oder an mehreren Standorten bereitstellen, unterliegen diese Bereitstellungen einer Reihe inhärenter Einschränkungen, wie z. B.:

- Wenn die Website die Verbindung zum gesamten oder einem Teil des öffentlichen Internets verliert, ist sie für Benutzer und Kunden nicht zugänglich, was erhebliche Auswirkungen auf das Geschäft haben kann.
- Bei Benutzern, die von geografisch entfernten Standorten aus auf die Website zugreifen, kann es zu großen und sehr variablen Verzögerungen kommen, die durch die große Anzahl von Roundtrips, die HTTP für die Übertragung von Inhalten benötigt, noch verstärkt werden.

Das Global Server Load Balancing (GSLB) der NetScaler Appliance überwindet diese Probleme, indem es den Datenverkehr auf Standorte verteilt, die an mehreren geografischen Standorten bere-

itgestellt werden. Durch die Bereitstellung von Inhalten von vielen verschiedenen Punkten im Internet mildert GSLB die Auswirkungen von Netzwerkbandbreitenengpässen und bietet Robustheit bei Netzwerkausfällen an einem bestimmten Standort. Benutzer können automatisch zur nächstgelegenen oder zum Zeitpunkt der Anfrage am wenigsten geladenen Website weitergeleitet werden, wodurch die Wahrscheinlichkeit langer Download-Verzögerungen und/oder Serviceunterbrechungen minimiert wird.

Sie können den globalen Serverlastenausgleich der NetScaler Appliance für folgende Zwecke verwenden:

- Notfallwiederherstellung oder Hochverfügbarkeit durch Konfiguration eines Active-Standby-Rechenzentrums-Setups, das aus einem aktiven und einem Standby-Rechenzentrum besteht. Tritt aufgrund eines Katastrophenereignisses ein Failover auf, wird das Standby-Rechenzentrum betriebsbereit.
- Hohe Verfügbarkeit und Geschwindigkeit durch Konfiguration eines aktiv-aktiven Rechenzentrums-Setups, das aus mehreren aktiven Rechenzentren besteht. Die Client-Anforderungen werden auf die aktiven Rechenzentren verteilt.
- Weiterleitung von Kundenanfragen an das Rechenzentrum, das in geografischer Entfernung oder Netzwerkentfernung am nächsten liegt, indem ein Proximity-Setup konfiguriert wird.
- Bei voller DNS-Auflösung verarbeitet GSLB DNS-Abfragen der Typen A, AAAA und CNAME, und die DNS-Funktionsoption kann DNS-Abfragen aller anderen Typen wie MX und PTR verarbeiten. Wenn die rekursive Auflösung aktiviert ist, leitet die Appliance DNS-Abfragen für Domänennamen weiter, die nicht auf der NetScaler Appliance konfiguriert sind.

Weitere Informationen finden Sie unter Globaler Server-Lastenausgleich.

Bandbreitenauslastung mit Cache-Umleitungsfunktion

May 11, 2023

Das Volumen des Web-Traffics im Internet ist enorm und ein großer Prozentsatz dieses Datenverkehrs ist überflüssig. Mehrere Clients fragen Webserver wiederholt nach denselben Inhalten, was zu einer ineffizienten Bandbreitennutzung führt. Um den ursprünglichen Webserver bei der Verarbeitung jeder Anfrage zu entlasten, können Internetdienstanbieter (ISPs) die Cache-Umleitungsfunktion der NetScaler-Appliance verwenden und den Inhalt von einem Cache-Server statt vom Originalserver bereitstellen. Die NetScaler-Appliance analysiert eingehende Anfragen, sendet Anfragen für zwischenspeicherbare Daten an Cache-Server und sendet nicht zwischenspeicherbare Anfragen und dynamische HTTP-Anfragen an Originalserver. Die Cache-Umleitungsfunktion von NetScaler basiert auf Richtlinien. Standardmäßig werden Anfragen, die einer Richtlinie entsprechen, an den Ursprungsserver gesendet, und alle anderen Anfragen werden an einen Cache-Server gesendet. Sie

können Content Switching mit Cache-Umleitung kombinieren, um selektive Inhalte zwischenzuspeichern und Inhalte von bestimmten Cacheservern für bestimmte Arten von angeforderten Inhalten bereitzustellen.

Weitere Informationen finden Sie unter Cache-Umleitung.

NetScaler TCP-Optimierung

May 11, 2023

Die NetScaler-Appliance bietet fortschrittliche TCP-Tuning- und Optimierungstechniken und -funktionen, die sich gut für moderne 3,5- und 4G-Netzwerke eignen und die Benutzererfahrung sowie die wahrgenommenen Download-Geschwindigkeiten erheblich verbessern.

Dieser Abschnitt konzentriert sich auf detaillierte Anweisungen, die relevant sind für:

- Auswahl und Einfügen eines geeigneten Modells der NetScaler T1000-Serie in ein Mobilfunknetz zur TCP-Optimierung
- Vollständige Konfigurationsanweisungen beziehen sich nicht nur auf die TCP-Optimierung, sondern auch auf die entsprechende Layer-2- und Layer-3-Konfiguration des T1-Geräts

Der Abschnitt umfasst die folgenden Themen:

- Erste Schritte
- Management-Netzwerk
- Lizenzierung
- Hohe Verfügbarkeit
- Gi-LAN-Integration
- Konfigurieren der TCP-Optimierung
- Optimierung der TCP-Leistung mithilfe von TCP NILE
- Analytics und Reporting
- Echtzeitstatistiken
- SNMP
- Technische Rezepte
- Leitfaden zur Fehlerbehebung
- Häufig gestellte Fragen

Erste Schritte

May 11, 2023

Hardware

NetScaler bietet eine Vielzahl von NetScaler-Modellen, die möglicherweise lose auf zwei Faktoren basieren:

- Die Kapazität reicht derzeit von Hunderten von Mbit/s für die Low-End-VPX-Appliance bis zu 160 Gbit/s für die High-End-Appliance der 25000 MPX-Serie
- Telco-tauglich, mit der Verfügbarkeit der T1000-Serie für Telco-Rechenzentren.

Ihr NetScaler-Vertriebs- oder Supportmitarbeiter kann Ihnen bei der Auswahl der geeigneten Hardware für Ihre Demo-, Test- oder Produktionsanforderungen behilflich sein.

Im Rest dieses Abschnitts wird ein NetScaler T1200 als Referenzhardware verwendet. Beachten Sie, dass abgesehen von oberflächlichen Unterschieden * in Bezug auf Anzahl und Notation der verfügbaren Schnittstellen (siehe Anmerkung) oder gut dokumentierten Einschränkungen von NetScaler VPX (siehe * Hinweis) die Anweisungen unabhängig vom ausgewählten NetScaler-Modell größtenteils wörtlich gelten sollten.

> **Hinweis**
>
> * Beispielsweise verfügt das T1010-Modell nur über 12x1GbE, das normalerweise als 1/1-1/12 gekennzeichnet ist, und nicht über die in diesem Dokument verwendete 10/x-Notation.
>
> ** Eine NetScaler VPX-Instanz unterstützt normalerweise keine LACP-Aggregation. Möglicherweise unterstützt sie auch kein VLAN-Tagging.

Ersteinrichtung

Über die serielle Konsole

Nachdem ein serielles Kabel angeschlossen wurde, können Sie sich mit den folgenden Anmeldeinformationen an der NetScaler-Appliance anmelden:

- Benutzername:nsroot
- Passwort: nsroot

Sobald Sie angemeldet sind, konfigurieren Sie die grundlegenden Details der NetScaler-Appliance, wie in der Abbildung unten gezeigt.

Beispiel:

```
set ns config  - IPAddress <ip_addr> -netmask <netmask>

saveconfig

reboot -warm
<!--NeedCopy-->
```

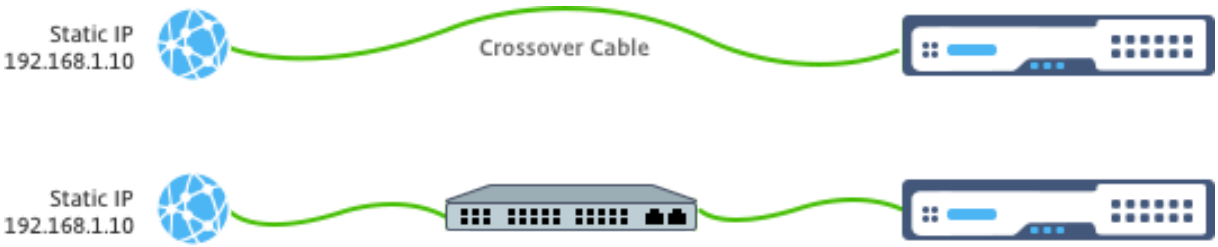

Nach dem Neustart der Appliance können Sie SSH für die weitere Konfiguration der T1100-Knoten verwenden.

Durch LOM

Über den Lights Out Management (LOM) Port an der Vorderseite der NetScaler-Appliance kann der Bediener die Appliance unabhängig vom Betriebssystem fernüberwachen und verwalten. Der Bediener kann die IP-Adresse ändern, aus- und wieder einschalten und einen Code-Dump durchführen, indem er über den LOM-Port eine Verbindung zur NetScaler-Appliance herstellt.

Die Standard-IP-Adresse des LOM-Ports ist 192.168.1.3

Abbildung. Erstkonfiguration des LOM-Moduls



Stellen Sie eine statische IP auf Ihrem Laptop ein und schließen Sie sie mit einem Crossover-Kabel direkt an die LOM-Schnittstelle oder an einen Switch in derselben Broadcast-Domäne wie die LOM-Schnittstelle an.

Geben Sie für die Erstkonfiguration die Standardadresse des Ports http://192.168.1.3 in einem Webbrowser ein und ändern Sie die Standard-IP-Adresse des LOM-Ports.

Weitere Informationen finden Sie in den Konfigurationshandbüchern.

Software

Die NetScaler TCP-Optimierung für Mobilfunknetze wird ständig weiterentwickelt. Die in diesem Dokument beschriebenen Funktionen und Optimierungen erfordern einen NetScaler Telco-Build. Hier ist ein Beispiel, das den NetScaler Telco-Build zeigt.

Beispiel:

```
1 show ver
2
3 NetScaler NS11.0: Build 64.957.nc, Date: Aug 26 2016, 02:00:23
4 <!--NeedCopy-->
```

Wenn der T1000 nicht mit der entsprechenden Build-Version ausgeliefert wurde, wenden Sie sich an den NetScaler-Kundensupport.

> **Wichtig**
>
> Beide Appliances sollten dasselbe Software-Image haben.

SSH-Client

Eine NetScaler-Appliance kann entweder mithilfe der CLI oder der HTML5-GUI konfiguriert werden. Dieser Abschnitt enthält jedoch nur CLI-basierte Anweisungen.

Während auf die CLI über die serielle NetScaler Konsole zugegriffen wird, wird normalerweise ein SSH-Client empfohlen, um die NetScaler-Remotekonfiguration zu ermöglichen.

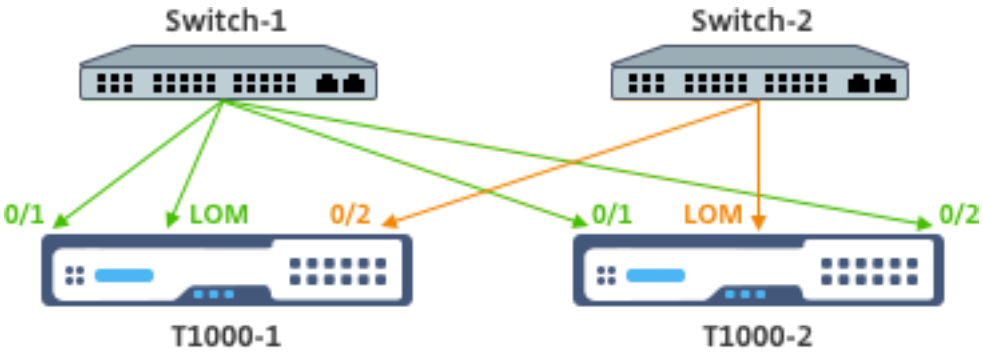
Management-Netzwerk

May 11, 2023

Verbindungen

Die meisten NetScaler-Geräte bieten redundante 1-GbE-OAM-Ports, die als 0/1 und 0/2 bezeichnet werden. Um Redundanz bei einem Switch-Ausfall zu gewährleisten, sollten Sie die entsprechenden Ports mit verschiedenen Upstream-Switches verbinden.

Eine allgemeine Übersicht über die empfohlene Konnektivität ist in der folgenden Abbildung dargestellt:



Nachdem die NetScaler-Appliance mit dem Verwaltungsnetzwerk verbunden ist, können nachfolgende Konfigurationsschritte remote über SSH oder Webkonnektivität zur CLI bzw. GUI ausgeführt werden.

Routing

Der Befehl add route kann verwendet werden, um alle für das Verwaltungsnetzwerk geeigneten Routen zu konfigurieren. Das entsprechende Gateway sollte im NSIP-Subnetz erreichbar sein, wie unten gezeigt.

Beispiel:

```
add route <network>  <netmask>  <gateway>
<!--NeedCopy-->
```

Lizenzierung

May 11, 2023

Eine gültige Lizenzdatei sollte auf der NetScaler Appliance installiert werden. Die Lizenz sollte mindestens so viele Gbit/s unterstützen wie der erwartete maximale Gi-LAN-Durchsatz.

Lizenzdateien sollten über einen SCP-Client in die /nsconfig/license der Appliance kopiert werden, wie in der Abbildung unten gezeigt.

Beispiel:

```
shell ls /nsconfig/license/

CNS_V3000_SERVER_PLT_Retail.lic ssl
<!--NeedCopy-->
```

Führen Sie einen Warmstart durch, um die neue Lizenz anzuwenden, wie in der Abbildung unten gezeigt.

Beispiel:

```
reboot -warm

Are you sure you want to restart NetScaler (Y/N)? [N]:y

Done
<!--NeedCopy-->
```

Nachdem der Neustart abgeschlossen ist, stellen Sie sicher, dass die Lizenz ordnungsgemäß angewendet wurde, indem Sie die Show License CLI verwenden.

Im folgenden Beispiel wurde eine 3-Gbit/s-Premium-Lizenz erfolgreich installiert.

Beispiel:


```
> show license

            License status:

                                    Web Logging: YES

                                            ...

                                Model Number ID: 3000

                                   License Type: Premium License

Done

<!--NeedCopy-->
```

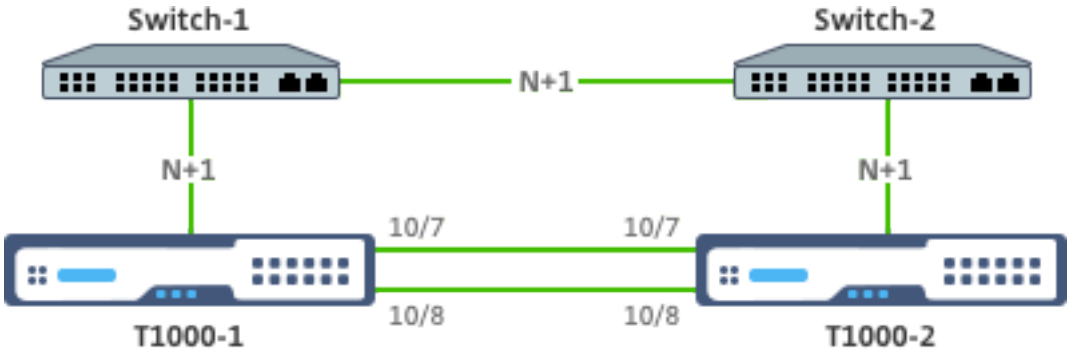
Hohe Verfügbarkeit

May 11, 2023

Hochverfügbarkeit (HA) bezieht sich auf einen aktiven Standby-Betriebsmodus eines NetScaler-Gerätepaars. Jedes Gerät hat seine eigene dedizierte Management-IP-Adresse. Alle anderen IP-Adressen gehören dem aktiven Gerät im Paar.

Verbindungen

Es gibt zwar mehrere Verbindungsoptionen für ein NetScaler HA-Paar, die am meisten empfohlene ist jedoch in der folgenden Abbildung dargestellt:



Im obigen Diagramm implizieren die roten N+1-Verbindungen zwischen jedem T1000 und dem jeweiligen Switch N+1-Redundanz - wie in Konnektivitäterläutert. Zum Beispiel ist ein 45 Gbps Gi-LAN N=5

ein geeigneter Wert, mit 6x10GbE LACP-Kanälen zwischen jedem Switch und dem entsprechenden T1000 sowie zwischen den beiden Switches.

Es wird ein zusätzliches Verknüpfungspaar zwischen dem NetScaler Paar empfohlen, um die HA-Kommunikation vom OAM-Netzwerk zu isolieren.

Gi-LAN-Integration

May 11, 2023

In der Regel wird eine NetScaler Appliance als separater L3-Inline-Knoten in das Gi-LAN eingefügt, ähnlich einem L3-Router.

Abbildung: Eine einfache Darstellung eines Gi-LAN

Verbindungen

Eine physische NetScaler-Konnektivität zu Upstream-Switches wird empfohlen, um eine ausreichende Redundanz zu gewährleisten. Angenommen, eine NetScaler Appliance ist in ein Gi-LAN eingefügt, das insgesamt 24 Gbit/s (Uplink+Downlink) verarbeitet, wird eine Konnektivität mit 4x10GbE oder mehr Schnittstellen empfohlen. Dies sorgt effektiv für eine N+1-Redundanz bei einem Verbindungsausfall.

Die entsprechenden Ports auf dem Upstream-Switch sollten für die LACP-Port-Aggregation konfiguriert werden. Die entsprechende Konfiguration auf NetScaler ist unten beschrieben:

Konnektivität Konfiguration:

```
set interface 10/1 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/2 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/3 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/4 -tagall ON -lacpMode ACTIVE -lacpKey 1
<!--NeedCopy-->
```


Sie können die entsprechenden Funktionen von LACP mit dem Befehl “show interface” überprüfen:

Schnittstelle zeigen:

```
sh interface LA/1

    1)      Interface LA/1 (802.3ad Link Aggregate) #39

             flags=0x4100c020 <ENABLED, UP, AGGREGATE, UP, HAMON, 802.1
                q>

             MTU=1500, native vlan=1, MAC=02:e0:ed:33:88:b0, uptime 340
                h11m56s

             Requested: media NONE, speed AUTO, duplex NONE, fctl NONE,

             throughput 0

             Actual: throughput 4000

             LLDP Mode: NONE,

             RX: Pkts(918446) Bytes(110087414) Errs(0) Drops(795989)
                Stalls(0)

             TX: Pkts(124113) Bytes(15255532) Errs(0) Drops(0) Stalls
                (0)

             NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
                Muted(0)

             Bandwidth thresholds are not set.

Disable the remaining unused interfaces and turn off the monitor.

set interface 10/5  - haMonitor OFF
<!--NeedCopy-->
```

Befehl:

```
set interface 10/24  - haMonitor OFF

disable interface 10/5

disable interface 10/24
<!--NeedCopy-->
```


Die Konfiguration physischer Schnittstellen wird nicht von den beiden NetScaler-Einheiten gemeinsam genutzt. Daher müssen die obigen Befehle im Falle einer HA-Paarbereitstellung auf beiden NetScaler-Knoten ausgeführt werden.

HA-Konfiguration

Alle anderen Konfigurationsparameter werden von den NetScaler Knoten eines HA-Paars gemeinsam genutzt. Daher sollte die HA-Synchronisierung vor der Ausführung anderer Konfigurationsbefehle aktiviert werden. Die grundlegende HA-Konfiguration umfasst die folgenden Schritte:

1. Verwendung der exakt gleichen NetScaler Hardware, Software und Lizenz: HA-Paare werden nicht zwischen verschiedenen Modellen (z. B. einem T1100 und einem MPX21550) oder denselben Modellen mit unterschiedlichen Firmware-Levels unterstützt. Lesen Sie die entsprechenden Anweisungen zum Upgrade eines vorhandenen HA-Paares - Upgrade auf Release 11.1.

2. Gründung des HA-Paars.

Beispiel:

```
netscaler-1> add HA node 1 <netscaler-2-NSIP>

netscaler-2> add HA node 1 <netscaler-1-NSIP>
<!--NeedCopy-->
```

3. Überprüfen Sie, ob die HA-Paar-Einrichtung den folgenden Befehl in beiden Knoten ausführt. Beide Knoten sollten sichtbar sein, einer von ihnen als Primär (aktiv), der andere als sekundärer (Standby).

Beispiel:

```
show HA node
<!--NeedCopy-->
```

4. Aktivieren Sie den ausfallsicheren Modus und MaxFlips. Dadurch wird sichergestellt, dass bei einem Ausfall des Routenmonitors auf beiden Knoten mindestens ein Knoten aktiv bleibt, ohne dass der Aktiv-/Standby-Status ständig wechselt.

Beispiel:

```
set HA node  -failsafe ON

set HA node -maxFlips 3 -maxFlipTime 1200
<!--NeedCopy-->
```


5. Aktivieren Sie abschließend die HA-Synchronisierung über die dedizierten Intra-NetScaler-Ports und nicht über das OAM-Netzwerk.

Beispiel:

```
add vlan 4080 -aliasName syncVlan

set HA node -syncvlan 4080
<!--NeedCopy-->
```

> **Hinweis**
>
> Das VLAN 4080 in den Befehlen im obigen Beispiel sollte nicht wörtlich genommen werden. Jede nicht verwendete VLAN-ID kann reserviert sein.

VLAN-Konfiguration

Nachdem die physikalischen Schnittstellen entsprechend konfiguriert wurden, können Sie die entsprechenden Gi-LAN-VLANs konfigurieren. Stellen Sie sich zum Beispiel eine ziemlich einfache Gi-LAN-Umgebung mit einem Ingress/Egress-VLAN-Paar mit 100/101-VLAN-Kennung vor.

Mit den folgenden Befehlen werden die entsprechenden VLANs über dem im vorherigen Schritt erstellten LACP-Kanal konfiguriert.

```
add vlan 100
add vlan 101
bind vlan 100 -ifnum LA/1 -tagged
bind vlan 101 -ifnum LA/1 -tagged
<!--NeedCopy-->
```

IPv4-Konfiguration

In der Regel benötigt eine NetScaler Appliance ein SNIP pro VLAN. Im folgenden Beispiel wird davon ausgegangen, dass die Netzwerke, die im Gi-LAN-Integrationsdiagramm am Anfang dieser Seite beschrieben sind, eine /24-Subnetzmaske haben:

```
add ns ip 192.168.1.254 255.255.255.0 -vserver DISABLED -mgmtAccess
    DISABLED
add ns ip 192.168.2.254 255.255.255.0 -vserver DISABLED -mgmtAccess
    DISABLED
<!--NeedCopy-->
```

Nachdem die SNIPs konfiguriert wurden, sollten sie mit dem entsprechenden VLAN verknüpft werden:


```
bind vlan 100  -IPAddress 192.168.1.254 255.255.255.0
bind vlan 101  -IPAddress 192.168.2.254 255.255.255.0
<!--NeedCopy-->
```

Statisches IPv4-Routing

Das im Abschnitt Management Network beschriebene Beispiel erfordert nur ein paar statische Routing-Regeln:

- Eine statische Route 10.0.0.0/8 zu den Clients über den Eingangs-Router
- Eine Standardroute zum Internet über den Egress-Router

Beispiel:

```
add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1
<!--NeedCopy-->
```

IPv4-richtlinienbasiertes (VLAN - VLAN) -Routing

Eine NetScaler Appliance ermöglicht richtlinienbasiertes Routing anstelle von statischem Routing, wobei Routing-Entscheidungen normalerweise eher mit der eingehenden Schnittstelle und/oder dem VLAN als mit der Ziel-IP vergeben werden. Richtlinienbasiertes Routing ist entweder eine bequeme Alternative, falls der IP-Adressbereich der Clientquelle regelmäßigen Änderungen unterliegt, oder eine zwingende Überlegung, falls die Ziel-IP-Adresse eines Pakets allein nicht ausreicht, um eine Routingentscheidung zu treffen (d. h. bei sich überlappenden Client-IP-Adressen über mehrere VLANs hinweg).

Beispiel:

```
add ns pbr fromWirelessToInternet ALLOW  -nextHop 192.168.2.1  -vlan
    100  -priority 10

Done

 add ns pbr fromInternetToWireless ALLOW  -nextHop 192.168.1.1  -vlan
     200  -priority 20

Done

apply ns pbrs
<!--NeedCopy-->
```


IPv6-Konfiguration

Die folgenden Befehle weisen IPv6 SNIP pro VLAN zu. Im folgenden Beispiel wird davon ausgegangen, dass die in der Abbildung skizzierten Netzwerke: Eine einfache Darstellung eines Gi-LAN auf dieser Seite eine /64-Subnetzmaske haben:

Befehl:

```
add ns ip6 fd00:192:168:1::254/64 -vServer DISABLED  - mgmtAccess
    DISABLED
add ns ip6 fd00:192:168:2::254/64 -vServer DISABLED  - mgmtAccess
    DISABLED
bind vlan 100 -IPAddress fd00:192:168:1::254/64
bind vlan 200 -IPAddress fd00:192:168:2::254/64
<!--NeedCopy-->
```

IPv6-Routing

Nachdem die IPv6-Adressierung abgeschlossen ist, kann das statische IPv6-Routing konfiguriert werden:

- Eine fd 00:10: :/64 statische Route zu den Clients über den Ingress-Router
- Eine Standardroute zum Internet über den Egress-Router

Beispiel:

```
add route6 fd00:10::/64 fd00:192:168:1::1
add route6 ::/0 fd00:192:168:2::1
<!--NeedCopy-->
```

Oder mit richtlinienbasiertem Routing:

Beispiel:

```
add ns pbr6 fromWirelessToInternetv6 ALLOW -vlan 100 -priority 10 -
    nextHop fd00:192:168:2::1

add ns pbr6 fromInternetToWirelessv6 ALLOW -vlan 200 -priority 20 -
    nextHop fd00:192:168:1::1

apply ns pbr6
<!--NeedCopy-->
```


LACP-Redundanz und Failover

Im Falle einer HA-Konfiguration wird empfohlen, die Durchsatzoption zu nutzen, um einen niedrigen Schwellenwert für den LACP-Kanal zu konfigurieren. Stellen Sie sich beispielsweise ein 25-Gbit/s-Gi-LAN und einen 4x10GbE-Kanal zwischen jeder NetScaler Appliance im HA-Paar und dem Upstream-Switch vor, um eine N+1-Link-Redundanz bereitzustellen:

Beispiel:

```
set interface LA/1 -haMonitor ON -throughput 29000
<!--NeedCopy-->
```

Im Falle eines Double-Link-Ausfalls zwischen dem primären Gerät und dem Upstream-Switch würde der maximal unterstützte Gi-LAN-Durchsatz auf 20 Gbit/s sinken. Ein niedriger Schwellenwert von 29 Gbit/s gemäß dem obigen Beispiel würde zu einem Redundanz-Switchover-Ereignis zum sekundären Gerät führen (das keine ähnlichen Verbindungsausfälle erlitten hat), sodass der Gi-LAN-Verkehr nicht beeinträchtigt wird.

Routen-Monitore

Zusätzlich zur LACP-Redundanz können Routenüberwachungsprüfungen konfiguriert und mit der HA-Paar-Konfiguration verknüpft werden. Routenüberwachungsprüfungen können nützlich sein, um Fehler zwischen der NetScaler Appliance und den Next-Hop-Routern zu erkennen, insbesondere wenn diese Router nicht direkt, sondern über einen Upstream-Switch verbunden sind.

Eine typische Konfiguration des HA-Routenmonitors gemäß dem Beispiel Gi-LAN in Abschnitt 2.5.1 ist nachstehend beschrieben:

```
add route 192.168.1.0 255.255.255.0 192.168.1.1 -msr ENABLED -monitor
    arp
add route 192.168.2.0 255.255.255.0 192.168.2.1 -msr ENABLED -monitor
    arp
bind HA node -routeMonitor 192.168.1.0 255.255.255.0
bind HA node -routeMonitor 192.168.2.0 255.255.255.0
<!--NeedCopy-->
```

TCP-Optimierungskonfiguration

May 11, 2023

Bevor Sie die TCP-Optimierung konfigurieren, wenden Sie die folgenden grundlegenden Konfigurationseinstellungen auf der NetScaler Appliance an:

Erstkonfiguration:

```
enable ns feature LB IPv6PT
enable ns mode FR L3 USIP MBF Edge USNIP PMTUD
disable ns feature SP
disable ns mode TCPB
set lb parameter -preferDirectRoute NO
set lb parameter -vServerSpecificMac ENABLED
set l4param -l2ConnMethod Vlan
set rsskeytype -rsstype SYMMETRIC
set ns param -useproxyport DISABLED
<!--NeedCopy-->
```

> **Hinweis**
>
> Starten Sie die NetScaler Appliance neu, wenn Sie den Systemparameter rsskeytype ändern.

TCP-Terminierung

Damit NetScaler T1 die TCP-Optimierung anwenden kann, muss zuerst der eingehende TCP-Verkehr beendet werden. Zu diesem Zweck sollte ein TCP-vserver mit Platzhaltern erstellt und konfiguriert werden, um eingehenden Datenverkehr abzufangen und ihn dann an den Internet-Router weiterzuleiten.

Statische oder dynamische Routing-Umgebung

In Umgebungen mit statischem oder dynamischem Routing kann sich vserver auf Routing-Tabelleninformationen verlassen, um Pakete an den Internet-Router weiterzuleiten. Die Standardroute muss auf den Internet-Router zeigen, und auch die Routing-Einträge für Client-Subnetze zum WLAN-Router sollten vorhanden sein:

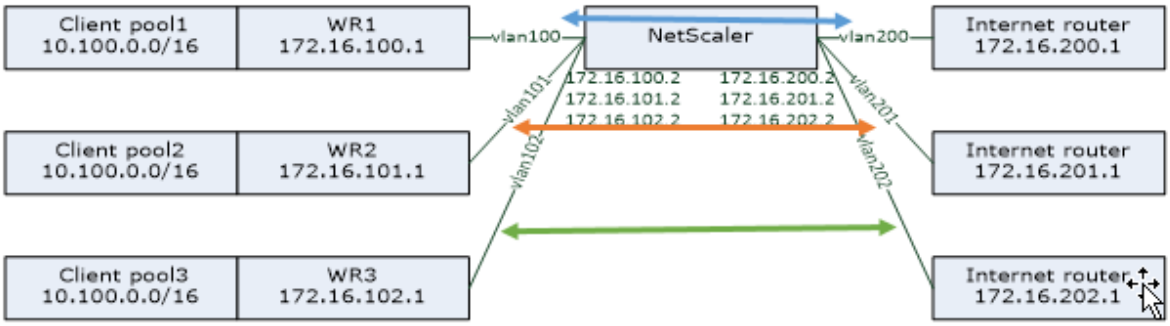
Beispiel:

```
add lb vserver vsrv-wireless TCP * * -persistenceType NONE -
    Listenpolicy "CLIENT.VLAN.ID.EQ(100) && SYS.VSERVER("vsrv-wireless")
    .STATE.EQ(UP)" -m IP -cltTimeout 9000
add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1
<!--NeedCopy-->
```

VLAN-to-VLAN (PBR) -Umgebung

Es gibt Kundenumgebungen, in denen der Abonnentenverkehr in mehrere Datenflüsse segmentiert ist und auf der Grundlage der Parameter des eingehenden Datenverkehrs an verschiedene Router weit-

ergeleitet werden muss. Policy Based Routing (PBR) kann verwendet werden, um Pakete basierend auf eingehenden Paketparametern wie VLAN, MAC-Adresse, Schnittstelle, Quell-IP, Quellport, Ziel-IP-Adresse und Zielport weiterzuleiten.



Beispiel:

```
add lb vserver vsrv-wireless TCP * * -m IP -l2Conn ON -listenpolicy "
    CLIENT.VLAN.ID.EQ(100) || CLIENT.VLAN.ID.EQ(101) || CLIENT.VLAN.ID.
    EQ(102)"

add ns pbr pbr-vlan100-to-vlan200 ALLOW -vlan 100 -nexthop 172.16.200.1

add ns pbr pbr-vlan101-to-vlan201 ALLOW -vlan 101 -nexthop 172.16.201.1

add ns pbr pbr-vlan102-to-vlan202 ALLOW -vlan 102 -nexthop 172.16.202.1
<!--NeedCopy-->
```

Die Verwendung von Policy Based Routing zur Weiterleitung von TCP-optimiertem Datenverkehr ist eine neue Funktion, die in Version 11.1 50.10 hinzugefügt wurde. In früheren Versionen ist es eine alternative Lösung für Multi-VLAN-Umgebungen, mehrere vServer-Entitäten im “Modus MAC” pro VLAN zu haben. Jeder vserver hat einen gebundenen Dienst, der den Internet-Router für den jeweiligen Flow darstellt.

Beispiel:

```
add server internet_router_1 172.16.200.1

add server internet_router_2 172.16.201.1

add server internet_router_3 172.16.202.1

add service svc-internet-1 internet_router_1 TCP * -usip YES -
    useproxyport NO

```



```
add service svc-internet-2 internet_router_2 TCP * -usip YES -
    useproxyport NO

add service svc-internet-3 internet_router_3 TCP * -usip YES -
    useproxyport NO

bind service svc-internet-1 -monitorName arp

bind service svc-internet-2 -monitorName arp

bind service svc-internet-3 -monitorName arp

add lb vserver vsrv-wireless-1 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
    (100) && SYS.VSERVER("vsrv-wireless-1").STATE.EQ(UP)" -m MAC -l2Conn
     ON

add lb vserver vsrv-wireless-2 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
    (101) && SYS.VSERVER("vsrv-wireless-2").STATE.EQ(UP)" -m MAC -l2Conn
     ON

add lb vserver vsrv-wireless-3 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
    (102) && SYS.VSERVER("vsrv-wireless-3").STATE.EQ(UP)" -m MAC -l2Conn
     ON

bind lb vserver vsrv-wireless-1 svc-internet-1

bind lb vserver vsrv-wireless-2 svc-internet-2

bind lb vserver vsrv-wireless-3 svc-internet-3
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der vServer-Modus ist MAC, im Gegensatz zu früheren Beispielen, in denen es der Modus IP ist. Dies ist erforderlich, um die Ziel-IP-Informationen zu speichern, wenn wir Dienste haben, die an vServer gebunden sind. Außerdem muss die zusätzliche PBR-Konfiguration nicht optimierten Datenverkehr weiterleiten.

TCP-Optimierung

Die sofort einsatzbereite NetScaler TCP-Terminierung ist für die TCP-Passthrough-Funktionalität konfiguriert. TCP-Passthrough bedeutet im Wesentlichen, dass NetScaler T1 einen Client-Server-TCP-Stream transparent abfangen kann, jedoch keine separaten Client/Server-Puffer beibehält oder auf andere Weise Optimierungstechniken anwendet.

Um die TCP-Optimierung zu aktivieren, wird ein TCP-Profil mit dem Namen nstcpprofile verwendet, um TCP-Konfigurationen anzugeben. Dieses wird verwendet, wenn auf Dienst- oder virtueller Serverebene keine TCP-Konfigurationen bereitgestellt werden und es wie folgt geändert werden sollte:

Befehl:

```
add ns tcpProfile nstcpprofile -WS ENABLED -SACK ENABLED -WSVal 8 -mss
    1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn kein Profil explizit erstellt und an vserver und service gebunden ist, ist das Profil nstcp_default_profile standardmäßig gebunden.
>
> Falls mehrere TCP-Profile erforderlich sind, können zusätzliche TCP-Profile erstellt und dem entsprechenden virtuellen Server zugeordnet werden

Befehl:

```
add ns tcpProfile custom_profile -WS ENABLED -SACK ENABLED -WSVal 8 -
    mss 1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
    ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
    spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
    fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT

set lb vserver vsrv-wireless -tcpProfileName custom_profile
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für Bereitstellungen mit vserver -m MAC und service sollte dasselbe Profil dem Dienst zugeordnet werden.

```
set service svc-internet -tcpProfileName custom_profile
<!--NeedCopy-->
```


TCP-Optimierungsmöglichkeiten

Die meisten relevanten TCP-Optimierungsfunktionen einer NetScaler Appliance werden über ein entsprechendes TCP-Profil verfügbar gemacht. Typische CLI-Parameter, die bei der Erstellung eines TCP-Profils berücksichtigt werden sollten, sind die folgenden:

1. **Fensterskalierung (WS)**: Die TCP-Fensterskalierung ermöglicht eine Erhöhung der Größe des TCP-Empfangsfensters auf über 65535 Byte. Es hilft, die TCP-Leistung insgesamt zu verbessern, insbesondere in Netzwerken mit hoher Bandbreite und langer Verzögerung. Es hilft bei der Reduzierung der Latenz und der Verbesserung der Reaktionszeit über TCP.
2. **Selektive Bestätigung (SACK)**: TCP SACK behebt das Problem des Verlusts mehrerer Pakete, wodurch die Gesamtdurchsatzkapazität reduziert wird. Mit einer selektiven Bestätigung kann der Empfänger den Absender über alle erfolgreich empfangenen Segmente informieren, sodass der Sender nur die Segmente erneut übertragen kann, die verloren gegangen sind. Diese Technik hilft T1, den Gesamtdurchsatz zu verbessern und die Verbindungslatenz zu reduzieren.
3. **Fensterskalierungsfaktor (WSVal)**: Faktor, der zur Berechnung der neuen Fenstergröße verwendet wird. Es muss mit einem hohen Wert konfiguriert werden, damit das von NS angekündigte Fenster mindestens der Puffergröße entspricht.
4. **Maximale Segmentgröße (MSS)**: MSS eines einzelnen TCP-Segments. Dieser Wert hängt von der MTU-Einstellung auf Zwischenroutern und Endclients ab. Ein Wert von 1460 entspricht einer MTU von 1500.
5. **maxBurst**: Maximale Anzahl von TCP-Segmenten, die in einem Burst zulässig sind.
6. **Größe des anfänglichen Überlastungsfensters (initialCwnd)**: Die Größe des anfänglichen Überlastungsfensters von TCP bestimmt die Anzahl der Byte, die zu Beginn der Transaktion noch ausstehen können. Es ermöglicht T1, diese vielen Byte zu senden, ohne sich um eine Überlastung der Leitung zu kümmern.
7. **Maximale OOO-Paketwarteschlangengröße (oooQSize)**: TCP verwaltet die Out-Of-Order-Warteschlange, um die OOO-Pakete in der TCP-Kommunikation zu halten. Diese Einstellung wirkt sich auf den Systemspeicher aus, wenn die Warteschlangengröße so lang ist, dass die Pakete im Laufzeitspeicher aufbewahrt werden müssen. Daher muss dies auf der Grundlage der Netzwerk- und Anwendungsmerkmale auf einem optimierten Niveau gehalten werden.
8. **Minimum RTO(minRTO)**: Das Timeout für die TCP-erneute Übertragung wird für jedes empfangene ACK auf der Grundlage der internen Implementierungslogik berechnet. Das standardmäßige Timeout für die erneute Übertragung liegt zunächst bei 1 Sekunde und kann mit dieser Einstellung angepasst werden. Für die zweite erneute Übertragung dieser Pakete wird RTO mit N*2 berechnet und dann wird N*4… N*8… bis zum letzten erneuten Übertragungsversuch fortgesetzt.
9. **bufferSize/sendBuffSize**: Diese beziehen sich auf die maximale Datenmenge, die der T1 vom Server empfangen und intern zwischenspeichern kann, ohne sie an den Client zu senden. Sie sollten auf einen Wert gesetzt werden, der größer (mindestens das Doppelte) als das Bandbreitenverzögerungsprodukt des zugrunde liegenden Übertragungskanals ist.

10. **Flavor**: Dies bezieht sich auf den Algorithmus zur Kontrolle der TCP-Überlastung. Gültige Werte sind Default, BIC, CUBIC, Westwood und Nile.
11. **Dynamische Empfangspufferung**: Ermöglicht die dynamische Anpassung des Empfangspuffers an die Speicher- und Netzwerkbedingungen. Es füllt den Puffer so weit auf, wie es erforderlich ist, um die Download-Pipe des Clients voll zu halten, anstatt einen Puffer mit fester Größe vom Server vorzulesen, da letzterer im TCP-Profil angegeben ist und normalerweise auf Kriterien wie 2*BDP für eine Verbindung basiert. NetScaler T1 überwacht die Netzwerkbedingungen für den Client und schätzt, wie viel er vom Server vorlesen sollte.
12. **Keep-Alive (KA)**: Senden Sie regelmäßige TCP-Keep-Alive-Tests (KA), um zu überprüfen, ob der Peer noch aktiv ist.
13. rstWindowAttenuate: Verteidigung von TCP vor Spoofing-Angriffen. Es wird mit einem korrigierenden ACK antworten, wenn eine Sequenznummer ungültig ist.
14. **rstmaxACK**: Aktiviert oder deaktiviert die Annahme von RST, das sich außerhalb des Fensters befindet, aber die höchste ACK-Sequenznummer wiedergibt.
15. **SpoofSynDrop**: Löschen ungültiger SYN-Pakete zum Schutz vor Spoofing.
16. **Explizite Überlastungsbenachrichtigung (ecn)**: Sie sendet eine Benachrichtigung über den Status der Netzwerküberlastung an den Absender der Daten und ergreift Korrekturmaßnahmen bei Datenüberlastung oder Datenbeschädigung.
17. **Forward RTO-Recovery**: Bei falschen erneuten Übertragungen werden die Congestion Control-Konfigurationen in ihren ursprünglichen Zustand zurückversetzt.
18. **Maximales TCP-Überlastungsfenster (maxcwnd)**: Die maximale TCP-Überlastungsfenstergröße ist vom Benutzer konfigurierbar.
19. **Forward Acknowledgment (FACK)**: Um TCP-Überlastung zu vermeiden, wird explizit die Gesamtzahl der im Netzwerk ausstehenden Datenbytes gemessen und dem Sender (entweder T1 oder ein Client) dabei geholfen, die Menge der in das Netzwerk injizierten Daten bei Timeouts für die erneute Übertragung zu kontrollieren.
20. **tcpmode**: TCP-Optimierungsmodi für ein bestimmtes Profil. Es gibt zwei TCP-Optimierungsmodi: Transparent und Endpoint.

    - Endpunkt. In diesem Modus verwaltet die Appliance die Client- und Serververbindungen getrennt.
    - Durchsichtig Im transparenten Modus müssen die Clients direkt auf die Server zugreifen, ohne dass ein virtueller Server dazwischenliegt. Die Server-IP-Adressen müssen öffentlich sein, da die Clients auf sie zugreifen können müssen.

Untätiges Löschen inaktiver Verbindungen

In einem Telekommunikationsnetz werden fast 50 Prozent der TCP-Verbindungen einer NetScaler-Appliance inaktiv, und die Appliance sendet RST-Pakete, um sie zu schließen. Die über Funkkanäle gesendeten Pakete aktivieren diese Kanäle unnötig, was zu einer Flut von Nachrichten führt, die

wiederum dazu führen, dass die Appliance eine Flut von Service-Reject-Nachrichten generiert. Das Standard-TCP-Profil enthält jetzt die Parameter DropHalfClosedConnOnTimeout und DropEstConnOnTimeout, die standardmäßig deaktiviert sind. Wenn Sie beide aktivieren, führt weder eine halbgeschlossene noch eine hergestellte Verbindung dazu, dass bei einem Timeout der Verbindung ein RST-Paket an den Client gesendet wird. Die Appliance unterbricht einfach die Verbindung.

```
set ns tcpProfile nstcpprofile  -DropHalfClosedConnOnTimeout ENABLED
set ns tcpProfile nstcpprofile  -DropEstConnOnTimeout ENABLED
<!--NeedCopy-->
```

Analytics und Reporting

May 11, 2023

Das TCP Speed Reporting ist eine NetScaler-Funktion, die TCP-Verbindungsstatistiken als Maß für die TCP-Download- und Upload-Leistung extrahiert und in TCP Insight-Berichten des NetScaler Application Delivery Management (ADM) verwendet wird. Um dies zu erreichen, überwacht NetScaler jede TCP-Verbindung, sucht Paketaufbrüche im Leerlaufzeitlimit und meldet Schlüsselmetriken (z. B. Byteanzahl, Anzahl der wiederübertragenen Byte und Dauer) für die identifizierte maximale Burst. TCP-Geschwindigkeitsberichterstattungsfunktion ist standardmäßig aktiviert, unterstützt sowohl TCP- als auch HTTP-vServer und hängt von der AppFlow/ULFD-Berichtsinfrastruktur ab.

Echtzeit-Statistiken

August 19, 2021

Der Befehl stat kann verwendet werden, um zu überprüfen, ob die TCP-Optimierung ordnungsgemäß angewendet wird:

Befehl:

```
> stat lb vserver vsrv-wireless
Virtual Server Summary
                      vsvrIP  port     Protocol        State   Health
                         actSvcs
vsrv...eless              *     0          TCP           UP      100
           1

            inactSvcs
vsrv...eless       0
```



```
8  Virtual Server Statistics
9                                                Rate (/s)
                                                    Total
10 Vserver hits                                          0
       10
11 Requests                                              0
                          0
12 Responses                                             0
                          0
13 Request bytes                                         0
       1580
14 Response bytes                                        0
       532594360
15 Total Packets rcvd                                    0
       216463
16 Total Packets sent                                    0
       369898
17 Current client connections                           --
                          0
18 Current Client Est connections                       --
                          0
19 Current server connections                           --
                          0
20 Requests in surge queue                              --
                          0
21 Requests in vserver's surgeQ                         --
                          0
22 Requests in service's surgeQs                        --
                          0
23 Spill Over Threshold                                 --
                          0
24 Spill Over Hits                                      --
                          0
25 Labeled Connection                                   --
                          0
26 Push Labeled Connection                              --
                          0
27 Deferred Request                                      0
                          0
28 Invalid Request/Response                             --
                          0
29 Invalid Request/Response Dropped                     --
                          0
30 Bound Service(s) Summary
31                          IP  port         Type        State     Hits
```



```
                                    Hits/s
32 svc-internet     192.168.2.2     0          TCP           UP       10
         0/s
33
34                  Req    Req/s      Rsp    Rsp/s Throughp ClntConn
                       SurgeQ
35 svc-internet       0      0/s        0      0/s        0        0
            0
36                   SvrConn   ReuseP  MaxConn ActvTran  SvrTTFB     Load
37 svc-internet         0        0        0        0        0        0
```

Die Gesamtzähler sollten für ein operatives System ständig steigen. Darüber hinaus sollten die Kurszähler ungleich Null sein.

> **Hinweis:**
>
> Die vorhergehende Ausgabe stammt aus einem betriebsbereiten Laborsystem, das die Nullrate erklärt.

SNMP

May 11, 2023

Der SNMP-Agent kann von einem Remote-Gerät aus (SNMP Manager) nach systemspezifischen Informationen abgefragt werden. Basierend auf der Abfrage sucht der Agent in der Management Information Base (MIB) nach dem Equal Object Identifier (OID) für die angeforderten Daten und sendet die Informationen an den SNMP-Manager. Im Folgenden sind die nützlichsten SNMP-OIDs für Telco-Bereitstellungen aufgeführt:

Speicher

- **ResMem-Nutzung (1.3.6.1.4.1.5951.4.1.1.41.2)**

Prozentsatz der Speicherauslastung auf NetScaler.

Paket-Engine-CPU

- **ResCPU-Auslastung (1.3.6.1.4.1.5951.4.1.1.41.1)**

Prozentsatz der CPU-Auslastung.

- **NSC-fähig (1.3.6.1.4.1.5951.4.1.1.41.6)**

Diese Tabelle enthält Informationen zu jeder CPU in NetScaler.

Indexiert auf: NscPuName

- **NSCP-Name (1.3.6.1.4.1.5951.4.1.1.41.6.1.1)**

Der Name der CPU.

- **NSCPU-Nutzung (1.3.6.1.4.1.5951.4.1.1.41.6.1.2)**

Prozentsatz der CPU-Auslastung.

Durchsatz

- **Alle NIC bis TRX MBits (1.3.6.1.4.1.5951.4.1.1.71.1)**

Anzahl der Megabit, die von der NetScaler-Appliance empfangen wurden.

- **Alle NIC bis TTXM-Bits (1.3.6.1.4.1.5951.4.1.1.71.2)**

Anzahl der von der NetScaler-Appliance übertragenen Megabit.

- **IP zu TRX PKTS (1.3.6.1.4.1.5951.4.1.1.43.25)**

Empfangene IP-Pakete.

- **IP zu TRX Mbit/s (1.3.6.1.4.1.5951.4.1.1.43.27)**

Megabit empfangener IP-Daten.

- **IP zu TTXPKT (1.3.6.1.4.1.5951.4.1.1.43.28)**

IP-Pakete wurden übertragen.

- **IP zu TTX Mbit/s (1.3.6.1.4.1.5951.4.1.1.43.30)**

Megabit an übertragenen IP-Daten.

Verbindungen

Aktive Verbindungen:

- **TCP ActiveServerConn (1.3.6.1.4.1.5951.4.1.1.46.8)**

Verbindungen zu einem Server, der gerade auf Anfragen reagiert.

Verbindungen insgesamt:

- **TCPCurServerConn (1.3.6.1.4.1.5951.4.1.1.46.1)**

Serververbindungen, einschließlich Verbindungen im Status Wird geöffnet, hergestellt und geschlossen.

- **TCPcurClientConn (1.3.6.1.4.1.5951.4.1.1.46.2)**

Client-Verbindungen, einschließlich Verbindungen im Status „Öffnet“, „Aufgebaut“ und „Wird geschlossen“.

Hinweis: Aufgrund des SYN-Cookies gilt dies nicht für den Client im Status „Öffnen“

- **TCP zu Zombie CLTConn Flushed (1.3.6.1.4.1.5951.4.1.1.46.26)**

Client-Verbindungen, die geleert werden, weil der Client seit einiger Zeit inaktiv war.

- **TCP zu ZombieSvrConn Flushed (1.3.6.1.4.1.5951.4.1.1.46.27)**

Serververbindungen, die geleert werden, weil sich seit einiger Zeit keine Clientanfragen in der Warteschlange befinden.

Errors

- **TCperrsynGive Up (1.3.6.1.4.1.5951.4.1.1.46.37)**

Versuche, eine Verbindung auf dem NetScaler herzustellen, bei dem ein Timeout auftrat.

- **TCP-Perr-Retransmit-Aufgabe (1.3.6.1.4.1.5951.4.1.1.46.60)**

Häufigkeit, mit der NetScaler eine Verbindung beendet, nachdem das Paket sieben Mal über diese Verbindung erneut übertragen wurde. Eine erneute Übertragung erfolgt, wenn das empfangende Ende das Paket nicht bestätigt.

- **Ifind-Karten (1.3.6.1.2.1.2.2.1.13)**

Die Anzahl der eingehenden Pakete, die als verworfen wurden, obwohl keine Fehler entdeckt wurden, die verhindern könnten, dass sie an ein übergeordnetes Protokoll übermittelt werden konnten. Ein möglicher Grund für das Verwerfen eines solchen Pakets könnte darin bestehen, Pufferspeicher freizugeben.

- **IfOut verwirft (1.3.6.1.2.1.2.2.1.19)**

Die Anzahl der ausgehenden Pakete, die als verworfen wurden, obwohl keine Fehler entdeckt wurden, die ihre Übertragung verhindern könnten. Ein möglicher Grund für das Verwerfen eines solchen Pakets könnte darin bestehen, Pufferspeicher freizugeben.

- **Iferrtx-Überlauf (1.3.6.1.4.1.5951.4.1.1.54.1.36)**

Anzahl der Pakete, die während der Übertragung auf der angegebenen Schnittstelle die Überlaufwarteschlangen passiert haben, seit die NetScaler-Appliance gestartet wurde oder die Schnittstellenstatistiken gelöscht wurden. Dies wird nur an überlasteten Ports erhöht.

Optimierte/Bypass-Verbindungen

- **TCP-Optimierung aktiviert (1.3.6.1.4.1.5951.4.1.1.46.131)**

Gesamtzahl der mit TCP-Optimierung aktivierten Verbindungen.

- **TCP-Optimierung wurde umgangen (1.3.6.1.4.1.5951.4.1.1.46.132)**

Die Gesamtanzahl der Verbindungen wurde TCP-Optimierung umgangen.

Technische Rezepte

May 11, 2023

Die NetScaler T1-Modelle bieten erweiterte Funktionen und eine leistungsstarke Richtlinienkonfigurationssprache, mit der komplexe Entscheidungen während der Laufzeit bewertet werden können.

Es ist zwar nicht möglich, alle Funktionen zu bewerten, die potenziell durch den Leitfaden zur Konfiguration der T1000 Funktionen und Richtlinien freigeschaltet werden, aber in den technischen Unterlagen wird die Umsetzung verschiedener Anforderungen der Telekommunikationsbetreiber berücksichtigt. Fühlen Sie sich frei, die „Rezepte“ so wiederzuverwenden, wie sie sind, oder passen Sie sie an Ihre Umgebung an.

Verbindungslimit pro Benutzer

Das NetScaler T1-Modell kann so konfiguriert werden, dass die Anzahl der Verbindungen pro eindeutiger Abonnenten-IP begrenzt wird. Mit der folgenden Konfiguration sind N gleichzeitige TCP-Verbindungen pro IP (CLIENT.IP.SRC) zulässig. Für jeden Verbindungsversuch, der den konfigurierten Schwellenwert überschreitet, sendet T1 einen RST. Für maximal 2 gleichzeitige Verbindungen pro Benutzer:

Befehl:

```
1 add stream selector streamSel_usrlimit CLIENT.IP.SRC
2 add ns limitIdentifier limitId_usrlimit -threshold 2 -mode CONNECTION -
     selectorName streamSel_usrlimit
3 add responder policy respPol_usrlimit "SYS.CHECK_LIMIT("
     limitId_usrlimit")" RESET
4 bind lb vserver vsrv-wireless -policyName respPol_usrlimit -priority 1
     -gotoPriorityExpression END
5 <!--NeedCopy-->
```

Reibungsloses Einfügen/Löschen von Vserver

Viele Betreiber machen sich Sorgen über eine Unterbrechung der TCP-Verbindungen, wenn das NetScaler T1-Modell zur TCP-Optimierung inline aktiviert oder zu Wartungszwecken deaktiviert wird.

Um zu verhindern, dass bestehende Verbindungen unterbrochen werden, wenn vserver eingeführt wird, muss die folgende Konfiguration angewendet werden, bevor vserver für die TCP-Optimierung konfiguriert oder aktiviert wird:

Befehl:

```
add ns acl acl-ingress ALLOW -vlan 100
add forwardingSession fwd-ingress -aclname acl-ingress
apply ns acls
<!--NeedCopy-->
```

Die Weiterleitung von Sitzungen erfolgt zusätzlich zum Routing (entweder statisch oder dynamisch oder PBR) und erstellt Sitzungseinträge für den gerouteten Verkehr (L3-Modus). Jede bestehende Verbindung wird verarbeitet, indem die Sitzung aufgrund der entsprechenden Sitzungen weitergeleitet wird. Nach der Einführung von vserver werden nur neue TCP-Verbindungen erfasst.

ACLs können so konfiguriert werden, dass sie nur bestimmte Ports wie vserver erfassen, um zu vermeiden, dass Sitzungen für unnötigen Datenverkehr erstellt werden, der Speicherplatz beansprucht. Eine weitere Option besteht darin, eine bestimmte Konfiguration nach der vserver-Aktivierung zu entfernen.

Zu Wartungszwecken sollte vserver deaktiviert werden und sein Status sollte als AUSSER BETRIEB angezeigt werden. In diesem Fall beendet der vserver standardmäßig alle Verbindungen sofort. Damit vserver weiterhin die bestehenden Verbindungen bedient und keine neuen akzeptiert, sollte die folgende Konfiguration angewendet werden:

Befehl:

```
set lb vserver vsrv-wireless -downStateFlush DISABLED
<!--NeedCopy-->
```

Neue Verbindungen durchlaufen die Routingtabelle, und entsprechende Sitzungseinträge werden aufgrund der Weiterleitung von Sitzungen erstellt.

Richtlinienbasiertes TCP-Profiling

Die richtlinienbasierte TCP-Profilauswahl ermöglicht es den Betreibern, das TCP-Profil dynamisch für Clients aus verschiedenen Verkehrsdomänen (z. B. 3G oder 4G) zu konfigurieren. Einige der QoS-Metriken unterscheiden sich für diese Verkehrsdomänen. Um eine bessere Leistung zu erzielen, müssen Sie einige der TCP-Parameter dynamisch ändern. Stellen Sie sich einen Fall vor, in dem Clients, die über 3G und 4G kommen, denselben vServer aufrufen und dasselbe TCP-Profil verwenden, was sich negativ auf die Leistung einiger Clients auswirkt. Die AppQoE-Funktionalität kann diese Clients klassifizieren und das TCP-Profil auf dem vserver dynamisch ändern.

Beispiel:


```
enable feature AppQoE

add ns tcpProfile nstcpprofile1 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 4000000 -flavor BIC -KA ENABLED -
    sendBuffsize 4000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 1000000 -fack ENABLED -tcpmode
    ENDPOINT

add ns tcpProfile nstcpprofile2 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 15 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 128000 -flavor BIC -KA ENABLED -
    sendBuffsize 6000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 64000 -fack ENABLED -tcpmode ENDPOINT

add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1

add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2

add appqoe policy appqoe_4G -rule "CLIENT.VLAN.ID.EQ(100)" -action
    action_1

add appqoe policy appqoe_3G -rule "CLIENT.VLAN.ID.EQ(200)" -action
    action_2

bind lb vserver vsrv-wireless -policyName appqoe_4G -priority 100

bind lb vserver vsrv-wireless -policyName appqoe_3G -priority 110
<!--NeedCopy-->
```

Das NetScaler T1-Modell ist in der Lage, die Abonnenteninformationen dynamisch über die Gx- oder Radius- oder Radius- und Gx-Schnittstelle zu empfangen und für jeden Abonnenten unterschiedliche TCP-Profile anzuwenden.

Befehl:

```
add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1

add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2

add appqoe policy appqoe_4G -rule "SUBSCRIBER.RULE_ACTIVE("3G")" -
    action action_1

add appqoe policy appqoe_3G -rule "SUBSCRIBER.RULE_ACTIVE("4G")" -
```



```
      action action_2
<!--NeedCopy-->
```

Informationen zur Integration des NetScaler T1-Modells in das Steuerungsebenennetz des Bedieners finden Sie unter Telco Subscriber Management.

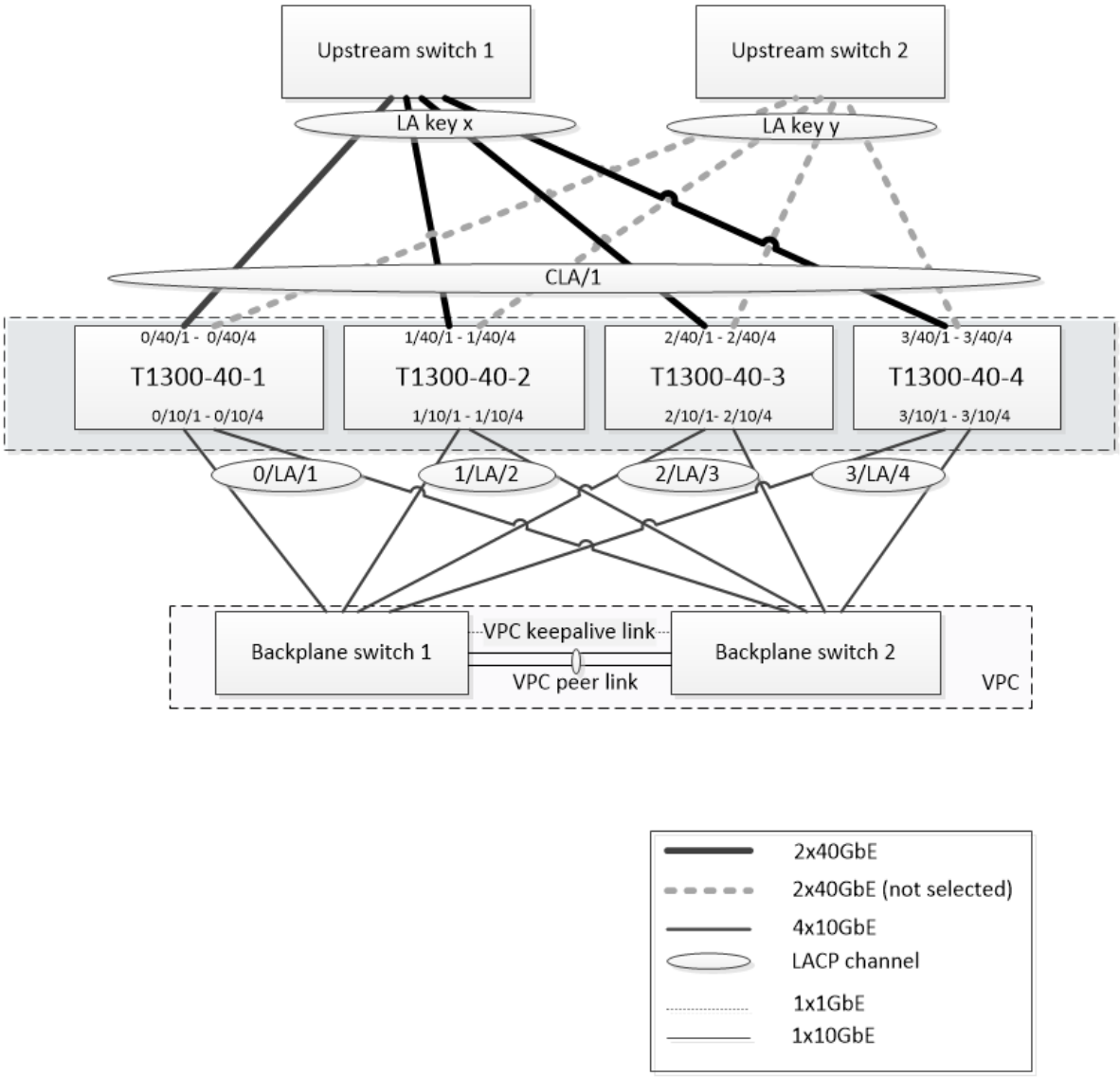
Skalierbarkeit

May 11, 2023

Da die TCP-Optimierung ressourcenintensiv ist, ist eine einzelne NetScaler-Appliance, selbst eine High-End-Appliance, möglicherweise nicht in der Lage, hohe Gi-LAN-Durchsätze aufrechtzuerhalten. Um die Kapazität Ihres Netzwerks zu erweitern, können Sie NetScaler-Appliances in einer N+1-Clusterformation bereitstellen. In einer Cluster-Bereitstellung arbeiten die NetScaler-Appliances als ein einziges System-Image zusammen. Der Client-Verkehr wird mit Hilfe eines externen Switch-Geräts auf die Clusterknoten verteilt.

Topologie

Abbildung 1 zeigt ein Beispiel für einen Cluster, der aus vier T1300-40G-Knoten besteht.



Das in Abbildung 1 gezeigte Setup hat die folgenden Eigenschaften:

1. Alle Clusterknoten gehören demselben Netzwerk an (auch bekannt als L2-Cluster).
2. Datenebene- und Backplane-Verkehr werden von verschiedenen Switches abgewickelt.
3. Unter der Annahme, dass der Gi-LAN-Durchsatz 200 Gbit/s beträgt und dass eine T1300-40G-Appliance einen Durchsatz von 80 Gbit/s aufrechterhalten kann, benötigen wir drei T1300-40G-Appliances. Um Redundanz bei einem Ausfall eines einzelnen Clusterknotens zu gewährleisten, stellen wir insgesamt vier Appliances bereit.
4. Jeder Knoten empfängt bis zu 67 Gbit/s Datenverkehr (50 Gbit/s unter normalen Betriebsbedingungen und 67 Gbit/s bei Ausfall eines einzelnen Clusterknotens). Daher benötigt er 2x40-Gbit/s-Verbindungen zum Upstream-Switch. Um Redundanz bei einem Switch-Ausfall zu gewährleisten, stellen wir einige Upstream-Switches bereit und verdoppeln die Anzahl der Verbindungen.
5. Cluster Link Aggregation (CLAG) wird verwendet, um den Datenverkehr auf Clusterknoten zu

verteilen. Eine einzige CLAG verarbeitet sowohl den Client- als auch den Serververkehr. Die Link-Redundanz ist auf dem CLAG aktiviert, sodass zu einem bestimmten Zeitpunkt nur ein „Unterkanal“ ausgewählt wird, der den Verkehr verarbeitet. Wenn eine Verbindung ausfällt oder der Durchsatz unter den angegebenen Schwellenwert fällt, wird der andere Unterkanal ausgewählt.

6. Der Upstream-Switch führt einen symmetrischen Port-Channel-Load-Balancing durch (z. B. den Source-Dest-IP-Only-Algorithmus von Cisco IOS 7.0 (8) N1 (1))), sodass vorwärts- und Rückwärtsverkehrsflüsse von demselben Clusterknoten verarbeitet werden. Diese Eigenschaft ist wünschenswert, da sie die Neuordnung von Paketen verhindert, die die TCP-Leistung beeinträchtigen würde.
7. Fünfzig Prozent des Datenverkehrs werden voraussichtlich über die Backplane gesteuert, was bedeutet, dass jeder Knoten bis zu 34 Gbit/s an andere Clusterknoten weiterleitet (25 Gbit/s unter normalen Betriebsbedingungen und 34 Gbit/s bei Ausfall eines einzelnen Clusterknotens). Daher benötigt jeder Knoten mindestens 4x10G-Verbindungen zum Backplane-Switch. Um Redundanz bei einem Switch-Ausfall zu gewährleisten, setzen wir einige Backplane-Switches ein und verdoppeln die Anzahl der Verbindungen. Link-Redundanz wird derzeit für die Backplane nicht unterstützt. Daher ist Cisco VPC oder eine gleichwertige Technologie erforderlich, um Redundanz auf Switch-Ebene zu erreichen.
8. Die MTU-Größe von gesteuerten Paketen beträgt 1578 Byte, daher müssen Backplane-Switches eine MTU von mehr als 1500 Byte unterstützen.

Hinweis: Das in Abbildung 1 dargestellte Design gilt auch für T1120- und T1310-Geräte. Für den T1310 würden wir 40-GbE-Schnittstellen für die Backplane-Verbindungen verwenden, da ihm 10GbE-Ports fehlen.

Hinweis: In diesem Dokument wird Cisco VPC zwar als Beispiel verwendet, bei der Arbeit mit Switches anderer Hersteller können jedoch alternative gleichwertige Lösungen verwendet werden, wie z. B. MLAG von Juniper.

Hinweis: Andere Topologien wie ECMP anstelle von CLAG sind zwar möglich, werden jedoch derzeit für diesen speziellen Anwendungsfall nicht unterstützt.

Konfiguration der TCP-Optimierung in einem NetScaler T1000-Cluster

Nachdem die physische Installation, die physische Konnektivität, die Softwareinstallation und die Lizenzierung abgeschlossen sind, können Sie mit der eigentlichen Clusterkonfiguration fortfahren. Die unten beschriebenen Konfigurationen gelten für den Cluster, der in Abbildung 1 dargestellt ist.

Hinweis: Weitere Informationen zur Clusterkonfiguration finden Sie unter Einrichten eines NetScaler-Clusters.

Angenommen, die vier T1300-Knoten in Abbildung 1 haben die folgenden NSIP-Adressen:

Vier T1300 Knoten mit NSIP-Adresse:


```
T1300-40-1: 10.102.29.60
T1300-40-2: 10.102.29.70
T1300-40-3: 10.102.29.80
T1300-40-4: 10.102.29.90
```

Der Cluster wird über die Cluster-IP (CLIP) -Adresse verwaltet, die als 10.78.16.61 angenommen wird.

Den Cluster einrichten

Um mit der Konfiguration des in Abbildung 1 gezeigten Clusters zu beginnen, melden Sie sich bei der ersten Appliance an, die Sie dem Cluster hinzufügen möchten (z. B. T1300-40-1), und gehen Sie wie folgt vor.

1. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

   Befehl:

   ```
   > add cluster instance 1
   > add cluster node 0 10.102.29.60 -state ACTIVE
   > add ns ip 10.102.29.61 255.255.255.255 -type clip
   > enable cluster instance 1
   > save ns config
   > reboot  - warm
   ```

2. Nach dem Neustart der Appliance stellen Sie eine Verbindung zur Cluster-IP-Adresse (CLIP) her, und fügen Sie den Rest der Knoten zum Cluster hinzu:

   Befehl:

   ```
   > add cluster node 1 10.102.29.70 -state ACTIVE
   > add cluster node 2 10.102.29.80 -state ACTIVE
   > add cluster node 3 10.102.29.90  - state ACTIVE
   > save ns config
   ```

3. Stellen Sie eine Verbindung mit der NSIP-Adresse jedes der neu hinzugefügten Knoten her, und treten Sie dem Cluster bei:

   Befehl:

   ```
   > join cluster -clip 10.102.29.61 -password nsroot
   > save ns config
   > reboot  - warm
   ```

4. Fahren Sie nach dem Neustart der Knoten mit der Backplane-Konfiguration fort. Geben Sie an der Cluster-IP-Adresse die folgenden Befehle ein, um einen LACP-Kanal für den Backplane-Link jedes Clusterknotens zu erstellen:

Befehl:

```
> set interface 0/10/[1-8] -lacpkey 1 -lacpmode ACTIVE
> set interface 1/10/[1-8] -lacpkey 2 -lacpmode ACTIVE
> set interface 2/10/[1-8] -lacpkey 3 -lacpmode ACTIVE
> set interface 3/10/[1-8] -lacpkey 4 -lacpmode ACTIVE
```

5. Konfigurieren Sie in ähnlicher Weise dynamische LA und VPC auf den Backplane-Switches. Stellen Sie sicher, dass die MTU der Backplane-Switch-Schnittstellen mindestens 1578 Byte beträgt.
6. Stellen Sie sicher, dass die Kanäle betriebsbereit sind:

   Befehl:

   ```
   > show channel 0/LA/1
   > show channel 1/LA/2
   > show channel 2/LA/3
   > show channel 3/LA/4
   ```

7. Konfigurieren Sie die Backplane-Schnittstellen des Cluster-Knotens.

   Befehl:

   ```
   > set cluster node 0 -backplane 0/LA/1
   > set cluster node 1 -backplane 1/LA/2
   > set cluster node 2 -backplane 2/LA/3
   > set cluster node 3 -backplane 3/LA/4
   ```

8. Überprüfen Sie den Clusterstatus, und stellen Sie sicher, dass der Cluster funktionsfähig ist:

   ```
   > show cluster instance
   > show cluster node
   ```

Weitere Informationen zum Cluster-Setup finden Sie unter Einrichten eines NetScaler-Clusters

Verteilung des Datenverkehrs über Clusterknoten

Nachdem Sie den NetScaler-Cluster gebildet haben, stellen Sie Cluster Link Aggregation (CLAG) bereit, um den Datenverkehr auf die Clusterknoten zu verteilen. Ein einziger CLAG-Link verarbeitet sowohl den Client- als auch den Serververkehr.

Führen Sie an der Cluster-IP-Adresse die folgenden Befehle aus, um die in Abbildung 1 gezeigte Cluster Link Aggregation (CLAG) -Gruppe zu erstellen:

Befehl:


```
> set interface 0/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 3/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
```

Konfigurieren Sie die dynamische Linkaggregation auf den externen Switches.

Aktivieren Sie dann die Link-Redundanz wie folgt:

Code:

```
> set channel CLA/1 -linkRedundancy ON -lrMinThroughput 240000
```

Überprüfen Sie schließlich den Kanalstatus, indem Sie Folgendes eingeben:

Befehl:

```
> show channel CLA/1
```

Der Kanal sollte UP sein und der tatsächliche Durchsatz sollte 320000 betragen.

Weitere Informationen zur Cluster-Link-Aggregation finden Sie in den folgenden Themen:

- Dynamische Cluster-Link-Aggregation
- Verknüpfen Sie Redundanz in einem Cluster mit LACP.

Da wir MAC-basierte Weiterleitung (MBF) verwenden, konfigurieren Sie einen Linkset und binden ihn wie folgt an die CLAG-Gruppe:

Befehl:

```
> add linkset LS/1
> bind linkset LS/1 -ifnum CLA/1
```

Weitere Informationen zu Linksets finden Sie in den folgenden Themen:

- Konfiguration von Linksets
- Verwenden des Cluster-LA-Kanals mit Linksets

Konfiguration von VLAN und IP-Adressen

Wir werden Striped IP-Konfiguration verwenden, was bedeutet, dass IP-Adressen auf allen Knoten aktiv sind (Standardeinstellung). Weitere Informationen zu diesem Thema finden Sie unter Gestreifte, teilweise gestreifte und gepunktete Konfigurationen .

1. Fügen Sie die Ein- und Ausgangs-SNIPs hinzu:

   Befehl:


```
> add ns ip 172.16.30.254 255.255.255.0  - type SNIP
> add ns ip 172.16.31.254 255.255.255.0  - type SNIP
> add ns ip6 fd00:172:16:30::254/112  - type SNIP
> add ns ip6 fd00:172:16:31::254/112  - type SNIP
```

2. Fügen Sie die entsprechenden VLANs hinzu:

   Befehl:

```
> add vlan 30 -aliasName wireless
> add vlan 31 -aliasName internet
```

3. Binden Sie VLANs mit IPs und Linkset:

   Befehl:

```
> bind vlan 31 -ifnum LS/1 -tagged
> bind vlan 30 -ifnum LS/1 -tagged
> bind vlan 30 -IPAddress 172.16.30.254 255.255.255.0
> bind vlan 31 -IPAddress 172.16.31.254 255.255.255.0
> bind vlan 30 -IPAddress fd00:172:16:30::254/112
> bind vlan 31 -IPAddress fd00:172:16:31::254/112
```

Bei Bedarf können mehr Ein- und Ausstieg VLANs hinzugefügt werden.

Konfiguration der TCP-Optimierung

An dieser Stelle haben wir alle clusterspezifischen Befehle angewendet. Um die Konfiguration abzuschließen, führen Sie die in TCP-Optimierungskonfigurationbeschriebenen Schritte aus.

Dynamisches Routing konfigurieren

Ein NetScaler-Cluster kann in die dynamische Routing-Umgebung des Kundennetzwerks integriert werden. Im Folgenden finden Sie ein Beispiel für eine dynamische Routing-Konfiguration mit dem BGP-Routing-Protokoll (OSPF wird ebenfalls unterstützt).

1. Aktivieren Sie über die CLIP-Adresse BGP und dynamisches Routing für eingehende und ausgehende IP-Adressen:

   Befehl:

```
> enable ns feature bgp
> set ns ip 172.16.30.254  - dynamicRouting ENABLED
> set ns ip 172.16.31.254  - dynamicRouting ENABLED
```


2. Öffnen Sie vtysh und konfigurieren Sie BGP für die Egress-Seite:

   Code:

```
> shell
root@ns# vtysh
ns# configure terminal
ns(config)# router bgp 65531
ns(config-router)# network 10.0.0.0/24
ns(config-router)# neighbor 172.16.31.100 remote-as 65530
ns(config-router)# neighbor 172.16.31.100 update-source
    172.16.31.254
ns(config-router)# exit
ns(config)# ns route-install propagate
ns(config)# ns route-install default
ns(config)# ns route-install bgp
ns(config)# exit
```

3. Konfigurieren Sie den egress-seitigen BGP-Peer, um die Standardroute zum NetScaler Cluster anzukündigen. Zum Beispiel:

   Befehl:

```
router bgp 65530
 bgp router-id 172.16.31.100
 network 0.0.0.0/0
 neighbor 172.16.31.254 remote-as 65531
```

4. Führen Sie ähnliche Schritte aus, um die Eindringseite zu konfigurieren.

5. Stellen Sie von vtysh aus sicher, dass die Konfiguration an alle Clusterknoten weitergegeben wird, indem Sie Folgendes eingeben:

   Befehl:

```
ns# show running-config
```

6. Melden Sie sich schließlich bei der NSIP-Adresse jedes Clusterknotens an und überprüfen Sie die von BGP-Peer angekündigten Routen:

   Befehl:

```
> show route | grep BGP
```


Optimierung der TCP-Leistung mit TCP-Nile

May 11, 2023

TCP verwendet die folgenden Optimierungstechniken und Strategien (oder Algorithmen) zur Überlastungskontrolle, um Netzwerkengpässe bei der Datenübertragung zu vermeiden.

Strategien zur Staukontrolle

Das Transmission Control Protocol (TCP) wird seit langem verwendet, um Internetverbindungen herzustellen und zu verwalten, Übertragungsfehler zu behandeln und Webanwendungen reibungslos mit Client-Geräten zu verbinden. Der Netzwerkverkehr ist jedoch schwieriger zu kontrollieren, da der Paketverlust nicht nur von der Überlastung des Netzwerks abhängt und eine Überlastung nicht unbedingt zu Paketverlusten führt. Um die Überlastung zu messen, sollte sich ein TCP-Algorithmus daher sowohl auf den Paketverlust als auch auf die Bandbreite konzentrieren.

NIL-Algorithmus

Citrix Systems hat einen neuen Algorithmus zur Überlastungskontrolle entwickelt, NILE, einen TCP-Optimierungsalgorithmus, der für Hochgeschwindigkeitsnetzwerke wie LTE, LTE Advanced und 3G entwickelt wurde. Nile befasst sich mit einzigartigen Herausforderungen, die durch Fading, zufällige oder überlastete Verluste, Neuübertragungen auf Verbindungsschicht und Trägeraggregation entstehen.

Der NIL-Algorithmus:

- Basiert Schätzungen der Warteschlangenlatenz auf Messungen von Hin- und Rücklaufzeiten.
- Verwendet eine Funktion zur Erhöhung des Überlastungsfensters, die umgekehrt proportional zur gemessenen Warteschlangenlatenz ist. Diese Methode führt dazu, dass sich der Netzwerküberlastungspunkt langsamer nähert als die Standard-TCP-Methode und reduziert die Paketverluste bei einer Überlastung.
- Kann anhand der geschätzten Warteschlangenlatenz zwischen zufälligen Verlusten und Datenverlusten aufgrund von Engpässen im Netzwerk unterscheiden.

Die Telekommunikationsdienstanbieter können den NILE-Algorithmus in ihrer TCP-Infrastruktur verwenden, um:

- Optimieren Sie Mobil- und Fernnetze — Der NILE-Algorithmus erzielt im Vergleich zu Standard-TCP einen höheren Durchsatz. Diese Funktion ist besonders wichtig für Mobil- und Fernnetze.
- Verringern Sie die wahrgenommene Latenz von Anwendungen und verbessern Sie das Nutzererlebnis — Der Nile-Algorithmus verwendet Informationen zum Paketverlust, um zu bestimmen,

ob das Übertragungsfenster vergrößert oder verkleinert werden sollte, und verwendet Informationen zur Wartezeit in der Warteschlange, um die Größe der Erhöhung oder Verringerung zu bestimmen. Diese dynamische Einstellung der Größe des Übertragungsfensters verringert die Anwendungslatenz im Netzwerk.

So konfigurieren Sie die NILE-Unterstützung mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns tcpProfile <name> [-flavor NILE]
<!--NeedCopy-->
```

Konfiguration der NILE-Unterstützung mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **System** > **Profile** > **TCP-Profile** und klicken Sie auf **TCP-Profile**.
2. Wählen Sie in der Dropdownliste **TCP-Flavor** die Option **NILE** aus.

Beispiel:

```
set ns tcpProfile tcpprofile1 -flavor NILE
<!--NeedCopy-->
```

PRR-Algorithmus (Proportional Rate Recovery)

TCP-Schnellwiederherstellungsmechanismen reduzieren die durch Paketverluste verursachte Weblatenz. Der neue PRR-Algorithmus (Proportional Rate Recovery) ist ein schneller Wiederherstellungsalgorithmus, der TCP-Daten während einer Loss Recovery auswertet. Das Muster ist dem Rate-Halving nachempfunden, indem der Bruchteil verwendet wird, der für das vom Staukontrollalgorithmus gewählte Zielfenster geeignet ist. Dadurch wird die Fensteranpassung minimiert, und die tatsächliche Fenstergröße am Ende der Wiederherstellung liegt nahe am Schwellenwert für langsamen Start (ssthresh).

Schnelles TCP-Öffnen (TFO)

TCP Fast Open (TFO) ist ein TCP-Mechanismus, der einen schnellen und sicheren Datenaustausch zwischen einem Client und einem Server während des ersten TCP-Handshakes ermöglicht. Diese Funktion ist als TCP-Option im TCP-Profil verfügbar, das an einen virtuellen Server einer NetScaler-Appliance gebunden ist. TFO verwendet ein TCP-Fast-Open-Cookie (ein Sicherheitscookie), das die NetScaler-Appliance generiert, um den Client zu validieren und zu authentifizieren, der eine TFO-Verbindung zum virtuellen Server initiiert. Mithilfe des TFO-Mechanismus können Sie die Netzwerklatenz einer

Anwendung um die Zeit reduzieren, die für einen vollständigen Roundtrip erforderlich ist, wodurch die Verzögerung bei kurzen TCP-Übertragungen erheblich reduziert wird.

So funktioniert TFO

Wenn ein Client versucht, eine TFO-Verbindung herzustellen, enthält er ein TCP-Fast-Open-Cookie mit dem anfänglichen SYN-Segment, um sich zu authentifizieren. Wenn die Authentifizierung erfolgreich ist, kann der virtuelle Server auf der NetScaler-Appliance Daten in das SYN-ACK-Segment aufnehmen, obwohl er das letzte ACK-Segment des Drei-Wege-Handshakes nicht empfangen hat. Dadurch wird im Vergleich zu einer normalen TCP-Verbindung, für die ein dreifacher Handshake erforderlich ist, bevor Daten ausgetauscht werden können, bis zu einem kompletten Round-Trip eingespart.

Ein Client und ein Backend-Server führen die folgenden Schritte durch, um eine TFO-Verbindung herzustellen und Daten während des ersten TCP-Handshakes sicher auszutauschen.

1. Wenn der Client kein TCP-Fast-Open-Cookie hat, um sich zu authentifizieren, sendet er eine Fast Open Cookie-Anfrage im SYN-Paket an den virtuellen Server auf der NetScaler-Appliance.
2. Wenn die TFO-Option in dem an den virtuellen Server gebundenen TCP-Profil aktiviert ist, generiert die Appliance ein Cookie (indem die IP-Adresse des Clients mit einem geheimen Schlüssel verschlüsselt wird) und antwortet dem Client mit einem SYN-ACK, das das generierte Fast Open Cookie in einem TCP-Optionsfeld enthält.
3. Der Client speichert das Cookie für zukünftige TFO-Verbindungen zu demselben virtuellen Server auf der Appliance.
4. Wenn der Client versucht, eine TFO-Verbindung zu demselben virtuellen Server herzustellen, sendet er SYN, das das zwischengespeicherte Fast Open Cookie (als TCP-Option) zusammen mit HTTP-Daten enthält.
5. Die NetScaler-Appliance validiert das Cookie, und wenn die Authentifizierung erfolgreich ist, akzeptiert der Server die Daten im SYN-Paket und bestätigt das Ereignis mit einem SYN-ACK, einem TFO-Cookie und einer HTTP-Antwort.

Hinweis: Wenn die Client-Authentifizierung fehlschlägt, löscht der Server die Daten und bestätigt das Ereignis nur mit einem SYN, das auf ein Sitzungs-Timeout hinweist.

1. Wenn auf der Serverseite die TFO-Option in einem an einen Dienst gebundenen TCP-Profil aktiviert ist, bestimmt die NetScaler-Appliance, ob das TCP Fast Open Cookie in dem Dienst vorhanden ist, zu dem sie versucht, eine Verbindung herzustellen.
2. Wenn das TCP Fast Open Cookie nicht vorhanden ist, sendet die Appliance eine Cookie-Anfrage im SYN-Paket.
3. Wenn der Backend-Server das Cookie sendet, speichert die Appliance das Cookie im Serverinformationscache.
4. Wenn die Appliance bereits über ein Cookie für das angegebene Ziel-IP-Paar verfügt, ersetzt sie das alte Cookie durch das neue.

5. Wenn das Cookie im Serverinformationscache verfügbar ist, wenn der virtuelle Server versucht, mithilfe derselben SNIP-Adresse erneut eine Verbindung zu demselben Backend-Server herzustellen, kombiniert die Appliance die Daten im SYN-Paket mit dem Cookie und sendet sie an den Backend-Server.
6. Der Backend-Server bestätigt das Ereignis sowohl mit Daten als auch mit einem SYN.

Hinweis: Wenn der Server das Ereignis nur mit einem SYN-Segment bestätigt, sendet die NetScaler-Appliance das Datenpaket sofort erneut, nachdem das SYN-Segment und die TCP-Optionen aus dem ursprünglichen Paket entfernt wurden.

Konfiguration von TCP Fast Open

Um die Funktion TCP Fast Open (TFO) zu verwenden, aktivieren Sie die Option TCP Fast Open im entsprechenden TCP-Profil und setzen Sie den Parameter TFO Cookie Timeout auf einen Wert, der den Sicherheitsanforderungen für dieses Profil entspricht.

So aktivieren oder deaktivieren Sie TFO mithilfe der Befehlszeile

Geben Sie in der Befehlszeile einen der folgenden Befehle ein, um TFO in einem neuen oder vorhandenen Profil zu aktivieren oder zu deaktivieren.

Hinweis: Der Standardwert ist DISABLED.

```
add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
unset tcpprofile <TCP Profile Name> - tcpFastOpen
<!--NeedCopy-->
```

Beispiele:

füge tcpprofile Profile1 hinzu — tcpFastOpen Set tcpprofile Profile1 — tcpFastOpen aktiviert
unset tcpprofile Profile1 — tcpFastOpen

So legen Sie den Timeout-Wert für das TCP-FastOpen-Cookie mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set tcpparam  - tcpfastOpenCookieTimeout <Timeout Value>
<!--NeedCopy-->
```

Beispiel:


```
set tcpprofile  - tcpfastOpenCookieTimeout 30secs
<!--NeedCopy-->
```

So konfigurieren Sie das TCP Fast Open mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Markieren Sie auf der Seite „ **TCP-Profil konfigurieren** “ das Kontrollkästchen **TCP Fast Open** .
3. Klicke auf **OK** und dann auf **Fertig**.

So konfigurieren Sie den TCP-Fast-Cookie-Timeout-Wert mithilfe der GUI

Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen** > **TCP-Parameter ändern** und dann zur Seite „ **TCP-Parameter konfigurieren**“, um den Timeout-Wert für das TCP-Fast-Open-Cookie festzulegen.

TCP-Hystart

Ein neuer TCP-Profilparameter, hystart, aktiviert den Hystart-Algorithmus, bei dem es sich um einen langsamen Start-Algorithmus handelt, der dynamisch einen sicheren Punkt für die Beendigung bestimmt (ssthresh). Es ermöglicht einen Übergang zur Vermeidung von Engpässen ohne starke Paketverluste. Dieser neue Parameter ist standardmäßig deaktiviert.

Wenn ein Stau erkannt wird, geht Hystart in eine Phase zur Vermeidung von Staus über. Wenn Sie es aktivieren, erhalten Sie einen besseren Durchsatz in Hochgeschwindigkeitsnetzwerken mit hohem Paketverlust. Dieser Algorithmus trägt dazu bei, bei der Verarbeitung von Transaktionen eine nahezu maximale Bandbreite aufrechtzuerhalten. Es kann daher den Durchsatz verbessern.

TCP-Hystart konfigurieren

Um die Hystart-Funktion zu verwenden, aktivieren Sie die Option Cubic Hystart im entsprechenden TCP-Profil.

So konfigurieren Sie Hystart mithilfe der Befehlszeilenschnittstelle (CLI)

Geben Sie an der Befehlszeile einen der folgenden Befehle ein, um Hystart in einem neuen oder vorhandenen TCP-Profil zu aktivieren oder zu deaktivieren.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
```



```
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Beispiele:

```
add tcpprofile Profile1 - tcpFastOpen
Set tcpprofile Profile1 - tcpFastOpen Enabled
unset tcpprofile Profile1 - tcpFastOpen
<!--NeedCopy-->
```

So konfigurieren Sie die Hystart-Support mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite „ **TCP-Profil konfigurieren** “ das Kontrollkästchen **Cubic Hystart** .
3. Klicke auf **OK** und dann auf **Fertig**.

Optimierungstechniken

TCP verwendet die folgenden Optimierungstechniken und -methoden für optimierte Flusskontrollen.

Richtlinienbasierte TCP-Profilauswahl

Der Netzwerkverkehr ist heute vielfältiger und bandbreitenintensiver als je zuvor. Angesichts des erhöhten Datenverkehrs ist der Effekt, den Quality of Service (QoS) auf die TCP-Leistung hat, erheblich. Um die QoS zu verbessern, können Sie jetzt AppQoE-Richtlinien mit verschiedenen TCP-Profilen für verschiedene Klassen von Netzwerkverkehr konfigurieren. Die AppQoE-Richtlinie klassifiziert den Datenverkehr eines virtuellen Servers, um ein TCP-Profil zuzuordnen, das für einen bestimmten Verkehrstyp wie 3G, 4G, LAN oder WAN optimiert ist.

Um dieses Feature zu verwenden, erstellen Sie für jedes TCP-Profil eine Richtlinienaktion, ordnen Sie eine Aktion AppQoE-Richtlinien zu und binden Sie die Richtlinien an die virtuellen Server mit Lastenausgleich.

Konfiguration der richtlinienbasierten TCP-Profilauswahl

Die Konfiguration der richtlinienbasierten TCP-Profilauswahl umfasst die folgenden Aufgaben:

- AppQoE aktivieren. Bevor Sie die TCP-Profilfunktion konfigurieren, müssen Sie die AppQoE-Funktion aktivieren.
- AppQoE-Aktion wird hinzugefügt. Nachdem Sie die AppQoE-Funktion aktiviert haben, konfigurieren Sie eine AppQoE-Aktion mit einem TCP-Profil.

- Konfiguration der AppQoE-basierten TCP-Profilauswahl. Um die TCP-Profilauswahl für verschiedene Verkehrsklassen zu implementieren, müssen Sie AppQoE-Richtlinien konfigurieren, anhand derer Ihre NetScaler-Appliance die Verbindungen unterscheiden und die richtige AppQoE-Aktion an jede Richtlinie binden kann.
- Bindung der AppQoE-Richtlinie an den virtuellen Server. Nachdem Sie die AppQoE-Richtlinien konfiguriert haben, müssen Sie sie an einen oder mehrere virtuelle Load Balancing-, Content Switching- oder Cache-Umleitungsserver binden.

Konfiguration über die Befehlszeilenschnittstelle

Um AppQOE mithilfe der Befehlszeilenschnittstelle zu aktivieren:

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Funktion zu aktivieren, und überprüfen Sie, ob sie aktiviert ist:

```
enable ns feature appqoe

show ns feature
<!--NeedCopy-->
```

Um ein TCP-Profil zu binden, während Sie eine AppQoE-Aktion mithilfe der Befehlszeilenschnittstelle erstellen

Geben Sie an der Befehlszeile den folgenden AppQoE-Aktionsbefehl mit der Option tcpprofiletobind ein.

Binden eines TCP-Profils:

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS |
    NS ) [<CustomFile>] [-altContentSvcName <string>] [-altContentPath <
    string>] [-maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth
     <positive_integer>] [-priqDepth <positive_integer>] [-
    dosTrigExpression <expression>] [-dosAction ( SimpleResponse |
    HICResponse )] [-tcpprofiletobind <string>]

show appqoe action
<!--NeedCopy-->
```

So konfigurieren Sie eine AppQoE-Richtlinie mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
add appqoe policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Um eine AppQoE-Richtlinie mithilfe der Befehlszeilenschnittstelle an virtuelle Server für Load Balancing, Cache-Umleitung oder Content Switching zu binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <
    priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <
    priority>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <
    priority>
<!--NeedCopy-->
```

Beispiel:

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
    ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500 -
    slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
    sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack ENABLED
    -tcpmode ENDPOINT

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
    action appact1

bind lb vserver lb2 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST

bind cs vserver cs1 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Konfiguration der richtlinienbasierten TCP-Profilerstellung mithilfe der GUI

Um AppQOE mithilfe der GUI zu aktivieren

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.

3. Aktivieren **Sie im Dialogfeld „Erweiterte Funktionen konfigurieren** “ das Kontrollkästchen **AppQoE** .
4. Klicken Sie auf **OK**.

So konfigurieren Sie die AppQoE-Richtlinie mithilfe der GUI

1. Navigieren Sie zu **App-Expert** > **AppQoE** > **Actions.**
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
3. Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
4. Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
5. Geben **Sie im Bildschirm AppQoE-Aktion erstellen** oder **AppQoE-Aktion konfigurieren** Werte für die Parameter ein, oder wählen Sie sie aus. Der Inhalt des Dialogfelds entspricht den unter „Parameter für die Konfiguration der AppQoE-Aktion“ beschriebenen Parametern wie folgt (ein Sternchen gibt einen erforderlichen Parameter an):
   a) Name—Name
   b) Aktionstyp — Antworten mit
   c) Priorität — Priorität
   d) Tiefe der Richtlinienwarteschlange — POLQDepth
   e) Warteschlangentiefe — PriqDepth
   f) DOS-Aktion — DOS-Aktion
6. Klicken Sie auf **Erstellen**.

So binden Sie die AppQoE-Richtlinie mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen Server aus und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie im Abschnitt **Richtlinien** auf (+), um eine AppQoE-Richtlinie zu binden.
3. Gehen Sie im Schieberegler **Richtlinien** wie folgt vor:
   a) Wählen Sie in der Dropdownliste einen Richtlinientyp als AppQoE aus.
   b) Wählen Sie einen Verkehrstyp aus der Dropdownliste aus.
4. Gehen Sie im Abschnitt **Richtlinienbindung** wie folgt vor:
   a) Klicken Sie auf **Neu**, um eine neue AppQoE-Richtlinie zu erstellen.
   b) Klicken Sie auf **Existing Policy**, um eine AppQoE-Richtlinie aus der Dropdownliste auszuwählen.
5. Legen Sie die Bindungspriorität fest und klicken Sie auf An die Richtlinie an den virtuellen Server **binden** .
6. Klicken Sie auf **Fertig**.

SACK-Blockgenerierung

Die TCP-Leistung verlangsamt sich, wenn mehrere Pakete in einem Datenfenster verloren gehen. In einem solchen Szenario überwindet ein SACK-Mechanismus (Selective Acknowledgement) in Kombination mit einer selektiven Wiederholungsrichtlinie diese Einschränkung. Für jedes eingehende Paket, das nicht in der richtigen Reihenfolge ist, müssen Sie einen SACK-Block generieren.

Wenn das Paket, das nicht in der Reihenfolge ist, in den Queue-Block für die Reassemblierung passt, fügen Sie die Paketinformationen in den Block ein und legen Sie die vollständigen Blockinformationen auf SACK-0 fest. Wenn ein Paket nicht in der richtigen Reihenfolge in den Zusammenbaublock passt, senden Sie das Paket als SACK-0 und wiederholen Sie die früheren SACK-Blöcke. Wenn ein Paket nicht in der richtigen Reihenfolge ein Duplikat ist und die Paketinformation auf SACK-0 gesetzt ist, dann D-Sack den Block.

Hinweis: Ein Paket wird als D-SACK betrachtet, wenn es sich um ein bestätigtes Paket oder um ein fehlerhaftes Paket handelt, das bereits empfangen wurde.

Kunde Reneging

Eine NetScaler-Appliance kann Client-Renegings während einer SACK-basierten Wiederherstellung verarbeiten.

Die Speicherprüfungen zur Markierung des Endpunkts auf der Leiterplatte berücksichtigen nicht den gesamten verfügbaren Speicher

Wenn in einer NetScaler-Appliance der Schwellenwert für die Speichernutzung auf 75 Prozent gesetzt wird, anstatt den gesamten verfügbaren Speicher zu nutzen, führt dies dazu, dass neue TCP-Verbindungen die TCP-Optimierung Bypass.

Unnötige Neuübertragungen aufgrund fehlender SACK-Blöcke

Wenn Sie in einem Modus ohne Endpunkt DUPACKS senden und SACK-Blöcke für einige Pakete fehlen, die nicht in der richtigen Reihenfolge sind, werden zusätzliche Neuübertragungen vom Server ausgelöst.

SNMP für die Anzahl der Verbindungen hat die Optimierung aufgrund von Überlastung umgangen

Die folgenden SNMP-IDs wurden einer NetScaler-Appliance hinzugefügt, um die Anzahl der Verbindungen zu verfolgen, bei denen die TCP-Optimierung aufgrund von Überlastung umgangen wurde.

1. 1.3.6.1.4.1.5951.4.1.1.46.13 (TCP-Optimierung aktiviert). Um die Gesamtzahl der mit der TCP-Optimierung aktivierten Verbindungen zu verfolgen.

2. 1.3.6.1.4.1.5951.4.1.1.46.132 (TCP-Optimierung wurde umgangen). Um die Gesamtzahl der Verbindungen zu verfolgen, wurde die TCP-Optimierung umgangen.

Dynamischer Empfangspuffer

Um die TCP-Leistung zu maximieren, kann eine NetScaler Appliance nun die Größe des TCP-Empfangspuffers dynamisch anpassen.

Leitfaden zur Fehlerbehebung

May 11, 2023

Technischer Support

Für alle Problembehebungs- und Eskalationsanfragen ist ein aktuelles NetScaler-TechSupport-Paket erforderlich, das die aktuelle Konfiguration, die installierte Firmware-Version, Protokolldateien, ausstehende Kerne und andere Informationen erfasst.

Beispiel:

```
show techsupport

showtechsupport data collector tool - $Revision: #5 $!
...
<!--NeedCopy-->
```

Alle Daten werden gesammelt unter

```
...
Archiving all the data into "/var/tmp/support/collector_P_192
    .168.121.117_18Jun2015_09_53.tar.gz" ....
Created a symbolic link for the archive with /var/tmp/support/support.
    tgz
/var/tmp/support/support.tgz  ---- points to ---> /var/tmp/support/
    collector_P_192.168.121.117_18Jun2015_09_53.tar.gz
<!--NeedCopy-->
```

Nachdem ein Techsupport-Paket generiert wurde, kann es mithilfe von SCP kopiert werden.

Spuren

NetScaler-TCP-Optimierungsprobleme erfordern normalerweise NetScaler-Traces, um die Fehler ordnungsgemäß zu beheben. Beachten Sie, dass man versuchen sollte, Spuren unter ähnlichen Bedingungen zu erfassen, d. h. auf derselben Zelle, zur gleichen Tageszeit, mit derselben Benutzerausrüstung und Anwendung und anderen.

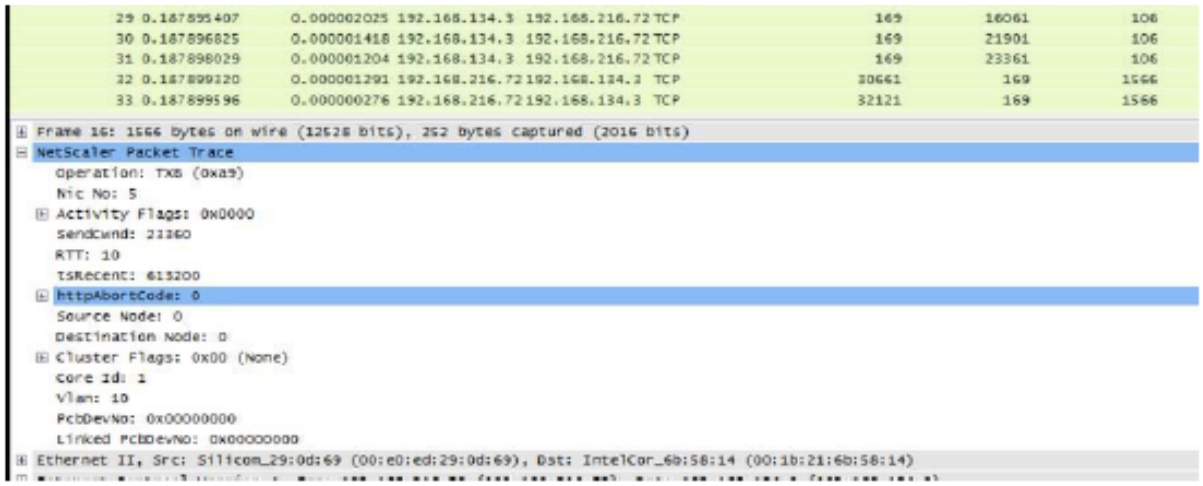
Die Befehle start nstrace und stop nstrace können verwendet werden, um Spuren zu erfassen:

- Es wird dringend empfohlen, den entsprechenden Filter zu verwenden, um zu verhindern, dass beim Trace überflüssige, überflüssige Pakete erfasst werden. Verwenden Sie beispielsweise start nstrace -filter 'IP == 10.20.30.40', um nur Pakete zu erfassen, die an die IP-Adresse 10.20.30.40 gesendet oder von dieser empfangen werden, was die IP-Adresse des Benutzergeräts ist.
- Verwenden Sie nicht die Option -tcpdump, da sie die für das Debuggen erforderlichen nstrace-Header entfernt.

Spurenanalyse

Nachdem ein NetScaler-Trace erfasst wurde, kann er mit Wireshark 1.12 oder höher betrachtet werden. Stellen Sie sicher, dass die erfassten Traces die entsprechenden NetScaler Packet Trace-Header enthalten, wie in der folgenden Bildschirmaufnahme dargestellt:

Die zusätzlichen Debug-Header sind auch in der folgenden Abbildung sichtbar:



Verbindungstabelle

Wenn das Problem mit der TCP-Optimierung zusammenhängt und reproduziert werden kann oder im Gange ist, ist es am besten, auch die Verbindungstabelle abzurufen, wenn das Problem vom primären T1-Knoten aus auftritt.

Um die Tabelle zu erhalten, müssen Sie zur BSD-Shell wechseln und den folgenden Befehl ausführen:

```
shell
...

nscli -U 127.0.0.1:nsroot:nsroot show connectiontable -detail full link
    > /var/tmp/contable.log
<!--NeedCopy-->
```

> **Hinweis**
>
> Der Befehl wird möglicherweise für einen längeren Zeitraum ausgeführt, und die Verwaltungs-CPU ist möglicherweise zu diesem Zeitpunkt belastet (hängt von der Anzahl der Verbindungstabelleneinträge ab), aber er hat keinen Einfluss auf den Dienst.

Häufig gestellte Fragen

May 11, 2023

Timeouts

> **Wichtig**
>
> Bevor Sie *einen nsapimgr-Knopf* verwenden, wenden Sie sich an den Citrix Kundensupport.

Im Folgenden finden Sie eine Liste verschiedener Timeouts für inaktive Verbindungen, die auf virtuellen NetScaler T1-Servern und -Diensten festgelegt werden können. Die für Client- oder Serververbindungen auf vServer- oder Serviceebene festgelegten Leerlauf-Timeouts gelten nur für Verbindungen im Status TCP ESTABLISHED und sind inaktiv.

- Virtueller Load Balancing-Server Der cltTimeout-Parameter gibt die Zeit in Sekunden an, in der eine Verbindung von einem Client zu einem virtuellen Load Balancing-Server inaktiv sein muss, bevor die Appliance die Verbindung schließt.
- Der Parameter Service SvrTimeout gibt die Zeit in Sekunden an, während der eine Verbindung von der Appliance zu einem Dienst oder Server inaktiv sein muss, bevor die Appliance die Verbindung schließt.
- Der Parameter Service cltTimeout gibt die Zeit in Sekunden an, in der eine Verbindung von einem Client zu einem Dienst inaktiv sein muss, bevor die Appliance die Verbindung schließt.

Wenn ein Dienst an einen virtuellen Load Balancing-Server gebunden ist, hat das cltTimeout für den virtuellen Load Balancing-Server Vorrang, und der Dienst cltTimeout for service wird ignoriert.

Falls kein Dienst an den virtuellen Load Balancing-Server gebunden ist, wird das globale Leerlaufzeitlimit, nämlich TCPServer, für serverseitige Verbindungen verwendet. Sie kann wie folgt konfiguriert werden:

Befehl:

```
set ns timeout -tcpServer 9000
<!--NeedCopy-->
```

Verbindungen in einem anderen Status haben unterschiedliche Timeout-Werte:

- Timeout im Leerlauf bei halb geöffneten Verbindungen: 120 Sekunden (fest codierter Wert)
- Timeout für TIME_WAIT-Verbindungen im Leerlauf: 40 Sekunden (fest codierter Wert)
- Timeout bei halbem Schließen von Verbindungen im Leerlauf. Standardmäßig ist es 10s und kann mithilfe des Snippets zwischen 1 s und 600 s konfiguriert werden.

Befehl:

```
 set ns timeout -halfclose 10
<!--NeedCopy-->
```

Wenn ein Timeout bei halbem Schließen ausgelöst wird, wird die Verbindung in den Zombie-Status versetzt. Wenn das Zombie-Timeout abläuft, wird das Zombie-Cleanup aktiviert und T1 sendet standardmäßig RST sowohl auf der Client- als auch auf der Serverseite für die angegebene Verbindung.

- Zombie-Timeout: Intervall, in dem der Zombie-Bereinigungsprozess ausgeführt werden muss, um inaktive TCP-Verbindungen zu bereinigen. Der Standard-Timeout-Wert ist 120 s und kann zwischen 1 s und 600 s konfiguriert werden.

Befehl:

```
set ns timeout -zombie 120
<!--NeedCopy-->
```

Tabelle mit maximaler Segmentgröße

Eine NetScaler T1-Appliance schützt vor SYN-Flood-Angriffen, indem sie SYN-Cookies verwendet, anstatt halboffene Verbindungen auf dem Systemspeicherstapel aufrechtzuerhalten. Die Appliance sendet ein Cookie an jeden Client, der eine TCP-Verbindung anfordert, behält jedoch nicht den Status halboffener Verbindungen bei. Stattdessen weist die Appliance Systemspeicher für eine Verbindung erst zu, wenn sie das letzte ACK-Paket empfängt oder, für HTTP-Verkehr, wenn eine HTTP-Anfrage empfangen wird. Dadurch werden SYN-Angriffe verhindert und die normale TCP-Kommunikation mit legitimen Clients kann unterbrechungsfrei fortgesetzt werden. Eine bestimmte Funktion ist standardmäßig aktiviert, ohne dass eine Option zum Deaktivieren vorhanden ist.

Es gibt jedoch einen Vorbehalt, da standardmäßige SYN-Cookies Verbindungen auf die Verwendung von nur acht MSS-Werten (Maximum Segment Size) beschränken. Wenn die Verbindungs-MMS mit keinem vordefinierten Wert übereinstimmt, wird sowohl auf der Client- als auch auf der Serverseite der nächste verfügbare niedrigere Wert verwendet.

Die vordefinierten TCP-Werte für maximale Segmentgröße (MSS) lauten wie folgt und können über einen neuen nsapimgr-Knopf konfiguriert werden.

1460	1440	1330	1220	956	536	384	128

Die neue MSS-Tabelle:

- Muss keine Jumbo-Frame-Unterstützung enthalten. Obwohl in der MSS-Tabelle standardmäßig 8 Werte für Jumbo-Frames reserviert sind, können die Tabelleneinstellungen so geändert werden, dass sie nur standardmäßige Frames in Ethernet-Größe enthalten.
- Sollte 16 Werte haben
- Sollte Werte in absteigender Reihenfolge haben
- Sollte 128 als letzten Wert enthalten

Wenn die neue MSS-Tabelle gültig ist, wird die Tabelle gespeichert und die alten Werte werden bei der SYN-Cookie-Rotation ausgetauscht. Andernfalls gibt die neue Tabelle einen Fehler zurück. Än-

derungen werden auf neue Verbindungen angewendet, während bestehende Verbindungen die alte MSS-Tabelle beibehalten, bis die Verbindungen ablaufen oder beendet werden.

Geben Sie den folgenden Befehl ein, um die aktuelle MSS-Tabelle in einer NetScaler-Appliance anzuzeigen.

Befehl:

```
>shell

#nsapimgr -d mss_table
```

Beispiel:

```
#nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1440,1330,1212,956,536,384,128
     }


Done.
```

Um die MSS-Tabelle zu ändern, geben Sie den folgenden Befehl ein:

Befehl:

```
>shell

#nsapimgr -s mss_table=<16 comma seperated values>
```

Beispiel:

```
#nsapimgr -ys mss_table
   =9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128
     }

```



```
10
11 Done.
```

Ein Beispiel, das Standardwerte für Ethernet-Größe verwendet, ist unten dargestellt:

Beispiel:

```
1 #nsapimgr -ys mss_table
     =1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128


2
3 # nsapimgr -d mss_table
4
5 MSS table
6
7 {
8  1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128
       }
9
10
11 Done.
```

Um diese Änderung auch nach dem Neustart der NetScaler Appliance dauerhaft zu machen, fügen Sie den Befehl `##nsapimgr -ys mss_table=<16 comma seperated values>` in die Datei "/nsconfig/rc.netscaler" ein. Wenn die Datei „rc.netscaler" nicht existiert, erstellen Sie sie im Ordner „/nsconfig" und hängen Sie dann den Befehl an.

Schutz vor Speicherüberlastung

Eine NetScaler Packet Processing Engine (PPE) beginnt, Verbindungen aus der TCP-Optimierung zu umgehen, wenn der von dieser einen PPE verwendete Speicher einen bestimmten hohen Wasserzeichenwert überschreitet. Wenn die PPE-Speicherauslastung ~2,6 GB übersteigt, werden *alle neuen* Verbindungen aus der Optimierung umgangen. Die bestehenden Verbindungen (die zuvor zur Optimierung zugelassen wurden) werden weiter optimiert. Dieser Wasserzeichenwert wurde bewusst ausgewählt und wird nicht zur Optimierung empfohlen.

> **Hinweis**
>
> Wenn Sie der Meinung sind, dass es einen guten Grund gibt, diesen Wasserzeichenwert zu ändern, wenden Sie sich an den Kundensupport.

Unterstützung für Happy Eyeballs Kunden

Wenn die NetScaler-Appliance ein SYN für ein Ziel empfängt, dessen Status unbekannt ist, überprüft die Appliance zunächst die Erreichbarkeit des Servers und bestätigt dann den Client. Dieser Prüfmechanismus ermöglicht es Clients mit dualen IP-Stacks, die Erreichbarkeit von Dual-Stack-Internetservern zu ermitteln. Wenn der Client feststellt, dass sowohl IPv6- als auch IPv4-Zugriff verfügbar sind, stellt er eine Verbindung zum Server her, der schneller reagiert, und setzt den anderen zurück. Wenn die Verbindung für die NetScaler-Appliance zurückgesetzt wird, wird die entsprechende serverseitige Verbindung zurückgesetzt.

Hinweis: Diese Funktion hat keine vom Benutzer konfigurierbaren TCP-Einstellungen, die auf der NetScaler-Appliance deaktiviert/aktiviert werden können.

Weitere Informationen zur Unterstützung von Happy Eyeballs finden Sie unter RFC 6555.

NetScaler Videooptimierung

June 19, 2023

> **Warnung:**
>
> Die Videooptimierung wird nur für eine Forward-Proxy-Telco-Lösung unterstützt. Aktivieren Sie die Videooptimierung nicht für andere Anwendungsfälle. Die Videooptimierung wird auf Admin-Partitions- und Clustertopologien nicht unterstützt.

Die NetScaler-Appliance bietet Optimierungstechniken und Funktionen zur Optimierung des ABR-Videoverkehrs für Videoverkehr über Mobilfunknetze. Dies verbessert die Benutzererfahrung und reduziert den Gesamtverbrauch der Netzwerkbandbreite.

Der Abschnitt umfasst die folgenden Themen:

- Erste Schritte
- Lizenzierung
- Konfigurieren der Videooptimierung über TCP
- Konfiguration der Videooptimierung über UDP

Erste Schritte

May 11, 2023

Mediendateien haben zu einem zunehmenden Datenverkehr über Mobilfunknetze geführt, und die Migration zu schnelleren Netzwerktechnologien hat das Volumen des verschlüsselten Videoverkehrs

dramatisch erhöht. Die herkömmliche Technologie zur Medienbereitstellung (Progressive Download) bietet bei einer hohen Übertragungsrate keine akzeptable Erlebnisqualität (QoE). Dies hat zur Einführung des Adaptive Bit Rate (ABR) -Protokolls geführt. Es kann die Streaming-Bitrate an die verfügbare Netzwerkbandbreite anpassen und die Streaming-Qualität so einschränken, dass sie der Kapazität des Mobilteils entspricht, das das Video empfängt. Das ABR-Protokoll funktioniert jedoch in Mobilfunknetzen nicht so gut wie über das Internet. Mobilfunkbetreiber müssen daher den ABR-Verkehr optimieren.

Eine NetScaler-Appliance verfügt über einzigartige Funktionen zur Erkennung von eingehendem Videoverkehr und zur selektiven Optimierung von ABR-Videos.

So funktioniert die NetScaler-Videooptimierung

Eine NetScaler-Appliance kann verschlüsselten ABR-Verkehr (einschließlich Facebook-Videoverkehr) über TCP und YouTube-ABR-Verkehr über QUIC identifizieren und optimieren. Die Appliance verfügt über die folgenden Funktionen:

1. Erkennt Videos mit progressivem Download (PD) über HTTP.
2. Erkennen und optimieren Sie ABR-Videos über HTTP.
3. Erkennen und optimieren Sie ABR-Videos über HTTPS.
4. Erkennen und optimieren Sie YouTube-ABR-Videos über QUIC.

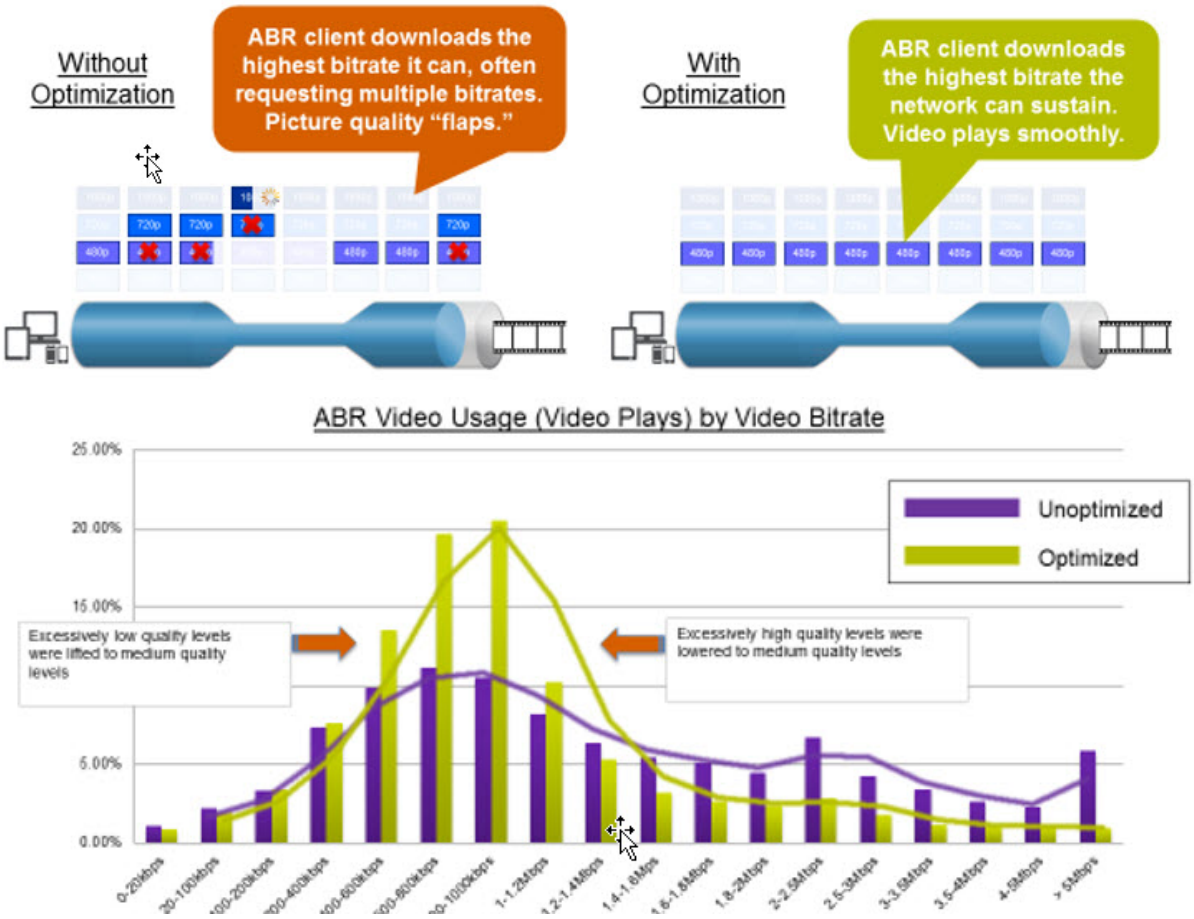
Außerdem verwendet die Appliance die folgenden Unterstützungsdomänen zur Erkennung von Videoverkehr über die TCP- und QUIC-Protokolle.

- Unverschlüsselte ABR-Videos über TCP. Die Appliance erkennt alle standardkonformen Video-Streaming-Websites. Die Appliance erkennt ABR-Sitzungen, indem sie den Payload-Header, die URL und die HTTP-Header des Antwortvideos überprüft.
- Verschlüsseltes ABR-Video über TCP. Die Appliance erkennt ABR-Sitzungen mithilfe eines generischen und heuristischen Algorithmus, der auf Domänen-, SSL-Header- und Verkehrsmustern basiert. Auf diese Weise verfügt die Appliance über eine integrierte Unterstützung zur Erkennung von Top-Video-Websites mit einer Genauigkeit von 95 Prozent, und wir fügen weiterhin Unterstützung für neue Videotypen hinzu. NetScaler verfügt auch über ein Programm zur zusätzlichen Überprüfung der am häufigsten verschlüsselten ABR-Websites für eine Region oder ein Land, um die Netzwerkabdeckung sicherzustellen.
- Verschlüsselte ABR-Videos über QUIC. Die Appliance erkennt ABR-Sitzungen für QUIC-basierte Videoanbieter wie YouTube. Der Erkennungsalgorithmus basiert auf einer Heuristik, die die QUIC-Header und die Domäne nutzt. NetScaler wird weiterhin Unterstützung für neuere Videoseiten hinzufügen, die QUIC verwenden.

Vorteile

Die Optimierung des ABR-Videoverkehrs kann die folgenden Vorteile bieten:

- Verwalten Sie das Netzwerk bei Überlastung in Spitzenzeiten.
- Verbessern Sie die Konsistenz der Videowiedergabe und reduzieren Sie Videoverzögerungen
- Aktivieren Sie neue Videodienstangebote (z. B. Binge-on-Videodienste).
- Ermöglichen Sie Kunden die Auswahl der besten nachhaltigen Videoqualität.
- Bieten Sie dem Abonnenten eine konsistente Benutzererfahrung.



Videooptimierung über TCP

Die NetScaler-Optimierung des ABR-Datenverkehrs über TCP funktioniert wie folgt:

1. HTTP- oder HTTPS-Verkehr, den die Appliance über TCP empfängt, wird an den entsprechenden virtuellen Load-Balancing-Server gesendet.
2. Die integrierten Erkennungsrichtlinien, die an den virtuellen Server gebunden sind, in Kombination mit anderen proprietären Erkennungsalgorithmen bewerten den Datenverkehr.
3. Die Richtlinien verwenden eine Reihe integrierter Videoerkennungssignaturen, um den Videotyp zu erkennen. Die Richtlinie, die den Traffic abgleicht, wendet eine Aktion an, die den Videotyp in einen der folgenden Kategorien einordnet:
   a) Klartext-PD

   b) Klartext-ABR
   c) Verschlüsseltes ABR
   d) Sonstiges
4. Die an denselben virtuellen Server gebundenen Optimierungsrichtlinien werten den Datenverkehr aus und bestimmen die Optimierungsbitrate, die auf den Verkehr angewendet werden soll.
5. Die Optimierungsbitrate wird angewendet, wenn es sich bei dem Datenverkehr entweder um Klartext-ABR oder um verschlüsseltes ABR handelt.

Ein Mobilfunkanbieter kann die Erlebnisqualität (QoE) verbessern, indem er die Download-Geschwindigkeit für 2G-, 3G- und 4G-Mobilfunkverkehr festlegt. Dies reduziert die Videostartzeiten oder Pufferereignisse. Durch die Optimierung kann auch die durch Videositzungen verbrauchte Netzwerkbandbreite reduziert werden.

Zu den Optimierungstechniken gehören dynamische Burst-Control und Zufallsstichproben.

Dynamische Burst-Steuerung

Die NetScaler ABR-Optimierung passt sich dynamisch an sich ändernde Netzwerkbedingungen an. Es ermöglicht eine anfängliche Burst-Rate, die das 1,3-fache der konfigurierten Taktrate für 15 Sekunden beträgt. Die anfängliche Burst-Rate gilt für den Beginn jeder optimierten ABR-Videositzung, auch wenn mehrere Sitzungen dieselbe TCP-Verbindung oder Gruppe von TCP-Verbindungen verwenden.

Die Appliance unterstützt auch Wiederherstellungs-Bursts für den Fall, dass die vom Netzwerk unterstützte Bitrate unter die konfigurierte Taktrate fällt. Wenn die effektive Bitrate beispielsweise in der 7. Sekunde sinkt und sich in der 15. Sekunde des ersten Burst-Zyklus erholt, gleicht die Appliance den Verlust während des nächsten Burst-Zyklus aus. Auf diese Weise optimiert die Appliance dynamisch die Netzwerkbandbreite für alle Abonnenten, sodass die Videoqualität pro Pixel konstant bleibt.

Hinweis: Wenn während eines ersten Bursts ein Wiederherstellungs-Burst auftritt, darf die Pacing-Bitrate die maximale Wiederherstellungs-Burst- und Initial-Burst-Rate nicht überschreiten (Sie dürfen den Wiederherstellungs-Burst-Faktor nicht zusätzlich zum anfänglichen Burst-Faktor hinzufügen). Andernfalls ist es möglicherweise so schnell, dass der Media Player in einen höheren Qualitätsmodus wechselt. Bei Bedarf können Sie jedoch die Dauer des Initial Burst verlängern, um die ungenutzte Bandbreite zu kompensieren.

Zufällige Stichprobe

Um die Einsparungen durch die Videooptimierung abzuschätzen, implementiert die NetScaler-Appliance Zufallsstichproben. Bei dieser Technik wählt die Appliance nach dem Zufallsprinzip einen konfigurierbaren Prozentsatz des erkannten Videoverkehrs aus (der Zufallsstichprobenparameter ist eine Ganzzahl zwischen 0 und 100, sodass weniger als 1 Prozent nicht möglich ist). Diese zufällig ausgewählten und nicht optimierten Transaktionen (und Sitzungen) werden zu einer Referenzgruppe,

und sie werden in den Transaktionsprotokollen identifiziert (zusammen mit anderen Merkmalen wie Bytegröße und Timerfeldern). Die Merkmale der optimierten Sitzungen werden ebenfalls protokolliert, und die Reporting Engine vergleicht die Statistiken der optimierten und der Referenzgruppen, um die Einsparungen durch die Optimierung abzuschätzen (einschließlich der Einsparungen durch die ABR-Optimierung).

Videooptimierung über UDP

Google hat ein neues Transportprotokoll namens QUIC eingeführt. Das QUIC-Protokoll von Google ist TCP+TLS+HTTP/2 sehr ähnlich und wird zusätzlich zu UDP implementiert. NetScaler kann YouTube-ABR-Videos erkennen, die über das QUIC-Protokoll gestreamt werden, und die ABR-Videooptimierung auf ähnliche Weise anwenden wie ABR über TCP.

Lizenzierung

May 11, 2023

Die Videooptimierungsfunktion funktioniert auf Telco-Plattformen mit dem Kauf einer CBM-Grundlizenz und einer CBM Premium-Lizenz. Für andere NetScaler-Plattformen funktioniert die Funktion mit dem Kauf einer CNS Premium-Lizenz. Bevor Sie die Videooptimierungsfunktion konfigurieren, muss Ihre Appliance über eine geeignete Lizenz verfügen.

Lizenzunterstützung für Telco-Plattformen:

- **cbm_Txxx_Server_Retail.lic**
- **cbm_Tpre_Server_Retail.lic**
- **CNS_WEBF_SSERVER_Retail.lic**

Wobei XXX der Durchsatz ist, zum Beispiel NetScaler T1000.

Lizenzunterstützung für andere NetScaler-Plattformen:

- **CNS_XXX_Server_PLT_Retail.lic**

Dabei ist XXX der Durchsatz.

Gehen Sie folgendermaßen vor, um eine Premium-Lizenzdatei hochzuladen:

1. Eine gültige Lizenzdatei sollte auf der NetScaler Appliance installiert werden. Die Lizenz sollte mindestens so viele Gbit/s unterstützen wie der erwartete maximale Gi-LAN-Durchsatz.

   Lizenzdateien sollten über einen SCP-Client in die /nsconfig/license der Appliance kopiert werden, wie in der Abbildung unten gezeigt.


```
> shell ls /nsconfig/license/
CNS_V3000_SERVER_PLT_Retail.lic ssl
<!--NeedCopy-->
```

2. Führen Sie einen Warmstart durch, um die neue Lizenz zu beantragen, wie in der Abbildung unten gezeigt.

```
> reboot -warm
Are you sure you want to restart NetScaler (Y/N)? [N]:y
 Done
<!--NeedCopy-->
```

3. Nachdem der Neustart abgeschlossen ist, stellen Sie sicher, dass die Lizenz ordnungsgemäß angewendet wurde, indem Sie die Show License CLI verwenden.

Im folgenden Beispiel wurde eine Premium-Lizenz mit Premium Edition erfolgreich installiert.

```
    > show license

                License status:

                                        Video Optimization: YES

                                                    ...

                                    Model Number ID: 110050

                                       License Type: Premium License
<!--NeedCopy-->
```

Konfigurieren der Videooptimierung über TCP

May 11, 2023

> **Warnung:**
>
> Im Rahmen der Videooptimierung ist die Video-Pacing-Funktionalität veraltet und wird in den kommenden Versionen von der NetScaler-Appliance entfernt.

Um den Videoverkehr über TCP zu optimieren, aktivieren Sie zunächst die Videooptimierungsfunktion. Die Appliance aktiviert dann die integrierten Erkennungsrichtlinien, um den eingehenden Videoverkehr zu erkennen und die Art des Videos zu identifizieren. Vom Benutzer konfigurierbare

Optimierungsrichtlinien für jeden Videotyp geben die Optimierungsbitrate an, die zur Optimierung des Datenverkehrs erforderlich ist.

Konfigurieren der Videooptimierung über TCP über die CLI

Um die Videooptimierung auf einer NetScaler-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben aus:

1. Aktivieren Sie die Videooptimierungsfunktion.
2. Fügen Sie virtuelle Server für den HTTP- und HTTPS-Verkehr hinzu.
3. Binden Sie alle integrierten Erkennungsrichtlinien an einen virtuellen Lastausgleichsserver für HTTP-Verkehr.
4. Binden Sie alle integrierten Erkennungsrichtlinien an einen virtuellen SSL-Bridge-Lastausgleichsserver für HTTPS-Verkehr.
5. Fügen Sie die gewünschten Optimierungsrichtlinien für HTTP- und HTTPS-Verkehr hinzu.
6. Binden Sie Optimierungsrichtlinien an einen virtuellen Lastausgleichsserver für den HTTP-Verkehr.
7. Binden Sie Optimierungsrichtlinien an einen virtuellen SSL-Bridge-Lastausgleichsserver für HTTPS-Verkehr.

Videooptimierung aktivieren

Wenn Sie möchten, dass die NetScaler-Appliance Videoverkehr erkennt, optimiert und meldet, müssen Sie die Funktion zur Videooptimierung aktivieren und die Optimierung auf ON setzen. Nachdem Sie die Funktion aktiviert haben, können Sie integrierte Erkennungsrichtlinien verwenden, um den eingehenden Videoverkehr zu identifizieren, und Sie können Optimierungsrichtlinien konfigurieren, um den verschlüsselten ABR-Verkehr zu optimieren. Um den ABR-Videoverkehr zu optimieren, müssen Sie die Download-Bitrate (auch als *Pacing-Rate*bezeichnet) konfigurieren.

Sie müssen auch die Lastausgleichsfunktion aktivieren, und wenn Sie die Videooptimierung für den HTTPS-Verkehr verwenden möchten, müssen Sie die SSL-Funktion aktivieren.

So aktivieren Sie die Videooptimierungsfunktion

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
enable ns feature VideoOptimization
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn Sie die Leistung der Videooptimierung und die Video-Insight-Berichte überwachen

> möchten, müssen Sie die AppFlow-Funktion aktivieren und dann auf die Video Analytics-Funktion in NetScaler Application Delivery Management (ADM) zugreifen. Weitere Informationen finden Sie in der Video Insight-Dokumentation .

Erstellen von virtuellen Servern für HTTP- und HTTPS-Videoverkehr

Eine NetScaler-Appliance verwendet verschiedene virtuelle Server, um die verschiedenen Arten des eingehenden Videoverkehrs zu erkennen und zu optimieren. Die Appliance unterstützt die folgenden Arten von virtuellen Servern für TCP-Verkehr.

- **Virtueller HTTP-Lastausgleichsserver**. Zur Erkennung von HTTP-Videoverkehr verwendet die Appliance einen virtuellen HTTP-Lastausgleichsserver. Es verwaltet HTTP-Videoanfragen, die die Appliance von Clients erhält.
- **Virtueller SSL-Bridge-Loadbalancing-Server**. Um verschlüsselten Videoverkehr zu erkennen, müssen Sie einen virtuellen SSL-Bridge-Server auf der Appliance konfigurieren.

So fügen Sie einen virtuellen HTTP-Lastausgleichsserver zum Erkennen von HTTP-Videoverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> HTTP * 80 -persistenceType NONE
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver ProxyVserver-HTTP HTTP * 80 -persistenceType NONE -
   cltTimeout 120
<!--NeedCopy-->
```

So fügen Sie einen virtuellen SSL Bridge-Server zur Erkennung von HTTPS-Videoverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> SSL_BRIDGE * 443 -persistenceType NONE
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver ProxyVserver-SSL SSL_BRIDGE * 443 -persistenceType NONE
   -cltTimeout 180
<!--NeedCopy-->
```


Binden integrierter Erkennungsrichtlinien an einen virtuellen HTTP-Lastausgleichsserver

Um Videoverkehr über eine HTTP-Verbindung zu erkennen, müssen Sie alle integrierten Erkennungsrichtlinien an einen virtuellen Lastausgleichsserver binden. Sie müssen die Richtlinien je nach Richtlinientyp entweder an die Anforderungs- oder Antwortzeitverarbeitung binden.

> **Hinweis:**
>
> Die Richtlinie zur `ns_videoopt_http_body_detection` Videooptimierung unterstützt die `CONNECT` HTTP-Anforderungsmethode nicht.

So binden Sie Erkennungsrichtlinien für verschiedene Videotypen an einen virtuellen HTTP-Lastausgleichsserver

Geben Sie an der Eingabeaufforderung den entsprechenden Befehl für jeden Typ ein. Die verfügbaren Befehle sind:

```
bind lb vserver <name> -policyName ns_videoopt_http_abr_netflix -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_netflix2 -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube2  -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>   -policyName ns_videoopt_http_pd_youtube3 -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>  -policyName ns_videoopt_http_abr_generic -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix -priority 400  type RESPONSE

```



```
bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix2 -priority 500 -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_youtube -priority 600  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube -priority 800  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube2 -priority 900 -type RESPONSE

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_pd_youtube3 -priority 1000 -type REQUEST

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_abr_generic -priority 1100 -type RESPONSE
<!--NeedCopy-->
```

Binden der Richtlinie zur Erkennung von HTTP-Body-Inhalten an den virtuellen Load Balancing

Um Videoverkehr über HTTP zu erkennen, müssen Sie die Richtlinie zur Erkennung von Textinhalten an den virtuellen Lastausgleichsserver binden. Sie können den folgenden Befehl verwenden:

```
bind lb vserver <name> -policyName ns_videoopt_http_body_detection -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-HTTP -policyName
    ns_videoopt_http_body_detection -priority 1500 -type REQUEST
<!--NeedCopy-->
```

Binden integrierter Erkennungsrichtlinien an einen virtuellen SSL-Bridge-Load Balancing Server

Um den Videoverkehr über eine HTTPS-Verbindung zu erkennen, müssen Sie integrierte Erkennungsrichtlinien an einen virtuellen SSL Bridge-Lastenausgleichsserver binden.

So binden Sie eine Erkennungsrichtlinie an einen virtuellen SSL-Bridge-Lastausgleichsserver

Geben Sie an der Eingabeaufforderung den entsprechenden Befehl für jeden Typ ein. Die verfügbaren Befehle sind:

```
bind lb vserver <name> -policyName ns_videoopt_https_abr_netflix -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_youtube -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_generic -
    priority <positive_integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_netflix -priority 120 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_youtube -priority 140 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_generic -priority 150 -type REQUEST
<!--NeedCopy-->
```

Hinzufügen von Optimierungsrichtlinien für das Pacing von ABR-Verkehr

Um den ABR-Verkehr zu optimieren, müssen Sie Optimierungsrichtlinien und die zugehörigen Aktionen konfigurieren. Anschließend binden Sie die Richtlinien an dieselben virtuellen Lastausgleichsserver, an die Sie die Erkennungsrichtlinien gebunden haben. Erstellen Sie für jede Richtlinie zuerst die Aktion, damit Sie sie beim Erstellen der Richtlinie einbeziehen können.

So fügen Sie eine Optimierungsaktion hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add videooptimization pacingaction <action Name> -rate <integer> [-
    comment <string>]
<!--NeedCopy-->
```

Wobei der **Ratenparameter** die Rate in Kbit/s angibt, mit der der Verkehr gesendet werden soll (die Schrittgeschwindigkeit).

Beispiel:

```
add videooptimization pacingaction MyOptAct2000 -rate 2000
<!--NeedCopy-->
```

So fügen Sie eine Optimierungsrichtlinie hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add videooptimization pacingpolicy <name> -rule <expression> -action <
   string>
<!--NeedCopy-->
```

Beispiel:

```
add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
   MyOptAct2000
<!--NeedCopy-->
```

Binden von Optimierungsrichtlinien an einen virtuellen HTTP-Lastausgleichsserver

Um den ABR-Videoverkehr über eine HTTP-Verbindung zu optimieren, müssen Sie die Optimierungsrichtlinien an einen virtuellen Lastausgleichsserver binden, an den die Erkennungsrichtlinien gebunden sind.

So binden Sie eine Optimierungsrichtlinie an einen virtuellen Load Balancing-Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind lb vserver <name> -policyName <policy_name> -priority <
   positive_integer> -type  (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-HTTP -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```


Binden von Optimierungsrichtlinien an virtuelle SSL-Bridge-Server

Um den ABR-Videoverkehr über eine HTTPS-Verbindung zu optimieren, müssen Sie die Optimierungsrichtlinien an den virtuellen SSL Bridge-Server binden, an den die integrierten Erkennungsrichtlinien gebunden sind.

So binden Sie eine Optimierungsrichtlinie an den virtuellen SSL Bridge-Server, um verschlüsselten Datenverkehr zu übertragen

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type  (REQUEST |RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-SSL -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```

Festlegen der Schrittparameter für die Videooptim

Mit der CLI können Sie die Schrittparameter für die Videooptimierung festlegen, z. B. den Prozentsatz der zufälligen Abtastung.

So stellen Sie den Prozentsatz der zufälligen Stichprobe ein

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set videooptimization parameter  - RandomSamplingPercentage <realNumber>
<!--NeedCopy-->
```

Wo ist eine RealNumber ein Wert zwischen 0,0 und 100,0.

Beispiel:

```
set videooptimization parameter -RandomSamplingPercentage 50
<!--NeedCopy-->
```

Konfigurieren der Videooptimierung über TCP über die GUI

Mit der GUI können Sie:

- Aktivieren Sie die Videooptimierungsfunktion.
- Erstellen Sie einen virtuellen HTTP-Lastausgleichsserver.
- Erstellen Sie einen virtuellen SSL-Bridge-Lastausgleichsserver.
- Binden Sie integrierte Erkennungsrichtlinien an den virtuellen HTTP-Lastausgleichsserver.
- Binden Sie integrierte Erkennungsrichtlinien an den virtuellen SSL-Bridge-Load Balancing Server.
- Erstellen Sie eine Optimierungsrichtlinie.
- Erstellen Sie eine Optimierungsaktion.
- Konfigurieren des Optimierungsschrittparameters.
- Binden Sie die Optimierungsrichtlinie an den virtuellen Lastausgleichsserver für den HTTP-Verkehr.
- Binden Sie die Optimierungsrichtlinie an den virtuellen SSL-Bridge-Lastausgleichsserver für HTTPS-Verkehr.

So aktivieren Sie die Videooptimierungsfunktion

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf den Link **Erweiterte Funktionen konfigurieren** .
3. Aktivieren Sie auf der Seite **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **Videooptimierung** .
4. Klicken Sie auf **OK**und dann auf **Schließen**.

So erstellen Sie einen virtuellen Lastausgleichsserver für den HTTP-Verkehr

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf dem Bildschirm Load Balancing Virtual Server die folgenden Parameter ein:
   a) **Name**. Name des virtuellen Lastausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als HTTP
   c) **Typ der IP-Adresse**. IP-Adresstyp: IPv4 oder IPv6.
   d) **IP-Adresse**. IPv4- oder IPv6-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Hafen**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So erstellen Sie einen virtuellen Lastausgleichsserver für den HTTPS-Verkehr

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf dem Bildschirm **Load Balancing Virtual Server** die folgenden Parameter ein:
   a) **Name**. Name des virtuellen Lastausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als SSL-Bridge.
   c) **Typ der IP-Adresse**. IP-Adresstyp: IPv4 oder IPv6.
   d) **IP-Adresse**. IPv4- oder IPv6-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Hafen**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

So binden Sie eine integrierte Erkennungsrichtlinie an einen virtuellen Lastausgleichsserver

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Wählen Sie im Detailbereich den virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
   a) Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
   b) Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
   c) Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.
   d) Wählen Sie Richtlinie aus. Wählen Sie in der Dropdownliste eine Richtlinie zur Erkennung von Videooptimierungen aus.
   e) Wählen Sie Typ. Wählen Sie den Richtlinientyp als Anforderung aus.
   f) Klicken Sie auf **Weiter**.
3. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus und klicken Sie auf **Schließen**.

So binden Sie eine integrierte Erkennungsrichtlinie an einen virtuellen SSL-Bridge-Lastausgleichsserver

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Wählen Sie im Detailbereich den virtuellen SSL-Bridge-Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.

4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.
   a) Wählen Sie Richtlinie aus. Wählen Sie in der Dropdownliste die Richtlinie zur Erkennung der Videooptimierung aus.
   b) Wählen Sie Typ. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus und klicken Sie auf **Schließen**.

So erstellen Sie eine Videooptimierungsaktion

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > ****Videooptimierung**** > **Pacing** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Schrittaktion zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsaktion.
   b) **ABR-Optimierungsrate (Kbps).** Tempo, mit der der ABR-Videoverkehr gesendet werden soll. Die Standardrate für die ABR-Optimierung beträgt 1000 Kbit/s. Der Mindestwert ist 1, und der Maximalwert ist 2147483647.
   c) **Kommentar**. Eine kurze Beschreibung der Aktion.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So erstellen Sie eine Richtlinie zur Videooptimierung

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > ****Videooptimierung**** > **Tempo** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Schrittrichtlinie zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsrichtlinie
   b) **Expression.** Benutzerdefinierte Regex-Ausdrücke, die die Richtlinie implementieren.
   c) **Aktion**. Optimierungsaktion im Zusammenhang mit der Richtlinie zur Handhabung des eingehenden Videoverkehrs.
   d) **UNDEF-Aktion.** Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
   e) **Kommentar**. Eine kurze Beschreibung der Richtlinie.
   f) **Aktion protokollieren.** Wählen Sie die Überwachungsprotokollaktion aus, mit der die gewünschten Protokollmeldungen erstellt werden.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen.**

So stellen Sie Schrittparameter für die Videooptimierung ein

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung**.
2. Klicken Sie auf der Seite **Videooptimierung** auf den Link **Einstellungen für die Videooptimierung ändern** .
3. Stellen Sie auf der Seite **Videooptimierungseinstellungen** den folgenden Parameter ein.
   a) **Prozentsatz der Zufallsstichprobe (%)**. Prozentsatz der für die Zufallsstichprobe ausgewählten Pakete.
4. Klicken Sie auf **OK** und auf **Schließen**.

So binden Sie eine Richtlinie zur Videooptimierung an einen virtuellen HTTP-Lastausgleichsserver

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung**.
2. Klicken Sie auf der Seite **Videooptimierung** auf den Link **Richtlinien-Manager für Videooptimierung Pacing** .
3. Stellen Sie die folgenden Parameter ein.
   a) **Bind-Punkt**. Der Punkt, an dem die Optimierungsrichtlinie während der Anforderungs- oder Antwortverarbeitung angewendet werden soll.
   b) **Art der Verbindung**. Verbindungstyp als Anfrage oder Antwort.
   c) **Virtueller Server**. Der virtuelle Lastausgleichsserver, an den die Richtlinie gebunden werden soll.
   d) Klicken Sie auf **Weiter**.
4. Führen Sie im Abschnitt **Punkt binden** einen der folgenden Schritte aus:
   a) Wählen Sie eine Richtlinie aus der Liste aus.
   b) Klicken Sie auf **Bindung hinzufügen**, um auf den Schieberegler **Richtlinien** zuzugreifen.
      i. Wählen Sie eine bestehende Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu.
      ii. Geben Sie verbindliche Details ein und klicken Sie auf **Binden**.
5. Klicken Sie auf **Schließen**.

So binden Sie eine Richtlinie zur Videooptimierung an einen virtuellen SSL-Bridge-Lastausgleichsserver

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > ****Videooptimierung****.
2. Klicken Sie auf der Seite **Videooptimierung** auf den Link **Richtlinien-Manager für Videooptimierung Pacing** .

3. Legen Sie auf der Seite **Richtlinien-Manager für die Videooptimierung** die folgenden Parameter fest.
   a) Bind-Punkt. Der Punkt, an dem die Optimierungsrichtlinie während der Anforderungs-/Antwortverarbeitung angewendet werden soll.
   b) Art der Verbindung. Verbindungstyp als Anfrage oder Antwort.
   c) Virtueller Server. Der virtuelle SSL-Bridge-Lastausgleichsserver, an den die Richtlinie gebunden werden soll.
4. Klicken Sie auf **Weiter**.
5. Führen Sie im Abschnitt **Punkt binden** einen der folgenden Schritte aus:
   a) Wählen Sie eine Richtlinienbindung aus der Liste aus.
   b) Klicken Sie auf **Bindung hinzufügen**, um auf den Schieberegler **Richtlinien** zuzugreifen.
      i. Wählen Sie eine bestehende Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu.
      ii. Geben Sie verbindliche Details ein und klicken Sie auf **Binden**.
6. Klicken Sie auf **Schließen**.

Konfiguration der Videooptimierung über UDP

May 11, 2023

Um den QUIC-ABR-Videoverkehr über UDP zu optimieren, aktivieren Sie zunächst die Videooptimierungsfunktion. Nachdem Sie die Konfiguration abgeschlossen haben, erkennt die Appliance QUIC-basierten ABR-Videoverkehr und wendet die auf der Appliance konfigurierte Optimierungsbitrate an.

Konfiguration der Videooptimierung für QUIC mithilfe der CLI

Um die Videooptimierung für QUIC-Videoverkehr über UDP zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie die Videooptimierung.
2. Erstellen Sie einen QUIC-Dienst.
3. Erstellen Sie einen virtuellen QUIC-Load-Balancing-Server.
4. Binden Sie den QUIC-Webdienst an den virtuellen Loading-Balancing-Server.
5. Erstellen Sie eine Richtlinie zur Videooptimierung für das Tempo des QUIC-basierten UDP-Datenverkehrs.
6. Binden Sie die Optimierungsrichtlinie an einen QUIC-basierten virtuellen Lastausgleichsserver.

Aktivierung der Videooptimierung für QUIC-Verkehr

Wenn Sie möchten, dass die NetScaler-Appliance Video-Traffic erkennt, optimiert und meldet, müssen Sie die Videooptimierungsfunktion aktivieren und die Optimierung aktivieren.

> **Hinweis**
>
> Wenn Sie die Videooptimierung für QUIC-Verkehr verwenden möchten, müssen Sie die Funktionen Load Balancing und AppFlow aktivieren.

Um die Videooptimierung zu aktivieren

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
enable ns feature VideoOptimization
<!--NeedCopy-->
```

Einen Dienst für QUIC-Verkehr erstellen

Eine NetScaler-Appliance verwendet einen QUIC-Dienst für den virtuellen Lastausgleichsserver, um im statischen Routing-Modus eine Verbindung zum Ausgangsrouter herzustellen.

> **Hinweis**
>
> Derzeit wird dynamisches Routing nicht unterstützt.

So erstellen Sie einen Load-Balancing-Webdienst für QUIC-Videoverkehr

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <router-IP> <serviceType> <port> -usip yes -
   useproxyport  [yes | no]
<!--NeedCopy-->
```

Beispiel:

```
add service svc-quic 10.102.29.200 QUIC 443  -usip yes  -useproxyport
   no

where IP address is the internet router address.
<!--NeedCopy-->
```


Einen virtuellen Lastausgleichsserver für QUIC-Verkehr erstellen

Eine NetScaler-Appliance verwendet einen virtuellen Lastausgleichsserver, um QUIC-Videoverkehr über UDP zu erkennen und zu optimieren.

So erstellen Sie einen virtuellen Lastausgleichsserver für QUIC-Videoverkehr

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port> -m MAC
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vs-quic QUIC * 443 -persistenceType NONE -m MAC -
    cltTimeout 120
<!--NeedCopy-->
```

Binden eines QUIC-Webdienstes an den virtuellen Load Balancing-Server

Nachdem Sie die Webdienste und den virtuellen Lastausgleichsserver für den QUIC-Verkehr erstellt haben, müssen Sie die Dienste an den virtuellen Server binden.

Um einen Webdienst an einen virtuellen Lastausgleichsserver für QUIC-Videoverkehr zu binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver vs-quic svc-quic
<!--NeedCopy-->
```

Erstellung einer Videooptimierungsrichtlinie für QUIC-basierten UDP-Verkehr

Um den QUIC-basierten UDP-Verkehr zu optimieren, müssen Sie die Richtlinien für das Optimierungstempo und die zugehörigen Aktionen konfigurieren. Anschließend müssen Sie die Richtlinien an QUIC-basierte virtuelle Load-Balancing-Server binden. Erstellen Sie für jede Richtlinie zunächst eine Aktion, damit Sie sie der Richtlinie zuordnen können.

So fügen Sie eine Optimierungsaktion hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add videooptimization pacingaction <action Name> -rate <integer> [-
     comment <string>]
2 <!--NeedCopy-->
```

Wobei der **Rate-Parameter** die Geschwindigkeit in Kbit/s angibt, mit der der Datenverkehr gesendet werden soll (die Pacing-Rate).

Beispiel:

```
1 set videooptimization parameter -QUICPacingRate 1000
2 <!--NeedCopy-->
```

wobei 1000 die gewünschte Taktrate in KBit/s darstellt.

So fügen Sie eine Optimierungsrichtlinie hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add videooptimization pacingpolicy <name> -rule <expression> -action <
     string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
     MyOptAct2000
2 <!--NeedCopy-->
```

Binden von Optimierungsrichtlinien an einen virtuellen QUIC Load Balancing-Server

Um den QUIC-Videoverkehr über eine UDP-Verbindung zu optimieren, müssen Sie die Optimierungsrichtlinien an einen virtuellen QUIC-Load-Balancing-Server binden.

So binden Sie eine Optimierungsrichtlinie an einen virtuellen QUIC Load Balancing-Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 bind lb vserver <name> -policyName <policy_name> -priority <
     positive_integer> -type (REQUEST)
2 <!--NeedCopy-->
```


> **Hinweis**
>
> Die Pacing-Richtlinien müssen nur zur Anforderungszeit an einen virtuellen QUIC-Load-Balancing-Server gebunden sein.

Beispiel:

```
bind lb vserver vs-quic -policyName myOptPolicy2000 -priority 3400 -
    type  REQUEST
<!--NeedCopy-->
```

Konfiguration der Videooptimierung für QUIC mithilfe der GUI

Um die Funktion auf der Appliance über die GUI zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Videooptimierung aktivieren
2. Konfiguration eines QUIC-Servers
3. QUIC-Dienst konfigurieren
4. Konfigurieren Sie einen virtuellen QUIC-Load-Balancing-Server
5. Binden Sie den QUIC-Webdienst an den virtuellen Load-Balancing-Server
6. Erstellen Sie eine Optimierungsrichtlinie.
7. Erstellen Sie eine Optimierungsaktion.
8. Konfigurieren des Optimierungsschrittparameters.
9. Binden Sie die Optimierungsrichtlinie an den virtuellen Lastausgleichsserver für QUIC-Verkehr.

Um die Videooptimierung zu aktivieren

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**System > Einstellungen**.**
2. Wählen Sie auf der Detailseite den Link **Erweiterte Funktionen konfigurieren** aus.
3. Aktivieren Sie auf der Seite **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **Videooptimierung** .

Um einen QUIC-Server zu erstellen

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Servers** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Server erstellen** die folgenden Parameter ein:
   a) Name. Name des QUIC-Servers.
   b) IP-Adresse. IP-Adresse des QUIC-Servers

c) Verkehrsdomäne. Domainname des Servers.
d) Aktivierung nach dem Erstellen. Ausgangszustand des Servers.
e) Kommentare. Kurze Informationen über den Server.

4. Klicken Sie auf **Erstellen.**

Um einen QUIC-Dienst zu erstellen

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Services**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Load Balancing Service** die folgenden Parameter ein:
   a) **Name des Dienstes**. Name des QUIC-Dienstes.
   b) **IP-Adresse**. Dem QUIC-Dienst zugewiesene IP-Adresse.
   c) **Protokoll**. Wählen Sie das Protokoll als QUIC aus.
   d) **Hafen**. Portnummer des Webdienstes.
4. Klicken Sie auf **OK**, um fortzufahren. Sie können dann andere optionale Parameter konfigurieren. Weitere Informationen finden Sie unter Dienste konfigurieren.
5. Nachdem Sie die optionalen Parameter konfiguriert haben, klicken Sie auf **OK** und **Schließen** .

So erstellen Sie einen virtuellen Lastausgleichsserver

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Load Balancing Virtual Server** die folgenden Parameter ein:
   a) **Name**. Name des virtuellen Lastausgleichsservers.
   b) **Protokoll**. Das vom Dienst zum Senden von QUIC-Anfragen verwendete Protokoll.
   c) Typ der IP-Adresse. IP-Adresstyp: IPv4 oder IPv6.
   d) **IP-Adresse**. Dem virtuellen Server zugewiesene IP 4- oder IP6-IP-Adresse.
   e) **Hafen**. Portnummer des virtuellen Servers.
4. Klicken Sie auf OK, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.

So binden Sie einen virtuellen Lastausgleichsserver an einen QUIC-Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und wählen Sie einen virtuellen Server aus.
2. Klicken Sie auf **Dienste und Dienstgruppen**, um das Fenster **Load Balancing Virtual Server Service Binding** aufzurufen.
3. Wählen Sie einen QUIC-basierten Webdienst aus und klicken Sie auf **Binden**.

4. Klicken Sie auf **Fertig**.

So binden Sie einen virtuellen Lastausgleichsserver an einen QUIC-Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und wählen Sie einen virtuellen Server aus.
2. Klicken Sie auf **Dienste und Dienstgruppen** , um das Fenster **Load Balancing Virtual Server Service Binding** aufzurufen.
3. Wählen Sie einen QUIC-basierten Webdienst aus und klicken Sie auf **Binden**.
4. Klicken Sie auf **Fertig**.

So erstellen Sie eine Videooptimierungsaktion für QUIC-Verkehr

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > ****Videooptimierung**** > **Pacing** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Schrittaktion zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsaktion.
   b) **ABR-Optimierungsrate (Kbps).** Tempo, mit der der ABR-Videoverkehr gesendet werden soll. Die Standardrate für die ABR-Optimierung beträgt 1000 Kbit/s. Der Mindestwert ist 1, und der Maximalwert ist 2147483647.
   c) **Kommentar**. Eine kurze Beschreibung der Aktion.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So erstellen Sie eine Richtlinie zur Videooptimierung für QUIC-Verkehr

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > ****Videooptimierung**** > **Tempo** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Schrittrichtlinie zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) Name. Name der Optimierungsrichtlinie
   b) Expression. Benutzerdefinierte Regrex-Ausdrücke, die die Richtlinie implementieren.
   c) Aktion. Optimierungsaktion im Zusammenhang mit der Richtlinie zur Handhabung des eingehenden Videoverkehrs.
   d) UNDEF-Aktion. Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
   e) Kommentar. Eine kurze Beschreibung der Richtlinie.
   f) Aktion protokollieren. Wählen Sie die Überwachungsprotokollaktion aus, mit der die gewünschten Protokollmeldungen erstellt werden.

4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So binden Sie eine Videooptimierungsrichtlinie an einen virtuellen QUIC-Load-Balancing-Server

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > ****Videooptimierung****.
2. Klicken Sie auf der Seite **Videooptimierung** auf den Link **Richtlinien-Manager für Videooptimierung Pacing** .
3. Legen Sie auf der Seite **Richtlinien-Manager für die Videooptimierung** die folgenden Parameter fest.
   a) Bind-Punkt. Der Punkt, an dem die Optimierungsrichtlinie während der Anforderungsverarbeitung angewendet werden soll. **Hinweis**: Die Pacing-Richtlinien dürfen nur zur Anforderungszeit an einen virtuellen QUIC-Load-Balancing-Server gebunden sein.
   b) Art der Verbindung. Verbindungstyp als Anfrage oder Antwort.
   c) Virtueller Server. Der virtuelle Lastausgleichsserver, an den die Richtlinie gebunden werden soll.
4. Klicken Sie auf **Weiter**.
5. Führen Sie im Abschnitt **Punkt binden** einen der folgenden Schritte aus:
   a) Wählen Sie eine Richtlinie aus der Liste aus.
   b) Klicken Sie auf **Bindung hinzufügen**, um auf den Schieberegler **Richtlinien** zuzugreifen.
      i. Wählen Sie eine bestehende Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu.
      ii. Geben Sie verbindliche Details ein und klicken Sie auf **Binden**.
6. Klicken Sie auf **Schließen**.

NetScaler URL-Filterung

August 15, 2023

> **Hinweis:**
>
> Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

Die URL-Filterung ermöglicht eine richtlinienbasierte Kontrolle von Websites, indem die in URLs enthaltenen Informationen verwendet werden. Diese Funktion hilft Netzwerkadministratoren, den Benutzerzugriff auf bösartige Websites in Mobilfunknetzen zu überwachen und zu kontrollieren.

Als Administrator können Sie eine URL-Filterrichtlinie mithilfe der URL-Kategorisierungsfunktion oder der URL-Liste konfigurieren.

URL-Liste. Steuert den Zugriff auf Websites und Webseiten auf der schwarzen Liste, indem der Zugriff auf URLs blockiert wird, die in einem in die Appliance importierten URL-Satz enthalten sind.

URL-Kategorisierung. Steuert den Zugriff auf Websites und Webseiten, indem der Datenverkehr basierend auf einer vordefinierten Liste von Kategorien gefiltert wird.

URL-Liste

August 15, 2023

Mit der URL-Listenfunktion können Sie den Zugriff auf benutzerdefinierte URL-Listen (bis zu einer Million Einträge) steuern. Die Funktion filtert Websites, indem eine URL-Filterrichtlinie angewendet wird, die an einen virtuellen Server gebunden ist.

Als Administrator müssen Sie die URL-Liste in die NetScaler-Appliance importieren. Diese importierte Liste wird intern als Richtliniendatensatz gespeichert, der als *URL-Satz*bezeichnet wird. Die Appliance wendet dann einen einzigartigen Algorithmus für den schnellen URL-Abgleich auf die eingehenden URL-Anfragen an. Wenn die eingehende URL-Anfrage mit einem Eintrag im Set übereinstimmt, wendet die Appliance die zugehörige Richtlinienaktion an, um den Zugriff zu kontrollieren.

Typen von URL-Listen

Jeder Eintrag in einem URL-Satz kann eine URL und optional die zugehörigen Metadaten (URL-Kategorie, Kategoriegruppen oder andere verwandte Daten) enthalten. Bei URLs mit Metadaten verwendet die Appliance einen Richtlinienausdruck, der die Metadaten auswertet. Weitere Informationen finden Sie unter URL-Sets.

Benutzerdefinierte URL-Liste. Sie können einen benutzerdefinierten URL-Satz mit bis zu 1.000.000 URL-Einträgen erstellen und ihn als Textdatei in Ihre Appliance importieren. Die Liste kann URLs mit oder ohne Metadaten enthalten (was einer URL-Kategorie ähneln könnte). Die NetScaler-Plattform erkennt automatisch, ob Metadaten vorhanden sind. Es unterstützt auch das sichere Speichern der importierten Listen. Weitere Informationen finden Sie unter URL-Set.

Sie können die URL-Liste hosten und die NetScaler Appliance so konfigurieren, dass die Liste regelmäßig aktualisiert wird, ohne dass ein manueller Eingriff erforderlich ist. Sobald die URL-Liste aktualisiert wurde, kann die Appliance die Metadaten und Kategorien automatisch erkennen, indem sie Richtlinienausdrücke verwendet, um jede eingehende URL auszuwerten und dann Aktionen wie Zulassen, Blockieren, Umleiten oder Benachrichtigen des Benutzers anzuwenden.

Richtlinienausdrücke für URL-Listen

In der folgenden Tabelle werden die grundlegenden Ausdrücke beschrieben, die Sie zur Bewertung des eingehenden Datenverkehrs verwenden können. Nachdem Sie eine URL-Liste in die Appliance importiert haben, wird sie als *URL-Set*bezeichnet.

Ausdruck	Vorgang
<URL expression>.URLSET_MATCHES_ANY (<URLSET>)	Wird mit TRUE ausgewertet, wenn die URL genau mit einem Eintrag im URL-Satz übereinstimmt.
<URL expression>. GET_URLSET_METADATA(<URLSET>)	Der Ausdruck GET_URLSET_METADATA () gibt die zugehörigen Metadaten zurück, wenn die URL genau mit einem Muster innerhalb des URL-Sets übereinstimmt. Eine leere Zeichenfolge wird zurückgegeben, wenn es keine Übereinstimmung gibt.
<URL expression>.GET_ URLSET_METADATA(<URLSET>).EQ(< METADATA>)	Wird mit TRUE ausgewertet, wenn die übereinstimmenden Metadaten gleich sind. <METADATA>
<URLexpression>.GET_URLSET_METADATA (<URLSET>).TYPECAST_LIST_T(‘,’).GET (0).EQ(<CATEGORY>)	Wird mit TRUE ausgewertet, wenn sich die übereinstimmenden Metadaten am Anfang der Kategorie befinden. Dieses Muster kann verwendet werden, um separate Felder innerhalb von Metadaten zu kodieren, aber nur für das 1st Feld.
HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL)	Verbindet die Host- und URL-Parameter, die dann als<URL expression> Abgleich verwendet werden können.

Richtlinienaktionen für URL-Listen

Die gängigste Durchsetzungsmaßnahme für URLs, die einer URL-Liste entsprechen, ist die Beschränkung des Zugriffs. Erstellen Sie eine URL-Listenrichtlinie mit einem Ausdruck, der der gewünschten URL-Liste entspricht, und einer Durchsetzungsmaßnahme. Die Verwendung der Richtliniengruppe hängt vom Typ des eingehenden Datenverkehrs (HTTP oder HTTPS) und dem auf der Appliance konfigurierten virtuellen Server ab. Sie können eine Responder-Richtlinie für HTTP-Verkehr oder eine Videooptimierungsrichtlinie für HTTPS-Verkehr verwenden. Geben Sie Aktionen an, die auf die URLs angewendet werden sollen, die den Ausdrücken in den Richtlinien entsprechen. In der folgenden Tabelle sind die verfügbaren Aktionen aufgeführt.

Action-Typ	Richtlinie	Beschreibung
ALLOW	Responder	Erlauben Sie der Anfrage, auf die Ziel-URL zuzugreifen.
REDIRECT	Responder	Leitet die Anfrage an die als Ziel angegebene URL weiter.
DENY	Responder	Lehnen Sie die Anfrage ab.
RESET	Responder, Videooptimierung	Setzt die Verbindung zurück.
DROP	Responder, Videooptimierung	Trennen Sie die Verbindung.

Voraussetzungen

Um die URL-Listenfunktion zu konfigurieren, stellen Sie sicher, dass Sie den folgenden Server konfiguriert haben.

DNS-Server für DNS-Anfragen

Sie müssen einen DNS-Server konfigurieren, wenn Sie einen URL-Satz aus einer Hostnamen-URL importieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state (
    ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
<!--NeedCopy-->
```

Beispiel:

```
add dns nameServer 10.140.50.5
<!--NeedCopy-->
```

Importieren einer benutzerdefinierten URL-Liste

Informationen zum Importieren eines URL-Sets finden Sie unter Thema “URL-Sets” .

Konfigurieren einer URL-Liste für HTTP-Datenverkehr

Die NetScaler-Appliance unterstützt HTTP- und HTTPS-Verkehr. Gehen Sie wie folgt vor, um einen virtuellen Lastausgleichsserver für HTTP-Verkehr zu konfigurieren und URL-Listenrichtlinien an den Server zu binden:

- Fügen Sie URL-Listenaktionen hinzu.
- Fügen Sie URL-Listenrichtlinien hinzu.
- Fügen Sie einen virtuellen HTTP-Load-Balancing-Server für HTTP-Verkehr hinzu
- Binden Sie die URL-Listenrichtlinien an den virtuellen HTTP-Load-Balancing-Server für HTTP-Verkehr

So fügen Sie eine URL-Listenaktion hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
    string>]
<!--NeedCopy-->
```

So fügen Sie einen virtuellen HTTP-Load-Balancing-Server für HTTP-Verkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
    imeout <secs>]
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout
    120
<!--NeedCopy-->
```

Um die URL-Listenrichtlinie an den virtuellen HTTP-Load-Balancing-Server zu binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Konfiguration der URL-Liste für HTTPS-Verkehr

Die NetScaler-Appliance unterstützt HTTP- und HTTPS-Verkehr. Gehen Sie wie folgt vor, um einen virtuellen SSL-Bridge-Load-Balancing-Server für HTTPS-Verkehr zu konfigurieren und URL-Listenrichtlinien an den Server zu binden:

- Fügen Sie URL-Listenaktionen hinzu.
- Fügen Sie URL-Listenrichtlinien hinzu.
- Fügen Sie einen virtuellen SSL-Bridge-Load-Balancing-Server für HTTP-Verkehr hinzu
- Binden Sie die URL-Listenrichtlinien an den virtuellen SSL-Bridge-Load-Balancing-Server für HTTP-Verkehr

So fügen Sie eine URL-Listenrichtlinie für HTTPS-Verkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add videooptimization detectionpolicy <name> -rule <expression> -action
      <string> [-undefAction <string>] [-comment <string>] [-logAction <
     string>]
2 <!--NeedCopy-->
```

So fügen Sie einen virtuellen SSL-Bridge-Load-Balancing-Server hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
     imeout <secs>]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -
     cltTimeout 180
2 <!--NeedCopy-->
```

So binden Sie die URL-Listenrichtlinie mithilfe der CLI an den SSL-Bridge-Lastenausgleich

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <vServerName> -policyName <string> [-priority <
     positive_integer>]
2 <!--NeedCopy-->
```

Konfiguration einer URL-Liste mithilfe der GUI

Mit der GUI können Sie:

- Importiert eine URL-Liste.

- Fügen Sie eine URL-Liste hinzu.
- Konfigurieren Sie die Aktionen in der URL-Liste.
- Konfigurieren Sie URL-Listenrichtlinien für HTTP-Verkehr.
- Fügen Sie einen virtuellen HTTP-Load-Balancing-Server für HTTP-Verkehr hinzu.
- Fügen Sie einen virtuellen SSL-Bridge-Load-Balancing-Server für HTTPS-Verkehr hinzu.
- Binden Sie URL-Listenrichtlinien an den virtuellen HTTP-Load-Balancing-Server.
- Binden Sie eine URL-Listenrichtlinie an den virtuellen SSL-Bridge-Load-Balancing-Server.

Um eine URL-Liste zu importieren

1. Erweitern Sie im Navigationsbereich **AppExpert** > **URL-Sets**.
2. Klicken Sie im Detailbereich auf **Importieren**.
3. Stellen Sie auf der Seite **„URL-Satz konfigurieren** “ die folgenden Parameter ein.
   a) **Name.** Name des URL-Sets.
   b) **URL**. Webadresse des Standorts, von dem aus auf das URL-Set zugegriffen werden soll.
   c) **Überschreiben**. Überschreiben Sie einen zuvor importierten URL-Satz.
   d) **Trennzeichen**. Zeichenfolge, die einen CSV-Dateidatensatz abgrenzt.
   e) **Zeilentrennzeichen.** In der CSV-Datei verwendetes Zeilentrennzeichen. Ein einzelner Zeichenwert ist zulässig, zum Beispiel „/n“.
   f) **Intervall**. Intervall in Sekunden, abgerundet auf die nächsten 15 Minuten, in dem der URL-Satz aktualisiert wird.
   g) **Privates Set.** Option, um den Export des URL-Sets zu verhindern
   h) **Kanarische URL**. Interne URL zum Testen, ob der Inhalt des URL-Sets vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um eine URL-Liste hinzuzufügen

1. Erweitern Sie im Navigationsbereich **AppExpert** > **URL-Sets**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **„URL-Satz erstellen** “ die folgenden Parameter ein.
   a) **Name.** Der Name des URL-Sets, das beim Import angegeben wurde.
   b) **Kommentare**. Eine kurze Beschreibung des URL-Sets.
4. Klicken Sie auf **Erstellen**.

So konfigurieren Sie eine URL-Listenaktion

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zur Registerkarte **Konfiguration** .
2. **Navigieren Sie im Menübereich zu**AppExpert**>**Responder > Actions**.**

3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Stellen Sie auf der Seite „ **Responder-Aktion erstellen** “ die folgenden Parameter ein.
   a) **Name.** Name der Richtlinienaktion „URL-Liste“.
   b) **Geben Sie ein**. Wählen Sie einen Aktionstyp aus.
   c) **Expression.** Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
   d) **Kommentare**. Eine kurze Beschreibung der politischen Maßnahme.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So konfigurieren Sie eine URL-Listenrichtlinie

1. **Erweitern Sie im Navigationsbereich**AppExpert**>**Responder > Policies**.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **Responder-Richtlinie erstellen** “ die folgenden Parameter ein.
   a) **Name.** Name der Richtlinienaktion „URL-Liste“.
   b) **Aktion**. Wählen Sie die Aktion „URL-Liste“ aus, die Sie der Richtlinie zuordnen möchten.
   c) **Aktion protokollieren**. Wählen Sie die Aktion protokollieren aus.
   d) **AppFlow**. Wählen Sie eine AppFlow-Aktion aus.
   e) **Expression.** Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
   f) **Kommentare**. Eine kurze Beschreibung der Richtlinie.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie einen virtuellen HTTP-Load-Balancing-Server hinzu

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf dem Bildschirm **Load Balancing Virtual Server** die folgenden Parameter ein:
   a) **Name.** Name des virtuellen Lastausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als HTTP.
   c) **IP-Adresstyp**. IP-adressierbarer Typ.
   d) **IP-Adresse**. Dem virtuellen Server zugewiesene IP 4- oder IP6-IP-Adresse.
   e) **Port**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.

So binden Sie eine URL-Listenrichtlinie an den virtuellen HTTP-Load-Balancing-Server

1. Navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Virtuelle Server** .

2. Wählen Sie im Detailbereich den virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.
   a) Wählen Sie Richtlinie. Wählen Sie in der Dropdownliste eine Richtlinie zur URL-Kategorisierung aus.
   b) Wählen Sie Typ. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite Richtlinien die URL-Listenrichtlinie aus der Liste aus und klicken Sie auf **Auswählen**.
8. Klicken Sie im Schieberegler **Richtlinien** auf **Binden** und **Schließen**.

So fügen Sie eine URL-Listenrichtlinie für HTTPS-Verkehr hinzu

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Konfiguration**>**Optimierung**>**Videoo**Erkennung**.**
2. Klicken Sie auf der **Erkennungsseite** auf den Link **Erkennungsrichtlinien für die Videooptimierung** .
3. Klicken Sie auf der Seite mit den **Erkennungsrichtlinien für die Videooptimierung** auf **Hinzufügen**.
4. Stellen Sie auf der Seite **Create Video Optimization Detection Policy** die folgenden Parameter ein.
   a) **Name.** Name der Optimierungsrichtlinie
   b) **Expression.** Konfigurieren Sie die Richtlinie mithilfe benutzerdefinierter Ausdrücke.
   c) **Aktion**. Optimierungsaktion im Zusammenhang mit der Richtlinie zur Handhabung des eingehenden Videoverkehrs.
   d) **UNDEF Aktion**. Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
   e) **Kommentar**. Eine kurze Beschreibung der Richtlinie.
   f) **Aktion protokollieren**. Wählen Sie eine Audit-Log-Aktion aus, die die Aktion angibt, die für die Protokollmeldungen ausgeführt werden soll.
5. Klicken Sie auf **Erstellen** und **Schließen**.

Um einen virtuellen SSL-Bridge-Load-Balancing-Server für HTTPS-Verkehr hinzuzufügen

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf dem Bildschirm **Load Balancing Virtual Server** die folgenden Parameter ein:

a) **Name.** Name des virtuellen Lastausgleichsservers.
b) **Protokoll**. Wählen Sie den Protokolltyp als SSL-Bridge.
c) **IP-Adresstyp**. IP-Adresstyp: IPv4 oder IPv6.
d) **IP-Adresse**. IPv4- oder IP6ViP-Adresse, die dem virtuellen Server zugewiesen wurde.
e) **Port**. Portnummer des virtuellen Servers.

4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter dem Thema „Einen virtuellen Server erstellen“.

Um eine URL-Listenrichtlinie an den virtuellen SSL-Bridge-Load-Balancing-Server zu binden

1. Navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Wählen Sie im Detailbereich den virtuellen SSL-Bridge-Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Stellen Sie die folgenden Parameter ein.
   a) **Wählen Sie Richtlinie.** Wählen Sie in der Dropdownliste die Videoerkennungsrichtlinie aus.
   b) **Wählen Sie Typ**. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus und klicken Sie auf **Schließen**.

Audit-Log-Messaging konfigurieren

Mithilfe der Prüfprotokollierung können Sie eine Bedingung oder Situation in jeder Phase des URL-Listenprozesses überprüfen. Wenn eine NetScaler-Appliance eine eingehende URL empfängt und die Responder-Richtlinie über einen erweiterten Richtlinienausdruck zum Festlegen von URLs verfügt, sammelt die Audit-Log-Funktion URL-Set-Informationen in der URL und speichert die Details als Protokollnachricht für jedes Ziel, das durch die Überwachungsprotokollierung zulässig ist.

Die Lognachricht enthält die folgenden Informationen:

1. Zeitstempel.
2. Nachrichtentyp protokollieren.
3. Die vordefinierten Protokollebenen (Kritisch, Fehler, Hinweis, Warnung, Information, Debug, Warnung und Notfall).
4. Loggen Sie Nachrichteninformationen ein, z. B. Name des URL-Sets, Richtlinienaktion, URL.

Um die Überwachungsprotokollierung für die Funktion „URL-Liste“ zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Überwachungsprotokollmeldung erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Audit-Protokollierung.

URL-Liste Semantik

In der folgenden Tabelle sind die URL-Abgleichsmuster aufgeführt und beschrieben, wie die URLs in einer URL-Liste mit den URLs für eingehende Anfragen abgeglichen werden. Zum Beispiel stimmt das Muster nur mit einer Seite bei `www.example.com/bar` überein `www.example.com/bar`. Um alle Seiten abzugleichen, deren URL mit `www.example.com/bar` beginnt, würden Sie am Ende der URL ein Sternchen (*) hinzufügen.

Semantik	URL-Muster	Übereinstimmend	Unübertroffen
Abgleich von Subdomains	domain.com	domain.com; `www.domain.com`; sub.one.domain.com	yourdomain.com; wwwdomain.com
URL-Abgleich, genauer Pfad	domain.com/example/bar/index.html	domain.com/example/bar/index.html; `www.domain.com/example/bar/index.html`; s.domain.com/example/bar/index.html	wwwdomaincom/example/bar/index; do-main.com/example/bar/index.html/o
URL-Abgleich, genauer Pfad	domain.com/example/l	domain.com/example/l; `www.domain.com/example/bar/index.html?`; s.domain.com/example	wwwdomaincom/example/bar/index; do-main.com/example/bar/index.html/o
URL-Abgleich, Unterpfadabgleich	domain.com/example/bar/	domain.com/beispiel/bar/; do-main.com/beispiel/bar/index.html; `www.domain.com/example/bar/index.html`; do-main.com/beispiel/bar/index.html/one.jpg	wwwdomaincom/example/bar/index

URL-Kategorisierung

August 15, 2023

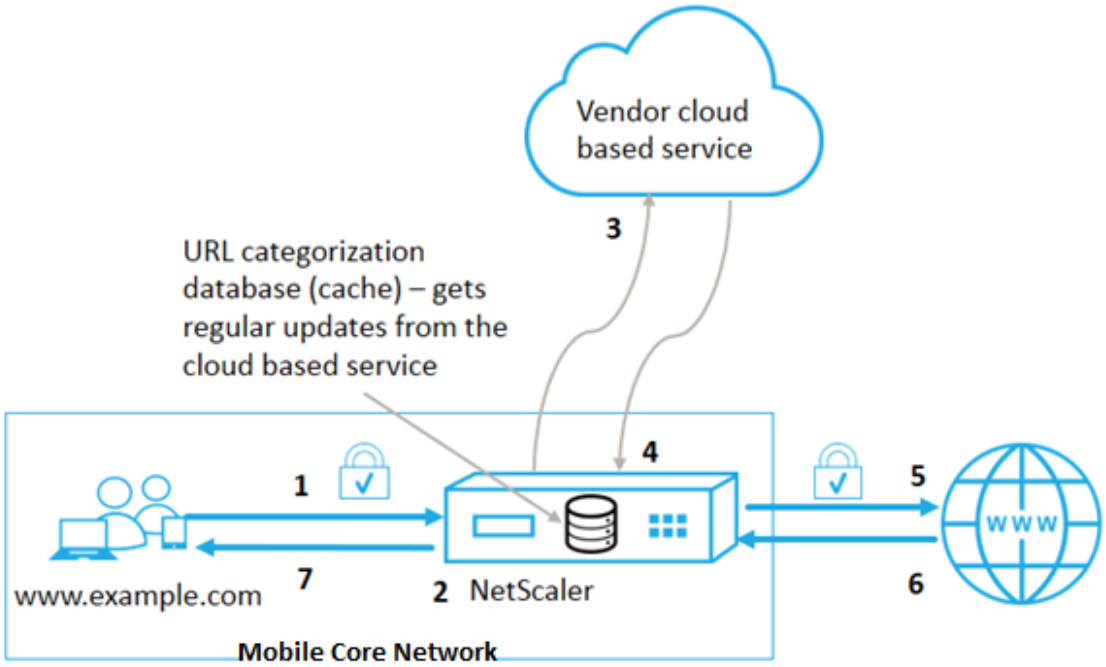
> **Hinweis:**
>
> Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

Die URL-Kategorisierung beschränkt den Benutzerzugriff auf bestimmte Websites und Website-Kategorien. Als abonnierter Dienst in Zusammenarbeit mit ermöglicht die Funktion Unternehmenskunden NetSTAR, den Webverkehr mithilfe einer kommerziellen Kategorisierungsdatenbank zu filtern. Die NetSTAR-Datenbank enthält eine große Anzahl (Milliarden) von URLs, die in verschiedene Kategorien eingeteilt sind, z. B. soziale Netzwerke, Glücksspiele, Inhalte für Erwachsene, neue Medien und Shopping. Zusätzlich zur Kategorisierung hat jede URL eine Reputationsbewertung, die basierend auf dem historischen Risikoprofil der Website auf dem neuesten Stand gehalten wird. Wir können NetSTAR-Daten verwenden, um den Datenverkehr zu filtern, indem wir erweiterte Richtlinien basierend auf Kategorien, Kategoriegruppen (wie Terrorismus, illegale Drogen) oder Reputationsbewertungen für Websites konfigurieren.

Sie können beispielsweise den Zugriff auf gefährliche Websites blockieren, z. B. Websites, die mit Malware infiziert sind, oder den Zugriff auf Inhalte für Erwachsene oder Streaming-Medien zur Unterhaltung selektiv einschränken.

So funktioniert die URL-Kategorisierung

Die folgende Abbildung zeigt, wie der NetScaler URL Filtering Service in eine kommerzielle URL-Kategorisierungsdatenbank und Cloud-Dienste für häufige Updates integriert ist.



Die Komponenten interagieren wie folgt:

1. Der Client sendet eine internetgebundene URL-Anfrage.
2. Eine NetScaler-Richtlinie versucht, die Anfrage anhand der Kategorisierungsdetails (wie Kategorie, Kategoriegruppe und Site-Reputations-Score) zu bewerten, die aus der URL-Kategorisierungsdatenbank abgerufen werden. Wenn die Datenbank die Kategoriedetails zurückgibt, springt der Prozess zu Schritt 5.
3. Wenn die Datenbank keine Kategorisierungsdetails zurückgibt, wird die Anfrage an einen cloudbasierten Suchdienst gesendet, der von einem Anbieter für die URL-Kategorisierung verwaltet wird. Die Appliance wartet jedoch nicht auf eine Antwort. Stattdessen markiert es die URL als Nicht kategorisiert und geht zu Schritt 5 über. Es überwacht jedoch weiterhin das Cloud-Abfrage-Feedback und verwendet es, um den Cache zu aktualisieren, sodass zukünftige Anfragen von der Cloud-Suche profitieren können.
4. Die NetScaler-Appliance erhält die URL-Kategoriedetails (Kategorie, Kategoriegruppe und Reputationswert) vom cloudbasierten Dienst und speichert sie im Cloud-Cache.
5. Wenn die Richtlinie die URL zulässt, wird die Anfrage an den Ursprungsserver gesendet. Andernfalls verwirft die Appliance die Anfrage oder leitet sie weiter oder antwortet mit einer benutzerdefinierten HTML-Seite.
6. Der Ursprungsserver antwortet mit den angeforderten Daten an die NetScaler-Appliance.
7. Die Appliance sendet die Antwort an den Client.

Sie können die URL-Filterfunktion verwenden, um Websites zu erkennen, die gegen die von der Regierung erlassenen Vorschriften zur sicheren Internetnutzung verstoßen, und Richtlinien zur Sper-

rung dieser Websites umzusetzen. Websites, auf denen Inhalte für Erwachsene, Streaming-Medien oder soziale Netzwerke gehostet werden, die als unsicher für Kinder eingestuft oder als illegal verboten wurden.

Voraussetzungen

Die Funktion funktioniert auf Telco-Plattformen mit dem Kauf einer CBM-Grundlizenz und einer CBM Premium-Lizenz. Für andere NetScaler-Plattformen funktioniert die Funktion mit dem Kauf einer CNS Premium-Lizenz.

Hinweis: Zusätzlich zu einer CBM-Grundlizenz und einer CBM Premium-Lizenz muss die Appliance über eine URL Threat Intelligence-Lizenz mit einem Abonnementdienst für 1 Jahr oder 3 Jahre verfügen. Bevor Sie die Funktion aktivieren und konfigurieren, müssen Sie die folgenden Lizenzen installieren:

Lizenzunterstützung für Telco-Plattformen:

- **CBM_TXXX_SERVER_Retail.lic**
- **CBM_TPRE_SERVER_Retail.lic**
- **CNS_WEBF_SSERVER_Retail.lic**

Wobei XXX der Durchsatz ist, zum Beispiel NetScaler T1000.

Lizenzunterstützung für andere NetScaler-Plattformen:

- **CNS_XXX_SERVER_PLT_Retail.lic**

Dabei ist XXX der Durchsatz.

Richtlinienausdrücke zur URL-Kategorisierung

In der folgenden Tabelle werden die verschiedenen Richtlinienausdrücke zur URL-Kategorisierung zur Identifizierung eingehender URLs aufgeführt und eine konfigurierte Aktion angewendet.

Ausdruck	Vorgang
<text>. URL_CATEGORIZE (< min_reputation>, <max_reputation>)	Gibt ein URL_CATEGORY-Objekt zurück. Reputation Score ist eine Zahl von 1 bis 4. Um Objekte zu erhalten, verwenden Sie alle Reputationswerte 0,0 als <min reputation> und . Wenn ist größer als 0, das zurückgegebene Objekt enthält keine Kategorie mit einem niedrigeren Ruf als . Wenn ist größer als 0, das zurückgegebene Objekt enthält keine Kategorie mit einem höheren Ruf als . Wenn die Kategorie nicht rechtzeitig aufgelöst wird, wird der undef-Wert zurückgegeben.
<url_category>. KATEGORIE	Gibt die Kategoriezeichenfolge für dieses Objekt zurück. Wenn die URL keine Kategorie hat oder wenn die URL falsch formatiert ist, lautet der zurückgegebene Wert „Uncategorized“.
<url_category>. GRUPPE	Gibt eine Zeichenfolge zurück, die die Kategoriegruppe des Objekts identifiziert. Dies ist eine Gruppierung von Kategorien auf höherer Ebene, die für Operationen nützlich ist, für die weniger detaillierte Informationen zur URL-Kategorie erforderlich sind. Wenn die URL keine Kategorie hat oder wenn die URL falsch formatiert ist, lautet der zurückgegebene Wert „Uncategorized“.
<url_category>. RUF	Gibt den Reputationswert als Zahl von 1 bis 4 zurück, wobei 4 den riskantesten Ruf angibt. Wenn die Kategorie „Nicht kategorisiert“ lautet, ist der Reputationswert 2.

Beispiele für Richtlinienausdrücke

Richtlinie	Politische Ausdrücke
Richtlinie zur Auswahl von Anfragen für URLs, die in der Kategorie Suchmaschine enthalten sind	füge die Responder-Richtlinie p1 ‘HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (0,0) hinzu. CATEGORY.EQ („Suchmaschine“)
Richtlinie zur Auswahl von Anfragen für URLs, die in der Kategoriengruppe „Erwachsene“ enthalten sind	füge die Responder-Richtlinie p1 ‘HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (0,0) hinzu. GROUP.EQ („Erwachsener“) ‘
Richtlinie zur Auswahl von Anfragen für Suchmaschinen-URLs mit einem Reputationswert von 4.	füge die Responder-Richtlinie p2 ‘HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (4,0) hinzu. CATEGORY.EQ („Suchmaschine“) ‘
Richtlinie zur Auswahl von Anfragen für Suchmaschinen- und Shopping-URLs	füge den Richtlinienpatset good_categories hinzu; binde die Richtlinie good_categories „Search Engine“; binde policy good_categories „Shopping“; füge die Responder-Richtlinie p3 hinzu ‘HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (0,0). KATEGORIE .EQUALS_ANY („good_categories“)
Richtlinie zur Auswahl von Anfragen für Suchmaschinen-URLs mit einem Reputationswert von 4.	füge die Responder-Richtlinie p5 ‘CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE (4,0) hinzu. CATEGORY.EQ („Suchmaschine“)

Richtlinienaktionen zur URL-Kategorisierung

Eine URL-Filterrichtlinie wertet den Traffic aus, um Anfragen zu identifizieren, die zu einer bestimmten Kategorie gehören. In der folgenden Tabelle sind die Aktionen aufgeführt, die Sie einer URL-Filterrichtlinie zuweisen können.

Politische Maßnahmen	Politische Gruppe	Beschreibung
ALLOW	Responder	Erlauben Sie der eingehenden Anfrage den Zugriff auf die Ziel-URL
REDIRECT	Responder	Leitet die eingehende Anfrage an die als Ziel angegebene URL weiter.

Politische Maßnahmen	Politische Gruppe	Beschreibung
DENY	Responder	Eingehende Anfrage ablehnen.
RESET	Responder, Videooptimierung	Verbindung zurücksetzen.
DROP	Responder, Videooptimierung	Verbindung trennen.

> **Hinweis**
>
> Für verschlüsselten Datenverkehr umfasst die VideoOptimierungsrichtlinie Aktionen, die die URL-Filteraktionen implementieren.

URL-Kategorisierung konfigurieren

Um die URL-Kategorisierung zu konfigurieren, aktivieren Sie zunächst die URL-Filterfunktion. Anschließend müssen Sie die Cache-Speicherlimits, die Kategorisierungsrichtlinie und die virtuellen Server für HTTP- und HTTPS-Verkehr konfigurieren. Konfiguration der URL-Kategorisierung mithilfe der CLI.

Gehen Sie wie folgt vor, um die CLI Configure URL-Kategorisierung auf einer NetScaler-Appliance zu verwenden:

- Richten Sie die URL-Kategorisierung ein.
  - Aktivieren Sie die URL-Filterfunktion.
  - Konfigurieren Sie gemeinsamen Speicher, um den Cache-Speicher zu begrenzen
  - Konfigurieren der URL-Kategorisierungsparameter
- Konfigurieren Sie die URL-Kategorisierung für den HTTP-Verkehr.
  - Fügen Sie URL-Kategorisierungsaktionen hinzu.
  - Fügen Sie URL-Kategorisierungsrichtlinien hinzu.
  - Fügen Sie einen virtuellen Lastausgleichsserver für HTTP-Verkehr hinzu.
  - Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen Load-Balancing-Server.
- Konfigurieren Sie die URL-Kategorisierung für HTTPS-Verkehr.
  - Fügen Sie URL-Kategorisierungsrichtlinien hinzu.
  - Fügen Sie einen virtuellen SSL-Bridge-Load-Balancing-Server hinzu.
  - Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen Load-Balancing-Server.

URL-Kategorisierung einrichten

Um die Funktion einzurichten, müssen Sie die Funktion zur URL-Kategorisierung aktivieren, die Filterparameter konfigurieren und das Limit für den gemeinsamen Speicher festlegen.

So aktivieren Sie die URL-Filterfunktion

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature URLFiltering VideoOptimization Responder IC SSL AppFlow
```

Um das Limit für gemeinsam genutzten Speicher zu konfigurieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set cache parameter [-memLimit <megaBytes>]
2 <!--NeedCopy-->
```

Wobei MemLimit das Speicherlimit für das Caching ist.

Beispiel:

```
set cache parameter -memLimit 10
```

Um URL-Kategorisierungsparameter zu konfigurieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
     [-TimeOfDayToUpdateDB <HH:MM>]
2 <!--NeedCopy-->
```

***Beispiel:**

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00
```

Konfiguration der URL-Kategorisierung für HTTP-Verkehr

Um die URL-Kategorisierungsfunktion für HTTP-Verkehr zu konfigurieren, müssen Sie einen virtuellen Load-Balancing-Server konfigurieren, URL-Kategorisierungsrichtlinien hinzufügen und die Richtlinien an den virtuellen Server binden. Auf diese Weise empfängt der virtuelle Server den HTTP-Verkehr und auf der Grundlage der Richtlinienbewertung weist das System eine Filteraktion zu.

So fügen Sie eine URL-Kategorisierungsaktion für HTTP-Verkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <string>]
```


Beispiel:

```
add responder action act_url_categorize respondwith "\"HTTP/1.1 200 OK\r\n\
r\n\" + HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY
 + \"\n\""
```

So fügen Sie eine URL-Kategorisierungsrichtlinie für HTTP-Verkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
string>] [-logAction <string>] [-appflowAction <string>]
```

Beispiel:

```
add responder policy pol_url_categorize_http "HTTP.REQ.HOSTNAME.APPEND(
HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Adult\")|| HTTP.REQ.HOSTNAME.
APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Gambling\")"RESET
```

So fügen Sie einen virtuellen HTTP-Load-Balancing-Server hinzu

Wenn noch kein virtueller Server für HTTP-Verkehr konfiguriert ist, geben Sie an der Befehlszeile Folgendes ein:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-clt Timeout
<secs>]
```

Beispiel:

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout 120
```

Um die URL-Kategorisierungsrichtlinie an den virtuellen Load-Balancing-Server zu binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Beispiel:

```
bind lb vserver vsrv-HTTP -policyName pol_url_categorize_http -priority 10
-gotoPriorityExpression END -type REQUEST
```

Konfiguration der URL-Kategorisierung für HTTPS-Verkehr

Um die URL-Kategorisierungsfunktion für HTTPS-Verkehr zu konfigurieren, müssen Sie einen virtuellen SSL-Bridge-Loading-Balancing-Server konfigurieren, URL-Kategorisierungsrichtlinien

hinzufügen und die Richtlinien an den virtuellen SSL-Bridge-Server binden. Auf diese Weise empfängt der Server den HTTPS-Verkehr und auf der Grundlage der Richtlinienbewertung weist das System eine Filteraktion zu.

So fügen Sie eine URL-Kategorisierungsrichtlinie für HTTPS-Verkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add videooptimization detectionpolicy <name> -rule <expression> -action <
string> [-undefAction <string>] [-comment <string>] [-logAction <string>]
```

Beispiel:

```
add videooptimization detectionpolicy pol_url_categorize_https_block_adult -
rule "CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(0,0).CATEGORY.EQ("Adult")' -
action RESET
```

Um einen virtuellen SSL-Bridge-Load-Balancing-Server hinzuzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT imeout
<secs>]
```

Beispiel:

```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -cltTimeout
 180
```

Um die Kategorisierungsrichtlinie an den virtuellen SSL-Bridge-Server zu binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Beispiel:

```
bind lb vserver vsrv-HTTPS -policyName pol_url_categorize_https_block_adult
 -priority 20 -type REQUEST
```

Konfiguration der URL-Kategorisierung mithilfe der GUI

Mit der GUI können Sie:

- Aktivieren Sie die Funktion zur URL-Kategorisierung.
- Fügen Sie URL-Kategorisierungsaktionen für HTTP-Verkehr hinzu.

- Fügen Sie URL-Kategorisierungsrichtlinien für HTTP-Verkehr hinzu.
- Fügen Sie URL-Kategorisierungsrichtlinien für HTTPS-Verkehr hinzu.
- Fügen Sie einen virtuellen Lastausgleichsserver für HTTP-Verkehr hinzu.
- Fügen Sie einen virtuellen SSL-Bridge-Load-Balancing-Server für HTTPS-Verkehr hinzu.
- Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen Load-Balancing-Server.
- Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen SSL-Bridge-Load-Balancing-Server.
- Konfigurieren Sie das Limit für den gemeinsamen Speicher.
- Konfigurieren der URL-Kategorisierungsparameter

Um die URL-Kategorisierung zu aktivieren

1. Erweitern Sie im Navigationsbereich **System** und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf den Link **Erweiterte Funktionen konfigurieren** .
3. Aktivieren Sie auf der Seite „ **Erweiterte Funktionen konfigurieren** “ das Kontrollkästchen **URL-Filterung** .
4. Klicken Sie auf **OK** und **schließen**.

So fügen Sie eine URL-Kategorisierungsaktion hinzu

1. **Erweitern Sie im Navigationsbereich**AppExpert**>**Responder > Action**.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **Responder-Aktion erstellen** “ die folgenden Parameter ein.
   a) **Name.** Name der Richtlinienaktion zur URL-Kategorisierung.
   b) **Geben Sie ein**. Wählen Sie einen Aktionstyp aus.
   c) **Expression.** Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
   d) **Kommentare**. Eine kurze Beschreibung der politischen Maßnahme.
4. Klicken Sie auf **Erstellen** und **Schließen**.

Um eine URL-Kategorisierungsrichtlinie für HTTP-Verkehr hinzuzufügen

1. **Erweitern Sie im Navigationsbereich**AppExpert**>**Responder > Policies**.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **Responder-Richtlinie erstellen** “ die folgenden Parameter ein.
   a) **Name.** Name der Richtlinienaktion zur URL-Kategorisierung.
   b) **Aktion**. Wählen Sie die Aktion zur URL-Kategorisierung aus, die Sie der Richtlinie zuordnen möchten.
   c) **Aktion protokollieren**. Wählen Sie die Aktion protokollieren aus.
   d) **AppFlow**. Wählen Sie eine AppFlow-Aktion aus.

e) **Expression.** Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
f) **Kommentare**. Eine kurze Beschreibung der politischen Maßnahme.

4. Klicken Sie auf **Erstellen** und **Schließen**.

Um eine Kategorisierungsrichtlinie für HTTPS-Verkehr hinzuzufügen

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Konfiguration**>**Optimierung**>**Videoo **Erkennung**.**
2. Klicken Sie auf der **Erkennungsseite** auf den Link **Erkennungsrichtlinien für die Videooptimierung** .
3. Klicken Sie auf der Seite mit den Erkennungsrichtlinien für die Videooptimierung auf **Hinzufügen**.
4. Stellen Sie auf der Seite **Create Video Optimization Detection Policy** die folgenden Parameter ein.
   a) **Name.** Name der Optimierungsrichtlinie
   b) **Expression.** Konfigurieren Sie die Richtlinie mithilfe benutzerdefinierter Ausdrücke.
   c) **Aktion**. Optimierungsaktion im Zusammenhang mit der Richtlinie zur Handhabung des eingehenden Videoverkehrs.
   d) **UNDEF Aktion**. Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
   e) **Kommentar**. Eine kurze Beschreibung der Richtlinie.
   f) **Log Action.** Wählen Sie eine Audit-Log-Aktion aus, die die Aktion angibt, die für die Protokollmeldungen ausgeführt werden soll.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie einen virtuellen Lastausgleichsserver für HTTP-Verkehr hinzu

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Load Balancing Virtual Server** die folgenden Parameter ein:
   a) **Name.** Name des virtuellen Lastausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als HTTP.
   c) **IP-Adresstyp.** IPv4 oder IPv6.
   d) **IP-Adresse.** IPv4 oder IPv6, dem virtuellen Server zugewiesene VIP-Adresse.
   e) **Port**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie einen virtuellen SSL-Bridge-Load-Balancing-Server hinzu

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Load Balancing Virtual Server** die folgenden Parameter ein:
   a) **Name.** Name des virtuellen Lastausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als SSL-Bridge.
   c) **IP-Adresstyp**. IP-adressierbarer Typ.
   d) **IP-Adresse**. Dem virtuellen Server zugewiesene IP 4- oder IP6-IP-Adresse.
   e) **Port**. Portnummer des virtuellen Servers.
4. Wählen Sie **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

Um eine URL-Kategorisierungsrichtlinie an den virtuellen HTTP-Load-Balancing-Server zu binden

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Wählen Sie im Detailbereich den virtuellen Load Balancing-Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Stellen Sie die folgenden Parameter ein.
   a) **Wählen Sie Richtlinie**. Wählen Sie in der Dropdownliste die URL-Kategorisierungsrichtlinie aus.
   b) **Wählen Sie Typ**. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die URL-Kategorisierungsrichtlinie aus der Liste aus und klicken Sie auf **Schließen**.

Um eine Kategorisierungsrichtlinie an den virtuellen SSL-Bridge-Load-Balancing-Server zu binden

1. Navigieren Sie zum Bildschirm **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Wählen Sie im Detailbereich den virtuellen SSL-Bridge-Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um den Schieberegler **Richtlinien** aufzurufen.
5. Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.

a) **Wählen Sie Richtlinie**. Wählen Sie in der Dropdownliste die Videoerkennungsrichtlinie aus.
b) **Wählen Sie Typ**. Wählen Sie den Richtlinientyp als Anforderung aus.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus und klicken Sie auf **Schließen**.

So konfigurieren Sie das Limit für gemeinsam genutzten Speicher

1. Melden Sie sich bei der Appliance an und navigieren Sie zu **Optimization** > **Integrated Caching**.
2. Klicken Sie im Detailbereich auf den Link **Cache-Einstellungen ändern** .
3. Stellen Sie auf der Seite **„Globale Cache-Einstellungen** “ die folgenden Parameter ein.
   a) **Speicherauslastungslimit (MB).**
   b) **Limit der aktiven Speichernutzung**.
   c) **Über den Header**.
   d) **Maximale Länge des Post-Texts, der zwischengespeichert werden soll**
   e) **Globale Aktion mit undefinierten Ergebnissen**
   f) **HA-Objektpersistenz aktivieren**
   g) **Überprüfen Sie, ob das zwischengespeicherte Objekt bestehen bleibt**
   h) **Vorabrufe**
4. Klicken Sie auf **OK** und **schließen**.

Um URL-Kategorisierungsparameter zu konfigurieren

1. Melden Sie sich bei der Appliance an und navigieren Sie zu **Sicherheit**.
2. Klicken Sie im Detailbereich auf den Link **URL-Filtereinstellungen ändern** .
3. Stellen Sie auf der Seite „ **URL-Filterparameter konfigurieren** “ die folgenden Parameter ein.
   a) Stunden zwischen DB-Aktualisierungen. Stunden des URL-Filters zwischen Datenbankaktualisierungen Minimalwert: 0 und Maximalwert: 720.
   b) Tageszeit zur Aktualisierung der DB. Uhrzeit der URL-Filterung zur Aktualisierung der Datenbank.
4. Klicken Sie auf **OK und dann** auf **Schließen.**

Audit-Log-Messaging konfigurieren

Wenn eine NetScaler-Appliance eine eingehende URL empfängt und die Responder-Richtlinie über einen URL-Filterausdruck verfügt, sammelt die Überwachungsprotokollfunktion Kategorisierungsinformationen und zeigt sie als Protokollmeldungen an jeden konfigurierten Zielüberwachungsprotokollserver an. Die Information wird protokolliert.

- Quell-IP-Adresse (die IP-Adresse des Clients, der die Anfrage gestellt hat).

- Ziel-IP-Adresse (die IP-Adresse des angeforderten Servers).
- Angeforderte URL, die das Schema, den Host und den Domainnamen (`http://www.example.com`) enthält.
- URL-Kategorie, die das URL-Filterframework zurückgibt.
- URL-Kategoriegruppe, die vom URL-Filterframework zurückgegeben wurde
- Die vom URL-Filter-Framework zurückgegebene URL-Reputationsnummer
- Gemäß der Richtlinie zur URL-Kategorisierung durchgeführte Aktion im Prüfprotokoll.

Um die Überwachungsprotokollierung für die URL-Liste zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Überwachungsprotokollmeldung erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

Speichern von Fehlern mit SYSLOG Messaging

Wenn in jeder Phase des URL-Filtervorgangs ein Fehler auf Systemebene auftritt, verwendet die NetScaler-Appliance den Audit-Log-Mechanismus, um Protokolle in der Datei ns.log zu speichern. Die Fehler werden als Textnachrichten im SYSLOG-Format gespeichert, sodass ein Administrator sie später in einer chronologischen Reihenfolge des Ereignisses anzeigen kann. Diese Protokolle werden auch zur Archivierung an einen externen SYSLOG-Server gesendet. Weitere Informationen finden Sie im Artikel CTX229399.

Wenn beispielsweise ein Fehler auftritt, wenn Sie das URL-Filter-SDK initialisieren, wird die Fehlermeldung im folgenden Nachrichtenformat gespeichert.

Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing NetStar SDK (SDK error=-1). (status=1).

Die NetScaler-Appliance speichert die Fehlermeldungen in vier verschiedenen Fehlerkategorien:

- Fehler beim Herunterladen. Wenn beim Versuch, die Kategorisierungsdatenbank herunterzuladen, ein Fehler auftritt.
- Scheitern der Integration. Wenn ein Fehler auftritt, wenn Sie ein Update in die vorhandene Kategorisierungsdatenbank integrieren.
- Fehler bei der Initialisierung. Wenn bei der Initialisierung der Funktion zur URL-Kategorisierung ein Fehler auftritt, legen Sie Kategorisierungsparameter fest oder beenden Sie einen Kategorisierungsdienst.
- Fehler beim Abrufen. Wenn ein Fehler auftritt, wenn die Appliance die Kategorisierungsdetails der Anforderung abruft.

URL-Reputationsbewertung

Die Funktion zur URL-Kategorisierung bietet eine richtlinienbasierte Steuerung zur Einschränkung von URLs auf der Sperrliste. Sie können den Zugriff auf Websites basierend auf der URL-Kategorie, dem Reputationswert oder der URL-Kategorie und dem Reputationswert steuern. Wenn ein Netzwerkadministrator einen Benutzer überwacht, der auf hochriskante Websites zugreift, kann er eine Responder-Richtlinie verwenden, die an den URL-Reputationswert gebunden ist, um solche riskanten Websites zu blockieren.

Nach Erhalt einer eingehenden URL-Anforderung ruft die Appliance die Kategorie und den Reputationswert aus der URL-Kategorisierungsdatenbank ab. Basierend auf dem von der Datenbank zurückgegebenen Reputationswert weist die Appliance Websites eine Reputationsbewertung zu. Der Wert kann zwischen 1 und 4 liegen, wobei 4 die riskanteste Art von Websites ist, wie in der folgenden Tabelle gezeigt.

URL Reputation Bewertung	Reputation Kommentar
1	Saubere Seite.
2	Unbekannter Standort.
3	Potenziell gefährlich oder mit einer gefährlichen Website verbunden.
4	Bösartige Seite.

FAQ

May 11, 2023

In diesem Abschnitt finden Sie die FAQ zu den folgenden NetScaler-Funktionen

- Admin-Partition
- AppFlow
- Call Home
- Clustering
- Verbindungsverwaltung
- Content Switching
- Debuggen
- Hardware
- Hohe Verfügbarkeit

- Integriertes Caching
- Installieren, Upgrade und Downgrade
- Lastausgleich
- NetScaler-Benutzeroberfläche
- SSL

Admin-Partition

May 11, 2023

Wo finde ich die NetScaler-Konfigurationsdatei für eine Partition?

*Die Konfigurationsdatei (*ns.conf*) für die Standardpartition ist im Verzeichnis /nsconfig verfügbar.* <partitionName>Für Admin-Partitionen ist die Datei im Verzeichnis */nsconfig/partitions/* verfügbar.

Wie kann ich integriertes Caching in einer partitionierten NetScaler-Appliance konfigurieren?

> **Hinweis**
>
> Integriertes Caching in Admin-Partitionen wird ab NetScaler 11.0 unterstützt.

Um integriertes Caching (IC) auf einem partitionierten NetScaler zu konfigurieren, kann der Superuser nach der Definition des IC-Speichers auf der Standardpartition den IC-Speicher auf jeder Admin-Partition so konfigurieren, dass der gesamte IC-Speicher, der allen Admin-Partitionen zugewiesen ist, den auf der Standardpartition definierten IC-Speicher nicht überschreitet. Der Speicher, der nicht für die Admin-Partitionen konfiguriert ist, bleibt für die Standardpartition verfügbar.

Wenn eine NetScaler-Appliance mit zwei Admin-Partitionen beispielsweise 10 GB IC-Speicher der Standardpartition zugewiesen hat und die IC-Speicherzuweisung für die beiden Admin-Partitionen wie folgt lautet:

- Partition 1: 4 GB
- Partition 2: 3 GB

Dann stehen für die Standardpartition 10 - (4 + 3) = 3 GB IC-Speicher zur Verwendung zur Verfügung.

> **Hinweis**
>
> Wenn der gesamte IC-Speicher von den Admin-Partitionen verwendet wird, ist kein IC-Speicher für die Standardpartition verfügbar.

Was ist der Umfang für L2- und L3-Parameter in Admin-Partitionen?

> **Hinweis**
>
> - Gültig ab NetScaler 11.0.
> - Damit ARP auf einer nicht standardmäßigen Partition funktioniert, müssen Sie den Parameter „proxyARP“ im Befehl „set l2param“ aktivieren.

Auf einer partitionierten NetScaler-Appliance sieht der Umfang der Aktualisierung der L2- und L3-Parameter wie folgt aus:

- Für L2-Parameter, die mit dem Befehl „set L2Param“ festgelegt wurden, können die folgenden Parameter nur von der Standardpartition aus aktualisiert werden, und ihre Werte gelten für alle Admin-Partitionen:

  MaxBridgeCollision, bdgSetting, GarponVridIntf, GarPreply, ProxyARP, ResetInterfaceOnHAFailover und skip_proxying_bsd_traffic.

  Die anderen L2-Parameter können in bestimmten Admin-Partitionen aktualisiert werden, und ihre Werte beziehen sich auf diese Partitionen.
- Bei L3-Parametern, die mit dem Befehl „set L3Param“ festgelegt wurden, können alle Parameter in bestimmten Admin-Partitionen aktualisiert werden, und ihre Werte sind lokal für diese Partitionen. Ebenso gelten die Werte, die in der Standardpartition aktualisiert werden, nur für die Standardpartition.

Wie aktiviere ich dynamisches Routing in einer Admin-Partition?

> **Hinweis**
>
> Dynamisches Routing in Admin-Partitionen wird ab NetScaler 11.0 unterstützt.

Dynamisches Routing (OSPF, RIP, BGP, ISIS, BGP+) ist zwar standardmäßig auf der Standardpartition aktiviert, in einer Admin-Partition muss es jedoch mithilfe des folgenden Befehls aktiviert werden:

```
> set L3Param -dynamicRouting ENABLED
```

> **Hinweis**
>
> Maximal 63 Partitionen können dynamisches Routing ausführen (62 Admin-Partitionen und 1 Standardpartition).

Wenn dynamisches Routing auf einer Admin-Partition aktiviert wird, wird ein virtueller Router (VR) erstellt.

- <partition-name>Jede VR verwaltet ihr eigenes vlan0, das als vlan0_ angezeigt wird.
- Alle ungebundenen IP-Adressen, die ZeBOS zugänglich sind, sind an vlan0 gebunden.
- Die Standard-VR (der Standardpartition) zeigt alle konfigurierten VRs.
- Die Standard-VR zeigt die VLANs, die an diese VRs gebunden sind (außer Standard-VLANs).

Wo finde ich die Logs für eine Partition?

NetScaler-Protokolle sind nicht partitionsspezifisch. Logeinträge für alle Partitionen müssen im Verzeichnis */var/log/* gespeichert werden.

Wie kann ich Audit-Logs für eine Admin-Partition abrufen?

In einem partitionierten NetScaler können Sie keine spezifischen Protokollserver für eine bestimmte Partition haben. Die Server, die auf der Standardpartition definiert sind, sind für alle Administratorpartitionen anwendbar. Um die Überwachungsprotokolle für eine bestimmte Partition anzuzeigen, müssen Sie daher den Befehl “Audit-Nachrichten anzeigen” verwenden.

> **Hinweis**
>
> Die Benutzer einer Admin-Partition haben keinen Zugriff auf die Shell und können daher nicht auf die Logdateien zugreifen.

Wie kann ich Weblogs für eine Admin-Partition abrufen?

Sie können die Weblogs für eine Admin-Partition wie folgt abrufen:

- **Für NetScaler 11.0 und neuere Versionen**

  Die Weblogging-Funktion muss auf jeder Partition aktiviert sein, für die Weblogging erforderlich ist. Mithilfe des NetScaler Web Logging (NSWL) -Clients ruft der NetScaler die Webprotokolle für alle Partitionen ab, denen der Benutzer zugeordnet ist.

- **Für Versionen vor NetScaler 11.0**

  Weblogs können nur von `nsroot` und anderen Superbenutzern abgerufen werden. Auch wenn Weblogging auf der Standardpartition aktiviert ist, ruft der NetScaler Web Logging (NSWL) -Client Webprotokolle für alle Partitionen ab.

Um die Partition für jeden Protokolleintrag anzuzeigen, passen Sie das Protokollformat an, sodass es die Option %P enthält. Anschließend können Sie die Protokolle filtern, um die Protokolle für eine bestimmte Partition anzuzeigen.

Wie kann ich den Trace für eine Admin-Partition abrufen?

Sie können den Trace für eine Admin-Partition wie folgt abrufen:

- **Für NetScaler 11.0 und neuere Versionen**

  In einer partitionierten NetScaler-Appliance kann der `nstrace` Vorgang auf einzelnen Administratorpartitionen ausgeführt werden. <partitionName>Die Trace-Dateien werden im Verzeichnis */var/partitions/ /nstrace/*gespeichert.

Hinweis: Sie können die Spur einer Admin-Partition nicht mithilfe der GUI abrufen. Sie müssen die CLI verwenden.

- **Für Versionen vor NetScaler 11.0**

  Der `nstrace` Vorgang kann nur auf der Standardpartition ausgeführt werden. Daher sind Paketerfassungen für das gesamte NetScaler-System verfügbar. Verwenden Sie auf VLAN-ID basierende Filter, um partitionsspezifische Paketerfassungen zu erhalten.

Wie kann ich das technische Support-Paket speziell für eine Admin-Partition erhalten?

Um das technische Support-Paket für eine bestimmte Partition zu erhalten, führen Sie den folgenden Befehl von der Standardpartition aus:

```
> show techsupport -scope partition <partitionName>
```

Hinweis: Dieser Befehl enthält auch systemspezifische Informationen.

AppFlow

May 11, 2023

- **Welcher Build von NetScaler unterstützt AppFlow?**

  AppFlow wird auf NetScaler-Appliances mit Version 9.3 und höher mit nCore Build unterstützt.

- **Welches Format verwendet AppFlow zur Übertragung von Daten?**

  AppFlow überträgt Informationen im Format Internet Protocol Flow Information eXport (IPFIX), einem offenen Standard der Internet Engineering Task Force (IETF), der in RFC 5101 definiert ist. IPFIX (die standardisierte Version von NetFlow von Cisco) wird häufig zur Überwachung von Netzwerkflussinformationen verwendet.

- **Was enthalten AppFlow-Datensätze?**

  AppFlow-Datensätze enthalten standardmäßige NetFlow- oder IPFIX-Informationen, wie Zeitstempel für den Beginn und das Ende eines Flusses, Paketanzahl und Byteanzahl. AppFlow-Datensätze enthalten auch Informationen auf Anwendungsebene (wie HTTP-URLs, HTTP-Anforderungsmethoden und Antwortstatuscodes, Serverantwortzeit und Latenz). IPFIX-Flow-Datensätze basieren auf Vorlagen, die vor dem Senden von Flow-Datensätzen gesendet werden müssen.

- **Warum führt der Versuch, einen virtuellen Server über die GUI zu öffnen, nach einem Upgrade auf NetScaler Version 9.3 Build 48.6 Cl zu der Fehlermeldung „Die AppFlow-Funktion ist nur auf NetScaler Ncore verfügbar“?**

AppFlow wird nur auf nCore Appliances unterstützt. Deaktivieren Sie beim Öffnen der Registerkarte “Konfiguration des virtuellen Servers” das Kontrollkästchen **AppFlow** .

- **Was enthält die Transaktions-ID in AppFlow Datensätzen?**

  Eine Transaktions-ID ist eine 32-Bit-Nummer ohne Vorzeichen, die eine Transaktion auf Anwendungsebene identifiziert. Für HTTP entspricht eine Transaktion einem Anforderungs- und Antwortpaar. Alle Flow-Datensätze, die diesem Anforderungs- und Antwortpaar entsprechen, haben dieselbe Transaktions-ID. Eine typische Transaktion hat vier Flow-Datensätze. Wenn der NetScaler die Antwort selbst generiert (bereitgestellt aus dem integrierten Cache oder durch eine Sicherheitsrichtlinie), gibt es möglicherweise nur zwei Flow-Datensätze für die Transaktion.

- **Was ist eine AppFlow Aktion?**

  Eine AppFlow-Aktion ist eine Reihe von Collectors, an die die Flow-Datensätze gesendet werden, wenn die zugehörige AppFlow-Richtlinie übereinstimmt.

- **Welche Befehle kann ich auf der NetScaler Appliance ausführen, um zu überprüfen, ob die AppFlow Aktion ein Treffer ist?**

  Die Aktion “AppFlow anzeigen”. Zum Beispiel:

```
> show appflow action
1) Name: aFL-act-collector-1
   Collectors: collector-1
   Hits: 0
   Action Reference Count: 2
  2) Name: apfl-act-collector-2-and-3
   Collectors: collector-2, collecter-3
   Hits: 0
   Action Reference Count: 1
  3) Name: apfl-act-collector-1-and-3
   Collectors: collector-1, collecter-3
   Hits: 0
   Action Reference Count: 1
<!--NeedCopy-->
```

- **Was ist ein AppFlow-Collector?**

Ein Collector empfängt von der NetScaler-Appliance generierte Flow-Datensätze. Um Flow-Records senden zu können, müssen Sie mindestens einen Collector angeben. Sie können bis zu vier angeben. Sie können ungenutzte Kollektoren entfernen.

- **Welche NetScaler-Version ist für die Verwendung von AppFlow erforderlich?**

  Verwenden Sie NetScaler Version 9.3.49.5 oder höher und denken Sie daran, dass AppFlow nur in den nCore-Builds verfügbar ist.

- **Welches Transportprotokoll verwendet AppFlow?**

  AppFlow verwendet UDP als Transportprotokoll.

- **Welche Ports müssen geöffnet werden, wenn ich eine Firewall im Netzwerk habe?**

  Anschluss 4739. Es ist der Standard-UDP-Port, den der AppFlow -Kollektor zum Abhören von IPFIX-Nachrichten verwendet. Wenn der Benutzer den Standardport ändert, muss dieser Port an der Firewall geöffnet werden.

- **Wie kann ich den Standardport ändern, den AppFlow verwendet?**

  Wenn Sie einen AppFlow-Collector mithilfe des Befehls add AppFlowCollector hinzufügen, können Sie den zu verwendenden Port angeben.

```
1  > add appflowCollector coll1 -IPAddress 10.102.29.251 -port 8000
2   Done
3  <!--NeedCopy-->
```

- **Was bewirkt die Einstellung clientTrafficOnly?**

  NetScaler generiert AppFlow-Datensätze nur für den clientseitigen Datenverkehr.

- **Wie viele Kollektoren können gleichzeitig konfiguriert werden?**

  Sie können auf der NetScaler Appliance bis zu vier AppFlow-Kollektoren gleichzeitig konfigurieren. Beachten Sie, dass die maximale Anzahl von Collectors, die auf einer NetScaler Appliance konfiguriert werden können, vier beträgt.

Call Home

June 2, 2023

- **Was ist Call Home auf einer NetScaler-Appliance?**

  Call Home überwacht und benachrichtigt kritische Ereignisse auf einer NetScaler-Appliance. Durch die Aktivierung von Call Home können Sie den Prozess der Fehlerbenachrichtigung automatisieren. Sie vermeiden es nicht nur, den NetScaler-Support anzurufen, eine Serviceanfrage zu stellen und Systemdaten hochzuladen, bevor der NetScaler-Support das Problem beheben kann, sondern Sie erkennen und lösen auch Probleme, bevor sie auftreten.

- **Ist Call Home standardmäßig auf einer NetScaler-Appliance aktiviert?**

  Ja, Call Home ist standardmäßig auf der Appliance aktiviert. Wenn Sie von einer älteren Version, in der Call Home standardmäßig deaktiviert war, auf die neueste Software aktualisieren, aktiviert der Upgrade-Vorgang die Funktion automatisch. Wenn Sie es später deaktivieren, wird

die aktualisierte Einstellung für alle weiteren Upgrades gespeichert. Weitere Informationen finden Sie unter Call Home.

- **Was sind die Voraussetzungen für die Arbeit von Call Home?**

  Zugang zu einer Internetverbindung.

  Hinweis: Wenn Ihre NetScaler-Appliance nicht über eine Internetverbindung verfügt, können Sie einen Proxyserver konfigurieren, über den NetScaler Systemprotokolle generieren und diese auf den Citrix Technical Support Server (CIS) hochladen kann.

- **Was sind die Vorteile der Verwendung von Call Home?**

  - Überwachen Sie Hardware- und Softwarefehler.
  - Benachrichtigen Sie das Auftreten kritischer Ereignisse, die sich auf Ihr Netzwerk auswirken.
  - Senden Sie Leistungsdaten und Systemprotokolle an Citrix an:
    * Analysieren und verbessern Sie die Produktqualität.
    * Bereitstellung von Informationen zur Fehlerbehebung in Echtzeit zur proaktiven Problemerkennung und schnelleren Problemlösung.

- **Welche Version der NetScaler-Software unterstützt Call Home?**

  NetScaler Version 10.0 und höher.

- **Welche NetScaler-Plattformmodelle unterstützen Call Home?**

  Die Call Home-Funktion ist standardmäßig auf allen NetScaler-Plattformen und allen Appliance-Modellen (MPX, VPX und SDX) aktiviert.

  - NetScaler MPX: Alle MPX-Modelle.
  - NetScaler VPX: Alle VPX-Modelle. Darüber hinaus wird es auf VPX-Appliances unterstützt, die ihre Lizenzen von externen oder zentralen Lizenzierungspools beziehen. Die Funktion bleibt jedoch die gleiche wie bei einer Standard-VPX-Appliance.
  - NetScaler SDX: Überwacht das Laufwerk und die zugewiesenen SSL-Chips auf Fehler oder Fehler. Die VPX-Instanzen haben jedoch keinen Zugriff auf die Power Supply Unit (PSU) und daher wird ihr Status nicht überwacht. In einer SDX-Plattform können Sie Call Home entweder direkt auf einer einzelnen Instanz oder über die SVM konfigurieren.

- **Sollte ich den SNMP-Alarm für Call Home konfigurieren, um Fehler zu melden?**

  Nein, Sie müssen SNMP für Call Home nicht konfigurieren, um Fehlerbedingungen zu überwachen, da SNMP- und Call Home-Uploads unabhängig voneinander sind. Wenn Sie jedes Mal benachrichtigt werden möchten, wenn ein Fehler auftritt, können Sie den SNMP-Alarm CALLHOME-UPLOAD-EVENT so konfigurieren, dass bei jedem Call Home-Upload eine SNMP-Warnung generiert wird. Die SNMP-Warnung informiert den lokalen Administrator über das Auftreten kritischer Ereignisse.

- **Wie kontaktiere ich einen technischen Support?**

  Für alle kritischen Hardware-Ereignisse erstellt Call Home automatisch eine Serviceanfrage an NetScaler. Bei anderen Fehlern können Sie sich nach Überprüfung der Systemprotokolle an das technische Support-Team von NetScaler wenden, um eine Serviceanfrage zur weiteren Untersuchung zu stellen. Um den Support zu kontaktieren, besuchen Sie https://www.netscaler.com/resources/support.

- **Welche Fehlerbedingungen überwacht Call Home in einer NetScaler Appliance?**

  Call Home unterstützt die Überwachung der folgenden Ereignisse in einer NetScaler-Appliance:

  - Fehler beim Compact Flash-Laufwerk
  - Fehler beim Festplattenlaufwerk
  - Ausfall des Netzteils
  - Ausfall der SSL-Karte
  - Warmer Neustart
  - Speicheranomalien
  - Das Ratenlimit wird gesenkt

- **Benötigen Sie eine separate Lizenz für Call Home?**

  Nein, Call Home benötigt keine separate Lizenz. Sie können es in allen NetScaler-Plattformlizenzen aktivieren.

- **Welche Daten sendet Call Home an den NetScaler-Supportserver und wie oft werden sie gesendet?**

  Call Home sammelt und sendet zwei Arten von Daten an die CIS. Sie sind:

  - Grundlegende Systeminformationen (laufende NetScaler-Version, Bereitstellungsmodus (Standalone, HA, Cluster), Hardwaredetails usw.). Es wird zum Zeitpunkt der Call Home-Registrierung und im Rahmen von regelmäßigen Herzschlägen gesendet. Der Herzschlag wird einmal alle 30 Tage gesendet, aber Sie können dieses Intervall zwischen 1 und 30 Tagen konfigurieren. Ein Wert von weniger als 5 Tagen wird jedoch nicht empfohlen, da häufige Uploads normalerweise nicht sehr nützlich sind.
  - Eine abgekürzte Version von, `show tech support bundle` wenn eine Fehlerbedingung vorliegt. Sie wird beim ersten Auftreten einer bestimmten Fehlerbedingung seit dem letzten Start der Appliance gesendet. Das heißt, ein erneutes Auftreten derselben Fehlerbedingung löst keinen weiteren Upload aus, es sei denn, die Appliance wurde nach dem vorherigen Auftreten neu gestartet.

- **Kann Call Home Systemprotokolle über einen Proxyserver generieren und hochladen?**

  Ja. Wenn Ihre NetScaler-Appliance nicht über eine direkte Internetverbindung verfügt, können Sie einen Proxyserver konfigurieren und Systemprotokolle auf den Citrix Technical Support Server (CIS) hochladen.

- **Kann ich Call Home Daten überprüfen, bevor sie an CIS gesendet werden?**

  Leider können Sie Call Home Daten nicht überprüfen, bevor sie an CIS gesendet werden. Call Home sammelt neben den Daten, die Sie bei der Kontaktaufnahme mit dem NetScaler-Supportteam angeben, keine weiteren Daten.

- **Wie sicher und privat sind die Call Home Uploads?**

  Call Home bietet Datensicherheit und Datenschutz auf folgende Weise:

  - Verwendet einen sicheren SSL/TLS-Kanal, um Daten an Citrix-Server zu übertragen.
  - Hochgeladene Daten werden nur von autorisiertem Personal überprüft und nicht an Dritte weitergegeben.

Clustering

August 19, 2021

Klicken Sie hier für häufig gestellte Fragen zum Clustering.

Verbindungsverwaltung

May 11, 2023

- **Was ist eine Admin-Verbindung?**

  Eine Admin-Verbindung stellt eine Verbindung zur NSIP-Adresse her und ermöglicht es Administratoren, die NetScaler-Appliance zu konfigurieren und zu überwachen.

- **Was sind die Arten von Admin-Verbindungen?**

  Es gibt zwei Arten von Admin-Verbindungen:

  - SSH-Verbindung — Admin-Benutzer verwenden einen SSH-Client, um sich über die NSIP-Adresse anzumelden.
  - NITRO-API-Verbindung — Admin-Benutzer verwenden NITRO-APIs, um den Anmeldeprozess bei der NetScaler Appliance zu automatisieren.

> **Hinweis**
>
> Admin-Benutzer können sich auch über die GUI anmelden, um sich anzumelden, indem sie einen Browser verwenden, um sich mit der NSIP-Adresse zu verbinden. Die GUI öffnet intern eine NI-

> TRO API-Verbindung. Daher entspricht eine GUI-Sitzung einer NITRO-API-Verbindung, und FAQs im Zusammenhang mit der NITRO-API gelten für die GUI.

- **Wie viele gleichzeitige Administratorverbindungen sind auf einer NetScaler Appliance zulässig?**

  Die Appliance ermöglicht bis zu 20 gleichzeitige Admin-Verbindungen.

- **Welche Anmeldeinformationen sind für eine Administratoranmeldung erforderlich?**

  Für die Administratoranmeldung sind ein Benutzername und ein Passwort erforderlich.

  Hinweis: Ein Authentifizierungsschlüssel kann anstelle eines Passworts verwendet werden.

- **Welche externen Authentifizierungsmethoden unterstützt eine NetScaler-Appliance?**

  Die Appliance unterstützt die folgenden externen Authentifizierungsmethoden:

  - RADIUS
  - LDAP
  - TACACS

- **Was ist ein Kunde?**

  Ein Client ist ein Gerät (Laptop oder Desktop), das vom Admin-Benutzer verwendet wird, um eine Admin-Verbindung zu öffnen.

- **Was ist ein Sitzungstoken?**

  Ein Sitzungstoken ist eine eindeutige Kennung, die die NetScaler-Appliance an einen Client ausgibt, der eine NITRO-API-Anmeldeanforderung sendet.

  - API-Clients können das Sitzungstoken wiederverwenden, wenn es nicht abgelaufen ist, für nachfolgende API-Anforderungen für neue TCP-Verbindungen
  - GUI-Clients öffnen intern NITRO-API-Verbindungen und halten das Sitzungstoken während der GUI-Sitzung aktiv.

- **Was ist eine aktive Sitzung auf einer NetScaler Appliance?**

  Eine CLI-Sitzung gilt als aktiv, wenn die Sitzung nicht abgelaufen ist und eine offene SSH-Verbindung mit einer NetScaler-Appliance besteht.

  Eine NITRO-API-Sitzung gilt als aktiv, wenn das Timeout für das Sitzungstoken auf der NetScaler-Appliance nicht abgelaufen ist.

- **Wie setzt NetScaler das Limit für gleichzeitige Verbindungen durch?**

  Jedes Mal, wenn die NetScaler-Appliance eine Administratorverbindungsanfrage (SSH oder NITRO API) empfängt, überprüft sie die Anzahl der geöffneten Admin-Verbindungen. Wenn die Zahl niedriger als 20 ist, wird eine neue Verbindung geöffnet.

- **Welcher Zähler gibt die Anzahl der Administratorverbindungen auf einer NetScaler-Appliance an?**

  Der Verbindungszähler (nsconfigd_cur_clients) gibt die Anzahl der aktiven Verbindungen an. Dieser Zähler wird erhöht, wenn ein Client eine neue Verbindung zur Appliance herstellt, und er wird verringert, wenn eine Verbindung geschlossen wird.

- **Welcher Leistungsindikator spiegelt die Anzahl der aktiven Token auf der NetScaler Appliance wider?**

  Der Zähler *configd_cur_tokens* spiegelt die Anzahl der aktiven Token auf der NetScaler Appliance wider.

- **Wie behandelt NetScaler Appliance Fehler bei einer Verbindung?**

  Die NetScaler-Appliance schließt sofort die Client-Verbindung (CLI, API und GUI), wenn bei einer Verbindung Fehler auftreten.

- **Wird eine CLI- oder GUI-Sitzung auf einer Verbindung zur Verwaltungsadresse auf das Admin-Verbindungslimit angerechnet?**

  Ja, alle CLI- und GUI-Verbindungen sind TCP-basierte Verbindungen, und jede TCP-Verbindung zur Verwaltungsadresse wird auf das Admin-Verbindungslimit angerechnet.

- **Wird eine NITRO-Sitzung auf das Admin-Verbindungslimit angerechnet?**

  Eine NITRO-Sitzung wird auf das Admin-Verbindungslimit angerechnet, wenn eine offene TCP-Verbindung mit dem von der NetScaler-Appliance ausgegebenen Sitzungstoken besteht.

- **Was ist der standardmäßige Zeitüberschreitungszeitraum für API-, GUI- und CLI-Sitzungen auf der NetScaler Appliance?**

  In der folgenden Tabelle wird der Standard-Timeout-Zeitraum für API-, GUI- und CLI-Sitzungen auf der NetScaler Appliance aufgeführt:

NetScaler Versionen	CLI Standard-Timeout-Periode (min)	API-Standard-Timeout-Periode (min)	Standard-Timeout-Periode für die GUI (min)
NetScaler 9.3	Ohne	30 Minuten	30 Minuten
NetScaler 10.1	Ohne	30 Minuten	30 Minuten
NetScaler 10.5 und höher	15 Minuten	30 Minuten	15 Minuten

- **Wie können Sie das Timeout der CLI-Sitzungen auf einer NetScaler Appliance festlegen?**

  Das CLI-Sitzungs-Timeout kann konfiguriert werden, indem Sie den folgenden Befehl an der

CLI-Eingabeaufforderung ausführen:

```
set cli mode -timeout \<xx seconds>
```

- **Wie überschreiben Sie die standardmäßige Zeitüberschreitung bei Verwendung der NITRO API?**

  Sie können den Standard-Timeoutzeitraum für eine NITRO-API überschreiben, indem Sie die Timeout-Dauer im Feld „Timeout“ des Anmeldeobjekts festlegen. Wenn das Sitzungs-Timeout auf Null gesetzt ist, hat das Sitzungstoken ein unendliches Timeout.

  Hinweis: Ein unendliches Timeout ist nicht ratsam, da Sitzungen ohne Timeout weiterhin auf die Anzahl der Admin-Verbindungen angerechnet werden.

- **Was passiert, wenn ein Benutzerkonto aus der NetScaler Appliance gelöscht wird, nachdem eine Administratorsitzung erstellt wurde?**

  Für interne Systembenutzer schließt die NetScaler Appliance die vorhandene CLI- oder NITRO-API-Sitzung.

  Für externe Systembenutzer bleibt die Sitzung aktiv, bis sie abläuft.

- **Können NITRO API-Clients ein einzelnes Session-Token verwenden, um mehrere Admin-Verbindungen auf der NetScaler Appliance zu öffnen?**

  Ja. Jede dieser Verbindungen wird auf das Admin-Verbindungslimit angerechnet.

- **Wenn der Verwaltungszugriff für eine SNIP-Adresse aktiviert ist, werden Admin-Verbindungen zu dieser Adresse mit dem Limit für die Anzahl der Admin-Verbindungen angerechnet?**

  Ja, Administratorverbindungen zur Verwaltungsadresse (SNIP) zählen auf das Admin-Verbindungslimit von NetScaler.

- **Kann sich ein NetScaler Administrator bei der NetScaler Appliance anmelden, nachdem die maximale Verbindungsgrenze erreicht ist?**

  Ja. Eine weitere Admin-Verbindung ist zulässig, nachdem das maximale Verbindungslimit erreicht wurde.

- **Können NITRO API-Endpunkte mehrere Admin-Verbindungen auf NetScaler der Appliance öffnen?**

  Ja, NITRO API-Endpunkte können mehrere Admin-Verbindungen öffnen und das Limit für die gleichzeitige Admin-Verbindung auf einer NetScaler Appliance ausschöpfen. In solchen Situationen ist eine zusätzliche SSH/CLI-Verbindung zulässig, und der Administrator kann das Schließen alter API-Sitzungen erzwingen oder die Dauer des Sitzungstimeouts für die vorhandenen API-Sitzungen reduzieren.

- **Kann ein Client mehrere API-Sitzungen auf einer NetScaler Appliance öffnen?**

  Ja, ein Client kann mehrere API-Sitzungen öffnen, indem er sich wiederholt anmeldet. Beispielsweise kann sich der Client nach einem Neustart wieder anmelden.
  Hinweis: Wiederholte Client-Anmeldungen werden auf das Admin-Verbindungslimit der NetScaler Appliance angerechnet.

- **Können API-Clients das gesamte Token-Limit für API-Sitzungen verwenden?**

  Ja, API-Clients können das gesamte Token-Limit für API-Sitzungen nutzen, das durch wiederholte Anmeldung bereitgestellt wird, ohne ein zuvor ausgegebenes Token zu verwenden.

  Hinweis: Wenn das Sitzungs-Timeout eines Clients Null ist, ist das Token für immer gültig. Wiederholte Anmeldungen mit neuen Sitzungstoken können auf das Limit für API-Sitzungstoken angerechnet werden.

- **Werden CLI-Sitzungen auf das API-Sitzungstoken-Limit angerechnet?**

  Nein, CLI-Sitzungen werden nicht auf das Token-Limit für API-Sitzungen angerechnet.

- **Können Admin-Benutzer Telnet verwenden, um eine CLI-Sitzung zu öffnen?**

  Nein. Nur ein SSH-Client kann eine CLI-Sitzung öffnen.

- **Welches Verbindungslimit und welches API-Sitzungslimit gelten für verschiedene NetScaler-Versionen?**

  In der folgenden Tabelle sind die maximalen Grenzwerte für gleichzeitige Administratorverbindungen und aktive API-Sitzungen aufgeführt, die für verschiedene NetScaler-Versionen gelten:

NetScaler Versionen	9.3	10.1 (Vor 130.x)	10.1 (Vor 130.10)	10.1 (Ab 130,10)
Maximale Anzahl gleichzeitiger Admin-Verbindungen	20	20	20	20
Maximale Anzahl aktiver API-Sitzungen*	1000	20	1000	1000

Hinweis:

- API-Sitzungen gelten als aktiv, wenn kein Timeout vorliegt. Wenn beispielsweise 500 API-Sitzungen erstellt wurden, 100 jedoch abgelaufen sind, sind 400 API-Sitzungen aktiv.
- Eine API-Sitzung muss keine TCP-Verbindung zur NetScaler-Appliance öffnen.

Content Switching

May 11, 2023

- **Ich habe eine Nicht-NetScaler-Lastausgleichs-Appliance im Netzwerk installiert. Ich möchte jedoch die Content Switching-Funktion der NetScaler-Appliance verwenden, um die Clientanforderungen an die Lastausgleichs-Appliance weiterzuleiten. Ist es möglich, die Content Switching-Funktion der NetScaler-Appliance mit einer Nicht-NetScaler-Lastausgleichs-Appliance zu verwenden?**

  Ja. Sie können die Content Switching-Funktion der NetScaler-Appliance mit der Lastausgleichsfunktion der NetScaler-Appliance oder einer Nicht-NetScaler-Lastausgleichs-Appliance verwenden. Wenn Sie jedoch die Nicht-NetScaler-Lastausgleichs-Appliance verwenden, stellen Sie sicher, dass Sie einen virtuellen Lastausgleichsserver auf der NetScaler-Appliance erstellen und ihn als Dienst an die Nicht-NetScaler-Lastausgleichs-Appliance binden.

- **Wie unterscheidet sich ein virtueller Content Switching-Server von einem virtuellen Lastausgleichsserver?**

  Ein virtueller Content Switching-Server kann die Clientanforderungen nur an andere virtuelle Server senden. Es kommuniziert nicht mit den Servern.

  Ein virtueller Lastausgleichsserver gleicht die Clientlast zwischen Servern aus und kommuniziert mit den Servern. Es überwacht die Serververfügbarkeit und kann verwendet werden, um verschiedene Lastausgleichsalgorithmen zur Verteilung der Verkehrslast anzuwenden.

  Content Switching ist eine Methode, mit der Clientanforderungen für bestimmte Arten von Inhalten über Lastausgleich virtueller Server an Zielserver weitergeleitet werden. Sie können die Clientanfragen an die Server weiterleiten, die für ihre Bearbeitung am besten geeignet sind. Dies führt zu geringeren Gemeinkosten für die Bearbeitung der Clientanforderungen auf den Servern.

- **Ich möchte die Content Switching-Funktion der NetScaler-Appliance implementieren, um die Clientanforderungen zu leiten. Welche Arten von Kundenanfragen kann ich mithilfe der Content Switching-Funktion richten?**

  Mithilfe der Content Switching-Funktion können Sie nur HTTP-, HTTPS-, FTP-, TCP-, Secure TCP- und RTSP-Clientanforderungen leiten. Um HTTPS-Clientanforderungen weiterzuleiten, müssen Sie die SSL-Offload-Funktion auf der Appliance konfigurieren.

- **Ich möchte Content Switching-Regeln auf der NetScaler-Appliance erstellen. Was sind die verschiedenen Elemente der Kundenanfrage, für die ich eine Content Switching-Regel erstellen kann?**

  Sie können die Content Switching-Regeln basierend auf den folgenden Elementen und ihren Werten in der Clientanforderung erstellen:

  - URL
  - URL-Token
  - HTTP-Version
  - HTTP-Header
  - Quell-IP-Adresse des Clients
  - Version des Clients
  - Ziel-TCP-Port

- **Ich verstehe, dass die Content Switching-Funktion der NetScaler-Appliance dazu beiträgt, die Leistung des Netzwerks zu verbessern. Stimmt das?**

  Ja. Sie können die Clientanfragen an die Server weiterleiten, die am besten geeignet sind, um sie zu bearbeiten. Das Ergebnis ist ein reduzierter Overhead für die Verarbeitung der Clientanforderungen auf den Servern.

- **Welche Funktion der NetScaler-Appliance sollte ich auf der NetScaler-Appliance konfigurieren, um die Site-Verwaltbarkeit und die Reaktionszeit auf die Clientanforderungen zu verbessern?**

  Sie können Content Switching in der NetScaler-Appliance konfigurieren, um die Site-Verwaltbarkeit und die Reaktionszeit auf die Clientanforderung zu verbessern. Mit dieser Funktion können Sie Content-Gruppen innerhalb desselben Domainnamens und derselben IP-Adresse erstellen. Dieser Ansatz ist flexibel, im Gegensatz zu dem üblichen Ansatz, den Inhalt explizit in verschiedene Domänennamen und IP-Adressen zu partitionieren, die für den Benutzer sichtbar sind.

  Mehrere Partitionen, die eine Website in verschiedene Domänennamen und IP-Adressen aufteilen, zwingen den Browser, für jede Domäne, die sie beim Rendern und Abrufen des Inhalts einer Webseite findet, eine separate Verbindung herzustellen. Diese zusätzlichen WAN-Verbindungen beeinträchtigen die Reaktionszeit für die Webseite.

- **Ich habe eine Website in einer Webserverfarm gehostet. Welche Vorteile bietet die NetScaler Content Switching-Funktion für diese Art von Setup?**

  Die Funktion zum Content Switching bietet die folgenden Vorteile auf einer NetScaler-Appliance auf einer Site, die auf einer Webserverfarm basiert:

  - Verwalten Sie den Inhalt der Website, indem Sie eine Content-Gruppe innerhalb derselben Domäne und IP-Adresse erstellen.
  - Erhöhen Sie die Reaktionszeit auf Clientanfragen, indem Sie die Content-Gruppe innerhalb derselben Domäne und IP-Adresse verwenden.
  - Vermeiden Sie die Notwendigkeit einer vollständigen domänenübergreifenden Inhaltsreplikation.
  - Aktivieren Sie die anwendungsspezifische Content-Partitionierung. Beispielsweise können Sie Clientanforderungen an einen Server weiterleiten, der nur dynamische Inhalte

oder nur statische Inhalte verarbeitet, sofern dies für die Anforderung angemessen ist.
  - Unterstützt das Multi-Homing mehrerer Domains auf demselben Server und verwendet dieselbe IP-Adresse.
  - Verwenden Sie Verbindungen zu den Servern wieder.

- **Ich möchte die Funktion zum Content Switching auf der NetScaler-Appliance implementieren. Ich möchte die Clientanfragen an die verschiedenen Server weiterleiten, nachdem ich die verschiedenen Parameter jeder Anfrage ausgewertet habe. Welchen Ansatz sollte ich verfolgen, um dieses Setup bei der Konfiguration der Content Switching-Funktion zu implementieren?**

  Sie können Richtlinienausdrücke verwenden, um Richtlinien für die Funktion zum Content Switching zu erstellen. Ein Ausdruck ist eine Bedingung, die ausgewertet wird, indem die Qualifikatoren der Clientanforderung mithilfe eines Operators mit einem Operanden verglichen werden. Sie können die folgenden Parameter der Clientanforderung verwenden, um einen Ausdruck zu erstellen:

  - **Methode**- HTTP-Anforderungsmethode.
  - **URL** - URL im HTTP-Header.
  - **URL-TOKEN** - Spezielle Token in der URL.
  - **VERSION** - Version der HTTP-Anfrage.
  - **URL QUERY** - Enthält die URL-Abfrage LEN, URL LEN und HTTP-Header.
  - **SOURCEIP** - IP-Adresse des Clients.

  Es folgt eine vollständige Liste der Operatoren, mit denen Sie einen Ausdruck erstellen können:

  - == (ist gleich)
  - ! = (ist nicht gleich)
  - EXISTS
  - NOT EXISTS
  - CONTAINS
  - NOT CONTAINS
  - GT (größer als)
  - LT (weniger als)

Sie können auch verschiedene Regeln erstellen, bei denen es sich um logische Aggregationen einer Reihe von Ausdrücken handelt. Sie können mehrere Ausdrücke kombinieren, um Regeln zu erstellen. Um Ausdrücke zu kombinieren, können Sie && (UND) und	(ODER) Betreiber. Sie können auch Klammern verwenden, um verschachtelte und komplexe Regeln zu erstellen.

- **Ich möchte eine regelbasierte Richtlinie zusammen mit einer URL-basierten Richtlinie für denselben virtuellen Content Switching-Server konfigurieren. Ist es möglich, beide Arten von Richtlinien für denselben virtuellen Content Switching-Server zu erstellen?**

  Ja. Sie können beide Arten von Richtlinien für denselben virtuellen Content Switching-Server erstellen. Stellen Sie jedoch sicher, dass Sie Prioritäten zuweisen, um einen angemessenen Vorrang für die Richtlinien festzulegen.

- **Ich möchte Content Switching-Richtlinien erstellen, die den Domainnamen zusammen mit einem Präfix und Suffix einer URL auswerten und die Clientanforderungen entsprechend leiten. Welche Art von Content Switching-Richtlinie sollte ich erstellen?**

  Sie können eine Richtlinie für Domäne und exakte URLs erstellen. Wenn diese Art von Richtlinie ausgewertet wird, wählt die NetScaler-Appliance eine Content-Gruppe aus, wenn der vollständige Domänenname und die URL in der Clientanforderung mit den konfigurierten übereinstimmen. Die Clientanforderung muss mit dem konfigurierten Domänennamen übereinstimmen und genau mit dem Präfix und Suffix der URL übereinstimmen, wenn sie konfiguriert sind.

- **Ich möchte Richtlinien zum Content Switching erstellen, die den Domainnamen zusammen mit einem teilweisen Präfix und Suffix der URL auswerten und die Clientanforderungen entsprechend leiten. Welche Art von Content Switching-Richtlinie sollte ich erstellen?**

  Sie können eine Domäne- und Platzhalter-URL-Richtlinie für den virtuellen Content Switching-Server erstellen. Wenn diese Art von Richtlinie ausgewertet wird, wählt die NetScaler-Appliance eine Content-Gruppe aus, wenn die Anforderung dem vollständigen Domänennamen entspricht und teilweise dem URL-Präfix entspricht.

- **Was ist eine Platzhalter-URL-Richtlinie?**

  Sie können Platzhalter verwenden, um teilweise URLs in Clientanforderungen an die URL auszuwerten, die Sie auf der NetScaler-Appliance konfiguriert haben. Sie können Platzhalter

in den folgenden Arten von URL-basierten Richtlinien verwenden:

- Nur Präfix. Der Ausdruck /sports/* entspricht beispielsweise allen URLs, die unter der URL /sports verfügbar sind. In ähnlicher Weise stimmt der Ausdruck /sports * mit allen URLs überein, deren Präfix /sports lautet.
- Nur Suffix. Zum Beispiel stimmt der Ausdruck /*.jsp mit allen URLs mit einer Dateinamenerweiterung von jsp überein.
- Präfix und Suffix. Der Ausdruck /sports/ *.jsp entspricht beispielsweise allen URLs unter der /sports/ URL, die auch die JSP-Dateinamenerweiterung haben. In ähnlicher Weise entspricht der Ausdruck /sports *.jsp alle URLs mit einem Präfix von /sports * und einer Dateinamenerweiterung von jsp.

- **Was ist eine Domänen- und Regelrichtlinie?**

  Wenn Sie eine Domäne- und Regelrichtlinie erstellen, muss die Clientanforderung mit der vollständigen Domäne und der auf der NetScaler-Appliance konfigurierten Regel übereinstimmen.

- **Was ist die Standardvorgabe für die Bewertung von Richtlinien?**

  Standardmäßig werden die regelbasierten Richtlinien zuerst ausgewertet.

- **Wenn ein Teil des Inhalts für alle Clientanforderungen identisch ist, welche Art von Priorität sollte ich für die Bewertung von Richtlinien verwenden?**

  Wenn ein Teil des Inhalts für alle Benutzer gleich ist und verschiedene Inhalte auf der Grundlage von Clientattributen bereitgestellt werden müssen, können Sie die URL-basierte Priorität für die Richtlinienbewertung verwenden.

- **Welche Policy-Express-Syntax wird beim Content Switching unterstützt?**

  Content Switching unterstützt zwei Arten von Richtlinienausdrücken:

  - **Klassische Syntax -** Klassische Syntax beim Content Switching beginnt mit dem Schlüsselwort REQ und ist weiter fortgeschritten als die Advanced-Richtlinie. Klassische Richtlinien können nicht an eine Aktion gebunden werden. Daher kann der virtuelle Zielserver für Lastenausgleich erst hinzugefügt werden, nachdem der virtuelle Content Switching-Server gebunden wurde.
  - **Erweiterte Richtlinie:** Erweiterte Richtlinien beginnen im Allgemeinen mit dem Schlüsselwort HTTP und sind einfacher zu konfigurieren. Eine virtuelle Ziel-Lastenausgleichsaktion kann an eine erweiterte Richtlinie gebunden werden, und die Richtlinie kann auf mehreren virtuellen Servern mit Content Switching verwendet werden.

- **Kann ich eine einzelne Content Switching-Richtlinie an mehrere virtuelle Server binden?**

  Ja. Sie können eine einzelne Content Switching-Richtlinie an mehrere virtuelle Server binden, indem Sie Richtlinien mit definierten Aktionen verwenden. Content Switching-Richtlinien, die eine Aktion verwenden, können an mehrere virtuelle Server mit Content Switching gebunden

werden, da der virtuelle Ziel-Lastausgleichsserver nicht mehr in der Content Switching-Richtlinie angegeben ist. Die Möglichkeit, eine einzelne Richtlinie an mehrere virtuelle Content Switching-Server zu binden, trägt dazu bei, die Größe der Content Switching-Konfiguration weiter zu reduzieren.

Weitere Informationen finden Sie in den folgenden Knowledge Center-Artikeln und in den NetScaler-Dokumentationsthemen:

- Siehe CTX122918 - Binden der gleichen Content Switching-Richtlinie an einen virtuellen Server mit zwei Content Switching auf einer NetScaler-Appliance.
- Weitere Informationen finden Sie unter CTX122736 - Binden derselben erweiterten Richtlinie an mehrere virtuelle Server mit Content Switching mithilfe von Richtlinienbeschriftungen.
- Konfigurieren von Basic Content Switching

- **Kann ich eine aktionsbasierte Richtlinie mit klassischen Ausdrücken erstellen?**

  Nein. Ab sofort unterstützt NetScaler keine Richtlinien, die klassische Syntaxausdrücke mit Aktionen verwenden. Der virtuelle Ziel-Lastenausgleichsserver muss beim Binden der Richtlinie hinzugefügt werden, anstatt ihn in einer Aktion zu definieren.

Debuggen

May 11, 2023

- **Wie kann ich die Schnittstelle (CLI, GUI oder API) ermitteln, über die eine Operation ausgeführt wurde?**

  Der NetScaler verfolgt die Schnittstellen, über die Operationen ausgeführt werden. Sie können diese Informationen in Syslogs (navigieren Sie in der GUI zu
  Konfiguration > System > Auditing > Prüfmeldungen > Syslog-Meldungen) oder in der Datei ns.log (im Verzeichnis /var/log/) einsehen.

  Beispielsweise werden Operationen, die über die API ausgeführt werden, als „API CMD_EXECUTED“ gekennzeichnet. „

Hardware

April 19, 2023

Klicken Sie hier für häufig gestellte Fragen zur MPX-Hardware.

Hohe Verfügbarkeit

August 19, 2021

- **Welche Ports werden verwendet, um die HA-bezogenen Informationen zwischen den Knoten in einer HA-Konfiguration auszutauschen?**

  In einer HA-Konfiguration verwenden beide Knoten die folgenden Ports, um Informationen für HA auszutauschen:

  - UDP-Port 3003, zum Austausch von Heartbeat-Paketen
  - Port 3010, für Synchronisation und Befehlsausbreitung

- **Welche Konfigurationen werden nicht in einer HA-Konfiguration im INC- oder Nicht-INC-Modus synchronisiert oder weitergegeben?**

  Konfigurationen, die mit den folgenden Befehlen implementiert werden, werden weder propagiert noch mit dem sekundären Knoten synchronisiert:

  - Alle knotenspezifischen HA-Konfigurationsbefehle. Zum Beispiel `add ha nodeset ha node`, und `bind ha node`.
  - Alle Interface-bezogenen Konfigurationsbefehle. Zum Beispiel, setzen Sie Schnittstelle und unset interface.
  - Alle kanalbezogenen Konfigurationsbefehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.

  Weitere Informationen zur HA-Konfiguration im INC-Modus finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

- **Welche Konfigurationen werden in einer HA-Konfiguration im INC-Modus nicht synchronisiert oder weitergegeben?**

  Die folgenden Konfigurationen werden weder synchronisiert noch weitergegeben. Jeder Knoten hat seinen eigenen.

  - MIPs
  - SNIPs
  - VLANs
  - Routen (außer LLB-Routen)
  - Routenüberwachung
  - RNAT Regeln (außer RNAT Regel mit VIP als NAT IP)
  - Dynamische Routing-Konfigurationen.

- **Was sind die Bedingungen, die die Synchronisation auslösen?**

  Die Synchronisierung wird durch eine der folgenden Bedingungen ausgelöst:

- Die Inkarnationsnummer des primären Knotens, der vom sekundären empfangen wird, stimmt nicht mit der des sekundären Knotens überein.
  Hinweis: Beide Knoten in einer HA-Konfiguration behalten einen Leistungsindikator namens *Inkarnationsnummer*, der die Anzahl der Konfigurationen in der Konfigurationsdatei des Knotens zählt. Jeder Knoten sendet seine Inkarnationsnummer an jeden anderen Knoten in den Heartbeat-Nachrichten. Die Inkarnationsnummer wird für die folgenden Befehle nicht erhöht:
  * Alle HA-Konfigurationsbefehle. Zum Beispiel `add ha nodeset ha node`, und `bind ha node`.
  * Alle Interface-bezogenen Befehle. Zum Beispiel, setzen Sie Schnittstelle und unset interface.
  * Alle kanalbezogenen Befehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.
- Der sekundäre Knoten wird nach einem Neustart angezeigt.
- Der primäre Knoten wird nach einem Failover sekundär.

- **Wird eine dem sekundären Knoten hinzugefügte Konfiguration auf dem primären Knoten synchronisiert?**

  Nein, eine dem sekundären Knoten hinzugefügte Konfiguration wird nicht mit dem primären Knoten synchronisiert.

- **Was könnte der Grund dafür sein, dass beide Knoten die primäre in einer HA-Konfiguration sein?**

  Der wahrscheinlichste Grund ist, dass der primäre und sekundäre Knoten beide fehlerfrei sind, aber der sekundäre nicht die Heartbeat-Pakete vom primären erhalten. Das Problem kann mit dem Netzwerk zwischen den Knoten liegen.

- **Steht bei einer HA-Konfiguration Probleme auf, wenn Sie die beiden Knoten mit unterschiedlichen Systemtakteinstellungen bereitstellen?**

  Unterschiedliche Systemtakteinstellungen auf den beiden Knoten können folgende Probleme verursachen:

  - Die Zeitstempel in den Protokolldateieinträgen stimmen nicht überein. Diese Situation macht es schwierig, die Protokolleinträge auf Probleme zu analysieren.
  - Nach einem Failover können Probleme mit jeder Art von Cookie-basierte Persistenz für den Lastenausgleich auftreten. Ein signifikanter Unterschied zwischen den Zeiten kann dazu führen, dass ein Cookie früher als erwartet abläuft, was zur Beendigung der Persistenzsitzung führt.
  - Ähnliche Überlegungen gelten für zeitbezogene Entscheidungen auf den Knoten.

- **Was sind die Bedingungen für den Ausfall des Befehls *force HA-Synchronisierung* ?**

  Die erzwungene Synchronisierung schlägt unter folgenden Umständen fehl:

  - Sie erzwingen die Synchronisierung, wenn die Synchronisation bereits ausgeführt wird.
  - Der sekundäre Knoten ist deaktiviert.
  - HA-Synchronisierung ist auf dem aktuellen sekundären Knoten deaktiviert.
  - Die HA-Propagierung ist auf dem aktuellen primären Knoten deaktiviert, und Sie erzwingen die Synchronisierung vom primären Knoten.

- **Was sind die Bedingungen für den Ausfall des Befehls “ *HA-Dateien synchronisieren* “?**

  Die Synchronisierung von Konfigurationsdateien schlägt fehl, wenn der sekundäre Knoten deaktiviert ist.

- **Wenn der sekundäre Knoten in einer HA-Konfiguration als primärer Knoten übernimmt, wechselt er in den sekundären Status zurück, wenn der ursprüngliche primäre Knoten wieder online ist?**

  Nein. Nachdem der sekundäre Knoten als primärer Knoten übernommen hat, bleibt er auch dann als primär, wenn der ursprüngliche primäre Knoten wieder online ist. Führen Sie zum Austausch des primären und sekundären Status der Knoten den Befehl *force failover* aus.

- **Was sind die Bedingungen für den Ausfall des *Force-Failover-Befehls*?**

  Ein erzwungenes Failover schlägt unter folgenden Umständen fehl:

  - Der sekundäre Knoten ist deaktiviert.
  - Der sekundäre Knoten ist so konfiguriert, dass er sekundär bleibt.
  - Der primäre Knoten ist so konfiguriert, dass er primär bleibt.
  - Der Status des Peer-Knotens ist unbekannt.

Integriertes Caching

May 11, 2023

Gruppen von Inhalten

- **Wie unterscheidet sich eine DEFAULT-Inhaltsgruppe von anderen Inhaltsgruppen?**

  Das Verhalten der DEFAULT-Inhaltsgruppe ist dasselbe wie bei jeder anderen Gruppe. Das einzige Attribut, das die DEFAULT-Inhaltsgruppe zu etwas Besonderem macht, ist das, wenn ein Objekt zwischengespeichert wird und keine Inhaltsgruppe erstellt wurde. Das Objekt wird in der DEFAULT-Gruppe zwischengespeichert.

- **Was ist die Option „Cache-Control“ auf Inhaltsgruppenebene?**

Sie können jeden Cache-Control-Header an den Browser senden. Es gibt eine Option auf Inhaltsgruppenebene, -CacheControl, mit der Sie den Cache-Control-Header angeben können, der in die Antwort an den Browser eingefügt werden soll.

- **Was ist die Option Minhit auf der Ebene der Inhaltsgruppen?**

  `Minhit` ist ein ganzzahliger Wert, der die Mindestanzahl der Auswahl für eine Cache-Richtlinie angibt, bevor das Objekt zwischengespeichert wird. Dieser Wert ist auf Inhaltsgruppenebene konfigurierbar. Im Folgenden finden Sie die Syntax, um diesen Wert über die CLI zu konfigurieren.

  ```
  add/set cache contentGroup \<Content_Group_Name> [-minHits \<Integer>]
  ```

- **Was nützt die Option expireAtLastByte?**

  Die Option expireAtLastByte ermöglicht es dem integrierten Cache, das Objekt ablaufen zu lassen, wenn es heruntergeladen wird. Nur Anfragen, bei denen es sich um ausstehende Anfragen handelt, werden dann aus dem Cache bedient. Alle neuen Anfragen werden an den Server gesendet. Diese Einstellung ist nützlich, wenn das Objekt häufig geändert wird, wie dies bei Aktienkursen der Fall ist. Dieser Ablaufmechanismus funktioniert zusammen mit der Flash-Cache-Funktion. Führen Sie den folgenden Befehl über die CLI aus, um eine ExpireAtLastByte-Option zu konfigurieren:

  ```
  add cache contentGroup \<Group_Name> -expireAtLastByte YES
  ```

Cache-Richtlinie

- **Was ist eine Caching-Richtlinie?**

  Richtlinien bestimmen, welche Transaktionen zwischengespeichert werden können und welche nicht. Außerdem fügen Richtlinien das standardmäßige HTTP-Caching-Verhalten hinzu oder überschreiben es. Richtlinien bestimmen eine Aktion, wie CACHE oder NOCACHE, abhängig von den spezifischen Merkmalen der Anfrage oder Antwort. Wenn eine Antwort den Richtlinienregeln entspricht, wird das Objekt in der Antwort der in der Richtlinie konfigurierten Inhaltsgruppe hinzugefügt. Wenn Sie keine Inhaltsgruppe konfiguriert haben, wird das Objekt der DEFAULT-Inhaltsgruppe hinzugefügt.

- **Was ist ein Policy-Hit?**

  Eine Auswahl erfolgt, wenn eine Anfrage oder Antwort mit einer Cache-Richtlinie übereinstimmt.

- **Was ist ein Fehlschuss?**

  Ein Fehler tritt auf, wenn eine Anfrage oder Antwort keiner Cache-Richtlinie entspricht. Ein Fehler kann auch auftreten, wenn die Anfrage oder Antwort mit einer Cache-Richtlinie übere-

instimmt, aber eine Überschreibung des RFC-Verhaltens verhindert, dass das Objekt im Cache gespeichert wird.

- **Ich habe die integrierte Caching-Funktion der NetScaler-Appliance konfiguriert. Beim Hinzufügen der folgenden Richtlinie wird eine Fehlermeldung angezeigt. Gibt es einen Fehler im Befehl?**

  ```
  add cache policy image_caching -rule exp1 | ns_ext_not_jpeg -action
  cache
  ```

  ```
  \> ERROR: No such command
  ```

  Im vorherigen Befehl muss der Ausdruck innerhalb der Anführungszeichen stehen. Ohne Anführungszeichen wird der Operator als Pipeoperator betrachtet.

Speicheranforderungen

- **Welche Befehle kann ich auf der NetScaler-Appliance ausführen, um den dem Cache zugewiesenen Speicher zu überprüfen?**

  Führen Sie einen der folgenden Befehle über die CLI aus, um den für den Cache zugewiesenen Speicher in der NetScaler-Appliance anzuzeigen:

  - `show cache parameter`

    Überprüfen Sie in der Ausgabe den Wert des Parameters Speicherauslastungslimit. Dies ist der maximale Speicher, der dem Cache zugewiesen wird.

  - `show cache \<Content_Group_Name>`

    Überprüfen Sie in der Ausgabe die Werte der Parameter Speichernutzung und Speicherauslastungslimit, die den für die einzelne Inhaltsgruppe verwendeten und zugewiesenen Speicher angeben.

- **Meine NetScaler-Appliance verfügt über 2 GB Arbeitsspeicher. Gibt es ein empfohlenes Speicherlimit für den Cache?**

  Für jedes Modell der NetScaler-Appliance können Sie dem Cache die Hälfte des Speichers zuweisen. Citrix empfiehlt jedoch, aufgrund der internen Speicherabhängigkeit etwas weniger als die Hälfte des Speichers zuzuweisen. Sie können den folgenden Befehl ausführen, um dem Cache 1 GB Speicher zuzuweisen:

  ```
  set cache parameter -memLimit 1024
  ```

- **Ist es möglich, Speicherplatz für einzelne Inhaltsgruppen zuzuweisen?**

  Ja. <Content_Group_Name><Integer>Obwohl Sie Speicher für den integrierten Cache global zuweisen, indem Sie den set-Cache-Parameter —memlimit ausführen<Integer>, können Sie einzelnen Inhaltsgruppen Speicher zuweisen, indem Sie den Befehl set cache —MemLimit

ausführen. Der maximale Speicher, den Sie Inhaltsgruppen (kombiniert) zuweisen können, darf den Speicher, den Sie dem integrierten Cache zugewiesen haben, nicht überschreiten.

- **Was ist die Abhängigkeit des Speichers zwischen integriertem Cache und TCP-Puffer?**

  Wenn die NetScaler-Appliance über 2 GB Speicher verfügt, reserviert die Appliance ungefähr 800 MB bis 900 MB Arbeitsspeicher, und der Rest wird dem FreeBSD-Betriebssystem zugewiesen. Daher können Sie dem integrierten Cache bis zu 512 MB Speicher zuweisen und der Rest wird dem TCP-Puffer zugewiesen.

- **Wirkt es sich auf den Caching-Prozess aus, wenn ich dem integrierten Cache keinen globalen Speicher zuweise?**

  Wenn Sie dem integrierten Cache keinen Speicher zuweisen, werden alle Anfragen an den Server gesendet. Führen Sie den Befehl show cache parameter aus, um sicherzustellen, dass Sie dem integrierten Cache Speicher zugewiesen haben. Eigentlich werden keine Objekte zwischengespeichert, wenn der globale Speicher 0 ist, also muss er zuerst gesetzt werden.

Überprüfungsbefehle

- **Welche Optionen gibt es für die Anzeige von Cache-Statistiken?**

  Sie können eine der folgenden Optionen verwenden, um die Statistiken für den Cache anzuzeigen:

  - `stat cache`

    Um die Zusammenfassung der Cache-Statistiken anzuzeigen.

  - `stat cache -detail`

    Um die vollständigen Details der Cache-Statistik anzuzeigen.

- **Welche Optionen gibt es für die Anzeige des zwischengespeicherten Inhalts?**

  Um den zwischengespeicherten Inhalt anzuzeigen, können Sie den `show cache object` Befehl ausführen.

- **Welchen Befehl kann ich ausführen, um die Eigenschaften eines im Cache gespeicherten Objekts anzuzeigen?**

  Wenn das im Cache gespeicherte Objekt beispielsweise GET //10.102.12.16:80/index.html ist, können Sie die Details zu dem Objekt anzeigen, indem Sie den folgenden Befehl über die CLI der Appliance ausführen:

  ```
  show cache object -url '/index.html'-host 10.102.3.96 -port 80
  ```

- **Ist es zwingend erforderlich, den Gruppennamen als Parameter anzugeben, um die parametrisierten Objekte im Cache anzuzeigen?**

Ja. Es ist zwingend erforderlich, den Gruppennamen als Parameter anzugeben, um die parametrisierten Objekte im Cache anzuzeigen. Stellen Sie sich zum Beispiel vor, dass Sie die folgenden Richtlinien mit derselben Regel hinzugefügt haben:

```
add cache policy p2 -rule ns_url_path_cgibin -action CACHE -
    storeInGroup g1
add cache policy p1 -rule ns_url_path_cgibin -action CACHE -
    storeInGroup g2
<!--NeedCopy-->
```

In diesem Fall wird bei mehreren Anfragen, wenn die Richtlinie p1 ausgewertet wird, ihr Auswahlzähler erhöht und die Richtlinie speichert das Objekt in der Gruppe g1, die über Auswahlparameter verfügt. Daher müssen Sie den folgenden Befehl ausführen, um die Objekte aus dem Cache anzuzeigen:

```
show cache object -url "/cgi-bin/setCookie.pl"-host 10.102.18.152
groupName g1
```

In ähnlicher Weise wird bei einer anderen Gruppe von Mehrfachanfragen, wenn die Richtlinie p2 ausgewertet wird, ihr Auswahlzähler erhöht und die Richtlinie speichert das Objekt in der g2-Gruppe, die keine Auswahlparameter hat. Daher müssen Sie den folgenden Befehl ausführen, um die Objekte aus dem Cache anzuzeigen:

```
show cache object -url "/cgi-bin/setCookie2.pl"-host 10.102.18.152
```

- **Ich stelle fest, dass die Ausgabe des Befehls nscachemgr einige leere Einträge enthält. Was sind das für Einträge?**

  Betrachten Sie die folgende Beispielausgabe des `nscachemgr` Befehls. Die leeren Einträge in dieser Ausgabe werden für Ihre Referenz fett hervorgehoben:

```
root@ns# /netscaler/nscachemgr -a
//10.102.3.89:80/image8.png
//10.102.3.97:80/staticdynamic.html
//10.102.3.97:80/
//10.102.3.89:80/image1.png
//10.102.3.89:80/file5.html
//10.102.3.96:80/
//10.102.3.97:80/bg_logo_segue.png
//10.102.3.89:80/file500.html
//10.102.3.92:80/
//10.102.3.96:80/cgi-bin/rfc/ccProxyReval.pl
Total URLs in IC = 10
<!--NeedCopy-->
```


Die leeren Einträge in der Ausgabe sind auf die Standard-Caching-Eigenschaften für GET/HTTP/1.1 zurückzuführen.

Objekte spülen

- **Wie kann ich ein selektives Objekt aus dem Cache löschen?**

  Sie können ein Objekt anhand seiner vollständigen URL eindeutig identifizieren. Um ein solches Objekt zu leeren, können Sie eine der folgenden Aufgaben ausführen:

  - Cache leeren
  - Inhaltsgruppe leeren
  - Das spezifische Objekt leeren

  Um das spezifische Objekt zu leeren, müssen Sie die Abfrageparameter angeben. Sie geben den Parameter InvalParam an, um das Objekt zu leeren. Dieser Parameter gilt nur für eine Abfrage.

- **Löst eine Änderung der Cache-Konfiguration das Leeren des Caches aus?**

  Ja. Wenn Sie zur Cache-Konfiguration wechseln, leeren alle SET-Cache-Befehle automatisch die entsprechenden Inhaltsgruppen.

- **Ich habe die Objekte auf dem Server aktualisiert. Muss ich die zwischengespeicherten Objekte leeren?**

  Ja. Wenn Sie Objekte auf dem Server aktualisieren, müssen Sie die zwischengespeicherten Objekte oder zumindest die relevanten Objekte und Inhaltsgruppen leeren. Der integrierte Cache ist von einem Update auf dem Server nicht betroffen. Es stellt die zwischengespeicherten Objekte weiterhin bereit, bis sie ablaufen.

Flash-Cache

- **Was ist die Flash-Cache-Funktion der NetScaler-Appliance?**

  Das Phänomen Flash Crowds tritt auf, wenn viele Kunden auf dieselben Inhalte zugreifen. Das Ergebnis ist ein plötzlicher Anstieg des Datenverkehrs zum Server. Die Flash-Cache-Funktion ermöglicht es der NetScaler-Appliance, die Leistung in einer solchen Situation zu verbessern, indem nur eine Anfrage an den Server gesendet wird. Alle anderen Anfragen werden auf der Appliance in die Warteschlange gestellt und die einzige Antwort wird auf die Anfragen gesendet. Sie können einen der folgenden Befehle verwenden, um die Fast Cache-Funktion zu aktivieren:

  - `add cache contentGroup \<Group_Name> -flashCache YES`
  - `set cache contentGroup \<Group_Name> -flashCache YES`

- **Was ist das Limit für Flash-Cache-Clients?**

Die Anzahl der Flash Cache-Clients hängt von der Verfügbarkeit der Ressourcen auf der NetScaler-Appliance ab.

Standardverhalten

- **Empfängt die NetScaler-Appliance nach Ablauf proaktiv Objekte?**

  Die NetScaler-Appliance empfängt nach Ablauf niemals proaktiv Objekte. Dies gilt auch für die negativen Objekte. Der erste Zugriff nach Ablauf löst eine Anfrage an den Server aus.

- **Fügt der integrierte Cache der Warteschlange Clients für die Bereitstellung hinzu, noch bevor er die Antwort empfängt?**

  Ja. Der integrierte Cache fügt der Warteschlange Clients für die Bereitstellung hinzu, noch bevor die Antwort empfangen wird.

- **Was ist der Standardwert für den Parameter „Gecached object using überprüfen“ der Cache-Konfiguration?**

  HOSTNAME_AND_IP ist der Standardwert.

- **Erstellt die NetScaler-Appliance Protokolleinträge in den Protokolldateien?**

  Ja. Die NetScaler-Appliance erstellt Protokolleinträge in den Protokolldateien.

- **Werden komprimierte Objekte im Cache gespeichert?**

  Ja. Komprimierte Objekte werden im Cache gespeichert.

Interoperabilität mit anderen Funktionen

- **Was passiert mit Objekten, die derzeit im Cache gespeichert sind und auf die über SSL VPN zugegriffen wird?**

  Objekte, die im Cache gespeichert sind und auf die regelmäßig zugegriffen werden, werden als Cache bereitgestellt, wenn Sie über das SSL-VPN aufgerufen werden.

- **Was passiert mit Objekten, die im Cache gespeichert sind, wenn über SSL VPN zugegriffen und später über eine reguläre Verbindung zugegriffen wird?**

  Die über den SSL-VPN-Zugriff gespeicherten Objekte werden als Auswahl dienen, wenn über die reguläre Verbindung zugegriffen wird.

- **Wie unterscheide ich bei der Verwendung von Weblogs Einträge, die auf eine vom Cache bereitgehaltene Antwort hinweisen, von denen, die vom Server bedient werden?**

  Für Antworten, die aus dem integrierten Cache bereitgestellt werden, enthält das Serverlogfeld den Wert IC. Für Antworten, die von einem Server bereitgestellt werden, enthält das Server-

protokollfeld den vom Server gesendeten Wert. Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für eine integrierte Caching-Transaktion:

```
"10.102.1.52 - "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0; .NET
 CLR 1.0.3705)""GET /"200 0 "IC"10.102.1.45"
```

Zusammen mit einer Client-Anfrage ist die protokollierte Antwort diejenige, die an den Client gesendet wird, und nicht unbedingt die vom Server gesendete.

> **Hinweis**
>
> Wenn Sie das Weblogging verwenden, enthalten die Antworten aus dem integrierten Cache den Wert IC im Serverlogfeld. Das Serverprotokollfeld ist im NSWL-Client mit der Formatspezifikation „%o1“ vorhanden.

Sonstiges

- **Was meinst du mit relexpiry und absexpiry?**

  Durch die Konfiguration `relexpiry` und bedeutet dies `absexpiry`, dass Sie den Header unabhängig davon, was in der Kopfzeile angezeigt wird, überschreiben. Sie können eine andere Ablaufeinstellung und die Ebene der Inhaltsgruppe konfigurieren. Mit `relexpiry`basiert der Ablauf des Headers auf dem Zeitpunkt, zu dem das Objekt vom NetScaler empfangen wird. Mit basiert der Ablauf auf der Zeit `absexpiry`, die auf dem NetScaler konfiguriert ist. `Relexpiry` ist in Sekundenschnelle konfiguriert. `Absexpiry` ist eine Tageszeit.

- **Was meinen Sie mit der Konfiguration von weakpos und heuristisch?**

  Die `weakpos` und Heuristik sind wie Fallback-Werte. Wenn es einen Ablauf-Header gibt, wird es nur berücksichtigt, wenn der zuletzt geänderte Header vorhanden ist. Die NetScaler-Appliance legt das Ablaufdatum auf der Grundlage des zuletzt geänderten Headers und des heuristischen Parameters fest. Die heuristische Ablaufberechnung bestimmt die Zeit bis zum Ablauf, indem der zuletzt geänderte Header überprüft wird. Ein gewisser Prozentsatz der Dauer seit der letzten Änderung des Objekts wird als Zeit bis zum Ablauf verwendet. Die Heuristik eines Objekts, das über einen längeren Zeitraum unverändert bleibt und wahrscheinlich längere Ablaufzeiträume hat. –heurExpiryParam gibt an, welchen Prozentwert in dieser Berechnung verwendet werden soll. Andernfalls verwendet die Appliance den `weakpos` Wert.

- **Was sollte ich beachten, bevor ich das dynamische Caching konfigurieren?**

  Wenn es einen Parameter gibt, der in Form eines Namenswerts vorliegt und nicht über die vollständige URL-Abfrage verfügt, oder wenn die Appliance den Parameter in einem Cookie-Header oder POST-Text empfängt, sollten Sie erwägen, dynamisches Caching zu konfigurieren. Um dynamisches Caching zu konfigurieren, müssen Sie den Parameter hitParams konfigurieren.

- **Wie wird die Hexadezimalkodierung in den Parameternamen unterstützt?**

Auf der NetScaler-Appliance wird die %HEXHEX-Codierung in den Parameternamen unterstützt. In den Namen, die Sie für HitParams oder InvalParams angeben, können Sie einen Namen angeben, der die %HEXHEX-Codierung in den Namen enthält. Beispielsweise sind Name, Name%65 und n %61m%65 gleichwertig.

- **Wie wird ein HitParam-Parameter ausgewählt?**

  Sehen Sie sich den folgenden Auszug eines HTTP-Headers für eine POST-Anfrage an:

```
POST /data2html.asp?param1=value1&param2=&param3&param4=value4
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, \*/\*
Referer: http://10.102.3.97/forms.html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 10.102.3.97
Content-Length: 153
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQGQGGRNY=NNLLKDADEENOAFLCCDGFGDMO
S1=This+text+is+only+text%2C+not+more+and+not+less%2C+%0D%0Ajust+
   text+to+be+itself%2C+namely+%22Text%22+to+be+posted+as+text
   +%28what+else...%29&B1=Submit
<!--NeedCopy-->
```

  In der vorherigen Anfrage können Sie S1 und B1, zu Ihrer Information fett hervorgehoben, als HitParams verwenden, je nach Ihren Anforderungen. Wenn Sie -matchCookies YES in der Inhaltsgruppe ASPSESSIONIDQGQGGRNY verwenden, können Sie diese Parameter auch als HitParams verwenden.

- **Was passiert mit den Clients in der Warteschlange, wenn die Antwort nicht zwischenspeicherbar ist?**

  Wenn die Antwort nicht zwischenspeicherbar ist, erhalten alle Clients in der Warteschlange dieselbe Antwort, die der erste Client erhält.

- **Kann ich die Funktionen Umfrage jedesmal (PET) und Flash Cache für dieselbe Inhaltsgruppe aktivieren?**

  Nein. Sie können PET und Flash Cache nicht für dieselbe Inhaltsgruppe aktivieren. Der integrierte Cache führt die AutoPet-Funktion für Flash-Cache-Inhaltsgruppen nicht aus. Die PET-Funktion stellt sicher, dass der integrierte Cache ein gespeichertes Objekt nicht ohne Rück-

sprache mit dem Server bedient. Sie können PET explizit für eine Inhaltsgruppe konfigurieren.

- **Wann werden die Logeinträge für die Clients in der Warteschlange erstellt?**

  Die Protokolleinträge werden für die Clients in der Warteschlange erstellt, kurz nachdem die Appliance den Antwortheader empfangen hat. Die Protokolleinträge werden nur erstellt, wenn der Antwortheader das Objekt nicht zwischenspeicherbar macht.

- **Was bedeuten die DNS-, HOSTNAME- und HOSTNAME_AND_IP-Werte des Parameters „Gecachte Objekte mithilfe des Cache-Konfigurationsparameters überprüfen“?**

  Die Bedeutungen lauten wie folgt:

  - `set cache parameter -verifyUsing HOSTNAME`

    Der Befehl ignoriert die Ziel-IP-Adresse.

  - `set cache parameter -verifyUsing HOSTNAME_AND_IP`

    Der Befehl entspricht der Ziel-IP-Adresse.

  - `set cache parameter -verifyUsing DNS`

    Der Befehl verwendet den DNS-Server.

- **Ich habe WeakNegrelExpiry auf 600 gesetzt, was 10 Minuten entspricht. Mir ist aufgefallen, dass 404-Antworten nicht zwischengespeichert werden. Was ist der Grund?**

  Das hängt vollständig von Ihrer Konfiguration ab. Standardmäßig werden 404-Antworten 10 Minuten lang zwischengespeichert. Wenn Sie möchten, dass alle 404-Antworten vom Server abgerufen werden, geben Sie —weakNegrelExpiry 0 an. Sie können —weakNegrelExpiry auf einen gewünschten Wert feineinstellen, z. B. auf einen höheren oder niedrigeren Wert, damit die 404-Antworten entsprechend zwischengespeichert werden. Wenn Sie —absExpiry für positive Antworten konfiguriert haben, führt dies möglicherweise nicht zu den gewünschten Ergebnissen.

- **Wenn der Benutzer mit dem Mozilla Firefox-Browser auf die Website zugreift, wird der aktualisierte Inhalt bereitgestellt. Wenn der Benutzer jedoch mithilfe des Microsoft Internet Explorer-Browsers auf die Website zugreift, werden veraltete Inhalte bereitgestellt. Was könnte der Grund sein?**

  Der Microsoft Internet Explorer-Browser bezieht den Inhalt möglicherweise aus seinem lokalen Cache und nicht aus dem integrierten NetScaler-Cache. Der Grund dafür kann sein, dass der Microsoft Internet Explorer-Browser den mit dem Ablaufdatum verbundenen Header in der Antwort nicht respektiert.

  Um dieses Problem zu beheben, können Sie den lokalen Cache des Internet Explorers deaktivieren und den Offline-Inhalt löschen. Nach dem Löschen des Offline-Inhalts muss der Browser den aktualisierten Inhalt anzeigen.

- **Was ist, wenn die Treffer Null sind?**

  Überprüfen Sie, ob die Serverzeit und die NS-Zeit synchronisiert sind. Und das eingestellte WeakPosrExpiry-Limit muss den Zeitunterschied zwischen NS und Server wie folgt berücksichtigen:

```
root@ns180# date
Tue May 15 18:53:52 IST 2012
<!--NeedCopy-->
```

- **Warum erhalten Richtlinien Treffer, aber nichts wird zwischengespeichert?**

  Stellen Sie sicher, dass dem integrierten Cache Speicher zugewiesen ist und dass die Zuweisung größer als Null ist.

- **Ist es möglich, die Cache-Zähler auf Null zu setzen?**

  Es gibt keine Befehlszeile oder GUI-Option, um die Cache-Zähler auf Null zu setzen, und das Leeren des Caches tut dies auch nicht. Wenn Sie das Feld neu starten, werden diese Leistungsindikatoren automatisch auf Null gesetzt.

Installation, Upgrade und Downgrade

September 1, 2023

Installation und Upgrade

Wie lade ich ein bestimmtes NetScaler Release-Build-Paket herunter?

Informationen zum Herunterladen eines bestimmten NetScaler Release-Build-Pakets finden Sie unter Herunterladen eines NetScaler-Versionspakets.

Wie aktualisiert man die Systemsoftware einer NetScaler Appliance?

Informationen zum Upgrade der Systemsoftware einer NetScaler Appliance finden Sie unter Upgrade einer eigenständigen NetScaler Appliance.

Wo finde ich die Versionshinweise für einen NetScaler Release Build?

In den Versionshinweisen für einen NetScaler-Release-Build ist Folgendes für den Release-Build aufgeführt:

- Verbesserungen

- Behobene Probleme
- Bekannte Probleme

Das Dokument mit den Versionshinweisen für einen NetScaler Release-Build befindet sich an folgenden Speicherorten:

- NetScaler Firmware oder virtuelle Appliance lädt die Seite eines bestimmten Release-Builds herunter.
- Seite mit denADC-Versionshinweisen auf der NetScaler-Dokumentationsseite

Wo finde ich Sicherheitsupdates für NetScaler Appliances?

Das NetScaler-Sicherheitsteam veröffentlicht regelmäßig Sicherheitsbulletins zu Common Vulnerabilities and Exposures (CVE) für alle verwandten NetScaler-Produkte. Diese Informationen finden Sie im Sicherheitsbulletin. Alternativ können Sie auf der NetScaler-Supportseitenach einem bestimmten CVE suchen.

Was ist die Verwendung der zebos.conf-Datei, die in einer NetScaler Version verfügbar ist?

Eine NetScaler-Appliance verwendet ZeBOS als Routing-Suite. Die in einer NetScaler-Version verfügbare Datei zebos.conf ist die Konfigurationsdatei für zebOS.

Ich möchte den SSH-Port (22) auf der NetScaler-Appliance auf einen anderen Port ändern. Ist es möglich, den SSH-Port der Appliance zu ändern?

Ja. Sie können den SSH-Port auf der NetScaler-Appliance ändern, indem Sie die Datei sshd_config im Verzeichnis /nsconfig bearbeiten. Wenn die Datei nicht im Verzeichnis /nsconfig existiert, kopieren Sie sie aus dem Verzeichnis /etc.

Bearbeiten Sie in der Datei sshd_config den Eintrag für Port 22 in Port<Number>, wobei <Number>die Zielportnummer steht. Wenn Sie die Appliance nicht neu starten und die Änderungen wirksam machen möchten, beenden Sie den `sshd` Prozess mit dem Befehl kill und starten Sie den Prozess erneut.

Das Flash-Verzeichnis fehlt in der NetScaler Appliance. Welches Verfahren muss ich befolgen, um das Flash-Verzeichnis zu mounten?

Gehen Sie folgendermaßen vor, um das Flash-Verzeichnis einzuhängen:

1. Starten Sie die NetScaler-Appliance im Einzelbenutzermodus.

   Wenn die Appliance gestartet wird, wird die folgende Meldung angezeigt:

Wählen Sie [Enter], um sofort zu booten, oder eine andere Taste für die Befehlszeile. [Kernel] wird in 10 Sekunden gebootet…“ Wählen Sie Leerzeichen aus und Sie müssen die folgende Aufforderung sehen:

Geben Sie ‘?’ ein für eine Liste von Befehlen, ‘help’ für detailliertere Hilfe.

2. Geben Sie den folgenden Befehl ein, um FreeBSD im Einzelbenutzermodus zu starten:

   booten —s

   Nach dem Start der Appliance wird die folgende Meldung angezeigt:

   Geben Sie den vollständigen Pfadnamen der Shell ein oder RETURN für /bin/sh:

3. Drücken Sie die Eingabetaste, um die #-Aufforderung anzuzeigen.
4. Führen Sie den folgenden Befehl aus, um das Flash-Verzeichnis zu mounten:

```
mount /dev/ad0s1a /flash

Note: If the preceding command displays an error message about
   permissions, run the following command to check the disk for
   consistency:

fsck /dev/ad0s1a

Run the mount command again to mount the flash directory.
```

5. Starten Sie die Appliance neu.
6. Führen Sie an der Shell-Eingabeaufforderung den folgenden Befehl aus, um zu überprüfen, ob das Flash-Verzeichnis bereitgestellt ist:

```
df -kh
```

Ich möchte mich bei der NetScaler Appliance anmelden, ohne das Kennwort einzugeben. Ist es möglich, SSH auf der Appliance so zu konfigurieren, dass dies möglich ist?

Ja. Sie können SSH auf der NetScaler-Appliance so konfigurieren, dass es sich ohne Kennwort anmeldet. Sie müssen jedoch Ihren Benutzernamen angeben. Gehen Sie wie folgt vor, um SSH für die Anmeldung ohne Kennwort zu konfigurieren:

1. Führen Sie den folgenden Befehl aus, um die öffentlichen und privaten Schlüssel zu generieren:

```
\# ssh-keygen -t rsa
```

2. Führen Sie den folgenden Befehl aus, um die Datei id_rsa.pub in das Verzeichnis .ssh des Remotehosts zu kopieren, an dem Sie sich anmelden möchten:


```
\# scp id_dsa.pub \<user>@\<remote_host>/.ssh/id_dsa.pub
```

3. Melden Sie sich beim Remotehost an.
4. Wechseln Sie in das Verzeichnis .ssh.
5. Führen Sie die folgenden Befehle aus, um den öffentlichen Schlüssel des Clients zu den bekannten öffentlichen Schlüsseln hinzuzufügen:

```
\# cat id_dsa.pub >> authorized_keys2

\# chmod 640 authorized_keys2

\# rm id_dsa.pub
```

Wie wird das BIOS der NetScaler Appliance zurückgesetzt? Unter welchen Umständen muss ich das BIOS zurücksetzen?

Führen Sie das folgende Verfahren aus, um das BIOS der NetScaler Appliance zurückzusetzen:

1. Verbinden Sie die Appliance über den seriellen Port.
2. Starten Sie die Appliance und drücken Sie die Löschtaste, wenn der Startvorgang beginnt.

   Wenn Sie während des POST-Vorgangs auf Löschen klicken, werden die BIOS-Einstellungen der Appliance angezeigt.
3. Aktivieren Sie die Exit-Seite der BIOS-Einstellungen.
4. Wählen Sie die Option Optimale Standardwerte laden. Das Meldungsfeld „Optimale Einstellungen laden“ wird angezeigt.
5. Wählen Sie OK.
6. Nehmen Sie auf den verschiedenen Tabs die folgenden Änderungen an den BIOS-Einstellungen vor:

   Tabulator
7. Aktivieren Sie die Exit-Seite der BIOS-Einstellungen.
8. Wählen Sie Änderungen speichern und Beenden aus.
9. Wählen Sie zur Bestätigung OK .
10. Stellen Sie sicher, dass die Appliance ordnungsgemäß gestartet wird und dass die serielle Konsole nach dem Start der Appliance die Ausgabe anzeigt.

    Sie müssen das BIOS zurücksetzen, wenn die serielle Konsole nicht reagiert. Dies geschieht normalerweise, nachdem Sie die Appliance aktualisiert haben und die serielle Konsole deaktiviert

ist. Sie können jedoch weiterhin mithilfe des Telnet- oder SSH-Hilfsprogramms auf die Appliance zugreifen.

Ich muss die NetScaler Appliance auf die Werkseinstellungen zurücksetzen. Welches Verfahren muss ich befolgen?

Um die NetScaler Appliance auf die Werkseinstellungen zurückzusetzen, müssen Sie zwei Umgebungen zurücksetzen: die NetScaler Anwendungsumgebung und die FreeBSD-Basisumgebung.
Gehen Sie wie folgt vor, um die NetScaler-Anwendungsumgebung der Appliance auf die Werkseinstellungen zurückzusetzen:

1. Erstellen Sie eine Backup der Datei /nsconfig/ns.conf der Appliance.
2. Löschen Sie die Datei /nsconfig/ns.conf.
3. Starten Sie die Appliance neu. Gehen Sie wie folgt vor, um die FreeBSD-Umgebung der Appliance auf die Werkseinstellungen zurückzusetzen:
   a) Installieren Sie ein neues NetScaler-Code-Image auf der Appliance. Dadurch werden mehrere Konfigurationsdateien auf FreeBSD-Ebene mit Standardwerten überschrieben.
   b) Löschen Sie alle Benutzer und Gruppen, die der Appliance hinzugefügt wurden, d. h. alle außer den Standardbenutzern.
   c) Löschen Sie die Datei /etc/resolv.conf.
   d) Löschen Sie die Einträge, die Sie der Datei /etc/hosts hinzugefügt haben.
   e) Wenn die Datei /etc/rc.netscaler existiert, löschen Sie sie.
   f) Öffnen Sie die Datei /etc/nsperm_group_suser und stellen Sie sicher, dass alle IOCTL-Einträge Kommentareinträge sind.
   g) Öffnen Sie die Datei /etc/rc.conf und stellen Sie sicher, dass der Eintrag syslogd_enable=no nicht in syslogd_enable=YES geändert wird.
   h) Öffnen Sie die Datei /etc/syslog.conf und stellen Sie sicher, dass die Datei keine zusätzlichen Einträge enthält.
   i) Löschen Sie den Inhalt der Dateien /var/nslog, /var/nstrace und /var/crash.
   j) Wenn der Syslog-Prozess auf der Appliance aktiviert ist und die Appliance lokal Protokolldateien erstellt, löschen Sie den Inhalt der Protokolldateien, die in der Datei /etc/syslog.conf aufgeführt sind. Die Dateien werden im Verzeichnis /var/log erstellt. Wenn der Syslog-Prozess beispielsweise Systemereignisse in die Datei /var/log/events schreibt und `sslvpn` auf Ereignisse auf die /var/log/sslvpnevents-Datei zugreift, löschen Sie diese Dateien.

Die Appliance zeigt auf der Konsole eine Meldung an, die der Meldung „21. Juni 12:20:18 ns /flash/ns-10.0-47.15: [1/2] dc0: NIC hängt Zustand #663: TX 10000/10000, RX 0, HF 0“ ähnelt. Was ist die Bedeutung dieser Botschaft?

Die Nachricht besteht aus den folgenden Komponenten (hier als Beispiele dargestellt):

- #663: Häufigkeit, mit der dieser Zustand auf der Appliance aufgetreten ist.
- TX 10000/10000: Anzahl der Pakete, die die Appliance zu übertragen versuchte, und Anzahl der übertragenen Pakete. Wenn beide Nummern identisch sind, wie in diesem Beispiel, hat die NIC alle Pakete übertragen, die die Appliance zu übertragen versuchte.
- RX 0: Anzahl der empfangenen Pakete. In diesem Beispiel wurde kein Paket empfangen.
- HF0: Anzahl der von der NIC gemeldeten Hardwareprobleme. In diesem Beispiel hat die NIC kein Hardwareproblem gemeldet.

Wenn die Appliance keine Pakete empfängt, meldet sie eine Hang-Bedingung, da sie in einem Netzwerk wahrscheinlich keine Pakete erhält. Wenn die Appliance jedoch an die Schnittstelle angeschlossen ist, können Sie diese Fehlermeldung ignorieren.

Nachdem ich die NetScaler Version auf der Appliance aktualisiert habe, zeigt die Appliance weiterhin die frühere Release/Build an. Was kann der Grund sein?

Die Appliance zeigt die Softwareversionsnummer aus der Datei /flash/boot/loader.conf an. Wenn der Kerneleintrag für die aktuelle NetScaler-Version in dieser Datei fehlt, zeigt die Appliance die letzte NetScaler-Release-Version an, für die der Eintrag verfügbar war.
Führen Sie folgende Schritte aus, um das Problem zu beheben:

1. Stellen Sie sicher, dass die Kernel-Datei im Verzeichnis /nsconfig vorhanden ist.
2. Suchen Sie in der Datei /flash/boot/loader.conf nach einem Eintrag für den Kernel.

   (Sie können davon ausgehen, dass der Eintrag für den Kernel des Releases/Builds, das Sie installiert haben, in der Datei fehlt.)
3. Öffnen Sie die Datei loader.conf in einem Texteditor, z. B. dem vi-Editor, und aktualisieren Sie den Kerneleintrag für die neue Release/den neuen Build.
4. Speichern und schließen Sie die Datei.
5. Wiederholen Sie die Schritte 2 bis Schritt 4 für die Datei /flash/boot/loader.conf.local.
6. Aktualisieren Sie den Eintrag release/build in der Datei ns.conf.
7. Starten Sie die Appliance neu.

Seit ich die NetScaler-Version der Appliance aktualisiert habe, zeigt das LCD-Display an der Vorderseite der Appliance die Meldung „Außer Betrieb“ oder es wird nichts angezeigt. Wie kann ich dieses Problem lösen?

Führen Sie den folgenden Befehl an der Shell-Eingabeaufforderung der Appliance aus:

```
1 /netscaler/nslcd -k
```


Ich habe das NetScaler Release/Build aktualisiert. Nach dem Upgrade-Vorgang kann die Appliance jedoch nicht gestartet werden. Kann ich die Software der Appliance auf die vorherige Version/den vorherigen Build herabstufen?

Ja. Sie können die Appliance mit der Kernel-Datei kernel.old starten. Wenn Sie die Appliance neu starten, drücken Sie die Taste F1, wenn die Appliance-Konsole die Meldung F1 drücken anzeigt. **Geben Sie kernel.old ein und drücken Sie die Eingabetaste.**

Nach dem Upgrade der NetScaler-Version auf der Appliance habe ich versehentlich die Kernel-Datei aus dem Verzeichnis /flash gelöscht. Daher kann ich das Gerät nicht starten. Gibt es eine Methode, um das Gerät in dieser Situation zu starten?

Ja. Sie können die Appliance mithilfe der Kernel-Datei `kernel.GENERIC` wie folgt starten:

1. Wenn Sie die Appliance neu starten, drücken Sie die Taste F1, wenn die Appliance-Konsole die Meldung F1 drücken anzeigt.
2. Geben Sie Kernel ein. GENERIC und drücken Sie Enter.
3. Melden Sie sich als Root-Benutzer an.
4. Installieren Sie die NetScaler-Version erneut.
5. Starten Sie die Appliance neu.

Nach dem Upgrade der Appliance-Software kann ich mich nicht an der Appliance anmelden und die folgende Meldung wird angezeigt. Ich habe versucht, dieses Problem mithilfe des Kennwortwiederherstellungsverfahrens zu lösen, war aber nicht erfolgreich. Habe ich etwas falsch gemacht?

```
```
login: nsroot
Password:
connect: No such file or directory
nsnet_connect: No such file or directory
Login incorrect
<!--NeedCopy--> ```
```

Sie können dieses Problem nicht mit der Kennwortwiederherstellungsprozedur beheben. NetScaler Release 12.1 oder höher verwendet das neue Lizenzierungssystem, das auf dem `Imgrd` Daemon basiert, der während des Startvorgangs ausgeführt wird. Damit dieser Daemon ordnungsgemäß funktioniert, muss der Hostname der NetScaler-Appliance, der in der Datei /nsconfig/rc.conf festgelegt ist, von einem Nameserver auf die NSIP-Adresse aufgelöst werden. <Host_Name>Alternativ können Sie eine Hosts-Datei im Verzeichnis /nsconfig erstellen und den 127.0.0.1-Eintrag zur Datei hinzufügen.

 
```

Stellen Sie außerdem sicher, dass Sie die Lizenzdateien in das Verzeichnis /nsconfig/license/ kopiert haben.

Während eines Upgrades eines Hochverfügbarkeitspaares wird die folgende Meldung wiederholt angezeigt. Was kann der Grund sein?

ns sshd [5035]: Fehler: Ungültiger Benutzername oder Kennwort
Diese Fehlermeldung wird angezeigt, wenn die an der Hochverfügbarkeitspaarung beteiligten Appliances entweder eine andere NetScaler Version oder einen anderen Build desselben Release haben. Auf den Appliances können unterschiedliche Versionen installiert sein, wenn Sie eine Appliance aktualisiert oder heruntergestuft haben, die andere jedoch nicht.
Ich möchte die Netzmaske der NSIP-Adresse auf einer NetScaler-Appliance ändern. Kann ich das tun, ohne einen Ausfall zu verursachen?
Eine Änderung der Netzmaske der NetScaler-IP kann zu einem kurzen Ausfall führen. Stellen Sie sicher, dass Sie die Netzmaske auf der sekundären Appliance ändern und dann das Hochverfügbarkeitspairing unterbrechen. Überprüfen Sie die Funktionalität des Geräts. Wenn alles wie erwartet funktioniert, stellen Sie das Hochverfügbarkeitspairing erneut her.
Um die Netzmaske auf der Appliance zu ändern, führen Sie den ‘config ns‘ Befehl an der CLI-Eingabeaufforderung aus und wählen Sie dann die zweite Option im Menü.
Ich habe ein Paar NetScaler-Appliances für hohe Verfügbarkeit konfiguriert. Nach dem Upgrade der Softwareversion von einer Vorschauversion auf eine endgültige Version stellte ich fest, dass einige der Appliance-Konfigurationen fehlen. Kann ich die verlorenen Konfigurationen abrufen?
Sie können das folgende Verfahren verwenden, um die Konfiguration wiederherzustellen:
1. Melden Sie sich an der NetScaler-Befehlszeile der primären Appliance an.
1. Führen Sie die folgenden Befehle aus:
save config
shell
\#cp /nsconfig/ns.conf /nsconfig/ns.conf.bkup
The ns.conf.bkup file is a backup for the running configuration.
1. Aktualisieren Sie die Software beider Appliances auf die endgültige Version.
1. Melden Sie sich an der NetScaler-Befehlszeile der primären Appliance an.
Können die primäre Appliance und die sekundäre Appliance separate Builds haben?
Es wird empfohlen, dieselbe Version und Build-Nummer sowohl auf der primären als auch auf der sekundären Appliance zu verwenden.
Können beide Appliances in einem Hochverfügbarkeitspaar (HA) gleichzeitig aktualisiert werden?
Nein. Aktualisieren Sie in einem HA-Paar zuerst den sekundären Knoten, und aktualisieren Sie dann den primären Knoten.
Weitere Informationen finden Sie unter [Upgrade eines Hochverfügbarkeitspaares](/de-de/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-HA-pair.html).
Unterstützt NetScaler Firmware-Upgrades in der Amazon Web Services-Cloud?

Ja.
Kann ich die NetScaler-Instanz unabhängig von der SDX-Version aktualisieren?
Es ist nicht erforderlich, die SDX-Version zu aktualisieren, wenn die NetScaler-Appliance aktualisiert wird. Einige Funktionen funktionieren jedoch möglicherweise nicht.
Kann ich den FTP-Server verwenden, um die NetScaler-Appliance zu aktualisieren?
Nein. Sie müssen zuerst die Firmware von der NetScaler-Website herunterladen, auf Ihrem lokalen Computer speichern und dann die Appliance aktualisieren.
Unterscheidet sich das Verfahren zum Aktualisieren der NetScaler-Appliance mit GSLB-Konfigurationen von einem Upgrade einer Appliance, die nicht an GSLB beteiligt ist?
Nein. Das Upgrade-Verfahren ähnelt dem grundlegenden Upgrade-Verfahren. Der einzige Unterschied besteht darin, dass Sie die eigenständigen oder HA-Appliances an verschiedenen Standorten schrittweise aktualisieren können.
Das Upgrade schlägt aufgrund einer ungültigen Konfiguration fehl. Wie behebe ich dieses Problem?
Ab Version NetScaler 13.1 werden klassische Ausdrücke in einigen Funktionen nicht unterstützt. In ähnlicher Weise wurden auch einige veraltete Funktionen entfernt. Weitere Informationen zu veralteten Funktionen und Befehlen finden Sie unter [Ankündigung einer Statusänderung für richtlinienbasierte Funktionen und Funktionen von NetScaler Classic](https://support.citrix.com/article/CTX296948/notice-of-status-change-announcement-for-citrix-adc-formerly-netscaler-adc-classic-policy-based-features-and-functionalities).
Wenn die Konfiguration Befehle enthält, die sich auf die veralteten oder entfernten Funktionen beziehen, schlägt das Upgrade fehl. Die veralteten Befehle lösen in Versionen 13.1 oder höher Fehler aus, sodass die Konfiguration verloren gehen kann. Verwenden Sie das ‘nspepi‘ Tool, um die ungültige oder klassische Konfiguration in eine gültige oder erweiterte Konfiguration zu konvertieren. Informationen zum ‘nspepi‘ Tool finden Sie unter [Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool](https://docs.netscaler.com/de-de/citrix-adc/current-release/appexpert/policies-and-expressions/introduction-to-policies-and-exp/converting-policy-expressions-nspepi-tool.html).
>**Hinweis:**
>
>Wenn Sie einen ungültigen Konfigurationsfehler sehen, empfehlen wir, die Option **Y** nicht zu verwenden, während Sie das ‘installns‘ Skript ausführen. Wenn Sie die Option **Y** verwenden, findet keine Konfigurationsprüfung statt und die ungültige Konfiguration kann verloren gehen.
>
> ![Ungültiger Konfigurationsfehler beim Upgrade](/en-us/citrix-adc/media/installns-script-configuration-error.png)
Downgrade
Ich habe eine NetScaler-Appliance erhalten, auf der die neueste NetScaler-Version installiert ist. Ich möchte jedoch die Softwareversion herabstufen. Kann ich das tun?
Nein. Wenn Sie versuchen, die Softwareversion herunterzustufen, funktioniert die Appliance

möglicherweise nicht wie erwartet, da die Datei ns.conf der späteren Version möglicherweise nicht mit der früheren Version kompatibel ist und die Appliance möglicherweise auf die Werkseinstellungen zurückgesetzt wird.
Beim Downgrade der NetScaler-Version habe ich die Anweisungen befolgt. Die Appliance zeigt jedoch die folgende Meldung an. Wie wird das Rollback-Verfahren auf einer NetScaler-Appliance durchgeführt?
root@LBCOL03B# ./installns
installns version (10.0-47.7) kernel (ns-10.0-47.7.gz)
Note:
Installation may pause for up to 3 minutes while data is written to the flash.
Caution:
Do not interrupt the installation process.
Doing so may cause the system to become unusable.
Installation will proceed in 5 seconds, CTRL-C to abort
No Valid NetScaler Version Detected
root@LBCOL03B#
Das Rollback-Verfahren ähnelt dem grundlegenden Upgrade-Verfahren. Wählen Sie den Ziel-Build aus, zu dem Sie zurücksetzen möchten, und führen Sie das Downgrade durch. Bevor Sie zu einer anderen Version zurückkehren, sollten Sie eine Kopie Ihrer aktuellen Konfigurationsdateien erstellen. Informationen zum Downgrade von einer Version finden Sie unter [Downgrade einer NetScaler Standalone Appliance](/de-de/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/downgrade-standalone-appliance.html).

Lastausgleich

May 11, 2023

- **Was sind die verschiedenen Load-Balancing-Richtlinien, die ich auf der NetScaler-Appliance erstellen kann?**

  Sie können die folgenden Arten von Load-Balancing-Richtlinien auf der NetScaler-Appliance erstellen:

  - Geringste Verbindungen
  - Runde Robin
  - Geringste Reaktionszeit
  - Geringste Bandbreite
  - Wenigste Pakete
  - URL-Hashing
  - Hashing von Domainnamen

- Hashing der Quell-IP-Adresse
- Hashing der Ziel-IP-Adresse
- Quell-IP — Ziel-IP-Hashing
- Token
- LRTM

- **Kann ich die Sicherheit der Webfarm erreichen, indem ich Load Balancing mithilfe der NetScaler-Appliance implementiere?**

  Ja. Sie können die Sicherheit der Webfarm erreichen, indem Sie den Lastenausgleich mithilfe der NetScaler-Appliance implementieren. Mit der NetScaler Appliance können Sie die folgenden Optionen der Load-Balancing-Funktion implementieren:

  - Verstecken von IP-Adressen: Ermöglicht es Ihnen, die eigentlichen Server aus Sicherheitsgründen und zur Erhaltung der IP-Adresse so zu installieren, dass sie sich in einem privaten IP-Adressraum befinden. Dieser Prozess ist für den Endbenutzer transparent, da die NetScaler-Appliance Anfragen im Namen des Servers akzeptiert. Im Modus zum Verstecken von Adressen isoliert die Appliance die beiden Netzwerke vollständig. Daher kann ein Client über eine andere VIP auf der Appliance für diesen Dienst auf einen Dienst zugreifen, der im privaten Subnetz ausgeführt wird, z. B. FTP- oder Telnet-Server.
  - Portzuordnung: Ermöglicht aus Sicherheitsgründen, dass die tatsächlichen TCP-Dienste auf nicht standardmäßigen Ports gehostet werden. Dieser Vorgang ist für den Endbenutzer transparent, da die NetScaler Appliance Anforderungen im Namen des Servers an die standardmäßige angekündigte IP-Adresse und Portnummer annimmt.

- **Welche Geräte kann ich zum Lastausgleich mit einer NetScaler Appliance verwenden?**

  Sie können die folgenden Geräte mit einer NetScaler Appliance ausgleichen:

  - Serverfarmen
  - Caches oder Reverse-Proxys
  - Firewall-Geräte
  - Systeme zur Erkennung von Eindringlingen
  - SSL-Offload-Geräte
  - Kompressionsgeräte
  - Content Inspection Server

- **Warum sollte ich die Load-Balancing-Funktion für die Website implementieren?**

  Sie können die Funktion Lastenausgleich für die Website implementieren, um folgende Vorteile zu nutzen:

  - Verkürzen Sie die Reaktionszeit: Wenn Sie die Load-Balancing-Funktion für die Website implementieren, ist einer der Hauptvorteile die Steigerung der Ladezeit, auf die Sie sich freuen können. Da sich zwei oder mehr Server die Last des Web-Traffics teilen, hat jeder

der Server eine geringere Traffic-Last als ein einzelner Server allein. Dies bedeutet, dass mehr Ressourcen zur Verfügung stehen, um die Kundenanfragen zu erfüllen. Dies führt zu einer schnelleren Website.

- Redundanz: Die Implementierung der Load-Balancing-Funktion führt zu einer gewissen Redundanz. Wenn die Website beispielsweise über drei Server ausgeglichen ist und einer von ihnen überhaupt nicht reagiert, können die anderen beiden weiterhin laufen und die Websitebesucher bemerken keine Ausfallzeiten. Jede Load Balancing-Lösung sendet sofort den Datenverkehr an den Back-End-Server, der nicht verfügbar ist.

- **Warum muss ich die Mac Based Forwarding (MBF) Option für Link Load Balancing (LLB) deaktivieren?**

  - Wenn Sie die MBF-Option aktivieren, berücksichtigt die NetScaler Appliance, dass der eingehende Datenverkehr vom Client und der ausgehende Datenverkehr zum selben Client über denselben Upstream-Router fließt. Die LLB-Funktion erfordert jedoch, dass der beste Weg für den Rückverkehr gewählt wird.
  - Das Aktivieren der MBF-Option unterbricht diesen Topologieentwurf, indem der ausgehende Datenverkehr über den Router gesendet wird, der den eingehenden Clientdatenverkehr weitergeleitet hat.

- **Welche verschiedenen Persistenztypen sind auf der NetScaler-Appliance verfügbar?**

  Die NetScaler-Appliance unterstützt die folgenden Persistenztypen:

  - Quell-IP
  - Cookieeinlage
  - SSL-Sitzungs-ID
  - URL passiv
  - Benutzerdefinierte Server-ID
  - Regel
  - DESTIP

Grafische Benutzeroberfläche (GUI)

May 11, 2023

- **Wenn ich Firefox verwende, um zwei NetScaler-Konfigurationen zu vergleichen, scheint der Browser einzufrieren?**

  Firefox zeigt schließlich den Unterschied in den Konfigurationen an, aber der Vorgang dauert sehr lange, wenn es mehr als 1000 Unterschiede gibt. Verwenden Sie Chrome für eine schnellere Reaktion.

- **Ich verwende einen MAC Safari-Browser, um einen NetScaler zu aktualisieren. Wenn ich im Upgrade-Assistenten auf die Schaltfläche Durchsuchen klicke, um die Build-Datei aus der Appliance auszuwählen, werden im Dialogfeld keine Dateien oder Ordner angezeigt. Wenn ich zurück zum Stammordner navigiere, zeigt das Dialogfeld den Ordner der obersten Ebene an, aber ich kann ihn nicht durchsuchen. Was soll ich tun?**

  Klicken Sie im Safari-Browser auf das Symbol Einstellungen und navigieren Sie zu **Einstellungen > Sicherheit > Website-Einstellungen verwalten > Java**. Ändern Sie den Wert der Einstellung **Beim Besuch anderer Websites** auf Im unsicheren Modus ausführen.

- **Was soll ich tun, bevor ich auf die GUI zugreife?**

  Bevor Sie auf eine neue Version der NetScaler-Software zugreifen:

  - Löschen Sie den Browser-Cache einschließlich Cookies.
  - Greifen Sie im Inkognitomodus des Browsers auf die GUI zu.
  - Greifen Sie auf GUI in einem anderen Browser zu.
  - Deaktivieren **Sie die Option Softwarebeschleunigung verwenden** in der Einstellung und starten Sie den Browser neu
  - Zugriff auf **Chrome: Erweiterungen**, löschen **Sie das Feld Aktivieren** und starten Sie den Chrome-Browser neu

- **Welchen Port sollte ich öffnen, um über HTTP oder HTTPS auf GUI zuzugreifen?**

  Im Folgenden werden die Standardportnummern für HTTP- und HTTPS-Verwaltungsdienste (GUI) in den NetScaler MPX-, VPX- und CPX-Appliances aufgeführt:

  - NetScaler MPX- und VPX-Appliances: 80 (HTTP) und 443 (HTTPS)
  - NetScaler CPX-Appliances: 9080 (HTTP) und 9443 (HTTPS)

  Außerdem können Sie Ports für HTTP- und HTTPS-Verwaltungsdienste (GUI) außer Port 80 und 443 konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von HTTP- und HTTPS-Management-Ports.

- **Mit welchen Browsern ist die GUI für verschiedene Betriebssysteme kompatibel?**

  In der folgenden Tabelle sind die kompatiblen Browser für NetScaler GUI Version 12.1, 13.0 und 13.1 aufgeführt:

Betriebssystem	Browser	Versionen
Windows 10 und später	Edge	110.1587.63 und später
Windows 10 und später	Mozilla Firefox	102 und später
Windows 10 und später	Chrome	108 und später
MAC	Mozilla Firefox	110.0.1 und später

Betriebssystem	Browser	Versionen
MAC	Safari	15.5 und später

SSL

August 19, 2021

Klicken Sie hier für häufig gestellte Fragen zu SSL.

Authentifizierung, Autorisierung und Überwachung des Anwendungsverkehrs

May 11, 2023

Viele Unternehmen beschränken den Website-Zugriff nur auf gültige Benutzer und kontrollieren die Zugriffsebene, die jedem Benutzer gestattet ist. Die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion ermöglicht es einem Site-Administrator, Zugriffskontrollen mit der NetScaler-Appliance zu verwalten, anstatt diese Steuerelemente für jede Anwendung separat zu verwalten. Durch die Authentifizierung auf der Appliance können diese Informationen auch über alle Websites innerhalb derselben Domäne weitergegeben werden, die von der Appliance geschützt sind.

Um Authentifizierung, Autorisierung und Überwachung zu verwenden, müssen Sie virtuelle Authentifizierungsserver für die Verarbeitung des Authentifizierungsprozesses und virtuelle Server für das Verkehrsmanagement konfigurieren, um den Datenverkehr zu Webanwendungen zu verarbeiten, die eine Authentifizierung erfordern. Sie konfigurieren Ihr DNS auch so, dass es jedem virtuellen Server FQDNs zuweist. Nach dem Konfigurieren der virtuellen Server konfigurieren Sie ein Benutzerkonto für jeden Benutzer, der sich über die NetScaler-Appliance authentifiziert, und optional erstellen Sie Gruppen und weisen Benutzerkonten Gruppen zu. Nachdem Sie Benutzerkonten und Gruppen erstellt haben, konfigurieren Sie Richtlinien, die der Appliance mitteilen, wie Benutzer authentifiziert werden sollen, auf welche Ressourcen Benutzer zugreifen können und wie Benutzersitzungen protokolliert werden. Um die Richtlinien in Kraft zu setzen, binden Sie jede Richtlinie global, an einen bestimmten virtuellen Server oder an die entsprechenden Benutzerkonten oder Gruppen. Nachdem Sie Ihre Richtlinien konfiguriert haben, passen Sie Benutzersitzungen an, indem Sie Sitzungseinstellungen konfigurieren und Ihre Sitzungsrichtlinien an den virtuellen Server für die Verkehrsverwaltung binden. Wenn Ihr Intranet Clientzertifikate verwendet, richten Sie schließlich die Konfiguration des Clientzertifikats ein.

Um zu verstehen, wie Authentifizierung, Autorisierung und Auditierung in einer verteilten Umgebung funktionieren, sollten Sie eine Organisation mit einem Intranet in Betracht ziehen, auf das ihre Mitarbeiter im Büro, zu Hause und auf Reisen zugreifen. Die Inhalte im Intranet sind vertraulich und erfordern einen sicheren Zugriff. Jeder Benutzer, der auf das Intranet zugreifen möchte, muss über einen gültigen Benutzernamen und ein gültiges Kennwort verfügen. Um diese Anforderungen zu erfüllen, tut der ADC Folgendes:

- Leitet den Benutzer auf die Anmeldeseite um, wenn der Benutzer auf das Intranet zugreift, ohne sich angemeldet zu haben.
- Sammelt die Anmeldeinformationen des Benutzers, liefert sie an den Authentifizierungsserver und speichert sie in einem Verzeichnis im Cache, auf das über das Lightweight Directory Access Protocol (LDAP) zugegriffen werden kann. Weitere Informationen finden Sie unter Bestimmen von Attributen in Ihrem LDAP-Verzeichnis.
- Überprüft, ob der Benutzer berechtigt ist, auf bestimmte Intranetinhalte zuzugreifen, bevor er die Anforderung des Benutzers an den Anwendungsserver übermittelt.
- Behält ein Sitzungstimeout bei, nach dem sich Benutzer erneut authentifizieren müssen, um wieder auf das Intranet zugreifen zu können. (Sie können das Timeout konfigurieren.)
- Protokolliert die Benutzerzugriffe, einschließlich ungültiger Anmeldeversuche, in einem Überwachungsprotokoll.

Unterstützte Authentifizierungsarten

- Lokal
- LDAP
- RADIUS
- SAML
- TACACS+
- Clientzertifikatauthentifizierung (einschließlich Smartcard-Authentifizierung)
- Web-Site
- Erweiterte Authentifizierung
- Formularbasierte Authentifizierung
- 401-basierte Authentifizierung
- Natives OTP
- Push Benachrichtigung
- E-Mail OTP
- reCaptcha

NetScaler Gateway unterstützt auch RSA SecurID, Gemalto Protiva und SafeWord. Sie verwenden einen RADIUS-Server, um diese Authentifizierungstypen zu konfigurieren.

Bevor Sie Authentifizierung, Autorisierung und Überwachung konfigurieren, müssen Sie mit dem Konfigurieren von Lastenausgleich, Content Switching und SSL auf der NetScaler-Appliance vertraut sein und verstehen.

Authentifizierung ohne Autorisierung

Die Autorisierung gibt die Netzwerkressourcen an, auf die Benutzer Zugriff haben, wenn sie sich an der Appliance anmelden. Die Standardeinstellung für die Autorisierung besteht darin, den Zugriff auf alle Netzwerkressourcen zu verweigern. Citrix empfiehlt, die globale Standardeinstellung zu verwenden und dann Autorisierungsrichtlinien zu erstellen, um die Netzwerkressourcen zu definieren, auf die Benutzer zugreifen können.

Sie konfigurieren die Autorisierung auf der Appliance mithilfe einer Autorisierungsrichtlinie und Ausdrücken. Nachdem Sie eine Autorisierungsrichtlinie erstellt haben, können Sie sie an die Benutzer oder Gruppen binden, die Sie auf der Appliance konfiguriert haben.

Sie können die Appliance so konfigurieren, dass sie nur Authentifizierung ohne Autorisierung verwendet. Wenn Sie die Authentifizierung ohne Autorisierung konfigurieren, führt die Appliance keine Gruppenautorisierungsprüfung durch. Die Richtlinien, die Sie für den Benutzer oder die Gruppe konfigurieren, werden dem Benutzer zugewiesen.

Authentifizierung, Autorisierung und Auditing aktivieren

Um die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion verwenden zu können, müssen Sie sie aktivieren. Sie können Authentifizierungs-, Autorisierungs- und Überwachungseinheiten — wie die virtuellen Authentifizierungs- und Verkehrsmanagementserver — konfigurieren, bevor Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion aktivieren, aber die Entitäten funktionieren erst, wenn die Funktion aktiviert ist.

So aktivieren Sie Authentifizierung, Autorisierung und Überwachung über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um Authentifizierung, Autorisierung und Überwachung zu aktivieren und die Konfiguration zu überprüfen:

```
1 enable ns feature AAA
2 <!--NeedCopy-->
```

So aktivieren Sie Authentifizierung, Autorisierung und Überwachung über die GUI

1. Navigieren Sie zu **System > Einstellungen**.
2. Klicken Sie im Detailbereich unter **Modi und Funktionen**auf **Grundfunktionen ändern**.

3. Aktivieren Sie im Dialogfeld **Grundfunktionen konfigurieren** das Kontrollkästchen **Authentifizierung, Autorisierung und Überwachung**.
4. Klicken Sie auf **OK**.

Authentifizierung deaktivieren

Wenn für Ihre Bereitstellung keine Authentifizierung erforderlich ist, können Sie sie deaktivieren. Sie können die Authentifizierung für jeden virtuellen Server deaktivieren, für den keine Authentifizierung erforderlich ist.

> **Wichtig:**
>
> **Wichtig:** Citrix empfiehlt, die Authentifizierung mit Vorsicht zu deaktivieren. Wenn Sie keinen externen Authentifizierungsserver verwenden, erstellen Sie lokale Benutzer und Gruppen, damit die Appliance Benutzer authentifizieren kann. Durch das Deaktivieren der Authentifizierung wird die Verwendung von Authentifizierungs-, Autorisierungs- und Buchhaltungsfunktionen gestoppt, die Verbindungen zur Appliance steuern und überwachen. Wenn Benutzer eine Webadresse eingeben, um eine Verbindung zur Appliance herzustellen, wird die Anmeldeseite nicht angezeigt.

Deaktivieren der Authentifizierung

1. Navigieren Sie zu **Konfiguration > NetScaler Gateway > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Deaktivieren Sie auf der Seite **Grundeinstellungen** das Kontrollkästchen **Authentifizierung aktivieren** .

Wie Authentifizierung, Autorisierung und Auditing funktionieren

May 11, 2023

Authentifizierung, Autorisierung und Überwachung bieten Sicherheit für eine verteilte Internetumgebung, indem es jedem Client mit den richtigen Anmeldeinformationen ermöglicht, sich von überall im Internet sicher mit geschützten Anwendungsservern zu verbinden. Diese Funktion beinhaltet die drei Sicherheitsfunktionen Authentifizierung, Autorisierung und Überwachung. Durch die Authentifizierung kann NetScaler die Anmeldeinformationen des Clients entweder lokal oder mit einem Authentifizierungsserver eines Drittanbieters überprüfen und nur zugelassenen Benutzern den Zugriff auf geschützte Server ermöglichen. Durch die Autorisierung kann der ADC überprüfen, auf welche Inhalte auf einem geschützten Server jeder Benutzer zugreifen kann. Durch die Überwachung kann der ADC die Aktivitäten jedes Benutzers auf einem geschützten Server aufzeichnen.

Um zu verstehen, wie Authentifizierung, Autorisierung und Auditierung in einer verteilten Umgebung funktionieren, sollten Sie eine Organisation mit einem Intranet in Betracht ziehen, auf das ihre Mitarbeiter im Büro, zu Hause und auf Reisen zugreifen. Die Inhalte im Intranet sind vertraulich und erfordern einen sicheren Zugriff. Jeder Benutzer, der auf das Intranet zugreifen möchte, muss über einen gültigen Benutzernamen und ein gültiges Kennwort verfügen. Um diese Anforderungen zu erfüllen, tut der ADC Folgendes:

- Leitet den Benutzer auf die Anmeldeseite um, wenn der Benutzer auf das Intranet zugreift, ohne sich angemeldet zu haben.
- Sammelt die Anmeldeinformationen des Benutzers, übermittelt sie an den Authentifizierungsserver und speichert sie in einem Verzeichnis, auf das über LDAP zugegriffen werden kann. Weitere Informationen finden Sie unter Bestimmen von Attributen in Ihrem LDAP-Verzeichnis.
- Überprüft, ob der Benutzer berechtigt ist, auf bestimmte Intranetinhalte zuzugreifen, bevor er die Anforderung des Benutzers an den Anwendungsserver übermittelt.
- Behält ein Sitzungstimeout bei, nach dem sich Benutzer erneut authentifizieren müssen, um wieder auf das Intranet zugreifen zu können. (Sie können das Timeout konfigurieren.)
- Protokolliert die Benutzerzugriffe, einschließlich ungültiger Anmeldeversuche, in einem Überwachungsprotokoll.

Konfigurieren von Authentifizierungs- und Überwachungsrichtlinien

Nachdem Sie Ihre Benutzer und Gruppen eingerichtet haben, konfigurieren Sie als Nächstes Authentifizierungsrichtlinien, Autorisierungsrichtlinien und Überwachungsrichtlinien, um festzulegen, welche Benutzer auf Ihr Intranet zugreifen dürfen, auf welche Ressourcen jeder Benutzer oder jede Gruppe zugreifen darf und auf welcher Detailstufe Authentifizierung, Autorisierung und Überwachung wird in den Audit-Protokollen aufbewahrt. Eine Authentifizierungsrichtlinie definiert die Art der Authentifizierung, die angewendet werden soll, wenn ein Benutzer versucht, sich anzumelden. Wenn eine externe Authentifizierung verwendet wird, gibt die Richtlinie auch den externen Authentifizierungsserver an. Autorisierungsrichtlinien legen die Netzwerkressourcen fest, auf die Benutzer und Gruppen nach der Anmeldung zugreifen können. Überwachungsrichtlinien definieren den Typ und den Speicherort des Überwachungsprotokolls.

Sie müssen jede Richtlinie binden, um sie in Kraft zu setzen. Sie binden Authentifizierungsrichtlinien an virtuelle Authentifizierungsserver, Autorisierungsrichtlinien an ein oder mehrere Benutzerkonten oder Gruppen und Überwachungsrichtlinien sowohl global als auch an ein oder mehrere Benutzerkonten oder Gruppen.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf

jede positive Ganzzahl festlegen. Im NetScaler-Betriebssystem arbeiten Richtlinienprioritäten in umgekehrter Reihenfolge: je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit Prioritäten von 10, 100 und 1000 haben, wird der Richtlinie zuerst eine Priorität von 10 zugewiesen, dann wird der Richtlinie eine Priorität von 100 zugewiesen, und schließlich hat die Richtlinie eine Reihenfolge von 1000 zugewiesen. Die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion implementiert nur die erste jeder Art von Richtlinie, mit der eine Anforderung übereinstimmt, keine zusätzlichen Richtlinien dieses Typs, mit denen auch eine Anforderung übereinstimmen könnte. Daher ist die Richtlinienpriorität wichtig, um die beabsichtigten Ergebnisse zu erhalten.

Sie können sich viel Raum lassen, um andere Richtlinien in beliebiger Reihenfolge hinzuzufügen, und sie dennoch so einstellen, dass sie in der gewünschten Reihenfolge bewertet werden, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen den einzelnen Richtlinien festlegen, wenn Sie die Richtlinien binden. Sie können dann jederzeit zusätzliche Richtlinien hinzufügen, ohne die Priorität einer vorhandenen Richtlinie neu zuweisen zu müssen.

Weitere Informationen zum Binden von Richtlinien auf der NetScaler-Appliance finden Sie in der NetScaler-Produktdokumentation.

Konfigurieren Sie die Richtlinie “No_Auth”, um bestimmten Datenverkehr zu umgehen

Sie können jetzt die Richtlinie No_Auth konfigurieren, um bestimmten Datenverkehr aus der Authentifizierung zu Bypass, wenn die 401-basierte Authentifizierung auf dem virtuellen Verkehrsverwaltungsserver aktiviert ist. Für einen solchen Verkehr müssen Sie eine “No_Auth” -Richtlinie binden.

So konfigurieren Sie die Richtlinie No_Auth, um bestimmten Datenverkehr über die CLI zu Bypass

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Beispiel:

```
add authentication policy ldap -rule ldapAct1 -action No_Auth
<!--NeedCopy-->
```


Grundkomponenten der Authentifizierung, Autorisierung und Audit-Konfiguration

May 11, 2023

Die grundlegenden Komponenten der Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration lauten wie folgt:

- **Virtueller Authentifizierungsserver** — Alle Authentifizierungsanfragen werden vom virtuellen Server für das Verkehrsmanagement (Load Balancing oder Content Switching) an den virtuellen Authentifizierungsserver umgeleitet. Dieser virtuelle Server verarbeitet die zugehörigen Authentifizierungsrichtlinien und bietet dementsprechend Zugriff auf die Anwendung. Weitere Informationen finden Sie unter Virtueller Authentifizierungsserver.
- **Authentifizierungsprofile** — Ein Authentifizierungsprofil gibt den virtuellen Authentifizierungsserver, den Authentifizierungshost, die Authentifizierungsdomäne und eine Authentifizierungsebene an.

Sie können ein oder mehrere Authentifizierungsprofile erstellen, um verschiedene Authentifizierungseinstellungen anzugeben und diese Authentifizierungsprofile basierend auf Ihren Anforderungen an relevante Traffic-Management-Server zu binden. Weitere Informationen finden Sie unter Authentifizierungsprofile.

- **Authentifizierungsrichtlinien** - Wenn sich Benutzer bei der NetScaler oder NetScaler Gateway Appliance anmelden, werden sie gemäß einer von Ihnen erstellten Richtlinie authentifiziert. Eine Authentifizierungsrichtlinie besteht aus einem Ausdruck und einer Aktion. Authentifizierungsrichtlinien verwenden NetScaler Ausdrücke. Weitere Informationen finden Sie unter Authentifizierungsrichtlinien.
- **Autorisierungsrichtlinien** - Wenn Sie eine Autorisierungsrichtlinie konfigurieren, können Sie sie so einstellen, dass sie den Zugriff auf Netzwerkressourcen im internen Netzwerk zulässt oder verweigert. Weitere Informationen finden Sie unter Autorisierungsrichtlinien.
- **Benutzer und Gruppen:** - Nachdem Sie die grundlegende Einrichtung für Authentifizierung, Autorisierung und Überwachung konfiguriert haben, erstellen Sie Benutzer und Gruppen. Sie erstellen zunächst ein Benutzerkonto für jede Person, die sich über die NetScaler-Appliance authentifiziert. Wenn Sie die lokale Authentifizierung verwenden, die von der NetScaler Appliance selbst gesteuert wird, erstellen Sie lokale Benutzerkonten und weisen jedem dieser Konten Kennwörter zu. Weitere Informationen finden Sie unter Benutzer und Gruppen.

Virtueller Authentifizierungsserver

May 11, 2023

Der virtuelle Traffic Management-Server (Load Balancing oder Content Switching) leitet alle Authentifizierungsanforderungen an den virtuellen Authentifizierungsserver um. Dieser virtuelle Server verarbeitet die zugehörigen Authentifizierungsrichtlinien und bietet dementsprechend Zugriff auf die Anwendung.

Hinweis: Sie können Traffic-Management-Richtlinien nicht an Authentifizierung, Autorisierung und Überwachung virtueller Server binden.

Richten Sie den virtuellen Authentifizierungsserver ein

Die Schritte beim Einrichten eines virtuellen Authentifizierungsservers sind:

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

```
enable ns feature AAA
<!--NeedCopy-->
```

2. Konfigurieren Sie einen virtuellen Authentifizierungsserver. Es muss vom Typ SSL sein und sicherstellen, dass das SSL-Zertifikatschlüsselpaar an den virtuellen Server gebunden wird.

```
add authentication vserver <name> SSL <ipaddress> <port>

bind ssl certkey <auth-vserver-name> <certkey>
<!--NeedCopy-->
```

3. Geben Sie den FQDN der Domäne für den virtuellen Authentifizierungsserver an.

```
set authentication vserver <name> -authenticationDomain <FQDN>
<!--NeedCopy-->
```

4. Ordnen Sie den virtuellen Authentifizierungsserver dem entsprechenden virtuellen Server für das Verkehrsmanagement zu.

   Zu beachtende Punkte:

   - Der FQDN des virtuellen Servers für die Verkehrsverwaltung muss sich in derselben Domäne wie der FQDN des virtuellen Authentifizierungsservers befinden, damit das Domänensitzungscookie ordnungsgemäß funktioniert. Auf dem virtuellen Server für das Verkehrsmanagement:
     - Aktiviere die Authentifizierung.

- Geben Sie den FQDN des virtuellen Authentifizierungsservers als Authentifizierungshost des virtuellen Servers für die Datenverkehrsverwaltung an.
- [Optional] Geben Sie die Authentifizierungsdomäne auf dem virtuellen Traffic Management-Server an.
- Wenn Sie die Authentifizierungsdomäne nicht konfigurieren, weist die Appliance einen FQDN zu, der aus dem FQDN des virtuellen Authentifizierungsservers ohne den Teil des Hostnamens besteht. Wenn der Domänenname des virtuellen Authentifizierungsservers beispielsweise **tm.xyz.bar.com**lautet, weist die Appliance **xyz.bar.com** als Authentifizierungsdomäne zu.
  * Für den Lastenausgleich:

```
set lb vserver <name> -authentication ON -
   authenticationhost <FQDN> [-authenticationdomain <
   authdomain>]
<!--NeedCopy-->
```

  * Zum Content Switching:

```
set cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

- Wenn Sie ein domänenweites Cookie für eine Authentifizierungsdomäne festlegen müssen, müssen Sie das Authentifizierungsprofil auf einem virtuellen Lastausgleichsserver aktivieren.

5. Stellen Sie sicher, dass beide virtuellen Server in Betrieb sind und korrekt konfiguriert sind.

```
show authentication vserver <name>
<!--NeedCopy-->
```

So richten Sie einen virtuellen Authentifizierungsserver über die GUI ein

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

   Navigieren Sie zu **System > Einstellungen**, klicken Sie auf **Grundfunktionen konfigurieren**und aktivieren Sie **Authentifizierung, Autorisierung und Überwachung**.

2. Konfigurieren Sie den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**, und konfigurieren Sie nach Bedarf.

3. Konfigurieren Sie den virtuellen Traffic Management-Server für die Authentifizierung.

   - **Für den Lastenausgleich:**

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und konfigurieren Sie den virtuellen Server nach Bedarf.

- **Zum Content Switching:**

  Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und konfigurieren Sie den virtuellen Server nach Bedarf.

4. - Überprüfen Sie das Authentifizierungs-Setup.

     Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**, und überprüfen Sie die Details des entsprechenden virtuellen Authentifizierungsservers.

Konfigurieren des virtuellen Authentifizierungsservers

Um Authentifizierung, Autorisierung und Überwachung zu konfigurieren, konfigurieren Sie zunächst einen virtuellen Authentifizierungsserver für den Umgang mit Authentifizierungsverkehr. Binden Sie als Nächstes ein SSL-Zertifikatschlüsselpaar an den virtuellen Server, damit es SSL-Verbindungen verarbeiten kann.
Weitere Informationen zum Konfigurieren von SSL und zum Erstellen eines Zertifikatschlüsselpaars finden Sie unter SSL-Zertifikate.

Konfigurieren eines virtuellen Authentifizierungsservers mit der CLI

Um einen virtuellen Authentifizierungsserver zu konfigurieren und die Konfiguration zu überprüfen, geben Sie an der Eingabeaufforderung die folgenden Befehle in derselben Reihenfolge ein:

```
add authentication vserver <name> ssl <ipaddress>

show authentication vserver <name>

bind ssl certkey <certkeyName>

show authentication vserver <name>

set authentication vserver <name>

show authentication vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
add authentication vserver Auth-Vserver-2 SSL 10.102.29.77 443 Done

```



```
3 show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done
4
5 bind ssl certkey Auth-Vserver-2 Auth-Cert-1 Done
6
7 show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: UP Client Idle Timeout
    : 180 sec Down state flush: DISABLED Disable Primary Vserver On Down
     : DISABLED Authentication : ON Current AAA Users: 0 Done
8
9 set authentication vserver Auth-Vserver-2
10
11 show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done
12 <!--NeedCopy-->
```

> **Hinweis**
>
> Der Parameter Authentication Domain ist veraltet. Verwenden Sie das Authentifizierungsprofil, um domänenweite Cookies

Konfigurieren eines virtuellen Authentifizierungsservers über die GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um einen neuen virtuellen Authentifizierungsserver zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen virtuellen Authentifizierungsserver zu ändern, wählen Sie den virtuellen Server aus und klicken dann auf **Bearbeiten**. Der Konfigurationsdialog öffnet sich mit dem erweiterten Bereich Grundeinstellungen.
3. Geben Sie die Werte für die Parameter wie folgt an (Sternchen gibt einen erforderlichen Parameter an):
   - name*—name (kann für einen zuvor erstellten virtuellen Server nicht geändert werden)
   - IP-Adresstyp* — IP-Adresstyp des virtuellen Authentifizierungsservers
   - IP-Adresse* — IP-Adresse des virtuellen Authentifizierungsservers

- Port* — TCP-Port, auf dem der virtuelle Server Verbindungen akzeptiert.
- Fehlgeschlagenes Anmelde-Timeout — failedLoginTimeout (Sekunden erlaubt, bevor die Anmeldung fehlschlägt, und der Benutzer muss den Anmeldevorgang erneut starten.)
- Max. Anmeldeversuche — MaxLoginAttempts (Anzahl der erlaubten Anmeldeversuche, bevor der Benutzer gesperrt wird)

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver verwendet nur das SSL-Protokoll und den Port 443, sodass diese Optionen ausgegraut sind. Alle Optionen, die nicht erwähnt werden, können ignoriert werden.

4. Klicken Sie auf **Weiter**, um den Bereich Zertifikate anzuzeigen.
5. Konfigurieren Sie im Bereich **Zertifikate** alle SSL-Zertifikate, die Sie mit diesem virtuellen Server verwenden möchten.
   - Um ein CA-Zertifikat zu konfigurieren, klicken Sie auf den Pfeil rechts neben CA Certificate, um das Dialogfeld CA Cert Key anzuzeigen, wählen Sie das Zertifikat aus, das Sie an diesen virtuellen Server binden möchten, und klicken Sie auf **Speichern**.
   - Um ein Serverzertifikat zu konfigurieren, klicken Sie auf den Pfeil rechts neben dem Serverzertifikat, und gehen Sie genauso vor wie für das CA-Zertifikat.
6. Klicken Sie auf **Weiter**, um den Bereich **Erweiterte Authentifizierungsrichtlinien** anzuzeigen.
7. Wenn Sie eine erweiterte Authentifizierungsrichtlinie an den virtuellen Server binden möchten, klicken Sie auf den Pfeil auf der rechten Seite der Zeile, um das Dialogfeld **Authentifizierungsrichtlinie** anzuzeigen, wählen Sie die Richtlinie aus, die Sie an den Server binden möchten, legen Sie die Priorität fest, und klicken Sie dann auf **OK**.
8. Klicken Sie auf **Fortfahren**, um den Bereich **Grundauthentifizierungsrichtlinien** anzuzeigen.
9. Wenn Sie eine Standardauthentifizierungsrichtlinie erstellen und an den virtuellen Server binden möchten, klicken Sie auf das Pluszeichen, um das Dialogfeld **Richtlinien** anzuzeigen, und befolgen Sie die Anweisungen, um die Richtlinie zu konfigurieren und an diesen virtuellen Server zu binden.
10. Klicken Sie auf **Weiter**, um den Bereich 401-basierte virtuelle Server anzuzeigen.
11. Konfigurieren Sie im Bereich 401-basierte virtuelle Server alle virtuellen Load Balancing- oder Content Switching-Server, die Sie an diesen virtuellen Server binden möchten.
    - Um einen virtuellen Lastausgleichsserver zu binden, klicken Sie auf den Pfeil rechts neben dem virtuellen Lastausgleichsserver, um das Dialogfeld Load Balancing Virtuelle Server anzuzeigen, und folgen Sie den Anweisungen.
    - Um einen virtuellen Content Switching-Server zu binden, klicken Sie auf den Pfeil rechts neben dem virtuellen Server für Content Switching, um das Dialogfeld Content Switching

Virtual Server anzuzeigen, und gehen Sie genauso vor wie beim Binden eines virtuellen LB-Servers.

12. Wenn Sie eine Gruppe erstellen oder konfigurieren möchten, klicken Sie im Bereich Gruppen auf den Pfeil, um das Dialogfeld Gruppen anzuzeigen, und befolgen Sie die Anweisungen.
13. Überprüfen Sie Ihre Einstellungen und klicken Sie auf Fertig, wenn Sie **fertig**sind. Das Dialogfenster wird geschlossen. Wenn Sie einen neuen virtuellen Authentifizierungsserver erstellt haben, wird dieser jetzt in der Liste des **Konfigurationsfensters** angezeigt.

Virtueller Server für das Verkehrsmanagement

Nachdem Sie Ihren virtuellen Authentifizierungsserver erstellt und konfiguriert haben, erstellen oder konfigurieren Sie als Nächstes einen virtuellen Traffic Management-Server und verknüpfen Ihren virtuellen Authentifizierungsserver damit. Sie können entweder einen virtuellen Lastausgleichs- oder Content Switching-Server für einen virtuellen Server zur Datenverkehrsverwaltung verwenden. Weitere Informationen zum Erstellen und Konfigurieren eines virtuellen Servers finden Sie im *Citrix Traffic Management Guide* bei Traffic Management.

> **Hinweis:**
>
> Der FQDN des virtuellen Servers für die Verkehrsverwaltung muss sich in derselben Domäne wie der FQDN des virtuellen Authentifizierungsservers befinden, damit das Cookie für die Domänensitzung ordnungsgemäß funktioniert.

Sie konfigurieren einen virtuellen Traffic Management-Server für Authentifizierung, Autorisierung und Überwachung, indem Sie die Authentifizierung aktivieren und dann den FQDN des Authentifizierungsservers dem virtuellen Server für das Verkehrsmanagement zuweisen. Sie können die Authentifizierungsdomäne derzeit auch auf dem virtuellen Server für die Verkehrsverwaltung konfigurieren. Wenn Sie diese Option nicht konfigurieren, weist die NetScaler-Appliance dem virtuellen Server für die Verkehrsverwaltung einen FQDN zu, der aus dem FQDN des virtuellen Authentifizierungsservers ohne den Hostnamen-Teil besteht. Wenn der Domänenname des virtuellen Authentifizierungsservers beispielsweise tm.xyz.bar.com lautet, weist die Appliance xyz.bar.com. als Authentifizierungsdomäne zu.

So konfigurieren Sie einen virtuellen Traffic Management-Server über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlsätze ein:

```
set lb vserver <name> -authentication ON -authenticationhost <FQDN> [-authenticationdomain <authdomain>]
show lb vserver <name>
set cs vserver <name> -authentication ON -authenticationhost <FQDN> [-authenticationdomain <authdomain>]
```



```
4 show cs vserver <name>
5 <!--NeedCopy-->
```

Beispiel:

```
1 set lb vserver vs-cont-sw -Authentication ON -AuthenticationHost mywiki
      .index.com Done
2
3 show lb vserver vs-cont-sw vs-cont-sw (0.0.0.0:0) - TCP Type: ADDRESS
      State: DOWN Last state change was at Wed Aug 19 10:03:15 2009 (+410
      ms) Time since last state change: 5 days, 20:00:40.290 Effective
      State: DOWN Client Idle Timeout: 9000 sec Down state flush: ENABLED
      Disable Primary Vserver On Down : DISABLED No. of Bound Services : 0
       (Total) 0 (Active) Configured Method: LEASTCONNECTION Mode: IP
      Persistence: NONE Connection Failover: DISABLED Authentication: ON
      Host: mywiki.index.com
4 Done
5 <!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Traffic Management-Server über die GUI

1. Führen Sie im Navigationsbereich einen der folgenden Schritte aus.
   - Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
   - Navigieren Sie zu **Traffic Management > Content Switching > Virtu**
   - Wählen Sie im Detailbereich den virtuellen Server aus, auf dem Sie die Authentifizierung aktivieren möchten, und klicken Sie dann auf **Bearbeiten**.
   - Geben Sie im Textfeld Domäne die Authentifizierungsdomäne ein.
   - Wählen Sie im Menü " **Erweitert** " auf der rechten Seite die Option **Authentifizierung**aus.
   - Wählen Sie entweder **Formularbasierte Authentifizierung** oder **401-basierte Authentifizierung**und geben Sie die Authentifizierungsinformationen ein.
     - Geben Sie für die formularbasierte Authentifizierung den Authentifizierungs-FQDN (den vollqualifizierten Domänennamen des Authentifizierungsservers), den virtuellen Authentifizierungsserver (die IP-Adresse des virtuellen Authentifizierungsservers) und das Authentifizierungsprofil (das für die Authentifizierung zu verwendende Profil) ein.
     - Geben Sie für 401-basierte Authentifizierung nur den virtuellen Authentifizierungsserver und das Authentifizierungsprofil ein.
   - Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass der virtuelle Server erfolgreich konfiguriert wurde.

Vereinfachte Unterstützung des Anmeldeprotokolls für Authentifizierung, Autorisierung und Überwachung

Das Anmeldeprotokoll zwischen Authentifizierung, Autorisierung und Überwachung virtueller Server für das Verkehrsmanagement und Authentifizierung, Autorisierung und Überwachung virtueller Server wird vereinfacht, um interne Mechanismen zu verwenden, anstatt die verschlüsselten Daten über Abfrageparameter zu senden. Mit dieser Funktion wird die Wiedergabe von Anfragen verhindert.

Konfigurieren Sie DNS

Damit das im Authentifizierungsprozess verwendete Domänensitzungscookie ordnungsgemäß funktioniert, müssen Sie DNS so konfigurieren, dass sowohl die Authentifizierungs- als auch die virtuellen Server für die Verkehrsverwaltung FQDNs in derselben Domäne zugewiesen werden. Informationen zum Konfigurieren von DNS-Adressdatensätzen finden Sie unter Domänennamensystem.

Überprüfen der Authentifizierung virtueller Server

Nachdem Sie virtuelle Authentifizierungs- und Verkehrsverwaltungsserver konfiguriert haben und bevor Sie Benutzerkonten erstellen, müssen Sie überprüfen, ob beide virtuellen Server korrekt konfiguriert sind und sich im Status UP befinden.

Konfigurieren einer NoAuth-Authentifizierung über die CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
show authentication vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
State: UP
Client Idle Timeout: 180 sec
Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
Done
<!--NeedCopy-->
```


Konfigurieren einer NoAuth-Authentifizierung über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler AAA - Anwendungsverkehr > Virtuelle Server**.
   Hinweis: Navigieren Sie von NetScaler Gateway zu **NetScaler Gateway > Virtuelle Server**.
2. Überprüfen Sie die Informationen im Bereich **Virtuelle AAA-Server**, um sicherzustellen, dass Ihre Konfiguration korrekt ist und Ihr virtueller Authentifizierungsserver Datenverkehr akzeptiert. Sie können einen bestimmten virtuellen Server auswählen, um detaillierte Informationen im Detailbereich anzuzeigen.

Richtlinien zur Autorisierung

May 11, 2023

Wenn Sie eine Autorisierungsrichtlinie konfigurieren, können Sie festlegen, dass sie den Zugriff auf Netzwerkressourcen im internen Netzwerk erlaubt oder verweigert. Verwenden Sie beispielsweise den folgenden Ausdruck, um Benutzern Zugriff auf das 10.3.3.0-Netzwerk zu gewähren:

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Autorisierungsrichtlinien werden auf Benutzer und Gruppen angewendet. Nachdem ein Benutzer authentifiziert wurde, führt NetScaler Gateway eine Gruppenautorisierungsprüfung durch, indem die Gruppeninformationen des Benutzers entweder von einem RADIUS-, LDAP- oder TACACS+-Server abgerufen werden. Wenn Gruppeninformationen für den Benutzer verfügbar sind, überprüft NetScaler Gateway die für die Gruppe zulässigen Netzwerkressourcen.

Um zu steuern, auf welche Ressourcen Benutzer zugreifen können, müssen Sie Autorisierungsrichtlinien erstellen. Wenn Sie keine Autorisierungsrichtlinien erstellen müssen, können Sie die globale Standardermächtigung konfigurieren.

Wenn Sie innerhalb der Autorisierungsrichtlinie einen Ausdruck erstellen, der den Zugriff auf einen Dateipfad verweigert, können Sie nur den Pfad des Unterverzeichnisses und nicht das Stammverzeichnis verwenden. Verwenden Sie zum Beispiel fs.path enthält “\\ dir1\\ dir2” anstelle von fs.path enthält “\\ rootdir\\ dir1\\ dir2”. Wenn Sie in diesem Beispiel die zweite Version verwenden, schlägt die Richtlinie fehl.

Nachdem Sie die Autorisierungsrichtlinie konfiguriert haben, binden Sie sie an einen Benutzer oder eine Gruppe.

Standardmäßig werden Autorisierungsrichtlinien zuerst anhand von Richtlinien validiert, die Sie an den virtuellen Server binden, und dann gegen global gebundene Richtlinien. Wenn Sie eine Richtlinie global binden und möchten, dass die globale Richtlinie Vorrang vor einer Richtlinie hat, die Sie an einen Benutzer, eine Gruppe oder einen virtuellen Server binden, können Sie die Prioritätsnummer

der Richtlinie ändern. Prioritätszahlen beginnen bei Null. Eine niedrigere Prioritätszahl gibt der Richtlinie eine höhere Priorität.

Wenn die globale Richtlinie beispielsweise eine Prioritätsnummer von eins hat und der Benutzer eine Priorität von zwei hat, wird zuerst die globale Authentifizierungsrichtlinie angewendet.

> **Wichtig:**
>
> - Klassische Autorisierungsrichtlinien werden nur auf TCP-Verkehr angewendet.
> - Erweiterte Autorisierungsrichtlinie kann auf alle Arten von Datenverkehr (TCP/UDP/ICMP/DNS) angewendet werden.
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if “type” is not explicitly mentioned or “type” is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Weitere Einzelheiten zu erweiterten Autorisierungsrichtlinien finden Sie im Artikel https://support.citrix.com/article/CTX232237.

Autorisierungsrichtlinie konfigurieren und binden

Konfigurieren Sie eine Autorisierungsrichtlinie mithilfe der GUI

1. Navigieren Sie zu **NetScaler Gateway > Richtlinien > Autorisierung**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.
4. Wählen Sie unter **Aktion**die Option **Zulassen** oder **Ablehnen**aus.
5. Klicken Sie in **Expression**auf **Expression Editor**.
6. Um mit der Konfiguration des Ausdrucks zu beginnen, klicken Sie auf **Auswählen** und wählen Sie die erforderlichen Elemente aus.
7. Klicken Sie auf **Fertig**, wenn Ihr Ausdruck vollständig ist.
8. Klicken Sie auf **Erstellen**.

Binden Sie mithilfe der GUI eine Autorisierungsrichtlinie an einen Benutzer

1. Navigieren Sie zu **NetScaler Gateway > Benutzerverwaltung**.
2. Klicken Sie auf **AAA-Benutzer**.
3. Wählen Sie im Detailbereich einen Benutzer aus und klicken Sie dann auf **Bearbeiten**.

4. Klicken Sie in **Erweiterte Einstellungen**auf **Autorisierungsrichtlinien**.
5. Wählen Sie auf der Seite **Policy Binding** eine Richtlinie aus oder erstellen Sie eine Richtlinie.
6. Legen Sie unter **Priorität**die Prioritätsnummer fest.
7. Wählen Sie unter **Typ**den Anforderungstyp aus und klicken Sie dann auf **OK**.

Binden Sie mithilfe der GUI eine Autorisierungsrichtlinie an eine Gruppe

1. Navigieren Sie zu **NetScaler Gateway > Benutzerverwaltung**.
2. Klicken Sie auf **AAA-Gruppen**.
3. Wählen Sie im Detailbereich eine Gruppe aus und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie in **Erweiterte Einstellungen**auf **Autorisierungsrichtlinien**.
5. Wählen Sie auf der Seite **Policy Binding** eine Richtlinie aus oder erstellen Sie eine Richtlinie.
6. Legen Sie unter **Priorität**die Prioritätsnummer fest.
7. Wählen Sie unter **Typ**den Anforderungstyp aus und klicken Sie dann auf **OK**.

Die Autorisierung gibt die Netzwerkressourcen an, auf die Benutzer zugreifen können, wenn sie sich bei NetScaler Gateway anmelden. Die Standardeinstellung für die Autorisierung besteht darin, den Zugriff auf alle Netzwerkressourcen zu verweigern. Citrix empfiehlt, die globale Standardeinstellung zu verwenden und dann Autorisierungsrichtlinien zu erstellen, um die Netzwerkressourcen zu definieren, auf die Benutzer zugreifen können.

Sie konfigurieren die Autorisierung auf NetScaler Gateway mithilfe einer Autorisierungsrichtlinie und Ausdrücken. Nachdem Sie eine Autorisierungsrichtlinie erstellt haben, können Sie sie an die Benutzer oder Gruppen binden, die Sie auf der Appliance konfiguriert haben.

Globale Standardautorisierung

Um die Ressourcen zu definieren, auf die Benutzer Zugriff im internen Netzwerk haben, können Sie die globale Standardermächtigung konfigurieren. Sie konfigurieren die globale Autorisierung, indem Sie den Zugriff auf Netzwerkressourcen global im internen Netzwerk zulassen oder verweigern.

Jede globale Autorisierungsaktion, die Sie erstellen, wird auf alle Benutzer angewendet, denen weder direkt noch über eine Gruppe eine Autorisierungsrichtlinie zugeordnet ist. Eine Benutzer- oder Gruppenautorisierungsrichtlinie überschreibt immer die globale Autorisierungsaktion. Wenn die Standardautorisierungsaktion auf Verweigern gesetzt ist, müssen Sie Autorisierungsrichtlinien für alle Benutzer oder Gruppen anwenden, um diesen Benutzern oder Gruppen den Zugriff auf Netzwerkressourcen zu ermöglichen. Diese Anforderung trägt zur Verbesserung der Sicherheit bei.

So legen Sie die globale Standardermächtigung fest:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration” im Navigationsbereich “NetScaler Gateway” und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungenauf Globale Einstellungen ändern.

3. Wählen Sie auf der Registerkarte Sicherheit neben Standardermächtigungsaktion die Option Zulassen oder Verweigern aus und klicken Sie auf OK.

Authentifizierungsprofile

May 11, 2023

Wenn Sie möchten, dass dieselben Authentifizierungseinstellungen von mehreren virtuellen Traffic-Management-Servern verwendet werden, können Sie ein Authentifizierungsprofil erstellen, das den virtuellen Authentifizierungsserver, den Authentifizierungshost, die Authentifizierungsdomäne und die Authentifizierungsebene angibt.

Dieses Authentifizierungsprofil kann den entsprechenden virtuellen Servern für das Verkehrsmanagement zugeordnet werden.

Ein Authentifizierungsprofil konfigurieren

Konfigurieren Sie ein Authentifizierungsprofil mithilfe der CLI

- Erstellen Sie das Authentifizierungsprofil und stellen Sie die erforderlichen Parameter ein.

  Zum Beispiel, um ein Profil mit einem virtuellen Authentifizierungsserver namens „AuthVS“ zu erstellen.

```
1  add authentication authnProfile authProfile1 -authnVsName authVS
      -authenticationHost authnVS.example.com -authenticationDomain
      example.com -authenticationLevel
2  <!--NeedCopy-->
```

> **Hinweis:**
>
> Die Gewichtung oder Stufe der Authentifizierung hängt von dem virtuellen Server ab, an den der Datenverkehr gebunden ist. Eine Sitzung, die durch Authentifizierung gegenüber dem virtuellen Verkehrsmanagementserver auf einer bestimmten Ebene erstellt wird, kann nicht verwendet werden, um auf den virtuellen Verkehrsmanagement-Server auf einer höheren Ebene zuzugreifen.

- Binden Sie das Authentifizierungsprofil an die entsprechenden virtuellen Server für das Verkehrsmanagement.

  Zum Beispiel, um AuthProfile1 an einen virtuellen Load-Balancing-Server namens „vserver1” zu binden.


```
set lb vserver vserver1 -authnProfile authProfile1
<!--NeedCopy-->
```

Konfigurieren Sie ein Authentifizierungsprofil mithilfe der GUI

Navigieren Sie auf der Registerkarte **Konfiguration** zu **Sicherheit > AAA — Anwendungsverkehr > Authentifizierungsprofil**und konfigurieren Sie das Authentifizierungsprofil nach Bedarf.

> **Hinweis:**
>
> - Sie können ein Authentifizierungsprofil auch mithilfe des NetScaler Gateway-Assistenten erstellen. Das Profil enthält alle Einstellungen für die Authentifizierungsrichtlinie. Sie konfigurieren das Profil, wenn Sie die Authentifizierungsrichtlinie erstellen.
> - Mit dem NetScaler Gateway-Assistenten können Sie den ausgewählten Authentifizierungstyp verwenden, um die Authentifizierung zu konfigurieren. Wenn Sie nach dem Ausführen des Assistenten andere Authentifizierungsrichtlinien konfigurieren möchten, können Sie das Konfigurationsdienstprogramm verwenden. Weitere Informationen zum NetScaler Gateway-Assistenten finden Sie unter Konfigurieren von Einstellungen mit dem NetScaler Gateway-Assistenten].

Authentifizierungsrichtlinien

May 11, 2023

Wenn sich Benutzer bei der NetScaler- oder NetScaler Gateway-Appliance anmelden, werden sie gemäß einer von Ihnen erstellten Richtlinie authentifiziert. Eine Authentifizierungsrichtlinie umfasst einen Ausdruck und eine Aktion. Authentifizierungsrichtlinien verwenden NetScaler Ausdrücke.

Nachdem Sie eine Authentifizierungsaktion und eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen Sie ihr eine Priorität zu. Wenn Sie es binden, benennen Sie es auch als primäre oder sekundäre Richtlinie. Primäre Richtlinien werden vor sekundären Richtlinien bewertet. In Konfigurationen, die beide Richtlinientypen verwenden, sind primäre Richtlinien normalerweise spezifischere Richtlinien, während sekundäre Richtlinien normalerweise allgemeinere Richtlinien sind. Es ist für die Authentifizierung aller Benutzerkonten vorgesehen, die die spezifischeren Kriterien nicht erfüllen. Die Richtlinie definiert den Authentifizierungstyp. Eine einzige Authentifizierungsrichtlinie kann für einfache Authentifizierungsanforderungen verwendet werden und ist normalerweise auf globaler Ebene gebunden. Sie können auch den Standardauthentifizierungstyp verwenden, der lokal ist. Wenn Sie

die lokale Authentifizierung konfigurieren, müssen Sie auch Benutzer und Gruppen auf der Appliance konfigurieren.

Sie können mehrere Authentifizierungsrichtlinien konfigurieren und binden, um ein detailliertes Authentifizierungsverfahren und virtuelle Server zu erstellen. Sie können beispielsweise die Kaskadierung und die Zwei-Faktor-Authentifizierung konfigurieren, indem Sie mehrere Richtlinien konfigurieren. Sie können auch die Priorität der Authentifizierungsrichtlinien festlegen, um zu bestimmen, welche Server und die Reihenfolge, in der die Appliance die Benutzeranmeldeinformationen überprüft. Eine Authentifizierungsrichtlinie beinhaltet einen Ausdruck und eine Aktion. Wenn Sie beispielsweise den Ausdruck auf True festlegen, wird bei der Benutzeranmeldung durch die Aktion die Benutzeranmeldung auf true ausgewertet, und Benutzer haben Zugriff auf Netzwerkressourcen.

Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie die Richtlinie entweder auf globaler Ebene oder an virtuelle Server. Wenn Sie mindestens eine Authentifizierungsrichtlinie an einen virtuellen Server binden, werden alle Authentifizierungsrichtlinien, die Sie an die globale Ebene gebunden haben, nicht verwendet, wenn sich Benutzer am virtuellen Server anmelden, es sei denn, der globale Authentifizierungstyp hat eine höhere Priorität als die an den virtuellen Server gebundene Richtlinie.

Wenn sich ein Benutzer an der Appliance anmeldet, wird die Authentifizierung in der folgenden Reihenfolge ausgewertet:

- Der virtuelle Server wird auf gebundene Authentifizierungsrichtlinien überprüft.
- Wenn Authentifizierungsrichtlinien nicht an den virtuellen Server gebunden sind, prüft die Appliance nach globalen Authentifizierungsrichtlinien.
- Wenn eine Authentifizierungsrichtlinie nicht an einen virtuellen Server oder global gebunden ist, wird der Benutzer über den Standardauthentifizierungstyp authentifiziert.

Wenn Sie LDAP- und RADIUS-Authentifizierungsrichtlinien konfigurieren und die Richtlinien für die Zwei-Faktor-Authentifizierung global binden möchten, können Sie die Richtlinie im Konfigurationsdienstprogramm auswählen und dann auswählen, ob es sich bei der Richtlinie um den primären oder sekundären Authentifizierungstyp handelt. Sie können auch eine Gruppenextraktionsrichtlinie konfigurieren.

> **Hinweis:**
>
> Der NetScaler oder das NetScaler Gateway-Gerät codiert nur UTF-8-Zeichen für die Authentifizierung und ist nicht mit Servern kompatibel, die ISO-8859-1-Zeichen verwenden.

Erstellen einer Authentifizierungsrichtlinie

Erstellen einer Authentifizierungsrichtlinie mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung**, und wählen Sie dann den Richtlinientyp aus, den Sie erstellen möchten.

Navigieren Sie für NetScaler Gateway zu **NetScaler Gateway > Richtlinien > Authentifizierung**.

2. Führen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine der folgenden Aktionen aus:
   - Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie im Dialogfeld Authentifizierungsrichtlinie erstellen oder Authentifizierungsrichtlinie konfigurieren die Werte für die Parameter ein oder wählen Sie sie aus.
   - **Name** — Richtlinienname (kann für eine zuvor konfigurierte Aktion nicht geändert werden)
   - **Authentifizierungstyp** — `authtype`
   - **Server** — `authVsName`
   - **Ausdruck** — Regel (Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdown-Liste ganz links unter dem Fenster Ausdruck auswählen und dann den Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und das Dropdown-Menü verwenden listet darin auf, um Ihren Ausdruck zu konstruieren.)
4. Klicken Sie auf **Erstellen** oder **auf OK**. Die von Ihnen erstellte Richtlinie wird auf der Seite Richtlinien angezeigt.
5. Klicken Sie auf die Registerkarte **Server**, und führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um einen vorhandenen Server zu verwenden, wählen Sie ihn aus, und klicken Sie dann auf.
   - Um einen Server zu erstellen, klicken Sie auf Hinzufügen und befolgen Sie die Anweisungen.
6. Wenn Sie diese Richtlinie als sekundäre Authentifizierungsrichtlinie festlegen möchten, klicken Sie auf der Registerkarte Authentifizierung auf Sekundär. Wenn Sie diese Richtlinie als primäre Authentifizierungsrichtlinie festlegen möchten, überspringen Sie diesen Schritt.
7. Klicken Sie auf **Richtlinie einfügen**.
8. Wählen Sie in der Dropdown-Liste die Richtlinie aus, die Sie an den virtuellen Authentifizierungsserver binden möchten.
9. Ändern Sie in der Spalte **Priorität** links die Standardpriorität, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge ausgewertet wird.
10. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

Ändern einer Authentifizierungsrichtlinie mithilfe der GUI

Sie können konfigurierte Authentifizierungsrichtlinien und -profile ändern, z. B. die IP-Adresse des Authentifizierungsservers oder den Ausdruck.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **NetScaler Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Sie können die Richtlinie auch unter **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**konfigurieren und dann den Richtlinientyp auswählen, den Sie ändern möchten.
2. Wählen Sie im Navigationsbereich unter Authentifizierung einen Authentifizierungstyp aus.
3. Wählen Sie im Detailbereich auf der Registerkarte Server einen Server aus und klicken Sie dann auf Öffnen.

Entfernen einer Authentifizierungsrichtlinie mithilfe der GUI

Wenn Sie einen Authentifizierungsserver aus Ihrem Netzwerk geändert oder entfernt haben, entfernen Sie die entsprechende Authentifizierungsrichtlinie aus NetScaler Gateway.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **NetScaler Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Um über ADC zu konfigurieren, navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**, und wählen Sie dann den Richtlinientyp aus, den Sie entfernen möchten.
2. Wählen Sie im Navigationsbereich unter Authentifizierung einen Authentifizierungstyp aus.
3. Wählen Sie im Detailbereich auf der Registerkarte Richtlinien eine Richtlinie aus und klicken Sie dann auf Entfernen.

Erstellen einer Authentifizierungsrichtlinie mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add authentication negotiatePolicy <name> <rule> <reqAction>

show authentication localPolicy <name>

bind authentication vserver <name> -policy <policyname> [-priority <
    priority>][-secondary]]

show authentication vserver <name>
<!--NeedCopy-->
```

Beispiel:


```
add authentication localPolicy Authn-Pol-1 ns_true
Done

show authentication localPolicy
1)      Name: Authn-Pol-1       Rule: ns_true          Request action:
   LOCAL   Done

bind authentication vserver Auth-Vserver-2 -policy Authn-Pol-1
Done

show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT State: UP Client
   Idle
Timeout: 180 sec Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
1)  Primary authentication policy name:  Authn-Pol-1 Priority: 0
Done
<!--NeedCopy-->
```

Ändern einer Authentifizierungsrichtlinie mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine vorhandene Authentifizierungsrichtlinie zu ändern:

```
set authentication localPolicy <name> <rule> [-reqaction <action>]
<!--NeedCopy-->
```

Beispiel

```
set authentication localPolicy Authn-Pol-1 'ns_true'
<!--NeedCopy-->
```

Entfernen einer Authentifizierungsrichtlinie mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Authentifizierungsrichtlinie zu entfernen:

```
rm authentication localPolicy <name>
<!--NeedCopy-->
```


Beispiel

```
rm authentication localPolicy Authn-Pol-1
<!--NeedCopy-->
```

Binden einer Authentifizierungsrichtlinie

Nachdem Sie die Authentifizierungsrichtlinien konfiguriert haben, binden Sie die Richtlinie entweder global oder an einen virtuellen Server. Sie können entweder das Konfigurationsdienstprogramm verwenden, um eine Authentifizierungsrichtlinie zu binden.

So binden Sie eine Authentifizierungsrichtlinie global mithilfe des Konfigurationsdienstprogramms:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **NetScaler Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Um von ADC aus zu konfigurieren, navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**
2. Klicken Sie auf eine Authentifizierungsart.
3. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf einen Server, und klicken Sie dann unter Aktion auf **Globale Bindungen**.
4. Klicken Sie auf der Registerkarte Primär oder Sekundär unter Details auf **Richtlinie einfügen**.
5. Wählen Sie unter Richtlinienname die Richtlinie aus, und klicken Sie dann auf **OK**.

   Hinweis: Wenn Sie die Richtlinie auswählen, setzt NetScaler Gateway den Ausdruck automatisch auf den Wert True.

So heben Sie die Bindung einer globalen Authentifizierungsrichtlinie mithilfe des Konfigurationsdienstprogramms auf:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **NetScaler Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Um von ADC aus zu konfigurieren, navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**
2. Klicken Sie auf der Registerkarte Richtlinien in Aktion auf **Globale Bindungen**.
3. Wählen Sie im Dialogfeld Authentifizierungsrichtlinien an Global binden/unbind auf der Registerkarte Primär oder Sekundär unter Richtlinienname die Richtlinie aus, klicken Sie auf Richtlinie **aufheben**, und klicken Sie dann auf **OK**.

Hinzufügen einer Authentifizierungsaktion

Hinzufügen einer Authentifizierungsaktion mithilfe der CLI

Wenn Sie die LOCAL-Authentifizierung nicht verwenden, müssen Sie eine explizite Authentifizierungsaktion hinzufügen. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 add authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Beispiel

```
1 add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
     serverport 1812 -authtimeout 15 -tacacsSecret "minotaur" -
     authorization OFF -accounting ON -auditFailedCmds OFF -
     defaultAuthenticationGroup "users"
2 <!--NeedCopy-->
```

Konfigurieren einer Authentifizierungsaktion mithilfe der CLI

Um eine vorhandene Authentifizierungsaktion zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 set authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Beispiel

```
1 set authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
     serverport 1812 -authtimeout 15 -tacacsSecret "minotaur" -
     authorization OFF -accounting ON -auditFailedCmds OFF -
     defaultAuthenticationGroup "users"
2 <!--NeedCopy-->
```

Entfernen einer Authentifizierungsaktion mithilfe der Befehlszeilenschnittstelle

Um eine vorhandene RADIUS-Aktion zu entfernen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 rm authentication radiusAction <name>
2 <!--NeedCopy-->
```


Beispiel

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```

Die NoAuth Authentifizierung

Die NetScaler-Appliance unterstützt die NoAuth-Authentifizierungsfunktion, mit der der Kunde einen DefaultAuthenticationGroup-Parameter im `noAuthAction` Befehl konfigurieren kann, wenn ein Benutzer diese Richtlinie ausführt. Der Administrator kann überprüfen, ob diese Gruppe in der Benutzergruppe vorhanden ist, um die Navigation des Benutzers durch die NoAuth-Richtlinie zu bestimmen.

So konfigurieren Sie eine NoAuth-Authentifizierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication noAuthAction <name> [-defaultAuthenticationGroup <
    string>]
<!--NeedCopy-->
```

Beispiel

```
add authentication noAuthAction noauthact -defaultAuthenticationGroup
    mynoauthgroup
<!--NeedCopy-->
```

Standardtypen für globale Authentifizierung

Wenn Sie NetScaler Gateway installiert und den NetScaler Gateway-Assistenten ausgeführt haben, haben Sie die Authentifizierung innerhalb des Assistenten konfiguriert. Diese Authentifizierungsrichtlinie ist automatisch an die globale Ebene von NetScaler Gateway gebunden. Der Authentifizierungstyp, den Sie im NetScaler Gateway-Assistenten konfigurieren, ist der Standardauthentifizierungstyp. Sie können den Standardautorisierungstyp ändern, indem Sie den NetScaler Gateway-Assistenten erneut ausführen, oder Sie können die globalen Authentifizierungseinstellungen im Konfigurationsdienstprogramm ändern.

Wenn Sie weitere Authentifizierungstypen hinzufügen müssen, können Sie Authentifizierungsrichtlinien auf NetScaler Gateway konfigurieren und die Richtlinien mithilfe des Konfigurationsdienstprogramms an NetScaler Gateway binden. Wenn Sie die Authentifizierung global konfigurieren, definieren Sie die Art der Authentifizierung, konfigurieren die Einstellungen und legen die maximale Anzahl von Benutzern fest, die authentifiziert werden können.

Nachdem Sie die Richtlinie konfiguriert und gebunden haben, können Sie die Priorität festlegen, um zu definieren, welcher Authentifizierungstyp Vorrang hat. Beispielsweise konfigurieren Sie LDAP- und RADIUS-Authentifizierungsrichtlinien. Wenn die LDAP-Richtlinie eine Prioritätsnummer von 10 hat und die RADIUS-Richtlinie eine Prioritätsnummer von 15 hat, hat die LDAP-Richtlinie Vorrang, unabhängig davon, wo Sie die einzelnen Richtlinien binden. Dies wird als kaskadierende Authentifizierung bezeichnet.

Sie können Anmeldeseiten aus dem In-Memory-Cache von NetScaler Gateway oder vom HTTP-Server bereitstellen, der auf NetScaler Gateway ausgeführt wird. Wenn Sie die Anmeldeseite aus dem In-Memory-Cache bereitstellen möchten, erfolgt die Bereitstellung der Anmeldeseite von NetScaler Gateway schneller als vom HTTP-Server. Wenn Sie die Anmeldeseite aus dem In-Memory-Cache bereitstellen, wird die Wartezeit reduziert, wenn sich viele Benutzer gleichzeitig anmelden. Sie können die Bereitstellung von Anmeldeseiten aus dem Cache nur als Teil einer globalen Authentifizierungsrichtlinie konfigurieren.

Sie können auch die IP-Adresse der Netzwerkadressübersetzung (NAT) konfigurieren, bei der es sich um eine bestimmte IP-Adresse für die Authentifizierung handelt. Diese IP-Adresse ist für die Authentifizierung eindeutig und nicht das NetScaler Gateway-Subnetz, zugeordnete oder virtuelle IP-Adressen. Dies ist eine optionale Einstellung.

> **Hinweis:**
>
> - Sie können den NetScaler Gateway-Assistenten nicht zum Konfigurieren der SAML-Authentifizierung verwenden.
> - Sie können den Schnellkonfigurations-Assistenten verwenden, um die LDAP-, RADIUS- und Clientzertifikatauthentifizierung zu konfigurieren. Wenn Sie den Assistenten ausführen, können Sie aus einem vorhandenen LDAP- oder RADIUS-Server auswählen, der auf NetScaler Gateway konfiguriert ist. Sie können die Einstellungen auch für LDAP oder RADIUS konfigurieren. Wenn Sie die Zwei-Faktor-Authentifizierung verwenden, empfiehlt Citrix die Verwendung von LDAP als primären Authentifizierungstyp.

Konfigurieren der globalen Standardauthentifizierung

1. Erweitern Sie in der GUI auf der Registerkarte Konfiguration im Navigationsbereich **NetScaler Gateway,** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Einstellungen auf **Authentifizierungseinstellungen ändern**.
3. Geben Sie im **Feld Maximale Anzahl an Benutzern**die Anzahl der Benutzer ein, die mit diesem Authentifizierungstyp authentifiziert werden können.
4. Geben Sie im **Feld NAT-IP-Adresse**die eindeutige IP-Adresse für die Authentifizierung ein.
5. Wählen Sie**Statisches Caching aktivieren aus, um Anmeldeseiten schneller bereitzustellen**.
6. Wählen Sie **Erweitertes Authentifizierungsfeedback aktivieren aus, um Benutzern eine Nachricht zu senden, falls die Authentifizierung fehlschlägt** Die Nachricht, die Benutzer

erhalten, enthält die Kennwortfehler, das deaktivierte oder gesperrte Konto oder der Benutzer wurde nicht gefunden, um nur einige zu nennen.

7. Wählen Sie unter **Standard-Authentifizierungstyp**den Authentifizierungstyp aus.
8. Konfigurieren Sie die Einstellungen für Ihren Authentifizierungstyp, und klicken Sie dann auf **OK**.

Unterstützung für das Abrufen aktueller Anmeldeversuche für einen Benutzer

Die NetScaler Appliance bietet eine Option zum Abrufen des Werts der aktuellen Anmeldeversuche für einen Benutzer durch einen neuen Ausdruck `aaa.user.login_attempts`. Der Ausdruck akzeptiert entweder ein Argument (Benutzername) oder kein Argument. Wenn es kein Argument gibt, holt der Ausdruck den Benutzernamen aus dem `aaa_session` oder `aaa_info`.

Sie können den `aaa.user.login_attempts` Ausdruck mit Authentifizierungsrichtlinien für die weitere Verarbeitung verwenden.

So konfigurieren Sie die Anzahl der Anmeldeversuche pro Benutzer mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add expression er aaa.user.login_attempts
```

Benutzer und Gruppen

May 11, 2023

Nachdem Sie die grundlegenden Einstellungen für Authentifizierung, Autorisierung und Überwachung konfiguriert haben, erstellen Sie Benutzer und Gruppen. Sie erstellen zunächst ein Benutzerkonto für jede Person, die sich über die NetScaler-Appliance authentifiziert. Wenn Sie die lokale Authentifizierung verwenden, die von der NetScaler Appliance selbst gesteuert wird, erstellen Sie lokale Benutzerkonten und weisen jedem dieser Konten Kennwörter zu.

Sie erstellen auch Benutzerkonten auf der NetScaler-Appliance, wenn Sie einen externen Authentifizierungsserver verwenden. In diesem Fall muss jedoch jedes Benutzerkonto genau mit einem Konto für diesen Benutzer auf dem externen Authentifizierungsserver übereinstimmen, und Sie weisen den Benutzerkonten, die Sie auf dem NetScaler erstellen, keine Passwörter zu. Der externe Authentifizierungsserver verwaltet die Passwörter für Benutzer, die sich beim externen Authentifizierungsserver authentifizieren.

Wenn Sie einen externen Authentifizierungsserver verwenden, können Sie trotzdem lokale Benutzerkonten auf der NetScaler-Appliance erstellen, wenn Sie beispielsweise temporären Benutzern

(wie Besuchern) die Anmeldung ermöglichen möchten, aber keine Einträge für diese Benutzer auf dem Authentifizierungsserver erstellen möchten. Sie weisen jedem lokalen Benutzerkonto ein Passwort zu, genau wie Sie es tun würden, wenn Sie die lokale Authentifizierung für alle Benutzerkonten verwenden würden.

Jedes Benutzerkonto muss an Richtlinien für Authentifizierung und Autorisierung gebunden sein. Um diese Aufgabe zu vereinfachen, können Sie eine oder mehrere Gruppen erstellen und ihnen Benutzerkonten zuweisen. Sie können dann Richtlinien an Gruppen statt an einzelne Benutzerkonten binden.

Richtlinien mit Gruppen konfigurieren

Nachdem Sie Gruppen konfiguriert haben, können Sie das Dialogfeld **Gruppe** verwenden, um Richtlinien und Einstellungen anzuwenden, die den Benutzerzugriff festlegen. Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen sie Gruppen hinzu, die auf NetScaler Gateway konfiguriert sind. Die Benutzer erben dann die Einstellungen für diese Gruppe.

Im Dialogfeld Gruppe können Sie die folgenden Richtlinien oder Einstellungen für eine **Gruppe** von Benutzern konfigurieren:

- Benutzer
- Richtlinien zur Autorisierung
- Richtlinien für die Prüfung
- Sitzungsrichtlinien
- Traffic-Richtlinien
- Lesezeichen
- Intranetanwendungen
- Intranet-IP-Adressen

In Ihrer Konfiguration haben Sie möglicherweise Benutzer, die zu mehr als einer Gruppe gehören. Darüber hinaus kann jede Gruppe über eine oder mehrere gebundene Sitzungsrichtlinien verfügen, wobei verschiedene Parameter konfiguriert sind. Benutzer, die zu mehr als einer Gruppe gehören, erben die Sitzungsrichtlinien, die allen Gruppen zugewiesen sind, zu denen der Benutzer gehört. Um sicherzustellen, welche Sitzungsrichtlinienbewertung Vorrang vor der anderen hat, müssen Sie die Priorität der Sitzungsrichtlinie festlegen.

Beispielsweise haben Sie Gruppe1, die an eine Sitzungsrichtlinie gebunden ist, die mit der Homepage www.homepage1.com konfiguriert ist. Group2 ist an eine Sitzungsrichtlinie gebunden, die mit der Homepage www.homepage2.com konfiguriert ist. Wenn diese Richtlinien ohne Prioritätsnummer oder mit derselben Prioritätsnummer an entsprechende Gruppen gebunden sind, hängt die Homepage, die Benutzern angezeigt wird, die beiden Gruppen angehören, davon ab, welche Richtlinie zuerst verarbeitet wird. Durch Festlegen einer niedrigeren Prioritätszahl, die höhere Priorität hat, für

die Sitzungsrichtlinie mit Homepage www.homepage1.com können Sie sicherstellen, dass Benutzer, die beiden Gruppen angehören, die Homepage www.homepage1.com erhalten.

Wenn Sitzungsrichtlinien keine Prioritätsnummer zugewiesen wurde oder dieselbe Prioritätsnummer hat, wird die Priorität in der folgenden Reihenfolge ausgewertet:

- Benutzer
- Gruppe
- Virtueller Server
- Global

Wenn Richtlinien an dieselbe Ebene ohne Prioritätsnummer gebunden sind oder wenn die Richtlinien dieselbe Prioritätsnummer haben, entspricht die Reihenfolge der Bewertung der Richtlinienbindungsreihenfolge. Richtlinien, die zuerst an eine Ebene gebunden sind, haben Vorrang vor später gebundenen Richtlinien.

Wenn wir einen Benutzer haben, der an mehrere Gruppen gebunden ist, wobei jede Gruppe IIP gebunden ist, kann der Benutzer kostenlose IP von jeder der gebundenen Gruppen erhalten.

Benutzer und Gruppen erstellen

Konfigurieren Sie die Authentifizierung, Autorisierung und Überwachung lokaler Benutzer mithilfe der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Benutzer**
   aus NetScaler Gateway, erweitern Sie **NetScaler Gateway > Benutzerverwaltung**und klicken Sie dann auf **AAA-Benutzer.**
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um ein neues Benutzerkonto zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um ein vorhandenes Benutzerkonto zu ändern, wählen Sie das Benutzerkonto aus, und klicken Sie dann auf **Öffnen**.
3. Geben **Sie im Dialogfeld AAA-Benutzer erstellen** in das Textfeld **Benutzername** einen Namen für den Benutzer ein.
4. Wenn Sie ein lokal authentifiziertes Benutzerkonto erstellen, deaktivieren Sie das Kontrollkästchen **Externe Authentifizierung** und geben Sie ein lokales Passwort ein, mit dem sich der Benutzer anmeldet.
5. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass der Benutzer erfolgreich konfiguriert wurde.

Konfigurieren Sie lokale Gruppen für Authentifizierung, Autorisierung und Überwachung und fügen Sie ihnen Benutzer hinzu, indem Sie das Konfigurationsprogramm verwenden

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Gruppen**
   von NetScaler Gateway, erweitern Sie **NetScaler Gateway > Benutzerverwaltung**und klicken Sie dann auf **AAA-Gruppen.**
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Gruppe zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine bestehende Gruppe zu ändern, wählen Sie die Gruppe aus, und klicken Sie dann auf **Bearbeiten**.
3. Wenn Sie eine neue Gruppe **erstellen, geben Sie im Dialogfeld AAA-Gruppe** erstellen in das Textfeld **Gruppenname** einen Namen für die Gruppe ein.
4. Klicken Sie rechts im Bereich **Erweitert** auf **AAA-Benutzer**.
   - Um der Gruppe einen Benutzer hinzuzufügen, wählen Sie den Benutzer aus, und klicken Sie dann auf **Hinzufügen**.
   - Um einen Benutzer aus der Gruppe zu entfernen, wählen Sie den Benutzer aus, und klicken Sie dann auf **Entfernen**.
   - Um ein neues Benutzerkonto zu erstellen und es der Gruppe hinzuzufügen, klicken Sie auf das **Plus-Symbol** und folgen Sie dann den Anweisungen unter „So konfigurieren Sie die Authentifizierung, Autorisierung und Überwachung lokaler Benutzer mithilfe des Konfigurationsprogramms“. „
5. Klicken Sie auf **Erstellen** oder **auf OK**. Die Gruppe, die Sie erstellt haben, wird auf der Seite **AAA-Gruppen** angezeigt.

Löschen Sie eine Gruppe mithilfe der GUI

Sie können Benutzergruppen auch aus NetScaler Gateway löschen.

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Gruppen**
   aus NetScaler Gateway, erweitern Sie Citrix **Gateway > Benutzerverwaltung** und klicken Sie dann auf **AAA-Gruppen.**
   Wählen Sie im Detailbereich die Gruppe aus, und klicken Sie dann auf Entfernen.

Konfigurieren Sie die Authentifizierung, Autorisierung und Überwachung lokaler Benutzer über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 add aaa group <groupname>
```



```
2
3 bind aaa group <groupname> -username <username>
4 <!--NeedCopy-->
```

Beispiel:

```
1 add aaa group group-2
2
3 bind aaa group group-2 -username user-2
4 <!--NeedCopy-->
```

Entfernen Sie Benutzer mithilfe der Befehlszeilenschnittstelle aus einer Authentifizierungs-, Autorisierungs- und Überwachungsgruppe

Entbinden Sie Benutzer an der Befehlszeile von der Gruppe, indem Sie den folgenden Befehl einmal für jedes Benutzerkonto eingeben, das an die Gruppe gebunden ist:

```
1 unbind aaa group <groupname> -username <username><!--NeedCopy-->
```

```
1 **Beispiel:**
2
3 <!--NeedCopy-->
```

unbind aaa group group-hr -username user-hr-1

```
1 ### Entfernen Sie eine Authentifizierungs-, Autorisierungs- und Ü
     berwachungsgruppe mithilfe der Befehlszeilenschnittstelle
2
3 Entfernen Sie zunächst alle Benutzer aus der Gruppe. Geben Sie dann an
     der Befehlszeile den folgenden Befehl ein, um eine NetScaler AAA-
     Gruppe zu entfernen und die Konfiguration zu überprüfen:
4
5 <!--NeedCopy-->
```

rm aaa group

```
1 **Beispiel:**
2
3 <!--NeedCopy-->
```

rm aaa group group-hr

```
1 > **Hinweis**
2 >
```



```
>Sie können keinen Benutzernamen mit Domäne hinzufügen, wenn der
    Benutzername bereits ohne Domäne hinzugefügt wurde. Wenn der
    Benutzername mit Domäne zuerst hinzugefügt wird, gefolgt von
    demselben Benutzernamen ohne Domäne, fügt die NetScaler-Appliance
    den Benutzernamen zur Benutzerliste hinzu.

Das folgende Beispiel zeigt, dass das Hinzufügen eines Benutzernamens
    mit Domäne nicht zulässig ist, wenn derselbe Benutzername ohne Domä
    ne hinzugefügt wird.

<!--NeedCopy-->
```

```
add aaa user u47985
Done
show aaa users
1) UserName: u47985
Done
add aaa user u47985@domain.com
ERROR: User already exists
‘‘‘
```

Das folgende Beispiel zeigt, wenn der Benutzername mit Domäne zuerst gefolgt von demselben Benutzernamen ohne Domäne hinzugefügt wird, dann fügt die NetScaler Appliance den Benutzernamen zur Benutzerliste hinzu.

```
> add aaa user u47985@domain.com
Done
> add aaa user u47985
Done
> sh aaa user
1)   UserName: u47985@domain.com
2)   UserName: u47985
```

‘‘‘

Authentifizierungsmethoden

May 11, 2023

Die NetScaler-Appliance kann Benutzer mit lokalen Benutzerkonten oder mithilfe eines externen Authentifizierungsservers authentifizieren. Die Appliance unterstützt die folgenden Authentifizierungstypen:

- **LOKAL:** Authentifiziert sich bei der NetScaler-Appliance mithilfe eines Kennworts ohne Verweis auf einen externen Authentifizierungsserver. Benutzerdaten werden lokal auf der NetScaler-Appliance gespeichert.
- **RADIUS:** Authentifizieren Sie sich bei einem externen RADIUS-Server.
- **LDAP:** Authentifiziert sich bei einem externen LDAP-Authentifizierungsserver.
- **TACACS:** Authentifiziert sich bei einem externen Terminal Access Controller Access-Control System (TACACS) -Authentifizierungsserver.
- **CERT:** Authentifiziert sich bei der NetScaler-Appliance mithilfe eines Client-Zertifikats ohne Verweis auf einen externen Authentifizierungsserver.
- **VERHANDELN:** Authentifiziert sich bei einem Kerberos-Authentifizierungsserver. Wenn bei der Kerberos-Authentifizierung ein Fehler auftritt, verwendet NetScaler die NTLM-Authentifizierung.
- **SAML:** Authentifiziert sich bei einem Server, der die Security Assertion Markup Language (SAML) unterstützt.
- **SAML IDP:** Konfiguriert den NetScaler so, dass er als Security Assertion Markup Language (SAML) Identity Provider (IdP) dient.
- **WEB:** Authentifiziert sich bei einem Webserver, stellt die Anmeldeinformationen bereit, die der Webserver in einer HTTP-Anfrage benötigt, und analysiert die Webserver-Antwort, um festzustellen, dass die Benutzerauthentifizierung erfolgreich war.
- **Natives OTP:** Die NetScaler-Appliance unterstützt Einmalkennwörter (OTPs), ohne dass ein Server eines Drittanbieters verwendet werden muss.
- **Push-Benachrichtigung:** NetScaler Gateway unterstützt Push-Benachrichtigungen für OTP. Benutzer müssen das auf ihren registrierten Geräten empfangene OTP nicht manuell eingeben, um sich bei NetScaler Gateway anzumelden. Administratoren können NetScaler Gateway so konfigurieren, dass Anmeldebenachrichtigungen mithilfe von Pushbenachrichtigungsdiensten an die registrierten Geräte der Benutzer gesendet werden.
- **E-Mail-OTP:** Mit der E-Mail-OTP-Methode können Sie sich mit dem Einmalkennwort (OTP) authentifizieren, das an die registrierte E-Mail-Adresse gesendet wird. Wenn Sie versuchen, sich bei einem Dienst zu authentifizieren, sendet der Server ein OTP an die registrierte E-Mail-Adresse des Benutzers.
- **reCAPTCHA-Authentifizierung** — NetScaler Gateway unterstützt die neue First-Class-Aktion „CaptchaAction“, die die reCAPTCHA-Konfiguration vereinfacht. Da es sich bei reCAPTCHA um eine erstklassige Aktion handelt, kann es ein eigenständiger Faktor sein. Sie können reCAPTCHA an einer beliebigen Stelle im nFactor-Flow einfügen.

- **nFactor-Authentifizierung:** Die Multifaktor-Authentifizierung erhöht die Sicherheit einer Anwendung, indem Benutzer mehrere Identitätsnachweise vorlegen müssen, um Zugriff zu erhalten. Die NetScaler Appliance bietet einen erweiterbaren und flexiblen Ansatz zur Konfiguration der Multifaktor-Authentifizierung. Dieser Ansatz wird als nFactor-Authentifizierungbezeichnet.
- **OAuth-Authentifizierung:** Die OAuth-Authentifizierung autorisiert und authentifiziert Benutzer für Dienste, die auf Anwendungen wie Google, Facebook und Twitter gehostet werden.

nFactor-Authentifizierung

September 1, 2023

> **Wichtig**
>
> - Die nFactor-Authentifizierung wird ab NetScaler 11.0 Build 62.x unterstützt.
> - Damit die nFactor-Authentifizierung mit NetScaler arbeitet, ist eine Advanced-Lizenz oder eine Premium-Lizenz erforderlich.
> - Ab Release 13.0 Build 67.x wird die nFactor-Authentifizierung nur mit der Standardlizenz für virtuelle Gateway/VPN-Server unterstützt. Weitere Informationen zur nFactor-Authentifizierung mit NetScaler Gateway finden Sie unter nFactor for Gateway-Authentifizierung.
> - Die nFactor-Authentifizierung wird für den Linux-Client nicht unterstützt.

Die Multifaktor-Authentifizierung erhöht die Sicherheit einer Anwendung, indem Benutzer mehrere Identitätsnachweise vorlegen müssen, um Zugriff zu erhalten. Die NetScaler Appliance bietet einen erweiterbaren und flexiblen Ansatz zur Konfiguration der Multifaktor-Authentifizierung. Dieser Ansatz wird als *nFactor-Authentifizierung*bezeichnet.

So funktioniert die nFactor-Authentifizierung

Jeder Authentifizierungsfaktor führt die folgenden Aufgaben aus:

- Sammelt Anmeldeinformationen vom Benutzer. Zu den von NetScaler unterstützten Authentifizierungsmechanismen gehören LDAP, RADIUS, SAML-Assertion, Clientzertifikat, OAuth OpenID Connect, Kerberos und so weiter.
- Wertet die bereitgestellten Anmeldeinformationen aus, um zu entscheiden, ob die Authentifizierung erfolgreich war, fehlgeschlagen ist oder die Aktionen wie Gruppenextraktion, Attributextraktion durchgeführt werden sollen.
- Basierend auf den Bewertungsergebnissen wird der Zugriff entweder gewährt, verweigert oder ein nächster Faktor wird ausgewählt.

- Wiederholen Sie diese Schritte, bis keine nächsten Faktoren mehr bewertet werden müssen.

Mit der nFactor-Authentifizierung können Sie:

- Konfigurieren Sie eine beliebige Anzahl von Authentifizierungsfaktoren.
- Basieren Sie die Auswahl des nächsten Faktors auf das Ergebnis der Ausführung des vorherigen Faktors.
- Passen Sie die Login-Schnittstelle an. Sie können beispielsweise die Labelnamen, Fehlermeldungen und den Hilfetext anpassen.
- Extrahieren Sie Benutzergruppeninformationen ohne Authentifizierung.
- Konfigurieren Sie Passthrough für einen Authentifizierungsfaktor. Dies bedeutet, dass für diesen Faktor keine explizite Login-Interaktion erforderlich ist.
- Konfigurieren Sie die Reihenfolge, in der verschiedene Authentifizierungstypen angewendet werden. Jeder der Authentifizierungsmechanismen, die auf der NetScaler-Appliance unterstützt werden, kann als jeder Faktor des nFactor-Authentifizierungs-Setups konfiguriert werden. Diese Faktoren werden in der Reihenfolge ausgeführt, in der sie konfiguriert sind.
- Konfigurieren Sie die NetScaler Appliance so, dass sie mit einem Authentifizierungsfaktor fortfährt, der ausgeführt werden muss, wenn die Authentifizierung fehlschlägt. Dazu konfigurieren Sie eine andere Authentifizierungsrichtlinie mit derselben Bedingung, jedoch mit der nächsthöheren Priorität und mit der Aktion auf “NO_AUTH” festgelegt. Sie müssen den nächsten Faktor konfigurieren, der den anzuwendenden alternativen Authentifizierungsmechanismus angeben muss.

Verschlüsselung von NetScaler Gateway-Anmeldeinformationen zur nFactor-Authentifizierung

NetScaler Gateway mit nFactor-Authentifizierung kann die Anmeldeanforderungsfelder verschlüsseln, die von einem Client (Browser oder SSO-Apps) während des Authentifizierungsprozesses eingereicht werden. Die Felder für verschlüsselte Anmeldeanfragen bieten eine zusätzliche Sicherheitsebene, um die sensiblen Daten des Benutzers vor der Offenlegung zu schützen.

Kompatible Browser

In der folgenden Tabelle sind die Browser zusammen mit Versionsdetails aufgeführt, die die Anmeldeverschlüsselung unterstützen.

Browser	Version
Chrome	78 und höher
Firefox	69 und höher
Edge	42 und höher

Browser	Version
Safari	11.0 und höher
Oper	66

Kompatible Clients

Im folgenden Abschnitt werden die Clients zusammen mit Versionsdetails aufgeführt, die die Verschlüsselung von NetScaler Gateway-Anmeldeinformationen unterstützen.

- Die Citrix Workspace-App unter Mac unterstützt die Verschlüsselung nur, wenn die Betriebssystemversion 10.14.x und höher ist.
- Die Citrix SSO App unter Mac unterstützt die Verschlüsselung nur, wenn die Betriebssystemversion 10.14.x und höher ist.
- Die Windows SSO-App hat keine Einschränkungen hinsichtlich der Kompatibilität.

So aktivieren Sie die Login-Verschlüsselung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

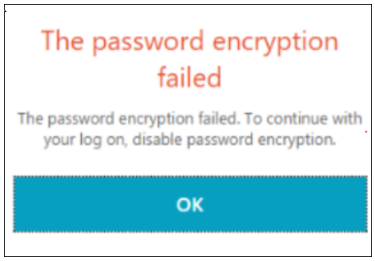
```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

> **Hinweis**
>
> Der Parameter loginEncryption ist standardmäßig auf DISABLED gesetzt. Sie müssen ihn auf ENABLE setzen.

So aktivieren Sie die Anmeldungsverschlüsselung mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr** und klicken Sie im Abschnitt**Authentifizierungseinstellungen** auf **AAA-Einstellungen für Authentifizierungseinstellungen ändern**.
2. Scrollen Sie auf der Seite **AAA-Parameter konfigurieren** nach unten zur Option **Login Encryption** und aktivieren Sie sie.

> **Wichtiger Hinweis zur Login-Verschlüsselung:**
>
> Wenn Sie versuchen, sich bei NetScaler Gateway anzumelden, wird in den folgenden Szenarien eine Fehlermeldung (siehe Screenshot) angezeigt:
>
> - Die Login-Verschlüsselung ist aktiviert.
> - Es wird ein nicht unterstützter Browser verwendet.

> Sie können den Vorschlag, die Login-Verschlüsselung zu deaktivieren, ignorieren. Stellen Sie jedoch sicher, dass Sie einen unterstützten Browser für eine erfolgreiche Anmeldung verwenden.
>
> 
>

nFactor Konzepte, Entitäten und Terminologie

May 11, 2023

In diesem Thema werden einige der wichtigsten an der nFactor-Authentifizierung beteiligten Entitäten und ihre Bedeutung beschrieben.

Login-Schema

nFactor entkoppelt die 'Ansicht', die Benutzeroberfläche, mit dem 'Modell', das die Laufzeitbehandlung darstellt. Die Ansicht von nFactor wird durch das Anmeldeschema definiert. Das Anmeldeschema ist eine Entität, die definiert, was der Benutzer sieht, und angibt, wie die Daten aus dem Benutzer extrahiert werden.

Zum Definieren einer Ansicht verweist das Anmeldeschema auf eine Datei auf dem Datenträger, der das Anmeldeformular definiert. Diese Datei muss der Spezifikation des "Citrix Common Forms Protocol" entsprechen. Diese Datei ist im Wesentlichen eine XML-Definition des Anmeldeformulars.

Zusätzlich zur XML-Datei enthält das Anmeldeschema erweiterte Richtlinienausdrücke, um Benutzernamen und Kennwort aus der Anmeldeanforderung des Benutzers abzurufen. Diese Ausdrücke sind optional und können weggelassen werden, wenn Benutzername und Kennwort des Benutzers mit den erwarteten Variablennamen in Form kommen.

Das Anmeldeschema definiert auch, ob der aktuelle Satz von Anmeldeinformationen als standardmäßige SingleSignOn-Anmeldeinformationen verwendet werden muss.

Das Anmeldeschema kann durch Ausführen des folgenden CLI-Befehls erstellt werden:

```
1    add authentication loginSchema <name> -authenticationSchema <string>
         [-userExpression <string>] [-passwdExpression <string>] [-
        userCredentialIndex <positive_integer>] [-passwordCredentialIndex
         <positive_integer>] [-authenticationStrength <positive_integer>]
         [-SSOCredentials ( YES | NO )]
```



```
<!--NeedCopy-->
```

> **Hinweis:**
>
> **SSOCredentials** geben an, ob die aktuellen Faktor-Anmeldeinformationen die standardmäßigen SSO-Anmeldeinformationen sind. Der Standardwert ist NEIN.
>
> In der nFactor-Authentifizierungskonfiguration werden die letzten Faktor-Anmeldeinformationen standardmäßig für SSO verwendet. Mithilfe der Konfiguration " **ssoCredentials** " können Anmeldeinformationen für den aktuellen Faktor verwendet werden. Falls diese Konfiguration auf verschiedene Faktoren festgelegt ist, hat der letzte Faktor, für den diese Konfiguration festgelegt ist, die Priorität.

Einzelheiten zu den einzelnen Parametern finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-loginSchema/#add-authentication-loginschema.

Bezeichnung der Richtlinie

Ein Policy Label ist eine Sammlung von Richtlinien. Es ist ein Konstrukt, das der Richtlinieninfrastruktur von NetScaler nicht fremd ist. Die Richtlinienbezeichnung definiert einen Authentifizierungsfaktor. Das heißt, es enthält alle Richtlinien, die erforderlich sind, um festzustellen, ob die Anmeldeinformationen des Benutzers erfüllt sind. Alle Richtlinien in einem Policy Label können als homogen angenommen werden. Die Richtlinienbezeichnung für die Authentifizierung kann keine Richtlinien unterschiedlichen Typs annehmen, z. B. Um es anders auszudrücken, überprüfen alle Richtlinien in einem Policy Label meistens dasselbe Kennwort/dieselben Anmeldeinformationen des Benutzers. Das Ergebnis von Richtlinien in einem PolicyLabel folgt der logischen ODER-Bedingung. Wenn die in der ersten Richtlinie angegebene Authentifizierung erfolgreich ist, werden andere darauf folgende Richtlinien übersprungen.

Die Richtlinienbezeichnung kann durch Ausführen des folgenden CLI-Befehls erstellt werden:

```
add authentication policy label mylabel  - loginSchema <>
<!--NeedCopy-->
```

Ein Policy Label verwendet das Anmeldeschema als Eigenschaft. Das Anmeldeschema definiert die Ansicht für dieses Policy Label. Wenn das Anmeldeschema nicht angegeben ist, wird ein implizites Anmeldeschema, LSCHEMA_INT, mit dieser Policy Label verknüpft. Das Anmeldeschema entscheidet, ob ein Policy Label zu einem Passthrough wird oder nicht.

Virtuelles Serverlabel

In der erweiterten Richtlinieninfrastruktur von NetScaler ist ein virtueller Server auch eine implizite Policy Label. Das liegt daran, dass der virtuelle Server auch mit mehr als einer Richtlinie gebunden werden kann. Ein virtueller Server ist jedoch etwas Besonderes, da er der Einstiegspunkt für den Clientverkehr ist und Richtlinien eines anderen Typs annehmen kann. Jede der Richtlinien, die es unter einem eigenen Label innerhalb des virtuellen Servers platziert hat. Daher ist der virtuelle Server ein Konglomerat von Labels.

Der nächste Faktor

Immer wenn eine Richtlinie an einen virtuellen Server oder eine Policy Label gebunden ist, kann sie mit dem nächsten Faktor angegeben werden. Der nächste Faktor bestimmt, was getan werden muss, wenn eine bestimmte Authentifizierung erfolgreich ist. Wenn es keinen nächsten Faktor gibt, ist damit der Authentifizierungsprozess für diesen Benutzer abgeschlossen.

Jede Richtlinie, die an einen virtuellen Server oder eine Policy Label gebunden ist, kann einen anderen nächsten Faktor haben. Dies ermöglicht ultimative Flexibilität, bei der der Erfolg jeder Richtlinie einen neuen Pfad für die Benutzerauthentifizierung definieren kann. Der Administrator kann diese Tatsache nutzen und clevere Fallback-Faktoren für Benutzer erstellen, die bestimmte Richtlinien nicht erfüllen.

Richtlinie ohne Authentifizierung

nFactor führt eine spezielle integrierte Richtlinie namens NO_AUTHN ein. Die NO_AUTHN-Richtlinie gibt immer Erfolg als Authentifizierungsergebnis zurück. Die `No-auth` Richtlinie kann erstellt werden, indem Sie den folgenden CLI-Befehl ausführen:

```
1 add authentication policy noauthpolicy -rule <> -action NO_AUTHN
2 <!--NeedCopy-->
```

Gemäß dem Befehl benötigt die `no-authentication` Richtlinie eine Regel, die ein beliebiger erweiterter Richtlinienausdruck sein kann. Das Authentifizierungsergebnis ist von NO_AUTHN immer erfolgreich.

Eine `no-auth`-Richtlinie an sich scheint keinen Mehrwert zu bieten. Wenn sie jedoch zusammen mit Passthrough-Richtlinienbezeichnungen verwendet wird, bietet es eine große Flexibilität, logische Entscheidungen zu treffen, um den Fluss der Benutzerauthentifizierung zu fördern. NO_AUTHN-Richtlinien und Passthrough-Faktoren bieten eine neue Dimension der Flexibilität von nFactor.

Hinweis: Sehen Sie sich die Beispiele für die Verwendung von `no-auth` und Passthrough in den nachfolgenden Abschnitten an.

Durchgangsfaktor/Etikett

Sobald der Benutzer die Authentifizierung auf dem virtuellen Server bestanden hat (für den ersten Faktor), erfolgen nachfolgende Authentifizierungen bei Richtlinienbezeichnungen oder benutzerdefinierten (sekundären) Faktoren.
Jede Richtlinienbeschriftung/jeder Faktor ist mit einer Anmeldeschemaentität verknüpft, um die Ansicht für diesen Faktor anzuzeigen. Auf diese Weise können Ansichten basierend auf dem Pfad angepasst werden, den der Benutzer eingeschlagen hätte, um zu einem bestimmten Faktor zu gelangen.

Es gibt spezielle Arten von Richtlinienbezeichnungen, die nicht explizit auf ein Anmeldeschema verweisen. Spezialisierte Richtlinienbezeichnungen verweisen auf ein Anmeldeschema, das nicht wirklich auf die XML-Datei für die Ansicht verweist. Diese Richtlinienbezeichnungen/-faktoren werden als “Passthrough” -Faktoren bezeichnet.

Passthrough-Faktoren können durch Ausführen der folgenden CLI-Befehle erstellt werden:

Beispiel 1:

```
1 add authentication policylabel example1
2 <!--NeedCopy-->
```

Beispiel 2:

```
1 add loginschema passthrough_schema  -authenticationSchema noschema
2
3 add authentication policylabel example2  -loginschema
     passthrough_schema
4 <!--NeedCopy-->
```

Der Passthrough-Faktor impliziert, dass das Authentifizierungs-, Autorisierungs- und Überwachungssubsystem nicht an den Benutzer zurückgehen darf, um die für diesen Faktor festgelegten Anmeldeinformationen abzurufen. Stattdessen ist es ein Hinweis für Authentifizierung, Autorisierung und Überwachung, um mit bereits erhaltenen Anmeldeinformationen fortzufahren. Dies ist nützlich in Fällen, in denen ein Benutzereingriff nicht erwünscht ist. Zum Beispiel

- Wenn dem Benutzer zwei Kennwortfelder angezeigt werden, benötigt der zweite Faktor nach dem ersten Faktor keinen Benutzereingriff.
- Wenn die Authentifizierung eines Typs (z. B. eines Zertifikats) abgeschlossen ist und der Administrator Gruppen für diesen Benutzer extrahieren muss.

Der Passthrough-Faktor kann mit `NO_AUTH` Richtlinien verwendet werden, um bedingte Sprünge zu erstellen.

nFactor-Authentifizierungsablauf

Die Authentifizierung beginnt immer auf dem virtuellen Server in nFactor. Virtueller Server definiert den ersten Faktor für den Benutzer. Das erste Formular, das der Benutzer sieht, wird vom virtuellen Server bedient. Das Anmeldeformular, das der Benutzer sieht, kann auf dem virtuellen Server mithilfe von Anmeldeschemarichtlinien angepasst werden. Wenn es keine Richtlinien für Anmeldeschemas gibt, werden dem Benutzer ein einziger Benutzername und ein Kennwortfeld angezeigt.

Wenn dem Benutzer mehr als ein Kennwortfeld in einem angepassten Formular angezeigt werden muss, müssen Richtlinien für das Anmeldeschema verwendet werden. Sie ermöglichen die Anzeige verschiedener Formulare basierend auf den konfigurierten Regeln (z. B. Intranetbenutzer im Vergleich zu externen Benutzern, Dienstanbieter A im Vergleich zu Dienstanbieter B).

Sobald die Benutzeranmeldeinformationen veröffentlicht wurden, beginnt die Authentifizierung beim virtuellen Authentifizierungsserver, dem ersten Faktor. Da der virtuelle Authentifizierungsserver mit mehreren Richtlinien konfiguriert werden kann, wird jede von ihnen in einer Reihenfolge ausgewertet. Zu einem bestimmten Zeitpunkt, wenn eine Authentifizierungsrichtlinie erfolgreich ist, wird der nächste dafür angegebene Faktor verwendet. Wenn es keinen nächsten Faktor gibt, wird der Authentifizierungsvorgang beendet. Wenn der nächste Faktor existiert, wird geprüft, ob dieser Faktor ein Passthrough-Faktor oder ein regulärer Faktor ist. Wenn das Passthrough ist, werden Authentifizierungsrichtlinien für diesen Faktor ohne Benutzereingriff ausgewertet. Andernfalls wird das mit diesem Faktor verknüpfte Anmeldeschema dem Benutzer angezeigt.

Beispiel für die Verwendung von Passthrough-Faktor und Richtlinien ohne Authentifizierung, um logische Entscheidungen zu treffen

Der Administrator möchte NextFactor basierend auf Gruppen entscheiden.

```
1  add authentication policylabel group check
2
3  add authentication policy admin group  - rule http.req.user.is_member_of
       ("Administrators")  - action NO_AUTHN
4
5  add authentication policy nonadmins  - rule true  - action NO_AUTHN
6
7  bind authentication policy label group check  - policy admingroup  - pri
       1  - nextFactor factor-for-admin
8
9  bind authentication policy label groupcheck  - policy nonadmins  - pri 10
        - nextfactor factor-for-others
10
11 add authentication policy first_factor_policy  - rule <> -action <>
12
```



```
bind authentication vserver <> -policy first_factor_policy  - priority
    10  - nextFactor groupcheck
<!--NeedCopy-->
```

NFactor-Authentifizierung konfigurieren

June 19, 2023

Mit der nFactor-Konfiguration können Sie mehrere Authentifizierungsfaktoren konfigurieren. Die nFactor-Konfiguration wird nur in NetScaler Advanced- und Premium-Editionen unterstützt.

Methoden zur Konfiguration von nFactor

Sie können die nFactor-Authentifizierung mit einer der folgenden Methoden konfigurieren:

- **nFactor Visualizer:** nFactor Visualizer ermöglicht es Ihnen, Faktoren oder Richtlinienbeschriftungen einfach in einem einzigen Bereich miteinander zu verknüpfen und auch die Verknüpfung der Faktoren im selben Bereich zu ändern. Sie können mit dem Visualizer einen nFactor-Flow erstellen und diesen Fluss an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver binden. Einzelheiten zu nFactor Visualizer und ein Beispiel für eine nFactor-Konfiguration mit dem Visualizer finden Sie unter nFactor Visualizer für eine vereinfachte Konfiguration.
- **NetScaler GUI:** Einzelheiten finden Sie im Abschnitt **Konfigurationselemente, die an der nFactor Konfiguration beteiligt sind**.
- **NetScaler CLI:** Ein Beispielausschnitt zur nFactor-Konfiguration mit der NetScaler CLI finden Sie unter Beispielausschnitt zur nFactor-Konfiguration unter Verwendung der NetScaler CLI.

> **Wichtig:** Dieses Thema enthält Details zum Konfigurieren von nFactor über die NetScaler GUI.

An der nFactor-Konfiguration beteiligte Konfigurationselemente

Die folgenden Elemente sind an der Konfiguration von nFactor beteiligt. Ausführliche Schritte finden Sie in den entsprechenden Abschnitten in diesem Thema.

Konfigurations-Element	Zu erledigende Aufgaben
Virtueller AAA-Server	Erstellen Sie einen virtuellen AAA-Server
	Binden Sie das Portal-Thema an den virtuellen AAA-Server

Konfigurations-Element	Zu erledigende Aufgaben
	Clientzertifikatauthentifizierung
Login-Schema	Konfigurieren eines Anmeldeschemaprofils
	Erstellen und Binden einer Login-Schemarichtlinie
Erweiterte Authentifizierungsrichtlinien	Erstellen erweiterter Authentifizierungsrichtlinien
	Binden Sie die erweiterte Authentifizierungsrichtlinie für den ersten Faktor an den virtuellen NetScaler AAA-Server
	Verwenden Sie extrahierte LDAP-Gruppen, um den nächsten Authentifizierungsfaktor auszuwählen
Bezeichnung für Authentifizierungsricht	Erstellen einer Authentifizierungsrichtlinien
	Beschriftung der Authentifizierungsrichtlinie binden
nFactor für NetScaler Gateway	Erstellen Sie ein Authentifizierungsprofil, um einen virtuellen NetScaler AAA-Server mit dem virtuellen NetScaler Gateway-Server zu verbinden
	Konfigurieren von SSL-Parametern und CA-Zertifikat für NetScaler Gateway
	Konfigurieren der NetScaler Gateway-Verkehrsrichtlinie für nFactor Single Sign-On bei StoreFront

So funktioniert nFactor

Wenn ein Benutzer eine Verbindung mit dem Authentifizierungs-, Autorisierungs- und Überwachungsserver oder dem virtuellen NetScaler Gateway-Server herstellt, ist die Reihenfolge der Ereignisse wie folgt:

1. Wenn die formularbasierte Authentifizierung verwendet wird, wird das Anmeldeschema angezeigt, das an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden ist.
2. Erweiterte Authentifizierungsrichtlinien, die an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden sind, werden ausgewertet

- Wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist und wenn der nächste Faktor (Bezeichnung der Authentifizierungsrichtlinie) konfiguriert ist, wird der nächste Faktor ausgewertet. Wenn Next Factor nicht konfiguriert ist, ist die Authentifizierung abgeschlossen und erfolgreich.
- Wenn die erweiterte Authentifizierungsrichtlinie fehlschlägt und Gehe zu Ausdruck auf Weiter festgelegt ist, wird die nächste gebundene erweiterte Authentifizierungsrichtlinie ausgewertet. Wenn keine der erweiterten Authentifizierungsrichtlinien erfolgreich ist, schlägt die Authentifizierung fehl.

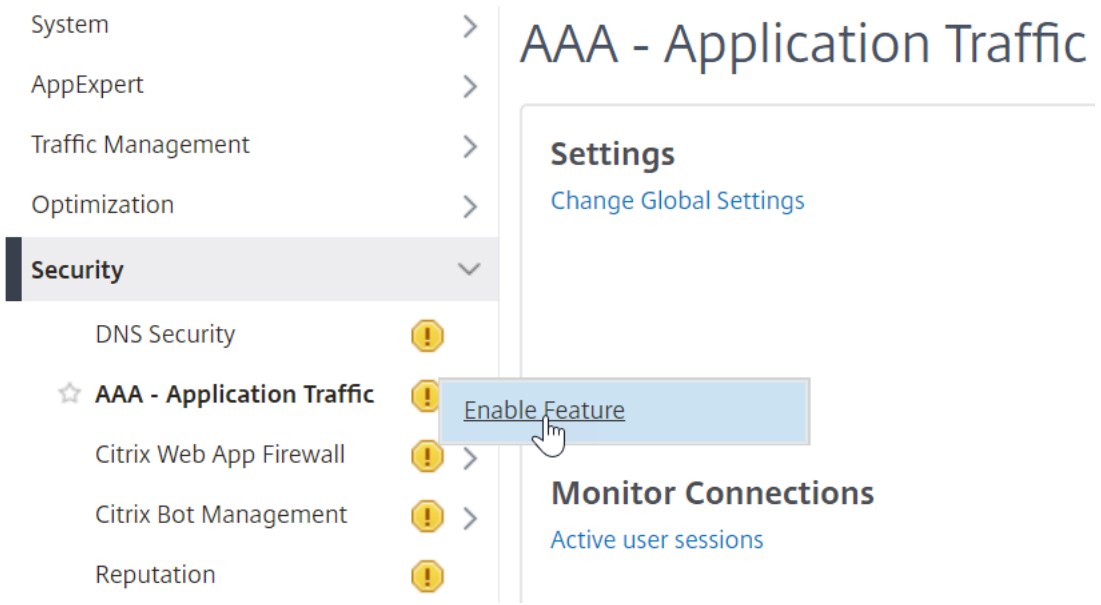
3. Wenn an das Label der nächsten Faktor-Authentifizierungsrichtlinie ein Login-Schema gebunden ist, wird es dem Benutzer angezeigt.
4. Die erweiterten Authentifizierungsrichtlinien, die an die Bezeichnung der nächsten Faktor-Authentifizierungsrichtlinie gebunden sind, werden ausgewertet
   - Wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist und wenn der nächste Faktor (Bezeichnung der Authentifizierungsrichtlinie) konfiguriert ist, wird der nächste Faktor ausgewertet.
   - Wenn Next Factor nicht konfiguriert ist, ist die Authentifizierung abgeschlossen und erfolgreich.
5. Wenn die erweiterte Authentifizierungsrichtlinie fehlschlägt und Gehe zu Ausdruck Weiter ist, wird die nächste gebundene erweiterte Authentifizierungsrichtlinie ausgewertet.
6. Wenn die Richtlinien erfolgreich sind, schlägt die Authentifizierung fehl.

Authentifizierung, Autorisierung und Überwachung des virtuellen Servers

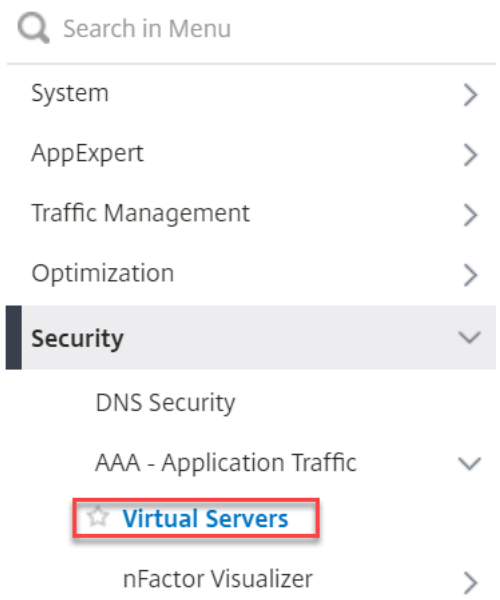
Um nFactor mit NetScaler Gateway zu verwenden, konfigurieren Sie es zunächst auf einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver. Anschließend verknüpfen Sie später den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver mit dem virtuellen NetScaler Gateway-Server.

Erstellen von Authentifizierung, Autorisierung und Überwachung von Virtual Server

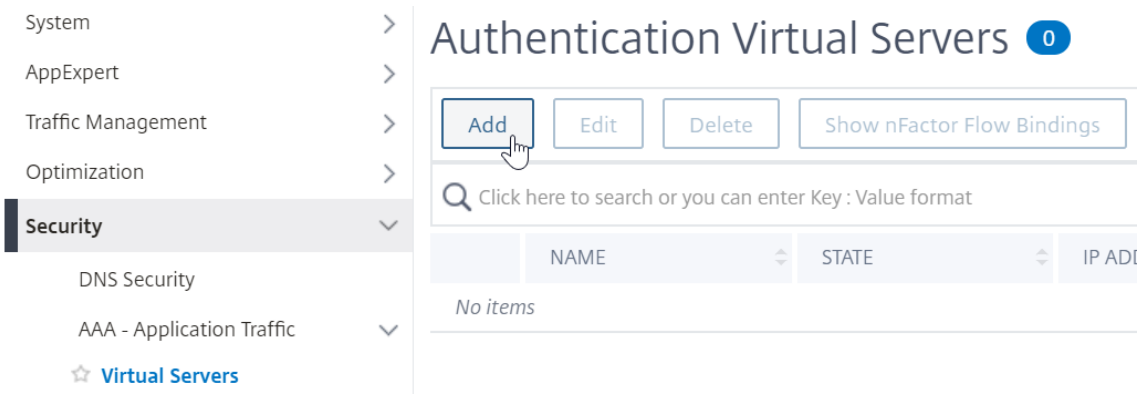
1. Wenn die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion noch nicht aktiviert ist, navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr**, und klicken Sie mit der rechten Maustaste, um die Funktion zu aktivieren.



2. Navigieren Sie zu **Konfiguration > Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**.

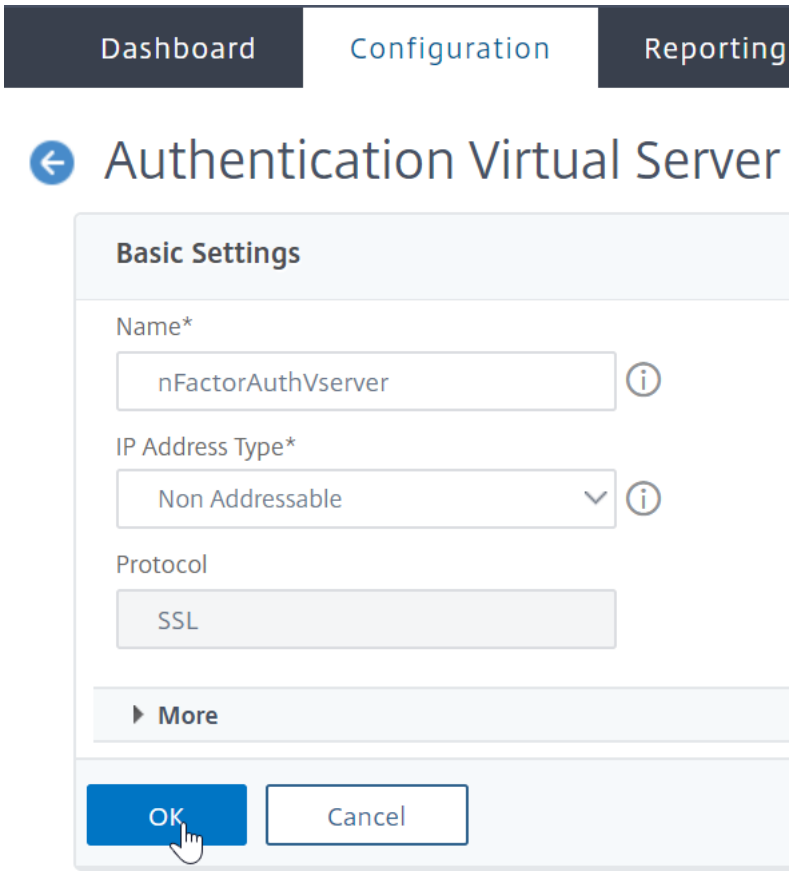


3. Klicken Sie auf **Hinzufügen**, um einen virtuellen Authentifizierungsserver zu erstellen.

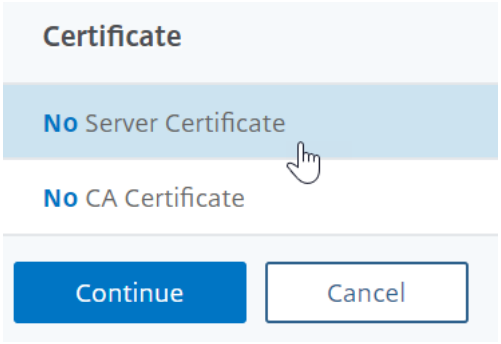


4. Geben Sie die folgenden Informationen ein und klicken Sie auf **OK**.

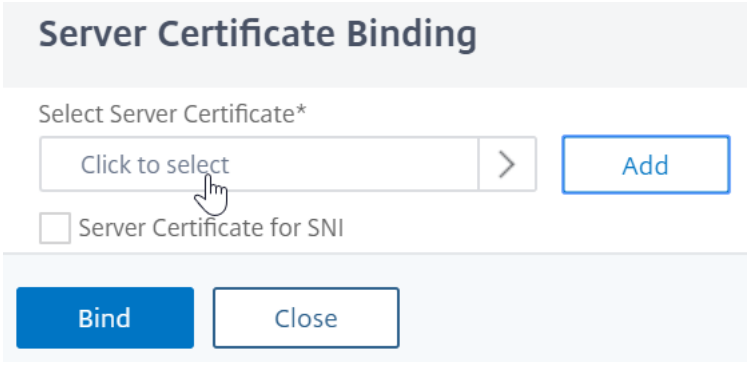
Name des Parameters	Beschreibung des Parameters
Name	Name für den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.
Typ der IP-Adresse	Ändern Sie den IP-Adresstyp in **Nicht adressierbar**, wenn dieser virtuelle Server nur für NetScaler Gateway verwendet wird.



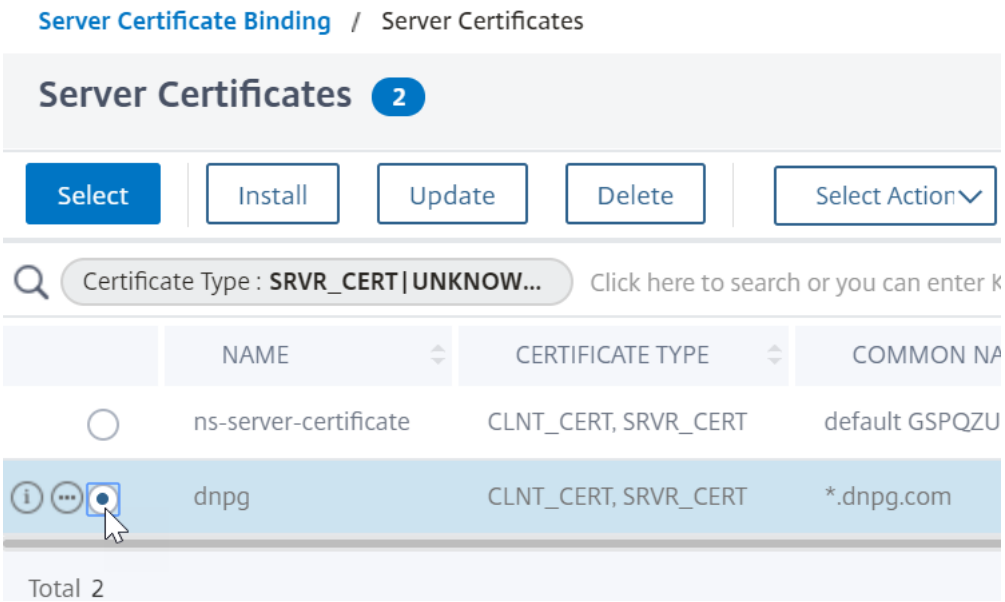
5. Wählen Sie unter Zertifikat **Kein Serverzertifikat**aus.



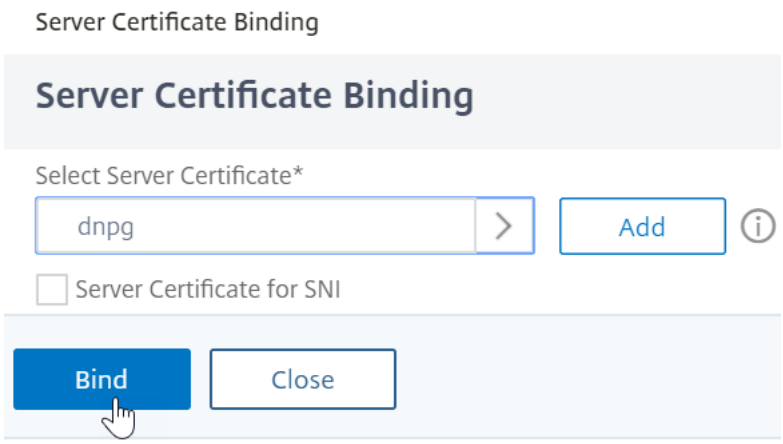
6. Klicken Sie auf den Text, **Klicken Sie**, um das Serverzertifikat auszuwählen.



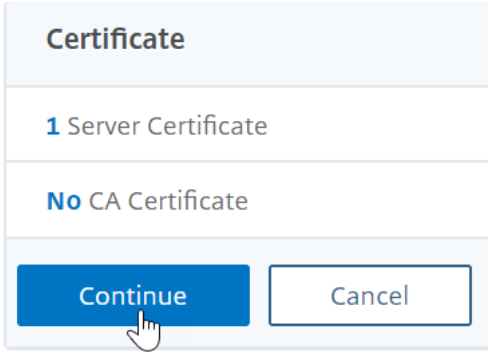
7. Klicken Sie auf das Optionsfeld neben einem Zertifikat für die Authentifizierung, Autorisierung und Überwachung von Virtual Server, und klicken Sie auf **Auswählen**. Das gewählte Zertifikat spielt keine Rolle, da auf diesen Server nicht direkt zugegriffen werden kann.



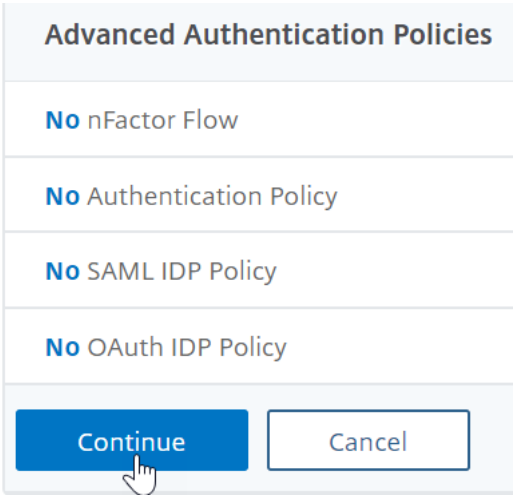
8. Klicken Sie auf **Bind**.



9. Klicken Sie auf **Weiter**, um den Abschnitt **Zertifikat** zu schließen.



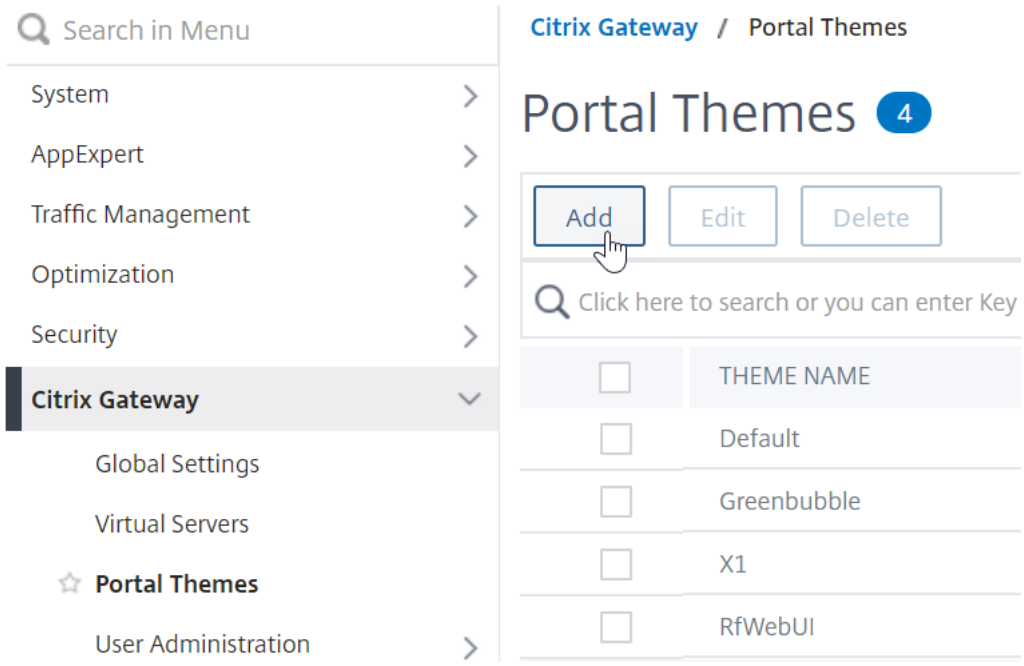
10. Klicken Sie auf **Weiter**.



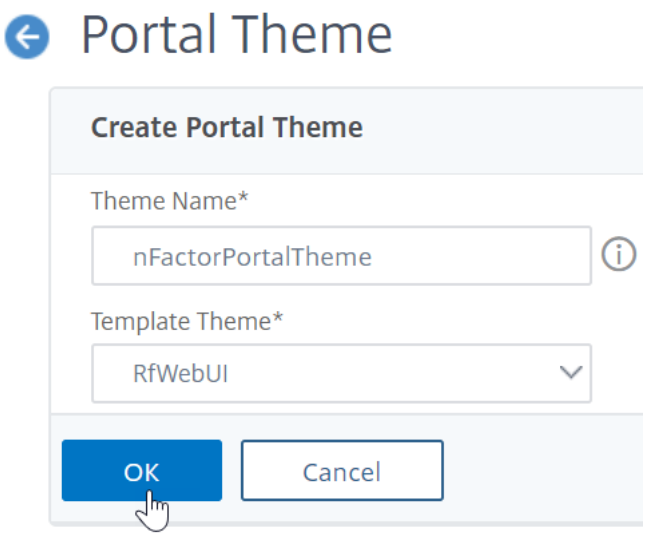
Binden Sie das Portaldesign an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver

1. Navigieren Sie zu **NetScaler Gateway > Portal Themes**, und fügen Sie ein Thema hinzu. Sie erstellen das Design unter NetScaler Gateway und binden es später an den virtuellen

Authentifizierungs-, Autorisierungs- und Überwachungsserver.

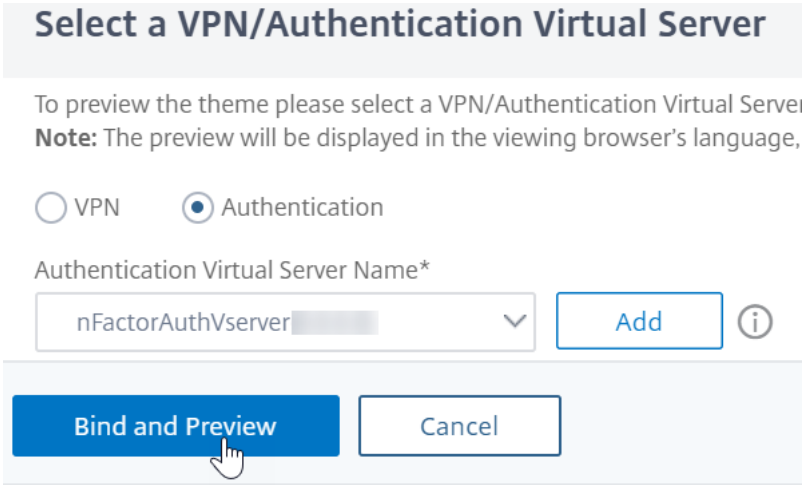


2. Erstellen Sie ein Thema basierend auf dem RfWebUI-Vorlagenthema.



3. Nachdem Sie das Thema wie gewünscht angepasst haben, klicken Sie oben auf der Bearbeitungsseite des Portal-Themas auf **Klicken, um das konfigurierte Thema zu binden und anzuzeigen**.

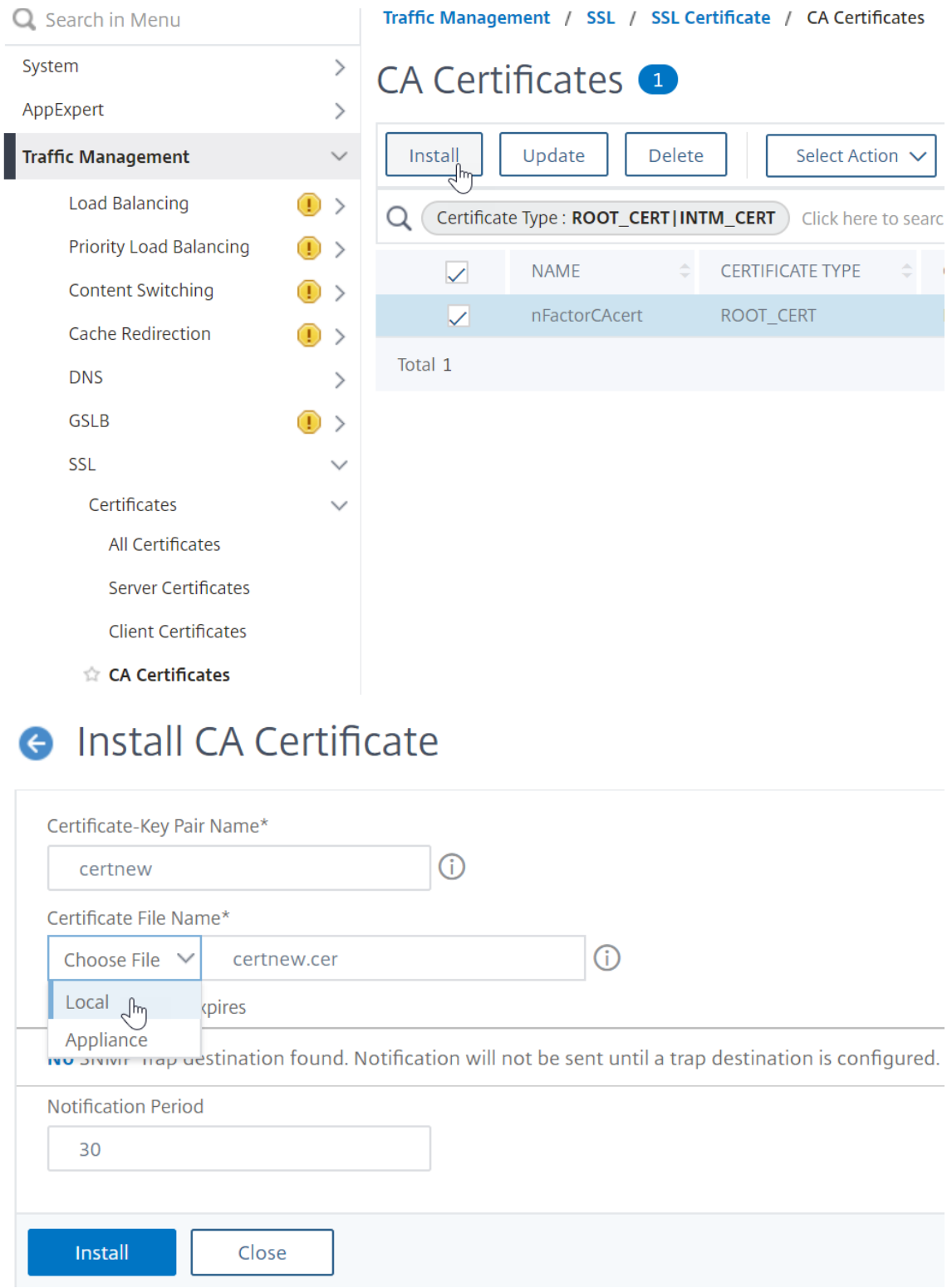
4. Ändern Sie die Auswahl auf Authentifizierung. Wählen Sie im Dropdown-Menü **Name des virtuellen Authentifizierungsservers** den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver aus, klicken Sie auf **Binden und Vorschau**, und schließen Sie das Vorschaufenster.



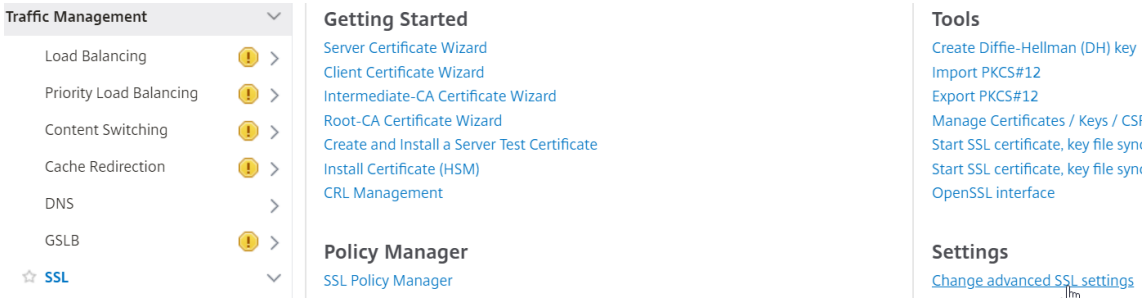
Aktivieren der Clientzertifikatauthentifizierung

Wenn einer Ihrer Authentifizierungsfaktoren das Clientzertifikat ist, müssen Sie eine SSL-Konfiguration für den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver durchführen:

1. Navigieren Sie zu **Traffic Management > SSL > Certificates > CA Certificates**, und installieren Sie das Stammzertifikat für den Aussteller der Clientzertifikate. Stammzertifikate haben keine Schlüsseldatei.



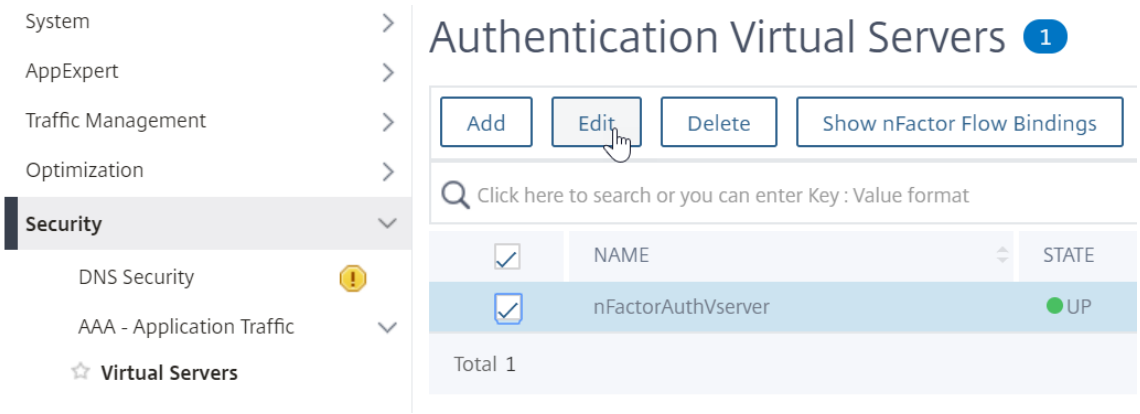
2. Navigieren Sie zu **Traffic Management > SSL > Erweiterte SSL-Einstellungen ändern**.



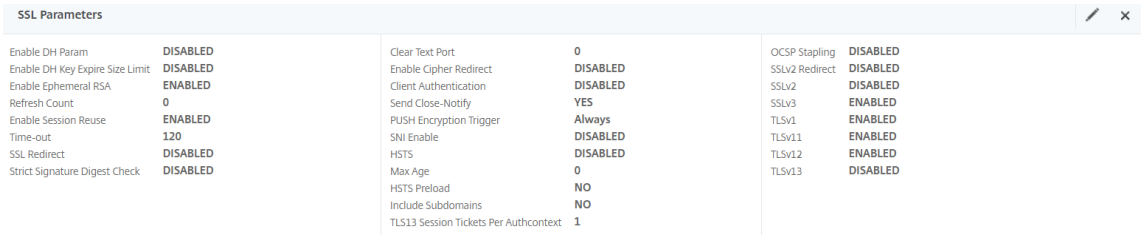
a) Scrollen Sie nach unten, um zu überprüfen, ob **StandardprofilAKTIVIERT**ist Wenn ja, müssen Sie ein SSL-Profil verwenden, um die Clientzertifikatauthentifizierung zu aktivieren. Andernfalls können Sie die Clientzertifikatauthentifizierung direkt auf dem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver im Abschnitt SSL-Parameter aktivieren.

3. Wenn Standard-SSL-Profile nicht aktiviert sind:

   a) Navigieren Sie zu **Sicherheit > AAA — Anwendung > Virtuelle Server**, und bearbeiten Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

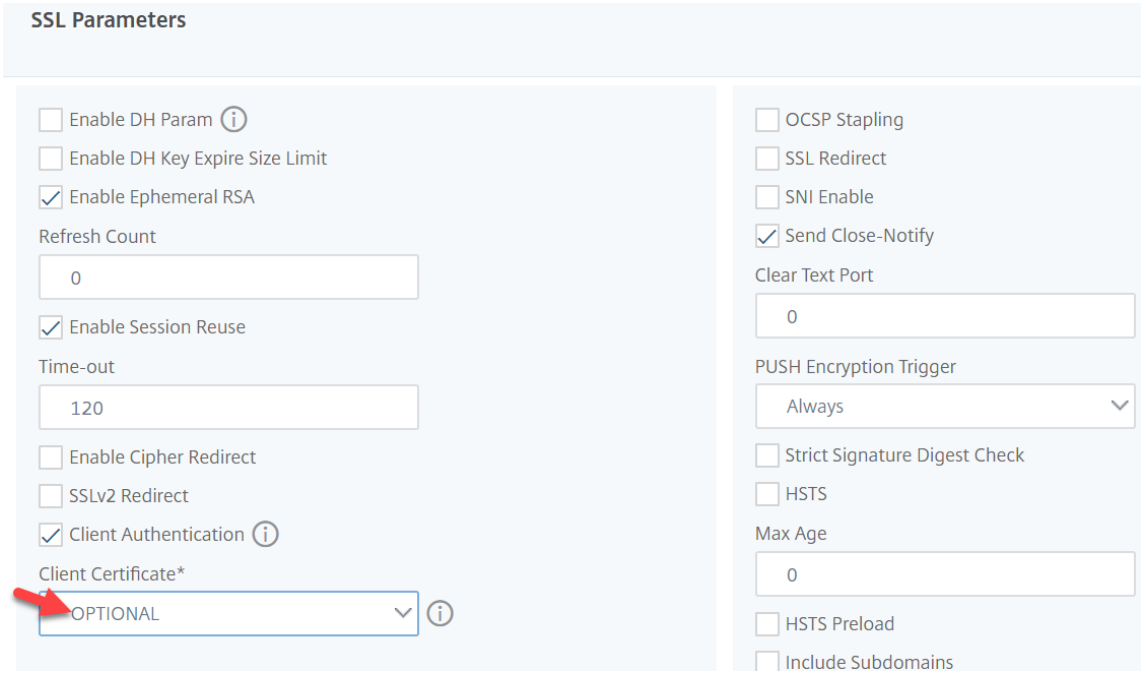


   a) Klicken Sie links im Abschnitt **SSL-Parameter** auf das Stiftsymbol.



   a) Markieren Sie das Kästchen neben **Clientauthentifizierung**.

   b) Stellen Sie sicher, dass im Dropdown-Menü **ClientzertifikatOptional**ausgewählt ist, und klicken Sie auf**OK**.



4. Wenn Standard-SSL-Profile aktiviert sind, erstellen Sie ein SSL-Profil mit aktivierter Clientauthentifizierung:

   a) Erweitern Sie im linken Menü System, und klicken Sie auf Profile.

   b) Wechseln Sie rechts oben zur Registerkarte SSL-Profil.

   c) Klicken Sie mit der rechten Maustaste auf das Profil ns_default_ssl_profile_frontend, und klicken Sie auf Hinzufügen. Dadurch werden Einstellungen aus dem Standardprofil kopiert.

   d) Gib dem Profil einen Namen. Der Zweck dieses Profils besteht darin, Clientzertifikate zu aktivieren.

   e) Scrollen Sie nach unten und suchen Sie das Kontrollkästchen Clientauthentifizierung Markieren Sie das Kästchen.

   f) Ändern Sie das Dropdown-Menü Clientzertifikat in OPTIONAL.

   g) Beim Kopieren des Standard-SSL-Profils werden die SSL-Verschlüsselungen nicht kopiert. Sie müssen sie wiederholen.

   h) Klicken Sie auf Fertig, wenn Sie das SSL-Profil erstellt haben.

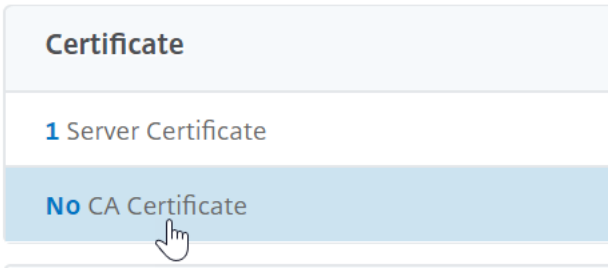
   i) Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**, und bearbeiten Sie einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

   j) Scrollen Sie nach unten zum Abschnitt SSL-Profil und klicken Sie auf den Stift.

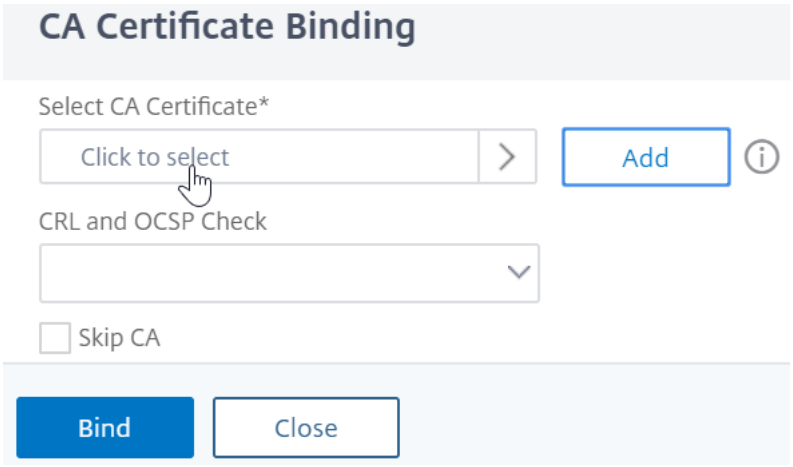
   k) Ändern Sie das Dropdown-Menü SSL-Profil in das Profil, für das Clientzertifikate aktiviert sind. Klicken Sie auf OK.

l) Scrollen Sie in diesem Artikel nach unten, bis Sie die Anweisungen zum Binden des CA-Zertifikats erreichen.

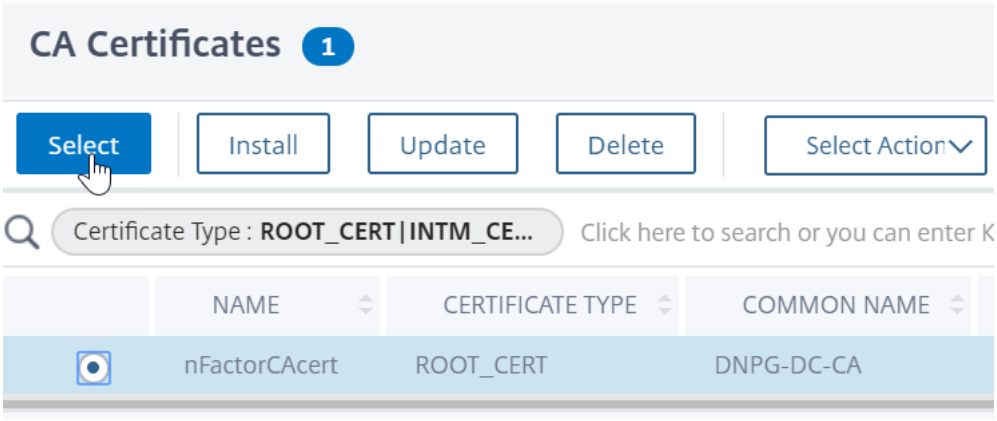
5. Klicken Sie links im Abschnitt **Zertifikate** auf die Stelle, an der **kein CA-Zertifikat**steht.



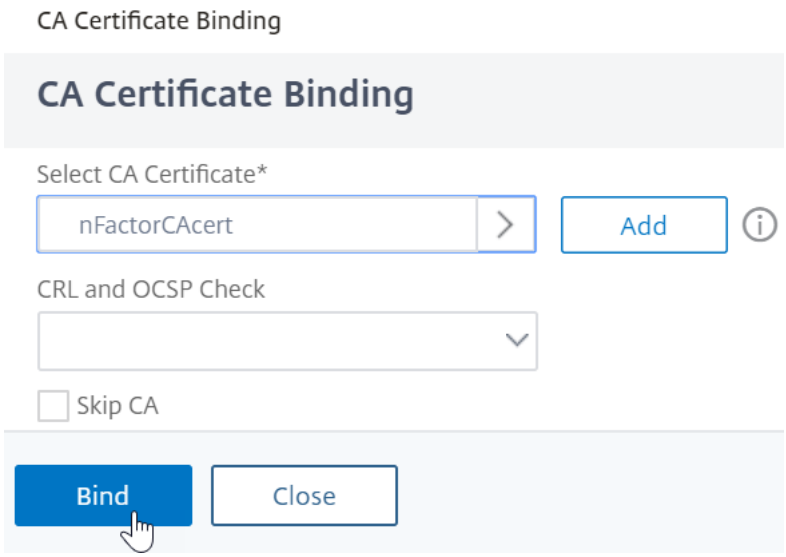
6. Klicken Sie auf den Text, **klicken Sie zum Auswählen**.



7. Klicken Sie auf das Optionsfeld neben dem Stammzertifikat für den Aussteller der Clientzertifikate, und klicken Sie auf **Auswählen**.



8. Klicken Sie auf **Bind**.



Anmeldeschema-XML-Datei

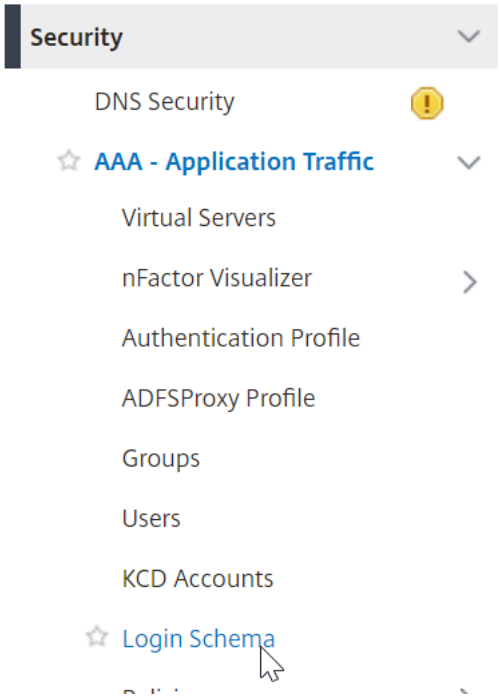
Das Anmeldeschema ist eine XML-Datei, die die Struktur formularbasierter Authentifizierungs-Anmeldeseiten bereitstellt.

nFactor impliziert mehrere Authentifizierungsfaktoren, die miteinander verkettet sind. Jeder Faktor kann verschiedene Login-Schema-Seiten/Dateien haben. In einigen Authentifizierungsszenarien können Benutzern mehrere Anmeldebildschirme angezeigt werden.

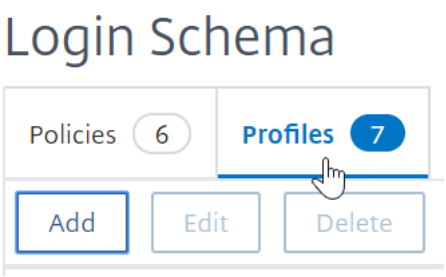
Konfigurieren eines Anmeldeschemaprofils

So konfigurieren Sie ein Login-Schema-Profil:

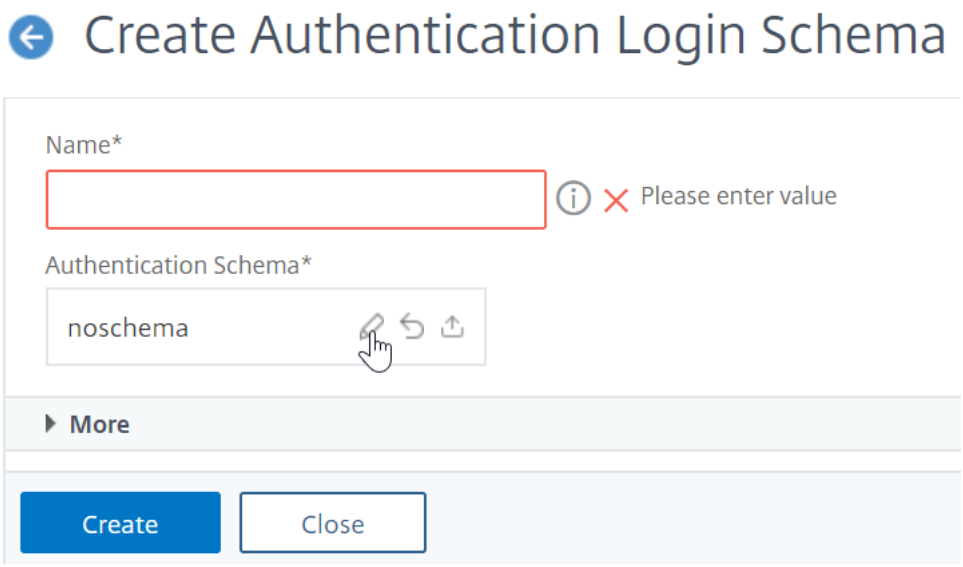
1. Erstellen oder bearbeiten Sie eine .XML-Datei für das Login Schema basierend auf Ihrem nFactor-Design.
2. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Anmeldeschema**.



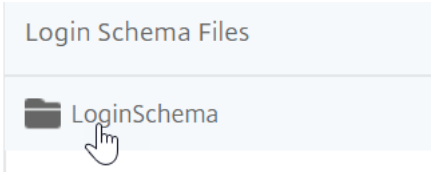
3. Wechseln Sie rechts zur Registerkarte **Profile** und klicken Sie auf **Hinzufügen**.



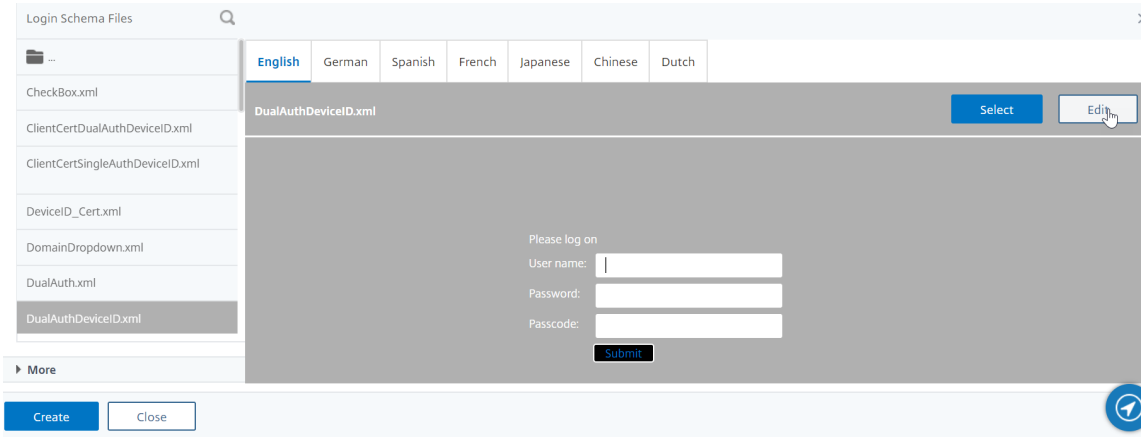
4. Klicken Sie im Feld **Authentifizierungsschema** auf das Stiftsymbol.



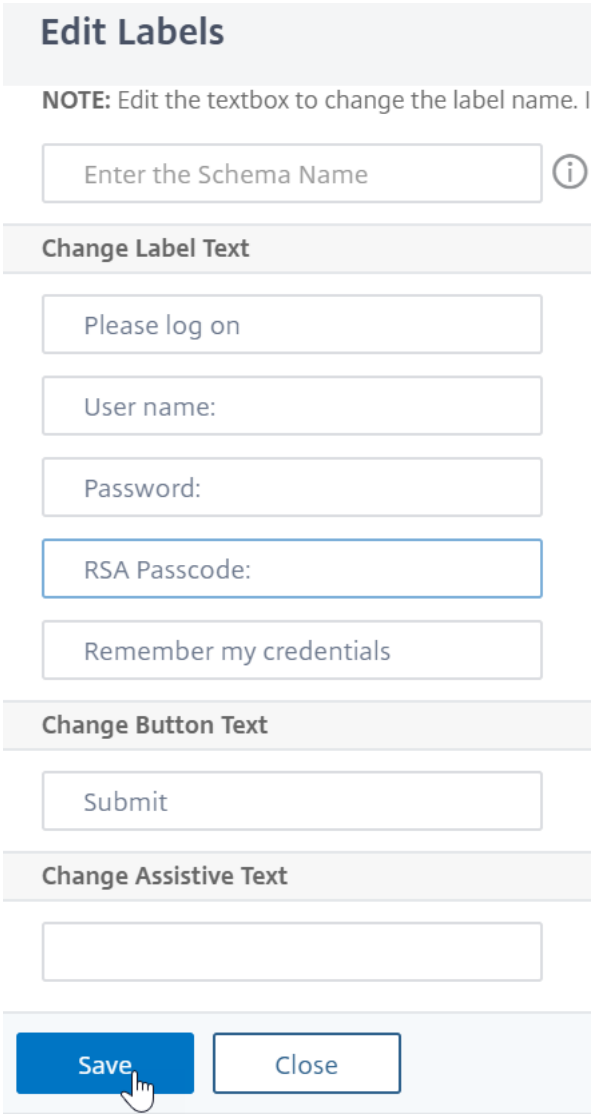
5. Klicken Sie auf den Ordner LoginSchema, um die darin enthaltenen Dateien zu sehen.



6. Markieren Sie eine der Dateien. Auf der rechten Seite sehen Sie eine Vorschau. Die Beschriftungen können geändert werden, indem Sie oben rechts auf die Schaltfläche **Bearbeiten** klicken.

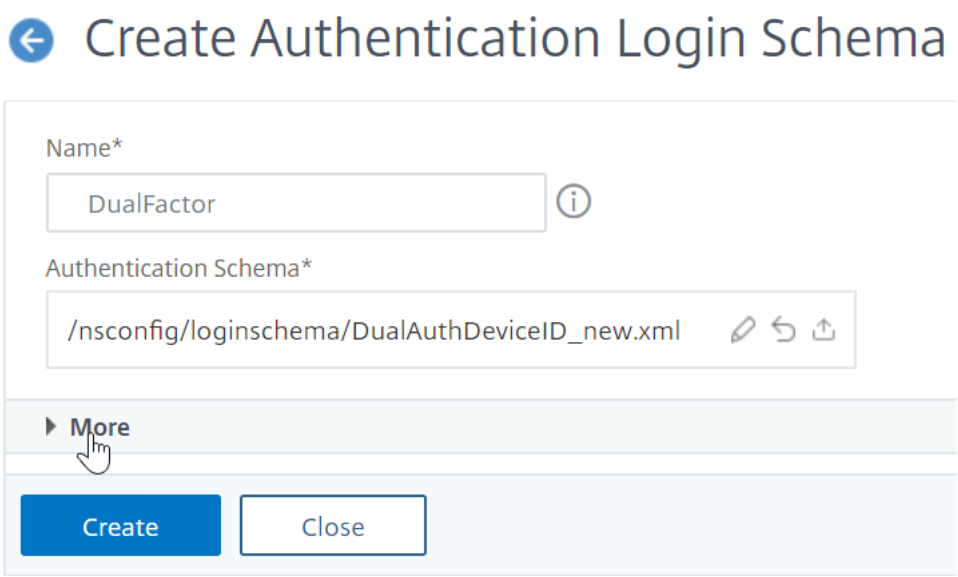


7. Wenn Sie die Änderungen speichern, wird unter /NSConfig/loginSchema eine neue Datei erstellt.



8. Klicken Sie rechts oben auf **Auswählen**.

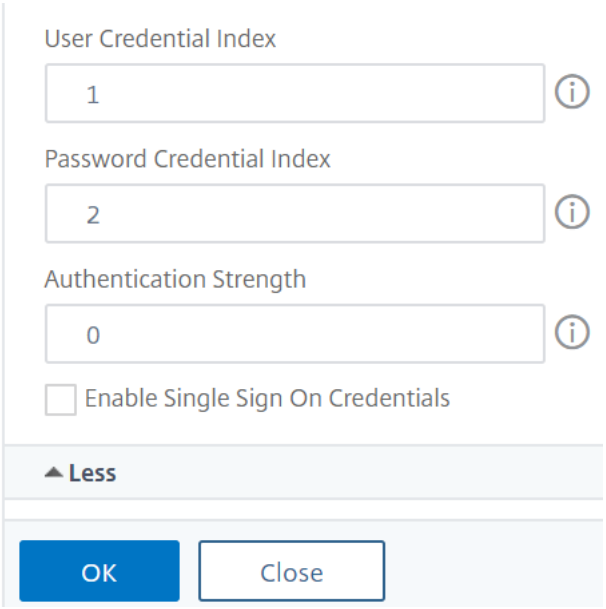
9. Geben Sie dem Anmeldeschema einen Namen und klicken Sie auf " **Mehr**".



10. Verwenden Sie den Benutzernamen und das Kennwort, die im Anmeldeschema für Single Sign-On (SSO) für einen Back-End-Dienst, z. B. StoreFront, eingegeben wurden.

    Sie können die im Anmeldeschema eingegebenen Anmeldeinformationen als Single Sign-On-Anmeldeinformationen verwenden, indem Sie eine der folgenden Methoden verwenden.

    - Klicken Sie unten auf der Seite **Authentifizierungsanmeldeschema erstellen** auf **Mehr** und wählen Sie **Single Sign On Credentials aktivieren**aus.
    - Klicken Sie unten auf der Seite **Authentifizierungsanmeldeschema erstellen** auf **Mehr**, und geben Sie eindeutige Werte für den Index der Benutzeranmeldeinformationen und den Index für Kennwort-Anmeldeinformationen ein. Diese Werte können zwischen 1 und 16 liegen. Später verweisen Sie auf diese Indexwerte in einer Verkehrsrichtlinien/einem Profil, indem Sie den Ausdruck AAA.USER.ATTRIBUTE (#) verwenden.



11. Klicken Sie auf **OK**, um das Login-Schemaprofil zu erstellen.

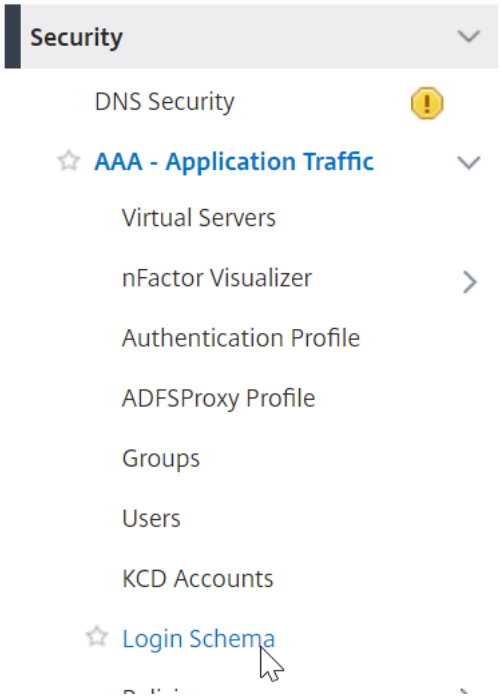
> **Hinweis:** Wenn Sie die Anmeldeschemadatei (.xml) später bearbeiten, müssen Sie das Anmeldeschemaprofil bearbeiten und die Anmeldeschemadatei (.xml-Datei) erneut auswählen, damit Änderungen übernommen werden.

Erstellen und Binden einer Login-Schemarichtlinie

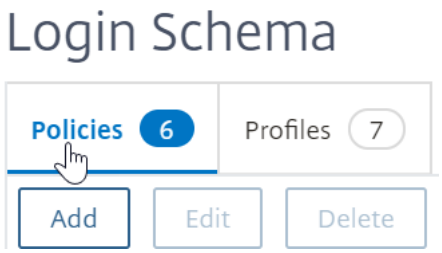
Um ein Anmeldeschemaprofil an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver zu binden, müssen Sie zunächst eine Richtlinie für das Anmeldeschema erstellen. Login-Schema-Richtlinien sind nicht erforderlich, wenn das Anmeldeschemaprofil an eine Authentifizierungsrichtlinienbezeichnung gebunden wird, wie später beschrieben.

So erstellen und binden Sie eine Login-Schema-Richtlinie:

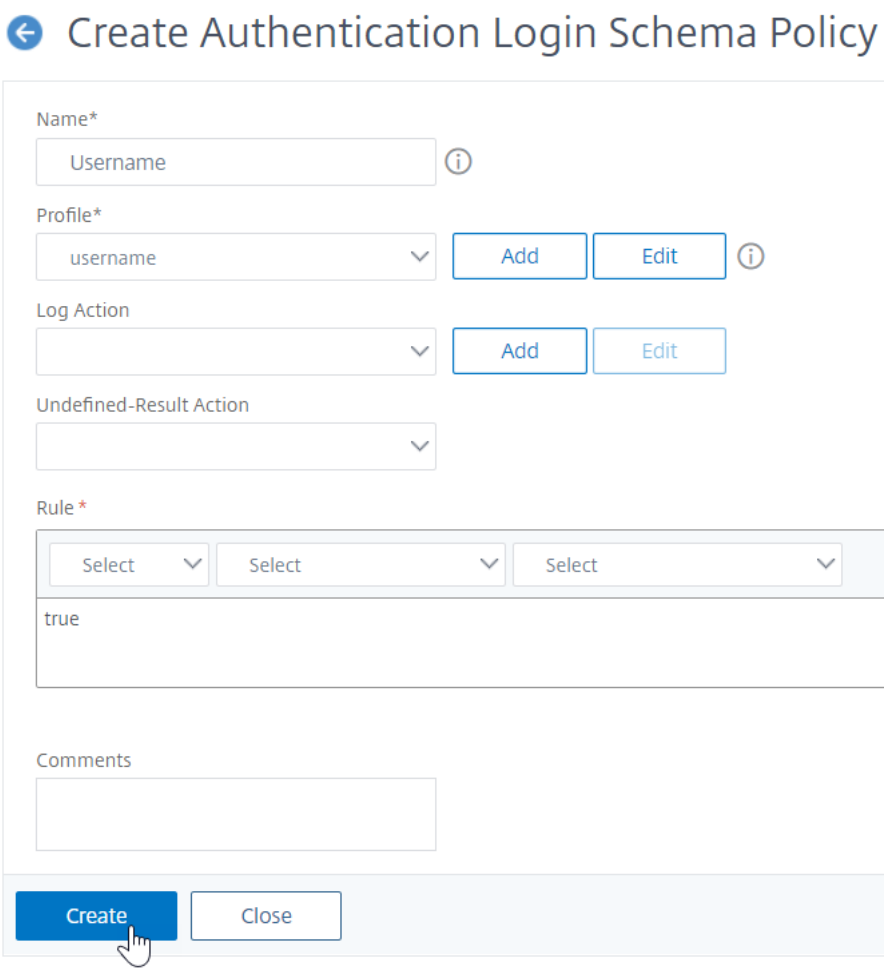
1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Anmeldeschema**.



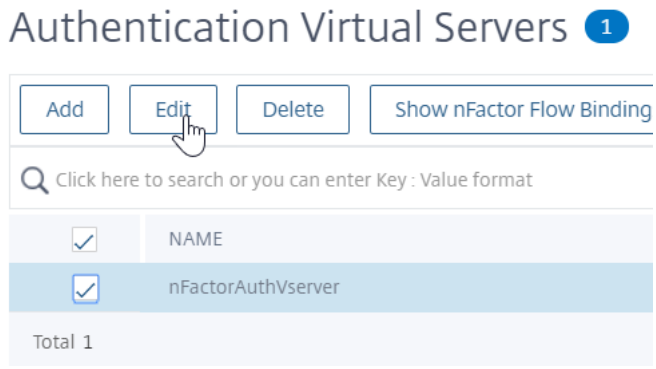
2. Klicken Sie auf der Registerkarte **Policies** auf **Add**.



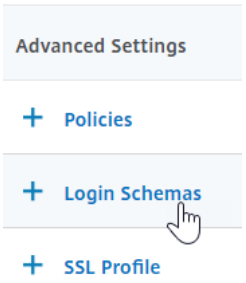
3. Verwenden Sie das Dropdown-Menü **Profil**, um das Anmeldeschema-Profil auszuwählen, das Sie bereits erstellt haben.
4. Geben Sie in das Feld **Regel** einen erweiterten Richtlinienausdruck ein und klicken Sie auf **Erstellen**.



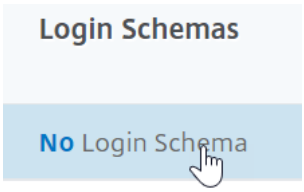
5. Navigieren Sie auf der linken Seite zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**, und bearbeiten Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.



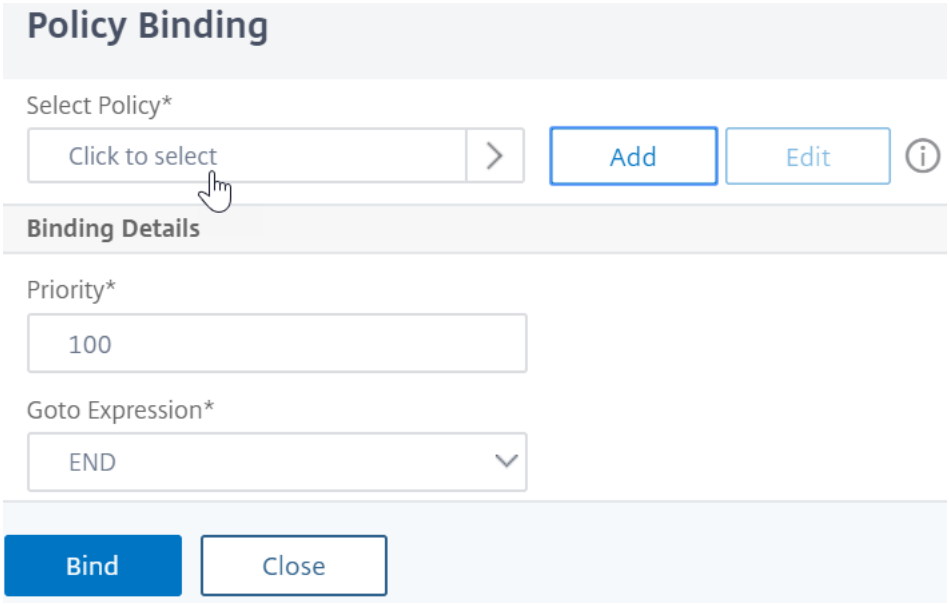
6. Klicken Sie in der Spalte Erweiterte Einstellungen auf **Anmeldeschemas**.



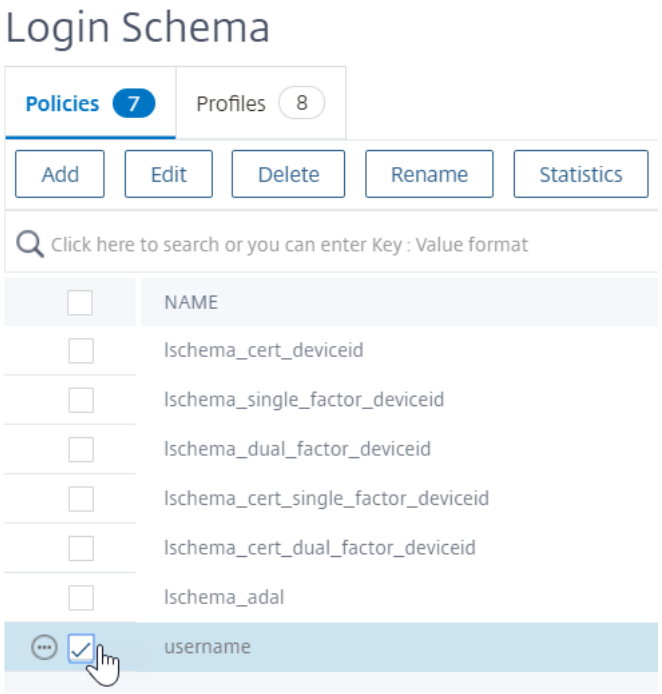
7. Klicken Sie im Abschnitt Anmeldeschemas auf den Text **Kein Anmeldeschema**.



8. Klicken Sie auf den Text, **klicken Sie zum Auswählen**.



9. Klicken Sie auf das Optionsfeld neben der Richtlinie für das Anmeldeschema und dann auf **Auswählen**. In dieser Liste werden nur Login-Schema-Richtlinien angezeigt. Login-Schemaprofile (ohne Richtlinie) werden nicht angezeigt.



10. Klicken Sie auf **Bind**.

Erweiterte Authentifizierungsrichtlinien

Authentifizierungsrichtlinien sind eine Kombination aus Richtlinienausdruck und Richtlinienmaßnahmen. Wenn der Ausdruck wahr ist, dann bewerten Sie die Authentifizierungsaktion.

Erstellen erweiterter Authentifizierungsrichtlinien

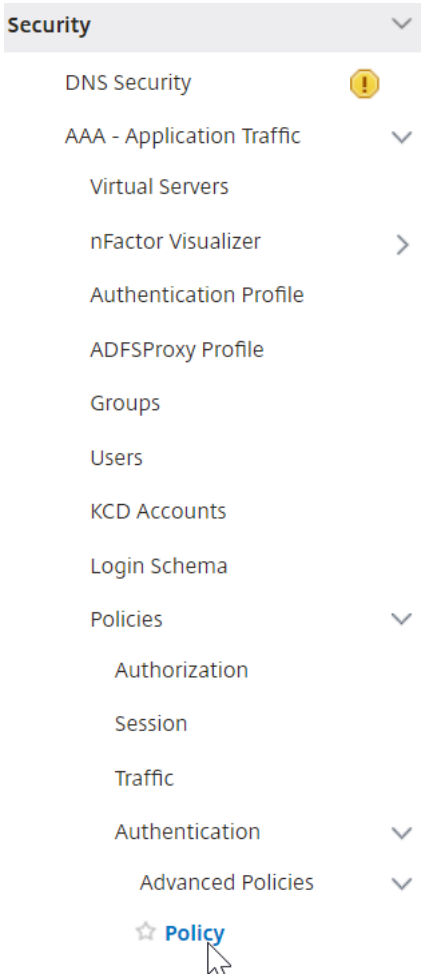
Authentifizierungsrichtlinien sind eine Kombination aus Richtlinienausdruck und Richtlinienaktion. Wenn der Ausdruck wahr ist, dann bewerten Sie die Authentifizierungsaktion.

Sie benötigen Authentifizierungsaktionen/Server (z. B. LDAP, RADIUS, CERT, SAML usw.)
Beim Erstellen einer erweiterten Authentifizierungsrichtlinie gibt es ein Pluszeichen (Hinzufügen), mit dem Sie Authentifizierungsaktionen/Server erstellen können.

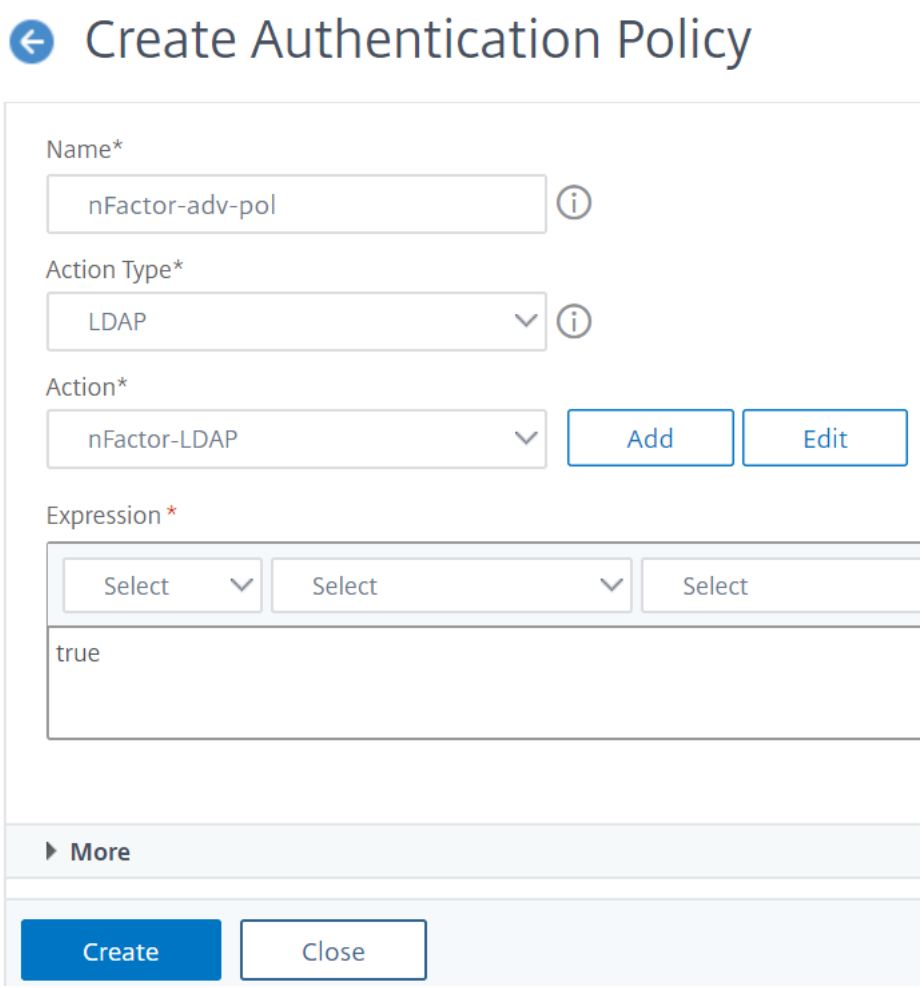
Oder Sie können Authentifizierungsaktionen (Server) erstellen, bevor Sie die erweiterte Authentifizierungsrichtlinie erstellen. Die Authentifizierungsserver befinden sich unter **Authentifizierung > Dashboard**. Klicken Sie auf der rechten Seite auf Hinzufügen, und wählen Sie einen Servertyp aus. Die Anweisungen zum Erstellen dieser Authentifizierungsserver sind hier nicht detailliert. Siehe die Verfahren Authentifizierung — NetScaler 12/NetScaler 12.1.

So erstellen Sie eine erweiterte Authentifizierungsrichtlinie:

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**



2. Führen Sie im Detailbereich einen der folgenden Schritte aus:
   - Um eine Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus und klicken dann auf **Bearbeiten**.
3. Geben **Sie im Dialogfeld Authentifizierungsrichtlinie erstellen** oder **Authentifizierungsrichtlinie konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus.



- **Name** — Der Name der Richtlinie. Für eine zuvor konfigurierte Richtlinie kann nicht geändert werden.
- **Aktionstyp** - Der Richtlinientyp: Cert, Negotiate, LDAP, RADIUS, SAML, SAMLIDP, TACACS oder WEBAUTH.
- **Aktion** — Die Authentifizierungsaktion (Profil), die mit der Richtlinie verknüpft werden soll. Sie können eine bestehende Authentifizierungsaktion auswählen oder auf das Plus klicken und eine Aktion des richtigen Typs erstellen.
- **Protokollaktion** — Die Überwachungsaktion, die mit der Richtlinie verknüpft werden soll. Sie können eine bestehende Audit-Aktion auswählen oder auf das Plus klicken und eine Aktion erstellen.
  Sie haben keine Aktionen konfiguriert, oder um eine Aktion zu erstellen, klicken Sie auf **Hinzufügen** und führen Sie die Schritte aus.
- **Ausdruck** - Die Regel, die Verbindungen auswählt, auf die Sie die angegebene Aktion anwenden möchten. Die Regel kann einfach (“wahr” wählt den gesamten Verkehr aus) oder komplex sein. Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unter dem Ausdrucksfenster auswählen und dann Ihren Ausdruck di-

rekt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen, und die darin bezeichnenden Dropdownlisten verwenden, um Ihre Ausdruck.)

- **Kommentar** - Sie können einen Kommentar eingeben, der die Art des Datenverkehrs beschreibt, für den diese Authentifizierungsrichtlinie gilt. Optional.

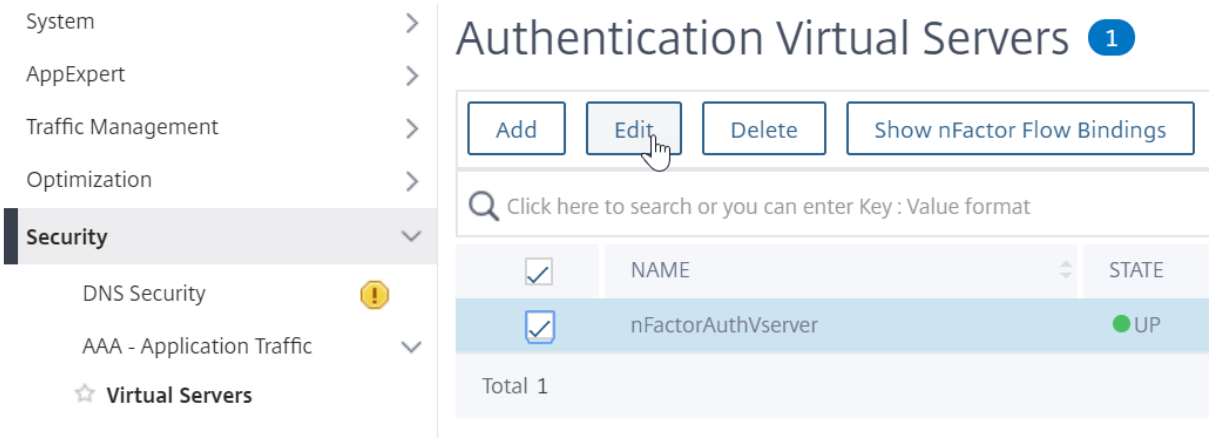
4. Klicken Sie auf **Create** und dann auf **Close**. Wenn Sie eine Richtlinie erstellt haben, wird diese Richtlinie auf der Seite Authentifizierungsrichtlinien und Server angezeigt.

Erstellen Sie je nach Bedarf zusätzliche erweiterte Authentifizierungsrichtlinien basierend auf Ihrem nFactor-Design.

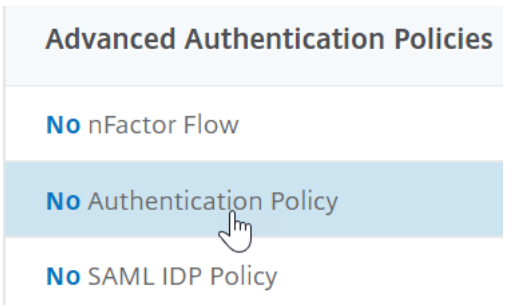
Binden Sie die erweiterte Authentifizierungsrichtlinie des ersten Faktors an Authentifizierung, Autorisierung und Überwachung

Sie können erweiterte Authentifizierungsrichtlinien direkt für den ersten virtuellen Faktor-Authentifizierungs-, Autorisierungs- und Überwachungsserver binden. Für die nächsten Faktoren müssen Sie die erweiterten Authentifizierungsrichtlinien an die Bezeichnungen der Authentifizierungsrichtlinie binden.

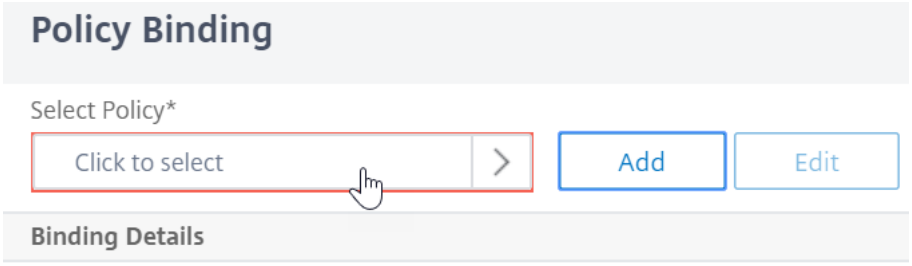
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**. Bearbeiten Sie einen vorhandenen virtuellen Server.



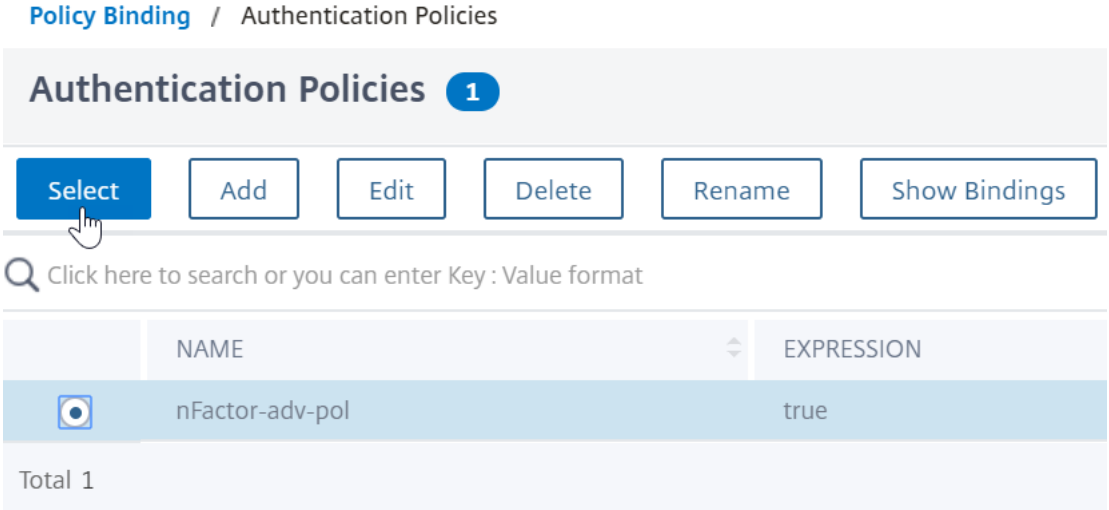
1. Klicken Sie links im Abschnitt Erweiterte Authentifizierungsrichtlinien auf **Keine Authentifizierungsrichtlinie**.



2. Klicken Sie unter **Richtlinie auswählen**auf den Text und **klicken Sie zum Auswählen**.

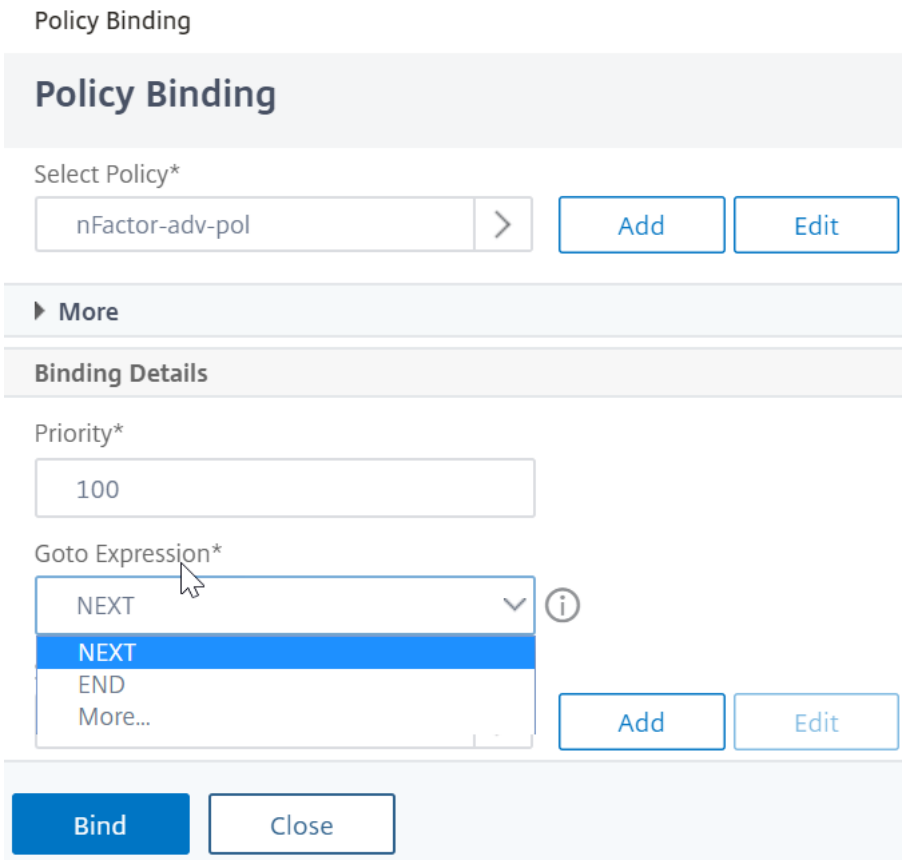


3. Klicken Sie auf das Optionsfeld neben der **erweiterten Authentifizierungsrichtlinie**und dann auf **Auswählen**.

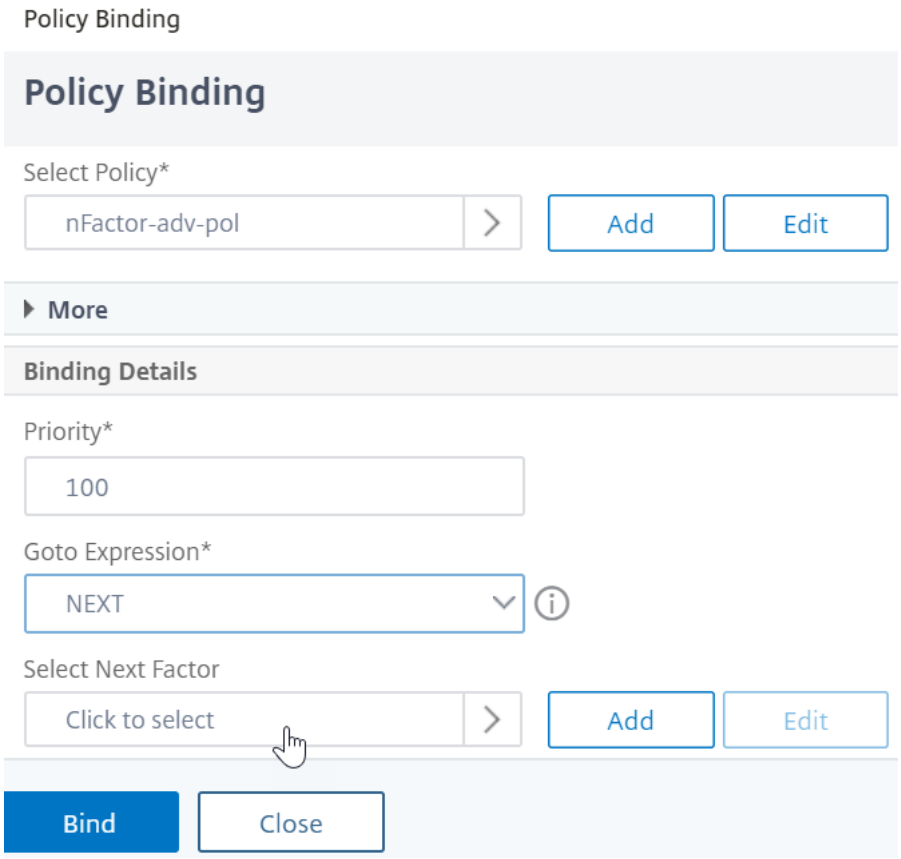


4. Im Abschnitt “Bindungsdetails” bestimmt der **Gehe zu Ausdruck**, was als Nächstes passiert, wenn diese erweiterte Authentifizierungsrichtlinie fehlschlägt.

   - Wenn **Gehe zu Ausdruck aufNEXT**festgelegt ist, wird die nächste erweiterte Authentifizierungsrichtlinie ausgewertet, die an diesen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden ist.
   - Wenn **Gehe zu Ausdruck aufEND**gesetzt ist oder wenn keine erweiterten Authentifizierungsrichtlinien mehr an diesen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden sind, wird die Authentifizierung abgeschlossen und als fehlgeschlagen markiert.



5. Unter **Nächsten Faktor auswählen**können Sie auswählen, dass auf eine Authentifizierungsrichtlinienbeschriftung verweisen kann. Der nächste Faktor wird nur bewertet, wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist. Klicken Sie abschließend auf **Bind**.



Verwenden Sie extrahierte LDAP-Gruppen, um den nächsten Authentifizierungsfaktor auszuwählen

Sie können extrahierte LDAP-Gruppen verwenden, um den nächsten Authentifizierungsfaktor ohne tatsächliche Authentifizierung mit LDAP auszuwählen.

1. Deaktivieren Sie beim Erstellen oder Bearbeiten eines LDAP-Servers oder einer LDAP-Aktion das Kontrollkästchen **Authentifizierung** .
2. Wählen Sie **unter Andere Einstellungen**die entsprechenden Werte in **Gruppenattribut** und **Unterattributname**aus.

Authentifizieren Sie das Policy Label

Wenn Sie eine erweiterte Authentifizierungsrichtlinie an den virtuellen Server für Authentifizierung, Autorisierung und Überwachung binden und einen nächsten Faktor ausgewählt haben, wird der nächste Faktor nur ausgewertet, wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist. Der nächste Faktor, der ausgewertet wird, ist ein Label für die Authentifizierungsrichtlinie.

Das Label der Authentifizierungsrichtlinie gibt eine Sammlung von Authentifizierungsrichtlinien für einen bestimmten Faktor an. Jedes Policy Label entspricht einem einzelnen Faktor. Es gibt auch

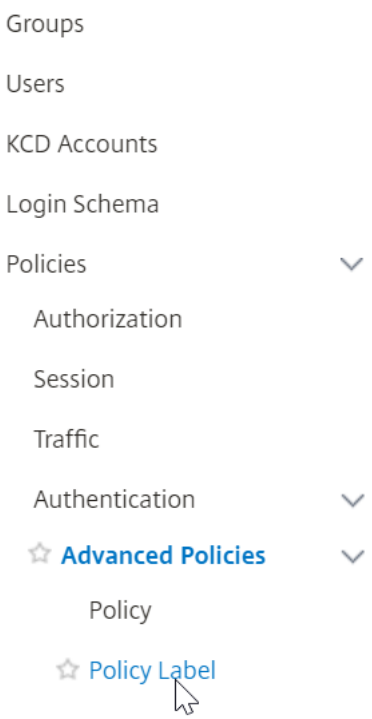
das Anmeldeformular an, das dem Benutzer vorgelegt werden muss. Die Bezeichnung der Authentifizierungsrichtlinie muss als nächster Faktor einer Authentifizierungsrichtlinie oder einer anderen Authentifizierungsrichtlinienbezeichnung gebunden sein.

Hinweis: Jeder Faktor benötigt kein Login-Schema. Das Anmeldeschemaprofil ist nur erforderlich, wenn Sie ein Anmeldeschema an ein Authentifizierungsrichtlinienlabel binden.

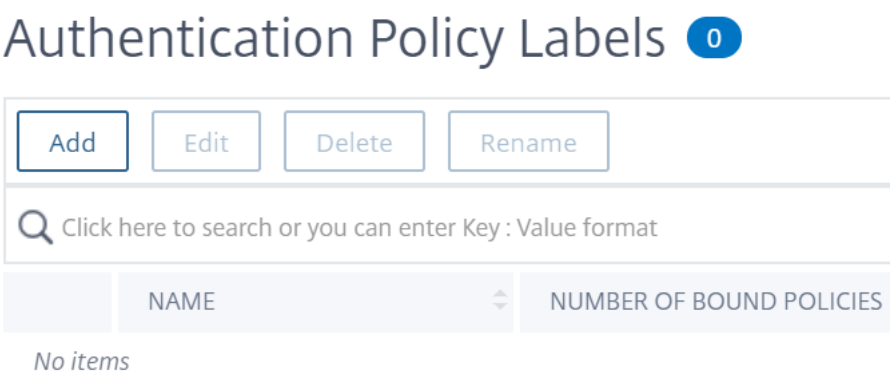
Erstellen einer Bezeichnung für die Authentifizierungsrichtlinie

Ein Policy Label gibt die Authentifizierungsrichtlinien für einen bestimmten Faktor an. Jedes Policy Label entspricht einem einzelnen Faktor. Das Policy Label gibt das Anmeldeformular an, das dem Benutzer vorgelegt werden muss. Das Policy Label muss als nächster Faktor einer Authentifizierungsrichtlinie oder einer anderen Authentifizierungsrichtlinienbezeichnung gebunden sein. In der Regel enthält ein Policy Label Authentifizierungsrichtlinien für einen bestimmten Authentifizierungsmechanismus. Sie können jedoch auch ein Policy Label haben, das Authentifizierungsrichtlinien für verschiedene Authentifizierungsmechanismen enthält.

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinienbezeichnung**.



2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

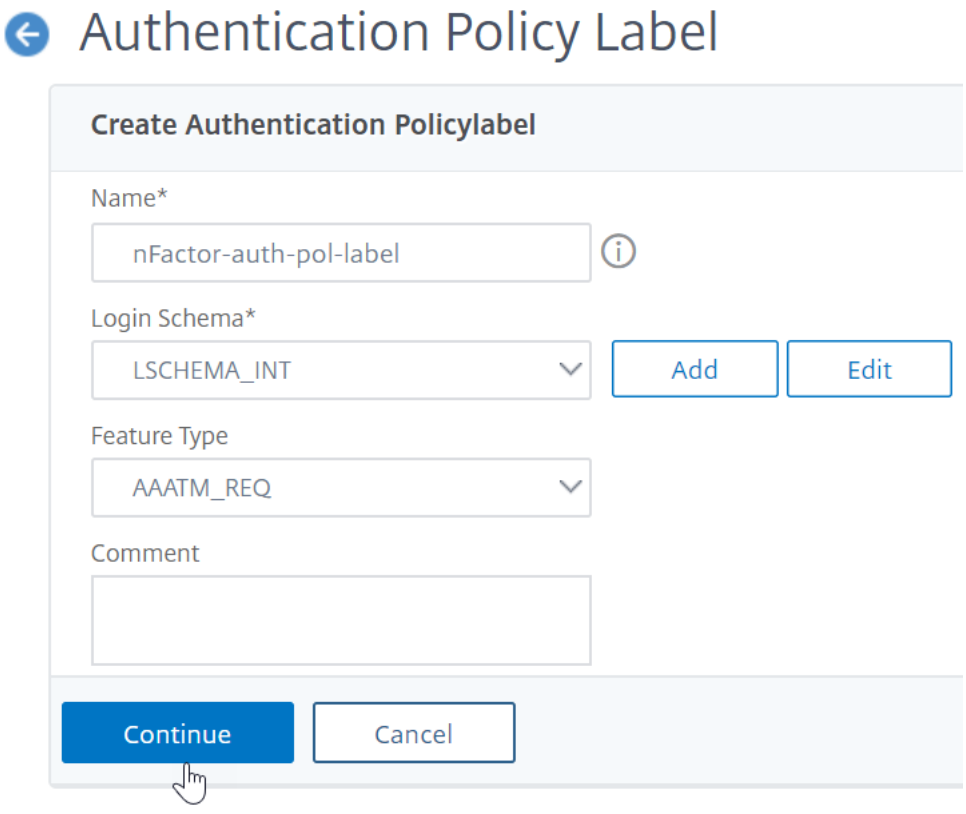


3. Füllen Sie die folgenden Felder aus, um ein Authentifizierungsrichtlinienlabel zu erstellen:

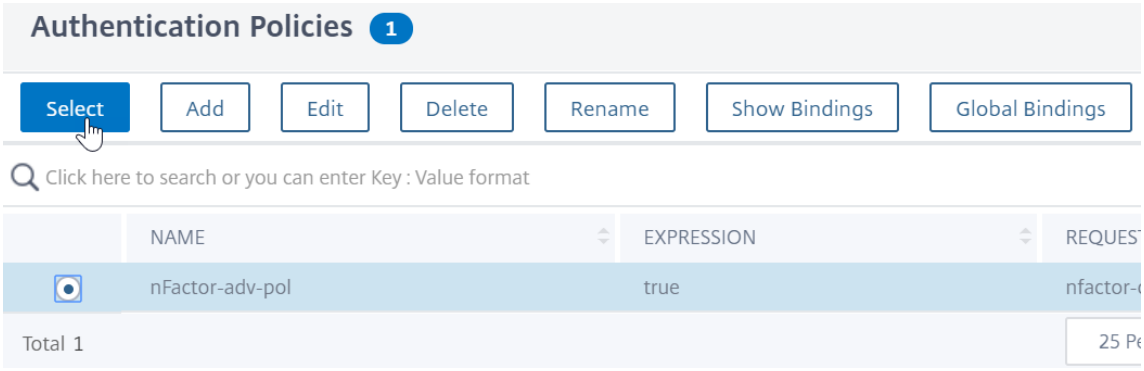
   a) Geben Sie den **Namen** für das neue Label für die Authentifizierungsrichtlinie ein.

   b) Wählen Sie das **Login-Schema** aus, das der Bezeichnung der Authentifizierungsrichtlinie WENN Sie dem Benutzer nichts anzeigen möchten, können Sie ein Anmeldeschemaprofil auswählen, das auf kein Schema festgelegt ist (LSCHEMA_INT).

   c) Klicken Sie auf " **Weiter**".



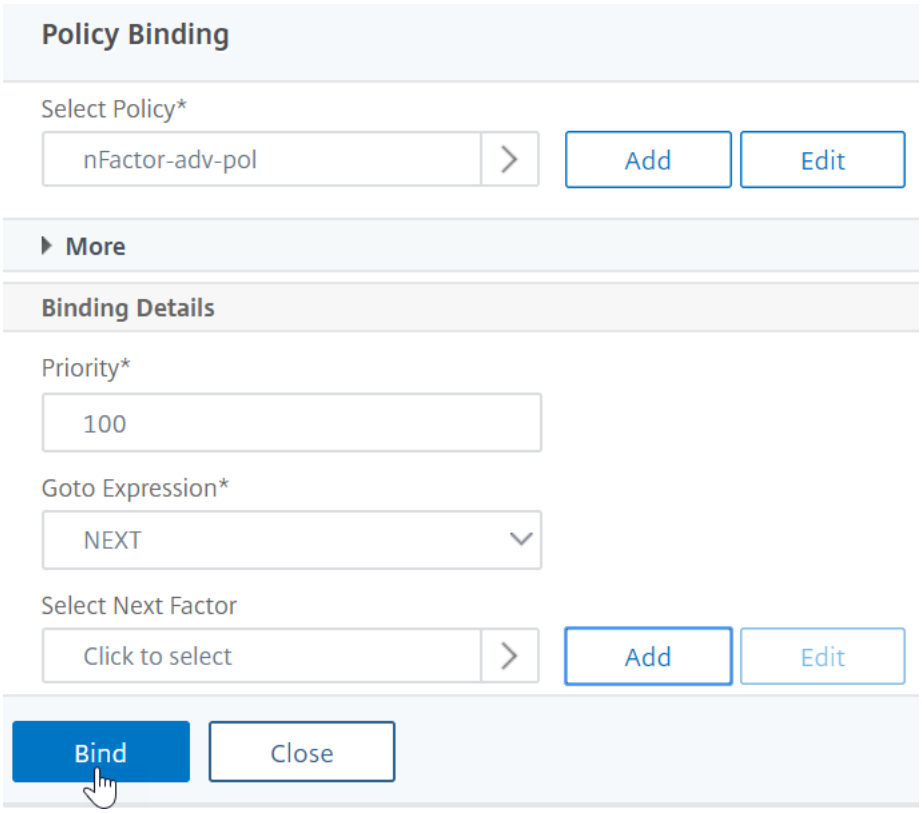
4. Klicken Sie im Abschnitt **Richtlinienbindung** auf die Stelle, an der **zum Auswählen klicken angezeigt**wird.
5. Wählen Sie die Authentifizierungsrichtlinie aus, die diesen Faktor auswertet.



6. Füllen Sie die folgenden Felder aus:

   a) Geben Sie die **Priorität** der Policy-Bindung ein.

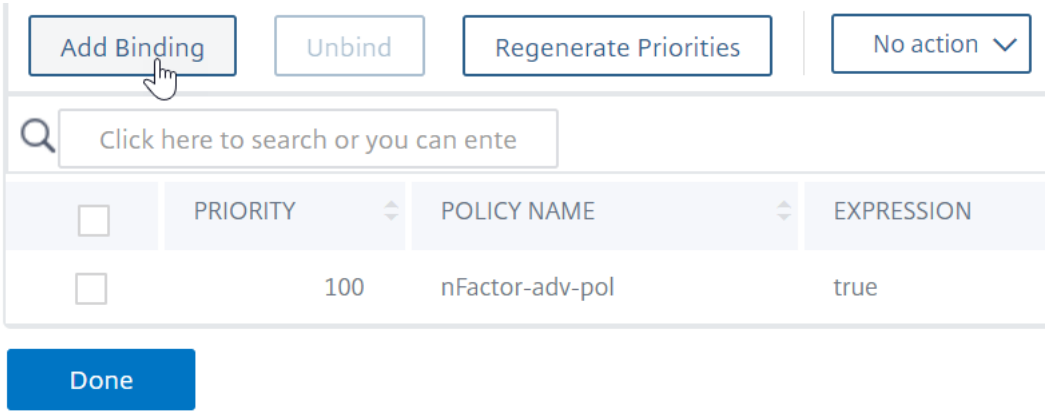
   b) Wählen Sie in **Gehe zu Ausdruck** die Option **NEXT** aus, wenn Sie erweiterte Authentifizierungsrichtlinien an diesen Faktor binden möchten, oder wählen Sie **END**.



7. Wenn Sie unter **Nächsten Faktor auswählen**einen weiteren Faktor hinzufügen möchten, klicken Sie auf, um das nächste Authentifizierungsrichtlinienlabel auszuwählen und zu binden (nächster Faktor).
   Wenn Sie den nächsten Faktor nicht auswählen und diese erweiterte Authentifizierungsrichtlinie erfolgreich ist, ist die Authentifizierung erfolgreich und abgeschlossen.

8. Klicken Sie auf **Bind**.

9. Sie können auf **Bindung hinzufügen** klicken, um dieser Richtlinienbezeichnung (Faktor) erweiterte Authentifizierungsrichtlinien hinzuzufügen. Klicken Sie nach **Abschluss auf Fertig** .



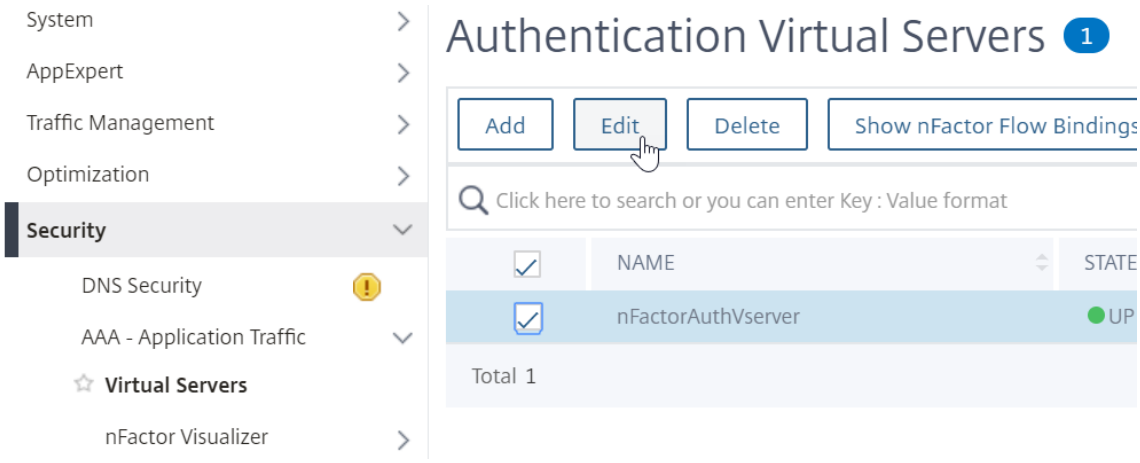
Beschriftung der Authentifizierungsrichtlinie binden

Nachdem Sie das Policy Label erstellt haben, binden Sie es an eine vorhandene erweiterte Authentifizierungsrichtlinienbindung, um die Faktoren miteinander zu verketten.

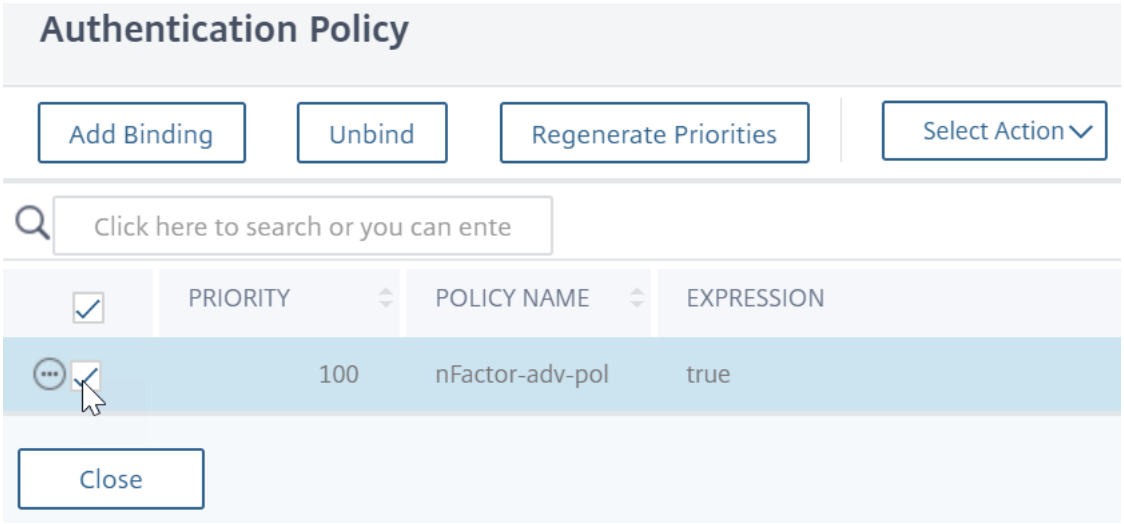
Sie können den nächsten Faktor auswählen, wenn Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver bearbeiten, der über eine erweiterte Authentifizierungsrichtlinie gebunden ist, oder wenn Sie eine andere Policy Label bearbeiten, um den nächsten Faktor einzubeziehen.

So bearbeiten Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver, an den bereits eine erweiterte Authentifizierungsrichtlinie gebunden ist

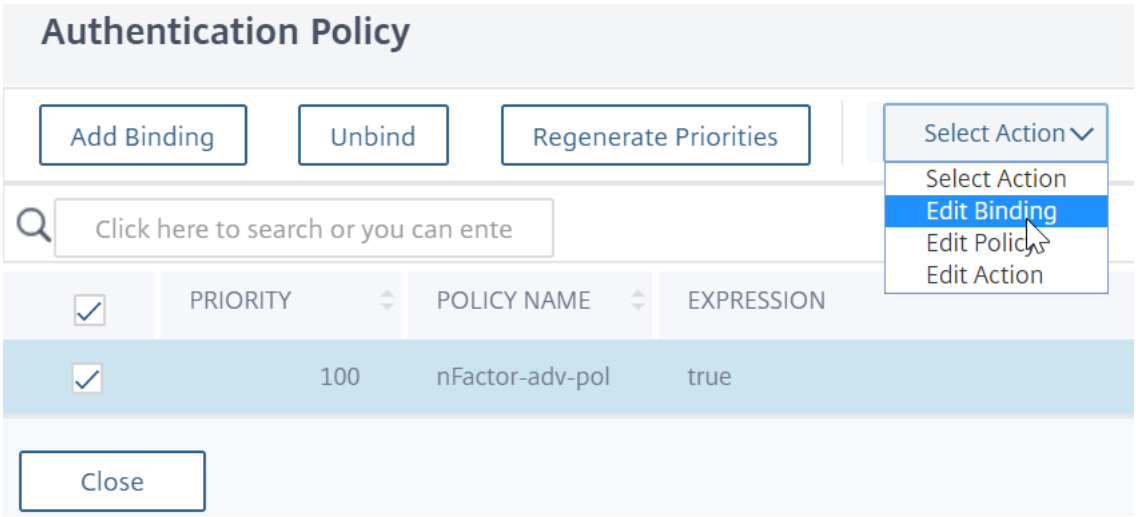
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server.** Wählen Sie den virtuellen Server aus und klicken Sie auf **Bearbeiten**.



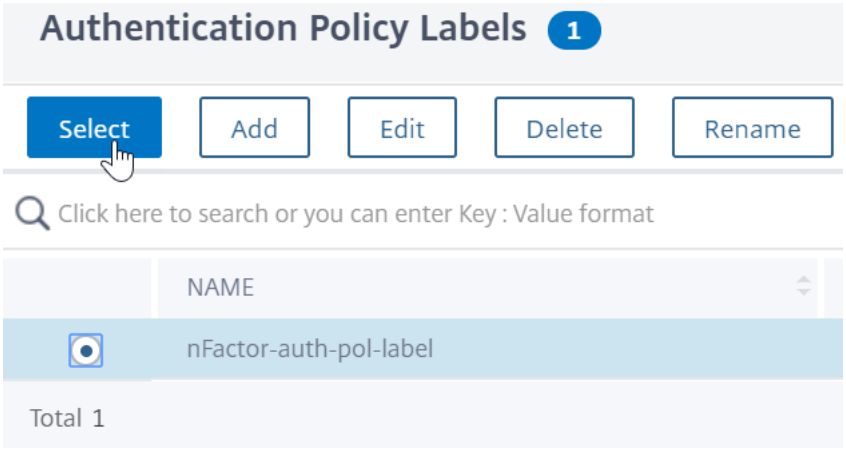
2. Klicken Sie links im Abschnitt **Erweiterte Authentifizierungsrichtlinien** auf eine bestehende Authentifizierungsrichtlinienbindung.



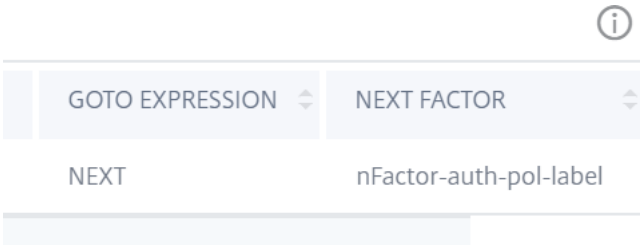
3. Klicken Sie unter **Aktion auswählen**auf **Bindung bearbeiten**.



4. Klicken Sie unter **Nächsten Faktor auswählen**auf und wählen Sie ein vorhandenes Authentifizierungsrichtlinienlabel aus (nächster Faktor).

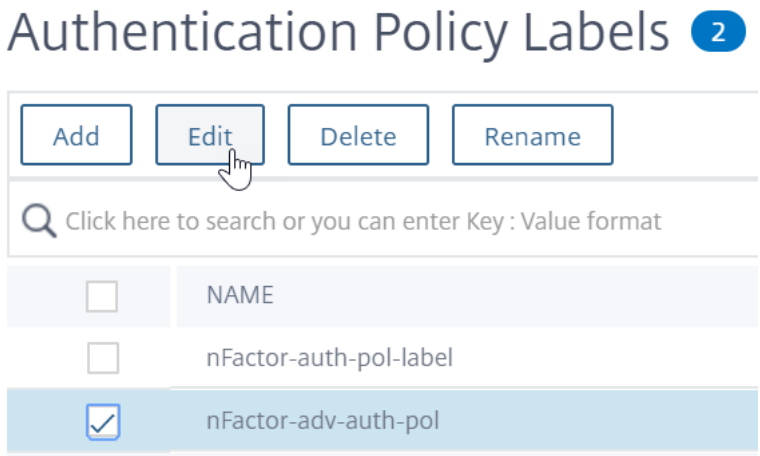


5. Klicken Sie auf **Bind**. Den nächsten Faktor sehen Sie ganz rechts.

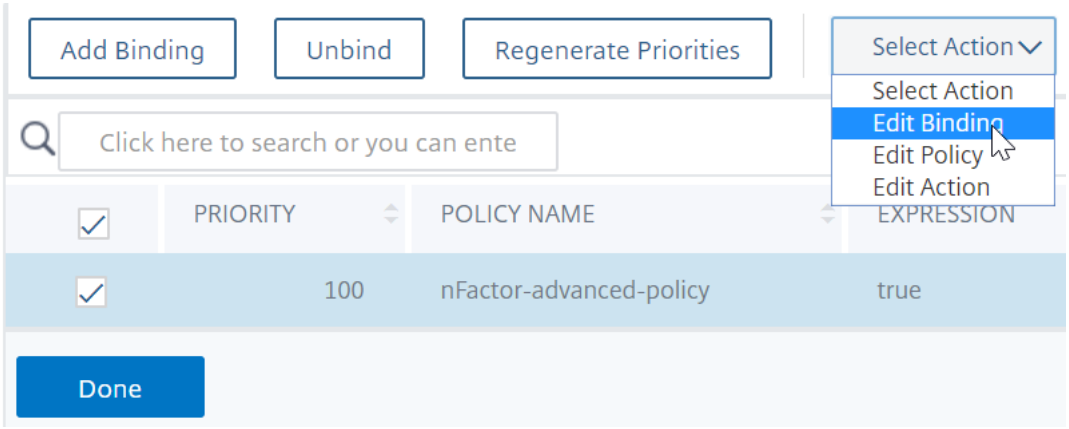


So fügen Sie eine Policy Label als nächsten Faktor zu einem anderen Policy Label hinzu

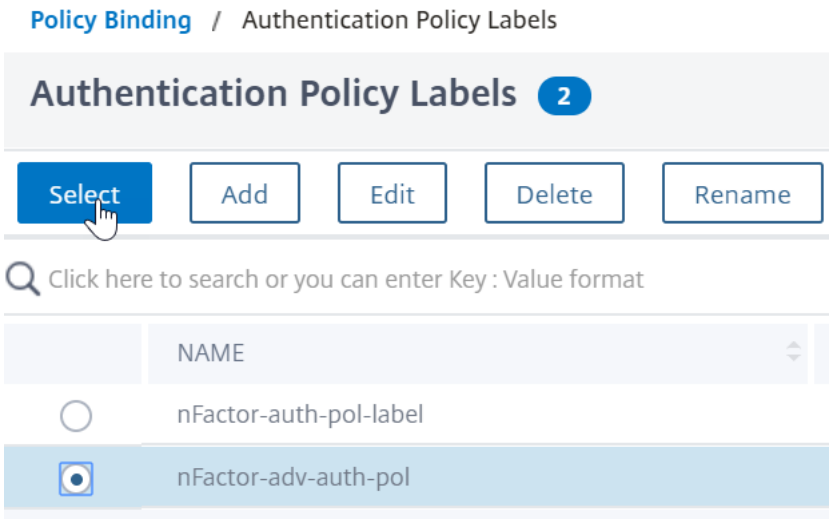
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinienbezeichnung**. Wählen Sie ein anderes Policy Label aus und klicken Sie auf **Bearbeiten.**



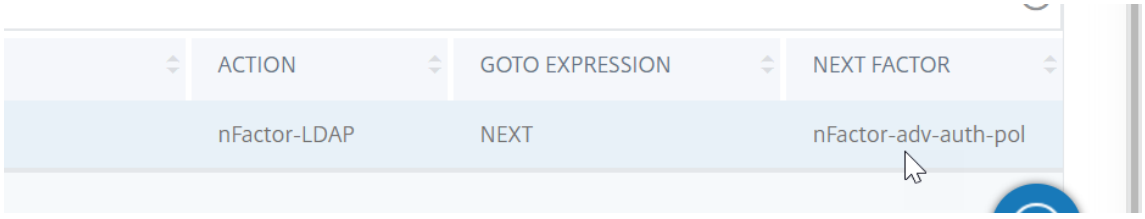
2. Klicken Sie unter **Aktion auswählen**auf **Bindung bearbeiten**.



3. Klicken **Sie unter Bindungsdetails > Nächsten Faktor**auswählen auf, um den nächsten Faktor auszuwählen.
4. Wählen Sie das Policy Label für den nächsten Faktor und klicken Sie auf die Schaltfläche **Auswählen** .



5. Klicken Sie auf **Binden.** Den nächsten Faktor sehen Sie auf der rechten Seite.

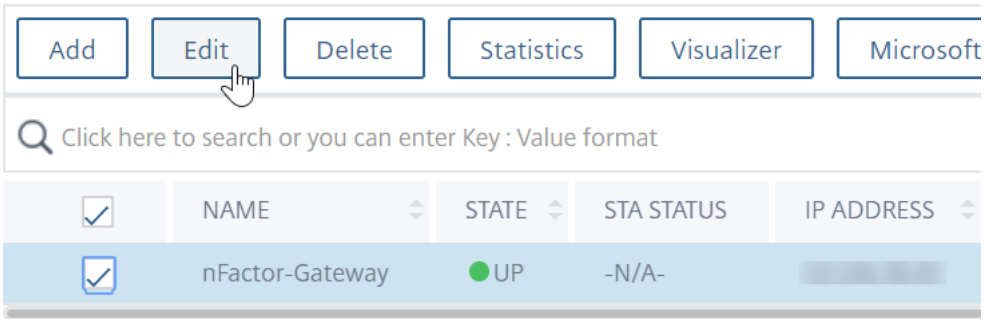


nFactor für NetScaler Gateway

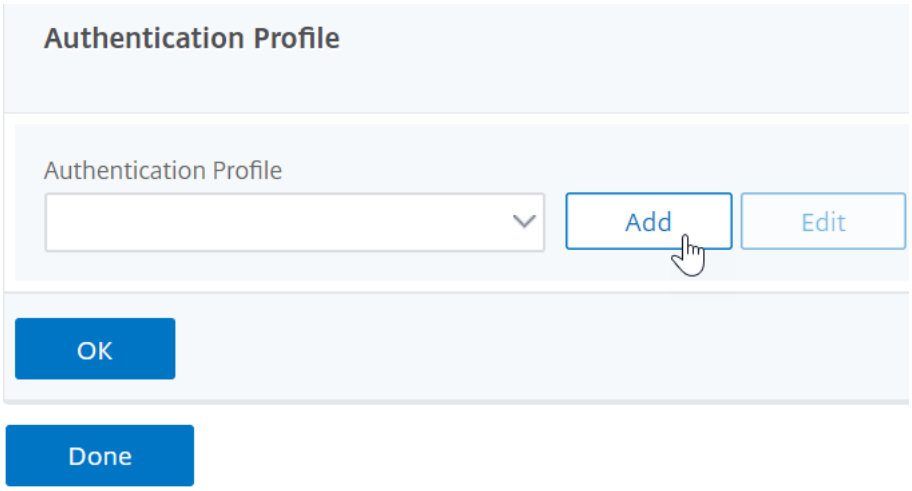
Um nFactor auf dem NetScaler Gateway zu aktivieren, muss ein Authentifizierungsprofil mit einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver verknüpft sein.

Erstellen eines Authentifizierungsprofils, um einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver mit dem virtuellen NetScaler Gateway

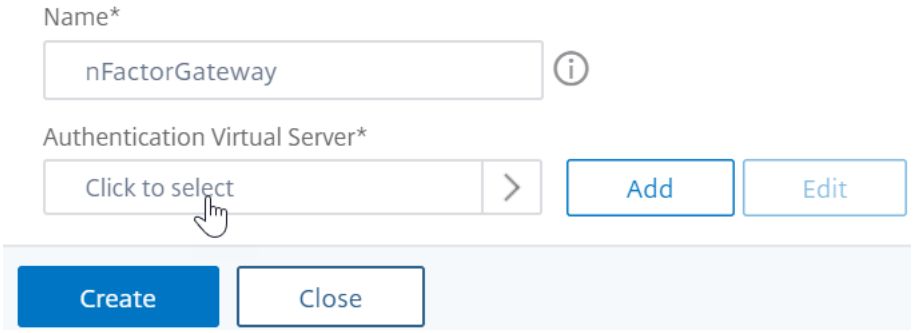
1. Navigieren Sie zu **NetScaler Gateway > Virtuelle Server** und wählen Sie einen vorhandenen virtuellen Gateway-Server aus, der bearbeitet werden soll.



2. Klicken Sie in **Erweiterte Einstellungen**auf **Authentifizierungsprofil**.
3. Klicken Sie unter **Authentifizierungsprofil** auf **Hinzufügen**.

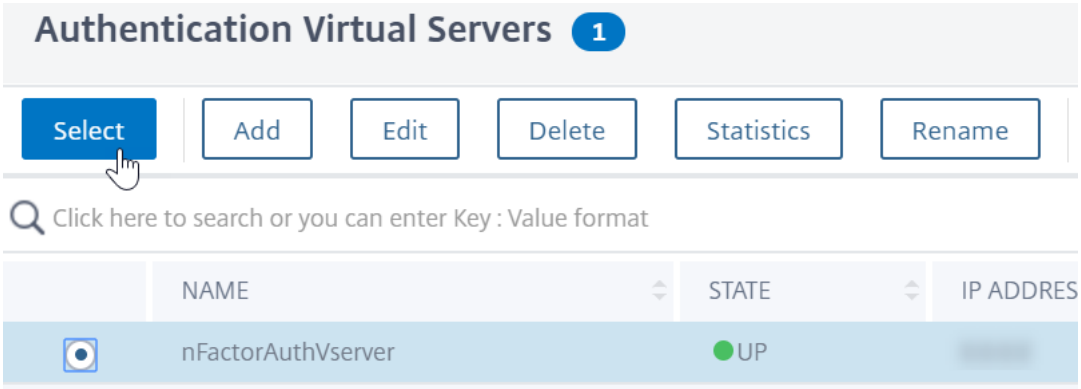


4. Geben Sie den Namen für das Authentifizierungsprofil ein und klicken Sie auf die Stelle, an der es heißt **Klicken zur Auswahl**

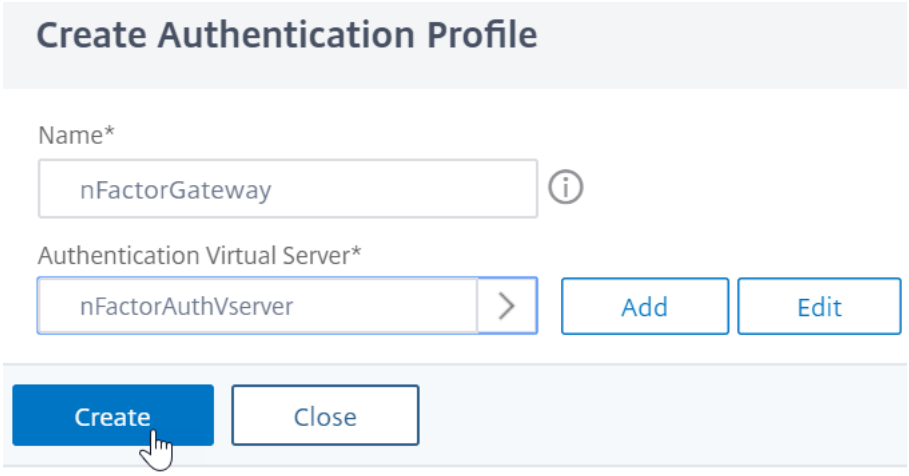


5. Wählen Sie unter **Virtueller Authentifizierungsserver** einen vorhandenen Server aus, auf dem das Anmeldeschema, eine erweiterte Authentifizierungsrichtlinie und Bezeichnun-

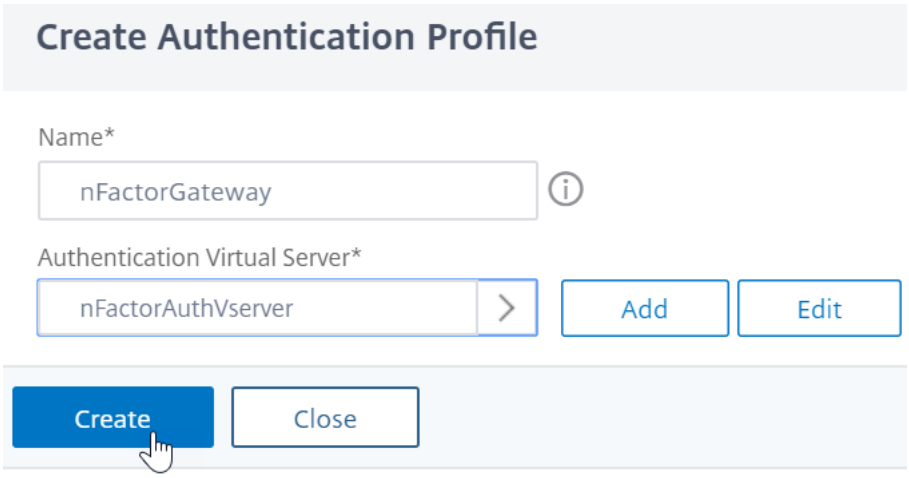
gen für Authentifizierungsrichtlinien konfiguriert sind. Sie können auch einen virtuellen Authentifizierungsserver erstellen. Der virtuelle Authentifizierungs-, Autorisierungs- und Überwachungsserver benötigt keine IP-Adresse. Klicken Sie auf **Select**.



6. Klicken Sie auf **Erstellen**.



7. Klicken Sie auf **OK** um den Abschnitt Authentifizierungsprofil zu schließen.



Hinweis: Wenn Sie einen der Faktoren als Client-Zertifikate konfiguriert haben, müssen Sie die SSL-

Parameter und das CA-Zertifikat konfigurieren.

Nachdem Sie das Authentifizierungsprofil mit einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver verknüpft haben und wenn Sie zu Ihrem NetScaler Gateway navigieren, können Sie die nFactor-Authentifizierungsbildschirme anzeigen.

Konfigurieren von SSL-Parametern und CA-Zertifikat

Wenn einer der Authentifizierungsfaktoren ein Zertifikat ist, müssen Sie eine SSL-Konfiguration auf dem virtuellen NetScaler Gateway-Server durchführen.

1. Navigieren Sie zu **Traffic Management > SSL > Certificates > CA Certificates**, und installieren Sie das Stammzertifikat für den Aussteller der Clientzertifikate. Zertifikate von Certificate Authority benötigen keine Schlüsseldateien.

   Wenn Standard-SSL-Profile aktiviert sind, haben Sie bereits ein SSL-Profil erstellt, für das die Clientauthentifizierung aktiviert ist.

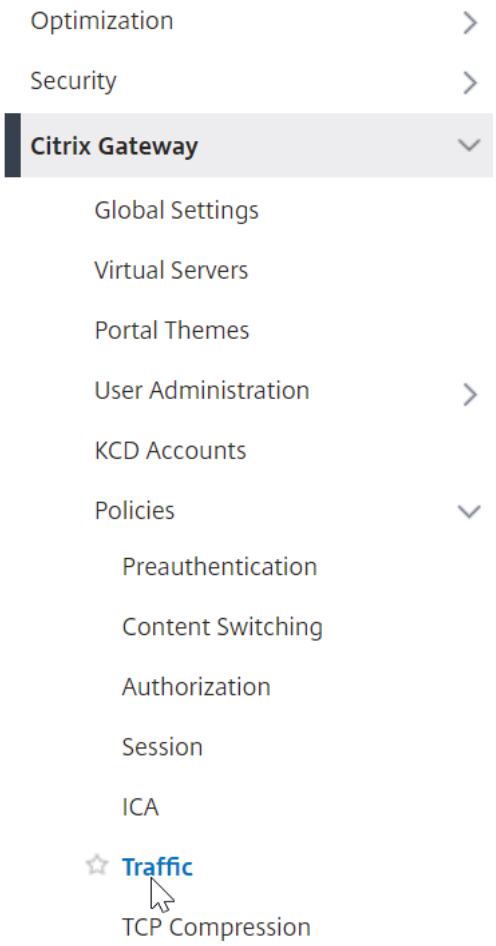
2. Navigieren Sie zu **NetScaler Gateway > Virtuelle Server**, und bearbeiten Sie einen vorhandenen virtuellen NetScaler Gateway-Server, der für nFactor aktiviert ist.
   - Wenn Standard-SSL-Profile aktiviert sind, klicken Sie auf das Bearbeitungssymbol.
   - Wählen Sie in der Liste SSL-Profil das SSL-Profil aus, für das die Clientauthentifizierung aktiviert und auf OPTIONAL festgelegt ist.
   - Wenn Standard-SSL-Profile nicht aktiviert sind, klicken Sie auf das Bearbeitungssymbol.
   - Aktivieren Sie das Kontrollkästchen Clientauthentifizierung.
   - Stellen Sie sicher, dass das Clientzertifikat auf Optional festgelegt ist
3. Klicken Sie auf OK.
4. Klicken Sie im Abschnitt Zertifikate auf **Kein CA-Zertifikat.**
5. Klicken Sie unter Select CA Certificate auf, um das Stammzertifikat für den Aussteller der Clientzertifikate auszuwählen und auszuwählen.
6. Klicken Sie auf Bind.

Hinweis: Möglicherweise müssen Sie auch alle Zwischen-CA-Zertifikate binden, die die Clientzertifikate ausgestellt haben.

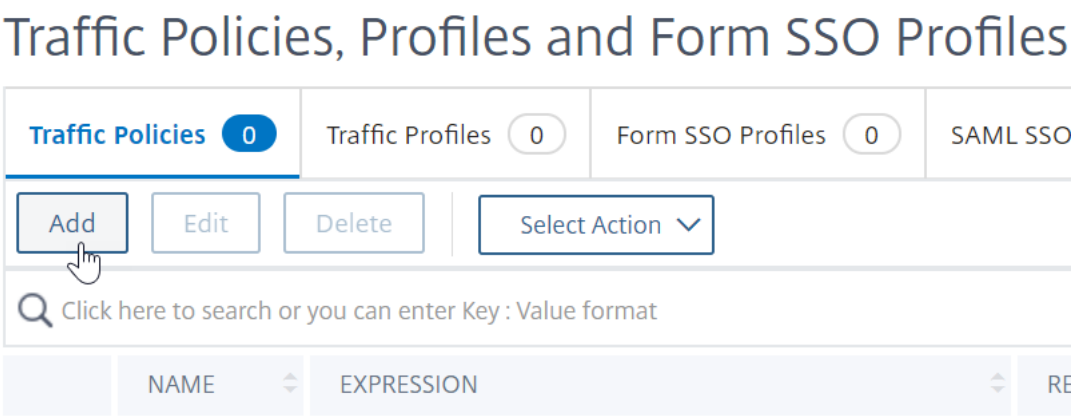
Konfigurieren der NetScaler Gateway-Verkehrsrichtlinie für nFactor Single Sign-On bei StoreFront

Für die einmalige Anmeldung bei StoreFront verwendet nFactor standardmäßig das zuletzt eingegebene Kennwort. Wenn LDAP nicht das zuletzt eingegebene Kennwort ist, müssen Sie eine Verkehrsrichtlinie/ein Profil erstellen, um das standardmäßige nFactor-Verhalten zu überschreiben.

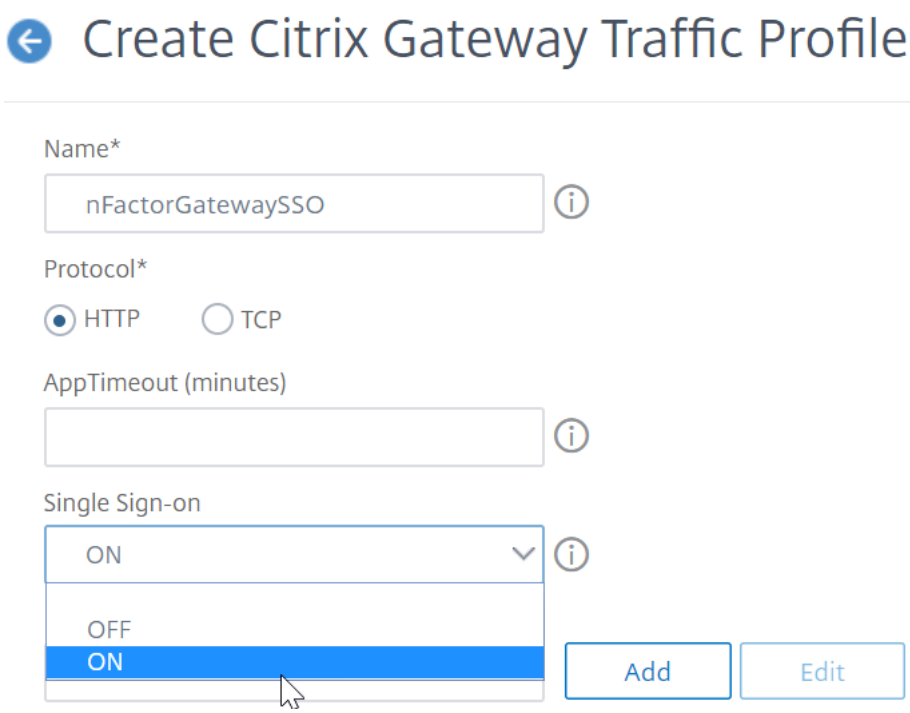
1. Navigieren Sie zu **NetScaler Gateway > Richtlinien > Verkehr**.



2. Klicken Sie auf der Registerkarte **Verkehrsprofile** auf **Hinzufügen**.

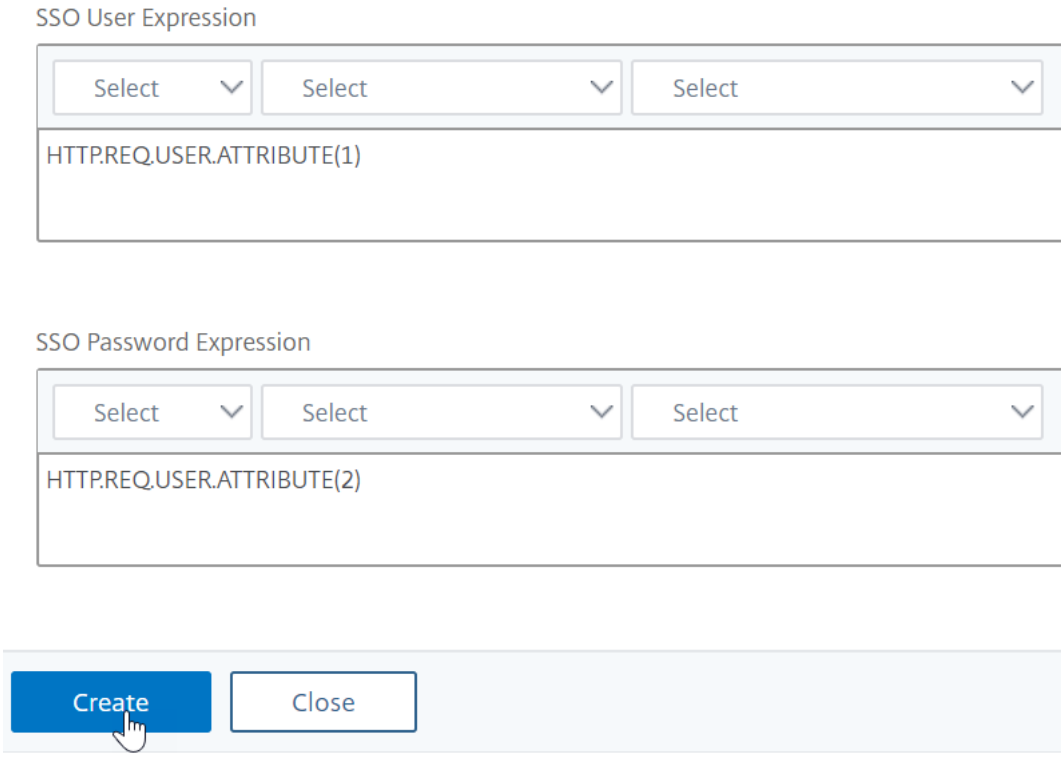


3. Geben Sie einen Namen für das Verkehrsprofil ein. Wählen Sie das **HTTP-Protokoll** aus. Wählen Sie unter **Einmaliges Anmelden** die Option **ON** aus.

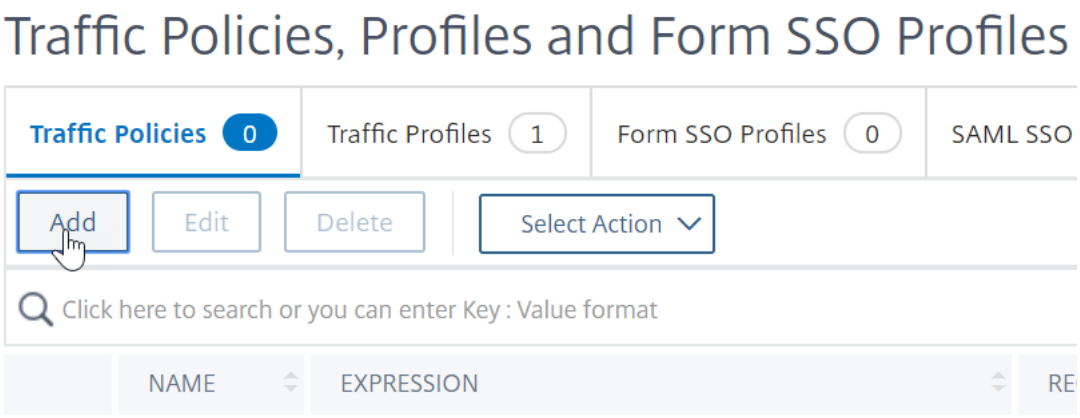


4. Geben Sie im **SSO-Ausdruck**einen AAA.USER.ATTRIBUTE (#) -Ausdruck ein, der den im Anmeldeschema angegebenen Indizes entspricht, und klicken Sie auf **Erstellen**.

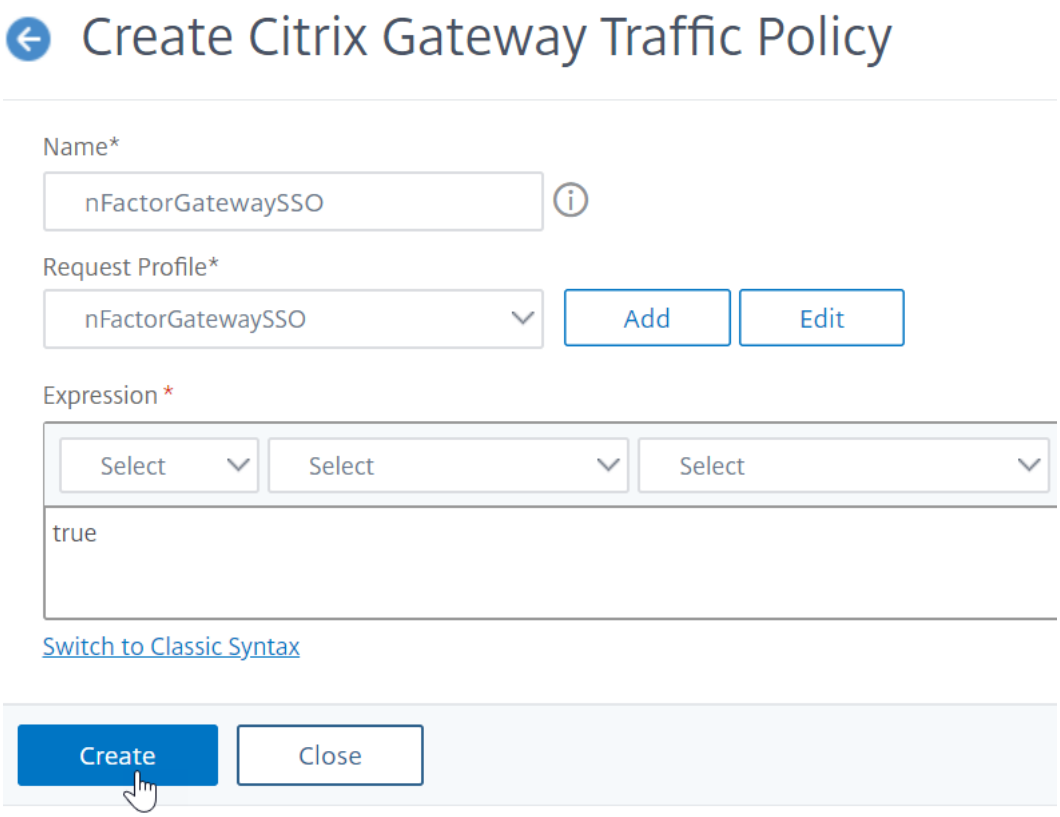
> **Hinweis**
> Der AAA.USER-Ausdruck ist jetzt implementiert, um die veralteten HTTP.REQ.USER-Ausdrücke zu ersetzen.



5. Klicken Sie auf **die Registerkarte Verkehrsrichtlinien** und dann auf **Hinzufügen**.



6. Geben Sie einen Namen für die Richtlinie ein. Wählen Sie das im vorherigen Schritt erstellte Verkehrsprofil aus. Geben Sie im Feld **Ausdruck**einen erweiterten Ausdruck ein und klicken Sie auf **Erstellen**.



7. Navigieren Sie zu **NetScaler Gateway > NetScaler Gateway Virtual Server**.
   - Wählen Sie einen vorhandenen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
   - Klicken Sie im Abschnitt **Richtlinien** auf das **+-Zeichen**.
   - Wählen Sie unter **Richtlinie wählen** die Option **Traffic** aus.
   - Wählen Sie unter **Typ wählen** die Option **Anfrage** aus.
   - Wählen Sie die von Ihnen erstellte Traffic-Richtlinie aus und klicken Sie dann auf **Bind**.

Beispielausschnitt zur nFactor-Konfiguration mithilfe der CLI

Um die schrittweisen Konfigurationen für die nFactor-Authentifizierung zu verstehen, sollten wir eine Zwei-Faktor-Authentifizierungsbereitstellung in Betracht ziehen, bei der der erste Faktor die LDAP-Authentifizierung und der zweite Faktor die RADIUS-Authentifizierung ist.

Bei dieser Beispielbereitstellung muss sich der Benutzer mit einem einzigen Anmeldeformular bei beiden Faktoren anmelden. Daher definieren wir ein einziges Anmeldeformular, das zwei Kennwörter akzeptiert. Das erste Kennwort wird für die LDAP-Authentifizierung und das andere für die RADIUS-Authentifizierung verwendet.
Hier sind die Konfigurationen, die ausgeführt werden:

1. Konfigurieren des virtuellen Lastausgleichsservers für die Authentifizierung

add lb vserver lbvs89 HTTP 1.136.19.55 80 -AuthenticationHost auth56.aaatm.com -Authentication ON

2. Konfigurieren Sie den virtuellen Authentifizierungsserver.

   add authentication vserver auth56 SSL 10.106.30.223 443 -AuthenticationDomain aaatm.com

3. Konfigurieren Sie das Anmeldeschema für das Anmeldeformular und binden Sie es an eine Richtlinie für das Anmeldeschema.

   add authentication loginSchema login1 -authenticationSchema login-2passwd.xml -userCredentialIndex 1 -passwordCredentialIndex 2

   Hinweis:

   Verwenden Sie den Benutzernamen und eines der Kennwörter, die im Anmeldeschema für Single Sign-On (SSO) für einen Back-End-Dienst eingegeben wurden, z. B. StoreFront. Sie können diese Indexwerte in der Verkehrsaktion referenzieren, indem Sie den Ausdruck AAA.USER.ATTRIBUTE (#) verwenden. Die Werte können zwischen 1 und 16 liegen.

   Alternativ können Sie die im Anmeldeschema eingegebenen Anmeldeinformationen als Single Sign-On-Anmeldeinformationen verwenden, indem Sie den folgenden Befehl verwenden.

```
add authentication loginSchema login1 -authenticationSchema login
    -2passwd.xml -SSOCredentials YES

 add authentication loginSchemaPolicy login1 -rule true -action
     login1
<!--NeedCopy-->
```

4. Konfigurieren Sie ein Anmeldeschema für den Passthrough und binden Sie es an ein Policy Label

```
add authentication loginSchema login2 -authenticationSchema
    noschema

add authentication policylabel label1 -loginSchema login2
<!--NeedCopy-->
```

5. Konfigurieren Sie die LDAP- und RADIUS-Richtlinien.

```
add authentication ldapAction ldapAct1 -serverIP 10.17.103.28 -
    ldapBase "dc=aaatm, dc=com" -ldapBindDn administrator@aaatm.com
     -ldapBindDnPassword 81
    qw1b99ui971mn1289op1abc12542389b1f6c111n0d98e1d78ae90c8545901 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
    samAccountName -groupAttrName memberOf -subAttributeName CN

add authentication Policy ldap -rule true -action ldapAct1
```



```
4
5 add authentication radiusAction radius -serverIP 10.101.14.3 -
      radKey
      n231d9a8cao8671or4a9ace940d8623babca0f092gfv4n5598ngc40b18876hj32
       -encrypted -encryptmethod ENCMTHD_3 -radNASip ENABLED -
      radNASid NS28.50 -radAttributeType 11 -ipAttributeType 8
6
7 add authentication Policy radius -rule true -action radius
8 <!--NeedCopy-->
```

6. Binden Sie die Richtlinie für das Anmeldeschema an den virtuellen Authentifizierungsserver

```
1 bind authentication vserver auth56 -policy login1 -priority 1 -
      gotoPriorityExpression END
2 <!--NeedCopy-->
```

7. Binden Sie die LDAP-Richtlinie (erster Faktor) an den virtuellen Authentifizierungsserver.

```
1 bind authentication vserver auth56 -policy ldap -priority 1 -
      nextFactor label1 -gotoPriorityExpression next
2 <!--NeedCopy-->
```

8. Binden Sie die RADIUS-Richtlinie (zweiter Faktor) an die Bezeichnung der Authentifizierungsrichtlinie.

```
1 bind authentication policylabel label1 -policyName radius -
      priority 2 -gotoPriorityExpression end
2 <!--NeedCopy-->
```

nFactor Visualizer für vereinfachte Konfiguration

May 11, 2023

Ab NetScaler Version 13.0 Build 36.27 wird die nFactor-Konfiguration über die GUI mithilfe des nFactor Visualizer vereinfacht. Der nFactor Visualizer hilft Administratoren dabei, mehrere Faktoren hinzuzufügen, ohne den Überblick über jeden Faktor zu verlieren. Die Gruppe der Faktoren, die im Flow enthalten sind, wird an einer Stelle angezeigt. Administratoren können die Erfolgs- und Fehlerpfade der Authentifizierung separat hinzufügen. Nach dem Erstellen des Flows müssen Administratoren den nFactor-Flow an einen virtuellen Authentifizierungsserver binden.

> **Hinweis**
>
> - Alle Faktoren, die von einem Administrator im nFactor-Flow erstellt wurden, werden für

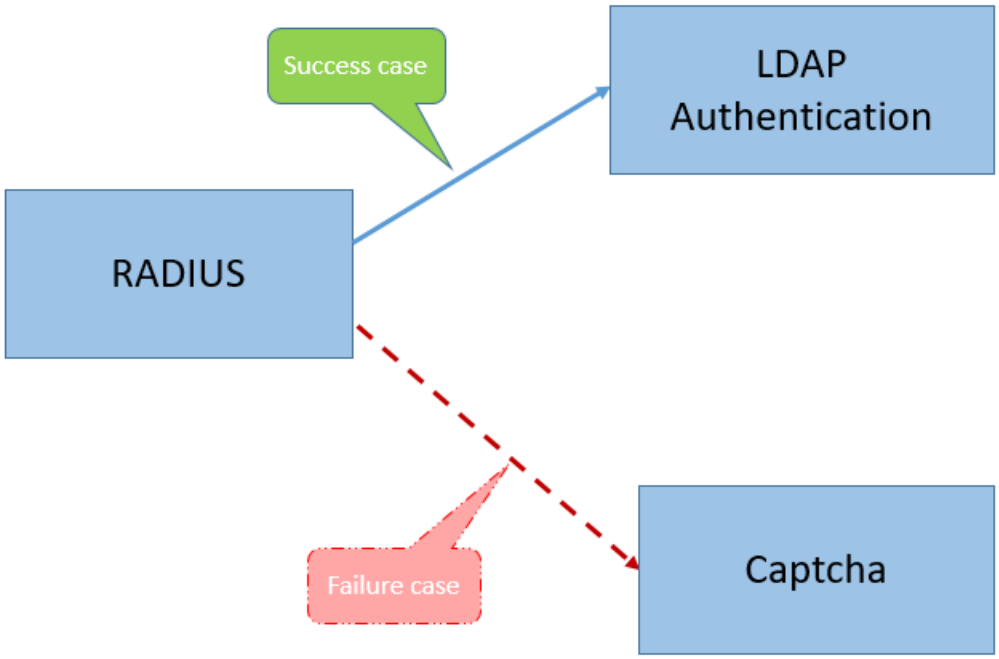
jede zukünftige Verwendung aufbewahrt.

- Ab NetScaler Feature Release 13.0 Build 64.35 und höher können Sie mithilfe des nFactor-Visualizers den nFactor-Flow mit einem Entscheidungsblock starten.

Bisher war die nFactor-Konfiguration umständlich, da die Administratoren viele Seiten besuchen mussten, um sie zu konfigurieren. Wenn eine Änderung erforderlich war, mussten die Admins die konfigurierten Abschnitte jedes Mal erneut aufrufen. Außerdem gab es keine Möglichkeit, die gesamte Konfiguration an einem Ort einzusehen.

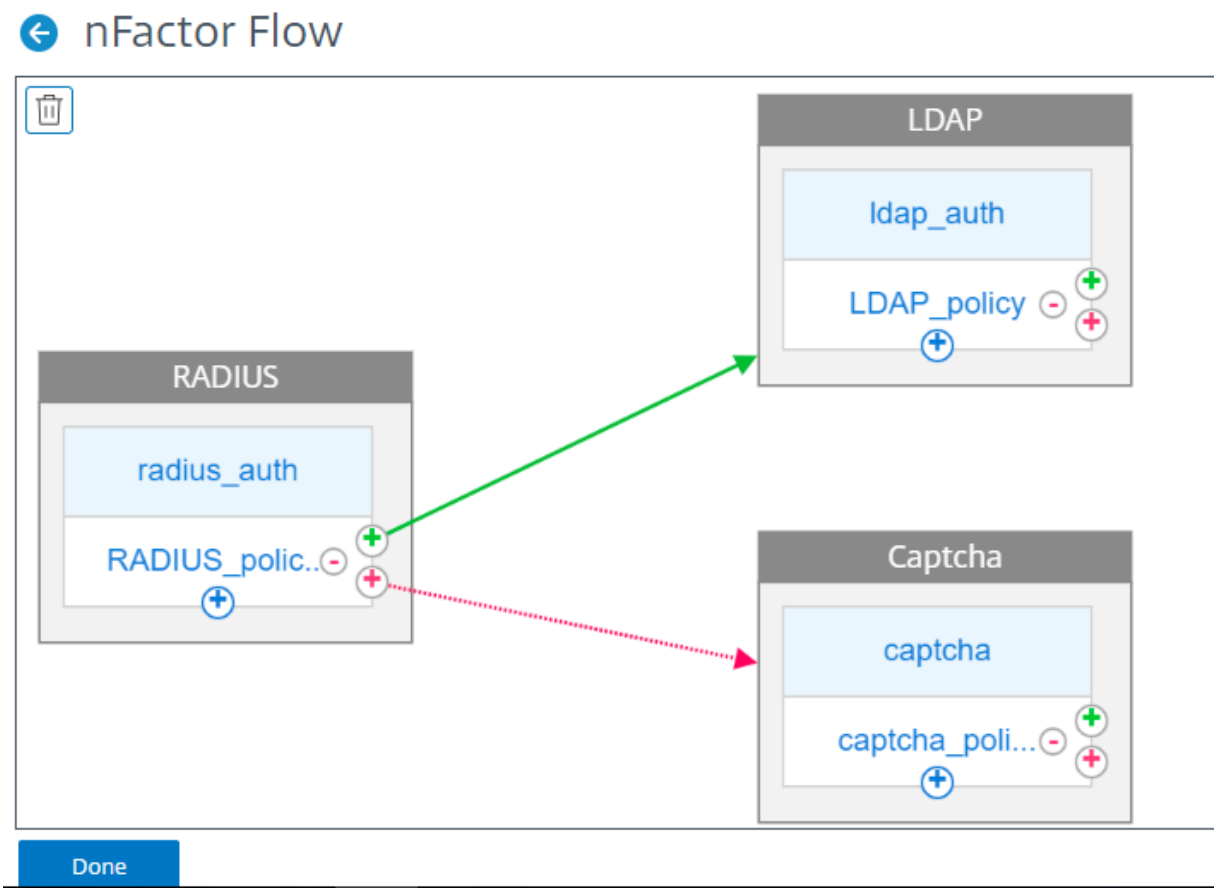
Anwendungsfall 1: RADIUS gefolgt von LDAP-Authentifizierung, andernfalls Fallback auf Captcha über nFactor Visualizer

Erzielen Sie die RADIUS-Authentifizierung als Authentifizierung der ersten Ebene, gefolgt von der LDAP-Authentifizierung. Falls RADIUS fehlschlägt, muss die Authentifizierung auf Captcha zurückgreifen.



Um diesen Anwendungsfall zu erreichen, können Sie den nFactor Visualizer verwenden. Der Visualizer bietet verschiedene Steuerelemente, mit denen dieser Flow und die zugehörigen Elemente hinzugefügt werden können.

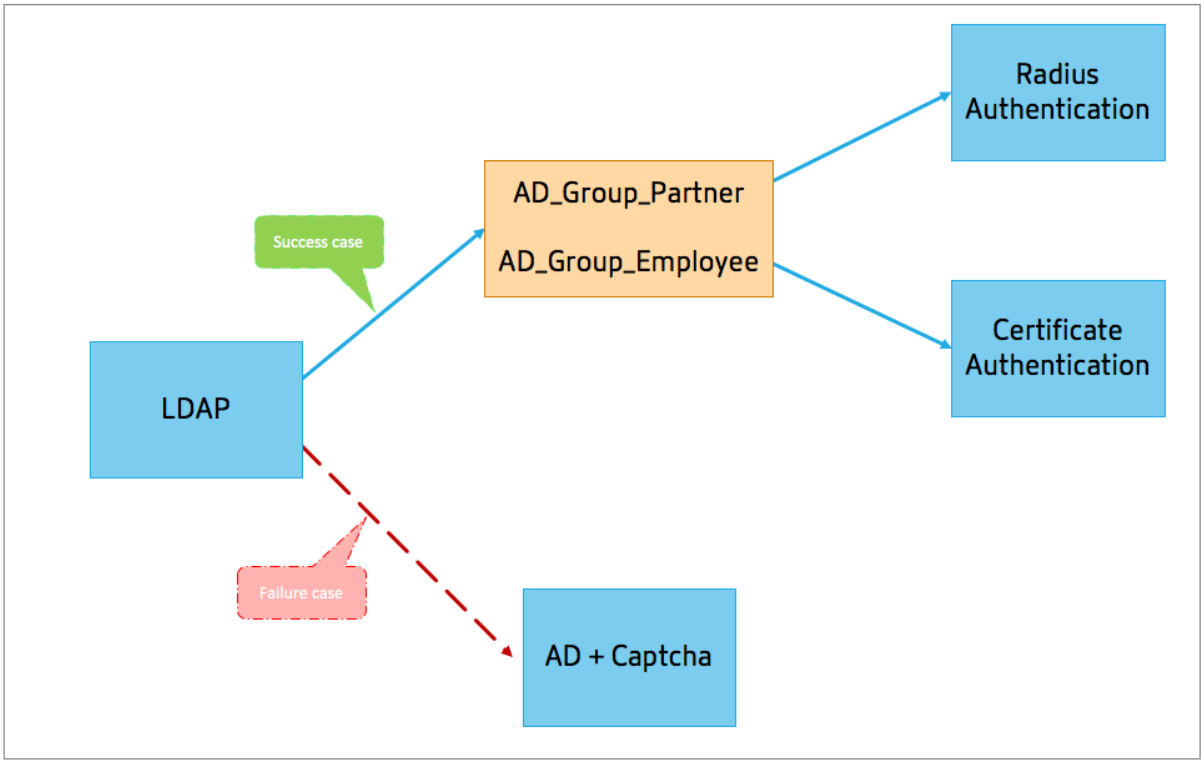
Die folgende Abbildung zeigt den nFactor-Flow, der für den zuvor genannten Anwendungsfall mithilfe des Visualizers erstellt wurde.



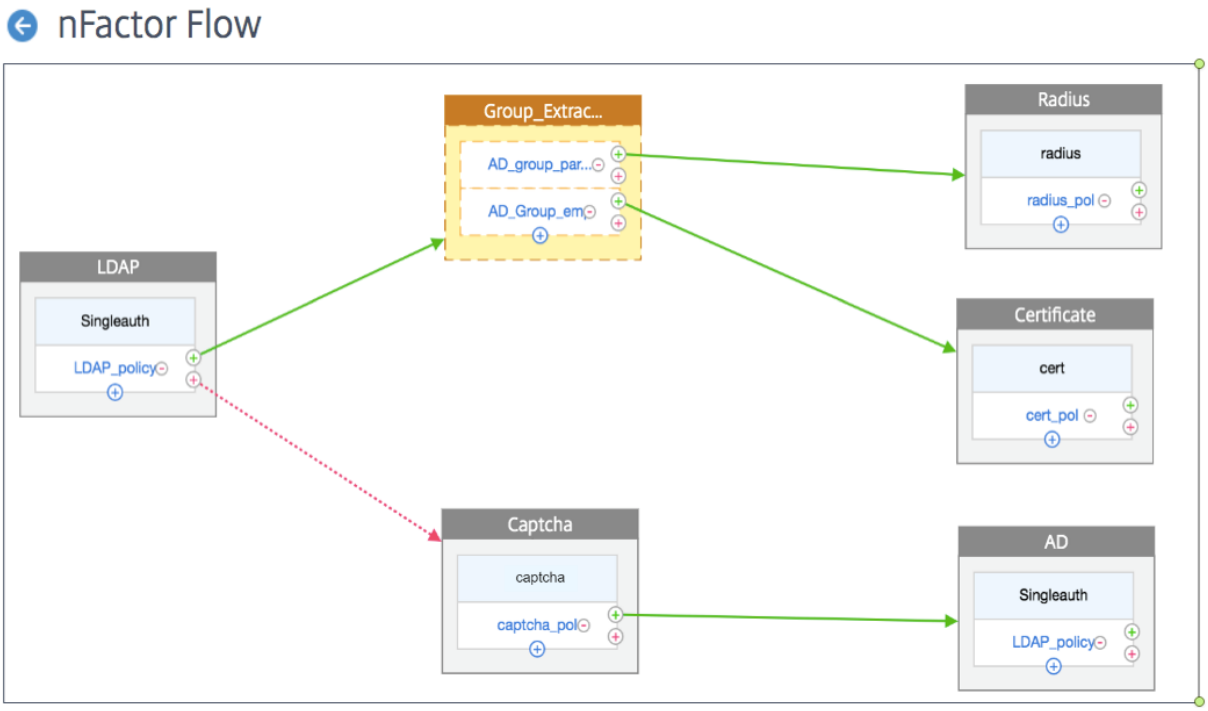
- **RADIUS.** Sie konfigurieren RADIUS als ersten Faktor. Sie fügen ein Anmeldeschema und eine Richtlinie hinzu. In diesem Beispiel sind radius_auth und RADIUS_Policy das Anmeldeschema und die Richtlinie, die hinzugefügt wurden. Für die RADIUS_Policy können Sie einen weiteren Faktor für den Erfolgsfall hinzufügen. In diesem Beispiel wird ein LDAP-Faktorblock für den Erfolgsfall hinzugefügt. Für den Fehlerfall können Sie einen Captcha-Faktor hinzufügen.
- **LDAP.** Sie konfigurieren die LDAP-Authentifizierung als zweiten Faktor. Sie fügen ein Anmeldeschema und eine Richtlinie hinzu. In diesem Beispiel sind ldap_auth und ldap_Policy das Anmeldeschema und die Richtlinie, die hinzugefügt wurden.
- **Captcha.** Für den Fall, dass die RADIUS-Richtlinie ausfällt, erstellen Sie einen Captcha-Faktor. In diesem Beispiel sind Captcha und captcha_policy das Anmeldeschema und die Richtlinie, die hinzugefügt wurden.

Anwendungsfall 2: LDAP gefolgt von einer RADIUS-/Zertifikatsauthentifizierung mit Captcha auf der Grundlage der LDAP-Gruppenmitgliedschaft über nFactor Visualizer

Erzielen Sie die RADIUS-Authentifizierung als Authentifizierung der ersten Ebene, gefolgt von der LDAP-Authentifizierung. Falls RADIUS fehlschlägt, muss die Authentifizierung auf Captcha zurückgreifen.



Die folgende Abbildung zeigt den nFactor-Flow, der für den zuvor genannten Anwendungsfall mithilfe des Visualizers erstellt wurde.



- **LDAP.** Sie konfigurieren LDAP als ersten Faktor. Sie fügen ein Anmeldeschema und eine Richtlinie hinzu. In diesem Beispiel sind SingleAuth und LDAP_Policy das Anmeldeschema

und die Richtlinie, die hinzugefügt wurden. Für die LDAP_Policy können Sie einen weiteren Faktor für den Erfolgsfall hinzufügen. In diesem Beispiel wird ein Entscheidungsblock für den Erfolgsfall hinzugefügt. Für den Fehlerfall können Sie Captcha gefolgt von AD-Faktor hinzufügen.

- **Gruppenextraktion LDAP.** Wurde der Entscheidungsblock für den LDAP-Erfolgsfall hinzugefügt. Der Entscheidungsblock wird als Verzweigungsfaktor verwendet, um die Benutzer auf der Grundlage der Policy-Regeln zu trennen. Visualizer ermöglicht nur die Konfiguration einer NO_AUTHN-Richtlinie für den Entscheidungsblock.

  In diesem Beispiel ist Group_Extraction_LDAP der Entscheidungsblock. Sie fügen diesem Entscheidungsblock zwei Richtlinien (`AD_Group_Partner and AD_Group_Employee`) hinzu. Wie in den Anwendungsfällen erläutert, verwenden alle Anfragen, die über die AD_Group_Partner-Richtlinie weitergeleitet werden, die RADIUS-Authentifizierung. Daher verbinden Sie den Erfolgsfall dieser Richtlinie mit dem nächsten Faktor, dem RADIUS-Faktor. In ähnlicher Weise verwenden alle Anfragen, die über die AD_Group_Employee-Richtlinie weitergeleitet werden, die Zertifizierungsauthentifizierung. Daher verbinden Sie den Erfolgsfall dieser Richtlinie mit dem nächsten Faktor, dem Authentifizierungsfaktor für die Zertifizierung.

  - **RADIUS.** Für den Erfolgsfall der AD_Group_Partner-Richtlinie erstellen Sie den RADIUS-Authentifizierungsfaktor.
  - **Zertifikat.** Für den Erfolgsfall der Richtlinie AD_Group_Employee erstellen Sie den Authentifizierungsfaktor für das Zertifikat.

- **Captcha.** Für den Fall, dass die LDAP-Richtlinie ausfällt, erstellen Sie zwei nächste Faktoren: Captcha und AD-Faktor.

> **Hinweis**
>
> - Wenn Sie einen Anwendungsfall haben, den Sie als erstes verzweigen möchten, können Sie entweder zwei Flows erstellen und diese getrennt binden oder einen Flow erstellen, bei dem der erste als Branch-Out verwendet wird, und ihn an den virtuellen Server binden.
> - Wenn Sie mehrere Blöcke haben und den gesamten Flow im nFactor Flow-Bildschirm anzeigen möchten, klicken Sie auf den Visualizer und ziehen Sie den Flow ganz nach links.
> - Citrix empfiehlt, die nFactor-Flows nur mithilfe der nFactor Flows-Seite zu ändern.

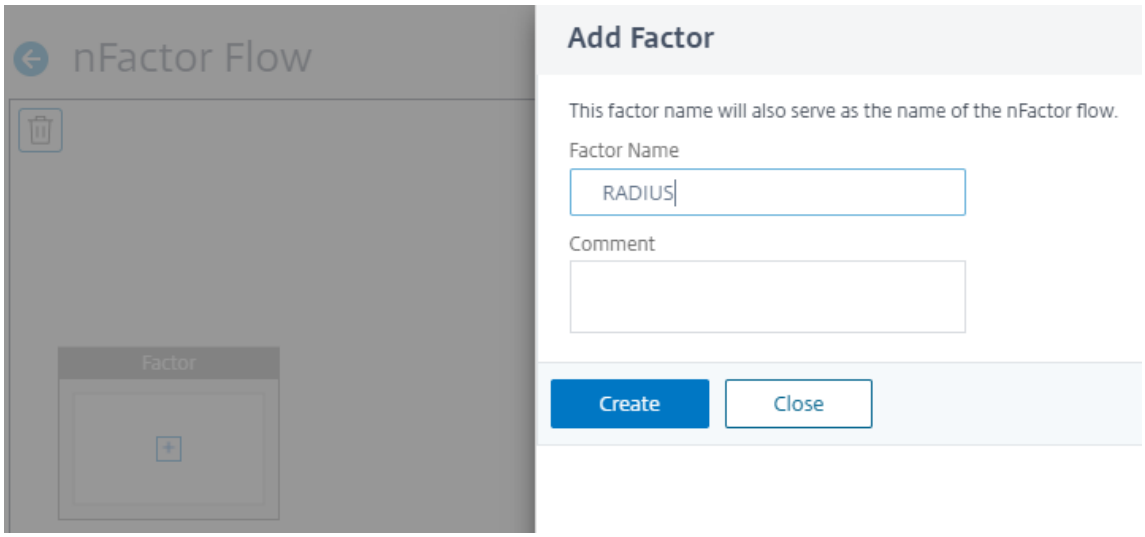
So konfigurieren Sie nFactor mithilfe des nFactor Visualizer

> **Hinweis:**
>
> Die folgende nFactor-Konfiguration ist ein einfaches Beispiel, das Ihnen hilft, die Szenariokonfigurationen für Anwendungsfall 1 durchzuführen.

1. Navigieren Sie zu **Sicherheit > AAA — Application Traffic > nFactor Visualizer > nFactor**Flows.

2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf der Seite **nFactor Flows** auf **+**, um einen ersten Faktor für den Flow hinzuzufügen. Der erste Faktor dient auch als Identifier für diesen nFactor-Flow.

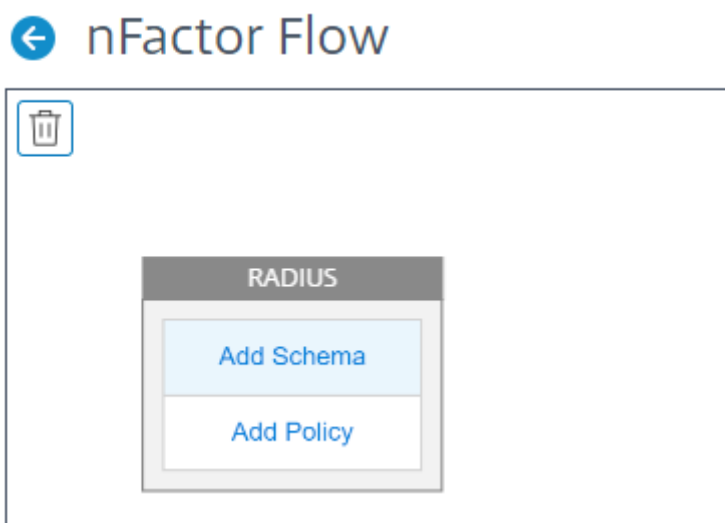
4. Geben Sie den Namen des Faktors ein und klicken Sie auf **Erstellen**.



Der Faktorname wird auf dem Faktorblock auf der nFactor Flow-Seite angezeigt.

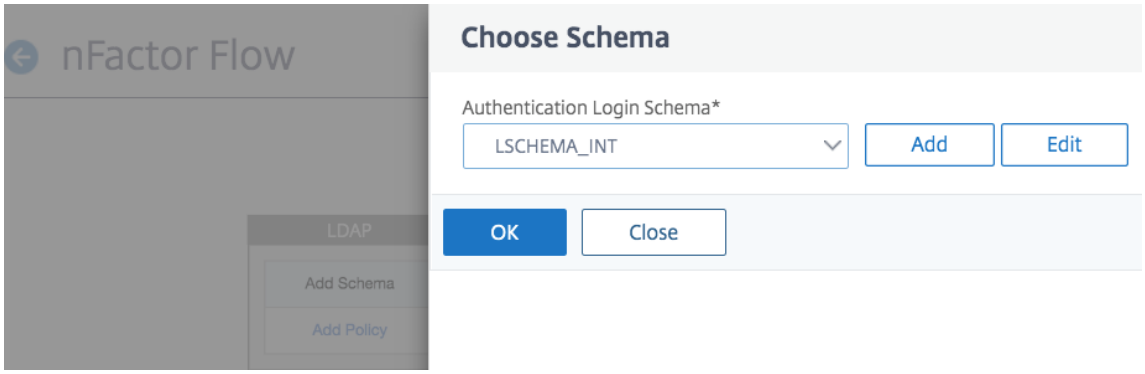
> **Hinweis**
>
> Citrix empfiehlt, dass Sie keine Richtlinienbezeichnungen wie, `__root` und als Suffix und `__<flow_name>_db_` als Präfix verwenden dürfen. Es wird als Faktorname verwendet, der im nFactor-Flow erstellt wird.

5. Sobald der RADIUS-Faktor erstellt wurde, müssen die Optionen Schema hinzufügen und Richtlinie hinzufügen erstellt werden.

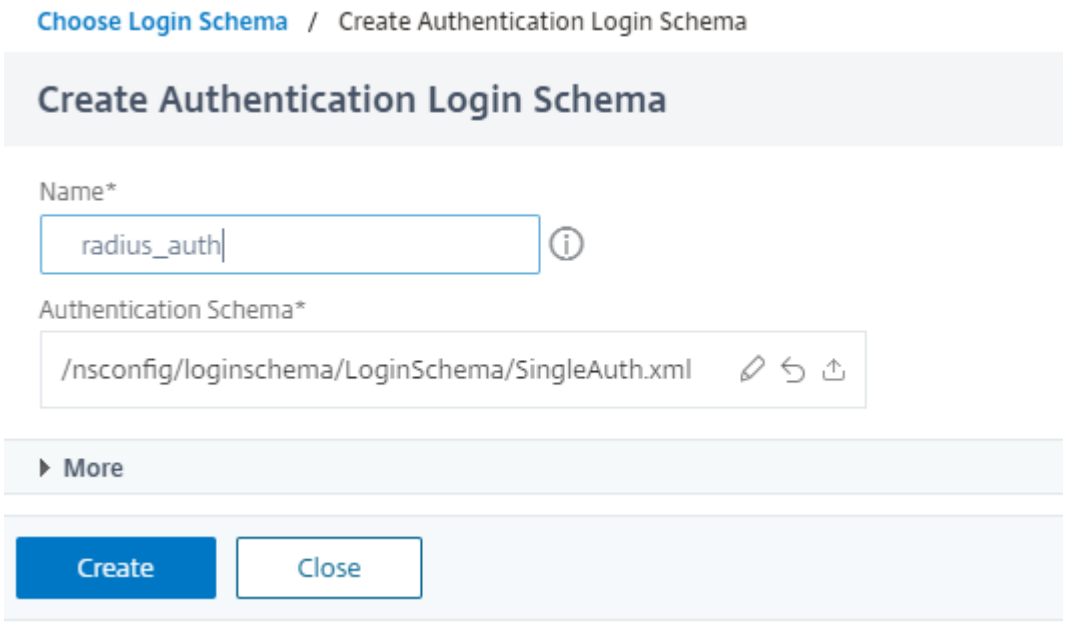


> **Hinweis**
>
> Weitere Informationen finden Sie unter Konzepte, Entitäten und Terminologie von nFactor.

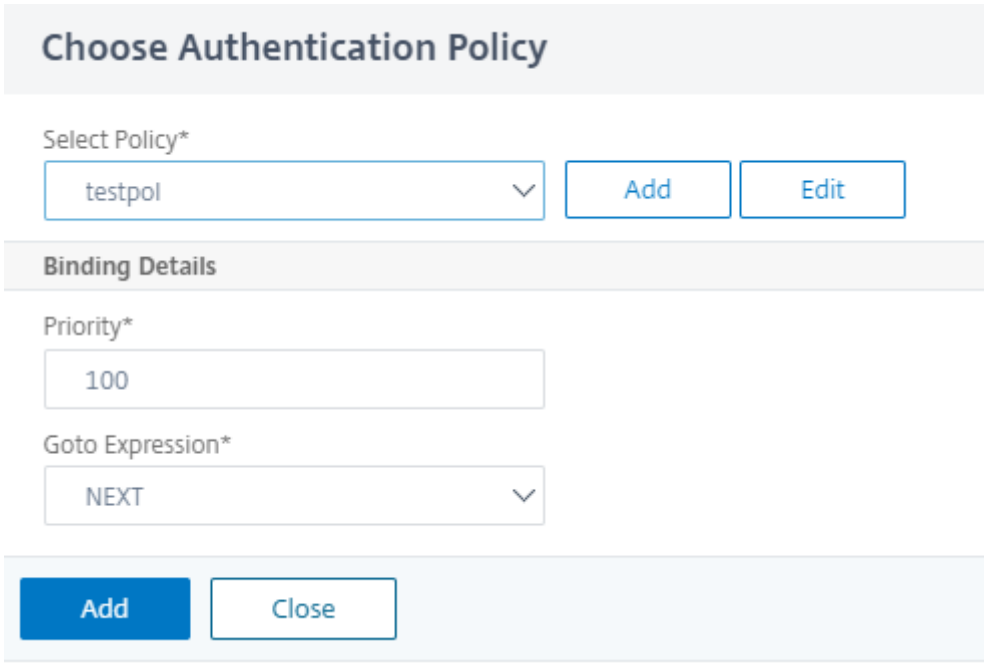
6. Klicken Sie auf **Schema hinzufügen**. Sie können entweder ein neues Anmeldeschema hinzufügen oder ein vorhandenes Anmeldeschema aus der Liste der **Anmeldeschemata für die Authentifizierung** auswählen.



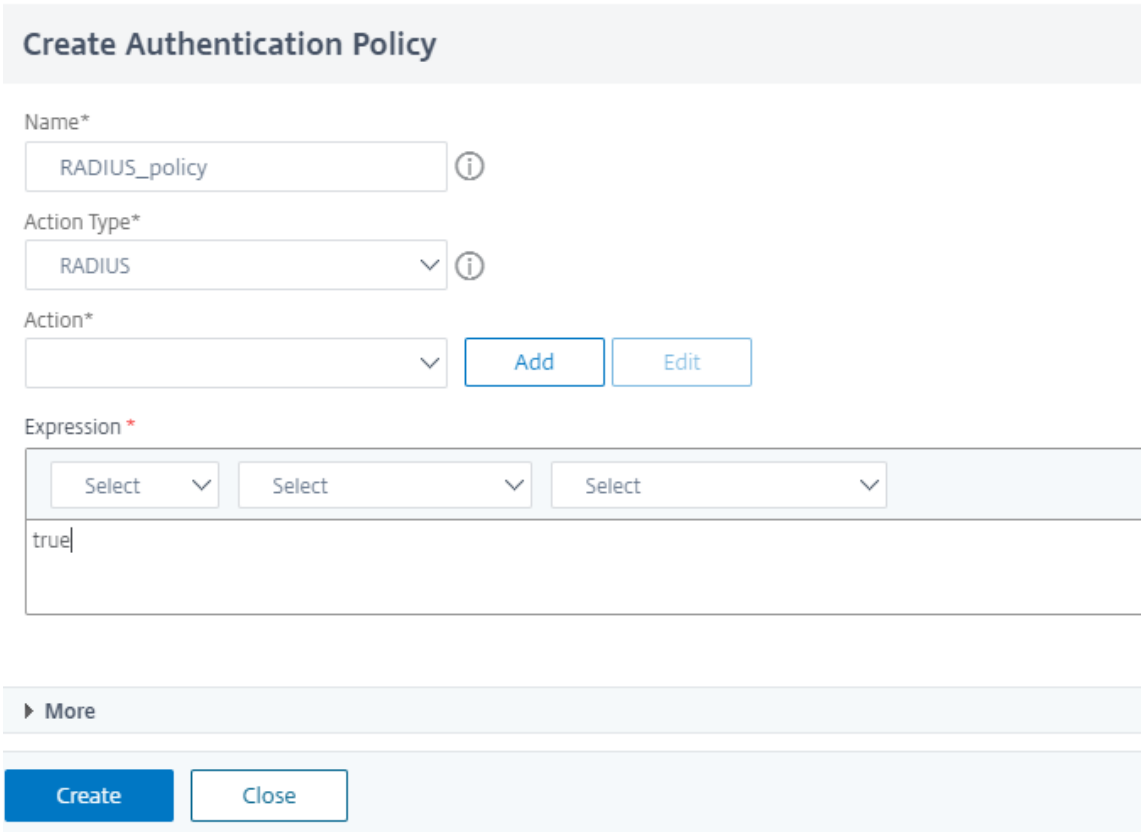
7. Um ein Anmeldeschema zu erstellen, klicken Sie auf **Hinzufügen** und geben Sie auf der Seite **Authentifizierungs-Anmeldeschema erstellen** den Namen für das Schema ein. Klicken Sie auf **Bearbeiten** (Stiftsymbol), um die **Anmeldeschemadateien** aus der Liste auszuwählen.



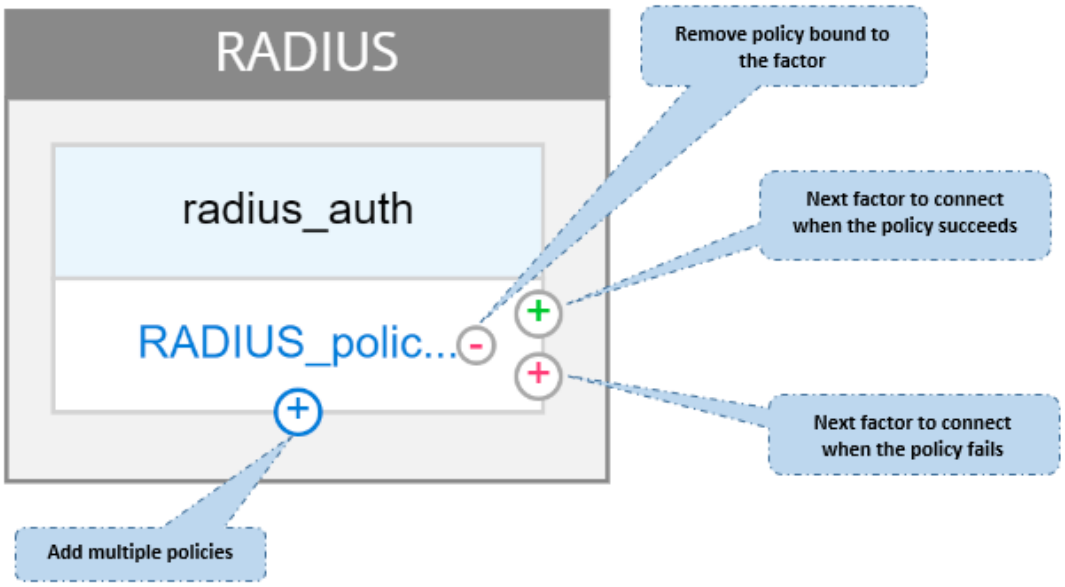
8. Klicken Sie auf **Richtlinie hinzufügen**. Sie können eine Authentifizierungsrichtlinie erstellen oder eine vorhandene Authentifizierungsrichtlinie auswählen.



9. Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen** und geben Sie auf der Seite „ **Authentifizierungsrichtlinie erstellen** “ den Namen für die Richtlinie ein und klicken Sie auf **Erstellen**.



10. Nachdem Sie dem Faktor ein Anmeldeschema und eine Richtlinie hinzugefügt haben, werden das Anmeldeschema und die Richtlinie auf dem Faktor im Visualizer angezeigt, wie in der folgenden Abbildung dargestellt. Für jeden bestimmten Faktor können Sie mehrere Richtlinien hinzufügen und den nächsten Faktor für den Erfolg und Misserfolg jeder Richtlinie definieren. Sie können auch die Richtlinien entfernen, die Teil des Faktors sind.



11. Nachdem Sie den Flow erstellt haben, können Sie den nFactor-Flow an einen virtuellen Authentifizierungsserver binden.

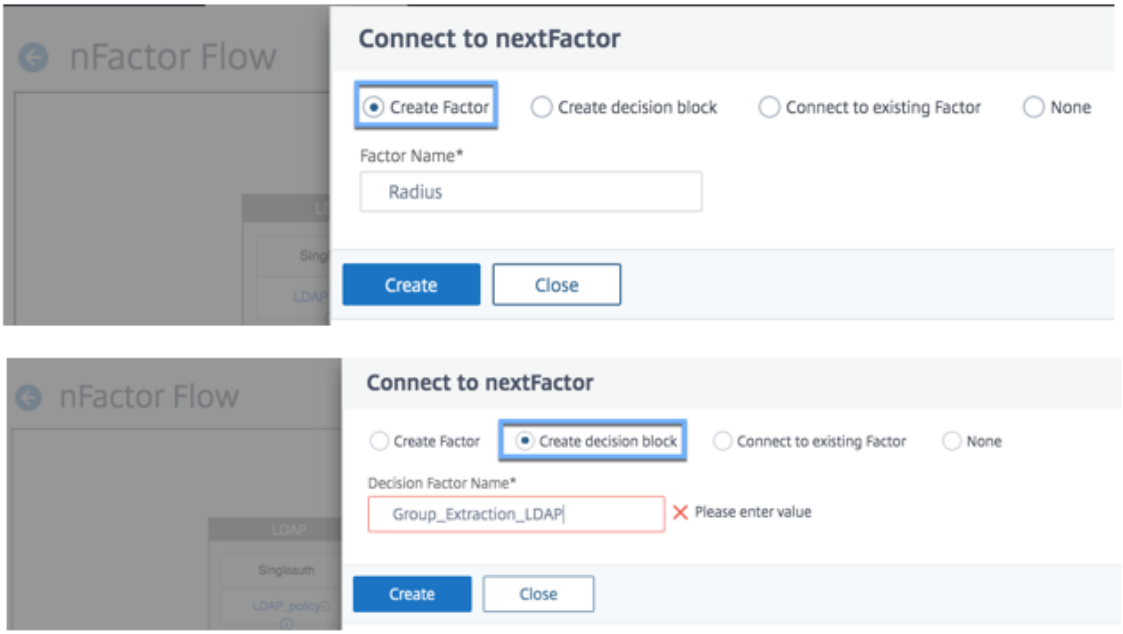
Den nächsten Faktor hinzufügen

Um den nächsten Faktor hinzuzufügen, können Sie je nach Anforderung eine der folgenden Optionen auswählen:

- **Faktor erstellen**. Erstellen Sie einen Faktor. Jeder Faktor, der in einem Flow erzeugt wird, ist ausschließlich für diesen Fluss bestimmt.
- **Erstellen Sie einen Entscheidungsblock.** Erstellen Sie einen Entscheidungsblock, der als Verzweigungsfaktor dient. Sie können dem Entscheidungsblock kein Anmeldeschema hinzufügen. Visualizer ermöglicht nur die Konfiguration einer NO_AUTHN-Richtlinie für den Entscheidungsblock.

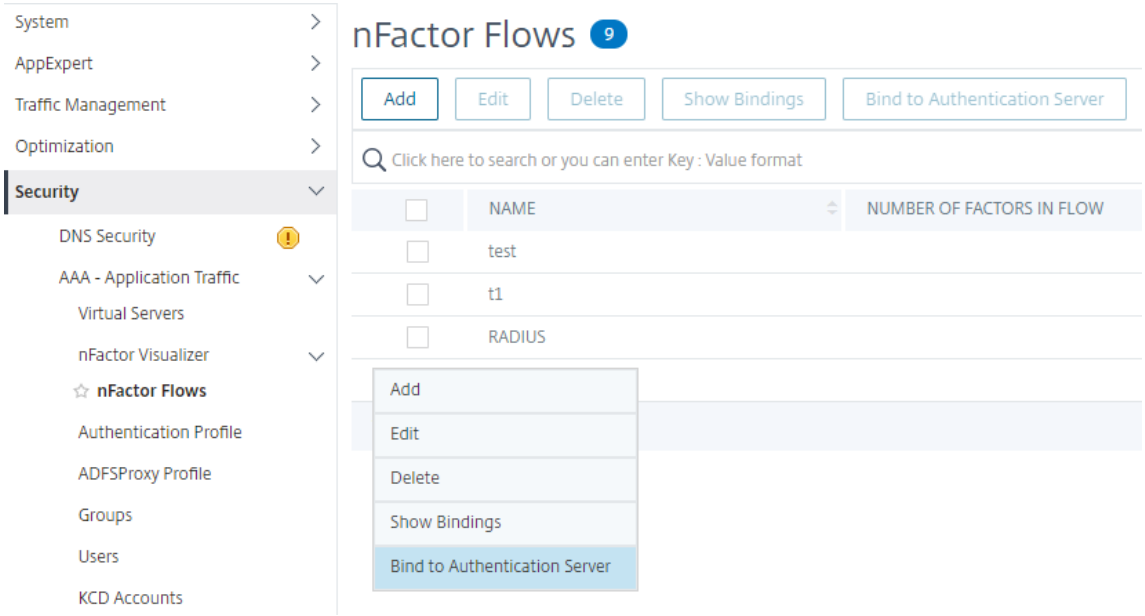
  > **Hinweis**
  >
  > Sie können den Entscheidungsblock nur über die NetScaler-GUI hinzufügen oder bearbeiten. Es gibt keine Möglichkeit, den Entscheidungsblock über den CLI-Befehl zu konfigurieren.

- Stellen Sie eine**Verbindung zu einem vorhandenen Factor**her. Wählen Sie einen vorhandenen Faktor als nächsten Faktor aus. Alle Faktoren, die in der vorhandenen Liste erscheinen, wurden ausschließlich für diesen Flow erstellt.
- **Keine.** Entfernen Sie eine bestehende Verbindung.



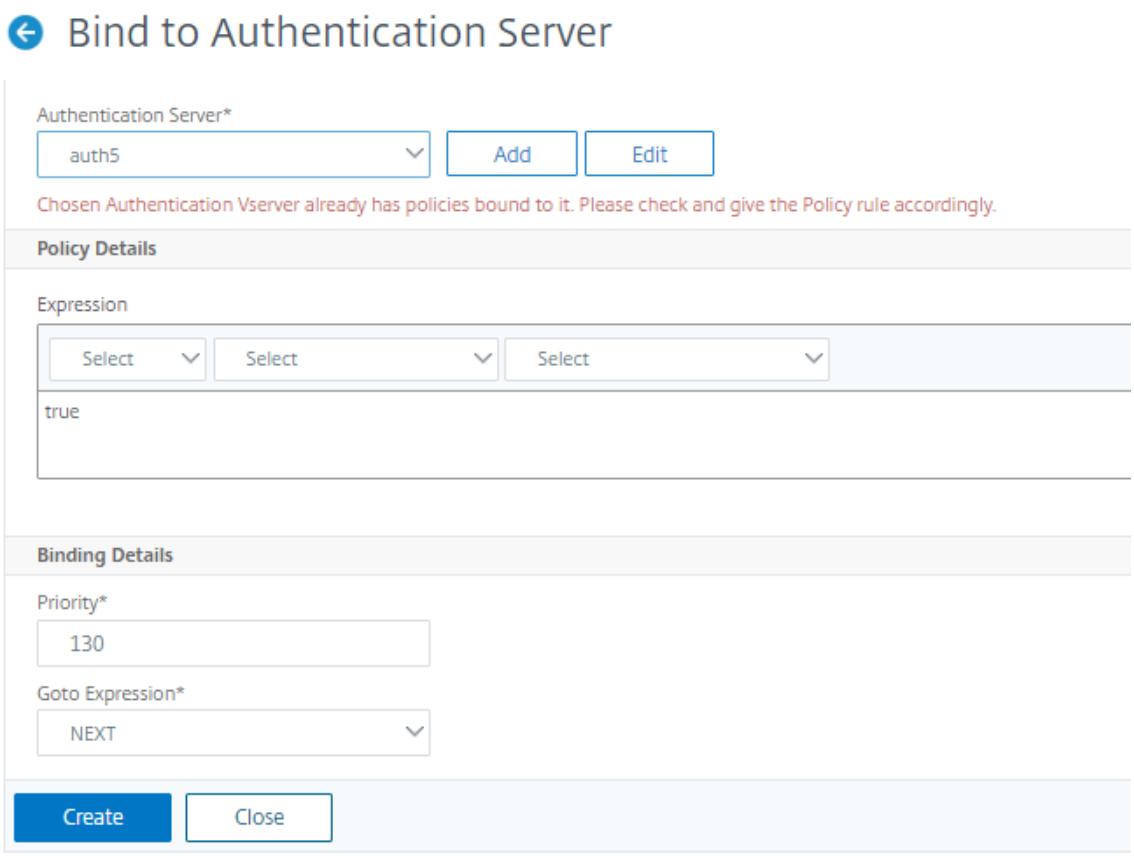
Um den nFactor-Flow an den Authentifizierungsserver zu binden

1. Wählen Sie auf der Seite **nFactor Flows** einen nFactor-Flow aus, den Sie lieber an einen virtuellen Authentifizierungsserver binden möchten.
2. Klicken Sie auf das Hamburgersymbol, **um die Option An Authentifizierungsserver binden** auszuwählen, oder klicken Sie im Detailbereich **auf An Authentifizierungsserver binden**.

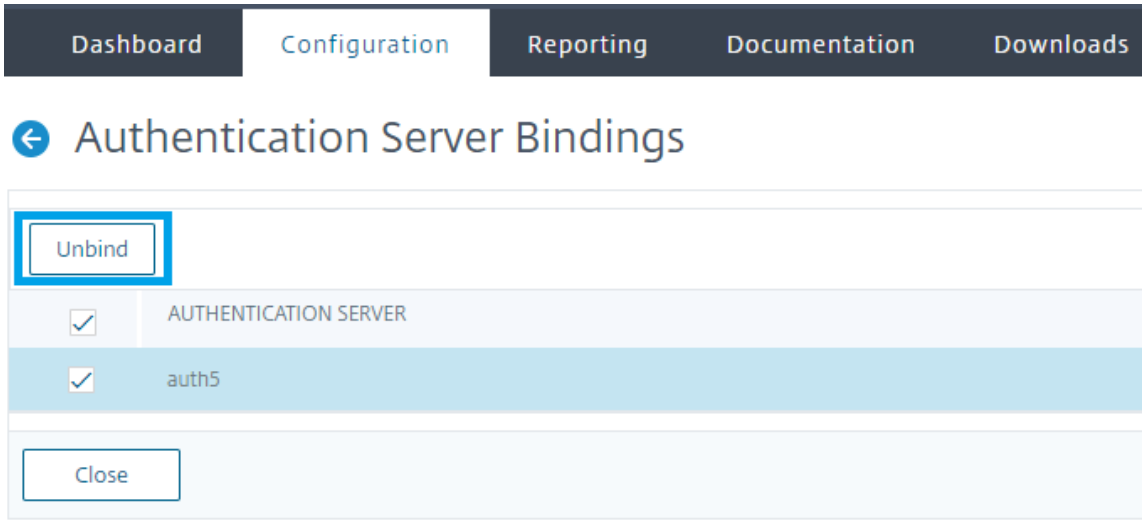


3. Auf der Seite **An Authentifizierungsserver binden** können Sie die folgenden Aktionen ausführen:

- Um einen **virtuellen Authentifizierungsserver**hinzuzufügen, klicken Sie auf **Hinzufügen**.
- Um einen vorhandenen Authentifizierungsserver aus der Liste auszuwählen, klicken Sie auf das Feld **Authentifizierungsserver** .



4. Klicken Sie auf dem Hamburger-Symbol auf **Bindungen anzeigen**, um die Bindungen anzuzeigen.
5. Gehen Sie wie folgt vor, um den Authentifizierungsserver vom spezifischen nFactor-Flow zu trennen:
   - Klicken Sie auf der **nFactor Flows-Seite** im Hamburger-Symbol auf **Bindungen anzeigen** .
   - Wählen Sie auf der Seite **Authentifizierungsserver-Bindungen** den Authentifizierungsserver aus, dessen Bindung aufgehoben werden soll, und klicken Sie auf **Bindung aufheben**. Klicken Sie auf **Schließen**.



Weitere Informationen zur nFactor-Authentifizierung finden Sie in den folgenden Themen:

- Konzept: Multi-Factor (nFactor) Authentifizierung.
- Workflow: Wie die nFactor-Authentifizierung funktioniert.
- Konfiguration: Konfigurieren der nFactor-Authentifizierung.

Verbesserungen am nFactor Visualizer

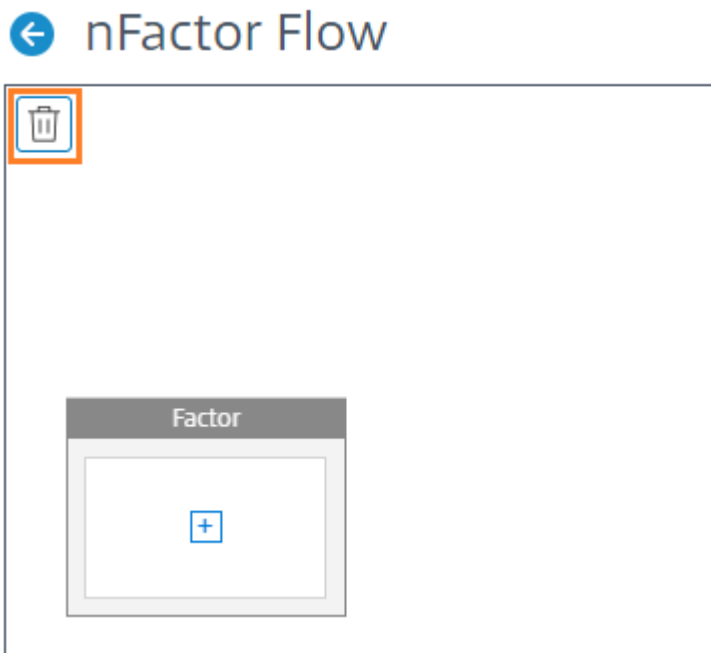
Ab NetScaler Version 13.0 Build 41.20 wurden die folgenden Verbesserungen im nFactor Visualizer vorgenommen.

- Administratoren können die erstellten Faktoren auf das Papierkorbsymbol verschieben.
- Sehen Sie sich die nFactor-Flows auf der Seite Virtueller Authentifizierungsserver an.

Mülleimersymbol. Administratoren können nur die Knoten löschen, die keine Verbindungen haben. Die zugrunde liegenden Richtlinien oder Schemas, die für den Faktor erstellt wurden, werden jedoch nicht gelöscht, wenn der Faktor in den Papierkorb verschoben wird.

Um das Papierkorbsymbol zu sehen,

1. Navigieren Sie zu **Sicherheit > AAA — Application Traffic > nFactor Visualizer > nFactor**Flows.

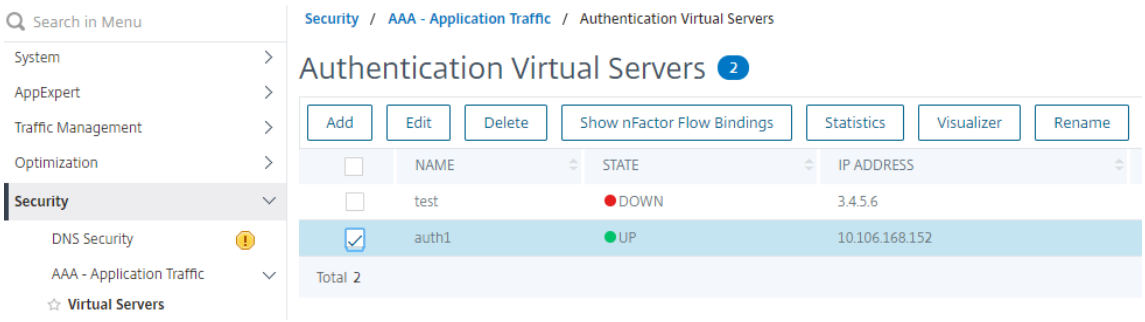


2. Um den Faktor zu löschen, klicken Sie auf den Faktorblock und ziehen Sie ihn in den Papierkorb.

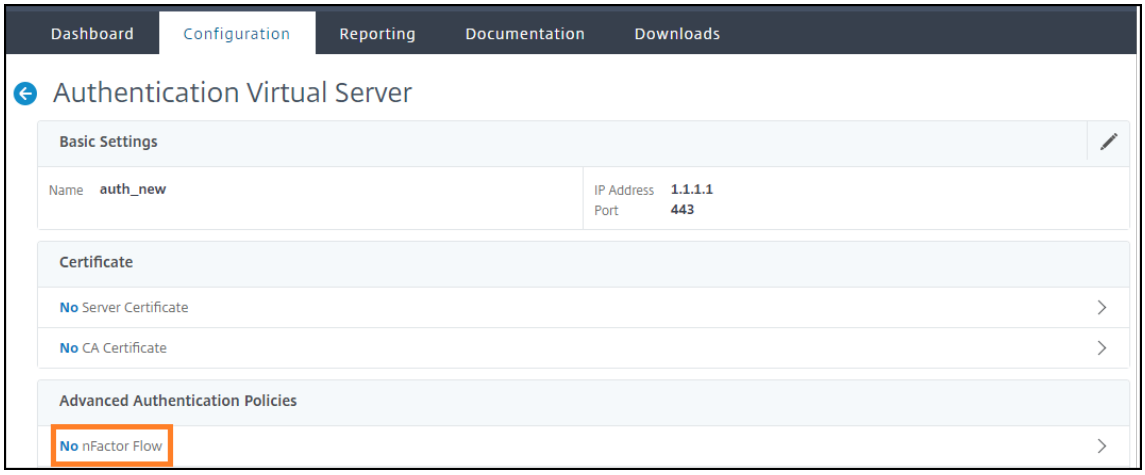
Zeigen Sie den nFactor-Flow vom virtuellen Authentifizierungsserveran. Administratoren können die erstellten nFactor-Flows auch auf der Seite Virtueller Authentifizierungsserver einsehen.

Um den nFactor-Flow auf der Seite „Virtueller Authentifizierungsserver“ anzuzeigen,

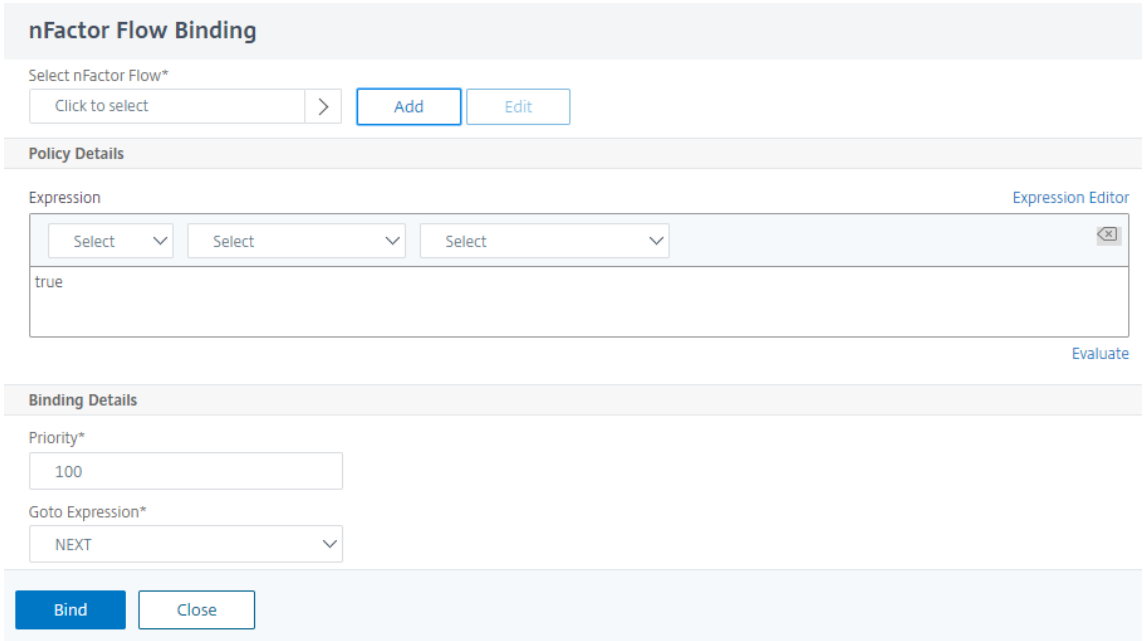
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**. Auf der Seite **Virtuelle Authentifizierungsserver** können Sie die folgenden Schritte ausführen:
   - Um einen virtuellen Authentifizierungsserver hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen virtuellen Authentifizierungsserver zu **bearbeiten, klicken Sie im Detailbereich auf Option Bearbeiten** .



2. Auf der Seite **Virtueller Authentifizierungsserver** können Sie die Option **nFactor Flow** unter **Advanced Authentication Policies**einsehen.



3. Wenn kein nFactor-Flow an den virtuellen Server gebunden ist, können Sie im Abschnitt **Erweiterte Authentifizierungsrichtlinien** auf die Option **Kein nFactor-Flow** klicken, um entweder einen neuen nFactor-Flow hinzuzufügen oder den vorhandenen nFactor-Flow aus der Liste auszuwählen.



nFactor Erweiterbarkeit

May 11, 2023

Das nFactor-Authentifizierungsframework bietet die Flexibilität, Anpassungen hinzuzufügen, um die Anmeldeoberfläche für eine umfangreiche Benutzererfahrung intuitiver zu gestalten. Sie können benutzerdefinierte Anmeldebeschriftungen, benutzerdefinierte Anmeldeinformationen, Benutzerober-

flächenanzeigen usw. hinzufügen.

Mit nFactor kann jeder Faktor seinen eigenen Anmeldebildschirm haben. In jedem Anmeldebildschirm können Sie Informationen aus einem der vorherigen Faktoren oder weitere Informationen anzeigen, die in anderen Faktoren nicht sichtbar sind. Ihr letzter Faktor kann beispielsweise eine informative Seite sein, auf der der Benutzer die Anweisungen liest und auf Weiter klickt.

Vor nFactor waren benutzerdefinierte Anmeldeseiten begrenzt und Anpassungen und benötigten Unterstützung. Es war möglich, die tmindex.html zu ersetzen oder Umschreibregeln anzuwenden, um einen Teil seines Verhaltens zu ändern. Es war jedoch nicht möglich, die zugrunde liegende Funktionalität zu erreichen.

Die folgenden nFactor-bezogenen Anpassungen werden in diesem Thema ausführlich erfasst.

- Anmelde-Labels
- Benutzeroberfläche anpassen, um Images anzuzeigen
- Anpassen des NetScaler nFactor-Anmeldeformulars

Annahmen

Sie sind mit nFactor, Shell-Befehlen, XML und Texteditoren vertraut.

Voraussetzungen

- Die in diesem Thema beschriebene Anpassung ist nur möglich, wenn das RFWeb-UI-Thema (oder themenbasiert) auf NetScaler konfiguriert ist.
- Die Authentifizierungsrichtlinie muss an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden sein, andernfalls funktioniert der Flow nicht wie vorgesehen.
- Sie haben folgende Artikel im Zusammenhang mit nFactor
  - XML-Schema
  - JavaScript
  - Aktionen zur Authentifizierung
  - Virtueller Authentifizierungsserver
  - NetScaler Version 11.1 und höher

Anmeldebeschriftungen anpassen

Um Anmeldebeschriftungen anzupassen, benötigen Sie Folgendes:

- Das XML-Schema, das beschreibt, wie die Anmeldeseite aussieht.
- Die Datei script.js, die das JavaScript enthält, das verwendet wird, um den Rendering-Prozess zu ändern.

> **Hinweis:**
>
> Die Datei script.js befindet sich im Verzeichnis /var/netscaler/logon/themes/<custom_theme>/.

Funktionsweise

Das JavaScript analysiert die XML-Datei und rendert jedes Element innerhalb des <Requirements>-Tags. Jedes Element entspricht einer Zeile im HTML-Formular. Zum Beispiel ist ein Anmeldefeld eine Zeile, das Kennwortfeld ist eine weitere Zeile, ebenso wie die Anmeldeschaltfläche. Um neue Zeilen einzuführen, müssen Sie sie mithilfe des StoreFront-SDK in der XML-Schemadatei angeben. Das StoreFront-SDK ermöglicht es der Anmeldeseite mit einem XML-Schema, das <Requirement>-Tag zu verwenden und Elemente darauf zu definieren. Diese Elemente ermöglichen die Verwendung von JavaScript, um in diesem Bereich alle benötigten HTML-Elemente einzuführen. In diesem Fall wird eine Zeile mit etwas Text in Form von HTML erstellt.

Das XML, das verwendet werden kann, lautet wie folgt:

```
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<!--NeedCopy-->
```

<Requirement>: Auf der Anmeldeseite bereitgestellter Speicherplatz. Der Berechtigungsnachweis füllt den Raum, und die anderen Teile leiten den Motor an die richtigen Informationen weiter. In diesem Fall geben Sie ein nsg-custom-cred. Dies ist als einfacher Text definiert und die Beschriftung ist für seinen Hauptteil definiert.
Die XML-Anforderung wird mit dem JavaScript-Code gekoppelt, um die erforderlichen Ergebnisse zu erzielen.

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {
```



```
8
9  return $("< Enter your HTML codes here>");
10  }
11  ,
12 // Instruction to parse the label as if it was a standard type
13 parseAsType: function () {
14
15 return "plain";
16  }
17
18  }
19  );
20 //Custom Credential Handler for Self Service Links
21 CTXS.ExtensionAPI.addCustomCredentialHandler({
22
23 getCredentialTypeName: function () {
24   return "nsg-custom-cred";  }
25  ,
26 getCredentialTypeMarkup: function (requirements) {
27
28 return $("<div/>");
29  }
30  ,
31  }
32  );
33 <!--NeedCopy-->
```

> **Wichtig:**
>
> Wenn Sie den HTML-Code hinzufügen, stellen Sie sicher, dass der Rückgabewert mit einem HTML-Tag beginnt.

Der XML-Teil gibt auf der Anmeldeseite an, was angezeigt werden soll, und der JavaScript-Code liefert den eigentlichen Text. Der Anmeldeinformationshandler öffnet den Raum und das Etikett füllt den Raum. Da der gesamte Authentifizierungsverkehr jetzt für das Umschreiben und den Responder unsichtbar ist, können Sie das Erscheinungsbild der Seite ändern.
Konfiguration zum Anpassen von Anmeldelab

1. Erstellen und binden Sie ein Thema basierend auf RFWeb.

```
1 add vpn portaltheme RfWebUI_MOD -basetheme RfWebUI
2
3 bind vpn vserver TESTAAA  - portaltheme RfWebUI_MOD
4 <!--NeedCopy-->
```


Der Pfad für die auf dem Thema basierenden Dateien ist im Verzeichnis verfügbar; /var/netscaler/logon/themes/RfWebUI_MOD

2. Fügen Sie am Ende der Datei script.js das folgende Snippet hinzu:

> **Hinweis:**
>
> Wenn die vorherigen Zeilen nicht in die richtige Datei aufgenommen werden, oder wenn keine JavaScript-Funktionen enthalten sind, kann das XML nicht geladen werden. Der Fehler kann nur in der Entwicklerkonsole des Browsers mit dem folgenden Text angezeigt werden: “Undefinierter Typ `nsg-custom-cred`.”

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
  return "nsg-custom-label";  }
 ,
getLabelTypeMarkup: function (requirements) {

return $("<a href="https://identity.test.com/identity/faces/
   register" style="font-size: 16px;" style="text-align: center;">
   Self Registration</a><br><a href="https://identity.test.com/
   identity/faces/forgotpassword" style="font-size: 16px;" style="
   text-align: center;">Forgot Password</a><br><a href="https://
   identity.test.com/identity/faces/forgotuserlogin" style="font-
   size: 16px;" style="text-align: center;">Forgot User Login</a
   >");
 }
 ,
// Instruction to parse the label as if it was a standard type
parseAsType: function () {

return "plain";
 }

 }
 );
//Custom Credential Handler for Self Service Links
CTXS.ExtensionAPI.addCustomCredentialHandler({

getCredentialTypeName: function () {
  return "nsg-custom-cred";  }
 ,
getCredentialTypeMarkup: function (requirements) {

```



```
return $("<div/>");
 }
 ,
 }
 );
<!--NeedCopy-->
```

> **Wichtig:**
>
> Wenn Sie den HTML-Code hinzufügen, stellen Sie sicher, dass der Rückgabewert mit einem HTML-Tag beginnt.

In diesem Beispiel verwendetes Anmeldeschema

```
<?xml version="1.0" encoding="utf-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext/>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/Citrix/Authentication/ExplicitForms/CancelAuthenticate</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement>
<Credential>
<ID>login</ID>
<SaveID>Username</SaveID>
<Type>username</Type>
</Credential>
<Label>
<Text>User name</Text>
<Type>plain</Type>
</Label>
<Input>
<AssistiveText>Please supply either domain\username or user@fully.qualified.domain</AssistiveText>
<Text>
<Secret>false</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue></InitialValue>
<Constraint>.+</Constraint>
```



```
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<ID>passwd</ID>
<SaveID>Password</SaveID>
<Type>password</Type>
</Credential>
<Label>
<Text>Password:</Text>
<Type>plain</Type>
</Label>
<Input>
<Text>
<Secret>true</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue/>
<Constraint>.+</Constraint>
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<Requirement>
<Credential>
<ID>loginBtn</ID>
<Type>none</Type>
</Credential>
<Label>
<Type>none</Type>
</Label>
<Input>
<Button>Please Log On</Button>
</Input>
</Requirement>
</Requirements>
</AuthenticationRequirements>
```



```
</AuthenticateResponse>
<!--NeedCopy-->
```

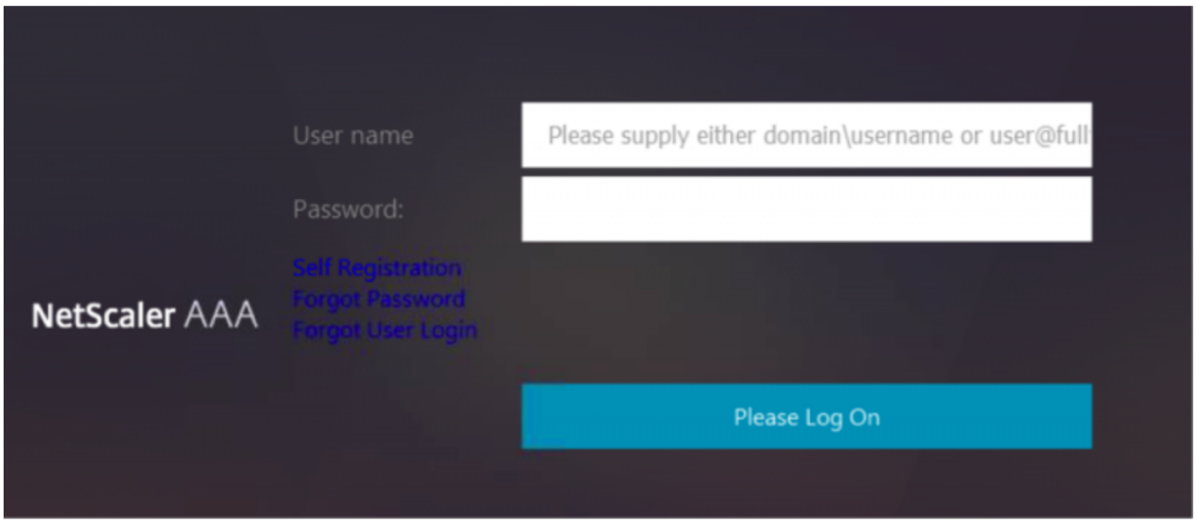
Führen Sie die folgenden Befehle aus, um das benutzerdefinierte Schema in die Konfiguration zu laden.

```
add authentication loginSchema custom -authenticationSchema custom.xml

add authentication loginSchemaPolicy custom -rule true -action custom

bind authentication vserver AAATEST -policy custom -priority 100 -
    gotoPriorityExpression END
<!--NeedCopy-->
```

In der folgenden Abbildung wird die Anmeldeseite angezeigt, die mit dieser Konfiguration gerendert wird.



Benutzeroberfläche anpassen, um Images anzuzeigen

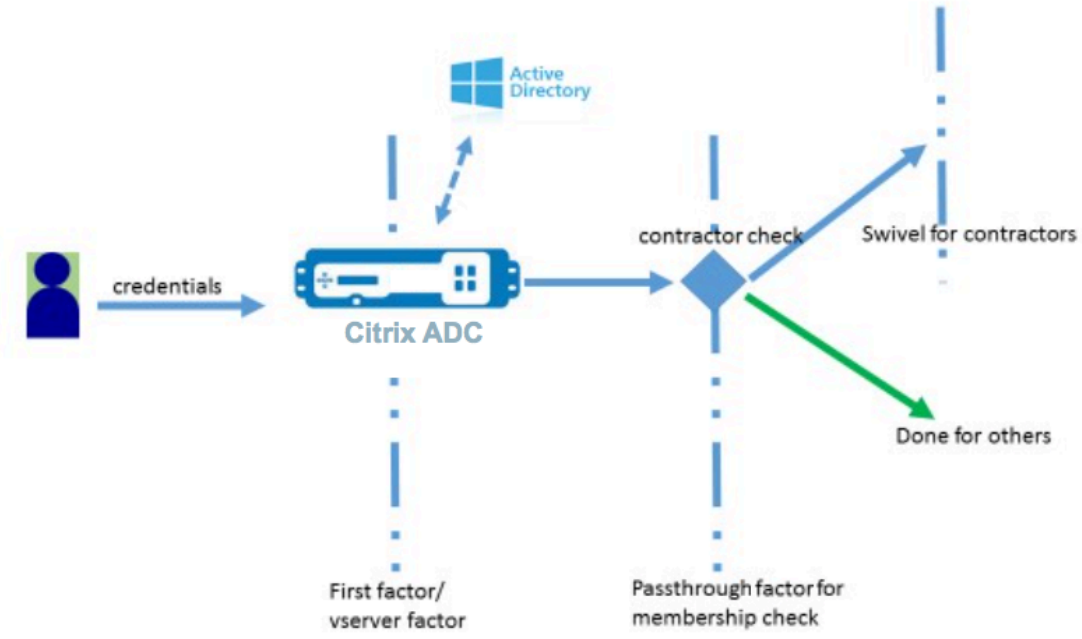
nFactor ermöglicht eine benutzerdefinierte Anzeige mithilfe von Anmeldeschemadateien. Möglicherweise sind weitere Anpassungen erforderlich, die nicht in den integrierten Anmeldeschemadateien angeboten werden. Zum Beispiel das Anzeigen eines Hyperlinks oder das Schreiben einer benutzerdefinierten Logik in der Benutzeroberfläche. Diese können mithilfe von "benutzerdefinierten Anmeldeinformationen" erreicht werden, die die Erweiterung des Anmeldeschemas und die entsprechende Javascript-Datei umfassen.

Anmeldeschemadateien befinden sich im Verzeichnis `/nsconfig/loginschema/LoginSchema`.

Für die Benutzeroberflächenanpassung zur Anzeige von Images wird ein Bereitstellungsablauf in der Integration "NetScaler-Swivel" als Beispiel verwendet.

Dieser Ablauf hat zwei Faktoren.

- Erster Faktor: Überprüft die AD-Anmeldeinformationen des Benutzers.
- Zweiter Faktor: Aufforderung zur Benutzeranmeldung basierend auf der Gruppenzugehörigkeit.



In diesem Ablauf durchlaufen alle Benutzer den ersten Faktor. Vor dem zweiten Faktor gibt es einen Pseudofaktor, um zu überprüfen, ob einige Benutzer im “Swivel” -Faktor weggelassen werden können. Wenn der Benutzer den “Swivel” -Faktor benötigt, werden ein Bild und ein Textfeld angezeigt, um den Code einzugeben.

Lösung

Die Lösung zum Anpassen der Benutzeroberfläche für die Anzeige von Bildern besteht aus zwei Teilen.

- Erweiterung des Anmeldeschemas
- Benutzerdefiniertes Skript zur Verarbeitung der Anmeldeschemaerweiterung.

Erweiterung des Anmeldeschemas

Um das Rendern von Formularen zu steuern, wird eine benutzerdefinierte “ID” /” Berechtigungsnachweis” in das Anmeldeschema eingefügt. Dies kann erreicht werden, indem das vorhandene Schema wiederverwendet und gemäß der Anforderung geändert wird.

In diesem Beispiel wird ein Anmeldeschema mit nur einem Textfeld (z. B. /nsconfig/loginschema/LoginSchema/OnlyPassword.xml) berücksichtigt.
Das folgende Snippet wurde dem Anmeldeschema hinzugefügt.


```
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><
   Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<!--NeedCopy-->
```

Im Snippet wird “swivel_cred” als “Typ” des Berechtigungsnachweises angegeben. Da dies nicht als integrierter “Berechtigungsnachweis” erkannt wird, sucht die Benutzeroberfläche nach einem Handler für diesen Typ und ruft ihn auf, falls er vorhanden ist.
Für diese Anmeldeinformationen wird ein Anfangswert gesendet, bei dem es sich um einen Ausdruck handelt, den NetScaler dynamisch ausfüllt. Im Beispiel ist es der Name des Benutzers, der verwendet wird, um den Swivel-Server über den Benutzernamen zu informieren. Es wird möglicherweise nicht ständig benötigt oder kann mit einigen anderen Daten ergänzt werden. Diese Angaben müssen nach Bedarf hinzugefügt werden.

Javascript zur Verarbeitung von benutzerdefinierten Anmeldeinformationen

Wenn die UI benutzerdefinierte Anmeldeinformationen findet, sucht sie nach einem Handler. Alle benutzerdefinierten Handler sind in /var/netscaler/logon/LogonPoint/custom/script.js für das Standardportaldesign geschrieben.

Für die benutzerdefinierten Portal-Themen befindet sich script.js im Verzeichnis /var/netscaler/logon/themes/<custom_theme>/.

Das folgende Skript wurde hinzugefügt, um Markup für benutzerdefinierte Anmeldeinformationen zu rendern.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
  return "swivel_cred";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        var image = $("<img/>");
        var username = requirements.input.text.initialValue; //Get the
           secret from the response
        image.attr({

```



```
15              "style" : "width:200px;height:200px;",
16              "id" : "qrcodeimg",
17              "<Enter your server URL here>"
18           }
19  );
20          div.append(image);
21          return div;
22       }
23
24  }
25  );
26 <!--NeedCopy-->
```

Dieses Snippet dient zur Behandlung des Markups für “swivel_cred”. Der hervorgehobene Anmeldeinformationsname muss mit dem zuvor in der Anmeldeschemaerweiterung angegebenen ‘Typ’ übereinstimmen.
Um Markup zu generieren, muss ein Bild hinzugefügt werden, dessen Quelle auf den Swivel-Server zeigt. Sobald dies erledigt ist, lädt die UI das Bild vom angegebenen Ort. Da dieses Anmeldeschema auch über ein Textfeld verfügt, rendert die Benutzeroberfläche dieses Textfeld.

> **Hinweis:**
>
> Der Administrator kann den “Stil” des Bildelements ändern, um die Größe des Bilds zu ändern. Derzeit ist es für 200x200 Pixel konfiguriert.

Konfiguration zum Anpassen der Benutzeroberfläche zur Anzeige von Bildern

Die nFactor-Konfiguration ist besser von unten nach oben aufgebaut, das ist der letzte Faktor zuerst, denn wenn Sie versuchen, ‘nextFactor’ für die vorherigen Faktoren anzugeben, benötigen Sie den Namen des nachfolgenden Faktors.

Konfiguration des Schwenkfaktors:

```
1 add loginschema swivel_image  -authenticationSchema /nsconfig/
     loginschema/SwivelImage.xml
2
3 add authentication policylabel SwivelFactor  -loginSchema swivel_image
4
5 bind authentication policylabel SwivelFactor  -policy <policy-to-check-
     swivel-image> -priority 10
6 <!--NeedCopy-->
```


> **Hinweis:**
>
> Laden Sie SwivelImage.xml aus dem im Beispiel verwendeten Anmeldeschema herunter.

Pseudofaktor für die Konfiguration der Gruppenprüfung:

```
add authentication policylabel GroupCheckFactor

add authentication policy contractors_auth_policy -rule 'http.req.user.is_member_of( "contractors" )' -action NO_AUTHN

add authentication policy not_contractors _auth_policy -rule true -action NO_AUTHN

bind authentication policylabel GroupCheckFactor -policy contractors_auth_policy -pri 10 -nextFactor SwivelFactor

bind authentication policylabel GroupCheckFactor -policy not_contractors_auth_policy -pri 20
<!--NeedCopy-->
```

Erster Faktor für die Active Directory-Anmeldung:

```
add ldapAction <>

add authentication policy user_login_auth_policy -rule true -action <>

bind authentication vserver <> -policy user_login_auth_policy -pri 10 -nextFactor GroupCheckFactor
<!--NeedCopy-->
```

In der Konfiguration werden drei Faktoren angegeben, von denen einer implizit/pseudo ist.

In diesem Beispiel verwendetes Anmeldeschema

Das Folgende ist ein Beispielschema mit Swivel-Anmeldeinformationen und einem Textfeld.

> **Hinweis:**
>
> Beim Kopieren von Daten für einen Webbrowser werden Angebote möglicherweise anders angezeigt. Kopieren Sie Daten in Editoren wie Notepad, bevor Sie sie in Dateien speichern.

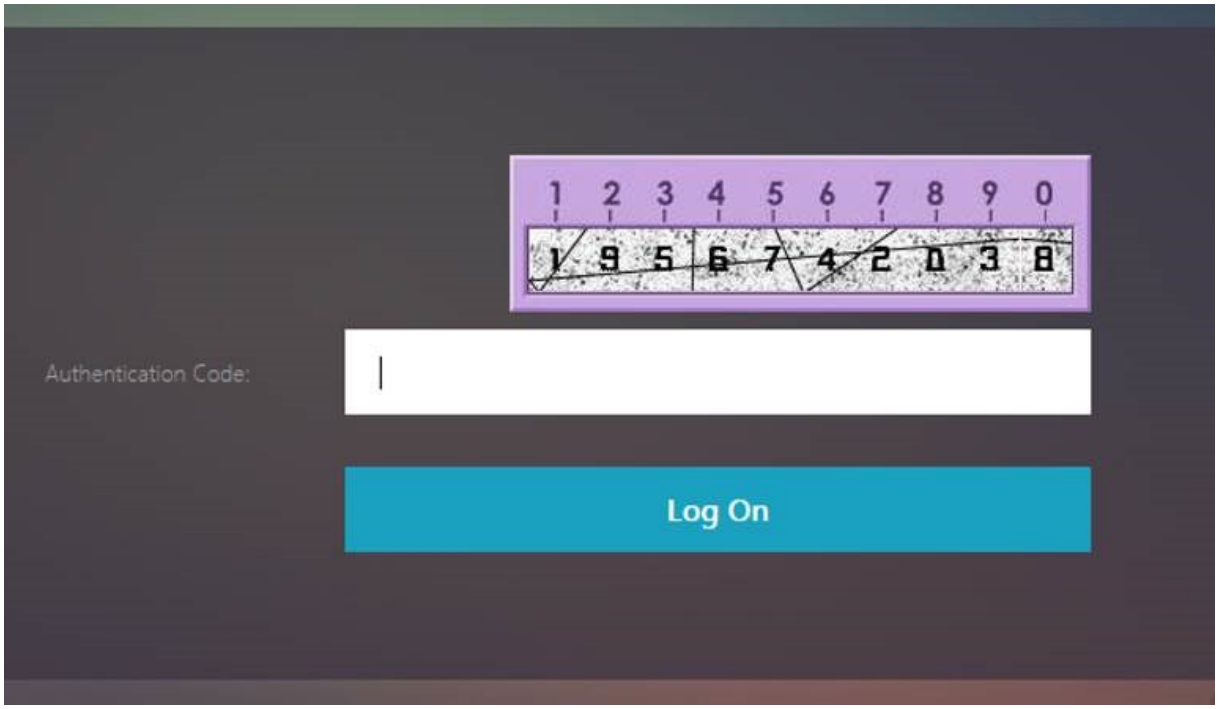
```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
```



```
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>Hello ${
 http.req.user.name }
 , Please enter passcode from above image.</Text><Type>confirmation</Type></Label><Input /></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>Remember my password</Text><Type>plain</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>Log On</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Ausgabe

Sobald die Konfiguration durchgeführt wurde, wird das folgende Bild angezeigt.



> **Hinweis:**
>
> Bildhöhe und -platzierung können im JavaScript geändert werden.

Anpassen des NetScaler nFactor-Anmeldeformulars, um Felder ein- oder auszublenden

Die RFWeb UI von NetScaler Gateway ermöglicht eine Vielzahl von Anpassungen. Diese Funktion in Kombination mit dem nFactor-Authentifizierungsframework ermöglicht es Kunden, komplexe Abläufe zu konfigurieren, ohne bestehende Workflows zu beeinträchtigen.

In diesem Beispiel sind zwei Authentifizierungsoptionen, OAuth und LDAP, in der Liste Anmeldetyp verfügbar. Wenn das Formular zum ersten Mal geladen wird, werden die Felder Benutzername und Kennwort (LDAP wird zuerst angezeigt) angezeigt. Wenn OAuth ausgewählt ist, werden alle Felder ausgeblendet, da OAuth eine Auslagerung der Authentifizierung an einen Drittanbieterserver impliziert. Auf diese Weise kann ein Administrator intuitive Workflows gemäß Benutzerkomfort konfigurieren.

> **Hinweis:**
>
> - Die Werte in der Liste Anmeldetyp können mit einfachen Änderungen an der Skriptdatei geändert werden.
> - In diesem Abschnitt wird nur der UI-Teil des Flows beschrieben. Die Laufzeitbehandlung der Authentifizierung liegt außerhalb des Geltungsbereichs dieses Artikels. Benutzern wird empfohlen, die nFactor-Dokumentation zur Authentifizierungskonfiguration zu lesen.

So passen Sie das nFactor-Anmeldeformular an

Das Anpassen des nFactor-Anmeldeformulars kann in zwei Teile unterteilt werden.

- Das richtige Anmeldeschema an die Benutzeroberfläche senden
- Schreiben eines Handlers zur Interpretation des Anmeldeschemas und der Benutzerauswahl

Senden Sie das richtige Anmeldeschema an die UI

In diesem Beispiel wird ein einfacher Anspruch/Anforderung im Anmeldeschema gesendet.

Dazu wird die Datei SingleAuth.xml geändert. Die SingleAuth.xml wird mit NetScaler-Firmware geliefert und ist im Verzeichnis `/nsconfig/loginschema/LoginSchema`.

Schritte zum Senden des Anmeldeschemas:

1. Melden Sie sich über SSH an und legen Sie auf die Shell (Typ “Shell”).
2. Kopieren Sie SingleAuth.xml zur Änderung in eine andere Datei.

   > **Hinweis:**
   >
   > Der Zielordner unterscheidet sich vom standardmäßigen NetScaler-Anmeldeschema-Ordner.
   >
   > cp /nsconfig/loginschema/LoginSchema/SingleAuth.xml /nsconfig/loginschema/SingleAuthDynamic.xml

3. Fügen Sie den folgenden Anspruch zu SingleAuthDynamic.xml hinzu.

```
<Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></Label></Requirement>
<!--NeedCopy-->
```

4. Konfigurieren Sie NetScaler so, dass dieses Anmeldeschema zum Laden des ersten Formulars gesendet wird.

```
add loginschema single_auth_dynamic -authenticationSchema SingleAuthDynamic.xml

add loginschemaPolicy single_auth_dynamic -rule true -action single_auth_dynamic

bind authentication vserver aaa_nfactor -policy single_auth_dynamic -pri 10
<!--NeedCopy-->
```


Änderungen an Skripten zum Laden von Formularen und zur Behandlung

Sie können das JavaScript ändern, das es einem Administrator ermöglicht, die Anzeige für das Anmeldeformular anzupassen. In diesem Beispiel werden der Benutzername und das Kennwortfeld angezeigt, wenn LDAP ausgewählt ist, und werden ausgeblendet, wenn OAuth ausgewählt ist. Der Administrator kann auch nur das Kennwort verbergen.

Administratoren müssen das folgende Snippet an “script.js” anhängen, das im Verzeichnis “/var/netscaler/logon/LogonPoint/custom” ist.

> **Hinweis:**
>
> Da es sich bei diesem Verzeichnis um ein globales Verzeichnis handelt, erstellen Sie ein Portaldesign und bearbeiten Sie die Datei “script.js” in diesem Ordner unter `"/var/netscaler/logon/themes/<THEME_NAME>"`.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
  return "nsg_dropdown";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        var select = $("<select name='nsg_dropdown'></select>").attr("
           id", "nsg_dropdown");

        var rsa = $("<option></option>").attr("selected", "selected").
           text("LDAP").val("LDAP");
        var OAuthID = $("<option></option>").text("OAuth").val("OAuth")
           ;
        select.append(rsa, OAuthID);

        select.change(function(e) {

            var value = $(this).val();
            var ldapPwd = $($(".credentialform").find(".
               CredentialTypepassword")[0]);
            var ldapUname = $($(".credentialform").find(".
               CredentialTypeusername"));
            if(value == "OAuth") {

                if (ldapPwd.length)
```



```
                        ldapPwd.hide();
                if (ldapUname.length)
                        ldapUname.hide();
            }
   else if(value == "LDAP") {

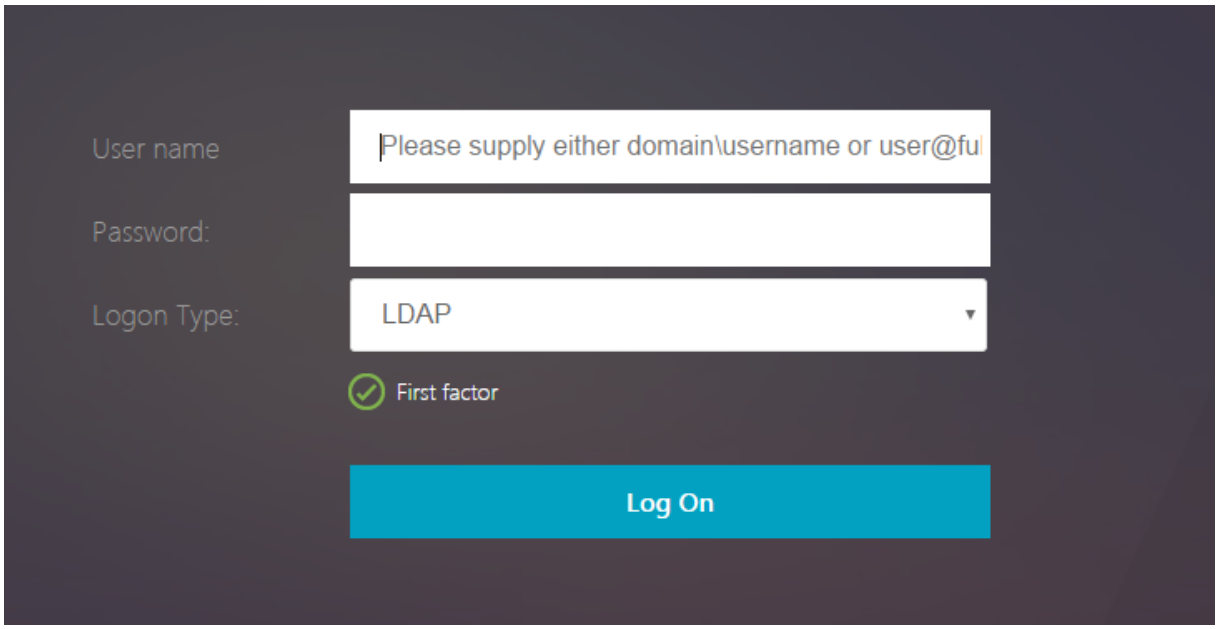
                if (ldapPwd.length)
                        ldapPwd.show();
                if (ldapUname.length)
                        ldapUname.show();
            }

          }
 );
       div.append(select);
        return div;
     }

 }
 );
<!--NeedCopy-->
```

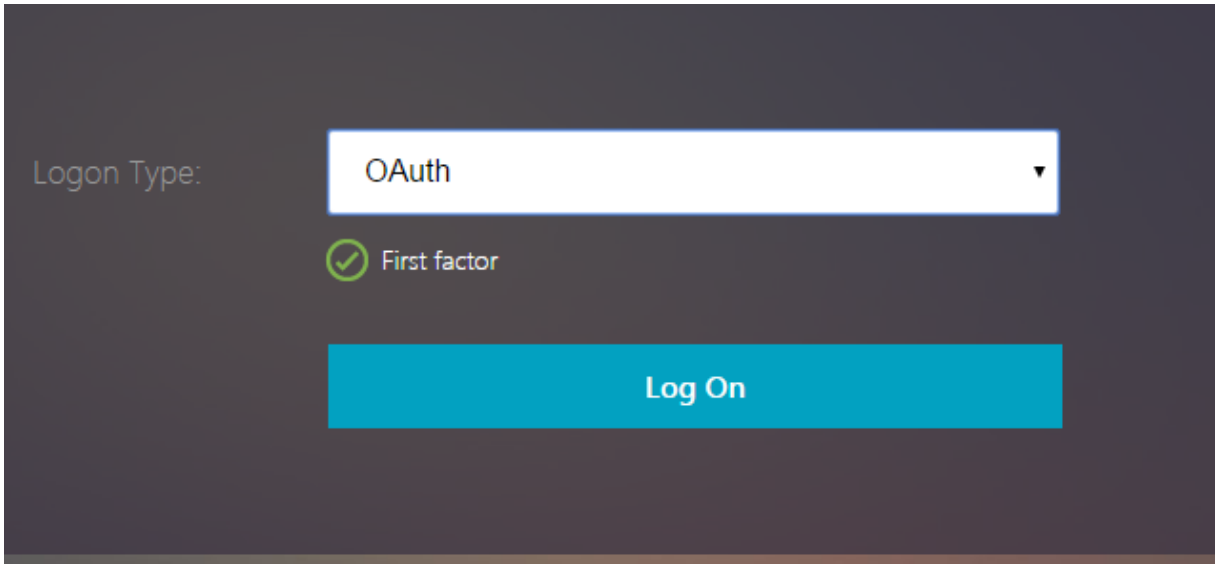
Erfahrung für Endbenutzer

Wenn ein Endbenutzer die Anmeldeseite zum ersten Mal lädt, wird der folgende Bildschirm angezeigt.



Wenn **OAuth** in **Anmeldetyp**ausgewählt ist, werden die Felder Benutzername und Kennwort ausge-

blendet.



Wenn **LDAP** ausgewählt ist, werden Benutzername und Kennwort angezeigt. Auf diese Weise kann die Anmeldeseite basierend auf der Benutzerauswahl dynamisch geladen werden.

In diesem Beispiel verwendetes Anmeldeschema

```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>User name</Text><Type>plain</Type></Label><Input><AssistiveText>Please supply either domain\username or user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint
```



```
      >.+</Constraint></Text></Input></Requirement>
13 <Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type
      ></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></
      Label></Requirement>
14 <Requirement><Credential><Type>none</Type></Credential><Label><Text>
      First factor</Text><Type>confirmation</Type></Label><Input /></
      Requirement>
15 <Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials
      </Type></Credential><Label><Text>Remember my password</Text><Type>
      plain</Type></Label><Input><CheckBox><InitialValue>false</
      InitialValue></CheckBox></Input></Requirement>
16 <Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential
      ><Label><Type>none</Type></Label><Input><Button>Log On</Button></
      Input></Requirement>
17 </Requirements>
18 </AuthenticationRequirements>
19 </AuthenticateResponse>
20 <!--NeedCopy-->
```

Hinweis:

Weitere Informationen zu verschiedenen nFactor-bezogenen Themen finden Sie unter nFactor-Authentifizierung.

Setzen eines Cookies mit nFactor

May 11, 2023

Sie können die benutzerdefinierten nFactor-Labels anwenden und ein Cookie als Faktor des Authentifizierungsflusses festlegen. Durch benutzerdefinierte Labels können Sie JavaScript verwenden, um das Anmeldeschema zu manipulieren.

Um ein Cookie als Faktor festzulegen, müssen Sie dem Benutzer keine Informationen anzeigen, die ohne Schema-Anmeldung ausgeführt werden. Stattdessen müssen Sie mit dem Browser des Benutzers interagieren, um das Anmeldeschema anzuweisen, die gewünschten Daten zu speichern. Ein Anmeldeschema ist erforderlich, um das Cookie zu setzen, wenn die Seite geladen wird. Das Cookie wird mit einem benutzerdefinierten Label und JavaScript-Code gesetzt.

Um einen Faktor zu implementieren, der ein Cookie setzt, erstellen Sie eine XML-Datei mit dem Namen cookie.xml, um das Schema im Verzeichnis /nsconfig/loginschema/ mit folgendem Inhalt zu speichern:

```
1 <?xml version="1.0" encoding="UTF-8"?>
```



```
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>

<Requirement>
<Credential><ID>nsg_cookie</ID><Type>nsg_cookie</Type></Credential>
<Label><Text>Logon Type:</Text><Type>Plain</Type></Label>
</Requirement>

<Requirement>
<Credential><ID>loginBtn</ID><Type>none</Type></Credential>
<Label><Type>none</Type></Label><Input><Button>Log On</Button></Input>
</Requirement>

</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

In diesem XML;

- Das benutzerdefinierte Label nsg_cookie wird verwendet, um das Cookie zu erstellen und das Formular sowie die Formularschaltfläche abzusenden.
- Das RFWebUI_Custom ist das neue Portal-Thema, das auf dem RFWebUI-Thema basiert.

Schritte zum Setzen eines Cookie mit nFactor

1. Erstellen Sie ein Portal-Thema basierend auf dem RFWebUI-Thema.

   ```
   add vpn portaltheme RfWebUI_custom -basetheme RfWebUI
   <!--NeedCopy-->
   ```

   Dieser Befehl erstellt einen Ordner für dieses Thema unter /var/netscaler/logon/themes/RfWebUI_Custom

2. Bearbeiten Sie die Datei /var/netscaler/logon/themes/RfWebUI_custom/script.js und fügen Sie das folgende Skript hinzu:


```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by
        the server
    getCredentialTypeName: function () {
  return "nsg_cookie";  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $("<div></div>");
        $(document).ready(function() {

        //Set cookie valid for 1000 days
        var exdays = 1000;
        var d = new Date();
        d.setTime(d.getTime() + (exdays\*24\*60\*60\*1000));
        var expires = "expires="+ d.toUTCString();
        document.cookie = "NSC_COOKIE_NAME=CookieValue;" + expires
            + ";path=/";

        //Submit form
        document.getElementById('loginBtn').click();
         }
 );
        return div;
     }

 }
 );
<!--NeedCopy-->
```

Dieser Code führt Folgendes aus:

- Wartet darauf, dass der Browser das Laden der Seite abgeschlossen hat
- Setzt ein Cookie namens NSC_COOKIE_NAME mit dem Wert CookieValue, gültig für 1000 Tage
- Sendet das Formular automatisch.

Das Cookie wird erstellt und der Benutzer muss nicht mit der Seite interagieren.

3. Erstellen Sie ein Anmeldeschema, das an die Policy Label gebunden wird, die den festgelegten Cookie-Faktor darstellt


```
add authentication loginSchema Cookie_LS -authenticationSchema "/
    nsconfig/loginschema/cookie.xml"
<!--NeedCopy-->
```

4. Erstellen Sie eine NO_AUTHN-Authentifizierungsrichtlinie, um sie an die Policy Label zu binden, die den festgelegten Cookie-Faktor darstellt.

```
add authentication Policy NO_AUTHN_POL -rule TRUE -action NO_AUTHN
<!--NeedCopy-->
```

   Diese Richtlinie wird immer als wahr ausgewertet und führt den Benutzer zum nächsten Faktor oder schließt den Authentifizierungsablauf ab.

5. Binden Sie das Portaldesign RFWebUI_Custom an den virtuellen NetScaler Gateway -Server oder den virtuellen NetScaler AAA-Server.

Beispielbereitstellungen mit nFactor-Authentifizierung

June 2, 2023

Im Folgenden sind die Beispielbereitstellungen mit nFactor-Authentifizierung aufgeführt:

- Zwei Kennwörter im Voraus erhalten, Passthrough im nächsten Faktor. Read
- Gruppenextraktion gefolgt von Zertifikat- oder LDAP-Authentifizierung, basierend auf der Gruppenmitgliedschaft. Read
- SAML gefolgt von LDAP- oder Zertifikatauthentifizierung, basierend auf Attributen, die während SAML extrahiert wurden Read
- SAML im ersten Faktor, gefolgt von Gruppenextraktion und dann LDAP- oder Zertifikatauthentifizierung, basierend auf extrahierten Gruppen. Read
- Vorfüllen des Benutzernamens aus dem Zertifikat. Read
- Zertifikatauthentifizierung gefolgt von Gruppenextraktion für 401 virtuelle Server mit aktiviertem Verkehrsmanagement. Read
- Benutzername und zwei Kennwörter mit Gruppenextraktion im dritten Faktor. Read
- Fallback von Zertifikaten auf LDAP in derselben Kaskade; ein virtueller Server für Zertifikat- und LDAP-Authentifizierung. Read
- LDAP im ersten Faktor und WebAuth im zweiten Faktor. Read
- Domänen-Dropdown im ersten Faktor, dann verschiedene Policy-Bewertungen basierend auf der Gruppe. Read
- Konfigurieren Sie die auf der E-Mail-ID (oder dem Benutzernamen) basierende Gruppenextraktion als ersten Faktor, um den Authentifizierungsablauf des nächsten Faktors zu bestimmen. Read

Wie macht man

May 11, 2023

Die Authentifizierung, Autorisierung und Prüfung von “How to Articles” sind einfache, relevante und leicht zu implementierende Artikel. Diese Artikel enthalten Informationen zu einigen der gängigen Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen wie LDAP-Authentifizierung und Multifaktor-Authentifizierung. Einige der beliebten Artikel zur Konfiguration und Fehlerbehebung bei der Authentifizierung über NetScaler finden Sie unter NetScaler Authentication: Wie mache ich?

Endpunktanalyse

Konfigurieren des Endpoint Analysis-Scans vor der Authentifizierung als Faktor bei der nFactor-Authentifizierung

Konfigurieren des Endpoint Analysis-Scans nach der Authentifizierung als Faktor bei der NetScaler nFactor-Authentifizierung

Konfigurieren Sie den EPA-Scan vor und nach der Authentifizierung als Faktor bei der nFactor-Authentifizierung

Konfigurieren des regelmäßigen Endpoint Analysis-Scans als Faktor bei der nFactor-Authentifizierung

Konfigurieren von NetScaler Gateway Vorauthentifizierung EPA-Scan für die Domänenprüfung

Konfigurationskombinationen aus erster Faktor und zweiter Faktor

Konfigurieren Sie nFactor für NetScaler Gateway mit WebAuth im ersten Faktor und LDAP mit Kennwortänderung im zweiten Faktor

Konfigurieren von SAML gefolgt von LDAP oder Zertifikatauthentifizierung basierend auf SAML-Attributextraktion in der nFactor-Authentifizierung

Konfigurieren Sie die Zertifikatauthentifizierung als ersten Faktor und LDAP als zweiten Faktor bei der NetScaler nFactor-Authentifizierung

Konfigurieren Sie die Zwei-Faktor-Authentifizierung mit einem Anmeldeschema und einem Passthrough-Schema in der NetScaler nFactor-Authentifizierung

Konfigurieren von Benutzernamen und zwei Kennwörtern mit Gruppenextraktion im dritten Faktor durch nFactor-Authentifizierung

Konfigurieren Sie das Dropdownmenü für Domäne, Benutzername und Kennwort in der ersten Faktor- und Richtlinienbewertung basierend auf Gruppen im nächsten Faktor

Konfigurieren Sie die eingabebasierte Gruppenextraktion der E-Mail-ID (oder des Benutzernamens) beim ersten Faktor, um den nächsten Faktor-Authentifizierungsablauf zu entscheiden

Konfigurieren Sie eine Domänen-Dropdownliste für Benutzereingaben im ersten Faktor, um den nächsten Faktor-Authentifizierungsablauf zu entscheiden

EULA als Authentifizierungsfaktor

Konfigurieren Sie EULA als Authentifizierungsfaktor im NetScaler nFactor-System

Füllen Sie den Benutzernamen aus dem Zertifikat

Konfigurieren Sie den Benutzernamen für das Vorfüllen aus dem Zertifikat in der NetScaler nFactor-Authentifizierung

Step-up-Authentifizierung

Konfiguration von nFactor für Anwendungen mit unterschiedlichen Anforderungen an Anmeldeseiten, einschließlich Step-up-Authentifizierung

SAML-Authentifizierung

May 11, 2023

Security Assertion Markup Language (SAML) ist ein XML-basierter Authentifizierungsmechanismus, der Single Sign-On-Funktion bietet und vom OASIS Security Services Technical Committee definiert wurde.

> Hinweis
>
> Ab NetScaler 12.0 Build 51.x füllt die NetScaler-Appliance, die als SAML Service Provider (SP) mit Multi-Factor (nFactor) -Authentifizierung verwendet wird, jetzt das Benutzernamenfeld auf der Anmeldeseite vorab aus. Die Appliance sendet ein NameID-Attribut als Teil einer SAML-Autorisierungsanfrage, ruft den NameID-Attributwert vom NetScaler SAML Identity Provider (IdP) ab und füllt das Benutzernamenfeld vorab aus.

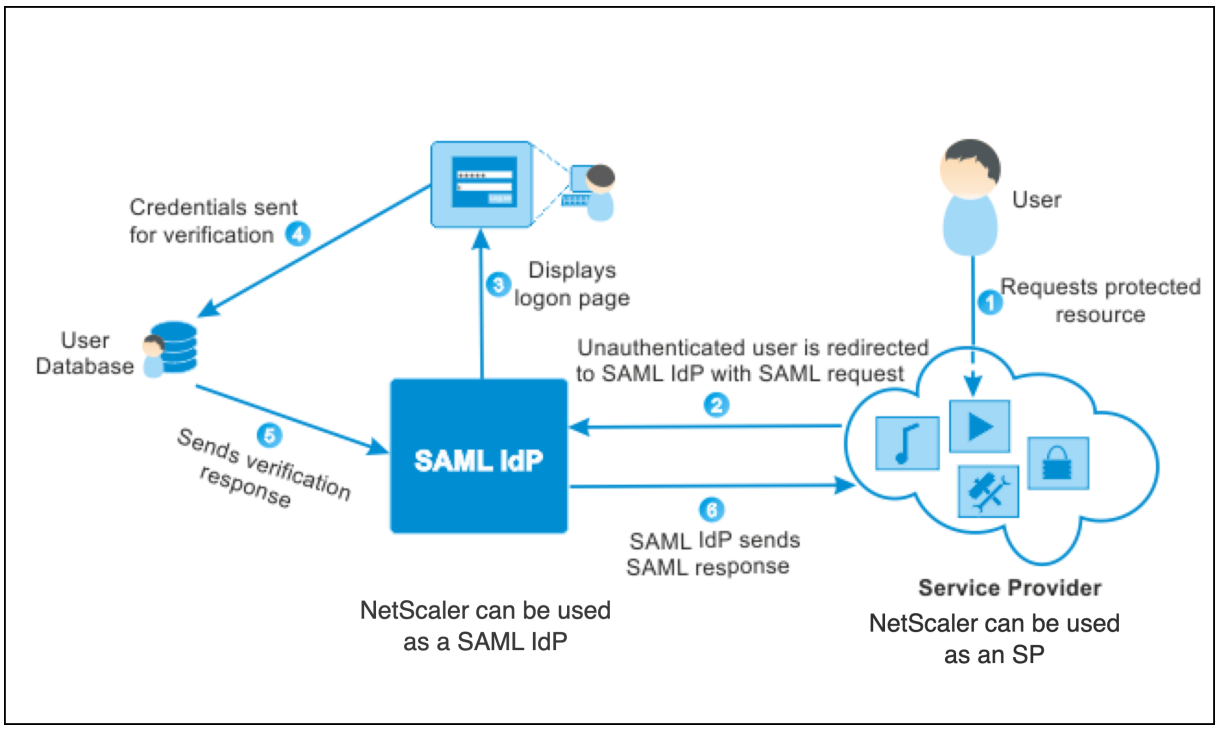
Warum sollten Sie die SAML-Authentifizierung verwenden

Stellen Sie sich ein Szenario vor, in dem ein Dienstanbieter (LargeProvider) eine Reihe von Anwendungen für einen Kunden hostet (BigCompany). BigCompany hat Benutzer, die nahtlos auf diese Anwendungen zugreifen müssen. In einem herkömmlichen Setup müsste LargeProvider eine Datenbank mit

Benutzern von BigCompany verwalten. Dies wirft bei jedem der folgenden Interessenvertreter einige Bedenken auf:

- LargeProvider muss die Sicherheit der Benutzerdaten gewährleisten.
- BigCompany muss die Benutzer validieren und die Benutzerdaten auf dem neuesten Stand halten, nicht nur in seiner eigenen Datenbank, sondern auch in der von LargeProvider verwalteten Benutzerdatenbank. Beispielsweise muss ein Benutzer, der aus der BigCompany-Datenbank entfernt wurde, auch aus der LargeProvider-Datenbank entfernt werden.
- Ein Benutzer muss sich bei jeder der gehosteten Anwendungen einzeln anmelden.

Der SAML-Authentifizierungsmechanismus bietet einen alternativen Ansatz. Das folgende Verteilungsdiagramm zeigt, wie SAML funktioniert (SP-initiierter Flow).



Die Bedenken, die sich aus den traditionellen Authentifizierungsmechanismen ergeben, werden wie folgt ausgeräumt:

- LargeProvider muss keine Datenbank für BigCompany-Benutzer verwalten. Ohne Identitätsmanagement kann sich LargeProvider auf die Bereitstellung besserer Dienste konzentrieren.
- BigCompany trägt nicht die Last, sicherzustellen, dass die LargeProvider-Benutzerdatenbank mit der eigenen Benutzerdatenbank synchronisiert wird.
- Ein Benutzer kann sich einmal bei einer Anwendung anmelden, die auf LargeProvider gehostet wird, und automatisch bei den anderen Anwendungen angemeldet werden, die dort gehostet werden.

Die NetScaler-Appliance kann als SAML Service Provider (SP) und SAML Identity Provider (IdP) bereitgestellt werden. Lesen Sie sich die entsprechenden Themen durch, um zu verstehen, welche Konfig-

urationen auf der NetScaler-Appliance ausgeführt werden müssen.

Eine NetScaler-Appliance, die als SAML-Dienstanbieter konfiguriert ist, kann jetzt eine Überprüfung der Zielgruppeneinschränkung erzwingen. Die Bedingung zur Beschränkung der Zielgruppen wird nur dann als „Gültig“ bewertet, wenn der SAML-Antwortende Mitglied mindestens einer der angegebenen Zielgruppen ist.

Sie können eine NetScaler-Appliance so konfigurieren, dass sie Attribute in SAML-Assertionen als Gruppenattribute analysiert. Wenn Sie sie als Gruppenattribute analysieren, kann die Appliance Richtlinien an die Gruppen binden.

NetScaler als SAML SP

May 11, 2023

Der SAML-Dienstanbieter (SP) ist eine vom Dienstanbieter bereitgestellte SAML-Entität. Wenn ein Benutzer versucht, auf eine geschützte Anwendung zuzugreifen, wertet der SP die Clientanforderung aus. Wenn der Client nicht authentifiziert ist (kein gültiges NSC_TMAA- oder NSC_TMAS-Cookie hat), leitet der SP die Anfrage an den SAML-Identitätsanbieter (IdP) weiter.

Der SP validiert auch SAML-Assertions, die vom IdP empfangen werden.

Wenn die NetScaler Appliance als SP konfiguriert ist, empfängt ein virtueller Server für das Verkehrsmanagement (Load Balancing oder Content Switching) alle Benutzeranfragen, die der entsprechenden SAML-Aktion zugeordnet sind.

Die NetScaler-Appliance unterstützt auch POST- und Redirect-Bindungen beim Abmelden.

> **Hinweis**
>
> Eine NetScaler-Appliance kann als SAML-SP in einer Bereitstellung verwendet werden, in der der SAML-IdP entweder auf der Appliance oder auf einem externen SAML-IdP konfiguriert ist.

Bei Verwendung als SAML-SP gilt eine NetScaler-Appliance:

- Kann die Benutzerinformationen (Attribute) aus dem SAML-Token extrahieren. Diese Informationen können dann in den Richtlinien verwendet werden, die auf der NetScaler-Appliance konfiguriert sind. Wenn Sie beispielsweise die Attribute GroupMember und **emailaddress** extrahieren möchten, geben Sie in der SamlAction den Parameter **Attribute2** als GroupMember und den **Attribute3-Parameter** als **emailaddress an**.

  > **Hinweis**
  >
  > Standardattribute wie Benutzername, Kennwort und Abmelde-URL dürfen in den Attributen 1—16 nicht extrahiert werden, da sie implizit analysiert und in der Sitzung

> gespeichert werden.

- Kann Attributnamen von bis zu 127 Byte aus einer eingehenden SAML-Assertion extrahieren. Das vorherige Limit lag bei 63 Byte.
- Unterstützt Post-, Redirect- und Artifact-Bindungen.

  > **Hinweis**
  >
  > Verwenden Sie die Umleitungsbindung nicht für große Datenmengen, wenn die Assertion nach der Aufblähung oder Dekodierung größer als 10.000 ist.

- Kann Assertionen entschlüsseln.
- Kann mehrwertige Attribute aus einer SAML-Assertion extrahieren. Diese Attribute werden in Form von verschachtelten XML-Tags gesendet, wie zum Beispiel:

  <AttributeValue> <AttributeValue>Value1</AttributeValue>
  <AttributeValue>Value2</AttributeValue>
  \</AttributeValue\>

  > **Hinweis**
  >
  > Ab NetScaler 13.0 Build 63.x und höher wurde die individuelle maximale Länge für SAML-Attribute auf maximal 40.000 Byte erhöht. Die Größe aller Attribute darf 40.000 Byte nicht überschreiten.

  Bei Vorlage von vorherigem XML kann die NetScaler-Appliance sowohl Value1 als auch Value2 als Werte eines bestimmten Attributs extrahieren, im Gegensatz zur alten Firmware, die nur Value1 extrahiert.

- Kann die Gültigkeit einer SAML-Assertion angeben.

  Wenn die Systemzeit auf NetScaler SAML IdP und Peer-SAML-SP nicht synchron ist, werden die Nachrichten möglicherweise von beiden Parteien ungültig gemacht. Um solche Fälle zu vermeiden, können Sie jetzt die Zeitdauer festlegen, für die die Assertionen gültig sind.

  Diese Dauer, die als “Skew Time” bezeichnet wird, gibt die Anzahl der Minuten an, für die die Nachricht akzeptiert werden kann. Die Skew Time kann auf dem SAML-SP und dem SAML-IdP konfiguriert werden.

- Kann ein zusätzliches Attribut namens ‘ForceAuth’ in der Authentifizierungsanfrage an einen externen IdP (Identitätsanbieter) senden. Standardmäßig ist ForceAuthn auf “False” gesetzt. Es kann auf “True” gesetzt werden, um dem IdP vorzuschlagen, die Authentifizierung trotz des vorhandenen Authentifizierungskontextes zu erzwingen. Außerdem führt NetScaler SP eine Authentifizierungsanforderung im Abfrageparameter aus, wenn es mit Artefaktbindung konfiguriert ist.

Konfigurieren der NetScaler-Appliance als SAML SP mit der CLI

1. Konfigurieren Sie eine SAML SP-Aktion.

   Beispiel

   Mit dem folgenden Befehl wird eine SAML-Aktion hinzugefügt, die nicht authentifizierte Benutzeranforderungen umleitet.

   ```
   add authentication samlAction SamlSPAct1 -samlIdPCertName nssp -samlSigningCertNa
    nssp -samlRedirectUrl https://auth1.example.com -relaystateRule "AAA.
   LOGIN.RELAYSTATE.EQ(\"https://lb.example1.com/\")"
   ```

   Wichtige Hinweise

   - Das Zertifikat, das für `-samlIdPCertName` im samlAction-Befehl angegeben wurde, muss mit dem entsprechenden Zertifikat von IdP übereinstimmen, damit die Signaturüberprüfung erfolgreich ist.
   - SAML unterstützt nur das RSA-Zertifikat. Andere Zertifikate wie HSM und FIPS werden nicht unterstützt.
   - Es wird empfohlen, einen vollständigen Domainnamen mit einem abschließenden '/' im Ausdruck zu verwenden.
   - Administratoren müssen einen Ausdruck für **relaysStateRule** im Befehl samlAction konfigurieren. Der Ausdruck muss die Liste der veröffentlichten Domänen enthalten, mit denen der Benutzer eine Verbindung herstellt, bevor er zum virtuellen Authentifizierungsserver umgeleitet wird. Der Ausdruck muss beispielsweise die Domänen des virtuellen Front-End-Servers (VPN, LB oder CS) enthalten, die diese SAML-Aktion zur Authentifizierung verwenden.

   > **Hinweis:**
   >
   > Wenn es mehrere SAML-Richtlinien als Teil einer IdP-Kette gibt, reicht es aus, eine Relay-State-Regel nur für die erste SAML-Richtlinie zu konfigurieren.

   Weitere Informationen zum Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction und https://support.citrix.com/article/CTX316577.

2. Konfigurieren Sie die SAML-Richtlinie.

   Beispiel

   Der folgende Befehl definiert eine SAML-Richtlinie, die die zuvor definierte SAML-Aktion auf den gesamten Datenverkehr anwendet.

   ```
   add authentication policy SamlSPPol1 -rule true -action SamlSPAct1
   ```

3. Binden Sie die SAML-Richtlinie an den virtuellen Authentifizierungsserver.

Beispiel

Der folgende Befehl bindet die SAML-Richtlinie an einen virtuellen Authentifizierungsserver mit dem Namen “av_saml”.

```
bind authentication vserver av_saml -policy SamlSPPol1
```

4. Binden Sie den virtuellen Authentifizierungsserver an den entsprechenden virtuellen Server für das Verkehrsmanagement.

   Beispiel

   Der folgende Befehl fügt einen virtuellen Lastausgleichsserver mit dem Namen “lb1_ssl” hinzu und ordnet den virtuellen Authentifizierungsserver mit dem Namen “av_saml” dem virtuellen Lastausgleichsserver zu.

   ```
   add lb vserver lb1_ssl SSL 10.217.28.224 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost auth1.example.com -Authentication ON
    -authnVsName av_saml
   ```

   Weitere Informationen zu dem Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction

Konfigurieren einer NetScaler-Appliance als SAML SP mit der GUI

1. Navigieren Sie zu **Sicherheit>AAA-Richtlinien>Authentifizierung> Grundrichtlinien>SAML**.
2. Wählen Sie die Registerkarte **Server** aus, klicken Sie auf **Hinzufügen**, geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

   Parameter-Beschreibungen:

   - Name - Name des Servers.
   - Umleitungs-URL — URL, mit der sich Benutzer authentifizieren. Einige IdPs haben spezielle URLs, die nur erreichbar sind, wenn sie sich in einem SAML-Setup befinden.
   - Single Logout URL — URL, die angegeben wurde, damit der NetScaler erkennen kann, wann der Client zurück an den IdP gesendet werden muss, um den Abmeldevorgang abzuschließen. Wir werden es in dieser einfachen Bereitstellung nicht verwenden.
   - SAML-Bindung — Ein Mechanismus, der verwendet wird, um SAML-Requestor- und Responder-Nachrichten zwischen dem SP und IdP zu transportieren. Wenn NetScaler als SP fungiert, unterstützt es Post-, Redirect- und Artifact-Bindungen. Die Standard-bindungsmethode ist POST.

     > **Hinweis:**
     >
     > Für die Artefaktbindung muss der Transportmechanismus auf dem SP und dem IdP

> derselbe sein.

- Logout-Bindung — Gibt den Transportmechanismus von SAML-Abmeldenachrichten an. Der standardmäßige Bindungsmechanismus ist Post.
- IdP-Zertifikatsname — IdPCert-Zertifikat (Base64), das unter dem SAML-Signaturzertifikat vorhanden ist.
- Benutzerfeld — Abschnitt des SAML-Authentifizierungsformulars des IdP, der den Benutzernamen enthält, den SP bei Bedarf extrahieren kann.
- Signieren des Zertifikatsnamens - Wählen Sie das SAML SP-Zertifikat (mit privatem Schlüssel) aus, das NetScaler verwendet, um Authentifizierungsanforderungen an den IdP zu signieren. Das gleiche Zertifikat (ohne privaten Schlüssel) muss in den IdP importiert werden, damit der IdP die Signatur der Authentifizierungsanforderung überprüfen kann. Die meisten IdPs benötigen den Namen des Signaturzertifikats nicht.
- IssuerName — Identifier. Eindeutige ID, die sowohl auf dem SP als auch auf dem IdP angegeben ist, um den Dienstanbieter untereinander zu identifizieren.
- Unsignierte Assertion ablehnen — Option, die Sie angeben können, wenn die Assertions vom IdP signiert werden müssen. Die Standardeinstellung ist EIN.
  - ON: Lehnt Assertions ohne Signatur ab
  - STRICT: Stellt sicher, dass sowohl Antwort als auch Assertion signiert sind
  - OFF: Erlaubt unsignierte Assertions
- Zielgruppe - Zielgruppe, für die eine vom IdP gesendete Assertion anwendbar ist. Dies ist in der Regel ein Entitätsname oder eine URL, die den Dienstanbieter darstellt.
- Signaturalgorithmus — Algorithmus, der zum Signieren/Überprüfen von SAML-Transaktionen verwendet wird. Der Standardwert ist RSA-SHA256.
- Digest-Methode — Algorithmus, der zur Berechnung/Überprüfung des Digest für SAML-Transaktionen verwendet werden soll. Der Standardwert ist SHA256.
- Standardauthentifizierungsgruppe — Die Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wenn die Authentifizierung erfolgreich ist.
- Gruppennamenfeld — Name des -Tags in einer Assertion, die Benutzergruppen enthält.
- Skew Time (Minuten) - Diese Option gibt den Uhrzeitversatz in Minuten an, den der NetScaler-Dienstanbieter für eine eingehende Assertion zulässt. Wenn Sie beispielsweise die Skew-Zeit auf 10 Minuten um 16:00 Uhr festlegen, ist die SAML-Assertion von 15:50 bis 16:10 Uhr gültig — insgesamt 20 Minuten. Die voreingestellte Skew-Zeit beträgt 5 Minuten.

3. Erstellen Sie eine entsprechende SAML-Richtlinie.

Navigieren Sie zu **Sicherheit > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Policy** und klicken Sie auf **Hinzufügen**.

Geben Sie auf der Seite **SAML-Authentifizierungsrichtlinie erstellen** die folgenden Details an:

- Name - Geben Sie einen Namen für die SAML-Richtlinie an.
- Aktionstyp — Wählen Sie **SAML** als Authentifizierungsaktionstyp aus.
- Aktion — Wählen Sie das SAML-Serverprofil aus, an das die SAML-Richtlinie gebunden werden soll.
- Ausdruck - Zeigt den Namen der Regel oder des Ausdrucks an, anhand dessen die SAML-Richtlinie bestimmt, ob sich der Benutzer beim SAML-Server authentifizieren muss. Stellen Sie im Textfeld den Wert “rule = true” ein, damit die SAML-Richtlinie wirksam wird und die entsprechende SAML-Aktion ausgeführt wird.

4. Binden Sie die SAML-Richtlinie an den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**, und ordnen Sie die SAML-Richtlinie dem virtuellen Authentifizierungsserver zu.

5. Ordnen Sie den Authentifizierungsserver dem entsprechenden virtuellen Verkehrsverwaltungsserver zu.

   Navigieren Sie zu **Traffic Management > Load Balancing** (oder **Content Switching**) > **Virtuelle Server**, wählen Sie den virtuellen Server aus und ordnen Sie ihm den virtuellen Authentifizierungsserver zu.

NetScaler als SAML-IdP

June 19, 2023

Der SAML-IdP (Identity Provider) ist eine SAML-Entität, die im Kundennetzwerk bereitgestellt wird. Der IdP erhält Anfragen vom SAML-SP und leitet Benutzer zu einer Anmeldeseite weiter, auf der sie ihre Anmeldeinformationen eingeben müssen. Der IdP authentifiziert diese Anmeldeinformationen mit dem Active Directory (externer Authentifizierungsserver wie LDAP) und generiert dann eine SAML-Assertion, die an den SP gesendet wird.

Der SP überprüft das Token, und dem Benutzer wird dann Zugriff auf die angeforderte geschützte Anwendung gewährt.

Wenn die NetScaler Appliance als IdP konfiguriert ist, werden alle Anfragen von einem virtuellen Authentifizierungsserver empfangen, der mit dem entsprechenden SAML-IdP-Profil verknüpft ist.

> **Hinweis**
>
> Eine NetScaler Appliance kann als IdP in einer Bereitstellung verwendet werden, in der der SAML-SP entweder auf der Appliance oder auf einem externen SAML-SP konfiguriert ist.

Bei Verwendung als SAML-IdP eine NetScaler Appliance:

- Unterstützt alle Authentifizierungsmethoden, die es für herkömmliche Anmeldungen unterstützt.
- Signiert digital Behauptungen.
- Unterstützt Einzelfaktor- und Zwei-Faktor-Authentifizierung. SAML darf nicht als sekundärer Authentifizierungsmechanismus konfiguriert werden.
- Kann Assertionen mithilfe des öffentlichen Schlüssels des SAML-SP verschlüsseln. Dies wird empfohlen, wenn die Assertion sensible Informationen enthält.
- Kann so konfiguriert werden, dass nur digital signierte Anfragen vom SAML-SP akzeptiert werden.
- Kann sich mit den folgenden 401-basierten Authentifizierungsmechanismen am SAML-IdP anmelden: Negotiate, NTLM und Certificate.
- Kann so konfiguriert werden, dass zusätzlich zum NameID-Attribut 16 Attribute gesendet werden. Die Attribute müssen vom entsprechenden Authentifizierungsserver extrahiert werden. Für jeden von ihnen können Sie den Namen, den Ausdruck, das Format und einen Anzeigenamen im SAML-IdP-Profil angeben.
- Wenn die NetScaler Appliance als SAML-IdP für mehrere SAML-SP konfiguriert ist, kann ein Benutzer Zugriff auf Anwendungen auf den verschiedenen SPs erhalten, ohne sich jedes Mal explizit zu authentifizieren. Die NetScaler Appliance erstellt ein Sitzungscookie für die erste Authentifizierung, und jede nachfolgende Anforderung verwendet dieses Cookie zur Authentifizierung.
- Kann mehrwertige Attribute in einer SAML-Assertion senden.
- Unterstützt Post- und Umleitungsbindungen. Die Unterstützung für Artefaktbindung wird in NetScaler Release 13.0 Build 36.27 eingeführt.
- Kann die Gültigkeit einer SAML-Assertion angeben.

  Wenn die Systemzeit auf NetScaler SAML IdP und Peer-SAML-SP nicht synchron ist, werden die Nachrichten möglicherweise von beiden Parteien ungültig gemacht. Um solche Fälle zu vermeiden, können Sie jetzt die Zeitdauer festlegen, für die die Assertionen gültig sind.

  Diese Dauer, die als “Skew-Zeit” bezeichnet wird, gibt die Anzahl der Minuten an, für die die Nachricht akzeptiert werden muss. Die Skew Time kann auf dem SAML-SP und dem SAML-IdP konfiguriert werden.

- Kann so konfiguriert werden, dass Assertionen nur für SAML-SPs verwendet werden, die auf dem IdP vorkonfiguriert sind oder denen er vertraut. Für diese Konfiguration muss der SAML-IdP die Dienstanbieter-ID (oder den Namen des Ausstellers) der entsprechenden SAML-SPs haben.

  > **Hinweis**
  >
  > - Bevor Sie fortfahren, stellen Sie sicher, dass Sie über eine Authentifizierungsrichtlinie verfügen, die an einen virtuellen LDAP-Authentifizierungsserver gebunden ist.
  > - Einzelheiten zur Konfiguration einer LDAP-Aktion zum Abrufen der erforderlichen Attribute finden Sie unter Unterstützung von Name-Value-Attributen fürdie LDAP-Authentifizierung.

Konfigurieren Sie eine NetScaler Appliance als SAML IdP mithilfe der CLI

1. Erstellen Sie ein SAML-IdP-Profil.

   Beispiel

   Hinzufügen von NetScaler Appliance als IdP mit SiteMinder als SP.

   ```
   add authentication samlIdPProfile samlIDPProf1 -samlSPCertName siteminder
   -cert -encryptAssertion ON -metadataUrl https://samlidp.example.com/
   metadata -samlIdPCertName ns-cert -assertionConsumerServiceURL https
   ://example.com/cgi/samlauth -rejectUnsignedRequests ON -signatureAlg
   RSA-SHA256 -digestMethod SHA256 -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.
   REGEX_MATCH(re##^https://example\.com/cgi/samlauth$##)
   ```

2. Konfigurieren Sie das SAML-IdP-Profil. Im folgenden Beispiel enthält die IdP-Sitzung das Attribut „userPrincipalName“.

   ```
   set samlidPProfile SAML-IDP-Profile -Attribute1 "userPrincipalName"-
   Attribute1Expr "AAA.USER.ATTRIBUTE(\"userPrincipalName\")"
   ```

   Wichtige Hinweise

   - Konfigurieren Sie im SAML-IdP-Profil **AcsURLRule**, die einen Ausdruck der Liste der anwendbaren Dienstanbieter-URLs für diesen IdP verwendet. Dieser Ausdruck hängt vom verwendeten SP ab. Wenn NetScaler als SP konfiguriert ist, lautet die ACS-URL `https://<SP-domain_name>/cgi/samlauth`. Für den Abgleich wird empfohlen, dass der Ausdruck eine vollständige URL enthält.
   - Wenn Sie möchten, dass der SAML-IdP nur eine ACS-URL zulässt, verwenden Sie den folgenden Befehl:

     Das folgende CLI-Beispiel verwendet `https://testlb.aaa.local` als ACS-URL:


```
set samlidpprofile SAML_IDP_profile -acsurlrule  "AAA.LOGIN.
    SAML_REQ_ACS_URL.eq("https://testlb.aaa.local")"
<!--NeedCopy-->
```

- Wenn Sie möchten, dass der SAML-IdP die ACS-URL mit einem regulären Ausdruck abgleicht, verwenden Sie den folgenden Ausdruck:

  `-acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.REGEX_MATCH(re##^https://example.com/cgi/samlauth$##)`

  Der obige Ausdruck stellt sicher, dass die ACS-URL mit übereinstimmt `https://example.com/cgi/samlauth`. Das „^“ -Zeichen am Anfang des regulären Ausdrucks stellt sicher, dass NetScaler nichts vor „https“ zulässt. Das „$“ -Zeichen am Ende des regulären Ausdrucks stellt sicher, dass NetScaler nach „samlauth“ nichts zulässt.

  Wenn der Ausdruck lautet `-acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.REGEX_MATCH (re##https://example.com/cgi/##)`, lässt der SAML-IdP jede ACS-URL zu, wie in den folgenden Beispielen gezeigt:

  - `https://example.com/cgi/samlauth`
  - `abcdhttps://example.com/cgi/xyz`
  - `https://example.com/cgi/abcde`

- SAML unterstützt nur das RSA-Zertifikat. Andere Zertifikate wie HSM, FIPS werden nicht unterstützt.

Weitere Informationen zum Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction und https://support.citrix.com/article/CTX316577.

- Wenn sich die IdP-Abmelde-URL von der Umleitungs-URL unterscheidet und der Benutzer länger als 2 Minuten auf der NetScaler-Anmeldeseite ist, wird ein Serverfehler`HTTP/1.1 Internal Server Error 43549` angezeigt, wenn der Benutzer versucht, sich zu authentifizieren. In den NetScaler-Protokollen wird eine Meldung angezeigt, die darauf hinweist, dass die Umleitungs-URL für eingehende Nachrichten nach der Abmeldung nicht in den erlaubten Abmeldeumleitungs-URLs für den Benutzer enthalten ist.

  Um dieses Problem zu beheben, binden Sie den Mustersatz wie im folgenden Beispiel gezeigt:

  ```
  bind patset ns_aaa_oauthidp_logout_redirect_uris "https://FQDN and
  path to the logout url"
  ```

3. Konfigurieren Sie die SAML-Authentifizierungsrichtlinie, und ordnen Sie das SAML-IdP-Profil als Aktion der Richtlinie zu.


```
add authentication samlIdPPolicy samlIDPPol1 -rule true -action samlIDPProf1
```

> **Hinweis:**
>
> Wenn der Richtlinienname ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „meine Richtlinie“ oder „meine Richtlinie“).

4. Binden Sie die Richtlinie an den virtuellen Authentifizierungsserver.

   ```
   bind authentication vserver saml-auth-vserver -policy samlIDPPol1 -
   priority 100
   ```

   Weitere Informationen zum Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlIdPProfile.

NetScaler Appliance als SAML IdP mithilfe der GUI konfigurieren

1. Konfigurieren Sie ein SAML-IdP-Profil. Dieses Profil wird verwendet, um die eingehenden Authentifizierungsanfragen vom SP zu überprüfen und die Assertion zu erstellen und zu signieren, bevor sie an den SP gesendet wird.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Erweiterte Authentifizierungsrichtlinien > SAML-IDP-Richtlinien**.

   Wählen Sie **Server**aus, klicken Sie auf **Hinzufügen**, geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

   Parameter-Beschreibungen:

   - Name — Der Name des neuen SAML-Single-Sign-On-Profils.
   - SAML IDP-Metadaten exportieren — Klicken Sie auf diesen Link, wenn Sie die Metadaten des SAML IdP-Profils auf einen virtuellen NetScaler Gateway VPN-Server exportieren möchten.
   - Metadaten importieren — Diese Option importiert die SAML-IdP-Metadaten. Diese Option ist standardmäßig aktiviert.
   - Assertion Consumer Service Url — Die URL, an die die Assertion gesendet werden soll.
   - Service Provider-Abmelde-URL — Der SP-Endpunkt, an den Abmeldenachrichten gesendet werden sollen.
   - Logout-Bindung — Gibt den Transportmechanismus der SAML-Abmeldenachrichten an. Verfügbare Optionen sind POST und REDIRECT.
   - SAML SP-Metadaten-URL — Die URL, die zum Abrufen der SAML-IdP-Metadaten verwendet wird.

> **Hinweis:**
>
> Wenn die SAML SP-Metadaten-URL konfiguriert ist, werden die folgenden Parameter aus dem SAML-IdP-Profil übernommen und in der SAML SP-Konfiguration automatisch ausgefüllt:
>
> - Assertion Consumer Service URL
> - Abmelde-URL des Dienstanbieters
> - SP-Zertifikatsname
> - Abmeldebindung
> - SAML-Bindung
> - Assertion unterschreiben

- Aktualisierungsintervall für Metadaten (Minuten) — Das Zeitintervall (in Minuten) für das Abrufen der Metadaten von der angegebenen Metadaten-URL. Das Standardzeitintervall ist 3600 Minuten.
- Assertion Consumer Service URL Rule — Ausdruck, der die zulässigen ACS-URLs definiert, die von einem SAML-SP stammen. Mit anderen Worten, es erlaubt Listen von ACS-URLs, um Angriffe zu verhindern, bei denen betrügerische ACS-URLs in SAML-Anfragen eingefügt werden.
- Assertion Consumer Service URL — Die URL, zu der der authentifizierte Benutzer umgeleitet wird.
- IdP-Zertifikatname - Zertifikatschlüsselpaar, das für die Authentifizierungsseite verwendet wird.
- Name des SP-Zertifikats - Zertifikat des Dienstanbieters In diesem Szenario ist der Schlüssel dafür nicht erforderlich.
- Assertion signieren - Die Option, die Behauptung und die Antwort zu signieren, wenn der Client zurück zum Dienstanbieter weitergeleitet wird.
- Name des Ausstellers — Ein Zeichenfolgenwert, der in der vom IdP ausgegebenen SAML-Assertion enthalten ist.
- Service Provider-ID — Eindeutige ID, die auf SP angegeben ist, um den Dienstanbieter zu identifizieren. Die ID kann beliebig sein und ist nicht unbedingt eine URL. Die ID muss jedoch sowohl für SP- als auch für IdP-Profile identisch sein.
- Standardauthentifizierungsgruppe — Die Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wenn eine Authentifizierung erfolgreich ist. Diese Gruppe ist nützlich für Administratoren, die den nFactor-Flow verwenden, um die geeigneten Konfigurationen für die weiterleitende Partei zu bestimmen. Wenn Sie beispielsweise eine Authentifizierungsrichtlinie konfigurieren, können Sie den Standardgruppennamen als Teil des folgenden Ausdrucks angeben:


```
AAA.USER.IS_MEMBER_OF("Default Authentication Group name").
```

- Unsignierte Anfragen ablehnen — Option, die Sie angeben können, um sicherzustellen, dass nur mit dem SP-Zertifikat signierte Assertions akzeptiert werden.
- Zielgruppe — Die Zielgruppe, an die die Assertion vom IdP gesendet wird. Dies ist normalerweise ein Entitätsname oder eine URL, die den SP darstellt.
- Skew Time (Minuten) - Skew Time (Minuten) - Diese Option gibt den Uhrzeitversatz in Minuten an, den der NetScaler Service Provider für eine eingehende Assertion zulässt. Wenn Sie beispielsweise die Skew-Zeit auf 10 Minuten um 16:00 Uhr festlegen, ist die SAML-Assertion von 15:50 bis 16:10 Uhr gültig — insgesamt 20 Minuten. Die voreingestellte Skew-Zeit beträgt 5 Minuten.
- NAME-ID-Format — Format der in der Assertion gesendeten Namenskennung.
- Namen-ID-Ausdruck — Ausdruck, der ausgewertet wird, um die in der Assertion zu sendende Namenskennung zu erhalten.
- Assertion signieren — Option zum Signieren von Teilen der vom IdP gesendeten Assertion. Die verfügbaren Optionen sind “Keine”, “Assertion”, “Antwort” oder “Beide”.
- Signaturalgorithmus - Algorithmus, der zum Signieren und Verifizieren der Behauptungen zwischen IdP und SP verwendet wird. Dies muss im IdP-Profil und im SP-Profil identisch sein.
- Digest Method - Algorithmus, der verwendet wird, um die Integrität der Assertions zwischen IdP und SP zu überprüfen. Dies muss im IdP-Profil und im SP-Profil identisch sein.
- SAML-Bindung — Ein Mechanismus, der verwendet wird, um SAML-Requestor- und Responder-Nachrichten zwischen dem SP und IdP zu transportieren. Wenn NetScaler als SP fungiert, unterstützt es Post-, Redirect- und Artifact-Bindungen. Die Standardbindungsmethode ist POST. Ordnen Sie die SAML-IdP-Richtlinie einem virtuellen Authentifizierungsserver zu. Für die Artefaktbindung muss der Transportmechanismus auf dem SP und dem IdP derselbe sein.
- Attribut 1 — Name des Attributs in der SAML-Assertion, dessen Wert extrahiert und als Attribut1 gespeichert werden muss. Ein ähnliches Muster gilt auch für die übrigen Attribute.
- Attribute1Expr — Ausdruck, der ausgewertet wird, um den Wert von Attribut 1 zu erhalten.
- attribute1FriendlyName — Name des Attributs 1, das in der SAML-Assertion gesendet werden muss.
- Attribute1Format — Format des Attributs 1, das in der SAML-Assertion gesendet werden soll.

2. Konfigurieren Sie die SAML-Authentifizierungsrichtlinie, und ordnen Sie das SAML-IdP-Profil als Aktion der Richtlinie zu.

Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Erweiterte Authentifizierungsrichtlinien > SAML-IDP-Richtlinien**.

Wählen Sie **Richtlinien**aus, klicken Sie auf **Hinzufügen**, geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

Parameter-Beschreibungen:

- Name — Name der SAML-IdP-Authentifizierungsrichtlinie.
- Aktion — Name des SAML-IdP-Profils, das auf Anfragen oder Verbindungen angewendet werden soll, die dieser Richtlinie entsprechen.
- Aktion protokollieren — Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anfrage dieser Richtlinie entspricht. Wählen Sie eine Log-Aktion aus der Dropdownliste aus oder erstellen Sie eine Log-Aktion, indem Sie auf Hinzufügen klicken.
- Aktion ohne definiertes Ergebnis — Aktion, die ausgeführt werden soll, wenn das Ergebnis der politischen Bewertung nicht definiert ist. Ein undefiniertes Ereignis weist auf einen internen Fehler hin. Es können nur die integrierten Aktionen verwendet werden.
- Kommentare — Alle Kommentare zur Aufbewahrung von Informationen zu dieser Richtlinie.

3. Ordnen Sie die SAML-IdP-Richtlinie einem virtuellen Authentifizierungsserver zu.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**und binden Sie die SAML-IdP-Richtlinie an den virtuellen Authentifizierungsserver.

Konfigurieren von SAML-Single-Sign-On

May 11, 2023

Um Single-Sign-On-Funktionen für Anwendungen bereitzustellen, die auf dem Dienstanbieter gehostet werden, können Sie SAML-Single-Sign-On auf dem SAML-SP konfigurieren.

Konfigurieren von SAML Single Sign-On über die Befehlszeile

1. Konfigurieren Sie das SAML-SSO-Profil.

   Beispiel

   Im folgenden Befehl ist Beispiel der virtuelle Lastenausgleichsserver, der über einen Weblink vom SharePoint-Portal verfügt. Nssp.example.com ist der virtuelle Datenverkehrsverwaltungsserver, der den SharePoint-Server Lastenausgleich ausgleicht.


```
add tm samlSSOProfile tm-saml-sso -samlSigningCertName nssp -
    assertionConsumerServiceURL "https://nssp2.example.com/cgi/
    samlauth" -relaystateRule "\\"https://nssp2.example.com/
    samlsso.html\\"" -sendPassword ON -samlIssuerName nssp.example
    .com
<!--NeedCopy-->
```

2. Verknüpfen Sie das SAML-SSO-Profil mit der Traffic-Aktion.

   Beispiel

   Der folgende Befehl aktiviert SSO und bindet das oben erstellte SAML-SSO-Profil an eine Verkehrsaktion.

```
add tm trafficAction html_act -SSO ON -samlSSOProfile tm-saml-sso
<!--NeedCopy-->
```

3. Konfigurieren Sie die Verkehrsrichtlinie, die angibt, wann die Aktion ausgeführt werden muss.

   Beispiel

   Mit dem folgenden Befehl wird die Verkehrsaktion einer Verkehrsrichtlinie zugeordnet.

```
add tm trafficPolicy html_pol "HTTP.REQ.URL.CONTAINS(\\"abc.html\\
    ")" html_act
<!--NeedCopy-->
```

4. Binden Sie die zuvor erstellte Verkehrsrichtlinie an einen virtuellen Datenverkehrsverwaltungsserver (Load Balancing oder Content Switching). Alternativ kann die Verkehrsrichtlinie global zugeordnet werden.

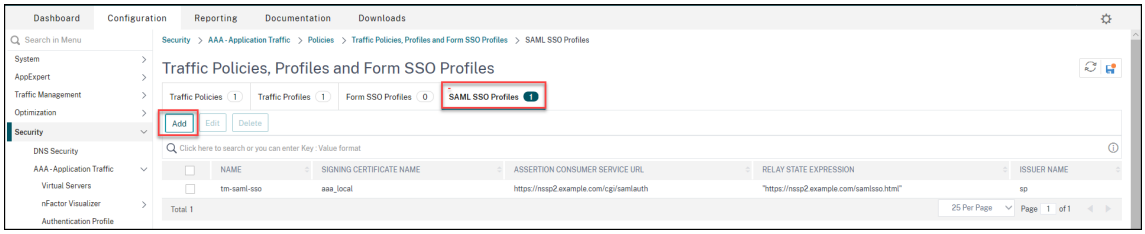
   > **Hinweis**
   >
   > Dieser virtuelle Datenverkehrsverwaltungsserver muss mit dem relevanten virtuellen Authentifizierungsserver verknüpft sein, der mit der SAML-Aktion verknüpft ist.

```
bind lb vserver lb1_ssl -policyName html_pol -priority 100 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Konfigurieren von SAML Single Sign-On mit der GUI

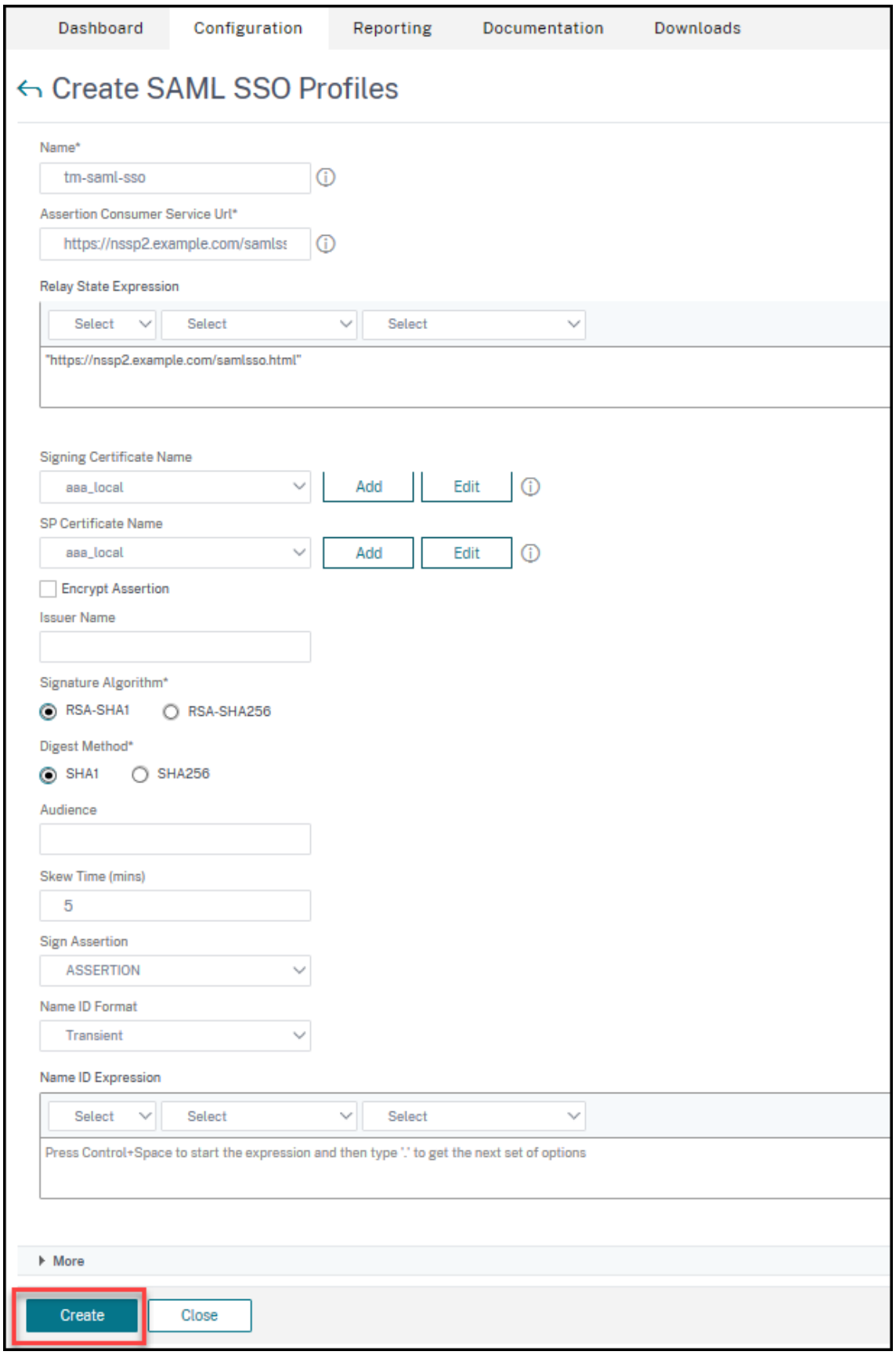
Um SAML Single Sign-On zu konfigurieren, müssen Sie das SAML-SSO-Profil, das Verkehrsprofil und die Datenverkehrsrichtlinie definieren und die Datenverkehrsrichtlinie an einen virtuellen Datenverkehrsverwaltungsserver oder global an die NetScaler-Appliance binden.

1. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Richtlinien > Traffic > SAML-SSO-Profile** und klicken Sie auf **Hinzufügen**.

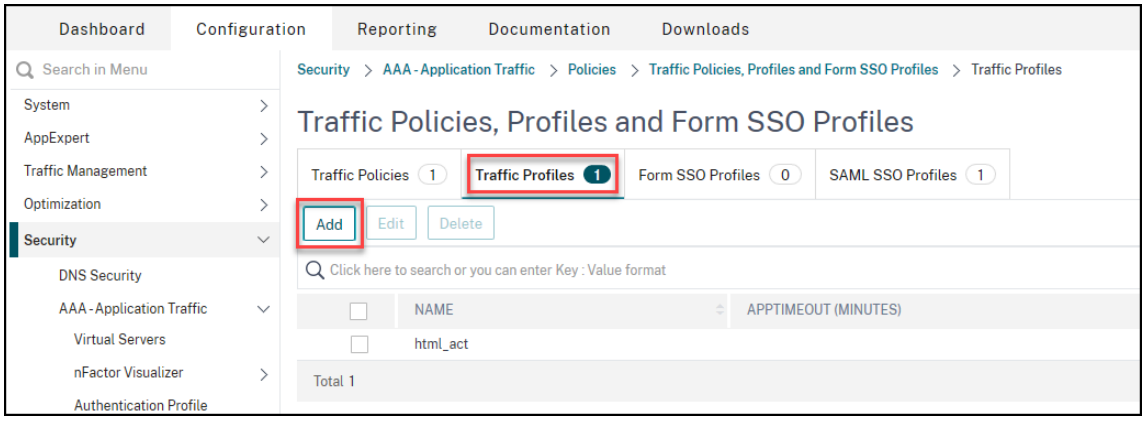


2. Geben Sie auf der Seite **SAML-SSO-Profile erstellen** Werte für die folgenden Felder ein und klicken Sie auf **Erstellen**.

   - Name - Name für das SAML SSO-Profil
   - Assertion Consumer Service Url - URL, an die die Behauptung gesendet werden soll
   - Signierzertifikatname - Name des SSL-Zertifikats, das zum Signieren von Assertion verwendet wird
   - Name des SP-Zertifikats - Name des SSL-Zertifikats einer Peer/empfangenden Partei, mit der Assertion verschlüsselt ist
   - Name des Ausstellers - Der Name, der in Anfragen verwendet werden soll, die von NetScaler an IdP gesendet werden, um NetScaler eindeutig zu identifizieren
   - Signaturalgorithmus - Algorithmus zur Signieren/Verifizierung von SAML-Transaktionen
   - Digest-Methode — Algorithmus, der zur Berechnung/Überprüfung des Digest für SAML-Transaktionen verwendet wird
   - Zielgruppe - Zielgruppe, für die eine vom IdP gesendete Assertion anwendbar ist. Dies ist normalerweise ein Entitätsname oder eine URL, die einen ServiceProvider darstellt
   - Zielgruppe - Zielgruppe, für die eine vom IdP gesendete Assertion anwendbar ist. Dies ist normalerweise ein Entitätsname oder eine URL, die einen ServiceProvider darstellt
   - Skew Time (min) - Die Anzahl der Minuten auf beiden Seiten der aktuellen Zeit, für die die Assertion gültig wäre
   - Assertion signieren — Option, um Teile der Assertion zu signieren, wenn NetScaler IdP eine sendet. Basierend auf der Benutzerauswahl kann entweder Assertion oder Response oder Beide oder keine signiert werden.
   - Name ID Format - Format der in Assertion gesendeten Namenskennung
   - Name-ID-Ausdruck — Ausdruck, der ausgewertet wird, um den NameIdentifier zu erhalten, der als Assertion gesendet werden soll

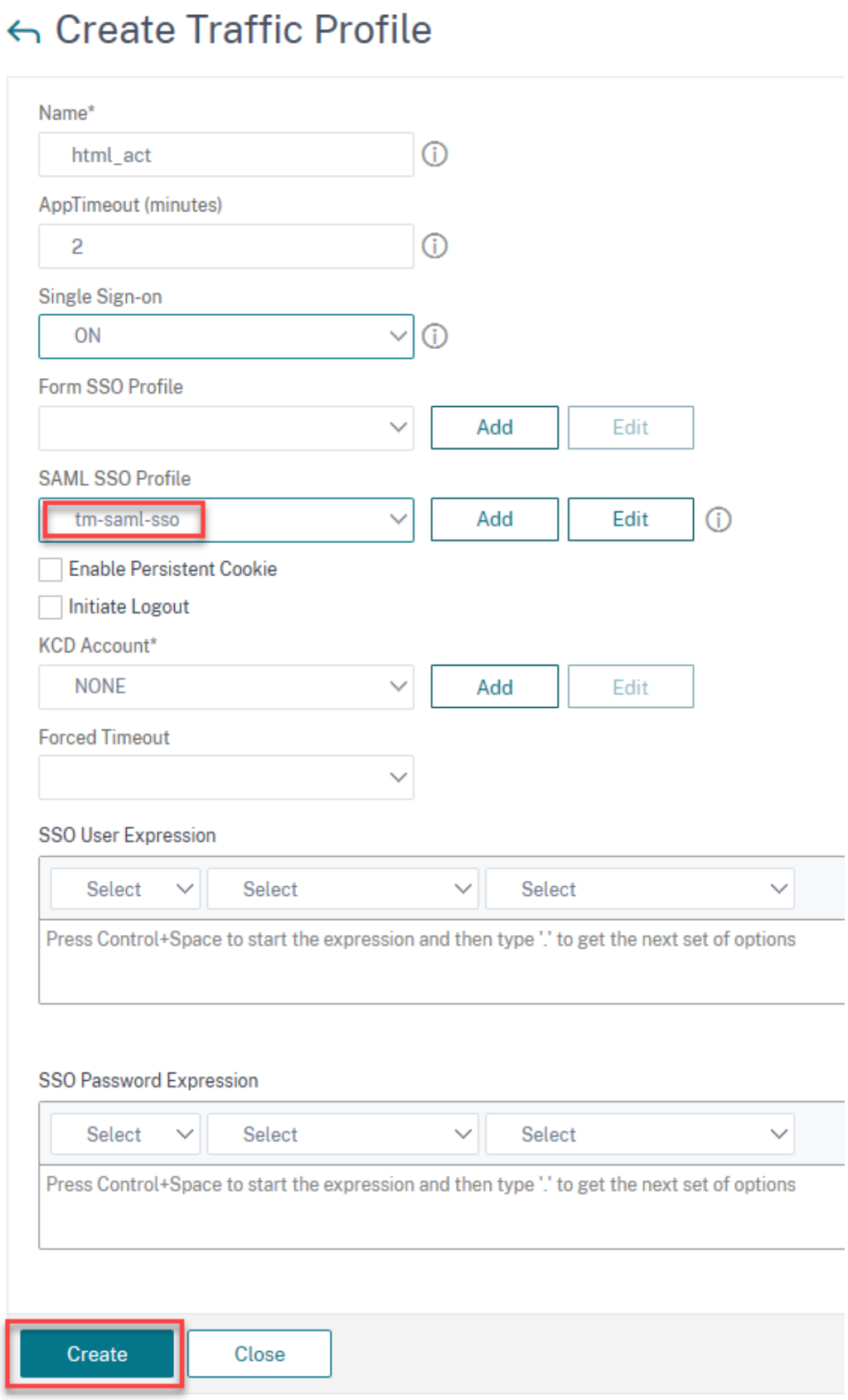


3. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Richtlinien>Traffic > Verkehrsprofile** und klicken Sie auf **Hinzufügen**.

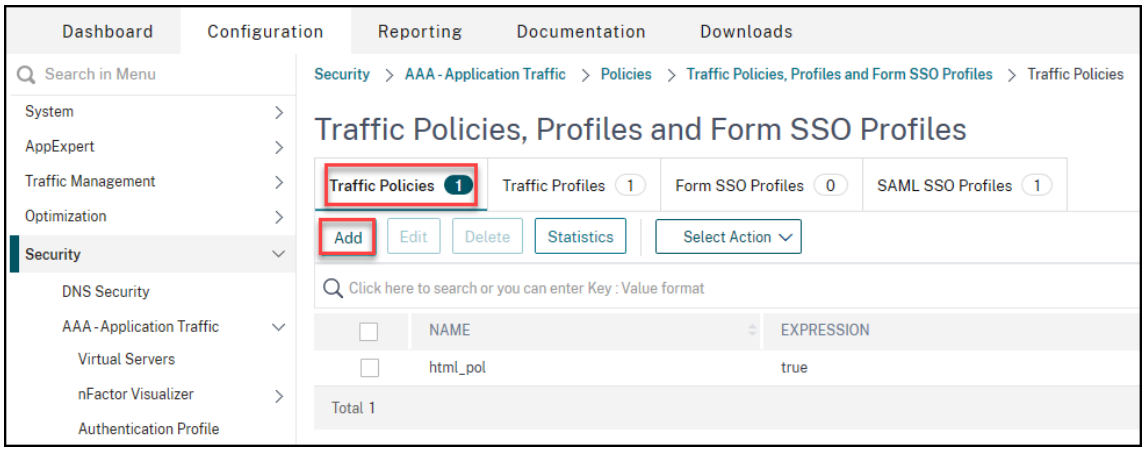


4. Geben Sie auf der Seite " **Verkehrsprofil erstellen** " Werte für die folgenden Felder ein und klicken Sie auf **Erstellen**.

   - Name - Name für die Verkehrsaktion.
   - AppTimeout (Minuten) - Zeitintervall der Benutzerinaktivität in Minuten, nach dem die Verbindung geschlossen wird.
   - Single Sign-On - Wählen Sie EIN
   - SAML SSO-Profil - Wählen Sie das erstellte SAML SSSO-Profil aus
   - KCD-Konto - Kerberos eingeschränkter Kontoname der Delegation
   - SSO-Benutzerausdruck — Ausdruck, der ausgewertet wird, um den Benutzernamen für SingleSignon zu erhalten
   - SSO Password Expression - Ausdruck, der ausgewertet wird, um ein Kennwort für Single-Signon zu erhalten

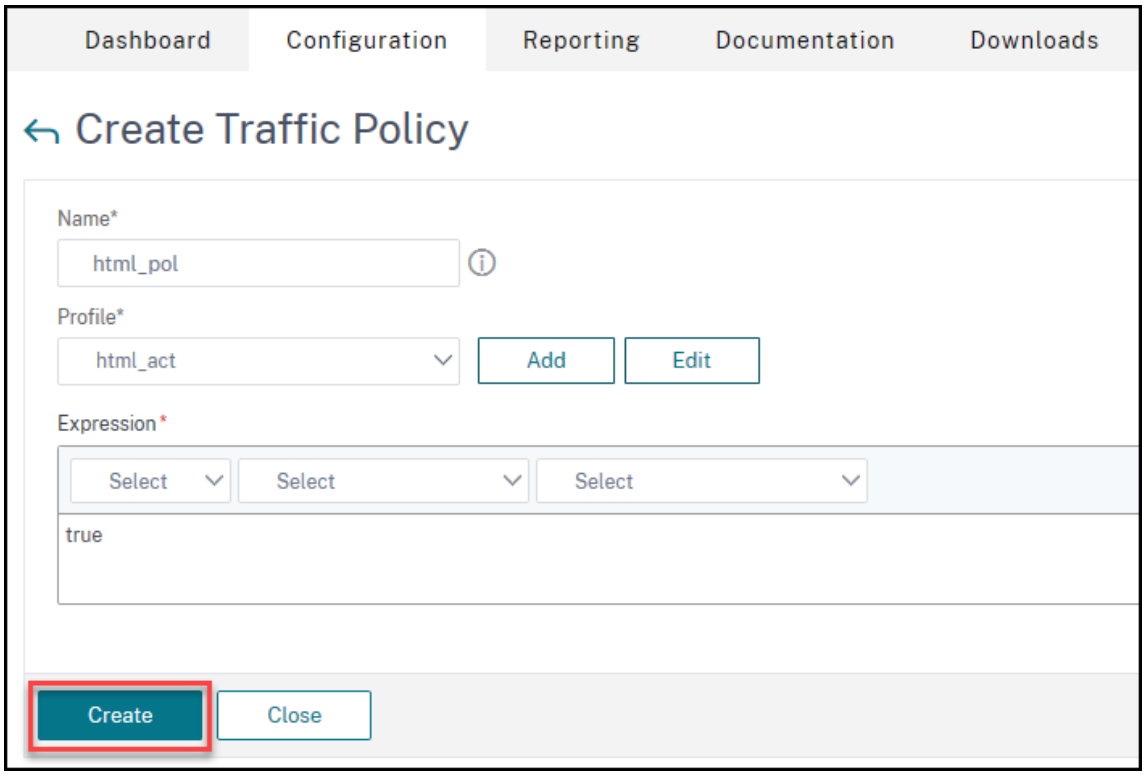


5. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Richtlinien > Traffic > Traffic Policys** und klicken Sie auf **Hinzufügen**.

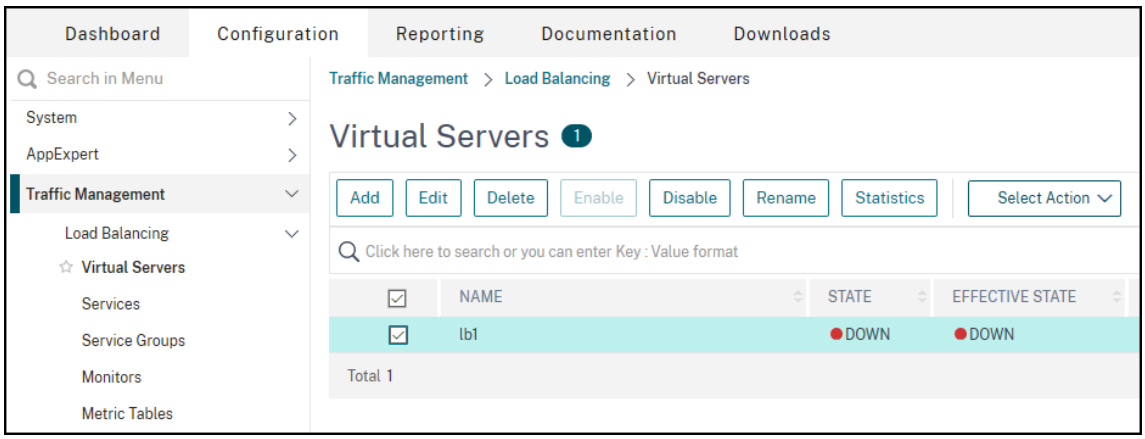


6. Geben Sie auf der Seite **Traffic-Richtlinie erstellen** Werte für Folgendes ein, und klicken Sie auf **Erstellen**.

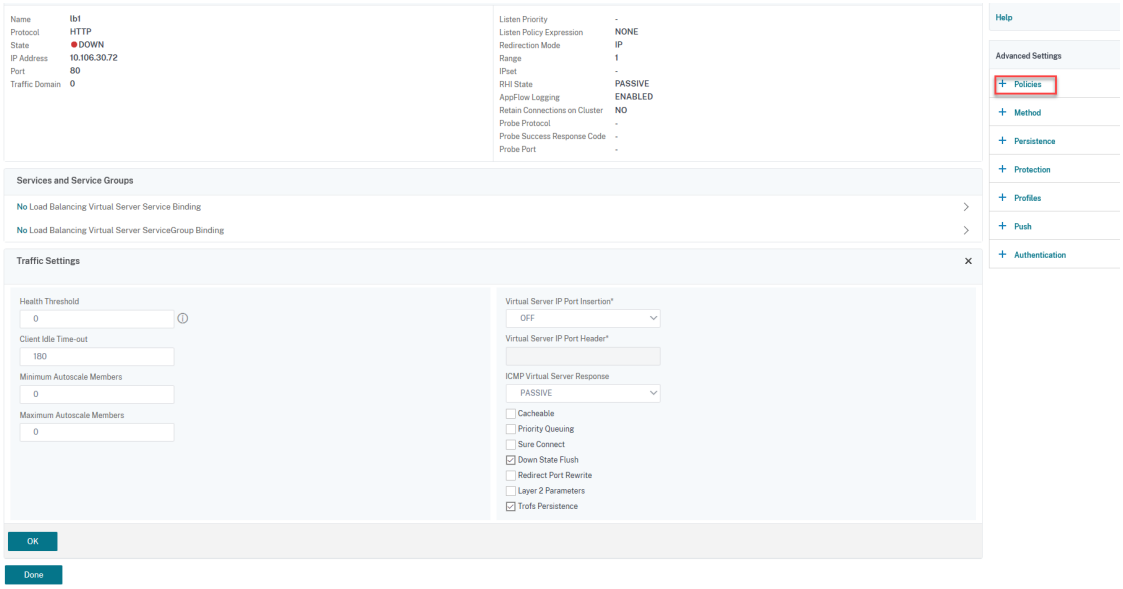
   - Name — Name der zu erstellenden Verkehrsrichtlinie
   - Profil — Wählen Sie das erstellte Verkehrsprofil
   - Ausdruck — Erweiterter Richtlinienausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Beispiel: true.



7. Um die Verkehrsrichtlinie an einen virtuellen Datenverkehrsverwaltungsserver zu binden, wählen Sie einen virtuellen Server aus.



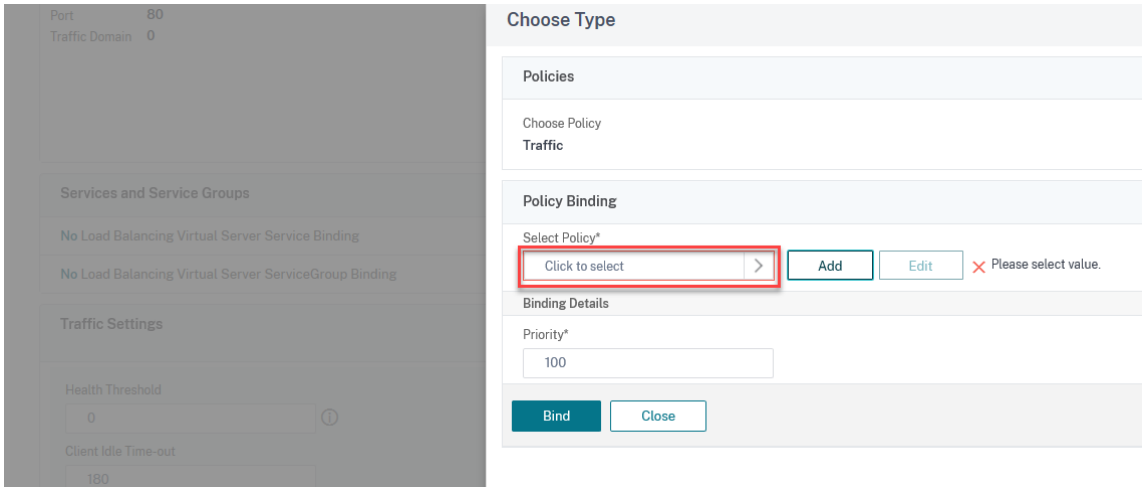
8. Klicken Sie auf **Richtlinien**.



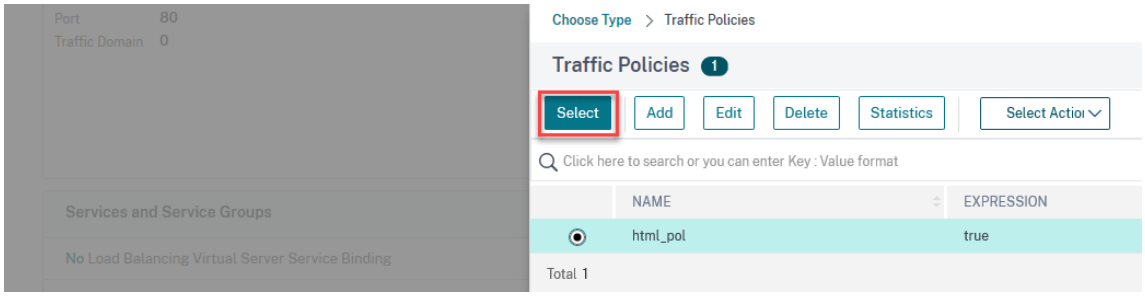
9. Wählen Sie im Feld **Richtlinie auswählen** die Option **Traffic** aus, wählen Sie im Feld **Typ auswählen** die Option **Anforderung** aus, und klicken Sie auf **Weiter**.

   ! [Klicken Sie hier, um eine Richtlinie hinzuzufügen (/en-us/citrix-adc/media/saml-9.png)

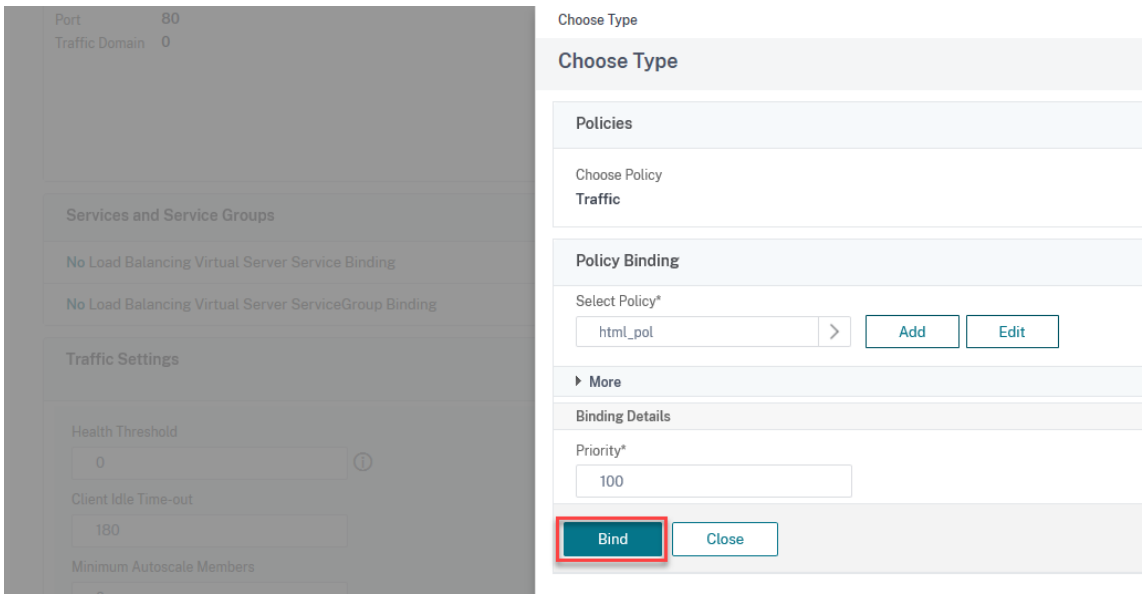
10. Klicken Sie im Feld **„Richtlinie** auswählen“, um den erstellten Traffic auszuwählen.



11. Klicken Sie auf **Select**.



12. Klicken Sie auf **Binden**, um die Datenverkehrsrichtlinie an den virtuellen Server zu binden.



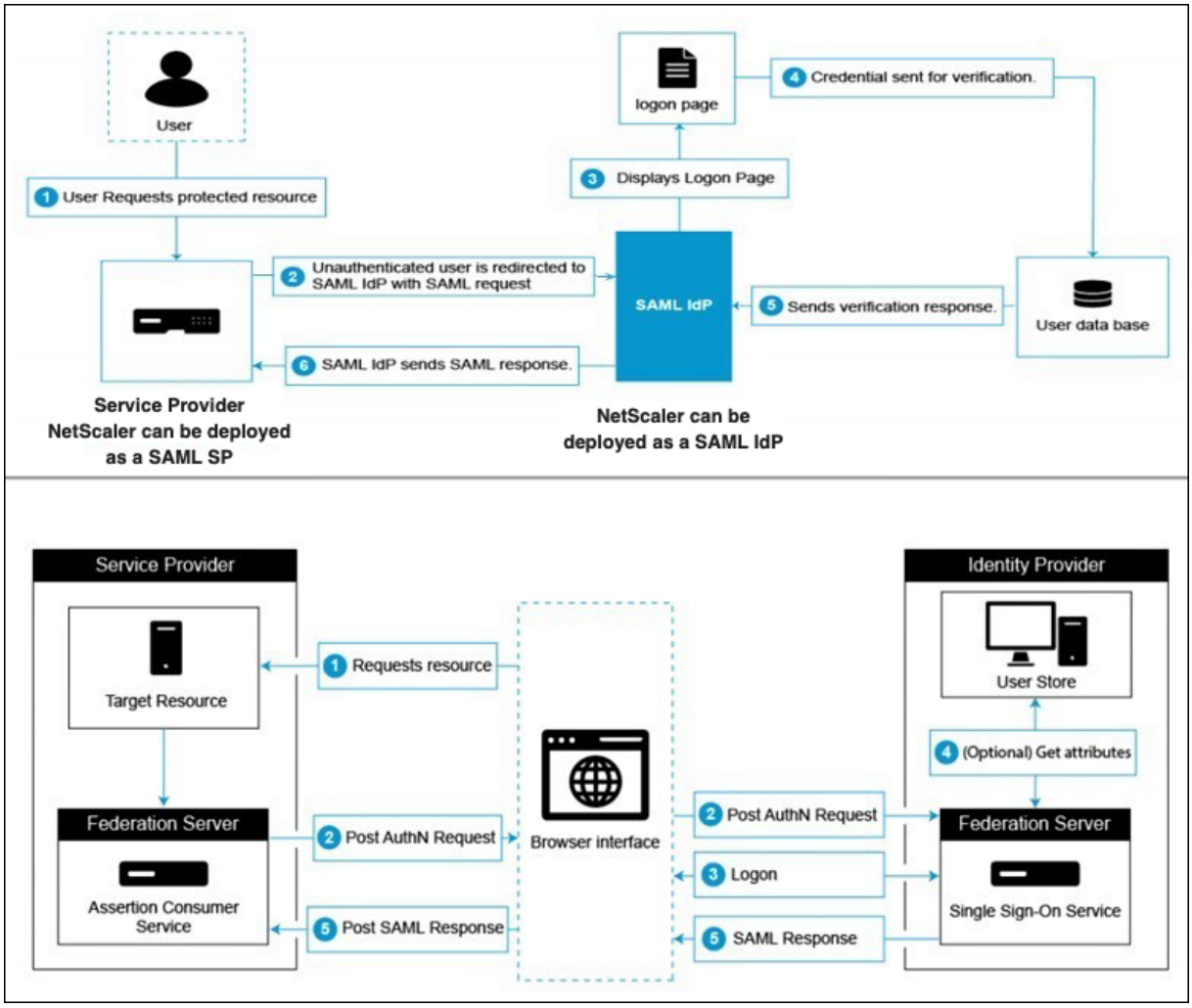
Azure AD als SAML IdP und NetScaler als SAML SP konfigurieren

September 11, 2023

Der SAML-Dienstanbieter (SAML SP) ist eine SAML-Entität, die vom Dienstanbieter bereitgestellt wird. Wenn ein Benutzer versucht, auf eine geschützte Anwendung zuzugreifen, wertet der SP die Client-Anfrage aus. Wenn der Client nicht authentifiziert ist (kein gültiges NSC_TMAA- oder NSC_TMAS-Cookie hat), leitet der SP die Anfrage an den SAML-Identitätsanbieter (IdP) weiter. Der SP validiert auch SAML-Assertionen, die vom IdP empfangen werden.

Der SAML-Identitätsanbieter (SAML IdP) ist eine SAML-Entität, die im Kundennetzwerk bereitgestellt wird. Der IdP empfängt Anfragen vom SAML-SP und leitet Benutzer auf eine Anmeldeseite weiter, auf der sie ihre Anmeldeinformationen eingeben müssen. Der IdP authentifiziert diese Anmeldeinformationen mit dem Benutzerverzeichnis (externer Authentifizierungsserver, z. B. LDAP) und generiert dann eine SAML-Assertion, die an den SP gesendet wird. Der SP validiert das Token und dem Benutzer wird dann Zugriff auf die angeforderte geschützte Anwendung gewährt.

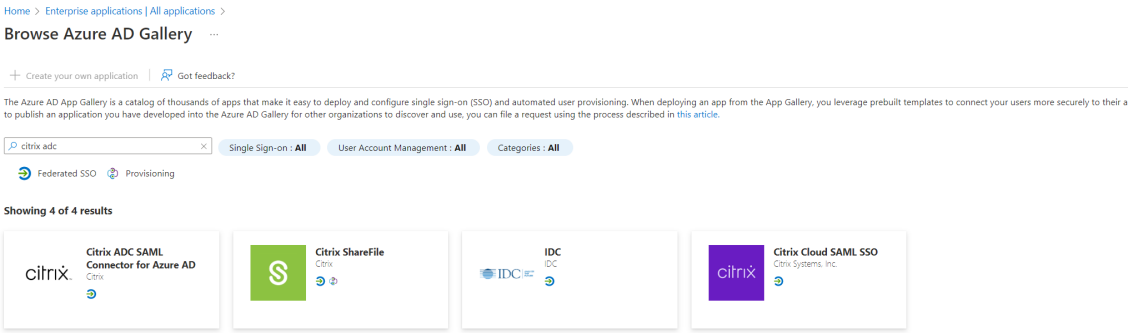
Das folgende Diagramm zeigt den SAML-Authentifizierungsmechanismus.



Azure AD AD-seitige Konfigurationen

Konfigurieren Sie Single-Sign-On-Einstellungen:

1. Klicken Sie im Azure-Portal auf **Azure Active Directory**.
2. Klicken Sie im Navigationsbereich unter dem Abschnitt **Verwalten** auf **Unternehmensanwendungen**. Eine Zufallsstichprobe der Anwendungen in Ihrem Azure AD-Mandanten wird angezeigt.
3. Geben Sie in der Suchleiste **NetScaler SAML Connector for Azure AD** ein.



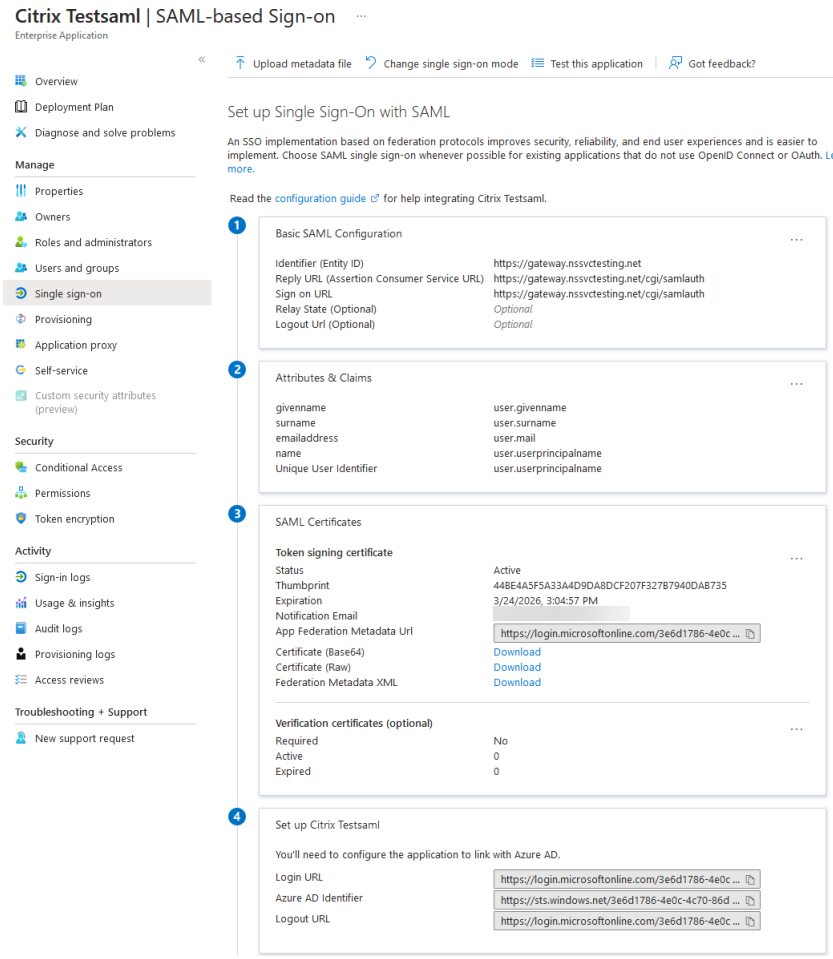
4. Wählen Sie im Abschnitt **Verwalten** die Option **Single Sign-On** aus.
5. Wählen Sie **SAML** aus, um Single Sign-On zu konfigurieren. Die Seite **Single Sign-On mit SAML einrichten - Vorschau** wird angezeigt. Hier fungiert Azure als SAML-IdP.
6. **Konfigurieren Sie grundlegende SAML-Optionen:**

   Identifikator (Entity ID) - Für einige Apps erforderlich. Identifiziert eindeutig die Anwendung, für die Single Sign-On konfiguriert wird. Azure AD sendet den Bezeichner als Zielgruppenparameter des SAML-Tokens an die Anwendung. Es wird erwartet, dass die Anwendung sie validiert. Dieser Wert erscheint auch als Entitäts-ID in allen SAML-Metadaten, die von der Anwendung bereitgestellt werden.

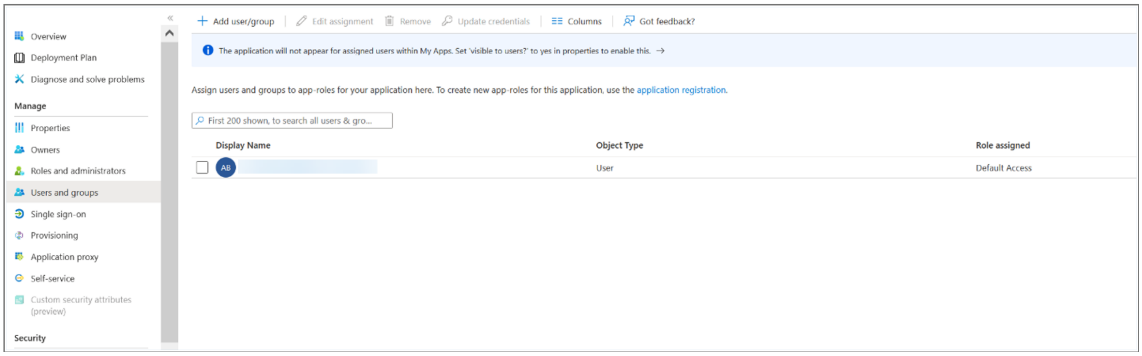
   Antwort URL - Obligatorisch. Gibt an, wo die Anwendung den Empfang des SAML-Tokens erwartet. Die Antwort-URL wird auch als Assertion Consumer Service (ACS) -URL bezeichnet. Geben Sie die Antwort-URL im Format an `http(s)://<SP_URL>/cgi/samlauth`.

   Anmelde-URL - Wenn ein Benutzer diese URL öffnet, leitet der Dienstanbieter zu Azure AD um, um sich zu authentifizieren und den Benutzer anzumelden.

   Relay-Status - Gibt an die Anwendung an, in die der Benutzer nach Abschluss der Authentifizierung umgeleitet werden soll.
7. Laden Sie das Zertifikat (Base64) aus dem Bereich **SAML-Zertifikate** herunter. Das Zertifikat wird bei der Konfiguration von NetScaler als SAML SP als SAML-SP als SAML-SP verwendet.



8. Sobald die Azure AD AD-seitige Konfiguration abgeschlossen ist, fügen Sie Benutzer und Benutzergruppen hinzu, die auf die Anwendung zugreifen dürfen. Gehen Sie zum Tab **Benutzer und Gruppen** und klicken Sie auf **+Benutzer/Gruppe hinzufügen**.



NetScaler-seitige Konfigurationen

1. Erstellen Sie eine SAML-Aktion.

   - Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehrsrichtlinien > Authen-**

tifizierung > Erweiterte Richtlinien > Aktionen > SAML.

- Klicken Sie auf **Hinzufügen**, geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

  Parameter-Beschreibung:

  Der Wert für fett gedruckte Parameter muss den Azure-Seitenkonfigurationen entnommen werden.

  - Name — Name des Servers
  - **URL umleiten** - Geben Sie die zuvor verwendete Anmelde-URL im Abschnitt Azure AD “Setup NetScaler” ein. `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`
  - Einzelne Abmelde-URL - `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`
  - SAML-Bindung — Ein Mechanismus, der verwendet wird, um SAML-Anforderungs- und Responder-Nachrichten zwischen dem SP und dem IdP zu transportieren. Wenn NetScaler als SP fungiert, unterstützt es Post-, Redirect- und Artifact-Bindungen. Die Standardbindungsmethode ist Post.
  - Logout-Bindung — Gibt den Transportmechanismus von SAML-Abmeldungsnachrichten an. Der Standard-Bindungsmechanismus ist Post.
  - **IDP-Zertifikatsname— IDPcert-Zertifikat (Base64), das im Abschnitt SAML-Zertifikate vorhanden ist.**

    ```
    add ssl certkey <IDP-CERT-NAME> -cert <Name of the IdP
       certificate downloaded above>
    <!--NeedCopy-->
    ```

  - **Benutzerfeld** - userprincipalName. EntNOMMEN aus dem Abschnitt „Benutzeratributе und Ansprüche“ von Azure IdP.
  - **Signierzertifikatname** - Für Azure AD nicht erforderlich. Wählen Sie das SAML-SP-Zertifikat (mit privatem Schlüssel) aus, das NetScaler verwendet, um Authentifizierungsanfragen an den IdP zu signieren. Das gleiche Zertifikat (ohne privaten Schlüssel) muss in den IdP importiert werden, damit der IdP die Signatur der Authentifizierungsanfrage überprüfen kann. Dieses Feld wird von den meisten IDPs nicht benötigt.
  - **issuerName** — Entitäts-ID oder der Bezeichner. `https://gateway.nssvctesting.net` in diesem Fall. In einem Lastausgleichs-Bereitstellungsszenario müssen Sie den FQDN des virtuellen Lastausgleichsservers verwenden.

- Unsignierte Assertion ablehnen — Option, die Sie angeben können, wenn die Assertionen des IdP signiert werden sollen. Die Standardeinstellung ist EIN.
- Zielgruppe — Zielgruppe, für die die vom IdP gesendete Assertion gilt. Dies ist normalerweise ein Entitätsname oder eine URL, die den Dienstanbieter darstellt.
- Signaturalgorithmus — Algorithmus, der zum Signieren/Verifizieren von SAML-Transaktionen verwendet wird. Der Standardwert ist RSA-SHA256.
- Digest-Methode — Algorithmus, der zur Berechnung/Überprüfung von Digest für SAML-Transaktionen verwendet wird. Der Standardwert ist SHA256.
- Standardauthentifizierungsgruppe — Die Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wenn die Authentifizierung erfolgreich ist.
- Feld Gruppenname — Name des Tags in einer Assertion, die Benutzergruppen enthält.
- Skew Time (Minuten) — Diese Option gibt den Zeitversatz in Minuten an, den der NetScaler Service Provider für eine eingehende Assertion zulässt. Wenn Sie beispielsweise die Skew-Zeit um 16:00 Uhr auf 10 Minuten festlegen, ist die SAML-Assertion von 15:50 bis 16:10 gültig, also insgesamt 20 Minuten. Die Standardschiefzeit beträgt 5 Minuten.
- Zwei-Faktor - AUS
- Angeforderter Authentifizierungskontext — exakt
- Authentifizierungsklassentyp — Keine
- Fingerabdruck senden — AUS
- Benutzername erzwingen — EIN
- Authentifizierung erzwingen — AUS
- SAML-Antwort speichern — AUS

2. Erstellen Sie eine entsprechende SAML-Richtlinie für die SAML-Aktion und binden Sie die Richtlinie an den virtuellen Authentifizierungsserver.
   - Navigieren Sie zu **Sicherheit > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Policy** und klicken Sie auf **Hinzufügen**.
   - Geben Sie auf der Seite **SAML-Authentifizierungsrichtlinie erstellen** die folgenden Details an:
     - Name — Geben Sie einen Namen für die SAML-Richtlinie an.
     - Aktionstyp — Wählen Sie SAML als Authentifizierungsaktionstyp aus.
     - Aktion — Wählen Sie das SAML-Serverprofil aus, an das die SAML-Richtlinie gebunden werden soll.

- Ausdruck — Zeigt den Namen der Regel oder des Ausdrucks an, anhand dessen die SAML-Richtlinie bestimmt, ob sich der Benutzer beim SAML-Server authentifizieren muss. Stellen Sie im Textfeld den Wert „rule = true“ ein, damit die SAML-Richtlinie wirksam wird und die entsprechende SAML-Aktion ausgeführt wird.

3. Binden Sie die SAML-Richtlinie an den virtuellen VPN-Server und verknüpfen Sie den virtuellen VPN-Server über ein Authentifizierungsprofil mit dem virtuellen Authentifizierungsserver. Einzelheiten zum Bindungsverfahren finden Sie unter Binden der Authentifizierungsrichtlinie.

Hinweis:

- Azure AD erwartet das Betreff-ID-Feld in der SAML-Anfrage nicht.
- Geben Sie den folgenden Befehl in der NetScaler CLI ein, damit NetScaler das Feld Subject ID nicht sendet.
  ```
  nsapimgr_wr.sh -ys call="ns_saml_dont_send_subject"
  ```
  Dieser Befehl ist nur in nFactor-Authentifizierungs-Workflows anwendbar.

Weitere Funktionen, die für SAML unterstützt werden

May 11, 2023

Die folgenden Funktionen werden für SAML unterstützt.

Metadaten-Lese- und Generierungsunterstützung für SAML SP und IdP Konfiguration

Die NetScaler-Appliance unterstützt jetzt Metadatendateien als Konfigurationsentitäten für SAML Service Provider (SP) und Identity Provider (IdP). Die Metadatendatei ist eine strukturierte XML-Datei, die die Konfiguration einer Entität beschreibt. Die Metadatendateien für SP und IdP sind getrennt. Je nach Bereitstellung kann ein SP oder eine IdP-Entität manchmal mehrere Metadatendateien haben.
Als Administrator können Sie Metadatendateien (SAML SP und IdP) in NetScaler exportieren und importieren.
Die Funktionen des Metadaten-Exports und -Imports für SAML SP und IdP werden in den folgenden Abschnitten erläutert.

Metadatenexport für SAML SP

Stellen Sie sich ein Beispiel vor, in dem der NetScaler als SAML SP konfiguriert ist und ein SAML-IdP Metadaten importieren möchte, die die NetScaler SP-Konfiguration enthalten. Angenommen, die NetScaler-Appliance ist bereits mit einem “SAMLAction” -Attribut konfiguriert, das die SAML SP-Konfiguration angibt.

Um Metadaten von Benutzern oder Administratoren zu exportieren, fragen Sie das NetScaler Gateway oder den virtuellen Authentifizierungsserver wie unten gezeigt ab:

```
https://vserver.company.com/metadata/samlsp/<action-name>
```

Metadatenimport für SAML SP

Derzeit verwendet die SAML Action-Konfiguration auf der NetScaler-Appliance verschiedene Parameter. Der Administrator gibt diese Parameter manuell an. Administratoren sind sich jedoch häufig der Nomenklatur nicht bewusst, wenn es darum geht, mit verschiedenen SAML-Systemen zu interagieren. Wenn Metadaten von IdP verfügbar sind, kann ein Großteil der Konfiguration in der Entität 'samlAction' vermieden werden. Tatsächlich könnte die gesamte IdP-spezifische Konfiguration weggelassen werden, wenn die IdP-Metadatendatei angegeben wird. Die 'samlAction'-Entität benötigt jetzt einen zusätzlichen Parameter, um die Konfiguration aus der Metadatendatei zu lesen.

Wenn Sie Metadaten in eine NetScaler-Appliance importieren, enthalten die Metadaten keine zu verwendenden Signaturalgorithmen, sondern die Endpunktdetails. Metadaten können mit bestimmten Algorithmen signiert werden, mit denen die Metadaten selbst überprüft werden können. Die Algorithmen werden nicht in der Entität 'SAMLAction' gespeichert.

Daher wird das, was Sie in der Entität 'SAMLAction' angeben, beim Senden der Daten verwendet. Eingehende Daten können einen anderen Algorithmus enthalten, den eine NetScaler-Appliance verarbeiten muss.

Sie können eine maximale Größe von 64 K Byte an Metadaten importieren.

Abrufen der Metadatendateien mit der Befehlszeilenschnittstelle.

```
set samlAction <name> [-metadataUrl <url> [-metadataRefreshInterval <
    int>] https://idp.citrix.com/samlidp/metadata.xml
```

> **Hinweis**
>
> Der Parameter metadataRefreshInterval ist das Intervall in Minuten zum Abrufen von Metadateninformationen von der angegebenen Metadaten-URL. Standardwert 36000.

Metadatenimport für SAML-IdP

Der Parameter "samlIdPProfile" benötigt ein neues Argument, um die gesamte Konfiguration zu lesen, die für SP spezifisch ist. Die SAML-IdP-Konfiguration kann vereinfacht werden, indem SP-spezifische Eigenschaften durch eine SP-Metadatendatei ersetzt werden. Diese Datei wird über HTTP abgefragt.

So lesen Sie die Metadatendatei über die Befehlszeilenschnittstelle:


```
set samlIdPProfile <name> [-metadataUrl <url>] [-
    metadataRefreshInterval <int>]
```

Name-Wert-Attribut-Unterstützung für SAML-Authentifizierung

Sie können jetzt SAML-Authentifizierungsattribute mit einem eindeutigen Namen zusammen mit Werten konfigurieren. Die Namen werden im SAML-Aktionsparameter konfiguriert und die Werte werden durch Abfragen der Namen abgerufen. Durch Angabe des Attributwerts für den Namen können Administratoren einfach nach dem Attributwert suchen, der dem Attributnamen zugeordnet ist. Außerdem müssen sich Administratoren das Attribut nicht mehr nur anhand seines Wertes merken.

> **Wichtig**
>
> - Im Befehl SAMLAction können Sie maximal 64 durch Komma getrennte Attribute mit einer Gesamtgröße von weniger als 2048 Byte konfigurieren.
> - Citrix empfiehlt die Verwendung der Attributliste. Die Verwendung von “Attribut 1 zu Attribut 16” führt zu einem Sitzungsfehler, wenn die Größe des extrahierten Attributs groß ist.

So konfigurieren Sie die Name-Wert-Attribute mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication samlAction <name> [-Attributes <string>]
```

Beispiel:

```
add authentication samlAction samlAct1 -attributes  “mail,sn,
    userprincipalName”
```

Assertion Consumer Service-URL-Unterstützung für SAML-IdP

Eine NetScaler-Appliance, die als SAML Identity Provider (IdP) konfiguriert ist, unterstützt jetzt die Assertion Consumer Service (ACS) -Indizierung, um die SAML Service Provider (SP) -Anforderung Der SAML-IdP importiert die ACS-Indizierungskonfiguration aus SP-Metadaten oder ermöglicht die manuelle Eingabe von ACS-Indexinformationen.
In der folgenden Tabelle sind einige Artikel aufgeführt, die sich speziell auf Bereitstellungen beziehen, bei denen die NetScaler-Appliance als SAML-SP oder SAML-IdP verwendet wird.

Einige Informationen zu anderen spezifischen Bereitstellungen:

- NetScaler als SAML SP auf FIPS-Gerät
- Konfigurieren von Office365 für Single Sign-On mit NetScaler als SAML-IdP

Unterstützung von WebView-Anmeldeinformationen für Authentifizierungsmechanismen

Die Authentifizierung einer NetScaler-Appliance kann jetzt das AuthV3-Protokoll unterstützen. Der WebView-Anmeldeinformationstyp im AuthV3-Protokoll unterstützt alle Arten von Authentifizierungsmechanismen (einschließlich SAML und OAuth). Der WebView-Anmeldeinformationstyp ist Teil von AuthV3, das von Citrix Receiver und Browser in Webanwendungen implementiert wird.

Im folgenden Beispiel wird der Ablauf von WebView-Ereignissen durch NetScaler Gateway und Citrix Receiver erläutert:

1. Der Citrix Receiver verhandelt mit NetScaler Gateway für die Unterstützung des AuthV3-Protokolls.
2. Die NetScaler-Appliance reagiert positiv und schlägt eine bestimmte Start-URL vor.
3. Citrix Receiver stellt dann eine Verbindung zum spezifischen Endpunkt (URL) her.
4. Das NetScaler Gateway sendet eine Antwort an den Client, um das WebView zu starten.
5. Citrix Receiver startet WebView und sendet eine erste Anfrage an die NetScaler-Appliance.
6. NetScaler-Appliance leitet den URI zum Anmeldeendpunkt des Browsers
7. Sobald die Authentifizierung abgeschlossen ist, sendet die NetScaler-Appliance eine Antwort auf den Abschluss an WebView.
8. Das WebView wird jetzt beendet und gibt die Steuerung an Citrix Receiver zurück, um das AuthV3-Protokoll für den Sitzungsaufbau fortzusetzen.

Erhöhung der SessionIndex-Größe in SAML SP

Die SessionIndex-Größe des SAML Service Providers (SP) wurde auf 96 Byte erhöht. Zuvor betrug die standardmäßige maximale Größe von SessionIndex 63 Byte.

> **Hinweis**
>
> Unterstützung in NetScaler 13.0 Build 36.x eingeführt

Unterstützung für benutzerdefinierte Authentifizierungsklassenreferenzen für SAML SP

Sie können ein benutzerdefiniertes Referenzattribut für die Authentifizierungsklasse im **SAML-Aktionsbefehl** konfigurieren. Mit dem benutzerdefinierten Klassenreferenzattribut für die Authentifizierung können Sie die Klassennamen in den entsprechenden SAML-Tags anpassen. Das

benutzerdefinierte Authentifizierungsklassenreferenzattribut zusammen mit dem Namespace wird als Teil der SAML SP-Authentifizierungsanforderung an den SAML-IdP gesendet.

Zuvor konnten Sie mit dem SAML-Aktionsbefehl nur einen Satz vordefinierter Klassen konfigurieren, die im authnCtxClassRef-Attribut definiert sind.

> **Wichtig**
>
> Stellen Sie beim Konfigurieren des Attributs customAuthnCtxClassRef Folgendes sicher:

- Die Namen der Klassen müssen alphanumerische Zeichen oder eine gültige URL mit den richtigen XML-Tags enthalten.
- Wenn Sie mehrere benutzerdefinierte Klassen konfigurieren müssen, muss jede Klasse durch Kommas getrennt werden

So konfigurieren Sie die customAuthnctxClassRef-Attribute über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

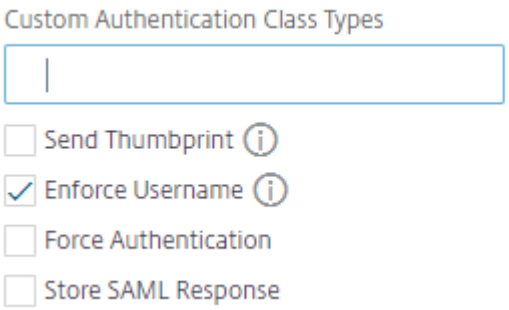
- Authentifizierung hinzufügen samlAction <name> [-customAuthnctxClassRef <string>]
- setze Authentifizierung samlAction <name> [-customAuthnctxClassRef <string>]

Beispiel:

- `add authentication samlAction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2`
- `set authentication samlAction samlact2 -customAuthnCtxClassRef http://www.class3.com/LoA1,http://www.class4.com/LoA2`

So konfigurieren Sie die customAuthnctxClassRef-Attribute mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > SAML**.
2. Wählen Sie auf der SAML-Seite die Registerkarte **Server** aus und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Create Authentication SAML Server** den Namen für die SAML-Aktion ein.
4. Scrollen Sie nach unten, um die Klassentypen im Abschnitt **Benutzerdefinierte Authentifizierungsklassen** zu konfigurieren.



Unterstützung für Artefakt-Bindung in SAML IdP

Die als SAML Identity Provider (IdP) konfigurierte NetScaler-Appliance unterstützt die Artefaktbindung. Die Artefaktbindung erhöht die Sicherheit von SAML IdP und hindert die böswilligen Benutzer daran, die Assertion zu überprüfen.

Assertion Consumer Service-URL-Unterstützung für SAML-IdP

Eine NetScaler-Appliance, die als SAML Identity Provider (IdP) konfiguriert ist, unterstützt jetzt die Assertion Consumer Service (ACS) -Indizierung, um die SAML Service Provider (SP) -Anforderung Der SAML-IdP importiert die ACS-Indizierungskonfiguration aus SP-Metadaten oder ermöglicht die manuelle Eingabe von ACS-Indexinformationen.

FIPS-Offload-Unterstützung

Eine NetScaler MPX FIPS-Appliance, die als SAML-Dienstanbieter verwendet wird, unterstützt jetzt verschlüsselte Zusicherungen. Außerdem kann eine NetScaler MPX FIPS-Appliance, die als SAML-Dienstanbieter oder SAML-Identitätsanbieter fungiert, jetzt für die Verwendung der SHA2-Algorithmen auf FIPS-Hardware konfiguriert werden.

> **Hinweis**
>
> Im FIPS-Modus wird nur der RSA-V1_5-Algorithmus als Schlüsseltransportalgorithmus unterstützt.

Konfigurieren der FIPS-Offload-Unterstützung mithilfe der Befehlszeilenschnittstelle:

1. SSL FIPS hinzufügen

   add ssl fipsKey fips-key

2. Erstellen Sie eine CSR und verwenden Sie sie auf dem CA-Server, um ein Zertifikat zu generieren. Sie können das Zertifikat dann in **/nsconfig/ssl**kopieren. Nehmen wir an, die Datei ist *fips3cert.cer*.


```
add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key<!--
NeedCopy-->
```

3. Geben Sie dieses Zertifikat in der SAML-Aktion für das SAML-SP-Modul an

```
set samlAction <name> -samlSigningCertName fips-cert<!--NeedCopy-->
```

4. Verwenden Sie das Zertifikat in samlIdpProfile für das SAML-IdP-Modul

```
set samlidpprofile fipstest -samlIdpCertName fips-cert<!--NeedCopy-->
```

Gängige SAML-Terminologien

Im Folgenden sind einige gebräuchliche SAML-Terminologien aufgeführt:

- **Assertion:** Eine SAML-Assertion ist ein XML-Dokument, das vom Identitätsanbieter nach der Authentifizierung des Benutzers an den Service Provider zurückgegeben wird. Die Assertion hat eine spezifische Struktur, wie im SAML-Standard definiert.
- **Arten von Assertions:** Im Folgenden sind die Arten von Assertion.
  - Authentifizierung - der Benutzer wird zu einem bestimmten Zeitpunkt mit einem bestimmten Mittel authentifiziert
  - Autorisierung - dem Benutzer wurde der Zugriff auf eine angegebene Ressource gewährt oder verweigert
  - Attribute - der Benutzer ist mit den angegebenen Attributen verknüpft
- **Assertion Consumer Service (ACS):** Der Endpunkt (URL) des Dienstanbieters, der für den Empfang und das Parsen einer SAML-Assertion verantwortlich ist
- **Zielgruppenbeschränkung:** Ein Wert innerhalb der SAML-Zusicherung, der angibt, für wen (und nur für wen) die Assertion bestimmt ist. Das “Publikum” ist der Dienstanbieter und ist normalerweise eine URL, kann aber technisch als eine beliebige Datenfolge formatiert werden.
- **Identitätsanbieter (IdP):** In Bezug auf SAML ist der Identitätsanbieter die Entität, die die Identität des Benutzers als Antwort auf eine Anfrage des Dienstanbieters überprüft.

  Der Identitätsanbieter ist für die Pflege und Authentifizierung der Benutzeridentität verantwortlich.
- **Service Provider (SP):** In Bezug auf SAML bietet der Service Provider (SP) dem Benutzer einen Dienst an und ermöglicht es dem Benutzer, sich mithilfe von SAML anzumelden. Wenn der Benutzer versucht, sich anzumelden, sendet der SP eine SAML-Authentifizierungsanforderung an den Identitätsanbieter (IdP)
- **SAML-Bindung:** SAML-Anforderer und Responder kommunizieren durch den Austausch von Nachrichten. Der Mechanismus zum Transportieren dieser Nachrichten wird als SAML-Bindung bezeichnet.

- **HTTP-Artefakt:** Eine der vom SAML-Protokoll unterstützten Bindungsoptionen. HTTP-Artefakt ist nützlich in Szenarien, in denen der SAML-Requester und der Responder einen HTTP-User-Agent verwenden und nicht die gesamte Nachricht übertragen möchten, weder aus technischen noch aus Sicherheitsgründen. Stattdessen wird ein SAML-Artefakt gesendet, bei dem es sich um eine eindeutige ID für die vollständigen Informationen handelt. Der IdP kann dann das Artefakt verwenden, um die vollständigen Informationen abzurufen. Der Artefakt-Aussteller muss den Status beibehalten, solange das Artefakt noch aussteht. Ein Artifact Resolution Service (ARS) muss eingerichtet werden.

  Das HTTP-Artefakt sendet das Artefakt als Abfrageparameter.

- **HTTP POST:** Eine der vom SAML-Protokoll unterstützten Bindungsoptionen.

  HTTP POST sendet den Nachrichteninhalt als POST-Parameter in der Nutzlast.

- **HTTP-Umleitung:** Eine der vom SAML-Protokoll unterstützten Bindungsoptionen.

  Wenn die HTTP-Umleitung verwendet wird, leitet der Dienstanbieter den Benutzer zum Identitätsanbieter weiter, wo die Anmeldung erfolgt, und der Identitätsanbieter leitet den Benutzer zurück zum Dienstanbieter. Die HTTP-Umleitung erfordert ein Eingreifen des Benutzeragenten (des Browsers).

  Die HTTP-Umleitung sendet den Nachrichteninhalt in der URL. Aus diesem Grund kann es nicht für die SAML-Antwort verwendet werden, da die Größe der Antwort normalerweise die von den meisten Browsern zulässige URL-Länge überschreitet.

  Hinweis: Die NetScaler-Appliance unterstützt POST- und Redirect-Bindungen während der Abmeldung.

- Metadaten: Metadaten sind die Konfigurationsdaten in SP und IdP, um zu wissen, wie man miteinander kommuniziert, was in XML-Standards enthalten sein wird

Weitere nützliche Citrix Artikel zur SAML-Authentifizierung

Möglicherweise finden Sie die folgenden Artikel zur SAML-Authentifizierung hilfreich.

- https://support.citrix.com/article/CTX277558
- https://support.citrix.com/article/CTX259127
- https://support.citrix.com/article/CTX228135
- https://support.citrix.com/article/CTX221631
- https://support.citrix.com/article/CTX138988

OAuth Authentifizierung

May 11, 2023

Die Authentifizierung, Autorisierung und Überwachung des Verkehrsmanagements unterstützt die Authentifizierung von OAuth und OpenID Connect (OIDC). Es autorisiert und authentifiziert Benutzer für Dienste, die auf Anwendungen wie Google, Facebook und Twitter gehostet werden.

Wichtige Hinweise

- NetScaler Advanced Edition und höher ist erforderlich, damit die Lösung funktioniert.
- Eine NetScaler-Appliance muss auf Version 12.1 oder höher sein, damit die Appliance mit OIDC als OAuth IdP funktioniert.
- OAuth auf einer NetScaler-Appliance ist für alle SAML-IdPs qualifiziert, die mit "OpenID Connect 2.0" kompatibel sind.

Eine NetScaler-Appliance kann so konfiguriert werden, dass sie sich mithilfe von SAML und OIDC als Service Provider (SP) oder Identity Provider (IdP) verhält. Zuvor unterstützte eine als IdP konfigurierte NetScaler-Appliance nur das SAML-Protokoll. Ab der NetScaler 12.1-Version unterstützt NetScaler auch das OIDC.

OIDC ist eine Erweiterung der OAuth Autorisierung/-Delegation. Eine NetScaler-Appliance unterstützt OAuth- und OIDC-Protokolle in derselben Klasse anderer Authentifizierungsmechanismen. OIDC ist ein Add-On zu OAuth, da es eine Möglichkeit bietet, Benutzerinformationen vom Autorisierungsserver abzurufen, im Gegensatz zu OAuth, das nur ein Token erhält, das für Benutzerinformationen nicht abgerufen werden kann.

Der Authentifizierungsmechanismus erleichtert die Inline-Überprüfung von OpenID-Token. Eine NetScaler-Appliance kann konfiguriert werden, um Zertifikate zu erhalten und Signaturen auf dem Token zu überprüfen.

Ein großer Vorteil der Verwendung der OAuth- und OIDC-Mechanismen besteht darin, dass die Benutzerinformationen nicht an die gehosteten Anwendungen gesendet werden. Daher wird das Risiko eines Identitätsdiebstahls erheblich reduziert.

Die für Authentifizierung, Autorisierung und Überwachung konfigurierte NetScaler-Appliance akzeptiert jetzt eingehende Token, die mit dem HMAC HS256-Algorithmus signiert werden. Darüber hinaus werden die öffentlichen Schlüssel des SAML Identity Provider (IdP) aus einer Datei gelesen, anstatt von einem URL-Endpunkt zu lernen.

In der NetScaler-Implementierung wird auf die Anwendung über den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsdatenverwaltungsserver zugegriffen. Um OAuth zu konfigurieren, müssen Sie also eine OAuth-Richtlinie konfigurieren, die dann einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver für das Verkehrsmanagement zugeordnet werden muss.

Konfigurieren Sie das OpenID Connect-Protokoll

Eine NetScaler-Appliance kann jetzt mithilfe des OIDC-Protokolls als Identitätsanbieter konfiguriert werden. Das OIDC-Protokoll stärkt die Funktionen zur Identitätsbereitstellung der NetScaler-Appliance. Sie können jetzt mit einer einmaligen Anmeldung auf die unternehmensweit gehostete Anwendung zugreifen. Das OIDC bietet mehr Sicherheit, indem es kein Benutzerkennwort überträgt, sondern mit Token mit einer bestimmten Lebensdauer arbeitet. OIDC wurde auch für die Integration in Nicht-Browser-Clients wie Apps und Dienste entwickelt. Daher verwenden viele Implementierungen OIDC in großem Umfang.

Vorteile der Unterstützung von OpenID Connect

- OIDC eliminiert den Aufwand für die Pflege mehrerer Authentifizierungskennwörter, da der Benutzer über eine einzige Identität im gesamten Unternehmen verfügt.
- OIDC bietet eine robuste Sicherheit für Ihr Kennwort, da das Kennwort nur mit Ihrem Identitätsanbieter und nicht mit einer Anwendung, auf die Sie zugreifen, geteilt wird.
- OIDC verfügt über eine enorme Interoperabilität mit verschiedenen Systemen, was es den gehosteten Anwendungen erleichtert, OpenID zu akzeptieren.
- OIDC ist ein einfaches Protokoll, das es nativen Clients ermöglicht, sich einfach in Server zu integrieren.

So konfigurieren Sie eine NetScaler-Appliance als IdP mithilfe des OpenID Connect-Protokolls über die GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > OAuth IdP**.
2. Klicken Sie auf **Profil** und dann auf **Hinzufügen.**

   Legen Sie im Bildschirm **Authentifizierung erstellen OAuth IDP-Profil** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.

   - **Name** — Name des Authentifizierungsprofils.
   - **Client-ID** — Eindeutige Zeichenfolge, die SP identifiziert.
   - **Client Secret** — Eindeutiges Geheimnis, das SP identifiziert.
   - **URL umleiten** — Endpunkt für SP, an dem Code/Token gepostet werden muss.
   - **Name des Ausstellers** — Zeichenfolge, die IdP identifiziert.
   - **Zielgruppe** — Zielempfänger für das Token, das vom IdP gesendet wird. Dies könnte vom Empfänger überprüft werden.
   - **Skew Time** — Die Zeit, für die das Token gültig bleibt.
   - **Standardauthentifizierungsgruppe** — Eine Gruppe, die der Sitzung für dieses Profil hinzugefügt wurde, um die Richtlinienbewertung zu vereinfachen und beim Anpassen

von Richtlinien zu helfen.

3. Klicken Sie auf **Richtlinien**, und klicken Sie auf **Hinzufügen.**
4. Legen Sie im Fenster **Richtlinie für OAuth IDP-Authentifizierung erstellen** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
   - **Name —** Der Name der Authentifizierungsrichtlinie.
   - **Aktion** — Name des zuvor erstellten Profils.
   - **Protokollaktion — Name der Aktion** des Nachrichtenprotokolls, die verwendet werden soll, wenn eine Anforderung dieser Richtlinie entspricht. Keine obligatorische Einreichung.
   - Aktion mit**undefiniertem Ergebnis — Aktion**, die ausgeführt werden soll, wenn das Ergebnis der Richtlinienbewertung nicht bestraft wird (UNDEF). Kein Pflichtfeld.
   - **Ausdruck** — Erweiterter Richtlinienausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Beispiel: true.
   - **Comments:** Kommentare zu der Richtlinie.

Binden der OAuthIDP-Richtlinie und der LDAP-Richtlinie an den virtuellen Authentifizierungsserver

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > LDAP**.
2. Klicken Sie im Bildschirm **LDAP-Aktionen** auf **Hinzufügen**.
3. Legen **Sie auf dem Bildschirm Create Authentication LDAP-Server** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
   - **Name —** Der Name der LDAP-Aktion
   - **Servername/ServerIP —** Bereitstellung von FQDN oder IP des LDAP-Servers
   - Wählen Sie geeignete Werte **für Sicherheitstyp, Port, Servertyp, Timeout**
   - Stellen Sie sicher, dass **Authentifizierung** aktiviert ist
   - **Basis-DN —** Basis, von der aus die LDAP-Suche gestartet werden soll. Zum Beispiel dc=aaa, dc = local.
   - **Administrator Bind DN:** Benutzername der Bindung an den LDAP-Server. Zum Beispiel admin@aaa.local.
   - **Administratorkennwort/Kennwort bestätigen: Kennwort zum Binden von LDAP**
   - Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen zu testen.
   - **Attribut für Server-Anmeldename:** Wählen Sie **“sAMAccountName”**
   - Andere Felder sind nicht Pflichtfelder und können daher nach Bedarf konfiguriert werden.
4. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie.**

5. Klicken Sie auf dem Bildschirm **Authentifizierungsrichtlinien** auf **Hinzufügen**.
6. Legen **Sie auf der Seite Authentifizierungsrichtlinie erstellen** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen.**
    - **Name —** Name der LDAP-Authentifizierungsrichtlinie.
    - **Aktionstyp —** Wählen Sie **LDAP aus.**
    - **Aktion —** Wählen Sie die LDAP-Aktion aus.
    - **Ausdruck —** Erweiterter Richtlinienausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Beispiel: true**.

So konfigurieren Sie die NetScaler-Appliance als IdP mithilfe des OpenID Connect-Protokolls mithilfe von CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add authentication OAuthIDPProfile <name> [-clientID <string>][-clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]<!--NeedCopy-->`
- `add authentication OAuthIdPPolicy <name> -rule <expression> [-action <string> [-undefAction <string>] [-comment <string>][-logAction <string >]<!--NeedCopy-->`
- `add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -ldapBase "dc=aaa,dc=local"<!--NeedCopy-->`
- `ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -ldapLoginName sAMAccountName<!--NeedCopy-->`
- `add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-act<!--NeedCopy-->`
- `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT<!--NeedCopy-->`
- `bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -priority 5 -gotoPriorityExpression END<!--NeedCopy-->`
- `bind vpn global -certkey <><!--NeedCopy-->`

> **Hinweis**
>
> Sie können mehr als einen Schlüssel binden. Öffentliche Teile von Zertifikaten, die gebunden sind, werden als Antwort auf gesendet `jwks\\_uri query (https://gw/oauth/idp/certs)`.

NetScaler als OAuth SP

May 11, 2023

Die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion zur Verkehrsverwaltung unterstützt die OAuth-Authentifizierung zur Authentifizierung von Benutzern gegenüber Anwendungen, die auf Anwendungen wie Google, Facebook und Twitter gehostet werden.

Wichtige Hinweise

- NetScaler Advanced Edition und höher ist erforderlich, damit die Lösung funktioniert.
- OAuth auf der NetScaler Appliance ist für alle SAML-IdPs qualifiziert, die mit “OpenID Connect 2.0” kompatibel sind.

> **Wichtig:**
>
> Die NetScaler Appliance reagiert möglicherweise mit einem CSRF-Fehler, wenn eine inhaltsreiche Website nach Ablauf der Sitzung mehrere Authentifizierungsanforderungen sendet. Als Problemumgehung wird empfohlen, dass Sie bei der Konfiguration der OAuth-Richtlinie sicherstellen, dass die Richtlinie sowohl für den Hostnamen als auch für den Pfad konfiguriert ist, die die Haupteintrittspunkte sind.

Konfigurieren von OAuth über die GUI

1. Konfigurieren Sie die OAuth -Aktion und -Richtlinie.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**, erstellen Sie eine Richtlinie mit OAuth als Aktionstyp, und verknüpfen Sie die erforderliche OAuth-Aktion mit der Richtlinie.

2. Ordnen Sie die OAuth-Richtlinie einem virtuellen Authentifizierungsserver zu.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Virtuelle Server**, und ordnen Sie die OAuth-Richtlinie dem virtuellen Authentifizierungsserver zu.

> **Hinweis:**
>
> Attribute (1 bis 16) können in der OAuth-Antwort extrahiert werden. Derzeit werden diese Attribute nicht ausgewertet. Sie werden zur zukünftigen Bezugnahme hinzugefügt.

Konfigurieren von OAuth über die CLI

1. Definieren Sie eine OAuth-Aktion.


```
add authentication OAuthAction <name> -authorizationEndpoint <URL>
     -tokenEndpoint <URL> [-idtokenDecryptEndpoint <URL>] -clientID
     <string> -clientSecret <string> [-defaultAuthenticationGroup <
    string>][-tenantID <string>][-GraphEndpoint <string>][-
    refreshInterval <positive_integer>] [-CertEndpoint <string>][-
    audience <string>][-userNameField <string>][-skewTime <mins>][-
    issuer <string>][-Attribute1 <string>][-Attribute2 <string>][-
    Attribute3 <string>]
<!--NeedCopy-->
```

2. Ordnen Sie die Aktion einer erweiterten Authentifizierungsrichtlinie zu.

```
add authentication Policy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Beispiel:

```
add authentication oauthAction a -authorizationEndpoint https://
    example.com/ -tokenEndpoint https://example.com/ -clientiD sadf
     -clientsecret df
<!--NeedCopy-->
```

Weitere Informationen zur Authentifizierung von OAuthAction-Parametern finden Sie unter Authentifizierung OAuthAction.

> **Hinweis:**
>
> Wenn ein CertEndPoint angegeben wird, fragt die NetScaler Appliance diesen Endpunkt mit der konfigurierten Frequenz ab, um die Schlüssel zu lernen.

Um einen NetScaler so zu konfigurieren, dass er die lokale Datei liest und Schlüssel aus dieser Datei analysiert, wird eine neue Konfigurationsoption wie folgt eingeführt:

```
set authentication OAuthAction <> -CertFilePath <path to local file
    with jwks>
<!--NeedCopy-->
```

Die OAuth-Funktion unterstützt jetzt die folgenden Funktionen in der Token-API von Relying Party (RP) und von der IdP-Seite von NetScaler Gateway und NetScaler.

- Unterstützung von PKCE (Proof Key for Code Exchange)
- Unterstützung für client_assertion

Unterstützung von Name-Wert-Attributen für OAuth-Authentifizierung

Sie können jetzt OAuth-Authentifizierungsattribute mit einem eindeutigen Namen zusammen mit den Werten konfigurieren. Die Namen werden im Aktionsparameter von OAuth entweder als "Attribute" konfiguriert und die Werte werden durch Abfragen der Namen abgerufen. Die extrahierten Attribute werden in der Authentifizierungs-, Autorisierungs- und Überwachungssitzung gespeichert. Administratoren können diese Attribute entweder mit `http.req.user.attribute("attribute name")` oder `http.req.user.attribute(1)` abfragen, basierend auf der ausgewählten Methode zur Angabe von Attributnamen.

Durch Angabe des Attributnamens können Administratoren einfach nach dem Attributwert suchen, der mit diesem Attributnamen verknüpft ist. Außerdem müssen sich Administratoren das "attribute1 to attribute16" nicht mehr allein anhand seiner Nummer merken.

> **Wichtig**
>
> In einem OAuth-Befehl können Sie maximal 64 durch Komma getrennte Attribute mit einer Gesamtgröße von weniger als 1024 Byte konfigurieren.
>
> **Hinweis**
>
> Der Sitzungsfehler kann vermieden werden, wenn die Gesamtwertgröße von "Attribut 1 bis Attribut 16" und die Werte der in "Attribute" angegebenen Attribute nicht mehr als 10 KB betragen.

So konfigurieren Sie die Name-Wert-Attribute mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication OAuthAction <name> [-Attributes <string>]

set authentication OAuthAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Beispiele:

```
add authentication OAuthAction a1  - attributes "email,company"  -
    attribute1 email

set authentication OAuthAction oAuthAct1 -attributes "mail,sn,
    userprincipalName"
<!--NeedCopy-->
```


NetScaler als OAuth IdP

September 18, 2023

Eine NetScaler-Appliance kann jetzt mithilfe des OpenID-Connect (OIDC) -Protokolls als Identitätsanbieter konfiguriert werden. Das OIDC-Protokoll stärkt die Funktionen zur Identitätsbereitstellung der NetScaler-Appliance. Sie können jetzt mit einem Single Sign-On auf die unternehmensweit gehostete Anwendung zugreifen, da OIDC mehr Sicherheit bietet, indem das Benutzerkennwort nicht übertragen wird, sondern Token mit einer bestimmten Lebensdauer verwendet werden. OpenID wurde auch für die Integration mit Nicht-Browser-Clients wie Apps und Diensten entwickelt. Daher wird das OIDC-Protokoll von vielen Implementierungen weitgehend übernommen.

> **Hinweis**
>
> NetScaler muss sich auf Version 12.1 oder höher befinden, damit die Appliance unter Verwendung des OIDC-Protokolls als OAuth-IdP funktioniert.

Vorteile der Verwendung von NetScaler als OAuth IdP

- Eliminiert den Aufwand für die Pflege mehrerer Authentifizierungskennwörter, da der Benutzer über eine einzige Identität in einer Organisation verfügt.
- Bietet eine robuste Sicherheit für Ihr Kennwort, da das Kennwort nur mit Ihrem Identitätsanbieter und nicht mit einer Anwendung, auf die Sie zugreifen, freigegeben wird.
- Bietet umfassende Interoperabilität mit verschiedenen Systemen und erleichtert es den gehosteten Anwendungen, OpenID zu akzeptieren.

> **Hinweis**
>
> NetScaler Advanced Edition und höher ist erforderlich, damit die Lösung funktioniert.

So konfigurieren Sie die NetScaler-Appliance mit der GUI als OAuth IdP

1. Erstellen Sie eine OAuth-IdP-Authentifizierungsrichtlinie.
    - Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > OAuth IDP**> Richtlinien.
    - Klicken Sie unter **Richtlinien**auf **Hinzufügen**.
    - **Legen Sie auf der Seite**Create Authentication OAuth IDP Policy**Werte für die folgenden Parameter fest und klicken Sie auf Create.**
        - Name: Der Name der Authentifizierungsrichtlinie.

- Aktion: Name des Authentifizierungs-OAuth-IdP-Profilprofils, das auf Anfragen oder Verbindungen angewendet werden soll, die dieser Richtlinie entsprechen. Ausführliche Schritte finden Sie in Schritt 2.
- Protokollaktion: Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anfrage dieser Richtlinie entspricht. Ausführliche Schritte finden Sie in Schritt 3. Das Feld ist optional.
- Aktion mit undefiniertem Ergebnis: Aktion, die durchgeführt werden muss, wenn das Ergebnis der Richtlinienbewertung nicht definiert ist. Ein undefiniertes Ereignis weist auf einen internen Fehler hin. Verfügbare Aktionen sind DROP und RESET. Das Feld ist optional.
- Ausdruck: Erweiterter Ausdruck, den die Richtlinie verwendet, um auf bestimmte Anfragen zu antworten. Weitere Informationen zu Richtlinien und Ausdrücken finden Sie unter Richtlinien und Ausdrücke.

2. Erstellen Sie eine OAuth-IdP-Authentifizierungsaktion.

   - **Klicken Sie auf der Seite**Create Authentication OAuth IDP Policy**im Feld**Aktion auf Hinzufügen**.**
   - **Legen Sie auf der daraufhin angezeigten Seite**Create Authentication OAuth IDP Profile**Werte für die folgenden Parameter fest und klicken Sie auf Create.**
     - Name: Name für das neue OAuth-IdP-Single-Sign-On-Profil.
     - Client-ID: Eindeutige Identität der vertrauenden Partei, die die Authentifizierung anfordert. Die maximal zulässige Länge beträgt 127 Zeichen.
     - Client Secret: Eindeutige geheime Zeichenfolge zur Autorisierung der vertrauenden Partei auf dem Autorisierungsserver. Die maximal zulässige Länge beträgt 239 Zeichen.
     - Umleitungs-URL: Der URL-Endpunkt der vertrauenden Partei, an den das OAuth-Token gesendet werden muss. Die maximal zulässige Länge beträgt 255 Zeichen.
     - Name des Ausstellers: Der Name, der in Anfragen verwendet werden soll, die von NetScaler an den IdP gesendet werden, um NetScaler eindeutig zu identifizieren. Die maximal zulässige Länge beträgt 127 Zeichen.
     - Zielgruppe: Zielempfänger für das Token, das vom IdP gesendet wird. Dies ist der Entitätsname oder die URL, die den Empfänger darstellt. Die maximal zulässige Länge beträgt 127 Zeichen.
     - Skew Time: Diese Option gibt die Dauer an, für die das vom NetScaler IdP gesendete Token gültig ist. Wenn die Schräglaufzeit beispielsweise auf 10 Minuten festgelegt ist, wäre das Token gültig von (aktuelle Zeit minus 10) Minuten bis (aktuelle Zeit plus 10) Minuten, also insgesamt 20 Minuten. Die Standarddauer beträgt 5 Minuten.
     - Standardauthentifizierungsgruppe: Gruppe, die der internen Gruppenliste der Sitzung hinzugefügt wurde. Dies ist nützlich für Administratoren, um die Kon-

figuration für die vertrauende Partei in einem nFactor-Flow zu bestimmen. Es kann im Ausdruck `AAA.USER.IS_MEMBER_OF("group name")` für Authentifizierungsrichtlinien verwendet werden, um den nFactor-Flow zu identifizieren, der sich auf die vertrauende Partei bezieht. Die maximal zulässige Länge beträgt 63 Zeichen.

- Metadaten-URL der vertrauenden Partei: Endpunkt, an dem der NetScaler IdP Details zur Konfiguration der vertrauenden Partei abrufen kann. Die Metadatenantwort muss Endpunkte `jwks_uri` für öffentliche Schlüssel der vertrauenden Partei enthalten. Die maximal zulässige Länge beträgt 255 Zeichen.
- Aktualisierungsintervall: Intervalle, in denen die Metadaten der vertrauenden Partei aktualisiert werden.
- Signature Service: Wählen Sie diese Option, um das Token zu verschlüsseln, wenn der NetScaler IdP eines sendet.
- Attribute: Name-Wert-Attributpaare, die in das ID-Token eingefügt werden sollen. Das Konfigurationsformat ist `name=value_expr@@@name2=value2_expr@@@`. Das `@@@` Format wird als Trennzeichen zwischen den Name-Wert-Paaren verwendet.
- Passwort senden: Wählen Sie diese Option, um das verschlüsselte Passwort im ID-Token zu senden.

3. Erstellen Sie eine Überwachungsnachrichtenaktion.
   - Klicken Sie auf der Seite **Create Authentication OAuth IDP Policy** im Feld **Log** Action auf **Hinzufügen** .
   - Legen Sie auf der Seite „ **Audit-Meldungsaktion erstellen** “ Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
     - Name: Name der Aktion für die Überwachungsnachricht.
     - Protokollebene: Audit-Protokollebene, die den Schweregrad der generierten Protokollnachricht angibt.
     - Ausdruck: Standard-Syntaxausdruck, der das Format und den Inhalt der Protokollnachricht definiert.
     - In newnslog einloggen: Sendet die Nachricht an den neuen NSLOG-Server.
4. Erstellen Sie einen OAuth-Authentifizierungsserver.
   - **Navigieren Sie zu**Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > OAUTH-Aktionen**und klicken Sie auf Hinzufügen.**
   - **Legen Sie auf der Seite**Create Authentication OAuth Server**Werte für die erforderlichen Parameter fest und klicken Sie auf Erstellen.**
5. Binden Sie die OAuth-IdP-Richtlinie an den Authentifizierungs-OAuth-Server.

Die OAuth-Funktion unterstützt jetzt die folgenden Funktionen in der Token-API von Relying Party (RP) und von der IdP-Seite von NetScaler Gateway und NetScaler.

- Unterstützung von PKCE (Proof Key for Code Exchange)
- Unterstützung für client_assertion

So konfigurieren Sie die NetScaler-Appliance als IdP mithilfe des OIDC-Protokolls mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <string>] [-undefAction <string>] [-comment <string>][-logAction <string>]

add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -ldapBase "dc=aaa,dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -ldapLoginName sAMAccountName

add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-act

bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -priority 5 -gotoPriorityExpression END

bind vpn global  - certkey <>
<!--NeedCopy-->
```

Hinweise:

- Sie können mehr als einen Schlüssel binden. Öffentliche Teile von Zertifikaten, die gebunden sind, werden als Antwort auf gesendet `jwks\\_uri query (https://gw/oauth/idp/certs)`.
- Der introspektive OAuth-IdP-Endpunkt unterstützt die Eigenschaft `active: true`.
- Wenn der virtuelle Authentifizierungsserver als OAuth-IdP konfiguriert ist, muss die bekannte URL des OAuth-IdP-Discovery-Endpunkts angegeben werden. `https://<netscaler`


```
    -oauth-idp-fqdn>/oauth/idp/.well-known/openid-configuration
```

Unterstützung von verschlüsselten Token im OIDC-Protokoll

Die NetScaler-Appliance mit dem OIDC-Mechanismus unterstützt jetzt das Senden von verschlüsselten Token zusammen mit signierten Token. Die NetScaler-Appliance verwendet JSON-Webverschlüsselungsspezifikationen zur Berechnung der verschlüsselten Token und unterstützt nur die kompakte Serialisierung von verschlüsselten Token. Um ein OpenID-Token zu verschlüsseln, benötigt eine NetScaler-Appliance den öffentlichen Schlüssel der angehörenden Partei (RP). Der öffentliche Schlüssel wird dynamisch abgerufen, indem der bekannte Konfigurationsendpunkt der vertrauenden Partei abgefragt wird.

Eine neue Option “relyingPartyMetadataURL” wurde im Profil “authentication OAuthIDPProfile” eingeführt.

So konfigurieren Sie den Endpunkt der vertrauenden Partei mithilfe von CLI

Geben Sie an der Befehlszeile Folgendes ein:

```
set authentication OAuthIDPProfile <name> [-relyingPartyMetadataURL <
    URL>] [-refreshInterval <mins>] [-status < >]
<!--NeedCopy-->
```

- **relyingPartyMetadataURL** - Endpunkt, an dem NetScaler IdP Details über die konfigurierte Anbietergesellschaft abrufen kann. Die Metadatenantwort muss Endpunkte für jwks_uri für öffentliche RP-Schlüssel enthalten.
- **refreshInterval** - Definiert die Rate, mit der dieser Endpunkt abgefragt werden muss, um die Zertifikate in Minuten zu aktualisieren.
- **status** - Spiegelt den Status des Abrufvorgangs wider. Der Status ist abgeschlossen, sobald die NetScaler-Appliance die öffentlichen Schlüssel erfolgreich abgerufen hat.

Beispiel,

```
set authentication OAuthIDPProfile sample_profile -
    relyingPartyMetadataURL https://rp.customer.com/metadata -
    refreshInterval 50 -status < >
<!--NeedCopy-->
```

Nachdem der Endpunkt konfiguriert wurde, fragt eine NetScaler-Appliance zunächst den bekannten Endpunkt der vertrauenden Partei ab, um die Konfiguration zu lesen. Derzeit verarbeitet die NetScaler-Appliance nur den Endpunkt “jwks_uri”.

- Wenn ‘jwks_uri’ in der Antwort nicht vorhanden ist, ist der Status des Profils nicht vollständig.

- Wenn “jwks_uri” in der Antwort vorhanden ist, fragt NetScaler diesen Endpunkt auch ab, um die öffentlichen Schlüssel der vertrauenden Partei zu lesen.

> **Hinweis:**
>
> Für die Token-Verschlüsselung werden nur RSAES-OAEP- und AES256-GCM-Verschlüsselungsalgorithmen unterstützt.

Unterstützung von benutzerdefinierten Attributen auf OpenID Connect

Die OpenID vertrauenden Parteien benötigen möglicherweise mehr als einen Benutzernamen oder einen Benutzerprinzipalnamen (UPN) im Token, um das Benutzerprofil zu erstellen oder Autorisierungsentscheidungen zu treffen. In den meisten Fällen müssen die Benutzergruppen Autorisierungsrichtlinien für den Benutzer anwenden. Manchmal sind weitere Details wie der Vor- oder Nachname für die Bereitstellung eines Benutzerkontos erforderlich.

NetScaler-Appliance, die als IdP konfiguriert ist, kann verwendet werden, um zusätzliche Attribute im OIDCid_token über Ausdrücke zu senden. Erweiterte Richtlinienausdrücke werden verwendet, um die benutzerdefinierten Attribute gemäß der Anforderung zu senden. Der Citrix IdP wertet die Ausdrücke aus, die den Attributen entsprechen, und berechnet dann das endgültige Token.

NetScaler-Appliance wendet automatisch JSONify auf die Ausgabedaten an. Beispielsweise sind Zahlen (wie SSN) oder boolesche Werte (true oder false) nicht von Anführungszeichen umgeben. Mehrwertige Attribute, wie Gruppen, werden innerhalb einer Array-Markierung platziert (“[” und “]”). Die komplexen Typattribute werden nicht automatisch berechnet, und Sie können den PI-Ausdruck dieser komplexen Werte entsprechend Ihrer Anforderung konfigurieren.

So konfigurieren Sie den Endpunkt der vertrauenden Partei mithilfe von CLI

Geben Sie an der Befehlszeile Folgendes ein:

```
set oauthidpprofile <name> -attributes <AAA-custom-attribute-pattern>
<!--NeedCopy-->
```

Die<AAA-custom-attribute-pattern> kann beschrieben werden als:

Attribute1=PI-Expression@@@attribute2=PI-Expression@@@

‘attribute1’, ‘attribute2’ sind literale Zeichenketten, die den Namen des Attributs darstellen, das in das ID-Token eingefügt werden soll.

> **Hinweis:**
>
> Sie können bis zu 2.000 Byte an Attributen konfigurieren.
>
> Beispiel:


```
set oauthidpprofile sample_1 -attributes q{ myname=http.req.user.name@@@ssn
="123456789"@@@jit="false"@@@groups=http.req.user.groups }
```

- Der vorangegangene PI-Ausdruck ist ein erweiterter Richtlinienausdruck, der den Wert darstellt, der für das Attribut verwendet werden soll. Der PI-Ausdruck kann verwendet werden, um ein Zeichenfolgenliteral zu senden, z. B. "'hartcodierte String"'. Das Zeichenkettenliteral ist von doppelten Anführungszeichen um einfache Anführungszeichen oder um doppelte Anführungszeichen um einen Anfang und ein Muster umgeben, wie bereits erwähnt, das Startmuster ist „q ()". Wenn der Wert des Attributs kein String-Literal ist, wird der Ausdruck zur Laufzeit ausgewertet und sein Wert wird im Token gesendet. Wenn der Wert zur Laufzeit leer ist, wird das entsprechende Attribut dem ID-Token nicht hinzugefügt.
- Wie im Beispiel definiert, ist "false" eine literale Zeichenfolge für das Attribut "jit". "ssn" hat auch einen fest codierten Referenzwert. Gruppen und "myname" sind PI-Ausdrücke, die Zeichenfolgen ergeben.

Unterstützung für aktiv-aktive GSLB-Bereitstellungen auf NetScaler Gateway

NetScaler Gateway, das mit dem OIDC-Protokoll als Identity Provider (IdP) konfiguriert ist, kann aktiv-aktive GSLB-Bereitstellungen unterstützen. Die aktiv-aktive GSLB-Bereitstellung auf dem NetScaler Gateway IdP ermöglicht den Lastausgleich einer eingehenden Benutzeranmeldeanforderung an mehreren geografischen Standorten.

Wichtig

Wir empfehlen Ihnen, CA-Zertifikate an den SSL-Dienst zu binden und die Zertifikatsvalidierung für den SSL-Dienst zu aktivieren, um die Sicherheit zu erhöhen.
Weitere Informationen zur Konfiguration des GSLB-Setups finden Sie unter Beispiel für ein GSLB-Setup und eineKonfiguration.

API-Authentifizierung mit der NetScaler Appliance

September 11, 2023

Es gibt einen Paradigmenwechsel in der Art und Weise, wie moderne Anwendungen mit ihren Kunden interagieren. Traditionell wurden Browserclients für den Zugriff auf Dienste verwendet. Anwendungen setzen Sitzungscookies, um den Benutzerkontext zu verfolgen. Moderne und verteilte Anwendungen machen es schwierig, Benutzersitzungen über Microservices hinweg aufrechtzuerhalten. Aus diesem Grund sind die meisten Anwendungszugriffe API-basiert geworden.
Die Clients, die mit diesen verteilten Diensten kommunizieren, haben sich ebenfalls weiterentwickelt. Die meisten Clients erhalten Token von einer vertrauenswürdigen Entität namens Authorization

Server, um Benutzeridentität und Zugriff nachzuweisen. Diese Clients präsentieren der Anwendung dann das Token bei jeder Zugriffsanforderung. Daher müssen herkömmliche Proxygeräte wie NetScaler weiterentwickelt werden, um diese Clients zu unterstützen. Eine NetScaler Appliance bietet Administratoren die Möglichkeit, solchen Datenverkehr zu handhaben. NetScaler kann als API-Gateway bereitgestellt werden, um den gesamten Datenverkehr, der für die veröffentlichten Dienste bestimmt ist, als Frontend bereitzustellen. Ein API-Gateway kann für traditionelle (Hybrid Multi Cloud oder HMC) oder Cloud-native Umgebungen eingesetzt werden. Das API-Gateway beendet den gesamten eingehenden Datenverkehr, um verschiedene Dienste wie Authentifizierung, Autorisierung, Ratenbegrenzung, Routing, Caching, SSL-Offload, Anwendungsfirewall usw. anzubieten. Daher wird es zu einer kritischen Komponente in der Infrastruktur.

Token-Typen

Tokens, die während des API-Zugriffs ausgetauscht werden, entsprechen größtenteils dem OAuth/OpenID Connect (OIDC) -Protokoll. Zugriffstoken, die nur für "delegierten Zugriff" verwendet werden, entsprechen dem OAuth-Protokoll, während ID-Token, die OIDC entsprechen, ebenfalls Benutzerinformationen enthalten.
Zugriffstoken sind normalerweise ein undurchsichtiger oder zufälliger Datenblock. Manchmal können sie jedoch signierte Token sein, die den JWT-Standards (JSON Web Token) entsprechen. ID-Token sind immer signierte JWTs.

API-Zugriff mit OAuth

Der OAuth-Authentifizierungstyp auf einer NetScaler Appliance kann verwendet werden, um sowohl OAuth- als auch OIDC-Protokolle zu verarbeiten. OIDC ist eine Erweiterung des OAuth-Protokolls.

OAuthAction auf einer NetScaler Appliance kann verwendet werden, um interaktive Clients wie Browser und native Clients wie Client-Apps zu verwalten. Interaktive Clients werden zur Anmeldung über das OIDC-Protokoll an den Identity Provider umgeleitet. Systemeigene Clients können Tokens Out-of-Band-Token abrufen und diese Token auf einer NetScaler Appliance für den Zugriff präsentieren.

> **Hinweis:**
>
> Das von Endpunkten erhaltene Zugriffstoken kann für nachfolgende Anfragen zwischengespeichert werden, wodurch die API-Leistung verbessert wird.

Um die Unterstützung von Token-Caching mithilfe der Befehlszeilenschnittstelle zu konfigurieren, geben Sie an der Befehlszeile den folgenden Befehl ein:

```
set aaaparameter -APITokenCache <ENABLED>
<!--NeedCopy-->
```


In den folgenden Abschnitten wird die API-Zugriffsmethode beschrieben, die von nativen Clients ausgeführt wird.

Virtueller Server für API-Zugriff

Um eine NetScaler-Appliance für einen API-Zugriff bereitzustellen, wird ein virtueller Traffic Management (TM) -Server mit 401-Authentifizierung bereitgestellt. Es ist einem virtuellen Authentifizierungsserver (Authentifizierung, Autorisierung und Prüfung) zugeordnet, auf dem die Authentifizierungs- und Sitzungsrichtlinien gespeichert werden. Der folgende Konfigurationsausschnitt erstellt einen solchen virtuellen Server.

```
Add lb vserver lb-api-access SSL <IP> 443 -authn401 On -AuthnVsName
   auth-api-access

Bind ssl vserver lb-api-access -certkeyName <ssl-cert-entity>

Add authentication vserver auth-api-access SSL
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie müssten einen Dienst an den virtuellen Server für die Verkehrsverwaltung und eine Authentifizierungsrichtlinie (mit OAuthAction wie folgt beschrieben) an den virtuellen Authentifizierungsserver binden, um die Konfiguration abzuschließen.

Nach dem Erstellen des virtuellen Servers muss eine OAuthAction zusammen mit der entsprechenden Richtlinie hinzugefügt werden. Je nach Tokentyp und anderen Sicherheitsmechanismen gibt es innerhalb einer OAuth-Aktion mehrere andere Optionen.

OAuth-Konfiguration für ID-Token

ID-Token sind immer signierte JWTs. Das heißt, sie tragen Header, Payload und Signatur. Da es sich um eigenständige Token handelt, kann eine NetScaler-Appliance diese Token lokal validieren. Um diese Token zu validieren, müsste die Appliance den öffentlichen Schlüssel des entsprechenden privaten Schlüssels kennen, der zum Signieren dieser Token verwendet wird.

Es folgt ein Beispiel für OAuthAction mit bestimmten obligatorischen Argumenten zusammen mit “certEndpoint”.

```
Add authentication OAuthAction oauth-api-access -clientid <your-
   client-id> -clientsecret <your-client-secret> -
   authorizationEndpoint <URL to which users would be redirected for
   login> -tokenEndpoint <endpoint at which tokens could be obtained>
    -certEndpoint <URL at which public keys of IdP are published>
```



```
2    <!--NeedCopy-->
```

Hierbei gilt:

- **Client-ID** — Eindeutige Zeichenfolge, die SP identifiziert. Der Autorisierungsserver leitet die Clientkonfiguration von dieser ID ab. Maximale Länge: 127.
- **Client Secret:** Geheime Zeichenfolge, die vom Benutzer und Autorisierungsserver erstellt wird. Maximale Länge: 239.
- **AuthorizationEndpoint** — URL, unter der sich Benutzer normalerweise anmelden würden (bei Verwendung interaktiver Clients).
- **TokenEndpoint** - URL auf dem Autorisierungsserver, an dem Token/Code abgerufen/ausgetauscht werden
- **CertEndPoint** — URL, unter der der Autorisierungsserver öffentliche Schlüssel veröffentlicht, die zum Signieren der Token verwendet werden. Der Autorisierungsserver kann mehr als einen Schlüssel veröffentlichen und einen davon zum Signieren von Tokens auswählen.

  > **Hinweis:**
  >
  > Client-ID/Client Secret/AuthorizationEndpoint/TokenEndpoint sind optionale Parameter für den API-Zugriff. Es empfiehlt sich jedoch, Werte für diese Parameter anzugeben, da die Aktionsentität für verschiedene Zwecke wiederverwendet werden kann.

In der vorherigen Konfiguration ist ‘certEndpoint’ für die ID-Token-Validierung unerlässlich. Dieser Endpunkt enthält öffentliche Schlüssel des Zertifikats, das zum Signieren der Token verwendet wurde. Diese öffentlichen Schlüssel müssen der JWK-Spezifikation (JSON Web Keys) entsprechen.

Sobald der CertEndpoint auf der NetScaler Appliance konfiguriert ist, fragt er den Endpoint regelmäßig ab (mit dem Standardintervall von 1 Tag, das in der Konfiguration angepasst werden kann), um die öffentlichen Schlüssel auf dem neuesten Stand zu halten. Nachdem die öffentlichen Schlüssel verfügbar sind, kann ADC eine lokale Validierung der eingehenden ID-Token durchführen.

OAuth-Konfiguration für undurchsichtige Zugriffstoken

Undurchsichtige Token können nicht lokal auf der NetScaler Appliance verifiziert werden. Diese müssen auf dem Autorisierungsserver validiert werden. Eine NetScaler Appliance verwendet das in den OAuth-Spezifikationen erwähnte „Introspection Protocol“, um diese Token zu verifizieren. In der OAuth-Konfiguration steht eine neue Option, introspecturL, zur Überprüfung undurchsichtiger Token zur Verfügung.

```
1    set oauthAction oauth-api-acccess -introspectURL <URL of the
        Authorization Server for introspection>
2    <!--NeedCopy-->
```


Das Format der Introspection-API entspricht der Spezifikation unter https://tools.ietf.org/html/rfc7662##section-2.1 wie folgt:

```
POST /introspect HTTP/1.1
Host: server.example.com
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
token=mF_9.B5f-4.1JqM&token_type_hint=access_token
<!--NeedCopy-->
```

Bindungsrichtlinie an den virtuellen Authentifizierungsserver

Sobald OAuthAction erstellt wurde, muss eine entsprechende Richtlinie für den Aufruf erstellt werden.

```
add authentication policy oauth-api-access -rule <> -action <oauth-
   api-access>

bind authentication vserver auth-api-access -policy oauth-api-access
   -pri 100
<!--NeedCopy-->
```

Zusätzliche Sicherheitseinstellungen auf einer NetScaler Appliance

Die Token-Validierung umfasst Überprüfungen der Token-Lebensdauer. Tokens außerhalb der akzeptablen Zeit werden abgelehnt. Im Folgenden finden Sie die zusätzlichen Einstellungen für zusätzliche Sicherheit. Es wird empfohlen, einige davon immer zu konfigurieren.

Zielgruppe: OAuth Action kann mit einem vorgesehenen Empfänger des Tokens konfiguriert werden. Alle Token werden mit dieser konfigurierten URL abgeglichen. Eine NetScaler-Appliance verfügt über eine zusätzliche Funktion, bei der das Zielgruppenfeld tatsächlich auf ein auf der Appliance festgelegtes Muster verweist. Mithilfe dieses Mustersatzes kann ein Administrator mehr als eine URL für die Zielgruppe konfigurieren.

```
add policy patset oauth_audiences

bind patset oauth_audiences https://app1.company.com

bind patset oauth_audiences https://app2.company.com

bind patset oauth_audiences httpsL//app1.company.com/path1

set oAuthAction oauth-api-access -audience oauth_audiences
```



```
10    <!--NeedCopy-->
```

Im vorherigen Beispiel wurde mehr als eine Zielgruppe in einem Mustersatz angegeben. Daher ist ein eingehendes Token nur zulässig, wenn es eine der konfigurierten URLs im Mustersatz enthält.

Aussteller: Identität des Servers, dessen Tokens akzeptiert werden sollen. Maximale Länge: 127. Es empfiehlt sich, den Aussteller der Token in OAuth-Aktion zu konfigurieren. Dadurch wird sichergestellt, dass vom falschen Autorisierungsserver ausgegebene Token nicht zulässig sind.

SkewTime: Gibt den zulässigen Taktversatz in der Anzahl der Minuten an, den eine NetScaler Appliance für ein eingehendes Token zulässt. Wenn SkewTime beispielsweise 10 ist, dann wäre das Token von (aktuelle Zeit — 10) Minuten bis (aktuelle Zeit + 10) Minuten gültig, also insgesamt 20 Minuten. Standardwert: 5

AllowedAlgorithms: Mit dieser Option kann der Administrator bestimmte Algorithmen in den eingehenden Tokens einschränken. Standardmäßig sind alle unterstützten Methoden zulässig. Diese können jedoch mit dieser Option gesteuert werden.

Die folgende Konfiguration stellt sicher, dass nur Token zulässig sind, die RS256 und RS512 verwenden:

```
1    set oAuthAction oauth-api-access -allowedAlgorithms RS256 RS512
2    <!--NeedCopy-->
```

Nachdem die vorherige Konfiguration durchgeführt wurde, sind nur Token zulässig, die RS256 und RS512 verwenden.

Umgehen von bestimmtem Datenverkehr bei der Authentifizierung

In vielen Fällen gibt es einige Discovery-APIs, auf die die Clients öffentlich zugreifen können. Diese APIs enthüllen in der Regel die Konfiguration und die Funktionen des Dienstes selbst. Ein Administrator kann die NetScaler Appliance so konfigurieren, dass die Authentifizierung über diese Metadaten-URLs mithilfe der Richtlinie „Keine Authentifizierung“ Bypass wird, die wie folgt beschrieben wird:

```
1    add authentication policy auth-bypass-policy -rule <> -action
        NO_AUTHN
2
3    bind authentication vserver auth-api-access -policy auth-bypass-
        policy -pri 110
4    <!--NeedCopy-->
```

NO_AUTHN ist eine implizite Aktion, die dazu führt, dass die Authentifizierung abgeschlossen wird, wenn die Regel zutrifft. Es gibt andere Verwendungsmöglichkeiten der NO_AUTHN-Aktion, die über den API-Zugriff hinausgehen.

LDAP-Authentifizierung

June 19, 2023

Wie bei anderen Arten von Authentifizierungsrichtlinien umfasst eine LDAP-Authentifizierungsrichtlinie (Lightweight Directory Access Protocol) einen Ausdruck und eine Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, bezeichnen Sie es auch als primäre oder sekundäre Richtlinie. Zusätzlich zu den Standardauthentifizierungsfunktionen kann LDAP auch andere Active Directory-Server (AD) nach Benutzerkonten für Benutzer durchsuchen, die nicht lokal existieren. Diese Funktion wird als Empfehlungsunterstützung oder Empfehlungsjagd bezeichnet.

Normalerweise konfigurieren Sie den NetScaler so, dass er die IP-Adresse des Authentifizierungsservers während der Authentifizierung verwendet. Mit LDAP-Authentifizierungsservern können Sie den ADC auch so konfigurieren, dass er den FQDN des LDAP-Servers anstelle seiner IP-Adresse verwendet, um Benutzer zu authentifizieren. Die Verwendung eines FQDN kann eine ansonsten viel komplexere Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration in Umgebungen vereinfachen, in denen sich der Authentifizierungsserver möglicherweise an einer von mehreren IP-Adressen befindet, aber immer einen einzigen FQDN verwendet. Um die Authentifizierung mithilfe des FQDN eines Servers anstelle seiner IP-Adresse zu konfigurieren, folgen Sie dem normalen Konfigurationsprozess, außer wenn Sie die Authentifizierungsaktion erstellen. Beim Erstellen der Aktion verwenden Sie den **ServerName-Parameter** anstelle des **ServerIP-Parameters** und ersetzen den FQDN des Servers durch seine IP-Adresse.

Bevor Sie entscheiden, ob Sie den ADC so konfigurieren, dass er die IP oder den FQDN Ihres LDAP-Servers zur Authentifizierung von Benutzern verwendet, sollten Sie bedenken, dass die Konfiguration von Authentifizierung, Autorisierung und Überwachung zur Authentifizierung bei einem FQDN anstelle einer IP-Adresse einen zusätzlichen Schritt zum Authentifizierungsprozess darstellt. Jedes Mal, wenn der ADC einen Benutzer authentifiziert, muss er den FQDN auflösen. Wenn sehr viele Benutzer versuchen, sich gleichzeitig zu authentifizieren, verlangsamen die daraus resultierenden DNS-Lookups möglicherweise den Authentifizierungsprozess.

Die LDAP-Empfehlungsunterstützung ist standardmäßig deaktiviert und kann nicht global aktiviert werden. Es muss explizit für jede LDAP-Aktion aktiviert sein. Stellen Sie sicher, dass der AD-Server dieselben akzeptiert `binddn credentials`, die mit dem verweisenden Server (GC) verwendet werden. Um die Empfehlungsunterstützung zu aktivieren, konfigurieren Sie eine LDAP-Aktion, um Verweisen zu folgen, und geben Sie die maximale Anzahl von Empfehlungen an, die folgen sollen.

Wenn die Empfehlungsunterstützung aktiviert ist und der NetScaler eine LDAP_REFERRAL-Antwort auf eine Anforderung erhält, folgt Authentifizierung, Autorisierung und Überwachung der Verweisung an den in der Empfehlung enthaltenen Active Directory-Server (AD) und führt das Update auf diesem Server durch. Zunächst sucht Authentifizierung, Autorisierung und Überwachung

den Empfehlungsserver in DNS und stellt eine Verbindung zu diesem Server her. Wenn die Empfehlungsrichtlinie SSL/TLS erfordert, stellt sie eine Verbindung über SSL/TLS her. Es bindet dann an den neuen Server mit dem `binddn credentials`, den es mit dem vorherigen Server verwendet hat, und führt den Vorgang aus, der die Empfehlung generiert hat. Diese Funktion ist für den Benutzer transparent.

Die Portnummern für LDAP-Verbindungen lauten:

- 389 für unsichere LDAP-Verbindungen (für Nur-Text-LDAP)
- 636 für sichere LDAP-Verbindungen (für SSL LDAP)
- 3268 für unsichere LDAP-Verbindungen von Microsoft (für Global Catalog Server im Klartext)
- 3269 für sichere LDAP-Verbindungen von Microsoft (für SSL Global Catalog Server)

Die folgende Tabelle enthält Beispiele für Benutzerattributfelder für LDAP-Server:

LDAP-Server	Benutzer-Attribut	Case sensitiv
Microsoft Active Directory-Server	sAMAccountName	Nein
Novell eDirectory	ou	Ja
IBM Verzeichnisserver	uid	Ja
Lotus-Domino	CN	Ja
Sun ONE Verzeichnis (ehemals iPlanet)	uid oder cn	Ja

Diese Tabelle enthält Beispiele für den Basis-DN:

LDAP-Server	Basis-DN
Microsoft Active Directory-Server	DC =`citrix`, DC = lokal
Novell eDirectory	ou=Benutzer, ou=dev
IBM Verzeichnisserver	cn=users
Lotus-Domino	OU=Stadt, O=`Citrix`, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	ou = Menschen, dc =`citrix`, dc = com

Die folgende Tabelle enthält Beispiele für Bind-DN:

LDAP-Server	Bind DN
Microsoft Active Directory-Server	CN=Administrator, CN=Benutzer, DC=citrix, DC = lokal
Novell eDirectory	cn=admin, o=citrix
IBM Verzeichnisserver	LDAP_dn
Lotus-Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Weitere Informationen zum Einrichten von Authentifizierungsrichtlinien im Allgemeinen finden Sie unter Authentifizierungsrichtlinien. Weitere Informationen zu NetScaler-Ausdrücken, die in der Richtlinienregel verwendet werden, finden Sie unter Richtlinien und Ausdrücke.

So erstellen Sie einen LDAP-Authentifizierungsserver mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

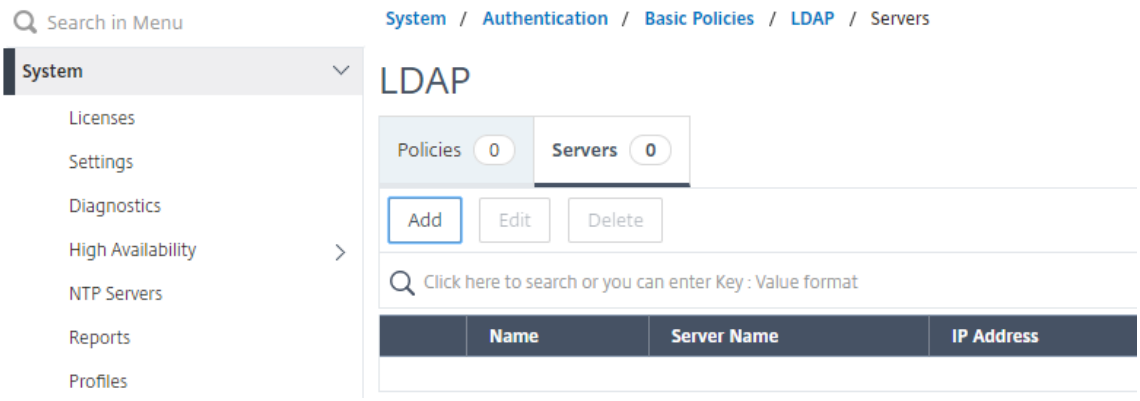
```
add authentication ldapAction <name> {
 -serverIP }
  <ip_addr|ipv6_addr|> | {
 -serverName <string> }
  }
```

Beispiel

```
add authentication ldapAction ldap_server -serverip 1.1.1.1 -serverName
    ldap_test
```

So erstellen Sie einen LDAP-Authentifizierungsserver mit der GUI

1. Navigieren Sie zu **System > Authentifizierung > Grundlegende Richtlinien > LDAP > Server > Hinzufügen**.



2. Konfigurieren Sie auf der Seite **Create Authentication LDAP Server** die Parameter für den LDAP-Server.
3. Klicken Sie auf **Erstellen**.

So aktivieren Sie eine Authentifizierungsrichtlinie mithilfe der CLI

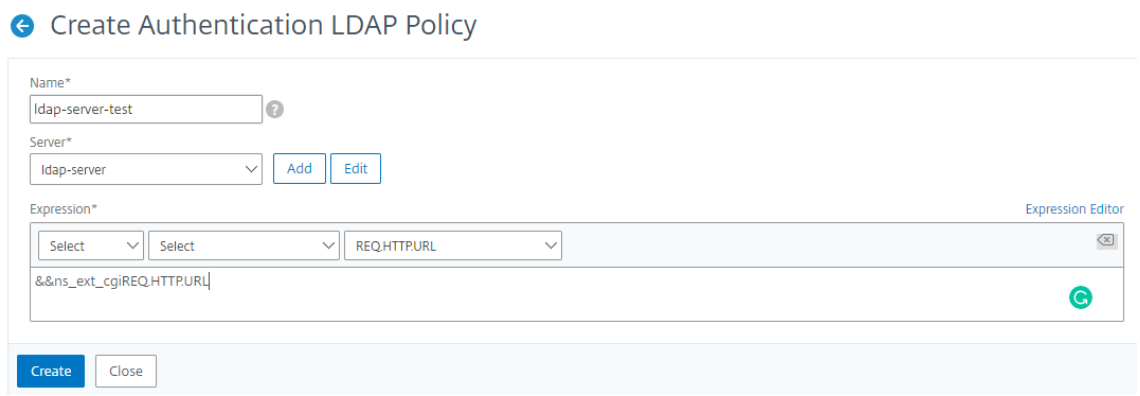
```
add authentication ldappolicy <name> <rule> [<reqAction>]
```

Beispiel:

```
add authentication ldappolicy ldap-service-policy ns_true ldap_Server
```

So erstellen Sie eine LDAP-Authentifizierungsrichtlinie mit der GUI

1. Navigieren Sie zu **System > Authentifizierung > Grundlegende Richtlinien > LDAP > Richtlinien > Hinzufügen**
2. Konfigurieren Sie auf der Seite **LDAP-Authentifizierungsrichtlinie erstellen** die Parameter für die LDAP-Richtlinie.



3. Klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Sie können LDAP-Server/-Richtlinien über die Registerkarte **Sicherheit** konfigurieren. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Grundlegende Richtlinien > LDAP > Server/Richtlinien**.

So aktivieren Sie die LDAP-Empfehlungsunterstützung mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
set authentication ldapAction <name> -followReferrals ON
set authentication ldapAction <name> -maxLDAPReferrals <integer>
<!--NeedCopy-->
```

Beispiel

```
set authentication ldapAction ldapAction-1 -followReferrals ON
set authentication ldapAction ldapAction-1 -maxLDAPReferrals 2
<!--NeedCopy-->
```

Schlüsselbasierte Authentifizierungsunterstützung für die LDAP-Benutzer

Mit der schlüsselbasierten Authentifizierung können Sie jetzt die Liste der öffentlichen Schlüssel abrufen, die auf dem Benutzerobjekt im LDAP-Server über SSH gespeichert sind. Die NetScaler-Appliance muss während des rollenbasierten Authentifizierungsprozesses (RBA) öffentliche SSH-Schlüssel vom LDAP-Server extrahieren. Der abgerufene öffentliche Schlüssel, der mit SSH kompatibel ist, muss es Ihnen ermöglichen, sich über die RBA-Methode anzumelden.

Ein neues Attribut “sshPublicKey” wird in den Befehlen “add authentication ldapAction” und “set authentication ldapAction” eingeführt. Wenn Sie dieses Attribut verwenden, können Sie die folgenden Vorteile erhalten:

- Kann den abgerufenen öffentlichen Schlüssel speichern, und die LDAP-Aktion verwendet dieses Attribut, um SSH-Schlüsselinformationen vom LDAP-Server abzurufen.
- Kann Attributnamen von bis zu 24 KB extrahieren.

> Hinweis
>
> Der externe Authentifizierungsserver wie LDAP wird nur zum Abrufen von SSH-Schlüsselinformationen verwendet. Es wird nicht für den Authentifizierungszweck verwendet.

Es folgt ein Beispiel für den Ablauf von Ereignissen durch SSH:

- Der SSH-Daemon sendet eine AAA_AUTHENTICATE-Anforderung mit leerem Kennwortfeld an den Authentifizierungs-, Autorisierungs- und Überwachungs-Daemonport

- Wenn LDAP für das Speichern des öffentlichen SSH-Schlüssels konfiguriert ist, antworten Authentifizierung, Autorisierung und Überwachung mit dem Attribut “sshPublicKey” zusammen mit anderen Attributen.
- Der SSH-Daemon überprüft diese Schlüssel mit den Clientschlüsseln.
- Der SSH-Daemon übergibt den Benutzernamen in der Anforderungsnutzlast, und Authentifizierung, Autorisierung und Überwachung geben die für diesen Benutzer spezifischen Schlüssel zusammen mit generischen Schlüsseln zurück.

Um das sshPublicKey -Attribut zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- Mit dem Add-Vorgang können Sie das Attribut “sshPublicKey” während der Konfiguration des Befehls `ldapAction` hinzufügen.

```
add authentication ldapAction <name> {
-serverIP <ip_addr|ipv6_addr|*> | {
-serverName <string> }
 }
 [-serverPort <port>] … [-Attribute1 <string>] … [-Attribute16
    <string>][-sshPublicKey <string>][-authentication off]
<!--NeedCopy-->
```

- Mit dem set-Vorgang können Sie das “sshPublicKey” -Attribut für einen bereits hinzugefügten ldapAction-Befehl konfigurieren.

```
set authentication ldapAction <name> [-sshPublicKey <string>][-
   authentication off]
<!--NeedCopy-->
```

Unterstützung von Namenswert-Attributen für LDAP-Authentifizierung

Sie können jetzt die Attribute der LDAP-Authentifizierung mit einem eindeutigen Namen zusammen mit Werten konfigurieren. Die Namen werden im LDAP-Aktionsparameter konfiguriert, und die Werte werden durch Abfrage des Namens abgerufen. Durch die Verwendung dieser Funktion kann ein NetScaler Appliance-Administrator nun die folgenden Vorteile erzielen:

- Minimiert den Aufwand für Administratoren, indem sie sich das Attribut nach Namen merken (nicht nur nach Wert)
- Verbessert die Suche, um den mit einem Namen verknüpften Attributwert abzufragen
- Bietet eine Option zum Extrahieren mehrerer Attribute

Um diese Funktion an der Eingabeaufforderung der NetScaler Appliance zu konfigurieren, geben Sie Folgendes ein:


```
add authentication ldapAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Beispiel

```
add authentication ldapAction ldapAct1 -attributes "company, mail"
<!--NeedCopy-->
```

Unterstützung für die Validierung der End-to-End-LDAP-Authentifizierung

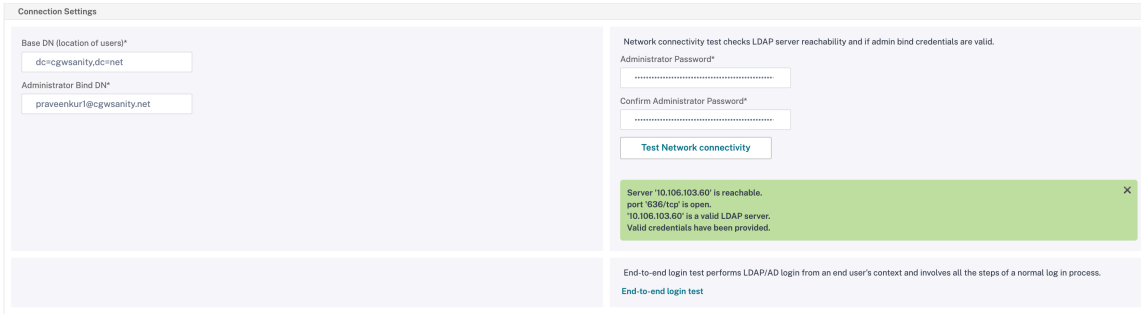
Die NetScaler Appliance kann jetzt die End-to-End-LDAP-Authentifizierung über die GUI validieren. Um diese Funktion zu überprüfen, wird eine neue “Test” -Schaltfläche in der GUI eingeführt. Ein NetScaler Appliance-Administrator kann diese Funktion verwenden, um die folgenden Vorteile zu erzielen:

- Konsolidiert den gesamten Fluss (Paket-Engine — NetScaler AAA-Daemon — externer Server) für eine bessere Analyse
- Verkürzt die Zeit bei der Überprüfung und Behebung von Problemen im Zusammenhang mit einzelnen Szenarien

Sie haben zwei Möglichkeiten, die Testergebnisse der LDAP-End-to-End-Authentifizierung über die grafische Benutzeroberfläche zu konfigurieren und anzuzeigen.

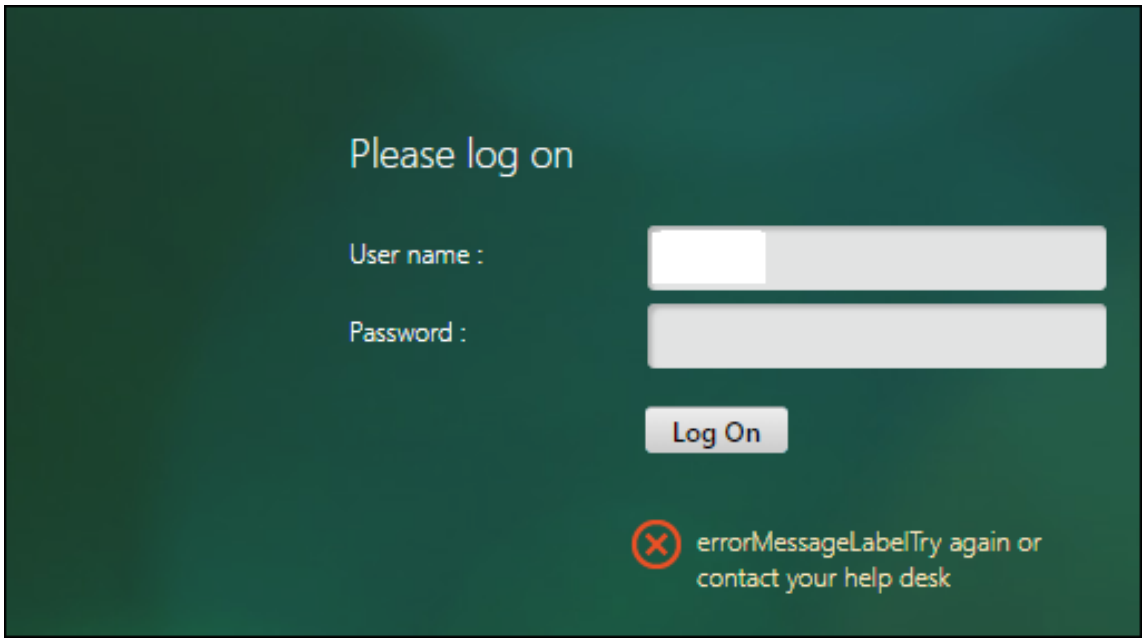
Von der Systemoption

1. Navigieren Sie zu **System > Authentifizierung > Grundlegende Richtlinien > LDAP,** und klicken Sie auf die Registerkarte **Server** .
2. Wählen Sie die verfügbare **LDAP-Aktion** aus der Liste aus.
3. Scrollen Sie auf der Seite **Configure Authentication LDAP Server** nach unten zum Abschnitt **Verbindungseinstellungen** .
4. Klicken Sie auf **Netzwerkkonnektivität testen** , um die LDAP-Serververbindung Sie können eine Popup-Meldung über eine erfolgreiche Verbindung zum LDAP-Server mit TCP-Portdetails und der Authentizität gültiger Anmeldeinformationen anzeigen.



5. Um die End-to-End-LDAP-Authentifizierung anzuzeigen, klicken Sie auf den Link **Ende-zu-Ende-Anmeldetest** .
6. Klicken Sie auf der Seite **Ende-zu-Ende-Anmeldetestauf Testen**.
   - Geben Sie auf der Authentifizierungsseite die gültigen Anmeldeinformationen für die Anmeldung ein. Der Erfolgsbildschirm wird angezeigt.

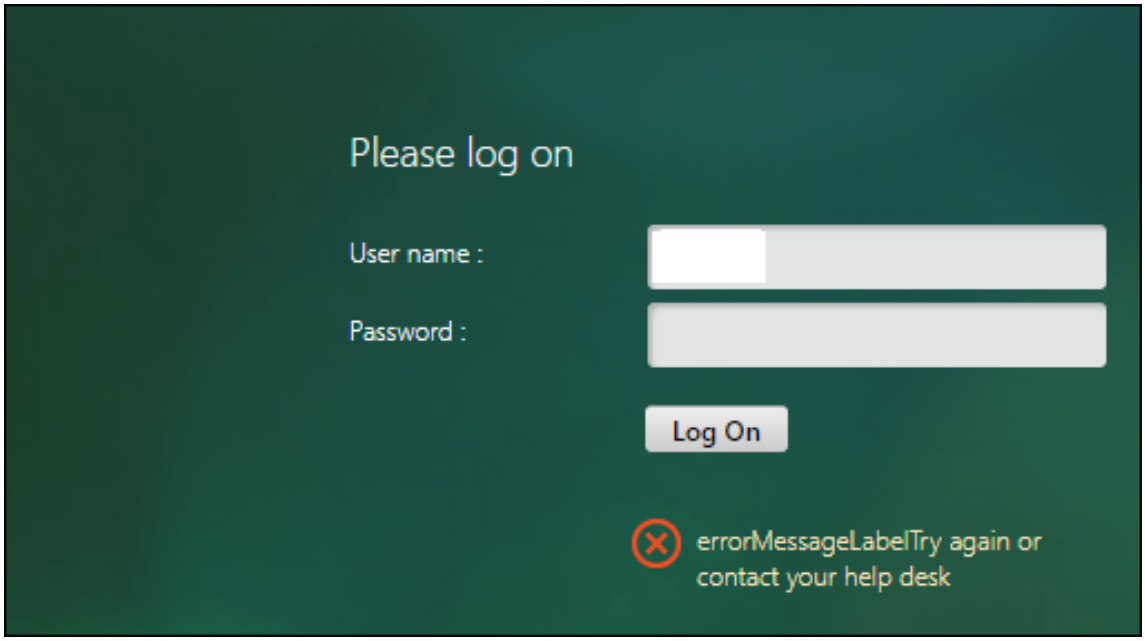
   - Wenn die Authentifizierung fehlschlägt, wird der Fehlerbildschirm angezeigt.



Über die Option Authentifizierung

1. Navigieren Sie zu **Authentifizierung > Dashboard**und wählen Sie die verfügbare LDAP-Aktion aus der Liste aus.
2. Auf der Seite **Configure Authentication LDAP Server** haben Sie im Abschnitt **Verbindungseinstellungen** zwei Optionen.
3. Um die LDAP-Server-Verbindung zu überprüfen, klicken Sie auf **LDAP-Erreichbarkeit testen** . Sie können eine Popup-Meldung über eine erfolgreiche Verbindung zum LDAP-Server mit TCP-Portdetails und der Authentizität gültiger Anmeldeinformationen anzeigen.
4. Um den End-to-End-LDAP-Authentifizierungsstatus anzuzeigen, klicken Sie auf den Link **Endbenutzerverbindung testen** .
5. Klicken Sie auf der Seite **Endbenutzerverbindungtesten auf Test**.
   - Geben Sie auf der Authentifizierungsseite die gültigen Anmeldeinformationen für die Anmeldung ein. Der Erfolgsbildschirm wird angezeigt.

   - Wenn die Authentifizierung fehlschlägt, wird der Fehlerbildschirm angezeigt.



Benachrichtigung 14 Tage vor Kennwortablauf für LDAP-Authentifizierung

Die NetScaler Appliance unterstützt jetzt eine 14-tägige Benachrichtigung zum Ablauf des Kennworts für die LDAP-basierte Authentifizierung. Mit dieser Funktion können Administratoren die Endbenutzer über den Ablauf des Kennworts informieren. Der Schwellenwert wird in Tagen angegeben. Die 14-tägige Benachrichtigung über den Ablauf des Kennworts ist ein Vorläufer des Self-Service-Kennwort-Reset (SSPR).

> **Hinweis**
>
> Der Höchstwert oder Schwellenwert für die Benachrichtigung über den Ablauf des Kennworts in Tagen beträgt 255 Tage.

Vorteile der Benachrichtigung über Ablauf des Kennworts

- Ermöglichen Sie Benutzern, ihre Kennwörter selbst zurückzusetzen, und bieten Sie Administratoren eine flexible Möglichkeit, den Endbenutzer innerhalb von Tagen über den Ablauf ihres Kennworts zu informieren.
- Eliminiert die Abhängigkeit von Endbenutzern, ihre Kennwort-Ablauftage zu verfolgen
- Sendet Benachrichtigungen an die VPN-Portalseite an die Benutzer (basierend auf der Anzahl der Tage), um ihr Kennwort vor Ablauf zu ändern.

> **Hinweis**
>
> Diese Funktion gilt nur für LDAP-basierte Authentifizierungsschemata, nicht für RADIUS oder TACACS.

Grundlegendes zur 14-tägigen Kennwort-Benachrichtigung

Die NetScaler Appliance ruft zwei Attribute (`Max-Pwd-Age and Pwd-Last-Set`) vom LDAP-Authentifizierungsserver ab.

- **Max-Pwd-Alter.** Dieses Attribut gibt die maximale Zeit in Intervallen von 100 Nanosekunden an, bis das Kennwort gültig ist. Der Wert wird als große Ganzzahl gespeichert, die die Anzahl der 100-Nanosekunden-Intervalle ab dem Zeitpunkt darstellt, an dem das Kennwort vor Ablauf des Kennworts festgelegt wurde.
- **Pwd-Letzter Satz.** Dieses Attribut bestimmt das Datum und die Uhrzeit, zu der das Kennwort für ein Konto zuletzt geändert wurde.

Durch das Abrufen der beiden Attribute vom LDAP-Authentifizierungsserver bestimmt die NetScaler Appliance die verbleibende Zeit, bis das Kennwort für einen bestimmten Benutzer abläuft. Diese Informationen werden gesammelt, wenn Benutzeranmeldeinformationen auf dem Authentifizierungsserver überprüft werden und eine Benachrichtigung an den Benutzer zurückgesendet wird.

Ein neuer Parameter “pwdExpiryNotification” wird für den Befehl `set aaa parameter` eingeführt. Mithilfe dieses Parameters kann ein Administrator die Anzahl der verbleibenden Tage bis zum Ablauf des Kennworts verfolgen. Die NetScaler Appliance kann jetzt den Endbenutzer über den Ablauf seines Kennworts informieren.

> **Hinweis**
>
> Derzeit funktioniert diese Funktion nur für Authentifizierungsserver mit Microsoft AD-Servern mit LDAP-Implementierung. Die Unterstützung für OpenLDAP-basierte Server wird später ins Visier genommen.

Es folgt ein Beispiel für den Ablauf der Ereignisse zum Festlegen einer 14-tägigen Benachrichtigung über den Ablauf des Kennworts:

1. Ein Administrator legt mithilfe der NetScaler Appliance eine Zeit (14 Tage) für den Ablauf des Kennworts fest.
2. Der Benutzer sendet eine HTTP- oder HTTPS-Anforderung, um auf eine Ressource auf dem Backend-Server zuzugreifen.
3. Vor dem Bereitstellen des Zugriffs überprüft die NetScaler Appliance die Benutzeranmeldeinformationen mit den auf dem LDAP-Authentifizierungsserver konfigurierten Informationen.
4. Zusammen mit dieser Abfrage an den Authentifizierungsserver führt die NetScaler Appliance die Anforderung aus, die Details der beiden Attribute abzurufen (`Max-Pwd-Age and Pwd-Last-Set`).
5. Abhängig von der verbleibenden Zeit bis zum Ablauf des Kennworts wird eine Ablaufbenachrichtigung angezeigt.
6. Der Benutzer ergreift dann geeignete Maßnahmen, um das Kennwort zu aktualisieren.

So konfigurieren Sie eine 14-tägige Ablaufbenachrichtigung mithilfe der Befehlszeilenschnittstelle

> **Hinweis**
>
> Die 14-tägige Ablaufbenachrichtigung kann für clientlose VPN- und Voll-VPN-Anwendungsfälle und nicht für ICA-Proxy konfiguriert werden.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
set aaa parameter  -pwdExpiryNotificationDays <positive_integer>

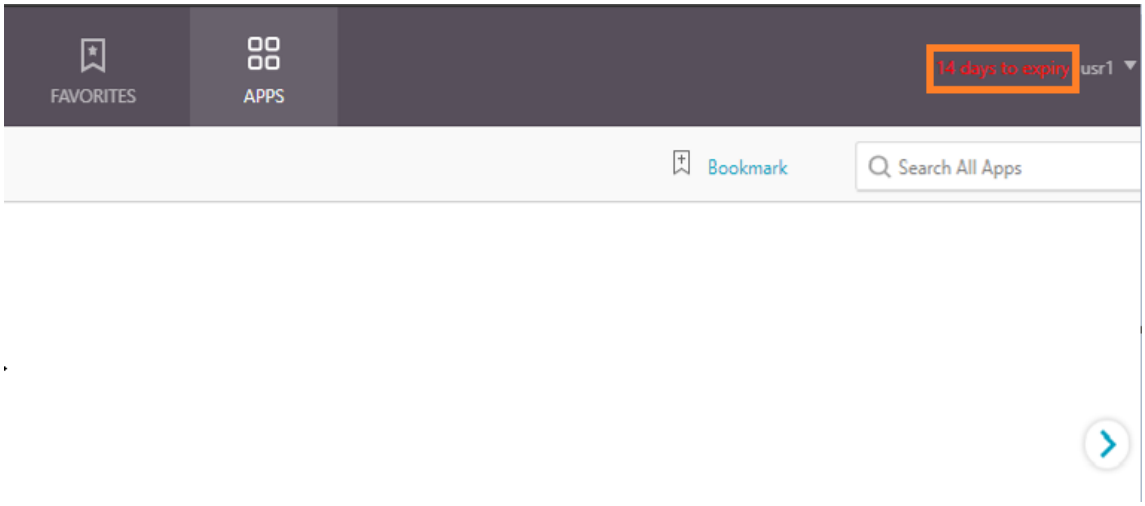
show aaa parameter
<!--NeedCopy-->
```

Beispiel

```
    > set aaa parameter -pwdExpiryNotificationDays 14
    Done
    > show aaa parameter                              Configured AAA
       parameters  EnableStaticPageCaching: YES
       EnableEnhancedAuthFeedback: NO  DefaultAuthType: LOCAL
       MaxAAAUsers:           Unlimited
                                              AAAD nat ip: None
                  EnableSessionStickiness : NO  aaaSessionLoglevel :
       INFORMATIONAL               AAAD Log Level : INFORMATIONAL
                       Dynamic address: OFF
       GUI mode: ON
       Max Saml Deflate Size: 1024             Password Expiry
          Notification Days: 14
<!--NeedCopy-->
```

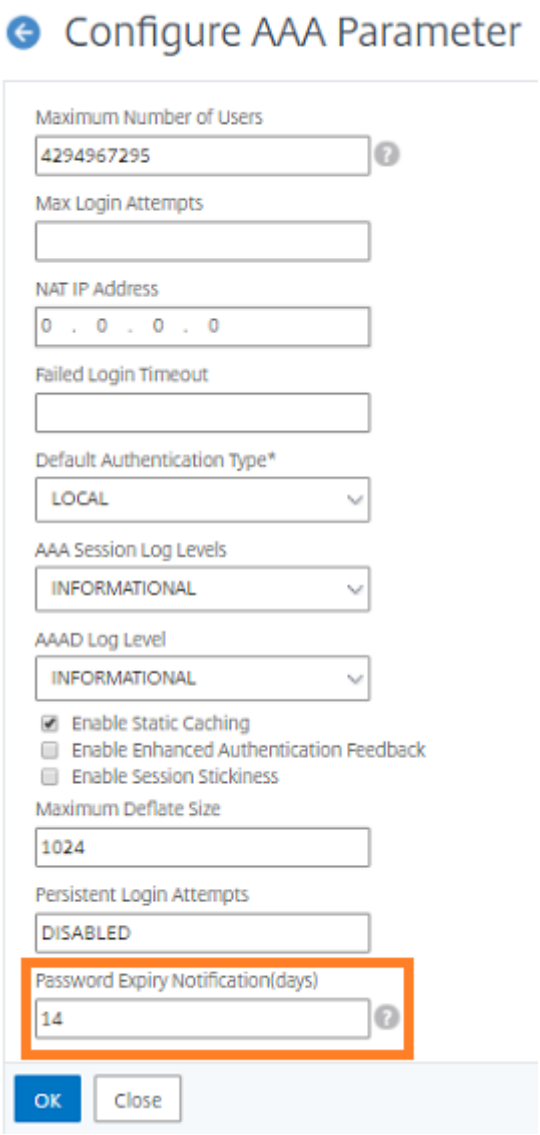
So konfigurieren Sie 14-Tage-Ablaufbenachrichtigung mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Authentifizierungseinstellungen**.
2. Klicke auf **AAA-Authentifizierungseinstellungen ändern**.
3. Geben Sie auf der Seite **AAA-Parameter konfigurieren** die Tage im Feld **Kennwortablaufbenachrichtigung (Tage)** an.



4. Klicken Sie auf **OK.**

   Die Benachrichtigung wird in der oberen rechten Ecke der VPN-Portalseite angezeigt.



LDAP-Authentifizierung auf der NetScaler-Appliance für Verwaltungszwecke konfigurieren

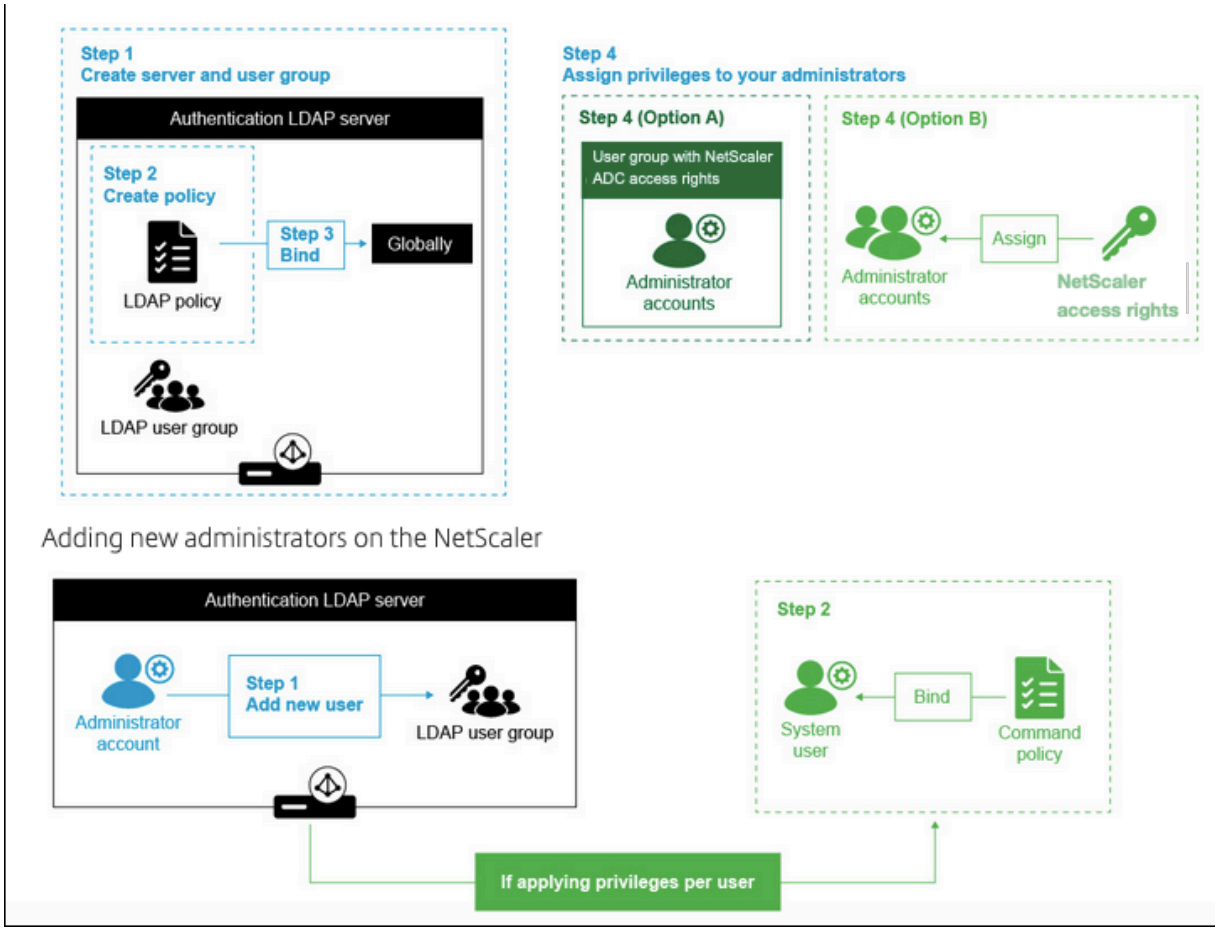
May 11, 2023

Sie können die Benutzeranmeldung bei der NetScaler Appliance mithilfe der Active Directory-Anmeldeinformationen (Benutzername und Kennwort) für Verwaltungszwecke (Superuser, schreibgeschützt, Netzwerkberechtigungen und alle anderen) konfigurieren.

Voraussetzungen

- Windows Active Directory-Domänencontroller
- Eine dedizierte Domänengruppe für NetScaler-Administratoren
- NetScaler Gateway 10.1 und höhere Versionen

Die folgenden Abbildungen veranschaulichen die LDAP-Authentifizierung auf der NetScaler Appliance.

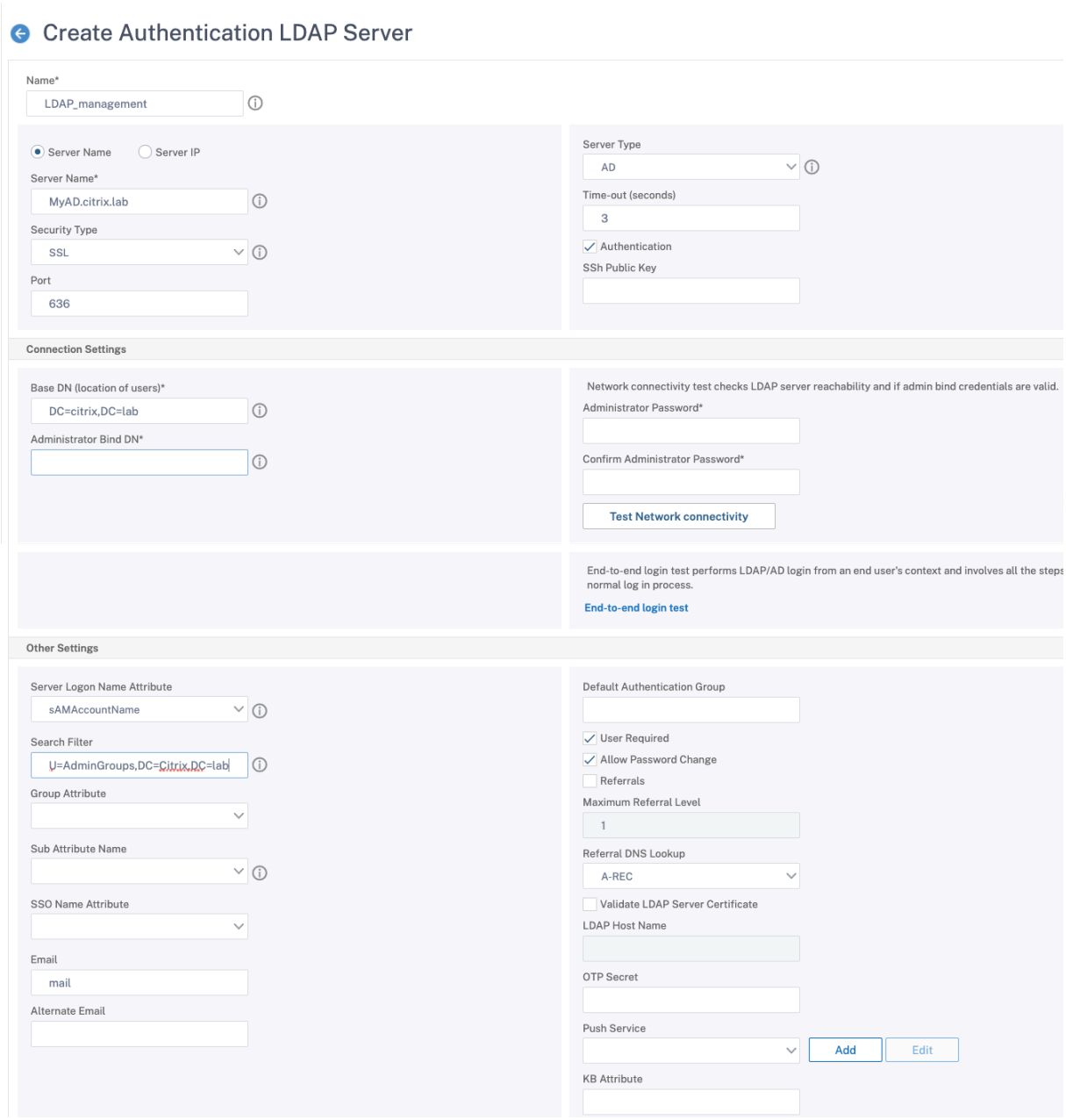


Konfigurationsschritte auf hoher Ebene

1. Erstellen Sie einen LDAP-Server
2. Erstellen einer LDAP-Richtlinie
3. Binden Sie die LDAP-Richtlinie
4. Weisen Sie Ihren Administratoren auf eine der folgenden Arten Berechtigungen zu
    - Berechtigungen auf Gruppe anwenden
    - Wenden Sie Berechtigungen für jeden Benutzer einzeln an

Erstellen eines Authentifizierungs-LDAP-Servers

1. Navigieren Sie zu **System > Authentifizierung > LDAP**.
2. Klicken Sie auf die Registerkarte **Server** und dann auf **Hinzufügen**.
3. Schließen Sie die Konfiguration ab, und klicken Sie dann auf **Erstellen**.



Hinweis:

In diesem Beispiel ist der Zugriff auf die NetScaler Appliance beschränkt, indem die Authentifizierung für die Benutzergruppenmitgliedschaft durch Festlegen des Suchfilters gefiltert wird. Der für dieses Beispiel verwendete Wert ist - & (memberof=CN=NSG_Admin, OU=AdminGroup,

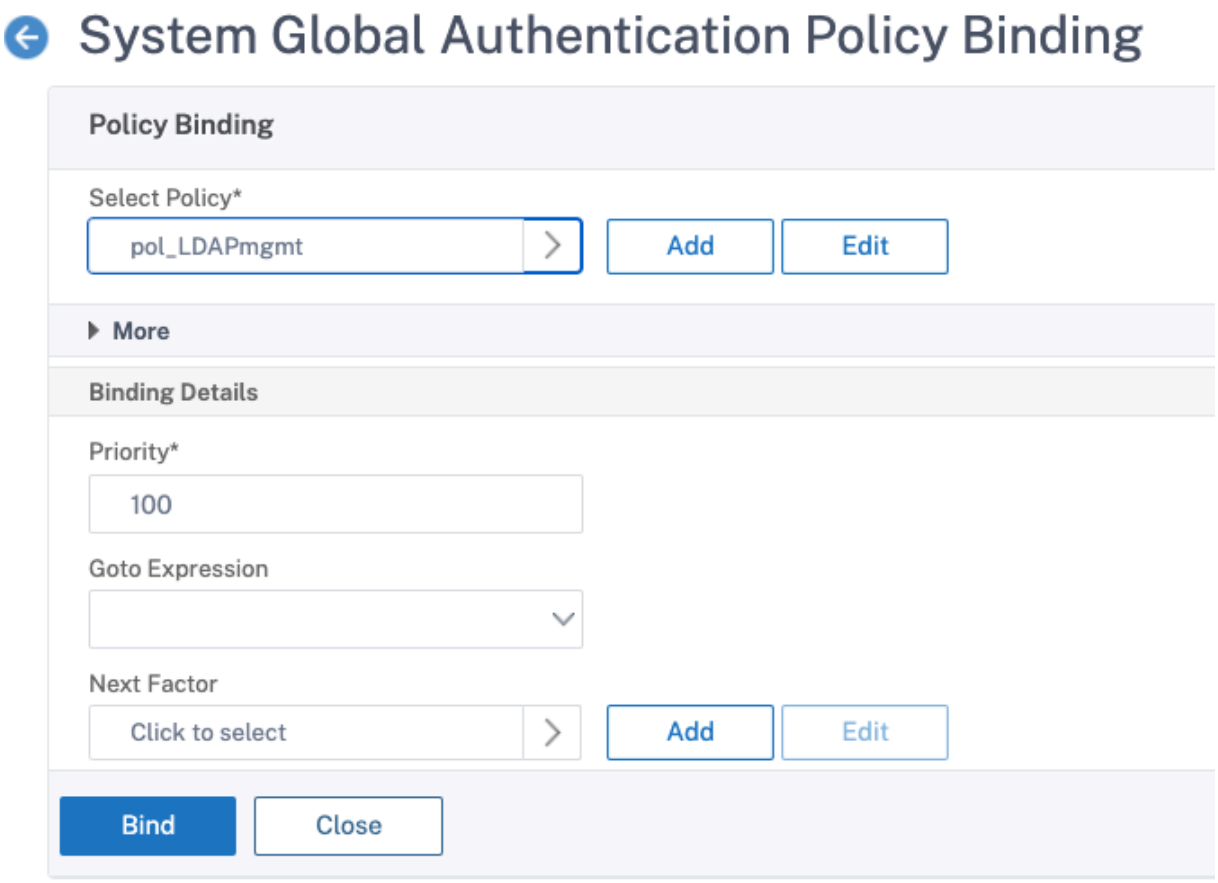
> dc=Citrix, dc=Lab)

Erstellen einer LDAP-Richtlinie

1. Navigieren Sie zu **System > Authentifizierung > Erweiterte Richtlinien > Richtlinie**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für die Richtlinie ein und wählen Sie den Server aus, den Sie in den vorherigen Schritten erstellt haben.
4. Geben Sie im Feld Ausdruckstext den entsprechenden Ausdruck ein, und klicken Sie dann auf **Erstellen**.

Binden Sie die LDAP-Richtlinie global

1. Navigieren Sie zu **System > Authentifizierung > Erweiterte Richtlinien > Richtlinie**.
2. Klicken Sie auf der Seite Authentifizierungsrichtlinien auf **Globale Bindungen**.
3. Wählen Sie die Richtlinie aus, die Sie erstellt haben (in diesem Beispiel pol_LDAPmgmt).
4. Wählen Sie entsprechend eine Priorität (je niedriger die Zahl, desto höher die Priorität)
5. Klicken Sie auf **Binden** und dann auf **Fertig**. In der Spalte **Global gebunden** wird ein grünes Häkchen angezeigt.



Weisen Sie Ihren Administratoren Berechtigungen zu

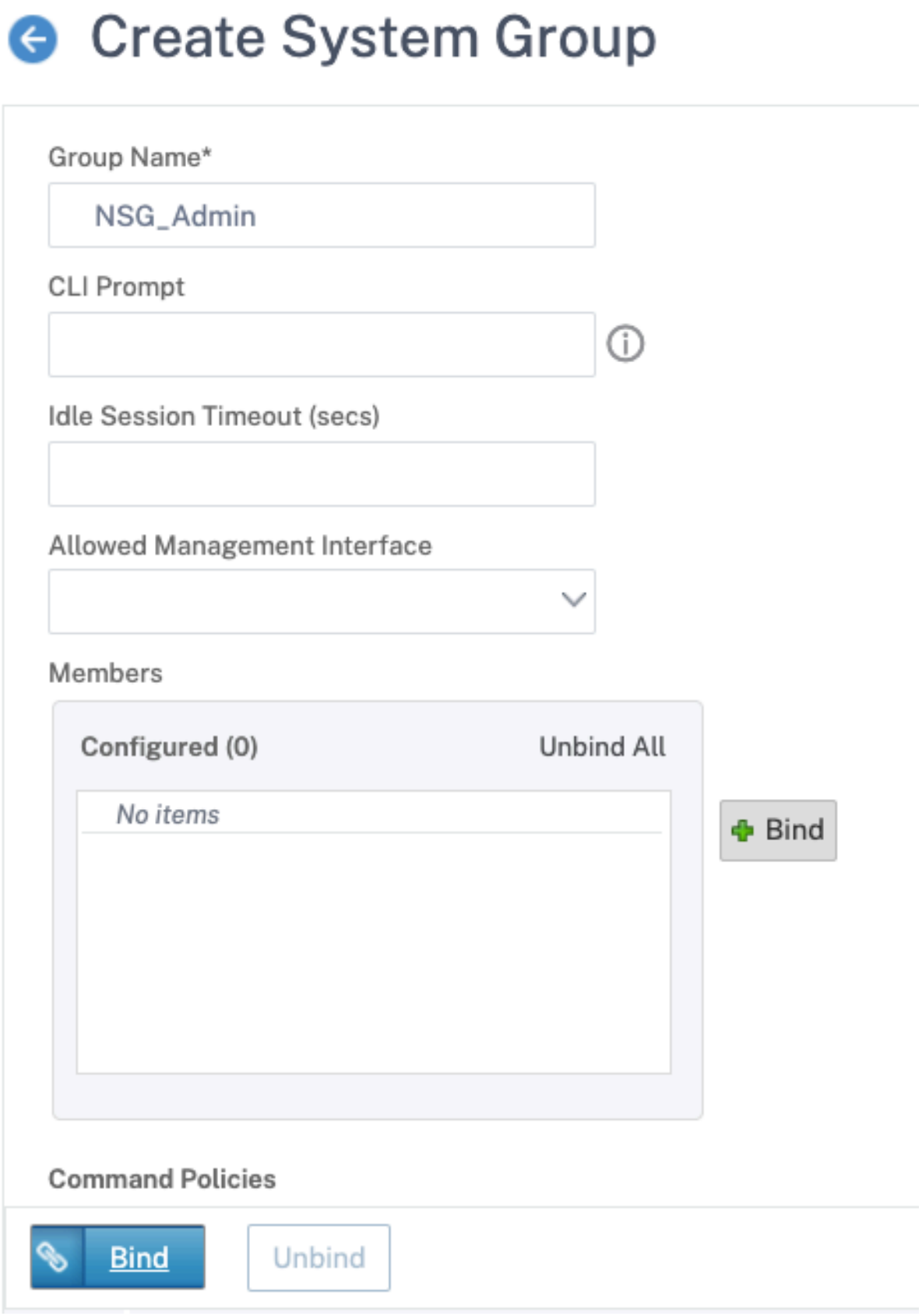
Sie können eine der beiden folgenden Optionen wählen.

- **Berechtigungen auf eine Gruppe anwenden:** Fügen Sie eine Gruppe in der NetScaler Appliance hinzu und weisen Sie jedem Benutzer, der Mitglied dieser Gruppe ist, dieselben Zugriffsrechte zu.
- **Wenden Sie Berechtigungen individuell für jeden Benutzer an:** Erstellen Sie jedes Benutzeradministratorkonto und weisen Sie jedem Benutzer Rechte zu.

Berechtigungen auf eine Gruppe anwenden

Wenn Sie Berechtigungen auf eine Gruppe anwenden, können Benutzer, die Mitglied der im Suchfilter konfigurierten Active Directory-Gruppe sind (in diesem Beispiel NSG_Admin), eine Verbindung zur NetScaler Management-Schnittstelle herstellen und über eine Superuser-Befehlsrichtlinie verfügen.

1. Navigieren Sie zu **System > Benutzerverwaltung > Gruppen**.
2. Geben Sie die Details gemäß der Anforderung ein und klicken Sie dann auf **Erstellen**.



Sie haben die Active Directory-Gruppe definiert, zu der die Benutzer gehören, und auch die Befehlsrichtlinienebene, die dem Konto bei der Anmeldung zugeordnet werden muss. Sie können der LDAP-Gruppe, die Sie im Suchfilter konfiguriert haben, neue Administratorbenutzer hinzufügen.

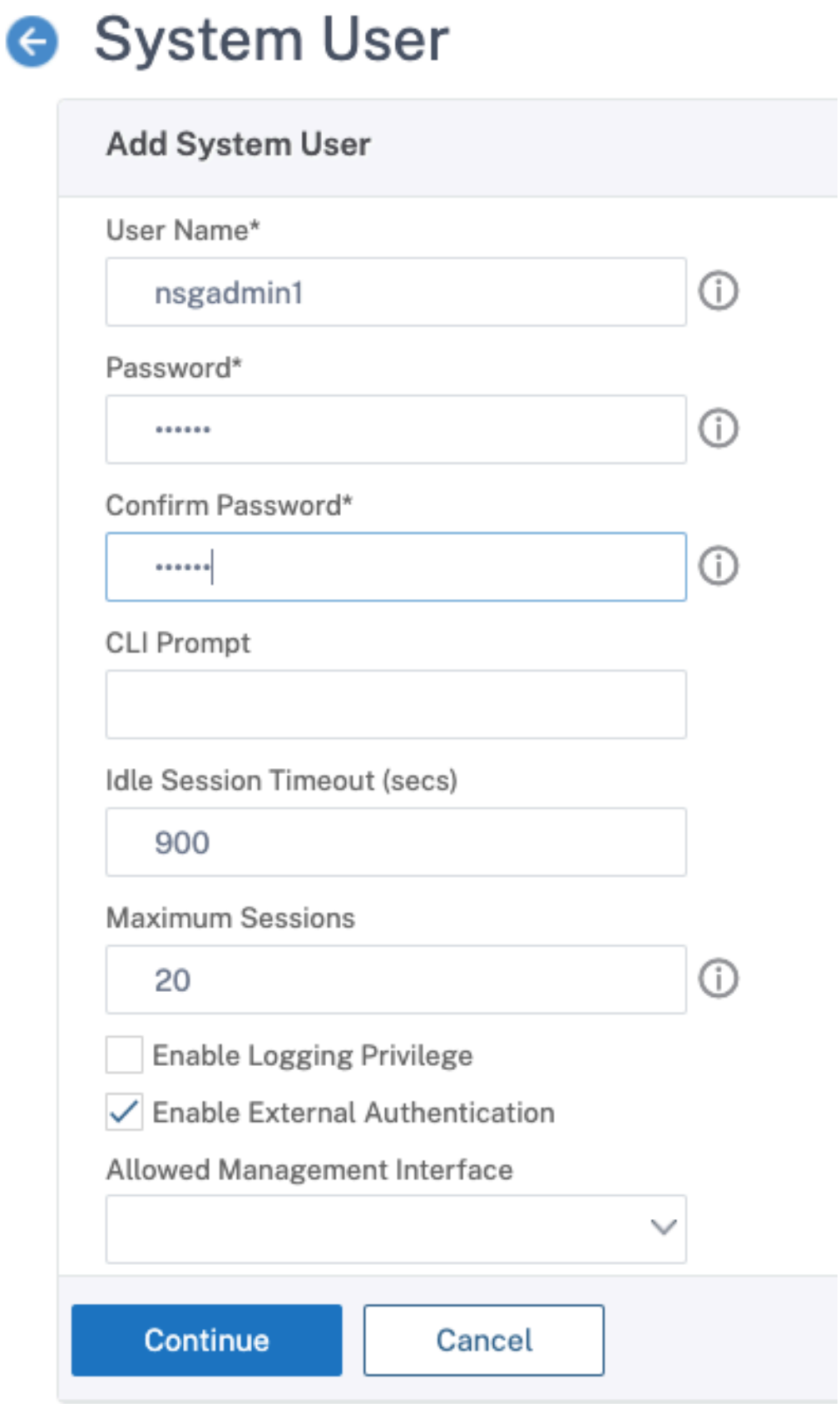
> **Hinweis:**
>
> Der Gruppenname muss mit dem Active Directory-Datensatz übereinstimmen.

Wenden Sie Berechtigungen für jeden Benutzer einzeln an

In diesem Szenario können Benutzer, die Mitglied Ihrer im Suchfilter konfigurierten Active Directory-Gruppe sind (in diesem Beispiel NSG_Admin), eine Verbindung zur NetScaler-Verwaltungsschnittstelle herstellen, haben jedoch keine Berechtigungen, bis Sie den bestimmten Benutzer auf der NetScaler Appliance erstellen und die Befehlsrichtlinie daran binden.

1. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie die Details gemäß der Anforderung ein.

   Hinweis: Achten Sie darauf, **Externe Authentifizierung aktivieren**auszuwählen.



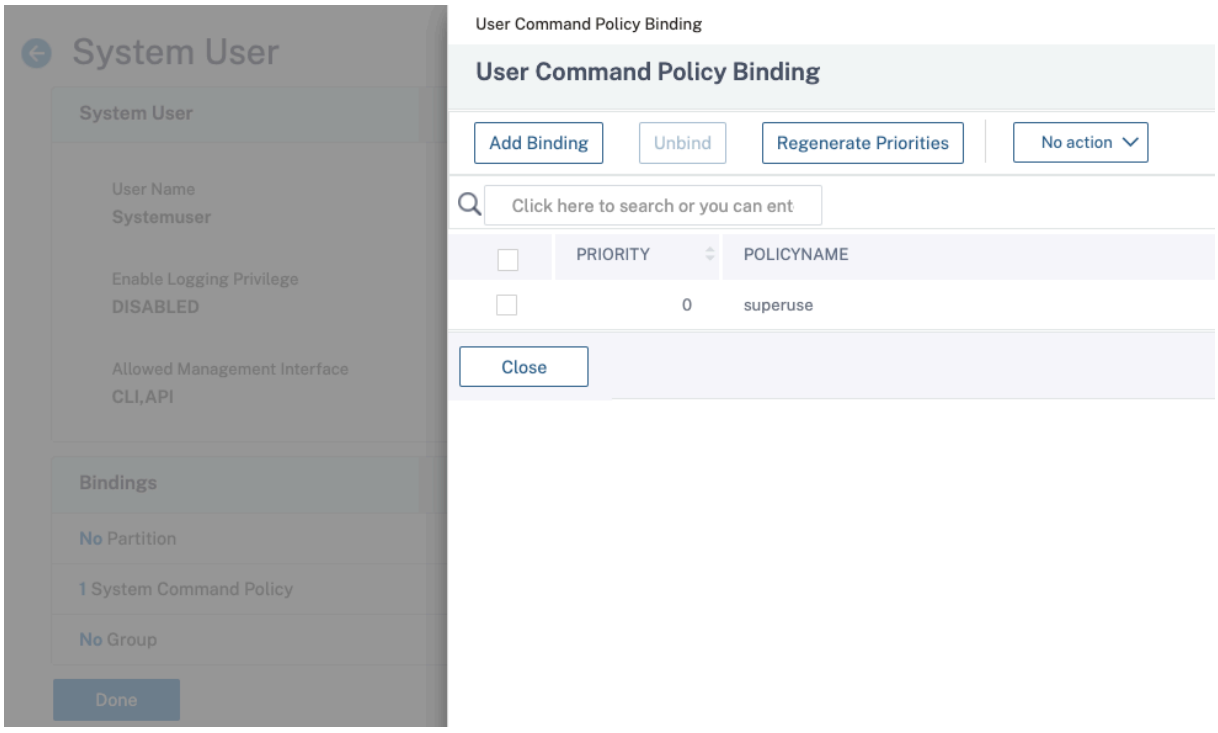
1. Klicken Sie auf **Weiter**.

Sie haben den Active Directory-Benutzer und die Befehlsrichtlinienebene definiert, die beim Anmelden mit dem Konto verknüpft werden müssen.

> **Hinweis:**
>
> - Der Benutzername muss mit dem Active Directory-Datensatz des vorhandenen Benutzers übereinstimmen.
> - Wenn Sie dem NetScaler einen Benutzer für die externe Authentifizierung hinzufügen, müssen Sie ein Kennwort angeben, falls die externe Authentifizierung nicht verfügbar ist. Damit die externe Authentifizierung ordnungsgemäß funktioniert, darf das interne Kennwort nicht mit dem LDAP-Kennwort des Benutzerkontos übereinstimmen.

Befehlsrichtlinie zum Benutzer hinzufügen

1. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
2. Wählen Sie den Benutzer aus, den Sie erstellt haben, und klicken Sie dann auf **Bearbeiten.**
3. Klicken Sie unter Bindungen auf **Systembefehlsrichtlinie**.
4. Wählen Sie die richtige Befehlsrichtlinie für Ihren Benutzer aus.
5. Klicken Sie auf **Binden** und dann auf **Schließen**.



Um weitere Administratoren hinzuzufügen;

- Fügen Sie die Administratorbenutzer der LDAP-Gruppe hinzu, die Sie im Suchfilter konfiguriert haben.

- Erstellen Sie den Systembenutzer in NetScaler und weisen Sie die richtige Befehlsrichtlinie zu.

So konfigurieren Sie die LDAP-Authentifizierung auf der NetScaler Appliance für Verwaltungszwecke mithilfe der CLI

Verwenden Sie die folgenden Befehle als Referenz, um die Anmeldung für eine Gruppe mit Superuser-Rechten auf der CLI der NetScaler Appliance zu konfigurieren.

1. Erstellen Sie einen LDAP-Server

```
add authentication ldapAction LDAP_mgmt -serverIP myAD.citrix.lab
    -serverPort 636 -ldapBase "DC=citrix,DC=lab" -ldapBindDn
    readonly@citrix.lab -ldapBindDnPassword -ldapLoginName
    sAMAccountName -searchFilter "&(memberof=CN=NSG_Admin,OU=
    AdminGroups,DC=citrix,DC=lab)" -groupAttrName memberOf
<!--NeedCopy-->
```

2. Richtlinie erstellen und LDAP

```
add authentication ldapPolicy pol_LDAPmgmt ns_true LDAP_mgmt
<!--NeedCopy-->
```

3. Bindung der LDAP-Richtlinie

```
bind system global pol_LDAPmgmt -priority 110
<!--NeedCopy-->
```

4. Weisen Sie Ihren Administratoren Berechtigungen zu

   - So wenden Sie Berechtigungen auf die Gruppe an

```
add system group NSG_Admin
bind system group NSG_Admin -policyName superuser 100
<!--NeedCopy-->
```

   - So wenden Sie Berechtigungen für jeden Benutzer einzeln an

```
add system user admyoa
bind system user admyoa superuser 100
<!--NeedCopy-->
```


LDAP nach dem SSL-Offload auf einen virtuellen Lastausgleichsserver konfigurieren

June 2, 2023

In einer NetScaler Appliance wird der AAAD-Prozess für die Durchführung der Standardauthentifizierung wie LDAP, RADIUS, TACACS für Verwaltungszugriff oder Authentifizierungsautorisierung und Gatewayzugriff verwendet. Da AAAD auf der Verwaltungs-CPU ausgeführt wird, kann es zu Problemen mit zeitweiligen Authentifizierungsfehlern kommen. Um diese Fehler zu vermeiden, kann der virtuelle Lastausgleichsserver verwendet werden, um die SSL-Funktionalität von AAAD auszulagern.

Vorteile der Auslagerung von SSL auf einen virtuellen Lastausgleichsserver

- Verbesserte AAAD-Leistung. In AAAD wird für jede Authentifizierungsanforderung für den LDAP-Server des SSL-Typs eine neue SSL-Sitzung eingerichtet. Da der AAAD-Prozess auf der Verwaltungs-CPU ausgeführt wird, wirkt sich das Einrichten der SSL-Sitzung auf die Leistung bei hohen Anforderungen an das AAAD aus. Das Auslagern der SSL-Funktionalität auf den virtuellen Lastausgleichsserver verbessert die Leistung des AAAD-Prozesses
- Rendern Sie das Client-Zertifikat zum Server Die Client-LDAP-Bibliothek in AAAD führt nur die Überprüfung von Serverzertifikaten durch, es gibt keine Unterstützung für das Rendern von Clientzertifikaten auf dem Server Da die gegenseitige SSL-Authentifizierung das Rendern des Clientzertifikats zum Herstellen der SSL-Verbindung erfordert, ermöglicht das Auslagern der SSL-Funktionalität auf den virtuellen Lastausgleichsserver das Rendern des Clientzertifikats an den Server

Konfigurieren Sie LDAP nach dem Auslagern von SSL auf den virtuellen Lastausgleichsserver

Hinweis: Nachdem Sie eine IP-Adresse des virtuellen Lastausgleichsservers für LDAP erstellt und den LDAP-Anforderungsserver auf die IP-Adresse des virtuellen Servers verwiesen haben, wird der Datenverkehr vom SNIP bezogen.

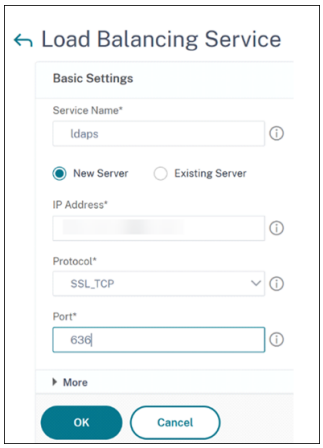
Voraussetzungen

- Stellen Sie sicher, dass sicheres LDAP auf den Domänencontrollern aktiviert ist, die die NetScaler Appliance für die Authentifizierung verwendet. Standardmäßig registrieren sich bei einer Unternehmenszertifizierungsstelle alle Domänencontroller mithilfe der Zertifikatsvorlage des Domänencontrollers für ein Zertifikat.

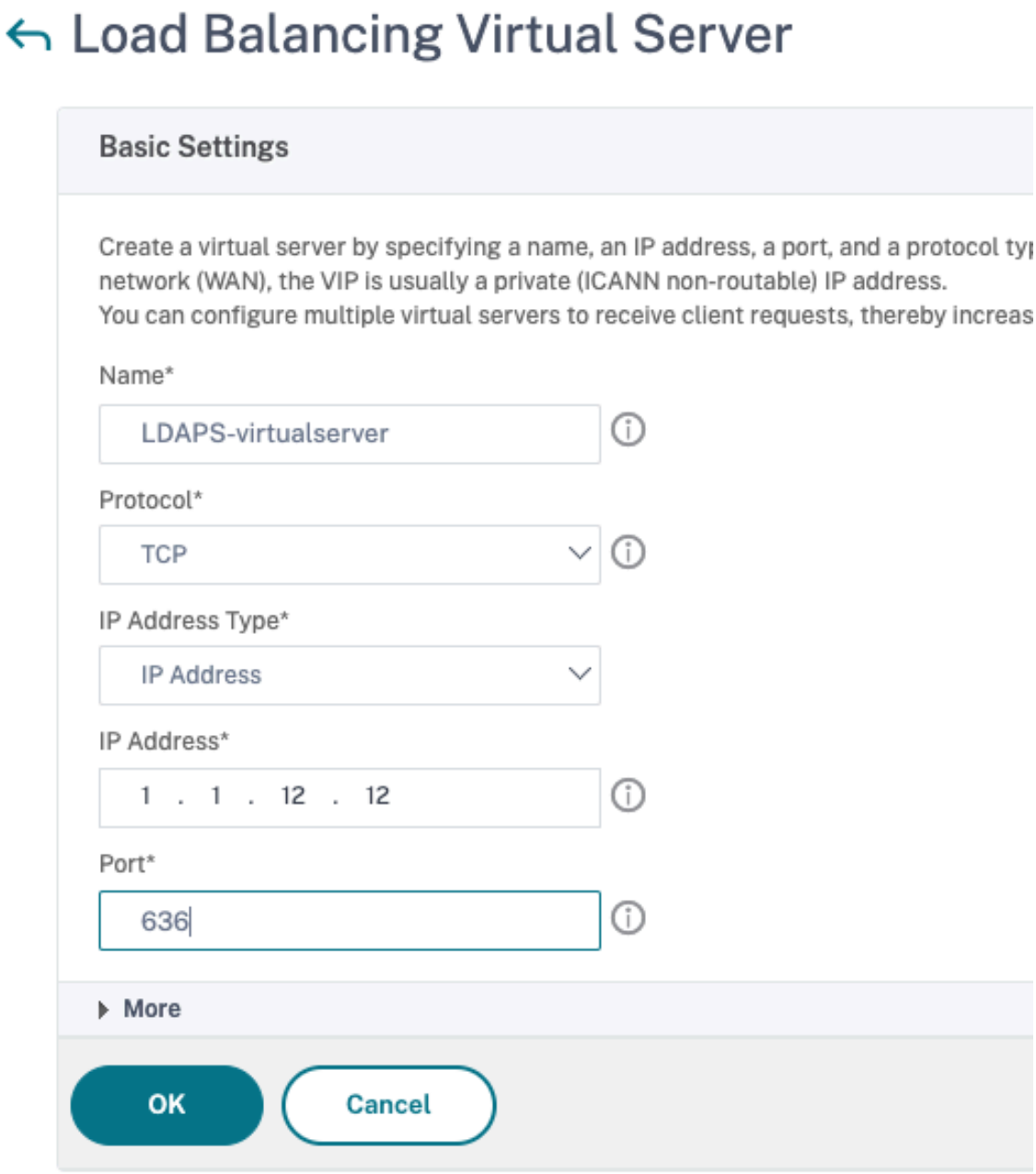
- Stellen Sie sicher, dass sicheres LDAP funktioniert, indem Sie die Datei ldp.exe verwenden und über Port 636 und SSL eine Verbindung zum Domänencontroller herstellen.

Konfigurieren Sie LDAP, nachdem Sie SSL mithilfe der GUI auf den virtuellen Load-Balancing-Server ausgelagert haben

1. Erstellen Sie einen Load Balancing-Dienst, dessen Protokoll auf SSL_TCP gesetzt ist.
   - Navigieren Sie zu **Traffic Management > Load Balancing > Services** und klicken Sie auf **Hinzufügen**.
   - Geben Sie die IP-Adresse des Domänencontrollers an und legen Sie die Portnummer auf 636 fest.
   - Klicken Sie auf **OK**.

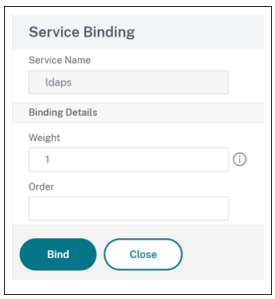


2. Erstellen Sie einen virtuellen Lastausgleichsserver für den LDAPS-Lastenausgleichsdienst.
   a) Navigieren Sie zu **Verkehrsmanagement > Load Balancing > Virtuelle Server**.
   b) Setzen Sie das Protokoll auf TCP, geben Sie die IP-Adresse ein, setzen Sie den Port auf 636 und klicken Sie auf **OK**.



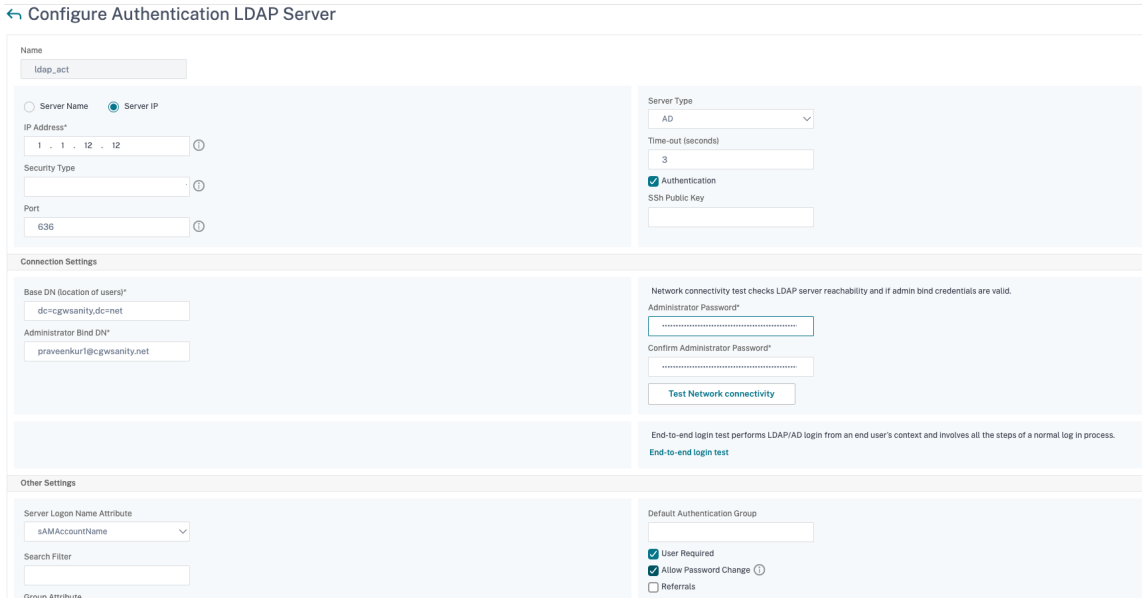
3. Binden Sie den LDAPS-Dienst an den virtuellen Load-Balancing-Server.
   - Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
   - Wählen Sie den virtuellen LDAP-Server aus. Die Seite **Load Balancing Virtual Server** wird angezeigt.
   - Klicken Sie im Abschnitt **Dienste und Dienstgruppen** auf **No Load Balancing Virtual Server Service Binding**. Die Seite **Service Binding** wird angezeigt.
   - Wählen Sie den Load Balancing-Dienst aus. Aktualisieren Sie die anderen erforderlichen Felder und klicken Sie auf **Binden**.

- Klicken Sie auf **Fertig**.



4. Ändern Sie nun den LDAP-Authentifizierungsrichtlinienserver so, dass er auf den virtuellen Lastausgleichsserver für sicheres LDAP verweist. Der Sicherheitstyp muss PLAINTEXT sein.

   a) Navigieren Sie zu **NetScaler Gateway > Richtlinien > Authentifizierung > LDAP**.
   b) Wählen Sie den LDAP-Server aus und klicken Sie auf **Bearbeiten**.
   c) Ändern Sie die IP-Adresse in die LDAPS-VIP, die auf der zuvor erstellten NetScaler Appliance gehostet wird.
   d) Ändern Sie den Sicherheitstyp in **PLAINTEXT**, ändern Sie den Port auf 636, aktivieren Sie bei Bedarf das Kontrollkästchen **Kennwortänderung zulassen** (SLDAP erlaubt Kennwortänderungen).
   e) Klicken Sie auf **Netzwerkverbindung testen**, um die Konnektivität zu überprüfen
   f) Klicken Sie auf **OK**.



Sie können das Authentifizierungs-Dashboard überprüfen, um zu bestätigen, dass der Status des LDAP-Servers UP ist. Überprüfen Sie außerdem die Authentifizierungsprotokolle, um sicherzustellen, dass die Authentifizierung wie vorgesehen funktioniert.

Konfigurieren Sie LDAP, nachdem Sie SSL mithilfe der CLI auf den virtuellen Load-Balancing-Server ausgelagert haben

1. Konfigurieren Sie einen LDAP-Server für den AAAD-Prozess. Die folgende Beispielkonfiguration stellt die SSL-Verbindung mit einem virtuellen Lastausgleichsserver ohne gegenseitige SSL-Authentifizierung her.

```
add authentication ldapAction ldap_act -serverIP 1.1.12.12 -
    serverPort 636 -secTYPE PLAINTEXT -ldapBase "dc=aaatm-test,dc=
    com" -ldapBindDn administrator@aaatm-test.com -
    ldapBindDnPassword <password> -ldapLoginName samAccountName
<!--NeedCopy-->
```

2. Konfigurieren Sie einen virtuellen Lastausgleichsserver für den virtuellen LDAP-Server. Der virtuelle Lastausgleichsserver ist vom Typ TCP.

```
add lb vserver ldaps TCP 1.1.1.12 636 -persistenceType NONE -
    cltTimeout 9000
<!--NeedCopy-->
```

3. Konfigurieren Sie einen Dienst für den virtuellen Lastausgleichsserver. Der Diensttyp ist SSL-TCP.

```
add service ldaps 1.1.10.1 SSL_TCP 636
<!--NeedCopy-->
```

4. Konfigurieren Sie ein CA-Zertifikat für den Dienst und legen Sie den Parameter “serverAuth” für die Validierung des Serverzertifikats fest.

```
bind ssl service ldaps -certkeyName ca-cert -CA
set ssl service ldaps -serverAuth enabled
<!--NeedCopy-->
```

5. Hängen Sie das Zertifikat an den Dienst an, der auf dem LDAP-Server gerendert wird.

```
bind ssl service ldaps -certkeyName usr_cert [client-certificate
    for client-authentication]
<!--NeedCopy-->
```

6. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.

```
bind lb vserver ldaps ldaps
<!--NeedCopy-->
```


RADIUS-Authentifizierung

May 11, 2023

Wie bei anderen Arten von Authentifizierungsrichtlinien besteht eine RADIUS-Authentifizierungsrichtlinie (Remote Authentication Dial In User Service) aus einem Ausdruck und einer Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, bezeichnen Sie es auch als primäre oder sekundäre Richtlinie. Für die Einrichtung einer RADIUS-Authentifizierungsrichtlinie gelten jedoch bestimmte spezielle Anforderungen, die im Folgenden beschrieben werden.

Normalerweise konfigurieren Sie den NetScaler so, dass er die IP-Adresse des Authentifizierungsservers während der Authentifizierung verwendet. Mit RADIUS-Authentifizierungsservern können Sie den ADC jetzt so konfigurieren, dass er den FQDN des RADIUS-Servers anstelle seiner IP-Adresse verwendet, um Benutzer zu authentifizieren. Die Verwendung eines FQDN kann eine ansonsten viel komplexere Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration in Umgebungen vereinfachen, in denen sich der Authentifizierungsserver möglicherweise an einer von mehreren IP-Adressen befindet, aber immer einen einzigen FQDN verwendet. Um die Authentifizierung mithilfe des FQDN eines Servers anstelle seiner IP-Adresse zu konfigurieren, folgen Sie dem normalen Konfigurationsprozess, außer wenn Sie die Authentifizierungsaktion erstellen. Beim Erstellen der Aktion ersetzen Sie den **serverName-Parameter** durch den **serverIP-Parameter.**

Bevor Sie entscheiden, ob Sie den NetScaler so konfigurieren, dass er die IP oder den FQDN Ihres RADIUS-Servers zur Authentifizierung von Benutzern verwendet, sollten Sie bedenken, dass die Konfiguration von Authentifizierung, Autorisierung und Überwachung für die Authentifizierung an einem FQDN statt an einer IP-Adresse dem Authentifizierungsprozess einen zusätzlichen Schritt hinzufügt. Jedes Mal, wenn der ADC einen Benutzer authentifiziert, muss er den FQDN auflösen. Wenn sehr viele Benutzer versuchen, sich gleichzeitig zu authentifizieren, verlangsamen die daraus resultierenden DNS-Lookups möglicherweise den Authentifizierungsprozess.

> **Hinweis**
>
> Bei diesen Anweisungen wird davon ausgegangen, dass Sie bereits mit dem RADIUS-Protokoll vertraut sind und Ihren ausgewählten RADIUS-Authentifizierungsserver bereits konfiguriert haben.

So fügen Sie mithilfe der Befehlszeilenschnittstelle eine Authentifizierungsaktion für einen RADIUS-Server hinzu

Wenn Sie sich bei einem RADIUS-Server authentifizieren, müssen Sie eine explizite Authentifizierungsaktion hinzufügen. Geben Sie dazu an der Befehlszeile den folgenden Befehl ein:


```
add authentication radiusAction <name> [-serverip <IP> | -serverName] <
    FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
     passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
     ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
     pwdVendorID <positive_integer> [-pwdAttributeType <
     positive_integer>]] [-defaultAuthenticationGroup <string>] [-
     callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

Im folgenden Beispiel wird eine RADIUS-Authentifizierungsaktion namens **Authn-Act-1** mit der Server-IP **10.218.24.65**, dem Server-Port **1812**, dem Authentifizierungs-Timeout von **15** Minuten, dem Radius-Schlüssel **WareTheLorax**, NAS-IP deaktiviert und NAS-ID **NAS1** hinzugefügt.

```
add authentication radiusaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
    DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

Das folgende Beispiel fügt dieselbe RADIUS-Authentifizierungsaktion hinzu, verwendet jedoch den Server-FQDN **rad01.example.com** anstelle der IP.

```
add authentication radiusaction Authn-Act-1 -serverName rad01.example.
    com -serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
    DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

So konfigurieren Sie eine Authentifizierungsaktion für einen externen RADIUS-Server mithilfe der Befehlszeile

Um eine vorhandene RADIUS-Aktion zu konfigurieren, geben Sie an der Befehlszeile den folgenden Befehl ein:

```
set authentication radiusAction <name> [-serverip <IP> | -serverName] <
    FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -radKey  }
```



```
3    [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
        <positive_integer>][-radAttributeType <positive_integer>][-
        radGroupsPrefix <string>] [-radGroupSeparator <string>][-
        passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
        ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
        pwdVendorID <positive_integer> [-pwdAttributeType <
        positive_integer>]] [-defaultAuthenticationGroup <string>] [-
        callingstationid ( ENABLED | DISABLED )]
4
5  <!--NeedCopy-->
```

So entfernen Sie eine Authentifizierungsaktion für einen externen RADIUS-Server mithilfe der Befehlszeilenschnittstelle

Um eine vorhandene RADIUS-Aktion zu entfernen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1  rm authentication radiusAction <name>
2
3  <!--NeedCopy-->
```

Beispiel

```
1  rm authentication radiusaction Authn-Act-1
2  Done
3
4  <!--NeedCopy-->
```

So konfigurieren Sie einen RADIUS-Server mithilfe des Konfigurationsprogramms

> **Hinweis**
>
> Im Konfigurationsdienstprogramm wird der Begriff Server anstelle von Aktion verwendet, bezieht sich jedoch auf dieselbe Aufgabe.

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Radius**
2. Führen Sie im Detailbereich auf der Registerkarte **Server** einen der folgenden Schritte aus:
   - Um einen neuen RADIUS-Server zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen RADIUS-Server zu ändern, wählen Sie den Server aus, und klicken Sie dann auf **Bearbeiten**.

3. Geben **Sie im Dialogfeld „RADIUS-Authentifizierungsserver erstellen** “ oder „ **Authentifizierungs-RADIUS-Server konfigurieren** “ Werte für die Parameter ein, oder wählen Sie sie aus. Um Parameter auszufüllen, die unter “ **Anrufstation-ID senden**” angezeigt werden, erweitern Sie **Details**.
    - name* — RadiusActionName (Kann für eine zuvor konfigurierte Aktion nicht geändert werden)
    - Authentifizierungstyp* — AuthType (Auf RADIUS gesetzt, kann nicht geändert werden)
    - Servername/IP-Adresse* — Wählen Sie entweder Servername oder Server-IP
        - Servername*—serverName <FQDN>
        - IP-Adresse *—ServerIP <IP> Wenn dem Server eine IPv6-IP-Adresse zugewiesen ist, aktivieren Sie das Kontrollkästchen IPv6.
    - Port* — Serverport
    - Timeout (Sekunden) * — AuthTimeout
    - Geheimer Schlüssel* — RadKey (gemeinsam genutzter RADIUS-Schlüssel.)
    - Bestätigen Sie den geheimen Schlüssel* — Geben Sie den gemeinsam genutzten RADIUS-Schlüssel ein zweites Mal ein. (Kein Befehlszeilenäquivalent.)
    - Rufstationsnummer senden—CallingStationID
    - Gruppen-Anbieter-ID — RadVendorID
    - Gruppenattributtyp — RadAttributeType
    - Anbieter-Identifier für die IP-Adresse — IPVendorID
    - PWD-Verkäufer-ID — PWD-Verkäufer-ID
    - Passwortkodierung — PassenCoding
    - Standardauthentifizierungsgruppe — Standardauthentifizierungsgruppe
    - NAS-ID — RAD-NASID
    - NAS-IP-Adressextraktion aktivieren—Radnasip
    - Gruppenpräfix — RadGroupsPrefix
    - Gruppentrennzeichen — RadGroupSeparator
    - IP-Adressattributtyp — IPAttributeType
    - Kennwortattributtyp — pwdAttributeType
    - Buchhaltung — Buchhaltung
4. Klicken Sie auf **Erstellen** oder **auf OK**. Die von Ihnen erstellte Richtlinie wird auf der Seite Server angezeigt.

Unterstützung für die Weitergabe des RADIUS-Attributs 66 (Tunnel-Client-Endpoint)

Die NetScaler-Appliance ermöglicht jetzt die Weitergabe des RADIUS-Attributs 66 (Tunnel-Client-Endpoint) während der RADIUS-Authentifizierung. Durch die Anwendung dieser Funktion wird die IP-Adresse des Clients im Rahmen einer zweiten Faktorauthentifizierung empfangen, indem sie ihnen anvertraut wird, risikobasierte Authentifizierungsentscheidungen zu treffen.

Das neue Attribut „TunnelEndPointClientIp“ wurde sowohl in den Befehlen „add authentication radiusAction“ als auch in „set radiusParams“ eingeführt.

Um diese Funktion zu verwenden, geben Sie an der Befehlszeile der NetScaler Appliance Folgendes ein:

```
add authentication radiusAction <name> {
 -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> }
  }
  [-serverPort <port>] … [-tunnelEndpointClientIP (ENABLED|DISABLED)]

set radiusParams {
 -serverIP <ip_addr|ipv6_addr|*> |{
 -serverName <string> }
  }
  [-serverPort<port>] … [-tunnelEndpointClientIP(ENABLED|DISABLED)]

<!--NeedCopy-->
```

Beispiel

```
add authentication radiusAction radius -severIP 1.217.22.20 -serverName
     FQDN -serverPort 1812 -tunnelEndpointClientIp ENABLED

set radiusParams -serverIp 1.217.22.20 -serverName FQDN1 -serverPort
    1812 -tunnelEndpointClientIP ENABLED

<!--NeedCopy-->
```

Unterstützung für die Validierung der End-to-End-RADIUS-Authentifizierung

Die NetScaler Appliance kann jetzt die End-to-End-RADIUS-Authentifizierung über eine GUI überprüfen. Um diese Funktion zu validieren, wird eine neue Schaltfläche “Test” in GUI eingeführt. Ein NetScaler Appliance-Administrator kann diese Funktion nutzen, um folgende Vorteile zu erzielen:

- Konsolidiert den vollständigen Ablauf (Paket-Engine - aaa Daemon - externer Server), um eine bessere Analyse zu ermöglichen

- Verkürzt die Zeit bei der Überprüfung und Behebung von Problemen im Zusammenhang mit einzelnen Szenarien

Sie haben zwei Möglichkeiten, die Testergebnisse der RADIUS-Ende-zu-Ende-Authentifizierung mithilfe der GUI zu konfigurieren und anzuzeigen.

Von der Systemoption

1. Navigieren Sie zu **System > Authentifizierung > Grundrichtlinien > RADIUS** und klicken Sie auf die Registerkarte **Server** .
2. Wählen Sie die verfügbare **RADIUS-Aktion** aus der Liste aus.
3. Auf der Seite „ **RADIUS-Authentifizierungsserver konfigurieren** “ haben Sie im Abschnitt **Verbindungseinstellungen** zwei Optionen.
4. Um die RADIUS-Serververbindung zu überprüfen, klicken Sie auf die Registerkarte **RADIUS-Erreichbarkeit testen** .
5. Um die durchgängige RADIUS-Authentifizierung anzuzeigen, klicken Sie auf den Link **Endbenutzerverbindung testen** .

Von der Authentifizierungsoption

1. Navigieren Sie zu **Authentifizierung > Dashboard**und wählen Sie die verfügbare RADIUS-Aktion aus der Liste aus.
2. Auf der Seite „ **RADIUS-Authentifizierungsserver konfigurieren** “ haben Sie im Abschnitt **Verbindungseinstellungen** zwei Optionen.
3. Um die RADIUS-Serververbindung zu überprüfen, klicken Sie auf die Registerkarte **RADIUS-Erreichbarkeit testen** .
4. Um den End-to-End-RADIUS-Authentifizierungsstatus anzuzeigen, klicken Sie auf **Endbenutzerverbindung testen** .

RADIUS-Authentifizierung mit TCP oder TLS

November 28, 2022

Ab Version 13.1—27.59 wird die RADIUS-Authentifizierung auch für TCP- und TLS-Protokolle unterstützt.

> **Hinweis:**
>
> - Die Option **RADIUS-Erreichbarkeit testen** wird für RADIUS auf den TCP- und TLS-Transporttypen nicht unterstützt.

> • Die RADIUS-Authentifizierung mit UDP wird auf FIPS-Appliances nicht unterstützt.

Konfigurieren Sie RADIUS über TCP mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication radiusAction <name> [-serverIP] [-serverPort ] [-
   transport <transport>]
<!--NeedCopy-->
```

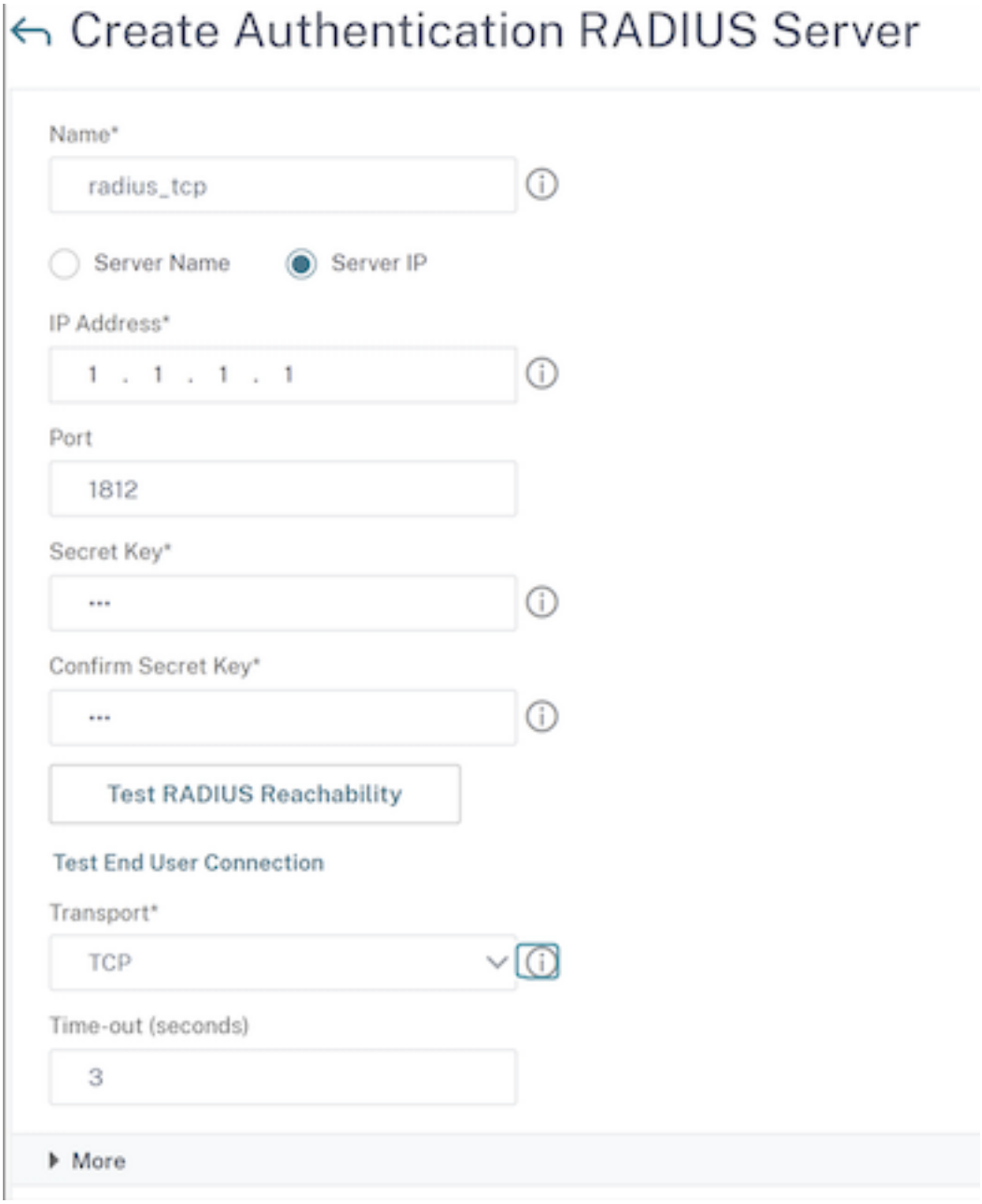
Beispiel:

```
add authentication radiusAction RadAction -serverIP 1.1.1.1 -radkey 123
    -transport TCP
<!--NeedCopy-->
```

Konfigurieren Sie RADIUS über TCP über die GUI

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > RADIUS**.
2. Wählen Sie einen vorhandenen Server aus oder erstellen Sie einen Server.

   Einzelheiten zum Erstellen eines Servers finden Sie unter So konfigurieren Sie einen RADIUS-Server über die GUI.



3. Wählen Sie unter **Transport**die Option **TCP** aus.
4. Klicken Sie auf **Erstellen**.

Konfigurieren Sie RADIUS über TLS mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add authentication radiusAction <name> [-serverIP] [-serverPort ] [-
     transport <transport>] [-targetLBVserver <string>]
2 <!--NeedCopy-->
```


Beispiel

```
add authentication radiusAction RadAction -serverIP 1.1.1.1 -radkey 123
    -transport TLS -targetLBVserver rad-lb
<!--NeedCopy-->
```

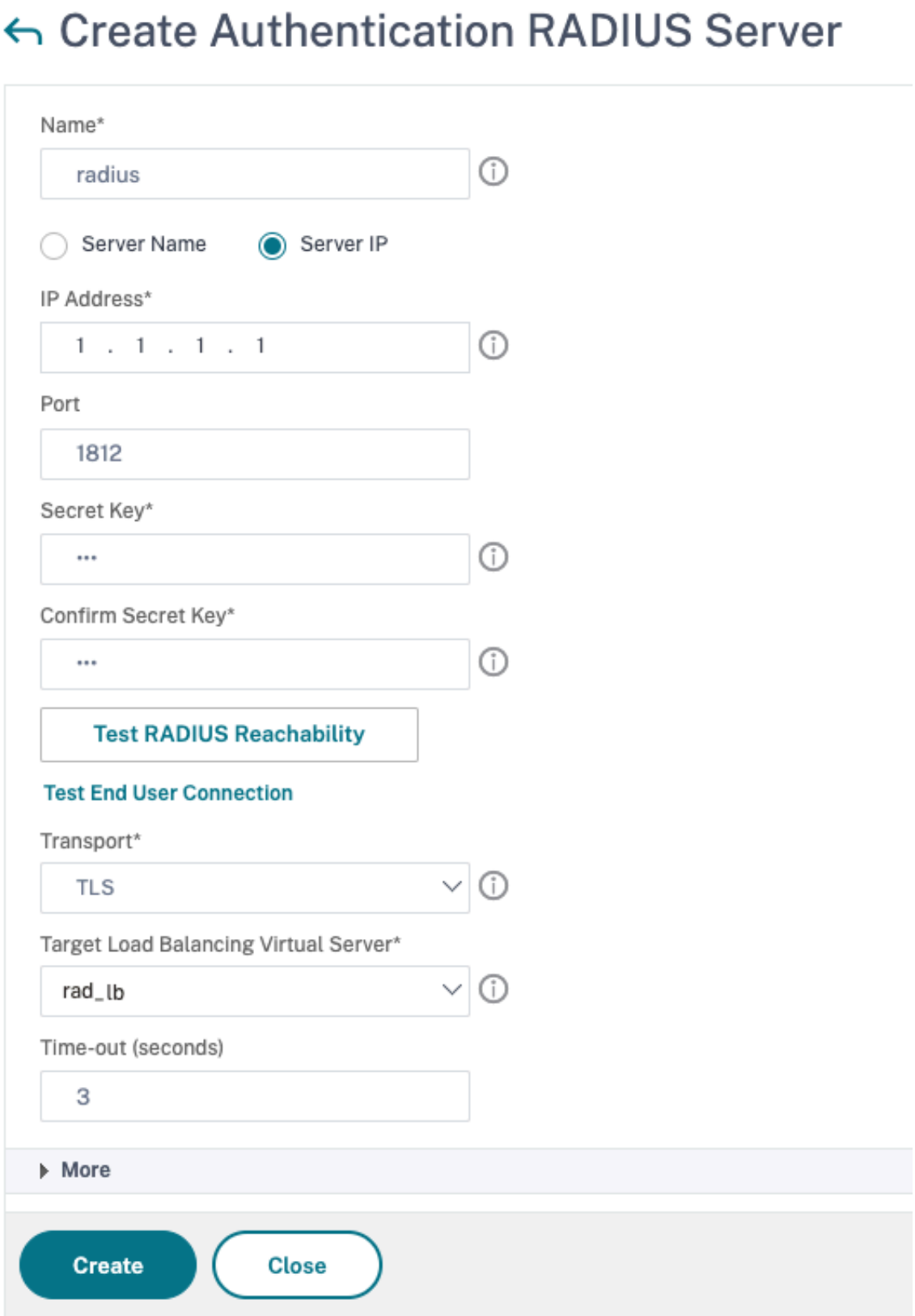
Hinweis:

- Servername wird für den TLS-Transporttyp nicht unterstützt.
- Konfigurieren Sie für den TLS-Transporttyp einen virtuellen Ziellastausgleichsserver vom Typ TCP und binden Sie einen Dienst vom Typ SSL_TCP an diesen virtuellen Server.
- Die IP-Adresse und die Portnummer, die für die RADIUS-Aktion konfiguriert sind, müssen mit der IP-Adresse und der Portnummer des konfigurierten virtuellen Ziel-Lastausgleichsservers übereinstimmen.

Konfigurieren Sie RADIUS über TLS über die GUI

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > Server**.
2. Wählen Sie einen vorhandenen Server aus oder erstellen Sie einen Server.

   Weitere Informationen zum Erstellen eines Servers finden Sie unter So konfigurieren Sie einen RADIUS-Server mithilfe der GUI.



3. Wählen Sie unter **Transport** die Option **TLS** aus.
4. Wählen Sie **unter Target Load Balancing Virtual Server**den virtuellen Server aus. Einzelheiten zum Erstellen eines virtuellen Lastausgleichsservers finden Sie unter Erstellen eines virtuellen Servers.

   > **Hinweis:**
   >
   > - Servername wird für den TLS-Transporttyp nicht unterstützt.
   > - Konfigurieren Sie für den TLS-Transporttyp einen virtuellen Ziellastausgleichsserver vom Typ TCP und binden Sie einen Dienst vom Typ SSL_TCP an diesen virtuellen Server.
   > - Die IP-Adresse und die Portnummer, die für die RADIUS-Aktion konfiguriert sind, müssen mit der IP-Adresse und der Portnummer des konfigurierten virtuellen Ziel-Lastausgleichsservers übereinstimmen.

5. Klicken Sie auf **Erstellen.**

TACACS-Authentifizierung

May 11, 2023

Die TACACS-Authentifizierungsrichtlinie authentifiziert sich bei einem externen Terminal Access Controller Access-Control System (TACACS) -Authentifizierungsserver.
Nachdem sich ein Benutzer bei einem TACACS-Server authentifiziert hat, stellt der NetScaler für alle nachfolgenden Autorisierungen eine Verbindung zu demselben TACACS-Server her. Wenn ein primärer TACACS-Server nicht verfügbar ist, verhindert diese Funktion jegliche Verzögerung, während der ADC auf das Timeout des ersten TACACS-Servers wartet. Dies geschieht, bevor die Autorisierungsanfrage erneut an den zweiten TACACS-Server gesendet wird.

> **Hinweis:**
>
> Der TACACS-Autorisierungsserver unterstützt keine Befehle, deren Zeichenkettenlänge 255 Zeichen überschreitet.
>
> **Problemumgehung:** Verwenden Sie die lokale Autorisierung anstelle eines TACACS-Autorisierungsservers.

Bei der Authentifizierung über einen TACACS-Server werden in den Protokollen zur Authentifizierung, Autorisierung und Überwachung des Verkehrsmanagements nur TACACS-Befehle erfolgreich ausgeführt. Es verhindert, dass in den Protokollen TACACS-Befehle angezeigt werden, die von Benutzern eingegeben wurden, die nicht autorisiert waren, sie auszuführen.

Ab NetScaler 12.0 Build 57.x blockiert das Terminal Access Controller Access-Control System (TACACS)

beim Senden der TACACS-Anfrage nicht den Authentifizierungs-, Autorisierungs- und Überwachungsdaemon. Sie ermöglichen die LDAP- und RADIUS-Authentifizierung, um mit der Anfrage fortzufahren. Die TACACS-Authentifizierungsanfrage wird fortgesetzt, sobald der TACACS-Server die TACACS-Anfrage bestätigt hat.

> **Wichtig:**
>
> - Citrix empfiehlt, keine TACACS-bezogenen Konfigurationen zu ändern, wenn Sie einen Befehl “clear ns config” ausführen.
> - TACACS-bezogene Konfigurationen, die sich auf erweiterte Richtlinien beziehen, werden gelöscht und erneut angewendet, wenn der Parameter „rbaConfig“ im Befehl „clear ns config“ für erweiterte Richtlinien auf NO gesetzt ist.

Unterstützung von Name-Wert-Attributen für die TACACS-Authentifizierung

Sie können jetzt TACACS-Authentifizierungsattribute mit einem eindeutigen Namen zusammen mit Werten konfigurieren. Die Namen werden im TACACS-Aktionsparameter konfiguriert und die Werte werden durch Abfragen der Namen abgerufen. Durch Angabe des Attributwerts für den Namen können Administratoren einfach nach dem Attributwert suchen, der dem Attributnamen zugeordnet ist. Außerdem müssen sich Administratoren das Attribut nicht mehr nur anhand seines Wertes merken.

> **Wichtig**
>
> - Im Befehl tacacsAction können Sie maximal 64 durch Kommas getrennte Attribute mit einer Gesamtgröße von weniger als 2048 Byte konfigurieren.

So konfigurieren Sie die Name-Wert-Attribute mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication tacacsAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Beispiel:

```
add authentication tacacsAction tacacsAct1 -attributes  “mail,sn,
   userprincipalName”
<!--NeedCopy-->
```

So fügen Sie mithilfe der Befehlszeilenschnittstelle eine Authentifizierungsaktion hinzu

Wenn Sie die LOCAL-Authentifizierung nicht verwenden, müssen Sie eine explizite Authentifizierungsaktion hinzufügen. Geben Sie an der Eingabeaufforderung den folgenden Befehl

ein:

```
add authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Beispiel

```
add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812                  -authtimeout 15 -tacacsSecret "
    minotaur" -authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup "users"
<!--NeedCopy-->
```

So konfigurieren Sie eine Authentifizierungsaktion mithilfe der Befehlszeilenschnittstelle

Um eine vorhandene Authentifizierungsaktion zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Beispiel

```
     > set authentication tacacsaction Authn-Act-1 -serverip
        10.218.24.65 -serverport 1812                  -authtimeout 15
        -tacacsSecret "minotaur" -authorization OFF -accounting ON -
        auditFailedCmds OFF -defaultAuthenticationGroup "users"    Done
<!--NeedCopy-->
```

So entfernen Sie eine Authentifizierungsaktion mithilfe der Befehlszeilenschnittstelle

Um eine vorhandene RADIUS-Aktion zu entfernen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm authentication radiusAction <name>
<!--NeedCopy-->
```

Beispiel

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```


Clientzertifikatauthentifizierung

June 19, 2023

Websites, die vertrauliche Inhalte enthalten, wie Online-Banking-Websites oder Websites mit persönlichen Daten von Mitarbeitern, benötigen manchmal Kundenzertifikate zur Authentifizierung. Um Authentifizierung, Autorisierung und Überwachung für die Authentifizierung von Benutzern auf der Grundlage von clientseitigen Zertifikatsattributen zu konfigurieren, aktivieren Sie zunächst die Client-Authentifizierung auf dem virtuellen Traffic Management-Server und binden das Stammzertifikat an den virtuellen Authentifizierungsserver. Anschließend implementieren Sie eine von zwei Optionen. Sie können den Standardauthentifizierungstyp auf dem virtuellen Authentifizierungsserver als CERT konfigurieren, oder Sie können eine Zertifikataktion erstellen, die definiert, was der NetScaler tun muss, um Benutzer basierend auf einem Clientzertifikat zu authentifizieren. In beiden Fällen muss Ihr Authentifizierungsserver CRLs unterstützen. Sie konfigurieren den ADC so, dass er den Benutzernamen aus dem Feld **subjectCN** oder einem anderen angegebenen Feld im Clientzertifikat extrahiert.

Wenn der Benutzer versucht, sich an einem virtuellen Authentifizierungsserver anzumelden, für den keine Authentifizierungsrichtlinie konfiguriert ist, und keine globale Kaskade konfiguriert ist, werden die Benutzernameninformationen aus dem angegebenen Feld des Zertifikats extrahiert. Wenn das erforderliche Feld extrahiert wird, ist die Authentifizierung erfolgreich. Wenn der Benutzer während des SSL-Handshakes kein gültiges Zertifikat angibt oder wenn die Extraktion des Benutzernamens fehlschlägt, schlägt die Authentifizierung fehl. Nach der Validierung des Clientzertifikats zeigt der ADC dem Benutzer eine Anmeldeseite an.

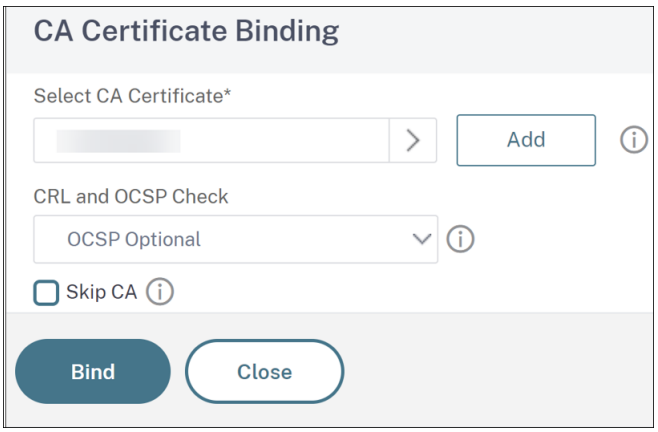
Bei den folgenden Verfahren wird davon ausgegangen, dass Sie bereits eine funktionierende Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration erstellt haben. Daher wird nur erläutert, wie die Authentifizierung mithilfe von Clientzertifikaten aktiviert wird. Bei diesen Verfahren wird auch davon ausgegangen, dass Sie Ihr Root-Zertifikat und Ihre Clientzertifikate erhalten und diese auf dem ADC im Verzeichnis /nsconfig/ssl abgelegt haben.

Konfigurieren der Clientzertifikatauthentifizierung

Konfigurieren Sie die Parameter des Client-Zertifikats mithilfe der GUI

1. Installieren Sie ein CA-Zertifikat und binden Sie es an einen virtuellen Authentifizierungsserver.
    a) Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**.
    b) Wählen Sie auf der daraufhin angezeigten Seite **Virtuelle Authentifizierungsserver** den virtuellen Server aus, den Sie für die Authentifizierung mit Clientzertifikaten konfigurieren möchten, und klicken Sie dann auf **Bearbeiten.**
    c) Navigieren Sie auf der Seite **Virtueller Authentifizierungsserver** zum Abschnitt **Zertifikat** und klicken Sie auf den Rechtspfeil „>“.

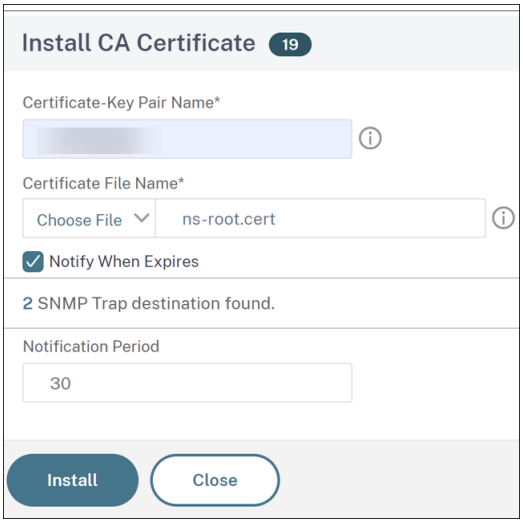
d) Wählen Sie auf der Seite **CA Certificate Binding** ein CA-Zertifikat aus, aktualisieren Sie die anderen erforderlichen Felder und klicken Sie auf **Binden**.



e) Wenn kein CA-Zertifikat verfügbar ist, wählen Sie **Hinzufügen**aus.

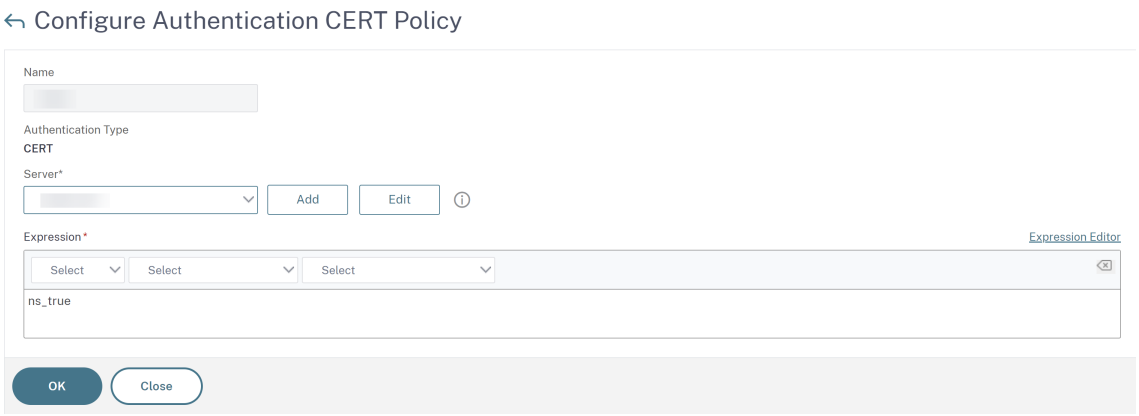
f) Aktualisieren Sie auf der Seite **Zertifikat installieren** die folgenden Felder und klicken Sie auf **Installieren** und dann auf **Schließen**.

- Name des Zertifikatsschlüsselpaars: Name für das Zertifikat und das Paar aus privatem Schlüssel
- Name der Zertifikatsdatei: Der Name der Zertifikatsdatei, die zur Bildung des Zertifikatsschlüsselpaars verwendet wird. Die Zertifikatsdatei muss auf der Festplatte oder dem Solid-State-Laufwerk des NetScalers vorhanden sein. Das Speichern eines Zertifikats an einem anderen Ort als dem Standardspeicherort kann zu Inkonsistenzen in einem Hochverfügbarkeits-Setup führen. Der Standardpfad ist /nsconfig/ssl/.
- Benachrichtigungszeitraum: Anzahl der Tage vor Ablauf des Zertifikats, an denen NetScaler den Administrator darüber informiert, dass das Zertifikat bald abläuft.
- Bei Ablauf benachrichtigen: Aktivieren Sie diese Option, um eine Warnung zu erhalten, wenn das Zertifikat bald abläuft.



g) Sobald das CA-Zertifikat installiert ist, rufen Sie die Seite „ **CA Certificate Binding** “ auf und binden Sie es an einen virtuellen Authentifizierungsserver.

2. Kehren Sie zur Seite **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server** zurück.
3. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Grundrichtlinien > CERT**.
4. Wählen Sie die Richtlinie aus, die Sie für die Authentifizierung mit Client-Zertifikaten konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
5. Gehen Sie auf der Seite **Configure Authentication CERT Policy** zur Dropdownliste **Server** und wählen Sie den virtuellen Server aus, der für die Authentifizierung mit Client-Zertifikaten konfiguriert ist.
6. Klicken Sie auf **OK**.



Konfigurieren Sie die Parameter des Client-Zertifikats mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein, um das Zertifikat zu konfigurieren und die Konfiguration zu überprüfen:

```
1  add ssl certKey <certkeyName> -cert <certFile> -key <keyFile> -password
       -inform <inform> -expiryMonitor <expiryMonitor> -notificationPeriod
       <notificationPeriod>
2
3  bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
      positive_integer>]
4
5  show ssl certKey [<certkeyName>]
6
7  set aaa parameter -defaultAuthType CERT
8
9  show aaa parameter
10
```



```
set aaa certParams -userNameField "Subject:CN"

show aaa certParams
<!--NeedCopy-->
```

Konfigurieren Sie die erweiterten Authentifizierungsrichtlinien für Client-Zertifikate mithilfe der GUI

1. Installieren Sie das CA-Zertifikat und binden Sie es an ein Zertifikatsschlüsselpaar.
   a) Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**.
   b) Wählen Sie auf der daraufhin angezeigten Seite **Virtuelle Authentifizierungsserver** den virtuellen Server aus, den Sie für die Authentifizierung mit Clientzertifikaten konfigurieren möchten, und klicken Sie dann auf **Bearbeiten.**
   c) Navigieren Sie auf der Seite **Virtueller Authentifizierungsserver** zum Abschnitt **Zertifikat** und klicken Sie auf den Rechtspfeil „>“.
   d) Wählen Sie auf der Seite **CA Certificate Binding** ein CA-Zertifikat aus, aktualisieren Sie die anderen erforderlichen Felder und klicken Sie auf **Binden**.
   e) Wenn kein CA-Zertifikat verfügbar ist, wählen Sie **Hinzufügen**aus.
   f) Aktualisieren Sie auf der Seite **Zertifikat installieren** die folgenden Felder und klicken Sie auf **Installieren** und dann auf **Schließen**.
      - Name des Zertifikatsschlüsselpaars: Name für das Zertifikat und das Paar aus privatem Schlüssel
      - Name der Zertifikatsdatei: Der Name der Zertifikatsdatei, die zur Bildung des Zertifikatsschlüsselpaars verwendet wird. Die Zertifikatsdatei muss auf der Festplatte oder dem Solid-State-Laufwerk des NetScalers vorhanden sein. Das Speichern eines Zertifikats an einem anderen Ort als dem Standardspeicherort kann zu Inkonsistenzen in einem Hochverfügbarkeits-Setup führen. Der Standardpfad ist /nsconfig/ssl/.
      - Benachrichtigungszeitraum: Anzahl der Tage vor Ablauf des Zertifikats, an denen NetScaler den Administrator darüber informiert, dass das Zertifikat bald abläuft.
      - Bei Ablauf benachrichtigen: Aktivieren Sie diese Option, um eine Warnung zu erhalten, wenn das Zertifikat bald abläuft.
   g) Sobald das CA-Zertifikat installiert ist, wechseln Sie zur Seite **CA Certificate Binding** und wiederholen Sie Schritt 4.
2. Kehren Sie zur Seite **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server** zurück.

> **Hinweis:**
>
> Wenn Sie ein gültiges CA-Zertifikat und ein Serverzertifikat für den virtuellen Server importiert haben, können Sie die **Schritte 1 und 2**überspringen.

3. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien**und wählen Sie dann **Richtlinie**aus.
4. Führen Sie auf der Seite **Authentifizierungsrichtlinien** einen der folgenden Schritte aus:
   - Um eine Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus und klicken dann auf **Bearbeiten**.
5. Geben Sie auf der Seite **Authentifizierungsrichtlinie erstellen** oder **Authentifizierungsrichtlinie konfigurieren** Werte für die Parameter ein, oder wählen Sie sie aus.
   - Name: Name der Richtlinie. Sie können den Namen einer zuvor konfigurierten Richtlinie nicht ändern.
   - Aktionstyp: Typ der Authentifizierungsaktion.
   - Aktion: Name der Authentifizierungsaktion, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt. Sie können eine vorhandene Authentifizierungsaktion auswählen oder auf **Hinzufügen** klicken und eine Aktion erstellen.
   - Ausdruck: Die Regel, die Verbindungen auswählt, auf die Sie die von Ihnen angegebene Aktion anwenden möchten. Die Regel kann einfach (“wahr” wählt den gesamten Verkehr aus) oder komplex sein. Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unter dem Ausdrucksfenster auswählen und dann Ihren Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen, und die darin enthaltenen Dropdownlisten verwenden, um Ihren Ausdruck zu definieren.
   - Aktion protokollieren: Name der Audit-Aktion, die verwendet werden soll, wenn eine Authentifizierungsanfrage dieser Richtlinie entspricht. Sie können eine bestehende Prüfungsaktion auswählen oder auf **Hinzufügen** klicken, um eine Aktion zu erstellen.
   - Kommentar: Sie können einen Kommentar eingeben, der die Art des Datenverkehrs beschreibt, für den diese Authentifizierungsrichtlinie gilt. Das Feld ist optional.
6. Klicken Sie auf **Erstellen** oder **OK**, und klicken Sie dann auf **Schließen**.

Passthrough für Clientzertifikate

Der NetScaler kann jetzt so konfiguriert werden, dass Clientzertifikate an geschützte Anwendungen weitergegeben werden, die Clientzertifikate für die Benutzerauthentifizierung benötigen. Der ADC authentifiziert zuerst den Benutzer, fügt dann das Clientzertifikat in die Anforderung ein und sendet es an die Anwendung. Diese Funktion wird konfiguriert, indem entsprechende SSL-Richtlinien hinzugefügt werden.

Das genaue Verhalten dieser Funktion, wenn ein Benutzer ein Clientzertifikat vorlegt, hängt von der Konfiguration des virtuellen VPN-Servers ab.

- Wenn der virtuelle VPN-Server so konfiguriert ist, dass er Clientzertifikate akzeptiert, diese aber nicht benötigt, fügt der ADC das Zertifikat in die Anforderung ein und leitet die Anfrage dann an die geschützte Anwendung weiter.
- Wenn auf dem virtuellen VPN-Server die Authentifizierung des Clientzertifikats deaktiviert ist, verhandelt der ADC das Authentifizierungsprotokoll neu und authentifiziert den Benutzer erneut, bevor er das Clientzertifikat in den Header einfügt und die Anforderung an die geschützte Anwendung weiterleitet.
- Wenn der virtuelle VPN-Server so konfiguriert ist, dass er eine Authentifizierung des Clientzertifikats erfordert, verwendet der ADC das Clientzertifikat, um den Benutzer zu authentifizieren, fügt dann das Zertifikat in den Header ein und leitet die Anforderung an die geschützte Anwendung weiter.

In all diesen Fällen konfigurieren Sie das Passthrough des Clientzertifikats wie folgt.

Erstellen und konfigurieren Sie den Passthrough für Client-Zertifikate mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 add vpn vserver <name> SSL <IP> 443
2 <!--NeedCopy-->
```

Ersetzen Sie **Name** durch einen Namen für den virtuellen Server. Der Name muss aus einem bis 127 ASCII-Zeichen bestehen, beginnend mit einem Buchstaben oder Unterstrich (_) und nur Buchstaben, Zahlen und Unterstrich, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-). Ersetzen Sie <IP> durch die dem virtuellen Server zugewiesene IP-Adresse.

```
1 set ssl vserver <name> -clientAuth ENABLED -clientCert <clientcert>
2 <!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen Servers, den Sie erstellt haben. Ersetzen Sie <clientCert> durch einen der folgenden Werte:

- disabled — Deaktiviert die Authentifizierung des Clientzertifikats auf dem virtuellen VPN-Server.
- mandatory — konfiguriert den virtuellen VPN-Server so, dass Clientzertifikate für die Authentifizierung erforderlich sind.
- optional — konfiguriert den virtuellen VPN-Server so, dass er die Authentifizierung mit Clientzertifikaten zulässt, sie aber nicht erfordert.

```
1 bind vpn vserver <name> -policy local
2 <!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen VPN-Servers, den Sie erstellt haben.


```
bind vpn vserver <name> -policy cert
<!--NeedCopy-->
```

Ersetzen Sie <name> druch den Namen des virtuellen VPN-Servers, den Sie erstellt haben.

```
bind ssl vserver <name> -certkeyName <certkeyname>
<!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen Servers, den Sie erstellt haben. Ersetzen Sie <certkeyName> druch den Schlüssel des Clientzertifikats.

```
bind ssl vserver <name> -certkeyName <cacertkeyname> -CA -ocspCheck
    Optional
<!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen Servers, den Sie erstellt haben. Ersetzen Sie <cacertkeyName> durch den Schlüssel des CA-Zertifikats.

```
add ssl action <actname> -clientCert ENABLED -certHeader CLIENT-CERT
<!--NeedCopy-->
```

Ersetzen Sie <actname> durch einen Namen für die SSL-Aktion.

```
add ssl policy <polname> -rule true -action <actname>
<!--NeedCopy-->
```

Ersetzen Sie <polname> durch einen Namen für Ihre neue SSL-Richtlinie. Ersetzen Sie <actname> durch den Namen der SSL-Aktion, die Sie erstellt haben.

```
bind ssl vserver <name> -policyName <polname> -priority 10
<!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen VPN-Servers.

Beispiel

```
add vpn vserver vs-certpassthru SSL 10.121.250.75 443
set ssl vserver vs-certpassthru -clientAuth ENABLED -clientCert
    optional
bind vpn vserver vs-certpassthru -policy local
bind vpn vserver vs-certpassthru -policy cert
bind ssl vserver vs-certpassthru -certkeyName mycertKey
bind ssl vserver vs-certpassthru -certkeyName mycertKey -CA -ocspCheck
    Optional
```



```
add ssl action act-certpassthru -clientCert ENABLED -certHeader CLIENT-
    CERT
add ssl policy pol-certpassthru -rule true -action act-certpassthru
bind ssl vserver vs-certpassthru -policyName pol-certpassthru -priority
     10
<!--NeedCopy-->
```

Authentifizierung aushandeln

May 11, 2023

Wie bei anderen Arten von Authentifizierungsrichtlinien besteht eine Negotiate-Authentifizierungsrichtlinie aus einem Ausdruck und einer Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, bezeichnen Sie es auch als primäre oder sekundäre Richtlinie.

Zusätzlich zu den Standardauthentifizierungsfunktionen kann der Befehl Negotiate Action jetzt Benutzerinformationen aus einer Keytab-Datei extrahieren, anstatt dass Sie diese Informationen manuell eingeben müssen. Wenn ein Keytab mehr als einen SPN hat, wählen Authentifizierung, Autorisierung und Überwachung den richtigen SPN aus. Sie können diese Funktion über die Befehlszeile oder mithilfe des Konfigurationsprogramms konfigurieren.

> **Hinweis**
>
> Bei diesen Anweisungen wird davon ausgegangen, dass Sie bereits mit dem LDAP-Protokoll vertraut sind und Ihren ausgewählten LDAP-Authentifizierungsserver bereits konfiguriert haben.

So konfigurieren Sie Authentifizierung, Autorisierung und Überwachung zum Extrahieren von Benutzerinformationen aus einer Keytab-Datei mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile den entsprechenden Befehl ein:

```
add authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd  }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]

```



```
set authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]
<!--NeedCopy-->
```

Parameter description

- **Name** — Name der Verhandlungsaktion, die verwendet werden soll.
- **domain — Domänenname** des Serviceprinzips, der NetScaler darstellt.
- **DomainUser — Der** Benutzername des Kontos, das dem NetScaler-Prinzip zugeordnet ist. Dies kann zusammen mit Domain und Passwort angegeben werden, wenn die Keytab-Datei nicht verfügbar ist. Wenn der Benutzername zusammen mit der Keytab-Datei angegeben wird, wird diese Keytab-Datei nach den Anmeldeinformationen dieses Benutzers durchsucht. Maximale Länge: 127
- **domainUserPasswd** — Passwort des Kontos, das dem NetScaler-Prinzip zugeordnet ist.
- **DefaultAuthenticationGroup** — Dies ist die Standardgruppe, die ausgewählt wird, wenn die Authentifizierung erfolgreich ist, zusätzlich zu den extrahierten Gruppen. Maximale Länge: 63
- **keytab** — Der Pfad zur Keytab-Datei, die zum Entschlüsseln von Kerberos-Tickets verwendet wird, die NetScaler präsentiert werden. Wenn Keytab nicht verfügbar ist, können Domäne/Benutzername/Passwort in der Konfiguration der Verhandlungsaktion angegeben werden. Maximale Länge: 127
- **ntlmPath** — Der Pfad zu der Site, die für die NTLM-Authentifizierung aktiviert ist, einschließlich des FQDN des Servers. Dies wird verwendet, wenn Clients auf NTLM zurückgreifen. Maximale Länge: 127

So konfigurieren Sie Authentifizierung, Autorisierung und Überwachung zum Extrahieren von Benutzerinformationen aus einer Keytab-Datei mithilfe des Konfigurationsprogramms

> Hinweis
>
> Im Konfigurationsdienstprogramm wird der Begriff Server anstelle von Aktion verwendet, bezieht sich jedoch auf dieselbe Aufgabe.

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Authentifizierung > Erweiterte Richtlinien > Aktionen > NEGOTIE-Aktionen**.
2. Führen Sie im Detailbereich auf der Registerkarte **Server** einen der folgenden Schritte aus:

- Wenn Sie eine neue **Verhandlungsaktion** erstellen möchten, klicken Sie auf **Hinzufügen**.
- Wenn Sie eine bestehende **Negotiate-Aktion** ändern möchten, wählen Sie im Datenbereich die Aktion aus, und klicken Sie dann auf **Bearbeiten**.

3. Wenn Sie eine neue ****Negotiate-Aktion**** erstellen, geben Sie im Textfeld Name einen Namen für Ihre neue Aktion ein. Der Name kann ein bis 127 Zeichen lang sein und aus Groß- und Kleinbuchstaben, Zahlen sowie Bindestrichen (-) und Unterstrichen (_) bestehen. Wenn Sie eine bestehende Negotiate-Aktion ändern, überspringen Sie diesen Schritt. Der Name ist schreibgeschützt; Sie können ihn nicht ändern.
4. Falls das Kontrollkästchen Keytab-Datei verwenden unter **Negotiate**noch nicht aktiviert ist, aktivieren Sie es.
5. Geben Sie in das Textfeld Keytab-Dateipfad den vollständigen Pfad und den Dateinamen der Keytab-Datei ein, die Sie verwenden möchten.
6. Geben Sie in das Textfeld Standardauthentifizierungsgruppe die Authentifizierungsgruppe ein, die Sie als Standard für diesen Benutzer festlegen möchten.
7. Klicken Sie auf **Erstellen** oder **OK**, um Ihre Änderungen zu speichern.

Hinweise, die bei der Verwendung erweiterter Verschlüsselungen für die Kerberos-Authentifizierung zu beachten sind

> - **Beispielkonfiguration bei Verwendung von Keytab:** Authentifizierung hinzufügen NegotiateAction neg_act_aes256 -keytab „/nsconfig/krb/lbvs_aes256.keytab“
> - **Verwenden Sie den folgenden Befehl, wenn keytab über mehrere Verschlüsselungstypen verfügt.** Der Befehl erfasst zusätzlich Domänenbenutzerparameter: add authentication negotiateAction neg_act_keytab_all -keytab “/nsconfig/krb/lbvs_all.keytab” -domainUser “HTTP/lbvs.aaa.local”
> - **Verwenden Sie die folgenden Befehle, wenn Benutzeranmeldeinformationen verwendet werden:** add authentication negotiateAction neg_act_user -domain AAA.LOCAL -domainUser “HTTP/lbvs.aaa.local” -domainUserPasswd <password>
> - Stellen Sie sicher, dass die richtigen **domainUser**-Informationen bereitgestellt werden. Sie können in AD nach dem Benutzeranmeldenamen suchen.

Web-Authentifizierung

May 11, 2023

Authentifizierung, Autorisierung und Überwachung ist nun in der Lage, einen Benutzer bei einem Webserver zu authentifizieren, indem er die Anmeldeinformationen bereitstellt, die der Webserver in einer HTTP-Anforderung benötigt, und die Antwort des Webservers analysieren, um

festzustellen, dass die Benutzerauthentifizierung erfolgreich war. Wie bei anderen Arten von Authentifizierungsrichtlinien besteht eine Webauthentifizierungsrichtlinie aus einem Ausdruck und einer Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, bezeichnen Sie es auch als primäre oder sekundäre Richtlinie.

Um die webbasierte Authentifizierung mit einem bestimmten Webserver einzurichten, erstellen Sie zunächst eine Webauthentifizierungsaktion. Da bei der Authentifizierung bei Webservern kein starres Format verwendet wird, müssen Sie beim Erstellen der Aktion genau angeben, welche Informationen der Webserver benötigt und in welchem Format. Zu diesem Zweck erstellen Sie einen Ausdruck in der NetScaler-Appliance Advanced-Richtlinie, der die folgenden Elemente enthält:

- **Server-IP**— Die IP-Adresse des Authentifizierungs-Webservers.
- **Serverport**— Der Port des Authentifizierungs-Webservers.
- **Authentifizierungsregel**— Ein Ausdruck in der NetScaler-Appliance Advanced-Richtlinie, der die Anmeldeinformationen des Benutzers in dem vom Webserver erwarteten Format enthält.
- **Schema**—HTTP (für unverschlüsselte Webauthentifizierung) oder HTTPS (für verschlüsselte Webauthentifizierung).
- **Erfolgsregel**— Ein Ausdruck in der NetScaler-Appliance Advanced-Richtlinie, der der Webserver-Antwortzeichenfolge entspricht, die angibt, dass sich der Benutzer erfolgreich authentifiziert

Befolgen Sie für alle anderen Parameter die normalen Regeln für den Befehl zum Hinzufügen der Authentifizierung.

Als Nächstes erstellen Sie eine Richtlinie, die mit dieser Aktion verknüpft ist. Die Richtlinie ähnelt einer LDAP-Richtlinie und verwendet wie LDAP-Richtlinien die NetScaler-Appliance-Syntax.

> **Hinweis**
>
> Bei diesen Anweisungen wird davon ausgegangen, dass Sie bereits mit den Authentifizierungsanforderungen der Webserver vertraut sind, bei denen Sie sich authentifizieren möchten, und den Webauthentifizierungsserver bereits konfiguriert haben.

So konfigurieren Sie eine Webauthentifizierungsaktion über die Befehlszeile

Um eine Webauthentifizierungsaktion an der Befehlszeile zu erstellen, geben Sie an der Befehlszeile den folgenden Befehl ein:

```
1 add authentication webAuthAction <name> -serverIP <ip_addr|ipv6_addr
    |\*> -serverPort <port|\*> [-fullReqExpr <string>] -scheme ( http |
    https ) -successRule <expression> [-defaultAuthenticationGroup <
    string>][-Attribute1 <string>][-Attribute2 <string>] [-Attribute3 <
    string>][-Attribute4 <string>] [-Attribute5 <string>][-Attribute6 <
```



```
    string>] [-Attribute7 <string>][-Attribute8 <string>] [-Attribute9 <
    string>][-Attribute10 <string>] [-Attribute11 <string>][-Attribute12
     <string>] [-Attribute13 <string>][-Attribute14 <string>] [-
    Attribute15 <string>][-Attribute16 <string>]
<!--NeedCopy-->
```

Beispiel

```
add policy expression post_data ""username=" + http.REQ.BODY(1000).
    SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&") + "&
    passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR
    ("passwd=")"

add policy expression length_post_data "("username= " + http.REQ.BODY
    (1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&")
     + "passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).
    AFTER_STR("passwd=")).length"

add authentication webAuthAction webAuth_POST -serverIP 10.106.187.54 -
    serverPort 80 -fullReqExpr q{
 "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." + http.req
    .version.major + "\r\nAccept:\*/\*\r\nHost: 10.106.187.54\r\
    nReferer: http://10.106.187.54/MyPHP/auth.php\r\nAccept-Language:
    en-US\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
    6.1; Trident/5.0)\r\nContent-Type: application/x-www-form-
    urlencoded\r\n" + "Content-Length: " + length_post_data + "\r\
    nConnection: Keep-Alive\r\n\r\n" + post_data }
  -scheme http -successRule "http.res.status.eq(200)"
<!--NeedCopy-->
```

So konfigurieren Sie eine Webauthentifizierungsaktion mithilfe des Konfigurationsprogramms

> **Hinweis**
>
> Im Konfigurationsdienstprogramm wird der Begriff Server anstelle von Aktion verwendet, bezieht sich jedoch auf dieselbe Aufgabe.

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > LDAP**.
2. Führen Sie im Detailbereich auf der Registerkarte **Server** einen der folgenden Schritte aus:
   - Wenn Sie eine neue Webauthentifizierungsaktion erstellen möchten, klicken Sie auf **Hinzufügen**.

- Wenn Sie eine vorhandene Webauthentifizierungsaktion ändern möchten, wählen Sie im Datenbereich die Aktion aus, und klicken Sie dann auf **Bearbeiten**.

3. Wenn Sie eine neue Webauthentifizierungsaktion **erstellen, geben Sie im Dialogfeld Authentifizierungs-Webserver** erstellen im Textfeld **Name** einen Namen für die neue Webauthentifizierungsaktion ein. Der Name kann ein bis 127 Zeichen lang sein und aus Groß- und Kleinbuchstaben, Zahlen sowie Bindestrich (-) und Unterstrichen (_) bestehen. Wenn Sie eine bestehende Webauthentifizierungsaktion ändern, überspringen Sie diesen Schritt. Der Name ist schreibgeschützt; Sie können ihn nicht ändern.
4. Geben Sie im Textfeld **Webserver-IP-Adresse** die IPv4- oder IPv6-IP-Adresse des Authentifizierungs-Webservers ein. Handelt es sich bei der Adresse um eine IPv6-IP-Adresse, aktivieren Sie zuerst das Kontrollkästchen IPv6.
5. Geben Sie im Textfeld Port die Portnummer ein, auf der der Webserver Verbindungen akzeptiert.
6. Wählen Sie in der Dropdownliste **Protokoll** die Option **HTTP** oder **HTTPS** aus.
7. Geben Sie im Textbereich HTTP-Request-Ausdruck einen regulären Ausdruck im PCRE-Format ein, der die Webserver-Anforderung erstellt, die die Anmeldeinformationen des Benutzers in dem vom Authentifizierungs-Webserver erwarteten Format enthält.
8. Geben Sie im Textbereich Ausdruck zur Überprüfung des Textbereichs Authentifizierung einen erweiterten Richtlinienausdruck der NetScaler-Appliance ein, der die Informationen in der Webserverantwortung beschreibt, die darauf hinweisen, dass die Benutzerauthentifizierung erfolgreich war.
9. Füllen Sie die verbleibenden Felder aus, wie in der Dokumentation zur allgemeinen Authentifizierungsaktion beschrieben.
10. Klicken Sie auf **OK**.

SMS-OTP für die Webauthentifizierung konfigurieren

June 19, 2023

NetScaler kann jetzt in einen SMS-Anbieter eines Drittanbieters integriert werden, um eine zusätzliche Authentifizierungsebene bereitzustellen.

Die NetScaler-Appliance kann so konfiguriert werden, dass ein OTP auf dem Handy des Benutzers als zweiten Authentifizierungsfaktor gesendet wird. Die Appliance legt dem Benutzer ein Anmeldeformular zur Eingabe des OTP nach erfolgreicher AD-Anmeldung vor. Erst nach der erfolgreichen Validierung der SMS-OTP-Authentifizierung wird dem Benutzer die angeforderte Ressource angezeigt.

Um die SMS-OTP-Authentifizierung zu erreichen, stützt sich die NetScaler-Appliance auf die folgenden Faktoren im Backend.

1. Authentifizieren Sie den Benutzer über die LDAP-Authentifizierung und extrahieren Sie die Handynummer des Benutzers.
2. Erstellen Sie OTP und speichern Sie es in der NS-Variablen. Konfiguration und Verwendung von Variablen.
3. Senden Sie das OTP über die WebAuth-Authentifizierungsmethode an die aus LDAP extrahierte Handynummer.
4. Validieren Sie das OTP.

Voraussetzungen

OTP Store konfigurieren

Administratoren richten eine Datenbank/einen Store ein, um OTPs zu speichern, die für die SMS-Authentifizierung verwendet werden, indem sie den folgenden CLI-Befehl verwenden.

```
add ns variable otp_store -type "map(text(65),text(6),100000)" -
    ifValueTooBig undef -ifNoValue undef -expires 5
<!--NeedCopy-->
```

Generieren Sie zufälliges OTP pro Benutzersitzung

Verwenden Sie den folgenden Befehl, um ein 6-stelliges zufälliges OTP pro Benutzersitzung zu generieren und im OTP-Store zu speichern.

```
add ns assignment generate_otp -variable "$otp_store[AAA.USER.SESSIONID
    ]" -set ("000000" + SYS.RANDOM.MUL(1000000).
    TYPECAST_UNSIGNED_LONG_AT.TYPECAST_TEXT_T).SUFFIX(6)
<!--NeedCopy-->
```

Konfigurieren Sie die SMS-OTP-Authentifizierung mit NetScaler

- Bevor Sie die Funktion zur Zwei-Faktor-Authentifizierung von SMS-Zwei-Faktor-Authentifizierung konfigurieren, müssen Sie eine LDAP-Authentifizierung auf einer NetScaler-Appliance als ersten Faktor bei aktivierter Authentifizierung konfiguriert haben. Anweisungen zum Konfigurieren der LDAP-Authentifizierung finden Sie unter So konfigurieren Sie die LDAP-Authentifizierung mit dem Konfigurationsdienstprogramm.
- Konfigurieren Sie LDAP und extrahieren Sie die Handynummer, die für die SMS-OTP-Authentifizierung verwendet werden soll.

Beispielkonfiguration für den ersten Faktor

```
add authentication ldapAction ldap_action -serverIP 1.1.1.1 -serverPort
     3268 -authTimeout 30 -ldapBase "dc=nsi-test,dc=com" -ldapBindDn
    Administrator@nsi-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samaccountname -groupAttrName memberOf -
    ssoNameAttribute samaccountname  -Attribute1 mobile -email mail

add authentication Policy ldap_policy -rule true -action ldap_action
<!--NeedCopy-->
```

> **Hinweis**
>
> Die Handynummer kann mit AAA.USER.ATTRIBUTE (1) extrahiert und beim Senden an den Backend-Server einbezogen werden.

Beispielkonfiguration für den zweiten Faktor

Mit der folgenden Beispielkonfiguration wird ein OTP generiert, das an den Endbenutzer gesendet werden soll.

```
add authentication policylabel set_otp -loginSchema LSCHEMA_INT

add authentication Policy set_otp -rule true -action test

add authentication policy cascade_noauth -rule true -action NO_AUTHN

add authentication Policy check_otp -rule "$test.valueExists(AAA.USER.
    SESSIONID)" -action NO_AUTHN

add authentication policylabel check_otp -loginSchema LSCHEMA_INTbind
    authentication policylabel set_otp -policyName set_otp -priority 1 -
    gotoPriorityExpression NEXT

bind authentication policylabel set_otp -policyName cascade_noauth -
    priority 2 -gotoPriorityExpression NEXT -nextFactor check_otpbind
    authentication policylabel check_otp -policyName wpp -priority 1 -
    gotoPriorityExpression NEXT

bind authentication policylabel check_otp -policyName
    wpp_cascade_noauth -priority 2 -gotoPriorityExpression NEXT -
    nextFactor otp_verifyadd authentication Policy wpp -rule true -
    action webAuth_POST

```



```
15 add authentication Policy wpp_cascade_noauth -rule true -action
      NO_AUTHNadd authentication Policy otp_verify -rule "AAA.LOGIN.
      PASSWORD.EQ($test[AAA.USER.SESSIONID])" -action NO_AUTHN
16
17 add authentication policylabel otp_verify -loginSchema onlyPassword
18
19 bind authentication policylabel otp_verify -policyName otp_verify -
      priority 1 -gotoPriorityExpression NEXTadd authentication vserver
      avs SSL 10.106.40.121 443
20
21 bind authentication vserver avs -policy ldap_policy  -priority 1 -
      nextFactor set_otp -gotoPriorityExpression NEXT
22 <!--NeedCopy-->
```

Beispielkonfiguration für einen dritten Faktor

Unter Verwendung der folgenden Beispielkonfiguration wird das in der Konfiguration des zweiten Faktors generierte OTP mithilfe der Webauthentifizierungsmethode an den Endbenutzer gesendet. Einzelheiten zur Webauthentifizierung finden Sie unter Webauthentifizierung.

- Beispiel einer Webauthentifizierungskonfiguration, wenn der SMS-Server die API über die GET-Methode verfügbar

```
1  add policy expression otp_exp_get ""method=sendMessage&send_to="
      + AAA.USER.ATTRIBUTE(1) + "&msg=OTP is " + $otp_store[AAA.USER
      .SESSIONID] + "for login into secure access  gateway. Valid
      till EXPIRE_TIME. Do not share the OTP with anyone for
      security reasons.&userid=#####&password=###=1.0""
2
3  add authentication webAuthAction webAuth_Get -serverIP
      10.106.168.210 -serverPort 8080 -fullReqExpr q{
4  "GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
      version.major + "." + http.req.version.minor.sub(1) + "\r\
      nAccept:\*/\*\r\nHost: <FQDN>\r\n" }
5   -successRule "http.res.status.eq(200)" -scheme http
6  <!--NeedCopy-->
```

- Beispiel für eine Webauthentifizierungskonfiguration, wenn der SMS-Server die API über die POST-Methode

```
1  add policy expression otp_exp_post ""Message: OTP is " +
      $otp_store[AAA.USER.SESSIONID] + "for login into secure access
        gateway. Valid till EXPIRE_TIME. Do not share the OTP with
      anyone for security reasons&Mobile:" + AAA.USER.ATTRIBUTE(1)"
```



```
2
3  add authentication webAuthAction webAuth_POST -serverIP
      10.106.168.210 -serverPort 8080 -fullReqExpr q{
4  "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." +
      http.req.version.major + "\r\nAccept:\*/\*\r\nHost:
      10.106.168.210 \r\nContent-Length: 10\r\n\r\n" + otp_exp_post
      }
5   -scheme http -successRule true
6  <!--NeedCopy-->
```

```
1  add authentication webAuthAction webAuth_Get -serverIP
      10.106.168.210 -serverPort 8080 -fullReqExpr q{
2  "GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
      version.major + "." + http.req.version.minor.sub(1) + "\r\
      nAccept:/\r\nHost: <FQDN>\r\n" }
3   -successRule "http.res.status.eq(200)" -scheme http
4
5  add policy expression otp_exp_post "$otp_store[AAA.USER.SESSIONID
      ]"
6  <!--NeedCopy-->
```

- Senden Sie abschließend das OTP.

```
1  add authentication Policy wpp -rule true -action webAuth_POST
2
3  add authentication policylabel send_otp -loginSchema LSCHEMA_INT
4  bind authentication policylabel send_otp -policyName wpp -
      priority 1 -gotoPriorityExpression NEXT
5  <!--NeedCopy-->
```

Beispielkonfiguration für den vierten Faktor

Überprüfen Sie anhand der folgenden Beispielkonfiguration das an den Endbenutzer gesendete OTP.

In dieser Konfiguration wird eine Richtlinienregel verwendet, um das OTP anhand des OTP zu validieren, das an den Endbenutzer gesendet wird.

```
1  add authentication Policy otp_verify -rule "AAA.LOGIN.PASSWORD.EQ(
      $otp_store[AAA.USER.SESSIONID])" -action NO_AUTHN
2
3  add authentication policylabel otp_verify -loginSchema onlyPassword
4
5  bind authentication policylabel otp_verify -policyName otp_verify -
      priority 1 -gotoPriorityExpression NEXT
```



```
6
7 <!--NeedCopy-->
```

Verwenden Sie den folgenden Befehl, um das OnlyPassword-Anmeldeschema hinzuzufügen:

```
1 add authentication loginSchema onlypassword -authenticationschema /
     nsconfig/loginschema/LoginSchema/OnlyPassword.xml"
2 <!--NeedCopy-->
```

Verknüpfen Sie alle Faktoren für eine erfolgreiche SMS-OTP-Authentifizierung

Verwenden Sie die folgenden CLI-Befehle, um alle Faktoren miteinander zu verknüpfen.

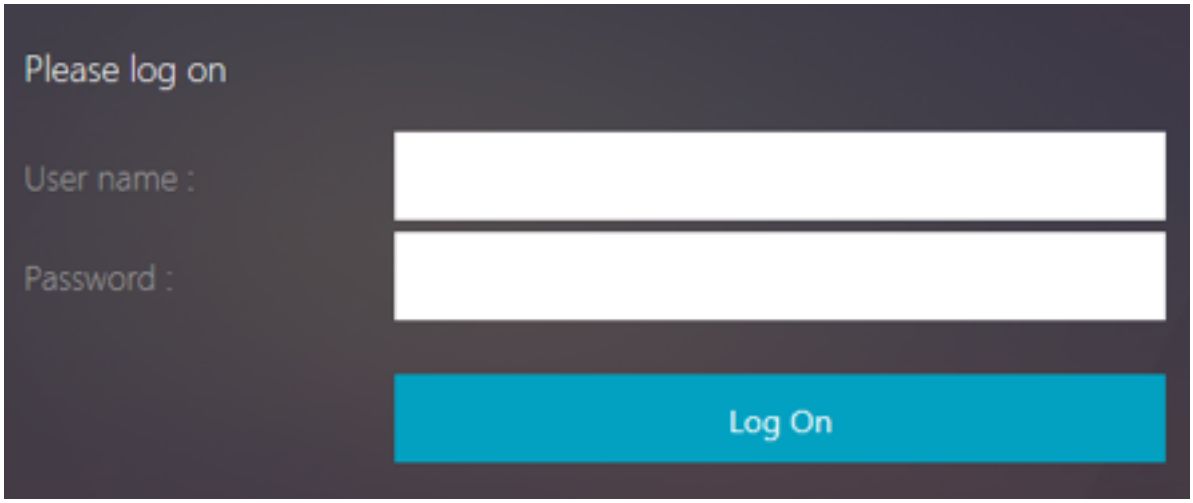
```
1 bind authentication policylabel send_otp -policyName wpp -priority 1 -
     gotoPriorityExpression NEXT -nextFactor otp_verify
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die Richtlinie für die kaskadierende Authentifizierung wurde hinzugefügt, um eine zuverlässige und kontinuierliche Authentifizierung für die Endbenutzer zu ermöglichen. Wenn der aktuelle Faktor ausfällt, wird der nächste Faktor so bewertet, dass das Benutzererlebnis nicht beeinträchtigt wird.

Formularbasierte Authentifizierung

August 19, 2021

Bei der formularbasierten Authentifizierung wird dem Endbenutzer ein Anmeldeformular angezeigt. Diese Art von Authentifizierungsformular unterstützt sowohl die Multifaktor-Authentifizierung (nFactor) als auch die klassische Authentifizierung.



Stellen Sie sicher, dass die formularbasierte Authentifizierung funktioniert:

- Auf dem virtuellen Lastausgleichsserver muss die Authentifizierung **eingeschaltet**sein.
- Der Parameter 'AuthenticationHost' muss angegeben werden, an den der Benutzer zur Authentifizierung umgeleitet werden muss. Der Befehl zum Konfigurieren des gleichen lautet wie folgt:

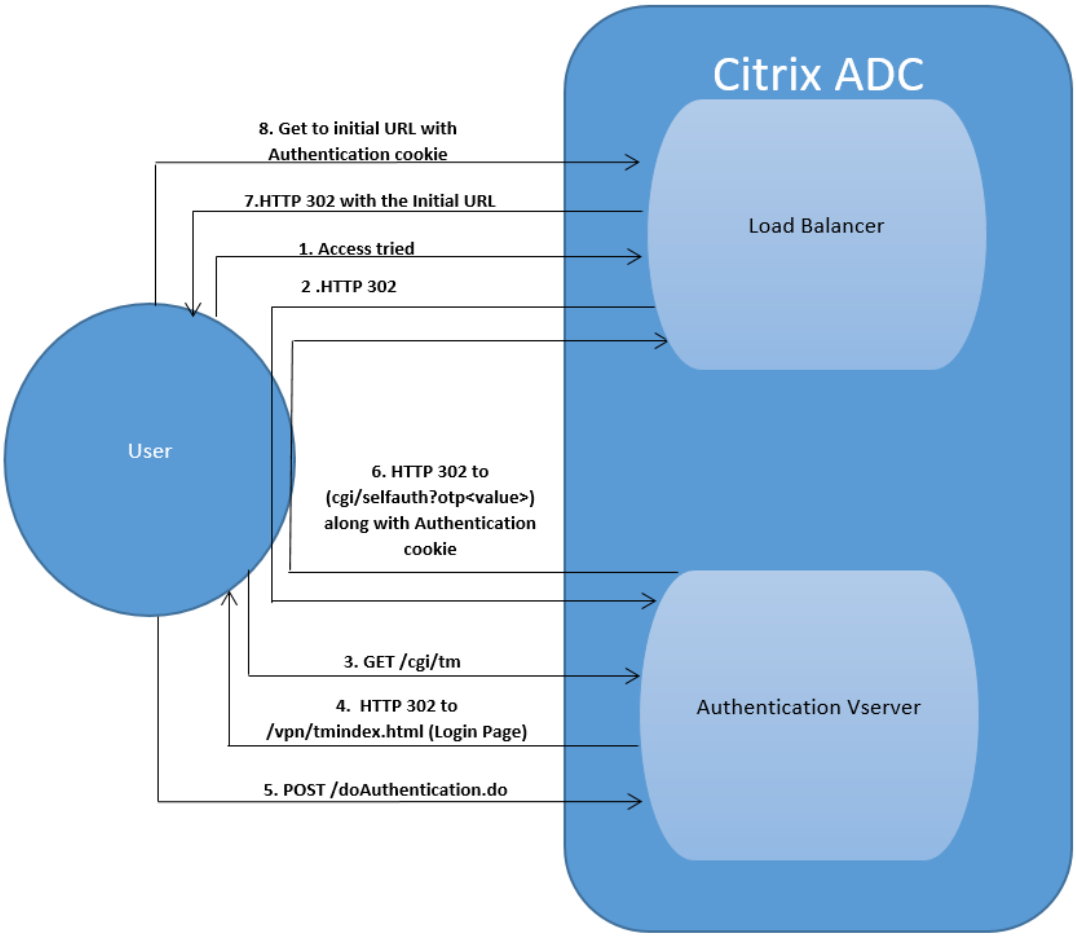
```
1  set lb vs lb1 -authentication on  - authenticationhost aaavs-ip/
      fqdn
```

- Die formularbasierte Authentifizierung ist mit einem Browser kompatibel, der HTML unterstützt

In den folgenden Schritten wird erläutert, wie die formularbasierte Authentifizierung funktioniert:

1. Der Client (Browser) sendet eine GET-Anforderung für eine URL auf dem virtuellen TM-Server (Load Balancing/CS).
2. Der virtuelle TM-Server ermittelt, dass der Client nicht authentifiziert wurde, und sendet eine HTTP 302-Antwort an den Client. Die Antwort enthält ein verstecktes Skript, das bewirkt, dass der Client eine GET-Anforderung für /cgi/tm an den virtuellen Authentifizierungsserver ausgibt.
3. Der Client sendet GET /cgi/tm mit der Ziel-URL an den virtuellen Authentifizierungsserver.
4. Der virtuelle Authentifizierungsserver sendet eine Umleitung an die Anmeldeseite.
5. Der Benutzer sendet seine Anmeldeinformationen mit POST /DoAuthentication.do an den virtuellen Authentifizierungsserver. Die Authentifizierung erfolgt durch den virtuellen Authentifizierungsserver.
6. Wenn die Anmeldeinformationen korrekt sind, sendet der virtuelle Authentifizierungsserver eine HTTP 302-Antwort an die cgi/selfauth-URL auf dem Lastausgleichsserver mit einem One-Token (OTP).
7. Der Lastausgleichsserver sendet HTTP 302 an den Client.

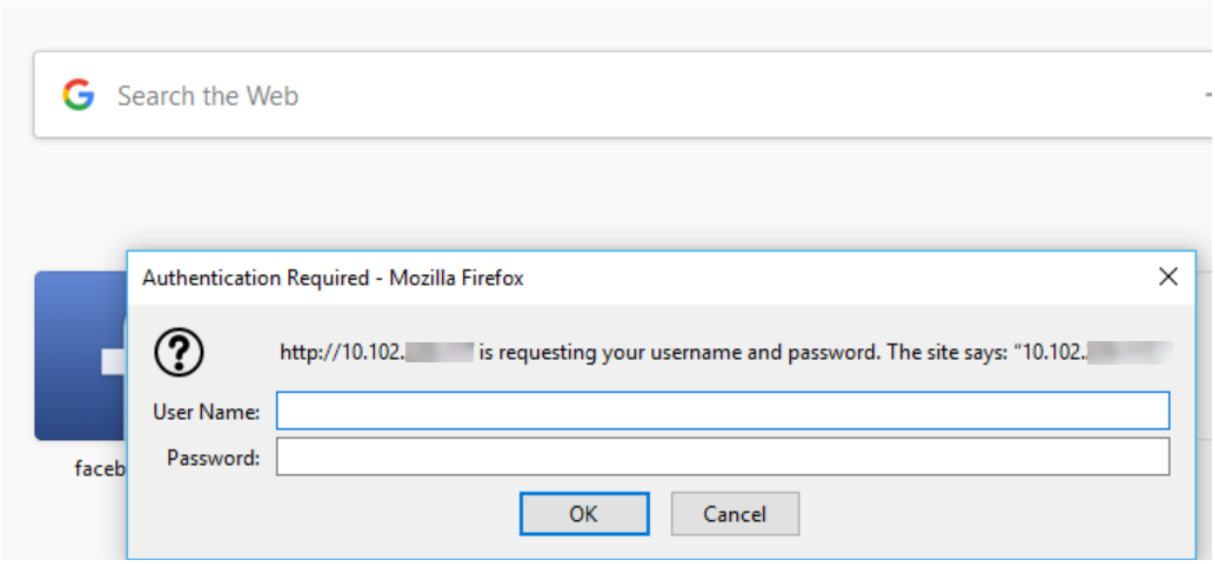
8. Der Client sendet eine GET-Anforderung für ihre ursprüngliche URL-Ziel-URL zusammen mit einem 32-Byte-Cookie.



401-basierte Authentifizierung

May 11, 2023

Mit der 401-basierten Authentifizierung zeigt die NetScaler-Appliance dem Endbenutzer ein Popup-Dialogfeld an.



Das formularbasierte AAA-TM arbeitet mit den Umleitungsnachrichten. Einige Anwendungen unterstützen keine Weiterleitungen. In solchen Fällen wird die 401-Authentifizierung mit aktivierter AAA-TM verwendet.

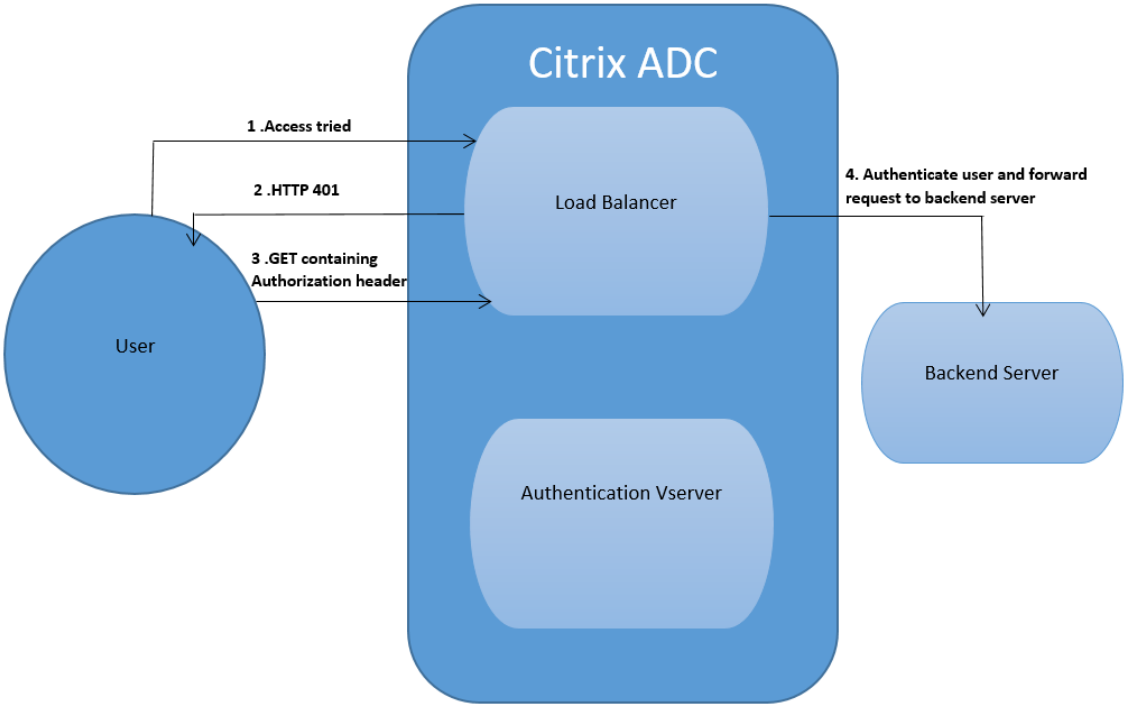
Aktivieren Sie die folgenden Parameter, damit 401 Authentication AAA-TM funktioniert.

- Der 'AuthNVSName' -Parameterwert für den virtuellen Lastausgleichsserver muss der Name des virtuellen Authentifizierungsservers sein, der zur Authentifizierung von Benutzern verwendet werden soll.
- 'authn401' -Parameter muss aktiviert sein. Der Befehl zum Konfigurieren des gleichen lautet wie folgt:

```
set lb vs lb1 -authn401 on -authnvsName <aaavs-name>
```

Die folgenden Schritte führen Sie durch, wie die 401-Authentifizierung funktioniert:

1. Der Benutzer versucht, über den virtuellen Lastausgleichsserver auf eine bestimmte URL zuzugreifen.
2. Der virtuelle Lastausgleichsserver sendet eine 401-HTTP-Antwort an den Benutzer zurück und gibt an, dass für den Zugriff eine Authentifizierung erforderlich ist.
3. Der Benutzer sendet seine Anmeldeinformationen im Autorisierungsheader an den virtuellen Lastausgleichsserver.
4. Der virtuelle Lastausgleichsserver authentifiziert den Benutzer und verbindet den Benutzer dann mit den Back-End-Servern.



> **Wichtig:**
>
> Bei einem virtuellen Load-Balancing-Server mit aktivierter 401-Authentifizierung können in kurzer Zeit mehrere Authentifizierungs- und Autorisierungssitzungen für denselben Benutzer erstellt werden. Diese Konfiguration kann zu einer Speicherspitze führen. Sie können die folgende Konfiguration auf der NetScaler-Appliance anwenden, um die Endclient-Anwendung zu debuggen und zu identifizieren.

```
set syslogparams -userDefinedAuditlog yes

add audit messageaction 401_log_act INFORMATIONAL '"LB-401 accessed:
    User: <" + AAA.USER.NAME + "> SessionID <"+ AAA.USER.SESSIONID + ">
    Client :<" + CLIENT.IP.SRC + "> accessed URL: <" + HTTP.REQ.URL +
    ">"'

add rewritepolicy rewrite_401_log true NOREWRITE -logAction 401_log_act

bind lb vserver <lb_name> -policyName rewrite_401_log -priority 100 -
    type reqUEST
<!--NeedCopy-->
```


Re-Captcha-Konfiguration für die nFactor-Authentifizierung

May 11, 2023

NetScaler Gateway unterstützt eine neue erstklassige Aktion `captchaAction`, die die Re-Captcha-Konfiguration vereinfacht. Da Re-Captcha eine erstklassige Aktion ist, kann sie ein eigener Faktor sein. Sie können Re-Captcha überall im nFactor-Flow injizieren.

Zuvor mussten Sie benutzerdefinierte WebAuth Richtlinien mit Änderungen an der RFWebUI schreiben. Mit Einführen von `captchaAction` müssen Sie das JavaScript nicht mehr ändern.

> **Wichtig:**
>
> Wenn Re-Captcha zusammen mit den Feldern für den Benutzernamen oder das Kennwort im Schema verwendet wird, ist die Schaltfläche **Senden** deaktiviert, bis Re-Captcha erfüllt ist.

Re-Captcha-Konfiguration

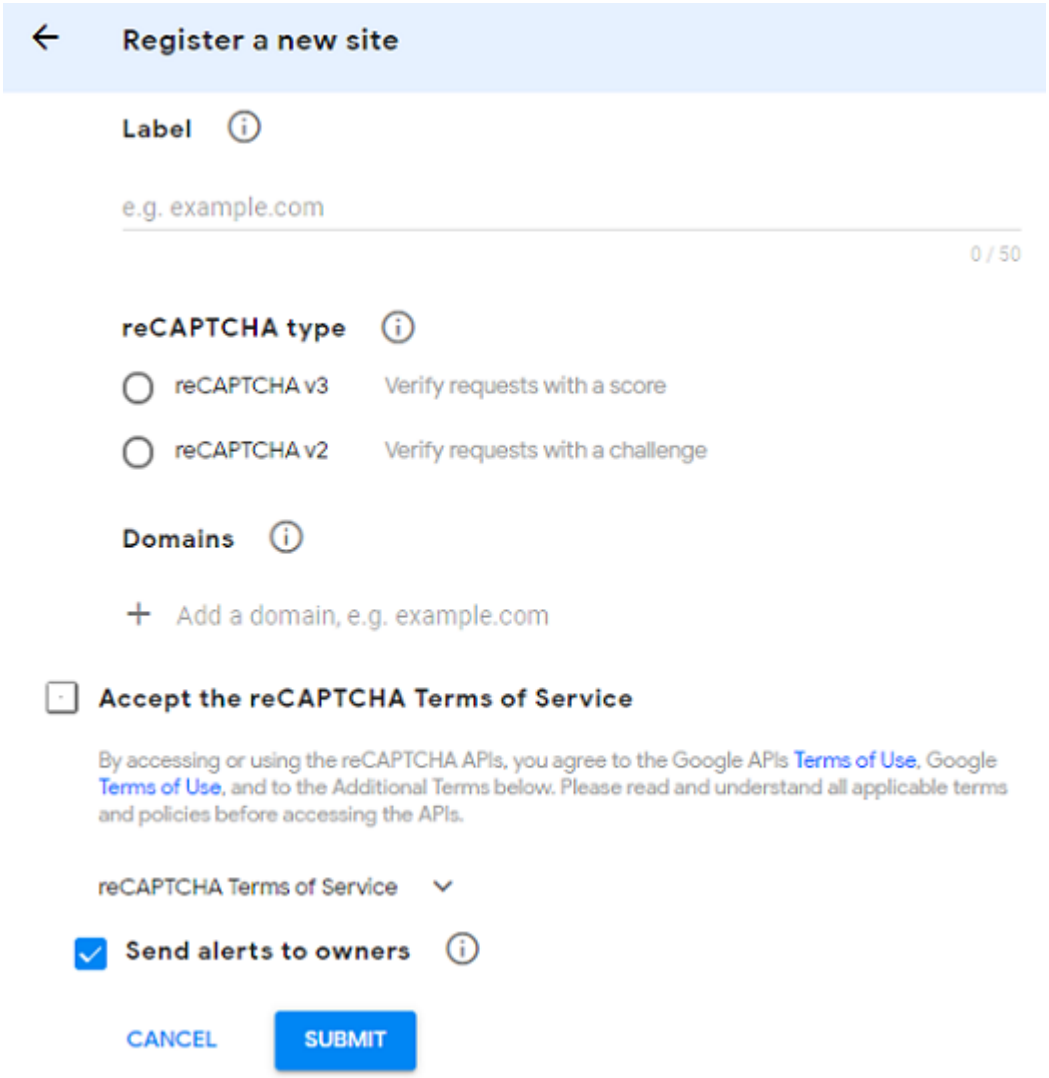
Die Re-Captcha-Konfiguration besteht aus zwei Teilen.

1. Konfiguration bei Google für die Registrierung von Re-Captcha.
2. Konfiguration auf der NetScaler Appliance zur Verwendung von Re-Captcha als Teil des Anmeldeflusses.

Re-Captcha-Konfiguration bei Google

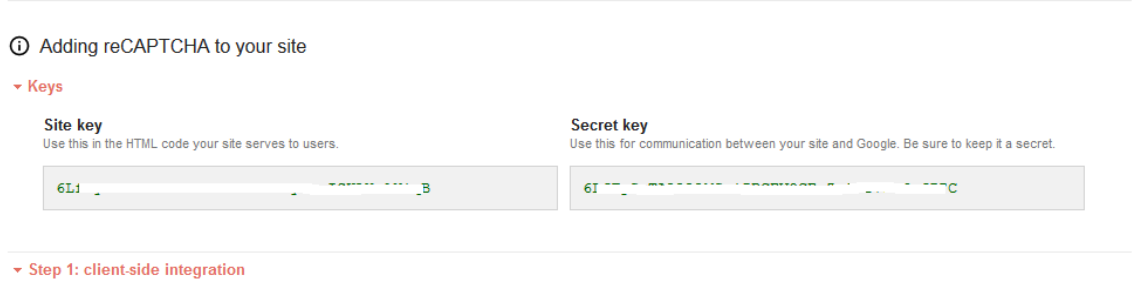
Registrieren Sie eine Domain für Re-Captcha unter https://www.google.com/recaptcha/admin#llist.

1. Wenn Sie zu dieser Seite navigieren, wird der folgende Bildschirm angezeigt.



> **Hinweis**
>
> Verwenden Sie nur reCAPTCHA v2. Unsichtbares Re-Captcha befindet sich noch in der Vorschau.

2. Nachdem eine Domain registriert wurde, werden “SiteKey” und “SecretKey” angezeigt.



> **Hinweis**
>
> Der “SiteKey” und “SecretKey” sind aus Sicherheitsgründen ausgegraut. “SecretKey” muss sicher aufbewahrt werden.

Re-Captcha-Konfiguration auf einer NetScaler Appliance

Die Re-Captcha-Konfiguration auf der NetScaler Appliance kann in drei Teile unterteilt werden:

- Bildschirm “Re-Captcha anzeigen”
- Veröffentlichen Sie die Re-Captcha-Antwort auf dem Google-Server
- Die LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Bildschirm “Re-Captcha anzeigen”

Die Anpassung des Anmeldeformulars erfolgt über das Anmeldeschema SingleAuthCaptcha.xml. Diese Anpassung wird auf dem virtuellen Authentifizierungsserver angegeben und zum Rendern des Anmeldeformulars an die Benutzeroberfläche gesendet. Das integrierte Anmeldeschema SingleAuthCaptcha.xml ist im Verzeichnis `/nsconfig/loginSchema/LoginSchema` auf der NetScaler-Appliance.

> **Wichtig**
>
> - Das Anmeldeschema SingleAuthCaptcha.xml kann verwendet werden, wenn LDAP als erster Faktor konfiguriert ist.
> - Basierend auf Ihrem Anwendungsfall und verschiedenen Schemas können Sie das vorhandene Schema ändern. Zum Beispiel, wenn Sie nur den Re-Captcha-Faktor (ohne Benutzername oder Kennwort) oder eine doppelte Authentifizierung mit Re-Captcha benötigen.
> - Wenn benutzerdefinierte Änderungen vorgenommen wurden oder die Datei umbenannt wird, empfiehlt Citrix, alle LoginSchemas aus dem Verzeichnis `/nsconfig/loginschema/LoginSchema` in das übergeordnete Verzeichnis `/nsconfig/loginschema` zu kopieren.

So konfigurieren Sie die Anzeige von Re-Captcha über die CLI

```
1 add authentication loginSchema singleauthcaptcha -authenticationSchema
    /nsconfig/loginschema/SingleAuthCaptcha.xml
2
3 add authentication loginSchemaPolicy singleauthcaptcha -rule true -
    action singleauthcaptcha
4
5 add authentication vserver auth SSL <IP> <Port>
6
```



```
add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>

bind ssl vserver auth -certkey vserver-cert

bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END
<!--NeedCopy-->
```

Veröffentlichen Sie die Re-Captcha-Antwort auf dem Google-Server

Nachdem Sie das Re-Captcha konfiguriert haben, das den Benutzern angezeigt werden muss, fügen die Administratoren die Konfiguration zum Google-Server hinzu, um die Re-Captcha-Antwort des Browsers zu überprüfen.

So überprüfen Sie die Re-Captcha-Antwort des Browsers

```
add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>

add authentication policy myrecaptcha -rule true -action myrecaptcha

bind authentication vserver auth -policy myrecaptcha -priority 1
<!--NeedCopy-->
```

Die folgenden Befehle sind erforderlich, um zu konfigurieren, ob AD-Authentifizierung gewünscht ist. Andernfalls können Sie diesen Schritt ignorieren.

```
add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup

add authenticationpolicy ldap-new -rule true -action ldap-new
<!--NeedCopy-->
```

Die LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Die LDAP-Authentifizierung erfolgt nach Re-Captcha, Sie fügen sie dem zweiten Faktor hinzu.


```
add authentication policylabel second-factor

bind authentication policylabel second-factor -policy ldap-new -
    priority 10

bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
<!--NeedCopy-->
```

Der Administrator muss entsprechende virtuelle Server hinzufügen, je nachdem, ob der virtuelle Lastausgleichsserver oder das NetScaler Gateway-Gerät für den Zugriff verwendet wird. Der Administrator muss den folgenden Befehl konfigurieren, wenn ein virtueller Lastausgleichsserver erforderlich ist:

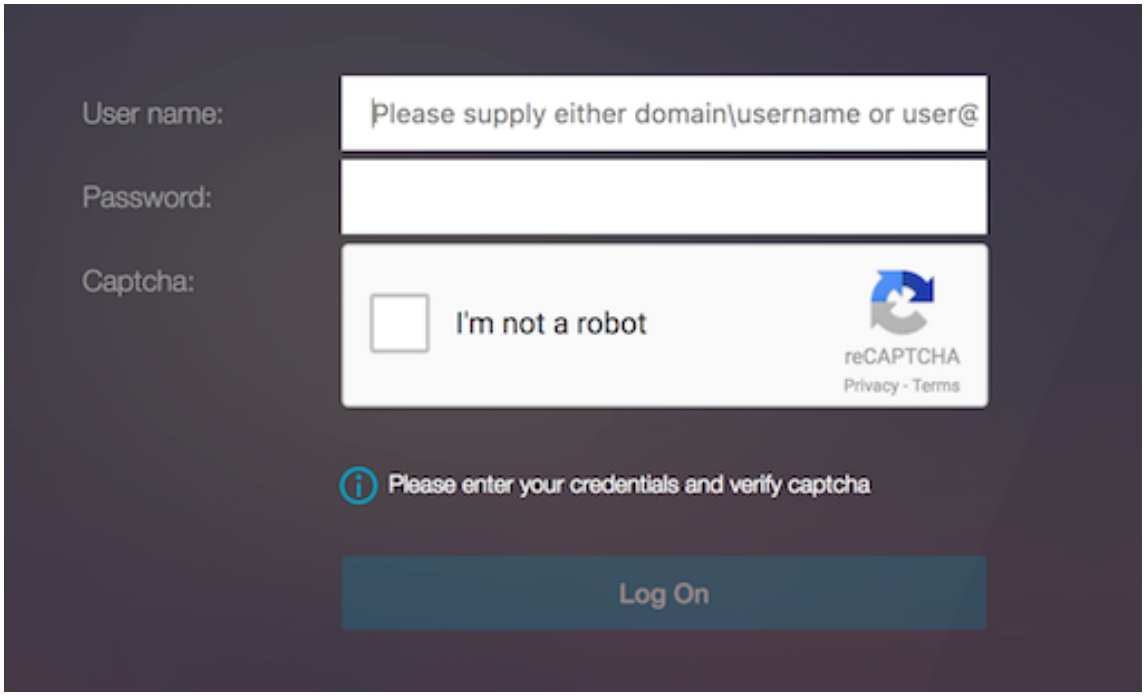
```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com
<!--NeedCopy-->
```

nssp.aaatm.com — Löst sich in einen virtuellen Authentifizierungsserver auf.

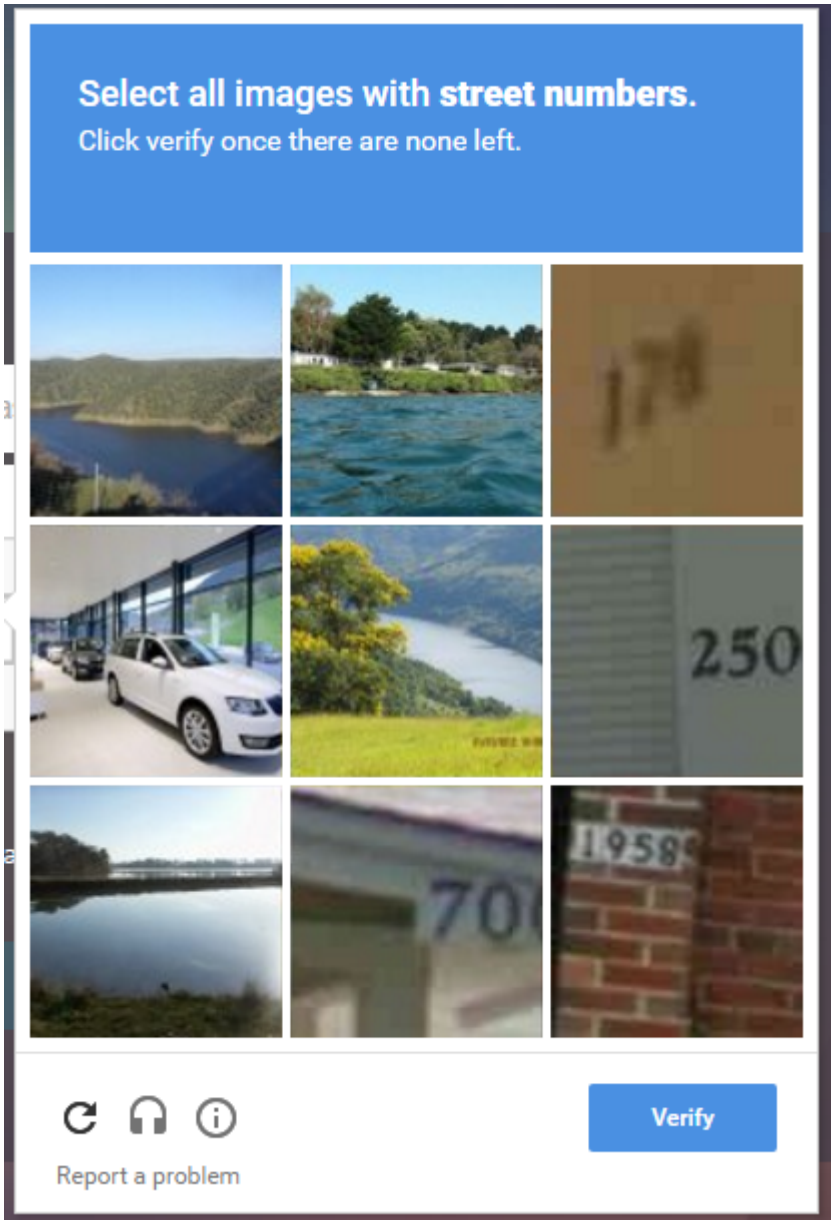
Benutzervalidierung von re-Captcha

Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, müssen Sie die folgende Benutzeroberfläche sehen.

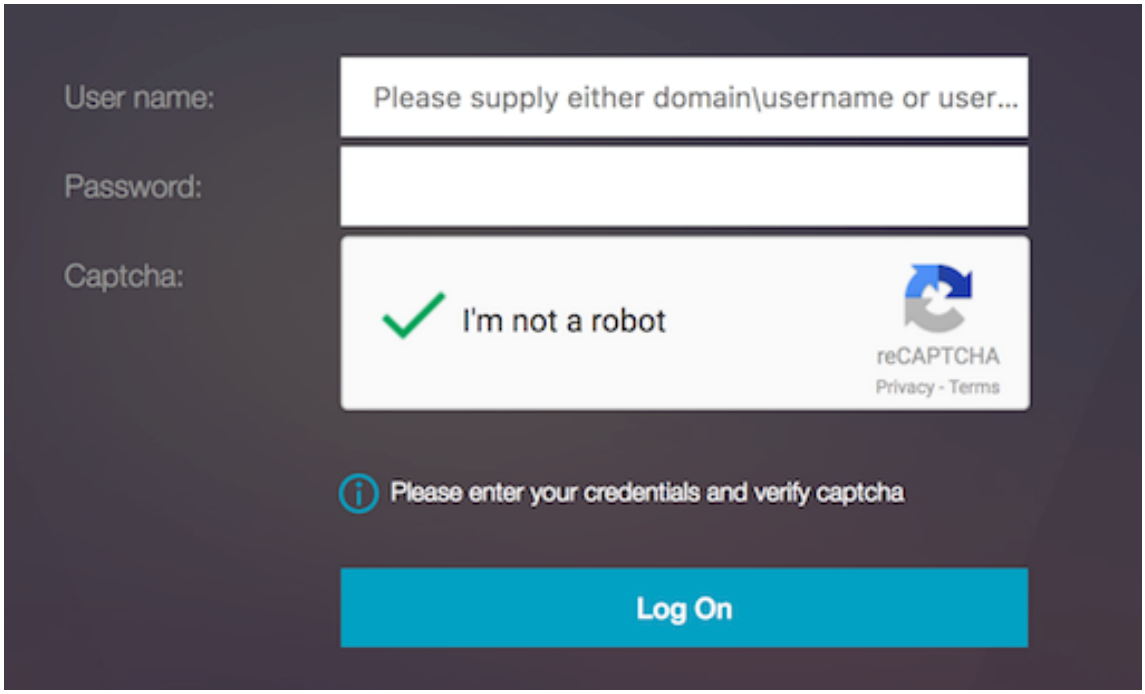
1. Sobald der virtuelle Authentifizierungsserver die Anmeldeseite geladen hat, wird der Anmeldebildschirm angezeigt. Die **Anmeldung** ist deaktiviert, bis Re-Captcha abgeschlossen ist.



2. Wähle Ich bin keine Roboter-Option. Das Re-Captcha-Widget wird angezeigt.



3. Sie werden durch eine Reihe von Re-Captcha-Bildern navigiert, bevor die Abschlussseite angezeigt wird.
4. Geben Sie die AD-Anmeldeinformationen ein, aktivieren Sie das Kontrollkästchen **Ich bin kein Roboter** und klicken Sie auf **Anmelden**. Wenn die Authentifizierung erfolgreich ist, werden Sie zur gewünschten Ressource weitergeleitet.



Hinweise:

- Wenn Re-Captcha mit der AD-Authentifizierung verwendet wird, ist die Schaltfläche **Senden** für Anmeldeinformationen deaktiviert, bis Re-Captcha abgeschlossen ist.
- Das Re-Captcha geschieht in einem eigenen Faktor. Daher müssen alle nachfolgenden Validierungen wie AD im `nextfactor` von Re-Captcha stattfinden.

Native OTP-Unterstützung für die Authentifizierung

September 18, 2023

NetScaler unterstützt Einmalkennwörter (OTPs), ohne dass ein Server eines Drittanbieters verwendet werden muss. Einmal-Kennwort ist eine hochsichere Option für die Authentifizierung bei sicheren Servern, da die generierte Nummer oder der Code zufällig ist. Zuvor boten spezialisierte Unternehmen wie RSA mit bestimmten Geräten, die Zufallszahlen generieren, die OTPs an.

Diese Funktion reduziert nicht nur die Kapital- und Betriebskosten, sondern verbessert auch die Kontrolle durch den Administrator, da die gesamte Konfiguration auf der NetScaler Appliance beibehalten wird.

Hinweis:

Da Server von Drittanbietern nicht mehr benötigt werden, muss der NetScaler-Administrator eine Schnittstelle zur Verwaltung und Validierung von Benutzergeräten konfigurieren.

Der Benutzer muss bei einem virtuellen NetScaler-Server registriert sein, um die OTP-Lösung verwenden zu können. Die Registrierung ist nur einmal pro Gerät erforderlich und kann auf bestimmte Umgebungen beschränkt werden. Die Konfiguration und Validierung eines registrierten Benutzers ähnelt der Konfiguration einer zusätzlichen Authentifizierungsrichtlinie.

Vorteile der nativen OTP-Unterstützung

- Senkt die Betriebskosten, da neben dem Active Directory keine zusätzliche Infrastruktur auf einem Authentifizierungsserver erforderlich ist.
- Konsolidiert die Konfiguration nur auf der NetScaler Appliance und bietet so Administratoren eine umfassende Kontrolle.
- Beseitigt die Abhängigkeit des Clients von einem zusätzlichen Authentifizierungsserver zur Generierung einer von den Clients erwarteten Zahl.

Nativer OTP-Workflow

Bei der nativen OTP-Lösung handelt es sich um einen zweifachen Prozess, und der Arbeitsablauf wird wie folgt klassifiziert:

- Geräteregistrierung
- Anmeldung für Endbenutzer

Wichtig:

> Sie können den Registrierungsprozess überspringen, wenn Sie Lösungen von Drittanbietern verwenden oder andere Geräte außer der NetScaler-Appliance verwalten. Die letzte Zeichenfolge, die Sie hinzufügen, muss das von NetScaler angegebene Format haben.

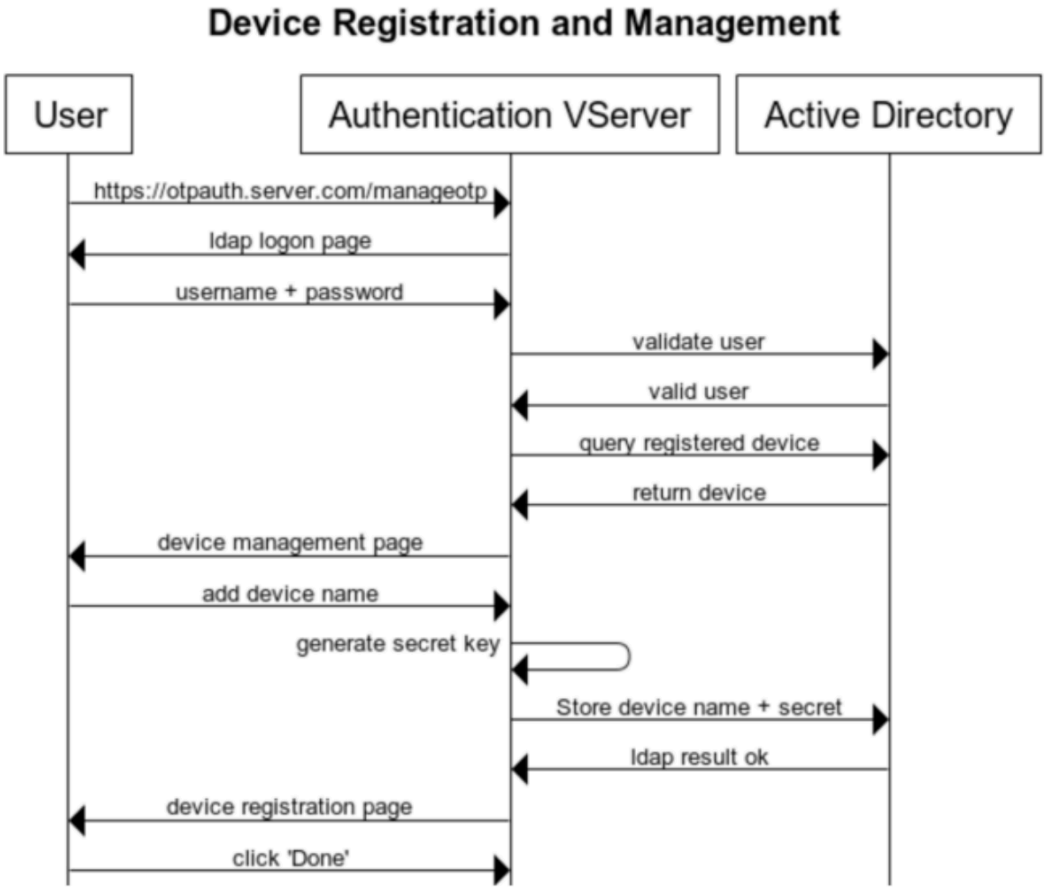
Die folgende Abbildung zeigt den Ablauf der Geräteregistrierung zur Registrierung eines neuen Geräts für den Empfang von OTP.

Hinweis:

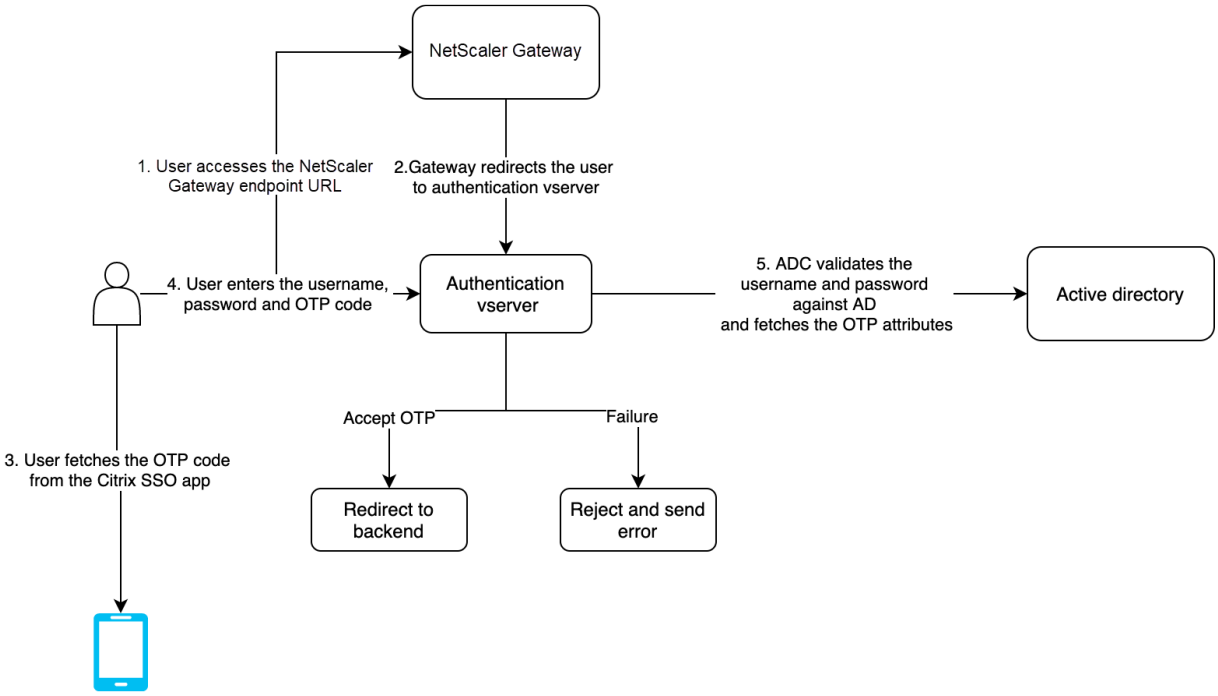
> Die Geräteregistrierung kann anhand einer Reihe von Faktoren erfolgen. Der Einzelfaktor (wie in der vorherigen Abbildung angegeben) wird als Beispiel verwendet, um den Prozess der Geräteregistrierung zu erläutern.

Die folgende Abbildung zeigt die Überprüfung von OTP durch das registrierte Gerät.

Die folgende Abbildung zeigt den Ablauf der Geräteregistrierung und -verwaltung.



Die folgende Abbildung zeigt den Endbenutzerablauf für die native OTP-Funktion.



Voraussetzungen

Um die native OTP-Funktion zu verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Die NetScaler Feature Release-Version ist 12.0 Build 51.24 und höher.
- Die Lizenz für die Advanced oder Premium Edition ist auf NetScaler Gateway installiert.
- NetScaler ist mit Management-IP konfiguriert, und auf die Managementkonsole kann sowohl über einen Browser als auch über die Befehlszeile zugegriffen werden.
- NetScaler ist mit einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver zur Authentifizierung von Benutzern konfiguriert. Weitere Informationen finden Sie unter Virtueller Authentifizierungsserver
- Die NetScaler Appliance ist mit Unified Gateway konfiguriert und das Authentifizierungs-, Autorisierungs- und Überwachungsprofil ist dem virtuellen Gateway-Server zugewiesen.
- Die native OTP-Lösung ist auf den nFactor-Authentifizierungsfluss beschränkt. Für die Konfiguration der Lösung sind erweiterte Richtlinien erforderlich. Weitere Informationen finden Sie unter Natives OTP

Stellen Sie außerdem Folgendes für Active Directory sicher:

- Eine minimale Attributlänge von 256 Zeichen.
- Der Attributtyp muss ‘DirectoryString’ sein, z. B. UserParameters. Diese Attribute können Zeichenkettenwerte enthalten.
- Der Typ der Attributzeichenfolge muss Unicode sein, wenn der Gerätename aus nicht-englischen Zeichen besteht.

- Der NetScaler LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.
- NetScaler Appliance und Client-Computer müssen mit einem gemeinsamen Network Time Server synchronisiert werden.

Konfigurieren Sie Native OTP mit der GUI

Die native OTP-Registrierung ist nicht nur eine Ein-Faktor-Authentifizierung. Die folgenden Abschnitte helfen Ihnen bei der Konfiguration der Einzel- und Zwei-Faktor-Authentifizierung.

Anmeldeschema für den ersten Faktor erstellen

1. Navigieren Sie zu **Sicherheit AAA > Anwendungsverkehr > Anmeldeschema**.
2. Gehen Sie zu **Profile** und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Authentifizierungs-Login-Schema erstellen** unter dem Feld **Name***lschema_single_auth_manage_otp* ein und klicken Sie neben **noschema** auf **Bearbeiten**.
4. Klicken Sie auf den Ordner **LoginSchema** .
5. Scrollen Sie nach unten, um **SingleAuthManageOTP.xml** auszuwählen, und klicken Sie auf **Auswählen**.
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Richtlinien** und dann auf **Hinzufügen**.
8. Geben **Sie im Fenster Create Authentication Login Schema Policy** die folgenden Werte ein.

   Vorname: lpol_single_auth_manage_otp_by_url

   Profil: Wählen Sie lschema_single_auth_manage_otp aus der Liste aus.

   Regel: `HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("manageotp")`

Konfiguration des virtuellen Servers für Authentifizierung, Autorisierung und Überwachung

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Authentifizierungsserver**. Klicken Sie hier, um den vorhandenen virtuellen Server zu bearbeiten. Weitere Informationen finden Sie unter Virtueller Authentifizierungsserver
2. Klicken Sie auf das **+**-Symbol neben **Anmeldeschemas** unter **Erweiterte Einstellungen** im rechten Fensterbereich.
3. Wählen Sie **Kein Anmeldeschema**aus.
4. Klicken Sie auf den Pfeil und wählen Sie die **lpol_single_auth_manage_otp_by_url** Policy aus, klicken Sie auf **Auswählen**und dann auf **Binden**.

5. Scrollen Sie nach oben und wählen Sie unter **Erweiterte Authentifizierungsrichtlinie** die Option **1 Authentifizierungsrichtlinie** aus.
6. Klicken Sie mit der rechten Maustaste auf die **nFactor-Richtlinie**, und wählen Sie **Bindung bearbeiten** aus. Klicken Sie mit der rechten Maustaste auf die bereits konfigurierte nFactor-Richtlinie oder beziehen Sie sich auf nFactor, um eine zu erstellen, und wählen Sie
7. Klicken Sie auf den Pfeil unter **Nächsten Faktor auswählen**, um eine vorhandene Konfiguration auszuwählen, oder klicken Sie auf **Hinzufügen**, um einen Faktor zu erstellen.
8. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinienlabel erstellen** Folgendes ein, und klicken Sie auf **Weiter** :

   Vorname: manage_otp_flow_label

   Anmeldeschema: Lschema_Int
9. Klicken Sie im Bildschirm **Authentication PolicyLabel** auf **Hinzufügen**, um eine Richtlinie zu erstellen.

   ```
   Create a policy for a normal LDAP server.
   ```
10. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinie erstellen** Folgendes ein:

    Vorname: auth_pol_ldap_native_otp
11. Wählen Sie den Aktionstyp als **LDAP** in der Liste **Aktionstyp** aus.
12. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Aktion zu erstellen.

    ```
    Create the first LDAP action with authentication enabled to be used for
     single factor.
    ```
13. Wählen Sie auf der Seite **LDAP-Server für Authentifizierung erstellen** das Optionsfeld **Server-IP** aus, deaktivieren Sie das Kontrollkästchen neben **Authentifizierung**, geben Sie die folgenden Werte ein und wählen Sie **Verbindung testen**aus. Im Folgenden finden Sie eine Beispielkonfiguration.

    Vorname: ldap_native_otp

    IP-Adresse: 192.8.xx.xx

    Base DN: DC = Training, DC = Labor

    Verwaltungsrätin: Administrator@training.lab

    Kennwort: `xxxxx`

    ```
    Create a policy for OTP .
    ```
14. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinie erstellen** Folgendes ein:

    Vorname: auth_pol_ldap_otp_action

15. Wählen Sie den Aktionstyp als **LDAP** in der Liste **Aktionstyp** aus.
16. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Aktion zu erstellen.

    `Create the second LDAP action to set OTP authenticator with OTP secret configuration and authentication unchecked.`
17. Wählen Sie auf der Seite **LDAP-Server für Authentifizierung erstellen** das Optionsfeld **Server-IP** aus, deaktivieren Sie das Kontrollkästchen neben **Authentifizierung**, geben Sie die folgenden Werte ein und wählen Sie **Verbindung testen**aus. Im Folgenden finden Sie eine Beispielkonfiguration.

    Vorname: ldap_otp_action

    IP-Adresse: 192.8.xx.xx

    Base DN: DC = Training, DC = Labor

    Verwaltungsrätin: Administrator@training.lab

    Kennwort: `xxxxx`
18. Scrollen Sie nach unten zum Abschnitt **Andere Einstellungen** . Verwenden Sie das Dropdownmenü, um die folgenden Optionen auszuwählen.
    Server-Anmeldename Attribut als **Neu** und geben Sie **userprincipalname ein**.
19. Verwenden Sie das Dropdownmenü, um **SSO-Namensattribut** als **Neu** auszuwählen und **userprincipalname**einzugeben.
20. Geben Sie “UserParameters” in das Feld **OTP Secret** ein und klicken Sie auf **Mehr**.
21. Geben Sie die folgenden Attribute ein.

    Attribute 1 = mail
    Attribute 2 = objectGUID
    Attribute 3 = immutableID
22. Klicken Sie auf **OK**.
23. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** den Ausdruck auf **true** fest und klicken Sie auf **Erstellen**.
24. Klicken Sie auf der Seite **Create Authentication Policylabel** auf **Binden**und dann auf **Fertig.**
25. Klicken Sie auf der Seite **Policy Binding** auf **Bind**.
26. Klicken Sie auf der Seite **Authentifizierungsrichtlinie** auf **Schließen**, und klicken Sie auf **Fertig**.

    `Create OTP for OTP verification.`
27. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinie erstellen** Folgendes ein:

    Name: auth_pol_ldap_otp_verifizieren

28. Wählen Sie den Aktionstyp als **LDAP** in der Liste **Aktionstyp** aus.
29. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Aktion zu erstellen.

    `Create the third LDAP action to verify OTP.`
30. Wählen Sie auf der Seite **LDAP-Server für Authentifizierung erstellen** das Optionsfeld **Server-IP** aus, deaktivieren Sie das Kontrollkästchen neben **Authentifizierung**, geben Sie die folgenden Werte ein und wählen Sie **Verbindung testen**aus. Im Folgenden finden Sie eine Beispielkonfiguration.

    Vorname: ldap_verify_otp

    IP-Adresse: 192.168.xx.xx

    Base DN: DC = Training, DC = Labor

    Verwaltungsrätin: Administrator@training.lab

    Kennwort: `xxxxx`
31. Scrollen Sie nach unten zum Abschnitt **Andere Einstellungen** . Verwenden Sie das Dropdownmenü, um die folgenden Optionen auszuwählen.
    Server-Anmeldename Attribut als **Neu** und geben Sie **userprincipalname ein**.
32. Verwenden Sie das Dropdownmenü, um **SSO-Namensattribut** als **Neu** auszuwählen und **userprincipalname**einzugeben.
33. Geben Sie “UserParameters” in das Feld **OTP Secret** ein und klicken Sie auf **Mehr**.
34. Geben Sie die folgenden Attribute ein.

    Attribute 1 = mail
    Attribute 2 = objectGUID
    Attribute 3 = immutableID
35. Klicken Sie auf **OK**.
36. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** den Ausdruck auf **true** fest und klicken Sie auf **Erstellen**.
37. Klicken Sie auf der Seite **Create Authentication Policylabel** auf **Binden**und dann auf **Fertig.**
38. Klicken Sie auf der Seite **Policy Binding** auf **Bind**.
39. Klicken Sie auf der Seite **Authentifizierungsrichtlinie** auf **Schließen**, und klicken Sie auf **Fertig**.

Sie haben wahrscheinlich noch keine Advanced Authentication Policy für Ihren normalen LDAP-Server.
Ändern Sie den Aktionstyp in LDAP.
Wählen Sie Ihren normalen LDAP-Server aus, bei dem die Authentifizierung aktiviert ist.

Geben Sie als Ausdruck true ein. Dabei wird die erweiterte Richtlinie anstelle der klassischen Syntax verwendet.
Klicken Sie auf **Erstellen**.

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver muss an das RFWebUI-Portaldesign gebunden sein. Binden Sie ein Serverzertifikat an den Server. Die Server-IP '1.2.3.5' muss einen entsprechenden FQDN haben, nämlich otpauth.server.com, für die spätere Verwendung.

Anmeldeschema für OTP mit dem zweiten Faktor erstellen

1. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Virtuelle Server**. Wählen Sie den virtuellen Server aus, der bearbeitet werden soll.
2. Scrollen Sie nach unten und wählen Sie **1 Login**
3. Klicken Sie auf **Bindung hinzufügen**.
4. Klicken Sie im Abschnitt **Richtlinienbindung** auf **Hinzufügen**, um eine Richtlinie hinzuzufügen.
5. Geben Sie auf der Seite **Authentifizierungs-Anmeldeschema-Richtlinie erstellen** den Namen der Richtlinie ein und klicken Sie auf **Hinzufügen**.
6. Geben Sie auf der Seite **Authentifizierungs-Anmeldeschema erstellen** den Namen des Anmeldeschemas ein und klicken Sie auf das Stiftsymbol neben **noschema**.
7. Klicken Sie auf den Ordner **LoginSchema**, wählen Sie **DualAuthManageOTP.xml** aus, und klicken Sie dann auf **Auswählen**.
8. Klicke auf **Mehr** und scrolle nach unten.
9. Geben Sie im Feld **Index für Kennwortanmeldeinformationen** 1 ein. Dadurch speichert nFactor das Benutzerkennwort im Authentifizierungs-, Autorisierungs- und Audit-Attribut #1, das später in einer Traffic-Richtlinie für Single Sign-On bei StoreFront verwendet werden kann. Wenn Sie dies nicht tun, versucht NetScaler Gateway, den Passcode zur Authentifizierung bei StoreFront zu verwenden, was nicht funktioniert.
10. Klicken Sie auf **Erstellen**.
11. Geben Sie im Abschnitt **Regel** die Option **True** ein. Klicken Sie auf **Erstellen**.
12. Klicken Sie auf **Bind**.
13. Beachten Sie die beiden Authentifizierungsfaktoren. Klicken Sie auf **Schließen**, und klicken Sie auf **Fertig**.

Verkehrspolitik für Single Sign-On

1. Navigieren Sie zu **NetScaler Gateway > Richtlinien > Datenverkehr**
2. Klicken Sie auf der Registerkarte **Verkehrsprofile** auf **Hinzufügen**.
3. Geben Sie einen Namen für das Verkehrsprofil ein.

4. Scrollen Sie im Feld SSO Password Expression nach unten und klicken Sie auf **Erstellen**. Hier verwenden wir das Passwortattribut für das Anmeldeschema, das für den zweiten Faktor OTP angegeben ist.

   ```
   AAA.USER.ATTRIBUTE(1)
   ```

5. Klicken Sie auf der Registerkarte **Traffic-Richtlinien** auf **Hinzufügen**.
6. Geben Sie im Feld **Name** einen Namen für die Verkehrsrichtlinie ein.
7. Wählen Sie im Feld **Anforderungsprofil** das von Ihnen erstellte Verkehrsprofil aus.
8. Geben Sie im Feld Ausdruck **True**ein. Wenn Ihr virtueller NetScaler Gateway-Server vollständiges VPN zulässt, ändern Sie den Ausdruck wie folgt.

   ```
   http.req.method.eq(post)||http.req.method.eq(get)&& false
   ```

9. Klicken Sie auf **Erstellen**.
10. Binden Sie die Verkehrsrichtlinie an einen virtuellen VPN-Server.
    - Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Authentifizierungsprofil**.
    - **Konfigurieren Sie das Authentifizierungsprofil, indem Sie den virtuellen NetScaler Gateway-Server auswählen und dann auf OK klicken.**
    - Navigieren Sie zu **Citrix Gateway > Citrix Gateway Virtual Servers** und wählen Sie den virtuellen Citrix Gateway-Server aus. Die Seite **VPN Virtual Server** wird angezeigt.
    - Klicken Sie im Abschnitt **Richtlinien** auf das Pluszeichen.
    - Wählen Sie als Richtlinientyp **Traffic** aus und klicken Sie auf **Weiter**.
    - Wählen Sie die Verkehrsrichtlinie aus und klicken Sie auf **Binden**.
    - Klicken Sie auf **Fertig**.

Content Switching-Richtlinie für die Verwaltung von OTP konfigurieren

Die folgenden Konfigurationen sind erforderlich, wenn Sie Unified Gateway verwenden.

1. Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**. Wählen Sie die Richtlinie für den Content Switching aus, klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten**.
2. Bearbeiten Sie den Ausdruck, um die folgende OR-Anweisung auszuwerten, und klicken Sie auf **OK**:

   ```
   is_vpn_url || HTTP.REQ.URL.CONTAINS("manageotp"
   ```

Konfigurieren Sie Native OTP mit der CLI

Sie benötigen die folgenden Informationen, um die OTP-Geräteverwaltungsseite zu konfigurieren:

- Dem virtuellen Authentifizierungsserver zugewiesene IP
- FQDN, der der zugewiesenen IP entspricht
- Serverzertifikat für den virtuellen Authentifizierungsserver

> **Hinweis:**
>
> Native OTP ist nur eine webbasierte Lösung.

So konfigurieren Sie die OTP-Geräteregistrierungs- und Verwaltungsseite

Virtuellen Authentifizierungsserver erstellen

```
1 ```
2 add authentication vserver authvs SSL 1.2.3.5 443
3 bind authentication vserver authvs -portaltheme RFWebUI
4 bind ssl vserver authvs -certkeyname otpauthcert
5 <!--NeedCopy--> ```
```

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver muss an das RFWebUI-Portalthema gebunden sein. Binden Sie ein Serverzertifikat an den Server. Die Server-IP '1.2.3.5' muss einen entsprechenden FQDN haben, nämlich otpauth.server.com, für die spätere Verwendung.

So erstellen Sie eine LDAP-Anmeldeaktion

```
1 add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
      -  serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
      ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

Beispiel:

```
1 add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
      serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
      administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
      ldapLoginName userprincipalname
```

So fügen Sie eine Authentifizierungsrichtlinie für die LDAP-Anmeldung hinzu

```
1 add authentication Policy auth_pol_ldap_logon -rule true -action
      ldap_logon_action
```


Um die Benutzeroberfläche über LoginSchema zu präsentieren

Benutzernamenfeld und Kennwortfeld für Benutzer bei der Anmeldung anzeigen

```
add authentication loginSchema lschema_single_auth_manage_otp -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/
    SingleAuthManageOTP.xml"
```

Geräteregistrierungs- und Verwaltungsseite anzeigen

Citrix empfiehlt zwei Möglichkeiten, den Bildschirm für die Geräteregistrierung und -verwaltung anzuzeigen: URL oder Hostname.

> **Hinweis:**
>
> Derzeit können Geräteregistrierung und Geräteverwaltung nur mit einem Browser durchgeführt werden.

- **Verwenden von URL**

  Wenn die URL '/manageotp' enthält

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **Verwenden des Hostnamens**

  Wenn der Hostname 'alt.server.com' ist

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

So konfigurieren Sie die Benutzeranmeldeseite mit der CLI

Sie benötigen die folgenden Informationen, um die Benutzeranmeldeseite zu konfigurieren:

- IP für einen virtuellen Lastausgleichsserver
- Entsprechender FQDN für den virtuellen Lastausgleichsserver
- Serverzertifikat für den virtuellen Lastausgleichsserver


```
bind ssl virtual server lbvs_https -certkeyname lbvs_server_cert
<!--NeedCopy-->
```

Der Back-End-Dienst im Load Balancing wird wie folgt dargestellt:

```
```
add service iis_backendsso_server_com 1.2.3.210 HTTP 80
bind lb vserver lbvs_https iis_backendsso_server_com
<!--NeedCopy--> ```
```

**So erstellen Sie eine Aktion zur OTP-Passcode-Validierung**

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
    authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>`
```

Beispiel:

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
    userParameters
```

> **Wichtig:**
>
> Der Unterschied zwischen der LDAP-Anmeldung und der OTP-Aktion besteht darin, dass die Authentifizierung deaktiviert und ein neuer Parameter `OTPSecret` eingeführt werden muss. Verwenden Sie nicht den AD-Attributwert.

So fügen Sie eine Authentifizierungsrichtlinie für die OTP-Passcode-Validierung hinzu

```
add authentication Policy auth_pol_otp_validation -rule true -action
    ldap_otp_action
```

Um die Zwei-Faktor-Authentifizierung über LoginSchema zu präsentieren

Fügen Sie die Benutzeroberfläche für die Zwei-Faktor-Authentifizierung hinzu.

```
add authentication loginSchema lscheme_dual_factor -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
    "
```


```

```
2 add authentication loginSchemaPolicy lpol_dual_factor -rule true -
    action lscheme_dual_factor
```

Um einen Passcode-Validierungsfaktor über das Policy-Label zu erstellen

Erstellen Sie ein Richtlinienlabel zum Verwalten von OTP-Flows für den nächsten Faktor (der erste Faktor ist die LDAP-Anmeldung)

```
1 add authentication loginSchema lschema_noschema -authenticationSchema
    noschema
2 add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema
```

Um die OTP-Richtlinie an das Richtlinienlabel zu binden

```
1 bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

Um den UI-Flow zu binden

Binden Sie die LDAP-Anmeldung gefolgt von der OTP-Validierung an den virtuellen Authentifizierungsserver.

```
1 bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT
2 bind authentication vserver authvs -policy lpol_dual_factor -priority
    30 -gotoPriorityExpression END
```

Um eine Verkehrsrichtlinie für Single Sign-On zu erstellen und sie an einen virtuellen VPN-Server zu binden

```
1 add vpn trafficAction vpn_html_pol http -userExpression aaa.user.
    attribute(1) -passwdExpression aaa.user.attribute(2)
2
3 add vpn trafficpolicy tf1 'http.req.method.eq(post)||http.req.method.eq
    (get) && false' vpn_html_pol
4
5 bind vpn vserver vpn1 -policy tf1 -priority 10
6 <!--NeedCopy-->
```


Registrieren Sie Ihr Gerät bei NetScaler

1. Navigieren Sie in Ihrem Browser zu Ihrem NetScaler-FQDN (erste öffentlich zugängliche IP) mit dem Suffix /manageotp. Zum Beispiel Login bei https://otpauth.server.com/manageotp mit Benutzeranmeldeinformationen.
2. Klicken Sie auf das **+-Symbol**, um ein Gerät hinzuzufügen.
3. Geben Sie einen Gerätenamen ein und drücken Sie **Los**. Auf dem Bildschirm erscheint ein Barcode.
4. Klicken Sie auf **Setup beginnen** und dann auf **Barcode scannen**.
5. Bewegen Sie die Gerätekamera über den QR-Code. Sie können den Code optional eingeben.

   > **Hinweis**:
   >
   > Der angezeigte QR-Code ist 3 Minuten gültig.

6. Nach erfolgreichem Scan wird Ihnen ein sechsstelliger zeitkritischer Code angezeigt, mit dem Sie sich anmelden können.
7. Klicken Sie zum Testen auf dem QR-Bildschirm auf **Fertig** und dann auf das grüne Häkchen rechts.
8. Wählen Sie Ihr Gerät aus dem Dropdownmenü aus, geben Sie den Code von Google Authenticator ein (muss blau und nicht rot sein) und klicken Sie auf **Los**.
9. Stellen Sie sicher, dass Sie sich über das Drop-down-Menü in der oberen rechten Ecke der Seite abmelden.

Melden Sie sich mit dem OTP bei NetScaler an

1. Navigieren Sie zu Ihrer ersten öffentlich zugänglichen URL und geben Sie Ihr OTP von Google Authenticator ein, um sich anzumelden.
2. Authentifizieren Sie sich auf der NetScaler Splash-Seite.

Speichern geheimer OTP-Daten in einem verschlüsselten Format

May 11, 2023

Ab NetScaler Version 13.0 Build 41.20 können die geheimen OTP-Daten in einem verschlüsselten Format anstelle von Klartext gespeichert werden.

Zuvor hat die NetScaler Appliance den OTP-Schlüssel als Klartext in AD gespeichert. Das Speichern von OTP-Geheimnissen im Klartext stellt ein Sicherheitsrisiko dar, da ein böswilliger Angreifer oder ein

Administrator die Daten ausnutzen könnte, indem er das gemeinsame Geheimnis anderer Benutzer einsieht.

Der Verschlüsselungsparameter ermöglicht die Verschlüsselung des OTP-Geheimnisses in AD. Wenn Sie ein neues Gerät mit NetScaler Version 13.0 Build 41.20 registrieren und den Verschlüsselungsparameter aktivieren, wird das OTP-Geheimnis standardmäßig in einem verschlüsselten Format gespeichert. Wenn der Verschlüsselungsparameter jedoch deaktiviert ist, wird das OTP-Geheimnis im Klartextformat gespeichert.

Für Geräte, die vor 13.0 Build 41.20 registriert wurden, müssen Sie als bewährte Methode die folgenden Schritte ausführen:

1. Aktualisieren Sie die 13.0 NetScaler Appliance auf 13.0 Build 41.20.
2. Aktivieren Sie den Verschlüsselungsparameter auf der Appliance.
3. Verwenden Sie das geheime OTP-Migrationstool, um geheime OTP-Daten vom Klartextformat in das verschlüsselte Format zu migrieren.

Einzelheiten zum geheimen OTP-Migrationstool finden Sie unter OTP-Verschlüsselungstool.

> **Wichtig** Citrix empfiehlt Ihnen als Administrator, um sicherzustellen, dass die folgenden Kriterien erfüllt sind:
>
> - Ein neues Zertifikat muss so konfiguriert werden, dass OTP-Geheimnisse verschlüsselt werden, wenn Sie KBA nicht als Teil der Self-Service-Kennwortrücksetzfunktion verwenden.
>   - To bind the certificate to VPN global, you can use the following command:
>
>     ```
>     bind vpn global -userDataEncryptionKey <certificate name>
>     ```
>
> - Wenn Sie bereits ein Zertifikat zum Verschlüsseln von KBA verwenden, können Sie dasselbe Zertifikat zum Verschlüsseln von OTP-Geheimnissen verwenden.
> - Neue OTP-Registrierungen erfolgen immer mit dem letzten gebundenen Zertifikat, da dieses die höchste Priorität hat. Wenn Sie im unten gezeigten Beispiel ein Zertifikat (cert1) binden und dann ein anderes Zertifikat (cert2) binden, wird cert2 für die Geräteregistrierung berücksichtigt. Wenn das für die Geräteregistrierung erforderliche Zertifikat fehlt, schlägt die Anmeldung des Endbenutzers fehl.
>
>   ```
>   1    bind vpn global -userDataEncryptionKey otp-cert1
>   2    bind vpn global -userDataEncryptionKey otp-cert2
>   3    <!--NeedCopy-->
>   ```
>
>   Im folgenden Beispiel wird das Zertifikat `cert2` als erster Eintrag in der Ausgabe des Befehls `show vpn global` angezeigt:
>
>   ‘‘‘
>
>   show vpn global

> Portalthema: RFWebUI
> Benutzerdatenverschlüsselungszertifikat: cert2
> Benutzerdatenverschlüsselungszertifikat: cert1
> 1) Name der VPN-Richtlinie für den clientlosen Zugriff: ns_cvpn_owa_policy Priorität: 95000
> Bindpunkt: REQ_DEFAULT
> 2) Name der VPN-Richtlinie für den clientlosen Zugriff: ns_cvpn_sp_policy Priorität: 96000
> Bindpunkt: REQ_DEFAULT
> 3) Name der VPN-Richtlinie für den clientlosen Zugriff: ns_cvpn_sp_2013_Richtlinienpriorität: 97000
> Bindpoint: REQ_DEFAULT
> 4) Name der VPN-Richtlinie für den clientlosen Zugriff: ns_cvpn_default_policy Priorität: 100000
> Bindpoint: REQ_DEFAULT
> ‘‘‘

So aktivieren Sie OTP-Verschlüsselungsdaten mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Beispiel

```
set aaa otpparameter -encryption ON
```

So konfigurieren Sie die OTP-Verschlüsselung mithilfe der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr** und klicken Sie im Abschnitt ****Authentifizierungseinstellungen auf Authentifizierung** ändern AAA OTP-Parameter** .
2. Wählen Sie auf der Seite „ **AAA-OTP-Parameter konfigurieren** “ die Option **Geheime OTP-Verschlüsselung**aus.
3. Klicken Sie auf OK.

Konfiguration der Anzahl der Endbenutzergeräte für den Empfang von OTP-Benachrichtigungen

Administratoren können jetzt die Anzahl der Geräte konfigurieren, die ein Endbenutzer registrieren kann, um eine OTP-Benachrichtigung oder Authentifizierung zu erhalten.

So konfigurieren Sie die Anzahl der Geräte in OTP mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

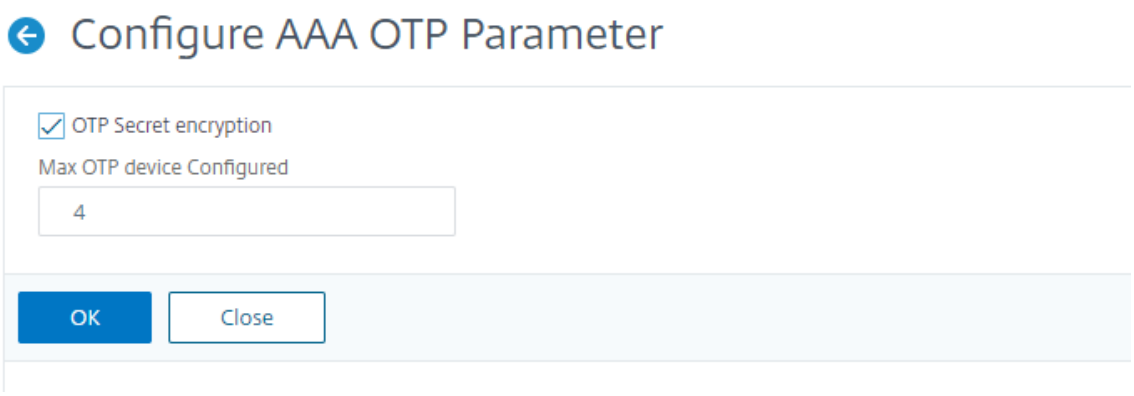
```
set aaa otpparameter [-maxOTPDevices <positive_integer>]
```

Beispiel

```
set aaa otpparameter -maxOTPDevices 4
```

So konfigurieren Sie die Anzahl der Geräte mithilfe der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr**und klicken Sie im Abschnitt ****Authentifizierungseinstellungen auf AAA-OTP-Parameter für die Authentifizierung** ändern** .
2. Geben Sie auf der Seite „ **AAA-OTP-Parameter konfigurieren** “ den Wert für das **konfigurierte Max OTP-Gerät**ein.
3. Klicken Sie auf **OK**.



OTP-Verschlüsselungstool

May 11, 2023

Ab NetScaler Release 13.0 Build 41.20 werden die geheimen OTP-Daten für erhöhte Sicherheit in einem verschlüsselten Format anstelle von Klartext gespeichert. Das Speichern eines OTP-Geheimnisses in verschlüsseltem Format erfolgt automatisch und erfordert keinen manuellen Eingriff.

Zuvor speicherte die NetScaler-Appliance ein OTP-Geheimnis als Nur-Text im Active Directory. Das Speichern eines OTP-Geheimnisses in einem Nur-Text-Format stellte eine Sicherheitsbedrohung dar,

da ein böswilliger Angreifer oder ein Administrator die Daten ausnutzen kann, indem er das gemeinsame Geheimnis anderer Benutzer anzeigt.

Das OTP-Verschlüsselungstool bietet folgende Vorteile:

- Führt nicht zu Datenverlust, selbst wenn Sie alte Geräte haben, die ein altes Format (Nur-Text) verwenden.
- Die Abwärtskompatibilitätsunterstützung mit einer alten NetScaler Gateway-Version hilft bei der Integration und Unterstützung der vorhandenen Geräte zusammen mit dem neuen Gerät.
- Mit dem OTP-Verschlüsselungstool können Administratoren alle geheimen OTP-Daten aller Benutzer gleichzeitig migrieren.

> **Hinweis:**
>
> Das OTP-Verschlüsselungstool verschlüsselt oder entschlüsselt keine KBA-Registrierungs- oder E-Mail-Registrierungsdaten.

Verwendung des OTP-Verschlüsselungswerkzeugs

Das OTP-Verschlüsselungstool kann für Folgendes verwendet werden:

- **Verschlüsselung**. Speichern Sie das OTP-Geheimnis in verschlüsseltem Format. Das Tool extrahiert die OTP-Daten der bei NetScaler registrierten Geräte und konvertiert dann die OTP-Daten im Nur-Text-Format in ein verschlüsseltes Format.
- **Entschlüsselung**. Setzen Sie das OTP-Geheimnis auf das Nur-Text-Format zurück.
- **Zertifikate aktualisieren**. Administratoren können das Zertifikat jederzeit auf ein neues Zertifikat aktualisieren. Administratoren können das Tool verwenden, um das neue Zertifikat einzugeben und alle Einträge mit den neuen Zertifikatsdaten zu aktualisieren. Der Zertifikatpfad muss entweder ein absoluter Pfad oder ein relativer Pfad sein.

> **Wichtig**
>
> - Sie müssen den Verschlüsselungsparameter in der NetScaler-Appliance aktivieren, um das OTP-Verschlüsselungstool verwenden zu können.
> - Für Geräte, die vor Build 41.20 bei NetScaler registriert wurden, müssen Sie Folgendes ausführen:
>   - Upgrade the 13.0 NetScaler appliance to 13.0 build 41.20.
>   - Enable the encryption parameter on the appliance.
>   - Use the OTP Secret migration tool to migrate OTP secret data from plain text format to encrypted format.
> - Das OTP-Verschlüsselungstool unterstützt nur einwertige Benutzerattribute. Benutzerattribute mit mehreren Werten werden nicht unterstützt.

OTP-Geheimdaten im Nur-Text-Format

Beispiel:

```
##@devicename=<16 or more bytes>&tag=<64bytes>&,
```

Wie Sie sehen können, ist das Startmuster für ein altes Format immer “#@” und ein Endmuster ist immer “&”. Alle Daten zwischen “Gerätename =” und Endmuster stellen OTP-Daten des Benutzers dar.

Geheime OTP-Daten im verschlüsselten Format

Das neue verschlüsselte Format von OTP-Daten hat das folgende Format:

Beispiel:

```
    {

         "otpdata" : {

          “devices” : {

                          “device1” :  “value1” ,
                          “device2” :  “value2” , …
                      }

             }

     }

<!--NeedCopy-->
```

Wobei value1 ein Base64-kodierter Wert von KID + IV +-Chiffredaten ist

Verschlüsselungsdaten sind wie folgt strukturiert:

```
    {

      secret:<16-byte secret>,
      tag : <64-byte tag value>
      alg: <algorithm used> (not mandatory, default is sha1, specify
         the algorithm only if it is not default)
     }

<!--NeedCopy-->
```

- In “devices” haben Sie einen Wert für jeden Namen. Der Wert ist base64encode(KID).base64encode(IV).base6

- KID ist der Schlüssel-ID-Wert, der verwendet wird, um das Zertifikat zu identifizieren, das für die geheime OTP-Datenverschlüsselung verwendet wird. Die Schlüssel-ID ist insbesondere nützlich, wenn mehrere Zertifikate für die geheime OTP-Datenverschlüsselung verwendet werden.
- In Standard-AES-Algorithmen wird IV immer als die ersten 16 oder 32 Byte Verschlüsselungsdaten gesendet. Sie können demselben Modell folgen.
- IV unterscheidet sich für jedes Gerät, obwohl der Schlüssel derselbe bleibt.

> **Hinweis:**
>
> Das verschlüsselte Format der OTP-Daten wird in einem Benutzerattribut AD gespeichert.

Einrichtung des OTP-Verschlüsselungstools

> **Hinweis**
>
> Um das OTP-Verschlüsselungstool auszuführen, empfiehlt Citrix, anstelle der NetScaler Appliance eine alternative Plattform mit Python-Umgebung zu verwenden.

Das OTP-Verschlüsselungstool befindet sich im Verzeichnis `\var\netscaler\otptool`. Sie müssen den Code von der NetScaler-Quelle herunterladen und das Tool mit den erforderlichen AD-Anmeldeinformationen ausführen.

- Voraussetzungen für die Verwendung des OTP-Verschlüsselungstools:
  - Installieren Sie Python 3.5 oder höher in der Umgebung, in der dieses Tool ausgeführt wird.
  - Installieren Sie pip3 oder neuere Versionen.
- Führen Sie die folgenden Befehle aus:
  - **pip install requirements.txt**. Installiert automatisch die Anforderungen
  - **python main.py**. Ruft das OTP-Verschlüsselungstool auf. Sie müssen die erforderlichen Argumente angeben, die Ihren Anforderungen für die Migration von geheimen OTP-Daten entsprechen.
- Das Tool kann von einer Shell-Eingabeaufforderung aus in `\var\netscaler\otptool` gefunden werden.
- Führen Sie das Tool mit den erforderlichen AD-Anmeldeinformationen aus.

OTP-Verschlüsselungstool-Schnittstelle

Die folgende Abbildung zeigt ein Beispiel für eine OTP-Verschlüsselungs-Tool-Schnittstelle. Die Schnittstelle enthält alle Argumente, die für die Verschlüsselung/Entschlüsselung/Zertifikatsaktualisierung definiert werden müssen. Außerdem wird eine kurze Beschreibung jedes Arguments erfasst.

Argument OPERATION

Sie müssen das Argument OPERATION definieren, um das OTP-Verschlüsselungstool für Verschlüsselung, Entschlüsselung oder Zertifikatsaktualisierung zu verwenden.

In der folgenden Tabelle sind einige Szenarien zusammengefasst, in denen Sie das OTP-Verschlüsselungstool und die entsprechenden Argumentwerte OPERATION verwenden können.

Szenario	Operations-Argumentwert und andere Argumente
Konvertieren Sie OTP-Schlüssel im Klartext in ein verschlüsseltes Format mit demselben Attribut	Geben Sie den Argumentwert OPERATION als 0 ein und geben Sie denselben Wert für das Quell- und Zielattribut an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute unixhomedirectory -operation 0 -cert_path aaatm_wild_all.cert`
Konvertieren Sie OTP-Schlüssel im Klartext-Format in ein verschlüsseltes Format mit einem anderen Attribut	Geben Sie den Argumentwert OPERATION als 0 ein und geben Sie die entsprechenden Werte für das Quell- und Zielattribut an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 0 -cert_path aaatm_wild_all.cert`

Szenario	Operations-Argumentwert und andere Argumente
Konvertiere die verschlüsselten Einträge zurück in Klartext	Geben Sie den Argumentwert OPERATION als 1 ein und geben Sie die entsprechenden Werte für das Quell- und Zielattribut an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 1 -cert_path aaatm_wild_all.cert`
Aktualisieren Sie das Zertifikat auf ein neues Zertifikat	Geben Sie den Argumentwert OPERATION als 2 ein und geben Sie das gesamte vorherige Zertifikat und die Details des neuen Zertifikats in den entsprechenden Argumenten an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -operation 2 -cert_path aaatm_wild_all.cert -new_cert_path aaatm_wild_all_new.cert`

CERT_PATH Argument

Das Argument CERT_PATH ist eine Datei, die das Zertifikat enthält, das im NetScaler zum Verschlüsseln der Daten verwendet wird. Der Benutzer muss dieses Argument für alle drei Vorgänge angeben, nämlich **Verschlüsselung**, **Entschlüsselung**und **Update-Zertifikate**.

Die CERT_PATH-Argumentdatei muss sowohl das Zertifikat als auch den zugehörigen privaten Schlüssel im PEM- oder CERT-Format enthalten (PFX wird nicht unterstützt).

Wenn beispielsweise die Zertifikate.cert- und certificate.key- Dateien der Zertifikatsdatei und ihrem privaten Schlüssel entsprechen, erstellt der folgende Befehl in einem Unix-ähnlichen System die Datei `certkey.merged`, die als Wert für das Flag cert_path verwendet werden kann.


```
$ cat certificate.cert certificate.key > certkey.merged
$
<!--NeedCopy-->
```

> **Zu beachtende Punkte zum Zertifikat**
>
> - Der Benutzer muss dasselbe Zertifikat bereitstellen, das global in der NetScaler Appliance für die Verschlüsselung von Benutzerdaten gebunden ist.
> - Das Zertifikat muss das Base64-codierte öffentliche Zertifikat und den entsprechenden privaten RSA-Schlüssel in derselben Datei enthalten.
> - Das Format des Zertifikats muss entweder PEM oder CERT sein. Das Zertifikat muss dem X509-Format entsprechen.
> - Das kennwortgeschützte Zertifikatsformat und die *PFX-Datei* werden von diesem Tool nicht akzeptiert. Der Benutzer muss die PFX-Zertifikate in *.cert* konvertieren, bevor er die Zertifikate an das Tool bereitstellt.

SEARCH_FILTER Argument

Das Argument SEARCH_FILTER wird verwendet, um die Active Directory-Domänen oder -Benutzer zu filtern.

Beispiele:

- `-search_filter "(sAMAccountName=OTP*)"`: Filtert Benutzer, deren samAccountNames (Benutzeranmeldenamen) mit „OTP“ beginnen.
- `-search_filter "(objectCategory=person)"`: Filtert die Objektkategorie des Typs Person.
- `-search_file "(objectclass=*)"`: Filtert alle Objekte.

Aktivieren der Verschlüsselungsoption in der NetScaler-Appliance

Um das Nur-Text-Format zu verschlüsseln, müssen Sie die Verschlüsselungsoption in der NetScaler-Appliance aktivieren.

Um OTP-Verschlüsselungsdaten mithilfe der CLI zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Beispiel:

```
set aaa otpparameter -encryption ON
```


Anwendungsfälle des OTP-Verschlüsselungstools

Das OTP-Verschlüsselungstool kann für die folgenden Anwendungsfälle verwendet werden.

Registrieren neuer Geräte bei der NetScaler-Appliance Version 13.0 Build 41.20

Wenn Sie Ihr neues Gerät bei der NetScaler-Appliance Version 13.0 Build 41.x registrieren und wenn die Verschlüsselungsoption aktiviert ist, werden die OTP-Daten in einem verschlüsselten Format gespeichert. Sie können einen manuellen Eingriff vermeiden.

Wenn die Verschlüsselungsoption nicht aktiviert ist, werden die OTP-Daten im Nur-Text-Format gespeichert.

Migrieren Sie OTP-Daten für die Geräte, die vor 13.0 Build 41.20 registriert wurden

Sie müssen Folgendes ausführen, um die geheimen OTP-Daten für die Geräte zu verschlüsseln, die vor dem 13.0 Build 41.20 bei der NetScaler Appliance registriert sind.

- Migrieren Sie mit dem Konvertierungstool OTP-Daten vom Nur-Text-Format in das verschlüsselte Format.
- Aktivieren Sie den Parameter “Encryption” auf der NetScaler Appliance.
  - So aktivieren Sie die Verschlüsselungsoption mithilfe der CLI:
    - `set aaa otpparameter -encryption ON`
  - So aktivieren Sie Verschlüsselungsoptionen mit der GUI:
    - Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr** und klicken Sie im Abschnitt ****Authentifizierungseinstellungen auf Authentifizierung** ändern AAA OTP-Parameter** .
    - Wählen Sie auf der Seite **AAA-OTP-Parameter konfigurieren** die Option **Geheime OTP-Verschlüsselung**aus, und klicken Sie auf **OK**.
  - Melden Sie sich mit den gültigen AD-Anmeldeinformationen an.
  - Wenn es erforderlich ist, registrieren Sie weitere Geräte (optional).

Migrieren Sie verschlüsselte Daten vom alten Zertifikat zum neuen Zertifikat

Wenn Administratoren das Zertifikat auf ein neues Zertifikat aktualisieren möchten, bietet das Tool die Möglichkeit, die neuen Zertifikatsdateneinträge zu aktualisieren.

So aktualisieren Sie das Zertifikat mithilfe der CLI auf ein neues Zertifikat

Geben Sie in der Befehlszeile Folgendes ein:

Beispiel:


```
python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local
-search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -
target_attribute userparameters -operation 2 -cert_path aaatm_wild_all.cert
 -new_cert_path aaatm_wild_all_new.cert
```

> **Hinweis**
>
> - Die Zertifikate müssen sowohl private als auch öffentliche Schlüssel haben.
> - Derzeit wird die Funktion nur für OTP bereitgestellt.

Erneutes Verschlüsseln oder Migrieren auf neues Zertifikat für Geräte, die nach dem Upgrade der Appliance auf 13.0 Build 41.20 mit Verschlüsselung registriert wurden

Der Administrator kann das Tool auf Geräten verwenden, die bereits mit einem Zertifikat verschlüsselt sind, und dieses Zertifikat mit einem neuen Zertifikat aktualisieren.

Verschlüsselte Daten zurück in das Nur-Text-Format umwandeln

Der Administrator kann das OTP-Geheimnis entschlüsseln und auf das ursprüngliche Nur-Text-Format zurücksetzen. Das OTP-Verschlüsselungstool durchsucht alle Benutzer nach einem OTP-Geheimnis im verschlüsselten Format und wandelt sie in ein entschlüsseltes Format um.

So aktualisieren Sie das Zertifikat mithilfe der CLI auf ein neues Zertifikat

Geben Sie in der Befehlszeile Folgendes ein:

Beispiel:

```
1 python3 main.py -Host 192.0.2.1 - Port 636 -username  ldapbind_user@aaa
     .local -search_base cn=users,dc=aaa,dc=local -source_attribute
     unixhomedirectory -target_attribute userparameters -operation 1
2 <!--NeedCopy-->
```

Problembehandlung

Das Tool generiert die folgenden Protokolldateien.

- **app.log**. Protokolliert alle wichtigen Ausführungsschritte und Informationen zu Fehlern, Warnungen und Ausfällen.
- **unmodified_users.txt**. Enthält eine Liste von Benutzer-DNs, die nicht vom reinen Text auf das verschlüsselte Format aktualisiert wurden. Diese Protokolle werden zu einem Fehler im Format generiert oder aus einem anderen Grund.

Pushbenachrichtigung für OTP

May 11, 2023

NetScaler Gateway unterstützt Pushbenachrichtigungen für OTP. Benutzer müssen das auf ihren registrierten Geräten empfangene OTP nicht manuell eingeben, um sich bei NetScaler Gateway anzumelden. Administratoren können NetScaler Gateway so konfigurieren, dass Anmeldebenachrichtigungen mithilfe von Pushbenachrichtigungsdiensten an die registrierten Geräte der Benutzer gesendet werden. Wenn Benutzer die Benachrichtigung erhalten, müssen sie einfach in der Benachrichtigung auf Zulassen tippen, um sich bei NetScaler Gateway anzumelden. Wenn das Gateway eine Bestätigung vom Benutzer erhält, identifiziert es die Quelle der Anfrage und sendet eine Antwort an diese Browserverbindung.

Wenn die Benachrichtigungsantwort nicht innerhalb des Timeout-Zeitraums (30 Sekunden) empfangen wird, werden Benutzer zur NetScaler Gateway-Anmeldeseite weitergeleitet. Die Benutzer können das OTP dann manuell eingeben oder auf Benachrichtigung **erneut senden klicken, um die Benachrichtigung** erneut auf dem registrierten Gerät zu erhalten.

Administratoren können mithilfe der für Pushbenachrichtigungen erstellten Anmeldeschemas die Pushbenachrichtigung als Standardauthentifizierung vornehmen.

> **Wichtig:**
>
> Die Pushbenachrichtigungsfunktion ist mit einer NetScaler Premium Edition-Lizenz verfügbar.

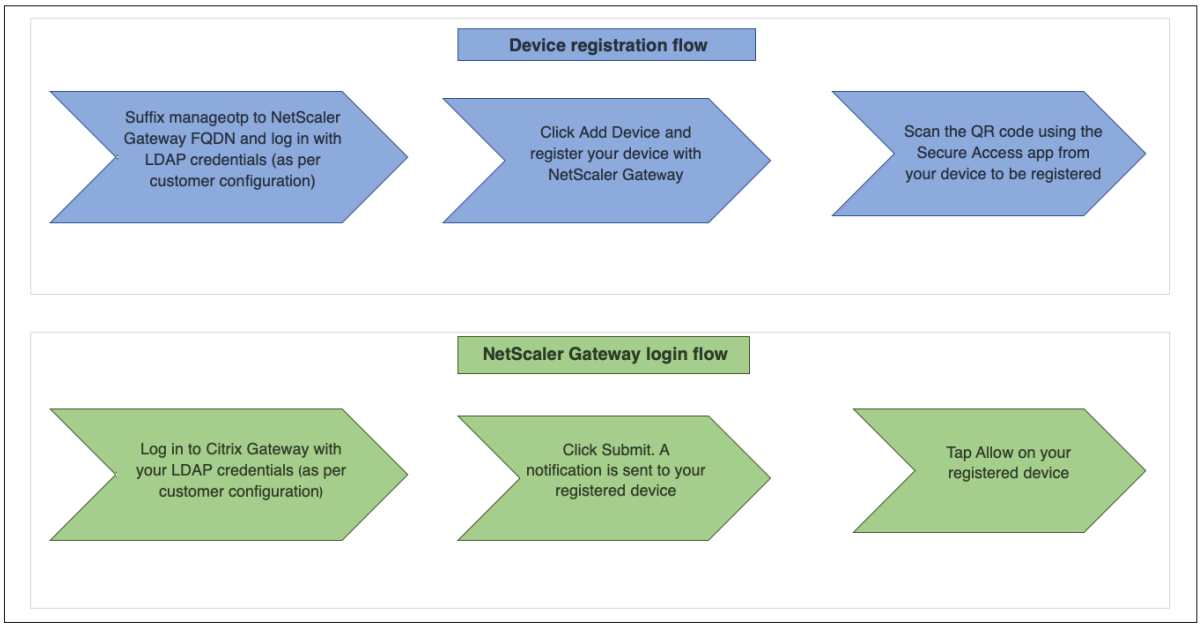
Vorteile von Pushbenachrichtigungen

- Pushbenachrichtigungen bieten einen sichereren Multifaktor-Authentifizierungsmechanismus. Die Authentifizierung bei NetScaler Gateway ist erst erfolgreich, wenn der Benutzer den Anmeldeversuch genehmigt.
- Pushbenachrichtigungen sind einfach zu verwalten und zu verwenden. Benutzer müssen die Citrix SSO Mobile App herunterladen und installieren, für die keine Administratorunterstützung erforderlich ist.
- Benutzer müssen den Code nicht kopieren oder sich merken. Sie müssen einfach auf das Gerät tippen, um sich authentifizieren zu lassen.
- Benutzer können mehrere Geräte registrieren.

Funktionsweise von Pushbenachrichtigungen

Der Workflow für Pushbenachrichtigungen kann in zwei Kategorien eingeteilt werden:

- Geräteregistrierung
- Login für Endbenutzer



Voraussetzungen für die Verwendung von Pushbenachrichtigungen

- Schließen Sie den Citrix Cloud-Onboarding-Prozess ab.
  1. Erstellen Sie ein Citrix Cloud-Unternehmenskonto oder treten Sie einem vorhandenen bei. Detaillierte Verfahren und Anweisungen zum weiteren Vorgehen finden Sie unter Anmelden für Citrix Cloud.
  2. Melden Sie sich bei an https://citrix.cloud.comund wählen Sie den Kunden aus.
  3. Wählen Sie im Menü **Identity and Access Management** aus und navigieren Sie dann zur Registerkarte **API-Zugriff**, um einen Client für das Konto zu erstellen.
  4. Kopieren Sie die ID, das Geheimnis und die Kunden-ID. Die ID und das Geheimnis sind erforderlich, um den Push-Dienst in NetScaler als “ClientID” bzw. “ClientSecret” zu konfigurieren.

> **Wichtig:**
>
> - Dieselben API-Anmeldeinformationen können in mehreren Rechenzentren verwendet werden.
> - Lokale NetScaler-Appliances müssen in der Lage sein, die Serveradressen mfa.cloud.com und trust.citrixworkspacesapi.net aufzulösen und sie müssen von der Appliance aus zugänglich sein. Dies soll sicherstellen, dass es keine Firewalls oder IP-Adressblöcke für diese Server über Port 443 gibt.

- Laden Sie die mobile Citrix SSO-App aus dem App Store und Play Store für iOS-Geräte bzw. Android-Geräte herunter. Pushbenachrichtigungen werden auf iOS ab Build 1.1.13 auf Android ab 2.3.5 unterstützt.

- Stellen Sie Folgendes für das Active Directory sicher.
  - Die minimale Attributlänge muss mindestens 256 Zeichen betragen.
  - Der Attributtyp muss ‘DirectoryString’ wie UserParameters sein. Diese Attribute können Zeichenfolgenwerte enthalten.
  - Der Typ der Attributzeichenfolge muss Unicode sein, wenn der Gerätename nicht-englische Zeichen enthält.
  - Der NetScaler LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.
  - NetScaler und der Clientcomputer müssen mit einem gemeinsamen Netzwerkzeitserver synchronisiert werden.

Konfiguration von Pushbenachrichtigungen

Im Folgenden sind die übergeordneten Schritte aufgeführt, die ausgeführt werden müssen, um die Pushbenachrichtigungsfunktion verwenden zu können.

- Der NetScaler Gateway-Administrator muss die Schnittstelle für die Verwaltung und Validierung von Benutzern konfigurieren.
  1. Konfigurieren Sie einen Push-Dienst.
  2. Konfigurieren Sie NetScaler Gateway für die OTP-Verwaltung und die Endbenutzer-Anmeldung.

     Benutzer müssen ihre Geräte beim Gateway registrieren, um sich bei NetScaler Gateway anzumelden.
  3. Registrieren Sie Ihr Gerät bei NetScaler Gateway.
  4. Melden Sie sich bei NetScaler Gateway an.

Erstellen Sie einen Push-Dienst

1. Navigieren Sie zu **Sicherheit** > **AAA-Anwendungsverkehr** > **Richtlinien** > **Authentifizierung** > **Erweiterte Richtlinien** > **Aktionen** > **Push-Dienst** und klicken Sie auf **Hinzufügen**.
2. Geben Sie **unter Name**den Namen des Push-Dienstes ein.
3. Geben Sie unter **Client-ID**die eindeutige Identität der vertrauenswürdigen Partei für die Kommunikation mit dem NetScaler Push-Server in der Cloud ein.
4. Geben Sie unter **Client Secret**das einzigartige Geheimnis der vertrauenswürdigen Partei für die Kommunikation mit dem NetScaler Push-Server in der Cloud ein.
5. Geben Sie unter **Kunden-ID**die Kunden-ID oder den Namen des Kontos in der Cloud ein, mit dem die Client-ID und das Client-Secret-Paar erstellt werden.

> **Wichtig**
>
> Die TLS 1.2-Version wird für den Push-Service benötigt. Weitere Informationen finden Sie unter TLS 1.2-Konfigurationsdetails.

Konfigurieren von NetScaler Gateway für OTP-Verwaltung und Endbenutzeranmeldung

Führen Sie die folgenden Schritte für die OTP-Verwaltung und die Endbenutzer-Anmeldung aus.

- Erstellen eines Anmeldeschemas für die OTP-Verwaltung
- Konfigurieren des virtuellen Servers für Authentifizierung, Autorisierung und Überwachung
- Konfigurieren von VPN- oder Lastausgleichs-Servern
- Konfigurieren des Policy Label
- Anmeldeschema für Endbenutzer-Anmeldung erstellen

Weitere Informationen zur Konfiguration finden Sie unter Native OTP-Unterstützung.

Wichtig: Für Pushbenachrichtigungen müssen Administratoren Folgendes explizit konfigurieren:

- Erstellen Sie einen Push-Dienst.
- Wählen Sie beim Erstellen eines Anmeldeschemas für die OTP-Verwaltung je nach Bedarf das Anmeldeschema SingleAuthManageOTP.xml oder ein gleichwertiges Schema aus.
- Wählen Sie beim Erstellen eines Anmeldeschemas für die Endbenutzeranmeldung je nach Bedarf das Anmeldeschema DualAuthOrPush.xml oder ein gleichwertiges Schema aus.

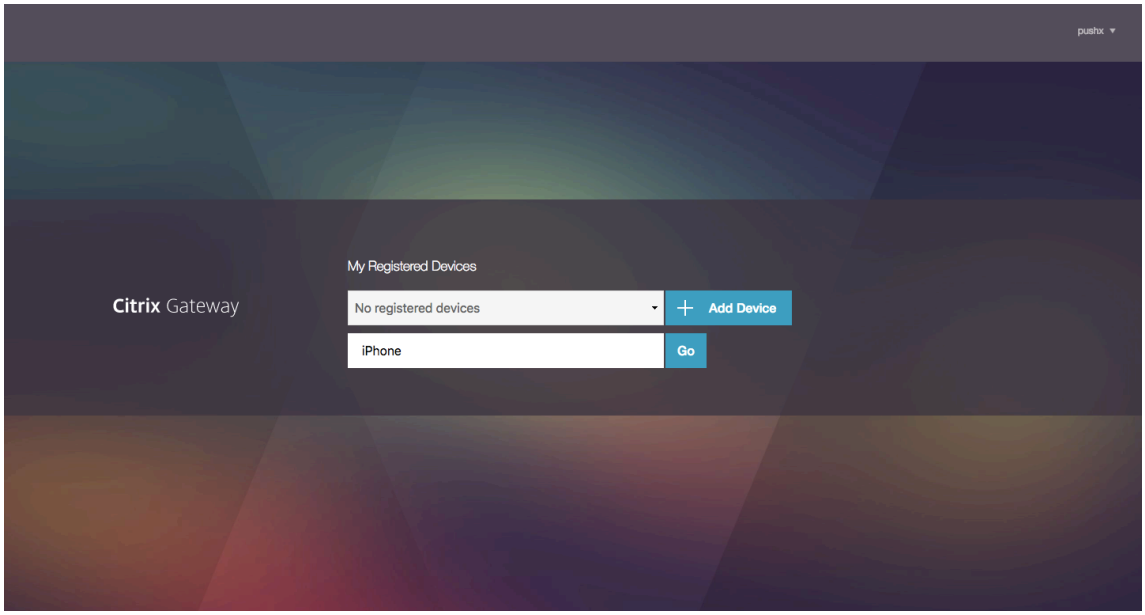
Registrieren Sie Ihr Gerät bei NetScaler Gateway

Benutzer müssen ihre Geräte bei NetScaler Gateway registrieren, um die Pushbenachrichtigungsfunktion nutzen zu können.

1. Navigieren Sie in Ihrem Webbrowser zu Ihrem NetScaler Gateway FQDN und setzen Sie **/manageotp** an den FQDN an.

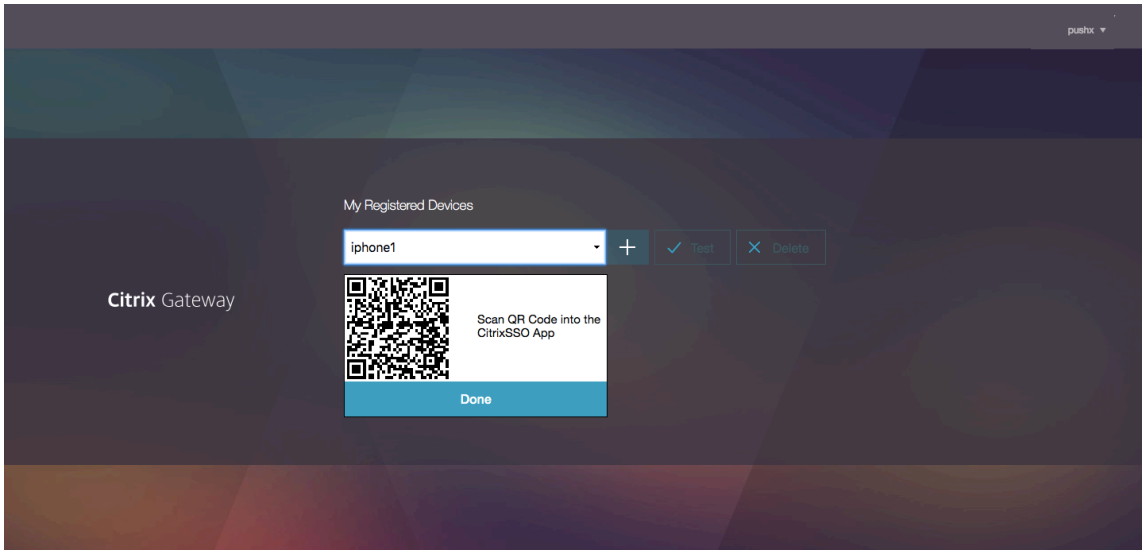
   Dadurch wird die Authentifizierungsseite geladen.
   Beispiel: https://gateway.company.com/manageotp

2. Melden Sie sich je nach Bedarf mit Ihren LDAP-Anmeldeinformationen oder geeigneten Zwei-Faktor-Authentifizierungsmechanismen an.



3. Klicken Sie auf **Gerät hinzufügen**.
4. Geben Sie einen Namen für Ihr Gerät ein und klicken Sie auf **Start**.

   Ein QR-Code wird auf der NetScaler Gateway-Browserseite angezeigt.

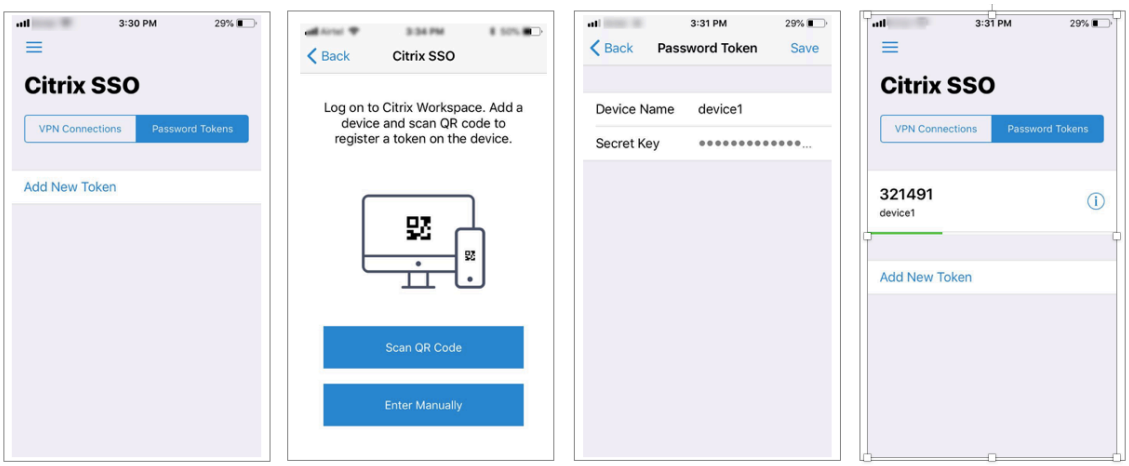


5. Scannen Sie diesen QR-Code mit der Citrix SSO-App von dem zu registrierenden Gerät.

   Citrix SSO validiert den QR-Code und registriert sich dann beim Gateway für Pushbenachrichtigungen. Wenn der Registrierungsprozess keine Fehler aufweist, wird das Token erfolgreich zur Kennwort-Token-Seite hinzugefügt.

   > **Wichtig:**
   >
   > Die Anmeldung schlägt fehl, wenn Sie den im QR-Code enthaltenen geheimen Schlüssel

manuell eingeben.



6. Wenn es keine zusätzlichen Geräte zum Hinzufügen/Verwalten gibt, melden Sie sich mit der Liste oben rechts auf der Seite ab.

Testen der Einmalkennwort-Authentifizierung

1. Um das OTP zu testen, klicken Sie in der Liste auf Ihr Gerät und dann auf **Testen**.
2. Geben Sie das OTP ein, das Sie auf Ihrem Gerät erhalten haben, und klicken Sie auf **Los**.

   Die Meldung “OTP-Überprüfung erfolgreich” wird angezeigt.
3. Melden Sie sich mit der Liste oben rechts auf der Seite ab.

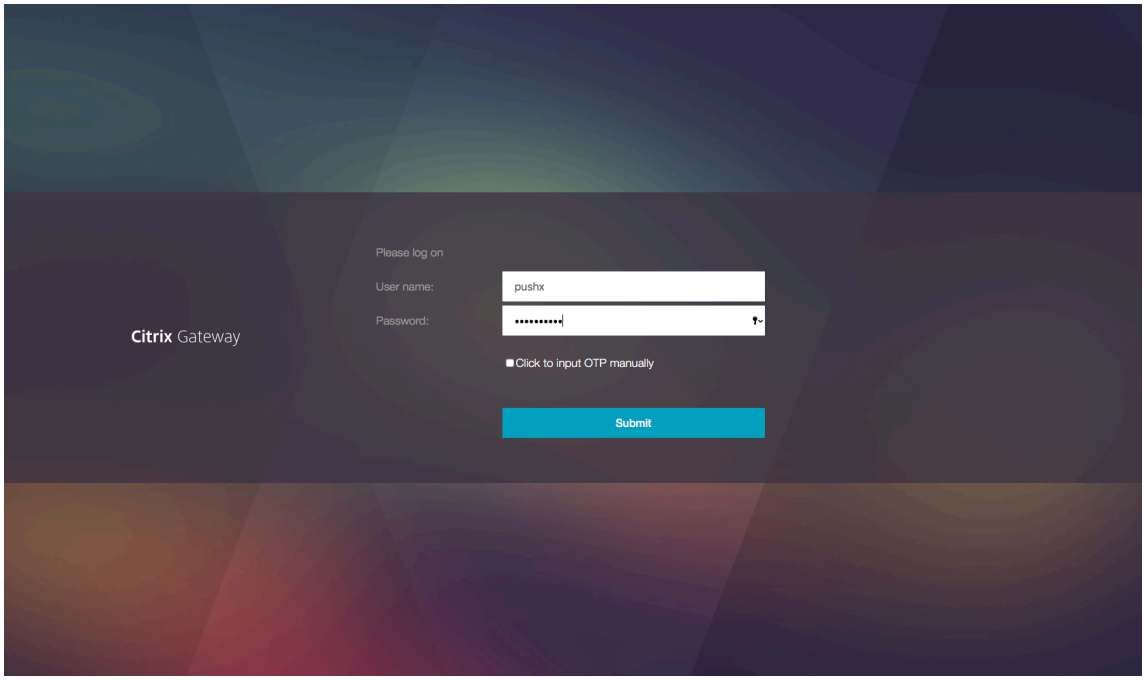
Hinweis: Sie können das OTP-Verwaltungsportal jederzeit verwenden, um die Authentifizierung zu testen, registrierte Geräte zu entfernen oder weitere Geräte zu registrieren.

Melden Sie sich bei NetScaler Gateway an

Nach der Registrierung ihrer Geräte bei NetScaler Gateway können Benutzer die Pushbenachrichtigungsfunktion für die Authentifizierung verwenden.

1. Navigieren Sie zu Ihrer NetScaler Gateway-Authentifizierungsseite (z. B.: https://gateway.company.com)

   Abhängig von der Konfiguration des Anmeldeschemas werden Sie aufgefordert, nur Ihre LDAP-Anmeldeinformationen einzugeben.

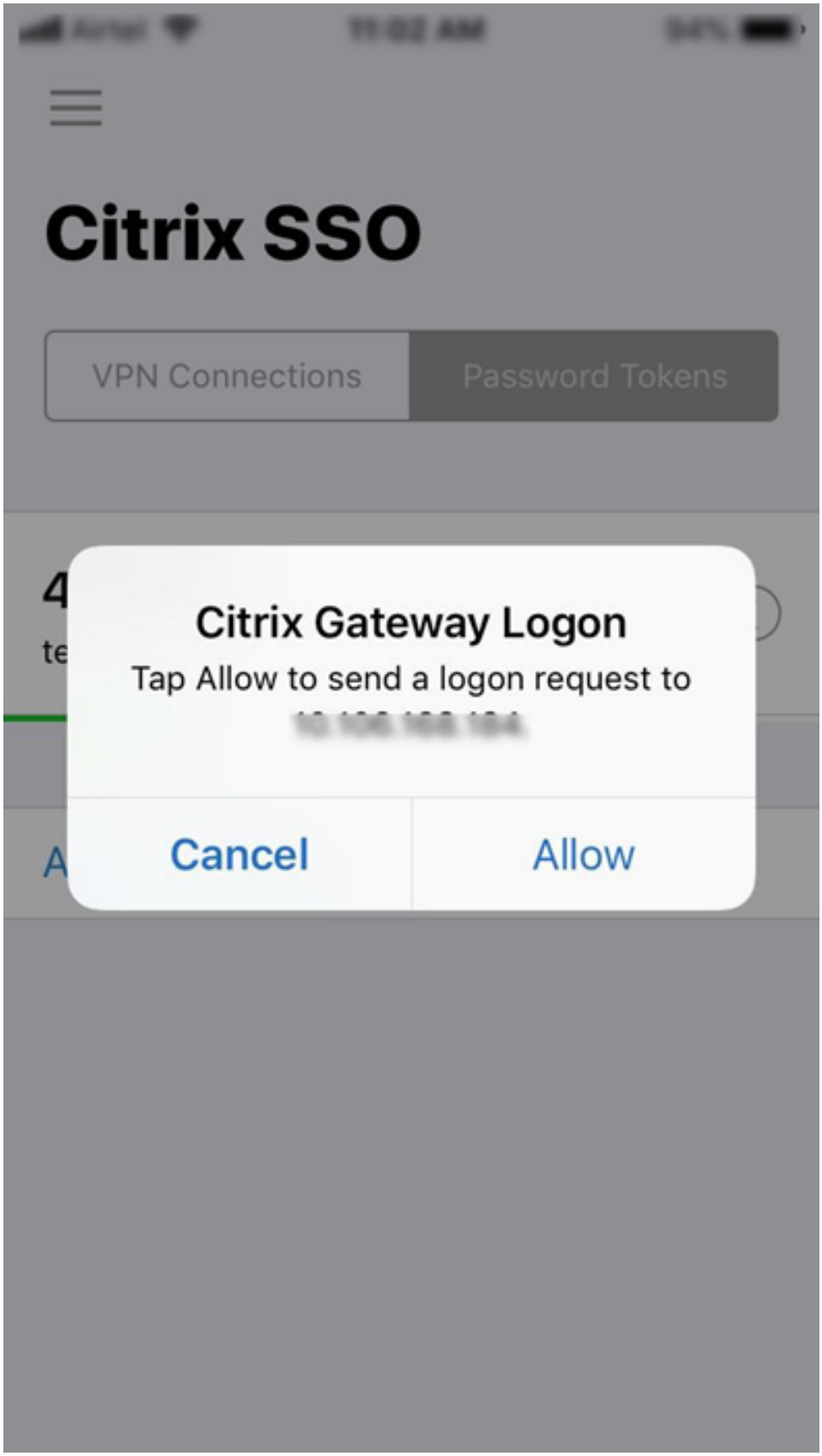


2. Geben Sie Ihren LDAP-Benutzernamen und Ihr Kennwort ein und wählen Sie dann **Senden**aus.

   Eine Benachrichtigung wird an Ihr registriertes Gerät gesendet.

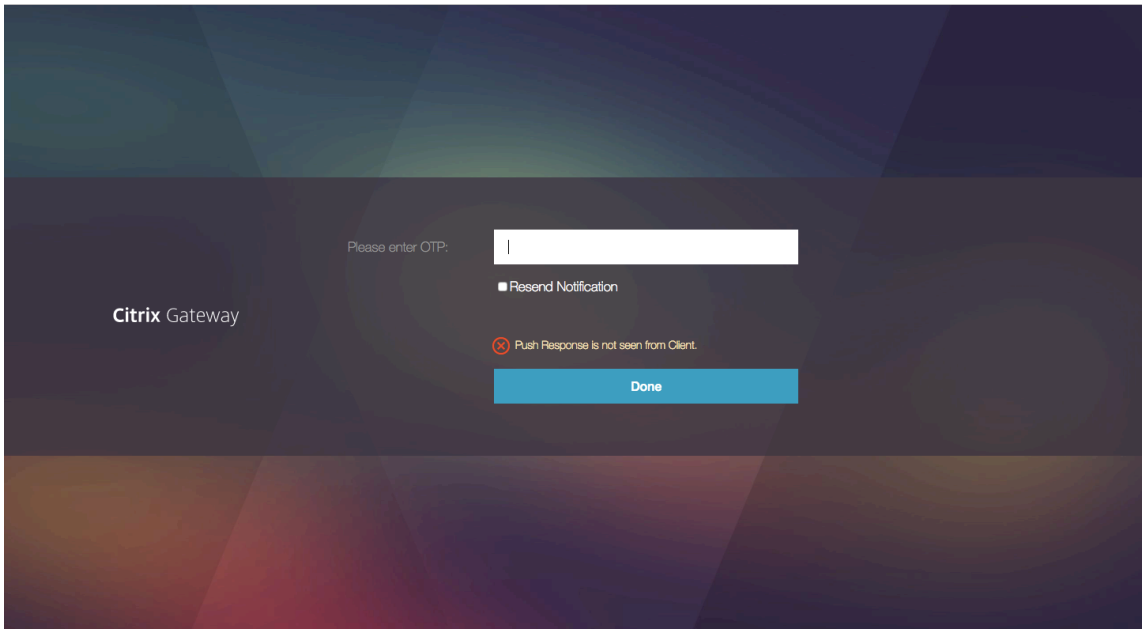
   Hinweis: Wenn Sie das OTP manuell eingeben möchten, müssen Sie **Klicken** auswählen, um OTP manuell einzugeben, und das OTP in das Feld **TOTP** eingeben.

3. Öffnen Sie die Citrix SSO-App auf Ihrem registrierten Gerät und tippen Sie auf **Zulassen**.



Hinweis:

- Auf einem iOS-Gerät werden Sie als zusätzlichen Authentifizierungsfaktor zur Eingabe von Touch-ID/Face-ID/Passcode aufgefordert.
- Der Authentifizierungsserver wartet auf die Antwort der Push-Serverbenachrichtigung, bis der konfigurierte Timeout-Zeitraum abgelaufen ist. Nach dem Timeout zeigt NetScaler Gateway die Anmeldeseite an. Die Benutzer können das OTP dann manuell eingeben oder auf Benachrichtigung **erneut senden klicken, um die Benachrichtigung** erneut auf dem registrierten Gerät zu erhalten. Basierend auf der von Ihnen ausgewählten Option validiert das Gateway das von Ihnen eingegebene Einmalpasswort oder sendet die Benachrichtigung erneut an Ihr registriertes Gerät.



- Es wird keine Benachrichtigung über einen Fehler bei der Anmeldung an Ihr registriertes Gerät gesendet.

Bedingungen für Ausfälle

- Die Geräteregistrierung schlägt in den folgenden Fällen möglicherweise fehl.
  - Das Serverzertifikat kann vom Endbenutzergerät nicht vertrauenswürdig sein.
  - NetScaler Gateway, das zur Registrierung für OTP verwendet wurde, ist für den Client nicht erreichbar.
- Die Benachrichtigungen können in den folgenden Fällen fehlschlagen.
  - Das Benutzergerät ist nicht mit dem Internet verbunden
  - Benachrichtigungen auf dem Benutzergerät sind blockiert
  - Der Benutzer genehmigt die Benachrichtigung auf dem Gerät nicht

In diesen Fällen wartet der Authentifizierungsserver, bis der konfigurierte Timeout-Zeitraum abläuft. Nach dem Timeout zeigt NetScaler Gateway eine Anmeldeseite mit den Optionen an, das OTP manuell einzugeben oder die Benachrichtigung erneut auf Ihrem registrierten Gerät zu senden. Basierend auf der ausgewählten Option erfolgt eine weitere Validierung.

Fehler-Protokolle

Im Folgenden sind die erwarteten Protokolle aufgeführt, wenn der OTP-Push-Dienst nicht erreichbar ist.

- Pushbenachrichtigung fehlgeschlagen, wenn das Benutzergerät nicht mit dem Internet verbunden ist - Push: Push Request konnte nicht auf "`client name`" für den Push-Dienst vorbereitet werden.
- Fehlerprotokoll für Geräteregistrierung - Push: Es sind keine Geräte registriert, um die Push-Anfrage an die Cloud für "`client name`" zu senden.
- Falls der Benutzer den Push nicht akzeptiert - Push: Antwort wird vom Client nicht gesehen, für "`user name`", überprüfen Sie die Wiederholungsoptionen.

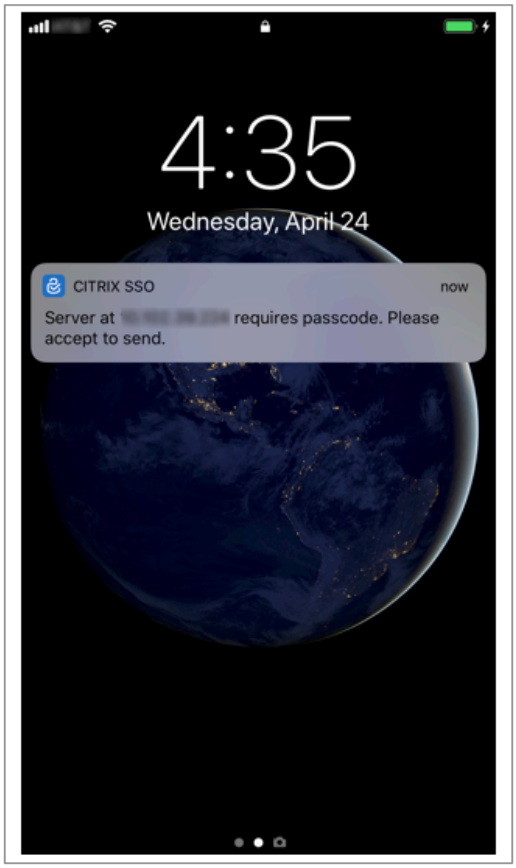
Citrix SSO-App-Verhalten unter iOS — weist darauf hin

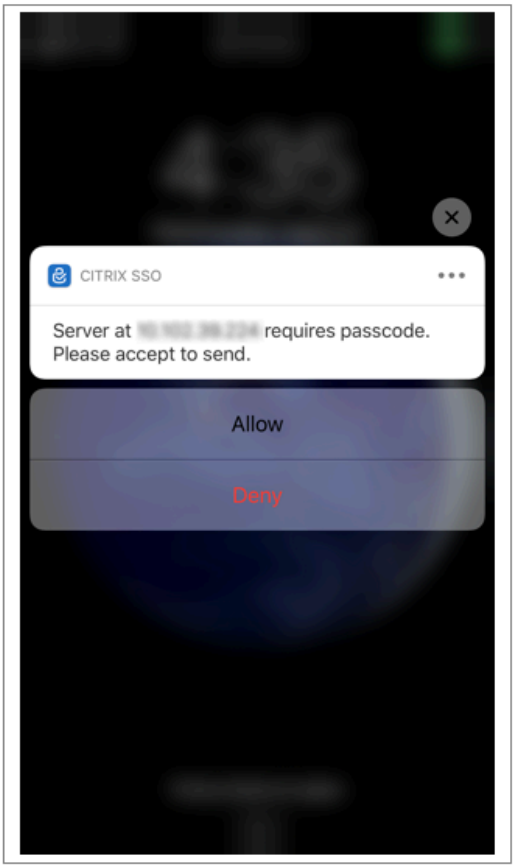
Verknüpfungen für Benachrichtigungen

Die Citrix SSO iOS-App bietet Unterstützung für umsetzbare Benachrichtigungen, um die Benutzerfreundlichkeit zu verbessern. Sobald eine Benachrichtigung auf einem iOS-Gerät eingegangen ist und das Gerät gesperrt ist oder sich die Citrix SSO-App nicht im Vordergrund befindet, können Benutzer die in der Benachrichtigung integrierten Verknüpfungen verwenden, um die Anmeldeanfrage entweder zu genehmigen oder abzulehnen.

Um auf Benachrichtigungsverknüpfungen zuzugreifen, müssen Benutzer je nach Hardware des Geräts entweder eine Berührung erzwingen (3D-Touch) oder die Benachrichtigung lange drücken. Durch Auswahl der Aktion Verknüpfung zulassen wird eine Anmeldeanfrage an NetScaler gesendet. Abhängig davon, wie die Authentifizierungsrichtlinie für den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver konfiguriert ist;

- Die Anmeldeanfrage kann im Hintergrund gesendet werden, ohne dass die App im Vordergrund gestartet oder das Gerät entsperrt werden muss.
- Die App fordert möglicherweise als zusätzlichen Faktor zur Eingabe von Touch-ID/Face-ID/Passcode auf. In diesem Fall wird die App im Vordergrund gestartet.



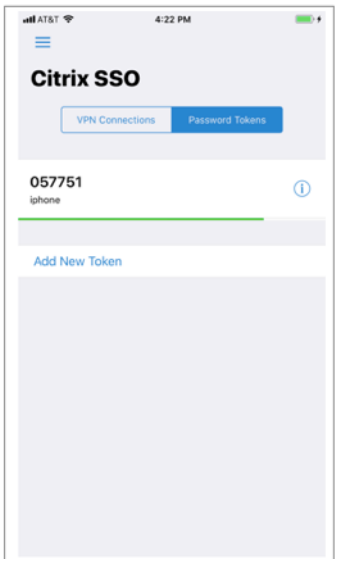


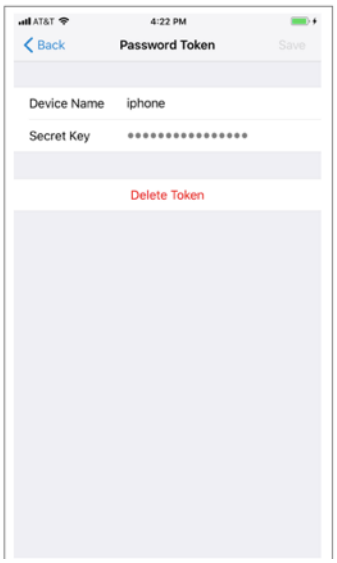
Löschen von Kennwort-Token von Citrix SSO

1. Um ein für Push registriertes Kennwort-Token in der Citrix SSO-App zu löschen, müssen Benutzer die folgenden Schritte ausführen:
2. Heben Sie die Registrierung des iOS-/Android-Geräts auf dem Gateway auf (entfernen). Der QR-Code zum Entfernen der Registrierung vom Gerät wird angezeigt.
3. Öffnen Sie die Citrix SSO-App und tippen Sie auf die Info-Schaltfläche des zu löschenden Kennwort-Tokens.
4. Tippen **Sie auf Token löschen** und scannen Sie den QR-Code.

Hinweis:

- Wenn der QR-Code gültig ist, wird das Token erfolgreich aus der Citrix SSO-App entfernt.
- Benutzer können auf Löschen erzwingen tippen, um ein Kennwort-Token zu löschen, ohne den QR-Code scannen zu müssen, wenn das Gerät bereits aus dem Gateway entfernt wurde. Erzwungenes Löschen kann dazu führen, dass das Gerät weiterhin Benachrichtigungen erhält, wenn das Gerät nicht aus NetScaler Gateway entfernt wurde.





E-Mail-OTP-Authentifizierung

May 11, 2023

E-Mail-OTP wird mit NetScaler 12.1 Build 51.x eingeführt. Mit der E-Mail-OTP-Methode können Sie sich mit dem Einmalkennwort (OTP) authentifizieren, das an die registrierte E-Mail-Adresse gesendet wird. Wenn Sie versuchen, sich bei einem Dienst zu authentifizieren, sendet der Server ein OTP an die registrierte E-Mail-Adresse des Benutzers.

Um die E-Mail-OTP-Funktion nutzen zu können, müssen Sie zuerst Ihre alternative E-Mail-ID registrieren. Eine alternative E-Mail-ID-Registrierung ist erforderlich, damit das OTP an diese E-Mail-ID gesendet werden kann, da Sie bei einer Kontosperrung oder wenn Sie das AD-Kennwort vergessen haben, nicht auf die primäre E-Mail-ID zugreifen können.

Sie können die E-Mail-OTP-Validierung ohne E-Mail-ID-Registrierung verwenden, wenn Sie die alternative E-Mail-ID bereits als Teil eines AD-Attributs angegeben haben. Sie können in der E-Mail-Aktion auf dasselbe Attribut verweisen, anstatt die alternative E-Mail-ID im Abschnitt E-Mail-Adresse anzugeben.

Voraussetzungen

Bevor Sie die E-Mail-OTP-Funktion konfigurieren, sollten Sie die folgenden Voraussetzungen prüfen:

- NetScaler Feature Release 12.1 Build 51.28 und höher
- Die E-Mail-OTP-Funktion ist nur im nFactor-Authentifizierungsablauf verfügbar.
  - Weitere Einzelheiten finden Sie unter https://support.citrix.com/pages/citrix-adc-authentication-how#nfactor

- Unterstützt für AAA-TM, NetScaler Gateway (Browser, Native Plug-in und Receiver).

Active Directory-Einstellung

- Unterstützte Version ist 2016/2012 und 2008 Active Directory-Domänenfunktionsebene
- Der Benutzername von NetScaler LdapBind muss Schreibzugriff auf den AD-Pfad des Benutzers haben

E-Mail Server

- Stellen Sie sicher, dass die Anmeldungsbasierte Authentifizierung auf dem SMTP-Server aktiviert ist, damit die E-Mail-OTP-Lösung funktioniert. NetScaler unterstützt nur die auf AUTH LOGIN basierende Authentifizierung, damit E-Mail-OTP funktioniert.
- Um sicherzustellen, dass die auf AUTH LOGIN basierende Authentifizierung aktiviert ist, geben Sie den folgenden Befehl auf dem SMTP-Server ein. Wenn die auf Anmeldung basierende Authentifizierung aktiviert ist, stellen Sie fest, dass der Text AUTH LOGIN in der Ausgabe **fett gedruckt** erscheint.

```
root@ns# telnet <IP address of the SMTP server><Port number of the server>
ehlo
root@ns# telnet 10.106.3.
Trying 10.106.
Connected to 10.106.
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22 Nov
2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
For information on how to enable login based authentication, see
https://support.microfocus.com/kb/doc.php?id=7020367
```

Einschränkungen

- Diese Funktion wird nur unterstützt, wenn das Authentifizierungs-Backend LDAP ist.
- Die bereits registrierte alternative E-Mail-ID wurde nicht angezeigt.
- Nur die alternative E-Mail-ID von der KBA-Registrierungsseite kann nicht aktualisiert werden.
- Die E-Mail-OTP-Authentifizierung kann nicht der erste Faktor im Authentifizierungsablauf sein. Dies ist beabsichtigt, um eine robuste Authentifizierung zu erreichen.

- Wenn sowohl alternative E-Mail-ID als auch KBA mit derselben Authentifizierungsaktion konfiguriert wurden, muss das Attribut für beide identisch sein.
- Für das native Plug-in und Receiver wird die Registrierung nur über einen Browser unterstützt.

Active Directory-Konfiguration

- E-Mail-OTP verwendet das Active Directory-Attribut als Benutzerdatenspeicher.
- Nachdem Sie die alternative E-Mail-ID registriert haben, wird die E-Mail-ID an die NetScaler-Appliance gesendet, und die Appliance speichert sie im konfigurierten KB-Attribut im AD-Benutzerobjekt.
- Die alternative E-Mail-ID wird verschlüsselt und im konfigurierten AD-Attribut gespeichert.

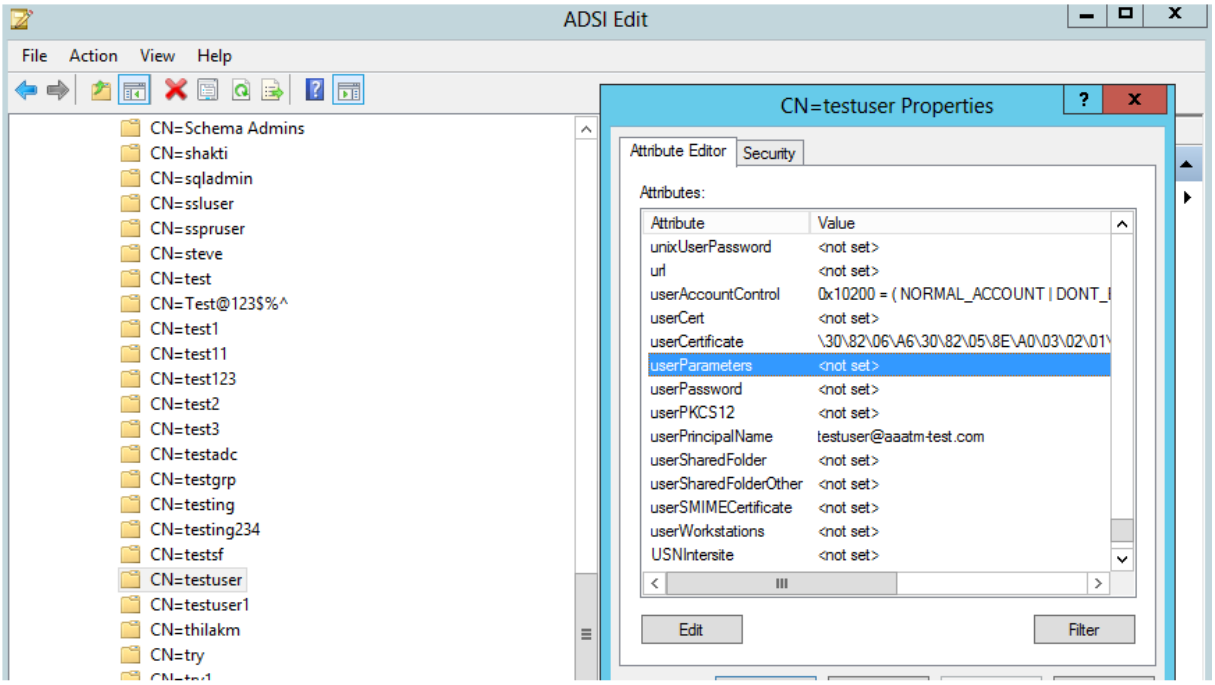
Beachten Sie beim Konfigurieren eines AD-Attributs Folgendes:

- Die unterstützte Länge des Attributnamens muss mindestens 128 Zeichen betragen.
- Der Attributtyp muss “DirectoryString” sein.
- Dasselbe AD-Attribut kann für Native OTP- und E-Mail-OTP-Registrierungsdaten verwendet werden.
- Der LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.

Verwenden vorhandener Attribute

Das in diesem Beispiel verwendete Attribut ist `Userparameters`. Da es sich um ein vorhandenes Attribut innerhalb des AD-Benutzers handelt, müssen Sie keine Änderungen am AD selbst vornehmen. Sie müssen jedoch sicherstellen, dass das Attribut nicht verwendet wird.

Um sicherzustellen, dass das Attribut nicht verwendet wird, navigieren Sie zu **ADSI** und wählen Sie Benutzer aus, klicken Sie mit der rechten Maustaste auf den Benutzer und scrollen Sie nach unten zur Attributliste. Sie müssen sehen, dass der Attributwert für **UserParametersnicht festgelegt ist**. Dies deutet darauf hin, dass das Attribut derzeit nicht verwendet wird.



Konfigurieren von E-Mail-OTP

Die E-Mail-OTP-Lösung besteht aus den folgenden zwei Teilen:

- E-Mail-Registrierung
- E-Mail-Validierung

Registrierung der E-Mail-ID

Führen Sie die folgende Konfiguration über die CLI durch, nachdem das KBA-Registrierungsschema erfolgreich erstellt wurde:

1. Binden Sie das Portalthema und das Zertifikat an VPN Global.

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine vorhergehende Zertifikatsbindung ist erforderlich, um die im AD-Attribut gespeicherten Benutzerdaten (KB Q&A und alternative Mail-ID registriert) zu verschlüsseln.

2. Erstellen Sie eine LDAP-Authentifizierungsrichtlinie.


```
add authentication ldapAction ldap -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL
add authentication Policy ldap -rule true -action ldap
<!--NeedCopy-->
```

3. Erstellen Sie eine LDAP-Authentifizierungsrichtlinie für die E-Mail-Registrierung.

```
add authentication ldapAction ldap_email_registration -serverIP
    10.102.2.2 -serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -
    ldapBindDn administrator@aaatm-test.com -ldapBindDnPassword
    freebsd -ldapLoginName samAccountName -secType SSL -KBAttribute
     userParameters -alternateEmailAttr userParameters
add authentication Policy ldap_email_registration -rule true -
    action ldap_email_registration
<!--NeedCopy-->
```

4. Erstellen Sie ein Anmeldeschema für die E-Mail-Registrierung und eine Policy Label.

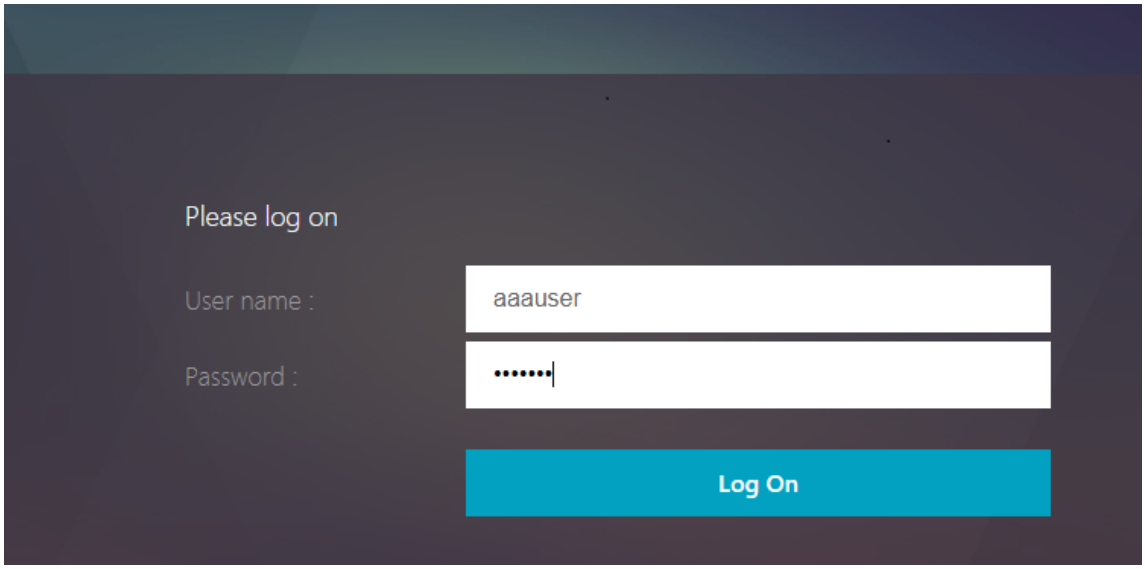
```
add authentication loginSchema onlyEmailRegistration -
    authenticationSchema /nsconfig/loginschema/LoginSchema/
    AltEmailRegister.xml
add authentication policylabel email_Registration_factor -
    loginSchema onlyEmailRegistration
bind authentication policylabel email_Registration_factor -
    policyName ldap_email_registration -priority 1 -
    gotoPriorityExpression NEXT
<!--NeedCopy-->
```

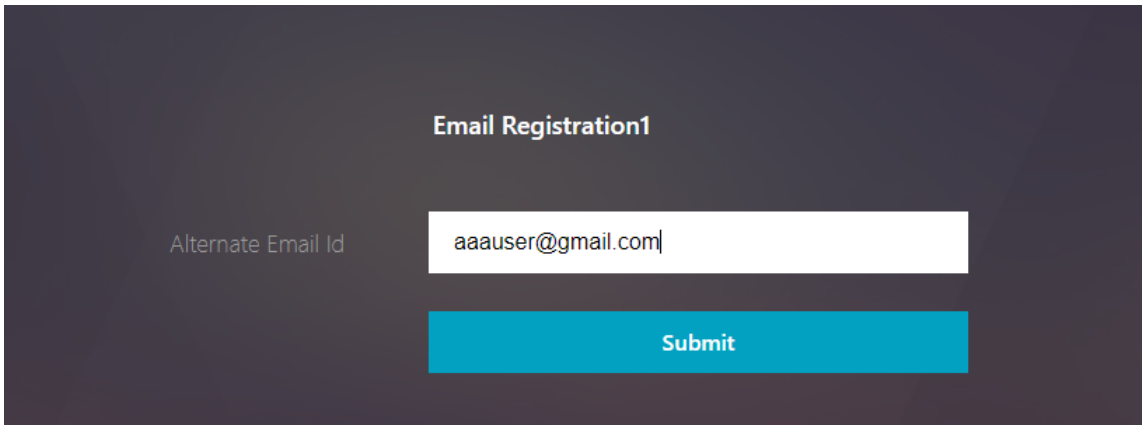
5. Binden Sie die Authentifizierungsrichtlinie an den virtuellen Authentifizierungsserver.

```
bind authentication vserver authvs  - policy ldap -priority 1 -
    nextFactor email_Registration_factor -gotoPriorityExpression
    NEXT
<!--NeedCopy-->
```

6. Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, müssen Sie den folgenden GUI-Bildschirm sehen. Wenn Sie beispielsweise über die URL zugreifen, wird https://lb1.server.com/ Ihnen eine erste Anmeldeseite angezeigt, für die nur die LDAP-Anmeldeinformationen erforderlich sind, gefolgt von einer alternativen E-Mail-Registrierungsseite.

   Hinweis: Die Domäne https://lb1.server.com/ kann entweder zum Gateway oder zu einem virtuellen Authentifizierungsserver gehören.





Hinweis:

- Sie können dasselbe Authentifizierungsschema sowohl für die KBA-Registrierung als auch für die E-Mail-ID-Registrierung verwenden.
- Bei der Konfiguration der KBA-Registrierung können Sie im Abschnitt **E-Mail-Registrierung die Option Alternative E-Mail registrieren** wählen, um eine alternative E-Mail-ID zu registrieren.

E-Mail-Validierung

Führen Sie die folgenden Schritte für die E-Mail-Validierung aus.

1. Binden Sie das Portal-Thema und das Zertifikat an VPN Global

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```


> **Hinweis:**
>
> Die vorherige Zertifikatsbindung ist erforderlich, um die im AD-Attribut gespeicherten Benutzerdaten (KB Q&A und alternative E-Mail-ID registriert) zu entschlüsseln.

2. Erstellen Sie eine LDAP-Authentifizierungsrichtlinie. LDAP muss ein wichtiger Faktor für den E-Mail-Validierungsfaktor sein, da Sie die E-Mail-ID oder die alternative E-Mail-ID des Benutzers für die E-Mail-OTP-Validierung benötigen.

```
add authentication ldapAction ldap1 -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -   ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL -KBAttribute
    userParameters -alternateEmailAttr userParameters
add authentication Policy ldap1 -rule true -action ldap1
<!--NeedCopy-->
```

3. Erstellen Sie eine E-Mail-Authentifizierungsrichtlinie.

```
add authentication emailAction email -userName sqladmin@aaa.com -
    password freebsd-encrypted -encryptmethod ENCMTHD_3 -serverURL
    "smtps://10.2.3.3:25" -content "OTP is $code" -
    defaultAuthenticationGroup emailgrp -emailAddress "aaa.user.
    attribute("alternate_mail")"
add authentication Policy email -rule true  - action email
<!--NeedCopy-->
```

   In dem zuvor erwähnten Befehl ist die **E-Mail-Adresse** die alternative E-Mail-ID, die bei der KBA-Registrierung angegeben wurde.

4. Erstellen Sie eine E-Mail-OTP-Validierungsrichtlinienbezeichnung.

```
add authentication policylabel email_Validation_factor
bind authentication policylabel email_Validation_factor -
    policyName email -priority 1 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

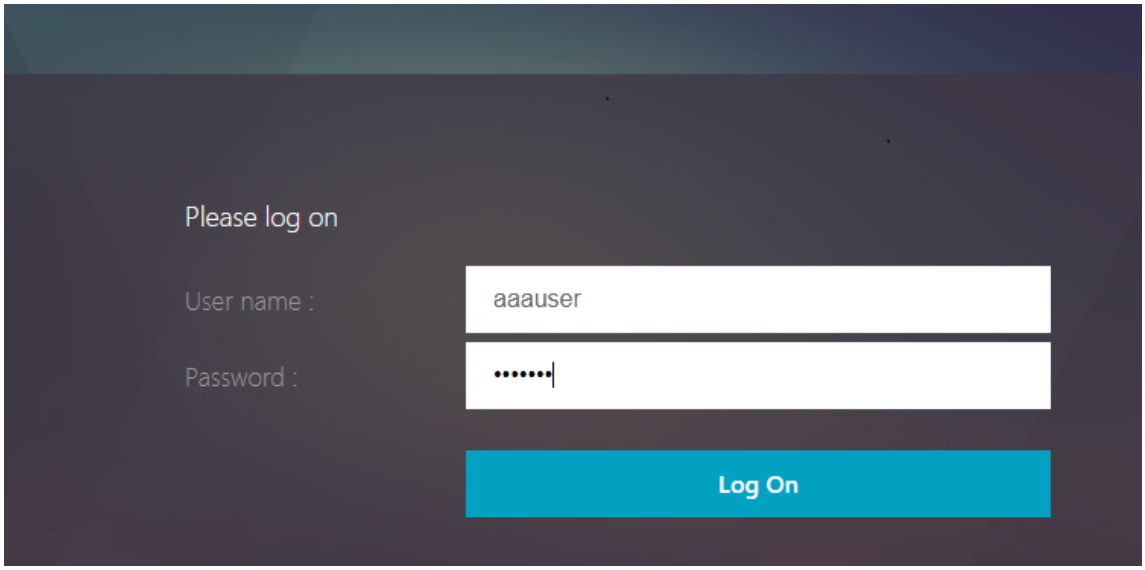
5. Binden Sie die Authentifizierungsrichtlinie an den virtuellen Authentifizierungsserver.

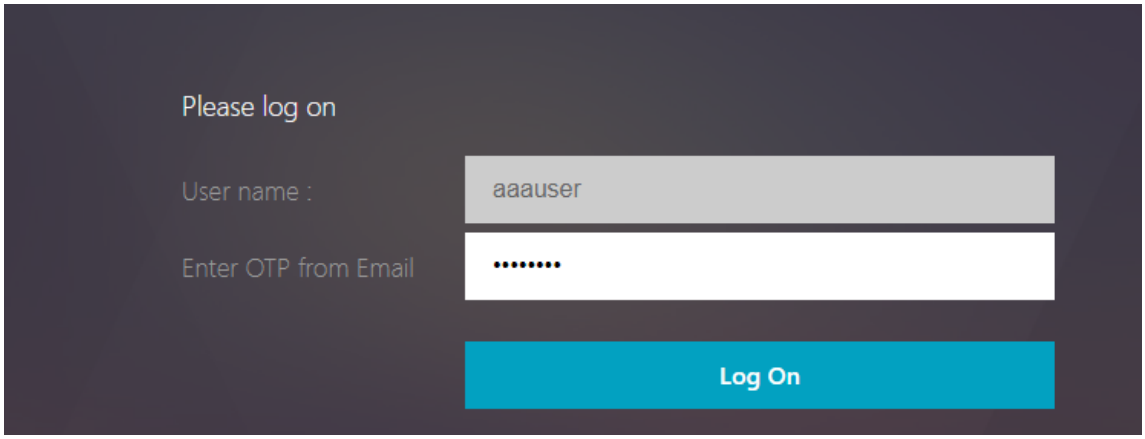
```
bind authentication vserver authvs  -  policy ldap1 -priority 1 -
    nextFactor email_Validation_factor -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

6. Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, müssen Sie den folgenden GUI-Bildschirm für die E-Mail-OTP-Validierung sehen. Wenn Sie

beispielsweise über die URL zugreifen, wird https://lb1.server.com/ Ihnen eine erste Anmeldeseite angezeigt, für die nur die LDAP-Anmeldeinformationen erforderlich sind, gefolgt von der Seite “EMAIL OTP-Validierung”.

> **Hinweis:**
>
> In der LDAP-Richtlinie muss konfiguriert werden, dass `alternateEmailAttr` die E-Mail-ID des Benutzers vom AD-Attribut abgefragt werden kann.





Problembehandlung

Bevor Sie das Protokoll analysieren, ist es besser, die Protokollebene wie folgt auf Debuggen festzulegen.

```
set syslogparams -loglevel DEBUG
<!--NeedCopy-->
```


Registrierung - Erfolgreiches Szenario

Die folgenden Einträge weisen auf eine erfolgreiche Benutzerregistrierung hin.

```
"ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1"
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  "
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw=="

<!--NeedCopy-->
```

Registrierung — Ausfallszenario

Auf der Benutzeranmeldeseite wird die folgende Fehlermeldung angezeigt: “Ihre Anfrage kann nicht abgeschlossen werden”. Dies deutet darauf hin, dass der Cert-Key, der zum Verschlüsseln der Benutzerdaten an das globale VPN gebunden werden soll, fehlt.

```
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:4 6 GMT
    0-PPE-1 : default SSLVPN Message 696 0 :  "Encrypt UserData: No
    Encryption cert is bound to vpn global"
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:46 GMT  0-
    PPE-1 : default SSLVPN Message 697 0 :  "KBA Register: Alternate
    email id Encrypted blob length is ZERO aaauser"
<!--NeedCopy-->
```

E-Mail-Validierung — Erfolgreiches Szenario

Die folgenden Einträge weisen auf eine erfolgreiche E-Mail-OTP-Validierung hin.

```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
<!--NeedCopy-->
```

E-Mail-Validierung — Ausfallszenario

Auf der Benutzeranmeldeseite wird die Fehlermeldung “Ihre Anfrage kann nicht abgeschlossen werden” angezeigt. Dies bedeutet, dass die anmeldungsbasierte Authentifizierung auf dem E-Mail-Server nicht aktiviert ist und dasselbe aktiviert werden muss.

```
" /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp
    [100]: void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID:
    8]SMTP Configuration is Secure..
```



```
2 /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[108]:
     void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID: 8]
     First login succeeded
3 Wed Mar  4 17:16:28 2020
4 /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/naaad.c[697]: main
     0-0: timer 2 firing...
5 /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[127]:
     void ThreadWorker_SendMailJob(SMTPJob*) 0-0: [POCO-ERROR][JobID: 8]
     Poco SMTP Mail Dispatch  Failed. SMTP TYPE:1, SMTPException:
     Exception occurs. SMTP Exception: The mail service does not support
     LOGIN authentication: 250-smtprelay.citrix.com Hello [10.9.154.239]
6 250-SIZE 62914560
7 250-PIPELINING
8 250-DSN
9 250-ENHANCEDSTATUSCODES
10 250-8BITMIME
11 250-BINARYMIME
12 250 CHUNKING
13 <!--NeedCopy-->
```

Re-Captcha-Konfiguration für die nFactor-Authentifizierung

May 11, 2023

NetScaler Gateway unterstützt eine neue erstklassige Aktion `captchaAction`, die die Re-Captcha-Konfiguration vereinfacht. Da Re-Captcha eine erstklassige Aktion ist, kann sie ein eigener Faktor sein. Sie können Re-Captcha überall im nFactor-Flow injizieren.

Zuvor mussten Sie benutzerdefinierte WebAuth Richtlinien mit Änderungen an der RFWebUI schreiben. Mit Einführen von `captchaAction` müssen Sie das JavaScript nicht mehr ändern.

> **Wichtig:**
>
> Wenn Re-Captcha zusammen mit den Feldern für den Benutzernamen oder das Kennwort im Schema verwendet wird, ist die Schaltfläche **Senden** deaktiviert, bis Re-Captcha erfüllt ist.

Re-Captcha-Konfiguration

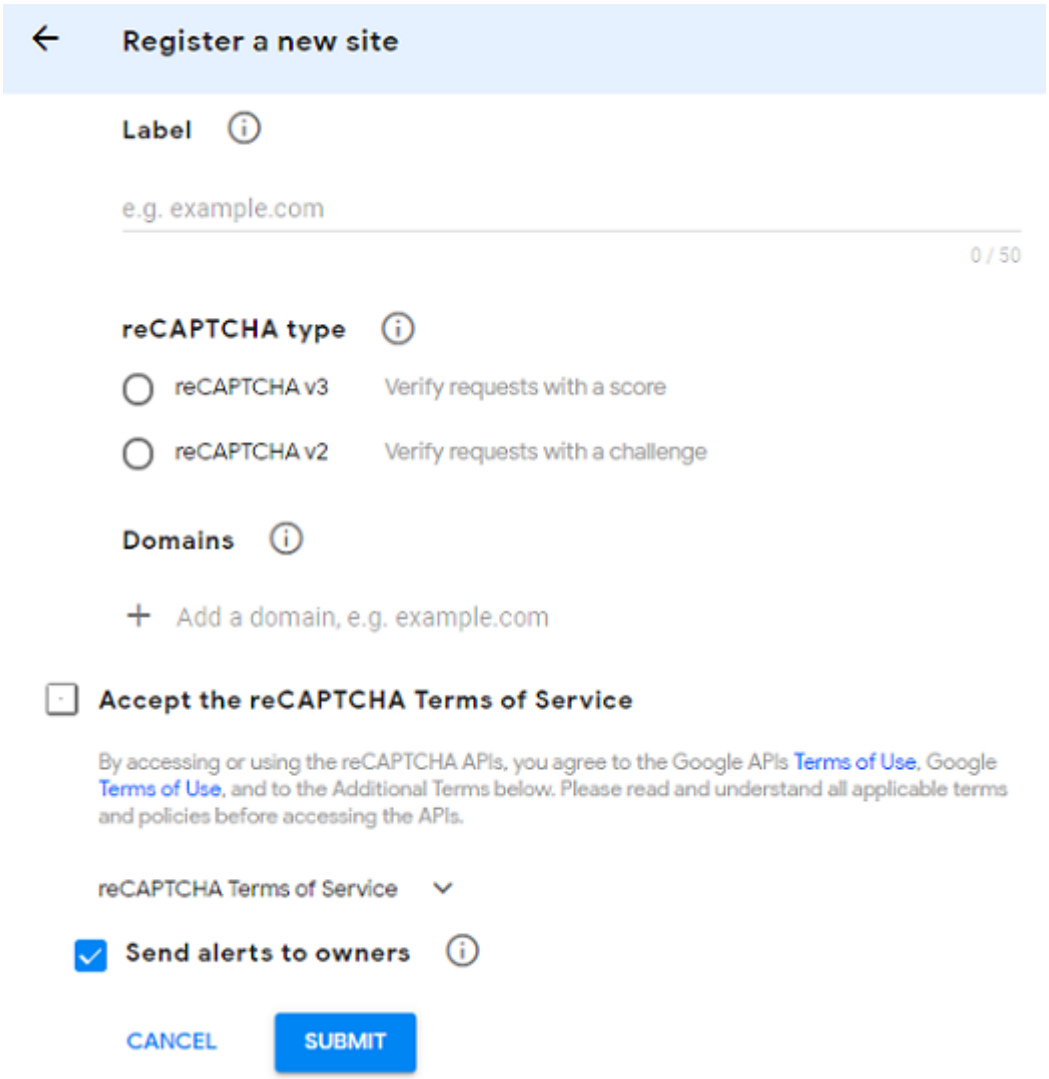
Die Re-Captcha-Konfiguration besteht aus zwei Teilen.

1. Konfiguration bei Google für die Registrierung von Re-Captcha.
2. Konfiguration auf der NetScaler Appliance zur Verwendung von Re-Captcha als Teil des Anmeldeflusses.

Re-Captcha-Konfiguration bei Google

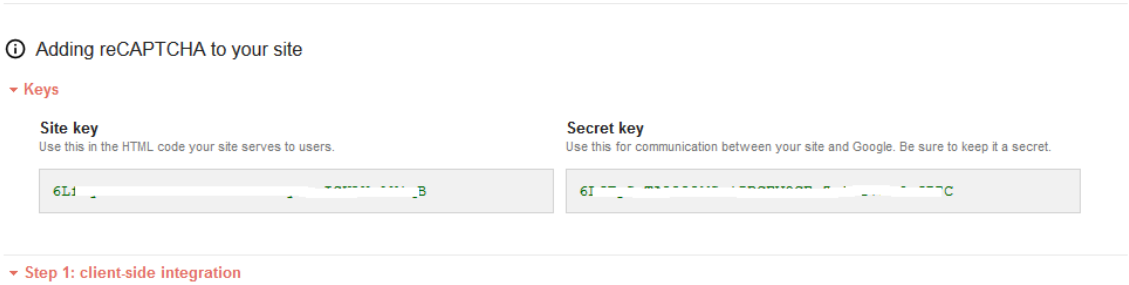
Registrieren Sie eine Domain für Re-Captcha unter https://www.google.com/recaptcha/admin#llist.

1. Wenn Sie zu dieser Seite navigieren, wird der folgende Bildschirm angezeigt.



> **Hinweis**
>
> Verwenden Sie nur reCAPTCHA v2. Unsichtbares Re-Captcha befindet sich noch in der Vorschau.

2. Nachdem eine Domain registriert wurde, werden “SiteKey” und “SecretKey” angezeigt.



> **Hinweis**
>
> Der “SiteKey” und “SecretKey” sind aus Sicherheitsgründen ausgegraut. “SecretKey” muss sicher aufbewahrt werden.

Re-Captcha-Konfiguration auf einer NetScaler Appliance

Die Re-Captcha-Konfiguration auf der NetScaler Appliance kann in drei Teile unterteilt werden:

- Bildschirm “Re-Captcha anzeigen”
- Veröffentlichen Sie die Re-Captcha-Antwort auf dem Google-Server
- Die LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Bildschirm “Re-Captcha anzeigen”

Die Anpassung des Anmeldeformulars erfolgt über das Anmeldeschema SingleAuthCaptcha.xml. Diese Anpassung wird auf dem virtuellen Authentifizierungsserver angegeben und zum Rendern des Anmeldeformulars an die Benutzeroberfläche gesendet. Das integrierte Anmeldeschema SingleAuthCaptcha.xml ist im Verzeichnis `/nsconfig/loginSchema/LoginSchema` auf der NetScaler-Appliance.

> **Wichtig**
>
> - Das Anmeldeschema SingleAuthCaptcha.xml kann verwendet werden, wenn LDAP als erster Faktor konfiguriert ist.
> - Basierend auf Ihrem Anwendungsfall und verschiedenen Schemas können Sie das vorhandene Schema ändern. Zum Beispiel, wenn Sie nur den Re-Captcha-Faktor (ohne Benutzername oder Kennwort) oder eine doppelte Authentifizierung mit Re-Captcha benötigen.
> - Wenn benutzerdefinierte Änderungen vorgenommen wurden oder die Datei umbenannt wird, empfiehlt Citrix, alle LoginSchemas aus dem Verzeichnis `/nsconfig/loginschema/LoginSchema` in das übergeordnete Verzeichnis `/nsconfig/loginschema` zu kopieren.

So konfigurieren Sie die Anzeige von Re-Captcha über die CLI


```
add authentication loginSchema singleauthcaptcha -authenticationSchema
    /nsconfig/loginschema/SingleAuthCaptcha.xml

add authentication loginSchemaPolicy singleauthcaptcha -rule true -
    action singleauthcaptcha

add authentication vserver auth SSL <IP> <Port>

add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-
    key-file>

bind ssl vserver auth -certkey vserver-cert

bind authentication vserver auth -policy singleauthcaptcha -priority 5
    -gotoPriorityExpression END
<!--NeedCopy-->
```

Veröffentlichen Sie die Re-Captcha-Antwort auf dem Google-Server

Nachdem Sie das Re-Captcha konfiguriert haben, das den Benutzern angezeigt werden muss, fügen die Administratoren die Konfiguration zum Google-Server hinzu, um die Re-Captcha-Antwort des Browsers zu überprüfen.

So überprüfen Sie die Re-Captcha-Antwort des Browsers

```
add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-
    from-google> -secretkey <secretkey-from-google>

add authentication policy myrecaptcha -rule true -action myrecaptcha

bind authentication vserver auth -policy myrecaptcha -priority 1
<!--NeedCopy-->
```

Die folgenden Befehle sind erforderlich, um zu konfigurieren, ob AD-Authentifizierung gewünscht ist. Andernfalls können Sie diesen Schritt ignorieren.

```
add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
    636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm
    .com -ldapBindDnPassword <password> -encrypted -encryptmethod
    ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -
    subAttributeName CN -secType SSL -passwdChange ENABLED -
    defaultAuthenticationGroup ldapGroup

```



```
add authenticationpolicy ldap-new -rule true -action ldap-new
<!--NeedCopy-->
```

Die LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Die LDAP-Authentifizierung erfolgt nach Re-Captcha, Sie fügen sie dem zweiten Faktor hinzu.

```
add authentication policylabel second-factor

bind authentication policylabel second-factor -policy ldap-new -
    priority 10

bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
<!--NeedCopy-->
```

Der Administrator muss entsprechende virtuelle Server hinzufügen, je nachdem, ob der virtuelle Lastausgleichsserver oder das NetScaler Gateway-Gerät für den Zugriff verwendet wird. Der Administrator muss den folgenden Befehl konfigurieren, wenn ein virtueller Lastausgleichsserver erforderlich ist:

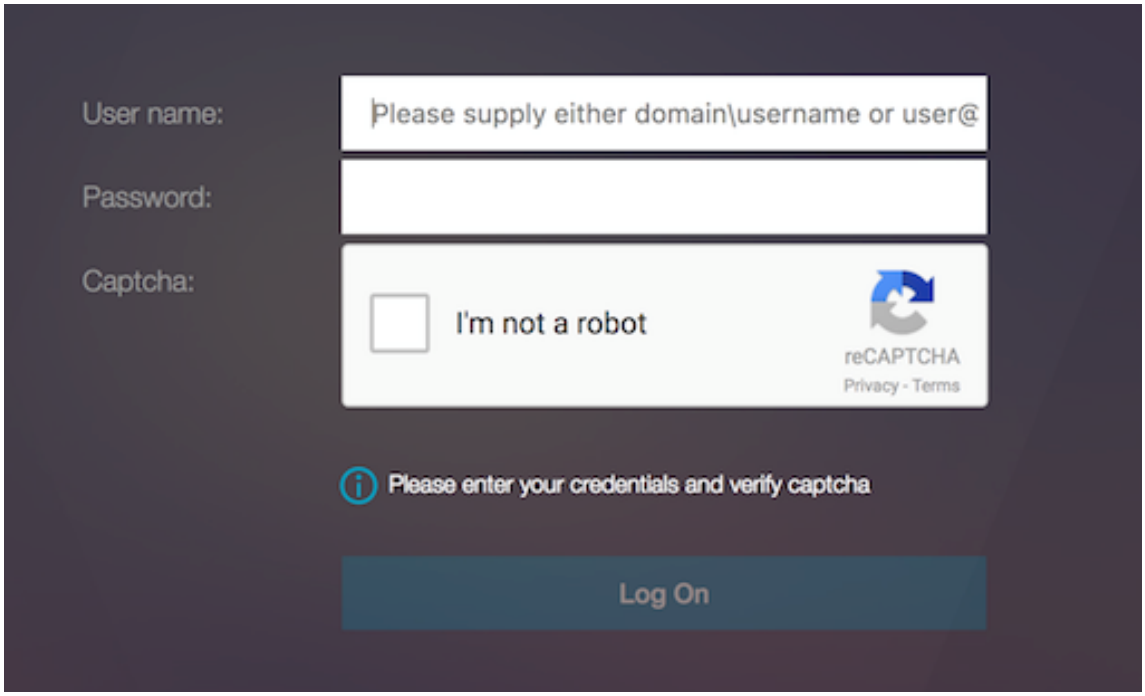
```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com
<!--NeedCopy-->
```

nssp.aaatm.com — Löst sich in einen virtuellen Authentifizierungsserver auf.

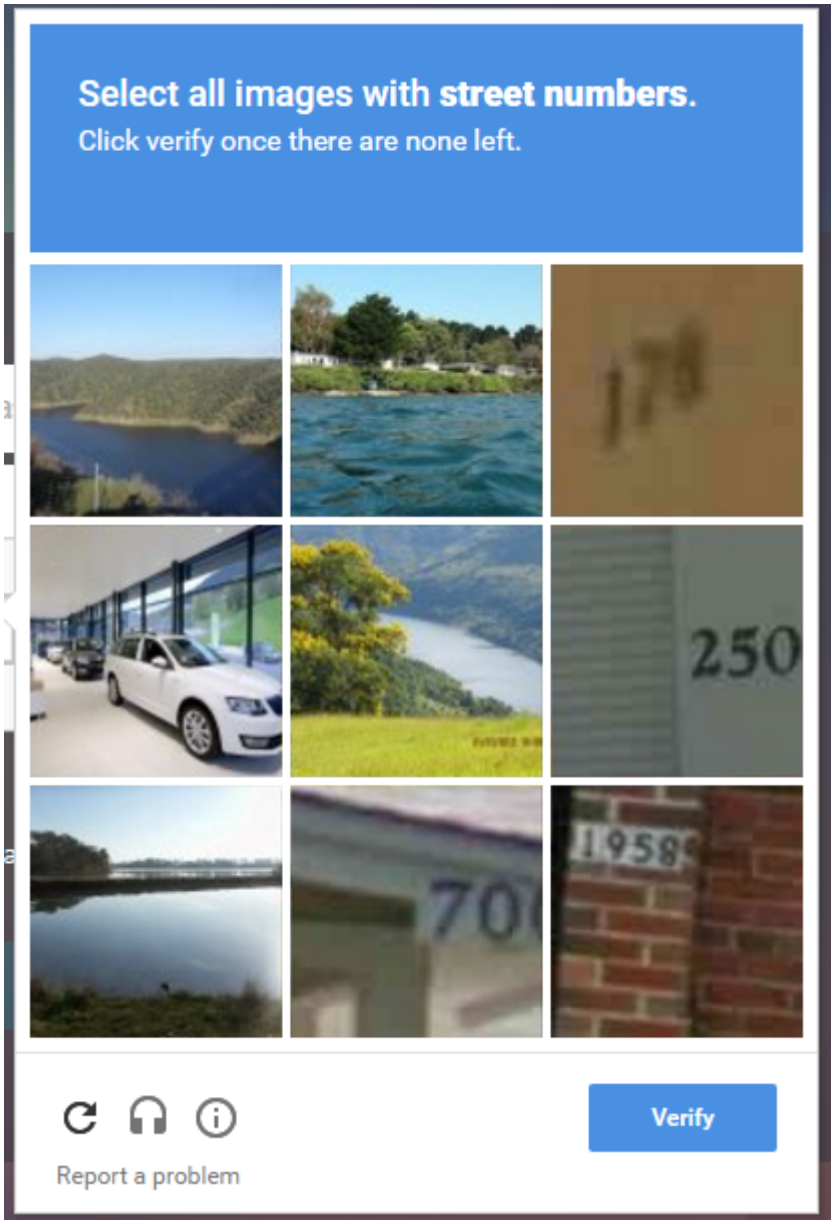
Benutzervalidierung von re-Captcha

Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, müssen Sie die folgende Benutzeroberfläche sehen.

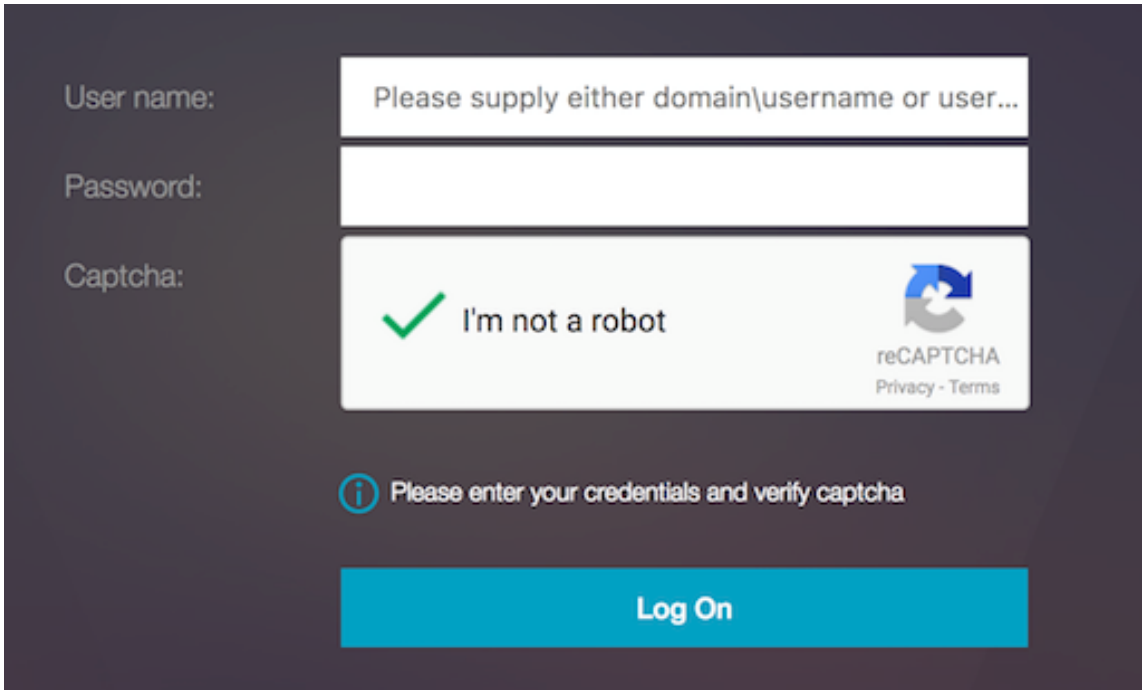
1. Sobald der virtuelle Authentifizierungsserver die Anmeldeseite geladen hat, wird der Anmeldebildschirm angezeigt. Die **Anmeldung** ist deaktiviert, bis Re-Captcha abgeschlossen ist.



2. Wähle Ich bin keine Roboter-Option. Das Re-Captcha-Widget wird angezeigt.



3. Sie werden durch eine Reihe von Re-Captcha-Bildern navigiert, bevor die Abschlussseite angezeigt wird.
4. Geben Sie die AD-Anmeldeinformationen ein, aktivieren Sie das Kontrollkästchen **Ich bin kein Roboter** und klicken Sie auf **Anmelden**. Wenn die Authentifizierung erfolgreich ist, werden Sie zur gewünschten Ressource weitergeleitet.



Hinweise:

- Wenn Re-Captcha mit der AD-Authentifizierung verwendet wird, ist die Schaltfläche **Senden** für Anmeldeinformationen deaktiviert, bis Re-Captcha abgeschlossen ist.
- Das Re-Captcha geschieht in einem eigenen Faktor. Daher müssen alle nachfolgenden Validierungen wie AD im `nextfactor` von Re-Captcha stattfinden.

Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration für häufig verwendete Protokolle

May 11, 2023

Für die Konfiguration der NetScaler Appliance für Authentifizierung, Autorisierung und Prüfung ist ein spezielles Setup auf der NetScaler Appliance und den Browsern der Clients erforderlich. Die Konfiguration variiert je nach Protokoll, das für die Authentifizierung, Autorisierung und Überwachung verwendet wird.

Weitere Informationen zum Konfigurieren der NetScaler Appliance für die Kerberos-Authentifizierung finden Sie unter Umgang mit Authentifizierung, Autorisierung und Auditing mit Kerberos/NTLM.

Authentifizierung, Autorisierung und Audits mit Kerberos/NTLM

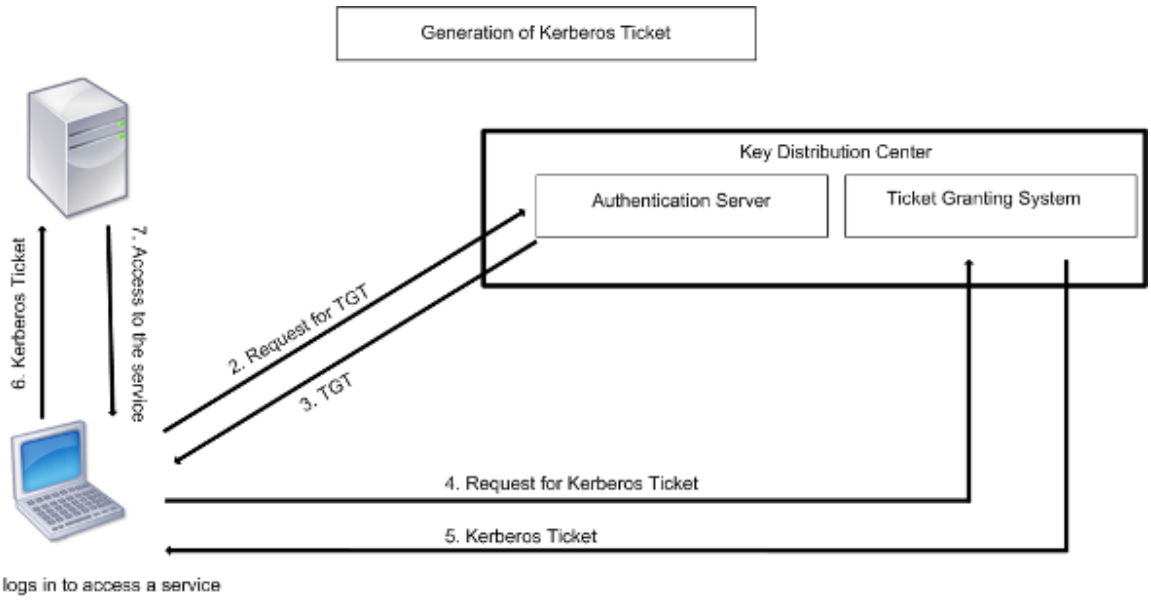
May 11, 2023

Kerberos, ein Authentifizierungsprotokoll für Computernetzwerke, bietet sichere Kommunikation über das Internet. Es wurde hauptsächlich für Client-Server-Anwendungen entwickelt und ermöglicht eine gegenseitige Authentifizierung, bei der Client und Server jeweils die Authentizität des anderen sicherstellen können. Kerberos verwendet einen vertrauenswürdigen Drittanbieter, das als Key Distribution Center (KDC) bezeichnet wird. Ein KDC besteht aus einem Authentifizierungsserver (AS), der einen Benutzer authentifiziert, und einem Ticket Granting Server (TGS).

Jede Entität im Netzwerk (Client oder Server) hat einen geheimen Schlüssel, der nur ihr selbst und dem KDC bekannt ist. Die Kenntnis dieses Schlüssels setzt die Authentizität der Entität voraus. Für die Kommunikation zwischen zwei Entitäten im Netzwerk generiert das KDC einen Sitzungsschlüssel, der als Kerberos-Ticket oder Serviceticket bezeichnet wird. Der Client fordert beim AS Anmeldeinformationen für einen bestimmten Server an. Der Kunde erhält dann ein Ticket, das als Ticket Granting Ticket (TGT) bezeichnet wird. Der Kunde kontaktiert dann das TGS und verwendet das TGT, das er von der AS erhalten hat, um seine Identität nachzuweisen, und bittet um eine Dienstleistung. Wenn der Kunde für den Service in Frage kommt, stellt das TGS dem Kunden ein Kerberos-Ticket aus. Der Client kontaktiert dann den Server, der den Dienst hostet (der als Serviceserver bezeichnet wird) und verwendet das Kerberos-Ticket, um nachzuweisen, dass er für den Empfang des Dienstes autorisiert ist. Das Kerberos-Ticket hat eine konfigurierbare Lebensdauer. Der Client authentifiziert sich nur einmal beim AS. Wenn es den physischen Server mehrmals kontaktiert, verwendet es das AS-Ticket erneut.

Die folgende Abbildung zeigt die grundlegende Funktionsweise des Kerberos-Protokolls.

Abbildung 1. **Funktionsweise von Kerberos**



Die Kerberos-Authentifizierung hat die folgenden Vorteile:

- Schnellere Authentifizierung. Wenn ein physischer Server ein Kerberos-Ticket von einem Client erhält, verfügt der Server über genügend Informationen, um den Client direkt zu authentifizieren. Für die Client-Authentifizierung muss kein Domänencontroller kontaktiert werden, weshalb der Authentifizierungsprozess schneller ist.
- Gegenseitige Authentifizierung. Wenn das KDC einem Client ein Kerberos-Ticket ausstellt und der Client das Ticket verwendet, um auf einen Dienst zuzugreifen, können nur authentifizierte Server das Kerberos-Ticket entschlüsseln. Wenn der virtuelle Server auf der NetScaler-Appliance das Kerberos-Ticket entschlüsseln kann, können Sie daraus schließen, dass sowohl der virtuelle Server als auch der Client authentifiziert sind. Somit erfolgt die Authentifizierung des Servers zusammen mit der Authentifizierung des Clients.
- Single Sign-On zwischen Windows und anderen Betriebssystemen, die Kerberos unterstützen.

Die Kerberos-Authentifizierung kann die folgenden Nachteile haben:

- Kerberos hat strenge Zeitanforderungen. Die Uhren der beteiligten Hosts müssen mit der Kerberos-Serveruhr synchronisiert werden, um sicherzustellen, dass die Authentifizierung nicht fehlschlägt. Sie können diesen Nachteil mildern, indem Sie die Network Time Protocol-Daemons verwenden, um die Host-Uhren synchron zu halten. Kerberos-Tickets haben einen Verfügbarkeitszeitraum, den Sie konfigurieren können.
- Kerberos benötigt, dass der zentrale Server kontinuierlich verfügbar ist. Wenn der Kerberos-Server ausgefallen ist, kann sich niemand anmelden. Sie können dieses Risiko minimieren, indem Sie mehrere Kerberos-Server und Fallback-Authentifizierungsmechanismen verwenden.
- Da die gesamte Authentifizierung von einem zentralen KDC gesteuert wird, kann jede Beeinträchtigung dieser Infrastruktur, z. B. der Diebstahl des Benutzerkennworts für eine lokale Workstation, es einem Angreifer ermöglichen, sich für einen beliebigen Benutzer auszugeben. Sie können dieses Risiko bis zu einem gewissen Grad mindern, indem Sie nur einen Desktop-Computer oder Laptop verwenden, dem Sie vertrauen, oder indem Sie die Vorauthentifizierung mithilfe eines Hardware-Tokens erzwingen.

Um die Kerberos-Authentifizierung verwenden zu können, müssen Sie sie auf der NetScaler-Appliance und auf jedem Client konfigurieren.

Optimierung der Kerberos-Authentifizierung bei Authentifizierung, Autorisierung und Überwachung

Die NetScaler Appliance optimiert und verbessert jetzt die Systemleistung bei der Kerberos-Authentifizierung. Der Authentifizierungs-, Autorisierungs- und Auditing-Daemon merkt sich die ausstehende Kerberos-Anfrage für denselben Benutzer, um die Belastung des Key Distribution Centers (KDC) zu vermeiden, wodurch doppelte Anforderungen vermieden werden.

Wie NetScaler Kerberos für die Clientauthentifizierung implementiert

May 11, 2023

> **Wichtig**
>
> Die Kerberos/NTLM-Authentifizierung wird nur in der NetScaler 9.3 nCore-Version oder höher unterstützt und kann nur für die Authentifizierung, Autorisierung und Überwachung virtueller Server für das Verkehrsmanagement verwendet werden.

NetScaler behandelt die an der Kerberos-Authentifizierung beteiligten Komponenten wie folgt:

Wichtiges Vertriebszentrum (KDC)

In den Versionen von Windows 2000 Server oder höheren Versionen sind der Domänencontroller und das KDC Teil des Windows Server. Wenn der Windows Server in Betrieb ist und läuft, bedeutet dies, dass der Domänencontroller und das KDC konfiguriert sind. Das KDC ist auch der Active Directory-Server.

> **Hinweis**
>
> Alle Kerberos-Interaktionen werden mit dem Windows-Kerberos-Domänencontroller validiert.

Authentifizierungsservice und Protokollverhandlung

Eine NetScaler-Appliance unterstützt die Kerberos-Authentifizierung auf den virtuellen Authentifizierungs-, Autorisierungs- und Auditing-Traffic-Management-Authentifizierungsservern. Wenn die Kerberos-Authentifizierung fehlschlägt, verwendet der NetScaler die NTLM-Authentifizierung.

Standardmäßig verwenden Windows 2000 Server und neuere Windows Server-Versionen Kerberos für die Authentifizierung, Autorisierung und Überwachung. Wenn Sie eine Authentifizierungsrichtlinie mit NEGOTIATE als Authentifizierungstyp erstellen, versucht NetScaler, das Kerberos-Protokoll für die Authentifizierung, Autorisierung und Überwachung zu verwenden. Wenn der Browser des Clients kein Kerberos-Ticket empfängt, verwendet der NetScaler die NTLM-Authentifizierung. Dieser Prozess wird als Verhandlung bezeichnet.

In einem der folgenden Fälle kann es vorkommen, dass der Client kein Kerberos-Ticket erhält:

- Kerberos wird auf dem Client nicht unterstützt.
- Kerberos ist auf dem Client nicht aktiviert.
- Der Client befindet sich in einer anderen Domäne als der des KDC.
- Das Access Directory auf dem KDC ist für den Client nicht zugänglich.

Für die Kerberos/NTLM-Authentifizierung verwendet der NetScaler nicht die Daten, die lokal auf der NetScaler-Appliance vorhanden sind.

Autorisierung

Der virtuelle Server für das Verkehrsmanagement kann ein virtueller Lastausgleichsserver oder ein virtueller Content-Switching-Server sein.

Auditing

Die NetScaler-Appliance unterstützt die Überwachung der Kerberos-Authentifizierung mit der folgenden Überwachungsprotokollierung:

- Vollständiges Prüfprotokoll der Aktivitäten der Endnutzer im Verkehrsmanagement
- SYSLOG und leistungsstarkes TCP-Logging
- Vollständiges Prüfprotokoll der Systemadministratoren
- Alle Systemereignisse
- Skriptfähiges Protokollformat

Unterstützte Umgebung

Die Kerberos-Authentifizierung benötigt keine spezielle Umgebung auf dem NetScaler. Der Client (Browser) muss die Kerberos-Authentifizierung unterstützen.

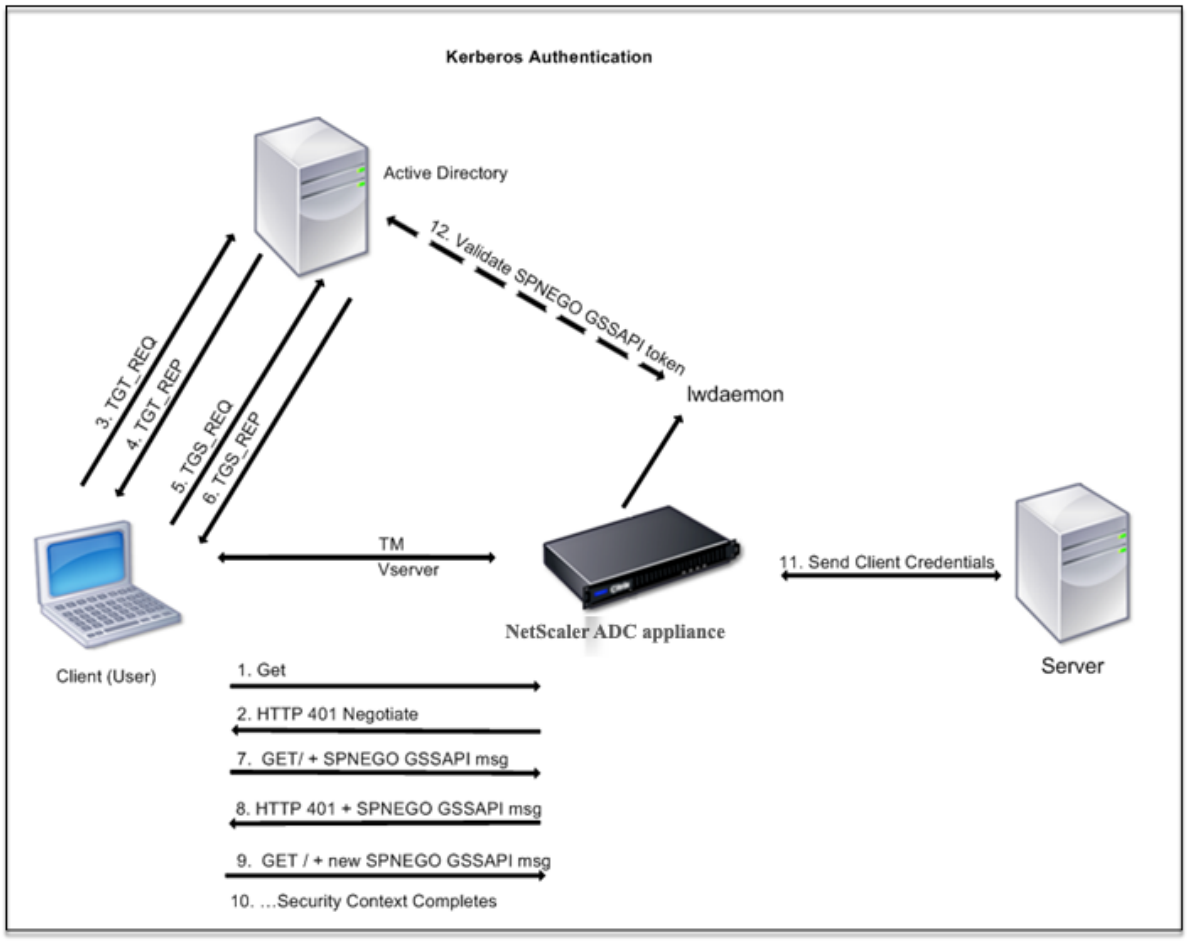
Hohe Verfügbarkeit

In einem Hochverfügbarkeits-Setup tritt nur der aktive NetScaler der Domäne bei. Im Falle eines Failovers verbindet der NetScaler lwagent-Daemon die sekundäre NetScaler-Appliance mit der Domäne. Für diese Funktion ist keine spezielle Konfiguration erforderlich.

Kerberos-Authentifizierungsprozess

Die folgende Abbildung zeigt einen typischen Prozess für die Kerberos-Authentifizierung in der NetScaler-Umgebung.

Abbildung 1. Kerberos-Authentifizierungsprozess auf NetScaler



Die Kerberos-Authentifizierung erfolgt in den folgenden Phasen:

Der Client authentifiziert sich beim KDC

1. Die NetScaler-Appliance empfängt eine Anfrage von einem Client.
2. Der virtuelle Server für das Verkehrsmanagement (Load Balancing oder Content Switching) auf der NetScaler-Appliance sendet eine Anfrage an den Client.
3. Um auf die Herausforderung zu antworten, erhält der Kunde ein Kerberos-Ticket.
   - Der Client sendet dem Authentifizierungsserver des KDC eine Anfrage für ein Ticket zur Ticketgewährung (TGT) und empfängt das TGT. (Siehe 3, 4 in der Abbildung, Kerberos-Authentifizierungsprozess.)
   - Der Client sendet das TGT an den Ticket Granting Server des KDC und erhält ein Kerberos-Ticket. (Siehe 5, 6 in der Abbildung, Kerberos-Authentifizierungsprozess.)

> **Hinweis**
>
> Der obige Authentifizierungsprozess ist nicht erforderlich, wenn der Client bereits über ein

> Kerberos-Ticket verfügt, dessen Gültigkeitsdauer noch nicht abgelaufen ist. Darüber hinaus erhalten Clients wie Web Services, .NET oder J2EE, die SPNEGO unterstützen, ein Kerberos-Ticket für den Zielserver, erstellen ein SPNEGO-Token und fügen das Token in den HTTP-Header ein, wenn sie eine HTTP-Anfrage senden. Sie durchlaufen den Client-Authentifizierungsprozess nicht.

Der Kunde fordert einen Service an.

1. Der Client sendet das Kerberos-Ticket, das das SPNEGO-Token und die HTTP-Anfrage enthält, an den virtuellen Traffic Management-Server auf dem NetScaler. Das SPNEGO-Token verfügt über die notwendigen GSSAPI-Daten.
2. Die NetScaler-Appliance stellt einen Sicherheitskontext zwischen dem Client und dem NetScaler her. Wenn der NetScaler die im Kerberos-Ticket bereitgestellten Daten nicht akzeptieren kann, wird der Client aufgefordert, ein anderes Ticket zu erhalten. Dieser Zyklus wiederholt sich, bis die GSSAPI-Daten akzeptabel sind und der Sicherheitskontext eingerichtet ist. Der virtuelle Traffic Management-Server auf dem NetScaler fungiert als HTTP-Proxy zwischen dem Client und dem physischen Server.

Die NetScaler-Appliance schließt die Authentifizierung ab.

1. Nachdem der Sicherheitskontext abgeschlossen ist, validiert der virtuelle Server für das Verkehrsmanagement das SPNEGO-Token.
2. Aus dem gültigen SPNEGO-Token extrahiert der virtuelle Server die Benutzer-ID und die GSS-Anmeldeinformationen und übergibt sie an den Authentifizierungsdaemon.
3. Eine erfolgreiche Authentifizierung schließt die Kerberos-Authentifizierung ab.

Konfigurieren der Kerberos-Authentifizierung auf der NetScaler-Appliance

May 12, 2023

In diesem Thema werden ausführliche Schritte zum Konfigurieren der Kerberos-Authentifizierung auf der NetScaler-Appliance mithilfe der CLI und der GUI beschrieben.

Konfigurieren der Kerberos-Authentifizierung auf der CLI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion, um die Authentifizierung von Datenverkehr auf der Appliance

   ns-cli-prompt **ns-funktion aktivieren** AAA

2. Fügen Sie die Keytab-Datei der NetScaler-Appliance hinzu. Eine Keytab-Datei ist erforderlich, um das während der Kerberos-Authentifizierung vom Client erhaltene Geheimnis zu entschlüsseln. Eine einzelne Keytab-Datei enthält Authentifizierungsdetails für alle Dienste, die an den virtuellen Verkehrsverwaltungsserver auf der NetScaler-Appliance gebunden sind.

   Generieren Sie zuerst die Keytab-Datei auf dem Active Directory-Server und übertragen Sie sie dann auf die NetScaler-Appliance.

   - Melden Sie sich mit dem folgenden Befehl beim Active Directory-Server an und fügen Sie einen Benutzer für die Kerberos-Authentifizierung hinzu.

     ```
     1  net user <username> <password> /add
     ```

     Hinweis

     Stellen Sie im Abschnitt **Benutzereigenschaften** sicher, dass die Option “Kennwort bei der nächsten Anmeldung ändern” nicht ausgewählt ist und die Option “Kennwort läuft nicht ab” ausgewählt ist.

   - Ordnen Sie den HTTP-Dienst dem obigen Benutzer zu und exportieren Sie die Keytab-Datei. Führen Sie beispielsweise den folgenden Befehl auf dem Active Directory-Server aus:

     ```
     1  ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM
           /pass <user password> /mapuser newacp\\dummy /ptype KRB5\
           _NT\_PRINCIPAL
     ```

     Hinweis

     Sie können mehr als einen Dienst zuordnen, wenn eine Authentifizierung für mehr als einen Dienst erforderlich ist. Wenn Sie weitere Dienste zuordnen möchten, wiederholen Sie den obigen Befehl für jeden Dienst. Sie können denselben Namen oder unterschiedliche Namen für die Ausgabedatei angeben.

   - Übertragen Sie die Keytab-Datei mit dem Unix-Befehl **ftp** oder einem anderen Dateiübertragungsprogramm Ihrer Wahl auf die NetScaler-Appliance. Laden Sie die Keytab-Datei in das Verzeichnis /nsconfig/krb/auf die NetScaler-Appliance hoch.

3. Die NetScaler-Appliance muss die IP-Adresse des Domänencontrollers aus dem vollqualifizierten Domänennamen (FQDN) beziehen. Citrix empfiehlt daher, den NetScaler mit einem DNS-Server zu konfigurieren.

   ns-cli-prompt> **add dns nameserver** <ip-address>

> **Hinweis**
>
> Alternativ können Sie statische Hosteinträge hinzufügen oder andere Mittel verwenden, damit die NetScaler-Appliance den FQDN-Namen des Domänencontrollers in eine IP-Adresse auflösen kann.

4. Konfigurieren Sie die Authentifizierungsaktion und ordnen Sie sie anschließend einer Authentifizierungsrichtlinie zu.

   - Konfigurieren Sie die Aushandlungsaktion.

     ns-cli-prompt> **add authentication negotiateAction** <name> -domain <domain name> -domainUser <domain user name> -domainUserPasswd <domain user password> -defaultAuthenticationGroup <default authentication group> -keytab <string> -NTLMPath <string>

     Hinweis: Wechseln Sie für die Konfiguration von Domänenbenutzern und Domänennamen zum Client und verwenden Sie den Befehl klist wie im folgenden Beispiel gezeigt:

     Client: username @ AAA.LOCAL

     Server: HTTP/onprem_idp.aaa.local @ AAA.LOCAL

     add authentication negotiateAction <name> -domain -domainUser <HTTP/onprem_idp.aaa.local>

   - Konfigurieren Sie die Verhandlungsrichtlinie, und ordnen Sie die Verhandlungsaktion dieser Richtlinie zu.

     ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Erstellen Sie einen virtuellen Authentifizierungsserver und verknüpfen Sie die Verhandlungsrichtlinie damit.

   - Erstellen Sie einen virtuellen Authentifizierungsserver.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>

   - Binden Sie die Aushandlungsrichtlinie an den virtuellen Authentifizierungsserver.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>

6. Verknüpfen Sie den virtuellen Authentifizierungsserver mit dem virtuellen Server der Verkehrsverwaltung (Load Balancing oder Content Switching).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

> **Hinweis**
>
> Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen, indem Sie Folgendes tun:
   - Greifen Sie mit dem FQDN auf den virtuellen Server zur Datenverkehrsverwaltung zu. Beispiel: Sample
   - Zeigen Sie die Details der Sitzung auf der CLI an.

     ns-cli-prompt> **show aaa session**

Konfigurieren der Kerberos-Authentifizierung auf der GUI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

   Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Grundfunktionen konfigurieren** und aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

2. Fügen Sie die Keytab-Datei hinzu, wie in Schritt 2 des oben genannten CLI-Verfahrens beschrieben.

3. Fügen Sie einen DNS-Server hinzu.

   Navigieren Sie zu **Traffic Management > DNS > Nameserver**, und geben Sie die IP-Adresse für den DNS-Server an.

4. Konfigurieren Sie die Aktion und Richtlinie **Aushandeln** .

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**, und erstellen Sie eine Richtlinie mit **Aushandeln** als Aktionstyp. Klicken Sie auf **HINZUFÜGEN**, um einen neuen Authentifizierungsverhandlungsserver zu erstellen, oder klicken Sie auf **Bearbeiten**, um die vorhandenen Details zu konfigur

5. Binden Sie die Aushandlungsrichtlinie an den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**, und verknüpfen **Sie die Aushandlungsrichtlinie** mit dem virtuellen Authentifizierungsserver.

6. Verknüpfen Sie den virtuellen Authentifizierungsserver mit dem virtuellen Server der Verkehrsverwaltung (Load Balancing oder Content Switching).

   Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und geben Sie die entsprechenden Authentifizierungseinstellungen an.

   > **Hinweis**
   >
   > Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen wie in Schritt 7 der oben genannten CLI-Prozedur beschrieben.

Kerberos-Authentifizierung auf einem Client konfigurieren

May 11, 2023

Die Kerberos-Unterstützung muss im Browser konfiguriert sein, um Kerberos für die Authentifizierung verwenden zu können. Sie können jeden Kerberos-kompatiblen Browser verwenden. Es folgen Anweisungen zur Konfiguration der Kerberos-Unterstützung in Internet Explorer und Mozilla Firefox. Informationen zu anderen Browsern finden Sie in der Dokumentation des Browsers.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Tools** die Option **Internetoptionen**aus.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Lokales Intranet**und dann auf **Websites.**
3. Vergewissern Sie sich, dass im Dialogfeld **Lokales Intranet** die Option Intranet-Netzwerk automatisch erkennen ausgewählt ist, und klicken Sie dann auf **Erweitert.**
4. Fügen Sie im Dialogfeld **Lokales Intranet** die Websites der Domänen des virtuellen Traffic-Management-Servers auf der NetScaler-Appliance hinzu. Die angegebenen Sites werden zu lokalen Intranetsites.
5. Klicken Sie auf **Schließen** oder **OK**, um die Dialogfelder zu schließen.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Vergewissern Sie sich, dass Kerberos auf Ihrem Computer ordnungsgemäß konfiguriert ist.
2. Geben Sie about:config in die URL-Leiste ein.
3. Geben Sie in das Textfeld Filter network.negotiate ein.
4. Ändern Sie network.negotiate-auth.delegation-uris in die Domain, die Sie hinzufügen möchten.
5. Ändern Sie network.negotiate-auth.trusted-uris in die Domain, die Sie hinzufügen möchten.

> **Hinweis:** Wenn Sie Windows verwenden, müssen Sie auch sspi in das Filtertextfeld eingeben und die Option network.auth.use-sspi in False ändern.

Offload der Kerberos-Authentifizierung von physischen Servern

June 2, 2023

Die NetScaler-Appliance kann Authentifizierungsaufgaben von Servern ausladen. Anstatt dass die physischen Server die Anforderungen von Clients authentifizieren, authentifiziert der NetScaler alle Clientanforderungen, bevor er sie an einen der an ihn gebundenen physischen Server weiterleitet. Die Benutzerauthentifizierung basiert auf Active Directory-Token.

Es gibt keine Authentifizierung zwischen dem NetScaler und dem physischen Server, und der Authentifizierungs-Offload ist für die Endbenutzer transparent. Nach der ersten Anmeldung an einem Windows-Computer muss der Endbenutzer keine zusätzlichen Authentifizierungsinformationen in ein Popup oder auf einer Anmeldeseite eingeben.

In der aktuellen Version der NetScaler-Appliance ist die Kerberos-Authentifizierung nur für die Authentifizierung, Autorisierung und Überwachung virtueller Traffic-Management-Server verfügbar. Die Kerberos-Authentifizierung wird für SSL VPN in der NetScaler Gateway Advanced Edition-Appliance oder für die NetScaler-Appliance-Verwaltung nicht unterstützt.

Die Kerberos-Authentifizierung erfordert eine Konfiguration auf der NetScaler-Appliance und in Client-Browsern.

So konfigurieren Sie die Kerberos-Authentifizierung auf der NetScaler-Appliance

> **Hinweis**
>
> Die in der folgenden Beispielkonfiguration verwendeten Kennwörter sind nur Beispiele und nicht die tatsächlichen Konfigurationskennwörter.

1. Erstellen Sie ein Benutzerkonto in Active Directory. Überprüfen Sie beim Erstellen eines Benutzerkontos die folgenden Optionen im Abschnitt Benutzereigenschaften:
   - Stellen Sie sicher, dass Sie die Option Kennwort bei der nächsten Anmeldung ändern nicht auswählen.
   - Achten Sie darauf, die Option Kennwort läuft nicht ab zu wählen.
2. Geben Sie auf dem AD-Server an der CLI-Eingabeaufforderung Folgendes ein:
   - ktpass -princ HTTP/kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass Citrix1 -out C:\kerbtabfile.txt

   > **Hinweis**
   >
   > Geben Sie den obigen Befehl unbedingt in einer einzigen Zeile ein. Die Ausgabe des obigen Befehls wird in die Datei C:\kerbtabfile.txt geschrieben.
3. Laden Sie die Datei kerbtabfile.txt mithilfe eines Secure Copy (SCP) -Clients in das Verzeichnis /etc der NetScaler-Appliance hoch.
4. Führen Sie den folgenden Befehl aus, um der NetScaler-Appliance einen DNS-Server hinzuzufügen.
   - add dns nameserver 1.2.3.4

   Die NetScaler-Appliance kann Kerberos-Anfragen ohne den DNS-Server nicht verarbeiten. Verwenden Sie unbedingt denselben DNS-Server, der in der Microsoft Windows-Domäne verwendet wird.

5. Wechseln Sie zur Befehlszeilenschnittstelle von NetScaler.
6. Führen Sie den folgenden Befehl aus, um einen Kerberos-Authentifizierungsserver zu erstellen:
   - Authentifizierung hinzufügen Aktion aushandeln KerberosServer - Domäne “crete.lab.net” -Domänenbenutzer kerbuser -DomainUserPasswd Citrix1 -keytab /var/mykcd.keytab

   > **Hinweis**
   >
   > Wenn keytab nicht verfügbar ist, können Sie die Parameter angeben: domain, domainUser und -DomainUserPasswd.

7. Führen Sie den folgenden Befehl aus, um eine Verhandlungsrichtlinie zu erstellen:
   - `add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200"KerberosServer<!--NeedCopy-->`
8. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu erstellen.
   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`
9. Führen Sie den folgenden Befehl aus, um die Kerberos-Richtlinie an den virtuellen Authentifizierungsserver zu binden:
   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`
10. Führen Sie den folgenden Befehl aus, um ein SSL-Zertifikat an den virtuellen Authentifizierungsserver zu binden. Sie können eines der Testzertifikate verwenden, das Sie über die GUI NetScaler-Appliance installieren können. Führen Sie den folgenden Befehl aus, um das ServerTestCert-Beispielzertifikat zu verwenden.
    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`
11. Erstellen Sie einen virtuellen HTTP-Lastausgleichsserver mit der IP-Adresse 192.168.17.200.

    Stellen Sie sicher, dass Sie über die Befehlszeilenschnittstelle für NetScaler 9.3-Versionen einen virtuellen Server erstellen, wenn diese älter als 9.3.47.8 sind.
12. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu konfigurieren:
    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`
13. Geben Sie den Hostnamen Example in die Adressleiste des Webbrowsers ein.

    Der Webbrowser zeigt ein Authentifizierungsdialogfeld an, da die Kerberos-Authentifizierung nicht im Browser eingerichtet ist.

> **Hinweis**
>
> Die Kerberos-Authentifizierung erfordert eine bestimmte Konfiguration auf dem Client. Stellen Sie sicher, dass der Client den Hostnamen auflösen kann, was dazu führt, dass der Webbrowser eine Verbindung zu einem virtuellen HTTP-Server herstellt.

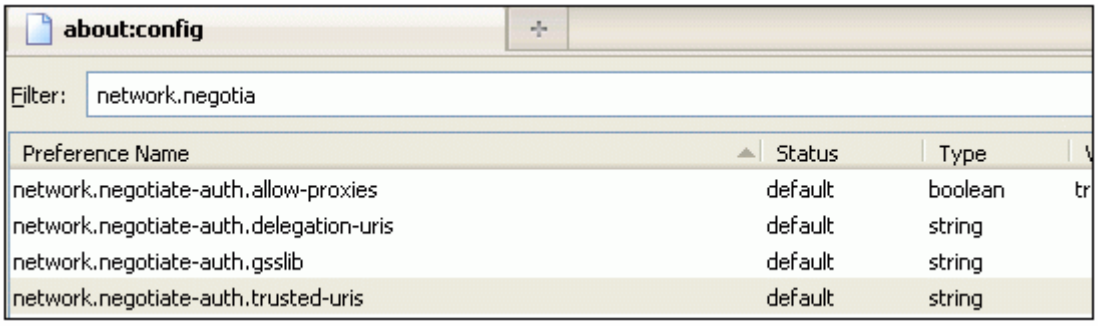
14. Konfigurieren Sie Kerberos im Webbrowser des Clientcomputers.
    - Informationen zur Konfiguration in Internet Explorer finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
    - Informationen zur Konfiguration in Mozilla Firefox finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
15. Überprüfen Sie, ob Sie ohne Authentifizierung auf den physischen Backend-Server zugreifen können.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Extras** die Option **Internetoptionen**.
2. Aktivieren Sie die Registerkarte **Sicherheit**.
3. Wählen Sie **Lokales Intranet** aus dem Abschnitt Wählen Sie eine Zone aus, um die Änderung der Sicherheitseinstellungen anzuzeigen.
4. Klicken Sie auf **Sites**.
5. Klicken Sie auf **Erweitert**.
6. Geben Sie die URL an, Beispiel, und klicken Sie auf **Hinzufügen**.
7. Starten Sie **Internet Explorer**neu.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Geben Sie about:config in die Adressleiste des Browsers ein.
2. Klicken Sie auf den Haftungsausschluss für Warnungen.
3. Geben Sie **network.negotiate-auth.trusted-uris** in das Feld **Filter** ein.
4. Doppelklicken Sie auf **Network.negotiate-auth.Trusted-URIS.** Ein Beispielbildschirm wird unten gezeigt.



5. Geben Sie im Dialogfeld Zeichenfolgenwert eingeben www.crete.lab.net an.
6. Starten Sie Firefox neu.

Single-Sign-On-Typen

May 11, 2023

Die NetScaler-Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen unterstützen die folgenden Single Sign-On-Typen.

- **NetScaler Kerberos Single Sign-On:** NetScaler Appliances unterstützen jetzt Single Sign-On (SSO) mithilfe des Kerberos 5-Protokolls. Benutzer melden sich bei einem Proxy an, dem Application Delivery Controller (ADC), der dann Zugriff auf geschützte Ressourcen ermöglicht. Weitere Informationen finden Sie unter NetScaler Kerberos Single Sign-On.
- **SSO für Basic-, Digest- und NTLM-Authentifizierung:** Die Single Sign-On (SSO) -Konfiguration in NetScaler und NetScaler Gateway kann auf globaler Ebene und auch pro Traffic-Ebene aktiviert werden. Standardmäßig ist die SSO-Konfiguration AUS und ein Administrator kann SSO pro Datenverkehr oder global aktivieren. Aus Sicherheitsgründen empfiehlt Citrix Administratoren, SSO global auszuschalten und pro Datenverkehr zu aktivieren. Diese Verbesserung soll die SSO-Konfiguration sicherer machen, indem bestimmte Arten von SSO-Methoden global deaktiviert werden. Weitere Informationen finden Sie unter SSO für Basic-, Digest- und NTLM-Authentifizierung.

NetScaler Kerberos Single Sign-On

May 11, 2023

NetScaler-Appliances unterstützen jetzt Single Sign-On (SSO) mithilfe des Kerberos 5-Protokolls. Benutzer melden sich bei einem Proxy an, dem Application Delivery Controller (ADC), der dann Zugriff auf geschützte Ressourcen ermöglicht.

Die NetScaler Kerberos SSO-Implementierung erfordert das Passwort des Benutzers für SSO-Methoden, die auf der Basis-, NTLM- oder formularbasierten Authentifizierung basieren. Das Benutzerkennwort ist für Kerberos SSO nicht erforderlich. Wenn Kerberos SSO fehlschlägt und die NetScaler-Appliance das Passwort des Benutzers hat, verwendet sie das Passwort, um NTLM-SSO zu versuchen.

Wenn das Passwort des Benutzers verfügbar ist, das KCD-Konto mit einem Realm konfiguriert ist und keine delegierten Benutzerinformationen vorhanden sind, gibt sich die Citrix AD Kerberos SSO-Engine für den Benutzer aus, um Zugriff auf autorisierte Ressourcen zu erhalten. Identitätswechsel wird auch als uneingeschränkte Delegierung bezeichnet.

Die NetScaler Kerberos SSO-Engine kann auch so konfiguriert werden, dass sie ein delegiertes Konto verwendet, um im Namen des Benutzers Zugriff auf geschützte Ressourcen zu erhalten. Für diese Konfiguration sind delegierte Benutzeranmeldeinformationen, ein Keytab oder ein delegiertes Benutzerzertifikat und ein entsprechendes CA-Zertifikat erforderlich. Eine Konfiguration, die ein delegiertes Konto verwendet, wird als eingeschränkte Delegierung bezeichnet.

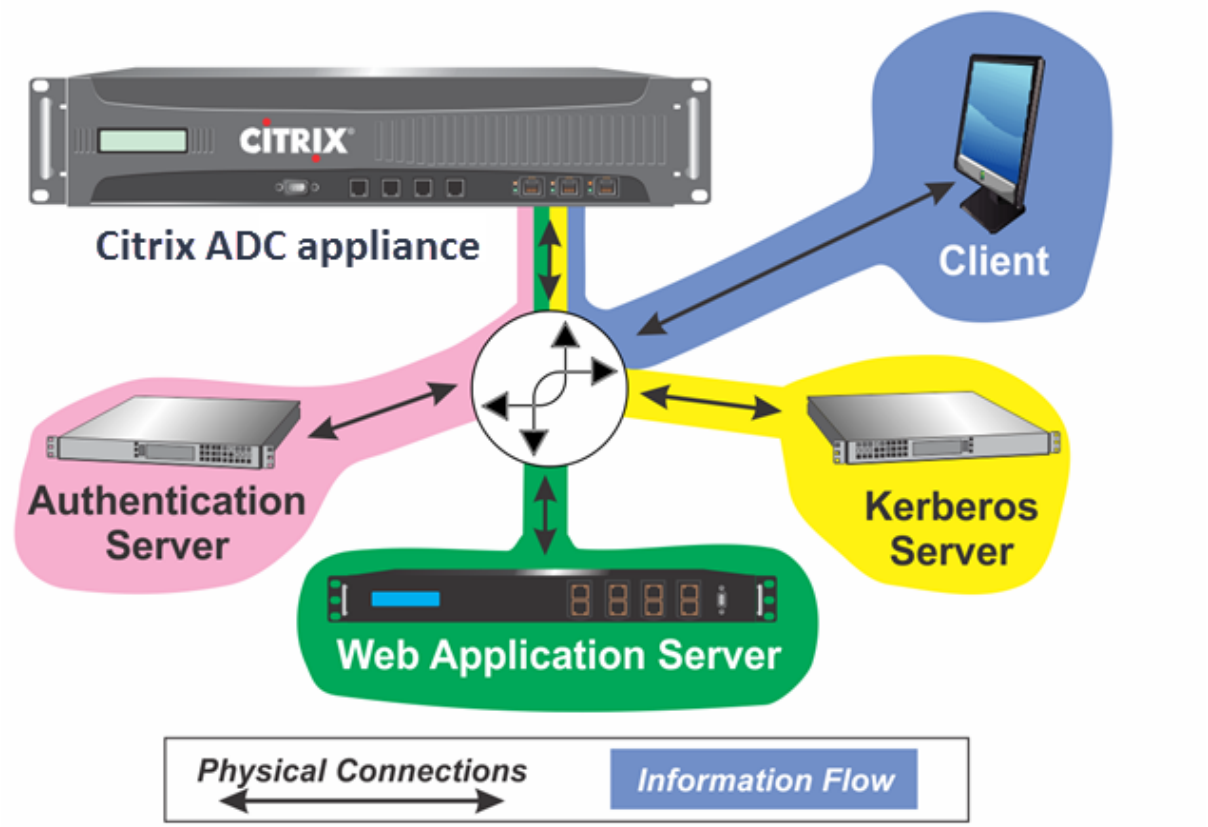
Ein Überblick über NetScaler Kerberos SSO

May 11, 2023

Um die NetScaler Kerberos SSO-Funktion verwenden zu können, authentifizieren sich Benutzer zunächst bei Kerberos oder einem unterstützten Authentifizierungsserver eines Drittanbieters. Nach der Authentifizierung fordert der Benutzer Zugriff auf eine geschützte Webanwendung an. Der Webserver antwortet mit einer Aufforderung zum Nachweis, dass der Benutzer berechtigt ist, auf diese Webanwendung zuzugreifen. Der Browser des Benutzers kontaktiert den Kerberos-Server, der überprüft, ob der Benutzer für den Zugriff auf diese Ressource autorisiert ist, und stellt dem Browser des Benutzers dann ein Serviceticket zur Verfügung, das den Nachweis liefert. Der Browser sendet die Anfrage des Benutzers mit dem angehängten Serviceticket erneut an den Webanwendungsserver. Der Webanwendungsserver überprüft das Serviceticket und ermöglicht dem Benutzer dann den Zugriff auf die Anwendung.

Das Verkehrsmanagement für Authentifizierung, Autorisierung und Überwachung implementiert diesen Prozess, wie in der folgenden Abbildung dargestellt. Das Diagramm veranschaulicht den Informationsfluss durch die NetScaler-Appliance und die Verwaltung des Authentifizierungs-, Autorisierungs- und Audit-Traffic-Managements in einem sicheren Netzwerk mit LDAP-Authentifizierung und Kerberos-Autorisierung. Umgebungen für Authentifizierung, Autorisierung und Überwachung des Verkehrsmanagements, die andere Authentifizierungstypen verwenden, haben im Wesentlichen denselben Informationsfluss, obwohl sie sich in einigen Details unterscheiden können.

Abbildung 1. Ein sicheres Netzwerk mit LDAP und Kerberos



Das Authentifizierungs-, Autorisierungs- und Auditing-Verkehrsmanagement mit Authentifizierung und Autorisierung in einer Kerberos-Umgebung erfordert, dass die folgenden Aktionen ausgeführt werden.

1. Der Client sendet eine Anforderung für eine Ressource an den virtuellen Traffic Management-Server auf der NetScaler-Appliance.
2. Der virtuelle Server für das Verkehrsmanagement leitet die Anfrage an den virtuellen Authentifizierungsserver weiter, der den Client authentifiziert und die Anfrage dann an den virtuellen Server für die Verkehrsverwaltung zurückleitet.
3. Der virtuelle Server für das Verkehrsmanagement sendet die Anfrage des Clients an den Webanwendungsserver.
4. Der Webanwendungsserver antwortet auf den virtuellen Traffic Management-Server mit einer 401-Meldung, die die Kerberos-Authentifizierung anfordert. Falls der Client Kerberos nicht unterstützt, wird auf die NTLM-Authentifizierung zurückgegriffen.
5. Der virtuelle Server für das Verkehrsmanagement kontaktiert den Kerberos-SSO-Daemon.
6. Der Kerberos-SSO-Daemon kontaktiert den Kerberos-Server und erhält ein Ticket Granting Ticket (TGT), mit dem er Servicetickets anfordern kann, die den Zugriff auf geschützte Anwendungen autorisieren.
7. Der Kerberos-SSO-Daemon ruft ein Serviceticket für den Benutzer ab und sendet dieses Ticket an den virtuellen Traffic Management-Server.

8. Der virtuelle Server für das Verkehrsmanagement fügt das Ticket an die erste Anfrage des Benutzers an und sendet die geänderte Anfrage an den Webanwendungsserver zurück.
9. Der Webanwendungsserver antwortet mit einer 200-OK-Meldung.

Diese Schritte sind für den Client transparent, der lediglich eine Anfrage sendet und die angeforderte Ressource empfängt.

Integration von NetScaler Kerberos SSO mit Authentifizierungsmethoden

Alle Authentifizierungsmechanismen für Authentifizierung, Autorisierung und Überwachung des Verkehrsmanagements unterstützen NetScaler Kerberos SSO. Das Verkehrsmanagement für Authentifizierung, Autorisierung und Überwachung unterstützt den Kerberos-SSO-Mechanismus mit den Kerberos-, CAC- (Smart Card) und SAML-Authentifizierungsmechanismen mit jeder Form der Client-Authentifizierung an der NetScaler-Appliance. Es unterstützt auch die SSO-Mechanismen HTTP-Basic, HTTP-Digest, Forms-based und NTLM (Versionen 1 und 2), wenn der Client entweder die HTTP-Basic- oder die formsbasierte Authentifizierung verwendet, um sich bei der NetScaler-Appliance anzumelden.

Die folgende Tabelle zeigt jede unterstützte clientseitige Authentifizierungsmethode und die unterstützte serverseitige Authentifizierungsmethode für diese clientseitige Methode.

Tabelle 1. Unterstützte Authentifizierungsmethoden

	Grundlagen/Übersicht/NTLM	Eingeschränkte Kerberos-Delegierung	Identitätswechsel
CAC (Smartcard): auf der SSL/T LS-Schicht		X	X
Formularbasiert (LDAP/RADIUS/TACACS)	X	X	X
HTTP-Grundlagen (LDAP/RADIUS/TACACS)	X	X	X
Kerberos		X	
NT LM v1/v2		X	X
SAML		X	
SAML Zwei-Faktor	X	X	X
Zertifikat Two-Factor	X	X	X

NetScaler SSO einrichten

May 11, 2023

Sie können NetScaler SSO so konfigurieren, dass es auf eine von zwei Arten funktioniert: durch Identitätswechsel oder durch Delegation. SSO durch Identitätswechsel ist eine einfachere Konfiguration als SSO durch Delegierung und ist daher vorzuziehen, wenn Ihre Konfiguration dies zulässt. Um NetScaler SSO durch Identitätswechsel zu konfigurieren, müssen Sie über den Benutzernamen und das Kennwort des Benutzers verfügen.

Um NetScaler SSO durch Delegierung zu konfigurieren, müssen Sie über die Anmeldeinformationen des delegierten Benutzers in einem der folgenden Formate verfügen: den Benutzernamen und das Kennwort des Benutzers, die Keytab-Konfiguration, die den Benutzernamen und ein verschlüsseltes Kennwort enthält, oder das delegierte Benutzerzertifikat und das entsprechende CA-Zertifikat.

Voraussetzungen für die Konfiguration von NetScaler SSO

Bevor Sie ein NetScaler SSO konfigurieren, muss Ihre NetScaler Appliance vollständig konfiguriert sein, um den Datenverkehr zu und die Authentifizierung für Ihre Webanwendungsserver zu verwalten. Daher müssen Sie entweder Load Balancing oder Content Switching und dann Authentifizierung, Autorisierung und Überwachung für diese Webanwendungsserver konfigurieren. Sie müssen auch das Routing zwischen der Appliance, Ihrem LDAP-Server und Ihrem Kerberos-Server überprüfen.

Wenn Ihr Netzwerk noch nicht auf diese Weise konfiguriert ist, führen Sie die folgenden Konfigurationsaufgaben aus:

- Konfigurieren Sie einen Server und einen Dienst für jeden Webanwendungsserver.
- Konfigurieren Sie einen virtuellen Traffic Management-Server für die Verarbeitung des Datenverkehrs zu und von Ihrem Webanwendungsserver.

Im Folgenden finden Sie kurze Anweisungen und Beispiele für die Ausführung dieser Aufgaben über die NetScaler Befehlszeile. Weitere Unterstützung finden Sie unter Einrichten eines virtuellen Authentifizierungsservers.

> **Hinweis**
>
> Ab NetScaler 13.1 Version wird die Traversierung zwischen Stammdomäne und Baumdomäne während der Kerberos-SSO-Authentifizierung für Backend-Server von der NetScaler-Appliance unterstützt.

So erstellen Sie einen Server und einen Dienst mit der CLI

Damit NetScaler SSO ein TGS (Service-Ticket) für einen Dienst abrufen kann, muss entweder der FQDN, der der Serverentität auf der NetScaler-Appliance zugewiesen ist, mit dem FQDN des Weban-

wendungsservers übereinstimmen, oder der Name der Serverentität muss mit dem NetBIOS-Namen des Webanwendungsservers übereinstimmen. Sie können einen der folgenden Ansätze wählen:

- Konfigurieren Sie die NetScaler-Serverentität, indem Sie den FQDN des Webanwendungsservers angeben.
- Konfigurieren Sie die NetScaler-Serverentität, indem Sie die IP-Adresse des Webanwendungsservers angeben, und weisen Sie der Serverentität denselben Namen wie den NetBIOS-Namen des Webanwendungsservers zu.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 -  add server name <serverFQDN>
2
3 -  add service name serverName serviceType port
4 <!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **serverName**. Ein Name für die NetScaler-Appliance, der verwendet werden soll, um auf diesen Server zu verweisen.
- **serverFQDN**. Der FQDN des Servers. Wenn dem Server keine Domäne zugewiesen ist, verwenden Sie die IP-Adresse des Servers und stellen Sie sicher, dass der Name der Servereinheit mit dem NetBIOS-Namen des Webanwendungsservers übereinstimmt.
- **serviceName**. Ein Name für die NetScaler-Appliance, der verwendet werden soll, um auf diesen Dienst zu verweisen.
- **Typ**. Das vom Dienst verwendete Protokoll, entweder HTTP oder MSSQLSVC.
- **Port**. Der Port, auf dem der Dienst lauscht. HTTP-Dienste hören normalerweise auf Port 80. Sichere HTTPS-Dienste hören normalerweise auf Port 443.

Beispiel:

In den folgenden Beispielen werden Server- und Diensteinträge auf der NetScaler-Appliance für den Webanwendungsserver was1.example.com hinzugefügt. Das erste Beispiel verwendet den FQDN des Webanwendungsservers; das zweite verwendet die IP-Adresse.

Um den Server und den Dienst mithilfe des Webanwendungsservers FQDN, was1.example.com, hinzuzufügen, geben Sie die folgenden Befehle ein:

```
1 add server was1 was1.example.com
2 add service was1service was1 HTTP 80
3 <!--NeedCopy-->
```

Um den Server und den Dienst mithilfe der IP des Webanwendungsservers und des NetBIOS-Namens hinzuzufügen, wobei die IP des Webanwendungsservers 10.237.64.87 und der NetBIOS-Name WAS1 lautet, geben Sie die folgenden Befehle ein:


```
add server WAS1 10.237.64.87
add service was1service WAS1 HTTP 80
<!--NeedCopy-->
```

So erstellen Sie über die CLI einen virtuellen Traffic Management-Server

Der virtuelle Traffic Management-Server verwaltet den Datenverkehr zwischen dem Client und dem Webanwendungsserver. Sie können entweder einen Lastausgleich- oder einen virtuellen Content Switching-Server als Traffic Management-Server verwenden. Die SSO-Konfiguration ist für beide Typen gleich.

Um einen virtuellen Lastausgleichsserver zu erstellen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add lb vserver <vserverName> <type> <IP> <port>
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **vServerName —Ein Name**für die NetScaler-Appliance, der verwendet werden soll, um auf diesen virtuellen Server zu verweisen.
- **type**—Das vom Dienst verwendete Protokoll, entweder HTTP oder MSSQLSVC.
- **IP**—Die dem virtuellen Server zugewiesene IP-Adresse. Dies wäre normalerweise eine von IANA reservierte, nicht öffentliche IP-Adresse in Ihrem LAN.
- **port**—Der Port, auf dem der Dienst lauscht. HTTP-Dienste hören normalerweise auf Port 80. Sichere HTTPS-Dienste hören normalerweise auf Port 443.

Beispiel:

Um einen virtuellen Lastausgleichsserver namens tmvserver1 zu einer Konfiguration hinzuzufügen, die den HTTP-Verkehr auf Port 80 verwaltet, ihm eine LAN-IP-Adresse von 10.217.28.20 zuzuweisen und dann den virtuellen Lastausgleichsserver an den wasservice1-Dienst zu binden, geben Sie die folgenden Befehle ein:

```
add lb vserver tmvserver1 HTTP 10.217.28.20 80
bind lb vserver tmvserv1 wasservice1
<!--NeedCopy-->
```

So erstellen Sie über die CLI einen virtuellen Authentifizierungsserver

Der virtuelle Authentifizierungsserver verwaltet den Authentifizierungsverkehr zwischen dem Client und dem Authentifizierungsserver (LDAP). Um einen virtuellen Authentifizierungsserver zu erstellen, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:


```
add authentication vserver <authvserverName> SSL <IP> 443
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **AuthvServerName —Ein Name** für die NetScaler-Appliance, der verwendet werden soll, um auf diesen virtuellen Authentifizierungsserver zu verweisen. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann geändert werden, nachdem der virtuelle Authentifizierungsserver mithilfe des Befehls rename authentication vserver hinzugefügt wurde.
- **IP**—Die IP-Adresse, die dem virtuellen Authentifizierungsserver zugewiesen ist. Wie beim virtuellen Server für das Verkehrsmanagement wäre diese Adresse normalerweise eine IANA-reservierte, nicht öffentliche IP in Ihrem LAN.
- **domain**—Die Domäne, die dem virtuellen Server zugewiesen ist. Dies ist normalerweise die Domäne Ihres Netzwerks. Es ist üblich, wenn auch nicht erforderlich, die Domäne bei der Konfiguration des virtuellen Authentifizierungsservers in Großbuchstaben einzugeben.

Beispiel:

Um einen virtuellen Authentifizierungsserver namens authverver1 zu Ihrer Konfiguration hinzuzufügen und ihm die LAN-IP 10.217.28.21 und die Domäne EXAMPLE.COM zuzuweisen, geben Sie die folgenden Befehle ein:

```
add authentication vserver authvserver1 SSL 10.217.28.21 443
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Traffic Management-Server für die Verwendung eines Authentifizierungsprofils

Der virtuelle Authentifizierungsserver kann für die Authentifizierung für eine einzelne Domäne oder für mehrere Domänen konfiguriert werden. Wenn es für die Unterstützung der Authentifizierung für mehrere Domänen konfiguriert ist, müssen Sie auch die Domäne für NetScaler SSO angeben, indem Sie ein Authentifizierungsprofil erstellen und dann den virtuellen Server für die Verkehrsverwaltung für die Verwendung dieses Authentifizierungsprofils konfigurieren.

> **Hinweis**
>
> Der virtuelle Server für das Verkehrsmanagement kann entweder ein virtueller Lastausgleichsserver (lb) oder ein Content Switching (cs) sein. Bei den folgenden Anweisungen wird davon ausgegangen, dass Sie einen virtuellen Lastausgleichsserver verwenden. Um einen virtuellen Content Switching-Server zu konfigurieren, ersetzen

> Sie einfach set cs vserver durch set lb vserver. Das Verfahren ist ansonsten dasselbe.

Um das Authentifizierungsprofil zu erstellen und dann das Authentifizierungsprofil auf einem virtuellen Traffic Management-Server zu konfigurieren, geben Sie die folgenden Befehle ein:

```
-  add authentication authnProfile <authnProfileName> {
 -authvserverName <string> }
  {
 -authenticationHost <string> }
  {
 -authenticationDomain <string> }

-  set lb vserver \<vserverName\> -authnProfile <authnprofileName>
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **authnProfileName**— Ein Name für das Authentifizierungsprofil. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und muss aus einem bis einunddreißig alphanumerischen oder Bindestrichen (-), Punkt (.) Pfund (#), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstrichen bestehen.
- **AuthvServerName**—Der Name des virtuellen Authentifizierungsservers, den dieses Profil für die Authentifizierung verwendet.
- **AuthenticationHost**— Hostname des virtuellen Authentifizierungsservers.
- **AuthenticationDomain**— Domäne, für die NetScaler SSO die Authentifizierung verarbeitet. Erforderlich, wenn der virtuelle Authentifizierungsserver die Authentifizierung für mehr als eine Domäne durchführt, damit die richtige Domäne enthalten ist, wenn die NetScaler-Appliance das Cookie des virtuellen Servers für die Verkehrsverwaltung festlegt.

Beispiel:

Um ein Authentifizierungsprofil mit dem Namen AuthnProfile1 für die Authentifizierung der Domäne example.com zu erstellen und den virtuellen Lastausgleichsserver vserver1 für die Verwendung des Authentifizierungsprofils AuthnProfile1 zu konfigurieren, geben Sie die folgenden Befehle ein:

```
add authentication authnProfile authnProfile1 -authnvsName
    authvsesrver1
      -authenticationHost authvsesrver1 -authenticationDomain example.
         com
set lb vserver vserver1 -authnProfile authnProfile1
<!--NeedCopy-->
```


Single Sign-On konfigurieren

October 4, 2023

Das Konfigurieren von NetScaler Single Sign-On (SSO) für die Authentifizierung durch Identitätswechsel ist einfacher als die Konfiguration von SSO für die Authentifizierung durch Delegierung und ist daher vorzuziehen, wenn Ihre Konfiguration dies zulässt. Sie erstellen ein KCD-Konto. Sie können das Kennwort des Benutzers verwenden.

Wenn Sie das Kennwort des Benutzers nicht haben, können Sie NetScaler SSO so konfigurieren, dass es sich durch Delegierung authentifiziert. Obwohl die Delegierungsmethode komplexer ist als die Konfiguration von SSO für die Authentifizierung durch Identitätswechsel, bietet sie Flexibilität, da die Anmeldeinformationen eines Benutzers möglicherweise nicht unter allen Umständen für die NetScaler-Appliance verfügbar sind.

Für Identitätswechsel oder Delegierung müssen Sie auch die integrierte Authentifizierung auf dem Webanwendungsserver aktivieren.

Integrierte Authentifizierung auf dem Webanwendungsserver aktivieren

Um NetScaler Kerberos SSO auf jedem Webanwendungsserver einzurichten, den Kerberos SSO verwaltet, verwenden Sie die Konfigurationsoberfläche auf diesem Server, um den Server so zu konfigurieren, dass eine Authentifizierung erforderlich ist. Wählen Sie die Kerberos-Authentifizierung (Aushandeln) nach Präferenz aus, mit Fallback auf NTLM für Clients, die Kerberos nicht unterstützen.

Im Folgenden finden Sie Anweisungen zum Konfigurieren des Microsoft Internet Information Server (IIS), sodass eine Authentifizierung erforderlich ist. Wenn Ihr Webanwendungsserver eine andere Software als IIS verwendet, finden Sie Anweisungen in der Dokumentation zu dieser Webserver-Software.

So konfigurieren Sie Microsoft IIS für die Verwendung der integrierten Authentifizierung

1. Melden Sie sich beim IIS-Server an und öffnen Sie **Internet Information Services Manager.**
2. Wählen Sie die Website aus, für die Sie die integrierte Authentifizierung aktivieren möchten. Um die integrierte Authentifizierung für alle von IISM verwalteten IIS-Webserver zu aktivieren, konfigurieren Sie die Authentifizierungseinstellungen für die Standardwebsite. Um die integrierte Authentifizierung für einzelne Dienste (wie Exchange, Exadmin, ExchWeb und Public) zu ermöglichen, konfigurieren Sie diese Authentifizierungseinstellungen für jeden Dienst einzeln.
3. Öffnen Sie das **Eigenschaften-Dialogfeld** für die Standardwebsite oder für den einzelnen Dienst, und klicken Sie auf die Registerkarte **Verzeichnissicherheit** .
4. Wählen Sie neben **Authentifizierung** und **Zugriffssteuerung**die Option **Bearbeiten aus.**
5. Deaktivieren Sie den anonymen Zugriff.

6. Aktivieren Sie die integrierte Windows-Authentifizierung (nur). Durch die Aktivierung der integrierten Windows-Authentifizierung muss die Protokollaushandlung für den Webserver automatisch auf Negotiate (NTLM) festgelegt werden, wodurch die Kerberos-Authentifizierung mit Fallback auf NTLM für nicht Kerberos-fähige Geräte angegeben wird. Wenn diese Option nicht automatisch ausgewählt wird, setzen Sie die Protokollaushandlung manuell auf Aushandeln, NTLM.

Richten Sie SSO durch Identitätswechsel ein

Sie können das KCD-Konto für NetScaler SSO durch Identitätswechsel konfigurieren. In dieser Konfiguration erhält die NetScaler-Appliance den Benutzernamen und das Kennwort des Benutzers, wenn sich der Benutzer beim Authentifizierungsserver authentifiziert, und verwendet diese Anmeldeinformationen, um sich als Benutzer auszugeben, um ein Ticket Granting Ticket (TGT) zu erhalten. Wenn der Benutzername im UPN-Format vorliegt, bezieht die Appliance den Bereich des Benutzers von UPN. Andernfalls erhält es den Namen und den Bereich des Benutzers, indem es ihn aus der SSO-Domäne extrahiert, die bei der Erstauthentifizierung verwendet wurde, oder aus dem Sitzungsprofil.

> **Hinweis**
>
> Sie können keinen Benutzernamen mit Domäne hinzufügen, wenn der Benutzername bereits ohne Domäne hinzugefügt wurde. Wenn der Benutzername mit Domäne zuerst hinzugefügt wird, gefolgt von demselben Benutzernamen ohne Domäne, fügt die NetScaler-Appliance den Benutzernamen zur Benutzerliste hinzu.

Bei der Konfiguration des KCD-Kontos müssen Sie den Realm-Parameter auf den Bereich des Dienstes festlegen, auf den der Benutzer zugreift. Derselbe Bereich wird auch als Bereich des Benutzers verwendet, wenn der Bereich des Benutzers nicht durch Authentifizierung mit der NetScaler-Appliance oder aus dem Sitzungsprofil abgerufen werden kann.

So erstellen Sie das KCD-Konto für SSO durch Identitätswechsel mit einem Kennwort

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add aaa kcdaccount <accountname> -realmStr <realm>

<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **accountname**. Der KCD-Kontoname.
- **realm**. Die Domäne, die dem NetScaler SSO zugewiesen ist.

Beispiel

Um ein KCD-Konto mit dem Namen kcdccount1 hinzuzufügen und das Schlüsselregister kcdvserver.keytab zu verwenden, geben Sie den folgenden Befehl ein:

```
add aaa kcdAccount kcdaccount1 -keytab kcdvserver.keytab

<!--NeedCopy-->
```

Informationen zur Konfiguration des Kerberos-Identitätswechsels über die NetScaler-GUI finden Sie unter NetScaler-Unterstützung.

SSO durch Delegierung konfigurieren

Um SSO nach Delegation zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- Wenn Sie die Delegierung durch ein delegiertes Benutzerzertifikat konfigurieren, installieren Sie die entsprechenden CA-Zertifikate auf der NetScaler-Appliance und fügen Sie sie der NetScaler-Konfiguration hinzu.
- Erstellen Sie das KCD-Konto auf der Appliance. Die Appliance verwendet dieses Konto, um Servicetickets für Ihre geschützten Anwendungen zu erhalten.
- Konfigurieren Sie den Active Directory-Server.

> **Hinweis**
>
> Weitere Informationen zum Erstellen eines KCD-Kontos und zum Konfigurieren auf der NetScaler-Appliance finden Sie in den folgenden Themen:
>
> - Authentifizierung, Autorisierung und Audits mit Kerberos/NTLM
> - Wie NetScaler Kerberos für die Clientauthentifizierung implementiert
> - Konfigurieren der Kerberos-Authentifizierung auf der NetScaler-Appliance

Installieren des Client-CA-Zertifikats auf der NetScaler-Appliance

Wenn Sie das NetScaler SSO mit einem Clientzertifikat konfigurieren, müssen Sie das entsprechende CA-Zertifikat für die Clientzertifikatdomäne (das Clientzertifizierungsstellenzertifikat) auf die NetScaler-Appliance kopieren und dann das CA-Zertifikat installieren. Verwenden Sie zum Kopieren des Clientzertifizierungsstellenzertifikats das Dateiübertragungsprogramm Ihrer Wahl, um das Zertifikat und die Privatschlüsseldatei auf die NetScaler-Appliance zu übertragen und die Dateien in /nsconfig/ssl zu speichern.

So installieren Sie das Client-CA-Zertifikat auf der NetScaler-Appliance

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add ssl certKey <certkeyName> -cert <cert> [(-key <key> [-password]) |
    -fipsKey <fipsKey>][-inform ( DER | PEM )][-expiryMonitor ( ENABLED
    | DISABLED | UNSET ) [-notificationPeriod <positive_integer>]] [-
    bundle ( YES | NO )]

<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **certkeyName**. Ein Name für das Client-CA-Zertifikat. Muss mit einem alphanumerischen ASCII-Zeichen oder einem Unterstrich (_) beginnen und muss aus einem bis einunddreißig Zeichen bestehen. Zulässige Zeichen sind alphanumerische ASCII-Zeichen, Unterstrich, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleichheitszeichen (=) und Bindestrich (-). Kann nicht geändert werden, nachdem das Zertifikat-Schlüsselpaar erstellt wurde. Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Zertifikat” oder “mein Zertifikat”).
- **cert**. Vollständiger Pfadname und Dateiname der X509-Zertifikatsdatei, die zur Bildung des Zertifikatsschlüsselpaars verwendet wurde. Die Zertifikatsdatei muss auf der NetScaler-Appliance im Verzeichnis /nsconfig/ssl/ gespeichert werden.
- **Schlüssel**. Vollständiger Pfadname und Dateiname der Datei, die den privaten Schlüssel zur X509-Zertifikatsdatei enthält. Die Schlüsseldatei muss auf der NetScaler-Appliance im Verzeichnis /nsconfig/ssl/ gespeichert werden.
- **password**. Wenn ein privater Schlüssel angegeben ist, wird die Passphrase verwendet, um den privaten Schlüssel zu verschlüsseln. Verwenden Sie diese Option, um verschlüsselte private Schlüssel im PEM-Format zu laden.
- **fipsKey**. Name des FIPS-Schlüssels, der im Hardware Security Module (HSM) einer FIPS-Appliance erstellt wurde, oder eines Schlüssels, der in das HSM importiert wurde.

  > **Hinweis**
  >
  > Sie können entweder einen Schlüssel oder einen FIPSkey angeben, aber nicht beide.

- **inform**. Format des Zertifikats und der Privatschlüsseldateien, entweder PEM oder DER.
- **passplain**. Passphrase, die zum Verschlüsseln des privaten Schlüssels verwendet wird. Erforderlich für das Hinzufügen eines verschlüsselten privaten Schlüssels im PEM-Format.
- **expiryMonitor**. Konfigurieren Sie die NetScaler-Appliance so, dass eine Warnung ausgegeben wird, wenn das Zertifikat bald abläuft. Mögliche Werte: ENABLED, DISABLED, UNSET.
- **notificationPeriod**. Wenn `expiryMonitor` ENABLED ist, die Anzahl der Tage, bis das Zertifikat abläuft, um eine Warnung auszustellen.

- **bundle**. Analysieren Sie die Zertifikatkette als einzelne Datei, nachdem Sie das Serverzertifikat mit dem Zertifikat seines Ausstellers in der Datei verknüpft haben. Mögliche Werte: YES, NO.

Beispiel

Im folgenden Beispiel wird das angegebene delegierte Benutzerzertifikat customer-cert.pem zusammen mit dem Schlüssel customer-key.pem zur NetScaler-Konfiguration hinzugefügt und das Kennwort, das Zertifikatsformat, die Ablaufüberwachung und die Benachrichtigungsfrist festgelegt.

Um das delegierte Benutzerzertifikat hinzuzufügen, geben Sie die folgenden Befehle ein:

```
add ssl certKey customer -cert "/nsconfig/ssl/customer-cert.pem"
-key "/nsconfig/ssl/customer-key.pem" -password "dontUseDefaultPWs!"
-inform PEM -expiryMonitor ENABLED [-notificationPeriod 14]

<!--NeedCopy-->
```

Erstellen des KCD-Kontos

Wenn Sie NetScaler SSO durch Delegierung konfigurieren, können Sie das KCD-Konto so konfigurieren, dass es den Anmeldenamen und das Kennwort des Benutzers verwendet, den Anmeldenamen und die Keytab des Benutzers verwendet oder das Clientzertifikat des Benutzers verwendet. Wenn Sie SSO mit Benutzernamen und Kennwort konfigurieren, verwendet die NetScaler-Appliance das delegierte Benutzerkonto, um ein Ticket Granting Ticket (TGT) zu erhalten, und verwendet dann das TGT, um Servicetickets für die spezifischen Dienste zu erhalten, die jeder Benutzer anfordert. Wenn Sie SSO mit der Keytab-Datei konfigurieren, verwendet die NetScaler-Appliance das delegierte Benutzerkonto und die Keytab-Informationen. Wenn Sie SSO mit einem delegierten Benutzerzertifikat konfigurieren, verwendet die NetScaler-Appliance das delegierte Benutzerzertifikat.

> **Hinweis:**
>
> Bereichsübergreifend muss der servicePrincipalName des delegierten Benutzers das Format `host/<name>` haben. Wenn er nicht in diesem Format vorliegt, ändern Sie den servicePrincipalName des delegierten Benutzers `<servicePrincipalName>` in `host/<service-account-samaccountname>`. Sie können das Attribut des delegierten Benutzerkontos im Domänencontroller überprüfen. Eine Methode zum Ändern besteht darin, das Attribut `logonName` des delegierten Benutzers zu ändern.

So erstellen Sie das KCD-Konto für SSO durch Delegierung mit einem Kennwort

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add aaa kcdAccount <kcdAccount> {
 -realmStr <string> }
```



```
  {
 -delegatedUser <string> }
  {
 -kcdPassword  }
  [-userRealm <string>]
[-enterpriseRealm <string>] [-serviceSPN <string>]
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **kcdAccount** — Ein Name für das KCD-Konto. Dies ist ein zwingendes Argument. Maximale Länge: 31
- **realmStr** - Der Bereich von Kerberos. Maximale Länge: 255
- **delegatedUser** — Der Benutzername, der die eingeschränkte Kerberos-Delegierung durchführen kann. Der delegierte Benutzername wird vom servicePrincipalName Ihres Domänencontrollers abgeleitet. Für Cross-Realm muss der servicePrincipalName des delegierten Benutzers das Format haben `host/<name>`. Maximale Länge: 255
- **kcdPassword** - Kennwort für delegierten Benutzer. Maximale Länge: 31
- **userRealm** - Bereich des Benutzers. Maximale Länge: 255
- **enterpriseRealm** - Enterprise-Bereich des Benutzers. Dies ist nur in bestimmten KDC-Bereitstellungen gegeben, in denen KDC den Enterprise-Benutzernamen anstelle von Principal Name erwartet. Maximale Länge: 255
- **serviceSPN** — Dienst-SPN. Wenn angegeben, wird dies zum Abrufen von Kerberos-Tickets verwendet. Wenn nicht angegeben, erstellt NetScaler SPN mit dem Dienst-FQDN. Maximale Länge: 255

Beispiel (UPN-Format):

Um ein KCD-Konto mit dem Namen kcdaccount1 zur NetScaler-Appliance-Konfiguration mit dem Kennwort Kennwort1 und einem Bereich von EXAMPLE.COM hinzuzufügen und das delegierte Benutzerkonto im UPN-Format (als root) anzugeben, geben Sie die folgenden Befehle ein:

```
add aaa kcdaccount kcdaccount1  - delegatedUser root
-kcdPassword password1 -realmStr EXAMPLE.COM

<!--NeedCopy-->
```

Beispiel (SPN-Format):

Um ein KCD-Konto mit dem Namen kcdaccount1 zur NetScaler-Appliance-Konfiguration mit dem Kennwort Kennwort1 und einem Bereich von EXAMPLE.COM hinzuzufügen und das delegierte Benutzerkonto im SPN-Format anzugeben, geben Sie die folgenden Befehle ein:

```
add aaa kcdAccount kcdaccount1 -realmStr EXAMPLE.COM
-delegatedUser "host/kcdvserver.example.com" -kcdPassword password1
```



```
3
4 <!--NeedCopy-->
```

Erstellen des KCD-Kontos für SSO durch Delegation mit einer Keytab

Wenn Sie eine Keytab-Datei für die Authentifizierung verwenden möchten, erstellen Sie zuerst die Keytab-Datei. Sie können die Keytab-Datei manuell erstellen, indem Sie sich am AD-Server anmelden und das Dienstprogramm `ktpass` verwenden, oder Sie können das NetScaler-Konfigurationsdienstprogramm verwenden, um ein Batchskript zu erstellen und dieses Skript dann auf dem AD-Server auszuführen, um die Keytab-Datei zu generieren. Verwenden Sie als Nächstes FTP oder ein anderes Dateiübertragungsprogramm, um die Keytab-Datei auf die NetScaler-Appliance zu übertragen und im Verzeichnis /nsconfig/krb abzulegen. Konfigurieren Sie abschließend das KCD-Konto für NetScaler SSO durch Delegierung und geben Sie der NetScaler-Appliance den Pfad und den Dateinamen der Keytab-Datei an.

> **Hinweis:**
>
> Wenn Sie für Cross-Realm die Keytab-Datei als Teil des KCD-Kontos abrufen möchten, verwenden Sie den folgenden Befehl für den aktualisierten delegierten Benutzernamen.
>
> Erstellen Sie im Domänencontroller eine aktualisierte Keytab-Datei.
>
> ```
> ktpass /princ <servicePrincipalName-with-prefix<host/>Of-delegateUser
> >@<DC REALM in uppercase> /ptype KRB5_NT_PRINCIPAL /mapuser <DC REALM
>  in uppercase>\<sAMAccountName> /pass <delegatedUserPassword> -out
> filepathfor.keytab
> ```
>
> Die Datei `filepathfor.keytab` kann in der NetScaler-Appliance abgelegt und als Teil der Keytab-Konfiguration im ADC KCD-Konto verwendet werden.

So erstellen Sie die Keytab-Datei manuell

Melden Sie sich an der AD-Server-Befehlszeile an und geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 ktpass princ <SPN> ptype KRB5_NT_PRINCIPAL mapuser <DOMAIN><username>
     pass <password> -out <File_Path>
2 <!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **SPN**. Der Dienstprinzipalname für das KCD-Dienstkonto.
- **DOMAIN**. Die Domäne des Active Directory-Servers.
- **username**. Der Benutzername des KSA-Kontos.

- **password**. Das Kennwort für das KSA-Konto.
- **path**. Der vollständige Pfadname des Verzeichnisses, in dem die Keytab-Datei gespeichert werden soll, nachdem sie generiert wurde.

So erstellen Sie mit dem NetScaler-Konfigurationsdienstprogramm ein Skript zum Generieren der Keytab-Datei

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr.**
2. Klicken Sie im Datenbereich unter **Kerberos Constrained Delegation**auf **Batch-Datei**, um Keytab zu generieren.
3. Legen Sie im Dialogfeld **KCD (Kerberos Constrained Delegation)-Keytab-Skript generieren** die folgenden Parameter fest:
   - **Domänenbenutzername**. Der Benutzername des KSA-Kontos.
   - **Domänenkennwort**. Das Kennwort für das KSA-Konto.
   - **Dienstprinzipal**. Der Name des Dienstprinzipals für die KSA.
   - **Name der Ausgabedatei**. Der vollständige Pfad und Dateiname, unter dem die Keytab-Datei auf dem AD-Server gespeichert werden soll.
4. Deaktivieren **Sie das Kontrollkästchen Domänenbenutzerkonto erstellen** .
5. Klicken Sie auf **Skript generieren**.
6. Melden Sie sich beim Active Directory-Server an und öffnen Sie ein Befehlszeilenfenster.
7. Kopieren Sie das Skript aus dem Fenster **Generiertes Skript** und fügen Sie es direkt in das Befehlszeilenfenster des Active Directory-Servers ein. Die keytab wird generiert und im Verzeichnis unter dem Dateinamen gespeichert, den Sie als **Ausgabedateiname** angegeben haben.
8. Verwenden Sie das Dateiübertragungsprogramm Ihrer Wahl, um die Keytab-Datei vom Active Directory-Server auf die NetScaler-Appliance zu kopieren und im Verzeichnis /nsconfig/krb abzulegen.

So erstellen Sie das KCD-Konto

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 add aaa kcdaccount <accountname>  - keytab <keytab>
2 <!--NeedCopy-->
```

Beispiel

Um ein KCD-Konto mit dem Namen kcdccount1 hinzuzufügen und das Keytab mit dem Namen kcdvserver.keytab zu verwenden, geben Sie die folgenden Befehle ein:

```
1 add aaa kcdaccount kcdaccount1  - keytab kcdvserver.keytab
2 <!--NeedCopy-->
```


So erstellen Sie das KCD-Konto für SSO durch Delegation mit einem delegierten Benutzerzertifikat

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add aaa kcdaccount <accountname> -realmStr <realm> -delegatedUser <
    user_nameSPN> -usercert <cert> -cacert <cacert>
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **accountname**. Ein Name für das KCD-Konto.
- **realmStr**. Der Bereich für das KCD-Konto, normalerweise die Domäne, für die SSO konfiguriert ist.
- **delegatedUser**. Der delegierte Benutzername im SPN-Format.
- **usercert**. Der vollständige Pfad und Name der delegierten Benutzerzertifikatdatei auf der NetScaler-Appliance. Das delegierte Benutzerzertifikat muss sowohl das Clientzertifikat als auch den privaten Schlüssel enthalten und muss im PEM-Format vorliegen. Wenn Sie die Smartcard-Authentifizierung verwenden, müssen Sie eine Smartcard-Zertifikatsvorlage erstellen, damit Zertifikate mit dem privaten Schlüssel importiert werden können.
- **cacert**. Der vollständige Pfad und der Name der CA-Zertifikatsdatei auf der NetScaler-Appliance.

Beispiel

Um ein KCD-Konto mit dem Namen kcdccount1 hinzuzufügen und das Schlüsselregister kcdvserver.keytab zu verwenden, geben Sie den folgenden Befehl ein:

```
add aaa kcdaccount kcdaccount1 -realmStr EXAMPLE.COM
     -delegatedUser "host/kcdvserver.example.com" -usercert /certs/
        usercert
     -cacert /cacerts/cacert
<!--NeedCopy-->
```

Active Directory für NetScaler SSO einrichten

Wenn Sie SSO durch Delegierung konfigurieren, müssen Sie nicht nur das KCD-Konto auf der NetScaler-Appliance erstellen, sondern auch ein passendes Kerberos-Dienstkonto (KSA) auf Ihrem LDAP-Active Directory-Server erstellen und den Server für SSO konfigurieren. Verwenden Sie zum Erstellen des KSA den Kontoerstellungsprozess auf dem Active Directory-Server. Um SSO auf dem Active Directory-Server zu konfigurieren, öffnen Sie das Eigenschaftenfenster für den KSA. Auf der Registerkarte **Delegierung** aktivieren Sie die folgenden Optionen: Vertrauen Sie diesem Benutzer für die Delegierung nur an bestimmte Dienste und Verwenden Sie ein beliebiges Authentifizierungsprotokoll. (Die Option “Nur Kerberos” funktioniert nicht, da sie keinen Protokollübergang oder

eingeschränkte Delegierung ermöglicht.) Fügen Sie abschließend die Dienste hinzu, die NetScaler SSO verwaltet.

> **Hinweis:**
>
> Wenn die Registerkarte Delegierung im Dialogfeld Eigenschaften des KSA-Kontos nicht angezeigt wird, müssen Sie den Active Directory-Server mit dem Befehlszeilentool Microsoft setspn so konfigurieren, dass die Registerkarte sichtbar ist, bevor Sie den KSA wie beschrieben konfigurieren können.

Konfigurieren der Delegierung für das Kerberos-Dienstkonto

1. Klicken Sie im Dialogfeld zur Konfiguration des LDAP-Kontos für das Kerberos-Dienstkonto, das Sie erstellt haben, auf die Registerkarte **Delegierung** .
2. Wählen Sie **Diesem Benutzer nur für die Delegierung an die angegebenen Dienste vertrauen**.
3. Wählen Sie unter Nur diesem Benutzer für die Delegierung an die angegebenen Dienste vertrauen die Option **Beliebiges Authentifizierungsprotokoll verwenden**.
4. Klicken Sie unter Dienste, denen dieses Konto delegierte Anmeldeinformationen präsentieren kann, auf **Hinzufügen.**
5. Klicken **Sie im Dialogfeld Dienste hinzufügen** auf **Benutzer** oder **Computer**, wählen Sie den Server aus, der die Ressourcen hostet, die dem Dienstkonto zugewiesen werden sollen, und klicken Sie dann auf **OK.**

   > **Hinweis:**
   >
   > - Die eingeschränkte Delegierung unterstützt keine Dienste, die in anderen Domänen als der dem Konto zugewiesenen Domäne gehostet werden, obwohl Kerberos möglicherweise eine Vertrauensbeziehung zu anderen Domänen hat.
   > - Verwenden Sie den folgenden Befehl, um `setspn` zu erstellen, wenn ein neuer Benutzer im Active Directory erstellt wird: `setspn -A host/kcdvserver.example.com example\kcdtest`

6. Zurück im Dialogfeld **Dienste hinzufügen** in der Liste Verfügbare Dienste wählen Sie die Dienste aus, die dem Dienstkonto zugewiesen sind. NetScaler SSO unterstützt die HTTP- und MSSQLSVC-Dienste.
7. Klicken Sie auf **OK.**

Konfigurationsänderungen, damit KCD untergeordnete Domänen unterstützen kann

Wenn das KCD-Konto mit `samAccountName` für `-delegatedUser` konfiguriert ist, funktioniert KCD nicht für Benutzer, die auf Dienste aus untergeordneten Domänen zugreifen. In diesem Fall können

Sie die Konfiguration auf der NetScaler-Appliance und im Active Directory ändern.

- Ändern Sie den Anmeldenamen des Dienstkontos <service-account-samaccountname> (das im KCD-Konto als delegateUser konfiguriert ist) in AD in das Format host/<service-account-samaccountname>.<completeUSERDNSDOMAIN> (z. B. host/svc_act.child.parent.com).

  Sie können das Dienstkonto manuell oder über den Befehl ktpass ändern. Das aktualisiert das Dienstkonto ktpass automatisch.

  ```
  ktpass /princ host/svc_act.child.parent.com@CHILD.PARENT.COM /ptype KRB5_NT_PRINCIPAL /mapuser CHILD\sv_act /pass serviceaccountpassword -out filepathfor.keytab
  ```

- Ändern Sie delegatedUser im KCD-Konto auf der NetScaler-Appliance.
- Ändern Sie den Parameter -delegatedUser im KCD-Konto in host/svc_act.child.parent.com

Zu beachtende Punkte, wenn erweiterte Verschlüsselungen zur Konfiguration des KCD-Kontos verwendet werden

> - **Beispielkonfiguration bei Verwendung von Keytab:** `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"`
> - **Verwenden Sie den folgenden Befehl, wenn keytab über mehrere Verschlüsselungstypen verfügt.** Der Befehl erfasst auch Domänenbenutzerparameter: `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"-domainUser "HTTP/lbvs.aaa.local"`
> - **Verwenden Sie die folgenden Befehle, wenn Benutzeranmeldeinformationen verwendet werden:** `add kcdaccount kslb2_user -realmStr AAA.LOCAL -delegatedUser lbvs -kcdPassword <password>`
> - Stellen Sie sicher, dass die richtigen **domainUser**-Informationen bereitgestellt werden. Sie können in AD nach dem Benutzeranmeldenamen suchen.

Generieren des KCD-Keytab-Skripts

May 11, 2023

Das Dialogfeld KCD Keytab Script generiert das Keytab-Skript, das wiederum die Keytab-Datei generiert, die für die Konfiguration von KCD auf dem NetScaler erforderlich ist.

Um das KCD-Keytab-Skript mithilfe des Konfigurationsdienstprogramms zu generieren

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr.**
2. Klicken Sie im Detailbereich unter **Kerberos Constrained Delegation**auf Batch-Datei, um Keytab zu generieren.
3. Füllen Sie im Dialogfeld „KCD (Kerberos Constrained Delegation) **Keytab-Skript** generieren“ die Felder wie unten beschrieben aus.
   - **Domänenbenutzername:** Der Name des Domänenbenutzers.
   - **Domain-Passwort:** Das Passwort für den Domänenbenutzer.
   - **Service Principal:** Der Service Principal.
   - **Name der Ausgabedatei:** Ein Dateiname für die KCD-Skriptdatei.
   - **Domänenbenutzerkonto erstellen:** Aktivieren Sie dieses Kontrollkästchen, um das angegebene Domänenbenutzerkonto zu erstellen.
4. Klicken Sie auf **Skript generieren**, um das Skript zu generieren. Das Skript wird generiert und im Textfeld **Generiertes Skript** unter der Schaltfläche **Skript generieren** angezeigt.
5. Kopieren Sie das Skript und speichern Sie es als Datei auf Ihrem AD-Domänencontroller. Sie müssen dieses Skript nun auf dem Domänencontroller ausführen, um die Keytab-Datei zu generieren, und dann die Keytab-Datei in das Verzeichnis /nsconfig/krb/ auf der NetScaler-Appliance kopieren.
6. Klicken Sie auf **OK.**

SSO für Basic-, Digest- und NTLM-Authentifizierung

May 11, 2023

Die Single Sign-On (SSO) -Konfiguration in NetScaler und NetScaler Gateway kann auf globaler Ebene und auch pro Verkehrsebene aktiviert werden. Standardmäßig ist die SSO-Konfiguration **AUS** und ein Administrator kann SSO pro Datenverkehr oder global aktivieren. Aus Sicherheitsgründen empfiehlt Citrix Administratoren, SSO global **auszuschalten** und es pro Datenverkehr zu aktivieren. Diese Erweiterung soll die SSO-Konfiguration sicherer machen, indem bestimmte Arten von SSO-Methoden weltweit nicht berücksichtigt werden.

> **Hinweis:**
>
> Ab NetScaler Feature Release 13.0 Build 64.35 und höher werden die folgenden SSO-Typen weltweit nicht berücksichtigt.
>
> - Grundlegende Authentifizierung
> - Digest Access-Authentifizierung

> - NTLM ohne Negotiate NTLM2-Schlüssel oder Negotiate-Zeichen

Nicht betroffene SSO-Typen

Die folgenden SSO-Typen sind von dieser Erweiterung nicht betroffen.

- Kerberos-Authentifizierung
- SAML-Authentifizierung
- Formularbasierte Authentifizierung
- OAuth-Trägerauthentifizierung
- NTLM mit Negotiate NTLM2-Schlüssel oder Negotiate-Zeichen

Beeinträchtigte Single Sign-On-Konfigurationen

Im Folgenden sind die betroffenen (entehrten) SSO-Konfigurationen aufgeführt.

Globale Konfigurationen

```
set tmsessionparam -SSO ON
set vpnparameter -SSO ON
add tmsessionaction tm_act -SSO ON
add vpn sessionaction tm_act -SSO ON
<!--NeedCopy-->
```

Konfigurationen pro Datenverkehr

```
add vpn trafficaction tf_act http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

> Sie können SSO als Ganzes aktivieren/deaktivieren und können einzelne SSO-Typen nicht ändern.

Anzuwendende Sicherheitsmaßnahmen

Als Teil der Sicherheitsmaßnahmen werden sicherheitsrelevante SSO-Typen in der globalen Konfiguration nicht berücksichtigt, sie sind jedoch nur über eine Traffic-Action-Konfiguration zulässig.
Wenn also ein Backend-Server Basic, Digest oder NTLM ohne Negotiate NTLM2-Schlüssel oder Negotiate Sign erwartet, kann der Administrator SSO nur über die folgende Konfiguration zulassen.

Traffic Action

```
add vpn trafficaction tf_act  http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

Traffic Richtlinie

```
add tm trafficpolicy <name> <rule> tf_act
add vpn trafficpolicy <name> <rule> tf-act
<!--NeedCopy-->
```

> Der Administrator muss eine entsprechende Regel für die Verkehrsrichtlinie konfiguriert haben, um sicherzustellen, dass SSO nur für vertrauenswürdige Back-End-Server aktiviert ist.

AAA-TM

Szenarien, die auf der globalen Konfiguration basieren:

```
set tmsessionparam -SSO ON
<!--NeedCopy-->
```

Workaround:

```
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol true tf_act
<!--NeedCopy-->
```

Binden Sie die folgende Verkehrsrichtlinie an alle virtuellen LB-Server, auf denen SSO erwartet wird:

```
bind lb vserver <LB VS Name> -policy tf_pol -priority 65345
<!--NeedCopy-->
```

Szenarien basierend auf der Konfiguration der Sitzungsrichtlinien:

```
add tmsessionaction tm_act -SSO ON
add tmsession policy <name> <rule> tm_act
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol <same rule as session Policy> tf_act
<!--NeedCopy-->
```

Bemerkenswerte Punkte:

- Der NetScaler AAA-Benutzer/die Gruppe für die vorherige Sitzungsrichtlinie muss durch eine Verkehrsrichtlinie ersetzt werden.
- Binden Sie die folgende Richtlinie an die virtuellen Lastausgleichsserver für die vorherige Sitzungsrichtlinie:

```
bind lb vserver [LB VS Name] -policy tf_pol -priority 65345
<!--NeedCopy-->
```

- Wenn eine Verkehrsrichtlinie mit einer anderen Priorität konfiguriert ist, ist der vorherige Befehl nicht hilfreich.

Der folgende Abschnitt befasst sich mit Szenarien, die auf Konflikten mit mehreren Verkehrsrichtlinien basieren, die einem Verkehr zugeordnet sind:

Für einen bestimmten TM-Verkehr wird nur eine TM-Verkehrsrichtlinie angewendet. Aufgrund der globalen Einstellungen der SSO-Funktionen ist die Anwendung einer zusätzlichen TM-Verkehrsrichtlinie mit niedriger Priorität möglicherweise nicht anwendbar, falls bereits eine TM-Verkehrsrichtlinie mit hoher Priorität (für die keine SSO-Konfiguration erforderlich ist) angewendet wird. Im folgenden Abschnitt wird die Methode beschrieben, mit der sichergestellt werden kann, dass solche Fälle behandelt werden.

Beachten Sie, dass die folgenden drei Verkehrsrichtlinien mit höherer Priorität auf virtuelle Load Balancing-Server (LB) angewendet werden:

```
add tm trafficaction tf_act1 <Addition config>
add tm trafficaction tf_act2 <Addition config>
add tm trafficaction tf_act3 <Addition config>

add tm trafficpolicy tf_pol1 <rule1> tf_act1
add tm trafficpolicy tf_pol2 <rule2> tf_act2
add tm trafficpolicy tf_pol3 <rule3> tf_act3

bind lb vserver <LB VS Name> -policy tf_pol1 -priority 100
bind lb vserver <LB VS Name> -policy tf_pol2 -priority 200
bind lb vserver <LB VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Fehleranfällige Methode - Um die globale SSO-Konfiguration zu lösen, fügen Sie die folgende Konfiguration hinzu:

```
add tm trafficaction tf_act_default -SSO ON
add tm trafficpolicy tf_pol_default true tf_act_default

bind lb vserver <LB VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```


Hinweis: Die vorhergehende Änderung kann SSO für Traffic, der trifft, <tf_pol1/tf_pol2/tf_pol3> wie für diese Traffic- und Verkehrsrichtlinie unterbrechen wird nicht angewendet.

Richtige Methode - Um dies zu mindern, muss die SSO-Eigenschaft für jede der entsprechenden Verkehrsaktionen einzeln angewendet werden:

Zum Beispiel muss im vorhergehenden Szenario die folgende Konfiguration zusammen mit angewendet werden, damit SSO für den Datenverkehr auf tf_pol1/tf_pol3 trifft .

```
add tm trafficaction tf_act1 <Addition config> -SSO ON
add tm trafficaction tf_act3 <Addition config> -SSO ON
<!--NeedCopy-->
```

NetScaler Gateway -Fälle

Szenarien, die auf der globalen Konfiguration basieren:

```
set vpnparameter -SSO ON
<!--NeedCopy-->
```

Workaround:

```
add vpn trafficaction vpn_tf_act http  -SSO ON
add vpn trafficpolicy vpn_tf_pol  true vpn_tf_act
bind the following traffic policy to all VPN virtual server where SSO
    is expected:
bind vpn vserver vpn_vs -policy vpn_tf_pol -priority 65345
<!--NeedCopy-->
```

Szenarien basierend auf der Konfiguration der Sitzungsrichtlinien:

```
add vpn sessionaction vpn_sess_act -SSO ON
add vpnsession policy <name> <rule> vpn_sess_act
<!--NeedCopy-->
```

Zu beachtende Punkte:

- Der NetScaler AAA-Benutzer/die Gruppe für die vorherige Sitzungsrichtlinie muss durch eine Verkehrsrichtlinie ersetzt werden.
- Binden Sie die folgende Richtlinie für die vorherige Sitzungsrichtlinie an die virtuellen LB-Server, `bind lb virtual server [LB VS Name] -policy tf_pol -priority 65345`.

- Wenn eine Verkehrsrichtlinie mit einer anderen Priorität konfiguriert ist, ist der vorherige Befehl nicht hilfreich. Der folgende Abschnitt befasst sich mit Szenarien, die auf Konflikten mit mehreren Verkehrsrichtlinien im Zusammenhang mit dem Verkehr beruhen.

Funktionsszenarien, die auf Konflikten mit mehreren Verkehrsrichtlinien basieren, die einem Verkehr zugeordnet sind:

Für einen bestimmten NetScaler Gateway-Verkehr wird nur eine VPN-Verkehrsrichtlinie angewendet. Aufgrund der globalen Einstellungen der SSO-Funktionen ist die Anwendung einer zusätzlichen VPN-Verkehrsrichtlinie mit niedriger Priorität möglicherweise nicht anwendbar, wenn es andere VPN-Verkehrsrichtlinien mit hoher Priorität gibt, für die keine SSO-Konfiguration erforderlich ist.

Im folgenden Abschnitt wird die Methode beschrieben, mit der sichergestellt werden kann, dass solche Fälle behandelt werden:

Bedenken Sie, dass es drei Verkehrsrichtlinien mit höherer Priorität gibt, die auf einen virtuellen VPN-Server angewendet werden:

```
add vpn trafficaction tf_act1 <Addition config>
add vpn trafficaction tf_act2 <Addition config>
add vpn trafficaction tf_act3 <Addition config>

add vpn trafficpolicy tf_pol1 <rule1> tf_act1
add vpn trafficpolicy tf_pol2 <rule2> tf_act2
add vpn trafficpolicy tf_pol3 <rule3> tf_act3

bind vpn vserver <VPN VS Name> -policy tf_pol1 -priority 100
bind vpn vserver <VPN VS Name> -policy tf_pol2 -priority 200
bind vpn vserver <VPN VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Fehleranfällige Methode: Um die globale SSO-Konfiguration zu lösen, fügen Sie die folgende Konfiguration hinzu:

```
add vpn trafficaction tf_act_default -SSO ON
add vpn trafficpolicy tf_pol_default true tf_act_default

bind vpn vserver <VPN VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```

Hinweis: Die vorhergehende Änderung kann SSO für den Traffic, der trifft, <tf_pol1/tf_pol2/tf_pol3> wie für diesen Traffic und die Verkehrsrichtlinie unterbrechen wird nicht angewendet.

Richtige Methode: Um dies zu mindern, muss die SSO-Eigenschaft für jede der entsprechenden Verkehrsaktionen einzeln angewendet werden.

Zum Beispiel im vorherigen Szenario muss die folgende Konfiguration zusammen mit angewendet werden, damit SSO für Datenverkehr auf tf_pol1/tf_pol3 trifft .

```
add vpn trafficaction tf_act1 [Additional config] -SSO ON

add vpn trafficaction tf_act3 [Additional config] -SSO ON
<!--NeedCopy-->
```

Rewrite für NetScaler Gateway und Authentifizierungsserver generierte Antworten

July 11, 2023

Rewrite bezieht sich auf das Neuschreiben einiger Informationen in den Anforderungen oder Antworten, die von der NetScaler-Appliance verarbeitet werden. Das Umschreiben kann dazu beitragen, Zugriff auf die angeforderten Inhalte zu gewähren, ohne unnötige Details über die tatsächliche Konfiguration der Website preiszugeben. Ausführliche Informationen zum Rewrite-Konzept finden Sie unter Rewrite

Ausgehend von NetScaler Release Build 13.0-76.29 wurde die Unterstützung für Rewrite-Richtlinien auf den virtuellen NetScaler Gateway-Server und vom Authentifizierungsserver generierte Antworten ausgeweitet.

> **Hinweis**
>
> Ein Bind-Typ **AAA_Response** wird eingeführt, um Rewrite-Richtlinien für virtuelle NetScaler Gateway-Server und vom Authentifizierungsserver generierte Antworten zu unterstützen.

Ein Beispiel für die Verwendung von Rewrite

Sie können Rewrite verwenden, um die on-premises verfügbaren Ressourcen NetScaler für die Citrix Cloud-Bereitstellung freizugeben. Dies kann durch die Implementierung von CORS Origin Resource Sharing sicher erreicht werden. Rewrite kann wie folgt verwendet werden, um den CORS-Header zu implementieren.

Beispiel-Konfiguration

```
add rewrite action cors_header_action insert_http_header access-control
    -allow-credentials \"true\"

add rewrite policy cors_header_pol true cors_header_action
```



```
4
5 add rewrite action non_cors_header_action insert_http_header X-Frame-
     Options \'\"DENY\"\'
6
7 add rewrite policy non_cors_header_pol true non_cors_header_action
8
9 bind authentication vserver av_cors -policy cors_header_pol -priority
     100 -type AAA_RESPONSE
10
11 bind vpn vserver av_cors -policy cors_header_pol -priority 100 -type
     AAA_RESPONSE
```

> **Hinweis:**
>
> Anweisungen zur Konfiguration einer Rewrite-Aktion und -Richtlinie mithilfe der GUI finden Sie unter Rewrite.

Unterstützung für Antwortheader der Inhaltssicherheitsrichtlinie für NetScaler Gateway und von virtuellen Servern generierte Authentifizierungsantworten

July 11, 2023

Ab NetScaler Release Build 13.0—76.29 wird der Content-Security-Policy (CSP) -Antwortheader für von NetScaler Gateway und virtuelle Authentifizierungsserver generierte Antworten unterstützt.

Der Content-Security-Policy (CSP) Response-Header ist eine Kombination von Richtlinien, die der Browser verwendet, um Cross-Site-Scripting (CSS) -Angriffe zu vermeiden.
Der HTTP-CSP-Antwortheader ermöglicht es Website-Administratoren, die Ressourcen zu steuern, die der Benutzeragent für eine bestimmte Seite laden darf. Mit wenigen Ausnahmen beinhalten Richtlinien hauptsächlich die Angabe von Serverursprüngen und Skript-Endpunkten. Dies schützt vor Cross-Site-Scripting-Angriffen.
Der CSP-Header wurde entwickelt, um die Art und Weise zu ändern, wie Browser Seiten rendern, und schützt damit vor verschiedenen standortübergreifenden Einschleusungen, einschließlich CSS. Es ist wichtig, den Header-Wert korrekt einzustellen, so dass der ordnungsgemäße Betrieb der Website nicht verhindert wird. Wenn der Header beispielsweise so eingestellt ist, dass er die Ausführung von Inline-JavaScript verhindert, darf die Website auf ihren Seiten kein Inline-JavaScript verwenden.

Im Folgenden sind die Vorteile des CSP-Antwort-Headers aufgeführt.

- Die Hauptfunktion eines CSP-Antwortheaders besteht darin, CSS-Angriffe zu verhindern.

- Neben der Einschränkung der Domänen, aus denen Inhalte geladen werden können, kann der Server angeben, welche Protokolle verwendet werden dürfen. Zum Beispiel (und idealerweise aus Sicherheitssicht) kann ein Server angeben, dass alle Inhalte unter Verwendung von HTTPS geladen werden müssen.
- CSP hilft dabei, NetScaler vor standortübergreifenden Scripting-Angriffen zu schützen, indem er Dateien wie “tmindex.html” und “homepage.html” sichert. Die Datei “tmindex.html” bezieht sich auf die Authentifizierung und die Datei “homepage.html” bezieht sich auf die veröffentlichten Apps/Links.

Konfigurieren des Content-Security-Policy-Headers für NetScaler Gateway und Authentifizierung von virtuellen Servern generierten Antworten

Um den CSP-Header zu aktivieren, müssen Sie Ihren Webserver so konfigurieren, dass er den CSP-HTTP-Header zurückgibt.

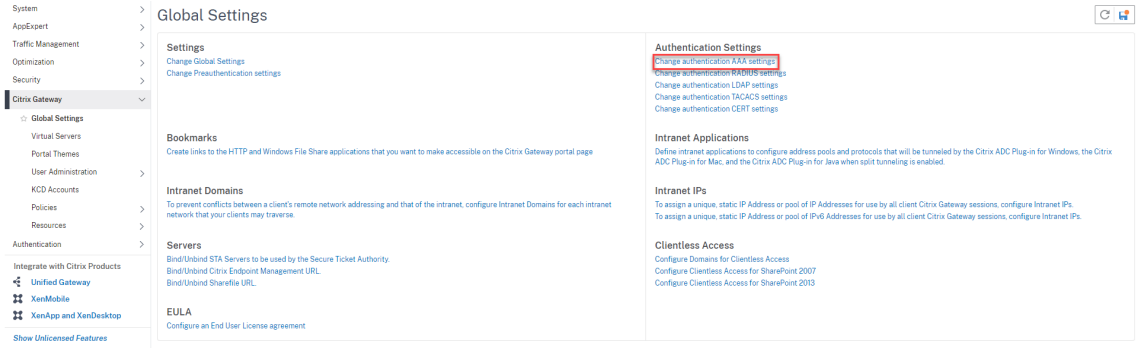
> **Wichtige Hinweise**
>
> - Standardmäßig ist der CSP-Header deaktiviert.
> - Beim Aktivieren oder Deaktivieren der Standard-CSP-Richtlinie wird empfohlen, den folgenden Befehl auszuführen. `Flush cache contentgroup loginstaticobjects`
> - Um den CSP für /logon/LogonPoint/index.html zu ändern, ändern Sie den Wert “Header set Content-Security-Policy” wie erforderlich in dem Abschnitt, der dem Anmeldeverzeichnis entspricht, das im Verzeichnis `/var/netscaler/logon` ist.
> - Anweisungen zur Konfiguration einer Rewrite-Aktion und -Richtlinie mithilfe der GUI finden Sie unter Rewrite.

Um CSP für den Authentifizierungsserver und von NetScaler Gateway generierte Antworten mit CLI zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

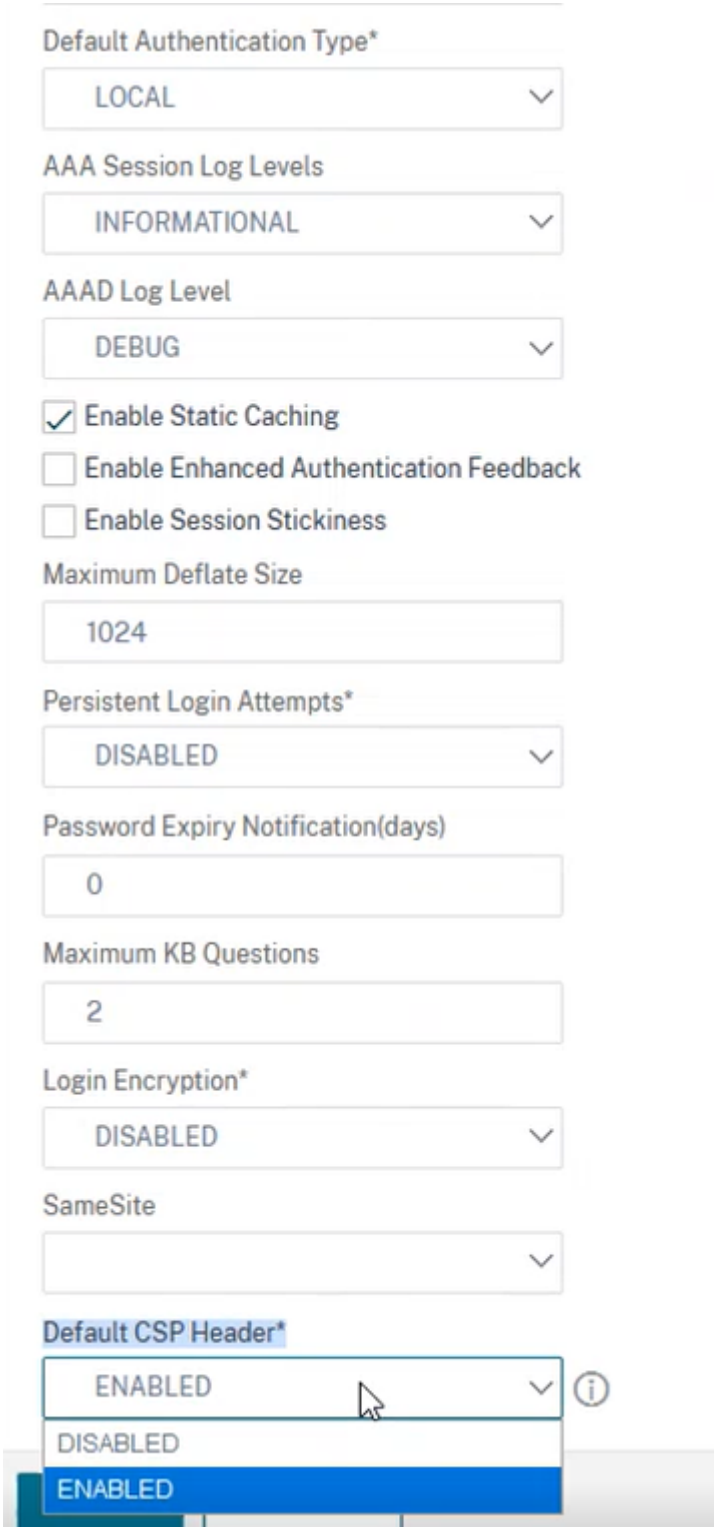
```
1 set aaa parameter -defaultCSPHeader <ENABLE/DISABLE>
```

So konfigurieren Sie CSP für NetScaler Gateway und Authentifizierung von virtuellen Servern generierten Antworten über die GUI.

1. Navigieren Sie zu **NetScaler Gateway > Globale Einstellungen** und klicken Sie unter **Authentifizierungseinstellungen auf AAA-Einstellungen für Authentifizierung ändern**.



2. Wählen Sie auf der Seite **AAA-Parameter konfigurieren** das Feld **In Standard-CSP-Header aktiviert** aus.



Ein Beispiel für die Anpassung der Kopfzeile von Content-Security-Policy

Im Folgenden finden Sie ein Beispiel für die Anpassung von CSP-Headern, um Images und Skripts nur aus den folgenden beiden angegebenen Quellen einzuschließen: `https://company.fqdn.com`, `https://example.com`.

Beispiel-Konfiguration

```
add rewrite action modify_csp insert_http_header Content-Security-
    Policy "\"default-src 'self'; script-src 'self' https://company.fqdn
    .com 'unsafe-inline' 'unsafe-eval'; connect-src 'self'; img-src http
    ://localhost:* https://example.com 'self' data: http: https:; style-
    src 'self' 'unsafe-inline'; font-src 'self'; frame-src 'self'; child
    -src 'self' com.citrix.agmacepa://* citrixng://* com.citrix.
    nsgclient://*; form-action 'self'; object-src 'self'; report-uri /
    nscsp_violation/report_uri\""

add rewrite policy add_csp true modify_csp

bind authentication vserver auth1 -policy add_csp -priority 1 -
    gotoPriorityExpression NEXT -type AAA_RESPONSE
```

Benutzerseitige Kennwortzurücksetzung

July 24, 2023

Das Self-Service-Kennwort-Zurücksetzen ist eine webbasierte Kennwortverwaltungslösung. Es ist sowohl in der Authentifizierungs-, Autorisierungs- und Überwachungsfunktion der NetScaler-Appliance als auch in NetScaler Gateway verfügbar. Dadurch entfällt die Abhängigkeit des Benutzers von der Unterstützung des Administrators beim Ändern des Kennworts.

Das Self-Service-Kennwort-Reset bietet dem Endbenutzer die Möglichkeit, ein Kennwort in den folgenden Szenarien sicher zurückzusetzen oder zu erstellen:

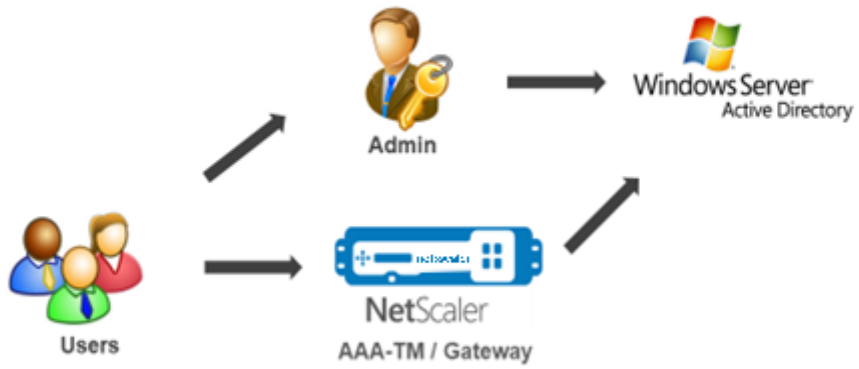
- Der Benutzer hat das Kennwort vergessen.
- Der Benutzer kann sich nicht anmelden.

Wenn ein Endbenutzer ein AD-Kennwort vergisst, musste sich der Endbenutzer an den AD-Administrator wenden, um das Kennwort zurückzusetzen. Mit der Self-Service-Funktion zum Zurücksetzen des Kennworts kann ein Endbenutzer das Kennwort ohne Eingreifen eines Administrators zurücksetzen.

Im Folgenden sind einige der Vorteile der Verwendung des Self-Service-Kennwort-Resets aufgeführt:

- Erhöhte Produktivität durch den automatischen Mechanismus zur Kennwortänderung, wodurch die Vorlaufzeit für Benutzer zum Zurücksetzen des Kennworts entfällt.
- Mit dem automatischen Kennwortänderungsmechanismus können sich Administratoren auf andere wichtige Aufgaben konzentrieren.

Die folgende Abbildung zeigt den Ablauf des Self-Service-Kennwortrücksetzens zum Zurücksetzen des Kennworts



Um das Self-Service-Kennwort zurücksetzen zu können, muss ein Benutzer entweder bei der NetScaler-Authentifizierung, -Autorisierung und -Überwachung oder beim virtuellen NetScaler Gateway-Server registriert sein.

Das Self-Service-Kennwort-Reset bietet folgende Funktionen:

- **Selbstregistrierung neuer Benutzer.** Sie können sich selbst als neuer Benutzer registrieren.
- **Konfigurieren Sie wissensbasierte Fragen.** Als Administrator können Sie eine Reihe von Fragen für Benutzer konfigurieren.
- **Alternative E-Mail-ID-Registrierung.** Sie müssen bei der Registrierung eine alternative E-Mail-ID angeben. Das OTP wird an die alternative E-Mail-ID gesendet, da der Benutzer das primäre E-Mail-ID-Kennwort vergessen hat.

  > **Hinweis:**
  >
  > Ab Version 12.1 Build 51.xx kann eine alternative E-Mail-ID-Registrierung als eigenständige Registrierung durchgeführt werden. Ein neues Anmeldeschema, **AltEmailRegister.xml**, wurde eingeführt, um nur eine alternative E-Mail-ID-Registrierung durchzuführen. Bisher

> konnte eine alternative E-Mail-ID-Registrierung nur während der KBA-Registrierung durchgeführt werden.

- **Kennwort vergessen zurücksetzen.** Der Benutzer kann das Kennwort zurücksetzen, indem er die wissensbasierten Fragen beantwortet. Als Administrator können Sie die Fragen konfigurieren und speichern.

Das Self-Service-Kennwort-Reset bietet die folgenden zwei neuen Authentifizierungsmechanismen:

- **Wissensbasierte Frage und Antwort.** Sie müssen sich bei NetScaler Authentication, Authorization and Auditing oder bei einem NetScaler Gateway registrieren, bevor Sie das wissensbasierte Frage- und Antwortschema auswählen können.
- **E-Mail-OTP-Authentifizierung.** Ein OTP wird an die alternative E-Mail-ID gesendet, die der Benutzer bei der Self-Service-Registrierung zum Zurücksetzen des Kennworts registriert hat.

> **Hinweis**
>
> Diese Authentifizierungsmechanismen können für die Self-Service-Anwendungsfälle zum Zurücksetzen des Kennworts und für beliebige Authentifizierungszwecke verwendet werden, die einem der vorhandenen Authentifizierungsmechanismen ähneln.

Voraussetzungen

Bevor Sie das Self-Service-Zurücksetzen des Kennworts konfigurieren, sollten Sie die folgenden Voraussetzungen prüfen:

- NetScaler Feature Release 12.1, Build 50.28.
- Die unterstützte Version ist die AD-Domänenfunktionsebene 2016, 2012 und 2008.
- Der an den NetScaler gebundene ldapBind-Benutzername muss Schreibzugriff auf den AD-Pfad des Benutzers haben.

  > **Hinweis**
  >
  > Self-Service-Kennwortrücksetzung wird nur im nFactor-Authentifizierungsfluss unterstützt. Weitere Informationen finden Sie unter nFactor-Authentifizierung über NetScaler.

Einschränkungen

Im Folgenden sind einige Einschränkungen beim Zurücksetzen des Self-Service-Kennworts aufgeführt:

- Self-Service-Kennwortrücksetzung wird auf LDAPS unterstützt. Self-Service-Kennwortrücksetzung ist nur verfügbar, wenn das Authentifizierungs-Backend LDAP (LDAP-Protokoll) ist.
- Der Benutzer kann die bereits registrierte alternative E-Mail-ID nicht sehen.

- Wissensbasierte Fragen und Antworten sowie die E-Mail-OTP-Authentifizierung und -Registrierung können nicht der erste Faktor im Authentifizierungsablauf sein.
- Für Native Plug-in und Receiver wird die Registrierung nur über den Browser unterstützt.
- Die Mindestzertifikatgröße, die für das Zurücksetzen von Self-Service-Kennwörtern verwendet wird, beträgt 1024 Byte und muss dem x.509-Standard entsprechen.
- Nur ein RSA-Zertifikat wird für das Self-Service-Kennwortrücksetzen unterstützt.

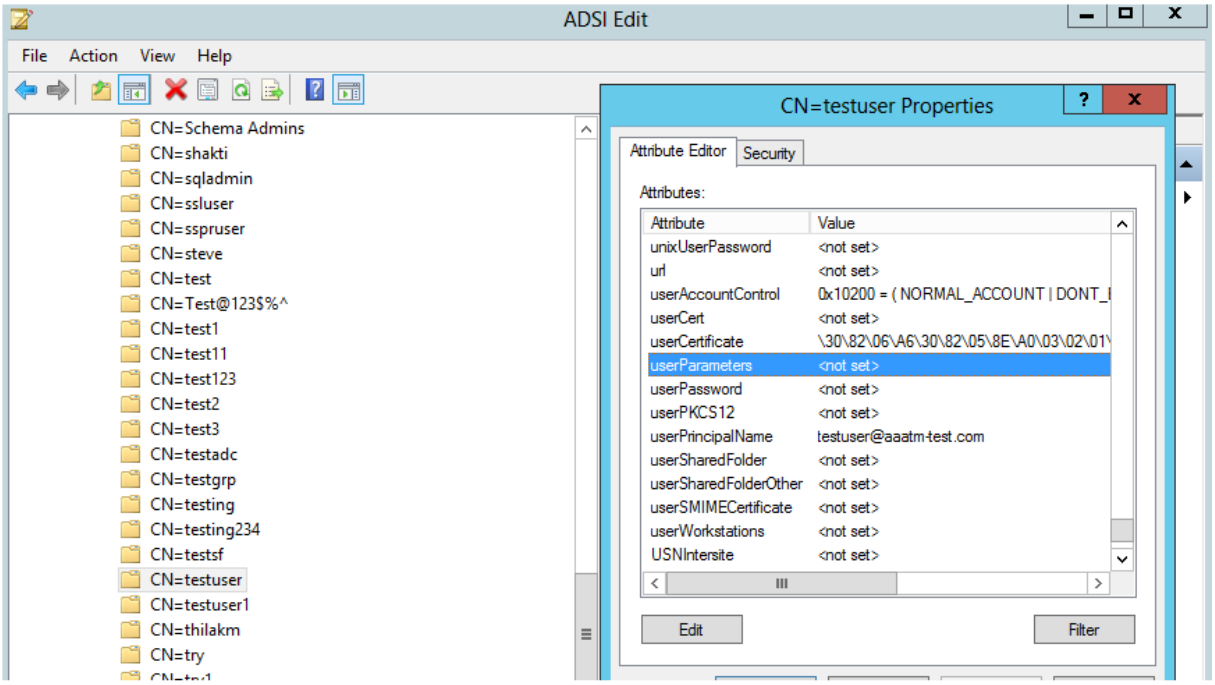
Active Directory-Einstellung

Die wissensbasierte Frage und Antwort von NetScaler sowie das E-Mail-OTP verwenden ein AD-Attribut zum Speichern von Benutzerdaten. Sie müssen ein AD-Attribut konfigurieren, um die Fragen und Antworten zusammen mit der alternativen E-Mail-ID zu speichern. Die NetScaler-Appliance speichert es im konfigurierten KB-Attribut im AD-Benutzerobjekt. Beachten Sie beim Konfigurieren eines AD-Attributs Folgendes:

- Das AD-Attribut muss eine maximale Länge von 32k unterstützen.
- Der Attributtyp muss ein ‘DirectoryString’ sein.
- Ein einzelnes AD-Attribut kann für wissensbasierte Fragen und Antworten sowie eine alternative E-Mail-ID verwendet werden.
- Ein einzelnes AD-Attribut kann nicht für Native OTP und wissensbasierte Fragen und Antworten oder alternative E-Mail-ID-Registrierung verwendet werden.
- Der NetScaler LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.

Sie können auch ein vorhandenes AD-Attribut verwenden. Stellen Sie jedoch sicher, dass das Attribut, das Sie verwenden möchten, nicht für andere Fälle verwendet wird. UserParameters ist beispielsweise ein vorhandenes Attribut innerhalb des AD-Benutzers, das Sie verwenden können. Um dieses Attribut zu überprüfen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **ADSI > Benutzer auswählen**.
2. Rechtsklicken Sie und scrollen Sie nach unten zur Attributliste.
3. Im Fensterbereich **cn=TestUser Properties** können Sie sehen, dass das **UserParameters-Attribut** nicht festgelegt ist.



Self-Service-Kennwort-Reset-

Um die Self-Service-Lösung zum Zurücksetzen des Kennworts auf einer NetScaler-Appliance zu implementieren, müssen Sie Folgendes ausführen:

- Self-Service-Kennwortrücksetzung (wissensbasierte Frage und Antwort/E-Mail-ID).
- Benutzeranmeldeseite (zum Zurücksetzen des Kennworts, einschließlich wissensbasierter Frage und Antwort sowie OTP-Validierung per E-Mail und endgültigem Kennwortrücksetzfaktor).

Ein Satz vordefinierter Fragenkatalog wird als JSON-Datei bereitgestellt. Als Administrator können Sie die Fragen auswählen und das Anmeldeschema zum Zurücksetzen des Self-Service-Kennwortrücksetzens über die NetScaler GUI erstellen. Sie können eine der folgenden Optionen wählen:

- Wählen Sie maximal vier systemdefinierte Fragen aus.
- Bieten Sie Benutzern die Möglichkeit, zwei Fragen und Antworten anzupassen.

So zeigen Sie die standardmäßige JSON-Datei für wissensbasierte Fragen von CLI an

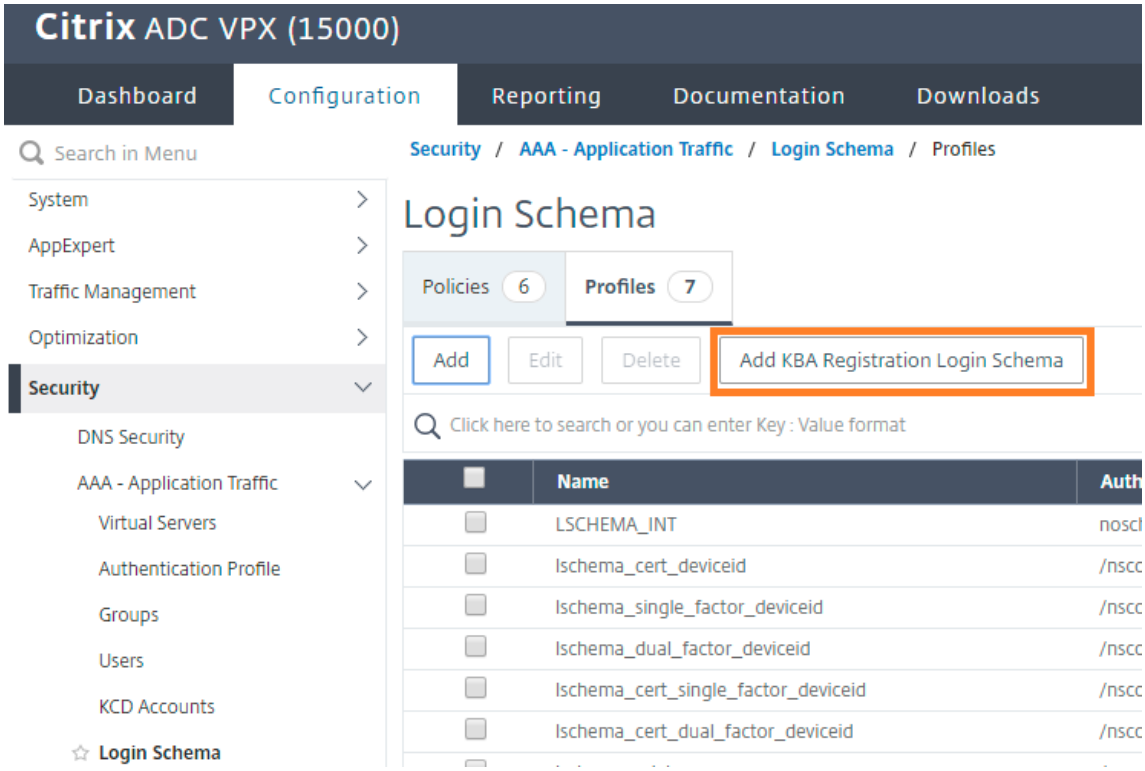
```
root@ns# cd /nsconfig/loginschema/LoginSchema/
root@ns# cat KBQuestions.json
[
    {"question":"What is the last name of the teacher who gave you your first failing
grade?"},
    {"question":"What is the name of your favourite childhood friend?"},
    {"question":"Where were you when you first heard about 9/11?"},
    {"question":"What is the name of a college you applied to but didn't attend?"},
    {"question":"What was the last name of your third grade teacher?"},
    {"question":"What was the name of your first stuffed animal?"},
    {"question":"What is the name of the teacher who gave you your first A?"},
    {"question":"What is the name of the city where you got lost?"},
    {"question":"In what city or town did your mother and father meet?"},
    {"question":"What was your most hated food as a child?"},
    {"question":"What was your most favourite food as a child?"},
    {"question":"What is your favourite website?"},
    {"question":"What is your most disliked website?"},
    {"question":"What is your dream job?"},
    {"question":"Why did the chicken cross the road?"},
    {"question":"Name your first boss."},
    {"question":"What is the name of your favorite school teacher?"},
    {"question":"What is the name of your favorite actor or actress?"},
    {"question":"What is the title of your favorite movie?"},
    {"question":"In what city or town did you spend most of your youth?"}
]
```

Hinweis

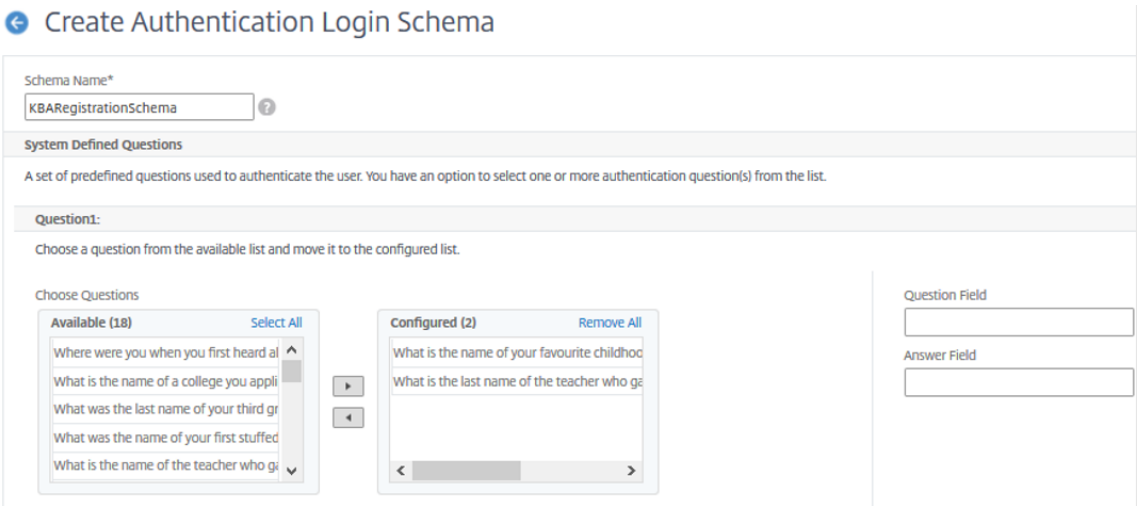
- NetScaler Gateway enthält standardmäßig den Satz systemdefinierter Fragen. Der Administrator kann die Datei “KbQuestions.json” bearbeiten, um die gewünschten Fragen aufzunehmen.
- Systemdefinierte Fragen werden nur auf Englisch angezeigt, und für diese Fragen ist keine Sprachlokalisierung verfügbar.

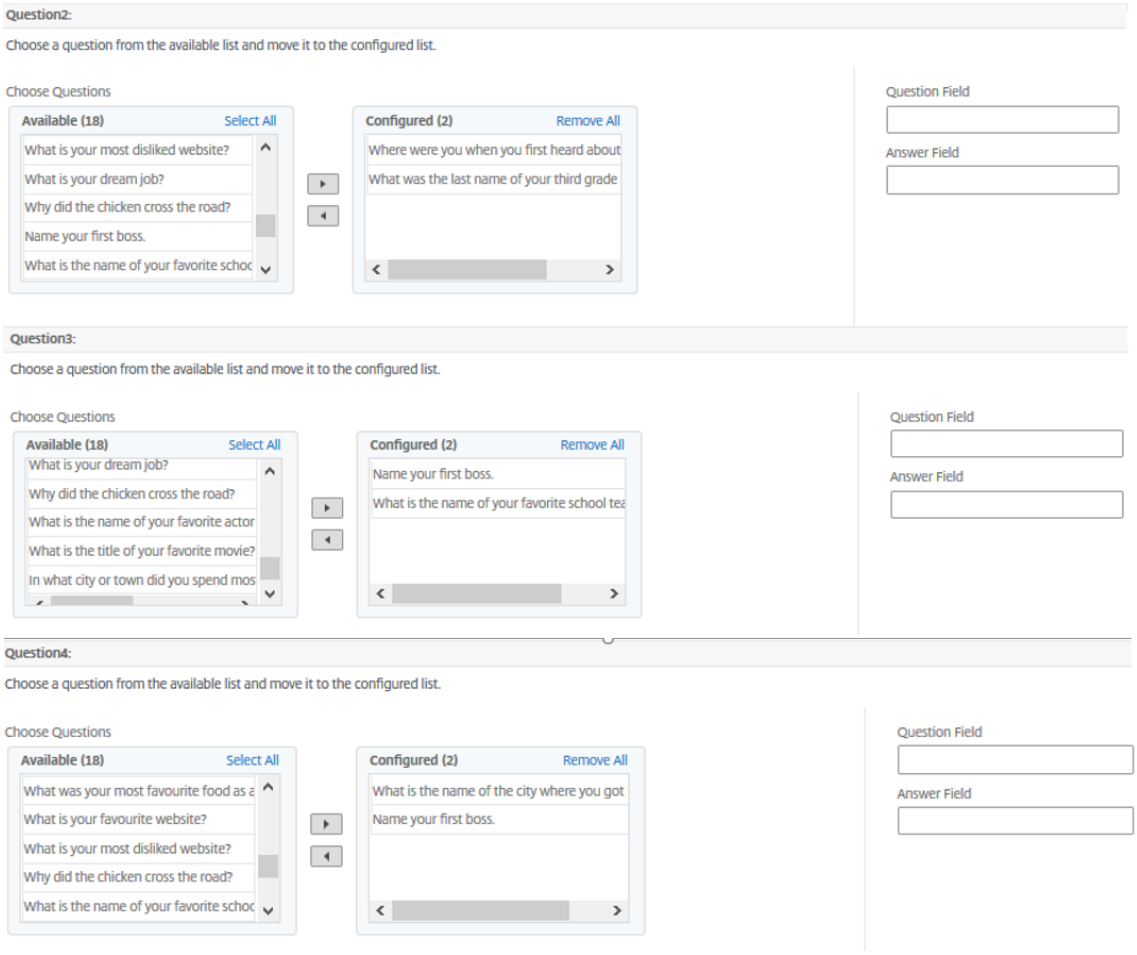
Um das wissensbasierte Frage-und-Antwort-Registrierungsschema über die GUI abzuschließen

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Anmeldeschema**.

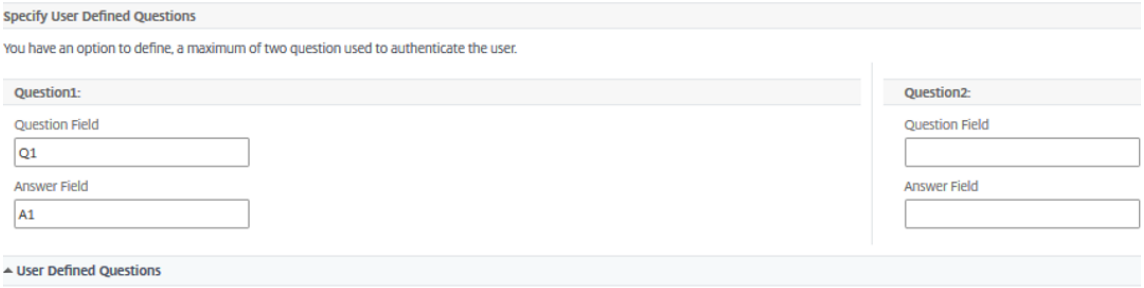


2. Klicken Sie auf der Seite **Anmeldeschema** auf **Profile**.
3. Klicken Sie auf **Anmeldeschema für die KBA-Registrierung hinzufügen**.
4. Geben Sie auf der Seite **Anmeldeschema für die Authentifizierung erstellen** einen Namen in das Feld **Schemaname** ein.

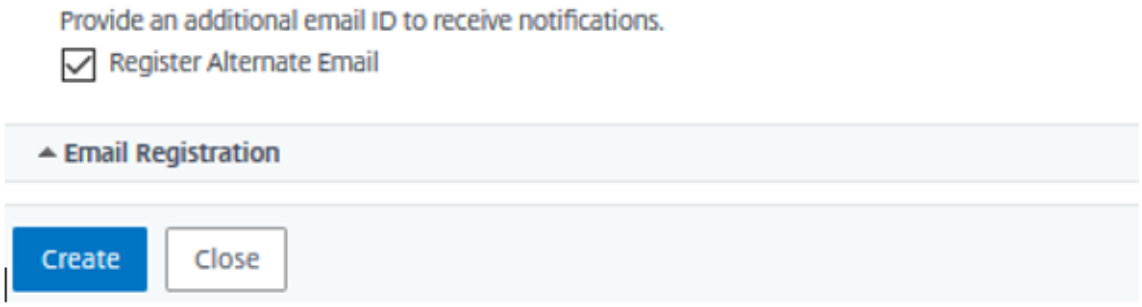




5. Wählen Sie die Fragen Ihrer Wahl aus und verschieben Sie sie in die Liste **Konfiguriert** .
6. Im Abschnitt **Benutzerdefinierte Fragen** können Sie Fragen und Antworten in den Feldern Q1 und A1 angeben.



7. Aktivieren Sie im Abschnitt **E-Mail-Registrierung** die Option **Alternative E-Mail registrieren** . Sie können die **alternative E-Mail-ID** auf der Anmeldeseite der Benutzerregistrierung registrieren, um das OTP zu erhalten.



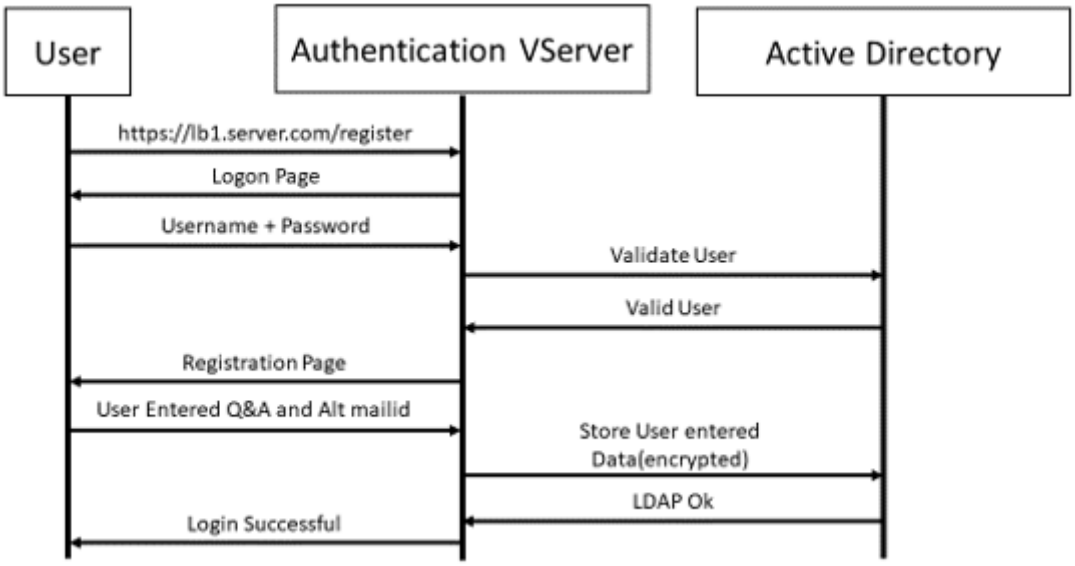
8. Klicken Sie auf **Erstellen**. Das einmal generierte Anmeldeschema zeigt dem Endbenutzer während des Registrierungsvorgangs alle konfigurierten Fragen an.

Workflow für die Benutzerregistrierung und -verwaltung über die CLI erstellen

Folgendes ist erforderlich, bevor Sie mit der Konfiguration beginnen:

- Dem virtuellen Authentifizierungsserver zugewiesene IP-Adresse
- FQDN entspricht der zugewiesenen IP-Adresse
- Serverzertifikat für Authentifizierung virtueller Server

Um die Geräteregistrierungs- und Verwaltungsseite einzurichten, benötigen Sie einen virtuellen Authentifizierungsserver. Die folgende Abbildung veranschaulicht die Benutzerregistrierung.



So erstellen Sie einen virtuellen Authentifizierungsserver

1. Konfigurieren Sie einen virtuellen Authentifizierungsserver. Es muss vom Typ SSL sein und stellen Sie sicher, dass Authentifizierungsserver mit Portalthema zu binden.


```
> add authentication vserver <vServerName> SSL <ipaddress> <port>
> bind authentication vserver <vServerName> [-portaltheme<string>]
```

2. Binden Sie SSL Virtual Server Certificate-Key-Paar.

```
> bind ssl vserver <vServerName> certkeyName <string>
```

Beispiel:

```
> add authentication vserver authvs SSL 1.2.3.4 443
> bind authentication vserver authvs -portaltheme RFWebUI
> bind ssl vserver authvs -certkeyname c1
```

So erstellen Sie eine LDAP-Anmeldeaktion

```
    > add authentication ldapAction <name> {
-serverIP <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE> ]
     [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
    ldapLoginName <USER FORMAT>]
```

> **Hinweis**
>
> Sie können jede Authentifizierungsrichtlinie als ersten Faktor konfigurieren.

Beispiel:

```
    > add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
       -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
      ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
      PASSWORD -ldapLoginName samAccountName -serverport 636 -sectype
      SSL -KBAttribute userParameters
```

So erstellen Sie eine Authentifizierungsrichtlinie für die LDAP-Anmeldung

```
    > add authentication policy <name> <rule> [<reqAction]
```

Beispiel:

```
    > add authentication policy ldap_logon -rule true -action
       ldap_logon_action
```


So erstellen Sie eine wissensbasierte Frage- und Antwortregistrierungsaktion

Zwei neue Parameter werden in `ldapAction` eingeführt. `KBAttribute` für die KBA-Authentifizierung (Registrierung und Validierung) und `alternateEmailAttr` für die Registrierung der alternativen E-Mail-ID des Benutzers.

```
1     > add authentication ldapAction <name> {
2  -serverIP  <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE>
      ] [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
      ldapLoginName <USER FORMAT>] [-KBAttribute <LDAP ATTRIBUTE>] [-
      alternateEmailAttr <LDAP ATTRIBUTE>]
```

Beispiel:

```
1     > add authentication ldapAction ldap1 -serverIP 1.2.3.4 -sectype
         ssl -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
         ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
         PASSWORD -ldapLoginName samAccountName -KBAttribute
         userParameters -alternateEmailAttr userParameters
```

Anzeige der Benutzerregistrierung und -verwaltung

Das Anmeldeschema “KBARegistrationSchema.xml” wird verwendet, um dem Endbenutzer die Benutzerregistrierungsseite anzuzeigen. Verwenden Sie die folgende Befehlszeilenschnittstelle, um das Anmeldeschema anzuzeigen.

```
1 > add authentication loginSchema <name> -authenticationSchema <string>
```

Beispiel:

```
1 > add authentication loginSchema kba_register -authenticationSchema /
     nsconfig/loginschema/LoginSchema/KBARegistrationSchema.xml
```

Citrix empfiehlt zwei Möglichkeiten zur Anzeige der Benutzerregistrierung und -verwaltung: URL oder LDAP-Attribut.

Verwenden von URL

Wenn der URL-Pfad “/register” enthält (z. B. https://lb1.server.com/register), wird die Benutzerregistrierungsseite unter Verwendung der URL angezeigt.

So erstellen und binden Sie die Registrierungsrichtlinie


```
> add authentication policylabel user_registration -loginSchema
    kba_register
> add authentication policy ldap1 -rule true -action ldap1
> bind authentication policylabel user_registration -policy ldap1 -
    priority 1
```

So binden Sie die Authentifizierungsrichtlinie an Authentifizierungs-, Autorisierungs- und Überwachungsserver, wenn die URL '/register' enthält

```
> add authentication policy ldap_logon -rule "http.req.cookie.value(\"
    NSC_TASS\").contains(\"register\")" -action ldap_logon
> bind authentication vserver authvs -policy ldap_logon -nextfactor
    user_registration -priority 1
```

So binden Sie Zertifikat an VPN global

```
bind vpn global -userDataEncryptionKey c1
```

> **Hinweis**
>
> - Sie müssen das Zertifikat binden, um die Benutzerdaten (KB Q&A und registrierte alternative E-Mail-ID) zu verschlüsseln, die im AD-Attribut gespeichert sind.
> - Wenn das Zertifikat abläuft, müssen Sie ein neues Zertifikat binden und die Registrierung erneut durchführen.

Verwenden des Attributs

Sie können eine Authentifizierungsrichtlinie an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver binden, um zu überprüfen, ob der Benutzer bereits registriert ist oder nicht. In diesem Ablauf muss jede der vorhergehenden Richtlinien vor dem wissensbasierten Frage- und Antwortregistrierungsfaktor LDAP mit dem konfigurierten KBA-Attribut sein. Hiermit wird überprüft, ob der AD-Benutzer registriert ist oder nicht ein AD-Attribut verwendet.

> **Wichtig**
>
> Die Regel "AAA.USER.ATTRIBUTE("kba_registered").EQ("0")" zwingt neue Benutzer, sich für wissensbasierte Fragen zu registrieren und alternative E-Mails zu beantworten.

So erstellen Sie eine Authentifizierungsrichtlinie, um zu überprüfen, ob der Benutzer noch nicht registriert ist


```
> add authentication policy switch_to_kba_register -rule "AAA.USER.
    ATTRIBUTE(\"kba_registered\").EQ(\"0\")" -action NO_AUTHN
> add authentication policy first_time_login_forced_kba_registration -
    rule true -action ldap1
```

So erstellen Sie ein Registrierungsrichtlinienlabel und binden es an die LDAP-Registrierungsrichtlinie

```
> add authentication policylabel auth_or_switch_register -loginSchema
    LSCHEMA_INT
> add authentication policylabel kba_registration -loginSchema
    kba_register

> bind authentication policylabel auth_or_switch_register -policy
    switch_to_kba_register -priority 1 -nextFactor kba_registration
> bind authentication policylabel kba_registration -policy
    first_time_login_forced_kba_registration -priority 1
```

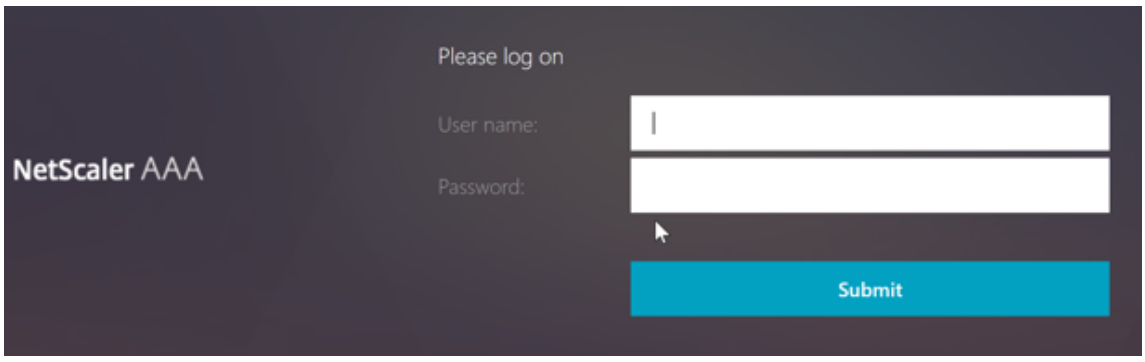
So binden Sie die Authentifizierungsrichtlinie an Authentifizierungs-, Autorisierungs- und Überwachungsserver des virtuellen Servers

```
bind authentication vserver authvs -policy ldap_logon -nextfactor
    auth_or_switch_register -priority 2
```

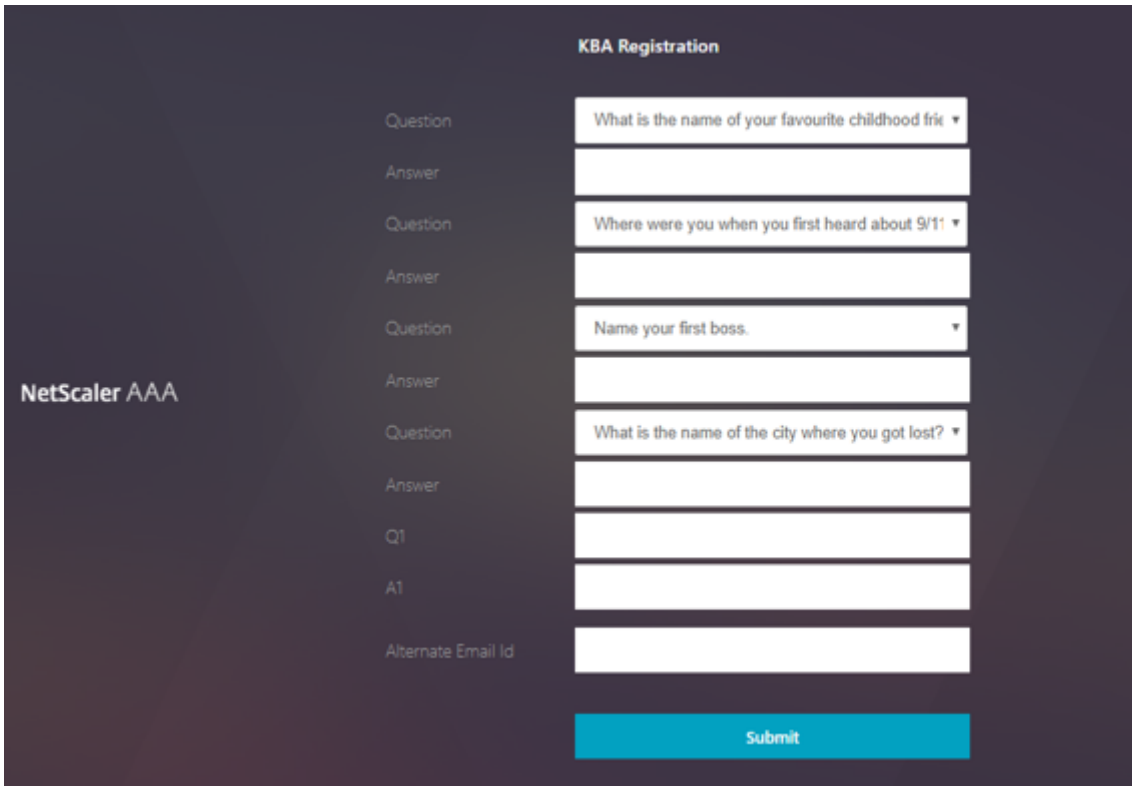
Benutzerregistrierung und Management-Validierung

Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, muss der folgende UI-Bildschirm angezeigt werden.

1. Geben Sie die URL des virtuellen Servers lb ein, z. B. https://lb1.server.com. Der Anmeldebildschirm wird angezeigt.



2. Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf **Submit**. Der Bildschirm **Benutzerregistrierung** wird angezeigt.



3. Wählen Sie die bevorzugte Frage aus der Dropdown-Liste aus und geben Sie die **Antwort** ein.
4. Klicken Sie auf **Submit**. Der Bildschirm mit der erfolgreichen Benutzerregistrierung wird angezeigt.

Benutzeranmeldeseite konfigurieren

In diesem Beispiel geht der Administrator davon aus, dass der erste Faktor die LDAP-Anmeldung ist (für die der Endbenutzer das Kennwort vergessen hat). Der Benutzer folgt dann der wissensbasierten Frage- und Antwortregistrierung und der OTP-Validierung der E-Mail-ID und setzt das Kennwort schließlich mithilfe des Self-Service-Kennwortrücksetzens zurück.

Sie können jeden der Authentifizierungsmechanismen für das Zurücksetzen des Self-Service-Kennworts verwenden. Citrix empfiehlt, entweder eine wissensbasierte Frage und Antwort zu haben und OTP per E-Mail oder beides zu senden, um einen starken Datenschutz zu gewährleisten und unrechtmäßige Rücksetzungen von Benutzerkennwörtern zu vermeiden.

Folgendes ist erforderlich, bevor Sie mit der Konfiguration der Benutzeranmeldeseite beginnen:

- IP für virtuellen Load-Balancer-Server
- Entsprechender FQDN für den virtuellen Load Balancer-Server
- Serverzertifikat für den Load Balancer

Erstellen eines virtuellen Load Balancer-Servers über die CLI

Um auf die interne Website zuzugreifen, müssen Sie einen virtuellen LB-Server erstellen, um den Back-End-Dienst zu starten und die Authentifizierungslogik an den virtuellen Authentifizierungsserver zu delegieren.

```
> add lb vserver lb1 SSL 1.2.3.162 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost otpauth.server.com -
   Authentication ON -authnVsName authvs

> bind ssl vserver lb1 -certkeyname c1
```

So stellen Sie den Back-End-Dienst beim Lastenausgleich dar:

```
> add service iis_backendsso_server_com 1.2.3.4 HTTP 80

> bind lb vserver lb1 iis_backendsso_server_com
```

LDAP-Aktion mit deaktivierter Authentifizierung als erste Richtlinie erstellen

```
> add authentication ldapAction ldap3 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
   administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
   ldapLoginName samAccountName -authentication disabled

> add authentication policy ldap3 -rule aaa.LOGIN.VALUE("passwdreset").
   EQ("1") -action ldap3
```

Erstellen einer wissensbasierten Frage- und Antwortvalidierungsaktion

Für die wissensbasierte Frage- und Antwortvalidierung im Self-Service-Ablauf zum Zurücksetzen des Kennworts müssen Sie den LDAP-Server mit deaktivierter Authentifizierung konfigurieren.

```
> add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP
   > -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
   ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
   KBAttribute  <LDAP ATTRIBUTE> - alternateEmailAttr <LDAP ATTRIBUTE>
   -authentication DISABLED
```

Beispiel:

```
> add authentication ldapAction ldap2 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
```



```
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
ldapLoginName samAccountName -KBAttribute userParameters -
alternateEmailAttr userParameters -authentication disabled
```

So erstellen Sie eine Authentifizierungsrichtlinie für die wissensbasierte Frage- und Antwortvalidierung mit CLI

```
add authentication policy kba_validation -rule true -action ldap2
```

Erstellen einer E-Mail-Validierungsaktion

LDAP muss ein wichtiger Faktor für den E-Mail-Validierungsfaktor sein, da Sie die E-Mail-ID oder die alternative E-Mail-ID des Benutzers als Teil der Registrierung zum Zurücksetzen des Kennworts im Self-Service benötigen.

> **Hinweis:**
>
> Damit die E-Mail-OTP-Lösung funktioniert, stellen Sie sicher, dass die anmeldungsbasierte Authentifizierung auf dem SMTP-Server aktiviert ist.

Um sicherzustellen, dass die anmeldungsbasierte Authentifizierung aktiviert ist, geben Sie den folgenden Befehl auf dem SMTP-Server ein. Wenn die auf Anmeldung basierende Authentifizierung aktiviert ist, stellen Sie fest, dass der Text **AUTH LOGIN** in der Ausgabe fett gedruckt erscheint.

```
root@ns# telnet <IP address of the SMTP server><Port number of the
   server>
ehlo
```

Beispiel:

```
root@ns# telnet 10.106.3.66 25
Trying 10.106.3.66...
Connected to 10.106.3.66.
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22
   Nov 2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.41.151]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
```



```
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
```

Weitere Informationen zum Aktivieren der anmeldungsbasierten Authentifizierung finden Sie unter https://support.microfocus.com/kb/doc.php?id=7020367.

So konfigurieren Sie E-Mail-Aktion mit CLI

```
add authentication emailAction emailact -userName sender@example.com -
    password <Password> -serverURL "smtps://smtp.example.com:25" -
    content "OTP is $code"
```

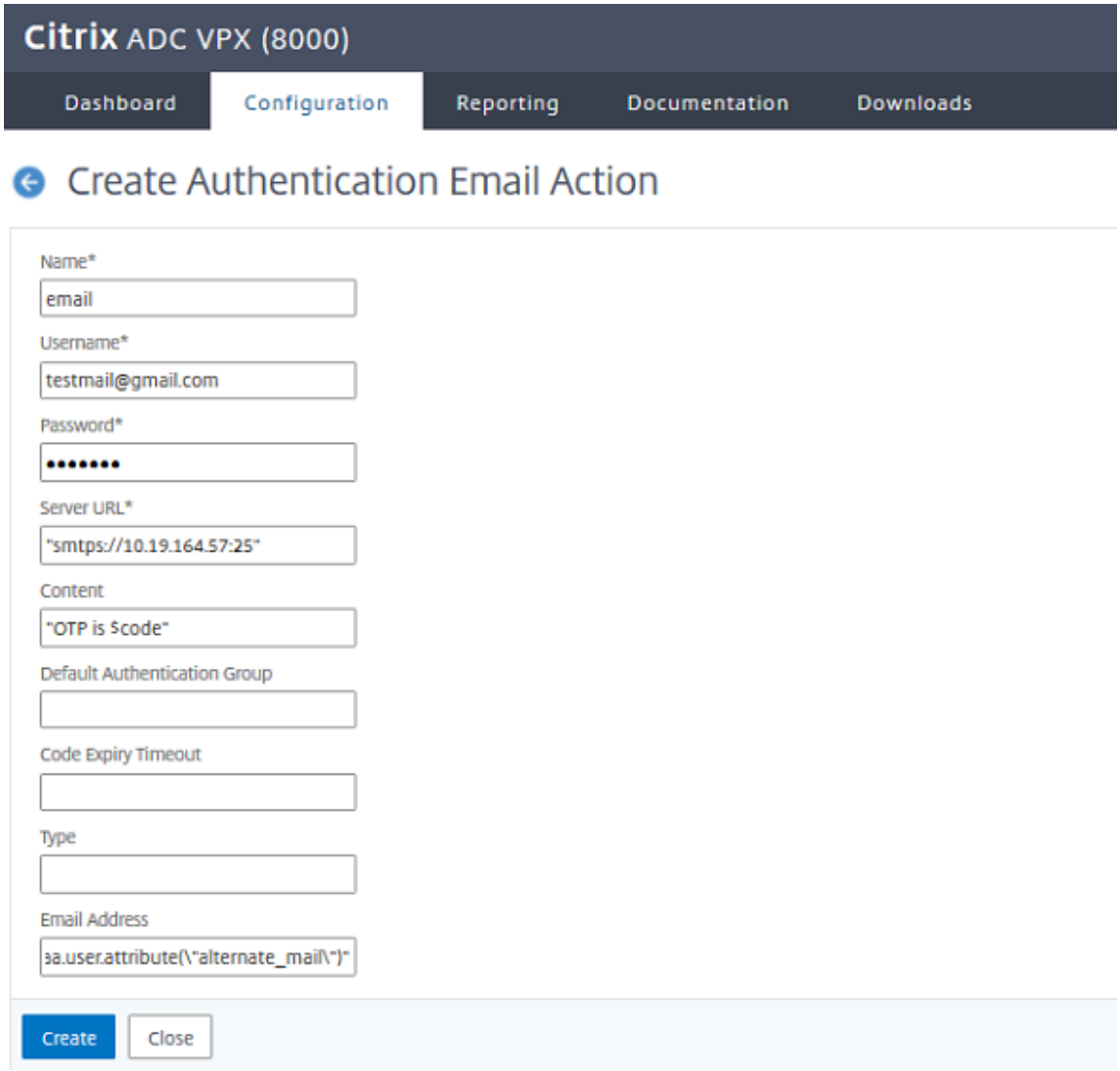
Beispiel:

```
add authentication emailAction email -userName testmail@gmail.com -
    password 298
    a34b1a1b7626cd5902bbb416d04076e5ac4f357532e949db94c0534832670 -
    encrypted -encryptmethod ENCMTHD_3 -serverURL "smtps
    ://10.19.164.57:25" -content "OTP is $code" -emailAddress "aaa.user.
    attribute(\"alternate_mail\")"
```

> **Hinweis**
>
> Der Parameter “EmailAddress” in der Konfiguration ist ein PI-Ausdruck. Daher ist dies so konfiguriert, dass entweder die standardmäßige Benutzer-E-Mail-ID aus der Sitzung oder die bereits registrierte alternative E-Mail-ID übernommen wird.

Konfigurieren der E-Mail-ID über die GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > E-Mail-Aktion für Authentifizierung**. Klicken Sie auf **Hinzufügen**.
2. Füllen Sie auf der Seite **Authentifizierungs-E-Mail-Aktion erstellen** die Details aus und klicken Sie auf **Erstellen**.



So erstellen Sie über die CLI eine Authentifizierungsrichtlinie für die E-Mail-Validierung

```
1 add authentication policy email_validation -rule true -action email
```

Erstellen einer Authentifizierungsrichtlinie für den Kennwortrücksetzfaktor

```
1 add authentication policy ldap_pwd -rule true -action ldap_logon_action
```

Präsentieren der Benutzeroberfläche über das Anmeldeschema

Es gibt drei LoginSchemas zum Zurücksetzen des Kennworts im Self-Service, um das Kennwort zurückzusetzen. Verwenden Sie die folgenden CLI-Befehle, um die drei Login-Schema anzuzeigen:


```
root@ns# cd  /nsconfig/loginschema/LoginSchema/
root@ns# ls -ltr | grep -i password
-r--r--r--  1 nobody  wheel  2088 Nov 13 08:38
   SingleAuthPasswordResetRem.xml
-r--r--r--  1 nobody  wheel  1541 Nov 13 08:38
   OnlyUsernamePasswordReset.xml
-r--r--r--  1 nobody  wheel  1391 Nov 13 08:38 OnlyPassword.xml
```

So erstellen Sie das Zurücksetzen einzelner Authentifizierungskennworte mit der CLI

```
> add authentication loginSchema lschema_password_reset -
   authenticationSchema "/nsconfig/loginschema/LoginSchema/
   SingleAuthPasswordResetRem.xml"

> add authentication loginSchemaPolicy lpol_password_reset -rule true -
   action lschema_password_reset
```

Erstellen eines wissensbasierten Frage-, Antwort- und E-Mail-OTP-Validierungsfaktors über Richtlinienlabel

Wenn der erste Faktor die LDAP-Anmeldung ist, können Sie mit der folgenden Befehle eine wissensbasierte Frage erstellen und OTP-Richtlinienbeschriftungen für den nächsten Faktor senden.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel kba_validation -loginSchema
   lschema_noschema

> add authentication policylabel email_validation -loginSchema
   lschema_noschema
```

Kennwortrücksetzungsfaktor über Richtlinienbezeichnung erstellen

Sie können den Kennwortrücksetzfaktor mithilfe der folgenden Befehle über die Policy Label erstellen.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

```



```
3 > add authentication policylabel password_reset -loginSchema
    lschema_noschema
4
5 > bind authentication policylabel password_reset -policyName ldap_pwd -
    priority 10 -gotoPriorityExpression NEXT
```

Binden Sie die wissensbasierte Frage-, Antwort- und E-Mail-Richtlinie mit den vorherigen erstellten Richtlinien mit den folgenden Befehlen.

```
1 > bind authentication policylabel email_validation -policyName
    email_validation -nextfactor password_reset -priority 10 -
    gotoPriorityExpression NEXT
2
3 > bind authentication policylabel kba_validation -policyName
    kba_validation -nextfactor email_validation -priority 10 -
    gotoPriorityExpression NEXT
```

Flow binden

Sie müssen den LDAP-Anmeldeablauf gemäß der Authentifizierungsrichtlinie für die LDAP-Anmeldung erstellt haben. In diesem Ablauf klickt der Benutzer auf den Link Kennwort vergessen, der auf der ersten LDAP-Anmeldeseite angezeigt wird, dann auf die KBA-Validierung, gefolgt von der OTP-Validierung und schließlich auf die Seite zum Zurücksetzen des Kennworts.

```
1 bind authentication vserver authvs -policy ldap3 -nextfactor
    kba_validation -priority 10 -gotoPriorityExpression NEXT
```

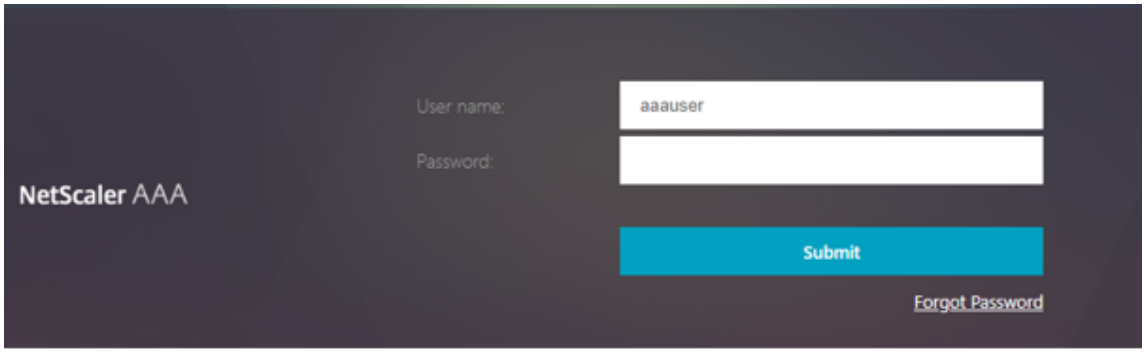
So binden Sie den gesamten UI-Flow

```
1 bind authentication vserver authvs -policy lpol_password_reset -
    priority 20 -gotoPriorityExpression END
```

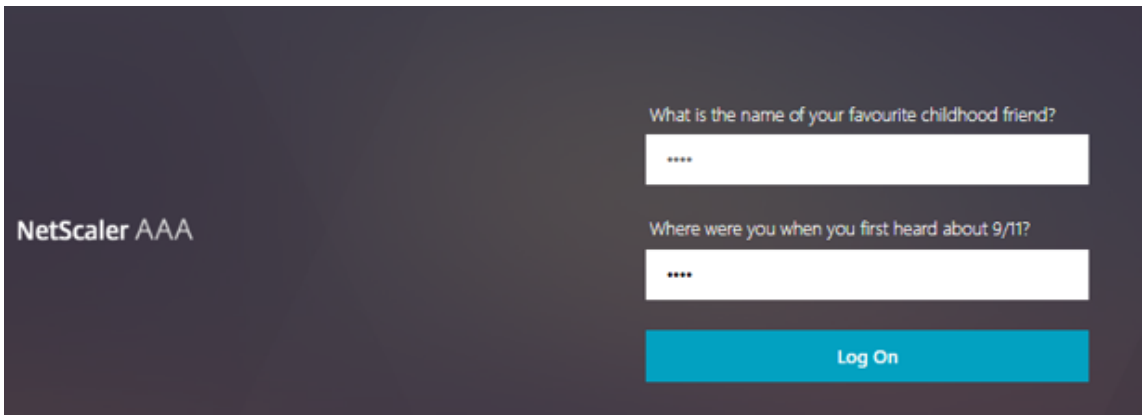
Workflow für Benutzeranmeldung zum Zurücksetzen des Kennworts

Es folgt ein Workflow für die Benutzeranmeldung, wenn der Benutzer das Kennwort zurücksetzen muss:

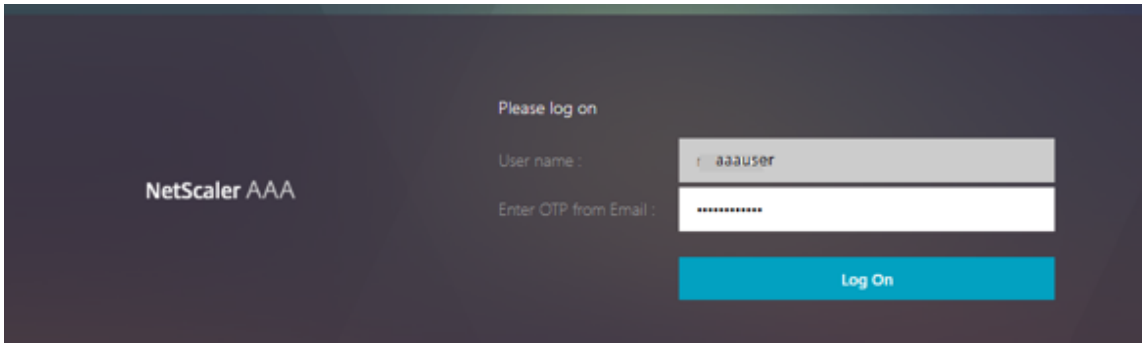
1. Geben Sie die URL des virtuellen Servers lb ein, z. B. https://lb1.server.com. Der Anmeldebildschirm wird angezeigt.



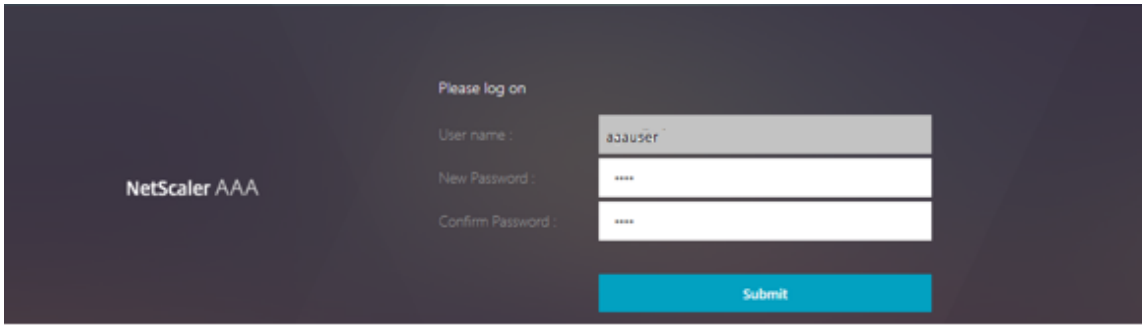
2. Klicken Sie auf **Kennwort vergessen**. Auf einem Validierungsbildschirm werden zwei Fragen von maximal sechs Fragen und Antworten angezeigt, die für einen AD-Benutzer registriert wurden.



3. Beantworten Sie die Fragen und klicken Sie **auf Anmelden**. Ein E-Mail-OTP-Validierungsbildschirm, in dem Sie das OTP eingeben müssen, das Sie mit der registrierten alternativen E-Mail-ID erhalten haben, wird angezeigt.



4. Geben Sie die E-Mail OTP ein. Sobald die E-Mail-OTP-Validierung erfolgreich war, wird die Seite zum Zurücksetzen des Kennworts angezeigt.



5. Gib ein neues Kennwort ein und bestätige das neue Kennwort. Klicken Sie auf **Submit**. Nachdem das Zurücksetzen des Kennworts erfolgreich war, wird der Bildschirm zum erfolgreichen Zurücksetzen des Kennworts angezeigt.

Sie können sich jetzt mit dem Kennwort zum Zurücksetzen anmelden.

Problembehandlung

NetScaler bietet eine Option zur Behebung einiger der grundlegenden Probleme, die bei der Verwendung des Self-Service-Kennwortrücksetzens auftreten können. Der folgende Abschnitt hilft Ihnen bei der Behebung einiger Probleme, die in bestimmten Bereichen auftreten können.

NS-Protokoll

Vor der Analyse des Protokolls wird empfohlen, die Protokollstufe mit dem folgenden Befehl zu debuggen:

```
1 > set syslogparams -loglevel DEBUG
```

Registrierung

Die folgende Meldung weist auf eine erfolgreiche Benutzerregistrierung hin.


```
"ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1"
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  "
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw=="
```

Wissensbasierte Frage- und Antwortvalidierung

Die folgende Meldung zeigt eine erfolgreiche wissensbasierte Frage- und Antwortvalidierung an.

```
"NFactor: Successfully completed KBA Validation, nextfactor is email"
```

E-Mail-ID-Validierung

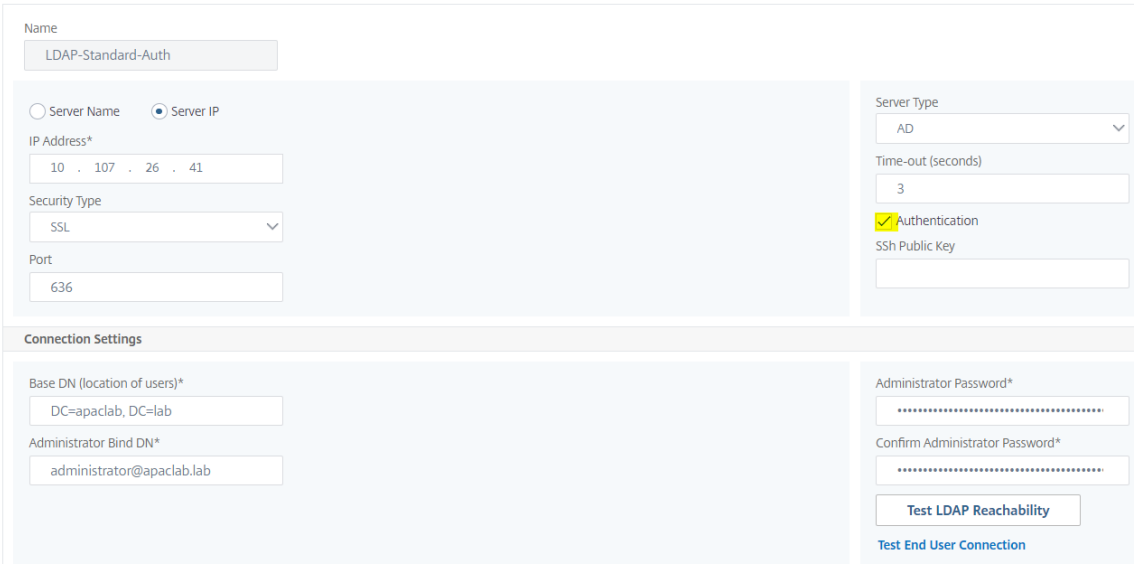
Die folgende Meldung zeigt an, dass das Kennwort erfolgreich zurückgesetzt wurde.

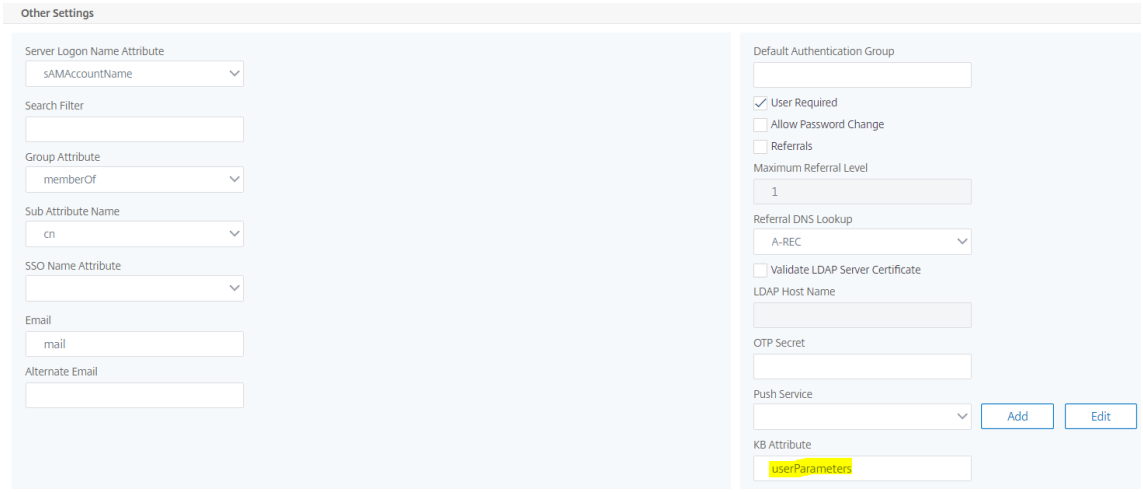
```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
```

Konfigurieren von SSPR mit nFactor Visualizer

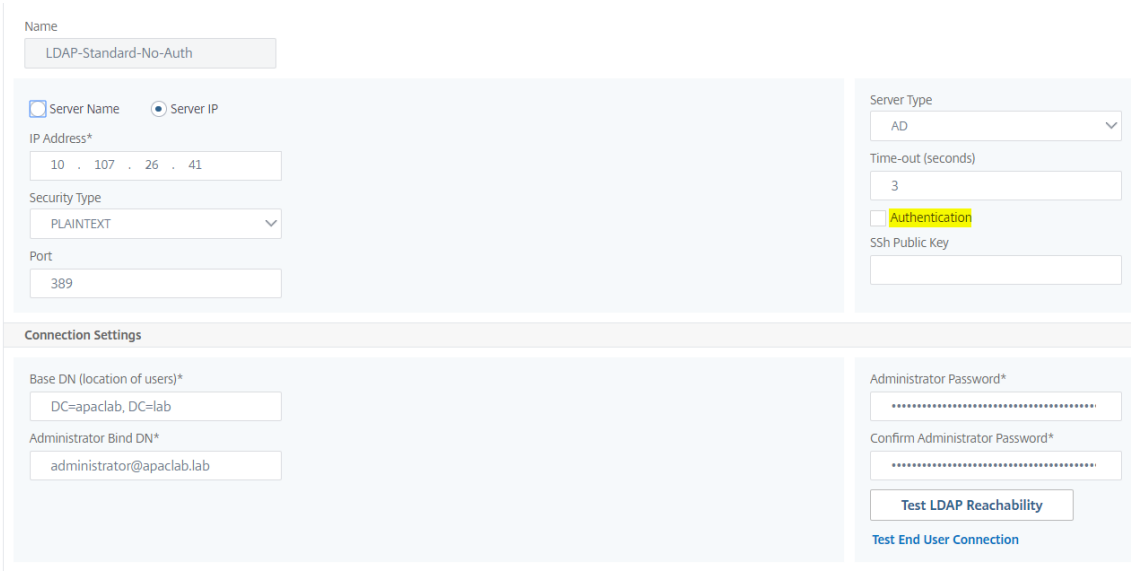
Bevor wir mit der SSPR-Konfiguration beginnen, müssen wir die folgenden LDAP-Server hinzufügen:

1. Standard-LDAP-Server mit aktivierter Authentifizierung für Benutzerauthentifizierung und angegebenem AD-Attribut.

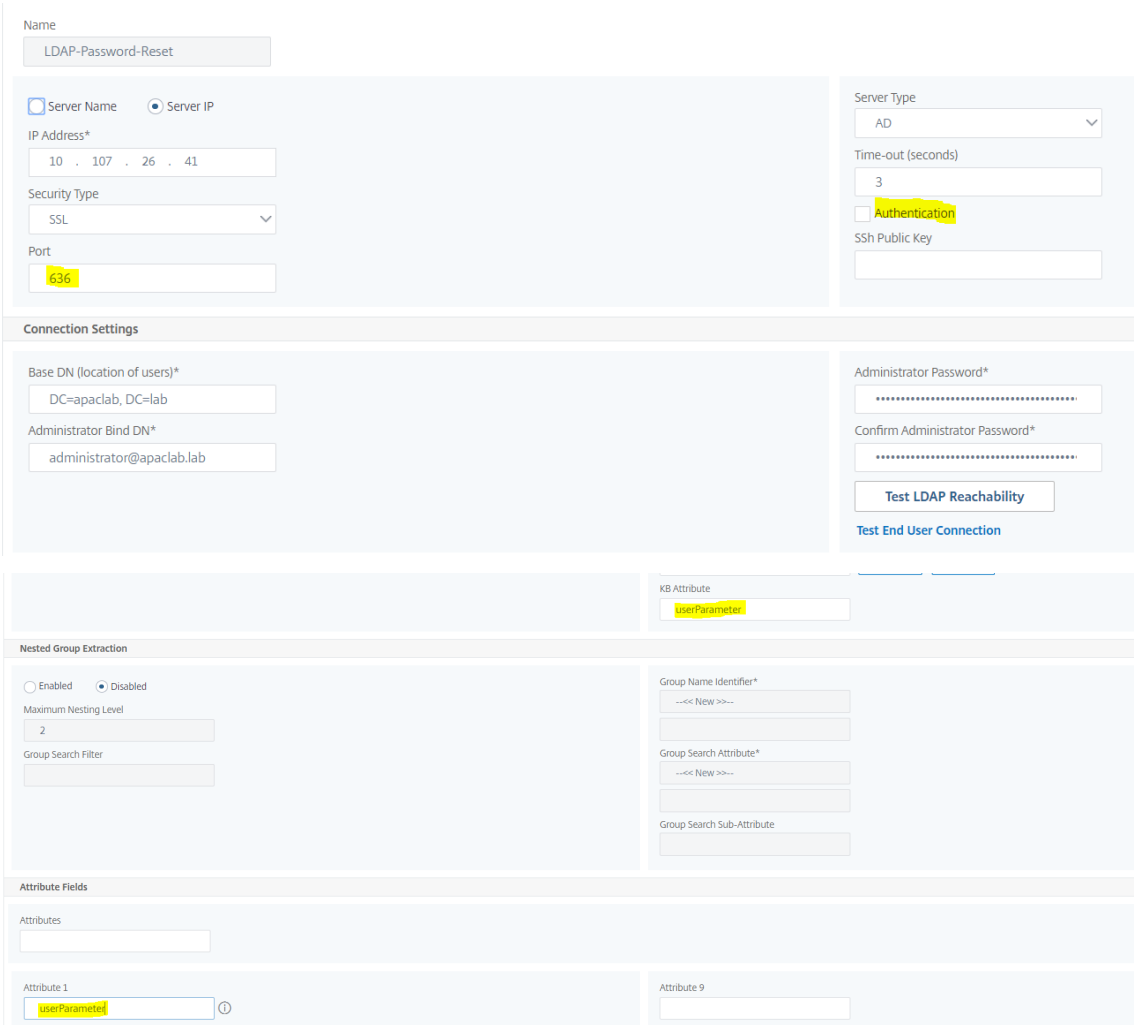




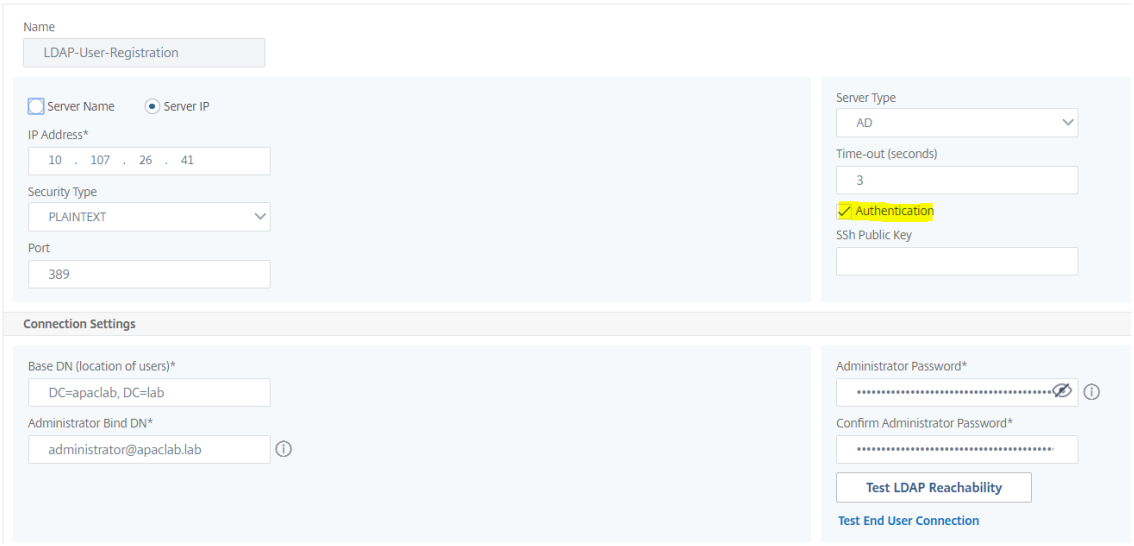
2. LDAP-Server für die Extraktion von Benutzerparametern ohne Authentifizierung.



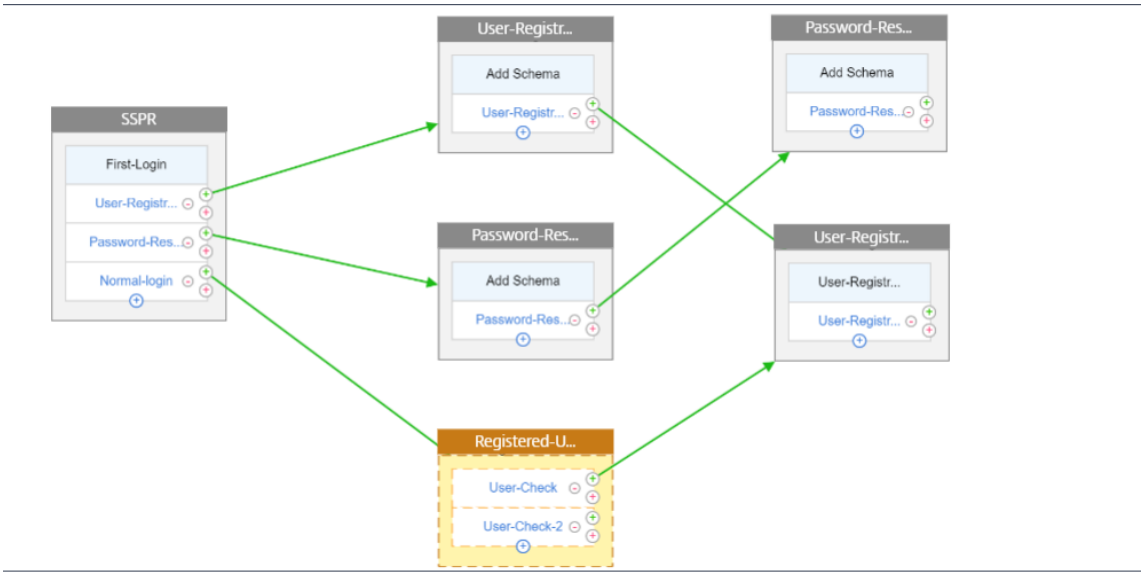
3. LDAP-Server zum Zurücksetzen des Kennworts auf SSL ohne Auth. Außerdem muss das AD-Attribut, das zum Speichern der Benutzerdetails verwendet werden soll, in diesem Server definiert werden.



4. LDAP-Server für Benutzerregistrierung mit aktivierter Authentifizierung und angegebenem AD-Attribut



5. Die folgende Abbildung zeigt den vollständigen Ablauf:



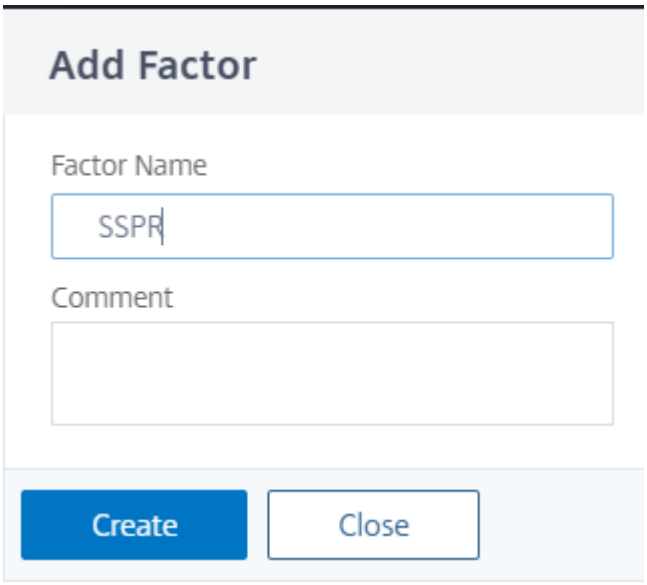
6. Binden Sie das Zertifikat global mithilfe des folgenden CLI-Befehls:

```
1 bind vpn global -userDataEncryptionKey Wildcard
```

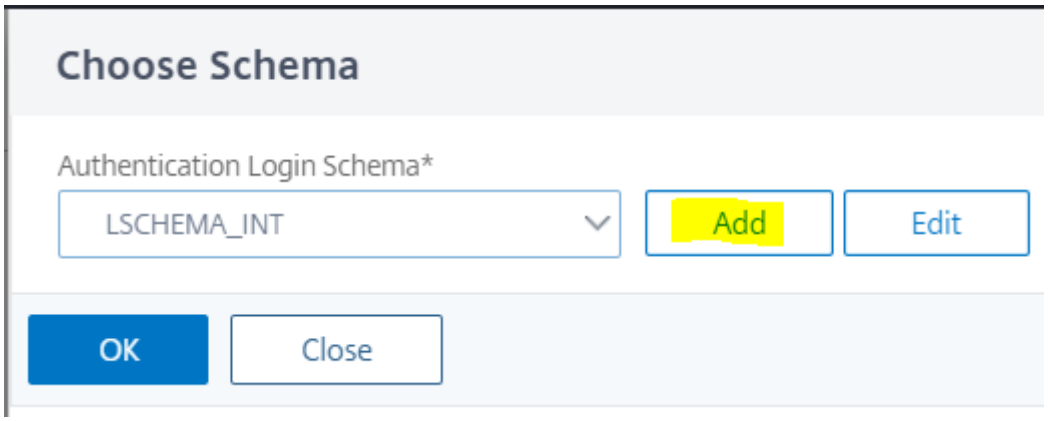
Nachdem die LDAP-Server hinzugefügt wurden, fahren Sie mit der nFactor-Konfiguration mit dem Visualizer fort

1. Navigieren Sie zu, **Sicherheit > AAA > Anwendungsdatenverkehr > nFactor Visualizer > nFactor Flows**, klicken Sie auf **Hinzufügen** und klicken Sie auf das Plus-Symbol im Feld.

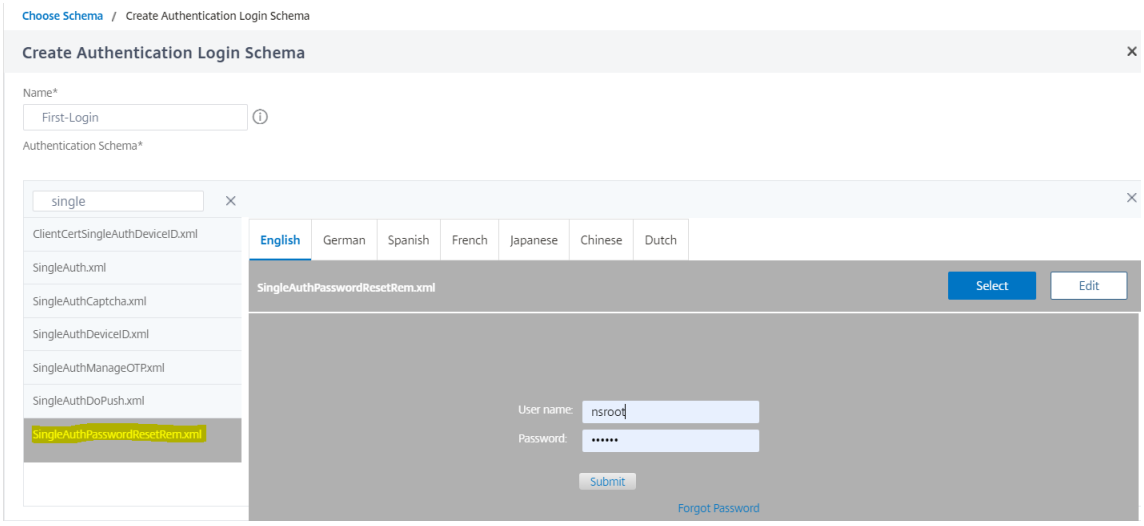
2. Gib dem Flow einen Namen.



3. Klicken Sie auf **Schema hinzufügen**, das als Standardschema dient. Klicken Sie auf der Anmeldeschemaseite auf **Hinzufügen** .



4. Nachdem Sie dem Schema einen Namen gegeben haben, wählen Sie das Schema aus. Klicken **Sie in der oberen rechten Ecke auf Auswählen**, um das Schema auszuwählen.



5. Klicken Sie auf **Erstellen** und dann auf **OK**.

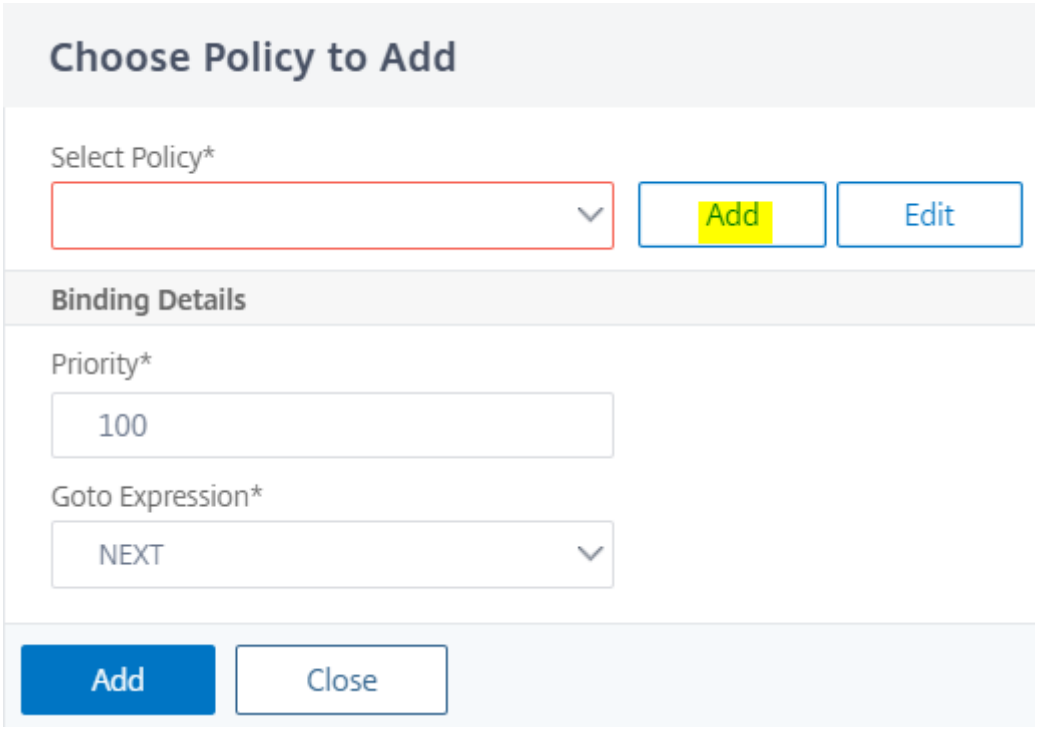
Sobald das Standardschema hinzugefügt wurde, müssen wir die folgenden drei Abläufe konfigurieren:

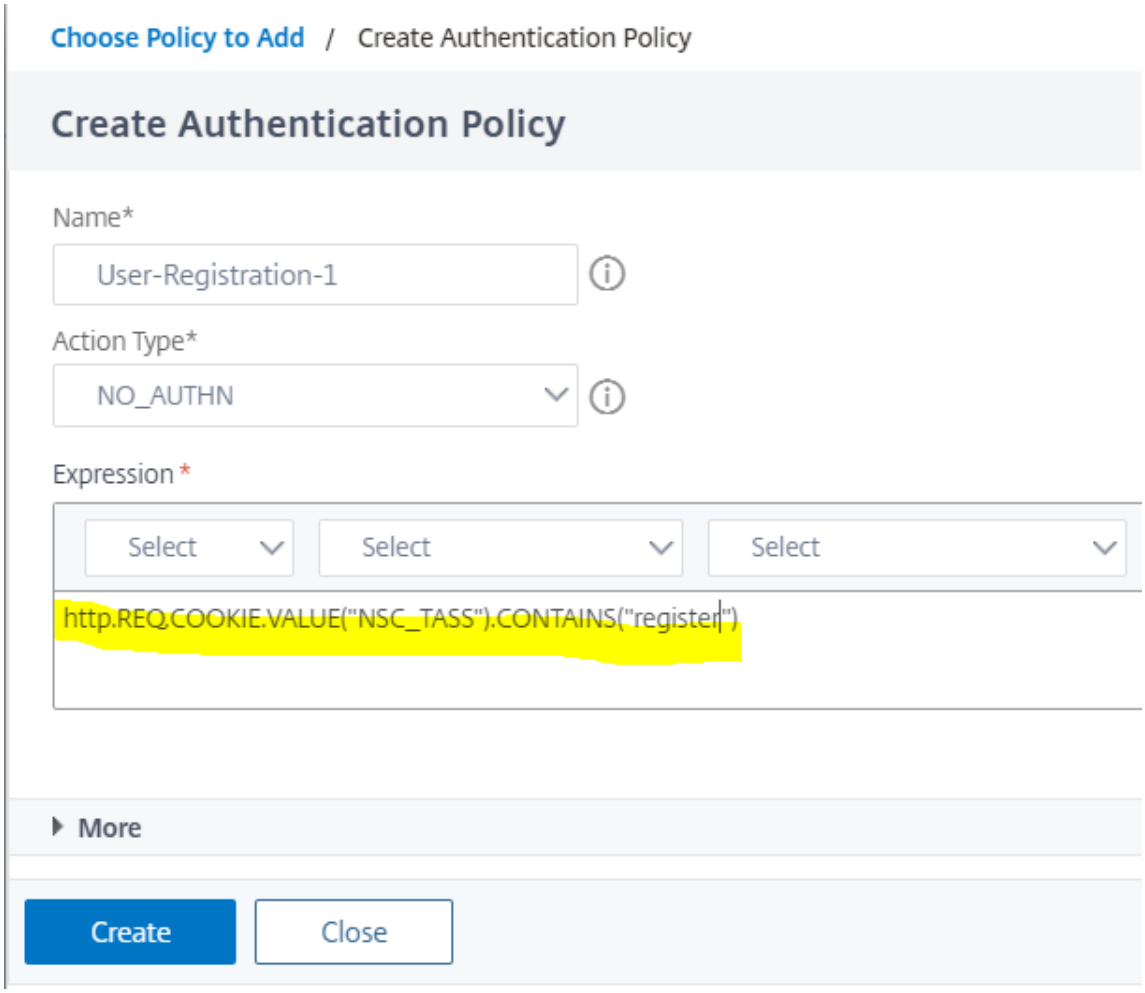
- **Benutzerregistrierung**: Für explizite Benutzerregistrierung
- **Kennwort zurücksetzen**: Zum Zurücksetzen des Kennworts
- **Normale Anmeldung + Prüfung registrierter Benutzer**: Falls der Benutzer registriert ist und das richtige Kennwort eingibt, ist der Benutzer angemeldet. Falls der Benutzer nicht registriert ist, wird der Benutzer zur Registrierungsseite weitergeleitet.

Registrierung von Benutzern

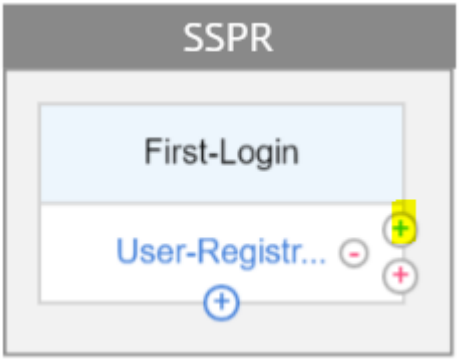
Lassen Sie uns dort weitermachen, wo wir nach dem Hinzufügen des Schemas gegangen sind.

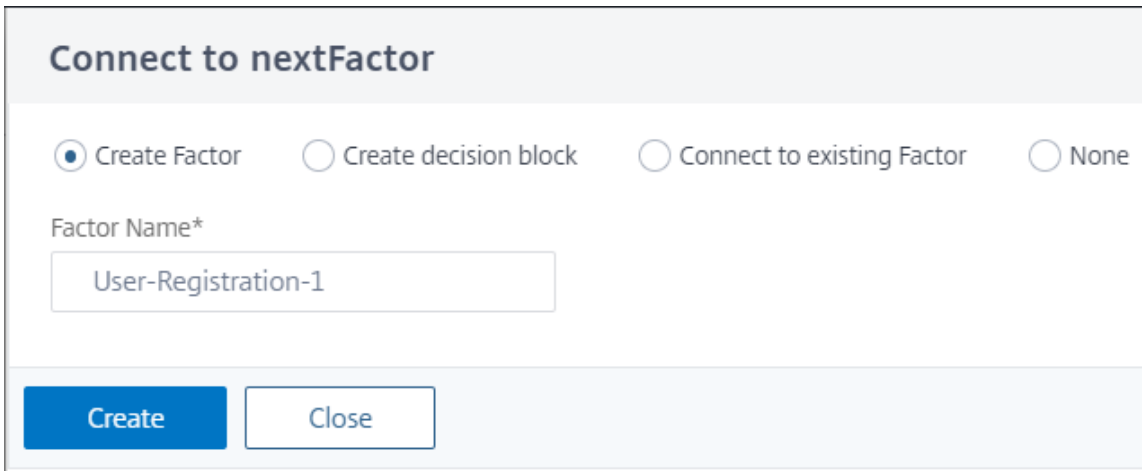
1. Klicken Sie auf **Richtlinie hinzufügen**, um zu überprüfen, ob der Benutzer versucht, sich explizit zu registrieren.



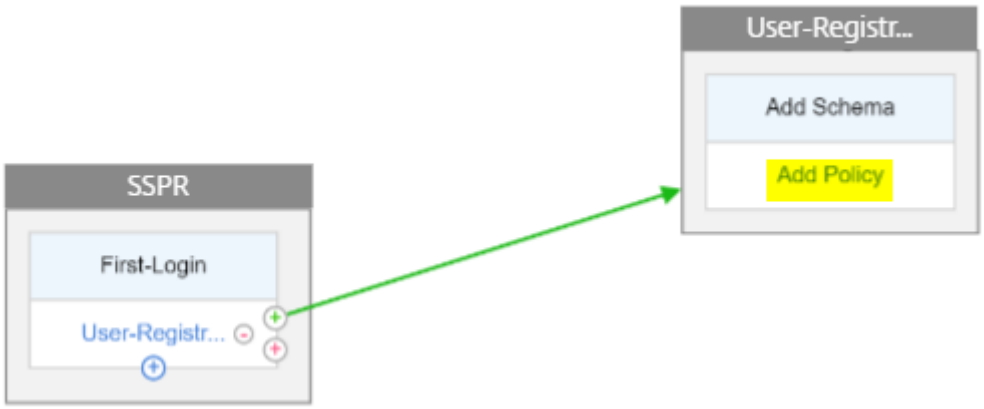


2. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
3. Klicken Sie auf das hervorgehobene grüne “+” -Symbol, um den nächsten Authentifizierungsfaktor zum Ablauf der Benutzerregistrierung hinzuzufügen.

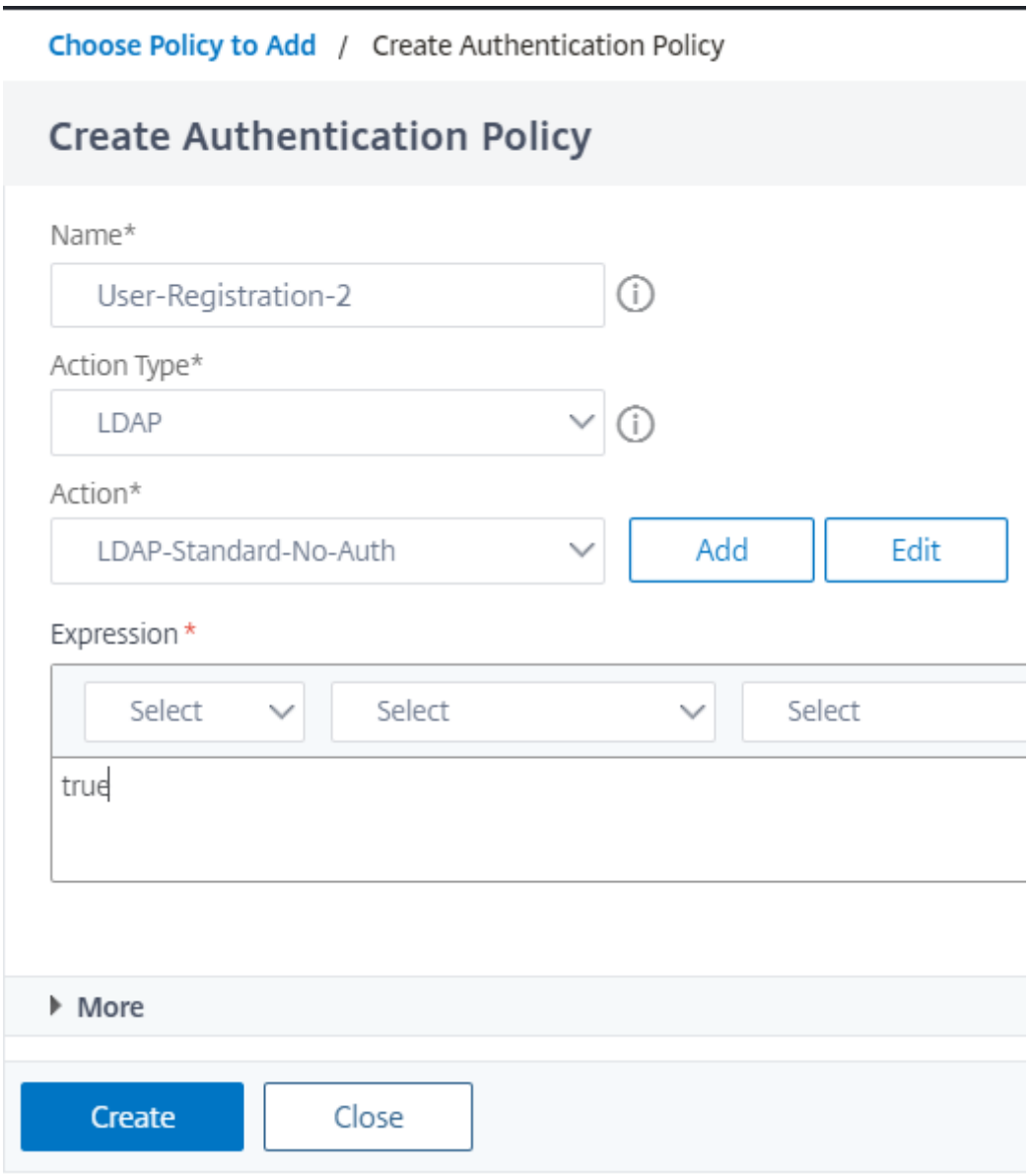




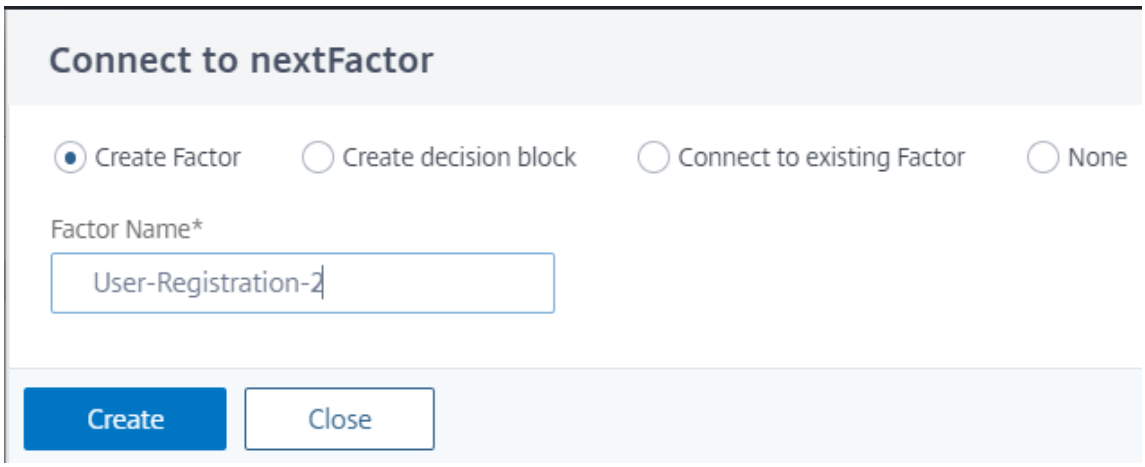
4. Klicken Sie auf **Erstellen**.
5. Klicken Sie auf **Richtlinie für den Faktor Benutzerregistrierung hinzufügen-1** .



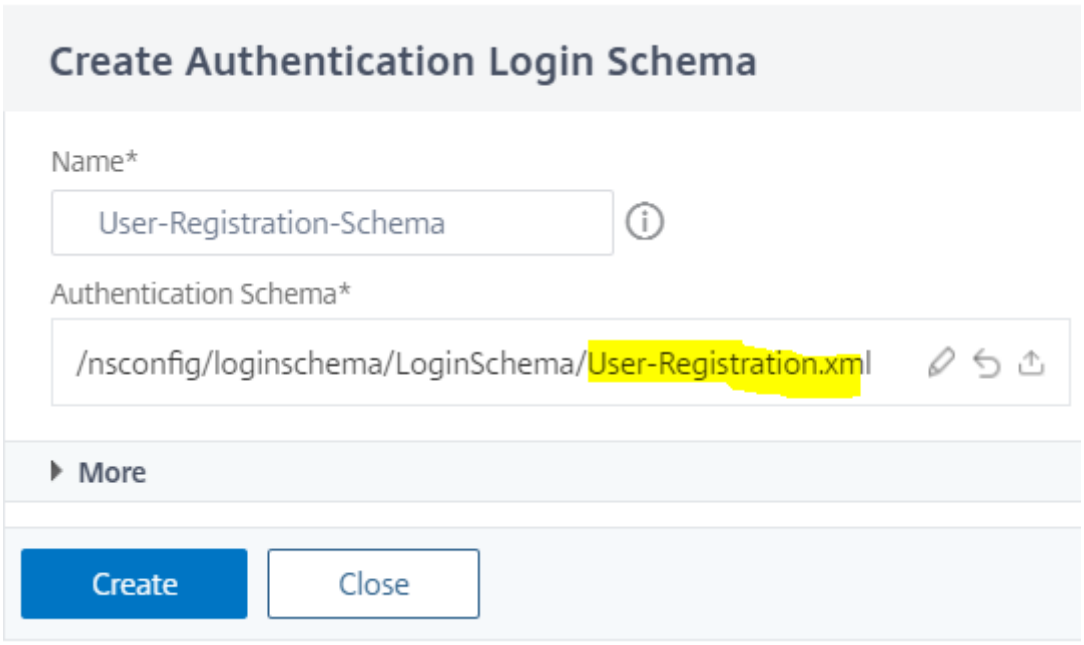
6. Erstellen Sie die Authentifizierungsrichtlinie. Diese Richtlinie extrahiert die Benutzerinformationen und validiert sie, bevor sie auf die Registrierungsseite umgeleitet werden.



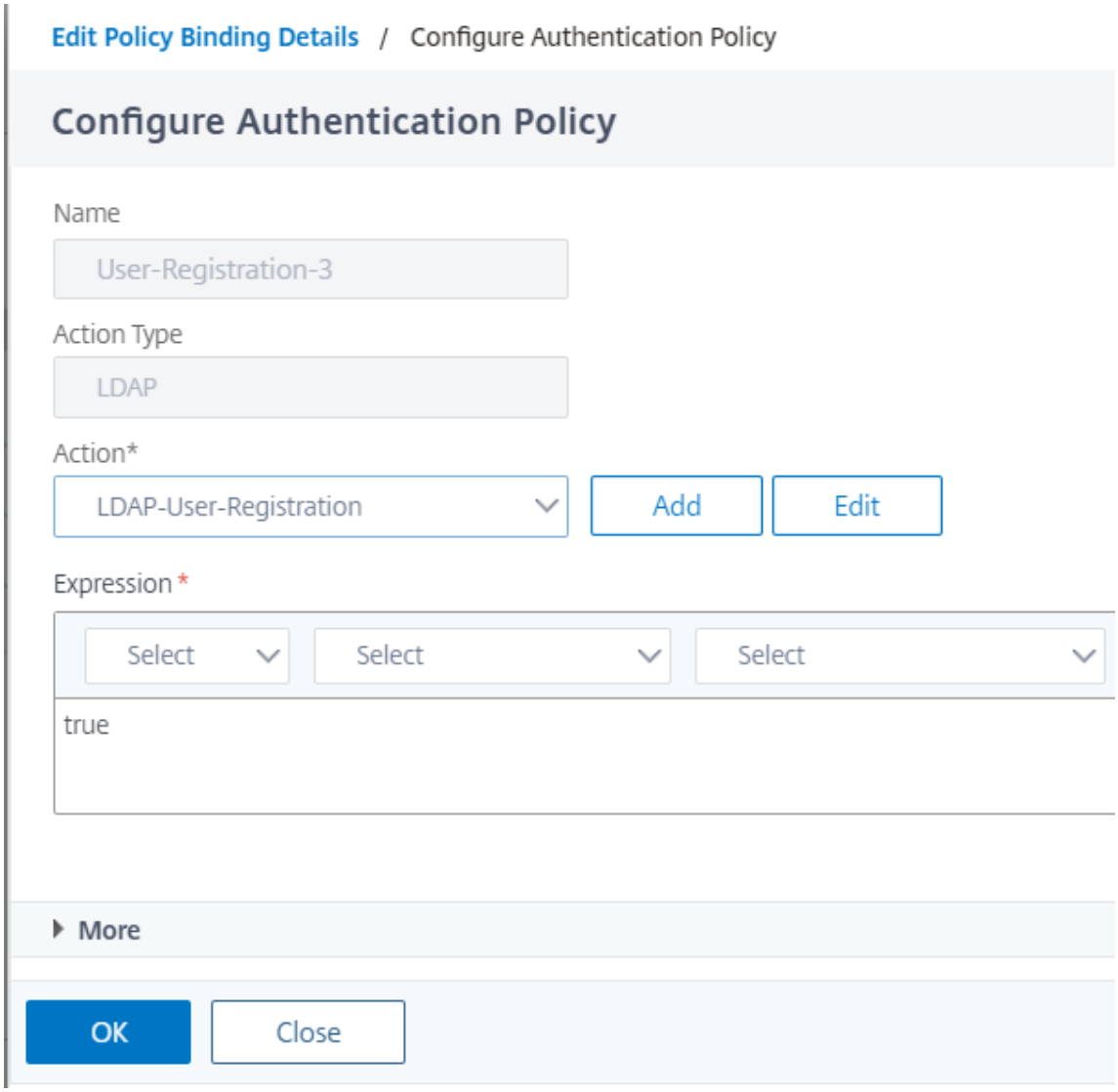
7. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
8. Klicken Sie nun auf das grüne “+” -Symbol, um einen weiteren Faktor für die Benutzerregistrierung zu erstellen, und klicken Sie auf **Erstellen**. Klicken Sie auf **Schema hinzufügen**.



9. Erstellen Sie das folgende Schema.



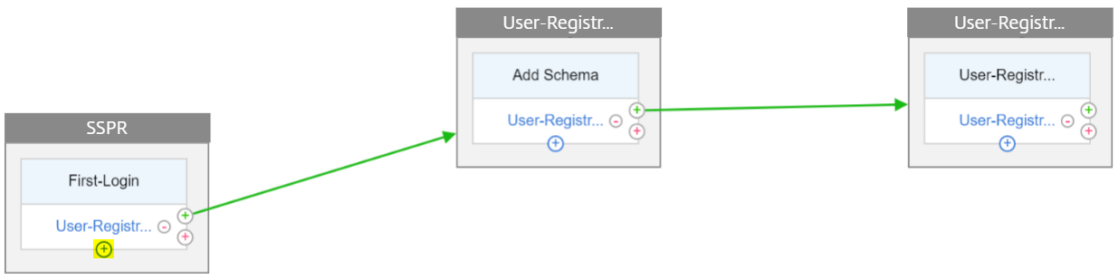
10. Klicken Sie auf **Richtlinie hinzufügen** und erstellen Sie die folgende Authentifizierungsrichtlinie.



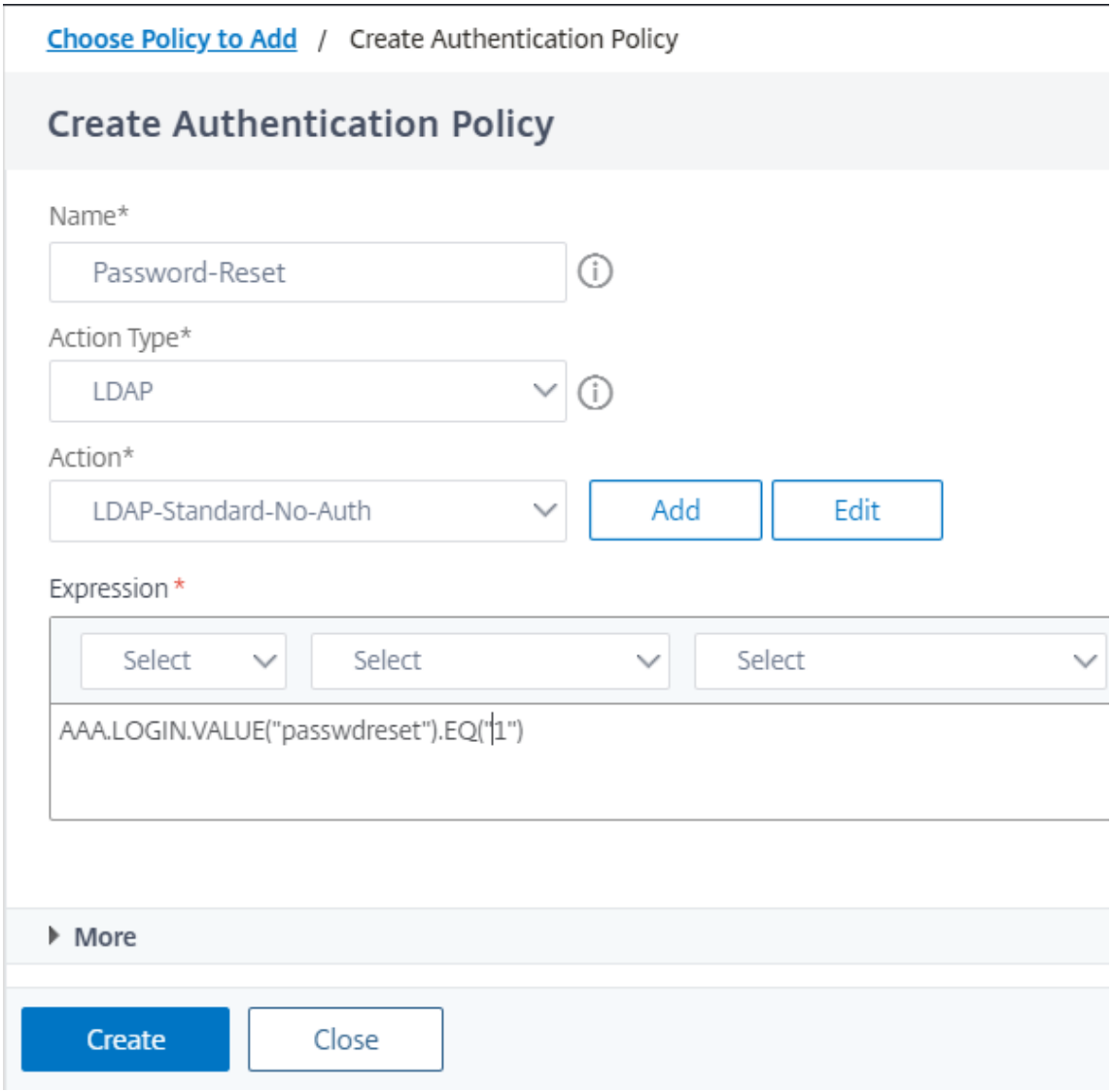
11. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.

Kennwort zurücksetzen

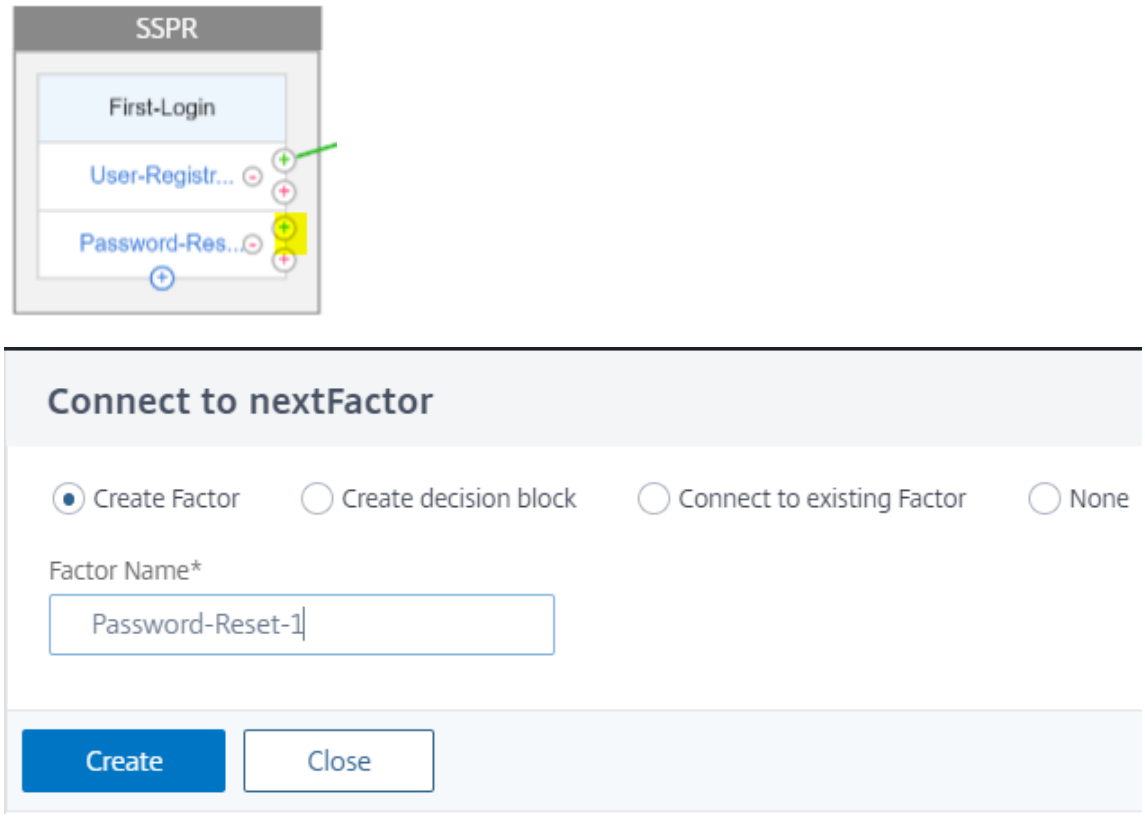
1. Klicken Sie auf das blaue “+” -Symbol, um eine weitere Richtlinie (Password Reset Flow) für den übergeordneten SSPR-Faktor hinzuzufügen.



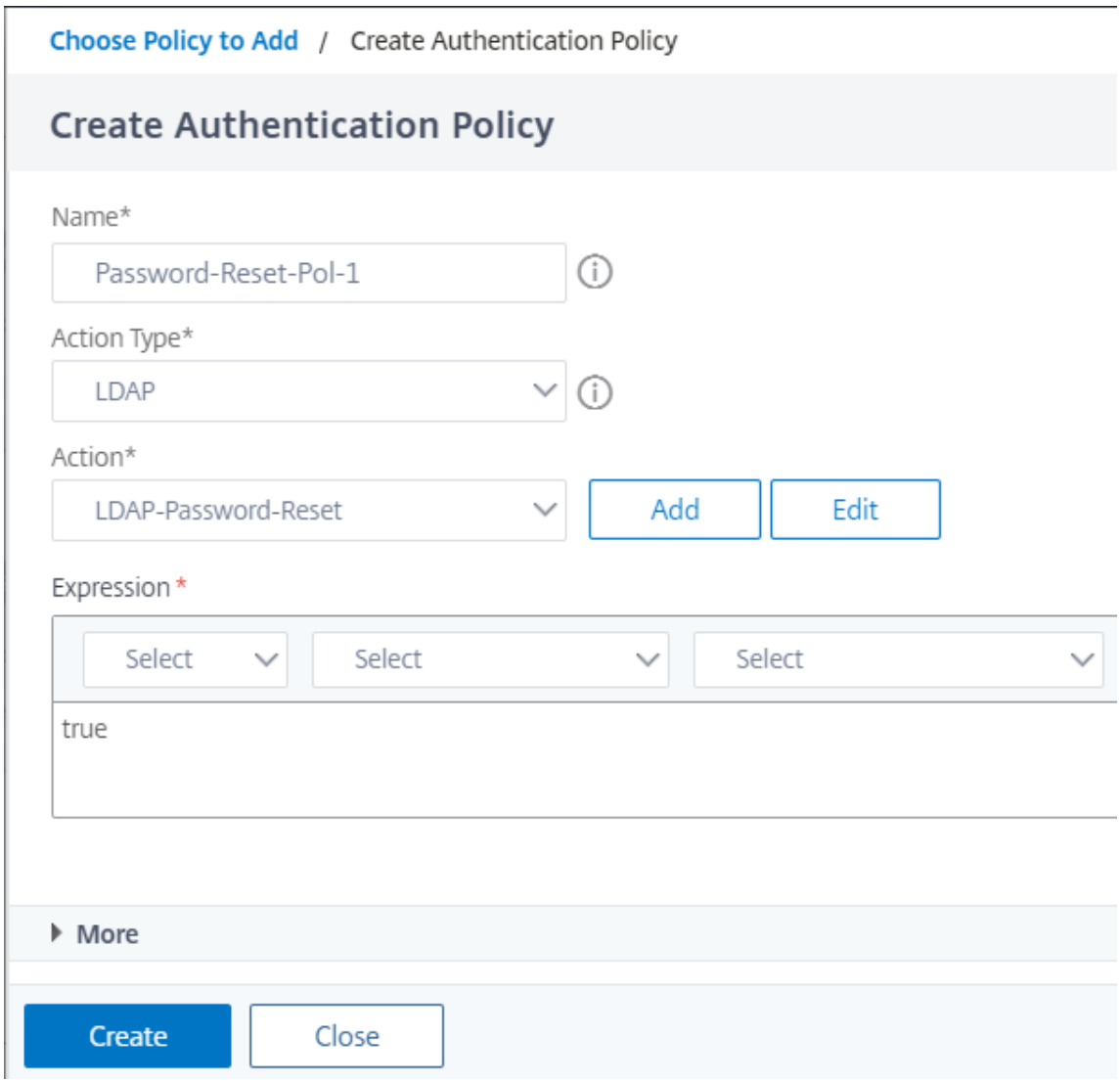
2. Klicken Sie auf **Hinzufügen** und erstellen Sie eine Authentifizierungsrichtlinie. Diese Richtlinie wird ausgelöst, wenn der Benutzer auf der Anmeldeseite auf “Kennwort vergessen” klickt.



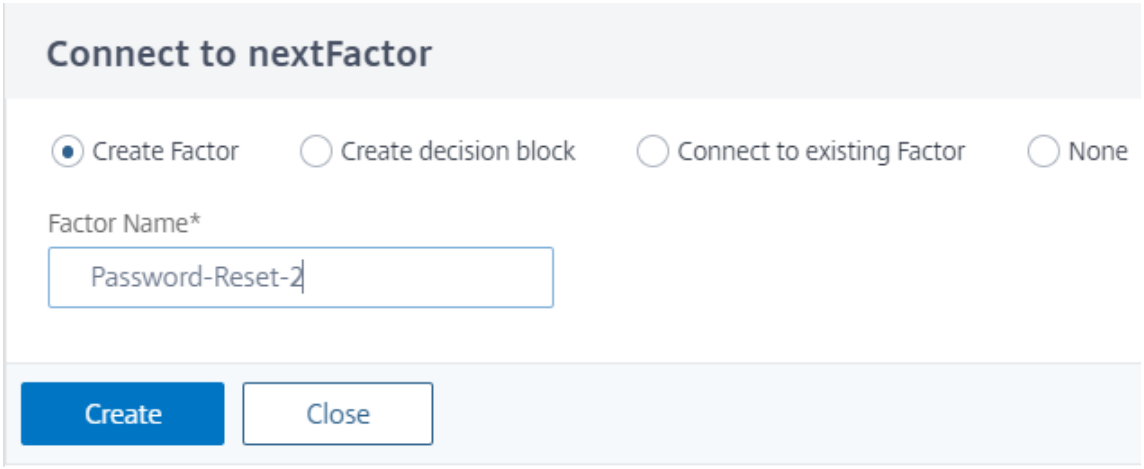
3. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
4. Klicken Sie auf das grüne “+” -Symbol für die Authentifizierungsrichtlinie zum Zurücksetzen des Kennworts, um einen weiteren Faktor hinzuzufügen.



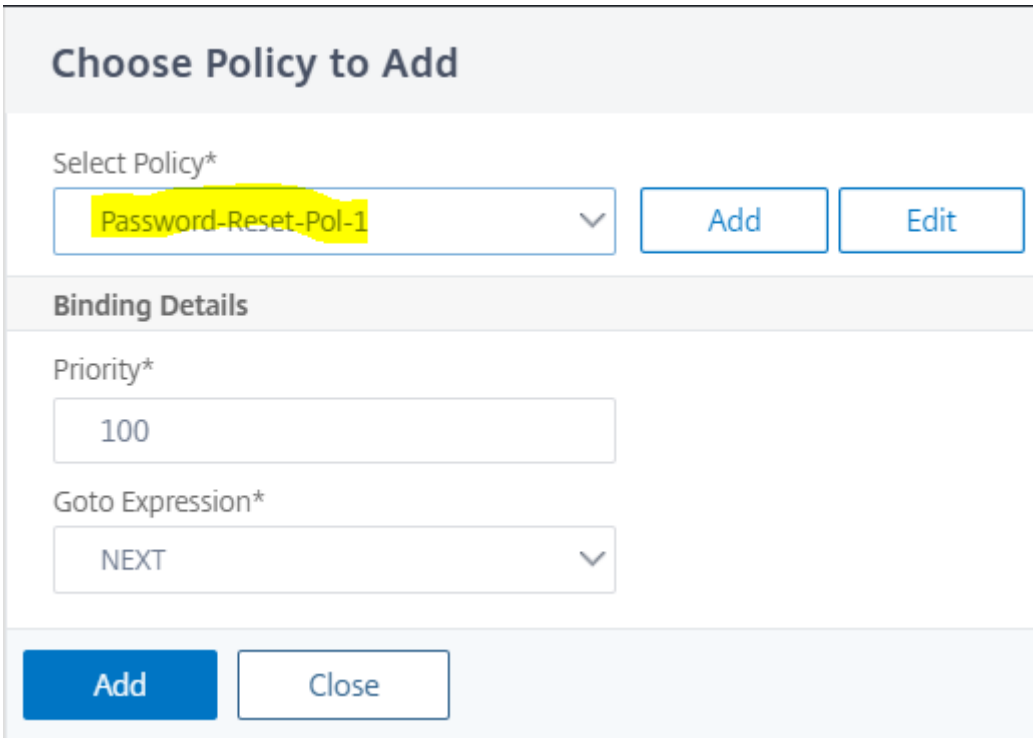
5. Klicken Sie auf **Erstellen**.
6. Klicken Sie auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie für den zuvor erstellten Faktor zu erstellen. Dieser Faktor dient zur Validierung des Benutzers.



7. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
8. Klicken Sie auf das grüne “+” -Symbol, um einen weiteren Faktor für den Kennwortfaktorfluss hinzuzufügen. Dadurch werden die Antworten zum Zurücksetzen des Kennworts überprüft. Klicken Sie auf **Erstellen**.

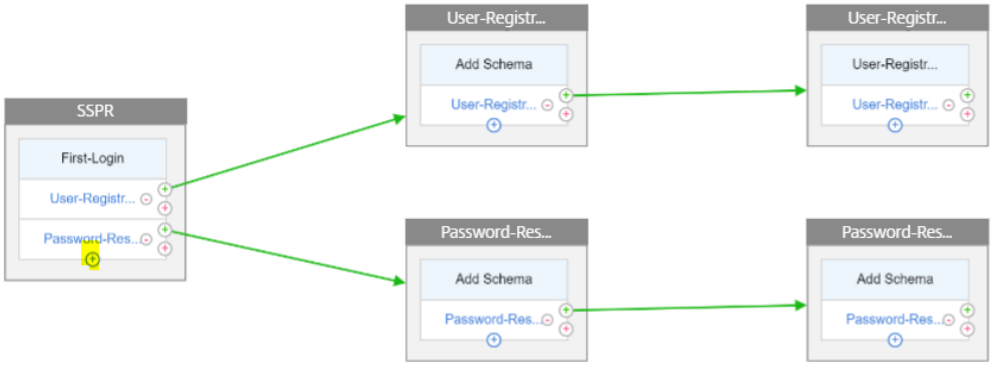


9. Klicken Sie auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie für den Faktor hinzuzufügen.
10. Wählen Sie im Dropdown-Menü dieselbe Authentifizierungsrichtlinie aus, die wir zuvor erstellt haben, und klicken Sie auf **Hinzufügen**.

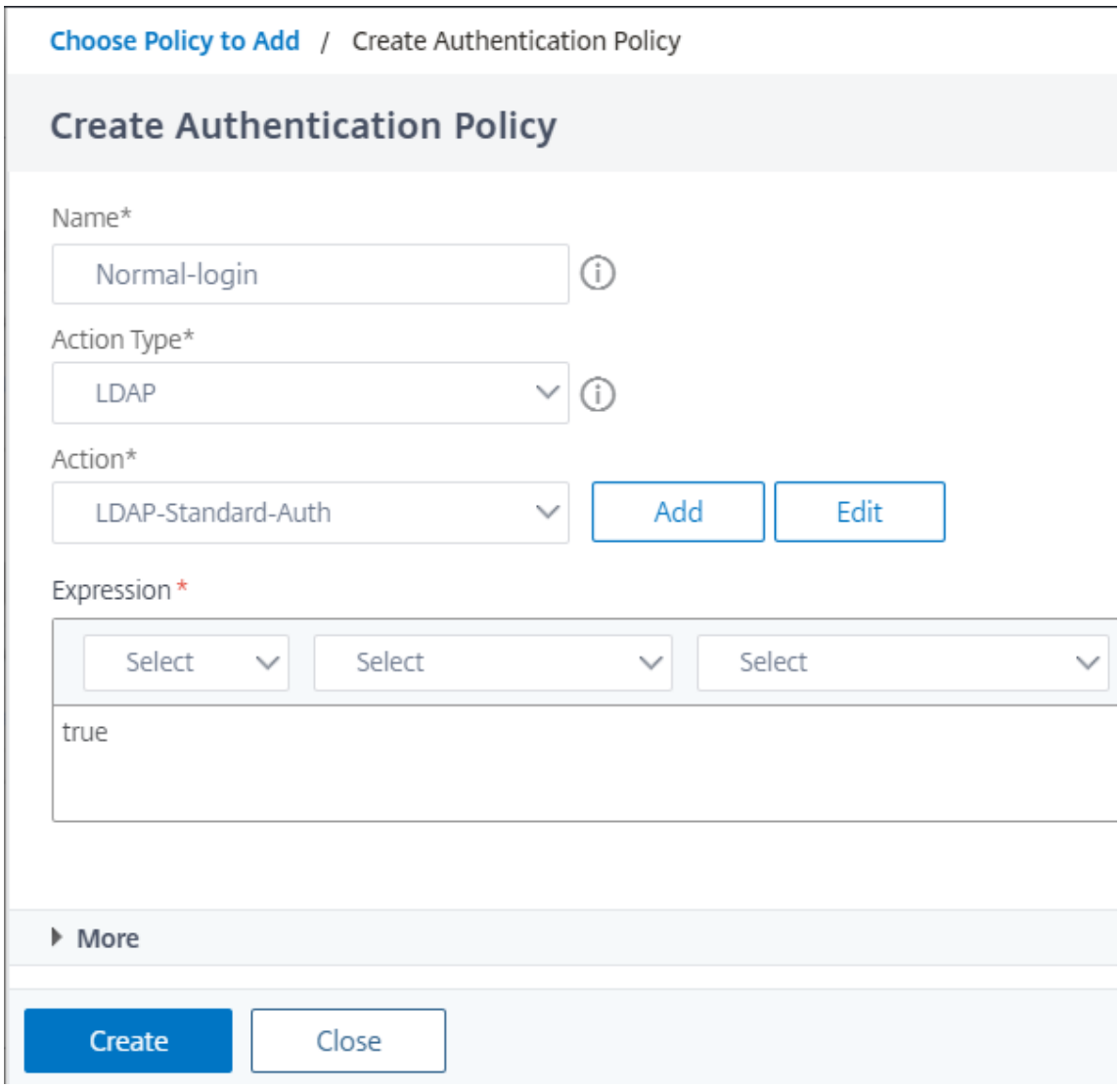


Normale Anmeldung + Überprüfung durch registrierte Benutzer

1. Klicken Sie auf das blaue “+” -Symbol, um dem übergeordneten SSPR-Faktor eine weitere Authentifizierungsrichtlinie (normaler Anmeldeablauf) hinzuzufügen.

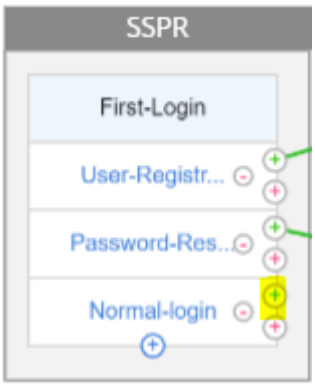


2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie für die normale Benutzeranmeldung zu erstellen.

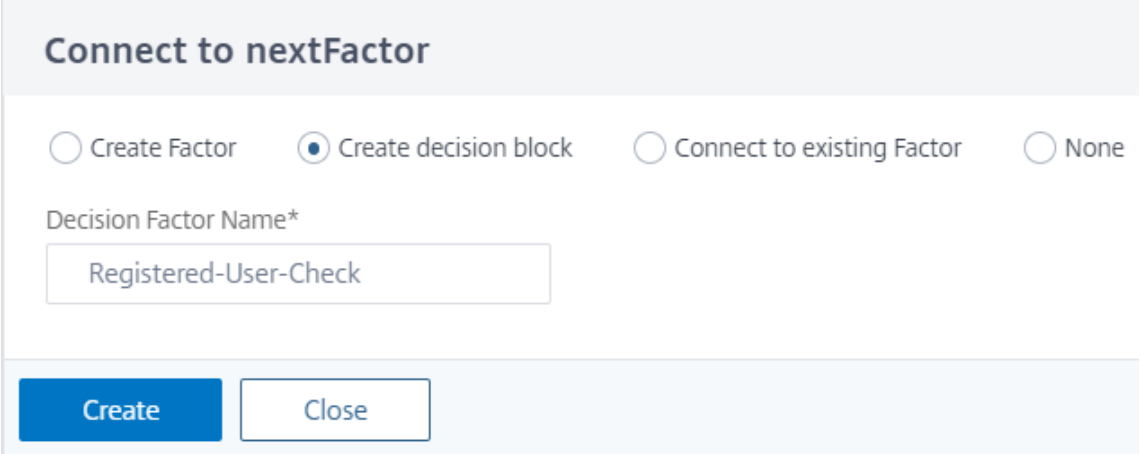


3. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.

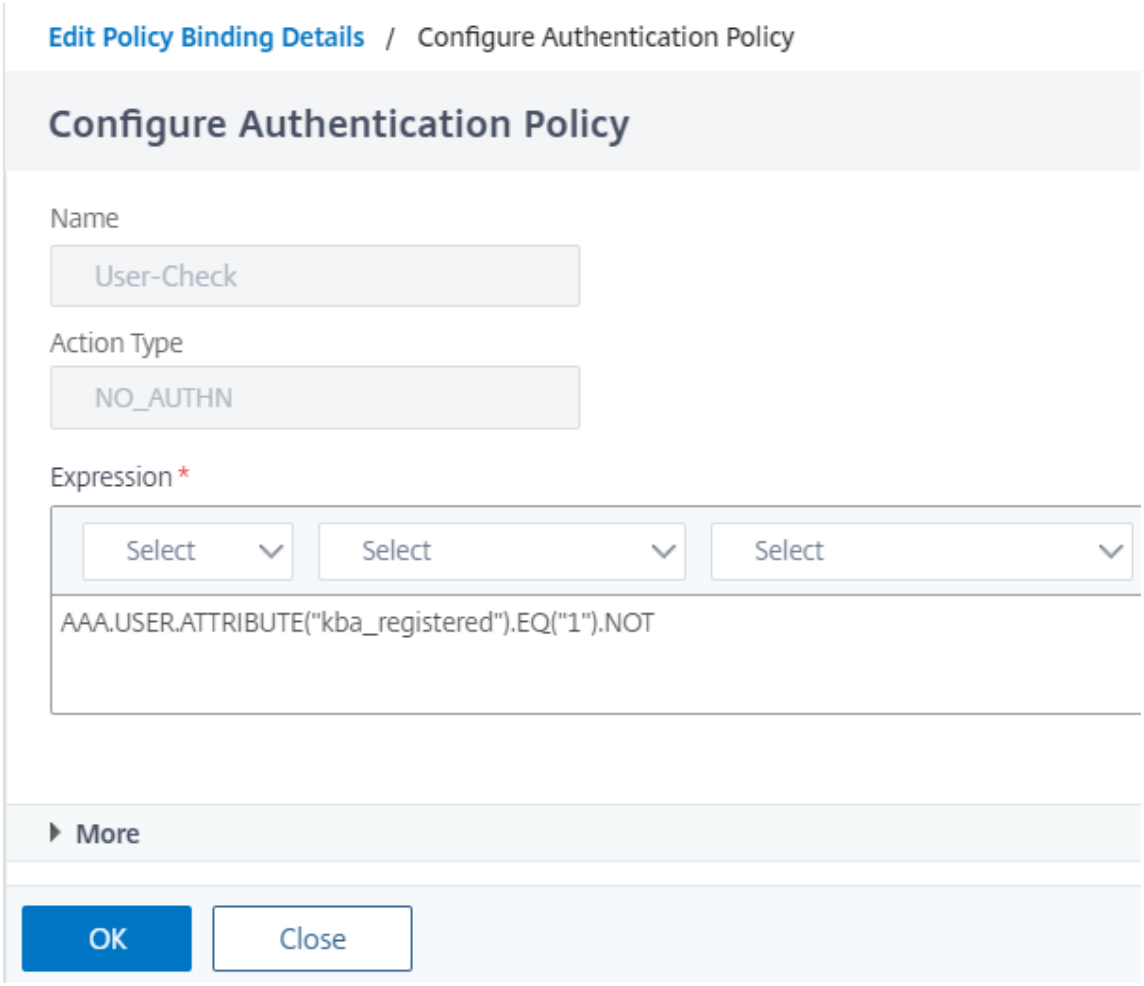
4. Klicken Sie auf das grüne “+” -Symbol für die zuvor erstellte Richtlinie, um einen weiteren Faktor hinzuzufügen, nämlich den Entscheidungsblock. Klicken Sie auf **Erstellen**.



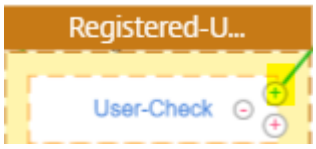
5. Klicken Sie auf **Erstellen**.



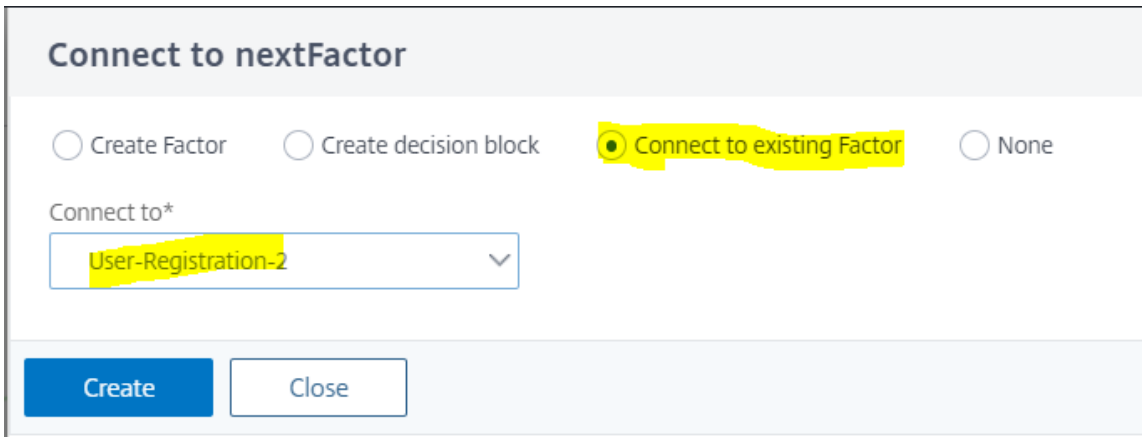
6. Klicken Sie auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie für diesen Entscheidungsfaktor zu erstellen.



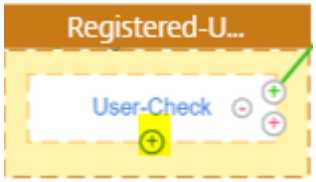
7. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**. Dadurch wird geprüft, ob der Benutzer registriert ist oder nicht.
8. Klicken Sie auf das grüne “+” -Symbol, um den Benutzer auf die Registrierungsrichtlinie hinzuweisen.



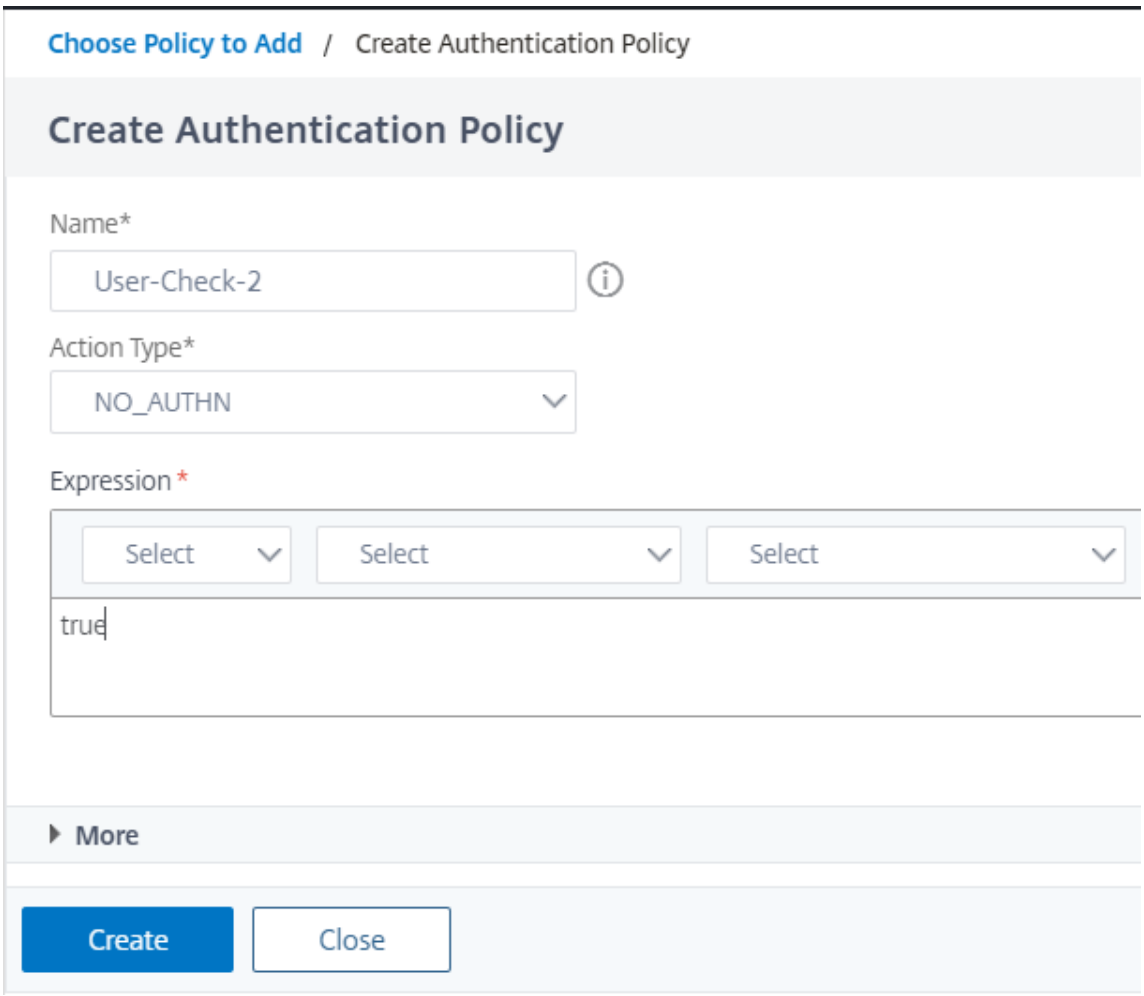
9. Wählen Sie den Registrierungsfaktor aus dem Dropdown-Menü aus und klicken Sie auf **Erstellen**.



10. Klicken Sie nun auf das blaue “+” -Symbol, um dem Entscheidungsblock eine weitere Richtlinie hinzuzufügen. Mit dieser Richtlinie kann der registrierte Benutzer die Authentifizierung beenden.



11. Klicke auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie zu erstellen.



12. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.

Abfragen während der Authentifizierung

May 11, 2023

Ausgehend von NetScaler Release Build 13.0.79.64 kann eine NetScaler Appliance während der Multifaktor-Authentifizierung für den Polling-Mechanismus konfiguriert werden.

Wenn Polling auf einer NetScaler Appliance konfiguriert ist, können Endpunkte (wie ein Webbrowser oder eine App) die Appliance während der Authentifizierung in den konfigurierten Intervallen abfragen (untersuchen), um den Status der übermittelten Authentifizierungsanforderung abzurufen.

Die Abfrage kann so konfiguriert werden, dass Authentifizierungen verarbeitet werden, wenn ein Endpunkt eine TCP-Verbindung während der Authentifizierung bei einer NetScaler Appliance unterbricht.

Wichtige Hinweise

- Die Polling-Konfiguration wird für LDAP-, RADIUS- und TACACS-Authentifizierungsmethoden unterstützt.
- Der Client kann Authentifizierungsanfragen ab dem zweiten Faktor untersuchen.

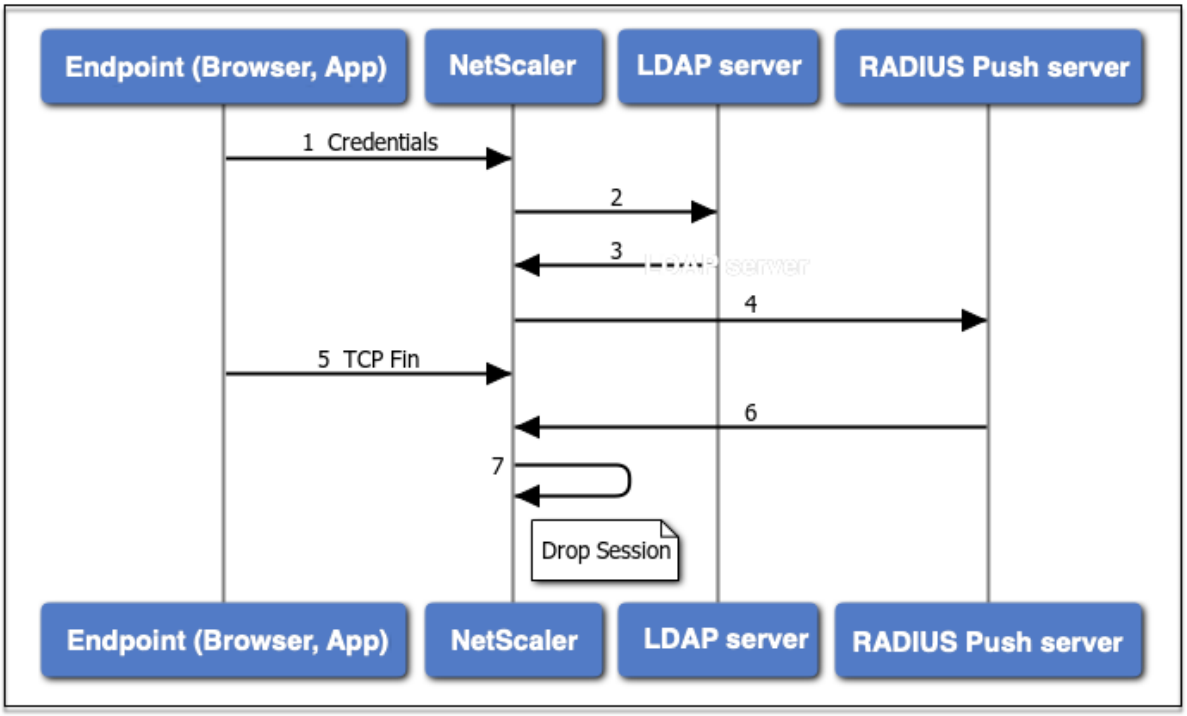
Warum sollte Polling konfiguriert werden?

Manchmal führt der Wechsel zwischen den Apps (z. B. einer Anmelde-App und einer Authentifikator-App) dazu, dass Endpunkte die Verbindung zur NetScaler Appliance verlieren, was zu einer Unterbrechung des Authentifizierungsflusses führt. Wenn Polling konfiguriert ist, kann diese Unterbrechung der Authentifizierung vermieden werden.

Den Polling-Mechanismus verstehen

Im Folgenden finden Sie ein Beispiel für den Ereignisfluss während der Authentifizierung, ohne dass Polling konfiguriert ist.

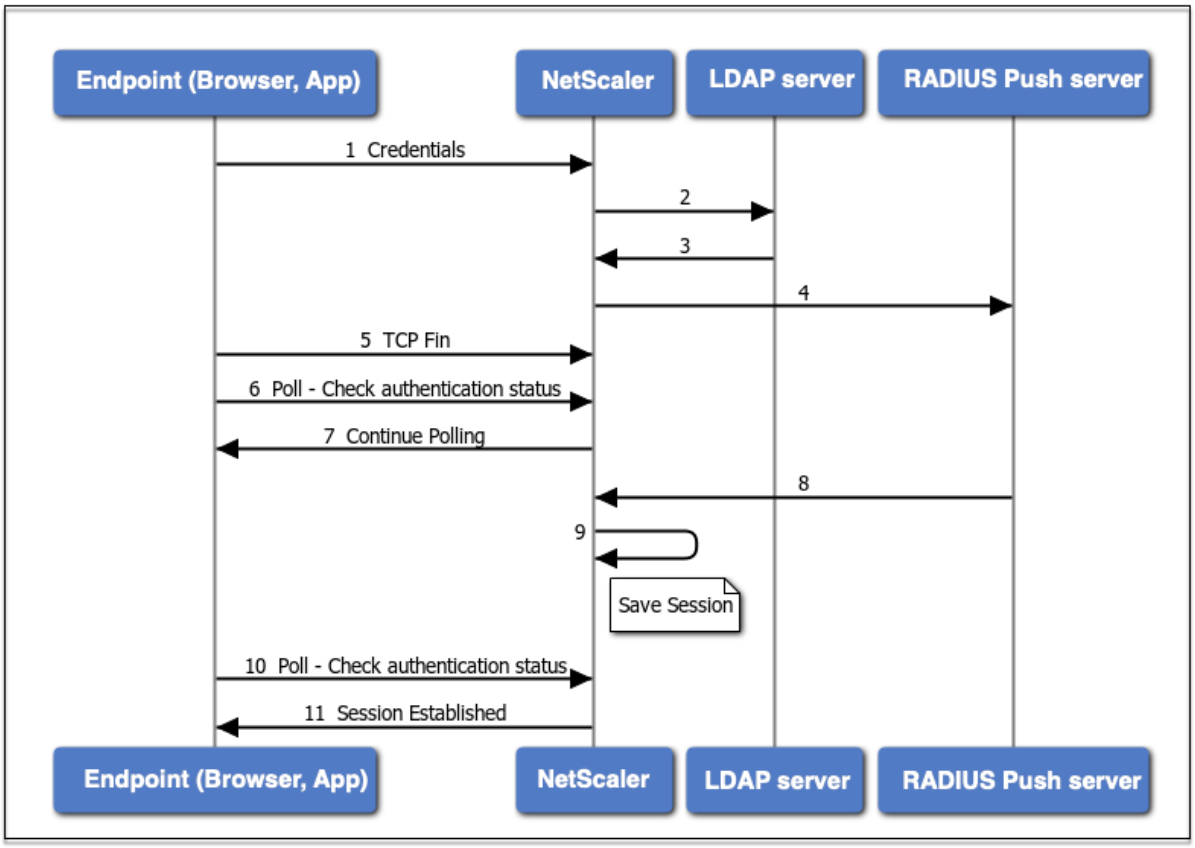
Der Abfragemechanismus ermöglicht es einer NetScaler-Appliance, eine laufende Authentifizierung mit dem Endpunkt fortzusetzen, ohne den Authentifizierungsprozess in einem seltenen Fall eines Zurücksetzens der TCP-Verbindung am Endpunkt neu starten zu müssen.



1. Ein Endpunkt (App oder Webbrowser) authentifiziert sich mit Anmeldeinformationen.

2. Der Benutzername und das Kennwort werden mit einem vorhandenen First-Faktor-Verzeichnis (LDAP/Active Directory) überprüft.
3. Wenn die richtigen Anmeldeinformationen angegeben werden, wechselt die Authentifizierung zum nächsten Faktor.
4. Zu diesem Zeitpunkt sendet die NetScaler Appliance eine Anfrage an den RADIUS-Push-Server.
5. Während die NetScaler Appliance auf eine Antwort vom RADIUS-Server wartet, unterbricht der Endpunkt die TCP-Verbindung.
6. Der NetScaler erhält eine Antwort vom RADIUS-Push-Server.
7. Da keine Client-TP-Verbindung gefunden wird, bricht die NetScaler Appliance die Sitzung ab und die Anmeldung schlägt fehl.

Im Folgenden finden Sie ein Beispiel für den Ereignisfluss während der Authentifizierung mit konfiguriertem Polling.



1. Ein Endpunkt (App oder Webbrowser) authentifiziert sich mit Anmeldeinformationen.
2. Der Benutzername und das Kennwort werden mit einem vorhandenen First-Faktor-Verzeichnis (LDAP/Active Directory) überprüft.
3. Wenn die richtigen Anmeldeinformationen angegeben werden, wechselt die Authentifizierung zum nächsten Faktor.
4. Zu diesem Zeitpunkt sendet die NetScaler Appliance eine Anfrage an den RADIUS-Push-Server.
5. Während die NetScaler Appliance auf eine Antwort vom RADIUS-Server wartet, unterbricht der

Endpunkt die TCP-Verbindung.

6. Endpoint sendet eine Umfrage (Probe) an die NetScaler Appliance, um nach dem Authentifizierungsstatus zu suchen.
7. Da die NetScaler Appliance keine Rückmeldung vom RADIUS-Server hört, fordert sie den Endpunkt auf, die Abfrage fortzusetzen.
8. Die NetScaler Appliance erhält eine Antwort vom RADIUS-Push-Server.
9. Da keine Client-TP-Verbindung gefunden wird, speichert ADC den Sitzungsstatus.
10. Endpoint fragt erneut ab, um nach dem Authentifizierungsstatus zu suchen.
11. Die NetScaler Appliance richtet die Sitzung ein und die Anmeldung ist erfolgreich.

Konfigurieren von Polling mit CLI

Im Folgenden finden Sie eine Beispiel-CLI Konfiguration.

Konfigurieren Sie den ersten Faktor

```
add authentication ldapAction ldap-new -serverIP 10.106.40.65 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword 2
    f63d3659103464a4fad0ade65e2ccfd4e8440e36ddff941d29796af03e01139 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
    groupAttrName memberof -subAttributeName CN -secType SSL -
    alternateEmailAttr userParameters

add authentication Policy ldap-new -rule true -action ldap-new

bind authentication vserver avs -policy ldap-new -priority 1 -
    nextFactor rad_factor
<!--NeedCopy-->
```

Konfigurieren Sie den zweiten Faktor

```
add authentication radiusAction rad1 -serverIP 10.102.229.120 -radKey 1
    b1613760143ce2371961e9a9eb5392c86a4954a62397f29a01b5d12b42ce232 -
    encrypted -encryptmethod ENCMTHD_3

add authentication Policy rad -rule true -action rad1
<!--NeedCopy-->
```

Konfigurieren Sie das Anmeldesschema Poll.xml


```
add authentication loginSchema polling_schema -authenticationSchema
    LoginSchema/Poll.xml

add authentication policylabel rad_factor -loginSchema polling_schema

bind authentication policylabel rad_factor -policyName rad -priority 1
    -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Konfigurieren von Polling mit GUI

Ausführliche Schritte zum Konfigurieren der Multifaktor-Authentifizierung mit der GUI finden Sie unter Konfigurieren der nFactor-Authentifizierung

Im Folgenden finden Sie die Beispielschritte auf hoher Ebene, die für die Konfiguration von NetScaler für Polling ab dem zweiten Faktor erforderlich sind.

1. Erstellen Sie einen ersten Faktor für die Authentifizierung, zum Beispiel LDAP.
2. Erstellen Sie einen zweiten Faktor für die Authentifizierung, z. B.
3. Fügen Sie **Poll.xml** in NetScaler (/nsConfig/loginschema/loginschema/) als Anmeldeschema für den zweiten Faktor hinzu.

Sitzungs- und Verkehrsmanagement

May 11, 2023

Sitzungseinstellungen

Nachdem Sie Ihre Authentifizierungs-, Autorisierungs- und Überwachungsprofile konfiguriert haben, konfigurieren Sie Sitzungseinstellungen, um Ihre Benutzersitzungen anzupassen. Die Sitzungseinstellungen lauten:

- **Das Sitzungs-Timeout.**

  Steuert den Zeitraum, nach dem der Benutzer automatisch getrennt wird und sich erneut authentifizieren muss, um auf Ihr Intranet zugreifen zu können.

- **Die standardmäßige Autorisierungseinstellung.**

  Bestimmt, ob die NetScaler-Appliance standardmäßig den Zugriff auf Inhalte zulässt oder verweigert, für die es keine spezifische Autorisierungsrichtlinie gibt.

- **Die Einstellung für einmaliges Anmelden.**

  Bestimmt, ob die NetScaler-Appliance Benutzer nach der Authentifizierung automatisch bei allen Webanwendungen anmeldet oder Benutzer zur Authentifizierung für jede Anwendung an die Anmeldeseite der Webanwendung weiterleitet.

- **Die Einstellung für den Berechtigungsindex.**

  Bestimmt, ob die NetScaler-Appliance die primären oder sekundären Authentifizierungsanmeldeinformationen für das einmalige Anmelden verwendet.

Um die Sitzungseinstellungen zu konfigurieren, können Sie einen von zwei Ansätzen wählen. Wenn Sie unterschiedliche Einstellungen für verschiedene Benutzerkonten oder Gruppen wünschen, erstellen Sie ein Profil für jedes Benutzerkonto oder jede Gruppe, für die Sie benutzerdefinierte Sitzungseinstellungen konfigurieren möchten. Sie erstellen auch Richtlinien, um die Verbindungen auszuwählen, auf die bestimmte Profile angewendet werden sollen, und binden die Richtlinien an Benutzer oder Gruppen. Sie können auch eine Richtlinie an den virtuellen Authentifizierungsserver binden, der den Datenverkehr verarbeitet, auf den Sie das Profil anwenden möchten.

Wenn Sie dieselben Einstellungen für alle Sitzungen wünschen oder die Standardeinstellungen für Sitzungen anpassen möchten, für die keine spezifischen Profile und Richtlinien konfiguriert sind, können Sie einfach die globalen Sitzungseinstellungen konfigurieren.

Sitzungsprofile

Um Ihre Benutzersitzungen anzupassen, erstellen Sie zunächst ein Sitzungsprofil. Das Sitzungsprofil ermöglicht es Ihnen, globale Einstellungen für einen der Sitzungsparameter zu überschreiben.

> **Hinweis**
>
> Die Begriffe “Sitzungsprofil” und “Sitzungsaktion” bedeuten dasselbe.

So erstellen Sie ein Sitzungsprofil über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein Sitzungsprofil zu erstellen und die Konfiguration zu überprüfen:

```
1 add tm sessionAction <name> [-sessTimeout <mins>] [-
     defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
     ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
     httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
      )] [-persistentCookieValidity <minutes>]
2
3 show tm sessionAction <name>
4 <!--NeedCopy-->
```


Beispiel

```
> add tm sessionAction session-profile -sessTimeout 30 -
    defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

So ändern Sie ein Sitzungsprofil über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein Sitzungsprofil zu ändern und die Konfiguration zu überprüfen:

```
set tm sessionAction <name> [-sessTimeout <mins>] [-
    defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
    ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
    httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
     )] [-persistentCookieValidity <minutes>]

show tm sessionAction
<!--NeedCopy-->
```

Beispiel

```
> set tm sessionAction session-profile -sessTimeout 30 -
    defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

So entfernen Sie ein Sitzungsprofil über die Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um ein Sitzungsprofil zu entfernen:

```
rm tm sessionAction <name>
<!--NeedCopy-->
```


So konfigurieren Sie Sitzungsprofile mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Sitzung.**
2. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Sitzung.**
3. Klicken Sie im Detailbereich auf die Registerkarte **Profile** .
4. Führen Sie auf der Registerkarte **Profile** einen der folgenden Schritte aus:
   - Um ein neues Sitzungsprofil zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um ein vorhandenes Sitzungsprofil zu ändern, wählen Sie das Profil aus und klicken dann auf **Bearbeiten.**
5. Geben Sie im Dialogfeld TM-Sitzungsprofil erstellen oder TM-Sitzungsprofil konfigurieren Werte für die Parameter ein oder wählen Sie sie aus.
   - name*—actionName (Kann für eine zuvor konfigurierte Sitzungsaktion nicht geändert werden.)
   - Sitzungs-Timeout — SessTimeout
   - Einmaliges Anmelden bei Webanwendungen — SSO
   - Standard-Autorisierungsaktion — DefaultAuthorizationAction
   - Index der Anmeldeinformationen — SSOCredential
   - Domäne für einmaliges Anmelden — SSODomain
   - Nur-HTTP-Cookie — Nur HTTP Cookie
   - Persistentes Cookie aktivieren — PersistentCookie
   - Persistente Cookie-Gültigkeit — Persistente Cookie-Gültigkeit
6. Klicken Sie auf **Erstellen** oder **auf OK**. Das von Ihnen erstellte Sitzungsprofil wird im Bereich Sitzungsrichtlinien und -profile angezeigt.

Sitzungsrichtlinien

Nachdem Sie ein oder mehrere Sitzungsprofile erstellt haben, erstellen Sie Sitzungsrichtlinien und binden die Richtlinien dann global oder an einen virtuellen Authentifizierungsserver, um sie in Kraft zu setzen.

So erstellen Sie eine Sitzungsrichtlinie über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Sitzungsrichtlinie zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add tm sessionPolicy <name> <rule> <action>
2 -  show tm sessionPolicy <name>
3 <!--NeedCopy-->
```

Beispiel

```
1 > add tm sessionPolicy session-pol "URL == /\*.png" session-profile
```



```
Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

So ändern Sie eine Sitzungsrichtlinie über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Sitzungsrichtlinie zu ändern und die Konfiguration zu überprüfen:

```
-  set tm sessionPolicy <name> [-rule <expression>] [-action <action>]
-  show tm sessionPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
> set tm sessionPolicy session-pol "URL == /\*.png" session-profile
 Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

So binden Sie eine Sitzungsrichtlinie über die Befehlszeile global

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Sitzungsrichtlinie global zu binden und die Konfiguration zu überprüfen:

```
bind tm global -policyName <policyname> [-priority <priority>]
<!--NeedCopy-->
```

Beispiel

```
> bind tm global -policyName session-pol
 Done

> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.png'
        Action: session-profile
        Policy is bound to following entities
```



```
        1) TM GLOBAL    PRIORITY : 0
 Done

<!--NeedCopy-->
```

So binden Sie eine Sitzungsrichtlinie über die Befehlszeile an einen virtuellen Authentifizierungsserver

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Sitzungsrichtlinie an eine virtuelle Authentifizierung zu binden und die Konfiguration zu überprüfen:

```
bind authentication vserver <name> -policy <policyname> [-priority <
   priority>]
<!--NeedCopy-->
```

Beispiel

```
bind authentication vserver auth-vserver-1 -policyName Session-Pol-1 -
   priority 1000
Done
<!--NeedCopy-->
```

So lösen Sie eine Sitzungsrichtlinie über die Befehlszeile von einem virtuellen Authentifizierungsserver

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer Sitzungsrichtlinie von einem virtuellen Authentifizierungsserver aufzuheben und die Konfiguration zu überprüfen:

```
unbind authentication vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Beispiel

```
unbind authentication vserver auth-vserver-1 -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

So lösen Sie die Bindung einer global gebundenen Sitzungsrichtlinie über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer global gebundenen Sitzungsrichtlinie aufzuheben:


```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Beispiel

```
unbind tm global -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

So entfernen Sie eine Sitzungsrichtlinie über die Befehlszeile

Trennen Sie zuerst die Sitzungsrichtlinie von global, und geben Sie dann an der Eingabeaufforderung die folgenden Befehle ein, um eine Sitzungsrichtlinie zu entfernen und die Konfiguration zu überprüfen:

```
rm tm sessionPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm sessionPolicy Session-Pol-1
Done

<!--NeedCopy-->
```

So konfigurieren und binden Sie Sitzungsrichtlinien mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Sitzung**.
2. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Sitzung**.
3. Führen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine der folgenden Aktionen aus:
   - Um eine neue Sitzungsrichtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine bestehende Sitzungsrichtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Bearbeiten**.
4. Geben **Sie im Dialogfeld Sitzungsrichtlinie erstellen** oder **Sitzungsrichtlinie konfigurieren** die Werte für die Parameter ein oder wählen Sie sie aus.
   - name* — policyName (Kann für eine zuvor konfigurierte Sitzungsrichtlinie nicht geändert werden.)
   - Profil anfordern*—actionName
   - Ausdruck* — Regel (Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unter dem Textbereich Ausdruck auswählen und dann Ihren

Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem Sie auf **Hinzufügen** klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und das Dropdown-Menü zu öffnen. listet darin auf, um deinen Ausdruck zu konstruieren.)

5. Klicken Sie auf **Erstellen** oder **auf OK**. Die von Ihnen erstellte Richtlinie wird im Detailbereich der Seite **Sitzungsrichtlinien** und **-profile** angezeigt.
6. Um eine Sitzungsrichtlinie global zu binden, wählen Sie im Detailbereich **Globale Bindungen** aus der Dropdownliste **Aktion** aus, und füllen Sie das Dialogfeld aus.
   - Wählen Sie den Namen der Sitzungsrichtlinie aus, die Sie global binden möchten.
   - Klicken Sie auf **OK**.
7. Um eine Sitzungsrichtlinie an einen virtuellen Authentifizierungsserver zu binden, klicken Sie im Navigationsbereich auf **Virtuelle Server**, und fügen Sie diese Richtlinie zur Richtlinienliste hinzu.
   - Wählen Sie im Detailbereich den virtuellen Server aus, und klicken Sie dann auf **Bearbeiten**.
   - Klicken Sie in der **Erweiterten Auswahl** rechts neben dem Detailbereich auf **Richtlinien**.
   - Wählen Sie eine Richtlinie aus oder klicken Sie auf das **Plus-Symbol**, um eine Richtlinie hinzuzufügen.
   - Ändern Sie in der Spalte **Priorität** links die Standardpriorität, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge ausgewertet wird.
   - Klicken Sie auf **OK**.
     In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

Globale Sitzungseinstellungen

Zusätzlich zum oder anstelle der Erstellung von Sitzungsprofilen und Richtlinien können Sie globale Sitzungseinstellungen konfigurieren. Diese Einstellungen steuern die Sitzungskonfiguration, wenn es keine explizite Richtlinie gibt, die sie überschreibt.

So konfigurieren Sie die Sitzungseinstellungen über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die globalen Sitzungseinstellungen zu konfigurieren und die Konfiguration zu überprüfen:

```
1 set tm sessionParameter [-sessTimeout <mins>][-
     defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
     ssoCredential ( PRIMARY | SECONDARY )][-ssoDomain <string>][-
     httpOnlyCookie ( YES | NO )][-persistentCookie ( ENABLED | DISABLED
     )] [-persistentCookieValidity <minutes>]
2 <!--NeedCopy-->
```


Beispiel

```
> set tm sessionParameter -sessTimeout 30
  Done
> set tm sessionParameter -defaultAuthorizationAction DENY
  Done
> set tm sessionParameter -SSO ON
  Done
> set tm sessionParameter -ssoCredential PRIMARY
  Done
<!--NeedCopy-->
```

So konfigurieren Sie die Sitzungseinstellungen mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr**
2. Klicken Sie im Detailbereich unter **Einstellungen**auf Globale Einstellungen ändern.
3. Geben Sie im Dialogfeld **Globale Sitzungseinstellungen** Werte für die Parameter ein oder wählen Sie sie aus.
   - Sitzungs-Timeout — SessTimeout
   - Standard-Autorisierungsaktion — DefaultAuthorizationAction
   - Einmaliges Anmelden bei Webanwendungen — SSO
   - Index der Anmeldeinformationen — SSOCredential
   - Domäne für einmaliges Anmelden — SSODomain
   - Nur-HTTP-Cookie — Nur HTTP Cookie
   - Persistentes Cookie aktivieren — PersistentCookie
   - Persistente Cookie-Gültigkeit (Minuten) — Persistente Cookie-Gültigkeit
   - Homepage—Homepage
4. Klicken Sie auf **OK**.

Traffic-Einstellungen

Wenn Sie formularbasiertes oder SAML-Single-Sign-On (SSO) für Ihre geschützten Anwendungen verwenden, konfigurieren Sie diese Funktion in den Verkehrseinstellungen. SSO ermöglicht es Ihren Benutzern, sich einmal anzumelden, um auf alle geschützten Anwendungen zuzugreifen, anstatt dass sie sich separat anmelden müssen, um auf jede einzelne zuzugreifen.

Formularbasiertes SSO ermöglicht es Ihnen, ein Webformular Ihres eigenen Designs als Anmeldemethode anstelle eines generischen Popup-Fensters zu verwenden. Sie können daher Ihr Firmenlogo und andere Informationen, die Ihre Benutzer möglicherweise sehen sollen, in das Anmeldeformular einfügen. SAML SSO ermöglicht es Ihnen, eine NetScaler-Appliance oder eine virtuelle Appliance-Instanz für die Authentifizierung bei einer anderen NetScaler-Appliance im

Namen von Benutzern zu konfigurieren, die sich bei der ersten Appliance authentifiziert haben.

Um einen der beiden SSO-Typen zu konfigurieren, erstellen Sie zunächst ein Formulare- oder SAML-SSO-Profil. Als Nächstes erstellen Sie ein Verkehrsprofil und verknüpfen es mit dem von Ihnen erstellten SSO-Profil. Als Nächstes erstellen Sie eine Richtlinie und verknüpfen sie mit dem Verkehrsprofil. Schließlich binden Sie die Richtlinie global oder an einen virtuellen Authentifizierungsserver, um Ihre Konfiguration in Kraft zu setzen.

Traffic-Profile

Nachdem Sie mindestens ein Formular oder ein SAML-SSO-Profil erstellt haben, müssen Sie als Nächstes ein Verkehrsprofil erstellen.

> **Hinweis:**
>
> In dieser Funktion bedeuten die Begriffe “Profil” und “Aktion” dasselbe.

So erstellen Sie ein Verkehrsprofil über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add tm trafficAction <name> [-appTimeout <mins>][-SSO ( ON | OFF ) [-
    formSSOAction <string>]][-persistentCookie ( ENABLED | DISABLED )][-
    InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Beispiel

```
add tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```

So ändern Sie ein Sitzungsprofil über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
set tm trafficAction <name> [-appTimeout <mins>] [-SSO ( ON | OFF ) [-
    formSSOAction <string>]] [-persistentCookie ( ENABLED | DISABLED )]
    [-InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Beispiel


```
set tm trafficAction Traffic-Prof-1  - appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```

So entfernen Sie ein Sitzungsprofil über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
rm tm trafficAction <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm trafficAction Traffic-Prof-1
<!--NeedCopy-->
```

So konfigurieren Sie Verkehrsprofile mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Verkehr.**
2. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Verkehr.**
3. Klicken Sie im Detailbereich auf die Registerkarte Profile.
4. Führen Sie auf der Registerkarte Profile einen der folgenden Schritte aus:
   - Um ein neues Verkehrsprofil zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um ein vorhandenes Verkehrsprofil zu ändern, wählen Sie das Profil aus und klicken dann auf **Bearbeiten.**
5. Geben **Sie im Dialogfeld Verkehrsprofil erstellen** oder **Verkehrsprofil konfigurieren** Werte für die Parameter an.
   - name*—name (Kann für eine zuvor konfigurierte Sitzungsaktion nicht geändert werden.)
   - App-Timeout — App-Timeout
   - Einmaliges Anmelden — SSO
   - Formular SSO-Aktion — FormsSOAction
   - SAML SSO-Aktion — SAMLSSO-Aktion
   - Persistentes Cookie aktivieren — PersistentCookie
   - Abmeldung initiieren — Logout initiieren
6. Klicken Sie auf **Erstellen** oder **auf OK**. Das von Ihnen erstellte Verkehrsprofil wird je nach Bedarf in den Verkehrsrichtlinien, Profilen und entweder im Bereich SSO-Profile oder SAML-SSO-Profile erstellen angezeigt.

Unterstützung für AAA.USER- und AAA.LOGIN-Ausdrücke

Der AAA.USER-Ausdruck ist jetzt implementiert, um die vorhandenen HTTP.REQ.USER-Ausdrücke zu ersetzen. Der AAA.USER-Ausdruck ist für den Umgang mit Nicht-HTTP-Datenverkehr wie dem Secure Web Gateway (SWG) und dem rollenbasierten Zugriff (RBA) anwendbar. Die AAA.USER-Ausdrücke entsprechen HTTP.REQ.USER-Ausdrücken.

Sie können den Ausdruck bei verschiedenen Aktionen oder Profilkonfiguration verwenden.

Geben Sie in der Befehlszeile Folgendes ein:

```
add tm trafficAction <name> [SSO (ON|OFF)] [-userExpression <string>]

add tm trafficAction <name> [SSO (ON|OFF)] [-passwdExpression <string>]

<!--NeedCopy-->
```

Beispiel

```
add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.NAME"

add tm trafficAction tm_act -SSO ON -userExpression "AAA.USER.PASSWD"

add tm trafficPolicy tm_pol true tm_act

bind lb vserver lb1 -policyName tm_pol -priority 2
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie den Ausdruck HTTP.REQ.USER verwenden, erscheint eine Warnmeldung “HTTP.REQ.USER eingestellt. Verwenden Sie stattdessen AAA.USER”.

- **AAA.LOGIN Expression.** Der LOGIN-Ausdruck steht für Pre-Login, auch als Anmeldeanforderung bezeichnet. Die Anmeldeanforderung kann von NetScaler Gateway, SAML IdP oder von OAuth Authentifizierung stammen. Der NetScaler abstrahiert die erforderlichen Attribute aus der Richtlinienkonfiguration. Der AAA.LOGIN-Ausdruck enthält die Attribute, die basierend auf folgendem abgerufen werden können:
  - **AAA.LOGIN.USERNAME.** Der Benutzername (falls gefunden) wird aus der aktuellen Anmeldeanforderung abgerufen. Derselbe Ausdruck, der auf eine Nicht-Anmeldeanforderung angewendet wird (bestimmt durch eine Authentifizierung, Autorisierung und Überwachung), führt zu einer leeren Zeichenfolge.
  - **AAA.LOGIN.PASSWORD.** Das Benutzerkennwort (falls gefunden) wird aus der aktuellen Anmeldeanfrage abgerufen. Der Ausdruck führt zu einer leeren Zeichenfolge, wenn das Kennwort nicht gefunden wird.

  - **AAA.LOGIN.PASSWORD2.** Das zweite Kennwort (falls gefunden) wird aus der Anmeldeanfrage abgerufen.
  - **AAA.LOGIN.DOMAIN.** Die Domäneninformationen werden aus der Anmeldeanfrage abgerufen.
- **AAA.USER.ATTRIBUTE (“#”).** Der Ausdruck wird verwendet, um das Benutzerattribut zu speichern. Hier kann # entweder ein ganzzahliger Wert (zwischen 1 und 16) oder ein Zeichenfolgenwert sein. Sie können diese Indexwerte verwenden, indem Sie den Ausdruck AAA.USER.ATTRIBUTE (“#”) verwenden. Das Authentifizierungs-, Autorisierungs- und Überwachungsmodul sucht das Benutzersitzungsattribut und `AAA.USER.ATTRIBUTE("##")` würde die Hash-Tabelle nach diesem bestimmten Attribut abfragen. Wenn beispielsweise `Attributes("samaccountname")` auf gesetzt ist, würde `AAA.USER.ATTRIBUTE("samaccountname")` die Hash-Map abfragen und den `samaccountname` entsprechenden Wert abrufen.

Traffic-Richtlinien

Nachdem Sie ein oder mehrere Formular-SSO- und Verkehrsprofile erstellt haben, erstellen Sie Verkehrsrichtlinien und binden die Richtlinien dann entweder global oder an einen virtuellen Traffic-Management-Server, um sie in Kraft zu setzen.

So erstellen Sie eine Verkehrsrichtlinie über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add tm trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Beispiel

```
add tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS(
   "login=true")" Traffic-Prof-1
<!--NeedCopy-->
```

So ändern Sie eine Verkehrsrichtlinie über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
set tm trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Beispiel


```
set tm trafficPolicy Traffic-Pol-1 "HTTP.REQ.HEADER("Cookie").CONTAINS(
    "login=true")" Traffic-Prof-1
<!--NeedCopy-->
```

So binden Sie eine Verkehrsrichtlinie über die Befehlszeile global

Geben Sie in der Befehlszeile Folgendes ein:

```
bind tm global -policyName <string> [-priority <priority>]
<!--NeedCopy-->
```

Beispiel

```
bind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

So binden Sie eine Verkehrsrichtlinie über die Befehlszeile an einen virtuellen Lastausgleich- oder Content Switching-Server

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
bind lb vserver <name> -policy <policyName> [-priority <priority>]

bind cs vserver <name> -policy <policyName> [-priority <priority>]
<!--NeedCopy-->
```

Beispiel

```
bind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1 -
    priority 1000
<!--NeedCopy-->
```

So lösen Sie die Bindung einer global gebundenen Verkehrsrichtlinie über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Beispiel


```
unbind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

So lösen Sie eine Verkehrsrichtlinie über die Befehlszeile von einem virtuellen Lastausgleich- oder Content Switching-Server

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
unbind lb vserver <name> -policy <policyname>

unbind cs vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Beispiel

```
unbind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1
<!--NeedCopy-->
```

So entfernen Sie eine Verkehrsrichtlinie über die Befehlszeile

Entbinden Sie zuerst die Sitzungsrichtlinie von global, und geben Sie dann an der Eingabeaufforderung Folgendes ein:

```
rm tm trafficPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm trafficPolicy Traffic-Pol-1
<!--NeedCopy-->
```

So konfigurieren und binden Sie Verkehrsrichtlinien mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Verkehr.**
2. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Verkehr.**
3. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Sitzungsrichtlinie zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um eine bestehende Sitzungsrichtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Bearbeiten.**

4. Geben **Sie im Dialogfeld “Traffic Policy erstellen** “ oder “ **Verkehrsrichtlinie konfigurieren** “ Werte für die Parameter an.
   - name* — policyName (Kann für eine zuvor konfigurierte Sitzungsrichtlinie nicht geändert werden.)
   - Profil* — Aktionsname
   - Ausdruck — Regel (Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unter dem Textbereich Ausdruck auswählen und dann Ihren Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und die Dropdownlisten darin zu verwenden konstruiere deinen Ausdruck.)
5. Klicken Sie auf **Erstellen** oder **auf OK**. Die von Ihnen erstellte Richtlinie wird im Detailbereich der Seite **Sitzungsrichtlinien** und **-profile** angezeigt.

Bilden Sie SSO-Profile

Um formularbasiertes SSO zu aktivieren und zu konfigurieren, erstellen Sie zunächst ein SSO-Profil.

> **Hinweis**
>
> - Formularbasiertes einmaliges Anmelden funktioniert nicht, wenn das Formular so angepasst ist, dass es Javascript enthält.
> - In dieser Funktion bedeuten die Begriffe “Profil” und “Aktion” dasselbe.

So erstellen Sie ein SSO-Formularprofil über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]

show tm formSSOAction [<name>]
<!--NeedCopy-->
```

Beispiel

```
add tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-nameValuePair "loginID passwd" -responsesize "9096"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
```



```
<!--NeedCopy-->
```

So ändern Sie ein Formular SSO über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
set tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]
<!--NeedCopy-->
```

Beispiel

```
set tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nameValuePair "loginID passwd" -responsesize "9096"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```

So entfernen Sie ein SSO-Formularprofil über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
rm tm formSSOAction <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm sessionAction SSO-Prof-1
<!--NeedCopy-->
```

So konfigurieren Sie SSO-Formular-Profile mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Verkehr**.
2. Klicken Sie im Detailbereich auf die Registerkarte **SSO-Profile für Formulare** .
3. Führen Sie auf der Registerkarte SSO-Profile für Formulare einen der folgenden Schritte aus:
   - Um ein neues Formular-SSO-Profil zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um ein vorhandenes Formular-SSO-Profil zu ändern, wählen Sie das Profil aus, und klicken Sie dann auf Bearbeiten.

4. Geben **Sie im Dialogfeld Formular-SSO-Profil erstellen** oder **Formular-SSO-Profil konfigurieren** die Werte für die Parameter an:
   - name*—name (Kann für eine zuvor konfigurierte Sitzungsaktion nicht geändert werden.)
   - Aktions-URL*—actionUrl
   - Feld Benutzername*—UserField
   - Kennwort-Feld*—PassField
   - Ausdruck* — SSOSuccessRule
   - Name/Wert-Paar — NameValuePair
   - Größe der Antwort — ResponseSize
   - Extraktion — NV-Typ
   - Methode einreichen — SubmitMethod
5. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**. Das Formular SSO-Profil, das Sie erstellt haben, wird im Bereich **Verkehrsrichtlinien**, **Profile**und **SSO-Formularprofile** angezeigt.

SAML SSO-Profile

Um SAML-basiertes SSO zu aktivieren und zu konfigurieren, erstellen Sie zunächst ein SAML-SSO-Profil.

So erstellen Sie ein SAML-SSO-Profil über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Beispiel

```
add tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```

So ändern Sie ein SAML-SSO über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:


```
set tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
<!--NeedCopy-->
```

Beispiel

```
set tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
<!--NeedCopy-->
```

So entfernen Sie ein SAML-SSO-Profil über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
rm tm samlSSOProfile <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm sessionAction saml-SSO-Prof-1
<!--NeedCopy-->
```

So konfigurieren Sie ein SAML-SSO-Profil mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Verkehr.**
2. Klicken Sie im Detailbereich auf die Registerkarte **SAML-SSO-Profile** .
3. Führen Sie auf der Registerkarte **SAML SSO-Profile** einen der folgenden Schritte aus:
   - Um ein neues SAML-SSO-Profil zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um ein vorhandenes SAML-SSO-Profil zu ändern, wählen Sie das Profil aus und klicken dann auf **OpenEdit**.
4. Legen **Sie im Dialogfeld SAML-SSO-Profile erstellen** oder im Dialogfeld **SAML-SSO-Profile konfigurieren** die folgenden Parameter fest:
   - Vorname*
   - Name des Signaturzertifikats*
   - ACS-URL*
   - Relaisstatusregel*
   - Kennwort senden
   - Name des Ausstellers

5. Klicken Sie auf **Erstellen** oder **OK**, und klicken Sie dann auf **Schließen.** Das von Ihnen erstellte SAML-SSO-Profil wird im Bereich Verkehrsrichtlinien, Profile und SAML-SSO-Profile angezeigt.

Sitzungstimeout für OWA 2010

Sie können jetzt OWA 2010-Verbindungen nach einer bestimmten Inaktivitätszeit zum Timeout zwingen. OWA sendet wiederholte Keepalive-Anfragen an den Server, um Timeouts zu verhindern. Wenn Sie die Verbindungen offen halten, kann das einmalige Anmelden beeinträchtigt werden.

So zwingen Sie OWA 2010 über die Befehlszeile zu einem Timeout nach einem bestimmten Zeitraum

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 add tm trafficAction <actname> [-forcedTimeout <forcedTimeout> -
     forcedTimeoutVal <mins>]
2 <!--NeedCopy-->
```

Ersetzen Sie <actname> durch den Namen Ihrer Verkehrsrichtlinie. Geben Sie für <mins> die Anzahl der Minuten ein, nach der ein erzwungenes Timeout eingeleitet werden soll. Ersetzen Sie <forcedTimeout> durch einen der folgenden Werte:

-**START** — Startet den Timer für erzwungenes Timeout, wenn noch kein Timer gestartet wurde. Wenn ein Lauftimer existiert, hat dies keine Auswirkung.
-**STOP** — Stoppt einen Lauftimer. Wenn kein Lauftimer gefunden wird, hat dies keine Auswirkung.
-**RESET** — Startet einen Lauftimer neu. Wenn kein Lauftimer gefunden wird, startet einen Timer, als ob die START-Option verwendet worden wäre.

```
1 add tm trafficPolicy <polname> <rule> <actname>
2 <!--NeedCopy-->
```

Ersetzen Sie <polname> durch den Namen Ihrer Verkehrsrichtlinie. Ersetzen Sie <rule> durch eine Regel in der NetScaler Advanced-Richtlinie.

```
1 bind lb vserver <vservername>  - policyName <name> -priority <number>
2 <!--NeedCopy-->
```

Ersetzen Sie <vservername> durch den Namen des virtuellen Servers für die Authentifizierung, Autorisierung und Überwachung des Verkehrsmanagements. Ersetzen Sie <priority> durch eine Ganzzahl, die die Priorität der Richtlinie angibt.

Beispiel


```
add tm trafficAction act-owa2010timeout -forcedTimeout RESET -
    forcedTimeoutVal 10
add tm trafficPolicy pol-owa2010timeout true act-owa2010timeout
bind lb vserver vs-owa2010 -policyName pol-owa2010timeout -priority 10
<!--NeedCopy-->
```

Ratenbegrenzung für NetScaler Gateway

May 11, 2023

Mit der Ratenbegrenzungsfunktion für NetScaler Gateway können Sie die maximale Last für eine bestimmte Netzwerkeinheit oder virtuelle Entität auf der NetScaler Gateway-Appliance definieren. Da das NetScaler Gateway-Gerät den gesamten nicht authentifizierten Datenverkehr verbraucht, ist das Gerät häufig Prozessanforderungen mit hoher Geschwindigkeit ausgesetzt. Mit der Ratenbegrenzungsfunktion können Sie das NetScaler Gateway Gerät so konfigurieren, dass die Datenverkehrsrate einer Entität überwacht und basierend auf dem Datenverkehr in Echtzeit vorbeugende Maßnahmen ergriffen werden. Weitere Informationen zur Funktionsweise der Ratenbegrenzung in einer NetScaler-Appliance finden Sie unter Ratenbegrenzung.

NetScaler verfügt über die Funktion zur Begrenzung der Rate, die Back-End-Server mit einer unvorhergesehenen Geschwindigkeit schützt. Da die Funktion für NetScaler den nicht authentifizierten Datenverkehr, den NetScaler Gateway verarbeitet, nicht bereitstellte, benötigte NetScaler Gateway seine eigenen ratenbegrenzenden Funktionen. Dies ist erforderlich, um eine unvorhergesehene Rate von Anfragen aus verschiedenen Quellen zu überprüfen, denen das NetScaler Gateway-Gerät ausgesetzt ist. Zum Beispiel nicht authentifizierte/Anmelde-/Steuerungsanfragen und bestimmte APIs, die für Endbenutzer- oder Gerätevalidierungen offengelegt wurden.

Häufige Anwendungsfälle für die Tarifbegrenzung

- Beschränken Sie die Anzahl der Anfragen pro Sekunde von einer URL.
- Trennen Sie eine Verbindung basierend auf Cookies, die auf Anfrage von einem bestimmten Host empfangen wurden, wenn die Anfrage das Ratenlimit überschreitet.
- Beschränken Sie die Anzahl der HTTP-Anfragen, die von demselben Host (mit einer bestimmten Subnetzmaske) eingehen und dieselbe Ziel-IP-Adresse haben.

Konfigurieren der Ratenbegrenzung für NetScaler Gateway

Voraussetzungen

Ein konfigurierter virtueller Authentifizierungsserver.

Wichtige Hinweise

- In den Konfigurationsschritten wird ein Sample-Limit Identifier konfiguriert. Dasselbe kann mit allen unterstützten Parametern wie Stream-Selektor, Modus konfiguriert werden. Eine erschöpfende Beschreibung der Ratenbegrenzungsfunktionen finden Sie unter Ratenbegrenzung.
- Die Richtlinie kann auch wie folgt an einen virtuellen VPN-Server gebunden werden. Sie benötigen einen konfigurierten virtuellen VPN-Server, um die Richtlinien mit dem folgenden Befehl zu binden.

```
bind vpn vserver  -policy denylogin  - pri 1  - type aaa_request
<!--NeedCopy-->
```

- AAA_REQUEST ist ein neu eingeführter Bindepunkt für Responder-Richtlinien. Die an diesem Bindepunkt konfigurierten Richtlinien werden auf alle eingehenden Anforderungen auf dem angegebenen virtuellen Server angewendet. Die Richtlinien werden für den nicht authentifizierten/kontrollierten Verkehr zuerst vor jeder anderen Verarbeitung verarbeitet.
- Das Binden der Richtlinie an den virtuellen NetScaler Gateway-Server ermöglicht die Ratenbegrenzung am AAA_REQUEST-Bindpunkt für den gesamten von NetScaler Gateway verbrauchten Datenverkehr, einschließlich nicht authentifizierter Anforderungen.
- Durch das Binden der Richtlinie an einen virtuellen Authentifizierungsserver werden die nicht authentifizierten/kontrollierten Anforderungen begrenzt, die den virtuellen Authentifizierungsserver treffen.

Um die Ratenbegrenzung über die Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add limitIdentifier <limitIdentifier name> -threshold <positive_integer
    > -timeslice <positive_integer> -mode <mode type>
<!--NeedCopy-->
```

Beispiel:

```
add limitIdentifier limit_one_login -threshold 10 -timeslice 4294967290
     -mode REQUEST_RATE
<!--NeedCopy-->
```



```
add responderaction denylogin respondwith  ‘ “HTTP/1.1 200 OK\r\n\r\n”
     +  “Request is denied due to unusual rate” ’
<!--NeedCopy-->
```

```
add responder policy denylogin 'sys.check_limit("limit_one_login")'
   denylogin
<!--NeedCopy-->
```

```
bind authentication vserver <vserver name> -policy denylogin  -pri 1  -
   type aaa_request
<!--NeedCopy-->
```

Beispiel:

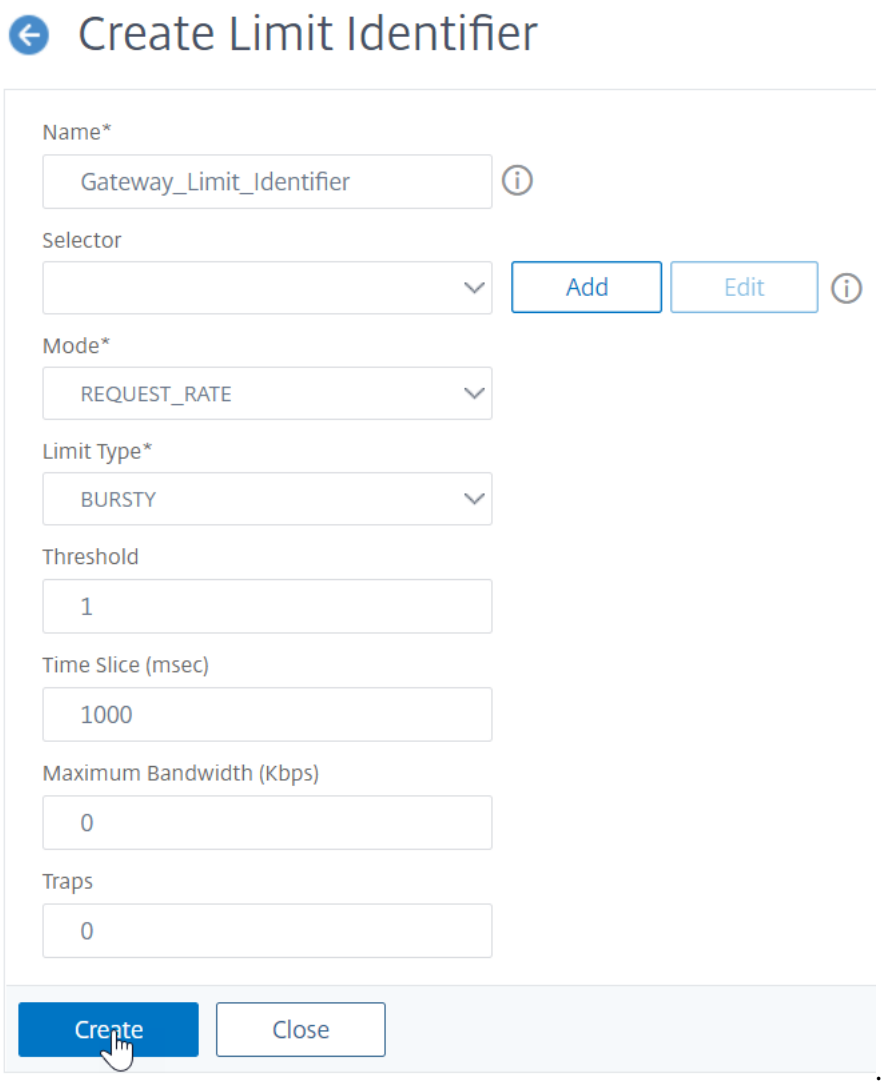
```
bind authentication vserver authvserver -policy denylogin  -pri 1  -
   type aaa_request
<!--NeedCopy-->
```

Beschreibung des Parameters

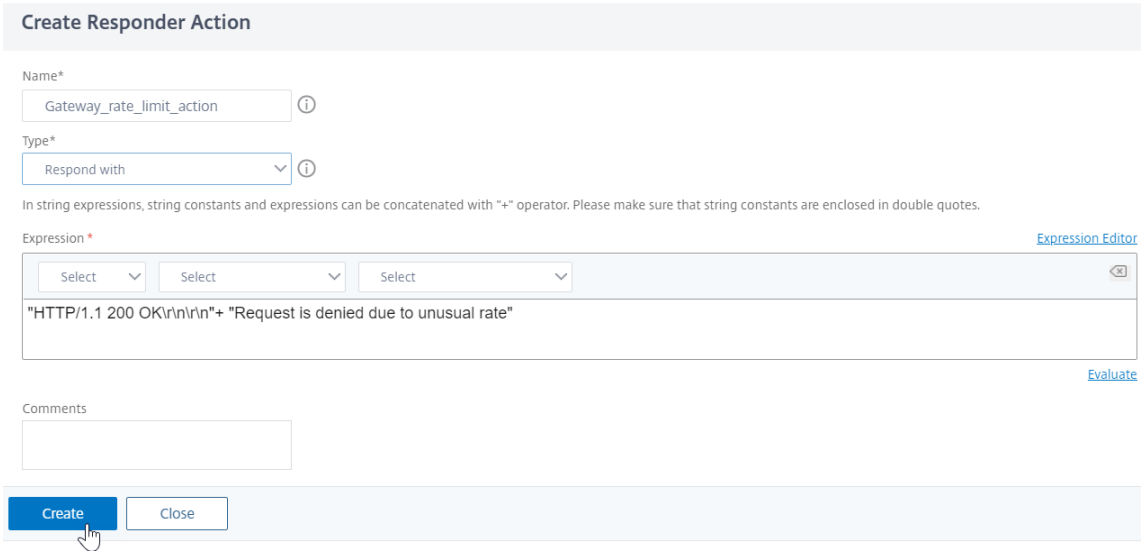
- **LimitIdentifier -** Name für eine Ratenbegrenzungs-ID. Muss mit einem ASCII-Buchstaben oder Unterstrich (_) beginnen und darf nur aus alphanumerischen ASCII-Zeichen oder Unterstrichen bestehen. Reservierte Wörter dürfen nicht verwendet werden. Dies ist ein zwingendes Argument. Maximale Länge: 31
- **Schwellenwert -** Eine maximale Anzahl von Anforderungen, die in der angegebenen Zeitleiste zulässig sind, wenn Anfragen (Modus ist als REQUEST_RATE festgelegt) pro Timeslice verfolgt werden. Wenn Verbindungen (Modus ist als CONNECTION eingestellt) verfolgt werden, ist dies die Gesamtzahl der Verbindungen, die durchgelassen würden. Standardwert: 1 Minimalwert: 1 Maximalwert: 4294967295
- **TimeSlice -** Zeitintervall in Millisekunden, angegeben in Vielfachen von 10, in dem Anfragen verfolgt werden, um zu überprüfen, ob sie den Schwellenwert überschreiten. Das Argument wird nur benötigt, wenn der Modus auf REQUEST_RATE gesetzt ist. Standardwert: 1000 Mindestwert: 10 Maximalwert: 4294967295
- **mode -** Definiert die Art des Traffics, der verfolgt werden soll.
  - REQUEST_RATE - Verfolgt Anforderungen/Timeslice.
  - CONNECTION - Verfolgt aktive Transaktionen.

So konfigurieren Sie die Ratenbegrenzung über die NetScaler-GUI:

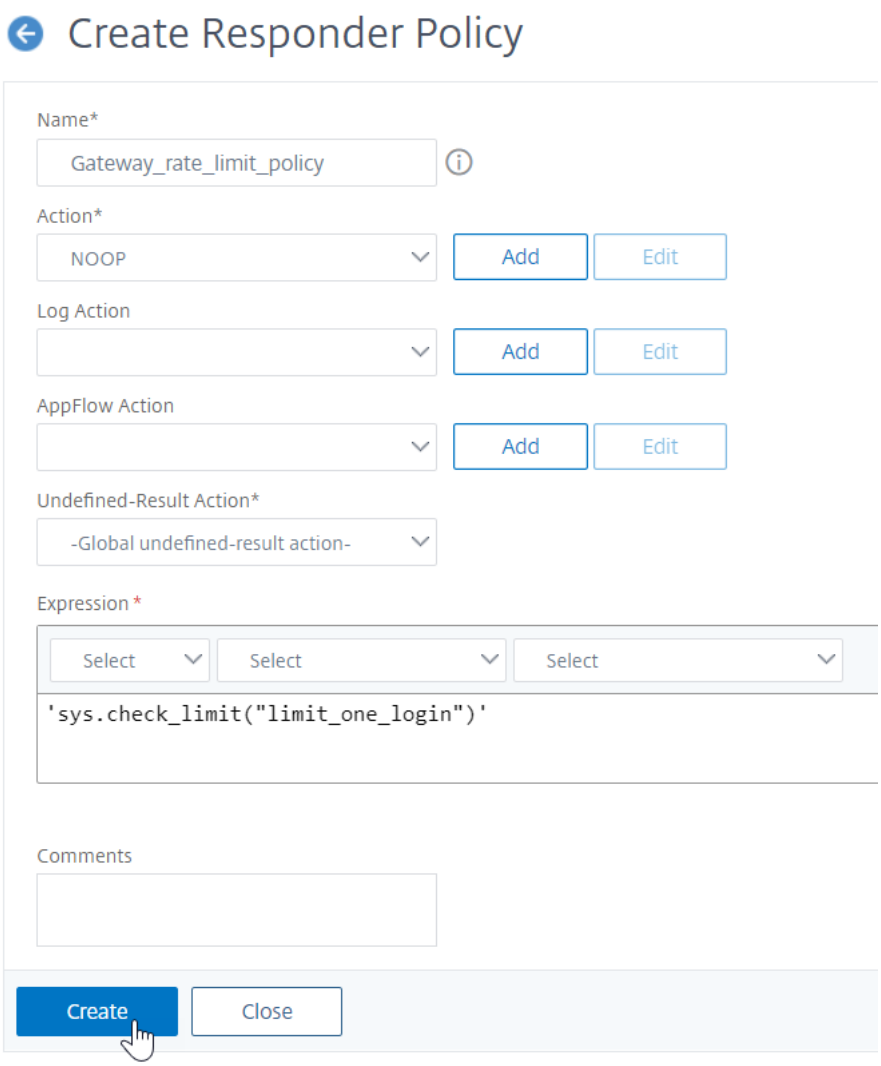
1. Navigieren Sie zu **AppExpert > Ratenbegrenzung > Limitkennungen**, klicken Sie auf **Hinzufügen**, und geben Sie die entsprechenden Details an, wie im CLI-Abschnitt angegeben.



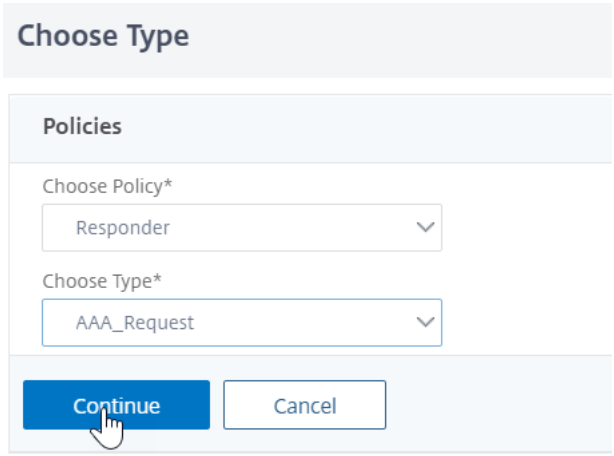
2. Navigieren Sie zu **AppExpert>Responder>Richtlinien**. Klicken Sie auf der Seite **Responder-Richtlinien** auf **Hinzufügen**.
3. Erstellen Sie auf der Seite **Responder Policy erstellen** eine Responder-Richtlinie mit einer Responder Action, die über die Limit-ID verfügt.
4. Um eine Responder Action zu erstellen, klicken Sie neben **Aktion** auf **Hinzufügen** und geben Sie einen Namen für die Responder Action ein.
5. Wählen Sie im Dropdown-Menü den Typ als **Antworten mit** aus, geben Sie den folgenden Ausdruck an: “HTTP/1.1 200 OK\ r\ n\ r\ n”+ “Anforderung wird aufgrund ungewöhnlicher Rate verweigert”, und klicken Sie auf **Erstellen**.



6. Um eine Responder Policy zu **erstellen, geben Sie auf der Seite Responder Policy** erstellen einen Namen für die Responder-Richtlinie ein, geben Sie den folgenden Ausdruck an: ‘sys.check_limit (“limit_one_login”) ‘, und klicken Sie auf **Erstellen**.



7. Binden Sie die Responder Policy an den virtuellen Authentifizierungsserver.
   - Gehen Sie zu **Sicherheit> AAA-Anwendungsverkehr> Virtueller Server**.
   - Wählen Sie den virtuellen Server aus.
   - Fügen Sie eine Richtlinie hinzu.
   - Wählen Sie die Responder Policy aus, die Sie an den Server binden möchten, und legen Sie die Priorität fest.
   - Wählen Sie den Typ als **AAA-REQUEST** und klicken Sie auf **Weiter**.



> **Hinweis:** Sie können die Ratenbegrenzung auch am AAA_REQUEST-Bindpunkt für den virtuellen VPN-Server aktivieren.

Konfiguration für die gängigen Anwendungsfälle zum Anwenden von Ratenbegrenzung auf NetScaler Gateway

Im Folgenden sind die Beispiele für Befehle zum Konfigurieren allgemeiner Anwendungsfälle aufgeführt.

- Beschränken Sie die Anzahl der Anfragen pro Sekunde von einer URL.

```
1  add stream selector ipStreamSelector http.req.url  “client.ip.src
       ”
2
3  add ns limitIdentifier ipLimitIdentifier  -threshold 4  -
       timeslice 1000  -mode request_rate  -limitType smooth  -
       selectorName ip StreamSelector
4
5  add responder policy ipLimitResponderPolicy  “http.req.url.
       contains(\” myasp.asp\” ) && sys.check_limit(\”
       ipLimitIdentifier\” )”  myWebSiteRedirectAction
6
7  bind authentication virtual server authvserver -policy denylogin
       -pri 1  -type aaa_request
8  <!--NeedCopy-->
```

- Lösen Sie eine Verbindung basierend auf Cookies, die auf Anfrage von www.yourcompany.com erhalten wurden, wenn die Anfrage das Tariflimit überschreitet.

```
1  add stream selector cacheStreamSelector  “http.req.cookie.value(\
       ” mycookie\” )”   “client.ip.src.subnet(24)”
2
```



```
add ns limitIdentifier myLimitIdentifier -Threshold 2 -
    timeSlice 3000 -selectorName reqCookieStreamSelector

add responder action sendRedirectURL redirect `"http://www.
    mycompany.com"` + http.req.url'

add responder policy rateLimitCookiePolicy

 “http.req.url.contains(\www.yourcompany.com) && sys.check_limit
    (\” myLimitIdentifier\” )” sendRedirectUrl

<!--NeedCopy-->
```

- Beschränken Sie die Anzahl der HTTP-Anfragen, die vom selben Host (mit einer Subnetzmaske von 32) eingehen und dieselbe Ziel-IP-Adresse haben.

```
add stream selector ipv6_sel “CLIENT.IPv6.src.subnet(32)” CLIENT
    .IPv6.dst

add ns limitIdentifier ipv6_id -imeSlice 20000 -selectorName
    ipv6_sel

add lb vserver ipv6_vip HTTP 3ffe:: 209 80 -persistenceType NONE
     -cltTime

add responder action redirect_page redirect “\” `http://
    redirectpage.com/\” "`

add responder policy ipv6_resp_pol “SYS.CHECK_LIMIT(\” ipv6_id\
    ” )” redirect_page

bind responder global ipv6_resp_pol 5 END -type DEFAULT
<!--NeedCopy-->
```

Autorisieren des Benutzerzugriffs auf Anwendungsressourcen

November 17, 2022

Sie können die Ressourcen steuern, auf die ein authentifizierter Benutzer innerhalb einer Anwendung zugreifen kann.

Ordnen Sie dazu jedem Benutzer eine Autorisierungsrichtlinie zu, entweder einzeln oder indem Sie die Richtlinie einer Benutzergruppe zuordnen. Die Autorisierungsrichtlinie muss Folgendes spezifizieren:

- **Regel.** Die Ressource, für die der Zugriff autorisiert werden muss. Dies kann mit einfachen oder erweiterten Ausdrücke spezifiziert werden.
- **Aktion.** Ob der Zugriff auf die Ressource erlaubt oder verweigert werden muss.

Standardmäßig wird allen Benutzern der Zugriff auf alle Ressourcen innerhalb einer Anwendung **VERWEIGERT**. Sie können diese standardmäßige Autorisierungsaktion jedoch so ändern, dass allen Benutzern der Zugriff **gewährt** wird (indem Sie die Sitzungsparameter im Sitzungsprofil oder die globalen Sitzungsparameter festlegen).

> **Warnung**
>
> Für optimale Sicherheit empfiehlt Citrix, die Standardautorisierungsaktion nicht von DENY in ALLOW zu ändern. Stattdessen wird empfohlen, spezifische Autorisierungsrichtlinien für Benutzer zu erstellen, die Zugriff auf bestimmte Ressourcen benötigen.

So konfigurieren Sie die Autorisierung über die CLI

1. Konfigurieren Sie die Autorisierungsrichtlinie.

   ns-cli-prompt> **add authorization policy <name> <rule> <action>**

2. Ordnen Sie die Richtlinie dem entsprechenden Benutzer oder der entsprechenden Gruppe zu.
   - Binden Sie die Richtlinie an einen bestimmten Benutzer.

     ns-cli-prompt> **bind aaa user <username> -policy** <policyname>
   - Binden Sie die Richtlinie an eine bestimmte Gruppe.

     ns-cli-prompt> **bind aaa group <groupName> -policy** <policyname>

So konfigurieren Sie die Autorisierung über die GUI (Registerkarte “Konfiguration”)

1. Erstellen Sie die Autorisierungsrichtlinie.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Autorisierung**, klicken Sie auf **Hinzufügen** und definieren Sie dann die Richtlinie nach Bedarf.

2. Ordnen Sie die Richtlinie dem entsprechenden Benutzer oder der entsprechenden Gruppe zu.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Benutzer** oder **Gruppen**und bearbeiten Sie den entsprechenden Benutzer oder die entsprechende Gruppe, um ihn der Autorisierungsrichtlinie zuzuordnen.

Beispiele für Autorisierungskonfigurationen

Im Folgenden finden Sie einige Beispielkonfigurationen, um den Benutzerzugriff auf einige Anwendungsressourcen zu autorisieren. Beachten Sie, dass dies CLI-Befehle sind. Sie können ähnliche Kon-

figurationen mit der GUI durchführen, allerdings dürfen Sie den Ausdruck nicht in Anführungszeichen (“) setzen.

- “‘
  add authorization policy authzpol1 “HTTP.REQ.URL.SUFFIX.EQ(“gif”)” ALLOW
  “‘
  -
  ```
  bind aaa user user1 -policy authzpol1
  ```
- “‘
  add authorization policy authzpol2 “HTTP.REQ.URL.SUFFIX.EQ(“png”)” DENY
  “‘
  -
  ```
  bind aaa group group1 -policy authzpol2
  <!--NeedCopy-->
  ```

Authentifizierte Sitzungen prüfen

May 11, 2023

Sie können die NetScaler-Appliance so konfigurieren, dass sie ein Protokoll aller Ereignisse führt, die in einer authentifizierten Sitzung ausgelöst werden. Anhand dieser Informationen können Sie Status- und Statusinformationen überprüfen, um den Verlauf für Benutzer in chronologischer Reihenfolge einzusehen.

Definieren Sie dazu eine Prüfungsrichtlinie, die Folgendes festlegt:

- **Protokolltyp.** Die Protokolle können remote (Syslog) oder lokal auf der NetScaler-Appliance (nslog) gespeichert werden.
- **Regel.** Die Bedingungen, unter denen die Protokolle gespeichert werden.
- **Aktion.** Details des Logservers und weitere Details zur Erstellung der Logeinträge.

Diese Prüfungsrichtlinie kann auf verschiedenen Ebenen konfiguriert werden: Benutzerebene, Gruppenebene, Authentifizierung, Autorisierung und Überwachung virtueller Server sowie globaler Systemebene. Die auf Benutzerebene konfigurierten Richtlinien haben die höchste Priorität.

> **Hinweis**
>
> In diesem Thema werden die Schritte zur Verwendung von Syslog beschrieben. Nehmen Sie die erforderlichen Änderungen vor, um nslog zu verwenden.

So konfigurieren Sie die Syslog-Überwachung mithilfe der CLI

1. Konfigurieren Sie den Auditserver mit den entsprechenden Protokolleinstellungen.

ns-cli-prompt> **add audit syslogAction <name> <serverIP> ...**

2. Konfigurieren Sie die Überwachungsrichtlinie, indem Sie den Auditserver zuordnen.

   ns-cli-prompt> **add audit syslogPolicy <name> <rule> <action>**

3. Ordnen Sie die Prüfungsrichtlinie einer der folgenden Entitäten zu:

   - Binden Sie die Richtlinie an einen bestimmten Benutzer.

     ns-cli-prompt> **bind aaa user <userName>-policy** <policyname> …

   - Binden Sie die Richtlinie an eine bestimmte Gruppe.

     ns-cli-prompt> **bind aaa group <groupName>-policy** <policyname> …

   - Binden Sie die Richtlinie an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

     ns-cli-prompt> **bind authentication vserver <name> -policy** <policyname> …

   - Binden Sie die Richtlinie global an die NetScaler-Appliance.

     ns-cli-prompt> **bind tm global -policyName** <policyname> …

So konfigurieren Sie die Syslog-Überwachung mithilfe der GUI (Registerkarte „Konfiguration“)

1. Konfigurieren Sie den Audit-Server und die Richtlinie.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Auditing > Syslog**und konfigurieren Sie den Server und die Richtlinie in den entsprechenden Tabs.

2. Ordnen Sie die Richtlinie einer der folgenden zu:

   - Binden Sie die Richtlinie an einen bestimmten Benutzer.

     Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Benutzer**und ordnen Sie die Autorisierungsrichtlinie dem entsprechenden Benutzer zu.

   - Binden Sie die Richtlinie an eine bestimmte Gruppe.

     Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Gruppen**und ordnen Sie die Autorisierungsrichtlinie der entsprechenden Gruppe zu.

   - Binden Sie die Richtlinie an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

     Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**und verknüpfen Sie die Autorisierungsrichtlinie mit dem entsprechenden virtuellen Server.

- Binden Sie die Richtlinie global an die NetScaler-Appliance.

  Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Auditing > Syslog oder**Nslog****, wählen Sie die Autorisierungsrichtlinie aus und klicken Sie auf **Aktion > Globale Bindungen, um die Richtlinie global** zu binden.

NetScaler als Active Directory Federation Services-Proxy

May 11, 2023

Active Directory Federation Services (ADFS) ist ein Microsoft-Dienst, der Active Directory-authentifizierten Clients das Single Sign-On (SSO)-Erlebnis für Ressourcen außerhalb des Unternehmensrechenzentrums ermöglicht. Eine ADFS-Serverfarm ermöglicht internen Benutzern den Zugriff auf externe, in der Cloud gehostete Dienste. Sobald jedoch externe Benutzer hinzukommen, muss den externen Benutzern die Möglichkeit gegeben werden, eine Remote-Verbindung herzustellen und über eine föderierte Identität auf cloudbasierte Dienste zuzugreifen. Die meisten Unternehmen ziehen es nicht vor, den ADFS-Server in der DMZ verfügbar zu halten. Daher spielt der ADFS-Proxy eine entscheidende Rolle bei der Remotebenutzerkonnektivität und dem Anwendungszugriff.

Seit mehr als einem Jahrzehnt spielt die NetScaler Appliance ähnliche Rollen bei der Remotebenutzerkonnektivität und dem Anwendungszugriff. Die NetScaler-Appliance wird zur bevorzugten Lösung, die als ADFS-Proxy zur Unterstützung einer neuen ADFS-Implementierung verwendet wird, um die folgenden Dienste zu aktivieren:

- Sichere Konnektivität.
- Authentifizierung und Behandlung von Federated Identity.

Weitere Informationen über NetScaler als SAML-IdP finden Sie unter NetScaler as a SAML IdP.

Vorteile des ADFS-Proxy

- Reduziert den Platzbedarf in der DMZ, um den Anforderungen der meisten Unternehmen gerecht zu werden.
- Bietet ein SSO-Erlebnis für Endbenutzer.
- Unterstützt umfangreiche Methoden zur Vorauthentifizierung und ermöglicht die Multifaktor-Authentifizierung.
- Unterstützt sowohl aktive als auch passive Clients.

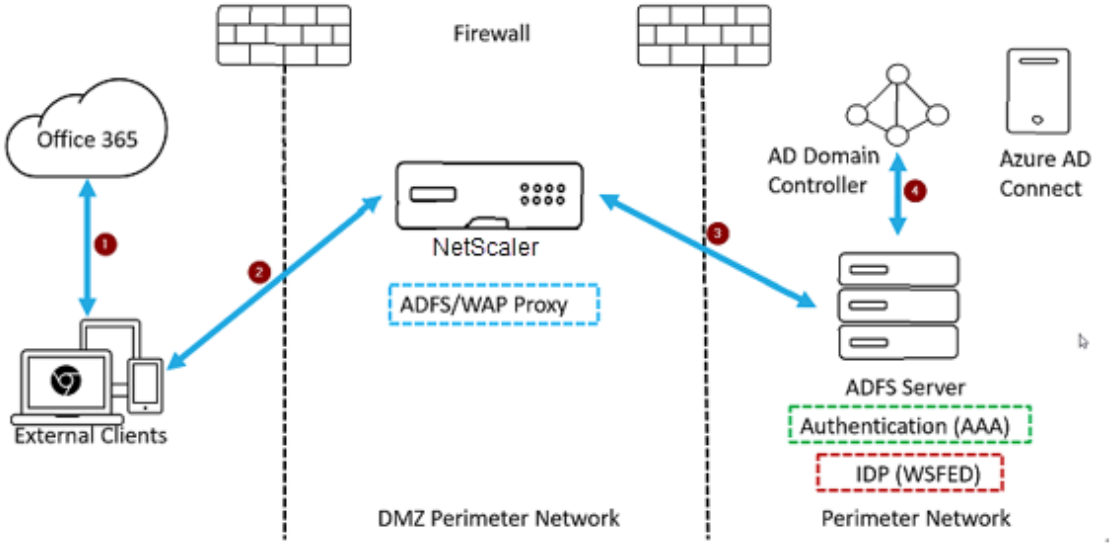
Voraussetzungen für die Verwendung von NetScaler als ADFS-Proxy

Bevor Sie die NetScaler Appliance als ADFS-Proxy konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Eine NetScaler Appliance mit 12.1 Build oder höher.
- ADFS-Server für die Domäne.
- Domain-SSL-Zertifikat.
- Virtuelle IP für den virtuellen Content Switching-Server.
- Aktivieren Sie die Funktionen Load Balancing, SSL-Offload, Content Switching, Rewrite sowie Authentifizierung, Autorisierung und Prüfung des Verkehrsmanagements auf der NetScaler Appliance.

Konfigurieren Sie die NetScaler-Appliance als ADFS-Proxy

Um diesen Anwendungsfall zu erreichen, konfigurieren Sie NetScaler als ADFS-Proxy in einer DMZ-Zone. Der ADFS-Server wird zusammen mit dem AD-Domänencontroller im Back-End konfiguriert.



1. Eine Client-Anfrage für den Zugriff auf Microsoft Office365 wird an NetScaler umgeleitet, das als ADFS-Proxy bereitgestellt wird.
2. Die Anmeldeinformationen des Benutzers werden an den ADFS-Server übergeben.
3. Der ADFS-Server authentifiziert die Anmeldeinformationen mit dem on-premises AD der Domäne.
4. Der ADFS-Server generiert nach erfolgreicher Validierung der Anmeldeinformationen mit AD ein Token, das zur Sitzungseinrichtung an Microsoft Office365 übergeben wird.

Im Folgenden sind die grundlegenden Schritte zur Konfiguration der NetScaler Appliance aufgeführt, bevor Sie sie als ADFS-Proxy konfigurieren.

Geben Sie an der NetScaler-Befehlszeile die folgenden Befehle ein:

1. Erstellen Sie ein SSL-Profil für das Back-End und aktivieren Sie SNI im SSL-Profil. Deaktivieren Sie SSLv3/TLS1.


```
add ssl profile <new SSL profile> -sslprofileType backEnd -sniEnable
ENABLED -ssl3 DISABLED -tls1 DISABLED -commonName <FQDN of ADFS>
```

2. Deaktivieren Sie SSLv3/TLS1 für den Dienst.

```
set ssl service <adfs service name> -sslProfile <SSL profile created in
 the above step>
```

3. SNI-Erweiterung für Back-End-Server-Handshakes aktivieren.

   - `set vpn parameter -backendServerSni ENABLED`
   - `set ssl parameter -denySSLReneg NONSECURE`

Konfigurieren Sie die NetScaler Appliance als ADFS-Proxy mithilfe der CLI

Die folgenden Abschnitte sind nach den Anforderungen zum Abschluss der Konfigurationsschritte kategorisiert.

So konfigurieren Sie den ADFS-Dienst

1. Konfigurieren Sie den ADFS-Dienst auf NetScaler für den ADFS-Server.

```
add service <Domain_ADFS_Service> <ADFS Server IP> SSL 443 -gslb NONE -
maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF
-cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
```

   Beispiel

   add service CTXTEST_ADFS_Service 1.1.1.1 SSL 443 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

2. Konfigurieren Sie den FQDN für den virtuellen Content Switching-Server und aktivieren Sie SNI.

```
set ssl service <Domain_ADFS_Service> -SNIEnable ENABLED -commonName <
sts.domain.com>
```

   Beispiel

   set ssl service CTXTEST_ADFS_Service -SNIEnable ENABLED -commonName sts.ctxtest.com

Konfigurieren des virtuellen ADFS-Lastausgleichsservers

> **Wichtig**
>
> Für sicheren Datenverkehr ist ein Domain-SSL-Zertifikat (SSL_CERT) erforderlich.

1. Konfigurieren Sie den virtuellen ADFS-Lastausgleichsserver.

   ```
   add lb vserver <Domain_ADFS_LBVS> SSL <IP_address> -persistenceType
   NONE -cltTimeout 180
   ```

   Beispiel

   ```
   add lb vserver CTXTEST_ADFS_LBVS SSL 192.168.1.0 -persistenceType NONE
   -cltTimeout 180
   ```

2. Binden Sie den virtuellen ADFS-Lastenausgleichsserver an den ADFS-Dienst.

   ```
   bind lb vserver <Domain_ADFS_LBVS> <Domain_ADFS_Service>
   ```

   Beispiel

   ```
   bind lb vserver CTXTEST_ADFS_LBVS CTXTEST_ADFS_Service
   ```

3. Binden Sie ein Schlüsselpaar für das Zertifikat eines virtuellen SSL-Servers.

   ```
   bind ssl vserver <Domain_ADFS_LBVS> -certkeyName <SSL_CERT>
   ```

   Beispiel

   ```
   bind ssl vserver CTXTEST_ADFS_LBVS -certkeyName ctxtest_newcert_2019
   ```

So konfigurieren Sie den virtuellen Content Switching-Server für die Domäne

> **Hinweis**
>
> Für einen virtuellen Content Switching-Server ist eine freie virtuelle IP (z. B. 2.2.2.2) erforderlich, die für eine öffentliche IP vorgesehen ist. Es muss sowohl für externen als auch für internen Verkehr erreichbar sein.

1. Erstellen Sie einen virtuellen Content Switching-Server mit kostenlosem VIP.

   ```
   add cs vserver <Domain_CSVS> SSL <FREE VIP> 443 -cltTimeout 180 -
   persistenceType NONE
   ```

   Beispiel

   ```
   add cs vserver CTXTEST_CSVS SSL 2.2.2.2 443 -cltTimeout 180 -persistenceType
    NONE
   ```

2. Binden Sie den virtuellen Content Switching-Server an den virtuellen Lastausgleichsserver.

   ```
   bind cs vserver <Domain_CSVS> -lbvserver <Domain_ADFS_LBVS>
   ```

   Beispiel

   - `bind cs vserver CTXTEST_CSVS -lbvserver CTXTEST_ADFS_LBVS`
   - `set ssl vserver CTXTEST_CSVS -sessReuse DISABLED`

3. Binden Sie ein Schlüsselpaar für das Zertifikat eines virtuellen SSL-Servers.

   ```
   bind ssl vserver <Domain_CSVS> -certkeyName <SSL_CERT>
   ```

   Beispiel

   ```
   bind ssl vserver CTXTEST_CSVS -certkeyName ctxtest_newcert_2019
   ```

Unterstützte Protokolle

Die von Microsoft bereitgestellten Protokolle spielen eine wichtige Rolle bei der Integration in die NetScaler Appliance. NetScaler als ADFS-Proxy unterstützt die folgenden Protokolle:

- **WS-Verbund**. Weitere Informationen finden Sie unter Protokoll des Web Services Federation.
- **ADFSPIP**. Weitere Informationen finden Sie unter Compliance des Active Directory-Verbunddienst-Proxy Integration Protocol

> **Hinweis**
>
> Die NetScaler Appliance unterstützt keine Gerätezertifikatauthentifizierung, wenn sie als ADFS-Proxy bereitgestellt wird.

Web Services Federation Protokoll

May 11, 2023

Web Services Federation (WS-Federation) ist ein Identitätsprotokoll, das es einem Security Token Service (STS) in einer Vertrauensdomäne ermöglicht, Authentifizierungsinformationen für einen STS in einer anderen Vertrauensdomäne bereitzustellen, wenn zwischen den beiden Domänen eine Vertrauensbeziehung besteht.

Vorteile von WS-Federation

WS-Federation unterstützt sowohl aktive als auch passive Clients, während SAML IdP nur passive Clients unterstützt.

- Aktive Kunden sind native Microsoft-Clients wie Outlook- und Office-Clients (Word, PowerPoint, Excel und OneNote).
- Passive Clients sind browserbasierte Clients wie Google Chrome, Mozilla Firefox und Internet Explorer.

Voraussetzungen für die Verwendung von NetScaler als WS-Federation

Bevor Sie die NetScaler-Appliance als ADFS-Proxy konfigurieren, überprüfen Sie Folgendes:

- Active Directory
- Domain-SSL-Zertifikat.
- Das NetScaler-SSL-Zertifikat und das ADFS-Tokensignierungszertifikat auf dem ADFS-Server müssen identisch sein.

> **Wichtig** SAML-IdP ist jetzt in der Lage, das WS-Federation-Protokoll zu verarbeiten. Um den WS-Federation-IdP zu konfigurieren, müssen Sie daher den SAML-IdP tatsächlich konfigurieren. Sie sehen keine Benutzeroberfläche, in der WS-Federation ausdrücklich erwähnt wird.

Funktionen, die von NetScaler unterstützt werden, wenn sie als ADFS-Proxy und WS-Federation IdP konfiguriert sind

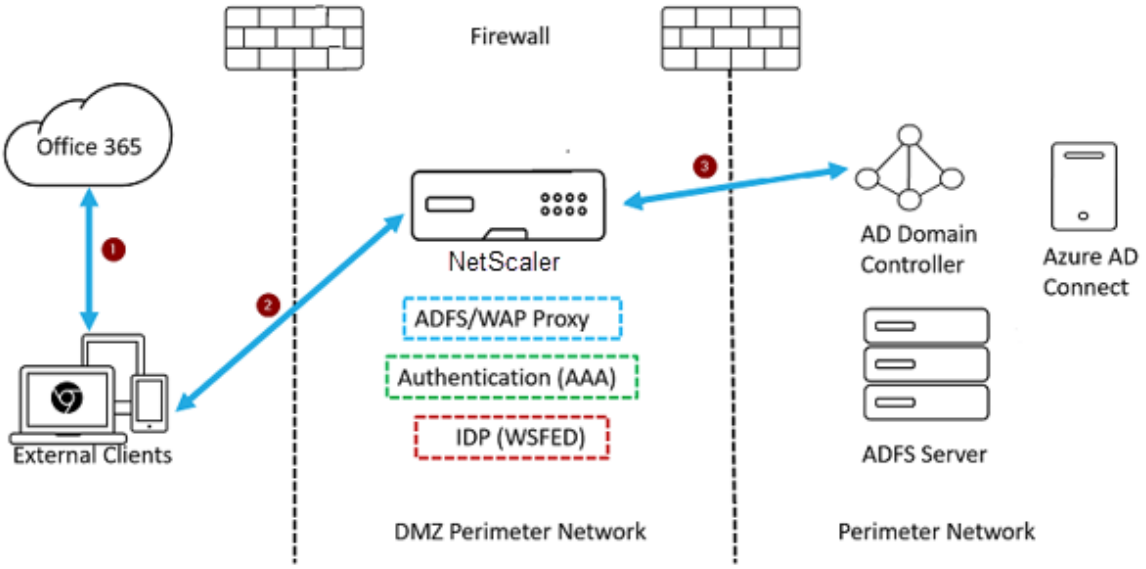
In der folgenden Tabelle sind die Funktionen aufgeführt, die von der NetScaler-Appliance unterstützt werden, wenn sie als ADFS-Proxy und WS-Federation-IdP konfiguriert ist.

Features	Konfigurieren Sie die NetScaler-Appliance als ADFS-Proxy	NetScaler als WS-Federation-IdP	NetScaler als ADFSPIP
Lastausgleich	Ja	Ja	Ja
SSL-Kündigung	Ja	Ja	Ja
Ratenbegrenzung	Ja	Ja	Ja
Konsolidierung (reduziert den Platzbedarf des DMZ-Servers und spart öffentliches IP)	Ja	Ja	Ja
Firewall für Webanwendungen (WAF)	Ja	Ja	Ja
Authentifizierung auf NetScaler Appliance auslagern	Ja	Ja (aktive und passive Kunden)	Ja
Single Sign-On (SSO)	Ja	Ja (aktive und passive Kunden)	Ja

Features	Konfigurieren Sie die NetScaler-Appliance als ADFS-Proxy	NetScaler als WS-Federation-IdP	NetScaler als ADFSPIP
Mehrstufige Authentifizierung (nFactor)	Nein	Ja (aktive und passive Kunden)	Ja
Azure-Multifaktor-Authentifizierung	Nein	Ja (aktive und passive Kunden)	Ja
ADFS-Serverfarm kann vermieden werden	Nein	Ja	Ja

NetScaler Appliance als WS-Federation IdP konfigurieren

Konfigurieren Sie NetScaler als WS-Federation IdP (SAML IdP) in einer DMZ-Zone. Der ADFS-Server wird zusammen mit dem AD-Domänencontroller im Back-End konfiguriert.



1. Die Client-Anfrage an Microsoft Office365 wird an die NetScaler-Appliance umgeleitet.
2. Der Benutzer gibt die Anmeldeinformationen für die Multifaktor-Authentifizierung ein.
3. NetScaler validiert die Anmeldeinformationen mit AD und generiert ein Token nativ auf der NetScaler-Appliance. Die Anmeldeinformationen werden für den Zugriff an Office365 übergeben.

> **Hinweis**
>
> Die Unterstützung von WS-Federation IdP erfolgt im Vergleich zum Load Balancer von F5 Networks nativ über die NetScaler-Appliance.

Konfigurieren Sie die NetScaler-Appliance mithilfe der CLI als WS-Federation IdP (SAML IdP)

Die folgenden Abschnitte sind nach den Anforderungen zum Abschluss der Konfigurationsschritte kategorisiert.

So konfigurieren Sie die LDAP-Authentifizierung und fügen eine Richtlinie hinzu

> **Wichtig**
>
> Für Domänenbenutzer müssen Sie Folgendes konfigurieren, um sich mit ihren Unternehmens-E-Mail-Adressen bei der NetScaler-Appliance anzumelden:

- Konfigurieren Sie den LDAP-Authentifizierungsserver und die LDAP-Richtlinie auf der NetScaler-Appliance.
- Binden Sie es an Ihre virtuelle Authentifizierungs-, Autorisierungs- und Auditing-IP-Adresse (die Verwendung einer vorhandenen LDAP-Konfiguration wird ebenfalls unterstützt).

```
add authentication ldapAction <Domain_LDAP_Action> -serverIP <Active
    Directory IP> -serverPort 636 -ldapBase "cn=Users,dc=domain,dc=com"
    -ldapBindDn "cn=administrator,cn=Users,dc=domain,dc=com" -
    ldapBindDnPassword <administrator password> -encrypted -
    encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
     memberOf -subAttributeName cn -secType SSL -ssoNameAttribute
    UserPrincipalName -followReferrals ON -Attribute1 mail -Attribute2
    objectGUID

add authentication Policy <Domain_LDAP_Policy> -rule true -action <
    Domain_LDAP_Action>
<!--NeedCopy-->
```

Beispiel

```
add authentication ldapAction CTXTEST_LDAP_Action -serverIP 3.3.3.3 -
    serverPort 636 -ldapBase "cn=Users,dc=ctxtest,dc=com" -ldapBindDn "
    cn=administrator,cn=Users,dc=ctxtest,dc=com" -ldapBindDnPassword
    xxxxxxxxxx -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
    sAMAccountName -groupAttrName memberOf -subAttributeName cn -secType
     SSL -ssoNameAttribute UserPrincipalName -followReferrals ON -
    Attribute1 mail -Attribute2 objectGUID
```



```
2
3 add authentication Policy CTXTEST_LDAP_Policy -rule true -action
     CTXTEST_LDAP_Action
4 <!--NeedCopy-->
```

So konfigurieren Sie NetScaler als WS-Federation IdP oder SAML IdP

Erstellen Sie eine WS-Federation IdP (SAML IdP) -Aktion und -Richtlinie für die Tokengenerierung. Binden Sie es später an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

```
1 add authentication samlIdPProfile <Domain_SAMLIDP_Profile> -
     samlIdPCertName <SSL_CERT> -assertionConsumerServiceURL "https://
     login.microsoftonline.com/login.srf" -samlIssuerName <Issuer Name
     for Office 365 in ADFS Server> -rejectUnsignedRequests OFF -audience
      urn:federation:MicrosoftOnline -NameIDFormat persistent -NameIDExpr
      "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1 IDPEmail -
     Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
2
3 add authentication samlIdPPolicy <Domain_SAMLIDP_Policy> -rule "HTTP.
     REQ.HEADER("referer").CONTAINS("microsoft") || true" -action <
     Domain_SAMLIDP_Profile>
4 <!--NeedCopy-->
```

Beispiel

```
1 add authentication samlIdPProfile CTXTEST_SAMLIDP_Profile -
     samlIdPCertName ctxtest_newcert_2019 -assertionConsumerServiceURL "
     https://login.microsoftonline.com/login.srf" -samlIssuerName "http
     ://ctxtest.com/adfs/services/trust/" -rejectUnsignedRequests OFF -
     audience urn:federation:MicrosoftOnline -NameIDFormat persistent -
     NameIDExpr "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1
     IDPEmail -Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
2
3 add authentication samlIdPPolicy CTXTEST_SAMLIDP_Policy -rule "HTTP.REQ
     .HEADER("referer").CONTAINS("microsoft") || true" -action
     CTXTEST_SAMLIDP_Profile
4 <!--NeedCopy-->
```

Um einen virtuellen Server für Authentifizierung, Autorisierung und Überwachung zu konfigurieren, um die Mitarbeiter zu authentifizieren, die sich mit Unternehmensanmeldeinformationen bei Office365 anmelden


```
add authentication vserver <Domain_AAA_VS> SSL <IP_address>`
<!--NeedCopy-->
```

Beispiel

```
add authentication vserver CTXTEST_AAA_VS SSL 192.168.1.0

bind authentication vserver CTXTEST_AAA_VS -portaltheme RfWebUI
<!--NeedCopy-->
```

Um den virtuellen Authentifizierungsserver und die Richtlinie zu binden

```
bind authentication vserver <Domain_AAA_VS> -policy <
    Domain_SAMLIDP_Policy> -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver <Domain_AAA_VS> -policy <Domain_LDAP_Policy
    > -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Beispiel

```
bind authentication vserver CTXTEST_AAA_VS -policy
    CTXTEST_SAMLIDP_Policy -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver CTXTEST_AAA_VS -policy CTXTEST_LDAP_Policy
    -priority 100 -gotoPriorityExpression NEXT

bind ssl vserver CTXTEST_AAA_VS -certkeyName ctxtest_newcert_2019
<!--NeedCopy-->
```

So konfigurieren Sie Content Switching

```
add cs action <Domain_CS_Action> -targetVserver <Domain_AAA_VS>

add cs policy <Domain_CS_Policy> -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action <Domain_CS_Action>
<!--NeedCopy-->
```

Beispiel

```
add cs action CTXTEST_CS_Action -targetVserver CTXTEST_AAA_VS

```



```
add cs policy CTXTEST_CS_Policy -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action CTXTEST_CS_Action
<!--NeedCopy-->
```

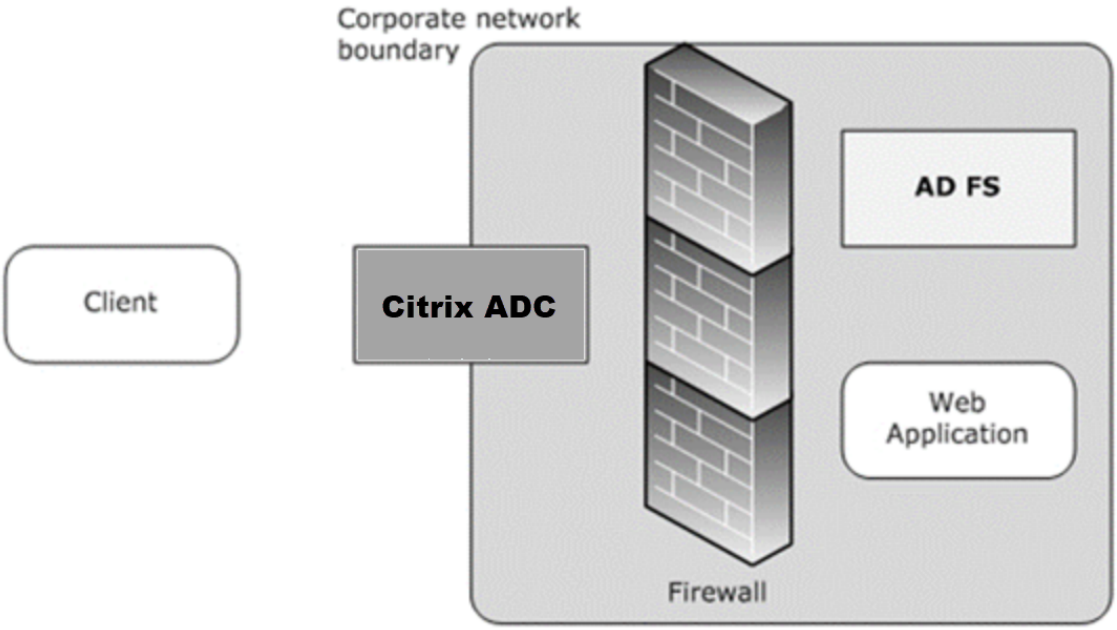
Um den virtuellen Content Switching-Server an die Richtlinie zu binden

```
bind cs vserver CTXTEST_CSVS -policyName CTXTEST_CS_Policy -priority
    100
<!--NeedCopy-->
```

Compliance des Active Directory-Verbunddienstproxy-

June 19, 2023

Wenn Drittanbieter-Proxys anstelle des Webanwendungsproxys verwendet werden sollen, müssen sie das MS-ADFSPIP-Protokoll unterstützen, das die ADFS- und WAP-Integrationsregeln festlegt. ADFSPIP integriert Active Directory Federation Services mit einem Authentifizierungs- und Anwendungsproxy, um Clients, die sich außerhalb dieser Grenze befinden, Zugriff auf Dienste innerhalb der Grenzen des Unternehmensnetzwerks zu ermöglichen.



Voraussetzungen

Um erfolgreich Vertrauen zwischen dem Proxyserver und der ADFS-Farm herzustellen, überprüfen Sie die folgende Konfiguration in der NetScaler-Appliance:

- Erstellen Sie ein SSL-Profil für das Backend und aktivieren Sie SNI im SSL-Profil. Deaktivieren Sie SSLv3/TLS1. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3
   DISABLED -tls1 DISABLED -commonName <FQDN of ADFS>
<!--NeedCopy-->
```

- Deaktivieren Sie SSLv3/TLS1 für den Dienst. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- SNI-Erweiterung für Back-End-Server-Handshakes aktivieren. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set vpn parameter  - backendServerSni ENABLED

set ssl parameter -denySSLReneg NONSECURE
<!--NeedCopy-->
```

> **Wichtig**
>
> Für Home Realm Discovery (HRD) -Szenarien, in denen die Authentifizierung auf den ADFS-Server verlagert werden muss, empfiehlt Citrix, sowohl die Authentifizierung als auch SSO auf der NetScaler-Appliance zu deaktivieren.

Mechanismus der Authentifizierung

Im Folgenden werden die Ereignisse auf hoher Ebene für die Authentifizierung beschrieben.

1. **Vertrauen mit dem ADFS-Server herstellen** — Der NetScaler-Server richtet Vertrauen zum ADFS-Server ein, indem er ein Clientzertifikat registriert. Sobald der Trust eingerichtet ist, stellt die NetScaler-Appliance das Vertrauen nach dem Neustart ohne Benutzereingriff wieder her.

   Nach Ablauf des Zertifikats müssen Sie die Vertrauensstellung erneut herstellen, indem Sie das ADFS-Proxy-Profil entfernen und erneut hinzufügen.

2. **Veröffentlichte Endpoints** — Die NetScaler-Appliance ruft nach der Vertrauensstellung automatisch die Liste der veröffentlichten Endpunkte auf dem ADFS-Server ab. Diese veröf-

fentlichten Endpunkte filtern die Anforderungen, die an den ADFS-Server weitergeleitet wurden.

3. **Einfügen von Headern in Clientanforderungen** - Wenn die NetScaler-Appliance Clientanforderungen tunnelt, werden die mit ADFSPIP verbundenen HTTP-Header dem Paket hinzugefügt, während sie an den ADFS-Server gesendet werden. Sie können die Zugriffssteuerung auf dem ADFS-Server basierend auf diesen Header-Werten implementieren. Die folgenden Header werden unterstützt.

   - X-MS-Proxy
   - X-MS-Endpoint-Absolute-Pfad
   - X-MS-weitergeleitete Client-IP
   - X-MS-Proxy
   - X-MS-Target-Rolle
   - X-MS-ADFS-Proxy-Client-IP

4. **Verwalten des Datenverkehrs** von Endbenutzern — Der Datenverkehr der Endbenutzer wird sicher an die gewünschten Ressourcen weitergeleitet.

   > **Hinweise:**
   >
   > - NetScaler verwendet eine formularbasierte Authentifizierung.
   > - NetScaler unterstützt nicht die Veröffentlichung einer Anwendung, die die Einhaltung des Active Directory Federation Service Proxy Integration Protocol verwendet.

Konfigurieren Sie NetScaler für die Unterstützung des ADFS-Servers

Voraussetzungen

- Konfigurieren Sie den Context Switching (CS) -Server als Front-End mit Authentifizierungs-, Autorisierungs- und Überwachungsserver hinter CS. Geben Sie in der Befehlszeile Folgendes ein:

```
add cs vserver <cs vserver name> SSL 10.220.xxx.xx 443
-cltTimeout 180 -AuthenticationHost <adfs server hostname> -
   Authentication OFF -persistenceType NONE
<!--NeedCopy-->
```

```
add cs action <action name1> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```

```
add cs action <action name2> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```



```
add cs policy <policy name1> -rule " http.req.url.contains("/adfs
   /services/trust") || http.req.url.contains("federationmetadata
   /2007-06/federationmetadata.xml")" -action <action name1>
<!--NeedCopy-->
```

```
add cs policy <policy name2> -rule "HTTP.REQ.URL.CONTAINS("/adfs/
   ls")" -action <action name2>
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -policyName <policy name1> -
   priority 100
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -policyName <policy name2> -
   priority 110
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -lbvserver <lb vserver name>
<!--NeedCopy-->
```

- Fügen Sie einen ADFS-Dienst hinzu. Geben Sie in der Befehlszeile Folgendes ein:

```
add service <adfs service name> <adfs server ip> SSL 443
<!--NeedCopy-->
```

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- Fügen Sie einen virtuellen Server mit Lastausgleich hinzu. Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <lb vserver name> SSL 0.0.0.0 0
<!--NeedCopy-->
```

```
set ssl vserver <lb vserver name> -sslProfile
   ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

- Binden Sie den Dienst an den Server mit Lastausgleich. Geben Sie in der Befehlszeile Folgendes ein:


```
1  bind lb vserver <lb vserver name> <adfs service name>
2  <!--NeedCopy-->
```

Um NetScaler für die Arbeit mit dem ADFS-Server zu konfigurieren, müssen Sie Folgendes tun:

1. Erstellen eines SSL-CertKey-Profilschlüssels zur Verwendung mit dem ADFS-Proxy-Profil
2. Erstellen eines ADFS-Proxyprofils
3. Ordnen Sie das ADFS-Proxyprofil dem virtuellen LB-Server zu

Erstellen Sie ein SSL-Zertifikat mit privatem Schlüssel zur Verwendung mit dem ADFS-Proxy-Profil

Geben Sie in der Befehlszeile Folgendes ein:

```
1     add ssl certkey <certkeyname>  -cert <certificate path> -key <
         keypath>
2  <!--NeedCopy-->
```

Hinweis: Die Zertifikatsdatei und die Schlüsseldatei müssen in der NetScaler-Appliance vorhanden sein.
Erstellen eines ADFS-Proxyprofils mit CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1  add authentication adfsProxyProfile  <profile name> -serverUrl <https:
      //<server FQDN or IP address>/> -username <adfs admin user name> -
      password <password for admin user> -certKeyName <name of the CertKey
       profile created above>
2  <!--NeedCopy-->
```

Wo;

Profilname — Name des zu erstellenden AFDS-Proxy-Profils

ServerUrl — Vollqualifizierter Domainname des ADFS-Dienstes einschließlich Protokoll und Port. Beispiel: `https://adfs.citrix.com`

`Username` — Benutzername eines Admin-Kontos, das auf dem ADFS-Server existiert

Kennwort — Kennwort des Admin-Kontos, das als Benutzername verwendet wird

certKeyName — Name des zuvor erstellten SSL certKey-Profils

Ordnen Sie das ADFS-Proxyprofil über die CLI dem virtuellen Lastausgleichsserver zu

In der ADFS-Bereitstellung werden zwei virtuelle Lastausgleichsserver verwendet, einer für den Clientdatenverkehr und der andere für den Metadatenaustausch. Das ADFS-Proxyprofil muss mit dem virtuellen Lastausgleichsserver verknüpft sein, der den ADFS-Server mit Front-End beendet.

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <adfs-proxy-lb> -adfsProxyProfile <name of the ADFS
   proxy profile>
<!--NeedCopy-->
```

Unterstützung der Erneuerung des Vertrauens für ADFSPIP

Sie können das Vertrauen der vorhandenen Zertifikate erneuern, die kurz vor dem Ablauf stehen oder wenn das vorhandene Zertifikat nicht gültig ist. Die Vertrauenserneuerung von Zertifikaten erfolgt nur, wenn die Vertrauensstellung zwischen der NetScaler-Appliance und dem ADFS-Server hergestellt wird. Um die Vertrauensstellung des Zertifikats zu erneuern, müssen Sie das neue Zertifikat bereitstellen.

> **Wichtig**
>
> Für die Erneuerung neuer Zertifikate ist ein manuelles Eingreifen erforderlich.

Im folgenden Beispiel werden die Schritte zur Erneuerung des Zertifikatsvertrauens aufgeführt:

1. Die NetScaler-Appliance sendet sowohl alte (SerializedTrustCertificate) als auch neue (SerializedReplacementCertificate) Zertifikate in POST-Anforderung an den ADFS-Server zur Erneuerung des Vertrauens.
2. Der ADFS-Server reagiert mit 200 OK erfolgreich, wenn das Vertrauen erfolgreich erneuert wurde.
3. Die NetScaler-Appliance aktualisiert den Status “ESTABLISHED_RENEW_SUCCESS”, wenn die Erneuerung des Vertrauens erfolgreich ist. Wenn die Erneuerung des Vertrauens fehlschlägt, wird der Status als “ESTABLISHED_RENEW_FAILED” aktualisiert und die NetScaler-Appliance verwendet weiterhin das alte Zertifikat.

> **Hinweis**
>
> Sie können den Cert-Schlüssel nicht aktualisieren, wenn er bereits an ein ADFS-Proxy-Profil gebunden ist.

So konfigurieren Sie die Vertrauenserneuerung von Zertifikaten über die CLI

Geben Sie in der Befehlszeile Folgendes ein:


```
set authentication adfsProxyProfile <name> [-CertKeyName <string>]
<!--NeedCopy-->
```

Beispiel:

```
set authentication adfsProxyProfile adfs_2  -CertKeyName ca_cert1
<!--NeedCopy-->
```

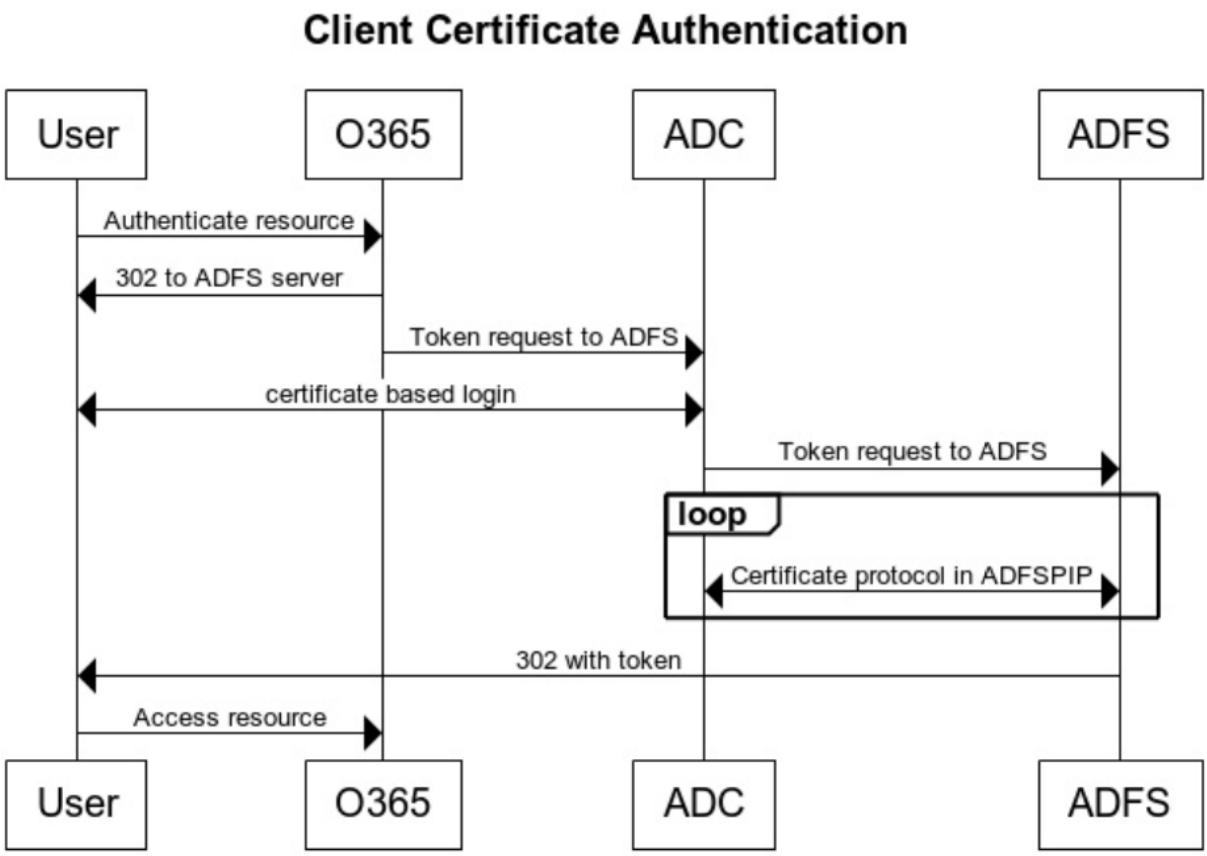
Clientzertifikatbasierte Authentifizierung auf dem ADFS-Server

Ab Windows Server 2016 führte Microsoft eine neue Methode zur Authentifizierung von Benutzern ein, wenn über Proxyserver auf ADFS zugegriffen wird. Endbenutzer können sich jetzt mit ihren Zertifikaten anmelden und vermeiden so die Verwendung eines Kennworts.

Endbenutzer greifen häufig über einen Proxy auf ADFS zu, insbesondere wenn sie sich nicht in den Räumlichkeiten befinden. Daher müssen ADFS-Proxyserver die Clientzertifikatauthentifizierung über das ADFSPIP-Protokoll unterstützen.

Wenn ADFS mit einer NetScaler-Appliance Lastenausgleich durchgeführt wird, müssen sich Benutzer zur Unterstützung der zertifikatbasierten Authentifizierung auf dem ADFS-Server ebenfalls mit dem Zertifikat bei der NetScaler-Appliance anmelden. Auf diese Weise kann NetScaler das Benutzerzertifikat an ADFS übergeben, um SSO für den ADFS-Server bereitzustellen.

Das folgende Diagramm zeigt den Ablauf der Clientzertifikatauthentifizierung.



Konfigurieren von SSO für den ADFS-Server mithilfe des Clientzertifikats

Um SSO für den ADFS-Server mithilfe des Clientzertifikats zu konfigurieren, müssen Sie zuerst die Clientzertifikatauthentifizierung auf der NetScaler-Appliance konfigurieren. Anschließend müssen Sie die Richtlinie zur Zertifikatsauthentifizierung an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver binden.

Darüber hinaus müssen Sie die folgenden Schritte ausführen.

- Ein zusätzlicher virtueller Kontextswitching-Server mit Port 49443 muss konfiguriert werden, und dieser virtuelle Kontextswitching-Server muss auf denselben virtuellen Lastausgleichsserver zeigen, der für alle Ports geöffnet ist, die Sie zuvor erstellt haben.
- Der Port 49443 muss zur Authentifizierung auf der NetScaler-Appliance geöffnet werden.
- Die Kontextswitching-Richtlinie muss an denselben virtuellen Lastausgleichsserver mit geöffnetem Port 443 gebunden sein, den Sie zuvor erstellt haben.
- Sie müssen denselben SSL-Dienst, den Sie zuvor erstellt haben, an den virtuellen Lastausgleichsserver binden.
- Wenn Sie bereits ein SSL-Profil für das Backend erstellt haben, müssen Sie dieses Profil verwenden.

Geben Sie in der Befehlszeile ein;

```
add cs vserver <name> <serviceType> <port>

bind cs vserver <name> (-lbvserver <string> | -vServer <string> | [-targetLBVserver <string>]

set ssl vserver <vServerName [-sslProfile <string>]

bind ssl vserver <vServerName -certkeyName <string>

add authentication certAction <action name>

add authentication Policy <policy name> -rule <expression> -action <action name>

add authentication policylable <label Name>

bind authentication policylabel <label Name> -policyName <name of the policy> -priority<integer>

<!--NeedCopy-->
```

Beispiel:

```
add cs vserver srv123_adfsproxy_csvs_tls SSL $VIP_1 49443

bind cs vserver srv123_adfsproxy_csvs_tls -lbvserver srv123_adfs_lbvserver

set ssl vserver srv123_adfsproxy_csvs_tls -sslProfile ns_default_ssl_profile_frontend

bind ssl vserver srv123_adfsproxy_csvs_tls -certkeyName srv123_wildcardcert

add authentication certAction adfsproxy-cert

add authentication Policy cert1 -rule TRUE -action adfsproxy-cert

add authentication policylable certfactor

bind authentication policylabel certfactor -policyName cert1 -priority 100

```



```
<!--NeedCopy-->
```

Informationen zum Konfigurieren des Clientzertifikats auf der NetScaler-Appliance finden Sie unter Konfigurieren der Clientzertifikatauthentifizierung mithilfe erweiterter Richtlinien.

Verwenden Sie ein lokales NetScaler Gateway als Identitätsanbieter für Citrix Cloud

August 15, 2023

Citrix Cloud unterstützt die Verwendung eines on-premises NetScaler Gateway als Identitätsanbieter für die Authentifizierung von Abonnenten, wenn diese sich bei ihrem Workspace anmelden.

Mithilfe der NetScaler Gateway-Authentifizierung können Sie:

- Fortdauernde Authentifizierung von Benutzern über das vorhandene NetScaler Gateway, damit sie über Citrix Workspace auf die Ressourcen in der On-Premises-Bereitstellung von Virtual Apps and Desktops zugreifen können.
- Verwenden Sie die NetScaler Gateway-Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen mit Citrix Workspace.
- Bieten Sie Ihren Benutzern Zugriff auf die Ressourcen, die sie über Citrix Workspace benötigen, indem Sie Funktionen wie Pass-Through-Authentifizierung, Smartcards, sichere Token, Richtlinien für bedingten Zugriff und Verbund verwenden.

Die Authentifizierung mit NetScaler Gateway wird für folgende Produktversionen unterstützt:

- NetScaler Gateway 13.0 41.20 Advanced Edition oder höher
- NetScaler Gateway 12.1 54.13 Advanced Edition oder höher

Voraussetzungen

- Cloud Connectors - Sie benötigen mindestens zwei Server, auf denen Sie die Citrix Cloud Connector-Software installieren können.
- Active Directory - Führen Sie die erforderlichen Prüfungen durch.
- Anforderungen für NetScaler Gateway
  - Verwenden Sie erweiterte Richtlinien auf dem on-premises Gateway aufgrund der Veraltung klassischer Richtlinien.
  - Bei der Konfiguration des Gateway für die Authentifizierung von Abonnenten von Citrix Workspace fungiert das Gateway als OpenID Connect-Anbieter. Nachrichten zwischen Citrix Cloud und Gateway entsprechen dem OIDC-Protokoll, was auch die digitale Signatur

von Token umfasst. Daher müssen Sie ein Zertifikat zur Signatur dieser Token konfigurieren.

- Taktsynchronisation - Das Gateway muss mit der NTP-Zeit synchronisiert sein.

Details finden Sie unter Voraussetzungen.

Erstellen einer OAuth IdP-Richtlinie auf dem lokalen NetScaler Gateway

> **Wichtig:**
>
> Sie müssen die Client-ID, die geheime und die Umleitungs-URL auf der Registerkarte **Citrix Cloud > Identitäts- und Zugriffsmanagement > Authentifizierung** generiert haben. Weitere Informationen finden Sie unter Verbinden eines on-premises NetScaler Gateway mit Citrix Cloud.

Das Erstellen einer OAuth IdP-Authentifizierungsrichtlinie umfasst die folgenden Aufgaben:

1. Erstellen eines OAuth-IdP-Profils
2. Fügen Sie eine OAuth IdP-Richtlinie hinzu.
3. Binden Sie die OAuth IdP-Richtlinie an einen virtuellen Authentifizierungsserver.
4. Binden Sie das Zertifikat global.

Erstellen eines OAuth IdP-Profils mit der CLI

Geben Sie in der Befehlszeile ein;

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]

add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=aaa,
    dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
    ldapLoginName sAMAccountName

add authentication policy <name> -rule <expression> -action <string>

bind authentication vserver auth_vs -policy <ldap_policy_name> -
    priority <integer> -gotoPriorityExpression NEXT

```

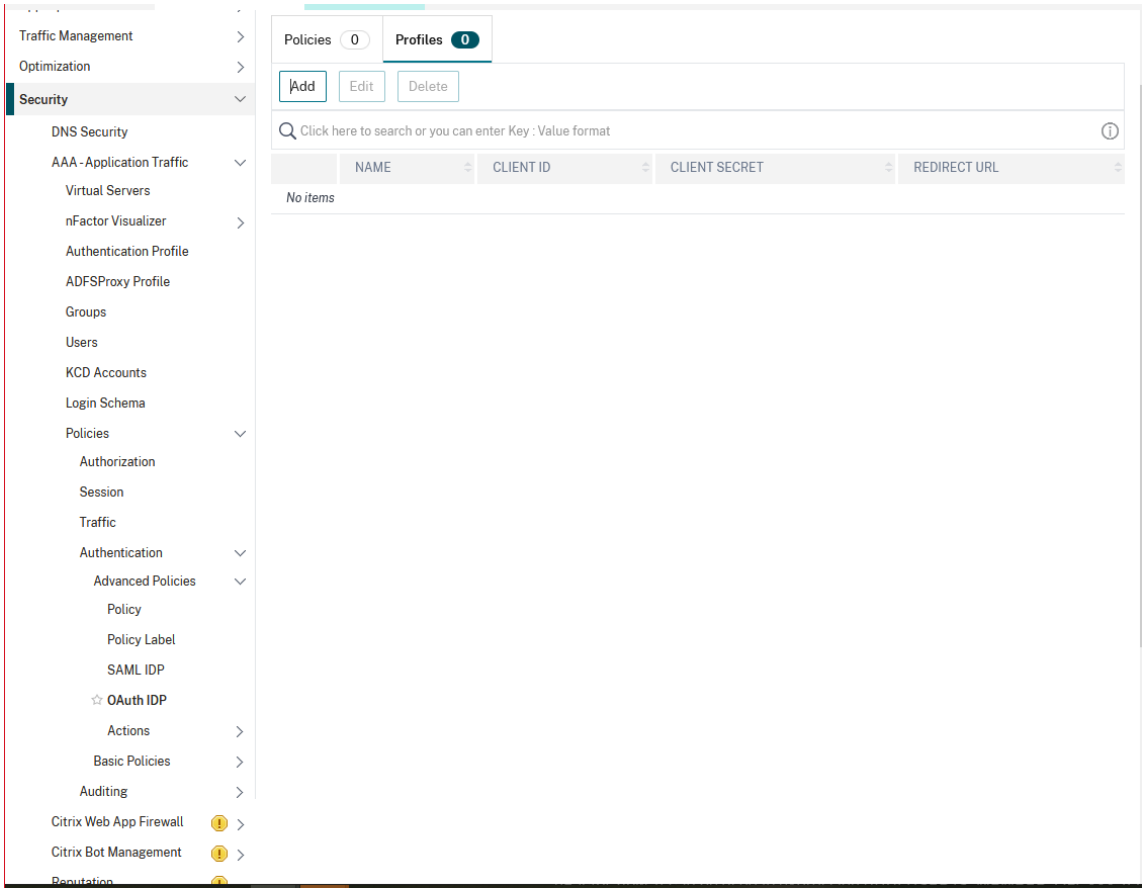


```
bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -
    priority <integer> -gotoPriorityExpression END

bind vpn global -certkeyName <>
<!--NeedCopy-->
```

Erstellen eines OAuth IdP-Profils mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > OAuth IDP**.



2. Wählen Sie auf der **OAuth IDP-Seite** die Registerkarte **Profile** aus und klicken Sie auf **Hinzufügen**.
3. Konfigurieren Sie das OAuth IdP-Profil.

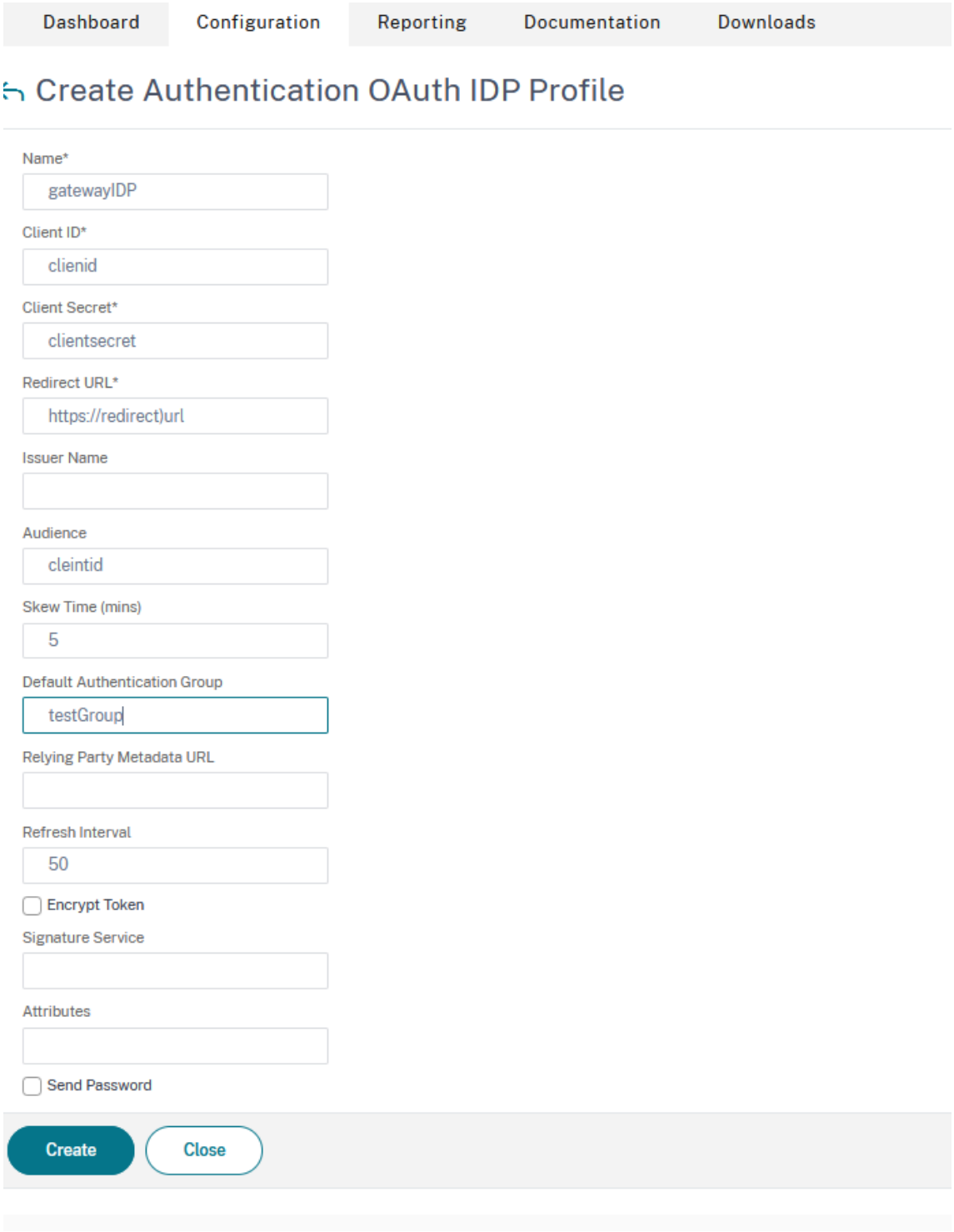
> **Hinweis:**
>
> - Kopieren Sie die Werte für Client-ID, Secret und Redirect URL aus der Registerkarte **Citrix Cloud > Identitäts- und Zugriffsmanagement > Authentifizierung** und fügen Sie sie ein, um die Verbindung zu Citrix Cloud herzustellen.

- Geben Sie die Gateway-URL im Beispiel für den **Ausstellernamen** korrekt ein: https://GatewayFQDN.com
- Kopieren Sie auch die Client-ID und fügen Sie sie auch in das Feld **Zielgruppe** ein.
- **Kennwort senden**: Aktivieren Sie diese Option für Single-Sign-On-Unterstützung. Standardmäßig ist diese Option deaktiviert.

4. Legen Sie im Bildschirm **Authentifizierung erstellen OAuth IDP-Profil** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.

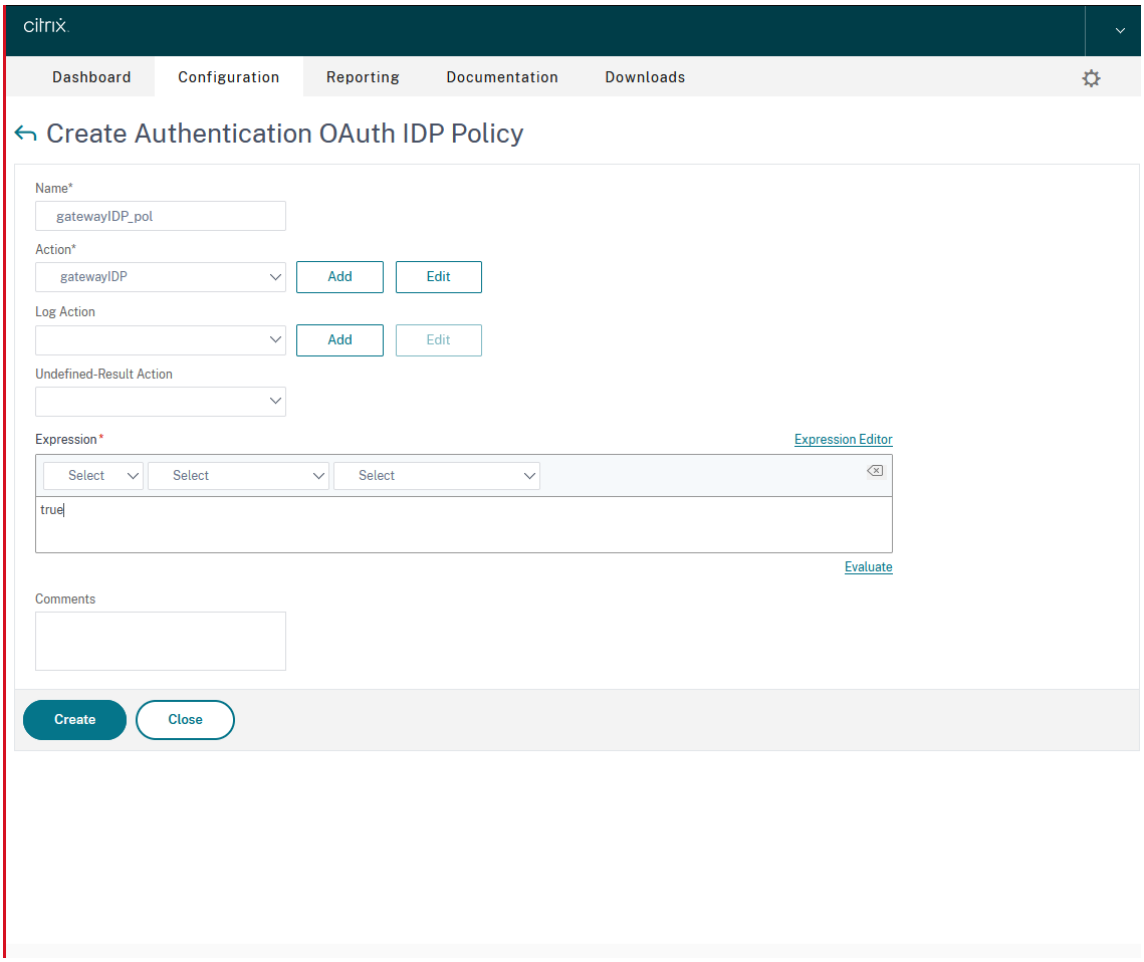
   - **Name** — Name des Authentifizierungsprofils. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen. Der Name darf nur Buchstaben, Zahlen und den Bindestrich (-), den Punkt (.) Pfund (#), das Leerzeichen (), das At (@), das Gleich (=), den Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem das Profil erstellt wurde.
   - **Client-ID** — Eindeutige Zeichenfolge, die SP identifiziert. Der Autorisierungsserver leitet die Clientkonfiguration von dieser ID ab. Maximale Länge: 127.
   - **Client Secret:** Geheime Zeichenfolge, die vom Benutzer und Autorisierungsserver erstellt wird. Maximale Länge: 239
   - **URL umleiten** — Endpunkt für SP, an dem Code/Token gepostet werden muss.
   - **Name des Ausstellers** — Identität des Servers, dessen Token akzeptiert werden sollen. Maximale Länge: 127. Beispiel:https://GatewayFQDN.com
   - **Zielgruppe** — Zielempfänger für das vom IdP gesendete Token. Dieses Token wird vom Empfänger geprüft.
   - **Zeitversatz** — Diese Option gibt den zulässigen Zeitversatz (in Minuten) an, den NetScaler für ein eingehendes Token zulässt. Wenn skewTime beispielsweise 10 ist, wäre das Token von (aktuelle Zeit - 10) min bis (aktuelle Zeit + 10) min gültig, das sind insgesamt 20 Minuten. Standardwert: 5.
   - **Standard-Authentifizierungsgruppe** — Eine Gruppe, die der internen Gruppenliste der Sitzung hinzugefügt wurde, wenn dieses Profil von IdP ausgewählt wird, das im nFactor Flow verwendet werden kann. Es kann im Ausdruck (AAA.USER.IS_MEMBER_OF (“xxx”)) für Authentifizierungsrichtlinien verwendet werden, um den zugehörigen nFactor-Flow zu identifizieren. Maximale Länge: 63

   Der Sitzung für dieses Profil wird eine Gruppe hinzugefügt, um die Richtlinienbewertung und das Anpassen von Richtlinien zu vereinfachen. Die Gruppe ist die Standardgruppe, die zusätzlich zu extrahierten Gruppen ausgewählt wird, wenn die Authentifizierung erfolgreich ausgeführt wird. Maximale Länge: 63.



5. Klicken Sie auf **Richtlinien**, und klicken Sie auf **Hinzufügen.**
6. Legen Sie im Fenster **Richtlinie für OAuth IDP-Authentifizierung erstellen** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
   - **Name** — Der Name der Authentifizierungsrichtlinie.

- **Action:** Name des zuvor erstellten Profils.
- **Log Action:** Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anforderung mit dieser Richtlinie übereinstimmt. Keine obligatorische Einreichung.
- Aktion mit**undefiniertem Ergebnis — Aktion**, die ausgeführt werden soll, wenn das Ergebnis der Richtlinienbewertung nicht bestraft wird (UNDEF). Kein Pflichtfeld.
- **Expression:** Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Beispiel: true.
- **Comments:** Kommentare zu der Richtlinie.



> **Hinweis:**
>
> Wenn **sendPassword** auf ON (standardmäßig OFF) eingestellt ist, werden Benutzeranmeldeinformationen verschlüsselt und über einen sicheren Kanal an Citrix Cloud weitergeleitet. Wenn Sie Benutzeranmeldeinformationen über einen sicheren Kanal übergeben, können Sie SSO an Citrix Virtual Apps and Desktops nach dem Start aktivieren.

Binden der OAuthIDP-Richtlinie und der LDAP-Richtlinie an den virtuellen Authentifizierungsserver

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > LDAP**.
2. Klicken Sie im Bildschirm **LDAP-Aktionen** auf **Hinzufügen**.
3. Legen Sie im Bildschirm **Authentifizierungs-LDAP-Server erstellen** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
   - **Name —** Der Name der LDAP-Aktion
   - **Servername/ServerIP —** Bereitstellung von FQDN oder IP des LDAP-Servers
   - Wählen Sie geeignete Werte **für Sicherheitstyp, Port, Servertyp, Timeout**
   - Stellen Sie sicher, dass **Authentifizierung** aktiviert ist
   - **Basis-DN —** Basis, von der aus die LDAP-Suche gestartet werden soll. Beispiel: `dc=aaa`, `dc=local`.
   - **Administrator Bind DN:** Benutzername der Bindung an den LDAP-Server. Beispiel: `admin@aaa.local`.
   - **Administratorkennwort/Kennwort bestätigen: Kennwort zum Binden von LDAP**
   - Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen zu testen.
   - **Attribut für Server-Anmeldename:** Wählen Sie **“sAMAccountName”**
   - Andere Felder sind nicht Pflichtfelder und können daher nach Bedarf konfiguriert werden.
4. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie.**
5. Klicken Sie im Bildschirm **Authentifizierungsrichtlinien** auf **Hinzufügen**.
6. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen.**
   - **Name —** Name der LDAP-Authentifizierungsrichtlinie.
   - **Aktionstyp —** Wählen Sie **LDAP aus.**
   - **Aktion —** Wählen Sie die LDAP-Aktion aus.
   - **Ausdruck —** Standard-Syntaxausdruck, den die Richtlinie verwendet, um auf bestimmte Anforderungen zu antworten. Beispiel: true**.

Referenzwerte für Authentifizierungskontextklassen speichern

NetScaler, der als on-premises IdP konfiguriert ist, kann ACR-Werte (Authentication Context Class Reference) speichern, die von Citrix Workspace zur Unterstützung der Multidomain-Anmeldefunktion der Citrix Workspace Platform (WSP) bereitgestellt werden.

Wenn Citrix Workspace die ACR-Werte an den OAuth-Autorisierungsendpunkt des NetScaler-IdP

sendet, speichert NetScaler die ACR-Werte. Sie können diese ACR-Werte verwenden, um den nächsten Faktor im nFactor-Flow zu bestimmen.

Die Anmeldung `/oauth/idp/` am OAuth-IdP-Autorisierungsendpunkt erhält eine Abfrage mit dem ACR-Wertparameter im folgenden Format. NetScaler speichert den ACR-Wert im Benutzersitzungsattribut.

```
GET /oauth/idp/login?response_type=code&scope=openid%20profile%20ctxs_cc&
acr_values=device_id:69eec3333333333+wsp:wspmultiurlmain.cloud.com&client_id
=test&redirect_uri=https%3A%2F%2Fav6.aaa.local%2Foauth%2Flogin&state=
Y3R4PXlFYkpFdEJOeDFLN0hUY2VCc1pBOGc2RjU3d21PcjJ2aXprZkhFSkdBTzVVTzM4eEZBUW1qTEFwR25DSE
&code_challenge_method=S256&code_challenge=IJgD-qaJZdhuGt3m262BjjMXrFTOwioV6uSBA
-uIY18
```

Im obigen Beispiel lautet `acr_values=device_id:69eec3333333333+wsp:wspmultiurlmain.cloud.com`der ACR-Wertparameter.

Im Folgenden finden Sie Ausdrucksbeispiele dafür, wie Sie ACR-Werte in einem nFactor-Flow verwenden können.

- Verwenden Sie den Ausdruck `aaa.user.wsp.eq("URL")` in Ihrer Richtlinienkonfiguration, um die WSP-URL abzurufen.

  Beispiel:

  ```
  add authentication policy wsp_check -rule aaa.user.wsp.eq("wspmultiurlmain
  .cloud.com ")-action ldap-act
  ```

- Verwenden Sie den Ausdruck `aaa.user.acr_values.value("device_id").eq(value)` in Ihrer Richtlinienkonfiguration, um die Geräte-ID aus dem ACR-Wertparameter abzurufen.

  Beispiel:

  ```
  add authentication policy acr_value_check -rule aaa.user.acr_values.
  value("device_id").eq("69eec3333333333")-action ldap-act
  ```

- Verwenden Sie den Ausdruck `aaa.user.acr_values.value("wsp").eq("URL")` in Ihrer Richtlinienkonfiguration, um den WSP-Wert aus dem ACR-Wertparameter abzurufen.

  Beispiel:

  ```
  add authentication policy acr_value_check -rule aaa.user.acr_values.
  value("wsp").eq("wspmultiurlmain.cloud.com")-action ldap-act
  ```


Unterstützung für aktiv-aktive GSLB-Bereitstellungen auf NetScaler Gateway

May 11, 2023

NetScaler Gateway, das mit dem OIDC-Protokoll als Identity Provider (IdP) konfiguriert ist, kann aktiv-aktive GSLB-Bereitstellungen unterstützen.

Weitere Informationen zum Konfigurieren eines GSLB-Setups finden Sie unter Beispiel für eine GSLB-Setup und -Konfiguration.

> **Wichtig:**
>
> Active-Active GSLB mit NetScaler Gateway als OAuth IdP wird für Citrix Cloud nicht unterstützt.

GSLB Active-Active-Unterstützung für Multifaktor-Authentifizierung mithilfe des Verbindungsproxys

Ab NetScaler Release 13.1 Build 12.x wird Unterstützung für die aktive GSLB-Bereitstellung für die Multifaktor-Authentifizierung mithilfe des Verbindungsproxys hinzugefügt. Diese Unterstützung gilt für NetScaler Gateway- und NetScaler-Authentifizierungs-, Autorisierungs- und Überwachungsszenarien. Der Verbindungsproxy wird verwendet, um Anfragen an die richtigen GSLB-Sites weiterzuleiten, sobald die Authentifizierung erfolgreich war. Einzelheiten zur Persistenz des Verbindungsproxys finden Sie unter Verbindungsproxy.

Funktionsweise

Das GSLB-Site-Persistenzcookie wird in die Authentifizierungsantwort eingefügt. Mit diesem Cookie identifiziert der NetScaler oder die NetScaler Gateway-Appliance, ob die Anforderung für eine lokale Site oder eine Remote-Site gilt. Die Anfragen werden dann entsprechend weitergeleitet.

> **Wichtig:**
>
> - Es wird nur eine aktive GSLB-Bereitstellung unterstützt.
> - Eltern-Kind-Topologie wird nicht unterstützt.
> - Der Persistenztyp in der GSLB-Bereitstellung muss als “ConnectionProxy” konfiguriert sein.

Konfigurationsunterstützung für SameSite-Cookie-Attribut

May 11, 2023

Das SameSite-Attribut gibt dem Browser an, ob das Cookie für den standortübergreifenden Kontext oder nur für den Kontext derselben Website verwendet werden kann. Wenn auf eine Anwendung in einem standortübergreifenden Kontext zugegriffen werden soll, ist dies außerdem nur über die HTTPS-Verbindung möglich. Einzelheiten finden Sie unter RFC6265.

Bis Februar 2020 wurde das SameSite-Attribut in NetScaler nicht explizit festgelegt. Der Browser nahm den Standardwert (Keine). Die Nichteinstellung des SameSite-Attributs hatte keine Auswirkungen auf das NetScaler Gateway und die Authentifizierungs-, Autorisierungs- und Auditing-Bereitstellungen.

Bei bestimmten Browser-Upgrades wie Google Chrome 80 ändert sich das standardmäßige domänenübergreifende Verhalten von Cookies. Das SameSite-Attribut kann auf einen der folgenden Werte festgelegt werden. Der Standardwert für Google Chrome ist auf Lax festgelegt. Für bestimmte Versionen anderer Browser ist der Standardwert für das SameSite-Attribut möglicherweise immer noch auf None festgelegt.

- **Keine**: Zeigt an, dass der Browser ein Cookie im seitenübergreifenden Kontext nur für sichere Verbindungen verwendet.
- **Lax**: Weist an, dass der Browser ein Cookie für Anfragen auf derselben Domain und für seitenübergreifende Anfragen verwendet. Für seitenübergreifende Zwecke können nur sichere HTTP-Methoden wie GET-Request das Cookie verwenden. Beispielsweise kann eine GET-Anfrage einer Subdomain abc.example.com mithilfe eines GET-Befehls das Cookie einer anderen Subdomain xyz.example.com lesen.
  Für Cross-Site werden nur sichere HTTP-Methoden verwendet, da sichere HTTP-Methoden den Serverstatus nicht ändern. Weitere Einzelheiten finden Sie unter https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite#lax
- **Streng**: Verwenden Sie das Cookie nur im selben Site-Kontext.

Wenn das Cookie kein SameSite-Attribut enthält, übernimmt Google Chrome die Funktionalität von SameSite = Lax.
Daher gibt Google Chrome bei Bereitstellungen innerhalb eines iFrames mit seitenübergreifendem Kontext, bei denen Cookies vom Browser eingefügt werden müssen, keine seitenübergreifenden Cookies weiter. Infolgedessen wird der Iframe auf der Website möglicherweise nicht geladen.

SameSite-Cookie-Attribut konfigurieren

Ein neues Cookie-Attribut mit dem Namen SameSite wird den virtuellen VPN- und Authentifizierungs-, Autorisierungs- und Auditing-Servern hinzugefügt. Dieses Attribut kann auf globaler Ebene und auf virtueller Serverebene festgelegt werden.

Um das SameSite-Attribut zu konfigurieren, müssen Sie wie folgt vorgehen:

1. Legen Sie das SameSite-Attribut für den virtuellen Server fest
2. Cookies an den Patset binden (wenn der Browser seitenübergreifende Cookies löscht)

Festlegen des SameSite-Attributs mithilfe der CLI

Verwenden Sie die folgenden Befehle, um das SameSite-Attribut auf virtueller Serverebene festzulegen.

```
set vpn vserver VP1 -SameSite [STRICT | LAX | None]
set authentication vserver AV1 -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Verwenden Sie die folgenden Befehle, um das SameSite-Attribut auf globaler Ebene festzulegen.

```
set aaa parameter -SameSite [STRICT | LAX | None]
set vpn parameter -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Hinweis: Die Einstellung auf virtueller Serverebene nimmt den Vorzug gegenüber der Einstellung auf globaler Ebene vor. Citrix empfiehlt, das SameSite-Cookie-Attribut auf virtueller Serverebene festzulegen.

Cookies mithilfe der CLI an den Patset binden

Wenn der Browser seitenübergreifende Cookies löscht, können Sie diese Cookie-Zeichenfolge an das bestehende NS_Cookies_SameSite-Patset binden, sodass das SameSite-Attribut zum Cookie hinzugefügt wird.

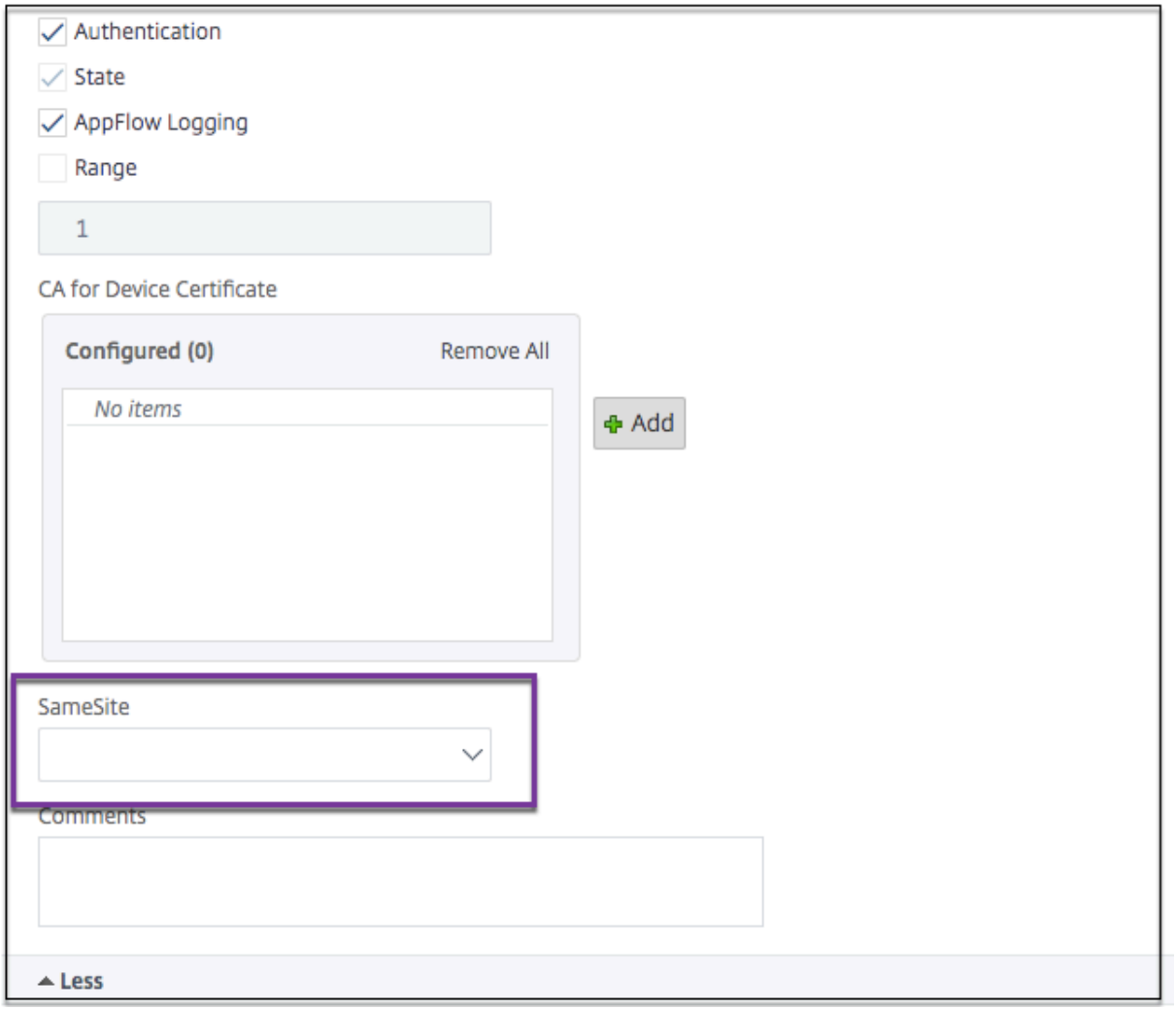
Beispiel:

```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

Festlegen des SameSite-Attributs über die GUI

Gehen Sie wie folgt vor, um das SameSite-Attribut auf virtueller Serverebene festzulegen:

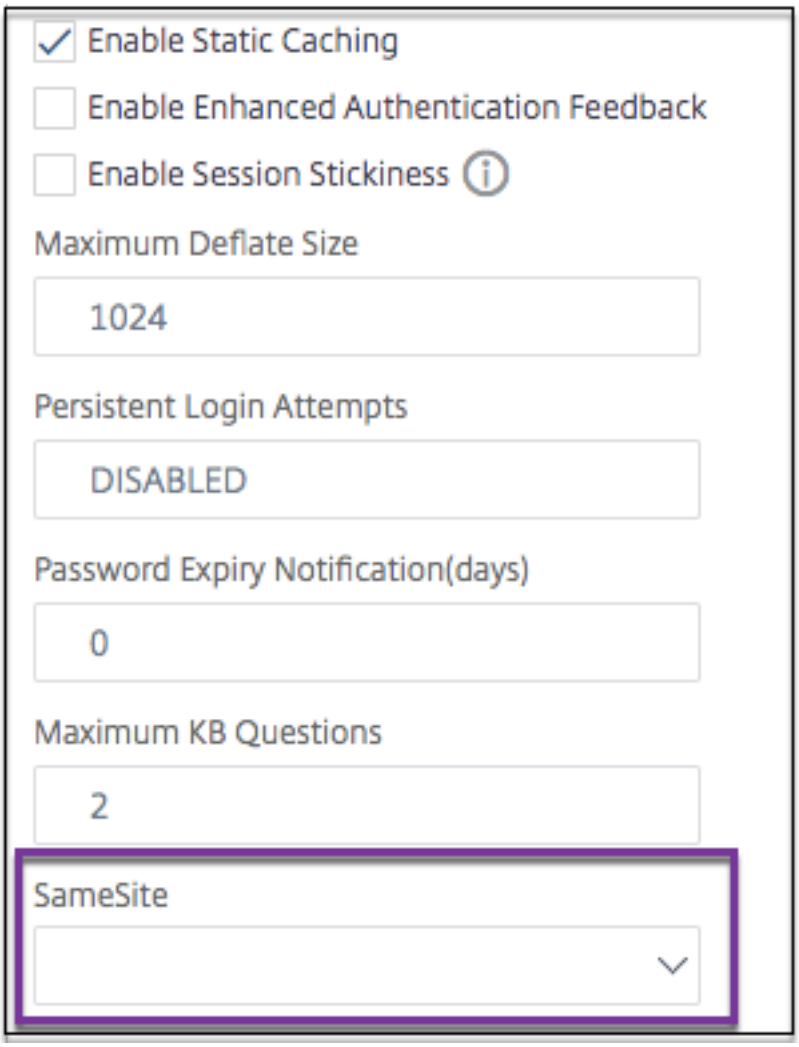
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server.**
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen**auf das Bearbeitungssymbol und dann auf **Mehr**.
4. Wählen Sie in **SameSite**die Option nach Bedarf aus.



Um das SameSite-Attribut auf globaler Ebene festzulegen:

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Authentifizierungseinstellungen ändern.**

2. Klicken Sie auf der Seite „ **AAA-Parameter konfigurieren** “ auf die **SameSite-Liste** und wählen Sie die gewünschte Option aus.



Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration für häufig verwendete Protokolle

May 11, 2023

Für die Konfiguration der NetScaler Appliance für Authentifizierung, Autorisierung und Prüfung ist ein spezielles Setup auf der NetScaler Appliance und den Browsern der Clients erforderlich. Die Konfiguration variiert je nach Protokoll, das für die Authentifizierung, Autorisierung und Überwachung verwendet wird.

Weitere Informationen zum Konfigurieren der NetScaler Appliance für die Kerberos-Authentifizierung finden Sie unter Umgang mit Authentifizierung, Autorisierung und Auditing mit Kerberos/NTLM.

Authentifizierung, Autorisierung und Audits mit Kerberos/NTLM

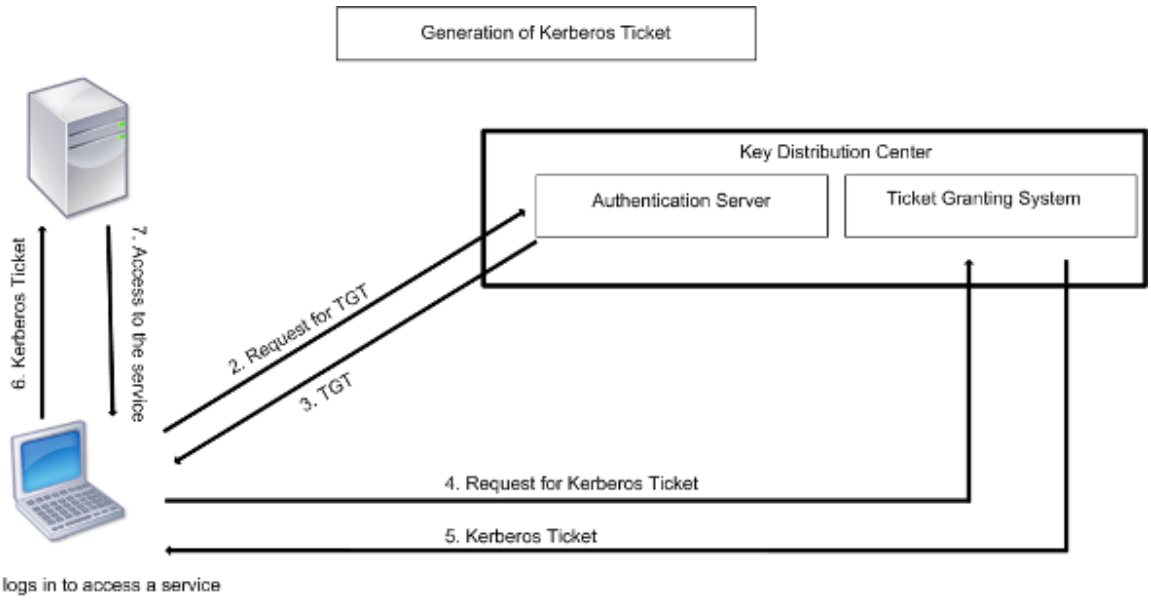
May 11, 2023

Kerberos, ein Authentifizierungsprotokoll für Computernetzwerke, bietet sichere Kommunikation über das Internet. Es wurde hauptsächlich für Client-Server-Anwendungen entwickelt und ermöglicht eine gegenseitige Authentifizierung, bei der Client und Server jeweils die Authentizität des anderen sicherstellen können. Kerberos verwendet einen vertrauenswürdigen Drittanbieter, das als Key Distribution Center (KDC) bezeichnet wird. Ein KDC besteht aus einem Authentifizierungsserver (AS), der einen Benutzer authentifiziert, und einem Ticket Granting Server (TGS).

Jede Entität im Netzwerk (Client oder Server) hat einen geheimen Schlüssel, der nur ihr selbst und dem KDC bekannt ist. Die Kenntnis dieses Schlüssels setzt die Authentizität der Entität voraus. Für die Kommunikation zwischen zwei Entitäten im Netzwerk generiert das KDC einen Sitzungsschlüssel, der als Kerberos-Ticket oder Serviceticket bezeichnet wird. Der Client fordert beim AS Anmeldeinformationen für einen bestimmten Server an. Der Kunde erhält dann ein Ticket, das als Ticket Granting Ticket (TGT) bezeichnet wird. Der Kunde kontaktiert dann das TGS und verwendet das TGT, das er von der AS erhalten hat, um seine Identität nachzuweisen, und bittet um eine Dienstleistung. Wenn der Kunde für den Service in Frage kommt, stellt das TGS dem Kunden ein Kerberos-Ticket aus. Der Client kontaktiert dann den Server, der den Dienst hostet (der als Serviceserver bezeichnet wird) und verwendet das Kerberos-Ticket, um nachzuweisen, dass er für den Empfang des Dienstes autorisiert ist. Das Kerberos-Ticket hat eine konfigurierbare Lebensdauer. Der Client authentifiziert sich nur einmal beim AS. Wenn es den physischen Server mehrmals kontaktiert, verwendet es das AS-Ticket erneut.

Die folgende Abbildung zeigt die grundlegende Funktionsweise des Kerberos-Protokolls.

Abbildung 1. **Funktionsweise von Kerberos**



Die Kerberos-Authentifizierung hat die folgenden Vorteile:

- Schnellere Authentifizierung. Wenn ein physischer Server ein Kerberos-Ticket von einem Client erhält, verfügt der Server über genügend Informationen, um den Client direkt zu authentifizieren. Für die Client-Authentifizierung muss kein Domänencontroller kontaktiert werden, weshalb der Authentifizierungsprozess schneller ist.
- Gegenseitige Authentifizierung. Wenn das KDC einem Client ein Kerberos-Ticket ausstellt und der Client das Ticket verwendet, um auf einen Dienst zuzugreifen, können nur authentifizierte Server das Kerberos-Ticket entschlüsseln. Wenn der virtuelle Server auf der NetScaler-Appliance das Kerberos-Ticket entschlüsseln kann, können Sie daraus schließen, dass sowohl der virtuelle Server als auch der Client authentifiziert sind. Somit erfolgt die Authentifizierung des Servers zusammen mit der Authentifizierung des Clients.
- Single Sign-On zwischen Windows und anderen Betriebssystemen, die Kerberos unterstützen.

Die Kerberos-Authentifizierung kann die folgenden Nachteile haben:

- Kerberos hat strenge Zeitanforderungen. Die Uhren der beteiligten Hosts müssen mit der Kerberos-Serveruhr synchronisiert werden, um sicherzustellen, dass die Authentifizierung nicht fehlschlägt. Sie können diesen Nachteil mildern, indem Sie die Network Time Protocol-Daemons verwenden, um die Host-Uhren synchron zu halten. Kerberos-Tickets haben einen Verfügbarkeitszeitraum, den Sie konfigurieren können.
- Kerberos benötigt, dass der zentrale Server kontinuierlich verfügbar ist. Wenn der Kerberos-Server ausgefallen ist, kann sich niemand anmelden. Sie können dieses Risiko minimieren, indem Sie mehrere Kerberos-Server und Fallback-Authentifizierungsmechanismen verwenden.
- Da die gesamte Authentifizierung von einem zentralen KDC gesteuert wird, kann jede Beeinträchtigung dieser Infrastruktur, z. B. der Diebstahl des Benutzerkennworts für eine lokale Workstation, es einem Angreifer ermöglichen, sich für einen beliebigen Benutzer auszugeben. Sie können dieses Risiko bis zu einem gewissen Grad mindern, indem Sie nur einen Desktop-Computer oder Laptop verwenden, dem Sie vertrauen, oder indem Sie die Vorauthentifizierung mithilfe eines Hardware-Tokens erzwingen.

Um die Kerberos-Authentifizierung verwenden zu können, müssen Sie sie auf der NetScaler-Appliance und auf jedem Client konfigurieren.

Optimierung der Kerberos-Authentifizierung bei Authentifizierung, Autorisierung und Überwachung

Die NetScaler Appliance optimiert und verbessert jetzt die Systemleistung bei der Kerberos-Authentifizierung. Der Authentifizierungs-, Autorisierungs- und Auditing-Daemon merkt sich die ausstehende Kerberos-Anfrage für denselben Benutzer, um die Belastung des Key Distribution Centers (KDC) zu vermeiden, wodurch doppelte Anforderungen vermieden werden.

Wie NetScaler Kerberos für die Clientauthentifizierung implementiert

May 11, 2023

> **Wichtig**
>
> Die Kerberos/NTLM-Authentifizierung wird nur in der NetScaler 9.3 nCore-Version oder höher unterstützt und kann nur für die Authentifizierung, Autorisierung und Überwachung virtueller Server für das Verkehrsmanagement verwendet werden.

NetScaler behandelt die an der Kerberos-Authentifizierung beteiligten Komponenten wie folgt:

Wichtiges Vertriebszentrum (KDC)

In den Versionen von Windows 2000 Server oder höheren Versionen sind der Domänencontroller und das KDC Teil des Windows Server. Wenn der Windows Server in Betrieb ist und läuft, bedeutet dies, dass der Domänencontroller und das KDC konfiguriert sind. Das KDC ist auch der Active Directory-Server.

> **Hinweis**
>
> Alle Kerberos-Interaktionen werden mit dem Windows-Kerberos-Domänencontroller validiert.

Authentifizierungsservice und Protokollverhandlung

Eine NetScaler-Appliance unterstützt die Kerberos-Authentifizierung auf den virtuellen Authentifizierungs-, Autorisierungs- und Auditing-Traffic-Management-Authentifizierungsservern. Wenn die Kerberos-Authentifizierung fehlschlägt, verwendet der NetScaler die NTLM-Authentifizierung.

Standardmäßig verwenden Windows 2000 Server und neuere Windows Server-Versionen Kerberos für die Authentifizierung, Autorisierung und Überwachung. Wenn Sie eine Authentifizierungsrichtlinie mit NEGOTIATE als Authentifizierungstyp erstellen, versucht NetScaler, das Kerberos-Protokoll für die Authentifizierung, Autorisierung und Überwachung zu verwenden. Wenn der Browser des Clients kein Kerberos-Ticket empfängt, verwendet der NetScaler die NTLM-Authentifizierung. Dieser Prozess wird als Verhandlung bezeichnet.

In einem der folgenden Fälle kann es vorkommen, dass der Client kein Kerberos-Ticket erhält:

- Kerberos wird auf dem Client nicht unterstützt.
- Kerberos ist auf dem Client nicht aktiviert.
- Der Client befindet sich in einer anderen Domäne als der des KDC.
- Das Access Directory auf dem KDC ist für den Client nicht zugänglich.

Für die Kerberos/NTLM-Authentifizierung verwendet der NetScaler nicht die Daten, die lokal auf der NetScaler-Appliance vorhanden sind.

Autorisierung

Der virtuelle Server für das Verkehrsmanagement kann ein virtueller Lastausgleichsserver oder ein virtueller Content-Switching-Server sein.

Auditing

Die NetScaler-Appliance unterstützt die Überwachung der Kerberos-Authentifizierung mit der folgenden Überwachungsprotokollierung:

- Vollständiges Prüfprotokoll der Aktivitäten der Endnutzer im Verkehrsmanagement
- SYSLOG und leistungsstarkes TCP-Logging
- Vollständiges Prüfprotokoll der Systemadministratoren
- Alle Systemereignisse
- Skriptfähiges Protokollformat

Unterstützte Umgebung

Die Kerberos-Authentifizierung benötigt keine spezielle Umgebung auf dem NetScaler. Der Client (Browser) muss die Kerberos-Authentifizierung unterstützen.

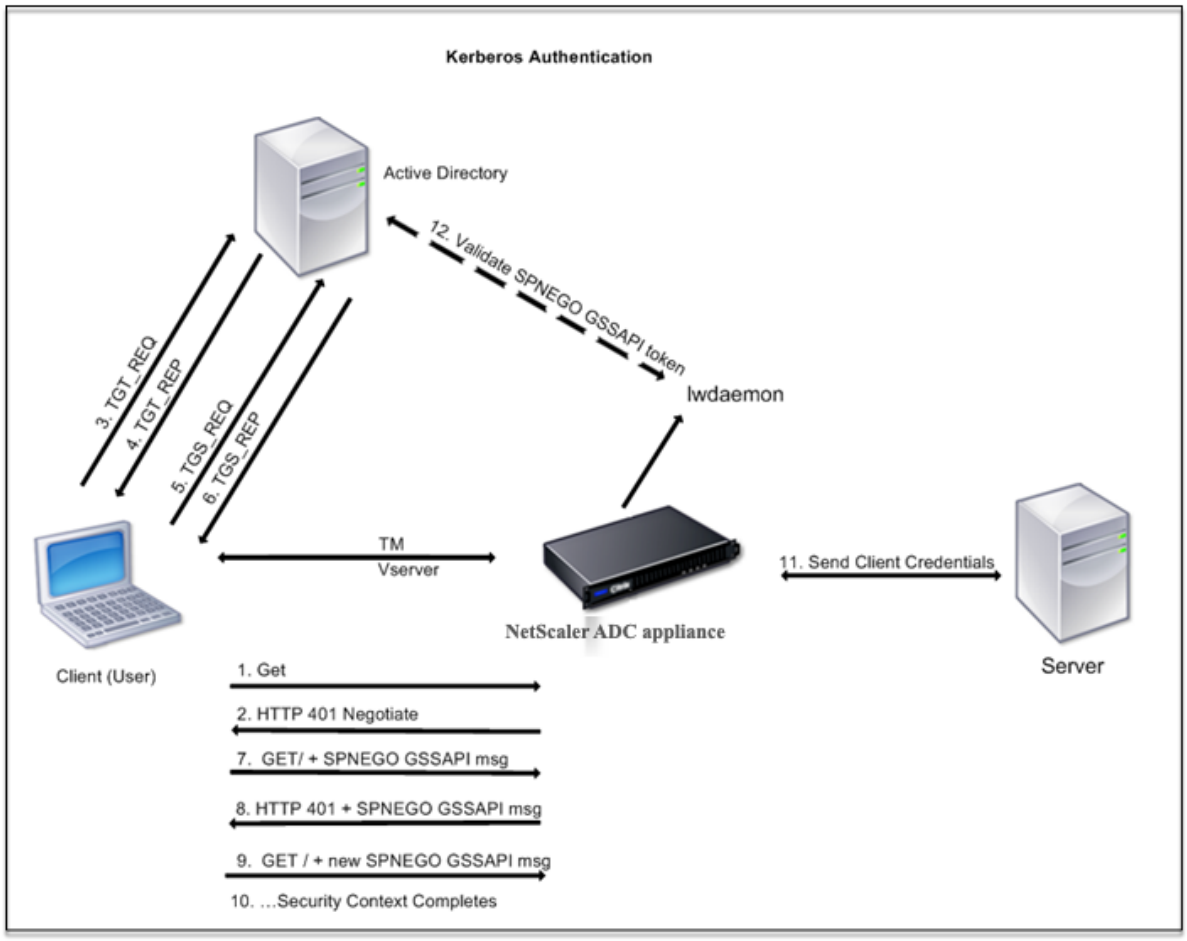
Hohe Verfügbarkeit

In einem Hochverfügbarkeits-Setup tritt nur der aktive NetScaler der Domäne bei. Im Falle eines Failovers verbindet der NetScaler lwagent-Daemon die sekundäre NetScaler-Appliance mit der Domäne. Für diese Funktion ist keine spezielle Konfiguration erforderlich.

Kerberos-Authentifizierungsprozess

Die folgende Abbildung zeigt einen typischen Prozess für die Kerberos-Authentifizierung in der NetScaler-Umgebung.

Abbildung 1. Kerberos-Authentifizierungsprozess auf NetScaler



Die Kerberos-Authentifizierung erfolgt in den folgenden Phasen:

Der Client authentifiziert sich beim KDC

1. Die NetScaler-Appliance empfängt eine Anfrage von einem Client.
2. Der virtuelle Server für das Verkehrsmanagement (Load Balancing oder Content Switching) auf der NetScaler-Appliance sendet eine Anfrage an den Client.
3. Um auf die Herausforderung zu antworten, erhält der Kunde ein Kerberos-Ticket.
   - Der Client sendet dem Authentifizierungsserver des KDC eine Anfrage für ein Ticket zur Ticketgewährung (TGT) und empfängt das TGT. (Siehe 3, 4 in der Abbildung, Kerberos-Authentifizierungsprozess.)
   - Der Client sendet das TGT an den Ticket Granting Server des KDC und erhält ein Kerberos-Ticket. (Siehe 5, 6 in der Abbildung, Kerberos-Authentifizierungsprozess.)

> **Hinweis**
>
> Der obige Authentifizierungsprozess ist nicht erforderlich, wenn der Client bereits über ein

> Kerberos-Ticket verfügt, dessen Gültigkeitsdauer noch nicht abgelaufen ist. Darüber hinaus erhalten Clients wie Web Services, .NET oder J2EE, die SPNEGO unterstützen, ein Kerberos-Ticket für den Zielserver, erstellen ein SPNEGO-Token und fügen das Token in den HTTP-Header ein, wenn sie eine HTTP-Anfrage senden. Sie durchlaufen den Client-Authentifizierungsprozess nicht.

Der Kunde fordert einen Service an.

1. Der Client sendet das Kerberos-Ticket, das das SPNEGO-Token und die HTTP-Anfrage enthält, an den virtuellen Traffic Management-Server auf dem NetScaler. Das SPNEGO-Token verfügt über die notwendigen GSSAPI-Daten.
2. Die NetScaler-Appliance stellt einen Sicherheitskontext zwischen dem Client und dem NetScaler her. Wenn der NetScaler die im Kerberos-Ticket bereitgestellten Daten nicht akzeptieren kann, wird der Client aufgefordert, ein anderes Ticket zu erhalten. Dieser Zyklus wiederholt sich, bis die GSSAPI-Daten akzeptabel sind und der Sicherheitskontext eingerichtet ist. Der virtuelle Traffic Management-Server auf dem NetScaler fungiert als HTTP-Proxy zwischen dem Client und dem physischen Server.

Die NetScaler-Appliance schließt die Authentifizierung ab.

1. Nachdem der Sicherheitskontext abgeschlossen ist, validiert der virtuelle Server für das Verkehrsmanagement das SPNEGO-Token.
2. Aus dem gültigen SPNEGO-Token extrahiert der virtuelle Server die Benutzer-ID und die GSS-Anmeldeinformationen und übergibt sie an den Authentifizierungsdaemon.
3. Eine erfolgreiche Authentifizierung schließt die Kerberos-Authentifizierung ab.

Konfigurieren der Kerberos-Authentifizierung auf der NetScaler-Appliance

May 12, 2023

In diesem Thema werden ausführliche Schritte zum Konfigurieren der Kerberos-Authentifizierung auf der NetScaler-Appliance mithilfe der CLI und der GUI beschrieben.

Konfigurieren der Kerberos-Authentifizierung auf der CLI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion, um die Authentifizierung von Datenverkehr auf der Appliance

   ns-cli-prompt **ns-funktion aktivieren** AAA

2. Fügen Sie die Keytab-Datei der NetScaler-Appliance hinzu. Eine Keytab-Datei ist erforderlich, um das während der Kerberos-Authentifizierung vom Client erhaltene Geheimnis zu entschlüsseln. Eine einzelne Keytab-Datei enthält Authentifizierungsdetails für alle Dienste, die an den virtuellen Verkehrsverwaltungsserver auf der NetScaler-Appliance gebunden sind.

   Generieren Sie zuerst die Keytab-Datei auf dem Active Directory-Server und übertragen Sie sie dann auf die NetScaler-Appliance.

   - Melden Sie sich mit dem folgenden Befehl beim Active Directory-Server an und fügen Sie einen Benutzer für die Kerberos-Authentifizierung hinzu.

     ```
     1  net user <username> <password> /add
     ```

     Hinweis

     Stellen Sie im Abschnitt **Benutzereigenschaften** sicher, dass die Option “Kennwort bei der nächsten Anmeldung ändern” nicht ausgewählt ist und die Option “Kennwort läuft nicht ab” ausgewählt ist.

   - Ordnen Sie den HTTP-Dienst dem obigen Benutzer zu und exportieren Sie die Keytab-Datei. Führen Sie beispielsweise den folgenden Befehl auf dem Active Directory-Server aus:

     ```
     1  ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM
           /pass <user password> /mapuser newacp\\dummy /ptype KRB5\
           _NT\_PRINCIPAL
     ```

     Hinweis

     Sie können mehr als einen Dienst zuordnen, wenn eine Authentifizierung für mehr als einen Dienst erforderlich ist. Wenn Sie weitere Dienste zuordnen möchten, wiederholen Sie den obigen Befehl für jeden Dienst. Sie können denselben Namen oder unterschiedliche Namen für die Ausgabedatei angeben.

   - Übertragen Sie die Keytab-Datei mit dem Unix-Befehl **ftp** oder einem anderen Dateiübertragungsprogramm Ihrer Wahl auf die NetScaler-Appliance. Laden Sie die Keytab-Datei in das Verzeichnis /nsconfig/krb/auf die NetScaler-Appliance hoch.

3. Die NetScaler-Appliance muss die IP-Adresse des Domänencontrollers aus dem vollqualifizierten Domänennamen (FQDN) beziehen. Citrix empfiehlt daher, den NetScaler mit einem DNS-Server zu konfigurieren.

   ns-cli-prompt> **add dns nameserver** <ip-address>

> **Hinweis**
>
> Alternativ können Sie statische Hosteinträge hinzufügen oder andere Mittel verwenden, damit die NetScaler-Appliance den FQDN-Namen des Domänencontrollers in eine IP-Adresse auflösen kann.

4. Konfigurieren Sie die Authentifizierungsaktion und ordnen Sie sie anschließend einer Authentifizierungsrichtlinie zu.

   - Konfigurieren Sie die Aushandlungsaktion.

     ns-cli-prompt> **add authentication negotiateAction** <name> -domain <domain name> -domainUser <domain user name> -domainUserPasswd <domain user password> -defaultAuthenticationGroup <default authentication group> -keytab <string> -NTLMPath <string>

     Hinweis: Wechseln Sie für die Konfiguration von Domänenbenutzern und Domänennamen zum Client und verwenden Sie den Befehl klist wie im folgenden Beispiel gezeigt:

     Client: username @ AAA.LOCAL

     Server: HTTP/onprem_idp.aaa.local @ AAA.LOCAL

     add authentication negotiateAction <name> -domain -domainUser <HTTP/onprem_idp.aaa.local>

   - Konfigurieren Sie die Verhandlungsrichtlinie, und ordnen Sie die Verhandlungsaktion dieser Richtlinie zu.

     ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Erstellen Sie einen virtuellen Authentifizierungsserver und verknüpfen Sie die Verhandlungsrichtlinie damit.

   - Erstellen Sie einen virtuellen Authentifizierungsserver.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>

   - Binden Sie die Aushandlungsrichtlinie an den virtuellen Authentifizierungsserver.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>

6. Verknüpfen Sie den virtuellen Authentifizierungsserver mit dem virtuellen Server der Verkehrsverwaltung (Load Balancing oder Content Switching).

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

> **Hinweis**
>
> Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen, indem Sie Folgendes tun:
   - Greifen Sie mit dem FQDN auf den virtuellen Server zur Datenverkehrsverwaltung zu. Beispiel: Sample
   - Zeigen Sie die Details der Sitzung auf der CLI an.

     ns-cli-prompt> **show aaa session**

Konfigurieren der Kerberos-Authentifizierung auf der GUI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

   Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Grundfunktionen konfigurieren** und aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

2. Fügen Sie die Keytab-Datei hinzu, wie in Schritt 2 des oben genannten CLI-Verfahrens beschrieben.

3. Fügen Sie einen DNS-Server hinzu.

   Navigieren Sie zu **Traffic Management > DNS > Nameserver**, und geben Sie die IP-Adresse für den DNS-Server an.

4. Konfigurieren Sie die Aktion und Richtlinie **Aushandeln** .

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**, und erstellen Sie eine Richtlinie mit **Aushandeln** als Aktionstyp. Klicken Sie auf **HINZUFÜGEN**, um einen neuen Authentifizierungsverhandlungsserver zu erstellen, oder klicken Sie auf **Bearbeiten**, um die vorhandenen Details zu konfigur

5. Binden Sie die Aushandlungsrichtlinie an den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**, und verknüpfen **Sie die Aushandlungsrichtlinie** mit dem virtuellen Authentifizierungsserver.

6. Verknüpfen Sie den virtuellen Authentifizierungsserver mit dem virtuellen Server der Verkehrsverwaltung (Load Balancing oder Content Switching).

   Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und geben Sie die entsprechenden Authentifizierungseinstellungen an.

   > **Hinweis**
   >
   > Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen wie in Schritt 7 der oben genannten CLI-Prozedur beschrieben.

Kerberos-Authentifizierung auf einem Client konfigurieren

May 11, 2023

Die Kerberos-Unterstützung muss im Browser konfiguriert sein, um Kerberos für die Authentifizierung verwenden zu können. Sie können jeden Kerberos-kompatiblen Browser verwenden. Es folgen Anweisungen zur Konfiguration der Kerberos-Unterstützung in Internet Explorer und Mozilla Firefox. Informationen zu anderen Browsern finden Sie in der Dokumentation des Browsers.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Tools** die Option **Internetoptionen**aus.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Lokales Intranet**und dann auf **Websites.**
3. Vergewissern Sie sich, dass im Dialogfeld **Lokales Intranet** die Option Intranet-Netzwerk automatisch erkennen ausgewählt ist, und klicken Sie dann auf **Erweitert.**
4. Fügen Sie im Dialogfeld **Lokales Intranet** die Websites der Domänen des virtuellen Traffic-Management-Servers auf der NetScaler-Appliance hinzu. Die angegebenen Sites werden zu lokalen Intranetsites.
5. Klicken Sie auf **Schließen** oder **OK**, um die Dialogfelder zu schließen.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Vergewissern Sie sich, dass Kerberos auf Ihrem Computer ordnungsgemäß konfiguriert ist.
2. Geben Sie about:config in die URL-Leiste ein.
3. Geben Sie in das Textfeld Filter network.negotiate ein.
4. Ändern Sie network.negotiate-auth.delegation-uris in die Domain, die Sie hinzufügen möchten.
5. Ändern Sie network.negotiate-auth.trusted-uris in die Domain, die Sie hinzufügen möchten.

> **Hinweis:** Wenn Sie Windows verwenden, müssen Sie auch sspi in das Filtertextfeld eingeben und die Option network.auth.use-sspi in False ändern.

Offload der Kerberos-Authentifizierung von physischen Servern

June 2, 2023

Die NetScaler-Appliance kann Authentifizierungsaufgaben von Servern ausladen. Anstatt dass die physischen Server die Anforderungen von Clients authentifizieren, authentifiziert der NetScaler alle Clientanforderungen, bevor er sie an einen der an ihn gebundenen physischen Server weiterleitet. Die Benutzerauthentifizierung basiert auf Active Directory-Token.

Es gibt keine Authentifizierung zwischen dem NetScaler und dem physischen Server, und der Authentifizierungs-Offload ist für die Endbenutzer transparent. Nach der ersten Anmeldung an einem Windows-Computer muss der Endbenutzer keine zusätzlichen Authentifizierungsinformationen in ein Popup oder auf einer Anmeldeseite eingeben.

In der aktuellen Version der NetScaler-Appliance ist die Kerberos-Authentifizierung nur für die Authentifizierung, Autorisierung und Überwachung virtueller Traffic-Management-Server verfügbar. Die Kerberos-Authentifizierung wird für SSL VPN in der NetScaler Gateway Advanced Edition-Appliance oder für die NetScaler-Appliance-Verwaltung nicht unterstützt.

Die Kerberos-Authentifizierung erfordert eine Konfiguration auf der NetScaler-Appliance und in Client-Browsern.

So konfigurieren Sie die Kerberos-Authentifizierung auf der NetScaler-Appliance

> **Hinweis**
>
> Die in der folgenden Beispielkonfiguration verwendeten Kennwörter sind nur Beispiele und nicht die tatsächlichen Konfigurationskennwörter.

1. Erstellen Sie ein Benutzerkonto in Active Directory. Überprüfen Sie beim Erstellen eines Benutzerkontos die folgenden Optionen im Abschnitt Benutzereigenschaften:
   - Stellen Sie sicher, dass Sie die Option Kennwort bei der nächsten Anmeldung ändern nicht auswählen.
   - Achten Sie darauf, die Option Kennwort läuft nicht ab zu wählen.
2. Geben Sie auf dem AD-Server an der CLI-Eingabeaufforderung Folgendes ein:
   - ktpass -princ HTTP/kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass Citrix1 -out C:\kerbtabfile.txt

   > **Hinweis**
   >
   > Geben Sie den obigen Befehl unbedingt in einer einzigen Zeile ein. Die Ausgabe des obigen Befehls wird in die Datei C:\kerbtabfile.txt geschrieben.
3. Laden Sie die Datei kerbtabfile.txt mithilfe eines Secure Copy (SCP) -Clients in das Verzeichnis /etc der NetScaler-Appliance hoch.
4. Führen Sie den folgenden Befehl aus, um der NetScaler-Appliance einen DNS-Server hinzuzufügen.
   - add dns nameserver 1.2.3.4

   Die NetScaler-Appliance kann Kerberos-Anfragen ohne den DNS-Server nicht verarbeiten. Verwenden Sie unbedingt denselben DNS-Server, der in der Microsoft Windows-Domäne verwendet wird.

5. Wechseln Sie zur Befehlszeilenschnittstelle von NetScaler.
6. Führen Sie den folgenden Befehl aus, um einen Kerberos-Authentifizierungsserver zu erstellen:
   - Authentifizierung hinzufügen Aktion aushandeln KerberosServer - Domäne “crete.lab.net” -Domänenbenutzer kerbuser -DomainUserPasswd Citrix1 -keytab /var/mykcd.keytab

   > **Hinweis**
   >
   > Wenn keytab nicht verfügbar ist, können Sie die Parameter angeben: domain, domainUser und -DomainUserPasswd.

7. Führen Sie den folgenden Befehl aus, um eine Verhandlungsrichtlinie zu erstellen:
   - `add authentication negotiatePolicy Kerberos-Policy "REQ.IP.DESTIP == 192.168.17.200"KerberosServer<!--NeedCopy-->`
8. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu erstellen.
   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`
9. Führen Sie den folgenden Befehl aus, um die Kerberos-Richtlinie an den virtuellen Authentifizierungsserver zu binden:
   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`
10. Führen Sie den folgenden Befehl aus, um ein SSL-Zertifikat an den virtuellen Authentifizierungsserver zu binden. Sie können eines der Testzertifikate verwenden, das Sie über die GUI NetScaler-Appliance installieren können. Führen Sie den folgenden Befehl aus, um das ServerTestCert-Beispielzertifikat zu verwenden.
    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`
11. Erstellen Sie einen virtuellen HTTP-Lastausgleichsserver mit der IP-Adresse 192.168.17.200.

    Stellen Sie sicher, dass Sie über die Befehlszeilenschnittstelle für NetScaler 9.3-Versionen einen virtuellen Server erstellen, wenn diese älter als 9.3.47.8 sind.
12. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu konfigurieren:
    - `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy-->`
13. Geben Sie den Hostnamen Example in die Adressleiste des Webbrowsers ein.

    Der Webbrowser zeigt ein Authentifizierungsdialogfeld an, da die Kerberos-Authentifizierung nicht im Browser eingerichtet ist.

> **Hinweis**
>
> Die Kerberos-Authentifizierung erfordert eine bestimmte Konfiguration auf dem Client. Stellen Sie sicher, dass der Client den Hostnamen auflösen kann, was dazu führt, dass der Webbrowser eine Verbindung zu einem virtuellen HTTP-Server herstellt.

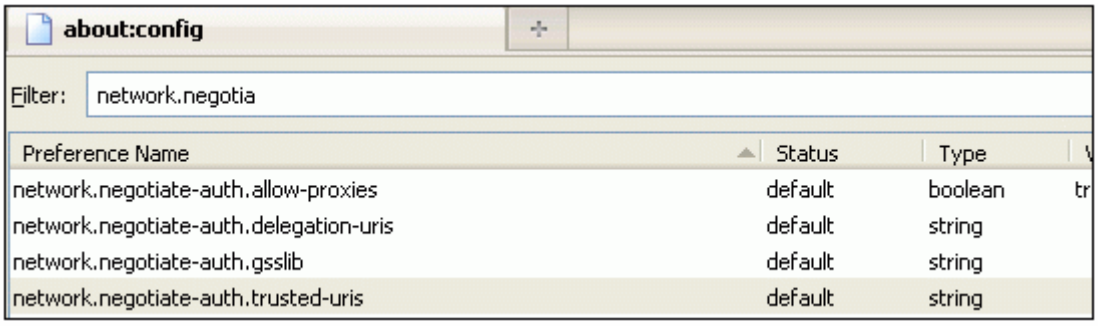
14. Konfigurieren Sie Kerberos im Webbrowser des Clientcomputers.
    - Informationen zur Konfiguration in Internet Explorer finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
    - Informationen zur Konfiguration in Mozilla Firefox finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
15. Überprüfen Sie, ob Sie ohne Authentifizierung auf den physischen Backend-Server zugreifen können.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Extras** die Option **Internetoptionen**.
2. Aktivieren Sie die Registerkarte **Sicherheit**.
3. Wählen Sie **Lokales Intranet** aus dem Abschnitt Wählen Sie eine Zone aus, um die Änderung der Sicherheitseinstellungen anzuzeigen.
4. Klicken Sie auf **Sites**.
5. Klicken Sie auf **Erweitert**.
6. Geben Sie die URL an, Beispiel, und klicken Sie auf **Hinzufügen**.
7. Starten Sie **Internet Explorer**neu.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Geben Sie about:config in die Adressleiste des Browsers ein.
2. Klicken Sie auf den Haftungsausschluss für Warnungen.
3. Geben Sie **network.negotiate-auth.trusted-uris** in das Feld **Filter** ein.
4. Doppelklicken Sie auf **Network.negotiate-auth.Trusted-URIS.** Ein Beispielbildschirm wird unten gezeigt.



5. Geben Sie im Dialogfeld Zeichenfolgenwert eingeben www.crete.lab.net an.
6. Starten Sie Firefox neu.

Behebung von Authentifizierungs- und Autorisierungsproblemen

May 11, 2023

Lokalisieren von Fehlermeldungen

Lokalisieren Sie Fehlermeldungen, die vom NetScaler nFactor-System generiert wurden

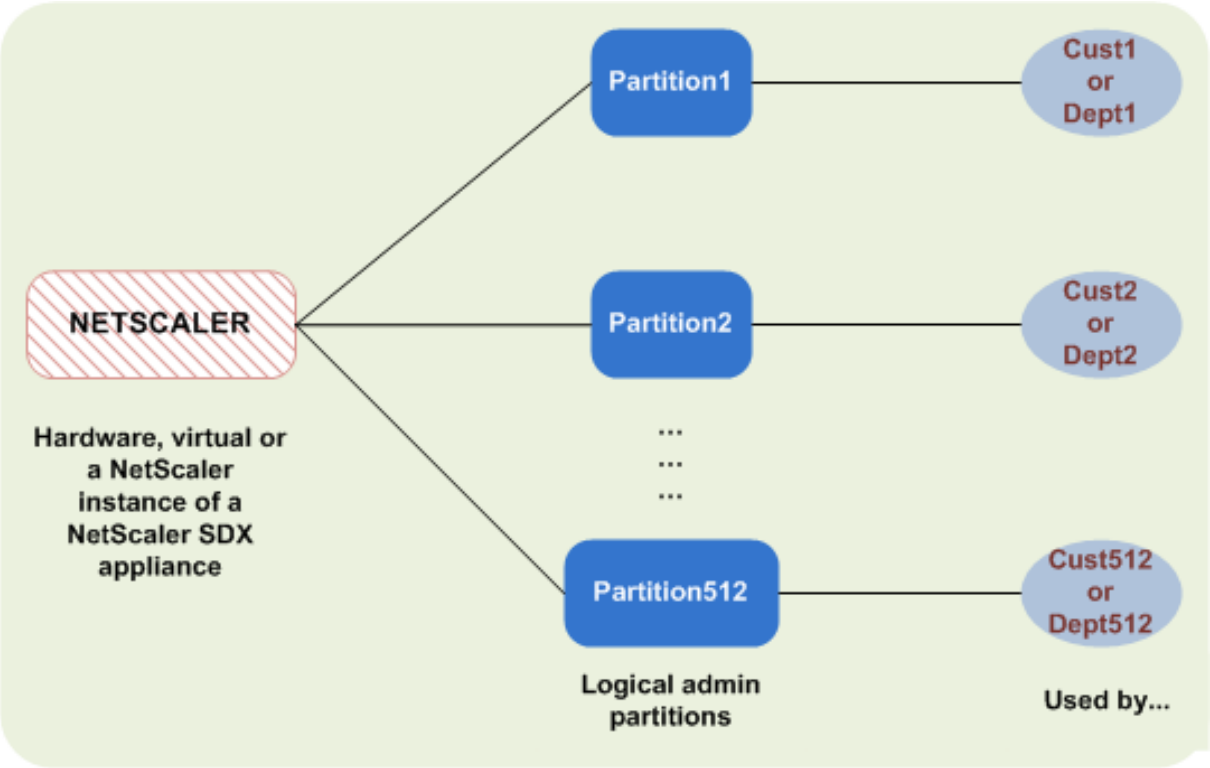
Beheben Sie Authentifizierungsprobleme mit dem Modul aaad.debug

Beheben von Authentifizierungsproblemen in NetScaler und NetScaler Gateway mit dem Modul aaad.debug

Administrator-Partition

May 11, 2023

Eine NetScaler-Appliance kann in logische Entitys partitioniert werden, die als Admin-Partitionen bezeichnet werden Jede Partition kann konfiguriert und als separate NetScaler-Appliance verwendet werden. Die folgende Abbildung zeigt die Partitionen eines NetScaler, die von verschiedenen Kunden und Abteilungen verwendet werden:



Eine partitionierte NetScaler-Appliance verfügt über eine einzelne Standardpartition und eine oder mehrere Admin-Partitionen. Die folgende Tabelle enthält weitere Details zu den beiden Partitionstypen:

> **Hinweis**
>
> In einer partitionierten Appliance kann der Modus BridgeGPDUs nur in der Standardpartition und nicht in den Administratorpartitionen aktiviert werden.

Verfügbarkeit:

Die NetScaler-Appliance wird mit einer einzigen Partition ausgeliefert, die als Standardpartition bezeichnet wird. Die Standardpartition wird auch nach der Partitionierung der NetScaler-Appliance beibehalten.

Muss explizit erstellt werden, wie unter Admin-Partitionen konfigurierenbeschrieben.

Anzahl der Partitionen:

Eins

Eine NetScaler-Appliance kann eine oder mehrere (maximal 512) Admin-Partitionen haben.

Benutzerzugriff und Rollen:

Alle NetScaler-Benutzer, die nicht mit einer *partitionsspezifischen* Befehlsrichtlinie verknüpft sind, können auf die Standardpartition zugreifen und diese konfigurieren. Wie immer schränkt die zugehörige Befehlsrichtlinie die Vorgänge ein, die ein Benutzer ausführen kann.

Der Benutzerzugriff und die Rollen werden von NetScaler Superusers erstellt, die auch die Benutzer für diese Partition angeben. Nur Superuser und zugehörige Benutzer der Partition können auf die Admin-Partition zugreifen und diese konfigurieren.

> **Hinweis**
>
> Partitionsbenutzer haben keinen Shell-Zugriff.

Datei-Struktur:

Alle Dateien in einer Standardpartition werden in der standardmäßigen NetScaler-Dateistruktur gespeichert.

Das Verzeichnis */nsconfig* speichert beispielsweise die NetScaler-Konfigurationsdatei und das Verzeichnis */var/log/* speichert die NetScaler-Protokolle.

Alle Dateien in einer Admin-Partition werden in Verzeichnispfaden gespeichert, die den Namen der Admin-Partition haben.

Beispielsweise wird die NetScaler-Konfigurationsdatei (ns.conf) im `/nsconfig/partitions/<partitionName>` Verzeichnis gespeichert. Andere partitionsspezifische Dateien werden in den `/var/partitions/<partitionName>` Verzeichnissen gespeichert.

Einige andere Pfade in einer Admin-Partition:

- Heruntergeladene Dateien: `/var/partitions/<partitionName>/download/`
- Log-Dateien: `/var/partitions/<partitionName>/log/`

> **Hinweis**
>
> Derzeit wird die Protokollierung auf Partitionsebene nicht unterstützt. Daher ist dieses Verzeichnis leer und alle Protokolle werden im `/var/log/` Verzeichnis gespeichert.

- Dateien im Zusammenhang mit dem SSL-CRL-Zertifikat: `/var/partitions/<partitionName>/netscaler/ssl`

Verfügbare Ressourcen:

Alle NetScaler-Ressourcen.

NetScaler-Ressourcen, die explizit der Admin-Partition zugewiesen sind.

Benutzerzugriff und Rollen

Bei der Authentifizierung und Autorisierung einer partitionierten NetScaler-Appliance kann ein Root-Administrator einer oder mehreren Partitionen einen Partitionsadministrator zuweisen. Der Partitionsadministrator kann Benutzer für diese Partition autorisieren, ohne andere Partitionen zu beeinträchtigen. Die Partitionsbenutzer sind berechtigt, nur über die SNIP-Adresse auf diese Partition zuzugreifen. Sowohl der Root-Administrator als auch der Partitionsadministrator können

den rollenbasierten Zugriff (RBA konfigurieren, indem Benutzer für den Zugriff auf verschiedene Anwendungen autorisiert werden.

Administratoren und Benutzerrollen können wie folgt beschrieben werden:

Root-Administrator. Greift über ihre NSIP-Adresse auf die partitionierte Appliance zu und kann dem Benutzer Zugriff auf eine oder mehrere Partitionen gewähren. Der Administrator kann auch Partitionsadministratoren einer oder mehreren Partitionen zuweisen. Der Administrator kann einen Partitionsadministrator von der Standardpartition mithilfe einer NSIP-Adresse erstellen oder zu einer Partition wechseln und dann einen Benutzer erstellen und einen Partitionsadministratorzugriff mit einer SNIP-Adresse zuweisen.

Partitions-Administrator. Greift über eine vom Root-Administrator zugewiesene NSIP-Adresse auf die angegebene Partition zu. Der Administrator kann rollenbasierten Zugriff auf den Partitionsbenutzerzugriff auf diese Partition zuweisen und auch die externe Serverauthentifizierung mithilfe einer partitionsspezifischen Konfiguration konfigurieren.

Systembenutzer. Greift über die NSIP-Adresse auf Partitionen zu. Hat Zugriff auf die vom Root-Administrator angegebenen Partitionen und Ressourcen.

Benutzer partitionieren. Greift über eine SNIP-Adresse auf eine Partition zu. Das Benutzerkonto wird vom Partitionsadministrator erstellt und der Benutzer hat Zugriff auf Ressourcen, nur innerhalb der Partition.

Wichtige Punkte

Im Folgenden sind einige Punkte aufgeführt, die Sie beim Bereitstellen eines rollenbasierten Zugriffs in einer Partition beachten sollten.

1. NetScaler-Benutzer, die über die NSIP-Adresse auf die GUI zugreifen, verwenden die Standard-Partitionsauthentifizierungskonfiguration, um sich bei der Appliance anzumelden.
2. Benutzer von Partitionssystemen, die über eine Partitions-SNIP-Adresse auf die GUI zugreifen, verwenden eine partitionsspezifische Authentifizierungskonfiguration, um sich bei der Appliance anzumelden.
3. Der in einer Partition erstellte Partitionsbenutzer kann sich nicht mit der NSIP-Adresse anmelden.
4. Der an eine Partition gebundene NetScaler-Benutzer kann sich nicht mit der SNIP-Adresse der Partition anmelden.
5. Systembenutzer, die sich über einen externen Authentifizierungsserver authentifizieren (z. B. LDAP, RADIUS, TACACS), müssen über eine SNIP-Adresse auf eine Partition zugreifen.

Anwendungsfall für die Verwaltung des rollenbasierten Zugriffs in einem partitionierten Setup

Betrachten Sie ein Szenario, in dem eine Unternehmensorganisation www.example.com mehrere Geschäftseinheiten und einen zentralisierten Administrator hat, der alle Instanzen in ihrem Netzwerk verwaltet. Sie möchten jedoch exklusive Benutzerberechtigungen und -umgebungen für jede Geschäftseinheit bereitstellen.

Im Folgenden finden Sie die Administratoren und Benutzer, die von der Standardkonfiguration für die Partitionsauthentifizierung und partitionenspezifische Konfiguration in einer partitionierten Appliance verwaltet

John: Root-Administrator

George: Partitionsadministrator

Adam: Systembenutzer

Jane: Partitions-Benutzer

John, ist der Root-Administrator einer partitionierten NetScaler-Appliance. John verwaltet alle Benutzerkonten und Administratorbenutzerkonten über Partitionen (z. B. P1, P2, P3, P4 und P5) innerhalb der Appliance. John bietet granularen rollenbasierten Zugriff auf Entitäten von der Standardpartition der Appliance. John erstellt Benutzerkonten und weist jedem Konto Partitionszugriff zu. George, der ein Netzwerkingenieur innerhalb der Organisation ist, bevorzugt einen rollenbasierten Zugriff auf wenige Anwendungen, die auf der Partition P2 ausgeführt werden. Basierend auf der Benutzerverwaltung erstellt John eine Partitionsadministratorrolle für George und verknüpft sein Benutzerkonto mit einer Partition-Admin-Befehlsrichtlinie in der P2-Partition. Adam ist ein weiterer Netzwerkingenieur, zieht es vor, auf eine Anwendung zuzugreifen, die auf P2 ausgeführt wird. John erstellt ein Systembenutzerkonto für Adam und verknüpft sein Benutzerkonto einer P2-Partition. Sobald das Konto erstellt wurde, kann sich Adam bei der Appliance anmelden, um über die NSIP-Adresse auf die NetScaler-Verwaltungsschnittstelle zuzugreifen, und kann basierend auf der Benutzer-/Gruppenbindung zur Partition P2 wechseln.

Angenommen, Jane, die eine andere Netzwerkingenieurin ist, möchte direkt auf eine Anwendung zugreifen, die nur auf der Partition P2 ausgeführt wird, George (Partitionsadministrator) kann ein Partitionsbenutzerkonto für sie erstellen und ihr Konto mit Befehlsrichtlinien für Autorisierungsberechtigungen verknüpfen. Janes Benutzerkonto, das in der Partition erstellt wurde, ist jetzt direkt mit P2 verknüpft. Jetzt kann Jane über die SNIP-Adresse auf die NetScaler-Verwaltungsschnittstelle zugreifen und kann nicht zu einer anderen Partition wechseln.

> **Hinweis**
>
> Wenn Janes Benutzerkonto von einem Partitionsadministrator in der Partition P2 erstellt wird, kann der Administrator nur über die SNIP-Adresse (die innerhalb der Partition erstellt wurde)

> auf die NetScaler-Verwaltungsschnittstelle zugreifen. Dem Administrator ist es nicht gestattet, über die NSIP-Adresse auf die Schnittstelle zuzugreifen. Ebenso, wenn Adams Benutzerkonto von einem Root-Administrator in der Standardpartition erstellt und an eine P2-Partition gebunden ist. Der Administrator kann auf die NetScaler-Verwaltungsschnittstelle nur über die NSIP-Adresse oder SNIP-Adresse zugreifen, die in der Standardpartition erstellt wurde (mit aktiviertem Verwaltungszugriff). Und es ist nicht gestattet, über die in der Administratorpartition erstellte SNIP-Adresse auf die Partitionsoberfläche zuzugreifen.

Konfigurieren von Rollen und Zuständigkeiten für Partitionsadministratoren

Im Folgenden finden Sie die Konfigurationen, die von einem Root-Administrator in einer Standardpartition durchgeführt werden.

Erstellen von Administratorpartitionen und Systembenutzern — Ein Root-Administrator erstellt Administratorpartitionen und Systembenutzer in der Standardpartition der Appliance. Der Administrator verknüpft die Benutzer dann verschiedenen Partitionen. Wenn Sie an eine oder mehrere Partitionen gebunden sind, können Sie basierend auf Benutzerbindungen von einer Partition zur anderen wechseln. Außerdem wird Ihr Zugriff auf eine oder mehrere gebundene Partitionen nur vom Root-Administrator autorisiert.

Autorisieren des Systembenutzers als Partitionsadministrator für eine bestimmte Partition — Sobald ein Benutzerkonto erstellt wurde, wechselt der Root-Administrator zu einer bestimmten Partition und autorisiert den Benutzer als Partitionsadministrator. Dies geschieht durch Zuweisen der Partition-Admin-Befehlsrichtlinie dem Benutzerkonto. Jetzt kann der Benutzer als Partitionsadministrator auf die Partition zugreifen und Entitäten innerhalb der Partition verwalten.

Im Folgenden finden Sie die Konfigurationen, die von einem Partitionsadministrator in einer administrativen Partition durchgeführt werden.

Konfigurieren der SNIP-Adresse in einer Administratorpartition- Der Partitionsadministrator meldet sich bei der Partition an und erstellt eine SNIP-Adresse und bietet Verwaltungszugriff auf die Adresse.

Erstellen und Binden eines Partitionssystembenutzers mit Partitionsbefehlsrichtlinie - Der Partitionsadministrator erstellt Partitionsbenutzer und definiert den Umfang des Benutzerzugriffs. Dies geschieht durch Binden des Benutzerkontos an Partitionsbefehlsrichtlinien.

Erstellen und Binden einer Partitionssystem-Benutzergruppen mit Partitionsbefehlsrichtlinie -Der Partitionsadministrator erstellt Partitionsbenutzergruppen und definiert den Umfang des Zugriffs auf Benutzergruppen. Dies geschieht durch Binden des Benutzergruppenkontos an Partitionsbefehlsrichtlinien.

Konfigurieren der externen Serverauthentifizierung für externe Benutzer (optional) -Diese Konfiguration dient zur Authentifizierung externer TACACS-Benutzer, die mit der SNIP-Adresse auf die Partition zugreifen.

Im Folgenden werden die Aufgaben aufgeführt, die beim Konfigurieren des rollenbasierten Zugriffs für Partitionsbenutzer in einer Administratorpartition ausgeführt werden

1. Erstellen einer administrativen Partition — Bevor Sie Partitionsbenutzer in einer Administratorpartition erstellen, müssen Sie zuerst die Partition erstellen. Als Root-Administrator können Sie mit dem Konfigurationsdienstprogramm oder einer Befehlszeilenschnittstelle eine Partition von der Standardpartition erstellen.
2. Benutzerzugriff von der Standardpartition auf Partition P2 wechseln - Wenn Sie Partitionsadministrator von der Standardpartition aus auf die Appliance zugreifen, können Sie von der Standardpartition zu einer bestimmten Partition wechseln. Partitionieren Sie beispielsweise P2 basierend auf Benutzerbindung.
3. Hinzufügen einer SNIP-Adresse zum Partitions-Benutzerkonto mit aktiviertem Verwaltungszugriff - nachdem Sie Ihren Zugriff auf eine Administrationspartition umgestellt haben. Sie erstellen eine SNIP-Adresse und gewähren Verwaltungszugriff auf die Adresse.
4. Erstellen und Binden eines Partitionssystembenutzers mit Partitionsbefehlsrichtlinie - Wenn Sie ein Partitionsadministrator sind, können Sie Partitionsbenutzer erstellen und den Umfang des Benutzerzugriffs definieren. Dies geschieht durch Binden des Benutzerkontos an Partitionsbefehlsrichtlinien.
5. Erstellen und Binden von Partitionsbenutzergruppen mit Partitionsbefehlsrichtlinie - Wenn Sie ein Partitionsadministrator sind, können Sie Partitionsbenutzergruppen erstellen und den Umfang der Benutzerzugriffssteuerung definieren. Dies geschieht durch Binden des Benutzergruppenkontos an Partitionsbefehlsrichtlinien.

Konfigurieren der externen Serverauthentifizierung für externe Benutzer (optional) -Diese Konfiguration dient zur Authentifizierung externer TACACS-Benutzer, die mit einer SNIP-Adresse auf die Partition zugreifen.

Vorteile der Verwendung von Admin-Partitionen

Sie können die folgenden Vorteile nutzen, indem Sie Admin-Partitionen für Ihre Bereitstellung verwenden:

- Ermöglicht die Delegierung des Verwaltungseigentums an eine Anwendung an den Kunden.
- Reduziert die Kosten des ADC-Eigentums, ohne Kompromisse bei Leistung und Benutzerfreundlichkeit einzugehen.
- Schützt vor ungerechtfertigten Konfigurationsänderungen. In einer nicht partitionierten NetScaler-Appliance können autorisierte Benutzer der anderen Anwendung absichtlich oder unbeabsichtigt Konfigurationen ändern, die für Ihre Anwendung erforderlich sind. Es kann zu unerwünschtem Verhalten führen. Diese Möglichkeit ist in einer partitionierten NetScaler-Appliance reduziert.
- Isoliert den Datenverkehr zwischen verschiedenen Anwendungen durch Verwendung dedizierter VLANs für jede Partition.

- Beschleunigt und ermöglicht die Skalierung von Anwendungsbereitstellungen.
- Ermöglicht die Verwaltung und Berichterstellung auf Anwendungsebene oder lokalisiert.

Lassen Sie uns einige Fälle analysieren, um die Szenarien zu verstehen, in denen Sie Admin-Partitionen verwenden können.

Anwendungsfall 1: Wie Admin-Partition in einem Unternehmensnetzwerk verwendet wird

Betrachten wir ein Szenario, dem ein Unternehmen namens **Foo.com**gegenübersteht.

- **Foo.com** hat einen einzigen NetScaler.
- Es gibt fünf Abteilungen und jede Abteilung hat eine Anwendung, die mit dem NetScaler bereitgestellt werden muss.
- Jede Anwendung muss unabhängig von einer anderen Gruppe von Benutzern oder Administratoren verwaltet werden.
- Andere Benutzer müssen vom Zugriff auf die Konfigurationen ausgeschlossen werden.
- Die Anwendung oder das Back-End muss Ressourcen wie IP-Adressen teilen können.
- Die globale IT-Abteilung muss in der Lage sein, Einstellungen auf NetScaler-Ebene zu steuern, die allen Partitionen gemeinsam sein müssen.
- Die Anwendungen müssen unabhängig voneinander sein. Ein Fehler bei der Konfiguration einer Anwendung darf sich nicht auf die andere auswirken.

Ein nicht partitionierter NetScaler könnte diese Anforderungen nicht erfüllen. Sie können jedoch all diese Anforderungen erfüllen, indem Sie einen NetScaler partitionieren.

Erstellen Sie einfach eine Partition für jede der Anwendungen, weisen Sie den Partitionen die erforderlichen Benutzer zu, geben Sie für jede Partition ein VLAN an und definieren Sie globale Einstellungen auf der Standardpartition.

Anwendungsfall 2: Wie eine Admin-Partition von einem Dienstanbieter verwendet wird

Betrachten wir ein Szenario, dem ein Dienstanbieter namens **BigProvider**gegenübersteht:

- BigProvider hat 5 Kunden: 3 kleine Unternehmen und 2 große Unternehmen.
- **SmallBiz**, **SmallerBiz**und **StartupBiz** benötigen nur die grundlegendste NetScaler-Funktionalität.
- **BigBiz** und **LargeBiz** sind größere Unternehmen und haben Anwendungen, die starken Verkehr anziehen. Sie möchten einige der komplexeren NetScaler-Funktionalität nutzen.

In einem nicht partitionierten Ansatz würde der NetScaler-Administrator normalerweise eine NetScaler SDX-Appliance verwenden und für jeden Kunden eine NetScaler-Instanz bereitstellen.

Die Lösung passt zu **BigBiz** und **LargeBiz**, da ihre Anwendungen die unverminderte Leistungsfähigkeit der gesamten nicht partitionierten NetScaler-Appliance benötigen. Diese Lösung ist jedoch möglicherweise nicht so kostengünstig für die Wartung von **SmallBiz**, **SmallerBiz**und **StartupBiz**.

Daher entscheidet **BigProvider** für folgende Lösung:

- Verwenden einer NetScaler SDX-Appliance zum Aufrufen dedizierter NetScaler-Instanzen für **BigBiz** und **LargeBz**.
- Verwenden eines einzelnen NetScaler, der in drei Partitionen partitioniert ist, jeweils eine für **SmallBiz**, **SmallerBiz**und **StartupBiz**.

Der NetScaler Administrator (Superuser) erstellt eine Admin-Partition für jeden dieser Kunden und gibt die Benutzer für die Partitionen an. Gibt auch die NetScaler-Ressourcen für die Partitionen an und gibt das VLAN an, das von dem Datenverkehr verwendet werden soll, der für jede der Partitionen bestimmt ist.

Unterstützung von NetScaler-Konfigurationen in der Admin-Partition

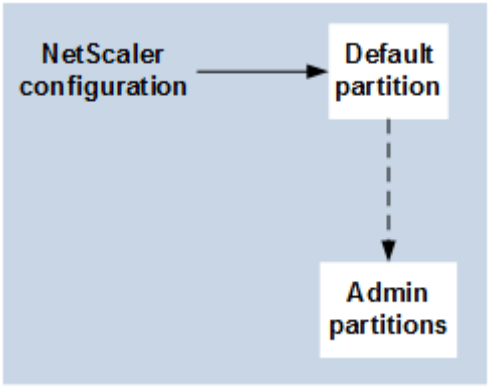
September 1, 2023

NetScaler-Konfigurationen können in die folgenden drei Arten von Konfigurationen unterteilt werden. Dies hängt von der Citrix-Konfiguration und der Partition ab, in der die Konfiguration ausgeführt wird.

> **Hinweis**
>
> - Admin-Partitionen können nicht in einem NetScaler-Cluster eingerichtet werden. Dies bedeutet, dass ein NetScaler-Cluster nicht partitioniert werden kann.
> - Admin-Partitionen können nicht auf einer NetScaler 14000 FIPS-Appliance eingerichtet werden.
> - Fall 3 listet die NetScaler-Funktionen auf, die in Admin-Partitionen nicht unterstützt werden.
> - Load Balancing-Vorlagen werden in Admin-Partitionen nicht unterstützt.

Fall 1 (globale Konfigurationen)

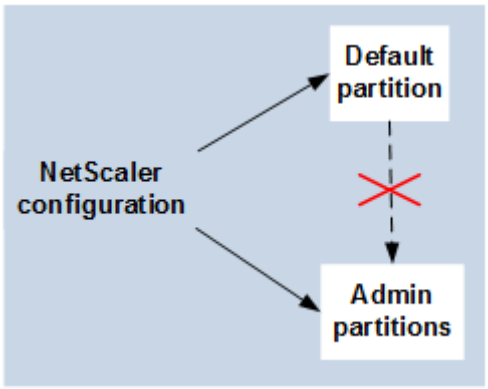
Konfigurationen, die NUR in der Standardpartition ausgeführt werden können und die verfügbar sind oder sich auf alle Admin-Partitionen auswirken.



- Aktualisierungen von integrierten Entitäten für Monitore, TCP-Profile, HTTP-Profile usw.
- Aktualisierungen globaler Parameter für Syslog, NSLOG, Weblog, Content Switching, IPSEC, SIP, DHCP, Überspannungsschutz, TCP-Pufferung und Systemerfassung.
- Hochverfügbarkeits-Konfigurationen (HA)
- Änderungen an Schnittstellen und VLAN
- Benutzerkonfigurationen

Fall 2 (partitionsspezifische Konfigurationen)

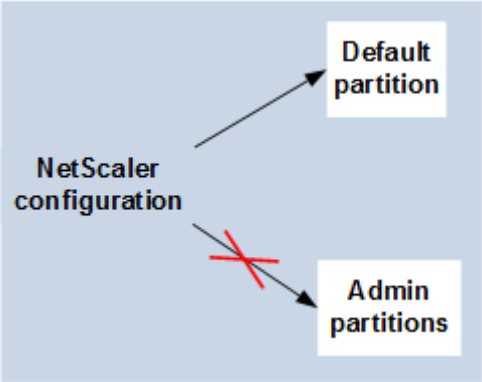
Konfigurationen, die unabhängig in Standard- und Admin-Partitionen durchgeführt werden können. Diese Konfigurationen gelten nur für die Partition, in der sie ausgeführt werden.



- Abrufen von Statistiken zum Verkehrsniveau für eine Partition.
- Der Partitionsadministrator kann IP-Bindungen für VLAN aktualisieren, das an diese Partition gebunden ist. Die Schnittstellenbindungen können jedoch nicht aktualisiert werden.
- Löschen von NetScaler-Konfigurationen.
- Funktionsspezifische Parameter für die folgenden Funktionen: AppFlow, AppQoE, HTTP-Komprimierung, DNS, TCP, HTTP, Verschlüsselung, Responder, Rewrite und SSL.
- Funktionsspezifische Konfigurationen wie virtuelle Server, Dienste, Monitore.

Fall 3

Konfigurationen, die auf Admin-Partitionen nicht durchgeführt werden können. Diese Funktionen können in der Standardpartition konfiguriert werden, haben jedoch keine Auswirkungen auf Admin-Partitionen.



> **Hinweis:**
>
> Konfigurationen, die auf Admin-Partitionen für eine bestimmte Version unterstützt werden, werden mit **Ja**gekennzeichnet.

Feature-Komponente	NetScaler-Funktion	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1	NetScaler 14.1
Netzwerke	Datenverkehr Dom	Nein (ab Build 60.13 nicht unterstützt)	Nein	Nein	Nein	Nein	Nein
Richtlinie	Erweiterbarkeit	Ja	Ja	Ja	Ja	Ja	Ja
Lastausgleich	DBS Autoscale	Ja	Ja	Ja	Ja	Ja	Ja
Lastausgleich	DNSSEC	Nein	Nein	Ja	Ja	Ja	Ja
Lastausgleich	Diameter	Ja	Ja	Ja	Ja	Ja	Ja
Lastausgleich	RTSP	Nein	Nein	Nein	Nein	Nein	Nein
Lastausgleich	Sicher Verbinden	Ja	Ja	Veraltet	Veraltet	Entfernt	Entfernt
Lastausgleich	Autoscale Servicegruppe	Ja	Ja	Ja	Ja	Ja	Ja

Feature-Komponente	NetScaler-Funktion	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1	NetScaler 14.1
Verwaltbarl	Externe RBA-Authentifizi	Ja	Ja	Ja	Ja	Ja	Ja
Verwaltbarkeit	RISE Cisco	Nein	Nein	Nein	Ja	Ja	Ja
Verwaltbarl	ACI-Cisco	Ja	Ja	Ja	Ja	Ja	Ja
Verwaltbarkeit	AppExpert	Ja	Ja	Ja	Ja	Ja	Ja
Verwaltbarl	HDX Insight	Nein	Nein	Nein	Nein	Nein	Nein
Verwaltbarkeit	Insight	Nein	Nein	Nein	Nein	Nein	Nein
VPN	Citrix Cloud-Bridge Connec-tor	Nein	Nein	Nein	Nein	Nein	Nein
VPN	NetScaler Gateway oder SSL VPN	Nein	Nein	Nein	Nein	Nein	Nein
VPN	SSL VPN ICA-Proxy	Nein	Nein	Nein	Nein	Nein	Nein
VPN	Webinterface auf NetScaler	Nein	Nein	Nein	Nein	Nein	Nein
SSL	SSL-Profil	Ja	Ja	Ja	Ja	Ja	Ja
SSL	SSL-FIPS	Nein	Nein	Nein	Nein	Nein	Nein
SSL	External-HSM	Nein	Nein	Nein	Nein	Nein	Nein
Infrarot	Cacheumleitung	Nein	Nein	Nein	Nein	Nein	Nein
Infrarot	Integriertes Caching	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerk	VXLAN	Ja	Ja	Ja	Ja	Ja	Ja

Feature-Komponente	NetScaler-Funktion	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1	NetScaler 14.1
Netzwerk	Ordnungsg Herunter-fahren	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerk	LSN	Nein	Nein	Nein	Nein	Nein	Nein
Netzwerk	IPv6 Ready Logo	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerk	vPath	Ja	Ja	Ja	Ja	Ja	Ja
Lastausglei	Datastream	Ja	Ja	Ja	Ja	Ja	Ja
Protokollierung	Webprotokollierung	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerk	L2 Param/L3 Param	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerk	GRE Tunnel	Ja	Ja	Ja	Ja	Ja	Ja
Balancing wird geladen	Skriptable-Überwachu	Ja	Ja	Ja	Ja	Ja	Ja
Lastausgleich	GSLB	Ja	Ja	Ja	Ja	Ja	Ja
Infrarot	Verbindung	Ja	Ja	Ja	Ja	Ja	Ja
Infrarot	FEO	Ja	Ja	Ja	Ja	Ja	Ja
Infrarot	Ns-Spur	Ja	Ja	Ja	Ja	Ja	Ja
Lastausgleich	Prioritätsque	Ja	Ja	Veraltet	Veraltet	Entfernt	Entfernt
Netzwerk	HDOSP	Ja	Ja	Veraltet	Veraltet	Entfernt	Entfernt
Netzwerk	Netto-Profil	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerk	Netzwerk (eingeschrä Funktion)	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerk	VRRP (eingeschränkte Funktion)	Ja	Ja	Ja	Ja	Ja	Ja

Feature-Komponente	NetScaler-Funktion	NetScaler 11.1	NetScaler 12.0	NetScaler 12.1	NetScaler 13.0	NetScaler 13.1	NetScaler 14.1
Protokollier	Audit-Protokollier (SYSLOG-TCP, LB von Syslog-Servern, SNIP-Unterstützu und FQDN-Unterstützu für Syslog)	Ja	Ja	Ja	Ja	Ja	Ja
VPN	NetScaler Gateway	Nein	Nein	Nein	Nein	Nein	Nein
VPN	AAA-TM	Ja	Ja	Ja	Ja	Ja	Ja
AppFlow	AppFlow	Nein	Ja (nur IPFIX)	Ja (nur IPFIX)	Ja	Ja	Ja
appFW	Anwendung Firewall	Nein	Nein	Nein	Nein	Nein	Nein
URL-Transformation	URL-Transformation	Nein	Nein	Nein	Nein	Nein	Nein
Lastausglei	TCP-Pufferung	Nein	Nein	Nein	Nein	Nein	Nein
Policies	OCSP-Responder	Ja	Ja	Ja	Ja	Ja	Ja
Auditprotok	SYSLOG-TCP	Nein	Ja	Ja	Ja	Ja	Ja
Optimierung	Front-End-Optimierung	Nein	Ja	Ja	Ja	Ja	Ja
AppQoE	AppQoE	Ja	Ja	Ja	Ja	Ja	Ja

In der vorherigen Tabelle sind einige der Funktionen im Setup der Admin-Partition als **eingeschränkte Funktionen** aufgeführt. Der folgende Abschnitt enthält den Grund, warum einige der Funktionen als **eingeschränkte Funktionen**bezeichnet werden.

- **VRRP**. Das VRRP ist eine eingeschränkte Funktion in der Admin-Partition aufgrund der folgenden Eigenschaften:
  - Das Hinzufügen oder Löschen von VRID kann nur über den Standardpartitionskontext erfolgen. Sobald jedoch eine VRID erstellt wurde, kann sie in nicht standardmäßigen Partitionen verwendet werden.
  - Die VRRP-Funktionalität wird nur über die dedizierten VLANs unterstützt.
  - Die VRRP-Funktionalität wird auf freigegebenen VLANs, die von der Admin-Partition verwendet werden, nicht unterstützt. Es ist intern blockiert. Während der Konfiguration wird keine Fehlermeldung angezeigt. Das Protokoll ist in einem freigegebenen VLAN (markiert oder nicht markiert) blockiert, das an eine Standard- oder eine administrative Partition gebunden ist.

> **Wichtig**
>
> Um die aktiv-aktive Bereitstellung mit VRRP zu unterstützen, müssen Haupt- und Backup-VIP dieselbe VRID verwenden. Verschiedene VRIDs können nicht verwendet werden.

- **Vernetzung**. Einige der Netzwerkkonfigurationen (L2 Param und L3 Param) werden im Partitionskontext nicht unterstützt oder gültig. Wenn Sie auf solche Konfigurationen stoßen, wird die folgende Fehlermeldung angezeigt. “FEHLER: Diese Konfigurationsoption wird auf der nicht standardmäßigen Partition nicht unterstützt. “

Konfigurieren von Administratorpartitionen

May 11, 2023

> **Wichtig**
>
> - Nur Superuser sind berechtigt, Admin-Partitionen zu erstellen und zu konfigurieren.
> - Sofern nicht anders angegeben, müssen Konfigurationen zum Einrichten einer Admin-Partition von der Standardpartition aus erfolgen.

Durch die Partitionierung einer NetScaler Appliance erstellen Sie mehrere Instanzen einer einzelnen NetScaler Appliance. Jede Instanz hat ihre eigenen Konfigurationen und der Datenverkehr jeder dieser Partitionen ist von der anderen isoliert. Dies geschieht, indem jeder Partition ein dediziertes VLAN oder ein freigegebenes VLAN zugewiesen wird.

Ein partitionierter NetScaler verfügt über eine Standardpartition und die erstellten Admin-Partitionen. Um eine Admin-Partition einzurichten, müssen Sie zuerst eine Partition mit den relevanten Ressourcen (Speicher, maximale Bandbreite und Verbindungen) erstellen. Geben Sie dann die Benutzer an, die auf die Partition zugreifen können, und die Berechtigungsstufe für jeden Benutzer auf der Partition.

Der Zugriff auf einen partitionierten NetScaler entspricht dem Zugriff auf einen nicht partitionierten NetScaler: über die NSIP-Adresse oder eine andere Verwaltungs-IP-Adresse. Nachdem Sie Ihre gültigen Anmeldeinformationen angegeben haben, werden Sie als Benutzer zu der Partition weitergeleitet, an die Sie gebunden sind. Alle von Ihnen erstellten Konfigurationen werden auf dieser Partition gespeichert. Wenn Sie mit mehr als einer Partition verknüpft sind, werden Sie zur ersten Partition weitergeleitet, mit der Sie verknüpft waren. Wenn Sie Entitäten auf einer Ihrer anderen Partitionen konfigurieren möchten, müssen Sie explizit zu dieser Partition wechseln.

Nach dem Zugriff auf die entsprechende Partition werden die von Ihnen durchführenden Konfigurationen auf dieser Partition gespeichert und sind spezifisch für diese Partition.

> **Hinweis**
>
> - NetScaler Superuser und andere Nicht-Partitionsbenutzer werden zur Standardpartition weitergeleitet.
> - Benutzer aller 512 Partitionen können sich gleichzeitig anmelden.

Tipp

Um mithilfe des SNIP (mit aktiviertem Verwaltungszugriff) über HTTPS auf eine partitionierte NetScaler-Appliance zuzugreifen, stellen Sie sicher, dass jede Partition über das Zertifikat ihres Partitionsadministrators verfügt. Innerhalb der Partition muss der Partitionsadministrator Folgendes tun:

1. Fügen Sie das Zertifikat dem NetScaler hinzu.

   ```
   add ssl certKey ns-server-certificate -cert ns-server.cert-key ns-server.key
   ```

2. Binden Sie es an einen Dienst mit dem Namen `nshttps-<SNIP>-3009`, wobei `<SNIP>` durch die SNIP-Adresse ersetzt werden muss, in diesem Fall 100.10.10.1.

   ```
   bind ssl service nshttps-100.10.10.1-3009 -certkeyName ns-server-certificate
   ```

Begrenzung der Partitionierung

In einer partitionierten NetScaler-Appliance kann ein Netzwerkadministrator eine Partition mit Partitionsressourcen wie Speicher, Bandbreite und Verbindungslimit erstellen, die als unbegrenzt konfig-

uriert sind. Dies geschieht, indem Null als Partitionsressourcenwert angegeben wird. Wobei Zero angibt, dass die Ressource auf der Partition unbegrenzt ist und bis zu Systemgrenzen verbraucht werden kann. Die Konfiguration von Partitionsressourcen ist nützlich, wenn Sie eine Datenverkehrsdomänenbereitstellung auf eine administrative Partition migrieren oder wenn Sie nichts über das Ressourcenzuweisungslimit für eine Partition in einer bestimmten Bereitstellung wissen.

Das Ressourcenlimit für eine administrative Partition ist wie folgt:

1. **Speicher partitionieren**. Es ist der maximal zugewiesene Speicher für eine Partition. Sie stellen sicher, dass Sie die Werte beim Erstellen einer Partition angeben.

   > **Hinweis**
   >
   > Ab NetScaler 12.0 können Sie beim Erstellen einer Partition das Speicherlimit auf Null setzen. Wenn bereits eine Partition mit einem bestimmten Speicherlimit erstellt wurde, können Sie das Limit auf einen beliebigen Wert reduzieren oder das Limit auf Null setzen.

   Parameter: maxMemLimit

   Maximaler Speicher wird in MB in einer Partition zugewiesen. Ein Nullwert gibt an, dass der Speicher auf der Partition unbegrenzt ist und bis zu den Systemgrenzen verbraucht werden kann.

   Standardwert: 10

2. **Partitionsbandbreite**. Maximal zugewiesene Bandbreite für eine Partition. Wenn Sie ein Limit angeben, stellen Sie sicher, dass es sich innerhalb des lizenzierten Durchsatzes der Appliance befindet. Andernfalls beschränken Sie die Bandbreite, die von der Partition verwendet wird, nicht. Der angegebene Grenzwert ist für die Bandbreite verantwortlich, die die Anwendung benötigt. Wenn die Anwendungsbandbreite das angegebene Limit überschreitet, werden Pakete gelöscht.

   > **Hinweis**
   >
   > Wenn Sie ab NetScaler 12.0 eine Partition erstellen können, können Sie das Partitionsbandbreitenlimit auf Null setzen. Wenn bereits eine Partition mit einer bestimmten Bandbreite erstellt wurde, können Sie die Bandbreite reduzieren oder das Limit auf Null setzen.

   Parameter: maxBandwidth

   Die maximale Bandbreite wird in Kbit/s in einer Partition zugewiesen. Ein Nullwert gibt an, dass die Bandbreite uneingeschränkt ist. Das heißt, die Partition kann bis zu den Systemgrenzen verbrauchen.

   Standardwert: 10240

   Maximaler Wert: 4294967295

3. **Partitions-Verbindung**. Maximale Anzahl gleichzeitiger Verbindungen, die in einer Partition geöffnet sein können. Der Wert muss den maximalen gleichzeitigen Fluss berücksichtigen, der

innerhalb der Partition erwartet wird. Die Partitionsverbindungen werden aus dem Partitionskontingentspeicher berücksichtigt. Zuvor wurden die Verbindungen aus dem Standardkontingentspeicher der Partition berücksichtigt. Es ist nur clientseitig konfiguriert, nicht für serverseitige Back-End-TCP-Verbindungen. Neue Verbindungen können nicht über diesen konfigurierten Wert hinaus hergestellt werden.

> **Hinweis**
>
> Ab NetScaler 12.0 können Sie eine Partition erstellen, bei der die Anzahl der offenen Verbindungen auf Null festgelegt ist. Wenn Sie bereits eine Partition mit einer bestimmten Anzahl offener Verbindungen erstellt haben, können Sie das Verbindungslimit reduzieren oder das Limit auf Null setzen.

Parameter: maxConnections

Maximale Anzahl gleichzeitiger Verbindungen, die in der Partition geöffnet sein können. Ein Nullwert gibt an, dass die Anzahl der offenen Verbindungen nicht begrenzt ist.

Standardwert: 1024

Mindestwert: 0

Maximaler Wert: 4294967295

Konfigurieren Sie eine Administratorpartition

Um eine Admin-Partition zu konfigurieren, führen Sie die folgenden Aufgaben aus.

So greifen Sie mit der CLI auf eine Admin-Partition zu

1. Melden Sie sich bei der NetScaler-Appliance an.
2. Prüfen Sie, ob Sie sich in der richtigen Partition befinden. In der Eingabeaufforderung wird der Name der aktuell ausgewählten Partition angezeigt.
3. Wenn ja, fahren Sie mit dem nächsten Schritt fort.
4. Wenn nein, rufen Sie eine Liste der Partitionen auf, mit denen Sie verknüpft sind, und wechseln Sie zur entsprechenden Partition.
   - `show system user <username>`
   - **`switch`** `ns partition <partitionName>`
5. Jetzt können Sie die erforderlichen Konfigurationen genauso wie ein nicht partitionierter NetScaler durchführen.

So greifen Sie mit der GUI auf eine Admin-Partition zu

1. Melden Sie sich bei der NetScaler-Appliance an.
2. Prüfen Sie, ob Sie sich in der richtigen Partition befinden. In der oberen Leiste der GUI wird der Name der aktuell ausgewählten Partition angezeigt.
   - Wenn ja, fahren Sie mit dem nächsten Schritt fort.
   - Wenn nein, navigieren Sie zu **Konfiguration > System > Partitionsverwaltung > Partitionen**, klicken Sie mit der rechten Maustaste auf die Partition, zu der Sie wechseln möchten, und wählen Sie **Wechseln**aus.
3. Jetzt können Sie die erforderlichen Konfigurationen genauso wie ein nicht partitionierter NetScaler durchführen.

Eine Admin-Partition hinzufügen

Der Root-Administrator fügt eine Administratorpartition von der Standardpartition hinzu und bindet die Partition an VLAN 2.

So erstellen Sie eine Administratorpartition mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add partition <partitionname>
```

Wechseln des Benutzerzugriffs von der Standardpartition zu einer Admin-Partition

Jetzt können Sie den Benutzerzugriff von der Standardpartition auf die Partition Par1 umstellen.

So wechseln Sie ein Benutzerkonto mit der CLI von der Standardpartition zu einer Admin-Partition:

Geben Sie in der Befehlszeile Folgendes ein:

```
Switch ns partition <pname>
```

Hinzufügen von SNIP-Adresse zu einem Partitions-Benutzerkonto mit aktiviertem Verwaltungszugriff

Erstellen Sie in der Partition eine SNIP-Adresse mit aktiviertem Verwaltungszugriff.

So fügen Sie dem Partitions-Benutzerkonto eine SNIP-Adresse hinzu, wobei der Verwaltungszugriff über die Befehlszeilenschnittstelle aktiviert ist:

Geben Sie in der Befehlszeile Folgendes ein:

```
> add ns ip <ip address> <subnet mask> -mgmtAccess enabled
```

Erstellen und Binden eines Partitionsbenutzers mit Partitionsbefehlsrichtlinie

Erstellen Sie in der Partition einen Partitionssystembenutzer und binden Sie den Benutzer mit Partition-Admin-Befehlsrichtlinien.

So erstellen und binden Sie einen Partitionssystembenutzer mit der Partitionsbefehlerrichtlinie über die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

```
> add system user <username> <password>

Done
```

Erstellen und Binden von Partitionsbenutzergruppen mit Partitionsbefehlsrichtlinie

Erstellen Sie in Partition Par1 eine Partitionssystem-Benutzergruppe und binden Sie die Gruppe mit Partitionsbefehlsrichtlinien wie Partitionsadministrator, Schreibgeschützt Partition, Partitionsoperator oder Partitionsnetzwerk.

So erstellen und binden Sie eine Partitionsbenutzergruppe mit der Befehlszeilenschnittstelle mit der Partitionsbefehlsrichtlinie:

```
1 > add system group <groupName>
2 > bind system group <groupname> (-userName | -policyName <cmdpolicy> <
    priority> | -partitionName)
```

Konfigurieren der externen Serverauthentifizierung für externe Benutzer

In der Partition Par1 können Sie eine externe Serverauthentifizierung konfigurieren, um externe TACACS-Benutzer zu authentifizieren, die über eine SNIP-Adresse auf die Partition zugreifen.

So konfigurieren Sie die externe Serverauthentifizierung für externe Benutzer mithilfe der Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

```
1 > add authentication tacacsaction <name> -serverip <IP> -tacacsSecret <
    secret key> -authorization ON -accounting ON
2 > add authentication policy <policname> -rule true -action <name>
3 > bind system global <policyname> -priority <value>1
```


Konfigurieren Sie ein Partitionssystem-Benutzerkonto in einer Partition mit der GUI

Um ein Partitionsbenutzerkonto in einer Administratorpartition zu konfigurieren, müssen Sie einen Partitionsbenutzer oder eine Partitionsbenutzergruppe erstellen und diese Partitionsbefehlsrichtlinien binden. Sie können auch die externe Serverauthentifizierung für einen externen Benutzer konfigurieren.

So erstellen Sie ein Partitionsbenutzerkonto in einer Partition mit der GUI

Navigieren Sie zu **System > Benutzerverwaltung**, klicken Sie auf **Benutzer**, um einen Benutzer des Partitionssystems hinzuzufügen, und binden Sie den Benutzer an Befehlsrichtlinien (partitionadmin/partitionread-only/partition-operator/partition-network).

So erstellen Sie ein Partitions-Benutzergruppenkonto in einer Partition über die GUI

Navigieren Sie zu **System > Benutzerverwaltung**, klicken Sie auf **Gruppen**, um eine Partitionssystem-Benutzergruppe hinzuzufügen und die Benutzergruppe an Befehlsrichtlinien (partitionadmin/partitionread-nur/Partitionoperator/Partitions-Netzwerk) zu binden.

So konfigurieren Sie die externe Serverauthentifizierung für externe Benutzer mit der GUI

Navigieren Sie zu **System > Authentifizierung > Basisaktionen** und klicken Sie auf **TACACS**, um einen TACACS-Server für die Authentifizierung externer Benutzer zu konfigurieren, die auf die Partition zugreifen.

Beispiel-Konfiguration

Die folgende Konfiguration zeigt, wie Sie einen Partitionsbenutzer oder eine Partitionsbenutzergruppe erstellen und diese Partitionsbefehlsrichtlinien binden. Außerdem, wie Sie die externe Serverauthentifizierung für die Authentifizierung eines externen Benutzers konfigurieren.

```
1 > add partition Par1
2 > switch ns partition Par1
3 > add ns ip 10.102.29.203 255.255.255.0 -mgmtAccessenabled
4 > add system user John Password
5 > bind system user Jane partition-read-only -priority 1
6 > add system group Retail
7 > bind system group Retail -policyname partition-network 1 (where 1 is
    the priority number)
8 > bind system group Retail  - username Jane
9 > add authentication tacacssaction tacuser  - serverip 10.102.29.200  -
    tacacsSecret Password  - authorization ON  - accounting ON
```



```
> add authentication policy polname -rule true -action tacacsAction
> bind system global polname -priority 1
```

Befehlsrichtlinien für eine Partitionsbenutzer und Partitionsbenutzergruppen in administrativer Partition

Befehle zum Autorisieren eines Benutzerkontos innerhalb der Administratorpartition	Befehlsrichtlinien, die in einer Administratorpartition verfügbar sind (integrierte Richtlinien)	Zugriffsart des Benutzerkontos
Systembenutzer hinzufügen	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)
Systemgruppe hinzufügen	Partitions-Netzwerk	SNIP (mit aktiviertem Verwaltungszugriff)
Authentifizierung hinzufügen `<action, policy>`, System global binden `<policy name>`	Partition schreibgeschützt	SNIP (mit aktiviertem Verwaltungszugriff)
Systembenutzer entfernen	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)
Systemgruppe entfernen	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)
`bind system cmdpolicy` an Systembenutzer; `bind system cmdpolicy` an Systemgruppe	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)

Konfigurieren Sie einen LACP Ethernet-Kanal auf der Standard-Admin-Partition

Mit dem Link Aggregation Control Protocol (LACP) können Sie mehrere Ports zu einer einzigen Hochgeschwindigkeitsverbindung (auch Kanal genannt) kombinieren. Eine LACP-fähige Appliance tauscht LACP Data Units (LACPDU) über den Kanal aus.

Es gibt drei LACP-Konfigurationsmodi, die Sie in der Standardpartition einer NetScaler-Appliance aktivieren können:

1. Aktiv. Ein Port im aktiven Modus sendet LACPDUs. Die Link-Aggregation wird gebildet, wenn sich das andere Ende der Ethernet-Verbindung im aktiven oder passiven LACP-Modus befindet.

2. Passiv. Ein Port im passiven Modus sendet LACPDUs nur, wenn er LACPDUs empfängt. Die Link-Aggregation wird gebildet, wenn sich das andere Ende der Ethernet-Verbindung im aktiven LACP-Modus befindet.
3. Deaktivieren: Link-Aggregation wird nicht gebildet.

> **Hinweis**
>
> Standardmäßig ist die Link-Aggregation in der Standardpartition der Appliance deaktiviert.

LACP tauscht LACPDU zwischen Geräten aus, die über eine Ethernet-Verbindung verbunden sind. Diese Geräte werden normalerweise als Akteur oder Partner bezeichnet.

Eine LACPDU-Dateneinheit enthält die folgenden Parameter:

- LACP-Modus. Aktiv, passiv oder deaktiviert.
- LACP-Timeout. Die Wartezeit vor dem Timing des Partners oder Schauspielers. Mögliche Werte: Long und Short. Standardeinstellung: Long.
- Port-Schlüssel. Um zwischen den verschiedenen Kanälen zu unterscheiden. Wenn der Schlüssel 1 ist, wird LA/1 erstellt. Wenn der Schlüssel 2 ist, wird LA/2 erstellt. Mögliche Werte: Integer von 1 bis 8. 4 bis 8 ist für Cluster CLAG.
- Port-Priorität. Mindestwert: 1. Maximaler Wert: 65535 Standardwert: 32768.
- Systempriorität. Verwendet diese Priorität zusammen mit dem System-MAC, um die System-ID zu bilden, um das System während der LACP-Verhandlungen mit dem Partner eindeutig zu identifizieren. Legt die Systempriorität von 1 und 65535 fest. Der Standardwert ist auf 32768 festgelegt.
- Schnittstelle. Unterstützt 8 Schnittstellen pro Kanal auf NetScaler 10.1 Appliance und unterstützt 16 Schnittstellen pro Kanal auf NetScaler 10.5- und 11.0 Appliances.

Nach dem Austausch von LACPDUs verhandeln Akteur und Partner die Einstellungen und entscheiden, ob die Ports zur Aggregation hinzugefügt werden sollen.

Konfigurieren und überprüfen Sie LACP

Der folgende Abschnitt zeigt, wie LACP in der Admin-Partition konfiguriert und überprüft wird.

So konfigurieren und überprüfen Sie LACP auf einer NetScaler-Appliance über die CLI

1. Aktivieren Sie LACP auf jeder Schnittstelle.

   ```
   set interface <Interface_ID> -lacpMode PASSIVE -lacpKey 1<!--NeedCopy
   -->
   ```

   Wenn Sie LACP auf einer Schnittstelle aktivieren, werden die Kanäle dynamisch erstellt. Wenn Sie LACP auf einer Schnittstelle aktivieren und LacpKey auf 1 setzen, wird die Schnittstelle automatisch an den Kanal LA/1 gebunden.

> **Hinweis**
>
> Wenn Sie eine Schnittstelle an einen Kanal binden, haben die Kanalparameter Vorrang vor den Schnittstellenparametern, sodass die Interface-Parameter ignoriert werden. Wenn ein Kanal dynamisch von LACP erstellt wird, können Sie die Operationen zum Hinzufügen, Binden, Aufheben oder Entfernen auf dem Kanal nicht ausführen. Ein dynamisch von LACP erstellter Kanal wird automatisch gelöscht, wenn Sie LACP auf allen Schnittstellen des Kanals deaktivieren.

2. Legen Sie die Systempriorität fest.

   ```
   set lacp -sysPriority <Positive_Integer><!--NeedCopy-->
   ```

3. Stellen Sie sicher, dass LACP wie erwartet funktioniert.

   “‘show interface

   ```
   1 ```show channel<!--NeedCopy-->
   ```

   ```
   show LACP<!--NeedCopy-->
   ```

   > **Hinweis**
   >
   > In einigen Versionen von Cisco Internetwork Operating System (iOS) führt das Ausführen des nativen <VLAN_ID>VLAN-Befehls Switchport trunk dazu, dass der Cisco-Switch LACP-PDUs taggt. Dies führt dazu, dass der LACP-Kanal zwischen dem Cisco-Switch und der NetScaler-Appliance ausfällt. Dieses Problem wirkt sich jedoch nicht auf die im vorherigen Verfahren konfigurierten statischen Link-Aggregationskanäle aus.

Speichern Sie die Konfiguration aller Admin-Partitionen von der Standardpartition

Administratoren können die Konfiguration aller Admin-Partitionen gleichzeitig von der Standardpartition aus speichern.

Speichern Sie alle Admin-Partitionen von der Standardpartition mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
save ns config -all
```

Unterstützung für partitions- und clusterbasierte benutzerdefinierte Berichte

Die NetScaler GUI zeigt nur die benutzerdefinierten Berichte an, die in der aktuellen Anzeigepartition oder im Cluster erstellt wurden.

Zuvor wurde die NetScaler GUI verwendet, um die Namen des benutzerdefinierten Berichts direkt in der Back-End-Datei zu speichern, ohne die zu differenzierende Partition oder den Clusternamen zu erwähnen.

So zeigen Sie die benutzerdefinierten Berichte der aktuellen Partition oder des aktuellen Clusters in der GUI an

- Navigieren Sie zur Registerkarte **Reporting** .
- Klicken Sie auf **Benutzerdefinierte Berichte**, um die Berichte anzuzeigen, die in der aktuellen Partition oder im Cluster erstellt wurden.

Unterstützung zum Binden globaler VPN-Zertifikate in einem partitionierten Setup für OAuth IdP

In einem partitionierten Setup können Sie die Zertifikate jetzt für OAuth-IdP-Bereitstellungen an VPN global binden.

So binden Sie die Zertifikate im Partitiontion-Setup mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
bind vpn global [-certkeyName <string>] [-userDataEncryptionKey <string
    >]
```

VLAN-Konfiguration für Admin-Partitionen

May 11, 2023

VLANs können als “dediziertes” VLAN oder “Shared” VLAN an eine Partition gebunden werden. Basierend auf Ihrer Bereitstellung können Sie ein VLAN an eine Partition binden, um den Netzwerkverkehr von anderen Partitionen zu isolieren.

Dediziertes VLAN — Ein VLAN, das nur an eine Partition gebunden ist, wobei die Option “Freigabe” deaktiviert ist und ein getaggtes VLAN sein muss. Beispielsweise erstellt ein Systemadministrator in einer Client-Server-Bereitstellung aus Sicherheitsgründen ein dediziertes VLAN für jede Partition auf der Serverseite.

Gemeinsames VLAN — Ein VLAN, das an mehrere Partitionen gebunden (gemeinsam genutzt) ist, wobei die Option “Freigabe” aktiviert ist. Wenn der Systemadministrator beispielsweise in einer

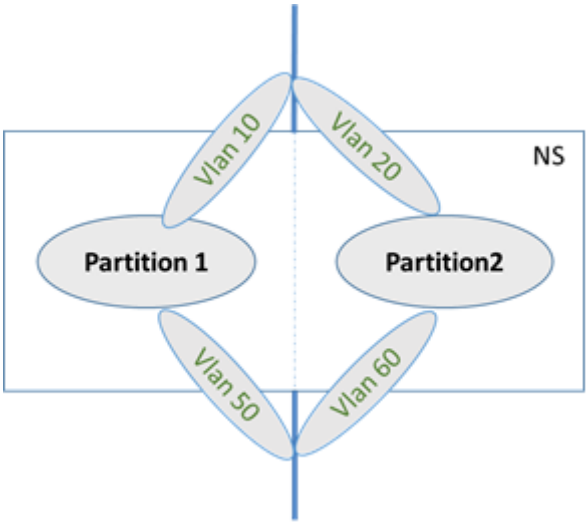
Client-Server-Bereitstellung keine Kontrolle über das clientseitige Netzwerk hat, wird ein VLAN erstellt und über mehrere Partitionen freigegeben.

Gemeinsam genutztes VLAN kann über mehrere Partitionen hinweg verwendet werden. Es wird in der Standardpartition erstellt und Sie können ein freigegebenes VLAN an mehrere Partitionen binden. Standardmäßig ist ein freigegebenes VLAN implizit an die Standardpartition gebunden und kann daher nicht explizit gebunden werden.

> **Hinweise**
>
> - Eine NetScaler-Appliance, die auf einer beliebigen Hypervisor-Plattform (ESX, KVM, Xen und Hyper-V) bereitgestellt wird, muss sowohl die folgenden Bedingungen in einer Partitionseinrichtung als auch in einer Datenverkehrsdomäne erfüllen:
>   - Enable the promiscuous mode, MAC changes, MAC spoofing, or forged transmit for shared VLANs with partition.
>   - Enable the VLAN with port group properties of the virtual switch, if the traffic is through a dedicated VLAN.
> - In einer partitionierten (Mehrmandanten) NetScaler-Appliance kann ein Systemadministrator den Datenverkehr isolieren, der zu einer bestimmten Partition oder Partitionen fließt. Dies geschieht durch Binden eines oder mehrerer VLANs an jede Partition. Ein VLAN kann für eine Partition oder für mehrere Partitionen freigegeben werden.
> - Internes Routing zwischen Partitionen, die auf derselben NetScaler Appliance gehostet werden, wird nicht unterstützt.

Dedizierte VLANs

Um den in eine Partition fließenden Datenverkehr zu isolieren, erstellen Sie ein VLAN und verknüpfen Sie es mit der Partition. Das VLAN ist dann nur für die zugehörige Partition sichtbar, und der durch das VLAN fließende Datenverkehr wird nur in der zugehörigen Partition klassifiziert und verarbeitet.



Gehen Sie wie folgt vor, um ein dediziertes VLAN für eine bestimmte Partition zu implementieren.

1. Fügen Sie ein VLAN hinzu (V1).
2. Binden Sie eine Netzwerkschnittstelle als getaggte Netzwerkschnittstelle an VLAN.
3. Erstellen Sie eine Partition (P1).
4. Binden Sie die Partition (P1) an das dedizierte VLAN (V1).

Konfigurieren Sie Folgendes über die CLI

- Erstellen Sie ein VLAN

  ```
  add vlan <id>
  ```

Beispiel

```
1     add vlan 100
```

- Binden Sie ein VLAN

  ```
  bind vlan <id> -ifnum <interface> -tagged
  ```

Beispiel

```
1     bind vlan 100  - ifnum 1/8 -tagged
```

- Erstellen Sie eine Partition

  ```
  Add ns partition <partition name> [-maxBandwidth <positive_integer>][-
  maxConn <positive_integer>] [-maxMemLimit <positive_integer>]
  ```

Beispiel


```
Add ns partition P1 -maxBandwidth 200 -maxconn 50 -maxmemlimit
    90

Done
```

- Binden einer Partition an ein VLAN

```
bind partition <partition-id> -vlan <id>
```

Beispiel

```
bind partition P1 -vlan 100
```

Konfigurieren eines dedizierten VLAN mit der NetScaler GUI

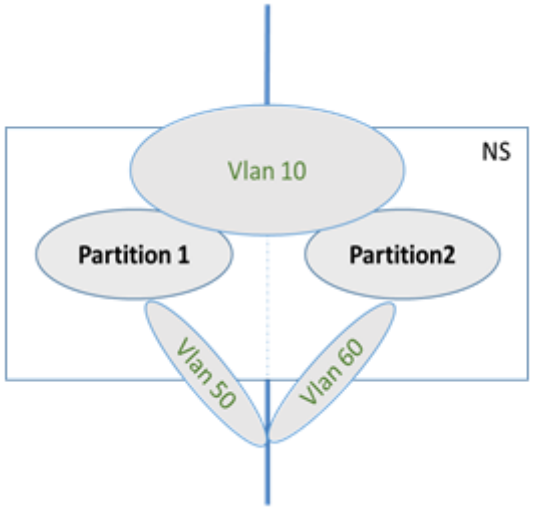
1. Navigieren Sie zu **Konfiguration > System > Netzwerk > VLANs*** und klicken Sie auf **Hinzufügen**, um ein VLAN zu erstellen.
2. Stellen Sie auf der Seite **VLAN erstellen** die folgenden Parameter ein:
   - VLAN-ID
   - Aliasname
   - Maximale Übertragungseinheit
   - Dynamisches Routing
   - IPv6 dynamisches Routing
   - Teilen von Partitionen
3. Wählen Sie im Abschnitt **Schnittstellenbindungen** eine oder mehrere Schnittstellen aus und binden Sie sie an das VLAN.
4. Wählen Sie im Abschnitt **IP-Bindungen** eine oder mehrere IP-Adressen aus und binden Sie an das VLAN.
5. Klicken Sie auf **OK** und **Fertig**.

Gemeinsames VLAN

In einer gemeinsam genutzten VLAN-Konfiguration hat jede Partition eine MAC-Adresse, und der im freigegebenen VLAN empfangene Datenverkehr wird nach MAC-Adresse klassifiziert. Es wird nur ein Layer3-VLAN empfohlen, da es den Subnetzverkehr einschränken kann. Eine Partitions-MAC-Adresse ist nur für eine gemeinsame VLAN-Bereitstellung anwendbar und wichtig.

> **Hinweis**
>
> Ab NetScaler Version 12.1 Build 51.16 unterstützt gemeinsam genutztes VLAN in einer partitionierten Appliance das dynamische Routingprotokoll.

Das folgende Diagramm zeigt, wie ein VLAN (VLAN 10) über zwei Partitionen gemeinsam genutzt wird.



Gehen Sie wie folgt vor, um eine freigegebene VLAN-Konfiguration bereitzustellen:

1. Erstellen Sie ein VLAN mit der Freigabeoption “aktiviert” oder aktivieren Sie die Freigabeoption für ein vorhandenes VLAN. Standardmäßig ist die Option “deaktiviert”.
2. Binden Sie die Partitionsschnittstelle an freigegebenes VLAN.
3. Erstellen Sie die Partitionen, jede mit ihrer eigenen PartitionMAC-Adresse.
4. Binden Sie die Partitionen an das freigegebene VLAN.

Konfigurieren eines freigegebenen VLAN über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um VLAN hinzuzufügen oder den Freigabe-Parameter eines vorhandenen VLANs festzulegen:

```
add vlan <id> [-sharing (ENABLED | DISABLED)]

set vlan <id> [-sharing (ENABLED | DISABLED)]

add vlan 100  -sharing ENABLED

set vlan 100  -sharing ENABLED
```


Binden einer Partition an ein freigegebenes VLAN mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
bind partition <partition-id> -vlan <id>

bind partition P1 - vlan 100

add ns partition P1 - maxBandwidth 200 - maxconn 50 - maxmemlimit 90
   -partitionMAC<mac_addr

Done
```

Konfigurieren einer Partition MAC-Adresse mit der CLI

```
set ns partition <partition name> [-partitionMAC<mac_addr>]

set ns partition P1 - partitionMAC 22:33:44:55:66:77
```

Binden von Partitionen an ein freigegebenes VLAN über die Befehlszeilenschnittstelle

```
bind partition <partition-id> -vlan <id>

bind partition <partition-id> -vlan <id>

bind partition P1 - vlan 100

bind partition P2 - vlan 100

bind partition P3 - vlan 100

bind partition P4 - vlan 100
```

Konfigurieren von freigegebenem VLAN mit der NetScaler GUI

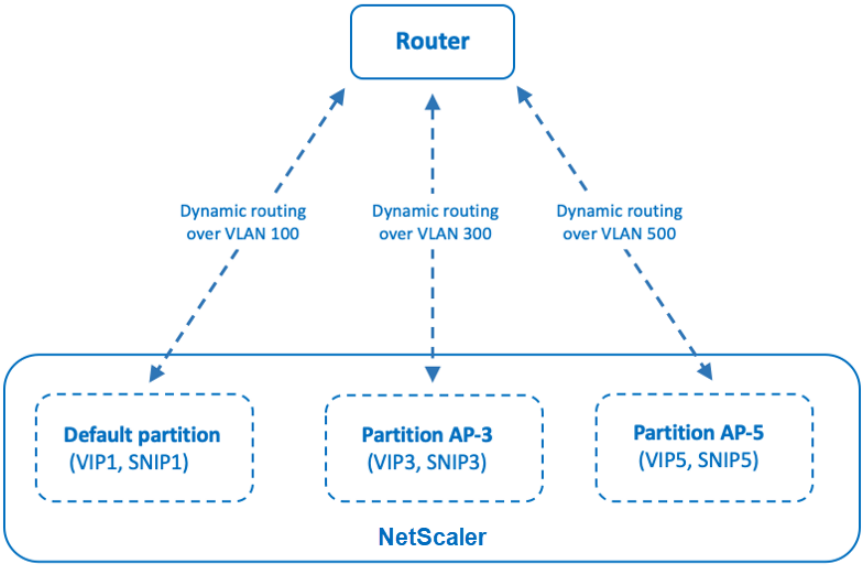
1. Navigieren Sie zu **Konfiguration > System > Netzwerk > VLANs**, wählen Sie dann ein **VLAN-Profil** aus und klicken Sie auf **Bearbeiten**, um den Parameter für die Partitionsfreigabe festzulegen.
2. Aktivieren Sie auf der Seite **VLAN erstellen** das Kontrollkästchen **Partitionsfreigabe** .
3. Klicke auf **OK** und dann auf **Fertig**.

Dynamisches Routing über ein freigegebenes VLAN über Admin-Partitionen hinweg

Admin-Partitionen in einer NetScaler-Appliance bieten eine Möglichkeit, mehrere Mandanten zu hosten.

Ab NetScaler Version 12.1 Build 51.16 unterstützt ein freigegebenes VLAN in einer partitionierten Appliance das dynamische Routingprotokoll. Das Routing kann in dedizierten oder gemeinsam genutzten VLANs konfiguriert werden, die mit Admin-Partitionen verknüpft sind.

Dediziertes VLAN einer Admin-Partition. In einem dedizierten VLAN wird der Datenpfad für den Mandanten mithilfe eines oder mehrerer VLANs identifiziert. Dies führt zu einer strengen Konfiguration und Datenpfadisolation für den Mandanten. Um den Zustand einer VIP-Adresse zu bewerben, ist dynamisches Routing in jeder Partition aktiviert und die Routing-Adjacenz wird pro Partition festgelegt.

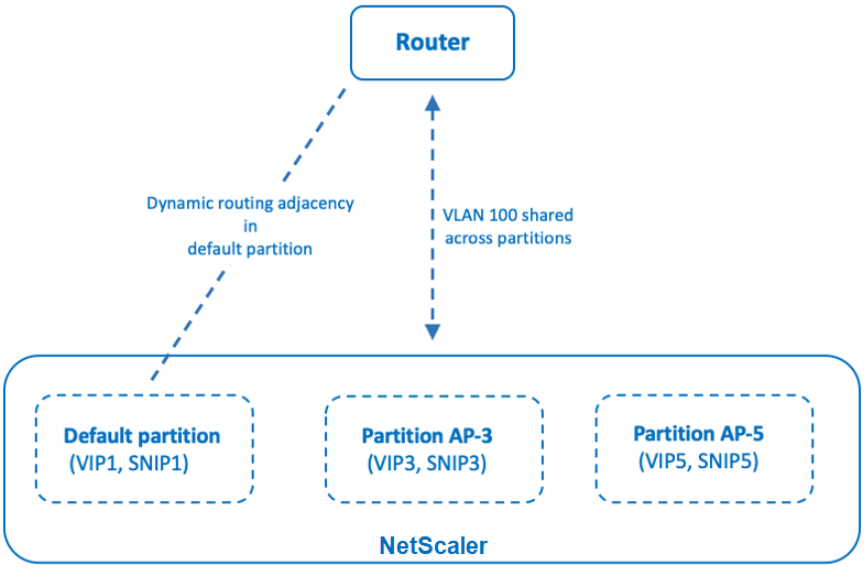


Dynamic routing over a dedicated VLAN per partition

Ein gemeinsam genutztes VLAN über Admin-Partitionenhinweg. In einem gemeinsam genutzten VLAN können VIP-Adressen, die in einer nicht standardmäßigen Partition konfiguriert sind, über eine einzelne Adjacenz oder ein Peering in der Standardpartition angekündigt werden. Eine SNIP-Adresse in der nicht standardmäßigen Partition wird als nächster Hop für alle VIP-Adressen (konfiguriert mit der Option **advertiseOnDefaultPartition**) in dieser nicht standardmäßigen Partition verwendet. Die konfigurierte SNIP-Adresse ist in den Routing-Ankündigungen als Next-Hop-IP-Adresse gekennzeichnet.

Betrachten Sie ein Beispiel für die Einrichtung von Administratorpartitionen in einer NetScaler-Appliance, VLAN 100 wird über die Standardpartition freigegeben und nicht standardmäßige Partitionen: AP-3 und AP-5. SNIP-Adressen SNIP1 wird in der Standardpartition hinzugefügt, SNIP3

wird in AP-3 hinzugefügt und SNIP5 wird in AP-5 hinzugefügt. SNIP1, SNIP3 und SNIP5 sind über den vlan-100 erreichbar. VIP-Adressen VIP1 wird in der Standardpartition hinzugefügt, VIP3 wird in AP-3 hinzugefügt und VIP5 wird in AP-5 hinzugefügt. VIP3 und VIP5 werden über die einzelne Adjacenz oder das Peering beworben, die in der Standardpartition gebildet werden.



Dynamic routing over a shared VLAN across partitions

Voraussetzungen

Stellen Sie vor dem Konfigurieren des dynamischen Routing über ein freigegebenes VLAN in einer nicht standardmäßigen Admin-Partition Folgendes sicher:

- **Dynamisches Routing wird im freigegebenen VLAN in der Standardpartition konfiguriert**. Das Konfigurieren des dynamischen Routing im freigegebenen VLAN in der Standardpartition umfasst die folgenden Schritte:
  1. Aktivieren Sie dynamisches Routing im freigegebenen VLAN.
  2. Fügen Sie eine SNIP-IP-Adresse mit aktiviertem dynamischem Routing hinzu. Diese SNIP-IP-Adresse wird für dynamisches Routing mit dem Upstream verwendet.
  3. Binden Sie das SNIP-IP-Subnetz an das freigegebene VLAN.
- **Ein oder mehrere dynamische Routingprotokolle ist auf der Standardpartition konfiguriert**. Weitere Informationen finden Sie unter Konfigurieren dynamischer Routingprotokolle.

Konfigurationsschritte

Das Konfigurieren des dynamischen Routing über ein freigegebenes VLAN in einer nicht standardmäßigen Admin-Partition besteht aus den folgenden Schritten:

1. **Fügen Sie eine SNIP-IP-Adresse in der nicht standardmäßigen Partition hinzu.** Diese SNIP-IP-Adresse muss sich im selben Subnetz der SNIP-IP-Adresse befinden, die für dynamisches Routing in der Standardpartition verwendet wird.
2. **Legen Sie die folgenden Parameter für die Ankündigung einer VIP-Adresse in einer nicht standardmäßigen Partition über das dynamische Routing fest oder aktivieren Sie sie**.
   - Host-Routen-Gateway (hostRtGw). Stellen Sie diesen Parameter auf die im vorherigen Schritt hinzugefügte SNIP-Adresse ein.
   - Ankündigen Sie auf der Standardpartition (advertiseOnDefaultPartition). Aktivieren Sie diesen Parameter.

Beispiel-Konfiguration

Betrachten Sie ein Beispiel für eine Einrichtung einer Admin-Partition in einer NetScaler-Appliance. Eine nicht standardmäßige Admin-Partition AP-3 ist auf dieser Appliance konfiguriert. Ein gemeinsam genutztes VLAN VLAN100 ist an AP-3 gebunden. Die folgende Beispielkonfiguration konfiguriert dynamisches Routing über VLAN100 in AP-3.

Schritte	Beispiel-Konfiguration
Auf Standard-Admin-Partition	-
Aktivieren Sie dynamisches Routing auf gemeinsam genutztem VLAN 100.	`set vlan 100 -dynamicRouting enabled`
Fügen Sie die SNIP-IP-Adresse 192.0.2.10 mit aktiviertem dynamischem Routing hinzu.Diese SNIP-IP-Adresse wird für dynamisches Routing mit dem Upstream verwendet.	`add ns ip 192.0.2.10 255.255.255.0 -type SNIP -dynamicRouting enabled`
Binden Sie das Subnetz von 192.0.2.10 an das gemeinsame VLAN 100.	`bind vlan 100 -IPAddress 192.0.2.10 255.255.255.0`
Auf nicht standardmäßiger Admin-Partition AP-3	-
Fügen Sie die SNIP-IP-Adresse 192.0.2.30 hinzu. Diese SNIP-IP-Adresse befindet sich im selben Subnetz wie die SNIP-IP-Adresse 192.0.2.10 auf der Standardpartition.	`add ns ip 192.0.2.30 255.255.255.0 -type SNIP`

Schritte	Beispiel-Konfiguration
Um die VIP-Adresse 203.0.113.300 mit dynamischem Routing zu bewerben, aktivieren Sie den Parameter advertiseOnDefaultPartition und setzen Sie den Parameter hostRtGw auf 192.0.2.30.	set ns ip 203.0.113.300 255.255.255.255 -hostRoute enabled -advertiseOnDefaultPartition enabled -hostRtGw 192.0.2.30

Dynamisches Routing von IPv6 über ein freigegebenes VLAN über eine Admin-Partition

Die Befehle enable ns feature IPv6PT und set L3Param -ipv6DynamicRouting ENABLED müssen aktiviert sein, damit eine IPv6-Adresse dynamisch über ein freigegebenes VLAN in einer Admin-Partition weiterleiten kann. Die folgenden Beispielkonfigurationen helfen Ihnen, das dynamische Routing von IPv6 über gemeinsam genutztes VLAN zu konfigurieren.

Beispiel-Konfiguration

Die folgende Beispielkonfiguration konfiguriert das dynamische Routing über VLAN 100 in AP-3.

Schritte	Beispiel-Konfiguration
Auf Standard-Admin-Partition	-
Aktivieren Sie dynamisches Routing auf gemeinsam genutztem VLAN 100.	set vlan 100 -dynamicRouting enabled
Fügen Sie die SNIP-IP-Adresse 2001:b:c:d□1/64 hinzu, wobei dynamisches Routing aktiviert ist.Die SNIP-IP-Adresse wird für das dynamische Routing mit dem Upstream verwendet.	add ns ip6 2001:b:c:d::1/64 -type SNIP -dynamicRouting enabled
Binden Sie Subnetz von 2001:b:c:d□1/64 an gemeinsam genutztes VLAN 100.	bind vlan 100 -IPAddress 2001:b:c:d::1/64
Auf nicht standardmäßiger Admin-Partition AP-3	-
Fügen Sie die SNIP-IP-Adresse 2001:b:c:d□2/64 hinzu. Diese SNIP-IP-Adresse befindet sich im selben Subnetz wie die SNIP-IP-Adresse 2001:b:c:d□ 2/64 auf der Standardpartition.	add ns ip6 2001:b:c:d::2/64 -type SNIP

Schritte	Beispiel-Konfiguration
Aktivieren Sie für Werbung VIP-Adresse 2002⊠1/128 mit dynamischem Routing den Parameter `advertiseOnDefaultPartition` und setzen Sie den Parameter `ip6hostRtGw` auf 2001:b:c:d⊠2.	`set ns ip6 2002::1/128 -hostRoute enabled -advertiseOnDefaultPartition enabled -ip6hostRtGw 2001:b:c:d::2`

Der in der Admin-Partition vorhandene VIP muss auf VTYSH der Standardpartition als Kernel-Route angezeigt werden.

```
> switch partition default
Done

>vtysh
ns#

ns# sh ipv6 route kernel

IPv6 routing table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
   IA - OSPF inter area, E1 - OSPF external type 1,
   E2 - OSPF external type 2, I - IS-IS, B - BGP
Timers: Uptime

K      2002::1/128 via 2001:b:c:d::2, vlan0, 01:24:15
                                >> on Default Partition, VIP : 2002::1
   present in AP known via SNIP6 : 2001:b:c:d::2 is present in AP as a
   Kernel Route
```

Es kann im Upstream angekündigt werden, indem die Option “Kernel weiterverteilen” unter OSPFv3/BGP+ in der Standardpartition verwendet wird.

```
ns# sh run router ipv6 ospf
!
router ipv6 ospf 1
redistribute kernel
!
```


Gemeinsames VLAN mit Admin-Partition auf der NetScaler SDX-Appliance

Auf einer SDX-Appliance müssen Sie die PMAC-Adresse mithilfe der Management Service-Benutzeroberfläche generieren und konfigurieren, bevor Sie die Admin-Partitionen mit gemeinsam genutzten VLANs verwenden. Mit dem Management Service können Sie Partitions-MAC-Adressen generieren, indem Sie:

- Verwenden einer Basis-MAC-Adresse
- Benutzerdefinierte MAC-Adressen angeben
- Zufällige Generierung von MAC-Adressen

> **Hinweise**
>
> - Die zufällig generierenden MAC-Adressen werden für andere Bereitstellungen außer Hochverfügbarkeit verwendet.
> - Nachdem Sie die MAC-Adressen der Partition generiert haben, müssen Sie die NetScaler Instanz neu starten, bevor Sie die Admin-Partitionen konfigurieren. Weitere Informationen zum Generieren von Partitions-MAC-Adressen von der SDX-Appliance finden Sie unter Generieren von Partitions-MAC-Adressen zum Konfigurieren der Admin-Partition auf einer NetScaler-Instanz in der SDX Appliance

VXLAN-Unterstützung für Admin-Partitionen

May 11, 2023

In einer partitionierten NetScaler-Appliance können Sie, ähnlich wie bei der Konfiguration eines VLAN, ein VXLAN in der Standardpartition konfigurieren. Nachdem Sie ein VXLAN konfiguriert haben, können Sie es an eine administrative Partition binden. Wenn ein VXLAN ein VLAN erweitert, das an eine Partition gebunden ist, bindet die Appliance das VXLAN an die Partition unter derselben Broadcast-Domäne. Es ist anwendbar, um ein VLAN aufzuheben, das ein VXLAN von der Partition entbindet.

Weitere Informationen zur Funktionsweise von VXLAN in einer NetScaler Appliance finden Sie unter VXLAN.

Weitere Informationen zur Funktionsweise von VLAN in einer partitionierten NetScaler Appliance finden Sie unter Admin-Partitionierung.

Punkte, die vor der Konfiguration eines VXLAN zu beachten sind

Beachten Sie die folgenden Punkte, bevor Sie ein VXLAN in einer partitionierten NetScaler-Appliance konfigurieren:

- Wenn Sie ein VLAN über VXLAN erweitern, stellen Sie sicher, dass das VLAN an die Partition gebunden ist.
- Nur ein Partitionsadministrator muss die IP und das dynamische Routing für das VXAN in der administrativen Partition konfigurieren.

Ein gemeinsam genutztes VXLAN wird in einer partitionierten Appliance nicht unterstützt. Daher kann ein VXLAN nicht mit einem gemeinsam genutzten VLAN gekennzeichnet werden, oder Sie können ein VLAN nicht zu einem gemeinsam genutzten VLAN machen, wenn es mit einem VXLAN gekennzeichnet ist.

Unterstützte VXLAN-Konfigurationen

Im Folgenden finden Sie die unterstützten VXLAN-Konfigurationen.

Erweiterung des VLAN über ein VXLAN in derselben Broadcast-Domäne

Die folgenden CLI-Schritte helfen Ihnen, ein VLAN über ein VXLAN und umgekehrt innerhalb derselben Broadcast-Domäne zu erweitern.

1. Hinzufügen eines VLAN in der Standardpartition

```
add vlan <id>
```

2. Erweitern Sie VLAN über ein VXLAN innerhalb derselben Broadcastdomäne.

```
add vxlan <vxlan id>  - vlan <id>
```

3. Konfigurieren Sie einen Peer `vtep`, der den gesamten BUM-Verkehr (Broadcast unbekannten Multicast) trägt.

> **Hinweis**
>
> Die Adresse `vtep` kann eine Multicast-Adresse sein.

```
add bridgetable -mac <mac_addr> -vxlan <positive_integer> -vtep <
    ip_addr> [-vni <positive_integer>][-deviceVlan <
    positive_integer>]
```

4. Binden Sie IP-Adressen an VXLAN.

```
bind vxlan <id> [-srcIP <ip_addr>][-IPAddress <ip_addr|ipv6_addr
    |*> [<netmask>]]
```

5. Binden Sie VLAN an eine administrative Partition.


```
bind partition <partition-id> -vxlan <id>

add vlan 3000

add vxlan 3000 -vlan 10

add bridgetable -mac 00:00:00:00:00:00 -vxlan 3000 -vtep
    10.102.58.8 -vni 11

bind vxlan 3000 - srcIP 10.102.101.15

bind partition p1 -vlan 10
```

SNMP-Unterstützung für Admin-Partitionen

May 11, 2023

Eine partitionierte NetScaler-Appliance verwendet die SNMP-Infrastruktur zur Begrenzung der Partitionsrate und zur Überwachung der Details zur Nutzung der Partitionsressourcen.

SNMP-Traps zur Begrenzung der Admin-Partitionsrate

Auf einer partitionierten NetScaler-Appliance kann ein PARTITION-RATE-LIMIT-Alarm neun SNMP-Traps erzeugen, um zu benachrichtigen, dass eine Partitionsressource (wie Bandbreite, Verbindung oder Speicher) ihr Limit erreicht hat oder zum Normalzustand zurückgekehrt ist.

Die folgenden neun SNMP-Traps werden generiert, wenn:

- Der**Schwellenwert von PartitionConn wurde erreicht.** Die Anzahl der aktiven Verbindungen für eine Partition überschreitet ihren hohen Schwellenwert in Prozent.
- **PartitionConnThresholdNormal.** Die Anzahl der aktiven Verbindungen ist kleiner oder gleich dem normalen Schwellenwert in Prozent.
- Der**Schwellenwert der Partition BW ist erreicht.** Die Bandbreitennutzung der Partition erreicht ihren hohen Schwellenwert in Prozent.
- **PartitionMemThreshold erreicht.** Die aktuelle Speichernutzung der Partition überschreitet den prozentualen Schwellenwert für den hohen Schwellenwert.
- **PartitionMemThresholdNormal.** Die aktuelle Speichernutzung der Partition wird kleiner oder gleich dem normalen Schwellenwert in Prozent.
- **PartitionMemLimit überschritten.** Die aktuelle Speichernutzung der Partition überschreitet den prozentualen Speichergrenzwert.

- **PartitionConnLimit überschritten.** Die Anzahl der aktiven Verbindungen für eine Partition überschreitet den konfigurierten Grenzwert und neue Verbindungen werden unterbrochen.
- **PartitionConnLimitNormal.** Die Anzahl der aktiven Verbindungen für eine Partition unterschreitet den konfigurierten Grenzwert und die Partition kann jetzt eine neue Verbindung akzeptieren.
- Das Limit für**Partition BW wurde überschritten.** Die aktuelle Bandbreitennutzung für eine Partition hat das konfigurierte Limit überschritten.

Die Schwellenwerte für die SNMP-Traps sind nicht konfigurierbar und lauten wie folgt:

- Hoher Schwellenwert = 80% (gilt für alle Traps mit Partitionsratenbegrenzung)
- Niedriger Schwellenwert = 60% (gilt für alle Traps mit Partitionsratenbegrenzung)
- Speicherlimit = 95% (gilt nur für Partitionsspeichertraps)

Konfiguration des PARTITION-RATE-LIMIT-Alarms

Um den PARTITION-RATE-LIMIT-Alarm in einer bestimmten Partition zu konfigurieren und die Generierung der SNMP-Trap-Meldungen zu aktivieren.

1. Den PARTITION-RATE-LIMIT-Alarm aktivieren
2. Alarm für PARTITION-RATE-LIMIT konfigurieren
3. SNMP-Trap-Ziel konfigurieren

Um den PARTITION-RATE-LIMIT-Alarm mit der CLI zu aktivieren

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
enable snmp alarm PARTITION-RATE-LIMIT

show snmp alarm PARTITION-RATE-LIMIT
```

So konfigurieren Sie den PARTITION-RATE-LIMIT-Alarm mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set snmp alarm PARTITION-RATE-LIMIT [-state ( ENABLED | DISABLED )] [-
    severity <severity>] [-logging ( ENABLED | DISABLED )]
```

So konfigurieren Sie das SNMP-Trap-Ziel mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:


```
add snmp trap <trapClass> <trapDestination> [-version <version>] [-td <
    positive_integer>] [-destPort <port>] [-communityName <string>] [-
    srcIP <ip_addr|ipv6_addr>] [-severity <severity>] [-allPartitions (
    ENABLED | DISABLED )]
```

So konfigurieren Sie den Alarm für Partitionsraten-Limit mit der GUI

Navigieren Sie zu **System > SNMP > Alarms**, wählen Sie **PARTITION-RATE-LIMIT-Alarm aus und konfigurieren Sie die** Alarmparameter.

So konfigurieren Sie das SNMP-Trap-Ziel mithilfe der GUI

Navigieren Sie zu **System > SNMP > Trap**und geben Sie die IP-Adresse des Zielgeräts an.

SNMP-Überwachung für die Auslastung der Partitionsressourcen

Mithilfe von SNMP können Sie die Ressourcennutzungsdetails einer Partition (wie Bandbreite, Verbindung und Speicher) in Echtzeit auf einer NetScaler-Appliance überwachen. Dazu wird vom SNMP-Manager eine SNMP-Anforderung (wie SNMP GET, SNMP GET BULK, SNMP GETNEXT oder SNMP WALK) gesendet.

> **Hinweis**
>
> Um die Partitionsressourcen zu überwachen, müssen Sie die SNMP-Community in der Standardpartition konfigurieren. Dabei wird die *PartitionTable* in der Standardpartition verwaltet und die SNMP-Kommunikation erfolgt über die NSIP-Adresse der Appliance.

Stellen Sie sich ein Szenario vor, in dem ein NetScaler-Administrator die Bandbreitennutzung der Partition P1 auf der Appliance wissen möchte. Der SNMP-Manager ruft diese Informationen ab, indem er eine SNMP-GET-Anfrage über die entsprechende OID (PartitionCurrentBandwidth) an die NSIP-Adresse der Appliance sendet. Der SNMP-Agent auf der Standardpartition ruft die aktuelle Bandbreitennutzung von P1 ab und sendet sie über die NSIP-Adresse an den SNMP-Manager.

In der folgenden Tabelle sind die SNMP-Zähler aufgeführt, die Teil von *PartitionTable* sind, und ihre Beschreibung:

SNMP-Parameter	SNMP-ID	Beschreibung
Name der Partition	1.3.6.1.4.1.5951.4.1.1.88.1.1	Name der Partition
Aktuelle Bandbreite der Partition	1.3.6.1.4.1.5951.4.1.1.88.1.2	Aktuelle Bandbreitennutzung der Partition.

SNMP-Parameter	SNMP-ID	Beschreibung
Aktuelle Verbindungen partitionieren	1.3.6.1.4.1.5951.4.1.1.88.1.3	Aktuelle Anzahl der aktiven Verbindungen der Partition.
Partition Speichernutzung PCNT	1.3.6.1.4.1.5951.4.1.1.88.1.4	Aktuelle Speichernutzung (in Prozent) der Partition.

Unterstützung des Überwachungsprotokolls für Admin-Partitionen

May 11, 2023

Auf einer partitionierten NetScaler-Appliance können Sie zur Verbesserung der Datensicherheit die Überwachungsprotokollierung in einer administrativen Partition mithilfe erweiterter Richtlinien konfigurieren. Beispielsweise möchten Sie möglicherweise Protokolle (Status und Statusinformationen) einer bestimmten Partition anzeigen. Je nach Autorisierungsgrad in der Partition greifen mehrere Benutzer auf verschiedene Funktionen zu.

Wichtige Punkte

1. Die von der Partition generierten Prüfprotokolle werden als eine einzige Protokolldatei (/var/log/ns.log) gespeichert.
2. Konfigurieren Sie die Subnetzadresse des Audit-Log-Servers (Syslog oder NS Log) als Quell-IP-Adresse in der Partition für das Senden der Audit-Log-Meldungen.
3. Die Standardpartition verwendet standardmäßig das NSIP als Quell-IP-Adresse für die Überwachungsprotokollnachrichten.
4. Sie können die Audit-Protokoll-Meldung anzeigen, indem Sie den Befehl “Audit-Nachrichten anzeigen” verwenden.

Informationen zur Konfiguration des Audit-Logs finden Sie unter Konfigurieren der NetScaler Appliance für die Audit-Protokollierung.

Konfigurieren der Überwachungsprotokollierung in partitionierter NetScaler Appliance

Führen Sie die folgenden Aufgaben aus, um die Überwachungsprotokollierung in einer administrativen Partition zu konfigurieren.

1. Konfigurieren Sie die IP-Adresse des Partitionssubnetzes. Eine IPv4-SNIP-Adresse einer administrativen Partition.

2. Konfigurieren Sie die Audit-Log-Aktion (Syslog und NS Log). Eine Audit-Aktion ist eine Sammlung von Informationen, die angeben, welche Nachrichten protokolliert werden sollen und wie die Nachrichten auf dem externen Protokollserver protokolliert werden.
3. Konfigurieren Sie Audit-Log-Richtlinien (Syslog und NS Log). Audit-Log-Richtlinien definieren Protokollmeldungen für die Quellpartition an den Syslog- oder NS-Log-Server.
4. Binden Sie die Audit-Log-Richtlinie an die SysGlobal- und NSGlobal-Entität. Binden Sie eine Audit-Log-Richtlinie an eine globale Systementität.
5. Überprüfen Sie die Audit-Log-Statistiken. Zeigen Sie die Audit-Log-Statistiken an und bewerten Sie die Konfiguration.

Konfigurieren Sie Folgendes über die CLI

1. Erstellen Sie die Subnetz-IP-Adresse einer Partition

   ```
   add ns ip <ip address> <subnet mask>
   ```

2. Eine Syslog-Aktion erstellen

   ```
   add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )] [-transport ( TCP |
   UDP )]
   ```

3. Eine NS-Log-Aktion erstellen

   ```
   add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
   <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )]
   ```

4. Erstellen Sie eine Syslog-Audit-Log-Richtlinie

   ```
   add audit syslogpolicy syslog-pol1 true audit-action1
   ```

5. Audit-Log-Richtlinien für das NS-Protokoll erstellen

   ```
   add audit nslogpolicy nslog-pol1 true audit-action1
   ```

6. Binden Sie eine Audit-Log-Richtlinie an die SyslogGlobal-Entität

   ```
   bind audit sysloglobal -policyName <name> -priority <priority_integer>
    -globalBindType SYSTEM_GLOBAL
   ```

7. Binden Sie eine Audit-Log-Richtlinie an die NSLogGlobal-Entität

   ```
   bind audit nslogglobal -policyName <name> -priority <priority_integer>
   -globalBindType SYSTEM_GLOBAL
   ```

8. Anzeige einer Audit-Log-Statistik

   ```
   stat audit -detail
   ```


Beispiel

```
add ns ip 10.102.1.1 255.255.255.0
add audit syslogAction syslog_action1 10.102.1.2 -logLevel
    INFORMATIONAL -dateFormat MMDDYYYY -transport UDP
add audit syslogpolicy syslog-pol1 true syslog_action1
bind audit sysloggloba l -policyName syslog-pol1 -priority 1 -
    globalBindType SYSTEM_GLOBAL
```

Speichern von Protokollen

Wenn der SYSLOG- oder NSLOG-Server Protokollinformationen von allen Partitionen sammelt, werden diese als Protokollmeldungen in der Datei ns.log gespeichert. Die Logmeldungen enthalten die folgenden Informationen:

- Name der Partition.
- Die IP-Adresse.
- Ein Zeitstempel.
- Meldungstyp
- Die vordefinierten Protokollebenen (Kritisch, Fehler, Hinweis, Warnung, Information, Debug, Warnung und Notfall)
- Die Nachrichteninformationen.

Konfigurierte PMAC-Adressen für freigegebene VLAN-Konfiguration anzeigen

May 11, 2023

Um ein Partitions-Setup mit freigegebener VLAN-Konfiguration zu verwenden, benötigen Sie eine virtuelle MAC-Adresse, die als Partitions-MAC (PMAC) -Adresse bezeichnet wird. Die Partition verwendet die PMAC-Adresse für ihre Kommunikation im freigegebenen VLAN. Für jede Partition wird eine eindeutige PMAC-Adresse konfiguriert und in allen freigegebenen VLANs verwendet, die an diese Partition gebunden sind. Im Fall einer Nicht-SDX-Plattform (VPX oder MPX) kann die PMAC-Adresse entweder vom Benutzer angegeben oder intern von einer NetScaler-Appliance generiert werden. Wenn die PMAC-Adresse nicht für eine Partition angegeben ist, wird sie intern generiert, wenn die Partition an das erste freigegebene VLAN gebunden ist. Während im Fall einer SDX-Plattform die PMAC-Adressen immer zuerst über das SVM-Tool konfiguriert und dann einer Partition zugewiesen werden müssen.

Um eine Liste der konfigurierten PMACs anzuzeigen, können Sie den Befehl **Show ns PartitionMac**

verwenden. Mit dem Befehl können Sie die konfigurierten PMACs entweder über die NetScaler CLI oder die GUI überprüfen. Der Befehl zeigt alle PMAC-Adressen und die entsprechenden Partitionen an (falls zugewiesen). Im Fall einer Nicht-SDX-Plattform zeigt der Befehl alle PMAC-Adressen und ihre entsprechenden Partitionen an, da die PMAC-Adresse einer Partition nur auf Bedarfsbasis zugewiesen wird (wenn eine Partition ein gemeinsam genutztes VLAN gebunden hat). Im Fall einer SDX-Plattform haben Sie jedoch möglicherweise einige nicht zugewiesene PMACs in der Liste.

Informationen zum Generieren von PMAC für die SDX-Plattform finden Sie unter Generieren von Partitions-MAC-Adressen .

Anzeige von PMACs mit der NetScaler CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
show ns partitionMAC
```

```
1 Partition MAC Partition Name
2
3 1) f2:0c:64:da:f6:d7
4
5 2) b4:0c:43:da:f6:d2
6
7 3) a6:e7:b2:6c:48:e0
8
9 Done
```

Anzeige von PMAC-Adressen mit der NetScaler GUI

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration > System > Partition MAC**.
2. Auf der Seite Partition MAC wird eine Liste der PMACs und ihrer Partitionen angezeigt.

AppExpert

May 11, 2023

Die folgenden Themen enthalten eine konzeptionelle Referenz und Konfigurationsanweisungen für den AppExpert und andere Funktionen der NetScaler-Appliance.

> **Hinweis**
>
> Informationen zu Richtlinienerweiterungen finden Sie unter Richtlinienerweiterungen.

- Action Analytics: Sammelt Laufzeitstatistiken auf der Grundlage vordefinierter Kriterien. Wenn Sie mit Richtlinien verwendet werden, bietet Ihnen die Funktion auch die Infrastruktur für die automatische Optimierung des Datenverkehrs in Echtzeit.
- AppExpert AppExpert Applications and Templates: Vereinfachen Sie Konfigurationsschritte für die Citrix® NetScaler® Appliance mithilfe von Anwendungen, Anwendungsvorlagen, NetScaler Gateway-Anwendungen und Entitätsvorlagen.
- AppQoe: Quality of Experience (AppQoE) auf Anwendungsebene integriert mehrere vorhandene richtlinienbasierte Sicherheitsfunktionen der NetScaler-Appliance in ein einziges integriertes Feature, das einen neuen Warteschlangenmechanismus, Fair Queuing, nutzt.
- Entitätsvorlage: Beschreibt, wie Entitätsvorlagen zum Einrichten und Konfigurieren einzelner NetScaler-Entitäten wie eine Richtlinie oder ein virtueller Server verwendet werden. Eine Entitätsvorlage stellt eine Spezifikation und eine Reihe von Standardeinstellungen für das Objekt bereit.
- HTTP-Callouts: Eine HTTP-Anforderung, die die NetScaler-Appliance generiert und an eine externe Anwendung sendet, wenn bestimmte Kriterien bei der Richtlinienbewertung erfüllt sind.
- Mustersätze: Erlaubt den Zeichenfolgenabgleich während der Auswertung einer erweiterten Richtlinie.
- Richtlinien und Ausdrücke: Regeln, die die Vorgänge bestimmen, die die NetScaler-Appliance ausführen muss.
- Ratenbegrenzung: Definiert die maximale Last für eine bestimmte Netzwerkentität oder eine virtuelle Entität auf der NetScaler-Appliance.
- Responder: Basiert Antworten darauf, wer die Anfrage sendet, woher sie gesendet wird, und andere Kriterien mit Auswirkungen auf die Sicherheit und das Systemmanagement.
- Rewrite: Schreibt Informationen in den von der NetScaler-Appliance behandelten Anfragen oder Antworten neu.
- String-Maps: Führen Sie einen Musterabgleich in allen NetScaler-Features durch, die die Standardrichtlinie verwenden.

Action-Analytik

May 11, 2023

Die Leistung Ihrer Website oder Anwendung hängt davon ab, wie gut Sie die Bereitstellung der am häufigsten angeforderten Inhalte optimieren. Techniken wie Caching und Komprimierung beschleunigen die Bereitstellung von Diensten für Clients, aber Sie müssen in der Lage sein, die am häufigsten angeforderten Ressourcen zu identifizieren und diese Ressourcen dann zwischenzuspeichern oder zu komprimieren. Sie können die am häufigsten verwendeten Ressourcen identifizieren, indem Sie Echtzeitstatistiken über den Website- oder Anwendungsverkehr aggregieren. Statistiken wie häufig auf eine Ressource im Verhältnis zu anderen Ressourcen zugegriffen wird und wie viel Bandbreite von diesen Ressourcen verbraucht wird, helfen Ihnen festzustellen, ob diese Ressourcen zwischengespeichert oder komprimiert werden müssen, um die Serverleistung und Netzwerkauslastung zu verbessern. Statistiken wie Reaktionszeiten und die Anzahl gleichzeitiger Verbindungen zur Anwendung helfen Ihnen festzustellen, ob Sie serverseitige Ressourcen erweitern müssen.

Wenn sich die Website oder Anwendung nicht häufig ändert, können Sie Produkte verwenden, die statistische Daten sammeln, die Statistiken manuell analysieren und die Bereitstellung von Inhalten optimieren. Wenn Sie jedoch keine manuellen Optimierungen durchführen möchten oder wenn Ihre Website oder Anwendung dynamischer Natur ist, benötigen Sie eine Infrastruktur, die nicht nur statistische Daten sammeln, sondern auch die Bereitstellung von Ressourcen auf der Grundlage der Statistiken automatisch optimieren kann. Auf der NetScaler-Appliance wird diese Funktionalität von der Action Analytics-Funktion bereitgestellt. Die Funktion arbeitet auf einer einzelnen NetScaler-Appliance und sammelt Laufzeitstatistiken auf der Grundlage von Kriterien, die Sie definieren. Bei Verwendung mit NetScaler Richtlinien bietet das Feature auch die Infrastruktur, die Sie für die automatische Optimierung des Datenverkehrs in Echtzeit benötigen.

Bei der Konfiguration der Aktionsanalysefunktion geben Sie die Anforderungsattribute an, für die Sie statistische Daten sammeln möchten, z. B. URLs und HTTP-Methoden, indem Sie erweiterte Richtlinienausdrücke in einer Entität konfigurieren, die als Selektor bezeichnet wird. Anschließend konfigurieren Sie einen Bezeichner, um Einstellungen wie das Abtastintervall und die Anzahl der Abtastproben zu konfigurieren. Sie konfigurieren auch eine Richtlinie, die es der Appliance ermöglicht, den Datenverkehr gemäß dem Selektor-Identifier-Paar auszuwerten. Schließlich binden Sie die Richtlinie an einen Bindepunkt, um mit dem Sammeln von Statistiken zu beginnen.

Die Appliance bietet Ihnen außerdem eine Reihe integrierter Selektoren, Identifikatoren und Responder-Richtlinien, mit denen Sie mit der Funktion beginnen können.

Die Appliance aggregiert die folgenden Statistiken:

- Die Anzahl der Anfragen.
- Die von den Anfragen verbrauchte Bandbreite.
- Die Reaktionszeit.
- Die Anzahl gleichzeitiger Verbindungen.

Sie können die Funktion so konfigurieren, dass die Datensätze zur Laufzeit für ein Attribut Ihrer Wahl sortiert werden. Sie können die statistischen Daten über die Befehlszeile oder des Stream-Sessions-Tools im Konfigurationsdienstprogramm anzeigen.

Konfigurieren eines Selektors

May 11, 2023

Ein Selektor ist ein Filter zur Identifizierung von Anfragen. Es besteht aus bis zu fünf einzelnen erweiterten Richtlinienausdrücken, die Anforderungsattribute wie die Client-IP-Adresse und die URL in der Anforderung identifizieren. Jeder Ausdruck ist ein nicht zusammengesetzter erweiterter Richtlinienausdruck und wird als in einer UND-Beziehung zu den anderen Ausdrücken betrachtet. Nachfolgend einige Beispiele für Selektorausdrücke:

- `HTTP.REQ.URL`
- `CLIENT.IP.SRC`
- `HTTP.RES.BODY(1000).AFTER_STR("<string>").BEFORE_STR("<string>")"`
- `CLIENT.IP.SRC.SUBNET(24)`

Selektoren werden in Konfigurationen zur Ratenbegrenzung und Aktionsanalyse verwendet. Ein Selektor ist in einer ratenbegrenzenden Konfiguration optional, in einer Action-Analytics-Konfiguration jedoch erforderlich.

Die Reihenfolge, in der Sie Parameter angeben, ist signifikant. Wenn Sie beispielsweise eine IP-Adresse und eine Domäne (in dieser Reihenfolge) in einem Selektor konfigurieren und dann die Domäne und die IP-Adresse (in umgekehrter Reihenfolge) in einem anderen Selektor angeben, betrachtet NetScaler diese Werte als eindeutig. Dies kann dazu führen, dass dieselbe Transaktion zweimal gezählt wird. Wenn mehrere Richtlinien denselben Selektor aufrufen, kann der NetScaler dieselbe Transaktion erneut mehr als einmal zählen.

Wenn Sie einen Ausdruck in einem Selektor ändern, wird möglicherweise eine Fehlermeldung angezeigt, wenn eine Policy Label, die ihn aufruft, an eine neue Richtlinienbezeichnung oder einen neuen Bindepunkt gebunden ist. Angenommen, Sie erstellen einen Selektor mit dem Namen myLimitSelector1, rufen ihn von myLimitID1 aus auf und rufen den Bezeichner aus einer DNS-Richtlinie namens DNSrateLimit1 auf. Wenn Sie den Ausdruck in myLimitSelector1 ändern, wird möglicherweise eine Fehlermeldung angezeigt, wenn Sie DNSRateLimit1 an einen neuen Bindepunkt binden. Die Problemumgehung besteht darin, diese Ausdrücke zu ändern, bevor die Richtlinien erstellt werden, die sie aufrufen.

Die NetScaler-Appliance bietet integrierte Selektoren pdf für einige der häufigsten Anwendungsfälle. Siehe PDF.

Sie können auch einen Selektor mit Ausdrücken konfigurieren, die die Anforderungsattribute Ihrer Wahl identifizieren. Beispielsweise möchten Sie möglicherweise einen Datensatz für eine Anforderung erstellen, die mit einem bestimmten Header eingeht. Um den Header auszuwerten, können Sie `HTTP.REQ.HEADER("<header_name>")` dem Selektor hinzufügen, den Sie verwenden möchten.

So konfigurieren Sie einen Selektor über die Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Selektor zu konfigurieren und die Konfiguration zu überprüfen:

- `add stream selector <name> <rule> ...`
- `show stream selector`

Beispiel

```
1  > add stream selector myselector HTTP.REQ.URL CLIENT.IP.SRC
2   Done
3  > show stream selector myselector
4      Name: myselector
5      Expressions:
6          1) HTTP.REQ.URL
7          2) CLIENT.IP.SRC
8   Done
9  >
10 <!--NeedCopy-->
```

So ändern oder entfernen Sie einen Selektor über die Befehlszeile:

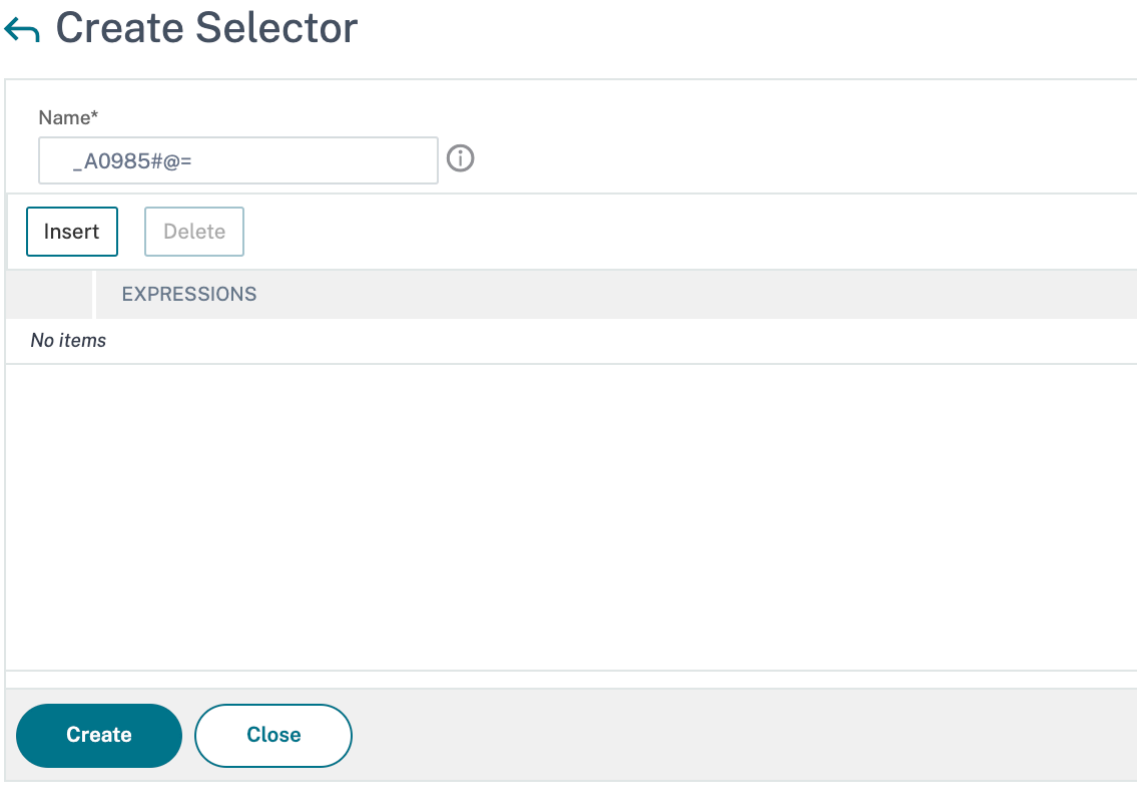
- Um einen Selektor zu ändern, geben Sie den Befehl set stream selector, den Namen des Selektors und den Regelparameter mit den Ausdrücken ein. Geben Sie die vorhandenen Ausdrücke ein, die Sie beibehalten möchten, zusammen mit den neuen Ausdrücken, die Sie hinzufügen möchten.
- Um einen Selektor zu entfernen, geben Sie den Befehl rm stream selector und den Namen des Selektors ein.

So konfigurieren Sie einen Selektor über die GUI:

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Selektoren**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um einen Selektor zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um einen Selektor zu ändern, wählen Sie den Selektor aus und klicken dann auf **Bearbeiten**.
3. Legen Sie auf der Seite **Auswahl erstellen** oder **Auswahl konfigurieren** die folgenden Parameter fest:
   - Name. Um einen Namen für den Selektor hinzuzufügen, geben Sie den Namen in das Feld **Name** ein. Der Name muss mit ASCII, alphanumerischem Zeichen oder Unterstrichen beginnen. Der Name darf nur alphanumerische ASCII-, Unterstrich-, Hash-, Punkt-, Leerzeichen-, Doppelpunkt-, Gleich- und Bindestriche enthalten.

- Ausdrücke. Um den Ausdruck zur Selektorkonfiguration hinzuzufügen, klicken Sie auf **Einfügen**. Um einen Ausdruck aus der Selektorkonfiguration zu entfernen, wählen Sie im Feld Ausdruck den Ausdruck aus, und klicken Sie dann auf **Löschen**. Hinweis: Geben Sie im Feld Ausdrücke einen gültigen Parameter ein. Geben Sie beispielsweise HTTP ein. Geben Sie dann einen Zeitraum nach diesem Parameter ein. Ein Dropdown-Menü wird angezeigt. Der Inhalt dieses Menüs enthält die Keywords, die dem ursprünglichen Keyword folgen können, das Sie eingegeben haben. Um das nächste Schlüsselwort in diesem Ausdruckspräfix auszuwählen, doppelklicken Sie im Dropdown-Menü auf die Auswahl. Im Textfeld **Ausdrücke** werden sowohl das erste als auch das zweite Schlüsselwort für das Ausdruckspräfix angezeigt, z. B. Fahren Sie mit dem Hinzufügen von Ausdruckskomponenten fort, bis der vollständige Ausdruck gebildet wird.

4. Klicken Sie auf **Einfügen**.
5. Fügen Sie bis zu fünf nicht zusammengesetzte Ausdrücke hinzu.
6. Klicken Sie auf **Erstellen** und dann auf **Schließen**.



Konfigurieren eines Stream-Bezeichners

May 11, 2023

Sie konfigurieren einen Stream-Identifier, um Parameter für die Erfassung statistischer Daten aus Anfragen anzugeben, die von einem bestimmten Selektor identifiziert wurden. Ein Identifier gibt den zu verwendenden Selektor, das Statistikerfassungsintervall, die Anzahl der Stichproben und das Feld an, nach dem die Datensätze sortiert werden sollen.

Die NetScaler-Appliance enthält die folgenden integrierten Stream-Identifier für gängige Anwendungsfälle. Alle integrierten Identifikatoren geben eine Probenzahl von 1 und ein Intervall von 1 Minute an. Darüber hinaus sortieren sie die Daten nach dem
REQUESTS-Attribut. Sie unterscheiden sich nur darin, dass sie verschiedenen eingebauten Selektoren zugeordnet sind. Jeder integrierte Bezeichner ist mit einem integrierten Selektor mit demselben Namen verknüpft (der eingebaute Identifier
top_URL ist beispielsweise dem integrierten
Selektor top_URL zugeordnet). Im Folgenden sind die integrierten Identifikatoren aufgeführt:

- Top_URL
- Top_Kunden
- Top_URL_Clients_LBVServer
- Top_URL_Clients_CSVServer
- Top_MSSQL_Query_DB_LBVServer
- Top_MYSQL_QUERY_DB_LBVSERVER

Weitere Informationen zu den integrierten Selektoren finden Sie unter Konfigurieren eines Selektors.

Hinweis: Die maximale Länge für das Speichern von Zeichenfolgenergebnissen von Selektoren (z. B. HTTP.REQ.URL) beträgt 60 Zeichen. Wenn die Zeichenfolge (z. B. URL) 1000 Zeichen lang ist, von denen 50 Zeichen ausreichen, um eine Zeichenfolge eindeutig zu identifizieren, verwenden Sie einen Ausdruck, um nur die erforderlichen 50 Zeichen zu extrahieren.

Sie können die Konfiguration einer integrierten Kennung nicht ändern. Sie können jedoch eine Kennung mit einer Konfiguration Ihrer Wahl erstellen.

So konfigurieren Sie einen Stream-Identifier mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Stream-ID zu konfigurieren und die Konfiguration zu überprüfen:

- `add stream identifier <name> <selectorName> [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]`
- `show stream identifier <name>`

Beispiel

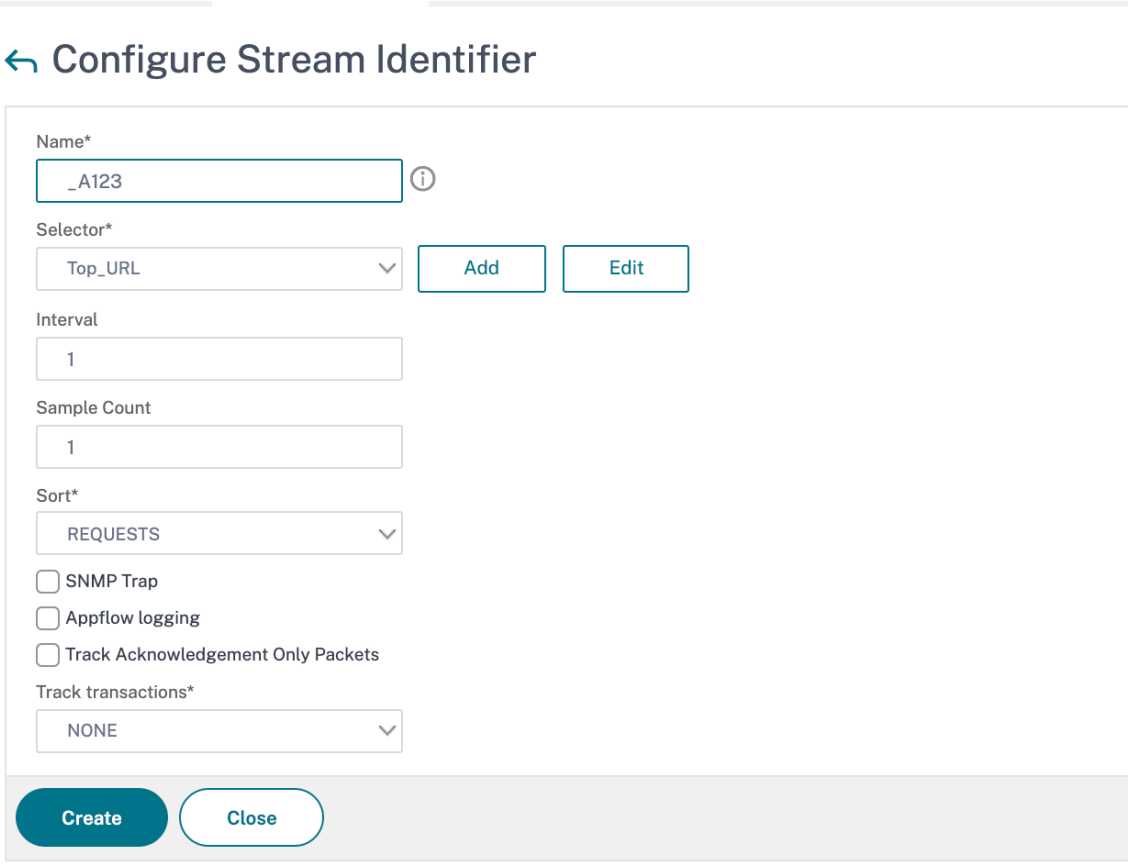
```
1 > add stream identifier myidentifier Top_URL -interval 10 -sampleCount
     100
2  Done
```



```
<!--NeedCopy-->
```

So konfigurieren Sie einen Stream-Identifier mithilfe der GUI

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Stream Identifiers**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um einen Stream-Identifier zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine Stream-ID zu ändern, wählen Sie die Kennung aus und klicken Sie dann auf **Bearbeiten**.
3. Stellen Sie auf der Seite „Stream-Identifier konfigurieren“ die folgenden Parameter ein:
   - Name
   - Selektor
   - Intervall
   - Anzahl der Proben
   - Sortieren
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.



Statistiken anzeigen

August 19, 2021

Sie können die gesammelten Statistiken im tabellarischen Format in der Befehlszeilenschnittstelle und im grafischen Format im Konfigurationsprogramm anzeigen.

Die folgende Tabelle beschreibt die gesammelten Statistiken:

Statistik	Spaltenname in der Ausgabe des Befehls <identifier name> stat stream identifier	Beschreibung
Anzahl der Anfragen	**Req**	Die Anzahl der Anforderungen, für die Datensätze in den letzten <interval> Minuten erstellt wurden.

Statistik	Spaltenname in der Ausgabe des Befehls <identifier name> stat stream identifier	Beschreibung
Verbraucht Bandbreite	**BandW**	Die Gesamtbandbreite, die von den Anforderungen belegt wurde, die in der letzten<interval> Anzahl von Minuten empfangen wurden. Die Gesamtbandbreite einer Anforderung ist die Bandbreite, die von der Anforderung und ihrer Antwort belegt wird. Der Wert wird auf den nächst höheren oder nächstniedrigeren Ganzzahlwert abgerundet. Es kann also geringfügig vom erwarteten Wert abweichen. Wenn der gesamte Bandbreitenverbrauch einer Anfrage beispielsweise 2,2 KB beträgt. Eine Instanz der Anforderung könnte angezeigt werden, dass sie 2 KB verbraucht hat. Es kann angezeigt werden, dass zwei Instanzen 4 KB verbraucht haben, aber drei Instanzen könnten angezeigt werden, dass sie 7 KB verbraucht haben.
Response time	**RspTime**	Die durchschnittliche Antwortzeit für alle Anforderungen, die in der letzten <interval> Anzahl von Minuten empfangen wurden.

Statistik	Spaltenname in der Ausgabe des Befehls <identifier name> stat stream identifier	Beschreibung
Gleichzeitige Verbindungen	**Conn**	Die Gesamtanzahl gleichzeitiger Verbindungen, die derzeit geöffnet sind.

So zeigen Sie die statistischen Daten an, die über die Befehlszeile für einen Stream-Bezeichner erfasst wurden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy <sortBy> [<sortOrder>]
```

Beispiele

Beispiel 1 sortiert die Ausgabe in der BandW-Spalte in absteigender Reihenfolge. Beispiel 2 sortiert die Ausgabe in Beispiel 1, in der Spalte **Req** und in aufsteigender Reihenfolge

Beispiel 1

```
> stat stream identifier myidentifier -sortBy BandW Descending -fullValues
Stream Session statistics
                    Req                BandW
User1               508               125924
User2              5020                12692
User3              2025                 4316

                RspTime                Conn
User1              5694                   0
User2               109                   0
User3                 3                   0
 Done
<!--NeedCopy-->
```

Beispiel 2

```
> stat stream identifier myidentifier -sortBy Req Ascending -fullValues
```

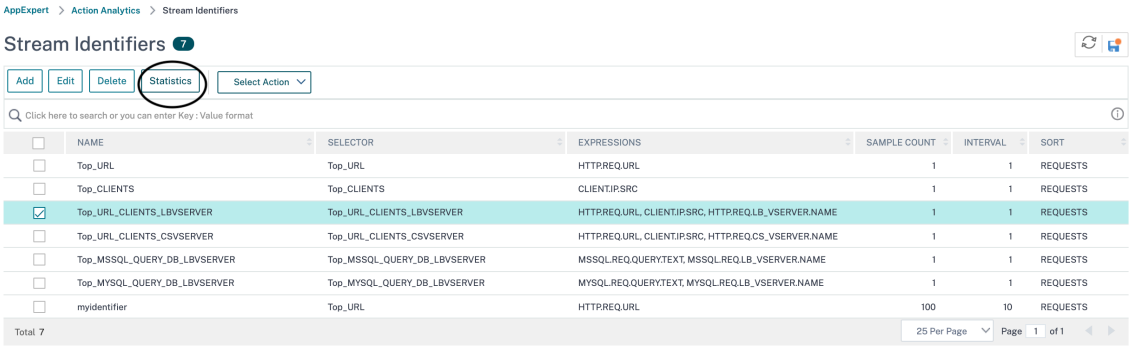


```
Stream Session statistics
                     Req                  BandW
User1                508                 125924
User3               2025                   4316
User2               5020                  12692

                  RspTime                  Conn
User1                5694                     0
User3                   3                     0
User2                 109                     0
 Done
<!--NeedCopy-->
```

So zeigen Sie die statistischen Daten an, die für einen Stream-Bezeichner mit der GUI erfasst wurden

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Stream Identifiers**.
2. Wählen Sie den Stream-Bezeichner aus, dessen Sitzungen Sie anzeigen möchten, und klicken Sie dann auf Statistiken. Informationen dazu, wie Sie die Ausgabe anhand der für verschiedene Selektorausdrücke gesammelten Werte gruppieren können.



Gruppieren von Datensätzen nach Attributwerten

January 19, 2021

Statistische Informationen wie die Anzahl der Zugriffe auf eine bestimmte URL insgesamt und pro Client sowie die Gesamtzahl der GET und POST-Anfragen pro Client können wertvolle Einblicke in die Frage geben, ob Ihre Ressourcen erweitert werden müssen, um den Bedarf zu erfüllen oder für die Lieferung optimiert zu werden. Um solche Statistiken zu erhalten, müssen Sie einen entsprechenden Satz von Selektorausdrücken verwenden und dann den Pattern-Parameter im Befehl stat stream identifier verwenden. Die Gruppierung basiert auf dem Muster, das im Befehl angegeben ist. Die Gruppierung kann gleichzeitig für die Werte mehrerer Ausdrücke durchgeführt werden.

In der Befehlszeilenschnittstelle können Sie die Ausgabe anhand von Mustern Ihrer Wahl gruppieren. Im Konfigurationsprogramm hängt das Muster von den Auswahlmöglichkeiten ab, die Sie beim Drill-down durch die Werte verschiedener Selektorausdrücke treffen. Betrachten Sie beispielsweise einen Selektor, der die Ausdrücke `HTTP.REQ.URL`, `CLIENT.IP.SRC` und `HTTP.REQ.LB_VSERVER.NAME` in dieser Reihenfolge hat. Auf der Statistik-Homepage werden Symbole für jeden dieser Ausdrücke angezeigt. Wenn Sie auf das Symbol für klicken `CLIENT.IP.SRC`, basiert die Ausgabe auf den Mustern *?*. Die Ausgabe zeigt Statistiken für jede Client-IP-Adresse an. Wenn Sie auf eine IP-Adresse klicken, basiert die Ausgabe auf den Muster* `<IP address>` ? und? `<IP address>` * wobei die IP-Adresse `<IP address>` ist, die Sie ausgewählt haben. Wenn Sie in der resultierenden Ausgabe auf eine URL klicken, wird das verwendete Muster verwendet`<URL> <IP address> ?`.

So gruppieren Sie die Datensätze anhand der Werte von Selektorausdrücken mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Datensätze anhand eines Selektorausdrucks zu gruppieren:

```
stat stream identifier <name> [<pattern> ...]
```

In den folgenden Beispielen wird ein anderes Muster verwendet, um die Auswirkungen des Musters auf die Ausgabe des Befehls stat stream identifier zu demonstrieren. Die Selektorausdrücke sind HTTP.REQ.URL und HTTP.REQ.HEADER (UserHeader) in dieser Reihenfolge. Die Anforderungen enthalten einen benutzerdefinierten Header, dessen Name UserHeader ist. Beachten Sie, dass sich in den Beispielen ein bestimmter statistischer Wert ändert, wie durch die Gruppierung bestimmt, aber die Summe der Werte für ein bestimmtes Feld bleibt gleich.

Beispiel 1

Im folgenden Befehl ist das verwendete Muster? ?. Die Appliance gruppiert die Ausgabe nach den Werten, die für beide Selektorausdrücke gesammelt wurden. Die Zeilenüberschriften bestehen aus den Ausdruckswerten, die durch ein Fragezeichen (?) getrennt sind. Die Zeile mit dem Header /mysite/mypage1.html? Ed zeigt Statistiken für Anfragen des Benutzers Ed für die URL /mysite/mypage1.html.

> **Hinweis:**
>
> Sie müssen sicherstellen, dass Sie den folgenden Befehl mit “?”statt “?”. Beispiel: Wenn Selektor einen Ausdruck verwendet - client.ip.src und client.tcp.srcport. Der Stat-Befehl, um die Ausgabe auf den für den Selektor gesammelten Werten zu gruppieren, ist ‘stat stream identifier myidentifier? ? -FullValues’ wie unten angegeben.

```
1 > stat stream identifier myidentifier ? ? -fullValues
2 Stream Session statistics
3                                          Req                 BandW
```



```
/mysite/mypage2.html?Grace                    1                    2553
/mysite/mypage1.html?Grace                    2                       4
/mysite/mypage1.html?Ed                       8                      16
/mysite/mypage2.html?Joe                      1                    2554
/mysite/mypage1.html?Joe                      5                      10
/mysite/?Joe                                  1                       4

                                         RspTime                    Conn
/mysite/mypage2.html?Grace                    0                       0
/mysite/mypage1.html?Grace                    0                       0
/mysite/mypage1.html?Ed                       0                       0
/mysite/mypage2.html?Joe                      0                       0
/mysite/mypage1.html?Joe                      0                       0
/mysite/?Joe                                  6                       0
 Done
<!--NeedCopy-->
```

Beispiel 2

Im folgenden Befehl ist das verwendete Muster *?. Die Appliance gruppiert die Ausgabe nach den Werten, die für den zweiten Ausdruck HTTP.REQ.HEADER (UserHeader) gesammelt wurden. Die Zeilen zeigen Statistiken für alle Anfragen von Benutzern Grace, Ed und Joe an.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den folgenden Befehl mit “?”statt “?”.

```
> stat stream identifier myidentifier * ?
Stream Session statistics
                    Req     BandW  RspTime     Conn
Grace                 3      2557        0        0
Ed                    8        16        0        0
Joe                   7      2568        6        0
 Done
<!--NeedCopy-->
```

Beispiel 3

Im folgenden Befehl ist das verwendete Muster? *, das ist das Standardmuster. Die Ausgabe wird nach den Werten gruppiert, die für den ersten Selektorausdruck gesammelt wurden. Jede Zeile zeigt Statistiken für eine URL an.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den folgenden Befehl mit “?”statt “?”.

```
> stat stream identifier myidentifier ? * -fullValues
```



```
Stream Session statistics

                                        Req                 BandW
/mysite/mypage2.html                      2                  5107
/mysite/mypage1.html                     15                    30
/mysite/                                  1                     4

                                     RspTime                 Conn
/mysite/mypage2.html                      0                     0
/mysite/mypage1.html                      0                     0
/mysite/                                  6                     0
 Done
<!--NeedCopy-->
```

Beispiel 4

Im folgenden Befehl wird das verwendete Muster verwendet `* *`. Die Appliance zeigt einen Satz kollektiver Statistiken für alle empfangenen Anforderungen ohne Zeilentitel an.

```
> stat stream identifier myidentifier * *
Stream Session statistics
                  Req    BandW  RspTime     Conn
                   18     5141        6        0
 Done
<!--NeedCopy-->
```

Beispiel 5

Im folgenden Befehl lautet das Muster /mysite/mypage1.html *. Die Appliance zeigt einen Satz kollektiver Statistiken für alle Anfragen an, die für die URL /mysite/mypage1.html empfangen wurden, ohne Zeilentitel.

```
> stat stream identifier myidentifier /mysite/mypage1.html *
Stream Session statistics
                  Req    BandW  RspTime     Conn
                   15       30        0        0
 Done
<!--NeedCopy-->
```

Löschen einer Stream-Sitzung

August 19, 2021

Sie können alle Datensätze leeren, die für einen Stream-Bezeichner gesammelt wurden.

So löschen Sie eine Stream-Sitzung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Streamsitzung zu löschen und die Ergebnisse zu überprüfen:

- clear stream session
- stat stream identifier

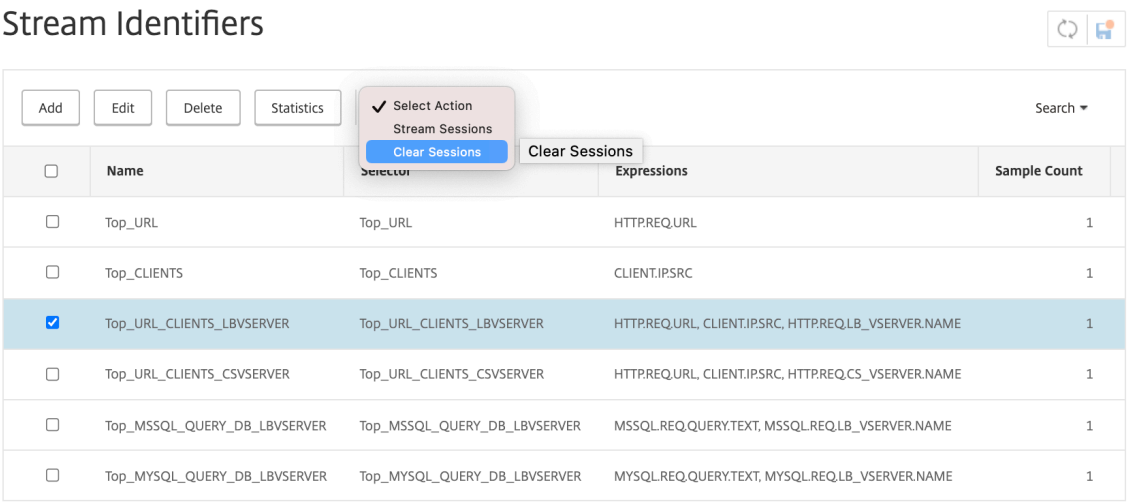
Beispiel

In diesem Beispiel wird zuerst der Befehl stat stream identifier verwendet, sodass ein Vergleich mit dem Befehl stat stream identifier durchgeführt werden kann, der zum Überprüfen des Ergebnisses des Befehls clear stream session verwendet wird.

```
>stat stream identifier myidentifier
Stream Session statistics
                  Req    BandW  RspTime     Conn
/aed....html        2        0        0        0
/                 636      303       12        0
 Done
>clear stream session myidentifier
 Done
>stat stream identifier myidentifier
 Done
<!--NeedCopy-->
```

So löschen Sie eine Stream-Sitzung mit der GUI

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Stream Identifiers**.
2. Wählen Sie den Stream-Bezeichner aus, dessen Sitzungen Sie löschen möchten, und klicken Sie dann auf **Sitzungen löschen**.



Richtlinie zur Optimierung des Datenverkehrs konfigurieren

May 11, 2023

Um das Selektor-Identifier-Paar in Ihrer Action-Analytics-Konfiguration in Kraft zu setzen, müssen Sie das Paar mit dem Punkt im Verkehrsfluss verknüpfen, an dem Sie Statistiken sammeln möchten. Sie können dies tun, indem Sie eine erweiterte Richtlinie konfigurieren und in der Richtlinienregel auf die Stream-ID verweisen. Sie können Komprimierungsrichtlinien, Caching-Richtlinien, Rewriterichtlinien, Anwendungsfirewall-Richtlinien, Responder-Richtlinien und alle anderen Richtlinien verwenden, deren Aktion auf einem booleschen Ausdruck basiert.

Die Action Analytics-Funktion führt eine Reihe von erweiterten Richtlinienausdrücken und Funktionen zum Sammeln und Auswerten von Daten ein. Der Ausdruck `ANALYTICS.STREAM(<identifier_name>)` wird verwendet, um auf den Bezeichner zu verweisen, den Sie verwenden möchten. Der Ausdruck COLLECT_STATS wird verwendet, um statistische Daten zu sammeln. Funktionen wie `IS_TOP(<uint>)` und `IS_TOP_FREQUENTS(<uint>)` werden verwendet, um automatische Entscheidungen zur Verkehrsoptimierung in Echtzeit zu treffen.

- **IS_TOP(<number>).** Findet, ob sich ein bestimmtes Objekt an der Spitze <number>von Elementen befindet. Zum Beispiel ist das Element unter den Top 10 Elementen. Wenn mehrere Elemente die Anzahl haben, werden sie als ähnlicher Natur betrachtet. Die Sortierfunktion muss eingeschaltet sein, um eine Undef-Bedingung zu vermeiden.
- **IS_TOP_FREQUENTS(<frequency>).** Findet, ob ein bestimmtes Objekt oben in dem mit <frequency> angegebenen Häufigkeitswert unter den Elementen im Top-Bereich ist. Zum Beispiel wird das Element unter den obersten 50% aller Top-Elemente beibehalten. Elemente mit denselben Werten werden als ähnlicher Natur angesehen. Die Sortierfunktion muss eingeschaltet sein, um eine Undef-Bedingung zu vermeiden.

Es ist Ihre Richtlinienkonfiguration, die bestimmt, ob die NetScaler-Appliance nur Daten aus dem Datenverkehr sammeln oder auch eine Aktion ausführen darf. Wenn die Appliance nur statistische Daten sammeln muss, können Sie eine Richtlinie mit der Regel `ANALYTICS.STREAM(<identifier_name>).COLLECT_STATS` und der Aktion NOOP konfigurieren. Die NOOP-Richtlinie muss die Richtlinie mit der höchsten Priorität am Bindepunkt sein. Diese Richtlinie ist ausreichend, wenn Sie nur Statistiken sammeln. Entscheidungen zur Verkehrsoptimierung, z. B. was komprimiert oder zwischengespeichert werden soll, müssen auf einer manuellen, regelmäßigen Auswertung der statistischen Daten basieren.

Wenn die Appliance zusätzlich zum Sammeln von Statistiken auch eine Aktion für den Datenverkehr ausführen muss, müssen Sie den gotoPriorityExpression-Parameter der NOOP-Richtlinie so konfigurieren, dass eine andere Richtlinie mit der gewünschten Regel und Aktion nachträglich ausgewertet wird. Diese zweite Richtlinie muss eine Regel enthalten, die mit dem Präfix `ANALYTICS.STREAM(<identifier_name>)` beginnt, und eine Funktion, die die Daten auswertet.

Es folgt ein Beispiel für zwei Responder-Richtlinien, die global konfiguriert und gebunden sind. Die Richtlinie responder_stat_collection ermöglicht es der Appliance, Statistiken basierend auf dem Bezeichner myidentifier zu sammeln. Die Richtlinie responder_notify wertet die gesammelten Daten aus.

Beispiel

```
> add responder action send_notification respondwith '"You are in the Top 10 list for bandwidth consumption"'
 Done
> add responder policy responder_stat_collection' ANALYTICS.STREAM("myidentifier").COLLECT_STATS' NOOP
Done
> add responder policy responder_notify 'ANALYTICS.STREAM("myidentifier").BANDWIDTH.IS_TOP(10)' send_notification
 Done
> bind responder global responder_stat_collection 10 NEXT
 Done
> bind responder global responder_notify 20 END
 Done
<!--NeedCopy-->
```

So begrenzen Sie den Bandbreitenverbrauch pro Benutzer oder Client-Gerät

August 19, 2021

Ihre Website, Anwendung oder Datei-Hosting-Dienst verfügt über endliche Netzwerk- und Server-Ressourcen, um alle ihre Benutzer zu bedienen. Eine der wichtigsten Ressourcen ist die Bandbreite. Ein erheblicher Bandbreitenverbrauch durch nur eine Teilmenge der Benutzerbasis kann zu einer Netzwerküberlastung und einer geringeren Ressourcenverfügbarkeit für andere Benutzer führen. Um Netzwerküberlastung zu verhindern, müssen Sie möglicherweise den Bandbreitenverbrauch eines Clients einschränken, indem Sie temporäre Dienstverweigerungsmethoden verwenden, z. B. die Reaktion auf eine Clientanforderung mit einer HTML-Seite, wenn dieser einen vorkonfigurierten Bandbreitenwert über einen bestimmten Zeitraum vor der Anforderung überschritten hat.

Im Allgemeinen können Sie den Bandbreitenverbrauch entweder pro Clientgerät oder pro Benutzer regulieren. Dieser Anwendungsfall zeigt, wie Sie den Bandbreitenverbrauch pro Client über einen Zeitraum von einer Stunde auf 100 MB begrenzen können. Der Anwendungsfall zeigt auch, wie Sie den Bandbreitenverbrauch pro Benutzer über einen Zeitraum von einer Stunde auf 100 MB regeln können, indem Sie einen benutzerdefinierten Header verwenden, der den Benutzernamen bereitstellt. In beiden Fällen wird die Verfolgung des Bandbreitenverbrauchs über einen bewegten Zeitraum von einer Stunde erreicht, indem der Intervallparameter in der Stream-ID auf 60 Minuten gesetzt wird. Die Anwendungsfälle zeigen auch, wie Sie eine HTML-Seite importieren können, die an einen Client gesendet werden soll, der den Grenzwert überschritten hat. Das Importieren einer HTML-Seite vereinfacht nicht nur die Konfiguration der Responder-Aktion in diesen Anwendungsfällen, sondern vereinfacht auch die Konfiguration aller Responder-Aktionen, die dieselbe Antwort benötigen.

So beschränken Sie den Bandbreitenverbrauch pro Benutzer oder Clientgerät mit der Befehlszeilenschnittstelle

Führen Sie in der Befehlszeilenschnittstelle die folgenden Aufgaben aus, um Aktionsanalysen für die Begrenzung des Bandbreitenverbrauchs eines Clients oder Benutzers zu konfigurieren. Jeder Schritt enthält Beispielbefehle und deren Ausgabe.

1. **Richten Sie Ihre Lastausgleichskonfiguration ein.** Konfigurieren Sie den Lastenausgleich virtuellen Server mysitevip, und konfigurieren Sie dann alle Dienste, die Sie benötigen. Binden Sie die Dienste an den virtuellen Server. Im folgenden Beispiel werden zehn Dienste erstellt und die Dienste an mysitevip gebunden.

```
> add lb vserver mysitevip HTTP 192.0.2.17 80
 Done
> add service service[1-10] 192.0.2.[240-249] HTTP 80
service "service1" added
service "service2" added
service "service3" added
.
.
.
service "service10" added
 Done
```



```
> bind lb vserver vserver1 service[1-10]
service "service1" bound
service "service2" bound
service "service3" bound
.
.
.
service "service10" bound
 Done
<!--NeedCopy-->
```

2. **Konfigurieren Sie den Stream-Selektor.** Konfigurieren Sie einen der folgenden Stream-Selektoren:

   - Um den Bandbreitenverbrauch pro Client zu begrenzen, konfigurieren Sie einen Stream-Selektor, der die Client-IP-Adresse identifiziert.

     ```
     > add stream selector myselector CLIENT.IP.SRC
      Done
     <!--NeedCopy-->
     ```

   - Um den Bandbreitenverbrauch pro Benutzer auf der Grundlage des Wertes eines Anforderungs-Headers, der den Benutzernamen bereitstellt, zu begrenzen, konfigurieren Sie einen Stream-Selektor, der den Header identifiziert. Im folgenden Beispiel lautet der Name der Kopfzeile UserHeader.

     ```
     > add stream selector myselector HTTP.REQ.HEADER( “UserHeader
        ” )
      Done
     <!--NeedCopy-->
     ```

3. **Konfigurieren Sie einen Stream-Bezeichner.** Konfigurieren Sie einen Stream-Bezeichner, der den Stream-Selektor verwendet. Stellen Sie den Intervallparameter auf 60 Minuten ein.

   ```
   > add stream identifier myidentifier myselector -interval 60 -
      sampleCount 1 -sort BANDWIDTH
    Done
   <!--NeedCopy-->
   ```

4. **Konfigurieren Sie die Responderaktion.** Importieren Sie die HTML-Seite, die Sie an Benutzer oder Clients senden möchten, die das Bandbreitenverbrauchslimit überschritten haben, und verwenden Sie dann die Seite in Responderaktion crossed_limits.

   ```
   > import responder htmlpage http://.1.1.1/stdpages/wait.html
      crossed-limits.html
   ```



```
2 This operation may take some time, Please wait...
3
4  Done
5 > add responder action crossed_limits respondwithhtmlpage crossed-
     limits.html
6  Done
7 <!--NeedCopy-->
```

5. **Konfigurieren Sie die Responder-Richtlinien.** Konfigurieren Sie die Responderrichtlinie myrespol1 mit der Regel ANALYTICS.STREAM (myidentifier) .COLLECT_STATS und der Aktion NOOP. Konfigurieren Sie dann die Richtlinie myrespol2, um zu bestimmen, ob ein Client oder Benutzer die Grenze von 100 MB überschritten hat. Die Richtlinie myrespol2 ist mit der Responderaktion crossed_limits konfiguriert.

```
1 > add responder policy myrespol1 'ANALYTICS.STREAM("myidentifier")
     .COLLECT_STATS' NOOP
2  Done
3 > add responder policy myrespol2 'ANALYTICS.STREAM("myidentifier")
     .BANDWIDTH.GT(104857600)' crossed_limits
4  Done
5 <!--NeedCopy-->
```

6. **Binden Sie die Responderrichtlinien an den virtuellen Lastausgleichsserver.** Die Richtlinie myrespol1, die nur statistische Daten sammelt, muss die höhere Priorität und einen GOTO-Ausdruck von NEXT haben.

```
1 > bind lb vserver mysitevip -policyName myrespol1 -priority 1 -
     gotoPriorityExpression NEXT
2  Done
3 > bind lb vserver mysitevip -policyName myrespol2 -priority 2 -
     gotoPriorityExpression END
4  Done
5 <!--NeedCopy-->
```

7. **Testen Sie die Konfiguration.** Testen Sie die Konfiguration, indem Sie HTTP-Testanforderungen von mehreren Clients oder Benutzern an den virtuellen Lastausgleichsserver senden und mithilfe des Befehls stat stream identifier die Statistiken anzeigen, die für den angegebenen Bezeichner gesammelt werden. Die folgende Ausgabe zeigt Statistiken für Clients an.

```
1 > stat stream identifier myidentifier -sortBy BandW  - fullValues
2 Stream Session statistics
3                            Req           BandW
4 192.0.2.30                 5000          3761
5 192.0.2.31                 29            2602
```



```
192.0.2.32                25              51

                          RspTime         Conn
192.0.2.30                2               0
192.0.2.31                0               0
192.0.2.32                0               0
 Done
>
<!--NeedCopy-->
```

AppExpert Anwendungen

May 11, 2023

> **Warnung**
>
> Die Funktionalität der Anwendungsvorlage ist veraltet. Als Alternative können Sie StyleBooks verwenden. Weitere Informationen finden Sie unter StyleBooks und Web Application Firewall StyleBook.

Eine AppExpert-Anwendung ist eine Sammlung von Konfigurationen, die Sie auf der NetScaler-Appliance einrichten. Die Verwaltung von AppExpert-Anwendungen wird durch eine GUI (GUI) vereinfacht, mit der Sie Teilmengen des Anwendungsverkehrs und eine bestimmte Reihe von Sicherheits- und Optimierungsrichtlinien für die Verarbeitung jeder Verkehrsuntermenge angeben können. Außerdem konsolidiert es Bereitstellungsschritte in einer Ansicht, sodass Sie schnell Ziel-IP-Adressen für Clients konfigurieren und Hostserver angeben können.

Nachdem die AppExpert Anwendung eingerichtet wurde, müssen Sie überprüfen, ob die Anwendung ordnungsgemäß funktioniert. Bei Bedarf können Sie die Konfiguration an Ihre Anforderungen anpassen.

In regelmäßigen Abständen können Sie die Konfiguration überprüfen und überwachen, indem Sie die Zähler für verschiedene Anwendungskomponenten, Statistiken und den Application Visualizer anzeigen. Sie können auch Authentifizierungs-, Autorisierungs- und Überwachungsrichtlinien (Authentifizierung, Autorisierung und Überwachung) für die Anwendung konfigurieren.

AppExpert Anwendungsterminologie

Im Folgenden werden die in der AppExpert-Anwendungsfunktion verwendeten Begriffe und die Beschreibungen der Entitäten aufgeführt, für die die Begriffe verwendet werden:

Öffentlicher Endpunkt. Die Kombination aus IP-Adresse und Port, mit der die NetScaler-Appliance Clientanforderungen für die zugehörige Webanwendung empfängt. Ein öffentlicher Endpunkt kann

so konfiguriert werden, dass er entweder HTTP- oder sicheren HTTP (HTTPS) -Verkehr empfängt. Alle Clientanfragen für die Webanwendung müssen an einen öffentlichen Endpunkt gesendet werden. Einer AppExpert-Anwendung können mehrere Endpunkte zugewiesen werden.

Einheit der Anwendung. Eine AppExpert-Anwendungseinheit, die eine Teilmenge des Webanwendungsverkehrs verarbeitet und eine Reihe von Diensten ausgleicht, die den zugehörigen Inhalt hosten. Die Teilmenge des Datenverkehrs, die eine Anwendungseinheit verwalten muss, wird durch eine Regel definiert. Jede Anwendungseinheit definiert auch ihre eigenen Richtlinien zur Verkehrsoptimierung und Sicherheit für die von ihr verwalteten Anfragen und Antworten. Die mit diesen Richtlinien verbundenen NetScaler-Dienste sind Kompression, Caching, Rewrite, Responder und Anwendungsfirewall.

Standardmäßig enthält jede AppExpert-Anwendung mit mindestens einer Anwendungseinheit eine Standardanwendungseinheit, die nicht gelöscht werden kann. Die Standardanwendungseinheit ist keiner Regel zur Identifizierung von Anforderungen zugeordnet und wird immer zuletzt in der Reihenfolge der Anwendungseinheiten platziert. Es definiert eine Reihe von Richtlinien für die Verarbeitung von Anfragen, die nicht mit den Regeln übereinstimmen, die für die anderen Anwendungseinheiten konfiguriert sind. Damit wird sichergestellt, dass alle Kundenanfragen bearbeitet werden.

Bedienung. Die Kombination aus der IP-Adresse des Servers, der die Webanwendungsinstanz hostet, und dem Port, dem die Anwendung auf dem Server zugeordnet ist, im Format `\<IP address\>:\<Port\>`. Eine Webanwendung, die viele Anfragen erfüllt, wird auf mehreren Servern gehostet. Jeder Server soll eine Instanz der Webanwendung hosten, und jede Instanz der Webanwendung wird durch einen Dienst auf der NetScaler-Appliance dargestellt.

Regel der Anwendungseinheit. Erweiterter Richtlinienausdruck, der die Eigenschaften einer Verkehrsuntermenge für eine Anwendungseinheit definiert. Die folgende Beispielregel ist ein erweiterter Richtlinienausdruck, der eine Verkehrsuntermenge identifiziert, die aus vier Imagetypen besteht:

```
HTTP.REQ.URL.SUFFIX.EQ("bmp")|| HTTP.REQ.URL.SUFFIX.EQ("gif")|| HTTP.REQ.
URL.SUFFIX.EQ("png")|| HTTP.REQ.URL.SUFFIX.EQ("jpg")
```

Weitere Informationen zu erweiterten Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

Teilmenge des Datenverkehrs. Eine Reihe von Kundenanfragen, die eine gemeinsame Reihe von Verkehrsoptimierungs- und Sicherheitsrichtlinien erfordern. Eine Datenverkehrsuntermenge wird von einer Anwendungseinheit verwaltet und durch eine Regel definiert.

So funktioniert die AppExpert Anwendung

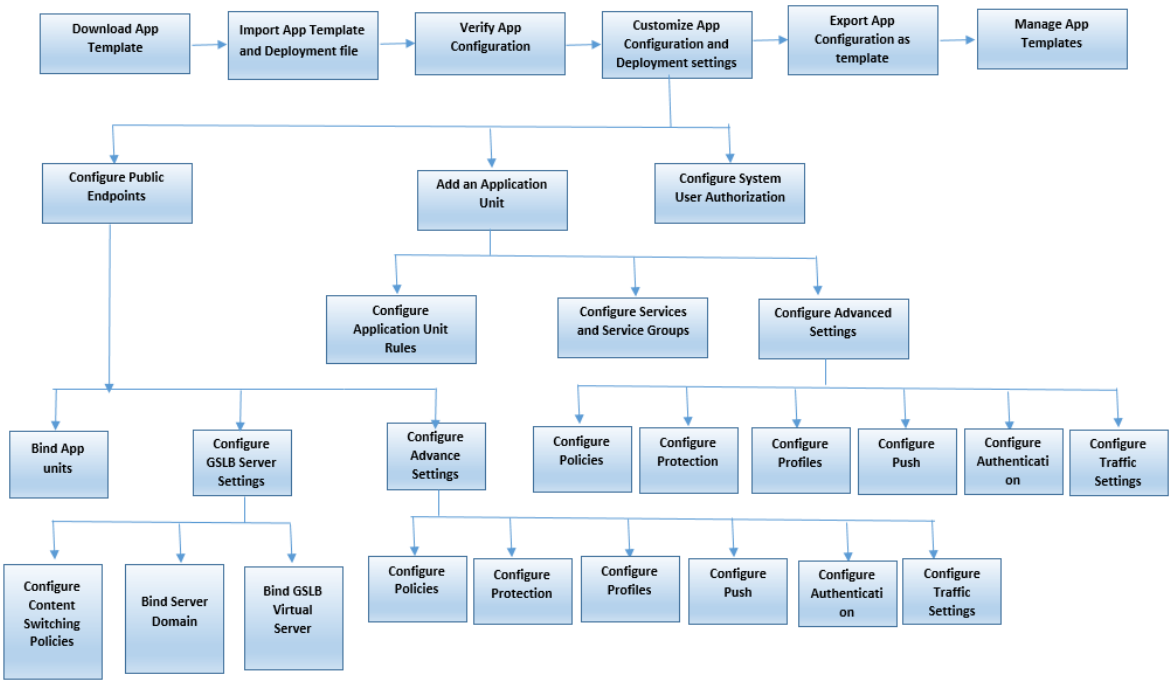
May 11, 2023

Wenn der Endpunkt eine Client-Anfrage erhält, wertet die NetScaler-Appliance die Anfrage anhand der Regel aus, die für die oberste Anwendungseinheit konfiguriert ist. Wenn die Anforderung diese Regel erfüllt, wird die Anforderung von den Richtlinien verarbeitet, die für die Anwendungseinheit konfiguriert sind, und dann an einen Dienst weitergeleitet. Die Wahl des Dienstes hängt davon ab, welche Dienste für die Anwendung konfiguriert sind, und von Einstellungen wie dem Load Balancing-Algorithmus und der Persistenzmethode, die für die Anwendungseinheit konfiguriert sind.

Wenn die Anforderung die Regel nicht erfüllt, wird die Anforderung anhand der Regel für die nächst oberste Anwendungseinheit ausgewertet. In dieser Reihenfolge wird die Anforderung anhand jeder Anwendungseinheitenregel ausgewertet, bis die Anforderung eine Regel erfüllt. Wenn die Anforderung keine der konfigurierten Regeln erfüllt, wird sie von der Standardanwendungseinheit verarbeitet, die immer die letzte Anwendungseinheit ist.

Sie können mehrere öffentliche Endpunkte für eine AppExpert-Anwendung konfigurieren. In einer solchen Konfiguration verarbeitet jede Anwendungseinheit standardmäßig Anforderungen, die von allen öffentlichen Endpunkten empfangen werden, und gleicht alle Dienste aus, die für die Anwendung konfiguriert sind. Sie können jedoch angeben, dass eine Anwendungseinheit den Datenverkehr nur von einer Teilmenge der öffentlichen Endpunkte verarbeitet und nur eine Teilmenge der Dienste ausgleicht, die für die AppExpert-Anwendung konfiguriert sind.

Das folgende Flussdiagramm zeigt die AppExpert Application-Ablaufsequenz für die Verwendung einer integrierten Anwendungsvorlage.



Wenn Sie lieber eine benutzerdefinierte Anwendung erstellen möchten, ohne eine Vorlage zu verwenden, gehen Sie wie folgt vor:

1. Erstellen Sie eine benutzerdefinierte Anwendung.
2. Konfiguration der Anwendungs- und Bereitstellungseinstellungen
3. Exportieren Sie die Konfiguration in neue Vorlagendateien (optional).
4. Importieren der Vorlagendateien in andere NetScaler-Appliances, die eine ähnliche AppExpert Anwendungskonfiguration erfordern

Konfiguration anpassen

May 11, 2023

Nachdem Sie überprüft haben, dass die AppExpert-Anwendung ordnungsgemäß funktioniert, können Sie die Konfiguration an Ihre Anforderungen anpassen.

Nachdem Sie überprüft haben, dass die AppExpert-Anwendungskonfiguration ordnungsgemäß funktioniert, können Sie die Anwendung und die Bereitstellungseinstellungen entsprechend Ihren Anforderungen konfigurieren. Wenn Sie eine Anwendungsvorlage und eine Bereitstellungsdatei importieren, füllt das System die Zielanwendung automatisch mit den verfügbaren Konfigurationseinstellungen (wie Anwendungseinheiten, Regeln für Anwendungseinheiten, Richtlinien, Persistenzeinstellungen, Load Balancing-Methoden, Profile und Verkehrseinstellungen). In dieser Anwendung können Sie Bereitstellungseinstellungen wie öffentliche Endpunkte, Dienste und Dienstgruppen für jede Traffic-Teilmenge konfigurieren. Wenn die AppExpert-Anwendung eine Traffic-Teilmenge verwalten soll, die nicht in der Vorlage enthalten ist, können Sie entweder eine Anwendungseinheit für eine Traffic-Teilmenge hinzufügen oder die vorhandene Anwendungseinheit ändern. Nachdem Sie die Konfiguration angepasst haben, können Sie auch die Reihenfolge der Auswertung für jede Traffic-Teilmenge angeben, die von der Anwendung verwaltet wird.

Die Konfiguration einer AppExpert Anwendung umfasst die folgenden Schritte:

1. Öffentliche Endpunkte konfigurieren
2. Anwendungseinheiten konfigurieren
3. Angeben der Reihenfolge der Auswertung
4. Anwendungskonfiguration mit Visualizer anzeigen

Sie können auch die Richtlinien konfigurieren, die die Vorlage bereitgestellt hat. Wenn die AppExpert Anwendungsvorlage keine Richtlinien für ein bestimmtes NetScaler Feature enthält, z. B. Rewrite oder Anwendungsfirewall, können Sie eigene Richtlinien konfigurieren.

Konfigurieren öffentlicher Endpunkte

June 21, 2022

Wenn Sie beim Import einer AppExpert-Anwendung keinen öffentlichen Endpunkt angegeben haben, können Sie öffentliche Endpunkte angeben, nachdem Sie die Anwendung erstellt haben. Sie können einen öffentlichen Endpunkt vom Typ HTTP und einen öffentlichen Endpunkt vom Typ HTTPS für Ihre AppExpert-Anwendung konfigurieren.

Wenn Endpunkte bereits für die Anwendung konfiguriert sind, können Sie Endpunkte von der AppExpert-Anwendung trennen und alle Endpunkte löschen, die Sie nicht mehr benötigen. Beachten Sie, dass, wenn Sie einen öffentlichen Endpunkt von der AppExpert-Anwendung trennen, der Endpunkt automatisch von der zugehörigen Anwendungseinheit getrennt wird, aber nicht aus dem System gelöscht wird.

So konfigurieren Sie öffentliche Endpunkte für eine AppExpert-Anwendung:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie öffentliche Endpoints konfigurieren möchten, und klicken Sie dann auf Bearbeiten.
3. Gehen Sie auf der Seite **Anwendungen** zum Abschnitt **Öffentliche Endpunkte** und klicken Sie auf das Bleistiftsymbol.
4. Stellen Sie im Schieberegler **Öffentliche Endpunkte** die folgenden Parameter ein.
    a) Typ des öffentlichen Endpunkts. Wählen Sie das Optionsfeld, um den Endpunkttyp zu definieren.
    b) Name. Name des öffentlichen Endpunkts.
    c) IP-Adresse. Die IP-Adresse des öffentlichen Endpunkts.
    d) Port. Portnummer des öffentlichen Endpunkts.
    e) Protokoll. Wählen Sie einen Protokolltyp als HTTP oder HTTPS aus.
5. Klicken Sie auf **Weiter.**
6. Wählen Sie im Abschnitt **Anwendungseinheiten** eine Anwendungseinheit aus der Liste aus.
7. Klicken Sie auf **Weiter**, um die Richtlinien und Serverdetails festzulegen.
8. Klicken Sie auf **OK** und dann auf Fertig.
9. Klicken Sie auf Schließen.

Weitere Informationen zu den Parametern im Dialogfeld " **Öffentliche Endpunkte konfigurieren** " finden Sie unter Content Switching.

Konfigurieren von Diensten und Dienstgruppen für eine Anwendungseinheit

June 21, 2022

Wenn Sie einen Dienst oder eine Dienstgruppe konfigurieren, ändern Sie entweder einen vorhandenen Dienst oder eine Dienstgruppe oder fügen der AppExpert-Anwendung neue Dienste hinzu. Sie fü-

gen Dienste oder Dienstgruppen hinzu, wenn Sie sie beim Importieren der Anwendungsvorlage nicht angegeben haben. Sie fügen auch Dienste und Dienstgruppen hinzu, wenn Sie die Anzahl der Server erhöhen, die Instanzen der Anwendung hosten. Sie können einen Dienst und eine Dienstgruppe für eine Anwendungseinheit erst konfigurieren, nachdem Sie den Dienst oder die Dienstgruppe für die AppExpert-Anwendung konfiguriert haben.

So konfigurieren Sie einen Dienst oder eine Dienstgruppe für die AppExpert-Anwendung:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung und klicken Sie dann auf **Bearbeiten.**
3. Wählen Sie auf der Seite **Anwendungen** eine Anwendungseinheit aus, und klicken Sie dann auf **Weiter**.
4. Gehen Sie im Abschnitt **Dienste und Dienstgruppen** wie folgt vor:
    a) Stellen Sie im Schieberegler Service Binding die folgenden Parameter ein.
        i. Service. Wählen Sie einen Load Balancing-Dienst aus der Liste aus oder erstellen Sie einen neuen Dienst.
        ii. Gewicht Geben Sie einen Gewichtswert für den Service an.
    b) Klicken Sie auf **Binden** und dann auf **Fertig.**
    c) Stellen Sie im Schieberegler ServiceGroup Binding die folgenden Parameter ein:
        i. Name der Dienstgruppe. Wählen Sie eine Lastausgleichsdienstgruppe aus, oder erstellen Sie eine neue Dienstgruppe.
        ii. Klicke auf **Binden** und dann auf **Fertig**.
    d) Klicken Sie auf **Fertig**.
5. Klicken Sie auf **Weiter**, um andere Konfigurationen festzulegen.

Erstellen von Anwendungseinheiten

June 21, 2022

Möglicherweise müssen Sie Anwendungseinheiten für Traffic-Teilmengen hinzufügen, die entweder spezifisch für Ihre Webanwendungsimplementierung sind oder nicht in der Vorlage definiert sind. Beim Erstellen einer Anwendungseinheit müssen Sie eine Regel für die Anwendungseinheit konfigurieren.

So erstellen Sie eine Anwendungseinheit für die AppExpert-Anwendung:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie eine Anwendungseinheit hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**.

3. Wechseln Sie auf der Seite **Anwendungen** zum Abschnitt **Anwendungseinheiten** und klicken Sie auf das **Stiftsymbol** .

So konfigurieren Sie Richtlinienausdrücke für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie eine Anwendungseinheit hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**.
3. Wechseln Sie auf der Seite **Anwendungen** zum Abschnitt **Anwendungseinheiten** und klicken Sie auf das Symbol **+**, um eine Unit zu erstellen und Richtlinienausdrücke hinzuzufügen.
4. Um das Format des neuen Ausdrucks anzugeben, führen Sie einen der folgenden Schritte aus:
   a) Um anzugeben, dass Sie einen Richtlinienausdruck im Feld Regel konfigurieren möchten, klicken Sie auf Klassische Syntax.
   b) Um anzugeben, dass Sie einen erweiterten Ausdruck im Feld Regel konfigurieren möchten, klicken Sie auf Erweiterte Richtlinie.
   c) Konfigurieren Sie im Feld Regel den Ausdruck.
5. Klicken Sie auf **OK**.

Konfigurieren von Regeln für Anwendungseinheiten

June 21, 2022

Möglicherweise möchten Sie eine Anwendungseinheitenregel so konfigurieren, dass bestimmte Arten von Datenverkehr eingeschlossen oder ausgeschlossen werden. Wenn Sie die Regel konfigurieren, können Sie auch die Syntax des Ausdrucks definieren.

So konfigurieren Sie eine Anwendungseinheitenregel:

1. Erweitern Sie im Navigationsbereich der GUI AppExpert, und klicken Sie dann auf **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendungseinheit, für die Sie die Regel ändern möchten, und klicken Sie dann auf **Öffnen**.
3. Gehen Sie im Dialogfeld Anwendungseinheit konfigurieren wie folgt vor:
   a) Um das Format des neuen Ausdrucks anzugeben, führen Sie einen der folgenden Schritte aus:
      - Um anzugeben, dass Sie einen erweiterten Richtlinienausdruck im Feld Regel konfigurieren möchten, klicken Sie auf **Klassische Syntax**.
      - Um im Feld Regel anzugeben, dass Sie einen erweiterten Ausdruck konfigurieren möchten, klicken Sie auf **Erweiterte Richtlinie**.
   b) Konfigurieren Sie im Feld Regel den Ausdruck.
4. Klicken Sie auf **OK**.

Konfigurieren von Richtlinien für Anwendungseinheiten

June 21, 2022

Für eine AppExpert-Anwendung können Sie Richtlinien für Komprimierung, Caching, Rewrite, Responder und Anwendungsfirewall konfigurieren. Die Vorlagen, die Sie von der Citrix Community-Website herunterladen, bieten Ihnen eine Reihe von Richtlinien, die die gängigsten Anwendungsverwaltungsanforderungen erfüllen. Möglicherweise möchten Sie diese Richtlinien verfeinern oder anpassen. Wenn der Satz von Richtlinien, die für eine bestimmte Anwendungseinheit bereitgestellt werden, keine Richtlinien für eine bestimmte Funktion enthält, können Sie Ihre eigenen Richtlinien für diese Funktion erstellen und binden.

Wenn Sie eine AppExpert-Anwendung erstellen, ohne eine Vorlage zu verwenden, müssen Sie alle Richtlinien konfigurieren, die die Webanwendung benötigt.

Die GUI verwendet verschiedene Symbole, um anzugeben, ob Richtlinien für eine Funktion konfiguriert sind oder nicht. Wenn für eine Anwendungseinheit eine Richtlinie für ein bestimmtes Feature konfiguriert ist, wird ein Symbol angezeigt, das die Funktion darstellt. Wenn beispielsweise eine Komprimierungsrichtlinie für eine Anwendungseinheit konfiguriert ist, wird in der Spalte Komprimierung für die Anwendungseinheit ein Komprimierungssymbol angezeigt. Für Funktionen, für die keine Richtlinie konfiguriert ist, wird ein Symbol mit einem Pluszeichen (+) angezeigt.

Hinweis: Wenn Sie Richtlinien für Anwendungseinheiten konfigurieren, müssen Sie möglicherweise Richtlinien und Ausdrücke konfigurieren, die entweder in der klassischen oder der erweiterten Richtlinie enthalten sind. Wenn Sie erweiterte Richtlinienrichtlinien konfigurieren, müssen Sie möglicherweise Parameter wie Gehe zu Ausdrücke angeben und Richtlinienbanken aufrufen.

Informationen zum Konfigurieren von Richtlinien und Ausdrücken in beiden Formaten finden Sie unter Richtlinien und Ausdrücke.

Komprimierungsrichtlinien konfigurieren

Sie können entweder klassische Richtlinien oder erweiterte Richtlinien verwenden, um die Komprimierung zu konfigurieren, aber Sie können die Komprimierungsrichtlinien beider Typen nicht an dieselbe Anwendungseinheit binden.

So konfigurieren Sie eine Komprimierungsrichtlinie für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich in der Zeile für die Anwendungseinheit, die Sie konfigurieren möchten, auf das Symbol in der Spalte Komprimierung.
3. Führen Sie im Dialogfeld Komprimierungsrichtlinien konfigurieren je nach den Konfigurationsaufgaben, die Sie ausführen möchten, eine oder mehrere der folgenden Aktionen aus:

- Klicken Sie auf Zu erweiterter Richtlinie wechseln, wenn Sie eine erweiterte Richtlinie zur Richtlinienkomprimierung konfigurieren möchten. Wenn Sie klassische Komprimierungsrichtlinien binden oder konfigurieren möchten und sich in der erweiterten Richtlinienansicht befinden, können Sie auf Zur klassischen Syntax wechseln klicken, um zur klassischen Richtlinienansicht zurückzukehren und gebundene klassische Richtlinien zu ändern oder neue klassische Komprimierungsrichtlinien zu erstellen und zu binden.
  Wichtig: Diese Einstellung legt auch fest, welche Richtlinien angezeigt werden, wenn Sie eine Richtlinie einfügen möchten. Wenn Sie sich beispielsweise in der Ansicht Erweiterte Richtlinie befinden und auf Richtlinie einfügen klicken, enthält die Liste, die in der Spalte Richtlinienname angezeigt wird, nur erweiterte Richtlinienrichtlinien. Sie können Richtlinien beider Typen nicht an eine Anwendungseinheit binden.
- Wenn Sie klassische Richtlinien konfigurieren möchten, klicken Sie entweder auf Anforderung oder Antwort, je nachdem, ob die Richtlinie zur Anforderungszeit oder zur Reaktionszeit ausgewertet werden soll.
  Sie können klassische Komprimierungsrichtlinien für Anforderungszeit und Reaktionszeit für eine Anwendungseinheit konfigurieren. Wenn nach der Auswertung aller Richtlinien für die Anforderungszeit keine Übereinstimmung gefunden wird, wertet die Appliance Reaktionszeitrichtlinien aus.
- Um eine Komprimierungsrichtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld Komprimierungsrichtlinie konfigurieren die Richtlinie, und klicken Sie dann auf OK.
  Informationen zum Ändern einer Komprimierungsrichtlinie finden Sie unter Komprimierung.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie aufheben.
- Um die einer Richtlinie zugewiesene Priorität zu ändern, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
- Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf Prioritäten neu generieren.
- Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen** und klicken Sie in der Liste, die in der Spalte Richtlinienname angezeigt wird, auf **Neue Richtlinie**. Konfigurieren Sie dann im Dialogfeld Komprimierungsrichtlinie erstellen die Richtlinie, und klicken Sie dann auf **Erstellen**.
  Informationen zum Ändern einer Komprimierungsrichtlinie finden Sie unter Komprimierung.
- Wenn Sie einen erweiterten Richtlinienausdruck konfigurieren, gehen Sie wie folgt vor:
  - Wählen Sie in der Spalte “Gehe-zu-Ausdruck” einen Gehe-zu-Ausdruck aus.
  - Geben Sie in der Spalte “Invoke” die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie als TRUE ausgewertet wird.

4. Klicken Sie auf **Änderungen übernehmen** und dann auf **Schließen**.

Konfigurieren von Caching-Richtlinien

Sie können nur erweiterte Richtlinienrichtlinien und Ausdrücke verwenden, um Caching-Richtlinien zu konfigurieren.

So konfigurieren Sie Caching-Richtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich in der Zeile für die Anwendungseinheit, die Sie konfigurieren möchten, auf das Symbol in der Spalte Caching.
3. Führen Sie im Dialogfeld Cache-Richtlinien konfigurieren je nach den Konfigurationsaufgaben, die Sie ausführen möchten, eine oder mehrere der folgenden Aktionen aus:
   - Klicken Sie entweder auf Anfrage oder Antwort, je nachdem, ob die Richtlinie zur Anforderungszeit oder zur Reaktionszeit ausgewertet werden soll.
     Sie können sowohl Caching-Richtlinien für die Anforderungszeit als auch für die Reaktionszeit für eine Anwendungseinheit konfigurieren. Wenn nach der Auswertung aller Richtlinien für die Anforderungszeit keine Übereinstimmung gefunden wird, wertet die Appliance Reaktionszeitrichtlinien aus.
   - Um eine Caching-Richtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld **Cache-Richtlinie konfigurieren** die Richtlinie, und klicken Sie dann auf **OK** .
     Informationen zum Ändern einer Caching-Richtlinie finden Sie unter Integriertes Caching.
   - Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie aufheben**.
   - Um die einer Richtlinie zugewiesene Priorität zu ändern, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
   - Um zugewiesene Prioritäten erneut zu generieren, klicken Sie auf **Prioritäten neu generieren**.
   - Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen** und klicken Sie in der Liste, die in der Spalte Richtlinienname angezeigt wird, auf **Neue Richtlinie**. Konfigurieren Sie dann im Dialogfeld **Cache-Richtlinie erstellen** die Richtlinie, und klicken Sie dann auf **Erstellen** .
     Informationen zum Ändern einer Caching-Richtlinie finden Sie unter Integriertes Caching.
   - Wählen Sie in der Spalte “Gehe-zu-Ausdruck” einen Gehe-zu-Ausdruck aus.
   - Geben Sie in der Spalte “Invoke” die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie als TRUE ausgewertet wird.
4. Klicken Sie auf **Änderungen übernehmen** und dann auf **Schließen**.

Konfigurieren von Rewriterichtlinien

Sie können nur erweiterte Richtlinienrichtlinien und Ausdrücke verwenden, um Richtlinien für das Rewrite zu konfigurieren.

So konfigurieren Sie Rewriterichtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich in der Zeile für die Anwendungseinheit, die Sie konfigurieren möchten, auf das Symbol in der Spalte Rewrite.
3. Führen Sie im Dialogfeld **Rewriterichtlinien konfigurieren** je nach den Konfigurationsaufgaben, die Sie ausführen möchten, eine oder mehrere der folgenden Aktionen aus:
   - Klicken Sie entweder auf Anfrage oder Antwort, je nachdem, ob die Richtlinie zur Anforderungszeit oder zur Reaktionszeit ausgewertet werden soll.
     Sie können sowohl Rewrite-Time als auch Reaktionszeit Rewriterichtlinien für eine Anwendungseinheit konfigurieren. Wenn nach der Auswertung aller Richtlinien für die Anforderungszeit keine Übereinstimmung gefunden wird, wertet die Appliance Reaktionszeitrichtlinien aus.
   - Um eine Rewriterichtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie ändern**. Ändern Sie dann im Dialogfeld Richtlinie neu schreiben konfigurieren die Richtlinie, und klicken Sie dann auf **OK**.
     Informationen zum Ändern einer Rewriterichtlinie finden Sie unter Rewrite.
   - Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie aufheben**.
   - Um die einer Richtlinie zugewiesene Priorität zu ändern, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
   - Um zugewiesene Prioritäten erneut zu generieren, klicken Sie auf **Prioritäten neu generieren**.
   - Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen**, und klicken Sie in der Liste, die in der Spalte **Richtlinienname** angezeigt wird, auf **Neue Richtlinie.** Konfigurieren Sie dann im Dialogfeld **Rewriterichtlinie erstellen** die Richtlinie, und klicken Sie dann auf **Erstellen** .
     Informationen zum Ändern einer Rewriterichtlinie finden Sie unter Rewrite.
   - Wählen Sie in der Spalte “Gehe-zu-Ausdruck” einen Gehe-zu-Ausdruck aus.
   - Geben Sie in der Spalte “Invoke” die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie als TRUE ausgewertet wird.
4. Klicken Sie auf **Änderungen übernehmen** und dann auf **Schließen**.

Konfigurieren von Responder-Richtlinien

Sie können nur erweiterte Richtlinienrichtlinien und Ausdrücke verwenden, um Responder-Richtlinien zu konfigurieren.

So konfigurieren Sie Responder-Richtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich in der Zeile für die Anwendungseinheit, die Sie konfigurieren möchten, auf das Symbol in der Spalte Responder.
3. Führen **Sie im Dialogfeld Responder-Richtlinien konfigurieren** je nach den Konfigurationsaufgaben, die Sie ausführen möchten, eine oder mehrere der folgenden Aktionen aus:
   - Um eine Filterrichtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie ändern**. Ändern Sie dann im Dialogfeld Responderrichtlinie konfigurieren die Richtlinie, und klicken Sie dann auf **OK**.
     Informationen zum Ändern einer Responder-Richtlinie finden Sie unter Responder.
   - Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie aufheben**.
   - Um die einer Richtlinie zugewiesene Priorität zu ändern, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
   - Um zugewiesene Prioritäten erneut zu generieren, klicken Sie auf **Prioritäten neu generieren**.
   - Um eine neue Richtlinie einzufügen, klicken Sie auf Richtlinie einfügen, und klicken Sie in der Liste, die in der Spalte Richtlinienname angezeigt wird, auf Neue Richtlinie. Konfigurieren Sie dann im Dialogfeld Responder-Richtlinie erstellen die Richtlinie, und klicken Sie dann auf Erstellen.
     Informationen zum Ändern einer Responder-Richtlinie finden Sie unter Responder.
   - Wählen Sie in der Spalte “Gehe-zu-Ausdruck” einen Gehe-zu-Ausdruck aus.
   - Geben Sie in der Spalte “Invoke” die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie als TRUE ausgewertet wird.
4. Klicken Sie auf **Änderungen übernehmen** und dann auf **Schließen**.

Konfigurieren von Anwendungsfirewall-Richtlinien

Sie können sowohl klassische als auch erweiterte Richtlinienrichtlinien und -ausdrücke für die Anwendungsfirewall konfigurieren. Wenn jedoch eine Richtlinie eines Typs bereits global oder an einen virtuellen Server gebunden ist, der auf der Appliance konfiguriert ist, können Sie eine Richtlinie des anderen Typs nicht an eine Anwendungseinheit binden. Wenn beispielsweise eine erweiterte Richtlinie bereits global oder an einen virtuellen Server gebunden ist, können Sie eine klassische Richtlinie nicht an eine Anwendungseinheit binden.

So konfigurieren Sie Anwendungsfirewall-Richtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich in der Zeile für die Anwendungseinheit, die Sie konfigurieren möchten, auf das Symbol in der Spalte **Anwendungsfirewall** .
3. Führen **Sie im Dialogfeld Anwendungsfirewall-Richtlinien konfigurieren** je nach den Konfigurationsaufgaben, die Sie ausführen möchten, eine oder mehrere der folgenden Aktionen aus:
   - Klicken Sie je nach Art des Ausdrucks, den Sie für die Anwendungsfirewall-Richtlinie konfigurieren möchten, entweder auf Klassischer Ausdruck oder auf Erweiterter Ausdruck.
     Wichtig: Diese Einstellung legt auch fest, welche Richtlinien angezeigt werden, wenn Sie eine Richtlinie einfügen möchten. Wenn Sie beispielsweise Erweiterter Ausdruck auswählen und auf **Richtlinie einfügen**klicken, enthält die Liste, die in der Spalte **Richtlinienname** angezeigt wird, nur erweiterte Richtlinienrichtlinien. Sie können Richtlinien beider Typen nicht an eine Anwendungseinheit binden. Diese Option ist nicht verfügbar, wenn eine Richtlinie eines Typs bereits global oder an einen virtuellen Server gebunden ist.
   - Um eine Anwendungsfirewall-Richtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld Anwendungsfirewall Richtlinie konfigurieren die Richtlinie, und klicken Sie dann auf OK.
     Informationen zum Ändern einer Anwendungs-Firewall-Richtlinie finden Sie unter Richtlinien.
   - Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie aufheben.
   - Um die einer Richtlinie zugewiesene Priorität zu ändern, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
   - Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf Prioritäten neu generieren.
   - Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen** und klicken Sie in der Liste, die in der Spalte **Richtlinienname** angezeigt wird, auf Neue Richtlinie. Konfigurieren Sie dann im Dialogfeld **Anwendungs-Firewall-Richtlinie erstellen** die Richtlinie, und klicken Sie dann auf **Erstellen** .
     Informationen zum Ändern einer Anwendungs-Firewall-Richtlinie finden Sie unter Richtlinien.
4. Klicken Sie auf **Änderungen übernehmen** und dann auf **Schließen**.

Anwendungseinheiten konfigurieren

May 11, 2023

So konfigurieren Sie eine Anwendungseinheit mit der GUI:

1. Navigieren Sie zum Abschnitt **AppExpert** > **Applications> Applications Unit** und klicken Sie dann auf das Plus-Symbol, um eine neue Anwendungseinheit für eine Traffic-Teilmenge hinzuzufügen.
2. Stellen Sie im Schieberegler **Anwendungseinheit** die folgenden Parameter ein:

   - Name
   - Ausdruck

   Sie können einen Ausdruck einfügen, indem Sie die Ausdruckskomponenten entweder manuell hinzufügen oder den Link Ausdrucks-Editor verwenden. Um einen Ausdruck manuell hinzuzufügen, geben Sie eine Selektorkomponente ein, und geben Sie dann einen Punkt (.) ein, um eine Liste anzuzeigen, aus der Sie die nächste Komponente auswählen können. Geben Sie beispielsweise HTTP und dann einen Punkt ein. Ein Dropdown-Menü wird angezeigt. Der Inhalt dieses Menüs enthält die Keywords, die dem ursprünglichen Keyword folgen können, das Sie eingegeben haben. Wählen Sie im Drop-down-Menü eine Komponente aus. Das Textfeld Ausdruck* zeigt jetzt die Komponenten an, die Sie dem Ausdruck hinzugefügt haben (z. B. HTTP.REQ). Fügen Sie weitere Komponenten hinzu, bis der vollständige Ausdruck gebildet ist.

   Wenn Sie Unterstützung beim Erstellen des Ausdrucks bevorzugen, können Sie den Link Ausdrucks-Editor verwenden. Auf der Seite Ausdrucks-Editor können Sie einen Ausdruck erstellen, indem Sie Komponenten aus den Dropdown-Feldern auswählen. Wählen Sie die Komponenten aus und klicken Sie auf Fertig, um den Ausdruck auf der Seite Anwendungseinheit einzufügen.
3. Klicken Sie auf **Weiter**, um Dienste und Dienstgruppen zu binden.
4. Klicken Sie auf den Abschnitt **Dienst**, um einen virtuellen Dienst auszuwählen oder hinzuzufügen und ihn an die Anwendungseinheit zu binden.
5. Klicken Sie auf **Fortfahren** und dann auf den Abschnitt **Dienstgruppe**, um eine virtuelle Dienstgruppe auszuwählen oder hinzuzufügen und sie an die Anwendungseinheit zu binden.
6. Klicken Sie auf **Bind** and **Continue**, um erweiterte Einstellungen (wie Richtlinien, Methode, Persistenz, Schutz, Profile, Push, Authentifizierung und Verkehrseinstellungen) für die Anwendungseinheit zu konfigurieren.
7. Klicken Sie in jedem Abschnitt auf das **Pluszeichen**, um die Konfigurationsparameter festzulegen.
8. Klicke auf **OK** und dann auf **Fertig**.

So bearbeiten Sie eine Anwendungseinheit für eine Anwendung mithilfe der GUI:

Gehen Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten** Wählen Sie im Abschnitt **Anwendungseinheit** eine Entität aus, klicken Sie auf das

Bearbeitungssymbol und ändern Sie die Einstellungen der Anwendungseinheit.

Hinweis: Sie können den Namen und den Regelausdruck für eine vorhandene Anwendungseinheit nicht ändern.

Mit den Video-Tutorials von NetScaler können Sie die Funktionen von NetScaler auf einfache Weise verstehen. Sehen Sie sichhttps://www.youtube.com/watch?v=bJ5_i8fV2hc Video an, um zu erfahren, wie Sie eine Anwendungseinheit konfigurieren.

Öffentliche Endpunkte für eine Anwendung konfigurieren

May 11, 2023

So konfigurieren Sie öffentliche Endpunkte für eine Anwendung mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendungseinheit aus, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie im Abschnitt **Öffentliche Endpunkte** auf **+**, um einen neuen öffentlichen Endpunkt zu konfigurieren.
3. Führen Sie im Schieberegler **Öffentliche Endpunkte** einen der folgenden Schritte aus:
   a) Klicken Sie auf **Neu**, um einen neuen Endpunkt zu erstellen
   b) Klicken Sie auf **Vorhandener öffentlicher Endpunkt**, um einen Endpunkt aus der Dropdownliste auszuwählen.
4. Stellen Sie die folgenden Endpunktparameter ein:
   a) Name
   b) IP-Adresse
   c) Protokoll
   d) Port
5. Klicken Sie auf **Weiter**, um zusätzliche Einstellungen wie Anwendungseinheiten, GSLB-Serverbindungen, Richtlinien, Profile, Push, Verkehrseinstellungen und Authentifizierung zu konfigurieren.
6. Klicke auf **OK** und dann auf **Fertig**.
7. Klicken Sie auf **Weiter** und dann **Fertig**.

So bearbeiten Sie einen öffentlichen Endpunkt für eine Anwendung mithilfe der GUI:

Navigieren Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten**. Wählen Sie im Abschnitt **Öffentliche Endpunkte** einen Endpunkt aus, klicken Sie auf das Stiftsymbol und ändern Sie die Endpunkteinstellungen.

So löschen Sie einen öffentlichen Endpunkt für eine Anwendung mithilfe der GUI:

Navigieren Sie zu **AppExpert** > **Applications** > **Public Endpoint und klicken Sie auf das Stiftsymbol,** um das Löschsymbol neben der Entity anzuzeigen.

Mit den Video-Tutorials von NetScaler können Sie die Funktionen von NetScaler auf einfache und einfache Weise verstehen. Sehen Sie sichhttps://www.youtube.com/watch?v=z4v-edQiVpw Video an, um zu erfahren, wie Sie einen öffentlichen Endpunkt konfigurieren.

Angeben der Reihenfolge der Auswertung von Anwendungseinheiten

June 21, 2022

Regeln für Anwendungseinheiten werden in der Reihenfolge ausgewertet, in der sie in der GUI platziert werden. Die Regel, die für die oberste Anwendungseinheit konfiguriert ist, wird immer zuerst konfiguriert, gefolgt von der Regel, die für die zweitoberste Anwendungseinheit konfiguriert ist, usw. Die Standardanwendungseinheit wird immer zuletzt bewertet.

Wenn eine Anforderung mit der Regel übereinstimmt, die für eine Anwendungseinheit konfiguriert ist, wird die Anforderung von der Anwendungseinheit verarbeitet, und es wird kein weiterer Abgleich durchgeführt. Daher wird die Reihenfolge der Bewertung von Anwendungseinheiten zu einem wichtigen Faktor, wenn sich die Traffic-Teilmengen für zwei oder mehr Anwendungseinheiten überschneiden. Wenn sich die Traffic-Teilmengen für zwei oder mehr Anwendungseinheiten überschneiden, müssen Sie die Reihenfolge angeben, in der eine eingehende Anforderung mit den Regeln für Anwendungseinheiten abgeglichen wird.

So legen Sie die Reihenfolge der Auswertung von Anwendungseinheiten fest:

1. Gehen Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten** Klicken Sie im Abschnitt **Anwendungseinheit** auf das **Bleistiftsymbol**, und bewegen Sie den Cursor dann über das Kontrollkästchen links neben dem Namen der Anwendungseinheit. Klicken Sie auf das Symbol, das neben dem Kontrollkästchen angezeigt wird, und halten Sie die Maus gedrückt, um die Anwendung an eine neue Position in der Prioritätsliste nach oben oder unten zu ziehen.

Persistenzgruppen für Anwendungseinheiten konfigurieren

May 11, 2023

Sie können eine Persistenzgruppe für die Anwendungseinheiten in einer AppExpert-Anwendung konfigurieren. Im Kontext einer AppExpert-Anwendung ist eine Persistenzgruppe eine Gruppe von Anwendungseinheiten, die Sie als eine Einheit behandeln können, um allgemeine Persistenzeinstellungen anzuwenden. Wenn die Anwendung in eine Anwendungsvorlagendatei exportiert wird, sind die Einstellungen für die Persistenzgruppe enthalten, und sie werden automatisch auf die Anwendungseinheiten angewendet, wenn Sie die AppExpert-Anwendung importieren.

So konfigurieren Sie eine Persistenzgruppe für eine Anwendung mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Dialogfeld **Anwendungsansicht** auf den Namen der Anwendung, für deren Anwendungseinheiten Sie eine Persistenzgruppe konfigurieren möchten, und klicken Sie dann auf **Persistenzgruppen**konfigurieren.
3. Führen **Sie im Dialogfeld Configure Persistency Groups** einen der folgenden Schritte aus:
   - Um eine Persistenzgruppe hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um eine Persistenzgruppe zu ändern, klicken Sie auf **Öffnen**.
4. Stellen **Sie im Dialogfeld Persistency-Gruppe erstellen** oder **Persistency-Gruppe konfigurieren** die folgenden Parameter ein:
   - Gruppenname — Name der Persistenzgruppe. Damit die NetScaler-Appliance die Persistenzgruppe als Teil der Anwendungskonfiguration erkennt, muss der Name der AppExpert-Anwendung als Präfix im Namen der Persistenzgruppe enthalten sein. Daher zeigt die Appliance standardmäßig das Präfix im Feld Gruppenname an, und Sie können dieses Präfix nicht entfernen. Geben Sie nach dem Präfix einen Namen Ihrer Wahl ein.
   - Persistenz — Art der Persistenz für den virtuellen Server. Wenn Sie SOURCEIP auswählen, geben Sie im Feld IPv4-Netzmaske eine Netzwerkmaske ein, die die Anzahl der Bits angibt, die die Appliance beim Erstellen von Persistenzsitzungen berücksichtigen muss. Wenn Sie COOKIEINSERT auswählen, geben Sie in den Feldern Cookie-Domain und Cookie-Name ein Domain-Attribut an, das in der Set-Cookie-Direktive gesendet werden soll, und einen Namen für das Cookie.
   - Timeout — Zeitraum, für den eine Persistenzsitzung in Kraft ist.
   - Backup-Persistenz — Art der Backup-Persistenz für die Gruppe.
   - Backup-Timeout — Zeitraum in Minuten, für den die Backup-Persistenz gültig ist.
   - Anwendungseinheiten — Um der Persistenzgruppe eine Anwendungseinheit hinzuzufügen, klicken Sie im Feld Verfügbare Anwendungseinheiten auf die Anwendungseinheit, und klicken Sie dann auf Hinzufügen. Um eine Anwendungseinheit aus der Persistenzgruppe zu entfernen, klicken Sie im Feld Konfigurierte Anwendungseinheiten auf die Anwendungseinheit und dann auf **Entfernen**.
5. Klicken Sie auf **OK**.

Anzeigen von AppExpert-Anwendungen und Konfigurieren von Entitäten mithilfe des Anwendungsvisualisierers

June 21, 2022

Die Visualizer-Funktion zeigt Ihnen eine grafische Darstellung der Konfiguration einer Anwendung. Sie enthält den Namen des öffentlichen Endpunkts, Anwendungseinheiten, die dem öffentlichen End-

punkt zugewiesen sind, und die Anzahl der Richtlinien und Dienste, die an die Anwendung gebunden sind. Sie können den Visualizer verwenden, um einen visuellen Überblick über die Konfiguration einer AppExpert-Anwendung zu erhalten und einige der angezeigten Entitäten zu konfigurieren. Standardmäßig zeigt der Visualizer Anwendungseinheiten, Dienste und Monitore für die ausgewählte Anwendung an.

So zeigen Sie eine AppExpert-Anwendung mit dem Application Visualizer an:

1. Gehen Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendungsentität aus und klicken Sie auf **Visualizer**

Benutzerauthentifizierung, Autorisierung und Überwachung konfigurieren

June 21, 2022

Sie können die Autorisierung für Benutzer und Gruppen konfigurieren, um dann auf eine AppExpert-Anwendung zugreifen zu können. Wenn der AAA-Benutzer oder die AAA-Gruppe, für die Sie Berechtigungen konfigurieren möchten, noch nicht erstellt wurde, können Sie ihn in AppExpert erstellen und dann Berechtigungen für den Anwendungszugriff konfigurieren.

So konfigurieren Sie AAA-Benutzer und AAA-Benutzergruppen für eine Anwendung mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendungseinheit aus, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Autorisierung**und konfigurieren Sie autorisierte Benutzer und Benutzergruppen.
3. Klicken Sie auf den Abschnitt **AAA-Benutzer**, um autorisierte Benutzer an die Anwendung zu binden.
4. Stellen Sie im Schieberegler **AAA-Benutzer** die Parameter ein.
5. Klicken Sie auf **Fortfahren** und dann im Abschnitt **Erweiterte Einstellungen** auf **Autorisierungsrichtlinien**.
6. Binden Sie im Schieberegler **Autorisierungsrichtlinie** eine Autorisierungsrichtlinie an die Anwendung.
7. Klicken Sie auf **Fortfahren** und dann im Abschnitt **Erweiterte Einstellungen** auf den Abschnitt **Autorisierungsgruppe**.
8. Binden Sie unter dem Schieberegler **AAA-Gruppenbindung** eine Autorisierungsbenutzergruppe an die Anwendung.
9. Klicken Sie auf **Fortfahren** und dann im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.

10. Binden Sie im Schieberegler **Richtlinien** eine **Überwachungssyslog** - oder **Audit-NsLog-Richtlinie** an die Anwendung.
11. Klicken Sie auf **Weiter** und dann **Fertig**.

So bearbeiten Sie AAA-Benutzer und AAA-Benutzergruppen für eine Anwendung mithilfe der GUI:

Navigieren Sie zu **AppExpert** > **Anwendungen** > **Erweiterte Einstellungen** und klicken Sie auf **Autorisierung**. Klicken Sie dann auf das Bearbeitungssymbol und geben Sie Werte für Benutzer- oder Benutzergruppenautorisierungseinstellungen an

So löschen Sie AAA-Benutzer und AAA-Benutzergruppen mithilfe der GUI:

Gehen Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten** Klicken Sie auf der Seite **Anwendungen** auf **Erweiterte Einstellungen** und dann auf **Autorisierung**. Klicken Sie auf das Löschsymbol neben der Entität.

Überwachen einer NetScaler-Anwendung

May 11, 2023

Nachdem Sie die AppExpert-Anwendung angepasst haben, können Sie Anwendungsstatistiken anzeigen, um sicherzustellen, dass die Anwendung und alle ihre Entitäten ordnungsgemäß funktionieren. Sie können den Application Visualizer auch verwenden, um Statistiken zu überwachen, die bestimmten Entitäten wie Richtlinien und virtuellen Servern zugeordnet sind.

Sie können auch die Trefferzähler für verschiedene Entitäten in regelmäßigen Abständen anzeigen, um sicherzustellen, dass die Zähler aktualisiert werden.

Anwendungsstatistiken anzeigen

Im Knoten **Anwendungen** können Sie eine Anwendung auswählen und die Statistikseite für die Anwendung aufrufen. Auf der Seite Statistiken können Sie den Zustand und den Status von öffentlichen Endpunkten und Anwendungseinheiten überwachen und die folgenden statistischen Informationen anzeigen:

- Anfragen und Antworten pro Sekunde für jeden der öffentlichen Endpunkte und Anwendungseinheiten.
- Byte pro Sekunde, an jedem Endpunkt, für eingehenden und ausgehenden Verkehr.
- Die Anwendungseinheit traf Zähler und die Anzahl der Client- und Serververbindungen für jede Anwendungseinheit.
- Statistiken für die Dienste, die an die Anwendungseinheiten gebunden sind.

Auf der Seite Statistiken können Sie auch CPU-Auslastung, Speicherauslastung und Systemprotokolle anzeigen.

So zeigen Sie Statistiken für eine Anwendung an:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich auf die Anwendung, für die Sie Statistiken anzeigen möchten, und klicken Sie dann auf **Statistiken**.

Überwachen einer Anwendung mit dem Application Visualizer

Sie können den Application Visualizer verwenden, um die Anzahl der Anforderungen zu überwachen, die zu einem bestimmten Zeitpunkt von den vservers pro Sekunde empfangen werden, und die Anzahl der Treffer pro Sekunde zu einem bestimmten Zeitpunkt für Rewrite-, Responder- und Cache-Richtlinien.

So zeigen Sie statistische Informationen für vServer, Rewrite-Richtlinien, Responder-Richtlinien und Cache-Richtlinien im Visualizer an:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Wählen Sie im Detailbereich die Anwendung aus, für die Sie statistische Informationen anzeigen möchten, und klicken Sie dann auf **Visualizer**.
3. Gehen Sie im Fenster **Application Visualizer** wie folgt vor:
   - Um die Statistiken anzuzeigen, klicken Sie auf **Statistik anzeigen**.
     Die statistischen Informationen werden auf den jeweiligen Knoten im Visualizer angezeigt. Diese Informationen werden nicht in Echtzeit aktualisiert und müssen manuell aktualisiert werden.
   - Um die statistischen Informationen zu aktualisieren, klicken Sie auf **Statistik aktualisieren**.

Treffer anzeigen

Die Trefferzähler, die für verschiedene AppExpert Anwendungsentitäten bereitgestellt werden, ermöglichen es Ihnen, die Funktionsweise öffentlicher Endpunkte und Anwendungseinheiten zu überwachen. Für eine Anwendung zeigt das Dialogfeld Treffer die Gesamtzahl der Anfragen an, die von jedem konfigurierten öffentlichen Endpunkt empfangen wurden. Für eine Anwendungseinheit zeigt das Dialogfeld Treffer die Anzahl der Anforderungen an, die die Anwendungseinheit von jedem öffentlichen Endpunkt verarbeitet hat, sowie die Gesamtanzahl der Treffer an. Anweisungen zum Anzeigen von Trefferzählern finden Sie unter Überprüfen und Testen der Konfiguration.

Eine Anwendung löschen

June 21, 2022

Wenn Sie eine Anwendung und ihre Anwendungseinheiten nicht mehr benötigen, können Sie sie löschen. Wenn Sie eine AppExpert-Anwendung löschen, werden Backend-Dienste nicht gelöscht, und alle öffentlichen Endpunkte, die von der Anwendung verwendet werden, werden für die Verwendung durch andere Anwendungen verfügbar.

Beim Löschen einer Anwendung werden Sie auch aufgefordert anzugeben, ob Sie gebundene Richtlinien und Aktionen löschen möchten, die an keiner anderen Stelle verwendet werden.

So löschen Sie eine Anwendungseinheit für eine Anwendung mithilfe der GUI:

Gehen Sie zu **AppExpert** > **Applications**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten** Klicken Sie im Abschnitt **Anwendungseinheit** auf das Löschsymbol neben der Entität

Konfigurieren der Anwendungsauthentifizierung, Autorisierung und Überwachung

June 21, 2022

Sie können Authentifizierung, Autorisierung und Überwachung (AAA) für die Anwendungen konfigurieren, die Sie auf der Appliance konfigurieren. Eine Authentifizierungsrichtlinie, die für eine Anwendung konfiguriert ist, definiert den Authentifizierungstyp, der angewendet wird, wenn ein Benutzer oder eine Gruppe versucht, auf die Anwendung zuzugreifen. Wenn eine externe Authentifizierung verwendet wird, gibt die Richtlinie auch den externen Authentifizierungsserver an. Für eine Anwendung konfigurierte Autorisierungsrichtlinien geben an, ob ein bestimmter Benutzer oder eine bestimmte Gruppe auf die Anwendung zugreifen kann. Überwachungsrichtlinien definieren den Typ des Überwachungsprotokolls, die Ebene, auf der die Protokollierung durchgeführt wird, und andere Einstellungen des Überwachungsservers. Authentifizierungs- und Überwachungsrichtlinien verwenden das klassische Richtlinienformat.

Authentifizierungsrichtlinien, Autorisierungsrichtlinien und Überwachungsrichtlinien können in beliebiger Reihenfolge konfiguriert werden. Bevor Sie jedoch AAA für eine Anwendung konfigurieren, müssen Sie einen öffentlichen Endpunkt für die Anwendung konfigurieren.

Zum Konfigurieren der Authentifizierung für eine Anwendung müssen ein Authentifizierungs-FQDN, ein virtueller Authentifizierungsserver, ein Serverzertifikat sowie Authentifizierungs- und Sitzungsrichtlinien angegeben werden. Authentifizierungsrichtlinien sind automatisch an den virtuellen Authentifizierungsserver gebunden, der für die Anwendung angegeben wurde.

So konfigurieren Sie die Authentifizierung für eine AppExpert-Anwendung:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   a) Klicken Sie auf Hinzufügen, um eine Authentifizierung für eine neue Anwendung hinzuzufügen.
   b) Klicken Sie auf Bearbeiten, um eine bestehende Anwendung zu ändern.
3. Wählen Sie auf der Seite **Anwendungen** eine Anwendungseinheit aus.
4. Klicken Sie auf der Slider-Seite **Application Unit** im Abschnitt **Erweiterte Einstellungen** auf Authentifizierung.
5. Wählen Sie im Abschnitt **Authentifizierung** den Authentifizierungstyp wie folgt aus:
   a) Formularbasierte Authentifizierung
   b) 401-basierte Authentifizierung
   c) Ohne
6. Klicken Sie auf **OK** und dann auf **Fertig**.

Anwendungsautorisierung konfigurieren

Sie können die Autorisierung für Benutzer und Gruppen konfigurieren, um dann auf eine AppExpert-Anwendung zugreifen zu können. Wenn der AAA-Benutzer oder die AAA-Gruppe, für die Sie Berechtigungen konfigurieren möchten, noch nicht erstellt wurde, können Sie ihn in AppExpert erstellen und dann Berechtigungen für den Anwendungszugriff konfigurieren.

So konfigurieren Sie Berechtigungen für einen AAA-Benutzer oder eine Gruppe für den Zugriff auf eine AppExpert-Anwendung:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich auf die AppExpert-Anwendung, für die Sie einen Benutzer- oder Gruppenzugriff konfigurieren möchten.
3. Klicken Sie auf der Seite **Anwendungen** auf Autorisierung. im Abschnitt **Erweiterte Einstellungen** .
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn sich der AAA-Benutzer oder die AAA-Gruppe, für die Sie Berechtigungen konfigurieren möchten, bereits in der Gruppen-/Benutzerstruktur befinden, ziehen Sie den Benutzer oder die Gruppe aus der Gruppen-/Benutzerstruktur auf den Knoten Benutzer oder Gruppen in der Anwendungsstruktur. Klicken Sie dann mit der rechten Maustaste auf den Benutzer oder die Gruppe und klicken Sie
   - Wenn der AAA-Benutzer oder die AAA-Gruppe, für die Sie Berechtigungen konfigurieren möchten, nicht auf der Appliance konfiguriert ist, klicken Sie in der Anwendungsstruktur mit der rechten Maustaste auf Benutzer oder Gruppen, und klicken Sie dann auf Hinzufügen. Geben Sie im Dialogfeld AAA-Gruppe erstellen oder AAA-Benutzer erstellen die Werte ein, klicken Sie auf Erstellen und dann auf Schließen.

Der Benutzer oder die Gruppe wird mit der auf Zulassen gesetzten Berechtigung erstellt. Um die Berechtigungseinstellung zu ändern, klicken Sie mit der rechten Maustaste auf die Gruppe oder den Benutzer, und klicken Sie dann auf die

5. Klicken Sie auf **Fertig** und dann auf **Schließen**.

Anwendungsüberwachung konfigurieren

Wenn Sie Überwachungsrichtlinien für eine Anwendung konfigurieren, müssen Sie den Server angeben, an den die Protokollnachrichten geleitet werden müssen, das Format der protokollierten Nachrichten und die Protokollebene. Optional können Sie weitere Einstellungen konfigurieren, z. B. die Protokollfunktion und das Datumsformat. Überwachungsrichtlinien sind automatisch an alle öffentlichen Endpunkte der AppExpert-Anwendung gebunden.

So konfigurieren Sie Überwachungsrichtlinien für eine Anwendung:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich auf die Anwendung, für die Sie Überwachungsrichtlinien konfigurieren möchten.
3. Klicken Sie auf der Schiebereglerseite der Anwendungseinheit im Abschnitt **Richtlinien** auf das Symbol +, um die Überwachungsrichtlinien zu konfigurieren.
4. Wählen Sie auf der Schiebereglerseite **Richtlinien** den Richtlinientyp Syslog-Überwachung oder NSlog-Überwachung aus und klicken Sie auf **Weiter**.
5. Legen Sie im Abschnitt Richtlinienbindung die folgenden Parameter fest.
   a) Wählen Sie eine Richtlinie für die Bindung aus. Wenn Sie keine Richtlinie für Bindungen haben, klicken Sie auf +, um eine neue Richtlinie zu erstellen.
   b) Um eine neue Überwachungsrichtlinie zu erstellen, klicken Sie unter Richtlinienname auf **Neue Richtlinie,** und gehen Sie dann auf der Seite **Richtlinie** wie folgt vor:
      i. Geben Sie in das Feld Name einen Namen für die Richtlinie ein.
      ii. Das Feld Name enthält bereits die Zeichenfolge, die am Anfang des Servernamens erforderlich ist. Die Zeichenfolge kann nicht geändert werden.
      iii. Wählen Sie in der Liste Auditing-Typ den Überwachungstyp aus (entweder SYSLOG oder NSLOG).
      iv. Wenn der Überwachungsserver, den Sie angeben möchten, bereits in der Serverliste aufgeführt ist, wählen Sie den Server aus der Liste aus, und klicken Sie dann auf Ändern, wenn Sie die Servereinstellungen ändern möchten. Ändern Sie im Dialogfeld Überwachungsserver konfigurieren die Einstellungen entsprechend, und klicken Sie dann auf OK. Weitere Informationen zu den Einstellungen im Dialogfeld Überwachungsserver konfigurieren finden Sie unter Auditing Authenticated Sessions.
      v. Wenn Sie einen neuen Überwachungsserver konfigurieren möchten, klicken Sie auf Neu, und geben Sie dann im Dialogfeld Überwachungsserver erstellen einen Namen

für den Server ein, geben Sie die IP-Adresse des Servers, die Portnummer und andere Einstellungen an. Klicken Sie zum Abschluss auf **OK**.

vi. Klicken Sie auf **Erstellen**.

c) Um die Prioritäten für die neuen Überwachungsrichtlinien zu ändern, die Sie erstellt haben, doppelklicken Sie unter Priorität für jede Richtlinie, für die Sie die Priorität ändern möchten, auf den Prioritätswert, und geben Sie einen neuen Prioritätswert ein.

d) Um Prioritäten erneut zu generieren, klicken Sie auf **Prioritäten neu generieren**.

e) Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie und dann auf **Richtlinie aufheben**.

f) Um eine Richtlinie zu ändern, klicken Sie auf die Richtlinie und dann auf **Richtlinie ändern.**

6. Klicken Sie auf **Apply Changes** und dann auf **Close**.

AAA für eine Anwendung deaktivieren

Nachdem Sie AAA für eine Anwendung konfiguriert haben, können Sie die AAA-Konfiguration für diese Anwendung deaktivieren. Wenn Sie AAA für eine Anwendung deaktivieren, geht die Konfiguration nicht verloren. Sie können AAA für die Anwendung aktivieren, wenn Sie die Konfiguration erneut anwenden möchten.

So aktivieren oder deaktivieren Sie AAA für eine Anwendung:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich auf die Anwendung, für die Sie AAA aktivieren oder deaktivieren möchten, und führen Sie dann einen der folgenden Schritte aus:
3. Um AAA für die Anwendung zu deaktivieren, klicken Sie auf **AAA ausschalten.**
4. Um AAA für die Anwendung zu aktivieren, klicken Sie **auf AAA aktivieren**.

Einrichten einer benutzerdefinierten NetScaler-Anwendung

May 11, 2023

Wenn eine AppExpert-Anwendungsvorlage für die Webanwendung, die Sie über die NetScaler-Appliance verwalten möchten, nicht verfügbar ist, oder wenn verfügbare AppExpert-Anwendungsvorlagen Ihren Anforderungen nicht entsprechen, können Sie eine AppExpert-Anwendung ohne Vorlage erstellen.

Um eine AppExpert-Anwendung ohne Vorlage zu erstellen, müssen Sie zunächst eine Anwendung und Anwendungseinheiten erstellen. Anschließend konfigurieren Sie öffentliche Endpunkte, Dienste und Dienstgruppen. Schließlich konfigurieren Sie die Richtlinien, die festlegen, wie der Anwendungsdatenverkehr bewertet und verarbeitet wird.

Nachdem Sie die Anwendungs- und Anwendungseinheiten erstellt und Richtlinien konfiguriert haben, müssen Sie die Konfiguration überprüfen und testen, um sicherzustellen, dass sie ordnungsgemäß funktioniert, genau wie bei der Konfiguration einer Anwendung mithilfe einer vorgefertigten AppExpert-Anwendungsvorlage. Anschließend müssen Sie die Anwendung überwachen, um sicherzustellen, dass die Anwendung und ihre Entitäten ordnungsgemäß funktionieren.

Eine Anwendung erstellen

Wenn Sie eine AppExpert-Anwendung erstellen, erstellt die Appliance einen Container, zu dem Sie Anwendungseinheiten hinzufügen können. Die Standardanwendungseinheit wird erst erstellt, wenn Sie die erste Anwendungseinheit erstellen.

So erstellen Sie eine AppExpert-Anwendung mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf **Anwendungen**, und klicken Sie dann auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Anwendung erstellen** unter Name einen Namen für die Anwendung ein, und klicken Sie dann auf **OK**.

Erstellen von Anwendungseinheiten

Für jede Teilmenge des Datenverkehrs, der mit Ihrer Webanwendung verknüpft ist, müssen Sie eine Anwendungseinheit erstellen.

So erstellen Sie eine Anwendungseinheit für die AppExpert-Anwendung mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie eine Anwendungseinheit hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**.
3. Klicken Sie auf **Erstellen**.

Öffentliche Endpunkte für eine AppExpert-Anwendung konfigurieren

Nachdem Sie alle Anwendungseinheiten erstellt haben, die Sie benötigen, müssen Sie einen oder mehrere öffentliche Endpunkte konfigurieren, damit Clients über die NetScaler-Appliance auf die Webanwendung zugreifen können.

So konfigurieren Sie öffentliche Endpunkte für eine AppExpert-Anwendung mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie öffentliche Endpoints konfigurieren möchten, und klicken Sie dann auf **Öffentliche Endpoints konfigurieren**.

3. Führen Sie im Dialogfeld Öffentliche Endpunkte wählen für die Anwendung einen der folgenden Schritte aus:
   - Wenn die gewünschten Endpunkte im Dialogfeld aufgeführt sind, klicken Sie auf die entsprechenden Kontrollkästchen.
   - Wenn Sie alle öffentlichen Endpunkte angeben möchten, klicken Sie auf **Alle aktivieren**.
   - Wenn Sie Endpunkte von der AppExpert-Anwendung trennen möchten, deaktivieren Sie die entsprechenden Kontrollkästchen.
   - Wenn Sie einen neuen öffentlichen Endpunkt erstellen möchten, klicken Sie auf **Hinzufügen**. Konfigurieren Sie dann im Dialogfeld Öffentliche Endpunkte erstellen die Endpunkteinstellungen, und klicken Sie dann auf **OK**.
     Im Dialogfeld **Öffentliche Endpunkte erstellen** können Sie nur den Namen, die IP-Adresse, den Port und das Protokoll für den Endpunkt angeben. Sie können zusätzliche Endpunkteinstellungen angeben, nachdem Sie den öffentlichen Endpunkt erstellt haben. Um zusätzliche Endpunkteinstellungen festzulegen, klicken Sie nach dem Erstellen des Endpunkts im Dialogfeld Öffentliche Endpunkte auswählen auf den Endpunkt, und klicken Sie dann auf **Öffnen**. Geben Sie dann im Dialogfeld **Öffentliche Endpunkte konfigurieren** zusätzliche Einstellungen ein, und klicken Sie dann auf **OK** .
     Weitere Informationen zu den Parametern in den Dialogfeldern **Public Endpoint erstellen** und **Public Endpoint konfigurieren** finden Sie unter Content Switching.
   - Wenn Sie einen öffentlichen Endpunkt ändern möchten, klicken Sie auf den Endpunkt, und klicken Sie dann auf **Öffnen**. Ändern Sie dann im Dialogfeld **Öffentlichen Endpunkt konfigurieren** die Einstellungen für den Endpunkt, und klicken Sie dann auf **OK**.
     Weitere Informationen zu den Parametern im Dialogfeld Configure Public Endpoint finden Sie unter Content Switching.
4. Klicken Sie auf **Schließen**.

Öffentliche Endpunkte für eine Anwendungseinheit konfigurieren

Für eine Anwendungseinheit geben Sie öffentliche Endpunkte wie öffentliche Endpunkte für eine Anwendung an, die aus einer AppExpert Anwendungsvorlage erstellt wird. Weitere Informationen zum Angeben einer Teilmenge der Endpunkte für eine Anwendungseinheit finden Sie unter Konfigurieren von Endpoints für eine Anwendungseinheit.

So konfigurieren Sie Endpunkte für eine Anwendungseinheit mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendungseinheit, für die Sie öffentliche Endpoints angeben möchten, und klicken Sie dann auf **Öffentliche Endpunkte konfigurieren**.
3. Führen **Sie im Dialogfeld Öffentliche Endpunkte wählen** für die Anwendungseinheit einen der folgenden Schritte aus:

- Wenn Sie Endpunkte für die Anwendungseinheit zum ersten Mal angeben, deaktivieren Sie die Kontrollkästchen der Endpunkte, die nicht an die Anwendungseinheit gebunden werden sollen.
- Wenn Sie Endpunkte angeben möchten, die im Dialogfeld aufgeführt, aber derzeit nicht an die Anwendungseinheit gebunden sind, klicken Sie auf die entsprechenden Kontrollkästchen.

4. Klicken Sie auf **OK**.

Dienste und Dienstgruppen für eine AppExpert-Anwendung konfigurieren

Dienste und Dienstgruppen sind für Anwendungseinheiten erst verfügbar, nachdem Sie die Dienste und Dienstgruppen für die AppExpert-Anwendung konfiguriert haben. Daher müssen Sie Dienste und Dienstgruppen für die AppExpert-Anwendung konfigurieren, bevor Sie die Dienste für die Anwendungseinheiten konfigurieren. Alle Dienste und Dienstgruppen, die Sie für eine AppExpert-Anwendung konfigurieren, müssen dasselbe Protokoll verwenden (entweder HTTP oder HTTPS). Das Verfahren zum Konfigurieren von Diensten und Dienstgruppen für eine AppExpert-Anwendung, die nicht aus einer Vorlage erstellt wird, entspricht dem für eine Anwendung, die aus einer Vorlage erstellt wurde.

So konfigurieren Sie einen Dienst oder eine Dienstgruppe für die AppExpert-Anwendung mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie Dienste oder Dienstgruppen konfigurieren möchten, und klicken Sie dann auf **Backend-Dienste konfigurieren**.
3. Führen Sie im Dialogfeld “Backend-Dienste konfigurieren “ einen der folgenden Schritte aus:
   - Um Dienste zu konfigurieren, klicken Sie auf die Registerkarte **Dienste** .
   - Um Dienstgruppen zu konfigurieren, klicken Sie auf die Registerkarte **Service Groups** .
4. Führen Sie auf der Registerkarte **Dienstoder Dienstgruppen** einen der folgenden Schritte aus:
   - Wenn die gewünschten Dienste oder Dienstgruppen auf der Registerkarte aufgeführt sind, klicken Sie auf die entsprechenden Kontrollkästchen.
   - Wenn Sie alle Dienste oder Dienstgruppen angeben möchten, klicken Sie auf **Alle aktivieren**.
   - Wenn Sie einen neuen Dienst oder eine neue Dienstgruppe erstellen möchten, klicken Sie auf **Hinzufügen**. Konfigurieren Sie dann im Dialogfeld **Dienst erstellen** oder **Dienstgruppe erstellen** die Einstellungen für den Dienst bzw. die Dienstgruppe, und klicken Sie dann auf **Erstellen**.
   - Wenn Sie einen Dienst ändern möchten, klicken Sie auf den Dienst und dann auf Öffnen. Konfigurieren Sie dann im Dialogfeld **Dienst konfigurieren** oder **Dienstgruppe erstellen** Einstellungen für den Dienst bzw. die Dienstgruppe, und klicken Sie dann auf **OK**.

Informationen zu den Einstellungen in den Dialogfeldern Service erstellen, Dienst konfigurieren und **Dienstgruppe erstellen** finden Sie unter Lastenausgleich.

Konfigurieren von Diensten und Servicegruppen für eine Anwendungseinheit

Nachdem Sie Dienste und Dienstgruppen konfiguriert haben, müssen Sie Dienste und Dienstgruppen für jede Anwendungseinheit konfigurieren. Dieser Schritt ist jedoch nicht erforderlich, wenn jeder Backend-Dienst den gesamten mit der Webanwendung verknüpften Inhalt hostet. Sie konfigurieren Dienste und Dienstgruppen für eine Anwendungseinheit, wenn der mit der Anwendungseinheit verknüpfte Inhalt nur auf einer Teilmenge der Backend-Server gehostet wird.

So konfigurieren Sie Dienste oder Dienstgruppen für eine Anwendungseinheit mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Applications**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendungseinheit, für die Sie einen Dienst oder eine Dienstgruppe konfigurieren möchten, und klicken Sie dann auf **Backend-Dienste konfigurieren**.
3. Führen **Sie im Dialogfeld "Backend-Dienste konfigurieren** " einen der folgenden Schritte aus:
   - Um Dienste zu konfigurieren, klicken Sie auf die Registerkarte **Dienste** .
   - Um Dienstgruppen zu konfigurieren, klicken Sie auf die Registerkarte **Dienstgruppen** .
4. Führen Sie auf der Registerkarte **Dienste** oder **Dienstgruppen** einen der folgenden Schritte aus:
   - Deaktivieren Sie die Kontrollkästchen, die den Diensten oder Dienstgruppen entsprechen, die nicht für die Anwendungseinheit konfiguriert werden sollen. Stellen Sie sicher, dass die Kontrollkästchen, die den Diensten oder Dienstgruppen entsprechen, die Sie für die Anwendungseinheit konfigurieren möchten, aktiviert sind. Geben Sie dann in der Spalte Gewicht das Gewicht an, das Sie jedem konfigurierten Dienst zuweisen möchten.
   - Um alle Dienste oder Dienstgruppen anzugeben, klicken Sie auf **Alle aktivieren**.
5. Geben Sie auf den Registerkarten **Methode** und **Persistenz** und **Erweitert** die gewünschten Parameter an.
6. Klicken Sie auf **OK**.

Richtlinien konfigurieren

Die Verfahren zum Konfigurieren von Richtlinien für eine AppExpert Anwendung, die ohne Verwendung einer Vorlage erstellt wird, entsprechen denen für eine AppExpert-Anwendung, die aus einer Vorlage erstellt wurde. Weitere Informationen finden Sie unter Konfigurieren von Richtlinien für Anwendungseinheiten.

NetScaler Gateway-Anwendungen

May 11, 2023

Wenn Sie eine AppExpert-Anwendung für die Verwaltung einer Webanwendung über die Citrix® NetScaler® -Appliance konfigurieren, erstellen Sie auch eine Reihe von Anwendungseinheiten und konfigurieren für jedes Gerät eine Reihe von Verkehrsoptimierungs- und Sicherheitsrichtlinien. Die Richtlinien, die Sie für jede Anwendungseinheit konfigurieren (Richtlinien für Funktionen wie Komprimierung, Caching und Neuschreiben), werten Datenverkehr aus, der nur für diese Einheit bestimmt ist. Zusätzlich zu diesen Richtlinien sollten Sie möglicherweise Access Gateway-Richtlinien für die gesamte Anwendung konfigurieren, um den Anwendungsverkehr beim Zugriff über das Access Gateway zu optimieren. Mit der Funktion Access Gateway-Anwendungen können Sie Access Gateway-Richtlinien (Autorisierung, Datenverkehr, Clientloser Zugriff und TCP-Komprimierung) für eine AppExpert-Anwendung konfigurieren. Nachdem Sie die NetScaler Gateway-Richtlinien für AppExpert-Anwendungen konfiguriert haben, können Sie die Richtlinienkonfiguration in die von Ihnen AppExpert-Anwendungsvorlagen aufnehmen.

Sie können auch NetScaler Gateway-Richtlinien für Intranetsubnetze, Dateifreigaben und andere Netzwerkressourcen konfigurieren. Schließlich können Sie Lesezeichen für AppExpert-Anwendungen und bestimmte Ressourcen erstellen, wenn Benutzer von der NetScaler Gateway-Startseite aus darauf zugreifen können sollen.

Sie können die Entitäten in der NetScaler Gateway-Anwendungsfunktion nur mithilfe der GUI konfigurieren.

So funktioniert eine NetScaler Gateway-Anwendung

Wenn Sie eine AppExpert-Anwendung im Knoten Anwendungen in der GUI erstellen, wird automatisch eine entsprechende Access Gateway-Anwendung im Knoten Access Gateway Applications erstellt. Darüber hinaus wird automatisch eine Regel für den Access Gateway-Anwendungseintrag erstellt, die den konfigurierten öffentlichen Endpunkt der AppExpert-Anwendung verwendet. Wenn mehrere Endpunkte für die AppExpert-Anwendung konfiguriert sind, umfasst die Regel alle konfigurierten öffentlichen Endpunkte. Die NetScaler-Appliance verwendet diese Regel, um alle konfigurierten Access Gateway-Richtlinien auf den Datenverkehr anzuwenden, der am öffentlichen Endpunkt der AppExpert-Anwendung empfangen wird. Der am öffentlichen Endpunkt der AppExpert-Anwendung empfangene Datenverkehr wird zunächst anhand der NetScaler Gateway-Richtlinien und dann anhand der Richtlinien bewertet, die für die Anwendungseinheiten der AppExpert-Anwendung konfiguriert wurden.

Die Regel, die für die Clientless Access-Richtlinien für eine Access Gateway-Anwendung erstellt wird, ist ein erweiterter Ausdruck, der auch den öffentlichen Endpunkt verwendet, der für die AppExpert-

Anwendung konfiguriert ist. Bevor Sie NetScaler Gateway-Richtlinien für eine AppExpert-Anwendung konfigurieren, müssen Sie daher öffentliche Endpunkte für die AppExpert-Anwendung konfigurieren.

Wenn Sie die NetScaler Gateway-Konfiguration in eine Anwendungsvorlage aufnehmen, sind bereitstellungsspezifische Informationen wie IP-Adresse und Portinformationen sowie die aus diesen Informationen erstellte Regel nicht in der Vorlage enthalten.

So funktioniert eine NetScaler-Konfiguration für eine Dateifreigabe

Auf der NetScaler-Appliance können Sie Autorisierungsrichtlinien für eine Dateifreigabe konfigurieren, die im Netzwerk Ihrer Organisation gehostet wird.

Wenn Sie eine Dateifreigabe erstellen, geben Sie einen Namen für die Dateifreigabe und den Netzwerkpfad zur Dateifreigabe an. Im Netzwerkpfad können Sie entweder den Namen des Servers oder die Server-IP-Adresse angeben. Eine Regel, die die Komponenten des Dateifreigabepfads verwendet, wird automatisch für die Dateifreigabe erstellt. Diese Regel ermöglicht es der Appliance, Anforderungen für Dateien zu identifizieren, die auf dem Dateifreigabe-Server gehostet werden Alle Autorisierungsrichtlinien, die für die Dateifreigabe konfiguriert sind, werden auf eingehende Anforderungen angewendet.

Die NetScaler-Konfiguration für eine Dateifreigabe kann nicht in AppExpert-Anwendungsvorlagen gespeichert werden.

So funktioniert eine NetScaler-Konfiguration für ein Intranetsubnetz

Für die Intranetsubnetze, die einen Teil Ihres Netzwerks bilden, können Sie Richtlinien für Autorisierung, Verkehr und TCP-Komprimierung auf der NetScaler-Appliance konfigurieren. Beim Hinzufügen eines Intranetsubnetzes geben Sie die IP-Adresse und die Netzmaske des Intranetsubnetzes an. Eine Regel, die diese beiden Parameter verwendet, wird automatisch für das Intranetsubnetz erstellt. Die Appliance wendet die konfigurierten Richtlinien auf alle Anforderungen an, bei denen eine Ziel-IP-Adresse und eine Netzmaske auf die IP-Adresse bzw. Netzmaske des Subnetzes festgelegt sind.

Die NetScaler-Konfiguration für ein Intranetsubnetz kann nicht in AppExpert-Anwendungsvorlagen gespeichert werden.

Funktionsweise der Kategorie “Andere Ressourcen”

In der Kategorie Andere Ressourcen können Sie Access Gateway-Richtlinien für jede Netzwerkressource mithilfe einer Regel Ihrer Wahl konfigurieren. Wenn Sie die NetScaler-Appliance für die Verarbeitung von Anforderungen für die Netzwerkressource konfigurieren, konfigurieren Sie einen klassischen Ausdruck, um die Anforderungen zu identifizieren, die mit der Netzwerkressource

verknüpft sind. Sie können Richtlinien für Autorisierung, Datenverkehr, Clientlosen Zugriff und TCP-Komprimierung für eine Netzwerkressource in Andere Ressourcen konfigurieren. Die NetScaler-Appliance wendet die konfigurierten NetScaler Gateway-Richtlinien auf alle Anforderungen an, die der konfigurierten Regel entsprechen.

Die NetScaler-Konfiguration für eine Netzwerkressource in Andere Ressourcen kann nicht in AppExpert-Anwendungsvorlagen gespeichert werden.

Benennungskonventionen

Die Funktion NetScaler Gateway-Anwendungen erzwingt eine Namenskonvention für einige der Entitäten, die Sie in dieser Funktion erstellen. Beispielsweise beginnen die Namen der Profile, die Sie für Verkehrsrichtlinien für ein Intranetsubnetz erstellen, immer mit einer Zeichenfolge, die aus dem Namen des Intranetsubnetzes gefolgt von einem Unterstrich (_) besteht. Der Name, den Sie für die Entität angeben, wird an diese Zeichenfolge angehängt. Wenn der Name eines Subnetzes “subnet1” ist, beginnt der Name des Profils mit “subnet1_”. Wenn eine solche Namenskonvention erforderlich ist (z. B. in das Textfeld, in das Sie den Namen einer Entität eingeben), fügt die Benutzeroberfläche automatisch die Zeichenfolge ein, mit der der Name der Entität beginnen muss, und Sie können sie nicht ändern.

Hinzufügen von Intranetsubnetzen

June 21, 2022

Sie können die Autorisierung und die Verkehrsrichtlinien für den Datenverkehr angeben, der für die in Ihrem Netzwerk konfigurierten Intranetsubnetze gebunden ist. Die Regeln für diese Richtlinien werden automatisch mithilfe der Parameter erstellt, die Sie für das Subnetz angeben.

So konfigurieren Sie ein Intranet-Subnetz mit der GUI:

1. Erweitern Sie im Navigationsbereich der GUI **AppExpert**, und klicken Sie dann auf Access Gateway-Anwendungen.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um ein Intranetsubnetz hinzuzufügen, klicken Sie auf **Intranet-Subnetze**und dann auf **Hinzufügen**.
   - Um ein Intranetsubnetz zu ändern, klicken Sie auf ein Intranetsubnetz und dann auf **Öffnen**.
3. Gehen **Sie im Dialogfeld Intranet-Subnet erstellen** oder **Intranetsubnet konfigurieren** wie folgt vor:
   a) Geben Sie in das Feld Name einen Namen für das Intranetsubnetz ein, das Sie hinzufügen. Dieser Parameter kann für ein vorhandenes Intranetsubnetz nicht geändert werden.

b) Geben Sie in das Feld IP-Adresse die IP-Adresse des Intranetsubnetzes ein.
c) Geben Sie in das Feld Netzmaske die Netzmaske ein, die für das Intranetsubnetz verwendet werden soll.
d) Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.

Andere Ressourcen hinzufügen

June 21, 2022

Für eine Netzwerkressource, die Sie zu anderen Ressourcen hinzufügen, müssen Sie einen erweiterten Richtlinienausdruck konfigurieren, der die Teilmenge des mit der Ressource verknüpften Datenverkehrs identifiziert.

So konfigurieren Sie eine Ressource in anderen Ressourcen über die GUI:

1. Erweitern Sie im Navigationsbereich der GUI AppExpert, und klicken Sie dann auf **Access Gateway Applications**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Ressource hinzuzufügen, klicken Sie auf **Andere Ressourcen**und dann auf **Hinzufügen**.
   - Um eine Ressource zu ändern, klicken Sie auf eine Ressource und dann auf **Öffnen**.
3. Gehen **Sie im Dialogfeld Ressource erstellenoder Ressource konfigurieren** wie folgt vor:
   a) Geben Sie im Feld Name einen Namen für die Ressource ein, die Sie hinzufügen. Dieser Parameter kann für eine vorhandene Ressource nicht geändert werden.
   b) Geben Sie im Feld Regel die Regel ein, die die Teilmenge des Datenverkehrs identifiziert, die mit der hinzugefügten Ressource verknüpft ist.
   Alternativ klicken Sie auf **Konfigurieren**, und erstellen Sie dann die Regel im Dialogfeld **Ausdruck erstellen** .
   c) Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.

Autorisierungsrichtlinien konfigurieren

May 11, 2023

Sie können NetScaler Gateway-Autorisierungsrichtlinien für AAA-Benutzer und -Gruppen für den Zugriff auf eine Ressource konfigurieren.

So konfigurieren Sie Berechtigungen für einen AAA-Benutzer oder eine AAA-Gruppe für den Zugriff auf eine Ressource mithilfe der GUI:

1. Erweitern Sie im Navigationsbereich der GUI AppExpert und klicken Sie dann auf **Access Gateway-Anwendungen**.
2. Klicken Sie im Detailbereich in der Spalte Autorisierung auf das Symbol für die Anwendung, Dateifreigabe, Intranetsubnetz oder Ressource, für die Sie Autorisierungsrichtlinien für AAA-Benutzer und -Gruppen konfigurieren möchten.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn sich der AAA-Benutzer oder die AAA-Gruppe, für die Sie Berechtigungen konfigurieren möchten, bereits in der Gruppen-/Benutzerstruktur befindet, ziehen Sie den Benutzer oder die Gruppe aus dem Baum Gruppen/Benutzer auf den Knoten Benutzer oder Gruppen in der Struktur <application name>. Klicken Sie dann mit der rechten Maustaste auf den Benutzer oder die Gruppe und klicken Sie auf **Zulassen**.
   - Wenn der AAA-Benutzer oder die AAA-Gruppe, für die Sie Berechtigungen konfigurieren möchten, nicht auf der Appliance konfiguriert ist, klicken Sie in der Struktur <application name> mit der rechten Maustaste auf Benutzer oder Gruppen, und klicken Sie dann auf **Hinzufügen**. Geben Sie im Dialogfeld **AAA-Gruppeerstellen oder AAA-Benutzer**erstellen die Werte ein, klicken Sie auf**Erstellen**und dann auf**Schließen**. Der Benutzer oder die Gruppe wird mit der auf Zulassen gesetzten Berechtigung erstellt. Um die Berechtigungseinstellung zu ändern, klicken Sie mit der rechten Maustaste auf die Gruppe oder den Benutzer, und klicken Sie dann auf die
4. Klicken Sie auf **Schließen**.

Konfigurieren von Verkehrsrichtlinien

May 11, 2023

Die Verkehrsrichtlinien, die Sie für die Ressourcen im Knoten NetScaler Gateway Applications konfigurieren, steuern Clientverbindungen zur Anwendung. Sie müssen keine Regel für die Ressource konfigurieren. Die Regel wird automatisch erstellt, wenn Sie die Ressource erstellen. Sie müssen nur ein Anforderungsprofil mit der Verkehrsrichtlinie verknüpfen. Im Verkehrsprofil geben Sie Parameter wie das Protokoll, das Anwendungs-Timeout und die Dateitypzuordnung an.

So konfigurieren Sie Verkehrsrichtlinien für eine Ressource

1. Erweitern Sie im Navigationsbereich der GUI AppExpert, und klicken Sie dann auf Access Gateway-Anwendungen.
2. Klicken Sie im Detailbereich in der Spalte Verkehr auf das Symbol für die Anwendung, Dateifreigabe, Intranet-Subnetz oder Ressource, für die Sie Verkehrsrichtlinien konfigurieren möchten.
3. Gehen Sie im Dialogfeld **Verkehrsrichtlinien konfigurieren** wie folgt vor:

- Um eine vorhandene Verkehrsrichtlinie anzugeben, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte Richtlinienname auf den Namen der Richtlinie.
- Um eine neue Richtlinie zu konfigurieren, klicken Sie auf Richtlinie einfügen, und klicken Sie dann in der Spalte Richtlinienname auf Neue Richtlinie. Geben Sie im Dialogfeld Traffic Policy erstellen im Feld Name nach dem Unterstrich (_) einen Namen für die Richtlinie ein. Wählen Sie dann in Anforderungsprofil entweder ein vorhandenes Anforderungsprofil aus oder klicken Sie auf Neu, um ein neues Anforderungsprofil zu konfigurieren. Sie können auch ein vorhandenes Profil auswählen und dann auf Ändern klicken, um das Profil zu ändern.
  Weitere Informationen zum Konfigurieren einer Verkehrsrichtlinie oder eines Profils finden Sie unter NetScaler Gateway.
- Um eine eingefügte Richtlinie zu ändern, klicken Sie in der Spalte Richtlinienname auf den Richtliniennamen und dann auf Richtlinie ändern. Um nur das zugehörige Profil zu ändern, klicken Sie in der Spalte Profil auf den Namen des Profils und dann auf **Profil ändern**.
- Um die den Richtlinien zugewiesenen Prioritäten neu zu generieren, klicken Sie auf **Prioritätenneu generieren**.
- Um einen neuen Prioritätswert für eine Richtlinie anzugeben, doppelklicken Sie in der Spalte Priorität auf die zugewiesene Priorität, und geben Sie dann den gewünschten Wert ein.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie und dann auf **Richtlinie aufheben**.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von clientlosen Zugriffsrichtlinien

May 11, 2023

Wenn der clientlose Zugriff für eine Ressource auf der NetScaler-Appliance konfiguriert ist, können Endbenutzer auf die Ressource zugreifen, ohne die NetScaler Gateway-Clientsoftware zu verwenden. Benutzer können Webbrowser verwenden, um auf Ressourcen wie Outlook Web Access zuzugreifen. Sie konfigurieren den clientlosen Zugriff für eine Ressource, indem Sie eine clientlose Zugriffsrichtlinie konfigurieren, die einem clientlosen Zugriffsprofil zugeordnet ist.

So konfigurieren Sie eine clientlose Zugriffsrichtlinie für eine Ressource im Knoten NetScaler Gateway Applications:

1. Erweitern Sie im Navigationsbereich der GUI **AppExpert**, und klicken Sie dann auf **Access Gateway-Anwendungen**.

2. Klicken Sie im Detailbereich in der Spalte **Clientloser Zugriff** auf das Symbol für die Anwendung, die Dateifreigabe, das Intranet-Subnetz oder die Ressource, für die Sie eine clientlose Zugriffsrichtlinie konfigurieren möchten.
3. Gehen Sie im Dialogfeld **Clientless-Zugriffsrichtlinien konfigurieren** wie folgt vor:
    - Um eine vorhandene clientlose Zugriffsrichtlinie anzugeben, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf den Namen der Richtlinie.
    - Um eine neue clientlose Zugriffsrichtlinie zu konfigurieren, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf **Neue Richtlinie**. Geben **Sie im Dialogfeld Clientlose Zugriffsrichtlinie erstellen** im Feld Name nach dem Unterstrich (_) einen Namen für die Richtlinie ein. Wählen Sie dann in Profil entweder ein vorhandenes Profil aus oder klicken Sie auf Neu, um ein neues Profil zu konfigurieren. Sie können auch ein vorhandenes Profil auswählen und dann auf **Ändern** klicken, um das Profil zu ändern.

      Weitere Informationen zum Konfigurieren einer Richtlinie oder eines Profils für clientlosen Zugriff finden Sie unter NetScaler Gateway.
    - Um eine von Ihnen eingefügte Richtlinie zu ändern, klicken Sie in der Spalte Richtlinienname auf den Richtliniennamen und dann auf **Richtlinie ändern**. Um nur das zugehörige Profil zu ändern, klicken Sie in der Spalte Profil auf den Namen des Profils und dann auf Profil ändern.
    - Um einen neuen Prioritätswert für eine Richtlinie anzugeben, doppelklicken Sie in der Spalte Priorität auf die zugewiesene Priorität, und geben Sie dann den gewünschten Wert ein.
    - Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie und dann auf **Richtlinie aufheben**.
4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von TCP-Komprimierungsrichtlinien

May 11, 2023

Sie können TCP-Komprimierungsrichtlinien für eine Anwendung konfigurieren, um die Leistung der Anwendung zu erhöhen. Die TCP-Komprimierung reduziert die Netzwerklatenz, reduziert den Bandbreitenbedarf und erhöht die Übertragungsgeschwindigkeit. Beim Konfigurieren einer TCP-Komprimierungsrichtlinie verknüpfen Sie eine Komprimierungsaktion mit der Richtlinie. Die Komprimierungsaktion gibt entweder Komprimieren, GZIP, Deflate oder NoCompress als Komprimierungstyp an. Weitere Informationen zu den Komprimierungsrichtlinien und Komprimierungsaktionen finden Sie unter NetScaler Gateway.

So konfigurieren Sie eine TCP-Komprimierungsrichtlinie für eine Ressource im Knoten NetScaler Gateway Applications

1. Erweitern Sie im Navigationsbereich der GUI **AppExpert**, und klicken Sie dann auf **Access Gateway-Anwendungen**.
2. Klicken Sie im Detailbereich in der Spalte TCP-Komprimierung auf das Symbol für die Anwendung, Dateifreigabe, das Intranet-Subnetz oder die Ressource, für die Sie eine TCP-Komprimierungsrichtlinie konfigurieren möchten.
3. Gehen Sie im Dialogfeld **TCP-Komprimierungsrichtlinien konfigurieren** wie folgt vor:
   - Um eine vorhandene TCP-Komprimierungsrichtlinie anzugeben, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf den Namen der Richtlinie.
   - Um eine neue TCP-Komprimierungsrichtlinie zu erstellen, klicken Sie auf Richtlinie einfügen, und klicken Sie dann in der Spalte Richtlinienname auf Neue Richtlinie. Geben Sie im Dialogfeld TCP-Komprimierungsrichtlinie erstellen im Feld Richtlinienname nach dem Unterstrich ("_") einen Namen für die Richtlinie ein. Wählen Sie dann in Aktion entweder eine vorhandene Aktion aus oder klicken Sie auf Neu und konfigurieren Sie eine neue Aktion. Sie können auch auf Ansicht klicken, um den konfigurierten Komprimierungstyp anzuzeigen.

     Weitere Informationen zum Konfigurieren einer TCP-Komprimierungsrichtlinie oder -aktion finden Sie unter NetScaler Gateway, Advanced Edition at NetScaler Gateway.
   - Um eine von Ihnen eingefügte Richtlinie zu ändern, klicken Sie in der Spalte Richtlinienname auf den Richtliniennamen und dann auf **Richtlinie ändern**.
   - Um die den Richtlinien zugewiesenen Prioritäten neu zu generieren, klicken Sie auf **Prioritätenneu generieren**.
   - Um einen neuen Prioritätswert für eine Richtlinie anzugeben, doppelklicken Sie in der Spalte Priorität auf die zugewiesene Priorität, und geben Sie dann den gewünschten Wert ein.
   - Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie und dann auf **Richtlinie aufheben**.
4. Klicken Sie auf **Apply Changes** und dann auf **Close**.

Bookmarks konfigurieren

June 21, 2022

Sie können Lesezeichen für interne Anwendungen oder Ressourcen konfigurieren, die für einen berechtigten Benutzer verfügbar sind. Anschließend können Sie das Lesezeichen global an einen Benutzer, eine Benutzergruppe oder einen virtuellen Server binden und es für den Benutzer im

Access Interface aktivieren. Die von Ihnen erstellten Lesezeichenverknüpfungen werden in den Website-Bereichen unter Unternehmenswebsites angezeigt.

Weitere Informationen finden Sie unter Erstellen und Anwenden von Weblinks .

AppQoE

May 11, 2023

AppQoE (Quality of Experience) auf Anwendungsebene integriert mehrere vorhandene richtlinienbasierte Sicherheitsfunktionen der NetScaler-Appliance in eine einzige integrierte Funktion, die die Vorteile eines neuen Warteschlangenmechanismus, Fair Queuing, nutzt. Fair Queuing verwaltet Anfragen an Webserver und Anwendungen mit Lastausgleich auf virtueller Serverebene statt auf Service-Ebene, sodass es vor dem Lastenausgleich die Warteschlange aller Anfragen an eine Website oder Anwendung als eine Gruppe vor dem Lastenausgleich bearbeiten kann, anstatt als separate Streams nach dem Lastausgleich.

- **Einfache Überlastung.** Jeder Server, egal wie robust, kann nur eine begrenzte Anzahl von Verbindungen gleichzeitig akzeptieren. Wenn eine geschützte Website oder Anwendung zu viele Anfragen gleichzeitig erhält, erkennt die Überspannungsschutzfunktion die Überlastung und stellt die überschüssigen Verbindungen in die Warteschlange, bis der Server sie akzeptieren kann. Die AppQoe-Funktion zeigt eine alternative Webseite an, die Benutzer darüber informiert, dass die von ihnen angeforderte Ressource nicht verfügbar ist.
- **Denial-of-Service-Angriffe (DOS).** Jede öffentlich zugängliche Ressource ist anfällig für Angriffe, deren Zweck es ist, diesen Dienst zu senken und legitimen Benutzern den Zugriff darauf zu verweigern. Die Überspannungsschutzfunktion hilft bei der Verwaltung von DOS-Angriffen zusätzlich zu anderen Arten von hoher Last. Darüber hinaus zielt die Funktion “HTTP Denial-of-Service Protection” auf DOS-Angriffe auf Ihre Websites ab, sendet Herausforderungen an mutmaßliche Angreifer und löscht Verbindungen, wenn die Clients keine entsprechende Antwort senden.

Bis zur aktuellen Version des NetScaler Betriebssystems wurden diese Features auf Service-Ebene implementiert, was bedeutet, dass jedem Dienst seine eigenen Warteschlangen zugewiesen wurden. Während Warteschlangen auf Service-Ebene funktionieren, haben sie auch einige Nachteile. Die meisten davon sind darauf zurückzuführen, dass die NetScaler-Appliance Lastausgleich vor der Implementierung der Schutzfunktionen, die auf Warteschlangen basieren, Anforderungen ausgleichen muss. Die Implementierung von Schutzfunktionen vor der Warteschlange hat verschiedene Vorteile, von denen einige unten aufgeführt sind:

- Verbindungen werden nicht geleert, wenn ein Dienst den Status wechselt, wie sie sich in einer Warteschlange auf Dienstebene befinden.

- In Zeiten hoher Belastung, wie z. B. einem Denial-of-Service-Angriff, kommen HTTP-DoS vor dem Lastenausgleich ins Spiel, sodass diese Funktionen unerwünschten oder niedrigeren Datenverkehr vom Load Balancer erkennen und umleiten können, bevor der Load Balancer damit zurechtkommen muss.

Zusätzlich zur Implementierung von Fair Queuing integriert AppQoe eine Reihe von Funktionen, die jeweils einen anderen Satz von Tools bieten, um ein gemeinsames Ziel zu erreichen: Schutz Ihrer vernetzten Ressourcen vor übermäßiger oder unangemessener Nachfrage. Wenn Sie diese Funktionen in ein gemeinsames Framework integrieren, können Sie sie einfacher konfigurieren und implementieren.

Aktivieren von AppQoE

August 19, 2021

Um AppQoE zu konfigurieren, müssen Sie zuerst die Funktion aktivieren.

So aktivieren Sie AppQoE mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- enable ns feature appqoe
- show ns feature

Beispiel:

```
> enable ns feature appqoe
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 ...
 1)     AppQoE                          AppQoE              ON
 Done
<!--NeedCopy-->
```

So aktivieren Sie AppQoE mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.

2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.
3. Aktivieren Sie im Dialogfeld **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **AppQoE**.
4. Klicken Sie auf **OK**.

AppQoE-Aktionen

May 11, 2023

Nachdem Sie die AppQoE-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen für die Bearbeitung der Anforderung konfigurieren.

> **Wichtig:**
>
> Zum Erstellen einer Aktion sind keine spezifischen individuellen Parameter erforderlich, Sie müssen jedoch mindestens einen Parameter angeben, da Sie die Aktion sonst nicht erstellen können.

So konfigurieren Sie eine AppQoE-Aktion mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appqoe action <name> [-priority <priority>] [-respondWith (ACS|NS)[<customfile>] [-altContentSvcName <string>] [-altContentPath <string>] [-maxConn <positive_integer>] [-delay <usecs>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-dosAction (**SimpleResponse** | **HICResponse**)]`
- `show appqoe action`

Beispiel

Gehen Sie wie folgt vor, um Priority-Queuing mit einer Policy-Warteschlangentiefe von 10 bzw. 1000 für Warteschlangen mit mittlerer bzw. niedrigster Priorität zu konfigurieren:

```
> add appqoe action appqoe-act-basic-prhigh -priority HIGH
 Done

> add appqoe action appqoe-act-basic-prmedium -priority MEDIUM -
    polqDepth 10
 Done

> add appqoe action appqoe-act-basic-prlow -priority LOW -polqDepth
    1000
```



```
 Done

> show appqoe action

1.       Name: appqoe-act-basic-prhigh
        ActionType: PRIORITY_QUEUING
        Priority: HIGH
        PolicyQdepth: 0
        Qdepth: 0

1.      Name: appqoe-act-basic-prmedium
        ActionType: PRIORITY_QUEUING
        Priority: MEDIUM
        PolicyQdepth: 10
        Qdepth: 0

1.      Name: appqoe-act-basic-prlow
        ActionType: PRIORITY_QUEUING
        Priority: LOW
        PolicyQdepth: 1000
        Qdepth: 0
Done
<!--NeedCopy-->
```

So ändern Sie eine vorhandene AppQoE-Aktion mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appqoe action <name> [-priority <priority>] [-altContentSvcName <string>] [-altContentPath <string>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-maxConn <positive_integer>] [-delay <usecs>] [-dosTrigExpression <expression>] [-dosAction ( SimpleResponse | HICResponse )]`
- `show appqoe action`

So entfernen Sie eine AppQoE-Aktion mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appqoe action <name>`
- `show appqoe action`

Parameter für die Konfiguration einer AppQoE-Aktion

- name. Ein Name für die neue Aktion oder der Name der vorhandenen Aktion, die Sie ändern möchten. Der Name kann mit einem Buchstaben, einer Zahl oder einem Unterstrich beginnen und aus Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen ( ), At-Zeichen (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) bestehen.
- Priorität. Die Prioritätswarteschlange, der die Anfrage zugewiesen ist. Wenn ein geschützter Webserver oder eine geschützte Anwendung stark ausgelastet ist und keine zusätzlichen Anfragen annehmen kann, gibt dies die Reihenfolge an, in der wartende Anfragen erfüllt werden müssen, wenn Ressourcen verfügbar sind. Es stehen folgende Optionen zur Auswahl:

1. **HOCH.** Erfüllt die Anfrage, sobald Ressourcen verfügbar sind.
2. **MITTEL.** Erfüllt die Anfrage, nachdem alle Anfragen in der Warteschlange mit HOHER Priorität erfüllt wurden.
3. **NIEDRIG.** Erfüllt die Anfrage, nachdem alle Anfragen in den Warteschlangen mit HOHER und MITTLERER Priorität erfüllt wurden.
4. **NIEDRIGSTE.** Erfüllt die Anfrage erst, nachdem alle Anfragen in Warteschlangen mit höherer Priorität erfüllt wurden.

Wenn die Priorität nicht konfiguriert ist, weist die NetScaler-Appliance die Anfrage standardmäßig der Warteschlange mit der NIEDRIGSTEN Priorität zu.

- Antworte mit. Konfiguriert den NetScaler so, dass er die angegebene Responder-Aktion ausführt, wenn der angegebene Schwellenwert erreicht ist. Muss mit einer der folgenden Einstellungen verwendet werden:
  - **ACS:** Bereitet Inhalte von einem alternativen Inhaltsdienst bereit. Schwellenwert: MaxConn (maximale Anzahl Verbindungen) oder Delay.
  - **NS: Bietet** eine integrierte Antwort vom NetScaler. Schwellenwert: MaxConn (maximale Anzahl Verbindungen) oder Delay.
  - **KEINE AKTION:** Es werden keine alternativen Inhalte bereitgestellt. Weist Verbindungen der Warteschlange mit der NIEDRIGSTEN Priorität zu, wenn der MaxConn- (maximale Anzahl Verbindungen) oder der Verzögerungsschwellenwert erreicht ist.
- Alt_Inhalt/SVC-Name. Wenn -ResponseWith ACS angegeben ist, ist dies der Name des alternativen Inhaltsdienstes, normalerweise eine absolute URL zu dem Webserver, der den alternativen Inhalt hostet.
- AltInhaltspfad. Wenn -ResponseWith (ACS | NS) angegeben ist, der Pfad zum alternativen Inhalt.
- OQ-Tiefe. Schwellenwert für die Tiefe der Policy-Warteschlange für die Policy-Warteschlange, die dieser Aktion zugeordnet ist. Wenn die Anzahl der Verbindungen in der Policy-Warteschlange, die dieser Aktion zugeordnet sind, auf die angegebene Anzahl ansteigt, werden nachfolgende Anfragen der NIEDRIGSTEN Policy-Warteschlange zugewiesen. Mindestwert: 1

Maximalwert: 4.294.967.294

- PRIQ-Tiefe. Schwellenwert für die Tiefe der Policy-Warteschlange für die angegebene Prioritätswarteschlange. Wenn die Anzahl der Anfragen in der angegebenen Warteschlange auf dem virtuellen Server, an den die mit der aktuellen Aktion verknüpfte Richtlinie gebunden ist, auf die angegebene Anzahl ansteigt, werden nachfolgende Anfragen der Warteschlange mit der NIEDRIGSTEN Priorität zugewiesen. Mindestwert: 1 Maximalwert: 4.294.967.294
- Max Conn. Die maximale Anzahl von Verbindungen, die für Anfragen geöffnet werden können, die der Richtlinienregel entsprechen. Mindestwert: 1 Maximalwert: 4.294.967.294
- Verzögerung. Der Verzögerungsschwellenwert in Mikrosekunden für Anfragen, die der Richtlinienregel entsprechen. Wenn eine übereinstimmende Anforderung länger als der Schwellenwert verzögert wurde, führt die
  NetScaler-Appliance die angegebene Aktion aus. Wenn KEINE AKTION angegeben ist, weist die Appliance Anfragen der Warteschlange mit der NIEDRIGSTEN Priorität zu. Mindestwert: 1 Maximalwert: 599999.999
- Dostrige-Ausdruck. Fügt eine optionale Prüfung der zweiten Ebene hinzu, um DoS-Aktionen auszulösen.
- DOS-Aktion. Maßnahmen, die ergriffen werden müssen, wenn die Appliance feststellt, dass sie oder ein geschützter Server einem DoS-Angriff ausgesetzt ist. Mögliche Werte: SimpleResponse, HicResponse.

Diese Werte spezifizieren HTTP-Challenge-Response-Methoden zur Überprüfung der Authentizität eingehender Anfragen, um einen HTTP-DDoS-Angriff abzuwehren.

Bei der Generierung und Validierung von HTTP-Challenge-Response verwendet AppQoE Cookies, um die Antwort des Clients zu validieren und zu überprüfen, ob der Client echt zu sein scheint. Beim Senden einer Herausforderung generiert eine NetScaler-Appliance zwei Cookies:

Header-Cookie (_DOSQ). Enthält clientspezifische Informationen, sodass die NetScaler-Appliance die Antwort überprüfen kann.

Körperkeks (_DOSH). Informationen, die zur Validierung des Client-Computers verwendet wurden. Der Browser des Clients (oder der Benutzer, im Fall von HIC) berechnet einen Wert für dieses Cookie. Die NetScaler-Appliance vergleicht diesen Wert mit dem erwarteten Wert, um den Client zu verifizieren.

Die Informationen, die die Appliance zur Berechnung des _DOSH-Werts an den Client sendet, basieren auf der DoS-Aktionskonfiguration.

1. SimpleResponse: In diesem Fall teilt eine NetScaler-Appliance den Wert auf und generiert einen JavaScript-Code, um den endgültigen Wert zu kombinieren. Ein Client-Computer, der in der Lage ist, den ursprünglichen Wert zu berechnen, gilt als echt.

2. HICResponse: In diesem Fall generiert eine NetScaler-Appliance zwei einstellige Zahlen und generiert Bilder für diese Zahlen. Dann fügt die Appliance mithilfe eines Backpatch-Frameworks diese Images als Base64-Zeichenketten ein.

Einschränkungen

1. Dies ist keine triviale CAPTCHA-Implementierung, weshalb dieser Begriff nicht verwendet wird.
2. Die Validierungsnummer basiert auf einer von NetScaler generierten Zahl, die sich 120 Sekunden lang nicht ändert. Diese Nummer sollte dynamisch oder kundenspezifisch sein.

So konfigurieren Sie eine AppQoE-Aktion mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **App-Expert** > **AppQoE** > **Actions.**
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben **Sie im Bildschirm AppQoE-Aktion erstellen** oder **AppQoE-Aktion konfigurieren** Werte für die Parameter ein, oder wählen Sie sie aus. Der Inhalt des Dialogfelds entspricht den unter „Parameter für die Konfiguration der AppQoE-Aktion“ beschriebenen Parametern wie folgt (ein Sternchen gibt einen erforderlichen Parameter an):
   - Name—Name
   - Aktionstyp — Antworten mit
   - Priorität — Priorität
   - Tiefe der Richtlinienwarteschlange — POLQDepth
   - Warteschlangentiefe — PriqDepth
   - DOS-Aktion — DOS-Aktion
4. Klicken Sie auf **Erstellen** oder **auf OK**.

AppQoE-Parameter

January 19, 2021

In den AppQoE-Parametern konfigurieren Sie die Sitzungsdauer einer AppQoE-Sitzung, den Dateinamen der Datei, die die angepasste Antwort enthält, und die Anzahl der Clientverbindungen, die in einer Warteschlange platziert werden können.

So konfigurieren Sie die AppQoE-Parametereinstellungen mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appqoe parameter [-sessionLife <secs>] [-avgwaitingclient <positive_integer>] [-MaxAltRespBandWidth <positive_integer>] [-dosAttackThresh <positive_integer>]`
- `show appqoe parameter`

Parameter für die Konfiguration der AppQoE-Parameter

- sessionLife

  Anzahl der Sekunden, die nach der Anzeige alternativer Inhalte gewartet werden müssen, bevor die Appliance denselben Inhalt erneut anzeigt. Standardwert: 300 Maximum Minimalwert: 1 Maximaler Wert: 4.294.967.294

- avgwaitingclient

  Die durchschnittliche Anzahl von Clientanforderungen, die sich in der Warteschlange des Dienstes befinden können. Standardwert: 1000000 Maximalwert: 4.294.967.294

- MaxAltRespBandWidth

  Die maximale Bandbreite, die beim Senden alternativer Antworten benötigt wird. Wenn das Maximum erreicht ist, beendet die Appliance das Senden des alternativen Inhalts, bis der Bandbreitenverbrauch sinkt. Standardwert: 100 Mindestwert: 1 Maximaler Wert: 4.294.967.294

- dosAtckThrsh

  Der Denial-of-Service-Angriffsschwellenwert. Die Anzahl der Verbindungen, die in Warteschlangen warten müssen, bevor die Appliance mit DoS-Schutzmaßnahmen reagiert. Standardwert: 2000 Mindestwert: 0 Maximaler Wert: 4.294.967.294

So konfigurieren Sie die AppQoE-Parametereinstellungen mit der GUI

1. Navigieren Sie zu **AppExpert** > **AppQoe**.
2. Klicken Sie im Detailbereich auf **AppQoE -Parameter konfigurieren**.
3. Geben Sie im Bildschirm **AppQoE-Parameter konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus. Der Inhalt des Dialogfensters entspricht den unter Parameter zur Konfiguration der AppQoE-Parameter beschriebenen Parametern wie folgt (Sternchen gibt einen erforderlichen Parameter an):
   - Sitzungsdauer (Sekunden)
   - sessionLife
   - Durchschnitt Clientwarten — avgwaitingclient

- Begrenzung der alternativen Antwortbandbreite (Mbit/s) — MaxAltRespBandWidth
- DOS-Angriffsschwelle —dosAttackThresh

4. Klicken Sie auf **OK**.

AppQoE-Richtlinien

May 11, 2023

Um AppQoE zu implementieren, müssen Sie mindestens eine Richtlinie konfigurieren, die Ihrem NetScaler mitteilt, wie die Verbindungen in einer bestimmten Warteschlange unterschieden werden sollen.

So konfigurieren Sie eine AppQoE-Richtlinie mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Beispiel:

Das folgende Beispiel wählt Anfragen mit einem User-Agent-Header aus, der „Android“ enthält, und weist sie der Warteschlange mit mittlerer Priorität zu. Diese Anfragen kommen von Smartphones und Tablets, auf denen das Google Android-Betriebssystem ausgeführt wird.

```
1  > add appqoe action appqoe-act-primd -priority MEDIUM
2  Done
3  > add appqoe policy appqoe-pol-primd -rule "HTTP.REQ.HEADER("User-Agent
       ").CONTAINS("Android")" -action appqoe-act-primd
4  Done
5  > sh appqoe policy appqoe-pol-primd
6          Name: appqoe-pol-primd
7          Rule: HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")
8          Action: appqoe-act-primd
9          Hits: 0
10
11 Done
12 <!--NeedCopy-->
```

Parameter für die Konfiguration einer AppQoE-Richtlinie

- name. Ein Name für die AppQoE-Richtlinie. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und aus einem bis 127 Buchstaben, Zahlen und den Symbolen

Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), At-Zeichen (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) bestehen. Sie sollten einen Namen wählen, anhand dessen die Art der Aktion identifiziert werden kann.

- Regel. Ein NetScaler-Ausdruck, der der Appliance mitteilt, welche Verbindungen sie verarbeiten soll.
- Aktion. Die AppQoE-Aktion, die ausgeführt werden soll, wenn eine Verbindung der Richtlinie entspricht.

So konfigurieren Sie eine AppQoE-Richtlinie mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **App-Expert** > **AppQoE** > **Policies**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus und klicken dann auf **Bearbeiten**.
3. Wenn Sie eine Richtlinie **erstellen, geben Sie im Dialogfeld AppQoE-Richtlinie** erstellen im Textfeld Name einen Namen für Ihre neue Richtlinie ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und aus einem bis 127 Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), At-Zeichen (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) bestehen. Sie sollten einen Namen wählen, der hilft, den Zweck und die Wirkung dieser Richtlinie zu identifizieren.

   Wenn Sie eine bestehende Richtlinie ändern, überspringen Sie diesen Schritt. Sie können den Namen einer vorhandenen Richtlinie nicht ändern.
4. Wählen Sie in der Dropdownliste **Aktion** die AppQoE-Aktion aus, die ausgeführt werden soll, wenn die Richtlinie einer Verbindung entspricht. Klicken Sie auf das Pluszeichen (+), um das Dialogfeld **AppQoE-Aktion hinzufügen** zu öffnen und eine neue Aktion hinzuzufügen.
5. Geben Sie in das Textfeld **Regel** entweder direkt den Richtlinienausdruck ein, oder klicken Sie auf Neu, um einen Richtlinienausdruck zu erstellen. Wenn Sie auf Neu klicken, gehen Sie wie folgt vor:

   a) Klicken **Sie im Dialogfeld Ausdruck erstellen** auf **Hinzufügen**.
   1 Wählen **Sie im Dialogfeld Ausdruck hinzufügen** einen gemeinsamen Ausdruck aus der Dropdownliste **Häufig verwendete Ausdrücke** aus, oder verwenden Sie die Dropdownlisten Ausdruck **erstellen, um den Ausdruck** zu erstellen, der definiert, welcher Datenverkehr gefiltert werden soll.
   Wenn Sie einen eigenen Ausdruck erstellen möchten, wählen Sie zunächst den ersten Be-

griff aus der ersten Dropdownliste auf der linken Seite des Bereichs “Ausdruck konstruieren” aus. In dieser Liste stehen folgende Optionen zur Auswahl:

- HTTP
- SYS
- CLIENT
- SERVER
- ANALYTICS
- TEXT

Die Standardauswahl ist HTTP. Nachdem Sie in der ersten Dropdownliste eine Auswahl getroffen haben (oder die Standardeinstellung akzeptiert haben), können Sie den nächsten Begriff in Ihrem Ausdruck aus der Dropdownliste rechts davon auswählen. Die Begriffe in dieser Liste und den folgenden Listen ändern sich je nach Ihrer vorherigen Auswahl. Die Listen enthalten nur Begriffe, bei denen es sich um gültige Optionen handelt. Wählen Sie so lange Begriffe aus, bis Sie den Ausdruck abgeschlossen haben.

a) Wenn Sie den gewünschten Ausdruck erstellt haben, klicken Sie auf **OK**. Der Ausdruck wird in das Textfeld **Ausdruck** eingefügt.

6. Klicken Sie auf **Erstellen**. Der Ausdruck wird im Textfeld **Regel** angezeigt.

Entitätsvorlage für den Lastausgleich virtueller Server

May 11, 2023

> **Warnung**
>
> Die Funktionalität der Entitätsvorlage ist ab NetScaler 13.0 Build 82.x veraltet und empfiehlt Citrix alternativ, die Style Books zu verwenden. Weitere Informationen finden Sie unter Thema Stilbücher .

Eine Entitätsvorlage ist eine Sammlung von Informationen zum Erstellen einer Vorlage für den Lastausgleich eines virtuellen Servers auf einer NetScaler Appliance. Es enthält eine Spezifikation und eine Reihe von Standardeinstellungen, die für einen virtuellen Lastausgleichsserver konfiguriert werden können. Mithilfe einer Vorlage, die eine Reihe von Standardeinstellungen definiert, können Sie schnell mehrere virtuelle Server konfigurieren, für die eine ähnliche Konfiguration erforderlich ist, und gleichzeitig mehrere Konfigurationsschritte überflüssig machen.

Sie können eine Entitätsvorlage erstellen, indem Sie die Details des virtuellen Load-Balancing-Servers in eine Vorlagendatei exportieren. Dies ist nur über die NetScaler-GUI möglich. Sie verwenden die NetScaler-GUI, um Entitätsvorlagen zu exportieren, zu importieren und zu verwalten. Sie können Entitätsvorlagen mit anderen Administratoren teilen und lokal auf Ihrer Appliance oder Ihrem Computer

gespeicherte Vorlagen verwalten. Sie können Entitätsvorlagen auch von der Appliance oder Ihrem lokalen Computer importieren.

Bevor Sie eine Vorlage erstellen, sollten Sie mit der Konfiguration des virtuellen Load-Balancing-Servers vertraut sein.

Vorlage für virtuellen Load-Balancing-Server

Vorlagen für Load Balancing-Entitäten werden auf dieselbe Weise erstellt wie NetScaler-Anwendungsvorlagen. Wenn Sie einen virtuellen Load Balancing-Server in eine Vorlagendatei exportieren, werden die folgenden beiden Dateien automatisch erstellt:

- Vorlagendatei für den virtuellen Load-Balancing-Server. Enthält XML-Elemente, die die Werte der Parameter speichern, die für den virtuellen Load Balancing-Server konfiguriert sind. Die Datei enthält auch XML-Elemente zum Speichern von Informationen über gebundene Richtlinien.
- Bereitstellungsdatei. Enthält XML-Elemente, die bereitstellungsspezifische Informationen wie Dienste, Dienstgruppen und konfigurierte Variablen speichern.
  In den Vorlagen- und Bereitstellungsdateien ist jede Einheit der Konfigurationsinformationen in einem bestimmten XML-Element gekapselt, das für diesen Einheitentyp bestimmt ist. Der Parameter für die Load-Balancing-Methode, lbMethod, ist beispielsweise in den Tags <lbmethod> und </lbmethod> eingekapselt.

> **Hinweis:**
>
> Nachdem Sie einen virtuellen Load-Balancing-Server exportiert haben, können Sie Elemente hinzufügen, Elemente entfernen und vorhandene Elemente ändern, bevor Sie die Konfigurationsinformationen in eine NetScaler-Appliance importieren.

So funktioniert eine Vorlage für einen virtuellen Load-Balancing-Server

Wenn Sie eine Vorlage für einen virtuellen Lastausgleichsserver erstellen, geben Sie Standardwerte für den Server an. Sie geben an, welche Werte schreibgeschützt sein müssen, welche Werte nicht angezeigt werden dürfen und welche Werte Benutzer konfigurieren können. Sie konfigurieren auch die Seiten, aus denen der Vorlagenimport-Assistent besteht. Alle Informationen und Einstellungen, die Sie angeben, werden in der Vorlagendatei gespeichert.
Wenn ein Benutzer die Vorlage in eine NetScaler-Appliance importiert, führt die GUI den Benutzer durch die verschiedenen Seiten, die Sie für die Vorlage konfiguriert haben. Die GUI zeigt die schreibgeschützten Parameterwerte an und fordert den Benutzer auf, Werte für die konfigurierbaren Parameter anzugeben. Nachdem der Benutzer die Anweisungen befolgt hat, erstellt die Appliance die Entität mit den konfigurierten Werten.

Sie können eine Entitätsvorlage für einen virtuellen Lastausgleichsserver vom Knoten Traffic Management aus erstellen oder ändern.
Um Details des virtuellen Servers in eine Vorlage zu exportieren, müssen Sie die folgenden Optionen und Einstellungen für die Vorlage angeben:

- Der Standardwert eines Parameters.
- Ob die Standardwerte für Benutzer sichtbar sind.
- Ob die Standardwerte von Benutzern geändert werden können.
- Die Anzahl der Seiten im Assistenten zum Importieren von Entitäten, einschließlich der Seitennamen, des Textes und der verfügbaren Parameter.
- Die Entitäten, die an die Entität gebunden sein müssen, für die die Vorlage erstellt wird.

Wenn Sie beispielsweise eine Vorlage für einen virtuellen Lastausgleichsserver erstellen, können Sie die Richtlinien angeben, die Sie an den virtuellen Server binden möchten, den Sie anhand der Vorlage erstellen. In der Vorlage sind jedoch nur verbindliche Informationen enthalten. Die gebundenen Entitäten sind nicht enthalten. Wenn die Entitätsvorlage in eine andere NetScaler-Appliance importiert wird, müssen die gebundenen Entitäten zum Zeitpunkt des Imports auf der Appliance vorhanden sein, damit die Bindung erfolgreich ist. Wenn keine der gebundenen Entitäten auf der Ziel-Appliance vorhanden ist, wird die Entität (für die die Vorlage konfiguriert wurde) ohne Bindungen erstellt. Wenn nur eine Teilmenge der gebundenen Entitäten auf der Ziel-Appliance vorhanden ist, sind sie an die Entität gebunden, die aus der Vorlage erstellt wurde.
Wenn Sie eine Vorlage für den virtuellen Load Balancing-Server exportieren, werden die Konfigurationseinstellungen der Entität in der Vorlage angezeigt. Alle gebundenen Entitäten sind standardmäßig ausgewählt, aber Sie können die Bindungen nach Bedarf ändern. Wie bei einer Vorlage, die nicht auf einer bestehenden Entität basiert, sind nur verbindliche Informationen enthalten und nicht die Entitäten. Sie können die Vorlage entweder mit den vorhandenen Konfigurationseinstellungen speichern oder die Einstellungen als Grundlage verwenden, um eine neue Konfiguration für eine Vorlage zu erstellen.

Konfigurieren Sie Variablen in der Vorlage für virtuelle Load-Balancing-Server

Vorlagen für virtuelle Lastausgleichsserver unterstützen die Deklaration von Variablen in den konfigurierten Lastausgleichsparametern sowie in gebundenen Richtlinien und Aktionen. Die Fähigkeit, Variablen zu deklarieren, ermöglicht es Ihnen, vorkonfigurierte Werte durch Werte zu ersetzen, die zu der Umgebung passen, in die Sie die Vorlage importieren.

Stellen Sie sich als Beispiel den folgenden Ausdruck vor, der für eine Richtlinie konfiguriert ist, die an einen virtuellen Lastausgleichsserver gebunden ist, für den Sie eine Vorlage erstellen. Der Ausdruck wertet den Wert des Accept-Language-Headers in einer HTTP-Anfrage aus.

```
HTTP.REQ.HEADER("Accept-Language").CONTAINS("en-us")
```

Wenn Sie möchten, dass der Wert des Headers beim Import konfigurierbar ist, können Sie die Zeichen-

folge en-us als Variable angeben.

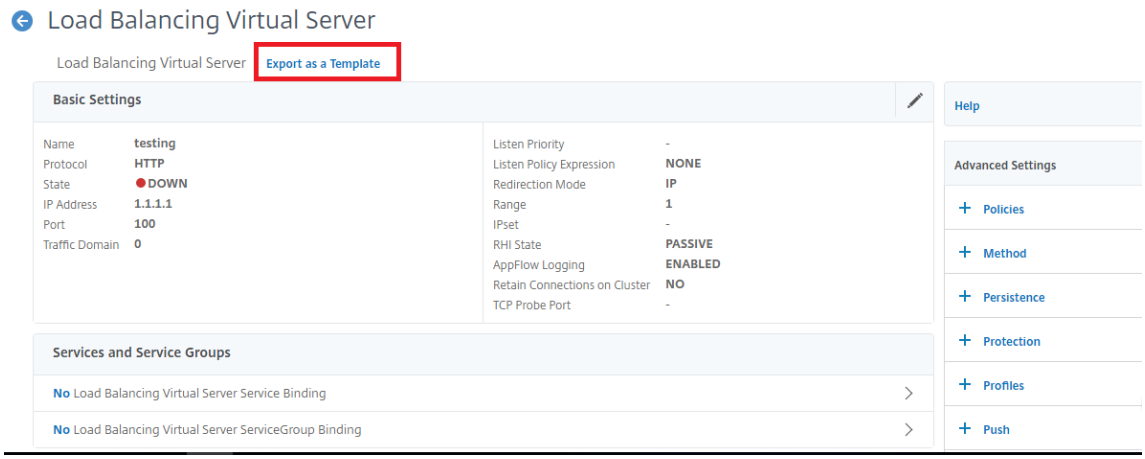
Nachdem Sie eine Variable erstellt haben, können Sie Folgendes tun:

- Weisen Sie einer vorhandenen Variablen mehr Strings zu. Nachdem Sie eine Variable für eine Zeichenfolge erstellt haben, können Sie andere Teile desselben oder eines anderen Ausdrucks auswählen und der Variablen zuweisen. Die Zeichenketten, die Sie einer Variablen zuweisen, müssen nicht dieselben sein. Beim Import werden alle Zeichenketten, die der Variablen zugewiesen sind, durch den von Ihnen angegebenen Wert ersetzt.
- Zeigt die Zeichenfolge oder Zeichenketten an, die der Variablen zugewiesen sind.
- Sehen Sie sich eine Liste aller Entitäten und Parameter an, die die Variable verwenden

So konfigurieren Sie Variablen in einer Vorlage für einen virtuellen Load-Balancing-Server

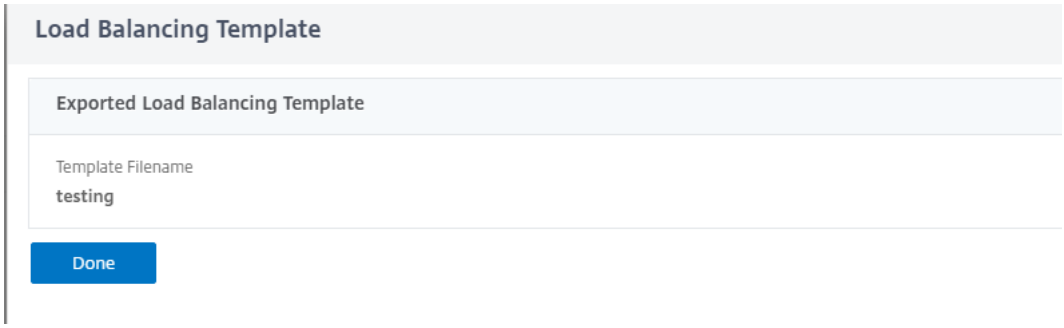
Gehen Sie wie folgt vor, um Variablen für eine Vorlage für einen virtuellen Load-Balancing-Server mithilfe der NetScaler-GUI zu konfigurieren.

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf den virtuellen Server, den Sie in eine Vorlagendatei exportieren möchten, und klicken Sie dann auf **Hinzufügen**.
3. Legen Sie auf der Seite **Virtueller Load Balancing Server erstellen** die Parameter des virtuellen Servers fest. Weitere Informationen zum Konfigurieren eines virtuellen Lastausgleichsservers finden Sie unter Funktionsweise des Lastenausgleichs
4. Wenn Sie die Parameter für den virtuellen Lastausgleichsserver festgelegt haben, klicken Sie auf **Fertig**.



5. Klicken Sie oben auf den Link **Als Vorlage** exportieren, um die Serverdetails als Vorlagendatei zu exportieren.
6. Geben Sie auf der Seite „ **Load Balancing-Vorlage erstellen** “ die Vorlageneinstellungen ein.

7. Klicken Sie auf **Fertig**.



Ändern Sie eine Vorlage für einen virtuellen Load-Balancing-Server

Sie können nur die Parameter, Bindungen und Seiten ändern, die für eine Vorlage konfiguriert wurden. Der Name und Speicherort der Vorlage, die bei der Erstellung der Vorlage angegeben wurden, können nicht geändert werden. Die NetScaler-Appliance bietet Ihnen nicht die Möglichkeit, eine Vorlage für einen virtuellen Load-Balancing-Server zu ändern.

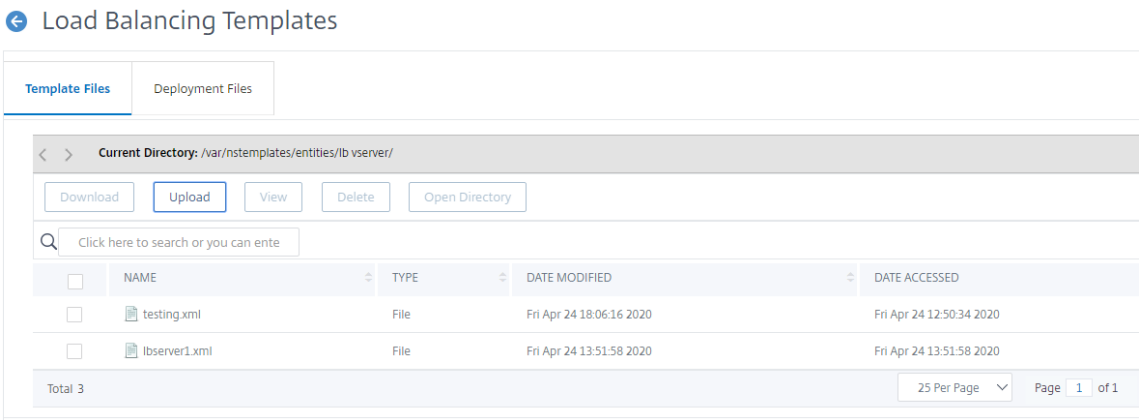
So ändern Sie einen virtuellen Lastausgleichsserver mithilfe der NetScaler-GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Ändern Sie auf der Seite **Load Balancing Virtual Server** die Entitätsparameter.
3. Klicken Sie auf Fertig.
4. Klicken Sie auf den Link **Als Vorlage exportieren** .
5. Die geänderten Änderungen sind jetzt in der Vorlagendatei für den virtuellen Load-Balancing-Server verfügbar.
6. Klicken Sie auf der Seite „ **Exportierte Load Balancing-Vorlage** “ auf **Fertig**.

Vorlagen für virtuelle Load-Balancing-Server verwalten

Mithilfe der NetScaler-GUI können Sie Vorlagendateien für virtuelle Server und Bereitstellungsdateien für den Lastausgleich organisieren.

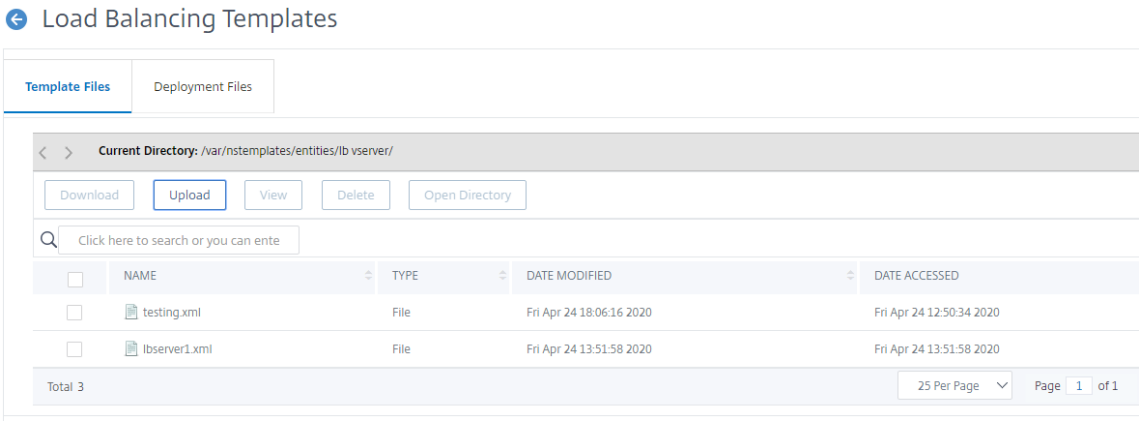
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie auf der Seite **Virtuelle Server** die **Aktion Vorlage verwalten**aus.
3. Klicken Sie auf der Seite **Load Balancing-Vorlagen** auf die Registerkarte **Vorlagendatei** .
4. Auf der Registerkarte **Vorlagendateien** können Sie eine Vorlage aus dem und in den Vorlagenordner der Appliance hochladen oder herunterladen.



5. Klicken Sie auf **Schließen**.

So laden Sie mithilfe der NetScaler-GUI eine Vorlage für virtuelle Serverentitäten für den Lastenausgleich hoch

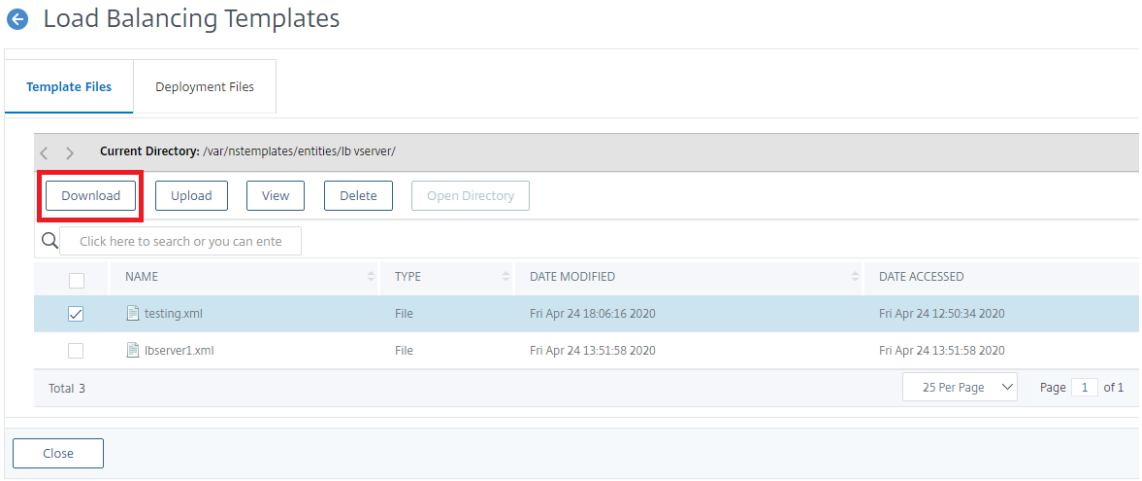
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie auf der Seite **Virtuelle Server** auf **Aktion auswählen** und wählen Sie dann **Vorlage verwalten**aus.
3. Klicken Sie auf der Seite Load Balancing-Vorlagen auf die Registerkarte **Vorlagendateien** .
4. Klicken Sie auf der Registerkarte **Vorlagendateien** auf **Hochladen**, um eine Vorlage hochzuladen.
5. Klicken Sie auf **Schließen**.



So laden Sie die Vorlage für Load Balancing-Serverentitäten mithilfe der NetScaler-GUI herunter

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.

2. Klicken Sie auf der Seite **Virtuelle Server** auf **Aktion auswählen** und wählen Sie dann **Vorlage verwalten**aus.
3. Klicken Sie auf der Seite **Load Balancing-Vorlagen** auf die Registerkarte **Vorlagendateien** .
4. Wählen Sie auf der Registerkarte Vorlagendateien eine Vorlagendatei aus und klicken Sie auf Herunterladen.
5. Klicken Sie auf Schließen.



Beispiel für eine Vorlage für einen virtuellen Load Balancing-Server und eine Bereitstellungsvorlage

Im Folgenden finden Sie ein Beispiel für eine Vorlagendatei, die von einem virtuellen Load-Balancing-Server namens „Lbvip“ erstellt wurde:

```
COPY

<?xml version="1.0" encoding="UTF-8" ?>
  <template>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <entitytemplate>
      <lbvserver_list>
        <lbvserver>
          <name>Lbvip</name>
          <servicetype>HTTP</servicetype>
          <ipv46>0.0.0.0</ipv46>
```



```
            <ipmask>*</ipmask>
            <port>0</port>
            <range>1</range>
            <persistencetype>NONE</persistencetype>
            <timeout>2</timeout>
            <persistencebackup>NONE</persistencebackup>
            <backuppersistencetimeout>2</backuppersistencetimeout>
            <lbmethod>LEASTCONNECTION</lbmethod>
            <persistmask>255.255.255.255</persistmask>
            <v6persistmasklen>128</v6persistmasklen>
            <pq>OFF</pq>
            <sc>OFF</sc>
            <m>IP</m>
            <datalength>0</datalength>
            <dataoffset>0</dataoffset>
            <sessionless>DISABLED</sessionless>
            <state>ENABLED</state>
            <connfailover>DISABLED</connfailover>
            <clttimeout>180</clttimeout>
            <somethod>NONE</somethod>
            <sopersistence>DISABLED</sopersistence>
            <sopersistencetimeout>2</sopersistencetimeout>
            <redirectportrewrite>DISABLED</redirectportrewrite>
            <downstateflush>DISABLED</downstateflush>
            <gt2gb>DISABLED</gt2gb>
            <ipmapping>0.0.0.0</ipmapping>
            <disableprimaryondown>DISABLED</disableprimaryondown>
            <insertvserveripport>OFF</insertvserveripport>
            <authentication>OFF</authentication>
            <authn401>OFF</authn401>
            <push>DISABLED</push>
            <pushlabel>none</pushlabel>
            <l2conn>OFF</l2conn>
            <appflowlog>DISABLED</appflowlog>
            <icmpvsrresponse>PASSIVE</icmpvsrresponse>
            <lbvserver_cmppolicy_binding_list>
              <lbvserver_cmppolicy_binding>
                <name>Lbvip</name>
                <policyname>NOPOLICY-COMPRESSION</policyname>
                <priority>100</priority>
                <gotopriorityexpression>END</gotopriorityexpression>
                <bindpoint>REQUEST</bindpoint>
              </lbvserver_cmppolicy_binding>
            </lbvserver_cmppolicy_binding_list>
          </lbvserver>
```



```
      </lbvserver_list>
    </entitytemplate>
  </template>
<!--NeedCopy-->
```

Beispiel für eine Deployment-Datei

Im vorangegangenen Beispiel folgt die Bereitstellungsdatei, die dem virtuellen Server zugeordnet ist:
COPY

```
<?xml version="1.0" encoding="UTF-8" ?>
  <template_deployment>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <service_list>
      <service>
      <ip>1.2.3.4</ip>
      <port>80</port>
      <servicetype>HTTP</servicetype>
      </service>
    </service_list>
    <servicegroup_list>
      <servicegroup>
        <name>svcgrp</name>
        <servicetype>HTTP</servicetype>
        <servicegroup_servicegroupmember_binding_list>
          <servicegroup_servicegroupmember_binding>
            <ip>1.2.3.90</ip>
            <port>80</port>
          </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.0</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.8.1</ip>
          <port>80</port>
        </servicegroup_servicegroupmember_binding>
        <servicegroup_servicegroupmember_binding>
          <ip>1.2.9.0</ip>
```



```
            <port>80</port>
          </servicegroup_servicegroupmember_binding>
        </servicegroup_servicegroupmember_binding_list>
      </servicegroup>
    </servicegroup_list>
</template_deployment>

<!--NeedCopy-->
```

HTTP-Callouts

May 11, 2023

Für bestimmte Arten von Anforderungen oder wenn bestimmte Kriterien während der Richtlinienbewertung erfüllt werden, möchten Sie möglicherweise die Richtlinienbewertung kurz unterdrücken, Informationen von einem Server abrufen und dann eine bestimmte Aktion ausführen, die von den abgerufenen Informationen abhängt. Zu anderen Zeiten, wenn Sie bestimmte Arten von Anfragen erhalten, möchten Sie möglicherweise eine Datenbank oder den auf einem Webserver gehosteten Inhalt aktualisieren. Mit HTTP-Callouts können Sie all diese Aufgaben ausführen.

Ein HTTP-Callout ist eine HTTP- oder HTTPS-Anforderung, die die NetScaler-Appliance generiert und an eine externe Anwendung sendet, wenn bestimmte Kriterien während der Richtlinienbewertung erfüllt werden. Die Informationen, die vom Server abgerufen werden, können durch erweiterte Richtlinienausdrücke analysiert und eine entsprechende Aktion durchgeführt werden. Sie können HTTP-Callouts für HTTP-Content Switching, TCP-Content Switching, Rewrite, Responder und für die tokenbasierte Methode des Lastausgleichs konfigurieren.

Bevor Sie ein HTTP-Callout konfigurieren, müssen Sie eine Anwendung auf dem Server einrichten, an die das Callout gesendet wird. Die Anwendung, die als *HTTP-Callout-Agent* bezeichnet wird, muss so konfiguriert sein, dass sie auf die HTTP-Callout-Anforderung mit den erforderlichen Informationen antwortet. Der HTTP-Callout-Agent kann auch ein Webserver sein, der die Daten bereitstellt, für die die NetScaler-Appliance das Callout sendet. Sie müssen sicherstellen, dass sich das Format der Antwort auf einen HTTP-Callout nicht von einem Aufruf zum anderen ändert.

Nachdem Sie den HTTP-Callout-Agent eingerichtet haben, konfigurieren Sie das HTTP-Callout auf der NetScaler-Appliance. Um das Callout aufzurufen, fügen Sie das Callout in eine erweiterte Richtlinie in die entsprechende NetScaler-Funktion ein und binden die Richtlinie dann an den Bindepunkt, an dem die Richtlinie ausgewertet werden soll.

Nachdem Sie den HTTP-Callout konfiguriert haben, müssen Sie die Konfiguration überprüfen, um sicherzustellen, dass das Callout ordnungsgemäß funktioniert.

So funktioniert ein HTTP-Callout

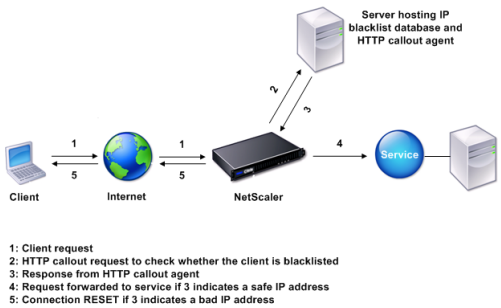
May 11, 2023

Wenn die NetScaler-Appliance eine Client-Anfrage empfängt, wertet die Appliance die Anfrage anhand der Richtlinien aus, die an verschiedene Bindungspunkte gebunden sind. Wenn die Appliance während dieser Bewertung auf den HTTP-Callout-Ausdruck trifft `SYS.HTTP_CALLOUT(<name>)`, stoppt sie die Richtlinienauswertung kurz und sendet eine Anfrage an den HTTP-Callout-Agenten, indem sie die für das angegebene HTTP-Callout konfigurierten Parameter verwendet. Nach Erhalt der Antwort überprüft die Appliance den angegebenen Teil der Antwort und führt dann entweder eine Aktion aus oder wertet die nächste Richtlinie aus, je nachdem, ob die Auswertung der Antwort des HTTP-Callout-Agenten TRUE bzw. FALSE ergibt. Wenn das HTTP-Callout beispielsweise in einer Responder-Richtlinie enthalten ist und die Auswertung der Antwort den Wert TRUE ergibt, führt die Appliance die mit der Responder-Richtlinie verknüpfte Aktion aus.

Wenn die HTTP-Callout-Konfiguration falsch oder unvollständig ist oder wenn sich das Callout rekursiv selbst aufruft, löst die Appliance eine UNDEF-Bedingung aus und aktualisiert den Zähler für undefinierte Treffer.

Die folgende Abbildung zeigt die Funktionsweise eines HTTP-Callouts, das von einer global gebundenen Responder-Richtlinie aus aufgerufen wird. Das HTTP-Callout ist so konfiguriert, dass es die IP-Adresse des Clients enthält, die einer eingehenden Anfrage zugeordnet ist. Wenn die NetScaler-Appliance eine Anfrage von einem Client empfängt, generiert die Appliance die Callout-Anforderung und sendet sie an den Callout-Server, der eine Datenbank mit IP-Adressen auf der schwarzen Liste hostet, und einen HTTP-Callout-Agent, der überprüft, ob die IP-Adresse des Clients in der Datenbank aufgeführt ist. Der HTTP-Callout-Agent empfängt die Callout-Anforderung, überprüft, ob die IP-Adresse des Clients aufgeführt ist, und sendet eine Antwort, die von der NetScaler-Appliance ausgewertet wird. Wenn die Antwort darauf hinweist, dass die IP-Adresse des Clients nicht auf der schwarzen Liste steht, leitet die Appliance die Antwort an den konfigurierten Dienst weiter. Wenn die IP-Adresse des Clients auf der schwarzen Liste steht, setzt die Appliance die Client-Verbindung zurück

Abbildung 1. HTTP-Callout-Entitätsmodell



Hinweise zum Format von HTTP-Anfragen und -Antworten

May 11, 2023

Die NetScaler-Appliance überprüft nicht, ob die HTTP-Callout-Anforderung gültig ist. Bevor Sie HTTP-Callouts konfigurieren, müssen Sie daher das Format einer HTTP-Anfrage kennen. Sie müssen auch das Format einer HTTP-Antwort kennen, da die Konfiguration eines HTTP-Callouts die Konfiguration von Ausdrücken beinhaltet, die die Antwort des HTTP-Callout-Agenten auswerten.

Dieser Abschnitt umfasst die folgenden Abschnitte:

- Format einer HTTP-Anfrage
- Format einer HTTP-Antwort

Format einer HTTP-Anfrage

Eine HTTP-Anfrage enthält eine Reihe von Zeilen, die jeweils mit einem Carrier-Return und einem Zeilenvorschub enden, der als eine der beiden dargestellt wird `<CR><LF> or \r\n`.

Die erste Zeile einer Anfrage (die *Nachrichtenzeile*) enthält die HTTP-Methode und das Ziel. Eine Meldungszeile für eine GET-Anfrage enthält beispielsweise das Schlüsselwort GET und eine Zeichenfolge, die das Objekt darstellt, das abgerufen werden soll, wie im folgenden Beispiel gezeigt:

```
GET /mysite/mydirectory/index.html HTTP/1.1\r\n
<!--NeedCopy-->
```

Der Rest der Anfrage enthält HTTP-Header, einschließlich eines erforderlichen Host-Headers und gegebenenfalls eines Nachrichtentexts.

Die Anfrage endet mit einer Bankverbindung (eine zusätzliche Bankverbindung `<CR><LF> or \r\n`).

Es folgt ein Beispiel für eine Anfrage:

```
Get /mysite/index.html HTTP/1.1\r\n
Host: 10.101.101.10\r\n
Accept: \*/\*\r\n
\r\n
<!--NeedCopy-->
```

Format einer HTTP-Antwort

Eine HTTP-Antwort enthält eine Statusmeldung, Antwort-HTTP-Header und das angeforderte Objekt oder, falls das angeforderte Objekt nicht bereitgestellt werden kann, eine Fehlermeldung.

Es folgt ein Beispiel für eine Antwort:

```
HTTP/1.1 200 OK\r\n
Content-Length: 55\r\n
Content-Type: text/html\r\n
Last-Modified: Wed, 12 Aug 1998 15:03:50 GMT\r\n
Accept-Ranges: bytes\r\n
ETag:  “04f97692cbd1:377” \r\n
Date: Thu, 19 Jun 2008 19:29:07 GMT\r\n
\r\n
<55-character response>
<!--NeedCopy-->
```

Konfigurieren eines HTTP-Callouts

May 11, 2023

Bei der Konfiguration eines HTTP-Callouts geben Sie den Typ der Anforderung (HTTP oder HTTPS), das Ziel und das Format der Anforderung an. Das erwartete Format der Antwort und schließlich der Teil der Antwort, den Sie analysieren möchten.

Für das Ziel geben Sie entweder die IP-Adresse und den Port des HTTP-Callout-Agenten an. Oder betreiben Sie einen Lastenausgleich, einen Content Switching oder einen virtuellen Cache-Umleitungsserver, um die HTTP-Callout-Anforderungen zu verwalten.

Im ersten Fall werden die HTTP-Callout-Anfragen direkt an den HTTP-Callout-Agent gesendet. Im zweiten Fall werden die HTTP-Callout-Anfragen an die virtuelle IP-Adresse (VIP) des angegebenen virtuellen Servers gesendet. Der virtuelle Server verarbeitet die Anforderung auf die gleiche Weise, wie er eine Clientanforderung verarbeitet. Wenn Sie beispielsweise erwarten, dass viele Callouts generiert werden, können Sie Instanzen des HTTP-Callout-Agenten auf mehreren Servern konfigurieren, diese Instanzen (als Dienste) an einen virtuellen Lastausgleichsserver binden und dann den virtuellen Lastausgleichsserver in der HTTP-Callout-Konfiguration angeben. Der virtuelle Lastausgleichsserver gleicht dann die Last auf den konfigurierten Instanzen aus, wie durch den Lastausgleichsalgorithmus bestimmt.

Für das Format der HTTP-Callout-Anforderung können Sie die einzelnen Attribute der HTTP-Calloutanforderung (eine attributbasierte HTTP-Callout) angeben oder die gesamte HTTP-Callout-Anforderung als erweiterten Richtlinienausdruck (eine ausdrucksbasierte HTTP-Callout) angeben.

Für das Format der HTTP-Callout-Anforderung können Sie die einzelnen Attribute der HTTP-Callout-Anforderung angeben (ein attributbasiertes HTTP-Callout), oder Sie können die gesamte HTTP-Callout-Anforderung als erweiterten Richtlinienausdruck (ausdrucksbasiertes HTTP-Callout) angeben.

Weitere Informationen finden Sie unter Policy-HttpCallout

Parameter	Beschreibung
Name	Name des Callouts, maximal 127 Zeichen
IP-Adresse und Port (*IP-Adresse/Port*) oder Name des virtuellen Servers (vserver)	IPv4- oder IPv6-Adresse des Servers, an den das Callout gesendet wird, oder ein Platzhalter und des Port auf dem Server, an den das Callout gesendet wird, oder ein Platzhalter. Oder der Name eines virtuellen Load Balancing-, Content Switching- oder Cache-Umleitungsservers mit einem Diensttyp von HTTP.
HTTP-Methode (HttpMethod)	HTTP-Methode (HttpMethod). Methode, die in der HTTP-Anforderung verwendet wird, die dieser Callout sendet. Gültige Werte: GET oder POST. Standardwert: GET.
Host-Ausdruck (HostExpr)	Host-Ausdruck (HostExpr). Erweiterter Textausdruck zum Konfigurieren des Host-Headers. Maximale Länge: 255 Der Ausdruck kann ein Literalwert sein oder ein erweiterter Ausdruck sein, der den Wert ableitet. Beispiele: “10.101.10.11”, “http.req.header (“Host”)”
URL-Stammausdruck (urlStemExpr)	URL-Stammausdruck (urlStemExpr) Ein erweiterter Zeichenfolgenausdruck zum Generieren des URL-Stammes. Maximale Länge: 8191 Der Ausdruck kann eine literale Zeichenfolge oder ein Ausdruck sein, der den Wert ableitet. Beispiele: “” /mysite/index.html “” “http.req.url”

Parameter	Beschreibung
HTTP-Header (Header)	HTTP-Header (Header). Erweiterter Textausdruck zum Einfügen von HTTP-Headern und deren Werten in die HTTP-Calloutanforderung. Geben Sie für jeden Header einen Wert an. Sie geben den Header-Namen als String und den Header-Wert als erweiterten Ausdruck an. Geben Sie die Header durch Leerzeichen getrennt an. Wie -Header cip (client.ip.src) hdr (http.req.header (“HDR”)). Die Anzahl der Header kann 8 betragen
Ausdruckbasierte Anfrage zum Senden an den Server (FullReqExpr)	Exakte HTTP-Anforderung, die der NetScaler als erweiterter Ausdruck an 8191 Zeichen senden soll. Wenn Sie diesen Parameter angeben, müssen Sie die Argumente HttpMethod, HostExpr, urlStemExpr, Header und Parameter weglassen. Der Anforderungsausdruck wird durch das Feature eingeschränkt, in dem das Callout verwendet wird. Beispielsweise kann ein HTTP.RES-Ausdruck nicht in einer Richtlinienbank zur Anforderungszeit oder in einer TCP-Content Switching-Richtlinienbank verwendet werden.
Ausdruckbasierte Anfrage zum Senden an den Server (BodyExpr)	Ein erweiterter Zeichenfolgenausdruck zum Generieren des Hauptkörpers der Anforderung. Der Ausdruck kann eine literale Zeichenfolge oder einen Ausdruck enthalten, der den Wert ableitet (z. B. client.ip.src). Schließt sich gegenseitig mit -FullReqExpr aus.

Parameter	Beschreibung
Parameter	Erweiterter Ausdruck zum Einfügen von Abfrageparametern in die HTTP-Anforderung, die der Callout sendet. Geben Sie einen Wert für jeden Parameter an, den Sie konfigurieren. Wenn die Callout-Anfrage die GET-Methode verwendet, werden diese Parameter in die URL eingefügt. Wenn die Callout-Anfrage die POST-Methode verwendet, werden diese Parameter in den POST-Text eingefügt. Sie konfigurieren den Namen des Abfrageparameters als String und den Wert als erweiterten Ausdruck. Die Parameterwerte sind URL-codiert. Geben Sie die durch Leerzeichen getrennten Parameter wie ⊠parameter name1 (“name1”) name2 (http.req.header (“hdr”)) an. Die maximal 8 Parameter können konfiguriert werden.
Rückgabetyp (ReturnType)	Typ der Daten, die die Zielanwendung in der Antwort auf den Callout zurückgibt. Gültige Werte: TEXT: Behandeln Sie den zurückgegebenen Wert als Textzeichenfolge. NUM: Behandeln Sie den zurückgegebenen Wert als Zahl. BOOL: Behandelt den zurückgegebenen Wert als booleschen Wert. Hinweis: Sie können den Rückgabetyp nicht ändern, nachdem er festgelegt wurde.

Parameter	Beschreibung
Ausdruck zum Extrahieren von Daten aus der Antwort (ResultExPR)	Erweiterter Ausdruck, der HTTP.RES-Objekte aus der Antwort auf die HTTP-Callout extrahiert. Die maximale Länge beträgt 8191. Die Operationen in diesem Ausdruck müssen mit dem Rückgabetyp übereinstimmen. Wenn Sie beispielsweise einen Rückgabetyp von Text konfigurieren, muss der Ergebnisausdruck ein textbasierter Ausdruck sein. Wenn der Rückgabetyp num ist, muss der Ergebnisausdruck (resultExpr) einen numerischen Wert ähnlich dem folgenden zurückgeben: “http.res.body (10000) .length” Hinweis: Wenn Sie manchmal einen Rückgabetyp von TEXT festlegen und das vom Server gesendete Ergebnis 16 KB überschreitet, kann der Ergebnisausdruck NULL zurückgeben. Wenn das Ergebnis beispielsweise eine verkettete Zeichenfolge ist, die 16 KB überschreitet.
Schema	Die Art des Schemas für den Callout-Server. Beispiel: HTTP, https
cacheForSecs	Dauer in Sekunden, für die die Callout-Antwort zwischengespeichert wird. Die zwischengespeicherten Antworten werden in einer integrierten Caching-Content-Gruppe namens “CalloutContentGroup” gespeichert. Wenn keine Dauer konfiguriert ist, werden die Callout-Antworten nur zwischengespeichert, es sei denn, eine normale Caching-Konfiguration wird verwendet, um sie zu zwischenspeichern. Dieser Parameter hat Vorrang vor jeder normalen Caching-Konfiguration, die sonst für diese Antworten gelten würde.

Hinweis: Die Appliance überprüft nicht die Gültigkeit der Anforderung. Sie müssen sicherstellen, dass es sich bei der Anfrage um eine gültige Anfrage handelt und keine vertraulichen Informationen en-

thält. Eine falsche oder unvollständige HTTP-Callout-Konfiguration führt zu einer Runtime-UNDEF-Bedingung, die keiner Aktion zugeordnet ist. Die UNDEF-Bedingung aktualisiert lediglich den Zähler Undefined Hits, wodurch Sie eine falsch konfigurierte HTTP-Callout beheben können. Die Appliance analysiert jedoch die HTTP-Callout-Anforderung, damit Sie bestimmte NetScaler-Funktionen für den Callout konfigurieren können. Dies kann zu einem HTTP-Callout führen, der sich selbst aufruft. Informationen zur Callout-Rekursion und wie Sie sie vermeiden können, finden Sie unter Vermeiden von HTTP-Callout-Rekursion.

Unabhängig davon, ob Sie HTTP-Anforderungsattribute oder einen Ausdruck verwenden, um das Format der HTTP-Callout-Anforderung zu definieren, müssen Sie das Format der Antwort vom HTTP-Callout-Agent und den Teil der Antwort angeben, den Sie auswerten möchten. Der Antworttyp kann ein boolescher Wert, eine Zahl oder Text sein. Nur basierend auf diesem Rückgabetyp können Sie die weiteren Ausdrucksmethoden für die Callout-Antwort verwenden. Wenn der Rückgabetyp eine Zahl ist, können Sie den zahlenbasierten Ausdruck für die Callout-Antwort verwenden. Der Teil der Antwort, den Sie auswerten möchten, wird durch einen Ausdruck angegeben. Wenn Sie beispielsweise angeben, dass die Antwort Text enthält, können Sie mit `HTTP.RES.BODY(<unit>)` angeben, dass die Appliance nur die ersten <unit>Bytes der Antwort des Callout-Agenten auswerten darf.

In der Befehlszeile erstellen Sie zunächst ein HTTP-Callout mit dem Befehl
add. Wenn Sie ein Callout hinzufügen, werden alle Parameter auf den Standardwert NONE festgelegt, mit Ausnahme der HTTP-Methode, die auf den Standardwert GET festgelegt ist. Anschließend konfigurieren Sie die Parameter des mit dem Befehl set. Der Befehl set wird verwendet, um beide Arten von Callouts zu konfigurieren (attributsbasiert und ausdrucksbasiert). Der Unterschied liegt in den Parametern, die für die Konfiguration der beiden Arten von Callouts verwendet werden. Die folgenden Befehlszeilenanweisungen enthalten also einen set-Befehl zum Konfigurieren eines attributbasierten Callouts und einen set-Befehl zum Konfigurieren eines ausdrucksbasierten Callouts. Im Konfigurationsprogramm werden alle diese Konfigurationsaufgaben in einem einzigen Dialogfeld ausgeführt.

Hinweis: Bevor Sie ein HTTP-Callout in eine Richtlinie einfügen, können Sie alle konfigurierten Parameter mit Ausnahme des Rückgabetyps ändern. Sobald sich ein HTTP-Callout in einer Richtlinie befindet, können Sie einen Ausdruck, der in dem Callout konfiguriert ist, nicht vollständig ändern. Beispielsweise können Sie HTTP.REQ.HEADER (“myval”) nicht in CLIENT.IP.SRC ändern. Sie können die Operatoren und Argumente ändern, die an den Ausdruck übergeben werden. Sie können z. B. `HTTP.REQ.HEADER("myVal1")` in `HTTP.REQ.HEADER("myVal2")` oder `HTTP.REQ.HEADER("myVal")` in `HTTP.REQ.HEADER("myVal").AFTER_STR(<string>)` ändern. Wenn der Befehl set fehlschlägt, erstellen Sie eine HTTP-Callout.

Bei der Konfiguration von HTTP-Callouts werden erweiterte Richtlinienausdrücke konfiguriert. Weitere Informationen zum Konfigurieren von erweiterten Richtlinienausdrücken finden Sie unter Konfigurieren erweiterter Richtlinienausdrücke: Erste Schritte.

So konfigurieren Sie ein HTTP-Callout mit der Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung Folgendes aus:

Erstellen Sie ein HTTP-Callout.

```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port<
    port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
    GET | POST )] [-hostExpr <expression>]  [-urlStemExpr <expression>]
    [-headers <name(value)> ...] [-parameters <name(value)> ...] [-
    bodyExpr <expression>] [-fullReqExpr <expression>] [-scheme ( http |
     https )] [-resultExpr <expression>] [-cacheForSecs <secs>] [-
    comment <string>]

<!--NeedCopy-->
```

Beispiel:

```
add policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader")-
    resultExpr "http.res.body(10000).length"

<!--NeedCopy-->
```

Ändern Sie die HTTP-Callout-Konfiguration.

```
set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr|\*>] [-
    port <port|\*>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)>
    ...] [-resultExpr <string>]

<!--NeedCopy-->
```

Beispiel:

```
> set policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader") -
    resultExpr "http.res.body(10000).length"
<!--NeedCopy-->
```

Konfigurieren Sie die HTTP-Callout mit dem FullReqExpr-Parameter.

```
set policy httpCallout <name> [-vServer <string>] [-returnType <
    returnType>] [-fullReqExpr <string>] [-resultExpr <string>]
```



```
<!--NeedCopy-->
```

Beispiel:

```
> set policy httpCallout mycallout1 -vserver lbv1 -returnType num
    fullReqExpr q{
 "GET " + http.req.url + "HTTP/" + http.req.version.major + "." + http.
    req.version.minor.sub(1) + "r\nHost:10.101.10.10\r\nAccept: \*/\*\r
    \n\r\n" }


<!--NeedCopy-->
```

Überprüfen Sie die Konfigurationen des HTTP-Callout.

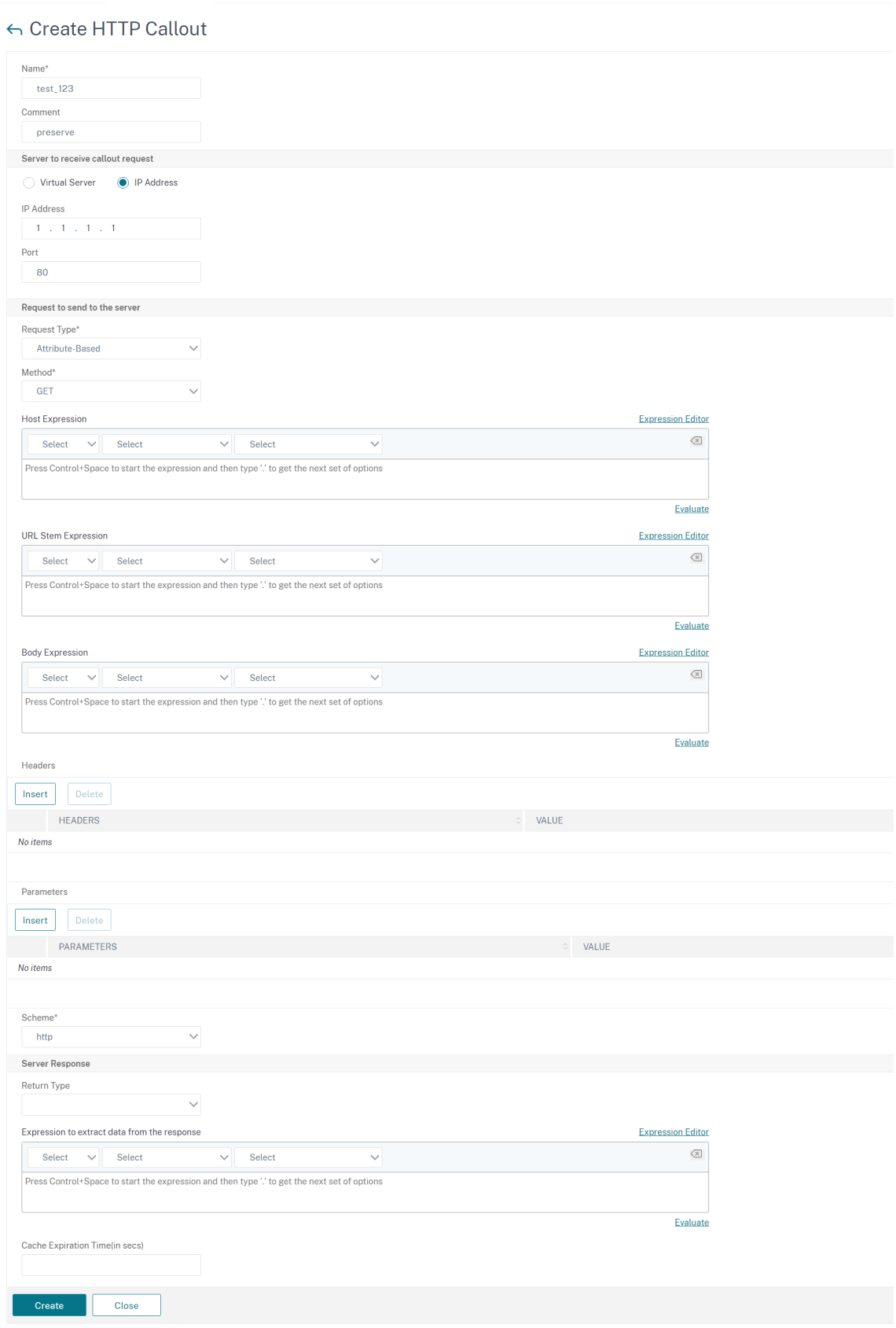
```
show policy httpCallout `<name>`

sh policy httpCallout mycallout1
> Name: mycallout1
>Vserver: lbv1 (UP)
Effective Vserver state: UP
Return type: TEXT
Scheme: HTTP
Full REQ expr: "GET " + http.req.url + "HTTP/" + http.req.version.major
    + "." + http.req.version.minor.sub(1)+ "r\nHost:10.101.10.10\r\
   nAccept: \*/\*\r\n\r\n"
Result expr: http.res.body(100)
Hits: 0
Undef Hits: 0
Done
>

<!--NeedCopy-->
```

So konfigurieren Sie ein HTTP-Callout mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **HTTP-Callouts**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Konfigurieren Sie im Dialogfeld **HTTP-Callout erstellen** die Parameter des HTTP-Callouts. Um eine Beschreibung des Parameters zu erhalten, bewegen Sie den Mauszeiger über das Kontrollkästchen.
4. Klicken Sie auf **Create** und dann auf **Close**.



Überprüfung der Konfiguration

May 11, 2023

Damit ein HTTP-Callout ordnungsgemäß funktioniert, müssen alle HTTP-Callout-Parameter und die mit dem Callout verknüpften Entitäten korrekt konfiguriert sein. Die NetScaler-Appliance überprüft zwar nicht die Gültigkeit der HTTP-Callout-Parameter, gibt aber den Status der gebundenen Entitäten an, nämlich den Server oder virtuellen Server, an den das HTTP-Callout gesendet wird. In der folgenden Tabelle sind die Symbole aufgeführt und die Bedingungen beschrieben, unter denen die Symbole angezeigt werden.

Symbol	Zeigt an, dass
	Der Status des Servers, der den HTTP-Callout-Agenten hostet, oder des virtuellen Servers für Load Balancing, Content Switching oder Cache-Umleitung, an den das HTTP-Callout gesendet wird, ist UP.
	Der Status des Servers, der den HTTP-Callout-Agenten hostet, oder des virtuellen Servers für Load Balancing, Content Switching oder Cache-Umleitung, an den das HTTP-Callout gesendet wird, ist AUSSER BETRIEB.
	Der Status des Servers, der den HTTP-Callout-Agenten hostet, oder des virtuellen Servers für Load Balancing, Content Switching oder Cache-Umleitung, an den das HTTP-Callout gesendet wird, ist DOWN.

Tabelle 1. Symbole, die den Status von Entitäten angeben, die an ein HTTP-Callout gebunden sind

Damit ein HTTP-Callout korrekt funktioniert, muss das Symbol immer grün sein. Wenn das Symbol nicht grün ist, überprüfen Sie den Status des Callout-Servers oder des virtuellen Servers, an den das HTTP-Callout gesendet wird. Wenn das HTTP-Callout nicht wie erwartet funktioniert, obwohl das Symbol grün ist, überprüfen Sie die für das Callout konfigurierten Parameter.

Sie können die Konfiguration auch überprüfen, indem Sie Testanforderungen senden, die der Richtlinie entsprechen, von der aus das HTTP-Callout aufgerufen wurde, den Trefferzähler für die Policy und den HTTP-Callout überprüfen und die Antworten überprüfen, die die NetScaler-Appliance

an den Client sendet.

Hinweis: Ein HTTP-Callout kann sich manchmal ein zweites Mal rekursiv aufrufen. In diesem Fall wird der Trefferzähler für jeden Callout, der von der Appliance generiert wird, um zwei Zähler erhöht. Damit der Treffer-Zähler den richtigen Wert anzeigt, müssen Sie das HTTP-Callout so konfigurieren, dass sie sich nicht ein zweites Mal aufruft. Weitere Informationen darüber, wie Sie die Rekursion von HTTP-Callouts vermeiden können, finden Sie unter Vermeiden von HTTP-Callout-Rekursion.

So zeigen Sie den Treffer-Zähler für ein HTTP-Callout an

1. Navigieren Sie zu **AppExpert** > **HTTP-Callouts**.
2. Klicken Sie im Detailbereich auf das HTTP-Callout, für das Sie den Trefferzähler anzeigen möchten, und sehen Sie sich dann die Treffer im **Detailbereich** an.

Aufrufen einer HTTP-Callout

May 11, 2023

Nachdem Sie ein HTTP-Callout konfiguriert haben, rufen Sie das Callout auf, indem Sie den Ausdruck `SYS.HTTP_CALLOUT(<name>)` in eine erweiterte Richtlinienregel einschließen. In diesem Ausdruck ist `<name>` der Name des HTTP-Callouts, den Sie aufrufen möchten.

Sie können erweiterte Richtlinienausdruck-Operatoren mit dem Callout-Ausdruck verwenden, um die Antwort zu verarbeiten und dann eine entsprechende Aktion durchzuführen. Der Rückgabetyp der Antwort des HTTP-Callout-Agenten bestimmt den Satz von Operatoren, die Sie für die Antwort verwenden können. Wenn der Teil der Antwort, den Sie analysieren möchten, Text ist, können Sie einen Textoperator verwenden, um die Antwort zu analysieren. Sie können beispielsweise den <string> Operator CONTAINS () verwenden, um zu überprüfen, ob der angegebene Teil der Antwort eine bestimmte Zeichenfolge enthält, wie im folgenden Beispiel:

```
1 SYS.HTTP_CALLOUT(mycallout).contains("Good IP address")
2 <!--NeedCopy-->
```

Wenn Sie den vorhergehenden Ausdruck in einer Responder Policy verwenden, können Sie eine entsprechende Responder Action konfigurieren.

Wenn der Teil der Antwort, den Sie auswerten möchten, eine Zahl ist, können Sie einen numerischen Operator wie GT (int) verwenden. Wenn die Antwort einen booleschen Wert enthält, können Sie einen booleschen Operator verwenden.

Hinweis: Ein HTTP-Callout kann sich rekursiv aufrufen. Die Rekursion von HTTP-Callouts kann vermieden werden, indem der HTTP-Callout-Ausdruck mit einem erweiterten Richtlinienausdruck kom-

biniert wird, der eine Rekursion verhindert. Informationen darüber, wie Sie die Rekursion von HTTP-Callouts vermeiden können, finden Sie unter Vermeiden von HTTP-Callout-Rekursion.

Sie können HTTP-Callouts auch kaskadieren, indem Sie Richtlinien konfigurieren, die jeweils ein Callout aufrufen, nachdem zuvor generierte Callouts ausgewertet wurden. In diesem Szenario kann ein zweiter Satz von Richtlinien nach dem Aufrufen eines Callouts, wenn die NetScaler-Appliance das Callout analysiert, bevor das Callout an den Callout-Server gesendet wird, das Callout auswerten und zusätzliche Callouts aufrufen, die wiederum durch einen dritten Satz von Richtlinien usw. ausgewertet werden können. Eine solche Implementierung wird im folgenden Beispiel beschrieben.

Zuerst können Sie einen HTTP-Callout namens myCallout1 konfigurieren und dann eine Responder Policy, Pol1, konfigurieren, um myCallout1 aufzurufen. Dann könnten Sie ein zweites HTTP-Callout, myCallout2, und eine Responder Policy, Pol2, konfigurieren. Sie konfigurieren Pol2, um myCallout1 auszuwerten und myCallout2 aufzurufen. Sie binden beide Responder-Richtlinien global.

Um eine Rekursion von HTTP-Callouts zu vermeiden, ist myCallout1 mit einem eindeutigen benutzerdefinierten HTTP-Header namens “Request1” konfiguriert. Pol1 ist so konfiguriert, dass die Rekursion von HTTP-Callouts mithilfe des erweiterten Richtlinienausdrucks vermieden wird.

```
HTTP.REQ.HEADER("Request1").EQ("Callout Request").NOT.
<!--NeedCopy-->
```

Pol2 verwendet denselben erweiterten Richtlinienausdruck, schließt jedoch den Operator.NOT aus, sodass die Richtlinie myCallout1 auswertet, wenn die NetScaler-Appliance ihn analysiert. Beachten Sie, dass myCallout2 seinen eigenen eindeutigen Header namens “Request2” identifiziert und Pol2 einen erweiterten Richtlinienausdruck enthält, um zu verhindern, dass myCallout2 sich rekursiv aufruft.

Beispiel:

```
> add policy httpCallout myCallout1

Done

> set policy httpCallout myCallout1 -IPAddress 10.102.3.95 -port 80 -
   returnType TEXT -hostExpr
 ""10.102.3.95"" -urlStemExpr ""/cgi-bin/check_clnt_from_database.pl""
    -headers Request1
("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.
   RES.BODY(100)"

Done

> add responder policy Pol1 "HTTP.REQ.HEADER("Request1").EQ("Callout
   Request").NOT &&
```



```
SYS.HTTP_CALLOUT(myCallout1).CONTAINS("IP Matched")" RESET

Done

> bind responder global Pol1 100 END -type OVERRIDE

Done

> add policy httpCallout myCallout2

Done

> set policy httpCallout myCallout2 -IPAddress 10.102.3.96 -port 80 -
   returnType TEXT -hostExpr
""10.102.3.96"" -urlStemExpr ""/cgi-bin/
   check_clnt_location_from_database.pl"" -headers Request2
("Callout Request") -parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.
   RES.BODY(200)"

 Done

> add responder policy Pol2 "HTTP.REQ.HEADER("Request2").EQ("Callout
   Request").NOT &&
 HTTP.REQ.HEADER("Request1").EQ("Callout Request") && SYS.HTTP_CALLOUT(
    myCallout2).CONTAINS
("APAC")" RESET

 Done

> bind responder global Pol2 110 END -type OVERRIDE

Done
<!--NeedCopy-->
```

Vermeiden von HTTP-Callout-Rekursion

May 11, 2023

Obwohl die NetScaler-Appliance nicht auf die Gültigkeit der HTTP-Callout-Anforderung prüft, analysiert sie die Anforderung einmal, bevor sie die Anforderung an den HTTP-Callout-Agenten sendet. Durch dieses Parsen kann die Appliance die Callout-Anforderung wie jede andere eingehende Anforderung behandeln, was es Ihnen wiederum ermöglicht, mehrere nützliche NetScaler-

Funktionen (wie integriertes Caching) für die Bearbeitung der Callout-Anforderung zu konfigurieren.

Während dieser Analyse kann die HTTP-Callout-Anforderung jedoch dieselbe Richtlinie auswählen und sich daher rekursiv aufrufen. Die Appliance erkennt den rekursiven Aufruf und löst eine undefinierte (UNDEF) -Bedingung aus. Der rekursive Aufruf führt jedoch dazu, dass die Auswahlzähler für Richtlinien und HTTP-Callouts um jeweils zwei Zählungen anstelle von jeweils einer Zählung erhöht werden.

Um zu verhindern, dass sich ein Callout selbst aufruft, müssen Sie mindestens ein eindeutiges Merkmal der HTTP-Callout-Anforderung identifizieren und dann alle Anforderungen mit diesem Merkmal von der Policy-Regel ausschließen, die den Callout aufruft. Sie können dies tun, indem Sie einen weiteren erweiterten Richtlinienausdruck in die Richtlinienregel ein Der Ausdruck muss dem Ausdruck `SYS.HTTP_CALLOUT(<name>)` vorangestellt sein, damit er ausgewertet wird, bevor der Callout-Ausdruck ausgewertet wird. Zum Beispiel:

```
<Expression that prevents callout recursion> OR SYS.HTTP_CALLOUT(<name
    >)
<!--NeedCopy-->
```

Wenn Sie eine Richtlinienregel auf diese Weise konfigurieren und die Appliance die Anforderung generiert und analysiert, wird die zusammengesetzte Regel als FALSE ausgewertet, das Callout wird kein zweites Mal generiert und die ausgewählten Zähler werden korrekt erhöht.

Eine Möglichkeit, einer HTTP-Callout-Anforderung ein eindeutiges Merkmal zuzuweisen, besteht darin, bei der Konfiguration des Callouts einen eindeutigen benutzerdefinierten HTTP-Header einzuschließen. Es folgt ein Beispiel für einen HTTP-Callout namens “myCallout”. Der Callout generiert eine HTTP-Anforderung, die prüft, ob die IP-Adresse eines Clients in einer Datenbank mit IP-Adressen auf der Sperrliste vorhanden ist. Das Callout enthält einen benutzerdefinierten Header namens “Request”, der auf den Wert “Callout Request” gesetzt ist. Eine global gebundene Responder Policy, “Pol1”, ruft den HTTP-Callout auf, schließt jedoch alle Anfragen aus, deren Request-Header auf diesen Wert festgelegt ist, wodurch ein zweiter Aufruf von myCallout verhindert wird. Der Ausdruck, der einen zweiten Aufruf verhindert, ist HTTP.REQ.HEADER(“Request”).EQ(“Callout Request”).NOT.

Beispiel:

```
> add policy httpCallout myCallout
 Done

> set policy httpCallout myCallout -IPAddress 10.102.3.95 -port 80 -
    returnType TEXT -hostExpr ""10.102.3.95"" -urlStemExpr ""/cgi-bin/
    check_clnt_from_database.pl"" -headers Request("Callout Request") -
    parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.RES.BODY(100)"
Done

```



```
> add responder policy Pol1 "HTTP.REQ.HEADER("Request").EQ("Callout
    Request").NOT && SYS.HTTP_CALLOUT(myCallout).CONTAINS("IP Matched")"
     RESET
Done

> bind responder global Pol1 100 END -type OVERRIDE
Done
<!--NeedCopy-->
```

> **Hinweis:**
> Sie können auch einen Ausdruck konfigurieren, um zu überprüfen, ob die Anforderungs-URL den für das HTTP-Callout konfigurierten Stammausdruck enthält. Um die Lösung zu implementieren, stellen Sie sicher, dass der HTTP-Callout-Agent nur auf HTTP-Callouts und nicht auf andere Anfragen antworten kann, die über die Appliance geleitet werden. Wenn der HTTP-Callout-Agent eine Anwendung oder ein Webserver ist, der andere Clientanforderungen bedient, verhindert ein solcher Ausdruck, dass die Appliance diese Clientanforderungen verarbeitet. Verwenden Sie stattdessen einen eindeutigen benutzerdefinierten Header wie oben beschrieben.

HTTP-Callout-Antworten zwischenspeichern

January 19, 2021

Um die Leistung bei der Verwendung von Callouts zu verbessern, können Sie die integrierte Caching-Funktion verwenden, um Callout-Antworten zwischenzuspeichern. Die Antworten werden in einer integrierten Caching-Content-Gruppe namens CalloutContentGroup für eine bestimmte Zeit gespeichert.

Hinweis: Um Callout-Antworten zwischenzuspeichern, stellen Sie sicher, dass die integrierte Caching-Funktion aktiviert ist.

So legen Sie die Cache-Dauer mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set policy httpCallout <name> -cacheForSecs <secs>
```

Beispiel:

```
> set httpcallout httpcallout1 -cacheForSecs 120
<!--NeedCopy-->
```


So legen Sie die Cache-Dauer mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **AppExpert > HTTP-Callouts**.
2. Wählen Sie im Detailbereich das HTTP-Callout aus, für die Sie die Cache-Dauer festlegen möchten, und klicken Sie auf **Öffnen**.
3. Geben Sie im Dialogfeld **HTTP-Callout konfigurieren** die **Cache-Ablaufzeit** an.
4. Stellen Sie sicher, dass Sie die richtige Zeitdauer eingegeben haben, und klicken Sie dann auf **OK**.

Anwendungsfall: Filtern von Clients über eine IP-Blacklist

May 11, 2023

HTTP-Callouts können verwendet werden, um Anfragen von Clients zu blockieren, die vom Administrator auf die Sperrliste gesetzt werden. Die Liste der Kunden kann eine öffentlich bekannte Sperrliste, eine Sperrliste, die Sie für Ihre Organisation pflegen, oder eine Kombination aus beiden sein.

Die NetScaler-Appliance überprüft die IP-Adresse des Clients mit der vorkonfigurierten Sperrliste und blockiert die Transaktion, wenn die IP-Adresse auf die schwarze Liste gesetzt wurde. Wenn die IP-Adresse nicht in der Liste enthalten ist, verarbeitet die Appliance die Transaktion.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie den Responder auf der NetScaler-Appliance.
2. Erstellen Sie ein HTTP-Callout auf der NetScaler-Appliance und konfigurieren Sie es mit Details zum externen Server und anderen erforderlichen Parametern.
3. Konfigurieren Sie eine Responder Policy, um die Antwort auf den HTTP-Callout zu analysieren, und binden Sie die Richtlinie dann global.
4. Erstellen Sie einen HTTP-Callout-Agent auf dem Remoteserver.

Responder aktivieren

Sie müssen den Responder aktivieren, bevor Sie ihn verwenden können.

So aktivieren Sie den Responder über die GUI

1. Stellen Sie sicher, dass Sie die Responder-Lizenz installiert haben.
2. Erweitern Sie im Konfigurationsprogramm AppExpert, klicken Sie mit der rechten Maustaste auf **Responder**und klicken Sie dann auf **Responder-Funktion aktivieren** .

Erstellen eines HTTP-Callouts auf der NetScaler-Appliance

Erstellen Sie ein HTTP-Callout, HTTP_Callout, mit den Parametereinstellungen in der folgenden Tabelle. Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout-PDF-Datei .

Konfigurieren einer Responder-Richtlinie und globales Binden

Nachdem Sie das HTTP-Callout konfiguriert haben, überprüfen Sie die Callout-Konfiguration und konfigurieren Sie dann eine Responder Policy, um das Callout aufzurufen. Während Sie eine Responder Policy im Unterknoten
Richtlinien erstellen und diese dann mithilfe des
Responder-Richtlinien-Managers global binden können, verwendet diese Demonstration den Responder-Richtlinien-Manager, um die Responder Policy zu erstellen und die Richtlinie global zu binden.

So erstellen Sie eine Responder Policy und binden sie global mit

1. Navigieren Sie zu **AppExpert** > **Responder**.
2. Klicken Sie im Detailbereich unter **Policy Manager**auf **Policy Manager**.
3. Klicken Sie im Dialogfeld **Responder Policy Manager** auf **Override Global**.
4. Klicken Sie auf **Richtlinie einfügen**und dann unter **Richtlinienname**auf **Neue Richtlinie**.
5. Gehen **Sie im Dialogfeld Responder-Richtlinie erstellen** wie folgt vor:
   a) Geben Sie in das Feld Name **PolicyResponder1**ein.
   b) Wählen Sie unter **AktionRESET**aus.
   c) Wählen Sie in **Aktion für undefiniertes Ergebnis**die Option **Globale Aktion mit undefiniertem Ergebnis** aus.
   d) Geben Sie unter **Ausdruck**den folgenden erweiterten Richtlinienausdruck ein:

```
"HTTP.REQ.HEADER("Request").EQ("Callout Request").NOT && SYS.
   HTTP_CALLOUT(HTTP_Callout).CONTAINS("IP Matched")"
<!--NeedCopy-->
```

   e) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Erstellen eines HTTP-Callout-Agenten auf dem Remoteserver

Sie müssen jetzt einen HTTP-Callout-Agent auf dem Remote-Callout-Server erstellen, der Callout-Anfragen von der NetScaler-Appliance empfängt und entsprechend antwortet. Der HTTP-Callout-Agent ist ein Skript, das für jede Bereitstellung unterschiedlich ist und unter Berücksichtigung der Serverspezifikationen wie dem Datenbanktyp und der unterstützten Skriptsprache geschrieben werden muss.

Es folgt ein Beispiel für einen Callout-Agent, der überprüft, ob die angegebene IP-Adresse Teil einer IP-Sperrliste ist. Der Agent wurde in der Perl-Skriptsprache geschrieben und verwendet eine MYSQL-Datenbank.

Das folgende CGI-Skript prüft auf dem Callout-Server nach einer bestimmten IP-Adresse.

```
#!/usr/bin/perl -w
print "Content-type: text/html\n\n";
        use DBI();
        use CGI qw(:standard);
#Take the Client IP address from the request query
        my $ip_to_check = param('cip');
# Where a MYSQL database is running
        my $dsn = 'DBI:mysql:BAD_CLIENT:localhost';
# Database username to connect with
        my $db_user_name =  'dbuser' ;
# Database password to connect with
        my $db_password = 'dbpassword';
        my ($id, $password);
# Connecting to the database
        my $dbh = DBI->connect($dsn, $db_user_name, $db_password);
        my $sth = $dbh->prepare(qq{
  select * from bad_clnt  }
 );
        $sth->execute();
        while (my ($ip_in_database) = $sth->fetchrow_array()) {

        chomp($ip_in_database);
# Check for IP match
        if ($ip_in_database eq $ip_to_check) {

              print "\n IP Matched\n";
                                                    $sth->finish();
                                               exit;
                 }

        }
```



```
32
33         print "\n IP Failed\n";
34         $sth->finish();
35         exit;
36 <!--NeedCopy-->
```

Anwendungsfall: ESI-Unterstützung für das dynamische Abrufen und Aktualisieren von Inhalten

May 11, 2023

Edge Side Includes (ESI) ist eine Markup-Sprache für die Assemblierung dynamischer Webinhalte auf Edge-Ebene. Es hilft bei der Beschleunigung dynamischer webbasierter Anwendungen, indem es eine einfache Markup-Sprache definiert, um zwischenspeicherbare und nicht zwischenspeicherbare Webseitenkomponenten zu beschreiben, die am Netzwerkrand aggregiert, zusammengestellt und bereitgestellt werden können. Durch die Verwendung von HTTP-Callouts auf der NetScaler-Appliance können Sie die ESI-Konstrukte durchlesen und Inhalte dynamisch aggregieren oder zusammenstellen.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie das Rewrite auf der NetScaler-Appliance.
2. Erstellen Sie ein HTTP-Callout auf der Appliance und konfigurieren Sie es mit Details zum externen Server und anderen erforderlichen Parametern.
3. Konfigurieren Sie eine Rewrite-Aktion , um den ESI-Inhalt durch den Callout-Antworttext zu ersetzen.
4. Konfigurieren Sie eine Rewriterichtlinie, um die Bedingungen anzugeben, unter denen die Aktion ausgeführt wird, und binden Sie dann die Rewriterichtlinie global.

Rewrite aktivieren

Das Rewrite muss aktiviert sein, bevor es auf der NetScaler-Appliance verwendet wird. Im folgenden Verfahren werden die Schritte zum Aktivieren der Rewritefunktion beschrieben.

So aktivieren Sie das Rewrite über die GUI

1. Stellen Sie sicher, dass Sie die Rewrite-Lizenz installiert haben.
2. Erweitern Sie im Konfigurationsdienstprogramm AppExpert, klicken Sie mit der rechten Maustaste auf Rewrite, und klicken Sie dann auf Funktion zum Rewrite aktivieren.

Erstellen eines HTTP-Callouts auf der NetScaler-Appliance

Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout.
Weitere Informationen zu den Parameterwerten finden Sie unter Parameter und Werte für HTTP-Callout-2 pdf.

Konfigurieren der Aktion Rewrite

Erstellen Sie eine Rewriteaktion, Action-Rewrite-1, um den ESI-Inhalt durch den Callout-Antworttext zu ersetzen. Verwenden Sie die in der folgenden Tabelle gezeigten Parametereinstellungen.

Tabelle 2. Parameter und Werte für Action-Rewrite-1

Parameter	Wert
Name	Action-Rewrite-1
Typ	Ersetzen
Ausdruck zur Auswahl der Zieltextreferenz	“HTTP.RES.BODY(500).AFTER_STR (\” <example>\”).BEFORE_STR (\”</example>\”)”
Zeichenfolgenausdruck für Ersetzungstext	“SYS.HTTP_CALLOUT(HTTP-Callout-2)”

So konfigurieren Sie die Rewrite-Aktion mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **AppExpert** > **Rewrite** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Neuschreibaktion erstellen** in das Feld Name **Action-Rewrite-1**ein.
4. Wählen Sie unter Typ die Option **ERSETZEN**aus.
5. Geben Sie unter **Ausdruck** den folgenden erweiterten Richtlinienausdruck ein, um den Zieltextreferenz auszuwählen:

```
"HTTP.RES.BODY(500).AFTER_STR("<example>").BEFORE_STR("<example>")
   "
<!--NeedCopy-->
```

6. Geben Sie im Zeichenfolgenausdruck für Ersetzungstext den folgenden Zeichenfolgenausdruck ein:

```
"SYS.HTTP_CALLOUT(HTTP-Callout-2)"
<!--NeedCopy-->
```


7. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Erstellen der Rewriterichtlinie und globales Binden

Erstellen Sie eine Rewriterichtlinie, Policy-Rewrite-1, mit den in der folgenden Tabelle gezeigten Parametereinstellungen. Sie können eine Rewriterichtlinie im Unterknoten
Richtlinien erstellen und diese dann mithilfe des Richtlinien-Managers zum
Rewrite global binden. Alternativ können Sie den
Rewrite Policy Manager verwenden, um diese beiden Aufgaben gleichzeitig auszuführen. Diese Demonstration verwendet den
Rewrite Policy Manager, um beide Aufgaben auszuführen.

Tabelle 3. Parameter und Werte für Policy-Rewrite-1

Parameter	Wert
Name	Policy-Rewrite-1
Aktion	Action_Rewrite-1
Aktion für undefiniertes Ergebnis	-Global undefined-result action-
Ausdruck	“HTTP.REQ.HEADER(“Name”).CONTAINS (“Callout”).NOT”

So konfigurieren Sie eine Rewriterichtlinie und binden sie mithilfe des Konfigurationsdienstprogramms global

1. Navigieren Sie zu **AppExpert** > **Rewrite**.
2. Klicken Sie im Detailbereich unter **Richtlinien-Manager**auf **Rewrite Policy Manager**.
3. Klicken Sie im Dialogfeld **Rewrite Policy Manager** auf **Global überschreiben**.
4. Klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf **Neue Richtlinie**.
5. Gehen Sie im Dialogfeld **Rewrite-Policy erstellen** wie folgt vor:
   1.Geben Sie in Name Policy-Rewrite-1 ein.
   a) Wählen Sie unter Aktion Action-Rewrite-1 aus.
   b) Wählen Sie in Aktion für undefiniertes Ergebnisdie Option Globale Aktion mit undefiniertem Ergebnis aus.
   c) Geben Sie unter Ausdruckden folgenden erweiterten Richtlinienausdruck ein:

```
"HTTP.REQ.HEADER("Name").CONTAINS("Callout").NOT"
<!--NeedCopy-->
```


a) Klicken Sie auf **Erstellen**und dann auf **Schließen**.

6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Anwendungsfall: Zugriffskontrolle und Authentifizierung

May 11, 2023

In Hochsicherheitszonen ist es zwingend erforderlich, den Benutzer extern zu authentifizieren, bevor Clients auf eine Ressource zugreifen. Auf der NetScaler-Appliance können Sie HTTP-Callouts verwenden, um den Benutzer extern zu authentifizieren, indem Sie die bereitgestellten Anmeldeinformationen auswerten. In diesem Beispiel wird davon ausgegangen, dass der Client den Benutzernamen und das Passwort in der Anfrage über HTTP-Header sendet. Dieselben Informationen könnten jedoch von der URL oder dem HTTP-Body abgerufen werden.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie die Responder-Funktion auf der NetScaler-Appliance.
2. Erstellen Sie ein HTTP-Callout auf der Appliance und konfigurieren Sie es mit Details zum externen Server und anderen erforderlichen Parametern.
3. Konfigurieren Sie eine Responder-Richtlinie, um die Antwort zu analysieren, und binden Sie die Richtlinie dann global.
4. Erstellen Sie einen Callout-Agenten auf dem Remoteserver.

Responder aktivieren

Die Responder-Funktion muss aktiviert sein, bevor sie auf der NetScaler-Appliance verwendet werden kann.

So aktivieren Sie den Responder mithilfe des Konfigurationsprogramms

1. Stellen Sie sicher, dass die Responder-Lizenz installiert ist.
2. Erweitern Sie im Konfigurationsprogramm AppExpert, klicken Sie mit der rechten Maustaste auf Responder und klicken Sie dann auf **Responder-Funktion aktivieren**.

Erstellen eines HTTP-Callouts auf der NetScaler-Appliance

Erstellen Sie ein HTTP-Callout, HTTP-Callout-3, mit den Parametereinstellungen in der folgenden Tabelle. Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout.

Tabelle 1. Parameter und Werte für HTTP-Callout-3

Parameter	Wert	Name
Name	Policy-Responder-3	

Parameter

Wert

Name

HTTP-Callout-3

Server für den Empfang einer Callout-Anforderung:

IP-Adresse

10.103.9.95

Port

80

Anfrage zum Senden an den Server:

Methode

GET

Ausdruck des Hosts

10.102.3.95

URL-Stammausdruck

„/cgi-bin/authenticate.pl“

Kopfzeilen:

Name

Anfrage

Werteausdruck

Callout-Anfrage

Parameter:

Name

Benutzername

Werteausdruck

HTTP.REQ.HEADER („Benutzername“) .VALUE (0)

Name

Kennwort

Werteausdruck

HTTP.REQ.HEADER („Passwort“) .VALUE (0)

Serverantwort:

Art der Rückgabe

TEXT

Ausdruck zum Extrahieren von Daten aus der Antwort

HTTP.RES.BODY(100)

Erstellen einer Responder-Richtlinie zur Analyse der Antwort

Erstellen Sie eine Responder-Richtlinie, Policy-Responder-3, die die Antwort vom Callout-Server überprüft und die Verbindung ZURÜCKSETZT, wenn die Quell-IP-Adresse auf die schwarze Liste gesetzt wurde. Erstellen Sie die Richtlinie mit den in der folgenden Tabelle aufgeführten Parametereinstellungen. Sie können zwar im Unterknoten
Richtlinien eine Responder-Richtlinie erstellen und sie dann mithilfe des Responder-Policy-Managers global binden. In dieser Demonstration wird jedoch
der Responder-Policy-Manager verwendet, um die
Responder-Richtlinie zu erstellen und die Richtlinie global zu binden.

Tabelle 2. Parameter und Werte für Policy-Responder-3

Parameter	Wert
Name	Policy-Responder-3
Aktion	RESET
Aktion mit undefiniertem Ergebnis	-Global undefined-result action-
Ausdruck	„HTTP.REQ.HEADER (\” Anfrage\“) .EQ (\ “Callout-Anforderung\“) .NOT && SYS.HTTP_CALLOUT (HTTP-Callout-3) .CONTAINS (\ “Authentifizierung fehlgeschlagen\“)“

Um eine Responder-Richtlinie zu erstellen und sie global zu binden, verwenden Sie das Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Responder**.
2. Klicken Sie im Detailbereich unter **Policy Manager**auf **Responder Policy Manager**.
3. Klicken Sie im Dialogfeld **Responder Policy Manager** auf **Override**Global.
4. Klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf **Neue Richtlinie**.
5. Gehen **Sie im Dialogfeld Responder-Richtlinie erstellen** wie folgt vor:
   a) Geben Sie im Feld Name den Wert Policy-Responder-3 ein.
   b) Wählen Sie unter Aktion die Option **ZURÜCKSETZEN**aus.
   c) Wählen Sie unter Aktion mit undefiniertem Ergebnis die Option Globale Aktion mit undefiniertem Ergebnis aus.
   d) Geben Sie in das Textfeld Ausdruck Folgendes ein:

```
"HTTP.REQ.HEADER("Request").EQ("Callout Request").NOT && SYS.
   HTTP_CALLOUT(HTTP-Callout-3).CONTAINS("Authentication Failed")"
<!--NeedCopy-->
```

   a) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Einen HTTP Callout-Agenten auf dem Remoteserver erstellen

Sie müssen jetzt einen HTTP-Callout-Agenten auf dem Remote-Callout-Server erstellen. Der HTTP-Callout-Agent empfängt Callout-Anfragen von der NetScaler-Appliance und reagiert entsprechend. Der Callout-Agent ist ein Skript, das für jede Bereitstellung unterschiedlich ist und unter Berücksichtigung der Serverspezifikationen, wie z. B. des Datenbanktyps und der unterstützten Skriptsprache, geschrieben werden muss.

Im Folgenden finden Sie ein Beispiel für einen Callout-Agent-Pseudocode, der überprüft, ob der angegebene Benutzername und das angegebene Passwort gültig sind. Der Agent kann in jeder Programmiersprache Ihrer Wahl implementiert werden. Der Pseudocode darf nur als Richtlinie für die Entwicklung des Callout-Agenten verwendet werden. Sie können zusätzliche Funktionen in das Programm integrieren.

Um den angegebenen Benutzernamen und das Passwort mithilfe von Pseudocode zu überprüfen

1. Akzeptieren Sie den in der Anfrage angegebenen Benutzernamen und das Passwort und formatieren Sie sie entsprechend.
2. Stellen Sie eine Verbindung zu der Datenbank her, die alle gültigen Benutzernamen und Passwörter enthält.
3. Überprüfen Sie die angegebenen Anmeldeinformationen anhand Ihrer Datenbank.
4. Formatieren Sie die Antwort so, wie es der HTTP-Callout erfordert.
5. Senden Sie die Antwort an die NetScaler Appliance.

Anwendungsfall: OWA-basierte Spamfilterung

May 11, 2023

Spam-Filterung ist die Fähigkeit, E-Mails, die nicht von einer bekannten oder vertrauenswürdigen Quelle stammen oder unangemessenen Inhalt haben, dynamisch zu blockieren. Die Spam-Filterung erfordert eine zugehörige Geschäftslogik, die darauf hinweist, dass es sich bei einer bestimmten Art von Nachricht um Spam handelt. Wenn die NetScaler-Appliance Outlook Web Access (OWA) -Nachrichten auf der Grundlage des HTTP-Protokolls verarbeitet, können HTTP-Callouts zum Filtern von Spam verwendet werden.

Sie können HTTP-Callouts verwenden, um einen beliebigen Teil der eingehenden Nachricht zu extrahieren und dies mit einem externen Callout-Server zu überprüfen, der mit Regeln konfiguriert wurde, anhand derer bestimmt wird, ob es sich bei einer Nachricht um eine legitime Nachricht oder um Spam handelt. Im Falle von Spam-E-Mails benachrichtigt die NetScaler Appliance den Absender aus Sicherheitsgründen nicht darüber, dass die E-Mail als Spam markiert ist.

Das folgende Beispiel führt eine sehr einfache Überprüfung auf verschiedene aufgelistete Keywords im E-Mail-Betreff durch. Diese Prüfungen können in einer Produktionsumgebung komplexer sein.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie die Responder-Funktion auf der NetScaler-Appliance.
2. Erstellen Sie ein HTTP-Callout auf der NetScaler-Appliance und konfigurieren Sie es mit Details zum externen Server und anderen erforderlichen Parametern.
3. Erstellen Sie eine Responder-Richtlinie, um die Antwort zu analysieren, und binden Sie die Richtlinie dann global.
4. Erstellen Sie einen Callout-Agenten auf dem Remoteserver.

Responder aktivieren

Die Responder-Funktion muss aktiviert sein, bevor sie auf der NetScaler-Appliance verwendet werden kann.

So aktivieren Sie den Responder über die GUI

1. Stellen Sie sicher, dass die Responder-Lizenz installiert ist.
2. Erweitern Sie im Konfigurationsprogramm AppExpert, klicken Sie mit der rechten Maustaste auf **Responder**und klicken Sie dann auf **Responder-Funktion aktivieren** .

Erstellen eines HTTP-Callouts auf der NetScaler-Appliance

Erstellen Sie ein HTTP-Callout, HTTP-Callout-4, mit den Parametereinstellungen in der folgenden Tabelle. Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout.

Weitere Informationen finden Sie unter Parameter und Werte für HTTP-Callout-4 pdf.

Erstellen einer Responderaktion

Erstellen Sie eine Responder-Aktion, Action-Responder-4. Erstellen Sie die Aktion mit den in der folgenden Tabelle angegebenen Parametereinstellungen.

Parameter	Wert
Name	Action-Responder-4
Typ	Antworte mit
Ziel	„” HTTP/1.1 200 OK\ r\ nServer: Microsoft-IIS/6.0\ r\ nX-Bereitgestellt von: ASP.NET\ r\ nInhaltslänge: 0\ r\ nMS-Webspeicher: 6.5.6944\ r\ nCache-Steuerung: kein Cache\ r\ n\ r\ n ““

Tabelle 2. Parameter und Werte für Action-Responder-4

So erstellen Sie eine Responder-Aktion mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **AppExpert** > **Responder** > **Actions**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.

3. Geben Sie im Dialogfeld **Responder-Aktion erstellen** unter Name den Text **Action-Responder-4**ein.
4. Klicken Sie unter Typ auf **Antworten mit**.
5. Geben Sie in Target Folgendes ein:

```
""HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By:
   ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\
   nCache-Control: no-cache\r\n\r\n""
<!--NeedCopy-->
```

6. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Erstellen einer Responder-Richtlinie zum Aufrufen des HTTP-Callouts

Erstellen Sie eine Responder-Richtlinie, Policy-Responder-4, die den Anfragetext überprüft und, falls der Text das Wort
Betreff enthält, den HTTP-Callout aufruft, um die E-Mail zu verifizieren. Erstellen Sie die Richtlinie mit den in der folgenden Tabelle aufgeführten Parametereinstellungen. Sie können zwar im Unterknoten Richtlinien eine Responder-Richtlinie erstellen und sie dann mithilfe des Responder-Policy-Managers global binden. In dieser Demonstration wird jedoch
der Responder Policy Manager verwendet, um die
Responder-Richtlinie zu erstellen und global zu binden.

Parameter	Wert
Name	Policy-Responder-4
Aktion	Action-Responder-4
Aktion mit undefiniertem Ergebnis	-Global undefined-result action-
Ausdruck	„HTTP.REQ.BODY (1000) .CONTAINS („urn:schemas:httpmail:subject“) && SYS.HTTP_CALLOUT (HTTP-CALLOUT-4)“

So erstellen Sie mithilfe des Konfigurationsdienstprogramms eine Responder-Richtlinie

1. Navigieren Sie zu **AppExpert** > **Responder**.
2. Klicken Sie im Detailbereich unter **Policy Manager**auf **Responder Policy** Manager.
3. Klicken Sie im Dialogfeld **Responder Policy Manager** auf **Override**Global.
4. Klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf **Neue Richtlinie**.

5. Gehen **Sie im Dialogfeld Responder-Richtlinie erstellen** wie folgt vor:
   a) Geben Sie im Feld Name den Wert **Policy-Responder-4**ein.
   b) Klicken Sie unter Aktion auf **Action-Responder-4**.
   c) Klicken Sie unter Aktion mit undefiniertem Ergebnis auf **Globale** Aktion mit undefiniertem Ergebnis.
   d) Geben Sie in das Textfeld **Ausdruck** Folgendes ein:

```
"HTTP.REQ.BODY(1000).CONTAINS("urn:schemas:httpmail:subject")
   && SYS.HTTP_CALLOUT(HTTP-Callout-4)"
<!--NeedCopy-->
```

   e) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Erstellen eines HTTP-Callout-Agenten auf dem Remoteserver

Sie müssen jetzt einen HTTP-Callout-Agenten auf dem Remote-Callout-Server erstellen. Der HTTP-Callout-Agent empfängt Callout-Anfragen von der NetScaler-Appliance und reagiert entsprechend. Der Callout-Agent ist ein Skript, das für jede Bereitstellung unterschiedlich ist und unter Berücksichtigung der Serverspezifikationen, wie z. B. des Datenbanktyps und der unterstützten Skriptsprache, geschrieben werden muss.

Der folgende Pseudocode enthält Anweisungen zum Erstellen eines Callout-Agents, der eine Liste von Wörtern überprüft, die allgemein als Spam-Mails verstanden werden. Der Agent kann in jeder Programmiersprache Ihrer Wahl implementiert werden. Der Pseudocode darf nur als Richtlinie für die Entwicklung des Callout-Agenten verwendet werden. Sie können zusätzliche Funktionen in das Programm integrieren.

Um Spam-E-Mails mithilfe von Pseudocode zu identifizieren

1. Akzeptieren Sie die E-Mail-Betreffzeile, die von der NetScaler-Appliance bereitgestellt wird.
2. Stellen Sie eine Verbindung zu der Datenbank her, die alle Begriffe enthält, anhand derer der E-Mail-Betreff überprüft wird.
3. Vergleichen Sie die Wörter im E-Mail-Betreff mit der Spam-Wortliste.
4. Formatieren Sie die Antwort so, wie es der HTTP-Callout erfordert.
5. Senden Sie die Antwort an die NetScaler Appliance.

Anwendungsfall: Dynamic Content Switching

January 19, 2021

Dieser Anwendungsfall ermöglicht ein dynamisches Content Switching über ein HTTP-Callout, um den Namen des virtuellen Lastenausgleichsservers zu erhalten, an den die Anforderung weitergeleitet wird.

1. Fügen Sie einen virtuellen Content Switching-Server hinzu.

```
add cs vserver cs_vserver1 HTTP 10.102.29.196 80
<!--NeedCopy-->
```

2. Erstellen Sie ein HTTP-Callout.

```
add policy httpCallout http_callout1
<!--NeedCopy-->
```

3. Konfigurieren Sie das HTTP-Callout so, dass sie mit dem Namen des virtuellen Lastausgleichsservers aus einer Anforderung reagiert, die die Client-IP-Adresse im HTTP-Header X-CLIENT-IP enthält.

```
> set policy httpCallout http_callout1 -IPAddress 10.217.14.23 -
   port 80 -returnType TEXT -hostExpr ""www.get-lbvip.com"" -
   urlStemExpr ""/index.html"" -headers X-CLIENT-IP(CLIENT.IP.SRC)
    -resultExpr "HTTP.RES.BODY(1000).AFTER_STR("<lbvip>").
   BEFORE_STR("<lbvip")"
<!--NeedCopy-->
```

4. Konfigurieren Sie die Content Switching-Aktion, um die Calloutantwort abzurufen.

```
add cs action cs_action1 -targetVserverExpr 'SYS.HTTP_CALLOUT(
   http_callout1)'
<!--NeedCopy-->
```

> Hinweis:
>
> Sie müssen einen virtuellen Lastausgleichsserver an den virtuellen Content Switching-Server binden, um Folgendes zu berücksichtigen:

- Die Nichtverfügbarkeit des virtuellen Lastausgleichsservers, auf den das Callout aufgelöst wird.
- Eine UNDEF-Bedingung, die sich aus dem Ausführen des Callouts ergibt.

```
> bind cs vserver cs_vserver1 -lbvserver default_lbvip
<!--NeedCopy-->
```

5. Konfigurieren Sie die Content Switching-Richtlinie.

```
add cs policy cs_policy1 -rule true -action cs_action1
```



```
<!--NeedCopy-->
```

6. Binden der Content Switching-Richtlinie an den virtuellen Content Switching-Server.

```
bind cs vserver cs_vserver1 -policyName cs_policy1 -priority 10
<!--NeedCopy-->
```

Mustersätze und Datensätze

March 10, 2023

Richtlinienausdrücke für Zeichenfolgenabgleichsoperationen bei einer großen Menge von Zeichenfolgenmustern werden tendenziell lang und komplex. Ressourcen, die durch die Auswertung solcher komplexen Ausdrücke verbraucht werden, sind in Bezug auf Verarbeitungszyklen, Speicher und Konfigurationsgröße von Bedeutung. Mithilfe des Musterabgleichs können Sie einfachere, weniger ressourcenintensive Ausdrücke erstellen.

Abhängig von der Art der Muster, die Sie abgleichen möchten, können Sie eine der folgenden Funktionen verwenden, um den Musterabgleich zu implementieren:

- Ein Mustersatz ist ein Array indizierter Muster, die für den Zeichenfolgenabgleich bei der Auswertung der Standard-Syntaxrichtlinie verwendet werden. Beispiel für einen Mustersatz: Bildtypen {svg, bmp, PNG, GIF, tiff, jpg}.
- Ein Datensatz ist eine spezielle Form von Mustersatz. Es ist ein Array von Mustern der Typen Zahl (Integer), IPv4-Adresse oder IPv6-Adresse.

Der Unterschied zwischen `patset` und `dataset` besteht darin, dass wir in `dataset` die Randbedingung vergleichen. Wenn die Eingabezeichenfolge beispielsweise 1.1.1.11 ist und davon ausgeht, dass das 1.1.1.1-Muster an a `patset` und a `dataset` des IPv4-Typs gebunden ist, wird eine `patset` Und-Datenmenge konfiguriert, um zu überprüfen, ob die IP-Adresse in der Anforderung vorhanden ist. `patset` gibt nach der Auswertung zurück, dass 1.1.1.1 in der Eingabe vorhanden ist, die Auswertung `dataset` jedoch falsch ist. Dies liegt an einem Boundary-Check-in, bei dem die IP-Adresse nicht Teil einer anderen IP-Adresse war. Das bedeutet, dass es nach dem gebundenen Muster keine ganze Zahl geben darf.

Oft können Sie entweder Mustersätze oder Datensätze verwenden. In Fällen, in denen Sie jedoch bestimmte Übereinstimmungen für numerische Daten oder IPv4- und IPv6-Adressen wünschen, müssen Sie Datensätze verwenden.

> **Hinweise:**
>
> - Mustersätze und Datensätze können nur in Standard-Syntaxrichtlinien verwendet werden.

> - Ab Version 13.1 Build 42.x und höher können Sie 50000 Muster an einen Mustersatz binden. Mit der Mustersatzdatei können nur 10000 Muster an einen Mustersatz gebunden werden. Wenn der Mustersatz beim Streaming verwendet wird, können außerdem nur 5000 Muster an diesen Mustersatz gebunden werden. Ein Mustersatz für das Streaming wird im Suchparameter Rewrite Action, im HTTP-Body oder im auf der TCP-Nutzlast basierenden Ausdruck verwendet.

So funktioniert der Zeichenkettenabgleich mit Mustersätzen und Datensätzen

May 11, 2023

Ein Mustersatz oder Datensatz enthält einen Satz von Mustern, und jedem Muster wird ein eindeutiger Index zugewiesen. Wenn eine Richtlinie auf ein Paket angewendet wird, identifiziert ein Ausdruck eine auszuwertende Zeichenfolge, und der Operator vergleicht die Zeichenfolge mit den im Mustersatz oder Datensatz definierten Mustern, bis eine Übereinstimmung gefunden wird oder alle Muster verglichen wurden. Dann gibt der Operator je nach Funktion entweder einen booleschen Wert zurück, der angibt, ob ein passendes Muster gefunden wurde oder nicht, oder den Index des Musters, das der Zeichenfolge entspricht.

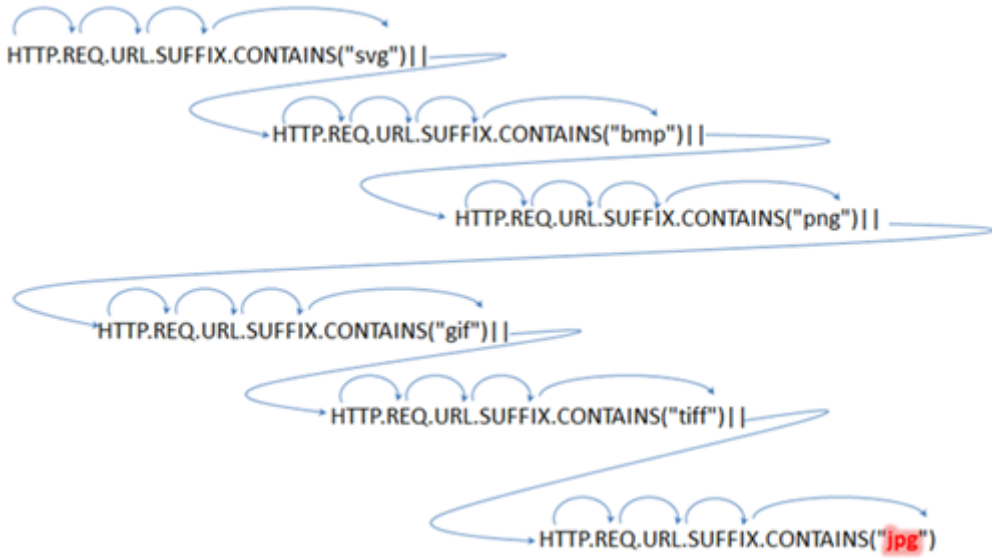
Hinweis: In diesem Thema wird die Funktionsweise eines Mustersatzes erläutert. Datensätze funktionieren auf die gleiche Weise. Der einzige Unterschied zwischen Mustersätzen und Datensätzen ist die Art der im Satz definierten Muster.

Betrachten Sie den folgenden Anwendungsfall, um zu verstehen, wie Muster für den Zeichenfolgenabgleich verwendet werden können.

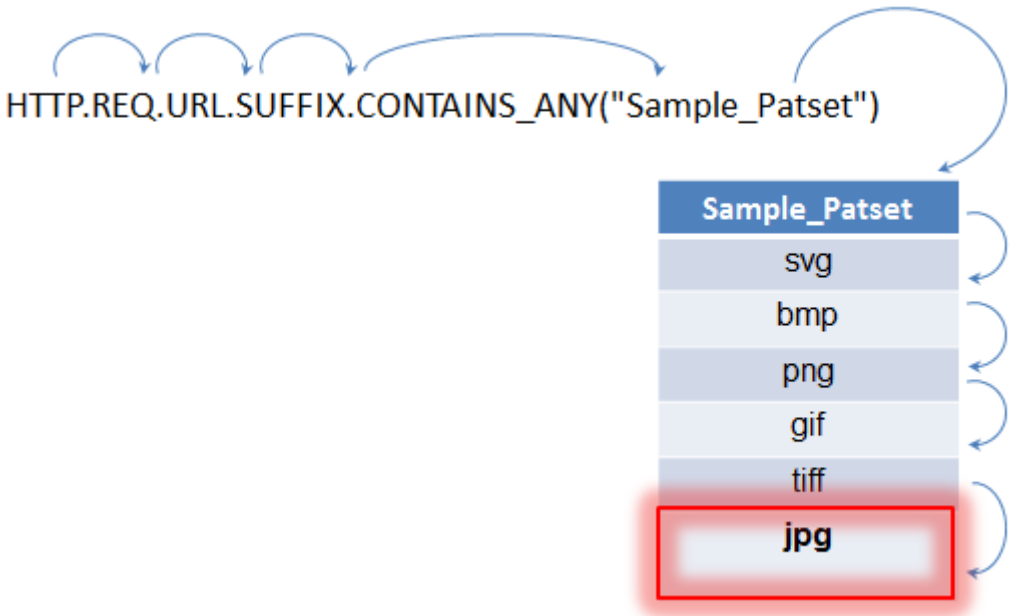
Sie möchten feststellen, ob das URL-Suffix (Zieltext) eine der Bilddateierweiterungen enthält. Ohne Mustersätze zu verwenden, müssten Sie einen komplexen Ausdruck wie folgt definieren:

```
1 HTTP.REQ.URL.SUFFIX.CONTAINS("svg") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("
     bmp") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("png") ¦¦
2 HTTP.REQ.URL.SUFFIX.CONTAINS("gif") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("
     tiff") ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS("jpg")
3 <!--NeedCopy-->
```

Wenn die URL das Suffix „jpg“ mit dem obigen zusammengesetzten Ausdruck hat, muss die NetScaler-Appliance den gesamten zusammengesetzten Ausdruck sequentiell von einem Unterausdruck zum nächsten durchlaufen, um festzustellen, dass sich die Anfrage auf ein JPG-Bild bezieht. Die folgende Abbildung zeigt die Schritte des Prozesses.



Wenn ein zusammengesetzter Ausdruck Hunderte von Unterausdrücken enthält, ist der obige Prozess ressourcenintensiv. Eine bessere Alternative ist ein Ausdruck, der einen Mustersatz aufruft, wie in der folgenden Abbildung dargestellt.



Während der Richtlinienauswertung, wie oben gezeigt, vergleicht der Operator (CONTAINS_ANY) die in der Anfrage identifizierte Zeichenfolge mit den im Mustersatz definierten Mustern, bis eine Übereinstimmung gefunden wird. Mit dem Ausdruck Sample_Patset werden die mehrfachen Iterationen durch sechs Unterausdrücke auf nur einen reduziert.

Da keine zusammengesetzten Ausdrücke konfiguriert werden müssen, die einen Zeichenfolgenabgleich mit mehreren OR-Operationen durchführen, vereinfachen Mustersätze oder Datensätze die Kon-

figuration und beschleunigen die Verarbeitung von Anfragen und Antworten.

Mustersatz konfigurieren

May 11, 2023

Um einen Mustersatz zu konfigurieren, müssen Sie die Zeichenketten angeben, die als Muster dienen sollen. Sie können jedem dieser Muster manuell einen eindeutigen Indexwert zuweisen, oder Sie können zulassen, dass die Indexwerte automatisch zugewiesen werden.

> **Hinweis:**
>
> Bei Mustersätzen wird zwischen Groß- und Kleinschreibung unterschieden (es sei denn, Sie geben den Ausdruck an, um Groß- und Kleinschreibung zu ignorieren). Daher ist das Zeichenfolgenmuster "product1" beispielsweise nicht dasselbe wie das Zeichenfolgenmuster "Product1".

Wichtige Punkte zu Indexwerten:

- Sie können denselben Indexwert nicht an mehr als ein Muster binden.
- Ein automatisch zugewiesener Indexwert ist eine Zahl größer als der höchste Indexwert der vorhandenen Muster innerhalb des Mustersatzes. Wenn der höchste Indexwert vorhandener Muster in einem Mustersatz beispielsweise 104 ist, ist der nächste automatisch zugewiesene Indexwert 105.
- Wenn Sie keinen Index für das erste Muster angeben, wird diesem Muster automatisch der Indexwert 1 zugewiesen.
- Indexwerte werden nicht automatisch regeneriert, wenn ein oder mehrere Muster gelöscht oder geändert werden. Wenn der Satz beispielsweise fünf Muster mit Indizes von 1 bis 5 enthält und wenn das Muster mit einem Index von 3 gelöscht wird, werden die anderen Indexwerte im Mustersatz nicht automatisch regeneriert, um Werte von 1 bis 4 zu erzeugen.
- Der maximale Indexwert, der einem Muster zugewiesen werden kann, ist 4294967290. Wenn dieser Wert bereits einem Muster im Satz zugewiesen ist, müssen Sie allen neu hinzugefügten Mustern manuell Indexwerte zuweisen. Ein unbenutzter Indexwert, der niedriger als ein aktuell verwendeter Wert ist, kann nicht automatisch zugewiesen werden.

Mustersatz über die Befehlszeilenschnittstelle konfigurieren

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Erstellen Sie einen Mustersatz.

   ```
   add policy patset <name>
   ```


Beispiel:

```
add policy patset samplepatset
```

1. Binden Sie Muster an den Mustersatz.

   ```
   bind policy patset <name> <string> [-index <positive_integer>][-charset
    ( ASCII | UTF_8 )] [-comment <string>]
   ```

Beispiel:

```
bind policy patset samplepatset product1 -index 1 -comment short description
 about the pattern bound to the pattern set
```

Hinweis: Wiederholen Sie diesen Schritt für alle Muster, die Sie an den Mustersatz binden möchten.

1. Überprüfen Sie die Konfiguration.

```
show policy patset <name>
```

Konfigurieren Sie einen Mustersatz über das Konfigurationsprogramm

1. Navigieren Sie zu **AppExpert** > **Pattern Sets**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um das Dialogfeld **Mustersatz erstellen** zu öffnen.
3. Geben Sie im Textfeld Name einen Namen für den Mustersatz an.
4. Geben Sie unter Muster angeben das erste Muster ein und geben Sie optional Werte für die folgenden Parameter an:
   - Backslash als Escape-Zeichen behandeln — Aktivieren Sie dieses Kontrollkästchen, um festzulegen, dass alle umgekehrten Schrägstriche, die Sie möglicherweise in das Muster aufnehmen, als Escape-Zeichen behandelt werden.
   - Index — Ein vom Benutzer zugewiesener Indexwert von 1 bis 4294967290.
5. Stellen Sie sicher, dass Sie die richtigen Zeichen eingegeben haben, und klicken Sie dann auf **Hinzufügen**.
6. Wiederholen Sie die Schritte 4 und 5, um weitere Muster hinzuzufügen, und klicken Sie dann auf **Erstellen**.

Konfiguration dateibasierter Mustersätze

Die NetScaler-Appliance unterstützt dateibasierte Mustersätze.

Dateibasierte Mustersätze über die CLI konfigurieren

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- Importieren Sie eine neue Mustersatzdatei in die NetScaler-Appliance.


```
import policy patsetfile <src> <name> -delimiter <char> -charset
   <ASCII | UTF_8>
<!--NeedCopy-->
```

Beispiel:

```
import policy patsetfile local:test.csv clientids_list -
   delimiter ,
<!--NeedCopy-->
```

Sie können eine Datei von einem lokalen Gerät, HTTP-Server oder FTP-Server importieren. Um die Datei von Ihrem lokalen Gerät hinzuzufügen, muss die Datei am Speicherort `/var/tmp` verfügbar sein.

- Fügen Sie der Paket-Engine eine Pattern-Set-Datei hinzu.

```
add policy patsetfile <patset filename>
<!--NeedCopy-->
```

Beispiel:

```
add policy patsetfile clientids_list
<!--NeedCopy-->
```

- Aktualisieren Sie eine vorhandene Pattern-Set-Datei auf der NetScaler-Appliance.

```
update policy patsetfile <patset filename>
<!--NeedCopy-->
```

Beispiel:

```
update policy patsetfile clientids_list
<!--NeedCopy-->
```

- Binden Sie Muster an den Mustersatz.

```
add policy patset <patset name> -patsetfile <patset filename>
<!--NeedCopy-->
```

Beispiel:

```
add policy patset clientid_patset -patsetfile clientids_list
<!--NeedCopy-->
```

- Überprüfen Sie die Konfiguration.


```
show policy patsetfile clientids_list

Name: clientids_list
Patset Name: clientid_patset
Number of Imported Patterns: 8
Number of Bound Patterns: 8
(All the patterns bound successfully)

Done
<!--NeedCopy-->
```

Dateibasierte Mustersätze über die GUI konfigurieren

1. Navigieren Sie zu **AppExpert-> Pattern Set Files**.
2. Klicken Sie im Bereich **Importiert** auf **Importieren**.
3. Wählen Sie auf der Seite **Policy Patset File konfigurieren** die Datei aus, die Sie importieren möchten, und klicken Sie auf **OK**.
4. Wählen Sie die importierte Datei aus und klicken Sie auf **Hinzufügen**.
5. Geben Sie auf der Seite **Policy-Patset-Datei erstellen** die Details ein und klicken Sie auf **Erstellen**, um einen Richtlinienmustersatz hinzuzufügen.

Konfigurieren eines Datensatzes

September 22, 2022

Um einen Datensatz zu konfigurieren, müssen Sie die Zeichenfolgen für den Server als Muster angeben, einen Typ zuweisen (Zahl, IPv4-Adresse oder IPv6-Adresse) und den Datensatzbereich konfigurieren. Sie können dem Muster manuell einen eindeutigen Indexwert zuweisen oder die automatische Zuweisung der Indexwerte zulassen. Das Dataset ist nicht mit HTTP oder einem 7-Layer-Protokoll verwandt. Es funktioniert nur bei Text oder Zeichenfolge. Es gibt verschiedene Arten von Datensätzen wie NUM, ULONG, IPv4, IPv6, MAC, DOUBLE. Sie können einen Typ auswählen und den Datensatzbereich basierend auf dem angegebenen Typ definieren.

> **Hinweis:**
>
> Bei Richtliniendatensätzen wird zwischen Groß- und Kleinschreibung unterschieden (es sei denn, Sie geben an, dass der Ausdruck sie ignorieren soll). Daher stimmt die MAC-Adresse ff:ff:ff:ff:ff beispielsweise nicht mit der MAC-Adresse FF:FF:FF:FF:FF:FF überein.

Die Regeln, die für Indexwerte von Datensätzen angewendet werden, sind ähnlich wie Mustersätze. Informationen zu Indexwerten finden Sie unter Konfigurieren eines Mustersatzes.

Konfigurieren eines Datensatzes

Führen Sie die folgenden Schritte aus, um einen Datensatz zu konfigurieren:

1. Hinzufügen eines Policy-Datensets
2. Bindungsmuster an einen Richtliniendatensatz
3. Hinzufügen eines Richtlinienausdrucks
4. Überprüfen der Richtlinienkonfiguration

Hinzufügen eines Policy-Datensets

Führen Sie an der Eingabeaufforderung Folgendes aus:

```
add policy dataset <name> <type>
```

Beispiel:

```
add policy dataset ds1 ipv4 -comment numbers
```

Binden eines Musters an den Datensatz

Geben Sie in der Befehlszeile Folgendes ein:

```
bind policy dataset <name> <value> [-index <positive_integer>] [-endRange <string>] [-comment <string>]
```

Beispiel:

```
bind policy dataset ds1 1.1.1.1 -endRange 1.1.1.10 -comment short description about the pattern bound to the data set
```

> **Hinweis:**
>
> Sie müssen diesen Schritt für alle Muster wiederholen, die Sie an den Datensatz binden möchten. Sie können nur bis zu 5000 Muster an einen Datensatz binden.
>
> Und ein Datensatzbereich darf sich nicht mit anderen Bereichen überschneiden, die an einen Datensatz gebunden sind, und darf keine Einzelwerte enthalten, die an den Datensatz gebunden sind. Wenn Sie einen Datensatz mit einem überlappenden Bereich binden, führt dies zu einem Fehler.

Beispiel:


```
add policy dataset ip_set ipv4
 Done
bind policy dataset ip_set 2.2.2.25
 Done
bind policy dataset ip_set 2.2.2.20 -endRange 2.2.2.30
ERROR: The range overlaps an existing range or includes a value bound
   to the dataset.
<!--NeedCopy-->
```

Ein Wert wird als in der Datenmenge enthalten betrachtet, wenn er entweder einem einzelnen an den Datensatz gebundenen Wert entspricht oder zwischen dem unteren Wert und dem oberen Wert (niedrigerer Wert <= Wert && Wert <- oberer Wert) für einen an den Datensatz gebundenen Bereich liegt.

Richtlinienausdruck in einem Richtliniendatensatz verwenden

Geben Sie in der Befehlszeile Folgendes ein:

```
add policy expression exp1 http.req.body(100).contains_any("ds1")
```

Wo,
Der Ausdruck prüft, ob in den ersten 100 Byte des Hauptteils der HTTP-Anforderung ein Muster (oder Muster innerhalb des Bereichs) vorhanden ist, das an den Datensatz ds1 gebunden ist.

Überprüfen der Datensatzkonfiguration

Geben Sie in der Befehlszeile Folgendes ein:

```
show policy dataset ds1
> show policy dataset ds1
```

Beispiel:

```
        Dataset:        ds1
         Type:   IPV4
1)       Bound Dataset Range from: 1.1.1.1       through: 1.1.1.10
          Index:  1
<!--NeedCopy-->
```

Konfigurieren eines Datensatzes mit dem Konfigurationsdienstprogramm

Folgen Sie den unten angegebenen Schritten, um einen Richtliniendatensatz zu konfigurieren:

1. Navigieren Sie zu **AppExpert > Datensätze**.

2. Klicken Sie im Detailbereich unter Datensätze auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Datensatz konfigurieren** die folgenden Parameter ein.
   a) Name. Name des Richtliniendatensatzes.
   b) Typ. Typ des Werts, der an den Datensatz gebunden werden soll.

   Konfigurieren des Datensatzes
4. Klicken Sie auf **Einfügen**, um den Datensatzwert eines bestimmten Typs zu binden.
   a) Wert. Wert des angegebenen Typs, der mit dem Datensatz verknüpft ist.
   b) Indizieren. Der Indexwert des Datensatzes.
   c) Bereich beenden. Der Datensatzeintrag. Dies ist ein Bereich <value> von <end_range>.
   d) Kommentare. Eine kurze Beschreibung des Datensatzes.

   Datensatzbindung
5. Klicken Sie auf **Einfügen** und **schließen**.
6. Geben Sie Kommentare ein.
7. Klicken Sie auf **Erstellen** und **Schließen**.

CIDR-Subnetznotation in IPv4- und IPv6-Adressen für Policy-Dataset

Die Richtlinien-Datensätze für IPv4 und IPv6-Adresse ermöglichen, dass der gebundene Wert Subnetze mit der CIDR-Notation sein kann. Die CIDR-Notation gibt die Adresse und den Bereich des Subnetzes an. CIDR-Notation <address>/<n>, wobei <address> die erste Adresse im Subnetz und eine Ganzzahl <n> ist, die die Anzahl der in der Subnetzmaske gesetzten Bits ganz links angibt, die den Bereich des Subnetzes definiert.

Beispiel: 192.128.0.0/10 stellt ein IPv4-Subnetz dar, das bei der Adresse 192.129.0.0 mit einer Maske 0xFFC0000 (255.192.0.0) beginnt.

Beispiel:

```
add policy dataset ds1 ipv4
bind policy dataset ds1 192.128.0.0/10
show policy dataset ds1
    Dataset: ds1
    Type: IPV4
Bound Dataset Value: 192.128.0.0/10 Index: 1 Comment: Subnet range from
    192.128.0.0 through 192.191.255.255

<!--NeedCopy-->
```

Ein Beispiel für die Verwendung dieses Datensatzes in einem Ausdruck:


```
add responder policy resp_ipv4_pol client.ip.src.typecast_text_t.
    equals_any("ds1") drop
<!--NeedCopy-->
```

Beispiel für ein IPv6-Subnetz:

Ein Beispiel für ein IPv6-Subnetz wäre 2001:db8:123::/56, das bei Adresse 2001:db8:123:: mit Maske FFFF:FFFF:FFFF:FF00:: beginnt.

```
add policy dataset ds2 ipv6
bind policy dataset ds2 2001:db8:123::/56
show policy dataset ds2
    Dataset: ds2
    Type: IPV61
Bound Dataset Value: 2001:db8:123::/56 Index: 1 Comment: Subnet range
    from 2001:db8:123:: through 2001:db8:123:ff:ffff:ffff:ffff:ffff

<!--NeedCopy-->
```

Die Startadresse des Subnetzes wird durch die angegebene Adresse bestimmt, die durch die Subnetzmaske maskiert ist. Eine Warnung wird ausgegeben, wenn die angegebene Adresse nicht mit der resultierenden Startadresse übereinstimmt.

Beispiel:

```
bind policy dataset ds1 192.168.0.0/10
Warning: Starting subnet address masked using subnet mask to create new
     starting address [192.128.0.0]
show policy dataset ds1
    Dataset: ds1
    Type: IPV4
Bound Dataset Value:192.168.0.0/10 Index: 1 Comment: Subnet range from
    192.128.0.0 through 192.191.255.255

<!--NeedCopy-->
```

Ein Beispiel für die Verwendung dieses Datensatzes in einem Ausdruck:

```
add responder policy resp_ipv6_pol client.ipv6.src.typecast_text_t.
    equals_any("ds2") drop
<!--NeedCopy-->
```


Verwenden von Mustersätzen und Datensätzen

October 8, 2021

Erweiterte Richtlinienausdrücke, die Mustersätze oder Datensätze als Argument verwenden, können verwendet werden, um Zeichenfolgenabgleichsoperationen durchzuführen.

Die Verwendung lautet wie folgt:

```
<text>.<operator>("<name>")
<!--NeedCopy-->
```

Wobei:

- <text> ist der Ausdruck, der eine Zeichenfolge in einem Paket identifiziert. Beispiel: HTTP.REQ.HEADER(“Host”).
- <operator> ist einer der in der Tabelle Pattern Set Types beschriebenen Operatoren pdf.

Informationen zur Verwendung von Beispielen finden Sie unter Beispielverwendung.

Beispiel für Verwendung

August 19, 2021

Um die Verwendung von Mustersätzen in Ausdrücken zu verstehen, betrachten Sie das Beispiel eines Mustersatzes namens imagetypes.

Muster	Indexwert
svg	1
bmp	2
png	3
gif	4
tiff	5
jpg	6

Tabelle 1. Mustersatz Bildtypen

Beispiel 1: Bestimmen Sie, ob das Suffix einer HTTP-Anforderung eine der Dateierweiterungen ist, die im Mustersatz imagetypes definiert sind.

- **Ausdruck.** HTTP.REQ.URL.SUFFIX.EQUALS_ANY(“imagetypes”)
- **Beispiel-URL.** `http://www.example.com/homepageicon.jpg`
- **Ergebnis.** TRUE

Beispiel 2: Bestimmen Sie, ob das Suffix einer HTTP-Anforderung eine der Dateierweiterungen ist, die im Mustersatz imagetypes definiert sind, und geben Sie den Index dieses Musters zurück.

- **Ausdruck.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”)
- **Beispiel-URL.** `http://www.example.com/mylogo.png`
- **Ergebnis.** 4 (Der Indexwert des Musters gif.)

Beispiel 3: Verwenden Sie den Indexwert eines Musters, um zu bestimmen, ob sich das URL-Suffix innerhalb eines angegebenen Indexwertebereichs befindet.

- **Ausdruck.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”).GE(3) && HTTP.REQ.URL.SUFFIX.EQUALS_
- **Beispiel-URL.** `http://www.example.com/mylogo.png`
- **Ergebnis.** TRUE (Der Indexwert von GIF-Dateitypen ist 4.)

Beispiel 4: Implementieren Sie einen Satz von Richtlinien für Dateierweiterungen bmp, jpg und png und einen anderen Satz von Richtlinien für GIF-, TIFF- und SVG-Dateien.

Ein Ausdruck, der den Index eines übereinstimmenden Musters zurückgibt, kann verwendet werden, um Verkehrsuntermengen für eine Webanwendung zu definieren. Die folgenden beiden Ausdrücke könnten in Content Switching-Richtlinien für einen virtuellen Content Switching-Server verwendet werden:

- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”).LE(3)
- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”).GE(4)

Variablen

May 11, 2023

Variablen sind benannte Objekte, die Informationen in Form von Tokens speichern. Diese Token werden innerhalb und zwischen verschiedenen Transaktionen auf der NetScaler Appliance für interne Berechnungen und Richtlinienverarbeitung verwendet.

Die NetScaler Appliance unterstützt die Erstellung von Variablen der folgenden Typen:

- **Singleton-Variablen.** Kann einen einzelnen Wert eines der folgenden Typen haben: ulong und text (max-size). Der ulong-Typ ist eine vorzeichenlose 64-Bit-Ganzzahl, der Texttyp ist eine Folge von Bytes und max-size ist die maximale Anzahl von Byte in der Sequenz.
- **Variablen zuordnen.** Maps enthalten Werte, die Schlüsseln zugeordnet sind: Jedes Schlüssel-Wert-Paar wird als Zuordnungseintrag bezeichnet. Der Schlüssel für jeden Eintrag ist innerhalb der Karte einzigartig. Karten werden wie folgt spezifiziert:

map (Schlüsseltyp, Werttyp, Maximalwerte).

Hierbei gilt:

- *key_type* ist der Datentyp des Schlüssels. Es ist vom Typ Text (maximale Größe).
- *value_type* ist der Datentyp der Werte der Map. Es kann vom Typ Ulong oder Text (maximale Größe) sein.
- *max-values* ist die maximale Anzahl von Einträgen, die die Map enthalten kann. Es ist vom Typ Ulong.

Die Werte für diese Variablen werden mithilfe von Zuweisungen festgelegt, die bei politischen Aktionen aufgerufen werden müssen.

Gültigkeitsbereich der Variablen

Eine Map-Variable oder eine Singleton-Variable kann einen globalen Gültigkeitsbereich haben. Alternativ kann der Gültigkeitsbereich einer Singleton-Variablen auf eine einzelne Transaktion beschränkt werden.

- **Globale Bereichsvariable** - Eine Variable mit globalem Gültigkeitsbereich (Standard) hat nur eine Instanz, und diese Instanz hat dieselben Werte für alle Kerne einer NetScaler Appliance und für alle Knoten einer Cluster- oder HA-Konfiguration. Globale Variablenwerte existieren, bis sie explizit gelöscht werden, bis sie ablaufen oder bis eine eigenständige Appliance neu gestartet wird oder bis alle Knoten einer Cluster- oder HA-Konfiguration neu gestartet werden.
- **Transaktionsbereichsvariable** - Eine Variable mit Transaktionsumfang hat für jede Transaktion, die von der NetScaler Appliance verarbeitet wird, eine separate Instanz mit einem eigenen Wert. Wenn die Transaktionsverarbeitung abgeschlossen ist, wird der Wert der Transaktionsvariablen gelöscht.

> **Hinweis**: Variablen für den Transaktionsumfang sind in NetScaler Version 10.5.e oder höher verfügbar.

Konfigurieren und Verwenden von Variablen

May 11, 2023

Sie müssen zuerst eine Variable erstellen und dann einen Wert zuweisen oder die Operation angeben, die für die Variable ausgeführt werden muss. Nachdem Sie diese Vorgänge ausgeführt haben, können Sie die Zuweisung als Richtlinienaktion verwenden.

Hinweis: Nach der Konfiguration können die Einstellungen einer Variablen nicht geändert oder zurückgesetzt werden. Wenn die Variable geändert werden muss, müssen die Variable und alle

Verweise auf die Variable (Ausdrücke und Zuweisungen) gelöscht werden. Die Variable kann dann mit neuen Einstellungen erneut hinzugefügt werden, und die Verweise (Ausdrücke und Zuweisungen) können erneut hinzugefügt werden.

So konfigurieren Sie Variablen mithilfe der Befehlszeilenschnittstelle

1. Erstellen Sie eine Variable.

```
add ns variable <name> -type <string> [-scope global] [-ifFull ( undef | lru )] [-ifValueTooBig ( undef | truncate )] [-ifNoValue ( undef | init )] [-init <string>] [-expires <positive_integer>] [-comment <string>]
<!--NeedCopy-->
```

Hinweis: Eine Beschreibung der Befehlsparameter finden Sie auf der Manpage „man add ns variable“.

Beispiel 1: Erstellen Sie eine Ulang-Variable mit dem Namen „my_counter“ und initialisieren Sie sie auf 1.

```
add ns variable my_counter  - type ulong -init 1
<!--NeedCopy-->
```

Beispiel 2: Erstellen Sie eine Map mit dem Namen „user_privilege_map“. Die Map wird Schlüssel mit einer maximalen Länge von 15 Zeichen und Textwerte mit einer maximalen Länge von 10 Zeichen mit einem Maximum von 10000 Einträgen enthalten.

```
add ns variable user_privilege_map -type map(text(15),text(10),10000)
<!--NeedCopy-->
```

Hinweis: Wenn die Map 10000 nicht abgelaufene Einträge enthält, wird bei Zuweisungen für neue Schlüssel einer der am wenigsten verwendeten Einträge wiederverwendet. Standardmäßig initialisiert ein Ausdruck, der versucht, einen Wert für einen nicht existierenden Schlüssel abzurufen, einen leeren Textwert.

Weisen Sie der Variablen den Wert zu, oder geben Sie die Operation an, die für die Variable ausgeführt werden soll. Dies geschieht, indem eine Aufgabe erstellt wird.

```
add ns assignment <name> -variable <expression> [-set <expression> | -add <expression> | -sub <expression> | -append <expression> | -clear ] [-comment <string>]
<!--NeedCopy-->
```

Hinweis: Eine Variable wird mithilfe des Variablenselektors ($) referenziert. Daher wird **$variable1** verwendet, um auf Text- oder Ulang-Variablen zu verweisen. In ähnlicher Weise wird **$variable2 [key-expression]** verwendet, um auf Map-Variablen zu verweisen.

Beispiel 1: Definieren Sie eine Zuweisung mit dem Namen „inc_my_counter“, die automatisch 1 zur Variablen „my_counter“ hinzufügt.

```
1 add ns assignment inc_my_counter -variable $my_counter -add 1
2 <!--NeedCopy-->
```

Beispiel 2: Definieren Sie eine Zuweisung mit dem Namen „set_user_privilege“, die der Variablen „user_privilege_map“ einen Eintrag für die IP-Adresse des Clients mit dem vom HTTP-Callout „get_user_privilege“ zurückgegebenen Wert hinzufügt.

```
1 add ns assignment set_user_privilege -variable $user_privilege_map[
     client.ip.src.typecast_text_t] -set sys.http.callout(
     get_user_privilege)
2 <!--NeedCopy-->
```

Hinweis: Wenn für diesen Schlüssel bereits ein Eintrag vorhanden ist, wird der Wert ersetzt. Andernfalls wird ein neuer Eintrag für den Schlüssel und den Wert hinzugefügt. Basierend auf der vorherigen Deklaration für user_privilege_map wird, falls die Map bereits 10000 Einträge enthält, einer der zuletzt verwendeten Einträge für den neuen Schlüssel und Wert wiederverwendet.

1. Rufen Sie die Variablenzuweisung in einer Richtlinie auf.

   Es gibt zwei Funktionen, die mit Kartenvariablen arbeiten können.

   - **$name.valueExists (Schlüsselausdruck).** Gibt „True“ zurück, wenn die Map, die durch den Schlüsselausdruck ausgewählt wurde, einen Wert enthält. Andernfalls wird false zurückgegeben. Diese Funktion aktualisiert die Ablaufzeit- und LRU-Informationen, wenn der Karteneintrag existiert, erstellt jedoch keinen neuen Karteneintrag, wenn der Wert nicht existiert.
   - **$name.valueCount.** Gibt die Anzahl der Werte zurück, die die Variable derzeit enthält. Dies ist die Anzahl der Einträge in einer Map. Für eine Singleton-Variable ist dies 0, wenn die Variable nicht initialisiert ist, oder andernfalls 1.

   Beispiel: Rufen Sie die Zuweisung mit dem Namen „set_user_privilege“ mit einer Komprimierungsrichtlinie auf.

```
1 add cmp policy set_user_privilege_pol -rule $user_privilege_map.
     valueExists(client.ip.src.typecast_text_t).not -resAction
     set_user_privilege
2 <!--NeedCopy-->
```

Anwendungsfall zum Einfügen eines HTTP-Headers in die Antwortseite

Das folgende Beispiel zeigt ein Beispiel für eine Singleton-Variable.

Fügen Sie eine Singleton-Variable vom Typ Text hinzu. Diese Variable kann maximal 100 Byte Daten enthalten.

```
add ns variable http_req_data -type text(100) -scope transaction
<!--NeedCopy-->
```

Fügen Sie eine Zuweisungsaktion hinzu, die verwendet wird, um die HTTP-Anforderungsdaten in der Variablen zu speichern.

```
add ns assignment set_http_req_data -variable $http_req_data -set http.
   req.body(100)
<!--NeedCopy-->
```

Fügen Sie eine Rewrite-Aktion hinzu, um den HTTP-Header einzufügen, dessen Wert aus der Variablen abgerufen wird.

```
add rewrite action act_ins_header insert_http_header user_name
   $http_req_data.after_str("user_name").before_str("password")
<!--NeedCopy-->
```

Fügen Sie eine Rewrite-Richtlinie hinzu, die während der Anfrage ausgewertet wird, und führen Sie Zuweisungsmaßnahmen zum Speichern von Daten durch. Wenn wir diese Richtlinie erreichen, ergreifen wir eine Zuweisungsaktion und speichern die Daten in der Variablen ns (http_req_data)

```
add rewrite policy pol_set_variable true set_http_req_data

bind rewrite global pol_set_variable 10 -type req_dEFAULT
<!--NeedCopy-->
```

Fügen Sie eine Rewrite-Policy hinzu, die in der Antwortzeit ausgewertet wird, und fügen Sie der Antwort einen HTTP-Header hinzu.

```
add rewrite policy pol_ins_header true act_ins_header

bind rewrite global pol_ins_header 10 -type res_dEFAULT
<!--NeedCopy-->
```

Aktion „Zuweisung“

In einer NetScaler-Appliance wird eine an die Richtlinie gebundene Zuweisungsaktion ausgelöst, wenn die Richtlinienregel als wahr ausgewertet wird. Die Aktion aktualisiert den Wert in der Variablen, der bei nachfolgenden Bewertungen der Policy-Regeln verwendet werden kann. Auf diese Weise kann dieselbe Variable aktualisiert und für nachfolgende politische Bewertungen in

derselben Funktion verwendet werden. Bisher führte die Appliance Zuweisungsaktionen erst aus, nachdem alle Richtlinien in der Funktion ausgewertet wurden und die Richtlinien der zugehörigen Zuweisungsaktionen als wahr bewertet wurden. Daher kann der durch die Zuweisungsaktion festgelegte Variablenwert bei den nachfolgenden Bewertungen der Richtlinienregeln innerhalb des Features nicht verwendet werden.

Diese Funktionalität lässt sich anhand eines Anwendungsfalls besser verstehen, der die Zugriffsliste für Clients auf einer NetScaler-Appliance steuert. Die Zugriffsentscheidung wird von einem separaten Webservice bereitgestellt. Die Anfrage `GET /client-access?<client-IP-address>` gibt eine Antwort mit "BLOCK" oder "ALLOW" im Text zurück. Das HTTP-Callout ist so konfiguriert, dass es die IP-Adresse des Clients enthält, die einer eingehenden Anfrage zugeordnet ist. Wenn die NetScaler-Appliance eine Anfrage von einem Client empfängt, generiert die Appliance die Callout-Anforderung und sendet sie an den Callout-Server, der eine Datenbank mit IP-Adressen auf der schwarzen Liste hostet, und einen HTTP-Callout-Agent, der überprüft, ob die IP-Adresse des Clients in der Datenbank aufgeführt ist. Der HTTP-Callout-Agent empfängt die Callout-Anforderung, überprüft, ob die IP-Adresse des Clients aufgeführt ist, und sendet eine Antwort. Die Antwort ist ein Statuscode 200, 302 zusammen mit „BLOCK" oder „ALLOW" im Text. Basierend auf dem Statuscode führt die Appliance die Richtlinienbewertung durch. Wenn die Richtlinienauswertung zutrifft, wird die Zuweisungsaktion sofort ausgelöst und die Aktion setzt den Wert auf die Variable. Die Appliance verwendet diesen Variablenwert und legt ihn für die nachfolgende Richtlinienbewertung im selben Modul fest.

Anwendungsfall für die Konfiguration einer Zuweisungsaktion

Gehen Sie wie folgt vor, um die Zuweisungsaktion zu konfigurieren und Variablen für nachfolgende Richtlinien zu verwenden:

1. Die Zugriffsentscheidung wird von einem separaten Webservice bereitgestellt, wobei die Anfrage eine Antwort mit BLOCK oder ALLOW im Text zurückgibt.

   ```
   GET /url-service>/url-allowed?<URL path>
   ```

2. Richten Sie eine Map-Variable ein, um die Zugriffsentscheidungen für URLs zu speichern.

   ```
   add ns variable url_list_map -type 'map(text(1000),text(10),10000)'
   ```

3. Richten Sie ein HTTP-Callout ein, um die Zugriffsanfrage an den Webservice zu senden.

   ```
   add policy httpCallout url_list_callout -vserver url_vs -returnType
   TEXT -urlStemExpr '"/url-allowed?" + HTTP.REQ.URL.PATH'-resultExpr '
   HTTP.RES.BODY(10)'
   ```

4. Richten Sie eine Zuweisungsaktion ein, um das Callout aufzurufen, um die Zugriffsentscheidung abzurufen, und weisen Sie es dem Map-Eintrag für die URL zu.

   ```
   add ns assignment client_access_assn -variable '$client_access_map[
   ```



```
CLIENT.IP.SRC.TYPECAST_TEXT_T]'-set SYS.HTTP_CALLOUT(client_access_callout
)
```

5. Richten Sie eine Responder-Aktion ein, um eine 403-Antwort zu senden, wenn eine URL-Anfrage blockiert wird.

   ```
   add responder action url_list_block_act respondwith '"HTTP/1.1 403
   Forbidden\\r\\n\\r\\n"'
   ```

6. Richten Sie eine Responder-Richtlinie ein, um den Map-Eintrag für die URL festzulegen, falls dieser noch nicht festgelegt ist. Bei der Erweiterung der Sofortmaßnahme wird der Karteneintragswert bei der Bewertung dieser Richtlinie festgelegt. Vor der Erweiterung wurde die Zuweisung erst durchgeführt, nachdem alle Responder-Richtlinien bewertet wurden. Die Entscheidung wird von einem separaten Webservice bereitgestellt.

   ```
   add responder policy url_list_assn_pol '!$url_list_map.VALUEEXISTS(HTTP
   .REQ.URL.PATH)'url_list_assn
   ```

7. Richten Sie eine Responder-Richtlinie ein, um den Zugriff auf eine URL zu blockieren, wenn ihr Map-Eintragswert BLOCK ist. Mit der Erweiterung der sofortigen Aktion steht der in der vorherigen Richtlinie festgelegte Karteneintrag für die Verwendung in dieser Richtlinie zur Verfügung. Vor der Erweiterung war der Karteneintrag zu diesem Zeitpunkt noch nicht gesetzt.

   ```
   add responder policy client_access_block_pol '$client_access_map[CLIENT
   .IP.SRC.TYPECAST_TEXT_T] == "BLOCK"'client_access_block_act
   ```

8. Binden Sie die Responder-Richtlinien an den virtuellen Server. **Hinweis**: Wir können die Richtlinien nicht global binden, da wir sie nicht für den HTTP-Callout auf einem separaten virtuellen Server ausführen möchten.

   ```
   bind lb vserver vs -policyName client_access_assn_pol -priority 10 -
   gotoPriorityExpression NEXT -type REQUEST
   bind lb vserver vs -policyName client_access_block_pol -priority 20 -
   gotoPriorityExpression END -type REQUEST
   ```

So konfigurieren Sie Variablen mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **AppExpert > NS-Variablen**, um eine Variable zu erstellen.
2. Navigieren Sie zu **AppExpert > NS Assignments**, um der Variablen Werte zuzuweisen.
3. Navigieren Sie zu dem entsprechenden Feature-Bereich, in dem Sie die Zuweisung als Aktion konfigurieren möchten.

Anwendungsfall: Benutzerberechtigungen zwischenspeichern

January 19, 2021

In diesem Anwendungsfall müssen Benutzerberechtigungen (GOLD, SILVER usw.) von einem externen Webdienst abgerufen werden.

Um diesen Anwendungsfall zu erreichen, führen Sie die folgenden Operationen aus

Erstellen Sie ein HTTP-Callout, um die Benutzerberechtigungen vom externen Webdienst abzurufen.

```
add policy httpcallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port <
    port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
    GET | POST )] [-hostExpr <string>] [-urlStemExpr <string>] [-headers
     <name(value)> ...] [-parameters <name(value)> ...] [-bodyExpr <
    string>][-fullReqExpr <string>] [-scheme ( http | https )] [-
    resultExpr <string>] [-cacheForSecs <secs>] [-comment <string>]

add policy httpcallout get_user_privilege -ipaddress 10.217.193.84 -
    port 80 -returnType text -httpMethod GET -hostExpr '"/
    get_user_privilege"' -resultExpr 'http.res.body(5)'
<!--NeedCopy-->
```

Speichern Sie die Berechtigungen in einer Variablen.

```
add ns variable <name> -type <string> [-scope ( global | transaction )
    ][-ifFull ( undef | lru )] [-ifValueTooBig ( undef | truncate )][-
    ifNoValue ( undef | init )] [-init <string>] [-expires <
    positive_integer>] [-comment <string>]

add ns variable user_privilege_map -type map(text(15),text(10),10000) -
    expires 1200

add ns assignment set_user_privilege -variable $user_privilege_map[
    client.ip.src] -set sys.http_callout(get_user_privilege)
<!--NeedCopy-->
```

Erstellen Sie eine Richtlinie, um zu überprüfen, ob bereits ein zwischengespeicherter Eintrag für die IP-Adresse des Clients vorhanden ist. Andernfalls wird das HTTP-Callout aufgerufen, um einen Zuordnungseintrag für den Client festzulegen.

```
add cmp policy <name> -rule <expression> -resAction <string>

```



```
add cmp policy set_user_privilege_pol -rule $user_privilege_map.
    valueExists(client.ip.src).not -resAction set_user_privilege>
<!--NeedCopy-->
```

Erstellen Sie eine Richtlinie, die komprimiert wird, wenn der zwischengespeicherte Berechtigungseintrag für den Client GOLD lautet.

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy compress_if_gold_privilege_pol -rule '
    $user_privilege_map[client.ip.src].eq("GOLD")' -resAction compress
<!--NeedCopy-->
```

Binden Sie die Komprimierungsrichtlinien global.

```
bind cmp global <policyName> [-priority <positive_integer>] [-state (
    ENABLED | DISABLED )] [-gotoPriorityExpression <expression>] [-type
    <type>] [-invoke (<labelType> <labelName>) ]

bind cmp global set_user_privilege_pol -priority 10 NEXT

bind cmp global compress_if_gold_privilege_pol -priority 20 END
<!--NeedCopy-->
```

Anwendungsfall: Begrenzung der Anzahl von Sitzungen

June 1, 2022

In diesem Anwendungsfall besteht die Anforderung darin, die Anzahl der aktiven Backend-Sitzungen zu begrenzen. In der Bereitstellung hat jede Sitzungsanmeldung eine Anmeldung in der URL und jede Sitzungsabmeldung hat eine Abmeldung in der URL. Bei erfolgreicher Anmeldung setzt das Backend ein Session-ID-Cookie mit einem eindeutigen 10-Zeichen-Wert.

Führen Sie die folgenden Schritte aus, um diesen Anwendungsfall zu erreichen:

1. Erstellen Sie eine Map-Variable, die jede aktive Sitzung speichern kann. Der Schlüssel der Map ist die Sessionid. Die Ablaufzeit für die Variable ist auf 600 Sekunden (10 Minuten) festgelegt.

   ```
   > add ns variable session_map -type map(text(10),ulong,100) -
       expires 600
   <!--NeedCopy-->
   ```


2. Erstellen Sie die folgenden Zuweisungen für die Map-Variable:

   - Erstellen Sie einen Eintrag für die Sitzungs-ID und setzen Sie diesen Wert auf 1 (dieser Wert wird nicht verwendet).

     ```
     > add ns assignment add_session -variable '$session_map[http.
        req.cookie.value("sessionid")]' -set 1
     <!--NeedCopy-->
     ```

   - Gibt den Eintrag für eine Sitzungs-ID frei, wodurch die Wertanzahl für session_map implizit verringert wird.

     ```
     > add ns assignment delete_session -variable '$session_map[
        http.req.cookie.value("sessionid")]' -clear
     <!--NeedCopy-->
     ```

3. Erstellen Sie Responder-Richtlinien für Folgendes:

   - Um zu überprüfen, ob ein Zuordnungseintrag für diese Sessionid in der HTTP-Anforderung existiert. Die Add_Session-Zuweisung wird ausgeführt, wenn der Zuordnungseintrag nicht existiert.

     ```
     > add responder policy add_session_pol 'http.req.url.contains
        ("example") || $session_map.valueExists(http.req.cookie.
        value("abc"))' add_session
     <!--NeedCopy-->
     ```

     Hinweis: Die Funktion
     valueExists () in der Richtlinie
     add_session_pol zählt als Referenz auf den Zuordnungseintrag der Sitzung, sodass jede Anforderung das Ablauf-Timeout für ihre Sitzung zurücksetzt. Wenn nach 10 Minuten keine Anfragen für eine Sitzung eingehen, wird der Eintrag der Sitzung freigegeben.

   - Um zu überprüfen, wann die Sitzung abgemeldet ist. Die delete_session -Zuweisung wird ausgeführt.

     ```
     add responder policy delete_session_pol "http.req.url.
        contains("Logout")" delete_session
     <!--NeedCopy-->
     ```

   - Um zu überprüfen, ob Anmeldeanfragen vorliegen und ob die Anzahl der aktiven Sitzungen 100 überschreitet. Wenn diese Bedingungen erfüllt sind, wird der Benutzer zur Begrenzung der Anzahl der Sitzungen auf eine Seite umgeleitet, die anzeigt, dass der Server ausgelastet ist.


```
add responder action redirect_too_busy redirect "/too_busy.
    html"
add responder policy check_login_pol "http.req.url.contains("
    example") && $session_map.valueCount > 100"
    redirect_too_busy
<!--NeedCopy-->
```

4. Binden Sie die Responder-Richtlinien global.

```
bind responder global add_session_pol 30 next
bind responder global delete_session_pol 10
bind responder global check_login_pol 20
<!--NeedCopy-->
```

Richtlinien und Ausdrücke

May 11, 2023

Die folgenden Themen enthalten die Konzept- und Referenzinformationen, die Sie für die Konfiguration erweiterter Richtlinien auf der Citrix® NetScaler® -Appliance benötigen.

Informationen über alle erweiterten Richtlinienausdrücke, die auf der NetScaler-Appliance unterstützt werden, finden Sie unter Richtlinienausdrücke

Einführung in Richtlinien und Ausdrücke	Beschreibt den Zweck von Ausdrücken, Richtlinien und Aktionen und wie verschiedene NetScaler-Anwendungen diese verwenden.
Konfigurieren erweiterter Richtlinien	Beschreibt die Struktur erweiterter Richtlinien und wie sie einzeln und als Policenbanken konfiguriert werden können.
Konfigurieren erweiterter Ausdrücke: Erste Schritte	Beschreibt Ausdruckssyntax und Semantik und stellt kurz vor, wie Ausdrücke und Richtlinien konfiguriert werden.
Erweiterte Ausdrücke: Text auswerten	Beschreibt Ausdrücke, die Sie konfigurieren, wenn Sie Text bearbeiten möchten (z. B. den Hauptteil einer HTTP-POST-Anforderung oder den Inhalt eines Benutzerzertifikats).
Erweiterte Ausdrücke: Arbeiten mit Daten, Zeiten und Zahlen	Beschreibt Ausdrücke, die Sie konfigurieren, wenn Sie mit irgendeiner Art von numerischen Daten arbeiten möchten (z. B. die Länge einer URL, die IP-Adresse eines Clients oder das Datum und die Uhrzeit, an dem eine HTTP-Anforderung gesendet wurde).
Erweiterte Ausdrücke: Parsen von HTTP-, TCP- und UDP-Daten	Beschreibt Ausdrücke zum Parsen

von IP- und IPv6-Adressen, MAC-Adressen und Daten, die für HTTP- und TCP-Verkehr spezifisch sind. |
| Erweiterte Ausdrücke: Parsen von SSL-Zertifikaten | Beschreibt, wie Ausdrücke für SSL-Verkehr und Clientzertifikate konfiguriert werden, z. B. wie das Ablaufdatum eines Zertifikats oder des Zertifikatsausstellers abgerufen wird.|
| Erweiterte Ausdrücke: IP- und MAC-Adressen, Durchsatz, VLAN-IDs | Beschreibt Ausdrücke, die Sie verwenden können, um mit anderen client- oder serverbezogenen Daten zu arbeiten, die in anderen Kapiteln nicht behandelt werden. |Typecasting Data | Beschreibt Ausdrücke für die Transformation von Daten eines Typs in einen anderen. |Reguläre Ausdrücke| Beschreibt, wie reguläre Ausdrücke als Argumente an Operatoren in fortgeschrittenen Ausdrücken übergeben werden. |
Ausdrucks-Referenz | Eine Referenz für erweiterte Ausdrucksargumente. | Zusammenfassende Beispiele für erweiterte Ausdrücke und Richtlinien | Beispiele für erweiterte Ausdrücke und Richtlinien, sowohl als Kurzreferenz als auch als Tutorial, die Sie für Ihren eigenen Gebrauch anpassen können. |
Tutorial Beispiele für erweiterte Richtlinien für Rewrite	Beispiele für erweiterte Richtlinien zur Verwendung in der Rewrite-Funktion.
Tutorial	Richtlinienbeispiele	Beispiele für Richtlinien für NetScaler-Funktionen wie Anwendungsfirewall und SSL.
Migration von Apache mod_rewrite Rules to Advanced Policies	Beispiele für Funktionen, die mit der mod_rewrite-Engine des Apache HTTP Servers geschrieben wurden, mit Beispielen für diese Funktionen nach der Übersetzung in Rewrite- und Responder-Richtlinien auf dem NetScaler.

Einführung in Richtlinien und Ausdrücke

May 11, 2023

Für viele NetScaler-Funktionen steuern Richtlinien, wie eine Funktion Daten auswertet. Eine Richtlinie verwendet einen logischen Ausdruck, der als Regel bezeichnet wird, um Daten auszuwerten, und wendet eine oder mehrere Aktionen basierend auf der Auswertung an. Alternativ kann eine Richtlinie ein Profil anwenden, das eine komplexe Aktion definiert.

Einige NetScaler-Funktionen verwenden erweiterte Richtlinien, die größere Funktionen als ältere klassische Richtlinien bieten. Wenn Sie auf eine neuere Version der NetScaler-Software migriert und klassische Richtlinien für Funktionen konfiguriert haben, die erweiterte Richtlinien verwenden, müssen Sie Richtlinien manuell auf eine erweiterte Richtlinieninfrastruktur migrieren.

Erweiterte Infrastruktur für Richtlinien

July 11, 2023

> **Warnung**
>
> Klassische Richtlinienausdrücke sind ab NetScaler 12.0 Build 56.20 veraltet. Alternativ empfiehlt Citrix die Verwendung von erweiterten Richtlinien. Weitere Informationen finden Sie unter Erweiterte Richtlinien

Die erweiterte Richtlinieninfrastruktur ermöglicht es Ihnen, viele Daten zu analysieren (z. B. den Text einer HTTP-Anforderung) und viele Operationen in der Richtlinienregel zu konfigurieren (z. B. die Umwandlung von Daten im Hauptteil einer Anforderung in einen HTTP-Header). Sie müssen die Richtlinie an einen bestimmten Punkt in der Verarbeitung binden, der den NetScaler-Funktionen zugeordnet ist. Der Bindepunkt ist ein Faktor, der bestimmt, wann die Richtlinie bewertet wird.

Vorteile der Verwendung erweiterter Richtlinien

Erweiterte Richtlinien verwenden eine leistungsstarke Ausdruckssprache, die auf einem Klassenobjektmodell basiert, und sie bieten mehrere Optionen, mit denen Sie das Verhalten verschiedener NetScaler-Funktionen konfigurieren können. Mit einer erweiterten Richtlinieninfrastruktur können Sie Folgendes tun:

- Führen Sie feinkörnige Analysen des Netzwerkverkehrs aus den Layern 2 bis 7 durch.
- Bewerten Sie einen beliebigen Teil des Headers oder des Hauptteils einer HTTP- oder HTTPS-Anforderung oder -Antwort.
- Binden Sie Richtlinien an die mehreren Bindepunkte, die die erweiterte Richtlinieninfrastruktur auf Standard-, Override- und virtueller Serverebene unterstützt.
- Verwenden Sie spezielle Tools wie Mustersätze, Policy-Labels, Ratenlimit-IDs, HTTP-Callouts und Variablen, mit denen Sie Richtlinien effektiv für komplexe Anwendungsfälle konfigurieren können.

Außerdem erweitert das Konfigurationsprogramm die robuste GUI-Unterstützung für erweiterte Richtlinieninfrastrukturen und Ausdrücke und ermöglicht Benutzern mit begrenzten Kenntnissen von Netzwerkprotokollen, Richtlinien schnell und einfach zu konfigurieren. Das Konfigurationsprogramm enthält auch eine Funktion zur Richtlinienbewertung für erweiterte Richtlinien. Sie können diese Funktion verwenden, um eine erweiterte Richtlinie zu evaluieren und ihr Verhalten zu testen, bevor Sie sie festlegen, wodurch das Risiko von Konfigurationsfehlern reduziert wird.

Grundkomponenten einer erweiterten Richtlinie

Im Folgenden sind einige Merkmale einer erweiterten Richtlinie aufgeführt:

- Name. Jede Richtlinie hat einen eindeutigen Namen.
- Regel. Die Regel ist ein logischer Ausdruck, mit dem die NetScaler-Funktion einen Datenverkehr oder ein anderes Objekt auswerten kann. Beispielsweise kann eine Regel dem NetScaler er-

möglichen, zu bestimmen, ob eine HTTP-Anforderung von einer bestimmten IP-Adresse stammt oder ob ein Cache-Control-Header in einer HTTP-Anforderung den Wert “Kein Cache” hat.

- Bindungen. Um sicherzustellen, dass der NetScaler bei Bedarf eine Richtlinie aufrufen kann, verknüpfen Sie die Richtlinie oder binden sie mit einem oder mehreren Verbindungspunkten.

  Sie können eine Richtlinie global oder an einen virtuellen Server binden. Weitere Informationen finden Sie unter Informationen zu Richtlinienbindungen.

- Eine zugeordnete Aktion. Eine Aktion ist eine von einer Richtlinie getrennte Einheit. Die Richtlinienbewertung führt letztendlich dazu, dass der NetScaler eine Aktion ausführt.

  Beispielsweise kann eine Richtlinie im integrierten Cache HTTP-Anfragen für GIF- oder JPEG-Dateien identifizieren. Eine Aktion, die Sie dieser Richtlinie zuordnen, bestimmt, dass die Antworten auf diese Arten von Anfragen aus dem Cache bedient werden.

Für einige Funktionen konfigurieren Sie Aktionen als Teil eines komplexeren Befehls, der als Profil bezeichnet wird.

Wie verschiedene NetScaler-Funktionen Richtlinien verwenden

Der NetScaler unterstützt verschiedene Funktionen, die auf Betriebsrichtlinien beruhen. In der folgenden Tabelle wird zusammengefasst, wie die NetScaler-Funktionen Richtlinien verwenden.

Featurename	So verwenden Sie Richtlinien in der Funktion
Rewrite	Um die Daten zu identifizieren, die Sie vor der Bereitstellung ändern möchten. Die Richtlinien enthalten Regeln zum Ändern der Daten. Sie können beispielsweise HTTP-Daten ändern, um eine Anforderung basierend auf der Adresse der eingehenden Anforderung an eine neue Homepage oder einen neuen Server oder einen ausgewählten Server umzuleiten, oder Sie können die Daten ändern, um Serverinformationen in einer Antwort aus Sicherheitsgründen zu maskieren. Die Funktion URL Transformer identifiziert URLs in HTTP-Transaktionen und Textdateien, um zu bewerten, ob eine URL transformiert werden muss.

Featurename	So verwenden Sie Richtlinien in der Funktion
Responder	Um das Verhalten der Responder-Funktion zu konfigurieren. Eine Responder Policy basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Regel ist mit einer Aktion verknüpft, die ausgeführt wird, wenn eine Anforderung der Regel entspricht.
Content Switching	Um anhand der Merkmale einer eingehenden Anforderung zu ermitteln, welcher Server oder welche Servergruppe für die Bearbeitung von Antworten verantwortlich ist. Anforderungsmerkmale umfassen Gerätetyp, Sprache, Cookies, HTTP-Methode, Inhaltstyp und zugehörige Cacheserver.
Cacheumleitung	Um festzustellen, ob Antworten von einem Cache oder von einem Ursprungsserver aus bedient werden.
Steuerung der Kompression	Um zu bestimmen, welche Art von Verkehr komprimiert werden muss.
DNS	Um verschiedene Teile von DNS-Anfragen und Antworten zu ändern
Clientloser VPN-Zugriff	Um zu bestimmen, wie das NetScaler Gateway Authentifizierung, Autorisierung, Überwachung und andere Funktionen durchführt, und definieren Rewriteregeln für den allgemeinen Webzugriff mit dem NetScaler Gateway.
Zwischenspeichern	Um zu bestimmen, ob eine Antwort vom Cache oder vom Originalserver bereitgestellt werden soll.
Richtlinie zur URL-Transformation	Um die Anfragen und Antworten auszuwählen, die der NetScaler mithilfe des URL-Transformationsprofils transformieren muss.
Anwendungsfirewallrichtlinie	Um verschiedenen Arten von Webinhalten unterschiedliche Filterregeln zuzuweisen.

Featurename	So verwenden Sie Richtlinien in der Funktion
Autorisierung	Um Zugriff auf die angeforderten Inhalte zu ermöglichen, ohne unnötige Details über die tatsächliche Konfiguration der Website preiszugeben.
TM-Verkehr	Um die Eigenschaften (wie Verbindungstimeout, Single Sign-On und Initiierung der Abmeldung) des Anwendungsdatenverkehrs zur Laufzeit festzulegen.
TM-Sitzung	Um Benutzersitzungen anzupassen, nachdem sich der Benutzer am virtuellen Autorisierungs-, Autorisierungs- und Kontoführungsserver angemeldet hat.
SSL-Richtlinien	Um ein Steuerelement oder eine Datenaktion zu definieren, die auf Anfragen ausgeführt werden soll. SSL-Richtlinien können daher als Kontrollrichtlinien und Datenrichtlinien kategorisiert werden. Eine Steuerungsrichtlinie verwendet eine Steuerungsaktion, z. B. das Erzwingen der Clientauthentifizierung. Eine Datenrichtlinie verwendet eine Datenaktion, z. B. das Einfügen einiger Daten in die Anforderung.
Autoscale	Um die Anzahl der virtuellen Server gemäß den definierten Bedingungen nahtlos und automatisch nach oben oder unten zu skalieren.
AppFlow	Damit NetScaler Flussdaten in Erfassungstools exportieren kann, die häufig für Netzwerk- oder Sicherheitsanalysen verwendet werden.

Featurename	So verwenden Sie Richtlinien in der Funktion
Optimierung von Inhalten	Um die Transaktionszeiten zwischen den Clients und den Servern zu reduzieren und den Bandbreitenverbrauch zu reduzieren. Auch um die Serverleistung zu verbessern, indem einige Aufgaben ausgelagert und andere effizienter gestaltet werden.
Überlauf	Um eine NetScaler-Regel zu verwenden, um die Bedingungen für das Auftreten von Spillover anzugeben. Die Regeln geben Ihnen die Flexibilität, den Spillover für verschiedene Betriebsbedingungen zu konfigurieren.
ICA	Um eine ICAP-Anfrage dynamisch zu generieren, empfangen Sie die ICAP-Antwort und protokollieren Sie die Inhaltsprüfungsdaten.
VPN-Sitzung	Auf einem NetScaler Gateway, um Endpoint Analysis (EPA) so zu konfigurieren, dass überprüft wird, ob ein Benutzergerät bestimmte Sicherheitsanforderungen erfüllt, und dem Benutzer entsprechend Zugriff auf interne Ressourcen gewährt wird.
VPN-Verkehr	Auf einem NetScaler Gateway, um Endpoint Analysis (EPA) so zu konfigurieren, dass überprüft wird, ob ein Benutzergerät bestimmte Sicherheitsanforderungen erfüllt, und dem Benutzer entsprechend Zugriff auf interne Ressourcen gewährt wird.
Syslog	Um zu definieren, welche Meldungen auf dem angegebenen Syslog-Server protokolliert werden sollen.
nslog	Um zu definieren, welche Nachrichten auf dem angegebenen nslog-Server protokolliert werden sollen.

Featurename	So verwenden Sie Richtlinien in der Funktion
Erkennung der Videooptimierung	Um eine benutzerdefinierte Bezeichnung für die Erkennungsrichtlinie zur Videooptimierung zu erstellen, an die Sie Erkennungsrichtlinien binden können. Ein Policy-Label ist ein Tool zur Bewertung einer Reihe von Richtlinien in einer bestimmten Reihenfolge. Mithilfe einer Richtlinienbezeichnung können Sie die Videooptimierungsfunktion so konfigurieren, dass sie die nächste Richtlinie auswählt, eine andere Richtlinienbezeichnung aufruft oder eine Richtlinienbewertung vollständig beendet, indem Sie überprüfen, ob die vorherige Richtlinie als WAHR oder FALSCH bewertet wurde.
Tunneling	Um die Art der Komprimierung zu definieren, die für den getunnelten Verkehr verwendet werden soll.
Prüfung der Inhalte	Um Anforderungen anzugeben, die der NetScaler ADC abfängt und die angegebene Aktion ausführt.
VPN-URL	Um einen Lesezeichen-Link zu einer externen oder internen Ressource zu erstellen, der auf dem Access Interface je nach Typ als Website-Link oder Dateifreigabelink angezeigt wird.

Featurename	So verwenden Sie Richtlinien in der Funktion
Bot	Um ein benutzerdefiniertes Bot-Richtlinienlabel zu erstellen, an das Sie Richtlinien binden können. Ein Policy-Label ist ein Tool zur Bewertung einer Reihe von Richtlinien in einer bestimmten Reihenfolge. Mithilfe einer Richtlinienbezeichnung können Sie die Responder-Funktion so konfigurieren, dass sie die nächste Richtlinie auswählt, eine andere Richtlinienbezeichnung aufruft oder eine Richtlinienbewertung vollständig beendet, indem Sie überprüfen, ob die vorherige Richtlinie als WAHR oder FALSCH bewertet wurde.
Richtlinie für VPN-Intranet-Anwendungen	Um Intranetanwendungen zu definieren, auf die über ein NetScaler Gateway zugegriffen werden soll.
SmartAccess	Um ein ICA-Zugriffsprofil zu erstellen, das den Status der Funktionen angibt (Standard oder Deaktiviert).
Lastausgleich	Um zu definieren, wie die Clientverbindungen auf die von ihm verwalteten Server mit Lastenausgleich verteilt werden.

Über Aktionen und Profile

Richtlinien selbst ergreifen keine Maßnahmen in Bezug auf Daten. Richtlinien bieten schreibgeschützte Logik für die Auswertung des Datenverkehrs. Damit eine Funktion einen Vorgang basierend auf einer Richtlinienbewertung ausführen kann, konfigurieren Sie Aktionen oder Profile und verknüpfen sie mit Richtlinien.

> **Hinweis:**
>
> Aktionen und Profile sind spezifisch für bestimmte Funktionen. Informationen zum Zuweisen von Aktionen und Profilen zu Funktionen finden Sie in der Dokumentation für die einzelnen Funktionen.

Über Aktionen

Aktionen sind Schritte, die der NetScaler abhängig von der Auswertung des Ausdrucks in der Richtlinie durchführt. Wenn beispielsweise ein Ausdruck in einer Richtlinie mit einer bestimmten Quell-IP-Adresse in einer Anforderung übereinstimmt, bestimmt die Aktion, die dieser Richtlinie zugeordnet ist, ob die Verbindung zulässig ist.

Die Arten von Aktionen, die der NetScaler ausführen kann, sind funktionsspezifisch. In Rewrite können Aktionen beispielsweise Text in einer Anforderung ersetzen, die Ziel-URL für eine Anforderung ändern usw. Im integrierten Caching bestimmen Aktionen, ob HTTP-Antworten aus dem Cache oder einem Ursprungsserver bereitgestellt werden.

In einigen NetScaler-Funktionen sind Aktionen vordefiniert, in anderen sind sie konfigurierbar. In einigen Fällen (z. B. Rewrite) konfigurieren Sie die Aktionen mithilfe derselben Ausdruckstypen, die Sie für die Konfiguration der zugehörigen Richtlinienregel verwenden.

> **Hinweis:**
>
> Nicht alle Kombinationen aus Feature, Protokoll, Richtung und Entität sind gültig.

Übersicht über Profile

Mit einigen NetScaler-Funktionen können Sie Profile oder sowohl Aktionen als auch Profile einer Richtlinie zuordnen. Ein Profil ist eine Sammlung von Einstellungen, die es der Funktion ermöglichen, eine komplexe Funktion auszuführen. In der Anwendungsfirewall kann ein Profil für XML-Daten beispielsweise mehrere Überprüfungsvorgänge ausführen, z. B. die Untersuchung der Daten auf illegale XML-Syntax oder Hinweise auf eine SQL-Einschleusung.

Informationen zu Richtlinienbindungen

Eine Richtlinie ist einer Entität zugeordnet oder an eine Entität gebunden, die das Aufrufen der Richtlinie ermöglicht. Beispielsweise können Sie eine Richtlinie an die Auswertung der Anforderungszeit binden, die für alle virtuellen Server gilt. Eine Sammlung von Richtlinien, die an einen bestimmten Bindepunkt gebunden sind, bildet eine Richtlinienbank.

Im Folgenden finden Sie eine Übersicht über die verschiedenen Arten von Bindepunkten für eine Richtlinie:

- Globale Uhrzeit anfordern. Eine Richtlinie kann für alle Komponenten in einer Funktion zur Anforderungszeit verfügbar sein.
- Reaktionszeit global. Eine Richtlinie kann für alle Komponenten in einer Funktion zur Reaktionszeit verfügbar sein.
- Anforderungszeit, spezifisch für virtuelle Server. Eine Richtlinie kann an die Anforderungszeitverarbeitung für einen bestimmten virtuellen Server gebunden sein. Sie können beispielsweise

eine Richtlinie für die Anforderungszeit an einen virtuellen Cache-Umleitungsserver binden, um sicherzustellen, dass bestimmte Anforderungen an einen virtuellen Lastausgleichsserver für den Cache weitergeleitet werden und andere Anforderungen an einen virtuellen Lastausgleichsserver für den Ursprung gesendet werden.

- Reaktionszeit, spezifisch für virtuelle Server. Eine Richtlinie kann auch an die Reaktionszeitverarbeitung für einen bestimmten virtuellen Server gebunden sein.
- Benutzerdefinierte Richtlinienbezeichnung. Für eine erweiterte Richtlinieninfrastruktur können Sie benutzerdefinierte Gruppierungen von Richtlinien (Richtlinienbanken) konfigurieren, indem Sie ein Policy-Label definieren und eine Reihe verwandter Richtlinien unter dem Policy-Label sammeln.
- Andere Bindungspunkte. Die Verfügbarkeit zusätzlicher Bindepunkte hängt von der Art der erweiterten Richtlinie und den Besonderheiten der jeweiligen NetScaler-Funktion ab.

Weitere Informationen zu erweiterten Richtlinienbindungen finden Sie unter Bindungsrichtlinien, die das Thema “Erweiterte Richtlinien” verwenden .

Informationen zur Evaluierungsreihenfolge von Richtlinien

Die Funktionen im NetScaler werden in einer bestimmten Reihenfolge verarbeitet, was die Auswertung der Richtlinien für die Funktion und die Ausführung der ausgewählten Aktionen umfasst. Weitere Informationen finden Sie unter Paketfluss.

Zu jedem Zeitpunkt der Nachrichtenverarbeitung wird die Richtlinienbewertung in Abhängigkeit von der folgenden Kombination durchgeführt:

- Protokoll (z. B. HTTP, SIP, TCP oder Diameter)
- Richtung (Anfrage oder Antwort)
- Funktion (wie Rewrite, Responder oder Bot)

Die Kombinationen können nicht verwechselt werden. Richtlinien werden in Gruppen von Richtlinien, die als Banken bezeichnet werden (auch Policy Label oder Bind Points genannt), in der folgenden Reihenfolge bewertet:

1. Globale Außerkraftsetzung
2. Spezifischer virtueller LB-Server verwendet
3. Wenn ein bestimmter virtueller CS-Server verwendet wird
4. Globaler Standard

Innerhalb einer Bank werden die Richtlinien von der niedrigsten bis zur höchsten Priorität bewertet. Wenn eine Richtlinienregel als falsch bewertet wird, geht die Bewertung automatisch zur nächsthöheren nummerierten Priorität in derselben Bank über. Wenn es in derselben Bank keine Richtlinienregeln gibt, wird die erste Richtlinie der nächsten Bank in der Reihenfolge bewertet. Wenn es keine Richtlinien mehr gibt, endet die Richtlinienbewertung. Wenn eine Richtlinienregel als wahr

bewertet wird, wird die entsprechende Aktion oder das entsprechende Profil für eine mögliche spätere Ausführung gespeichert.

Wenn die Richtlinie als wahr bewertet wird, wird der Wert “gotoPriorityExpression” überprüft. Wenn “gotoPriorityExpression” auf “END” gesetzt ist, wird die Richtlinienbewertung beendet. Bei “NEXT” wird die nächste Richtlinie (wie oben beschrieben) ausgewertet. Wenn es sich um einen Ausdruck handelt, wird dieser Ausdruck ausgewertet und als Nächstes die Richtlinie mit dieser Priorität ausgewählt.

> **Hinweis**
>
> Die Standardeinstellung für “gotoPriorityExpression” ist “END”. Für einige Funktionen, die alle Aktionen ausführen können, wird jedoch empfohlen, den Wert “gotoPriorityExpression” explizit anzugeben.

Sobald die Richtlinienbewertung beendet ist, führt die Funktion die geordnete Liste der Aktionen oder Profile aus. Die Funktionen führen entweder alle Aktionen aus (z. B. Rewrite) oder eine Aktion (z. B. Responder oder Bot). Wenn einer Funktion, die nur eine Aktion oder ein Profil ausführen kann, mehr als eine Aktion oder ein Profil zugeordnet sind, wird standardmäßig die letzte ausgeführt. Wenn keine Aktionen oder Profile ausgewählt sind, führt die Funktion ihre Standardaktion aus.

Reihenfolge der Bewertung basierend auf dem Verkehrsfluss

Einige Richtlinien wirken sich auf das Ergebnis anderer Richtlinien aus. Es folgen Beispiele:

- Wenn eine Antwort aus dem integrierten Cache bereitgestellt wird, verarbeiten einige andere NetScaler-Funktionen die Antwort oder die Anforderung, die sie initiiert hat, nicht.
- Wenn die Anwendungsfirewall eine eingehende Anforderung ablehnt, können sie von anderen Features nicht verarbeitet werden.
- Die meisten Aktionen, die vom Responder ausgeführt werden, beenden die weitere Verarbeitung.
- Die von Rewrite ausgeführten Aktionen “Löschen” und “Zurücksetzen” beenden die weitere Verarbeitung.

Erweiterte Richtlinienausdrücke

May 11, 2023

Eine der grundlegendsten Komponenten einer Richtlinie ist ihre Regel. Eine Richtlinienregel ist ein logischer Ausdruck, der es der Richtlinie ermöglicht, den Datenverkehr zu analysieren. Der größte Teil der Funktionalität der Richtlinie leitet sich von ihrem Ausdruck ab.

Ein Ausdruck stimmt Merkmale von Verkehr oder anderen Daten mit einem oder mehreren Parametern und Werten überein. Ein Ausdruck kann beispielsweise NetScaler ermöglichen, Folgendes zu erreichen:

- Bestimmen Sie, ob eine Anforderung ein Zertifikat enthält.
- Bestimmen Sie die IP-Adresse eines Clients, der eine TCP-Anfrage gesendet hat.
- Identifizieren Sie die Daten, die eine HTTP-Anforderung enthält (z. B. eine beliebte Tabellenkalkulation oder Textverarbeitungsanwendung).
- Berechnen Sie die Länge einer HTTP-Anforderung.

Informationen zu erweiterten Richtlinienausdrücken

Jede Funktion, die eine erweiterte Richtlinieninfrastruktur verwendet, verwendet auch erweiterte Ausdrücke. Informationen darüber, welche Funktionen erweiterte Richtlinien verwenden, finden Sie in der Tabelle NetScaler Feature, Richtlinientyp und Richtlinienverwendung.

Erweiterte Richtlinienausdrücke haben einige andere Verwendungszwecke. Zusätzlich zum Konfigurieren von erweiterten Ausdrücken in Richtlinienregeln konfigurieren Sie erweiterte Ausdrücke in den folgenden Situationen:

- Integriertes Caching:

  Sie verwenden erweiterte Richtlinienausdrücke, um einen Selektor für eine Content-Gruppe im integrierten Cache zu konfigurieren.

- Lastenausgleich:

  Sie verwenden erweiterte Richtlinienausdrücke, um die Token-Extraktion für einen virtuellen Lastausgleichsserver zu konfigurieren, der die TOKEN-Methode für den Lastausgleich verwendet.

- Schreiben Sie um:

  Sie verwenden erweiterte Richtlinienausdrücke, um Rewrite-Aktionen zu konfigurieren.

- Tarifbasierte Richtlinien:

  Sie verwenden erweiterte Richtlinienausdrücke, um Limit-Selektoren zu konfigurieren, wenn Sie eine Richtlinie konfigurieren, um die Geschwindigkeit des Datenverkehrs zu verschiedenen Servern zu steuern.

Nachfolgend einige einfache Beispiele für erweiterte Richtlinienausdrücke:

- Eine HTTP-Anforderungs-URL enthält nicht mehr als 500 Zeichen.

```
http.req.url.length \<= 500
```

- Eine HTTP-Anforderung enthält ein Cookie mit weniger als 500 Zeichen.


```
http.req.cookie.length \< 500
```

- Eine HTTP-Anforderungs-URL enthält eine bestimmte Textzeichenfolge.

```
http.req.url.contains(".html")
```

Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool

August 15, 2023

> **Hinweis:**
>
> Sie können das NSPEPI- und Preconfig-Check-Tool vom öffentlichen GitHub herunterladen. Weitere Informationen finden Sie auf der GitHub NEPEPI-Seite und auf der README-Seite für ausführliche Anweisungen zum Herunterladen, Installieren und Verwenden der Tools. Wir empfehlen Kunden, die in GitHub verfügbaren Tools für die vollständigste und aktuellste Version zu verwenden.

Klassische richtlinienbasierte Features und Funktionen sind ab NetScaler 12.0 Build 56.20 veraltet. Als Alternative empfiehlt Citrix die Verwendung der erweiterten Richtlinieninfrastruktur. Im Rahmen dieser Bemühungen müssen Sie beim Upgrade auf NetScaler 12.1 Build 56.20 oder höher die richtlinienbasierten Funktionen und Funktionen von Classic durch die entsprechenden nicht veralteten Funktionen und Funktionen ersetzen. Außerdem müssen Sie klassische Richtlinien und Ausdrücke in erweiterte Richtlinien und Ausdrücke konvertieren. Außerdem unterstützen alle neuen NetScaler-Funktionen nur erweiterte Richtlinieninfrastruktur.

Das Tool `nspepi` kann Folgendes ausführen:

1. Konvertieren Sie klassische Richtlinienausdrücke in erweiterte Richtlinienausdrücke.
2. Konvertieren Sie bestimmte Classic-Richtlinien und deren Entitätsbindungen in erweiterte Richtlinien und Bindungen.
3. Konvertieren Sie ein paar weitere veraltete Funktionen in ihre entsprechenden nicht veralteten Funktionen.
4. Konvertieren Sie klassische Filterbefehle in erweiterte Filterbefehle.

> **Hinweis:**
>
> Nachdem das Tool `nspepi` die ns.conf-Konfigurationsdatei erfolgreich konvertiert hat, zeigt das Tool die konvertierte Datei als neue Datei mit dem Präfix “new_” an. Wenn die konvertierte Konfigurationsdatei Fehler oder Warnungen enthält, müssen Sie diese im Rahmen des Konvertierungsprozesses manuell beheben. Nach der Konvertierung müssen Sie die Datei in der Testumgebung testen und dann verwenden, um die eigentliche ns.conf-Konfigurationsdatei zu ersetzen. Nach dem Testen müssen Sie die Appliance für die neu konvertierte oder feste

> ns.conf-Konfigurationsdatei neu starten.

Funktionen, die nur klassische Richtlinien oder Ausdrücke unterstützen, sind veraltet und können durch die entsprechenden nicht veralteten Funktionen ersetzt werden.

> **Hinweis:**
>
> Informationen zur älteren Version des Tools `nspepi` sind in einem PDF-Format verfügbar. Weitere Informationen finden Sie unter Klassische Richtlinienkonvertierung mithilfe des nspepi-Tool vor 12.1-51.16 PDF.

Konvertierungswarnungen und Fehlerdateien

Bevor Sie das Tool für Ihre Konvertierung verwenden, sollten Sie nur wenige Warnungen beachten:

1. Alle Warnungen und Fehler werden an die Konsole ausgegeben. Es wird eine Warndatei erstellt, in der die Konfigurationsdateien gespeichert werden.
2. Die Warnungs- und Fehlerdatei hat den gleichen Namen wie die Eingabedatei, jedoch mit dem Präfix “warn_”, das dem Dateinamen hinzugefügt wurde. Während der Ausdrucksumwandlung (bei Verwendung von -e) werden die Warnungen im aktuellen Verzeichnis mit dem Namen “warn_expr” angezeigt.

> **Hinweis:**
>
> Diese Datei hat ein Standard-Protokolldateiformat mit Datums-/Zeitstempel und Protokollebene. Frühere Instanzen der Datei werden mit Suffixen wie “.1”, “.2” usw. beibehalten, da das Tool mehrmals ausgeführt wird. Es werden höchstens 10 Instanzen beibehalten.

Konvertiertes Dateiformat

Beim Konvertieren einer Konfigurationsdatei (mit “-f”) wird die konvertierte Datei in dasselbe Verzeichnis abgelegt, in dem die Eingabekonfigurationsdatei mit demselben Namen, aber einem Präfix “neu_” existiert.

Befehle oder Funktionen, die vom nspepi-Konvertierungstool verarbeitet werden

Im Folgenden werden die Befehle aufgeführt, die während des automatischen Konvertierungsprozesses verarbeitet werden.

- Die folgenden Classic-Richtlinien und ihre Ausdrücke werden in erweiterte Richtlinien und Ausdrücke umgewandelt. Die Konvertierung umfasst Entitätsbindungen und globale Bindungen.

1. add appfw policy
2. add cmp policy
3. add cr policy

4. add cs policy
5. add tm sessionPolicy
6. add filter action
7. add filter policy
8. Filterrichtlinienbindung an Lastenausgleich, Content Switching, Cache-Umleitung und global.

> **Hinweis:**
>
> Für "add tm sessionPolicy" können Sie jedoch nicht an globale Überschreibungen in erweiterten Richtlinien binden.

- Der in "add lb virtual server" konfigurierte Regelparameter wird vom klassischen Ausdruck in den erweiterten Ausdruck konvertiert.
- Der im Befehl "add ns httpProfile" oder "set ns httpProfile" konfigurierte SPDY-Parameter wird in "-http2 ENABLED" geändert.
- Benannte Ausdrücke (Befehle "Richtlinienausdruck hinzufügen"). Jeder klassische benannte Richtlinienausdruck wird in den entsprechenden benannten erweiterten Ausdruck umgewandelt, wobei "nspepi_adv_" als Präfix festgelegt ist. Darüber hinaus wird die Verwendung benannter Ausdrücke für die konvertierten Classic-Ausdrücke in die entsprechenden erweiterten benannten Ausdrücke geändert. Darüber hinaus hat jeder benannte Ausdruck zwei benannte Ausdrücke, wobei einer Classic und der andere Advanced ist (wie unten gezeigt).
- Tunnel TrafficPolicy Konvertierung wird unterstützt.
- Umgang mit integrierten klassischen Richtlinienbindungen in CMP, CR und Tunnel.
- Patclass Feature wird in Pat Set Feature umgewandelt.
- Der Parameter "-pattern" im Befehl "add rewrite action" wird umgewandelt, um den Parameter "-search" zu verwenden.
- Q- und S-Präfixe von erweiterten Ausdrücken werden in äquivalente, nicht veraltete erweiterte Ausdrücke umgewandelt. Diese Ausdrücke sind in jedem Befehl zu sehen, in dem erweiterte Ausdrücke zulässig sind.

Zum Beispiel:

```
add policy expression classic_expr ns_true
Converts to:
add policy expression classic_expr ns_true
add policy expression nspepi_adv_classic_expr TRUE
<!--NeedCopy-->
```

- Der im Befehl "set cmp parameter" konfigurierte policyType-Parameter wird entfernt. Standardmäßig ist der Richtlinientyp "Advanced".

Konvertieren klassischer Filterbefehle in erweiterte Filterbefehle

Das Tool `nspepi` kann Befehle basierend auf klassischen Filteraktionen wie Hinzufügen, Binden usw. in erweiterte Filterbefehle konvertieren.

Das nepepi-Tool unterstützt jedoch die folgenden Filterbefehle nicht.

1. add filter action <`action Name`> FORWARD <`service name`>
2. add filter action <`action name`> ADD prebody
3. add filter action <`action name`> ADD postbody

> **Hinweis:**
>
> 1. Wenn es in ns.conf Rewrite- oder Responder-Features gibt und ihre Richtlinien global mit dem Ausdruck `GOTO` als `END` oder `USER_INVOCATION_RESULT`gebunden sind und der Bindetyp ist `REQ_X` oder `RES_X` dann konvertiert das Tool Bindungsfilterbefehle teilweise und kommentiert. Bei der manuellen Konvertierung wird ein Fehler angezeigt.
> 2. Wenn es vorhandene Rewrite- oder Responder-Funktionen gibt und deren Richtlinien an virtuelle Server (z. B. Load Balancing, Content Switching oder Cache-Umleitung) vom Typ HTTPS mit `GOTO - END` oder `USER_INVOCATION_RESULT` gebunden sind , konvertiert das Tool Bindungsfilterbefehle teilweise und kommentiert dann Kommentare aus. Für die manuelle Konvertierung wird eine Warnung angezeigt.

Beispiel

Es folgt eine Beispieleingabe:

```
add lb vserver v1 http 1.1.1.1 80 -persistenceType NONE -cltTimeout
    9000
add cs vserver csv1 HTTP 1.1.1.2 80 -cltTimeout 180 -persistenceType
    NONE
add cr vserver crv1 HTTP 1.1.1.3 80 -cacheType FORWARD
add service svc1 1.1.1.4 http 80
add filter action fact_add add 'header:value'
add filter action fact_variable add 'H1:%%HTTP.TRANSID%%'
add filter action fact_prebody add prebody
add filter action fact_error_act1 ERRORCODE 200 "<HTML>Good URL</HTML>"
add filter action fact_forward_act1 FORWARD svc1
add filter policy fpol_add_res -rule ns_true -resAction fact_add
add filter policy fpol_error_res -rule ns_true -resAction
    fact_error_act1
add filter policy fpol_error_req -rule ns_true -reqAction
    fact_error_act1
add filter policy fpol_add_req -rule ns_true -reqAction fact_add
```



```
add filter policy fpol_variable_req -rule ns_true -reqAction
    fact_variable
add filter policy fpol_variable_res -rule ns_true -resAction
    fact_variable
add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
bind lb vserver v1 -policyName fpol_add_res
bind lb vserver v1 -policyName fpol_add_req
bind lb vserver v1 -policyName fpol_error_res
bind lb vserver v1 -policyName fpol_error_req
bind lb vserver v1 -policyName fpol_variable_res
bind lb vserver v1 -policyName fpol_variable_req
bind lb vserver v1 -policyName fpol_forward_req
bind cs vserver csv1 -policyName fpol_add_req
bind cs vserver csv1 -policyName fpol_add_res
bind cs vserver csv1 -policyName fpol_error_res
bind cs vserver csv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_add_req
bind cr vserver crv1 -policyName fpol_add_res
bind cr vserver crv1 -policyName fpol_error_res
bind cr vserver crv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_forward_req
bind filter global fpol_add_req
bind filter global fpol_add_res
bind filter global fpol_error_req
bind filter global fpol_error_res
bind filter global fpol_variable_req
bind filter global fpol_variable_res
bind filter global fpol_variable_res -state DISABLED
bind filter global fpol_prebody_req
bind filter global fpol_forward_req
After conversion, warning/error messages will be displayed for manual
    effort.
Warning files:
cat warn_<input file name>:
2019-11-07 17:13:34,724: ERROR - Conversion of [add filter action
    fact_prebody add prebody] not supported in this tool.
2019-11-07 17:13:34,739: ERROR - Conversion of [add filter action
    fact_forward_act1 FORWARD svc1] not supported in this tool.
2019-11-07 17:13:38,042: ERROR - Conversion of [add filter policy
    fpol_prebody_req -rule ns_true -reqAction fact_prebody] not
```



```
    supported in this tool.
50  2019-11-07 17:13:38,497: ERROR - Conversion of [add filter policy
    fpol_prebody_res -rule ns_true -resAction fact_prebody] not
    supported in this tool.
51  2019-11-07 17:13:39,035: ERROR - Conversion of [add filter policy
    fpol_forward_req -rule ns_true -reqAction fact_forward_act1] not
    supported in this tool.
52  2019-11-07 17:13:39,060: WARNING - Following bind command is commented
    out because state is disabled. Advanced expressions only have a
    fixed ordering of the types of bindings without interleaving, except
     that global bindings are allowed before all other bindings and
    after all bindings. If you have global bindings in the middle of non
    -global bindings or any other interleaving then you will need to
    reorder all your bindings for that feature and direction. Refer to
    nspepi documentation. If command is required please take a backup
    because comments will not be saved in ns.conf after triggering 'save
     ns config': bind filter global fpol_variable_res -state DISABLED
53
54
55  <!--NeedCopy-->
```

Es folgt eine Beispielausgabe. Alle konvertierten Befehle werden kommentiert.

```
1  cat new_<input file name>
2  add rewrite action fact_add insert_http_header header ""value""
3  add filter action fact_prebody add prebody
4  add filter action fact_forward_act1 FORWARD svc1
5  add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
6  add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
7  add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
8  bind lb vserver v1 -policyName fpol_forward_req
9  bind cr vserver crv1 -policyName fpol_forward_req
10 #bind filter global fpol_variable_res -state DISABLED
11 bind filter global fpol_prebody_req
12 bind filter global fpol_forward_req
13 add rewrite action nspepi_adv_fact_variable insert_http_header H1 HTTP.
    RES.TXID
14 add rewrite action fact_variable insert_http_header H1 HTTP.REQ.TXID
15 add responder action fact_error_act1 respondwith "HTTP.REQ.VERSION.
    APPEND(" 200 OK\r
16 nConnection: close\r
17 nContent-Length: 21\r\n\r
```



```
n<HTML>Good URL</HTML>")"
add rewrite action nspepi_adv_fact_error_act1 replace_http_res "HTTP.REQ.VERSION.APPEND(" 200 OK\r
nConnection: close\r
nContent-Length: 21\r\n\r
n<HTML>Good URL</HTML>")"
add rewrite policy fpol_add_res TRUE fact_add
add rewrite policy fpol_error_res TRUE nspepi_adv_fact_error_act1
add responder policy fpol_error_req TRUE fact_error_act1
add rewrite policy fpol_add_req TRUE fact_add
add rewrite policy fpol_variable_req TRUE fact_variable
add rewrite policy fpol_variable_res TRUE nspepi_adv_fact_variable
set cmp parameter -policyType ADVANCED
bind rewrite global fpol_add_req 100 NEXT -type REQ_DEFAULT
bind rewrite global fpol_variable_req 200 NEXT -type REQ_DEFAULT
bind rewrite global fpol_add_res 100 NEXT -type RES_DEFAULT
bind rewrite global fpol_error_res 200 NEXT -type RES_DEFAULT
bind rewrite global fpol_variable_res 300 NEXT -type RES_DEFAULT
bind responder global fpol_error_req 100 END -type REQ_DEFAULT
bind lb vserver v1 -policyName fpol_add_res -type RESPONSE -priority 100 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_res -type RESPONSE -priority 200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_variable_res -type RESPONSE -priority 300 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_add_req -type REQUEST -priority 100 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_variable_req -type REQUEST -priority 200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_req -type REQUEST -priority 100 -gotoPriorityExpression END
bind cs vserver csv1 -policyName fpol_add_req -type REQUEST -priority 100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_add_res -type RESPONSE -priority 100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_res -type RESPONSE -priority 200 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_req -type REQUEST -priority 100 -gotoPriorityExpression END
bind cr vserver crv1 -policyName fpol_add_req -type REQUEST -priority 100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_add_res -type RESPONSE -priority 100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_error_res -type RESPONSE -priority 200 -gotoPriorityExpression NEXT
```



```
49 bind cr vserver crv1 -policyName fpol_error_req -type REQUEST -priority
       100 -gotoPriorityExpression END
50
51 <!--NeedCopy-->
```

Konvertieren Sie klassische Filterbefehle in erweiterte Feature-Befehle, wenn vorhandene Rewrite- oder Responder-Richtlinienbindungen den goto Ausdruck END oder USE_INNVOCATION haben

Wenn bei dieser Konvertierung eine Rewriterichtlinie an einen oder mehrere virtuelle Server gebunden ist und der Server über END oder USE_INVOCATION_RESULT verfügt, kommentiert das Tool die Befehle.

Beispiel

Es folgt ein Beispiel für einen Eingabebefehl:

```
1  COPY
2  add filter policy fpol1 -rule ns_true -resAction reset
3  add filter policy fpol2 -rule ns_true -reqAction reset
4  add rewrite policy pol1 true NOREWRITE
5  add rewrite policylabel pl http_res
6  bind rewrite policylabel pl pol1 1
7  bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
       -invoke policylabel pl
8  add responder policy pol2 true NOOP
9  add responder policylabel pl -policylabeltype HTTP
10 bind responder policylabel pl pol2 1
11 bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
       REQ_DEFAULT -invoke policylabel pl
12 bind lb vserver v1_tcp -policyName pol1 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
13 bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
14 bind lb vserver v1_tcp -policyName pol2 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
15 bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
16 bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
       gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
17 bind lb vserver v1_http -policyName fpol1
18 bind cs vserver csv1_http -policyName fpol1
19 bind lb vserver v2_http -policyName fpol2
```



```
bind cs vserver csv2_http -policyName fpol2
bind cr vserver crv2_http -policyName fpol2
bind filter global fpol1 -priority 100
bind filter global fpol2 -priority 100
<!--NeedCopy-->
```

Es folgt ein Beispiel für einen Ausgabebefehl:

```
COPY
add rewrite policy pol1 true NOREWRITE
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
add responder policy pol2 true NOOP
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
add rewrite policy fpol1 TRUE RESET
add responder policy fpol2 TRUE RESET
#bind lb vserver v1_http -policyName fpol1 -type RESPONSE
#bind cs vserver csv1_http -policyName fpol1 -type RESPONSE
#bind rewrite global fpol1 100 -type RES_DEFAULT
#bind lb vserver v2_http -policyName fpol2 -type REQUEST
#bind cs vserver csv2_http -policyName fpol2 -type REQUEST
#bind cr vserver crv2_http -policyName fpol2 -type REQUEST
#bind responder global fpol2 100 -type REQ_DEFAULT
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
   -invoke policylabel pl
bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
   REQ_DEFAULT -invoke policylabel pl
bind lb vserver v1_tcp -policyName pol1 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind lb vserver v1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST-

<!--NeedCopy-->
```


Befehle oder Funktionen, die nicht vom nspepi-Konvertierungstool verarbeitet werden

Im Folgenden sind einige Befehle aufgeführt, die im Rahmen des automatischen Konvertierungsprozesses nicht behandelt werden.

- Einige Bindungen können nicht konvertiert werden, wenn es ein gewisses Überlappen von Prioritäten zwischen globalen und nicht-globalen Bindungspunkten, zwischen Benutzern und Gruppen sowie zwischen Bindungen an verschiedene Entitäten gibt. Bei diesen wurde die betroffene Konfiguration auskommentiert und ein Fehler erzeugt. Solche Konfigurationen müssen manuell umgewandelt werden.
- Sowohl klassische als auch erweiterte Richtlinien können an cmp global gebunden werden. Es gibt viele Fälle, in denen sich die Funktionalität ändert, sobald Classic-Richtlinien in erweiterte Richtlinien umgewandelt wurden. Wir haben Befehle umgewandelt, die durch das Auskommentieren einiger Richtlinien gelöst werden können. Dennoch gibt es einige Befehle, die nicht konvertiert werden können. In solchen Fällen wird ein Fehler erzeugt und die Konvertierung muss manuell erfolgen.
- Nicht alle Verwendungen von in Classic integrierten benannten Ausdrücken werden in äquivalente erweiterte benannte Ausdrücke umgewandelt.
- Client-Sicherheitsausdrücke werden nicht behandelt.
- Sicher verbinden (SC)
- Prioritäts-Warteschlange (PQ)
- HTTP-Denial-of-Service-Angriff (HDOS)
- HTML-Einschleusung
- Authentifizierung
- Autorisierung
- VPN
- Syslog
- Nslog
- Dateibasierte Classic-Ausdrücke werden nicht behandelt.

> **Hinweis:**
>
> Für einige Funktionen wie Patclass/filter wird die Befehlssyntax geändert. Wenn es cmd-Richtlinien gibt, müssen die cmd-Richtlinien möglicherweise je nach Kundenanforderung geändert werden.

Bekannte Probleme

Die folgenden Szenarien führen zu Fehlern im `nspepi` Tool

- Wenn bei der Konvertierung eines Ausdrucks ein Problem auftritt

- Wenn ein benannter Richtlinienausdruck den Parameter -ClientSecurityMessage verwendet, weil dieser Parameter im erweiterten Richtlinienausdruck nicht unterstützt wird
- Beim Lastenausgleich handelt es sich bei einem virtuellen Serverregelausdruck um einen komplexen Ausdruck mit mehreren INHALTSbasierten Ausdrücken.
- Fehler bei der Konvertierung der CMP-Funktionen
  - Wenn sowohl klassische als auch fortschrittliche Richtlinien an globale Richtlinien gebunden sind.
  - Wenn klassische Richtlinien gebunden sind und der cmp-Parameter erweitert ist.
  - Wenn erweiterte Richtlinien gebunden sind und der cmp-Parameter klassisch ist.
  - Wenn klassische Richtlinien an einen virtuellen Server und erweiterte Richtlinien an einen globalen Server gebunden sind.
  - Wenn erweiterte Richtlinien an einen virtuellen Server und klassische Richtlinien an einen globalen Server gebunden sind.
  - Wenn klassische Richtlinien an einen virtuellen Server gebunden sind und sowohl klassische als auch erweiterte Richtlinien an einen globalen Server gebunden sind.
  - Wenn erweiterte Richtlinien an einen virtuellen Server gebunden sind und sowohl klassische als auch erweiterte Richtlinien an einen globalen Server gebunden sind.
- Wenn der klassisch benannte Ausdruck denselben Namen wie der Callout-Entitätsname hat
- Wenn der Name des klassischen Ausdrucks für den erweiterten Ausdruck ungültig ist
- Wenn die konvertierte Ausdruckslänge mehr als 1499 Zeichen beträgt
- Wenn der klassische Ausdruck Client-Sicherheitsausdrücke oder dateibasierte Ausdrücke enthält

Warnung

Die folgenden Szenarien zeigen die Warnungen im `nspepi` Tool

- Wenn der Regelausdruck des virtuellen Lastausgleichsservers ein boolescher Ausdruck ist, führt der entsprechende erweiterte Ausdruck zu einem booleschen Wert im Zeichenkettenformat. Dies führt zu einer Änderung der Funktionalität, wenn die Regel für `persistenceType` oder `lbMethod` verwendet wird. Um die Änderung der Funktionalität zu vermeiden, wird der Befehl geändert, indem das `keywords rule` und entfernt wird `persistenceType`.
- Wenn das Statusfeld des Bindungsbefehls DISABLED ist. Wenn der Status deaktiviert ist, wird der Befehl nicht verwendet. Der State-Parameter wird in der erweiterten Konfiguration nicht unterstützt. Wenn wir diese Konfiguration also konvertieren, ändert sich die Funktionalität. Wenn der Befehl erforderlich ist, erstellen Sie bitte eine Backup, da Kommentare nach dem Auslösen von `save ns config` nicht in `ns.conf` gespeichert werden.

Warnung bei der Konvertierung von CMP-Funktionen:

- Wenn ein globaler CMP-Parameter-Richtlinientyp auf CLASSIC gesetzt ist und erweiterte Richtlinien an global gebunden sind. Ohne Konvertierung werden begrenzte erweiterte

Richtlinien nicht bewertet, da der globale Richtlinientyp auf CLASSIC festgelegt ist. Nach der Konvertierung würde der Richtlinientyp in ADVANCED umgewandelt. Wenn wir also die vorhandenen globalen erweiterten Bindungen nicht kommentieren, werden diese Bindungen ausgewertet und können die Funktionalität ändern.

- Wenn der globale CMP-Parameter für den Richtlinientyp auf ADVANCED gesetzt ist und klassische Richtlinien an globale Richtlinien gebunden sind. Ohne Konvertierung würden diese globalen klassischen Bindungen nicht ausgewertet, da der globale Richtlinientyp ADVANCED ist. Um die Funktionalität zu erhalten, kommentieren wir also die konvertierte Konfiguration. Andernfalls werden konvertierte erweiterte Richtlinien bewertet und können die Funktionalität ändern.

> **Hinweis:**
>
> Alle klassischen Richtlinienbindungen mit deaktivierter Option -state werden auskommentiert. Die Option -state ist für erweiterte Richtlinienbindungen nicht verfügbar.

Ausführen des nspepi-Tools

Das Folgende ist ein Befehlszeilenbeispiel zum Ausführen des Tools `nspepi`. Dieses Tool wird von der Befehlszeile der Shell aus ausgeführt (Sie müssen den Befehl "Shell" an den NetScaler "CLI" eingeben, um dorthin zu gelangen). Entweder "-f" oder "-e" muss angegeben werden, um eine Konvertierung durchzuführen. Die Verwendung von "-d" ist für Citrix Mitarbeiter vorgesehen, um sie zu Supportzwecken zu analysieren.

```
usage: nspepi [-h] (-e <classic policy expression> | -f <path to ns
    config file>)[-d] [-v] [-V

Convert classic policy expressions to advanced policy expressions and
    deprecated commands to non-deprecated
commands.

optional arguments:
-h, --help show this help message and exit
-e <classic policy expression>, --expression <classic policy expression
    >
convert classic policy expression to advanced policy
expression (maximum length of 8191 allowed)
-f <path to ns config file>, --infile <path to ns config file>
convert netscaler config file
-d, --debug log debug output
-v, --verbose show verbose output
-V, --version show program's version number and exit
<!--NeedCopy-->
```


Beispiele für die Verwendung:

1. `nspepi -e "req.tcp.destport == 80"`
2. `nspepi -f /var/nsconfig/ns.conf`

Im Folgenden finden Sie einige Beispiele für das Ausführen des Tools `nspepi` über die CLI

Beispielausgabe für den Parameter —e:

```
root@ns# nspepi -e "req.http.header foo == "bar""
"HTTP.REQ.HEADER("foo").EQ("bar")"
<!--NeedCopy-->
```

Beispielausgabe für den Parameter -f:

```
root@ns# cat sample.conf
add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
   originUSIP OFF
add cr policy cr_pol1 -rule ns_true
bind cr vserver cr_vs -policyName cr_pol1
<!--NeedCopy-->
```

Ausführen von nspepi mit dem Parameter -f:

```
nspepi -f sample.conf
<!--NeedCopy-->
```

Die konvertierte Konfiguration ist in einer neuen Datei verfügbar `new_sample.conf`.
Überprüfen Sie die Datei `warn_sample.conf` auf Warnungen oder Fehler, die möglicherweise generiert wurden.

Beispielausgabe des Parameters -f zusammen mit dem Parameter -v

```
nspepi -f sample.conf -v
INFO - add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180
    -originUSIP OFF
INFO - add cr policy cr_pol1 -rule TRUE -action ORIGIN
INFO - bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
   gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Die konvertierte Konfiguration ist in einer neuen Datei verfügbar `new_sample.conf`.
Überprüfen Sie die Datei `warn_sample.conf` auf Warnungen oder Fehler, die möglicherweise generiert wurden.

Konvertierte Config-Datei:


```
root@ns# cat new_sample.conf
add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
    originUSIP OFF
add cr policy cr_pol1 -rule TRUE -action ORIGIN
set cmp parameter -policyType ADVANCED
bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
    gotoPriorityExpression END -type REQUEST

<!--NeedCopy-->
```

Beispielausgabe einer Beispielkonfiguration ohne Fehler oder Warnungen:

```
nspepi -f sample_2.conf
<!--NeedCopy-->
```

Die konvertierte Konfiguration ist in einer neuen Datei verfügbar `new_sample_2.conf`.
Überprüfen Sie die Datei `warn_sample_2.conf` auf Warnungen oder Fehler, die möglicherweise generiert wurden.

Beispielausgabe einer Beispielkonfiguration mit Warnungen:

```
root@ns# cat sample_2.conf
add policy expression security_expr "req.tcp.destport == 80" -
    clientSecurityMessage "Not allowed"
set cmp parameter -policyType CLASSIC
add cmp policy cmp_pol1 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol2 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
bind cmp global cmp_pol1
bind cmp global cmp_pol2 -state DISABLED
bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
    RES_DEFAULT
bind lb vserver lb_vs -policyName cmp_pol2
root@ns#
<!--NeedCopy-->
```

Beispiel für das Ausführen von nspepi mit dem Parameter -f:

```
root@ns# nspepi -f sample_2.conf
ERROR - Error in converting expression security_expr : conversion of
    clientSecurityMessage based expression is not supported.
WARNING - Following bind command is commented out because state is
    disabled. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
```



```
      have global bindings in the middle of non-global bindings or any
     other interleaving then you will need to reorder all your bindings
     for that feature and direction. Refer to nspepi documentation. If
     command is required please take a backup because comments will not
     be saved in ns.conf after triggering 'save ns config': bind cmp
     global cmp_pol2 -state DISABLED
4 Warning - Bindings of advanced CMP policies to cmp global are commented
      out, because initial global cmp parameter is classic but advanced
     policies are bound. Now global cmp parameter policy type is set to
     advanced. If commands are required please take a backup because
     comments will not be saved in ns.conf after triggering 'save ns
     config'. Advanced expressions only have a fixed ordering of the
     types of bindings without interleaving, except that global bindings
     are allowed before all other bindings and after all bindings. If you
      have global bindings in the middle of non-global bindings or any
     other interleaving then you will need to reorder all your bindings
     for that feature and direction. Refer to nspepi documentation.
5 root@ns#
6 <!--NeedCopy-->
```

Konvertierte Datei:

```
1  root@ns# cat new_sample_2.conf
2  add policy expression security_expr "req.tcp.destport == 80" -
      clientSecurityMessage "Not allowed"
3  set cmp parameter -policyType ADVANCED
4  add cmp policy cmp_pol1 -rule TRUE -resAction COMPRESS
5  add cmp policy cmp_pol2 -rule TRUE -resAction COMPRESS
6  add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
7  #bind cmp global cmp_pol2 -state DISABLED
8  #bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
       RES_DEFAULT
9  bind cmp global cmp_pol1 -priority 100 -gotoPriorityExpression END -
      type RES_DEFAULT
10 bind lb vserver lb_vs -policyName cmp_pol2 -priority 100 -
      gotoPriorityExpression END -type RESPONSE
11 root@ns#
12 <!--NeedCopy-->
```

Warn-Datei:

```
1  root@ns# cat warn_sample_2.conf
2  2019-02-28 06:20:10,590: ERROR - Error in converting expression
      security_expr : conversion of clientSecurityMessage based expression
       is not supported.
```



```
3 2019-02-28 06:20:12,187: WARNING - Following bind command is commented
     out because state is disabled. Advanced expressions only have a
     fixed ordering of the types of bindings without interleaving, except
      that global bindings are allowed before all other bindings and
     after all bindings. If you have global bindings in the middle of non
     -global bindings or any other interleaving then you will need to
     reorder all your bindings for that feature and direction. Refer to
     nspepi documentation. If command is required please take a backup
     because comments will not be saved in ns.conf after triggering 'save
      ns config': bind cmp global cmp_pol2 -state DISABLED
4 2019-02-28 06:20:12,191: WARNING - Bindings of advanced CMP policies to
      cmp global are commented out, because initial global cmp parameter
     is classic but advanced policies are bound. Now global cmp parameter
      policy type is set to advanced. If commands are required please
     take a backup because comments will not be saved in ns.conf after
     triggering 'save ns config'. Advanced expressions only have a fixed
     ordering of the types of bindings without interleaving, except that
     global bindings are allowed before all other bindings and after all
     bindings. If you have global bindings in the middle of non-global
     bindings or any other interleaving then you will need to reorder all
      your bindings for that feature and direction. Refer to nspepi
     documentation.
5 root@ns#
6 <!--NeedCopy-->
```

Verbindliche Prioritäten

Erweiterte Richtlinien erlauben kein willkürliches Interleaving nach Priorität zwischen global und nicht-global sowie zwischen verschiedenen Bindungstypen. Wenn Sie sich auf ein solches Interleaving von Classic-Richtlinienprioritäten verlassen, müssen Sie die Prioritäten anpassen, um den erweiterten Richtlinienregeln zu entsprechen und das gewünschte Verhalten zu erzielen.
Prioritäten in erweiterten Richtlinien sind lokal an einem Bindepunkt. Ein Bindepunkt ist eine eindeutige Kombination aus Protokoll, Feature, Richtung und Entität (Entitäten sind bestimmte virtuelle Server, Benutzer, Gruppen, Dienste und entweder globale Überschreibung oder globale Standardeinstellung). Politische Prioritäten werden nicht über Bindepunkte hinweg befolgt.

Für ein bestimmtes Protokoll, eine bestimmte Funktion und Richtung ist die Reihenfolge der Bewertung der erweiterten Richtlinien wie folgt:

- Globale Überschreibung.
- (Aktueller) Authentifizierungs-, Autorisierungs- und Überwachungsbenutzer.
- Authentifizierungs-, Autorisierungs- und Überwachungsgruppen (bei denen der Benutzer Mitglied ist) in der Reihenfolge des Gewichts - die Reihenfolge ist nicht definiert, wenn zwei oder

mehr Gruppen das gleiche Gewicht haben.
- Virtueller LB-Server, auf dem entweder die Anforderung empfangen wurde oder der Content Switching ausgewählt hat.
- Virtueller Content Switching-Server, virtueller Cache-Umleitungsserver, auf dem die Anforderung empfangen wurde.
- Durch Load Balancing ausgewählter Dienst.
- Globale Standardeinstellung.

Für die Bewertung der Autorisierungsrichtlinie lautet die Reihenfolge:

- Systeme überschreiben.
- Virtueller Lastausgleichsserver, auf dem entweder die Anforderung empfangen wurde oder der CS ausgewählt hat.
- Virtueller Content Switching-Server, auf dem die Anforderung empfangen wurde.
- Standardeinstellung des Systems.

Innerhalb jedes Bindepunkts werden die Richtlinien in der Reihenfolge ihrer Priorität von der niedrigsten bis zur höchsten Nummerierung ausgewertet. Richtlinien werden nur für das verwendete Protokoll und die Richtung ausgewertet, von der die Nachricht empfangen wurde.

Klassische Richtlinienbindungen, die eine manuelle Neupriorisierung erfordern

Hier sind einige Arten von Classic-Richtlinienbindungen, die eine manuelle Neupriorisierung erfordern, um Ihre Anforderungen zu erfüllen. All dies ist für ein bestimmtes Merkmal und die Richtung.

- Klassische Prioritäten, die die Prioritätszahl gegenüber der Richtung der oben genannten Entitätstyplisten erhöhen. Zum Beispiel ist eine Bindung eines virtuellen Content Switching-Servers niedriger als eine Bindung eines virtuellen Lastausgleichsservers.
- Klassische Prioritäten, die mit Authentifizierungs-, Autorisierungs- und Überwachungsgruppen überlappen. Ein Teil einer Gruppe steht vor einer anderen Gruppe und ein weiterer Teil ist hinter einem Teil dieser anderen Gruppe her.
- Klassische Prioritäten, deren Anzahl außer der Reihenfolge der Gewichtungen von Authentifizierungs-, Autorisierungs- und Überwachungsgruppen zunimmt.
- Klassische globale Prioritäten, die weniger als einige nicht-globale Priorität und dieselben globalen Prioritäten sind größer als einige andere nicht-globale Priorität (d. h. jedes Segment von Prioritäten, das eine nicht-globale Priorität ist, gefolgt von einem oder mehreren Globals, gefolgt von einem nicht-globalen).

Die Tools `NSPEPI` und `check_invalid_config` können auf den Systemen `CentOS` und `Ubuntu` ausgeführt werden

Die folgenden Module sind die Voraussetzungen für die Verwendung dieser Tools:

- Python
- Perl
- Python-Pip-Modul
- PLY-Modul für Python
- Switch.pm für Perl

Wenn Python 3 installiert ist, erstellen Sie beispielsweise einen Softlink `"ln -s /usr/bin/python3 /usr/bin/python"`.

Führen Sie die folgenden Befehle aus, um das Python-Pip-Modul, das PLY-Modul für Python und Switch.pm für Perl in CentOS zu installieren:

- `sudo yum install -y perl-Switch`
- `sudo yum install python-pip`
- `sudo yum install python-ply`

Führen Sie die folgenden Befehle aus, um das Python-Pip-Modul, das PLY-Modul für Python und Switch.pm für Perl in Ubuntu zu installieren:

- `sudo apt install libswitch-perl`
- `sudo apt install python-ply`
- `sudo apt install python-pip or sudo apt install python3-pip`

Tool zur Überprüfung der Vorkonfiguration

June 2, 2023

> **Hinweis:**
>
> Sie können das NSPEPI- und das Preconfig-Check-Tool vom öffentlichen GitHub herunterladen. Weitere Informationen finden Sie auf GitHub NEPEPI Seite und GitHub Preconfig Seite für detaillierte Anweisungen zum Herunterladen der Tools. Wir empfehlen Kunden, die in GitHub verfügbaren Tools für die vollständigste und aktuellste Version zu verwenden.

In den Versionen NetScaler 12.1, 13.0 und 13.1 ist ein Vorvalidierungstool verfügbar, mit dem überprüft werden kann, ob in einer Feature-Konfiguration noch ungültige oder entfernte Funktionen verwendet werden. Die Tools validieren die Datei `nsconfig`, wenn sie Befehle oder Parameter in einem Befehl enthält, der in der NetScaler 13.1 Version entfernt wurde. Wenn das Validierungsergebnis die Verwendung entfernter oder ungültiger Befehle anzeigt, müssen Sie vor dem Upgrade Ihrer Appliance zuerst die Konfiguration auf die von Citrix empfohlene Alternative ändern.

Das Tool validiert auch die Verwendung von klassischen Richtlinienausdrücken, die in der Featurekonfiguration verwendet werden, die Classic-Richtlinien nicht unterstützen. Sie können entweder manuell ändern oder das Tool `nspepi` verwenden.

Das Tool validiert die folgende Verwendung:

1. Klassische Richtlinienausdrücke in den Funktionen Content Switching, Cache-Umleitung, AppFW, SSL und CMP.
2. Filterfunktion (auch Content-Filter genannt) - Aktionen, Richtlinien und Bindung
3. SPDY im HTTP-Profil, sichere Verbindung (SC), Priority Queuing (PQ), HTTP Denial of Service (DoS) und HTML Injection Funktionen.
4. Klassische Ausdrücke in Persistenzregeln für den Lastausgleich.
5. Parameter “Pattern” und “bypassSafetyCheck” in Rewrite-Aktionen.
6. “patclass” -Konfigurationseinheit.
7. “HTTP.REQ.BODY” ohne Argument in erweiterten Ausdrücken.
8. Q- und S-Präfixe in erweiterten Ausdrücken.
9. Parameter “PolicyType” für die cmp-Parametereinstellung.

Führen Sie das Tool vor der erneuten Überprüfung in UNIX Shell aus

Geben Sie in der Befehlszeile Folgendes ein:

```
check_invalid_config <config_file>
<!--NeedCopy-->
```

Beispiel:

```
root@ns## check_invalid_config/nsconfig/ns.conf
```

Wo ist die Konfigurationsdatei die NetScaler-Konfigurationsdatei. Die Datei muss aus einer gespeicherten Konfiguration wie `ns.conf` sein.

Beispielausgabe mit Validierungsfehlern

Es folgt eine Beispielausgabe der Konfigurationsdatei mit Fehlern in NetScaler Version 13.1:

```
add cmp policy cmp_pol -rule ns_true -resAction GZIP
add cs policy cs_pol_2 -rule ns_true
add cs policy cs_pol_3 -domain www.abc.com
add cs policy cs_pol_4 -url "/abc"
add rewrite action act_1 replace_all "http.req.body(1000)" http.req.url
    -pattern abcd
add rewrite action act_123 replace_all http.req.url ""aaaa"" -pattern
   abcd
add responder action ract respondwith "Q.URL + Q.HEADER("abcd")"
add appfw policy aff_pol_1 "http.req.body.length.gt(10)" APPFW_BYPASS
add appfw policy aff_pol ns_true APPFW_BYPASS

```



```
<!--NeedCopy-->
```

Wenn Sie diese Fehler erhalten haben, können Sie das Upgradetool `nspepi` verwenden, um Ihre Konfiguration zu konvertieren oder Ihre Konfiguration manuell zu konvertieren. Weitere Informationen finden Sie im Thema nspepi tool .

> **Hinweis:**
>
> Sie können das Tool `nspepi` nur auf NetScaler Version 12.1, 13.0 und höher ausführen.

Beispielausgabe ohne Validierungsfehler

Es folgt eine Beispielausgabe der Konfigurationsdatei ohne entfernte oder ungültige Konfiguration:

```
root@ns# check_invalid_config /var/tmp/new_ns.conf
No issue detected with the configuration.
root@ns#
<!--NeedCopy-->
```

Häufig gestellte Fragen zu auslaufenden klassischen Richtlinien

September 1, 2023

- **Welche klassischen Richtlinien sind ab NetScaler ab Version 12.0 veraltet?**

  Alle Funktionen und Funktionen, die in der Tabelle " Veraltete Richtlinien " erwähnt werden, sind von NetScaler Release 12.0 Build 56.20 veraltet. In den folgenden Tabellen (im PDF-Format) finden Sie Informationen zu veralteten Funktionen und Richtlinien.

  - Tabelle 1 für veraltete Richtlinien und ihre Alternative.
  - Tabelle 2 für veraltete NetScaler-Funktionalitäten und ihre Alternative mit Konfigurationsdetails.

- **Wie kann ich klassische richtlinienbasierte Funktionen und Funktionen in Advanced Policy konvertieren?**

  Sie können das proprietäre Tool `nspepi` von NetScaler verwenden, um Befehle, Ausdrücke und Konfigurationen zu konvertieren. Das Tool `nspepi` hilft dabei, alle klassischen Ausdrücke in der NetScaler-Konfiguration in die erweiterten Richtlinienausdrücke zu konvertieren. Weitere Informationen zum Tool `nspepi` finden Sie unter Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool.

- **Aus welcher Version sind klassische richtlinienbasierte Funktionen und Funktionalitäten veraltet?**

NetScaler 12.0 Build 56.20 und höher.

- **Aus welcher Version werden die veralteten klassischen richtlinienbasierten Funktionen und Funktionen von der NetScaler-Appliance entfernt?**

  NetScaler ab Version 13.1. Weitere Informationen finden Sie in der Tabelle Veraltete Richtlinien .

- **Welche Schritte müssen ausgeführt werden, wenn ich meine Appliance auf einen Build aktualisiere, der die klassischen richtlinienbasierten Funktionen nicht unterstützt?**

  Ab NetScaler Version 13.1 werden klassische richtlinienbasierte Funktionen nicht unterstützt. Bevor Sie auf NetScaler 13.1 oder höhere Versionen aktualisieren, empfehlen wir Ihnen, das `nspepi` Tool auszuführen, um die Datei zu konvertieren. `ns.conf` Informationen zum `nspepi` Tool finden Sie unter Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool.

- **Wie lange werden die veralteten Funktionen auf einer NetScaler-Appliance unterstützt?**

  NetScaler unterstützt die klassische Richtlinie und ihre Verwendung in Versionen nach NetScaler Version 13.0 nicht.

  Klassische Richtlinien und Ausdrücke sind ab 12.0 Build 56.20 veraltet (von der Verwendung abgehalten und NICHT entfernt). Die Richtlinien und Ausdrücke funktionieren an allen Stellen auf die gleiche Weise, wie sie in allen Builds von Release 13.0 funktioniert haben. Ab Version NetScaler 13.1 wurden jedoch bestimmte auf Classic-Richtlinien basierende Merkmale und Funktionalitäten entfernt.

- **Muss ich meine Appliance neu starten, nachdem ich die Konfigurationsdatei konvertiert habe?**

  Ja, Sie müssen die NetScaler-Instanz nach erfolgreicher Konvertierung der Datei `ns.config` neu starten.

Bevor Sie fortfahren

May 11, 2023

Stellen Sie vor dem Konfigurieren von Ausdrücken und Richtlinien sicher, dass Sie die relevante NetScaler-Funktion und die Struktur Ihrer Daten wie folgt verstehen:

- Lesen Sie die Dokumentation zu der entsprechenden Funktion.
- Sehen Sie sich den Datenstrom nach dem Datentyp an, den Sie konfigurieren möchten.

Möglicherweise möchten Sie eine Verfolgung der Art des Datenverkehrs oder Inhalts durchführen, den Sie konfigurieren möchten. Auf diese Weise erhalten Sie eine Vorstellung von den Parametern und

Werten sowie den Operationen für diese Parameter und Werte, die Sie in einem Ausdruck angeben müssen.

Hinweis: Der NetScaler unterstützt erweiterte Richtlinien innerhalb einer Funktion. Sie können nicht beide Typen in derselben Funktion haben. In den letzten Versionen wurden einige NetScaler-Funktionen von der Verwendung von Richtlinien und Ausdrücken zu erweiterten Richtlinien und Ausdrücken migriert. Wenn eine für Sie interessante Funktion in das erweiterte Richtlinienformat geändert wurde, müssen Sie möglicherweise die älteren Informationen manuell migrieren. Im Folgenden finden Sie Richtlinien für die Entscheidung, ob Sie Ihre Richtlinien migrieren müssen:

- Wenn Sie klassische Richtlinien in einer Version der Integrated Caching-Funktion vor Version 9.0 konfiguriert und dann auf Version 9.0 oder höher aktualisieren, hat dies keine Auswirkungen. Alle Legacy-Richtlinien werden in das erweiterte Richtlinienformat migriert.
- Bei anderen Features müssen Sie klassische Richtlinien und Ausdrücke manuell in die erweiterte Syntax migrieren, wenn das Feature zur erweiterten Richtlinie migriert wurde.

Konfiguration einer fortschrittlichen Richtlinieninfrastruktur

May 11, 2023

Sie können erweiterte Richtlinien für verschiedene NetScaler-Funktionen erstellen, darunter DNS, Rewrite, Responder und Integrated Caching sowie die Funktion für den clientlosen Zugriff im NetScaler Gateway. Richtlinien steuern das Verhalten dieser Funktionen.

Wenn Sie eine Richtlinie erstellen, weisen Sie ihr einen Namen, eine Regel (einen Ausdruck), funktionsspezifische Attribute und eine Aktion zu, die ausgeführt wird, wenn Daten mit der Richtlinie übereinstimmen. Nachdem Sie die Richtlinie erstellt haben, bestimmen Sie, wann sie aufgerufen wird, indem Sie sie global oder entweder an die Anforderungs- oder Antwortzeitverarbeitung für einen virtuellen Server binden.

Policen, die denselben Verbindungspunkt haben, werden als *Policy-Bank*bezeichnet. Beispielsweise bilden alle Richtlinien, die an einen virtuellen Server gebunden sind, die Richtlinienbank für den virtuellen Server. Wenn Sie die Richtlinie verbindlich festlegen, weisen Sie ihr eine Prioritätsstufe zu, um festzulegen, wann sie im Vergleich zu anderen Richtlinien in der Bank in Anspruch genommen wird. Zusätzlich zur Zuweisung einer Prioritätsstufe können Sie eine beliebige Bewertungsreihenfolge für Richtlinien in einer Bank konfigurieren, indem Sie Goto-Ausdrücke angeben.

Zusätzlich zu den Richtlinienbanken, die einem integrierten Bindpunkt oder einem virtuellen Server zugeordnet sind, können Sie *Richtlinienlabels*konfigurieren. Ein Policy-Label ist eine Policy-Bank, die durch einen beliebigen Namen gekennzeichnet ist. Sie rufen ein Policy-Label und die darin enthaltenen Richtlinien aus einer globalen oder für virtuelle Server spezifischen Policy-Bank auf. Ein Policy-Label oder eine Policy-Bank für virtuelle Server können von mehreren Policy-Banks aus aufgerufen

werden.

Für einige Features können Sie den Richtlinien-Manager verwenden, um Richtlinien zu konfigurieren und zu binden.

Regeln für Namen in Identifikatoren, die in Richtlinien verwendet werden

May 11, 2023

Die Namen der Bezeichner in dem benannten Ausdruck, dem HTTP-Callout, dem Mustersatz und den Funktionen zur Geschwindigkeitsbegrenzung müssen mit einem ASCII-Alphabet oder einem Unterstrich (_) beginnen. Die übrigen Zeichen können alphanumerische ASCII-Zeichen oder Unterstriche (_) sein.

Die Namen dieser Identifikatoren dürfen nicht mit den folgenden reservierten Wörtern beginnen:

- Die Wörter ALT, TRUE oder FALSE oder der einstellige Bezeichner Q oder S.
- Der spezielle Syntaxindikator RE (für reguläre Ausdrücke) oder XP (für XPath-Ausdrücke).
- Ausdruckspräfixe, die derzeit die folgenden sind:
  - CLIENT
  - VERLÄNGERN
  - HTTP
  - SERVER
  - SYS
  - ZIEL
  - TEXT
  - URL
  - MYSQL
  - MSSQL

Darüber hinaus dürfen die Namen dieser Bezeichner nicht mit den Namen der in der Richtlinieninfrastruktur verwendeten Aufzählungskonstanten übereinstimmen. Der Name eines Bezeichners darf beispielsweise nicht IGNORECASE, YEAR oder LATIN2_CZECH_CS (ein MySQL-Zeichensatz) lauten.

Hinweis: Die NetScaler-Appliance führt einen Vergleich von Bezeichnern mit diesen Wörtern und Aufzählungskonstanten durch, unabhängig von Groß- und Kleinschreibung. Beispielsweise können Namen der Bezeichner nicht mit TRUE, TRUE oder TRUE beginnen.

Erstellen oder Ändern einer Richtlinie

June 2, 2023

Alle Richtlinien haben einige gemeinsame Elemente. Das Erstellen einer Richtlinie besteht zumindest darin, die Richtlinie zu benennen und eine Regel zu konfigurieren. Die Richtlinienkonfigurationstools für die verschiedenen Features weisen Überlappungsbereiche auf, aber auch Unterschiede auf. Weitere Informationen zum Konfigurieren einer Richtlinie für ein bestimmtes Feature, einschließlich der Zuordnung einer Aktion mit der Richtlinie, finden Sie in der Dokumentation des Features.

Um eine Richtlinie zu erstellen, legen Sie zunächst den Zweck der Richtlinie fest. Beispielsweise können Sie eine Richtlinie definieren, die HTTP-Anforderungen für Bilddateien identifiziert, oder Clientanforderungen, die ein SSL-Zertifikat enthalten. Sie müssen nicht nur den Informationstyp kennen, mit dem die Richtlinie arbeiten soll, sondern auch das Format der Daten kennen, die von der Richtlinie analysiert werden.

Bestimmen Sie als Nächstes, ob die Richtlinie global anwendbar ist oder ob sie sich auf einen bestimmten virtuellen Server bezieht. Berücksichtigen Sie auch die Auswirkung, die die Reihenfolge, in der Ihre Richtlinien ausgewertet werden (die durch die Bindung der Richtlinien bestimmt wird) auf die Richtlinie hat, die Sie konfigurieren möchten.

Erstellen einer Richtlinie mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Richtlinie zu erstellen und die Konfiguration zu überprüfen:

```
- add responder|dns|cs|rewrite|cache policy <policyName> -rule <
   expression> [<feature-specific information>]

- show rewrite policy <name>
<!--NeedCopy-->
```

Beispiel 1:

```
add rewrite policy "pol_remove-ae" true "act_remove-ae"
Done
> show rewrite policy pol_remove-ae
            Name: pol_remove-ae
            Rule: true
            RewriteAction: act_remove-ae
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
```



```
            Bound to: GLOBAL RES_OVERRIDE
            Priority: 90
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Beispiel 2:

```
add cache policy BranchReportsCachePolicy -rule q{
 http.req.url.query.value("actionoverride").contains("branchReport s")
    }
  -action cache
Done
show cache policy BranchReportsCachePolicy
            Name: BranchReportsCachePolicy
            Rule: http.req.url.query.value("actionoverride").contains("
               branchReports")
            CacheAction: CACHE
            Stored in group: DEFAULT
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
Done
<!--NeedCopy-->
```

Hinweis: In der Befehlszeile müssen Anführungszeichen innerhalb einer Richtlinienregel (dem Ausdruck) maskiert oder durch das Trennzeichen q getrennt werden. Weitere Informationen finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.

Erstellen oder Ändern einer Richtlinie mit der GUI

1. Erweitern Sie im Navigationsbereich den Namen des Features, für das Sie eine Richtlinie konfigurieren möchten, und klicken Sie dann auf **Richtlinien**. Sie können beispielsweise **Content Switching, Integriertes Caching, DNS, Umschreiben oder Responder** auswählen.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, oder wählen Sie eine vorhandene Richtlinie aus, und klicken Sie auf **Öffnen**. Ein Dialogfeld zur Richtlinienkonfiguration wird angezeigt.
3. Geben Sie Werte für die folgenden Parameter an. (Ein Sternchen gibt einen erforderlichen Parameter an. Für einen Begriff in Klammern finden Sie im entsprechenden Parameter unter Parameter zum Erstellen oder Ändern einer Richtlinie.)
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
5. Klicken Sie auf **Speichern**. Eine Richtlinie wird hinzugefügt.
   Hinweis: Nachdem Sie eine Richtlinie erstellt haben, können Sie die Details der Richtlinie anzeigen, indem Sie im Konfigurationsbereich auf den Richtlinieneintrag klicken. Details, die

hervorgehoben und unterstrichen sind, sind Links zu der entsprechenden Entität (z. B. einem benannten Ausdruck).

Beispiele für Richtlinienkonfiguration

August 19, 2021

In diesen Beispielen wird gezeigt, wie Richtlinien und die zugehörigen Aktionen an der Befehlszeilenschnittstelle eingegeben werden. Im Konfigurationsdienstprogramm werden die Ausdrücke im Fenster Ausdruck des Dialogfelds Feature-Konfiguration für das integrierte Cache- oder Rewrite-Feature angezeigt.

Es folgt ein Beispiel für die Erstellung einer Caching-Richtlinie. Beachten Sie, dass Aktionen zum Zwischenspeichern von Richtlinien integriert sind, sodass Sie sie nicht getrennt von der Richtlinie konfigurieren müssen.

```
1   add cache policy BranchReportsCachePolicy -rule q{
2  http.req.url.query.value("actionoverride").contains("branchReports") }
3   -action cache
4 <!--NeedCopy-->
```

Es folgt ein Beispiel für eine Richtlinie zum Umschreiben und eine Aktion:

```
1  add rewrite action myAction1 INSERT_HTTP_HEADER "myHeader" "
      valueForMyHeader"
2  add rewrite policy myPolicy1 "http.req.url.contains("myURLstring")"
      myAction1
3 <!--NeedCopy-->
```

Hinweis: In der Befehlszeile müssen Anführungszeichen innerhalb einer Richtlinienregel (dem Ausdruck) maskiert oder durch das Trennzeichen q getrennt werden. Weitere Informationen finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.

Konfigurieren und binden Sie Richtlinien mit dem Policy Manager

May 11, 2023

> **Warnung:**
>
> Klassische Richtlinienausdrücke werden ab NetScaler 12.0 Build 56.20 nicht mehr unterstützt. Alternativ empfiehlt Citrix die Verwendung von erweiterten Richtlinien. Weitere Informationen

> finden Sie unter Erweiterte Richtlinien.

Einige Anwendungen bieten einen spezialisierten Policy Manager im NetScaler Konfigurationsprogramm, um die Konfiguration von Richtlinienbanken zu vereinfachen. Sie können damit auch Richtlinien und Aktionen suchen und löschen, die nicht verwendet werden.

Der Policy Manager ist derzeit für die Funktionen Rewrite, Integriertes Caching, Responder und Komprimierung verfügbar.

Im Folgenden sind Tastaturäquivalente für die Verfahren in diesem Abschnitt aufgeführt:

- Um eine Zelle im Richtlinien-Manager zu bearbeiten, können Sie zu der Zelle wechseln und auf F2 klicken oder die Leertaste auf der Tastatur drücken.
- Um einen Eintrag in einem Dropdown-Menü auszuwählen, können Sie zum Eintrag wechseln, die Leertaste drücken, um das Dropdown-Menü anzuzeigen, mit den Pfeiltasten NACH OBEN und NACH UNTEN zu dem gewünschten Eintrag navigieren und die Leertaste erneut drücken, um den Eintrag auszuwählen.
- Um eine Auswahl in einem Dropdown-Menü abzubrechen, drücken Sie die Escape-Taste.
- Um eine Richtlinie einzufügen, wechseln Sie zu der Zeile über der Einfügemarke und drücken Sie Steuerung+Einfügen, oder klicken Sie auf Richtlinie einfügen.
- Um eine Richtlinie zu entfernen, wechseln Sie zu der Zeile, die die Richtlinie enthält, und drücken Sie die Entf-Taste.

Hinweis: Beachten Sie, dass NetScaler beim Löschen der Richtlinie die Goto Expression-Werte anderer Richtlinien in der Bank durchsucht. Wenn einer dieser Goto Expression-Werte der Prioritätsstufe der gelöschten Richtlinie entspricht, werden sie entfernt.

Konfigurieren von Richtlinienbindungen mithilfe des Richtlinienmanagers

1. Klicken Sie im Navigationsbereich auf die Funktion, für die Sie Richtlinien konfigurieren möchten. Die Wahlmöglichkeiten sind Responder, Integriertes Caching, Rewrite oder Komprimieren.
2. Klicken Sie im Detailbereich auf **Policy Manager**.
3. Wenn Sie Bindungen für Richtlinien konfigurieren möchten, die die erweiterte Richtlinie verwenden, klicken Sie jederzeit auf die Schaltfläche Zu erweiterter Richtlinie wechseln, wenn Sie Bindungen für Richtlinien konfigurieren möchten, die die erweiterte Richtlinie verwenden.
4. Für andere Features als Responder, um den Bindepunkt anzugeben, klicken Sie auf Anforderung oder Antwort, und klicken Sie dann auf einen der Anforderungs- oder Reaktionszeitbindungspunkte. Die Optionen lauten Override Global, LB Virtual Server, CS Virtual Server, Default Global oder Policy Label. Wenn Sie den Responder konfigurieren, sind die Flusstypen Request und Response nicht verfügbar.

5. Um eine Richtlinie an diesen Bindepunkt zu binden, klicken Sie auf Richtlinie einfügen, und wählen Sie eine zuvor konfigurierte Richtlinie, ein NOPOLICY-Label oder die Option Neue Richtlinie aus. Je nach ausgewählter Option haben Sie die folgenden Möglichkeiten:

   - **Neue Richtlinie:** Erstellen Sie die Richtlinie wie unter "Richtlinie erstellen oder ändern" beschrieben, und konfigurieren Sie dann die Prioritätsstufe, den GoTo-Ausdruck und den Richtlinienaufruf, wie in der Tabelle beschrieben, "Format jedes Eintrags in einer Richtlinienbank. "
   - **Bestehende Richtlinie**, **NOPOLICY**, oder `NOPOLICY\<feature name\>`: Konfigurieren Sie die Prioritätsstufe, den GoTo-Ausdruck und den Richtlinienaufruf wie in der Tabelle beschrieben "Format jedes Eintrags in einer Richtlinienbank. " Die Optionen **NOPOLICY** oder `NOPOLICY\<feature name\>` sind nur für Richtlinien verfügbar, die erweiterte Richtlinien verwenden.

6. Wiederholen Sie die vorherigen Schritte, um dieser Policy-Bank Einträge hinzuzufügen.

7. Um die Prioritätsstufe für einen Eintrag zu ändern, können Sie einen der folgenden Schritte ausführen:

   - Doppelklicken Sie auf das Feld Priorität für einen Eintrag und bearbeiten Sie den Wert.
   - Klicken und ziehen Sie eine Richtlinie in eine andere Zeile in der Tabelle.
   - Klicken Sie auf Prioritäten neu generieren.

   In allen drei Fällen werden die Prioritätsstufen aller anderen Richtlinien nach Bedarf geändert, um dem neuen Wert Rechnung zu tragen. Gehe zu Ausdrücke mit Integer-Werten werden ebenfalls automatisch aktualisiert. Wenn Sie beispielsweise einen Prioritätswert von 10 auf 100 ändern, werden alle Richtlinien mit einem Gehe zu Ausdruck von 10 auf den Wert 100 aktualisiert.

8. Um den Richtlinien-, Aktions- oder Richtlinienbankaufruf für eine Zeile in der Tabelle zu ändern, klicken Sie auf den Pfeil nach unten rechts neben dem Eintrag, und führen Sie eine der folgenden Aktionen aus:

   - Um die Richtlinie zu ändern, wählen Sie einen anderen Richtliniennamen aus oder wählen Sie Neue Richtlinie aus und führen Sie die Schritte unter Richtlinie erstellen oder ändernaus.
   - Um den Springen-Ausdruck zu ändern, wählen Sie Weiter, Ende, USE_INVOCATION_RESULT, oder wählen Sie mehr aus, und geben Sie einen Ausdruck ein, dessen Ergebnis die Prioritätsstufe eines anderen Eintrags in dieser Richtlinienbank zurückgibt.
   - Um einen Aufruf zu ändern, wählen Sie eine vorhandene Richtlinienbank aus, oder klicken Sie auf Neues Policy Label, und führen Sie die Schritte unter Richtlinie an eine Richtlinienbezeichnung bindenaus.

9. Um die Bindung einer Richtlinie oder eines Richtlinienbezeichnungsaufrufs von dieser Bank aufzuheben, klicken Sie auf ein beliebiges Feld in der Zeile, das die Richtlinie oder die Richtlinienbezeichnung enthält, und klicken Sie dann auf Richtlinie aufheben.

10. Wenn Sie fertig sind, klicken Sie auf Änderungen übernehmen. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich gebunden ist.

Entfernen Sie ungenutzte Richtlinien mithilfe des Policy Managers

1. Klicken Sie im Navigationsbereich auf die Funktion, für die Sie die Richtlinienbank konfigurieren möchten. Die Wahlmöglichkeiten sind Responder, Integrated Caching oder Rewrite.
2. Klicken Sie im Detailbereich auf <Feature Name> Policy Manager.
3. Klicken Sie im Dialogfeld **Funktionsname> Policy**Manager auf**Cleanup Configuration**.
4. Wählen Sie im Dialogfeld **Bereinigungskonfiguration** die Elemente aus, die Sie löschen möchten, und klicken Sie dann auf **Entfernen**.
5. Klicken Sie im Dialogfeld "Entfernen" auf **Ja**.
6. Klicken Sie auf **Schließen**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich entfernt wurde.

Bindung einer Richtlinie aufheben

January 19, 2021

Wenn Sie eine Richtlinie neu zuweisen oder löschen möchten, müssen Sie zunächst die Bindung entfernen.

Aufheben der Bindung einer integrierten Caching-, Umschreibe- oder Komprimierungsrichtlinie weltweit mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine integrierte Caching-, Umschreibe- oder Komprimierungsrichtlinie global aufzuheben und die Konfiguration zu überprüfen:

```
- unbind cache|rewrite|cmp global <policyName> [-type req_override|
   req_default|res_override|res_default] [-priority <positiveInteger>]

- show cache|rewrite|cmp global
<!--NeedCopy-->
```

Beispiel:

```
> unbind cache global_nonPostReq
Done
> show cache global
    1)      Global bindpoint: REQ_DEFAULT
```



```
5               Number of bound policies: 1
6
7      2)       Global bindpoint: RES_DEFAULT
8               Number of bound policies: 1
9
10 Done
11 <!--NeedCopy-->
```

Die Priorität ist nur für die Richtlinie Dummy mit dem Namen NOPOLICY erforderlich.

Aufheben der Bindung einer Responder-Richtlinie global mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer Responder-Richtlinie global aufzuheben und die Konfiguration zu überprüfen:

```
1 -  unbind responder global <policyName> [-type override|default] [-
     priority <positiveInteger>]
2
3 -  show responder global
4 <!--NeedCopy-->
```

Beispiel:

```
1 > unbind responder global pol404Error
2 Done
3 > show responder global
4      1)       Global bindpoint: REQ_DEFAULT
5               Number of bound policies: 1
6 Done
7 <!--NeedCopy-->
```

Die Priorität ist nur für die Richtlinie Dummy mit dem Namen NOPOLICY erforderlich.

Bindung einer DNS-Richtlinie global mit der CLI aufheben

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer DNS-Richtlinie global aufzuheben und die Konfiguration zu überprüfen:

```
1 -  unbind responder global <policyName>
2
3 -  unbind responder global
4 <!--NeedCopy-->
```

Beispiel:


```
unbind dns global dfgdfg
Done
show dns global
    Policy name : dfgdfggfhg
            Priority : 100
            Goto expression : END
Done
<!--NeedCopy-->
```

Aufheben der Bindung einer erweiterten Richtlinie von einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer erweiterten Richtlinie von einem virtuellen Server zu lösen und die Konfiguration zu überprüfen:

```
-  unbind cs vserver <name> -policyName <policyName> [-priority <
   positiveInteger>] [-type REQUEST|RESPONSE]

-  show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
unbind cs vserver vs-cont-switch  -policyName pol1
Done
> show cs vserver vs-cont-switch
            vs-cont-switch (10.102.29.10:80) - HTTP Type: CONTENT
            State: UP
            Last state change was at Wed Aug 19 08:56:55 2009 (+18 ms)
            Time since last state change: 0 days, 02:47:55.750
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            State Update: DISABLED
            Default:        Content Precedence: RULE
            Vserver IP and Port insertion: OFF
            Case Sensitivity: ON
            Push: DISABLED  Push VServer:
            Push Label Rule: none
Done
<!--NeedCopy-->
```


Die Priorität ist nur für die Richtlinie Dummy mit dem Namen NOPOLICY erforderlich.

Aufheben der Bindung einer integrierten Caching-, Responder-, Rewrite- oder Komprimierungsrichtlinie Advanced Policy global mit der GUI

1. Klicken Sie im Navigationsbereich auf das Feature mit der Richtlinie, die Sie aufheben möchten (z. B. Integrated Caching)
2. Klicken Sie im Detailbereich auf den Richtlinienmanager für <Feature Name>.
3. Wählen Sie im Dialogfeld **Richtlinien-Manager** den Bindepunkt mit der Richtlinie aus, die Sie aufheben möchten, z. B. Advanced Global.
4. Klicken Sie auf den Richtliniennamen, den Sie die Bindung aufheben möchten, und klicken Sie dann auf Richtlinie aufheben.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf **Schließen**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich aufgehoben wurde.

Bindung einer DNS-Richtlinie global mit der GUI aufheben

1. Navigieren Sie zu **Traffic Management** > **DNS** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**.
3. Wählen Sie im Dialogfeld **Globale Bindungen** die Richtlinie aus und klicken Sie auf **Richtlinie aufheben**.
4. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich aufgehoben wurde.

Aufheben der Bindung einer erweiterten Richtlinie von einem virtuellen Lastausgleichs- oder Content Switching-Server über die GUI

1. Navigieren Sie zu **Verkehrsverwaltung**, erweitern Sie Load Balancing oder Content Switching, und klicken Sie dann auf **Virtuelle Server**.
2. Doppelklicken Sie im Detailbereich auf den virtuellen Server, von dem Sie die Bindung der Richtlinie aufheben möchten.
3. Deaktivieren Sie auf der Registerkarte **Richtlinien** in der Spalte **Aktiv** das Kontrollkästchen neben der Richtlinie, die Sie aufheben möchten.
4. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich aufgehoben wurde.

Richtlinien-Labels erstellen

May 11, 2023

Zusätzlich zu den integrierten Verbindungspunkten, an denen Sie Policy-Banks einrichten, können Sie auch benutzerdefinierte Policy-Labels konfigurieren und ihnen Richtlinien zuordnen.

Innerhalb eines Richtlinienlabels binden Sie Richtlinien und legen die Reihenfolge fest, in der jede Richtlinie im Verhältnis zu anderen Richtlinien in der Richtlinienbank für das Richtlinienlabel bewertet wird. Der NetScaler ermöglicht es Ihnen auch, eine beliebige Bewertungsreihenfolge wie folgt zu definieren:

- Sie können „goto“ -Ausdrücke verwenden, um auf den nächsten Eintrag in der Bank zu verweisen, der nach dem aktuellen ausgewertet werden soll.
- Sie können einen Eintrag in einer Richtlinienbank verwenden, um eine andere Bank aufzurufen.

Jedes Feature bestimmt den Typ der Richtlinie, die Sie an ein Richtlinienlabel binden können, den Typ des virtuellen Load-Balancing-Servers, an den Sie das Label binden können, und den Typ des virtuellen Content Switching-Servers, von dem aus das Label aufgerufen werden kann. Beispielsweise kann ein TCP-Richtlinienlabel nur an einen virtuellen TCP-Lastausgleichsserver gebunden werden. Sie können HTTP-Richtlinien nicht an ein Richtlinienlabel dieses Typs binden. Und Sie können ein TCP-Richtlinienlabel nur von einem virtuellen TCP-Content-Switching-Server aus aufrufen.

Nachdem Sie ein neues Policy-Label konfiguriert haben, können Sie es von einer oder mehreren Banken aus für die integrierten Bindungspunkte aufrufen.

Erstellen Sie mithilfe der CLI ein Label für die Caching-Richtlinie

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Bezeichnung für die Caching-Richtlinie zu erstellen und die Konfiguration zu überprüfen:

```
-  add cache policylabel <labelName> -evaluates req|res

-  show cache policylabel<labelName>
<!--NeedCopy-->
```

Beispiel:

```
> add cache policylabel lbl-cache-pol -evaluates req
Done

> show cache policylabel lbl-cache-pol
            Label Name: lbl-cache-pol
            Evaluates: REQ
```



```
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Erstellen Sie mithilfe der CLI ein Richtlinienlabel für den Content Switching

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Content Switching-Policy-Bezeichnung zu erstellen und die Konfiguration zu überprüfen:

```
-  add cs policylabel <labelName> http|tcp|rtsp|ssl

-  show cs policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
> add cs policylabel lbl-cs-pol http
Done
> show cs policylabel lbl-cs-pol
            Label Name: lbl-cs-pol
            Label Type: HTTP
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Erstellen Sie mithilfe der CLI ein Rewrite-Richtlinienlabel

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Rewrite-Richtlinienlabel zu erstellen und die Konfiguration zu überprüfen:

```
-  add rewrite policylabel <labelName> http_req|http_res|url|text|
   clientless_vpn_req|clientless_vpn_res

-  show rewrite policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
> add rewrite policylabel lbl-rewrt-pol http_req
Done

```



```
> show rewrite policylabel lbl-rewrt-pol
            Label Name: lbl-rewrt-pol
            Transform Name: http_req
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Erstellen Sie mithilfe der CLI ein Responder-Richtlinienlabel

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Responder-Richtlinienlabel zu erstellen und die Konfiguration zu überprüfen:

```
-  add responder policylabel <labelName>

-  show responder policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
> add responder policylabel lbl-respndr-pol
Done

> show responder policylabel lbl-respndr-pol
            Label Name: lbl-respndr-pol
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Hinweis: Rufen Sie dieses Policy-Label von einer Policy-Bank aus auf. Weitere Informationen finden Sie im Abschnitt „Eine Richtlinie an ein Richtlinienlabel binden“.

Erstellen Sie ein Richtlinienlabel mithilfe der GUI

1. Erweitern Sie im Navigationsbereich das Feature, für das Sie ein Richtlinienlabel erstellen möchten, und klicken Sie dann auf **Richtlinienlabels**. Zur Auswahl stehen Integrated Caching, Rewrite, Content Switching oder Responder.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Feld Name einen eindeutigen Namen für dieses Richtlinienlabel ein.
4. Geben Sie funktionsspezifische Informationen für das Richtlinienlabel ein. Beispielsweise würden Sie für Integriertes Caching im Dropdownmenü Evaluates die Option REQ auswählen, wenn

dieses Richtlinienlabel Richtlinien für die Anforderungszeit enthalten soll, oder RES auswählen, wenn dieses Richtlinienlabel Richtlinien für die Reaktionszeit enthalten soll. Für Rewrite würden Sie einen Transformationsnamen wählen.

5. Klicken Sie auf **Erstellen**.
6. Konfigurieren Sie eine der integrierten Policy-Banks, um dieses Policy-Label aufzurufen. Weitere Informationen finden Sie im Abschnitt „Eine Richtlinie an ein Richtlinienlabel binden“. Eine Meldung in der Statusleiste weist darauf hin, dass das Richtlinienlabel erfolgreich erstellt wurde.

Binden Sie eine Richtlinie an ein Richtlinienlabel

Wie bei Policy-Banks, die an die integrierten Bindungspunkte gebunden sind, ist jeder Eintrag in einem Policy-Label eine Richtlinie, die an das Policy-Label gebunden ist. Wie bei Richtlinien, die global oder an einen vServer gebunden sind, kann jede Richtlinie, die an das Richtlinienlabel gebunden ist, auch eine Richtlinienbank oder ein Richtlinienlabel aufrufen, das ausgewertet wird, nachdem der aktuelle Eintrag verarbeitet wurde. In der folgenden Tabelle sind die Einträge in einem Richtlinienlabel zusammengefasst.

- **Name**. Der Name einer Richtlinie oder, um eine andere Richtlinienbank aufzurufen, ohne eine Richtlinie zu bewerten, der Dummy -Richtlinienname NOPOLICY.

  Sie können NOPOLICY mehr als einmal in einer Policenbank angeben, aber Sie können eine benannte Policy nur einmal angeben.

- **Priority**. Eine ganze Zahl. Diese Einstellung kann mit dem Goto-Ausdruck verwendet werden.

- **Gehe zu Expression**. Legt die nächste Richtlinie fest, die in dieser Bank bewertet werden soll. Sie können einen der folgenden Werte angeben:

  - **WEITER**. Gehen Sie zu der Richtlinie mit der nächsthöheren Priorität.
  - **ENDE**. Beenden Sie die Bewertung.
  - **VERWENDEN SIE DAS AUFRUFERGEBNIS**. Gilt, wenn dieser Eintrag eine andere Policenbank aufruft. Wenn das letzte Goto in der aufgerufenen Bank den Wert END hat, wird die Auswertung beendet. Wenn das letzte Goto etwas anderes als END ist, führt die aktuelle Policy-Bank einen NEXT-Befehl durch.
  - **Positive Zahl:** Die Prioritätsnummer der nächsten zu bewertenden Richtlinie.
  - **Numerischer Ausdruck**. Ein Ausdruck, der die Prioritätsnummer der nächsten zu bewertenden Richtlinie erzeugt.

  Goto kann nur in einer Richtlinienbank durchgeführt werden.

  Wenn Sie den Goto-Ausdruck weglassen, entspricht dies der Angabe von END.

- **Aufruftyp.** Bezeichnet einen Policenbanktyp. Der Wert kann einer der folgenden sein:

  - **Fordern Sie Vserver**an. Ruft Richtlinien zur Anforderungszeit auf, die einem virtuellen Server zugeordnet sind.

  - **Antwort Vserver.** Ruft Richtlinien für die Reaktionszeit auf, die einem virtuellen Server zugeordnet sind.
  - **Etikett der Richtlinie**. Ruft eine andere Policy-Bank auf, die durch das Policy-Label der Bank gekennzeichnet ist.

- **Name des Aufrufs.** Der Name eines virtuellen Servers oder einer Richtlinienbezeichnung, abhängig vom Wert, den Sie für den Aufruftyp angegeben haben.

Ein Richtlinienlabel oder eine Richtlinienbank für virtuelle Server konfigurieren

May 11, 2023

Nachdem Sie Richtlinien erstellt und Richtlinienbanken erstellt haben, indem Sie die Richtlinien verbindlich festgelegt haben, können Sie eine zusätzliche Konfiguration von Richtlinien innerhalb eines Labels oder einer Richtlinienbank vornehmen. Bevor Sie beispielsweise den Aufruf einer externen Policybank konfigurieren, sollten Sie warten, bis Sie diese Policybank konfiguriert haben.

Dieses Artikel enthält die folgenden Abschnitte:

- Ein Richtlinienlabel konfigurieren
- Eine Policybank für einen virtuellen Server konfigurieren

Ein Richtlinienlabel konfigurieren

Ein Richtlinienlabel besteht aus einer Reihe von Richtlinien und Aufrufen anderer Richtlinienlabels und virtueller serverspezifischer Richtlinienbanken. Mit einem Invoke-Parameter können Sie ein Policy-Label oder eine virtuelle serverspezifische Policybank von jeder anderen Policy-Bank aus aufrufen. Mit einem speziellen NoPolicy-Eintrag können Sie eine externe Bank aufrufen, ohne einen Ausdruck (eine Regel) zu verarbeiten. Der NoPolicy-Eintrag ist eine „Dummy“ -Richtlinie, die keine Regel enthält.

Beachten Sie bei der Konfiguration von Policy-Labels über die NetScaler-Befehlszeile die folgenden Ausführungen der Befehlssyntax:

- gotoPriorityExpression wird wie in Tabelle 2 beschrieben konfiguriert. Format jedes Eintrags in einer Richtlinienbank des Abschnitts “Einträge in einer Richtlinienbank” in Bind-Richtlinien mit erweiterten Richtlinien.
- Das Argument type ist erforderlich. Dies ist anders als eine verbindliche konventionelle Politik, bei der dieses Argument optional ist.
- Sie können die Bank der Richtlinien aufrufen, die an einen virtuellen Server gebunden sind, indem Sie dieselbe Methode verwenden, die Sie zum Aufrufen eines Richtlinienlabels verwenden.

Konfigurieren Sie ein Richtlinienlabel mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Richtlinienlabel zu konfigurieren und die Konfiguration zu überprüfen:

```
- bind cache|rewrite|responder policylabel <policylabelName> -
   policyName <policyName> -priority <priority> [-
   gotoPriorityExpression <gotoprioritыExpression>] [-invoke reqvserver
   |resvserver|policylabel <policyLabelName>|<vserverName>]

- show cache|rewrite|responder policylabel <policylabelName>
<!--NeedCopy-->
```

Beispiel:

```
bind cache policylabel _reqBuiltinDefaults -policyName  _nonGetReq -
   priority 100
Done
show cache policylabel _reqBuiltinDefaults
            Label Name: _reqBuiltinDefaults
            Evaluates: REQ
            Number of bound policies: 3
            Number of times invoked: 0
    1)      Policy Name: _nonGetReq
            Priority: 100
            GotoPriorityExpression: END
    2)      Policy Name: _advancedConditionalReq
            Priority: 200
            GotoPriorityExpression: END

    3)      Policy Name: _personalizedReq
            Priority: 300
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Rufen Sie mithilfe der CLI ein Policy-Label aus einer neu geschriebenen Policy-Bank mit einem NOPOLICY-Eintrag auf

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Richtlinienlabel aus einer Rewrite-Richtlinienbank mit einem NOPOLICY-Eintrag aufzurufen und die Konfiguration zu überprüfen:

```
- bind rewrite global <policyName> <priority> <gotoPriorityExpression>
   -type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke
   reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>
```



```
2
3 -  show rewrite global
4 <!--NeedCopy-->
```

Beispiel:

```
1 > bind rewrite global NOPOLICY 100 -type REQ_DEFAULT -invoke
     policylabel lbl-rewrt-pol
2 Done
3 > show rewrite global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7     2)      Global bindpoint: REQ_OVERRIDE
8             Number of bound policies: 1
9 Done
10 <!--NeedCopy-->
```

Rufen Sie mithilfe der CLI ein Richtlinienlabel aus einer integrierten Caching-Richtlinienbank auf

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Richtlinienlabel aus einer integrierten Caching-Richtlinienbank aufzurufen und die Konfiguration zu überprüfen:

```
1 -  bind cache global NOPOLICY -priority <priority> -
     gotoPriorityExpression <gotoprioritыExpression> -type REQ_OVERRIDE|
     REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke reqvserver|resvserver|
     policylabel <policyLabelName>|<vserverName>
2
3 -  show cache global
4 <!--NeedCopy-->
```

Beispiel:

```
1 bind cache global NOPOLICY -priority 100 -gotoPriorityExpression END -
     type REQ_DEFAULT -invoke policylabel lbl-cache-pol
2 Done
3 > show cache global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 2
6
7     2)      Global bindpoint: RES_DEFAULT
8             Number of bound policies: 1
9
```



```
Done
<!--NeedCopy-->
```

Rufen Sie mithilfe der CLI ein Policy-Label aus einer Responder-Richtlinienbank auf

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Richtlinienlabel aus einer Responder-Richtlinienbank aufzurufen und die Konfiguration zu überprüfen:

```
- bind responder global NOPOLICY <priority> <gotoprioritыExpression> -
   type OVERRIDE|DEFAULT -invoke vserver|policylabel <policyLabelName
   >|<vserverName>

- show responder global
<!--NeedCopy-->
```

Beispiel:

```
> bind responder global NOPOLICY 100 NEXT -type DEFAULT -invoke
   policylabel lbl-respndr-pol
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

Done
<!--NeedCopy-->
```

Konfigurieren Sie ein Richtlinienlabel mithilfe der GUI

1. Erweitern Sie im Navigationsbereich die Funktion, für die Sie ein Richtlinienlabel konfigurieren möchten, und klicken Sie dann auf Richtlinienlabels. Zur Auswahl stehen Integrated Caching, Rewrite oder Responder.
2. Doppelklicken Sie im Detailbereich auf das Label, das Sie konfigurieren möchten.
3. Wenn Sie dieser Richtlinienbezeichnung eine neue Richtlinie hinzufügen, klicken Sie auf Richtlinie einfügen, und wählen Sie im Feld Richtlinienname die Option Neue Richtlinie aus. Weitere Informationen zum Hinzufügen einer Richtlinie finden Sie unter Erstellen oder Ändern einer Richtlinie. Wenn Sie eine Richtlinienbank aufrufen und keine Regel vor dem Aufruf ausgewertet werden soll, klicken Sie auf Richtlinie einfügen, und wählen Sie im Feld Richtlinienname die Option NOPOLICY aus.
4. Konfigurieren Sie für jeden Eintrag in diesem Richtlinienlabel Folgendes:

- **Name der Richtlinie:**

  Dies wird bereits durch den Policy-Namen, die neue Richtlinie oder den NOPOLICY-Eintrag bestimmt, den Sie in diese Bank eingegeben haben.

- **Priorität:**

  Ein numerischer Wert, der entweder eine absolute Reihenfolge der Auswertung innerhalb der Bank bestimmt oder in Verbindung mit einem Goto-Ausdruck verwendet wird.

- **Ausdruck:**

  Die politische Regel. Richtlinienausdrücke werden in den folgenden Kapiteln ausführlich beschrieben. Eine Einführung finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.

- **Aktion:**

  Die zu ergreifenden Maßnahmen, wenn diese Richtlinie als WAHR bewertet wird.

- **Gehe zu Expression:**

  Optional. Wird verwendet, um die Prioritätsstufe zu erweitern, um die nächste Policy oder Richtlinienbank zu bestimmen, die bewertet werden soll. Weitere Informationen zu möglichen Werten für einen Goto-Ausdruck finden Sie in Tabelle 2. Format jedes Eintrags in einer Richtlinienbank des Abschnitts “Einträge in einer Richtlinienbank” in Bind-Richtlinien mit erweiterten Richtlinien.

- **Aufrufen:**

  Optional. Ruft eine andere Policy-Bank auf.

5. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste weist darauf hin, dass das Richtlinienlabel erfolgreich konfiguriert wurde.

Eine Policybank für einen virtuellen Server konfigurieren

Sie können eine Reihe von Richtlinien für einen virtuellen Server konfigurieren. Die Richtlinienbank kann einzelne Richtlinien enthalten, und jeder Eintrag in der Richtlinienbank kann optional ein Richtlinienlabel oder eine Richtlinienbank aufrufen, die Sie für einen anderen virtuellen Server konfiguriert haben. Wenn Sie ein Policy-Label oder eine Policy-Bank aufrufen, können Sie dies tun, ohne einen Ausdruck (eine Regel) auszulösen, indem Sie anstelle eines Richtliniennamens einen NOPOLICY-Dummy-Eintrag auswählen.

Hinzufügen von Richtlinien zu einer Richtlinienbank für virtuelle Server mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um Richtlinien zu einer Richtlinienbank für virtuelle Server hinzuzufügen und die Konfiguration zu überprüfen:


```
- bind lb|cs vserver <virtualServerName> <serviceType> [-policyName <
   policyName>] [-priority <positiveInteger>] [-gotoPriorityExpression
   <expression>] [-type REQUEST|RESPONSE]

- show lb|cs vserver <virtualServerName>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vs-cont-sw TCP
Done
show lb vserver vs-cont-sw
            vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
            State: DOWN
            Last state change was at Wed Aug 19 10:04:02 2009 (+279 ms)
            Time since last state change: 0 days, 00:02:14.420
            Effective State: DOWN
            Client Idle Timeout: 9000 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Connection Failover: DISABLED
Done
<!--NeedCopy-->
```

Rufen Sie mithilfe der CLI ein Policy-Label aus einer virtuellen Server-Richtlinienbank mit einem NOPOLICY-Eintrag auf

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Richtlinienlabel aus einer virtuellen Server-Richtlinienbank mit einem NOPOLICY-Eintrag aufzurufen und die Konfiguration zu überprüfen:

```
- bind lb|cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
   NOPOLICY-CACHE|NOPOLICY-RESPONDER -priority <integer> -type REQUEST|
   RESPONSE -gotoPriorityExpression <gotopriorityExpression> -invoke
   reqVserver|resVserver|policyLabel <vserverName>|<labelName>

- show lb vserver
<!--NeedCopy-->
```

Beispiel:


```
> bind lb vserver vs-cont-sw -policyname NOPOLICY-REWRITE -priority 200
    -type REQUEST -gotoPriorityExpression NEXT -invoke policyLabel lbl-
   rewrt-pol
Done
<!--NeedCopy-->
```

Konfigurieren Sie eine virtuelle Serverrichtlinienbank mithilfe der GUI

1. Erweitern Sie im linken Navigationsbereich gegebenenfalls ** **Traffic Management** > **Load Balancing**, **Traffic Management** > **Content Switching**, **Traffic Management** > **SSL Offload**, **Sicherheit** > **AAA - Application Traffic** oder **NetScaler Gateway**, und klicken Sie dann auf **Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie im Dialogfeld **Virtuellen Server konfigurieren** auf die Registerkarte **Richtlinien**.
4. Um in dieser Bank eine neue Richtlinie zu erstellen, klicken Sie auf das Symbol für den Typ der Richtlinie oder die Richtlinienbezeichnung, die Sie der Richtlinienbank des virtuellen Servers hinzufügen möchten, und klicken Sie auf **Richtlinie einfügen**. Beachten Sie, dass Sie, wenn Sie ein Richtlinienlabel aufrufen möchten, ohne eine Richtlinienregel auszuwerten, die „Dummy“ -Richtlinie von NOPOLICY auswählen.
5. Um einen vorhandenen Eintrag in dieser Policybank zu konfigurieren, geben Sie Folgendes ein:
   - **Priorität:**

     Ein numerischer Wert, der entweder eine absolute Reihenfolge der Auswertung innerhalb der Bank bestimmt oder in Verbindung mit einem Goto-Ausdruck verwendet wird.
   - **Ausdruck:**

     Die politische Regel. Richtlinienausdrücke werden in den folgenden Kapiteln ausführlich beschrieben. Eine Einführung finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.
   - **Aktion:**

     Die zu ergreifenden Maßnahmen, wenn diese Richtlinie als WAHR bewertet wird.
   - **Gehe zu Expression:**

     Optional. Legt die nächste Policy-Bewertung oder Richtlinienbank fest. Weitere Informationen zu möglichen Werten für einen Goto-Ausdruck finden Sie im Abschnitt “Einträge in einer Richtlinienbank” unter Bind-Richtlinien mit erweiterten Richtlinien.

- **Aufrufen:**

  Optional. Um eine andere Richtlinienbank aufzurufen, wählen Sie den Namen der Policy Label oder der virtuellen Server Richtlinienbank, die Sie aufrufen möchten.

6. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich konfiguriert wurde.

Rufen Sie ein Richtlinienlabel oder eine virtuelle Server-Richtlinienbank auf oder entfernen Sie sie

March 10, 2023

Im Gegensatz zu einer Richtlinie, die nur einmal gebunden werden kann, können Sie ein Richtlinienlabel oder die Policy-Bank eines virtuellen Servers beliebig oft verwenden, indem Sie sie aufrufen. Der Aufruf kann von zwei Orten aus durchgeführt werden:

- Von der Bindung für eine benannte Policy in einer Richtlinienbank.
- Aus der Bindung für einen NOPOLICY Dummy Eintrag in einer Richtlinienbank.

In der Regel muss die Richtlinienbezeichnung vom gleichen Typ sein wie die Richtlinie, von der aus sie aufgerufen wird. Beispielsweise würden Sie ein Responder-Richtlinienlabel aus einer Responder-Richtlinie aufrufen.

Hinweis: Wenn Sie einen globalen NOPOLICY-Eintrag in einer Policy-Bank über die Befehlszeile binden oder die Bindung aufheben, geben Sie eine Priorität an, um einen NOPOLICY-Eintrag von einem anderen zu unterscheiden.

Rufen Sie mithilfe der CLI ein Rewrite- oder ein integriertes Caching-Richtlinienlabel auf

Geben Sie an der Befehlszeile einen der folgenden Befehle ein, um ein Rewrite- oder Integrated Caching Policy Label aufzurufen und die Konfiguration zu überprüfen:

```
1 - bind cache global <policy> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
    RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
    <label_name>
2
3 - bind rewrite global<policy> -priority <positive_integer> [-
    gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
    RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
    <label_name>
```



```
4
5 -  show cache global|show rewrite global
6 <!--NeedCopy-->
```

Beispiel:

```
1 > bind cache global _nonPostReq2 -priority 100 -type req_override -
     invoke
2     policylabel lbl-cache-pol
3 Done
4 > show cache global
5     1)      Global bindpoint: REQ_DEFAULT
6             Number of bound policies: 2
7
8     2)      Global bindpoint: RES_DEFAULT
9             Number of bound policies: 1
10
11    3)      Global bindpoint: REQ_OVERRIDE
12            Number of bound policies: 1
13
14 Done
15 <!--NeedCopy-->
```

Aufrufen einer Responder-Richtlinienbezeichnung mit der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Responder-Richtlinienlabel aufzurufen und die Konfiguration zu überprüfen:

```
1 -  bind responder global <policy_Name> <priority_as_positive_integer>
     [<gotoPriorityExpression>] -type REQ_OVERRIDE|REQ_DEFAULT|OVERRIDE|
     DEFAULT -invoke vserver|policylabel <label_name>
2
3 -  show responder global
4 <!--NeedCopy-->
```

Beispiel:

```
1 > bind responder global pol404Error1 300 -invoke policylabel lbl-
     respndr-pol
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 2
6
```



```
Done
<!--NeedCopy-->
```

Aufrufen einer virtuellen Serverrichtlinienbank mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Virtual Server Richtlinienbank aufzurufen und die Konfiguration zu überprüfen:

```
- bind lb vserver <vserver_name> -policyName <policy_Name> -priority <positive_integer> [-gotoPriorityExpression <expression>] -type REQUEST|RESPONSE -invoke reqvserver|resvserver|policylabel <policy_Label_Name>

- bind lb vserver <vserver_name>
<!--NeedCopy-->
```

Beispiel:

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 100
Done

> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+166 ms)
            Time since last state change: 28 days, 06:37:49.250
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none

    1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority: 100   Hits: 0

    2)      Policy : pol-ssl Priority:0
```



```
26      3)      Policy : ns_cmp_msapp Priority:100
27      4)      Policy : cf-pol Priority:1      Inherited
28  Done
29  <!--NeedCopy-->
```

Entfernen eines Umschreibens oder einer integrierten Caching-Richtlinienbezeichnung mit der CLI

Geben Sie an der Befehlszeile einen der folgenden Befehle ein, um eine Rewrite- oder Integrated Caching-Richtlinienbezeichnung zu entfernen und die Konfiguration zu überprüfen:

```
1  -  unbind rewrite global <policyName> -priority <positiveInteger> -type
       REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT
2
3  -  unbind cache global <policyName> -priority <positiveInteger> -type
      REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT
4
5  -  show rewrite global|show cache global
6  <!--NeedCopy-->
```

Beispiel:

```
1  > unbind rewrite global NOPOLICY -priority 100 -type REQ_OVERRIDE
2  > show rewrite global
3  Done
4      1)      Global bindpoint: REQ_DEFAULT
5              Number of bound policies: 1
6
7  Done
8  <!--NeedCopy-->
```

Entfernen einer Responder-Richtlinienbezeichnung mit der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Responder-Richtlinienlabel zu entfernen und die Konfiguration zu überprüfen:

```
1  -  unbind responder global <policyName> -priority <positiveInteger> -
      type OVERRIDE|DEFAULT
2
3  -  show responder global
4  <!--NeedCopy-->
```

Beispiel:


```
> unbind responder global NOPOLICY -priority 100 -type REQ_DEFAULT
Done
> show responder global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 1

Done
<!--NeedCopy-->
```

Entfernen einer virtuellen Server-Richtlinienbezeichnung mit der CLI

Geben Sie an der Befehlszeile einen der folgenden Befehle ein, um eine virtuelle Server-Richtlinienbezeichnung zu entfernen und die Konfiguration zu überprüfen:

```
-  unbind lb vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
   NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
   positiveInteger>

-  unbind cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
   NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <
   positiveInteger>

-  show lb vserver|show cs vserver
<!--NeedCopy-->
```

Beispiel:

```
> unbind lb vserver lbvip -policyName ns_cmp_msapp -priority 200
Done
> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+161 ms)
            Time since last state change: 28 days, 06:47:54.600
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
```



```
17              Vserver IP and Port insertion: OFF
18              Push: DISABLED  Push VServer:
19              Push Multi Clients: NO
20              Push Label Rule: none
21
22      1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
            100   Hits: 0
23
24      1)      Policy : pol-ssl Priority:0
25      2)      Policy : cf-pol Priority:1      Inherited
26  Done
27  <!--NeedCopy-->
```

Aufrufen einer Richtlinienbezeichnung oder einer virtuellen Serverrichtlinienbank mit der GUI

1. Binden Sie eine Richtlinie, wie unter Richtlinie global bindenbeschrieben, Binden Sie eine Richtlinie an einen virtuellen Serveroder Binden Sie eine Richtlinie an eine Policy Label. Alternativ können Sie anstelle eines Richtliniennamens einen NOPOLICY Dummy -Eintrag eingeben. Dies geschieht, wenn Sie vor der Auswertung der Richtlinienbank keine Policy evaluieren möchten.
2. Wählen Sie im Feld Aufrufen den Namen des Richtlinienlabels oder der virtuellen Server-Richtlinienbank aus, die Sie auswerten möchten, ob der Datenverkehr der gebundenen Richtlinie entspricht. Eine Meldung in der Statusleiste gibt an, dass das Richtlinienlabel oder die virtuelle Server-Richtlinienbank erfolgreich aufgerufen wurde.

Entfernen eines Richtlinienbezeichnungsaufrufs mit der GUI

1. Öffnen Sie die Richtlinie und löschen Sie das Feld Invoke. Durch das Aufheben der Bindung der Richtlinie wird auch der Aufruf der Beschriftung entfernt. Eine Meldung in der Statusleiste weist darauf hin, dass die Richtlinienbezeichnung erfolgreich entfernt wurde.

Konfiguration eines erweiterten Richtlinienausdrucks: Erste Schritte

May 11, 2023

Erweiterte Richtlinien werten Daten auf der Grundlage von Informationen aus, die Sie in den erweiterten Richtlinienformeln angeben. Ein erweiterter Richtlinienausdruck analysiert Datenelemente (z. B. HTTP-Header, Quell-IP-Adressen, die NetScaler-Systemzeit und POST-Textdaten). Zusätzlich zur

Konfiguration eines erweiterten Richtlinienausdrucks in einer Richtlinie konfigurieren Sie in einigen NetScaler-Funktionen den erweiterten Richtlinienausdruck außerhalb des Kontextes einer Richtlinie.

Um einen erweiterten Richtlinienausdruck zu erstellen, wählen Sie ein Präfix aus, das ein Datenelement identifiziert, das Sie analysieren möchten, und geben dann einen Vorgang an, der mit den Daten ausgeführt werden soll. Beispielsweise kann eine Operation ein Datenelement mit einer von Ihnen angegebenen Textzeichenfolge abgleichen oder eine Textzeichenfolge in einen HTTP-Header umwandeln. Andere Operationen gleichen eine zurückgegebene Zeichenfolge mit einer Reihe von Zeichenfolgen oder einem Zeichenkettenmuster ab. Sie konfigurieren zusammengesetzte Ausdrücke, indem Sie boolesche und arithmetische Operatoren angeben und die Reihenfolge der Auswertung mithilfe von Klammern steuern.

Advanced Policy Expression kann auch klassische Ausdrücke enthalten. Sie können einem häufig verwendeten Ausdruck einen Namen zuweisen, um zu vermeiden, dass der Ausdruck wiederholt erstellt werden muss.

Richtlinien und einige andere Entitäten beinhalten Regeln, die der NetScaler verwendet, um ein Paket im durch das System fließenden Verkehr auszuwerten, Daten aus dem NetScaler-System selbst zu extrahieren, eine Anfrage (einen „Callout“) an eine externe Anwendung zu senden oder um ein anderes Datenelement zu analysieren. Eine Regel hat die Form eines logischen Ausdrucks, der mit dem Datenverkehr verglichen wird und letztendlich die Werte WAHR oder FALSCH zurückgibt.

Die Elemente der Regel können selbst WAHR oder FALSCH, Zeichenfolgen oder numerische Werte zurückgeben.

Bevor Sie einen erweiterten Richtlinienausdruck konfigurieren, müssen Sie die Eigenschaften der Daten verstehen, die die Richtlinie oder eine andere Entität auswerten soll. Wenn Sie beispielsweise mit der integrierten Caching-Funktion arbeiten, bestimmt eine Richtlinie, welche Daten im Cache gespeichert werden können. Mit integriertem Caching müssen Sie die URLs, Header und anderen Daten in den HTTP-Anfragen und -Antworten kennen, die der NetScaler empfängt. Mit diesem Wissen können Sie Richtlinien konfigurieren, die den tatsächlichen Daten entsprechen, und NetScaler in die Lage versetzen, das Caching für den HTTP-Verkehr zu verwalten. Diese Informationen helfen Ihnen, den Ausdruckstyp zu bestimmen, den Sie in der Richtlinie konfigurieren müssen.

Grundelemente eines erweiterten Richtlinienausdrucks

May 11, 2023

Ein erweiterter Richtlinienausdruck besteht mindestens aus einem Präfix (oder einem einzelnen Element, das anstelle eines Präfixes verwendet wird). Die meisten Ausdrücke geben auch eine Operation an, die an den Daten ausgeführt werden soll, die das Präfix identifiziert. Sie formatieren einen Ausdruck mit bis zu 1.499 Zeichen wie folgt:


```
<prefix>.<operation> [<compound-operator> <prefix>.<operation>. . .]
```

wobei

- <prefix>

  ist ein Ankerpunkt für den Beginn eines Ausdrucks.

  Das Präfix ist ein durch Punkte getrennter Schlüssel, der eine Dateneinheit identifiziert. Das folgende Präfix untersucht beispielsweise HTTP-Anfragen auf das Vorhandensein eines Headers namens Content-Type:

  http.req.header („Inhaltstyp“)

  Präfixe können auch einzeln verwendet werden, um den Wert des Objekts zurückzugeben, das das Präfix identifiziert.

- <operation>

  identifiziert eine Bewertung, die an den durch das Präfix identifizierten Daten durchgeführt werden soll.

  Stellen Sie sich zum Beispiel den folgenden Ausdruck vor:

  http.req.header („Inhaltstyp“) .eq („text/html“)

  In diesem Ausdruck ist Folgendes die Operatorkomponente:

  eq („text/html“)

  Dieser Operator bewirkt, dass NetScaler alle HTTP-Anforderungen auswertet, die einen Content-Type-Header enthalten, und insbesondere, um festzustellen, ob der Wert dieses Headers gleich der Zeichenfolge text/html ist. Weitere Informationen finden Sie unter “Operationen. “

- <compound-operator>

  ist ein boolescher oder arithmetischer Operator, der aus mehreren Präfix- oder Präfix.operationselementen einen zusammengesetzten Ausdruck bildet.

  Stellen Sie sich zum Beispiel den folgenden Ausdruck vor:

  http.req.header („Inhaltstyp“) .eq („text/html“) & http.req.url.contains („.html“)

Präfixe

Ein Ausdruckspräfix steht für ein diskretes Datenelement. Ein Ausdruckspräfix kann beispielsweise eine HTTP-URL, einen HTTP-Cookie-Header oder eine Zeichenfolge im Hauptteil einer HTTP-POST-Anforderung darstellen. Ein Ausdruckspräfix kann eine Vielzahl von Datentypen identifizieren und zurückgeben, darunter die folgenden:

- Eine Client-IP-Adresse in einem TCP/IP-Paket

- NetScaler-Systemzeit
- Ein externes Callout über HTTP
- Ein TCP- oder UDP-Datensatztyp

In den meisten Fällen beginnt ein Ausdruckspräfix mit einem der folgenden Schlüsselwörter:

- KUNDE:
  - Identifiziert ein Merkmal des Clients, das entweder eine Anfrage sendet oder eine Antwort empfängt, wie in den folgenden Beispielen:
  - Das Präfix client.ip.dst bezeichnet die Ziel-IP-Adresse in der Anfrage oder Antwort.
  - Das Präfix client.ip.src bezeichnet die Quell-IP-Adresse.
- HTTP:
  - Identifiziert ein Element in einer HTTP-Anfrage oder einer Antwort, wie in den folgenden Beispielen:
  - Das Präfix http.req.body (integer) bezeichnet den Hauptteil der HTTP-Anfrage als mehrzeiliges Textobjekt, bis zu der in Integer angegebenen Zeichenposition.
  - Das Präfix http.req.header („header_name“) bezeichnet einen HTTP-Header, wie in header_name angegeben.
  - Das Präfix http.req.url bezeichnet eine HTTP-URL im URL-kodierten Format.
- SERVER:

  Identifiziert ein Element auf dem Server, das entweder eine Anfrage verarbeitet oder eine Antwort sendet.
- SAGT:

  Identifiziert ein Merkmal des NetScaler, der den Datenverkehr verarbeitet.

  Hinweis: Beachten Sie, dass DNS-Richtlinien nur SYS-, CLIENT- und SERVER-Objekte unterstützen.

  Darüber hinaus kann die Clientless VPN-Funktion im NetScaler Gateway die folgenden Arten von Präfixen verwenden:
- TEXT:

  Identifiziert jedes Textelement in einer Anfrage oder Antwort.
- ZIEL:

  Identifiziert das Ziel einer Verbindung.
- URL:

  Identifiziert ein Element im URL-Teil einer HTTP-Anfrage oder -Antwort.

Als allgemeine Faustregel gilt, dass jedes Ausdruckspräfix ein eigenständiger Ausdruck sein kann. Das folgende Präfix ist beispielsweise ein vollständiger Ausdruck, der den Inhalt des HTTP-Headers zurückgibt, der im Zeichenfolgenargument angegeben ist (in Anführungszeichen eingeschlossen):

```
http.res.header.("myheader")
```

Oder Sie können Präfixe mit einfachen Operationen kombinieren, um die Werte TRUE und FALSE zu ermitteln. Im Folgenden wird beispielsweise der Wert TRUE oder FALSE zurückgegeben:

```
http.res.header.("myheader").exists
```

Sie können auch komplexe Operationen für einzelne Präfixe und mehrere Präfixe innerhalb eines Ausdrucks verwenden, wie im folgenden Beispiel:

```
http.req.url.length + http.req.cookie.length <= 500
```

Welche Ausdruckspräfixe Sie angeben können, hängt von der NetScaler-Funktion ab. In der folgenden Tabelle werden die Ausdruckspräfixe beschrieben, die für jedes Feature von Interesse sind.

Feature	Typen von Ausdruckspräfixen, die im Feature verwendet werden
DNS	SYSTEM, CLIENT, SERVER
Responder in den Schutzfunktionen	HTTP, SYS, CLIENT
Content Switching	HTTP, SYS, CLIENT
Rewrite	HTTP, SYS, CLIENT, SERVER, URL, TEXT, ZIEL, VPN
Integriertes Caching	HTTP, SYS, CLIENT, SERVER
NetScaler Gateway, Clientloser Zugriff	HTTP, SYS, CLIENT, SERVER, URL, TEXT, ZIEL, VPN

Tabelle 1. Zulässige Arten von Ausdruckspräfixen in verschiedenen NetScaler-Funktionen

Hinweis: Einzelheiten zu den zulässigen Ausdruckspräfixen in einer Funktion finden Sie in der Dokumentation zu dieser Funktion.

Ausdrücke mit einem Element

Die einfachste Art von erweitertem Richtlinienausdruck enthält ein einzelnes Element. Bei diesem Element kann es sich um eines der folgenden Elemente handeln:

- wahr. Ein erweiterter Richtlinienausdruck kann einfach aus dem Wert true bestehen. Dieser Ausdruckstyp gibt immer den Wert TRUE zurück. Es ist nützlich, um politische Aktionen zu verketten und Goto-Ausdrücke auszulösen.

- falsch. Ein erweiterter Richtlinienausdruck kann einfach aus dem Wert false bestehen. Dieser Ausdruckstyp gibt immer den Wert FALSE zurück.
- Ein Präfix für einen zusammengesetzten Ausdruck. Beispielsweise ist das Präfix HTTP.REQ.HOSTNAME ein vollständiger Ausdruck, der einen Hostnamen zurückgibt, und HTTP.REQ.URL ist ein vollständiger Ausdruck, der eine URL zurückgibt. Das Präfix könnte auch in Verbindung mit Operationen und zusätzlichen Präfixen verwendet werden, um einen zusammengesetzten Ausdruck zu bilden.

Operationen

In den meisten Ausdrücken geben Sie auch eine Operation für die Daten an, die das Präfix identifiziert. Angenommen, Sie geben das folgende Präfix an:

```
http.req.url
```

Dieses Präfix extrahiert URLs in HTTP-Anfragen. Für dieses Ausdruckspräfix müssen keine Operatoren in einem Ausdruck verwendet werden. Wenn Sie jedoch einen Ausdruck konfigurieren, der HTTP-Anforderungs-URLs verarbeitet, können Sie Operationen angeben, die bestimmte Eigenschaften der URL analysieren. Im Folgenden sind einige Möglichkeiten aufgeführt:

- Suchen Sie in der URL nach einem bestimmten Hostnamen.
- Suchen Sie in der URL nach einem bestimmten Pfad.
- Bewerten Sie die Länge der URL.
- Suchen Sie in der URL nach einer Zeichenfolge, die einen Zeitstempel angibt, und konvertieren Sie sie in GMT.

Im Folgenden finden Sie ein Beispiel für ein Präfix, das einen HTTP-Header mit dem Namen Server identifiziert, und für eine Operation, die im Header-Wert nach der Zeichenfolge IIS sucht:

```
http.res.header("Server").contains("IIS")
```

Im Folgenden finden Sie ein Beispiel für ein Präfix, das Hostnamen identifiziert, und einen Vorgang, der nach der Zeichenfolge „www.mycompany.com“ als Wert des Namens sucht:

```
http.req.hostname.eq("www.mycompany.com")
```

Grundlegende Operationen mit Ausdruckspräfixen

In der folgenden Tabelle werden einige der grundlegenden Operationen beschrieben, die mit Ausdruckspräfixen ausgeführt werden können.

Vorgang	Bestimmt, ob oder nicht
CONTAINS(<string>)	Das Objekt entspricht <string>. Es folgt ein Beispiel: http.req.header („Cache-Control“) .contains („no-cache“)
EXISTS	Ein bestimmtes Objekt ist in einem Objekt vorhanden. Es folgt ein Beispiel: http.res.header („myHDR“) .exists
EQ(<text>)	Ein bestimmter nichtnumerischer Wert ist in einem Objekt vorhanden. Es folgt ein Beispiel: http.req.method.eq (post)
EQ(<integer>)	Ein bestimmter numerischer Wert ist in einem Objekt vorhanden. Es folgt ein Beispiel: client.ip.dst.eq (10.100.10.100)
LT(<integer>)	Der Wert eines Objekts ist kleiner als ein bestimmter Wert. Es folgt ein Beispiel: http.req.content_length.lt (5000)
GT(<integer>)	Der Wert eines Objekts ist größer als ein bestimmter Wert. Es folgt ein Beispiel: http.req.content_length.gt (5)

In der folgenden Tabelle sind einige der verfügbaren Operationstypen zusammengefasst.

Art des Vorgangs	Beschreibung
Textoperationen	Ordnen Sie einzelne Zeichenketten und Zeichenketten einem beliebigen Teil eines Ziels zu. Das Ziel kann eine ganze Zeichenfolge, der Anfang einer Zeichenfolge oder ein beliebiger Textabschnitt zwischen dem Anfang und dem Ende der Zeichenfolge sein. Sie können beispielsweise die Zeichenfolge „XYZ“ aus „XYZSomeText“ extrahieren. Oder Sie können einen HTTP-Header-Wert mit einem Array verschiedener Zeichenketten vergleichen. Sie können Text auch in einen anderen Datentyp umwandeln. Im Folgenden finden Sie Beispiele: Transformieren Sie eine Zeichenfolge in einen Integer-Wert, erstellen Sie eine Liste aus den Abfragezeichenfolgen in einer URL und transformieren Sie eine Zeichenfolge in einen Zeitwert.
Numerische Operationen	Numerische Operationen umfassen das Anwenden von arithmetischen Operatoren, das Auswerten der Inhaltslänge, die Anzahl der Elemente in einer Liste, Datums-, Uhrzeit- und IP-Adressen.

Zusammengesetzte erweiterte Richtlinienausdrücke

May 11, 2023

Sie können einen erweiterten Richtlinienausdruck mit booleschen oder arithmetischen Operatoren und atomaren Operationen konfigurieren. Der folgende zusammengesetzte Ausdruck hat ein boolesches UND:

```
http.req.hostname.eq("mycompany.com")&& http.req.method.eq(post)
```

Der folgende Ausdruck fügt den Wert zweier Ziele hinzu und vergleicht das Ergebnis mit einem dritten Wert:

```
http.req.url.length + http.req.cookie.length \<= 500
```


Ein zusammengesetzter Ausdruck kann eine beliebige Anzahl von logischen und arithmetischen Operatoren haben.

Der folgende Ausdruck wertet die Länge einer HTTP-Anforderung aus. Dieser Ausdruck basiert auf der URL und dem Cookie.
Dieser Ausdruck wertet den Text in der Kopfzeile aus. Führt auch ein boolesches UND für diese beiden Ergebnisse aus:

```
http.req.url.length + http.req.cookie.length \<= 500 && http.req.header.
contains("some text")
```

Sie können Klammern verwenden, um die Reihenfolge der Auswertung in einem zusammengesetzten Ausdruck zu steuern.

Boolesche Werte in zusammengesetzten Ausdrücken

Sie konfigurieren zusammengesetzte Ausdrücke mit den folgenden Operatoren:

- &&.

  Dieser Operator ist ein logisches AND. Damit der Ausdruck auf TRUE ausgewertet werden kann, müssen alle Komponenten auf TRUE ausgewertet werden.

  Beispiel:

  http.req.url.hostname.eq (MyHost) && http.req.header (MyHeader) .exists

- ||.

  Dieser Operator ist ein logisches ODER. Wenn eine Komponente des Ausdrucks zu TRUE ausgewertet wird, ist der gesamte Ausdruck TRUE.

- !.

  P Ist ein logisches NICHT für den Ausdruck.

Manchmal bietet das NetScaler-Konfigurationsdienstprogramm Operatoren UND, NICHT und ODER im Dialogfeld **Ausdruck hinzufügen** an. Diese zusammengesetzten Ausdrücke sind jedoch von eingeschränktem Nutzen. Citrix empfiehlt die Verwendung der Operatoren &&, || und! So konfigurieren Sie zusammengesetzte Ausdrücke, die Boolesche Logik verwenden.

Klammern in zusammengesetzten Ausdrücken

Sie können Klammern verwenden, um die Reihenfolge der Auswertung eines Ausdrucks zu steuern. Ein Beispiel:

```
http.req.url.contains("myCompany.com")|| (http.req.url.hostname.eq("myHost"
)&& http.req.header("myHeader").exists)
```


Das Folgende ist ein weiteres Beispiel:

```
(http.req.header("Content-Type").exists && http.req.header("Content-Type").
eq("text/html"))|| (http.req.header("Transfer-Encoding").exists || http.req
.header("Content-Length").exists)
```

Zusammengesetzte Operationen für Zeichenfolgen

In der folgenden Tabelle werden Operatoren beschrieben, mit denen Sie zusammengesetzte Operationen für Zeichenfolgendaten konfigurieren können.

Operationen, die einen Zeichenfolgenwert erzeugen	Beschreibung
str + str	Verkettet den Wert des Ausdrucks links vom Operator mit dem Wert auf der rechten Seite. Beispiel: http.req.hostname + http.req.url.protocol
str + num	Verkettet den Wert des Ausdrucks links vom Operator mit einem numerischen Wert auf der rechten Seite. Beispiel: http.req.hostname + http.req.url.content_length
num + str	Verkettet den numerischen Wert des Ausdrucks auf der linken Seite des Operators mit einem Zeichenfolgenwert auf der rechten Seite. Beispiel: http.req.url.content_length + http.req.url.hostname
str + ip	Verkettet den Zeichenfolgenwert des Ausdrucks auf der linken Seite des Operators mit einem IP-Adresswert auf der rechten Seite. Beispiel: http.req.hostname + 10.00.000.00
IP + str	Verkettet den IP-Adresswert des Ausdrucks links vom Operator mit einem Zeichenfolgenwert auf der rechten Seite. Beispiel: client.ip.dst + http.req.url.hostname

Operationen, die einen Zeichenfolgenwert erzeugen	Beschreibung
str1 ALT str2	Verwendet string2, wenn die Auswertung von String1 zu einer undef-Ausnahme führt oder das Ergebnis eine Nullzeichenfolge ist. Ansonsten verwendet string1 und wertet niemals String2 aus. Beispiel: http.req.hostname alt client.ip.src

Operationen an Zeichenfolgen, die ein Ergebnis von TRUE oder FALSE erzeugen	Beschreibung
str == str	Wertet aus, ob die Zeichenfolgen auf beiden Seiten des Operators identisch sind. Es folgt ein Beispiel: http.req.header(“myheader”) == http.res.header(“myheader”)
str <= str	Wertet aus, ob die Zeichenfolge auf der linken Seite des Operators der Zeichenfolge auf der rechten Seite entspricht oder alphabetisch vorangeht.
str >= str	Wertet aus, ob die Zeichenfolge auf der linken Seite des Operators der Zeichenfolge auf der rechten Seite entspricht oder ihr alphabetisch folgt.
str < str	Wertet aus, ob die Zeichenfolge auf der linken Seite des Operators der Zeichenfolge auf der rechten Seite alphabetisch vorausgeht.
str > str	Wertet aus, ob die Zeichenfolge auf der linken Seite des Operators der Zeichenfolge auf der rechten Seite alphabetisch folgt.
str !!= str	Wertet aus, ob die Zeichenfolgen auf beiden Seiten des Operators unterschiedlich sind.

Logische Operationen an Strings	Beschreibung
bool && bool	Dieser Operator ist ein logisches AND. Bei der Auswertung der Komponenten des zusammengesetzten Ausdrucks müssen alle Komponenten, die durch DAS UND verbunden sind, auf TRUE ausgewertet werden. Es folgt ein Beispiel: http.req.method.eq(GET) && http.req.url.query.contains(“viewReport && my_pagelabel”)
bool || bool	Dieser Operator ist ein logisches ODER. Wenn bei der Auswertung der Komponenten des zusammengesetzten Ausdrucks eine Komponente des Ausdrucks, der zu OR gehört, mit TRUE ausgewertet wird, ist der gesamte Ausdruck WAHR. Es folgt ein Beispiel: http.req.url.contains („.js“) || http.res.header. („Inhaltstyp“). Contains(“javascript”)
bool	Führt ein logisches NOT für den Ausdruck aus.

Zusammengesetzte Operationen für Zahlen

Sie können zusammengesetzte numerische Ausdrücke konfigurieren. Der folgende Ausdruck gibt beispielsweise einen numerischen Wert zurück, der die Summe einer HTTP-Headerlänge und einer URL-Länge ist:

```
http.req.header.length + http.req.url.length
```

In den folgenden Tabellen werden Operatoren beschrieben, mit denen Sie zusammengesetzte Ausdrücke für numerische Daten konfigurieren können.

Arithmetische Operationen auf Zahlen	Beschreibung
num + num	Addieren Sie den Wert des Ausdrucks auf der linken Seite des Operators zum Wert des Ausdrucks auf der rechten Seite. Es folgt ein Beispiel: http.req.content_length + http.req.url.length

Arithmetische Operationen auf Zahlen	Beschreibung
num — num	Subtrahieren Sie den Wert des Ausdrucks rechts vom Operator vom Wert des Ausdrucks auf der linken Seite.
num*num	Multiplizieren Sie den Wert des Ausdrucks links vom Operator mit dem Wert des Ausdrucks auf der rechten Seite. Es folgt ein Beispiel: client.interface.rxthroughput* 9
num / num	Teilen Sie den Wert des Ausdrucks links vom Operator durch den Wert des Ausdrucks auf der rechten Seite.
num% num	Berechnen Sie den Modulo oder den numerischen Rest einer Division des Wertes des Ausdrucks links vom Operator durch den Wert des Ausdrucks auf der rechten Seite. Zum Beispiel entsprechen die Werte “15 mod 4” 3 und “12 mod 4” gleich 0.
~number	Gibt eine Zahl zurück, nachdem eine bitweise logische Negation der Zahl angewendet wurde. Das folgende Beispiel geht davon aus, dass numeric.expression 12 (binär 1100) zurückgibt: ~numeric.expression. Das Ergebnis der Anwendung des Operator ~ ist -11 (ein binärer 1110011, insgesamt 32 Bit mit allen nach links). Beachten Sie, dass alle zurückgegebenen Werte von weniger als 32 Bit vor dem Anwenden des Operators implizit Nullen auf der linken Seite haben, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung
Zahl ^ Zahl	Vergleicht zwei Bitmuster gleicher Länge und führt eine XOR-Operation für jedes Paar entsprechender Bits in jedem Zahlenargument durch, wobei 1 zurückgegeben wird, wenn die Bits unterschiedlich sind, und 0, wenn sie gleich sind. Gibt eine Zahl zurück, nachdem ein bitweises XOR auf das Integer-Argument und den aktuellen Zahlenwert angewendet wurde. Wenn die Werte im bitweisen Vergleich gleich sind, ist der zurückgegebene Wert eine 0. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) zurückgibt und numeric.expression2 10 (binär 1010) zurückgibt: numeric.expression1 ^ numeric.expression2 Das Ergebnis der Anwendung des Operator ^ auf den gesamten Ausdruck ist 6 (binär 0110). Beachten Sie, dass alle zurückgegebenen Werte von weniger als 32 Bit vor dem Anwenden des Operators implizit Nullen auf der linken Seite haben, um sie 32 Bit breit zu machen.
Zahl | Zahl	Gibt eine Zahl zurück, nachdem ein bitweises ODER auf die Zahlenwerte angewendet wurde. Wenn einer der Werte im bitweisen Vergleich eine 1 ist, ist der zurückgegebene Wert eine 1. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) und numeric.expression2 10 (binär 1010) zurückgibt: numeric.expression1 | numeric.expression2 Das Ergebnis der Anwendung des Operator | auf den gesamten Ausdruck ist 14 (binär 1110). Beachten Sie, dass alle zurückgegebenen Werte von weniger als 32 Bit vor dem Anwenden des Operators implizit Nullen auf der linken Seite haben, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung
number & number	Vergleicht zwei Bitmuster gleicher Länge und führt eine bitweise UND -Operation für jedes Paar entsprechender Bits aus, wobei 1 zurückgegeben wird, wenn beide Bits einen Wert von 1 enthalten, und 0, wenn eines der beiden Bits 0 ist. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) und numeric.expression2 10 (binär 1010) zurückgibt: numeric.expression1 & numeric.expression2 Der gesamte Ausdruck wird als 8 (binär 1000) ausgewertet. Beachten Sie, dass alle zurückgegebenen Werte von weniger als 32 Bit vor dem Anwenden des Operators implizit Nullen auf der linken Seite haben, um sie 32 Bit breit zu machen.
num « num	Gibt eine Zahl nach einer bitweisen linken Verschiebung des Zahlenwertes um die rechte Zahl Argument Anzahl der Bits zurück. Beachten Sie, dass die Anzahl der verschobenen Bits Integer Modulo 32 ist. Das folgende Beispiel geht davon aus, dass numeric.expression1 12 (binär 1100) zurückgibt und numerisch.expression2 3 zurückgibt: numerisch.ausdruck1 « numerisch.ausdruck2 Das Ergebnis der Anwendung des LSHIFT-Operators ist 96 (eine binäre 1100000) .Beachten Sie, dass alle zurückgegebenen Werte von weniger als 32 Bit vor dem Anwenden des Operators haben implizit Nullen auf der linken Seite, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung
num » num	Gibt eine Zahl nach einer bitweisen rechten Verschiebung des Zahlenwertes um die ganzzahlige Argumentanzahl der Bits zurück. Beachten Sie, dass die Anzahl der verschobenen Bits Integer Modulo 32 ist. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) und numeric.expression2 3 zurückgibt: numeric.expression1 » numeric.expression2 Das Ergebnis der Anwendung des RSHIFT-Operators ist 1 (binär 0001). Beachten Sie, dass alle zurückgegebenen Werte von weniger als 32 Bit vor dem Anwenden des Operators implizit Nullen auf der linken Seite haben, um sie 32 Bit breit zu machen.

Numerische Operatoren, die ein Ergebnis von TRUE oder FALSE erzeugen	Beschreibung
———–	———————————————————————————
num = num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator dem Wert des Ausdrucks auf der rechten Seite entspricht.
num! = num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator nicht dem Wert des Ausdrucks auf der rechten Seite entspricht.	
num > num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator größer ist als der Wert des Ausdrucks auf der rechten Seite.
num < num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator kleiner ist als der Wert des Ausdrucks auf der rechten Seite.
num >= num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator größer oder gleich dem Wert des Ausdrucks auf der rechten Seite ist.
num <= num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator kleiner oder gleich dem Wert des Ausdrucks auf der rechten Seite ist

Funktionen für Datentypen in der Richtlinieninfrastruktur

Die NetScaler-Richtlinieninfrastruktur unterstützt die folgenden numerischen Datentypen:

- Integer (32 Bit)
- Vorzeichenlos lang (64 Bit)
- Doppelt (64 Bit)

Einfache Ausdrücke können alle diese Datentypen zurückgeben. Sie können auch zusammengesetzte Ausdrücke erstellen, die arithmetische Operatoren und logische Operatoren verwenden, um die Werte dieser Datentypen auszuwerten oder zurückzugeben. Sie können alle diese Werte auch in Richtlinienausdrücken verwenden. Literal Konstanten vom Typ unsigned long können durch Anhängen der Zeichenfolge ul an die Zahl angegeben werden. Literale Konstanten vom Typ double enthalten einen Punkt (.), einen Exponenten oder beides.

Arithmetische Operatoren, logische Operatoren und Typförderung

In zusammengesetzten Ausdrücken können die folgenden standardmäßigen arithmetischen und logischen Operatoren für die doppelten und vorzeichenlosen langen Datentypen verwendet werden:

- +, -, * und/
- %, ~, ^, &, |, «, and » (gelten nicht für Double)
- ==,! =, >, <, >= und <=

Alle diese Operatoren haben die gleiche Bedeutung wie in der Programmiersprache C.

In allen Fällen von gemischten Operationen zwischen Operanden vom Typ integer, unsigned long und double. Die Typenförderung wird durchgeführt, um die Operation an den Operanden desselben Typs durchzuführen. Die Operation fördert einen Typ mit niedrigerer Rangfolge für den Operanden mit der höchsten Rangfolge. Die Rangfolge (höher nach niedriger) lautet wie folgt:

- Doppelt
- Unsigned long
- Ganzzahl

Eine Operation, die ein numerisches Ergebnis zurückgibt, gibt also ein Ergebnis des höchsten Typs zurück, der an der Operation beteiligt ist.

Beispiel: Wenn die Operanden vom Typ Integer und Long ohne Vorzeichen sind, wird der Integer-Operand automatisch in den Typ unsigned long konvertiert. Diese Typkonvertierung erfolgt in einfachen Ausdrücken. Der durch das Ausdruckspräfix identifizierte Datentyp stimmt nicht mit dem Datentyp überein, der als Argument an die Funktion übergeben wird. In der Operation HTTP.REQ.CONTENT_LENGTH.DIV(3ul) gibt das Präfix HTTP.REQ.CONTENT_LENGTH eine Ganzzahl zurück, die zu einem Long ohne Vorzeichen wird. Unsigned long: Der Datentyp, der als Argument an die DIV () -Funktion übergeben wird, wird eine lange Division ohne Vorzeichen ausgeführt. Ebenso kann das Argument in einem Ausdruck heraufgestuft werden. Zum Beispiel fördert HTTP.REQ.HEADER(“myHeader”).TYPECAST_DOUBLE_AT.DIV(5) die ganze Zahl 5 zur Eingabe von Double und führt eine Division mit doppelter Genauigkeit durch.

Informationen zu Ausdrücken zum Umwandeln von Daten eines Typs in Daten eines anderen Typs finden Sie unter Typecasting von Daten.

Geben Sie den Zeichensatz in Ausdrücken an

May 11, 2023

Die Policy-Infrastruktur auf der NetScaler-Appliance unterstützt ASCII- und UTF-8-Zeichensätze. Der Standard-Zeichensatz ist ASCII. Wenn der Verkehr, für den Sie einen Ausdruck konfigurieren, nur aus ASCII-Zeichen besteht, müssen Sie den Zeichensatz im Ausdruck nicht angeben. Die Appliance erlaubt alle Zeichenketten- und Zeichenliterale, die Binärzeichen enthalten. Die UTF-8-Zeichensätze erfordern jedoch weiterhin, dass die Zeichenketten- und Zeichenliterale gültig sind.

```
CLIENT.TCP.PAYLOAD(100).CONTAINS("\xff\x02")
```

In einem Ausdruck muss die Funktion SET_CHAR_SET () an der Stelle im Ausdruck eingeführt werden, nach der die Datenverarbeitung im angegebenen Zeichensatz durchgeführt werden muss. For example, in the expression HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In the preceding example/).CONTAINS_ANY(“Greek_ alphabet”), if the strings stored in the pattern set “Greek_alphabet” are in UTF-8, you must include the SET_CHAR_SET(UTF_8) function immediately before the CONTAINS_ANY(“<string>”) function, as follows:

```
HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In
the preceding example/).SET_CHAR_SET(UTF_8).CONTAINS_ANY("Greek_ alphabet")
```

Die Funktion SET_CHAR_SET () legt den Zeichensatz für die gesamte Weiterverarbeitung (d. h. für alle nachfolgenden Funktionen) im Ausdruck fest, sofern er nicht später im Ausdruck durch eine andere SET_CHAR_SET () -Funktion überschrieben wird, die den Zeichensatz ändert. Therefore, if all the functions in a given simple expression are intended for UTF-8, you can include the SET_CHAR_SET(UTF_8) function immediately after functions that identify text (for example, the HEADER(“<name>”) or BODY(<int>) functions). Wenn im zweiten Beispiel, das auf den ersten Absatz oben folgt, die an die Funktionen AFTER_REGEX () und BEFORE_REGEX () übergebenen ASCII-Argumente in UTF-8-Zeichenketten geändert werden, können Sie die SET_CHAR_SET (UTF_8) -Funktion unmittelbar nach der BODY (1000) -Funktion wie folgt einschließen:

```
HTTP.REQ.BODY(1000).SET_CHAR_SET(UTF_8).AFTER_REGEX(re/Bücher/).BEFORE_REGEX
(re/Wörterbuch/).CONTAINS_ANY("Greek_alphabet")
```

Der UTF-8-Zeichensatz ist ein Obersatz des ASCII-Zeichensatzes, sodass für den ASCII-Zeichensatz konfigurierte Ausdrücke weiterhin wie erwartet funktionieren, wenn Sie den Zeichensatz auf UTF-8 ändern.

Zusammengesetzte Ausdrücke mit unterschiedlichen Zeichensätzen

Wenn in einem zusammengesetzten Ausdruck eine Teilmenge von Ausdrücken so konfiguriert ist, dass sie mit Daten im ASCII-Zeichensatz funktioniert und die übrigen Ausdrücke so konfiguriert sind, dass

sie mit Daten im UTF-8-Zeichensatz arbeiten, wird der für jeden einzelnen Ausdruck angegebene Zeichensatz berücksichtigt, wenn die Ausdrücke einzeln ausgewertet werden. Bei der Verarbeitung des zusammengesetzten Ausdrucks, unmittelbar vor der Verarbeitung der Operatoren, stuft die Appliance den Zeichensatz der zurückgegebenen ASCII-Werte jedoch auf UTF-8 um. Im folgenden zusammengesetzten Ausdruck wertet der erste einfache Ausdruck beispielsweise Daten im ASCII-Zeichensatz aus, während der zweite einfache Ausdruck Daten im UTF-8-Zeichensatz auswertet:

```
HTTP.REQ.HEADER("MyHeader")== HTTP.REQ.BODY(10).SET_CHAR_SET(UTF_8)
```

Bei der Verarbeitung des zusammengesetzten Ausdrucks stellt die NetScaler-Appliance jedoch unmittelbar vor der Auswertung des booleschen Operators „ist gleich“ den Zeichensatz des von HTTP.REQ.HEADER („myHeader“) zurückgegebenen Werts auf UTF-8 um.

Der erste einfache Ausdruck im folgenden Beispiel wertet Daten im ASCII-Zeichensatz aus. Wenn die NetScaler-Appliance jedoch den zusammengesetzten Ausdruck verarbeitet, unmittelbar bevor die Ergebnisse der beiden einfachen Ausdrücke miteinander verknüpft werden, stuft die Appliance den Zeichensatz des von HTTP.REQ.BODY (10) zurückgegebenen Werts auf UTF-8 um.

```
HTTP.REQ.BODY(10)+ HTTP.REQ.HEADER("MyHeader").SET_CHAR_SET(UTF_8)
```

Daher gibt der zusammengesetzte Ausdruck Daten im UTF-8-Zeichensatz zurück.

Geben Sie den Zeichensatz auf der Grundlage des Zeichensatzes des Datenverkehrs an

Sie können den Zeichensatz basierend auf den Verkehrsmerkmalen auf UTF-8 setzen. Wenn Sie sich nicht sicher sind, ob der Zeichensatz des ausgewerteten Datenverkehrs UTF-8 ist, können Sie einen zusammengesetzten Ausdruck konfigurieren, bei dem der erste Ausdruck nach UTF-8-Verkehr sucht und nachfolgende Ausdrücke den Zeichensatz auf UTF-8 setzen. Es folgt ein Beispiel für einen zusammengesetzten Ausdruck, der zuerst den Wert von „charset“ im Content-Type-Header der Anfrage auf „UTF-8“ überprüft, bevor überprüft wird, ob die ersten 1000 Byte der Anfrage die UTF-8-Zeichenfolge Bücher enthalten:

```
HTTP.REQ.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).TYPECAST_NVLIST_T
('=', '; ', '"').VALUE("charset").EQ("UTF-8")&& HTTP.REQ.BODY(1000).SET_CHAR_SET
(UTF_8).CONTAINS("Bücher")
```

Wenn Sie sicher sind, dass der Zeichensatz des ausgewerteten Datenverkehrs UTF-8 ist, ist der zweite Ausdruck im Beispiel ausreichend.

Zeichen- und Zeichenkettenliterale in Ausdrücken

Bei der Auswertung von Ausdrücken gelten Zeichenliterale und Zeichenfolgenliterale, die in einfache Anführungszeichen (‘) bzw. Anführungszeichen („) eingeschlossen sind, als Literale im UTF-8-Zeichensatz, selbst wenn der aktuelle Zeichensatz ASCII ist. Wenn in einem bestimmten Ausdruck

eine Funktion mit Zeichen- oder Zeichenkettenliteralen im ASCII-Zeichensatz arbeitet und Sie ein Nicht-ASCII-Zeichen in das Literal aufnehmen, wird ein Fehler zurückgegeben.

> **Hinweis**:
>
> Die Zeichenkettenliterale in fortgeschrittenen politischen Ausdrücken sind jetzt genauso lang wie der politische Ausdruck. Der Ausdruck darf 1499 Byte oder 8191 Byte lang sein.

Werte im Hexadezimal- und Oktalformat

Bei der Konfiguration eines Ausdrucks können Sie Werte im Oktal- und Hexadezimalformat eingeben. Jedes Hexadezimal- oder Oktalbyte wird jedoch als UTF-8-Byte betrachtet. Ungültige UTF-8-Bytes führen zu Fehlern, unabhängig davon, ob der Wert manuell eingegeben oder aus der Zwischenablage eingefügt wurde. Beispielsweise ist „\ xce\ x20" ein ungültiges UTF-8-Zeichen, da auf „c8" nicht „20" folgen kann (auf jedes Byte in einer Mehrbyte-UTF-8-Zeichenfolge muss das High-Bit gesetzt sein). Ein weiteres Beispiel für ein ungültiges UTF-8-Zeichen ist „\ xce\ xa9", da die Hexadezimalzeichen durch ein Leerzeichen getrennt sind.

Funktionen, die UTF-8-Zeichenketten zurückgeben

Nur die Funktionen `text>.XPATH` und `<text>.XPATH_JSON` geben immer UTF-8-Zeichenketten zurück. Die folgenden MYSQL-Routinen bestimmen zur Laufzeit, welcher Zeichensatz zurückgegeben wird, abhängig von den Daten im Protokoll:

- `MYSQL_CLIENT_T.USER`
- `MYSQL_CLIENT_T.DATABASE`
- `MYSQL_REQ_QUERY_T.COMMAND`
- `MYSQL_REQ_QUERY_T.TEXT`
- `MYSQL_REQ_QUERY_T.TEXT(<unsigned int>)`
- `MYSQL_RES_ERROR_T.SQLSTATE`
- `MYSQL_RES_ERROR_T.MESSAGE`
- `MYSQL_RES_FIELD_T.CATALOG`
- `MYSQL_RES_FIELD_T.DB`
- `MYSQL_RES_FIELD_T.TABLE`
- `MSQL_RES_FIELD_T.ORIGINAL_TABLE`
- `MYSQL_RES_FIELD_T.NAME`
- `MYSQL_RES_FIELD_T.ORIGINAL_NAME`
- `MYSQL_RES_OK_T.MESSAGE`
- `MYSQL_RES_ROW_T.TEXT_ELEM(<unsigned int>)`

Terminalverbindungseinstellungen für UTF-8

Wenn Sie eine Verbindung zur NetScaler-Appliance mithilfe einer Terminalverbindung einrichten (z. B. mithilfe von PuTTY), müssen Sie den Zeichensatz für die Übertragung von Daten auf UTF-8 festlegen.

Minimale und maximale Funktionen in einer fortschrittlichen politischen Formulierung

Die erweiterten Richtlinienausdrücke unterstützen die folgenden Mindest- und Maximalfunktionen.

1. `(<expression1>.max(<expression2>)` - gibt das Maximum der beiden Werte zurück.
2. `(<expression1>.min(<expression2>)` - gibt das Minimum der beiden Werte zurück.

Konfigurieren erweiterter Richtlinienausdrücke in einer Richtlinie

October 8, 2021

Sie können einen erweiterten Richtlinienausdruck mit bis zu 1.499 Zeichen in einer Richtlinie konfigurieren. Die Benutzeroberfläche für erweiterte Richtlinienausdrücke hängt in gewissem Maße von der Funktion ab, für die Sie den Ausdruck konfigurieren, und davon, ob Sie einen Ausdruck für eine Richtlinie oder für eine andere Verwendung konfigurieren.

Wenn Sie Ausdrücke in der Befehlszeile konfigurieren, begrenzen Sie den Ausdruck mithilfe von Anführungszeichen (“.” oder ‘:. ‘). Innerhalb eines Ausdrucks entkommen Sie zusätzlichen Anführungszeichen mithilfe eines umgekehrten Schrägstrichs (). Beispielsweise sind die folgenden Standardmethoden zum Entkommen von Anführungszeichen in einem Ausdruck:

```
"\"abc\""
```

```
 '\"abc\"'
```

Sie müssen auch einen umgekehrten Schrägstrich verwenden, um Fragezeichen und andere umgekehrte Schrägstriche in der Befehlszeile zu vermeiden. Zum Beispiel der Ausdruck http.req.url.contains (“?”) erfordert einen Backslash, damit das Fragezeichen analysiert wird. Beachten Sie, dass das Backslash-Zeichen nicht in der Befehlszeile angezeigt wird, nachdem Sie das Fragezeichen eingegeben haben. Wenn Sie andererseits einen umgekehrten Schrägstrich entkommen (z. B. im Ausdruck ‘http.req.url.contains (“\\ http”) ‘), werden die Escape-Zeichen in der Befehlszeile wiedergegeben.

Um einen Eintrag lesbarer zu machen, können Sie die Anführungszeichen für einen gesamten Ausdruck entkommen. Am Anfang des Ausdrucks geben Sie die Escape-Sequenz “q” plus eines der folgenden Sonderzeichen ein:/{<	~$^+=&%@‘?.

Am Ende des Ausdrucks geben Sie wie folgt nur das Sonderzeichen ein:

```
q@http.req.url.contains("sometext") && http.req.cookie.exists@

q~http.req.url.contains("sometext") && http.req.cookie.exists~
<!--NeedCopy-->
```

Beachten Sie, dass ein Ausdruck, der das {Trennzeichen verwendet, mit} geschlossen wird.

Für einige Funktionen (z. B. integriertes Caching und Responder) bietet das Dialogfeld zur Richtlinienkonfiguration ein sekundäres Dialogfeld zum Konfigurieren von Ausdrücken. In diesem Dialogfeld können Sie aus Dropdownlisten wählen, die die verfügbaren Wahlmöglichkeiten an jedem Punkt während der Ausdruckskonfiguration anzeigen. Sie können bei Verwendung dieser Konfigurationsdialoge keine arithmetischen Operatoren verwenden, aber die meisten anderen erweiterten Richtlinienausdrucksfunktionen sind verfügbar. Um arithmetische Operatoren zu verwenden, schreiben Sie Ihre Ausdrücke im Freiformformat.

Konfigurieren einer erweiterten Richtliniensyntaxregel über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine erweiterte Richtlinienregel zu konfigurieren und die Konfiguration zu überprüfen:

1. `add cache|dns|rewrite|cs policyName **-rule** expression featureSpecificParameter **-action**`
2. `show cache|dns|rewrite|cs policyName`
   Es folgt ein Beispiel für die Konfiguration einer Caching-Richtlinie:

   Beispiel:

```
> add cache policy pol-cache -rule http.req.content_length.le(5) -
    action INVAL
 Done

> show cache policy pol-cache
        Name: pol-cache
        Rule: http.req.content_length.le(5)
```



```
7          CacheAction: INVAL
8          Invalidate groups: DEFAULT
9          UndefAction: Use Global
10         Hits: 0
11         Undef Hits: 0
12
13  Done
14 <!--NeedCopy-->
```

Konfigurieren eines erweiterten Richtlinienausdrucks über die GUI

1. Klicken Sie im Navigationsbereich auf den Namen der Funktion, für die Sie eine Richtlinie konfigurieren möchten. Sie können beispielsweise Integriertes Caching, Responder, DNS, Rewrite oder Content Switching auswählen und dann auf **Richtlinien**klicken.
2. Klicken Sie auf Hinzufügen.
3. Klicken Sie für die meisten Features in das Feld **Ausdruck** . Für Content Switching, klicken Sie auf **Konfigurieren**.
4. Klicken Sie auf das **Präfix-Symbol** (das Haus) und wählen Sie das erste Ausdruckspräfix aus der Dropdownliste aus. In Responder lauten die Optionen beispielsweise HTTP, SYS und CLIENT. Der nächste Satz anwendbarer Optionen wird in einer Dropdownliste angezeigt.
5. Doppelklicken Sie auf die nächste Option, um sie auszuwählen, und geben Sie dann einen Punkt ein (.). Auch hier wird eine Reihe anwendbarer Optionen in einer anderen Dropdownliste angezeigt.
6. Wählen Sie weiterhin Optionen aus, bis ein Eingabefeld (durch Klammern signalisiert) angezeigt wird. Wenn Sie ein Eingabefeld sehen, geben Sie einen entsprechenden Wert in die Klammern ein. Wenn Sie beispielsweise GT (int) (größer als, Integer-Format) auswählen, geben Sie eine Ganzzahl in Klammern an. Textzeichenfolgen werden durch Anführungszeichen begrenzt. Es folgt ein Beispiel:

   ```
   HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

7. Um einen Operator zwischen zwei Teilen eines zusammengesetzten Ausdrucks einzufügen, klicken Sie auf das Symbol Operatoren (das Sigma) und wählen Sie den Operatortyp aus. Es folgt ein Beispiel für einen konfigurierten Ausdruck mit einem booleschen ODER (signalisiert durch doppelte vertikale Balken, ||):

   ```
   HTTP.REQ.URL.EQ("www.mycompany.com")||HTTP.REQ.BODY(1000).BETWEEN("this
   ","that")
   ```

8. Um einen benannten Ausdruck einzufügen, klicken Sie auf den Pfeil nach unten neben dem Symbol Hinzufügen (das Pluszeichen) und wählen Sie einen benannten Ausdruck aus.

9. Um einen Ausdruck mithilfe von Dropdown-Menüs zu konfigurieren und integrierte Ausdrücke einzufügen, klicken Sie auf das Symbol Hinzufügen (das Pluszeichen). Das Dialogfeld **Ausdruck hinzufügen** funktioniert ähnlich wie das Hauptdialogfeld, bietet jedoch Dropdownlisten zur Auswahl von Optionen und bietet Textfelder für die Dateneingabe anstelle von Klammern. Dieses Dialogfeld enthält auch eine Dropdownliste “Häufig verwendete Ausdrücke”, in die häufig verwendete Ausdrücke eingefügt werden. Wenn Sie mit dem Hinzufügen des Ausdrucks fertig sind, klicken Sie auf **OK**.
10. Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Eine Meldung in der Statusleiste zeigt an, dass der Richtlinienausdruck erfolgreich konfiguriert wurde.

Testen eines erweiterten Richtlinienausdrucks über die GUI

1. Klicken Sie im Navigationsbereich auf den Namen der Funktion, für die Sie eine Richtlinie konfigurieren möchten (z. B. können Sie Integriertes Caching, Responder, DNS, Rewrite oder Content Switching auswählen), und klicken Sie dann auf Richtlinien.
2. Wählen Sie eine Richtlinie aus und klicken Sie auf **Öffnen**.
3. Um den Ausdruck zu testen, klicken Sie auf das Symbol “Auswerten” (das Häkchen).
4. Wählen Sie im Dialogfeld Ausdrucksauswertung den Flow-Typ aus, der mit dem Ausdruck übereinstimmt.
5. Fügen Sie im Feld **HTTP-Anforderungsdaten** oder **HTTP-Antwortdaten** die HTTP-Anforderung oder Antwort ein, die Sie mit dem Ausdruck analysieren möchten, und klicken Sie auf **Auswerten**. Beachten Sie, dass Sie eine vollständige HTTP-Anfrage oder -Antwort angeben müssen und der Header und der Text durch eine Leerzeile getrennt sein sollten. Einige Programme, die HTTP-Header abfangen, fangen die Antwort nicht ebenfalls ab. Wenn Sie nur den Header kopieren und einfügen, fügen Sie am Ende des Headers eine leere Zeile ein, um eine vollständige HTTP-Anforderung oder -Antwort zu erstellen.
6. Klicken Sie auf **Schließen**, um dieses Dialogfeld zu schließen.

Konfigurieren benannter erweiterter Richtlinien

October 8, 2021

Anstatt denselben Ausdruck mehrmals in mehrere Richtlinien einzugeben, können Sie einen benannten Ausdruck konfigurieren und auf den Namen verweisen, wenn Sie den Ausdruck in einer Richtlinie verwenden möchten. Beispielsweise könnten Sie die folgenden benannten Ausdrücke erstellen:

- Dieser Ausdruck:

  ```
  http.req.body(100).contains("this")
  ```


- Dieser Ausdruck:

```
http.req.body(100).contains("that")
```

Sie können diese benannten Ausdrücke dann in einem Richtlinienausdruck verwenden. Zum Beispiel ist das Folgende ein rechtlicher Ausdruck, der auf den vorhergehenden Beispielen basiert:

Dieser Ausdruck	Dieser Ausdruck

Sie können den Namen eines erweiterten Richtlinienausdrucks als Präfix für eine Funktion verwenden. Der benannte Ausdruck kann entweder ein einfacher Ausdruck oder ein zusammengesetzter Ausdruck sein. Die Funktion muss eine sein, die mit dem Datentyp arbeiten kann, der vom benannten Ausdruck zurückgegeben wird.

Beispiel 1: Einfacher benannter Ausdruck als Präfix

Der folgende einfache benannte Ausdruck, der eine Textzeichenfolge identifiziert, kann als Präfix für die <string>Funktion AFTER_STR (“ “) verwendet werden, die mit Textdaten arbeitet:

```
HTTP.REQ.BODY(1000)
```

Wenn der Name des Ausdrucks Top1KB lautet, können Sie Top1KB.after_Str (“Benutzername”) anstelle von HTTP.REQ.BODY (1000) .AFTER_STR (“Benutzername”) verwenden.

Beispiel 2: Zusammengesetzter benannter Ausdruck als Präfix

Sie können einen zusammengesetzten benannten Ausdruck namens basic_header_value erstellen, um den Benutzernamen in einer Anforderung, einen Doppelpunkt (:) und das Kennwort des Benutzers wie folgt zu verketten:

```
add policy expression basic_header_value "HTTP.REQ.USER.NAME + \":\" + HTTP
.REQ.USER.PASSWD"
```

Sie können dann den Namen des Ausdrucks in einer Rewriteaktion verwenden, wie im folgenden Beispiel gezeigt:

```
add rewrite action insert_b64encoded_authorization insert_http_header
authorization '"Basic " + basic_header_value.b64encode'
```

Im Beispiel wird in dem Ausdruck, der verwendet wird, um den Wert des benutzerdefinierten Headers zu konstruieren, der B64-Codierungsalgorithmus auf die Zeichenfolge angewendet, die von dem zusammengesetzten benannten Ausdruck zurückgegeben wird.

Sie können auch einen benannten Ausdruck (entweder allein oder als Präfix für eine Funktion) verwenden, um den Textausdruck für das Ersetzungsziel in einem Rewrite zu erstellen.

Konfigurieren eines benannten erweiterten Richtlinienausdrucks über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen benannten Ausdruck zu konfigurieren und die Konfiguration zu überprüfen:

```
1 -  add policy expression <name><value>
2
3 -  show policy expression <name>
4 <!--NeedCopy-->
```

Beispiel:

```
1 > add policy expression myExp "http.req.body(100).contains("the other")
     "
2 Done
3
4 > show policy expression myExp
5     1)      Name: myExp  Expr: "http.req.body(100).contains("the other"
          )"  Hits: 0 Type : ADVANCED
6 Done
7 <!--NeedCopy-->
```

Der Ausdruck kann bis zu 1.499 Zeichen lang sein.

Konfigurieren Sie einen benannten Ausdruck über die GUI

1. Erweitern Sie im Navigationsbereich **AppExpert**, und klicken Sie dann auf **Ausdrücke**.
2. Klicken Sie auf **Erweiterte Ausdrücke**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie einen Namen und eine Beschreibung für den Ausdruck ein.
5. Konfigurieren Sie den Ausdruck mithilfe des unter Erweiterten Richtlinienausdruck konfigurierenbeschriebenen Prozess. Eine Meldung in der Statusleiste zeigt an, dass der Richtlinienausdruck erfolgreich konfiguriert wurde.

Konfigurieren erweiterter Richtlinienausdrücke außerhalb des Kontexts einer Richtlinie

August 19, 2021

Eine Reihe von Funktionen, einschließlich der folgenden, kann einen erweiterten Richtlinienausdruck erfordern, der nicht Teil einer Richtlinie ist:

- Integrierte Caching-Auswahlen:

  In der Definition des Selektors definieren Sie mehrere nicht-zusammengesetzte Ausdrücke (Selectlets). Jedes Selectlet befindet sich in einer impliziten logischen UND-Beziehung zu den anderen.

- Lastenausgleich:

  Sie konfigurieren einen Ausdruck für die TOKEN-Methode des Lastenausgleichs für einen virtuellen Lastausgleichsserver.

- Aktionen umschreiben:

  Ausdrücke definieren den Speicherort der Umschreibaktion und den Typ des durchzuführenden Umschreibens, abhängig vom Typ der Umschreibaktion, die Sie konfigurieren. Beispielsweise verwendet eine DELETE -Aktion nur einen Zielausdruck. Eine REPLACE -Aktion verwendet einen Zielausdruck und einen Ausdruck, um den Ersetzungstext zu konfigurieren.

- Preisbasierte Richtlinien:

  Sie verwenden erweiterte Richtlinienausdrücke, um Limit-Selektoren zu konfigurieren. Sie können diese Selektoren verwenden, wenn Sie Richtlinien konfigurieren, um die Rate des Datenverkehrs auf verschiedene Server zu drosseln. In der Definition des Selektors definieren Sie bis zu fünf nicht-zusammengesetzte Ausdrücke (Selectlets). Jedes Selectlet befindet sich in einem impliziten logischen UND mit den anderen.

Konfigurieren eines erweiterten Richtlinienausdrucks außerhalb einer Richtlinie mit der CLI (Beispiel für die Cache-Auswahl)

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen erweiterten Richtlinienausdruck außerhalb einer Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
-  add cache selector <selectorName> <rule>
-  show cache selector <selectorName>
<!--NeedCopy-->
```

Beispiel:

```
> add cache selector mainpageSelector "http.req.cookie.value("ABC_def")
   "
    "http.req.url.query.value("_ghi")"selector "mainpageSelector" added
Done
> show cache selector mainpageSelector
            Name: mainpageSelector
            Expressions:
                    1) http.req.cookie.value("ABC_def")
```



```
                    2) http.req.url.query.value("_ghi")
Done
<!--NeedCopy-->
```

Es folgt ein äquivalenter Befehl, der das lesbarere q-Trennzeichen verwendet, wie unter Konfigurieren von erweiterten Richtlinienausdrücken in einer Richtlinie beschrieben:

```
> add cache selector mainpageSelector2 q~http.req.cookie.value("ABC_def
   ")~
    q~http.req.url.query.value("_ghi")~selector "mainpageSelector2"
       added
Done
> show cache selector mainpageSelector2
            Name: mainpageSelector2
            Expressions:
                    1) http.req.cookie.value("ABC_def")
                    2) http.req.url.query.value("_ghi")
Done
<!--NeedCopy-->
```

Erweiterte Richtlinienausdrücke: Auswerten von Text

January 19, 2021

Sie können eine Richtlinie mit einem erweiterten Richtlinienausdruck konfigurieren, der Text in einer Anforderung oder Antwort auswertet. Erweiterte Richtlinien-Textausdrücke können von einfachen Ausdrücken reichen, die Zeichenfolgenabgleich in HTTP-Headern durchführen, bis hin zu komplexen Ausdrücken, die Text kodieren und dekodieren. Sie können Textausdrücke so konfigurieren, dass zwischen Groß- und Kleinschreibung unterschieden wird und Leerzeichen verwendet oder ignoriert werden. Sie können komplexe Textausdrücke auch konfigurieren, indem Sie Textausdrücke mit booleschen Operatoren kombinieren

Sie können Ausdruckspräfixe und Operatoren für die Auswertung von HTTP-Anforderungen, HTTP-Antworten sowie VPN- und Clientless-VPN-Daten verwenden. Textausdruck-Präfixe sind jedoch nicht auf die Auswertung dieser Elemente Ihres Datenverkehrs beschränkt.

Informationen zu Textausdrücken

May 11, 2023

Sie können verschiedene Ausdrücke für die Arbeit mit Text konfigurieren, der durch die NetScaler-Appliance fließt. Im Folgenden finden Sie einige Beispiele, wie Sie Text mithilfe eines erweiterten Richtlinienausdrucks analysieren können:

- Stellen Sie fest, dass ein bestimmter HTTP-Header existiert.

  Beispielsweise können Sie HTTP-Anfragen identifizieren, die einen bestimmten Accept-Language-Header enthalten, um die Anforderung an einen bestimmten Server zu leiten.

- Bestimmen Sie, dass eine bestimmte HTTP-URL eine bestimmte Zeichenfolge enthält.

  Beispielsweise möchten Sie möglicherweise Anfragen für bestimmte URLs blockieren. Beachten Sie, dass die Zeichenfolge am Anfang, in der Mitte oder am Ende einer anderen Zeichenfolge auftreten kann.

- Identifizieren Sie eine POST-Anfrage, die an eine bestimmte Anwendung gerichtet ist.

  Beispielsweise möchten Sie möglicherweise alle POST-Anfragen identifizieren, die an eine Datenbankanwendung gerichtet sind, um zwischengespeicherte Anwendungsdaten zu aktualisieren.

Beachten Sie, dass es spezielle Tools zum Anzeigen des Datenstroms für HTTP-Anfragen und -Antworten gibt. Sie können die Tools verwenden, um den Datenstrom anzuzeigen.

Informationen zu Operationen auf Text

Ein textbasierter Ausdruck besteht aus mindestens einem Präfix zur Identifizierung eines Datenelements und normalerweise (wenn auch nicht immer) einer Operation für dieses Präfix. Textbasierte Vorgänge können für jeden Teil einer Anfrage oder einer Antwort gelten. Zu den grundlegenden Operationen für Text gehören verschiedene Arten von Zeichenfolgenübereinstimmungen.

Zum Beispiel vergleicht der folgende Ausdruck einen Header-Wert mit einer Zeichenfolge:

```
http.req.header("myHeader").contains("some-text")
```

Die folgenden Ausdrücke sind Beispiele für den Abgleich eines Dateityps in einer Anforderung:

```
http.req.url.suffix.contains("jpeg")
```

```
http.req.url.suffix.eq("jpeg")
```

In den vorangegangenen Beispielen erlaubt der Operator “contains” eine teilweise Übereinstimmung und der EQ-Operator sucht nach einer exakten Übereinstimmung.

Andere Operationen sind verfügbar, um die Zeichenfolge vor der Auswertung zu formatieren. Sie können beispielsweise Textoperationen verwenden, um Anführungszeichen und Leerzeichen zu entfernen, die Zeichenfolge in Kleinbuchstaben umzuwandeln oder Zeichenfolgen zu verketten.

> **Hinweis**:
>
> Komplexe Operationen sind verfügbar, um einen auf Mustern basierenden Abgleich durchzuführen oder einen Textformattyp in einen anderen Typ zu konvertieren.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Mustersätze und Datensätze.
- Reguläre Ausdrücke.
- Typecasting von Daten.

Compounding und Rangfolge in Textausdrücken

Sie können verschiedene Operatoren anwenden, um Textpräfixe oder Ausdrücke zu kombinieren. Beispielsweise verkettet der folgende Ausdruck die zurückgegebenen Werte jedes Präfixes:

```
http.req.hostname + http.req.url
```

Es folgt ein Beispiel für einen zusammengesetzten Textausdruck, der ein logisches UND verwendet. Beide Komponenten dieses Ausdrucks müssen TRUE sein, damit eine Anforderung mit dem Ausdruck übereinstimmt:

```
http.req.method.eq(post)&& http.req.body(1024).startswith("destination=")
```

> **Hinweis:**
>
> Weitere Informationen zu Operatoren für die Compoundierung finden Sie unter Zusammengesetzte erweiterte Ausdrücke.

Kategorien von Textausdrücken

Die Hauptkategorien von Textausdrücken, die Sie konfigurieren können, sind:

- Informationen in HTTP-Headern, HTTP-URLs und dem POST-Text in HTTP-Anforderungen.

  Weitere Informationen finden Sie unter Ausdruckspräfixe für Text in HTTP-Anfragen und -Antworten.

- Informationen zu einem VPN oder einem clientlosen VPN.

  Weitere Informationen finden Sie unter Ausdruckspräfixe für VPNs und clientlose VPNs.

- TCP-Nutzlastinformationen.

  Weitere Informationen zu TCP-Nutzlastausdrücken finden Sie unter Erweiterte Richtlinienausdrücke: Analysieren von HTTP-, TCP- und UDP-Daten.

- Text in einem SSL-Zertifikat (Secure Sockets Layer).

Informationen zu Textausdrücken für SSL- und SSL-Zertifikatsdaten finden Sie unter Erweiterte Richtlinienausdrücke: Analysieren von SSL-Zertifikaten und Ausdrücken für SSL-Zertifikatdaten.

> **Hinweis:**
>
> Das Analysieren eines Dokumentkörpers, z. B. des Hauptteils einer POST-Anforderung, kann sich auf die Leistung auswirken. Möglicherweise möchten Sie die Auswirkungen von Richtlinien auf die Leistung testen, die einen Dokumentenkörper bewerten.

Richtlinien für Textausdrücke

Unter dem Gesichtspunkt der Leistung ist es typischerweise am besten, protokollbewusste Funktionen in einem Ausdruck zu verwenden. Der folgende Ausdruck verwendet beispielsweise eine protokollbewusste Funktion:

```
HTTP.REQ.URL.QUERY
```

Der vorherige Ausdruck schneidet besser ab als der folgende äquivalente Ausdruck, der auf dem Parsen von Zeichenfolgen basiert:

```
HTTP.REQ.URL.AFTER_STR("?")
```

Im ersten Fall betrachtet der Ausdruck speziell die URL-Abfrage. Im zweiten Fall scannt der Ausdruck die Daten auf das erste Auftreten eines Fragezeichens.

Es gibt auch einen Leistungsvorteil von strukturiertem Analysieren von Text, wie im folgenden Ausdruck:

```
HTTP.REQ.HEADER("Example").TYPECAST_LIST_T(',').GET(1)
```

(Weitere Informationen zum Typecasting finden Sie unter Typecasting von Daten. Der Typecast-Ausdruck, der kommagetrennte Daten sammelt und sie in eine Liste strukturiert, würde normalerweise besser funktionieren als das folgende unstrukturierte Äquivalent:

```
HTTP.REQ.HEADER("Example").AFTER_STR(",").BEFORE_STR(",")
```

Schließlich haben unstrukturierte Textausdrücke typischerweise eine bessere Leistung als reguläre Ausdrücke. Zum Beispiel ist das Folgende ein unstrukturierter Textausdruck:

```
HTTP.REQ.HEADER("Example").AFTER_STR("more")
```

Der vorherige Ausdruck würde im Allgemeinen eine bessere Leistung bieten als das folgende Äquivalent, bei dem ein regulärer Ausdruck verwendet wird:

```
HTTP.REQ.HEADER("Example").AFTER_REGEX(re/more/)
```

Weitere Informationen zu regulären Ausdrücken finden Sie unter Reguläre Ausdrücke.

Ausdruckspräfixe für Text in HTTP-Anfragen und Antworten

May 11, 2023

Eine HTTP-Anforderung oder -Antwort enthält typischerweise Text, z. B. in Form von Headern, Header-Werten, URLs und POST-Haupttext. Sie können Ausdrücke so konfigurieren, dass sie mit einem oder mehreren dieser textbasierten Elemente in einer HTTP-Anforderung oder -Antwort arbeiten.

Weitere Informationen zu Parametern finden Sie unter Referenz zum erweiterten Richtlinienausdruck von NetScaler.

In den folgenden Themen finden Sie weitere Informationen zur Konfiguration mit erweitertem Ausdruck.

- Zusammengesetzte erweiterte Richtlinienausdrücke
- Erweiterte Richtlinienausdrücke: IP- und MAC-Adressen, Durchsatz, VLAN-IDs
- Erweiterte Richtlinienausdrücke: SSL parsen
- Erweiterte Richtlinienausdrücke: Arbeiten mit Datum, Uhrzeit und Zahlen
- Grundelemente eines erweiterten Richtlinienausdrucks
- Erweiterte Richtlinienausdrücke: Text auswerten
- Erweiterte Richtlinienausdrücke: Parsen von HTTP-, TCP- und UDP-Daten
- Zusammenfassende Beispiele für Standard-Syntaxausdrücke und Richtlinien

Ausdruckspräfixe für VPNs und clientlose VPNs

August 19, 2021

Das erweiterte Richtlinienmodul enthält Präfixe, die spezifisch für das Parsen von VPN- oder clientlosen VPN-Daten sind. Diese Daten umfassen Folgendes:

- Hostnamen, Domänen und URLs im VPN-Datenverkehr.
- Protokolle im VPN-Datenverkehr.
- Abfragen im VPN-Datenverkehr.

Diese Textelemente sind oft URLs und Komponenten von URLs. Zusätzlich zum Anwenden der textbasierten Vorgänge auf diese Elemente können Sie diese Elemente mithilfe von Operationen analysieren, die für das Analysieren von URLs spezifisch sind. Weitere Informationen finden Sie unter Ausdrücke zum Extrahieren von URL-Segmenten

Informationen zu VPN-Ausdruckspräfixen finden Sie unter VPN-Ausdruckstabelle.

Grundlegende Operationen auf Text

October 8, 2021

Zu den grundlegenden Operationen für Text gehören Operationen für den Zeichenfolgenabgleich, das Berechnen der Länge einer Zeichenfolge und das Steuern der Groß- und Kleinschreibung. Sie können Leerzeichen in eine Zeichenfolge aufnehmen, die als Argument an einen Ausdruck übergeben wird, aber die Zeichenfolge darf 255 Zeichen nicht überschreiten.

String-Vergleichsfunktionen

In der folgenden Tabelle sind grundlegende Zeichenfolgenabgleichsoperationen aufgeführt, bei denen die Funktionen ein boolesches TRUE oder FALSE zurückgeben.

Funktion	Beschreibung
`<text>.CONTAINS(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Ziel enthält `<string>`. Beispiel:`http.req.url.contains(".jpeg")`
`<text>.EQ(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Ziel exakt mit übereinstimmt `<string>`. Beispielsweise gibt der folgende Ausdruck ein boolesches TRUE für eine URL mit dem Hostnamen “myhostabc” zurück: `http.req.url.hostname.eq("myhostabc")`
`<text>.STARTSWITH(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Ziel mit beginnt `<string>`. Beispielsweise gibt der folgende Ausdruck ein boolesches TRUE für eine URL mit dem Hostnamen “myhostabc” zurück: `http.req.url.hostname.startswith("myhost")`
`<text>.ENDSWITH(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Ziel mit endet<string>. Beispielsweise gibt der folgende Ausdruck ein boolesches TRUE für eine URL mit dem Hostnamen “myhostabc” zurück: `http.req.url.hostname.endswith("abc")`

Funktion	Beschreibung
`<text>.NE(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix nicht dem Zeichenfolgenargument entspricht. Wenn das Präfix einen Wert ohne Zeichenfolge zurückgibt, wird das Argument Funktion mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Werts verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)or SET_TEXT_MODE(NOIGNORECASE)`und mit ASCII- und UTF-8-Zeichensätzen verwenden.
`<text>.GT(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch größer als das Zeichenfolgenargument ist. Wenn das Präfix einen Wert ohne Zeichenfolge zurückgibt, wird das Argument Funktion mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Werts verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)` und sowohl mit ASCII- als auch mit UTF-8-Zeichensätzen verwenden.
`<text>.GE(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch größer oder gleich dem String-Argument ist. Wenn das Präfix einen Wert ohne Zeichenfolge zurückgibt, wird das Argument Funktion mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Werts verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)` und sowohl mit ASCII- als auch mit UTF-8-Zeichensätzen verwenden.

Funktion	Beschreibung
`<text>.LT(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch kleiner als das Zeichenfolgenargument ist. Wenn das Präfix einen Wert ohne Zeichenfolge zurückgibt, wird das Argument Funktion mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Werts verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)` und sowohl mit ASCII- als auch mit UTF-8-Zeichensätzen verwenden.
`<text>.LE(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch kleiner oder gleich dem String-Argument ist. Wenn das Präfix einen Wert ohne Zeichenfolge zurückgibt, wird das Argument Funktion mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Werts verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)` und sowohl mit ASCII- als auch mit UTF-8-Zeichensätzen verwenden.

Berechnen Sie die Länge einer Zeichenfolge

Die Operation `<text>.LENGTH` gibt einen numerischen Wert zurück, der der Anzahl der Zeichen (nicht Byte) in einer Zeichenfolge entspricht:

```
<text>.LENGTH
```

Beispielsweise möchten Sie möglicherweise Anforderungs-URLs identifizieren, die eine bestimmte Länge überschreiten. Es folgt ein Ausdruck, der dieses Beispiel implementiert:

```
HTTP.REQ.URL.LENGTH < 500
```

Nachdem Sie die Zeichen oder Elemente in einer Zeichenfolge gezählt haben, können Sie numerische Operationen darauf anwenden. Weitere Informationen finden Sie unter Erweiterte Richtlinienaus-

drücke: Arbeiten mit Daten, Zeiten und Zahlen.

Betrachten, ignorieren und Ändern von Groß- und Kleinschreibung

Die folgenden Funktionen arbeiten für die Groß-/Kleinschreibung (Groß- oder Kleinschreibung) der Zeichen in der Zeichenfolge.

Funktion	Beschreibung	
`<text>.SET_TEXT_MODE` (IGNORECASE	NOIGNORECASE)	Diese Funktion schaltet die Groß- und Kleinschreibung für alle Textoperationen ein oder aus.
`<text>.TO_LOWER`	Wandelt das Ziel für einen Textblock von bis zu 2 Kilobyte (KB) in Kleinbuchstaben um. Gibt UNDEF zurück, wenn das Ziel 2 KB überschreitet. For example, the string “ABCd:” is converted to “abcd:”.	
`<text>.TO_UPPER`	Converts the target to uppercase. Gibt UNDEF zurück, wenn das Ziel 2 KB überschreitet. For example, the string “abcD:” is converted to “ABCD:”.	

Entfernt bestimmte Zeichen aus einer Zeichenfolge

Sie können die Funktion STRIP_CHARS (`<string>`) verwenden, um bestimmte Zeichen aus dem Text zu entfernen, der von einem Präfix für erweiterte Richtlinienausdrücke (die Eingabezeichenfolge) zurückgegeben wird. Alle Instanzen der Zeichen, die Sie im Argument angeben, werden aus der Eingabezeichenfolge entfernt. Sie können eine beliebige Textmethode für die resultierende Zeichenfolge verwenden, einschließlich der Methoden, die zum Abgleichen der Zeichenfolge mit einem Mustersatz verwendet werden.

Beispielsweise entfernt die Funktion `STRIP\\_CHARS(<string>)` im Ausdruck `CLIENT.UDP.DNS.DOMAIN.STRIP\\_CHARS(".-\\_")` alle Punkte (.) , Bindestriche (-) und Unterstriche (_) vom Domainnamen, der durch das Präfix CLIENT.UDP.DNS.DOMAIN zurückgegeben wird. Wenn der zurück-

gegebene Domainname “ein.dom_ai_n-name” lautet, gibt die Funktion den String “adomainname” zurück.

Im folgenden Beispiel wird die resultierende Zeichenfolge mit einem Mustersatz namens “listofdomains” verglichen:

```
CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS(".-_").CONTAINS_ANY("listofdomains")
```

Hinweis: Sie können die Zeichenfolge, die von der Funktion `STRIP_CHARS(<string>)` zurückgegeben wird, nicht neu schreiben.

Die folgenden Funktionen entfernen übereinstimmende Zeichen vom Anfang und Ende einer bestimmten Zeichenfolgeneingabe.

Funktion	Beschreibung
`<text>.STRIP_START_CHARS(s)`	Entfernet übereinstimmende Zeichen vom Anfang der Eingabezeichenfolge, bis das erste nicht übereinstimmende Zeichen gefunden wird, und gibt den Rest der Zeichenfolge zurück. Sie müssen die Zeichen, die Sie entfernen möchten, als einzelne Zeichenfolge in Anführungszeichen angeben. Wenn der Name eines Headers beispielsweise TestLang lautet und:*/en_us:sein Wert ist, entfernt HTTP.RES.HEADER (“TestLang”) .STRIP_START_CHARS (“:”)* die angegebenen Zeichen vom Anfang des Wertes des Headers, bis das erste nicht übereinstimmende Zeichen e gefunden wird und zurückgeben_us: als Zeichenfolge.

Funktion	Beschreibung
<text>.STRIP_END_CHARS (s)	Entfernet übereinstimmende Zeichen vom Ende der Eingabezeichenfolge bis zum ersten nicht übereinstimmenden Zeichen und gibt den Rest der Zeichenfolge zurück. Sie müssen die Zeichen, die Sie entfernen möchten, als einzelne Zeichenfolge in Anführungszeichen angeben. Wenn der Name eines Headers beispielsweise TestLang lautet und:/*en_us:sein Wert ist, entfernt HTTP.RES.HEADER (“TestLang”) .STRIP_START_CHARS (“:*”) die angegebenen Zeichen vom Ende des Werts des Headers, bis die ersten nicht übereinstimmenden Zeichen gefunden werden und gibt: /_en_us als Zeichenfolge zurück.

Hängen Sie eine Zeichenfolge an eine andere Zeichenfolge

Sie können die Funktion APPEND () verwenden, um die Zeichenfolgendarstellung des Arguments an die Zeichenfolgendarstellung des von der vorhergehenden Funktion zurückgegebenen Werts anzuhängen. Die vorhergehende Funktion kann eine sein, die eine Zahl, einen vorzeichenlosen Long, Double, einen Zeitwert, eine IPv4-Adresse oder eine IPv6-Adresse zurückgibt. Das Argument kann eine Textzeichenfolge, eine Zahl, eine vorzeichenlose Long-, Double-, Zeitwert-, IPv4-Adresse oder IPv6-Adresse sein. Der resultierende Zeichenfolgenwert ist derselbe Zeichenfolgenwert, der mit dem Operator + erhalten wird.

Komplexe Operationen an Text

May 11, 2023

Zusätzlich zum einfachen Zeichenfolgenabgleich können Sie Ausdrücke konfigurieren, die die Zeichenfolgenlänge und den Textblock auf Muster statt auf bestimmte Zeichenfolgen untersuchen.

Beachten Sie bei jeder textbasierten Operation Folgendes:

- Für jede Operation, die ein Zeichenfolgenargument akzeptiert, darf die Zeichenfolge 255 Zeichen nicht überschreiten.
- Sie können Leerraum einschließen, wenn Sie eine Zeichenfolge in einen Ausdruck angeben.

Operationen an der Länge einer Zeichenfolge

Die folgenden Operationen extrahieren Zeichenfolgen nach einer Zeichenanzahl.

Zeichenzähler-Operation	Beschreibung
`<text>.TRUNCATE(<count>)`	Gibt eine Zeichenfolge zurück, nachdem das Ende des Ziels um die Anzahl der Zeichen in abgeschnitten wurde `<count>`. Wenn die gesamte Zeichenfolge kürzer als ist `<count>`, wird nichts zurückgegeben.
`<text>.TRUNCATE(<character>, <count>)`	Gibt eine Zeichenfolge zurück, nachdem der Text nach `<character>` um die in `<count>` angegebene Anzahl von Zeichen abgeschnitten wurde.
`<text>.PREFIX(<character>, <count>)`	Wählt das längste Präfix im Ziel aus, das höchstens `<count>` Vorkommen von `<character>` hat.
`<text>.SUFFIX(<character>, <count>)`	Wählt das längste Suffix im Ziel aus, das höchstens `<count>` Vorkommen von `<character>` hat. Betrachten Sie beispielsweise den folgenden Antworttext: `peninsula`. Der folgende Ausdruck gibt den Wert `sula: http.res.body(100).suffix('n',0)` zurück. Der folgende Ausdruck gibt `insula: http.res.body(100).suffix('n',1)` zurück. Der folgende Ausdruck gibt den Wert `peninsula: http.res.body(100).suffix('n',2)` zurück. Der folgende Ausdruck gibt den Wert `peninsula: http.res.body(100).suffix('n',3)` zurück.
`<text>.SUBSTR(<starting_offset>, <length>)`	Wählen Sie eine Zeichenfolge mit der `<length>`Anzahl von Zeichen aus dem Zielobjekt aus. Beginne mit dem Extrahieren der Zeichenfolge nach dem `<starting_offset>`. Wenn die Anzahl der Zeichen nach dem Offset unter dem Wert des Arguments `<length>` liegt, wählen Sie alle verbleibenden Zeichen aus.

Zeichenzähler-Operation	Beschreibung
`<text>.SKIP(<character>, <count>)`	Wählen Sie eine Zeichenfolge aus dem Ziel aus, nachdem Sie das längste Präfix übersprungen haben, das höchstens `<count>` Vorkommen von `<character>` hat.

Operationen für einen Teil einer Zeichenfolge

In der Tabelle String-Operationen erfahren Sie, wie Sie eine Teilmenge einer größeren Zeichenfolge extrahieren, indem Sie eine der Operationen verwenden.

Operationen zum Vergleich der alphanumerischen Reihenfolge zweier Strings

Die COMPARE-Operation untersucht das erste nicht übereinstimmende Zeichen zweier verschiedener Zeichenfolgen. Diese Operation basiert auf der lexikografischen Reihenfolge, die bei der Bestellung von Begriffen in Wörterbüchern verwendet wird.

Diese Operation gibt die arithmetische Differenz zwischen den ASCII-Werten der ersten nicht übereinstimmenden Zeichen in den verglichenen Zeichenfolgen zurück. Die folgenden Unterschiede sind Beispiele:

- Der Unterschied zwischen “abc” und “und” ist -1 (basierend auf dem dritten paarweisen Zeichenvergleich).
- Der Unterschied zwischen “@” und “abc” beträgt -33.
- Der Unterschied zwischen “1” und “abc” beträgt -47.

Es folgt die Syntax für die COMPARE-Operation.

```
<text>.COMPARE(<string>)
```

Extrahieren einer Ganzzahl aus einer Zeichenfolge von Bytes, die Text darstellen

In der Integer-Extraktionstabelle erfahren Sie, wie Sie eine Bytezeichenfolge behandeln, die Text als eine Folge von Bytes darstellt, 8 Bit, 16 Bit oder 32 Bit aus der Sequenz extrahiert und dann die extrahierten Bits in eine Ganzzahl konvertiert.

Konvertieren von Text in einen Hash-Wert

Sie können eine Textzeichenfolge mithilfe der HASH-Funktion in einen Hash-Wert konvertieren. Diese Funktion gibt als Ergebnis der Operation eine positive 31-Bit-Ganzzahl zurück. Es folgt das Format des Ausdrucks:

<text>.HASH

Diese Funktion ignoriert Groß- und Leerräume. Beispielsweise würden die beiden Zeichenfolgen Ab c und bc nach der Operation denselben Hash-Wert erzeugen.

Kodieren und dekodieren Sie Text durch Anwenden des Base64-Codierungsalgorithmus

Die folgenden beiden Funktionen codieren und dekodieren eine Textzeichenfolge, indem sie den Base64-Codierungsalgorithmus anwenden.

Funktion	Beschreibung
text.B64ENCODE	Kodiert die Textzeichenfolge (durch Text gekennzeichnet) durch Anwendung des Base64-Codierungsalgorithmus.
text.B64DECODE	Dekodiert die Base64-codierte Zeichenfolge (durch Text gekennzeichnet) durch Anwendung des Base64-Decodierungsalgorithmus. Die Operation löst ein UNDEF aus, wenn Text nicht im B64-codierten Format vorliegt.

Verfeinern Sie die Suche in einer Rewrite-Aktion mithilfe der Funktion EXTEND

Die Funktion EXTEND wird in Rewrite-Aktionen verwendet, die Muster oder Mustersätze angeben und auf die Körper von HTTP-Paketen abzielen. Wenn eine Musterübereinstimmung gefunden wird, erweitert die Funktion EXTEND den Suchbereich um eine vordefinierte Anzahl von Byte auf beiden Seiten der übereinstimmenden Zeichenfolge. Ein regulärer Ausdruck kann dann verwendet werden, um Übereinstimmungen in dieser erweiterten Region neu zu schreiben. Rewrite-Aktionen, die mit der Funktion EXTEND konfiguriert sind, führen Rewrites schneller durch als Rewrite-Aktionen, bei denen ganze HTTP-Bodies nur mit regulären Ausdrücken ausgewertet werden.

Das Format der EXTEND-Funktion ist EXTEND (m, n), wobei m und n die Anzahl der Byte sind, um die der Umfang der Suche vor bzw. nach dem übereinstimmenden Muster erweitert wird. Wenn eine Übereinstimmung gefunden wird, umfasst der neue Suchbereich m Byte, die unmittelbar vor der übereinstimmenden Zeichenfolge stehen, die Zeichenfolge selbst und die n Byte, die der Zeichenfolge folgen. Ein regulärer Ausdruck kann dann verwendet werden, um einen Teil dieser neuen Zeichenfolge neu zu schreiben.

Die Funktion EXTEND kann nur verwendet werden, wenn die Rewrite-Aktion , in der sie verwendet wird, die folgenden Anforderungen erfüllt:

- Die Suche erfolgt mithilfe von Mustern oder Mustersätzen (keine regulären Ausdrücke)
- Die Rewriteaktion wertet nur die Körper von HTTP-Paketen aus.

Außerdem kann die Funktion EXTEND nur mit den folgenden Arten von Rewrite-Aktionen verwendet werden:

- replace_all
- insert_after_all
- delete_all
- insert_before_all

Beispielsweise möchten Sie möglicherweise alle Instanzen von “” undhttp://exampleurl.com/“http://exampleurl.au/” in den ersten 1000 Byte des Körpers löschen. Zu diesem Zweck können Sie eine Rewriteaktion konfigurieren, um nach allen Instanzen der Zeichenfolge exampleurl zu suchen, den Suchbereich auf beiden Seiten der Zeichenfolge zu erweitern, wenn eine Übereinstimmung gefunden wird, und dann einen regulären Ausdruck verwenden, um das Rewrite in der erweiterten Region durchzuführen. Das folgende Beispiel erweitert den Umfang der Suche um 20 Byte nach links und 50 Byte rechts von der übereinstimmenden Zeichenfolge:

```
add rewrite action delurl_example delete_all 'HTTP.REQ.BODY(1000)'-search
exampleurl -refineSearch 'extend(20,50).regex_select(re##http://exampleurl
.(com|au)##)'
```

Konvertieren von Text in Hexadezimalformat

Die folgende Funktion wandelt Text in das Hexadezimalformat um und extrahiert die resultierende Zeichenfolge:

```
<text>.BLOB_TO_HEX(<string>)
```

Zum Beispiel wandelt diese Funktion die Bytezeichenfolge “abc” in “61:62:63” um.

Verschlüsseln und Entschlüsseln von Text

In erweiterten Richtlinienausdrücken können Sie die Funktionen ENCRYPT und DECRYPT verwenden, um Text zu verschlüsseln und zu entschlüsseln. Daten, die von der ENCRYPT-Funktion auf einer bestimmten NetScaler-Appliance oder einem Hochverfügbarkeitspaar (HA) verschlüsselt wurden, sind für die Entschlüsselung durch die DECRYPT-Funktion auf derselben NetScaler-Appliance oder demselben HA-Paar vorgesehen. Die Appliance unterstützt die Verschlüsselungsmethoden RC4, DES3, AES128, AES192 und AES256. Der für die Verschlüsselung erforderliche Schlüsselwert ist nicht vom Benutzer spezifizierbar. Wenn eine Verschlüsselungsmethode festgelegt ist, generiert die Appliance automatisch einen zufälligen Schlüsselwert, der für die angegebene Methode geeignet ist. Die Standardmethode ist die AES256-Verschlüsselung, die die sicherste und von Citrix empfohlene Verschlüsselungsmethode ist.

Sie müssen die Verschlüsselung nicht konfigurieren, es sei denn, Sie möchten die Verschlüsselungsmethode ändern oder die Appliance soll einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode generieren.

Hinweis: Sie können auch XML-Nutzlasten verschlüsseln und entschlüsseln. Informationen zu den Funktionen zum Verschlüsseln und Entschlüsseln von XML-Nutzlasten finden Sie unter Verschlüsseln und Entschlüsseln von XML-Nutzlasten.

Verschlüsselung konfigurieren

Während des Starts führt die Appliance den Befehl set ns EncryptionParams mit standardmäßig der AES256-Verschlüsselungsmethode aus und verwendet einen zufällig generierten Schlüsselwert, der für die AES256-Verschlüsselung geeignet ist. Die Appliance verschlüsselt auch den Schlüsselwert und speichert den Befehl mit dem verschlüsselten Schlüsselwert in der NetScaler-Konfigurationsdatei. Daher ist die Verschlüsselungsmethode AES256 standardmäßig für die Funktionen ENCRYPT und DECRYPT aktiviert. Der Schlüsselwert, der in der Konfigurationsdatei gespeichert wird, bleibt bei Neustarts bestehen, obwohl die Appliance den Befehl bei jedem Neustart ausführt.

Sie können den Befehl set ns EncryptionParams manuell ausführen oder das Konfigurationsdienstprogramm verwenden, wenn Sie die Verschlüsselungsmethode ändern möchten oder wenn die Appliance einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode generieren soll. Um die CLI zum Ändern der Verschlüsselungsmethode zu verwenden, legen Sie nur den Methodenparameter fest, wie in “**Beispiel 1: Ändern der Verschlüsselungsmethode**gezeigt. “ Wenn Sie möchten, dass die Appliance einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode generiert, setzen Sie den Methodenparameter auf die aktuelle Verschlüsselungsmethode und den KeyValue-Parameter auf eine leere Zeichenfolge (“”), wie in “**Beispiel 2: Generieren eines neuen Schlüsselwerts für die aktuelle Verschlüsselungsmethode**gezeigt. “ Nachdem Sie einen neuen Schlüsselwert generiert haben, müssen Sie die Konfiguration speichern. Wenn Sie die Konfiguration nicht speichern, verwendet die Appliance den neu generierten Schlüsselwert nur bis zum nächsten Neustart, woraufhin sie auf den Schlüsselwert in der gespeicherten Konfiguration zurückkehrt.

Konfigurieren Sie die Verschlüsselung über die GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Bereich **Einstellungen** auf **Verschlüsselungsparameter ändern** .
3. Führen **Sie im Dialogfeld Verschlüsselungsparameter ändern** einen der folgenden Schritte aus:
    - Um die Verschlüsselungsmethode zu ändern, wählen Sie in der Liste Methode die gewünschte Verschlüsselungsmethode aus.
    - Um einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode zu generieren, klicken Sie auf Neuen Schlüssel für die ausgewählte Methode generieren.

4. Klicken Sie auf **OK**.

Verwenden Sie die Funktionen ENCRYPT und DECRYPT

Sie können die Funktionen ENCRYPT und DECRYPT mit jedem Ausdruck-Präfix verwenden, das Text zurückgibt. Beispielsweise können Sie die Funktionen ENCRYPT und DECRYPT in Rewriterichtlinien für die Cookie-Verschlüsselung verwenden. Im folgenden Beispiel verschlüsseln die Rewrite-Aktionen ein Cookie namens MyCookie, das von einem Back-End-Dienst gesetzt wird, und entschlüsseln dasselbe Cookie, wenn es von einem Client zurückgegeben wird:

```
1 add rewrite action my-cookie-encrypt-action replace "HTTP.RES.
    SET_COOKIE.COOKIE("MyCookie").VALUE(0)" "HTTP.RES.SET_COOKIE.COOKIE(
    "MyCookie").VALUE(0).ENCRYPT"
2
3 add rewrite action my-cookie-decrypt-action replace "HTTP.REQ.COOKIE.
    VALUE("MyCookie")" "HTTP.REQ.COOKIE.VALUE("MyCookie").DECRYPT"
4 <!--NeedCopy-->
```

Nachdem Sie Richtlinien für die Verschlüsselung und Entschlüsselung konfiguriert haben, speichern Sie die Konfiguration, um die Richtlinien in Kraft zu setzen.

Konfiguration des Verschlüsselungsschlüssels für die Verschlüsselung

In erweiterten Richtlinienausdrücken können Sie die Funktionen ENCRYPT und DECRYPT zum Verschlüsseln und Entschlüsseln von Text in einer Anfrage oder Antwort verwenden. Die von der ENCRYPT-Funktion auf einer Appliance verschlüsselten Daten (Standalone, Hochverfügbarkeit oder Cluster) sollen von derselben Appliance durch die DECRYPT-Funktion entschlüsselt werden. Die Appliance unterstützt die Verschlüsselungsmethoden RC4, DES, Triple-DES, AES92 und AES256, und jede dieser Methoden verwendet einen geheimen Schlüssel für die Verschlüsselung und Entschlüsselung von Daten. Sie können jede dieser Methoden verwenden, um Daten auf zwei Arten zu verschlüsseln und zu entschlüsseln - Selbstverschlüsselung und Verschlüsselung durch Dritte.

Die Selbstverschlüsselungsfunktion in einer Appliance (Standalone, Hochverfügbarkeit oder Cluster) verschlüsselt und entschlüsselt Daten durch Auswertung des Header-Werts. Ein Beispiel, um dies zu verstehen, ist die HTTP-Cookie-Verschlüsselung. Der Ausdruck wertet den Header aus, verschlüsselt den HTTP-Cookie-Wert im Set-Cookie-Header in der ausgehenden Antwort und entschlüsselt dann den Cookie-Wert, wenn er im Cookie-Header einer nachfolgenden eingehenden Anforderung des Clients zurückgegeben wird. Der Schlüsselwert ist nicht vom Benutzer konfigurierbar. Wenn stattdessen eine Verschlüsselungsmethode im Befehl set ns EncryptionParams konfiguriert ist, generiert die Appliance automatisch einen zufälligen Schlüsselwert für die konfigurierte Methode. Standardmäßig verwendet der Befehl die Verschlüsselungsmethode AES256, die die hochsichere Methode ist, und Citrix empfiehlt diese Methode.

Die Verschlüsselungsfunktion eines Drittanbieters verschlüsselt oder entschlüsselt Daten mit einer Drittanbieteranwendung. Beispielsweise kann ein Client Daten in einer Anforderung verschlüsseln und die Appliance entschlüsselt die Daten, bevor sie an den Back-End-Server gesendet werden oder umgekehrt. Um dies durchzuführen, müssen die Appliance und die Drittanbieteranwendung einen geheimen Schlüssel gemeinsam nutzen. Auf der Appliance können Sie den geheimen Schlüssel direkt mithilfe eines Verschlüsselungsschlüsselobjekts konfigurieren, und der Schlüsselwert wird automatisch von der Appliance für eine stärkere Verschlüsselung generiert. Derselbe Schlüssel wird manuell auf der Appliance eines Drittanbieters konfiguriert, sodass sowohl Appliance als auch Drittanbieteranwendungen denselben Schlüssel zum Verschlüsseln und Entschlüsseln von Daten verwenden können.

Hinweis: Mithilfe der Verschlüsselung von Drittanbietern können Sie auch XML-Nutzdaten verschlüsseln und entschlüsseln. Informationen zu den Funktionen zum Verschlüsseln und Entschlüsseln von XML-Nutzdaten finden Sie unter “Verschlüsseln und Entschlüsseln von XML-Nutzlasten.

Verschlüsselungsmethoden

Eine Verschlüsselungsmethode bietet zwei Funktionen: eine Verschlüsselungsfunktion, die eine Klartext-Bytesequenz in eine Chiffretext-Bytesequenz umwandelt, und eine Entschlüsselungsfunktion, die den Chiffretext zurück in den Klartext umwandelt. Verschlüsselungsmethoden verwenden Bytesequenzen, die als Schlüssel bezeichnet werden, um Verschlüsselung und Entschlüsselung durchzuführen. Verschlüsselungsmethoden, die denselben Schlüssel für die Verschlüsselung und Entschlüsselung verwenden, werden als symmetrisch bezeichnet. Verschlüsselungsmethoden, die unterschiedliche Schlüssel für die Verschlüsselung und Entschlüsselung verwenden, sind asymmetrisch. Die bemerkenswertesten Beispiele für asymmetrische Verschlüsselungen sind die Kryptographie mit öffentlichen Schlüsseln, bei der ein öffentlicher Schlüssel verwendet wird, der jedem zur Verschlüsselung zur Verfügung steht, und einen privaten Schlüssel, der nur dem Entschlüsseler bekannt ist.

Eine gute Verschlüsselungsmethode macht es unmöglich, Chiffretext zu entschlüsseln (“knacken”), wenn Sie den Schlüssel nicht besitzen. “Unmachbar” bedeutet wirklich, dass das Knacken des Verschlüsselungstextes mehr Zeit und Rechenressourcen in Anspruch nehmen würde, als es wert ist. Wenn Computer leistungsfähiger und billiger werden, werden Verschlüsselungen, die früher nicht geknackt werden konnten, praktikabler. Im Laufe der Zeit werden auch Fehler in Verschlüsselungsmethoden (oder deren Implementierungen) festgestellt, die das Knacken erleichtern. Neuere Verschlüsselungsmethoden werden daher älteren vorgezogen. Im Allgemeinen bieten Schlüssel mit längerer Länge eine bessere Sicherheit als kürzere Schlüssel, auf Kosten längerer Verschlüsselungs- und Entschlüsselungszeiten.

Eine Verschlüsselungsmethode kann Stream-Chiffren oder Blockchiffren verwenden. RC4 ist die meist gesicherte Stream-Chiffrers und wird nur für Legacy-Anwendungen verwendet. Blockchiffren können Polsterung enthalten.

Stream-Chiffren

Eine Stream-Verschlüsselungsmethode arbeitet mit einzelnen Bytes. Auf NetScaler -Appliances ist nur eine Stream-Verschlüsselung verfügbar: RC4, das eine Schlüssellänge von 128 Bit (16 Byte) verwendet. Für einen bestimmten Schlüssel generiert RC4 eine pseudozufällige Bytefolge, rufen Sie einen Keystream auf, der mit dem Klartext X-ored ist, um den Chiffretext zu erzeugen. RC4 gilt nicht mehr als sicher und sollte nur verwendet werden, wenn dies von älteren Anwendungen erforderlich ist.

Blockchiffren

Eine Blockchiffrierungsmethode arbeitet mit einem festen Byte-Block. Eine NetScaler-Appliance bietet zwei Blockchiffren: Data Encryption Standard (DES) und den Advanced Encryption Standard (AES). DES verwendet eine Blockgröße von 8 Byte und (auf einer NetScaler-Appliance) zwei Optionen für die Schlüssellänge: 64 Bit (8 Byte), von denen 56 Bit Daten und 8 Bit Parität sind, und Triple-DES, eine Schlüssellänge von 192 Bit (24 Byte). AES hat eine Blockgröße von 16 Byte und (auf NetScaler) drei Möglichkeiten für die Schlüssellänge: 128 Bit (16 Byte), 192 Bit (24 Byte) und 256 Bit (32 Byte).

Padding

Wenn der Klartext für eine Blockchiffre keine ganzzahlige Anzahl von Blöcken ist, kann das Auffüllen mit mehr Bytes erforderlich sein. Angenommen, der Klartext lautet “xyzzy” (Hex 78797a7a79). Für einen 8-Byte-Triple-DES-Block müsste dieser Wert aufgefüllt werden, um 8 Byte zu erzeugen. Das Füllschema muss es der Entschlüsselungsfunktion ermöglichen, die Länge des ursprünglichen Klartextes nach der Entschlüsselung zu bestimmen. Im Folgenden sind einige derzeit verwendete Füllschemata aufgeführt (n ist die Anzahl der hinzugefügten Byte):

- PKCS7: Addiert jeweils n Byte Wert. Zum Beispiel 78797a7a79030303. Dies ist das Füllschema, das von der Richtlinienfunktion OpenSSL und ENCRYPT () verwendet wird. Das PKCS5-Polsterschema ist dasselbe wie bei PKCS7.
- ANSI X.923: Addiert n-1 Nullbyte und ein letztes Byte des Wertes n. Zum Beispiel 78797a7a79000003.
- ISO 10126: Addiert n-1 zufällige Byte und ein letztes Byte des Wertes n. Zum Beispiel 78797a7a79xxxx03, wobei xx ein beliebiger Bytewert sein kann. Die Richtlinienfunktion DECRYPT () akzeptiert dieses Füllschema, das es ihr auch ermöglicht, die Schemata PKCS7 und ANSI X.923 zu akzeptieren.
- ISO/IEC 7816-4: Fügt ein 0x80 Byte und n-1 Nullbyte hinzu. Zum Beispiel 78797a7a79800000. Dies wird auch OneAndZeros-Polsterung genannt.
- Null: Fügt n Nullbyte hinzu. Beispiel: 78797a7a79000000. Dies kann nur mit Klartext verwendet werden, der keine NUL-Bytes enthält.

Wenn eine Füllung verwendet wird und der Klartext eine ganzzahlige Anzahl von Blöcken ist, wird normalerweise ein zusätzlicher Block hinzugefügt, damit die Entschlüsselungsfunktion die

ursprüngliche Klartext-Länge eindeutig bestimmen kann. Für PCKS7 und 8-Byte-Block wäre dies 0808080808080808.

Betriebsmodi

Es gibt eine Reihe verschiedener Betriebsmodi für Blockchiffren, die angeben, wie mehrere Klartext-Blöcke verschlüsselt werden. Einige Modi verwenden einen Initialisierungsvektor (IV), einen Datenblock außer dem Klartext, der zum Starten des Verschlüsselungsprozesses verwendet wird. Es empfiehlt sich, für jede Verschlüsselung eine andere IV zu verwenden, damit derselbe Klartext einen anderen Chiffretext erzeugt. Die IV muss nicht geheim sein und wird daher dem Chiffretext vorangestellt. Zu den Modi gehören:

- Elektronisches Codebuch (EZB): Jeder Klartext-Block wird unabhängig verschlüsselt. Eine IV wird nicht verwendet. Das Auffüllen ist erforderlich, wenn der Klartext kein Vielfaches der Verschlüsselungsblockgröße ist. Derselbe Klartext und Schlüssel erzeugen immer denselben Chiffretext. Aus diesem Grund gilt die EZB als weniger sicher als andere Modi und sollte nur für Legacy-Anwendungen verwendet werden.
- Cipher Block Chaining (CBC): Jeder Klartextblock wird mit dem vorherigen Chiffretext-Block oder der IV für den ersten Block xored, bevor er verschlüsselt wird. Das Auffüllen ist erforderlich, wenn der Klartext kein Vielfaches der Verschlüsselungsblockgröße ist. Dies ist der Modus, der mit der NetScaler EncryptionParams-Methode verwendet wird.
- Verschlüsselungsfeedback (CFB): Der vorherige Chiffretextblock oder die IV für den ersten Block wird verschlüsselt und die Ausgabe wird mit dem aktuellen Klartext-Block XORed, um den aktuellen Chiffretext-Block zu erstellen. Die Rückkopplung kann 1 Bit, 8 Bit oder 128 Bit betragen. Da der Klartext mit dem Chiffretext XORed ist, ist kein Auffüllen erforderlich.
- Ausgabe-Feedback (OFB): Ein Keystream wird generiert, indem die Chiffre nacheinander auf die IV angewendet wird und die Keystream-Blöcke mit dem Klartext XORing. Eine Polsterung ist nicht erforderlich.

Konfigurieren von Verschlüsselungsschlüsseln für die Verschlüsselung

Im Folgenden werden die Konfigurationsaufgaben aufgeführt, die bei der Konfiguration des Verschlüsselungsschlüssels ausgeführt

1. Hinzufügen eines Verschlüsselungsschlüssels. Konfiguriert einen Verschlüsselungsschlüssel für eine angegebene Verschlüsselungsmethode mit einem bestimmten Schlüsselwert.
2. Änderung eines Verschlüsselungsschlüssels. Sie können Parameter für einen konfigurierten Verschlüsselungsschlüssel bearbeiten.
3. Einen Verschlüsselungsschlüssel aufheben. Setzt Parameter für einen konfigurierten Verschlüsselungsschlüssel auf ihre Standardwerte. Ein EncryptionKey-Wert mit dem Namen muss existieren. Setzt das Auffüllen auf DEFAULT (bestimmt durch die Methode), Löscht eine vorhan-

dene IV, wodurch ENCRYPT () eine zufällige IV generiert. Löscht einen vorhandenen Kommentar. Die Methode und der Schlüsselwert können nicht zurückgesetzt werden.

4. Einen Verschlüsselungsschlüssel entfernen. Löscht einen konfigurierten Verschlüsselungsschlüssel. Der Schlüssel kann keine Referenzen haben.
5. Zeigt einen Verschlüsselungsschlüssel an. Zeigt Parameter für den konfigurierten Verschlüsselungsschlüssel oder alle konfigurierten Schlüssel an. Wenn der Name weggelassen wird, wird der Schlüsselwert nicht angezeigt.

Fügen Sie über die CLI einen Verschlüsselungsschlüssel hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns encryptionKey <name> -method <method> [-keyValue <keyvalue>][-
padding (OFF | ON)] [-iv <hexstring>] -keyValue <keyvalue> [-comment <
string>]
```

Hierbei gilt:

```
<method> = ( NONE | RC4 | DES3 | AES128 | AES192 | AES256 | DES | DES-
    CBC | DES-CFB | DES-OFB | DES-ECB | DES3-CBC | DES3-CFB | DES3-OFB |
     DES3-ECB | AES128-CBC | AES128-CFB | AES128-OFB | AES128-ECB |
    AES192-CBC | AES192-CFB | AES192-OFB | AES192-ECB | AES256-CBC |
    AES256-CFB | AES256-OFB | AES256-ECB ) <hexstring> = hex-encoded
    byte sequence
<!--NeedCopy-->
```

Die obigen Verschlüsselungsmethoden spezifizieren den Betriebsmodus mit CBC als Standardbetriebsmodus. Daher entsprechen die Methoden DES, DES2, AES128, AES192 und AES256 den Methoden DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC und AES256-CBC.

Ändern eines Verschlüsselungsschlüssels über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns encryptionKey <name> [-method <method>] [-keyValue <keyvalue>] [-
padding ( OFF | ON )] [-iv <string>] [-comment <string>]
```

Einen Verschlüsselungsschlüssel über die CLI aufheben

Geben Sie in der Befehlszeile Folgendes ein:

```
unset ns encryptionKey <name> [-padding] [-iv] [-comment]
```


Entfernen Sie einen Verschlüsselungsschlüssel über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
rm ns encryptionKey <name>
```

Zeigen Sie einen Verschlüsselungsschlüssel über die CLI an

Geben Sie in der Befehlszeile Folgendes ein:

Beispiel:

```
show ns encryptionKey [<name>]

add ns encryptionKey my_key -method aes256 -keyValue 26
    ea5537b7e0746089476e5658f9327c0b10c3b4778c673a5b38cee182874711 -iv
    c2bf0b2e15c15004d6b14bcdc7e5e365
set ns encryptionKey my_key -keyValue
    b8742b163abcf62d639837bbee3cef9fb5842d82d00dfe6548831d2bd1d93476
unset ns encryptionKey my_key -iv
rm ns encryptionKey my_key
show ns encryptionKey my_key
Name: my_key
Method: AES256
Padding: DEFAULT
Key Value: (not disclosed)
<!--NeedCopy-->
```

Fügen Sie über die GUI einen Verschlüsselungsschlüssel hinzu

Navigieren Sie zu **System** > **Verschlüsselungsschlüssel** und klicken Sie auf **Hinzufügen**, um einen Verschlüsselungsschlüssel zu erstellen.

Ändern Sie einen Verschlüsselungsschlüssel über die GUI

Navigieren Sie zu **System** > **Encryption Keys** und klicken Sie auf **Bearbeiten**, um Parameter für einen konfigurierten Verschlüsselungsschlüssel zu ändern.

Entfernen Sie einen Verschlüsselungsschlüssel über die GUI

Navigieren Sie zu **System** > **Verschlüsselungsschlüssel** und klicken Sie auf **Löschen**.

ENCRYPT- und DECRYPT-Funktionen für die Verschlüsselung von Drittanbietern

Es folgt die ENCRYPT-Funktion, die für die Verschlüsselung von Drittanbietern verwendet wird.

```
ENCRYPT (encryptionKey, out_encoding)
```

Hierbei gilt:

Eingabedaten für die Appliance sind der zu verschlüsselnde Text

EncryptionKey: Ein optionaler Zeichenfolgenparameter, der das konfigurierte Verschlüsselungsschlüsselobjekt zur Bereitstellung der Verschlüsselungsmethode, des geheimen Schlüsselwerts und anderer Verschlüsselungsparameter angibt. Wenn diese nicht angegeben wird, verwendet die Methode den automatisch generierten Schlüsselwert, der mit dem Befehl set ns EncryptionParams verknüpft ist.

out_encoding: Dieser Wert gibt an, wie die Ausgabe codiert wird. Wenn weggelassen, wird die BASE64-Codierung verwendet.

Eingabe:

```
BASE64: original PEM base64-encoding: 6 bits (0..63) encoded as one
    ASCII character:
                0..23 = 'A'..'Z', 24..51 = 'a'..'z', 52..61 = '0'..'9
                    ', 62 = '+', 63 = '/', '=' = pad byte.
    BASE64URL:  URL and Filename safe base64-encoding: same as BASE64
         except 62 = '-', 63 = '_'
    HEX_UPPER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
        '.
    HEX_LOWER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'a'..'f
        '.
    HEX_COLONS: Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
        '; ':' between each hex byte. Matches BLOB_TO_HEX() output
        format
    HEX:  For input, accepts HEX_UPPER, HEX_LOWER, and HEX_COLONS
        format. For output, produces HEX_LOWER format
<!--NeedCopy-->
```

Ausgabe: Die Ausgabe ist ein Text, der mit der angegebenen Methode und dem angegebenen Schlüssel verschlüsselt und mit einer bestimmten Ausgabecodierung codiert wurde. Es fügt eine generierte IV vor dem verschlüsselten Text für Blockmethoden und -modi ein, die eine IV erfordern, und entweder wird keine IV für den EncryptionKey angegeben oder der EncryptionKey wird weggelassen.

Es folgt die DECRYPT-Funktion, die für die Entschlüsselung durch Dritte verwendet wird.

```
DECRYPT(encryptionKey, in_encoding)
```

Hierbei gilt:

Eingabedaten sind ein verschlüsselter Text mit der angegebenen Methode und Schlüssel, der mit der angegebenen Eingabecodierung codiert ist. Es wird erwartet, dass dieser Text eine generierte IV enthält, bevor der verschlüsselte Text für Blockmethoden und -modi, die eine IV erfordern, und entweder wird keine IV für den EncryptionKey angegeben oder der EncryptionKey weggelassen wird.

encryptionKey — Ein optionaler Zeichenfolgenparameter, der das konfigurierte EncryptionKey-Objekt zur Bereitstellung der Verschlüsselungsmethode, des geheimen Schlüssels und anderer Verschlüsselungsparameter angibt. Wenn nicht angegeben, werden die Methode und der automatisch generierte Schlüssel verwendet, die mit der EncryptionParams-Einstellung verknüpft sind.

in_encoding — Ein optionaler Aufzählungsparameter, der angibt, wie die Eingabe voraussichtlich codiert wird. Die Werte entsprechen der out_encoding von ENCRYPT. Wenn es weggelassen wird, wird die BASE64-Codierung erwartet.

Die Ausgabedaten sind ein uncodierter entschlüsselter Text.

Varianten und optionale Parameter

Im Folgenden sind die Varianten dieser Funktionen mit den optionalen Parametern aufgeführt:

Variante	Beschreibung
ENCRYPT	Verwenden Sie den Befehl EncryptionParams und den Ausgabecodierungsparameter BASE64.
ENCRYPT(out_encoding)	Verwenden Sie EncryptionParams und den angegebenen Ausgabe-Kodierungsparameter.
ENCRYPT(encryptionKey)	Verwenden Sie den angegebenen EncryptionKey- und BASE64-Ausgabecodierungsparameter.
ENCRYPT(encryptionKey, out_encoding)	Verwenden Sie den angegebenen EncryptionKey und den Ausgabecodierungsparameter.
DECRYPT	Verwenden Sie den Befehl EncryptionParams und den BASE64-Eingabecodierungsparameter
DECRYPT(out_encoding)	Verwenden Sie den EncryptionParams-Befehl und den angegebenen Eingabecodierungsparameter.

Variante	Beschreibung
DECRYPT(encryptionKey)	Verwenden Sie den angegebenen EncryptionKey- und BASE64-Eingabecodierungsparameter
DECRYPT(encryptionKey, out_encoding)	Verwenden Sie den angegebenen EncryptionKey und den Eingabecodierungsparameter

Konfigurieren Sie HMAC-Schlüssel

NetScaler-Appliances unterstützen eine Funktion Hashed Message Authentication Code (HMAC), die eine Digest-Methode oder einen Hash von Eingabetext mithilfe eines geheimen Schlüssels berechnet, der zwischen einem Nachrichtenabsender und einem Nachrichtenempfänger gemeinsam genutzt wird. Die Digest-Methode (abgeleitet von einer RFC 2104-Technik) authentifiziert den Absender und stellt sicher, dass der Nachrichteninhalt nicht verändert wurde. Wenn ein Client beispielsweise eine Nachricht mit dem freigegebenen HMAC-Schlüssel an eine NetScaler-Appliance sendet, verwenden erweiterte Richtlinienausdrücke (PI) die HMAC-Funktion, um den Hash-basierten Code für den ausgewählten Text zu berechnen. Wenn der Empfänger die Nachricht dann mit dem geheimen Schlüssel erhält, berechnet er den HMAC neu, indem er ihn mit dem ursprünglichen HMAC vergleicht, um festzustellen, ob die Nachricht geändert wurde. Die HMAC-Funktion wird von Standalone-Appliances und von Appliances in einer Hochverfügbarkeitskonfiguration oder in einem Cluster unterstützt. Die Verwendung ähnelt der Konfiguration eines Verschlüsselungsschlüssels.

Die Befehle add ns hmackey und set ns hmackey enthalten einen Parameter, der die Digest-Methode und den gemeinsamen geheimen Schlüssel angibt, die für die HMAC-Berechnung verwendet werden sollen.

Um einen HMAC-Schlüssel zu konfigurieren, müssen Sie Folgendes ausführen:

1. Hinzufügen eines HMAC-Schlüssels. Konfiguriert einen HMAC-Schlüssel mit einem bestimmten Schlüsselwert.
2. Ändern eines HMAC-Schlüssels. Ändert Parameter für einen konfigurierten HMAC-Schlüssel. Die Digest-Methode kann geändert werden, ohne den Schlüsselwert zu ändern, da die Länge des Schlüsselwerts nicht durch den Digest bestimmt wird. Es ist jedoch ratsam, beim Ändern des Digest einen neuen Schlüssel anzugeben.
3. Einen HMAC-Schlüssel aufheben. Setzt Parameter für einen konfigurierten HMAC-Schlüssel auf ihre Standardwerte. Ein HMacKey Objekt mit dem Namen muss existieren. Der einzige Parameter, der nicht gesetzt werden kann, ist der Kommentar, der gelöscht wird.
4. Einen HMAC-Schlüssel entfernen. Löscht einen konfigurierten Schlüssel. Der Schlüssel kann keine Referenzen haben.

5. Zeigen Sie einen HMAC-Schlüssel an. Zeigt Parameter für den konfigurierten HMAC-Wechselstromschlüssel oder alle konfigurierten Tasten an. Wenn der Name weggelassen wird, wird der Schlüsselwert nicht angezeigt.

Konfigurieren Sie einen eindeutigen und zufälligen HMAC-Schlüssel

Sie können automatisch einen eindeutigen HMAC-Schlüssel generieren. Wenn es sich bei Ihrer Appliance um eine Clusterkonfiguration handelt, wird der HMAC-Schlüssel zu Beginn des Prozesses generiert und an alle Knoten und Paket-Engines verteilt. Dadurch wird sichergestellt, dass der HMAC-Schlüssel für alle Paket-Engines und alle Knoten im Cluster gleich ist.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns hmacKey <your_key> -digest <digest> -keyValue <keyvalue>
```

Beispiel:

```
add ns hmacKey <name> -digest sha1 -keyValue AUTO
```

Hierbei gilt:

- Die Namenssyntax ist korrekt und dupliziert nicht den Namen eines vorhandenen Schlüssels.
- Der “AUTO” KeyValue kann in den set-Befehlen verwendet werden, um neue Schlüssel für bestehende EncrytionKey- und HMacKey-Objekte zu generieren.

> **Hinweis:**
>
> Die automatische Schlüsselgenerierung ist nützlich, wenn die NetScaler-Appliance Daten mit dem Schlüssel verschlüsselt und entschlüsselt oder einen HMAC-Schlüssel generiert und überprüft. Da der Schlüsselwert selbst bei der Anzeige bereits verschlüsselt ist, können Sie den generierten Schlüsselwert nicht zur Verwendung durch eine andere Partei abrufen.

Beispiel:

```
add ns hmacKey my_hmac_key -digest sha1 -keyValue 0c753c6c5ef859189cacdf95b506d02c179
```

Die obigen Verschlüsselungsmethoden spezifizieren den Betriebsmodus mit CBC als Standardbetriebsmodus. Daher entsprechen die Methoden DES, DES2, AES128, AES192 und AES256 den Methoden DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC und AES256-CBC.

Ändern eines HMAC-Schlüssels über die CLI

Dieser Befehl ändert die für einen HMAC-Schlüssel konfigurierten Parameter. Sie können den Digest ändern, ohne den Schlüsselwert zu ändern, da die Länge des Schlüsselwerts nicht durch den Digest bestimmt wird. Es ist jedoch ratsam, beim Ändern des Digest einen neuen Schlüssel anzugeben. Geben Sie in der Befehlszeile Folgendes ein:


```
set ns hmacKey <name> [-digst <digest>] [-keyValue <keyvalue>]
[-comment <string>]

<!--NeedCopy-->
```

HMAC-Schlüssel über die CLI aufheben

Mit diesem Befehl werden für einen HMAC-Schlüssel konfigurierte Parameter mit ihren Standardwerten festgelegt. Ein HMacKey Objekt mit dem Namen muss existieren. Der einzige Parameter, den Sie aufheben können, ist die Kommentaroption, die gelöscht wird. Geben Sie in der Befehlszeile Folgendes ein:

```
unset ns hmacKey <name> -comment
```

Entfernen Sie einen HMAC-Schlüssel über die CLI

Dieser Befehl löscht den konfigurierten Hmac-Schlüssel. Der Schlüssel kann keine Referenzen haben. Geben Sie in der Befehlszeile Folgendes ein:

```
rm ns hmacKey <name>
```

Zeigen Sie einen HMAC-Schlüssel über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
show ns encryptionKey [<name>]

add ns hmacKey my_hmac_key -digest sha1 -keyValue 0
    c753c6c5ef859189cacdf95b506d02c1797407d
set ns hmacKey my_hmac_key -keyValue
    f348c594341a840a1f641a1cf24aa24c15eb1317
rm ns hmacKey my_hmac_key
show ns hmacKey my_hmac_key
           Name: my_hmac_key
     Digest: SHA1
     Key Value: (not disclosed)
<!--NeedCopy-->
```


Erweiterte Richtlinienausdrücke: Arbeiten mit Datum, Uhrzeit und Zahlen

May 11, 2023

Die meisten numerischen Daten, die die NetScaler-Appliance verarbeitet, bestehen aus Datum und Uhrzeit. Die Appliance arbeitet nicht nur mit Datum und Uhrzeit, sondern verarbeitet auch andere numerische Daten, wie z. B. die Länge von HTTP-Anfragen und -Antworten. Um diese Daten zu verarbeiten, können Sie erweiterte Richtlinienausdrücke konfigurieren, die Zahlen verarbeiten.

Ein numerischer Ausdruck besteht aus einem Ausdruckspräfix, das eine Zahl zurückgibt, und manchmal, aber nicht immer, einem Operator, der eine Operation mit der Zahl ausführen kann. Beispiele für Ausdruckspräfixe, die Zahlen zurückgeben `SYS.TIME.DAY`, sind `HTTP.REQ.CONTENT_LENGTH`, und `HTTP.RES.BODY.LENGTH`. `Numeric` Operatoren können mit jedem Präfixausdruck arbeiten, der Daten im numerischen Format zurückgibt. Der Operator `GT(<int>)` kann beispielsweise mit jedem Präfixausdruck wie HTTP.REQ.CONTENT_LENGTH verwendet werden, der eine Ganzzahl zurückgibt.

Format von Datum und Uhrzeit in einem Ausdruck

May 11, 2023

Wenn Sie einen erweiterten Richtlinienausdruck in einer Richtlinie konfigurieren, die mit Datum und Uhrzeit arbeitet (z. B. die NetScaler-Systemzeit oder ein Datum in einem SSL-Zertifikat), geben Sie ein Zeitformat wie folgt an:

```
GMT|LOCAL [<yyyy>] [<month>] [<d>] [<h>] [<m>] [<s>]
```

Es gilt:

- <yyyy> ist ein vierstelliges Jahr nach GMT oder LOCAL.
- <month> ist eine dreistellige Abkürzung für den Monat, zum Beispiel Jan, Dez.
- <d> ist ein Wochentag oder eine Ganzzahl für das Datum.

  Sie können den Tag nicht als Montag, Dienstag usw. angeben. Sie geben entweder eine Ganzzahl für einen bestimmten Tag des Monats an, oder Sie geben ein Datum als ersten, zweiten, dritten Wochentag des Monats usw. an. Im Folgenden finden Sie Beispiele für die Angabe eines Wochentags:

  - Sun_1 ist der erste Sonntag des Monats.
  - Sun_3 ist der dritte Sonntag im Monat.

  - Wed_3 ist der dritte Mittwoch im Monat.
  - 30 ist ein Beispiel für ein genaues Datum in einem Monat.
- <h> ist die Stunde, zum Beispiel 10h.
- <s> ist die Anzahl der Sekunden, zum Beispiel 30s.

Der folgende Beispielausdruck ist wahr, wenn das Datum zwischen Januar 2008 und Januar 2009 liegt, basierend auf GMT.

```
http.req.date.between(GMT 2008 Jan, GMT 2009 Jan)
```

Der folgende Beispielausdruck gilt für März und alle Monate, die auf März im Kalenderjahr folgen, basierend auf GMT:

```
sys.time.ge(GMT 2008 Mar)
```

Wenn Sie ein Datum und eine Uhrzeit angeben, beachten Sie, dass das Format Groß-/Kleinschreibung beachtet und die genaue Anzahl der Leerzeichen zwischen den Einträgen beibehalten muss.

```
**Note:**

In an expression that requires two time values, both must use GMT or
    both must use LOCAL. You cannot mix the two in an expression.

Unlike when you use the SYS.TIME prefix in an advanced policy
    expression, if you specify SYS.TIME in a rewrite action, the
    NetScaler returns a string in conventional date format (for example,
     Sun, 06 Nov 1994 08:49:37 GMT). For example, the following rewrite
    action replaces the http.res.date header with the NetScaler system
    time in a conventional date format:

add rewrite action sync_date replace http.res.date sys.time
```

Ausdrücke für die NetScaler-Systemzeit

May 11, 2023

Das SYS.TIME-Ausdruckspräfix extrahiert die NetScaler-Systemzeit. Sie können Ausdrücke konfigurieren, die festlegen, ob ein bestimmtes Ereignis zu einer bestimmten Zeit oder innerhalb eines bestimmten Zeitbereichs gemäß der NetScaler-Systemzeit eingetreten ist.

In der folgenden Tabelle werden die Ausdrücke beschrieben, die Sie mithilfe des SYS.TIME-Präfixes erstellen können.

- **SYS.TIME.BETWEEN(<time1>, <time2>):**

  Gibt den booleschen Wert TRUE zurück, wenn der zurückgegebene Wert später als <time1> und vor <time2> ist.

  Sie formatieren die Argumente <time1>, <time2> wie folgt:

  - Sie müssen beide GMT oder beide LOCAL sein.
  - <time2> muss später als <time1> sein.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der erste Sonntag des Monats ist, können Sie Folgendes angeben:

  - sys.time.between (GMT 2004, GMT 2006)
  - sys.time.between (GMT 2004 Januar, GMT 2006 November)
  - sys.time.between (GMT 2004 Januar, GMT 2006)
  - sys.time.between (GMT 2005 Mai Sun_1, GMT 2005 Mai Sun_3)
  - sys.time.between (GMT 1. Mai 2005, GMT Mai 2005 1)
  - sys.time.between (LOCAL 2005 1. Mai, LOCAL Mai 2005 1)

- **SYS.TIME.DAY:**

  Gibt den aktuellen Tag des Monats als Zahl zwischen 1 und 31 zurück.

- **SYS.TIME.EQ(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn die aktuelle Uhrzeit dem Argument <time> entspricht.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.eq (GMT 2005) (TRUE in diesem Beispiel.)
  - sys.time.eq (GMT 2005 Dez.) (In diesem Beispiel FALSCH.)
  - sys.time.eq (LOCAL 2005 May) (Wird in diesem Beispiel je nach aktueller Zeitzone als TRUE oder FALSE ausgewertet.)
  - sys.time.eq (GMT 10h) (TRUE in diesem Beispiel.)
  - sys.time.eq (GMT 10h 30s) (TRUE in diesem Beispiel.)
  - sys.time.eq (GMT 10. Mai) (TRUE in diesem Beispiel.)
  - sys.time.eq (GMT Sun) (TRUE in diesem Beispiel.)
  - sys.time.eq (GMT May Sun_1) (TRUE in diesem Beispiel.)

- **SYS.TIME.NE(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn die aktuelle Uhrzeit nicht dem Argument <time> entspricht.

- **SYS.TIME.GE(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn die aktuelle Uhrzeit später oder gleich <time> ist.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.ge (GMT 2004) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT 2005 Jan) (TRUE in diesem Beispiel.)
  - sys.time.ge (LOCAL 2005 May) (in diesem Beispiel TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - sys.time.ge (GMT 8h) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT 30m) (in diesem Beispiel FALSCH.)
  - sys.time.ge (GMT 10. Mai) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT Mai, 10 Uhr 0 Uhr) (In diesem Beispiel TRUE.)
  - sys.time.ge (GMT Sun) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT May Sun_1) (TRUE in diesem Beispiel.)

- **SYS.TIME.GT(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn der Zeitwert nach dem Argument <time> liegt.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.gt (GMT 2004) (TRUE in diesem Beispiel.)
  - sys.time.gt (GMT 2005 Jan) (TRUE in diesem Beispiel.)
  - sys.time.gt (LOCAL Mai 2005) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - sys.time.gt (GMT 8h) (TRUE in diesem Beispiel.)
  - sys.time.gt (GMT 30m) (in diesem Beispiel FALSCH.)
  - sys.time.gt (GMT 10. Mai) (in diesem Beispiel FALSCH.)
  - sys.time.gt (GMT Mai, 10 Uhr 0 Uhr) (In diesem Beispiel TRUE.)
  - sys.time.gt (GMT Sun) (in diesem Beispiel FALSCH.)
  - sys.time.gt (GMT May Sun_1) (in diesem Beispiel FALSCH.)

- **SYS.TIME.HOURS:**

  Gibt die aktuelle Stunde als Ganzzahl von 0 bis 23 zurück.

- **SYS.TIME.LE(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn der aktuelle Zeitwert vor oder gleich dem Argument <time> ist.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der

erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

- sys.time.le (GMT 2006) (TRUE in diesem Beispiel.)
- sys.time.le (GMT 2005 Dez.) (TRUE in diesem Beispiel.)
- sys.time.le (LOCAL Mai 2005) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
- sys.time.le (GMT 8h) (in diesem Beispiel FALSCH.)
- sys.time.le (GMT 30m) (TRUE in diesem Beispiel.)
- sys.time.le (GMT 10. Mai) (TRUE in diesem Beispiel.)
- sys.time.le (GMT, 11. Juni) (TRUE in diesem Beispiel.)
- sys.time.le (GMT Wed) (TRUE in diesem Beispiel.)
- sys.time.le (GMT May Sun_1) (TRUE in diesem Beispiel.)

- **SYS.TIME.LT(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn der aktuelle Zeitwert vor dem Argument <time> liegt.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.lt (GMT 2006) (TRUE in diesem Beispiel.)
  - sys.time.lt.time.lt (GMT 2005 Dez.) (TRUE in diesem Beispiel.)
  - sys.time.lt (LOCAL Mai 2005) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - sys.time.lt (GMT 8h) (in diesem Beispiel FALSCH.)
  - sys.time.lt (GMT 30m) (TRUE in diesem Beispiel.)
  - sys.time.lt (GMT, 10. Mai) (in diesem Beispiel FALSCH.)
  - sys.time.lt (GMT, 11. Juni) (TRUE in diesem Beispiel.)
  - sys.time.lt (GMT Wed) (TRUE in diesem Beispiel.)
  - sys.time.lt (GMT May Sun_1) (in diesem Beispiel FALSCH.)

- **SYS.TIME.MINUTES:**

  Gibt die aktuelle Minute als Ganzzahl von 0 bis 59 zurück.

- **SYS.TIME.MONTH:**

  Extrahiert den aktuellen Monat und gibt eine Ganzzahl von 1 (Januar) bis 12 (Dezember) zurück.

- **SYS.TIME.RELATIVE_BOOT:**

  Berechnet die Anzahl der Sekunden bis zum nächsten vorherigen oder geplanten Neustart und gibt eine Ganzzahl zurück.

  Wenn die kürzeste Startzeit in der Vergangenheit liegt, ist die Ganzzahl negativ. Liegt sie in der Zukunft, ist die Ganzzahl positiv.

- **SYS.TIME.RELATIVE_NOW:**

  Berechnet die Anzahl der Sekunden zwischen der aktuellen NetScaler-Systemzeit und der angegebenen Zeit und gibt eine Ganzzahl zurück, die die Differenz angibt.

  Liegt die angegebene Zeit in der Vergangenheit, ist die Ganzzahl negativ; liegt sie in der Zukunft, ist die Ganzzahl positiv.

- **SYS.TIME.SEKUNDEN:**

  Extrahiert die Sekunden aus der aktuellen NetScaler-Systemzeit und gibt diesen Wert als Ganzzahl von 0 bis 59 zurück.

- **SYS.TIME.WEEKDAY:**

  Gibt den aktuellen Wochentag als Wert von 0 (Sonntag) bis 6 (Samstag) zurück.

- **SYS.TIME.WITHIN (<time1>, <time2>):**

  Wenn Sie in <time1> ein Zeitelement weglassen, z. B. den Tag oder die Stunde, wird davon ausgegangen, dass es den niedrigsten Wert in seinem Bereich hat. Wenn Sie in <time2> ein Element weglassen, wird davon ausgegangen, dass es den höchsten Wert in seinem Bereich hat.

  Die Bereiche für die Zeitelemente lauten wie folgt: Monat 1-12, Tag 1-31, Wochentag 0-6, Stunde 0-23, Minuten 0-59 und Sekunden 0-59. Wenn Sie das Jahr angeben, müssen Sie dies in <time1> und <time2> tun.

  Wenn die Uhrzeit beispielsweise GMT 2005, 10. Mai, 10 Uhr, 15 Uhr, 30 Uhr ist und es der zweite Dienstag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.within (GMT 2004, GMT 2006) (TRUE in diesem Beispiel.)
  - sys.time.within (GMT 2004 Jan, GMT 2006 Mär) (FALSCH, Mai liegt nicht im Bereich Januar bis März.)
  - sys.time.within (GMT Feb, GMT) (WAHR, Mai liegt im Bereich von Februar bis Dezember.)
  - sys.time.within (GMT Sun_1, GMT Sun_3) (WAHR, der zweite Dienstag liegt zwischen dem ersten Sonntag und dem dritten Sonntag.)
  - sys.time.within (GMT 2005, 1. Mai 2005, 1:17 Uhr) (TRUE in diesem Beispiel.)
  - sys.time.within (LOCAL 2005 1. Mai, LOCAL Mai 2005 1) (WAHR oder FALSCH, abhängig von der NetScaler-Systemzeitzone.)

- **SYS.TIME.YEAR:**

  Extrahiert das Jahr aus der aktuellen Systemzeit und gibt diesen Wert als vierstellige Ganzzahl zurück.

Ausdrücke für SSL-Zertifikatsdaten

May 11, 2023

Sie können die Gültigkeitsdauer von SSL-Zertifikaten bestimmen, indem Sie einen Ausdruck konfigurieren, der das folgende Präfix enthält:

```
CLIENT.SSL.CLIENT_CERT
```

Der folgende Beispielausdruck entspricht einer bestimmten Ablaufzeit den Informationen im Zertifikat:

```
client.ssl.client_cert.valid_not_after.eq(GMT 2009)
```

In der folgenden Tabelle werden zeitbasierte Operationen mit SSL-Zertifikaten beschrieben. Um den gewünschten Ausdruck zu erhalten, ersetzen Sie *certificate* im Ausdruck in der ersten Spalte durch den Präfixausdruck „CLIENT.SSL.CLIENT_CERT“.

- `<certificate>.VALID_NOT_AFTER`:

  Gibt den letzten Tag vor Ablauf des Zertifikats zurück. Das Rückgabeformat ist die Anzahl der Sekunden seit GMT am 1. Januar 1970 (0 Stunden, 0 Minuten, 0 Sekunden).

- **<certificate>.VALID_NOT_AFTER.BETWEEN(<time1>, <time2>):**

  Gibt einen booleschen TRUE-Wert zurück, wenn die Gültigkeitsdauer des Zertifikats zwischen den Argumenten <time1> und <time2> liegt. <time1> und <time2> müssen vollständig angegeben werden. Es folgen Beispiele:

  GMT 1995 Jan ist vollständig spezifiziert.

  GMT Jan ist nicht vollständig spezifiziert

  GMT 1995 20 ist nicht vollständig spezifiziert.

  GMT Jan Mon_2 ist nicht vollständig spezifiziert.

  Die Argumnte <time1> und <time2> müssen sowohl GMT als auch LOCAL sein und <time2> muss größer als <time1> sein.

  Wenn es beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr 30 Uhr und der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung stehen in Klammern).

  - . .zwischen (GMT 2004, GMT 2006) (WAHR)
  - .. zwischen (GMT 2004 Januar, GMT 2006 November) (WAHR)
  - .. zwischen (GMT 2004 Januar, GMT 2006) (WAHR)
  - . .between (GMT 2005 Mai Sun_1, GMT 2005 Mai Sun_3) (WAHR)
  - . .between (GMT 1. Mai 2005, 1 GMT Mai 2005) (WAHR)

- . .between (LOCAL 2005 1. Mai, LOCAL Mai 2005 1) (WAHR oder FALSCH, abhängig von der NetScaler-Systemzeitzone.)

- **<certificate>.VALID_NOT_AFTER.DAY:**

  Extrahiert den letzten Tag des Monats, in dem das Zertifikat gültig ist, und gibt je nach Datum eine Zahl zwischen 1 und 31 zurück.

- **<certificate>.VALID_NOT_AFTER.EQ(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn die Zeit dem Argument <time> entspricht.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Bewertungsergebnisse für dieses Beispiel stehen in Klammern):

  - . .eq (GMT 2005) (WAHR)
  - . .eq (GMT 2005 Dez.) (FALSCH)
  - . .eq (LOCAL 2005 May) (WAHR oder FALSCH, abhängig von der aktuellen Zeitzone)
  - . .eq (GMT 10 h) (WAHR)
  - . .eq (GMT 10h 30s) (WAHR)
  - . .eq (GMT, 10. Mai) (WAHR)
  - . .eq (GMT Sun) (WAHR)
  - . .eq (GMT Mai-Sonntag 1) (WAHR)

- **<certificate>.VALID_NOT_AFTER.GE(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn der Zeitwert größer oder gleich dem Argument <time> ist.

  Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung für dieses Beispiel stehen in Klammern):

  - . .ge (GMT 2004) (WAHR)
  - . .ge (GMT 2005 Januar) (WAHR)
  - . .ge (LOCAL 2005 May) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - . .ge (GMT 8h) (WAHR)
  - . .ge (GMT 30 m) (FALSCH)
  - . .ge (GMT, 10. Mai) (WAHR)
  - .. .ge (GMT. Mai, 10 Uhr, 0 Uhr) (WAHR)
  - . .ge (GMT Sun) (WAHR)
  - . .ge (GMT Mai-Sonnne_1) (WAHR)

- **<certificate>.VALID_NOT_AFTER.GT(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn der Zeitwert größer als das Argument <time> ist.

Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung für dieses Beispiel stehen in Klammern):

- . .gt (GMT 2004) (WAHR)
- . .gt (GMT 2005 Jan) (WAHR)
- . .gt (LOCAL Mai 2005) (WAHR oder FALSCH, abhängig von der aktuellen Zeitzone.)
- . .gt (GMT 8h) (WAHR)
- . .gt (GMT 30 m) (FALSCH)
- . .gt (GMT, 10. Mai) (FALSCH)
- . .gt (GMT Sun) (FALSCH)
- . .gt (GMT Mai-Sonnne_1) (FALSCH)

- **<certificate>.VALID_NOT_AFTER.HOURS:**

  Extrahiert die letzte Stunde, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 23 zurück.

- **<certificate>.VALID_NOT_AFTER.LE(<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem Argument <time> vorausgeht oder gleich ist.

  Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung für dieses Beispiel stehen in Klammern):

  - . .le (GMT 2006) (WAHR)
  - .. .le (GMT 2005 Dez.) (WAHR)
  - . .le (LOCAL 2005 May) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - . .le (GMT 8h) (FALSCH)
  - . .le (GMT 30 m) (WAHR)
  - .. .le (GMT, 10. Mai) (WAHR)
  - .. .le (GMT, 11. Juni) (WAHR)
  - .. .le (GMT Mi) (TRUE)
  - .. .le (GMT Mai-Sonnne_1) (WAHR)

- **<certificate>.VALID_NOT_AFTER.LT(<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem Argument <time> vorausgeht.

  Wenn die aktuelle Uhrzeit beispielsweise am 1. Mai 2005 um 10 Uhr 15 Uhr 30 Uhr ist und es der erste Sonntag des Monats ist, können Sie Folgendes angeben:

  - . .lt (GMT 2006) (WAHR)
  - . .lt (GMT 2005 Dez.) (WAHR)
  - . .lt (LOCAL Mai 2005) (WAHR oder FALSCH, abhängig von der aktuellen Zeitzone.)

- . .lt (GMT 8h) (FALSCH)
- . .lt (GMT 30 m) (WAHR)
- . .lt (GMT 10. Mai) (FALSCH)
- .. .lt (GMT, 11. Juni) (WAHR)
- .. .lt (GMT Mi) (TRUE)
- . .lt (GMT Mai-Sonnne_1) (FALSCH)

- **<certificate>.VALID_NOT_AFTER.MINUTES:**

  Extrahiert die letzte Minute, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 59 zurück.

- **<certificate>.VALID_NOT_AFTER.MONTH:**

  Extrahiert den letzten Monat, in dem das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 1 (Januar) bis 12 (Dezember) zurück.

- **<certificate>.VALID_NOT_AFTER.RELATIVE_BOOT:**

  Berechnet die Anzahl der Sekunden bis zum nächsten vorherigen oder geplanten Neustart und gibt eine Ganzzahl zurück. Wenn die kürzeste Startzeit in der Vergangenheit liegt, ist die Ganzzahl negativ. Liegt sie in der Zukunft, ist die Ganzzahl positiv.

- **<certificate>.VALID_NOT_AFTER.RELATIVE_NOW;**

  Berechnet die Anzahl der Sekunden zwischen der aktuellen Systemzeit und der angegebenen Zeit und gibt eine Ganzzahl zurück. Liegt die Zeit in der Vergangenheit, ist die Ganzzahl negativ; liegt sie in der Zukunft, ist die Ganzzahl positiv.

- **<certificate>.VALID_NOT_AFTER.SECONDS:**

  Extrahiert die letzte Sekunde, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 59 zurück.

- **<certificate>.VALID_NOT_AFTER.WEEKDAY:**

  Extrahiert den letzten Wochentag, an dem das Zertifikat gültig ist. Gibt eine Zahl zwischen 0 (Sonntag) und 6 (Samstag) zurück, um den Wochentag im Zeitwert anzugeben.

- **<certificate>.VALID_NOT_AFTER.WITHIN(<time1>, <time2>):**

  Gibt den booleschen Wert TRUE zurück, wenn die Zeit innerhalb aller Bereiche liegt, die durch die Elemente in <time1> und <time2> definiert sind.

  Wenn Sie ein Zeitelement in <time1> weglassen, wird davon ausgegangen, dass es den niedrigsten Wert in seinem Bereich hat. Wenn Sie ein Element in <time2> weglassen, wird davon ausgegangen, dass es den höchsten Wert in seinem Bereich hat. Wenn Sie in <time1> ein Jahr angeben, müssen Sie es in <time2> angeben.

Die Bereiche für Zeitelemente lauten wie folgt: Monat 1-12, Tag 1-31, Wochentag 0-6, Stunde 0-23, Minuten 0-59 und Sekunden 0-59. Damit das Ergebnis TRUE ist, muss jedes Element der Zeit in dem Bereich existieren, den Sie in <time1>, <time2> angeben.

Wenn die Zeit beispielsweise GMT 2005, 10. Mai, 10 Uhr 15 Uhr 30 Uhr ist und es der zweite Dienstag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung stehen in Klammern):

- . .within (GMT 2004, GMT 2006) (WAHR)
- . .within (GMT 2004 Jan, GMT 2006 Mar) (FALSCH, Mai liegt nicht im Bereich Januar bis März.)
- . .within (GMT Feb, GMT) (WAHR, Mai liegt im Bereich von Februar bis Dezember)
- . .within (GMT Sun_1, GMT Sun_3) (WAHR, der zweite Dienstag liegt im Bereich vom ersten Sonntag bis zum dritten Sonntag)
- . .within (GMT 2005, 1. Mai 2005, 1 17 Uhr) (WAHR)
- . .within (LOCAL 2005 1. Mai, LOCAL Mai 2005 1) (WAHR oder FALSCH, abhängig von der NetScaler-Systemzeitzone)

- **<certificate>.VALID_NOT_AFTER.YEAR:**

  Extrahiert das letzte Jahr, in dem das Zertifikat gültig ist, und gibt eine vierstellige Ganzzahl zurück.

- **<certificate>.VALID_NOT_BEFORE:**

  Gibt das Datum zurück, an dem das Client-Zertifikat gültig wird.

  Das Rückgabeformat ist die Anzahl der Sekunden seit GMT am 1. Januar 1970 (0 Stunden, 0 Minuten, 0 Sekunden).

- **<certificate>.VALID_NOT_BEFORE.BETWEEN(<time1>, <time2>):**

  Gibt den booleschen Wert TRUE zurück, wenn der Zeitwert zwischen den beiden Zeitargumenten liegt. Die Argumente <time1> und <time2> müssen beide vollständig angegeben werden.

  Es folgen Beispiele:

  GMT 1995 Jan ist vollständig spezifiziert.
  GMT Jan ist nicht vollständig spezifiziert.
  GMT 1995 20 ist nicht vollständig spezifiziert.
  GMT Jan Mon_2 ist nicht vollständig spezifiziert.
  Die Zeitargumente müssen sowohl GMT als auch LOCAL sein und <time2> muss größer als <time1> sein.

  Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung für dieses Beispiel stehen in Klammern):

- . .zwischen (GMT 2004, GMT 2006) (WAHR)
- .. zwischen (GMT 2004 Januar, GMT 2006 November) (WAHR)
- .. zwischen (GMT 2004 Januar, GMT 2006) (WAHR)
- . .between (GMT 2005 Mai Sun_1, GMT 2005 Mai Sun_3) (WAHR)
- . .between (GMT 1. Mai 2005, 1 GMT Mai 2005) (WAHR)
- . .between (LOCAL 2005 1. Mai, LOCAL Mai 2005 1) (WAHR oder FALSCH, abhängig von der NetScaler-Systemzeitzone.)

- **<certificate>.VALID_NOT_BEFORE.DAY:**

  Extrahiert den letzten Tag des Monats, in dem das Zertifikat gültig ist, und gibt diesen Wert als Zahl zwischen 1 und 31 zurück, die diesen Tag darstellt.

- **<certificate>.VALID_NOT_BEFORE.EQ(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn die Zeit dem Argument <time> entspricht.

  Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung für dieses Beispiel stehen in Klammern):

  - . .eq (GMT 2005) (WAHR)
  - . .eq (GMT 2005 Dez.) (FALSCH)
  - . .eq (LOCAL 2005 May) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - . .eq (GMT 10 h) (WAHR)
  - . .eq (GMT 10h 30s) (WAHR)
  - . .eq (GMT, 10. Mai) (WAHR)
  - . .eq (GMT Sun) (WAHR)
  - . .eq (GMT Mai-Sonntag 1) (WAHR)

- **<certificate>.VALID_NOT_BEFORE.GE(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn die Zeit größer (nach) oder gleich dem Argument <time> ist.

  Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung stehen in Klammern):

  - . .ge (GMT 2004) (WAHR)
  - . .ge (GMT 2005 Januar) (WAHR)
  - . .ge (LOCAL 2005 May) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - . .ge (GMT 8h) (WAHR)
  - . .ge (GMT 30 m) (FALSCH)
  - . .ge (GMT, 10. Mai) (WAHR)
  - .. .ge (GMT. Mai, 10 Uhr, 0 Uhr) (WAHR)

- . .ge (GMT Sun) (WAHR)
- . .ge (GMT Mai-Sonnne_1) (WAHR)

- **<certificate>.VALID_NOT_BEFORE.GT(<time>):**

  Gibt den booleschen Wert TRUE zurück, wenn die Zeit nach dem Argument <time> liegt.

  Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung stehen in Klammern):

  - . .gt (GMT 2004) (WAHR)
  - . .gt (GMT 2005 Jan) (WAHR)
  - . .gt (LOCAL Mai 2005) (WAHR oder FALSCH, abhängig von der aktuellen Zeitzone.)
  - . .gt (GMT 8h) (WAHR)
  - . .gt (GMT 30 m) (FALSCH)
  - . .gt (GMT, 10. Mai) (FALSCH)
  - .. .gt (GMT 10. Mai, 10 Uhr, 0 Uhr) (WAHR)
  - . .gt (GMT Sun) (FALSCH)
  - . .gt (GMT Mai-Sonnne_1) (FALSCH)

- **<certificate>.VALID_NOT_BEFORE.HOURS:**

  Extrahiert die letzte Stunde, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 23 zurück.

- **<certificate>.VALID_NOT_BEFORE.LE(<time>)

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem Argument <time> vorausgeht oder gleich ist.

  Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung für dieses Beispiel stehen in Klammern):

  - . .le (GMT 2006) (WAHR)
  - .. .le (GMT 2005 Dez.) (WAHR)
  - . .le (LOCAL 2005 May) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - .. .le (GMT 8h) (FALSCH)
    . - . .le (GMT 30 m) (WAHR)
  - .. .le (GMT, 10. Mai) (WAHR)
  - .. .le (GMT, 11. Juni) (WAHR)
  - .. .le (GMT Mi) (TRUE)
  - .. .le (GMT Mai-Sonnne_1) (WAHR)

- **<certificate>.VALID_NOT_BEFORE.LT(<time>):**

Gibt einen booleschen TRUE zurück, wenn die Zeit dem Argument <time> vorausgeht.

Wenn der Zeitwert beispielsweise GMT 2005, 1. Mai, 10 Uhr 15 Uhr, 30 Uhr lautet und es sich um den ersten Sonntag des Monats Mai im Jahr 2005 handelt, können Sie Folgendes angeben (die Ergebnisse der Auswertung für dieses Beispiel stehen in Klammern):

- . .lt (GMT 2006) (WAHR)
- . .lt (GMT 2005 Dez.) (WAHR)
- . .lt (LOCAL Mai 2005) (WAHR oder FALSCH, abhängig von der aktuellen Zeitzone.)
- . .lt (GMT 8h) (FALSCH)
- . .lt (GMT 30 m) (WAHR)
- . .lt (GMT 10. Mai) (FALSCH)
- .. .lt (GMT, 11. Juni) (WAHR)
- .. .lt (GMT Mi) (TRUE)
- . .lt (GMT Mai-Sonnne_1) (FALSCH)

- **<certificate>.VALID_NOT_BEFORE.MINUTES:**

  Extrahiert die letzte Minute, in der das Zertifikat gültig ist. Gibt die aktuelle Minute als Ganzzahl von 0 bis 59 zurück.

- **<certificate>.VALID_NOT_BEFORE.MONTH:**

  Extrahiert den letzten Monat, in dem das Zertifikat gültig ist. Gibt den aktuellen Monat als Ganzzahl von 1 (Januar) bis 12 (Dezember) zurück.

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_BOOT:**

  Berechnet die Anzahl der Sekunden bis zum nächsten vorherigen oder geplanten NetScaler-Neustart und gibt eine Ganzzahl zurück. Wenn die kürzeste Startzeit in der Vergangenheit liegt, ist die Ganzzahl negativ. Liegt sie in der Zukunft, ist die Ganzzahl positiv.

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_NOW:**

  Gibt die Anzahl der Sekunden zwischen der aktuellen NetScaler-Systemzeit und der angegebenen Zeit als Ganzzahl zurück. Wenn die angegebene Zeit in der Vergangenheit liegt, ist die Ganzzahl negativ. Liegt sie in der Zukunft, ist die Ganzzahl positiv.

- **<certificate>.VALID_NOT_BEFORE.SECONDS:**

  Extrahiert die letzte Sekunde, in der das Zertifikat gültig ist. Gibt die aktuelle Sekunde als Ganzzahl von 0 bis 59 zurück.

- **<certificate>.VALID_NOT_BEFORE.WEEKDAY:**

  Extrahiert den letzten Wochentag, an dem das Zertifikat gültig ist. Gibt den Wochentag als Zahl zwischen 0 (Sonntag) und 6 (Samstag) zurück.

- **<certificate>.VALID_NOT_BEFORE.WITHIN(<time1>, <time2>):**

Gibt den booleschen Wert TRUE zurück, wenn jedes Zeitelement innerhalb des in den Argumenten <time1>, <time2> definierten Bereichs liegt.

Wenn Sie ein Zeitelement in <time1> weglassen, wird davon ausgegangen, dass es den niedrigsten Wert in seinem Bereich hat. Wenn Sie ein Zeitelement in <time2> weglassen, wird davon ausgegangen, dass es den höchsten Wert in seinem Bereich hat. Wenn Sie ein Jahr in <time1> angeben, muss es in <time2> angegeben werden. Die Bereiche für Zeitelemente lauten wie folgt: Monat 1-12, Tag 1-31, Wochentag 0-6, Stunde 0-23, Minuten 0-59 und Sekunden 0-59.

Wenn die Uhrzeit beispielsweise GMT 2005, 10. Mai, 10 Uhr, 15 Uhr, 30 Uhr ist und es der zweite Dienstag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung stehen in Klammern):

- . .within (GMT 2004, GMT 2006) (WAHR)
- . .within (GMT 2004 Jan, GMT 2006 Mar) (FALSCH, Mai liegt nicht im Bereich Januar bis März.)
- . .within (GMT Feb, GMT) (WAHR, Mai liegt im Bereich von Februar bis Dezember.)
- . .within (GMT Sun_1, GMT Sun_3) (WAHR, der zweite Dienstag liegt zwischen dem ersten Sonntag und dem dritten Sonntag.)
- . .within (GMT 2005, 1. Mai 2005, 1 17 Uhr) (WAHR)
- . .within (LOCAL 2005 1. Mai, LOCAL Mai 2005 1) (WAHR oder FALSCH, abhängig von der NetScaler-Systemzeitzone)

- **<certificate>.VALID_NOT_BEFORE.YEAR:**

  Extrahiert das letzte Jahr, in dem das Zertifikat gültig ist. Gibt das aktuelle Jahr als vierstellige Ganzzahl zurück.

Ausdrücke für HTTP-Anforderungs- und Antwortdaten

October 8, 2021

Die folgenden Ausdruckspräfixe geben den Inhalt des HTTP Date-Headers als Text oder als Datumsobjekt zurück. Diese Werte können wie folgt ausgewertet werden:

- Als Zahl. Der numerische Wert eines HTTP Date-Headers wird in Form der Anzahl der Sekunden seit dem 1. Januar 1970 zurückgegeben.

  Beispielsweise gibt der Ausdruck http.req.date.mod (86400) die Anzahl der Sekunden seit Tagesbeginn zurück. Diese Werte können mit denselben Operationen ausgewertet werden wie andere nicht datumsbezogene numerische Daten. Weitere Informationen finden Sie unter Ausdruckspräfixe für andere numerische Daten als Datum und Uhrzeit.

- Als HTTP-Header. Datum-Header können mit den gleichen Operationen wie andere HTTP-Header ausgewertet werden.

  Weitere Informationen finden Sie unter Erweiterte Richtlinienausdrücke: Parsen von HTTP-, TCP- und UDP-Daten.

- Als Text. Datumskopfzeilen können mit den gleichen Operationen wie andere Zeichenfolgen ausgewertet werden.

Weitere Informationen finden Sie unter Erweiterte Richtlinienausdrücke: Text auswerten.

Prefix	Beschreibung
HTTP.REQ.DATE	Gibt den Inhalt des HTTP Date-Headers als Text oder als Datumsobjekt zurück. Die erkannten Datumsformate sind: RFC822. Sun, 06 Jan 1980 08:49:37 GMT, RFC850. Sunday, 06-Jan-80 09:49:37 GMT, and ASCTIME. Sun Jan 6 08:49:37 1980.
HTTP.RES.DATE	Gibt den Inhalt des HTTP Date-Headers als Text oder als Datumsobjekt zurück. Die erkannten Datumsformate sind: RFC822. Sun, 06 Jan 1980 8:49:37 GMT, RFC850. Sunday, 06-Jan-80 9:49:37 GMT, and ASCTIME. Sun Jan 6 08:49:37 1980.

Generieren Sie den Wochentag als String in kurzen und langen Formaten

January 19, 2021

Die Funktionen `WEEKDAY_STRING_SHORT` und `WEEKDAY_STRING` erzeugen den Wochentag als String in kurzen und langen Formaten. Die zurückgegebenen Strings sind immer in Englisch. Das Präfix, das mit diesen Funktionen verwendet wird, muss den Wochentag im ganzzahligen Format zurückgeben und der akzeptable Bereich für den vom Präfix zurückgegebenen Wert ist 0-6. Daher können Sie ein beliebiges Präfix verwenden, das eine ganze Zahl im zulässigen Bereich zurückgibt. Eine UNDEF-Bedingung wird ausgelöst, wenn der zurückgegebene Wert nicht in diesem Bereich liegt oder wenn die Speicherzuweisung fehlschlägt.

Im Folgenden sind die Beschreibungen der Funktionen:

Funktion	Beschreibung
<prefix>.WEEKDAY_STRING_SHORT	Gibt den Wochentag im Kurzformat zurück. Die Kurzform ist immer 3 Zeichen lang mit einem Anfangssatz und die restlichen Zeichen in Kleinbuchstaben. Beispiel: SYS.TIME.WEEKDAY.WEEKDAY_STRING_SHORT gibt Sun zurück, wenn der von der Funktion WEEKDAY zurückgegebene Wert 0 ist, und Sat, wenn der vom Präfix zurückgegebene Wert 6 lautet.
<prefix>.WEEKDAY_STRING	Gibt den Wochentag im Langformat zurück. Die lange Form hat immer ein Anfangsbuchstaben, wobei die restlichen Zeichen in Kleinbuchstaben enthalten sind. SYS.TIME.WEEKDAY.WEEKDAY_STRING“ Gibt beispielsweise Sonntag zurück, wenn der von der Funktion WEEKDAY zurückgegebene Wert 0 ist, und Samstag, wenn der vom Präfix zurückgegebene Wert 6 ist.

Ausdruckspräfixe für numerische Daten außer Datum und Uhrzeit

August 19, 2021

Sie können nicht nur Ausdrücke konfigurieren, die pünktlich ausgeführt werden, sondern auch Ausdrücke für die folgenden numerischen Datentypen konfigurieren:

- Die Länge der HTTP-Anforderungen, die Anzahl der HTTP-Header in einer Anforderung usw.

  Weitere Informationen finden Sie unter Ausdrücke für numerische HTTP-Nutzlastdaten außer Datumsangaben.

- IP- und MAC-Adressen.

  Weitere Informationen finden Sie unter Ausdrücke für IP-Adressen und IP-Subnetze.

- Client- und Serverdaten in Bezug auf Schnittstellen-IDs und Transaktionsdurchsatzrate.

  Weitere Informationen finden Sie unter Ausdrücke für numerische Client- und Serverdaten.

- Numerische Daten in Clientzertifikaten mit Ausnahme von Datumsangaben.

Informationen zu diesen Präfixen, einschließlich der Anzahl der Tage bis zum Ablauf des Zertifikats und der Größe des Verschlüsselungsschlüssels, finden Sie unter Präfixe für numerische Daten in SSL-Zertifikaten.

Konvertieren von Zahlen in Text

August 19, 2021

Die folgenden Funktionen erzeugen binäre Zeichenfolgen aus einer Zahl, die von einem Ausdruckspräfix zurückgegeben wird. Diese Funktionen sind besonders nützlich in der TCP-Rewrite-Funktion als Ersatzzeichenfolgen für Binärdaten. Weitere Informationen zur Funktion zum Umschreiben von TCP finden Sie unter Umschreiben.

Alle Funktionen geben einen Wert vom Typ Text zurück. Die Endiannität, die einige Funktionen als Parameter akzeptieren, ist entweder LITTLE_ENDIAN oder BIG_ENDIAN.

Funktion	Beschreibung
<number>.SIGNED8_STRING	Erzeugt eine 8-Bit-binäre Zeichenfolge mit Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_SIGNED8 (16) .SUB (3) .SIGNED8_STRING
<number>.UNSIGNED8_STRING	Erzeugt eine 8-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED8 (31) .ADD (3) .UNSIGNED8_STRING
<number>.SIGNED16_STRING (<endianness>)	Erzeugt eine 16-Bit-binäre Zeichenfolge mit Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .SKIP (12) .GET_SIGNED16 (0, BIG_ENDIAN) .SUB (4) .SIGNED16_STRING (BIG_ENDIAN)

Funktion	Beschreibung
<number>.UNSIGNED16_STRING (<endianness>)	Erzeugt eine 16-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED16 (47, LITTLE_ENDIAN) .ADD (7) .UNSIGNED16_STRING (LITTLE_ENDIAN)
<number>.SIGNED32_STRING (<endianness>)	Erzeugt eine 32-Bit-Binärzeichenfolge mit Vorzeichen, die die Zahl darstellt. Beispiel: HTTP.REQ.BODY (100) .AFTER_STR (“delim”) .GET_SIGNED32 (0, BIG_ENDIAN) .SUB (1) .SIGNED32_STRING (BIG_ENDIAN)
<unsigned_long_number>.UNSIGNED8_STRING	Erzeugt eine 8-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED8 (24) .TYPECAST_UNSIGNED_LONG_AT.ADD (12) .UNSIGNED8_STRING
<unsigned_long_number>.UNSIGNED16_STRING (<endianness>)	Erzeugt eine 16-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED16 (23, LITTLE_ENDIAN) .TYPECAST_UNSIGNED_LONG_AT.ADD (10) .UNSIGNED16_STRING (LITTLE_ENDIAN)
<unsigned_long_number>.UNSIGNED32_STRING (<endianness>)	Erzeugt eine 32-Bit-Binärzeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .AFTER_STR (“delim2”) .GET_UNSIGNED32 (0, BIG_ENDIAN) .ADD (2) .UNSIGNED32_STRING (BIG_ENDIAN)

Virtuelle Server-basierte Ausdrücke

October 8, 2021

Mit dem Ausdruckspräfix `SYS.VSERVER("<vserver-name>")` können Sie einen virtuellen Server identifizieren. Mit diesem Präfix können Sie die folgenden Funktionen verwenden, um Informationen zum angegebenen virtuellen Server abzurufen:

- **THROUGHPUT.** Gibt den Durchsatz des virtuellen Servers in Mbit/s (Megabit pro Sekunde) zurück. Der zurückgegebene Wert ist eine vorzeichenlose lange Zahl.

  Usage: SYS.VSERVER(“vserver”).THROUGHPUT

- **CONNECTIONS.** Gibt die Anzahl der Verbindungen zurück, die vom virtuellen Server verwaltet werden. Der zurückgegebene Wert ist eine vorzeichenlose lange Zahl.

  Usage: SYS.VSERVER(“vserver”).CONNECTIONS

- **STATE.** Gibt den Status des virtuellen Servers zurück. Der zurückgegebene Wert ist UP, DOWN oder OUT_OF_SERVICE. Einer dieser Werte kann daher als Argument an den EQ () -Operator übergeben werden, um einen Vergleich durchzuführen, der zu einem booleschen TRUE oder FALSE führt.

  Usage: SYS.VSERVER(“vserver”).STATE

- **HEALTH.** Gibt den Prozentsatz der Dienste in einem UP-Status für den angegebenen virtuellen Server zurück. Der zurückgegebene Wert ist eine Ganzzahl.

  Usage: SYS.VSERVER(“vserver”).HEALTH

- **RESPTIME.** Gibt die Reaktionszeit als Integer zurück, die die Anzahl der Mikrosekunden angibt. Die Reaktionszeit ist der durchschnittliche TTFB (Time To First Byte) aller Dienste, die an den virtuellen Server gebunden sind.

  Usage: SYS.VSERVER(“vserver”).RESPTIME

- **SURGECOUNT.** Gibt die Anzahl der Anforderungen in der Überspannungswarteschlange des virtuellen Servers zurück. Der zurückgegebene Wert ist eine Ganzzahl.

  Usage: SYS.VSERVER(“vserver”).SURGECOUNT

Beispiel 1:

Die folgende Rewriterichtlinie bricht die Verarbeitung des Rewrites ab, wenn die Anzahl der Verbindungen auf dem virtuellen Lastausgleichsserver LBVServer 10000 überschreitet:

```
add rewrite policy norewrite_pol sys.vserver("LBvserver").connections.gt
(10000)norewrite
```

Beispiel 2:

Die folgende Rewriteaktion fügt einen benutzerdefinierten Header, TP, ein, dessen Wert durchgehend auf dem virtuellen Server LBVServer ist:

```
add rewrite action tp_header insert_http_header TP SYS.VSERVER("LBvserver")
.THROUGHPUT
```

Beispiel 3:

Die folgende Überwachungsprotokollnachrichtigungsaktion schreibt den durchschnittlichen TTFB der Dienste, die an einen virtuellen Server gebunden sind, in die newslog-Protokolldatei:

```
add audit messageaction log_vserver_resptime_act INFORMATIONAL "\"NS
Response Time to Servers:\" + sys.vserver(\"ssllb\").resptime + \" millisec
\""-logtoNewnslog YES
```

Erweiterte Richtlinienausdrücke: Analysieren von HTTP-, TCP- und UDP-Daten

May 11, 2023

Sie können erweiterte Richtlinienausdrücke konfigurieren, um die Nutzlast in einer HTTP-Anforderung oder -Antwort auszuwerten. Die Nutzlast, die einer HTTP-Verbindung zugeordnet ist, umfasst HTTP-Header (Standard- oder benutzerdefinierte Header), Textkörper und Verbindungs-URL. Sie können die Nutzlast auch in einem TCP- oder einem UDP-Paket auswerten und verarbeiten. Bei HTTP-Verbindungen können Sie beispielsweise überprüfen, ob ein bestimmter HTTP-Header vorhanden ist oder ob die URL einen bestimmten Abfrageparameter enthält.

Sie können Ausdrücke konfigurieren, um die URL-Codierung zu transformieren und die “sichere” HTML- oder XML-Codierung für die nachfolgende Auswertung anzuwenden. Sie können auch XPATH- und JSON-Präfixe verwenden, um das Datum in XML- bzw. JSON-Dateien auszuwerten.

Sie können auch textbasierte und numerische erweiterte Richtlinienausdrücke verwenden, um HTTP-Anforderungs- und Antwortdaten auszuwerten. Weitere Informationen finden Sie unter Erweiterte Richtlinienausdrücke: Text auswerten und Erweiterte Richtlinienausdrücke: Arbeiten mit Datum, Uhrzeit und Zahlen.

Ausdrücke zur Identifizierung des Protokolls in einem eingehenden IP-Paket

May 11, 2023

In der folgenden Tabelle sind die Ausdrücke aufgeführt, mit denen Sie das Protokoll in einem eingehenden Paket identifizieren können.

Ausdruck	Beschreibung
CLIENT.IP.PROTOCOL	Identifiziert das Protokoll in IPv4-Paketen, die von Clients gesendet werden.
CLIENT.IPV6.PROTOCOL	Identifiziert das Protokoll in IPv6-Paketen, die von Clients gesendet werden.
SERVER.IP.PROTOCOL	Identifiziert das Protokoll in IPv4-Paketen, die von Servern gesendet werden.
SERVER.IPV6.PROTOCOL	Identifiziert das Protokoll in IPv6-Paketen, die von Servern gesendet werden.

Argumente für die PROTOCOL-Funktion

Sie können die Protokollnummer der Internet Assigned Numbers Authority (IANA) an die PROTOCOL-Funktion übergeben. Wenn Sie beispielsweise ermitteln möchten, ob das Protokoll in einem eingehenden Paket TCP ist, können Sie CLIENT.IP.PROTOCOL.EQ (6) verwenden, wobei 6 die von der IANA zugewiesene Protokollnummer für TCP ist. Bei einigen Protokollen können Sie anstelle der Protokollnummer einen Aufzählungswert übergeben. Beispielsweise können Sie anstelle von CLIENT.IP.PROTOCOL.EQ (6) CLIENT.IP.PROTOCOL.EQ (TCP) verwenden. In der folgenden Tabelle sind die Protokolle aufgeführt, für die Sie Aufzählungswerte verwenden können, sowie die entsprechenden Aufzählungswerte zur Verwendung mit der PROTOCOL-Funktion.

Protokoll	Aufzählungswert
Transmission Control Protocol (TCP)	TCP
Benutzer-Datagramm-Protokoll (UDP)	UDP
Internet Control Message Protocol (ICMP)	ICMP
IP Authentication Header (AH) für die Bereitstellung von Authentifizierungsdiensten in IPv4 und IPv6	AH
Encapsulating Security Payload (ESP) -Protokoll	ESP
Allgemeine Routing-Kapselung (GRE)	GRE
IP-in-IP-Kapselungsprotokoll	IPIP

Protokoll	Aufzählungswert
Internet Control Message Protocol für IPv6 (ICMPv6)	ICMPv6
Fragment-Header für IPv6	FRAGMENT

Anwendungsfallszenarien

Die Protokollausdrücke können sowohl in anforderungsbasierten als auch in antwortbasierten Richtlinien verwendet werden. Sie können die Ausdrücke in verschiedenen NetScaler-Funktionen verwenden, z. B. in Load-Balancing, WAN-Optimierung, Content Switching, Rewrite- und Listen-Richtlinien. Sie können die Ausdrücke mit Funktionen wie EQ () und NE () verwenden, um das Protokoll in einer Richtlinie zu identifizieren und eine Aktion auszuführen.

Im Folgenden finden Sie einige Anwendungsfälle für die Ausdrücke:

- In Branch Repeater-Load-Balancing-Konfigurationen können Sie die Ausdrücke in einer Listen-Policy für den virtuellen Wildcard-Server verwenden. Sie können beispielsweise den virtuellen Wildcard-Server mit der Listenrichtlinie CLIENT.IP.PROTOCOL.EQ (TCP) konfigurieren, sodass der virtuelle Server nur TCP-Verkehr verarbeitet und einfach den gesamten Nicht-TCP-Verkehr überbrückt. Sie können zwar anstelle der Abhörrichtlinie eine Zugriffskontrollliste verwenden, die Abhörrichtlinie bietet jedoch eine bessere Kontrolle darüber, welcher Datenverkehr verarbeitet wird.
- Für virtuelle Content Switching-Server vom Typ ANY können Sie Inhaltswechselrichtlinien konfigurieren, die Anfragen auf der Grundlage des Protokolls in eingehenden Paketen umschalten. Sie können beispielsweise Content Switching-Richtlinien so konfigurieren, dass der gesamte TCP-Verkehr an einen virtuellen Lastausgleichsserver und der gesamte Nicht-TCP-Verkehr an einen anderen virtuellen Lastausgleichsserver weitergeleitet wird.
- Sie können die clientbasierten Ausdrücke verwenden, um die Persistenz auf der Grundlage des Protokolls zu konfigurieren. Beispielsweise können Sie CLIENT.IP.PROTOCOL verwenden, um die Persistenz auf der Grundlage der Protokolle in eingehenden IPv4-Paketen zu konfigurieren.

Ausdrücke für HTTP- und Cache-Control-Header

August 19, 2021

Eine gängige Methode zur Auswertung des HTTP-Datenverkehrs besteht darin, die Header in einer Anforderung oder einer Antwort zu untersuchen. Ein Header kann eine Reihe von Funktionen ausführen, einschließlich der folgenden:

- Geben Sie Cookies an, die Daten über den Absender enthalten.
- Identifizieren Sie den Datentyp, der übertragen wird.
- Identifizieren Sie die Route, die die Daten zurückgelegt haben (die Via Header).

> **Hinweis:**
>
> Wenn eine Operation verwendet wird, um Kopf- und Textdaten auszuwerten, überschreibt die kopfbasierte Operation immer den textbasierten Vorgang. Beispielsweise überschreibt die AFTER_STR-Operation, wenn sie auf einen Header angewendet wird, textbasierte AFTER_STR-Operationen für alle Instanzen des aktuellen Headertyps.

Präfixe für HTTP-Header

Die Tabelle Präfixe für HTTP-Header für Ausdruckspräfixe, die HTTP-Header extrahieren.

Operationen für HTTP-Header

Die Tabelle Operationen für HTTP-Header für Operationen, die Sie mit den Präfixen für HTTP-Header angeben können.

Präfixe für Cache-Control-Header

Die folgenden Präfixe gelten speziell für Cache-Control-Header.

HTTP-Header-Präfix	Beschreibung
HTTP.REQ.CACHE_CONTROL	Gibt einen Cache-Control-Header in einer HTTP-Anforderung zurück.
HTTP.RES.CACHE_CONTROL	Gibt einen Cache-Control-Header in einer HTTP-Antwort zurück.

Operationen für Cache-Control-Header

Sie können jede der Operationen für HTTP-Header auf Cache-Control-Header anwenden.

Darüber hinaus identifizieren die folgenden Vorgänge bestimmte Typen von Cache-Control-Headern. Informationen zu diesen Header-Typen finden Sie unter RFC 2616.

HTTP-Header-Vorgang	Beschreibung
`Cache-Control header.NAME(<integer>)`	Gibt als Textwert den Namen des Cache-Control-Headers zurück, der der n-ten Komponente in einer Name-Wert-Liste entspricht, wie von angegeben`<integer>`. Der Index der Name-Wert-Komponente ist 0-basiert. Wenn der Wert `<integer>`, der durch das Argument Integer angegeben wird, größer ist als die Anzahl der Komponenten in der Liste, wird ein leeres Textobjekt zurückgegeben. Es folgt ein Beispiel: `http.req.cache_control.name(3).contains("some_text")`
Cache-Control header.IS_INVALID	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header nicht in der Anforderung oder Antwort vorhanden ist. Es folgt ein Beispiel: `http.req.cache_control.is_invalid`
`Cache-Control header.IS_PRIVATE`	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Privat hat. Es folgt ein Beispiel: `http.req.cache_control.is_private`
Cache-Control header.IS_PUBLIC	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Privat hat. Es folgt ein Beispiel: http.req.cache_control.is_public
Cache-Control header.IS_NO_STORE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert No-Store hat. Es folgt ein Beispiel: http.req.cache_control.is_no_store
Cache-Control header.IS_NO_CACHE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert No-Cache hat. Es folgt ein Beispiel: http.req.cache_control.is_no_cache

HTTP-Header-Vorgang	Beschreibung
Cache-Control header.IS_MAX_AGE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Max-Age hat. Es folgt ein Beispiel: http.req.cache_control.is_max_age
Cache-Control header.IS_MIN_FRESH	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Min-Fresh hat. Es folgt ein Beispiel: http.req.cache_control.is_min_fresh
Cache-Control header.IS_MAX_STALE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Max-Stale hat. Es folgt ein Beispiel: http.req.cache_control.is_max_stale
Cache-Control header.IS_MUST_REVALIDATE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Must-Revalidate hat. Es folgt ein Beispiel: http.req.cache_control.is_must_revalidate
Cache-Control header.IS_NO_TRANSFORM	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert No-Transform hat. Es folgt ein Beispiel: http.req.cache_control.is_no_transform
Cache-Control header.IS_ONLY_IF_CACHED	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Only-If-Cached aufweist. Es folgt ein Beispiel: http.req.cache_control.is_only_if_cached
Cache-Control header.IS_PROXY_REVALIDATE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Proxy-Revalidate aufweist. Es folgt ein Beispiel: http.req.cache_control.is_proxy_revalidate
Cache-Control header.IS_S_MAXAGE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert S-Maxage hat. Es folgt ein Beispiel: http.req.cache_control.is_s_maxage
Cache-Control header.IS_UNKNOWN	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header einen unbekannten Typ hat. Es folgt ein Beispiel: http.req.cache_control.is_unknown

HTTP-Header-Vorgang	Beschreibung
Cache-Control header.MAX_AGE	Gibt den Wert des Cache-Control-Headers Max-Age zurück. Wenn dieser Header nicht vorhanden ist oder ungültig ist, wird 0 zurückgegeben. Es folgt ein Beispiel: http.req.cache_control.max_age.le(3)
Cache-Control header.MAX_STALE	Gibt den Wert des Cache-Control-Headers Max-Stale zurück. Wenn dieser Header nicht vorhanden ist oder ungültig ist, wird 0 zurückgegeben. Es folgt ein Beispiel: http.req.cache_control.max_stale.le(3)
Cache-Control header.MIN_FRESH	Gibt den Wert des Cache-Control-Headers Min-Fresh zurück. Wenn dieser Header nicht vorhanden ist oder ungültig ist, wird 0 zurückgegeben. Es folgt ein Beispiel: http.req.cache_control.min_fresh.le(3)
Cache-Control header.S_MAXAGE	Gibt den Wert des Cache-Control-Headers S-Maxage zurück. Wenn dieser Header nicht vorhanden oder ungültig ist, wird 0 zurückgesendet. Es folgt ein Beispiel: http.req.cache_control.s_maxage.eq(2)

Ausdrücke zum Extrahieren von URLs

August 19, 2021

Sie können URLs und Teile von URLs extrahieren, z. B. den Hostnamen oder ein Segment des URL-Pfads. Der folgende Ausdruck identifiziert beispielsweise HTTP-Anforderungen für Bilddateien, indem Bilddatei-Suffixe aus der URL extrahiert werden:

```
http.req.url.suffix.eq("jpeg")|| http.req.url.suffix.eq("gif")
```

Die meisten Ausdrücke für URLs arbeiten mit Text und werden unter Ausdruckspräfixe für Text in HTTP-Anfragen und Antwortenbeschrieben. In diesem Abschnitt wird die GET-Operation erläutert. Die GET-Operation extrahiert Text, wenn sie mit den folgenden Präfixen verwendet wird:

- HTTP.REQ.URL.PATH
- VPN.BASEURL.PATH

- VPN.CLIENTLESS_BASEURL.PATH

In der folgenden Tabelle werden Präfixe für HTTP-URLs beschrieben.

URL-Präfix	Beschreibung
HTTP.REQ.URL.PATH.GET (<n>)	Gibt einen Schrägstrich (/) getrennte Liste aus dem URL-Pfad zurück. Betrachten Sie beispielsweise die folgende URL:<`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`>. Der folgende Ausdruck gibt dir1 von dieser URL zurück:<`http.req.url.path.get(1)`>. Der folgende Ausdruck gibt dir2 zurück: http.req.url.path.get (2)
HTTP.REQ.URL.PATH.GET_REVERSE (<n>)	Gibt einen Schrägstrich (/) getrennte Liste vom URL-Pfad zurück, beginnend am Ende des Pfades. Betrachten Sie beispielsweise die folgende URL:<`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`>. Der folgende Ausdruck gibt index.html von dieser URL zurück:<`http.req.url.path.get_reverse(0)`>. Der folgende Ausdruck gibt dir3 zurück: http.req.url.path.get_reverse (1)

Ausdrücke für HTTP-Statuscodes und numerische HTTP-Nutzlastdaten außer Datumsangaben

January 19, 2021

In der folgenden Tabelle werden Präfixe für numerische Werte in anderen HTTP-Daten als Datumsangaben beschrieben.

Prefix	Beschreibung
HTTP.REQ.CONTENT_LENGTH	Gibt die Länge einer HTTP-Anforderung als Zahl zurück. Es folgt ein Beispiel: http.req.content_length < 500
HTTP.RES.CONTENT_LENGTH	Gibt die Länge der HTTP-Antwort als Zahl zurück. Es folgt ein Beispiel: http.res.content_length <= 1000
HTTP.RES.STATUS	Gibt den Antwortstatuscode zurück
HTTP.RES.IS_REDIRECT	Gibt einen booleschen TRUE zurück, wenn der Antwortcode einer Umleitung zugeordnet ist. Im Folgenden sind die Redirect-Antwortcodes: 300 (Multiple Choices), 301 (Permanent verschoben), 302 (Found), 303 (Siehe Andere), 305 (Proxy verwenden) und 307 (Temporäre Umleitung). Hinweis: Statuscode 304 gilt nicht als Umleitungs-HTTP-Antwortstatuscode. Statuscode 306 wird nicht verwendet.

SIP-Ausdrücke

May 11, 2023

Die Sprache für Richtlinienausdrücke von NetScaler Advanced enthält eine Reihe von Ausdrücken, die für SIP-Verbindungen (Session Initiation Protocol) verwendet werden. Diese Ausdrücke sollen in Richtlinien für jedes unterstützte Protokoll verwendet werden, das auf Anforderungs-/Antwortbasis arbeitet. Diese Ausdrücke können für Content Switching, Ratenbegrenzung, Responder und Umschreibrichtlinien verwendet werden.

Für SIP-Ausdrücke, die in Responder-Richtlinien verwendet werden, gelten bestimmte Einschränkungen. Auf einem virtuellen SIP-Lastausgleichsserver sind nur die Aktionen DROP, NOOP oder RESPONDWITH zulässig. Responder-Richtlinien können an einen virtuellen Lastausgleichsserver, einen globalen Override-Bindpunkt, einen globalen Standardbindpunkt oder ein sip_uddp-Richtlinienlabel gebunden werden.

Das vom SIP-Protokoll verwendete Header-Format ähnelt dem des HTTP-Protokolls, sodass viele der neuen Ausdrücke ähnlich wie ihre HTTP-Analoga aussehen und funktionieren. Jeder SIP-Header besteht aus einer Zeile, die die SIP-Methode, die URL und die Version enthält, gefolgt von einer Reihe von Name-Wert-Paaren, die wie HTTP-Header aussehen.

Im Folgenden finden Sie ein Beispiel für einen SIP-Header, auf den in den folgenden Ausdruckstabellen verwiesen wird:

```
INVITE sip:16@www.sip.com:5060;transport=udp SIP/2.0
Record-Route: <sip:200.200.100.22;lr=on>
Via: SIP/2.0/UDP 200.200.100.22;branch=z9hG4bK444b.c8e103d1.0;rport
   =5060;
    received=10.102.84.18
Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;
    received=10.102.84.160
From: "12" <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53
   cc0185
To: "16" <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185
Call-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180
Max-Forwards: 69CSeq: 101 INVITE
User-Agent: Cisco-CP7940G/8.0
Contact: <sip:12@10.102.84.180:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces,join,norefersub
Content-Length: 277
Content-Type: application/sdp
Content-Disposition: session;handling=optiona
<!--NeedCopy-->
```

SIP-Referenztabellen

Die folgenden Tabellen enthalten Listen von Ausdrücken, die auf SIP-Headern ausgeführt werden. Die erste Tabelle enthält Ausdrücke, die für Anforderungsheader gelten. Die meisten antwortbasierten Ausdrücke sind fast identisch mit den entsprechenden anforderungsbasierten Ausdrücken. Um einen Antwortausdruck aus dem entsprechenden Anforderungsausdruck zu erstellen, ändern Sie die ersten beiden Abschnitte des Ausdrucks von SIP.REQ in SIP.RES und nehmen weitere offensichtliche Anpassungen vor. Die zweite Tabelle enthält die Antwortausdrücke, die nur für Antworten gelten und für die es keine Anforderungsäquivalente gibt. Sie können jedes Element in den folgenden Tabellen als eigenständigen vollständigen Ausdruck verwenden, oder Sie können verschiedene Operatoren verwenden, um diese Ausdruckselemente mit anderen zu kombinieren, um komplexere Ausdrücke zu bilden.

SIP-Anforderungsausdrücke

Ausdruck	Beschreibung
SIP.REQ.METHOD	Arbeitet nach der Methode der SIP-Anfrage. Die unterstützten SIP-Anforderungsmethoden sind ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE und UPDATE. Dieser Ausdruck ist eine Ableitung der Textklasse, sodass alle Operationen, die auf Text anwendbar sind, auf diese Methode anwendbar sind. Beispielsweise gibt dieser Ausdruck für eine SIP-Anfrage von INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0 das Ergebnis INVITE zurück.
SIP.REQ.URL	Arbeitet mit der SIP-Anforderungs-URL. Dieser Ausdruck ist eine Ableitung der Textklasse, sodass alle Operationen, die auf Text anwendbar sind, auf diese Methode anwendbar sind. For example, for a SIP request of INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0, this expression re-turnssip:16@10.102.84.181:5060;transport=udp.
SIP.REQ.URL.PROTOCOL	Gibt das URL-Protokoll zurück. For example, for a SIP URL ofsip:16@www.sip.com:5060;transport=udp, this expression returns sip.
SIP.REQ.URL.HOSTNAME	Gibt den Hostnamen-Teil der SIP-URL zurück. For example, for a SIP URL ofsip:16@www.sip.com:5060;transport=udp, this expression returns www.sip.com:5060.
SIP.REQ.URL.HOSTNAME.PORT	Gibt den Port-Teil des SIP-URL-Hostnamens zurück. Wenn kein Port angegeben ist, gibt dieser Ausdruck den Standard-SIP-Port 5060 zurück. For example, for a SIP hostname of www.sip.com:5060, this expression returns 5060.

Ausdruck	Beschreibung
SIP.REQ.URL.HOSTNAME.DOMAIN	Gibt den Teil des Domainnamens des SIP-URL-Hostnamens zurück. Wenn der Host eine IP-Adresse ist, gibt dieser Ausdruck ein falsches Ergebnis zurück. Für den SIP-Hostnamen www.sip.com:5060 gibt dieser Ausdruck beispielsweise sip.com zurück. Für einen SIP-Hostnamen von 192.168.43. 15:5060 gibt dieser Ausdruck einen Fehler zurück.
SIP.REQ.URL.HOSTNAME.SERVER	Gibt den Serverteil des Hosts zurück. Für den SIP-Hostnamen www.sip.com:5060 gibt dieser Ausdruck beispielsweise www zurück.
SIP.REQ.URL.USERNAME	Gibt den Benutzernamen zurück, der dem Zeichen @ vorangeht. Für eine SIP-URL von sip: 16@www.sip.com:5060; transport=udp gibt dieser Ausdruck 16 zurück.
SIP.REQ.VERSION	Gibt die SIP-Versionsnummer in der Anfrage zurück. For example, for a SIP request of INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0, this expression returns SIP/2.0.
SIP.REQ.VERSION.MAJOR	Gibt die Hauptversionsnummer zurück (die Zahl links neben dem Punkt). Für eine SIP-Versionsnummer von SIP/2.0 gibt dieser Ausdruck beispielsweise 2 zurück.
SIP.REQ.VERSION.MINOR	Gibt die Nebenversionsnummer zurück (die Zahl rechts neben dem Punkt). Für eine SIP-Versionsnummer von SIP/2.0 gibt dieser Ausdruck beispielsweise 0 zurück.
SIP.REQ.CONTENT_LENGTH	Gibt den Inhalt des Content-Length-Headers zurück. Dieser Ausdruck ist eine Ableitung der Klasse sip_header_t, sodass alle Operationen verwendet werden können, die für SIP-Header verfügbar sind. Für einen SIP-Content-Length-Header mit Content-Length: 277 gibt dieser Ausdruck beispielsweise 277 zurück.

Ausdruck	Beschreibung
SIP.REQ.TO	Gibt den Inhalt des To Headers zurück. Beispiel: Bei einem SIP To-Header von To: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185 zurück.
SIP.REQ.TO.ADDRESS	Gibt die SIP-URI zurück, die sich im Objekt sip_url befindet. Alle Operationen, die für SIP-URIs verfügbar sind, können verwendet werden. Beispiel: Bei einem SIP To-Header von To: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck sip:16@sip_example.com zurück.
SIP.REQ.TO.DISPLAY_NAME	Gibt den Teil des Anzeigenamens des To -Headers zurück. Beispiel: Bei einem SIP To-Header von To: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck 16 zurück.
SIP.REQ.TO.TAG	Gibt den Wert des Tags aus dem “Tag”-Namen-Wertepaar im TO-Header zurück. Beispiel: Bei einem SIP To-Header von To: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck 00127f54ec85a6d90cc14f45-53cc0185 zurück.
SIP.REQ.FROM	Gibt den Inhalt des Frod-Headers zurück. For example, for a SIP From header of From: “12” <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, this expression returns sip:12@sip_example.com.

Ausdruck	Beschreibung
SIP.REQ.FROM.ADDRESS	Gibt die SIP-URI zurück, die sich im Objekt sip_url befindet. Alle Operationen, die für SIP-URIs verfügbar sind, können verwendet werden. For example, for a SIP From header of From: “12” <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, this expression returns sip:12@sip_example.com.
SIP.REQ.FROM.DISPLAY_NAME	Gibt den Teil des Anzeigenamens des To -Headers zurück. For example, for a SIP From header of From: “12” <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, this expression returns 12.
SIP.REQ.FROM.TAG	Gibt den Wert des Tags aus dem “Tag”-Namen-Wertepaar im TO-Header zurück. For example, for a SIP From header of From: “12” <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, this expression returns 00127f54ec85a6d90cc14f45-53cc0185.
SIP.REQ.VIA	Gibt den vollständigen Via-Header zurück. Wenn die Anfrage mehrere Via-Header enthält, wird der letzte Via-Header zurückgegeben. Für die beiden Via-Header im Beispiel-SIP-Header gibt dieser Ausdruck beispielsweise Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re zurück.
SIP.REQ.VIA.SENTBY_ADDRESS	Gibt die Adresse zurück, von der die Anfrage gesendet wurde. For example, for the Via header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re this expression returns 10.102.84.180.

Ausdruck	Beschreibung
SIP.REQ.VIA.SENTBY_PORT	Gibt den Port zurück, der die Anfrage gesendet hat. For example, for the Via header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re this expression returns 5060.
SIP.REQ.VIA.RPORT	Gibt den Wert aus dem Paar Name/Wert des Berichts zurück. For example, for the Via header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re this expression returns 5060.
SIP.REQ.VIA.BRANCH	Gibt den Wert aus dem Zweigname/Wertepaar zurück. For example, for the Via header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re this expression returns z9hG4bK03e76d0b.
SIP.REQ.VIA.RECEIVED	Gibt den Wert aus dem empfangenen Name-Wert-Paar zurück. For example, for the Via header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re this expression returns 10.102.84.160.
SIP.REQ.CALLID	Gibt den Inhalt des Callid-Headers zurück. Dieser Ausdruck ist eine Ableitung der Klasse sip_header_t, sodass alle Operationen verwendet werden können, die für SIP-Header verfügbar sind. For example, for a SIP Callid header ofCall-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180, this expression returns00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180.
SIP.REQ.CSEQ	Gibt die CSEQ-Nummer aus dem CSEQ als Ganzzahl zurück. Für einen SIP-CSEQ-Header von CSeq: 101 INVITE gibt dieser Ausdruck beispielsweise 101 zurück.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>)	Gibt den angegebenen SIP-Header zurück. Ersetzen Sie <header_name> durch den Namen des gewünschten Headers. Um beispielsweise den SIP From-Header zurückzugeben, geben Sie SIP.REQ.HEADER(“From”) ein.
SIP.REQ.HEADER(\<header_name>).INSTANCE(\)	Gibt die angegebene Instanz des angegebenen SIP-Headers zurück. Es können mehrere Instanzen desselben SIP-Headers auftreten. Wenn Sie eine bestimmte Instanz eines solchen SIP-Headers benötigen (z. B. einen bestimmten Via-Header), können Sie diesen Header angeben, indem Sie eine Zahl als die eingeben<line_number>. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet. In other words, SIP.REQ.HEADER(“Via”).INSTANCE(0) returns the last instance of the Via header, while SIP.REQ.HEADER(“Via”).INSTANCE(1) returns the last instance but one of the Via header, and so on. For example, if used on the example SIP header, SIP.REQ.HEADER(“Via”).INSTANCE(1) returnsVia: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060.
SIP.REQ.HEADER(\<header_name>).VALUE(\)	Gibt den Inhalt der angegebenen Instanz des angegebenen SIP-Headers zurück. Die Verwendung ist fast dieselbe wie beim vorherigen Ausdruck. For example, if used on the SIP header example in the preceding table entry, SIP.REQ.HEADER(“Via”).VALUE(1) returns SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).COUNT	Gibt die Anzahl der Instanzen eines bestimmten Headers als Ganzzahl zurück. Wenn es beispielsweise im obigen SIP-Header-Beispiel verwendet wird, gibt SIP.REQ.HEADER(“Via”).COUNT den Wert 2 zurück.
SIP.REQ.HEADER(<header_name>).EXISTS	Gibt den booleschen Wert true oder false zurück, je nachdem, ob der angegebene Header existiert oder nicht. Wenn es beispielsweise im obigen SIP-Header-Beispiel verwendet wird, gibt SIP.REQ.HEADER(“Expires”).EXISTS den Wert true zurück, während SIP.REQ.HEADER(“Caller-ID”).EXISTS den Wert false zurückgibt.
SIP.REQ.HEADER(<header_name>).LIST	Gibt die kommagetrennte Parameterliste im angegebenen Header zurück. Wenn SIP.REQ.HEADER(“Allow”).LIST beispielsweise für das obige SIP-Header-Beispiel verwendet wird, gibt sie ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,U zurück. Sie können die Zeichenfolge .GET (<list_item_number>) anhängen, um ein bestimmtes Listenelement auszuwählen. Um beispielsweise das erste Element (ACK) aus der obigen Liste abzurufen, geben Sie SIP.REQ.HEADER(“Allow”).LIST.GET(0) ein. Um das zweite Element (BYE) zu extrahieren, geben Sie SIP.REQ.HEADER(“Allow”).LIST.GET(1) ein. Hinweis: Wenn der angegebene Header eine Liste von Name-Wert-Paaren enthält, wird das gesamte Name-Wert-Paar zurückgegeben.

Ausdruck	Beschreibung
SIP.REQ.HEADER(\<header_name>).TYPECAST_S	Typecasts <header_name> to <in_header_name>. Jeder Text kann in die Klasse sip_header_t eingegeben werden. Danach können alle Header-basierten Operationen verwendet werden. Nachdem Sie diesen Vorgang ausgeführt haben, können Sie alle Operationen anwenden, die mit verwendet werden können<in_header_name>. Der Ausdruck SIP.REQ.CONTENT_LENGTH.TYPECAST_SIP_HEADER_T typisiert beispielsweise alle Instanzen des Content-Length-Headers. Nachdem Sie diesen Vorgang ausgeführt haben, können Sie alle Header-Operationen auf alle Instanzen des angegebenen Headers anwenden.
SIP.REQ.HEADER(<header_name>).CONTAINS(<string>)	Gibt boolean true zurück, wenn die angegebene Textzeichenfolge in einer Instanz des angegebenen Headers vorhanden ist. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).EQUALS_ANY	Gibt den booleschen Wert true zurück, wenn ein mit <patset> verknüpftes Muster mit dem Inhalt in einer Instanz des angegebenen Headers übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).CONTAINS_ANY(<patset>)	Gibt den booleschen Wert true zurück, wenn ein mit <patset> verknüpftes Muster mit dem Inhalt in einer Instanz des angegebenen Headers übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).CONTAINS_IN	Gibt den Index des übereinstimmenden Musters zurück, das mit <patset> verknüpft ist, wenn dieses Muster mit dem Inhalt in einer Instanz des angegebenen Headers übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).EQUALS_INDEX(<patset>)	Gibt den Index des übereinstimmenden Musters zurück, das mit <patset> verknüpft ist, wenn dieses Muster mit einer Instanz des angegebenen Headers übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).SUBSTR(<stri	Wenn die angegebene Zeichenfolge in einer Instanz des angegebenen Headers vorhanden ist, gibt dieser Ausdruck diese Zeichenfolge zurück. For example, for the SIP header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re returns “rport=5060”.SIP.REQ.HEADER(“Via”).SUBSTR(“rport=5061”) returns an empty string.
SIP.REQ.HEADER(<header_name>).AFTER_STR(<string>)	Wenn die angegebene Zeichenfolge in einer Instanz des angegebenen Headers vorhanden ist, gibt dieser Ausdruck die Zeichenfolge unmittelbar hinter dieser Zeichenfolge zurück. For example, for the SIP header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re the expression SIP.REQ.HEADER(“Via”).AFTER_STR(“rport=”) returns 5060.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).REGEX_MATC	Gibt boolean true zurück, wenn der angegebene reguläre Ausdruck (Regex) mit einer Instanz des angegebenen Headers übereinstimmt. Sie müssen den regulären Ausdruck im folgenden Format angeben: re<delimiter>regular expression<same delimiter>. Der reguläre Ausdruck darf nicht länger als 1499 Zeichen sein. Es muss der PCRE-Bibliothek für reguläre Ausdrücke entsprechen. Dokumentation http://www.pcre.org/pcre.txt zur Syntax regulärer PCRE-Ausdrücke finden Sie unter. Die pcrepattern-Manpage enthält auch nützliche Informationen zur Spezifizierung von Mustern mithilfe regulärer PCRE-Ausdrücke. Die in diesem Ausdruck unterstützte Syntax regulärer Ausdrücke weist einige Unterschiede zu PCRE auf. Rückverweise sind nicht zulässig. Sie sollten rekursive reguläre Ausdrücke vermeiden. Obwohl einige funktionieren, funktionieren viele nicht. Das Metazeichen Punkt (.) entspricht Zeilenumbrüchen. Unicode wird nicht unterstützt.set_text_mode (IGNORECASE) überschreibt das (? i) interne Option, die im regulären Ausdruck angegeben ist.
SIP.REQ.HEADER(<header_name>).REGEX_SELECT(<regex>)	Wenn die angegebene Regex mit einem beliebigen Text in einer Instanz der angegebenen Kopfzeile übereinstimmt, gibt dieser Ausdruck den Text zurück. Zum Beispiel für den SIP-Header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re gibt der Ausdruck SIP.REQ.HEADER(“Via”).REGEX_SELECT(“received=[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}”) Folgendes zurück: received=10.102.84.160.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).AFTER_REGE	Wenn der angegebene Regex mit einem Text in einer beliebigen Instanz des angegebenen Headers übereinstimmt, gibt dieser Ausdruck die Zeichenfolge unmittelbar nach diesem Text zurück. Für den SIP-Header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re gibt der Ausdruck SIP.REQ.HEADER(“Via”).AFTER_REGEX(“received=”) Folgendes zurück: 10.102.84.160.
SIP.REQ.HEADER(<header_name>).BEFORE_REGEX(<regex>)	Wenn der angegebene Regex mit einem Text in einer beliebigen Instanz des angegebenen Headers übereinstimmt, gibt dieser Ausdruck die Zeichenfolge unmittelbar vor diesem Text zurück. Zum Beispiel für den SIP-Header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re gibt der Ausdruck SIP.REQ.HEADER(“Via”).BEFORE_REGEX(“[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}”) Folgendes zurück: received=.
SIP.REQ.FULL_HEADER	Gibt den gesamten SIP-Header zurück, einschließlich des abschließenden CR/LF.
SIP.REQ.IS_VALID	Gibt den booleschen Wert true zurück, wenn das Anforderungsformat gültig ist.
SIP.REQ.BODY(<length>)	Gibt den Anforderungstext bis zur angegebenen Länge zurück. Wenn die angegebene Länge größer als die Länge des Anforderungstexts ist, gibt dieser Ausdruck den gesamten Anforderungstext zurück.
SIP.REQ.LB_VSERVER	Gibt den Namen des virtuellen Load-Balancing-Servers (LB vserver) zurück, der die aktuelle Anfrage bedient.
SIP.REQ.CS_VSERVER	Gibt den Namen des virtuellen Content Switching-Servers (CS vserver) zurück, der die aktuelle Anfrage bedient.

SIP-Antwortausdrücke

Ausdruck	Beschreibung
SIP.RES.STATUS	Gibt den SIP-Antwortstatuscode zurück. Wenn die erste Zeile der Antwort beispielsweise SIP/2.0 100 Trying lautet, gibt dieser Ausdruck 100 zurück.
SIP.RES.STATUS_MSG	Gibt die SIP-Antwortstatusmeldung zurück. Lautet die erste Zeile der Antwort beispielsweise SIP/2.0 100 Trying, gibt dieser Ausdruck Trying zurück.
SIP.RES.IS_REDIRECT	Gibt den booleschen Wert true zurück, wenn der Antwortcode eine Weiterleitung ist.
SIP.RES.METHOD	Gibt die Antwortmethode zurück, die aus der Anforderungsmethodenzeichenfolge im CSEq-Header extrahiert wurde.

Operationen für HTTP-, HTML- und XML-Kodierung und „sichere“ Zeichen

May 11, 2023

Die folgenden Operationen funktionieren mit der Kodierung von HTML-Daten in einer Anfrage oder Antwort und mit XML-Daten in einem POST-Text.

- **<text>.HTML_XML_SAFE:**
  Transformiert Sonderzeichen in ein sicheres XML-Format, wie in den folgenden Beispielen:

  Eine nach links zeigende Winkelklammer (<) wird in < umgewandelt Eine nach rechts zeigende Winkelklammer (>)
  wird in > Ein kaufmännisches Und-Zeichen (&) umgewandelt wird
  in & Diese Operation schützt vor
  Cross-Site-Scripting-Angriffen. Die maximale Länge des transformierten Textes beträgt 2048 Byte. Dies ist ein schreibgeschützter Vorgang.

  Nach dem Anwenden der Transformation werden zusätzliche Operatoren, die Sie im Ausdruck angeben, auf den ausgewählten Text angewendet. Es folgt ein Beispiel:

  http.req.url.query.html_xml_safe. enthält („myQueryString“)

- **<text>.HTTP_HEADER_SAFE:**
  Konvertiert alle Neue-Zeile-Zeichen (‘\n’) im eingegebenen Text in ‘%0A’, damit die Eingabe sicher in HTTP-Headern verwendet werden kann.

  Diese Operation schützt vor Angriffen, bei denen die Reaktion aufgeteilt wird.

  Die maximale Länge des transformierten Textes beträgt 2048 Byte. Dies ist ein schreibgeschützter Vorgang.

- **<text>.HTTP_URL_SAFE:**
  Konvertiert unsichere URL-Zeichen in ‘%xx’-Werte, wobei “xx” eine hexadezimale Darstellung des Eingabezeichens ist. Beispielsweise wird das Ampersand (&) in der URL-sicheren Kodierung als %26 dargestellt. Die maximale Länge des transformierten Textes beträgt 2048 Byte. Dies ist ein schreibgeschützter Vorgang.

  Im Folgenden finden Sie URL-sichere Zeichen. Alle anderen sind unsicher:

  - Alphanumerische Zeichen: a-z, A-Z, 0-9
  - Sternchen: „*“
  - Ampersand: „&“
  - AT-Zeichen: „@“
  - Doppelpunkt: „:“
  - Komma: „,“
  - Dollar: „$“
  - Punkt:“. „
  - Entspricht: „=“
  - Ausrufezeichen: „! „
  - Bindestrich: „-“
  - Klammern öffnen und schließen: „(„, „)“
  - Prozent: „%“
  - Plus: „+“
  - Semikolon: „;“
  - Einfaches Anführungszeichen: „’“
  - Schrägstrich: „/“
  - Fragezeichen: „? „
  - Tilde: „~“
  - Unterstrich: „_“

- **<text>.MARK_SAFE:**

  Markiert den Text als sicher, ohne irgendeine Art von Datentransformation anzuwenden.

- **<text>.SET_TEXT_MODE(URLENCODED|NOURLENCODED)**

  Transformiert die gesamte %HH-Kodierung im Bytestream. Diese Operation funktioniert mit Zeichen (nicht mit Bytes). Standardmäßig steht ein einzelnes Byte für ein Zeichen in ASCII-

Codierung. Wenn Sie jedoch den URLENCODED-Modus angeben, können drei Byte ein Zeichen darstellen.

Im folgenden Beispiel wählt eine PREFIX (3) -Operation die ersten 3 Zeichen in einem Ziel aus.

```
http.req.url.hostname.prefix(3)
```

Im folgenden Beispiel kann der NetScaler bis zu 9 Byte aus dem Ziel auswählen:

```
http.req.url.hostname.set_text_mode(urlencoded).prefix(3)
```

- **<text>.SET_TEXT_MODE(PLUS_AS_SPACE|NO_PLUS_AS_SPACE):**

  Gibt an, wie das Pluszeichen (+) behandelt wird. Die Option PLUS_AS_SPACE ersetzt ein Pluszeichen durch Leerzeichen. Zum Beispiel wird aus dem Text „Hallo+Welt“ „Hallo Welt“. „ Die Option NO_PLUS_AS_SPACE lässt Pluszeichen so, wie sie sind.

- **<text>.SET_TEXT_MODE(BACKSLASH_ENCODED|NO_BACKSLASH_ENCODED):**

  Gibt an, ob für das durch <text> dargestellte Textobjekt eine Backslash-Dekodierung durchgeführt wird.

  Wenn BACKSLASH_ENCODED angegeben ist, führt der SET_TEXT_MODE-Operator die folgenden Operationen für das Textobjekt aus:

  - Jedes Vorkommen von „\ XXX“ wird durch das Zeichen „Y“ ersetzt (wobei XXX für eine Zahl im Oktalsystem und Y für das ASCII-Äquivalent von XXX steht). Der gültige Bereich von Oktalwerten für diese Art der Kodierung liegt zwischen 0 und 377. Beispielsweise werden der codierte Text „http\ 72//“ und „http\ 072//“ beide dekodiert <http://>, wobei der Doppelpunkt (:) das ASCII-Äquivalent des Oktalwerts „72” ist.
  - Jedes Vorkommen von „\ xHH“ wird durch das Zeichen „Y“ ersetzt (HH steht für eine Zahl im Hexadezimalsystem und Y steht für das ASCII-Äquivalent von HH). Zum Beispiel wird der codierte Text „http\ x3a//“ dekodiert <http://>, wobei der Doppelpunkt (:) das ASCII-Äquivalent des Hexadezimalwerts „3a“ ist.
  - Jedes Vorkommen von „\ uWWxx“ wird durch die Zeichenfolge „YZ“ ersetzt (wobei WW und XX für zwei verschiedene Hexadezimalwerte stehen und Y und Z ihre ASCII-Äquivalente von WW bzw. XX darstellen). Zum Beispiel werden die codierten Texte „http%u3a2f/“ und „http%u003a//“ beide dekodiert, wobei „3a“ und „2f“ zwei Hexadezimalwerte sind und der Doppelpunkt (:) und der Schrägstrich („/“) jeweils ihre ASCII-Entsprechungen darstellen. <http://>
  - Alle Vorkommen von „\ b“, „\ n“, „\ t“, „\ f“ und „\ r“ werden durch die entsprechenden ASCII-Zeichen ersetzt.

  Wenn NO_BACKSLASH_ENCODED angegeben ist, wird für das Textobjekt keine Backslash-Dekodierung durchgeführt.

- **<text>.SET_TEXT_MODE(BAD_ENCODE_RAISE_UNDEF|NO_BAD_ENCODE_RAISE_UNDEF):**

Führt die zugehörige undefinierte Aktion aus, wenn entweder der URLENCODED- oder der BACKSLASH_ENCODED-Modus eingestellt ist und in dem durch <text> dargestellten Textobjekt eine schlechte Codierung gefunden wird, die dem angegebenen Kodierungsmodus entspricht.

Wenn NO_BAD_ENCODE_RAISE_UNDEF angegeben ist, wird die zugehörige undefinierte Aktion nicht ausgeführt, wenn das durch<text> dargestellte Textobjekt fehlerhafte Codierung enthält.

Ausdrücke für TCP-, UDP- und VLAN-Daten

May 11, 2023

TCP- und UDP-Daten haben die Form einer Zeichenfolge oder einer Zahl. Für Ausdruckspräfixe, die Zeichenfolgenwerte für TCP- und UDP-Daten zurückgeben, können Sie beliebige textbasierte Vorgänge anwenden. Weitere Informationen finden Sie unter Erweiterte Richtlinienausdrücke: Text auswerten.

Für Ausdruckspräfixe, die numerischen Wert zurückgeben, z. B. einen Quellport, können Sie eine arithmetische Operation anwenden. Weitere Informationen finden Sie unter Grundlegende Operationen für Ausdruckspräfixe und Zusammengesetzte Operationen für Zahlen.

In der folgenden Tabelle werden Präfixe beschrieben, die TCP- und UDP-Daten vom Client extrahieren.

GET-Operation	Beschreibung
CLIENT.TCP.PAYLOAD(<integer>)	Gibt TCP-Payload-Daten als Zeichenfolge zurück, die mit dem ersten Zeichen in der Nutzlast beginnt und bis zur Anzahl der Zeichen im <integer> Argument fortgesetzt wird. Sie können jede textbasierte Operation auf dieses Präfix anwenden.
CLIENT.TCP.SRCPORT	Gibt die ID des Quellports des aktuellen Pakets als Zahl zurück.
CLIENT.TCP.DSTPORT	Gibt die ID des Zielports des aktuellen Pakets als Zahl zurück.

GET-Operation	Beschreibung
CLIENT.TCP.OPTIONS	Gibt die vom Client festgelegten TCP-Optionen zurück. Beispiele für TCP-Optionen sind Maximum Segment Size (MSS), Window Scale, Selective Acknowledgements (SACK) und Time Stamp Option. Die Operatoren COUNT, TYPE(<type>) und TYPE_NAME(<m>) können mit diesem Präfix verwendet werden. Die vom Server festgelegten TCP-Optionen finden Sie im Präfix SERVER.TCP.OPTIONS.
CLIENT.TCP.OPTIONS.COUNT	Gibt die Anzahl der TCP-Optionen zurück, die der Client festgelegt hat.
CLIENT.TCP.OPTIONS.TYPE(<type>)	Gibt den Wert der TCP-Option zurück, deren Typ (oder Optionstyp) als Argument angegeben ist. Der Wert wird als Bytefolge im Big-Endian-Format (oder Netzwerk-Byte-Reihenfolge) zurückgegeben. Parameter: Typ - Typwert
CLIENT.TCP.OPTIONS.TYPE_NAME(<m>)	Gibt den Wert der TCP-Option zurück, deren Aufzählungskonstante als Argument angegeben ist. Die Aufzählungskonstanten, die Sie als Argument übergeben können, sind REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW und MAXSEG. Verwenden Sie CLIENT.TCP.OPTIONS.TYPE(<type>), um die Art der TCP-Option anstelle dieser Aufzählungskonstanten anzugeben. Für andere TCP-Optionen müssen Sie CLIENT.TCP.OPTIONS.TYPE(<type>) verwenden. Parameter: m - Aufzählungskonstante für TCP-Optionen
CLIENT.TCP.REPEATER_OPTION.EXISTS	Gibt den booleschen Wert TRUE zurück, wenn Repeater-TCP-Optionen existieren.
CLIENT.TCP.REPEATER_OPTION.IP	Gibt die IPv4-Adresse des Branch Repeaters aus den TCP-Optionen des Repeaters zurück.
CLIENT.TCP.REPEATER_OPTION.MAC	Gibt die MAC-Adresse des Branch Repeaters aus den TCP-Optionen des Repeaters zurück.

GET-Operation	Beschreibung
CLIENT.UDP.DNS.DOMAIN	Gibt den DNS-Domainnamen zurück.
CLIENT.UDP.DNS.DOMAIN.EQ(“<hostname>”)	Gibt den booleschen Wert TRUE zurück, wenn der Domänenname mit dem Argument <hostname> übereinstimmt. Bei dem Vergleich wird die Groß- und Kleinschreibung nicht berücksichtigt. Es folgt ein Beispiel: client.udp.dns.domain.eq („www.mycompany.com“)
CLIENT.UDP.DNS.IS_AAAAREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatztyp AAAA ist. Diese Arten von Datensätzen geben eine IPv6-Adresse bei Forward-Lookups an.
CLIENT.UDP.DNS.IS_ANYREC	Gibt den booleschen Wert TRUE zurück, wenn es sich um einen beliebigen Datensatztyp handelt.
CLIENT.UDP.DNS.IS_AREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatz vom Typ A ist. Datensätze vom Typ A geben die Hostadresse an.
CLIENT.UDP.DNS.IS_CNAMEREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatz vom Typ CNAME ist. In Systemen, die mehrere Namen verwenden, um eine Ressource zu identifizieren, gibt es einen kanonischen Namen und eine Reihe von Aliasen. Der CNAME liefert den kanonischen Namen.
CLIENT.UDP.DNS.IS_MXREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatz vom Typ MX (Mail Exchanger) ist. Dieser DNS-Eintrag beschreibt eine Priorität und einen Hostnamen. Die MX-Einträge für denselben Domainnamen geben die E-Mail-Server in der Domain und die Priorität für jeden Server an.

GET-Operation	Beschreibung
CLIENT.UDP.DNS.IS_NSREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatz vom Typ NS ist. Dies ist ein Nameserver-Datensatz, der einen Hostnamen mit einem zugehörigen A-Record enthält. Dies ermöglicht das Auffinden des Domainnamens, der dem NS-Eintrag zugeordnet ist.
CLIENT.UDP.DNS.IS_PTRREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatz vom Typ PTR ist. Dies ist ein Domainnamenzeiger und wird häufig verwendet, um einen Domainnamen mit einer IPv4-Adresse zu verknüpfen.
CLIENT.UDP.DNS.IS_SOAREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatz vom Typ SOA ist. Dies ist der Beginn des Autoritätsauftrags.
CLIENT.UDP.DNS.IS_SRVREC	Gibt den booleschen Wert TRUE zurück, wenn der Datensatz vom Typ SRV ist. Dies ist eine allgemeinere Version des MX-Eintrags.
CLIENT.UDP.DSTPORT	Gibt die numerische ID des UDP-Zielports des aktuellen Pakets zurück.
CLIENT.UDP.SRCPORT	Gibt die numerische ID des UDP-Quellports des aktuellen Pakets zurück.
CLIENT.UDP.LENGTH	Gibt die numerische ID der UDP-Länge des aktuellen Pakets zurück.
CLIENT.UDP.CHECKSUM	Gibt die numerische ID der UDP-Prüfsumme des aktuellen Pakets zurück.
CLIENT.UDP.PAYLOAD	Gibt die UDP-Payload des aktuellen Pakets zurück.
CLIENT.UDP.RADIUS	Gibt RADIUS-Daten für das aktuelle Paket zurück.
CLIENT.UDP.RADIUS.ATTR_TYPE(<type>)	Gibt den Wert für den als Argument angegebenen Attributtyp zurück.
CLIENT.UDP.RADIUS.USERNAME	Gibt den RADIUS-Benutzernamen zurück.
CLIENT.TCP.MSS	Gibt die maximale Segmentgröße (MSS) für die aktuelle Verbindung als Zahl zurück.

GET-Operation	Beschreibung
CLIENT.VLAN.ID	Gibt die numerische ID des VLAN zurück, über das das aktuelle Paket in den NetScaler gelangt ist.

In der folgenden Tabelle werden Präfixe beschrieben, die TCP- und UDP-Daten vom Server extrahieren.

GET-Operation	Beschreibung
SERVER.TCP.DSTPORT	Gibt die numerische ID des Zielports des aktuellen Pakets zurück.
SERVER.TCP.SRCPORT	Gibt die numerische ID des Quellports des aktuellen Pakets zurück.
SERVER.TCP.OPTIONEN	Gibt die vom Server festgelegten TCP-Optionen zurück. Beispiele für TCP-Optionen sind Maximum Segment Size (MSS), Window Scale, Selective Acknowledgements (SACK) und Time Stamp Option. Die Operatoren COUNT, TYPE(<type>) und TYPE_NAME(<m>) können mit diesem Präfix verwendet werden. Die vom Client festgelegten TCP-Optionen finden Sie im Präfix CLIENT.TCP.OPTIONS.
SERVER.TCP.OPTIONS.COUNT	Gibt die Anzahl der TCP-Optionen zurück, die der Server festgelegt hat.
SERVER.TCP.OPTIONS.TYPE(<type>)	Gibt den Wert der TCP-Option zurück, deren Typ (oder Optionstyp) als Argument angegeben ist. Der Wert wird als Bytefolge im Big-Endian-Format (oder Netzwerk-Byte-Reihenfolge) zurückgegeben. Parameter: Typ - Typwert

GET-Operation	Beschreibung
SERVER.TCP.OPTIONS.TYPE_NAME(<m>)	Gibt den Wert der TCP-Option zurück, deren Aufzählungskonstante als Argument angegeben ist. Die Aufzählungskonstanten, die Sie als Argument übergeben können, sind REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW und MAXSEG. Verwenden Sie CLIENT.TCP.OPTIONS.TYPE(<type>), um die Art der TCP-Option anstelle dieser Aufzählungskonstanten anzugeben. Für andere TCP-Optionen müssen Sie CLIENT.TCP.OPTIONS.TYPE(<type>) verwenden. Parameter: m - Aufzählungskonstante für TCP-Optionen
SERVER.VLAN	Funktioniert in dem VLAN, über das das aktuelle Paket in den NetScaler gelangt ist.
SERVER.UDP.DSTPORT	Gibt die numerische ID des UDP-Zielports des aktuellen Pakets zurück.
SERVER.UDP.SRCPORT	Gibt die numerische ID des UDP-Quellports des aktuellen Pakets zurück.
SERVER.UDP.LENGTH	Gibt die numerische ID der UDP-Länge des aktuellen Pakets zurück.
SERVER.UDP.CHECKSUM	Gibt die numerische ID der UDP-Prüfsumme des aktuellen Pakets zurück.
SERVER.UDP.PAYLOAD	Gibt die UDP-Payload des aktuellen Pakets zurück.
SERVER.VLAN.ID	Gibt die numerische ID des VLAN zurück, über das das aktuelle Paket in den NetScaler gelangt ist.

Ausdrücke zum Auswerten einer DNS-Nachricht und Identifizieren ihres Trägerprotokolls

January 25, 2022

Sie können DNS-Anfragen und -Antworten auswerten, indem Sie Ausdrücke verwenden, die mit DNS.REQ bzw. DNS.RES beginnen. Sie können auch das Transportschichtprotokoll identifizieren, das zum Senden der DNS-Nachrichten verwendet wird.

Die folgenden Funktionen geben den Inhalt einer DNS-Abfrage zurück.

Funktion	Beschreibung
DNS.REQ.QUESTION.DOMAIN	Gibt den Domainnamen (den Wert des Feldes QNAME) im Fragenabschnitt der DNS-Abfrage zurück. Der Domainname wird als Textzeichenfolge zurückgegeben, die an EQ (), NE () und alle anderen Funktionen, die mit Text arbeiten, übergeben werden kann.
DNS.REQ.QUESTION.TYPE	Gibt den Abfragetyp (den Wert des Feldes QTYPE) in der DNS-Abfrage zurück. Das Feld gibt den Typ des Ressourceneintrags an (z. B. A, NS oder CNAME), für den der Namenserver abgefragt wird. Der zurückgegebene Wert kann mit einem der folgenden Werte verglichen werden, indem die Funktionen EQ () und NE () verwendet werden: A, AAAA, NS, SRV, PTR, CNAME, SOA, MX und ANY. Hinweis: Sie können nur die Funktionen EQ () und NE () mit der Funktion TYPE verwenden. Beispiel: DNS.REQ.QUESTION.TYPE.EQ (MX)

Die folgenden Funktionen geben den Inhalt einer DNS-Antwort zurück.

Funktion	Beschreibung
DNS.RES.HEADER.RCODE	Gibt den Antwortcode (den Wert des RCODE-Feldes) im Header-Abschnitt der DNS-Antwort zurück. Sie können nur die Funktionen EQ () und NE () mit der Funktion RCODE verwenden. Es folgen die möglichen Werte: NOERROR, FORMERR, SERVFAIL, NXDOMAIN, NOTIMP und REFUSED.

Funktion	Beschreibung
DNS.RES.QUESTION.DOMAIN	Gibt den Domainnamen (den Wert des Feldes QNAME) im Fragenabschnitt der DNS-Antwort zurück. Der Domainname wird als Textzeichenfolge zurückgegeben, die an EQ (), NE () und alle anderen Funktionen, die mit Text arbeiten, übergeben werden kann.
DNS.RES.QUESTION.TYPE	Gibt den Abfragetyp (den Wert des Feldes QTYPE) im Fragenabschnitt der DNS-Antwort zurück. Das Feld gibt den Typ des Ressourceneintrags an (z. B. A, NS oder CNAME), der in der Antwort enthalten ist. Der zurückgegebene Wert kann mit einem der folgenden Werte verglichen werden, indem die Funktionen EQ () und NE () verwendet werden: A, AAAA, NS, SRV, PTR, CNAME, SOA, MX und ANY. Sie können nur die Funktionen EQ () und NE () mit der Funktion TYPE verwenden. Beispiel: DNS.RES.QUESTION.TYPE.EQ (SOA)

Die folgenden Funktionen geben den Protokollnamen der Transportschicht zurück.

Funktion	Beschreibung
DNS.REQ.TRANSPORT	Gibt den Namen des Transportschichtprotokolls zurück, das zum Senden der DNS-Abfrage verwendet wurde. Mögliche zurückgegebene Werte sind TCP und UDP. Sie können nur die Funktionen EQ () und NE () mit der Funktion TRANSPORT verwenden. Beispiel: DNS.REQ.TRANSPORT.EQ (TCP)
DNS.RES.TRANSPORT	Gibt den Namen des Transportschichtprotokolls zurück, das für die DNS-Antwort verwendet wurde. Mögliche zurückgegebene Werte sind TCP und UDP. Sie können nur die Funktionen EQ () und NE () mit der Funktion TRANSPORT verwenden. Beispiel: DNS.RES.TRANSPORT.EQ (TCP)

Die folgenden Funktionen geben den Namen des übereinstimmenden Speicherorts zurück, wenn die Abfrage die DNS-ECS-Option enthält oder nicht.

Funktion	Beschreibung
DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION	Gibt den Namen des übereinstimmenden Speicherorts zurück, der in der Abfrage mit der Option DNS ECS verwendet wurde. Beispiel :(DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION (“.CH… “)
client.ip.src.matches_location	Gibt den Namen des übereinstimmenden Speicherorts zurück, der in der Abfrage ohne die DNS-ECS-Option verwendet wurde. Beispiel: (Client.IP.src.Matches_Location (“.CH… “)
DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION ODER client.IP.SRC.Matches_LOCATION	Allgemeiner Ausdruck, der in der Richtlinie verwendet wird, wenn der DNS-Verkehr möglicherweise die ECS-Option in der Abfrage hat oder nicht. Example: “(((DNS.REQ.OPT.ECS.IP.MATCHES_LOCATION(“.CH…..”).typec ALT (client.IP.SRC.MATCHES_LOCATION(“.CH…..”).typecast_text_t

XPath- und HTML-, XML- oder JSON-Ausdrücke

August 19, 2021

Die erweiterte Richtlinieninfrastruktur unterstützt Ausdrücke zum Auswerten und Abrufen von Daten aus HTML-, XML- und JavaScript-Object Notation (JSON) -Dateien. Auf diese Weise können Sie bestimmte Knoten in einem HTML-, XML- oder JSON-Dokument suchen, feststellen, ob ein Knoten in der Datei vorhanden ist, Knoten in XML-Kontexten suchen (z. B. Knoten mit bestimmten Eltern oder ein bestimmtes Attribut mit einem bestimmten Wert) und den Inhalt dieser Knoten zurückgeben. Darüber hinaus können Sie XPath-Ausdrücke in Rewrite-Ausdrücken verwenden.

Die Implementierung des erweiterten Richtlinienausdrucks für XPath umfasst ein Präfix für erweiterte Richtlinienausdrücke (z. B. “HTTP.REQ.BODY”), das HTML- oder XML-Text bezeichnet, und den XPATH-Operator, der den XPath-Ausdruck als Argument verwendet.

HTML-Dateien sind eine weitgehend freie Sammlung von Tags und Textelementen. Sie können den

XPATH_HTML-Operator verwenden, der einen XPath-Ausdruck als Argument verwendet, um HTML-Dateien zu verarbeiten. JSON-Dateien sind entweder eine Sammlung von Namen/Wert-Paaren oder eine geordnete Liste von Werten. Sie können den XPATH_JSON-Operator verwenden, der einen XPath-Ausdruck als Argument verwendet, um JSON-Dateien zu verarbeiten.

- **<text>.XPATH(xpathex):**

  Verwenden Sie eine XML-Datei und geben Sie einen booleschen Wert zurück.

  Der folgende Ausdruck gibt beispielsweise einen booleschen TRUE zurück, wenn ein Knoten namens “creator” innerhalb der ersten 1000 Byte der XML-Datei unter dem Knoten “Book” existiert.

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%boolean(//Book/creator)%)
  ```

  Parameter:

  xpathex - XPath Boolescher Ausdruck

- **<text>.XPATH(xpathex):**

  Arbeiten Sie auf einer XML-Datei und geben Sie einen Wert des Datentyps “double. “

  Der folgende Ausdruck konvertiert beispielsweise die Zeichenfolge “36” (ein Preiswert) in einen Wert vom Datentyp “double”, wenn sich die Zeichenfolge in den ersten 1000 Byte der XML-Datei befindet:

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%number(/Book/price)%)
  ```

  Parameter:

  xpathex - XPath - numerischer Ausdruck

Beispiel:

```
    <Book>
    <creator>
        <Person>
            <name>Milton</name>
        </Person>
    </creator>
    <title>Paradise Lost</title>
    </Book>
<!--NeedCopy-->
```

- **<text>.XPATH(xpathex):**

  Arbeiten Sie an einer XML-Datei und geben Sie einen Knotensatz oder eine Zeichenfolge zurück. Knotensätze werden mit der Standard-XPath-String-Konvertierungsroutine in entsprechende Strings konvertiert.

Der folgende Ausdruck wählt beispielsweise alle Knoten aus, die von “/book/creator” (einem Knotensatz) in den ersten 1000 Bytes des Körpers eingeschlossen sind:

```
HTTP.REQ.BODY(1000).XPATH(xp%/Book/creator%)
```

Parameter:

xpathex - XPath-Ausdruck

- **<text>.XPATH_HTML(xpathex)**

  Arbeiten Sie an einer HTML-Datei und geben Sie einen Textwert zurück.

  Der folgende Ausdruck funktioniert beispielsweise für eine HTML-Datei und gibt den Text zurück, der in <title\></title\> Tags eingeschlossen ist, wenn das title-HTML-Element in den ersten 1000 Bytes gefunden wird:

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML(xp%/html/head/title%)
  ```

  Parameter:

  xpathex - XPath-Textausdruck

- **<text>.XPATH_HTML_WITH_MARKUP(xpathex)**

  Arbeiten Sie an einer HTML-Datei und geben Sie eine Zeichenfolge zurück, die den gesamten ausgewählten Teil des Dokuments enthält, einschließlich Markups, z. B. das Einschließen der umschließenden Element-Tags.

  Der folgende Ausdruck wirkt auf die HTML-Datei und wählt den gesamten Inhalt innerhalb des <\title>-Tags, einschließlich Markup.

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML_WITH_MARKUP( xp%/html/head/title%)
  ```

  Der durch den Ausdruck ausgewählte Teil des HTML-Body wird zur weiteren Verarbeitung markiert.

  Parameter:

  xpathex - XPath-Ausdruck

- **<text>.XPATH_JSON(xpathex)**

  Arbeiten Sie an einer JSON-Datei und geben Sie einen booleschen Wert zurück.

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’ } }

  Der folgende Ausdruck arbeitet für die JSON-Datei und gibt einen booleschen TRUE zurück, wenn die JSON-Datei einen Knoten namens “creator” enthält, dessen übergeordneter Knoten “Book” in den ersten 1000 Bytes lautet:

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%boolean(/Book/creator)%)
  ```


Parameter:

xpathex - XPath Boolescher Ausdruck

- **<text>.XPATH_JSON(xpathex)**

  Arbeiten Sie auf einer JSON-Datei und geben Sie einen Wert vom Datentyp “double. “

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’, ”preis” :”36”}}

  Der folgende Ausdruck arbeitet für die JSON-Datei und konvertiert die Zeichenfolge “36” in einen Wert vom Datentyp “double”, wenn die Zeichenfolge in den ersten 1000 Bytes der JSON-Datei vorhanden ist.

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%number(/Book/price)%)
  ```

  Parameter:

  xpathex - XPath - numerischer Ausdruck

- **<text>.XPATH_JSON(xpathex)**

  Arbeiten Sie an einer JSON-Datei und geben Sie einen Knotensatz oder eine Zeichenfolge zurück. Knotensätze werden mit der Standard-XPath-String-Konvertierungsroutine in entsprechende Strings konvertiert.

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’ } }

  Der folgende Ausdruck wählt alle Knoten aus, die in den ersten 1000 Bytes des Hauptteils der JSON-Datei von ”/Book” (einem Knotensatz) eingeschlossen sind, und gibt den entsprechenden String-Wert zurück, der ist”<name><title>”:

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%/Book%)
  ```

  Parameter:

  xpathex - XPath-Ausdruck

- **<text>XPATH_JSON_WITH_MARKUP (xpathex)**

  Verwenden Sie eine XML-Datei, und geben Sie eine Zeichenfolge zurück, die den gesamten Teil des Dokuments für den Ergebnisknoten enthält, einschließlich Markups, z. B. das Einschließen der umschließenden Element-Tags.

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’ } }

Der folgende Ausdruck arbeitet auf der JSON-Datei und wählt alle Knoten aus, die von “/book/creator” in den ersten 1000 Bytes des Körpers eingeschlossen sind, also “creator: {person: {name: <name> ‘}}. “

```
HTTP.REQ.BODY(1000).XPATH_JSON_WITH_MARKUP(xp%/Book/creator%)
```

Der Teil des JSON-Body, der durch den Ausdruck ausgewählt wird, wird zur weiteren Verarbeitung markiert.

Parameter:

xpathex - XPath-Ausdruck

- **<text>XPATH_WITH_MARKUP (xpathex):**

  Verwenden Sie eine XML-Datei, und geben Sie eine Zeichenfolge zurück, die den gesamten Teil des Dokuments für den Ergebnisknoten enthält, einschließlich Markups, z. B. das Einschließen der umschließenden Element-Tags.

  Der folgende Ausdruck arbeitet beispielsweise mit einer XML-Datei und wählt alle Knoten aus, die von “/book/creator” in den ersten 1000 Byte des Hauptteils eingeschlossen sind.

  ```
  HTTP.REQ.BODY(1000).XPATH_WITH_MARKUP(xp%/Book/creator%)
  ```

  Der Teil des JSON-Body, der durch den Ausdruck ausgewählt wird, wird zur weiteren Verarbeitung markiert.

  Parameter:

  xpathex - XPath-Ausdruck

Verschlüsseln und Entschlüsseln von XML-Nutzdaten

May 11, 2023

Sie können die Funktionen XML_ENCRYPT () und XML_DECRYPT () in erweiterten Richtlinienausdrücken verwenden, um XML-Daten zu verschlüsseln bzw. zu entschlüsseln. Diese Funktionen entsprechen dem unter “definierten W3C-XML-Verschlüsselungsstandardhttp://www.w3.org/TR/2001/PR-xmldsig-core-20010820/. “ XML_ENCRYPT () und XML_DECRYPT () unterstützen eine Teilmenge der XML Encryption Spezifikation. In der Teilmenge verwendet die Datenverschlüsselung eine Massenverschlüsselungsmethode (RC4, DES3, AES128, AES192 oder AES256), und ein öffentlicher RSA-Schlüssel wird verwendet, um den Massenverschlüsselungsschlüssel zu verschlüsseln.

Hinweis: Wenn Sie Text in einer Nutzlast verschlüsseln und entschlüsseln möchten, müssen Sie die Funktionen ENCRYPT und DECRYPT verwenden. Weitere Informationen zu diesen Funktionen finden Sie unter Verschlüsseln und Entschlüsseln von Text.

Die Funktionen XML_ENCRYPT() und XML_DECRYPT() sind nicht abhängig vom Verschlüsselungs- und Entschlüsselungsdienst, der von den Befehlen ENCRYPT und DECRYPT für Text verwendet wird. Die Verschlüsselungsmethode wird explizit als Argument für die Funktion XML_ENCRYPT () angegeben. Die Funktion `XML_DECRYPT()` erhält die Informationen über die angegebene Verschlüsselungsmethode aus dem Element `<xenc:EncryptedData>`. Im Folgenden finden Sie eine Zusammenfassung der XML-Verschlüsselungs- und Entschlüsselungsfunktionen:

- Das Element `XML_ENCRYPT(<certKeyName>, <method> [, <flags>])**. Returns an <xenc:EncryptedData>`, das den verschlüsselten Eingabetext und den Verschlüsselungsschlüssel enthält, der selbst wiederum mit RSA verschlüsselt wird.
- `XML_DECRYPT(<certKeyName>)`. Gibt den entschlüsselten Text aus dem Eingabeelement `<xenc:EncryptedData>` zurück, das die Verschlüsselungsmethode und den RSA-verschlüsselten Schlüssel enthält.

Hinweis: Das Element `<xenc:EncryptedData>` ist in der W3C XML Encryption Spezifikation definiert.

Es folgen Beschreibungen der Argumente:

- **certKeyName:** Wählt ein X.509-Zertifikat mit einem öffentlichen RSA-Schlüssel für XML_ENCRYPT () oder einen privaten RSA-Schlüssel für XML_DECRYPT (). Der Zertifikatschlüssel muss zuvor durch den Befehl `add ssl certKey` erstellt worden sein.
- **Methode:** Gibt an, welche Verschlüsselungsmethode für die Verschlüsselung der XML-Daten verwendet werden soll. Mögliche Werte: RC4, DES3, AES128, AES192, AES256.
- **flags:** Eine Bitmaske, die die folgenden optionalen Schlüsselinformationen (`<ds:KeyInfo>`) angibt, die in das Element `<xenc:EncryptedData>` aufgenommen werden sollen, das von `XML_ENCRYPT()` generiert wird:
  - **1** - Fügen Sie ein KeyName-Element in den certKeyName ein. Das Element ist `<ds:KeyName>`.
  - **2** - Fügen Sie ein KeyValue-Element mit dem öffentlichen RSA-Schlüssel aus dem Zertifikat ein. Das Element ist `<ds:KeyValue>`.
  - **4** - Fügen Sie ein X509IssuerSerial-Element mit der Seriennummer des Zertifikats und dem Aussteller-DN hinzu. Das Element ist `<ds:X509IssuserSerial>`.
  - **8** - Fügen Sie ein x509SubjectName-Element mit dem Betreff-DN des Zertifikats ein. Das Element ist `<ds:X509SubjectName>`.
  - **16** - Fügen Sie dem gesamten Zertifikat ein X509Certificate-Element bei. Das Element ist `<ds:X509Certificate>`.

Verwenden Sie die Funktionen XML_ENCRYPT () und XML_DECRYPT () in Ausdrücken

Die XML-Verschlüsselungsfunktion verwendet SSL-Zertifikatschlüsselpaare, um X.509-Zertifikate (mit öffentlichen RSA-Schlüsseln) für die Schlüsselverschlüsselung und private RSA-Schlüssel für die Schlüsselentschlüsselung bereitzustellen. Bevor Sie die Funktion XML_ENCRYPT () in einem Ausdruck verwenden, müssen Sie daher ein SSL-Zertifikatschlüsselpaar erstellen. Der folgende Befehl erstellt ein SSL-Zertifikatschlüsselpaar, mein-certkey, mit dem X.509-Zertifikat, my-cert.pem, und der privaten Schlüsseldatei my-key.pem.

```
add ssl certKey my-certkey -cert my-cert.pem -key my-key.pem -passcrypt
kxPeMRYnitY=
```

Die folgenden CLI-Befehle erstellen Rewrite-Aktionen und Richtlinien zum Verschlüsseln und Entschlüsseln von XML-Inhalten.

```
1  add rewrite action my-xml-encrypt-action replace "HTTP.RES.BODY(10000).
       XPATH_WITH_MARKUP(xp%/%)" "HTTP.RES.BODY(10000).XPATH_WITH_MARKUP(xp
       %/%).XML_ENCRYPT("my-certkey", AES256, 31)"
2
3  add rewrite action my-xml-decrypt-action replace "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)" "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%).XML_DECRYPT("my-certkey"
       )"
4
5  add rewrite policy my-xml-encrypt-policy "HTTP.REQ.URL.CONTAINS("xml-
       encrypt")" my-xml-encrypt-action
6
7  add rewrite policy my-xml-decrypt-policy "HTTP.REQ.BODY(10000).XPATH(xp
       %boolean(//xenc:EncryptedData)%)" my-xml-decrypt-action
8
9  bind rewrite global my-xml-encrypt-policy 30
10
11 bind rewrite global my-xml-decrypt-policy 30
12 <!--NeedCopy-->
```

Im obigen Beispiel verschlüsselt die Rewriteaktion my-xml-encrypt-action das gesamte XML-Dokument (XPATH_WITH_MARKUP (xp%/%)) in der Anforderung, indem die Massenverschlüsselungsmethode AES-256 und der öffentliche RSA-Schlüssel von my-certkey verwendet werden, um den Massenverschlüsselungsschlüssel zu verschlüsseln. Die Aktion ersetzt das Dokument durch ein <xenc:EncryptedData> Element, das die verschlüsselten Daten und einen verschlüsselten Schlüssel enthält. Die durch 31 dargestellten Flaggen enthalten alle optionalen <ds:KeyInfo> Elemente.

Die Aktion my-xml-decrypt-action entschlüsselt das erste <xenc:EncryptedData> Element in der Antwort (XPATH_WITH_MARKUP (xp%//XENC:EncryptedData%)). Dies erfordert das vorherige

Hinzufügen des XENC-XML-Namespace mithilfe des folgenden CLI-Befehls:

```
add ns xmlnamespace xenc http://www.w3.org/2001/04/xmlenc##
```

Die Aktion my-xml-decrypt-action verwendet den privaten RSA-Schlüssel in my-certkey, um den verschlüsselten Schlüssel zu entschlüsseln, und verwendet dann die im Element angegebene Massenverschlüsselungsmethode, um den verschlüsselten Inhalt zu entschlüsseln. Schließlich ersetzt die Aktion das verschlüsselte Datenelement durch den entschlüsselten Inhalt.

Die Rewriterichtlinie von my-xml-encrypt-policy wendet meine-xml-encrypt-action auf Anfragen nach URLs an, die xml-encrypt enthalten. Die Aktion verschlüsselt die gesamte Antwort eines auf der NetScaler-Appliance konfigurierten Dienstes.

Die Rewriterichtlinie my-xml-decrypt-policy wendet my-xml-decrypt-action auf Anfragen an, die ein <xenc:EncryptedData> Element enthalten (XPATH (xp%//xenc:EncryptedData%) gibt eine nicht leere Zeichenfolge zurück). Die Aktion entschlüsselt die verschlüsselten Daten in Anforderungen, die für einen Dienst gebunden sind, der auf der NetScaler-Appliance konfiguriert ist.

Erweiterte Richtlinienausdrücke: SSL parsen

November 3, 2022

Es gibt erweiterte Richtlinienausdrücke, um SSL-Zertifikate und Hello-Nachrichten des SSL-Clients zu analysieren.

Analysieren Sie SSL-Zertifikate

Sie können erweiterte Richtlinienausdrücke verwenden, um X.509 Secure Sockets Layer (SSL) Clientzertifikate auszuwerten. Ein Clientzertifikat ist ein elektronisches Dokument, mit dem die Identität eines Benutzers authentifiziert werden kann. Ein Clientzertifikat enthält (mindestens) Versionsinformationen, eine Seriennummer, eine Signaturalgorithmus-ID, einen Ausstellernamen, eine Gültigkeitsdauer, einen Antragstellernamen (Benutzer), einen öffentlichen Schlüssel und Signaturen.

Sie können sowohl SSL-Verbindungen als auch Daten in Clientzertifikaten untersuchen. Beispielsweise möchten Sie möglicherweise SSL-Anforderungen, die Verschlüsselungen mit niedriger Stärke verwenden, an eine bestimmte virtuelle Serverfarm mit Lastausgleich senden. Der folgende Befehl ist ein Beispiel für eine Content Switching-Richtlinie, die die Verschlüsselungsstärke in einer Anforderung analysiert und Verschlüsselungsstärken kleiner oder gleich 40 entspricht:

```
add cs policy p1 -rule "client.ssl.cipher_bits.le(40)"
```

Als weiteres Beispiel können Sie eine Richtlinie konfigurieren, die bestimmt, ob eine Anforderung ein Clientzertifikat enthält:


```
add cs policy p2 -rule "client.ssl.client_cert exists"
```

Sie können auch eine Richtlinie konfigurieren, die bestimmte Informationen in einem Clientzertifikat untersucht. Die folgende Richtlinie überprüft beispielsweise, ob das Zertifikat einen oder mehrere Tage vor Ablauf hat:

```
add cs policy p2 -rule "client.ssl.client_cert exists && client.ssl.client_cert
.days_to_expire.ge(1)"
```

Ein Beispiel für die Verwendung von JA3 Fingerabdrücken:

```
add ssl policy ja3_pol -rule "CLIENT.SSL.JA3_FINGERPRINT.EQ(bb4c15a90e93a25ddc1627439
)"-action reset
```

Oder ein Beispiel für die Verwendung von JA3-Fingerabdrücken mit Patset:

```
1 add policy patset pat1
2 bind policy patset pat1 bb4c15a90e93a25ddc16274395bce4c6 -index 1
3 bind policy patset pat1 cd3c15a90e93a25ddc16274395bce6b4 -index 2
4 add ssl policy ssl_ja3_pol -rule CLIENT.SSL.JA3_FINGERPRINT.
     contains_any("pat1") -action reset
5 <!--NeedCopy-->
```

> **Hinweis**
>
> Informationen zum Analysieren von Datums und Uhrzeiten in einem Zertifikat finden Sie unter Format von Datums und Zeiten in einem Ausdruck und Ausdrücke für SSL-Zertifikatdaten.

Präfixe für textbasierte SSL- und Zertifikatsdaten

In der folgenden Tabelle werden Ausdruckspräfixe beschrieben, die textbasierte Elemente in SSL-Transaktionen und Clientzertifikaten identifizieren.

Tabelle 1. Präfixe, die Text oder boolesche Werte für SSL- und Clientzertifikatsdaten zurückgeben

Präfix	Beschreibung
CLIENT.SSL.CLIENT_CERT	Gibt das SSL-Clientzertifikat in der aktuellen SSL-Transaktion zurück.
CLIENT.SSL.CLIENT_CERT.TO_PEM	Gibt das SSL-Clientzertifikat im Binärformat zurück.
CLIENT.SSL.CIPHER_EXPORTABLE	Gibt ein boolesches TRUE zurück, wenn die kryptografische SSL-Verschlüsselung exportierbar ist.

Präfix	Beschreibung
CLIENT.SSL.CIPHER_NAME	Gibt den Namen der SSL-Verschlüsselung zurück, wenn sie von einer SSL-Verbindung aufgerufen wird, und eine NULL-Zeichenfolge, wenn sie von einer Nicht-SSL-Verbindung aufgerufen wird.
CLIENT.SSL.IS_SSL	Gibt ein boolesches TRUE zurück, wenn die aktuelle Verbindung SSL-basiert ist.
CLIENT.SSL.JA3_FINGERPRINT	Gibt ein boolesches TRUE zurück, wenn der konfigurierte JA3-Fingerabdruck mit dem JA3-Fingerabdruck in der Hello-Nachricht des Clients übereinstimmt. **Hinweis:** Dieser Ausdruck ist in Version 13.1 Build 12.x und höher verfügbar.

Präfixe für numerische Daten in SSL-Zertifikaten

In der folgenden Tabelle werden Präfixe beschrieben, die numerische Daten außer Datumsangaben in SSL-Zertifikaten auswerten. Diese Präfixe können mit den Operationen verwendet werden, die unter Grundlegende Operationen für Ausdruckspräfixe und zusammengesetzte Operationen für Zahlenbeschrieben sind.

Tabelle 2. Präfixe, die numerische Daten außer Daten in SSL-Zertifikaten auswerten

Präfix	Beschreibung
CLIENT.SSL.CLIENT_CERT.DAYS_TO_EXPIRE	Gibt die Anzahl der Tage zurück, an denen das Zertifikat gültig ist, oder gibt -1 für abgelaufene Zertifikate zurück.
CLIENT.SSL.CLIENT_CERT.PK_SIZE	Gibt die Größe des öffentlichen Schlüssels zurück, der im Zertifikat verwendet wird.
CLIENT.SSL.CLIENT_CERT.VERSION	Gibt die Versionsnummer des Zertifikats zurück. Wenn die Verbindung nicht SSL-basiert ist, wird Null (0) zurückgegeben.
CLIENT.SSL.CIPHER_BITS	Gibt die Anzahl der Bits im kryptographischen Schlüssel zurück. Gibt 0 zurück, wenn die Verbindung nicht SSL-basiert ist.

Präfix	Beschreibung
CLIENT.SSL.VERSION	Gibt eine Zahl zurück, die die SSL-Protokollversion darstellt, wie folgt: 0. Die Transaktion ist nicht SSL-basiert: 0x002. Die Transaktion ist SSLv2:0x300. Die Transaktion ist SSLv3:0x301. Die Transaktion ist TLSv1:0x302. Die Transaktion ist TLS 1.1:0x303. Die Transaktion ist TLS 1.2:0x304. Die Transaktion ist TLS 1.3.

> **Hinweis**
>
> Informationen zu Ausdrücken im Zusammenhang mit Ablaufdatum in einem Zertifikat finden Sie unter Ausdrücke für SSL-Zertifikatdaten.

Ausdrücke für SSL-Zertifikate

Sie können SSL-Zertifikate analysieren, indem Sie Ausdrücke konfigurieren, die das folgende Präfix verwenden:

CLIENT.SSL.CLIENT_CERT

In diesem Abschnitt werden die Ausdrücke beschrieben, die Sie für Zertifikate konfigurieren können, ausgenommen Ausdrücke, die den Zertifikatablauf untersuchen. Zeitbasierte Vorgänge werden unter Erweiterte Richtlinienausdrücke: Arbeiten mit Datumsangaben, Zeiten und Zahlenbeschrieben.

In der folgenden Tabelle werden die Vorgänge beschrieben, die Sie für das Präfix CLIENT.SSL.CLIENT_CERT angeben können.

Tabelle 3. Vorgänge, die mit dem Präfix CLIENT.SSL.CLIENT_CERT angegeben werden können

SSL-Zertifikat Betrieb	Beschreibung
`<certificate>.EXISTS`	Gibt ein boolesches TRUE zurück, wenn der Client über ein SSL-Zertifikat verfügt.

SSL-Zertifikat Betrieb	Beschreibung
`<certificate>.ISSUER`	Gibt den Distinguished Name (DN) des Ausstellers im Zertifikat als Name-Wert-Liste zurück. Ein Gleichheitszeichen (“=”) ist das Trennzeichen für den Namen und den Wert, und der Schrägstrich (“/”) ist das Trennzeichen, das die Name-Wert-Paare trennt. Es folgt ein Beispiel für den zurückgegebenen DN: `/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com`
`<certificate>.ISSUER.IGNORE_EMPTY_ELEMENTS`	Gibt den Emittenten zurück und ignoriert die leeren Elemente in einer Name-Wert-Liste. Beispielsweise, Bedenken Sie Folgendes: `Cert-Issuer: /c=in/st=kar//l=bangelore //o=mycompany/ou=sales/ /emailAddress=myuserid@mycompany.com`. Die folgende Rewrite-Aktion gibt basierend auf der vorhergehenden Emittentendefinition eine Anzahl von 6 zurück: `sh rewrite action insert_ssl_header Name: insert_ssl Operation: insert_http_header Target:Cert-Issuer Value:CLIENT.SSL.CLIENT_CERT.ISSUER.COUNT`. Wenn Sie jedoch den Wert in den folgenden ändern, ist die zurückgegebene Anzahl 9: `CLIENT.SSL.CLIENT_CERT.ISSUER.IGNORE_EMPTY_ELEMENTS.COUNT`

SSL-Zertifikat Betrieb	Beschreibung
`<certificate>. SERIALNUMBER`	Gibt die Seriennummer des Zertifikats als hexadezimale Zeichenfolge in Großbuchstaben ohne führende Nullen zurück. Wenn die Seriennummer des Zertifikats beispielsweise 04daa1e44bd2e7769638a0058b4964bd lautet, hilft der folgende Ausdruck bei der Zuordnung der Seriennummer `CLIENT.SSL.CLIENT_CERT.SERIALNUMBER .SET_TEXT_MODE(IGNORECASE).CONTAINS (\"4daa1e44bd2e7769638a0058b4964bd \")`

Parse SSL-Client hallo

Sie können die Hello-Nachricht des SSL-Clients analysieren, indem Sie Ausdrücke konfigurieren, die das folgende Präfix verwenden:

Präfix	Beschreibung
CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXC(	Entspricht dem im Ausdruck angegebenen Hex-Code mit den Hex-Codes der Verschlüsselungssammlungen, die in der Hello-Nachricht des Clients empfangen wurden.
CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION	Version, die im Hello-Nachrichtenheader des Clients empfangen wurde.
CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE	Gibt true zurück, wenn ein Client oder Server eine Sitzungsneuverhandlung initiiert.
CLIENT.SSL.CLIENT_HELLO.IS_REUSE	Gibt true zurück, wenn die Appliance die SSL-Sitzung basierend auf der in der Client-Hallo-Nachricht empfangenen Sitzungs-ID ungleich Null wiederverwendet.
CLIENT.SSL.CLIENT_HELLO.IS_SCSV	Gibt true zurück, wenn die Signaling Cipher Suite Value (SCSV) -Funktion in der Hello-Nachricht des Clients angekündigt wird. Der Hexadezimalcode für Fallback SCSV ist 0x5600.

Präfix	Beschreibung
CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET	Gibt true zurück, wenn in der Client-Hallo-Nachricht eine Sitzungsticket-Erweiterung mit einer Länge ungleich Null angekündigt wird.
CLIENT.SSL.CLIENT_HELLO.LENGTH	Länge, die im Hello-Nachrichtenheader des Clients empfangen wurde.
CLIENT.SSL.CLIENT_HELLO.SNI	Gibt den Servernamen zurück, der in der Erweiterung “Servername” der Hello-Nachricht des Clients empfangen wurde.
CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPRC	Gibt true zurück, wenn das Anwendungsprotokoll in der Erweiterung ALPN, das in der Hello-Nachricht des Clients empfangen wurde, mit dem im Ausdruck angegebenen Protokoll übereinstimmt

Diese Ausdrücke können am Bindungspunkt CLIENTHELLO_REQ verwendet werden. Weitere Informationen finden Sie unter Bindung von SSL-Richtlinien.

Erweiterte Richtlinienausdrücke: IP- und MAC-Adressen, Durchsatz, VLAN-IDs

May 11, 2023

Sie können Präfixe für erweiterte Richtlinienausdrücke verwenden, die IPv4- und IPv6-Adressen, MAC-Adressen, IP-Subnetze, nützliche Client- und Serverdaten wie die Durchsatzraten an den Schnittstellenports (Rx, Tx und RxTx) und die IDs der VLANs, über die Pakete empfangen werden, zurückgeben. Sie können dann verschiedene Operatoren verwenden, um die Daten auszuwerten, die von diesen Ausdruckspräfixen zurückgegeben werden.

Ausdrücke für IP-Adressen und IP-Subnetze

Sie können erweiterte Richtlinienausdrücke verwenden, um Adressen und Subnetze auszuwerten, die im Format Internet Protocol Version 4 (IPv4) oder Internet Protocol Version 6 (IPv6) vorliegen. Ausdruckspräfixe für IPv6-Adressen und Subnetze enthalten IPv6 im Präfix. Ausdruckspräfixe für IPv4-Adressen und Subnetze enthalten IP im Präfix. Es folgt ein Beispiel für einen Ausdruck, der angibt, ob

eine Anforderung von einem bestimmten IPv4-Subnetz stammt.

```
client.ip.src.in_subnet(147.1.0.0/16)
<!--NeedCopy-->
```

Im Folgenden finden Sie zwei Beispiele für Rewriterichtlinien, die das Subnetz untersuchen, von dem das Paket empfangen wird, und eine Rewrite-Aktion für den Host-Header ausführen. Wenn diese beiden Richtlinien konfiguriert sind, hängt die durchgeführte Rewrite-Aktion vom Subnetz in der Anforderung ab. Diese beiden Richtlinien werten IP-Adressen aus, die im IPv4-Adressformat vorliegen.

```
- add rewrite action URL1-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany1.com""
- add rewrite policy URL1-rewrite-policy "http.req.header("Host").
   contains("www.test1.com") && client.ip.src.in_subnet(147.1.0.0/16)"
   URL1-rewrite-action
- add rewrite action URL2-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany2.com""
- add rewrite policy URL2-rewrite-policy "http.req.header("Host").
   contains("www.test2.com") && client.ip.src.in_subnet(10.202.0.0/16)"
    URL2-rewrite-action
<!--NeedCopy-->
```

> **Hinweis**
>
> Die vorangegangenen Beispiele sind Befehle, die Sie an der NetScaler Befehlszeilenschnittstelle (CLI) eingeben. Daher muss jedem Anführungszeichen ein umgekehrter Schrägstrich (\) vorangestellt werden. Weitere Informationen finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken in einer Richtlinie. “

Präfixe für IPV4-Adressen und IP-Subnetze

In der folgenden Tabelle werden Präfixe beschrieben, die IPv4-Adressen und Subnetze sowie Segmente von IPv4-Adressen zurückgeben. Sie können numerische Operatoren und Operatoren verwenden, die für IPv4-Adressen spezifisch sind. Weitere Informationen zu numerischen Operationen finden Sie unter “Grundoperationen für Ausdruckspräfixe” und “Zusammengesetzte Operationen für Zahlen. “

Tabelle 1. Präfixe, die IP- und MAC-Adressen auswerten

Präfix	Beschreibung
CLIENT.IP.SRC	Gibt die Quell-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.

Präfix	Beschreibung
CLIENT.IP.DST	Gibt die Ziel-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.
SERVER.IP.SRC	Gibt die Quell-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.
SERVER.IP.DST	Gibt die Ziel-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.

Operationen für IPV4-Adressen

In der Tabelle Präfix für IPV4-Operationen werden die Operatoren beschrieben, die mit Präfixen verwendet werden können, die eine IPv4-Adresse zurückgeben.

Informationen zu IPv6-Ausdrücken

Das IPv6-Adressformat ermöglicht mehr Flexibilität als das ältere IPv4-Format. IPv6-Adressen liegen im Hexadezimalformat vor (RFC 2373). In den folgenden Beispielen ist Beispiel 1 eine IPv6-Adresse, Beispiel 2 ist eine URL, die die IPv6-Adresse enthält, und Beispiel 3 enthält die IPv6-Adresse und eine Portnummer.

Beispiel 1:

```
9901:0ab1:22a2:88a3:3333:4a4b:5555:6666
<!--NeedCopy-->
```

Beispiel 2:

```
http://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]/
<!--NeedCopy-->
```

Beispiel 3:

```
https://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]:8080/
<!--NeedCopy-->
```

In Beispiel 3 trennen die Klammern die IP-Adresse von der Portnummer (8080).

Beachten Sie, dass Sie den Operator '+' nur verwenden können, um IPv6-Ausdrücke mit anderen Ausdrücken zu kombinieren. Die Ausgabe ist eine Verkettung der Zeichenfolgenwerte, die von den einzelnen Ausdrücken zurückgegeben werden. Sie können keinen anderen arithmetischen Operator mit einem IPv6-Ausdruck verwenden. Die folgende Syntax ist ein Beispiel:


```
client.ipv6.src + server.ip.dst
<!--NeedCopy-->
```

Wenn beispielsweise die IPv6-Quelladresse des Clients lautet `ABCD:1234::ABCD`und die IPv4-Adresse des Serverziels lautet `10.100.10.100`, wird der vorhergehende Ausdruck zurückgegeben `"ABCD:1234::ABCD10.100.10.100"`.

Beachten Sie, dass die NetScaler-Appliance, wenn sie ein IPv6-Paket empfängt, eine temporäre IPv4-Adresse aus einem nicht verwendeten IPv4-Adressbereich zuweist und die Quelladresse des Pakets an diese temporäre Adresse ändert. Zur Reaktionszeit wird die Quelladresse des ausgehenden Pakets durch die ursprüngliche IPv6-Adresse ersetzt.

> **Hinweis**
>
> Sie können einen IPv6-Ausdruck mit jedem anderen Ausdruck kombinieren, außer einem Ausdruck, der ein boolesches Ergebnis erzeugt.

Ausdruckspräfixe für IPv6-Adressen

Die IPv6-Adressen, die von den Ausdruckspräfixen in der folgenden Tabelle zurückgegeben werden, können als Textdaten behandelt werden. Beispielsweise gibt das Präfix client.ipv6.dst die Ziel-IPv6-Adresse als Zeichenfolge zurück, die als Text ausgewertet werden kann.

In der folgenden Tabelle werden Ausdruckspräfixe beschrieben, die eine IPv6-Adresse zurückgeben.

Tabelle 3. IPv6-Ausdruckspräfixe, die Text zurückgeben

Präfix	Beschreibung
CLIENT.IPV6	Arbeitet mit der IPv6-Adresse in dem aktuellen Paket.
CLIENT.IPV6.DST	Gibt die IPv6-Adresse im Zielfeld des IP-Headers zurück.
CLIENT.IPV6.SRC	Gibt die IPv6-Adresse im Quellfeld des IP-Headers zurück. Im Folgenden finden Sie Beispiele: `client.ipv6.src.in_subnet (2007::2008/64)` `client.ipv6.src.get1.le(2008)`
SERVER.IPV6	Arbeitet mit der IPv6-Adresse in dem aktuellen Paket.
SERVER.IPV6.DST	Gibt die IPv6-Adresse im Zielfeld des IP-Headers zurück.

Präfix	Beschreibung
SERVER.IPV6.SRC	Gibt die IPv6-Adresse im Quellfeld des IP-Headers zurück. Im Folgenden finden Sie Beispiele: `server.ipv6.src.in_subnet (2007::2008/64)` `server.ipv6.src.get1.le(2008)`

Operationen für IPv6-Präfixe

In der folgenden Tabelle werden die Operatoren beschrieben, die mit Präfixen verwendet werden können, die eine IPv6-Adresse zurückgeben:

Tabelle 4. Vorgänge, die IPv6-Adressen auswerten

IPv6-Betrieb	Beschreibung
`<ipv6>.EQ(<IPv6_address>`	Gibt ein boolesches TRUE zurück, wenn der IP-Adresswert dem `<IPv6_address>` Argument entspricht. Es folgt ein Beispiel: `client.ipv6.dst.eq(ABCD:1234::ABCD)`
`<ipv6>.GET1. . .GET8`	Gibt ein Segment einer IPv6-Adresse als Zahl zurück. Die folgenden Beispielausdrücke rufen Segmente von der IPv6-Adresse 1000:1001:CD10:0000:0000:89AB:4567:CDEF: `client.ipv6.dst.get5 extracts 0000` ab, was der fünfte Bitsatz in der Adresse ist. `client.ipv6.dst.get6 extracts 89AB.` `client.ipv6.dst.get7 extracts 4567.` Sie können numerische Operationen für diese Segmente ausführen. Beachten Sie, dass Sie beim Abrufen einer vollständigen IPv6-Adresse keine numerischen Vorgänge ausführen können. Dies liegt daran, dass Ausdrücke, die eine gesamte IPv6-Adresse zurückgeben, wie CLIENT.IPV6.SRC, die Adresse im Textformat zurückgeben.

IPv6-Betrieb	Beschreibung
<ipv6>.IN_SUBNET(<subnet>)	Gibt ein boolesches TRUE zurück, wenn sich der IPv6-Adresswert in dem durch das <subnet> Argument angegebenen Subnetz befindet. Es folgt ein Beispiel: client.ipv6.dst.eq(1000:1001:CD10:0000:0000:89AB:4567:CDEF/60)
<ipv6>.IS_IPV4	Gibt ein boolesches TRUE zurück, wenn dies ein IPv4-Client ist, und gibt ein boolesches FALSE zurück, wenn dies nicht der Fall ist.
<ipv6>.SUBNET(<n>)	Gibt die IPv6-Adresse zurück, nachdem die als Argument angegebene Subnetzmaske angewendet wurde. Die Subnetzmaske kann Werte zwischen 0 und 128 annehmen. Beispiel: CLIENT.IPV6.SRC.SUBNET(24)

Ausdrücke für MAC-Adressen

Eine MAC-Adresse besteht aus durch Doppelpunkt getrennten Hexadezimalwerten im Format ##:##:##:##:##:##, wobei jedes “#” entweder eine Zahl von 0 bis 9 oder einen Buchstaben von A bis F. darstellt. Erweiterte Richtlinienausdruckspräfixe und -Operatoren stehen für die Auswertung von Quell- und Ziel-MAC-Adressen zur Verfügung.

Präfixe für MAC-Adressen

In der folgenden Tabelle werden Präfixe beschrieben, die MAC-Adressen zurückgeben.

Tabelle 5. Präfixe, die MAC-Adressen auswerten

Präfix	Beschreibung
client.ether.dstmac	Gibt die MAC-Adresse im Zielfeld des Ethernet-Headers zurück.
client.ether.srcmac	Gibt die MAC-Adresse im Quellfeld des Ethernet-Headers zurück.

Operationen für MAC-Adressen

In der folgenden Tabelle werden die Operatoren beschrieben, die mit Präfixen verwendet werden können, die eine MAC-Adresse zurückgeben.

Tabelle 6. Vorgänge auf MAC-Adressen

Präfix	Beschreibung
`<mac address>.EQ(<address>)`	Gibt ein boolesches TRUE zurück, wenn der Wert der MAC-Adresse dem `<address>` Argument entspricht.
`<mac address>.GET1. . .GET4`	Gibt einen numerischen Wert zurück, der aus dem Segment der MAC-Adresse extrahiert wurde, das in der GET-Operation angegeben ist. Wenn die MAC-Adresse beispielsweise 12:34:56:78:9 a:bc lautet, gibt Folgendes 34 zurück: `client.ether.dstmac.get2`

Ausdrücke für numerische Client- und Serverdaten

In der folgenden Tabelle werden Präfixe für die Arbeit mit numerischen Client- und Serverdaten beschrieben, einschließlich Durchsatz, Portnummern und VLAN-IDs.

Tabelle 7. Präfixe, die numerische Client- und Serverdaten auswerten

Präfix	**Beschreibung**
client.interface.rxthroughput	Gibt eine Ganzzahl zurück, die den Durchsatz des empfangenen Rohverkehrs in Kilobyte pro Sekunde (KBit/s) für die letzten sieben Sekunden darstellt.
client.interface.txthroughput	Gibt eine Ganzzahl zurück, die den Durchsatz des übertragenen Rohverkehrs in KBit/s für die letzten sieben Sekunden darstellt.
client.interface.rxtxthroughput	Gibt eine Ganzzahl zurück, die den rohen empfangenen und übertragenen Verkehrsdurchsatz in KBit/s für die letzten sieben Sekunden darstellt.

Präfix	Beschreibung
server.interface.rxthroughput	Gibt eine Ganzzahl zurück, die den Durchsatz des empfangenen Rohdatenverkehrs in KBit/s für die letzten sieben Sekunden darstellt.
server.interface.txthroughput	Gibt eine Ganzzahl zurück, die den Durchsatz des übertragenen Rohverkehrs in KBit/s für die letzten sieben Sekunden darstellt.
server.interface.rxtxthroughput	Gibt eine Ganzzahl zurück, die den rohen empfangenen und übertragenen Verkehrsdurchsatz in KBit/s für die letzten sieben Sekunden darstellt.
server.vlan.id	Gibt eine numerische ID des VLAN zurück, über das das aktuelle Paket in den NetScaler gelangt ist.
client.vlan.id	Gibt eine numerische ID für das VLAN zurück, über das das aktuelle Paket den NetScaler eingegeben hat.

Erweiterte Richtlinienausdrücke: Stream Analytics Funktionen

January 19, 2021

Stream Analytics-Ausdrücke beginnen mit dem <identifier_name> Präfix ANALYTICS.STREAM (). In der folgenden Liste werden die Funktionen beschrieben, die mit diesem Präfix verwendet werden können.

- **COLLECT_STATS**

  Sammeln Sie statistische Daten aus den Anforderungen, die anhand der Richtlinie ausgewertet werden, und erstellen Sie für jede Anforderung einen Datensatz.

- **REQUESTS**

  Gibt die Anzahl der Anforderungen zurück, die für die angegebene Datensatzgruppierung vorhanden sind. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **BANDWIDTH**

  Gibt die Bandbreitenstatistik für die angegebene Datensatzgruppierung zurück. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **RESPTIME**

Gibt die Antwortzeitstatistik für die angegebene Datensatzgruppierung zurück. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **CONNECTIONS**

  Gibt die Anzahl der gleichzeitigen Verbindungen zurück, die für die angegebene Datensatzgruppierung vorhanden sind. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **IS_TOP(n)**

  Gibt einen booleschen TRUE zurück, wenn der statistische Wert für die angegebene Datensatzgruppierung einer der obersten n Gruppen ist. Andernfalls geben Sie einen booleschen FALSE zurück.

- **CHECK_LIMIT**

  Gibt einen booleschen TRUE zurück, wenn die Statistik für die angegebene Datensatzgruppierung das vorkonfigurierte Limit erreicht hat. Andernfalls geben Sie einen booleschen FALSE zurück.

Erweiterte Richtlinienausdrücke: DataStream

May 11, 2023

Die Richtlinieninfrastruktur auf der NetScaler-Appliance umfasst Ausdrücke, mit denen Sie den Datenbankserververkehr auswerten und verarbeiten können, wenn die Appliance zwischen einer Farm von Anwendungsservern und den zugehörigen Datenbankservern bereitgestellt wird.

Dieses Artikel enthält die folgenden Abschnitte:

- Ausdrücke für das MySQL-Protokoll
- Ausdrücke für die Bewertung von Microsoft SQL Server-Verbindungen

Ausdrücke für das MySQL-Protokoll

Die folgenden Ausdrücke bewerten den Datenverkehr im Zusammenhang mit MySQL-Datenbankservern. Sie können die anforderungsbasierten Ausdrücke (Ausdrücke, die mit MYSQL.CLIENT und MYSQL.REQ beginnen) in Richtlinien verwenden, um Entscheidungen zum Umschalten von Anfragen am Bindungspunkt des virtuellen Content-Switching-Servers zu treffen, und die antwortbasierten Ausdrücke (Ausdrücke, die mit MYSQL.RES beginnen), um Serverantworten auf vom Benutzer konfigurierte Integritätsmonitore auszuwerten.

- **MYSQL.CLIENT.** Arbeitet mit den Client-Eigenschaften einer MySQL-Verbindung.

- **MYSQL.CLIENT.CAPABILITIES.** Gibt den Satz von Flags zurück, den der Client während der Authentifizierung im Capability-Feld des Handshake-Initialisierungspakets gesetzt hat. Beispiele für die gesetzten Flags sind CLIENT_FOUND_ROWS, CLIENT_COMPRESS und CLIENT_SSL.
- **MYSQL.CLIENT.CHAR_SET.** Gibt die Aufzählungskonstante zurück, die dem vom Client verwendeten Zeichensatz zugewiesen ist. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Präfix verwendet. Im Folgenden sind die Aufzählungskonstanten für Zeichensätze aufgeführt:
  - LATIN2_CZECH_CS
  - DEC8_SWEDISH_CI
  - CP850_GENERAL_CI
  - GRIECHISCH_ALLGEMEIN_CI
  - LATIN1_GERMAN1_CI
  - HP8_ENGLISH_CI
  - KOI8R_GENERAL_CI
  - LATIN1_SWEDISH_CI
  - LATIN2_GENERAL_CI
  - SWE7_SWEDISH_CI
  - ASCII_ALLGEMEIN_CI
  - CP1251_BULGARIAN_CI
  - LATIN1_DANISH_CI
  - HEBRÄISCH_ALLGEMEIN_CI
  - LATIN7_ESTONIAN_CS
  - LATIN2_HUNGARIAN_CI
  - KOI8U_GENERAL_CI
  - CP1251_UKRAINIAN_CI
  - CP1250_GENERAL_CI
  - LATIN2_CROATIAN_CI
  - CP1257_LITHUANIAN_CI
  - LATIN5_TURKISH_CI
  - LATIN1_GERMAN2_CI
  - ARMSCII8_GENERAL_CI
  - UTF8_GENERAL_CI
  - CP1250_CZECH_CS
  - CP866_GENERAL_CI
  - KEYBCS2_GENERAL_CI
  - MACCE_GENERAL_CI
  - MACROMAN_GENERAL_CI
  - CP852_GENERAL_CI
  - LATIN7_GENERAL_CI

- LATIN7_GENERAL_CS
- MACCE_BIN
- CP1250_CROATIAN_CI
- LATIN1_BIN
- LATIN1_GENERAL_CI
- LATIN1_GENERAL_CS
- CP1251_BIN
- CP1251_GENERAL_CI
- CP1251_GENERAL_CS
- MACROMAN_BIN
- CP1256_GENERAL_CI
- CP1257_BIN
- CP1257_GENERAL_CI
- ARMSCII8_BIN
- ASCII_BIN
- CP1250_BIN
- CP1256_BIN
- CP866_BIN
- DEC8_BIN
- GRIECHISCH_BIN
- HEBRÄISCH_BIN
- HP8_BIN
- KEYBCS2_BIN
- KOI8R_BIN
- KOI8U_BIN
- LATIN2_BIN
- LATIN5_BIN
- LATIN7_BIN
- CP850_BIN
- CP852_BIN
- SWE7_BIN
- UTF8_BIN
- GEOSTD8_GENERAL_CI
- GEOSTD8_BIN
- LATIN1_SPANISH_CI
- UTF8_UNICODE_CI
- UTF8_ICELANDIC_CI
- UTF8_LATVIAN_CI
- UTF8_ROMANIAN_CI

  - UTF8_SLOVENIAN_CI
  - UTF8_POLISH_CI
  - UTF8_ESTONIAN_CI
  - UTF8_SPANISH_CI
  - UTF8_SWEDISH_CI
  - UTF8_TURKISH_CI
  - UTF8_CZECH_CI
  - UTF8_DANISH_CI
  - UTF8_LITHUANIAN_CI
  - UTF8_SLOVAK_CI
  - UTF8_SPANISH2_CI
  - UTF8_ROMAN_CI
  - UTF8_PERSIAN_CI
  - UTF8_ESPERANTO_CI
  - UTF8_HUNGARIAN_CI
  - UNGÜLTIGER ZEICHENSATZ

- **MYSQL.CLIENT.DATABASE.** Gibt den Namen der Datenbank zurück, die in dem Authentifizierungspaket angegeben ist, das der Client an den Datenbankserver sendet. Dies ist das Databasename-Attribut.
- MYSQL.CLIENT.USER. Gibt den Benutzernamen (im Authentifizierungspaket) zurück, mit dem der Client versucht, eine Verbindung zur Datenbank herzustellen. Dies ist das Benutzerattribut.
- **MYSQL.REQ.** Arbeitet auf einer MySQL-Anfrage.
- **MYSQL.REQ.COMMAND.** Identifiziert die Aufzählungskonstante, die dem Befehlstyp in der Anforderung zugewiesen ist. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Präfix verwendet. Im Folgenden sind die Werte der Aufzählungskonstante aufgeführt:

  - SCHLAF
  - BEENDEN
  - INIT_DB
  - ABFRAGEN
  - FELDLISTE
  - CREATE_DB
  - DROP_DB
  - AUFFRISCHEN
  - ABSCHALTUNG
  - STATISTIKEN
  - PROZESS_INFO
  - VERBINDEN

  - PROCESS_KILL
  - DEBUG
  - PING
  - ZEIT
  - VERZÖGERTES EINFÜGEN
  - BENUTZER ÄNDERN
  - BINLOG_DUMP
  - TABLE_DUMP
  - CONNECT_OUT
  - SKLAVE REGISTRIEREN
  - STMT_PREPARE
  - STMT_EXECUTE
  - STMT_SEND_LONG_DATA
  - STMT_CLOSE
  - STMT_RESET
  - OPTION SETZEN
  - STMT_FETCH

- **MYSQL.REQ.QUERY.** Identifiziert die Abfrage in der MySQL-Anfrage.
- **MYSQL.REQ.QUERY.COMMAND.** Gibt das erste Schlüsselwort in der MySQL-Abfrage zurück.
- **MYSQL.REQ.QUERY.SIZE.** Gibt die Größe der Anforderungsabfrage im Integer-Format zurück. Die SIZE-Methode ähnelt der CONTENT_LENGTH-Methode, die die Länge einer HTTP-Anfrage oder -Antwort zurückgibt.
- **MYSQL.REQ.QUERY.TEXT.** Gibt eine Zeichenfolge zurück, die die gesamte Abfrage abdeckt.
- **MYSQL.REQ.QUERY.TEXT(<n>).** Gibt die ersten n Byte der MySQL-Abfrage als Zeichenfolge zurück. Dies ist ähnlich wie HTTP.BODY(<n>).

  Parameter:

  n — Anzahl der zurückzugebenden Bytes

- **MYSQL.RES.** Arbeitet mit einer MySQL-Antwort.
- **MYSQL.RES.ATLEAST_ROWS_COUNT(<i>).** Prüft, ob die Antwort mindestens eine Anzahl von Zeilen enthält, und gibt den booleschen Wert TRUE oder FALSE zurück, um das Ergebnis anzugeben.

  Parameter:

  i - Anzahl der Zeilen

- **MYSQL.RES.FEHLER.** Identifiziert das MySQL-Fehlerobjekt. Das Fehlerobjekt enthält die Fehlernummer und die Fehlermeldung.

- **MYSQL.RES.ERROR.MESSAGE.** Gibt die Fehlermeldung zurück, die aus der Fehlerantwort des Servers abgerufen wurde.
- **MYSQL.RES.ERROR.NUM.** Gibt die Fehlernummer zurück, die aus der Fehlerantwort des Servers abgerufen wird.
- **MYSQL.RES.ERROR.SQLSTATE.** Gibt den Wert des SQLSTATE-Feldes in der Fehlerantwort des Servers zurück. Der MySQL-Server übersetzt Fehlernummernwerte in SQLSTATE-Werte.
- **MYSQL.RES.FIELD(<i>).** Identifiziert das Paket, das i^{th entspricht} individuelles Feld in der Antwort des Servers. Jedes Feldpaket beschreibt die Eigenschaften der zugeordneten Spalte. Die Paketzahl (i) beginnt bei 0.

  Parameter:

  i - Paketnummer
- **MYSQL.RES.FIELD(<i>).CATALOG.** Gibt die Katalogeigenschaft des Feldpakets zurück.
- **MYSQL.RES.FIELD(<i>).CHAR_SET.** Gibt den Zeichensatz der Spalte zurück. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Präfix verwendet.
- **MYSQL.RES.FIELD(<i>).DATATYPE.** Gibt eine Aufzählungskonstante zurück, die den Datentyp der Spalte darstellt. Dies ist das Typattribut (auch enum_field_type genannt) der Spalte. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Präfix verwendet. Die möglichen Werte für die verschiedenen Datentypen sind:
  - DEZIMALZAHL
  - WINZIG
  - KURZ
  - LANG
  - SCHWEBEN
  - VERDOPPELN
  - NULL
  - ZEITSTEMPEL
  - LANG
  - INT24
  - DATUM
  - ZEIT
  - DATUM/UHRZEIT
  - JAHR
  - NEUES DATUM
  - VARCHAR (neu in MySQL 5.0)

  - BIT (neu in MySQL 5.0)
  - NEWDECIMAL (neu in MySQL 5.0)
  - AUFZÄHLUNG
  - SETZEN
  - TINY_BLOB
  - MEDIUM_BLOB
  - LONG_BLOB
  - KLECKS
  - VAR_STRING
  - SCHNUR
  - GEOMETRIE

- **MYSQL.RES.FIELD(<i>).DB.** Gibt das Datenbank-Identifier (db) -Attribut des Feldpakets zurück.
- **MYSQL.RES.FIELD(<i>).DECIMALS.** Gibt die Anzahl der Stellen nach dem Dezimaltrennzeichen zurück, wenn der Typ DECIMAL oder NUMERIC ist. Dies ist das Dezimalattribut des Feldpakets.
- **MYSQL.RES.FIELD(<i>).FLAGS.** Gibt die Flags-Eigenschaft des Feldpakets zurück. Im Folgenden sind die möglichen hexadezimalen Flag-Werte aufgeführt:
  - 0001: NOT_NULL_FLAG
  - 0002: PRI_KEY_FLAG
  - 0004: UNIQUE_KEY_FLAG
  - 0008: FLAGGE MIT MEHREREN SCHLÜSSELN
  - 0010: BLOB_FLAG
  - 0020: FLAGGE OHNE SIGNATUR
  - 0040: NULLFÜLL-FLAGGE
  - 0080: BINÄRE FLAGGE
  - 0100: ENUM_FLAG
  - 0200: AUTO_INCREMENT_FLAG
  - 0400: ZEITSTEMPEL_FLAGGE
  - 0800: FLAGGE SETZEN
- **MYSQL.RES.FIELD(<i>).LENGTH.** Gibt die Länge der Spalte zurück. Dies ist der Wert des Längenattributs des Feldpakets. Der zurückgegebene Wert ist möglicherweise größer als der tatsächliche Wert. Beispielsweise kann eine Instanz einer VARCHAR (2) -Spalte den Wert 2 zurückgeben, selbst wenn sie nur ein Zeichen enthält.
- **MYSQL.RES.FIELD(<i>).NAME.** Gibt den Spaltenbezeichner zurück (den Namen nach der AS-Klausel, falls vorhanden). Dies ist das Namensattribut des Feldpakets.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_NAME.** Gibt den ursprünglichen Spaltenbezeichner zurück (vor der AS-Klausel, falls vorhanden). Dies ist das org_name-Attribut des Feldpakets.

- **MYSQL.RES.FIELD(<i>).ORIGINAL_TABLE.** Gibt den ursprünglichen Tabellenbezeichner der Spalte zurück (vor der AS-Klausel, falls vorhanden). Dies ist das org_table-Attribut des Feldpakets.
- **MYSQL.RES.FIELD(<i>).TABLE.** Gibt den Tabellenbezeichner der Spalte zurück (nach der AS-Klausel, falls vorhanden). Dies ist das Tabellenattribut des Feldpakets.
- **MYSQL.RES.FIELDS_COUNT.** Gibt die Anzahl der Feldpakete in der Antwort zurück (das field_count-Attribut des OK-Pakets).
- **MYSQL.RES.OK.** Identifiziert das vom Datenbankserver gesendete OK-Paket.
- **MYSQL.RES.OK.AFFECTED_ROWS.** Gibt die Anzahl der Zeilen zurück, die von einer INSERT-, UPDATE- oder DELETE-Abfrage betroffen sind. Dies ist der Wert des Attributs affected_rows des OK-Pakets.
- **MYSQL.RES.OK.INSERT_ID.** Identifiziert das unique_id-Attribut des OK-Pakets. Wenn durch die aktuelle MySQL-Anweisung oder Abfrage keine automatisch inkrementierte Identität generiert wird, ist der Wert von unique_id und damit der vom Ausdruck zurückgegebene Wert 0.
- **MYSQL.RES.OK.MESSAGE.** Gibt die Nachrichteneigenschaft des OK-Pakets zurück.
- **MYSQL.RES.OK.STATUS.** Identifiziert die Bitzeichenfolge im server_status-Attribut des OK-Pakets. Clients können den Serverstatus verwenden, um zu überprüfen, ob der aktuelle Befehl Teil einer laufenden Transaktion ist. Die Bits in der Server_status-Bitzeichenfolge entsprechen den folgenden Feldern (in der angegebenen Reihenfolge):
  - IN DER TRANSAKTION
  - AUTO_COMMIT
  - MEHR ERGEBNISSE
  - MEHRFACHABFRAGE
  - FALSCHER INDEX VERWENDET
  - KEIN INDEX VERWENDET
  - CURSOR IST VORHANDEN
  - LETZTE ZEILE GESEHEN
  - DATENBANK WURDE GELÖSCHT
  - KEIN BACKSLASH-ESCAPES
- **MYSQL.RES.OK.WARNING_COUNT.** Gibt das warning_count-Attribut des OK-Pakets zurück.
- **MYSQL.RES.ROW(<i>).** Identifiziert das Paket, das i^{th entspricht} einzelne Zeile in der Antwort des Datenbankservers.

  Parameter:

  i - Zeilennummer

- **MYSQL.RES.ROW(<i>).DOUBLE_ELEM(<j>).** Prüft, ob das jth Spalte des ith Zeile der Tabelle ist NULL. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0. Daher sind Zeile i und Spalte j tatsächlich das (i+1)th Zeile und (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.ROW(<i>).IS_NULL_ELEM(j).** Prüft, ob das jth Spalte des ith Zeile der Tabelle ist NULL. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0. Daher sind Zeile i und Spalte j tatsächlich das (i+1)th Zeile und (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.ROW(<i>).NUM_ELEM(<j>).** Gibt einen ganzzahligen Wert aus j^{th zurück} Spalte des ith Zeile der Tabelle. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0. Daher sind Zeile i und Spalte j tatsächlich das (i+1)th Zeile und (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.ROW(<i>).TEXT_ELEM(j).** Gibt eine Zeichenfolge aus j^{th zurück} Spalte des ith Zeile der Tabelle. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0. Daher sind Zeile i und Spalte j tatsächlich das (i+1)th Zeile und (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.TYPE.** Gibt eine Aufzählungskonstante für den Antworttyp zurück. Seine Werte können ERROR, OK und RESULT_SET sein. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Präfix verwendet.

Ausdrücke für die Bewertung von Microsoft SQL-Serververbindungen

Die folgenden Ausdrücke werten den Datenverkehr aus, der mit Microsoft SQL Server-Datenbankservern verknüpft ist. Sie können die anforderungsbasierten Ausdrücke (Ausdrücke, die mit MSSQL.CLIENT und MSSQL.REQ beginnen) in Richtlinien verwenden, um Entscheidungen zum Umschalten von Anfragen am Bindungspunkt des virtuellen Content-Switching-Servers zu treffen, und die antwortbasierten Ausdrücke (Ausdrücke, die mit MSSQL.RES beginnen), um Serverantworten auf benutzerkonfigurierte Integritätsmonitore auszuwerten.

Ausdruck	Beschreibung
MSSQL.CLIENT.CAPABILITIES	Gibt die Felder OptionFlags1, OptionFlags2, OptionFlags3 und TypeFlags des Login7Authentication-Pakets in dieser Reihenfolge als 4-Byte-Ganzzahl zurück. Jedes Feld ist 1 Byte lang und spezifiziert eine Reihe von Client-Funktionen.
MSSQL.CLIENT.DATABASE	Gibt den Namen der Client-Datenbank zurück. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.CLIENT.USER	Gibt den Benutzernamen zurück, mit dem sich der Client authentifiziert hat. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.REQ.COMMAND	Gibt eine Aufzählungskonstante zurück, die den Befehlstyp in der Anforderung identifiziert, die an einen Microsoft SQL Server-Datenbankserver gesendet wurde. Der zurückgegebene Wert ist vom Typ Text. Beispiele für die Werte der Aufzählungskonstante sind QUERY, RESPONSE, RPC und ATTENTION. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Ausdruck verwendet.
MSSQL.REQ.QUERY.COMMAND	Gibt das erste Schlüsselwort in der SQL-Abfrage zurück. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.REQ.QUERY.SIZE	Gibt die Größe der SQL-Abfrage in der Anfrage zurück. Der zurückgegebene Wert ist eine Zahl.

Ausdruck	Beschreibung
MSSQL.REQ.QUERY.TEXT	Gibt die gesamte SQL-Abfrage als Zeichenfolge zurück. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.REQ.QUERY.TEXT(<n>)	Gibt die ersten n Byte der SQL-Abfrage zurück. Der zurückgegebene Wert ist vom Typ Text. Parameter: n - Anzahl der Bytes
MSSQL.REQ.RPC.NAME	Gibt den Namen der Prozedur zurück, die in einer RPC-Anfrage (Remote Procedure Call) aufgerufen wird. Der Name wird als Zeichenfolge zurückgegeben.
MSSQL.REQ.RPC.IS_PROCID	Gibt einen booleschen Wert zurück, der angibt, ob die RPC-Anforderung (Remote Procedure Call) eine Prozedur-ID oder einen RPC-Namen enthält. Ein Rückgabewert von TRUE gibt an, dass die Anforderung eine Prozedur-ID enthält, und ein Rückgabewert von FALSE gibt an, dass die Anforderung einen RPC-Namen enthält.
MSSQL.REQ.RPC.PROCID	Gibt die Prozedur-ID der RPC-Anfrage (Remote Procedure Call) als Ganzzahl zurück.
MSSQL.REQ.RPC.BODY **Hinweis:** Nicht verfügbar für Versionen vor 10.1.	Gibt den Text der SQL-Anfrage als Zeichenfolge in Form von Parametern zurück, die als durch Kommas getrennte „a=b“ -Klauseln dargestellt werden, wobei „a“ der RPC-Parametername und „b“ sein Wert ist.
MSSQL.REQ.RPC.BODY(n) **Hinweis:** Nicht verfügbar für Versionen vor 10.1.	Gibt einen Teil des Hauptteils der SQL-Anfrage als Zeichenfolge in Form von Parametern zurück, die als durch Kommas getrennte „a=b“ -Klauseln dargestellt werden, wobei „a“ der RPC-Parametername und „b“ sein Wert ist. Parameter werden nur aus den ersten „n“ Bytes der Anfrage zurückgegeben, wobei der SQL-Header übersprungen wird. Es werden nur vollständige Name-Wert-Paare zurückgegeben.

Ausdruck	Beschreibung
MSSQL.RES.ATLEAST_ROWS_COUNT(i)	Prüft, ob die Antwort mindestens eine Anzahl von Zeilen enthält. Der zurückgegebene Wert ist ein boolescher Wert TRUE oder FalseValue. Parameter: i - Anzahl der Zeilen
MSSQL.RES.DONE.ROWCOUNT	Gibt die Anzahl der Zeilen zurück, die von einer INSERT-, UPDATE- oder DELETE-Abfrage betroffen sind. Der zurückgegebene Wert ist vom Typ unsigned long.
MSSQL.RES.DONE.STATUS	Gibt das Statusfeld des DONE-Tokens zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wurde. Der zurückgegebene Wert ist eine Zahl.
MSSQL.RES.ERROR.MESSAGE	Gibt die Fehlermeldung des ERROR-Tokens zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wurde. Dies ist der Wert des Felds MsgText im ERROR-Token. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.RES.ERROR.NUM	Gibt die Fehlernummer aus dem ERROR-Token zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wurde. Dies ist der Wert des Zahlenfeldes im ERROR-Token. Der zurückgegebene Wert ist eine Zahl.
MSSQL.RES.ERROR.STATE	Gibt den Fehlerstatus des ERROR-Tokens zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wurde. Dies ist der Wert des Felds State im ERROR-Token. Der zurückgegebene Wert ist eine Zahl.

Ausdruck	Beschreibung
MSSQL.RES.FIELD(<i>).DATATYPE	Gibt den Datentyp des it-Feldes in der Serverantwort zurück. Die Funktionen EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Präfix verwendet. Der folgende Ausdruck gibt beispielsweise den booleschen Wert TRUE zurück, wenn die DATATYPE-Funktion den Wert datetime für das dritte Feld in der Antwort zurückgibt: MSSQL.RES.FIELD(<2>).DATATYPE.EQ(datetime) Parameters: i - Row number
MSSQL.RES.FIELD(<i>).LENGTH	Gibt die maximal mögliche Länge des it-Feldes in der Serverantwort zurück. Der zurückgegebene Wert ist eine Zahl. Parameter: i - Zeilennummer
MSSQL.RES.FIELD(<i>).NAME	Gibt den Namen des ith-Feldes in der Serverantwort zurück. Der zurückgegebene Wert ist vom Typ Text. Parameter: i - Zeilennummer
MSSQL.RES.ROW(<i>).DOUBLE_ELEM(<j>)	Gibt einen Wert vom Typ double aus der J-ten Spalte der 9. Zeile der Tabelle zurück. Wenn der Wert kein Doppelwert ist, wird eine UNDEF-Bedingung ausgelöst. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) -te Zeile bzw. die (j + 1) -te Spalte. Parameter: i - Zeilennummer j - Spaltennummer

Ausdruck	Beschreibung
MSSQL.RES.ROW(<i>).NUM_ELEM(j)	Gibt einen Ganzzahlwert aus der J-ten Spalte einer Zeile der Tabelle zurück. Wenn der Wert kein Integer-Wert ist, wird eine UNDEF-Bedingung ausgelöst. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) -te Zeile bzw. die (j + 1) -te Spalte. Parameter: i - Zeilennummer j - Spaltennummer
MSSQL.RES.ROW(<i>).IS_NULL_ELEM(j)	Prüft, ob die jte Spalte der ersten Zeile der Tabelle NULL ist, und gibt als Ergebnis den booleschen Wert TRUE oder FALSE zurück. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) -te Zeile bzw. die (j + 1) -te Spalte. Parameter: i - Zeilennummer j - Spaltennummer
MSSQL.RES.ROW(<i>).TEXT_ELEM(j)	Gibt eine Textzeichenfolge aus der jth-ten Spalte einer Zeile der Tabelle zurück. Gemäß den C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) -te Zeile bzw. die (j + 1) -te Spalte. Parameter: i - Zeilennummer j - Spaltennummer
MSSQL.RES.TYPE	Gibt eine Aufzählungskonstante zurück, die den Antworttyp identifiziert. Im Folgenden sind die möglichen Rückgabewerte aufgeführt: ERROR, OK und RESULT_SET. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Ausdruck verwendet.

Typumwandlung von Daten

August 19, 2021

Sie können Daten eines Typs (z. B. Text oder Ganzzahl) aus Anfragen und Antworten extrahieren und in Daten eines anderen Typs transformieren. Beispielsweise können Sie eine Zeichenfolge extrahieren und die Zeichenfolge in ein Zeitformat umwandeln. Sie können auch eine Zeichenfolge aus einem HTTP-Anforderungskörper extrahieren und sie wie ein HTTP-Header behandeln oder einen Wert aus einem Anforderungsheader extrahieren und in einen Antwort-Header eines anderen Typs einfügen.

Nach dem Typumstellen der Daten können Sie jeden Vorgang anwenden, der für den neuen Datentyp geeignet ist. Wenn Sie beispielsweise Text in einen HTTP-Header eingeben, können Sie jeden Vorgang anwenden, der auf HTTP-Header anwendbar ist, auf den zurückgegebenen Wert.

Weitere Informationen zum Typecasting von Daten finden Sie in der PDF-Datei Typecasting Operations .

Reguläre Ausdrücke

May 11, 2023

Wenn Sie Zeichenfolgenabgleichsoperationen ausführen möchten, die komplexer sind als die Operationen, die Sie mit den Operatoren CONTAINS("<string>") oder EQ("<string>") ausführen, verwenden Sie reguläre Ausdrücke. Die Richtlinieninfrastruktur auf der Citrix® NetScaler® Appliance umfasst Operatoren, an die Sie reguläre Ausdrücke als Argumente für den Textabgleich übergeben können. Zu den Namen der Operatoren, die mit regulären Ausdrücken arbeiten, gehört die Zeichenfolge REGEX. Die regulären Ausdrücke, die Sie als Argumente übergeben, müssen der Syntax für reguläre Ausdrücke entsprechen, die in beschrieben ist. "<http://www.pcre.org/pcre.txt>." Sie können mehr über reguläre Ausdrücke unter "<http://www.regular-expressions.info/quickstart.html>" und unter erfahren "<http://www.silverstones.com/thebat/Regex.html>."

Der Zieltext für einen Operator, der mit regulären Ausdrücken arbeitet, kann entweder Text oder der Wert eines HTTP-Headers sein. Es folgt das Format eines erweiterten Richtlinienausdrucks, der einen Operator für reguläre Ausdrücke verwendet, um Text zu verwenden:

```
<text>.<regex_operator>(re<delimiter><regex_pattern><delimiter>)
```

Die Zeichenfolge <text> stellt das Präfix für den erweiterten Richtlinienausdruck dar, das eine Textzeichenfolge in einem Paket identifiziert (z. B. HTTP.REQ.URL). Die Zeichenfolge <regex_operator> repräsentiert den Operator für reguläre Ausdrücke Der reguläre Ausdruck beginnt immer mit der

Zeichenfolge re. Ein Paar übereinstimmender Trennzeichen, dargestellt durch <delimiter>, umschließt die Zeichenfolge <regex_pattern>, die den regulären Ausdruck darstellt.

Der folgende Beispielausdruck prüft, ob die URL in einem HTTP-Paket die Zeichenfolge *.jpeg enthält (wobei * es sich um einen Platzhalter handelt) und gibt ein boolesches TRUE oder FALSE zurück, um das Ergebnis anzuzeigen. Der reguläre Ausdruck ist in ein Paar von Schrägstrichen (/) eingeschlossen, die als Trennzeichen dienen.

```
http.req.url.regex_match(re/.<asterisk>\.jpeg/)
```

Operatoren für reguläre Ausdrücke können kombiniert werden, um den Umfang einer Suche zu definieren oder zu verfeinern. <text>.AFTER_REGEX(reregex_pattern1).BEFORE_REGEX(reregex_pattern2) gibt beispielsweise an, dass das Ziel für den Zeichenfolgenabgleich der Text zwischen den Mustern regex_pattern1 und regex_pattern2 ist. Sie können einen Textoperator für den Bereich verwenden, der durch die Operatoren für reguläre Ausdrücke definiert ist. Beispielsweise können Sie den Operator CONTAINS ("<string>") verwenden, um zu überprüfen, ob der definierte Bereich die Zeichenfolge abc enthält:

```
<text>.AFTER_REGEX(re/regex_pattern1).BEFORE_REGEX(re/regex_pattern2/).
CONTAINS("abc")
```

> **Hinweis**
>
> Der Prozess der Auswertung eines regulären Ausdrucks benötigt inhärent mehr Zeit als für einen Operator wie CONTAINS ("<string>") oder EQ ("<string>"), die mit einfachen Zeichenfolgenargumenten arbeiten. Sie sollten reguläre Ausdrücke nur verwenden, wenn Ihre Anforderung außerhalb des Bereichs anderer Operatoren liegt.

Grundlegende Eigenschaften regulärer Ausdrücke

May 11, 2023

Im Folgenden sind die wichtigsten Merkmale regulärer Ausdrücke aufgeführt, wie sie auf der NetScaler-Appliance definiert sind:

- Ein regulärer Ausdruck beginnt immer mit der Zeichenfolge „re“, gefolgt von einem Paar von Trennzeichen (sogenannten Trennzeichen), die den regulären Ausdruck umschließen, den Sie verwenden möchten.

Beispielsweise verwendet re#<regex_pattern># das Nummernzeichen (#) als Trennzeichen.

- Ein regulärer Ausdruck darf 1499 Zeichen nicht überschreiten.
- Der Ziffernabgleich kann mit der Zeichenfolge\ d (ein umgekehrter Schrägstrich gefolgt von d) durchgeführt werden.

- Leerzeichen können durch die Verwendung von\ s (ein umgekehrter Schrägstrich gefolgt von s) dargestellt werden.
- Ein regulärer Ausdruck kann Leerzeichen enthalten.

Im Folgenden sind die Unterschiede zwischen der NetScaler-Syntax und der PCRE-Syntax aufgeführt:

- Der NetScaler erlaubt keine Rückverweise in regulären Ausdrücken.
- Sie sollten keine rekursiven regulären Ausdrücke verwenden.
- Das Punkt-Metazeichen entspricht auch dem Zeilenumbruchzeichen.
- Unicode wird nicht unterstützt.
- Die Operation SET_TEXT_MODE (IGNORECASE) überschreibt die (? i) interne Option im regulären Ausdruck.

Operationen für reguläre Ausdrücke

October 8, 2021

In der folgenden Tabelle werden die Operatoren beschrieben, die mit regulären Ausdrücken arbeiten. Die Operation, die von einem Operator für reguläre Ausdrücke in einem bestimmten erweiterten Richtlinienausdruck ausgeführt wird, hängt davon ab, ob das Ausdruckspräfix Text oder HTTP-Header identifiziert. Operationen, die Header auswerten, überschreiben alle textbasierten Operationen für alle Instanzen des angegebenen Header-Typs. Wenn Sie einen Operator verwenden, <text>ersetzen Sie durch das Präfix für erweiterte Richtlinienausdrücke, das Sie zum Identifizieren von Text konfigurieren möchten.

Operation für reguläre Ausdrücke	Beschreibung
<text>.BEFORE_REGEX (<regular expression>)	Wählt den Text aus, der der Zeichenfolge vorausgeht, die dem <regular expression>Argument entspricht. Wenn der reguläre Ausdruck mit keinen Daten im Ziel übereinstimmt, gibt der Ausdruck ein Textobjekt mit der Länge 0 zurück. Der folgende Ausdruck wählt die Zeichenfolge “text” aus “text/plain”. http.res.header (“content-type”) .before_regex (re#/#)

Operation für reguläre Ausdrücke	Beschreibung
<text>.AFTER_REGEX (<regular expression>)	Wählt den Text aus, der der Zeichenfolge folgt, die dem <regular expression>Argument entspricht. Wenn der reguläre Ausdruck mit keinem Text im Ziel übereinstimmt, gibt der Ausdruck ein Textobjekt mit der Länge 0 zurück. Der folgende Ausdruck extrahiert “Beispiel” aus “myExample”: http.req.header (“etag”) .after_regex (re/my/)
<text>.REGEX_SELECT (<regular expression>)	Wählt eine Zeichenfolge aus, die dem <regular expression>Argument entspricht. Wenn der reguläre Ausdruck nicht mit dem Ziel übereinstimmt, wird ein Textobjekt der Länge 0 zurückgegeben. Das folgende Beispiel extrahiert die Zeichenfolge “NS-CACHE-9.0:90” aus einem Via-Header: http.req.header (“via”) .regex_select (re! NS-CACHE-\ d.\ d:\ s*\ d {1,3}!)

Operation für reguläre Ausdrücke	Beschreibung
<text>.REGEX_MATCH (<regular expression>)	Gibt TRUE zurück, wenn das Ziel einem <regular expression>Argument mit bis zu 1499 Zeichen entspricht. Der reguläre Ausdruck muss das folgende Format haben: re <delimiter>regulärer Ausdruck< delimiter> Beide Trennzeichen müssen gleich sein. Zusätzlich muss der reguläre Ausdruck der Perl-kompatiblen (PCRE) Bibliothekssyntax für reguläre Ausdrücke entsprechen. Weitere Information finden Sie unter http://www.pcre.org/pcre.txt. Siehe insbesondere die Manpage pcrepattern. Beachten Sie jedoch Folgendes: Rückverweise sind nicht zulässig. Rekursive reguläre Ausdrücke werden nicht empfohlen. Das Punkt-Metazeichen entspricht auch dem Zeilenumbruchzeichen. Der Unicode-Zeichensatz wird nicht unterstützt. SET_TEXT_MODE (IGNORECASE) überschreibt die (?i) interne Option im regulären Ausdruck angegeben. The following are examples: http.req.hostname.regex_match(re/[[:alpha:]]+(abc){2,3}/) and http.req.url.set_text_mode(urlencoded).regex_match(re#(a*b- The following example matches ab and aB: http.req.url.regex_match(re/a(?i)b/) The following example matches ab, aB, Ab and AB: http.req.url.set_text_mode(ignorecase).regex_match(re/ab/) The following example performs a case-insensitive, multiline match in which the dot meta-character also matches a newline character: http.req.body.regex_match(re/(?ixm) (^ab (.*) cd$) /)

Zusammenfassende Beispiele für erweiterte Richtlinienausdrücke und Richtlinien

May 11, 2023

Die folgende Tabelle enthält Beispiele für erweiterte Richtlinienausdrücke, die Sie als Grundlage für Ihre eigenen erweiterten Richtlinienausdrücke verwenden können.

Tabelle 1. Beispiele für erweiterte Richtlinienausdrücke

Ausdruck-Typ	Beispiel Ausdrücke
Sehen Sie sich die in der HTTP-Anforderung verwendete Methode an.	`http.req.method.eq(post)http.req.method.eq(get)`

Prüfen Sie den Cache-Control - oder Pragma-Header-Wert in einer HTTP-Anforderung (req) oder Response (res).	`http.req.header("Cache-Control").contains("no-store")`
	`http.req.header("Cache-Control").contains("no-cache")`
	`http.req.header("Pragma").contains("no-cache")`
	`http.res.header("Cache-Control").contains("private")`
	`http.res.header("Cache-Control").contains("public")`
	`http.res.header("Cache-Control").contains("must-revalidate")http.res.header("Cache-Control").contains ("proxy-revalidate")`
	`http.res.header("Cache-Control").contains("max-age")`

Prüfen Sie, ob ein Header in einer Anfrage (req) oder Antwort (res) vorhanden ist.	`http.req.header("myHeader").exists` `http.res.header("myHeader").exists`

Ausdruck-Typ	Beispiel Ausdrücke
Suchen Sie in einer HTTP-Anforderung basierend auf der Dateierweiterung nach einem bestimmten Dateityp.	`http.req.url.contains(".html")http.req.url.contains(".cgi")http.req.url.contains(".asp")http.req.url.contains(".exe")http.req.url.contains(".cfm")http.req.url.contains(".ex")http.req.url.contains(".shtml")http.req.url.contains(".htx")http.req.url.contains("/cgi-bin/")http.req.url.contains("/exec/")http.req.url.contains("/bin/")`
Suchen Sie in einer HTTP-Anfrage nach etwas anderem als einem bestimmten Dateityp.	`http.req.url.contains(".png").not; http.req.url.contains(".jpeg").not`
Überprüfen Sie den Dateityp, der in einer HTTP-Antwort basierend auf dem Content-Type-Header gesendet wird.	`http.res.header("Content-Type").contains("text")http.res.header("Content-Type").contains "application/msword")http.res.header("Content-Type").contains("vnd.ms-excel")http.res.header("Content-Type").contains("application/vnd.ms-powerpoint"); http.res.header("Content-Type").contains("text/css"); http.res.header("Content-Type").contains("text/xml"); http.res.header("Content-Type").contains("image/")`
Überprüfen Sie, ob diese Antwort einen Ablaufheader enthält.	`http.res.header("Expires").exists`
Überprüfen Sie in einer Antwort auf einen Set-Cookie-Header.	`http.res.header("Set-Cookie").exists`
Überprüfen Sie den Agenten, der die Antwort gesendet hat.	`http.res.header("User-Agent").contains("Mozilla/4.7")http.res.header("User-Agent").contains("MSIE")`

Ausdruck-Typ	Beispiel Ausdrücke
Überprüfen Sie, ob die ersten 1024 Bytes des Body einer Anfrage mit der Zeichenfolge “some text” beginnen.	`http.req.body(1024).contains("some text")`

Die folgende Tabelle zeigt Beispiele für Richtlinienkonfigurationen und Bindungen für häufig verwendete Funktionen.

Tabelle 2. Beispiele für erweiterte Richtlinienausdrücke und Richtlinien

Zweck	Beispiel
Verwenden Sie die Rewrite-Funktion, um Vorkommen von `http://with https://` im Hauptteil einer HTTP-Antwort zu ersetzen.	`add rewrite action httpRewriteAction replace_all http.res.body(50000)"\"https://\""-search http://add rewrite policy demo_rep34312 "http.res.body(50000).contains(\"http://\")" httpRewriteAction`
Ersetzen Sie alle Vorkommen von “abcd” durch “1234” in den ersten 1000 Byte des HTTP-Hauptkörpers.	`add rewrite action abcdTo1234Action replace_all "http.req.body(1000)""\"1234\""-search abcd add rewrite policy abcdTo1234Policy "http.req.body(1000).contains(\"abcd\")" abcdTo1234Action bind rewrite global abcdTo1234Policy 100 END -type REQ_OVERRIDE`
Downgrade der HTTP-Version auf 1.0, um zu verhindern, dass der Server HTTP-Antworten chunkiert.	`add rewrite action downgradeTo1.0Action replace http.req.version.minor "\"0\""add rewrite policy downgradeTo1.0Policy "http.req.version.minor.eq(1)"downgradeTo1.0Action bind lb vserver myLBVserver -policyName downgradeTo1.0Policy -priority 100 -gotoPriorityExpression NEXT -type REQUEST`

Zweck	Beispiel
Entfernen Sie in allen Antworten Verweise auf das HTTP- oder HTTPS-Protokoll. Wenn die Verbindung des Benutzers HTTP ist, wird der Link mithilfe von HTTP geöffnet, und wenn die Verbindung des Benutzers HTTPS ist, wird der Link mithilfe von HTTPS geöffnet.	`add rewrite action remove_http_https replace_all "http.res.body(1000000).set_text_mode(ignorecase)""\"//\""-search "re~https?://|HTTPS?://~"add rewrite policy remove_http_https true remove_http_https bind lb vserver test_vsvr -policyName remove_http_https -priority 20 -gotoPriorityExpression NEXT -type RESPONSE`
Schreiben Sie Instanzen von http: in allen URLs um.	`add responder action httpToHttpsAction redirect "\"https://\" + http.req.hostname + http.req.url"add responder policy httpToHttpsPolicy "!CLIENT.SSL.IS_SSL"httpToHttpsAction bind responder global httpToHttpsPolicy 1 END -type OVERRIDE`
Ändern Sie eine URL, um von URL A nach URL B umzuleiten. In diesem Beispiel wird “file5.html” an den Pfad angehängt.	`add responder action appendFile5Action redirect \"http://\" + http.req.hostname + http.req.url + \"/file5.html\""add responder policy appendFile5Policy "http.req.url.eq(\"/testsite\")" appendFile5Action bind responder global appendFile5Policy 1 END -type OVERRIDE`

Zweck	Beispiel
Leiten Sie eine externe URL auf eine interne URL um.	`add rewrite action act_external_to_internal REPLACE 'http.req.hostname.server'"www.my.host.com"'add rewrite policy pol_external_to_internal 'http.req.hostname.server.eq("www.external.host.com")'act_external_to_internal bind rewrite global pol_external_to_internal 100 END -type REQ_OVERRIDE`
Leiten Sie Anfragen an www.example.com um, die eine Abfragezeichenfolge haben, an www.webn.example.com. Der Wert n wird von einem Serverparameter in der Abfragezeichenfolge abgeleitet, z. B. server=5.	`add rewrite action act_redirect_query REPLACE q##http.req.header("Host").before_str(".example.com")'"Web"+ http.req.url.query.value("server")## add rewrite policy pol_redirect_query q##http.req.header("Host").eq("www.example.com")&& http.req.url.contains("?")'act_redirect_query##`
Beschränken Sie die Anzahl der Anfragen pro Sekunde von einer URL.	`add ns limitSelector ip_limit_selector http.req.url "client.ip.src"add ns limitIdentifier ip_limit_identifier -threshold 4 -timeSlice 3600 -mode request_rate -limitType smooth -selectorName ip_limit_selector add responder action my_Web_site_redirect_action redirect "\"http://www.mycompany.com/\""add responder policy ip_limit_responder_policy "http.req.url.contains(\"myasp.asp\")&& sys.check_limit (\"ip_limit_identifier\")"my_Web_site_redirect_action bind responder global ip_limit_responder_policy 100 END -type default`

Zweck	Beispiel
Überprüfen Sie die IP-Adresse des Clients, geben Sie die Anforderung jedoch weiter, ohne die Anforderung zu ändern.	`add rewrite policy check_client_ip_policy 'HTTP.REQ. HEADER ("x-forwarded-for").EXISTS HTTP.REQ.HEADER ("client-ip"). EXISTS'NOREWRITE bind rewrite global check_client_ip_policy 100 END`
Entfernen Sie alte Header aus einer Anforderung und fügen Sie einen NS-Client-Header ein.	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy 'HTTP. REQ.HEADER("x-forwarded-for"). EXISTS'del_x_forwarded_for add rewrite policy check_client_ip_policy 'HTTP.REQ. HEADER("client-ip").EXISTS' del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client ' CLIENT.IP.SRC'add rewrite policy insert_ns_client_policy 'HTTP.REQ. HEADER("x-forwarded-for").EXISTS HTTP.REQ.HEADER("client-ip").EXISTS 'insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END`

Zweck	Beispiel
Entfernen Sie alte Header aus einer Anforderung, fügen Sie einen NS-Client-Header ein und ändern Sie dann die Aktion “Header einfügen”, sodass der Wert des eingefügten Headers die IP-Werte des Clients aus den alten Headern und die Verbindungs-IP-Adresse der NetScaler-Appliance enthält. Beachten Sie, dass in diesem Beispiel das vorherige Beispiel wiederholt wird, mit Ausnahme der Aktion zum Rewriterichtlinie des endgültigen Satzes.	‘add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy ‘HTTP.REQ.HEADER(“x-forwarded-for”).EXISTS’ del_x_forwarded_for add rewrite policy check_client_ip_policy ‘HTTP.REQ.HEADER(“client-ip”).EXISTS’ del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client ‘CLIENT.IP.SRC’ add rewrite policy insert_ns_client_policy ‘HTTP.REQ.HEADER(“x-forwarded-for”).EXISTS HTTP.REQ.HEADER(“client-ip”).EXISTS’ insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END set rewrite action insert_ns_client_header -stringBuilderExpr ‘HTTP.REQ.HEADER(“x-forwarded-for”).VALUE(0) + “ “ + HTTP.REQ.HEADER(“client-ip”).VALUE(0) + “ “ + CLIENT.IP.SRC’

Tutorial-Beispiele für erweiterte Rewriterichtlinien

August 4, 2023

Mit dem Rewrite können Sie einen beliebigen Teil eines HTTP-Headers ändern, und für Antworten können Sie den HTTP-Hauptteil ändern. Sie können diese Funktion verwenden, um mehrere nützliche Aufgaben auszuführen, z. B. das Entfernen unnötiger HTTP-Header, das Maskieren interner URLs, das Umleiten von Webseiten und das Umleiten von Abfragen oder Schlüsselwörtern.

In den folgenden Beispielen erstellen Sie zunächst eine Rewrite-Aktion und eine Rewriterichtlinie. Dann binden Sie die Richtlinie global.

Dieses Dokument enthält die folgenden Details:

- Umleiten einer externen URL auf eine interne URL
- Umleiten einer Abfrage
- Umschreiben von HTTP in HTTPS
- Entfernen unerwünschter Kopfzeilen
- Reduzieren von Webserver-Umleitungen
- Maskieren des Server-Headers
- Konvertieren von Klartext in eine URL-codierte Zeichenfolge und auf entgegengesetzte Weise

Weitere Informationen zu den Befehlen und Syntaxbeschreibungen finden Sie auf der Seite Rewrite-Befehlsreferenz.

Umleiten einer externen URL zu einer internen URL

In diesem Beispiel wird beschrieben, wie eine Rewrite-Aktion erstellt und eine Richtlinie neu geschrieben wird, die eine externe URL an eine interne URL umleitet. Sie erstellen eine Aktion namens act_external_to_internal, die das Rewrite durchführt. Anschließend erstellen Sie eine Richtlinie namens pol_external_to_internal.

So leiten Sie eine externe URL über die Befehlszeilenschnittstelle an eine interne URL um

- Um die Rewriteaktion zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add rewrite action act_external_to_internal REPLACE “http.req.hostname.
server” “\” host_name_of_internal_Web_server\” ”
```

- Um die Rewriterichtlinie zu erstellen, geben Sie an der NetScaler-Eingabeaufforderung Folgendes ein:

```
add rewrite policy pol_external_to_internal "http.req.hostname.server.eq(\"
host_name_of_external_Web_server\")"act_external_to_internal
```

- Binden Sie die Richtlinie global.

So leiten Sie eine externe URL mithilfe des Konfigurationsdienstprogramms an eine interne URL um

1. Navigieren Sie zu **AppExpert** > **Rewrite** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld “Rewrite-Aktion erstellen** “ den Namen act_external_to_internal ein.
4. Um den Hostnamen des HTTP-Servers durch den internen Servernamen zu **ersetzen, wählen Sie Ersetzen** aus dem Listenfeld Typ.

5. Geben Sie im Feld Header-Name **Host**ein.
6. Geben Sie im Zeichenfolgenausdruck für ein Ersetzungstextfeld den internen Hostnamen Ihres Webservers ein.
7. Klicken Sie auf **Create** und dann auf **Close**.
8. Klicken Sie im Navigationsbereich auf **Richtlinien**.
9. Klicken Sie im Detailbereich auf **Hinzufügen**.
10. Geben Sie im Feld Name pol_external_to_internal ein. Diese Richtlinie erkennt Verbindungen zum Webserver.
11. **Wählen Sie im Dropdownmenü Aktion die Aktion act_external_to_internal aus.**
12. Konstruieren Sie im Ausdruckseditor den folgenden Ausdruck:

```
HTTP.REQ.HOSTNAME.SERVER.EQ("www.example.com")
<!--NeedCopy-->
```

1. Binden Sie Ihre neue Richtlinie global.

Umleiten einer Abfrage

In diesem Beispiel wird beschrieben, wie eine Rewrite-Aktion erstellt und eine Richtlinie neu geschrieben wird, die eine Abfrage an die richtige URL umleitet. Das Beispiel geht davon aus, dass die Anfrage einen Host-Header enthält, der auf **www.example.com** gesetzt ist, und eine GET-Methode mit der **Zeichenfolge /query.cgi? Server=5**. Die Umleitung extrahiert den Domänennamen aus dem Host-Header und die Nummer aus der Abfragezeichenfolge und leitet die Abfrage des Benutzers an den Server **Web5.example.com**um, wo der Rest der Abfrage des Benutzers verarbeitet wird.

> **Hinweis:**
>
> Obwohl die folgenden Befehle in mehreren Zeilen angezeigt werden, müssen Sie sie in einer einzigen Zeile ohne Zeilenumbrüche eingeben.

So leiten Sie eine Abfrage mit der CLI an die entsprechende URL um

- Um eine Rewrite-Aktion namens act_redirect_query zu erstellen, die den Hostnamen des HTTP-Servers durch den internen Servernamen ersetzt, geben Sie Folgendes ein:

```
add rewrite action act_redirect_query REPLACE http.req.header("Host").
before_str(".example.com")'"Web" + http.req.url.query.value("server")'
```

- Um eine Rewriterichtlinie mit dem Namen pol_redirect_query zu erstellen, geben Sie die folgenden Befehle an der NetScaler-Eingabeaufforderung ein. Diese Richtlinie erkennt Verbindungen zum Webserver, die eine Abfragezeichenfolge enthalten. Wenden Sie diese Richtlinie nicht auf Verbindungen an, die keine Abfragezeichenfolge enthalten:


```
add rewrite policy pol_redirect_query 'http.req.header("Host").eq(www.
example.com)&& http.req.url.contains("?")'act_redirect_query
```

- Binden Sie Ihre neue Richtlinie global.

Da diese Rewriterichtlinie sehr spezifisch ist und vor anderen Rewriterichtlinien ausgeführt werden muss, ist es ratsam, ihr eine hohe Priorität zuzuweisen. Wenn Sie ihm eine Priorität von 1 zuweisen, wird sie zuerst ausgewertet.

Umschreiben von HTTP in HTTPS

In diesem Beispiel wird beschrieben, wie Webserver-Antworten neu geschrieben werden, um alle URLs zu finden, die mit der Zeichenfolge “HTTP” beginnen, und diese Zeichenfolge durch “https” ersetzen. Sie können damit vermeiden, Webseiten aktualisieren zu müssen, nachdem Sie einen Server von HTTP auf HTTPS verschoben haben.

So leiten Sie HTTP-URLs mit der CLI an HTTPS um

- Um eine Rewrite-Aktion namens act_replace_http_with_https zu erstellen, die alle Instanzen der Zeichenfolge “HTTP” durch die Zeichenfolge “https” ersetzt, geben Sie den folgenden Befehl ein:

```
add rewrite action act_replace_http_with_https replace_all 'http.res.body
(100)''"https"'-search text("http")
```

- Um eine Rewriterichtlinie mit dem Namen pol_replace_http_with_https zu erstellen, die Verbindungen zum Webserver erkennt, geben Sie den folgenden Befehl ein:

```
add rewrite policy pol_replace_http_with_https TRUE act_replace_http_with_https
 NOREWRITE
```

- Binden Sie Ihre neue Richtlinie global.

Informationen zur Behebung dieses Rewritevorgangs finden Sie unter “Fallstudie: Rewriterichtlinie von HTTP-Links in HTTPS funktioniert nicht. “

Entfernen unerwünschter Kopfzeilen

In diesem Beispiel wird erläutert, wie eine Rewriterichtlinie verwendet wird, um unerwünschte Header zu entfernen. Konkret zeigt das Beispiel, wie die folgenden Header entfernt werden:

- **Akzeptieren Sie den Kodierungskopf.** Das Entfernen des Accept Encoding Headers aus HTTP-Antworten verhindert die Komprimierung der Antwort.

- **Kopfzeile für Inhaltsstandort.** Durch das Entfernen des Content Location-Headers aus HTTP-Antworten wird verhindert, dass Ihr Server einem Hacker Informationen zur Verfügung stellt, die eine Sicherheitsverletzung zulassen könnten.

Um Header aus HTTP-Antworten zu löschen, erstellen Sie eine Rewriteaktion und eine Rewriterichtlinie und binden die Richtlinie global.

So erstellen Sie die entsprechende Rewrite-Aktion mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um entweder den Header Accept Encoding zu entfernen und die Antwortkomprimierung zu verhindern, oder den Inhaltsspeicher-Header zu entfernen:

- `add rewrite action "act_remove-ae"delete_http_header "Accept-Encoding"`
- `add rewrite action "act_remove-cl"delete_http_header "Content-Location"`

So erstellen Sie die entsprechende Rewriterichtlinie mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um entweder den Header Encoding akzeptieren oder den Header Content Location zu entfernen:

- `add rewrite policy "pol_remove-ae"true "act_remove-ae"`
- `add rewrite policy "pol_remove-cl"true "act_remove-cl"`

So binden Sie die Richtlinie global mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die erstellte Richtlinie global zu binden:

- `bind rewrite global pol_remove_ae 100`
- `bind rewrite global pol_remove_cl 200`

Reduzieren von Webserver-Umleitungen

In diesem Beispiel wird erläutert, wie Sie eine Rewriterichtlinie verwenden, um Verbindungen zu Ihrer Homepage und anderen URLs zu ändern, die mit einem Schrägstrich (/) auf die Standardindexseite für den Server enden, wodurch Umleitungen vermieden und die Belastung des Servers verringert wird.

So ändern Sie HTTP-Anfragen auf Verzeichnisebene so, dass sie die Standard-Homepage mit der CLI einschließen

- Geben Sie Folgendes ein, um eine Rewrite-Aktion mit dem Namen action-default-homepage zu erstellen, die URLs, die mit einem Schrägstrich enden, so dass sie die Standardstartseite in-

dex.html enthält:

```
add rewrite action "action-default-homepage"replace http.req.url.path "\"/
index.html\""
```

- Um eine Rewriterichtlinie mit dem Namen policy-default-homepage zu erstellen, die Verbindungen zu Ihrer Homepage erkennt und Ihre neue Aktion anwendet, geben Sie Folgendes ein:

```
add rewrite policy "policy-default-homepage"q\##http.req.url.path.EQ("/")"
action-default-homepage"\##
```

- Binden Sie Ihre neue Richtlinie global, um sie in Kraft zu setzen.

Maskieren des Server-Headers

In diesem Beispiel wird erläutert, wie Sie eine Rewriterichtlinie verwenden, um die Informationen im Server-Header in HTTP-Antworten vom Webserver zu maskieren. Dieser Header enthält Informationen, mit denen Hacker Ihre Website gefährden können. Während das Maskieren des Headers einen erfahrenen Hacker nicht daran hindert, Informationen über Ihren Server zu finden, erschwert dies das Hacken Ihres Webservers und ermutigt Hacker, weniger gut geschützte Ziele auszuwählen.

So maskieren Sie den Server-Header in Antworten von der CLI

1. Um eine Rewrite -Aktion namens act_mask-server zu erstellen, die den Inhalt des Server-Headers durch eine nicht informative Zeichenfolge ersetzt, geben Sie Folgendes ein:

```
add rewrite action "act_mask-server"replace "http.RES.HEADER(\"Server\")""
\"Web Server 1.0\""
```

1. Um eine Rewriterichtlinie mit dem Namen pol_mask-server zu erstellen, die alle Verbindungen erkennt, geben Sie Folgendes ein:

```
add rewrite policy "pol_mask-server"true "act_mask-server"
```

1. Binden Sie Ihre neue Richtlinie global, um sie in Kraft zu setzen.

Wie konvertiert man Nur-Text in eine URL-codierte Zeichenfolge und auf entgegengesetzte Weise

Die folgenden Ausdrücke wandeln Nur-Text in eine URL-codierte Zeichenfolge und umgekehrt um:

1. URL_RESERVED_CHARS_SAFE (string to URL ENCODED).

Beispiel:

```
("abc def&123").URL_RESERVED_CHARS_SAFE
Output will be
```



```
 “abc%20def%26123”  which is url encoded.
<!--NeedCopy-->
```

1. SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE. (URL ENCODED to string)

Beispiel:

```
("abc%20def%26123").SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE
Output will be
 “abc def&123”
<!--NeedCopy-->
```

Beispiele für Rewrite und Responder Policy

October 8, 2021

Im Folgenden finden Sie einige Beispiele für Rewrite- und Responder-Richtlinien:

Beispiel 1: So fügen Sie einen lokalen Client-IP-Header mit der Befehlszeilenschnittstelle hinzu

```
add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
   IP.SRC'
add rewrite policy pol_ins_client http.req.is_valid act_ins_client
bind rewrite global pol_ins_client 300 END

namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:06:48 GMT
* Server Apache/2.2.15 (CentOS) is not blacklisted
< Server: Apache/2.2.15 (CentOS)
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
```



```
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
< NS-Client: 10.102.1.98
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$

<!--NeedCopy-->
```

Beispiel 2: Maskieren Sie den HTTP-Servertyp

```
add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server") ""Web Server 1.0""
add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:15:42 GMT
* Server Web Server 1.0 is not blacklisted
< Server: Web Server 1.0
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: "816c5-5-58bbc1e73cdd3"
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$
<!--NeedCopy-->
```

Beispiel 3: Reagieren Sie, indem Sie zu einer anderen URL umleiten, wenn eine URL empfangen wird

```
> add responder action act1 redirect ""www.google.com""
```



```
 Done
> add responder policy pol1 'HTTP.REQ.URL.CONTAINS("file")' act1
 Done
> bind responder global pol1 1
 Done
>

name:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 302 Found : Moved Temporarily
< Location: www.google.com
< Connection: close
< Cache-Control: no-cache
< Pragma: no-cache
<
* Closing connection 0
name@obelix:~$
<!--NeedCopy-->
```

Beispiel 4: Antworte mit einer Nachricht, die ein beliebiger Ausdruck oder ein Text sein kann

```
add responder action act123 respondwith ""Please reach out to
   administrator""
add responder policy pol1 "HTTP.REQ.URL.CONTAINS("file")" act123
bind responder global pol1 100 END

name@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10..Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc"
   )" Redirect-Action
```



```
12
13 Binding to LB Virtual Server:
14
15 >bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -
      gotoPriorityExpression END -type REQUEST.
16 * Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
17 > GET /testsite/file5.html HTTP/1.1
18 > User-Agent: curl/7.35.0
19 > Host: 10.10.10.10
20 > Accept: \*/\*
21 >
22 * Connection #0 to host 10.10.10.10 left intact
23 Please reach out to administratort_name@obelix:~$
24 <!--NeedCopy-->
```

Beispiel 5: Reagieren Sie mit einer importierten HTML-Seite

```
1  import responder htmlpage http://10.10.10.10)/testsite/file5.html
      page112
2  add responder action act1 respondwithHtmlpage page1
3  add responder policy pol1 true act1
4  bind responder global pol1 100
5
6  name@obelix:~$ curl -v http://10.10.10.10)/testsite/file5.html
7  * Hostname was NOT found in DNS cache
8  *   Trying 10.10.10.10...
9  * Connected to 10.10.10.10 (10.10.10.10)) port 80 (#0)
10 > GET /testsite/file5.html HTTP/1.1
11 > User-Agent: curl/7.35.0
12 > Host: 10.102.58.140
13 > Accept: \*/\*
14 >
15 < HTTP/1.1 200 OK
16 < Content-Length: 5
17 < Content-Type: text/html
18 <
19 * Connection #0 to host 10.10.10.10 left intact
20 JLEwxt_name@obelix:~$
21 <!--NeedCopy-->
```

Beispiel 6: Umleitung von URL basierend auf HOSTNAME mithilfe der Responder-Richtlinie


```
Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/
   dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc"
   )" Redirect-Action

Binding to LB Virtual Server:

>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -
   gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Ratenlimit

May 11, 2023

Mit der Ratenbegrenzungsfunktion können Sie die maximale Last für eine bestimmte Netzwerkeinheit oder virtuelle Entität auf der NetScaler-Appliance definieren. Mit dieser Funktion können Sie die Appliance so konfigurieren, dass die mit der Entität verbundene Verkehrsrate überwacht und basierend auf der Verkehrsrate in Echtzeit vorbeugende Maßnahmen ergriffen werden. Diese Funktion ist besonders nützlich, wenn das Netzwerk von einem feindlichen Client angegriffen wird, der der Appliance eine Flut von Anfragen sendet. Sie können die Risiken mindern, die sich auf die Verfügbarkeit von Ressourcen für Clients auswirken, und Sie können die Zuverlässigkeit des Netzwerks und der Ressourcen, die die Appliance verwaltet, verbessern.

Sie können die Verkehrsrate überwachen und steuern, die virtuellen und benutzerdefinierten Entitäten zugeordnet ist, einschließlich virtueller Server, URLs, Domänen und Kombinationen von URLs und Domänen. Sie können die Verkehrsrate drosseln, wenn sie zu hoch ist, Basisinformationen über die Verkehrsrate zwischenspeichern und den Datenverkehr an einen bestimmten virtuellen Lastausgleichsserver umleiten, wenn die Verkehrsrate ein vordefiniertes Limit überschreitet. Sie können ratenbasierte Überwachung auf HTTP-, TCP- und DNS-Anfragen anwenden.

Um die Verkehrsrate für ein bestimmtes Szenario zu überwachen, konfigurieren Sie eine *Ratenbegrenzung*. Ein Ratenbegrenzungsbezeichner gibt numerische Schwellenwerte an, z. B. die maximale Anzahl von Anfragen oder Verbindungen (eines bestimmten Typs), die in einem bestimmten Zeitraum zulässig sind, der als *Zeitscheibe*bezeichnet wird.

Optional können Sie Filter konfigurieren, die als *Stream-Selektoren*bezeichnet werden, und sie bei der Konfiguration der Bezeichner mit Ratenbegrenzungskennungen verknüpfen. Nachdem Sie den

optionalen Stream-Selektor und den Limit-Bezeichner konfiguriert haben, müssen Sie die Limit-ID aus einer erweiterten Richtlinie aufrufen. Sie können Bezeichner von jeder Funktion aus aufrufen, in der der Bezeichner nützlich sein kann, einschließlich Rewrite, Responder, DNS und integriertes Caching.

Sie können SNMP-Traps für Kursbegrenzungskennungen global aktivieren und deaktivieren. Jedes Trap enthält kumulative Daten für das konfigurierte Datenerfassungsintervall (Zeitabschnitt) des Grenzwertbezeichners, es sei denn, Sie haben mehrere Traps angegeben, die pro Zeitabschnitt generiert werden sollen. Weitere Informationen zum Konfigurieren von SNMP-Traps und -Managern finden Sie unter SNMP.

Konfigurieren eines Stream-Selektors

May 11, 2023

Ein Traffic Stream-Selektor ist ein optionaler Filter zur Identifizierung einer Entität, für die Sie den Zugriff drosseln möchten. Der Selektor wird auf eine Anforderung oder eine Antwort angewendet und wählt Datenpunkte (Schlüssel) aus, die von einem Rate Stream Identifier analysiert werden können. Diese Datenpunkte können auf fast jedem Merkmal des Datenverkehrs basieren, einschließlich IP-Adressen, Subnetzen, Domainnamen, TCP- oder UDP-Identifikatoren und bestimmten Zeichenfolgen oder Erweiterungen in URLs.

Ein Stream-Selektor besteht aus einzelnen erweiterten Richtlinienausdrücken, die als Selectlets bezeichnet werden. Jedes Selectlet ist ein nicht zusammengesetzter erweiterter Richtlinienausdruck. Ein Traffic Stream-Selektor kann bis zu fünf nicht zusammengesetzte Ausdrücke enthalten, die als Selectlets bezeichnet werden. Jedes Selectlet wird als in einer UND-Beziehung zu den anderen Ausdrücken betrachtet. Nachfolgend einige Beispiele für Selectlets:

```
1 http.req.url
2 http.res.body(1000>after_str("car_model").before_str("made_in")"
3 "client.ip.src.subnet(24)"
4 <!--NeedCopy-->
```

Die Reihenfolge, in der Sie Parameter angeben, ist signifikant. Wenn Sie beispielsweise eine IP-Adresse und eine Domäne (in dieser Reihenfolge) in einem Selektor konfigurieren und dann die Domäne und die IP-Adresse (in umgekehrter Reihenfolge) in einem anderen Selektor angeben, betrachtet NetScaler diese Werte als eindeutig. Dies kann dazu führen, dass dieselbe Transaktion zweimal gezählt wird. Wenn mehrere Richtlinien denselben Selektor aufrufen, kann der NetScaler dieselbe Transaktion erneut mehr als einmal zählen.

Hinweis: Wenn Sie einen Ausdruck in einem Stream-Selektor ändern, wird möglicherweise eine Fehlermeldung angezeigt, wenn eine Policy Label, die ihn aufruft, an eine neue Richtlinienbezeichnung oder einen neuen Bindepunkt gebunden ist. Angenommen, Sie erstellen einen Stream-Selektor

mit dem Namen myStreamSelector1, rufen ihn von myLimitID1 aus auf und rufen den Bezeichner aus einer DNS-Richtlinie namens DNSRateLimit1 auf. Wenn Sie den Ausdruck in mystreamSelector1 ändern, wird möglicherweise eine Fehlermeldung angezeigt, wenn Sie DNSRateLimit1 an einen neuen Bindepunkt binden. Die Problemumgehung besteht darin, diese Ausdrücke zu ändern, bevor die Richtlinien erstellt werden, die sie aufrufen.

So konfigurieren Sie einen Traffic Stream-Selektor über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add stream selector <name> <rule> ...
<!--NeedCopy-->
```

Beispiel:

```
add stream selector myStreamSel HTTP.REQ.URL CLIENT.IP.SRC
<!--NeedCopy-->
```

So konfigurieren Sie einen Stream-Selektor mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu AppExpert > Ratenbegrenzung > Selektoren, klicken Sie auf Hinzufügen und geben Sie die relevanten Details an.

Konfigurieren einer Kennung des Verkehrsratenlimits

August 15, 2023

Ein Ratenbegrenzungsbezeichner prüft innerhalb eines bestimmten Zeitintervalls, ob die Menge des Datenverkehrs einen bestimmten Wert überschreitet. Der Bezeichner gibt ein “Boolesches TRUE” zurück, wenn die Menge des Datenverkehrs ein Limit innerhalb eines bestimmten Zeitintervalls überschreitet. Wenn Sie einen Grenzbezeichner in den zusammengesetzten DAvanced-Richtlinienausdruck in eine Richtlinienregel aufnehmen, müssen Sie einen Stream-Selektor einschließen. Wenn Sie nicht angeben, wird der Grenzwertbezeichner auf alle Anforderungen oder Antworten angewendet, die durch die zusammengesetzten Ausdrücke identifiziert werden.

> **Hinweis:**
>
> Die maximale Länge für das Speichern von Zeichenfolgenergebnissen (z. B. HTTP.REQ.URL) beträgt 60 Zeichen. Wenn die Zeichenfolge (z. B. URL) 1000 Zeichen lang ist, von denen 50 Zeichen

> lang genug sind, um eine Zeichenfolge eindeutig zu identifizieren, können Sie einen Ausdruck verwenden, um die erforderlichen 50 Zeichen zu extrahieren.

So konfigurieren Sie eine Traffic Limit-ID über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns limitIdentifier <limitIdentifier> -threshold <positive_integer>
    -timeSlice <positive_integer> -mode <mode> -limitType ( BURSTY |
    SMOOTH ) -selectorName <string> -maxBandwidth <positive_integer> -
    trapsInTimeSlice <positive_integer>
<!--NeedCopy-->
```

Beschreibung des Arguments

limitIdentifier. Name für eine Kennung für eine Ratenbegrenzung. Muss mit einem ASCII-Buchstaben oder Unterstrich (_) beginnen und darf nur aus alphanumerischen ASCII-Zeichen oder Unterstrichen bestehen. Reservierte Wörter dürfen nicht verwendet werden. Dies ist ein zwingendes Argument. Maximale Länge: 31

threshold. Eine maximale Anzahl von Anforderungen, die in der angegebenen Zeitleiste zulässig sind, wenn Anfragen (Modus ist als REQUEST_RATE festgelegt) pro Timeslice verfolgt werden. Wenn Verbindungen (Modus ist als CONNECTION eingestellt) verfolgt werden, ist dies die Gesamtzahl der Verbindungen, die durchgelassen würden. Standardwert: 1 Minimalwert: 1 Maximalwert: 4294967295

timeSlice. Zeitintervall in Millisekunden, angegeben in Vielfachen von 10, in dem Anfragen verfolgt werden, um zu überprüfen, ob sie den Schwellenwert überschreiten. Dieses Argument wird nur benötigt, wenn der Modus auf REQUEST_RATE gesetzt ist. Standardwert: 1000 Mindestwert: 10 Maximalwert: 4294967295

mode. Definiert die Art des Traffics, der verfolgt werden soll.

1. REQUEST_RATE. Verfolgt Anforderungen/Timeslice.
2. CONNECTION. Verfolgt aktive Transaktionen.

limitType. Definiert die Art des Limits.

- **Glatt**: Verteilt die Last gleichmäßig auf jedes Zeitfenster des eingestellten Zeitrahmens. Wird für konsistenten Anwendungsverkehr verwendet.
- **Bursty**: Ermöglicht die Weiterleitung von Anfragen, wenn die Last unter dem eingestellten Schwellenwert liegt. Wird für sporadischen Anwendungsverkehr verwendet. Es ist hilfreich, wenn die Belastung innerhalb des eingestellten Zeitrahmens jederzeit Spitzenwerte erreicht.

Beispielsweise sind die festgelegten maximalen Anfragen 100 und der Zeitrahmen 10 Sekunden. Wenn Ihre Anwendung in der ersten Sekunde 80 Anfragen erhält, verhalten sich diese Limittypen unterschiedlich. Der Bursty-Limit-Typ ermöglicht die Weiterleitung der Anfragen, da die Last unter dem festgelegten Schwellenwert liegt. Der Smooth-Limit-Typ erlaubt jedoch nur 10 Anfragen pro Sekunde. Es wendet also die konfigurierte Aktion für die überschüssige Last an.

selectorName. Name des Ratenbegrenzungs-Selektors. Wenn dieses Argument NULL ist, wird die Ratenbegrenzung auf den gesamten Datenverkehr angewendet, der vom virtuellen Server oder dem NetScaler empfangen wird (je nachdem, ob der Grenzwert an einen virtuellen Server oder global gebunden ist) ohne **Filterung. Maximale Länge: 31**

maxBandwidth. Maximal zulässige Bandbreite in KBit/s. Minimaler Wert: 0 Maximalwert: 4294967287

Beispiel:

Konfigurieren des Traffic Rate Limit Identifier im BURSTY-Modus:

```
1 add ns limitIdentifier 100_request_limit -threshold 100 -timeSlice 1000
      -mode REQUEST_RATE -limitType BURSTY -selectorName
     limit_100_requests_selector -trapsInTimeSlice 30
2 <!--NeedCopy-->
```

Konfigurieren der Kennung des Verkehrsratenlimits im SMOOTH-Modus:

```
1 add ns limitidentifier limit_req -mode request_rate -limitType smooth -
     timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
2 <!--NeedCopy-->
```

So konfigurieren Sie eine Traffic-Limit-ID mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu AppExpert > Ratenbegrenzung > Limitkennungen, klicken Sie auf Hinzufügen und geben Sie die entsprechenden Details an.

Konfigurieren und Binden einer Traffic-Ratenrichtlinie

May 11, 2023

Sie implementieren ein ratenbasiertes Anwendungsverhalten, indem Sie eine Richtlinie in einer entsprechenden NetScaler-Funktion konfigurieren. Die Funktion muss erweiterte Richtlinien unterstützen. Der Richtlinienausdruck muss das folgende Ausdruckspräfix enthalten, damit das Feature die Verkehrsrate analysieren kann:


```
sys.check_limit(<limit_identifier>)
<!--NeedCopy-->
```

Wobei limit_identifier der Name eines Grenzwertbezeichners ist.

Der Richtlinienausdruck muss ein zusammengesetzter Ausdruck sein, der mindestens zwei Komponenten enthält:

- Ein Ausdruck, der den Traffic identifiziert, auf den der Ratenbegrenzungsbezeichner angewendet wird. Zum Beispiel:

```
    http.req.url.contains("my_aspx.aspx").
<!--NeedCopy-->
```

- Ein Ausdruck, der einen Ratenbegrenzungsbezeichner identifiziert, z. B. sys.check_limit (“my_limit_identifier”). Dies muss der letzte Ausdruck im politischen Ausdruck sein.

So konfigurieren Sie eine ratenbasierte Richtlinie über die Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine ratenbasierte Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
add cache|dns|rewrite|responder policy <policy_name> -rule expression
    && sys.check_limit("<LimitIdentifierName>") [<feature-specific
    information>]
<!--NeedCopy-->
```

Es folgt ein vollständiges Beispiel für eine ratenbasierte Richtlinienregel. Beachten Sie, dass in diesem Beispiel davon ausgegangen wird, dass Sie die Responder Action send_direct_url konfiguriert haben, die mit der Richtlinie verknüpft ist. Beachten Sie, dass der Parameter sys.check_limit das letzte Element des Richtlinienausdrucks sein muss:

```
add responder policy responder_threshold_policy "http.req.url.contains(
    "myindex.html") && sys.check_limit("my_limit_identifier")"
    send_direct_url
<!--NeedCopy-->
```

Informationen zum globalen Binden einer Richtlinie oder an einen virtuellen Server finden Sie unter Binden erweiterter Richtlinienrichtlinien.

So konfigurieren Sie eine ratenbasierte Richtlinie mit dem Konfigurationsdienstprogramm

1. Erweitern Sie im Navigationsbereich die Funktion, in der Sie eine Richtlinie konfigurieren möchten (z. B. integriertes Caching, Rewrite oder Responder), und klicken Sie dann auf Richtlinien.
2. Klicken Sie im Detailbereich auf "Hinzufügen". Geben Sie unter Name einen eindeutigen Namen für die Richtlinie ein.
3. Geben Sie unter Ausdruck die Richtlinienregel ein und stellen Sie sicher, dass Sie den Parameter sys.check_limit als letzte Komponente des Ausdrucks einschließen. Zum Beispiel:

```
http.req.url.contains("my_aspx.aspx") && sys.check_limit("
    my_limit_identifier")
<!--NeedCopy-->
```

4. Geben Sie funktionsspezifische Informationen zur Richtlinie ein.

   Beispielsweise müssen Sie die Richtlinie möglicherweise einer Aktion oder einem Profil zuordnen. Weitere Informationen finden Sie in der funktionsspezifischen Dokumentation.
5. Klicken Sie auf Erstellenund dann auf Schließen.
6. Klicken Sie auf Speichern.

Traffic Rate anzeigen

January 19, 2021

Wenn der Datenverkehr über einen oder mehrere virtuelle Server einer ratenbasierten Richtlinie entspricht, können Sie die Rate dieses Datenverkehrs anzeigen. Die Kursstatistiken werden in der Limit-ID verwaltet, die Sie in der Regel für die ratenbasierte Richtlinie benannt haben. Wenn mehr als eine Richtlinie denselben Grenzbezeichner verwendet, können Sie die Datenverkehrsrate anzeigen, wie sie durch Treffer für alle Richtlinien definiert ist, die den jeweiligen Grenzbezeichner verwenden.

So zeigen Sie die Datenverkehrsrate mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Datenverkehrsrate anzuzeigen:

```
show ns limitSessions <limitIdentifier>
<!--NeedCopy-->
```


Beispiel:

```
sh limitsession myLimitSession
<!--NeedCopy-->
```

So zeigen Sie die Datenverkehrsrate mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu AppExpert > Ratenbegrenzung > Limit-Kennungen.
2. Wählen Sie einen Grenzbezeichner aus, dessen Verkehrsrate Sie anzeigen möchten.
3. Klicken Sie auf die Schaltfläche Sitzungen anzeigen. Wenn der Datenverkehr über einen oder mehrere virtuelle Server einer Richtlinie zur Begrenzung der Rate entspricht, die diesen Grenzbezeichner verwendet (und die Treffer innerhalb des konfigurierten Zeitabschnitts für diesen Bezeichner liegen), wird das Dialogfeld Sitzungsdetails angezeigt. Andernfalls erhalten Sie eine Meldung Keine Sitzung vorhanden.

Testen einer ratenbasierten Richtlinie

May 11, 2023

Um eine ratenbasierte Richtlinie zu testen, können Sie Datenverkehr an jeden virtuellen Server senden, an den eine ratenbasierte Richtlinie gebunden ist.

Aufgabenübersicht: Testen einer tarifbasierten Politik

1. Konfigurieren Sie einen Stream-Selektor (optional) und eine Ratenbegrenzungskennung (erforderlich). Zum Beispiel:

```
add stream selector sel_subnet Q.URL "CLIENT.IP.SRC.SUBNET(24)"
add ns limitIdentifier k_subnet -Threshold 4 -timeSlice 3600 -mode
     REQUEST_RATE  -limittype smooth  -selectorName sel_subnet  -
    trapsInTimeSlice 8
<!--NeedCopy-->
```

2. Konfigurieren Sie die Aktion, die Sie der Richtlinie zuordnen möchten, die die Ratenbegrenzungs-ID verwendet. Zum Beispiel:

```
add responder action resp_redirect redirect ""http://response_site
    .com/""
<!--NeedCopy-->
```


3. Konfigurieren Sie eine Richtlinie, die das Ausdruckspräfix sys.check_limit verwendet, um den Ratengrenzbezeichner aufzurufen. Die Richtlinie kann beispielsweise wie folgt eine Ratenbegrenzungskennung auf alle Anfragen anwenden, die aus einem bestimmten Subnetz eingehen:

```
add responder policy resp_subnet "SYS.CHECK_LIMIT("k_subnet")"
   resp_redirect
<!--NeedCopy-->
```

4. Binden Sie die Richtlinie global oder an einen virtuellen Server. Zum Beispiel:

```
bind responder global resp_subnet 6 END -type DEFAULT
<!--NeedCopy-->
```

5. Senden Sie in einer Browser-Adressleiste eine Test-HTTP-Anfrage an einen virtuellen Server. Zum Beispiel:

```
http://<IP of a vserver>/testsite/test.txt
<!--NeedCopy-->
```

6. Geben Sie an der NetScaler Eingabeaufforderung Folgendes ein:

```
show ns limitSessions \<limitIdentifier\>
<!--NeedCopy-->
```

Beispiel

```
> sh limitsession k_subnet
1)      Time Remaining:       98 secs  Hits: 2
                            Action Taken: 0
        Total Hash:    1718618  Hash String: /test.txt
        IPs gathered:
                1) 10.217.253.0
        Active Transactions: 0
 Done
>
<!--NeedCopy-->
```

7. Wiederholen Sie die Abfrage, und überprüfen Sie erneut die Statistik der Begrenzungskennung, um zu überprüfen, ob die Statistiken korrekt aktualisiert werden.

Beispiele für tarifbasierte Richtlinien

May 11, 2023

In diesem Thema werden einige Beispiele für tarifbasierte Richtlinien aufgeführt.

Beschränken Sie die Anzahl der Anfragen von einer URL

Führen Sie die folgenden Befehle aus, um die Anzahl der Anfragen pro Sekunde von einer URL zu begrenzen:

```
add stream selector ipStreamSelector http.req.url "client.ip.src" add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeSlice 1000 -mode request_rate -limitType smooth -selectorName ipStreamSelector

add responder action myWebSiteRedirectAction redirect ""http: //www.mycompany .com/""

add responder policy ipLimitResponderPolicy "http.req-url.contains("myasp.asp") && sys.check_limit("ipLimitIdentifier")" myWebSiteRedirectaction

bind responder global ipLimitResponderPolicy 100 END -type default
<!--NeedCopy-->
```

Eine Antwort für die Anforderungs-URL zwischenspeichern

Führen Sie die folgenden Befehle aus, um eine Antwort zwischenzuspeichern, wenn die URL-Rate der Anforderung 5 pro 20000 Millisekunden überschreitet:

```
add stream selector cacheStreamSelector http.req.url add ns limitidentifier cacheRateLimitIdentifier -threshold 5 -timeSlice 2000 -selectorName cacheStreamSelector

add cache policy cacheRateLimitPolicy -rule "http req.method.eq(get) && sys.check_limit "cacheRateLimitIdentifier")" -action cache

bind cache global cacheRateLimitPolicy -priority 10
<!--NeedCopy-->
```

Eine auf Cookies basierende Verbindung beenden

Führen Sie die folgenden Befehle aus, um eine Verbindung auf der Grundlage der in Anfragen eingegangenen Cookies von `www.mycompany.com` zu beenden, falls die Anfragen das Ratenlimit überschreiten:


```
add stream selector reqCookieStreamSelector "http req.cookie «value("
    mycookie")" "client.ip.src.subnet(24)"

add ns limitIdentifier myLimitIdentifier -Threshold 2 -timeSlice 3000 -
    selectorName reqCookieStreamSelector

add responder action sendRedirectUrl redirect '"http://www.mycompany.
    com" + http.req.url' -bypassSafetyCheck YES

add responder policy rateLimitCookiePolicy "http. req.url.contains("www
    .yourcompany.com") && sys check_limit("myLimitIdentifier")"
    sendRedirectUrl
<!--NeedCopy-->
```

Löscht ein DNS-Paket von einer bestimmten IP-Adresse

Führen Sie die folgenden Befehle aus, um ein DNS-Paket zu löschen, wenn die Anfragen von einer bestimmten Client-IP-Adresse und DNS-Domäne das Ratenlimit überschreiten:

```
add stream selector dropDNSStreamSelector client udp.dns.domain client.
    ip.src
add ns limitIdentifier dropDNSRateIdentifier -timeslice 20000 -mode
    request_rate -selectorName dropDNSStreamSelector -maxBandwidth 1 -
    trapsintimeslice 20

add dns policy dnsDropOnClientRatePolicy "sys check_limit ("
    dropDNSRateIdentifier")" -drop yes
<!--NeedCopy-->
```

Beschränken Sie die Anzahl der HTTP-Anfragen von demselben Host

Führen Sie die folgenden Befehle aus, um die Anzahl der HTTP-Anfragen zu begrenzen, die von demselben Host mit einer Subnetzmaske von 32 eingehen und dieselbe Ziel-IP-Adresse haben:

```
add stream selector ipv6_sel "CLIENT.IPv6.src.subne (32)" CLIENT.IPv6.
    dst Q.URL
add ns limitIdentifier ipvé_id -imeSlice 20000 -selectorName ipvé_sel
add lb vserver ipv6é_vip HTTP 3ffe::209 80 -persistenceType NONE -
    cltTimeout 180
add responder action redirect_page redirect ""http://redirectpage.com
    /""
```



```
add responder policy ipvé_resp_pol "SYS.CHECK_LIMIT("ipv6_id")"
    redirect_page
bind responder global ipv6_resp_pol 5 END -type DEFAULT
<!--NeedCopy-->
```

Beispiele für Anwendungsfälle für ratenbasierte Richtlinien

May 11, 2023

In den folgenden Szenarien werden zwei Anwendungen ratenbasierter Richtlinien im globalen Serverlastenausgleich (GSLB) beschrieben:

- Das erste Szenario beschreibt die Verwendung einer ratenbasierten Richtlinie, die Datenverkehr an ein neues Rechenzentrum sendet, wenn die Rate der DNS-Anfragen 1000 pro Sekunde übersteigt.
- Wenn im zweiten Szenario innerhalb eines bestimmten Zeitraums mehr als fünf DNS-Anfragen für einen lokalen DNS-Client (LDNS) eingehen, werden die zusätzlichen Anfragen verworfen.

Umleitung des Verkehrs auf der Grundlage der Verkehrsrate

In diesem Szenario konfigurieren Sie eine auf der Nähe basierende Load-Balancing-Methode und eine Richtlinie zur Geschwindigkeitsbegrenzung, die DNS-Anfragen für eine bestimmte Region identifiziert. In der Richtlinie zur Geschwindigkeitsbegrenzung geben Sie einen Schwellenwert von 1000 DNS-Anfragen pro Sekunde an. Eine DNS-Richtlinie wendet die Richtlinie zur Ratenbegrenzung auf DNS-Anfragen für die Region „Europe.GB.17.London.UK-East.ISP-UK“ an. „ Gemäß der DNS-Richtlinie müssen DNS-Anfragen, die den Schwellenwert für die Ratenbegrenzung überschreiten, beginnend mit der Anforderung 1001 und bis zum Ende des Ein-Sekunden-Intervalls, an die IP-Adressen weitergeleitet werden, die der Region „North America.US.TX.Dallas.US-East.ISP-US“ zugeordnet sind. ”

Die folgende Konfiguration veranschaulicht dieses Szenario:

```
add stream selector DNSSelector1 client.udp.dns.domain

add ns limitIdentifier DNSLimitIdentifier1 -threshold 5 -timeSlice 1000
     -selectorName DNSSelector1

add dns policy DNSLimitPolicy1 "client.ip.src.matches_location("Europe.
    GB.17.London.\*.\*") &&
sys.check_limit("DNSLimitIdentifier1")" -preferredLocation "North
    America.US.TX.Dallas.\*.\*"
```



```
7
8 bind dns global DNSLimitPolicy1 5
9 <!--NeedCopy-->
```

Löschen von DNS-Anfragen auf der Grundlage der Verkehrsrate

Im folgenden Beispiel für den globalen Serverlastenausgleich konfigurieren Sie eine Richtlinie zur Geschwindigkeitsbegrenzung, die es zulässt, dass maximal fünf DNS-Anfragen in einem bestimmten Intervall pro Domain zur Lösung an einen LDNS-Client weitergeleitet werden. Alle Anfragen, die diese Rate überschreiten, werden verworfen. Diese Art von Richtlinie kann dazu beitragen, den NetScaler vor der Ausbeutung von Ressourcen zu schützen. Wenn in diesem Szenario beispielsweise die Time to Live (TTL) für eine Verbindung fünf Sekunden beträgt, verhindert diese Richtlinie, dass das LDNS eine Domain anfordert. Stattdessen werden Daten verwendet, die auf dem NetScaler zwischengespeichert werden.

```
1  add stream selector LDNSSelector1 client.udp.dns.domain client.ip.src
2
3  add ns limitIdentifier LDNSLimitIdentifier1 -threshold 5 -timeSlice
       1000 -selectorName LDNSSelector1
4
5  add dns policy LDNSPolicy1 "client.udp.dns.domain.contains(".") && sys.
       check_limit("LDNSLimitIdentifier1")" -drop YES
6
7  bind dns global LDNSPolicy1 6
8
9  show gslb vserver gvip
10
11 gvip - HTTP     State: UP
12 Last state change was at Mon Sep  8 11:50:48 2008 (+711 ms)
13 Time since last state change: 1 days, 02:55:08.830
14 Configured Method: STATICPROXIMITY
15 BackupMethod: ROUNDROBIN
16 No. of Bound Services :  3 (Total)       3 (Active)
17 Persistence: NONE       Persistence ID: 100
18 Disable Primary Vserver on Down: DISABLED       Site Persistence: NONE
19 Backup Session Timeout: 0
20 Empty Down Response: DISABLED
21 Multi IP Response: DISABLED Dynamic Weights: DISABLED
22 Cname Flag: DISABLED
23 Effective State Considered: NONE
24 1.     site11_svc(10.100.00.00: 80)- HTTP State: UP    Weight: 1
25 Dynamic Weight: 0       Cumulative Weight: 1
26 Effective State: UP
```



```
Threshold : BELOW
Location: Europe.GB.17.London.UK-East.ISP-UK
2.      site12_svc(10.101.00.100: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.TX.Dallas.US-East.ISP-US
3.      site13_svc(10.102.00.200: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.NJ.Salem.US-Mid.ISP-US
4.      www.gslbindia.com        TTL: 5 secn
Cookie Timeout: 0 min   Site domain TTL: 3600 sec
Done
<!--NeedCopy-->
```

Ratenbegrenzung für Verkehrsdomänen

May 11, 2023

Sie können die Ratenbegrenzung für Traffic-Domains konfigurieren. Der folgende Ausdruck in der NetScaler-Ausdruckssprache für identifiziert den Datenverkehr, der mit Verkehrsdomänen verknüpft ist.

- client.traffic_domain.id

Sie können die Ratenbegrenzung für den Datenverkehr konfigurieren, der einer bestimmten Verkehrsdomäne, einer Reihe von Verkehrsdomänen oder allen Verkehrsdomänen zugeordnet ist.

Um die Ratenbegrenzung für Datenverkehrsdomänen zu konfigurieren, führen Sie die folgenden Schritte auf einer NetScaler-Appliance aus, indem Sie das Konfigurationsprogramm oder die NetScaler-Befehlszeile verwenden:

1. Konfigurieren Sie einen Stream-Selektor, der den Ausdruck client.traffic_domain.id verwendet, um den Datenverkehr zu identifizieren, der den Traffic-Domains zugeordnet ist und der ratenbegrenzt werden soll.
2. Konfigurieren Sie eine Ratenbegrenzungskennung, die Parameter wie den maximalen Schwellenwert für den zu begrenzenden Verkehr angibt. In diesem Schritt ordnen Sie dem Ratenbegrenzer auch einen Stream-Selector zu.
3. Konfigurieren Sie eine Aktion, die Sie der Richtlinie zuordnen möchten, die die Ratenbegrenzungs-ID verwendet.

4. Konfigurieren Sie eine Richtlinie, die das Ausdruckspräfix sys.check_limit verwendet, um den Ratengrenzbezeichner aufzurufen, und ordnen Sie die Aktion dieser Richtlinie zu.
5. Binden Sie die Richtlinie global.

Stellen Sie sich ein Beispiel vor, in dem zwei Verkehrsdomänen mit den IDs 10 und 20 auf NetScaler NS1 konfiguriert sind. In der Verkehrsdomäne 10 ist LB1-TD-1 für den Lastenausgleich der Server S1 und S2 konfiguriert; LB2-TD1 ist für den Lastenausgleich der Server S3 und S4 konfiguriert.

In der Verkehrsdomäne 20 ist LB1-TD-2 für den Lastenausgleich der Server S5 und S6 konfiguriert; LB2-TD2 ist für den Lastenausgleich der Server S7 und S8 konfiguriert.

In der folgenden Tabelle sind einige Beispiele für Richtlinien zur Ratenbegrenzung für Verkehrsdomänen im Beispiel-Setup aufgeführt.

Zweck	CLI-Befehle
Beschränken Sie die Anzahl der Anfragen auf 10 pro Sekunde für jede der Verkehrsdomänen.	Stream-Selektor hinzufügen tdratelimit-1 CLIENT.TRAFFIC_DOMAIN.ID füge ns LimitIdentifier limitIdf-1 -threshold 10 -SelectorName tdratelimit-1 -trapsInTimeSlice 0 füge die Responderrichtlinie hinzu ratelimit-pol „sys.check_limit (\" limitidf-1\")“ DROP bind responder global ratelimit-pol 1
Beschränken Sie die Anzahl der Anfragen auf 5 pro Client pro Sekunde für jede der Verkehrsdomänen.	füge den Stream-Selektor hinzu tdandclientip CLIENT.IP.SRC, CLIENT.TRAFFIC_DOMAIN.ID füge ns LimitIdentifier hinzu td_limitidf -threshold 5 -SelectorName tdandclientip -trapsInTimeSlice 5 füge die Responderrichtlinie hinzu tdratelimit-pol „sys.check_limit (\" td_limitidf\")“ DROP bind Responder global tdratelimit-pol 2
Beschränken Sie die Anzahl der Anfragen, die für eine bestimmte Verkehrsdomäne (z. B. Verkehrsdomäne 10) gesendet werden, auf 30 Anfragen alle 3 Sekunden.	Stream-Selektor hinzufügen tratelimit CLIENT.TRAFFIC_DOMAIN.ID füge ns LimitIdentifier hinzu td10_limitidf -threshold 30 -TimeSlice 3000 -SelectorName tratelimit -trapsInTimeSlice 5 füge Responder-Richtlinie hinzu td10ratelimit „client.traffic_domain.id==10 && sys.check_limit (\" td10_limitidf\")“ DROP bind responder globales td10-Ratenlimit 3

Zweck	CLI-Befehle
Beschränken Sie die Anzahl der Verbindungen auf 5 pro Client pro Sekunde für eine bestimmte Verkehrsdomäne (z. B. Verkehrsdomäne 20).	füge den Stream-Selektor hinzu tdandclientip CLIENT.IP.SRC CLIENT.TRAFFIC_DOMAIN.ID füge ns LimitIdentifier hinzu td20_limitidf -threshold 5 -mode CONNECTION -SelectorName tdandclientip -trapsIntimeSlice 5 füge die Responder-Richtlinie hinzu td20_ratelimit „client.traffic_domain.id==20 && sys.check_limit (\" td20_limitidf\")“ DROP bindet den Responder global td20_ratelimit 4

Konfigurieren des Zinslimits auf Paketebene

January 25, 2022

Sie können einen Stream-Selektor und eine Responder Policy konfigurieren, um Statistiken auf Paketebene zu sammeln, die durch alle vom Selektor identifizierten Verbindungen fließen. Wenn die Anzahl der Pakete pro Sekunde den konfigurierten Schwellenwert überschreitet, wendet die Richtlinie die konfigurierte Aktion an (RESET oder DROP). Sie können diese Richtlinien für alle Arten von virtuellen Servern konfigurieren. Pakete aller Größen werden berücksichtigt.

Führen Sie zum Konfigurieren der Ratenbegrenzung auf Paketebene die folgenden Aufgaben aus

1. Lastenausgleich aktivieren
2. Stream-Selektor hinzufügen
3. Stream-ID hinzufügen
4. Responder-Richtlinie hinzufügen
5. Virtuellen Lastausgleichsserver hinzufügen
6. Responder Policy binden

So aktivieren Sie die Lastausgleich-Funktion

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature lb
<!--NeedCopy-->
```


Einen Stream-Selektor hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add stream selector packetlimitselector client.ip.src client.tcp.
     srcport client.ip.dst client.tcp.dstport
2 <!--NeedCopy-->
```

So fügen Sie eine Stream-ID hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add stream identifier packetlimitidentifier packetlimitselector -
     interval 1
2 <!--NeedCopy-->
```

Um die Verfolgung von Nur-ACK-Paketen zu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set stream identifier packetlimitidentifier  - trackAckOnlyPackets
     ENABLED
2 <!--NeedCopy-->
```

So fügen Sie eine Responder Policy hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
     packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", <
     max_threshold_PPS>, ACTION, 0/1)" NOOP
2 <!--NeedCopy-->
```

Hierbei gilt:

- <max_threshold_PPS>ist die maximale Anzahl von Paketen, die über die Verbindung pro Sekunde zulässig sind.
- ACTION kann DROP oder RESET sein.
- 0 oder 1 steht für den Limittyp; 0 steht für den Grenzwerttyp BURSTY und 1 für den Grenzwerttyp SMOOTH.

Beispiel:


```
add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
    packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", 40, RESET, 0)"
     NOOP
<!--NeedCopy-->
```

So fügen Sie einen virtuellen Lastausgleichsserver hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-lb-1 HTTP 10.102.20.200 80
<!--NeedCopy-->
```

So binden Sie eine Responder Policy

Nachdem der Selektor und die Responder Policy konfiguriert wurden, kann die Richtlinie global oder an den spezifischen virtuellen Server gebunden werden.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
bind responder global <policyName> <priority> [<gotoPriorityExpression
    >] [-type <type>] [-invoke  (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

ODER

```
bind lb vserver <name>@  (-policyName <string>@ [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Beispiele:

```
bind responder global packet_rate_sessionpolicy 101 END -type
    REQ_DEFAULT

bind responder global packet_rate_sessionpolicy 102 END -type

bind lb vserver v1 -policyname packet_rate_sessionpolicy -priority 10
<!--NeedCopy-->
```


Responder

May 11, 2023

> **Warnung**
>
> Filterfunktionen, die klassische Richtlinien verwenden, sind veraltet und als Alternative empfiehlt Citrix Ihnen, die Rewrite- und Responder-Funktionen mit erweiterter Richtlinieninfrastruktur zu verwenden.

Die heutigen komplexen Webkonfigurationen erfordern oft unterschiedliche Antworten auf HTTP-Anfragen, die oberflächlich betrachtet ähnlich erscheinen. Wenn Benutzer eine Webseite aufrufen, möchten Sie möglicherweise je nach geografischem Standort des Benutzers, Browserspezifikation oder Sprachen, die der Browser akzeptiert, und der Reihenfolge der Präferenzen eine andere Seite bereitstellen. Möglicherweise möchten Sie die Verbindung unterbrechen, wenn die Anfrage aus einem IP-Bereich kommt, der DDoS-Angriffe ausgelöst oder Hacking-Versuche initiiert hat.

Responder unterstützt Protokolle wie TCP, DNS (UDP) und HTTP. Wenn der Responder auf Ihrer Appliance aktiviert ist, können Serverantworten darauf basieren, wer die Anfrage sendet, von wo sie gesendet wird, sowie auf anderen Kriterien mit Auswirkungen auf Sicherheit und Systemverwaltung. Die Funktion ist einfach und schnell zu verwenden. Durch die Vermeidung des Aufrufs komplexerer Funktionen werden die CPU-Zyklen und der Zeitaufwand für die Bearbeitung von Anfragen reduziert, die keine komplexe Verarbeitung erfordern.

Wenn Sie beim Umgang mit vertraulichen Daten wie Finanzinformationen sicherstellen möchten, dass der Kunde eine sichere Verbindung verwendet, um auf einer Website zu surfen, können Sie die Anfrage an eine sichere Verbindung umleiten, indem Sie `https://` anstelle von `http://`

Gehen Sie wie folgt vor, um einen Responder zu verwenden:

- Aktivieren Sie eine Responder-Funktion auf der Appliance.
- Konfigurieren Sie eine Responder-Aktion. Die Aktion kann darin bestehen, eine benutzerdefinierte Antwort zu generieren, eine Anfrage an eine andere Webseite umzuleiten oder eine Verbindung zurückzusetzen.
- Konfigurieren Sie eine Responder-Richtlinie. Die Richtlinie bestimmt die Anfragen (Traffic), bei denen eine Maßnahme ergriffen werden muss.
- Binden Sie jede Richtlinie an einen Bindungspunkt, um sie in Kraft zu setzen. Ein Bindungspunkt bezieht sich auf eine Entität, an der die NetScaler-Appliance den Datenverkehr untersucht, um festzustellen, ob er mit einer Richtlinie übereinstimmt. Ein Bindpunkt kann beispielsweise ein virtueller Lastausgleichsserver sein.

Sie können eine Standardaktion für Anfragen angeben, die keiner Richtlinie entsprechen, und Sie können die Sicherheitsüberprüfung bei Aktionen Bypass, die andernfalls zu Fehlermeldungen führen würden.

Die Rewrite-Funktion von NetScaler hilft dabei, einige Informationen in den von NetScaler verarbeiteten Anfragen oder Antworten umzuschreiben. Der folgende Abschnitt zeigt einige Unterschiede zwischen den beiden Funktionen.

Vergleich zwischen Rewrite und Responder Optionen

Der Hauptunterschied zwischen der Rewrite-Funktion und der Responder-Funktion ist wie folgt:

Responder kann nicht für Antwort- oder serverbasierte Ausdrücke verwendet werden. Der Responder kann je nach Clientparametern nur für die folgenden Szenarien verwendet werden:

- Umleiten einer HTTP-Anfrage auf neue Websites oder Webseiten
- Reagieren mit einer benutzerdefinierten Antwort
- Löschen oder Zurücksetzen einer Verbindung auf Anforderungsebene

Wenn es eine Responder Policy gibt, prüft NetScaler die Anfrage des Clients, ergreift Maßnahmen gemäß den geltenden Richtlinien, sendet die Antwort an den Client und schließt die Verbindung mit dem Client.

Wenn es eine Rewriterichtlinie gibt, prüft NetScaler die Anforderung des Clients oder die Antwort vom Server, ergreift Maßnahmen gemäß den geltenden Richtlinien und leitet den Datenverkehr an den Client oder den Server weiter.

Im Allgemeinen wird empfohlen, einen Responder zu verwenden, wenn die Appliance eine Verbindung basierend auf einem anforderungsbasierten Parameter zurücksetzen oder beenden soll. Verwenden Sie einen Responder, um den Traffic umzuleiten, oder antworten Sie mit benutzerdefinierten Nachrichten. Verwenden Sie Rewrite zum Bearbeiten von Daten auf HTTP-Anforderungen und -Antworten.

Aktivieren der Responder-Funktion

May 11, 2023

Um die Responder-Funktion verwenden zu können, müssen Sie sie zuerst aktivieren.

So aktivieren Sie die Responder-Funktion mithilfe der NetScaler CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Responder-Funktion zu aktivieren und die Konfiguration zu überprüfen:

- `enable ns feature <feature>`
- `show ns feature`

Beispiel:


```
enable ns feature Responder
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 .
 .
 .
 19)     Responder                       RESPONDER           ON
 20)     NetScaler Push                  push                OFF
 Done
>
<!--NeedCopy-->
```

So aktivieren Sie die Responder-Funktion über die GUI:

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter **Modi** und **Funktionen** auf **Erweiterte Funktionen ändern**.
3. Aktivieren Sie im Dialogfeld **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **Responder**, und klicken Sie dann auf **OK**.
4. In den **Funktion(en) aktivieren/deaktivieren?** klicken Sie auf **JA**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert wurde.

Konfigurieren der Responder Action

June 2, 2023

Nachdem Sie die Responder-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen für die Bearbeitung von Anfragen konfigurieren. Der Responder unterstützt die folgenden Arten von Aktionen:

- **Antworte mit**. Sendet die durch den Target-Ausdruck definierte Antwort, ohne die Anforderung an einen Webserver weiterzuleiten. (Die NetScaler-Appliance ersetzt und fungiert als Webserver.) Verwenden Sie diese Art von Aktion, um eine einfache HTML-basierte Antwort manuell zu definieren. Normalerweise besteht der Text für eine Aktion “Antworten mit” aus einem Webserver-Fehlercode und einer kurzen HTML-Seite.
- **Antworten Sie mit SQL OK**. Sendet die angegebene SQL OK-Antwort, die durch den Target-Ausdruck definiert ist. Verwenden Sie diese Art von Aktion, um eine SQL-OK-Antwort auf eine

SQL-Abfrage zu senden.

- **Antworten Sie mit SQL-Fehler**. Sendet die angegebene SQL-Fehler-Antwort, die durch den Target-Ausdruck definiert ist Verwenden Sie diese Art von Aktion, um eine SQL-Fehlerantwort auf eine SQL-Abfrage zu senden.
- **Antworten Sie mit der HTML-Seite**. Sendet die angegebene HTML-Seite als Antwort. Sie können aus einer Dropdownliste von HTML-Seiten wählen, die zuvor hochgeladen wurden, oder eine neue HTML-Seite hochladen. Verwenden Sie diese Art von Aktion, um eine importierte HTML-Seite als Antwort zu senden. Die Appliance antwortet mit einem benutzerdefinierten Header in der Responsewithhtmlpage-Responder-Aktion. Sie können bis zu acht benutzerdefinierte Header konfigurieren. Die importierte HTML-Seite wird im Verzeichnis `/var/download/responder` gespeichert.
- **Umleitung**. Leitet die Anfrage an eine andere Webseite oder einen anderen Webserver um. Eine Umleitungsaktion kann Anfragen, die ursprünglich an eine “Dummy” -Website gesendet wurden, die in DNS existiert, für die es jedoch keinen tatsächlichen Webserver gibt, an eine tatsächliche Website umleiten. Es kann auch Suchanfragen an eine entsprechende URL umleiten. Normalerweise besteht das Umleitungsziel für eine Umleitungsaktion aus einer vollständigen URL.

Konfigurieren Sie eine Responder-Aktion mithilfe der CLI:

Zeigt die aktuellen Einstellungen für die angegebene Responder Action an. Wenn kein Aktionsname angegeben wird, zeigen Sie eine Liste aller derzeit auf der NetScaler-Appliance konfigurierten Responderaktionen mit abgekürzten Einstellungen an.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Responder Action zu konfigurieren und die Konfiguration zu überprüfen:

- `add responder action <name> <type> <target>`
- `show responder action`

Parameter:

- **Name**. Name der Responder Action. Maximale Länge: 127
- **Typ**. Art der Responder Action. Es kann sein: (respondwith).
- **target**. Ein Ausdruck, der angibt, womit geantwortet werden soll.
- **htmlpage**. Option, die angibt, mit einer HTML-Seite zu antworten.
- **hits**. Die Häufigkeit, mit der die Maßnahme ergriffen wurde.
- **referenceCount**. Die Anzahl der Verweise auf die Aktion.
- **undefHits**. Die Häufigkeit, mit der die Aktion zu UNDEF geführt hat.
- **comment**. Jede Art von Informationen über diese Responder Action.

- **builtin**. Markierung, um festzustellen, ob die Responder-Aktion integriert ist oder nicht.

Beispiel:

```
Create a responder action that displays a “Not Found” error page for URLs that do not exist:

> add responder action act404Error respondWith '"HTTP/1.1 404 Not Found\r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."'
Done

> show responder action

1) Name: act404Error
Operation: respondwith
Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

Create a responder action that displays a “Not Found” error page for URLs that do not exist:

add responder action act404Error respondWith '"HTTP/1.1 404 Not Found\r\n\r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."'
Done
> show responder action

1) Name: act404Error
Operation: respondwith
Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web server."
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Ändern Sie eine vorhandene Responder-Aktion mithilfe der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine vorhandene Responder

Action zu ändern und die Konfiguration zu überprüfen:

- `set responder action <name> -target <string>`
- `show responder action`

Beispiel:

```
set responder action act404Error  -target '"HTTP/1.1 404 Not Found\r\n\
    r\n"+ HTTP.REQ.URL.HTTP_URL_SAFE + " does not exist on the web
    server."'
 Done
> show responder action

1)      Name: act404Error
        Operation: respondwith
        Target: "HTTP/1.1 404 Not Found" + HTTP.REQ.URL.HTTP_URL_SAFE +
            " does not exist on the web server."
        Hits: 0
        Undef Hits: 0
        Action Reference Count: 0
 Done

<!--NeedCopy-->
```

Entfernen Sie eine Responder-Aktion mithilfe der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Responder Action zu entfernen und die Konfiguration zu überprüfen:

- `rm responder action <name>`
- `show responder action`

Beispiel:

```
rm responder action act404Error
 Done

> show responder action
 Done

<!--NeedCopy-->
```

Fügen Sie mithilfe der CLI benutzerdefinierte Header als Antwort mit der Responder-Aktion responsewithhtmlpage hinzu:

Eine NetScaler Appliance kann jetzt mit benutzerdefinierten Headern in der Responsewithhtmlpage-Responder-Aktion antworten. Sie können bis zu acht benutzerdefinierte Header konfigurieren. Zuvor

reagierte die Appliance nur mit den statischen Headern `Content-type:text/html` und `Content-Length:<value>`.

> **Hinweis:**
>
> In der benutzerdefinierten Header-Konfiguration können Sie auch den Header-Wert “Content-Type” überschreiben.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <expression>] [-headers <name(value)> ...]
```

Hierbei gilt:

Name: Name für die Responder-Aktion. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Hash (#), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann geändert werden, nachdem die Responder Policy hinzugefügt wurde.

Typ: Art der Responder-Aktion. Verfügbare Einstellungen funktionieren wie folgt:

1. **respondwith <target>** - Beantworten Sie die Anfrage mit dem als Ziel angegebenen Ausdruck.
2. **respondwithhtmlpage** — Beantworten Sie die Anfrage mit dem hochgeladenen HTML-Seitenobjekt, das als Ziel angegeben ist.
3. **redirect** — Leitet die Anfrage an die als Ziel angegebene URL weiter.
4. **sqlresponse_ok** - Sendet eine SQL OK-Antwort.
5. **sqlresponse_error** — Sendet eine SQL-FEHLER-Antwort. Dies ist ein zwingendes Argument. Mögliche Werte: `noop`, `respondwith`, `redirect`, `respondwithhtmlpage`, `sqlresponse_ok`, `sqlresponse_error`

Ziel: Ausdruck, der angibt, womit geantwortet werden soll. Typischerweise eine URL für Umleitungsrichtlinien oder ein Standardsyntaxausdruck. Zusätzlich zu den Standardsyntaxausdrücken von NetScaler, die auf Informationen in der Anfrage verweisen, kann ein String Builder-Ausdruck Text und HTML sowie einfache Escape-Codes enthalten, die neue Zeilen und Absätze definieren. Setzen Sie jedes String Builder-Ausdruckselement (entweder einen NetScaler-Standardsyntaxausdruck oder eine Zeichenfolge) in doppelte Anführungszeichen. Verwenden Sie das Pluszeichen (+), um die Elemente zu verbinden.

htmlpage: Für `respondwithhtmlpage`-Richtlinien der Name des HTML-Seitenobjekts, das als Antwort verwendet werden soll. Sie müssen zuerst das Seitenobjekt importieren. Maximale Länge: 31

Kommentar: Jegliche Art von Informationen zu dieser Responder-Aktion. Maximale Länge: 255

responseStatusCode: HTTP-Antwortstatuscode, zum Beispiel 200, 302, 404 usw. Der

Standardwert für den Typ `redirect action` ist 302 und für `respondwithhtmlpage` ist 200 Mindestwert: 100 Maximalwert: 599

ReasonPhrase: Ausdruck, der die Grundphrase der HTTP-Antwort angibt. Die Grundphrase kann ein Zeichenfolgenliteral mit Anführungszeichen oder ein PI-Ausdruck sein. Beispiel: `"Invalid URL: " + HTTP.REQ.URL Maximum Length: 8191`

Header: Ein oder mehrere Header, die in die HTTP-Antwort eingefügt werden sollen. Jeder Header wird als `"name(expr),"` angegeben, wobei expr ein Ausdruck ist, der zur Laufzeit ausgewertet wird, um den Wert für den benannten Header bereitzustellen. Sie können maximal acht Header für eine Responder Action konfigurieren.

Konfigurieren Sie eine Responder-Aktion mithilfe der GUI:

1. Navigieren Sie zu **AppExpert > Responder > Actions**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine bestehende Aktion zu ändern, wählen Sie die Aktion aus und klicken dann auf **Öffnen**.
3. Klicken Sie auf **Erstellen** oder **OK**, je nachdem, ob Sie eine Aktion erstellen oder eine vorhandene Aktion ändern.
4. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert wurde.
5. Um eine Responder Action zu löschen, wählen Sie die Aktion aus und klicken dann auf **Entfernen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Funktion deaktiviert wurde.

Hinzufügen eines Ausdrucks mithilfe des Dialogfelds **Ausdruck hinzufügen**

1. Klicken Sie im Dialogfeld **Responder-Aktion erstellen** oder **Responder-Aktion konfigurieren** auf **Hinzufügen**.
2. Wählen Sie im Dialogfeld **Ausdruck hinzufügen** im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.
   - HTTP. Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
   - SYS. Eine oder mehrere geschützte Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - CLIENT. Der Computer, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - ANALYTICS. Die mit der Anfrage verbundenen Analysedaten. Wählen Sie diese Option, wenn Sie Anforderungsmetadaten untersuchen möchten.
   - SIP. Eine SIP-Anfrage. Wählen Sie diese Option, wenn Sie einen Aspekt einer SIP-Anfrage untersuchen möchten. Wenn Sie Ihre Auswahl treffen, werden im Listenfeld ganz rechts

die entsprechenden Begriffe für den nächsten Teil Ihres Ausdrucks aufgeführt.

3. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahl hängt davon ab, welche Wahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, wird im Hilfefenster unterhalb des Fensters "Ausdruck konstruieren" (das leer war) eine Hilfe zur Beschreibung des Zwecks und der Verwendung des gerade gewählten Begriffs angezeigt.
4. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.

Konfigurieren der globalen HTTP-Aktion

Sie können die globale HTTP-Aktion so konfigurieren, dass eine Responder Action aufgerufen wird, wenn eine HTTP-Anforderung ein Timeout hat. Um diese Funktion zu konfigurieren, müssen Sie zuerst die Responder Action erstellen, die Sie aufrufen möchten. Konfigurieren Sie dann die globale HTTP-Timeout-Aktion, um auf ein Timeout mit dieser Responder-Aktion zu reagieren.

Konfigurieren Sie die globale HTTP-Aktion mithilfe der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

- `set ns httpProfile -reqTimeoutAction <responder action name>`
- `save ns config`

Ersetzen Sie durch den Namen der Responder-Aktion. `<responder action name>`

Einen HTML-Seitenimport konfigurieren

Wenn eine NetScaler Appliance mit einer benutzerdefinierten Nachricht antwortet, können wir mit einer HTML-Datei antworten. Sie können die Datei mit dem Befehl "**`import`** `responder htmlpage`" importieren und diese Datei dann im Befehl `add responder action <act name> respondwithhtmlpage <file name>` verwenden. Sie können die Datei auch über die NetScaler GUI importieren. Sie können eine gewünschte HTML-Seite in den Appliance-Ordner importieren und die Seite während der Laufzeit des Responder hochladen.

Importieren Sie eine HTML-Seite mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
import responder htmlpage [<src>] <name> [-comment <string>] [-overwrite][-CAcertFile <string>]
```

Beispiel:


```
import responder htmlpage http://www.example.com/page.html my-responder-
page -CAcertFile my_root_ca_cert
```

Wo,
Ein CA-Zertifikat wird zur Überprüfung des Client-Zertifikats verwendet. Das Zertifikat muss mit dem CLI-Befehl "**import** ssl certfile" oder einem gleichwertigen Befehl über eine API oder GUI importiert werden. Wenn kein Zertifikatsname konfiguriert ist, werden standardmäßige Root-CA-Zertifikate für die Zertifikatsüberprüfung verwendet.

Importieren einer HTML-Seite aus dem lokalen Dateisystem

Sie können auch eine HTML-Seite aus dem lokalen Dateisystem importieren. Um zu importieren, kopieren Sie die Datei mit SCP oder auf andere Weise in das Verzeichnis /var/tmp/ und importieren Sie sie dann mit dem Schlüsselwort "local:". Beispiel:

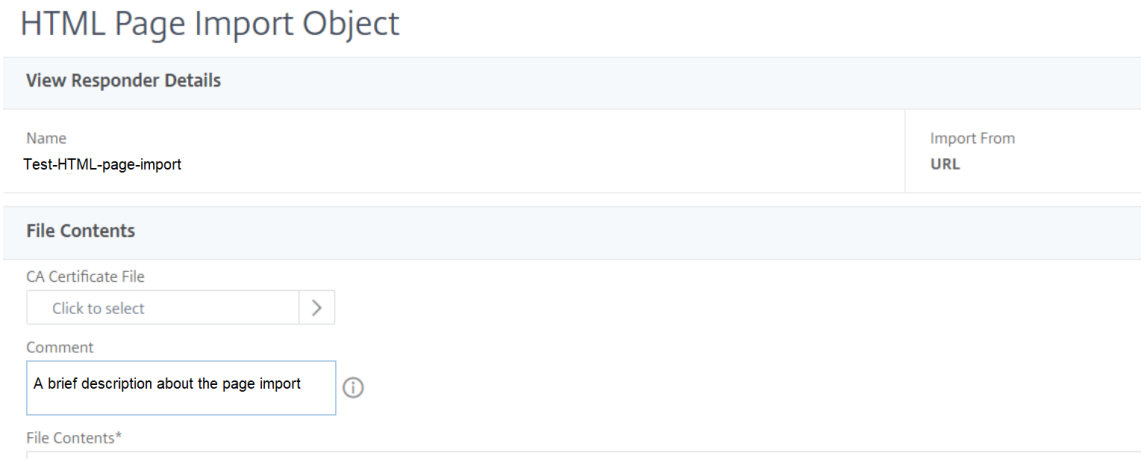
```
import responder htmlpage local:my_local_file.html my_local_file
```

Wobei `my_local_file.html` im Verzeichnis "/var/tmp/" ist.

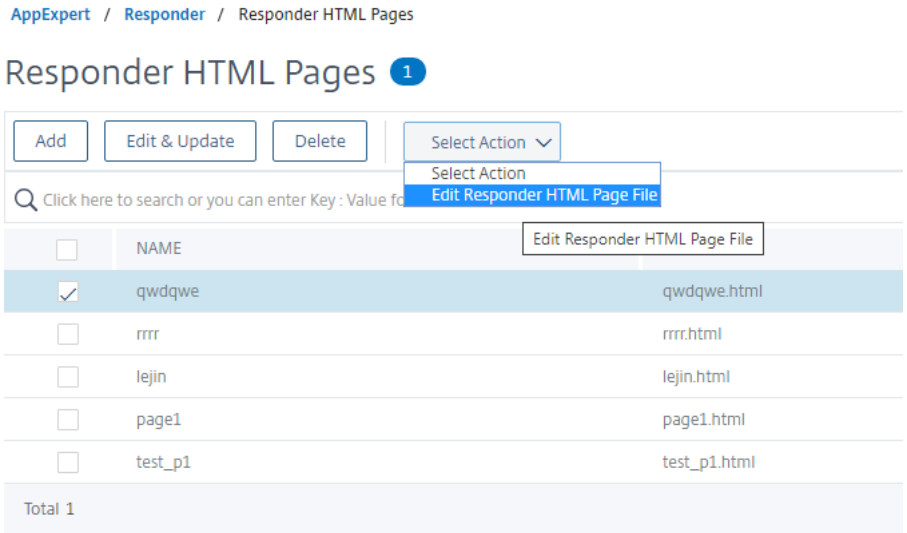
> **Beachten Sie**
>
> , dass das Schlüsselwort "local:" nur die Datei im Verzeichnis "/var/tmp/" durchsucht. Bei nicht standardmäßigen Partitionen müssen Sie die Datei in das partitionsspezifische tmp-Verzeichnis kopieren, das sich in `/var/partitions/<partition name>/tmp` befindet.

Importieren Sie eine HTML-Seite mithilfe der GUI

1. Navigieren Sie zu **AppExpert** > **Responder** > **HTML-Seiten-Importe**.
2. Klicken Sie im Detailbereich **Responder HTML Imports** auf **Hinzufügen**.
3. Legen Sie auf der **Seite "Objekt importieren" von HTML-Seiten** die folgenden Parameter fest:
    a) Name. Name der HTML-Seite.
    b) Importieren von. Importiert aus Datei, Text oder Text.
    c) URL. Wählen Sie aus, um den URL-Speicherort der HTML-Datei einzugeben.
    d) Datei. Wählen Sie die HTML-Datei aus dem Appliance-Verzeichnis aus.
    e) Text. Markieren Sie die HTML-Datei als Text.
4. Klicken Sie auf **Weiter**.
5. Überprüfen Sie die HTML-Seite des Responder.
6. Klicken Sie auf **Fertig**.



Um eine HTML-Seite zu bearbeiten, können Sie eine Datei auswählen und in der Dropdownliste **Aktion auswählen** auf **Responder-HTML-Seitendatei bearbeiten** klicken.



Konfigurieren einer Responder Policy

September 1, 2023

Nachdem Sie eine Responder Action konfiguriert haben, müssen Sie als Nächstes eine Responder Policy konfigurieren, um die Anforderungen auszuwählen, auf die die NetScaler-Appliance antworten soll. Eine Responder Policy basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Regel ist mit einer Aktion verknüpft, die ausgeführt wird, wenn eine Anforderung der Regel entspricht.

Hinweis: Zum Erstellen und Verwalten von Responder-Richtlinien bietet die GUI Unterstützung, die an der NetScaler-Eingabeaufforderung nicht verfügbar ist.

So konfigurieren Sie eine Responder Policy mithilfe der NetScaler-Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction <actionName>`
- `show responder policy <name>`

Beispiel:

```
> add responder policy policyThree "CLIENT.IP.SRC.IN_SUBNET
   (222.222.0.0/16)" RESET
 Done
> show responder policy policyThree

        Name: policyThree
        Rule: CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
        Responder Action: RESET
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0
 Done
<!--NeedCopy-->
```

So ändern Sie eine vorhandene Responder Policy mithilfe der NetScaler-Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>]`
- `show responder policy <name>`

So entfernen Sie eine Responder Policy mithilfe der NetScaler-Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `rm responder policy <name>`
- `show responder policy`

Beispiel:

```
>rm responder policy pol404Error
 Done

> show responder policy
 Done
<!--NeedCopy-->
```


So konfigurieren Sie eine Responder Policy über die GUI:

1. Navigieren Sie zu **AppExpert > Responder > Richtlinien**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie auf **Erstellen** oder **OK**, je nachdem, ob Sie eine Richtlinie erstellen oder eine bestehende Richtlinie ändern möchten.
4. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature konfiguriert wurde.

Binden einer Responder-Richtlinie

May 11, 2023

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie entweder global binden, sodass sie für den gesamten Datenverkehr gilt, der durch den NetScaler fließt, oder für einen bestimmten virtuellen Server, sodass die Richtlinie nur für Anforderungen gilt, deren Ziel-IP-Adresse der VIP dieses virtuellen Servers ist.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf jede positive Ganzzahl festlegen.

Im NetScaler-Betriebssystem funktionieren die Richtlinienprioritäten in umgekehrter Reihenfolge — je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit Prioritäten von 10, 100 und 1000 haben, wird der Richtlinie zuerst eine Priorität von 10 zugewiesen, dann wird der Richtlinie eine Priorität von 100 zugewiesen, und schließlich hat die Richtlinie eine Reihenfolge von 1000 zugewiesen. Die Responderfunktion implementiert nur die erste Richtlinie, mit der eine Anforderung übereinstimmt, und keine zusätzlichen Richtlinien, mit denen sie möglicherweise auch übereinstimmt. Daher ist die Richtlinienpriorität wichtig, um die von Ihnen beabsichtigten Ergebnisse zu erzielen.

Sie können sich ausreichend Raum lassen, um weitere Richtlinien in beliebiger Reihenfolge hinzuzufügen, und sie dennoch so festlegen, dass sie in der von Ihnen gewünschten Reihenfolge ausgewertet werden, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen den einzelnen Richtlinien festlegen, wenn Sie sie global binden. Sie können dann jederzeit weitere Richtlinien hinzufügen, ohne die Priorität einer vorhandenen Richtlinie neu zuweisen zu müssen.

Weitere Informationen zum Binden von Richtlinien im NetScaler finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Responder-Richtlinien sind an TCP-basierte virtuelle Server gebunden.

So binden Sie eine Responder Policy global mithilfe der NetScaler-Befehlszeile:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Responder Policy global zu binden und die Konfiguration zu überprüfen:

- `bind responder global <policyName> <priority> [<gotoPriorityExpression> [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show responder global`

Beispiel:

```
> bind responder global poliError 100
 Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```

So binden Sie die Responder Policy mithilfe der NetScaler-Befehlszeile an einen bestimmten virtuellen Server:

Geben Sie in der Befehlszeile Folgendes ein:

- `bind lb vserver <name> -policyname <policy_name> -priority <priority>`
- `show lb vserver vs-loadbal <name>`

Beispiel:

```
> bind lb vserver vs-loadbal -policyName policyTwo -priority 100
 Done
> show lb vserver
1)      vs-loadbal (10.102.29.20:80) - HTTP     Type: ADDRESS
        State: OUT OF SERVICE
        Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
        Time since last state change: 2 days, 00:58:03.260
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
```



```
15          Mode: IP
16          Persistence: NONE
17          Vserver IP and Port insertion: OFF
18          Push: DISABLED  Push VServer:
19          Push Multi Clients: NO
20          Push Label Rule: none
21  2)      vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
22          State: DOWN
23          Last state change was at Wed Aug 19 10:03:46 2009 (+213 ms)
24          Time since last state change: 2 days, 00:00:04.260
25          Effective State: DOWN
26          Client Idle Timeout: 9000 sec
27          Down state flush: ENABLED
28          Disable Primary Vserver On Down : DISABLED
29          No. of Bound Services :  0 (Total)       0 (Active)
30          Configured Method: LEASTCONNECTION
31          Mode: IP
32          Persistence: NONE
33          Connection Failover: DISABLED
34   Done
35  <!--NeedCopy-->
```

So binden Sie eine Responder Policy global mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Responder** > **Policies**.
2. Wählen Sie auf der Seite **Responderrichtlinien** eine Responder Policy aus, und klicken Sie dann auf **Richtlinien-Manager**.
3. Wählen Sie im Dialogfeld “ **Responder-Richtlinien-Manager** “ “Punkte binden” die Option “Global”
4. Klicken Sie auf **Richtlinie einfügen**, um eine neue Zeile einzufügen und eine Dropdown-Liste aller Richtlinien für ungebundene Responders anzuzeigen.
5. Klicken Sie auf eine der Richtlinien in der Liste. Diese Richtlinie wird in die Liste der global gebundenen Responder-Richtlinien aufgenommen.
6. Klicken Sie auf **Änderungen übernehmen**.
7. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Konfiguration erfolgreich abgeschlossen wurde.

So binden Sie eine Responder Policy mithilfe der GUI an einen bestimmten virtuellen Server:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie auf der Seite **Load Balancing Virtual** Servers den virtuellen Server aus, an den Sie die Responder Policy binden möchten, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Dialogfeld Virtuellen Server (Load Balancing) konfigurieren** die Registerkarte **Richtlinien**, auf der eine Liste aller auf Ihrer NetScaler Appliance konfigurierten

Richtlinien angezeigt wird.
4. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie an diesen virtuellen Server binden möchten.
5. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Konfiguration erfolgreich abgeschlossen wurde.

Festlegen der Standardaktion für eine Responder-Richtlinie

May 11, 2023

Die NetScaler-Appliance generiert ein undefiniertes Ereignis (UNDEF-Ereignis), wenn eine Anfrage nicht mit einer Responder-Richtlinie übereinstimmt. Die Appliance führt dann die Standardaktion aus, die undefinierten Ereignissen zugewiesen ist. Standardmäßig leitet die Aktion die Anfrage an die nächste Funktion wie Load Balancing, Inhaltsfilterung usw. weiter. Dieses Standardverhalten stellt sicher, dass die Anfragen keine spezielle Responderaktion erfordern, um an Ihre Webserver gesendet zu werden. Außerdem erhalten die Kunden Zugriff auf die von ihnen angeforderten Inhalte.

Wenn eine oder mehrere Websites, die Ihre NetScaler-Appliance schützt, jedoch eine erhebliche Anzahl ungültiger oder böswilliger Anfragen erhalten, sollten Sie möglicherweise die Standardaktion ändern, sodass entweder die Client-Verbindung zurückgesetzt oder die Anfrage gelöscht wird. Bei dieser Art von Konfiguration würden Sie eine oder mehrere Responder-Richtlinien schreiben, die allen legitimen Anfragen entsprechen, und diese Anfragen einfach an ihre ursprünglichen Ziele weiterleiten. Ihre NetScaler-Appliance würde dann alle anderen Anfragen blockieren, wie in der von Ihnen konfigurierten Standardaktion angegeben.

Sie können einem undefinierten Ereignis eine der folgenden Aktionen zuweisen:

- **NEE.** Die NOOP-Aktion bricht die Responderverarbeitung ab, verändert aber nicht den Paketfluss. Damit die Appliance weiterhin Anfragen verarbeitet, die keiner Responder-Richtlinie entsprechen, und sie schließlich an die angeforderte URL weiterleitet, sofern keine andere Funktion eingreift und die Anfrage blockiert oder umleitet. Diese Aktion eignet sich für normale Anfragen an Ihre Webserver und ist die Standardeinstellung.
- **ZURÜCKSETZEN**. Wenn die undefinierte Aktion auf RESET gesetzt ist, setzt die Appliance die Client-Verbindung zurück und informiert den Client darüber, dass er seine Sitzung mit dem Webserver wiederherstellen muss. Die Aktion eignet sich für wiederholte Anfragen nach Webseiten, die nicht existieren, oder für Verbindungen, bei denen es sich möglicherweise um Versuche handelt, Ihre geschützten Websites zu hacken oder zu untersuchen.
- **FALLEN LASSEN**. Wenn die undefinierte Aktion auf DROP gesetzt ist, verwirft die Appliance die Anfrage im Hintergrund, ohne dem Client in irgendeiner Weise zu antworten. Diese Aktion

eignet sich für Anfragen, die Teil eines DDoS-Angriffs oder eines anderen anhaltenden Angriffs auf Ihre Server zu sein scheinen.

Hinweis: UNDEF-Ereignisse werden nur für Clientanfragen ausgelöst. Für Antworten werden keine UNDEF-Ereignisse ausgelöst.

Gehen Sie wie folgt vor, um die undefinierte Aktion mithilfe der NetScaler-Befehlszeile festzulegen:

Geben Sie an der Befehlszeile den folgenden Befehl ein, um die undefinierte Aktion festzulegen und die Konfiguration zu überprüfen:

- `set responder param -undefAction (RESET|DROP|NOOP)[-timeout <msecs>]`
- `show responder param`

Hierbei gilt:

timeout — Maximale Zeit in Millisekunden, damit alle Richtlinien und die ausgewählten Aktionen ohne Unterbrechung verarbeitet werden können. Wenn das Timeout erreicht ist, führt die Auswertung dazu, dass ein UNDEF ausgelöst wird und keine weitere Verarbeitung durchgeführt wird.

Mindestwert: 1

Maximalwert: 5000

Beispiel:

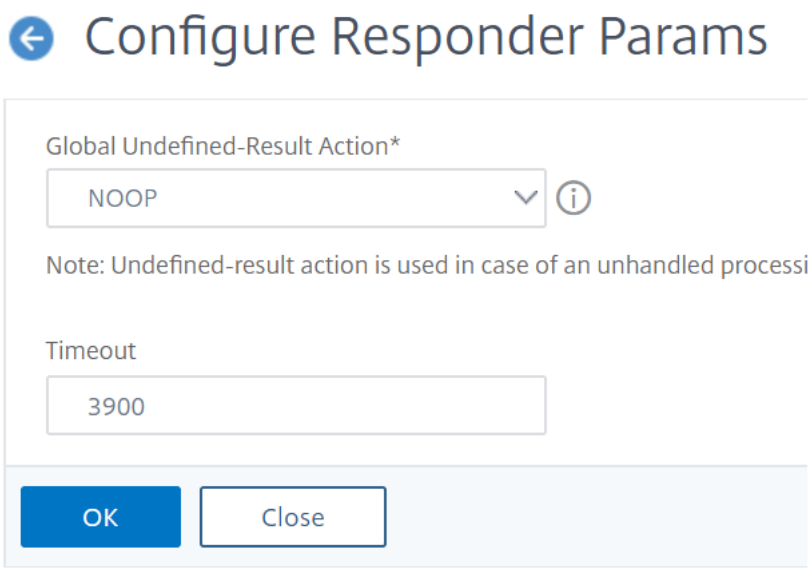
```
>set responder param -undefAction RESET -timeout 3900
 Done
> show responder param
Action Name: RESET
Timeout: 3900
 Done
>
<!--NeedCopy-->
```

Stellen Sie die undefinierte Aktion mithilfe der GUI ein

1. Navigieren Sie zu **AppExpert** > **Responder**und klicken Sie dann unter **Einstellungen**auf den Link **Responder-Einstellungen ändern** .
2. Stellen Sie auf der Seite **„Responder-Parameter** festlegen“ die folgenden Parameter ein:
   a) Globale Aktion mit undefiniertem Ergebnis. Eine Aktion mit undefiniertem Ergebnis wird bei einer unbehandelten Verarbeitungsausnahme in den Responder-Richtlinien und -Aktionen bevorzugt. Wählen Sie **NOOP**, **RESET**oder **DROP**.
   b) Auszeit. Maximale Zeit in Millisekunden, damit alle Richtlinien und die ausgewählten Aktionen ohne Unterbrechung verarbeitet werden können. Wenn das Timeout erreicht ist,

führt die Auswertung dazu, dass ein UNDEF ausgelöst wird und keine weitere Verarbeitung durchgeführt wird.

3. Klicken Sie auf **OK**.



Beispiele für Responder Action und Policy

May 11, 2023

Aktionen und Richtlinien der Responder sind leistungsstark und komplex, aber Sie können mit relativ einfachen Anwendungen beginnen.

Beispiel: Blockieren des Zugriffs von bestimmten IPs

Die folgenden Verfahren blockieren den Zugriff auf Ihre geschützte Website (n) durch Clients, die vom CIDR 222.222.0.0/16 stammen. Der Responder sendet eine Fehlermeldung, dass der Client nicht berechtigt ist, auf die angeforderte URL zuzugreifen.

So blockieren Sie den Zugriff mithilfe der NetScaler-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Zugriff zu blockieren:

- Responder Action hinzufügen act_unauthorized response mit “HTTP/1.1 403 Forbidden\ r\ n\ r\ n” + “Client:” + CLIENT.IP.SRC + “ist nicht berechtigt, auf URL zuzugreifen:” + “HTTP.REQ.URL.HTTP_URL_SAFE”’
- Responder Policy hinzugefügt pol_un “CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)” act_unauthorized
- binden Responder global pol_un 10

So blockieren Sie den Zugriff mit der GUI:

1. Erweitern Sie im Navigationsbereich **Responder**, und klicken Sie dann auf **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Gehen **Sie im Dialogfeld Responderaktion erstellen** wie folgt vor:
   a) Geben Sie in das Textfeld **Name** act_unauthorized ein.
   b) Wählen Sie unter Typ die Option Antworten mit aus.
   c) Geben Sie im Bereich Zieltext die folgende Zeichenfolge ein: “HTTP/1.1 403 Forbidden\ r\ n\ r\ n” + “Client:” + CLIENT.IP.SRC + “ist nicht berechtigt, auf die URL zuzugreifen:” + HTTP.REQ.URL.HTTP_URL_SAFE
   d) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder Action mit dem Namen act_unauthorized wird jetzt auf der Seite **Responderaktionen** angezeigt.
4. Klicken Sie im Navigationsbereich auf **Richtlinien**.
5. Klicken Sie im Detailbereich auf **Hinzufügen**.
6. Gehen **Sie im Dialogfeld Responder-Richtlinie erstellen** wie folgt vor:
   a) Geben Sie in das Textfeld Name pol_unauthorized ein.
   b) Wählen Sie unter **Aktion**die Option act_unauthorized aus.
   c) Geben Sie im Fenster **Ausdruck** die folgende Regel ein: CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
   d) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder-Richtlinie mit dem Namen pol_unauthorized wird nun auf der Seite **Responder-Richtlinien** angezeigt.
7. Binden Sie Ihre neue Richtlinie pol_unauthorized global, wie unter Binding a Responder Policybeschrieben.

Beispiel: Umleiten eines Clients zu einer neuen URL

Mit den folgenden Verfahren werden Clients, die innerhalb des CIDR 222.222.0.0/16 auf Ihre geschützte Website (s) zugreifen, zu einer angegebenen URL umgeleitet.

So leiten Sie Clients mithilfe der NetScaler-Befehlszeile um:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um Clients umzuleiten und die Konfiguration zu überprüfen:

- Responder Action hinzufügen act_redirect Weiterleitung `"<http://www.example.com/404.html>"`
- Responder Action anzeigen act_redirect
- Responder Policy hinzufügen pol_redirect “CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)” act_redirect
- Responder Policy anzeigen pol_redirect

- binden Responder global pol_redirect 10

Beispiel:

```
> add responder action act_redirect redirect `" http ://www.example.com
    /404.html "`
Done

> add responder policy pol_redirect "CLIENT.IP.SRC.IN_SUBNET
    (222.222.0.0/16)" act_redirect
Done
<!--NeedCopy-->
```

So leiten Sie Clients mit der GUI um:

1. Navigieren Sie zu **AppExpert** > **Responder** > **Actions**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Gehen **Sie im Dialogfeld Responderaktion erstellen** wie folgt vor:
   a) Geben Sie im Textfeld **Name** den Text act_redirect ein.
   b) Wählen Sie unter Typ die Option **Umleitung**aus.
   c) Geben Sie im Bereich **Zieltext** die folgende Zeichenfolge ein: `"<http://www.example.com/404.html>"`
   d) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder Action mit dem Namen act_redirect wird jetzt auf der Seite **Responderaktionen** angezeigt.
4. Klicken Sie im Navigationsbereich auf **Richtlinien**.
5. Klicken Sie im Detailbereich auf **Hinzufügen**.
6. Gehen **Sie im Dialogfeld Responder-Richtlinie erstellen** wie folgt vor:
   a) Geben Sie in das Textfeld **Name** pol_redirect ein.
   b) Wählen Sie unter **Aktion**die Option act_redirect aus.
   c) Geben Sie im Fenster **Ausdruck** die folgende Regel ein: CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
   d) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder-Richtlinie mit dem Namen pol_redirect wird nun auf der Seite **Responder-Richtlinien** angezeigt.
7. Binden Sie Ihre neue Richtlinie pol_redirect global, wie unter Binding a Responder Policybeschrieben.

Durchmesser-Unterstützung für Responder

May 11, 2023

Die Responder-Funktion unterstützt jetzt das Diameter-Protokoll. Sie können Responder so konfigurieren, dass er auf Diameter-Anfragen genauso reagiert wie HTTP- und TCP-Anfragen. Sie können Responder beispielsweise so konfigurieren, dass er auf Anfragen von einem bestimmten Diameter-Ursprung mit einer Weiterleitung zu einer für Mobilgeräte optimierten Webseite reagiert. Es wurden eine Reihe von NetScaler-Ausdrücken hinzugefügt, die die Untersuchung des Diameter-Headers und der Attributwertpaare (AVPs) unterstützen. Diese Ausdrücke unterstützen die Suche nach bestimmten AVPs nach Index, ID oder Namen, untersuchen die Informationen in jedem AVP und senden eine entsprechende Antwort.

So konfigurieren Sie Responder so, dass er auf eine Diameter-Anfrage reagiert:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add responder action <actname> RESPONDWITH "DIAMETER.NEW_REDIRECT(\"aaa://host.example.com\")"`

  Für <actname>, ersetzen Sie Ihre neue Aktion durch einen Namen. Der Name kann aus einem bis 127 Zeichen bestehen und Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie `aaa://host.example.com` durch die URL des Diameter-Hosts, zu dem Sie Verbindungen umleiten möchten.

- add responder policy <polname> “diameter.req.avp(264).value.eq(“host1.example.net”)” <actname>

  Für <polname>, ersetzen Sie einen Namen für Ihre neue Richtlinie. Wie bei <actname>kann der Name aus einem bis 127 Zeichen bestehen und Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie für host1.example.net den Namen des ursprünglichen Hosts der Anfragen, die Sie umleiten möchten. Ersetzen Sie durch den Namen der Aktion, die Sie gerade erstellt haben. <actname>

- `bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST`

  Ersetzen Sie <vservername> durch den Namen des virtuellen Load-Balancing-Servers, an den Sie die Richtlinie binden möchten. Ersetzen Sie <polname> durch den Namen der Richtlinie, die Sie gerade erstellt haben. Ersetzen Sie <priority> durch eine Priorität für die Richtlinie.

Beispiel:

Um eine Responder-Aktion und -Richtlinie zu erstellen, um auf Diameter-Anfragen zu antworten, die von „host1.example.net“ stammen, mit einer Weiterleitung zu „host.example.com“, könnten Sie die folgende Aktion und Richtlinie hinzufügen und die Richtlinie wie gezeigt binden.

```
1 > add responder action act_resp-dm-redirect RESPONDWITH "DIAMETER.
     NEW_REDIRECT("aaa://host.example.com")"
2 Done
3
```



```
> add responder pol_resp-dm-redirect "diameter.req.avp(264).value.eq("
    host1.example.net")" act_resp-dm-redirect
Done

> bind lb vserver vs1 -policyName pol_resp-dm-redirect -priority 10 -
    type REQUEST
Done
<!--NeedCopy-->
```

RADIUS-Unterstützung für Responder

May 11, 2023

Die NetScaler-Ausdruckssprache enthält Ausdrücke, mit denen Informationen aus RADIUS-Anfragen extrahiert und bearbeitet werden können. Mit diesen Ausdrücken können Sie die Responder-Funktion verwenden, um auf RADIUS-Anfragen zu antworten. Ihre Responder-Richtlinien und -Aktionen können jeden Ausdruck verwenden, der für eine RADIUS-Anfrage angemessen oder relevant ist. Die verfügbaren Ausdrücke ermöglichen es Ihnen, den RADIUS-Nachrichtentyp zu identifizieren, jedes Attributwertpaar (AVP) aus der Verbindung zu extrahieren und auf der Grundlage dieser Informationen verschiedene Antworten zu senden. Sie können auch Richtlinienlabels erstellen, die alle Responder-Richtlinien für RADIUS-Verbindungen aufrufen.

Sie können RADIUS-Ausdrücke verwenden, um einfache Antworten zu erstellen, für die keine Kommunikation mit dem RADIUS-Server erforderlich ist, an den die Anfrage gesendet wurde. Wenn eine Responder-Richtlinie einer Verbindung entspricht, erstellt und sendet NetScaler die entsprechende RADIUS-Antwort, ohne den RADIUS-Authentifizierungsserver zu kontaktieren. Wenn die Quell-IP-Adresse einer RADIUS-Anfrage beispielsweise aus einem Subnetz stammt, das in der Responder-Richtlinie angegeben ist, kann der NetScaler auf diese Anfrage mit einer Meldung zur Zugriffsverweigerung antworten oder die Anfrage einfach verwerfen.

Sie können auch Richtlinienlabels erstellen, um bestimmte Arten von RADIUS-Anfragen anhand einer Reihe von Richtlinien weiterzuleiten, die für diese Anfragen geeignet sind.

Hinweis: Die aktuellen RADIUS-Ausdrücke funktionieren nicht mit RADIUS-IPv6-Attributen.

In der NetScaler-Dokumentation für Ausdrücke, die RADIUS unterstützen, wird davon ausgegangen, dass Sie mit der grundlegenden Struktur und dem Zweck der RADIUS-Kommunikation vertraut sind. Wenn Sie weitere Informationen zu RADIUS benötigen, lesen Sie in der RADIUS-Serverdokumentation nach oder suchen Sie online nach einer Einführung in das RADIUS-Protokoll.

Konfiguration von Responder-Richtlinien für RADIUS

Das folgende Verfahren verwendet die NetScaler-Befehlszeile, um eine Responder-Aktion und -Richtlinie zu konfigurieren und die Richtlinie an einen RADIUS-spezifischen globalen Bindungspunkt zu binden.

Gehen Sie wie folgt vor, um eine Responder-Aktion und -Richtlinie zu konfigurieren und die Richtlinie zu binden:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>` wobei `<bindPoint>` steht für einen der RADIUS-spezifischen globalen Bindungspunkte.

RADIUS-Ausdrücke für Responder

In einer Responderkonfiguration können Sie die folgenden NetScaler-Ausdrücke verwenden, um auf verschiedene Teile einer RADIUS-Anfrage zu verweisen.

Identifizierung des Verbindungstyps:

- RADIUS.IS_CLIENT. Gibt TRUE zurück, wenn es sich bei der Verbindung um eine RADIUS-Clientnachricht (Anfrage) handelt.
- RADIUS.IS_SERVER. Gibt TRUE zurück, wenn es sich bei der Verbindung um eine RADIUS-Servernachricht (Antwort) handelt.

Ausdrücke anfordern:

- `RADIUS.REQ.CODE`. Gibt die Zahl zurück, die dem RADIUS-Anforderungstyp entspricht. Eine Ableitung der Klasse num_at. Eine RADIUS-Zugriffsanfrage würde beispielsweise 1 (eins) zurückgeben. Eine RADIUS-Buchhaltungsanfrage würde 4 zurückgeben.
- `RADIUS.REQ.LENGTH`. Gibt die Länge der RADIUS-Anfrage einschließlich des Headers zurück. Eine Ableitung der Klasse num_at.
- `RADIUS.REQ.IDENTIFIER`. Gibt den RADIUS-Anforderungsbezeichner zurück, eine Nummer, die jeder Anfrage zugewiesen wird und die es ermöglicht, die Anfrage mit der entsprechenden Antwort abzugleichen. Eine Ableitung der Klasse num_at.
- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`. Gibt den Wert des ersten Auftretens dieses AVP als Zeichenfolge vom Typ text_t zurück.
- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`. Gibt die angegebene Instanz des AVP als Zeichenfolge vom Typ raVP_T zurück. Ein bestimmter RADIUS-AVP kann in einer RADIUS-Nachricht mehrfach vorkommen. INSTANCE (0) gibt die erste Instanz zurück, INSTANCE (1) gibt die zweite Instanz zurück und so weiter, bis zu sechzehn Instanzen.

- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`. Gibt den Wert der angegebenen Instanz des AVP als Zeichenfolge vom Typ text_t zurück.
- `RADIUS.REQ.AVP(<AVP code no>).COUNT`. Gibt die Anzahl der Instanzen eines bestimmten AVP in einer RADIUS-Verbindung als Ganzzahl zurück.
- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`. Gibt TRUE zurück, wenn der angegebene AVP-Typ in der Nachricht vorhanden ist, oder FALSE, wenn dies nicht der Fall ist.

Antwortausdrücke:

RADIUS-Antwortausdrücke sind identisch mit RADIUS-Anforderungsausdrücken, mit der Ausnahme, dass RES REQ ersetzt.

Typisierungen von AVP-Werten:

Der ADC unterstützt Ausdrücke zur Typisierung von RADIUS-AVP-Werten in die Datentypen Text, Integer, unsigned Integer, Long, unsigned Long, IPv4-Adresse, IPv6-Adresse, IPv6-Adresse, IPv6-Präfix und Zeit. Die Syntax ist dieselbe wie bei anderen NetScaler-Typecast-Ausdrücken.

Beispiel:

Der ADC unterstützt Ausdrücke zur Typisierung von RADIUS-AVP-Werten in die Datentypen Text, Integer, unsigned Integer, Long, unsigned Long, IPv4-Adresse, IPv6-Adresse, IPv6-Adresse, IPv6-Präfix und Zeit. Die Syntax ist dieselbe wie bei anderen NetScaler-Typecast-Ausdrücken.

```
1 RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
2 <!--NeedCopy-->
```

Ausdrücke vom Typ AVP:

Der NetScaler unterstützt Ausdrücke zum Extrahieren von RADIUS-AVP-Werten mithilfe der in RFC2865 und RFC2866 beschriebenen zugewiesenen Integer-Codes. Sie können auch Text-Aliase verwenden, um dieselbe Aufgabe zu erledigen. Es folgen einige Beispiele.

- RADIUS.REQ.AVP (1) .VALUE oder RADIUS.REQ.USERNAME.VALUE. Extrahiert den RADIUS-Benutzernamenwert.
- RADIUS.REQ.AVP (4). VALUE oder RADIUS.REQ. acct_Session_ID.Wert. Extrahiert die accT-Session-ID AVP (Code 44) aus der Nachricht.
- RADIUS.REQ.AVP (26). VALUE oder RADIUS.REQ.VENDOR_SPECIFIC.VALUE. Extrahiert den herstellerspezifischen Wert.

Die Werte der am häufigsten verwendeten RADIUS-AVPs können auf dieselbe Weise extrahiert werden.

RADIUS-Bindepunkte:

Vier globale Bindungspunkte sind für Richtlinien verfügbar, die RADIUS-Ausdrücke enthalten.

- RADIUS_REQ_OVERRIDE. Warteschlange für Richtlinien zur Priorität/Außerkraftsetzung von Anfragen.

- RADIUS_REQ_DEFAULT. Standardwarteschlange für Anforderungsrichtlinien.
- RADIUS_RES_OVERRIDE. Warteschlange für Antwortrichtlinien zur Priorität/Außerkraftsetzung.
- RADIUS_RES_DEFAULT. Standardwarteschlange für Antwortrichtlinien.

RADIUS-Responderspezifische Ausdrücke:

- RADIUS_RESPONDWITH. Antworten Sie mit der angegebenen RADIUS-Antwort. Die Antwort wird mit NetScaler-Ausdrücken erstellt, sowohl mit RADIUS-Ausdrücken als auch mit allen anderen zutreffenden Ausdrücken.
- RADIUS.NEUE_ANTWORT. Sendet eine neue RADIUS-Antwort an den Benutzer.
- RADIUS.NEW_ACCESSREJECT. Lehnt die RADIUS-Anfrage ab.
- RADIUS.NEW_AVP. Fügt der Antwort den angegebenen neuen AVP hinzu.

Anwendungsfälle

Im Folgenden finden Sie Anwendungsfälle für RADIUS mit Responder.

Sperren von RADIUS-Anfragen aus einem bestimmten Netzwerk

Um die Responder-Funktion so zu konfigurieren, dass Authentifizierungsanfragen von einem bestimmten Netzwerk blockiert werden, erstellen Sie zunächst eine Responder-Aktion, die Anfragen ablehnt. Verwenden Sie die Aktion in einer Richtlinie, die Anfragen aus den Netzwerken auswählt, die Sie blockieren möchten. Binden Sie die Responder-Richtlinie an einen RADIUS-spezifischen globalen Bindungspunkt und geben Sie Folgendes an:

- Die Priorität
- END als NextExpr-Wert, um sicherzustellen, dass die Bewertung der Richtlinie beendet wird, wenn diese Richtlinie eingehalten wird
- RADIUS_REQ_OVERRIDE als die Warteschlange, der Sie die Richtlinie zuweisen, sodass sie vor den Richtlinien ausgewertet wird, die der Standardwarteschlange zugewiesen wurden

So konfigurieren Sie Responder so, dass Anmeldungen aus einem bestimmten Netzwerk blockiert werden**

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder global <polName> <priority> <nextExpr> -type <bindPoint>`

Beispiel:

```
> add responder action rspActRadiusReject respondwith radius.
   new_accessreject
Done

```



```
4 > add responder policy rspPolRadiusReject client.ip.src.in_subnet
     (10.224.85.0/24) rspActRadiusReject
5 Done
6
7 > bind responder global rspPolRadiusReject 1 END -type
     RADIUS_REQ_OVERRIDE
8 <!--NeedCopy-->
```

DNS-Unterstützung für die Responder-Funktion

May 11, 2023

Sie können die Responder-Funktion so konfigurieren, dass sie auf DNS-Anfragen genauso reagiert wie auf HTTP- und TCP-Anfragen. Sie könnten es beispielsweise so konfigurieren, dass DNS-Antworten über UDP gesendet werden und sichergestellt wird, dass die DNS-Anfragen vom Client über TCP gesendet werden. Eine Reihe von NetScaler-Ausdrücken unterstützen die Untersuchung des DNS-Headers in der Anfrage. Diese Ausdrücke untersuchen bestimmte Header-Felder und senden eine entsprechende Antwort.

- **DNS-Ausdrücke**. In einer Responderkonfiguration können Sie die folgenden NetScaler-Ausdrücke verwenden, um auf verschiedene Teile einer DNS-Anfrage zu verweisen:

Ausdrücke	Beschreibungen
DNS.NEW_RESPONSE	Erstellt basierend auf der Anfrage eine neue leere DNS-Antwort.
DNS.NEW_RESPONSE <AA, TC, rcode>	Erstellt eine neue DNS-Antwort auf der Grundlage der angegebenen Parameter.

- **DNS-Bindungspunkte**. Die folgenden globalen Bindungspunkte sind für Richtlinien verfügbar, die DNS-Ausdrücke enthalten.

Punkte binden	Beschreibungen
DNS_REQ_OVERRIDE	Warteschlange für Richtlinien zur Priorität/Außerkraftsetzung von Anfragen.
DNS_REQ_DEFAULT	Standardwarteschlange für Anforderungsrichtlinien.

Zusätzlich zu den Standardbindungspunkten können Sie Richtlinienlabels des Typs DNS erstellen und DNS-Richtlinien an diese binden.

Konfiguration der Responder-Richtlinien für DNS

Das folgende Verfahren verwendet die NetScaler-Befehlszeile, um eine Responder-Aktion und -Richtlinie zu konfigurieren und die Richtlinie an einen Responder-spezifischen globalen Bindungspunkt zu binden.

So konfigurieren Sie den Responder so, dass er auf eine DNS-Anfrage reagiert:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

1. `add responder action <actName> <actType>`

   Für <actname>, ersetzen Sie Ihre neue Aktion durch einen Namen. Der Name kann 1 bis 127 Zeichen lang sein und Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. <actType>Ersetzen Sie durch den Responder-Aktionstyp *respondWith*.

2. `add responder policy <polName> <rule> <actName>`

   Für <polname>, ersetzen Sie einen Namen für Ihre neue Richtlinie. Denn <actname>der Name kann 1 bis 127 Zeichen lang sein und Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie durch den Namen der Aktion, die Sie gerade erstellt haben. <actname>

3. `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>`

   Geben Sie für <bindPoint>einen der Responderspezifischen globalen Bindungspunkte an. <polName>Ersetzen Sie ihn durch den Namen der Richtlinie, die Sie gerade erstellt haben. Geben Sie für <priority>die Priorität der Richtlinie an.

Beispielkonfiguration — Alle DNS-Anfragen über TCP erzwingen:

Um alle DNS-Anforderungen über TCP zu erzwingen, erstellen Sie eine Responder-Aktion, die das TC-Bit und rcode als NOERROR setzt.

```
> add responder action resp_act_set_tc_bit respondwith DNS.NEW_RESPONSE
   (true, true, NOERROR)
Done

> add responder policy enforce_tcp  dns.REQ.TRANSPORT.EQ(udp)
   resp_act_set_tc_bit
Done

>bind lb vserver dns_udp  - policyName  enforce_tcp   -type request  -
   priority 100
Done
<!--NeedCopy-->
```


MQTT-Unterstützung für Responder

May 11, 2023

Die Responder-Funktion unterstützt das MQTT-Protokoll. Sie können Responder-Richtlinien so konfigurieren, dass auf der Grundlage der Parameter in der eingehenden MQTT-Nachricht eine Aktion ausgeführt wird.

Die Aktion reagiert mit einem der folgenden Befehle auf eine neue Verbindung:

- DROP
- RESET
- NOOP
- Eine Responder-Aktion, um eine neue MQTT CONNACK-Antwort zu initiieren.

Konfiguration von Responder-Richtlinien für MQTT

Nachdem Sie die Responder-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen für die Bearbeitung von MQTT-Anfragen konfigurieren. Konfigurieren Sie dann eine Responder-Richtlinie. Sie können die Responder-Richtlinien global oder an einen bestimmten virtuellen Load-Balancing-Server oder einen virtuellen Content Switching-Server binden.

Die folgenden Bindungspunkte sind verfügbar, um die Responder-Richtlinien global zu binden:

- MQTT_REQ_DEFAULT
- MQTT_REQ_OVERRIDE
- MQTT_JUMBO_REQ_DEFAULT
- MQTT_JUMBO_REQ_OVERRIDE

Die folgenden Bindungspunkte sind verfügbar, um die Responder-Richtlinien an einen virtuellen Content Switching- oder Load-Balancing-Server zu binden:

- REQUEST
- MQTT_JUMBO_REQ (dieser Bindpunkt wird nur für Jumbo-Pakete verwendet)

So konfigurieren Sie den Responder so, dass er mithilfe der CLI auf eine MQTT-Anforderung reagiert

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

Konfigurieren Sie eine Responder-Aktion.

```
add responder action <actName> <actType>
<!--NeedCopy-->
```


- Für `actname`, ersetzen Sie Ihre neue Aktion durch einen Namen. Der Name kann 1—127 Zeichen lang sein und Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.
- Ersetzen Sie den `actType`Aktionstyp Respondwith durch einen Responder-Aktionstyp.

Beispiel:

```
add responder action mqtt_connack_unsup_ver respondwith MQTT.
   NEW_CONNACK(132)
<!--NeedCopy-->
```

Konfigurieren Sie eine Responder-Richtlinie. Die NetScaler-Appliance reagiert auf die MQTT-Anfragen, die durch diese Responder-Richtlinie ausgewählt werden.

```
add responder policy <polName> <rule> <actname>
<!--NeedCopy-->
```

- Für `polname`, ersetzen Sie einen Namen für Ihre neue Richtlinie.
- `actname`Ersetzen Sie ihn durch den Namen der Aktion, die Sie erstellt haben.

Beispiel:

```
add responder policy reject_lower_version "MQTT.HEADER.COMMAND.EQ(
   CONNECT) && MQTT.VERSION.LT(3)" mqtt_connack_unsup_ver
<!--NeedCopy-->
```

Binden Sie die Responder-Richtlinie an einen bestimmten virtuellen Load-Balancing-Server oder einen virtuellen Content Switching-Server. Die Richtlinie gilt nur für MQTT-Anfragen, deren Ziel-IP-Adresse die VIP dieses virtuellen Servers ist.

```
bind lb vserver <name> -policyName <policy_name> -priority <priority>

bind cs vserver <name> -policyName <policy_name> -priority <priority>
<!--NeedCopy-->
```

- Ersetzen Sie ihn durch den Namen der Richtlinie, die Sie erstellt haben. `policy_name`
- Geben Sie für `priority`die Priorität der Richtlinie an.

Beispiel:

```
bind lb vserver lb1 -policyName reject_lower_version -priority 50

bind cs vserver mqtt_frontend_cs -policyName reject_lower_version -
   priority 5
<!--NeedCopy-->
```


Anwendungsfall 1: Filtern Sie Clients anhand des Benutzernamens oder der Client-ID

Der Administrator kann eine MQTT-Responder-Richtlinie konfigurieren, um die Verbindung basierend auf dem Benutzernamen oder der Client-ID in der MQTT CONNECT-Nachricht abzulehnen.

Beispielkonfiguration für das Filtern von Clients anhand der Client-ID

```
add policy patset filter_clients
bind policy patset filter_clients client1

add responder action mqtt_connack_invalid_client respondwith MQTT.
   NEW_CONNACK(2)

add responder policy reject_clients "MQTT.HEADER.COMMAND.EQ(CONNECT) &&
    mqtt.connect.clientid.equals_any("filter_clients")"
   mqtt_connack_invalid_client

bind cs vserver mqtt_frontend_cs -policyName reject_clients -priority 5
<!--NeedCopy-->
```

Anwendungsfall 2: Beschränken Sie die maximale Nachrichtenlänge von MQTT-Nachrichten, um Jumbo-Pakete zu verarbeiten

Der Administrator kann eine MQTT-Responder-Richtlinie konfigurieren, um die Client-Verbindung zu unterbrechen, wenn die Länge der Nachricht einen bestimmten Schwellenwert überschreitet, oder je nach Anforderung die erforderlichen Maßnahmen ergreifen.

Um Jumbo-Pakete zu verarbeiten, sind die Responder-Richtlinien mit einem der folgenden Regelmuster an den Jumbo-Bindpunkt gebunden:

- MQTT.MESSAGE_LENGTH
- MQTT.COMMAND
- MQTT.FROM_CLIENT
- MQTT.FROM_SERVER

Richtlinien, die an Jumbo-Bind-Punkte gebunden sind, werden nur für Jumbo-Pakete ausgewertet.

Beispielkonfiguration zur Begrenzung der maximalen Nachrichtenlänge von MQTT-Nachrichten

```
set lb parameter -dropmqttjumbomessage no

```



```
3 add responder policy drop_large_message MQTT.MESSAGE_LENGTH.GT(100000)
    reset
4
5 bind cs vserver mqtt_frontend_cs -policyName drop_large_message -
    priority 10
6 <!--NeedCopy-->
```

In diesem Beispiel ist der Parameter `dropmqttjumbomessage` auf NEIN gesetzt. Daher verarbeitet die ADC-Appliance die Nachrichten mit einer Länge von mehr als 64.000 Byte und weniger als 1.00.000 Byte. Die Nachrichten mit einer Länge von mehr als 1.00.000 Byte werden zurückgesetzt.

So leiten Sie eine HTTP-Anfrage mithilfe des Responders an HTTPS um

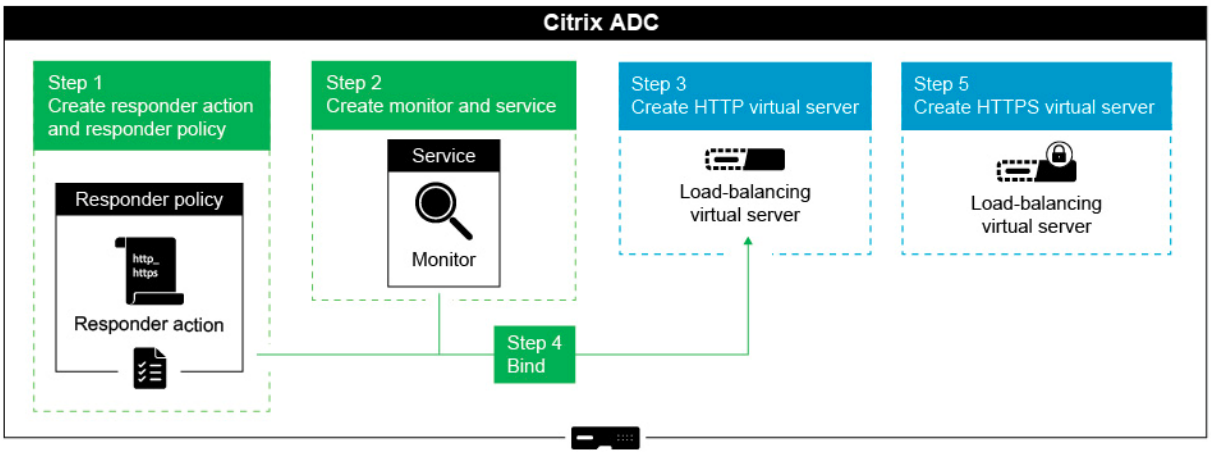
May 11, 2023

In diesem Artikel wird erklärt, wie Sie die Responder-Funktion mit einem Lastausgleich für virtuelle Server-IP-Adressen konfigurieren und Clientanfragen von HTTP auf HTTPS umleiten.

Stellen Sie sich ein Szenario vor, in dem ein Benutzer versuchen könnte, auf eine sichere Website zuzugreifen, indem er eine HTTP-Anfrage sendet. Anstatt die Anfrage zu löschen, sollten Sie die Anfrage an eine sichere Website weiterleiten. Sie können die Responder-Funktion verwenden, um die Anfrage an die sichere Website umzuleiten, ohne den Pfad und die URL-Abfrage zu ändern, auf die der Benutzer zugreifen möchte.

Wie der NetScaler-Responder eine Anfrage von HTTP zu HTTPS umleitet

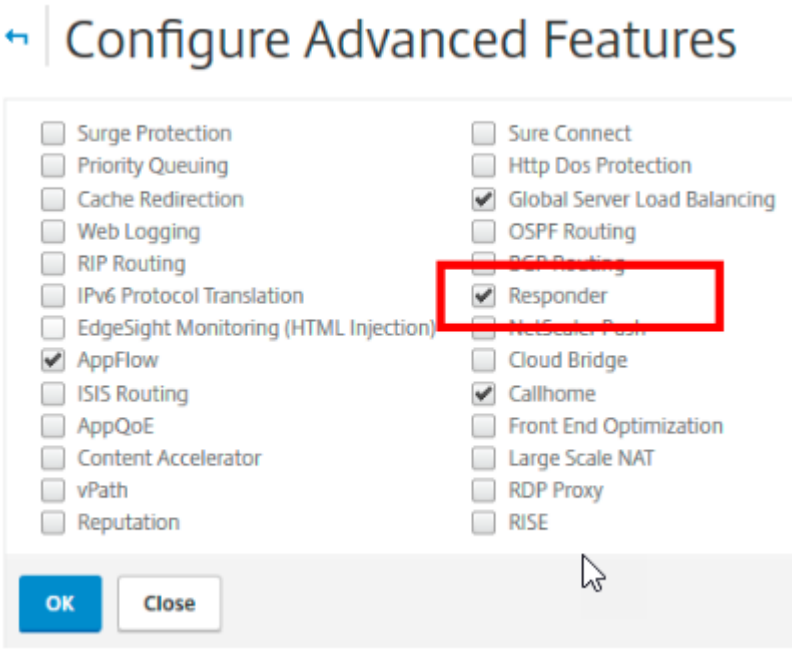
Die folgende Abbildung zeigt Schritt für Schritt, wie die Appliance eine Anfrage umleitet.



> **Hinweis**: Die Navigationspfade und Screenshots stammen von NetScaler 11.0.

Gehen Sie wie folgt vor, um die Responder-Funktion zusammen mit den Load Balancing-VIP-Adressen einer NetScaler-Appliance so zu konfigurieren, dass Clientanfragen von HTTP zu HTTPS umgeleitet werden.

1. Aktivieren Sie die Responder-Funktion auf der Appliance. Navigieren Sie zu **System** > **Einstellungen** > **Erweiterte Funktionen konfigurieren** > **Responder**.



2. Erstellen Sie eine Responder-Aktion und geben Sie im Feld Name einen geeigneten Namen an, z. B. http_to_https_actn.
3. **Um eine Responder-Aktion zu erstellen, erweitern Sie im Navigationsbereich**AppExpert**>**Responder**, klicken Sie auf**Aktionen**und dann auf Hinzufügen.**
4. Wählen Sie Umleitung als Typ aus.
5. Geben Sie in das Feld **Ausdruck** den folgenden Ausdruck ein:

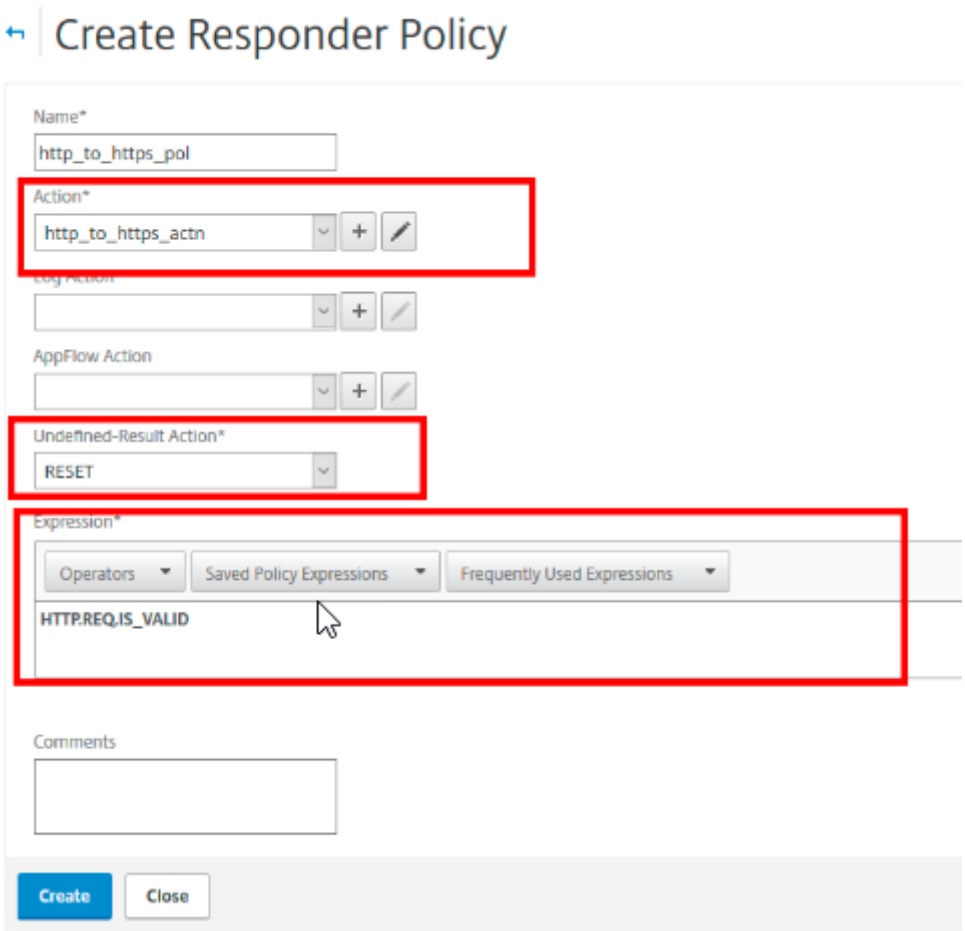
   ```
   "https://"+ HTTP.REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY
   .HTTP_URL_SAFE.
   ```

6. Stellen Sie in NetScaler Version 9.0 und 10.0 sicher, dass die Option **Bypass Safety Check** deaktiviert ist.

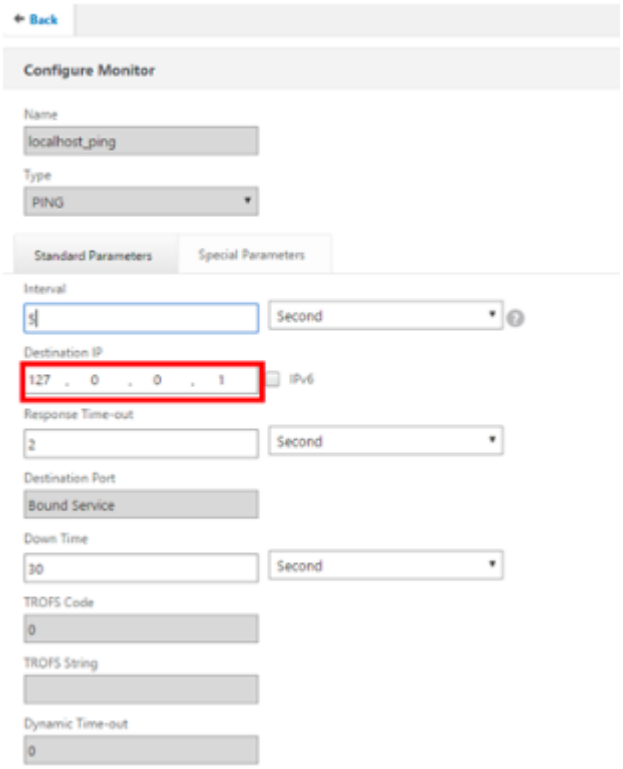
   Hinweis: Diese Option ist ab NetScaler 11.0 nicht mehr verfügbar.

7. Erstellen Sie eine **Responder-Richtlinie** und geben Sie im Feld Name einen entsprechenden Namen an, z. B. http_to_https_pol.

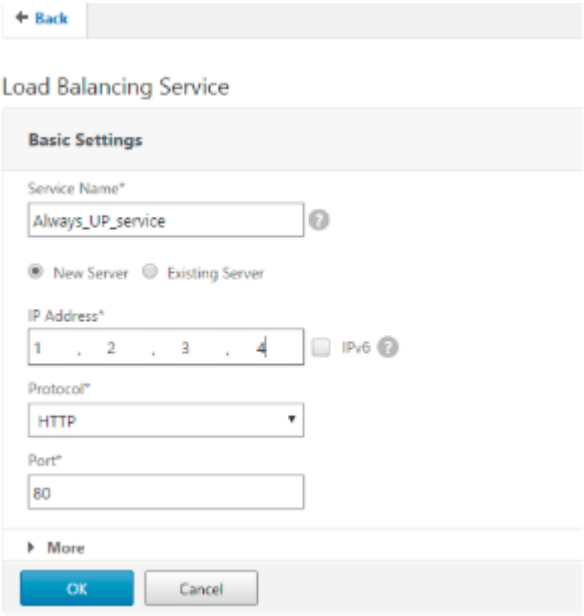
8. **Um eine Responder-Richtlinie zu erstellen, erweitern Sie im Navigationsbereich**AppExpert**>**Responder**, klicken Sie auf**Richtlinien**und dann auf Hinzufügen.**
9. Wählen Sie in der Aktionsliste den Namen der Aktion aus, die Sie erstellt haben.
10. Wählen Sie in der Liste Undefinierte Aktionen die Option ZURÜCKSETZEN aus.
11. Geben Sie den Ausdruck **HTTP.REQ.IS_VALID** in das Feld **Ausdruck** ein, wie im folgenden Screenshot gezeigt.



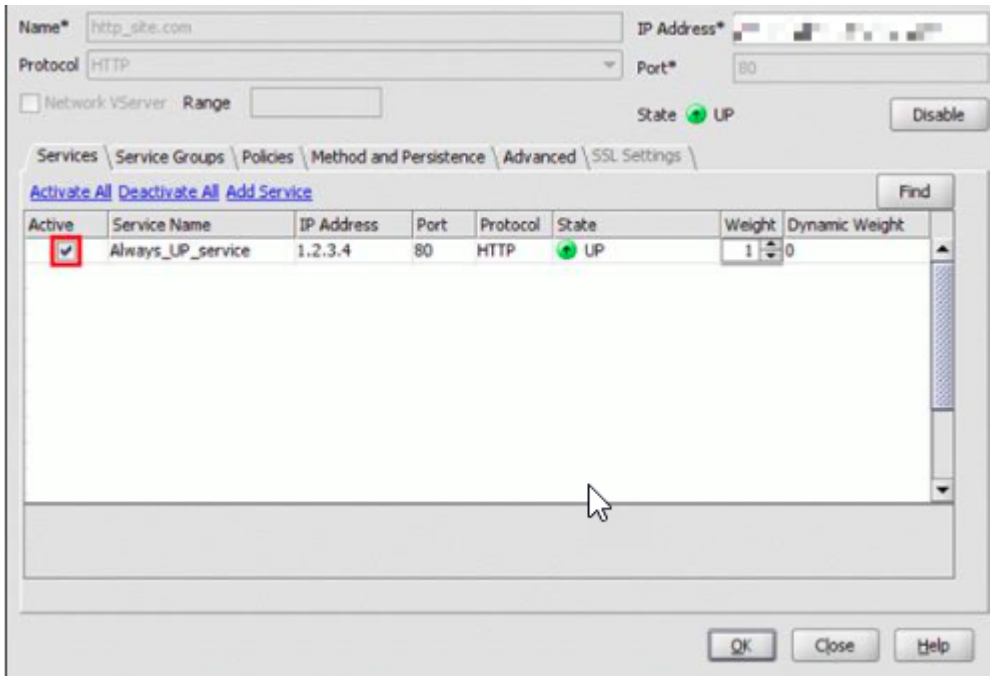
1. Erstellen Sie einen Monitor, dessen Status immer als UP gekennzeichnet ist, und geben Sie im Feld Name einen entsprechenden Namen an, z. B. localhost_ping.
2. Um einen Monitor zu erstellen, erweitern Sie im Navigationsbereich **Load Balancing**, klicken Sie auf **Monitore** und dann auf **Hinzufügen**.
3. Geben Sie im Feld **Ziel-IP** die 127.0.0.1-IP-Adresse an, wie im folgenden Screenshot gezeigt.



4. **Erstellen Sie einen Dienst und geben Sie im Feld Name einen entsprechenden Namen an, z. B. Always_up_Service.**
5. Um einen Dienst zu erstellen, erweitern Sie im Navigationsbereich **Load Balancing**, klicken Sie auf **Dienste** und dann auf **Hinzufügen**.
6. Geben Sie im Feld **Server** eine nicht existierende IP-Adresse an.



7. Geben Sie 80 in das Feld **Port** ein.
8. Fügen Sie den erstellten Monitor aus der Liste **Verfügbare Monitore** hinzu.
9. Erstellen Sie einen virtuellen Load Balancing-Server und geben Sie im Feld Name einen entsprechenden **Namen** an.
10. Um einen virtuellen Load Balancing-Server zu erstellen, erweitern Sie im Navigationsbereich **Load Balancing**, klicken Sie auf **Dienste** und dann auf **Hinzufügen**.
11. Geben Sie die IP-Adresse der Website im Feld IP-Adresse an.
12. Wählen Sie HTTP aus der Protokollliste aus.
13. Geben Sie 80 in das Feld Port ein.
14. Wählen Sie in NetScaler Version 9.0 und 10.0 auf der Registerkarte Dienste die Option Aktiv für den Dienst, den Sie erstellt haben, wie im folgenden Screenshot gezeigt. Diese Option ist in NetScaler Version 11.0 veraltet.



15. Klicken Sie auf die Registerkarte **Richtlinien**.
16. Binden Sie die von Ihnen erstellte Responder-Richtlinie an die HTTP Load Balancing-VIP-Adresse der Website.
17. Erstellen Sie einen sicheren virtuellen Load Balancing-Server mit der IP-Adresse der Website und dem Port 443.

Führen Sie die folgenden Befehle aus, um über die Befehlszeilenschnittstelle der Appliance eine Konfiguration zu erstellen, die dem vorherigen Verfahren ähnelt:


```
enable ns feature responder
add responder action http_to_https_actn redirect ""https://" + http.req
    .hostname.HTTP_URL_SAFE + http.REQ.URL.PATH_AND_QUERY.HTTP_URL_SAFE"
add responder policy http_to_https_pol HTTP.REQ.IS_VALID
    http_to_https_actn RESET
add lb monitor localhost_ping PING -LRTM ENABLED -destIP 127.0.0.1
add service Always_UP_service 1.2.3.4 HTTP 80 -gslb NONE -maxClient 0 -
    maxReq 0 -cip ENABLED dummy -usip NO -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP YES
bind lb monitor localhost_ping Always_UP_service
add lb vserver http_site.com HTTP 10.217.96.238 80 -persistenceType
    COOKIEINSERT -timeout 0 -cltTimeout 180
bind lb vserver http_site.com Always_UP_service
bind lb vserver http_site.com -policyName http_to_https_pol -priority 1
     -gotoPriorityExpression END
<!--NeedCopy-->
```

Hinweise:

- Der Status des virtuellen Load Balancing Redirect-Servers mit Port 80 muss AKTIV sein, damit die Umleitung funktioniert.
- Webbrowser leiten möglicherweise nicht korrekt um, wenn der virtuelle HTTPS-Server nicht aktiv ist.
- Dieses Umleitungs-Setup ermöglicht Situationen, in denen mehrere Domains an dieselbe IP-Adresse gebunden sind.
- Wenn der Client eine ungültige HTTP-Anforderung an den virtuellen Umleitungsserver sendet, sendet die Appliance einen RESET Meldungscode.

Problembehandlung

May 11, 2023

Wenn die Responder-Funktion nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf NetScaler-Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Problembehandlung

Optimale Ergebnisse erzielen Sie, wenn Sie die folgenden Ressourcen verwenden, um ein Problem mit dem integrierten Cache auf einer NetScaler-Appliance zu beheben:

- Die Datei ns.conf
- Die relevanten Trace-Dateien vom Client und der NetScaler-Appliance

Zusätzlich zu den oben genannten Ressourcen beschleunigen die folgenden Tools die Fehlerbehebung:

- Die iehttpheaders oder ein ähnliches Hilfsprogramm
- Die Wireshark-Anwendung, die auf die NetScaler-Trace-Dateien zugeschnitten ist

Behebung von Responder-Problemen

- **Problem**

  Die Responder-Funktion ist konfiguriert, aber die Responder-Aktion funktioniert nicht.

  Auflösung

  - Stellen Sie sicher, dass die Funktion aktiviert ist.
  - Überprüfen Sie die Trefferzähler aller Richtlinien, um festzustellen, ob die Zähler erhöht werden.
  - Stellen Sie sicher, dass die Richtlinien und Aktionen korrekt konfiguriert sind.
  - Stellen Sie sicher, dass die Maßnahmen und Richtlinien angemessen miteinander verknüpft sind.
  - Zeichnen Sie die Paket-Traces auf dem Client und der NetScaler-Appliance auf und analysieren Sie sie, um Hinweise auf das Problem zu erhalten.
  - Zeichnen Sie die IEHttpHeaters Paket-Traces auf dem Client auf und überprüfen Sie die HTTP-Anfragen und -Antworten, um Hinweise auf das Problem zu erhalten.

- **Problem**

  Sie müssen eine Wartungsseite erstellen.

  Auflösung

1. Konfigurieren Sie die Dienste und den virtuellen Server.
2. Konfigurieren Sie einen virtuellen Backup-Server mit einem daran gebundenen Dienst. Dadurch wird sichergestellt, dass der Status der Website immer als AKTIV angezeigt wird.
3. Konfigurieren Sie den primären virtuellen Server so, dass er den virtuellen Backup-Server als Backup verwendet.
4. Erstellen Sie eine Responder-Aktion mit einem geeigneten Ziel. Im Folgenden finden Sie ein Beispiel als Referenz:

   ```
   add responder action sorry_page respondwith q{ "HTTP/1.0 200 OK"+"\r\n\
   r\n"+ "<html><body>Sorry, this page is not available\</body>\</html>"+
   "\r\n"}
   ```


5. Erstellen Sie eine Responder-Richtlinie und binden Sie die Aktion daran.
6. Binden Sie die Responder-Richtlinie an den virtuellen Backup-Server.

Rewrite

July 4, 2023

> **Warnung:**
>
> Filterfunktionen, die klassische Richtlinien verwenden, sind veraltet und als Alternative empfiehlt Citrix Ihnen, die Rewrite- und Responder-Funktionen mit erweiterter Richtlinieninfrastruktur zu verwenden.

Rewrite bezieht sich auf das Neuschreiben einiger Informationen in den Anforderungen oder Antworten, die von der NetScaler-Appliance verarbeitet werden. Das Umschreiben kann dabei helfen, Zugriff auf den angeforderten Inhalt zu gewähren, ohne unnötige Details über die tatsächliche Konfiguration der Website preiszugeben. Einige Situationen, in denen die Rewritefunktion nützlich ist, sind folgende:

- Um die Sicherheit zu verbessern, kann der NetScaler alle `https://` den Antworttext in `http://links` neu schreiben.
- Bei der SSL-Offload-Bereitstellung müssen die unsicheren Links in der Antwort in sichere Verbindungen umgewandelt werden. Mit der Rewrite-Option können Sie alle `http://links` in `https://` neu schreiben, um sicherzustellen, dass die ausgehenden Antworten von NetScaler an den Client über die gesicherten Links verfügen.
- Wenn eine Website eine Fehlerseite anzeigen muss, können Sie anstelle der standardmäßigen 404-Fehlerseite eine benutzerdefinierte Fehlerseite anzeigen. Wenn Sie beispielsweise anstelle einer Fehlerseite die Homepage oder Sitemap der Website anzeigen, bleibt der Besucher auf der Website, anstatt sich von der Website zu entfernen.
- Wenn Sie eine neue Website starten möchten, aber die alte URL verwenden möchten, können Sie die Option Rewrite verwenden.
- Wenn ein Thema auf einer Website eine komplizierte URL hat, können Sie es mit einer einfachen, leicht zu merkenden URL (auch als “coole URL” bezeichnet) neu schreiben.
- Sie können den Standardseitennamen an die URL einer Website anhängen. Wenn die Standardseite der Website eines Unternehmens beispielsweise lautet `http://www.abc.com/index.php`, wenn der Benutzer “abc.com” in die Adressleiste des Browsers eingibt, können Sie die URL auf “abc.com/index.php” neu schreiben.

Wenn Sie die Rewritefunktion aktivieren, kann NetScaler die Header und den Hauptteil von HTTP-Anfragen und -Antworten ändern.

Um HTTP-Anfragen und -Antworten neu zu schreiben, können Sie protokollbewusste NetScaler-Richtlinienausdrücke in den von Ihnen konfigurierten Rewriterichtlinien verwenden. Die virtuellen Server, die die HTTP-Anfragen und -Antworten verwalten, müssen vom Typ
HTTP oder
SSL sein. Im HTTP-Verkehr können Sie die folgenden Aktionen ausführen:

- Ändern Sie die URL einer Anfrage
- Header hinzufügen, ändern oder löschen
- Fügen Sie eine bestimmte Zeichenfolge innerhalb des Textkörpers oder der Kopfzeilen hinzu, ersetzen oder löschen Sie sie.

Für ein Rewrite von TCP-Nutzdaten betrachten Sie die Nutzlast als einen rohen Byte-Stream. Jeder der virtuellen Server, die die TCP-Verbindungen verwalten, muss vom Typ TCP oder SSL_TCP sein. Der Begriff TCP-Rewrite bezieht sich auf das Rewrite von TCP-Nutzdaten, bei denen es sich nicht um HTTP-Daten handelt. Im TCP-Datenverkehr können Sie einen beliebigen Teil der TCP-Nutzlast hinzufügen, ändern oder löschen.

Beispiele zur Verwendung der Rewrite-Funktion finden Sie unter Beispiele für Rewrite-Aktionen und -richtlinien.

Vergleich zwischen Rewrite und Responder Optionen

Der Hauptunterschied zwischen der Rewrite-Funktion und der Responder-Funktion ist wie folgt:

Responder kann nicht für Antwort- oder serverbasierte Ausdrücke verwendet werden. Der Responder kann je nach Clientparametern nur für die folgenden Szenarien verwendet werden:

- Umleiten einer HTTP-Anfrage auf neue Websites oder Webseiten
- Reagieren mit einer benutzerdefinierten Antwort
- Löschen oder Zurücksetzen einer Verbindung auf Anforderungsebene

Wenn es eine Responder Policy gibt, prüft NetScaler die Anfrage des Clients, ergreift Maßnahmen gemäß den geltenden Richtlinien, sendet die Antwort an den Client und schließt die Verbindung mit dem Client.

Wenn es eine Rewriterichtlinie gibt, prüft NetScaler die Anforderung des Clients oder die Antwort vom Server, ergreift Maßnahmen gemäß den geltenden Richtlinien und leitet den Datenverkehr an den Client oder den Server weiter.

Im Allgemeinen wird empfohlen, einen Responder zu verwenden, wenn NetScaler eine Verbindung basierend auf einem Client oder einem anforderungsbasierten Parameter zurücksetzen oder löschen soll. Verwenden Sie den Responder, um den Datenverkehr umzuleiten oder mit be-

nutzerdefinierten Nachrichten zu antworten. Verwenden Sie Rewrite zum Bearbeiten von Daten auf HTTP-Anforderungen und -Antworten.

Wie das Rewrite funktioniert

Eine Rewriterichtlinie besteht aus einer Regel und einer Aktion. Die Regel bestimmt den Datenverkehr, auf den das Rewrite angewendet wird, und die Aktion bestimmt die vom NetScaler zu ergreifende Aktion. Sie können mehrere Rewriterichtlinien definieren. Geben Sie für jede Richtlinie den Bindepunkt und die Priorität an.

Ein Bindepunkt bezieht sich auf einen Punkt im Verkehrsfluss, an dem der NetScaler den Datenverkehr untersucht, um zu überprüfen, ob eine Rewriterichtlinie darauf angewendet werden kann. Sie können eine Richtlinie an einen bestimmten virtuellen Lastausgleich- oder Content Switching-Server binden oder die Richtlinie global machen, wenn Sie möchten, dass die Richtlinie auf den gesamten Datenverkehr angewendet wird, der vom NetScaler verarbeitet wird. Diese Richtlinien werden als globale Richtlinien bezeichnet.

Zusätzlich zu den benutzerdefinierten Richtlinien verfügt der NetScaler über einige Standardrichtlinien. Sie können eine Standardrichtlinie nicht ändern oder löschen.

Um die Richtlinien auszuwerten, befolgt NetScaler diese Reihenfolge:

- Globale Richtlinien
- An bestimmte virtuelle Server gebundene Richtlinien
- Standardrichtlinien

> **Hinweis:**
>
> NetScaler kann eine Rewriterichtlinie nur anwenden, wenn sie an einen Punkt gebunden ist.

NetScaler implementiert die Funktion zum Rewrite in den folgenden Schritten:

- Die NetScaler-Appliance sucht nach globalen Richtlinien und sucht dann an einzelnen Bindepunkten nach Richtlinien.
- Wenn mehrere Richtlinien an einen Bindepunkt gebunden sind, wertet NetScaler die Richtlinien in der Reihenfolge ihrer Priorität aus. Die Richtlinie mit der höchsten Priorität wird zuerst bewertet. Wenn die Richtlinie nach der Bewertung jeder Richtlinie auf TRUE ausgewertet wird, wird die Aktion hinzugefügt, die mit der Richtlinie verknüpft ist, die die zugehörige Aktion ausgeführt wird. Eine Übereinstimmung tritt auf, wenn die in der Richtlinienregel angegebenen Merkmale den Merkmalen der zu bewertenden Anforderung oder Antwort entsprechen.
- Für jede Richtlinie können Sie zusätzlich zu der Aktion die Richtlinie angeben, die ausgewertet werden muss, nachdem die aktuelle Richtlinie ausgewertet wurde. Diese Richtlinie wird als “Gehe zum Ausdruck” bezeichnet. Wenn für jede Richtlinie ein Gehe zu Ausdruck (gotoPriori-

tyExpr) angegeben ist, wertet NetScaler die Richtlinie “Gehe zu Ausdruck” aus. Es ignoriert die Richtlinie mit der nächsthöchsten Priorität.

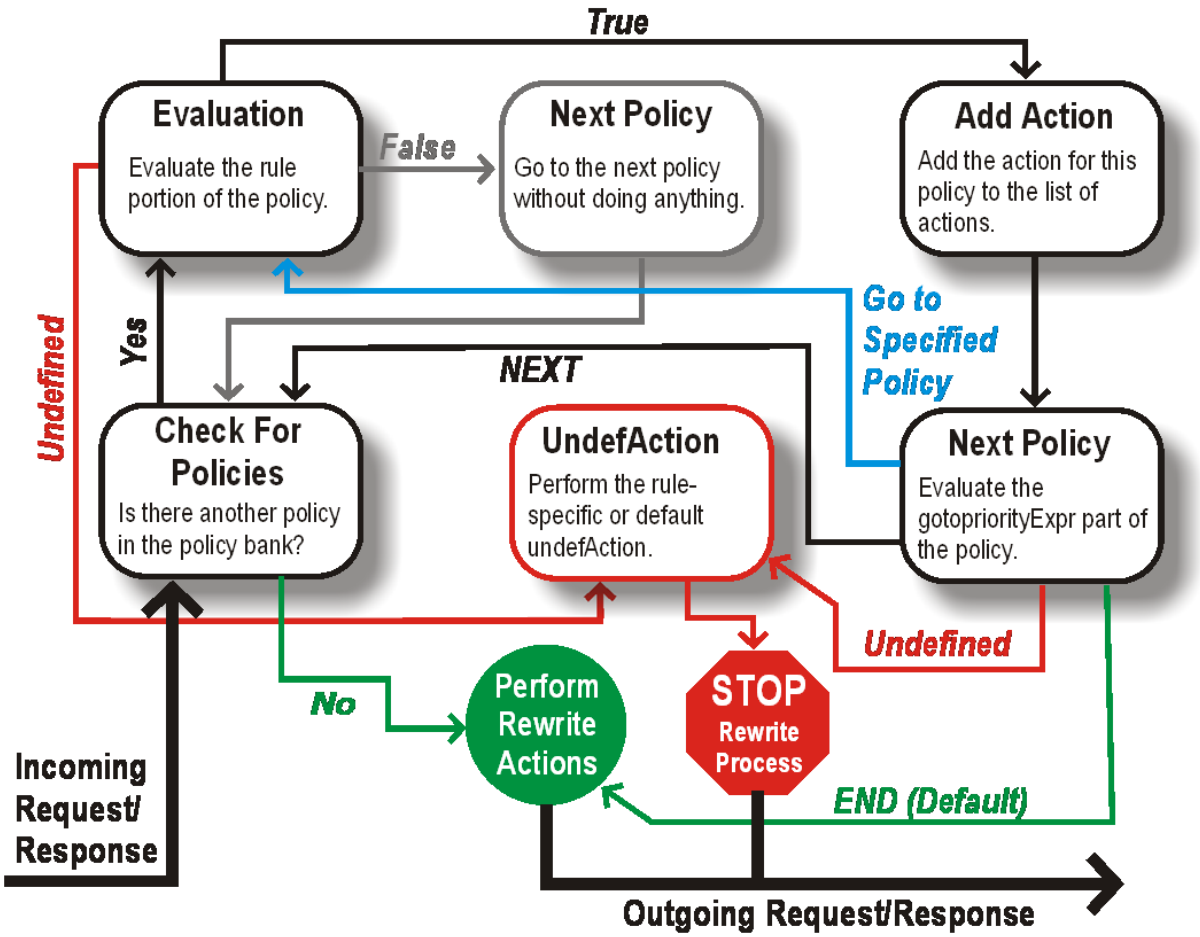
Sie können die Priorität der Richtlinie angeben, um die Richtlinie “Gehe zu Ausdruck” anzugeben. Sie können den Namen der Richtlinie nicht verwenden. Wenn Sie möchten, dass NetScaler nach der Auswertung einer bestimmten Richtlinie keine anderen Richtlinien mehr auswertet, können Sie den Gehe zu Ausdruck auf “ENDE” setzen.

- Nachdem alle Richtlinien ausgewertet wurden oder wenn eine Richtlinie den Gehe zu Ausdruck als END festgelegt hat, beginnt NetScaler die Aktionen entsprechend der Liste der Aktionen auszuführen.

Weitere Informationen zum Konfigurieren von Rewriterichtlinien finden Sie unter Konfigurieren einer Rewriterichtlinie und zum Binden von Rewriterichtlinien finden Sie unter Binden einer Rewriterichtlinie.

Die folgende Abbildung zeigt, wie NetScaler eine Anforderung oder Antwort verarbeitet, wenn das Rewrite-Feature verwendet wird.

Abbildung 1. Der Rewrite-Prozess



Politische Bewertung

Die Richtlinie mit der höchsten Priorität wird zuerst bewertet. NetScaler stoppt die Auswertung von Rewriterichtlinien nicht, wenn eine Übereinstimmung gefunden wird. Es wertet alle auf dem NetScaler konfigurierten Rewriterichtlinien aus.

- Wenn eine Richtlinie auf TRUE ausgewertet wird, folgt der NetScaler dem folgenden Verfahren:
  - Wenn für die Richtlinie Gehe zu Ausdruck auf END festgelegt ist, stoppt NetScaler die Auswertung aller anderen Richtlinien und beginnt mit dem Rewrite.
  - Der gotoPriorityExpression kann auf “NEXT”, “END”, eine ganze Zahl oder “INVOCATION_LIST” gesetzt werden. Der Wert bestimmt die Richtlinie mit der nächsten Priorität. Die folgende Tabelle zeigt die von NetScaler für jeden Wert des Ausdrucks ergriffene Aktion.

Wert des Ausdrucks	Aktion
NEXT	Die Richtlinie mit der nächsten Priorität wird ausgewertet.
END	Die Bewertung der Richtlinien stoppt.
<an integer>	Die Richtlinie mit der angegebenen Priorität wird ausgewertet.
INVOCATION_LIST	Gehe zu NEXT oder END wird basierend auf dem Ergebnis der Aufrufliste angewendet.

- Wenn eine Richtlinie als FALSE ausgewertet wird, setzt der NetScaler die Auswertung in der Reihenfolge ihrer Priorität fort.
- Wenn eine Richtlinie zu UNDEFINED ausgewertet wird (aufgrund eines Fehlers nicht für den empfangenen Datenverkehr ausgewertet werden kann), führt der NetScaler die Aktion aus, die der UNDEFINIERTEN Bedingung zugewiesen ist (als UnDEFaction bezeichnet), und stoppt die weitere Auswertung von Richtlinien.

Der NetScaler beginnt mit dem eigentlichen Umschreiben erst, nachdem die Auswertung abgeschlossen ist. Es bezieht sich auf die Liste der Aktionen, die durch Richtlinien identifiziert wurden, die auf TRUE ausgewertet werden, und beginnt mit dem Umschreiben. Nachdem alle Aktionen in der Liste implementiert wurden, leitet der NetScaler den Datenverkehr nach Bedarf weiter.

> **Hinweis:**
>
> Stellen Sie sicher, dass die Richtlinien keine widersprüchlichen oder überlappenden Aktionen für denselben Teil des HTTP-Headers oder Textkörpers oder der TCP-Nutzlast angeben. Wenn ein solcher Konflikt auftritt, stößt der NetScaler auf eine undefinierte Situation und bricht das

> Rewrite ab.

Rewrite-Aktionen

Geben Sie auf der NetScaler-Appliance die auszuführenden Aktionen an, z. B. das Hinzufügen, Ersetzen oder Löschen von Text im Hauptteil oder das Hinzufügen, Ändern oder Löschen von Headern oder Änderungen an der TCP-Nutzlast als Rewriteaktionen. Weitere Informationen zu Rewrite-Aktionen finden Sie unter Konfigurieren einer Rewrite-Aktion.

In der folgenden Tabelle werden die Schritte beschrieben, die NetScaler ausführen kann, wenn eine Richtlinie TRUE bewertet.

Aktion	Ergebnis
Einfügen	Die für die Richtlinie angegebene Rewriteaktion wird ausgeführt.
NOREWRITE	Die Anfrage oder Antwort wird nicht umgeschrieben. NetScaler leitet den Datenverkehr weiter, ohne einen Teil der Nachricht neu zu schreiben.
RESET	Die Verbindung wird auf TCP-Ebene abgebrochen.
DROP	Die Nachricht wird verworfen.

> **Hinweis**:
>
> Für jede Richtlinie können Sie die Unteraktion (Aktion, die ergriffen werden muss, wenn die Richtlinie zu UNDEFINED ausgewertet wird) als NOREWRITE, RESET oder DROP konfigurieren.

Führen Sie die folgenden Schritte aus, um die Funktion “
Rewrite” zu verwenden:

- Aktivieren Sie die Funktion auf dem NetScaler.
- Definieren Sie Rewrite-Aktionen.
- Definieren Sie Richtlinien für das Rewrite.
- Binden Sie die Richtlinien an einen Bindepunkt, um eine Richtlinie in Kraft zu setzen.

Rewrite aktivieren

Aktivieren Sie die Funktion zum Rewrite auf der NetScaler-Appliance, wenn Sie die HTTP- oder TCP-Anforderungen oder -Antworten neu schreiben möchten. Wenn das Feature aktiviert ist, führt

NetScaler Rewrite-Aktionen gemäß den angegebenen Richtlinien durch. Weitere Informationen finden Sie unter Funktionsweise von Rewrite.

So aktivieren Sie das Rewrite-Feature mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Rewritefunktion zu aktivieren und die Konfiguration zu überprüfen:

- enable ns-Funktion REWRITE
- show ns feature

Beispiel:

```
> enable ns feature REWRITE
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 .
 .
 .
 1)     Rewrite                         REWRITE             ON
 .
 .
 1)     NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

So aktivieren Sie die Rewrite-Funktion über die GUI

1. Klicken Sie im Navigationsbereich auf **System**und dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter Modi und Funktionen auf **Grundfunktionen konfigurieren**.
3. Aktivieren Sie im Dialogfeld **Grundfunktionen konfigurieren** das Kontrollkästchen Rewrite, und klicken Sie dann auf **OK**.
4. Klicken Sie im Dialogfeld **Feature(s) aktivieren/deaktivieren** auf **Ja**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das ausgewählte Feature aktiviert wurde.

Konfigurieren einer Rewrite-Aktion

> **Warnung**
>
> Die Pattern-Funktion in einer Rewrite-Aktion ist ab NetScaler 12.0 Build 56.20 veraltet, und Citrix empfiehlt Ihnen alternativ, den Aktionsparameter Rewrite Search zu verwenden.

Eine Rewrite-Aktion zeigt Änderungen an, die an einer Anfrage oder Antwort vorgenommen wurden, bevor sie an einen Server oder Client gesendet wurden.

Ausdrücke definieren Folgendes:

- Schreiben Sie den Aktionstyp neu.
- Ort der Rewrite-Aktion.
- Schreiben Sie den Aktionskonfiguration neu.

Beispielsweise verwendet eine DELETE-Aktion nur einen Zielausdruck. Eine REPLACE-Aktion verwendet einen Zielausdruck und einen Ausdruck, um den Ersetzungstext zu konfigurieren.

Nachdem Sie die Rewrite-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen konfigurieren, es sei denn, eine integrierte Rewrite-Aktion reicht aus. Alle integrierten Aktionen haben Namen, die mit der Zeichenfolge ns_cvpn beginnen, gefolgt von einer Reihe von Buchstaben und Unterstrichen. Integrierte Aktionen führen nützliche und komplexe Aufgaben aus, z. B. das Dekodieren von Teilen einer clientlosen VPN-Anfrage oder Antwort oder das Ändern von JavaScript- oder XML-Daten. Die integrierten Aktionen können angezeigt, aktiviert und deaktiviert werden, können jedoch nicht geändert oder gelöscht werden.

> Hinweis:
>
> Aktionstypen, die nur für HTTP-Rewrite verwendet werden können, werden in der Spalte **Rewrite-Aktionstyp** identifiziert.

Weitere Informationen finden Sie unter **Typenparameter**.

Erstellen Sie eine Rewrite-Aktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Rewrite-Aktion zu erstellen und die Konfiguration zu überprüfen:

- `add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-search <expression>] [refineSearch <expression>] [-comment<string>]`
- `show rewrite action <name>`

Weitere Informationen finden Sie in der Tabelle Rewrite-Aktionstypen und deren Argumente .

Die Rewrite-Funktion verfügt über die folgenden integrierten Aktionen:

- NOREWRITE - Sendet die Anfrage oder Antwort an den Benutzer, ohne sie neu zu schreiben.
- RESET - Setzt die Verbindung zurück und benachrichtigt den Browser des Benutzers, damit der Benutzer die Anfrage erneut senden kann.
- DROP - Löscht die Verbindung, ohne eine Antwort an den Benutzer zu senden.

Einer der folgenden Flow-Typen ist implizit mit jeder Aktion verknüpft:

- Request - Aktion gilt für die Anfrage.
- Response - Aktion gilt für die Antwort.
- Neutral - Aktion gilt sowohl für Anfragen als auch für Antworten.

Name

Name für die benutzerdefinierte Rewrite-Aktion. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Hash (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann geändert werden, nachdem die Rewriterichtlinie hinzugefügt wurde.

Typ-Parameter

Der **Type-Parameter** zeigt den Typ der benutzerdefinierten Rewrite-Aktion an.

Im Folgenden sind die Werte des **Type-Parameters** aufgeführt:

- `REPLACE <target> <string_builder_expr>`. Ersetzt die Zielzeichenfolge durch den String-Builder-Ausdruck.

Beispiel:

```
> add rewrite action replace_http_act replace http.res.body(100) '"
   new_replaced_data"'
Done
> sh rewrite action replace_http_act
Name: replace_http_act
Operation: replace
Target:http.res.body(100)
Value:"new_replaced_data"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_ALL <target> <string_builder_expr1> -(search)<s>` - Ersetzt in der von `<target>`angegebenen Anfrage oder Antwort alle Vorkommen der Zeichenfolge definiert von `<pattern_to_search>` durch durch durch durch `<string_builder_expr>`. Sie können die Suchoption verwenden, um die zu ersetzenden Zeichenketten zu finden.

Beispiel:


```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY
   (100000)" ""https://""-search "patset("pat_list_2")" -refineSearch "
   EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done

> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:"https://"
Search: patset("pat_list_2")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_HTTP_RES <string_builder_expr>`. Ersetzt die vollständige HTTP-Antwort durch die durch den String-Builder-Ausdruck definierte Zeichenfolge.

Beispiel:

```
> add rewrite action replace_http_res_act replace_http_res '"HTTP/1.1
   200 OK\r\n\r\nSending from ADC"'
 Done
> sh rewrite action replace_http_res_act
Name: replace_http_res_act
Operation: replace_http_res
Target:"HTTP/1.1 200 OK
Sending from ADC"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


- REPLACE_SIP_RES <target>. Ersetzt die vollständige SIP-Antwort durch die durch <target> angegebene Zeichenfolge.

Beispiel:

```
> add rewrite action replace_sip_res_act replace_sip_res '"HTTP/1.1 200 OK\r\n\r\nSending from ADC"'
Done
> sh rewrite action replace_sip_res_act
Name: replace_sip_res_act
Operation: replace_sip_res
Target:"HTTP/1.1 200 OK
Sending from ADC"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_HTTP_HEADER <header_string> <contents_string_builder_expr>. Fügt den von angegebenen HTTP-Header header_string und den von angegebenen Header-Inhalt ein contents_string_builder_expr.

Beispiel:

```
> add rewrite action ins_cip_header insert_http_header "CIP" "CLIENT.IP.SRC"
Done
> sh rewrite action ins_cip_header
Name: ins_cip_header
Operation: insert_http_header
Target:CIP
Value:CLIENT.IP.SRC
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_HTTP_HEADER <target>. Löscht den HTTP-Header, der mit <target> angegeben wurde

Beispiel:


```
> add rewrite action del_true_client_ip_header delete_http_header "True-Client-IP"
Done
> sh rewrite action del_true_client_ip_header
Name: del_true_client_ip_header
Operation: delete_http_header
Target:True-Client-IP
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_HTTP_HEADER <target>. Ersetzt den Header-Namen aller Vorkommen des durch <target> angegebenen HTTP-Headers durch einen beschädigten Namen, so dass er vom Empfänger nicht erkannt wird Beispiel: MY_HEADER wird in MHEY_ADER geändert.

Beispiel:

```
> add rewrite action corrupt_content_length_hdr corrupt_http_header "Content-Length"
Done
> sh rewrite action corrupt_content_length_hdr
Name: corrupt_content_length_hdr
Operation: corrupt_http_header
Target:Content-Length
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE <string_builder_expr1> <string_builder_expr1>. Findet die in <string_builder_expr1> angegebene Zeichenfolge und fügt die Zeichenfolge in <string_builder_expr2> davor ein.

```
> add rewrite action insert_before_ex_act insert_before http.res.body(100) '"Add this string in the starting"'
Done
> sh rewrite action insert_before_ex_act
Name: insert_before_ex_act
Operation: insert_before
Target:http.res.body(100)
```



```
Value:"Add this string in the starting"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2>. Sucht in der von angegebenen Anfrage oder Antwort nach allen Vorkommen der Zeichenfolge <target>, die in angegeben ist und fügt die in angegebene Zeichenfolge ein davor. Sie können die Suchoption verwenden, um die Zeichenketten zu finden.

Beispiel:

```
> add policy patset pat
 Done
> bind policy patset pat abcd
 Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + "refineSearch_testing"' -search patset("
    pat") -refineSearch extend(10,10)
 Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + "refineSearch_testing"
Search: patset("pat")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER <string_builder_expr1> <string_builder_expr2>. Fügt die von angegebene Zeichenfolge string_builder_expr2 nach der Zeichenfolge ein string_builder_expr1.

Beispiel:

```
> add rewrite action insert_after_act insert_after http.req.body(100) '
    "add this string after 100 bytes"'
```



```
Done
> sh rewrite action insert_after_act
Name: insert_after_act
Operation: insert_after
Target:http.req.body(100)
Value:"add this string after 100 bytes"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER_ALL <target> <string_builder_expr1> -(search)<string_builder_expr2>. Sucht in der von <target>angegebenen Anfrage oder Antwort nach allen Vorkommen der von angegebenen Zeichenfolge <string_builder_expr2> und fügt die von angegebene Zeichenfolge <string_builder_expr1> danach ein. Sie können die Suchfunktion verwenden, um die Zeichenfolgen zu finden.

Beispiel:

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
   (100) '"refineSearch_testing"' -search text("abc") -refineSearch
   extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE <target>. Löscht die durch target angegebene Zeichenfolge.

Beispiel:

```
> add rewrite action delete_ex_act delete http.req.header("HDR")
Done
```



```
> sh rewrite action delete_ex_act
Name: delete_ex_act
Operation: delete
Target:http.req.header("HDR")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_ALL <target> -(search)<string_builder_expr>. In der von <target >angegebenen Anforderung oder Antwort sucht und löscht alle Vorkommen der durch angegebenen Zeichenfolge <string_builder_expr>. Sie können die Suchfunktion verwenden, um die Zeichenfolgen zu finden.

Beispiel:

```
>add rewrite action refineSearch_act_4 delete_all "HTTP.RES.BODY(50000)
    " -search text("Windows Desktops") -refineSearch "EXTEND(40,40).
    REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s`\*`<\\/AppData>#)"
Done
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s
    `\*`</AppData>#)
Search: text("Windows Desktops")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DIAMETER_HEADER_FIELD <target> <field value>. Ändern Sie in der Anforderung oder den Antworten das durch <target> angegebene Kopfzeilenfeld. Verwenden Sie Diameter.req.flags.SET(<flag>) oder Diameter.req.flags.UNSET<flag> wie stringbuilderexpression, um Flags zu setzen oder aufzuheben.

Beispiel:

```
> add rewrite action replace_diameter_field_ex_act
    replace_diameter_header_field diameter.req.flags diameter.req.flags.
```



```
    set(PROXIABLE)
Done
> sh rewrite action replace_diameter_field_ex_act
Name: replace_diameter_field_ex_act
Operation: replace_diameter_header_field
Target:diameter.req.flags
Value:diameter.req.flags.set(PROXIABLE)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DNS_HEADER_FIELD <target>. In der Anforderung oder Antwort ändert das durch <target> angegebene Header-Feld.

Beispiel:

```
> add rewrite action replace_dns_hdr_act replace_dns_header_field dns.
    req.header.flags.set(AA)
Done
> sh rewrite action replace_dns_hdr_act
Name: replace_dns_hdr_act
Operation: replace_dns_header_field
Target:dns.req.header.flags.set(AA)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_DNS_ANSWER_SECTION <target>. Ersetzen Sie den DNS-Antwortabschnitt in der Antwort. Dies gilt nur für A- und AAAA-Datensätze. Verwenden Sie die Ausdrücke DNS.NEW_RRSET_A und NS.NEW_RRSET_AAAA, um den neuen Antwortabschnitt zu konfigurieren.

Beispiel:

```
> add rewrite action replace_dns_ans_act replace_dns_answer_section
    DNS.NEW_RRSET_A("1.1.1.1", 10)
Done
> sh rewrite action replace_dns_ans_act
Name: replace_dns_ans_act
Operation: replace_dns_answer_section
Target:DNS.NEW_RRSET_A("1.1.1.1", 10)
```



```
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `CLIENTLESS_VPN_DECODE<target>`. Dekodiert das vom Ziel angegebene Muster im clientlosen VPN-Format.

Beispiel:

```
> add rewrite action cvpn_decode_act_1 clientless_vpn_decode http.req.
   body(100)
Done
> sh rewrite action cvpn_decode_act_1
Name: cvpn_decode_act_1
Operation: clientless_vpn_decode
Target:http.req.body(100)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `CLIENTLESS_VPN_DECODE_ALL<target>-search<expression>`. Dekodiert ALLE durch den Suchparameter angegebenen Muster im clientlosen VPN-Format.

Beispiel:

```
> add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
   -search text("abcd")
Done
> sh rewrite action act1
Name: act1
Operation: clientless_vpn_decode_all
Target:http.req.body(100)
Search: text("abcd")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


- CLIENTLESS_VPN_ENCODE<target>. Codiert das von target angegebene Muster im clientlosen VPN-Format.

Beispiel:

```
> add rewrite action cvpn_encode_act_1 clientless_vpn_encode http.req.body(100)
Done
> sh rewrite action cvpn_encode_act_1
Name: cvpn_encode_act_1
Operation: clientless_vpn_encode
Target:http.req.body(100)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CLIENTLESS_VPN_ENCODE_ALL<target>-search<expression>. Kodiert ALLE Muster angegebenen Suchparameter im clientlosen VPN-Format.

Beispiel:

```
> add rewrite action act2 clientless_vpn_encode_all http.req.body(100) -search text("abcd")
Done
> sh rewrite action act2
Name: act1
Operation: clientless_vpn_encode_all
Target:http.req.body(100)
Search: text("abcd")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_SIP_HEADER<target>. Ersetzt den Header-Namen aller Vorkommen des durch <target> angegebenen SIP-Headers durch einen beschädigten Namen, damit der Empfänger ihn nicht erkennt.

Beispiel:

```
> add rewrite action corrupt_sip_hdr_act corrupt_sip_header SIP_HDR
```



```
Done
> sh rewrite action corrupt_sip_hdr_act
Name: corrupt_sip_hdr_act
Operation: corrupt_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_SIP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Fügt den durch <header_string_builder_expr> angegebenen SIP-Header und Header-Inhalt ein, der durch <contents_string_builder_expr> angegeben ist.

Beispiel:

```
> add rewrite action insert_sip_hdr_act insert_sip_header SIP_HDR '"
   inserting_sip_header"'
 Done
>sh rewrite action insert_sip_hdr_act
Name: insert_sip_hdr_act
Operation: insert_sip_header
Target:SIP_HDR
Value:"inserting_sip_header"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_SIP_HEADER<target>. Löscht den SIP-Header, der von <target> angegeben wurde

Beispiel:

```
> add rewrite action delete_sip_hdr delete_sip_header  SIP_HDR
Done
> sh rewrite action delete_sip_hdr
Name: delete_sip_hdr
Operation: delete_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
```



```
Done

<!--NeedCopy-->
```

Target-Parameter

Der Target-Parameter Ist ein Ausdruck, der angibt, welcher Teil der Anforderung oder Antwort neu geschrieben werden soll.

StringBuilderExpr

Der StringBuilderExpr Ist ein Ausdruck, der den Inhalt angibt, der an der angegebenen Stelle in die Anforderung oder Antwort eingefügt werden soll. Dieser Ausdruck ersetzt eine angegebene Zeichenfolge.

Beispiel 1. Einfügen eines HTTP-Headers mit der Client-IP:

```
> add rewrite action insertact INSERT_HTTP_HEADER "client-IP" CLIENT.IP
    .SRC
Done
> show rewrite action insertact
Name: insertact
Operation: insert_http_header
Target:Client-IP
Value:CLIENT.IP.SRC
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Beispiel 2. Strings in einer TCP-Nutzlast ersetzen (TCP Rewrite):

```
> add rewrite action client_tcp_payload_replace_all REPLACE_ALL
  'client.tcp.payload(1000)' '"new-string"' -search text("old-string")
Done
> show rewrite action client_tcp_payload_replace_all
Name: client_tcp_payload_replace_all
Operation: replace_all
Target:client.tcp.payload(1000)
Value:"new-string"
Search: text("old-string")
```



```
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Suchen Sie einen Teil der Anfrage oder Antwort zum Neuschreiben

Die Suchfunktion hilft dabei, alle Instanzen des erforderlichen Musters in der Anfrage oder Antwort zu finden.

Die Suchfunktion muss in den folgenden Aktionstypen verwendet werden:

- INSERT_BEFORE_ALL
- INSERT_AFTER_ALL
- REPLACE_ALL
- DELETE_ALL
- CLIENTLESS_VPN_ENCODE_ALL
- CLIENTLESS_VPN_DECODE_ALL

Die Suchfunktion kann nicht mit den folgenden Aktionstypen verwendet werden:

- INSERT_HTTP_HEADER
- INSERT_BEFORE
- INSERT_AFTER
- REPLACE
- Löschen
- DELETE_HTTP_HEADER
- CORRUPT_HTTP_HEADER
- REPLACE_HTTP_RES
- CLIENTLESS_VPN_ENCODE
- CLIENTLESS_VPN_DECODE
- INSERT_SIP_HEADER
- DELETE_SIP_HEADER
- CORRUPT_SIP_HEADER
- REPLACE_DIAMETER_HEADER_FIELD
- REPLACE_DNS_ANSWER_SECTION
- REPLACE_DNS_HEADER_FIELD
- REPLACE_SIP_RES

Die folgenden Suchtypen werden unterstützt:

- Text - eine literale Zeichenfolge
  Beispiel: -search text (“hello”)
- Regulärer Ausdruck - Muster, das verwendet wird, um mehrere Strings in der Anfrage oder Antwort abzugleichen
  Beispiel: -search regex(re~^hello*~)
- XPATH - Ein XPATH-Ausdruck zur Suche nach XML.
  Beispiel: -search xpath(xp%/a/b%)
- JSON - Ein XPATH-Ausdruck zur Suche nach JSON.
  Beispiel: -search xpath_json(xp%/a/b%)
  HTML - Ein XPATH-Ausdruck zur Suche nach HTML
  Beispiel: -search xpath_html(xp%/html/body%)
  Patset - Dies durchsucht alle Muster, die an die Patset-Entität gebunden sind.
  Beispiel: -search patset(“patset1”)
- Datset - Dies durchsucht alle Muster, die an die Datset-Entität gebunden sind.
  Beispiel Suchdatensatz (“dataset1”)
- AVP - AVP-Nummer, die verwendet wird, um mehrere AVPs in einer Durchmesser-/Radius-Nachricht abzugleichen
  Beispiel: -search avp(999)

Verfeinern Sie die Suchergebnisse

Sie können die Funktion “Suche eingrenzen” verwenden, um die zusätzlichen Kriterien für die Verfeinerung der Suchergebnisse anzugeben. Die Funktion “Suche eingrenzen” kann nur verwendet werden, wenn die Suchfunktion verwendet wird.
Der Suchparameter “Verfeinern” beginnt immer mit der Operation “extend (m, n)”, wobei ‘m’ einige Bytes links vom Suchergebnis angibt und ‘n’ mehrere Bytes rechts neben dem Suchergebnis angibt, um den ausgewählten Bereich zu erweitern.

Wenn die konfigurierte Rewrite-Aktion lautet:

```
> add rewrite action test_refine_search replace_all http.res.body(10) '
    " testing_refine_search" ' -search text("abc") -refineSearch extend
    (1,1)
And the HTTP response body is abcxxxx456.

<!--NeedCopy-->
```

Dann findet der Suchparameter das Muster “abc” und da der RefineSearch-Parameter auch so konfiguriert ist, dass er ein zusätzliches 1 Byte links und ein zusätzliches Byte rechts vom übereinstimmenden Muster überprüft. Der resultierende ersetzte Text ist: abcx. Die Ausgabe dieser Aktion ist also `testing_refine_searchxxx456`.

Beispiel 1: Verwenden der Suchfunktion Verfeinern im Aktionstyp INSERT_BEFORE_ALL.

```
> add policy patset pat
Done
> bind policy patset pat abcd
Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + "refineSearch_testing"' -search patset("
    pat") -refineSearch extend(10,10)
Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + "refineSearch_testing"
Search: patset("pat")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Beispiel 2: Verwenden der Suchfunktion “Suche eingrenzen” im Aktionstyp INSERT_AFTER_ALL.

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
    (100) '"refineSearch_testing"' -search text("abc") -refineSearch
    extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Beispiel 3: Verwenden der Suchfunktion Verfeinern im Aktionstyp REPLACE_ALL.


```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 "www.abc.com"
Done
> bind policy patset pat_list_2 "www.def.com"
Done
> add rewrite action refineSearch_act_31 replace_all "HTTP.RES.BODY
    (100000)" ""https://"" -search "patset("pat_list_2")" -refineSearch
    "EXTEND(7,0).REGEX_SELECT(re#http://#)"
Done
> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:"https://"
Search: patset("pat_list_2")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Beispiel 4: Verwenden der Suchfunktion “Suche eingrenzen” im Aktionstyp DELETE_ALL.

```
>add rewrite action refineSearch_act_4 delete_all "HTTP.RES.BODY(50000)
    " -search text("Windows Desktops") -refineSearch "EXTEND(40,40).
    REGEX_SELECT(re#\s*<AppData>.\*\s\*<\\/AppData>#)"
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s*<AppData>.\*\s\*</
    AppData>#)
Search: text("Windows Desktops")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Beispiel 5: Verwenden der Funktion “Suche eingrenzen” im Aktionstyp CLIENTLESS_VPN_ENCODE_ALL.

”’

```
add rewrite action act2 clientless_vpn_encode_all http.req.body(100) -search text(“abcd”)
Done
sh rewrite action act2
Name: act1
Operation: clientless_vpn_encode_all
Target:http.req.body(100)
Search: text(“abcd”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
```

”’

Beispiel 6: Verwenden der Funktion “Suche eingrenzen” im Aktionstyp CLIENTLESS_VPN_DECODE_ALL.

```
> add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
   -search text("abcd")
Done
> sh rewrite action act1
Name: act1
Operation: clientless_vpn_decode_all
Target:http.req.body(100)
Search: text("abcd")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Ändern Sie eine vorhandene Rewrite-Aktion über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine vorhandene Rewrite-Aktion zu ändern und die Konfiguration zu überprüfen:

- `set rewrite action <name> [-target <expression>] [-stringBuilderExpr <expression>] [-search <expression>] [-refineSearch <expression>] [-comment <string>]`

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die geänderte Konfiguration zu überprüfen

- `show rewrite action <name>`

Beispiel:

```
> set rewrite action insertact -target "Client-IP"
 Done
> show rewrite action insertact

Name: insertact
Operation: insert_http_header   Target:Client-IP
Value:CLIENT.IP.SRC
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Entfernen Sie eine Rewrite-Aktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Rewrite-Aktion zu entfernen:

```
rm rewrite action <name>
```

Beispiel:

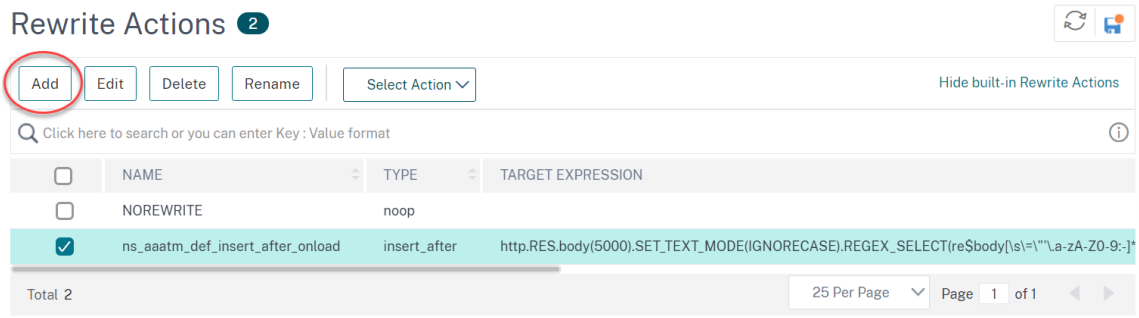
```
> rm rewrite action insertact
Done

<!--NeedCopy-->
```

Konfigurieren Sie eine Rewrite-Aktion mit dem Konfigurationsdienstprogramm

1. Gehen Sie zu **AppExpert > Rewrite > Actions**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf **Erstellen** oder **auf OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Aktion erfolgreich konfiguriert wurde.
4. Wiederholen Sie die Schritte 2 bis 4, um beliebig viele Rewriteaktionen zu erstellen oder zu ändern.

5. Klicken Sie auf **Schließen**.



Hinzufügen eines Ausdrucks mithilfe des Dialogfelds Ausdruck hinzufügen

1. Klicken Sie im Dialogfeld **Rewrite-Aktion erstellen** oder **Rewrite-Aktion konfigurieren** unter dem Textbereich für das einzugebende Typargument auf **Hinzufügen**.
2. Wählen Sie im Dialogfeld **Ausdruck hinzufügen** im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.
   - HTTP. Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
   - SYS. Die geschützten Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - CLIENT. Der Computer, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.

Wenn Sie Ihre Auswahl treffen, werden im Listenfeld ganz rechts die entsprechenden Begriffe für den nächsten Teil Ihres Ausdrucks aufgeführt.

1. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahl hängt davon ab, welche Wahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, wird im Hilfefenster unterhalb des Fensters “Ausdruck konstruieren” (das leer war) eine Hilfe zur Beschreibung des Zwecks und der Verwendung des gerade gewählten Begriffs angezeigt.
2. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.
   Weitere Informationen zur Sprache der PI-Ausdrücke und zum Erstellen von Ausdrücken für Responder-Richtlinien finden Sie unter “Richtlinien und Ausdrücke. “

Wenn Sie die Wirkung einer Rewrite-Aktion testen möchten, wenn sie auf HTTP-Beispieldaten verwendet wird, können Sie den Rewrite Expression Evaluator verwenden.

TCP-Nutzlasten neu schreiben

Zielausdrücke in Aktionen für TCP-Rewrite müssen mit einem der folgenden Ausdruckspräfixe beginnen:

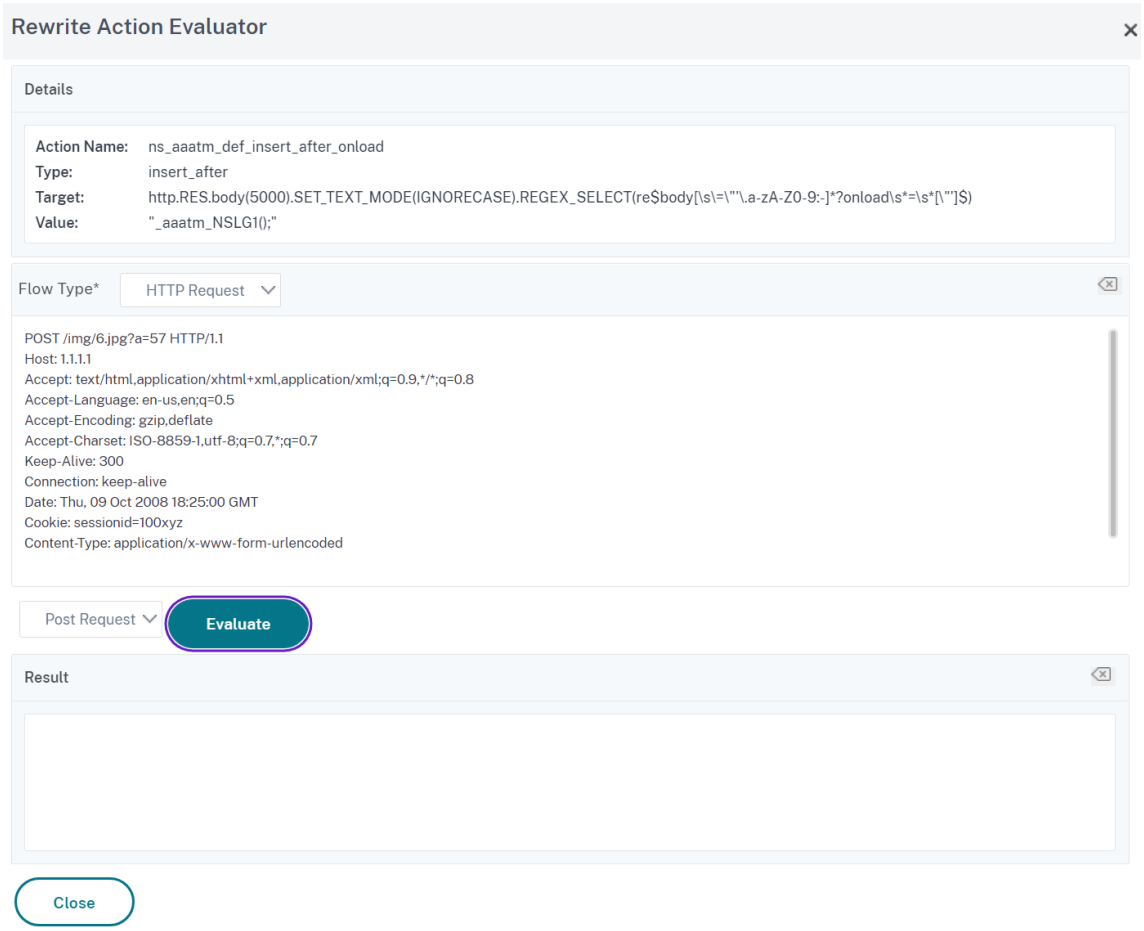
- **CLIENT.TCP.PAYLOAD.** Zum Umschreiben von TCP-Nutzlasten in Clientanfragen. Zum Beispiel CLIENT.TCP.PAYLOAD(10000).AFTER_STR(“string1”).
- **SERVER.TCP.PAYLOAD.** Zum Umschreiben von TCP-Nutzlasten in Serverantworten. Zum Beispiel SERVER.TCP.PAYLOAD(1000).B64DECODE.BETWEEN(“string1”,”string2”).

Bewerten Sie eine Rewrite-Aktion im Dialogfeld Rewrite Expression Evaluator

1. Wählen Sie im Detailbereich **Rewrite-Aktionen** die Rewrite-Aktion aus, die Sie auswerten möchten, und klicken Sie dann auf **Auswerten**.
2. Geben Sie im Dialogfeld Rewrite Expression Evaluator Werte für die folgenden Parameter an. (Ein Sternchen gibt einen erforderlichen Parameter an.)

   Rewrite Action (Rewrite Action) — Wenn die neu zu bewertende Aktion noch nicht ausgewählt ist, wählen Sie sie aus der Dropdownliste aus. Nachdem Sie eine Aktion “Rewrite” ausgewählt haben, werden im Abschnitt Details die Details der ausgewählten Aktion “Rewrite” angezeigt.
   Neu — Wählen Sie Neu aus, um das Dialogfeld “Rewrite-Aktion erstellen” zu öffnen und eine Neuschreibaktion zu erstellen.
   Ändern — Wählen Sie Ändern aus, um das Dialogfeld “Rewrite-Aktion konfigurieren” zu öffnen und die ausgewählte Neuschreibaktion zu ändern.
   Flow-Typ — Gibt an, ob die ausgewählte Rewrite-Aktion mit HTTP-Anforderungsdaten oder HTTP-Antwortdaten getestet werden soll. Der Standardwert ist Request. Wenn Sie mit Antwortdaten testen möchten, wählen Sie Antwort aus.
   HTTP-Anforderung/Antwortdaten* — Dient zur Bereitstellung der HTTP-Daten, die der Rewrite Action Evaluator zum Testen verwendet wird. Sie können die Daten direkt in das Fenster einfügen oder auf Sample klicken, um einige Beispiel-HTTP-Header einzufügen.
   Zeilenende anzeigen — Gibt an, ob End-of-Line-Zeichen (\ n) im Unix-Stil am Ende jeder Zeile von HTTP-Beispieldaten angezeigt werden sollen.
   Beispiel — Fügt Beispiel-HTTP-Daten in das Fenster “HTTP-Request/Response Data” ein. Sie können entweder GET- oder POST-Daten wählen.
   Durchsuchen — Öffnet ein lokales Suchfenster, in dem Sie eine Datei mit Beispiel-HTTP-Daten von einem lokalen oder Netzwerkspeicherort auswählen können.
   Clear—Löscht die aktuellen Beispiel-HTTP-Daten aus dem Fenster “HTTP-Request/Response Data”.

3. Klicken Sie auf Bewerten. Der **Rewrite Expression Evaluator** wertet die Auswirkung der Aktion “Rewrite” auf die ausgewählten Beispieldaten aus und zeigt die Ergebnisse an, die durch die ausgewählte Aktion **Rewrite** im Fenster **Ergebnisse** geändert wurden. Hinzufügungen und Löschungen werden wie in der Legende in der unteren linken Ecke des Dialogfelds angegeben hervorgehoben.
4. Evaluieren Sie Rewrite-Aktionen weiter, bis Sie festgestellt haben, dass alle Ihre Aktionen die gewünschte Wirkung haben.
    - Sie können die ausgewählte Rewrite-Aktion ändern und die geänderte Version testen, indem Sie auf **Ändern** klicken, um das Dialogfeld **Rewrite-Aktion konfigurieren** zu öffnen, Ihre Änderungen vorzunehmen und zu speichern, und dann erneut auf Auswerten klicken.
    - Sie können eine andere Rewrite-Aktion mit denselben Anforderungs- oder Antwortdaten auswerten, indem Sie sie in der Dropdownliste **Aktion neu schreiben** auswählen und dann erneut auf **Auswerten** klicken.
5. Klicken Sie auf **Schließen**, um das Auswertungsprogramm **Rewrite Expression** zu schließen und zum Bereich **Rewrite-Aktionen** zurückzukehren.
6. Um eine Rewrite-Aktion zu löschen, wählen Sie die Rewrite-Aktion aus, die Sie löschen möchten, klicken Sie dann auf **Entfernen** und bestätigen Sie bei Aufforderung Ihre Auswahl, indem Sie auf **OK** klicken.



Rewriterichtlinie konfigurieren

Nachdem Sie alle erforderlichen Rewrite-Aktionen erstellt haben, müssen Sie mindestens eine Rewriterichtlinie erstellen, um die Anforderungen auszuwählen, die die NetScaler-Appliance neu schreiben soll.

Eine Rewriterichtlinie besteht aus einer Regel, die selbst aus einem oder mehreren Ausdrücken besteht, und einer zugehörigen Aktion, die ausgeführt wird, wenn eine Anforderung oder Antwort mit der Regel übereinstimmt. Richtlinienregeln für die Auswertung von HTTP-Anfragen und -Antworten können auf fast jedem Teil einer Anfrage oder Antwort basieren.

Obwohl Sie TCP-Rewrite-Aktionen nicht verwenden können, um andere Daten als die TCP-Nutzlast neu zu schreiben, können Sie die Richtlinienregeln für TCP-Rewriterichtlinien auf die Informationen in der Transportschicht und die Schichten unter der Transportschicht stützen.

Wenn eine konfigurierte Regel mit einer Anforderung oder Antwort übereinstimmt, wird die entsprechende Richtlinie ausgelöst und die damit verbundene Aktion wird ausgeführt.

> **Hinweis:**
>
> Sie können entweder die Befehlszeilenschnittstelle oder die GUI verwenden, um Rewriterichtlinien zu erstellen und zu konfigurieren. Benutzer, die mit der Befehlszeilenschnittstelle und der Ausdruckssprache für NetScaler Policy nicht genau vertraut sind, werden die Verwendung der GUI normalerweise viel einfacher finden.

So fügen Sie eine neue Rewriterichtlinie mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine neue Rewriterichtlinie hinzuzufügen und die Konfiguration zu überprüfen:

- `<add rewrite policy <name> <expression> <action> [<undefaction>]`
- `<show rewrite policy <name>`

Beispiel 1. HTTP-Inhalt umschreiben

```
> add rewrite policyNew "HTTP.RES.IS_VALID" insertact NOREWRITE
 Done
> show rewrite policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertact
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

Beispiel 2. Rewrite einer TCP-Nutzlast (TCP-Rewrite):

```
> add rewrite policy client_tcp_payload_policy CLIENT.IP.SRC.EQ
   (172.168.12.232) client_tcp_payload_replace_all
 Done
> show rewrite policy client_tcp_payload_policy
        Name: client_tcp_payload_policy
        Rule: CLIENT.IP.SRC.EQ(172.168.12.232)
        RewriteAction: client_tcp_payload_replace_all
        UndefAction: Use Global
        LogAction: Use Global
        Hits: 0
        Undef Hits: 0

 Done
>
<!--NeedCopy-->
```


So ändern Sie eine vorhandene Rewriterichtlinie über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine vorhandene Rewriterichtlinie zu ändern und die Konfiguration zu überprüfen:

- `<set rewrite policy <name> -rule <expression> -action <action> [<undefaction>]`
- `<show rewrite policy <name>`

Beispiel:

```
> set rewrite policyNew -rule "HTTP.RES.IS_VALID" -action insertaction
 Done

> show rewrite policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertaction
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

 Done
<!--NeedCopy-->
```

So entfernen Sie eine Rewriterichtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Rewriterichtlinie zu entfernen:

```
rm rewrite policy <name>
```

Beispiel:

```
> rm rewrite policyNew
Done
<!--NeedCopy-->
```

So konfigurieren Sie eine Rewriterichtlinie über die GUI

1. Gehen Sie zu **AppExpert > Rewrite > Policies**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Richtlinie zu erstellen, klicken Sie auf Hinzufügen.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf Öffnen.

3. Klicken Sie auf **Erstellen** oder **auf OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.
4. Wiederholen Sie die Schritte 2 bis 4, um beliebig viele Rewriteaktionen zu erstellen oder zu ändern.
5. Klicken Sie auf **Schließen**. Um eine Neuschreibrichtlinie zu löschen, wählen Sie die zu löschende Rewriterichtlinie aus, klicken Sie auf **Entfernen**, und bestätigen Sie, wenn Sie dazu aufgefordert werden, Ihre Auswahl durch Klicken auf **OK**zu bestätigen.

Binden einer Rewriterichtlinie

Nachdem Sie eine Rewriterichtlinie erstellt haben, müssen Sie sie binden, um sie in Kraft zu setzen. Sie können Ihre Richtlinie an Global binden, wenn Sie sie auf den gesamten Datenverkehr anwenden möchten, der durch Ihren NetScaler fließt, oder Sie können Ihre Richtlinie an einen bestimmten virtuellen Server oder Bindepunkt binden, um nur diesen virtuellen Server zu leiten oder den eingehenden Datenverkehr des Punkts an diese Richtlinie zu binden. Wenn eine eingehende Anforderung mit einer Rewriterichtlinie übereinstimmt, wird die mit dieser Richtlinie verknüpfte Aktion ausgeführt.

Rewriterichtlinien für die Auswertung von HTTP-Anfragen und -Antworten können an virtuelle Server vom Typ HTTP oder SSL gebunden werden, oder sie können an die Bindungspunkte REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE und RES_DEFAULT gebunden werden. Rewriterichtlinien für das Rewrite von TCP können nur an virtuelle Server vom Typ TCP oder SSL_TCP oder an die Bindungspunkte OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE und
OTHERTCP_RES_DEFAULT gebunden werden.

> **Hinweis:**
>
> Der Begriff OTHERTCP wird im Kontext der NetScaler-Appliance verwendet, um sich auf alle TCP- oder SSL_TCP-Anforderungen und -Antworten zu beziehen, die Sie unabhängig von den Protokollen, die die TCP-Pakete kapseln, als rohen Byte-Stream behandeln möchten.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf jede positive Ganzzahl festlegen.

Im NetScaler-Betriebssystem arbeiten Richtlinienprioritäten in umgekehrter Reihenfolge - je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit Prioritäten von 10, 100 und 1000 haben, wird der Richtlinie zuerst eine Priorität von 10 zugewiesen, dann wird der Richtlinie eine Priorität von 100 zugewiesen, und schließlich hat die Richtlinie eine Reihenfolge von 1000 zugewiesen.

Im Gegensatz zu den meisten anderen Funktionen des NetScaler-Betriebssystems bewertet und implementiert die Rewrite-Funktion weiterhin Richtlinien, nachdem eine Anforderung mit einer

Richtlinie übereinstimmt. Die Auswirkung einer bestimmten Aktionsrichtlinie auf eine Anfrage oder Antwort ist jedoch häufig unterschiedlich, je nachdem, ob sie vor oder nach einer anderen Aktion durchgeführt wird. Priorität ist wichtig, um die von Ihnen beabsichtigten Ergebnisse zu erzielen.

Sie können sich viel Raum lassen, um andere Richtlinien in beliebiger Reihenfolge hinzuzufügen, und sie dennoch so einstellen, dass sie in der gewünschten Reihenfolge bewertet werden, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen den einzelnen Richtlinien festlegen, wenn Sie sie binden. In diesem Fall können Sie jederzeit weitere Richtlinien hinzufügen, ohne die Priorität einer bestehenden Richtlinie neu zuweisen zu müssen.

Wenn Sie eine Rewriterichtlinie binden, haben Sie auch die Möglichkeit, der Richtlinie einen GoTo-Ausdruck (gotoPriorityExpression) zuzuweisen. Ein Goto Ausdruck kann eine beliebige positive Ganzzahl sein, die der Priorität entspricht, die einer anderen Richtlinie zugewiesen wurde, die eine höhere Priorität als die Richtlinie hat, die den GoTo-Ausdruck enthält. Wenn Sie einer Richtlinie einen GoTo-Ausdruck zuweisen und eine Anforderung oder Antwort mit der Richtlinie übereinstimmt, wird NetScaler sofort zu der Richtlinie wechseln, deren Priorität dem Goto Ausdruck entspricht. Es überspringt alle Richtlinien mit Prioritätsnummern, die niedriger als die der aktuellen Richtlinie sind, aber höher als die Prioritätsnummer des Gehe zu Ausdrucks sind, und bewertet diese Richtlinien nicht.

So binden Sie eine Rewriterichtlinie über die Befehlszeile global

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Rewriterichtlinie global zu binden und die Konfiguration zu überprüfen:

- `bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show rewrite global`

Beispiel:

```
>bind rewrite global policyNew 10
 Done

> show rewrite global
1)      Global bindpoint: RES_DEFAULT
        Number of bound policies: 1

2)      Global bindpoint: REQ_OVERRIDE
        Number of bound policies: 1

 Done
<!--NeedCopy-->
```

So binden Sie die Rewriterichtlinie über die Befehlszeile an einen bestimmten virtuellen Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Rewriterichtlinie an einen bestimmten virtuellen Server zu binden und die Konfiguration zu überprüfen:

- `bind lb vserver <name>@ (<serviceName>@ [-weight <positive_integer>])| <serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>)] )`
- `show lb vserver <name>`

Beispiel:

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 50
 Done
>
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+226 ms)
        Time since last state change: 28 days, 01:57:26.350
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:50
2)      Policy : cf-pol Priority:1      Inherited
 Done
<!--NeedCopy-->
```

So binden Sie eine Rewriterichtlinie über die GUI an einen Bindepunkt

1. Navigieren Sie zu **AppExpert** >**Rewrite** > **Richtlinien**.
2. Wählen Sie im Detailbereich die Rewriterichtlinie aus, die Sie global binden möchten, und klicken Sie dann auf **Richtlinien-Manager**.
3. Führen Sie im Dialogfeld **Rewriterichtlinienmanager** im Menü **Punkte binden** einen der folgenden Schritte aus:

a) Wenn Sie Bindungen für HTTP-Rewriterichtlinien konfigurieren möchten, klicken Sie auf **HTTP**und dann entweder auf **Anforderung** oder **Antwort**, je nachdem, ob Sie anforderungsbasierte Rewriterichtlinien oder reaktionsbasierte Rewriterichtlinien konfigurieren möchten.
b) Wenn Sie Bindungen für TCP-Rewriterichtlinien konfigurieren möchten, klicken Sie auf **TCP**, und klicken Sie dann entweder auf **Client** oder **Server**, je nachdem, ob Sie clientseitige TCP-Rewriterichtlinien oder serverseitige TCP-Rewriterichtlinien konfigurieren möchten.

4. Klicken Sie auf den Bindepunkt, an den Sie die Rewriterichtlinie binden möchten. Im Dialogfeld **Rewriterichtlinien-Manager** werden alle Rewriterichtlinien angezeigt, die an den ausgewählten Bindepunkt gebunden sind.
5. Klicken Sie auf **Richtlinie** einfügen, um eine neue Zeile einzufügen und eine Dropdownliste mit allen verfügbaren, ungebundenen Rewriterichtlinien anzuzeigen.
6. Klicken Sie auf die Richtlinie, die Sie an den Bindepunkt binden möchten. Die Richtlinie wird in die Liste der an den Bindepunkt gebundenen Rewriterichtlinien eingefügt.
7. In der Spalte **Priorität** können Sie die Priorität auf eine beliebige positive Ganzzahl ändern. Weitere Informationen zu diesem Parameter finden Sie unter Priorität in “Parameter zum Binden einer Rewriterichtlinie”.
8. Wenn Sie Richtlinien überspringen und direkt zu einer bestimmten Richtlinie wechseln möchten, wenn die aktuelle Richtlinie übereinstimmt, ändern Sie den Wert in der Spalte Gehe zu Ausdruck so, dass er der Priorität der nächsten anzuwendenden Richtlinie entspricht. Weitere Informationen zu diesem Parameter finden Sie unter gotoPriorityExpression in “Parameter zum Binden einer Rewriterichtlinie”.
9. Um eine Richtlinie zu ändern, klicken Sie auf die Richtlinie und dann auf **Richtlinie ändern**.
10. Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie und dann auf **Richtlinie aufheben**.
11. Um eine Aktion zu ändern, klicken Sie in der Spalte Aktion auf die Aktion, die Sie ändern möchten, und klicken Sie dann auf **Aktion ändern**.
12. Um eine Aufrufbeschriftung zu ändern, klicken Sie in der Spalte **Aufrufen** auf das Aufruflabel, das Sie ändern möchten, und klicken Sie dann auf **Aufrufbeschriftung ändern**.
13. Um die Prioritäten aller Richtlinien neu zu generieren, die an den gerade konfigurierten Bindepunkt gebunden sind, klicken Sie auf **Prioritäten neu generieren**. Die Richtlinien behalten ihre bestehenden Prioritäten im Vergleich zu den anderen Richtlinien bei, aber die Prioritäten werden in ein Vielfaches von 10 umnummeriert.
14. Klicken Sie auf **Änderungen übernehmen**.
15. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

So binden Sie eine Rewriterichtlinie über die GUI an einen bestimmten virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.

2. Wählen Sie in der Liste der virtuellen Server im Detailbereich den virtuellen Server aus, an den Sie die Rewriterichtlinie binden möchten, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing)** die Registerkarte **Richtlinien** aus. Alle auf Ihrem NetScaler konfigurierten Richtlinien werden in der Liste angezeigt.
4. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie an diesen virtuellen Server binden möchten.
5. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

Konfigurieren von Richtlinienbeschriftungen

Wenn Sie eine komplexere Richtlinienstruktur aufbauen möchten, als von einzelnen Richtlinien unterstützt wird, können Sie Richtlinienbeschriftungen erstellen und diese dann wie Richtlinien binden. Ein Policy Label ist ein benutzerdefinierter Punkt, an den Richtlinien gebunden sind. Wenn ein Policy Label aufgerufen wird, werden alle an sie gebundenen Richtlinien in der Reihenfolge der von Ihnen konfigurierten Priorität ausgewertet. Ein Policy Label kann eine oder mehrere Richtlinien enthalten, von denen jeder ein eigenes Ergebnis zugewiesen werden kann. Eine Übereinstimmung mit einer Policy Label im Richtlinienlabel kann dazu führen, dass mit der nächsten Policy Label fortgefahren wird, ein anderes Richtlinienlabel oder eine entsprechende Ressource aufgerufen wird oder die Richtlinienbewertung sofort beendet wird und die Kontrolle an die Policy Label zurückgegeben wird, die das Richtlinienlabel aufgerufen hat.

Eine Richtlinienbezeichnung zum Rewrite besteht aus einem Namen, einem Transformationsnamen, der den in der Richtlinienbezeichnung enthaltenen Richtlinientyp beschreibt, und einer Liste von Richtlinien, die an die Richtlinienbezeichnung gebunden sind. Jede Richtlinie, die an die Policy Label gebunden ist, enthält alle unter Neuschreibenrichtlinie konfigurierenbeschriebenen Elemente.

Hinweis: Sie können entweder die Befehlszeilenschnittstelle oder die GUI verwenden, um Rewriterichtlinienbeschriftungen zu erstellen und zu konfigurieren. Benutzer, die mit der Befehlszeilenschnittstelle und der NetScaler Policy Infrastructure (PI) -Sprache nicht genau vertraut sind, finden die Verwendung der GUI normalerweise viel einfacher.

So konfigurieren Sie eine Rewriterichtlinienbezeichnung über die Befehlszeile

Um ein Rewriterichtlinienlabel hinzuzufügen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add rewrite policylabel <labelName> <transform>
```

Um beispielsweise eine Rewriterichtlinienbezeichnung namens PollabelHttpResponses hinzuzufügen, um alle Richtlinien zu gruppieren, die für HTTP-Antworten funktionieren, geben Sie Folgendes ein:


```
add rewrite policy label polLabelHTTPResponses http_res
```

Geben Sie an der **NetScaler-Eingabeaufforderung** den folgenden Befehl ein, um ein vorhandenes Rewriterichtlinienlabel zu ändern:

```
set rewrite policy <name> <transform>
```

> **Hinweis:**
>
> Der Befehl set rewrite policy verwendet dieselben Optionen wie der Befehl add rewrite policy.

Um ein Rewriterichtlinienlabel zu entfernen, geben Sie an der **NetScaler-Eingabeaufforderung** den folgenden Befehl ein:

```
rm rewrite policy<name>
```

Um beispielsweise eine Rewriterichtlinienbezeichnung namens PollabelHttpResponses zu entfernen, geben Sie Folgendes ein:

```
rm rewrite policy polLabelHTTPResponses
```

So konfigurieren Sie eine Rewriterichtlinienbezeichnung über die GUI

1. Navigieren Sie zu **AppExpert** > **Rewrite** > **Policy Labels**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um ein Policy Label zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um ein vorhandenes Richtlinienlabel zu ändern, wählen Sie die Policy Label aus, und klicken Sie dann auf **Öffnen**.
3. Fügen Sie Richtlinien hinzu oder entfernen Sie Richtlinien aus der Liste, die an das Policy Label gebunden ist.
   - Um der Liste eine Richtlinie hinzuzufügen, klicken Sie auf **Richtlinie einfügen**, und wählen Sie eine Richtlinie aus der Dropdownliste aus. Sie können eine Richtlinie erstellen und zur Liste hinzufügen, indem Sie in der Liste Neue Richtlinie wählen und den Anweisungen unter Konfigurieren einer Rewriterichtlinie folgen.
   - Um eine Richtlinie aus der Liste zu entfernen, wählen Sie diese Richtlinie aus, und klicken Sie dann auf Richtlinie aufheben.
4. Ändern Sie die Priorität jeder Richtlinie, indem Sie die Zahl in der Spalte Priorität bearbeiten. Sie können Richtlinien auch automatisch neu nummerieren, indem Sie auf Prioritäten neu generieren klicken.
5. Klicken Sie auf **Erstellen** oder **OK**, und klicken Sie dann auf **Schließen**.
   Um ein Policy Label zu entfernen, wählen Sie es aus und klicken dann auf **Entfernen**. Um ein Policy Label umzubenennen, wählen Sie es aus und klicken Sie dann auf **Umbenennen**. Bearbeiten Sie den Namen der Richtlinie, und klicken Sie dann auf **OK**, um Ihre Änderungen zu speichern.

Verhalten des Content-Length-Headers bei einer Streaming-Rewrite-Aktion

June 19, 2023

Der Content-Length-Header ist eine der Möglichkeiten, die Länge der Nachricht (in Byte) in einer HTTP-Anfrage oder -Antwort anzugeben. Neben dem Content-Length-Header können Sie die Länge der Nachricht auch auf eine der folgenden Arten angeben:

- Blockierte Kodierung
- FIN-Kündigung

In einem Streaming-Prozess sendet der NetScaler nach der Verarbeitung der Rewrite-Aktion kontinuierlich Daten. Da die Daten kontinuierlich gesendet werden und nicht vom NetScaler gespeichert werden, ist die tatsächliche Länge der Nachricht, die an den Client gesendet würde, nicht bekannt. Daher kann der korrekte Wert des Content-Length-Headers in der Antwort nicht erwähnt werden.

Um den Streaming-Prozess zu unterstützen, konvertiert die Rewrite-Funktion von NetScaler die Art und Weise, wie die Länge der Nachricht angegeben wird, vom Content-Length-Header in die FIN-Terminierung. Im Rahmen der Konvertierung beschädigt der NetScaler den Content-Length-Header, indem er die ersten vier Zeichen des Headernamens neu anordnet.

In HTTP wird vom Client erwartet, dass er Header ignoriert, die er nicht versteht. Der Client versteht also den beschädigten Content-Length-Headernamen nicht und ignoriert daher den Header. Um die Leistung des NetScaler zu verbessern, wird der Header beschädigt statt gelöscht. Wenn Sie den Headernamen beschädigen, anstatt ihn zu löschen, wird eine Neuberechnung der Prüfsumme vermieden, da die Prüfsumme nicht geändert wird, wenn dieselben Bytes in einer anderen Reihenfolge sind.

Stellen Sie sich zum Beispiel die folgende HTTP-Anfrage vor:

```
1 GET / HTTP/1.1
2 Accept: application/x-ms-application, image/jpeg, application/xaml+xml,
      image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-
     excel, application/vnd.ms-powerpoint, application/msword, /
3 Accept-Language: en-GB
4 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
     Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
      3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; CMDTDF; MS-RTC
     LM 8)
5 Accept-Encoding: gzip, deflate
6 Host: test.example.net
7 Connection: Keep-Alive
8 <!--NeedCopy-->
```


In einem funktionierenden Szenario lautet die Antwort zwischen NetScaler und dem Backend-Server auf diese HTTP-Anfrage wie folgt:

```
HTTP/1.1 200 OK
Content-Length: 10967
Connection: close
var SERVER_URL = 'https\x3a\x2f\x2ftest.example.net\x2f';
var WEB_SERVER_HOST = 'test.example.net';
<!--NeedCopy-->
```

Die Antwort, die der Client von NetScaler in einem nicht funktionierenden Szenario erhält, lautet jedoch wie folgt. Der `Content-Length`-Header wird umbenannt in `ntcoent-Length`.

```
HTTP/1.1 200 OK
ntCoent-Length: 10967
nnCoection: close
var SERVER_URL = 'https\x3a\x2f\x2ftest.example.net\x2f';
var WEB_SERVER_HOST = 'test.example.net';
<!--NeedCopy-->
```

Im Allgemeinen unterstützen die Client-Anwendungen alle drei Transaktionsarten: Content-Length-Header, Chunked-Codierung und FIN-Termination. Die Konvertierung vom Content-Length-Header zur FIN-Termination darf also keine Probleme verursachen. Wenn die Anwendung jedoch aufgrund dieser Änderung nicht funktioniert, müssen Sie den Streaming-Prozess deaktivieren.

So deaktivieren Sie den Streaming-Prozess in einer Rewrite-Richtlinie

Sie können den Streaming-Prozess in einer Rewrite-Richtlinie auf eine der folgenden Arten deaktivieren:

1. Fügen Sie eine Nicht-Streaming-Aktion hinzu, die mit einer Rewrite-Richtlinie verknüpft ist und an eine höhere Priorität gebunden ist. Die Aktion muss so sein, dass sie die Reaktion nicht verändert.

   Beispiel:

   ```
   add rewrite action non_stream_act replace_all HTTP.RES.BODY(1000000)
   HTTP.RES.FULL_HEADER -search text("pattern_which_will_not_match_in_body
   ")
   ```

   Der Wert des Hauptteils in dieser Rewrite-Aktion muss höher sein als der Wert, auf dem die aktuelle Streaming-Aktion ausgeführt wird.

2. Verwenden Sie statt der Streaming-Konfiguration die Nicht-Streaming-Konfiguration.

> **Hinweis:**
>
> Der Übergang von der Streaming-Verarbeitung zur Verarbeitung ohne Streaming kann sich auf die Leistung des NetScaler auswirken.

Eine Streaming-Konfiguration kann beispielsweise wie folgt in eine Nicht-Streaming-Konfiguration konvertiert werden:

Streaming-Konfiguration:

```
add rewrite action rw_act_1 replace_all HTTP.RES.BODY(1000) ""http"" -search text("http")

add policy patset pat_list
bind policy patset pat_list abcd
bind policy patset pat_list defg

add rewrite action rw_act_2 replace_all HTTP.RES.BODY(1000) ""replaced_data"" -search patset("pat_list")
<!--NeedCopy-->
```

Konfiguration ohne Streaming:

```
add rewrite action rw_act_1 replace_all HTTP.RES.BODY(1000) ""http"" -search regex(re/http/)

add rewrite action rw_act_1 replace_all HTTP.RES.BODY(1000) ""http"" -search regex(re/abcd|defg/)
<!--NeedCopy-->
```

Beispiele für Rewrite-Aktionen und -richtlinien

May 11, 2023

Die Beispiele in diesem Abschnitt zeigen, wie Rewrite konfiguriert wird, um verschiedene nützliche Aufgaben auszuführen. Die Beispiele finden im Serverraum von Example Manufacturing Inc. statt, einem mittelständischen Fertigungsunternehmen, das seine Website nutzt, um einen erheblichen Teil seines Vertriebs, seiner Lieferungen und seines Kundensupports zu verwalten.

Example Manufacturing hat zwei Domains: example.com für seine Website und E-Mails an Kunden und example.net für sein Intranet. Kunden verwenden die Beispielwebsite, um Bestellungen aufzugeben, Angebote anzufordern, nach Produkten zu suchen und den Kundendienst und den technischen Support zu kontaktieren.

Als wichtiger Teil der Umsatzquelle von Example muss die Website schnell reagieren und die Kundendaten vertraulich behandeln. Example verfügt daher über mehrere Webserver und verwendet NetScaler-Appliances, um die Auslastung der Website auszugleichen und den Datenverkehr zu und von den Webservern zu verwalten.

Die Beispiel-Systemadministratoren verwenden die Rewrite-Funktionen, um die folgenden Aufgaben auszuführen:

Beispiel 1: Löschen Sie alte X-Forwarded-For- und Client-IP-Header

Example Inc. entfernt alte X-Forwarded-For- und Client-IP-HTTP-Header aus eingehenden Anfragen.

Beispiel 2: Hinzufügen eines lokalen Client-IP-Headers

Example Inc. fügt eingehenden Anfragen einen neuen, lokalen Client-IP-Header hinzu.

Beispiel 3: Sichere und unsichere Verbindungen taggen

Example Inc. kennzeichnet eingehende Anfragen mit einem Header, der angibt, ob es sich bei der Verbindung um eine sichere Verbindung handelt.

Beispiel 4: Maskieren des HTTP-Servertyps

Example Inc. modifiziert den HTTP-Server: -Header, sodass nicht autorisierte Benutzer und bösartiger Code diesen Header nicht verwenden können, um die verwendete HTTP-Serversoftware zu ermitteln.

Beispiel 5: Umleiten einer externe URL zu einer internen URL

Example Inc. verbirgt Informationen über die tatsächlichen Namen seiner Webserver und die Konfiguration seines Serverraums vor Benutzern, um die URLs auf seiner Website kürzer und leichter zu merken zu machen und die Sicherheit auf seiner Website zu verbessern.

Beispiel 6: Migrieren der Apache Rewrite Modul-Regeln

Example Inc. verlagerte seine Apache-Rewrite-Regeln auf eine NetScaler-Appliance und übersetzte die auf Apache Perl basierende Skriptsyntax in die NetScaler-Rewrite-Regelsyntax.

Beispiel 7: Umleitung von Marketing-Keywords

Die Marketingabteilung von Example Inc. richtet vereinfachte URLs für bestimmte vordefinierte Stichwortsuchen auf der Website des Unternehmens ein.

Beispiel 8: Abfragen an den abgefragten Server weiterleiten.

Example Inc. leitet bestimmte Abfrageanfragen an den entsprechenden Server weiter.

Beispiel 9: Homepage-Umleitung

Example Inc. hat kürzlich einen kleineren Konkurrenten übernommen und leitet nun Anfragen an die Homepage des übernommenen Unternehmens auf eine Seite auf seiner eigenen Website weiter.

Beispiel 10: Richtlinienbasierte RSA-Verschlüsselung

Example Inc. verschlüsselt vordefinierte und benutzerdefinierte HTTP-Header- oder Textinhalte mithilfe eines öffentlichen PEM-RSA-Schlüssels.

Für jede dieser Aufgaben müssen die Systemadministratoren Aktionen und Richtlinien neu schreiben und sie an einen gültigen Bindungspunkt auf dem NetScaler binden.

Beispiel 1: Löschen alter X-Forwarded-For- und Client-IP-Header

May 11, 2023

Example Inc. möchte alte X-Forwarded-For- und Client-IP-HTTP-Header aus eingehenden Anfragen entfernen, sodass die einzigen X-Forwarded-For-Header, die angezeigt werden, die vom lokalen Server hinzugefügt wurden. Diese Konfiguration kann über die NetScaler-Befehlszeile oder das Konfigurationsprogramm vorgenommen werden. Der Systemadministrator von Example Inc. ist ein Netzwerkingenieur der alten Schule und zieht es vor, wenn möglich, eine CLI zu verwenden, möchte aber sichergehen, dass er die Schnittstelle des Konfigurationsprogramms versteht, damit er neuen Systemadministratoren im Team zeigen kann, wie sie verwendet wird.

Die folgenden Beispiele zeigen, wie jede Konfiguration sowohl mit der CLI als auch mit dem Konfigurationsprogramm durchgeführt wird. Die Prozeduren werden unter der Annahme abgekürzt, dass Benutzer bereits die Grundlagen zum Erstellen von Umschreibaktionen, Erstellen von Umschreibrichtlinien und Bindungsrichtlinien kennen.

- Ausführlichere Informationen zum Erstellen von Rewrite-Aktionen finden Sie unter Konfigurieren einer Rewrite-Aktion.
- Ausführlichere Informationen zum Erstellen von Rewrite-Richtlinien finden Sie unter Konfigurieren einer Rewrite-Richtlinie.
- Ausführlichere Informationen zum Binden von Rewrite-Richtlinien finden Sie unter Binden einer Rewrite-Richtlinie.

So löschen Sie alte X-Forwarded und Client-IP-Header aus einer Anforderung mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

```
add rewrite action act_del_xfor delete_http_header x-forwarded-for
add rewrite action act_del_cip delete_http_header client-ip
add rewrite policy pol_check_xfor 'HTTP.REQ.HEADER("x-forwarded-for").
    EXISTS' act_del_xfor
add rewrite policy pol_check_cip 'HTTP.REQ.HEADER("client-ip").EXISTS'
    act_del_cip
bind rewrite global pol_check_xfor 100 200
```



```
6 bind rewrite global pol_check_cip 200 300
7 <!--NeedCopy-->
```

So löschen Sie alte X-Forwarded- und Client-IP-Header aus einer Anfrage mithilfe des Konfigurationsprogramms

Erstellen Sie im Dialogfeld „Rewrite-Aktion erstellen“ zwei Rewrite-Aktionen mit den folgenden Beschreibungen.

Name	Typ	Argument (e)
act_del_xfor	delete_http_header	x-weitergeleitete für
act_del_cip	delete_http_header	Client-IP

Erstellen Sie im Dialogfeld „Rewrite-Richtlinie erstellen“ zwei Rewrite-Richtlinien mit den folgenden Beschreibungen.

Name	Ausdruck	Aktion
pol_check_xfor	‘HTTP.REQ.HEADER („x-forwarded-for“) .EXISTS’	act_del_xfor
pol_check_cip	‘HTTP.REQ.HEADER („Client-IP“) .EXISTS’	act_del_cip

Binden Sie beide Richtlinien an globale Richtlinien, indem Sie die unten angegebenen Prioritäten und goto-Ausdruckswerte zuweisen.

Name	Priorität	Gehe zu Expression
pol_check_xfor	100	200
pol_check_cip	200	300

Alle alten X-Forwarded-For- und Client-IP-HTTP-Header werden jetzt aus eingehenden Anfragen gelöscht.

Beispiel 2: Hinzufügen eines lokalen Client-IP-Headers

August 19, 2021

Example Inc. möchte eingehenden Anforderungen einen lokalen Client-IP-HTTP-Header hinzufügen. Dieses Beispiel enthält zwei leicht unterschiedliche Versionen derselben Grundaufgabe.

So fügen Sie mit der Befehlszeilenschnittstelle einen lokalen Client-IP-Header hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

```
1 add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
     IP.SRC'
2 add rewrite policy pol_ins_client 'HTTP.REQ.HEADER("x-forwarded-for").
     EXISTS || HTTP.REQ.HEADER("client-ip").EXISTS' act_ins_client
3 bind rewrite global pol_ins_client 300 END
4 <!--NeedCopy-->
```

So fügen Sie mit dem Konfigurationsdienstprogramm einen lokalen Client-IP-Header hinzu

Erstellen Sie im Dialogfeld Rewrite Action erstellen eine Umschreiben Aktion mit der folgenden Beschreibung.

Name	Typ	Argument (e)
act_ins_client	insert_http_header	NS-Client 'CLIENT.IP.SRC'

Erstellen Sie im Dialogfeld Rewrite-Richtlinie erstellen eine Richtlinie zum Umschreiben mit der folgenden Beschreibung.

Name	Ausdruck	Aktion
pol_ins_client	'HTTP.REQ.HEADER ("x-forwarded-for") .EXISTS || HTTP.REQ.HEADER ("client-ip") .EXISTS'	act_ins_client

Binden Sie die Richtlinie an Global, Zuweisen der Prioritäten und Gehe zu Ausdruckswerten unten

gezeigt.

Name	Priorität	Gehe zu Ausdruck
pol_ins_client	100	Neben

Beispiel 3: Sichere und unsichere Verbindungen taggen

May 11, 2023

Example Inc. möchte eingehende Anfragen mit einem Header kennzeichnen, der angibt, ob es sich bei der Verbindung um eine sichere Verbindung handelt oder nicht. Dies hilft dem Server, sichere Verbindungen im Auge zu behalten, nachdem der NetScaler die Verbindungen entschlüsselt hat.

Um diese Konfiguration zu implementieren, erstellen Sie zunächst Rewrite-Aktionen mit den in den folgenden Tabellen angegebenen Werten. Diese Aktionen kennzeichnen Verbindungen zu Port 80 als unsichere Verbindungen und Verbindungen zu Port 443 als sichere Verbindungen.

Name der Aktion	Art der Rewrite-Aktion	Name der Kopfzeile	Wert
Action-Rewrite-SSL_Ja	INSERT_HTTP_HEADER	SSL	JA

Name der Aktion	Art der Rewrite-Aktion	Name der Kopfzeile	Wert
Action-Rewrite-SSL_NEIN	INSERT_HTTP_HEADER	SSL	NEIN

Anschließend würden Sie eine Rewrite-Richtlinie mit den in den folgenden Tabellen angegebenen Werten erstellen. Diese Richtlinien überprüfen eingehende Anfragen, um festzustellen, welche Anfragen an Port 80 und welche an Port 443 weitergeleitet werden. Die Richtlinien fügen dann den richtigen SSL-Header hinzu.

Name der Richtlinie	Name der Aktion	Undefinierte Aktion	Ausdruck
Richtlinie neu schreiben SSL_Ja	Action-Rewrite-SSL_Ja	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (443)

Name der Richtlinie	Name der Aktion	Undefinierte Aktion	Ausdruck
Policy-Rewrite-SSL_NEIN	Action-Rewrite-SSL_NEIN	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (80)

Schließlich würden Sie die Rewrite-Richtlinien an NetScaler binden, der ersten Richtlinie eine Priorität von 200 und der zweiten eine Priorität von 300 zuweisen und den goto-Ausdruck beider Richtlinien auf END setzen.

Jede eingehende Verbindung zu Port 80 hat nun einen SSL:NO HTTP-Header hinzugefügt und jede eingehende Verbindung zu Port 443 hat einen SSL:YES HTTP-Header hinzugefügt.

Beispiel 4: Maskieren des HTTP-Servertyps

October 8, 2021

Example Inc. möchte den HTTP-Server Header so ändern, dass nicht autorisierte Benutzer und bösartiger Code den Header nicht verwenden können, um die vom HTTP-Server verwendete Software zu identifizieren.

Um den HTTP Server Header zu ändern, würden Sie eine Rewrite-Aktion und eine Rewriterichtlinie mit den Werten in den folgenden Tabellen erstellen.

Aktionsname	Art der Rewrite-Aktion	Ausdruck zur Auswahl der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Server_Mask	REPLACE	HTTP.RES.HEADER(“Se	“Web Server 1.0”

Name der Richtlinie	Aktionsname	Undefinierte Aktion	Ausdruck
Policy-Rewrite-Server_Mask	Action-Rewrite-Server_Mask	NOREWRITE	HTTP.RES.IS_VALID

Beispielbefehle:

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("
Server")"\"Web Server 1.0\""
```



```
> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-
Server_Mask NOREWRITE
```

Sie würden dann die Rewriterichtlinie global binden, eine Priorität von 100 zuweisen und den Gehe zu Prioritätsausdruck der Richtlinie auf END setzen.

Der HTTP Server: Header wurde jetzt geändert, um “Web Server 1.0” zu lesen, was die eigentliche HTTP-Serversoftware maskiert, die von der Website Example Inc. verwendet wird.

Beispiel 5: Umleiten einer externen URL auf eine interne URL

January 28, 2022

Example Inc. möchte seine tatsächliche Serverraumkonfiguration vor Benutzern verbergen, um die Sicherheit auf seinen Webservern zu verbessern.

Um die Sicherheit zu verbessern, würden Sie eine Umschreibaktion mit den Werten erstellen, wie in den folgenden Tabellen dargestellt. Bei Anforderungsheadern wird die Aktion in der Tabelle von `www.example.com` zu web.hq.example.net geändert. Bei Response-Headern macht die Aktion das Gegenteil und übersetzt `web.hq.example.net` in `www.example.com`.

Name der Aktion	Art der Rewrite-Aktion	Ausdruck zur Auswahl der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Request_Server_Replac	REPLACE	HTTP.REQ.HOSTNAME.S	“Web.hq.example.net”
Action-Rewrite-Response_Server_Replace	REPLACE	HTTP.RES.HEADER(“Server”)	“www.example.com”

Die erste Richtlinie prüft eingehende Anfragen, um festzustellen, ob sie gültig sind. Wenn sie gültig sind, führt sie die Aktion Action-Rewrite-Request_Server_Replace aus. Die zweite Richtlinie überprüft die Antworten, um festzustellen, ob sie vom Server stammen `web.hq.example.net`. Wenn dies der Fall ist, führt es die Aktion Action-Rewrite-Response_Server_Replace aus.

Beispiele für Rewrite-Aktionen und Richtlinien zum Umleiten einer externen URL.

```
add rewrite action Action-Rewrite-Request_Server_Replace REPLACE HTTP.REQ.
HOSTNAME.SERVER '"Web.hq.example.net"'
```

```
add rewrite action Action-Rewrite-Response_Server_Replace REPLACE HTTP.RES.
HEADER("Server")'"www.example.com"'
```



```
add rewrite policy Rewrite-Request_Server_Replace HTTP.REQ.HOSTNAME.SERVER.
EQ("www.example.com")Action-Rewrite-Request_Server_Replace NOREWRITE

add rewrite policy Rewrite-Response_Server_Replace HTTP.REQ.HEADER("Server"
).EQ("Web.hq.example.net")Action-Rewrite-Response_Server_Replace
```

Schließlich würden Sie die Rewrite-Richtlinien binden und jeweils eine Priorität von 500 zuweisen, da sie in verschiedenen Richtlinienbank sind und keinen Konflikt verursachen. Setzen Sie den goto-Ausdruck für beide Bindungen auf NEXT.

```
bind rewrite global Policy-Rewrite-Request_Server_Replace 500 END -type
REQ_DEFAULT

bind rewrite global Policy-Rewrite-Response_Server_Replace 500 END -type
RES_DEFAULT
```

Alle Instanzen von `www.example.com` in den Anforderungsheadern werden jetzt in geändert `web.hq.example.net`, und alle Instanzen von In-Response-Headern werden jetzt `web.hq.example.net` in geändert `www.example.com`.

Beispiel 6: Migrieren der Apache Rewrite Modul-Regeln

May 11, 2023

Example Inc. verwendet derzeit das Apache Rewrite-Modul, um Suchanfragen zu verarbeiten, die an seine Webserver gesendet werden, und diese Anfragen auf der Grundlage der Informationen in der Anforderungs-URL an den entsprechenden Server umzuleiten. Example Inc. möchte die Einrichtung vereinfachen, indem es diese Regeln auf die NetScaler-Plattform migriert.

Nachfolgend sind mehrere Apache-Rewrite-Regeln aufgeführt, die Example derzeit verwendet. Diese Regeln leiten Suchanfragen an eine spezielle Ergebnisseite weiter, wenn sie keine SiteID-Zeichenfolge haben oder wenn sie eine SiteID-Zeichenfolge haben, die Null (0) entspricht, oder auf die Standard-ergebnisseite, wenn diese Bedingungen nicht zutreffen.

Im Folgenden sind die aktuellen Apache-Rewrite-Regeln aufgeführt:

- RewriteCond% {REQUEST_FILENAME} ^/search$ [NC]
- Schreiben Sie erneut% {QUERY_STRING}! SiteID= [ODER]
- RewriteCond %{QUERY_STRING} SiteId=0
- RewriteSecond% {QUERY_STRING} callname=Ergebnisse anzeigen [NC]
- Regel neu schreiben ^.*$ results2.html [P, L]
- RewriteCond% {REQUEST_FILENAME} ^/search$ [NC]
- RewriteSecond% {QUERY_STRING} callname=Ergebnisse anzeigen [NC]
- Regel neu schreiben ^.*$ /results.html [P, L]

Um diese Apache-Rewrite-Regeln auf dem NetScaler zu implementieren, würden Sie Rewrite-Aktionen mit den Werten in den folgenden Tabellen erstellen.

Name der Aktion	Art der Rewrite-Aktion	Ausdruck zur Auswahl der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Aktion umschreiben - Dis-play_Results_NullSiteI[	REPLACE	HTTP.REQ.URL	“/results2.html”
Aktion — Umschreiben — Ergebnisse anzeigen	REPLACE	HTTP.REQ.URL	“/results2.html”

Anschließend würden Sie Rewrite-Richtlinien mit den Werten erstellen, die in den folgenden Tabellen aufgeführt sind.

Name der Richtlinie	Name der Aktion	Undefinierte Aktion	Ausdruck
Richtlinie umschreiben - Dis-play_Results_NullSiteI[	Aktion umschreiben - Dis-play_Results_NullSiteI[	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD (IGNORECASE) .EQ („/search“) && (! HTTP.REQ.URL.QUERY.CONTAINS („SiteID=“) || HTTP.REQ.URL.QUERY.CONTAINS („SiteID=0”) || HTTP.REQ.URL.QUERY.SET_TEXT_MO (IGNORECASE) .CONTAINS („call-Name=DisplayResults“))
Richtlinie neu schreiben — Ergebnisse anzeigen	Aktion — Umschreiben — Ergebnisse anzeigen	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD (IGNORECASE) .EQ („/search“) || HTTP.REQ.URL.QUERY.SET_TEXT_MO (IGNORECASE) .CONTAINS („call-Name=DisplayResults“))

Schließlich würden Sie die Rewrite-Richtlinien binden, indem Sie der ersten eine Priorität von 600

und der zweiten eine Priorität von 700 zuweisen und dann den goto-Ausdruck für beide Bindungen auf NEXT setzen.

NetScaler verarbeitet diese Suchanfragen nun genau so, wie es der Webserver getan hat, bevor die Regeln des Apache-Rewrite-Moduls migriert wurden.

Beispiel 7: Umleitung von Marketing-Keywords

May 11, 2023

Die Marketingabteilung von Example Inc. möchte vereinfachte URLs für bestimmte vordefinierte Stichwortsuchen auf der Website des Unternehmens einrichten. Für diese Keywords möchte es die URL wie unten gezeigt neu definieren.

- Externe URL:

```
http://www.example.com/\<marketingkeyword\>
```

- Interne URL:

```
http://www.example.com/go/kwsearch.asp?keyword=\<marketingkeyword\>
```

Um die Umleitung für Marketing-Keywords einzurichten, würden Sie eine Umschreibeaktion mit den Werten in der folgenden Tabelle erstellen.

Name der Aktion	Art der Rewrite-Aktion	Ausdruck zur Auswahl des Zielorts	Zeichenfolgenausdruck für Ersetzungstext
Aktion — Umschreiben — URL ändern	INSERT_BEFORE	HTTP.REQ.URL.PATH.GE (1)	„go/kwsearch.aspkeyword=”l“

Sie würden dann eine Rewriterichtlinie mit den Werten in der folgenden Tabelle erstellen.

Name der Richtlinie	Name der Aktion	Undefinierte Aktion	Ausdruck
Richtlinie umschreiben — URL ändern	Aktion — Umschreiben — URL ändern	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ („www.example.com“)

Schließlich würden Sie die Rewriterichtlinie binden und ihr eine Priorität von 800 zuweisen. Im Gegensatz zu den vorherigen Rewrite-Richtlinien sollte diese Richtlinie die letzte sein, die auf eine Anfrage

angewendet wird, die ihren Kriterien entspricht. Aus diesem Grund setzt der NetScaler-Administrator seinen Goto Priority Expression auf END.

Jede Anfrage, die ein Marketing-Keyword verwendet, wird auf die CGI-Seite für die Schlüsselwortsuche umgeleitet, woraufhin eine Suche durchgeführt und alle verbleibenden Richtlinien übersprungen werden.

Beispiel 8: Abfragen an den abgefragten Server umleiten

October 8, 2021

Example Inc. möchte Abfrageanforderungen an den entsprechenden Server umleiten, wie hier gezeigt.

- `<Request: GET /query.cgi?server=5HOST: www.example.com`
- `<Redirect URL: <http://web-5.example.com/>`

Um diese Umleitung zu implementieren, erstellen Sie zunächst eine Rewriteaktion mit den Werten in der folgenden Tabelle.

Aktionsname	Art der Rewrite-Aktion	Ausdruck zur Auswahl der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Aktion - Rewrite-Replace_Hostheader	REPLACE	HTTP.REQ.HEADER (“Host”) .BEFORE_STR (“.example.com”)	“Server-“ + HTTP.REQ.URL.QUERY.VALUE (“Web”)

Sie würden dann eine Rewriterichtlinie mit den Werten in der folgenden Tabelle erstellen.

Name der Richtlinie	Aktionsname	Undefinierte Aktion	Ausdruck
`Policy-Rewrite-Replace_Hostheader`	`Action-Rewrite-Replace_Hostheader`	NOREWRITE	`HTTP.REQ.HEADER("Host").EQ("www.example.com")`

Beispielbefehle:

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER("Server")"\"Web Server 1.0\""
```



```
Done

> add rewrite policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-
Server_Mask NOREWRITE
Done
```

Schließlich würden Sie die Rewriterichtlinie binden und ihr eine Priorität von 900 zuweisen. Da diese Richtlinie die letzte Richtlinie sein sollte, die auf eine Anforderung angewendet wird, die ihren Kriterien entspricht, setzen Sie den goto Ausdruck auf END.

Eingehende Anfragen an eine URL, die mit beginnt, `<http://www.example.com/query.cgi?server>=` werden an die Servernummer in der Abfrage umgeleitet.

Beispiel 9: Homepage-Umleitung

May 11, 2023

New Company, Inc. hat kürzlich einen kleineren Konkurrenten, Purchased Company, übernommen und möchte die Homepage von Purchased Company auf eine neue Seite auf seiner eigenen Website umleiten, wie hier gezeigt.

- Alte URL: http://www.purchasedcompany.com/*
- Neue URL: http://www.newcompany.com/products/page.htm

Um Anfragen an die Homepage des gekauften Unternehmens weiterzuleiten, erstellen Sie Rewrite-Aktionen mit den Werten in der folgenden Tabelle.

Name der Aktion	Art der Rewrite-Aktion	Ausdruck zur Auswahl der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Aktion umschreiben_URL ersetzen	REPLACE	HTTP.REQ.URL.PATH_A	„/products/page.htm“
Aktion — Neuschreiben — Host ersetzen	REPLACE	HTTP.REQ.HOSTNAME	„www.newcompany.com“

```
1 add rewrite action action-Rewrite-Replace_URLr REPLACE HTTP.REQ.URL.
     PATH_AND_QUERY  “/products/page.htm”
2
3 add rewrite action action-Rewrite-Replace_Host REPLACE HTTP.REQ.
```



```
    HOSTNAME  “www.newcompany.com”
<!--NeedCopy-->
```

Anschließend würden Sie Rewrite-Richtlinien mit den Werten in der folgenden Tabelle erstellen.

Name der Richtlinie	Name der Aktion	Undefinierte Aktion	Ausdruck
Richtlinie umschreiben-ersetzen-Keine	Aktion — Umschreiben — Ersetzen — Keine	NOREWRITE	! HTTP.REQ.HOSTNAME.SERVER.EQ („www.purchasedcompany.com“)
Policy-Rewrite-Replace-Host	Aktion — Neuschreiben — Host ersetzen	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ („www.purchasedcompany.com“)

```
add rewrite policy Policy-Rewrite-Replace-None !HTTP.REQ.HOSTNAME.
    SERVER.EQ( “www.purchasedcompany.com” ) Action-Rewrite-Replace-None
    NOREWRITE

add rewrite policy Policy-Rewrite-Replace-Host HTTP.REQ.HOSTNAME.SERVER
    .EQ( “www.purchasedcompany.com” ) Action-Rewrite-Replace_Host
    NOREWRITE
<!--NeedCopy-->
```

Schließlich würden Sie die Rewrite-Richtlinien global binden und der ersten eine Priorität von 100 und der zweiten eine Priorität von 200 zuweisen.

```
bind rewrite global Policy-Rewrite-Replace-None 100

bind rewrite global Policy-Rewrite-Replace-Host 200
<!--NeedCopy-->
```

Anfragen an die alte Website des übernommenen Unternehmens werden nun auf die richtige Seite auf der Homepage des neuen Unternehmens weitergeleitet.

Beispiel 10: Richtlinienbasierte RSA-Verschlüsselung

May 11, 2023

Der RSA-Algorithmus verwendet die Funktion PKEY_ENCRYPT_PEM (), um vordefinierte und benutzerdefinierte HTTP-Header- oder Textinhalte zu verschlüsseln. Die Funktion akzeptiert nur

öffentliche RSA-Schlüssel (keine privaten Schlüssel) und die verschlüsselten Daten dürfen nicht länger als die Länge des öffentlichen Schlüssels sein. Wenn die zu verschlüsselnden Daten kürzer als die Schlüssellänge sind, verwendet der Algorithmus die Füllmethode RSA_PKCS1.

In einem Beispielszenario kann die Funktion zusammen mit der Funktion B64ENCODE () in einer Rewrite-Aktion verwendet werden, um einen HTTP-Header-Wert durch einen Wert zu ersetzen, der mit einem öffentlichen RSA-Schlüssel verschlüsselt wurde. Die verschlüsselten Daten werden dann vom Empfänger mithilfe des privaten RSA-Schlüssels entschlüsselt.

Sie können die Funktion mithilfe einer Rewrite-Richtlinie implementieren. Dazu müssen Sie die folgenden Aufgaben ausführen:

1. Fügen Sie den öffentlichen RSA-Schlüssel als Richtlinienausdruck hinzu.
2. Erstellen Sie eine Rewrite-Aktion.
3. Erstellen Sie eine Rewrite-Richtlinie.
4. Binden Sie die Rewrite-Richtlinie als global ein.
5. RSA-Verschlüsselung überprüfen

Richtlinienbasierte RSA-Verschlüsselung mit der NetScaler Befehlszeilenschnittstelle

Führen Sie die folgenden Aufgaben aus, um die richtlinienbasierte RSA-Verschlüsselung mit der NetScaler Befehlszeilenschnittstelle zu konfigurieren.

So fügen Sie mit der NetScaler Befehlszeilenschnittstelle einen öffentlichen RSA-Schlüssel als Richtlinienausdruckhinzu:

```
1 add policy expression pubkey '"-----BEGIN RSA PUBLIC KEY-----
     MIGJAoGBAKl5vgQEj73Kxp+9
     yn1v5gPR1pnc4oLM2a0kaWwBOsB6rzCIy6znwnvwCY1xRvQhRlJSAyJbloL7wZFIJ2FOR8Cz
     +8ZQWXU2syG+udi4EnWqLgFYowF9zK+o79az597eNPAjsHZ/C2oL/+6qY5a/
     f1z8bQPrHC4GpFfAEJhh/+NnAgMBAAE=-----END RSA PUBLIC KEY-----"'
2 <!--NeedCopy-->
```

So fügen Sie eine Aktion zum Verschlüsseln einer HTTP-Header-Anforderung mit der NetScaler Befehlszeilenschnittstellehinzu:

```
add rewrite action encrypt_act insert_http_header encrypted_data

HTTP.REQ.HEADER("data_to_encrypt").PKEY_ENCRYPT_PEM(pubkey).B64ENCODE
```

So fügen Sie Rewrite-Richtlinie mit der NetScaler Befehlszeilenschnittstellehinzu:

```
1 add rewrite policy encrypt_pol 'HTTP.REQ.HEADER("data_to_encrypt").
     EXISTS' encrypt_act
2 <!--NeedCopy-->
```


So binden Sie die Umschreibungsrichtlinie global mit der NetScaler Befehlszeilenschnittstelle:

```
bind rewrite global encrypt_pol 10 -type RES_DEFAULT
```

So überprüfen Sie die RSA-Verschlüsselung mit der NetScaler Befehlszeilenschnittstelle:

```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

* About to connect() to 10.217.24.7 port 80 (#0)

*  Trying 10.217.24.7...

*  connected

*  Connected to 10.217.24.7 (10.217.24.7) port 80 (#0)

> GET / HTTP/1.1
> User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
   OpenSSL/0.9.8y zlib/1.2.3
> Host: 10.217.24.7
> Accept: \*/\*
> data_to_encrypt: Now is the time that tries men's souls
>
< HTTP/1.1 200 OK
< Date: Mon, 09 Oct 2017 05:22:37 GMT
< Server: Apache/2.2.24 (FreeBSD) mod_ssl/2.2.24 OpenSSL/0.9.8y DAV/2
< Last-Modified: Thu, 20 Feb 2014 20:29:06 GMT
< ETag: "6bd9f2-2c-4f2dc5b570880"
< Accept-Ranges: bytes
< Content-Length: 44
< Content-Type: text/html
< encrypted_data: UliegKBJqZd7JdaC49XMLEK1+eQN2rEfevypW91gKvBVlaKM9N9/
   C2BKuztS99SE0xQaisidzN5IgeIcpQMn+
   CiKYVlLzPG1RuhGaqHYzIt6C8A842da7xE4OlV5SHwScqkqZ5aVrXc3EwtUksna7jOLr40aLeXnnB
   /DB11pUAE=
<
* Connection #0 to host 10.217.24.7 left intact
<html><body><h1>It works!</h1></body></html>* Closing connection #0

<!--NeedCopy-->
```

Die nachfolgende Ausführung dieses Curl-Befehls mit denselben zu verschlüsselnden Daten zeigt, dass die verschlüsselten Daten bei jeder Ausführung unterschiedlich sind. Dies liegt daran, dass das Padding zufällige Byte am Anfang der zu verschlüsselnden Daten einfügt, wodurch die verschlüsselten Daten jedes Mal anders sind.


```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

< encrypted_data:
   DaOjtl1Pl4DlQKf58MMeL4cFwFvZwhjMqv5aUYM5Iyzk4UpwIYhpRvgTNu2lXEVc1H0tcR1EGC
   /ViQncLc4EbTurCWLbzjce3+fknnMmzF0lRT6ZZXWbMvsNFOxDA1SnuAgwxWXy/
   ooe9Wy6SYsL2oi1sr5wTG+RihDd9zP+P14=

>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/

. . .

< encrypted_data: eej6YbGP68yHn48qFUvi+fkG+OiO8j3yYLScrRBU+
   TPQ8WeDVaWnDNAVLvL0ZYHHAU1W2YDRYb+8
   cdKHLpW36QbI6Q5FfBuWKZSI2hSyUvypTpCoAYcHXFv0ns+tRtg0EPNNj+
   lyGjKQWtFi6K8IXXISoDy42FblKIlaA7gEriY=
<!--NeedCopy-->
```

Richtlinienbasierte RSA-Verschlüsselung mithilfe der GUI

Mit der GUI können Sie die folgenden Aufgaben ausführen:

Um den öffentlichen RSA-Schlüssel als Richtlinienausdruck mithilfe der GUI hinzuzufügen, gehen Sie wie folgt vor:

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Configurations**>**AppExpert > Advanced Expressions**.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um einen öffentlichen RSA-Schlüssel als erweiterten Richtlinienausdruck zu definieren.
3. Stellen Sie auf der Seite „Ausdruck erstellen“ die folgenden Parameter ein:
   a) Name des Ausdrucks. Name des erweiterten Ausdrucks.
   b) Expression. Definieren Sie den öffentlichen RSA-Schlüssel mit dem Ausdrucksеditor als erweiterten Ausdruck.
   c) Kommentare. Eine kurze Beschreibung des Ausdrucks.
4. Klicken Sie auf **Erstellen**.

Um eine Rewrite-Aktion hinzuzufügen, um eine HTTP-Header-Anfrage mithilfe der GUI zu verschlüsseln:

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Configurations**>**AppExpert > **Rewrite**** > Actions.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Neuschreibaktion hinzuzufügen.

3. Stellen **Sie im Bildschirm „Rewrite-Aktion erstellen** “ die folgenden Parameter ein:
   a) Name. Name der Rewrite-Aktion.
   b) Typ. Wählen Sie den Aktionstyp als INSERT_HTTP_HEADER aus.
   c) Verwenden Sie den Aktionstyp, um eine Kopfzeile einzufügen. Geben Sie den Namen des HTTP-Headers ein, der neu geschrieben werden muss.
   d) Expression. Name des erweiterten Richtlinienausdrucks, der der Aktion zugeordnet ist.
   e) Kommentare. Eine kurze Beschreibung der Rewrite-Aktion.
4. Klicken Sie auf **Erstellen**.

Gehen Sie wie folgt vor, um mithilfe der GUI eine erweiterte Rewrite-Richtlinie hinzuzufügen:

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Configurations**>**AppExpert > **Rewrite**** > Policies.**
2. Klicken Sie auf der Seite **Richtlinien neu schreiben** auf **Hinzufügen**, um eine Richtlinie zum Umschreiben hinzuzufügen.
3. Stellen Sie auf der Seite **Create Rewrite Policy** die folgenden Parameter ein:
   a) Name. Name der Rewrite-Richtlinie.
   b) Aktion. Name der Umschreibeaktion, die ausgeführt werden soll, wenn die Anforderung oder Antwort dieser Umschreiberichtlinie entspricht.
   c) Aktion protokollieren. Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anfrage dieser Richtlinie entspricht.
   d) Aktion mit undefiniertem Ergebnis. Durchzuführende Maßnahmen, wenn das Ergebnis der politischen Bewertung nicht definiert ist.
   e) Expression. Name des erweiterten Richtlinienausdrucks, der die Aktion auslöst.
   f) Kommentare. Eine kurze Beschreibung der Rewrite-Aktion.
4. Klicken Sie auf **Erstellen**.

Um die Rewrite-Richtlinie global zu binden, verwenden Sie die GUI:

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Configurations**>**AppExpert > **Rewrite**** > Policies.**
2. Wählen Sie im Fenster **Richtlinien neu schreiben** eine Rewrite-Richtlinie aus, die Sie binden möchten, und klicken Sie auf **Policy**Manager.
3. Stellen Sie auf der Seite Rewrite Policy Manager im Abschnitt Bind Points die folgenden Parameter ein:
   a) Bind-Punkt. Wählen Sie den Bindungspunkt als Standard Global aus.
   b) Protokoll. Wählen Sie den Protokolltyp als HTTP aus.
   c) Art der Verbindung. Wählen Sie den Verbindungstyp als Anfrage aus.
   d) Klicken Sie auf **Weiter**, um den Abschnitt **Richtlinienbindung** aufzurufen.
   e) Wählen Sie im Abschnitt **Richtlinienbindung** die Rewrite-Richtlinie aus und legen Sie die Bindungsparameter fest.
4. Klicken Sie auf **Bind**.

Beispiel 11: Richtlinienbasierte RSA-Verschlüsselung ohne Füllvorgang

May 11, 2023

Die Richtlinienfunktion PKEY_ENCRYPT_PEM_NO_PADDING () verwendet vor der Durchführung der RSA-Verschlüsselung den RSA-Algorithmus ohne Füllvorgang. Die Richtlinienfunktion funktioniert genauso wie die Funktion PKEY_ENCRYPT_PEM (), außer dass sie die Methode RSA_NO_PADDING anstelle von RSA_PKCS1_PADDING verwendet. Der pkey-Parameter ist eine Textzeichenfolge mit einem PEM-kodierten öffentlichen RSA-Schlüssel. Ähnlich wie bei PKEY_ENCRYPT_PEM () können Sie einen Richtlinienausdruck für den Schlüssel verwenden.

Sie können die Funktion mithilfe einer Rewrite-Richtlinie implementieren. Dazu müssen Sie die folgenden Aufgaben ausführen:

1. Fügen Sie den öffentlichen RSA-Schlüssel als Richtlinienausdruck hinzu.
2. Erstellen Sie eine Rewrite-Aktion.

Richtlinienbasierte RSA-Verschlüsselung mit der NetScaler Befehlszeilenschnittstelle

Führen Sie die folgenden Aufgaben aus, um die richtlinienbasierte RSA-Verschlüsselung mit der NetScaler Befehlszeilenschnittstelle zu konfigurieren.

So fügen Sie mit der NetScaler Befehlszeilenschnittstelle einen öffentlichen RSA-Schlüssel ohne Auffüllunghinzu:

```
1 add expression rsa_pub_key_4096 '"-----BEGIN RSA PUBLIC KEY-----" + "
     MIICCgKCAgEArrwBldKd48xrpOSRPMrg+eNAO0ODU6t5b/WYQLdElqNv7WpefBrA" +
     "nwI2s619gEU1r4zoLqL7l5ALtt5Z+F0JBYfOzBzOky0GtEJ5iX5GP4QxT65J3nHH" +
      "4MTF3acmjvXxclmaKXEFlaVIzW7FTr3Luw/CnOjflAB403Q6F9VBVvQmOVYWnqoI"
     + "+0q1VIg6Q1pAcvdKBiOf85BBofE5EIbZ/1Jt0CdbsV568l+8ve7BnSUncFHoRR3O"
      + "/VfSsDuNWZf7n3RNMzxEuIA72UGPzNYFQzvcPOdzd0aN7jAXw0mgC/NSvKzGKHlo
     " + "mUYYBzlVQdDMZWnd6jSzsBRXSXxsNEy/
     RuXwplrA5epo7JdCoMkfeI4vUXm6MNr8" + "
     TQdFqIc1pdnOsbRf9ec62XbcfR7P8CDTsmLSaagx3rjenPdB+LTWKw2VUF+YONIg" +
     "jM3fyFef9ovVhLhS5HvMqFGs8P75W+d7BOIbIu3EngACiEJOpYSsETD4WgPK6Iyv" +
      "j6cxsLeYMtElTb0fBIIqysCHdmjF3M1lqdqp4dKs3+W798GJZYM5MxZKUzrBi0Xu"
     + "e7GtSh2aimsfQureUD+0z0RN2umeDsYcA1ghXMclDP+jLS1lnrv0Yvo+TKcm9b8G"
      + "uR/drbCrCsGyWFW+bsAu3AWz9S6TePurP5unRmNNvXpH5DRgsYl3d50CAwEAAQ
     ==" + "-----END RSA PUBLIC KEY-----"
2 <!--NeedCopy-->
```

So fügen Sie mit der NetScaler Befehlszeilenschnittstelle Umschreibaktion für keinen Ausdruck der Auffüllrichtliniehinzu:


```
add rewrite action rsa_encrypt_act insertHttpHeader encrypted 'HTTP.REQ.
HEADER("plaintext").PKEY_ENCRYPT_PEM_NO_PADDING(rsa_pub_key_4096)
```

Richtlinienbasierte RSA-Verschlüsselung ohne Padding-Option mithilfe der GUI

Mit der GUI können Sie die folgenden Aufgaben ausführen:

Um den öffentlichen RSA-Schlüssel ohne Auffüllen als Richtlinienausdruck hinzuzufügen, verwenden Sie die GUI:

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Configurations**>**AppExpert > Advanced Expressions**.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um einen öffentlichen RSA-Schlüssel als erweiterten Richtlinienausdruck zu definieren.
3. Stellen Sie auf der Seite „Ausdruck erstellen“ die folgenden Parameter ein:
   a) Name des Ausdrucks. Name des erweiterten Ausdrucks.
   b) Expression. Definieren Sie den öffentlichen RSA-Schlüssel mit dem Ausdrucksеditor als erweiterten Ausdruck.
   Hinweis: Die maximale Zeichenkettenlänge in einem Richtlinienausdruck beträgt 255 Zeichen. Für jeden Schlüssel, der länger als 1024 Bit ist, müssen Sie den Schlüssel in kleinere Blöcke aufteilen und die Chunks zu „chunk1” + „chunk2” +… zusammenfügen.
   c) Kommentare. Eine kurze Beschreibung des Ausdrucks.
4. Klicken Sie auf **Erstellen**.

Um mithilfe der GUI eine Aktion umzuschreiben, gehen Sie wie folgtvor:

1. **Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu**Configurations**>**AppExpert > **Rewrite**** > Actions.**
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Neuschreibaktion hinzuzufügen.
3. Stellen **Sie im Bildschirm „Rewrite-Aktion erstellen** “ die folgenden Parameter ein:
   a) Name. Name der Rewrite-Aktion.
   b) Typ. Wählen Sie den Aktionstyp als INSERT_HTTP_HEADER aus.
   c) Verwenden Sie den Aktionstyp, um eine Kopfzeile einzufügen. Geben Sie den Namen des HTTP-Headers ein, der neu geschrieben werden muss.
   d) Expression. Name des erweiterten Richtlinienausdrucks, der der Aktion zugeordnet ist.
   e) Kommentare. Eine kurze Beschreibung der Rewrite-Aktion.
4. Klicken Sie auf **Erstellen**.

Beispiel 12: Konfigurieren des Rewrite, um den Hostnamen und die URL in der Clientanforderung auf der NetScaler-Appliance zu ändern

May 11, 2023

Die Rewrite-Funktion auf einer NetScaler-Appliance wird verwendet, um die in der Client-Anfrage verfügbare URL in eine andere URL zu konvertieren, die der Back-End-Server verstehen kann. Mit der Rewrite-Funktion können Sie die folgenden Vorteile erzielen:

- Erhöht die Sicherheit, indem die tatsächliche URL der Ressource, die vom Client angefordert wird, ausgeblendet wird.
- Verhindert, dass der unbefugte Benutzer Zugriff auf die Netzwerkressourcen erhält.

Stellen Sie sich ein Beispiel vor, in dem Ihre aktuelle Organisation von einer anderen Organisation übernommen wird. Für Administratoren wird es zu einer schwierigen Aufgabe, jeden Benutzer der übernommenen Organisation über die neue Webadresse zu informieren. In diesem Szenario ist es praktisch, die Rewrite-Funktion zu verwenden, um den Hostnamen und die URL in den Kundenanfragen für die Website der übernommenen Organisation zu ändern. Sie können Rewrite verwenden, um die URLs in der Client-Anfrage vorübergehend zu ändern, wenn die Website gewartet wird.

Im folgenden Abschnitt wird das Verfahren zum Ändern des Hostnamens und der URL in einer Client-Anfrage mithilfe der Rewrite-Funktion beschrieben.

Stellen Sie sich ein Beispiel vor, bei dem der Benutzer eine `http://www.example.com` URL in den Webbrowser eingibt. Der Website-Administrator möchte, dass die NetScaler-Appliance die vorherige URL in der Client-Anfrage als konvertiert. `http://myexample.example.net.in/resource/inventory/s?t=112`

Im vorherigen Beispiel möchte der Website-Administrator, dass die NetScaler-Appliance den Domainnamen „example.com“ durch „myexample.example.net.in“ und die URL durch „resource/inventory/s? t=112”.

Führen Sie Folgendes mit der CLI aus

1. Melden Sie sich mit SSH bei der NetScaler Appliance an.
2. Aktionen zum Umschreiben hinzufügen.
   - `add rewrite action rewrite_doman_url_repalce_act replace HTTP.REQ.URL "\"http://myexample.example.net.in/resource/inventory/s?t=112\""`
3. Fügen Sie Richtlinien zum Umschreiben für die Umschreibaktionen hinzu.

- `add rewrite policy rewrite_domain_url_pol HTTP.REQ.HOSTNAME.EQ("www.example.com")rewrite_doman_url_repalce_act`

4. Binden Sie die Umschreibungsrichtlinien an einen virtuellen Server.

   - `bind lb vserver rewrite_LB -policyName rewrite_domain_url_pol -priority 100 -gotoPriorityExpression END -type REQUEST`

URL-Transformation

February 24, 2022

Die URL-Transformationsfunktion bietet eine Methode zum Ändern aller URLs in bestimmten Anforderungen von einer externen Version, die von externen Benutzern angezeigt wird, zu einer internen URL, die nur von Ihren Webservern und IT-Mitarbeitern angezeigt wird. Sie können Benutzeranforderungen nahtlos umleiten, ohne dass die Netzwerkstruktur Benutzern zugänglich gemacht wird. Sie können auch komplexe interne URLs ändern, die Benutzer möglicherweise schwer merken können, in einfacheren, einfacheren externen URLs.

> **Hinweis:**
>
> Bevor Sie die URL-Transformationsfunktion verwenden können, müssen Sie die Funktion Umschreiben aktivieren. Informationen zum Aktivieren der Funktion "Umschreiben" finden Sie unter Aktivieren des Rewrite-Feature.
>
> URL-Transformationsfunktion schreibt URLs im HTML-Antworttext um und wird nicht auf JavaScript und andere Variablen angewendet.

Um mit der Konfiguration der URL-Transformation zu beginnen, erstellen Sie Profile, die jeweils eine bestimmte Transformation beschreiben. Innerhalb jedes Profils erstellen Sie eine oder mehrere Aktionen, die die Transformation detailliert beschreiben. Als Nächstes erstellen Sie Richtlinien, die jeweils einen Typ der zu transformierenden HTTP-Anforderung identifizieren, und Sie ordnen jede Richtlinie einem entsprechenden Profil zu. Schließlich binden Sie jede Richtlinie global an, um sie in Kraft zu setzen.

Konfigurieren von URL-Transformationen

May 11, 2023

Ein Profil beschreibt eine bestimmte URL-Transformation als eine Reihe von Aktionen. Das Profil dient in erster Linie als Container für die Aktionen und bestimmt die Reihenfolge, in der die Aktionen

ausgeführt werden. Die meisten Transformationen transformieren einen externen Hostnamen und optionalen Pfad in einen anderen, internen Hostnamen und Pfad. Die meisten nützlichen Transformationen sind einfach und erfordern nur eine einzige Aktion. Sie können jedoch mehrere Aktionen verwenden, um komplexe Transformationen durchzuführen.

Sie können keine Aktionen erstellen und sie dann zu einem Profil hinzufügen. Sie müssen zuerst das Profil erstellen und dann Aktionen hinzufügen. In der CLI sind das Erstellen einer Aktion und das Konfigurieren der Aktion separate Schritte. Das Erstellen eines Profils und das Konfigurieren des Profils sind separate Schritte sowohl in der CLI als auch im Konfigurationsprogramm.

So erstellen Sie ein URL-Transformationsprofil mithilfe der NetScaler-Befehlszeile

Geben Sie an der NetScaler-Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein, um ein URL-Transformationsprofil zu erstellen und die Konfiguration zu überprüfen. Anschließend können Sie den zweiten und dritten Befehl wiederholen, um weitere Aktionen zu konfigurieren:

- `add transform profile <profileName> -type URL [-onlyTransformAbsURLinBody (ON|OFF)] \[-comment <comment>]`
- `add transform action <name> <profileName> <priority>`
- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]`
- `show transform profile <name>`

Beispiel:

```
> add transform profile shoppingcart -type URL
 Done
> add transform action actshopping shoppingcart 1000
 Done
> set transform action actshopping -priority 1000 -reqUrlFrom 'shopping
   .example.com' -reqUrlInto 'www.example.net/shopping' -resUrlFrom '
   www.example.net/shopping' -resUrlInto 'shopping.example.com' -
   cookieDomainFrom 'example.com' -cookieDomainInto 'example.net' -
   state ENABLED -comment 'URL transformation for shopping cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
```



```
 Done
<!--NeedCopy-->
```

So ändern Sie ein vorhandenes URL-Transformationsprofil oder eine Aktion mithilfe der NetScaler-Befehlszeile

Geben Sie an der NetScaler-Befehlszeile die folgenden Befehle ein, um ein vorhandenes URL-Transformationsprofil oder eine Aktion zu ändern und die Konfiguration zu überprüfen:

Hinweis: Verwenden Sie den Befehl set transform profile bzw. set transform action. Der Befehl set transform profile verwendet dieselben Argumente wie der Befehl add transform profile, und set transform action ist derselbe Befehl, der für die Erstkonfiguration verwendet wurde.

- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]`
- `show transform profile <name>`

Beispiel:

```
> set transform action actshopping -priority 1000 -reqUrlFrom '
   searching.example.net' -reqUrlInto 'www.example.net/searching' -
   resUrlFrom 'www.example.net/searching' -resUrlInto 'searching.
   example.com' -cookieDomainInto 'example.net' -state ENABLED -comment
    'URL transformation for searching cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

So entfernen Sie ein URL-Transformationsprofil und Aktionen mithilfe der NetScaler-Befehlszeile

Entfernen Sie zunächst alle mit diesem Profil verknüpften Aktionen, indem Sie den folgenden Befehl einmal für jede Aktion eingeben:

- rm transform action <name> Nachdem Sie alle mit einem Profil verknüpften Aktionen entfernt haben, entfernen Sie das Profil wie unten gezeigt.
- rm-Transformationsprofil <name>

So erstellen Sie ein URL-Transformationsprofil mithilfe des Konfigurationsdienstprogramms

1. Erweitern Sie im Navigationsbereich **Rewrite**, erweitern Sie URL-Transformation und klicken Sie dann auf **Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld „URL-Transformationsprofil erstellen** “ Werte für die Parameter ein, oder wählen Sie sie aus. Der Inhalt des Dialogfelds entspricht den unter „Parameter für die Konfiguration von URL-Transformationsprofilen“ beschriebenen Parametern wie folgt (ein Sternchen gibt einen erforderlichen Parameter an):
   - Name* — Name
   - Kommentar — Kommentar
   - Transformiere nur absolute URLs im Antworttext — OnlyTransformAbsurLinBody
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Profil erfolgreich konfiguriert wurde.

So konfigurieren Sie ein URL-Transformationsprofil und Aktionen mithilfe des Konfigurationsdienstprogramms

1. Erweitern Sie im Navigationsbereich **Rewrite**, erweitern Sie URL-Transformation und klicken Sie dann auf **Profile**.
2. Wählen Sie im Detailbereich das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Führen **Sie im Dialogfeld „URL-Transformationsprofil konfigurieren** “ einen der folgenden Schritte aus.
   - Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine bestehende Aktion zu ändern, wählen Sie die Aktion aus und klicken dann auf **Öffnen**.
4. Füllen Sie das Dialogfeld „ **URL-Transformationsaktion erstellen** “ oder „ **URL-Transformationsaktion ändern** “ aus, indem Sie Werte für die Parameter eingeben oder auswählen. Der Inhalt des Dialogfelds entspricht den unter „Parameter für die Konfiguration von URL-Transformationsprofilen“ beschriebenen Parametern wie folgt (ein Sternchen gibt einen erforderlichen Parameter an):
   - Aktionsname* — name
   - Kommentare — Kommentar
   - Priorität* — Priorität

- URL anfordern von — ReqUrlFrom
- URL anfordern INTO — ReqURLInto
- Antwort-URL von — ResUrlFrom
- Antwort-URL into — Resurlinto
- Cookie-Domain von — CookieDomainVon
- Cookie-Domain INTO — CookieDomainINTO
- Aktiviert — Status

5. Speichern Sie Ihre Änderungen.
   - Wenn Sie eine neue Aktion erstellen, klicken Sie auf **Erstellen**und dann auf **Schließen**.
   - Wenn Sie eine bestehende Aktion ändern, klicken Sie auf **OK.**
     In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Profil erfolgreich konfiguriert wurde.
6. Wiederholen Sie die Schritte 3 bis 5, um weitere Aktionen zu erstellen oder zu ändern.
7. Um eine Aktion zu löschen, wählen Sie die Aktion aus und klicken Sie dann auf Entfernen. Wenn Sie dazu aufgefordert werden, klicken Sie auf OK, um den Löschvorgang zu bestätigen.
8. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld URL-Transformationsprofil ändern zu schließen.
9. Um ein Profil zu löschen, wählen Sie im Detailbereich das Profil aus, und klicken Sie dann auf **Entfernen**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Konfigurieren von URL-Transformationen

May 11, 2023

Nachdem Sie ein URL-Transformationsprofil erstellt haben, erstellen Sie als Nächstes eine URL-Transformationsrichtlinie, um die Anfragen und Antworten auszuwählen, die der NetScaler mithilfe des Profils transformieren soll. Bei der URL-Transformation werden jede Anfrage und die Antwort darauf als eine Einheit betrachtet, sodass URL-Transformationsrichtlinien nur ausgewertet werden, wenn eine Anfrage eingeht. Wenn eine Richtlinie übereinstimmt, transformiert der NetScaler sowohl die Anfrage als auch die Antwort.

Hinweis: Die Funktionen zur URL-Transformation und zum Umschreiben können während der Anforderungsverarbeitung nicht beide auf demselben HTTP-Header ausgeführt werden. Aus diesem Grund müssen Sie, wenn Sie eine URL-Transformation auf eine Anfrage anwenden möchten, sicherstellen, dass keiner der HTTP-Header, die sie modifizieren wird, durch eine Umschreibaktion manipuliert wird.

So konfigurieren Sie eine URL-Transformationsrichtlinie mithilfe der NetScaler-Befehlszeile

Sie müssen eine neue Richtlinie erstellen. In der Befehlszeile kann eine bestehende Richtlinie nur entfernt werden. Geben Sie an der NetScaler-Befehlszeile die folgenden Befehle ein, um eine URL-Transformationsrichtlinie zu konfigurieren und die Konfiguration zu überprüfen:

- `<add transform policy <name> <rule> <profileName>`
- `<show transform policy <name>`

Beispiel:

```
> add transform policy polsearch  HTTP.REQ.URL.SUFFIX.EQ("Searching")
   prosearching
 Done
> show transform policy polsearch
1)      Name: polsearch
        Rule: HTTP.REQ.URL.SUFFIX.EQ("Searching")
        Profile: prosearching
        Priority: 0
        Hits: 0
 Done
<!--NeedCopy-->
```

So entfernen Sie eine URL-Transformationsrichtlinie mithilfe der NetScaler-Befehlszeile

Geben Sie an der NetScaler-Befehlszeile den folgenden Befehl ein, um eine URL-Transformationsrichtlinie zu entfernen:

```
rm transform policy <name>
```

Beispiel:

```
> rm transform policy polsearch
Done
<!--NeedCopy-->
```

So konfigurieren Sie eine URL-Transformationsrichtlinie mithilfe des Konfigurationsdienstprogramms

1. Erweitern Sie im Navigationsbereich **Rewrite**, erweitern Sie URL-Transformation und klicken Sie dann auf **Richtlinien**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:

- Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
- Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.

3. Geben **Sie im Dialogfeld URL-Transformationsrichtlinie erstellen** oder **URL-Transformationsrichtlinie konfigurieren** Werte für die Parameter ein, oder wählen Sie sie aus. Der Inhalt des Dialogfelds entspricht den unter „Parameter für die Konfiguration von URL-Transformationsrichtlinien“ beschriebenen Parametern wie folgt (ein Sternchen gibt einen erforderlichen Parameter an):

   - Name* — Name (Kann für eine zuvor konfigurierte Richtlinie nicht geändert werden.)
   - Profil* — Profilname
   - Ausdruck — Regel

   Wenn Sie Hilfe beim Erstellen eines Ausdrucks für eine neue Richtlinie benötigen, können Sie entweder die Strg-Taste gedrückt halten und die Leertaste drücken, während sich der Cursor im Textfeld Ausdruck befindet. Um den Ausdruck zu erstellen, können Sie ihn direkt wie unten beschrieben eingeben oder das Dialogfeld Ausdruck hinzufügen verwenden.

4. Klicken Sie auf **Präfix**und wählen Sie das Präfix für Ihren Ausdruck aus.

   Ihre Auswahlmöglichkeiten:

   - HTTP — Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
   - SYS — Die geschützte (n) Website (n). Wählen Sie diese Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - Client — der Computer, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - Server — der Computer, an den die Anfrage gesendet wurde. Wählen Sie diese Option, wenn Sie einige Aspekte des Empfängers der Anfrage untersuchen möchten.
   - URL — Die URL der Anfrage. Wählen Sie diese Option, wenn Sie einen Aspekt der URL untersuchen möchten, an die die Anfrage gesendet wurde.
   - Text — Eine beliebige Textzeichenfolge in der Anfrage. Wählen Sie diese Option, wenn Sie eine Textzeichenfolge in der Anfrage untersuchen möchten.
   - Ziel — Das Ziel der Anfrage. Wählen Sie diese Option, wenn Sie einen Aspekt des Anforderungsziels untersuchen möchten.

   Nachdem Sie ein Präfix ausgewählt haben, zeigt NetScaler ein zweiteiliges Eingabeaufforderungsfenster an, in dem oben die möglichen nächsten Optionen und unten eine kurze Erläuterung der Bedeutung der ausgewählten Auswahl angezeigt werden. Die Auswahlmöglichkeiten hängen davon ab, welches Präfix Sie gewählt haben.

5. Wählen Sie Ihr nächstes Semester aus.

Wenn Sie HTTP als Präfix ausgewählt haben, stehen Ihnen REQ zur Verfügung, das HTTP-Anfragen spezifiziert, und RES, das HTTP-Antworten spezifiziert. Wenn Sie ein anderes Präfix gewählt haben, sind Ihre Auswahlmöglichkeiten vielfältiger. Um Hilfe zu einer bestimmten Auswahl zu erhalten, klicken Sie einmal auf diese Auswahl, um Informationen darüber im unteren Eingabeaufforderungsfenster anzuzeigen.

Wenn Sie sich sicher sind, welche Option Sie wählen möchten, doppelklicken Sie darauf, um sie in das Ausdrucksfenster einzufügen.

1. Geben Sie einen Zeitraum ein, und wählen Sie dann weitere Begriffe aus den Listenfeldern aus, die rechts neben dem vorherigen Listenfeld angezeigt werden. Sie geben die entsprechenden Textzeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis Ihr Ausdruck abgeschlossen ist.
2. Klicken Sie auf **Erstellen** oder **OK**, je nachdem, ob Sie eine neue Richtlinie erstellen oder eine vorhandene Richtlinie ändern.
3. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

So fügen Sie über das Dialogfeld Ausdruck hinzufügen einen Ausdruck hinzu

1. Klicken Sie im Dialogfeld **Responder-Aktion erstellen** oder **Responder-Aktion konfigurieren** auf **Hinzufügen**.
2. Wählen Sie im Dialogfeld **Ausdruck hinzufügen** im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.
    - HTTP. Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
    - SYS. Die geschützte (n) Website (n). Wählen Sie diese Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
    - CLIENT. Der Computer, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
    - SERVER. Der Computer, an den die Anfrage gesendet wurde. Wählen Sie diese Option, wenn Sie einige Aspekte des Empfängers der Anfrage untersuchen möchten.
    - URL. Die URL der Anfrage. Wählen Sie diese Option, wenn Sie einen Aspekt der URL untersuchen möchten, an die die Anfrage gesendet wurde.
    - TEXT. Eine beliebige Textzeichenfolge in der Anfrage. Wählen Sie diese Option, wenn Sie eine Textzeichenfolge in der Anfrage untersuchen möchten.
    - ZIEL. Das Ziel der Anfrage. Wählen Sie diese Option, wenn Sie einen Aspekt des Anforderungsziels untersuchen möchten.

      Wenn Sie Ihre Auswahl treffen, werden im Listenfeld ganz rechts die entsprechenden Begriffe für den nächsten Teil Ihres Ausdrucks aufgeführt.

3. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahl hängt davon ab, welche Wahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, wird im Hilfefenster unterhalb des Fensters "Ausdruck konstruieren" (das leer war) eine Hilfe zur Beschreibung des Zwecks und der Verwendung des gerade gewählten Begriffs angezeigt.
4. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.

Global verbindliche URL-Transformationsrichtlinien

May 11, 2023

Nachdem Sie Ihre URL-Transformationsrichtlinien konfiguriert haben, binden Sie sie an Global oder einen Bindungspunkt, um sie in Kraft zu setzen. Nach dem Binden wird jede Anfrage oder Antwort, die einer URL-Transformationsrichtlinie entspricht, durch das dieser Richtlinie zugeordnete Profil transformiert.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf jede positive Ganzzahl festlegen. Im NetScaler OS funktionieren die Richtlinienprioritäten in umgekehrter Reihenfolge — je höher die Zahl, desto niedriger die Priorität.

Da die URL-Transformationsfunktion nur die erste Richtlinie implementiert, der eine Anfrage entspricht, und keine zusätzlichen Richtlinien, denen sie möglicherweise entspricht, ist die Richtlinienpriorität wichtig, um die von Ihnen angestrebten Ergebnisse zu erzielen. Wenn Sie Ihrer ersten Richtlinie eine niedrige Priorität zuweisen (z. B. 1000), weisen Sie den NetScaler an, sie nur auszuführen, wenn andere Richtlinien mit einer höheren Priorität keiner Anfrage entsprechen. Wenn Sie Ihrer ersten Richtlinie eine hohe Priorität einräumen (z. B. 1), weisen Sie den NetScaler an, sie zuerst auszuführen, und überspringen alle anderen Richtlinien, die ebenfalls zutreffen könnten. Sie können sich ausreichend Spielraum lassen, um weitere Richtlinien in beliebiger Reihenfolge hinzuzufügen, ohne Prioritäten neu zuweisen zu müssen, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen den einzelnen Richtlinien festlegen, wenn Sie Ihre Richtlinien global binden.

Hinweis: URL-Transformationsrichtlinien können nicht an TCP-basierte virtuelle Server gebunden werden.

So binden Sie eine URL-Transformationsrichtlinie mithilfe der NetScaler-Befehlszeile

Geben Sie an der NetScaler-Befehlszeile die folgenden Befehle ein, um eine URL-Transformationsrichtlinie global zu binden und die Konfiguration zu überprüfen:

- `bind transform global <policyName> <priority>`
- `show transform global`

Beispiel:

```
> bind transform global polisearching 100
 Done
> show transform global
1)      Policy Name: polisearching
        Priority: 100

 Done
<!--NeedCopy-->
```

So binden Sie eine URL-Transformationsrichtlinie mithilfe des Konfigurationsdienstprogramms

1. Erweitern Sie im Navigationsbereich Rewrite, dann URL-Transformation und klicken Sie dann auf **Richtlinien.
2. Klicken Sie im Detailbereich auf **Policy Manager**.
3. Wählen Sie im Dialogfeld **Transform Policy Manager** den Bindungspunkt aus, an den Sie die Richtlinie binden möchten**. Es stehen folgende Optionen zur Auswahl:
   - **Global überschreiben.** Richtlinien, die an diesen Bindpunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen auf der NetScaler-Appliance und werden vor allen anderen Richtlinien angewendet.
   - **LB Virtueller Server.** Richtlinien, die an einen virtuellen Lastausgleichsserver gebunden sind, werden nur auf den Datenverkehr angewendet, der von diesem virtuellen Lastausgleichsserver verarbeitet wird, und sie werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie LB Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Load-Balancing-Server auswählen, an den Sie diese Richtlinie binden möchten.
   - **CS Virtueller Server.** Richtlinien, die an einen virtuellen Content Switching-Server gebunden sind, werden nur auf den Datenverkehr angewendet, der von diesem virtuellen Content Switching-Server verarbeitet wird, und sie werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie CS Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Content Switching-Server auswählen, an den Sie diese Richtlinie binden möchten.
   - **Standard Global.** Richtlinien, die an diesen Bindpunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der NetScaler-Appliance.
   - **Richtlinien-Etikett.** Richtlinien, die an ein Richtlinienlabel gebunden sind, verarbeiten den Datenverkehr, den das Richtlinienlabel an sie weiterleitet. Das Richtlinienlabel bes-

timmt die Reihenfolge, in der Richtlinien auf diesen Verkehr angewendet werden.

4. Wählen Sie Richtlinie einfügen aus, um eine neue Zeile einzufügen und eine Dropdownliste mit allen verfügbaren, ungebundenen URL-Transformationsrichtlinien anzuzeigen.
5. Wählen Sie die Richtlinie aus, die Sie binden möchten, oder wählen Sie Neue Richtlinie, um eine neue Richtlinie zu erstellen. Die Richtlinie, die Sie ausgewählt oder erstellt haben, wird in die Liste der global gebundenen URL-Transformationsrichtlinien eingefügt.
6. Nehmen Sie weitere Anpassungen an der Bindung vor.
   - Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten neu generieren auswählen, um die Prioritäten gleichmäßig neu zu nummerieren.
   - Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld Transformationsrichtlinie konfigurieren zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.
   - Um den Goto-Ausdruck festzulegen, doppelklicken Sie auf das Feld in der Spaltenüberschrift Goto Expression, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
   - Um die Option Invoke einzustellen, doppelklicken Sie auf das Feld in der Spaltenüberschrift Invoke, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
7. Wiederholen Sie die Schritte 3 bis 6, um weitere URL-Transformationsrichtlinien hinzuzufügen, die Sie global binden möchten.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

RADIUS-Unterstützung für die Rewrite-Funktion

May 11, 2023

Die NetScaler-Ausdruckssprache umfasst Ausdrücke, mit denen Informationen aus RADIUS-Nachrichten in Anfragen und Antworten extrahiert und bearbeitet werden können. Mit diesen Ausdrücken können Sie die Rewrite-Funktion verwenden, um Teile einer RADIUS-Nachricht zu ändern, bevor sie an ihr Ziel gesendet wird. Ihre Rewrite-Richtlinien und -Aktionen können jeden Ausdruck verwenden, der für eine RADIUS-Nachricht geeignet oder relevant ist. Mit den verfügbaren Ausdrücken können Sie den RADIUS-Nachrichtentyp identifizieren, ein beliebiges Attributwertpaar (AVP) aus der Verbindung extrahieren und RADIUS-AVPs ändern. Sie können auch Richtlinienlabels für RADIUS-Verbindungen erstellen.

Sie können die neuen RADIUS-Ausdrücke in Rewrite-Regeln für eine Reihe von Zwecken verwenden. Sie könnten zum Beispiel:

- Entfernen Sie den Abschnitt Domäne\ des RADIUS-Benutzernamens AVP, um Single Sign-On (SSO) zu vereinfachen.
- Fügen Sie einen anbieterspezifischen AVP ein, z. B. das MSISDN-Feld, das im Betrieb von Telefongesellschaften verwendet wird, um Abonnenteninformationen zu enthalten.

Sie können auch Richtlinienlabels erstellen, um bestimmte Arten von RADIUS-Anfragen anhand einer Reihe von Richtlinien weiterzuleiten, die für diese Anfragen geeignet sind.

> **Hinweis**:
>
> RADIUS for Rewrite weist die folgenden Einschränkungen auf:

- Der NetScaler signiert keine neu geschriebenen RADIUS-Anfragen oder -Antworten erneut. Wenn der RADIUS-Authentifizierungsserver signierte RADIUS-Nachrichten benötigt, schlägt die Authentifizierung fehl.
- Die derzeit verfügbaren RADIUS-Ausdrücke funktionieren nicht mit RADIUS-IPv6-Attributen.

In der NetScaler-Dokumentation für Ausdrücke, die RADIUS unterstützen, wird davon ausgegangen, dass Sie mit der grundlegenden Struktur und dem Zweck der RADIUS-Kommunikation vertraut sind. Wenn Sie weitere Informationen zu RADIUS benötigen, lesen Sie in der RADIUS-Serverdokumentation nach oder suchen Sie online nach einer Einführung in das RADIUS-Protokoll.

Konfiguration von Rewrite-Richtlinien für RADIUS

Das folgende Verfahren verwendet die NetScaler-Befehlszeile, um eine Neuschreibaktion und -richtlinie zu konfigurieren und die Richtlinie an einen für das Umschreiben spezifischen globalen Bindungspunkt zu binden.

Gehen Sie wie folgt vor, um eine Rewrite-Aktion und -Richtlinie zu konfigurieren und die Richtlinie zu binden:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add rewrite action <actName> <actType>`
- `add rewrite policy <polName> <rule> <actName>`
- `bind rewrite policy <polName> <priority> <nextExpr> -type <bindPoint>`
  wobei `<bindPoint>` steht für einen der Rewrite-spezifischen globalen Bindungspunkte.

RADIUS-Ausdrücke für Rewrite

In einer Rewrite-Konfiguration können Sie die folgenden NetScaler-Ausdrücke verwenden, um auf verschiedene Teile einer RADIUS-Anfrage oder -Antwort zu verweisen.

Identifizierung des Verbindungstyps:

- `RADIUS.IS_CLIENT`

  Gibt TRUE zurück, wenn es sich bei der Verbindung um eine RADIUS-Clientnachricht (Anfrage) handelt.

- `RADIUS.IS_SERVER`

  Gibt TRUE zurück, wenn es sich bei der Verbindung um eine RADIUS-Servernachricht (Antwort) handelt.

Ausdrücke anfordern:

- `RADIUS.REQ.CODE`

  Gibt die Zahl zurück, die dem RADIUS-Anforderungstyp entspricht. Eine Ableitung der Klasse num_at. Eine RADIUS-Zugriffsanfrage würde beispielsweise 1 (eins) zurückgeben. Eine RADIUS-Buchhaltungsanfrage würde 4 zurückgeben.

- `RADIUS.REQ.LENGTH`

  Gibt die Länge der RADIUS-Anfrage einschließlich des Headers zurück. Eine Ableitung der Klasse num_at.

- `RADIUS.REQ.IDENTIFIER`

  Gibt den RADIUS-Anforderungsbezeichner zurück, eine Nummer, die jeder Anfrage zugewiesen wird und die es ermöglicht, die Anfrage mit der entsprechenden Antwort abzugleichen. Eine Ableitung der Klasse
  num_at.

- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`

  Gibt den Wert des ersten Auftretens dieses AVP als Zeichenfolge vom Typ
  text_t zurück.

- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`

  Gibt die angegebene Instanz des AVP als Zeichenfolge vom Typ raVP_T zurück. Ein bestimmter RADIUS-AVP kann in einer RADIUS-Nachricht mehrfach vorkommen. INSTANCE (0) gibt die erste Instanz zurück, INSTANCE (1) gibt die zweite Instanz zurück und so weiter, bis zu sechzehn Instanzen.

- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`

  Gibt den Wert der angegebenen Instanz des AVP als Zeichenfolge vom Typ
  text_t zurück.

- `RADIUS.REQ.AVP(<AVP code no>).COUNT`

  Gibt die Anzahl der Instanzen eines bestimmten AVP in einer RADIUS-Verbindung als Ganzzahl zurück.

- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`

  Gibt TRUE zurück, wenn der angegebene AVP-Typ in der Nachricht vorhanden ist, oder FALSE, wenn dies nicht der Fall ist.

Antwortausdrücke:

RADIUS-Antwortausdrücke sind identisch mit RADIUS-Anforderungsausdrücken, mit der Ausnahme, dass RES REQ ersetzt.

Typisierungen von AVP-Werten:

Der ADC unterstützt Ausdrücke zur Typisierung von RADIUS-AVP-Werten in die Datentypen Text, Integer, unsigned Integer, Long, unsigned Long, IPv4-Adresse, IPv6-Adresse, IPv6-Adresse, IPv6-Präfix und Zeit. Die Syntax ist dieselbe wie bei anderen NetScaler-Typecast-Ausdrücken.

Beispiel:

Der ADC unterstützt Ausdrücke zur Typisierung von RADIUS-AVP-Werten in die Datentypen Text, Integer, unsigned Integer, Long, unsigned Long, IPv4-Adresse, IPv6-Adresse, IPv6-Adresse, IPv6-Präfix und Zeit. Die Syntax ist dieselbe wie bei anderen NetScaler-Typecast-Ausdrücken.

```
1 RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
2 <!--NeedCopy-->
```

Ausdrücke vom Typ AVP:

Der NetScaler unterstützt Ausdrücke zum Extrahieren von RADIUS-AVP-Werten mithilfe der in RFC2865 und RFC2866 beschriebenen zugewiesenen Integer-Codes. Sie können auch Text-Aliase verwenden, um dieselbe Aufgabe zu erledigen. Es folgen einige Beispiele.

- `RADIUS.REQ.AVP (1).VALUE or RADIUS.REQ.USERNAME.value`

  Extrahiert den RADIUS-Benutzernamenwert.

- `RADIUS.REQ.AVP (4). VALUE or RADIUS.REQ. ACCT\\_SESSION\\_ID.value`

  Extrahiert die accT-Session-ID AVP (Code 44) aus der Nachricht.

- `RADIUS.REQ.AVP (26). VALUE or RADIUS.REQ.VENDOR\\_SPECIFIC.VALUE`

  Extrahiert den herstellerspezifischen Wert.

Die Werte der am häufigsten verwendeten RADIUS-AVPs können auf dieselbe Weise extrahiert werden.

RADIUS-Bindepunkte:

Vier globale Bindungspunkte sind für Richtlinien verfügbar, die RADIUS-Ausdrücke enthalten.

- `RADIUS_REQ_OVERRIDE`

  Warteschlange für Richtlinien zur Priorität/Außerkraftsetzung von Anfragen.

- RADIUS_REQ_DEFAULT

  Standardwarteschlange für Anforderungsrichtlinien.

- RADIUS_RES_OVERRIDE

  Warteschlange für Antwortrichtlinien zur Priorität/Außerkraftsetzung.

- RADIUS_RES_DEFAULT

  Standardwarteschlange für Antwortrichtlinien.

Spezifische RADIUS-Rewrite-Ausdrücke:

- RADIUS.NEW_AVP

  Gibt den angegebenen RADIUS-AVP als Zeichenfolge zurück.

- RADIUS.NEW_AVP_INTEGER32

  Gibt den angegebenen RADIUS-AVP als Ganzzahl zurück.

- RADIUS.NEW_AVP_UNSIGNED32

  Gibt den angegebenen RADIUS-AVP als Ganzzahl ohne Vorzeichen zurück.

- RADIUS.NEW_VENDOR_SPEC_AVP(<ID>, <definition>)

  Fügt der Verbindung die angegebenen erweiterten herstellerspezifischen AVPs hinzu. Ersetzen Sie durch eine lange Zahl. <ID> <definition>Ersetzen Sie den AVP durch eine Zeichenfolge, die die Daten enthält.

- RADIUS.REQ.AVP_START

  Gibt die Position zwischen dem Ende des RADIUS-Headers und dem Anfang der AVPs zurück. Wird in Rewrite-Aktionen verwendet.

  Beispiel:

```
1     add rewrite action insert1 insert_after radius.req.avp_start radius
          .new_avp(33, "NEW AVP")
2 <!--NeedCopy-->
```

- RADIUS.REQ.AVP_END

  Gibt die Position am Ende der Radius-Nachricht (oder mit anderen Worten am Ende aller AVPs) in der Radius-Nachricht zurück. Wird verwendet, wenn Rewrite-Aktionen ausgeführt werden.

  Beispiel:

```
1     add rewrite action insert2 insert_before radius.req.avp_end "radius
          .new_avp(33, "NEW AVP")"
2 <!--NeedCopy-->
```


- `RADIUS.REQ.AVP_LIST`

  Gibt die Position am Anfang der AVPs in einer RADIUS-Nachricht und die Länge der RADIUS-Nachricht ohne den Header zurück. Mit anderen Worten, gibt alle AVPs in einer RADIUS-Nachricht zurück. Wird verwendet, um Rewrite-Aktionen auszuführen.

  Beispiel:

```
1     add rewrite action insert3 insert_before_all radius.req.avp_list "
         radius.new_avp(33, "NEW AVP")" -search "avp(33)"
2  <!--NeedCopy-->
```

Gültige Rewrite-Action-Typenfür RADIUS:

Die Rewrite-Aktionstypen, die mit RADIUS-Ausdrücken verwendet werden können, sind:

- INSERT_AFTER
- INSERT_BEFORE
- INSERT_AFTER_ALL
- INSERT_BEFORE_ALL
- LÖSCHEN
- DELETE_ALL
- REPLACE
- REPLACE_ALL

Alle `INSERT_ actions` können verwendet werden, um einen RADIUS-AVP in eine RADIUS-Verbindung einzufügen.

Anwendungsfälle

Im Folgenden finden Sie Anwendungsfälle für RADIUS mit Rewrite.

Den Benutzernamen AVP umschreiben

Um die Rewrite-Funktion so zu konfigurieren, dass die Zeichenfolge Domain\ string aus dem RADIUS-Benutzernamen AVP entfernt wird, erstellen Sie zunächst eine REWRITE-REPLACE-Aktion, wie im Beispiel unten gezeigt. Verwenden Sie die Aktion in einer Rewrite-Richtlinie, die alle RADIUS-Anforderungen auswählt. Binden Sie die Richtlinie an einen globalen Bindungspunkt. Wenn Sie dies tun, legen Sie die Priorität auf die entsprechende Stufe fest, damit alle Blockier- oder Ablehnungsrichtlinien zuerst wirksam werden. Stellen Sie jedoch sicher, dass alle Anfragen, die nicht blockiert oder abgelehnt wurden, neu geschrieben werden. Setzen Sie den Goto-Ausdruck (GoToPriorityExpr) auf NEXT, um die Richtlinienauswertung fortzusetzen, und hängen Sie die Richtlinie an die RADIUS_REQ_DEFAULT-Warteschlange an.

Beispiel:


```
add rewrite action rwActRadiusDomainDel replace radius.req.user_name q/
    RADIUS.NEW_AVP(1,RADIUS.REQ.USER_NAME.VALUE.AFTER_STR(" "))/
add rewrite policy RadiusRemoveDomainPol true rwActRadiusDomainDel
<!--NeedCopy-->
```

> **Hinweis**:
>
> Die Rewrite-Richtlinie für RADIUS gilt nicht für einen virtuellen Gateway-Server. Wenn ein virtueller Gateway-Server für den Lastenausgleich verwendet wird, muss RADIUS konfiguriert und die Rewrite-Richtlinie muss an einen virtuellen RADIUS-Lastenausgleichsserver gebunden werden.

Einen herstellerspezifischen AVP einfügen

Um die Rewrite-Aktion so zu konfigurieren, dass ein herstellerspezifisches AVP eingefügt wird, das den Inhalt des MSISDN-Feldes enthält, erstellen Sie zunächst eine INSERT-Aktion zum Umschreiben, die das MSISDN-Feld in die Anfrage einfügt. Verwenden Sie die Aktion in einer Rewrite-Richtlinie, die alle RADIUS-Anforderungen auswählt. Binden Sie die Richtlinie an eine globale Richtlinie, indem Sie die Priorität auf eine entsprechende Ebene und die anderen Parameter festlegen, wie im folgenden Beispiel gezeigt.

Beispiel:

```
add rewrite action rwActRadiusInsMSISDN insert_after radius.req.
    avp_start RADIUS.NEW_VENDOR_SPEC_AVP(<VENDOR ID>, "RADIUS.NEW_AVP(<
    Attribute Code>, <MSISDN>)")
add rewrite policy rwPolRadiusInsMSISDN true rwActRadiusInsMSISDN
bind rewrite global rwPolRadiusInsMSISDN 100 NEXT -type
    RADIUS_REQ_DEFAULT
<!--NeedCopy-->
```

Durchmesser-Unterstützung für Rewrite

May 11, 2023

Die Rewrite-Funktion unterstützt jetzt das Diameter-Protokoll. Sie können Rewrite so konfigurieren, dass Diameter-Anfragen und -Antworten wie HTTP- oder TCP-Anfragen und -Antworten geändert werden. So können Sie Rewrite verwenden, um den Fluss von Diameter-Anfragen zu verwalten und die erforderlichen Änderungen vorzunehmen. Wenn beispielsweise der Wert „Origin-Host“ in einer Diameter-Anfrage unangemessen ist, können Sie Rewrite verwenden, um ihn durch einen Wert zu ersetzen, der für den Diameter-Server akzeptabel ist.

So konfigurieren Sie Rewrite, um eine Durchmesseranforderung zu ändern

Um die Rewrite-Funktion so zu konfigurieren, dass der Origin-Host in einer Durchmesseranforderung durch einen anderen Wert ersetzt wird, geben Sie an der Befehlszeile die folgenden Befehle ein:

- <add rewrite action <actname> replace “DIAMETER.REQ.AVP(264,\“NetScaler.example.net\”)”
  Ersetzen Sie <actname> mit dem Namen für Ihre neue Aktion. Der Name kann aus einem bis 127 Zeichen bestehen und Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie für netscaler.example.net den Host-Origin, den Sie verwenden möchten, anstelle des ursprünglichen Hostnamens.
- add rewrite policy <polname> “diameter.req.avp(264).value.eq(\“host.example.com\”)” <actname>
  Ersetzen Sie <polname> mit dem Namen für Ihre neue Aktion. Wie bei <actname> kann der Name aus 1 bis 127 Zeichen bestehen und Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie host.example.com durch den Namen des Host-Origin, den Sie ändern möchten. Ersetzen Sie <actname> durch den Namen der Aktion, die Sie gerade erstellt haben.
- bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST
  Geben Sie für <vservername> den Namen des virtuellen Load Balancing-Servers ein, an den Sie die Richtlinie binden möchten. Ersetzen Sie <polname> durch den Namen der Richtlinie, die Sie gerade erstellt haben. Ersetzen Sie <priority> durch eine Priorität für die Richtlinie.

Beispiel:

Um eine Rewrite-Aktion und -Richtlinie zu erstellen, um alle Diameter Host-Origins von „host.example.com“ in „Netscaler.Example.net“ zu ändern, könnten Sie die folgende Aktion und Richtlinie hinzufügen und die Richtlinie wie gezeigt binden.

```
1 > add rewrite action rw_act_replace_avp replace "diameter.req.avp(264)"
     "diameter.new.avp(264,"NetScaler.example.net")"
2 > add rewrite policy rw_diam_pol "diameter.req.avp(264).value.eq("
    client.realm2.net")" rw_act_replace_avp
3 > bind lb vserver vs1 -policyName rw_diam_pol -priority 10 -type
    REQUEST
4
5 Done
6 <!--NeedCopy-->
```

DNS-Unterstützung für das Rewrite-Feature

May 11, 2023

Sie können die Rewrite-Funktion so konfigurieren, dass DNS-Anfragen und -Antworten geändert werden, wie Sie es für HTTP- oder TCP-Anfragen und -Antworten tun würden. Sie können Rewrite verwenden, um den Fluss von DNS-Anfragen zu verwalten und die erforderlichen Änderungen im Header oder im Antwortbereich vorzunehmen. Wenn in der DNS-Antwort beispielsweise kein AA-Bit im Header-Flag gesetzt ist, können Sie Rewrite verwenden, um das AA-Bit in der DNS-Antwort festzulegen und es an den Client zu senden.

DNS-Ausdrücke

In einer Rewrite-Konfiguration können Sie die folgenden NetScaler Ausdrücke verwenden, um auf verschiedene Teile einer DNS-Anforderung oder -Antwort zu verweisen:

Siehe Ausdrücke und Beschreibungen

DNS-Bindungspunkte

Die folgenden globalen Bindungspunkte sind für Richtlinien verfügbar, die DNS-Ausdrücke enthalten.

Punkte binden	Beschreibung
DNS_REQ_OVERRIDE	Überschreiben Sie die Warteschlange für Anforderungsrichtlinien.
DNS_REQ_DEFAULT	Standardwarteschlange für Anforderungsrichtlinien.
DNS_RES_OVERRIDE	Überschreiben Sie die Warteschlange für Antwortrichtlinien.
DNS_RES_DEFAULT	Standardwarteschlange für Antwortrichtlinien.

Zusätzlich zu den Standardbindungspunkten können Sie Richtlinienlabels vom Typ DNS_REQ oder DNS_RES erstellen und DNS-Richtlinien an diese binden.

Aktionstypen für DNS neu schreiben

- **replace_dns_answer_section —Diese Aktion ersetzt den Abschnitt**DNS-Antworten durch den definierten Ausdruck in der DNS-Richtlinie.
- **replace_dns_header_field**—Überprüft den Opcode-Typ in der DNS-Anfrage. Gibt True oder False zurück und gibt an, ob der Opcode-Typ in der DNS-Anfrage mit dem angegebenen Opcode-Typ übereinstimmt. Diese Aktion ersetzt den DNS-Header-Abschnitt durch den definierten Ausdruck in der DNS-Richtlinie.

Konfiguration von Rewrite-Richtlinien für DNS

Das folgende Verfahren verwendet die NetScaler-Befehlszeile, um eine Neuschreibaktion und -richtlinie zu konfigurieren und die Richtlinie an einen für das Umschreiben spezifischen globalen Bindungspunkt zu binden.

Konfigurieren Sie die Rewrite-Aktion und -Richtlinie und binden Sie die Richtlinie für DNS

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

1. `add rewrite action <actName> <actType>`

   Für <actname>, ersetzen Sie Ihre neue Aktion durch einen Namen. Der Name kann 1 bis 127 Zeichen lang sein und Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Geben Sie für <actType>die für DNS-Ausdrücke bereitgestellten Rewrite-Aktionstypen an.

2. `add rewrite policy <polName> <rule> <actName>`

   Für <polname>, ersetzen Sie einen Namen für Ihre neue Richtlinie. Denn <actname>der Name kann 1 bis 127 Zeichen lang sein und Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie durch den Namen der Aktion, die Sie gerade erstellt haben. <actname>

3. `bind rewrite global <polName> <priority> <gotoPriorityExpression> -type <bindPoint>`

   <polName>Ersetzen Sie ihn durch den Namen der Richtlinie, die Sie gerade erstellt haben. Geben Sie für <priority>die Priorität der Richtlinie an. <bindPoint>Ersetzen Sie durch einen der rewrite-spezifischen globalen Bindungspunkte.

Beispiel:

Stellen Sie die AA-Bit-DNS-Anfrage ein, um den virtuellen Server mit Lastenausgleich zu verwalten.

Mit den folgenden Befehlen wird die NetScaler-Appliance so konfiguriert, dass sie als autorisierender DNS-Server für alle von ihr bereitgestellten Abfragen fungiert.

```
add rewrite action set_aa replace_dns_header_field dns.req.header.flags
    .set(aa)
add rewrite policy pol !dns.req.header.flags.is_set(aa)  set_aa
bind rewrite global  pol  100  -type dns_res_override
<!--NeedCopy-->
```

Ändern Sie die Antwortantwort und den Header-Abschnitt.

Wenn der Server mit einer NX-Domäne antwortet, können Sie die Rewrite-Aktion so einrichten, dass die Antwort durch die angegebene IP-Adresse ersetzt wird. Ein NOPOLICY-REWRITE ermöglicht es Ihnen, eine externe Bank aufzurufen, ohne einen Ausdruck zu verarbeiten (eine Regel). Bei diesem

Eintrag handelt es sich um eine Scheinrichtlinie, die keine Regel enthält, den Eintrag jedoch an ein Richtlinienlabel oder an virtuelle Serverspezifische Policy-Banks weiterleitet.

```
add rewrite action set_aa_res replace_dns_header_field "dns.res.header.flags.set(aa)"
add rewrite action modify_nxdomain_res replace_dns_answer_section "dns.new_rrset_a("10.102.218.160",300)"
add rewrite policy set_res_aa true set_aa_res
add add rewrite policy modify_answer "dns.RES.HEADER.RCODE.EQ(nxdomain) && dns.RES.QUESTION.TYPE.EQ(A)"
modify_nxdomain_res
add rewrite policylabel MODIFY_NODATA dns_res
bind rewrite policylabel MODIFY_NODATA modify_answer 10 END
bind rewrite policylabel MODIFY_NODATA set_res_aa 11 END
bind lb vserver v1 -policyName NOPOLICY-REWRITE -priority 11 -gotoPriorityExpression END -type
RESPONSE -invoke policylabel MODIFY_NODATA
<!--NeedCopy-->
```

Einschränkungen:

- Rewrite-Richtlinien werden nur ausgewertet, wenn die NetScaler-Appliance als DNS-Proxyserver konfiguriert ist und ein Cachefehler vorliegt.
- Wenn das Flag Recursion Available (RA) im Header auf JA gesetzt ist, wird das RA-Flag bei den Umschreibungen nicht geändert.
- Wenn das RA-Flag im Header auf YES gesetzt ist, wird das CD-Flag im Header unabhängig von einer Umschreibung geändert.

MQTT-Unterstützung für Rewrite

May 11, 2023

Die Rewrite-Funktion unterstützt das MQTT-Protokoll. Sie können Rewrite-Richtlinien so konfigurieren, dass sie Aktionen basierend auf den Parametern in den MQTT-Clientanforderungen und Serverantworten ausführen.

Rewrite-Aktion für MQTT

Die Rewrite-Aktion für MQTT zeigt die Änderungen an der MQTT-Anforderung oder -Antwort an, bevor sie an einen Server oder Client gesendet wurde.

Ausdruck:


```
add rewrite action <name> <rewrite_type> <target> <rewrite_action>
```

Rewrite-Typ für MQTT

Abhängig vom Typ der verwendeten Regel zum Neuschreiben von Ausdrücken werden die folgenden MQTT-Rewrite-Typen unterstützt:

- `replace_mqtt`
- `insert_before_mqtt`
- `insert_after_mqtt`
- `delete_mqtt`
- `insert_mqtt`

Rewrite-Ziel für MQTT

In den folgenden Beispielbeispielen verwendet MQTT-Rewrite Richtlinienausdrücke, um den Teil der zu ändernden Anforderung (Ziel) und die durchzuführende Änderung (Zeichenfolgenausdruck) anzugeben:

- Rewrite einer Client-ID im Verbindungspaket über den Aktionstyp `replace_mqtt`.

  ```
  add rewrite action rwact1 replace_mqtt MQTT.CONNECT.CLIENTID "\"xyz\""
  ```

- Rewrite von Topic in der Veröffentlichungsanforderung über den Aktionstyp `replace_mqtt`.

  ```
  add rewrite action rwact1 replace_mqtt MQTT.PUBLISH.TOPIC "\"testing/
  test123\""
  ```

- Rewrite zum Einfügen einer Eigenschaft mit dem Aktionstyp insert_mqtt.

  ```
  add rewrite action rwact1 insert_mqtt MQTT.NEW_PROPERTY("prop1", "test"
  )
  ```

- Löschen Sie ein Thema mit dem Aktionstyp delete_mqtt.

  ```
  add rewrite action rwact2 delete_mqtt MQTT.SUBSCRIBE.TOPIC_FILTERS.
  TOPIC(1)
  ```

Rewrite-Aktion für MQTT

Im Folgenden sind die vordefinierten Rewrite-Aktionen für MQTT aufgeführt:

- `MQTT.NEW_KEEPALIVE(interval)`
- `MQTT.NEW_PACKET_IDENTIFIER(packetID)`
- `MQTT.NEW_REASON_CODE(retCode)`
- `MQTT.NEW_PUBLISH(topic_name, payload)`

- `MQTT.NEW_CONNECT_USERNAME(username)`
- `MQTT.NEW_CONNECT_WILL_MESSAGE(will_topic, will_payload, will_Qos, will_retain)`
- `MQTT.NEW_TOPIC(topic, qos)`
- `MQTT.NEW_TOPIC(topic)`
- `MQTT.NEW_PROPERTY(key, value)`

Beispiel für die vordefinierte Rewrite-Aktion:

```
add rewrite action rwact1 replace_mqtt MQTT.CONNECT.KEEPALIVE MQTT.NEW_KEEPALIVE (90)
```

Beispiel für die benutzerdefinierte Rewrite-Aktion:

```
add rewrite action rwact1 replace_mqtt MQTT.CONNECT.USERNAME "\"user1\""
```

Rewrite-Richtlinie für MQTT

Eine Rewrite-Richtlinie für MQTT besteht aus einer Regel und einer Aktion. Die Regel bestimmt den MQTT-Datenverkehr, auf den das Rewrite angewendet wird, und die Aktion bestimmt die von der NetScaler-Appliance auszuführende Aktion.

Ausdruck:

```
add rewrite policy <name> <rewrite_rule> <rewrite_action>
```

Beispiel:

```
add rewrite action insert_mqtt_username insert_mqtt MQTT.NEW_CONNECT_USERNAME ("user1")

add rewrite policy rewrite_mqtt_username "MQTT.COMMAND.EQ(CONNECT)&& MQTT.CONNECT.USERNAME.LENGTH.EQUALS(0)insert_mqtt_username
```

Bindungspunkte für MQTT

Sie können eine Rewrite-Richtlinie global oder an einen bestimmten virtuellen Lastausgleichsserver oder virtuellen Content Switching-Server binden.
Im Folgenden sind die globalen Bindepunkte:

- `MQTT_REQ_DEFAULT`
- `MQTT_REQ_OVERRIDE`
- `MQTT_RES_DEFAULT`
- `MQTT_RES_OVERRIDE`

Ausdruck:

- `bind rewrite global <policyName> <priority> [-type MQTT_REQ_OVERRIDE | MQTT_REQ_DEFAULT | MQTT_RES_OVERRIDE | MQTT_RES_DEFAULT]`
- `bind lb|cs vserver <virtualServerName> -policyName <policyName> -priority <positiveInteger> -type REQUEST|RESPONSE`

Beispiel:

- `bind rewrite global pol1 10 -type MQTT_REQ_DEFAULT`
- `add/bind lb vserver v1 -policyName pol1 -type reqUEST -priority 10`

Konfigurieren einer Rewrite-Richtlinie für MQTT

Um eine Rewrite-Richtlinie zu konfigurieren, führen Sie die Schritte aus und geben Sie die Befehle an der Eingabeaufforderung ein:

1. Aktivieren Sie Rewrite auf der NetScaler-Appliance.

   ```
   enable ns feature REWRITE
   ```

2. Fügen Sie eine Rewrite-Aktion hinzu.

   ```
   add rewrite action rwact1 replace_mqtt MQTT.CONNECT.KEEPALIVE MQTT.NEW_KEEPALIVE(10)
   ```

3. Fügen Sie eine Rewrite-Richtlinie hinzu.

   ```
   add rewrite policy pol1 MQTT.COMMAND.EQ(CONNECT)rwact1
   ```

4. Konfigurieren eines virtuellen MQTT-Lastausgleichsservers.

   ```
   add lb vserver v1 MQTT 1.1.1.1 1883
   ```

5. Binden Sie die Rewrite-Richtlinie global oder an einen bestimmten virtuellen Lastausgleichsserver.

   ```
   bind rewrite global pol1 10 -type MQTT_REQ_DEFAULT
   ```

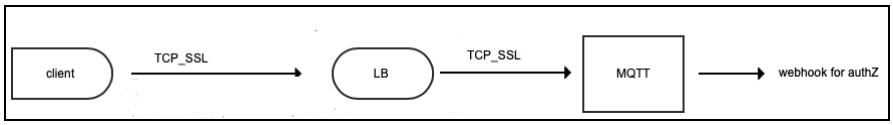
   ```
   add/bind lb vserver v1 -policyName pol1 -type REQUEST -priority 10
   ```

Anwendungsfall 1: Ersetzen Sie den Benutzernamen in der MQTT CONNECT-Nachricht durch den Zertifikatsnamen

Der Administrator kann eine MQTT-Rewrite-Richtlinie konfigurieren, um den Benutzernamen durch den Zertifikatsnamen des Clients zu ersetzen.

Betrachten wir ein Beispiel. Die Clientanfrage hat eine `MQTT CONNECT` Nachricht, die den Benutzernamen als “admin” enthält. Dieser Benutzername muss durch die Seriennummer (16-stellig) ersetzt werden, die aus dem Clientzertifikat (Zertifikatsname) extrahiert wird.

Die folgende Abbildung zeigt den Arbeitsablauf:



1. Eine Transport Control Protocol (TCP) -Anforderung wird an den Load Balancer gesendet.
2. Im Load Balancer wird der Benutzername durch den Zertifikatsnamen ersetzt.
3. Die Anfrage wird an den MQTT-Broker weitergeleitet.
4. Dieser neue Benutzername wird für die Autorisierung über die Webhook-Nutzlast verwendet.

Beispielkonfiguration:

```
add rewrite action mqtt_rw_unameact1 replace_mqtt MQTT.CONNECT.USERNAME
CLIENT.SSL.CLIENT_CERT.SERIALNUMBER

add rewrite policy mqtt_rw_uname_pol1 "MQTT.COMMAND.EQ(CONNECT)"mqtt_rw_unameact1


bind cs vserver mqtt_frontend_cs -policyName mqtt_rw_uname_pol1 -priority
10 -gotoPriorityExpression END -type REQUEST
```

Anwendungsfall 2: Abonnement für ein neues THEMA bereitstellen

Der Administrator kann ein Abonnement für ein neues THEMA bereitstellen. Betrachten wir ein Beispiel. Eine Kundenanfrage hat ein Abonnement für THEMA 1. Der Administrator kann eine Rewrite-Richtlinie konfigurieren, um ein Abonnement für ein neues THEMA 2 bereitzustellen. Das Abonnement kann davor oder danach eingefügt werden.

Beispielkonfiguration:

- `add rewrite action act2 insert_before_mqtt MQTT.TOPIC_FILTERS.TOPIC(1) MQTT.NEW_TOPIC(topic2, 2)`
- `add rewrite policy policy2 “MQTT.COMMAND.EQ(SUBSCRIBE)&& MQTT.SUBSCRIBE . TOPIC_FILTERS.TOPIC.CONTAINS(\"test\")"act2`

String-Maps

May 11, 2023

Sie können Zeichenfolgenzuordnungen verwenden, um einen Musterabgleich in allen NetScaler-Funktionen durchzuführen, die die Standardrichtliniensyntax verwenden. Eine String-Map ist eine

NetScaler-Entität, die aus Schlüssel-Wert-Paaren besteht. Die Schlüssel und Werte sind Zeichenfolgen im ASCII- oder UTF-8-Format. Beim Stringvergleich werden zwei neue Funktionen verwendet, `MAP_STRING(<string_map_name>)` und `IS_STRINGMAP_KEY(<string_map_name>)`.

Eine Richtlinienkonfiguration, die Zeichenfolgenzuordnungen verwendet, ist besser als eine, die Zeichenfolgenabgleich durch Richtlinienausdrücke durchführt, und Sie benötigen weniger Richtlinien, um Zeichenfolgenabgleich mit einer großen Anzahl von Schlüssel-Wert-Paaren durchzuführen. String-Maps sind außerdem intuitiv, einfach zu konfigurieren und führen zu einer kleineren Konfiguration.

So funktionieren String-Maps

String-Maps ähneln in ihrer Struktur Mustersätzen (ein Mustersatz definiert eine Zuordnung von Indexwerten zu Zeichenfolgen; eine String-Map definiert eine Zuordnung von Zeichenfolgen zu Zeichenfolgen) und die Konfigurationsbefehle für String-Maps (Befehle wie Hinzufügen, Bind, Unbind, Remove und Show) ähneln syntaktisch der Konfiguration Befehle für Mustersätze. Ebenso wie bei Indexwerten in einem Mustersatz muss jeder Schlüssel in einer String-Map in der gesamten Map eindeutig sein. Die folgende Tabelle zeigt eine String-Map namens url_string_map, die URLs als Schlüssel und Werte enthält.

Schlüssel	Wert
/url_1.html	`http://www.redirect_url_1.com/url_1.html`
/url_2.html	`http://www.redirect_url_2.com/url_2.html`
/url_3.html	`http://www.redirect_url_1.com/url_1.html`

Tabelle 1. String-Map “url_string_map”

In der folgenden Tabelle werden die beiden Funktionen beschrieben, die eingeführt wurden, um den Zeichenfolgenabgleich mit Schlüsseln in einer String-Map zu ermöglichen. Der Zeichenfolgenabgleich wird immer mit den Schlüsseln durchgeführt. Zusätzlich führen die folgenden Funktionen einen Vergleich zwischen den Schlüsseln in der String-Map und der vollständigen Zeichenfolge durch, die vom Ausdruck-Präfix zurückgegeben wird. Die Beispiele in den Beschreibungen beziehen sich auf das vorangehende Beispiel.

Vollendete Informationen zu den beiden Funktionen, die zum Aktivieren des String-Abgleichs mit Schlüsseln in einer String-Map eingeführt wurden, finden Sie unter String Map Funktionstabelle pdf.

Konfigurieren einer Zeichenfolgenzuordnung

Sie erstellen zuerst eine String-Map und binden dann Schlüssel-Wert-Paare daran. Sie können eine String-Map über die Befehlszeilenschnittstelle (CLI) oder das Konfigurationsdienstprogramm erstellen.

So konfigurieren Sie eine String-Map über die Befehlszeile

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Erstellen Sie eine String-Map.

```
add policy stringmap <name> -comment <string>
```

1. Bindet ein Schlüssel-Wert-Paar an die String-Map.

```
bind policy stringmap <name> <key> <value> [-comment <string>]
```

Beispiel:

```
1 bind policy stringmap url_string_map1 "/url_1.html" "http://www.
     redirect_url_1.com/url_1.html"
2 <!--NeedCopy-->
```

So konfigurieren Sie eine Zeichenfolgenzuordnung über die NetScaler GUI

Navigieren Sie zu **AppExpert** > **String Maps**, klicken Sie auf **Hinzufügen** und geben Sie die entsprechenden Details an.

Beispiel: Responder Policy mit einer Umleitungsaktion

Der folgende Anwendungsfall beinhaltet eine Responder Policy mit einer Umleitungsaktion. Im Beispiel unten erstellen die ersten vier Befehle die String-Map url_string_map und binden die drei im vorherigen Beispiel verwendeten Schlüssel-Wert-Paare. Nachdem Sie die Map erstellt und die Schlüssel-Wert-Paare gebunden haben, erstellen Sie eine Responder Action (act_url_redirects), die den Client zur entsprechenden URL in der String-Map oder zu www.default.com umleitet. Sie konfigurieren auch eine Responder Policy (pol_url_directs), die prüft, ob angeforderte URLs mit einem der Schlüssel in url_string_map übereinstimmen, und dann die konfigurierte Aktion ausführt. Schließlich binden Sie die Responder Policy an den virtuellen Content Switching-Server, der die auszuwertenden Clientanforderungen empfängt.

```
add stringmap url_string_map
```

```
bind stringmap url_string_map /url_1.html http://www.redirect_url_1.com/
url_1.html
```



```
bind stringmap url_string_map /url_2.html http://www.redirect_url_2.com/
url_2.html

bind stringmap url_string_map /url_3.html http://www.redirect_url_1.com/
url_1.html
```

‘Responder-Aktion hinzufügen act_url_directs–Weiterleitung ‘HTTP.REQ.URL.MAP_STRING (“url_string_map”) ALT “www.default.com”’

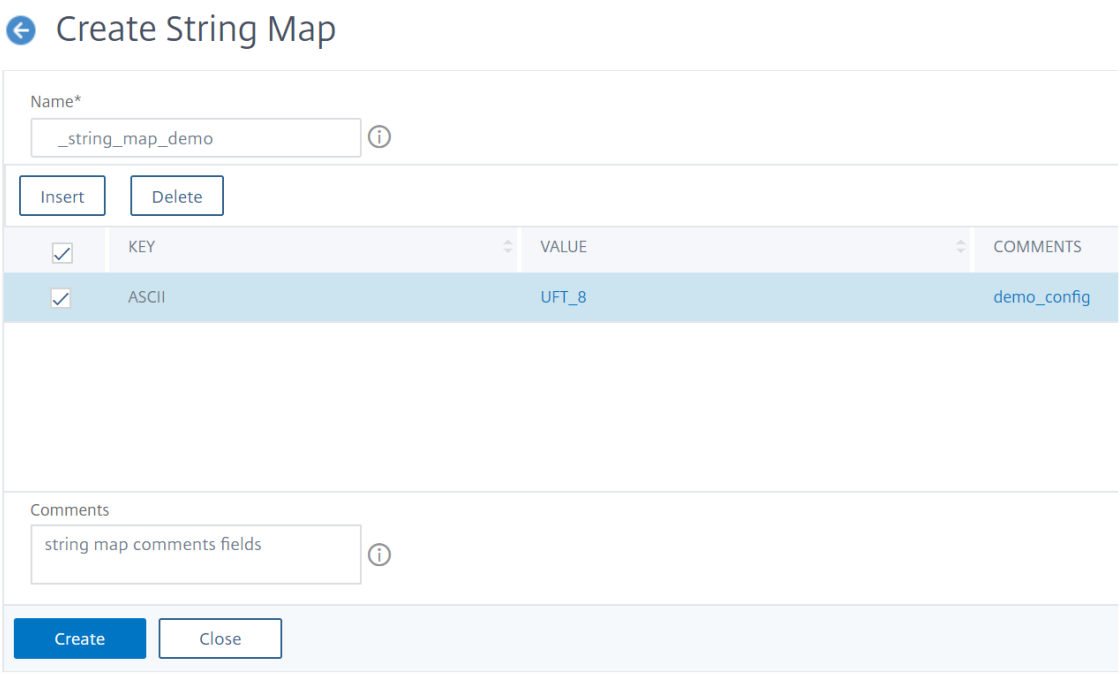
```
add responder policy pol_url_redirects TRUE act_url_redirects

bind cs vserver csw_redirect -policyname pol_url_redirects -priority 1 -
type request
```

So konfigurieren Sie eine Zeichenfolgenzuordnung über die NetScaler GUI

Folgen Sie dem unten angegebenen Verfahren, um eine String-Map zu konfigurieren.

1. Erweitern Sie im Navigationsbereich **AppExpert** und klicken Sie auf **String Maps**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **String-Map erstellen** die folgenden Parameter fest:
   - Name. Name der String-Map.
   - Konfigurieren Sie den Schlüsselwert. ASCII-basierter Schlüsselwerteintrag, der an die Zeichenfolgenzuordnung gebunden ist
   - Kommentare. Eine kurze Beschreibung der an die String-Map gebundenen Schlüsselwerte.
4. Klicken Sie auf **Erstellen** und **Schließen**.



URL-Sets

January 21, 2021

Mit dieser Funktion können Sie eine Million URLs in die Sperrliste eintragen. Der Abschnitt enthält die folgenden Themen:

- Schnelleinstieg
- Verwenden von erweiterten Richtlinienausdrücken für die URL-Auswertung
- Konfigurieren eines URL-Sets
- URL-Muster-Semantik
- URL-Kategorien auf der Sperrliste

Erste Schritte

June 19, 2023

Um den Zugriff auf eingeschränkte Websites zu verhindern, verwendet eine NetScaler-Appliance einen speziellen URL-Abgleichsalgorithmus. Der Algorithmus verwendet einen URL-Satz, der eine Liste von URLs mit bis zu 1 Million (1.000.000) blockierten Einträgen enthalten kann. Das globale Limit liegt bei 1 Million Einträgen. Sie können entweder einen URL-Satz mit 1 Million Einträgen oder mehrere URL-Sets mit insgesamt 1 Million Einträgen hinzufügen.

> **Hinweis:**
>
> Vermeiden Sie die Verwendung vieler URL-Sets. Wir empfehlen Ihnen, eine begrenzte Anzahl von URL-Sets zu verwenden, die auf dem für den URL-Satz verfügbaren Speicher basiert.

Jeder Eintrag kann Metadaten enthalten, die URL-Kategorien und Kategoriegruppen als indizierte Muster definieren. Die Appliance kann auch regelmäßig hochsensible URL-Sets herunterladen, die von Internetbehörden (mit Regierungswebsites) oder Internetorganisationen verwaltet werden. Sobald der URL-Satz von einer Website heruntergeladen und in die Appliance importiert wurde, verschlüsselt die Appliance die URL-Sets (wie von diesen Agenturen verlangt). Die verschlüsselten URL-Sets werden vertraulich behandelt und die Einträge werden nicht manipuliert.

Die NetScaler-Appliance verwendet erweiterte Richtlinien, um zu bestimmen, ob eine eingehende URL blockiert, zugelassen oder umgeleitet werden muss. Diese Richtlinien verwenden erweiterte Ausdrücke, um eingehende URLs anhand von Einträgen auf der Sperrliste zu bewerten. Ein Eintrag kann Metadaten enthalten. Für Einträge, die keine Metadaten haben, können Sie einen Ausdruck verwenden, der die URL anhand einer exakten Zeichenfolgenübereinstimmung auswertet. Für andere URLs können Sie zusätzlich zu einem Ausdruck, der nach einer exakten Zeichenfolge sucht, einen Ausdruck verwenden, der die Metadaten der URL auswertet.

Anwendungsfall für Richtlinien für sicheren Internetzugang für ISP/Telekommunikationsunternehmen

Ein URL-Satz ermöglicht es einem ISP (ISP) oder einem Telekommunikationskunden, von der Regierung vorgeschriebene Richtlinien für einen sicheren Internetzugang durchzusetzen, wie z. B.:

1. Sperren Sie den Zugriff auf illegale Internetseiten (Kindesmissbrauch, Drogen usw.)
2. Sicheres Surfen für Kinder

Mit einer NetScaler-Appliance können Sie in regelmäßigen Abständen URL-Sets herunterladen, die von Internetbehörden oder unabhängigen Internetorganisationen verwaltet werden. Die Appliance lädt die Liste regelmäßig herunter und aktualisiert sie sicher. Die Liste wird als vertrauliche URL-Sätze gespeichert, sodass sie nicht manipuliert oder von Menschen lesbar ist. Der regelmäßig heruntergeladene URL-Satz fungiert als Satz auf der Sperrliste für URL-Bewertungszwecke.

Wenn Sie eine private URL eingerichtet haben und der Inhalt der Liste vertraulich behandelt wird und der Netzwerkadministrator nichts über die in der Sperrliste enthaltenen URLs weiß. Um sicherzustellen, dass die Richtlinie korrekt konfiguriert ist und auf die richtige Liste verwiesen wird, musst du die Canary-URL konfigurieren und sie zum URL-Set hinzufügen. Mithilfe der Canary-URL kann der Administrator über die Appliance die private URL anfordern, um sicherzustellen, dass sie für jede URL-Anforderung gesucht wird.

Erweiterte Richtlinienausdrücke für die URL-Auswertung

January 19, 2021

In der folgenden Tabelle werden die Ausdrücke beschrieben, mit denen Sie eingehende URLs mit Einträgen in einem URL-Set auswerten können.

Hinweis<URL expression>: HTTP.REQ.URL wird generalisiert, um als

Ausdruck	Vorgang
—	—
<URL expression>.URLSET_MATCHES_ANY	Wertet TRUE aus, wenn die URL genau mit einem Eintrag im URL-Set übereinstimmt.
<URL expression>.GET_URLSET_METADATA (<URLSET>)	Der Ausdruck GET_URLSET_METADATA () gibt die zugeordneten Metadaten zurück, wenn die URL genau einem Muster innerhalb des URL-Sets entspricht. Eine leere Zeichenfolge wird zurückgegeben, wenn keine Übereinstimmung vorhanden ist.
<URL expression>.GET_<URLSET>URLSET_METADATA () .EQ (<METADATA>	Wertet TRUE aus, wenn die übereinstimmenden Metadaten gleich sind <METADATA>.
<URL expression><URLSET>““.GET_URLSET_METADATA () .TYPECAST_LIST_T (‘,’) .GET (0) .EQ (<CATEGORY>) |Wertet TRUE aus, wenn sich die übereinstimmenden Metadaten am Anfang der Kategorie befindet. Dieses Muster kann verwendet werden, um separate Felder innerhalb von Metadaten zu kodieren, aber nur mit dem ersten Feld übereinstimmen.| |HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) |Verbindet die Host- und URL-Parameter, die dann als`<URL expression>` Abgleich verwendet werden können.|<!--NeedCopy-->‘

Konfigurieren des URL-Sets

May 11, 2023

Sie können die folgenden Aufgaben ausführen, um einen URL-Satz zu konfigurieren und URLs auf einer NetScaler-Plattform einzuschränken:

1. Importieren Sie einen URL-Satz (laden Sie es herunter und verschlüsseln Sie es). Wenn Sie eine URL importieren, die in einer NetScaler-Appliance festgelegt ist, können Sie:

- Um die URL-Datei herunterzuladen.
- So fügen Sie die Datei der Appliance hinzu.
- Um die Datei zu verschlüsseln.
  Bis Sie die zum System festgelegte URL hinzufügen, ist sie für den Benutzer nicht sichtbar.

Sie können ein Set auf folgende Weise herunterladen:

- Laden Sie eine einmalig festgelegte URL von einem Remoteserver herunter und geben Sie sie als `http://myserver.com/file_with_urlset.csv`
- füge eine Datei unter dem `/var/tmp/` Pfad in ADC hinzu und verwende den Befehl wie im Beispiel:

```
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
> import policy urlset top10
k -url local:test_urlset.csv -delimiter "," -rowSeparator "n" -interval
    10 -privateSet -canaryUrl http://www.in.gr
Done

<!--NeedCopy-->
```

Der importierte URL-Satz wird weiter in verschiedene Kategorien und Kategoriegruppen in der Datenbank unterteilt. Dies ist nur gültig, wenn in den Metadaten der URL-Set-Datei Kategorien vorhanden sind.

Hinweis: Es besteht die Möglichkeit, dass Sie URL-Muster ohne Metadaten haben.

Nachdem Sie die Datei importiert haben, können Sie Dateieigenschaften aktualisieren, löschen oder anzeigen. Nachdem die Datei in die Appliance verschoben wurde, können Sie die Einträge ändern, indem Sie weitere Zeilen hinzufügen.

Der importierte Satz wird dann in einem verschlüsselten Dateiformat im NetScaler-Verzeichnis gespeichert. Die importierte Liste enthält Millionen von URL-Einträgen. Zu den folgenden “Die importierte Liste kann bis zu 1 Million URL-Einträge enthalten. Andernfalls gibt die Appliance eine Fehlermeldung zurück, die besagt, dass der Wert den Grenzwert überschreitet. Wenn der importierte URL-Set Einträge auf der Sperrliste mit Metadaten enthält, werden die Metadaten von der Appliance beim Importieren erkannt.

Nachdem Sie einen URL-Satz importiert und zur Appliance hinzugefügt haben, steht der URL-Set für erweiterte Richtlinien zur Identifizierung der korrekten URL zur Verfügung, die während der eingehenden URL-Auswertung festgelegt wurde. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY(<URL set name>)`

1. Aktualisieren einer auf der NetScaler-Appliance festgelegten URL. Nachdem Sie die Datei in die Appliance verschoben haben, können Sie in diesem Intervall eine URL-Datei mithilfe der Befehlszeilenschnittstelle manuell aktualisieren.
2. Exportieren eines URL-Sets. Wenn Sie eine Backup des URL-Sets bevorzugen, können Sie die Liste der URL-Muster exportieren und eine Kopie davon unter einer Ziel-URL speichern. Überprüfen Sie vor dem Exportieren, ob der URL-Satz als privat gekennzeichnet ist. Wenn als privat

gekennzeichnet ist, kann der URL-Satz nicht exportiert werden. Die Exportfunktion funktioniert nicht mit Private Set. Ein neuer URL-Satz `myurl` würde also ohne definiertes privates Set importiert und dann in eine andere Datei in einem lokalen Pfad exportiert, wie folgt:

```
> shell touch /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
Done
> export urlset myurl -url local:test_urlset_export.csv

> import urlset myurl -url local:test_urlset.csv
Done
(a non-private urlset is imported)

<!--NeedCopy-->
```

1. Ein URL-Satz wird entfernt. Wenn Sie einen URL-Satz von Einträgen auf der Sperrliste löschen möchten, können Sie den Befehl “remove” verwenden, um den URL-Satz von der NetScaler-Appliance zu löschen.
2. Zeigt einen URL-Satz an. Sie können die Eigenschaften einer URL anzeigen, die mit dem Befehl show festgelegt wurde.

> **Hinweis:** URLs mit Abfrageteil werden während des Imports entfernt.

Beispiel:

```
show urlset
Name: top100 PatternCount: 100 Delimiter:  RowSeparator: Interval: 0
Done
<!--NeedCopy-->
```

Importieren Sie eine mit Meta festgelegte URL mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile Folgendes ein:

```
import urlset <name> [-overwrite] [ - delimiter <character>] [-
   rowSeparator <character>] [-url] <url> [-interval <seconds>] [-
   privateSet] [-canaryUrl <URL>]
<!--NeedCopy-->
```


Hierbei gilt:

Delimiter ist ein CSV-Dateisatz mit dem Standardwert 44 festgelegt.

RowSeparator ist ein Zeilentrennzeichen für CSV-Dateien, bei dem der Standardwert auf 10 festgelegt ist.

Intervall ist das Zeitintervall in Sekunden, das auf die nächsten 15 Minuten gerundet wird, bei denen die Aktualisierung des URL-Sets erfolgt.

canaryUrl ist eine URL, die zum Testen verwendet wird, wenn der Inhalt des URL-Sets vertraulich behandelt wird.

Beispiel

```
import policy urlset -url local:test_urlset.csv -delimiter ","-rowSeparator
 "n"-interval 10 -privateSet -canaryUrl http://www.in.gr
```

Führen Sie eine explizite Subdomain-Übereinstimmung für einen importierten URL-Set aus

Sie können jetzt eine explizite Subdomain-Übereinstimmung für einen importierten URL-Satz durchführen. Ein neuer Parameter, “SubDomainExactMatch”, wird dem Befehl “import policy urlSet” hinzugefügt. Wenn Sie den Parameter aktivieren, führt der URL-Filter-Algorithmus eine explizite Subdomain-Übereinstimmung durch. Wenn die eingehende URL beispielsweise “news.example.com” lautet und der Eintrag im URL-Set “example.com” lautet, stimmt der Algorithmus nicht mit den URLs überein.

Geben Sie in der Befehlszeile Folgendes ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```

Beispiel:

```
import policy urlset forth_urlset -url local:test_urlset.csv -interval 3600
 -subdomainExactMatch
```

So zeigen Sie die mit der Befehlszeilenschnittstelle festgelegte URL an

Geben Sie in der Befehlszeile Folgendes ein:

```
show urlset <name>
```

Beispiel:

Geben Sie in der Befehlszeile Folgendes ein:


```
        URLset     Count
        ------     -----
1)      top1k      100
 Done

> show urlset top1k
        Count      Delimiter  Interval   RowSeparator
        -----      ---------  --------   ------------
        100             ,        0         0x0a
 Done
>

<!--NeedCopy-->
```

So zeigen Sie den URL-Satz an, der über die Befehlszeilenschnittstelle importiert wurde

Geben Sie in der Befehlszeile Folgendes ein:

```
show urlset -imported
```

Beispiel:

Geben Sie in der Befehlszeile Folgendes ein:

```
        URLset
        ------
1)      top1k
 Done
<!--NeedCopy-->
```

So zeigen Sie URL-Set an mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
show urlset <name>
```

So exportieren Sie eine URL, die über die Befehlszeilenschnittstelle festgelegt wurde

Geben Sie in der Befehlszeile Folgendes ein:

```
export urlset <name> <url>
```


So fügen Sie eine URL hinzu, die über die Befehlszeilenschnittstelle festgelegt wurde

Geben Sie in der Befehlszeile Folgendes ein:

```
add urlset <urlset_name>
```

So aktualisieren Sie eine URL, die über die Befehlszeilenschnittstelle festgelegt wurde

Geben Sie in der Befehlszeile Folgendes ein:

```
update urlset <name>
```

So entfernen Sie einen URL-Set-Befehl mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
remove urlset <name>
```

Beispiel:

> Hinweis:
>
> Bevor Sie ein URLSet importieren oder exportieren, müssen Sie sicherstellen, dass die Dateien `test_urlset_export.csv` und `test_urlset.csv` erstellt wurden und unter dem Verzeichnis `/var/tmp` verfügbar sind.

```
import policy urlset -url local:test_urlset.csv -delimiter "," -
   rowSeparator "n" -interval 10 -privateSet -overwrite  - canaryUrl
   http://www.in.gr

add policy urlset top10k

update policy urlset top10k

sh policy urlset

sh policy urlset top10k

export policy urlset urlset1 -url local:test_urlset_export.csv

import policy urlset top10k -url local:test_urlset.csv  - privateSet

add policy urlset top10k

update policy urlset top10k

show policy urlset top10k
```



```
<!--NeedCopy-->
```

Importierte URL-Sets anzeigen

Sie können jetzt zusätzlich zu hinzugefügten URL-Sets importierte URL-Sets anzeigen. Um dies zu tun, wird dem Befehl “show url set” ein neuer Parameter “importiert” hinzugefügt. Wenn Sie diese Option aktivieren, zeigt die Appliance alle importierten URL-Sets an und unterscheidet die importierten URL-Sets von den hinzugefügten URL-Sätzen.

Geben Sie in der Befehlszeile Folgendes ein:

```
show policy urlset [<name>] [-imported]
```

Beispiel:

```
show policy urlset -imported
```

So importieren Sie eine URL, die mit der GUI festgelegt wurde

Navigieren Sie zu **AppExpert** > **URL-Sets**und klicken Sie auf **Importieren**, um den URL-Satz herunterzuladen.

So fügen Sie eine URL hinzu, die mit der GUI festgelegt wurde

Navigieren Sie zu **AppExpert** > **URL-Sets**und klicken Sie auf **Hinzufügen**, um eine URL-Set-Datei für den heruntergeladenen URL-Satz zu erstellen.

So bearbeiten Sie eine URL, die mit der GUI festgelegt wurde

Navigieren Sie zu **AppExpert** > **URL-Sets**, wählen Sie einen URL-Satz aus und klicken Sie zum Ändern auf **Bearbeiten** .

So aktualisieren Sie eine mit der GUI festgelegte URL

Navigieren Sie zu **AppExpert** > **URL-Sets,** wählen Sie einen URL-Satz aus und klicken Sie auf **URL-Set** aktualisieren, um den URL-Satz mit den neuesten Änderungen an der Datei zu aktualisieren.

So exportieren Sie eine mit der GUI festgelegte URL

Navigieren Sie zu **AppExpert > URL-Sets**, wählen Sie einen URL-Satz aus und klicken Sie auf **URL-Set** exportieren, um die URL-Muster in einem Set auf eine Ziel-URL zu exportieren und an diesem Speicherort zu speichern.

URL-Muster-Semantik

August 19, 2021

Die folgende Tabelle zeigt die URL-Muster, die zum Angeben der Liste der Seiten verwendet werden sollen, die gefiltert werden sollen. Zum Beispiel `http://www.example.com/bar` stimmt das URL-Muster mit einer einzelnen Seite überein `http://www.example.com/bar`. Um alle Seiten abzudecken, auf denen die URL mit www.example.com/bar beginnt, müssen Sie am Ende explizit ein '*' hinzufügen.

Weitere Informationen finden Sie unter Tabelle mit URL-Muster-Metadaten .

URL-Kategorien

August 19, 2021

Es folgt eine Liste der Kategorien auf der Sperrliste.

S.no	Kategorien auf der Sperrliste
1	Illegale Aktivitäten
2	Illegale Drogen
3	Medikamente
4	Marihuana
5	Terrorismus/Extremismus
6	Waffen
7	Hass/Verleumdung
8	Gewalt/Suizid
9	Rechtsfragen allgemein
10	Erotik/Pornografie
11	Nacktbilder
12	Sexuelle Dienste
13	Erwachseneninhalte (Suche/Links)
14	Computerkriminalität/Hacking
15	Malware

S.no	Kategorien auf der Sperrliste
16	Remote-Proxyserver
17	Suchmaschinen-Caches
18	Übersetzungen
19	Dating/Singlebörsen
20	Hochzeit/Ehe
21	Börsenkurse
22	Onlinehandel
23	Versicherungen
24	Finanzprodukte
25	Glücksspiel allgemein
26	Lotterie
27	Onlinespiele
28	Spiele
29	Auktionen
30	Shopping/Einzelhandel
31	Immobilien
32	IT-Online-Shopping
33	Webbasierte Chats
34	Instant Messaging/Sofortnachrichten
35	Web-basierte E-Mail
36	E-Mail-Abonnements
37	Bulletin Boards
38	IT-Foren
39	Persönliche Webseiten/Blogs
40	Downloads
41	Programmdownloads
42	Speicherdienste
43	Streamingmedien
44	Arbeitsmarkt

S.no	Kategorien auf der Sperrliste
45	Karrieretipps
46	Nebengeschäft
47	Grotesk
48	Veranstaltungen
49	Beliebte Artikel
50	Erwachseneninhalte (Magazine/Nachrichten)
51	Tabakwaren
52	Trinken
53	Alkohol
54	Fetisch
55	Sexueller Ausdruck (Text)
56	Cosplay/Kostüme/Freizeit
57	Okkultes
58	Heim und Familie
59	Profisport
60	Sport allgemein
61	Lebensereignisse
62	Reisen und Tourismus
63	Öffentliche Reiseagenturen
64	Öffentlicher Nahverkehr
65	Unterkünfte
66	Musik
67	Horoskop/Astrologie/Wahrsagerei
68	Entertainer/Prominente
69	Essen/Gourmetküche
70	Entertainment/Veranstaltungsorte/Aktivitäten
71	Traditionelle Religionen
72	Religionen
73	Politik

S.no	Kategorien auf der Sperrliste
74	Reklame/Werbebanner
75	Gewinnspiele/Preise
76	SPAM
77	Nachrichten
78	Automobil
79	Handel und Business
80	Computer und Internet
81	Website zum Bereich Bildung
82	Behörden
83	Integrität
84	Internettelefonie
85	Militär
86	Peer to Peer /Torrent/Filesharing
87	Hobbys und Freizeit
88	Referenz
89	Suchmaschinen und Portale
90	Sexuelle Aufklärung
91	SMS- und Mobilfunkdienste
92	Mobile Apps und Herausgeber
93	Spyware
94	Infrastruktur und Netzwerke für die Inhaltsübermittlung
95	Kinderwebsites
96	Bademode und Dessous
97	Kunst und Kultur
98	Hosting von Websites
99	Philanthropie und gemeinnützige Organisationen
100	Fotosuche und Fototauschbörsen

S.no	Kategorien auf der Sperrliste
101	Klingeltöne
102	Mode und Schönheit
103	Mobile App-Stores
104	Domainparking
105	Emoticons
106	Mobilfunkbetreiber
107	Botnetze
108	Infizierte Websites
109	Phishing-Websites
110	Keylogger
111	Mobile Malware
112	Kein Inhalt
113	Landwirtschaft
114	Architektur
115	Organisationen/Branchenverbände/Gewerkschaften
116	Bücher/eBooks
117	BOT Phone Home
118	DDNS
119	Nicht unterstützte URL
120	Rechtswesen
121	Lokales/Nachbarschaft
122	Sonstiges
123	Onlinemagazine
124	Haustiere/Tierarzt
125	Piraterie und Urheberrechtsverstöße
126	Private IP-Adressen
127	Recycling/Umweltschutz
128	Wissenschaft
129	Kultur und Gesellschaft

S.no	Kategorien auf der Sperrliste
130	Transportdienstleistungen & Fracht
131	Film und Fotografie
132	Museen und Geschichte
133	eLearning
134	Soziale Netzwerke allgemein
135	Facebook
136	Facebook: Posts
137	Facebook: Kommentar
138	Facebook: Freunde
139	Facebook: Foto hochladen
140	Facebook: Veranstaltungen
141	Facebook: Apps
142	Facebook: Chat
143	Facebook: Fragen
144	Facebook: Video hochladen
145	Facebook: Gruppen
146	Facebook: Spiele
147	LinkedIn
148	LinkedIn: Aktuelles
149	LinkedIn: E-Mail
150	LinkedIn: Verbindungen
151	LinkedIn: Jobs
152	Twitter
153	Twitter: Posts
154	Twitter: E-Mail
155	Twitter: Abonnieren
156	YouTube
157	YouTube: Kommentar
158	YouTube: Video hochladen

S.no	Kategorien auf der Sperrliste
159	YouTube: Teilen
160	Instagram
161	Instagram: Hochladen
162	Instagram: Kommentar
163	Instagram: Private Nachricht
164	Tumblr
165	Tumblr: Posts
166	Tumblr: Kommentar
167	Tumblr: Foto oder Video hochladen
168	Google+
169	Google+: Posts
170	Google+: Kommentar
171	Google+: Foto hochladen
172	Google+: Video hochladen
173	Google+: Videochat
174	Pinterest
175	Pinterest: Pin/Markierung
176	Vine: Hochladen
177	Vine: Kommentar
178	Vine: Nachricht
179	Ask.fm
180	Ask.fm: Frage
181	Ask.fm: Antwort
182	YikYak
183	YikYak: Posts
184	YikYak: Kommentar
185	Wordpress
186	Wordpress: Posts

S.no	Kategorien auf der Sperrliste
187	Wordpress: Hochladen

AppFlow

May 11, 2023

Die NetScaler-Appliance ist ein zentraler Steuerungspunkt für den gesamten Anwendungsverkehr im Rechenzentrum. Es sammelt Informationen auf Fluss- und Benutzersitzungsebene, die für die Überwachung der Anwendungsleistung, Analyse und Business Intelligence-Anwendungen wertvoll sind. Es sammelt auch Leistungsdaten von Webseiten und Datenbankinformationen. AppFlow überträgt die Informationen mithilfe des Internet Protocol Flow Information Export-Formats (IPFIX), bei dem es sich um einen offenen Internet Engineering Task Force (IETF) -Standard handelt, der in RFC 5101 definiert ist. IPFIX (die standardisierte Version von NetFlow von Cisco) wird häufig zur Überwachung von Netzwerkflussinformationen verwendet. AppFlow definiert neue Informationselemente, um Informationen auf Anwendungsebene, Leistungsdaten von Webseiten und Datenbankinformationen darzustellen.

Unter Verwendung von UDP als Transportprotokoll überträgt AppFlow die gesammelten Daten, die als *Flow-Datensätze*bezeichnet werden, an einen oder mehrere IPv4-Sammler. Die Kollektoren aggregieren die Flow-Datensätze und generieren Echtzeit- oder historische Berichte.

AppFlow bietet Sichtbarkeit auf Transaktionsebene für HTTP-, SSL-, TCP-, SSL_TCP-Flows und HDX Insight-Flüsse. Sie können die Flow-Typen, die Sie überwachen möchten, testen und filtern.

> **Hinweis**
>
> Weitere Informationen zu HDX Insight finden Sie unter HDX Insight.

AppFlow verwendet Aktionen und Richtlinien, um Datensätze für einen ausgewählten Flow an bestimmte Kollektoren zu senden. Eine AppFlow-Aktion gibt an, welche Gruppe von Collectoren die AppFlow-Datensätze erhalten. Richtlinien, die auf erweiterten Ausdrücken basieren, können so konfiguriert werden, dass sie Flows auswählen, für die Flow-Datensätze an die durch die zugehörige AppFlow-Aktion angegebenen Collectors gesendet werden.

Um die Arten von Flows einzuschränken, können Sie AppFlow für einen virtuellen Server aktivieren. AppFlow kann auch Statistiken für den virtuellen Server bereitstellen.

Sie können AppFlow auch für einen bestimmten Dienst aktivieren, der einen Anwendungsserver darstellt, und den Datenverkehr zu diesem Anwendungsserver überwachen.

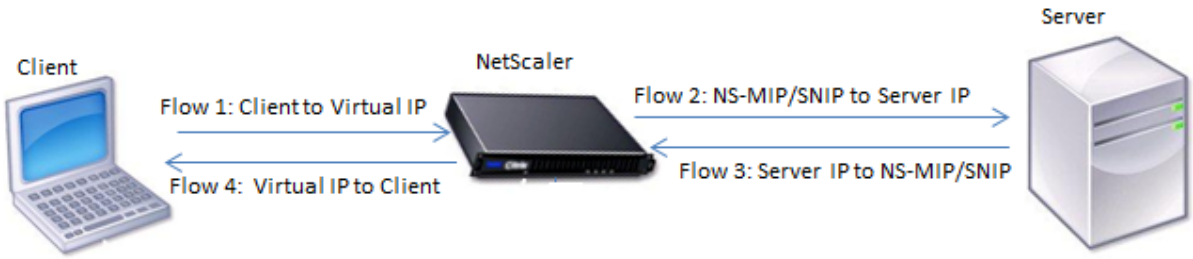
Hinweis: Diese Funktion wird nur auf NetScaler NCore-Builds unterstützt.

So funktioniert AppFlow

Im häufigsten Bereitstellungsszenario fließt eingehender Datenverkehr zu einer virtuellen IP-Adresse (VIP) auf der NetScaler-Appliance und wird auf einen Server ausbalanciert. Ausgehender Datenverkehr fließt vom Server zu einer zugeordneten oder Subnetz-IP-Adresse auf dem NetScaler und vom VIP zum Client. Ein Fluss ist eine unidirektionale Sammlung von IP-Paketen, die durch die folgenden fünf Tupel identifiziert wird: SourceIP, SourcePort, DesTip, DestPort und Protokoll.

Die folgende Abbildung beschreibt, wie die AppFlow-Funktion funktioniert.

Abbildung 1. NetScaler-Flowsequenz



Wie in der Abbildung gezeigt, hängen die Netzwerkflusskennungen für jeden Abschnitt einer Transaktion von der Richtung des Datenverkehrs ab.

Die verschiedenen Flüsse, die einen Flow-Datensatz bilden, sind:

Fluss 1: <Client-IP, Client-Port, VIP-IP, VIP-port, Protocol>

Fluss 2: <NS-MIP/SNIP, NS-port, Server-IP, Server-Port, Protocol>

Fluss 3: <Server-IP, Server-Port, NS-MIP/SNIP, NS-Port, Protocol>

Fluss 4: <VIP-IP, VIP-port, Client-IP, Client-Port, Protocol>

Um dem Collector zu helfen, alle vier Flows in einer Transaktion zu verknüpfen, fügt AppFlow jedem Flow ein benutzerdefiniertes TransactionID-Element hinzu. Für Content Switching auf Anwendungsebene, z. B. HTTP, ist es möglich, dass eine einzelne Client-TCP-Verbindung für jede Anforderung auf verschiedene Back-End-TCP-Verbindungen ausgeglichen wird. AppFlow stellt eine Reihe von Datensätzen für jede Transaktion bereit.

Flow Aufzeichnungen

AppFlow-Datensätze enthalten standardmäßige NetFlow- oder IPFIX-Informationen, wie Zeitstempel für den Beginn und das Ende eines Flusses, Paketanzahl und Byteanzahl. AppFlow-Datensätze enthalten auch Informationen auf Anwendungsebene (wie HTTP-URLs, HTTP-Anforderungsmethoden und Antwortstatuscodes, Serverreaktionszeit und Latenz). Leistungsdaten der Webseite (z. B. die Ladezeit der Seite, die Renderzeit der Seite und die auf der Seite verbrachte Zeit). Und Datenbankinformationen (wie Datenbankprotokoll, Status der Datenbankantwort und Größe der Datenbank-Antwort).

IPFIX-Flow-Datensätze basieren auf Vorlagen, die vor dem Senden von Flow-Datensätzen gesendet werden müssen.

Vorlagen

AppFlow definiert eine Reihe von Vorlagen, eine für jede Art von Fluss. Jede Vorlage enthält eine Reihe von Standardinformationselementen (IEs) und unternehmensspezifischen Informationselementen (EIEs). IPFIX-Vorlagen definieren die Reihenfolge und Größe der Informationselemente (Internet Explorer) im Flow-Datensatz. Die Vorlagen werden in regelmäßigen Abständen an die Sammler gesendet, wie in RFC 5101 beschrieben.

Eine Vorlage kann die folgenden EIEs enthalten:

- transactionID

  Eine vorzeichenlose 32-Bit-Nummer, die eine Transaktion auf Anwendungsebene identifiziert. Für HTTP entspricht es einem Anforderungs- und Antwortpaar. Alle Flow-Datensätze, die diesem Anforderungs- und Antwortpaar entsprechen, haben dieselbe Transaktions-ID. Im häufigsten Fall gibt es vier `uniflow` Datensätze, die dieser Transaktion entsprechen. Wenn der NetScaler die Antwort selbst generiert (bereitgestellt aus dem integrierten Cache oder durch eine Sicherheitsrichtlinie), gibt es möglicherweise nur zwei Flussdatensätze für diese Transaktion.

- connectionID

  Eine vorzeichenlose 32-Bit-Nummer, die eine Layer-4-Verbindung (TCP oder UDP) identifiziert. Die NetScaler-Flows sind bidirektional, mit zwei separaten Flussdatensätzen für jede Richtung des Flusses. Dieses Informationselement kann verwendet werden, um die beiden Flüsse zu verknüpfen.

  Für den NetScaler ist eine ConnectionID ein Bezeichner für die Verbindungsdatenstruktur, um den Fortschritt einer Verbindung zu verfolgen. In einer HTTP-Transaktion kann eine bestimmte ConnectionID beispielsweise mehrere TransactionID-Elemente enthalten, die mehreren Anfragen entsprechen, die an diese Verbindung gestellt wurden.

- tcpRTT

  Die an der TCP-Verbindung gemessene Roundtrip-Zeit in Millisekunden. Es kann als Metrik verwendet werden, um die Client- oder Serverlatenz im Netzwerk zu bestimmen.

- httpRequestMethod

  Eine 8-Bit-Zahl, die die in der Transaktion verwendete HTTP-Methode angibt. Eine Optionsvorlage mit der Nummer-zu-Methode-Zuordnung wird zusammen mit der Vorlage gesendet.

- httpRequestSize

  Eine vorzeichenlose 32-Bit-Zahl, die die Größe der Nutzdaten der Anforderung angibt.

- httpRequestURL

  Die vom Client angeforderte HTTP-URL.

- httpUserAgent

  Die Quelle eingehender Anfragen an den Webserver.

- httpResponseStatus

  Eine 32-Bit-Zahl ohne Vorzeichen, die den Statuscode der Antwort angibt.

- httpResponseSize

  Eine 32-Bit-Zahl ohne Vorzeichen, die die Größe der Antwort angibt.

- httpResponseTimeToFirstByte

  Eine 32-Bit-Zahl ohne Vorzeichen, die die Zeit angibt, die zum Empfangen des ersten Bytes der Antwort gebraucht wurde.

- httpResponseTimeToLastByte

  Eine 32-Bit-Zahl ohne Vorzeichen, die die Zeit angibt, die zum Empfangen des letzten Bytes der Antwort gebraucht wurde.

- flowFlags

  Ein 64-Bit-Flag ohne Vorzeichen, das verwendet wird, um verschiedene Flussbedingungen anzuzeigen.

EIEs für Leistungsdaten von Webseiten

- clientInteractionStartTime

  Zeitpunkt, zu dem der Browser das erste Byte der Antwort erhält, um Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.

- clientInteractionEndTime

  Zeitpunkt, zu dem der Browser das letzte Byte an Antwort erhalten hat, um alle Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.

- clientRenderStartTime

  Zeitpunkt, zu dem der Browser beginnt, die Seite zu rendern.

- clientRenderEndTime

  Zeitpunkt, zu dem ein Browser die gesamte Seite einschließlich der eingebetteten Objekte beendet hat.

EIEs für Datenbankinformationen

- dbProtocolName

  Eine vorzeichenlose 8-Bit-Zahl, die das Datenbankprotokoll angibt. Gültige Werte sind 1 für MS SQL und 2 für MySQL.

- dbReqType

  Eine vorzeichenlose 8-Bit-Zahl, die die in der Transaktion verwendete Datenbankanforderungsmethode angibt. Gültige Werte für MS SQL sind 1 ist für QUERY, 2 für TRANSACTION und 3 für RPC. Gültige Werte für MySQL finden Sie in der MySQL-Dokumentation.

- dbReqString

  Zeigt die Zeichenfolge der Datenbankanforderung ohne den Header an.

- dbRespStatus

  Eine 64-Bit-Zahl ohne Vorzeichen, die den Status der vom Webserver empfangenen Datenbankantwort angibt.

- dbRespLength

  Eine 64-Bit-Zahl ohne Vorzeichen, die die Größe der Antwort angibt.

- dbRespStatString

  Die vom Webserver empfangene Zeichenfolge für den Antwortstatus.

Konfigurieren der AppFlow Funktion

May 11, 2023

Sie können AppFlow auf die gleiche Weise wie die meisten anderen richtlinienbasierten Funktionen konfigurieren. Zunächst aktivieren Sie die AppFlow-Funktion. Dann geben Sie die Kollektoren an, an die die Durchflussdatensätze gesendet werden. Danach definieren Sie Aktionen, bei denen es sich um konfigurierte Collectors handelt. Anschließend konfigurieren Sie eine oder mehrere Richtlinien und ordnen jeder Richtlinie eine Aktion zu. Die Richtlinie weist die NetScaler-Appliance an, Anfragen auszuwählen, deren Ablaufdatensätze an die zugehörige Aktion gesendet werden. Schließlich binden Sie jede Richtlinie entweder global oder an den spezifischen virtuellen Server, um sie in Kraft zu setzen.

Sie können AppFlow-Parameter weiter festlegen, um das Aktualisierungsintervall der Vorlage festzulegen und den Export von httpURL-, httpCookie- und httpReferer-Informationen zu ermöglichen. Auf jedem Collector müssen Sie die NetScaler IP-Adresse als Adresse des Exporters angeben.

> **Hinweis**
>
> Informationen zur Konfiguration des NetScaler als Exporter auf dem Collector finden Sie in der Dokumentation für den jeweiligen Collector.

Das Konfigurationsdienstprogramm bietet Tools, mit denen Benutzer die Richtlinien und Aktionen definieren können. Es bestimmt genau, wie die NetScaler-Appliance Datensätze für einen bestimmten Flow an eine Gruppe von Collectors exportiert (Aktion). Die Befehlszeilenschnittstelle bietet einen entsprechenden Satz von CLI-basierten Befehlen für erfahrene Benutzer, die eine Befehlszeile bevorzugen.

AppFlow aktivieren

Um die AppFlow-Funktion verwenden zu können, müssen Sie sie zunächst aktivieren.

> **Hinweis**
>
> AppFlow kann nur auf nCore NetScaler-Appliances aktiviert werden.

Aktivieren Sie die AppFlow-Funktion über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
enable ns feature AppFlow

<!--NeedCopy-->
```

Aktivieren Sie die AppFlow-Funktion über das Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen**, klicken Sie auf **Erweiterte Funktionen konfigurieren** und wählen Sie die Option **AppFlow** aus.

Einen Collector angeben

Ein Collector empfängt AppFlow-Datensätze, die von der NetScaler-Appliance generiert wurden. Um die AppFlow-Datensätze zu senden, müssen Sie mindestens einen Collector angeben. Standardmäßig hört der Collector IPFIX-Nachrichten auf dem UDP-Port 4739 ab. Sie können den Standardanschluss ändern, wenn Sie den Collector konfigurieren. In ähnlicher Weise wird NSIP standardmäßig als Quell-IP für AppFlow-Verkehr verwendet. Sie können diese Standard-Quell-IP bei der Konfiguration eines Collectors in eine SNIP-Adresse ändern. Sie können auch nicht verwendete Collectors entfernen.

Angeben eines Collectors über die Befehlszeilenschnittstelle

> **Wichtig**
>
> Ab NetScaler Version 12.1 Build 55.13 können Sie den Typ des Collectors angeben, den Sie verwenden möchten. Ein neuer Parameter “Transport” wird im Befehl `add appflow collector` eingeführt. Standardmäßig lauscht der Collector IPFIX-Nachrichten. Sie können den Kollektortyp entweder auf `logstream` oder `ipfix` oder rest ändern, indem Sie den Parameter “Transport” verwenden. Weitere Informationen zur Konfiguration finden Sie im Beispiel.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Collector hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add appflow collector <name> -IPAddress <ipaddress> -port <
     port_number> -netprofile <netprofile_name> -Transport <Transport>
2
3 -  show appflow collector <name>
4
5 <!--NeedCopy-->
```

Beispiel

```
1 add appflow collector col1 -IPaddress 10.102.29.251 -port 8000 -
     netprofile n2 -Transport ipfix
2
3 <!--NeedCopy-->
```

Geben Sie mehrere Collectors über die Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um dieselben Daten hinzuzufügen und an mehrere Collectors zu senden:

```
1  add appflow collector <collector1> -IPAddress <IP>
2
3  add appflow collector <collector2> -IPAddress <IP>
4
5  add appflow action <action> -collectors <collector1> <collector2>
6
7  add appflow policy <policy> true <action>
8
9  bind lbvserver <lbvserver> -policy <policy> -priority <priority>
10 <!--NeedCopy-->
```


Geben Sie einen oder mehrere Collectors über das Konfigurationsdienstprogramm an

Navigieren Sie zu **System > AppFlow > Collectors**, und erstellen Sie den AppFlow-Kollektor.

AppFlow-Aktion konfigurieren

Eine AppFlow-Aktion ist ein Set-Collector, an den die Flow-Datensätze gesendet werden, wenn die zugehörige AppFlow-Richtlinie übereinstimmt.

Konfigurieren Sie eine AppFlow-Aktion über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine AppFlow-Aktion zu konfigurieren und die Konfiguration zu überprüfen:

```
1 add appflow action <name> --collectors <string> ... [-
     clientSideMeasurements (Enabled|Disabled) ] [-comment <string>]
2
3 show appflow action
4
5 <!--NeedCopy-->
```

Beispiel

```
1 add appflow action apfl-act-collector-1-and-3 -collectors collector-1
     collecter-3
2
3 <!--NeedCopy-->
```

Konfigurieren Sie eine AppFlow-Aktion über das Konfigurationsdienstprogramm

Navigieren Sie zu **System > AppFlow > Actions**, und erstellen Sie die AppFlow-Aktion.

AppFlow-Richtlinie konfigurieren

Nachdem Sie eine AppFlow-Aktion konfiguriert haben, müssen Sie als Nächstes eine AppFlow-Richtlinie konfigurieren. Eine AppFlow-Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht.

> **Hinweis**

> Zum Erstellen und Verwalten von AppFlow-Richtlinien bietet das Konfigurationsdienstprogramm Unterstützung, die in der Befehlszeilenschnittstelle nicht verfügbar ist.

Konfigurieren Sie eine AppFlow-Richtlinie über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine AppFlow-Richtlinie hinzuzufügen und die Konfiguration zu überprüfen:

```
add appflow policy <name> <rule> <action>

show appflow policy <name>

<!--NeedCopy-->
```

Beispiel

```
add appflow policy apfl-pol-tcp-dsprt client.TCP.DSTPORT.EQ(22) apfl-
    act-collector-1-and-3

<!--NeedCopy-->
```

Konfigurieren Sie eine AppFlow-Richtlinie über das Konfigurationsdienstprogramm

Navigieren Sie zu **System > AppFlow > Policies**und erstellen Sie die AppFlow-Richtlinie.

Hinzufügen eines Ausdrucks mithilfe des Dialogfelds „ Ausdruck hinzufügen “

1. Wählen Sie im Dialogfeld Ausdruck hinzufügen im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.

   -
   HTTP
   Das HTTP-Protokoll. Wählen Sie die Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
   -
   SSL

   ```
   Die geschützten Websites. Wählen Sie die Option, wenn Sie einen
       Aspekt der Anfrage untersuchen möchten, der sich auf den Empfä
       nger der Anfrage bezieht. -
   CLIENT

   ```



```
4 The computer that sent the request. Choose the option if you want
    to examine some aspect of the sender of the request. Wenn Sie
    Ihre Auswahl treffen, werden im Listenfeld ganz rechts die
    entsprechenden Begriffe für den nächsten Teil Ihres Ausdrucks
    aufgeführt.
```

2. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahl hängt davon ab, welche Wahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, wird im Hilfefenster unterhalb des Fensters "Ausdruck konstruieren" (das leer war) eine Hilfe zur Beschreibung des Zwecks und der Verwendung des gerade gewählten Begriffs angezeigt.
3. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.

Binden einer AppFlow-Richtlinie

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie entweder global binden, sodass sie für den gesamten Datenverkehr gilt, der über den NetScaler fließt, oder für einen bestimmten virtuellen Server, sodass die Richtlinie nur für den Datenverkehr gilt, der sich auf diesen virtuellen Server bezieht.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf jede positive Ganzzahl festlegen.

Im NetScaler-Betriebssystem funktionieren die Richtlinienprioritäten in umgekehrter Reihenfolge — je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit Prioritäten von 10, 100 und 1000 haben, wird die Richtlinie, der eine Priorität von 10 zugewiesen wurde, zuerst ausgeführt. Später wurde die Richtlinie mit einer Priorität von 100 zugewiesen, und schließlich wies die Richtlinie eine Reihenfolge von 1000 zu.

Sie können sich ausreichend Raum lassen, um weitere Richtlinien in beliebiger Reihenfolge hinzuzufügen, und sie dennoch so einstellen, dass sie in der von Ihnen gewünschten Reihenfolge bewertet werden. Sie können dies erreichen, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen den einzelnen Richtlinien festlegen, wenn Sie sie global binden. Sie können dann jederzeit weitere Richtlinien hinzufügen, ohne die Priorität einer vorhandenen Richtlinie ändern zu müssen.

Binden Sie eine AppFlow-Richtlinie global über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine AppFlow-Richtlinie global zu binden und die Konfiguration zu überprüfen:


```
bind appflow global <policyName> <priority> [<gotoPriorityExpression [-
    type <type>] [-invoke (<labelType> <labelName>)]

show appflow global

<!--NeedCopy-->
```

Beispiel

```
bind appflow global af_policy_lb1_10.102.71.190 1 NEXT -type
    REQ_OVERRIDE -invoke vserver google

<!--NeedCopy-->
```

Binden Sie eine AppFlow-Richtlinie über die Befehlszeilenschnittstelle an einen bestimmten virtuellen Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine AppFlow-Richtlinie an einen bestimmten virtuellen Server zu binden und die Konfiguration zu überprüfen:

```
bind lb vserver <name> -policyname <policy_name> -priority <priority>

<!--NeedCopy-->
```

Beispiel

```
bind lb vserver google -policyname af_policy_google_10.102.19.179 -
    priority 251

<!--NeedCopy-->
```

Binden Sie eine AppFlow-Richtlinie global über das Konfigurationsdienstprogramm

Navigieren Sie zu **System > AppFlow**, klicken Sie auf **AppFlow Policy Manager**, wählen Sie den entsprechenden Bindepunkt (Standard Global) und den Verbindungstyp aus, und binden Sie dann die AppFlow-Richtlinie.

Binden Sie eine AppFlow-Richtlinie über das Konfigurationsdienstprogramm an einen bestimmten virtuellen Server

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, wählen Sie den virtuellen Server aus, klicken Sie auf **Policies**und binden Sie die AppFlow-Richtlinie.

AppFlow für virtuelle Server aktivieren

Wenn Sie nur den Verkehr durch bestimmte virtuelle Server überwachen möchten, aktivieren Sie AppFlow speziell für diese virtuellen Server. Sie können AppFlow für Load Balancing, Content Switching, Cache-Umleitung, SSL-VPN, GSLB und virtuelle Authentifizierungsserver aktivieren.

Aktivieren Sie AppFlow für einen virtuellen Server über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver <name> <protocol> <IPAddress> <port> -appflowLog ENABLED

<!--NeedCopy-->
```

Beispiel

```
set cs vserver Vserver-CS-1 HTTP 10.102.29.161 80 -appflowLog ENABLED

<!--NeedCopy-->
```

Aktivieren Sie AppFlow für einen virtuellen Server über das Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie den virtuellen Server aus und aktivieren Sie die Option AppFlow Logging.

AppFlow für einen Service aktivieren

Sie können AppFlow für Dienste aktivieren, die an die virtuellen Load Balancing-Server gebunden werden sollen.

Aktivieren Sie AppFlow für einen Dienst über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
set service <name> -appflowLog ENABLED

<!--NeedCopy-->
```

Beispiel

```
set service ser -appflowLog ENABLED

<!--NeedCopy-->
```

Aktivieren Sie AppFlow für einen Dienst über das Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, wählen Sie den Dienst aus und aktivieren Sie die Option AppFlow Logging.

Legen Sie die AppFlow-Parameter fest

Sie können AppFlow-Parameter festlegen, um den Export von Daten in die Collectors anzupassen.

Legen Sie die AppFlow-Parameter über die Befehlszeilenschnittstelle fest

> **Wichtig**
>
> - Ab NetScaler Release 12.1 Build 55.13 können Sie mit dem NSIP `Logstream`-Datensätze anstelle des SNIP senden. Ein neuer Parameter “logstreamOverNSIP” wird im Befehl `set appflow param` eingeführt. Standardmäßig ist der Parameter “logstreamOverNSIP” DISABLED, Sie müssen ihn auf ENABLE setzen. Weitere Informationen zur Konfiguration finden Sie im Beispiel.
> - Ab NetScaler Version 13.0 Build 58.x können Sie die Web-SaaS-Anwendungsoption in der AppFlow-Funktion aktivieren. Es kann aktiviert werden, um die Datennutzung von Web- oder SaaS-Anwendungen vom Citrix Gateway-Dienst zu empfangen. Weitere Informationen zur Konfiguration finden Sie im Beispiel.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die AppFlow-Parameter festzulegen und die Einstellungen zu überprüfen:

```
-  set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>]
    [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-
   httpUrl ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-httpCookie ( \*\*
   ENABLED\*\* | \*\*DISABLED\*\* )] [-httpReferer ( \*\*ENABLED\*\* |
   \*\*DISABLED\*\* )] [-httpMethod ( \*\*ENABLED\*\* | \*\*DISABLED
```



```
      \*\* )] [-httpHost ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
      httpUserAgent ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
      httpXForwardedFor ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )][-
      clientTrafficOnly ( \*\*YES\*\* | \*\*NO\*\*)] [-
      webSaaSAppUsageReporting ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
      logstreamOverNSIP ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )]
2
3 -  show appflow Param
4
5 <!--NeedCopy-->
```

Beispiel

```
1 set appflow Param -templateRefresh 240 -udpPmtu 128 -httpUrl enabled -
     webSaaSAppUsageReporting ENABLED -logstreamOverNSIP ENABLED
2
3 <!--NeedCopy-->
```

Legen Sie die AppFlow-Parameter über das Konfigurationsdienstprogramm fest

Navigieren Sie zu **System > AppFlow**, klicken Sie auf **AppFlow-Einstellungen ändern**und geben Sie die entsprechenden AppFlow-Parameter an.

Unterstützung für die Verschleierung der Abonnenten-ID

Ab NetScaler Release 13.0 Build 35.xx wurde die AppFlow-Konfiguration erweitert, um den Algorithmus “subscriberIdObfuscation” zum Verschleiern von MSISDN in Layer 4 oder Layer 7, AppFlow-Datensätzen, zu unterstützen. Bevor Sie den Algorithmus jedoch als MD5 oder SHA256 konfigurieren, müssen Sie ihn zunächst als AppFlow-Parameter aktivieren. Der Parameter ist standardmäßig deaktiviert.

Konfigurieren Sie den Abonnenten-ID-Verschleierungsalgorithmus über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set appflow param [-subscriberIdObfuscation ( ENABLED | DISABLED )  [-
     subscriberIdObfuscationAlgo ( MD5 | SHA256 )]]
2
3 <!--NeedCopy-->
```

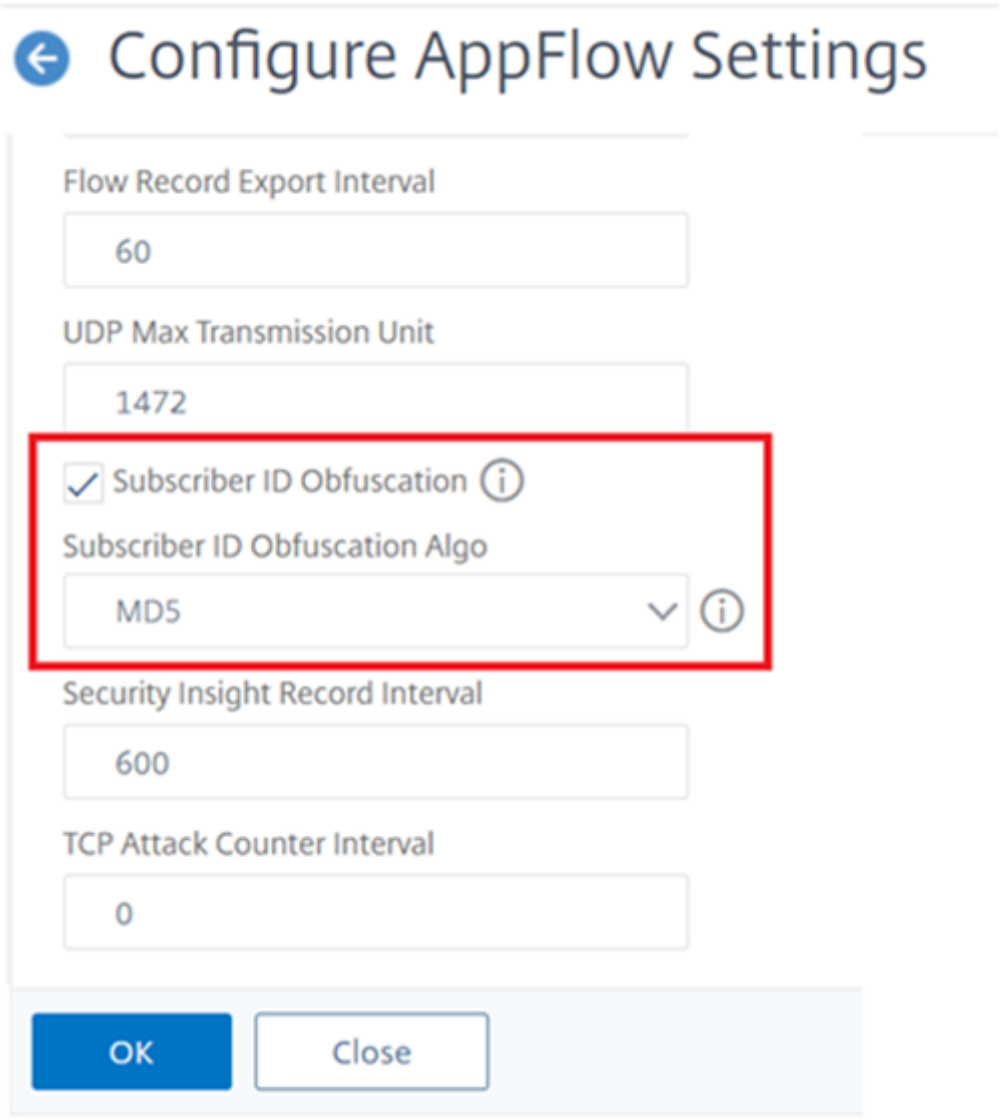

Beispiel

```
set appflow param  -subscriberIdObfuscation ENABLED  -
    subscriberIdObfuscationAlgo SHA256

<!--NeedCopy-->
```

Konfigurieren Sie den Abonnenten-ID-Verschleierungsalgorithmus über die GUI

1. Navigieren Sie zu **System > AppFlow**.
2. Klicken Sie im Detailbereich AppFlow unter **Einstellungen** auf **AppFlow-Einstellung ändern**.
3. Legen Sie auf der Seite AppFlow-Einstellungen konfigurieren die folgenden Parameter fest:
   - **Verschleierung der Abonnenten-ID.** Aktivieren Sie die Option zur Verschleierung von MSISDN in L4/L7 AppFlow-Datensätzen.
   - **Abonnenten-ID-Verschleierung Algo.** Wählen Sie den Algorithmus-Typ als MD5 oder SHA256.
4. Klicken Sie auf **OK** und auf **Schließen**.



Beispiel: AppFlow für DataStream konfigurieren

Das folgende Beispiel zeigt das Verfahren zum Konfigurieren von AppFlow für DataStream über die Befehlszeilenschnittstelle.

```
enable feature appflow

add db user sa password freebsd

add lbvserver lb0 MSSQL 10.102.147.97 1433 -appflowLog ENABLED

add service sv0 10.103.24.132 MSSQL 1433 -appflowLog ENABLED

```



```
bind lbvserver lb0 sv0

add appflow collector col0 -IPAddress 10.102.147.90

add appflow action act0 -collectors col0

add appflow policy pol0 "mssql.req.query.text.contains("select")" act0

bind lbvserver lb0 -policyName pol0 -priority 10

<!--NeedCopy-->
```

Wenn die NetScaler-Appliance eine Datenbankanforderung empfängt, wertet die Appliance die Anfrage anhand einer konfigurierten Richtlinie aus. Wenn eine Übereinstimmung gefunden wird, werden die Details an den AppFlow -Kollektor gesendet, der in der Richtlinie konfiguriert ist.

Konfigurieren des Metrics Collectors

Metrics Collector ist ein Dienst, den Sie auf NetScaler aktivieren können, um Metriken von NetScaler zu sammeln und an verschiedene Endpunkte zu exportieren. Sie können Metriken in zwei Formaten exportieren: Avro und Prometheus. Die exportierten Metriken können verarbeitet und visualisiert werden, um aussagekräftige Erkenntnisse zu erhalten. Standardmäßig unterstützt der Metrics Collector den Export von Zeitreihenanalysedaten alle 30 Sekunden. Sie können ihn jedoch als Wert zwischen 30 und 300 Sekunden konfigurieren, sodass Sie das Intervall für den Export der Profildaten der Zeitreihenanalyse festlegen können.

Gehen Sie wie folgt vor, um einen Metriksammler mithilfe der CLI zu konfigurieren.

1. Konfigurieren Sie einen Collector-Dienst mit IP-Adresse, Protokoll und Port mithilfe des folgenden Befehls.

   ```
   add service <metrics_service_name> <ip-address> <protocol> <port>
   ```

   Beispiel:

   ```
   add service metrics_service1 192.168.1.1 HTTP 5563
   ```

2. Konfigurieren Sie das Analytics-Zeitreihenprofil, um Metrikdaten an den Collector-Service zu senden. Geben Sie den Collector-Dienst, die Häufigkeit für den Export von Metriken und den Ausgabemodus an.

   ```
   set analytics profile ns_analytics_time_series_profile -collectors
        <metrics_service_name> -type timeseries -metrics ENABLED
      metricsExportFrequency <30-300> -outputMode <avro/prometheus>
   ```


Beispiel:

```
set analytics profile ns_analytics_time_series_profile -collectors
     metrics_service1 -type timeseries -metrics Enabled
    metricsExportFrequency 90 -outputMode prometheus --serveMode
    PUSH
```

> **Hinweis:**
>
> In diesem Beispiel wird das Standard-Zeitreihenprofil verwendet `ns_analytics_time_series_profi`. Wenn Sie ein Zeitreihenprofil erstellen möchten, können Sie den `add analytics profile` Befehl verwenden.

In diesem Beispiel ist die Exporthäufigkeit von Metriken auf 90 Sekunden und der Exportmodus auf Prometheus festgelegt.

Überprüfen Sie die Konfiguration des Metrikkollektors mit dem `show analytics profile <analytics-profile-name>` folgenden Befehl:

```
show analytics profile ns_analytics_time_series_profile

    Name: ns_analytics_time_series_profile
    Collector: metrics_service1
    Profile-type: timeseries
        Output Mode: Prometheus
        Metrics: ENABLED
          Schema File: schema.json
          Metrics Export Frequency: 90
        Events: DISABLED
        Auditlog: DISABLED
        Serve mode: Pull
    Reference Count: 0
```

Debuggen von Metrics Collector

Die erforderlichen Debugging-Protokolle werden in `/var/nslog/metricscollector.log` gespeichert.

Generierung von Metrikdateien

Die Dateien `metrics_<format>_log.*` werden im Ordner `/var/nslog/` generiert.

Unterstützung dynamischer Schemas im Metrics Collector

Mit der Unterstützung dynamischer Schemazähler kann eine Schemadatei, die eine Liste von Leistungsindikatoren enthält, zur Laufzeit basierend auf der Anforderung aktualisiert werden. Standardmäßig ist die Datei `/var/metrics_conf/schema.json`mit einer Liste von Leistungsindikatoren konfiguriert.

> **Hinweis:**
>
> Die Standardschemadatei von Metrics Collector `/var/metrics_conf/schema.json` kann auf einer NetScaler-Appliance installiert werden, indem Sie das Installationsverfahren verwenden.

Konfigurieren Sie den Metrik-Collector für das Abonnieren von Zählern über die CLI

Starten Sie den Metrikenexport, indem Sie einen Collector-Service konfigurieren

Geben Sie in der Befehlszeile Folgendes ein:

```
set analytics profile ns_analytics_time_series_profile -metrics ENABLED
     -collectors <collector_name> -schemaFile  schema.json -outputMode <
    avro | prometheus>

<!--NeedCopy-->
```

> **Hinweis:**
>
> `schema.json` ist die standardmäßige SchemaFile-Konfiguration.

Eine neue Schemadatei mit einem erforderlichen Satz von Zählern kann mit dem CLI-Befehl für den Export des Metrik-Collectors konfiguriert werden. Die Schemadatei muss am Speicherort `/var/metrics_conf/` vorhanden sein.

Die Schemadatei mit der gesamten Liste von Zählern (reference_schema.json), die von stats infra unterstützt werden, ist am Speicherort `/var/metrics_conf/` vorhanden. Diese Datei kann als Referenz verwendet werden, um eine benutzerdefinierte Liste von Zählern zu erstellen.

Konfigurieren einer Schemadatei mit der CLI

```
set analytics profile ns_analytics_time_series_profile -metrics ENABLED
     -collectors <collector name> -schemaFile <schema file_name> -
    outputMode <avro | prometheus>

<!--NeedCopy-->
```

Eine neue Schemadatei mit den erforderlichen Leistungsindikatoren kann mit dem vorherigen CLI-Befehl für den Export des Metriksammlers hinzugefügt und konfiguriert werden.

Die Referenzschemadatei mit der gesamten Liste von Leistungsindikatoren (reference_schema.json), die von stats infra unterstützt werden, sind im Speicherort /var/metrics_conf/ vorhanden. Diese Datei kann als Referenz verwendet werden, um eine benutzerdefinierte Liste von Zählern zu erstellen.

Überprüfen Sie die Ausgabe der CLI-Konfiguration an der Eingabeaufforderung:

```
show analytics profile ns_analytics_time_series_profile

    Name: ns_analytics_time_series_profile
    Collector: <collector_name>
    Profile-type: timeseries
    Output Mode: avro
    Metrics: ENABLED
    Schema File: schema.json
    Events: ENABLED
    Auditlog: DISABLED
    Serve mode: Push
    Reference Count: 0

<!--NeedCopy-->
```

Schritte zum Aktualisieren der Liste der exportierten Leistungsindikatoren

Im folgenden Verfahren werden die Schritte zum Aktualisieren der Liste der exportierten Leistungsindikatoren beschrieben:

1. Aktualisieren Sie die benutzerdefinierte/neue Schemadatei.
2. Deaktivieren oder aktivieren Sie Metriken mit der Option -metrics, die in der CLI-Konfiguration für die Verwendung der aktualisierten Schemadatei angezeigt wird.

Unterstützung mehrerer Zeitreihenprofile

Der Metriksammler unterstützt bis zu drei Zeitreihenprofilkonfigurationen auf der NetScaler-Appliance.
Sie können jede Zeitreihe so konfigurieren, dass sie Folgendes hat.

- Collector.
- Schemadatei, die die erforderlichen Leistungsindikatoren für den Export enthält.
- Das Datenformat, in dem die Metriken exportiert werden sollen.
- Die Option zum Aktivieren oder Deaktivieren von Messwert-Überwachungsprotokollen und Ereignissen

Mit der Unterstützung mehrerer Zeitreihenprofile kann der Metrik-Kollektor gleichzeitig einen anderen Satz (basierend auf der konfigurierten Schemadatei) von Metriken an verschiedene Collectors in verschiedenen Formaten (AVRO, Prometheus, Influx) exportieren.

Hinzufügen eines Zeitreihenprofils über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add analytics profile <profile_name> -type timeseries
<!--NeedCopy-->
```

Zeitreihenprofil mit der CLI konfigurieren

Geben Sie in der Befehlszeile Folgendes ein:

```
set analytics profile <profile_name> -metrics <DISABLED|ENABLED> -
    auditlogs <DISABLED|ENABLED> -events <DISABLED|ENABLED> -collectors
    <collector_name> -schemaFile schema.json -outputMode <avro | influx
    | prometheus>

<!--NeedCopy-->
```

Namenskonventionen für Protokolldateien mit Unterstützung mehrerer Zeitreihenprofile

- Avro-Protokolldateien werden generiert als `metrics_avro_<profile_name>_log.*`.
- Prometheus-Protokolldateien werden als generiert `metrics_prom_<profile_name>.log`.

> **Hinweise:**
>
> - Obwohl Metriken für alle konfigurierten Zeitreihenprofile aktiviert werden können, können Ereignisse und Überwachungsprotokolle nur für ein Profil aktiviert werden.
> - Die dynamische Schemafunktion wird ab Version 13.1 Build 23.16 unterstützt.
> - Das mehrfache Zeitreihenprofil wird ab Version 13.1 Build 33.6 unterstützt.

Exportieren von Leistungsdaten von Webseiten in den AppFlow Collector

May 11, 2023

Die EdgeSight Monitoring-Anwendung bietet Webseiten-Überwachungsdaten, mit denen Sie die Leistung verschiedener Webanwendungen überwachen können, die in einer NetScaler-Umgebung

bereitgestellt werden. Sie können diese Daten jetzt in AppFlow-Collectors exportieren, um eine eingehende Analyse der Webseitenanwendungen zu erhalten. AppFlow, der auf dem IPFIX-Standard basiert, liefert spezifischere Informationen über die Leistung von Webanwendungen als EdgeSight-Monitoring allein.

Sie können sowohl den Lastausgleich als auch den virtuellen Content Switching-Server konfigurieren, um EdgeSight Monitoring-Daten in AppFlow -Sammler zu exportieren. Bevor Sie einen virtuellen Server für den AppFlow-Export konfigurieren, ordnen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring-Responder-Richtlinie zu.

Die folgenden Leistungsdaten der Webseite werden in AppFlow exportiert:

- **Seitenladezeit**. Verstrichene Zeit in Millisekunden, von dem Zeitpunkt an, zu dem der Browser das erste Byte einer Antwort empfängt, bis der Benutzer beginnt, mit der Seite zu interagieren. In diesem Stadium werden möglicherweise nicht alle Seiteninhalte geladen.
- **Renderzeit der Seite**. Verstrichene Zeit in Millisekunden, ab dem der Browser das erste Antwortbyte erhält, bis entweder der gesamte Seiteninhalt gerendert wurde oder die Aktion zum Laden der Seite abgelaufen ist.
- **Verbrachte Zeit auf der Seite**. Zeit, die von Benutzern auf einer Seite verbracht wird. Stellt die Zeit von einer Seitenanforderung zur nächsten dar.

AppFlow überträgt die Performance-Daten mithilfe des IPFIX-Formats (Internet Protocol Flow Information Export), bei dem es sich um einen offenen IETF-Standard (Internet Engineering Task Force) handelt, der in RFC 5101 definiert ist. Die AppFlow-Vorlagen verwenden die folgenden unternehmensspezifischen Informationselemente (EIEs), um die Informationen zu exportieren:

- **Endzeit des Clients**. Zeitpunkt, zu dem der Browser das letzte Byte einer Antwort erhalten hat, um alle Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.
- **Startzeit für das Laden des Clients**. Zeitpunkt, zu dem der Browser das erste Byte der Antwort erhält, um Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.
- **Endzeit des Client-Rendering-Clients**. Zeitpunkt, zu dem ein Browser die gesamte Seite einschließlich der eingebetteten Objekte beendet hat.
- **Client-Render-Startzeit**. Zeitpunkt, zu dem der Browser mit dem Rendern der Seite begonnen hat.

Voraussetzungen für den Export von Leistungsdaten von Webseiten in AppFlow Collectors

Bevor Sie die AppFlow -Aktion mit der AppFlow-Richtlinie verknüpfen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die AppFlow-Funktion wurde aktiviert und konfiguriert.
- Die Responder-Funktion wurde aktiviert.
- Die EdgeSight-Überwachungsfunktion wurde aktiviert.

- Die EdgeSight-Überwachung wurde auf den virtuellen Lastausgleichs- oder Content Switching-Servern aktiviert, die an die Dienste von Anwendungen gebunden sind, für die Sie die Performance-Daten erfassen möchten.

Verknüpfen einer AppFlow-Aktion mit der EdgeSight-Monitoring-Responder-Richtlinie

Um die Leistungsdaten der Webseite in den AppFlow-Collector zu exportieren, müssen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring-Responder-Richtlinie verknüpfen. Eine AppFlow -Aktion gibt an, welche Kollektoren den Datenverkehr empfangen.

So verknüpfen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring Responder-Richtlinie über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set responder policy <name> -appflowAction <action_Name>
<!--NeedCopy-->
```

Beispiel

```
set responder policy pol -appflowAction actn
<!--NeedCopy-->
```

So verknüpfen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring-Responder-Richtlinie über die grafische Benutzeroberfläche

1. Navigieren Sie zu **AppExpert** > **Responder** > **Policies**.
2. Wählen Sie im Detailbereich eine Responder-Richtlinie für die EdgeSight Monitoring aus, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Dialogfeld Responder-Richtlinie konfigurieren** in der Dropdownliste **AppFlow-Aktion** die AppFlow-Aktion aus, die mit den Collectors verknüpft ist, an die Sie die Leistungsdaten der Webseite senden möchten.
4. Klicken Sie auf **OK**.

Konfigurieren eines virtuellen Servers zum Exportieren von EdgeSight-Statistiken in AppFlow-Collectors

Um EdgeSight-Statistikinformationen von einem virtuellen Server in den AppFlow -Kollektor zu exportieren, müssen Sie dem virtuellen Server eine AppFlow-Aktion zuordnen.

So verknüpfen Sie eine AppFlow-Aktion mit einem virtuellen Load Balancing- oder Content Switching-Server über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**. Sie können auch zu **Traffic Management** > **Content Switching** > **Virtuelle Server**navigieren.
2. Wählen Sie im Detailbereich einen virtuellen Server oder mehrere virtuelle Server aus, und klicken Sie dann auf **EdgeSight-Überwachung aktivieren**.
3. Aktivieren Sie im Dialogfeld EdgeSight-Überwachung aktivieren das Kontrollkästchen **EdgeSight-Statistiken nach Appflow exportieren** .
4. Wählen Sie in der Dropdownliste AppFlow-Aktion die **AppFlow-Aktion** aus. Die AppFlow -Aktion definiert die Liste der AppFlow -Kollektoren, in die EdgeSight-Monitoring-Statistiken exportiert werden. Wenn Sie mehrere virtuelle Lastenausgleichsserver ausgewählt haben, ist dieselbe AppFlow-Aktion mit den an sie gebundenen Responder-Richtlinien verknüpft. Später können Sie die AppFlow-Aktion, die für jeden der ausgewählten virtuellen Load Balancing-Server konfiguriert wurde, gegebenenfalls einzeln ändern.
5. Klicken Sie auf **OK**.

Sitzungszuverlässigkeit bei NetScaler Hochverfügbarkeitspaar

May 11, 2023

Wenn während einer ICA-Sitzung eine Netzwerkunterbrechung oder ein Geräte-Failover auftritt, kann bei der Wiederverbindung einer Sitzung eine von zwei Mechanismen verwendet werden: Sitzungszuverlässigkeit oder Automatische Wiederverbindung des Clients.

Zuverlässigkeit der Sitzung. Der bevorzugte Modus ist eine reibungslose Erfahrung für den Benutzer. Die Störung ist bei kurzen Netzwerkunterbrechungen kaum wahrnehmbar.

Automatische Wiederverbindung von Clients: Die Fallback-Option beinhaltet einen Neustart des Clients. Dieser Mechanismus ist für den Benutzer störend und wird nicht immer unterstützt.

Empfänger können ihre ICA-Sitzungen mithilfe der Funktion zur Zuverlässigkeit von ICA-Sitzungen nahtlos wieder verbinden, wenn HDX Insight aktiviert ist.
Diese Funktion funktioniert sowohl in der eigenständigen Konfiguration als auch in einer NetScaler HA-Paarkonfiguration und sogar dann, wenn ein NetScaler-Failover auftritt.

> **Hinweis:**
>
> - NetScaler-Appliances müssen auf der Softwareversion 11.1 Build 49.16 oder höher ausgeführt werden.
> - Sie dürfen den Sitzungszuverlässigkeitsmodus nicht aktivieren oder deaktivieren, wenn die NetScaler-Appliances über aktive Verbindungen verfügen.

- Das Aktivieren oder Deaktivieren der Funktion bei noch aktiven Verbindungen führt dazu, dass HDX Insight die Analyse dieser Sitzungen nach einem Failover beendet. Dies führt zum Verlust von Informationen über die Sitzungen.
- Die Sitzungszuverlässigkeit bei einem Hochverfügbarkeitssetup ist für die NetScaler-Softwareversion 11.1 49.16 oder höher standardmäßig deaktiviert. Die Sitzungszuverlässigkeit wird bei einem Hochverfügbarkeitssetup nur unterstützt, wenn auf beiden Knoten des Setups derselbe Build ausgeführt wird (z. B. Version 11.1 Build 53). Mit anderen Worten, Sitzungszuverlässigkeit wird bei einem Hochverfügbarkeitssetup nicht unterstützt, wenn auf beiden Knoten unterschiedliche Builds ausgeführt werden (z. B. ein Knoten mit Version 11.1 Build 53 und der andere Version 11.1 Build 56). Die Sitzungszuverlässigkeit für SSL VDA wird unterstützt, wenn die folgenden Bedingungen erfüllt sind:
  - The "EnableSRonHAFailover" parameter in the `set ica parameter` command must be YES.
  - The HTTPS must be used instead of HTTP while configuring the virtual server.
- Wenn HDX Insight aktiviert ist, verbinden sich grundlegende Verschlüsselungsanwendungen und -desktops nach einem Hochverfügbarkeitsfailover wieder, selbst wenn der Parameter EnableSronhaLover deaktiviert ist.

So konfigurieren Sie die Sitzungszuverlässigkeit mit CLI:

1. Verwenden Sie in der Befehlszeile die standardmäßigen Anmeldeinformationen des Systemadministrators, um sich am System anzumelden.
2. Um die Sitzungszuverlässigkeit bei HA-Failover zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein: `set ica parameter EnableSRonHAFailover YES`
3. Um die Sitzungszuverlässigkeit bei HA-Failover zu deaktivieren, geben Sie an der Eingabeaufforderung Folgendes ein: `set ica parameter EnableSRonHAFailover NO`

So aktivieren Sie die Sitzungszuverlässigkeit bei HA-Failover über die grafische Benutzeroberfläche:

1. Geben Sie in einem Webbrowser die IP-Adresse der primären NetScaler Instanz im HA-Paar ein (z. B.http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Einstellungen**, und klicken Sie auf **ICA-Parameter ändern**.
4. Wählen Sie im Abschnitt **Ändern der ICA-Parameter** die Option **Sitzungszuverlässigkeit bei HA-Failover** aus.
5. Klicken Sie auf **OK**.

Einschränkungen

- Das Aktivieren dieser Funktion führt zu einem erhöhten Bandbreitenverbrauch, der darauf zurückzuführen ist, dass die ICA-Komprimierung durch die Funktion deaktiviert wurde. Und

der zusätzliche Datenverkehr zwischen den primären und sekundären Knoten, um sie synchron zu halten.
- Diese Funktion wird nur im Aktiv-Passiv-Modus unterstützt. Der Aktiv-Aktiv-Modus wird derzeit nicht unterstützt.
- Wenn HDX Insight aktiviert ist und die Sitzungszuverlässigkeit auf dem HA-Regler auf NEIN gesetzt ist, wird im NetScaler High Availability Failover-Szenario nur der ACR-Wiederverbindungsmodus unterstützt. Der HA-Regler deaktiviert die Sitzungszuverlässigkeit nicht, wenn HDX Insight deaktiviert ist.

Die **Session Reconnect Semantik-Tabelle** lautet wie folgt:

Session verbindet Semantik

Status	EnableSRonHAFailover Yes	EnableSRonHAFailover No (Standard)
HDX Insight aktiviert	Wiederverbinden der Sitzung für ICA-Sitzung funktioniert	Die Wiederverbindung von Sitzungen für ICA-Sitzungen funktioniert nicht
HDX Insight deaktiviert	Wiederverbinden der Sitzung für ICA-Sitzung funktioniert	Wiederverbinden von Sitzungen für ICA-Sitzungen funktioniert

Wichtige Hinweise

- Die Sitzungszuverlässigkeit für ICA-Sitzungen funktioniert standardmäßig mit NetScaler Gateway.
- Die Sitzungszuverlässigkeit für ICA-Sitzungen funktioniert nicht, wenn die beiden folgenden Bedingungen erfüllt sind:
  - HDX Insight ist aktiviert
  - EnableSRonHAFailover ist auf NO gesetzt
- Das Festlegen des EnableSRonHAFailover-Reglers auf YES oder NO macht keinen Unterschied, wenn HDX Insight deaktiviert ist.

NetScaler Web App Firewall

June 19, 2023

Die NetScaler Web App Firewall bietet einfach zu konfigurierende Optionen, um eine Vielzahl von Anwendungssicherheitsanforderungen zu erfüllen. Web App Firewall-Profile, die aus einer Reihe

von Sicherheitsprüfungen bestehen, können verwendet werden, um sowohl die Anfragen als auch die Antworten zu schützen, indem umfassende Inspektionen auf Paketebene durchgeführt werden. Jedes Profil enthält eine Option, mit der Sie grundlegende oder erweiterte Schutzmaßnahmen auswählen können. Einige Schutzmaßnahmen erfordern möglicherweise die Verwendung anderer Dateien. Beispielsweise können für XML-Validierungsprüfungen WSDL- oder Schemadateien erforderlich sein. Die Profile können auch andere Dateien verwenden, z. B. Signaturen oder Fehlerobjekte. Diese Dateien können lokal hinzugefügt oder im Vorfeld importiert und zur späteren Verwendung auf der Appliance gespeichert werden.

Jede Richtlinie identifiziert einen Typ von Datenverkehr, und dieser Datenverkehr wird auf die Sicherheitsüberprüfungsverletzungen überprüft, die in dem Profil angegeben sind, das der Richtlinie zugeordnet ist. Die Richtlinien können unterschiedliche Bindungspunkte haben, die den Geltungsbereich der Richtlinie bestimmen. Beispielsweise wird eine Richtlinie, die an einen bestimmten virtuellen Server gebunden ist, nur für den Datenverkehr aufgerufen und ausgewertet, der durch diesen virtuellen Server fließt. Die Richtlinien werden in der Reihenfolge ihrer festgelegten Prioritäten bewertet, und die erste, die der Anfrage oder Antwort entspricht, wird angewendet.

- Schnelle Bereitstellung des Web App Firewall-Schutzes

  Sie können das folgende Verfahren für die schnelle Bereitstellung der Web App Firewall-Sicherheit verwenden:

  1. Fügen Sie ein Web App Firewall-Profil hinzu und wählen Sie den entsprechenden Typ (html, xml, JSON) für die Sicherheitsanforderungen der Anwendung aus.
  2. Wählen Sie das erforderliche Sicherheitsniveau (Basic oder Advanced).
  3. Fügen Sie die erforderlichen Dateien wie Signaturen oder WSDL hinzu oder importieren Sie sie.
  4. Konfigurieren Sie das Profil für die Verwendung der Dateien und nehmen Sie alle anderen erforderlichen Änderungen an den Standardeinstellungen vor.
  5. Fügen Sie eine Web App Firewall-Richtlinie für dieses Profil hinzu.
  6. Binden Sie die Richtlinie an den Zielbindepunkt und geben Sie die Priorität an.

- Web App Firewall Entitäten

  Profil— Ein Web App Firewall-Profil gibt an, worauf zu achten ist und was zu tun ist. Es prüft sowohl die Anfrage als auch die Antwort, um festzustellen, welche potenziellen Sicherheitsverstöße überprüft werden müssen und welche Maßnahmen bei der Verarbeitung einer Transaktion ergriffen werden müssen. Ein Profil kann eine HTML-, XML- oder HTML- und XML-Payload schützen. Abhängig von den Sicherheitsanforderungen der Anwendung können Sie entweder ein Basisprofil oder ein erweitertes Profil erstellen. Ein Basisprofil kann vor bekannten Angriffen schützen. Wenn eine höhere Sicherheit erforderlich ist, können Sie ein erweitertes Profil bereitstellen, um den kontrollierten Zugriff auf die Anwendungsressourcen zu ermöglichen und Zero-Day-Angriffe zu blockieren. Ein Basisprofil kann jedoch geändert werden, um erweiterte

Schutzfunktionen zu bieten, und umgekehrt. Es stehen mehrere Aktionsoptionen (z. B. blockieren, protokollieren, lernen und transformieren) zur Verfügung. Erweiterte Sicherheitsprüfungen verwenden möglicherweise Sitzungscookies und versteckte Formular-Tags zur Steuerung und Überwachung der Client-Verbindungen. Web App Firewall Profile können die ausgelösten Verstöße lernen und die Relaxationsregeln vorschlagen.

Grundlegender Schutz—Ein Basisprofil enthält einen vorkonfigurierten Satz von Regeln für die Lockerung von Start-URL und URL verweigern. Diese Relaxationsregeln legen fest, welche Anfragen erlaubt und welche abgelehnt werden müssen. Eingehende Anfragen werden mit diesen Listen abgeglichen und die konfigurierten Aktionen werden angewendet. Auf diese Weise kann der Benutzer Anwendungen mit minimaler Konfiguration für Entspannungsregeln sichern. Die Start-URL-Regeln schützen vor erzwungenen Surfen. Bekannte Webserver-Schwachstellen, die von Hackern ausgenutzt werden, können erkannt und blockiert werden, indem eine Reihe von standardmäßigen Deny-URL-Regeln aktiviert wird. Häufig gestartete Angriffe wie Pufferüberlauf, SQL oder siteübergreifende Skripterstellung können ebenfalls leicht erkannt werden.

Erweiterter Schutz— Wie der Name schon sagt, werden erweiterte Schutzmaßnahmen für Anwendungen verwendet, die höhere Sicherheitsanforderungen haben. Relaxationsregeln sind so konfiguriert, dass nur der Zugriff auf bestimmte Daten ermöglicht und der Rest blockiert wird. Dieses positive Sicherheitsmodell mildert unbekannte Angriffe, die durch grundlegende Sicherheitsüberprüfungen möglicherweise nicht erkannt werden. Zusätzlich zu allen grundlegenden Schutzmaßnahmen verfolgt ein erweitertes Profil die Benutzersitzung, indem es das Surfen steuert, nach Cookies sucht, Eingabeanforderungen für verschiedene Formularfelder spezifiziert und vor Manipulation von Formularen oder seitenübergreifenden Angriffen zur Fälschung von Anfragen schützt. Das Lernen, das den Verkehr beobachtet und die entsprechenden Entlastungen einleitet, ist für viele Sicherheitschecks standardmäßig aktiviert. Obwohl sie einfach zu bedienen sind, erfordern erweiterte Schutzmaßnahmen gebührende Berücksichtigung, da sie eine engere Sicherheit bieten, aber auch mehr Verarbeitung erfordern und keine Verwendung von Caching zulassen, was die Leistung beeinträchtigen kann.

Importieren— Die Importfunktion ist nützlich, wenn Web App Firewall-Profile externe Dateien verwenden müssen, dh Dateien, die auf einem externen oder internen Webserver gehostet werden, oder die von einem lokalen Computer kopiert werden müssen. Das Importieren einer Datei und das Speichern auf der Appliance ist nützlich, insbesondere in Situationen, in denen Sie den Zugriff auf externe Websites steuern müssen oder in denen die Kompilierung lange dauert, große Dateien über HA-Bereitstellungen synchronisiert werden müssen, oder Sie können eine Datei wiederverwenden, indem Sie sie auf mehrere Geräte kopieren. Beispiel:

- WSDLs, die auf externen Webservern gehostet werden, können lokal importiert werden, bevor der Zugriff auf externe Websites blockiert wird.
- Große Signaturdateien, die von einem externen Scan-Tool wie Cenzic generiert wurden, können mithilfe eines Schemas auf der NetScaler ADC-Appliance importiert und vorkom-

piliert werden.
- Eine benutzerdefinierte HTML- oder XML-Fehlerseite kann von einem externen Webserver importiert oder aus einer lokalen Datei kopiert werden.

Signaturen— Signaturen sind mächtig, da sie Musterabgleich verwenden, um bösartige Angriffe zu erkennen und so konfiguriert werden können, dass sie sowohl die Anforderung als auch die Antwort einer Transaktion überprüfen. Sie sind eine bevorzugte Option, wenn eine anpassbare Sicherheitslösung benötigt wird. Für die Aktion, die ausgeführt werden soll, wenn eine Signaturübereinstimmung erkannt wird, stehen mehrere Optionen zur Verfügung (z. B. blockieren, protokollieren, lernen und transformieren). Die Web App Firewall verfügt über ein integriertes Standardsignaturobjekt, das aus mehr als 1.300 Signaturregeln besteht, mit der Option, die neuesten Regeln mithilfe der automatischen Aktualisierungsfunktion abzurufen. Regeln, die von anderen Scan-Tools erstellt wurden, können ebenfalls importiert werden. Das Signaturobjekt kann angepasst werden, indem neue Regeln hinzugefügt werden, die mit den anderen im Web App Firewall-Profil angegebenen Sicherheitsprüfungen funktionieren können. Eine Signaturregel kann mehrere Muster haben und kann einen Verstoß nur kennzeichnen, wenn alle Muster übereinstimmen, wodurch Fehlalarme vermieden werden. Die sorgfältige Auswahl eines wörtlichen Musters `fastmatch` für eine Regel kann die Bearbeitungszeit erheblich optimieren.

Richtlinien— Web App Firewall-Richtlinien werden verwendet, um den Datenverkehr in verschiedene Typen zu filtern und zu trennen. Dies bietet die Flexibilität, verschiedene Sicherheitsebenen für die Anwendungsdaten zu implementieren. Der Zugriff auf hochsensible Daten kann durch erweiterte Sicherheitsprüfungen erfolgen, während weniger sensible Daten durch grundlegende Sicherheitsinspektionen geschützt werden. Richtlinien können auch so konfiguriert werden, dass die Sicherheitskontrolle auf harmlosen Datenverkehr Bypass wird. Höhere Sicherheit erfordert mehr Verarbeitung, sodass eine sorgfältige Gestaltung der Richtlinien die gewünschte Sicherheit sowie eine optimierte Leistung bieten kann. Die Priorität der Richtlinie bestimmt die Reihenfolge, in der sie bewertet wird, und ihr Bindungspunkt bestimmt den Anwendungsbereich.

Highlights

1. Fähigkeit, eine Vielzahl von Anwendungen abzusichern, indem verschiedene Datentypen geschützt werden, das richtige Sicherheitsniveau für verschiedene Ressourcen implementiert und dennoch maximale Leistung erzielt wird.
2. Flexibilität beim Hinzufügen oder Ändern einer Sicherheitskonfiguration. Sie können die Sicherheitskontrollen verschärfen oder lockern, indem Sie grundlegende und erweiterte Schutzmaßnahmen aktivieren oder deaktivieren.
3. Option zur Konvertierung eines HTML-Profils in ein XML- oder Web2.0-Profil (HTML+XML) und umgekehrt, was die Flexibilität bietet, Sicherheit für verschiedene Payload-Typen hinzuzufü-

gen.

4. Einfach zu implementierende Aktionen, um Angriffe zu blockieren, sie in Protokollen zu überwachen, Statistiken zu sammeln oder sogar einige Angriffsfolgen zu transformieren, um sie unschädlich zu machen.
5. Fähigkeit, Angriffe durch die Prüfung eingehender Anfragen zu erkennen und den Verlust sensibler Daten zu verhindern, indem die von den Servern gesendeten Antworten überprüft werden.
6. Fähigkeit, aus dem Verkehrsmuster zu lernen, um Empfehlungen für leicht editierbare Lockerungsregeln zu erhalten, die eingesetzt werden können, um Ausnahmen zuzulassen.
7. Hybrides Sicherheitsmodell, das die Macht anpassbarer Signaturen nutzt, um Angriffe zu blockieren, die bestimmten Mustern entsprechen, und das die Flexibilität bietet, die Prüfungen des positiven Sicherheitsmodells für grundlegende oder erweiterte Sicherheitsvorkehrungen zu verwenden.
8. Verfügbarkeit umfassender Konfigurationsberichte, einschließlich Informationen zur PCI-DSS-Konformität.

Häufig gestellte Fragen und Bereitstellungshandbuch

June 19, 2023

F: Warum ist NetScaler Web App Firewall die bevorzugte Wahl für die Sicherung von Anwendungen?

Mit den folgenden Funktionen bietet die NetScaler Web App Firewall eine umfassende Sicherheitslösung:

- **Hybrides Sicherheitsmodell:** Mit dem NetScaler Hybrid-Sicherheitsmodell können Sie sowohl ein positives Sicherheitsmodell als auch ein negatives Sicherheitsmodell nutzen, um eine Konfiguration zu erstellen, die für Ihre Anwendungen ideal geeignet ist.
  - **Positives Sicherheitsmodell** schützt vor Pufferüberlauf, CGI-BIN-Parametermanipulation, Formular-/Hidden-Feld-Manipulation, kraftvollem Surfen, Cookie- oder Sitzungsvergiftung, defekten ACLs, Cross-Site Scripting (Cross-Site-Scripting), Befehlseinschleusung, SQL-Einschleusung, Fehlerauslösung empfindlich Informationsleck, unsichere Verwendung von Kryptographie, Server-Fehlkonfiguration, Hintertüren und Debug-Optionen, ratenbasierte Durchsetzung von Richtlinien, bekannte Plattformschwachstellen, Zero-Day-Exploits, Cross Site Request Forgery (CSRF) und das Auslaufen von Kreditkarten und anderen sensiblen Daten.
  - Das**negative Sicherheitsmodell** verwendet umfangreiche Signaturen, um sich vor L7- und HTTP-Anwendungsschwachstellen zu schützen. Die Web App Firewall ist in mehrere Scan-Tools von Drittanbietern integriert, z. B. in die von Cenzic, Qualys, Whitehat und

IBM angebotenen. Die eingebauten XSLT-Dateien ermöglichen den einfachen Import von Regeln, die in Verbindung mit den Snort-basierten Regeln im nativen Format verwendet werden können. Eine automatische Update-Funktion erhält die neuesten Updates für neue Schwachstellen.

Das positive Sicherheitsmodell könnte die bevorzugte Wahl für den Schutz von Anwendungen sein, die einen hohen Sicherheitsbedarf haben, da es Ihnen die Möglichkeit gibt, vollständig zu steuern, wer auf welche Daten zugreifen kann. Du erlaubst nur was du willst und blockierst den Rest. Dieses Modell beinhaltet eine integrierte Sicherheitsüberprüfungskonfiguration, die mit wenigen Klicks einsetzbar ist. Beachten Sie jedoch, dass der Verarbeitungsaufwand umso größer ist, je enger die Sicherheit ist.

Das negative Sicherheitsmodell könnte für kundenspezifische Anwendungen vorzuziehen sein. Mit den Signaturen können Sie mehrere Bedingungen kombinieren, und eine Übereinstimmung und die angegebene Aktion werden nur ausgelöst, wenn alle Bedingungen erfüllt sind. Du blockierst nur das, was du nicht willst und erlaubst den Rest. Ein bestimmtes Fast-Match-Muster an einem bestimmten Ort kann den Verarbeitungsaufwand erheblich reduzieren, um die Leistung zu optimieren. Die Option, basierend auf den spezifischen Sicherheitsanforderungen Ihrer Anwendungen eigene Signaturregeln hinzuzufügen, gibt Ihnen die Flexibilität, Ihre eigenen benutzerdefinierten Sicherheitslösungen zu entwickeln.

- **Erkennung und Schutz auf der Anforderungs- sowie Antwortseite:** Sie können die eingehenden Anfragen überprüfen, um verdächtiges Verhalten zu erkennen und geeignete Maßnahmen zu ergreifen, und Sie können die Antworten überprüfen, um sensible Daten zu erkennen und vor dem Auslaufen sensibler Daten zu schützen.
- **Umfangreicher Satz integrierter Schutzmaßnahmen für HTML-, XML- und JSON-Nutzlasten:** Die Web App Firewall bietet 19 verschiedene Sicherheitsüberprüfungen. Sechs davon (wie Start-URL und Verweigerungs-URL) gelten sowohl für HTML- als auch für XML-Daten. Fünf Prüfungen (wie Field Consistency und Field Format) sind spezifisch für HTML, und acht (wie XML-Format und Webdienst-Interoperabilität) sind spezifisch für XML-Nutzlasten. Diese Funktion beinhaltet eine Vielzahl von Aktionen und Optionen. Mit URL Closure können Sie beispielsweise die Navigation durch Ihre Website steuern und optimieren, um sich vor kraftvollem Surfen zu schützen, ohne Entspannungsregeln konfigurieren zu müssen, um jede einzelne legitime URL zuzulassen. Sie haben die Möglichkeit, die sensiblen Daten, wie Kreditkartennummern, in der Antwort zu entfernen oder zu löschen. Sei es SOAP-Array-Angriffsschutz, XML Denial of Service (XDoS), WSDL-Scan-Prävention, Attachment-Check oder eine beliebige Anzahl anderer XML-Angriffe, Sie haben die Gewissheit, dass Sie über einen ironclad Shield verfügen, der Ihre Daten schützt, wenn Ihre Anwendungen durch die Web App Firewall geschützt sind. Mit den Signaturen können Sie Regeln mithilfe von XPath-Ausdrücken konfigurieren, um Verletzungen im Hauptteil sowie im Header einer JSON-Nutzlast zu erkennen.
- **GWT:** Unterstützung für den Schutz von Google Web Toolkit-Anwendungen zum Schutz vor Ver-

stößen gegen SQL, Cross-Site Scripting und Form Field Consistency Check.

- **Java-freie, benutzerfreundliche grafische Benutzeroberfläche (GUI):** Eine intuitive Benutzeroberfläche und vorkonfigurierte Sicherheitsüberprüfungen erleichtern die Bereitstellung von Sicherheit durch Klicken auf wenige Schaltflächen. Ein Assistent fordert Sie auf und leitet Sie an, die erforderlichen Elemente wie Profile, Richtlinien, Signaturen und Bindungen zu erstellen. Die HTML5-basierte GUI ist frei von jeglicher Java-Abhängigkeit. Die Leistung ist deutlich besser als die der älteren, Java-basierten Versionen.
- **Benutzerfreundliche und automatisierbare CLI:** Die meisten Konfigurationsoptionen, die in der GUI verfügbar sind, sind auch in der Befehlszeilenschnittstelle (CLI) verfügbar. Die CLI-Befehle können von einer Batch-Datei ausgeführt werden und sind einfach zu automatisieren.
- **Unterstützung für REST-API:** Das NetScaler NITRO-Protokoll unterstützt eine Vielzahl von REST-APIs, um die Konfiguration der Web App Firewall zu automatisieren und relevante Statistiken für die laufende Überwachung von Sicherheitsverletzungen zu sammeln.
- **Lernen:** Die Fähigkeit der Web App Firewall, durch Überwachung des Datenverkehrs zu lernen, um die Sicherheit zu optimieren, ist sehr benutzerfreundlich. Die Lernmaschine empfiehlt Regeln, die es einfach machen, Entspannungen ohne Kenntnisse in regulären Ausdrücken einzusetzen.
- **RegEx-Editor-Unterstützung:** Reguläre Ausdrücke bieten eine elegante Lösung für das Dilemma, Regeln konsolidieren und dennoch die Suche optimieren zu wollen. Sie können die Leistungsfähigkeit regulärer Ausdrücke nutzen, um URLs, Feldnamen, Signaturmuster usw. zu konfigurieren. Der umfangreiche integrierte GUI RegEx Editor bietet Ihnen eine Kurzreferenz für die Ausdrücke und bietet eine bequeme Möglichkeit, Ihre RegEx auf Genauigkeit zu validieren und zu testen.
- **Benutzerdefinierte Fehlerseite:** Blockierte Anfragen können auf eine Fehler-URL umgeleitet werden. Sie haben auch die Möglichkeit, ein benutzerdefiniertes Fehlerobjekt anzuzeigen, das unterstützte Variablen und erweiterte NetScaler-Richtlinien (erweiterte PI-Ausdrücke) verwendet, um Informationen zur Fehlerbehebung für den Client einzubetten.
- **PCI-DSS, Statistiken und andere Verstöße:** Die umfangreichen Berichte machen es einfach, die PCI-DSS-Compliance-Anforderungen zu erfüllen, Statistiken über Verkehrszähler zu sammeln und Verstoßberichte für alle Profile oder nur ein Profil anzuzeigen.
- **Protokollierung und Click-to-Rule aus dem Protokoll:** Detaillierte Protokollierung wird sowohl für das native als auch für das CEF-Format unterstützt. Die Web App Firewall bietet Ihnen die Möglichkeit, gezielte Protokollmeldungen im Syslog-Viewer zu filtern. Mit einem einfachen Klick auf eine Schaltfläche können Sie eine Protokollnachricht auswählen und eine entsprechende Entspannungsregel bereitstellen. Sie haben die Flexibilität, Protokollnachrichten anzupassen und unterstützen auch das Generieren von Webprotokollen. Weitere Informationen finden Sie im Thema Web App Firewall-Protokolle.

- **Verletzungsprotokolle in Trace-Datensätze einschließen:** Die Möglichkeit, Protokollmeldungen in die Ablaufverfolgungsdatensätze einzuschließen, macht es sehr einfach, unerwartetes Verhalten wie Zurücksetzen und Blockieren zu debuggen.
- **Klonen:** Mit der nützlichen Profiloption Import/Export können Sie die Sicherheitskonfiguration von einer NetScaler-Appliance auf andere klonen. Exportoptionen für gelernte Daten machen es einfach, die erlernten Regeln in eine Excel-Datei zu exportieren. Sie können sie dann vom Eigentümer des Antrags überprüfen und genehmigen lassen, bevor Sie sie beantragen.
- **Eine AppExpert-Vorlage** (eine Reihe von Konfigurationseinstellungen) kann so gestaltet werden, dass sie einen angemessenen Schutz für Ihre Websites bietet. Sie können die Bereitstellung eines ähnlichen Schutzes auf anderen Appliances vereinfachen und beschleunigen, indem Sie diese Cookie-Cutter-Vorlagen in eine Vorlage exportieren.

Weitere Informationen finden Sie im Thema AppExpert-Vorlage.

- **Sitzungslose Sicherheitsprüfungen:** Durch die Bereitstellung sitzungsloser Sicherheitsprüfungen können Sie den Speicherbedarf reduzieren und die Verarbeitung beschleunigen.
- **Interoperabilität mit anderen NetScaler-Funktionen:** Die Web App Firewall arbeitet nahtlos mit anderen NetScaler-Funktionen wie Rewrite, URL-Transformation, integriertem Caching, CVPN und Ratenbegrenzung zusammen.
- **Unterstützung von PI-Ausdrücken in Richtlinien:** Sie können die Leistungsfähigkeit erweiterter PI-Ausdrücke nutzen, um Richtlinien zu entwerfen, mit denen verschiedene Sicherheitsstufen für verschiedene Teile Ihrer Anwendung implementiert werden können.
- **Unterstützung für IPv6:** Die Web App Firewall unterstützt sowohl IPv4- als auch IPv6-Protokolle.
- **Geolokationsbasierter Sicherheitsschutz:** Sie haben die Flexibilität, NetScaler Advanced Policy (PI Expressions) zur Konfiguration standortbasierter Richtlinien zu verwenden, die in Verbindung mit einer integrierten Standortdatenbank verwendet werden können, um den Firewallschutz individuell anzupassen. Sie können die Standorte identifizieren, von denen böswillige Anfragen stammen, und das gewünschte Maß an Sicherheitsüberprüfungen für Anfragen durchsetzen, die von einem bestimmten geografischen Standort stammen.
- **Leistung:** Anforderungsseitiges **Streaming** verbessert die Leistung erheblich. Sobald ein Feld verarbeitet wird, werden die resultierenden Daten an das Back-End weitergeleitet, während die Auswertung für die verbleibenden Felder fortgesetzt wird. Die Verbesserung der Verarbeitungszeit ist besonders beim Umgang mit großen Pfosten signifikant.
- **Weitere Sicherheitsfunktionen:** Die Web App Firewall verfügt über mehrere andere Sicherheitseinstellungen, mit denen Sie die Sicherheit Ihrer Daten gewährleisten können. Mit **Confidential Field** können Sie beispielsweise das Durchsickern vertraulicher Informationen in den Protokollnachrichten blockieren, und **Strip HTML Comment** ermöglicht es Ihnen, die HTML-Kommentare aus der Antwort zu entfernen, bevor Sie sie an den Client weiterleiten. **Feldtypen** können verwendet werden, um anzugeben, welche Eingaben in den an Ihre Anwendung über-

mittelten Formularen zulässig sind.

F: Was muss ich tun, um die Web App Firewall zu konfigurieren?

Führen Sie folgende Schritte aus:

- Fügen Sie ein Web App Firewall-Profil hinzu und wählen Sie den entsprechenden Typ (html, xml, web2.0) für die Sicherheitsanforderungen der Anwendung aus.
- Wählen Sie das erforderliche Sicherheitsniveau (Basic oder Advanced).
- Fügen Sie die erforderlichen Dateien wie Signaturen oder WSDL hinzu oder importieren Sie sie.
- Konfigurieren Sie das Profil für die Verwendung der Dateien und nehmen Sie alle anderen erforderlichen Änderungen an den Standardeinstellungen vor.
- Fügen Sie eine Web App Firewall-Richtlinie für dieses Profil hinzu.
- Binden Sie die Richtlinie an den Zielbindepunkt und geben Sie die Priorität an.

F: Woher weiß ich, welchen Profiltyp ich wählen soll?

Das Web App Firewall-Profil bietet Schutz für sowohl HTML- als auch XML-Nutzlasten. Je nach Bedarf Ihrer Anwendung können Sie entweder ein HTML-Profil oder ein XML-Profil wählen. Wenn Ihre Anwendung sowohl HTML- als auch XML-Daten unterstützt, können Sie ein Web2.0-Profil wählen.

F: Was ist der Unterschied zwischen einfachen und erweiterten Profilen? Wie entscheide ich, welches ich brauche?

Die Entscheidung, ein Basic- oder Advance-Profil zu verwenden, hängt von den Sicherheitsbedürfnissen Ihrer Anwendung ab. Ein Basisprofil enthält einen vorkonfigurierten Satz von Regeln zur Entspannung von Start-URL und URL verweigern. Diese Entspannungsregeln legen fest, welche Anfragen zulässig sind und welche abgelehnt werden. Eingehende Anfragen werden mit den vorkonfigurierten Regeln abgeglichen, und die konfigurierten Aktionen werden angewendet. Der Benutzer kann Anwendungen mit minimaler Konfiguration von Entspannungsregeln sichern. Die Start-URL-Regeln schützen vor erzwungenen Surfen. Bekannte Webserver-Schwachstellen, die von Hackern ausgenutzt werden, können erkannt und blockiert werden, indem eine Reihe von standardmäßigen Deny-URL-Regeln aktiviert wird. Häufig gestartete Angriffe wie Pufferüberlauf, SQL oder Cross-Site Scripting können ebenfalls leicht erkannt werden.

Wie der Name schon sagt, gelten erweiterte Schutzmaßnahmen für Anwendungen mit höheren Sicherheitsanforderungen. Relaxationsregeln sind so konfiguriert, dass nur der Zugriff auf bestimmte Daten ermöglicht und der Rest blockiert wird. Dieses positive Sicherheitsmodell mildert unbekannte Angriffe, die durch grundlegende Sicherheitsüberprüfungen möglicherweise nicht erkannt werden. Zusätzlich zu allen grundlegenden Schutzmaßnahmen verfolgt ein erweitertes Profil eine Benutzersitzung, indem es das Surfen steuert, nach Cookies sucht, Eingabeanforderungen für

verschiedene Formularfelder festlegt und vor Manipulation von Formularen oder Cross-Site Request Forgery-Angriffen schützt. Lernen, das den Verkehr beobachtet und entsprechende Lockerungen empfiehlt, ist standardmäßig für viele Sicherheitsüberprüfungen aktiviert. Obwohl sie einfach zu bedienen sind, müssen erweiterte Schutzmaßnahmen gebührend berücksichtigt werden, da sie eine höhere Sicherheit bieten, aber auch mehr Verarbeitung erfordern. Einige Sicherheitsüberprüfungen erlauben keine Verwendung von Caching, was die Leistung beeinträchtigen kann.

Beachten Sie bei der Entscheidung, ob Sie einfache oder erweiterte Profile verwenden möchten, die folgenden Punkte:

- Grundlegende und erweiterte Profile beginnen gerade mit Vorlagen. Sie können das Basisprofil jederzeit ändern, um erweiterte Sicherheitsfunktionen bereitzustellen, und umgekehrt.
- Erweiterte Sicherheitsüberprüfungen erfordern mehr Verarbeitung und können die Leistung beeinträchtigen. Wenn Ihre Anwendung keine erweiterte Sicherheit benötigt, sollten Sie möglicherweise mit einem Basisprofil beginnen und die für Ihre Anwendung erforderliche Sicherheit erhöhen.
- Sie möchten nicht alle Sicherheitsüberprüfungen aktivieren, es sei denn, Ihre Anwendung benötigt sie.

F: Was ist eine Richtlinie? Wie wähle ich den Bindepunkt aus und setze die Priorität?

Web App Firewall-Richtlinien können Ihnen dabei helfen, Ihren Datenverkehr in logische Gruppen zu sortieren, um verschiedene Ebenen der Sicherheitsimplementierung zu konfigurieren. Wählen Sie sorgfältig die Bindungspunkte für die Richtlinien aus, um festzustellen, welcher Datenverkehr mit welcher Richtlinie übereinstimmt. Wenn Sie beispielsweise möchten, dass jede eingehende Anforderung auf SQL/Cross-Site-Scripting-Angriffe überprüft wird, können Sie eine generische Richtlinie erstellen und global binden. Oder wenn Sie strengere Sicherheitsüberprüfungen auf den Datenverkehr eines virtuellen Servers anwenden möchten, der Anwendungen hostet, die sensible Daten enthalten, können Sie eine Richtlinie an diesen virtuellen Server binden.

Eine sorgfältige Zuweisung von Prioritäten kann die Verkehrsverarbeitung verbessern. Sie möchten spezifischeren Richtlinien höhere Prioritäten und generischen Richtlinien niedrigere Prioritäten zuweisen. Beachten Sie, dass die Priorität umso niedriger ist, je höher die Zahl ist. Eine Richtlinie mit einer Priorität von 10 wird vor einer Richtlinie bewertet, die eine Priorität von 15 hat.

Sie können verschiedene Sicherheitsstufen für verschiedene Arten von Inhalten anwenden, z. B. können Anfragen nach statischen Objekten wie Bildern und Text mithilfe einer Richtlinie umgangen werden, und Anfragen für andere vertrauliche Inhalte können mithilfe einer zweiten Richtlinie einer sehr strengen Prüfung unterzogen werden.

F: Wie konfiguriere ich die Regeln zur Sicherung meiner Anwendung?

Die Web App Firewall macht es sehr einfach, das richtige Sicherheitsniveau für Ihre Website zu entwerfen. Sie können mehrere Web App Firewall-Richtlinien haben, die an verschiedene Web App Firewall-Profile gebunden sind, um verschiedene Ebenen von Sicherheitsüberprüfungen für Ihre Anwendungen zu implementieren. Sie können die Protokolle zunächst überwachen, um zu beobachten, welche Sicherheitsbedrohungen erkannt werden und welche Verstöße ausgelöst werden. Sie können die Entspannungsregeln entweder manuell hinzufügen oder die empfohlenen gelernten Regeln der Web App Firewall nutzen, um die erforderlichen Entspannungen bereitzustellen, um Fehlalarme zu vermeiden.

Die NetScaler Web App Firewall bietet **Visualizer-Unterstützung** in der GUI, was die Regelverwaltung sehr einfach macht. Sie können alle Daten einfach auf einem Bildschirm anzeigen und mit einem Klick auf mehrere Regeln eingehen. Der größte Vorteil des Visualizers besteht darin, dass er reguläre Ausdrücke empfiehlt, um mehrere Regeln zu konsolidieren. Sie können eine Teilmenge der Regeln auswählen, wobei Ihre Auswahl auf dem Trennzeichen und der Aktions-URL basiert. Visualizer-Unterstützung ist verfügbar, um 1) erlernte Regeln und 2) Entspannungsregeln anzuzeigen.

1. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Entspannungen einzusetzen. Sie können auch Regeln überspringen (ignorieren).
2. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel hinzuzufügen oder eine bestehende zu bearbeiten. Sie können eine Gruppe von Regeln auch aktivieren oder deaktivieren, indem Sie einen Knoten auswählen und im Entspannungsvisualisierer auf die Schaltfläche **Aktivieren** oder **Deaktivieren** klicken.

F: Was sind Signaturen? Woher weiß ich, welche Signaturen zu verwenden sind?

Eine Signatur ist ein Objekt, das mehrere Regeln haben kann. Jede Regel besteht aus einem oder mehreren Mustern, die einem bestimmten Satz von Aktionen zugeordnet werden können. Die Web App Firewall verfügt über ein integriertes Standardsignaturobjekt, das aus mehr als 1.300 Signaturregeln besteht, mit der Option, mithilfe der **automatischen Update-Funktion** die neuesten Regeln abzurufen, um Schutz vor neuen Sicherheitslücken zu erhalten. Regeln, die von anderen Scan-Tools erstellt wurden, können ebenfalls importiert werden.

Signaturen sind sehr leistungsfähig, da sie Musterabgleich verwenden, um böswillige Angriffe zu erkennen, und so konfiguriert werden können, dass sowohl die Anfrage als auch die Antwort einer Transaktion überprüft werden. Sie sind eine bevorzugte Option, wenn eine anpassbare Sicherheitslösung benötigt wird. Mehrere Aktionsoptionen (z. B. Blockieren, Protokollieren, Lernen und Transformieren) stehen zur Verfügung, wenn eine Signaturübereinstimmung erkannt wird. Die Standardsignaturen decken Regeln zum Schutz verschiedener Arten von Anwendungen ab, wie web-cgi, web-coldfusion, web-frontpage, web-iis, web-php, web-client, web-activex, web-shell-shock und

web-struts. Um den Anforderungen Ihrer Anwendung gerecht zu werden, können Sie die Regeln einer bestimmten Kategorie auswählen und bereitstellen.

Tipps zur Verwendung von Signaturen:

- Sie können einfach eine Kopie des Standardsignaturobjekts erstellen und es ändern, um die benötigten Regeln zu aktivieren und die gewünschten Aktionen zu konfigurieren.
- Das Signaturobjekt kann durch Hinzufügen neuer Regeln angepasst werden, die in Verbindung mit anderen Signaturregeln funktionieren können.
- Die Signaturregeln können auch so konfiguriert werden, dass sie in Verbindung mit den im Web App Firewall-Profil angegebenen Sicherheitsüberprüfungen funktionieren. Wenn eine Übereinstimmung, die auf einen Verstoß hinweist, sowohl durch eine Signatur als auch durch eine Sicherheitsüberprüfung festgestellt wird, wird die restriktivere Aktion durchgesetzt.
- Eine Signaturregel kann mehrere Muster aufweisen und so konfiguriert werden, dass eine Verletzung nur dann markiert wird, wenn alle Muster übereinstimmen, wodurch Fehlalarme vermieden werden.
- Eine sorgfältige Auswahl eines wörtlichen Fast-Match-Musters für eine Regel kann die Verarbeitungszeit erheblich optimieren.

F: Funktioniert die Web App Firewall mit anderen NetScaler-Funktionen?

Die Web App Firewall ist vollständig in die NetScaler-Appliance integriert und arbeitet nahtlos mit anderen Funktionen zusammen. Sie können maximale Sicherheit für Ihre Anwendung konfigurieren, indem Sie andere NetScaler-Sicherheitsfunktionen in Verbindung mit der Web App Firewall verwenden. Beispielsweise kann **AAA-TM** verwendet werden, um den Benutzer zu authentifizieren, die Berechtigung des Benutzers für den Zugriff auf den Inhalt zu überprüfen und die Zugriffe zu protokollieren, einschließlich ungültiger Anmeldeversuche. **Rewrite** kann verwendet werden, um die URL zu ändern oder Header hinzuzufügen, zu ändern oder zu löschen, und **Responder** kann verwendet werden, um benutzerdefinierte Inhalte an verschiedene Benutzer zu liefern. Sie können die maximale Belastung für Ihre Website definieren, indem Sie die **Ratenbegrenzung** verwenden, um den Verkehr zu überwachen und die Rate zu drosseln, wenn er zu hoch ist. Der**HTTP-Denial-of-Service (DoS)** -Schutz kann dabei helfen, zwischen echten HTTP-Clients und böswilligen DoS-Clients zu unterscheiden. Sie können den Umfang der Sicherheitsüberprüfung einschränken, indem Sie die Web App Firewall-Richtlinien an virtuelle Server binden und gleichzeitig die Benutzererfahrung optimieren, indem Sie die **Load Balancing-Funktion** zur Verwaltung stark genutzter Anwendungen verwenden. Anfragen nach statischen Objekten wie Bildern oder Text können die Überprüfung der Sicherheitsüberprüfung Bypass und das **integrierte Caching** oder die **Komprimierung** nutzen, um die Bandbreitennutzung für solche Inhalte zu optimieren.

F: Wie wird die Nutzlast von der Web App Firewall und den anderen NetScaler Funktionen verarbeitet?

Ein Diagramm mit Details des L7-Paketflusses in einer NetScaler-Appliance ist im Abschnitt Verarbeitungsreihenfolge der Features verfügbar.

F: Was ist der empfohlene Workflow für die Bereitstellung der Web App Firewall?

Nachdem Sie nun die Vorteile der Verwendung des hochmodernen Sicherheitsschutzes der NetScaler Web App Firewall kennen, möchten Sie möglicherweise zusätzliche Informationen sammeln, die Ihnen bei der Entwicklung der optimalen Lösung für Ihre Sicherheitsanforderungen helfen können. Citrix empfiehlt Folgendes:

- **Kennen Sie Ihre Umgebung:** Wenn Sie Ihre Umgebung kennen, können Sie die beste Sicherheitsschutzlösung (Signaturen, Sicherheitsüberprüfungen oder beides) für Ihre Anforderungen ermitteln. Bevor Sie mit der Konfiguration beginnen, müssen Sie die folgenden Informationen sammeln.
  - **Betriebssystem:** Welches Betriebssystem (MS Windows, Linux, BSD, Unix, andere) haben Sie?
  - **Webserver:** Welchen Webserver (IIS, Apache oder NetScaler Enterprise Server) laufen Sie?
  - **Anwendung:** Welche Art von Anwendungen laufen auf Ihrem Anwendungsserver (z. B. ASP.NET, PHP, Cold Fusion, ActiveX, FrontPage, Struts, CGI, Apache Tomcat, Domino und WebLogic)?
  - Haben Sie maßgeschneiderte Anwendungen oder Standardanwendungen (z. B. Oracle, SAP)? Welche Version verwenden Sie?
  - **SSL:** Benötigen Sie SSL? Wenn ja, welche Schlüsselgröße (512, 1024, 2048, 4096) wird zum Signieren von Zertifikaten verwendet?
  - **Verkehrsvolumen:** Wie hoch ist die durchschnittliche Traffic-Rate durch Ihre Anwendungen? Haben Sie saisonale oder zeitspezifische Spitzen im Verkehr?
  - **Serverfarm:** Wie viele Server haben Sie? Müssen Sie Load Balancing verwenden?
  - **Datenbank:** Welche Art von Datenbank (MS-SQL, MySQL, Oracle, Postgres, SQLite, nosql, Sybase, Informix usw.) verwenden Sie?
  - **DB-Konnektivität:** Welche Art von Datenbankkonnektivität haben Sie (DSN, Verbindungszeichenfolge pro Datei, Verbindungszeichenfolge für eine einzelne Datei) und welche Treiber werden verwendet?
- **Identifizieren Sie Ihre Sicherheitsanforderungen:** Möglicherweise möchten Sie bewerten, welche Anwendungen oder spezifischen Daten maximalen Sicherheitsschutz benötigen, welche weniger anfällig sind und für welche die Sicherheitsinspektion sicher umgangen werden kann. Dies hilft Ihnen bei der Erstellung einer optimalen Konfiguration und beim Entwerfen geeigneter Richtlinien und Bindungspunkte zur Segregierung des Datenverkehrs. Beispielsweise möchten Sie möglicherweise eine Richtlinie konfigurieren, um die Sicherheit-

süberprüfung von Anforderungen für statische Webinhalte wie Bilder, MP3-Dateien und Filme zu Bypass, und eine andere Richtlinie so konfigurieren, dass erweiterte Sicherheitsüberprüfungen auf Anforderungen nach dynamischen Inhalten angewendet werden. Sie können mehrere Richtlinien und Profile verwenden, um verschiedene Inhalte derselben Anwendung zu schützen.

- **Lizenzanforderung:** NetScaler bietet eine einheitliche Lösung zur Optimierung der Leistung Ihrer Anwendung, indem es zahlreiche Funktionen wie Load Balancing, Content Switching, Caching, Komprimierung, Responder, Rewrite und Inhaltsfilterung nutzt, um nur einige zu nennen. Wenn Sie die gewünschten Funktionen identifizieren, können Sie entscheiden, welche Lizenz Sie benötigen.
- **Installieren und Baseline einer NetScaler-Appliance:** Erstellen Sie einen virtuellen Server und führen Sie Testverkehr durch diesen aus, um sich ein Bild von der Geschwindigkeit und Menge des Datenverkehrs zu machen, der durch Ihr System fließt. Diese Informationen helfen Ihnen, Ihren Kapazitätsbedarf zu identifizieren und die richtige Appliance (VPX, MPX oder SDX) auszuwählen.
- **Bereitstellen der Web App Firewall:** Verwenden Sie den Web App Firewall-Assistenten, um mit einer einfachen Sicherheitskonfiguration fortzufahren. Der Assistent führt Sie durch mehrere Bildschirme und fordert Sie auf, ein Profil, eine Richtlinie, eine Signatur und Sicherheitsüberprüfungen hinzuzufügen.
  - **Profil:** Wählen Sie einen aussagekräftigen Namen und den entsprechenden Typ (HTML, XML oder WEB 2.0) für Ihr Profil. Die Richtlinie und Signaturen werden automatisch unter demselben Namen generiert.
  - **Richtlinie:** Die automatisch generierte Richtlinie hat den Standardausdruck (true), der den gesamten Datenverkehr auswählt und global gebunden ist. Dies ist ein guter Ausgangspunkt, es sei denn, Sie denken an eine bestimmte Richtlinie, die Sie verwenden möchten.
  - **Schutz:** Der Assistent hilft Ihnen dabei, das hybride Sicherheitsmodell zu nutzen, in dem Sie die Standardsignaturen verwenden können, die eine Vielzahl von Regeln zum Schutz verschiedener Arten von Anwendungen bieten. Im**einfachen** Bearbeitungsmodus können Sie die verschiedenen Kategorien (CGI, Cold Fusion, PHP usw.) anzeigen. Sie können eine oder mehrere Kategorien auswählen, um ein bestimmtes Regelwerk zu identifizieren, das für Ihre Anwendung gilt. Verwenden Sie die Option **Aktion**, um alle Signaturregeln in den ausgewählten Kategorien zu aktivieren. Stellen Sie sicher, dass das Blockieren deaktiviert ist, damit Sie den Verkehr überwachen können, bevor Sie die Sicherheit erhöhen. Klicken Sie auf **Weiter**. Im Bereich **Tiefenschutz angeben** können Sie nach Bedarf Änderungen vornehmen, um die Schutzmaßnahmen für die Sicherheitsüberprüfung bereitzustellen. In den meisten Fällen reichen grundlegende Schutzmaßnahmen für die anfängliche Sicherheitskonfiguration aus. Lassen Sie den Verkehr eine Weile laufen, um eine repräsentative Stichprobe der Sicherheitsinspektionsdaten zu sammeln.

- **Verschärfung der Sicherheit:** Nachdem Sie die Web App Firewall bereitgestellt und den Datenverkehr eine Weile beobachtet haben, können Sie die Sicherheit Ihrer Anwendungen erhöhen, indem Sie Entspannungen bereitstellen und dann das Blockieren aktivieren. **Learning**, **Visualizer**und **Click to Deploy-Regeln** sind nützliche Funktionen, mit denen Sie Ihre Konfiguration sehr einfach anpassen können, um genau das richtige Maß an Entspannung zu erzielen. An dieser Stelle können Sie auch den Richtlinienausdruck ändern und/oder zusätzliche Richtlinien und Profile konfigurieren, um die gewünschten Sicherheitsstufen für verschiedene Arten von Inhalten zu implementieren.
- **Debuggen:** Wenn Sie ein unerwartetes Verhalten Ihrer Anwendung feststellen, bietet die Web App Firewall verschiedene Optionen zum einfachen Debuggen:
  * **Protokoll**. Wenn legitime Anfragen blockiert werden, müssen Sie zunächst die Datei ns.log überprüfen, um festzustellen, ob eine unerwartete Verletzung der Sicherheitsüberprüfung ausgelöst wird.
  * **Deaktivieren Sie die Funktion.** Wenn Sie keine Verstöße feststellen, aber immer noch unerwartetes Verhalten feststellen, z. B. eine Anwendung, die teilweise Antworten zurücksetzt oder sendet, können Sie die Web App Firewall-Funktion für das Debuggen deaktivieren. Wenn das Problem weiterhin besteht, schließt es die Web App Firewall als Verdächtigen aus.
  * **Verfolgen Sie Datensätze mit Protokollnachrichten.** Wenn das Problem anscheinend mit der Web App Firewall zusammenhängt und genauer betrachtet werden muss, haben Sie die Möglichkeit, Nachrichten über Sicherheitsverletzungen in eine Nstrace aufzunehmen. Sie können Follow TCP-Stream im Trace verwenden, um die Details der einzelnen Transaktion, einschließlich Header, Payload und die entsprechende Log-Nachricht, zusammen auf demselben Bildschirm anzuzeigen. Einzelheiten zur Verwendung dieser Funktionalität finden Sie in den Anhängen.

Einführung in die NetScaler Web App Firewall

September 11, 2023

Die NetScaler Web App Firewall verhindert Sicherheitsverletzungen, Datenverlust und mögliche unbefugte Änderungen an Websites, die auf vertrauliche Geschäfts- oder Kundeninformationen zugreifen. Dazu filtert es sowohl Anfragen als auch Antworten, untersucht sie auf Hinweise auf böswillige Aktivitäten und blockiert Anfragen, die solche Aktivitäten aufweisen. Ihre Website ist nicht nur vor gängigen Angriffsarten geschützt, sondern auch vor neuen, noch unbekannten Angriffen. Die Web App Firewall schützt nicht nur Webserver und Websites vor unbefugtem Zugriff, sondern schützt auch vor Sicherheitslücken in veraltetem CGI-Code oder -Skripts, Web-Frameworks, Webserver-Software und anderen zugrunde liegenden Betriebssystemen.

Die NetScaler Web App Firewall ist als eigenständige Appliance oder als Funktion auf einer virtuellen NetScaler-Appliance (VPX) verfügbar. In der Web App Firewall-Dokumentation bezieht sich der Begriff NetScaler auf die Plattform, auf der die Web App Firewall ausgeführt wird, unabhängig davon, ob es sich bei dieser Plattform um eine dedizierte Firewall-Appliance, einen NetScaler, auf dem auch andere Funktionen konfiguriert wurden, oder um einen NetScaler VPX handelt.

Um die Web App Firewall verwenden zu können, müssen Sie mindestens eine Sicherheitskonfiguration erstellen, um Verbindungen zu blockieren, die gegen die Regeln verstoßen, die Sie für Ihre geschützten Websites festgelegt haben. Die Anzahl der Sicherheitskonfigurationen, die Sie möglicherweise erstellen möchten, hängt von der Komplexität Ihrer Website ab. Manchmal reicht eine einzige Konfiguration aus. In anderen Fällen, insbesondere bei interaktiven Websites, Websites, die auf Datenbankserver zugreifen, Onlineshops mit Einkaufswagen, benötigen Sie möglicherweise verschiedene Konfigurationen, um sensible Daten bestmöglich zu schützen, ohne viel Aufwand für Inhalte zu verschwenden, die nicht anfällig für bestimmte Arten von Angriffen sind. Sie können die Standardeinstellungen für die globalen Einstellungen, die sich auf alle Sicherheitskonfigurationen auswirken, häufig unverändert lassen. Sie können die globalen Einstellungen jedoch ändern, wenn sie mit anderen Teilen Ihrer Konfiguration in Konflikt stehen oder Sie es vorziehen, sie anzupassen.

Sicherheit von Webanwendungen

Webanwendungssicherheit ist Netzwerksicherheit für Computer und Programme, die über die Protokolle HTTP und HTTPS kommunizieren. Dies ist ein breiter Bereich, in dem es viele Sicherheitslücken und -schwächen gibt. Betriebssysteme auf Servern und Clients weisen Sicherheitsprobleme auf und sind anfällig für Angriffe. Webserver-Software und Technologien, die Websites ermöglichen, wie CGI, Java, JavaScript, PERL und PHP, weisen grundlegende Sicherheitslücken auf. Browser und andere Client-Anwendungen, die mit webfähigen Anwendungen kommunizieren, weisen ebenfalls Sicherheitslücken auf. Websites, die jede Technologie außer der einfachsten HTML-Technologie verwenden, einschließlich Websites, die die Interaktion mit Besuchern ermöglichen, weisen häufig eigene Sicherheitslücken auf.

In der Vergangenheit war eine Sicherheitsverletzung oft nur ein Ärgernis, aber heute ist das selten der Fall. Beispielsweise waren Angriffe, bei denen sich ein Hacker Zugriff auf einen Webserver verschaffte und unbefugte Änderungen an einer Website vornahm (unkenntlich gemacht), früher weit verbreitet. Sie wurden in der Regel von Hackern ins Leben gerufen, die keine andere Motivation hatten, als anderen Hackern ihre Fähigkeiten zu demonstrieren oder die Zielperson oder das Unternehmen in Verlegenheit zu bringen. Die meisten aktuellen Sicherheitsverletzungen sind jedoch auf den Wunsch nach Geld zurückzuführen. Die meisten versuchen, eines oder beide der folgenden Ziele zu erreichen: sensible und potenziell wertvolle private Informationen zu erhalten oder unbefugten Zugriff auf und Kontrolle über eine Website oder einen Webserver zu erlangen.

Bestimmte Formen von Webangriffen konzentrieren sich darauf, an private Informationen zu gelangen. Diese Angriffe sind oft sogar gegen Websites möglich, die sicher genug sind, um zu ver-

hindern, dass ein Angreifer die volle Kontrolle übernimmt. Zu den Informationen, die ein Angreifer von einer Website abrufen kann, können Kundennamen, Adressen, Telefonnummern, Sozialversicherungsnummern, Kreditkartennummern, Krankenakten und andere private Informationen gehören. Der Angreifer kann diese Informationen dann verwenden oder an andere verkaufen. Ein Großteil der durch solche Angriffe erlangten Informationen ist gesetzlich geschützt, und alle sind durch Gewohnheiten und Erwartungen geschützt. Ein solcher Verstoß kann schwerwiegende Folgen für Kunden haben, deren private Daten gefährdet sind. Bestenfalls müssen diese Kunden wachsam sein, um zu verhindern, dass andere ihre Kreditkarten missbrauchen, unbefugte Kreditkonten in ihrem Namen eröffnen oder sich ihre Identität direkt aneignen (Identitätsdiebstahl). Im schlimmsten Fall könnten die Kunden mit ruinierten Kreditratings konfrontiert werden oder sogar für kriminelle Aktivitäten verantwortlich gemacht werden, an denen sie nicht beteiligt waren.

Andere Webangriffe zielen darauf ab, die Kontrolle über eine Website oder den Server, auf dem sie betrieben wird, zu erlangen (oder zu *kompromittieren*), oder beides. Ein Hacker, der die Kontrolle über eine Website oder einen Server erlangt, kann diese verwenden, um nicht autorisierte Inhalte zu hosten, als Proxy für Inhalte zu fungieren, die auf einem anderen Webserver gehostet werden, SMTP-Dienste für den Versand unerwünschter Massen-E-Mails bereitzustellen oder DNS-Dienste zur Unterstützung solcher Aktivitäten auf anderen gefährdeten Webservern bereitzustellen. Die meisten Websites, die auf kompromittierten Webservern gehostet werden, fördern fragwürdige oder schlichtweg betrügerische Unternehmen. Beispielsweise werden die meisten Phishing-Websites und Websites zur Ausbeutung von Kindern auf kompromittierten Webservern gehostet.

Der Schutz Ihrer Websites und Webdienste vor diesen Angriffen erfordert eine mehrschichtige Abwehr, die sowohl bekannte Angriffe mit identifizierbaren Merkmalen abwehren als auch vor unbekannten Angriffen schützen kann, die häufig erkannt werden können, weil sie anders aussehen als der normale Traffic auf Ihre Websites und Webdienste.

Bekannte Webangriffe

Die erste Verteidigungslinie für Ihre Websites ist der Schutz vor der großen Anzahl von Angriffen, von denen bekannt ist, dass sie existieren und von Websicherheitsexperten beobachtet und analysiert wurden. Zu den häufigsten Arten von Angriffen auf HTML-basierte Websites gehören:

- **Buffer-Overflow-Angriffe.** Das Senden einer langen URL, eines langen Cookie oder einer langen Information an einen Webserver führt dazu, dass das System hängen bleibt, abstürzt oder unbefugten Zugriff auf das zugrunde liegende Betriebssystem gewährt. Ein Angriff mit einem Pufferüberlauf kann verwendet werden, um Zugriff auf nicht autorisierte Informationen zu erhalten, einen Webserver zu kompromittieren oder beides.
- **Cookie-Sicherheitsangriffe.** Senden eines modifizierten Cookie an einen Webserver, normalerweise in der Hoffnung, mithilfe gefälschter Anmeldeinformationen Zugriff auf nicht autorisierte Inhalte zu erhalten.

- **Kräftiges Surfen.** Direkter Zugriff auf URLs auf einer Website, ohne zu den URLs mit Hyperlinks auf der Startseite oder anderen gängigen Start-URLs auf der Website zu navigieren. Einzelne Fälle von gewaltsamem Surfen können darauf hindeuten, dass ein Benutzer eine Seite auf Ihrer Website mit einem Lesezeichen versehen hat. Wiederholte Versuche, auf nicht existierende Inhalte zuzugreifen, oder auf Inhalte, auf die Benutzer niemals direkt zugreifen dürfen, stellen jedoch häufig einen Angriff auf die Sicherheit der Website dar. Forceful Browsing wird normalerweise verwendet, um Zugriff auf nicht autorisierte Informationen zu erhalten, kann aber auch mit einem Pufferüberlaufangriff kombiniert werden, um Ihren Server zu kompromittieren.
- **Sicherheitsangriffe auf Webformulare.** Senden unangemessener Inhalte in einem Webformular an Ihre Website. Zu unangemessenen Inhalten können modifizierte versteckte Felder, HTML oder Code in einem Feld gehören, das nur für alphanumerische Daten bestimmt ist, eine zu lange Zeichenfolge in einem Feld, das nur eine kurze Zeichenfolge akzeptiert, eine alphanumerische Zeichenfolge in einem Feld, das nur eine Ganzzahl akzeptiert, und eine Vielzahl anderer Daten, von denen Ihre Website nicht erwartet, dass sie in diesem Webformular empfangen werden. Ein Sicherheitsangriff auf ein Webformular kann entweder dazu verwendet werden, unautorisierte Informationen von Ihrer Website zu erhalten oder die Website direkt zu gefährden, normalerweise in Kombination mit einem Pufferüberlaufangriff.

Zwei spezielle Arten von Angriffen auf die Sicherheit von Webformularen verdienen besondere Erwähnung:

- **SQL-Injection-Angriffe.** Senden eines oder mehrerer aktiver SQL-Befehle in einem Webformular oder als Teil einer URL mit dem Ziel, dass eine SQL-Datenbank den Befehl oder die Befehle ausführt. SQL-Injection-Angriffe werden normalerweise verwendet, um nicht autorisierte Informationen zu erhalten.
- **Cross-Site-Scripting-Angriffe.** Die Verwendung einer URL oder eines Skripts auf einer Webseite verstößt gegen die Same-Origin-Richtlinie, die es Skripten untersagt, Eigenschaften von einer anderen Website abzurufen oder Inhalte auf einer anderen Website zu ändern. Da Skripte Informationen abrufen und Dateien auf Ihrer Website ändern können, kann der Zugriff eines Skripts auf Inhalte auf einer anderen Website einem Angreifer die Möglichkeit bieten, an unbefugte Informationen zu gelangen, einen Webserver zu kompromittieren oder beides zu gefährden.

Angriffe auf XML-basierte Webdienste lassen sich normalerweise in mindestens eine der beiden folgenden Kategorien einteilen: Versuche, unangemessene Inhalte an einen Webdienst zu senden, oder Versuche, die Sicherheit eines Webdienstes zu verletzen. Zu den häufigsten Arten von Angriffen auf XML-basierte Webdienste gehören:

- **Bösartiger Code oder Objekte.** XML-Anfragen, die Code oder Objekte enthalten, die entweder direkt vertrauliche Informationen abrufen oder einem Angreifer die Kontrolle über den Webdienst oder den zugrunde liegenden Server geben können.
- **Schlecht formatierte XML-Anfragen.** XML-Anfragen, die nicht der W3C-XML-Spezifikation

entsprechen und daher die Sicherheit eines unsicheren Webdienstes verletzen können

- **Denial-of-Service (DoS) -Angriffe.** XML-Anfragen, die wiederholt und in großen Mengen gesendet werden, um den Ziel-Webdienst zu überfordern und legitimen Benutzern den Zugriff auf den Webservice zu verweigern.

Neben standardmäßigen XML-basierten Angriffen sind XML-Webdienste und Web 2.0-Sites auch anfällig für SQL-Injection- und Cross-Site-Scripting-Angriffe, wie unten beschrieben:

- **SQL-Injection-Angriffe.** Senden eines oder mehrerer aktiver SQL-Befehle in einer XML-basierten Anfrage mit dem Ziel, dass eine SQL-Datenbank diesen Befehl oder diese Befehle ausführt. Wie bei HTML-SQL-Injection-Angriffen werden XML-SQL-Injection-Angriffe normalerweise verwendet, um nicht autorisierte Informationen zu erhalten.
- **Cross-Site-Scripting-Angriffe.** Die Verwendung eines Skripts, das in einer XML-basierten Anwendung enthalten ist, um gegen die Same-Origin-Richtlinie zu verstoßen, die es Skripten nicht erlaubt, Eigenschaften von einer anderen Anwendung abzurufen oder Inhalte in einer anderen Anwendung zu ändern. Da Skripts mithilfe Ihrer XML-Anwendung Informationen abrufen und Dateien ändern können, kann ein Angreifer, wenn Sie einem Skript Zugriff auf Inhalte gewähren, die zu einer anderen Anwendung gehören, die Möglichkeit bieten, an nicht autorisierte Informationen zu gelangen, die Anwendung zu kompromittieren oder beides.

Bekannte Webangriffe können in der Regel gestoppt werden, indem der Website-Verkehr nach bestimmten Merkmalen (Signaturen) gefiltert wird, die immer für einen bestimmten Angriff auftreten und niemals im legitimen Datenverkehr vorkommen dürfen. Dieser Ansatz hat den Vorteil, dass er relativ wenig Ressourcen erfordert und ein relativ geringes Risiko von Fehlalarmen birgt. Daher ist es ein wertvolles Tool zur Bekämpfung von Angriffen auf Websites und Webdienste und zur Konfiguration des grundlegenden Signaturschutzes.

Unbekannte Webangriffe

Die größte Bedrohung für Websites und Anwendungen geht nicht von bekannten Angriffen aus, sondern von unbekannten Angriffen. Die meisten unbekannten Angriffe lassen sich in eine von zwei Kategorien einteilen: neu gestartete Angriffe, gegen die Sicherheitsfirmen noch keine wirksame Abwehr entwickelt haben (Zero-Day-Attacken), und gezielte Angriffe auf eine bestimmte Website oder einen Webdienst und nicht auf viele Websites oder Webdienste (Spear-Angriffe). Diese Angriffe zielen, wie auch bekannte Angriffe, darauf ab, vertrauliche private Informationen zu erhalten, die Website oder den Webdienst zu kompromittieren und es zu ermöglichen, sie für weitere Angriffe oder beide Ziele zu verwenden.

Zero-Day-Angriffe stellen eine große Bedrohung für alle Benutzer dar. Bei diesen Angriffen handelt es sich in der Regel um dieselben Typen wie bekannte Angriffe. Zero-Day-Angriffe beinhalten häufig injiziertes SQL, ein Cross-Site-Script, eine Cross-Site-Request-Forgery oder eine andere Art von Angriff, die bekannten Angriffen ähnelt. In der Regel zielen sie auf Sicherheitslücken ab, von denen die

Entwickler der Zielsoftware, Website oder des Webdienstes entweder nichts wissen oder von denen sie erfahren haben. Sicherheitsfirmen haben daher keine Abwehrmaßnahmen gegen diese Angriffe entwickelt, und selbst wenn sie es getan haben, haben die Benutzer die Patches nicht erhalten und installiert oder die zum Schutz vor diesen Angriffen erforderlichen Abhilfemaßnahmen durchgeführt. Die Zeit zwischen der Entdeckung eines Zero-Day-Angriffs und der Verfügbarkeit einer Abwehr (das Sicherheitsfenster) wird immer kürzer, aber die Täter können immer noch mit Stunden oder sogar Tagen rechnen, in denen viele Websites und Webdienste keinen spezifischen Schutz vor dem Angriff haben.

Spear-Angriffe stellen eine große Bedrohung dar, richten sich jedoch nur an eine bestimmte Benutzergruppe. Eine übliche Art von Spear-Attacke, ein Spear-Phishing, richtet sich gegen Kunden einer bestimmten Bank oder eines Finanzinstituts oder (seltener) gegen Mitarbeiter eines bestimmten Unternehmens oder einer bestimmten Organisation. Im Gegensatz zu anderen Phishing-Methoden, bei denen es sich oft um grob geschriebene Fälschungen handelt, die ein Benutzer, der mit der tatsächlichen Kommunikation dieser Bank oder dieses Finanzinstituts vertraut ist, erkennen kann, sind Spear-Phishes buchstabengenau und überzeugend. Sie können spezifische Informationen enthalten, die für den Einzelnen spezifisch sind, die auf den ersten Blick kein Fremder wissen oder erhalten darf. Der Spear-Phisher ist somit in der Lage, die Zielperson davon zu überzeugen, die angeforderten Informationen bereitzustellen, die der Phisher dann verwenden kann, um Konten zu plündern, unrechtmäßig erlangtes Geld aus anderen Quellen zu verarbeiten oder sich Zugang zu anderen, noch sensibleren Informationen zu verschaffen.

Beide Angriffsarten weisen bestimmte Merkmale auf, die normalerweise erkannt werden können, allerdings nicht mithilfe statischer Muster, die nach bestimmten Merkmalen suchen, wie dies bei Standardsignaturen der Fall ist. Die Erkennung dieser Arten von Angriffen erfordert ausgefeiltere und ressourcenintensivere Ansätze, wie heuristische Filterung und positive Sicherheitsmodellsysteme. Heuristisches Filtern sucht nicht nach bestimmten Mustern, sondern nach Verhaltensmustern. Systeme mit positivem Sicherheitsmodell modellieren das normale Verhalten der Website oder des Webdienstes, den sie schützen, und blockieren dann Verbindungen, die nicht in dieses normale Nutzungsmodell passen. URL-basierte und webformularbasierte Sicherheitsprüfungen erfassen die normale Nutzung Ihrer Websites und kontrollieren dann, wie Benutzer mit Ihren Websites interagieren. Dabei werden sowohl heuristische als auch positive Sicherheitsvorkehrungen verwendet, um anomalen oder unerwarteten Traffic zu blockieren. Sowohl heuristische als auch positive Sicherheit können, wenn sie richtig konzipiert und eingesetzt werden, die meisten Angriffe abfangen, die Signaturen übersehen. Sie benötigen jedoch erheblich mehr Ressourcen als Signaturen, und Sie müssen einige Zeit damit verbringen, sie richtig zu konfigurieren, um Fehlalarme zu vermeiden. Sie werden daher nicht als primäre Verteidigungslinie verwendet, sondern als Backups von Signaturen oder anderen weniger ressourcenintensiven Ansätzen.

Indem Sie diese erweiterten Schutzmaßnahmen zusätzlich zu den Signaturen konfigurieren, erstellen Sie ein hybrides Sicherheitsmodell, mit dem die Web App Firewall umfassenden Schutz vor bekannten und unbekannten Angriffen bietet.

So funktioniert NetScaler Web App Firewall

Wenn Sie die Web App Firewall installieren, erstellen Sie eine anfängliche Sicherheitskonfiguration, die aus einer Richtlinie, einem Profil und einem Signaturobjekt besteht. Die Richtlinie ist eine Regel, die den zu filternden Verkehr identifiziert, und das Profil identifiziert die Muster und Verhaltenstypen, die zugelassen oder blockiert werden sollen, wenn der Verkehr gefiltert wird. Die einfachsten Muster, die als Signaturen bezeichnet werden, werden nicht innerhalb des Profils angegeben, sondern in einem Signaturobjekt, das dem Profil zugeordnet ist.

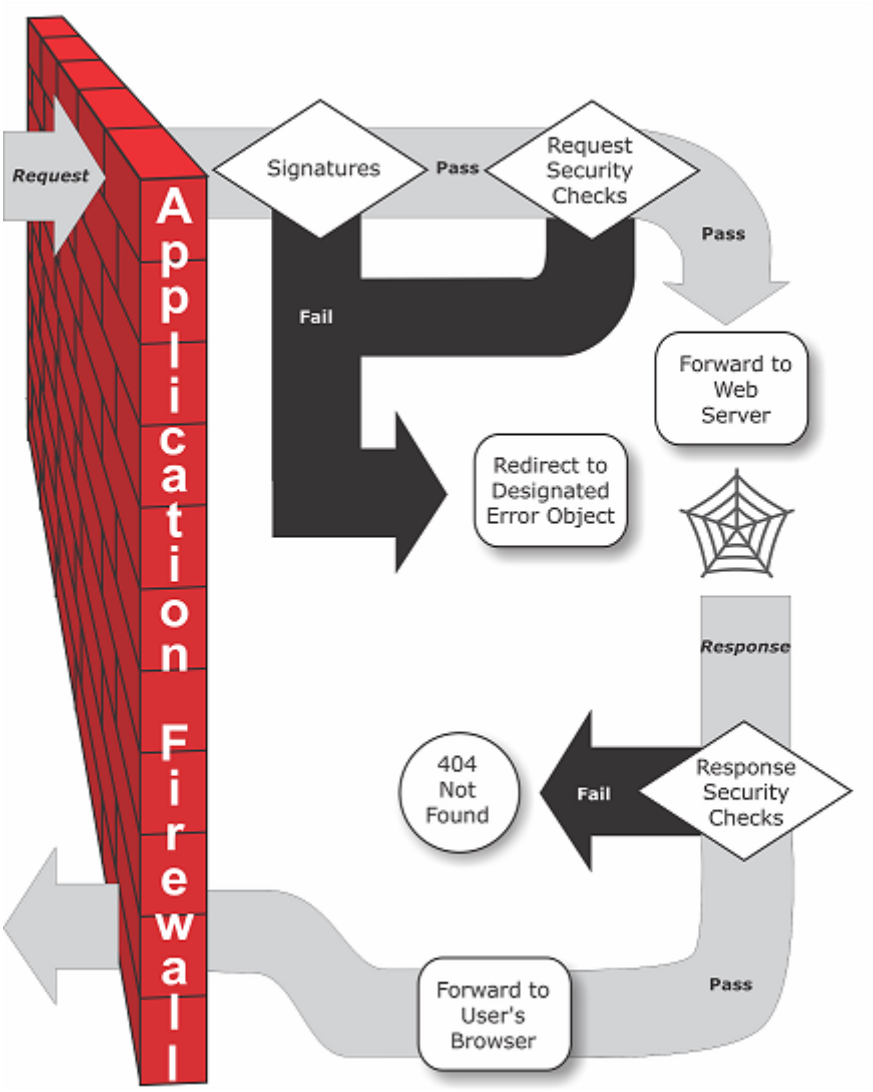
Eine Signatur ist eine Zeichenfolge oder ein Muster, das einer bekannten Art von Angriff entspricht. Die Web App Firewall enthält über tausend Signaturen in sieben Kategorien, die sich jeweils gegen Angriffe auf bestimmte Arten von Webservern und Webinhalten richten. NetScaler aktualisiert die Liste mit neuen Signaturen, sobald neue Bedrohungen erkannt werden. Während der Konfiguration geben Sie die Signaturkategorien an, die für die Webserver und Inhalte geeignet sind, die Sie schützen müssen. Signaturen bieten einen guten Basisschutz bei geringem Verarbeitungsaufwand. Wenn Ihre Anwendungen spezielle Sicherheitslücken aufweisen oder Sie einen Angriff gegen sie entdecken, für den keine Signatur existiert, können Sie Ihre eigenen Signaturen hinzufügen.

Die fortschrittlicheren Schutzmaßnahmen werden als Sicherheitschecks bezeichnet. Eine Sicherheitsüberprüfung ist eine strengere, algorithmische Prüfung einer Anfrage auf bestimmte Muster oder Verhaltensarten, die auf einen Angriff hinweisen oder eine Bedrohung für Ihre geschützten Websites und Webdienste darstellen könnten. Es kann beispielsweise eine Anfrage identifizieren, mit der versucht wird, eine bestimmte Art von Operation auszuführen, die möglicherweise die Sicherheit verletzt, oder eine Antwort, die vertrauliche private Informationen wie eine Sozialversicherungsnummer oder Kreditkartennummer enthält. Während der Konfiguration geben Sie die Sicherheitsüberprüfungen an, die für die Webserver und Inhalte, die Sie schützen müssen, geeignet sind. Die Sicherheitsüberprüfungen sind restriktiv. Viele von ihnen können legitime Anfragen und Antworten blockieren, wenn Sie bei der Konfiguration nicht die entsprechenden Ausnahmen (Lockerungen) hinzufügen. Es ist nicht schwierig, die benötigten Ausnahmen zu identifizieren, wenn Sie die adaptive Lernfunktion verwenden, die die normale Nutzung Ihrer Website beobachtet und empfohlene Ausnahmen erstellt.

Die Web App Firewall kann entweder als Layer-3-Netzwerkgerät oder als Layer-2-Netzwerkbrücke zwischen Ihren Servern und Ihren Benutzern installiert werden, normalerweise hinter dem Router oder der Firewall Ihres Unternehmens. Es muss an einem Ort installiert werden, an dem es den Datenverkehr zwischen den Webservern, die Sie schützen möchten, und dem Hub oder Switch, über den Benutzer auf diese Webserver zugreifen, abfangen kann. Anschließend konfigurieren Sie das Netzwerk so, dass Anfragen an die Web App Firewall statt direkt an Ihre Webserver und Antworten an die Web App Firewall statt direkt an Ihre Benutzer gesendet werden. Die Web App Firewall filtert diesen Datenverkehr, bevor sie ihn an sein endgültiges Ziel weiterleitet, und verwendet dabei sowohl ihren internen Regelsatz als auch Ihre Ergänzungen und Änderungen. Es blockiert oder macht alle Aktivitäten unschädlich, die es als schädlich erkennt, und leitet dann den verbleibenden Verkehr an den Webserver weiter. Die folgende Abbildung gibt einen Überblick über den Filtervorgang.

> **Hinweis:**
>
> In der Abbildung wird die Anwendung einer Richtlinie auf eingehenden Verkehr nicht berücksichtigt. Es veranschaulicht eine Sicherheitskonfiguration, bei der die Richtlinie darin besteht, alle Anfragen zu verarbeiten. Außerdem wurde in dieser Konfiguration ein Signaturobjekt konfiguriert und dem Profil zugeordnet, und Sicherheitsüberprüfungen wurden im Profil konfiguriert.

Abbildung 1. Ein Flussdiagramm der Web App Firewall Filterung



Wie die Abbildung zeigt, untersucht die Web App Firewall die Anfrage zunächst, um sicherzustellen, dass sie nicht mit einer Signatur übereinstimmt, wenn ein Benutzer eine URL auf einer geschützten Website anfordert. Wenn die Anfrage mit einer Signatur übereinstimmt, zeigt die NetScaler Web App Firewall entweder das Fehlerobjekt an (eine Webseite, die sich auf der Web App Firewall-Appliance befindet und die Sie mithilfe der Importfunktion konfigurieren können) oder leitet die Anfrage an die angegebene Fehler-URL (die Fehlerseite) weiter. Signaturen benötigen nicht so viele Ressourcen

wie Sicherheitsüberprüfungen. Das Erkennen und Stoppen von Angriffen, die anhand einer Signatur erkannt werden, bevor eine der Sicherheitsüberprüfungen ausgeführt wird, reduziert also die Serverlast.

Wenn eine Anfrage die Signaturprüfung besteht, wendet die Web App Firewall die aktivierten Sicherheitsüberprüfungen für Anfragen an. Die Sicherheitsüberprüfungen der Anfrage stellen sicher, dass die Anfrage für Ihre Website oder Ihren Webservice geeignet ist und kein Material enthält, das eine Bedrohung darstellen könnte. Bei Sicherheitsüberprüfungen wird die Anforderung beispielsweise auf Anzeichen untersucht, die darauf hinweisen, dass sie möglicherweise von einem unerwarteten Typ ist, unerwarteten Inhalt anfordert oder unerwartete und möglicherweise schädliche Webformulardaten, SQL-Befehle oder Skripts enthält. Wenn die Anfrage eine Sicherheitsprüfung nicht besteht, bereinigt die Web App Firewall die Anfrage entweder und sendet sie dann zurück an die NetScaler Appliance (oder die virtuelle NetScaler Appliance) oder zeigt das Fehlerobjekt an. Wenn die Anforderung die Sicherheitsprüfungen besteht, wird sie an die NetScaler Appliance zurückgesendet, die alle anderen Verarbeitungsvorgänge abschließt und die Anfrage an den geschützten Webserver weiterleitet.

Wenn die Website oder der Webdienst eine Antwort an den Benutzer sendet, wendet die Web App Firewall die aktivierten Antwortsicherheitsprüfungen an. Bei den Sicherheitschecks wird die Antwort auf undichte vertrauliche Informationen, Anzeichen einer Verunstaltung der Website oder andere Inhalte untersucht, die nicht vorhanden sein dürfen. Wenn die Antwort eine Sicherheitsüberprüfung nicht besteht, entfernt die Web App Firewall entweder den Inhalt, der nicht vorhanden sein darf, oder blockiert die Antwort. Wenn die Antwort die Sicherheitsprüfungen besteht, wird sie an die NetScaler Appliance zurückgesendet, die sie an den Benutzer weiterleitet.

Funktionen der NetScaler Web App Firewall

Die grundlegenden Funktionen der Web App Firewall sind Richtlinien, Profile und Signaturen, die ein hybrides Sicherheitsmodell bereitstellen, wie unter Bekannte Webangriffe, Unbekannte Webangriffeund Funktionsweise der Web App Firewallbeschrieben. Besonders hervorzuheben ist die Lernfunktion, die den Datenverkehr zu Ihren geschützten Anwendungen beobachtet und geeignete Konfigurationseinstellungen für bestimmte Sicherheitsüberprüfungen empfiehlt.

Die Importfunktion verwaltet Dateien, die Sie auf die Web App Firewall hochladen. Diese Dateien werden dann von der Web App Firewall bei verschiedenen Sicherheitsprüfungen oder bei der Reaktion auf eine Verbindung verwendet, die einer Sicherheitsüberprüfung entspricht.

Sie können die Funktionen für Protokolle, Statistiken und Berichte verwenden, um die Leistung der Web App Firewall zu bewerten und mögliche Schutzbedürfnisse zu ermitteln.

Wie NetScaler Web App Firewall den Anwendungsdatenverkehr ändert

Die NetScaler Web App Firewall beeinflusst das Verhalten einer Webanwendung, die sie schützt, indem sie Folgendes ändert:

- Cookies
- HTTP-Header
- Formulare/Daten

NetScaler Web App Firewall-Sitzungscookie

Um den Status der Sitzung aufrechtzuerhalten, generiert NetScaler Web App Firewall ein eigenes Sitzungscookie. Dieses Cookie wird nur zwischen dem Webbrowser und der NetScaler Web Application Firewall und nicht an den Webserver weitergegeben. Wenn ein Hacker versucht, das Sitzungscookie zu ändern, löscht die Web App Firewall das Cookie, bevor die Anfrage an den Server weitergeleitet wird, und behandelt die Anfrage als neue Benutzersitzung. Das Sitzungscookie ist vorhanden, solange der Webbrowser geöffnet ist. Wenn der Webbrowser geschlossen wird, wird das Application Firewall-Sitzungscookie ungültig. Der Status der Sitzung enthält die Informationen der vom Client besuchten URLs und Formulare.

Das konfigurierbare Web App Firewall -Sitzungscookie lautet `citrix_ns_id`.

Ab NetScaler Build 12.1, 54 und 13.0 ist die Cookie-Konsistenz sitzungslos, und das Hinzufügen des von der Appliance `citrix_ns_id` generierten Sitzungscookies wird nicht erzwungen. Weitere Informationen zur Konfiguration von Cookies finden Sie unter Engine-Einstellungen.

NetScaler Web App Firewall-Cookies

Viele Webanwendungen generieren Cookies, um benutzer- oder sitzungsspezifische Informationen zu verfolgen. Bei diesen Informationen kann es sich um Benutzerpräferenzen oder Einkaufswagenartikel handeln. Ein Webanwendungs-Cookie kann einer der folgenden zwei Typen sein:

- **Persistente Cookies** — Diese Cookies werden lokal auf dem Computer gespeichert und beim nächsten Besuch der Website erneut verwendet. Diese Art von Cookie enthält in der Regel Informationen über den Benutzer, wie Anmeldung, Kennwort oder Einstellungen.
- **Sitzungscookies oder transiente Cookies** — Diese Cookies werden nur während der Sitzung verwendet und nach Beendigung der Sitzung zerstört. Diese Art von Cookie enthält Informationen zum Anwendungsstatus, z. B. Artikel im Einkaufswagen oder Anmeldeinformationen für die Sitzung.

Hacker können versuchen, Anwendungscookies zu modifizieren oder zu stehlen, um eine Benutzersitzung zu kapern oder sich als Benutzer auszugeben. Die Anwendungsfirewall verhindert solche Versuche, indem sie die Anwendungs-Cookies hasht und dann weitere Cookies mit den digitalen Signaturen hinzufügt. Durch die Nachverfolgung der Cookies stellt die Application Firewall sicher, dass die Cookies zwischen dem Client-Browser und der Application Firewall nicht verändert oder kompromittiert werden. Die Anwendungsfirewall ändert die Anwendungs-Cookies nicht.

Die NetScaler Web App Firewall generiert die folgenden Standard-Cookies, um die Anwendungs-Cookies zu verfolgen:

- **Dauerhafte Cookies**: `citrix_ns_id_wlf`. Hinweis: wlf steht für wird ewig leben.
- **Sitzungs- oder Transiente Cookies**: `citrix_ns_id_wat`. Hinweis: wat steht für wird vorübergehend handeln.
  Um die Anwendungscookies zu verfolgen, gruppiert die Application Firewall die permanenten oder Sitzungsanwendungscookies zusammen und hasht und signiert dann alle Cookies zusammen. Daher generiert die Application Firewall ein `wlf`-Cookie, um alle dauerhaften Anwendungscookies zu verfolgen, und ein `wat`-Cookie, um alle Anwendungssitzungscookies zu verfolgen.

Die folgende Tabelle zeigt die Anzahl und die Arten von Cookies, die von der Application Firewall auf der Grundlage der von der Webanwendung generierten Cookies generiert werden:

Vor der NetScaler Web App Firewall	Ziel
Ein persistenter Cookie	Persistentes Cookie: `citix_ns_id_wlf`
Ein vorübergehendes Cookie	Vorübergehendes Cookie: `citix_ns_id_wat`
Mehrere persistente Cookies, mehrere transiente Cookies	Ein persistentes Cookie: `citrix_ns_id_wlf`, Ein transientes Cookie: `citix_ns_id_wat`

NetScaler Web App Firewall ermöglicht die Verschlüsselung des Anwendungs-Cookies. Die Application Firewall bietet auch die Möglichkeit, das von der Anwendung gesendete Sitzungscookie als Proxy zu verwenden, indem es zusammen mit den restlichen Sitzungsdaten der Application Firewall gespeichert und nicht an den Client gesendet wird. Wenn ein Client eine Anfrage an die Anwendung sendet, die ein Application Firewall-Sitzungscookie enthält, fügt Application Firewall das von der Anwendung gesendete Cookie wieder in die Anfrage ein, bevor die Anfrage an die ursprüngliche Anwendung weitergeleitet wird. Die Anwendungsfirewall ermöglicht auch das Hinzufügen der Flags HttpOnly und/oder Secure zu Cookies.

Wie sich die Anwendungsfirewall auf HTTP-Header auswirkt

Sowohl HTTPS-Anfragen als auch HTTPS-Antworten verwenden Header, um Informationen über eine oder mehrere HTTPS-Nachrichten zu senden. Eine Kopfzeile besteht aus einer Reihe von Zeilen, wobei jede Zeile einen Namen, gefolgt von einem Doppelpunkt und einem Leerzeichen sowie einem Wert enthält. Der Host-Header hat beispielsweise das folgende Format:

```
Host: www.citrix.com
```

Einige Header-Felder werden sowohl in Anfrage- als auch in Antwort-Headern verwendet, während andere nur für eine Anfrage oder eine Antwort geeignet sind. Die Anwendungsfirewall kann einige

Header in einer oder mehreren HTTPS-Anfragen oder -Antworten hinzufügen, ändern oder löschen, um die Sicherheit der Anwendung zu gewährleisten.

Von der NetScaler Web App Firewall verworfene Anforderungsheader

Viele der Anforderungsheader im Zusammenhang mit dem Caching werden gelöscht, um jede Anfrage im Kontext einer Sitzung anzuzeigen. Wenn die Anfrage einen Codierungs-Header enthält, damit der Webserver komprimierte Antworten senden kann, löscht die Application Firewall diesen Header, sodass der Inhalt der unkomprimierten Serverantwort von der Web App Firewall überprüft wird, um zu verhindern, dass sensible Daten an den Client gelangen.

Die Application Firewall löscht die folgenden Anforderungsheader:

- Bereich — Wird für die Wiederherstellung nach fehlgeschlagenen oder teilweisen Dateiübertragungen verwendet.
- If-Range — Ermöglicht einem Client, ein Teilobjekt abzurufen, wenn er einen Teil dieses Objekts bereits in seinem Cache enthält (bedingtes GET).
- If-Modified-Since — Wenn das angeforderte Objekt seit dem in diesem Feld angegebenen Zeitpunkt nicht geändert wurde, wird keine Entität vom Server zurückgegeben. Sie erhalten einen HTTP 304-Fehler, der nicht geändert wurde.
- If-None-Match — Ermöglicht effiziente Aktualisierungen zwischengespeicherter Informationen mit minimalem Overhead.
- Accept-Encoding — Welche Kodierungsmethoden sind für ein bestimmtes Objekt zulässig, z. B. gzip.

Von der NetScaler Web App Firewall geänderter Anforderungsheader

Wenn ein Webbrowser die Protokolle HTTP/1.0 oder früher verwendet, öffnet und schließt der Browser nach Erhalt jeder Antwort kontinuierlich die TCP-Socket-Verbindung. Dies erhöht den Overhead des Webservers und verhindert die Aufrechterhaltung des Sitzungsstatus. Das HTTP/1.1-Protokoll ermöglicht es, dass die Verbindung während der Sitzung geöffnet bleibt. Die Application Firewall ändert den folgenden Anforderungsheader, um HTTP/1.1 zwischen der Anwendungsfirewall und dem Webserver zu verwenden, unabhängig von dem vom Webbrowser verwendeten Protokoll:
Verbindung: keep-alive

Von der NetScaler Web App Firewall hinzugefügte Anforderungsheader

Die Application Firewall fungiert als Reverse-Proxy und ersetzt die ursprüngliche Quell-IP-Adresse der Sitzung durch die IP-Adresse der Application Firewall. Daher weisen alle im Webserver-Protokoll protokollierten Anfragen darauf hin, dass die Anfragen von der Application Firewall gesendet wurden.

Von der NetScaler Web App Firewall gelöschter Antwortheader

Die Anwendungsfirewall blockiert oder ändert möglicherweise Inhalte wie das Entfernen von Kreditkartennummern oder das Entfernen von Kommentaren, was zu einer Größenabweichung führen kann. Um ein solches Szenario zu verhindern, löscht die Application Firewall den folgenden Header:

Inhaltslänge — Gibt die Größe der an den Empfänger gesendeten Nachricht an.
Von der Application Firewall geänderte Antwortheader

Viele der von der Application Firewall modifizierten Antwortheader beziehen sich auf das Caching. Das Zwischenspeichern von Headern in HTTP (S) -Antworten muss geändert werden, um den Webbrowser zu zwingen, immer eine Anfrage an den Webserver für die neuesten Daten zu senden und nicht den lokalen Cache zu verwenden. Einige ASP-Anwendungen verwenden jedoch separate Plug-ins, um dynamische Inhalte anzuzeigen, und erfordern möglicherweise die Möglichkeit, die Daten vorübergehend im Browser zwischenzuspeichern. Um temporäres Zwischenspeichern von Daten zu ermöglichen, wenn Advanced Security-Schutzmaßnahmen wie FFC, URL-Schließung oder CSRF-Prüfungen aktiviert sind, fügt Application Firewall die Cache-Control-Header in der Serverantwort hinzu oder ändert sie mithilfe der folgenden Logik:

- Wenn Server Pragma: no-cache sendet, führt die Application Firewall keine Änderung durch.
- Wenn die Clientanfrage HTTP 1.0 ist, fügt die Application Firewall Pragma: no-cache ein.
- Wenn Client Request HTTP 1.1 ist und Cache-Control: no-store hat, nimmt die Application Firewall keine Änderungen vor.
- Wenn die Client-Anfrage HTTP 1.1 ist und die Serverantwort einen Cache-Control-Header ohne Store- oder Cache-Direktive hat, nimmt die Application Firewall keine Änderungen vor.
- Wenn die Client-Anfrage HTTP 1.1 ist und die Serverantwort entweder No Cache-Control Header hat oder der Cache-Control-Header keine Store- oder No-Cache-Direktive hat, führt die Application Firewall die folgenden Aufgaben aus:

1. Fügt Cache-Control ein: max-age=3, must revalidate, private.
2. Fügt X-Cache-Control-Orig = Originalwert des Cache-Control-Headers ein.
3. Löscht zuletzt geänderte Kopfzeile.
4. Ersetzt Etag.
5. Fügt X-Expires-Orig=Originalwert des vom Server gesendeten Expire-Headers ein.
6. Ändert den Expires-Header und setzt das Ablaufdatum der Webseite auf die Vergangenheit, sodass sie immer wieder abgerufen wird.
7. Ändert Accept-Ranges und setzt ihn auf None.

Um vorübergehend zwischengespeicherte Daten im Client-Browser zu ersetzen, wenn Application Firewall die Antwort ändert, z. B. für StripComments, X-out/Remove SafeObject, xout oder remove Credit Card oder URL Transform, ergreift Application Firewall die folgenden Aktionen:

1. Löscht die letzte Änderung vom Server, bevor sie an den Client weitergeleitet wird.

2. Ersetzt Etag durch einen Wert, der von Application Firewall bestimmt wird.

Von der NetScaler Web App Firewall hinzugefügte Antwortheader

- `Transfer-Encoding`: Aufgeschlüsselt. Dieser Header streamt Informationen zurück an einen Client, ohne dass Sie die Gesamtlänge der Antwort kennen müssen, bevor Sie die Antwort senden. Dieser Header ist erforderlich, da der Content-Length-Header entfernt wurde.
- `Set-Cookie`: Die von der Application Firewall hinzugefügten Cookies.
- `Xet-Cookie`: Wenn die Sitzung gültig ist und die Antwort im Cache nicht abgelaufen ist, können Sie aus dem Cache servieren und müssen kein neues Cookie senden, da die Sitzung noch gültig ist. In einem solchen Szenario wird das Set-Cookie in Xet-Cookie geändert. Für den Webbrowser.

Wie Formulardaten betroffen sind

Die Application Firewall schützt vor Angriffen, bei denen versucht wird, den Inhalt des vom Server gesendeten Originalformulars zu ändern. Es kann auch vor Cross-Site Request-Forgery-Angriffen schützen. Die Application Firewall erreicht dies, indem sie das versteckte Formular-Tag as_fid in die Seite einfügt.

Beispiel:`<input type="hidden"name="as_fid"value="VRgWq0I196Jmg/+LOY7C"/>`

Das versteckte Feld as_fid wird für die Feldkonsistenz verwendet. Dieses Feld wird von Application Firewall verwendet, um alle Felder des Formulars zu verfolgen, einschließlich der versteckten Feldname/Wertepaare, und um sicherzustellen, dass keines der vom Server gesendeten Felder des Formulars auf der Clientseite geändert wird. Die CSRF-Prüfung verwendet auch dieses eindeutige Formular-Tag as_fid, um sicherzustellen, dass die vom Benutzer übermittelten Formulare dem Benutzer in dieser Sitzung zugestellt wurden und kein Hacker versucht, die Benutzersitzung zu kapern.

Formularprüfung ohne Sitzung

Application Firewall bietet auch eine Option zum Schutz von Formulardaten mithilfe von sitzungsloser Feldkonsistenz. Dies ist nützlich für Anwendungen, bei denen die Formulare möglicherweise eine große Anzahl dynamischer versteckter Felder enthalten, die zu einer hohen Speicherzuweisung pro Sitzung durch die Anwendungsfirewall führen. Die Konsistenzprüfung von Feldern ohne Sitzung wird durchgeführt, indem ein weiteres ausgeblendetes Feld as_ffc_field nur für POST-Anfragen oder sowohl für GET- als auch für POST-Anfragen eingefügt wird, basierend auf der konfigurierten Einstellung. Die Application Firewall ändert die Methode GET in POST, wenn sie das Formular an den Client weiterleitet. Die Appliance setzt die Methode dann auf GET zurück, wenn sie an den Server zurückgesendet wird. Der Wert as_ffc_field kann groß sein, da er den verschlüsselten

Digest des Formulars enthält, das zugestellt wird. Das Folgende ist ein Beispiel für die sitzungslose Formularprüfung:

```
<input type="hidden" name="as_ffc_field" value="CwAAAAVIGLD/
    luRRi1Wu1rbYrFYargEDcO5xVAxsEnMP1megXuQfiDTGbwk0fpgndMHqfMbzfAFdjwR+
    TOm1oT
+u+Svo9+NuloPhtnbkxGtNe7gB/o8GlxEcK9ZkIIVv3oIL/
    nIPSRWJljgpWgafzVx7wtugNwnn8/
    GdnhneLCJTaYU7ScnC6LexJDLisI1xsEeONWt8Zm
+vJTa3mTebDY6LVyhDpDQfBgI1XLgfLTexAUzSNWHYyloqPruGYfnRPw+
    DIGf6gGwn1BYLEsRHKNbjJBrKpOJo9JzhEqdtZ1g3bMzEF9PocPvM1Hpvi5T6VB
/YFunUFM4f+bD7EAVcugdhovzb71CsSQX5+qcC1B8WjQ==" />
<!--NeedCopy-->
```

Entfernen von HTML-Kommentaren

Die Application Firewall bietet auch die Möglichkeit, alle HTML-Kommentare in den Antworten zu entfernen, bevor sie an den Client gesendet werden. Dies betrifft nicht nur Formulare, sondern alle Antwortseiten. Die Application Firewall sucht und entfernt jeden Text, der zwischen “<!-“ und “->” Kommentar-Tags. Die Tags weisen weiterhin darauf hin, dass an dieser Stelle des HTML-Quellcodes ein Kommentar vorhanden war. Jeder Text, der in andere HTML- oder JavaScript-Tags eingebettet ist, wird ignoriert.
Einige Anwendungen funktionieren möglicherweise nicht richtig, wenn JavaScript falsch in Kommentar-Tags eingebettet ist. Ein Vergleich des Seitenquellcodes vor und nach dem Entfernen der Kommentare durch die Application Firewall kann dabei helfen, festzustellen, ob in einem der gelöschten Kommentare das erforderliche JavaScript eingebettet war.

Schutz Ihrer Kreditkarte

Die Application Firewall bietet die Möglichkeit, die Header und den Text der Antwort zu überprüfen und die Kreditkartennummern entweder zu entfernen oder zu löschen, bevor die Antwort an den Client weitergeleitet wird. Derzeit bietet Application Firewall Schutz für die folgenden gängigen Kreditkarten: American Express, Diners Club, Discover, JCB, MasterCard und Visa. Die X-Out-Aktion funktioniert unabhängig von der Block-Aktion.

Sicherer Objektschutz

Ähnlich wie bei Kreditkartennummern kann auch der Verlust anderer sensibler Daten verhindert werden, indem die Sicherheitsüberprüfung Application Firewall Safe Object verwendet wird, um die vertraulichen Inhalte in der Antwort entweder zu entfernen oder zu löschen.

Siteübergreifendes Scripting transformiert Aktionen

Wenn die Transformation für Cross-Site Scripting aktiviert ist, ändert die Web App Firewall `"<"into "%26lt;"and ">"into "%26gt;"` in den Anforderungen. Wenn die Einstellung checkRequestHeaders in der Web App Firewall aktiviert ist, überprüft die Web App Firewall die Anforderungsheader und wandelt diese Zeichen auch in Header und Cookies um. Die Transformationsaktion blockiert oder transformiert keine Werte, die ursprünglich vom Server gesendet wurden. Es gibt eine Reihe von Standardattributen und -tags für Cross-Site Scripting, die die Web App Firewall zulässt. Eine Standardliste verweigerter Cross-Site-Scripting-Muster wird ebenfalls bereitgestellt. Diese können angepasst werden, indem Sie das Signaturobjekt auswählen und in der GUI auf den **Dialog SQL/Cross-Site-Scripting-Muster verwalten** klicken.

Transformieren von SQL-Sonderzeichen

Application Firewall hat die folgenden Standard-Transformationsregeln für SQL-Sonderzeichen:

Unter	Ziel	Verwandlung
‘(einfaches Anführungszeichen, d. h. %27)	”	Noch ein einziges Zitat
\ (Backslash, der %5C ist)	|Weiterer Backslash hinzugefügt	
; (Semikolon, das ist%3B)		Fallengelassen

Wenn die Transformation von Sonderzeichen aktiviert ist und CheckRequestHeaders auf ON gesetzt ist, erfolgt die Transformation von Sonderzeichen auch in Headern und Cookies.
Hinweis: Einige Anforderungsheader wie User-Agent, Accept-Encoding enthalten normalerweise Semikolons und können von der SQL-Transformation beeinflusst werden.

Verhalten der NetScaler Web App Firewall, bei dem der EXPECT-Header beschädigt wird

1. Immer wenn NetScaler eine HTTP-Anfrage mit dem EXPECT-Header empfängt, sendet NetScaler im Namen des Backend-Servers die EXPECT: 100 -continue-Antwort an den Client.
2. Dieses Verhalten ist darauf zurückzuführen, dass der Application Firewall-Schutz für die gesamte Anfrage ausgeführt werden muss, bevor die Anfrage an den Server weitergeleitet wird. NetScaler muss die gesamte Anfrage vom Client abrufen.
3. Nach Erhalt einer `100 continue`-Antwort sendet der Client den verbleibenden Teil der Anfrage, der die Anfrage vervollständigt.

4. NetScaler führt dann alle Schutzmaßnahmen aus und leitet die Anfrage dann an den Server weiter.
5. Jetzt, da NetScaler die komplette Anfrage weiterleitet, wird der EXPECT-Header, der in der ursprünglichen Anfrage kam, veraltet, sodass NetScaler diesen Header beschädigt und an den Server sendet.
6. Der Server ignoriert beim Empfang der Anfrage jeden beschädigten Header.

Konfigurieren der Web App Firewall

June 2, 2023

Sie können die NetScaler Web App Firewall (Web App Firewall) mithilfe einer der folgenden Methoden konfigurieren:

- **Web App Firewall-Assistent.** Ein Dialogfeld, das aus einer Reihe von Bildschirmen besteht, die Sie durch den Konfigurationsprozess führen.
- **AppExpert-Vorlage für das NetScaler-Webinterface.** Eine AppExpert-Vorlage (eine Reihe von Konfigurationseinstellungen), die entwickelt wurden, um Websites angemessen zu schützen. Diese AppExpert-Vorlage enthält die entsprechenden Web App Firewall-Konfigurationseinstellungen zum Schutz vieler Websites.
- **NetScaler-Benutzeroberfläche.** Die webbasierte Konfigurationsoberfläche.
- **NetScaler-Befehlszeilenschnittstelle.** Die Befehlszeilen-Konfigurationsschnittstelle.

Citrix empfiehlt, den Web App Firewall Wizard zu verwenden. Für die meisten Benutzer ist dies die einfachste Methode, die Web App Firewall zu konfigurieren, und sie wurde entwickelt, um Fehler zu vermeiden. Wenn Sie über einen neuen NetScaler oder VPX verfügen, den Sie hauptsächlich zum Schutz von Websites verwenden werden, ist die AppExpert-Vorlage für das Webinterface möglicherweise die bessere Option, da sie eine gute Standardkonfiguration bietet, nicht nur für die Web App Firewall, sondern für die gesamte Appliance. Sowohl die GUI als auch die Befehlszeilenschnittstelle sind für erfahrene Benutzer gedacht, in erster Linie um eine vorhandene Konfiguration zu ändern oder erweiterte Optionen zu verwenden.

Web App Firewall Wizard

Der Web App Firewall-Assistent ist ein Dialogfeld, das aus mehreren Bildschirmen besteht, in denen Sie aufgefordert werden, jeden Teil einer einfachen Konfiguration zu konfigurieren. Die Web App Firewall erstellt dann die entsprechenden Konfigurationselemente aus den Informationen, die Sie ihr geben. Dies ist die einfachste und für die meisten Zwecke die beste Methode, die Web App Firewall zu konfigurieren.

Um den Assistenten zu verwenden, stellen Sie mit dem Browser Ihrer Wahl eine Verbindung zur GUI her. Wenn die Verbindung hergestellt ist, überprüfen Sie, ob die Web App Firewall aktiviert ist, und führen Sie dann den Web App Firewall-Assistenten aus, der Sie zur Eingabe von Konfigurationsinformationen auffordert. Sie müssen nicht alle angeforderten Informationen angeben, wenn Sie den Assistenten zum ersten Mal verwenden. Stattdessen können Sie Standardeinstellungen akzeptieren, einige relativ einfache Konfigurationsaufgaben ausführen, um wichtige Funktionen zu aktivieren, und dann der Web App Firewall erlauben, wichtige Informationen zu sammeln, um Sie bei der Konfiguration zu unterstützen.

Wenn der Assistent Sie beispielsweise auffordert, eine Regel für die Auswahl des zu verarbeitenden Datenverkehrs anzugeben, können Sie die Standardeinstellung akzeptieren, bei der der gesamte Datenverkehr ausgewählt wird. Wenn Ihnen eine Liste von Signaturen angezeigt wird, können Sie die entsprechenden Signaturkategorien aktivieren und die Erfassung von Statistiken für diese Signaturen aktivieren. Bei dieser Erstkonfiguration können Sie die erweiterten Schutzfunktionen (Sicherheitsüberprüfungen) überspringen. Der Assistent erstellt automatisch die entsprechende Richtlinie, das Signaturobjekt und das entsprechende Profil (zusammen die Sicherheitskonfiguration) und bindet die Richtlinie an die globale Richtlinie. Die Web App Firewall beginnt dann, Verbindungen zu Ihren geschützten Websites zu filtern, alle Verbindungen zu protokollieren, die mit einer oder mehreren der von Ihnen aktivierten Signaturen übereinstimmen, und Statistiken über die Verbindungen zu sammeln, denen jede Signatur entspricht. Nachdem die Web App Firewall einen Teil des Datenverkehrs verarbeitet hat, können Sie den Assistenten erneut ausführen und die Protokolle und Statistiken überprüfen, um festzustellen, ob eine der von Ihnen aktivierten Signaturen dem legitimen Verkehr entspricht. Nachdem Sie ermittelt haben, welche Signaturen den Datenverkehr identifizieren, den Sie blockieren möchten, können Sie die Sperrung für diese Signaturen aktivieren. Wenn Ihre Website oder Ihr Webdienst nicht komplex ist, kein SQL verwendet und keinen Zugriff auf vertrauliche private Informationen hat, bietet diese grundlegende Sicherheitskonfiguration wahrscheinlich einen angemessenen Schutz.

Möglicherweise benötigen Sie zusätzlichen Schutz, wenn Ihre Website beispielsweise dynamisch ist. Inhalte, die Skripts verwenden, benötigen möglicherweise Schutz vor websiteübergreifenden Skriptangriffen. Webinhalte, die SQL verwenden — wie Einkaufswagen, viele Blogs und die meisten Content-Management-Systeme — müssen möglicherweise vor SQL-Injection-Angriffen geschützt werden. Websites und Webdienste, die vertrauliche private Informationen wie Sozialversicherungsnummern oder Kreditkartennummern sammeln, müssen möglicherweise vor einer unbeabsichtigten Offenlegung dieser Informationen geschützt werden. Bestimmte Arten von Webserver- oder XML-Server-Software müssen möglicherweise vor Angriffsarten geschützt werden, die auf diese Software zugeschnitten sind. Eine weitere Überlegung ist, dass bestimmte Elemente Ihrer Websites oder Webdienste möglicherweise einen anderen Schutz erfordern als andere Elemente. Anhand der Protokolle und Statistiken der Web App Firewall können Sie die zusätzlichen Schutzmaßnahmen ermitteln, die Sie möglicherweise benötigen.

Nachdem Sie entschieden haben, welche erweiterten Schutzfunktionen für Ihre Websites und Web-

dienste erforderlich sind, können Sie den Assistenten erneut ausführen, um diese Schutzmaßnahmen zu konfigurieren. Bei bestimmten Sicherheitskontrollen müssen Sie Ausnahmen (Lockerungen) eingeben, um zu verhindern, dass die Überprüfung legitimen Datenverkehr blockiert. Sie können dies manuell tun, aber in der Regel ist es einfacher, die Funktion für adaptives Lernen zu aktivieren und ihr die erforderliche Entspannung empfehlen zu lassen. Sie können den Assistenten so oft wie nötig verwenden, um Ihre grundlegende Sicherheitskonfiguration zu verbessern und/oder zusätzliche Sicherheitskonfigurationen zu erstellen.

Der Assistent automatisiert einige Aufgaben, die Sie manuell ausführen müssten, wenn Sie den Assistenten nicht verwenden würden. Es erstellt automatisch eine Richtlinie, ein Signaturobjekt und ein Profil und weist ihnen den Namen zu, den Sie angegeben haben, als Sie nach dem Namen Ihrer Konfiguration gefragt wurden. Der Assistent fügt dem Profil außerdem Ihre erweiterten Schutzeinstellungen hinzu, bindet das Signaturobjekt an das Profil, verknüpft das Profil mit der Richtlinie und setzt die Richtlinie in Kraft, indem er sie an Global bindet.

Einige Aufgaben können im Wizard nicht ausgeführt werden. Sie können den Assistenten nicht verwenden, um eine Richtlinie an einen anderen Bindpunkt als Global zu binden. Wenn Sie möchten, dass das Profil nur für einen bestimmten Teil Ihrer Konfiguration gilt, müssen Sie die Bindung manuell konfigurieren. Sie können die Engine-Einstellungen oder bestimmte andere globale Konfigurationsoptionen im Assistenten nicht konfigurieren. Sie können zwar eine der erweiterten Schutzeinstellungen im Assistenten konfigurieren, aber wenn Sie eine bestimmte Einstellung in einer einzigen Sicherheitsprüfung ändern möchten, ist es möglicherweise einfacher, dies auf den manuellen Konfigurationsbildschirmen in der GUI zu tun.

Weitere Informationen zur Verwendung des Web App Firewall-Assistenten finden Sie unter Der Web App Firewall-Assistent.

Die NetScaler Web Interface AppExpert Vorlage

AppExpert Templates sind ein anderer und einfacherer Ansatz zur Konfiguration und Verwaltung komplexer Unternehmensanwendungen. Die AppExpert-Anzeige in der GUI besteht aus einer Tabelle. Anwendungen werden in der Spalte ganz links aufgeführt, wobei die NetScaler-Funktionen, die für diese Anwendung gelten, jeweils in einer eigenen Spalte auf der rechten Seite angezeigt werden. (In der AppExpert-Oberfläche werden die Funktionen, die einer Anwendung zugeordnet sind, als *Anwendungseinheiten* bezeichnet.) In der AppExpert-Oberfläche konfigurieren Sie den interessanten Traffic für jede Anwendung und aktivieren Regeln für Komprimierung, Caching, Rewrite, Filterung, Responder und die Web App Firewall, anstatt jede Funktion einzeln konfigurieren zu müssen.

Web Interface AppExpert Template enthält Regeln für die folgenden Web App Firewall -Signaturen und Sicherheitsprüfungen:

- **URL-Prüfung verweigern.** Erkennt Verbindungen zu Inhalten, die bekanntermaßen ein Sicherheitsrisiko darstellen, oder zu anderen URLs, die Sie festlegen.

- **Pufferüberlauf-Prüfung.** Erkennt Versuche, einen Pufferüberlauf auf einem geschützten Webserver zu verursachen.
- **Überprüfung der Cookie-Konsistenz.** Erkennt bösartige Änderungen an Cookies, die von einer geschützten Website gesetzt werden.
- **Konsistenzprüfung für Formularfelder.** Erkennt Änderungen an der Struktur eines Webformulars auf einer geschützten Website.
- **Überprüfung der CSRF-Formularkennzeichnung.** Erkennt Angriffe zur siteübergreifenden Anforderungsfälschung.
- **Überprüfung der Feldformate.** Erkennt unangemessene Informationen, die in Webformularen auf einer geschützten Website hochgeladen wurden.
- **Überprüfung der HTML SQL-Einschleusung.** Erkennt Versuche, nicht autorisierten SQL-Code zu injizieren.
- **HTML-Site-übergreifende Skript-Überprüfung** Erkennt Cross-Site-Scripting-Angriffe.

Informationen zum Installieren und Verwenden einer AppExpert-Vorlage finden Sie unter AppExpert AppExpert AppApplications and Templates.

Die GUI

Die GUI ist eine webbasierte Oberfläche, die Zugriff auf alle Konfigurationsoptionen für die Web App Firewall-Funktion bietet, einschließlich erweiterter Konfigurations- und Verwaltungsoptionen, die in keinem anderen Konfigurationstool oder einer anderen Benutzeroberfläche verfügbar sind. Insbesondere können viele erweiterte Signaturoptionen nur in der GUI konfiguriert werden. Sie können die von der Lernfunktion generierten Empfehlungen nur in der GUI überprüfen. Sie können Richtlinien nur in der GUI an einen anderen Bindepunkt als Global binden.

Eine Beschreibung der GUI finden Sie unter Die Web App Firewall-Konfigurationsschnittstellen. Weitere Informationen zur Verwendung der GUI zum Konfigurieren der Web App Firewall finden Sie unter Manuelle Konfiguration mit der GUI.

Anweisungen zum Konfigurieren der Web App Firewall über die grafische Benutzeroberfläche finden Sie unter Manuelle Konfiguration mit der GUI. Informationen zur Citrix-ADC-GUI finden Sie unter Die Web App Firewall-Konfigurationsschnittstellen.

Die NetScaler Befehlszeilenschnittstelle

Die NetScaler-Befehlszeilenschnittstelle ist eine modifizierte UNIX-Shell, die auf der FreeBSD-Bash-Shell basiert. Um die Web App Firewall über die Befehlszeilenschnittstelle zu konfigurieren, geben Sie Befehle an der Eingabeaufforderung ein und drücken die Eingabetaste, genau wie bei jeder anderen Unix-Shell. Sie können die meisten Parameter und Optionen für die Web App Firewall mithilfe der NetScaler-Befehlszeile konfigurieren. Ausnahmen sind die Signaturfunktion, von denen viele Op-

tionen nur über die GUI oder den Web App Firewall Assistenten konfiguriert werden können, und die Lernfunktion, deren Empfehlungen nur in der GUI überprüft werden können.

Anweisungen zum Konfigurieren der Web App Firewall mithilfe der NetScaler-Befehlszeile finden Sie unter Manuelle Konfiguration mit der Befehlszeilenschnittstelle.

NetScaler Web App Firewall aktivieren

May 11, 2023

Bevor Sie eine Sicherheitskonfiguration erstellen können, müssen Sie die NetScaler Web App Firewall-Funktion auf der Appliance aktivieren.

Wichtige Punkte

- Wenn Sie eine dedizierte NetScaler Web App Firewall-Appliance konfigurieren oder eine vorhandene Appliance aktualisieren, ist die Funktion bereits aktiviert. Sie müssen keines der hier beschriebenen Verfahren ausführen.
- Wenn Sie einen neuen NetScaler oder VPX haben, müssen Sie die NetScaler Web App Firewall-Funktion aktivieren, bevor Sie sie konfigurieren.
- Wenn Sie einen NetScaler oder VPX von einer früheren Version aktualisieren, müssen Sie zuerst die NetScaler Web App Firewall-Funktion aktivieren, bevor Sie sie konfigurieren.

> **Hinweis:**
>
> Wenn Sie einen NetScaler oder VPX von einer früheren Version aktualisieren, müssen Sie möglicherweise die Lizenzen auf Ihrer Appliance aktualisieren, bevor Sie NetScaler Web App Firewall aktivieren. Erkundigen Sie sich bei Ihrem NetScaler-Vertreter oder Wiederverkäufer, um die richtige Lizenz zu erhalten.

Aktivieren der NetScaler Web App Firewall über die Befehlszeilenschnittstelle

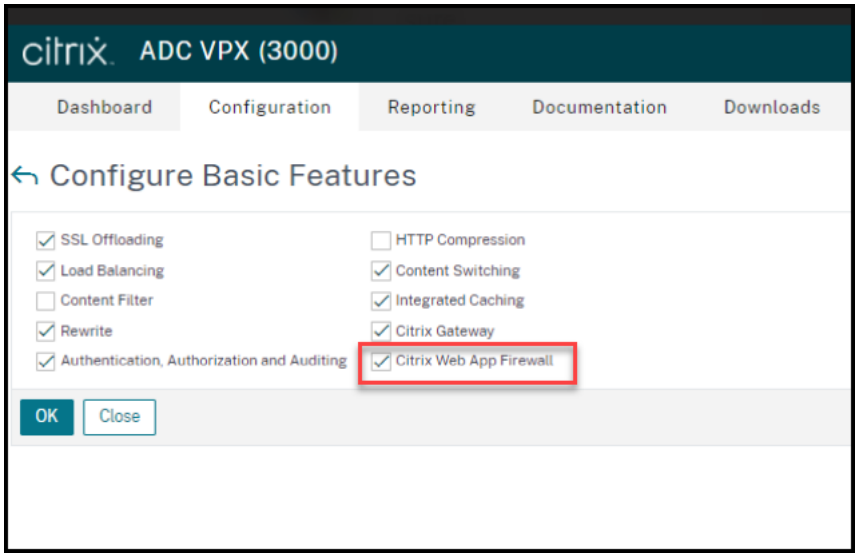
Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
enable ns feature AppFW
```

Aktivieren Sie die Web App Firewall mithilfe der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.

3. Wählen Sie auf der Seite „ **Erweiterte Funktionen konfigurieren** “ die Option **NetScaler Web App Firewall**aus.
4. Klicken Sie auf **OK**.



Der Web App Firewall-Assistent

May 11, 2023

Im Gegensatz zu den meisten Assistenten wurde der NetScaler Web App Firewall-Assistent nicht nur dazu entwickelt, den Erstkonfigurationsprozess zu vereinfachen, sondern auch zuvor erstellte Konfigurationen zu ändern und Ihr Web App Firewall-Setup beizubehalten. Ein typischer Benutzer führt den Assistenten mehrmals aus, wobei jedes Mal einige Bildschirme übersprungen werden.

Der Web App Firewall Wizard erstellt automatisch Profile, Richtlinien und Signaturen.

Den Wizard öffnen

Um den Web App Firewall Wizard auszuführen, öffnen Sie die GUI und gehen Sie wie folgt vor:

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Getting Started**auf **Application Firewall Wizard**. Der Assistent wird geöffnet.

Weitere Informationen zur GUI finden Sie unter Die Web App Firewall Configuration Interfaces.

Die Bildschirme des Assistenten

Der Web App Firewall-Assistent zeigt die folgenden Bildschirme auf einer tabellarischen Seite an:

1. Namen angeben: Geben Sie auf diesem Bildschirm beim Erstellen einer neuen Sicherheitskonfiguration einen aussagekräftigen Namen und den entsprechenden Typ (HTML, XML oder WEB 2.0) für Ihr Profil an. Die Standardrichtlinie und die Signaturen werden automatisch unter Verwendung desselben Namens generiert.

Name des Profils

Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrichsymbol beginnen und aus 1 bis 31 Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), At (@), Gleichheit (=), Doppelpunkt (:) und Unterstrich (_) bestehen. Wählen Sie einen Namen, anhand dessen andere leicht erkennen können, welche Inhalte Ihre neue Sicherheitskonfiguration schützt.

> **Hinweis:**
>
> Da der Assistent diesen Namen sowohl für die Richtlinie als auch für das Profil verwendet, ist er auf 31 Zeichen begrenzt. Manuell erstellte Richtlinien können Namen mit einer Länge von bis zu 127 Zeichen haben.

Wenn Sie eine vorhandene Konfiguration ändern, wählen Sie Bestehende Konfiguration ändern und wählen Sie dann in der Dropdownliste Name den Namen der vorhandenen Konfiguration aus, die Sie ändern möchten.

> **Hinweis:**
>
> In dieser Liste werden nur Richtlinien angezeigt, die an einen globalen oder an einen Bindungspunkt gebunden sind. Sie können eine ungebundene Richtlinie nicht mithilfe des Application Firewall-Assistenten ändern. Sie müssen es entweder manuell an Global oder einen Bindungspunkt binden oder es manuell ändern. (Zur manuellen Änderung in der GUI) **Application Firewall >**Richtlinien**>**Firewall-Bereich****, wählen Sie die Richtlinie aus und klicken Sie auf **Öffnen**.

Profiltyp

Auf diesem Bildschirm wählen Sie auch einen Profiltyp aus. Der Profiltyp bestimmt die Arten des erweiterten Schutzes (Sicherheitsprüfungen), die konfiguriert werden können. Da bestimmte Arten von Inhalten nicht für bestimmte Arten von Sicherheitsbedrohungen anfällig sind, spart die Einschränkung der Liste der verfügbaren Prüfungen Zeit bei der Konfiguration. Die Typen von Web App Firewall-Profilen sind:

- Webanwendung (HTML). Jede HTML-basierte Website, die keine XML- oder Web 2.0-Technologien verwendet.
- XML-Anwendung (XML, SOAP). Jeder XML-basierte Webdienst.
- Web 2.0-Anwendung (HTML, XML, REST). Jede Web 2.0-Site, die HTML- und XML-basierte Inhalte kombiniert, z. B. eine Atom-basierte Website, ein Blog, ein RSS-Feed oder ein Wiki.

Hinweis: Wenn Sie sich nicht sicher sind, welche Art von Inhalten auf Ihrer Website verwendet wird,

können Sie Web 2.0-Anwendung wählen, um sicherzustellen, dass Sie alle Arten von Webanwendungsinhalten schützen.

2. Regel angeben: Auf diesem Bildschirm geben Sie die Richtlinienregel (Ausdruck) an, die den Datenverkehr definiert, den die aktuelle Konfiguration untersucht. Wenn Sie eine Erstkonfiguration zum Schutz Ihrer Websites und Webdienste erstellen, können Sie den Standardwert **true**akzeptieren, der den gesamten Webverkehr auswählt.

Wenn Sie möchten, dass diese Sicherheitskonfiguration nicht den gesamten HTTP-Verkehr, der durch die Appliance geleitet wird, sondern bestimmten Datenverkehr untersucht, können Sie eine Richtlinienregel schreiben, die den Traffic angibt, den sie untersuchen soll. Die Regeln sind in der NetScaler Expressions Language geschrieben, einer voll funktionsfähigen objektorientierten Programmiersprache.

Hinweis: Zusätzlich zur Syntax der Standardausdrücke unterstützt das NetScaler-Betriebssystem aus Gründen der Abwärtskompatibilität die Syntax für klassische Ausdrücke von NetScaler auf NetScaler Classic- und NCore-Appliances und virtuellen Appliances. Klassische Ausdrücke werden auf NetScaler Cluster-Appliances und virtuellen Appliances nicht unterstützt. Aktuelle Benutzer, die ihre vorhandenen Konfigurationen in den NetScaler Cluster migrieren möchten, müssen alle Richtlinien, die klassische Ausdrücke enthalten, in die Standardausdrucksyntax migrieren.

- Eine einfache Beschreibung zur Verwendung der Syntax für NetScaler-Ausdrücke zum Erstellen von Web App Firewall-Regeln und eine Liste nützlicher Regeln finden Sie unter Firewall-Richtlinien.
- Eine ausführliche Erklärung zum Erstellen von Richtlinienregeln in der Syntax von NetScaler Ausdrücken finden Sie unter Richtlinien und Ausdrücke.

4. Wählen Sie Signaturen: Auf diesem Bildschirm wählen Sie die Signaturkategorien aus, die Sie zum Schutz Ihrer Websites und Webdienste verwenden möchten.

Dies ist kein obligatorischer Schritt. Sie können ihn überspringen, wenn Sie möchten, und zum Bildschirm **Specify Deep Protections** wechseln. Wenn der Bildschirm “Signaturen auswählen” übersprungen wird, werden nur ein Profil und die zugehörigen Richtlinien erstellt, und die Signaturen werden nicht erstellt.

Sie können **Neue Signatur erstellen** oder **Bestehende Signatur auswählen**.

Wenn Sie eine neue Sicherheitskonfiguration erstellen, sind die ausgewählten Signaturkategorien aktiviert und werden standardmäßig in einem neuen Signaturobjekt aufgezeichnet. Dem neuen Signaturobjekt wird derselbe Name zugewiesen, den Sie auf dem Bildschirm “Namen angeben” eingegeben haben, als Name der Sicherheitskonfiguration.

Wenn Sie bereits Signaturobjekte konfiguriert haben und eines davon als Signaturobjekt verwenden möchten, das der Sicherheitskonfiguration zugeordnet ist, die Sie erstellen, klicken Sie auf **Bestehende Signatur auswählen** und wählen Sie ein Signaturobjekt aus der Liste Signaturen aus.

Wenn Sie eine vorhandene Sicherheitskonfiguration ändern, können Sie auf Bestehende Signatur auswählen klicken und der Sicherheitskonfiguration ein anderes Signaturobjekt zuweisen.

Wenn Sie auf Neue Signatur erstellen klicken, können Sie den Bearbeitungsmodus auf **Einfach** oder **Erweitert**wählen.

1. **Signaturschutz angeben (einfacher Modus)**

Der einfache Modus ermöglicht eine einfache Konfiguration der Signatur mit einer voreingestellten Liste von Schutzdefinitionen für gängige Anwendungen wie IIS (Internet Information Server), PHP und ActiveX. Die Standardkategorien im einfachen Modus sind:

- CGI. Schutz vor Angriffen auf Websites, die CGI-Skripts in jeder Sprache verwenden, einschließlich PERL-Skripts, Unix-Shell-Skripts und Python-Skripts.
- Cold Fusion. Schutz vor Angriffen auf Websites, die die Adobe Systems® ColdFusion® Webentwicklungsplattform verwenden.
- FrontPage. Schutz vor Angriffen auf Websites, die die Microsoft® FrontPage® Webentwicklungsplattform verwenden.
- PHP. Schutz vor Angriffen auf Websites, die die Open-Source-Webentwicklungsskriptsprache PHP verwenden.
- Client side. Schutz vor Angriffen auf clientseitige Tools, die für den Zugriff auf Ihre geschützten Websites verwendet werden, wie Microsoft Internet Explorer, Mozilla Firefox, den Opera-Browser und den Adobe Acrobat Reader.
- Microsoft IIS. Schutz vor Angriffen auf Websites, auf denen der Microsoft Internet Information Server (IIS) ausgeführt wird
- Diverses. Schutz vor Angriffen auf andere serverseitige Tools wie Webserver und Datenbankserver.

Auf diesem Bildschirm wählen Sie die Aktionen aus, die den Signaturkategorien zugeordnet sind, die Sie auf dem Bildschirm “Signaturen auswählen” ausgewählt haben. Die Aktionen, die Sie konfigurieren können, sind:

- Blockieren
- Protokoll
- Statistiken

Standardmäßig sind die Aktionen Log und Stats aktiviert, aber nicht die Aktion Blockieren. Um Aktionen zu konfigurieren, klicken Sie auf **Einstellungen**. Sie können die Aktionseinstellungen aller ausgewählten Kategorien mithilfe der Dropdownliste **Aktion** ändern.

1. **Signaturschutz angeben (Erweiterter Modus)**

Der erweiterte Modus ermöglicht eine genauere Kontrolle der Signaturdefinitionen und bietet deutlich mehr Informationen. Verwenden Sie den erweiterten Modus, wenn Sie vollständige Kontrolle über die Signaturdefinition wünschen.

Der Inhalt dieses Bildschirms entspricht dem Inhalt des Dialogfelds “Signatures-Objekt ändern”, wie unter Konfigurieren oder Ändern eines Signatures-Objektsbeschrieben. In diesem Bildschirm können Sie Aktionen konfigurieren, indem Sie entweder auf die Dropdownliste **Aktionen** oder auf das Aktionsmenü klicken, das als Kreis mit drei Punkten angezeigt wird.

7. Deep Protections angeben: Auf diesem Bildschirm wählen Sie die erweiterten Schutzmaßnahmen (auch Sicherheitsüberprüfungen oder einfach Prüfungen genannt) aus, die Sie zum Schutz Ihrer Websites und Webdienste verwenden möchten. Welche Prüfungen verfügbar sind, hängt vom Profiltyp ab, den Sie auf dem Bildschirm “Namen angeben” ausgewählt haben. Alle Prüfungen sind für Web 2.0-Anwendungsprofile verfügbar.

Weitere Informationen finden Sie unter Überblick über Sicherheitsprüfungenund unter Erweiterte Formularschutzprüfungen.

Sie konfigurieren die Aktionen für den erweiterten Schutz, den Sie aktiviert haben.Die Aktionen, die Sie konfigurieren können, sind:

- Blockieren: blockiert Verbindungen, die der Signatur entsprechen. Diese Funktion ist standardmäßig deaktiviert.
- Protokoll: protokolliert Verbindungen, die der Signatur entsprechen, für eine spätere Analyse. Standardmäßig aktiviert.
- Statistiken: führt Statistiken für jede Signatur, die zeigt, wie viele Verbindungen zugeordnet wurden, und enthält bestimmte andere Informationen über die Arten von Verbindungen, die blockiert wurden. Diese Funktion ist standardmäßig deaktiviert.
- Lernen. Beobachten Sie den Traffic auf dieser Website oder diesem Webservice und verwenden Sie Verbindungen, die wiederholt gegen diese Prüfung verstoßen, um empfohlene Ausnahmen von der Überprüfung oder neue Regeln für die Überprüfung zu generieren. Nur für einige Schecks verfügbar. Weitere Informationen zur Lernfunktion finden Sie unter Konfigurieren und Verwenden der Lernfunktionund wie Lernen funktioniert und wie Ausnahmen (Entspannungen) konfiguriert oder erlernte Regeln für eine Überprüfung bereitstellen, finden Sie unter Manuelle Konfiguration mit der GUI.

Um Aktionen zu konfigurieren, aktivieren Sie den Schutz, indem Sie auf das Kontrollkästchen klicken, und klicken Sie dann auf **Aktionseinstellungen**, um die erforderlichen Aktionen auszuwählen. Wählen Sie ggf. andere Parameter aus, und klicken Sie dann auf **OK**, um das Fenster Aktionseinstellungen zu schließen.

Um alle Protokolle für eine bestimmte Prüfung anzuzeigen, wählen Sie diese Prüfung aus, und klicken Sie dann auf **Protokolle**, um den Syslog Viewer anzuzeigen, wie in Web App Firewall Logsbeschrieben. Wenn eine Sicherheitsüberprüfung den legitimen Zugriff auf Ihre geschützte Website oder Ihren

geschützten Webdienst blockiert, können Sie eine Entspannung für diese Sicherheitsprüfung erstellen und implementieren, indem Sie ein Protokoll auswählen, das die unerwünschte Blockierung anzeigt, und dann auf **Bereitstellen**klicken.

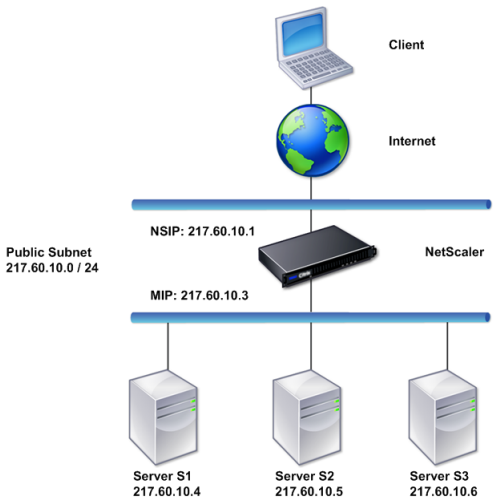
Nachdem Sie die Angabe der Aktionseinstellungen abgeschlossen haben, klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.

Im Folgenden finden Sie vier Verfahren, die zeigen, wie bestimmte Konfigurationstypen mithilfe des Web App Firewall-Assistenten durchgeführt werden.

Erstellen Sie eine neue Konfiguration

Gehen Sie wie folgt vor, um mithilfe des Application Firewall-Assistenten eine neue Firewallkonfiguration und Signaturobjekte zu erstellen.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Getting Started**auf **Application Firewall. Der Assistent wird geöffnet.



3. Wählen Sie im Bildschirm **Namen angeben** die Option **Neue Konfiguration erstellen.
4. Geben Sie im Feld **Name** einen Namen ein, und klicken Sie dann auf **Weiter**.
5. Klicken **Sie im Bildschirm „Regel angeben** “ erneut auf **Weiter** .
6. Wählen Sie im Bildschirm **Signaturen auswählen** die Option **Neue Signatur erstellen** und **Einfach** als Bearbeitungsmodus aus, und klicken Sie dann auf **Weiter**.
7. Konfigurieren Sie im Bildschirm **Signaturschutz angeben** die erforderlichen Einstellungen. Weitere Informationen darüber, welche Signaturen für das Blockieren in Betracht gezogen

werden sollten und wie Sie feststellen können, wann Sie das Blockieren für eine Signatur sicher aktivieren können, finden Sie unter Signaturen.

8. Konfigurieren Sie im Bildschirm **Deep Protections angeben** die erforderlichen Aktionen und Parameter in den **Aktionseinstellungen**.
9. Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, um den Application Firewall-Assistenten zu schließen.

Ändern Sie eine bestehende Konfiguration

Gehen Sie wie folgt vor, um eine bestehende Konfiguration und bestehende Signaturkategorien zu ändern.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Getting Started**auf **Application Firewall Wizard**. Der Assistent wird geöffnet.
3. Wählen Sie auf dem Bildschirm **Namen angeben** die Option “Bestehende Konfiguration ändern” und wählen Sie in der Dropdownliste **Name** die Sicherheitskonfiguration aus, die Sie bei der neuen Konfiguration erstellt haben, und klicken Sie dann auf **Weiter**.
4. Klicken Sie im Fenster **Regel angeben** auf “Weiter”, um den Standardwert “true” beizubehalten. Wenn Sie die Regel ändern möchten, führen Sie die unter Konfigurieren eines benutzerdefinierten Richtlinienausdrucks beschriebenen Schritte aus.
5. Klicken Sie im Bildschirm **Signaturen auswählen** auf **Vorhandene Signatur auswählen**. Wählen Sie in der Dropdownliste **Vorhandene Unterschrift** die entsprechende Option aus, und klicken Sie dann auf **Weiter**. Der Bildschirm mit erweitertem Signaturschutz wird angezeigt.
   Hinweis: Wenn Sie eine vorhandene Signatur auswählen, ist der Standardbearbeitungsmodus für signaturgeschützt auf “Erweitert”.
6. Konfigurieren Sie im Bildschirm Signaturschutz angeben die erforderlichen Einstellungen, und klicken Sie auf **Weiter**. Weitere Informationen darüber, welche Signaturen für das Blockieren in Betracht gezogen werden sollten und wie Sie feststellen können, wann Sie das Blockieren für eine Signatur sicher aktivieren können, finden Sie unter Signaturen.
7. Konfigurieren Sie im Fenster **Deep Protections angeben** die Einstellungen, und klicken Sie auf **Weiter**.
8. Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, um den **Web App Firewall-Assistenten**zu schließen.

Erstellen Sie eine neue Konfiguration ohne Signaturen

Gehen Sie wie folgt vor, um mit dem Application Firewall Wizard den Bildschirm “Signaturen auswählen” zu überspringen und eine neue Konfiguration zu erstellen, die nur das Profil und die

zugehörigen Richtlinien enthält, aber keine Signaturen enthält.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Getting Started**auf **Application Firewall Wizard**. Der Assistent wird geöffnet.
3. Wählen Sie auf dem Bildschirm „ **Namen angeben** “ die Option **Neue Konfiguration erstellen**aus.
4. Geben Sie im Feld **Name** einen Namen ein, und klicken Sie dann auf **Weiter**.
5. Klicken Sie im Bildschirm **Regel angeben** erneut auf **Weiter**.
6. Klicken Sie im Bildschirm **Signaturen auswählen** auf **Überspringen**.
7. Konfigurieren Sie im Bildschirm **Deep Protections angeben** die erforderlichen Aktionen und Parameter in den **Aktionseinstellungen**.
8. Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, um den Application Firewall Wizard zu schließen.

Benutzerdefinierten Richtlinienausdruck konfigurieren

Gehen Sie wie folgt vor, um mit dem Application Firewall Wizard eine spezielle Sicherheitskonfiguration zu erstellen, die nur bestimmte Inhalte schützt. In diesem Fall erstellen Sie eine neue Sicherheitskonfiguration, anstatt die ursprüngliche Konfiguration zu ändern. Für diese Art der Sicherheitskonfiguration ist eine benutzerdefinierte Regel erforderlich, sodass die Richtlinie die Konfiguration nur auf den ausgewählten Webverkehr anwendet.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Getting Started**auf **Application Firewall Wizard**.
3. Geben Sie auf dem Bildschirm “Namen angeben” einen Namen für Ihre neue Sicherheitskonfiguration in das Textfeld Name ein, wählen Sie den Typ der Sicherheitskonfiguration aus der Dropdownliste Typ aus, und klicken Sie dann auf **Weiter**.
4. Geben Sie auf dem Bildschirm **Regel angeben** eine Regel ein, die nur dem Inhalt entspricht, den diese Webanwendung schützen soll. Verwenden Sie die Dropdownliste **Häufig verwendete Ausdrücke** und den **Ausdrucksеditor**, um einen benutzerdefinierten Ausdruck zu erstellen. Wenn Sie fertig sind, klicken Sie auf **Weiter**.
5. Wählen Sie im Bildschirm **Signaturen auswählen** den Bearbeitungsmodus aus, und klicken Sie dann auf **Weiter**.
6. Konfigurieren Sie im Bildschirm **Signaturschutz angeben** die erforderlichen Einstellungen.
7. Konfigurieren Sie im Bildschirm **Deep Protections angeben** die erforderlichen Aktionen und Parameter in den **Aktionseinstellungen**.
8. Wenn Sie fertig sind, klicken Sie auf **Fertig stellen**, um den **Application Firewall Wizard**zu schließen.

Manuelle Konfiguration

August 19, 2021

Wenn Sie ein Profil an einen anderen Bindepunkt als Global binden möchten, müssen Sie die Bindung manuell konfigurieren. Bestimmte Sicherheitsprüfungen erfordern außerdem, dass Sie entweder die erforderlichen Ausnahmen manuell eingeben oder die Lernfunktion aktivieren, um die Ausnahmen zu generieren, die Ihre Websites und Webdienste benötigen. Einige dieser Aufgaben können nicht mithilfe des Web App Firewall Assistenten ausgeführt werden.

Wenn Sie mit der Funktionsweise der Web App Firewall vertraut sind und eine manuelle Konfiguration bevorzugen, können Sie ein Signaturobjekt und ein Profil manuell konfigurieren, das Signaturobjekt dem Profil zuordnen, eine Richtlinie mit einer Regel erstellen, die dem zu konfigurierenden Webdatenverkehr entspricht, und die Richtlinie zuordnen. mit dem Profil. Anschließend binden Sie die Richtlinie an Global oder an einen Bindepunkt, um sie in Kraft zu setzen, und Sie haben eine vollständige Sicherheitskonfiguration erstellt.

Für die manuelle Konfiguration können Sie die GUI (eine grafische Oberfläche) oder die Befehlszeile verwenden. Citrix empfiehlt die Verwendung der GUI. Nicht alle Konfigurationsaufgaben können über die Befehlszeile ausgeführt werden. Bestimmte Aufgaben, wie das Aktivieren von Signaturen und das Überprüfen von erlernten Daten, müssen in der GUI ausgeführt werden. Die meisten anderen Aufgaben sind in der GUI einfacher durchzuführen.

Konfiguration replizieren

Wenn Sie die Web App Firewall manuell mit der GUI (GUI) oder der Befehlszeilenschnittstelle (CLI) konfigurieren, wird die Konfiguration in der Datei /nsconfig/ns.conf gespeichert. Sie können die Befehle in dieser Datei verwenden, um die Konfiguration auf einer anderen Appliance zu replizieren. Sie können die Befehle einzeln ausschneiden und in die CLI einfügen, oder Sie können mehrere Befehle in einer Textdatei im Ordner /var/tmp speichern und als Batchdatei ausführen. Es folgt ein Beispiel für die Ausführung einer Batchdatei mit Befehlen, die aus der Datei /nsconfig/ns.conf einer anderen Appliance kopiert wurden:

```
> batch -f /var/tmp/appfw_add.txt
```

> **Warnung:**
>
> Importbefehle werden nicht in der Datei ns.conf gespeichert. Bevor Sie Befehle aus der Datei ns.conf ausführen, um die Konfiguration auf einer anderen Appliance zu replizieren, müssen Sie alle in der Konfiguration verwendeten Objekte (z. B. Signaturen, Fehlerseite, WSDL und Schema) in die Appliance importieren, auf der Sie die Konfiguration replizieren. Der Befehl add zum Hinzufügen eines in einer ns.conf-Datei gespeicherten Web App Firewall-Profils

> enthält möglicherweise den Namen eines importierten Objekts, aber ein solcher Befehl schlägt möglicherweise fehl, wenn er auf einer anderen Appliance ausgeführt wird, wenn das referenzierte Objekt auf dieser Appliance nicht vorhanden ist.

Weitere Informationen zu Import- oder Exportdetails für die Replikation der Konfiguration finden Sie unter Signaturexportund Themen über allgemeine Importexporte .

Manuelle Konfiguration mithilfe der NetScaler-GUI

May 11, 2023

Wenn Sie die Web App Firewall-Funktion manuell konfigurieren müssen, empfiehlt Citrix, das NetScaler-GUI-Verfahren zu verwenden.

Um ein Signaturobjekt zu erstellen und zu konfigurieren

Bevor Sie die Signaturen konfigurieren können, müssen Sie anhand der entsprechenden Standardvorlage für Signaturobjekte ein Signaturobjekt erstellen. Weisen Sie der Kopie einen neuen Namen zu, und konfigurieren Sie dann die Kopie. Sie können die Standardsignaturobjekte nicht direkt konfigurieren oder ändern. Das folgende Verfahren enthält grundlegende Anweisungen zum Konfigurieren eines Signaturobjekts. Ausführlichere Anweisungen finden Sie unter Manuelles Konfigurieren der Signature-Funktion.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie als Vorlage verwenden möchten, und klicken Sie dann auf **Hinzufügen**.

   Ihre Auswahlmöglichkeiten:

   - **Standardsignaturen.** Enthält die Signaturregeln, die SQL-Einschleusungsregeln und die Cross-Site-Scripting-Regeln.
   - **XPath-Einschleusung.** Enthält alle Elemente der Standardsignaturen und enthält zusätzlich die XPath-Injektionsregeln.
3. Geben **Sie im Dialogfeld Signaturobjekt hinzufügen** einen Namen für Ihr neues Signaturobjekt ein, klicken Sie auf OK und dann auf **Schließen**. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrichsymbol beginnen und aus einem bis 31 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), bei (@), gleich (=) und Unterstrichen (_) bestehen.
4. Wählen Sie das Signaturobjekt aus, das Sie erstellt haben, und klicken Sie dann auf **Öffnen**.

5. Stellen **Sie im Dialogfeld „Signaturobjekt ändern** “ links die Optionen „ **Filterkriterien** anzeigen“ ein, um die Filterelemente anzuzeigen, die Sie konfigurieren möchten.

   Wenn Sie diese Optionen ändern, werden die von Ihnen angegebenen Ergebnisse im Fenster Gefilterte Ergebnisse rechts angezeigt. Weitere Informationen zu den Kategorien von Signaturen finden Sie unter Signaturen.

6. Konfigurieren Sie im Bereich **Gefilterte Ergebnisse** die Einstellungen für eine Signatur, indem Sie die entsprechenden Kontrollkästchen aktivieren und deaktivieren.
7. Wenn Sie fertig sind, klicken Sie auf **Schließen**.

So erstellen Sie ein Web App Firewall-Profil mit der GUI

Zum Erstellen eines Web App Firewall-Profils müssen Sie nur wenige Konfigurationsdetails angeben.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Web App Firewall-Profil erstellen** einen Namen für Ihr Profil ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und aus einem bis 31 Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), at (@), Gleichheit (=), Doppelpunkt (:) und Unterstrich (_) bestehen.

4. Wählen Sie den Profiltyp aus der Dropdownliste aus.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So konfigurieren Sie ein Web App Firewall-Profil über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich das zu konfigurierende Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Konfigurieren Sie im Dialogfeld **Web App Firewall-Profil konfigurieren** auf der Registerkarte **Sicherheitsüberprüfungen** die Sicherheitsüberprüfungen.

   - Um eine Aktion für eine Prüfung zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie in der Liste das Kontrollkästchen für diese Aktion.
   - Um weitere Parameter für die Prüfungen zu konfigurieren, die sie haben, klicken Sie in der Liste auf den blauen Chevron ganz rechts neben dieser Prüfung. Konfigurieren Sie im daraufhin angezeigten Dialogfeld die Parameter. Diese variieren von Scheck zu Scheck.

     Sie können auch eine Prüfung auswählen und unten im Dialogfeld auf Öffnen klicken, um das Dialogfeld Entspannung konfigurieren oder Regel konfigurieren für diese Überprüfung

anzuzeigen. Diese Dialogfelder variieren auch von Prüfung zu Prüfung. Die meisten von ihnen enthalten eine Registerkarte Schecks und eine Registerkarte Allgemein . Wenn die Prüfung Entspannungen oder benutzerdefinierte Regeln unterstützt, enthält die Registerkarte Prüfungen eine Schaltfläche Hinzufügen, wodurch ein weiteres Dialogfeld geöffnet wird, in dem Sie eine Entspannung oder Regel für die Prüfung angeben können. (Eine Entspannung ist eine Regel, um bestimmten Verkehr vom Scheck auszunehmen.) Wenn Entspannungen bereits konfiguriert wurden, können Sie eine auswählen und auf Öffnen klicken, um sie zu ändern.

- Um gelernte Ausnahmen oder Regeln für eine Prüfung zu überprüfen, wählen Sie die Prüfung aus, und klicken Sie dann auf Erlernte Verletzungen. Wählen Sie im Dialogfeld Gelernte Regeln verwalten nacheinander jede gelernte Ausnahme oder Regel aus.
  - Um die Ausnahme oder Regel zu bearbeiten und sie dann zur Liste hinzuzufügen, klicken Sie auf **Bearbeiten und bereitstellen**.
  - Um die Ausnahme oder Regel ohne Änderung zu akzeptieren, klicken Sie auf **Bereitstellen**.
  - Um die Ausnahme oder Regel aus der Liste zu entfernen, klicken Sie auf **Überspringen**.
- Um die Liste der zu überprüfenden Ausnahmen oder Regeln zu aktualisieren, klicken Sie auf **Aktualisieren**.
- **Um den**Learning Visualizer**zu öffnen und damit die erlernten Regeln zu überprüfen, klicken Sie auf Visualizer.**
- Um die Protokolleinträge für Verbindungen zu überprüfen, die einer Prüfung entsprechen, wählen Sie die Prüfung aus und klicken Sie dann auf **Protokolle**. Anhand dieser Informationen können Sie ermitteln, welche Checks mit Angriffen übereinstimmen, sodass Sie die Blockierung für diese Prüfungen aktivieren können. Sie können diese Informationen auch verwenden, um zu bestimmen, welche Prüfungen mit dem legitimen Datenverkehr übereinstimmen, sodass Sie eine entsprechende Ausnahme konfigurieren können, um diese legitimen Verbindungen zuzulassen. Weitere Informationen zu den Protokollen finden Sie unter Protokolle, Statistiken und Berichte.
- Um eine Überprüfung vollständig zu deaktivieren, deaktivieren Sie in der Liste alle Kontrollkästchen rechts neben dieser Prüfung.

4. Konfigurieren Sie auf der Registerkarte **Einstellungen** die Profileinstellungen.
   - Um das Profil mit dem Signatursatz zu verknüpfen, den Sie zuvor erstellt und konfiguriert haben, wählen Sie unter **Allgemeine Einstellungen**diesen Signatursatz in der Dropdownliste Signaturen aus.

> **Hinweis:**
>
> Sie können die Bildlaufleiste auf der rechten Seite des Dialogfelds verwenden, um nach unten zu scrollen und den Abschnitt Allgemeine Einstellungen anzuzeigen.

- Um ein HTML- oder XML-Fehlerobjekt zu konfigurieren, wählen Sie das Objekt aus der entsprechenden Dropdownliste aus.

  > **Hinweis:**
  >
  > Sie müssen zuerst das Fehlerobjekt, das Sie verwenden möchten, im Importbereich hochladen.

- Um den Standard-XML-Inhaltstyp zu konfigurieren, geben Sie die Zeichenfolge für den Inhaltstyp direkt in die Textfelder Standardanforderung und Standardantwort ein, oder klicken Sie auf Zulässige Inhaltstypen verwalten, um die Liste der zulässigen Inhaltstypen zu verwalten.

5. Wenn Sie die Lernfunktion verwenden möchten, klicken Sie auf Lernen, und konfigurieren Sie die Lerneinstellungen für das Profil. Weitere Informationen finden Sie unter Konfigurieren und Lernen Feature.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Profilbereich zurückzukehren.

Konfiguration einer Web App Firewall-Regel oder Lockerung

In diesem Dialogfeld konfigurieren Sie zwei verschiedene Arten von Informationen, je nachdem, welche Sicherheitsüberprüfung Sie konfigurieren. In den meisten Fällen konfigurieren Sie eine Ausnahme (oder Lockerung) für die Sicherheitsüberprüfung. Wenn Sie die Prüfung „URL ablehnen“ oder „Feldformate“ konfigurieren, konfigurieren Sie eine Ergänzung (oder Regel). Der Prozess für beide ist derselbe.

So konfigurieren Sie eine Relaxationsregel mithilfe der NetScaler-GUI

1. **Navigieren Sie zu**Sicherheit**>**NetScaler Web App Firewall > Profile**.**
2. Wählen Sie im Bereich **Profile** das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Web App Firewall-Profil konfigurieren** im Abschnitt **Erweiterte Einstellungen** auf **Relaxationsregel** . Der Abschnitt **Entspannungsregeln** enthält die vollständige Liste der Lockerungsregeln für die Web App Firewall.
4. Klicken Sie auf eine Sicherheitsregel, die Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.

5. Die Seite mit den URL-Entspannungsregeln enthält eine Liste von Aktionen, die Sie für diese Regel konfigurieren können, sowie eine Liste vorhandener Lockerungen oder Regeln. Die Liste ist möglicherweise leer, wenn Sie weder manuell irgendwelche Lockerungen hinzugefügt noch alle von der Lernmaschine empfohlenen Lockerungen genehmigt haben. Unter der Liste befindet sich eine Reihe von Schaltflächen, mit denen Sie die Lockerungen in der Liste hinzufügen, ändern, löschen, aktivieren oder deaktivieren können.
6. Gehen Sie wie folgt vor, um eine Entspannung oder Regel hinzuzufügen oder zu ändern:
   - Um eine neue Entspannung hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Entspannung zu ändern, wählen Sie die Entspannung aus, die Sie ändern möchten, und klicken Sie dann auf **Öffnen**.

   Die Seite mit den **Relaxationsregeln für die Start-URL** wird angezeigt. Mit Ausnahme des Titels sind diese Dialogfelder identisch.
7. Füllen Sie das Dialogfeld wie unten beschrieben aus. Die Dialogfelder für jede Prüfung sind unterschiedlich. Die folgende Liste deckt alle Elemente ab, die in einem beliebigen Dialogfeld erscheinen können.
   - **Aktiviertes Kontrollkästchen**— Wählen Sie dieses Kontrollkästchen aus, um diese Relaxation oder Regel aktiv zu verwenden. Deaktivieren Sie das Kontrollkästchen, um sie zu deaktivieren.
   - **Inhaltstyp des Anhangs**— Das Content-Type-Attribut eines XML-Anhangs. Geben Sie im Textbereich einen regulären Ausdruck ein, der dem Content-Type-Attribut der zuzulassen XML-Anlagen entspricht.
   - **Aktions-URL**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, an die die in das Webformular eingegebenen Daten übermittelt werden.
   - **Cookie**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der das Cookie definiert.
   - **Feldname**— Ein Webformular-Feldnamenelement kann mit Feldname, Formularfeld oder einem anderen ähnlichen Namen beschriftet sein. Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der den Namen des Formularfeldes definiert.
   - **Von Origin-URL**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, die das Webformular hostet.
   - **Aus Aktions-URL**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, an die die in das Webformular eingegebenen Daten übermittelt werden.
   - **Name**— Ein XML-Element- oder Attributname. Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der den Namen des Elements oder Attributs definiert.

- **URL**— Ein URL-Element kann als Aktions-URL, Ablehnungs-URL, Formular-Aktions-URL, Formular-Ursprungs-URL, Start-URL oder einfach als URL bezeichnet werden. Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert.
- **Format**— Der Abschnitt „Format“ enthält mehrere Einstellungen, darunter Listenfelder und Textfelder. Folgendes kann auftreten:
  - **Typ**— Wählen Sie in der Dropdownliste Typ einen Feldtyp aus. Um eine neue Feldtypdefinition hinzuzufügen, klicken Sie auf Verwalten—
  - **Mindestlänge**— Geben Sie eine positive Ganzzahl ein, die die Mindestlänge in Zeichen darstellt, wenn Sie Benutzer zwingen möchten, dieses Feld auszufüllen. Standard: 0 (Ermöglicht es, das Feld leer zu lassen.)
  - **Maximale Länge**— Um die Länge der Daten in diesem Feld zu begrenzen, geben Sie eine positive Ganzzahl ein, die die maximale Länge in Zeichen darstellt. Standard: 65535
- **Position**— Wählen Sie aus der Dropdownliste das Element der Anforderung aus, auf das Ihre Entspannung angewendet wird. Für HTML-Sicherheitsprüfungen stehen folgende Optionen zur Verfügung:
  - FormField — Formularfelder in Webformularen.
  - Header — Header anfordern.
  - Cookie-Set-Cookie-Header.

  Für XML-Sicherheitsprüfungen stehen folgende Optionen zur Verfügung:
  - ELEMENT — XML-Element.
  - ATTRIBUE — XML-Attribut.
- **Maximale Anlagengröße**— Die maximal zulässige Größe in Byte für einen XML-Anhang.
- **Kommentare**— Geben Sie im Textbereich einen Kommentar ein. Optional.

Hinweis: Für jedes Element, das einen regulären Ausdruck erfordert, können Sie den regulären Ausdruck eingeben, das Menü „Regex-Tokens“ verwenden, um reguläre Ausdruckselemente und Symbole direkt in das Textfeld einzufügen, oder auf **Regex-Editor** klicken, um das Dialogfeld „ **Regulären Ausdruck hinzufügen** “ zu öffnen und es zum Erstellen des Ausdrucks zu verwenden.

8. Um eine Entspannung oder Regel zu entfernen, wählen Sie sie aus, und klicken Sie dann auf **Löschen**.
9. Um eine Entspannung oder Regel zu aktivieren, wählen Sie sie aus, und klicken Sie dann auf **Aktivieren**.
10. Um eine Entspannung oder Regel zu deaktivieren, wählen Sie sie aus, und klicken Sie dann auf **Deaktivieren**.

11. Um die Einstellungen und Beziehungen aller vorhandenen Relaxationen in einer integrierten interaktiven Grafikdarstellung zu konfigurieren, klicken Sie auf **Visualizer**, und verwenden Sie die Anzeigetools.

    > **Hinweis:**
    >
    > Die Schaltfläche **Visualizer** wird nicht in allen Dialogfeldern für die Überprüfung der Entspannung angezeigt.

12. Um die erlernten Regeln für diese Prüfung zu überprüfen, klicken Sie auf Lernen und führen Sie die Schritte unter So konfigurieren und verwenden Sie die Lernfunktionaus
13. Klicken Sie auf **OK**.

So konfigurieren Sie die erlernten Regeln mithilfe der NetScaler-GUI

1. **Navigieren Sie zu**Sicherheit**>**NetScaler Web App Firewall > Profile**.**
2. Wählen Sie im Bereich **Profile** das Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite mit dem **NetScaler Web App Firewall-Profil** in den **erweitertenEinstellungen auf Gelernte Regeln**. Im Abschnitt**Gelernte Regeln** finden Sie eine Liste der Sicherheitsüberprüfungen, die im aktuellen Profil verfügbar sind und die Lernfunktion unterstützen.
4. Um die Lernschwellen zu konfigurieren, wählen Sie eine Sicherheitsüberprüfung aus und klicken Sie auf **Einstellungen**.
5. Auf der Seite **Einstellungen für dynamische Profilerstellung und Lernregeln** können Sie die Einstellungen festlegen. Weitere Informationen finden Sie unter Dynamische Profileinstellungen

    - **Mindestzahlschwelle.** Je nachdem, welche Lerneinstellungen Sie für die Sicherheitsüberprüfung konfigurieren, bezieht sich der Schwellenwert für die Mindestanzahl der Benutzersitzungen, die insgesamt eingehalten werden müssen, auf die Mindestanzahl von Anfragen, die eingehalten werden müssen, oder auf die Mindestanzahl, mit der ein bestimmtes Formularfeld eingehalten werden muss, bevor eine erlernte Entspannung generiert wird. Standard: 1
    - **Prozentsatz des Schwellenwerts.** Je nachdem, welche Lerneinstellungen der Sicherheitsüberprüfung Sie konfigurieren, bezieht sich der Schwellenwert in Prozent auf den Prozentsatz der gesamten beobachteten Benutzersitzungen, die gegen die Sicherheitsüberprüfung verstoßen haben, auf den Prozentsatz der Anfragen oder auf den Prozentsatz, mit dem ein Formularfeld mit einem bestimmten Feldtyp übereinstimmte, vor erlernte Entspannung wird erzeugt. Standard: 0

6. Um alle gelernten Daten zu entfernen und die Lernfunktion zurückzusetzen, sodass sie ihre Beobachtungen erneut von vorne beginnen muss, wählen Sie die Aktion **Alle gelernten Daten entfernen** .

   > **Hinweis:**
   >
   > Mit dieser Schaltfläche werden nur gelernte Empfehlungen entfernt, die nicht geprüft und entweder genehmigt oder übersprungen wurden. Erlernte Entspannungen, die akzeptiert und eingesetzt wurden, werden nicht beseitigt.

7. Um die Lernmaschine auf den Datenverkehr von einer bestimmten Gruppe von IPs zu beschränken, klicken Sie auf **Trusted Learning Clients**und fügen Sie die zu verwendenden IP-Adressen zur Liste hinzu.

   a) Um der Liste der vertrauenswürdigen Lernclients eine IP-Adresse oder einen IP-Adressbereich hinzuzufügen, klicken Sie auf **Hinzufügen**.
   b) **Klicken Sie auf der Seite**AppFirewall-Profile to Trusted Clint Binding**auf Hinzufügen.**
   c) Markieren Sie das Kontrollkästchen **Aktiviert**, um die Funktion zu aktivieren.
   d) Geben Sie in das** Feld Trusted Learning Client die IP-Adresse oder einen IP-Adressbereich im CIDR-Format ein.
   e) Geben Sie im Textbereich **Kommentare** einen Kommentar ein, der diese IP-Adresse oder diesen Bereich beschreibt.
   f) Klicken Sie auf **Erstellen** und **Schließen**.

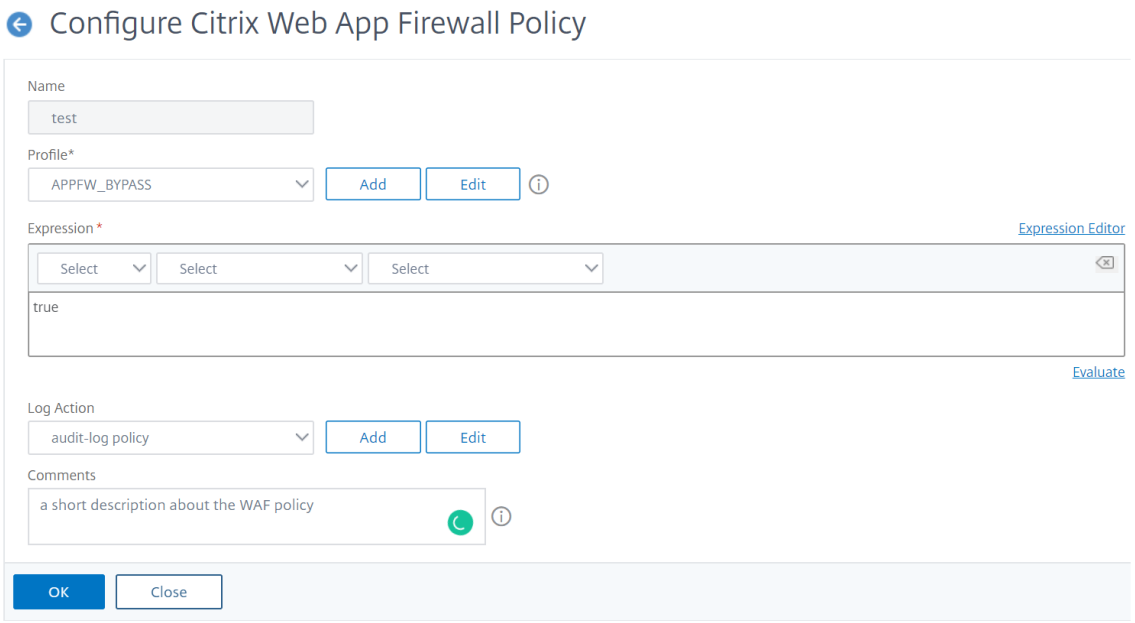
8. Um eine vorhandene IP-Adresse oder einen Bereich zu ändern, klicken Sie auf die IP-Adresse oder den Bereich und dann auf **Bearbeiten**. Mit Ausnahme des Namens ist das angezeigte Dialogfeld identisch mit dem Dialogfeld Trusted Learning Clients hinzufügen.
9. Um eine IP-Adresse oder einen Bereich zu deaktivieren oder zu aktivieren, sie jedoch in der Liste zu belassen, klicken Sie auf die IP-Adresse oder den Bereich und dann gegebenenfalls auf **Deaktivieren** oder **Aktivieren**.
10. Um eine IP-Adresse oder einen Bereich vollständig zu entfernen, klicken Sie auf die IP-Adresse oder den Bereich und dann auf **Löschen**.
11. Klicken Sie auf **Schließen**, um zur **NetScaler Web App Firewall-Profilseite** zurückzukehren.

So erstellen Sie eine NetScaler Web App Firewall-Richtlinie mithilfe der NetScaler-GUI

1. Navigieren Sie zu **Sicherheit** > **NetScaler Web App Firewall** > **Richtlinien**.
2. Klicken Sie auf der Seite **Richtlinien** auf den Link **NetScaler Web App Firewall Policy** .
3. **Klicken Sie auf der Seite mit den NetScaler Web App Firewall-Richtlinien auf Hinzufügen.**
4. Stellen Sie auf der Seite NetScaler Web App Firewall-Richtlinie erstellen die folgenden Parameter ein.

a) Name. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und aus einem bis 128 Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), at (@), Gleichheit (=), Doppelpunkt (:) und Unterstrich (_) bestehen.
b) Steckbrief. Wählen Sie in der Dropdown-Liste Profil das Profil aus, das Sie dieser Richtlinie zuordnen möchten. Sie können ein Profil erstellen, das mit Ihrer Richtlinie verknüpft wird, indem Sie auf Neu klicken, und Sie können ein vorhandenes Profil ändern, indem Sie auf **Ändern**klicken.
c) Expression. Erstellen Sie im Textbereich Ausdruck eine Regel für Ihre Richtlinie.
d) Aktion protokollieren. Fügen Sie eine Log-Aktion hinzu, oder Sie können eine bestehende Log-Aktion ändern.
e) Kommentare. Eine kurze Beschreibung der Richtlinie.

5. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.



So erstellen oder konfigurieren Sie eine Web App Firewall-Regel (Ausdruck)

Die Richtlinienregel, auch *Ausdruck*genannt, definiert den Webverkehr, den die Web App Firewall mithilfe des mit der Richtlinie verknüpften Profils filtert. Wie andere NetScaler-Richtlinienregeln (oder *-ausdrücke*) verwenden die Web App Firewall-Regeln die Syntax von NetScaler-Ausdrücken. Diese Syntax ist leistungsstark, flexibel und erweiterbar. Es ist zu komplex, um es in diesen Anweisungen vollständig zu beschreiben. Sie können das folgende Verfahren verwenden, um eine einfache Firewall-Richtlinienregel zu erstellen, oder Sie können sie als Überblick über den Richtlinienerstellungsprozess lesen.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie im Web App Firewall-Assistenten oder in

der NetScaler-GUI zum entsprechenden Speicherort, um Ihre Richtlinienregel zu erstellen:

- Wenn Sie eine Richtlinie im Web App Firewall-Assistenten konfigurieren, klicken Sie im Navigationsbereich auf **NetScaler Web App Firewall Wizard**, klicken Sie dann im Detailbereich auf **NetScaler Web App Firewall Wizard**, und navigieren Sie dann zur Registerkarte Regel **angeben** .
- Wählen **Sie auf der Seite Regel angeben** das Präfix für Ihren Ausdruck aus der Dropdownliste aus. Ihre Auswahlmöglichkeiten:
- **HTTP.** Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
- **SYS.** Eine oder mehrere geschützte Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
- **CLIENT.** Der Computer, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
- **SERVER.** Der Computer, an den die Anfrage gesendet wurde. Wählen Sie diese Option, wenn Sie einige Aspekte des Empfängers der Anfrage untersuchen möchten.

Nachdem Sie ein Präfix ausgewählt haben, zeigt die Web App Firewall ein zweiteiliges Eingabeaufforderungsfenster an, in dem oben die möglichen nächsten Optionen angezeigt werden, und eine kurze Erklärung, was die ausgewählte Auswahl unten bedeutet.

2. Wähle dein nächstes Semester.

   Wenn Sie HTTP als Präfix ausgewählt haben, ist Ihre einzige Wahl REQ, das das Request/Response-Paar angibt. (Die Web App Firewall arbeitet bei der Anfrage und Antwort als Einheit statt auf jeder separat.) Wenn Sie ein anderes Präfix gewählt haben, sind Ihre Auswahl vielfältiger. Um Hilfe zu einer bestimmten Auswahl zu erhalten, klicken Sie einmal auf diese Auswahl, um Informationen darüber im unteren Eingabeaufforderungsfenster anzuzeigen.

   Wenn Sie entschieden haben, welchen Begriff Sie möchten, doppelklicken Sie darauf, um ihn in das Ausdrucksfenster einzufügen.

3. Geben Sie einen Zeitraum nach dem gerade gewählten Term ein. Sie werden dann aufgefordert, Ihren nächsten Begriff zu wählen, wie im vorherigen Schritt beschrieben. Wenn für einen Begriff die Eingabe eines Wertes erforderlich ist, geben Sie den entsprechenden Wert ein. Wenn Sie beispielsweise HTTP.REQ.HEADER (“”) wählen, geben Sie den Kopfzeilennamen zwischen den Anführungszeichen ein.
4. Wählen Sie weiterhin Begriffe aus den Eingabeaufforderungen aus und geben Sie alle benötigten Werte ein, bis Ihr Ausdruck beendet ist.

   Im Folgenden finden Sie einige Beispiele für Ausdrücke für bestimmte Zwecke.

- **Spezifischer Webhost.** So stimmen Sie den Datenverkehr von einem bestimmten Webhost ab:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Ersetzen Sie shopping.example.com durch den Namen des Webhosts, den Sie abgleichen möchten.

- **Bestimmter Webordner oder -verzeichnis.** So stimmen Sie den Datenverkehr aus einem bestimmten Ordner oder Verzeichnis auf einem Webhost ab:

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
```

Ersetzen Sie für www.example.com den Namen des Webhosts. Ersetzen Sie für Ordner den Ordner oder Pfad durch den Inhalt, den Sie abgleichen möchten. Wenn sich Ihr Warenkorb beispielsweise in einem Ordner namens /solutions/orders befindet, ersetzen Sie diese Zeichenfolge durch Ordner.

- **Bestimmte Art von Inhalt: GIF-Bilder.** So passen Sie Bilder im GIF-Format an:

```
HTTP.REQ.URL.ENDSWITH(".png")
```

Um Bilder in anderen Formaten zu entsprechen, ersetzen Sie anstelle von .png eine andere Zeichenfolge.

- **Spezifischer Inhaltstyp: Skripts.** So passen Sie alle CGI-Skripts an, die sich im CGI-BIN-Verzeichnis befinden:

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
```

So passen Sie alle JavaScripts mit .js-Erweiterungen an:

```
HTTP.REQ.URL.ENDSWITH(".js")
```

Weitere Informationen zum Erstellen von Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Wenn Sie die Befehlszeile zum Konfigurieren einer Richtlinie verwenden, denken Sie daran, doppelte Anführungszeichen in NetScaler-Ausdrücken zu umgehen. Der folgende Ausdruck ist beispielsweise korrekt, wenn er in die GUI eingegeben wird:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Wenn Sie es jedoch über die Befehlszeile eingeben, müssen Sie stattdessen Folgendes eingeben:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

```
1 ![Policy expression configuration](/en-us/citrix-adc/media/waf-rule.png
     )
```


So fügen Sie eine Firewallregel (Ausdruck) mithilfe des Dialogfelds Ausdruck hinzufügen hinzu

Das Dialogfeld **Ausdruck hinzufügen** (auch als Ausdrucksеditor bezeichnet) hilft Benutzern, die mit der Sprache der NetScaler-Ausdrücke nicht vertraut sind, eine Richtlinie zu erstellen, die dem Datenverkehr entspricht, den sie filtern möchten.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie im Web App Firewall-Assistenten oder in der NetScaler GUI zum entsprechenden Speicherort:
   - Wenn Sie eine Richtlinie im **Web App Firewall-Assistenten** konfigurieren, klicken Sie im Navigationsbereich auf **Web App Firewall**, klicken Sie dann im Detailbereich auf **Web App Firewall-Assistent**, und navigieren Sie dann zum Fenster **Regel angeben** .
   - Wenn Sie eine Richtlinie manuell konfigurieren, erweitern Sie im Navigationsbereich **Web App Firewall**, **Richtlinien**und dann **Firewall**. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Richtlinie zu erstellen. Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
2. Klicken Sie auf dem Bildschirm **Regel angeben** im Dialogfeld **Web App-Firewall-Profil erstellen** oder im Dialogfeld **Web App Firewall-Profil konfigurieren** auf **Hinzufügen**.
3. Wählen **Sie im Dialogfeld Ausdruck hinzufügen** im Bereich Ausdruck konstruieren im ersten Listenfeld eines der folgenden Präfixe aus:
   - **HTTP.** Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht. Die Standardauswahl.
   - **SYS.** Eine oder mehrere geschützte Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - **CLIENT.** Der Computer, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - **SERVER.** Der Computer, an den die Anfrage gesendet wurde. Wählen Sie diese Option, wenn Sie einige Aspekte des Empfängers der Anfrage untersuchen möchten.
4. Wählen Sie im zweiten Listenfeld Ihren nächsten Begriff aus. Die verfügbaren Begriffe unterscheiden sich je nach Auswahl, die Sie im vorherigen Schritt getroffen haben, da das Dialogfeld die Liste automatisch so anpasst, dass sie nur die Begriffe enthält, die für den Kontext gültig sind. Wenn Sie beispielsweise im vorherigen Listenfeld HTTP ausgewählt haben, ist REQ für Anfragen die einzige Wahl. Da die Web App Firewall Anfragen und zugehörige Antworten als eine einzige Einheit behandelt und beide filtert, müssen Sie keine spezifischen Antworten separat eingehen. Nachdem Sie Ihren zweiten Begriff gewählt haben, erscheint rechts neben dem zweiten ein drittes Listenfeld. Im Hilfefenster wird eine Beschreibung des zweiten Begriffs angezeigt, und im Fenster Vorschauausdruck wird Ihr Ausdruck angezeigt.
5. Wählen Sie im dritten Listenfeld den nächsten Begriff aus. Rechts erscheint ein neues Listenfeld, und das Hilfefenster ändert sich, um eine Beschreibung des neuen Begriffs anzuzeigen. Das Fenster Vorschauausdruck wird aktualisiert, um den Ausdruck so anzuzeigen, wie Sie ihn bis zu

diesem Zeitpunkt angegeben haben.

6. Wählen Sie weiterhin Begriffe aus und wenn Sie dazu aufgefordert werden, Argumente auszufüllen, bis Ihr Ausdruck vollständig ist. Wenn Sie einen Fehler machen oder Ihren Ausdruck ändern möchten, nachdem Sie bereits einen Begriff ausgewählt haben, können Sie einfach einen anderen Begriff wählen. Der Ausdruck wird geändert, und alle Argumente oder weitere Begriffe, die Sie nach dem geänderten Begriff hinzugefügt haben, werden gelöscht.
7. Wenn Sie mit der Erstellung Ihres Ausdrucks fertig sind, klicken Sie auf OK, um das Dialogfeld Ausdruck hinzufügen zu schließen. Ihr Ausdruck wird in den Ausdruckstextbereich eingefügt.

So binden Sie eine Web App Firewall-Richtlinie mithilfe der NetScaler-GUI

1. Führen Sie einen der folgenden Schritte aus:
   - Navigieren Sie zu **Sicherheit** > **Web App Firewall**und klicken Sie im Detailbereich auf **Application Firewall Policy Manager**.
   - **Navigieren Sie zu**Sicherheit**>**NetScaler Web App Firewall**>**Richtlinien**>**Firewall**und klicken Sie im Bereich „NetScaler Web App Firewall Policies“ auf Policy Manager.**
2. Wählen Sie im Dialogfeld **Anwendungsfirewall Policy Manager** aus der Dropdownliste den Bindpunkt aus, an den Sie die Richtlinie binden möchten. Es stehen folgende Optionen zur Auswahl:
   - **Global überschreiben.** Richtlinien, die an diesen Bindpunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen auf der NetScaler-Appliance und werden vor allen anderen Richtlinien angewendet.
   - **LB Virtueller Server.** Richtlinien, die an einen virtuellen Lastausgleichsserver gebunden sind, werden nur auf den Datenverkehr angewendet, der von diesem virtuellen Lastausgleichsserver verarbeitet wird, und sie werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie LB Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Load-Balancing-Server auswählen, an den Sie diese Richtlinie binden möchten.
   - **CS Virtueller Server.** Richtlinien, die an einen virtuellen Content Switching-Server gebunden sind, werden nur auf den Datenverkehr angewendet, der von diesem virtuellen Content Switching-Server verarbeitet wird, und sie werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie CS Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Content Switching-Server auswählen, an den Sie diese Richtlinie binden möchten.
   - **Standard Global.** Richtlinien, die an diesen Bindpunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der NetScaler-Appliance.
   - **Richtlinien-Etikett.** Richtlinien, die an ein Richtlinienlabel gebunden sind, verarbeiten den Datenverkehr, den das Richtlinienlabel an sie weiterleitet. Das Richtlinienlabel bestimmt die Reihenfolge, in der Richtlinien auf diesen Verkehr angewendet werden.
   - **Keine.** Binden Sie die Richtlinie an keinen Bindungspunkt.

3. Klicken Sie auf **Weiter**. Eine Liste der vorhandenen Web App Firewall-Richtlinien wird angezeigt.
4. Wählen Sie die Richtlinie aus, die Sie binden möchten, indem Sie darauf klicken.
5. Nehmen Sie weitere Anpassungen an der Bindung vor.
    - Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten **neu generieren auswählen, um die Prioritäten** gleichmäßig neu zu nummerieren.
    - Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld **Web App Firewall-Richtlinie konfigurieren** zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.
    - Um den Gehe zu Ausdruck festzulegen, doppelklicken Sie auf das Feld in der Spaltenüberschrift **Gehe zu Ausdruck**, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
    - Um die Option "Aufrufen" festzulegen, doppelklicken Sie auf das Feld in der Spaltenüberschrift "Aufrufen", um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
6. Wiederholen Sie die Schritte 3 bis 6, um weitere Web App Firewall-Richtlinien hinzuzufügen, die Sie global binden möchten.
7. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich gebunden wurde.

Manuelle Konfiguration Mithilfe der Befehlszeilenschnittstelle

May 11, 2023

> **Hinweis:**
>
> Wenn Sie die Web App Firewall-Funktion manuell konfigurieren müssen, empfiehlt Citrix, das NetScaler-GUI-Verfahren zu verwenden.

Sie können die Web App Firewall Funktionen über die **NetScaler** Befehlszeilenschnittstelle konfigurieren. Es gibt jedoch wichtige Ausnahmen. Sie können Signaturen nicht über die Befehlszeilenschnittstelle aktivieren. Es gibt rund 1.000 Standardsignaturen in sieben Kategorien, und die Aufgabe ist für die Befehlszeilenschnittstelle zu komplex. Sie können Funktionen über die Befehlszeile aktivieren oder deaktivieren und Parameter konfigurieren, manuelle Lockerungen können jedoch nicht konfiguriert werden. Sie können die Funktion für adaptives Lernen zwar über die Befehlszeile konfigurieren und das Lernen aktivieren, aber Sie können erlernte Lockerungen oder erlernte Regeln nicht überprüfen und genehmigen oder überspringen. Die Befehlszeilenschnittstelle richtet sich an fortgeschrittene Benutzer, die mit der Verwendung der NetScaler-Appliance und der Web App Firewall vertraut sind.

Um die Web App Firewall mithilfe der NetScaler-Befehlszeile manuell zu konfigurieren, melden Sie

sich mit einem Telnet- oder Secure Shell-Client Ihrer Wahl an der NetScaler-Befehlszeile an.

So erstellen Sie ein Profil mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw profile <name> [-defaults ( basic | advanced )]`
- `set appfw profile <name> -type ( HTML | XML | HTML XML )`
- `save ns config`

Beispiel

Im folgenden Beispiel wird ein Profil mit dem Namen pr-basic mit grundlegenden Standardeinstellungen hinzugefügt und einen Profiltyp von HTML zugewiesen. Dies ist die geeignete Erstkonfiguration für ein Profil zum Schutz einer HTML-Website.

```
1 add appfw profile pr-basic -defaults basic
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

So konfigurieren Sie ein Profil mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> <arg1> [<arg2> ...]` wobei `<arg1>` einen Parameter darstellt und `<arg2>` entweder einen anderen Parameter oder den Wert darstellt, der dem Parameter zugewiesen werden soll, der durch `<arg1>` gekennzeichnet ist. Eine Beschreibung der Parameter, die beim Konfigurieren bestimmter Sicherheitsprüfungen verwendet werden sollen, finden Sie unter Erweiterter Schutz und dessen Unterthemen. Beschreibungen der anderen Parameter finden Sie unter Parameter zum Erstellen eines Profils.
- `save ns config`

Beispiel

Das folgende Beispiel zeigt, wie Sie ein mit grundlegenden Standardeinstellungen erstelltes HTML-Profil konfigurieren, um mit dem Schutz einer einfachen HTML-basierten Website zu beginnen. In diesem Beispiel werden die Protokollierung und Verwaltung von Statistiken für die meisten Sicherheitsprüfungen aktiviert, das Blockieren wird jedoch nur für die Prüfungen aktiviert, die eine niedrige Falsch-Positiv-Rate aufweisen und keine spezielle Konfiguration erfordern. Es aktiviert auch die Transformation von unsicherem HTML und unsicherem SQL, wodurch Angriffe verhindert werden, Anfragen

an Ihre Websites jedoch nicht blockiert werden. Wenn Protokollierung und Statistik aktiviert sind, können Sie die Protokolle später überprüfen, um festzustellen, ob Sie das Blockieren für eine bestimmte Sicherheitsüberprüfung aktivieren möchten.

```
set appfw profile -startURLAction log stats
set appfw profile -denyURLAction block log stats
set appfw profile -cookieConsistencyAction log stats
set appfw profile -crossSiteScriptingAction log stats
set appfw profile -crossSiteScriptingTransformUnsafeHTML ON
set appfw profile -fieldConsistencyAction log stats
set appfw profile -SQLInjectionAction log stats
set appfw profile -SQLInjectionTransformSpecialChars ON
set appfw profile -SQLInjectionOnlyCheckFieldsWithSQLChars ON
set appfw profile -SQLInjectionParseComments checkall
set appfw profile -fieldFormatAction log stats
set appfw profile -bufferOverflowAction block log stats
set appfw profile -CSRFtagAction log stats
save ns config
<!--NeedCopy-->
```

Um eine Richtlinie zu erstellen und zu konfigurieren

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw policy <name> <rule> <profile>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird eine Richtlinie mit dem Namen pl-blog mit einer Regel hinzugefügt, die den gesamten Datenverkehr zum oder vom Host blog.example.com abfängt und diese Richtlinie dem Profil pr-Blog zuordnet.

```
add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
    ")" pr-blog
<!--NeedCopy-->
```

So binden Sie eine Web App Firewall-Richtlinie

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw global <policyName> <priority>`
- `save ns config`

Beispiel

Das folgende Beispiel bindet die Richtlinie mit dem Namen pl-blog und weist ihr die Priorität 10 zu.

```
bind appfw global pl-blog 10
save ns config
<!--NeedCopy-->
```

So konfigurieren Sie das Sitzungslimit pro PE

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw settings <session limit>`

Beispiel

Im folgenden Beispiel wird das Sitzungslimit pro PE konfiguriert.

```
> set appfw settings -sessionLimit 500000`

Done

Default value:100000   Max value:500000 per PE
<!--NeedCopy-->
```

Signaturen

May 11, 2023

Die Web App Firewall-Signaturen bieten spezifische, konfigurierbare Regeln, um den Schutz Ihrer Websites vor bekannten Angriffen zu vereinfachen. Eine Signatur stellt ein Muster dar, das eine Komponente eines bekannten Angriffs auf ein Betriebssystem, einen Webserver, eine Website, einen XML-basierten Webdienst oder eine andere Ressource ist. Ein umfangreicher Satz vorkonfigurierter, integrierter oder nativer Regeln der Web App Firewall bietet eine benutzerfreundliche Sicherheitslösung, die die Leistungsfähigkeit des Pattern-Matchings nutzt, um Angriffe zu erkennen und vor Anwendungsschwachstellen zu schützen.

Sie können Ihre eigenen Signaturen erstellen oder Signaturen in den integrierten Vorlagen verwenden. Die Web App Firewall verfügt über zwei integrierte Vorlagen:

- **Standardsignaturen**: Diese Vorlage enthält eine vorkonfigurierte Liste mit über 1.300 Signaturen sowie eine vollständige Liste von SQL-Injection-Schlüsselwörtern, SQL-Spezialzeichenfolgen,

SQL-Transformregeln und SQL-Platzzeichen. Es enthält auch abgelehnte Muster für siteübergreifende Skripterstellung sowie zulässige Attribute und Tags für siteübergreifende Skripterstellung. Dies ist eine schreibgeschützte Vorlage. Sie können den Inhalt anzeigen, aber Sie können in dieser Vorlage nichts hinzufügen, bearbeiten oder löschen. Um es zu verwenden, müssen Sie eine Kopie erstellen. In Ihrer eigenen Kopie können Sie die Signaturregeln aktivieren, die Sie auf Ihren Datenverkehr anwenden möchten, und die Aktionen angeben, die ausgeführt werden sollen, wenn die Signaturregeln dem Datenverkehr entsprechen.

Die Web App Firewall-Signaturen stammen aus den von Snortveröffentlichten Regeln, einem Open-Source-Einbruchschutzsystem, das Echtzeit-Verkehrsanalysen durchführen kann, um verschiedene Angriffe und Prüfungen zu erkennen.

- ***Xpath Injection Patterns**: Diese Vorlage enthält einen vorkonfigurierten Satz von Literal- und PCRE-Schlüsselwörtern sowie speziellen Zeichenketten, die zur Erkennung von XPath-Injektionsangriffen (XML Path Language) verwendet werden.

Leere Signaturen: Sie können nicht nur eine Kopie der integrierten Vorlage *Standardsignaturen erstellen, sondern auch eine leere Signaturvorlage verwenden, um ein Signaturobjekt zu erstellen. Das Signaturobjekt, das Sie mit der Option für leere Signaturen erstellen, hat keine systemeigenen Signaturregeln, verfügt aber, genau wie das *Default-Template, über alle integrierten SQL/Cross-Site Scripting-Entitäten.

Signaturen im externen Format: Die Web App Firewall unterstützt auch Signaturen im externen Format. Sie können den Scanbericht eines Drittanbieters mithilfe der XSLT-Dateien importieren, die von der NetScaler Web App Firewall unterstützt werden. Für die folgenden Scan-Tools steht eine Reihe integrierter XSLT-Dateien zur Verfügung, um Dateien im externen Format in das native Format zu übersetzen:

- Cenzic
- Tiefgehende Sicherheit für Web-Apps
- IBM AppScan Enterprise
- IBM AppScan Standard.
- Qualys
- Qualys Cloud
- Weißer Hat
- Hewlett Packard Enterprise WebInspect
- Rapid7 Appspider
- Acunetix

Sicherheitsschutz für Ihre Anwendung

Strengere Sicherheitsvorkehrungen erhöhen den Verarbeitungsaufwand. Signaturen bieten die folgenden Bereitstellungsoptionen, mit denen Sie den Schutz Ihrer Anwendungen optimieren können:

- **Negatives Sicherheitsmodell**: Beim negativen Sicherheitsmodell verwenden Sie eine Vielzahl vorkonfigurierter Signaturregeln, um die Leistungsfähigkeit des Musterabgleichs anzuwenden, um Angriffe zu erkennen und sich vor Anwendungsschwachstellen zu schützen. Du blockierst nur das, was du nicht willst und erlaubst den Rest. Sie können Ihre eigenen Signaturregeln hinzufügen, die auf den spezifischen Sicherheitsanforderungen Ihrer Anwendungen basieren, um Ihre eigenen maßgeschneiderten Sicherheitslösungen zu entwerfen.
- **Hybrides Sicherheitsmodell**: Zusätzlich zur Verwendung von Signaturen können Sie positive Sicherheitsprüfungen verwenden, um eine Konfiguration zu erstellen, die ideal für Ihre Anwendungen geeignet ist. Verwenden Sie Signaturen, um Dinge zu blockieren, die Sie nicht möchten, und setzen Sie positive Sicherheitsprüfungen ein, um durchzusetzen, was erlaubt ist.

Um Ihre Anwendung mithilfe von Signaturen zu schützen, müssen Sie ein oder mehrere Profile für die Verwendung Ihres Signaturobjekts konfigurieren. In einer hybriden Sicherheitskonfiguration werden die SQL-Injection- und Cross-Site-Scripting-Muster sowie die SQL-Transformationsregeln in Ihrem Signaturobjekt nicht nur von den Signaturregeln verwendet, sondern auch von den positiven Sicherheitsprüfungen, die im Web App Firewall-Profil konfiguriert sind, das das Signaturobjekt verwendet, konfiguriert sind.

Die Web App Firewall untersucht den Datenverkehr zu Ihren geschützten Websites und Webdiensten, um Datenverkehr zu erkennen, der einer Signatur entspricht. Eine Übereinstimmung wird nur ausgelöst, wenn jedes Muster in der Regel mit dem Datenverkehr übereinstimmt. Wenn eine Übereinstimmung auftritt, werden die angegebenen Aktionen für die Regel aufgerufen. Sie können eine Fehlerseite oder ein Fehlerobjekt anzeigen, wenn eine Anfrage blockiert wird. Protokollnachrichten können Ihnen helfen, Angriffe zu identifizieren, die gegen Ihre Anwendung gestartet werden. Wenn Sie Statistiken aktivieren, speichert die Web App Firewall Daten über Anfragen, die einer Web App Firewall-Signatur oder Sicherheitsüberprüfung entsprechen.

Wenn der Datenverkehr sowohl mit einer Signatur als auch mit einer positiven Sicherheitsprüfung übereinstimmt, werden die restriktiveren der beiden Aktionen durchgesetzt. Wenn beispielsweise eine Anforderung mit einer Signaturregel übereinstimmt, für die die Blockaktion deaktiviert ist, aber die Anforderung auch mit einer positiven SQL Injection Sicherheitsprüfung übereinstimmt, für die die Aktion blockiert ist, wird die Anforderung blockiert. In diesem Fall wird die Signaturverletzung möglicherweise protokolliert `<not blocked>`, obwohl die Anfrage durch die SQL-Injection-Prüfung blockiert wird.

Anpassung: Bei Bedarf können Sie einem Signaturobjekt Ihre eigenen Regeln hinzufügen. Sie können auch die SQL/Cross-Site-Scripting-Muster anpassen. Die Option, basierend auf den spezifischen Sicherheitsanforderungen Ihrer Anwendungen eigene Signaturregeln hinzuzufügen, gibt Ihnen die Flexibilität, Ihre eigenen benutzerdefinierten Sicherheitslösungen zu entwickeln. Du blockierst nur das, was du nicht willst und erlaubst den Rest. Ein bestimmtes Fast-Match-Muster an einem bestimmten Ort kann den Verarbeitungsaufwand erheblich reduzieren, um die Leistung zu optimieren. Sie können SQL-Injection- und Cross-Site-Scripting-Muster hinzufügen, ändern oder entfernen. Inte-

grierte RegEx- und Expression-Editoren helfen Ihnen dabei, Ihre Muster zu konfigurieren und deren Richtigkeit zu überprüfen.

Automatische Aktualisierung: Sie können das Signaturobjekt manuell aktualisieren, um die neuesten Signaturregeln zu erhalten, oder Sie können die automatische Aktualisierungsfunktion anwenden, sodass die Web App Firewall die Signaturen automatisch über den cloudbasierten Web App Firewall-Aktualisierungsdienst aktualisieren kann.

> **Hinweis:**
>
> Wenn bei der automatischen Aktualisierung neue Signaturregeln hinzugefügt werden, sind sie standardmäßig deaktiviert. Sie müssen die aktualisierten Signaturen regelmäßig überprüfen und die neu hinzugefügten Regeln aktivieren, die für den Schutz Ihrer Anwendungen relevant sind.
>
> Sie müssen CORS so konfigurieren, dass Signaturen auf IIS-Servern gehostet werden.
>
> Die Funktion zur automatischen Signaturaktualisierung funktioniert auf dem lokalen Webserver nicht, wenn Sie über die NetScaler-GUI auf die URL zugreifen.

Erste Schritte

Die Verwendung von Citrix-Signaturen zum Schutz Ihrer Anwendung ist einfach und kann in wenigen einfachen Schritten durchgeführt werden:

1. Fügen Sie ein Signaturobjekt hinzu.
   - Sie können den Assistenten verwenden, der Sie auffordert, die gesamte Web App Firewall-Konfiguration zu erstellen, einschließlich des Hinzufügens des Profils und der Richtlinie, der Auswahl und Aktivierung von Signaturen und der Angabe von Aktionen für Signaturen und positive Sicherheitsprüfungen. Das Signaturobjekt wird automatisch erstellt.
   - Sie können eine Kopie des Signaturobjekts aus der Vorlage *Standardsignaturen erstellen, eine leere Vorlage verwenden, um eine Signatur mit Ihren eigenen benutzerdefinierten Regeln zu erstellen, oder eine externe Formatsignatur hinzufügen. Aktivieren Sie die Regeln und konfigurieren Sie die Aktionen, die Sie anwenden möchten.
1. Konfigurieren Sie das Web App Firewall-Zielprofil für die Verwendung dieses Signaturobjekts.
2. Senden Sie Traffic, um die Funktionalität zu überprüfen

Highlights

- Das Objekt Standardsignaturen ist eine Vorlage. Es kann nicht bearbeitet oder gelöscht werden. Um es zu verwenden, müssen Sie eine Kopie erstellen. In Ihrer eigenen Kopie können Sie

die Regeln und die gewünschte Aktion für jede Regel aktivieren, wie es für Ihre Anwendung erforderlich ist. Um die Anwendung zu schützen, müssen Sie das Zielprofil so konfigurieren, dass es diese Signatur verwendet.

- Die Verarbeitung von Signaturmustern ist mit Aufwand verbunden. Versuchen Sie, nur die Signaturen zu aktivieren, die für den Schutz Ihrer Anwendung geeignet sind, anstatt alle Signaturregeln zu aktivieren.
- Jedes Muster in der Regel muss übereinstimmen, um eine Signaturübereinstimmung auszulösen.
- Sie können Ihre eigenen benutzerdefinierten Regeln hinzufügen, um eingehende Anfragen zu überprüfen und verschiedene Arten von Angriffen zu erkennen, z. B. SQL-Injection oder Cross-Site-Scripting-Angriffe. Sie können auch Regeln hinzufügen, um die Antworten zu überprüfen, um das Durchsickern vertraulicher Informationen wie Kreditkartennummern zu erkennen und zu blockieren.
- Sie können eine Kopie eines vorhandenen Signaturobjekts erstellen und es anpassen, indem Sie Regeln und SQL-/Cross-Site-Scripting-Muster hinzufügen oder bearbeiten, um eine andere Anwendung zu schützen.
- Sie können die automatische Aktualisierung verwenden, um die neueste Version der Web App Firewall-Standardregeln herunterzuladen, ohne dass eine kontinuierliche Überwachung erforderlich ist, um die Verfügbarkeit des neuen Updates zu überprüfen.
- Ein Signaturobjekt kann von mehr als einem Profil verwendet werden. Auch nachdem Sie ein oder mehrere Profile für die Verwendung eines Signaturobjekts konfiguriert haben, können Sie Signaturen weiterhin aktivieren oder deaktivieren oder die Aktionseinstellungen ändern. Sie können Ihre eigenen benutzerdefinierten Signaturregeln manuell erstellen und ändern. Die Änderungen gelten für alle Profile, die derzeit für die Verwendung dieses Signaturobjekts konfiguriert sind.
- Sie können Signaturen konfigurieren, um Verstöße in verschiedenen Arten von Payloads wie HTML, XML, JSON und GWT zu erkennen.
- Sie können ein konfiguriertes Signaturobjekt exportieren und in eine andere NetScaler-Appliance importieren, um Ihre benutzerdefinierten Signaturregeln einfach zu replizieren.

Signaturen sind Muster, die mit einer bekannten Sicherheitslücke in Verbindung stehen. Mithilfe des Signaturschutzes können Sie den Datenverkehr identifizieren, der versucht, diese Sicherheitsanfälligkeiten auszunutzen, und spezifische Maßnahmen ergreifen.

Signaturen sind in Kategorien unterteilt. Sie können die Leistung optimieren und den Verarbeitungsaufwand reduzieren, indem Sie nur die Regeln in den Kategorien aktivieren, die zum Schutz Ihrer Anwendung geeignet sind.

Manuelles Konfigurieren des Signatur-Features

August 19, 2021

Um Signaturen zum Schutz Ihrer Websites zu verwenden, müssen Sie die Regeln überprüfen und diejenigen aktivieren und konfigurieren, die Sie anwenden möchten. Die Regeln sind standardmäßig deaktiviert. Citrix empfiehlt, dass Sie alle Regeln aktivieren, die für die Art des Inhalts gelten, den Ihre Website verwendet.

Um die Signaturfunktion manuell zu konfigurieren, verwenden Sie einen Browser, um eine Verbindung mit der GUI herzustellen. Erstellen Sie dann ein Signaturobjekt aus einer integrierten Vorlage, einem vorhandenen Signaturobjekt oder durch Importieren einer Datei. Konfigurieren Sie als Nächstes das neue Signatures-Objekt wie unter Konfigurieren oder Ändern eines Signatures-Objektsbeschrieben.

Hinzufügen oder Entfernen eines Signaturobjekts

May 11, 2023

Sie können der Web App Firewall ein neues Signaturobjekt hinzufügen, indem Sie:

- Eine eingebaute Vorlage kopieren.
- Kopieren eines vorhandenen Signaturobjekts.
- Importieren eines Signaturobjekts aus einer externen Datei.

Die Signaturdatei enthält die CPU-Auslastung, das letzte anwendbare Jahr und Details zum Schweregrad. Sie können die CPU-Auslastung, das letzte Jahr und den CVE-Schweregrad jedes Mal sehen, wenn eine Signaturdatei regelmäßig geändert und hochgeladen wird. Nachdem Sie diese Werte beobachtet haben, können Sie entscheiden, ob Sie die Signatur auf der Appliance aktivieren oder deaktivieren möchten.

Sie müssen die GUI verwenden, um eine Vorlage oder ein vorhandenes Signaturobjekt zu kopieren. Sie können entweder die GUI oder die Befehlszeile verwenden, um ein Signaturobjekt zu importieren. Sie können auch entweder die GUI oder die Befehlszeile verwenden, um ein Signaturobjekt zu entfernen.

So erstellen Sie ein Signaturobjekt aus einer Vorlage

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie als Vorlage verwenden möchten.

   Ihre Auswahlmöglichkeiten:

- **Standardsignaturen.** Enthält die Signaturregeln, die SQL-Einschleusungsregeln und die Cross-Site-Scripting-Regeln.
- **XPath-Einschleusung.** Enthält die XPath-Einschleusungsmuster.
- **Jedes vorhandene Signaturobjekt.**

> **Achtung:**
>
> Wenn Sie keinen Signaturtyp wählen, der als Vorlage verwendet werden soll, werden Sie von der Web App Firewall aufgefordert, Signaturen von Grund auf neu zu erstellen.

3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie im Dialogfeld Signaturobjekt hinzufügen einen Namen für das neue Signaturobjekt ein, und klicken Sie dann auf OK. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrichsymbol beginnen und aus einem bis 31 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), bei (@), gleich (=) und Unterstrichen (_) bestehen.
5. Klicken Sie auf **Schließen**.

So erstellen Sie ein Signaturobjekt durch Importieren einer Datei

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Wählen **Sie im Dialogfeld Signaturen-Objekt hinzufügen** das Format der Signaturen aus, die Sie importieren möchten.
   - Um eine Signaturdatei im NetScaler-Format zu importieren, wählen Sie die Registerkarte **Natives Format** .
   - Um eine Datei im externen Signaturformat zu importieren, wählen Sie die Registerkarte **Externes Format** .
4. Wählen Sie die Datei aus, die Sie zum Erstellen Ihres Signaturobjekts verwenden möchten.
   - Um eine native Signaturdatei im NetScaler-Format zu importieren, wählen Sie im Abschnitt Importieren entweder Aus lokaler Datei importieren oder Aus URL importieren aus, und geben Sie dann den Pfad oder die URL der Datei ein oder navigieren Sie zu ihm.
   - Um eine Datei im Format Cenzic, IBM AppScan, Qualys oder Whitehat zu importieren, wählen Sie im Abschnitt XSLT die Option Integrierte XSLT-Datei verwenden, Lokale Datei verwenden oder Referenz von URL aus. Wenn Sie als Nächstes Integrierte XSLT-Datei verwenden gewählt haben, wählen Sie das entsprechende Dateiformat aus der Liste aus. Wenn Sie Lokale Datei oder Referenz von URL verwenden ausgewählt haben, geben Sie den Pfad oder die URL zur Datei ein oder navigieren Sie zu ihm.
5. Klicken Sie auf **Hinzufügen**und dann auf **Schließen**.

So erstellen Sie ein Signaturobjekt durch Importieren einer Datei mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite] [-merge] [-sha1 <string>]`
- `save ns config`

Beispiel #1

Im folgenden Beispiel wird ein Signaturobjekt aus einer Datei mit dem Namen signatures.xml erstellt und ihm den Namen mySignatures zugewiesen.

```
import appfw signatures local:signatures.xml MySignatures
save ns config
<!--NeedCopy-->
```

So fügen Sie einzelne Signaturen mithilfe der CLI hinzu

Sie können Signaturen anhand ihrer IDs oder Kategorie auswählen und dann Aktionen festlegen. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
import appfw signature <source> <name> [-sigRuleId| -sigCategory] [Rule-IDs | Category name] -Enabled [ON | OFF] [-Action LOG BLOCK]
<!--NeedCopy-->
```

- **Beispiele für die Verwendung von Signatur-IDs**

  Das folgende Beispiel aktiviert die Signaturen anhand ihrer Regel-IDs und legt die Protokoll- und Blockaktionen fest:

  ```
  import appfw signature DEFAULT object_name -sigRuleId 1001 9882 2000 1250 810 -Enabled ON -Action LOG BLOCK
  <!--NeedCopy-->
  ```

  Im folgenden Beispiel wird die Signatur anhand ihrer ID hinzugefügt, ohne sie zu aktivieren:

  ```
  import appfw signature DEFAULT object_name -sigRuleId 810 -Enabled OFF
  <!--NeedCopy-->
  ```

- **Beispiele für die Verwendung der Signaturkategorie**

Das folgende Beispiel aktiviert die Signaturen nach `web-misc` Kategorie und legt die Protokoll- und Blockaktionen fest:

```
1 import appfw signature DEFAULT object_name -sigCategory web-misc
     -Enabled ON -Action LOG BLOCK
2 <!--NeedCopy-->
```

Im folgenden Beispiel werden die Signaturen nach `web-misc` Kategorie hinzugefügt, ohne sie zu aktivieren:

```
1 import appfw signature DEFAULT object_name -sigCategory web-misc
     -Enabled OFF
2 <!--NeedCopy-->
```

So entfernen Sie ein Signaturobjekt mit der GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie entfernen möchten.
3. Klicken Sie auf **Entfernen**.

So entfernen Sie ein Signatures-Objekt mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appfw signatures <name>`
- `save ns config`

Konfiguration oder Änderung eines Signaturobjekts

June 19, 2023

Sie konfigurieren ein Signaturobjekt, nachdem Sie es erstellt haben, oder ändern ein vorhandenes Signaturobjekt, um Signaturkategorien oder bestimmte Signaturen zu aktivieren oder zu deaktivieren, und konfigurieren, wie die Web App Firewall reagiert, wenn eine Signatur mit einer Verbindung übereinstimmt.

Um ein Signaturobjekt zu konfigurieren oder zu ändern

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.

2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Stellen **Sie im Dialogfeld „Signaturobjekt ändern** “ links die Optionen „ **Filterkriterien** anzeigen“ ein, um die Filterelemente anzuzeigen, die Sie konfigurieren möchten.

   Wenn Sie diese Optionen ändern, werden die von Ihnen angeforderten Ergebnisse im Fenster Gefilterte Ergebnisse auf der rechten Seite angezeigt.

   - Um nur ausgewählte Signaturkategorien anzuzeigen, aktivieren oder deaktivieren Sie die entsprechenden Kontrollkästchen für die Signaturkategorie. Ab Version 13.1 Build 48.x können Sie CVE im linken Bereich verwenden, um sich die für das ausgewählte Jahr veröffentlichten Sicherheitslücken anzusehen.
     Die Signaturkategorien sind:

Name	Art des Angriffs, vor dem diese Signatur schützt
cgi	CGI-Skripts. Enthält Perl- und UNIX-Shell-Skripts.
Auftraggeber	Browser und andere Clients.
kalte Fusion	Websites, die den Adobe Systems ColdFusion-Anwendungsserver verwenden.
Titelseite	Websites, die den FrontPage-Server von Microsoft verwenden.
iis	Websites, die den Microsoft Internet Information Server (IIS) verwenden.
sonstig	Verschiedene Angriffe.
php	Websites, die PHP verwenden
Web-ActiveX	Websites, die ActiveX-Steuerelemente enthalten.
Web-Struts	Websites, die Apache Struts enthalten, bei denen es sich um Java-EE-basierte Applets handelt.
CVE	Listet die CVEs auf, die für das ausgewählte Jahr veröffentlicht wurden.

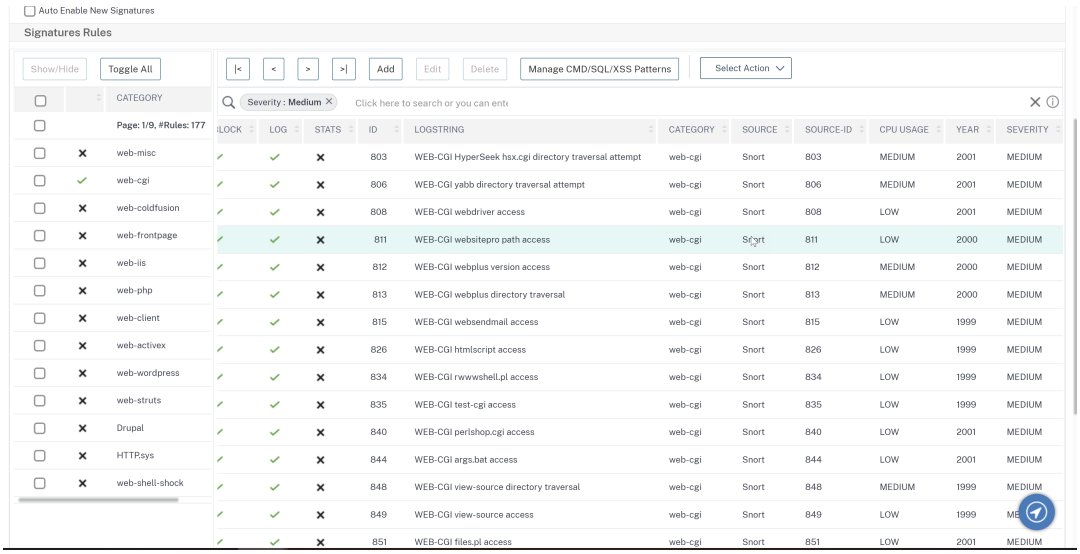
   - Um nur Signaturen anzuzeigen, für die bestimmte Prüfaktionen aktiviert sind, aktivieren Sie das Kontrollkästchen ON für jede dieser Aktionen, deaktivieren Sie die Kontrollkästchen ON für die anderen Aktionen und deaktivieren Sie alle Kontrollkästchen

AUS. Um nur Signaturen anzuzeigen, für die eine bestimmte Prüfaktion deaktiviert ist, aktivieren Sie die entsprechenden Kontrollkästchen aus und deaktivieren Sie alle aktivierten Kontrollkästchen. Um Signaturen unabhängig davon anzuzeigen, ob für sie eine Prüfaktion aktiviert oder deaktiviert ist, aktivieren oder deaktivieren Sie die Kontrollkästchen EIN und AUS für diese Aktion. Die Überprüfungsaktionen sind:

Kriterium	Beschreibung
Aktiviert	Die Signatur ist aktiviert. Die Web App Firewall sucht nur nach Signaturen, die bei der Verarbeitung des Datenverkehrs aktiviert sind.
Blockieren	Verbindungen, die dieser Signatur entsprechen, werden blockiert.
Protokoll	Für jede Verbindung, die dieser Signatur entspricht, wird ein Protokolleintrag erstellt.
Statistiken	Die Web App Firewall nimmt jede Verbindung, die dieser Signatur entspricht, in die Statistiken auf, die sie für diese Prüfung generiert.

- Um die im Ergebnisfenster angezeigten Details weiter zu filtern, verwenden Sie die Suchleiste über dem Ergebnisfenster. Wählen Sie in der Suchleiste die Eigenschaften aus, die Sie filtern möchten, geben Sie den Wert ein und drücken Sie die Eingabetaste. Es filtert weiter den Inhalt, der bereits im Ergebnisfenster angezeigt wird, und listet die Details auf der Grundlage des eingegebenen Werts auf.

  Beispiel: In der folgenden Abbildung ist Web-CGI in den Optionen „Filterkriterien anzeigen“ auf der linken Seite als Kategorie ausgewählt. Die Details der Web-CGI-Signatur sind im Ergebnisfenster auf der rechten Seite aufgeführt. Um die Details anhand des Schweregrads weiter zu filtern, wird in der Suchleiste der Schweregrad als Eigenschaft ausgewählt und als Wert Medium eingegeben. Die Web-CGI-Signaturen mit mittlerem Schweregrad werden im Ergebnisfenster aufgeführt.



- Um alle Anzeigefilterkriterien auf die Standardeinstellungen zurückzusetzen und alle Signaturen anzuzeigen, klicken Sie auf Alle anzeigen.

> **Hinweis**
>
> Die Anzahl der im gefilterten Ergebnisfenster aufgelisteten Elemente beträgt 20. Die Paginierung ist links über den Optionen „Filterkriterien anzeigen“ verfügbar.

1. Um Informationen zu einer bestimmten Signatur zu erhalten, wählen Sie die Signatur aus und klicken Sie dann auf den blauen Doppelpfeil im Feld Mehr. Das Meldungsfeld Signature Rule Vulnerability Detail wird angezeigt. Es enthält Informationen über den Zweck der Signatur und enthält Links zu externen webbasierten Informationen über die Sicherheitslücke oder Sicherheitslücken, die diese Signatur behebt. Um auf einen externen Link zuzugreifen, klicken Sie auf den blauen Doppelpfeil links neben der Beschreibung dieses Links.
2. Konfigurieren Sie die Einstellungen für eine Signatur, indem Sie die entsprechenden Kontrollkästchen aktivieren.
3. Wenn Sie dem Signature-Objekt eine lokale Signaturregel hinzufügen oder eine vorhandene lokale Signaturregel ändern möchten, lesen Sie den Signatur-Editor.
4. Wenn Sie keine SQL-Injection, siteübergreifendes Skripting oder Xpath-Injectionsmuster benötigen, klicken Sie auf OK, und klicken Sie dann auf Schließen. Andernfalls klicken Sie in der unteren linken Ecke des Detailfensters auf SQL/Cross-Site Scripting Patterns verwalten.
5. Navigieren Sie im Dialogfeld SQL/Cross-Site-Skriptmuster verwalten im Fenster Gefilterte Ergebnisse zu der Musterkategorie und dem Muster, die Sie konfigurieren möchten. Informationen zu den SQL-Einschleusungsmustern finden Sie unter HTML SQL Injection Check. Informationen zu den Cross-Site-Skriptmustern finden Sie unter HTML Cross-Site Scripting Check.
6. So fügen Sie ein neues Muster hinzu:

a) Wählen Sie den Zweig aus, zu dem Sie das neue Muster hinzufügen möchten.
b) Klicken Sie direkt unter dem unteren Bereich des Fensters **Gefilterte Ergebnisse** auf die Schaltfläche **Hinzufügen** .
c) Füllen Sie im Dialogfeld Signaturelement erstellen das Textfeld Element mit dem Muster aus, das Sie hinzufügen möchten. Wenn Sie dem Zweig der Transformationsregeln ein Transformationsmuster hinzufügen, füllen Sie unter Elemente das Textfeld Von mit dem Muster aus, das Sie ändern möchten, und das Textfeld Bis mit dem Muster, in das Sie das vorherige Muster ändern möchten.
d) Klicken Sie auf **OK**.

7. Um ein vorhandenes Muster zu ändern:

a) Wählen Sie im Fenster **Gefilterte Ergebnisse** den Zweig aus, der das Muster enthält, das Sie ändern möchten.
b) Wählen Sie im Detailfenster unter dem Fenster **Gefilterte Ergebnisse** das Muster aus, das Sie ändern möchten.
c) Klicken Sie auf **Ändern**.
d) Ändern Sie im Dialogfeld **Signaturelement ändern** im Textfeld **Element** das Muster. Wenn Sie ein Transformationsmuster ändern, können Sie eines oder beide Muster unter Elemente in den Textfeldern Von und Bis ändern.
e) Klicken Sie auf **OK**.

8. Um ein Muster zu entfernen, wählen Sie das Muster aus, das Sie entfernen möchten, und klicken Sie dann unter dem Detailbereich unter dem Fenster **Gefilterte Ergebnisse** auf die Schaltfläche **Entfernen** . Wenn Sie dazu aufgefordert werden, bestätigen Sie Ihre Auswahl, indem Sie auf **Schließen**klicken.

9. Um die Kategorie Patterns zum Cross-Site Scripting-Zweig hinzuzufügen, gehen Sie wie folgt vor:

a) Wählen Sie den Zweig aus, zu dem Sie die Musterkategorie hinzufügen möchten.

b) Klicken Sie direkt unter dem Fenster **Gefilterte Ergebnisse** auf die Schaltfläche **Hinzufügen** .

> **Hinweis:** Derzeit können Sie dem Cross-Site-Scripting-Zweig nur eine Kategorie, benannte Muster, hinzufügen. Nachdem Sie also auf **Hinzufügen**geklickt haben, müssen Sie die Standardauswahl akzeptieren, nämlich Muster.

c) Klicken Sie auf **OK**.

10. Um einen Zweig zu entfernen, wählen Sie diesen Zweig aus und klicken Sie dann direkt unter dem Fenster **Gefilterte Ergebnisse** auf die Schaltfläche Entfernen. Wenn Sie dazu aufgefordert werden, bestätigen Sie Ihre Auswahl, indem Sie auf **OK**klicken.

> **Hinweis:** Wenn Sie einen Standardzweig entfernen, entfernen Sie alle Muster in diesem Zweig. Dadurch können die Sicherheitsprüfungen, die diese Informationen verwenden, deaktiviert werden.

11. Wenn Sie mit der Änderung der SQL-Injection-, Cross-Site Scripting- und XPath-Injektionsmuster fertig sind, klicken Sie auf **OK**und dann auf **Schließen**, um zum Dialogfeld **Signaturobjekt ändern** zurückzukehren.
12. Klicken Sie zu einem beliebigen Zeitpunkt auf **OK**, um Ihre Änderungen zu speichern. Wenn Sie mit der Konfiguration des Signaturobjekts fertig sind, klicken Sie auf **Schließen**.

Schutz von JSON-Anwendungen mithilfe von Signaturen

May 11, 2023

JavaScript Object Notation (JSON) ist ein textbasierter offener Standard, der von der Skriptsprache JavaScript abgeleitet ist. JSON wird für die menschenlesbare Darstellung einfacher Datenstrukturen und assoziativer Arrays, sogenannter Objekte, bevorzugt. Es dient als Alternative zu XML und wird hauptsächlich zur Übertragung serialisierter Datenstrukturen für die Kommunikation mit Webanwendungen verwendet. Die JSON-Dateien werden normalerweise mit der Erweiterung.json gespeichert.

Die JSON-Payload wird normalerweise mit dem als **application/json**angegebenen MIME-Typ gesendet. Die anderen „Standard“ -Inhaltstypen für JSON sind:

- **Anwendung/X-Javascript**
- **Text/Javascript**
- **text/x-javascript**
- **text/x-json**

Verwendung der NetScaler Web App Firewall-Signaturen zum Schutz von JSON-Anwendungen

Um JSON-Anfragen zuzulassen, ist die Appliance mit dem JSON-Inhaltstyp vorkonfiguriert, wie in der folgenden show-Command-Ausgabe dargestellt:

```
> sh appfw jsonContentType
1)      JSONContenttypevalue:  "^application/json$" IsRegex:  REGEX
Done
<!--NeedCopy-->
```

Die NetScaler Web App Firewall verarbeitet den Beitragstext nur für die folgenden Inhaltstypen:

- **application/x-www-form-urlencoded**

- **multipart/form-data**
- **text/x-gwt-rpc**

Die Anfragen, die mit anderen Content-Type-Headern, einschließlich application/json (oder einem anderen zulässigen Inhaltstyp), eingehen, werden nach der Header-Prüfung an das Backend weitergeleitet. Der Posttext solcher Anfragen wird nicht auf Verstöße gegen die Sicherheitsüberprüfung überprüft, selbst wenn die Sicherheitsprüfungen des Profils wie SQL oder Cross-Site Scripting aktiviert sind.

Um JSON-Anwendungen zu schützen und Verstöße zu erkennen, können Web App Firewall-Signaturen verwendet werden. Alle Anfragen, die den erlaubten Content-Type-Header enthalten, werden von der Web App Firewall auf Signaturabgleich verarbeitet. Sie können Ihre eigenen benutzerdefinierten Signaturregeln zur Verarbeitung von JSON-Payloads hinzufügen, um verschiedene Sicherheitsprüfungen durchzuführen (z. B. Cross-Site Scripting, SQL und Field Consistency), um Verstöße in den Headern sowie im Beitragstext zu erkennen und bestimmte Maßnahmen zu ergreifen.

> **Tipp**
>
> Im Gegensatz zu den anderen integrierten Standardeinstellungen kann der vorkonfigurierte JSON-Inhaltstyp mithilfe der CLI oder der GUI (GUI) bearbeitet oder entfernt werden. Wenn legitime Anforderungen für JSON-Anwendungen blockiert werden und Inhaltstypverletzungen auslösen, überprüfen Sie, ob der Inhaltstypwert genau konfiguriert ist. Weitere Informationen darüber, wie Web App Firewall Content-Typ-Header verarbeitet, finden Sie unter Schutz von Inhaltstypen

So fügen Sie JSON-Inhaltstyp mit der Befehlszeilenschnittstelle hinzu oder entfernen Sie sie

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add appfw jsonContentType ^application/json$ IsRegEx REGEX
```

```
rm appfw JSONContentType "^application/json$"
```

So verwalten Sie JSON-Inhaltstypen mithilfe der GUI

Navigieren Sie zu **Sicherheit** > **Web App Firewall** und wählen Sie im Abschnitt **Einstellungen** die Option **JSON-Inhaltstypen verwalten**aus.

Fügen Sie im Fenster **JSONWeb App Firewall Inhaltstyp konfigurieren** JSON-Inhaltstypen hinzu, bearbeiten oder löschen Sie JSON-Inhaltstypen entsprechend den Anforderungen Ihrer Anwendungen.

Konfiguration des Signaturschutzes zur Erkennung von Angriffen in JSON-Payload

Zusätzlich zu einem gültigen JSON-Inhaltstyp müssen Sie Signaturen konfigurieren, um die Muster anzugeben, die, wenn sie in einer JSON-Anfrage erkannt werden, auf eine Sicherheitsverletzung hinweisen. Die angegebenen Aktionen, wie Blockieren und Protokollieren, werden ausgeführt, wenn eine eingehende Anforderung eine Übereinstimmung mit allen Zielmustern in der Signaturregel auslöst.

Um eine benutzerdefinierte Signaturregel hinzuzufügen, empfiehlt Citrix, die GUI zu verwenden. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall** > **Signaturen**. Doppelklicken Sie auf das Zielsignaturobjekt, um auf das Bedienfeld **Web App Firewall-Signaturen bearbeiten** zuzugreifen. Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Aktionen, die Kategorie, die Protokollzeichenfolge, die Regelmuster usw. zu konfigurieren. Die Web App Firewall überprüft zwar alle zulässigen Nutzdaten vom Inhaltstyp auf Signaturübereinstimmungen, Sie können die Verarbeitung jedoch optimieren, indem Sie den JSON-Ausdruck in der Regel angeben. Wenn Sie ein neues Regelmuster **hinzufügen**, wählen Sie in den Drop-down-Optionen für **Match** die Option **Ausdruck** aus und geben Sie den Ziel-Match-Ausdruck aus Ihrer JSON-Payload an, um die spezifischen Anfragen zu identifizieren, die überprüft werden müssen. Ein Ausdruck muss mit einem **TEXT** beginnen. Präfix. Sie können weitere Regelmuster hinzufügen, um zusätzliche Übereinstimmungsmuster zur Identifizierung des Angriffs festzulegen.

Das folgende Beispiel zeigt eine Signaturregel. Wenn im POST-Text der JSON-Payload ein seitenübergreifendes Skript-Tag erkannt wird, das dem angegebenen XPATH_JSON-Ausdruck entspricht, wird eine Signaturübereinstimmung ausgelöst.

Beispiel für eine Signatur zur Erkennung von Cross-Site Scripting in JSON-Payload

```
<SignatureRule actions="log,stats" category="JSON" enabled="ON" id="
    1000001" severity="" source="" type="" version="1">

  <PatternList>

    <RequestPatterns>

      <Pattern>

        <Location area="HTTP_POST_BODY"/>

        <Match type="Expression">TEXT.XPATH_JSON(xp%/glossary/title%).
            CONTAINS("example glossary")</Match>

      </Pattern>

      <Pattern>
```



```
16
17          <Location area="HTTP_METHOD"/>
18
19          <Match type="LITERAL">POST</Match>
20
21        </Pattern>
22
23        <Pattern>
24
25          <Location area="HTTP_POST_BODY"/>
26
27          <Match type="CrossSiteScripting"/>
28
29         </Pattern>
30
31      </RequestPatterns>
32
33    </PatternList>
34
35    <LogString>Cross-site scripting violation detected in json payload</
        LogString>
36
37    <Comment/>
38
39 </SignatureRule>
40 <!--NeedCopy-->
```

Beispiel für die Payload

Die folgende Payload löst den Signatur-Match aus, da sie das Cross-Site-Scripting-Tag <Gotcha!!>.

```
1 {
2  "glossary": {
3  "title": "example glossary","GlossDiv": {
4  "title": "S","GlossList": {
5  "GlossEntry": {
6  "ID": "SGML","SortAs": "SGML","GlossTerm": "Standard Generalized
      Markup Language","Acronym": "SGML","Abbrev": "ISO 8879:1986","
      GlossDef": {
7  "para": "A meta-markup language, used to create markup languages \*\*<
      Gotcha!!>\*\* such as DocBook.","GlossSeeAlso": ["GML", "XML"] }
8  ,"GlossSee": "markup" }
9   }
```



```
10    }
11    }
12    }
13
14 <!--NeedCopy-->
```

Beispiel für die Lognachricht

```
1 Aug 21 12:21:42 <local0.info> 10.217.31.239 08/21/2015:23:21:42 GMT ns
     0-PPE-1 : APPFW APPFW_SIGNATURE_MATCH 1471 0 :  10.217.253.62 990-
     PPE0 NtJnVMNnvPeQJnaUzXYW/GTvAQsA010 prof1 http://10.217.31.212/FFC/
     login_post.php Signature violation rule ID 1000001: cross-site
     scripting violation detected in json payload  <not blocked>
2 <!--NeedCopy-->
```

> **Hinweis**
>
> Wenn du dieselbe Payload sendest, nachdem du das Cross-Site-Script-Tag entfernt hast (**<Gotcha!!**>), der Signaturregelabgleich wird nicht ausgelöst.

Highlights

- Verwenden Sie Web App Firewall-Signaturen, um Cross-Site Scripting, SQL und andere Verstöße zu erkennen, um JSON-Payload zu schützen.
- Stellen Sie sicher, dass der JSON-Inhaltstyp auf der Appliance als zulässiger Inhaltstyp konfiguriert ist.
- Stellen Sie sicher, dass der Inhaltstyp in der Payload dem konfigurierten JSON-Inhaltstyp entspricht.
- Stellen Sie sicher, dass alle in der Signaturregel konfigurierten Muster übereinstimmen, damit die ausgelöste Signaturverletzung ausgelöst wird.
- Wenn Sie eine Signaturregel hinzufügen, MUSS sie mindestens ein Regelmuster haben, das dem Ausdruck in der JSON-Payload entspricht. Alle PI-Ausdrücke in Signaturregeln müssen mit dem Präfix TEXT. beginnen und vom Typ Boolean sein.

Schützen Sie Anwendungs- oder JSON-Inhaltstypen mit SQL- und Cross-Site-Scripting-kodierten Payloads mithilfe von Richtlinien und Signaturen

NetScaler Web App Firewall kann Anwendungs- oder JSON-Inhaltstypen mithilfe von Richtlinien und Signaturen schützen.

Überprüfen Sie den Anwendungs- oder JSON-Inhaltstyp auf SQL-Injection mithilfe von Richtlinien

Sie müssen die folgenden Richtlinien hinzufügen und sie global an den virtuellen Server binden, um SQL-Injection zu unterstützen.

```
add appfw policy sqli_1 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_])))(select|insert|delete|update|drop|create|alter|grant
|revoke|commit|rollback|shutdown|union|intersect|minus|case|decode|where
|group|begin|join|exists|distinct|add|modify|constraint|null|like|exec|
execute|char|or|and|sp_sdidebug)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK

add appfw policy sqli_2 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_])))(xp_availablemedia|xp_cmdshell|xp_deletemail|xp_dirtree
|xp_dropwebtask|xp_dsninfo|xp_enumdsn|xp_enumerrorlogs|xp_enumgroups|
xp_enumqueuedtasks|xp_eventlog|xp_findnextmsg|xp_fixeddrives|xp_getfiledetails
|xp_getnetname|xp_grantlogin|xp_logevent|xp_loginconfig|xp_logininfo|
xp_makewebtask|xp_msver|xp_regread|xp_perfend|xp_perfmonitor|xp_perfsample
|xp_perfstart|xp_readerrorlog|xp_readmail|xp_revokelogin|xp_runwebtask|
xp_schedulersignal|xp_sendmail|xp_servicecontrol|xp_snmp_getstate|xp_snmp_raisetrap
|xp_sprintf|xp_sqlinventory|xp_sqlregister|xp_sqltrace|xp_sscanf|xp_startmail
|xp_stopmail|xp_subdirs|xp_unc_to_drive)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK


add appfw policy sqli_3 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_])))(sysobjects|syscolumns|MSysACEs|MSysObjects|MSysQueries
|MSysRelationships)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK

add appfw policy sqli_4 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A
)|(?<=[^a-zA-Z0-9_])))(SYS\.USER_OBJECTS|SYS\.TAB|SYS\.USER_TABLES|SYS\.
USER_VIEWS|SYS\.ALL_TABLES|SYS\.USER_TAB_COLUMNS|SYS\.USER_CONSTRAINTS|SYS
\.USER_TRIGGERS|SYS\.USER_CATALOG|SYS\.ALL_CATALOG|SYS\.ALL_CONSTRAINTS|SYS
\.ALL_OBJECTS|SYS\.ALL_TAB_COLUMNS|SYS\.ALL_TAB_PRIVS|SYS\.ALL_TRIGGERS|SYS
\.ALL_USERS|SYS\.ALL_VIEWS|SYS\.USER_ROLE_PRIVS|SYS\.USER_SYS_PRIVS|SYS\.
USER_TAB_PRIVS)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```


Überprüfen des Anwendungs- oder JSON-Inhaltstyps mit Signaturen

Sie können dem Signaturobjekt im Anwendungsfirewallprofil die folgenden Signaturregeln hinzufügen, um die SQL-Injektion für den JSON-Inhaltstyp zu unterstützen.

> **Hinweis:**
>
> Post Body-Signaturen sind CPU-intensiv.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2013-2018 Citrix Systems, Inc. All rights reserved. -->
<SignaturesFile schema_version="6" version="0" minor_schema_version="0"
    >
     <Signatures>
         <SignatureRule id="4000000" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
                         <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#(((\A)
                            |(?<=[^a-zA-Z0-9_])))(select|insert|delete|
                            update|drop|create|alter|grant|revoke|commit
                            |rollback|shutdown|union|intersect|minus|
                            case|decode|where|group|begin|join|exists|
                            distinct|add|modify|constraint|null|like|
                            exec|execute|char|or|and|sp_sdidebug)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                     </Pattern>
                     <Pattern type="fastmatch">
                         <Location area="HTTP_METHOD"/>
                         <Match type="LITERAL">T</Match>
                     </Pattern>
                 </RequestPatterns>
             </PatternList>
             <LogString>sql Injection</LogString>
             <Comment/>
         </SignatureRule>
         <SignatureRule id="4000001" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
```



```
                    <Pattern>
                        <Location area="HTTP_POST_BODY"/>
                        <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                            |(?<=[^a-zA-Z0-9_]))(xp_availablemedia|
                            xp_cmdshell|xp_deletemail|xp_dirtree|
                            xp_dropwebtask|xp_dsninfo|xp_enumdsn|
                            xp_enumerrorlogs|xp_enumgroups|
                            xp_enumqueuedtasks|xp_eventlog|
                            xp_findnextmsg|xp_fixeddrives|
                            xp_getfiledetails|xp_getnetname|
                            xp_grantlogin|xp_logevent|xp_loginconfig|
                            xp_logininfo|xp_makewebtask|xp_msver|
                            xp_regread|xp_perfend|xp_perfmonitor|
                            xp_perfsample|xp_perfstart|xp_readerrorlog|
                            xp_readmail|xp_revokelogin|xp_runwebtask|
                            xp_schedulersignal|xp_sendmail|
                            xp_servicecontrol|xp_snmp_getstate|
                            xp_snmp_raisetrap|xp_sprintf|xp_sqlinventory
                            |xp_sqlregister|xp_sqltrace|xp_sscanf|
                            xp_startmail|xp_stopmail|xp_subdirs|
                            xp_unc_to_drive)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                    </Pattern>
                    <Pattern type="fastmatch">
                        <Location area="HTTP_METHOD"/>
                        <Match type="LITERAL">T</Match>
                    </Pattern>
                </RequestPatterns>
            </PatternList>
            <LogString>sql Injection</LogString>
            <Comment/>
        </SignatureRule>
        <SignatureRule id="4000002" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
            <PatternList>
                <RequestPatterns>
                    <Pattern>
                        <Location area="HTTP_POST_BODY"/>
                        <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                            |(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|
```



```
                                MSysACEs|MSysObjects|MSysQueries|
                                MSysRelationships)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                        </Pattern>
                        <Pattern type="fastmatch">
                            <Location area="HTTP_METHOD"/>
                            <Match type="LITERAL">T</Match>
                        </Pattern>
                    </RequestPatterns>
                </PatternList>
                <LogString>sql Injection</LogString>
                <Comment/>
            </SignatureRule>
            <SignatureRule id="4000003" enabled="ON" actions="log,block"
               category="sql" source="" severity="" type="" version="1"
               sourceid="" harmscore="">
                <PatternList>
                    <RequestPatterns>
                        <Pattern>
                            <Location area="HTTP_POST_BODY"/>
                            <Match type="Expression">TEXT.SET_TEXT_MODE(
                               IGNORECASE).SET_TEXT_MODE(URLENCODED).
                               DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                               |(?<=[^a-zA-Z0-9_]))(SYS.USER_OBJECTS|SYS.
                               TAB|SYS.USER_TABLES|SYS.USER_VIEWS|SYS.
                               ALL_TABLES|SYS.USER_TAB_COLUMNS|SYS.
                               USER_CONSTRAINTS|SYS.USER_TRIGGERS|SYS.
                               USER_CATALOG|SYS.ALL_CATALOG|SYS.
                               ALL_CONSTRAINTS|SYS.ALL_OBJECTS|SYS.
                               ALL_TAB_COLUMNS|SYS.ALL_TAB_PRIVS|SYS.
                               ALL_TRIGGERS|SYS.ALL_USERS|SYS.ALL_VIEWS|SYS
                               .USER_ROLE_PRIVS|SYS.USER_SYS_PRIVS|SYS.
                               USER_TAB_PRIVS)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                        </Pattern>
                        <Pattern type="fastmatch">
                            <Location area="HTTP_METHOD"/>
                            <Match type="LITERAL">T</Match>
                        </Pattern>
                    </RequestPatterns>
                </PatternList>
                <LogString>sql Injection</LogString>
                <Comment/>
            </SignatureRule>
        </Signatures>
```



```
</SignaturesFile>

<!--NeedCopy-->
```

Aktualisierung eines Signaturobjekts

May 11, 2023

Sie müssen Ihre Signaturobjekte regelmäßig aktualisieren, um sicherzustellen, dass Ihre Web App Firewall Schutz vor aktuellen Bedrohungen bietet. Sie müssen regelmäßig sowohl die Standardsignaturen der Web App Firewall als auch alle Signaturen aktualisieren, die Sie aus einem unterstützten Tool zum Scannen von Sicherheitslücken importieren.

NetScaler aktualisiert regelmäßig die Standardsignaturen für die Web App Firewall. Sie können die Standardsignaturen manuell oder automatisch aktualisieren. In beiden Fällen fragen Sie Ihren NetScaler-Vertreter oder NetScaler-Reseller nach der URL für den Zugriff auf die Updates. Sie können automatische Updates der Signaturen im systemeigenen NetScaler-Format in den Dialogfeldern „Engine-Einstellungen“ und „Einstellungen für automatische Signaturaktupdates“ aktivieren.

Die meisten Hersteller von Tools zum Scannen von Sicherheitslücken aktualisieren die Tools regelmäßig. Die meisten Websites ändern sich auch häufig. Sie müssen Ihr Tool aktualisieren und Ihre Websites regelmäßig erneut scannen, die resultierenden Signaturen in eine Datei exportieren und in Ihre Web App Firewall-Konfiguration importieren.

> **Tipp**
>
> Wenn Sie die Web App Firewall-Signaturen über die NetScaler-Befehlszeile aktualisieren, müssen Sie zuerst die Standardsignaturen aktualisieren und dann weitere Aktualisierungsbefehle ausführen, um jede benutzerdefinierte Signaturdatei zu aktualisieren, die auf den Standardsignaturen basiert. Wenn Sie nicht zuerst die Standardsignaturen aktualisieren, verhindert ein Versionskonflikt die Aktualisierung der benutzerdefinierten Signaturdateien.
>
> **Hinweis**
>
> Folgendes gilt für das Zusammenführen eines Signaturobjekts eines Drittanbieters mit einem benutzerdefinierten Signaturobjekt mit systemeigenen Regeln und vom Benutzer hinzugefügten Regeln:
>
> Wenn eine Signatur der Version 0 mit einer neuen importierten Datei zusammengeführt wird, bleiben die resultierenden Signaturen als Version 0 erhalten.
>
> Das bedeutet, dass alle systemeigenen (oder integrierten) Regeln in der importierten Datei nach der Zusammenführung ignoriert werden. Dadurch wird sichergestellt, dass die Signaturen der

> Version 0 nach einer Zusammenführung unverändert beibehalten werden.
>
> Um die systemeigenen Regeln in die importierte Datei für die Zusammenführung aufzunehmen, müssen Sie vor der Zusammenführung zunächst die vorhandenen Signaturen von Version 0 aktualisieren. Das bedeutet, dass Sie den Versions-0-Charakter der vorhandenen Signaturen aufgeben müssen.
>
> Wenn es ein NetScaler-Release-Upgrade gibt, wird die Datei "default_signatures.xml" zum neuen Build hinzugefügt und die Datei "updated_signature.xml" wird aus dem älteren Build entfernt. Wenn nach dem Upgrade die Funktion zur automatischen Signatumaktualisierung aktiviert ist, aktualisiert die Appliance die vorhandene Signatur auf die neueste Version des Builds und generiert die Datei "updated_signature.xml".

So aktualisieren Sie die Web App Firewall-Signaturen von der Quelle aus mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `update appfw signatures <name> [-mergedefault]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird das Signaturobjekt mySignatures anhand des Standardsignaturobjekts aktualisiert, indem neue Signaturen im Standardsignaturobjekt mit den vorhandenen Signaturen zusammengeführt werden. Dieser Befehl überschreibt keine vom Benutzer erstellten Signaturen oder Signaturen, die aus einer anderen Quelle importiert wurden, z. B. von einem zugelassenen Tool zum Scannen von Sicherheitslücken.

```
update appfw signatures MySignatures -mergedefault
save ns config
<!--NeedCopy-->
```

Aktualisieren eines Signaturobjekts aus einer NetScaler-Formatdatei

NetScaler aktualisiert regelmäßig die Signaturen für die Web App Firewall. Sie müssen die Signaturen auf Ihrer Web App Firewall regelmäßig aktualisieren, um sicherzustellen, dass Ihre Web App Firewall die aktuelle Liste verwendet. Fragen Sie Ihren NetScaler-Vertreter oder NetScaler-Reseller nach der URL für den Zugriff auf die Updates.

So aktualisieren Sie ein Signaturobjekt aus einer Datei im NetScaler-Format mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `update appfw signatures <name> [-mergeDefault]`
- `save ns config`

So aktualisieren Sie ein Signaturobjekt aus einer Datei im NetScaler-Format mithilfe der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie aktualisieren möchten.
3. Wählen Sie in der Dropdownliste **Aktion** die Option **Zusammenführen**aus.
4. Wählen **Sie im Dialogfeld „Signaturobjekt aktualisieren** “ eine der folgenden Optionen aus.
   - **Von URL importieren**— Wählen Sie diese Option, wenn Sie Signaturupdates von einer Web-URL herunterladen.
   - **Aus lokaler Datei importieren**— Wählen Sie diese Option, wenn Sie Signaturaktualisierungen aus einer Datei auf Ihrer lokalen Festplatte, Netzwerkfestplatte oder einem anderen Speichergerät importieren.
5. Geben Sie im Textbereich die URL ein, oder geben Sie die lokale Datei ein, oder suchen Sie nach der lokalen Datei.
6. Klicken Sie auf **Update**. Die Aktualisierungsdatei wird importiert, und das Dialogfeld „Signaturen aktualisieren“ nimmt ein Format an, das fast identisch mit dem des Dialogfelds „ **Signaturobjekt ändern** “ ist. Im Dialogfeld **Signaturobjekt aktualisieren** werden alle Zweige mit neuen oder geänderten Signaturregeln, SQL-Injections- oder siteübergreifenden Skriptmustern und XPath-Injectionsmustern angezeigt, sofern vorhanden.
7. Überprüfen und konfigurieren Sie die neuen und geänderten Signaturen.
8. Wenn Sie fertig sind, klicken Sie auf **OK**und dann auf **Schließen**.

Aktualisierung eines Signaturobjekts über ein unterstütztes Tool zum Scannen von Sicherheitslücken

> **Hinweis:**
>
> Bevor Sie ein Signaturobjekt aus einer Datei aktualisieren, müssen Sie die Datei erstellen, indem Sie Signaturen aus dem Tool zum Scannen von Sicherheitslücken exportieren.

So importieren und aktualisieren Sie Signaturen aus einem Tool zum Scannen von Sicherheitslücken

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Signaturen**.

2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie aktualisieren möchten, und klicken Sie dann auf **Zusammenführen**.
3. Wählen **Sie im Dialogfeld Signaturobjekt aktualisieren** auf der Registerkarte **Externes Format** im Abschnitt Import eine der folgenden Optionen aus.
   - **Von URL importieren**— Wählen Sie diese Option, wenn Sie Signaturupdates von einer Web-URL herunterladen.
   - **Aus lokaler Datei importieren**— Wählen Sie diese Option, wenn Sie Signaturaktualisierungen aus einer Datei auf Ihrer lokalen Festplatte oder einer Netzwerkfestplatte oder einem anderen Speichergerät importieren.
4. Geben Sie im Textbereich die URL ein, oder suchen Sie nach dem Pfad zur lokalen Datei oder geben Sie ihn ein.
5. Wählen Sie im Abschnitt XSLT eine der folgenden Optionen aus.
   - **Integrierte XSLT-Datei verwenden**— Wählen Sie diese Option, wenn Sie eine integrierte XSLT-Datei verwenden möchten.
   - **Lokale XSLT-Datei verwenden**— Wählen Sie diese Option, um eine XSLT-Datei auf Ihrem lokalen Computer zu verwenden.
   - **XSLT von URL aus referenzieren**— Wählen Sie diese Option, um eine XSLT-Datei von einer Web-URL zu importieren.
6. Wenn Sie die Option Integrierte XSLT-Datei verwenden ausgewählt haben, wählen Sie in der Dropdownliste Integriertes XSLT die Datei, die Sie verwenden möchten, aus den folgenden Optionen aus:
   - **Cenzic.**
   - **Deep_Security_für_Web-Apps.**
   - **Hewlett Packard Enterprise WebInspect.**
   - **IBM-AppScan-Unternehmen.**
   - **IBM-AppScan-Standard.**
   - **Qualys.**
   - **Weißer Hat.**
7. Klicken Sie auf **Update**. Die Update-Datei wird importiert, und das Dialogfeld Signaturen aktualisieren ändert sich in ein Format, das fast identisch mit dem des Dialogfelds Signatures-Objekt ändern ist, das unter Signatures-Objekt konfigurieren oder ändernbeschrieben wird. Im Dialogfeld **Signaturobjekt aktualisieren** werden alle Zweige mit neuen oder geänderten Signaturregeln, SQL-Injections- oder siteübergreifenden Skriptmustern und XPath-Injectionsmustern angezeigt, sofern vorhanden.
8. Überprüfen und konfigurieren Sie die neuen und geänderten Signaturen.
9. Wenn Sie fertig sind, klicken Sie auf **OK**und dann auf **Schließen**.

Automatische Aktualisierung der Signatur

May 11, 2023

Die Funktion "Signature Auto Update" in der Web Application Firewall ermöglicht es dem Benutzer, die neuesten Signaturen zu erhalten, um die Webanwendung vor neuen Schwachstellen zu schützen. Die Funktion zur automatischen Aktualisierung bietet einen besseren Schutz, ohne dass ein fortlaufender manueller Eingriff erforderlich ist, um die neuesten Updates zu erhalten.

Die Signaturen werden stündlich automatisch aktualisiert und müssen nicht regelmäßig auf die Verfügbarkeit des neuesten Updates überprüft werden. Sobald Sie das automatische Signatur-Update aktiviert haben, stellt die NetScaler-Appliance eine Verbindung mit dem Server her, der die Signaturen hostet, um zu prüfen, ob eine neuere Version verfügbar ist.

Anpassbarer Standort

Die neuesten Application Firewall-Signaturen werden auf Amazon gehostet, das als Standardsignatur-URL konfiguriert ist, um nach dem neuesten Update zu suchen.

Der Benutzer hat jedoch die Möglichkeit, diese Signaturzuordnungsdateien auf seinen internen Server herunterzuladen. Der Benutzer kann dann einen anderen Signatur-URL-Pfad konfigurieren, um die Signaturzuordnungsdateien von einem lokalen Server herunterzuladen. Damit die Funktion zur automatischen Aktualisierung funktioniert, müssen Sie möglicherweise den DNS-Server für den Zugriff auf die externe Site konfigurieren.

Signaturen aktualisieren

Alle benutzerdefinierten Signaturobjekte, die mit dem appfw-Standardsignaturobjekt erstellt werden, haben eine Version größer als Null. Wenn Sie das automatische Update der Signatur aktivieren, werden alle Signaturen automatisch aktualisiert.

Wenn der Benutzer Signaturen mit dem externen Format wie Cenzic oder Qualys importiert hat, werden die Signaturen mit der Version als Null importiert. Wenn der Benutzer ein Signaturobjekt mit der leeren Vorlage erstellt hat, wird es in ähnlicher Weise als Nullversionssignatur erstellt. Diese Signaturen werden nicht automatisch aktualisiert, da der Benutzer möglicherweise nicht an der Verwaltung der nicht verwendeten Standardsignaturen interessiert ist.

Die Web Application Firewall ermöglicht dem Benutzer jedoch auch die Flexibilität, diese Signaturen manuell auszuwählen und zu aktualisieren, um den vorhandenen Regeln die Standardsignaturregeln hinzuzufügen. Nachdem die Signaturen manuell aktualisiert wurden, ändert sich die Version und dann werden die Signaturen zusammen mit den anderen Signaturen automatisch aktualisiert.

Konfigurieren des automatischen Updates der Signatur

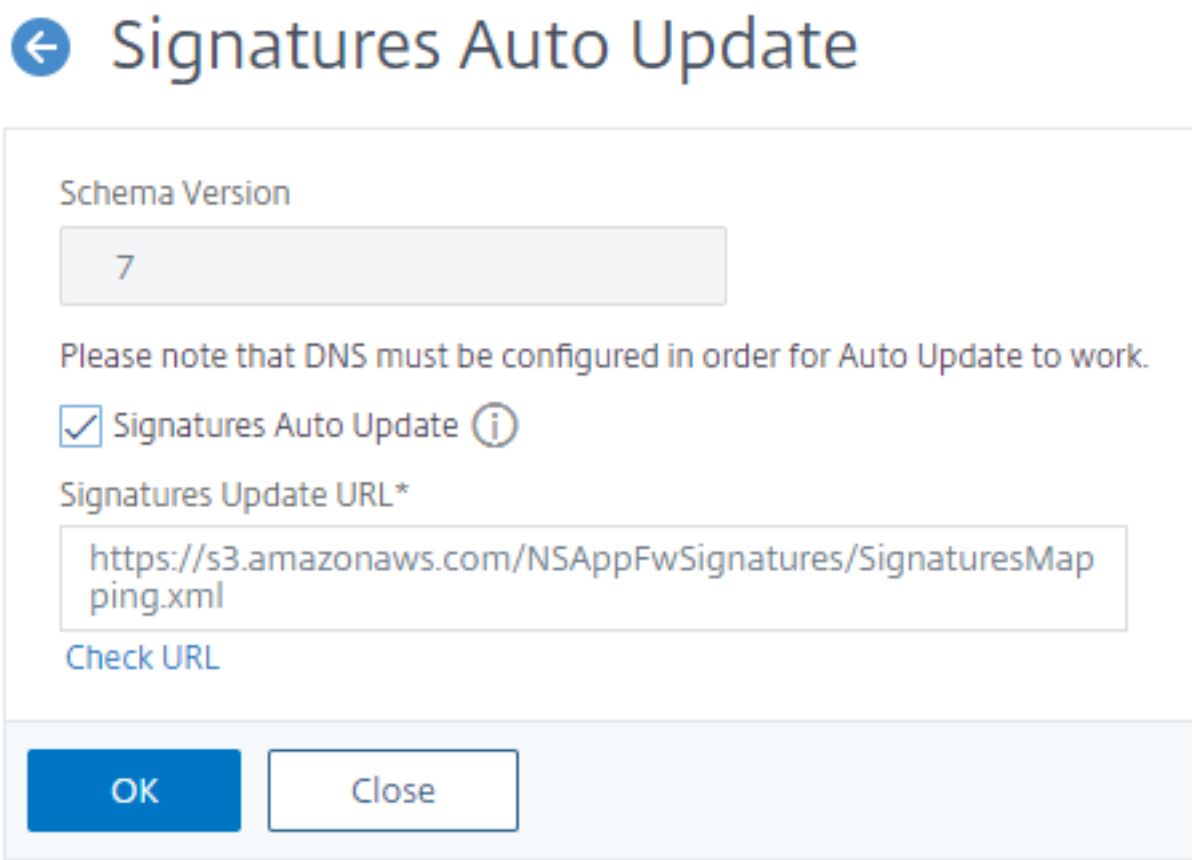
So konfigurieren Sie die Funktion zur automatischen Aktualisierung der Signatur mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw settings SignatureAutoUpdate on
set appfw settings SignatureUrl https://s3.amazonaws.com/
    NSAppFwSignatures/SignaturesMapping.xml
<!--NeedCopy-->
```

So konfigurieren Sie das automatische Update der Signatur mit der GUI:

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Wählen Sie unter **AktionEinstellungen automatisch aktualisieren**aus.
3. Aktivieren Sie die Option " **Automatische Aktualisierung von Signaturen**".
4. Sie können bei Bedarf einen benutzerdefinierten Pfad für die Signaturaktualisierungs-URL angeben. Klicken Sie auf **Zurücksetzen**, um auf den Standard zurückzusetzen `s3.amazonaws.com server`.
5. Klicken Sie auf **OK**.



Signaturen manuell aktualisieren

Um eine Nullversionssignatur oder eine andere benutzerdefinierte Signatur manuell zu aktualisieren, müssen Sie zuerst das neueste Update für die Standardsignaturen erhalten und diese dann zum Aktualisieren der benutzerdefinierten Zielsignatur verwenden.

Führen Sie die folgenden Befehle von der CLI aus, um eine Signaturdatei zu aktualisieren:

```
update appfw signatures "*Default Signatures"
update appfw signatures cenzic  -mergedefault
<!--NeedCopy-->
```

> **Hinweis:**
>
> `Default Signatures` Es wird Groß-/Kleinschreibung Cenzic im vorherigen Befehl ist der Name der Signaturdatei, die aktualisiert wird.

Importieren von Standardsignaturen ohne Internetzugang

Es wird empfohlen, einen Proxy-Server so zu konfigurieren, dass er auf den Amazon (AWS) -Server verweist, um das neueste Update zu erhalten. Wenn die NetScaler Appliance jedoch keine Internetverbindung zu den externen Sites hat, kann der Benutzer die aktualisierten Signaturdateien auf einem lokalen Server speichern. Die Appliance kann die Signaturen dann vom lokalen Server herunterladen. In diesem Szenario muss der Benutzer ständig die **Amazon-Website** überprüfen, um die neuesten Updates zu erhalten. Sie können die Signaturdatei mit der entsprechenden sha1-Datei herunterladen und überprüfen, die mit dem **öffentlichen Schlüssel von Citrix** zum Schutz vor Manipulationen erstellt wurde.

Führen Sie das folgende Verfahren aus, um die Signatures-Dateien auf einen lokalen Server zu kopieren:

1. Erstellen Sie ein lokales Verzeichnis wie <`MySignatures`> auf einem lokalen Server.
2. Öffnen Sie die AWS-Site.
3. Kopieren Sie die Datei `SignaturesMapping.xml` in den Ordner <`MySignatures`>.

Wenn Sie die Datei `SignaturesMapping.xml` öffnen, können Sie alle XML-Dateien für Signaturen und die entsprechenden sha1-Dateien für verschiedene unterstützte Versionen sehen. Ein solches Paar wird im folgenden Screenshot hervorgehoben:

1. Erstellen Sie ein Unterverzeichnis <`sigs`> im Ordner <`MySignatures`>.
2. Kopieren Sie alle Paare der Tags `*.xml files listed in the` <`file`> und die Dateien `*.xml.sha1`, die in den entsprechenden Tags <`sha1`> der Datei `SignaturesMapping.xml` aufgeführt werden, in den Ordner <`sigs`>. Im Folgenden sind einige Beispieldateien aufgeführt, die in den Ordner <`sigs`> kopiert werden:

https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml.sha1
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml.sha1

> **Hinweis:**
>
> Sie können dem Ordner <MySignatures>e inen beliebigen Namen geben und er kann sich an jedem Speicherort befinden, aber das Unterverzeichnis <sigs> muss ein Unterverzeichnis in dem Ordner <MySignatures> sein, in den die Zuordnungsdatei kopiert ist. Stellen Sie außerdem sicher, dass der Unterverzeichnisname, wie in der SignaturesMapping.xml gezeigt, den genauen Namen <sigs> haben muss und die Groß- und Kleinschreibung beachtet wird. Alle Signaturdateien und die entsprechenden sha1-Dateien sollten unter dieses Verzeichnis <sigs> kopiert werden.

Nachdem Sie den Inhalt vom gehosteten Amazon-Webserver auf den lokalen Server gespiegelt haben, ändern Sie den Pfad zum neuen lokalen Webserver, um ihn als signatureUrl für die automatische Aktualisierung festzulegen. Führen Sie beispielsweise den folgenden Befehl über die Befehlszeilenschnittstelle der Appliance aus:

```
1 set appfw settings SignatureUrl https://myserver.example.net/
     MySignatures/SignaturesMapping.xml
2 <!--NeedCopy-->
```

Der Update-Vorgang kann je nach Anzahl der zu aktualisierenden Signaturen mehrere Minuten dauern. Lassen Sie genügend Zeit, bis der Update-Vorgang abgeschlossen ist.

Wenn Sie auf einen Fehler stoßen “Fehler beim Zugriff auf URL! “Befolgen Sie während der Konfiguration die Schritte, um es zu beheben.

1. Fügen Sie die URL https://myserver.example.net zu /netscaler/ns_gui/admin_ui/php/application/controllers/common/utils.php hinzu, damit die Sicherheit der Inhaltssicherheitsrichtlinie (CSP) den URL-Zugriff nicht blockiert. Bitte beachten Sie, dass diese Einstellungen bei einem Upgrade nicht bestehen. Der Benutzer muss es nach dem Upgrade erneut hinzufügen.

```
1 $configuration_view_connect_src = "connect-src 'self' https://app.pendo
     .io https://s3.amazonaws.comhttps://myserver.example.net;";
2 <!--NeedCopy-->
```

1. Der Benutzer muss den Webserver https://myserver.example.net so konfigurieren, dass er auf die folgenden CORS-Header für https://myserver.example.net/MySignatures/SignaturesMapping.xml antwortet

```
1 Access-Control-Allow-Methods: GET
```



```
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 3000
<!--NeedCopy-->
```

Richtlinien zum Aktualisieren von Signaturen

Beim Aktualisieren von Signaturen werden folgende Richtlinien verwendet:

- Die Signaturen werden aktualisiert, wenn die Signaturaktualisierungs-URL ein Signaturobjekt enthält, das dieselbe oder neuere Version hat.
- Jede Signaturregel ist mit einer Regel-ID und einer Versionsnummer verknüpft. Beispiel: `<SignatureRule id="803"version="16"…>`
- Die Signaturregel aus der eingehenden Signature-Datei mit derselben ID und Versionsnummer wie die vorhandene wird ignoriert, auch wenn sie unterschiedliche Muster oder Protokollzeichenfolgen hat.
- Eine Signaturregel mit einer neuen ID wird hinzugefügt. Alle Aktionen und aktiviertes Flag werden aus der neuen Datei verwendet.

  > **Hinweis:**
  >
  > Sie müssen die aktualisierten Signaturen regelmäßig überprüfen, um die neu hinzugefügten Regeln zu aktivieren und andere Aktionseinstellungen gemäß den Anforderungen der Anwendung zu ändern.

- Regeln mit derselben ID, aber mit einer neueren Versionsnummer ersetzen die vorhandene. Alle Aktionen und aktiviertes Flag aus der vorhandenen Regel bleiben erhalten.

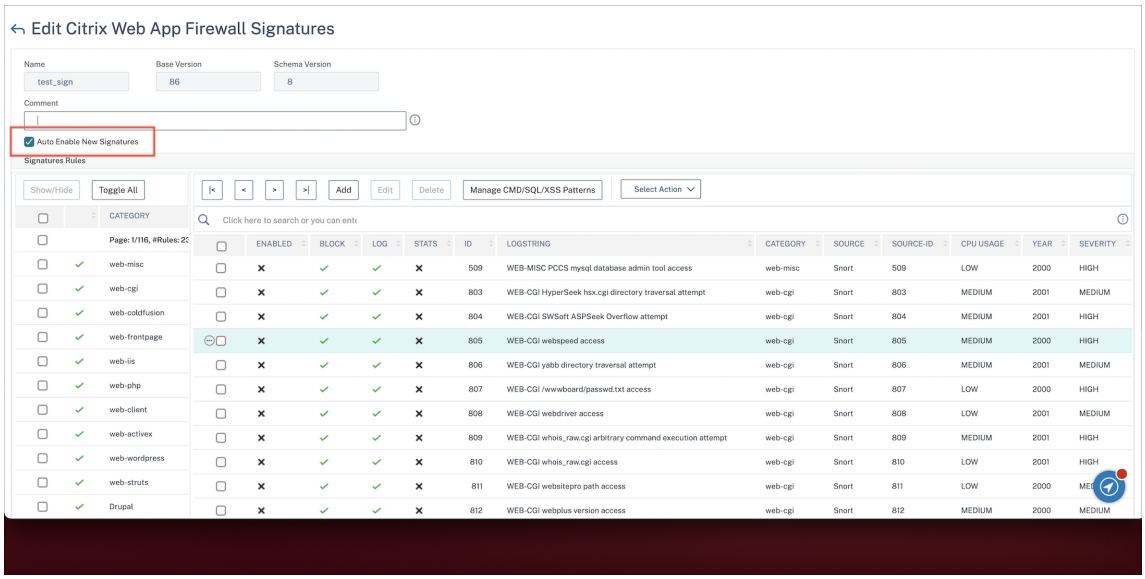
> **Tipp:**
>
> Wenn Sie die Signaturen von der CLI aus aktualisieren, müssen Sie zuerst die Standardsignaturen aktualisieren. Sie müssen dann Aktualisierungsbefehle hinzufügen, um jede benutzerdefinierte Signaturdatei zu aktualisieren, die auf den Standardsignaturen basiert. Wenn Sie die Standardsignaturen nicht zuerst aktualisieren, verhindert ein Fehler bei der Nichtübereinstimmung der Version die Aktualisierung der Datei benutzerdefinierter Signaturen.

Neue Signaturen automatisch aktivieren

Ab Version 13.1 Build 27.x und höher können Sie die Option **Neue Signaturen automatisch aktivieren** auswählen, damit neue WAF-Signatur-Standardregeln nach einem Update automatisch aktiviert werden.

Automatische Aktivierung neuer Signaturen über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Wählen Sie eine Signatur und klicken Sie auf **Bearbeiten**
3. Wählen Sie **Neue Signaturen automatisch aktivieren** aus.



Neue Signaturen automatisch mit der CLI aktivieren

Geben Sie in der Befehlszeile Folgendes ein:

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType Snort] [-autoEnableNewSignatures ( ON | OFF )]
```

Beispiel:

```
import signatures http://www.example.com/ns/signatures.xml my-signature -autoEnableNewSignatures ON
```

Integration von SNORT-Regeln

May 11, 2023

Bei böswilligen Angriffen auf Webanwendungen ist es wichtig, Ihr internes Netzwerk zu schützen. Bösartige Daten wirken sich nicht nur auf Schnittstellenebene auf Ihre Webanwendungen aus, sondern bösartige Pakete erreichen auch die Andwendungslayer. Um solche Angriffe zu verhindern, ist

es wichtig, ein System zur Erkennung und Verhinderung von Eindringlingen zu konfigurieren, das Ihr internes Netzwerk untersucht.

Snort-Regeln sind in die Appliance integriert, um böswillige Angriffe in Datenpaketen auf Andwendungslayer zu untersuchen. Sie können die Snort-Regeln herunterladen und in WAF-Signaturregeln konvertieren. Die Signaturen verfügen über eine regelbasierte Konfiguration, mit der bösartige Aktivitäten wie DOS-Angriffe, Pufferüberläufe, Stealth-Portscans, CGI-Angriffe, SMB-Untersuchungen und Betriebssystem-Fingerabdruckversuche erkannt werden können. Durch die Integration von Snort-Regeln können Sie Ihre Sicherheitslösung auf Schnittstellen- und Anwendungsebene stärken.

Snort-Regeln konfigurieren

Die Konfiguration beginnt damit, dass zuerst die Snort-Regeln heruntergeladen und dann in die WAF-Signaturregeln importiert werden. Sobald Sie die Regeln in WAF-Signaturen umgewandelt haben, können die Regeln als WAF-Sicherheitschecks verwendet werden. Die Snort-basierten Signaturregeln untersuchen das eingehende Datenpaket, um festzustellen, ob es böswillige Angriffe auf Ihr Netzwerk gibt.

Ein neuer Parameter, „VendorType“, wurde dem Importbefehl hinzugefügt, um Snort-Regeln in WAF-Signaturen zu konvertieren.

Der Parameter „VendorType“ ist auf SNORT nur für Snort-Regeln gesetzt.

Downloaden Sie snort-Regeln mithilfe der Befehlszeilenschnittstelle

Sie können die Snort-Regeln als Textdatei von der folgenden URL herunterladen:

```
https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
```

Importieren von Snort-Regeln mithilfe der Befehlszeilenschnittstelle

Nach dem Herunterladen können Sie die Snort-Regeln in Ihre Appliance importieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>]
[-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType
Snort]
```

Beispiel:

```
import appfw signatures http://www.example.com/ns/signatures.xml sig-snort -
comment “signatures from snort rules” -VendorType snort
```

Argumente:

Src. URL (Protokoll, Host, Pfad und Dateiname) für den Speicherort, an dem das importierte Signaturobjekt gespeichert werden soll.

> **Hinweis:**
>
> Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, für den Zugriff eine Clientzertifikatauthentifizierung erforderlich ist Obligatorisches Argument für die maximale Länge: 2047

Name. Name, der dem Signaturobjekt auf dem NetScaler zugewiesen werden soll. Obligatorisches Argument mit maximaler Länge: 31

Kommentar. Beschreibung, wie Informationen über das Signaturobjekt aufbewahrt werden. Maximale Länge: 255
überschreiben. Überschreiben Sie alle vorhandenen Signaturobjekte mit demselben Namen.

Verschmelzen. Führt die bestehende Signatur mit neuen Signaturregeln zusammen.

Konservierte Fraktionen. Behält die definierten Aktionen der Signaturregeln bei.

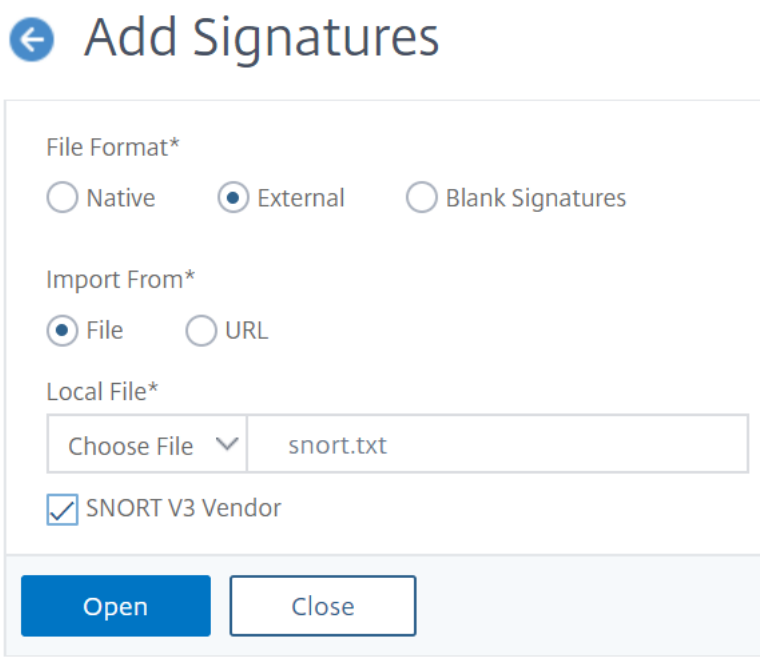
Typ des Anbieters. Drittanbieter zur Generierung der WAF-Signaturen. Mögliche Werte: Snort.

Konfigurieren Sie Snort-Regeln mithilfe der NetScaler-GUI

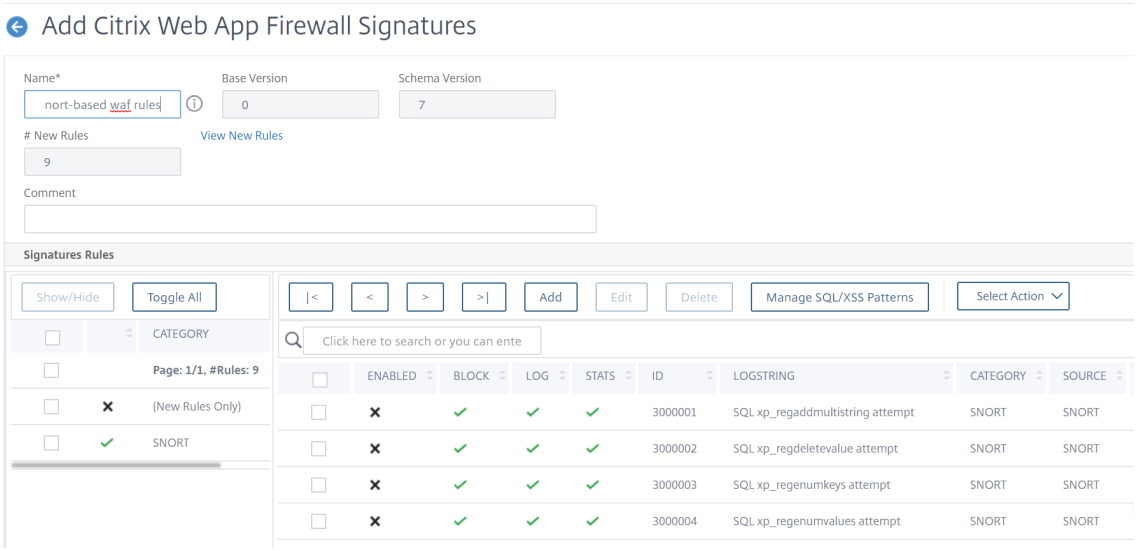
Die GUI-Konfiguration für Snort-Regeln ähnelt der Konfiguration anderer externer Webanwendungsscanner wie Cenzic, Qualys, Whitehat.

Gehen Sie wie folgt vor, um Snort zu konfigurieren:

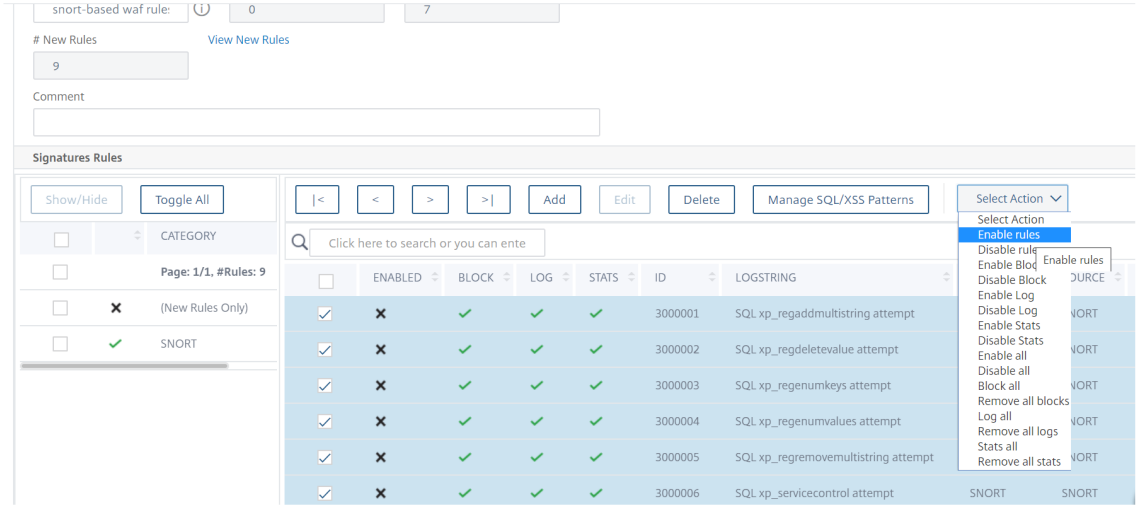
1. Navigieren Sie zu **Konfiguration > Sicherheit > NetScaler Web App Firewall**Signaturen.
2. Klicken Sie auf der Seite **Signaturen** auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Signaturen hinzufügen** die folgenden Parameter ein, um die Snort-Regeln zu konfigurieren.
    a) Dateiformat. Wählen Sie das Dateiformat als extern aus.
    b) Importieren aus. Wählen Sie die Importoption als Snort-Datei oder URL, um die URL einzugeben.
    c) Snort V3-Anbieter. Markieren Sie das Kontrollkästchen, um Snort-Regeln aus einer Datei oder einer URL zu importieren.
4. Klicken Sie auf **Öffnen**.



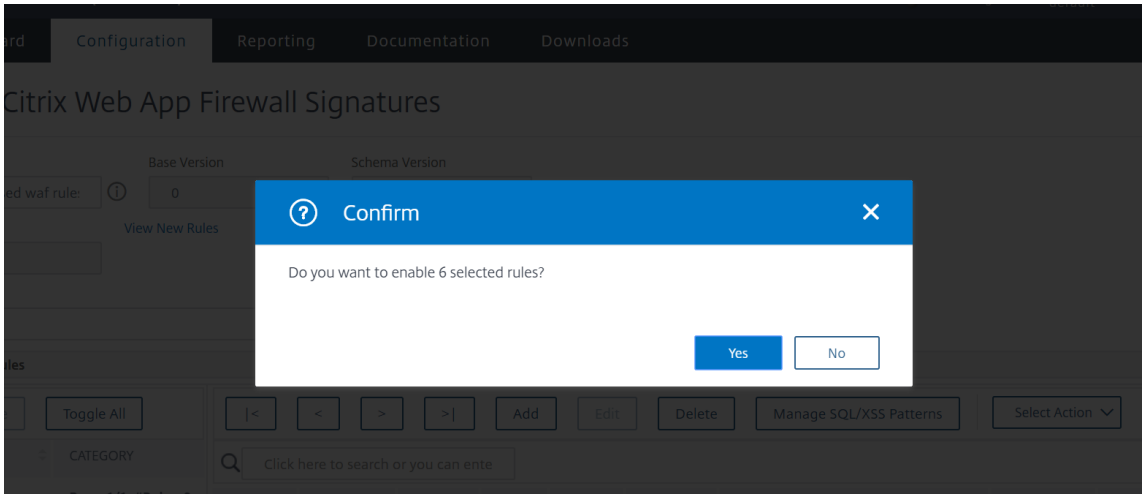
Die Appliance importiert die Snort-Regeln als auf Snorts basierende WAF-Signaturregeln.



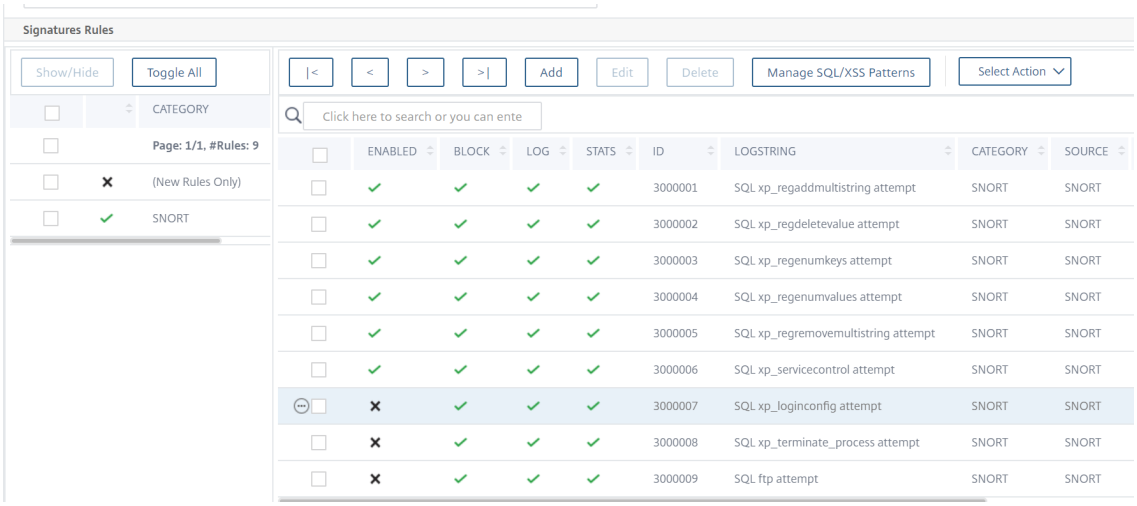
Es hat sich bewährt, Filteraktionen zu verwenden, um Snort-Regeln zu aktivieren, die Sie lieber als WAF-Signaturregeln auf die Appliance importieren möchten.



5. Klicken Sie zur Bestätigung auf **Ja**.



6. Die ausgewählten Regeln sind auf der Appliance aktiviert.



7. Klicken Sie auf **OK**.

Exportieren eines Signaturobjekts in eine Datei

May 11, 2023

Sie exportieren ein Signaturobjekt in eine Datei, sodass Sie es in einen anderen NetScaler importieren können.

Um ein Signaturobjekt in eine Datei zu exportieren

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie konfigurieren möchten.
3. Wählen Sie in der Dropdownliste **Aktionen** die Option **Exportieren**aus.
4. Geben Sie im Dialogfeld **Signaturobjekt exportieren** im Textfeld **Lokale Datei** den Pfad und Namen der Datei ein, in die Sie das Signaturobjekt exportieren möchten, oder verwenden Sie das Dialogfeld **Durchsuchen**, um einen Pfad und einen Namen festzulegen.
5. Klicken Sie auf **OK**.

Bearbeiten Sie Signaturen, um Regeln hinzuzufügen oder zu ändern

May 11, 2023

Sie können die benutzerdefinierten Signaturen bearbeiten, um eine Regel hinzuzufügen oder zu ändern. Eine lokale Signaturregel hat dieselben Attribute wie eine Standardsignaturregel von Citrix und funktioniert auf die gleiche Weise. Sie aktivieren oder deaktivieren es und konfigurieren die Signaturaktionen dafür, genau wie bei einer Standardsignatur.

Fügen Sie eine lokale Regel hinzu, wenn Sie Ihre Websites und Dienste vor einem bekannten Angriff schützen müssen, bei dem die vorhandenen Signaturen nicht übereinstimmen. Sie könnten beispielsweise eine neue Angriffsart entdecken und ihre Merkmale anhand der Protokolle auf Ihrem Webserver ermitteln, oder Sie könnten Informationen von Drittanbietern über eine neue Art von Angriff erhalten.

Das Herzstück einer Signaturregel sind die *Regelmuster*, die zusammen die Merkmale des Angriffs beschreiben, denen die Regel entsprechen soll. Jedes Muster kann aus einer einfachen Zeichenfolge, einem regulären Ausdruck im PCRE-Format oder den integrierten SQL-Injection- oder Cross-Site-Scripting-Mustern bestehen.

Möglicherweise möchten Sie eine Signaturregel ändern, indem Sie ein neues Muster hinzufügen oder ein vorhandenes Muster so ändern, dass es einem Angriff entspricht. So können Sie beispielsweise von Änderungen an einem Angriff erfahren oder ein besseres Muster ermitteln, indem Sie die Protokolle auf Ihrem Webserver oder anhand von Informationen von Drittanbietern untersuchen.

Hinzufügen oder Ändern einer lokalen Signaturregel

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich die benutzerdefinierten Signaturen aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Signaturregeln** auf **Hinzufügen**. Der Bereich **Signaturregel** wird angezeigt.
4. Konfigurieren Sie die Aktionen für eine Signatur, indem Sie die entsprechenden Kontrollkästchen aktivieren.
    - **Aktiviert.** Aktiviert die neue Signaturregel. Wenn Sie dies nicht auswählen, wird diese neue Signaturregel zu Ihrer Konfiguration hinzugefügt, ist jedoch inaktiv.
    - **Blockieren.** Sperrt Verbindungen, die gegen diese Signaturregel verstoßen.
    - **Loggen.** Protokolliert Verstöße gegen diese Signaturregel im NetScaler-Protokoll.
    - **Statistik.** Nimmt Verstöße gegen diese Signaturregel in die Statistik auf.
    - **Remove.** Löscht Informationen, die der Signaturregel entsprechen, aus der Antwort. (Gilt nur für Antwortregeln.)
    - **X-Out.** Maskiert Informationen, die der Signaturregel entsprechen, mit dem Buchstaben X. (Gilt nur für Antwortregeln.)
    - **Duplikate zulassen.** Erlaubt Duplikate dieser Signaturregel in diesem Signaturobjekt.
5. Wählen Sie in der Dropdownliste Kategorie eine **Kategorie** für die neue Signaturregel aus.

   Wenn Sie eine Kategorie erstellen möchten, klicken Sie auf **Hinzufügen**. Weitere Informationen finden Sie unter Hinzufügen einer Kategorie für Signaturregeln.
6. Geben Sie im Textfeld **LogString** eine kurze Beschreibung der Signaturregel ein, die in den Protokollen verwendet werden soll.
7. **Geben Sie in das Textfeld Kommentar einen Kommentar ein.** Optional:
8. Klicken Sie auf **Mehr**, um die erweiterten Optionen zu ändern.
    a) Um HTML-Kommentare zu entfernen, bevor diese Signaturregel angewendet wird, wählen Sie in der Dropdownliste Kommentare entfernen die Option Alle oder Skript-Tag ausschließen.
    b) Um die CSRF-Referrer-Header-Prüfung zu aktivieren, wählen Sie im Optionsfeld CSRF-Referrer-Header-Prüfung entweder das Optionsfeld Falls vorhanden oder Immer aus.
    c) Um die Regelkennung, die dieser lokalen Signaturregel zugewiesen ist, manuell zu ändern, ändern Sie die Nummer im Textfeld Regelkennung. Die ID muss eine positive Ganzzahl zwischen 1000000 und 1999999 sein, die noch keiner lokalen Signaturregel zugewiesen wurde.
    d) Um der neuen Signaturregel eine Versionsnummer zuzuweisen, ändern Sie die Nummer im Textfeld Versionsnummer.

e) Um eine Quell-ID zuzuweisen, ändern Sie die Zeichenfolge im Textfeld Quell-ID.
f) Um die Quelle anzugeben, wählen Sie in der Dropdownliste Quelle die Option Lokal oder Snort aus, oder klicken Sie rechts neben der Liste auf das Symbol Hinzufügen und fügen Sie eine neue Quelle hinzu.
g) Um Verstößen gegen diese lokale Signaturregel einen Schadenswert zuzuweisen, geben Sie eine Zahl zwischen 1 und 10 in das Textfeld Harm Score ein.
h) Um dieser lokalen Signaturregel einen Schweregrad zuzuweisen, wählen Sie in der Dropdownliste Schweregrad die Option Hoch, Mittel oder Niedrig aus, oder klicken Sie rechts neben der Liste auf das Symbol Hinzufügen und fügen Sie einen neuen Schweregrad hinzu.
i) Um dieser lokalen Signaturregel einen Verstoßtyp zuzuweisen, wählen Sie in der Dropdownliste Typ die Option Anfällig oder Warnung aus, oder klicken Sie rechts neben der Liste auf das Symbol Hinzufügen und fügen Sie einen neuen Verstoßtyp hinzu.

9. Klicken Sie unter **Regelmuster**auf **Hinzufügen**, um ein Muster hinzuzufügen. Sie können auch die vorhandenen Muster bearbeiten. Klicken Sie dazu auf **Bearbeiten**.

   Weitere Informationen zum Hinzufügen oder Bearbeiten von Mustern finden Sie unter Signaturregelmuster.

10. Klicken Sie auf **OK**.

Eine Kategorie für Signaturregeln hinzufügen

Wenn Sie Signaturregeln in eine Kategorie einordnen, können Sie die Aktionen für eine Gruppe von Signaturen anstatt für jede einzelne Signatur konfigurieren. Möglicherweise möchten Sie dies aus den folgenden Gründen tun:

- **Einfache Auswahl.** Nehmen wir beispielsweise an, dass alle Signaturregeln in einer bestimmten Gruppe vor Angriffen auf eine bestimmte Art von Webserversoftware oder -technologie schützen. Wenn Ihre geschützten Websites diese Software oder Technologie verwenden, möchten Sie sie alle aktivieren. Wenn sie dies nicht tun, möchten Sie keine von ihnen aktivieren.
- **Einfache Erstkonfiguration.** Es ist am einfachsten, Standardwerte für eine Gruppe von Signaturen als Kategorie festzulegen, anstatt sie einzeln festzulegen. Anschließend können Sie nach Bedarf Änderungen an den einzelnen Signaturen vornehmen.
- **Einfache laufende Konfiguration.** Es ist einfacher, Signaturen zu konfigurieren, wenn Sie nur solche anzeigen können, die bestimmte Kriterien erfüllen, z. B. die Zugehörigkeit zu einer bestimmten Kategorie.

Hinzufügen von Signaturregelmustern

May 11, 2023

Sie können ein Muster hinzufügen oder ein vorhandenes Muster ändern, um eine Zeichenfolge oder einen Ausdruck anzugeben, der einen Angriff kennzeichnet, sofern die Signatur übereinstimmt. Um die Muster zu erkennen, die ein Angriff aufweist, können Sie die Protokolle auf Ihrem Webserver überprüfen. Sie können ein Tool verwenden, um Verbindungsdaten in Echtzeit zu beobachten, oder die Zeichenfolge oder den Ausdruck aus einem Bericht eines Drittanbieters über den Angriff abrufen.

> **Wichtig** Ein neues Muster, das Sie einer Signaturregel hinzufügen, steht in einer UND-Beziehung zu den vorhandenen Mustern. Fügen Sie einer vorhandenen Signaturregel kein Muster hinzu, wenn Sie nicht möchten, dass ein potenzieller Angriff alle Muster mit der Signatur übereinstimmen muss.

Jedes Muster kann aus einer einfachen Zeichenfolge, einem regulären Ausdruck im PCRE-Format oder dem integrierten SQL-Injection- oder Cross-Site-Scripting-Muster bestehen. Bevor Sie versuchen, ein Muster hinzuzufügen, das auf einem regulären Ausdruck basiert, müssen Sie sicherstellen, dass Sie reguläre Ausdrücke im PCRE-Format verstehen. PCRE-Ausdrücke sind komplex und leistungsstark. Wenn Sie nicht verstehen, wie sie funktionieren, können Sie unbeabsichtigt ein Muster erstellen, das mit etwas übereinstimmt, das Sie nicht wollten (*falsch positiv*), oder das nicht mit etwas übereinstimmt, das Sie wollten (*falsch negativ*).

Benutzerdefiniertes Signaturmuster für nicht standardmäßige Inhaltstypen

Die NetScaler Web App Firewall (WAF) unterstützt jetzt einen neuen Standort für die Überprüfung kanonischer Inhalte. Standardmäßig blockiert WAF keine codierte Nutzlast mit nicht standardmäßigen Inhaltstypen. Wenn diese Inhaltstypen auf der Whitelist stehen und keine konfigurierte Aktion angewendet wird, filtert die SQL- und Cross-Site-Scripting-Schutzprüfung keine SQL- oder Cross-Site-Scripting-Angriffe in den codierten Payloads. Um das Problem zu lösen, kann ein Benutzer mit diesem neuen Speicherort (HTTP_CANON_POST_BODY) eine benutzerdefinierte Signaturregel erstellen, die die codierten Payloads auf nicht standardmäßige Inhaltstypen untersucht. Wenn es einen SQL- oder Cross-Site-Scripting-Angriff gibt, blockiert sie den Datenverkehr nach der Kanonisierung des Beitragstextes.

> **Hinweis:**
>
> Diese Unterstützung gilt nur für HTTP-Anfragen.

Wenn Sie mit regulären Ausdrücken im PCRE-Format noch nicht vertraut sind, können Sie die folgenden Ressourcen verwenden, um die Grundlagen zu erlernen oder Hilfe bei bestimmten Problemen zu erhalten:

- “Mastering Regular Expressions,” Third Edition. Copyright (c) 2006 von Jeffrey Friedl. O’Reilly Media, ISBN: 9780596528126.
- “Regular Expressions Cookbook”. Copyright (c) 2009 von Jan Goyvaerts und Steven Levithan. O’Reilly Media, ISBN: 9780596520687
- PCRE-Hauptseite/Spezifikation
- PCRE Man Page/Spezifikation
- Wikipedia-PCRE-Eintrag
- PCRE-Mailingliste

Wenn Sie Nicht-ASCII-Zeichen in einem regulären Ausdruck im PCRE-Format codieren müssen, unterstützt die NetScaler-Plattform die Kodierung von hexadezimalen UTF-8-Codes. Weitere Informationen finden Sie unter PCRE-Zeichenkodierungsformat.

Ein Signaturregelmuster konfigurieren

Wenn Sie eine Signatur bearbeiten, können Sie das Regelmuster hinzufügen oder bearbeiten. Informationen zum Hinzufügen oder Ändern der Signaturregeln finden Sie unter Signaturen bearbeiten, um Regeln hinzuzufügen oder zu ändern.

- **Typ** — Wählen Sie den Verbindungstyp aus, dem das Muster entsprechen soll.
  - **Anfrage** — Sie entspricht den Anforderungselementen oder Funktionen wie eingefügtem SQL-Code, Angriffen auf Webformulare, seitenübergreifende Skripts oder unangemessene URLs.
  - **Antwort** — Sie entspricht den Antwortelementen oder Funktionen wie Kreditkartennummern oder Tresor-Objekten.
- **Standort** — Wählen Sie einen **Bereich** aus, der mit diesem Muster untersucht werden soll. In diesem Bereich wird beschrieben, welche Elemente der HTTP-Anfrage oder -Antwort auf dieses Muster untersucht werden sollen. Basierend auf dem ausgewählten Mustertyp werden die Optionen in der **Bereichsliste** angezeigt. Sie hängen vom ausgewählten Mustertyp ab.

  Für den **Anforderungsmustertyp** werden Elemente angezeigt, die für HTTP-Anfragen relevant sind.
  - **HTTP_ANY**. Alle Teile der HTTP-Verbindung.
  - **HTTP_COOKIE**. Alle Cookies in den HTTP-Anforderungsheadern nach allen Cookie-Transformationen werden durchgeführt.

    > **Hinweis** Sucht nicht nach den “Set-Cookie:”-Headern der HTTP-Antwort.
  - **HTTP_FORM_FIELD**. Formularfelder und ihr Inhalt nach URL-Dekodierung, prozentualer Dekodierung und Entfernung überschüssiger Leerzeichen. Sie können das `<Location >` Tag verwenden, um die Liste der zu durchsuchenden Formularfeldnamen weiter einzuschränken.

- **HTTP-HEADER.** Die Wertanteile des HTTP-Headers nach allen Cross-Site Scripting- oder URL-Dekodierungstransformationen.
- **HTTP_METHOD**. Die HTTP-Anforderungsmethode.
- **HTTP_URL**. Der Wertanteil der URL in den HTTP-Headern, ohne Abfrage- oder Fragmentports, nach der Konvertierung in den UTF-*-Zeichensatz, der URL-Dekodierung, dem Entfernen von Leerzeichen und der Konvertierung relativer URLs in absolute URLs. Beinhaltet keine Dekodierung von HTML-Entitäten.
- **HTTP_ORIGIN_URL**. Die Quell-URL eines Webformulars.
- **HTTP_POST_BODY**. Der HTTP-Posttext und die darin enthaltenen Webformulardaten.
- **HTTP_RAW_COOKIE**. Alle HTTP-Anforderungs-Cookies, einschließlich des Namensteils “Cookie:”.
  Hinweis: Sucht nicht nach den “Set-Cookie:”-Headern der HTTP-Antwort.
- **HTTP_RAW_HEADER**. Der gesamte HTTP-Header mit einzelnen Headern, die durch Zeilenvorschubzeichen (\ n) oder Carrie-Return-/Zeilenvorschubzeichenfolgen (\ r\ n) getrennt sind.

Für den **Antworttyp** werden Elemente angezeigt, die für HTTP-Antworten relevant sind.

- **HTTP_RAW_RESP_HEADER**. Der gesamte Antwortheader, einschließlich der Namens- und Wertteile des Antwortheaders nach Abschluss der URL-Transformation, und der vollständige Antwortstatus. Wie bei HTTP_RAW_HEADER werden einzelne Header durch Zeilenvorschubzeichen (\ n) oder Wagenrücklauf/Zeilenvorschub-Zeichenketten (\r\n) getrennt.
- **HTTP_RAW_SET_COOKIE**. Der gesamte Set-Cookie-Header, nachdem alle URL-Transformationen durchgeführt wurden

  > **Hinweis:**
  >
  > Durch die URL-Transformation können sowohl die Domain- als auch die Pfadteile des Set-Cookie-Headers geändert werden.

- **HTTP_RAW_URL**. Die gesamte Anforderungs-URL, bevor irgendwelche URL-Transformationen durchgeführt werden, einschließlich aller Abfrage- oder Fragmentteile.
- **HTTP_RESP_HEADER**. Der Werteteil der vollständigen Antwortheader, nachdem alle URL-Transformationen durchgeführt wurden.
- **HTTP_RESP_BODY**. Der HTTP-Antworttext
- **HTTP_SET_COOKIE**. Alle “Set-Cookie”-Header in den HTTP-Antwortheadern.
- **HTTP_STATUS_CODE**. Der HTTP-Statuscode.

- **HTTP_STATUS_MESSAGE**. Die HTTP-Statusmeldung.

Wenn Sie eine Option aus der **Bereichsliste** auswählen, werden die Optionen für den ausgewählten Bereich dynamisch geändert.

- **Any.** Prüft Feldnamen oder URLs.
- **Wörtlich.** Prüft Feldnamen oder URLs, die eine literale Zeichenfolge enthalten. Nachdem Sie Literal ausgewählt haben, wird ein Textfeld angezeigt. Geben Sie die gewünschte Literalzeichenfolge in das Textfeld ein.
- **PCRE.** Prüft Feldnamen oder URLs, die einem regulären Ausdruck im PCRE-Format entsprechen. Nachdem Sie diese Option ausgewählt haben, wird das Fenster für reguläre Ausdrücke angezeigt. Geben Sie den regulären Ausdruck in das Fenster ein. Sie können die **Regex-Token** verwenden, um häufig verwendete reguläre Ausdruckselemente am Cursor einzufügen, oder Sie können auf Regex-Editor klicken, um das Dialogfeld Editor für reguläre Ausdrücke anzuzeigen, das Sie bei der Erstellung des gewünschten regulären Ausdrucks unterstützt.
- **Expression.** Prüft Feldnamen oder URLs, die einem NetScaler-Standardausdruck entsprechen.

- **Muster** — Ein Muster ist eine literale Zeichenfolge oder ein regulärer Ausdruck im PCRE-Format, der das Muster definiert, dem Sie entsprechen möchten. Wählen Sie den **Spieltyp** aus der Liste aus.
  - **Wörtlich.** Eine Literalzeichenfolge.
  - **PCRE.** Ein regulärer Ausdruck im PCRE-Format.

    > **Hinweis**
    >
    > Wenn Sie PCRE wählen, werden die Tools für reguläre Ausdrücke unter dem Musterfenster aktiviert. Diese Tools sind für die meisten anderen Mustertypen nicht nützlich.

  - **Expression.** Ein Ausdruck in der NetScaler-Standardausdruckssprache ist dieselbe Ausdruckssprache für die Erstellung von Web App Firewall-Richtlinien auf der NetScaler-Appliance. Obwohl die NetScaler Expressions Language ursprünglich für Richtlinienregeln entwickelt wurde, ist sie eine hochflexible Allzwecksprache, die auch zur Definition eines Signaturmusters verwendet werden kann.

    Wenn Sie Expression wählen, wird der NetScaler Expression Editor unter dem Pattern-Fenster angezeigt. Weitere Informationen zum Ausdrucks-Editor und Anweisungen zur Verwendung finden Sie unter So fügen Sie eine Firewallregel (Ausdruck) mithilfe des Dialogfelds Ausdruck hinzufügen hinzu
  - **SQL-Einschleusung**. Weist die Web App Firewall an, am angegebenen Ort nach injiziertem SQL zu suchen.

- **CrossSiteScripting**. Weist die Web App Firewall an, am angegebenen Ort nach Cross-Site-Skripten zu suchen.
- **CommandInjection**. Weist die NetScaler Web App Firewall an, nach injizierten bösartigen Befehlen am angegebenen Ort zu suchen.
- **SQLInjectionGrammar**. Weist die NetScaler Web App Firewall an, an der angegebenen Stelle nach injizierter SQL-Grammatik zu suchen. Vor allem, wenn häufig verwendete Wörter wie `Select` und `From` in einer HTTP-Anfrage verwendet werden.
- **CommandInjectionGrammar**. Weist die NetScaler Web App Firewall an, an der angegebenen Stelle nach injizierter bösartiger Befehlsgrammatik zu suchen. Insbesondere, wenn ein häufig verwendetes Wort wie "Exit" in einer HTTP-Anfrage verwendet wird.

Wenn Sie weitere Einstellungen konfigurieren möchten, geben Sie Folgendes an:

- **Offset**. Die Anzahl der Zeichen, die übersprungen werden müssen, bevor mit der Übereinstimmung nach diesem Muster begonnen wird. Sie verwenden dieses Feld, um mit der Untersuchung einer Zeichenfolge an einer anderen Stelle als dem ersten Zeichen zu beginnen.
- **Tiefe**. Wie viele Zeichen vom Startpunkt aus auf Übereinstimmungen untersucht werden sollen. Sie verwenden dieses Feld, um die Suche nach einer großen Zeichenfolge auf eine bestimmte Anzahl von Zeichen zu beschränken.
- **Minimale Länge**. Die zu durchsuchende Zeichenfolge muss mindestens die angegebene Anzahl von Byte lang sein. Kürzere Saiten sind nicht aufeinander abgestimmt.
- **Maximale Länge**. Die zu suchende Zeichenfolge darf nicht länger als die angegebene Anzahl von Byte sein. Längere Zeichenketten werden nicht gefunden.
- **Suchmethode**. Ein beschriftetes Kontrollkästchen `fastmatch`. Sie können die Option `fastmatch` nur für ein literales Muster aktivieren, um die Leistung zu verbessern.

> **Hinweis**
>
> Bis Sie im Bereich **Signaturregelmuster** auf **OK** klicken, werden Ihre Änderungen nicht gespeichert. Schließen Sie eines dieser Dialogfelder nicht, ohne auf **OK** zu klicken, es sei denn, Sie möchten die Änderungen verwerfen.

Um Regeln zu importieren und zusammenzuführen

May 11, 2023

Wenn Sie den Signatureditor verwenden, um einen Import- und Zusammenführungsvorgang von der GUI aus durchzuführen, können Sie jetzt die neuen, aktualisierten, doppelten und ungültigen Regeln sehen.

Der Signatur-Editor zeigt die folgenden vier neuen Zeilen an:

1. Neue Regeln
2. Aktualisierte Regeln
3. Doppelte Regeln
4. Ungültige Regeln

Die Ausgabe der Filter „Nur neue Regeln“ und „Nur aktualisierte Regeln“ wird auch im Bereich „Kategoriefilter“ des Fensters „Bearbeiten“ im Signatureditor angezeigt.

Sie müssen die Dateien aus der GUI importieren, um die entsprechenden Links für neue, doppelte, ungültige und aktualisierte Regeln zu sehen.

Verfahren zum Import von Signaturregeln:

1. Gehen Sie in der NetScaler-Web-GUI zu **Konfiguration > Sicherheit > NetScaler Web**App Firewall Signatures. Klicken Sie im Fenster Signaturen auf **Hinzufügen**. Wählen Sie dann **Dateiformat** > **Nativ**, **Importieren von** > **URL** und fügen Sie im Feld “URL” den obigen Link hinzu. Wenn Sie nicht auf die URL zugreifen können, können Sie die XML-Datenherunterladen.
2. Nachdem Sie auf **Öffnen**geklickt haben, wird die Signaturdatei geöffnet, und Sie können Links für neue Regel und ungültige Regeln sehen.
3. Wenn Sie eine3rd Partei-Signaturregel importieren, werden 90 neue Regeln und 9 doppelte Regeln in der importierten XML-Datei angezeigt. Wenn Sie nicht auf die URL zugreifen können, können Sie die XML-Datenherunterladen.

Signaturaktualisierungen bei Hochverfügbarkeitsbereitstellung und Build-Upgrades

January 19, 2021

Die Signaturaktualisierung erfolgt auf dem primären Knoten. Während die Signaturen auf dem primären Knoten aktualisiert werden, werden die aktualisierten Dateien gleichzeitig mit dem sekundären Knoten synchronisiert.

Die Standardsignatur wird immer zuerst aktualisiert, und dann werden die restlichen benutzerdefinierten Signaturen aktualisiert.

Herstellen einer Verbindung mit Amazon AWS

Der Standard-Routen-NSIP wird verwendet, um eine Verbindung mit Amazon AWS herzustellen. Wenn es ein bestimmtes Anwendungsfallszenario gibt, in dem SNIP verwendet wird, und wenn mehrere SNIPs vorhanden sind, wird der erste, der die ARP-Antwort von der Hosting-Site empfängt, die Route enthalten.

Signaturaktualisierungen bei Versions-Upgrades

Im Falle eines Upgrades, wenn der NS eine ältere Basisversion für die Signaturen hat, wird *Standardsignatur automatisch aktualisiert, wenn eine neuere Signaturversion verfügbar ist.

Wenn sich das Schema geändert hat, wird die Schemaversion aller Signaturobjekte aktualisiert, wenn die Version aktualisiert wird.

Bei der Basisversion der benutzerdefinierten Signaturen unterscheidet sich das Verhalten in Release 10.5 gegenüber Version 11.0.

In Release 10.5 wurde nur die Standardsignatur aktualisiert, und die Basisversion der restlichen Signaturen blieb nach dem Build-Upgrade unverändert.

In Release 11.0 hat sich dieses Verhalten geändert. Wenn die Appliance aktualisiert wird, um einen neuen Build zu installieren, werden nicht nur das Signaturobjekt *Default, sondern alle anderen benutzerdefinierten Signaturen, die derzeit in der Appliance vorhanden sind, ebenfalls aktualisiert und haben nach dem Build-Upgrade dieselbe Version.

Sowohl in 10.5 als auch 11.0 Release-Builds werden die *Default Signatures sowie alle Signaturen, die ungleich Null sind, automatisch auf die neueste veröffentlichte Signaturversion aktualisiert und haben dieselbe Basisversion.

Übersicht über Sicherheitsprüfungen

August 19, 2021

Die erweiterten Schutzmechanismen der Web App Firewall (Sicherheitsprüfungen) sind eine Reihe von Filtern, die komplexe oder unbekannte Angriffe auf Ihre geschützten Websites und Webdienste abfangen sollen. Die Sicherheitsprüfungen verwenden Heuristik, positive Sicherheit und andere Techniken, um Angriffe zu erkennen, die möglicherweise nicht allein von Signaturen erkannt werden. Sie konfigurieren die Sicherheitsprüfungen, indem Sie ein Web App Firewall Profil erstellen und konfigurieren. Dabei handelt es sich um eine Sammlung von benutzerdefinierten Einstellungen, die der Web App Firewall mitteilen, welche Sicherheitsprüfungen verwendet werden sollen und wie eine Anforderung oder Antwort verarbeitet werden soll, bei der eine Sicherheitsprüfung fehlgeschlagen ist. Ein Profil ist einem Signaturobjekt und einer Richtlinie zum Erstellen einer Sicherheitskonfiguration zugeordnet.

Die Web App Firewall bietet zwanzig Sicherheitsprüfungen, die sich in den angestrebten Angriffstypen und der Komplexität ihrer Konfiguration stark unterscheiden. Die Sicherheitsprüfungen sind in folgende Kategorien unterteilt:

- **Gemeinsame Sicherheitsprüfungen.** Überprüfungen, die für alle Aspekte der Websicherheit gelten, die entweder keinen Inhalt beinhalten oder für alle Arten von Inhalten gleichermaßen

gelten.

- **HTML-Sicherheitsprüfungen.** Überprüfungen, die HTML-Anforderungen und Antworten untersuchen. Diese Prüfungen gelten für HTML-basierte Websites und die HTML-Teile von Web 2.0-Sites, die gemischte HTML- und XML-Inhalte enthalten.
- **XML-Sicherheitsprüfungen.** Überprüfungen, die XML-Anforderungen und Antworten untersuchen. Diese Prüfungen gelten für XML-basierte Webdienste und für die XML-Teile von Web 2.0-Websites.

Die Sicherheitsprüfungen schützen vor einer Vielzahl von Angriffen, darunter Angriffe auf Schwachstellen auf Sicherheitslücken in Betriebssystemen und Webserversoftware, Schwachstellen in der SQL-Datenbank, Fehler beim Design und Codieren von Websites und Webdiensten sowie Ausfälle beim Schutz von Websites, die auf sensible Informationen hosten oder darauf zugreifen können.

Alle Sicherheitsprüfungen verfügen über eine Reihe von Konfigurationsoptionen, die Prüfaktionen, mit denen gesteuert wird, wie die Web App Firewall eine Verbindung verarbeitet, die einer Prüfung entspricht. Für alle Sicherheitsprüfungen stehen drei Prüfaktionen zur Verfügung. Sie sind:

- **Blockieren** Verbindungen blockieren, die mit der Signatur übereinstimmen. Diese Funktion ist standardmäßig deaktiviert.
- **Melden Sie sich** Protokollieren Sie Verbindungen, die mit der Signatur übereinstimmen, für eine spätere Analyse. Standardmäßig aktiviert.
- **Statistiken.** Verwalten Sie Statistiken für jede Signatur, die zeigen, wie viele Verbindungen sie übereinstimmten, und geben Sie bestimmte andere Informationen über die Typen von Verbindungen, die blockiert wurden. Diese Funktion ist standardmäßig deaktiviert.

Für mehr als die Hälfte der Überprüfungsaktionen ist eine vierte Prüfaktion **Lernen** verfügbar. Es beobachtet den Datenverkehr zu einer geschützten Website oder einem geschützten Webdienst und verwendet Verbindungen, die wiederholt gegen die Sicherheitsprüfung verstoßen, um empfohlene Ausnahmen (Entspannungen) des Schecks oder neue Regeln für die Überprüfung zu generieren. Zusätzlich zu den Überprüfungsaktionen verfügen bestimmte Sicherheitsüberprüfungen über Parameter, die die Regeln steuern, mit denen die Prüfung ermittelt wird, welche Verbindungen gegen diese Prüfung verstoßen, oder die die Antwort der Web App Firewall auf Verbindungen konfigurieren, die gegen die Prüfung verstoßen. Diese Parameter unterscheiden sich für jede Prüfung und werden in der Dokumentation für jede Prüfung beschrieben.

Um Sicherheitsprüfungen zu konfigurieren, können Sie den Web App Firewall-Assistenten verwenden, wie im Web App Firewall-Assistentbeschrieben, oder Sie können die Sicherheitsprüfungen manuell konfigurieren, wie unter Manuelle Konfiguration mit der GUIbeschrieben. Einige Aufgaben, wie das manuelle Eingeben von Entspannungen oder Regeln oder das Überprüfen von erlernten Daten, können nur über die GUI und nicht über die Befehlszeile ausgeführt werden. Die Verwendung des Assistenten ist in der Regel die beste Konfigurationsmethode, aber in einigen Fällen kann die manuelle Konfiguration einfacher sein, wenn Sie mit ihm vertraut sind und einfach die Konfiguration für eine einzelne Sicherheitsprüfung anpassen möchten.

Unabhängig davon, welche Methode Sie zum Konfigurieren der Sicherheitsprüfungen verwenden, erfordert jede Sicherheitsprüfung, dass bestimmte Aufgaben ausgeführt werden. Viele Überprüfungen erfordern, dass Sie Ausnahmen (Relaxationen) angeben, um das Blockieren von legitimen Datenverkehr zu verhindern, bevor Sie die Sperre für diese Sicherheitsprüfung aktivieren. Sie können dies manuell tun, indem Sie die Protokolleinträge beobachten, nachdem ein bestimmter Datenverkehr gefiltert wurde und dann die erforderlichen Ausnahmen erstellen. In der Regel ist es jedoch viel einfacher, die Lernfunktion zu aktivieren und den Verkehr zu beobachten und die notwendigen Ausnahmen zu empfehlen.

Web App Firewall verwendet während der Verarbeitung der Transaktionen Packet Engines (PE). Jede Paketengine hat ein Limit von 100.000 Sitzungen, was für die meisten Bereitstellungsszenarien ausreichend ist. Wenn die Web App Firewall jedoch hohen Datenverkehr verarbeitet und das Sitzungstimeout mit einem höheren Wert konfiguriert ist, können die Sitzungen angesammelt werden. Wenn die Anzahl der Live Web App Firewall -Sitzungen die Grenze von 100.000 pro PE überschreitet, werden die Verletzungen der Web App Firewall Sicherheitsprüfung möglicherweise nicht an die Security Insight-Appliance gesendet. Das Senkung des Sitzungstimeouts auf einen kleineren Wert oder die Verwendung des Sitzungslos-Modus für die Sicherheitsprüfungen mit sitzungslosem URL-Schließen oder Sitzungslos-Feldkonsistenz kann dazu beitragen, dass die Sitzungen akkumuliert werden. Wenn dies in Szenarien, in denen Transaktionen möglicherweise längere Sitzungen erfordern, keine praktikable Option ist, wird ein Upgrade auf eine übergeordnete Plattform mit mehr Paketmodul empfohlen.

Unterstützung für zwischengespeicherte AppFirewall wird hinzugefügt, und die maximale Sitzungseinstellung über die CLI pro Kern wird auf 50.000 Sitzungen festgelegt.

Höchster Schutz

May 11, 2023

Vier der Schutzmaßnahmen der Web App Firewall sind besonders wirksam gegen gängige Arten von Webangriffen und werden daher häufiger eingesetzt als alle anderen. Sie sind:

- **Site-übergreifendes HTML-Skript.** Untersucht Anfragen und Antworten auf Skripts, die versuchen, auf Inhalte auf einer anderen Website zuzugreifen oder diese zu ändern als der, auf der sich das Skript befindet. Wenn diese Überprüfung ein solches Skript findet, macht es entweder das Skript harmlos, bevor die Anforderung oder Antwort an das Ziel weitergeleitet wird, oder es blockiert die Verbindung.
- **HTML-SQL-Einschleusung.** Untersucht Anfragen, die Formularfelddaten enthalten, auf Versuche, SQL-Befehle in eine SQL-Datenbank einzufügen. Wenn diese Überprüfung injizierten SQL-Code erkennt, blockiert sie entweder die Anforderung oder macht den injizierten SQL-Code

harmlos, bevor die Anforderung an den Webserver weitergeleitet wird.

Hinweis: Wenn die beiden folgenden Bedingungen auf Ihre Konfiguration zutreffen, müssen Sie sicherstellen, dass Ihre Web App Firewall korrekt konfiguriert ist:

- Wenn Sie die HTML Cross-Site Scripting-Überprüfung oder die HTML-SQL-Injection-Prüfung (oder beide) aktivieren, und
- Ihre geschützten Websites akzeptieren Datei-Uploads oder enthalten Webformulare, die große POST-Text-Daten enthalten können.

Weitere Informationen zum Konfigurieren der Web App Firewall für diesen Fall finden Sie unter Konfigurieren der Application Firewall.

- **Pufferüberlauf.** Untersucht Anfragen, um Versuche zu erkennen, einen Pufferüberlauf auf dem Webserver auszulösen.
- **Konsistenz von Cookies.** Untersucht Cookies, die bei Benutzeranfragen zurückgegeben werden, um sicherzustellen, dass sie mit den Cookies übereinstimmen, die Ihr Webserver für diesen Benutzer gesetzt hat. Wenn ein modifiziertes Cookie gefunden wird, wird es aus der Anforderung entfernt, bevor die Anforderung an den Webserver weitergeleitet wird.

Die Überprüfung auf einen Buffer Overflow ist einfach; Sie können die Blockierung normalerweise sofort aktivieren. Die anderen drei Top-Level-Prüfungen sind erheblich komplexer und müssen konfiguriert werden, bevor Sie sie sicher verwenden können, um den Datenverkehr zu blockieren. NetScaler empfiehlt nachdrücklich, dass Sie nicht versuchen, diese Prüfungen manuell zu konfigurieren, sondern die Lernfunktion aktivieren und zulassen, dass sie die erforderlichen Ausnahmen generiert.

Site-übergreifende HTML-Skriptprüfung

May 11, 2023

Die HTML Cross-Site Scripting-Prüfung untersucht sowohl die Header als auch die POST-Texte von Benutzeranfragen auf mögliche Cross-Site-Scripting-Angriffe. Wenn es ein seitenübergreifendes Skript findet, modifiziert (*transformiert*) es entweder die Anfrage, um den Angriff unschädlich zu machen, oder blockiert die Anfrage.

> **Hinweis:**
>
> Die Prüfung von HTML Cross-Site Scripting (Cross-Site-Scripting) funktioniert nur für den Inhaltstyp, die Inhaltslänge usw. Stellen Sie außerdem sicher, dass die Option “CheckRequestHeaders” in Ihrem Web Application Firewall Profil aktiviert ist.

Sie können den Missbrauch der Skripts auf Ihren geschützten Sites verhindern, indem Sie die HTML Cross-Site Scripting-Skripts verwenden, die gegen *dieselbe Ursprungsregel*verstoßen, die besagt, dass

Skripts auf keinem Server, sondern auf dem Server, auf dem sie sich befinden, zugreifen oder diese ändern dürfen. Jedes Skript, das gegen dieselbe Ursprungsregel verstößt, wird als siteübergreifendes Skript bezeichnet, und die Praxis, Skripts zum Zugriff auf oder Ändern von Inhalten auf einem anderen Server zu verwenden, wird als siteübergreifende Skripts bezeichnet. Der Grund, warum Cross-Site Scripting ein Sicherheitsproblem darstellt, besteht darin, dass ein Webserver, der Cross-Site Scripting ermöglicht, mit einem Skript angegriffen werden kann, das sich nicht auf diesem Webserver befindet, sondern auf einem anderen Webserver, z. B. einem, der dem Angreifer gehört und von diesem kontrolliert wird.

Leider verfügen viele Unternehmen über eine große installierte Basis von Webinhalten mit Javascript, die gegen dieselbe Ursprungsregel verstoßen. Wenn Sie die HTML Cross-Site Scripting-Prüfung auf einer solchen Site aktivieren, müssen Sie die entsprechenden Ausnahmen generieren, damit die Prüfung keine legitimen Aktivitäten blockiert.

Die Web App Firewall bietet verschiedene Aktionsoptionen für die Implementierung von HTML Cross-Site Scripting Schutz. Zusätzlich zu den Aktionen **Blockieren**, **Protokollieren**, **Statistiken** und **Lernen** haben Sie auch die Möglichkeit, **Site-übergreifende Skripte zu transformieren**, um einen Angriff unschädlich zu machen, indem die Entität die Script-Tags in der gesendeten Anforderung codiert. Sie können den Parameter Vollständige URLs für Cross-Site Scripting überprüfen konfigurieren, um anzugeben, ob Sie nicht nur die Abfrageparameter, sondern die gesamte URL überprüfen möchten, um einen Cross-Site-Scripting-Angriff zu erkennen. Sie können den Parameter **InspectQueryContentTypes** so konfigurieren, dass der Teil der Anforderungsabfrage auf den Cross-Site-Scripting-Angriff auf die spezifischen Inhaltstypen überprüft wird.

Sie können Entspannungen einsetzen, um Fehlalarme zu vermeiden. Die Lernengine der Web App Firewall kann Empfehlungen zum Konfigurieren von Relaxationsregeln enthalten.

Um einen optimierten HTML Cross-Site Scripting-Schutz für Ihre Anwendung zu konfigurieren, konfigurieren Sie eine der folgenden Aktionen:

- **Blockieren**— Wenn Sie Block aktivieren, wird die Blockaktion ausgelöst, wenn die websiteübergreifenden Scripting-Tags in der Anforderung erkannt werden.
- **Log**— Wenn Sie die Protokollfunktion aktivieren, generiert die HTML-Site-Scripting-Prüfung Protokollmeldungen, die die Aktionen angeben, die ausgeführt werden. Wenn Block deaktiviert ist, wird für jeden Header oder jedes Formularfeld, in dem die Cross-Site-Scripting-Verletzung erkannt wurde, eine separate Protokollnachricht generiert. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. In ähnlicher Weise wird eine Protokollnachricht pro Anforderung für den Transformationsvorgang generiert, auch wenn Cross-Site-Scripting-Tags in mehrere Felder umgewandelt werden. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
- **Statistiken**— Wenn diese Option aktiviert ist, sammelt die Statistikfunktion Statistiken zu Verstößen und Protokollen. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise

darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um zu prüfen, ob Sie die neuen Entspannungsregeln konfigurieren oder die vorhandenen ändern müssen.

- **Lernen**— Wenn Sie sich nicht sicher sind, welche Entspannungsregeln für Ihre Anwendung am besten geeignet sind, können Sie die Lernfunktion verwenden, um basierend auf den erlernten Daten Empfehlungen für HTML-Site-Scripting-Regeln zu generieren. Die Web App Firewall Learning Engine überwacht den Datenverkehr und gibt auf der Grundlage der beobachteten Werte Lernempfehlungen ab. Um einen optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie die Lernoption möglicherweise für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Regeln bereitstellen und das Lernen deaktivieren.
- **Siteübergreifende Skripts transformieren**— Wenn diese Option aktiviert ist, nimmt die Web App Firewall folgende Änderungen an Anforderungen vor, die mit der Prüfung für HTML Cross-Site Scripting übereinstimmen:
  - Linke eckige Klammer (<) zum Äquivalent der HTML-Zeichenentität (<)
  - Rechtwinklige Klammer (>) zu HTML-Zeichenentitätsäquivalent (>)

Dadurch wird sichergestellt, dass Browser keine unsicheren HTML-Tags wie `<script>`z. B. interpretieren und dadurch schädlichen Code ausführen. Wenn Sie sowohl die Prüfung der Anforderungsheader als auch die Transformation aktivieren, werden alle Sonderzeichen in Anforderungsheadern ebenfalls geändert. Wenn die Skripts auf Ihrer geschützten Site Cross-Site-Scripting-Funktionen enthalten, Ihre Site jedoch nicht darauf angewiesen ist, dass diese Skripts ordnungsgemäß funktionieren, können Sie das Blockieren sicher deaktivieren und die Transformation aktivieren. Diese Konfiguration stellt sicher, dass kein legitimer Webverkehr blockiert wird, während potenzielle Cross-Site-Scripting-Angriffe gestoppt werden.

- **Prüfen Sie die vollständigen URLs für Cross-Site Scripting**. Wenn die Überprüfung vollständiger URLs aktiviert ist, untersucht die Web App Firewall ganze URLs auf HTML-Site-Scripting-Angriffe, anstatt nur die Abfrageteile der URLs zu überprüfen.
- **Markieren Sie Header der Anforderung**. Wenn die Headerüberprüfung anfordern aktiviert ist, untersucht die Web App Firewall die Header von Anfragen für websiteübergreifende HTML-Scripting-Angriffe, anstatt nur URLs. Wenn Sie die GUI verwenden, können Sie diesen Parameter auf der Registerkarte “Einstellungen” des Web App Firewall-Profils aktivieren.
- **InspectQueryContentTypes**. Wenn Abfrageprüfung anfordern konfiguriert ist, untersucht die App Firewall die Abfrage von Anforderungen für Cross-Site-Scripting-Angriffe auf die spezifischen Inhaltstypen. Wenn Sie die GUI verwenden, können Sie diesen Parameter auf der Registerkarte “Einstellungen” des App Firewall-Profils konfigurieren.

> **Wichtig:**
>
> Im Rahmen der Streaming-Änderungen wurde die Web App Firewall Verarbeitung der Cross-Site-

> Scripting-Tags geändert. Diese Änderung gilt ab 11.0 Builds. Diese Änderung ist auch für die Erweiterungs-Builds von 10.5.e relevant, die das Streaming auf Anforderungsseite unterstützen. In früheren Versionen wurde das Vorhandensein einer offenen Klammer (<) oder einer schließenden Klammer (>) oder beiden (<>) als Cross-Site-Scripting-Verletzung gekennzeichnet. Das Verhalten wurde in den Builds geändert, die Unterstützung für das Streaming auf der Anforderungsseite beinhalten Nur das Zeichen in der engen Klammer (>) wird nicht mehr als Angriff betrachtet. Anfragen werden auch dann geblockt, wenn ein Zeichen in offener Klammer (<) vorhanden ist, und werden als Angriff betrachtet. Der Cross-Site-Scripting-Angriff wird markiert.

Site-übergreifendes Scripting Feinkörnige

Die Web App Firewall bietet Ihnen die Möglichkeit, ein bestimmtes Formularfeld, einen Header oder ein Cookie von der websiteübergreifenden Überprüfung des Scripting auszunehmen. Sie können die Prüfung für eines oder mehrere dieser Felder vollständig Bypass, indem Sie die Entspannungsregeln konfigurieren.

Mit der Web App Firewall können Sie durch Feinabstimmung der Entspannungsregeln strengere Sicherheit implementieren. Eine Anwendung erfordert möglicherweise die Flexibilität, um bestimmte Muster zuzulassen, aber die Konfiguration einer Entspannungsregel zur Bypass der Sicherheitsüberprüfung könnte die Anwendung anfällig für Angriffe machen, da das Zielfeld von der Überprüfung auf Cross-Site-Scripting-Angriffsmuster ausgenommen ist. Cross-Site-Scripting Die feinkörnige Entspannung bietet die Möglichkeit, bestimmte Attribute, Tags und Muster zuzulassen. Der Rest der Attribute, Tags und Muster ist gesperrt. Beispielsweise verfügt die Web App Firewall derzeit über einen Standardsatz von mehr als 125 verweigerten Mustern. Da Hacker diese Muster bei standortübergreifenden Skript-Angriffen verwenden können, kennzeichnet die Web App Firewall sie als potenzielle Bedrohungen. Sie können ein oder mehrere Muster lockern, die für den jeweiligen Standort als sicher gelten. Der Rest der potenziell gefährlichen Cross-Site-Scripting-Muster wird weiterhin auf den Zielort überprüft und löst weiterhin die Verstöße gegen die Sicherheitsüberprüfung aus. Sie haben jetzt eine viel strengere Kontrolle.

Die in Relaxationen verwendeten Befehle haben optionale Parameter für **Werttyp** und **Wertausdruck**. Der Werttyp kann leer gelassen werden oder Sie haben die Möglichkeit, **Tag** oder **Attribut** oder **Muster**auszuwählen. Wenn Sie den Werttyp leer lassen, wird das konfigurierte Feld der angegebenen URL von der Cross-Site Scripting-Prüfung ausgenommen. Wenn Sie einen Werttyp auswählen, müssen Sie einen Wertausdruck angeben. Sie können angeben, ob der Wertausdruck ein regulärer Ausdruck oder eine literale Zeichenfolge ist. Wenn die Eingabe mit der Liste “Zulässig” und “Verweigert” abgeglichen wird, werden nur die in den Entspannungsregeln konfigurierten angegebenen Ausdrücke ausgenommen.

Die Web App Firewall verfügt über die folgenden integrierten Listen für das Cross-Site Scripting:

1. **Cross-Site Scripting Zulässige Attribute**: Es sind 52 standardmäßig zulässige Attribute wie

abbr, **accesskey**, **align**, **alt**, **axis**, **bgcolor**, **border**, **cell padding**, **cell**abstand, **char**, **charoff**, **charset** und so weiter

2. **Cross-Site Scripting Zulässige Tags**: Es sind 47 Standard-Tags zulässig, z. B. **address**, **basefont**, **bgsound**, **big**, **blockquote**, **bg**, **br**, **caption**, **center**, ****cite,** ****dd**, **del** und so weiter
3. **Cross-Site Scripting Denied Patterns**: Es gibt 129 Standardeinstellungen für verweigerte Muster, wie **FSCommand**, **Javascript:**, **onAbort**, **onActivate** und so weiter

> **Warnung**
>
> Die Aktionsadressen der Web App Firewall sind reguläre Ausdrücke. Beim Konfigurieren von siteübergreifenden HTML-Relaxationsregeln für Skripts können Sie **Name**und **Value Expression** als Literal oder RegEx angeben. Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die Regel definieren, die Sie als Ausnahme hinzufügen möchten, und sonst nichts. Die unvorsichtige Verwendung von Platzhaltern und insbesondere des Punkt-Sternchen-Metazeichens (.*) oder der Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht möchten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die HTML Cross-Site Scripting Prüfung sonst blockiert hätte.

Zu berücksichtigende Punkte:

- Der Wertausdruck ist ein optionales Argument. Ein Feldname hat möglicherweise keinen Wertausdruck.
- Ein Feldname kann an Ausdrücke mit mehreren Werten gebunden werden.
- Wertausdrücken muss ein Werttyp zugewiesen werden. Der Cross-Site Scripting -Werttyp kann sein: 1) Tag, 2) Attribut oder 3) Muster.
- Sie können mehrere Entspannungsregeln pro Feldname/URL-Kombination festlegen
- Die Namen der Formularfelder und die Aktionsadressen unterscheiden nicht zwischen Groß- und Kleinschreibung

Konfigurieren der HTML-Site-Scripting-Prüfung über die Befehlszeile

So konfigurieren Sie HTML Cross-Site Scripting, überprüfen Sie Aktionen und andere Parameter mithilfe der Befehlszeile

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um die HTML Cross-Site Scripting Check zu konfigurieren:

- setze appfw-Profilthema .
- `<name> -crossSiteScriptingAction (([block] [learn] [log] [stats])| [** none**])`
- [appfw-Profilthema festlegen.

- <name> **-crossSiteScriptingTransformUnsafeHTML** (ON | OFF)
- setze appfw-Profilthema.
- <name> -crossSiteScriptingCheckCompleteURLs (ON | OFF)
- setze appfw-Profilthema.
- ‘ - checkRequestHeaders (ON \| OFF)
- <name> - CheckRequestQueryNonHtml (ON | OFF)

So konfigurieren Sie ein HTML Cross-Site Scripting, überprüfen Sie die Entspannungsregel mithilfe der Befehlszeile

Verwenden Sie den Befehl bind oder unbind, um die Bindung wie folgt hinzuzufügen oder zu löschen:

- bind appfw profile <name> -crossSiteScripting <String> [isRegex (REGEX | NOTREGEX)] <formActionURL> [-location <location>] [-valueType (Tag|Attribute|Pattern)[<valueExpression>] [-isValueRegex (REGEX | NOTREGEX)]]
- unbind appfw profile <name> -crossSiteScripting <String> <formActionURL> [-location <location>] [-valueType (Tag |Attribute|Pattern)[<valueExpression>]]

Verwenden der GUI zur Konfiguration der websiteübergreifenden HTML-Skriptprüfung

In der GUI können Sie das HTML Cross-Site Scripting Check im Bereich für das Profil konfigurieren, das mit Ihrer Anwendung verknüpft ist.

So konfigurieren oder ändern Sie die HTML Cross-Site Scripting Prüfung mit der GUI

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

In der Tabelle zur Sicherheitsüberprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsüberprüfungen angezeigt. Sie haben 2 Möglichkeiten für die Konfiguration:

a. Wenn Sie die Aktionen **Blockieren**, **Protokollieren**, **Statistiken**und **Lernen** für das HTML Cross-Site Scripting aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf **OK**klicken und dann auf **Speichern und schließen** klicken, um die **Bereich Sicherheitsüberprüfung** .

b. Wenn Sie weitere Optionen für diese Sicherheitsüberprüfung konfigurieren möchten, doppelklicken Sie auf **HTML Cross-Site Scripting**, oder wählen Sie die Zeile aus und klicken auf **Aktionseinstellungen**, um die folgenden Optionen anzuzeigen:

Siteübergreifende Skripts transformieren — Transformieren Sie unsichere Skript-Tags.

Vollständige URLs für Cross-Site-Scriptingprüfen — Anstatt nur den Abfrageteil der URL zu überprüfen, überprüfen Sie die vollständige URL auf websiteübergreifende Skriptverletzungen.

Nachdem Sie eine der obigen Einstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsüberprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt **Sicherheitsprüfungen** vorgenommen haben, und klicken Sie dann auf **Speichern und Schließen**, um den Bereich **Sicherheitsüberprüfung** zu schließen.

Um die Einstellung **Header der Anforderung überprüfen** zu aktivieren oder zu deaktivieren, klicken Sie im Bereich **Erweiterte Einstellungen** auf **Profileinstellungen**. Aktivieren oder deaktivieren Sie in den **allgemeinen Einstellungen**das **Kontrollkästchen Header der Anforderung** überprüfen. Klicken Sie auf **OK**. Sie können entweder das **X-Symbol** oben rechts im Bereich **Profileinstellungen** verwenden, um diesen Abschnitt zu schließen, oder wenn Sie dieses Profil konfiguriert haben, können Sie auf **Fertig** klicken, um zur **Anwendungsfirewall** > **Profil**zurückzukehren.

Um die Einstellung **Anfrage für Abfrage ohne HTML prüfen** zu aktivieren oder zu deaktivieren, klicken Sie im Bereich **Erweiterte Einstellungen** auf **Profileinstellungen**. Aktivieren oder deaktivieren Sie in den **allgemeinen Einstellungen**das **Kontrollkästchen Anfrage Nicht-HTML** abfragen. Klicken Sie auf **OK**. Sie können entweder das X-Symbol oben rechts im Bereich **Profileinstellungen** verwenden, um diesen Abschnitt zu schließen, oder wenn Sie dieses Profil konfiguriert haben, können Sie auf **Fertig** klicken, um zur **App Firewall > Profil**zurückzukehren.

So konfigurieren Sie eine Entspannungsregel für HTML Cross-Site Scripting über die GUI

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Doppelklicken Sie in der Tabelle Entspannungsregeln auf den Eintrag **HTML Cross-Site Scripting**, oder wählen Sie ihn aus und klicken Sie auf **Bearbeiten**.
4. Führen **Sie im Dialogfeld Regeln zur Lockerung von HTML-Site-Skripten** die Vorgänge zum **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren**oder **Deaktivieren** für Entspannungsregeln aus.

> **Hinweis**
>
> Wenn Sie eine neue Regel hinzufügen, wird das Feld " **Wertausdruck** " nur angezeigt, wenn Sie im Feld " **Werttyp** " die Option " **Tag** " oder " **Attribut** oder **Muster** " ausgewählt haben.

So verwalten Sie die Entspannungsregeln für HTML Cross-Site Scripting mithilfe des Visualizers

Für eine konsolidierte Ansicht aller Entspannungsregeln können Sie die Zeile **HTML Cross-Site Scripting** in der Tabelle Entspannungsregeln markieren und auf **Visualizer**klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine vorhandene zu **bearbeiten** . Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer

klicken.

So zeigen Sie die Cross-Site Scripting-Muster über die GUI an oder passen sie an

Sie können die GUI verwenden, um die Standardliste der für das Cross-Site Scripting zulässigen Attribute oder zulässigen Tags anzuzeigen oder anzupassen. Sie können auch die Standardliste der Site-übergreifenden Scripting-Muster anzeigen oder anpassen.

Die Standardlisten sind unter **Anwendungsfirewall** > **Signaturen** > **Standardsignaturen**angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, wird die standardmäßige Liste der zulässigen und verweigerten Cross-Site-Scripting, die im Objekt Standardsignaturen angegeben ist, vom Profil für die Sicherheitsüberprüfung von Cross-Site Scripting verwendet. Die im Standardsignaturobjekt angegebenen Tags, Attributes und Patterns sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese ändern oder ändern möchten, erstellen Sie eine Kopie des Default Signatures -Objekts, um ein benutzerdefiniertes Signaturobjekt zu erstellen. Nehmen Sie Änderungen in den Listen “Zulässig” oder “Verboten” im neuen benutzerdefinierten Signaturobjekt vor und verwenden Sie dieses Signaturobjekt in Ihrem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten Listen “Zulässige” und “Verweigerte” verwenden möchten.

1. Um standardmäßige Cross-Site-Scripting-Muster anzuzeigen:

a. Navigieren Sie zu **Application Firewall** > **Signaturen**, wählen Sie **Standardsignaturen**und klicken Sie auf **Bearbeiten**. Klicken Sie anschließend auf **SQL/Cross-Site-Scripting-Muster verwalten**.

In der Tabelle **“SQL/Cross-Site-Scripting-Pfade verwalten** “ werden die folgenden drei Zeilen zum Cross-Site Scripting angezeigt:

```
xss/allowed/attribute
```

```
xss/allowed/tag
```

```
xss/denied/pattern
```

b. Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden Cross-Site-Scripting-Elemente (Tag, Attribut, Muster) anzuzeigen, die von der Web App Firewall **Cross-Site Scripting** Prüfung verwendet werden.

1. **So passen Sie Cross-Site-Scripting-Elemente**an: Sie können das benutzerdefinierte Signaturobjekt bearbeiten, um das zulässige Tag, zulässige Attribute und verweigerte Muster anzupassen. Sie können neue Einträge hinzufügen oder vorhandene entfernen.

a. Navigieren Sie zu **Application Firewall** > **Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Bearbeiten**. Klicken Sie auf **SQL/Cross-Site-Scripting-Musterverwalten, um die Tabelle SQL/Cross-Site-Scripting-Pfade** verwalten anzuzeigen.

b. Wählen Sie die Site-übergreifende Ziel-Scripting-Zeile aus.

i. Klicken Sie auf **Elemente verwalten**, um **das entsprechende Cross-Site-Scripting-Element hinzuzufügen**, zu **bearbeiten** oder zu **entfernen** .

ii. Klicken Sie auf **Entfernen**, um die ausgewählte Zeile zu entfernen.

> **Warnung:**
>
> Sie müssen vorsichtig sein, bevor Sie ein standardmäßiges Cross-Site-Scripting-Element entfernen oder ändern oder den Cross-Site Scripting -Pfad löschen, um die gesamte Zeile zu entfernen. Die Signaturregeln und die Cross-Site Scripting-Sicherheitsprüfung stützen sich auf diese Elemente, um Angriffe zum Schutz Ihrer Anwendungen zu erkennen. Das Anpassen der Cross-Site-Scripting-Elemente kann Ihre Anwendung anfällig für Cross-Site-Scripting-Angriffe machen, wenn das erforderliche Pattern während der Bearbeitung entfernt wird.

Lernen Sie Verstöße gegen HTML-Site-Scripting (Cross-Site-Scripting)

Wenn das Lernen aktiviert ist, überwacht die Lernengine der NetScaler Web App Firewall den Datenverkehr und lernt die Verstöße gegen die Cross-Site Scripting Skripting-URL. Sie können die Regeln für Cross-Site-Scripting-URLs regelmäßig überprüfen und sie auf falsch positive Szenarien anwenden.

> **Hinweis:**
>
> In einer Cluster-Konfiguration müssen alle Knoten dieselbe Version haben, um die Regeln für die websiteübergreifende Skripting-URL bereitstellen zu können.

Als Teil der Lernkonfiguration bietet die Web App Firewall feinkörniges HTML-Site-Scripting-Lernen. Die Lernmaschine gibt Empfehlungen zum beobachteten Werttyp (Tag, Attribut, Muster) und zum entsprechenden Value-Ausdruck, der in den Eingabefeldern beobachtet wird. Zusätzlich zur Überprüfung der blockierten Anforderungen, um festzustellen, ob die aktuelle Regel zu restriktiv ist und gelockert werden muss, können Sie die von der Lern-Engine generierten Regeln überprüfen, um festzustellen, welcher Werttyp und welcher Werteausdruck Verstöße auslösen und in den Relaxationsregeln behandelt werden müssen.

> **Hinweis:**
>
> Die Lern-Engine der Web App Firewall kann nur die ersten 128 Byte des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen enthält, die für die ersten 128 Bytes übereinstimmen, kann die Lern-Engine möglicherweise nicht zwischen ihnen unterscheiden. In ähnlicher Weise kann die bereitgestellte Entspannungsregel versehentlich alle diese Felder von der HTML-Site-Scripting-Überprüfung lockern.
>
> **Tipp:**
>
> Site-übergreifende Scripting-Tags, die länger als 12 Zeichen sind, werden nicht richtig erlernt oder protokolliert.
>
> Wenn Sie eine größere Tag-Länge zum Lernen benötigen, können Sie ein großes, nicht erscheinendes Tag in **as_Cross-Site Scripting_Allowed_Tags_List** für die Länge ‘x’ hinzufügen.

Der Lernprozess von HTML Cross-Site Scripting reduziert Fehlalarme bei Cross-Site-Scripting-Angriffen. Wenn das Lernen aktiviert ist, können Sie alle Verstöße in einer Anforderung lernen und möglicherweise eine Lockerung auf mehrere Tags, Attribute oder Muster anwenden, ohne dass eine Wiederholung erforderlich ist.

Wenn eine Nutzlast beispielsweise 15 benutzerdefinierte Tags enthält, die jeweils zu einer Verletzung führen, können Sie die feinkörnige Entspannung für alle Tags anwenden, die als Verstoß gekennzeichnet sind, anstatt den Vorgang zu wiederholen, um die Entspannung für jeweils ein Tag anzuwenden.

Szenario 1: Lernen aktiviert und Block aktiviert:
In diesem Szenario lernt die NetScaler-Appliance alle Verstöße in benutzerdefinierten Tags/Attributen/Mustern, und die Anforderung wird blockiert und jede Verletzung wird protokolliert. Das Verhalten ist konsistent für Verstöße, die im Formularfeld, Header oder Cookie identifiziert wurden.

Szenario 2: Lernen aktiviert und Block deaktiviert:
In diesem Szenario lernt die NetScaler-Appliance die Verletzungen in benutzerdefinierten Tags/Attributen/Mustern und jede der Verletzungen wird protokolliert. Die Anfrage ist nicht gesperrt. Das Verhalten ist konsistent für Verstöße, die im Formularfeld, Header oder Cookie identifiziert wurden.

So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `show appfw learningdata <profilename> crossSiteScripting`
- `rm appfw learningdata <profilename> -crossSiteScripting <string> <formActionURL> [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> **crossSiteScripting*`

Konfigurieren Sie die Cross-Site-Scripting-Feinkornentspannung Bypass um benutzerdefinierte Tags

Sie können die Site-übergreifende Entspannung von Skripten im Web-App-Firewall-Profil konfigurieren, um benutzerdefinierte Tags/Attribute/Muster zu Bypass, die nicht in der Zulassungsliste enthalten sind.
Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile p1 -crossSiteScripting <string> <formActionURL> -valueType
 <valueType> <value expression>
```

Beispiel:

```
bind appfw profile profile1 -crossSiteScripting formfield1 http://1.1.1.1 -
valueType Tag tag1
```

So zeigen Sie erlernte Daten mit der GUI an oder verwenden sie

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **“Erweiterte Einstellungen** “ auf **Gelernte Regeln**. Sie können den Eintrag **HTML Cross-Site Scripting** in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die erlernten Regeln zuzugreifen. In der Tabelle werden die Spalten **Feldname**, Eine**Aktions-URL**, **Werttyp**, **Wert**und **Treffer** angezeigt. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Entspannungsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

Sie haben auch die Möglichkeit, eine zusammenfassende Ansicht der erlernten Relaxationen anzuzeigen, indem Sie den Eintrag **HTML Cross-Site Scripting** in der Tabelle Gelernte Regeln auswählen und auf **Visualizer** klicken, um eine konsolidierte Ansicht aller erlernten Verletzungen zu erhalten. Der Visualizer macht es einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Ergreifen einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke empfohlen werden, um mehrere Regeln zu konsolidieren. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Zahl aus einer Dropdown-Liste auswählen. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Entspannungen einzusetzen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Verwenden der Protokollfunktion mit der HTML Cross-Site Scripting Prüfung

Wenn die Protokollaktion aktiviert ist, werden die Verstöße gegen die HTML-Site-Scripting-Sicherheitsüberprüfung im Überwachungsprotokoll als **AppFW_Cross-Site-Scripting-Verletzungen** protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und schließen Sie die ns.logs im `/var/log/` Ordner an, um auf die Protokollmeldungen zuzugreifen, die sich auf die HTML-Site-Scripting-Verstöße beziehen:

```
Shell
tail -f /var/log/ns.log | grep APPFW_cross-site scripting
```

Beispiel für eine Protokollmeldung bei Verstößen gegen die Cross-Site Scripting-Sicherheitsprüfung im CEF-Protokollformat:

```
1 Jul 11 00:45:51 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_cross-site scripting\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=4840 method=GET request=http://aaron.
```



```
      stratum8.net/FFC/CreditCardMind.html?abc=%3Cdef%3E msg=\*\*Cross-
      site script check failed for field abc="Bad tag: def"\*\* cn1=133
      cn2=294 cs1=pr_ffc cs2=PPE1 cs3=eUljypvLa0BbabwfGVE52Sewg9U0001 cs4=
      ALERT cs5=2015 act=\*\*not blocked\*\*
<!--NeedCopy-->
```

Beispiel für eine Protokollmeldung von Verstößen gegen die Cross-Site Scripting-Sicherheitsüberprüfung im nativen Protokollformat mit Transformationsaktion

```
Jul 11 01:00:28 <local0.info> 10.217.31.98 07/11/2015:01:00:28 GMT ns
    0-PPE-0 : default APPFW \*\*APPFW_cross-site scripting\*\* 132 0 :
    10.217.253.62 392-PPE0 eUljypvLa0BbabwfGVE52Sewg9U0001 pr_ffc http:
    //aaron.stratum8.net/FFC/login.php?login_name=%3CBOB%3E&passwd=&
    drinking_pref=on &text_area=&loginButton=ClickToLogin&as_sfid=
    AAAAAAVFqmYL68IGvkrcn2pzehjfIkm5E6EZ9FL8YLvIW_41AvAATuKYe9N7uGThSpEAxbb0iBx55j
    -FC4llF \*\*Cross-site script special characters seen in fields <
    transformed>\*\*
<!--NeedCopy-->
```

Greifen Sie mit der GUI auf die Protokollmeldungen zu

Die GUI enthält ein nützliches Tool (Syslog Viewer) zur Analyse der Logmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Application Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Sicherheitsüberprüfungen**. Markieren Sie die Zeile **HTML Cross-Site Scripting** und klicken Sie auf **Protokolle**. Wenn Sie direkt von der HTML-Cross-Site Scripting-Prüfung des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen heraus und zeigt nur die Protokolle an, die sich auf diese Verstöße gegen die Sicherheitsüberprüfung beziehen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt **Prüfmeldungen** auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen ausgelöst werden können.
- Navigieren Sie zu **Application Firewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt Prüfmeldungen auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung.

Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **HTML-Cross-Site**

Scripting-Überprüfung auszuwählen, filtern Sie, indem Sie **APPFW** in der Dropdownliste Optionen für **Modul**auswählen. Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **AppFW_Cross-Site Scripting** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden nur Protokollmeldungen im Syslog-Viewer angezeigt, die sich auf die **Sicherheitsüberprüfungen von HTML Cross-Site Scripting** beziehen.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollnachricht setzen, werden mehrere Optionen wie **Modul**, **Ereignistyp**, **Ereignis-ID**, **Client-IP** usw. unter der Protokollmeldung angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Die Funktion**“Zum Bereitstellen klicken”** ist nur in der GUI verfügbar. Sie können den Syslog Viewer nicht nur zum Anzeigen der Protokolle verwenden, sondern auch zum Bereitstellen der Relaxierungsregeln für das HTML Cross-Site Scripting basierend auf den Protokollmeldungen für Verstöße gegen die Web App Firewall Sicherheitsüberprüfung. Die Protokollmeldungen müssen für diesen Vorgang im CEF-Protokollformat vorliegen. Die Funktion zum Bereitstellen klicken ist nur für Protokollmeldungen verfügbar, die durch die Blockierung (oder nicht Blockierung) generiert wurden. Sie können keine Entspannungsregel für eine Protokollmeldung über den Transformationsvorgang bereitstellen.

Um eine Entspannungsregel aus dem Syslog Viewer bereitzustellen, wählen Sie die Protokollmeldung aus. In der oberen rechten Ecke des Kästchens **Syslog Viewer** der ausgewählten Zeile wird ein Kontrollkästchen angezeigt. Aktivieren Sie das Kontrollkästchen, und wählen Sie dann eine Option aus der Liste **Aktion** aus, um die Entspannungsregel bereitzustellen. **“Bearbeiten und Bereitstellen**”, “ **Bereitstellen**” und “ **Alle bereitstellen** “ sind als **Aktionsoptionen** verfügbar.

Die HTML-Site-Scripting-Regeln, die mithilfe der Option **“Zum Bereitstellen klicken”** bereitgestellt werden, sind die Empfehlungen zur Feinkornentspannung nicht enthalten.

Konfigurieren Sie die Funktion “Click to Deployment” über die GUI

1. Wählen Sie im Syslog Viewer in den **ModuloptionenAPPFW** aus.
2. Wählen Sie das **app_Cross-Site-Scripting** als **Ereignistyp** aus, um die entsprechenden Protokollmeldungen zu filtern.
3. Markieren Sie das Kontrollkästchen, um die auszubringende Regel zu identifizieren.
4. Verwenden Sie die Dropdownliste **Aktion** mit Optionen, um die Entspannungsregel bereitzustellen.
5. Stellen Sie sicher, dass die Regel im entsprechenden Abschnitt zur Entspannungsregel angezeigt wird.

Statistiken für Verstöße gegen das HTML Cross-Site Scripting

Wenn die Statistikaktion aktiviert ist, wird der Zähler für die HTML-Site-Scripting-Prüfung inkrementiert, wenn die Web App Firewall Maßnahmen für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn die Blockaktion beispielsweise aktiviert ist, erhöht die Anforderung für eine Seite, die 3 HTML Cross-Site Scripting Verletzungen enthält, den Statistikzähler um eins, da die Seite gesperrt wird, wenn die erste Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikzähler für Verstöße und die Protokolle um drei, da jeder Verstoß eine separate Protokollnachricht generiert.

Um HTML Cross-Site Scripting anzuzeigen, überprüfen Sie die Statistiken mithilfe der Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
> sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> **stat appfw profile** <profile name>
```

Anzeigen von HTML-Site-Scripting-Statistiken über die GUI

1. Navigieren Sie zu **Sicherheit** > **Anwendungsfirewall > Profile > Statistiken**.
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Bildlaufleiste, um die Statistiken zu Verstößen und Protokollen des HTML-Site-Scripting anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

- **Integrierte Unterstützung für den Schutz vor HTML-Site Scripting-Angriffen**— Die NetScaler Web App Firewall schützt vor Cross-Site Scripting-Angriffen, indem sie eine Kombination aus zulässigen Attributen und Tags überwacht und Muster in der empfangenen Nutzlast verweigert. Alle integrierten standardmäßigen zulässigen Tags, zulässigen Attribute und verweigerten Muster, die von der websiteübergreifenden Skriptprüfung verwendet werden, sind in der Datei /netscaler/default_custom_settings.xml angegeben.
- **Anpassung**— Sie können die Standardliste von Tags, Attributen und Mustern ändern, um die Cross-Site Scripting-Sicherheitsüberprüfung an die spezifischen Anforderungen Ihrer Anwendung anzupassen. Erstellen Sie eine Kopie des Standardsignaturobjekts, ändern Sie vorhandene Einträge oder fügen Sie neue hinzu. Binden Sie dieses Signaturobjekt an Ihr Profil, um die benutzerdefinierte Konfiguration zu nutzen.

- **Hybrides Sicherheitsmodell**— Sowohl Signaturen als auch umfassender Sicherheitsschutz verwenden die SQL/Cross-Site-Scripting-Muster, die in dem Signaturobjekt angegeben sind, das an das Profil gebunden ist. Wenn kein Signaturobjekt an das Profil gebunden ist, werden die im Standardsignaturobjekt vorhandenen SQL/Cross-Site-Scripting-Muster verwendet.
- **Transform**—Beachten Sie Folgendes über den Transformationsvorgang:

Der Transformationsvorgang funktioniert unabhängig von den anderen Einstellungen der Cross-Site Scripting-Aktion. Wenn Transformation aktiviert ist und Block, Protokoll, Statistik und Lernen alle deaktiviert sind, werden Cross-Site-Scripting-Tags transformiert.

Wenn die Blockaktion aktiviert ist, hat sie Vorrang vor der Transformationsaktion.

- **Feinkörnige Entspannung und Lernen**. Optimieren Sie die Entspannungsregel, um eine Teilmenge von Cross-Site-Scripting-Elementen von der Sicherheitsüberprüfung zu lockern, aber den Rest zu erkennen Die Lern-Engine empfiehlt einen bestimmten Werttyp und Wertausdrücke basierend auf den beobachteten Daten.
- **Zum Bereitstellen klicken**— Wählen Sie im Syslog-Viewer eine oder mehrere Cross-Site Scripting -Verletzungsprotokollmeldungen aus und stellen Sie sie als Entspannungsregeln bereit.
- **Charset**—Der Standardzeichensatz für das Profil muss je nach Bedarf der Anwendung festgelegt werden. Standardmäßig ist der Zeichensatz des Profils auf Englisch US (ISO-8859-1) eingestellt. Wenn eine Anforderung ohne den angegebenen Zeichensatz empfangen wird, verarbeitet die Web App Firewall die Anforderung so, als ob es sich um ISO-8859-1 handelt. Das offene Klammerzeichen (<) or the close bracket character (>) wird nicht als Cross-Site-Scripting-Tags interpretiert, wenn diese Zeichen in anderen Zeichensätzen codiert sind. Wenn eine Anforderung beispielsweise eine UTF-8-Zeichenkette “%uff1cscript%uff1e**“**enthält, der Zeichensatz jedoch nicht auf der Anforderungsseite angegeben ist, wird die Cross-Site-Skripterstellungsverletzung möglicherweise nur ausgelöst, wenn der Standardzeichensatz für das Profil als Unicode angegeben ist.

Prüfung auf HTML SQL-Einschleusung

May 11, 2023

Viele Webanwendungen haben Webformulare, die SQL für die Kommunikation mit relationalen Datenbankservern verwenden. Bösartiger Code oder ein Hacker können ein unsicheres Webformular verwenden, um SQL-Befehle an den Webserver zu senden. Die Web App Firewall HTML SQL Injection Check bietet spezielle Schutzmaßnahmen gegen das Einschleusen von nicht autorisiertem SQL-Code, der die Sicherheit verletzen Wenn die Web App Firewall in einer Benutzeranforderung nicht autorisierten SQL-Code erkennt, wandelt sie die Anforderung entweder um, um den SQL-Code inaktiv zu machen, oder blockiert die Anforderung. Die Web App Firewall untersucht die Anforderungsnutzlast für injizierten SQL-Code an drei Orten: 1) POST-Text, 2) Header und 3) Cookies.

Um einen Abfrageteil in Anfragen für injizierten SQL-Code zu untersuchen, konfigurieren Sie bitte eine Einstellung des Anwendungs-Firewall-Profils “InspectQueryContentTypes” für die spezifischen Inhaltstypen.

Ein Standardsatz von Schlüsselwörtern und Sonderzeichen enthält bekannte Schlüsselwörter und Sonderzeichen, die häufig zum Starten von SQL-Angriffen verwendet werden. Sie können neue Muster hinzufügen und den Standardsatz bearbeiten, um die SQL-Prüfung anzupassen. Die Web App Firewall bietet verschiedene Aktionsoptionen für die Implementierung des SQL Injection-Schutzes. Neben den Aktionen **Blockieren**, **Protokollieren**, **Statistiken** und **Lernen** bietet das Web App Firewall Profil auch die Möglichkeit, **SQL-Sonderzeichen umzuwandeln**, um einen Angriff unschädlich zu machen.

Zusätzlich zu den Aktionen gibt es mehrere Parameter, die für die SQL-Einschleusung-Verarbeitung konfiguriert werden können. Sie können nach **SQL-Platzhalterzeichen**suchen. Sie können den SQL-Einschleusung-Typ ändern und eine der 4 Optionen auswählen (**SqlKeyword,**SqlSPLChar****, **SqlSPLCharandKeyword**, **SqlSPLCharorKeyword**), um anzugeben, wie die SQL-Schlüsselwörter und SQL-Sonderzeichen bei der Verarbeitung der Nutzlast ausgewertet werden sollen. Der **Parameter SQL Comments Handling** bietet Ihnen die Möglichkeit, den Typ der Kommentare anzugeben, die bei der Erkennung von SQL Injection überprüft oder ausgenommen werden müssen.

Sie können Entspannungen einsetzen, um Fehlalarme zu vermeiden. Die Lernengine der Web App Firewall kann Empfehlungen zum Konfigurieren von Relaxationsregeln enthalten.

Zum Konfigurieren eines optimierten SQL Injection-Schutzes für Ihre Anwendung stehen folgende Optionen zur Verfügung:

Block—Die Blockaktion wird nur ausgelöst, wenn die Eingabe mit der SQL-Einschleusungstypspezifikation übereinstimmt. Wenn beispielsweise **SQLSplCharAndKeyword** als SQL-Einschleusungstyp konfiguriert ist, wird eine Anforderung nicht blockiert, wenn sie keine Schlüsselwörter enthält, selbst wenn SQL-Sonderzeichen in der Eingabe erkannt werden. Eine solche Anforderung wird blockiert, wenn der SQL-Einschleusungstyp entweder auf **SqlSPLChar**oder **SqlSPLCharorKeyword**festgelegt ist.

Log— Wenn Sie die Protokollfunktion aktivieren, generiert die SQL Injection-Prüfung Protokollmeldungen, die die ausgeführten Aktionen angeben. Wenn die Blockaktion deaktiviert ist, wird für jedes Eingabefeld, in dem der SQL-Verstoß festgestellt wurde, eine separate Protokollmeldung generiert. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. In ähnlicher Weise wird eine Protokollnachricht pro Anforderung für den Transformationsvorgang generiert, auch wenn SQL-Sonderzeichen in mehrere Felder umgewandelt werden. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.

Statistiken— Wenn diese Option aktiviert ist, sammelt die Statistikfunktion Statistiken zu Verstößen und Protokollen. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um zu sehen, ob Sie neue Entspannungsregeln konfigurieren

oder die vorhandenen ändern müssen.

Lernen— Wenn Sie nicht sicher sind, welche SQL-Entspannungsregeln für Ihre Anwendung ideal geeignet sind, können Sie die Lernfunktion verwenden, um basierend auf den erlernten Daten Empfehlungen zu generieren. Die Web App Firewall Learning Engine überwacht den Datenverkehr und gibt auf der Grundlage der beobachteten Werte Empfehlungen zum SQL-Lernen ab. Um einen optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie die Lernoption möglicherweise für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Regeln bereitstellen und das Lernen deaktivieren.

SQL-Sonderzeichen transformieren— Die Web App Firewall berücksichtigt drei Zeichen, einfaches, gerades Anführungszeichen (‘) `(\)`, Backslash und Semikolon (;) als Sonderzeichen für die Verarbeitung der SQL-Sicherheitsprüfung. Die Funktion “SQL Transformation” ändert den SQL-Einschleusung-Code in einer HTML-Anforderung, um sicherzustellen, dass die Anforderung unschädlich gemacht wird. Die geänderte HTML-Anforderung wird dann an den Server gesendet. Alle standardmäßigen Transformationsregeln sind in der Datei /netscaler/default_custom_settings.xml angegeben.

Durch die Transformationsoperation wird der SQL-Code inaktiv, indem die folgenden Änderungen an der Anforderung vorgenommen werden:

- Einfaches gerades Anführungszeichen (‘) bis zum doppelten geraden Anführungszeichen (“).
- Backslash `(\)` zu doppeltem Backslash `(\)`.
- Semikolon (;) wird vollständig verworfen.

Diese drei Zeichen (spezielle Zeichenfolgen) sind notwendig, um Befehle an einen SQL-Server auszugeben. Sofern einem SQL-Befehl keine spezielle Zeichenfolge vorangestellt wird, ignorieren die meisten SQL-Server diesen Befehl. Daher verhindern die Änderungen, die die Web App Firewall bei aktivierter Transformation durchführt, dass ein Angreifer Active SQL injiziert. Nachdem diese Änderungen vorgenommen wurden, kann die Anfrage sicher an Ihre geschützte Website weitergeleitet werden. Wenn Webformulare auf Ihrer geschützten Website legitim spezielle SQL-Zeichenfolgen enthalten können, die Webformulare jedoch nicht auf die speziellen Zeichenfolgen angewiesen sind, um ordnungsgemäß zu funktionieren, können Sie die Blockierung deaktivieren und die Transformation aktivieren, um das Blockieren legitimer Webformulardaten zu verhindern, ohne den Schutz zu verringern, den Web App Firewall Ihren geschützten Websites bietet.

Die Transformationsoperation funktioniert unabhängig von der Einstellung des **SQL-Injection-Typs** . Wenn die Transformation aktiviert ist und der SQL Injection-Typ als SQL-Schlüsselwort angegeben wird, werden SQL-Sonderzeichen auch dann transformiert, wenn die Anforderung keine Schlüsselwörter enthält.

> **Tipp**
>
> Normalerweise aktivieren Sie entweder die Transformation oder das Blockieren, aber nicht

> beide. Wenn die Blockaktion aktiviert ist, hat sie Vorrang vor der Transformationsaktion. Wenn Sie die Blockierung aktiviert haben, ist die Aktivierung der Transformation redundant.

Auf SQL-Platzhalterzeichen suchen — Wildcard-Zeichenkönnen verwendet werden, um die Auswahl einer SQL-Anweisung (SQL-SELECT) zu erweitern. Diese Wildcard-Operatoren können mit den Operatoren **LIKE** und **NOT LIKE** verwendet werden, um einen Wert mit ähnlichen Werten zu vergleichen. Die Prozentzeichen (%) und Unterstriche (_) werden häufig als Platzhalter verwendet. Das Prozentzeichen entspricht dem Sternchen-Platzhalterzeichen (*), das mit MS-DOS verwendet wird, und entspricht null, einem oder mehreren Zeichen in einem Feld. Der Unterstrich ähnelt dem MS-DOS-Fragezeichen (?) Platzhalterzeichen. Es stimmt mit einer einzelnen Zahl oder einem Zeichen in einem Ausdruck überein.

Sie können beispielsweise die folgende Abfrage verwenden, um eine Zeichenfolgensuche durchzuführen, um alle Kunden zu finden, deren Namen das D-Zeichen enthalten.

WÄHLEN Sie* vom Kunden WHERE-Namen wie “%D%”:

Im folgenden Beispiel werden die Operatoren kombiniert, um Gehaltswerte zu finden, die an zweiter und dritter Stelle 0 haben.

WÄHLEN Sie* vom Kunden WHERE Gehalt wie ‘_ 00% ‘:

Verschiedene DBMS-Anbieter haben die Platzhalterzeichen um zusätzliche Operatoren erweitert. Die NetScaler Web App Firewall kann vor Angriffen schützen, die durch das Eingeben dieser Platzhalterzeichen gestartet werden. Die 5 standardmäßigen Platzhalterzeichen sind Prozent (%), Unterstrich (_), Caret (^), öffnende Klammer ([) und schließende Klammer (]). Dieser Schutz gilt sowohl für HTML- als auch für XML-Profile.

Die Standard-Platzhalterzeichen sind eine Liste von Literalen, die in der ***Standardsignaturen angegeben sind**:

- `<wildchar type=” LITERAL” >%</wildchar>`
- `<wildchar type=” LITERAL” >_</wildchar>`
- `<wildchar type=” LITERAL” >^</wildchar>`
- `<wildchar type=” LITERAL” >[</wildchar>`
- `<wildchar type=” LITERAL” >]</wildchar>`

Platzhalterzeichen in einem Angriff können PCRE sein, wie [^A-F]. Die Web App Firewall unterstützt auch PCRE-Platzhalter, aber die obigen Platzhalterzeichen reichen aus, um die meisten Angriffe zu blockieren.

> **Hinweis:**
>
> Die SQL-Platzhalterzeichenprüfung unterscheidet sich von der SQL-Sonderzeichenprüfung. Diese Option muss mit Vorsicht verwendet werden, um Fehlalarme zu vermeiden.

Check Request mit SQL-Einschleusung-Typ— Die Web App Firewall bietet 4 Optionen, um die gewünschte Strenge für die SQL Injection-Prüfung basierend auf den individuellen Anforderungen

der Anwendung zu implementieren. Die Anforderung wird mit der Spezifikation des Injektionstyps zur Erkennung von SQL-Verletzungen abgeglichen. Die 4 Optionen für den SQL-Einschleusung-Typ sind:

- **SQL-Sonderzeichen und -Schlüsselwort**— Sowohl ein SQL-Schlüsselwort als auch ein SQL-Sonderzeichen müssen in der Eingabe vorhanden sein, um eine SQL-Verletzung auszulösen. Diese am wenigsten restriktive Einstellung ist auch die Standardeinstellung.
- **SQL-Sonderzeichen**—Mindestens eines der Sonderzeichen muss in der Eingabe vorhanden sein, um eine SQL-Verletzung auszulösen.
- **SQL-Schlüsselwort**— Mindestens eines der angegebenen SQL-Schlüsselwörter muss in der Eingabe vorhanden sein, um eine SQL-Verletzung auszulösen. Wählen Sie diese Option nicht ohne angemessene Berücksichtigung aus. Um Fehlalarme zu vermeiden, stellen Sie sicher, dass keines der Schlüsselwörter in den Eingaben erwartet wird.
- **SQL-Sonderzeichen oder Schlüsselwort**— Entweder das Schlüsselwort oder die Sonderzeichenfolge müssen in der Eingabe vorhanden sein, um die Sicherheitsüberprüfung auszulösen.

> **Tipp:**
>
> Wenn Sie die Web App Firewall so konfigurieren, dass sie nach Eingaben suchen, die ein SQL-Sonderzeichen enthalten, überspringt die Web App-Firewall Webformularfelder, die keine Sonderzeichen enthalten. Da die meisten SQL-Server keine SQL-Befehle verarbeiten, denen kein Sonderzeichen vorangestellt ist, kann die Aktivierung dieser Option die Web App Firewall erheblich entlasten und die Verarbeitung beschleunigen, ohne dass Ihre geschützten Websites gefährdet werden.

Verarbeitung von SQL-Kommentaren— Standardmäßig prüft die Web App Firewall alle SQL-Kommentare auf injizierte SQL-Befehle. Viele SQL-Server ignorieren jedoch alles in einem Kommentar, auch wenn ein SQL-Sonderzeichen vorangestellt ist. Für eine schnellere Verarbeitung, wenn Ihr SQL-Server Kommentare ignoriert, können Sie die Web App Firewall so konfigurieren, dass Kommentare übersprungen werden, wenn Sie Anforderungen für injiziertes SQL prüfen. Die Optionen für die Verarbeitung von SQL-Kommentaren sind:

- **ANSI**—Überspringt SQL-Kommentare im ANSI-Format, die normalerweise von UNIX-basierten SQL-Datenbanken verwendet werden. Zum Beispiel:
  - — (Zwei Bindestriche) - Dies ist ein Kommentar, der mit zwei Bindestrichen beginnt und mit Zeilenende endet.
  - {} - Klammern (Klammern umschließen den Kommentar. Das {steht vor dem Kommentar und das} folgt ihm. Klammern können ein- oder mehrzeilige Kommentare abgrenzen, Kommentare können jedoch nicht verschachtelt werden)
  - `/**/: C style comments (Does not allow nested comments). Please note /*! <comment that begin with slash followed by asterisk and exclamation mark is not a comment > */`
  - MySQL Server unterstützt einige Varianten von Kommentaren im C-Stil. Diese ermöglichen

es Ihnen, Code zu schreiben, der MySQL Erweiterungen enthält, aber immer noch portabel ist, indem Sie Kommentare der folgenden Form verwenden: `/*! MySQL-specific code */`

  - . #: Mysql-Kommentare: Dies ist ein Kommentar, der mit dem Zeichen # beginnt.

- **Verschachtelt**— Verschachtelte SQL-Kommentare überspringen, die normalerweise von Microsoft SQL Server verwendet werden. Zum Beispiel; — (Zwei Bindestriche) und **/* */** (Erlaubt verschachtelte Kommentare)
- **ANSI/verschachtelt**—Überspringen Sie Kommentare, die sowohl den ANSI- als auch den verschachtelten SQL-Kommentarstandards entsprechen. Kommentare, die nur dem ANSI-Standard oder nur dem verschachtelten Standard entsprechen, werden weiterhin auf injizierte SQL überprüft.
- **Alle Kommentare überprüfen**— Überprüfen Sie die gesamte Anforderung für injiziertes SQL, ohne etwas zu überspringen. Dies ist die Standardeinstellung.

> **Tipp**
>
> Normalerweise dürfen Sie die Option Verschachtelt oder ANSI/Verschachtelt nicht wählen, es sei denn, Ihre Back-End-Datenbank wird auf Microsoft SQL Server ausgeführt. Die meisten anderen Typen von SQL Server-Software erkennen verschachtelte Kommentare nicht. Wenn verschachtelte Kommentare in einer Anfrage erscheinen, die an einen anderen SQL-Servertyp gerichtet ist, deuten sie möglicherweise auf einen Versuch hin, die Sicherheit auf diesem Server zu verletzen.

Request-Header prüfen— Aktivieren Sie diese Option, wenn Sie nicht nur die Eingabe in den Formularfeldern untersuchen, sondern auch die Anforderungsheader auf HTML-SQL-Einschleusung-Angriffe untersuchen möchten. Wenn Sie die GUI verwenden, können Sie diesen Parameter im Bereich **Erweiterte Einstellungen** -> **Profileinstellungen** des Web App Firewall Profils aktivieren.

> **Hinweis:**
>
> Wenn Sie das Header-Flag “Anforderung prüfen” aktivieren, müssen Sie möglicherweise eine Entspannungsregel für den **User-Agent-Header** konfigurieren. Das Vorhandensein des SQL-Schlüsselworts **like** und des SQL-Sonderzeichens Semikolon (**;**) kann falsch positive und Blockanforderungen auslösen, die diesen Header enthalten.
>
> **Warnung**
>
> Wenn Sie sowohl die Überprüfung des Anforderungsheaders als auch die Transformation aktivieren, werden alle SQL-Sonderzeichen in den Kopfzeilen ebenfalls transformiert. Die Header Accept, Accept-Charset, Accept-Encoding, Accept-Language, Expect und User-Agent enthalten normalerweise Semikolons (;). Die gleichzeitige Aktivierung von Request-Header-Überprüfung und Transformation kann zu Fehlern führen

inspectQueryContentTypes — Konfigurieren Sie diese Option, wenn Sie den Teil der Anforderungsabfrage auf SQL-Einschleusung-Angriffe auf bestimmte Inhaltstypen untersuchen

möchten. Wenn Sie die GUI verwenden, können Sie diesen Parameter im Bereich **Erweiterte Einstellungen** -> **Profileinstellungen** des App Firewall-Profils konfigurieren.

SQL Feinkörnige Entspannungen

Die Web App Firewall bietet Ihnen die Möglichkeit, ein bestimmtes Formularfeld, einen Header oder ein Cookie von der SQL Injection-Prüfung auszunehmen. Sie können die Prüfung für eines oder mehrere dieser Felder vollständig Bypass, indem Sie die Entspannungsregeln für die SQL Injection-Prüfung konfigurieren.

Mit der Web App Firewall können Sie durch Feinabstimmung der Entspannungsregeln strengere Sicherheit implementieren. Eine Anwendung erfordert möglicherweise die Flexibilität, um bestimmte Muster zuzulassen, aber die Konfiguration einer Relaxationsregel zum Umgehen der Sicherheitsprüfung kann die Anwendung anfällig für Angriffe machen, da das Zielfeld von der Prüfung auf SQL-Angriffsmuster ausgenommen ist. Die feinkörnige SQL-Entspannung bietet die Möglichkeit, bestimmte Muster zuzulassen und den Rest zu blockieren. Beispielsweise verfügt die Web App Firewall derzeit über einen Standardsatz von mehr als 100 SQL-Schlüsselwörtern. Da Hacker diese Schlüsselwörter in SQL Injection-Angriffen verwenden können, kennzeichnet die Web App Firewall sie als potenzielle Bedrohungen. Sie können ein oder mehrere Keywords entspannen, die für den bestimmten Standort als sicher gelten. Die restlichen potenziell gefährlichen SQL-Schlüsselwörter werden weiterhin auf den Zielspeicherort überprüft und lösen weiterhin die Sicherheitsüberprüfungsverstöße aus. Sie haben jetzt eine viel strengere Kontrolle.

Die in Relaxationen verwendeten Befehle haben optionale Parameter für **Werttyp** und **Wertausdruck**. Sie können angeben, ob der Wertausdruck ein regulärer Ausdruck oder eine literale Zeichenfolge ist. Der Werttyp kann leer gelassen werden oder Sie haben die Möglichkeit, **Keyword** oder **SpecialString** oder **WildChar** auszuwählen.

> **Warnung:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen- oder Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht möchten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder einen Angriff zulassen, den die HTML SQL Injection-Prüfung sonst blockiert hätte.

Zu berücksichtigende Punkte:

- Der Wertausdruck ist ein optionales Argument. Ein Feldname hat möglicherweise keinen Wertausdruck.
- Ein Feldname kann an Ausdrücke mit mehreren Werten gebunden werden.

- Wertausdrücken muss ein Werttyp zugewiesen werden. Der SQL-Werttyp kann sein: 1) Schlüsselwort, 2) SpecialString oder 3) WildChar.
- Sie können mehrere Entspannungsregeln pro Feldname/URL-Kombination festlegen.

Verwenden der Befehlszeile zum Konfigurieren der SQL Injection Check

So konfigurieren Sie SQL Injection-Aktionen und andere Parameter mithilfe der Befehlszeile:

In der Befehlszeilenschnittstelle können Sie entweder den Befehl **set appfw profile** oder den Befehl **add appfw profile** verwenden, um den SQL Injection-Schutz zu konfigurieren. Sie können die Block-, Learn-, Log-Aktionen und Statistiken aktivieren und angeben, ob Sie die in SQL Injection-Angriffszeichenfolgen verwendeten Sonderzeichen transformieren möchten, um den Angriff zu deaktivieren. Wählen Sie den Typ des SQL-Angriffsmusters (Schlüsselwörter, Platzhalterzeichen, spezielle Zeichenfolgen) aus, den Sie in den Payloads erkennen möchten, und geben Sie an, ob die Web App Firewall auch die Anforderungskopfzeilen auf Verletzungen von SQL Injection überprüfen soll. Verwenden Sie den Befehl **unset appfw profile**, um die konfigurierten Einstellungen auf ihre Standardeinstellungen zurückzusetzen. Jeder der folgenden Befehle legt nur einen Parameter fest, aber Sie können mehrere Parameter in einen einzelnen Befehl aufnehmen:

- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -SQLInjectionAction ([block] [learn] [log] [stats])| [none])
- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -SQLInjectionTransformSpecialChars (**ON** | OFF)
- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -**SQLInjectionCheckSQLWildChars** (**ON** |**OFF**)
- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- **<name> -**SQLInjectionType** ([**SQLKeyword**] | [**SQLSplChar**] | [**SQLSplCharANDKeyword**] | [**SQLSplCharORKeyword**])
- **legen Sie das Anwendungs-Firewall-Profil** fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -**SQLInjectionParseComments** ([**checkall**] | [**ansi|nested **] | [**ansinested**])
- **legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -CheckRequestHeaders (ON | OFF) Parameterbeschreibungen unten auf der Seite.
- <name> - CheckRequestQueryNonHtml (ON | OFF) Parameterbeschreibungen unten

auf der Seite.

So konfigurieren Sie eine SQL Injection-Entspannungsregel mit der Befehlszeilenschnittstelle

Verwenden Sie den Befehl bind oder unbind, um die Bindung wie folgt hinzuzufügen oder zu löschen:

- `bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor|SpecialString|Wildchar)[<valueExpression>][-isValueRegex (REGEX | NOTREGEX)]]`
- `unbind appfw profile <name> -SQLInjection <String> <formActionURL> [-location <location>] [-valueTyp (Keyword|SpecialString|Wildchar)[<valueExpression>]]`

> **Hinweis:**
>
> Sie können die Liste der SQL-Schlüsselwörter aus dem Inhalt der Standardsignaturdatei finden, indem Sie das View-Signaturobjekt anzeigen, das eine Liste von SQL-Schlüsselwörtern und SQL-Sonderzeichen enthält.

Verwenden der GUI zum Konfigurieren der SQL Injection Security Check

In der GUI können Sie die Sicherheitsüberprüfung von SQL Injection im Bereich für das mit Ihrer Anwendung verknüpfte Profil konfigurieren.

So konfigurieren oder ändern Sie die SQL Injection-Prüfung mit der GUI

1. Navigieren Sie zu **Application Firewall > Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

In der Tabelle zur Sicherheitsüberprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsüberprüfungen angezeigt. Sie haben 2 Möglichkeiten für die Konfiguration:

a. Wenn Sie Block-, Log-, Statistiken- und Lernaktionen für HTML SQL Injection aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf **OK**klicken und dann auf **Speichern und Schließen** klicken, um den Bereich **Sicherheitsprüfung** zu schließen.

b. Wenn Sie weitere Optionen für diese Sicherheitsprüfung konfigurieren möchten, doppelklicken Sie auf HTML SQL Injection oder wählen Sie die Zeile aus und klicken Sie auf **Aktionseinstellungen**, um die folgenden Optionen anzuzeigen:

SQL-Sonderzeichentransformieren —Transformieren Sie alle SQL-Sonderzeichen in der Anforderung.

Suchen Sie nach SQL-Platzhalterzeichen— Betrachten Sie SQL-Platzhalterzeichen in der Payload als Angriffsmuster.

Überprüfen Sie die Anforderung mit—Type der SQL-Einschleusung (SqlKeyword, SqlSplChar, SqlSplcharandKeyword oder SqlSplcharorKeyword), die überprüft werden soll.

SQL Comments Handling— Art der zu prüfenden Kommentare (Alle Kommentare prüfen, ANSI, Verschachtelt oder ANSI/verschachtelt).

Nachdem Sie eine der obigen Einstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsüberprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern und schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

So konfigurieren Sie eine Regel zur Entspannung von SQL Injection über die GUI

- Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
- Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
- Doppelklicken Sie in der Tabelle Entspannungsregeln auf den Eintrag " **HTML SQL Injection** " oder wählen Sie ihn aus und klicken Sie auf **Bearbeiten**.
- Führen **Sie im Dialogfeld "Entspannungsregeln für HTML SQL Injection** " Vorgänge zum **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren**oder **Deaktivieren** für Entspannungsregeln aus.

> **Hinweis**
>
> Wenn Sie eine neue Regel hinzufügen, wird das Feld **Wertausdruck** nur angezeigt, wenn Sie im Feld **Werttyp** die Option **Schlüsselwort** oder **SpecialString** oder **WildChar** auswählen.

So verwalten Sie Regeln zur Entspannung von SQL-Einschleusung mit dem Visualizer

Um eine konsolidierte Ansicht aller Relaxationsregeln zu erhalten, können Sie die Zeile **HTML SQL Injection** markieren und auf **Visualizer** klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine vorhandene zu **bearbeiten** . Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

Anzeigen oder Anpassen von Einschleusungsmustern über die grafische Benutzeroberfläche

Sie können die GUI verwenden, um die Einschleusungsmuster anzuzeigen oder anzupassen.

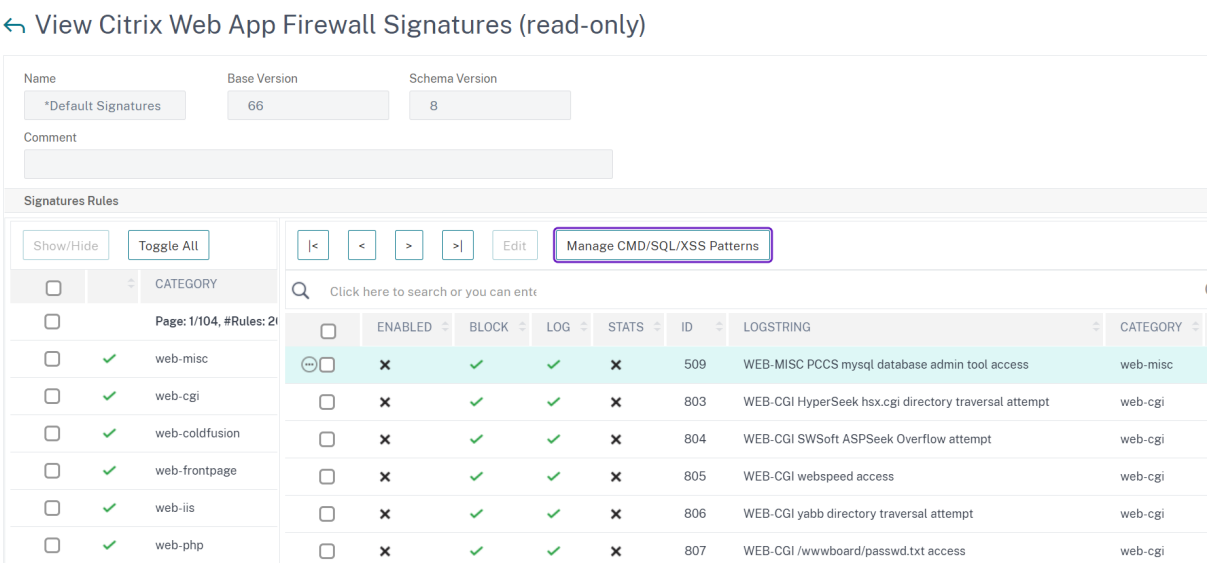
Die Standard-SQL-Muster sind in der Standardsignaturdatei angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, werden die im Standardsignaturobjekt angegebenen Standard-Injection-Pattern

vom Profil für die Verarbeitung der Sicherheitsprüfung des Befehls verwendet. Die im Standardsignaturobjekt angegebenen Regeln und Muster sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese Muster ändern oder ändern möchten, erstellen Sie eine Kopie des Standardobjekts sSignatures, um ein benutzerdefiniertes Signaturobjekt zu erstellen. Nehmen Sie Änderungen an den Befehlseinschleusungsmustern im neuen benutzerdefinierten Signaturobjekt vor und verwenden Sie dieses Signaturobjekt in Ihrem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten Muster verwenden möchten.

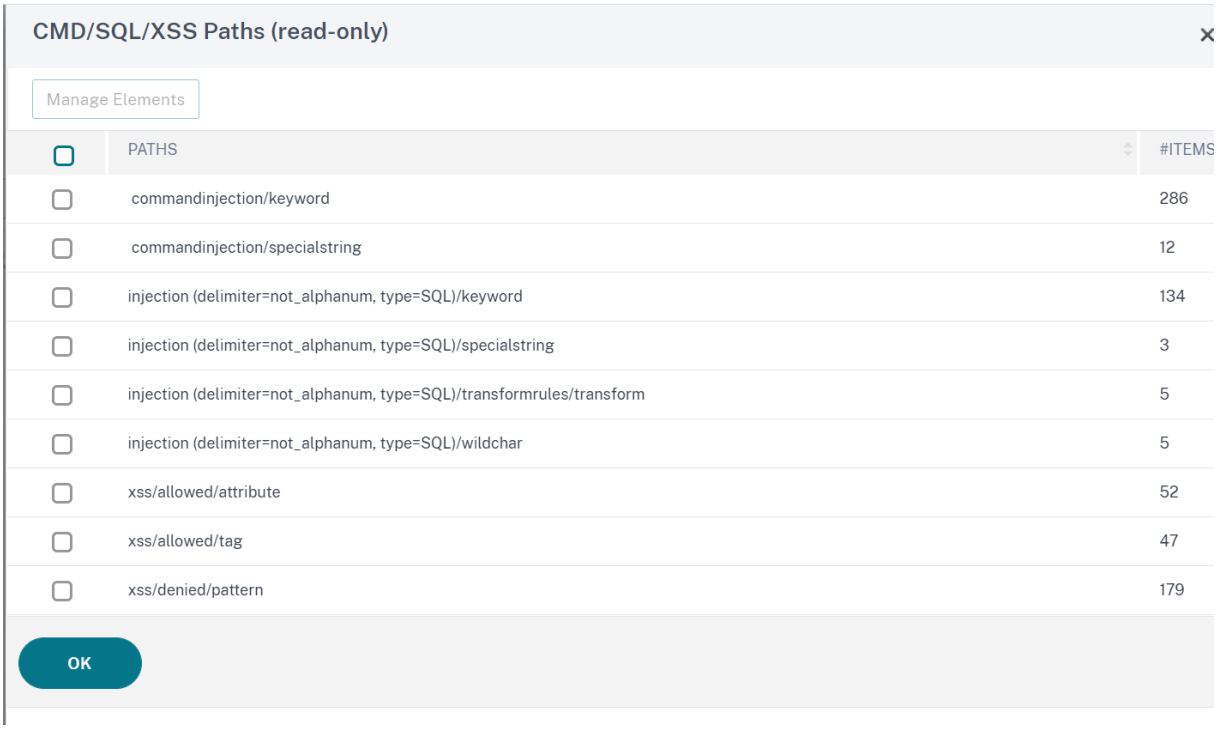
Weitere Informationen finden Sie unter Signaturen

So zeigen Sie die Standard-Einschleusungsmuster mit der GUI an:

1. Navigieren Sie zu **Application Firewall > Signaturen**, wählen Sie ***Standardsignaturen**aus und klicken Sie auf **Bearbeiten**.



1. Klicken Sie auf **CMD/SQL/XSS-Muster verwalten**. Die Tabelle **SQL/Cross-Site-Skriptpfade verwalten** zeigt Muster in Bezug auf CMD/SQL/XS-Einschleusung:



1. Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden Einschleusungsmuster (Schlüsselwörter, spezielle Zeichenfolgen, Transformationsregeln oder die Platzhalterzeichen) anzuzeigen, die von der Injection-Prüfung des Befehls Web App Firewall verwendet werden.

Verwenden der Lernfunktion mit der SQL Injection Check

Wenn die Lernaktion aktiviert ist, überwacht die Web App Firewall Learning Engine den Datenverkehr und lernt die ausgelösten Verstöße. Sie können diese gelernten Regeln regelmäßig überprüfen. Nach entsprechender Prüfung können Sie die gelernte Regel als eine Relaxierungsregel für SQL-Einschleusung bereitstellen.

SQL Injection Learning Enhancement— Eine Lernerweiterung für die Web App Firewall wurde in Version 11.0 der NetScaler Software eingeführt. Um eine feinkörnige SQL Injection-Entspannung bereitzustellen, bietet die Web App Firewall feinkörniges SQL Injection-Lernen. Die Lern-Engine gibt Empfehlungen bezüglich des beobachteten Werttyps (Schlüsselwort, SpecialString, Wildchar) und des entsprechenden Value-Ausdrucks, der in den Eingabefeldern beobachtet wird. Zusätzlich zur Überprüfung der blockierten Anforderungen, um festzustellen, ob die aktuelle Regel zu restriktiv ist und gelockert werden muss, können Sie die von der Lern-Engine generierten Regeln überprüfen, um festzustellen, welcher Werttyp und welcher Werteausdruck Verstöße auslösen und in den Relaxationsregeln behandelt werden müssen.

> **Wichtig**
>
> Die Lern-Engine der Web App Firewall kann nur die ersten 128 Byte des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen enthält, die für die ersten 128 Bytes übereinstimmen, kann die Lern-Engine möglicherweise nicht zwischen ihnen unterscheiden. In ähnlicher Weise kann die bereitgestellte Relaxationsregel versehentlich alle Felder von der SQL Injection Inspektion entspannen.
>
> **Hinweis** Um das SQL zu Bypass, indem Sie den User-Agent-Header einchecken, verwenden Sie die folgende Entspannungsregel:
>
> ```
> bind appfw profile your_profile_name -SQLInjection User-Agent ".*"-
> location HEADER
> ```

So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `show appfw learningdata <profilename> SQLInjection`
- `rm appfw learningdata <profilename> -SQLInjection <string> <formActionURL > [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> SQLInjection`

So zeigen Sie erlernte Daten mit der GUI an oder verwenden sie

1. Navigieren Sie zu **Application Firewall > Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **“Erweiterte Einstellungen** “ auf **Gelernte Regeln**. Sie können den Eintrag **HTML SQL Injection** in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die erlernten Regeln zuzugreifen. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Entspannungsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

Sie haben auch die Möglichkeit, eine zusammengefasste Ansicht der gelernten Entspannungen anzuzeigen, indem Sie den Eintrag **HTML SQL Injection** in der Tabelle Learned Rules auswählen und auf **Visualizer** klicken, um eine konsolidierte Ansicht aller gelernten Verletzungen zu erhalten. Der Visualizer macht es einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Ergreifen einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke empfohlen werden, um mehrere Regeln zu konsolidieren. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Zahl aus einer Dropdown-Liste auswählen. Der Visualizer für erlernte Regeln

bietet die Möglichkeit, die Regeln zu bearbeiten und als Entspannungen einzusetzen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Verwenden der Protokollfunktion mit der SQL Injection Check

Wenn die Protokollaktion aktiviert ist, werden die Verletzungen der Sicherheitsüberprüfung von HTML SQL Injection als **APPFW_SQL-Verletzungen** im Überwachungsprotokoll protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und schließen Sie die ns.logs im Ordner **/var/log/**, um auf die Protokollmeldungen zuzugreifen, die sich auf die SQL Injection-Verstöße beziehen:

```
> Shell
```

```
## tail -f /var/log/ns.log | grep APPFW_SQL
```

Beispiel für eine HTML SQL Injection-Protokollmeldung, wenn die Anforderung transformiert wird

```
1 Jun 26 21:08:41 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
      .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=54001
       method=GET request=http://aaron.stratum8.net/FFC/login.php?
      login_name=%27+or&passwd=and+%3B&drinking_pref=on&text_area=select
      +*+from+%5C+%3B&loginButton=ClickToLogin&as_sfid=AAAAAAXjnGN5gLH-
      hvhTOpIySEIqES7BjFRs5Mq0fwPp-3ZHDi5yWlRWByj0cVbMyy-
      Ens2vaaiULKOcUri4OD4kbXWwSY5s7I3QkDsrvIgCYMC9BMvBwY2wbNcSqCwk52lfE0k
      %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c msg= Special
      characters seen in fields cn1=74 cn2=762 cs1=pr_ffc cs2=PPE1 cs3=9
      ztIlf9p1H7p6Xtzn6NMygTv/QM0002 cs4=ALERT cs5=2015 act=transformed
2 <!--NeedCopy-->
```

Beispiel für eine HTML SQL Injection-Protokollmeldung, wenn die Post-Anforderung blockiert ist

```
1 Jun 26 21:30:34 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
      .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=9459
      method=POST request=http://aaron.stratum8.net/FFC/login_post.php msg
      =SQL Keyword check failed for field text_area="(')" cn1=78 cn2=834
      cs1=pr_ffc cs2=PPE1 cs3=eVJMMPtZ2XgylGrHjkx3rZLfBCI0002 cs4=ALERT
      cs5=2015 act=blocked
2 <!--NeedCopy-->
```

> **Hinweis**
>
> Im Rahmen der Streaming-Änderungen in 10.5.e Builds (Enhancement Builds) und 11.0 Build

> on wards verarbeiten wir die Eingabedaten jetzt in Blöcken. RegEx Pattern-Matching ist jetzt für zusammenhängende Zeichenfolgen auf 4K beschränkt. Mit dieser Änderung können die SQL-Verstoßprotokollmeldungen andere Informationen im Vergleich zu früheren Builds enthalten. Das Schlüsselwort und das Sonderzeichen in der Eingabe können durch viele Bytes getrennt werden. Wir behalten nun den Überblick über die SQL-Schlüsselwörter und spezielle Zeichenfolgen bei der Verarbeitung der Daten, anstatt den gesamten Eingabewert zu puffern. Zusätzlich zum Feldnamen enthält die Protokollnachricht jetzt das SQL-Schlüsselwort oder das SQL-Sonderzeichen oder sowohl das SQL-Schlüsselwort als auch das SQL-Sonderzeichen, wie in der konfigurierten Einstellung festgelegt. Der Rest der Eingabe ist nicht mehr in der Protokollnachricht enthalten, wie im folgenden Beispiel gezeigt:
>
> **Beispiel:**
>
> Wenn die Web App Firewall die SQL-Verletzung erkennt, wird in 10.5 möglicherweise die gesamte Eingabezeichenfolge in die Protokollmeldung aufgenommen, wie unten dargestellt:
>
> ```
> SQL Keyword check failed for field text=\"select a name from testbed1
> ;(;)\".*<blocked>
> ```
>
> In den Erweiterungs-Builds von 10.5.e, die anforderungsseitiges Streaming und ab Build 11.0, protokollieren wir nur den Feldnamen, das Schlüsselwort und das Sonderzeichen (falls zutreffend) in der Protokollnachricht, wie unten gezeigt:
>
> ```
> SQL Keyword check failed for field **text="select(;)"<blocked>
> ```
>
> Diese Änderung gilt für Anforderungen, die Anwendung/x-www-form-urlencodedoder Multipart/Form-Daten oder Text-/x-gwt-rpc Inhaltstypen enthalten. Protokollmeldungen, die während der Verarbeitung von **JSON** - oder **XML-Nutzdaten** generiert werden, sind von dieser Änderung nicht betroffen.

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die GUI enthält ein nützliches Tool (**Syslog Viewer**) zur Analyse der Logmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Application Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Sicherheitsüberprüfungen**. Markieren Sie die Zeile **HTML SQL Injection**, und klicken Sie auf **Protokolle** Wenn Sie direkt von der HTML-SQL-Einschleusung-Prüfung des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen heraus und zeigt nur die Protokolle an, die zu diesen Verstößen gegen die Sicherheitsüberprüfung gehören.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Prüfmeldungen auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen

ausgelöst werden können.

- Navigieren Sie zu **Application Firewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt Prüfmeldungen auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung.

Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **HTML-SQL-Einschleusung-Prüfung** auszuwählen, filtern Sie, indem Sie **APPFW** in der Dropdownliste auswählen Optionen für **Module**. Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_SQL** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog-Viewer nur Protokollmeldungen angezeigt, die zu den Verletzungen der **SQL Injection-Sicherheitsüberprüfung** gehören.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollnachricht setzen, werden mehrere Optionen wie **Modul**, **Ereignistyp**, **Ereignis-ID**, **Client-IP** usw. unterhalb der Protokollmeldung angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Die Funktion**“Zum Bereitstellen klicken”** ist nur in der GUI verfügbar. Sie können den Syslog-Viewer nicht nur zum Anzeigen der Protokolle verwenden, sondern auch zum Bereitstellen von Entspannungsregeln für HTML SQL Injection basierend auf den Protokollmeldungen für Verstöße gegen die Sicherheitsüberprüfung der Web App Firewall. Die Protokollmeldungen müssen für diesen Vorgang im CEF-Protokollformat vorliegen. Die Funktion zum Bereitstellen klicken ist nur für Protokollmeldungen verfügbar, die durch die Blockierung (oder nicht Blockierung) generiert wurden. Sie können keine Entspannungsregel für eine Protokollmeldung über den Transformationsvorgang bereitstellen.

Um eine Entspannungsregel aus dem Syslog Viewer bereitzustellen, wählen Sie die Protokollmeldung aus. In der oberen rechten Ecke des Kästchens **Syslog Viewer** der ausgewählten Zeile wird ein Kontrollkästchen angezeigt. Aktivieren Sie das Kontrollkästchen, und wählen Sie dann eine Option aus der Liste Aktion aus, um die Entspannungsregel bereitzustellen. **“Bearbeiten und Bereitstellen**”, “ **Bereitstellen**” und “ **Alle bereitstellen** “ sind als **Aktionsoptionen** verfügbar.

Die SQL-Einschleusung-Regeln, die mithilfe der Option “Zum Bereitstellen klicken” bereitgestellt werden, sind die Empfehlungen zur Feinkornentspannung nicht enthalten.

So verwenden Sie die Click-to-Deploy-Funktion in der GUI:

1. Wählen Sie im Syslog Viewer in den **Moduloptionen** die Option **Anwendungsfirewall** aus.
2. Wählen Sie **APP_SQL** als **Ereignistyp** aus, um die entsprechenden Protokollmeldungen zu filtern.
3. Markieren Sie das Kontrollkästchen, um die auszubringende Regel zu identifizieren.
4. Verwenden Sie die Dropdownliste **Aktion** mit Optionen, um die Entspannungsregel bereitzustellen.

5. Stellen Sie sicher, dass die Regel im entsprechenden Abschnitt zur Entspannungsregel angezeigt wird.

Statistiken für die SQL Injection Verstöße

Wenn die Statistikaktion aktiviert ist, wird der Zähler für die SQL Injection-Prüfung inkrementiert, wenn die Web App Firewall Maßnahmen für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Blockaktion aktiviert ist, erhöht die Anforderung für eine Seite, die 3 SQL-Einschleusung-Verletzungen enthält, den Statistikzähler um eins, da die Seite blockiert wird, sobald die erste Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikzähler für Verstöße und die Protokolle um drei, da jeder Verstoß eine separate Protokollnachricht generiert.

So zeigen Sie SQL Injection-Prüfstatistiken mit der Befehlszeile an:

Geben Sie in der Befehlszeile Folgendes ein:

> **sh appfw Statistiken**

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> stat appfw profile <profile name>
```

So zeigen Sie HTML SQL Injection-Statistiken mit der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Anwendungsfirewall**.
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Bildlaufleiste, um die Statistiken über Verstöße und Protokolle von HTML SQL Injection anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

Beachten Sie die folgenden Punkte zur Prüfung von SQL Injection:

- **Integrierte Unterstützung für den Schutz von SQL Injection**— Die NetScaler Web App Firewall schützt vor SQL Injection, indem sie eine Kombination aus SQL-Schlüsselwörtern und Sonderzeichen in den Formularparametern überwacht Alle SQL-Schlüsselwörter, Sonderzeichen, Platzhalterzeichen und Standardtransformationsregeln werden in der Datei /netscaler/default_custom_settings.xml angegeben.
- **Anpassung**: Sie können die Standardschlüsselwörter, Sonderzeichen, Platzhalterzeichen und Transformationsregeln ändern, um die Überprüfung der SQL-Sicherheitsprüfung an die spezifischen Anforderungen Ihrer Anwendung anzupassen. Erstellen Sie eine Kopie des Standardsig-

naturobjekts, ändern Sie vorhandene Einträge oder fügen Sie neue hinzu. Binden Sie dieses Signaturobjekt an Ihr Profil, um die benutzerdefinierte Konfiguration zu nutzen.

- **Hybrides Sicherheitsmodell**— Sowohl Signaturen als auch umfassender Sicherheitsschutz verwenden die SQL/Cross-Site-Scripting-Muster, die in dem Signaturobjekt angegeben sind, das an das Profil gebunden ist. Wenn kein Signaturobjekt an das Profil gebunden ist, werden die im Standardsignaturobjekt vorhandenen SQL/Cross-Site-Scripting-Muster verwendet.
- **Transform**—Beachten Sie Folgendes über den Transformationsvorgang:
  - Der Transformationsvorgang funktioniert unabhängig von den anderen SQL Injection-Aktionseinstellungen. Wenn die Transformation aktiviert ist und Block, Log, Statistiken und Lernen alle deaktiviert sind, werden SQL-Sonderzeichen transformiert.
  - Wenn SQL Transformation aktiviert ist, werden Benutzeranfragen an die Back-End-Server gesendet, nachdem die SQL-Sonderzeichen im Nicht-Blockmodus transformiert wurden. Wenn die Blockaktion aktiviert ist, hat sie Vorrang vor der Transformationsaktion. Wenn der Einschleusungstyp als SQL-Sonderzeichen angegeben ist und der Block aktiviert ist, wird die Anforderung trotz der Transformationsaktion blockiert.
- **Fine Grained Relaxation and Learning**— Optimieren Sie die Entspannungsregel, um eine Teilmenge von SQL-Elementen aus der Sicherheitskontrolle zu entspannen, aber den Rest zu erkennen. Die Lern-Engine empfiehlt einen bestimmten Werttyp und Wertausdrücke basierend auf den beobachteten Daten.
- **Zum Bereitstellen klicken**— Wählen Sie eine oder mehrere SQL-Verletzungsprotokollmeldungen im Syslog-Viewer aus und stellen Sie sie als Entspannungsregeln bereit.

SQL-Grammatikschutz für HTML- und JSON-Nutzlast

May 11, 2023

NetScaler Web App Firewall verwendet einen Pattern-Match-Ansatz zum Erkennen von SQL-Injection-Angriffen in HTTP und JSON Payloads. Der Ansatz verwendet eine Reihe von vordefinierten Schlüsselwörtern und (oder) Sonderzeichen, um einen Angriff zu erkennen und ihn als Verstoß zu kennzeichnen. Obwohl dieser Ansatz effektiv ist, kann dies zu vielen Fehlalarmen führen, was dazu führt, dass eine oder mehrere Entspannungsregeln hinzugefügt werden. Insbesondere wenn häufig verwendete Wörter wie “Select” und “From” in einer HTTP- oder JSON-Anfrage verwendet werden. Wir können Fehlalarme reduzieren, indem wir die Überprüfung des SQL-Grammatikschutzes HTML und die JSON Nutzlast implementieren.

Im bestehenden Pattern-Match-Ansatz wird ein SQL-Injection-Angriff identifiziert, wenn ein vordefiniertes Schlüsselwort und/oder ein Sonderzeichen in einer HTTP-Anforderung vorhanden ist. In diesem Fall muss die Anweisung keine gültige SQL-Anweisung sein. Im grammatikbasierten Ansatz wird jedoch ein SQL-Injection-Angriff nur erkannt, wenn ein Schlüsselwort oder ein Sonderzeichen

in einer SQL-Anweisung vorhanden ist oder Teil einer SQL-Anweisung ist, wodurch falsch positive Szenarien reduziert werden.

Szenario zur Nutzung des SQL-Grammatikschutzes

Betrachten Sie eine Erklärung “Wählen Sie meine Tickets aus und treffen wir uns auf der Gewerkschaftsstation” in einer HTTP-Anfrage. Obwohl die Anweisung keine gültige SQL-Anweisung ist, erkennt der vorhandene Pattern-Match-Ansatz die Anforderung als SQL-Injection-Angriff, da die Anweisung Schlüsselwörter wie “Select”, “und” und “Union” verwendet. Im Falle des SQL-Grammatikansatzes wird die Anweisung jedoch nicht als Verstoßangriff erkannt, da die Schlüsselwörter nicht in einer gültigen SQL-Anweisung vorhanden sind oder nicht Teil einer gültigen SQL-Anweisung sind.

Der grammatikbasierte Ansatz kann auch für die Erkennung von SQL-Injection-Angriffen in `JSON` Payloads konfiguriert werden. Um eine Entspannungsregel hinzuzufügen, können Sie die bestehenden Entspannungsregeln wiederverwenden. Feinkörnige Entspannungsregeln gelten auch für die SQL-Grammatik, für Regeln mit “ValueType” “Schlüsselwort”. In der `JSON` SQL-Grammatik kann die vorhandene URL-basierte Methode wiederverwendet werden.

Konfigurieren Sie den grammatikbasierten SQL-Schutz mit der CLI

Um die grammatikbasierte SQL-Erkennung zu implementieren, müssen Sie den Parameter “SqLinjectionGrammar” im Web App Firewall-Profil konfigurieren. In der Standardeinstellung ist der Parameter deaktiviert. Alle vorhandenen SQL Injection-Aktionen werden mit Ausnahme des Lernens unterstützt. Jedes neue Profil, das nach einem Upgrade erstellt wurde, unterstützt die SQL-Injection-Grammatik und hat weiterhin den Standardtyp als “Sonderzeichen oder Schlüsselwort” und muss explizit aktiviert sein.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile profile1 -SQLInjectionAction Block -SQLInjectionGrammar ON
```

Konfigurieren Sie den SQL-Pattern-Match-Schutz und den grammatikbasierten Schutz über die Befehlszeilenschnittstelle

Wenn Sie sowohl Grammatik-basierte als auch Pattern-Match-Ansätze aktiviert haben, führt die Appliance zuerst eine grammatikbasierte Erkennung durch, und wenn eine SQL-Einschleusungserkennung

mit dem Aktionstyp auf blockiert festgelegt ist, wird die Anforderung blockiert (ohne die Erkennung mithilfe von Pattern-Match zu überprüfen).

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
      SQLInjectionGrammar ON  - SQLInjectionType <Any action other than  '
      None' : SQLSplCharANDKeyword/ SQLSplCharORKeyword/ SQLSplChar/
      SQLKeyword>
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType SQLSplChar
```

Konfigurieren Sie SQL Injection Check nur mit grammatikbasiertem Schutz über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
      SQLInjectionGrammar ON  - SQLInjectionType None
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType None
```

Binden Sie Entspannungsregeln für den grammatikbasierten SQL-Schutz über die Befehlszeilenschnittstelle

Wenn Ihre Anwendung erfordert, dass Sie die SQL Einschleusungsprüfung für ein bestimmtes “ELEMENT” oder “ATTRIBUT” in der Nutzlast Bypass müssen, müssen Sie eine Entspannungsregel konfigurieren.

> **Hinweis:**
>
> Entspannungsregeln mit ValueType “Schlüsselwort” werden nur ausgewertet, wenn die Appliance mithilfe der SQL Grammatik die Erkennung durchführt.

Die Relaxationsregeln für die SQL-Befehlseinschleusungsprüfung haben folgende Syntax. Geben Sie in der Befehlszeile Folgendes ein:


```
bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|
    NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
    |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
    NOTREGEX) ]]
<!--NeedCopy-->
```

Beispiel:

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Konfigurieren Sie den grammatikbasierten SQL-Schutz für JSON-Nutzlast über die Befehlszeilenschnittstelle

Um die grammatikbasierte SQL-Erkennung für die JSON-Nutzlast zu implementieren, müssen Sie den Parameter “JsonSqLinjectionGrammar” im Web App Firewall-Profil konfigurieren. In der Standardeinstellung ist der Parameter deaktiviert. Alle vorhandenen SQL Injection-Aktionen werden mit Ausnahme des Lernens unterstützt. Jedes neue Profil, das nach einem Upgrade erstellt wurde, unterstützt die SQL-Injection-Grammatik und hat weiterhin den Standardtyp als “Sonderzeichen oder Schlüsselwort” und Sie müssen es explizit aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON/OFF
<!--NeedCopy-->
```

Beispiel:

```
add appfw profile profile1 -type JSON -JSONSQLInjectionAction Block -JSONSQLInjectionG
 ON
```

Konfigurieren Sie den SQL-Muster-Match-Schutz und den grammatikbasierten Schutz über die Befehlszeilenschnittstelle

Wenn Sie sowohl Grammatik-basierte als auch Pattern-Match-Prüfungen aktiviert haben, führt die Appliance zuerst eine grammatikbasierte Erkennung durch, und wenn eine SQL-Einschleusungserkennung mit dem Aktionstyp auf blockiert festgelegt ist, wird die Anforderung blockiert (ohne die Erkennung mithilfe von Pattern-Match zu überprüfen).

> **Hinweis:**
>
> Entspannungsregeln mit ValueType “Schlüsselwort” werden nur ausgewertet, wenn die Appliance die Erkennung mithilfe der SQL-Grammatik durchführt.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType <Any
     action other than  'None' : SQLSplCharANDKeyword/
    SQLSplCharORKeyword/ SQLSplChar/ SQLKeyword>
<!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType SQLSplChar
```

Konfigurieren Sie den grammatikbasierten SQL-Schutz für JSON-Nutzlast über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
    action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType None
    `\
<!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType None
```

Binden Sie URL-basierte Entspannungsregeln für JSON SQL grammatikbasierten Schutz über die Befehlszeilenschnittstelle

Wenn Ihre Anwendung erfordert, dass Sie die JSON-Befehlseinschleusungsprüfung für ein bestimmtes “ELEMENT” oder “ATTRIBUT” in der Nutzlast umgehen müssen, können Sie eine Entspannungsregel konfigurieren.
Die Relaxationsregeln für die JSON-Befehlseinschleusungsprüfung haben folgende Syntax. Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile <profile name>  - JSONCMDURL <expression> -comment <
    string> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED ) -state (
    ENABLED | DISABLED )
```



```
<!--NeedCopy-->
```

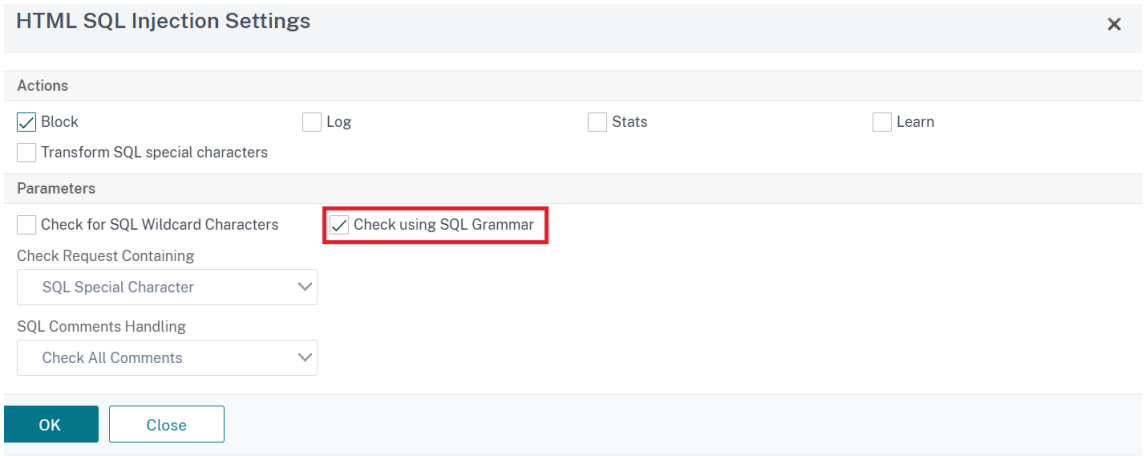
Beispiel:

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```

Konfigurieren Sie den grammatikbasierten SQL-Schutz über die grafische Benutzeroberfläche

Führen Sie die GUI-Prozedur ab, um die grammatikbasierte HTML SQL Injection Erkennung zu konfigurieren

1. Navigieren Sie im Navigationsbereich zu **Sicherheit > Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall-Profilseite** unter **ErweiterteEinstellungen auf Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu Einstellungen für **HTML SQL Injection** .
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.
6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **Einstellungen für HMTL SQL Injection** aufzurufen.

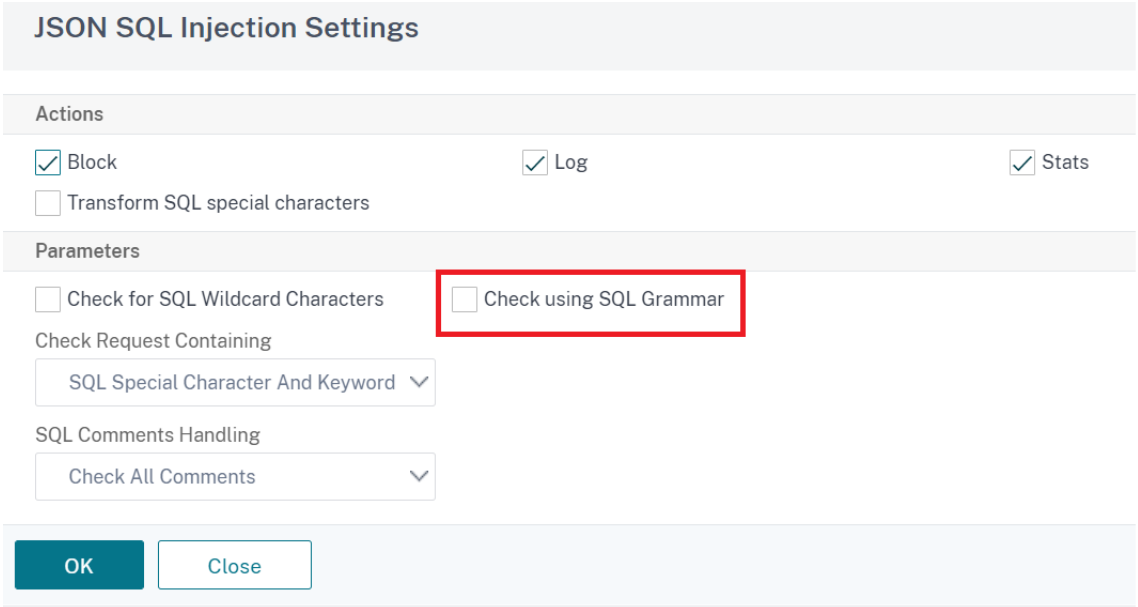


7. Aktivieren Sie das **Kontrollkästchen Mit SQL-Grammatik** prüfen.
8. Klicken Sie auf **OK**.

Konfigurieren Sie den grammatikbasierten SQL-Schutz für JSON-Nutzlast über die grafische Benutzeroberfläche

Führen Sie die GUI-Prozedur ab, um die grammatikbasierte JSON SQL Injection Erkennung zu konfigurieren.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit > Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall-Profilseite** unter **ErweiterteEinstellungen auf Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu den **JSON-SQL-Einschleusung-Einstellungen** .
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.
6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON SQL Injection Settings** aufzurufen.
7. Aktivieren Sie das **Kontrollkästchen Mit SQL-Grammatik** prüfen.
8. Klicken Sie auf **OK**.



Grammatikbasierter Schutz vor Befehlseinschleusung für HTML-Payload

May 11, 2023

NetScaler Web App Firewall verwendet einen Pattern-Match-Ansatz zur Erkennung von Befehlseinschleusungsangriffen in HTML-Payloads Der Ansatz verwendet eine Reihe vordefinierter Schlüsselwörter und (oder) Sonderzeichen, um einen Angriff zu erkennen und ihn als Verstoß zu kennzeichnen. Obwohl dieser Ansatz effektiv ist, kann er zu vielen Fehlalarmen führen, die dazu führen, dass eine oder mehrere Relaxationsregeln hinzugefügt werden. Insbesondere, wenn ein häufig verwendetes Wort wie "Exit" in einer HTTP-Anfrage verwendet wird. Wir können Fehlalarme reduzieren, indem wir den grammatikbasierten Schutz vor Befehlseinschleusung für die HTML-Payload implementieren.

Beim Pattern-Match-Ansatz wird ein Befehlseinschleusungsangriff identifiziert, wenn ein vordefiniertes Schlüsselwort und (oder) ein Sonderzeichen in einer HTTP-Anforderung vorhanden ist. In diesem Fall muss die Anweisung keine gültige Befehlseinschleusungsanweisung sein. Beim grammatikbasierten Ansatz wird ein Befehlseinschleusungsangriff jedoch nur erkannt, wenn ein Schlüsselwort oder ein Sonderzeichen in einer Befehlseinschleusungsanweisung vorhanden ist. Daher werden falsch positive Szenarien reduziert.

Anwendungsszenario für grammatikbasierten Schutz vor Befehlseinschleusung

Betrachten Sie eine Aussage: "Rush towards the exit!" in einer HTTP-Anfrage. Obwohl die Anweisung keine gültige Befehlseinschleusungsanweisung ist, erkennt der Pattern-Match-Ansatz die Anforderung aufgrund des Schlüsselworts "exit" als Befehlseinschleusungsangriff. Beim grammatikbasierten Ansatz des Befehlseinschleusungsschutz wird die Anweisung jedoch nicht als Angriff erkannt, da die Schlüsselwörter in einer gültigen Befehlseinschleusunganweisung nicht vorhanden sind.

Konfigurieren der grammatikbasierten Schutzparameter gegen Befehlseinschleusungsangriffe über die Befehlszeilenschnittstelle

Um die grammatikbasierte Erkennung von Befehlseinschleusung zu implementieren, müssen Sie den Parameter "CMDInjectionGrammar" im Web App Firewall-Profil konfigurieren. In der Standardeinstellung ist der Parameter deaktiviert. Alle vorhandenen Befehlseinschleusungaktionen außer Lernen werden unterstützt. Jedes nach einem Upgrade neu erstellte Profil unterstützt die Befehlseinschleusungsgrammatik. Das neue Profil hat weiterhin den Standardtyp "Sonderzeichen oder Schlüsselwort", und die Befehlseinschleusungsgrammatik muss explizit aktiviert sein.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add appfw profile <profile-name>  - CMDInjectionAction <action-name> -
     CMDInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Beispiel:


```
add appfw profile profile1 -CMDInjectionAction Block -
    CMDInjectionGrammar ON
<!--NeedCopy-->
```

Konfigurieren des Musterübereinstimmungsschutz und des grammatikbasierten Schutz vor Befehlseinschleusung über die CLI

Wenn Sie sowohl grammatikbasierte als auch Musterübereinstimmungsansätze aktiviert haben, führt die Appliance zunächst eine grammatikbasierte Erkennung durch. Wenn eine Befehlseinschleusung erkannt wird, bei der der Aktionstyp auf "Block" gesetzt ist, wird die Anforderung blockiert (ohne Überprüfung der Erkennung über Pattern-Match).

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <profile-name> -CMDInjectionAction <action-name> -
    CMDInjectionGrammar ON -CMDInjectionType <Any action other than 'None' : CMDSplCharANDKeyword/ CMDSplCharORKeyword/ CMDSplChar/ CMDKeyword>
<!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -CMDInjectionAction block - CMDInjectionGrammar ON -CMDInjectionType CMDSplChar
<!--NeedCopy-->
```

Konfigurieren der Befehlseinschleusungsprüfung nur mit grammatikbasiertem Schutz über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <profile-name> -CMDInjectionAction <action-name> -
    CMDInjectionGrammar ON -CMDInjectionType None
<!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -CMDInjectionAction block - CMDInjectionGrammar ON -CMDInjectionType None
<!--NeedCopy-->
```


Binden Sie Relaxationsregeln für den grammatikbasierten Schutz vor Befehlseinschleusung über die CLI

Wenn Ihre Anwendung erfordert, dass Sie die Befehlseinschleusungsprüfung für ein bestimmtes “ELEMENT” oder “ATTRIBUTE” in der HTML-Payload Bypass müssen, müssen Sie eine Relaxationsregel konfigurieren.

> **Hinweis:**
>
> Relaxationsregeln mit valueType “keyword” werden nur ausgewertet, wenn die Appliance die Erkennung über Befehlseinschleusungsgrammatik durchführt.

Die Relaxationsregeln für die Befehlseinschleusungsprüfung haben folgende Syntax. Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile <name> -CMDInjection <String> [isRegex(REGEX|
    NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
    |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
    NOTREGEX) ]]
<!--NeedCopy-->
```

Beispiel:

```
bind appfw profile p1 -cmdinjection abc http://10.10.10.10/

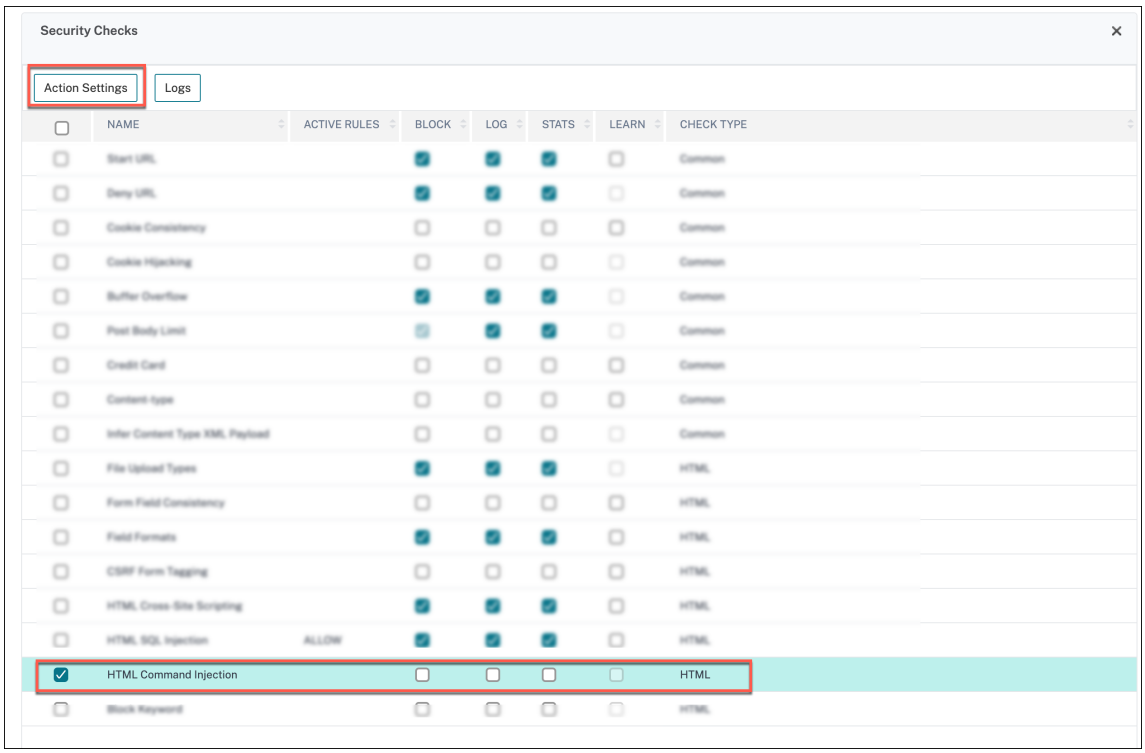
bind appfw profile p1  - cmdinjection 'abc[0-9]+' http://10.10.10.10/ -
    isregex regEX

bind appfw profile p1  - cmdinjection 'name' http://10.10.10.10/ -
    valueType Keyword 'exi[a-z]+' -isvalueRegex regEX
<!--NeedCopy-->
```

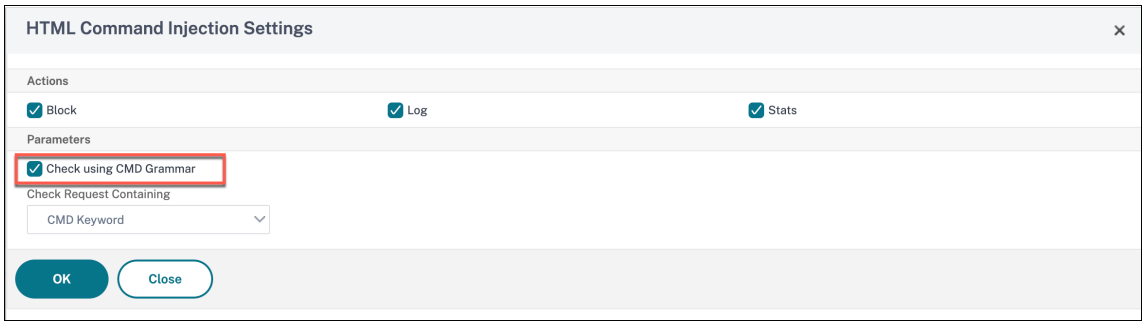
Konfigurieren des grammatikbasierten Schutz vor Befehlseinschleusung über die GUI

Führen Sie die folgenden Schritte aus, um die grammatikbasierte Erkennung von HTML-Befehlseinschleusung zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall-Profil > Profile**.
2. Wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Gehen Sie zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsüberprüfungen**.
4. Aktivieren Sie das Kontrollkästchen **HTML Command Injection** und klicken Sie auf **Aktionseinstellungen**.



5. Aktivieren Sie das Kontrollkästchen **Mit CMD-Grammatik überprüfen**.
6. Wählen Sie unter **Prüfanforderung enthalten** die Option **Keine**



7. Klicken Sie auf**OK**.

Regeln zur Entspannung und Ablehnung von HTML-SQL-Injection-Angriffen

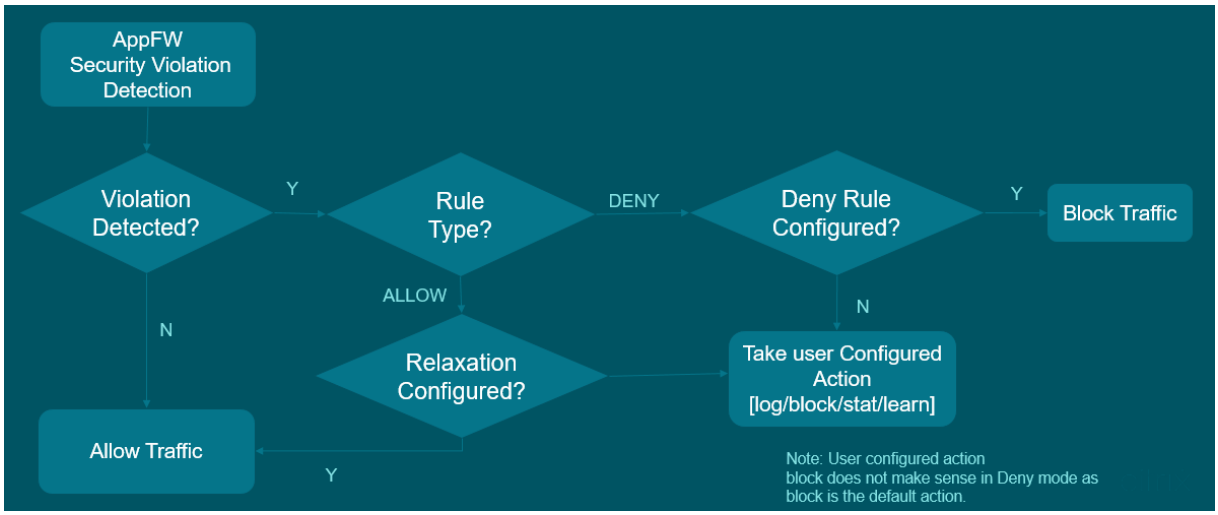
August 19, 2021

Wenn ein eingehender Datenverkehr vorliegt, prüft die Logik zur Erkennung von Verstößen auf Verkehrsverstöße. Wenn keine HTML-SQL-Injection-Angriffe erkannt werden, darf der Datenverkehr bestehen. Wenn jedoch ein Verstoß festgestellt wird, definieren die Regeln für Entspannung (Zu-

lassen) und Verweigern, wie mit den Verstößen umzugehen sind. Wenn die Sicherheitsprüfung im Zulassungsmodus (Standardmodus) konfiguriert ist, wird der erkannte Verstoß blockiert, es sei denn, der Benutzer hat explizit eine Entspannungs- oder Zulassungsregel konfiguriert.

Neben dem Zulassungsmodus kann die Sicherheitsprüfung auch im Ablehnmodus konfiguriert werden und Verweigerregeln für die Behandlung von Verstößen verwenden. Wenn die Sicherheitsprüfung in diesem Modus konfiguriert ist, werden die erkannten Verstöße blockiert, wenn ein Benutzer explizit eine Ablehnregel konfiguriert hat. Wenn keine Ablehnungsregeln konfiguriert sind, wird die vom Benutzer konfigurierte Aktion angewendet.

In der folgenden Abbildung wird erläutert, wie Betriebsmodi zugelassen und verweigert werden:



1. Wenn ein Verstoß festgestellt wird, definieren die Regeln für Entspannung (Zulassen) und Verweigern, wie mit den Verstößen umzugehen sind.
2. Wenn die Sicherheitsprüfung im Verweigerungsmodus konfiguriert ist (falls sie im Zulassungsmodus konfiguriert ist, springen Sie zu Schritt 5), wird der Verstoß blockiert, es sei denn, Sie haben explizit eine Ablehnungsregel konfiguriert.
3. Wenn der Verstoß mit einer Ablehnregel übereinstimmt, blockiert die Appliance den Datenverkehr.
4. Wenn der Verkehrsverstoß nicht mit einer Regel übereinstimmt, wendet die Appliance eine benutzerdefinierte Aktion an (blockieren, zurücksetzen oder löschen).
5. Wenn die Sicherheitsprüfung im Zulassungsmodus konfiguriert ist, prüft das Web App Firewall-Modul, ob eine Zulassungsregel konfiguriert ist.
6. Wenn der Verstoß mit einer Zulassungsregel übereinstimmt, lässt die Appliance den Datenverkehr andernfalls Bypass, er wird blockiert.

Konfigurieren des Entspannungs- und Durchsetzungsmodus

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set appfw profile <name>   - SQLInjectionAction [block stats learn]  -
    SQLInjectionRuleType [ALLOW DENY]
<!--NeedCopy-->
```

Beispiel:

```
set appfw profile prof1 sqlInjectionAction block -sqlInjectionRuleType
ALLOW DENY
```

Binden Sie Entspannungs- und Durchsetzungsregeln an das Web Application Firewall-

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind appfw profile <name> -SQLInjection <string> <formActionURL>
<!--NeedCopy-->
```

Beispiel:

```
bind appfw profile p1 -SQLInjection field_f1 "/login.php"-RuleType ALLOW
bind appfw profile p2 -SQLInjection field_f1 "/login.php"-RuleType ALLOW
```

Überprüfung für HTML-Befehlseinschleusungsschutz

May 11, 2023

Die **HTML-Befehlseinschleusungsprüfung** untersucht, ob der eingehende Datenverkehr nicht autorisierte Befehle enthält, die die Systemsicherheit unterbrechen oder das System ändern. Wenn der Datenverkehr bei Erkennung böswillige Befehle enthält, blockiert die Appliance die Anfrage oder führt die konfigurierte Aktion aus.

Das NetScaler Web App Firewall-Profil wurde jetzt um eine neue Sicherheitsüberprüfung für Command-Injection-Angriffe erweitert. Wenn die Command Injection Security Check den Datenverkehr untersucht und bösartige Befehle erkennt, blockiert die Appliance die Anfrage oder führt die konfigurierte Aktion aus.

Bei einem Command-Injection-Angriff zielt der Angreifer darauf ab, nicht autorisierte Befehle auf dem NetScaler-Betriebssystem auszuführen. Um dies zu erreichen, schleust der Angreifer Betriebssystembefehle über eine anfällige Anwendung ein. Eine NetScaler-Appliance ist anfällig für Injektionsangriffe, wenn die Anwendung unsichere Daten (Formulare, Cookies oder Header) an die System-Shell weitergibt.

So funktioniert der Befehlseinschleusungsschutz

1. Bei einer eingehenden Anfrage untersucht WAF den Traffic auf Schlüsselwörter oder Sonderzeichen. Wenn die eingehende Anfrage keine Muster enthält, die mit einem der abgelehnten Schlüsselwörter oder Sonderzeichen übereinstimmen, ist die Anfrage zulässig. Andernfalls wird die Anforderung basierend auf der konfigurierten Aktion blockiert, verworfen oder umgeleitet.
2. Wenn Sie es vorziehen, ein Schlüsselwort oder ein Sonderzeichen von der Liste auszunehmen, können Sie eine Lockerungsregel anwenden, um die Sicherheitsüberprüfung unter bestimmten Bedingungen zu Bypass.
3. Sie können die Protokollierung aktivieren, um Protokollmeldungen zu generieren Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
4. Sie können die Statistikfunktion auch aktivieren, um statistische Daten zu Verstößen und Protokollen zu sammeln. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anforderungen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um festzustellen, ob Sie die neue Entspannungsregel konfigurieren oder die vorhandene ändern müssen.

Schlüsselwörter und Sonderzeichen, die für die Befehlseinschleusung verweigert werden

Um Command-Injection-Angriffe zu erkennen und zu blockieren, verfügt die Appliance über eine Reihe von Mustern (Schlüsselwörter und Sonderzeichen), die in der Standardsignaturdatei definiert sind. Es folgt eine Liste der blockierten Schlüsselwörter beim Erkennen von Befehlseinschleusungsverstößen

```
    <commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>
<!--NeedCopy-->
```

In der Signaturdatei definierte Sonderzeichen sind:

```
| ; & $ > < '\ ! >> ##
```


Konfiguration des Command Injection Check mithilfe der CLI

In der Befehlszeilenschnittstelle können Sie entweder den Befehl set the profile oder den Befehl add the profile verwenden, um die Einstellungen für die Befehlsinjektion zu konfigurieren. Sie können die Block-, Protokoll- und Statistikaktionen aktivieren. Sie müssen auch die Schlüsselwörter und Zeichenketten festlegen, die Sie in den Payloads erkennen möchten.

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Hinweis:**
>
> Standardmäßig ist die Befehlseinschleusungsaktion auf “Keine” festgelegt. Außerdem wird der Standardeinschleusungsstyp des Befehls als festgelegt `CmdSplCharANDKeyWord`.

Beispiel:

```
set appfw profile profile1 -cmdInjectionAction block -CMDInjectionType
CmdSplChar
```

Dabei sind die verfügbaren Befehlsinjektionsaktionen wie folgt:

- Keine — Deaktiviert den Befehlseinschleusungsschutz.
- Log — Protokollieren von Befehlseinschleusungsverstößen für die Sicherheitsprüfung
- Blockieren - blockiert Datenverkehr, der gegen die Befehlseinschleusungsüberprüfung verstößt.
- Statistik - Generiert Statistiken für Sicherheitsverletzungen durch Befehlseinschleusung.

Dabei sind die folgenden Befehlsinjektionstypen verfügbar:

- Befehl splChar. Prüft Sonderzeichen
- cmdSchlüsselwort. Prüft Schlüsselwörter zur Befehlseinspeisung
- cmdSPLCharandSchlüsselwort. Prüft Sonderzeichen und Befehlseinfügung. Schlüsselwörter und Blöcke nur, wenn beide vorhanden sind.
- cmdSPLCHARORSchlüsselwort. Prüft Sonderzeichen und Schlüsselwörter zur Befehlseinspeisung und blockiert, wenn eines von ihnen gefunden wird.

Konfiguration von Relaxationsregeln für die Schutzüberprüfung durch Befehlseinschleusung

Wenn Ihre Anwendung verlangt, dass Sie die Command Injection Inspection für ein bestimmtes ELEMENT oder ATTRIBUTE in der Payload Bypass, können Sie eine Relaxationsregel konfigurieren.

Die Relaxationsregeln für den Befehl Injection Inspection haben die folgende Syntax:


```
bind appfw profile <profile name> -cmdInjection <string> <URL> -isregex <
REGEX/NOTREGEX>
```

Beispiel für Relaxationsregel für Regex im Header

```
bind appfw profile sample -CMDInjection hdr "http://10.10.10.10/"-location
heaDER -valueType Keyword '[a-z]+grep'-isvalueRegex REGEX
```

Infolgedessen befreit die Injektion den Befehl Injection Check ermöglicht Header, der Varianten von “grep” `hdr` enthält.

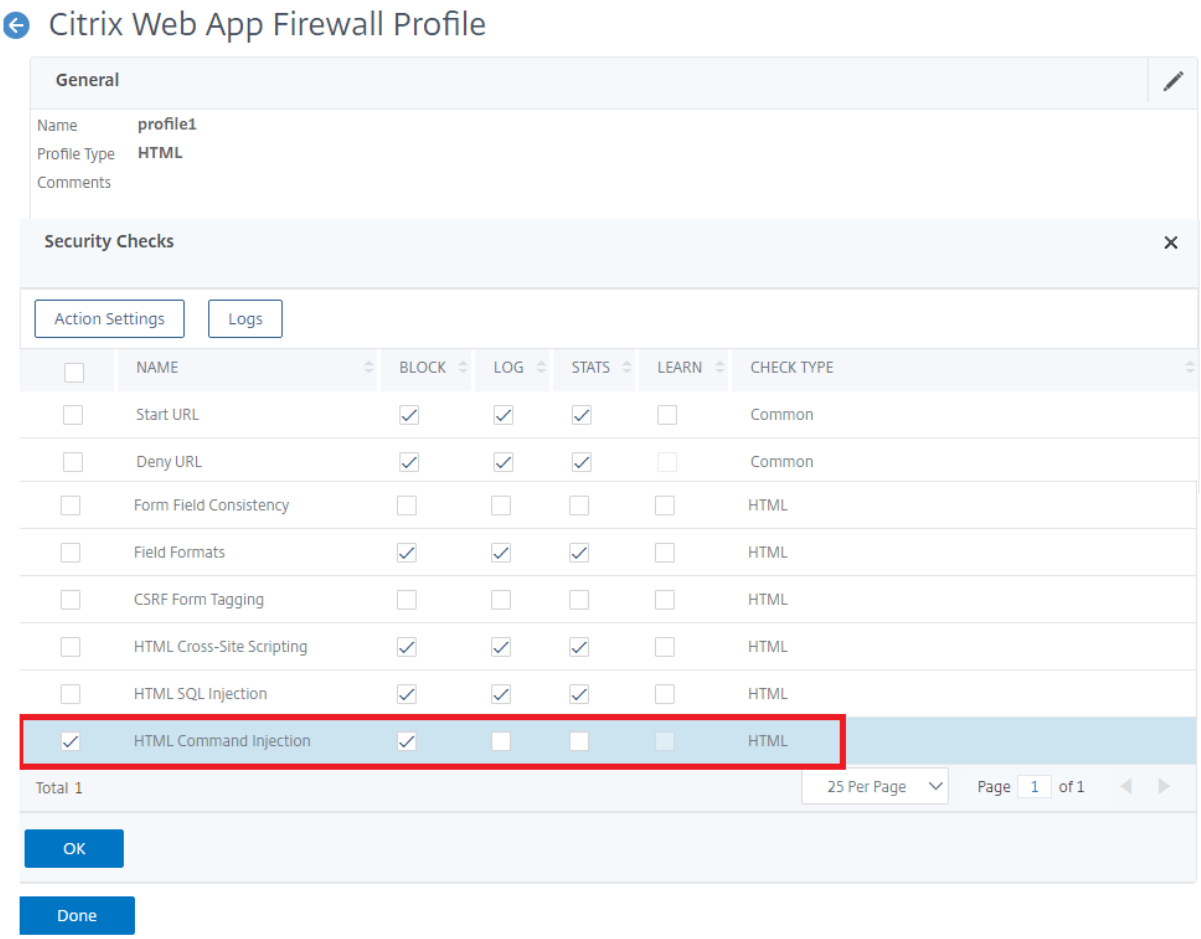
Beispiel für Relaxationsregel mit ValueType als Regex im Cookie

```
bind appfw profile sample -CMDInjection ck_login "http://10.10.10.10/"-
location cookie -valueType Keyword 'pkg[a-z]+'-isvalueRegex REGEX
```

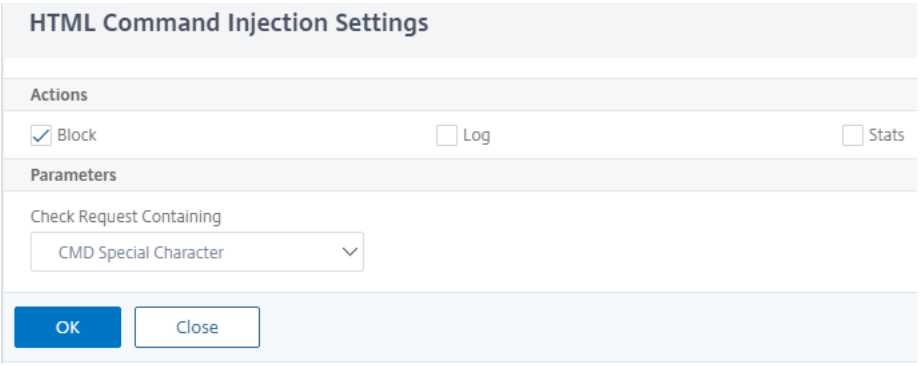
Konfiguration der Befehlsinjektionsprüfung mithilfe der NetScaler-GUI

Gehen Sie wie folgt vor, um den Befehl Injection Check zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall und Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der **NetScaler Web App Firewall-Profilseite** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.



1. Wählen Sie im Abschnitt **Sicherheitsprüfungen** die Option **HTML Command Injection** aus und klicken Sie auf **Aktionseinstellungen** .
2. Stellen Sie auf der Seite mit den **Einstellungen für die HTML-Command Injection** die folgenden Parameter ein:
   a) Aktionen. Wählen Sie eine oder mehrere Aktionen aus, die für die Sicherheitsprüfung durch Command Injection ausgeführt werden sollen.
   b) Überprüfen Sie die Anfrage enthält. Wählen Sie ein Befehlseinschleusungsmuster, um zu überprüfen, ob die eingehende Anforderung das Muster enthält.
3. Klicken Sie auf **OK**.



Anzeigen oder Anpassen von Befehlseinschleusungsmustern über die grafische Benutzeroberfläche

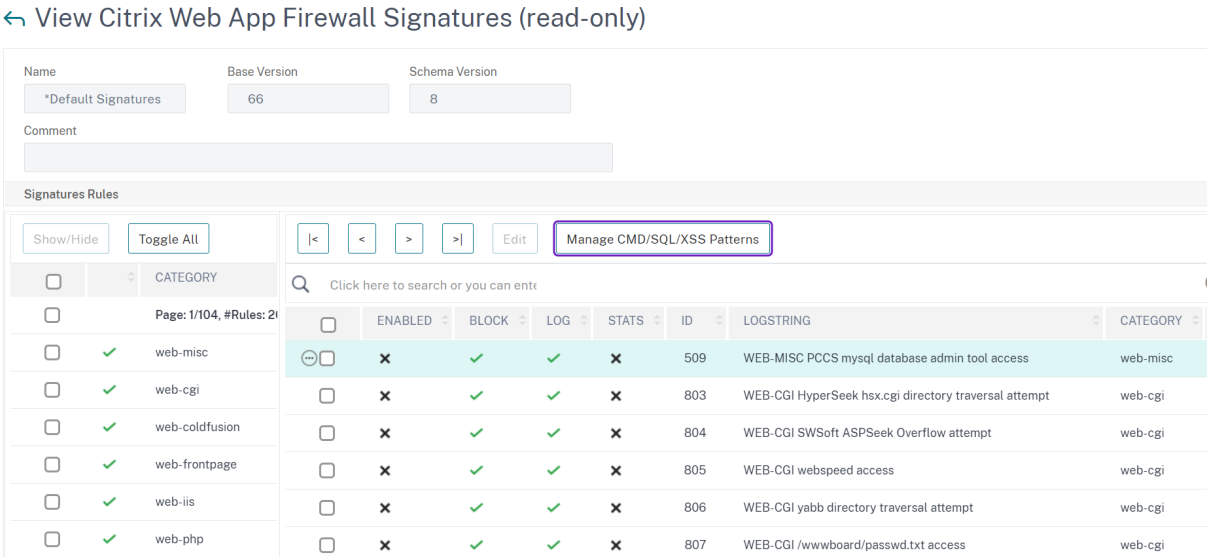
Sie können die GUI verwenden, um die Injection-Pattern des **HTML-Befehls** anzuzeigen oder anzupassen.

Die Standardbefehl-Einschleusungsmuster sind in der Standardsignaturdatei angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, werden die im Standardsignatur-Objekt angegebenen Standard-HTML-Befehlseinschleusungsmuster vom Profil für die Verarbeitung der Sicherheitsprüfung der Befehlseinschleusung verwendet. Die im Standardsignaturobjekt angegebenen Regeln und Muster sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese Muster ändern oder ändern möchten, erstellen Sie eine Kopie des Standardobjekts sSignatures, um ein benutzerdefiniertes Signaturobjekt zu erstellen. Nehmen Sie Änderungen an den Befehlseinschleusungsmustern im neuen benutzerdefinierten Signaturobjekt vor und verwenden Sie dieses Signaturobjekt in Ihrem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten Muster verwenden möchten.

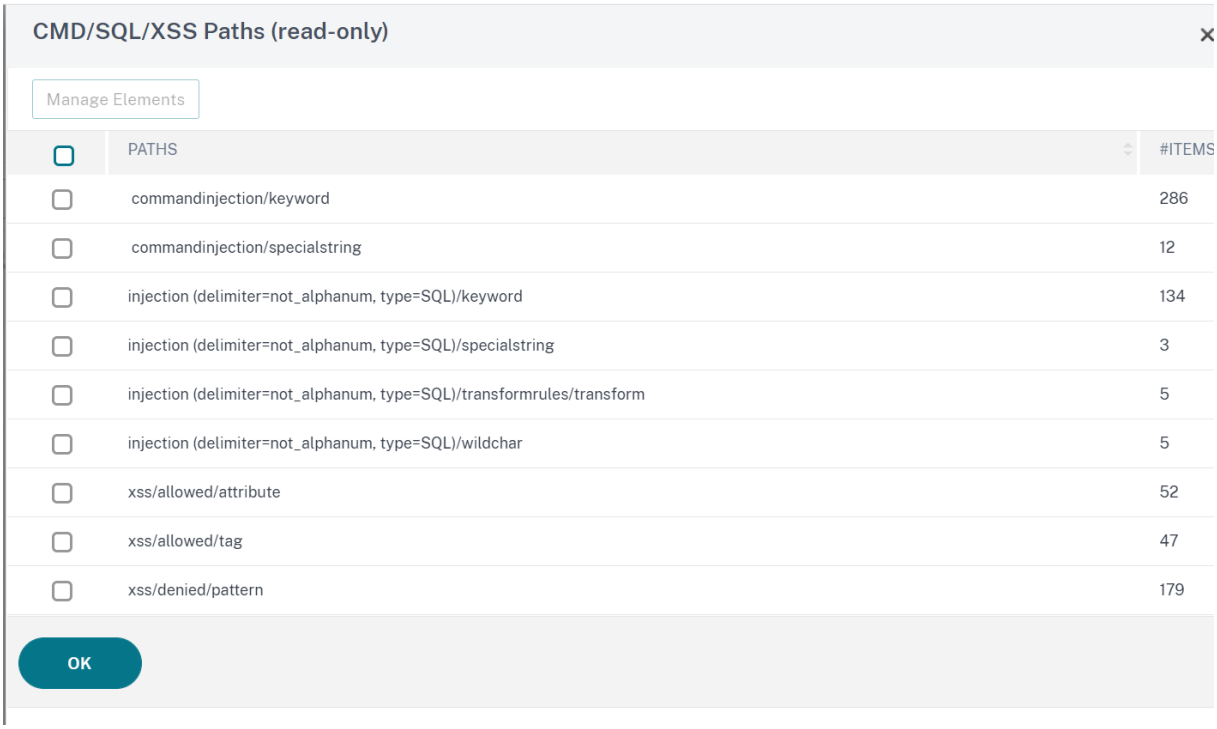
Weitere Informationen finden Sie unter Signaturen

So zeigen Sie die Standardeinschleusungsmuster für Befehle über die GUI an:

1. Navigieren Sie zu **Application Firewall > Signaturen**, wählen Sie ***Standardsignaturen**aus und klicken Sie auf **Bearbeiten**.



1. Klicken Sie auf **CMD/SQL/XSS-Muster verwalten**. Die Tabelle **CMD/SQL/XSS Paths (schreibgeschützt)** zeigt Muster im Zusammenhang mit der `CMD`/`SQL`/`XSS`-Einschleusung:



1. Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden Befehlseinschleusungsmuster (Schlüsselwörter, spezielle Zeichenfolgen, Transformationsregeln oder Platzhalterzeichen) anzuzeigen, die von der Injection-Prüfung des Web App Firewall-Befehls verwendet werden.

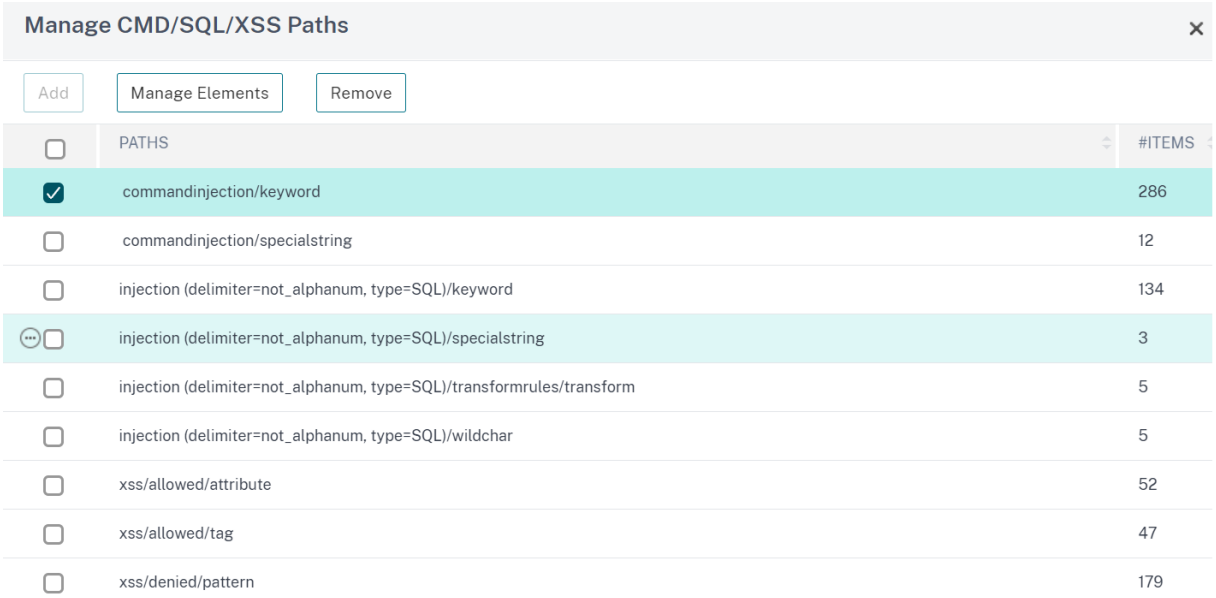
So passen Sie ein Befehlseinschleusungsmuster mit der GUI an

Sie können das benutzerdefinierte Signaturobjekt bearbeiten, um die **CMD-Schlüsselwörter**, Son-

derzeichenfolgen und Platzhalterzeichen anzupassen. Sie können neue Einträge hinzufügen oder vorhandene entfernen. Sie können die Transformationsregeln für die spezielle Zeichenfolgen für die Befehlseinschleusung ändern.

1. Navigieren Sie zu **Application Firewall > Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Hinzufügen**. Klicken Sie auf **CMD/SQL/XSS-Muster verwalten**.
2. Wählen Sie auf der Seite **CMD/SQL/XSS-Pfade verwalten** die Ziel-CMD-Einschleusungszeile aus.
3. Klicken Sie auf **Elemente verwalten**, **Hinzufügen** oder **Entfernen** eines Befehlseinschleusungselements.

   > **Warnung:**
   >
   > Sie müssen vorsichtig sein, bevor Sie ein Standard-Befehlseinschleusungselement entfernen oder ändern, oder den CMD-Pfad löschen, um die gesamte Zeile zu entfernen. Die Signaturregeln und die Sicherheitsprüfung der Befehlseinschleusung beruhen auf diesen Elementen, um Angriffe auf Befehlseinschleusung zu erkennen, um Ihre Anwendungen zu schützen. Das Anpassen der SQL-Muster kann Ihre Anwendung anfällig für Befehlseinschleusungsangriffe machen, wenn das erforderliche Muster während der Bearbeitung entfernt wird.



Anzeigen von Statistiken zum Befehlseinschleusungsdatenverkehr und -verletzungen

Auf der Seite “ **NetScaler Web App Firewall Statistics** “ werden Details zu Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format angezeigt.

So zeigen Sie Sicherheitsstatistiken mithilfe der Befehlszeilenschnittstelle an.

Geben Sie in der Befehlszeile Folgendes ein:

```
stat appfw profile profile1
```

Appfw-Profil Verkehrsstatistiken	Geschwindigkeit (/s)	Gesamt
Anfragen	0	0
Byte anfragen	0	0
Antworten	0	0
Antwort Byte	0	0
Bricht ab	0	0
Leitet	0	0
Langfristige Reaktionszeit (ms)	–	0
Letzte Reaktionszeit von Ave (ms)	–	0

Statistiken zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
Start-URL	0	0
URL verweigern	0	0
Referer-Header	0	0
Pufferüberlauf	0	0
Cookie-Konsistenz	0	0
Cookie-Entführung	0	0
CSRF-Formular-Tag	0	0
Site-übergreifendes HTML	0	0
HTML SQL injection	0	0
Feld-Format	0	0
Field consistency	0	0
Kreditkarte	0	0
Sicheres Objekt	0	0

Statistiken zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
Verstöße gegen die Signatur	0	0
Inhaltstyp	0	0
JSON-Denial-of-Service-Angriff	0	0
JSON-SQL-Einschleusung	0	0
JSON-Cross-Site Scripting	0	0
Dateiuploadtyp	0	0
Ableiten der XML-Nutzlast für Inhaltstypen	0	0
HTML-Befehlseinschleusung	0	0
XML-Format	0	0
XML-Denial-of-Service-Angriff (XDoS)	0	0
XML-Nachrichtenüberprüfung	0	0
Interoperabilität der Webdienste	0	0
XML SQL Injection	0	0
Site-übergreifende XML-Skrip	0	0
XML-Anhang	0	0
SOAP-Fehlerverletzungen	0	0
Generische XML-Verstöße	0	0
Verstöße insgesamt	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
Starten der URL-Protokolle	0	0
URL-Protokolle verweigern	0	0
Referer-Header-Protokolle	0	0
Pufferüberlauf-Protokolle	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
Protokolle zur Cookie-Konsistenz	0	0
Protokolle zur Cookie-Entführung	0	0
CSRF aus Tag-Protokollen	0	0
HTML-Cross-Site Scripting-Protokolle	0	0
HTML Cross-Site Scripting-Transformationsprotokolle	0	0
HTML SQL-Einschleusungsprotokolle	0	0
HTML SQL Transformationsprotokolle	0	0
Protokolle im Feldformat	0	0
Protokolle zur Feldkonsistenz	0	0
Kreditkarten	0	0
Protokolle zur Kreditkarten-Transformation	0	0
Sichere Objektprotokolle	0	0
Signatur-Protokolle	0	0
Inhalts-Typ-Protokolle	0	0
JSON-Denial-of-Service-Protokolle	0	0
JSON SQL-Einschleusungsprotokolle	0	0
JSON-Site-Scripting-Protokolle	0	0
Protokolle zum Hochladen von Dateien	0	0
Ableiten der XML-Nutzlast des Inhaltstyps L	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
HTML-Befehlseinschleusungsprotokolle	0	0
Protokolle im XML-Format	0	0
XML Denial of Service (XDoS) -Protokolle	0	0
Protokolle zur XML-Nachrichtenüberprüfung	0	0
WSI-Protokolle	0	0
XML SQL Injection-Protokolle	0	0
XML-Cross-Site Scripting-Protokolle	0	0
Protokolle für XML-Anhänge	0	0
SOAP-Fehlerlogs	0	0
Generische XML-Protokolle	0	0
Gesamtzahl der Protokollmeldungen	0	0

Statistikrate für Serverfehler (/s) > Gesamt |
|—|–|–|
HTTP Client Errors (4xx Resp) | 0 | 0|
HTTP Server Errors (5xx Resp) | 0 | 0 |

Anzeigen von Statistiken zur HTML-Befehlsinjektion mithilfe der NetScaler-GUI

Führen Sie die folgenden Schritte aus, um Befehlseinschleusungsstatistiken anzuzeigen:

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Web App Firewall-Profil aus und klicken Sie auf **Statistiken**.
3. Auf der Seite mit den **NetScaler Web App Firewall-Statistiken** werden der Datenverkehr und die Verstöße gegen HTML-Befehle angezeigt.
4. Sie können die **Tabellarische Ansicht** wählen oder zur **grafischen Ansicht** wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.

Verkehrsstatistik für HTML-Befehlsinjektion

HTML SQL Injection logs	0	0
HTML SQL transform logs	0	0
Field format logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0
HTML Command Injection logs	0	0
XML Format logs	0	0
XML Denial of Service(XDoS) logs	0	0
XML Message Validation logs	0	0
WSI logs	0	0
XML SQL Injection logs	0	0
XML XSS logs	0	0
XML Attachment logs	0	0

Statistik über Verstöße gegen HTML-Befehlsinjektionen

HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%
XML Format	0	0	0%
XML Denial of Service (XDoS)	0	0	
XML Message Validation	0	0	
Web Services Interoperability	0	0	

Unterstützung benutzerdefinierter Keywords für HTML-Nutzlast

September 18, 2023

Ab NetScaler Version 13.1 Build 27.xx können Sie Schlüsselwörter Ihrer Wahl hinzufügen und überprüfen, ob diese konfigurierten Schlüsselwörter in der HTML-Payload vorhanden sind.

Für SQL- und Befehlseinschleusung gibt es einen vordefinierten Satz von Schlüsselwörtern oder Mustern, nach denen in den eingehenden Anforderungen gesucht wird. Diese vordefinierten Schlüsselwortsätze decken möglicherweise nicht alle Schlüsselwörter gemäß Ihren Anforderungen ab und können zu einer Erhöhung der Anzahl von Fehlalarmen führen. Mit dieser Funktion können Sie Schlüsselwörter hinzufügen, die bei den Einschleusungsschutzprüfungen für SQL und Befehle nicht behandelt werden, und somit die Fehlalarme reduzieren

Nach dem Hinzufügen der Schlüsselwörter können Sie die NetScaler-Appliance so konfigurieren, dass sie überprüft, ob die hinzugefügten Schlüsselwörter in den eingehenden Anforderungen erkannt werden. Anschließend können Sie die NetScaler-Appliance für eine der folgenden Aktionen konfigurieren:

- **Keine** — Es werden keine Maßnahmen ergriffen. Diese Aktion ist die Standardeinstellung.
- **Protokoll** — Protokolliert alle Anfragen, die mit der URL übereinstimmen und die konfigurierten Schlüsselwörter haben.
- **Blockieren** — Blockieren Sie alle Anfragen, die der URL entsprechen und die konfigurierten Schlüsselwörter haben.
- **Statistiken** — Erhöhen Sie den Protokollzähler für jede Anforderung, die mit der URL übereinstimmt und die konfigurierten Schlüsselwörter enthält.

Hinzufügen benutzerdefinierter Schlüsselwörter mit der CLI

Das Hinzufügen eines benutzerdefinierten Schlüsselworts über die CLI umfasst die folgenden Schritte:

1. Konfigurieren Sie ein Firewallprofil für Webanwendungen und definieren Sie eine Aktion, wenn das benutzerdefinierte Schlüsselwort in der eingehenden Anforderung erkannt wird.

```
set appfw profile <profile-name>  - blockKeywordAction (block | log
    | stats | none)
<!--NeedCopy-->
```

   Standardmäßig ist -blockKeywordAction auf none gesetzt.

   Beispiel:

```
set appfw profile test_profile -blockKeywordAction none
<!--NeedCopy-->
```


2. Binden Sie das Firewallprofil der Webanwendung mit Ihren benutzerdefinierten Schlüsselwörtern.

```
bind appfw profile <profile_name> -blockKeyword <keyword_name> -
    BlockKeywordType <literal|PCRE > -fieldName <field_name> -
    formURL <URL> -isFieldNameRegex <REGEX|NOTREGEX> -state <enable
    /disable> -comment <text>
<!--NeedCopy-->
```

Beispiel:

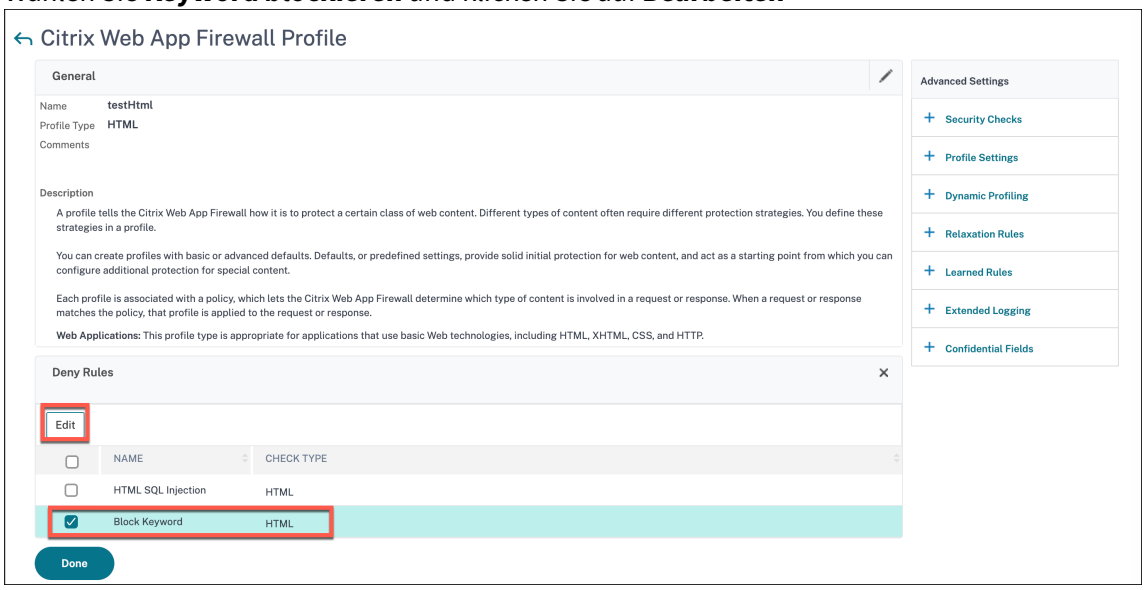
Um **blockword** als benutzerdefiniertes Schlüsselwort hinzuzufügen und es an **test_profile** zu binden, führen Sie den folgenden Befehl aus:

```
bind appfw profile test_profile -blockKeyword "blockword"
    BlockKeywordType literal -fieldName "firstname" -formURL "/
    signup.php" -state enable
<!--NeedCopy-->
```

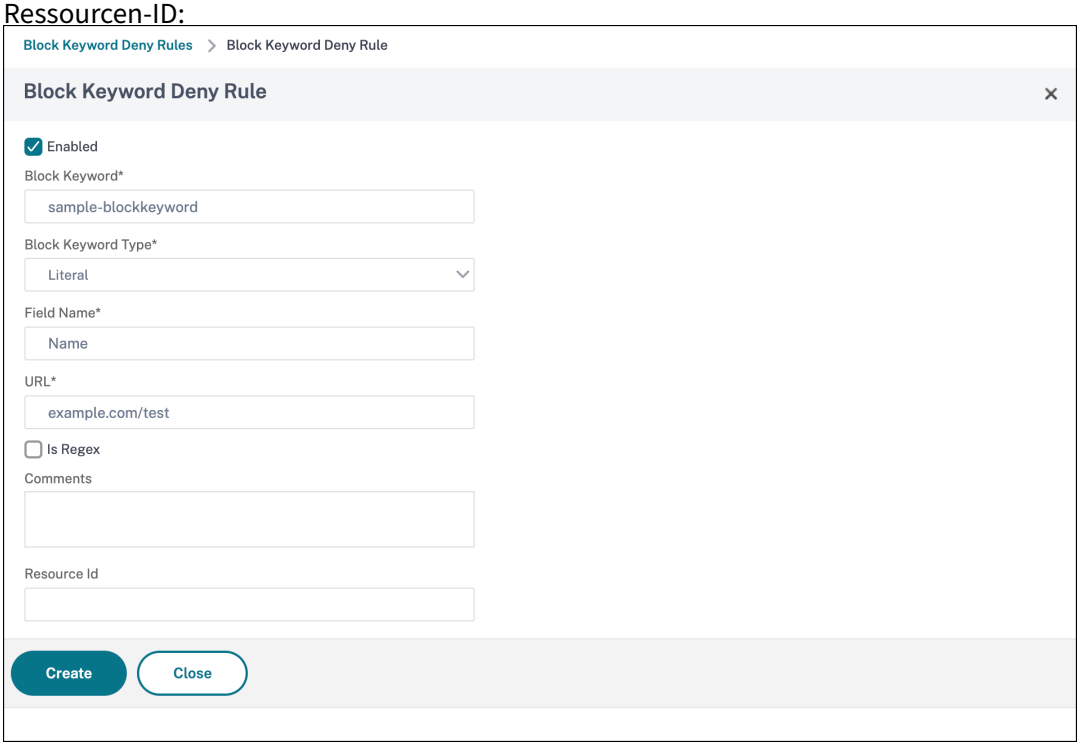
> **Hinweis:**
>
> Sie können eine URL oder einen FQDN in den URL-Parameter eingeben. Der FQDN unterstützt sowohl das HTTP- als auch das HTTPS-Protokoll.

Hinzufügen von benutzerdefinierten Schlüsselwörtern über die GUI

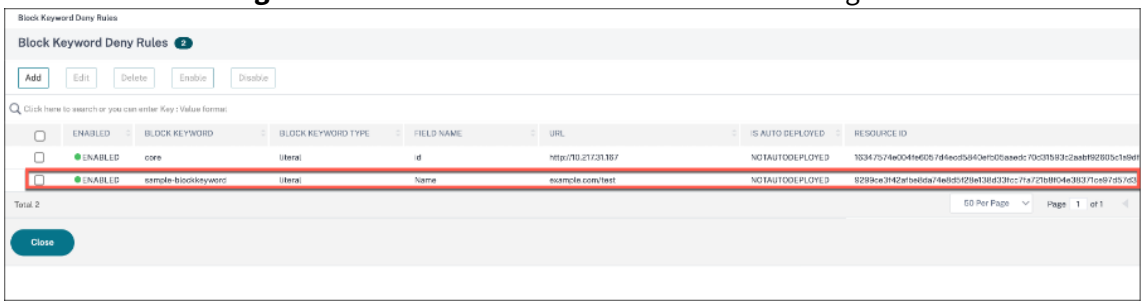
1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall-Profil > Profile**.
2. Wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Gehen Sie zum Abschnitt**Erweiterte Einstellungen**und klicken Sie auf **Regeln ablehnen**.
4. Wählen Sie **Keyword blockieren** und klicken Sie auf **Bearbeiten**



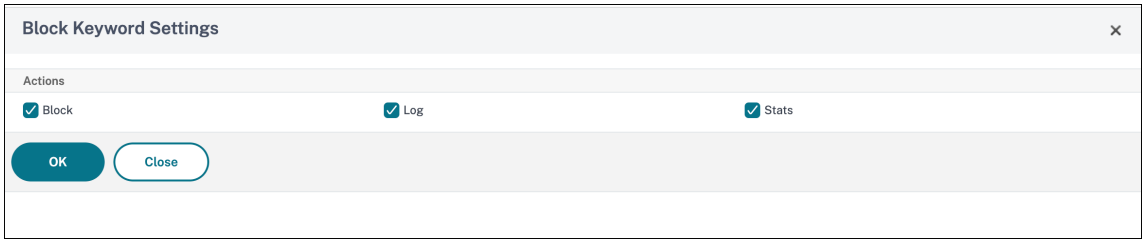
5. Klicken Sie auf **Hinzufügen** und legen Sie die folgenden Parameter fest:
   - Aktivieren
   - Schlüsselwort blockieren
   - Keyword-Typ blockieren
   - Feldname
   - URL
   - Ist Regex
   - Anmerkungen
   - Ressourcen-ID:



6. Klicken Sie auf **Erstellen**. Das benutzerdefinierte Schlüsselwort, das Sie hinzugefügt haben, wird auf der Seite **Regeln zum Blockieren von Schlüsselwörtern** aufgeführt.



7. Gehen Sie zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsüberprüfungen**.
8. Wählen Sie **Schlüsselwort blockieren** und klicken Sie auf **Aktionseinstellungen**.



9. Wählen Sie die erforderlichen Aktionen aus und klicken Sie auf **OK**.

Zeigen Sie benutzerdefinierte Schlüsselwort-Statistiken mit der CLI an

Um die Statistiken über benutzerdefinierte Schlüsselwörter anzuzeigen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
stat appfw profile <profile name>
<!--NeedCopy-->
```

Beispiel

```
stat appfw profile test_profile
<!--NeedCopy-->
```

Anzeigen benutzerdefinierter Keyword-Statistiken über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein **Web App Firewall-Profil** aus und klicken Sie auf **Statistiken**. Auf der Seite mit den**NetScaler Web App Firewall-Statistiken**werden die Details zu benutzerdefiniertem Schlüsselwortverkehr und Verstößen angezeigt.
3. Sie können die**Tabellarische Ansicht**wählen oder zur**grafischen Ansicht**wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.

Schutz vor Angriffen durch externe XML-Entitäten (XXE)

May 11, 2023

Der Schutz vor Angriffen mit XML External Entities (XXE) untersucht, ob eine eingehende Payload unbefugte XML-Eingaben enthält, die sich auf Entitäten außerhalb der vertrauenswürdigen Domain beziehen, in der sich die Webanwendung befindet. Der XXE-Angriff tritt auf, wenn Sie einen schwachen XML-Parser haben, der eine XML-Payload mit Eingaben analysiert, die Verweise auf externe Entitäten enthalten.

Wenn der XML-Parser in einer NetScaler Appliance nicht ordnungsgemäß konfiguriert ist, kann die Ausnutzung der Sicherheitsanfälligkeit gefährlich sein. Es ermöglicht einem Angreifer, sensible Daten auf dem Webserver zu lesen. Führe den Denial-of-Service-Angriff aus und so weiter. Daher ist es wichtig, die Appliance vor XXE-Angriffen zu schützen. Web Application Firewall ist in der Lage, die Appliance vor XXE-Angriffen zu schützen, solange der Inhaltstyp als XML identifiziert wird. Um zu verhindern, dass ein böswilliger Benutzer diesen Schutzmechanismus umgeht, blockiert WAF eine eingehende Anforderung, wenn der "abgeleitete" Inhaltstyp in den HTTP-Headern nicht mit dem Inhaltstyp des Körpers übereinstimmt. Dieser Mechanismus verhindert die Umgehung des XXE-Angriffsschutzes, wenn ein standardmäßiger oder nicht standardmäßiger Inhaltstyp auf der Positivliste verwendet wird.

Einige der möglichen XXE-Bedrohungen, die eine NetScaler Appliance betreffen, sind:

- Lecks vertraulicher Daten
- Denial-of-Service (DOS) -Angriffe
- Serverseitige Fälschungsanforderungen
- Port-Scannen

Konfigurieren des XXE-Einschleusungsschutzes für externe XML-Entitäten

So konfigurieren Sie die Prüfung von externen XML-Entitäten (XXE) mithilfe der Befehlszeilenschnittstelle:
In der Befehlszeilenschnittstelle können Sie den Befehl Application Firewall-Profil hinzufügen oder ändern, um die **XXE-Einstellungen** zu konfigurieren. Sie können die Block-, Protokoll- und Statistikaktionen aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <name> [-inferContentTypeXmlPayloadAction <inferContentTypeXmlPayloa
 <block | log | stats | none>]
```

> Hinweis:
>
> Standardmäßig ist die XXE-Aktion auf "none" festgelegt.

Beispiel:

```
set appfw profile profile1 -inferContentTypeXmlPayloadAction Block
```

Wo sind Aktionstypen:

Sperren: Die Anfrage wird ausnahmslos für die URLs in der Anfrage blockiert.

Protokoll: Wenn eine Diskrepanz zwischen dem Inhaltstyp in einem HTTP-Anforderungsheader und der Payload auftritt, müssen Informationen über die verletzende Anfrage in der Protokollnachricht enthalten sein.

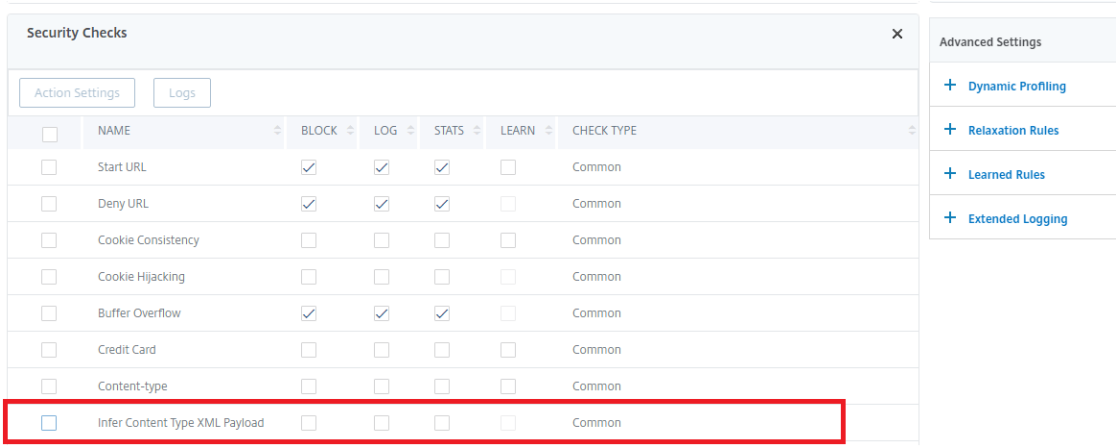
Statistiken: Wenn eine Nichtübereinstimmung der Inhaltstypen festgestellt wird, werden die entsprechenden Statistiken für diesen Verstoßtyp erhöht.

Keine: Wenn eine Nichtübereinstimmung der Inhaltstypen festgestellt wird, werden keine Maßnahmen ergriffen. Keiner kann mit einem anderen Aktionstyp kombiniert werden. Die Standardaktion ist auf Keine festgelegt.

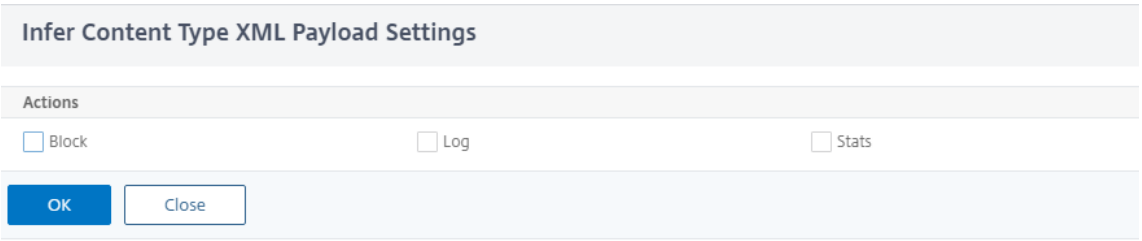
Konfigurieren Sie den XXE-Injection-Check mithilfe der NetScaler-GUI

Gehen Sie wie folgt vor, um den XXE-Injektionscheck zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der **NetScaler Web App Firewall-Profilseite** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.



4. Wählen Sie im Abschnitt **Sicherheitsprüfungen** die Option **Infer Content Type XML Payload** aus und klicken Sie auf **Aktionseinstellungen** .
5. Stellen Sie auf der Seite „XML-Payload-Einstellungen für den Inhaltstyp ableiten“ die folgenden Parameter ein:
   a) Aktionen. Wählen Sie eine oder mehrere Aktionen aus, die für die XXE-Injection-Sicherheitsprüfung ausgeführt werden sollen.
6. Klicken Sie auf **OK**.



Statistiken zu Datenverkehr und Verstößen gegen XXE-Injektionen anzeigen

Auf der Seite “ NetScaler Web App Firewall Statistics “ werden Details zu Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format angezeigt.

So zeigen Sie Sicherheitsstatistiken mithilfe der Befehlszeilenschnittstelle an.

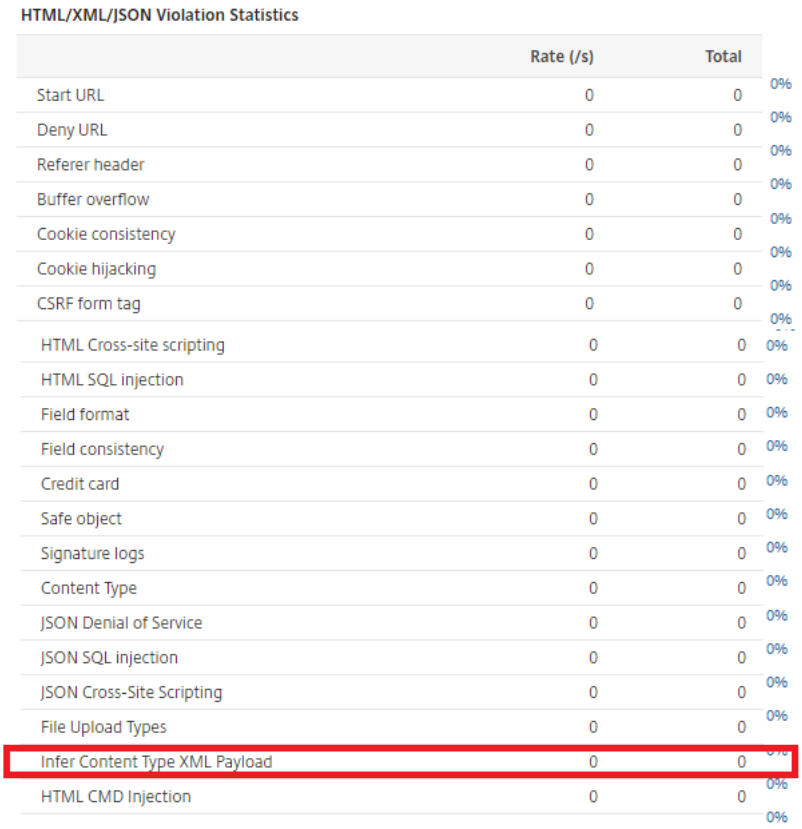
Geben Sie in der Befehlszeile Folgendes ein:

```
stat appfw profile profile1
```

Anzeigen von XXE-Injektionsstatistiken mithilfe der NetScaler-GUI

Gehen Sie wie folgt vor, um die XXE-Injektionsstatistiken einzusehen:

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Web App Firewall-Profil aus und klicken Sie auf **Statistiken**.
3. Auf der Seite mit den **NetScaler Web App Firewall-Statistiken** werden der Datenverkehr und die Verstöße gegen XXE-Befehlsinjektionen angezeigt.
4. Sie können die **Tabellarische Ansicht** wählen oder zur **grafischen Ansicht** wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.



HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%

Überprüfung des Pufferüberlaufs

May 11, 2023

Die Pufferüberlaufprüfung erkennt Versuche, einen Pufferüberlauf auf dem Webserver zu verursachen. Wenn die Web App Firewall feststellt, dass die URL, die Cookies oder der Header länger als die konfigurierte Länge sind, blockiert sie die Anfrage, da dies zu einem Pufferüberlauf führen kann.

Die Pufferüberlaufprüfung verhindert Angriffe auf unsichere Betriebssystem- oder Webserver-Software, die abstürzen oder sich unvorhersehbar verhalten können, wenn sie eine Datenzeichenfolge empfängt, die größer ist als sie verarbeiten kann. Richtige Programmiertechniken verhindern Pufferüberläufe, indem eingehende Daten überprüft werden und überlange Zeichenketten entweder zurückgewiesen oder gekürzt werden. Viele Programme überprüfen jedoch nicht alle eingehenden Daten und sind daher anfällig für Pufferüberläufe. Dieses Problem betrifft insbesondere ältere Versionen von Web-Server-Software und Betriebssystemen, von denen viele noch verwendet werden.

Mit der Sicherheitsüberprüfung Buffer Overflow können Sie die Aktionen **Block**, **Log**und **Stats** konfigurieren. Darüber hinaus können Sie auch die folgenden Parameter konfigurieren:

- **Maximale URL-Länge**. Die maximale Länge, die die Web App Firewall in einer angeforderten URL zulässt. Anfragen mit längeren URLs werden blockiert. **Mögliche Werte**: 0—65535. **Standard**: 1024
- **Maximale Cookielänge**. Die maximale Länge, die die Web App Firewall für alle Cookies in einer Anfrage zulässt. Anfragen mit längeren Cookies lösen die Verstöße aus. **Mögliche Werte**: 0—65535. **Standard**: 4096
- **Maximale Kopfzeilenlänge**. Die maximale Länge, die die Web App Firewall für HTTP-Header zulässt. Anfragen mit längeren Kopfzeilen werden blockiert. **Mögliche Werte**: 0—65535. **Standard**: 4096
- **Länge der Abfragezeichenfolge**. Maximal zulässige Länge für eine Abfragezeichenfolge in einer eingehenden Anfrage. Anfragen mit längeren Abfragen werden blockiert. Mögliche Werte: 0—65535. Standard: 1024
- **Gesamtlänge der Anfrage**. Maximale Anforderungslänge für eine eingehende Anforderung. Anfragen mit längerer Länge werden blockiert. Mögliche Werte: 0—65535. Standard: 24820

Konfiguration der Buffer Overflow-Sicherheitsprüfung über die Befehlszeile

So konfigurieren Sie Buffer Overflow, Sicherheitsüberprüfungsaktionen und andere Parameter mithilfe der Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <name> -bufferOverflowMaxURLLength <positive_integer> -
bufferOverflowMaxHeaderLength <positive_integer> - bufferOverflowMaxCookieLength
```



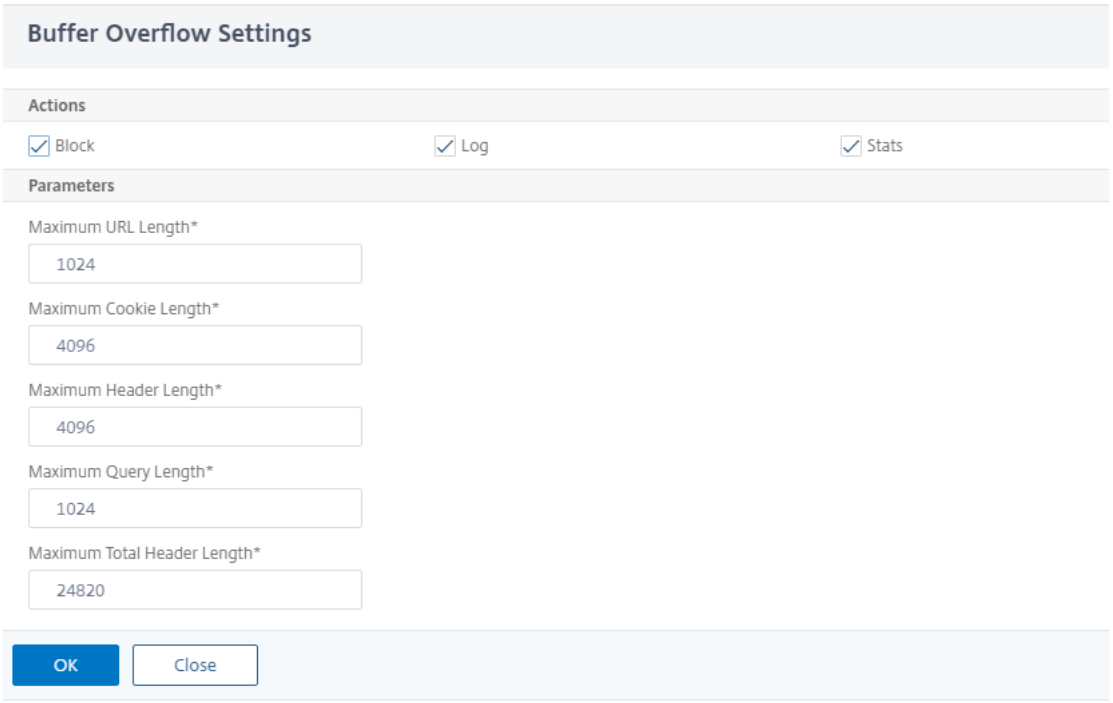
```
 <positive_integer> -bufferOverflowMaxQueryLength <positive_integer> -
bufferOverflowMaxTotalHeaderLength <positive_integer>
```

Beispiel:

```
add appfw profile profile1 -bufferOverflowMaxURLLength 7000 -bufferOverflowMaxHeaderLe
 7250 - bufferOverflowMaxCookieLength 7100 -bufferOverflowMaxQueryLength
7300 -bufferOverflowMaxTotalHeaderLength 7300
```

Konfigurieren Sie die Sicherheitsprüfung für den Pufferüberlauf mithilfe der NetScaler-GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** und **Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der **NetScaler Web App Firewall Profilseite** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.
4. Wählen Sie im Abschnitt **Sicherheitsprüfungen** die Option **Buffer Overflow** aus und klicken Sie auf **Aktionseinstellungen**.
5. Stellen Sie auf der Seite **Buffer Overflow Settings** die folgenden Parameter ein.
   a. Aktionen. Wählen Sie eine oder mehrere Aktionen aus, die für die Sicherheitsprüfung durch Command Injection ausgeführt werden sollen.
   b. Maximale URL-Länge. Maximale Länge in Zeichen für URLs auf Ihren geschützten Websites. Anfragen mit längeren URLs werden blockiert.
   c. Maximale Cookielänge. Maximale Länge in Zeichen für Cookies, die an Ihre geschützten Websites gesendet werden. Anfragen mit längeren Cookies werden blockiert.
   d. Maximale Header-Länge. Maximale Länge in Zeichen für HTTP-Header in Anfragen, die an Ihre geschützten Websites gesendet werden. Anfragen mit längeren Kopfzeilen werden blockiert.
   e. Maximale Abfragelänge. Maximale Länge in Byte für eine Abfragezeichenfolge, die an Ihre geschützten Websites gesendet wird. Anfragen mit längeren Abfragezeichenfolgen werden blockiert.
   f. Maximale Gesamt-Header-Länge. Maximale Länge in Byte für die gesamte HTTP-Headerlänge von Anfragen, die an Ihre geschützten Websites gesendet werden. Der Mindestwert von this und maxHeaderLen in HttpProfile wird verwendet. Anfragen mit längerer Länge werden blockiert.
6. Klicken Sie auf **OK** und auf **Schließen**.



Verwendung der Protokollfunktion mit dem Buffer Overflow Security Check

****Wenn die Protokollaktion aktiviert ist, werden die Verstöße gegen die Buffer Overflow-Sicherheitsprüfung im Audit-Log als **APPFW_BUFFEROVERFLOW_URL-, APPFW_BUFFEROVERFLOW_COOK und APPFW_BUFFEROVERFLOW_HDR-Verstößeprotokolliert.**** Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

Wenn Sie die Protokolle mithilfe der GUI überprüfen, können Sie die Click-to-Deploy-Funktion verwenden, um die in den Protokollen angegebenen Lockerungen vorzunehmen.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und verfolgen Sie die ns.logs im Ordner **/var/log/, um auf die Logmeldungen** zuzugreifen, die sich auf die Buffer Overflow-Verstöße beziehen:

```
1 > \*\*Shell\*\*
2 > \*\*tail -f /var/log/ns.log | grep APPFW_BUFFEROVERFLOW\*\*
3 <!--NeedCopy-->
```

Beispiel für eine CEF-Protokollmeldung, die eine BufferOverflowMaxCookieLength-Verletzung im Nichtblockmodus anzeigt

```
1 Oct 22 17:35:20 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
      .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_COOKIE\*\*|6|src=10.217.253.62
```



```
    geolocation=Unknown spt=41198 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=Cookie header length(43) is
    greater than maximum allowed(16).\*\* cn1=119 cn2=465 cs1=
    owa_profile cs2=PPE1 cs3=wvOOOb+cJ2ZRbstZpyeNXIqLj7Y0001 cs4=ALERT
    cs5=2015 \*\*act=not blocked\*\*
<!--NeedCopy-->
```

Beispiel für eine CEF-Protokollmeldung, die eine BufferOverflowMaxUrlLength-Verletzung im Nicht-Blockmodus anzeigt

```
Oct 22 18:39:56 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_URL\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=19171 method=GET request=http://aaron.
    stratum8.net/FFC/sc11.html \*\*msg=URL length(39) is greater than
    maximum allowed(20).\*\* cn1=707 cn2=402 cs1=owa_profile cs2=PPE0
    cs3=kW49GcKbnwKByByi3+jeNzfgWa80000 cs4=ALERT cs5=2015 \*\*act=not
    blocked\*\*
<!--NeedCopy-->
```

Beispiel für eine Logmeldung im Native Format, die eine BufferOverflowMaxHeaderLength-Verletzung im Blockmodus anzeigt

```
Oct 22 18:44:00 <local0.info> 10.217.31.98 10/22/2015:18:44:00 GMT ns
    0-PPE-2 : default APPFW \*\*APPFW_BUFFEROVERFLOW_HDR\*\* 155 0 :
    10.217.253.62 374-PPE2 khhBEeY4DB8V2D3H2sMLkXmfWnA0002 owa_profile
    \*\*Header(User-Agent) length(82) is greater than maximum allowed
    (10)\*\* : http://aaron.stratum8.net/ \*\*<blocked>\*\*
<!--NeedCopy-->
```

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die GUI enthält ein nützliches Tool (**Syslog Viewer**) zur Analyse der Logmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Application Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Sicherheitsüberprüfungen**. Markieren Sie die Zeile **Buffer Overflow** und klicken Sie auf **Logs**. Wenn Sie direkt über den Buffer Overflow Security Check des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen heraus und zeigt nur die Protokolle an, die sich auf diese Sicherheitsüberprüfungsverstöße beziehen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Prüfmeldungen auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung. Dies ist nützlich für das

Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen ausgelöst werden können.

- Navigieren Sie zu **Application Firewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt **Prüfmeldungen** auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung.

Der XML-basierte Syslog-Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **Pufferüberlaufprüfung** auszuwählen, filtern Sie, indem Sie **APPFW** in der Dropdownliste Optionen für **Modul** auswählen. **Die Liste der**Ereignistypen**bietet drei Optionen:**APPFW_BUFFEROVERFLOW_URL, APPFW_BUFFEROVERFLOW_COOKIE und A PPFW_BUFFEROVERFLOW_HDR****, um alle Protokollmeldungen anzuzeigen, die sich auf die Sicherheitsüberprüfung**für den Pufferüberlauf beziehen.** Sie können eine oder mehrere Optionen auswählen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_BUFFEROVERFLOW_COOKIE** aktivieren und auf die Schaltfläche **Anwenden** klicken, werden im Syslog-Viewer nur Protokollmeldungen angezeigt, die sich auf Verstöße gegen die **Buffer Overflow-Sicherheitsprüfung** für den Cookie-Header beziehen. Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollmeldung setzen, werden unter der Protokollmeldung mehrere Optionen wie **Modul**, **Ereignistyp, Ereignis-ID**und **Client-IP**angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Click-to-Deploy: Die GUI bietet Click-to-Deploy-Funktionen, die derzeit nur für die Pufferüberlauf-Logmeldungen unterstützt werden, die sich auf Verstöße gegen die URL-Länge beziehen. Mit dem Syslog-Viewer können Sie nicht nur die ausgelösten Verstöße einsehen, sondern auch fundierte Entscheidungen treffen, die auf der beobachteten Länge der blockierten Nachrichten basieren. Wenn der aktuelle Wert zu restriktiv ist und falsch positive Ergebnisse auslöst, können Sie eine Nachricht auswählen und sie bereitstellen, um den aktuellen Wert durch den in der Nachricht angezeigten URL-Längenwert zu ersetzen. Die Protokollmeldungen müssen für diesen Vorgang im CEF-Protokollformat vorliegen. Wenn die Lockerung für eine Protokollmeldung eingesetzt werden kann, wird am rechten Rand des**Syslog-Viewer-Felds in der Zeile**ein Kontrollkästchen angezeigt. Markieren Sie das Kontrollkästchen und wählen Sie dann eine Option aus der**Aktionsliste**aus, um die Entspannung bereitzustellen.**“Bearbeiten und Bereitstellen**”, “**Bereitstellen**” und “**Alle bereitstellen**” sind als**Aktionsoptionen**verfügbar. Sie können den Filter**APPFW_BUFFEROVERFLOW_URL** verwenden, um alle Protokollnachrichten zu isolieren, die sich auf die konfigurierten URL-Längenverletzungen beziehen.

Wenn Sie eine einzelne Protokollnachricht auswählen, sind alle drei Aktionsoptionen **Bearbeiten und Bereitstellen, Bereitstellenund Alle bereitstellen** verfügbar. Wenn Sie **Bearbeiten und Deploy**wählen, wird das Dialogfeld mit den **Buffer Overflow-Einstellungen** angezeigt. Die neue URL-Länge, die in der Anfrage beobachtet wurde, wird in das **Eingabefeld Maximale URL-Länge**

eingefügt. Wenn Sie ohne Änderungen auf **Schließen** klicken, bleiben die aktuell konfigurierten Werte unverändert. Wenn Sie auf die Schaltfläche **OK** klicken, ersetzt der neue Wert der maximalen URL-Länge den vorherigen Wert.

> **Hinweis**
>
> Die Kontrollkästchen für **Block**-, **Protokoll** - und **Statistikaktionen** sind im angezeigten **Einstellungsdialog für Buffer Overflow** deaktiviert und müssen neu konfiguriert werden, wenn Sie die Option **Bearbeiten und** Bereitstellen auswählen. Stellen Sie sicher, dass diese Kontrollkästchen aktiviert sind, bevor Sie auf **OK**klicken. Andernfalls wird die neue URL-Länge konfiguriert, die Aktionen jedoch auf „ **Keine**“ gesetzt.

Wenn Sie die Kontrollkästchen für mehrere Protokollmeldungen aktivieren, können Sie die Option **Bereitstellen** oder **Alle bereitstellen** verwenden. Wenn die bereitgestellten Protokollnachrichten unterschiedliche URL-Längen haben, wird der konfigurierte Wert durch den höchsten Wert für die URL-Länge ersetzt, der in den ausgewählten Nachrichten beobachtet wurde. Die Bereitstellung der Regel führt nur dazu, dass der Wert von **bufferOverflowMaxUrlLength** geändert wird. Konfigurierte Aktionen werden beibehalten und bleiben unverändert.

Um die Click-to-Deploy-Funktionalität in der GUI zu verwenden

1. Wählen Sie im Syslog Viewer in den **ModuloptionenAPPFW** aus.
2. **Aktivieren Sie das Kontrollkästchen**APPFW_BUFFEROVERFLOW_URL**als Ereignistyp, um die entsprechenden Protokollmeldungen zu filtern.**
3. Aktivieren Sie das Kontrollkästchen, um die Regel auszuwählen.
4. Verwenden Sie die Dropdownliste **Aktion** mit den Optionen, um die Entspannung einzusetzen.
5. Navigieren Sie zu **Application Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Sicherheitsprüfungen**, um den Bereich mit den Einstellungen für den **Buffer Overflow** aufzurufen und zu überprüfen, ob der Wert für die **maximale URL-Länge** aktualisiert wurde.

Statistiken für die Buffer Overflow-Verstöße

Wenn die Statistikaktion aktiviert ist, wird der Zähler für die Pufferüberlauf-Sicherheitsprüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Aktion Blockieren aktiviert ist, erhöht eine Anfrage für eine Seite, die drei Buffer Overflow-Verstöße enthält, den Statistikzähler um eins, da die Seite blockiert wird, wenn der erste Verstoß erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anfrage den Statistikzähler für Verstöße, da bei jeder Verletzung eine separate Protokollmeldung generiert wird.

So zeigen Sie die Buffer Overflow Security Check-Statistiken mithilfe der Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

```
> sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> stat appfw profile <profile name>
```

So zeigen Sie Buffer Overflow-Statistiken mithilfe der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Anwendungsfirewall**.
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Scrollleiste, um die Statistiken zu Buffer Overflow-Verstößen und Protokollen einzusehen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

- Mit der Pufferüberlauf-Sicherheitsprüfung können Sie Grenzwerte konfigurieren, um die maximale Länge der zulässigen URLs, Cookies und Header durchzusetzen.
- Mit den Aktionen**Block**, **Log** und **Stats** können Sie den Datenverkehr überwachen und den optimalen Schutz für Ihre Anwendung konfigurieren.
- Mit dem Syslog-Viewer können Sie alle Protokollmeldungen filtern und anzeigen, die sich auf Verstöße gegen den Pufferüberlauf beziehen.
- Die**Click-to-Deploy-Funktion** wird für die **BufferOverflowMaxURLength-Verstöße** unterstützt. Sie können eine einzelne Regel auswählen und implementieren, oder Sie können mehrere Protokollnachrichten auswählen, um den aktuell konfigurierten Wert der maximal zulässigen Länge der URL zu optimieren und zu lockern. Der höchste Wert der URL aus der ausgewählten Gruppe wird als neuer Wert festgelegt, um all diese Anfragen zuzulassen, die derzeit als Verstöße gekennzeichnet sind.
- Die Web App Firewall wertet jetzt einzelne Cookies aus, wenn sie die eingehende Anfrage untersucht. Wenn die Länge eines im Cookie-Header empfangenen Cookies die konfigurierte **BufferOverflowMaxCookieLength überschreitet, wird die Buffer Overflow-Verletzung**ausgelöst.

> **Wichtig**
>
> In Version 10.5.e (in einigen Versionen mit Zwischenverbesserungen vor dem Build 59.13xx.e) und in der Version 11.0 (in Builds vor 65.x) wurde die Verarbeitung des Cookie-Headers durch die Web App Firewall geändert. In diesen Versionen wird jedes Cookie einzeln ausgewertet, und wenn die Länge eines im Cookie-Header empfangenen Cookies die konfigurierte bufferOverflowMaxCookieLength überschreitet, wird die Pufferüberlaufverletzung ausgelöst. Infolge dieser Änderung sind Anforderungen, die in 10.5 und früheren Release-Builds blockiert wurden, möglicherweise zulässig, da die Länge des gesamten Cookie-Headers nicht für die Bestimmung

> der Cookie-Länge berechnet wird. ** In einigen Situationen ist die gesamte Cookie-Größe, die an den Server weitergeleitet wird, möglicherweise größer als der akzeptierte Wert, und der Server reagiert möglicherweise mit “400 Bad Request”.
>
> Diese Änderung wurde rückgängig gemacht. Das Verhalten in den 10.5.e ->59.13xx.e und nachfolgenden 10.5.e-Erweiterungsversionen zusätzlich zu Version 65.x 11.0 und nachfolgenden Builds ähnelt jetzt dem der Builds ohne Erweiterung von Version 10.5. Der gesamte rohe Cookie-Header wird jetzt bei der Berechnung der Länge des Cookies berücksichtigt. Umgebende Räume und die Semikolon-Zeichen (;), die die Name-Wert-Paare trennen, werden ebenfalls bei der Bestimmung der Cookie-Länge berücksichtigt.

Web App Firewall-Unterstützung für das Google Web Toolkit

May 11, 2023

Hinweis: Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

Webserver, die den Remote Procedure Call (RPC) -Mechanismen des Google Web Toolkit (GWT) folgen, können durch die NetScaler Web App Firewall gesichert werden, ohne dass eine spezielle Konfiguration erforderlich ist, um die GWT-Unterstützung zu aktivieren.

Was ist GWT

Das GWT wird für die Erstellung und Optimierung komplexer Hochleistungs-Webanwendungen von Personen verwendet, die keine Erfahrung mit XMLHttpRequest und JavaScript haben. Dieses kostenlose Open-Source-Entwicklungs-Toolkit wird in großem Umfang für die Entwicklung kleiner und großer Anwendungen verwendet und häufig für die Anzeige von browserbasierten Daten wie Suchergebnissen für Flüge, Hotels usw. verwendet. Das GWT bietet einen Kernsatz von Java-APIs und Widgets zum Schreiben optimierter JavaScript-Skripts, die auf den meisten Browsern und mobilen Geräten ausgeführt werden können. Das GWT RPC-Framework erleichtert den Client- und Serverkomponenten der Webanwendung den Austausch von Java-Objekten über HTTP. GWT RPC-Dienste sind nicht dasselbe wie Webdienste, die auf SOAP oder REST basieren. Sie sind einfach eine einfache Methode für die Übertragung von Daten zwischen dem Server und der GWT-Anwendung auf dem Client. GWT kümmert sich um die Serialisierung der Java-Objekte und tauscht die Argumente in den Methodenaufrufen und den Rückgabewert aus.

Beliebte Websites, die GWT verwenden, finden Sie unter

https://www.quora.com/What-web-applications-use-Google-Web-Toolkit-%28GWT%29

So funktioniert eine GWT-Anfrage

Die GWT-RPC-Anfrage ist durch eine Pipe getrennt und hat eine variable Anzahl von Argumenten. Es wird als Payload von HTTP POST übertragen und hat die folgenden Werte:

1. Inhaltstyp = text/x-gwt-rpc. Charset kann ein beliebiger Wert sein.
2. Methode = POST.

Sowohl GET- als auch POST-HTTP-Anfragen werden als gültige GWT-Anfragen betrachtet, wenn der Inhaltstyp „text/x-gwt-rpc“ ist. Abfragezeichenfolgen werden jetzt als Teil von GWT-Anfragen unterstützt. Konfigurieren Sie den Parameter „inspectQueryContentTypes“ des App Firewall-Profils auf „OTHER“, um den Anforderungsabfrageteil auf den Inhaltstyp „text/x-gwt-rpc“ zu untersuchen.

Das folgende Beispiel zeigt eine gültige Payload für eine GWT-Anfrage:

```
1 5|0|8|http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com
     .test.client.TestService|testMethod|java.lang.String|java.lang.
     Integer| myInput1|java.lang.Integer/3438268394|1|2|3|4|2|5|6|7|8|1|
2 <!--NeedCopy-->
```

Die Anfrage kann in drei Teile unterteilt werden:

a) `Header: 5|0|8|`

Die ersten 3 Ziffern `5|0|8|` in der obigen Anfrage stehen jeweils für “Version, Subversion und Größe der Tabelle”. Dies müssen positive Ganzzahlen sein.

b) Stringtabelle:

```
http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com.test.
client.TestService|testMethod|java.lang.String|java.lang.Integer|myInput1|
java.lang.Integer/3438268394|
```

Die Elemente der obigen durch Pipe getrennten Zeichenfolgentabelle enthalten die vom Benutzer bereitgestellten Eingaben. Diese Eingaben werden für die Web App Firewall-Prüfungen analysiert und wie folgt identifiziert:

- 1.: `http://localhost:8080/test/`

  Dies ist die Anforderungs-URL.

- 2.: `16878339F02B83818D264AE430C20468`

  Eindeutige HEX-Kennung. Eine Anfrage gilt als falsch formatiert, wenn diese Zeichenfolge Nicht-Hex-Zeichen enthält.

- 3.: `com.test.client.TestService`

  Name der Serviceklasse

- 4.: `testMethod`

  Name der Servicemethode

- Ab 5.: `java.lang.String|java.lang.Integer|myInput1|java.lang.Integer/3438268394`

  Datentypen und Daten. Nicht-primitive Datentypen werden spezifiziert als

  `<container>.<sub-cntnr>.name/<integer><identifier>`

c) `Payload`: `1|2|3|4|2|5|6|7|8|1|`

Die Payload besteht aus Verweisen auf die Elemente in der String-Tabelle. Diese Ganzzahlwerte können nicht größer sein als die Anzahl der Elemente in der Zeichenfolgentabelle.

Web App Firewall-Schutz für GWT-Anwendungen

Die Web App Firewall versteht und interpretiert GWT-RPC-Anfragen, überprüft die Payload auf Verstöße gegen die Sicherheitsüberprüfung und ergreift bestimmte Maßnahmen.

Die Header- und Cookie-Prüfungen der Web App Firewall für GWT-Anfragen ähneln denen für andere Anforderungsformate. Nach der entsprechenden URL-Dekodierung und Zeichensatzkonvertierung werden alle Parameter in der Stringtabelle überprüft. Der GWT-Anforderungstext enthält keine Feldnamen, sondern nur die Feldwerte. Die Eingabewerte können anhand des angegebenen Formats überprüft werden, indem die Web App Firewall Field Format Check verwendet wird, mit der auch die Länge der Eingabe gesteuert werden kann. Die **Cross-Site Scripting** - und **SQL-Injection-Angriffe** in den Eingaben können von der Web App Firewall leicht erkannt und vereitelt werden.

Lern- und Entspannungsregeln: Das Erlernen und Anwenden von Entspannungsregeln werden für GWT-Anfragen unterstützt. Die Web App Firewall-Regeln haben die Form von <actionURL> <fieldName>. Das GWT-Anforderungsformat hat keine Feldnamen und erfordert daher eine spezielle Behandlung. Die Web App Firewall fügt Dummy-Feldnamen in die erlernten Regeln ein, die als Relaxationsregeln verwendet werden können. Das -isRegex-Flag funktioniert genauso wie bei Regeln, die nicht unter GWT fallen.

- Aktions-URL:

  Mehrere Dienste, die auf einen RPC reagieren, können auf demselben Webserver konfiguriert werden. Die HTTP-Anfrage hat die URL des Webservers, nicht des eigentlichen Dienstes, der den RPC verarbeitet. Daher wird die Entspannung nicht auf der Grundlage der HTTP-Anforderungs-URL angewendet, da dies alle Dienste auf dieser URL für das Zielfeld lockern würde. Für GWT-Anfragen verwendet die Web App Firewall die URL des tatsächlichen Dienstes, der in der GWT-Payload im vierten Feld der String-Tabelle zu finden ist.

- Feldname:

Da der GWT-Anforderungstext nur Feldwerte enthält, fügt die Web App Firewall bei der Empfehlung erlernter Regeln Scheinfeldnamen wie 1, 2 usw. ein.

Beispiel für eine gelernte GWT-Regel

```
POST /abcd/def/gh HTTP/1.1
Content-type: text/x-gwt-rpc
Host: 10.217.222.75
Content-length: 157

5|0|8|http://localhost:8080/acdtest/|16878339
   F02Baf83818D264AE430C20468|
com.test.client.TestService|testMethod|java.lang.String%3b|java.
   lang.Integer|onblur|

  The learn data will be as follows:
> sh learningdata pr1 crossSiteScripting
Profile: pr1    SecurityCheck: crossSiteScripting
1)  Url:    http://localhost:8080/acdtest/  >> From GWT Payload.
    Field:  10
    Hits:   1
 Done
<!--NeedCopy-->
```

Beispiel für eine GWT-Relaxationsregel

```
bind appfw profile pr1 -crossSiteScripting 1 abcd -isregex NOTREGEX
```

Protokollmeldungen: Die Web App Firewall generiert Protokollmeldungen für die Verstöße gegen die Sicherheitsüberprüfung, die in den GWT-Anfragen festgestellt wurden. Eine durch eine falsch formatierte GWT-Anfrage generierte Protokollnachricht enthält zur einfachen Identifizierung die Zeichenfolge „GWT“.

Beispiel für eine Lognachricht für eine falsch formatierte GWT-Anfrage:

```
Dec 5 21:48:02 <local0.notice> 10.217.31.247 12/05/2014:21:48:02 GMT ns
0-PPE-0 : APPFW Message 696 0 : "GWT RPC request with malformed payload. <
blocked>”
```

Unterschied bei der Verarbeitung von GWT- und Nicht-GWT-Anfragen:

Dieselbe Payload kann verschiedene Verstöße gegen die Web App Firewall-Sicherheitsüberprüfung für verschiedene Inhaltstypen auslösen. Betrachten Sie das folgende Beispiel:

```
5|0|8|http://localhost:8080/acdtest/|16878339F02Baf83818D264AE430C20468|com
.test.client.TestService|testMethod|java.lang.String%3b|java.lang.Integer|
select|
```


Inhaltstyp: application/x-www-form-urlencoded:

Eine mit diesem Inhaltstyp gesendete Anfrage führt zu einer SQL-Verletzung, wenn der SQL Injection Type so konfiguriert ist, dass er eine der vier verfügbaren Optionen verwendet: sqlSplcharAndKeyword, sqlSplcharOrKeyword, sqlKeyword oder sqlSplChar. Die Web App Firewall betrachtet bei der Verarbeitung der obigen Payload '&' als Feldtrennzeichen und '=' als das Name-Wert-Trennzeichen. Da keines dieser Zeichen irgendwo im Beitragstext vorkommt, wird der gesamte Inhalt als ein einziger Feldname behandelt. Der Feldname in dieser Anfrage enthält sowohl ein SQL-Sonderzeichen (;) als auch ein SQL-Schlüsselwort (select). Daher werden Verstöße für alle vier SQL-Injection-Typoptionen erkannt.

Inhaltstyp: text/x-gwt-rpc:

Eine mit diesem Inhaltstyp gesendete Anfrage löst nur dann eine SQL-Verletzung aus, wenn der SQL-Injection-Typ auf eine der folgenden drei Optionen gesetzt ist: SqlSplcharOrKeyword, SqlKeyword oder SqlSplChar. Es wird keine Verletzung ausgelöst, wenn der SQL-Injektionstyp auf sqlSplcharAndKeyword gesetzt ist, was die Standardoption ist. Die Web App Firewall betrachtet den vertikalen Balken | als Feldtrennzeichen für die obige Payload in der GWT-Anfrage. Daher wird der Beitragstext in verschiedene Formularfeldwerte unterteilt, und Formularfeldnamen werden hinzugefügt (gemäß der zuvor beschriebenen Konvention). Aufgrund dieser Aufteilung werden das SQL-Sonderzeichen und das SQL-Schlüsselwort zu Teilen separater Formularfelder.

Formularfeld 8: `java.lang.String%3b -\> %3b is the (;)char`

Formularfeld 10: `select`

Wenn der SQL-Injection-Typ auf **SQLSplChar**gesetzt ist, gibt Feld 8 daher die SQL-Verletzung an. Für **SqlKeyword**gibt Feld 10 den Verstoß an. Jedes dieser beiden Felder kann auf eine Verletzung hinweisen, wenn der SQL-Inject-Typ mit der Option **SqlSplCharOrKeyword** konfiguriert ist, die nach dem Vorhandensein eines Schlüsselworts oder eines Sonderzeichens sucht. ****Für die Standardoption **SqlSplCharAndKeyword** wurde kein Verstoß festgestellt, da es kein einzelnes Feld gibt, das einen Wert hat, der sowohl SqlSplChar als auch SqlKeyword zusammen enthält.****

Tipps:

- Es ist keine spezielle Web App Firewall-Konfiguration erforderlich, um die GWT-Unterstützung zu aktivieren.
- Der Inhaltstyp muss text/x-gwt-rpc sein.
- Das Erlernen und Implementieren der Lockerungsregeln für alle relevanten Web App Firewall-Sicherheitsprüfungen, die auf GWT-Payload angewendet werden, funktioniert genauso wie bei den anderen unterstützten Inhaltstypen.
- Nur POST-Anfragen werden für GWT als gültig angesehen. Alle anderen Anforderungsmethoden werden blockiert, wenn der Inhaltstyp text/x-gwt-rpc ist.
- GWT-Anfragen unterliegen dem konfigurierten POST-Body-Limit des Profils.

- Die Einstellung „Sitzungslos“ für die Sicherheitsüberprüfungen ist nicht anwendbar und wird ignoriert.
- Das CEF-Protokollformat wird für die GWT-Protokollnachrichten unterstützt.

Cookie-Schutz

May 11, 2023

Ein Cookie ist ein kleines Datenpaket, das von einem Webserver an einen Clientbrowser gesendet wird. Cookies enthalten sensible Daten wie Kennwörter, Details zur Benutzerauthentifizierung und Anmeldeinformationen über eine HTTP-Verbindung und werden in einem Webbrowser gespeichert. Daher ist es äußerst wichtig, Cookies vor Angreifern zu schützen, die Informationen stehlen.

Konsistenzprüfung von Cookies: Untersucht Cookies, die bei Benutzeranfragen zurückgegeben werden, um sicherzustellen, dass sie mit den Cookies übereinstimmen, die Ihr Webserver für diesen Benutzer gesetzt hat. Wenn ein modifiziertes Cookie gefunden wird, wird es aus der Anforderung entfernt, bevor die Anforderung an den Webserver weitergeleitet wird. Weitere Informationen finden Sie unter Thema Überprüfung der Cookie-Konsistenzprüfung .

Schutz vor Cookie-Hijacking: Hijacking bezieht sich auf eine Situation, in der ein Angreifer einen unbefugten Zugriff auf Cookies erhält. Um Cookie vor autorisiertem Zugriff zu schützen, fordert die NetScaler Web App Firewall (WAF) die TLS-Verbindung vom Client zusammen mit der WAF-Cookie-Konsistenzvalidierung heraus. Für jede neue Clientanforderung validiert die Appliance die TLS-Verbindung und überprüft auch die Konsistenz von Anwendungs- und Sitzungscookie in der Anforderung. Weitere Informationen finden Sie unter Thema Schutz bei Cookie-Hijacking .

`SameSite` SameSite-Cookie-Attribut: Das Attribut in der Set-Cookie-HTTP-Antwort ermöglicht es Ihnen zu erklären, ob Ihr Cookie auf einen Erstanbieter- oder gleichen Site-Kontext beschränkt sein muss. Die Cookie-Einstellung mindert Angriffe und bietet eine gesicherte Webkommunikation. Weitere Informationen finden Sie unter Thema SameSite-Cookie-Attribut .

Überprüfung der Cookie-Konsistenz

January 26, 2023

Bei der Cookie-Konsistenzprüfung werden von Benutzern zurückgegebene Cookies untersucht, um sicherzustellen, dass sie mit den Cookies übereinstimmen, die Ihre Website für diesen Benutzer festgelegt hat. Wenn ein modifiziertes Cookie gefunden wird, wird es aus der Anforderung entfernt, bevor die Anfrage an den Webserver weitergeleitet wird. Sie können die Cookie-Konsistenzprüfung auch so konfigurieren, dass alle von ihm verarbeiteten Server-Cookies umgewandelt werden, indem Sie die

Cookies verschlüsseln, die Cookies per Proxy senden oder Flags zu den Cookies hinzufügen. Diese Prüfung gilt für Anfragen und Antworten.

Ein Angreifer würde normalerweise ein Cookie modifizieren, um Zugriff auf sensible private Informationen zu erhalten, indem er sich als zuvor authentifizierter Benutzer ausgibt, oder um einen Pufferüberlauf zu verursachen. Die Pufferüberlaufprüfung schützt vor Versuchen, einen Pufferüberlauf zu verursachen, indem ein langes Cookie verwendet wird. Die Cookie-Konsistenzprüfung konzentriert sich auf das erste Szenario.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Cookie-Konsistenzprüfung ändern auf der Registerkarte
Allgemein die folgenden Aktionen aktivieren oder deaktivieren:

- Blockieren
- Protokoll
- Erfahren Sie mehr
- Statistik
- Transformieren. Wenn diese Option aktiviert ist, ändert die Aktion “Transformieren” alle Cookies wie in den folgenden Einstellungen angegeben:
  - **Verschlüsseln von Servercookies.** Verschlüsseln Sie die von Ihrem Webserver gesetzten Cookies, mit Ausnahme der in der Entspannungsliste zur Überprüfung der Cookie-Konsistenz aufgeführten Cookies, bevor Sie die Antwort an den Client weiterleiten. Verschlüsselte Cookies werden entschlüsselt, wenn der Client eine nachfolgende Anfrage sendet, und die entschlüsselten Cookies werden wieder in die Anfrage eingefügt, bevor sie an den geschützten Webserver weitergeleitet werden. Geben Sie eine der folgenden Verschlüsselungsarten an:
    * **None.** Verschlüsseln oder entschlüsseln Sie keine Cookies. Die Standardeinstellung.
    * **Nur entschlüsseln.** Entschlüsseln Sie nur verschlüsselte Cookies. Verschlüsseln Sie keine Cookies.
    * **Nur Sitzung verschlüsseln.** Verschlüsseln Sie nur Sitzungscookies. Verschlüsseln Sie keine persistenten Cookies. Entschlüsseln Sie alle verschlüsselten Cookies.
    * **Verschlüsseln Sie alles.** Verschlüsseln Sie sowohl Sitzungs- als auch dauerhafte Cookies. Entschlüsseln Sie alle verschlüsselten Cookies.
      Hinweis: Beim Verschlüsseln von Cookies fügt die Web App Firewall dem Cookie das **HttpOnly-Flag** hinzu. Dieses Flag verhindert, dass Skripts auf den Cookie zugreifen und diese analysieren. Das Flag verhindert daher, dass ein skriptbasierter Virus oder Trojaner auf ein entschlüsseltes Cookie zugreift und diese Informationen verwendet, um die Sicherheit zu verletzen. Dies erfolgt unabhängig von den Parametereinstellungen für hinzuzufügende Flags in Cookies, die unabhängig von den Parametereinstellungen für Server-Cookies verschlüsseln gehandhabt werden.
- **Proxyserver Cookies.** Proxy für alle nicht persistenten (Sitzungs-) Cookies, die von Ihrem Webserver gesetzt wurden, mit Ausnahme der Cookies, die in der Entspannungsliste für die

Prüfung der Cookies werden mithilfe des vorhandenen Web App Firewall-Sitzungscookies per Proxy übertragen. Die Web App Firewall entfernt Sitzungscookies, die vom geschützten Webserver gesetzt wurden, und speichert sie lokal, bevor die Antwort an den Client weitergeleitet wird. Wenn der Client eine nachfolgende Anfrage sendet, fügt die Web App Firewall die Sitzungscookies erneut in die Anforderung ein, bevor sie an den geschützten Webserver weitergeleitet werden. Geben Sie eine der folgenden Einstellungen an:

- **None.** Verwenden Sie keine Proxycookies. Die Standardeinstellung.
- **Nur Sitzung.** Nur Proxysitzungscookies. Keine persistenten Cookies als Proxy verwenden Hinweis: Wenn Sie das Cookie-Proxy nach der Aktivierung deaktivieren (setzen Sie diesen Wert auf Keine, nachdem es auf Nur Sitzung gesetzt wurde), wird die Cookie-Proxying für Sitzungen beibehalten, die vor der Deaktivierung eingerichtet wurden. Sie können diese Funktion daher sicher deaktivieren, während die Web App Firewall Benutzersitzungen verarbeitet.

- **In Cookies hinzuzufügende Flags**. Fügen Sie während der Transformation Flags zu Cookies hinzu. Geben Sie eine der folgenden Einstellungen an:
  - **None.** Fügen Sie keine Flags zu Cookies hinzu. Die Standardeinstellung.
  - **Nur HTTP.** Füge das HttpOnly-Flag allen Cookies hinzu. Browser, die das HttpOnly-Flag unterstützen, erlauben Skripten keinen Zugriff auf Cookies, für die dieses Flag gesetzt ist
  - **Sicher**. Fügen Sie das Secure-Flag zu Cookies hinzu, die nur über eine SSL-Verbindung gesendet werden sollen. Browser, die das Secure Flag unterstützen, senden die markierten Cookies nicht über eine unsichere Verbindung.
  - **Alles.** Fügen Sie das HttpOnly-Flag zu allen Cookies und das Secure-Flag zu Cookies hinzu, die nur über eine SSL-Verbindung gesendet werden sollen.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um die Cookie-Konsistenzprüfung zu konfigurieren:

- `set appfw profile <name> -cookieConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`
- `set appfw profile <name> -cookieTransforms ([**ON**] | [**OFF**])`
- `set appfw profile <name> -cookieEncryption ([**none**] | [**decryptOnly**] | [**encryptSession**] | [**encryptAll**])`
- `set appfw profile <name> -cookieProxying ([**none**] | [**sessionOnly**])`
- `set appfw profile <name> -addCookieFlags ([**none**] | [**httpOnly**] | [**secure**] | [**all**])`

Um Relaxationen für die Cookie-Konsistenzprüfung festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Checks des Dialogfelds Cookie-Konsistenzprüfung ändern auf Hinzufügen, um das Dialogfeld Cookie-Konsistenzprüfung hinzufügen zu öffnen, oder wählen Sie eine vorhandene Entspannung aus und klicken Sie auf Öffnen, um das Dialogfeld Entspannung der Cookie-Konsistenzprüfung ändern zu öffnen. Beide Dialogfelder bieten dieselben Optionen für die

Konfiguration einer Entspannung.

Im Folgenden finden Sie Beispiele für die Lockerung der Cookie-Konsistenz:

- **Anmeldefelder.** Der folgende Ausdruck befreit alle Cookie-Namen, die mit der Zeichenfolge logon_ beginnen, gefolgt von einer Reihe von Buchstaben oder Zahlen, die mindestens zwei Zeichen lang und nicht mehr als fünfzehn Zeichen lang ist:

```
^logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Anmeldefelder (Sonderzeichen).** Der folgende Ausdruck schließt alle Cookie-Namen aus, die mit der Zeichenfolge türkçe-logon_ beginnen, gefolgt von einer Reihe von Buchstaben oder Zahlen, die mindestens zwei Zeichen lang und nicht mehr als fünfzehn Zeichen lang ist:

```
^txC3xBCrkxC3xA7e-logon_[0-9A-Za-z]{
2,15 }
$
<!--NeedCopy-->
```

- **Beliebige Zeichenfolgen.** Erlaubt, dass Cookies, die die Zeichenfolge sc-item_enthalten, gefolgt von der ID eines Artikels, den der Benutzer zu seinem Warenkorb hinzugefügt hat ([0-9A-Za-z]+), einem zweiten Unterstrich (_) und schließlich der Anzahl dieser Artikel, die er möchte `([1-9][0-9]?)`, vom Benutzer geändert werden können:

```
^sc-item_[0-9A-Za-z]+_[1-9][0-9]?$
<!--NeedCopy-->
```

Achtung: Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und sonst nichts. Die unvorsichtige Verwendung von Wildcards und insbesondere der Punkt-Sternchen-Kombination (.*) kann zu Ergebnissen führen, die Sie nicht wollen oder erwarten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten oder einen Angriff zulassen, den die Cookie-Konsistenzprüfung anderweitig hätte geblockt.

Schutz vor Cookie-Hijacking

May 11, 2023

Der Schutz vor Cookie-Hijacking mildert Angriffe von Hackern, die Cookies stehlen. Bei dem Sicherheitsangriff übernimmt ein Angreifer eine Benutzersitzung, um sich unbefugten Zugriff auf eine Webanwendung zu verschaffen. Wenn ein Benutzer eine Website besucht, beispielsweise eine Bankanwendung, baut die Website eine Sitzung mit dem Browser auf. Während der Sitzung speichert die Anwendung die Benutzerdetails wie Anmeldeinformationen und Seitenbesuche in einer Cookie-Datei. Die Cookie-Datei wird dann in der Antwort an den Client-Browser gesendet. Der Browser speichert die Cookies, um aktive Sitzungen aufrechtzuerhalten. Der Angreifer kann diese Cookies entweder manuell aus dem Cookie-Speicher des Browsers oder über eine Rouge-Browsererweiterung stehlen. Der Angreifer verwendet diese Cookies dann, um Zugriff auf die Webanwendungssitzungen des Benutzers zu erhalten.

Um Cookie-Angriffe abzuwehren, fordert die NetScaler Web App Firewall (WAF) die TLS-Verbindung vom Client zusammen mit der WAF-Cookie-Konsistenzüberprüfung heraus. Für jede neue Clientanforderung validiert die Appliance die TLS-Verbindung und überprüft auch die Konsistenz von Anwendungs- und Sitzungscookie in der Anforderung. Wenn ein Angreifer versucht, Anwendungscookies und Sitzungscookies, die vom Opfer gestohlen wurden, zu mischen und abzugleichen, schlägt die Validierung der Cookie-Konsistenz fehl, und die konfigurierte Cookie-Hijack-Aktion wird angewendet. Weitere Informationen zur Cookie-Konsistenz finden Sie unter Cookie-Konsistenzprüfung.

> **Hinweis:**
>
> Die Cookie-Hijacking-Funktion unterstützt Protokollierung und SNMP-Traps. Weitere Informationen zur Protokollierung finden Sie unter ADM-Thema und weitere Informationen zur SNMP-Konfiguration finden Sie unter SNMP-Thema.

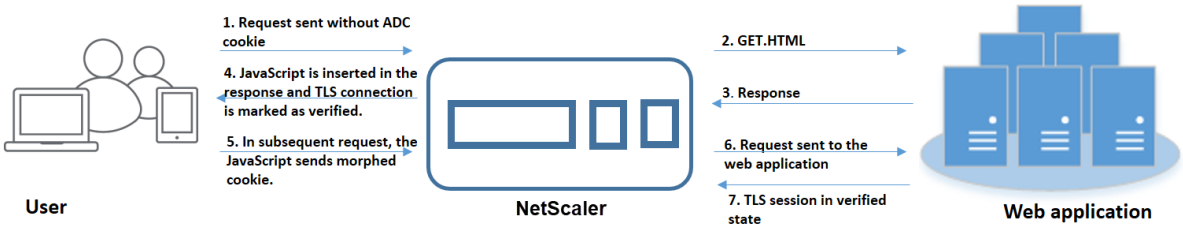
Einschränkungen

- JavaScript muss im Client-Browser aktiviert sein.
- Der Cookie-Hijacking Schutz wird auf TLS Version 1.3 nicht unterstützt.
- Begrenzte Unterstützung für den Internet Explorer (IE) -Browser, da der Browser die SSL-Verbindungen nicht wiederverwendet. Führt zu mehreren Weiterleitungen, die für eine Anfrage gesendet werden, die schließlich zu einem Fehler “MAX READCEED” im IE-Browser führen.

Funktionsweise des Cookie-Hijacking Schutzes

In den folgenden Szenarien wird erläutert, wie der Schutz vor Cookie-Hijacking in einer NetScaler Appliance funktioniert.

Szenario 1: Benutzer, der ohne Sitzungscookie auf die erste Webseite zugreift

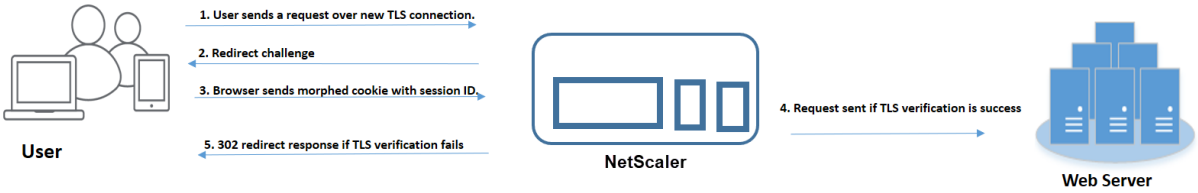


1. Der Benutzer versucht, sich bei einer Webanwendung zu authentifizieren und beginnt, auf die erste Webseite zuzugreifen, ohne dass ein ADC-Sitzungscookie in der Anfrage enthalten ist.
2. Wenn die Anforderung empfangen wird, erstellt die Appliance eine Anwendungs-Firewall-Sitzung mit einer Sitzungscookie-ID.
3. Dadurch wird eine TLS-Verbindung für die Sitzung initiiert. Da das JavaScript nicht gesendet und im Client-Browser ausgeführt wird, markiert die Appliance die TLS-Verbindung als validiert und es ist keine Abfrage erforderlich.

   > **Hinweis:**
   >
   > Selbst wenn ein Angreifer versucht, alle App-Cookie-IDs von einem Opfer zu senden, ohne das Sitzungscookie zu senden, erkennt die Appliance das Problem und entfernt alle App-Cookies in der Anfrage, bevor sie die Anfrage an den Backend-Server weiterleitet. Der Backend-Server berücksichtigt diese Anfrage ohne App-Cookie und nimmt dies gemäß seiner Konfiguration erforderlich.

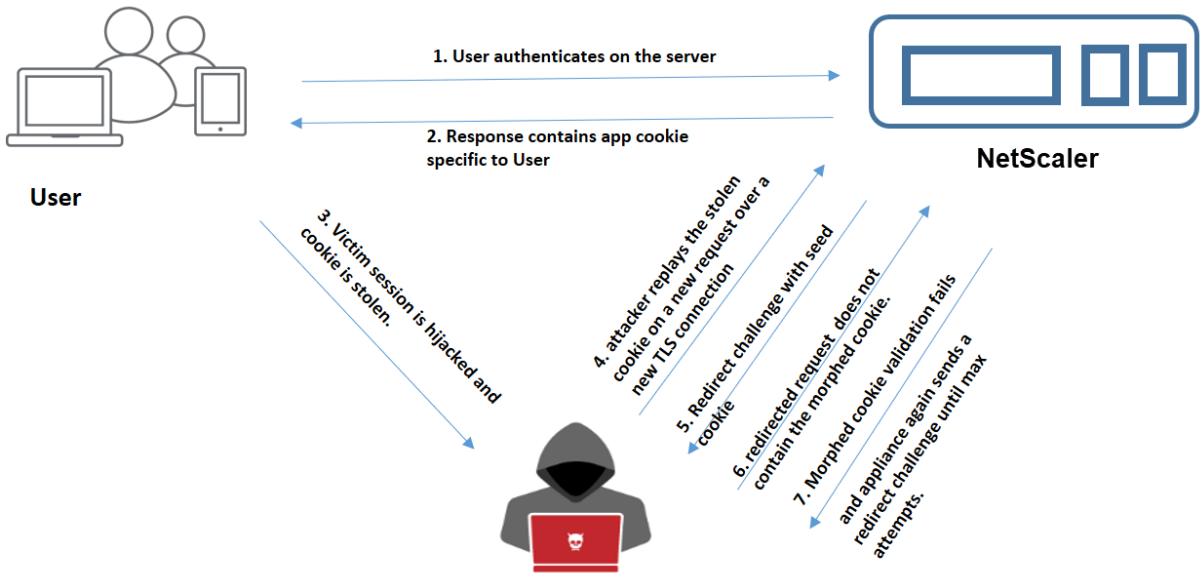
4. Wenn der Backend-Server eine Antwort sendet, empfängt die Appliance die Antwort und leitet sie mit einem JavaScript-Sitzungstoken und einem Seed-Cookie weiter. Die Appliance markiert dann die TLS-Verbindung als verifiziert.
5. Wenn der Client-Browser die Antwort empfängt, führt der Browser das JavaScript aus und generiert mithilfe des Sitzungstokens und des Seed-Cookies eine morphierte Cookie-ID.
6. Wenn ein Benutzer eine nachfolgende Anfrage über die TLS-Verbindung sendet, umgeht die Appliance die morphierte Cookie-Validierung. Dies liegt daran, dass die TLS-Verbindung bereits validiert wurde.

Szenario 2: Benutzer, der über eine neue TLS-Verbindung mit Sitzungscookie auf aufeinanderfolgende Webseiten zugreift



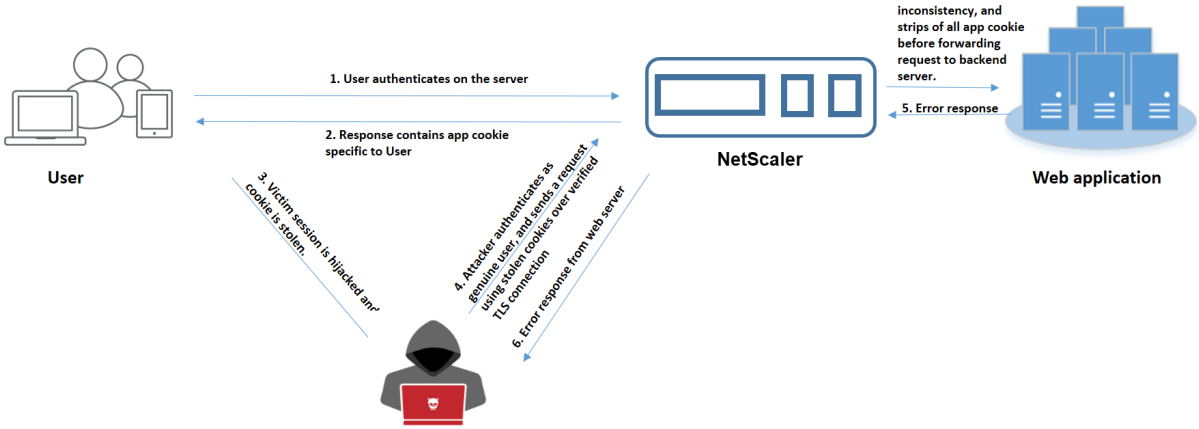
1. Wenn ein Benutzer eine HTTP-Anfrage für aufeinanderfolgende Seiten über eine neue TLS-Verbindung sendet, sendet der Browser die Sitzungs-Cookie-ID und die morphierte Cookie-ID.
2. Da es sich um eine neue TLS-Verbindung handelt, erkennt die Appliance die TLS-Verbindung und fordert den Client mit einer Umleitungsantwort mit einem Seed-Cookie.
3. Der Client berechnet nach Erhalt der Antwort vom ADC das morphierte Cookie anhand des Tokens der Sitzung und des neuen Seed-Cookies.
4. Der Client sendet dann dieses neu berechnete Morphed-Cookie zusammen mit einer Sitzungs-ID.
5. Wenn das innerhalb der ADC-Appliance berechnete Morphed-Cookie und das über die Anforderung gesendete Cookie übereinstimmen, wird die TLS-Verbindung als verifiziert markiert.
6. Wenn sich das berechnete Morphed-Cookie von dem in der Client-Anfrage vorhandenen unterscheidet, schlägt die Validierung fehl. Danach sendet die Appliance die Herausforderung zurück an den Client, um ein korrektes Morphed-Cookie zu senden.

Szenario 3: Angreifer gibt sich als nicht authentifizierter Benutzer aus



1. Wenn sich ein Benutzer bei der Webanwendung authentifiziert, verwendet der Angreifer verschiedene Techniken, um die Cookies zu stehlen und erneut abzuspielen.
2. Da es sich um eine neue TLS-Verbindung des Angreifers handelt, sendet der ADC eine Umleitungsaufforderung zusammen mit einem neuen Seed-Cookie.
3. Da auf dem Angreifer kein JavaScript ausgeführt wird, enthält die Antwort des Angreifers auf die umgeleitete Anfrage nicht das morphierte Cookie.
4. Dies führt zu einem Fehler bei der morphierten Cookie-Validierung auf der ADC-Appliance-Seite. Die Appliance sendet erneut eine Umleitungsaufforderung an den Client.
5. Wenn die Anzahl der Morphed-Cookie-Validierungsversuche den Schwellenwert überschreitet, kennzeichnet die Appliance den Status als Cookie-Hijacking.
6. Wenn der Angreifer versucht, Anwendungscookies und Sitzungscookies, die dem Opfer gestohlen wurden, zu mischen und zuzuordnen, schlägt die Cookie-Konsistenzprüfung fehl und die Appliance wendet die konfigurierte Cookie-Hijack-Aktion an.

Szenario 4: Angreifer gibt sich als authentifizierter Benutzer aus



1. Angreifer können auch versuchen, sich in einer Webanwendung als echter Benutzer zu authentifizieren und die Cookies des Opfers erneut abzuspielen, um Zugriff auf die Web-Sitzung zu erhalten.
2. Die ADC-Appliance erkennt auch solche Identitätsangreifer. Obwohl eine verifizierte TLS-Verbindung vom Angreifer verwendet wird, um das Cookie eines Opfers erneut abzuspielen, überprüft die ADC-Appliance dennoch, ob das Sitzungscookie und das Anwendungscookie in der Anforderung konsistent sind. Die Appliance überprüft die Konsistenz eines Anwendungscookies mithilfe des Sitzungscookies in der Anforderung. Da die Anfrage das Sitzungscookie eines Angreifers und das App-Cookie eines Opfers enthält, schlägt die Überprüfung der Cookie-Konsistenz fehl.
3. Infolgedessen wendet die Appliance die konfigurierte Cookie-Hijack-Aktion an. Wenn die konfigurierte Aktion als “Blockieren” festgelegt ist, entfernt die Appliance alle Anwendungscookies und sendet die Anforderung an den Backend-Server.

4. Der Backend-Server empfängt eine Anfrage ohne Anwendungscookie und reagiert daher auf eine Fehlerantwort an den Angreifer, z. B. “Benutzer nicht angemeldet”.

Cookie-Hijacking über die CLI konfigurieren

Sie können ein bestimmtes Anwendungs-Firewallprofil auswählen und eine oder mehrere Aktionen festlegen, die das Hijacking von Cookie verhindern.

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <name> [-cookieHijackingAction <action-name> <block | log
 | stats | none>]
```

> **Hinweis:**
>
> Standardmäßig ist die Aktion auf “none” gesetzt.

Beispiel:

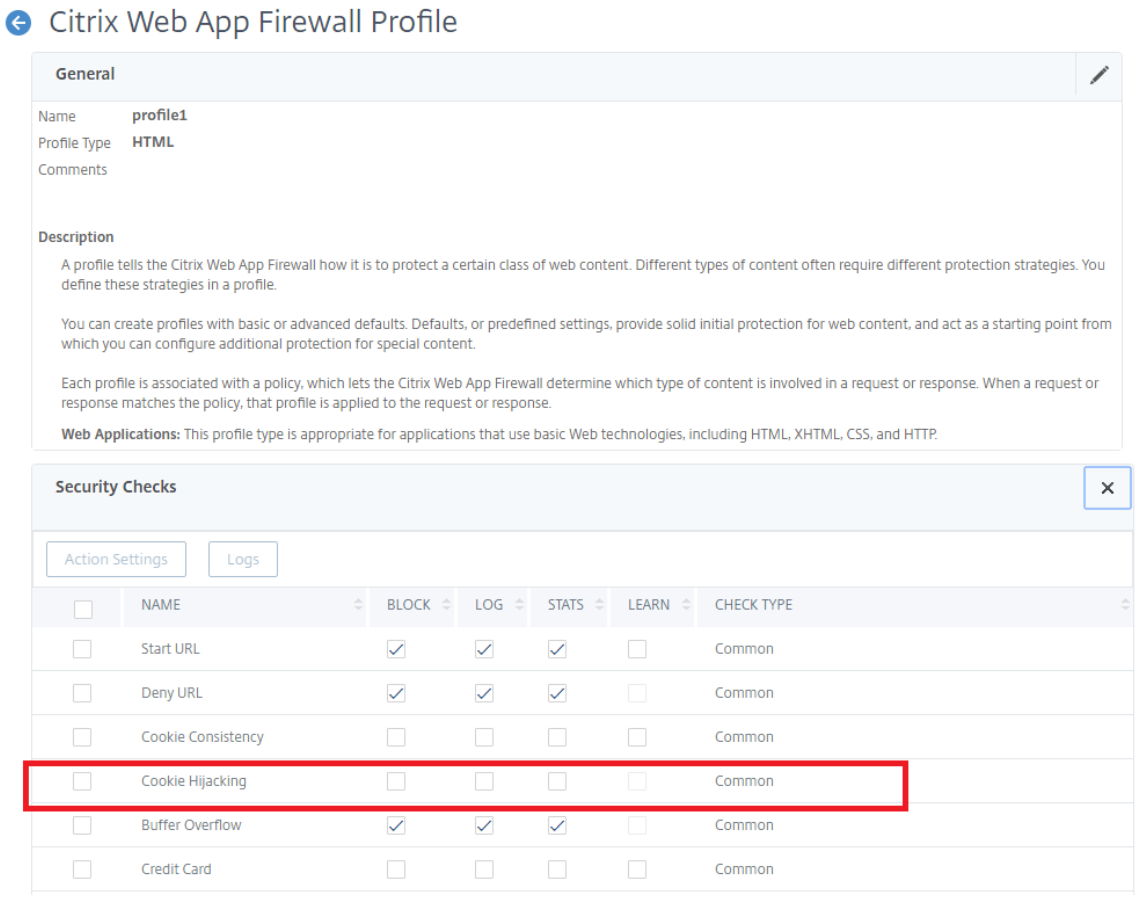
```
set appfw profile profile1 - cookieHijackingAction Block
```

Wo sind Aktionstypen:

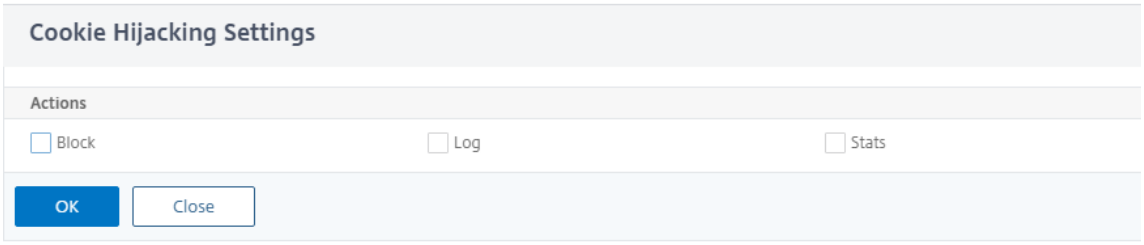
Blockieren: Blockiert Verbindungen, die gegen diese Sicherheitsüberprüfung verstoßen.
Protokoll: Verstöße gegen diese Sicherheitsüberprüfung protokollieren.
Statistiken: Generieren Sie Statistiken für diese Sicherheitsüberprüfung.
Keine: Deaktivieren Sie alle Aktionen für diese Sicherheitsüberprüfung.

Konfigurieren Sie die Cookie-Hijacking über die NetScaler GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der **NetScaler Web App Firewall Profilseite** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.



4. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** die Option **Cookie-Hijacking** aus und klicken Sie dann auf **Aktionseinstellungen** .
5. Wählen Sie auf der Seite **Cookie-Hijacking-Einstellungen** eine oder mehrere Aktionen aus, um das Hijacking von Cookies zu verhindern.
6. Klicken Sie auf **OK**.



Fügen Sie über die NetScaler GUI eine Relaxationsregel für die Überprüfung der Cookie-Konsistenz hinzu

Um Fehlalarme bei der Überprüfung der Cookie-Konsistenz zu behandeln, können Sie eine Relaxationsregel für Cookies hinzufügen, die von der Cookie-Validierung ausgenommen werden können.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **NetScaler Web App Firewall-Profil** zum Abschnitt **Erweiterte Einstellungen**, und klicken Sie auf **Relaxationsregeln**.
4. Wählen Sie im Abschnitt **Relaxationsregeln** die Option **Cookie-Konsistenz** aus und klicken Sie auf **Aktion**.
5. Legen Sie auf der Seite **Regel zur Entspannung der Cookie-Konsistenz** die folgenden Parameter fest.
   a) Aktiviert. Wählen Sie aus, ob Sie die Relaxationsregel aktivieren möchten.
   b) Ist Cookie-Name Regex. Wählen Sie aus, ob der Cookie-Name ein regulärer Ausdruck ist.
   c) Name des Cookies. Geben Sie den Namen des Cookie ein, das von der Cookie-Validierung ausgenommen werden kann.
   d) Regex-Editor. Klicken Sie auf diese Option, um die Details für reguläre Ausdrücke bereitzustellen.
   e) Kommentare. Eine kurze Beschreibung des Cookie.
6. Klicken Sie auf **Erstellen** und **Schließen**.

Statistiken zu Cookie-Hijacking-Datenverkehr und Verstößen in der CLI anzeigen

Zeigen Sie Details zu Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format an.

So zeigen Sie Sicherheitsstatistiken an:

Geben Sie in der Befehlszeile Folgendes ein:

```
stat appfw profile profile1
```

Appfw-Profil Verkehrsstatistiken	Geschwindigkeit (/s)	Gesamt
Anfragen	0	0
Byte anfragen	0	0
Antworten	0	0
Antwort Byte	0	0
Bricht ab	0	0
Leitet	0	0
Langfristige Reaktionszeit (ms)	–	0

Appfw-Profil Verkehrsstatistiken	Geschwindigkeit (/s)	Gesamt
Letzte Reaktionszeit von Ave (ms)	–	0

Statistik zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
Start-URL	0	0
URL verweigern	0	0
Referer-Header	0	0
Pufferüberlauf	0	0
Cookie-Konsistenz	0	0
Cookie-Entführung	0	0
CSRF-Formular-Tag	0	0
Site-übergreifendes HTML	0	0
HTML SQL injection	0	0
Feld-Format	0	0
Field consistency	0	0
Kreditkarte	0	0
Sicheres Objekt	0	0
Verstöße gegen die Signatur	0	0
Inhaltstyp	0	0
JSON-Denial-of-Service-Angriff	0	0
JSON-SQL-Einschleusung	0	0
JSON-Cross-Site Scripting	0	0
Dateiuploadtyp	0	0
Ableiten der XML-Nutzlast für Inhaltstypen	0	0
HTML-Befehlseinschleusung	0	0
XML-Format	0	0

Statistik zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
XML-Denial-of-Service-Angriff (XDoS)	0	0
XML-Nachrichtenüberprüfung	0	0
Interoperabilität der Webdienste	0	0
XML SQL Injection	0	0
Site-übergreifende XML-Skrip	0	0
XML-Anhang	0	0
SOAP-Fehlerverletzungen	0	0
Generische XML-Verstöße	0	0
Verstöße insgesamt	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
Starten der URL-Protokolle	0	0
URL-Protokolle verweigern	0	0
Referer-Header-Protokolle	0	0
Pufferüberlauf-Protokolle	0	0
Pufferüberlauf-Protokolle	0	0
Protokolle zur Cookie-Konsistenz	0	0
Protokolle zur Cookie-Entführung	0	0
CSRF-Formulartag-Protokolle	0	0
HTML-Cross-Site Scripting-Protokolle	0	0
HTML Cross-Site Scripting-Transformationsprotokolle	0	0
HTML SQL-Einschleusungsprotokolle	0	0

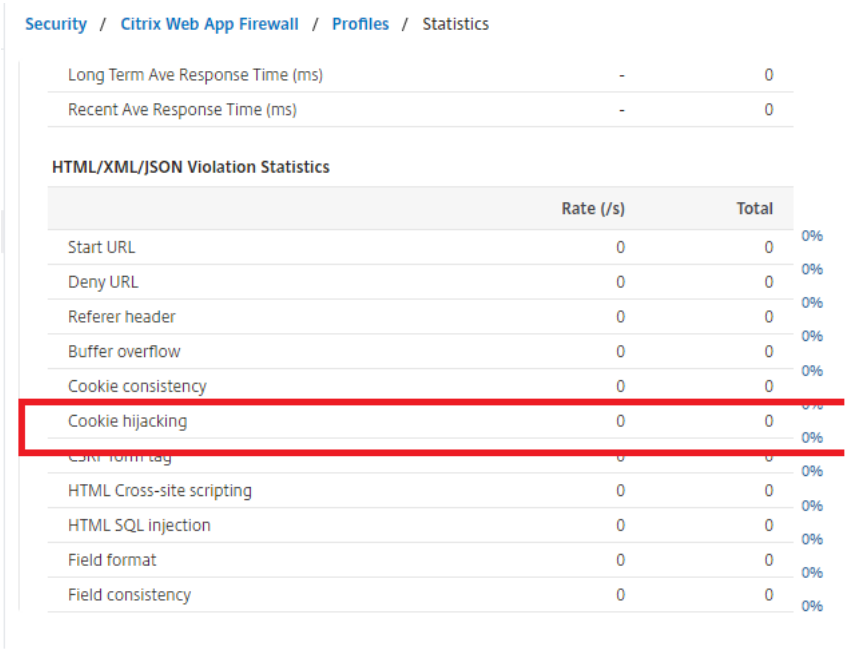
HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
HTML SQL Transformationsprotokolle	0	0
Protokolle im Feldformat	0	0
Protokolle zur Feldkonsistenz	0	0
Kreditkarten	0	0
Protokolle zur Kreditkarten-Transformation	0	0
Sichere Objektprotokolle	0	0
Signatur-Protokolle	0	0
Inhalts-Typ-Protokolle	0	0
JSON-Denial-of-Service-Protokolle	0	0
JSON SQL-Einschleusungsprotokolle	0	0
JSON-Site-Scripting-Protokolle	0	0
Protokolle zum Hochladen von Dateien	0	0
Ableiten der XML-Nutzlast des Inhaltstyps L	0	0
HTML-Befehlseinschleusungsprotokol	0	0
Protokolle im XML-Format	0	0
XML Denial of Service (XDoS) -Protokolle	0	0
Protokolle zur XML-Nachrichtenüberprüfung	0	0
WSI-Protokolle	0	0
XML SQL Injection-Protokolle	0	0
XML-Cross-Site Scripting-Protokolle	0	0
Protokolle für XML-Anhänge	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
SOAP-Fehlerlogs	0	0
Generische XML-Protokolle	0	0
Gesamtzahl der Protokollmeldungen	0	0

Statistiken zur Reaktion auf Serverfehler	Geschwindigkeit (/s)	Gesamt
HTTP-Client-Fehler (4xx Resp)	0	0
HTTP-Serverfehler (5xx)	0	0

Zeigen Sie über die GUI Statistiken zu Cookie-Hijacking-Datenverkehr und Verstößen an

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein **Web App Firewall-Profil** aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **Statistiken der NetScaler Web App Firewall** werden die Details des Cookie-Hijacking-Datenverkehrs und der Verstöße angezeigt
4. Sie können die **Tabellarische Ansicht** wählen oder zur **grafischen Ansicht** wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.



SameSite-Cookie-Attribut

May 11, 2023

Für eine sichere Webkommunikation hat Google die Verwendung des Cookie-Attributs `SameSite` vorgeschrieben. Durch die Einhaltung der neuen Richtlinie `SameSite` von Google Chrome kann die NetScaler-Appliance Drittanbieter-Cookies mit dem im Header `set-cookie` festgelegten Attribut `SameSite` verwalten. Die Cookie-Einstellung mindert Angriffe und bietet eine gesicherte Webkommunikation.

Bis Februar 2020 wurde das Attribut `SameSite` nicht explizit im Cookie festgelegt. Der Browser hat den Standardwert „Keine“ angenommen. Mit bestimmten Browser-Upgrades wie Google Chrome 80 ändert sich jedoch das standardmäßige domänenübergreifende Verhalten von Cookies.

Cookie-Attributwert festlegen

Das Attribut `SameSite` ist auf einen der folgenden Werte festgelegt, und für den Google Chrome-Browser ist der Standardwert auf “Lax” festgelegt.

Keine. Weist den Browser an, das Cookie für Anfragen im standortübergreifenden Kontext nur auf sicheren Verbindungen zu verwenden.

Lax. Weist den Browser an, das Cookie für Anfragen im Kontext derselben Website zu verwenden. Im Cross-Site-Kontext können nur sichere HTTP-Methoden wie GET-Request das Cookie verwenden.

Streng. Verwenden Sie das Cookie nur, wenn der Benutzer die Domain explizit anfordert.

> **Hinweis:**
>
> Wenn set-cookies (einschließlich Firewall-Sitzungscookies) über das `SameSite`-Attribut verfügen und das Attribut-Flag `addcookiesamesite` im Web Application Firewall-Profil aktiviert ist, wird das Attribut `SameSite` entsprechend dem im Profil konfigurierten Wert überschrieben.

Konfigurieren Sie das SameSite-Attribut im Web App Firewall-Profil mithilfe der CLI

Um das Attribut `SameSite` zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie das Cookie-Attribut `SameSite`.
2. Stellen Sie das Cookie-Attribut für die Appfw-Sitzungscookies ein.

Aktiviere das 'Samesite' Cookie-Attribut

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile-name> -insertCookieSameSiteAttribute ( ON | OFF)
```

Beispiel:

```
set appfw profile p1 -insertCookieSameSiteAttribute ON
```

Legen Sie denselben Site-Cookie-Attributwert für Web Application Firewall-Sitzungscookies fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile-name> - cookieSameSiteAttribute ( LAX | NONE |
STRICT )
```

Beispiel:

```
set appfw profile p1 - cookieSameSiteAttribute LAX
```

Wo es Attributtypen gibt,

Keine. Das Cookie-Attribut SameSite ist auf „None“ gesetzt und für alle WAF- und Anwendungscookies als sicher markiert.

Lax. Das Cookie-Attribut SameSite ist für alle WAF- und Anwendungscookies auf „Lax“ gesetzt.

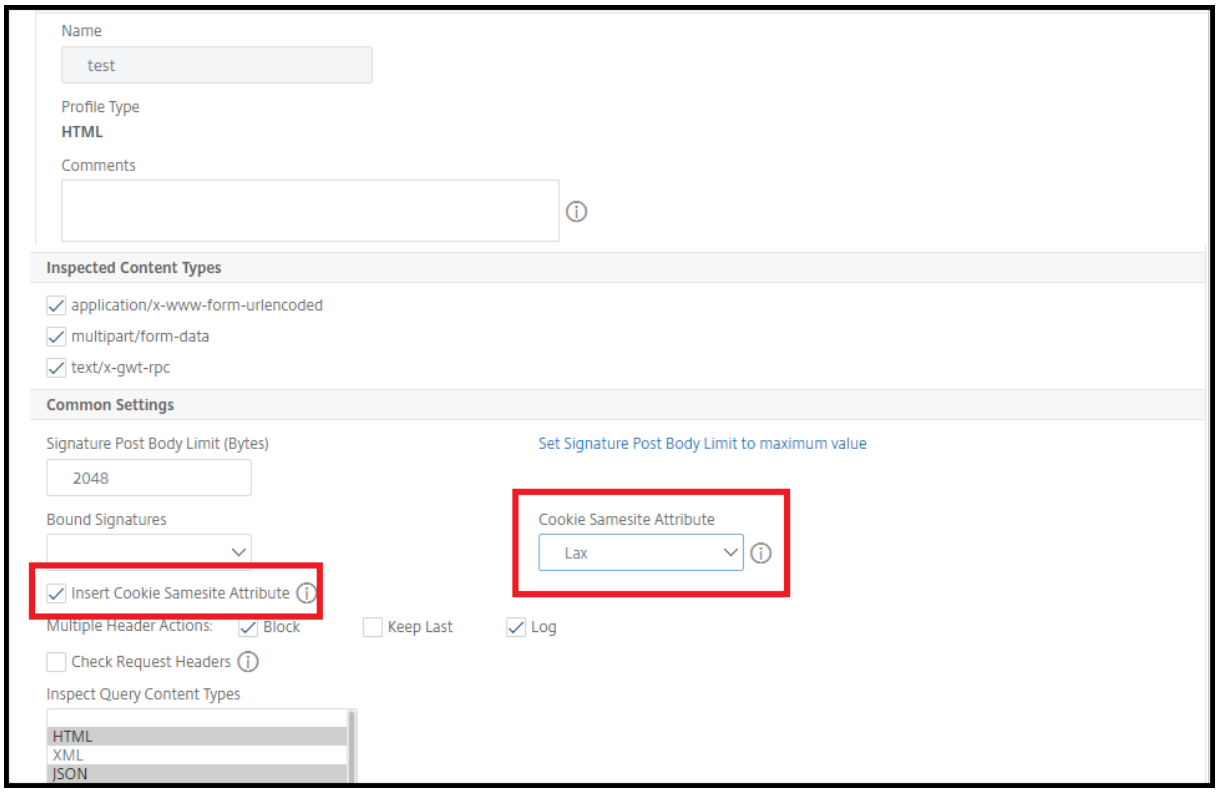
Streng. Das Cookie-Attribut SameSite ist für alle WAF- und Anwendungscookies auf „Lax“ gesetzt.

Konfigurieren Sie das SameSite-Cookie-Attribut im Web App Firewall-Profil mithilfe der GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der **NetScaler Web App Firewall Profilseite** unter **Erweiterte**Einstellungen auf Profileinstellungen**.
4. Stellen Sie im Abschnitt **Profileinstellungen** die folgenden Parameter ein:

   a. Fügen Sie das Cookie-Attribut `Samesite` ein. Markieren Sie das Kontrollkästchen, um das Cookie-Attribut `Samesite` zu aktivieren.
   b. Cookie Samesite Attribute. Wählen Sie eine Option aus der Dropdownliste aus, um den `Samesite` Cookie-Wert festzulegen.

5. Klicken Sie auf **OK** und **Fertig**.



Überprüfungen zur Vermeidung von Datenlecks

January 19, 2021

Die Datenleak-Prevention prüft Filterantworten, um ein Versenden vertraulicher Informationen wie Kreditkartennummern und Sozialversicherungsnummern an nicht autorisierte Empfänger zu verhindern.

Kreditkartencheck

May 11, 2023

Wenn Sie über eine Anwendung verfügen, die Kreditkarten akzeptiert, oder wenn Ihre Websites Zugriff auf Datenbankserver haben, auf denen Kreditkartennummern gespeichert sind, müssen Sie DLP-Maßnahmen (Data Leak Prevention) verwenden und den Schutz für jeden von Ihnen akzeptierten Kreditkartentyp konfigurieren.

Der NetScaler Web App Firewall Credit Card Check verhindert, dass Angreifer Sicherheitslücken zur Verhinderung von Datenlecks ausnutzen, um an die Kreditkartennummern Ihrer Kunden zu gelangen. Mit einfachen Konfigurationsschritten können Sie den Schutz einer oder mehrerer der folgenden Kreditkarten durchsetzen: 1) Visa, 2) Master Card, 3) Discover, 4) American Express (Amex), 5) JCB und 6) Diners Club.

Die Kreditkartensicherheitsprüfung untersucht die Serverantworten, um Instanzen der Ziel-Kreditkartennummern zu identifizieren, und führt eine bestimmte Aktion durch, wenn eine solche Nummer gefunden wird. Die Aktion kann darin bestehen, die Antwort zu transformieren, indem alle bis auf die letzte Zifferngruppe in der Kreditkartennummer ausgeblendet werden, oder die Antwort blockiert wird, wenn sie mehr als eine bestimmte Anzahl von Kreditkartennummern enthält. Wenn Sie beide angeben, hat die Blockaktion Vorrang. Die Einstellung Maximal zulässige Kreditkarten pro Seite bestimmt, wann die Sperraktion aufgerufen wird. Die Standardeinstellung 0 (auf der Seite sind keine Kreditkartennummern zulässig) ist am sichersten, Sie können jedoch bis zu 255 zulassen. Je nachdem, wo der Verstoß in der Antwort erkannt wird und die Blockieraktion ausgelöst wird, erhalten Sie in der Antwort möglicherweise weniger als die maximal zulässige Anzahl von Kreditkarten.

Um Fehlalarme zu vermeiden, können Sie Lockerungen anwenden, um bestimmte Nummern von der Kreditkartenprüfung auszunehmen. Eine Sozialversicherungsnummer, eine Bestellnummer oder eine Google-Kontonummer können beispielsweise einer Kreditkartennummer ähneln. Sie können einzelne Zahlen angeben oder einen regulären Ausdruck verwenden, um die Ziffernfolge anzugeben, die bei der Verarbeitung der Antwort-URL für die Kreditkartenprüfung umgangen werden soll.

Wenn Sie sich nicht sicher sind, welche Kreditkartennummern ausgenommen werden sollen, können Sie die Lernfunktion verwenden, um Empfehlungen auf der Grundlage der erlernten Daten zu generieren. Um einen optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie diese Option für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Lockerungen anwenden und das Lernen deaktivieren.

Wenn Sie die Protokollfunktion aktivieren, generiert die Kreditkartenprüfung Protokollmeldungen, in denen die durchgeführten Aktionen angegeben sind. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl von Protokollmeldungen kann auf vereitelte Zugriffsversuche hindeuten. Standardmäßig ist der Parameter doSecureCreditCardLogging auf ON gesetzt, sodass die Kreditkartennummer nicht in der Protokollnachricht enthalten ist, die durch den Safe-Commerce-Verstoß (Kreditkarte) generiert wurde.

Die Statistikfunktion sammelt Statistiken über Verstöße und Protokolle. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird.

Um die Kreditkarten-Sicherheitsprüfung zum Schutz Ihrer Anwendung zu konfigurieren, konfigurieren Sie das Profil, das die Überprüfung des Datenverkehrs zu und von dieser Anwendung regelt.

> **Hinweis**:
>
> Eine Website, die nicht auf eine SQL-Datenbank zugreift, hat normalerweise keinen Zugriff auf vertrauliche private Informationen wie Kreditkartennummern.

Verwenden der Befehlszeile zur Konfiguration des Kreditkartenschecks

In der Befehlszeilenschnittstelle können Sie entweder den Befehl set appfw profile oder den Befehl add appfw profile verwenden, um die Kreditkartenüberprüfung zu aktivieren und anzugeben, welche Aktionen ausgeführt werden sollen. Sie können den Befehl unset appfw profile verwenden, um zu den Standardeinstellungen zurückzukehren. Um Lockerungen anzugeben, verwenden Sie den Befehl bind appfw, um Kreditkartennummern an das Profil zu binden.

So konfigurieren Sie eine Kreditkartenprüfung mithilfe der Befehlszeile

Verwenden Sie entweder den Befehl set appfw profile oder den Befehl add appfw profile wie folgt:

- `set appfw profile <name> -creditCardAction ( ([block][learn] [log][ stats])| [none])`
- `set appfw profile <name> -creditCard (VISA | MASTERCARD | DISCOVER | AMEX | JCB | DINERSCLUB)`
- `set appfw profile <name> -creditCardMaxAllowed <integer>`
- `set appfw profile <name> -creditCardXOut ([ON] | [OFF])<name> -doSecureCreditCard ([ON] | [OFF])`
- So konfigurieren Sie eine Regel zur Kreditkartenentlastung mithilfe der Befehlszeile

  Verwenden Sie den Befehl bind, um die Kreditkartennummer an das Profil zu binden. Um eine Kreditkartennummer aus einem Profil zu entfernen, verwenden Sie den Befehl unbind mit denselben Argumenten, die Sie für den Befehl bind verwendet haben. Sie können den Befehl show verwenden, um die an ein Profil gebundenen Kreditkartennummern anzuzeigen.

- Um eine Kreditkartennummer an ein Profil zu binden

  ```
  bind appfw profile <profile-name> -creditCardNumber <any number/regex>
  “<url>”
  ```

  Beispiel: Appfw-Profil binden test_profile -CredCardNumber 378282246310005 `http://www.example.com/credit\\_card\\_test.html`

  - So heben Sie die Bindung einer Kreditkartennummer an ein Profil auf

    ```
    unbind appfw profile <profile-name> -creditCardNumber <credit card
    number / regex> <url>
    ```

  - Um die Liste der an ein Profil gebundenen Kreditkartennummern anzuzeigen.

    ```
    show appfw profile <profile>
    ```

Verwendung der GUI zur Konfiguration der Kreditkartenprüfung

In der GUI konfigurieren Sie die Kreditkartensicherheitsprüfung im Bereich für das Ihrer Anwendung zugeordnete Profil.

Um die Kreditkarten-Sicherheitsprüfung mithilfe der GUI hinzuzufügen oder zu ändern

1. Navigieren Sie zu **Web App Firewall** > **Profile, markieren** Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

   In der Tabelle zur Sicherheitsüberprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsüberprüfungen angezeigt. Sie haben 2 Möglichkeiten für die Konfiguration:

   a) Wenn Sie nur die Aktionen Sperren, Protokollieren, Statistiken und Lernen für Kreditkarten aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf **OK**klicken und dann auf **Speichern** und **Schließen** klicken, um den Bereich **Sicherheitsüberprüfung** zu schließen.

   b) Wenn Sie zusätzliche Optionen für diese Sicherheitsüberprüfung konfigurieren möchten, doppelklicken Sie auf Kreditkarte, oder wählen Sie die Zeile aus und klicken Sie auf **Aktionseinstellungen**, um weitere Optionen wie folgt anzuzeigen:

      - Ausblenden — Maskieren Sie jede Kreditkartennummer, die in einer Antwort erkannt wurde, indem Sie jede Ziffer, mit Ausnahme der Ziffern in der letzten Gruppe, durch den Buchstaben „X“ ersetzen.
      - Maximal zulässige Kreditkartenanzahl pro Seite — Geben Sie die Anzahl der Kreditkarten an, die an den Client weitergeleitet werden können, ohne eine Sperraktion auszulösen.

- Geschützte Kreditkarten. Aktivieren oder deaktivieren Sie ein Kontrollkästchen, um den Schutz für jeden Kreditkartentyp zu aktivieren oder zu deaktivieren.
- Sie können die Aktionen Sperren, Protokollieren, Statistiken und Lernen auch im Bereich Kreditkarteneinstellungen bearbeiten.
  Nachdem Sie eine der oben genannten Änderungen vorgenommen haben, klicken Sie auf OK, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf OK, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf Speichern und Schließen, um den Bereich Sicherheitsüberprüfung zu schließen.

3. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Profileinstellungen**. Um die sichere Protokollierung von Kreditkartennummern zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie das Kontrollkästchen **Sichere Kreditkartenprotokollierung** . (In der Standardeinstellung ist es ausgewählt).

   Klicken Sie auf **OK**, um die Änderungen zu speichern.

- So konfigurieren Sie mithilfe der GUI eine Regel zur Kreditkartenentlastung

  1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
  2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**. Die Tabelle mit den Relaxationsregeln enthält einen Kreditkarteneintrag. Sie können auf diese Zeile doppelklicken oder diese Zeile auswählen und auf **Bearbeiten** klicken, um das Dialogfeld „ **Regeln zur Kreditkartenlockerung** “ aufzurufen. Sie können die Operationen Hinzufügen, Bearbeiten, Löschen, Aktivierenoder Deaktivieren für Relaxationsregeln ausführen.

Nutzung der Lernfunktion beim Kreditkartencheck

Wenn die Lernaktion aktiviert ist, überwacht die Web App Firewall Learning Engine den Datenverkehr und lernt die ausgelösten Verstöße. Sie können diese gelernten Regeln regelmäßig überprüfen. Wenn Sie nach reiflicher Überlegung eine bestimmte Ziffernfolge von der Kreditkarten-Sicherheitsprüfung ausnehmen möchten, können Sie die erlernte Regel als Lockerungsregel anwenden.

- So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

  ```
  show appfw learningdata <profilename> creditCardNumber
  ```

  ```
  rm appfw learningdata <profilename> -creditcardNumber <credit card
  number> "<url>"
  ```

  ```
  export appfw learningdata <profilename> creditCardNumber
  ```

- So zeigen Sie erlernte Daten mit der GUI an oder verwenden sie

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **“Erweiterte Einstellungen** “ auf **Gelernte Regeln**. Sie können den Eintrag Kreditkarte in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die gelernten Regeln zuzugreifen. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Entspannungsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

Sie haben auch die Möglichkeit, eine zusammengefasste Ansicht der erlernten Lockerungen anzuzeigen, indem Sie in der Tabelle Gelernte Regeln den Eintrag Kreditkarte auswählen und auf Visualizer klicken, um eine konsolidierte Ansicht aller erlernten Verstöße zu erhalten. Der Visualizer macht es sehr einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Ergreifen einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke empfohlen werden, um mehrere Regeln zu konsolidieren. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Zahl aus einer Dropdown-Liste auswählen. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Entspannungen einzusetzen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Nutzung der Log-Funktion bei der Kreditkartenprüfung

Wenn die Protokollaktion aktiviert ist, werden die Verstöße gegen die Kreditkartensicherheitsprüfung im Audit-Log als APPFW_SAFECOMMERCE- oder APPFW_SAFECOMMERCE_XFORM-Verstöße protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

Die Standardeinstellung für doSecureCreditCardLogging ist ON. Wenn Sie es auf OFF ändern, sind sowohl die Kreditkartennummer als auch der Typ in der Protokollmeldung enthalten.

Abhängig von den für die Kreditkartenprüfungen konfigurierten Einstellungen können die von der Anwendungs-Firewall generierten Protokollmeldungen die folgenden Informationen enthalten:

- Die Antwort wurde blockiert oder nicht blockiert.
- Kreditkartennummern wurden transformiert (mit X ausgeblendet). Für jede transformierte Kreditkartennummer wird eine separate Protokollnachricht generiert, sodass bei der Verarbeitung einer einzigen Antwort mehrere Protokollmeldungen generiert werden können.
- Die Antwort enthielt die maximale Anzahl potenzieller Kreditkartennummern.
- Kreditkartennummern und ihre entsprechenden Typen.

- So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

  Wechseln Sie zur Shell und verfolgen Sie die ns.logs im Ordner /var/log/, um auf die Protokollnachrichten zuzugreifen, die sich auf die Kreditkartenverstöße beziehen:

  - Shell
  - schwanz -f /var/log/ns.log | grep SAFECOMMERCE

- So greifen Sie mit der GUI auf die Protokollmeldungen zu

  1. Die GUI enthält ein sehr nützliches Tool (Syslog Viewer) zur Analyse der Logmeldungen. Sie haben mehrere Optionen, um auf den Syslog-Viewer zuzugreifen: Navigieren Sie zum **Zielprofil** > **Sicherheitsprüfungen**. Markieren Sie die Zeile Kreditkarte und klicken Sie auf Protokolle. Wenn Sie direkt von der Kreditkarten-Sicherheitsüberprüfung des Profils aus auf die Protokolle zugreifen, werden die Protokollmeldungen herausgefiltert und nur die Protokolle angezeigt, die sich auf diese Verstöße gegen die Sicherheitsüberprüfung beziehen.

  2. Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Prüfmeldungen auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen ausgelöst werden können.

     Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um auf Protokollmeldungen über Verstöße gegen die Kreditkartensicherheitsüberprüfung zuzugreifen, filtern Sie, indem Sie in den Dropdownoptionen für Modul APPFW auswählen. Der Event-Typ zeigt eine Vielzahl von Optionen an, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise die Kontrollkästchen APPFW_SAFECOMMERCE und APPFW_SAFECOMMERCE_XFORM aktivieren und auf die Schaltfläche Anwenden klicken, werden im Syslog Viewer nur Protokollmeldungen angezeigt, die sich auf Verstöße gegen die Kreditkartensicherheitsprüfung beziehen.

     Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollmeldung setzen, werden mehrere Optionen, wie Module und EventType, unter der Protokollmeldung angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in den Protokollen hervorzuheben.

Beispiel für eine Protokollnachricht im systemeigenen Format, wenn die Antwort nicht blockiert wird

```
1 May 29 01:26:31 <local0.info> 10.217.31.98 05/29/2015:01:26:31 GMT ns
     0-PPE-0 :
2 default APPFW APPFW_SAFECOMMERCE 2181 0 :  10.217.253.62 1098-PPE0
```



```
4erNfkaHy0IeGP+nv2S9Rsdu77I0000 pr_ffc http://aaron.stratum8.net/FFC/
    CreditCardMind.html
Maximum number of potential credit card numbers seen <not blocked>
<!--NeedCopy-->
```

Beispiel für eine Protokollnachricht im CEF-Format, wenn die Antwort transformiert wird

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE_XFORM|6|src
    =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
    CreditCardMind.html
msg=Transformed (xout) potential credit card numbers seen in server
    response
cn1=66 cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002
cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Beispiel für eine Protokollmeldung im CEF-Format, wenn die Antwort blockiert wird. Die Kreditkartennummer und der Typ der Kreditkarte können im Protokoll eingesehen werden, da der Parameter doSecureCreditCardLogging deaktiviert ist.

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE|6|src
    =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
    CreditCardMind.html
msg=Credit Card number 4505050504030302 of type Visa is seen in
    response cn1=68
cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002 cs4=
    ALERT cs5=2015
act=blocked
<!--NeedCopy-->
```

Statistiken zu den Kreditkartenverstößen

Wenn die Statistikaktion aktiviert ist, wird der entsprechende Zähler für die Kreditkartenüberprüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Erhöhung des Protokollzählers kann je nach den konfigurierten Einstellungen variieren. Wenn beispielsweise die Aktion „Sperren“ aktiviert ist und die Einstellung „Maximal zulässige Kreditkarte“ 0 ist, erhöht die Anforderung für eine Seite, die 20 Kreditkartennummern enthält, den Statistikzähler um eins,

wenn die Seite gesperrt wird, sobald die erste Kreditkartennummer erkannt wird. Wenn der Block jedoch deaktiviert und die Transformation aktiviert ist, erhöht die Verarbeitung derselben Anfrage den Statistikzähler für Protokolle um 20, da jede Kreditkartentransformation eine separate Protokollmeldung generiert.

- So zeigen Sie Kreditkartenstatistiken mithilfe der Befehlszeile an

  Geben Sie in der Befehlszeile Folgendes ein:

  ```
  sh appfw stats
  ```

  Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

  ```
  stat appfw profile <profile name>
  ```

  Um Kreditkartenstatistiken mithilfe der GUI anzuzeigen

  1. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall**.
  2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
  3. Verwenden Sie die Scrollleiste, um die Statistiken zu Kreditkartenverstößen und -protokollen einzusehen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

Beachten Sie die folgenden Punkte zur Kreditkarten-Sicherheitsprüfung:

- Die Web App Firewall ermöglicht es Ihnen, Kreditkarteninformationen zu schützen und alle Versuche zu erkennen, auf diese vertraulichen Daten zuzugreifen.
- Um den Kreditkartenschutzcheck nutzen zu können, müssen Sie mindestens einen Kreditkartentyp und eine Aktion angeben. Die Prüfung wird dann auf HTML-, XML- und Web 2.0-Profile angewendet.
- Sie können die Ausgabe des Befehls sh appfw profile und grep for creditCard über die Pipeline leiten, um die gesamte kreditkartenspezifische Konfiguration zu sehen. Beispielsweise zeigt sh appfw profile my_profile | grep CreditCard die konfigurierten Einstellungen verschiedener Parameter sowie die Lockerungsregeln für die Kreditkartenüberprüfung für das Web App Firewall-Profil mit dem Namen my_profile an.
- Sie können bestimmte Nummern von der Kreditkarteninspektion ausschließen, ohne die Sicherheitskontrolle für die übrigen Kreditkartennummern zu umgehen.
- Entspannung ist für alle durch die Web App Firewall geschützten Kreditkartenmuster verfügbar. In der GUI können Sie den Visualizer verwenden, um die Operationen Hinzufügen, Bearbeiten, Löschen, Aktivieren oder Deaktivieren für Relaxationsregeln festzulegen.
- Die Web App Firewall Learning Engine kann den ausgehenden Datenverkehr überwachen und auf der Grundlage beobachteter Verstöße Regeln empfehlen. Visualizer-Unterstützung ist auch

für die Verwaltung der erlernten Kreditkartenregeln in der GUI verfügbar. Sie können die erlernten Regeln bearbeiten und anwenden oder sie nach sorgfältiger Prüfung überspringen.

- Die Einstellung für die Anzahl der zulässigen Kreditkarten gilt für jede Antwort. Sie bezieht sich nicht auf die kumulierte Summe der Kreditkartennummern, die während der gesamten Benutzersitzung beobachtet wurden.
- Die Anzahl der ausstehenden Ziffern hängt von der Länge der Kreditkartennummern ab. Zehn Ziffern sind bei Kreditkarten mit 13 bis 15 Ziffern durch ein X gekennzeichnet. Zwölf Ziffern sind bei Kreditkarten mit 16 Ziffern mit einem X gekennzeichnet. Wenn Ihre Anwendung nicht das Senden der gesamten Kreditkartennummer als Antwort erfordert, empfiehlt Citrix, dass Sie diese Aktion aktivieren, um die Ziffern in den Kreditkartennummern zu maskieren.
- Die X-out-Operation transformiert alle Kreditkarten und funktioniert unabhängig von den konfigurierten Einstellungen für die maximale Anzahl zulässiger Kreditkarten. Wenn die Antwort beispielsweise 4 Kreditkarten enthält und der Parameter creditCardMaxAllowed auf 10 gesetzt ist, sind alle 4 Kreditkarten zwar ausgeschlossen, aber nicht gesperrt. Wenn die Kreditkartennummern im Dokument verteilt sind, kann es sein, dass eine Teilantwort mit X'd-Out-Nummern an den Kunden gesendet wird, bevor die Antwort blockiert wird.
- Deaktivieren Sie den Parameter doSecureCreditCardLogging nicht, bevor Sie dies sorgfältig geprüft haben. Wenn dieser Parameter deaktiviert ist, werden die Kreditkartennummern angezeigt und sind in den Protokollmeldungen abrufbar. Diese Zahlen werden in den Protokollen nicht maskiert, auch wenn die X-out-Aktion aktiviert ist. Wenn Sie Protokolle an einen Remote-Syslog-Server senden und die Protokolle kompromittiert sind, können die Kreditkartennummern offengelegt werden.
- Wenn die Antwortseite wegen einer Kreditkartenverletzung blockiert ist, leitet die Web App Firewall nicht zur Fehlerseite um.

Sichere Objektprüfung

May 11, 2023

Die Safe-Object-Prüfung bietet vom Benutzer konfigurierbaren Schutz für vertrauliche Geschäftsinformationen wie Kundennummern, Bestellnummern und länder- oder regionsspezifische Telefonnummern oder Postleitzahlen. Ein benutzerdefinierter regulärer Ausdruck oder ein benutzerdefiniertes Plug-In teilt der Web App Firewall das Format dieser Informationen mit und definiert die Regeln, die zu deren Schutz verwendet werden sollen. Wenn eine Zeichenfolge in einer Benutzeranforderung mit einer sicheren Objektdefinition übereinstimmt, blockiert die Web App Firewall entweder die Antwort, maskiert die geschützten Informationen oder entfernt die geschützten Informationen aus der Antwort, bevor sie an den Benutzer gesendet werden, je nachdem, wie Sie diese bestimmte Regel für sichere Objekte konfiguriert haben.

Der Safe Object Check verhindert, dass Angreifer eine Sicherheitslücke in Ihrer Webserver-Software oder auf Ihrer Website ausnutzen, um an sensible private Informationen wie Firmenkreditkartennummern oder Sozialversicherungsnummern zu gelangen. Wenn Ihre Websites keinen Zugriff auf diese Art von Informationen haben, müssen Sie diese Prüfung nicht konfigurieren. Wenn Sie über einen Einkaufswagen oder eine andere Anwendung verfügen, die auf diese Informationen zugreifen kann, oder Ihre Websites Zugriff auf Datenbankserver haben, die solche Informationen enthalten, müssen Sie den Schutz für jede Art von sensiblen privaten Informationen konfigurieren, die Sie verarbeiten und speichern.

> **Hinweis:**
>
> Eine Website, die nicht auf eine SQL-Datenbank zugreift, hat normalerweise keinen Zugriff auf vertrauliche private Informationen.

Die sichere Objektprüfung unterscheidet sich von der bei jeder anderen Prüfung. Jeder sichere Objektausdruck, den Sie erstellen, entspricht einer separaten Sicherheitsüberprüfung, ähnlich der Kreditkartenprüfung, für diese Art von Informationen.

Konfigurieren Sie die sichere Objektprüfung mit der GUI

> **Hinweis:**
>
> Sie müssen die sichere Objektprüfung nur mit der GUI konfigurieren. Die Befehlszeilenschnittstelle wird nicht unterstützt.

So fügen Sie eine Sicherheitsüberprüfung für sichere Objekte über die GUI hinzu:

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie das gewünschte Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
4. Wählen Sie **Sicheres Objekt** und klicken Sie auf **Bearbeiten**
5. Klicken Sie auf **Hinzufügen** und konfigurieren Sie Folgendes:
    - **Sicherer Objektname.** Ein Name für Ihr neues sicheres Objekt. Der Name kann mit einem Buchstaben, einer Zahl oder einem Unterstrich beginnen. Der Name kann aus einem bis 255 Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), At-Zeichen (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstrich (_) bestehen.
    - **Aktionen.** Aktivieren oder deaktivieren Sie die Aktionen **Blockieren**, **Protokollieren**und **Statistiken** sowie die folgenden Aktionen:
        - **X-Out.** Maskieren Sie alle Informationen, die dem sicheren Objektausdruck entsprechen, mit dem Buchstaben “X”.

  - **Remove.** Entfernen Sie alle Informationen, die dem sicheren Objektausdruck entsprechen.

- **Regulärer Ausdruck.** Geben Sie einen PCRE-kompatiblen regulären Ausdruck ein, der das sichere Objekt definiert. Sie können den regulären Ausdruck auf eine der folgenden Arten erstellen:
  - Geben Sie den regulären Ausdruck direkt in das Textfeld ein
  - Mithilfe des Menüs **Regex-Tokens** können Sie reguläre Ausdruckselemente und Symbole direkt in das Textfeld eingeben
  - Öffnen Sie den Editor für reguläre Ausdrücke und verwenden Sie ihn zum Erstellen des Ausdrucks. Der reguläre Ausdruck darf nur aus ASCII-Zeichen bestehen. Schneiden Sie keine Zeichen aus, die nicht Teil des grundlegenden ASCII-Sets mit 128 Zeichen sind, und fügen Sie sie nicht ein. Wenn Sie Nicht-ASCII-Zeichen einschließen möchten, müssen Sie diese Zeichen manuell im hexadezimalen PCRE-Zeichencodierungsformat eingeben.

    > **Hinweis:**
    >
    > Verwenden Sie keine Startanker (^) am Anfang von Safe-Object-Ausdrücken oder Endanker ($) am Ende von Safe-Object-Ausdrücken. Diese PCRE-Entitäten werden in Safe-Object-Ausdrücken nicht unterstützt und führen bei Verwendung dazu, dass Ihr Ausdruck nicht mit dem übereinstimmt, was er eigentlich erreichen sollte.

- **Maximale Spieldauer.** Geben Sie eine positive Ganzzahl ein, die die maximale Länge der Zeichenfolge darstellt, die Sie abgleichen möchten. Wenn Sie beispielsweise die US-Sozialversicherungsnummern abgleichen möchten, geben Sie die Nummer 11 in dieses Feld ein. Dadurch kann Ihr regulärer Ausdruck einer Zeichenfolge mit neun Ziffern und zwei Bindestrichen entsprechen. Wenn Sie die kalifornischen Führerscheinnummern abgleichen möchten, geben Sie die Nummer acht (8) ein.

  > **Achtung:**
  >
  > Wenn Sie keine maximale Übereinstimmungslänge festlegen, verwendet die Web App Firewall beim Filtern nach Zeichenfolgen, die Ihren sicheren Objektausdrücken entsprechen, den Standardwert eins (1). Infolgedessen stimmen die meisten sicheren Objektausdrücke nicht mit ihren Zielzeichenfolgen überein.

Sie können einen vorhandenen Ausdruck ändern, indem Sie den gewünschten Ausdruck auswählen, auf **Öffnen** klicken und dann den Ausdruck im Dialogfeld **Sicheres Objekt ändern** konfigurieren.

Im Folgenden finden Sie Beispiele für reguläre Ausdrücke zur Überprüfung sicherer Objekte:

- Suchen Sie nach Zeichenfolgen, bei denen es sich anscheinend um US-amerikanische Sozialversicherungsnummern (SSN) handelt. Die SSN besteht aus den folgenden Zeichen in der angegebenen Reihenfolge:

  - Drei Ziffern (von denen die erste nicht Null sein darf)
  - Ein Bindestrich
  - Zwei weitere Ziffern
  - Ein zweiter Bindestrich
  - Eine Reihe von vier weiteren Ziffern

```
[1-9][0-9]{
3,3 }
-[0-9]{
2,2 }
-[0-9]{
4,4 }

<!--NeedCopy-->
```

- Suchen Sie nach Zeichenfolgen, bei denen es sich anscheinend um kalifornische Führerscheinausweise handelt, die mit einem Buchstaben beginnen und auf die eine Zeichenfolge aus genau sieben Ziffern folgt:

```
[A-Za-z][0-9]{
7,7 }

<!--NeedCopy-->
```

- Suchen Sie nach Zeichenfolgen, die als Kunden-IDs erscheinen. Die Kunden-IDs bestehen in der angegebenen Reihenfolge aus folgenden Bestandteilen:
  - Eine Zeichenfolge aus fünf hexadezimalen Zeichen (alle Ziffern und die Buchstaben A bis F)
  - Ein Bindestrich
  - Ein Drei-Buchstaben-Code
  - Ein zweiter Bindestrich
  - Eine Zeichenfolge aus 10 Ziffern

```
[0-9A-Fa-f]{
5,5 }
-[A-Za-z]{
3,3 }
-[0-9]{
10,10 }

<!--NeedCopy-->
```


> **Achtung:**
>
> Reguläre Ausdrücke sind leistungsstark. Wenn Sie mit regulären Ausdrücken im PCRE-Format weniger vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass der reguläre Ausdruck genau den Typ der Zeichenfolge definiert, den Sie als sichere Objektdefinition hinzufügen möchten. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen/Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht wollten oder erwarten, z. B. zum Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten.

Erweiterte Formularschutzprüfungen

December 3, 2021

Die erweiterten Formularschutzprüfungen untersuchen Webformulardaten, um zu verhindern, dass Angreifer Ihr System gefährden, indem sie die Webformulare auf Ihren Websites ändern oder unerwartete Arten und Mengen von Daten in einem Formular an Ihre Website senden.

> **Hinweis:**
>
> SQL-, Cross-Site Scripting-, FFC- und FieldFormat-Schutzprüfungen werden angewendet, wenn **Upload-Dateien von Sicherheitsprüfungen ausschließen** nicht gesetzt ist

Ein Datei-Upload ist auch ein Formularelement, das über das Feld für den **Namen des** Steuerelements verfügt, das als Teil des Formulars gesendet wird.

Weitere Informationen finden Sie auf dieser Seite: Formulare

> **Hinweis**
>
> Der Formularschutz schließt verschachtelte Formulare, wenn formularbasierte Prüfungen aktiviert sind. Damit soll sichergestellt werden, dass der HTML-Standard eingehalten wird.

Prüfung der Feldformate

May 11, 2023

Die Feldformat-Überprüfung überprüft die Daten, die Benutzer in Webformularen an Ihre Websites senden. Dabei werden sowohl die Länge als auch der Typ der Daten untersucht, um sicherzustellen, dass sie für das Formularfeld geeignet sind, in dem sie angezeigt werden. Wenn die Web App Firewall in einer Benutzeranforderung unangemessene Webformulardaten erkennt, blockiert sie die Anfrage.

Die Feldformatprüfung verhindert, dass ein Angreifer unangemessene Webformulardaten an Ihre Website sendet, und verhindert so bestimmte Arten von Angriffen auf Ihre Website und Datenbankserver. Wenn ein bestimmtes Feld beispielsweise erwartet, dass der Benutzer eine Telefonnummer eingibt, untersucht die Prüfung Feldformate die vom Benutzer übermittelte Eingabe, um sicherzustellen, dass die Daten dem Format einer Telefonnummer entsprechen. Wenn für ein bestimmtes Feld ein Vorname erwartet wird, stellt die Prüfung der Feldformate sicher, dass die Daten in diesem Feld von einem Typ und einer Länge sind, die für einen Vornamen geeignet sind. Es macht dasselbe für jedes Formularfeld, das Sie konfigurieren, um es zu schützen.

Diese Prüfung gilt nur für HTML-Anfragen. Sie gilt nicht für XML-Anfragen. Sie können Feldformatprüfungen in HTML-Profilen oder Web 2.0-Profilen konfigurieren, um die HTML-Payload zum Schutz Ihrer Anwendungen zu überprüfen. Die Web App Firewall unterstützt auch den Field Format Check-Schutz für Google Web Toolkit (GWT) -Anwendungen.

Für die Prüfung der Feldformate müssen Sie eine oder mehrere Aktionen aktivieren. Die Web App Firewall untersucht die übermittelten Eingaben und wendet die angegebenen Aktionen an.

> **Hinweis**
>
> Die Regeln für das Feldformat verschärfen die Regeln. Sie aus erlernten Daten zur Entspannungsliste hinzuzufügen, wirkt wie eine Sperrregel.
>
> Um die Regeln für Feldformate zu lockern, entfernen Sie bitte einen bestimmten „Feldnamen“ aus der Liste der Feldformat-Relaxationen.

Sie haben die Möglichkeit, die Standardfeldformate festzulegen, um den Feldtyp und die Mindest- und Höchstlänge der Daten festzulegen, die in jedem Formularfeld auf jedem Webformular erwartet werden, das Sie schützen möchten. Sie können Relaxationsregeln verwenden, um ein Feldformat für ein einzelnes Feld eines bestimmten Formulars zu konfigurieren. Es können mehrere Regeln hinzugefügt werden, um den Feldnamen, die Aktions-URL und die Feldformate anzugeben. Geben Sie Feldformate an, um verschiedene Arten von Eingaben in verschiedenen Formularfeldern zu akzeptieren. Die Lernfunktion kann Empfehlungen für die Entspannungsregeln geben.

Aktionen**im Feldformat — Sie können die Aktionen**„Blockieren“, „Loggen“, „Statistiken“ und „Lernen“ aktivieren. Mindestens eine dieser Aktionen muss aktiviert sein, um den Field Format Check-Schutz zu aktivieren.

- **Blockieren**. Wenn Sie Block aktivieren, wird die Blockaktion ausgelöst, wenn die Eingabe nicht dem angegebenen Feldformat entspricht. Wenn eine Regel für das Zielfeld konfiguriert wurde, wird die Eingabe anhand der angegebenen Regel überprüft. Andernfalls wird es anhand der Standardfeldformatspezifikation überprüft. Jede Nichtübereinstimmung des Feldtyps oder der Angabe der Min/Max-Länge führt dazu, dass die Anfrage blockiert wird.
- **Loggen**. Wenn Sie die Protokollfunktion aktivieren, generiert die Feldformatprüfung Protokollmeldungen, in denen die Aktionen angegeben sind, die ausgeführt werden. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen block-

iert werden. Ein starker Anstieg der Anzahl von Protokollmeldungen kann auf böswillige Angriffsversuche hinweisen.

- **Statistiken**. Wenn diese Option aktiviert ist, sammelt die Statistikfunktion Statistiken über Verstöße und Protokolle. Ein unerwarteter Anstieg des Statistikzählers könnte darauf hindeuten, dass Ihre Anwendung angegriffen wird, oder Sie müssen möglicherweise die Konfiguration erneut überprüfen, um festzustellen, ob das angegebene Feldformat zu restriktiv ist.
- **Lernen**. Wenn Sie sich nicht sicher sind, welche Feldtypen oder Werte für Mindest- und Maximallänge für Ihre Anwendung ideal geeignet sind, können Sie die Lernfunktion verwenden, um Empfehlungen auf der Grundlage der gelernten Daten zu generieren. Die Web App Firewall Learning Engine überwacht den Datenverkehr und gibt Empfehlungen für Feldformate auf der Grundlage der beobachteten Werte. Um einen optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie die Lernoption möglicherweise für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Regeln bereitstellen und das Lernen deaktivieren.
  Hinweis: Die Lern-Engine der Web App Firewall kann nur die ersten 128 Byte des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen enthält, die für die ersten 128 Bytes übereinstimmen, kann die Lern-Engine möglicherweise nicht zwischen ihnen unterscheiden. In ähnlicher Weise kann die eingesetzte Entspannungsregel versehentlich alle diese Felder lockern.

Standardfeldformat— Zusätzlich zur Konfiguration der Aktionen können Sie das Standardfeldformat konfigurieren, um den Datentyp anzugeben, der in allen Formularfeldern für Ihre Anwendung erwartet wird. Als Feldformattyp kann ein Feldtyp ausgewählt werden. Die Parameter Minimallänge und Maximale Länge können verwendet werden, um die Länge der zulässigen Eingaben festzulegen. Als Alternative zu Feldtypen können Sie Character Maps verwenden, um anzugeben, was in einem Feld zulässig ist (außer in Cluster-Bereitstellungen).

- **Feldtyp**— Feldtypen sind benannte Ausdrücke, denen Sie Prioritätswerte zuweisen. Feldtypausdrücke geben die zulässigen Eingaben an und werden mit den übermittelten Daten abgeglichen, um festzustellen, ob die empfangenen Werte mit den zulässigen Werten übereinstimmen. Die Feldtypen werden in der Reihenfolge ihrer Prioritätsnummern geprüft. Eine niedrigere Zahl weist auf eine höhere Priorität hin. Die Web App Firewall bietet Ihnen die Möglichkeit, Ihre eigenen Feldtypen hinzuzufügen und ihnen die gewünschten Prioritäten zuzuweisen. Der Prioritätswert kann zwischen 0 und 64000 liegen. Die folgenden integrierten Feldtypen werden bereitgestellt, um den Konfigurationsprozess zu vereinfachen:

```
1  > sh appfw fieldtype
2  1)      Name:  integer           Regex:  "^[+-]?[0-9]+$"
3                  Priority:  30            Comment:  Integer
4                  Builtin:  IMMUTABLE
5  2)      Name:  alpha             Regex:  "^[a-zA-Z]+$"
6                  Priority:  40            Comment:  "Alpha
```



```
                    characters"
7                Builtin:  IMMUTABLE
8   3)       Name:  alphanum          Regex:  "^[a-zA-Z0-9]+$"
9                    Priority:  50            Comment:  "Alpha-numeric
                         characters"
10                   Builtin:  IMMUTABLE
11  4)       Name:  nohtml            Regex:  "^[^&<>]\*$"
12                   Priority:  60            Comment:  "Not HTML"
13                   Builtin:  IMMUTABLE
14  5)       Name:  any               Regex:  "^.\*$"
15               Priority:  70            Comment:  Anything
16                   Builtin:  IMMUTABLE
17      Done
18  >
19  <!--NeedCopy-->
```

> **Hinweis:** Die integrierten Feldtypen sind UNVERÄNDERLICH. Sie können nicht geändert oder entfernt werden. Alle Feldtypen, die Sie hinzufügen, sind ÄNDERBAR. Sie können sie bearbeiten oder entfernen.

Die Konfiguration eines Feldtyps als Standardfeldformat kann nützlich sein, wenn Sie über einen PCRE-Ausdruck verfügen, der die gültigen Eingaben in allen oder den meisten Formularfeldern für Ihre Anwendung identifizieren und die ungültigen Eingaben ausschließen kann. Wenn beispielsweise erwartet wird, dass alle Eingaben in Ihren Antragsformularen nur Zahlen und Buchstaben enthalten, sollten Sie das integrierte Feldtyp-Alphanum als Standardfeldtyp verwenden. Jedes nicht alphanumerische Zeichen wie ein umgekehrter Schrägstrich () oder ein Semikolon; in der Eingabe löst eine Verletzung aus. Sie können auch eigene benutzerdefinierte Feldtypen hinzufügen und diese verwenden, um Standardfeldformate zu konfigurieren. Wenn Sie beispielsweise die Kleinbuchstaben „x“, „y“ und „z“ zu den einzig zulässigen Alphazeichen machen möchten, können Sie einen benutzerdefinierten Feldtyp mit dem regulären Ausdruck „^ [x-z] +$“ konfigurieren. Sie können ihm eine höhere Priorität (niedrigere Prioritätsnummer) als die integrierten Feldtypen zuweisen und sie als Standardfeldtyp verwenden.

- **Mindestlänge** — Die standardmäßige Mindestdatenlänge, die Formularfeldern in Webformularen zugewiesen wird, die keine explizite Einstellung haben. Dieser Parameter ist standardmäßig auf 0 gesetzt, sodass der Benutzer das Feld leer lassen kann. Jede höhere Einstellung zwingt die Benutzer, das Feld auszufüllen.

  Vorsicht: Wenn der Mindestlängenwert 0 ist, der Feldtyp aber Integer, Alpha oder Alphawert ist, wird eine Anfrage blockiert, wenn trotz der Einstellung für die Mindestlänge ein Eingabefeld leer gelassen wird. Das liegt daran, dass der RegEx für diese Feldtypen ein +-Zeichen enthält, was ein oder mehrere Zeichen bedeutet. Um eine Ganzzahl von einem Alpha-Zeichen zu unterscheiden, ist mindestens ein Zeichen erforderlich.

- **Maximale Länge**— Die standardmäßige maximale Datenlänge, die Formularfeldern in Webformularen zugewiesen wird, für die keine explizite Einstellung vorhanden ist. Dieser Parameter ist standardmäßig auf 65535 gesetzt.

  > **Hinweis:** Zeichen im Vergleich zu Bytes. Die Mindest- und Höchstlängen für die Feldformate geben die Anzahl der Byte an, nicht die Anzahl der Zeichen. Sprachen mit einer Zeichendarstellung von mehr als einem Byte können dazu führen, dass das Limit überschritten wird, wenn weniger Zeichen als die für den Maximalwert konfigurierte Zahl vorliegen. Bei einer Doppelbyte-Zeichendarstellung erlaubt der Maximalwert von 9 beispielsweise nicht mehr als 4 Zeichen.
  > **Tipp:** Mit der GUI können Sie UTF-8-Zeichen direkt in die GUI ausschneiden und einfügen, ohne sie in Hex konvertieren zu müssen.

- **Zeichenzuordnungen**: Die Web App Firewall-Lernengine empfiehlt nicht nur die Feldtypen, sondern bietet Ihnen auch die zusätzliche Option „Zeichenzuordnungen verwenden“, um die Regeln für die Formatprüfung anzuwenden. Eine Zeichentabelle ist ein Satz aller Zeichen, die in einem bestimmten Formularfeld zulässig sind. Mithilfe von Zeichenzuordnungen können Sie die Feldformatspezifikation so anpassen, dass bestimmte Zeichen zugelassen oder nicht zugelassen werden. Für jedes Formularfeld wird eine separate Zeichentabelle generiert. Die Alpha- und numerischen Zeichen werden in Zeichentabelle unterschiedlich behandelt. Wenn ein Alpha-Zeichen in der Eingabe erscheint, sind alle Alpha-Zeichen [a-zA-Z] gemäß dem empfohlenen PCRE-Ausdruck in der Zeichentabelle zulässig. Ebenso sind alle Ziffern [0-9] zulässig, wenn eine Ziffer enthalten ist. Nicht druckbare Zeichen werden mit dem x-Konstrukt angegeben. Für die Empfehlungen zur Zeichentabelle werden nur Einzelbyte-Zeichen mit Werten zwischen 0 und 255 berücksichtigt.

  Eine Zeichentabelle kann spezifischer sein als die entsprechende Feldtypempfehlung. In manchen Situationen sind Charakterkarten möglicherweise die bessere Option, da Sie dadurch eine genauere Kontrolle über die Anzahl der Zeichen haben, die als Eingabe zulässig sind. Die bereitgestellten Zeichenzuordnungen werden als Zeichenketten angezeigt, die mit dem Präfix „CM“ beginnen, gefolgt von Ziffern. Die Priorität für die Charakterkarten beginnt bei 10000. Wie bei vom Benutzer hinzugefügten Feldtypen können Sie eine Zeichentabelle hinzufügen, bearbeiten oder entfernen. Charakterkarten, die derzeit in den bereitgestellten Regeln verwendet werden, können nicht geändert oder entfernt werden.

  Hinweis: Charakterkarten werden in Cluster-Bereitstellungen nicht unterstützt.

> **Hinweis**
>
> Wenn Sie eine Regel für Feldformate mit einem beliebigen integrierten Feldtyp hinzufügen und die Zeichentabelle anstelle von Feldtyp verwenden und speichern, werden die Änderungen nicht gespeichert und die Regel wird weiterhin mit Feldtyp angezeigt.

> Wenn die Zeichentabelle einem der integrierten Typen entspricht, wird der Feldtyp wiederverwendet, anstatt eine neue Zeichentabelle zu erstellen.

Konfiguration der Feldformatprüfung über die Befehlszeile

In der Befehlszeilenschnittstelle können Sie den Befehl add appfw fieldtype verwenden, um einen neuen Feldtyp hinzuzufügen. Sie können entweder den Befehl set appfw profile oder den Befehl add appfw profile verwenden, um die Feldformatprüfung zu konfigurieren und anzugeben, welche Aktionen ausgeführt werden sollen. Sie können den Befehl unset appfw profile verwenden, um die konfigurierten Einstellungen auf ihre Standardwerte zurückzusetzen. Um eine Feldformatregel anzugeben, verwenden Sie den Befehl bind appfw, um einen Feldtyp an ein Formularfeld und die Aktions-URL zusammen mit den Angaben zur Mindest- und Maximallänge zu binden.

Um einen Feldtyp mithilfe der Befehlszeile hinzuzufügen, zu entfernen oder anzuzeigen:

Verwenden Sie den Befehl add, um einen Feldtyp hinzuzufügen. Sie müssen den Namen, den regulären Ausdruck und die Priorität angeben, wenn Sie einen neuen Feldtyp hinzufügen. Sie haben auch die Möglichkeit, einen Kommentar hinzuzufügen. Sie können den Befehl show verwenden, um die konfigurierten Feldtypen anzuzeigen. Sie können einen Feldtyp auch löschen, indem Sie den Befehl remove verwenden, für den nur der Name des Feldtyps erforderlich ist.

```
add [appfw] fieldType <name> <regex> <priority> [-comment <string>]
```

Wobei:

<regex> ist ein regulärer Ausdruck

<priority> ist eine positive_integer

Beispiel:

```
add fieldtype "Cust_Zipcode" "^[0-9]{
 5 }
 [-][0-9]{
 4 }
 $" 4

-  show [appfw] fieldType [<name>]

    Example: sh fieldtype

    sh appfw fieldtype

    sh appfw fieldtype cust_zipcode

-  `rm [appfw] fieldType <name>`
```



```
16
17      Example: rm fieldtype cusT_ziPcode
18
19      `rm appfw fieldtype cusT_ziPcode`
20  <!--NeedCopy-->
```

> **Hinweis:** Wie oben gezeigt, ist die Verwendung von „appfw“ im Befehl optional. Beispielsweise sind „Add FieldType“ oder „Add appfw FieldType“ beide gültige Optionen. Die Namen der Feldtypen unterscheiden aufgrund der Normalisierung nicht zwischen Groß- und Kleinschreibung. Wie in den obigen Beispielen gezeigt, beziehen sich Cust_Zipcode, cust_zipcode und Cust_ZipCode auf denselben Feldtyp.

Um ein Feldformat zu konfigurieren, überprüfen Sie es mithilfe der Befehlszeile

Verwenden Sie entweder den Befehl set appfw profile oder den Befehl add appfw profile wie folgt:

- `set appfw profile <name> -fieldFormatAction (([block] [learn] [log] [ stats])| [none])`
- `set appfw profile <name>-defaultFieldFormatType <string>`
- `set appfw profile <name> -defaultFieldFormatMinLength <integer>`
- `set appfw profile <name> -defaultFieldFormatMaxLength <integer>`

So konfigurieren Sie eine Relaxationsregel für das Feldformat mithilfe der Befehlszeile

```
1  bind appfw profile <name> (-fieldFormat <string> <formActionURL>  <
       fieldType>
2  [-fieldFormatMinLength <positive_integer>]  [-fieldFormatMaxLength <
       positive_integer>]
3  [-isRegex ( REGEX | NOTREGEX )])
4  <!--NeedCopy-->
```

Beispiel:

```
1  bind appfw profile pr_ffc -fieldFormat "login_name" ".*/login.php"
       integer -fieldformatMinLength 3 -FieldformatMaxlength 6
2  <!--NeedCopy-->
```

Verwendung der GUI zur Konfiguration der Feldformate (Sicherheitscheck)

In der GUI können Sie die Feldtypen verwalten. Sie können auch die Sicherheitsprüfung Feldformate im Bereich für das Ihrer Anwendung zugeordnete Profil konfigurieren.

Um einen Feldtyp mithilfe der GUI hinzuzufügen, zu ändern oder zu entfernen

1. Navigieren Sie zum Knoten Application Firewall. Klicken Sie in den Einstellungen auf **Feldtypen verwalten**, um das Dialogfeld „Anwendungs-Firewall-Feldtyp konfigurieren“ aufzurufen.

2. Klicken Sie auf **Hinzufügen**, um einen neuen Feldtyp hinzuzufügen. Folgen Sie den Anweisungen in diesem Bereich und klicken Sie auf Erstellen. Sie können auch jeden vom Benutzer hinzugefügten Feldtyp bearbeiten oder löschen, wenn er derzeit nicht von einer bereitgestellten Regel verwendet wird.

Um die Feldformate hinzuzufügen oder zu ändern, überprüfen Sie die Sicherheitsüberprüfung mithilfe der GUI

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

   In der Tabelle zur Sicherheitsüberprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsüberprüfungen angezeigt. Sie haben 2 Möglichkeiten für die Konfiguration:

   a) Wenn Sie nur die Aktionen **Blockieren**, **Protokollieren**, **Statistiken**und **Lernen** für Feldformate aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf **OK**klicken und dann auf **Speichern und Schließen** klicken, um den Bereich Sicherheitsprüfung zu schließen.
   b) Wenn Sie zusätzliche Optionen für diese Sicherheitsüberprüfung konfigurieren möchten, doppelklicken Sie auf Feldformate, oder wählen Sie die Zeile aus und klicken Sie auf Aktionseinstellungen, um die folgenden Optionen für das **Standardfeldformat**anzuzeigen:
      - **Feldtyp**— Wählen Sie den Feldtyp aus, den Sie als Standardfeldtyp konfigurieren möchten. Sie können die integrierten und benutzerdefinierten Feldtypen auswählen. Die eingesetzten Charakterkarten sind ebenfalls in der Liste enthalten und können ausgewählt werden.
      - **Mindestlänge**— Geben Sie die Mindestanzahl von Zeichen an, die in jedem Feld enthalten sein müssen. Mögliche Werte: 0-65535.
      - **Maximale Länge**— Geben Sie die maximale Anzahl von Zeichen an, die in jedem Feld enthalten sein müssen. Mögliche Werte: 1-65535.
        Sie können die Aktionen **Blockieren**, **Protokollieren**, **Statistiken** und **Lernen** auch im Bereich Feldformateinstellungen bearbeiten.

   Nachdem Sie eine der oben genannten Änderungen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern und schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

So konfigurieren Sie eine Relaxationsregel für Feldformate mithilfe der GUI

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie

auf **Bearbeiten**.

2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**. Die Tabelle mit den Relaxationsregeln enthält einen Eintrag für Feldformate. Sie können auf diese Zeile doppelklicken oder diese Zeile auswählen und auf die Schaltfläche Bearbeiten klicken, um das Dialogfeld „Relaxationsregeln für Feldformate“ aufzurufen. Sie können die Operationen **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren**oder **Deaktivieren** für Relaxationsregeln ausführen.

Für eine konsolidierte Ansicht aller Relaxationsregeln können Sie die Zeile Feldformate markieren und auf Visualizer klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel hinzuzufügen oder eine vorhandene zu bearbeiten . Sie können auch eine Gruppe von Regeln aktivieren oder deaktivieren, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

Verwendung der Lernfunktion mit dem Field Formats Check

Wenn die Lernaktion aktiviert ist, überwacht die Web App Firewall Learning Engine den Datenverkehr und lernt die ausgelösten Verstöße. Sie können diese gelernten Regeln regelmäßig überprüfen. Nach reiflicher Überlegung können Sie die erlernte Regel als Relaxationsregel für das Feldformat anwenden.

Verbesserung des Lernens in Feldformaten— In Version 11.0 wurde eine Lernerweiterung der Web App Firewall eingeführt. In den vorherigen Versionen stoppt die Web App Firewall-Lernengine die Überwachung der gültigen Anfragen, sobald die erlernten Feldformatempfehlungen bereitgestellt wurden, um auf der Grundlage der neuen Datenpunkte neue Regeln zu empfehlen. Dies schränkt den konfigurierten Sicherheitsschutz ein, da die Lerndatenbank keine Repräsentationen der neuen Daten enthält, die in den gültigen Anfragen enthalten sind, die bei der Sicherheitsüberprüfung verarbeitet wurden.

Verstöße sind nicht mehr mit Lernen verbunden. Die Lernmaschine lernt und gibt unabhängig von den Verstößen Empfehlungen für die Feldformate ab. Die Lernmaschine überprüft nicht nur die blockierten Anfragen, um festzustellen, ob das aktuelle Feldformat zu restriktiv ist und gelockert werden muss, sondern überwacht auch die zulässigen Anfragen, um festzustellen, ob das aktuelle Feldformat zu permissiv ist, und ermöglicht es, die Sicherheit durch die Implementierung einer restriktiveren Regel zu erhöhen.

Im Folgenden finden Sie eine Zusammenfassung des Lernverhaltens von Field Formats:

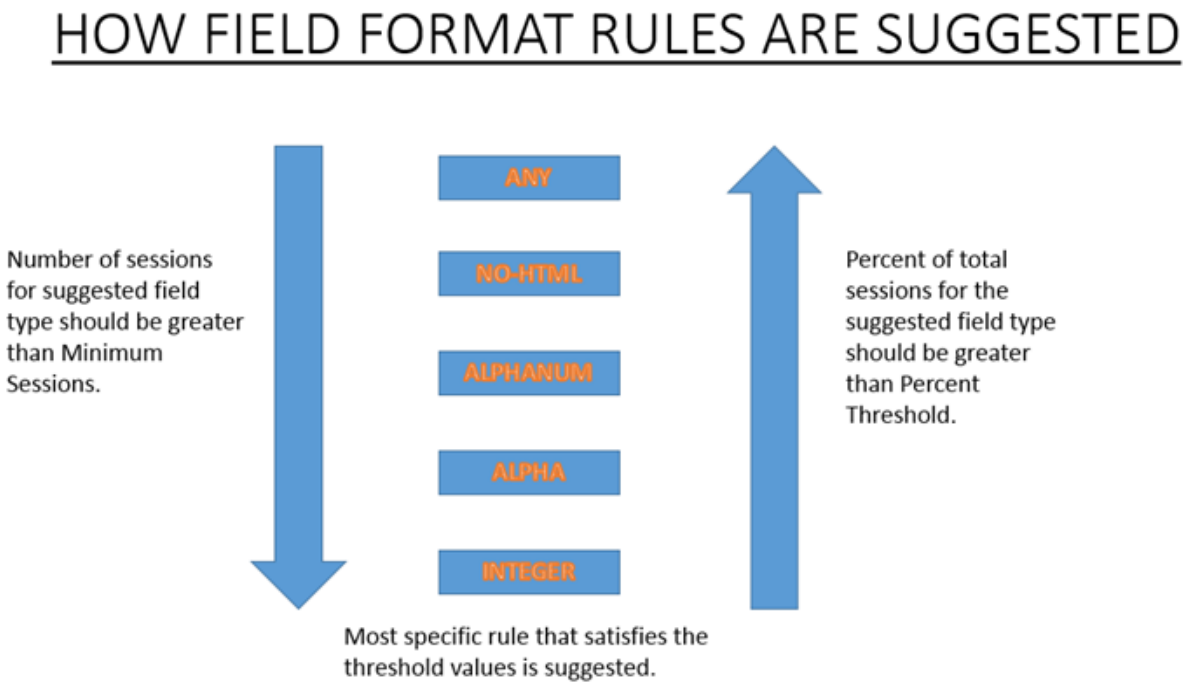
Es**ist kein Feldformat gebunden**— Das Verhalten bleibt in diesem Szenario unverändert. Alle Lerndaten werden an die aslearn-Engine gesendet. Die Lernmaschine schlägt eine Feldformatregel vor, die auf dem Datensatz basiert.

Das**Feldformat ist gebunden**: In den vorherigen Versionen werden beobachtete Daten nur im Falle eines Verstoßes an die aslearn-Engine gesendet. Die Lernmaschine schlägt eine Feldformatregel vor,

die auf dem Datensatz basiert. In der Version 11.0 werden alle Daten an die Aslearn-Engine gesendet, auch wenn kein Verstoß ausgelöst wurde. Die Lernmaschine schlägt eine Feldformatregel vor, die auf dem gesamten Datensatz aller empfangenen Eingaben basiert.

Anwendungsfall zur Verbesserung des Lernens:

Wenn die erlernten Regeln für das anfängliche Feldformat auf einer kleinen Datenstichprobe basieren, können einige untypische Werte zu einer Empfehlung führen, die für das Zielfeld zu nachsichtig ist. Das kontinuierliche Lernen ermöglicht es der Web App Firewall, Datenpunkte aus jeder Anfrage zu beobachten, um eine repräsentative Stichprobe für die erlernten Empfehlungen zu sammeln. Dies ist hilfreich, um die Sicherheit weiter zu erhöhen und das optimale Eingabeformat mit einem angemessenen Bereichswert bereitzustellen.



Das Lernen im Feldformat nutzt die Priorität der Feldtypen sowie die konfigurierten Einstellungen der folgenden Lernschwellen:

- **FieldFormatMinThreshold**— Die Mindestanzahl, mit der ein bestimmtes Formularfeld beobachtet werden muss, bevor eine erlernte Entspannung generiert wird. Standard: 1.
- **FieldFormatPercentThreshold**— Der Prozentsatz, mit dem ein Formularfeld einem bestimmten Feldtyp entsprach, bevor eine erlernte Entspannung generiert wird. Standard: 0.

Die Regelempfehlungen für Feldformate basieren auf den folgenden Kriterien:

- **Empfehlungen für Feldtypen**— Die Empfehlungen für Feldtypen richten sich nach den zugewiesenen Prioritäten der vorhandenen Feldtypen und den angegebenen Schwellenwerten für das Feldformat. Die Prioritäten bestimmen die Reihenfolge, in der die Feldtypen mit den

Eingaben abgeglichen werden. Eine niedrigere Zahl gibt eine höhere Priorität an. Beispielsweise hat der Feldtyp Integer die höhere Priorität (30) und wird daher vor dem Feldtyp alphanum (50) ausgewertet. Die Schwellenwerte bestimmen die Anzahl der Eingaben, die ausgewertet wurden, um eine repräsentative Stichprobe für den Datenpunkt zu erheben. Es ist wichtig, den konfigurierten Feldtypen die richtige Priorität zuzuweisen und einen geeigneten **LearningSeting-Wert** für die Parameter **FieldFormatPercentThreshold und FieldFormatMinThresholdzu konfigurieren, um die richtige Empfehlung für das Feldformat** zu erhalten. Der Feldtyp mit der höchsten Priorität, basierend auf den konfigurierten Schwellenwerten, wird zuerst mit den Eingaben abgeglichen. Wenn es eine Übereinstimmung gibt, wird dieser Feldtyp ohne Berücksichtigung der anderen Feldtypen vorgeschlagen. Beispielsweise stimmen die drei Standardfeldtypen Integer, Alphanum und Any überein, wenn alle Eingaben nur Zahlen enthalten. Integer wird jedoch empfohlen, da sie die höchste Priorität hat.

- **Empfehlungen für Mindest- und Maximallänge**— Die Berechnungen für die Mindest- und Maximallänge für das Feldformat werden unabhängig von der Bestimmung des Feldtyps durchgeführt. Die Längenberechnungen für das Feldformat basieren auf der durchschnittlichen Länge aller beobachteten Eingaben. Die Hälfte dieses berechneten Durchschnitts wird als Mindestwert vorgeschlagen, und der doppelte Wert dieses Durchschnitts wird als Maximalwert vorgeschlagen. Der Bereich für die Mindestlänge liegt zwischen 0 und 65535 und der Bereich für die maximale Länge zwischen 1 und 65535. Der konfigurierte Wert für die Mindestlänge darf die maximale Länge nicht überschreiten.
- **Behandlung von Leerzeichen**— Die Feldformatprüfung zählt jedes Leerzeichen, wenn die Länge der Feldformate überprüft wird. Führende oder nachstehende Leerzeichen werden nicht entfernt, und mehrere aufeinanderfolgende Leerzeichen in der Mitte der Eingabezeichenfolge werden bei der Eingabeverarbeitung nicht mehr zu einem einzigen Leerzeichen zusammengefasst.

Beispiel zur Veranschaulichung der Empfehlungen zum Feldformat:

```
Total requests: 100
Number of Req with Field Type:
Int : 22            (22 int values)  -  22%
Alpha : 44                  (44 alpha values)  -  44%
Alphanum: 14            (14 + 44 + 22 = 80 alphanum values) = 80%
noHTML: 10              (80 + 10 = 90 noHTML values) = 90%
any : 10                     (90 + 10 = 100 any values) = 100%

% threshold                              Suggested Field Type
0-22               int
23-44              alpha
45-80              alphanum
81-90              noHTML
91-100             any
```



```
15 <!--NeedCopy-->
```

So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

```
1 show appfw learningdata <profilename> FieldFormat
2 rm appfw learningdata <profilename> -fieldFormat <string>  <
     formActionURL>
3 export appfw learningdata <profilename> FieldFormat
4 <!--NeedCopy-->
```

So zeigen Sie erlernte Daten mit der GUI an oder verwenden sie

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **“Erweiterte Einstellungen** “ auf **Gelernte Regeln**. Sie können den Eintrag Feldformate in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die gelernten Regeln zuzugreifen. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Entspannungsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

   Sie haben auch die Möglichkeit, eine zusammengefasste Ansicht der erlernten Lockerungen anzuzeigen, indem Sie in der Tabelle Gelernte Regeln den Eintrag Feldformate auswählen und auf Visualizer klicken, um eine konsolidierte Ansicht aller erlernten Verstöße zu erhalten. Der Visualizer macht es sehr einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Ergreifen einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke empfohlen werden, um mehrere Regeln zu konsolidieren. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Zahl aus einer Dropdown-Liste auswählen. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Entspannungen einzusetzen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Verwenden der Protokollfunktion mit der Feldformatprüfung

Wenn die Protokollaktion aktiviert ist, werden die Verstöße gegen die Sicherheitsüberprüfung von Field Formats im Audit-Log als APPFW_FIELDFORMAT-Verstöße protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und verfolgen Sie die ns.logs im Ordner /var/log/, um auf die Protokollmeldungen zuzugreifen, die sich auf die Verstöße gegen Feldformate beziehen:

- `Shell`
- `tail -f /var/log/ns.log | grep APPFW_FIELDFORMAT`

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die GUI enthält ein sehr nützliches Tool (Syslog Viewer) zur Analyse der Logmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Application Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Sicherheitsüberprüfungen**. Markieren Sie die Zeile Feldformate und klicken Sie auf **Protokolle**. Wenn Sie direkt von der **Sicherheitsprüfung „Feldformate“** des Profils aus auf die Protokolle zugreifen, werden die Protokollmeldungen herausgefiltert und nur die Protokolle angezeigt, die sich auf diese Sicherheitsüberprüfungsverstöße beziehen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt **Prüfmeldungen** auf den Link **Syslog-Meldungen, um den**Syslog-Viewer**aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen ausgelöst werden können.
- Navigieren Sie zu **Application Firewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt **Prüfmeldungen** auf den Link Syslog-Meldungen, um den Syslog-Viewer aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung.

  Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um auf Protokollmeldungen über Verstöße gegen die Sicherheitsüberprüfung von Feldformaten zuzugreifen, filtern Sie, indem Sie in den Dropdownoptionen für Modul APPFW auswählen. Der Event-Typ zeigt eine Vielzahl von Optionen an, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_FIELDFORMAT** aktivieren und auf die Schaltfläche **Anwenden** klicken, werden im Syslog Viewer nur Protokollmeldungen angezeigt, die sich auf Verstöße gegen die Sicherheitsüberprüfung von Field Formats beziehen.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollmeldung setzen, werden mehrere Optionen, wie Module und EventType, unter der Protokollmeldung angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in den Protokollen hervorzuheben.

Beispiel für eine Protokollnachricht im systemeigenen Format, wenn die Anfrage nicht blockiert wird

```
1 Jun 10 22:32:26 <local0.info> 10.217.31.98 06/10/2015:22:32:26 GMT ns
     0-PPE-0 :
```



```
default APPFW APPFW_FIELDFORMAT 97 0 :  10.217.253.62 562-PPE0
x1MV+YnNGzQFM3Bsy2wti4bhXio0001 pr_ffc http://aaron.stratum8.net/FFC/
    login_post.php
Field format check failed for field passwd="65568888sz-*_" <not blocked
    >
Example of a CEF format log message when the request is blocked
Jun 11 00:03:51 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_FIELDFORMAT|6|src
    =10.217.253.62 spt=27076
method=POST requet=http://aaron.stratum8.net/FFC/maxlen_post.php msg=
    Field format check
failed for field text_area="" cn1=108 cn2=644 cs1=pr_ffc cs2=PPE0
cs3=GaUROfl1Nx1jJTvja5twH5BBqI0000 cs4=ALERT cs5=2015 act=blocked
<!--NeedCopy-->
```

Statistiken für Verstöße gegen Feldformate

Wenn die Statistikaktion aktiviert ist, wird der entsprechende Zähler für die Feldformatprüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Erhöhung des Protokollzählers kann je nach den konfigurierten Einstellungen variieren. Wenn beispielsweise die Aktion Blockieren aktiviert ist, erhöht die Anfrage nach einer Seite, die 3 Feldformatverstöße enthält, den Statistikzähler um eins, da die Seite blockiert wird, sobald der erste Verstoß gegen Feldformate erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anfrage den Statistikzähler für Verstöße und die Protokolle um 3, da jeder Verstoß gegen Feldformate eine separate Protokollmeldung generiert.

So zeigen Sie Feldformatestatistiken mithilfe der Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

```
sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
stat appfw profile <profile name>
```

So zeigen Sie Feldformatestatistiken mithilfe der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Anwendungsfirewall**.
2. Greifen Sie im rechten Bereich auf den Statistik-Link zu.
3. Verwenden Sie die Scrollleiste, um die Statistiken zu Verstößen gegen Feldformate und zu Protokollen einzusehen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Einsatztipp

- Aktiviere Aktionen im Feldformat protokollieren, lernen und Statistiken.
- Nachdem Sie eine repräsentative Stichprobe des Datenverkehrs zu Ihrer Anwendung durchgeführt haben, überprüfen Sie die erlernten Empfehlungen.
- Wenn ein Feldtyp von den meisten gelernten Regeln empfohlen wird, konfigurieren Sie diesen Feldtyp als Standardfeldtyp. Verwenden Sie für Mindest- und Höchstlängen den breitesten Bereich, der in diesen Regeln vorgeschlagen wird.
- Stellen Sie Regeln für andere Felder bereit, für die andere Feldtypen oder unterschiedliche Mindest- und Maximallängen besser geeignet sind.
- Aktiviere das Blockieren und deaktiviere das Lernen.
- Überwachen Sie Statistiken und Protokolle. Wenn immer noch eine erhebliche Anzahl von Verstößen ausgelöst wird, sollten Sie die Protokollmeldungen überprüfen, um sicherzustellen, dass es sich bei den Verstößen um böswillige Anfragen handelt, die blockiert worden sein müssen. Wenn gültige Anfragen als Verstöße gekennzeichnet werden, können Sie entweder die konfigurierte Feldformatregel bearbeiten, um sie weiter zu lockern, oder das Lernen erneut aktivieren, um Empfehlungen auf der Grundlage der neuen Datenpunkte zu erhalten.

> **Hinweis:** Sie können Ihre Konfiguration optimieren, indem Sie neue Lernempfehlungen erhalten.

Highlights

Beachten Sie die folgenden Punkte zur Feldformat-Sicherheitsprüfung:

- **Schutz**— Durch die Konfiguration optimaler Feldformatregeln können Sie sich vor vielen Angriffen schützen. Wenn Sie beispielsweise angeben, dass ein Feld nur Ganzzahlen enthalten kann, können Hacker mithilfe dieses Felds keine SQL-Injection- oder Cross-Site-Scripting-Angriffe starten, da die für den Start solcher Angriffe erforderlichen Eingaben die konfigurierten Feldformatanforderungen nicht erfüllen.
- **Leistung**— Sie können die zulässige Mindest- und Höchstlänge für die Eingaben in den Feldformatregeln einschränken. Dies kann verhindern, dass ein böswilliger Benutzer zu große Eingabezeichenfolgen eingibt, um den Verarbeitungsaufwand auf dem Server zu erhöhen, oder schlimmer noch, dazu führen, dass der Server aufgrund eines Stack-Überlaufs den Core ausgibt. Durch die Begrenzung der Eingabegröße können Sie die Zeit verkürzen, die für die Bearbeitung legitimer Anfragen benötigt wird.
- **Feldformate konfigurieren**— Sie müssen eine der Aktionen (Blockieren, Loggen, Statistiken, Lernen) aktivieren, um den Feldformatschutz zu aktivieren. Sie können auch die Feldformatregeln angeben, um die zulässigen Eingaben in Ihren Formularfeldern zu identifizieren.
- **Auswahl von Charakterkarten vs. Feldtypen**— Sowohl Zeichenzuordnungen als auch Feldtypen verwenden reguläre Ausdrücke. Eine Zeichenzuordnung stellt jedoch einen

spezifischeren Ausdruck bereit, indem die Liste der zulässigen Zeichen eingeschränkt wird. Beispielsweise könnte die Lernengine für eine Eingabe wie janedoe@citrix.com den Feldtyp nohtml, aber die Zeichentabelle [empfehlen. @-zA-Z] könnte spezifischer sein, da es die erlaubte Menge von Nicht-Alpha-Zeichen einschränkt. Die Option Zeichenzuordnung erlaubt neben Alpha-Zeichen nur zwei Nicht-Alpha-Zeichen: Punkt (.) und at (@).

- **Kontinuierliches Lernen**— Die Web App Firewall überwacht und berücksichtigt alle eingehenden Daten (Verstöße sowie zulässige Eingaben), um eine Lerntabelle für die Empfehlung von Regeln zu erstellen. Die Regeln werden überarbeitet und aktualisiert, sobald neue eingehende Daten eintreffen. Neue Feldformatregeln werden für ein Feld vorgeschlagen, auch wenn es bereits über eine gebundene Feldformatregel verfügt. Wenn die konfigurierten Feldformate zu restriktiv sind und die gültigen Anfragen blockieren, können Sie ein lockereres Feldformat verwenden. Ebenso können Sie, wenn die aktuellen Feldformate zu allgemein sind, die Sicherheit weiter verfeinern und erhöhen, indem Sie ein restriktiveres Feldformat verwenden.
- **Regeln überschreiben**— Wenn eine Regel bereits für eine Kombination aus Feld und URL bereitgestellt wurde, ermöglicht die GUI dem Benutzer, das Feldformat zu aktualisieren. In einem Dialogfeld werden Sie zur Bestätigung aufgefordert, die bestehende Regel zu ersetzen. Wenn Sie die Befehlszeilenschnittstelle verwenden, müssen Sie die vorherige Bindung explizit aufheben und dann die neue Regel binden.
- **Mehrfachübereinstimmung**— Wenn mehrere Feldformate mit einem bestimmten Feldnamen und seiner Aktions-URL übereinstimmen, wählt die Web App Firewall willkürlich eines davon aus, das angewendet werden soll.
- **Puffergrenze**— Wenn sich ein Feldwert über mehrere Streaming-Puffer erstreckt und das Format für diese beiden Teile des Feldwerts unterschiedlich ist, wird ein Feldformat, das „any“ entspricht, an die Lerndatenbank gesendet.
- **Feldformat vs. Feldkonsistenzprüfung**— Sowohl die Feldformatprüfung als auch die Feldkonsistenzprüfung sind formularbasierte Schutzprüfungen. Die Prüfung der Feldformate bietet einen anderen Schutz als die Konsistenzprüfung für Formularfelder. Die Konsistenzprüfung für Formularfelder stellt sicher, dass die Struktur der von Benutzern zurückgegebenen Webformulare intakt ist, dass die im HTML konfigurierten Datenformatbeschränkungen eingehalten werden und dass Daten in versteckten Feldern nicht geändert wurden. Dies ist ohne spezifische Kenntnisse über Ihre Webformulare möglich, außer denen, die es aus dem Webformular selbst ableitet. Die Prüfung der Feldformate überprüft, ob die Daten in jedem Formularfeld den spezifischen Formatierungsbeschränkungen entsprechen, die Sie manuell konfiguriert haben, oder ob die Lernfunktion generiert und von Ihnen genehmigt wurde. Mit anderen Worten, die Konsistenzprüfung für Formularfelder erzwingt die allgemeine Webformularsicherheit, während die Feldformat-Prüfung die spezifischen Regeln für die zulässigen Eingaben für Ihre Webformulare durchsetzt.

Konsistenzprüfung des Formularfelds

August 19, 2021

Die Konsistenzprüfung für Formularfelder untersucht die von Benutzern Ihrer Website zurückgegebenen Webformulare und stellt sicher, dass Webformulare vom Kunden nicht unangemessen geändert wurden. Diese Prüfung gilt nur für HTML-Anfragen, die ein Webformular enthalten, mit oder ohne Daten. Es gilt nicht für XML-Anforderungen.

Die Konsistenzprüfung für Formularfelder verhindert, dass Kunden beim Ausfüllen und Absenden eines Formulars nicht autorisierte Änderungen an der Struktur der Webformulare auf Ihrer Website vornehmen. Es stellt außerdem sicher, dass die von einem Benutzer übermittelten Daten die HTML-Einschränkungen für Länge und Typ erfüllen und dass Daten in ausgeblendeten Feldern nicht geändert werden. Dies verhindert, dass ein Angreifer ein Webformular manipuliert und das geänderte Formular verwendet, um unbefugten Zugriff auf die Website zu erhalten, die Ausgabe eines Kontaktformulars umzuleiten, das ein unsicheres Skript verwendet und dadurch unerwünschte Massen-E-Mails sendet, oder eine Schwachstelle in Ihrer Webserversoftware auszunutzen, um die Kontrolle über das Internet zu erlangen -Server oder das zugrunde liegende Betriebssystem. Webformulare sind auf vielen Websites ein schwaches Bindeglied und ziehen eine Vielzahl von Angriffen an.

Die Konsistenzprüfung für Formularfelder überprüft alle folgenden Punkte:

- Wenn ein Feld an den Benutzer gesendet wird, stellt die Überprüfung sicher, dass es vom Benutzer zurückgegeben wird.
- Die Prüfung erzwingt HTML-Feldlängen und -typen.

> **Hinweis:**
>
> - Die Konsistenzprüfung für Formularfelder erzwingt HTML-Beschränkungen für Datentyp und Länge, überprüft jedoch nicht anderweitig die Daten in Webformularen. Sie können das Kontrollkästchen Feldformate verwenden, um Regeln einzurichten, mit denen Daten überprüft werden, die in bestimmten Formularfeldern in Ihren Webformularen zurückgegeben werden.
> - Der Konsistenzschutz für Formularfelder fügt ein verstecktes Feld “as_fid” in die Antwortformulare ein, das an den Client gesendet wird. Das gleiche versteckte Feld wird von ADC entfernt, wenn der Kunde das Formular einreicht. Wenn clientseitiges JavaScript in den Formularfeldern eine Prüfsummenberechnung durchführt und dieselbe Prüfsumme im Backend überprüft wird, kann dies zu einem Bruch der Anwendung führen. In diesem Szenario wird empfohlen, das versteckte Feld für die Anwendungsfirewall-Formularfeldkonsistenz “as_fid” von der clientseitigen JavaScript-Prüfsummenberechnung zu lockern.

- Wenn Ihr Webserver kein Feld an den Benutzer sendet, erlaubt die Prüfung dem Benutzer nicht, dieses Feld hinzuzufügen und Daten darin zurückzugeben.
- Wenn es sich bei einem Feld um ein schreibgeschütztes oder ausgeblendetes Feld handelt, wird überprüft, ob sich die Daten nicht geändert haben.
- Wenn es sich bei einem Feld um ein Listenfeld oder ein Optionsfeld handelt, wird überprüft, ob die Daten in der Antwort einem der Werte in diesem Feld entsprechen.

Wenn ein von einem Benutzer zurückgegebenes Webformular gegen eine oder mehrere der Konsistenzprüfungen des Formularfelds verstößt und Sie die Web App Firewall nicht so konfiguriert haben, dass dieses Webformular gegen die Konsistenzprüfungen von Formularfeldern verstößt, wird die Anforderung blockiert.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Konsistenzprüfung für Formularfelder ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren, Lernen und Statistiken aktivieren oder deaktivieren.

Sie konfigurieren auch Sitzungslose Feldkonsistenz auf der Registerkarte Allgemein. Wenn Sessionless Field Consistency aktiviert ist, überprüft die Web App Firewall nur die Webformularstruktur und verzichtet auf die Teile der Formularfeldkonsistenzprüfung, die von der Pflege der Sitzungsinformationen abhängen. Dies kann die Konsistenzprüfung des Formularfelds mit geringer Sicherheitsstrafe für Websites beschleunigen, die viele Formulare verwenden. Um Sitzungslose Feldkonsistenz in allen Webformularen zu verwenden, wählen Sie On. Um es nur für Formulare zu verwenden, die mit der HTTP POST-Methode übermittelt wurden, wählen Sie PostOnly

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die Konsistenzprüfung für Formularfelder zu konfigurieren:

- `set appfw profile <name> -fieldConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`

Um Relaxationen für die Konsistenzprüfung des Formularfelds festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Prüfungen des Dialogfelds Konsistenzprüfung für Formularfelder ändern auf Hinzufügen, um das Dialogfeld Konsistenzprüfung hinzufügen zu öffnen, oder wählen Sie eine vorhandene Entspannung aus, und klicken Sie auf Öffnen, um das Dialogfeld Konsistenzprüfung für Formularfelder ändern zu öffnen. In beiden Dialogfeldern finden Sie die gleichen Optionen zum Konfigurieren einer Entspannung, wie unter Manuelle Konfiguration durch Verwendung der GUIbeschrieben.

Im Folgenden finden Sie Beispiele für die Konsistenzprüfung von Formularfeld-Konsistenzprüfungen:

Formularfeldnamen:

- Wählen Sie Formularfelder mit dem Namen UserType:

```
1  ^UserType$
```



```
<!--NeedCopy-->
```

- Wählen Sie Formularfelder mit Namen aus, die mit UserType_ beginnen und eine Zeichenfolge folgen, die mit einem Buchstaben oder einer Zahl beginnt und aus einem bis einundzwanzig Buchstaben, Zahlen oder dem Apostroph oder Bindestrich besteht:

```
^UserType_[0-9A-Za-z][0-9A-Za-z'-]{
0,20 }
$
<!--NeedCopy-->
```

- Wählen Sie Formularfelder mit Namen aus, die mit Türkisch-UserType_ beginnen und andernfalls mit dem vorherigen Ausdruck identisch sind, außer dass sie türkische Sonderzeichen enthalten können:

```
^T\xC3\xBCrk\xC3\xA7e-UserType_([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa
   -f])+$
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine vollständige Beschreibung der unterstützten Sonderzeichen und deren ordnungsgemäße Kodierung finden Sie unter PCRE-Zeichenkodierungsformat .

- Wählen Sie Formularfeldnamen aus, die mit einem Buchstaben oder einer Zahl beginnen, nur aus einer Kombination aus Buchstaben und/oder Zahlen bestehen und die die Zeichenfolge Num an beliebiger Stelle in der Zeichenfolge enthalten:

```
^[0-9A-Za-z]\*Num[0-9A-Za-z]\*$
<!--NeedCopy-->
```

URLs für Formularfeldaktionen:

- Wählen Sie URLs, die mit einer beliebigen Zeichenfolge nach der Abfrage beginnen`http://www.example.com/search.pl?` und diese enthalten, außer für eine neue Abfrage:

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Wählen Sie URLs aus, die mit `http://www.example-español.com` beginnen und Pfade und Dateinamen haben, die aus Groß- und Kleinbuchstaben, Zahlen, Nicht-ASCII-Sonderzeichen und ausgewählten Symbolen im Pfad bestehen. Das Zeichen ñ und alle anderen Sonderzeichen werden als codierte UTF-8-Zeichenfolgen dargestellt, die den Hexadezimalcode enthalten, der jedem Sonderzeichen im UTF-8-Zeichensatz zugewiesen ist:


```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Wählen Sie alle URLs aus, die die Zeichenfolge /search.cgi? enthalten:

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

> **Achtung:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Wildcards und insbesondere der Punkt-Sternchen-Kombination (.*) kann zu Ergebnissen führen, die Sie nicht wollen oder erwarten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten oder einen Angriff zulassen, den die Cookie-Konsistenzprüfung anderweitig hätte geblockt.

Prüfung der Kennzeichnung von CSRF-Formularen

May 11, 2023

Der Cross Site Request Forgery (CSRF)-Formulartaggingcheck kennzeichnet jedes Webformular, das von einer geschützten Website an Benutzer gesendet wird, mit einer eindeutigen und unvorhersehbaren FormID und untersucht dann die von Benutzern zurückgegebenen Webformulare, um sicherzustellen, dass die angegebene FormID korrekt ist. Diese Prüfung schützt vor websiteübergreifenden Anforderungsfälschungen. Diese Prüfung gilt nur für HTML-Anfragen, die ein Webformular mit oder ohne Daten enthalten. Sie gilt nicht für XML-Anfragen.

Der CSRF Form Tagging Check verhindert, dass Angreifer ihre eigenen Webformulare verwenden, um umfangreiche Formularantworten mit Daten an Ihre geschützten Websites zu senden. Diese Prüfung erfordert im Vergleich zu bestimmten anderen Sicherheitsüberprüfungen, die Webformulare eingehend analysieren, relativ wenig CPU-Verarbeitungskapazität. Es ist daher in der Lage, großvolumige Angriffe abzuwehren, ohne die Leistung der geschützten Website oder der Web App Firewall selbst ernsthaft zu beeinträchtigen.

Bevor Sie die CSRF Form Tagging-Prüfung aktivieren, müssen Sie Folgendes beachten:

- Sie müssen das Tagging von Formularen aktivieren. Die CSRF-Prüfung hängt vom Formular-Tagging ab und funktioniert ohne dieses nicht.
- Sie müssen die integrierte Caching-Funktion von NetScaler für alle Webseiten deaktivieren, die Formulare enthalten, die durch dieses Profil geschützt sind. Die integrierte Caching-Funktion und das CSRF-Formular-Tagging sind nicht kompatibel.
- Sie müssen erwägen, die Referer-Überprüfung zu aktivieren. Die Referer-Überprüfung ist Teil der Start-URL-Prüfung, verhindert jedoch seitenübergreifende Anforderungsfälschungen und nicht Verstöße gegen die Start-URL. Die Referer-Überprüfung belastet die CPU auch weniger als die CSRF Form Tagging-Prüfung. Wenn eine Anfrage gegen die Referer-Überprüfung verstößt, wird sie sofort blockiert, sodass die CSRF Form Tagging-Prüfung nicht aufgerufen wird.
- Die CSRF-Formular-Tagging-Prüfung funktioniert nicht bei Webformularen, die unterschiedliche Domänen in der Formular-URL und der Formular-Aktions-URL verwenden. CSRF Form Tagging kann beispielsweise ein Webformular mit einer Formularursprungs-URL von `http://www.example.com` und einer Formularaktions-URL von `http://www.example.org/form`.pl nicht schützen, da example.com und example.org unterschiedliche Domänen sind.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld CSRF Form Tagging Check ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Loggen, Lernen und Statistik aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um den CSRF Form Tagging Check zu konfigurieren:

- `set appfw profile <name> -CSRFtagAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Um Lockerungen für die CSRF Form Tagging-Prüfung festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Prüfungen des Dialogfelds Überprüfung der CSRF-Formularkennzeichnung ändern auf Hinzufügen, um das Dialogfeld Relaxation der CSRF-Formularkennzeichnung hinzufügen zu öffnen, oder wählen Sie eine vorhandene Relaxation aus und klicken Sie auf Öffnen, um das Dialogfeld Relaxation ändern zu öffnen. Beide Dialogfelder bieten dieselben Optionen für die Konfiguration einer Entspannung.

Eine Warnung wird generiert, wenn Sie das NetScaler Web App Firewall-Sitzungslimit auf einen Wert von 0 oder weniger setzen, da sich eine solche Einstellung auf die erweiterte Schutzüberprüfung auswirkt, die eine ordnungsgemäß funktionierende Web App Firewall-Sitzung erfordert.

Im Folgenden finden Sie Beispiele für Lockerungen von CSRF-Formular-Tagging-Checks:

Hinweis: Die folgenden Ausdrücke sind URL-Ausdrücke, die sowohl in den URL-Rollen Form Origin URL als auch Form Action URL verwendet werden können.

- Wählen Sie URLs aus, die mit einer beliebigen Zeichenfolge nach der Abfrage beginnen `http://www.example.com/search.pl?` und diese enthalten, mit Ausnahme einer neuen Abfrage:


```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Wählen Sie URLs, die mit Pfaden `http://www.example-español.com` und Dateinamen beginnen und diese enthalten, die aus Groß- und Kleinbuchstaben, Zahlen, Nicht-ASCII-Sonderzeichen und ausgewählten Symbolen im Pfad bestehen. Das ñ-Zeichen und alle anderen Sonderzeichen werden als codierte UTF-8-Zeichenketten dargestellt, die den Hexadezimalcode enthalten, der jedem Sonderzeichen im UTF-8-Zeichensatz zugewiesen ist:

```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Wählen Sie alle URLs aus, die die Zeichenfolge /search.cgi enthalten? :

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

Wichtig

Reguläre Ausdrücke sind leistungsstark. Wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Kombination aus Punkt und Stern (.*) aus Metazeichen und Platzhaltern kann zu unerwünschten Ergebnissen führen, z. B. zum Sperren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die Prüfung andernfalls blockiert hätte.

Tipp

Wenn der Referrer-Header enableValidate unter der Start-URL-Aktion aktiviert ist, stellen Sie sicher, dass die Referrer-Header-URL auch zu StartUrl hinzugefügt wird.

Hinweis

Wenn NetScaler das appfw_session_limit erreicht und CSRF-Prüfungen aktiviert sind, friert die Webanwendung ein.

Um das Einfrieren von Webanwendungen zu verhindern, verringern Sie das Sitzungs-Timeout und erhöhen Sie das Sitzungslimit, indem Sie die folgenden Befehle verwenden:

Über die CLI: > setappfw-Einstellungen —sessiontimeout 300 Von der Shell

> aus: root @ns # nsapimgr_wr.sh -s appfw_session_limit=200000
>
> Das Protokollieren und Generieren von SNMP-Alarmen, wenn appfw_session_limit erreicht ist, hilft Ihnen bei der Behebung und beim Debuggen von Problemen.

Verwaltung von CSRF-Formularen zur Kennzeichnung von Checks

May 11, 2023

Sie konfigurieren eine Ausnahme (oder Lockerung) für die CSRF-Formular-Tagging-Sicherheitsprüfung im Dialogfeld „Cross-Site Request Forgery Tagging Check Relaxation hinzufügen“ oder im Dialogfeld „Cross-Site Request Forgery Tagging Check Relaxation“ ändern.

Um ein CSRF-Formular-Tagging zu konfigurieren, überprüfen Sie die Entspannung mithilfe der GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Web App Firewall-Profil konfigurieren** auf die Registerkarte **Sicherheitsprüfungen** . Die Registerkarte **Sicherheitsprüfungen** enthält die Liste der Web App Firewall-Sicherheitsprüfungen.
4. Gehen Sie wie folgt vor, um eine CSRF-Relaxation hinzuzufügen oder zu ändern:
   - Um eine neue Entspannung hinzuzufügen, klicken Sie auf Hinzufügen.
   - Um eine vorhandene Entspannung zu ändern, wählen Sie die Entspannung aus, die Sie ändern möchten, und klicken Sie dann auf **Öffnen**.

   Das Dialogfeld **Cross-Site Request Forgery Tagging Check Relaxation hinzufügen oder Relaxation** für **Cross-Site Request Forgery Tagging Check Relaxation ändern** wird angezeigt. Mit Ausnahme des Titels sind diese Dialogfelder identisch.
5. Füllen Sie das Dialogfeld wie unten beschrieben aus.
   - **Aktiviertes Kontrollkästchen**— Wählen Sie dieses Kontrollkästchen aus, um diese Relaxation oder Regel aktiv zu verwenden. Deaktivieren Sie das Kontrollkästchen, um sie zu deaktivieren.
   - **Quell-URL des Formulars**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, die das Formular hostet.

- **URL der Formularaktion**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, an die die in das Formular eingegebenen Daten übermittelt werden.
- **Kommentare**— Geben Sie im Textbereich einen Kommentar ein. Optional.

> **Hinweis:**
>
> Für jedes Element, das einen regulären Ausdruck erfordert, können Sie den regulären Ausdruck eingeben, das Menü „ **Regex-Tokens** “ verwenden, um reguläre Ausdruckselemente und Symbole direkt in das Textfeld einzufügen, oder auf **Regex-Editor** klicken, um das Dialogfeld „ **Regulären Ausdruck hinzufügen** “ zu öffnen und es zum Erstellen des Ausdrucks zu verwenden.

6. Klicken Sie auf **OK**. Das Dialogfeld **Cross-Site Request Forgery Tagging Check Relaxation hinzufügen oder Relaxation** für **Cross-Site Request Forgery Tagging Check Relaxation ändern** wird geschlossen, und Sie kehren zum Dialogfeld **Cross-Site Request Forgery Tagging Check modifizieren** zurück.
7. Um eine Entspannung oder Regel zu entfernen, wählen Sie sie aus, und klicken Sie dann auf **Entfernen**.
8. Um eine Entspannung oder Regel zu aktivieren, wählen Sie sie aus, und klicken Sie dann auf **Aktivieren**.
9. Um eine Entspannung oder Regel zu deaktivieren, wählen Sie sie aus, und klicken Sie dann auf **Deaktivieren**.
10. Um die Einstellungen und Beziehungen aller vorhandenen Relaxationen in einer integrierten interaktiven Grafikdarstellung zu konfigurieren, klicken Sie auf **Visualizer**, und verwenden Sie die Anzeigetools.
11. Um erlernte Regeln für die CSRF-Prüfung zu überprüfen und zu konfigurieren, klicken Sie auf **Lernen** und führen Sie die Schritte unter So konfigurieren und verwenden Sie die Lernfunktionaus.
12. Klicken Sie auf **OK**.

NetScaler Web App Firewall auf Azure bereitstellen

September 11, 2023

NetScaler Web App Firewall ist eine Lösung der Enterprise-Klasse, die modernsten Schutz für moderne Anwendungen bietet. NetScaler Web App Firewall mindert Bedrohungen für öffentlich zugängliche Ressourcen wie Websites, Webanwendungen und APIs. Die NetScaler Web App Firewall umfasst

IP-Reputationsbasierte Filterung, Bot-Abwehr, Schutz vor OWASP Top 10-Anwendungsbedrohungen, Layer-7-DDoS-Schutz und mehr. Ebenfalls enthalten sind Optionen zur Durchsetzung der Authentifizierung, starke SSL/TLS-Chiffren, TLS 1.3, Ratenbegrenzung und Rewrite-Richtlinien. NetScaler Web App Firewall verwendet sowohl grundlegende als auch erweiterte WAF-Schutzmaßnahmen und bietet umfassenden Schutz für Ihre Anwendungen mit beispielloser Benutzerfreundlichkeit. Es ist eine Frage von Minuten, bis Sie loslegen können. Darüber hinaus spart NetScaler Web App Firewall den Benutzern durch die Verwendung eines automatisierten Lernmodells, das als dynamisches Profiling bezeichnet wird, wertvolle Zeit. Indem NetScaler Web App Firewall automatisch lernt, wie eine geschützte Anwendung funktioniert, passt sie sich der Anwendung an, selbst wenn Entwickler die Anwendungen bereitstellen und ändern. NetScaler Web App Firewall hilft bei der Einhaltung aller wichtigen behördlichen Standards und Gremien, einschließlich PCI-DSS, HIPAA und mehr. Mit unseren CloudFormation-Vorlagen war es noch nie so einfach, schnell einsatzbereit zu sein. Mit Auto Scaling können Benutzer sicher sein, dass ihre Anwendungen auch bei wachsendem Datenverkehr geschützt bleiben.

Die NetScaler Web App Firewall kann entweder als Layer-3-Netzwerkgerät oder als Layer-2-Netzwerkbrücke zwischen Kundenservern und Kundenbenutzern installiert werden, normalerweise hinter dem Router oder der Firewall des Kundenunternehmens. Weitere Informationen finden Sie unter Einführung in die NetScaler Web App Firewall.

NetScaler Web App Firewall Bereitstellungsstrategie

1. Der Einsatz der Web Application Firewall dient der Bewertung, welche Anwendungen oder spezifischen Daten maximalen Sicherheitsschutz benötigen, welche weniger anfällig sind und für welche Sicherheitsüberprüfungen sicher umgangen werden können. Dies hilft Benutzern dabei, eine optimale Konfiguration zu finden und geeignete Richtlinien und Verbindungspunkte zur Trennung des Datenverkehrs zu entwerfen. Beispielsweise möchten Benutzer möglicherweise eine Richtlinie konfigurieren, um die Sicherheitsinspektion von Anfragen nach statischen Webinhalten wie Bildern, MP3-Dateien und Filmen zu Bypass, und eine andere Richtlinie konfigurieren, um erweiterte Sicherheitsprüfungen auf Anfragen nach dynamischen Inhalten anzuwenden. Benutzer können mehrere Richtlinien und Profile verwenden, um unterschiedliche Inhalte derselben Anwendung zu schützen.
2. Erstellen Sie als Grundlage für die Bereitstellung einen virtuellen Server und führen Sie Testdatenverkehr durch diesen aus, um sich ein Bild von der Geschwindigkeit und Menge des Datenverkehrs zu machen, der durch das Benutzersystem fließt.
3. Stellen Sie die Web Application Firewall bereit. Verwenden Sie NetScaler ADM und das Web Application Firewall StyleBook, um die Web Application Firewall zu konfigurieren. Einzelheiten finden Sie im Abschnitt StyleBook weiter unten in diesem Handbuch.
4. Implementieren Sie die NetScaler Web App Firewall und OWASP Top Ten.

Die drei Schutzmaßnahmen der Web Application Firewall sind besonders wirksam gegen gängige Arten von Webangriffen und werden daher häufiger eingesetzt als alle anderen. Daher sollten sie bei der ersten Bereitstellung implementiert werden. Sie sind:

- **HTML Cross-Site Scripting**: Untersucht Anfragen und Antworten auf Skripte, die versuchen, auf Inhalte auf einer anderen Website als der, auf der sich das Skript befindet, zuzugreifen oder diese zu ändern. Wenn diese Prüfung ein solches Skript findet, macht sie das Skript entweder unschädlich, bevor die Anfrage oder Antwort an ihr Ziel weitergeleitet wird, oder sie blockiert die Verbindung.
- **HTML-SQL-Injection**: Untersucht Anfragen, die Formularfelddaten enthalten, auf Versuche, SQL-Befehle in eine SQL-Datenbank einzufügen. Wenn diese Prüfung injizierten SQL-Code erkennt, blockiert sie entweder die Anfrage oder macht den injizierten SQL-Code unschädlich, bevor die Anfrage an den Webserver weitergeleitet wird.

  > **Hinweis:**
  >
  > Stellen Sie sicher, dass Ihre Web App Firewall korrekt konfiguriert ist, damit die folgenden Bedingungen in Ihrer Konfiguration gelten:

```
>\*  Wenn Benutzer die HTML Cross-Site Scripting-Prüfung oder die HTML SQL Injection-Prüfung (oder beide) aktivieren.
>
>\*  Benutzergeschützte Websites akzeptieren Datei-Uploads oder enthalten Webformulare, die große POST-Textdaten enthalten können.
```

Weitere Informationen zur Konfiguration der Web Application Firewall für diesen Fall finden Sie unter Konfiguration der Anwendungsfirewall: Konfiguration der Web App Firewall.

- **Pufferüberlauf**: Untersucht Anfragen, um Versuche zu erkennen, einen Pufferüberlauf auf dem Webserver zu verursachen.

Konfiguration der Web Application Firewall

Stellen Sie sicher, dass die NetScaler Web App Firewall bereits aktiviert ist und ordnungsgemäß funktioniert. Es wird empfohlen, NetScaler Web App Firewall mit dem Web Application Firewall StyleBook zu konfigurieren. Für die meisten Benutzer ist dies die einfachste Methode, die Web Application Firewall zu konfigurieren, und sie wurde entwickelt, um Fehler zu vermeiden. Sowohl die GUI als auch die Befehlszeilenschnittstelle richten sich an erfahrene Benutzer, hauptsächlich um eine bestehende Konfiguration zu ändern oder erweiterte Optionen zu verwenden.

SQL-Injektion

Die HTML-SQL-Injection-Prüfung der NetScaler Web App Firewall bietet spezielle Schutzmaßnahmen gegen die Injektion von nicht autorisiertem SQL-Code, der die Sicherheit von Benutzeranwendungen beeinträchtigen könnte. NetScaler Web App Firewall untersucht die Anforderungsnutzlast für injizierten SQL-Code an drei Stellen: 1) POST-Text, 2) Header und 3) Cookies. Weitere Informationen finden Sie unter HTML SQL Injection Check.

Siteübergreifendes Scripting

Bei der Prüfung von HTML Cross-Site Scripting (Cross-Site Scripting) werden sowohl die Header als auch die POST-Texte von Benutzeranfragen auf mögliche Cross-Site-Scripting-Angriffe untersucht. Findet es ein Cross-Site-Script, modifiziert (transformiert) es entweder die Anfrage, um den Angriff unschädlich zu machen, oder blockiert die Anfrage. Weitere Informationen finden Sie unter HTML Cross-Site Scripting Check.

Überprüfung des Pufferüberlaufs

Die Pufferüberlaufprüfung erkennt Versuche, einen Pufferüberlauf auf dem Webserver auszulösen. Wenn die Web Application Firewall feststellt, dass die URL, die Cookies oder der Header länger als die konfigurierte Länge sind, blockiert sie die Anfrage, da dies zu einem Pufferüberlauf führen kann. Weitere Informationen finden Sie unter Pufferüberlaufprüfung.

Virtuelles Patchen/Signaturen

Die Signaturen enthalten spezifische, konfigurierbare Regeln, um den Schutz von Benutzerwebsites vor bekannten Angriffen zu vereinfachen. Eine Signatur stellt ein Muster dar, das Bestandteil eines bekannten Angriffs auf ein Betriebssystem, einen Webserver, eine Website, einen XML-basierten Webdienst oder eine andere Ressource ist. Ein umfangreicher Satz vorkonfigurierter integrierter oder systemeigener Regeln bietet eine einfach zu bedienende Sicherheitslösung, die das Potenzial des Musterabgleichs nutzt, um Angriffe zu erkennen und vor Anwendungsschwachstellen zu schützen. Weitere Informationen finden Sie unter Signaturen.

Die NetScaler Web App Firewall unterstützt sowohl die **automatische als auch die manuelle Aktualisierung** von Signaturen.
Wir empfehlen außerdem die **automatische Aktualisierung** für Signaturen zu aktivieren, um auf dem neuesten Stand zu bleiben.

Diese Signaturdateien werden in der AWS-Umgebung gehostet, und es ist wichtig, den ausgehenden Zugriff auf NetScaler-IP-Adressen von Netzwerk-Firewalls aus zuzulassen, um die neuesten Signaturdateien abzurufen. Die Aktualisierung von Signaturen auf dem NetScaler während der Verarbeitung von Echtzeitverkehr hat keine Auswirkung.

Analysen zur Anwendungssicherheit

Das**Application Security Dashboard**bietet einen ganzheitlichen Überblick über den Sicherheitsstatus von Benutzeranwendungen. Es zeigt beispielsweise wichtige Sicherheitsmetriken wie Sicherheitsverletzungen, Signaturverletzungen und Bedrohungsindizes. Das Anwendungssicherheits-Dashboard zeigt auch angriffsbezogene Informationen wie Syn-Attacken, Angriffe auf kleine Fenster und DNS-Flood-Angriffe für den entdeckten NetScaler an.

> **Hinweis:**
>
> Um die Metriken des Anwendungssicherheits-Dashboards anzuzeigen, sollte AppFlow for Security Insight auf den NetScaler-Instanzen aktiviert sein, die Benutzer überwachen möchten.

So zeigen Sie die Sicherheitsmetriken einer NetScaler-Instanz im Anwendungssicherheits-Dashboard an:

1. Melden Sie sich mit den Administratoranmeldedaten bei NetScaler ADM an.
2. Navigieren Sie zu**Applications > App Security Dashboard**und wählen Sie die Instanz-IP-Adresse aus der Geräteliste aus.

Benutzer können die im Application Security Investigator gemeldeten Unstimmigkeiten weiter untersuchen, indem sie auf die im Diagramm dargestellten Blasen klicken.

Zentralisiertes Lernen auf ADM

NetScaler Web App Firewall schützt Benutzer-Webanwendungen vor böswilligen Angriffen wie SQL-Injection und Cross-Site Scripting (XSS). Um Datenschutzverletzungen zu verhindern und den richtigen Sicherheitsschutz zu bieten, müssen Benutzer ihren Datenverkehr auf Bedrohungen und verwertbare Echtzeitdaten zu Angriffen überwachen. Manchmal kann es sich bei den gemeldeten Angriffen um falsch positive Ergebnisse handeln, und diese müssen ausnahmsweise angegeben werden.

Das zentralisierte Lernen auf NetScaler ADM ist ein sich wiederholender Musterfilter, der es der WAF ermöglicht, das Verhalten (die normalen Aktivitäten) von Benutzer-Webanwendungen zu lernen.

Basierend auf der Überwachung generiert die Engine eine Liste mit vorgeschlagenen Regeln oder Ausnahmen für jede Sicherheitsüberprüfung, die auf den HTTP-Verkehr angewendet wird.

Es ist viel einfacher, Entspannungsregeln mithilfe der Learning Engine bereitzustellen, als sie manuell als notwendige Entspannungen bereitzustellen.

Um die Lernfunktion bereitzustellen, müssen Benutzer zunächst ein Web Application Firewall-Profil (Satz von Sicherheitseinstellungen) auf dem Benutzer NetScaler konfigurieren. Weitere Informationen finden Sie unter Web App Firewall-Profile erstellen.

NetScaler ADM generiert für jede Sicherheitsüberprüfung eine Liste von Ausnahmen (Lockerungen). Als Administrator können Sie die Liste der Ausnahmen in NetScaler ADM überprüfen und entscheiden, ob Sie sie bereitstellen oder überspringen möchten.

Mit der WAF-Lernfunktion in NetScaler ADM können Sie:

- Konfigurieren Sie ein Lernprofil mit den folgenden Sicherheitsüberprüfungen.
  - Pufferüberlauf
  - Siteübergreifendes HTML-Scripting

    > **Hinweis:**
    >
    > Die standortübergreifende Skriptbeschränkung gilt nur für FormField.

  - HTML-SQL-Injektion

    > **Hinweis:**
    >
    > Für die HTML-SQL-Injection-Prüfung müssen Benutzer`set -sqlinjectionTransformSpecialC ONundset -sqlinjectiontype sqlspclcharorkeywords` in NetScaler konfigurieren .
- Überprüfen Sie die Relaxationsregeln in NetScaler ADM und entscheiden Sie, ob Sie die erforderlichen Maßnahmen ergreifen möchten (bereitstellen oder überspringen).
- Erhalten Sie die Benachrichtigungen per E-Mail, Slack und ServiceNow.
- Verwenden Sie das Dashboard, um Details zur Entspannung anzuzeigen.

So verwenden Sie das WAF-Lernen in NetScaler ADM:

1. Das Lernprofil konfigurieren: Das Lernprofilkonfigurieren
2. Siehe die Entspannungsregeln: Entspannungsregeln und Leerlaufregeln anzeigen
3. Verwenden Sie das WAF-Lern-Dashboard: WAF-Lern-Dashboard anzeigen

Stilbücher

StyleBooks vereinfachen die Verwaltung komplexer NetScaler-Konfigurationen für Benutzeranwendungen. Ein StyleBook ist eine Vorlage, mit der Benutzer NetScaler-Konfigurationen erstellen und verwalten können. Hier geht es den Benutzern hauptsächlich um das StyleBook, mit dem die Web Application Firewall bereitgestellt wird. Weitere Informationen zu StyleBooks finden Sie unter StyleBooks.

Analytik von Sicherheitseinblicken

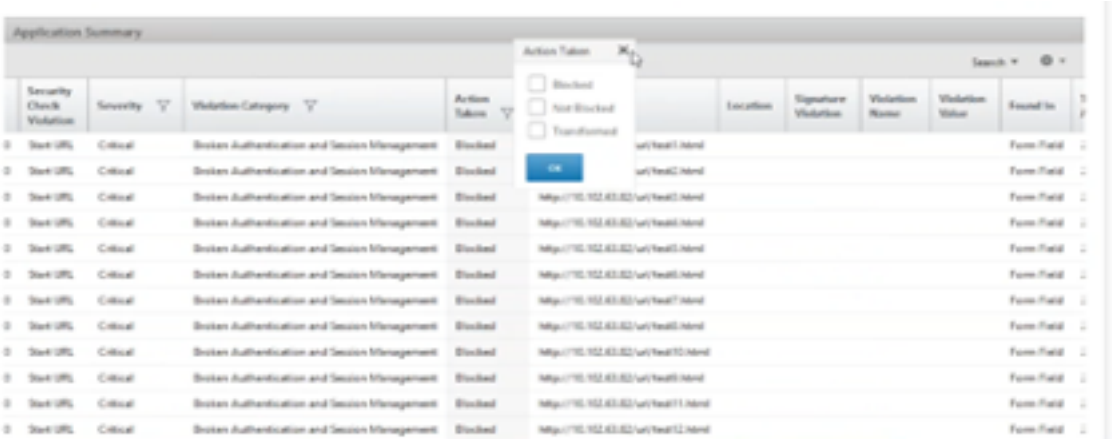
Web- und Webdienstanwendungen, die dem Internet ausgesetzt sind, sind zunehmend anfällig für Angriffe geworden. Um Anwendungen vor Angriffen zu schützen, benötigen Benutzer Einblicke in Art und Ausmaß vergangener, gegenwärtiger und drohender Bedrohungen, verwertbare Echtzeitdaten zu Angriffen und Empfehlungen für Gegenmaßnahmen. Security Insight bietet eine zentrale Lösung, mit der Benutzer den Sicherheitsstatus von Benutzeranwendungen beurteilen und Korrekturmaßnahmen zum Schutz von Benutzeranwendungen ergreifen können.
Weitere Informationen finden Sie unter Security Insight.

Erhalten Sie detaillierte Informationen über Sicherheitsverletzungen

Benutzer möchten möglicherweise eine Liste der Angriffe auf eine Anwendung einsehen und Einblicke in die Art und Schwere der Angriffe, die von der ADC-Instanz ergriffenen Maßnahmen, die angeforderten Ressourcen und die Quelle der Angriffe erhalten.

Beispielsweise möchten Benutzer möglicherweise ermitteln, wie viele Angriffe auf Microsoft Lync blockiert wurden, welche Ressourcen angefordert wurden und welche IP-Adressen die Quellen haben.

Klicken Sie im**Security Insight-Dashboard**auf**Lync** > **Gesamtzahl der Verstöße**. Klicken Sie in der Tabelle in der Spaltenüberschrift**Aktion**ausgeführt auf das Filtersymbol, und wählen Sie dann**Blockiert**aus.



Informationen zu den Ressourcen, die angefordert wurden, finden Sie in der Spalte**URL**. Informationen zu den Quellen der Angriffe finden Sie in der Spalte**Client-IP**.

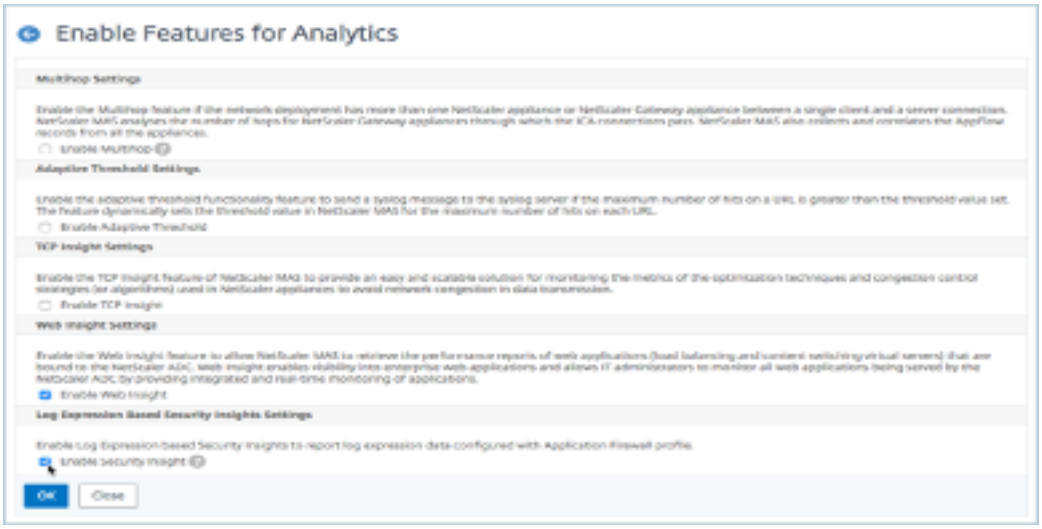
Details zum Protokollausdruck anzeigen

NetScaler verwendet Protokollausdrücke, die mit dem Application Firewall-Profil konfiguriert sind, um Maßnahmen gegen Angriffe auf eine Anwendung im Benutzerunternehmen zu ergreifen. In **Security Insight**können Benutzer die Werte anzeigen, die für die von der ADC-Instanz verwendeten Protokollausdrücke zurückgegeben wurden. Zu diesen Werten gehören Anforderungsheader, Anforderungstext usw. Zusätzlich zu den Werten für den Protokollausdruck können Benutzer auch den Namen des Protokollausdrucks und den Kommentar für den Protokollausdruck anzeigen, der im Application Firewall-Profil definiert ist, das die ADC-Instanz verwendet hat, um Maßnahmen gegen den Angriff zu ergreifen.

Voraussetzungen:

Stellen Sie sicher, dass Benutzer:

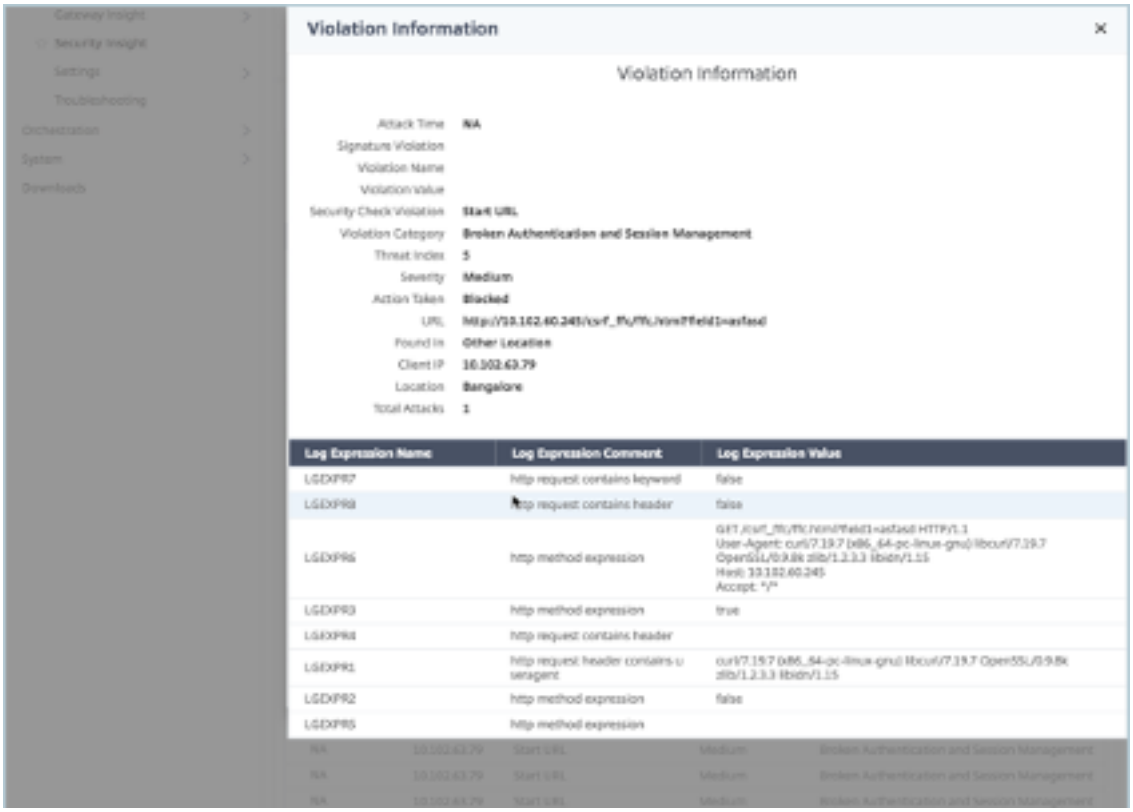
- Konfigurieren Sie Protokollausdrücke im Application Firewall-Profil. Weitere Informationen finden Sie unter Application Firewall.
- Aktivieren Sie auf Protokollausdrücken basierende Security Insights-Einstellungen in NetScaler ADM. Führen Sie folgende Schritte aus:
  - Navigieren Sie zu**Analytics** > **Einstellungen**und klicken Sie auf**Funktionen für Analytics aktivieren**.
  - Wählen Sie auf der Seite „Features für Analytics**aktivieren“ im Abschnitt „Auf Logausdruck basierende Security InsightSetting**“ die Option „Enable Security Insight**“**aus



Beispielsweise möchten Sie möglicherweise die Werte des Protokollausdrucks anzeigen, der von der

ADC-Instanz für die Aktion zurückgegeben wurde, die sie bei einem Angriff auf Microsoft Lync im Benutzerunternehmen ausgeführt hat.

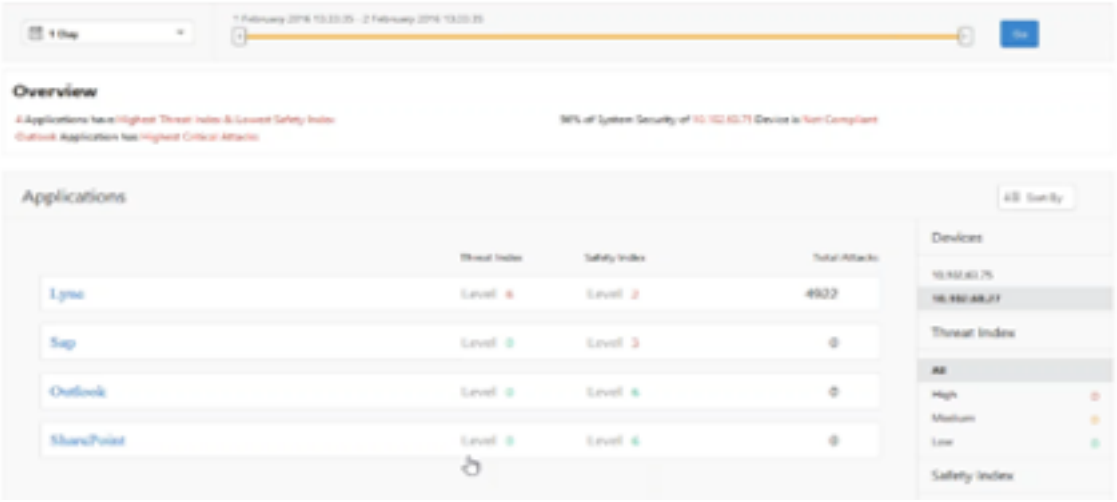
Navigieren Sie im **Security Insight-Dashboard**zu**Lync** > **Gesamtzahl der Verstöße**. Klicken Sie in der Tabelle Anwendungszusammenfassung auf die URL, um die vollständigen Details des Verstoßes auf der Seite**Informationen zur Verletzung**anzuzeigen, einschließlich des Namens des Protokollausdrucks, des Kommentars und der von der ADC-Instanz für die Aktion zurückgegebenen Werte.



Ermitteln Sie den Sicherheitsindex, bevor Sie die Konfiguration bereitstellen. Sicherheitsverletzungen treten auf, nachdem Benutzer die Sicherheitskonfiguration auf einer ADC-Instanz bereitgestellt haben. Benutzer möchten jedoch möglicherweise die Wirksamkeit der Sicherheitskonfiguration bewerten, bevor sie sie bereitstellen.

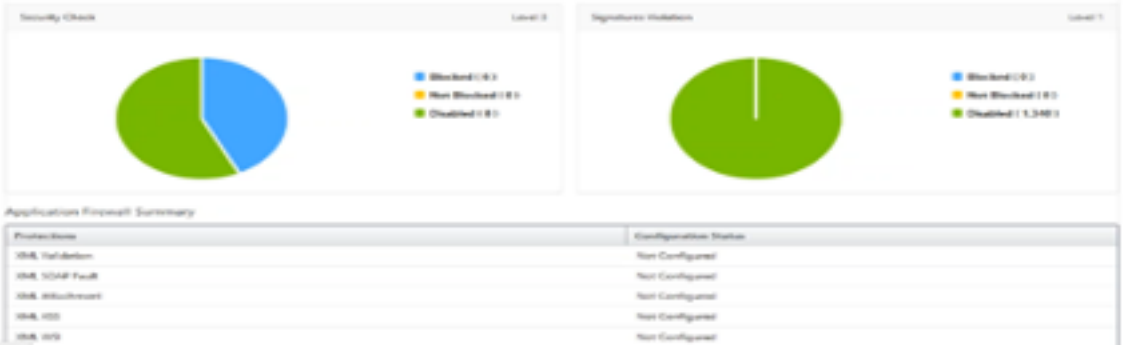
Beispielsweise möchten Benutzer möglicherweise den Sicherheitsindex der Konfiguration für die SAP-Anwendung auf der ADC-Instanz mit der IP-Adresse 10.102.60.27 bewerten.

Klicken Sie im**Security Insight Insight-Dashboard**unter**Geräte**auf die IP-Adresse der ADC-Instanz, die Benutzer konfiguriert haben. Benutzer können sehen, dass sowohl der Bedrohungsindex als auch die Gesamtzahl der Angriffe 0 sind. Der Bedrohungsindex spiegelt direkt die Anzahl und Art der Angriffe auf die Anwendung wider. Keine Angriffe bedeuten, dass die Anwendung keiner Bedrohung ausgesetzt ist.



Klicken Sie auf**SAP** > **Safety Index** > **SAP_Profile**und bewerten Sie die angezeigten Sicherheitsindex-informationen.

In der Zusammenfassung der Anwendungsfirewall können Benutzer den Konfigurationsstatus verschiedener Schutzeinstellungen einsehen. Wenn eine Einstellung auf Protokollierung gesetzt ist oder wenn eine Einstellung nicht konfiguriert ist, wird der Anwendung ein niedrigerer Sicherheitsindex zugewiesen.



Sicherheitsverstöße

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfällig für Angriffe geworden. Mit NetScaler ADM können Sie verwertbare Details zu Verstößen visualisieren, um Anwendungen vor Angriffen zu schützen.

Details zu Sicherheitsverletzungen bei Anwendungen anzeigen

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfälliger für Angriffe geworden. Mit NetScaler ADM können Benutzer umsetzbare Details zu Verstößen visualisieren, um Anwendungen vor Angriffen zu schützen. Navigieren Sie zu**Sicherheit**>**Sicherheitsverletzungen** für eine zentrale Lösung, um:

- Greifen Sie auf die Sicherheitsverletzungen der Anwendung basierend auf ihren Kategorien wie**Netzwerk**,**Bot**und**WAF**zu
- Ergreifen Sie Korrekturmaßnahmen, um die Anwendungen zu sichern

Um die Sicherheitsverletzungen in NetScaler ADM anzuzeigen, stellen Sie Folgendes sicher:

- Benutzer haben eine Premium-Lizenz für den NetScaler (für WAF- und BOT-Verstöße).
- Benutzer haben eine Lizenz für die virtuellen Load-Balancing- oder Content Switching-Server (für WAF und BOT) beantragt. Weitere Informationen finden Sie unter Lizenzierung auf virtuellen Servern verwalten.
- Benutzer können weitere Einstellungen aktivieren. Weitere Informationen finden Sie in dem Verfahren, das im Abschnitt Einrichtung der NetScaler-Produktdokumentation verfügbar ist: Einrichtung.

Kategorien von Verstößen

Mit NetScaler ADM können Benutzer die in All Violations verfügbaren Verstöße anzeigen:

einrichten

Stellen Sie bei Verstößen sicher, dass**Metrics Collector** aktiviert ist. Standardmäßig ist**Metrics Collector** auf dem NetScaler aktiviert. Weitere Informationen finden Sie unterIntelligent App Analytics konfigurieren.

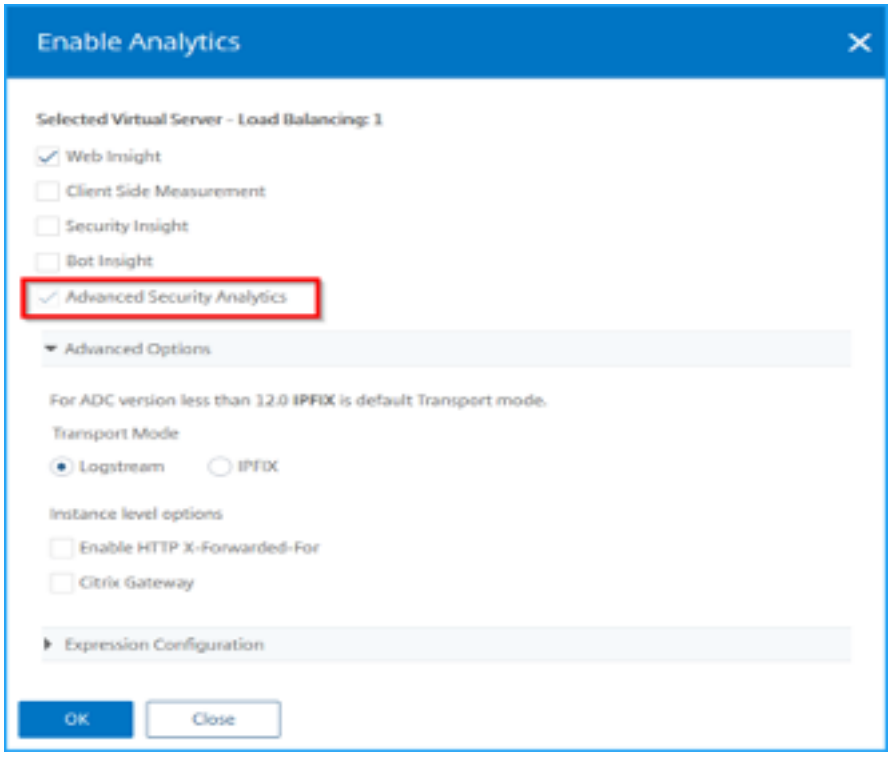
Ermöglichen Sie erweiterte Sicherheitsanalysen

- Navigieren Sie zu**Netzwerke**>**Instances**>**NetScaler**, und wählen Sie den Instanztyp aus. Zum Beispiel MPX.

- Wählen Sie die NetScaler-Instanz aus und wählen Sie in der Liste**Aktion auswählen** die Option Analytics**konfigurieren**aus.
- Wählen Sie den virtuellen Server aus und klicken Sie auf**Analytics aktivieren**.
- Gehen Sie im Fenster**Enable Analytics** wie folgt vor:
  - Wählen Sie**Web Insight**aus. Nachdem Benutzer Web Insight ausgewählt haben, wird die schreibgeschützte**Advanced Security Analytics-Option**automatisch aktiviert.

> **Hinweis:**
>
> Die Option**Advanced Security Analytics** wird nur für Premium-lizenzierte ADC-Instanzen angezeigt.

  - Wählen Sie**Logstream** als Transportmodus
  - Der Ausdruck ist standardmäßig wahr
  - Klicken Sie auf**OK**



Einstellungen für Web-Transaktionen aktivieren

- Navigieren Sie zu**Analytics**>**Einstellungen**.

Die Seite**Einstellungen**wird angezeigt.

- Klicken Sie auf**Funktionen für Analytics aktivieren**.

- Wählen Sie unter**Web-Transaktionseinstellungen**die Option**Alle**aus.

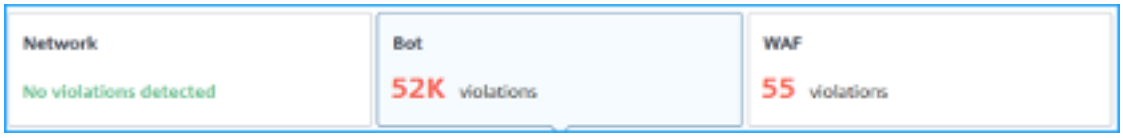
- Klicken Sie auf**Ok**.

Dashboard für Sicherheitsverletzungen

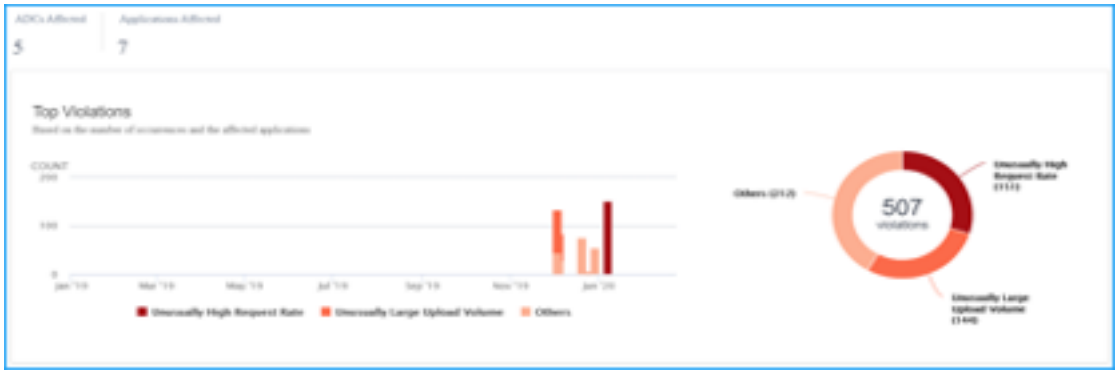
Im Dashboard für Sicherheitsverletzungen können Benutzer Folgendes einsehen:

- Die Gesamtzahl der Verstöße trat in allen NetScaler und Anwendungen auf. Die Gesamtzahl der Verstöße wird basierend auf der ausgewählten Zeitdauer angezeigt.

- Gesamtzahl der Verstöße in jeder Kategorie.



- Gesamtzahl der betroffenen ADCs, der Gesamtzahl der betroffenen Anwendungen und der häufigsten Verstöße, basierend auf der Gesamtzahl der Fälle und der betroffenen Anwendungen.



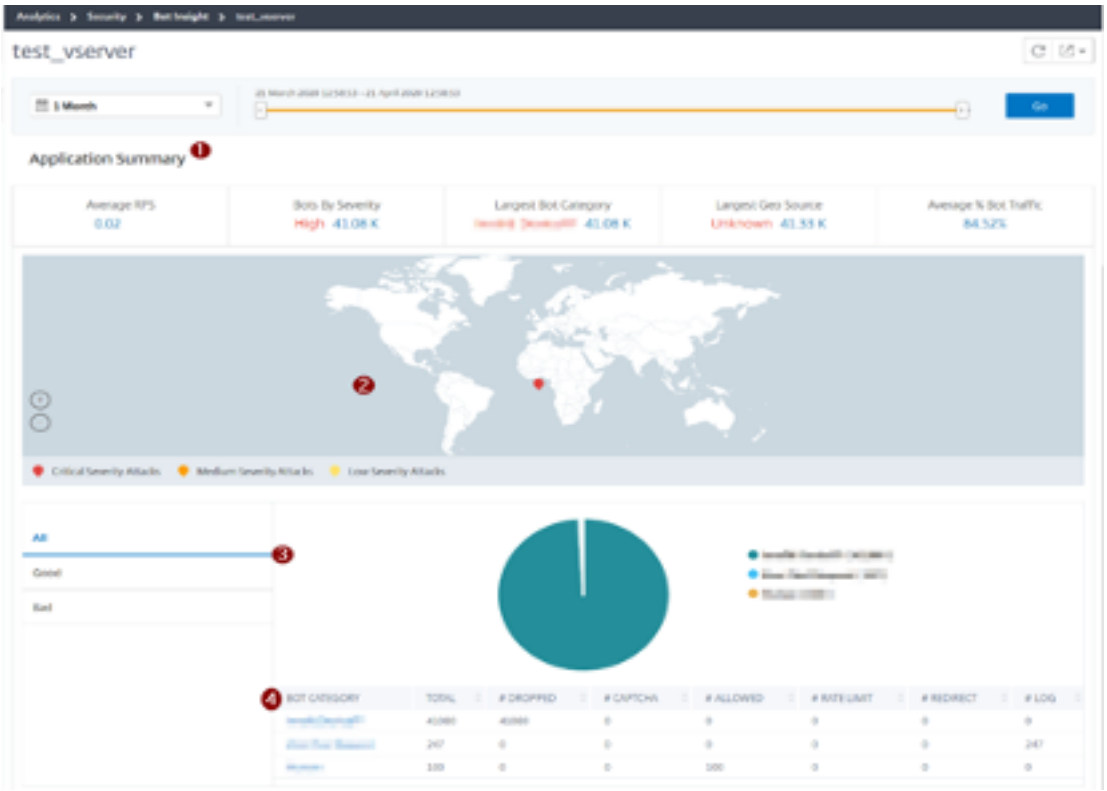
Weitere Informationen zu Verstößen finden Sie unter Alle Verstöße.

Bot-Einblick

Konfigurieren Sie BOT Insight in NetScaler. Weitere Informationen finden Sie unter Bot.

Bots ansehen

Klicken Sie auf den virtuellen Server, um die**Anwendungszusammenfassung**anzuzeigen



1. Enthält die Zusammenfassung der Anwendung, z. B.:

   - **Durchschnittlicher RPS**— Gibt die durchschnittlichen Bot-Transaktionsanforderungen pro Sekunde (RPS) an, die auf virtuellen Servern empfangen wurden.
   - **Bots nach Schweregrad**— Zeigt an, dass basierend auf dem Schweregrad die höchsten Bot-Transaktionen stattgefunden haben. Der Schweregrad wird basierend auf**Kritisch**,**Hoch**,**Mittel**und**Niedrig**kategorisiert.

   Wenn die virtuellen Server beispielsweise 11770 Bots mit hohem Schweregrad und 1550 Bots mit kritischem Schweregrad haben, zeigt NetScaler ADM unter**Bots nach SchweregradKritisch 1,55 K**an.

   - **Größte Bot-Kategorie** — Gibt an, dass basierend auf der Bot-Kategorie die meisten Bot-Angriffe stattgefunden haben.

   Wenn die virtuellen Server beispielsweise 8000 blockierte Bots, 5000 zugelassene Bots

und 10000 Rate Limit Exceeded haben, zeigt NetScaler ADM unter Größter Bot-Kategorie die Rate Limit Exceeded 10 K**an.**

- **Größte Geoquelle** — Gibt an, dass je nach Region die meisten Bot-Angriffe stattfanden.

Wenn die virtuellen Server beispielsweise 5000 Bot-Angriffe in Santa Clara, 7000 Bot-Angriffe in London und 9000 Bot-Angriffe in Bangalore haben, zeigt NetScaler ADM**Bangalore 9 K unter LargestGeo Source**an.

- **Durchschnittlicher% Bot-Traffic**— Gibt das menschliche Bot-Verhältnis an.

2. Zeigt den Schweregrad der Bot-Angriffe basierend auf Standorten in der Kartenansicht an
3. Zeigt die Arten von Bot-Angriffen an (Gut, Schlecht und alle)
4. Zeigt die Gesamtzahl der Bot-Angriffe zusammen mit den entsprechenden konfigurierten Aktionen an. Wenn Sie beispielsweise Folgendes konfiguriert haben:
   - IP-Adressbereich (192.140.14.9 bis 192.140.14.254) als Blocklisten-Bots und Auswahl von Löschen als Aktion für diese IP-Adressbereiche
   - IP-Bereich (192.140.15.4 bis 192.140.15.254) als Blocklisten-Bots und ausgewählt, um eine Protokollnachricht als Aktion für diese IP-Bereiche zu erstellen

     In diesem Szenario zeigt NetScaler ADM Folgendes an:

     - Gesamtzahl der blockierten Bots
     - Gesamtzahl Bots unter**Dropped**
     - Gesamtzahl der Bots im Log

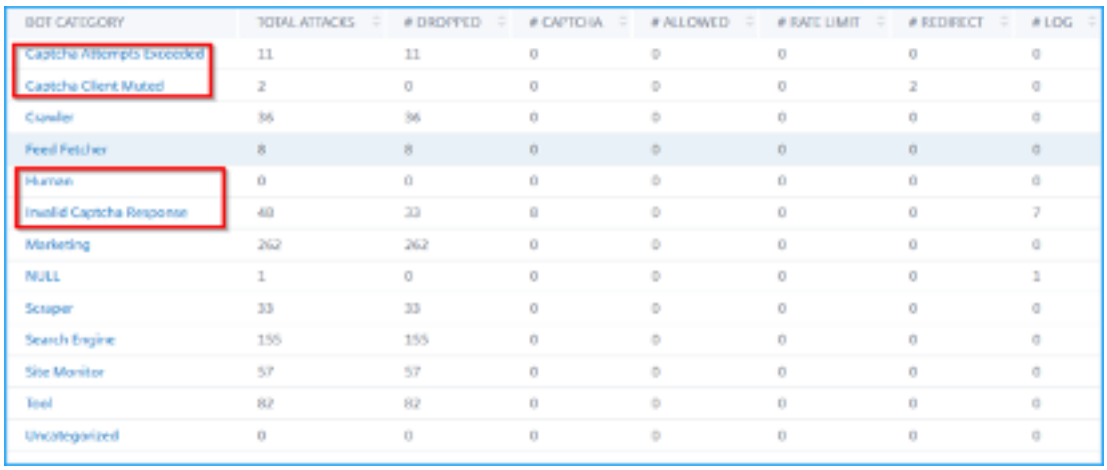
CAPTCHA-Bots ansehen

Auf Webseiten sollen CAPTCHAs erkennen, ob der eingehende Traffic von einem Menschen oder einem automatisierten Bot stammt. Um die CAPTCHA-Aktivitäten in NetScaler ADM anzuzeigen, müssen Benutzer CAPTCHA als Bot-Aktion für IP-Reputations- und Gerätefingerabdruckerkennungstechniken in einer NetScaler ADM-Instanz konfigurieren. Weitere Informationen finden Sie unterBot-Management konfigurieren.

Im Folgenden sind die CAPTCHA-Aktivitäten aufgeführt, die NetScaler ADM in Bot Insight anzeigt:

- **Captcha-Versuche überschritten**— Gibt die maximale Anzahl von CAPTCHA-Versuchen nach Anmeldefehlern an
- **Captcha-Client stummgeschaltet**— Gibt die Anzahl der Client-Anfragen an, die verworfen oder umgeleitet wurden, da diese Anfragen zuvor mit der CAPTCHA-Herausforderung als fehlerhafte Bots erkannt wurden

- **Human**— Bezeichnet die Captcha-Einträge, die von den menschlichen Benutzern durchgeführt wurden
- **Ungültige Captcha-Antwort**— Gibt die Anzahl der falschen CAPTCHA-Antworten an, die vom Bot oder Menschen empfangen wurden, wenn NetScaler eine CAPTCHA-Herausforderung sendet

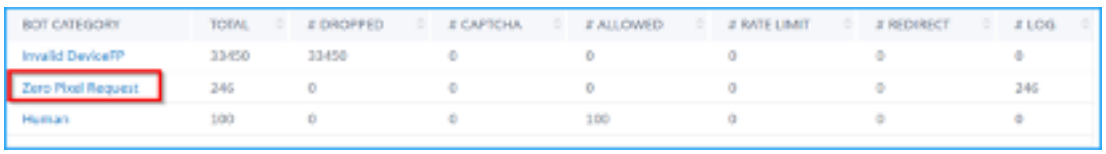


Botfallen ansehen

Um Bot-Traps in NetScaler ADM anzuzeigen, müssen Sie den Bot-Trap in NetScaler konfigurieren. Weitere Informationen finden Sie unterBot-Management konfigurieren.

Um die Botfalle zu identifizieren, ist auf der Webseite ein Skript aktiviert, das vor Menschen verborgen ist, aber nicht vor Bots. NetScaler ADM identifiziert und meldet die Bot-Traps, wenn die Bots auf dieses Skript zugreifen.

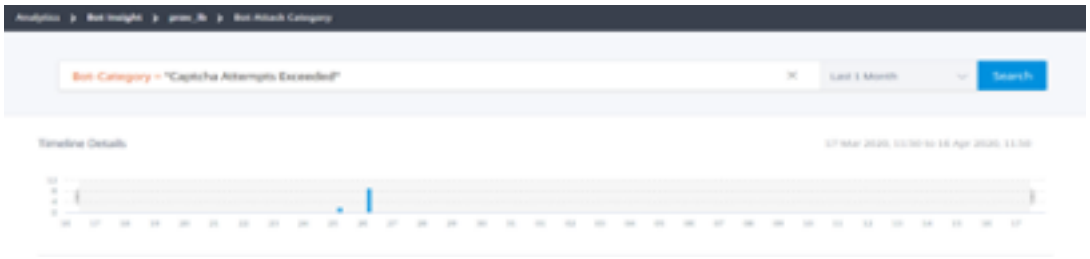
Klicken Sie auf den virtuellen Server und wählen Sie**Null Pixel Request**



Bot-Details anzeigen

Weitere Informationen erhalten Sie, indem Sie unter**Bot-Kategorie auf den Bot-Angriffstyp**klicken.

Die Details wie Angriffszeit und Gesamtzahl der Bot-Angriffe für die ausgewählte Captcha-Kategorie werden angezeigt.



Benutzer können das Balkendiagramm auch ziehen, um den spezifischen Zeitraum auszuwählen, der bei Bot-Angriffen angezeigt werden soll.

Um weitere Informationen zum Bot-Angriff zu erhalten, klicken Sie zum Erweitern.

- **Instanz-IP** — Gibt die IP-Adresse der NetScaler-Instanz an.
- **Gesamtzahl der Bots** — Gibt an, dass die Gesamtzahl der Bot-Angriffe für diesen bestimmten Zeitraum stattgefunden hat.
- **HTTP-Anforderungs-URL** — Gibt die URL an, die für Captcha-Berichte konfiguriert ist.
- **Landesvorwahl** — Gibt das Land an, in dem der Bot-Angriff stattgefunden hat.
- **Region** — Gibt die Region an, in der der Bot-Angriff stattgefunden hat.
- **Profilname** — Gibt den Profilnamen an, den Benutzer bei der Konfiguration angegeben haben.

Erweiterte Suche

Benutzer können auch das Suchtextfeld und die Zeitdauerliste verwenden, wo sie Bot-Details gemäß den Benutzeranforderungen anzeigen können. Wenn Benutzer auf das Suchfeld klicken, erhalten sie im Suchfeld die folgende Liste mit Suchvorschlägen.

- **Instanz-IP — IP-Adresse**der NetScaler-Instanz.
- **Client-IP** — Client-IP-Adresse.
- **Bot-Typ** — Bot-Typ wie Gut oder Schlecht.
- **Schweregrad**— Schweregrad des Bot-Angriffs.
- Aktion**ergriffen —**Maßnahmen , die nach dem Bot-Angriff ergriffen wurden, z. B. Drop, Keine Aktion, Redirect.
- **Bot-Kategorie** — Kategorie des Bot-Angriffs wie Blockliste, Zulassungsliste, Fingerabdruck. Basierend auf einer Kategorie können Benutzer ihr eine Bot-Aktion zuordnen.
- **Bot-Detection** — Bot-Erkennungstypen (Blockliste, Zulassungsliste usw.), die Benutzer auf NetScaler konfiguriert haben.
- **Standort** — Region/Land, in dem der Bot-Angriff stattgefunden hat
- **Request-url — URL**, die die möglichen Bot-Angriffe enthält

Benutzer können in den Benutzersuchabfragen auch Operatoren verwenden, um den Fokus der Benutzersuche einzugrenzen. Zum Beispiel, wenn Benutzer alle bösartigen Bots sehen möchten:

- Klicken Sie auf das Suchfeld und wählen Sie**Bot-Type**
- Klicken Sie erneut auf das Suchfeld und wählen Sie den Operator**=**
- Klicken Sie erneut auf das Suchfeld und wählen Sie**Schlecht**
- Klicken Sie auf**Suchen**, um die Ergebnisse anzuzeigen

Ungewöhnlich hohe Anfragerate

Benutzer können den eingehenden und ausgehenden Verkehr von oder zu einer Anwendung steuern. Ein Bot-Angriff kann eine ungewöhnlich hohe Anforderungsrate verursachen. Wenn Benutzer beispielsweise eine Anwendung so konfigurieren, dass sie 100 Anfragen pro Minute zulässt, und wenn Benutzer 350 Anfragen beobachten, handelt es sich möglicherweise um einen Bot-Angriff.

Mithilfe des Indikators**Ungewöhnlich hohe Anforderungsrate**können Benutzer die ungewöhnliche Anforderungsrate analysieren, die an die Anwendung eingegangen ist.

Unter**Veranstaltungsdetails**können Benutzer Folgendes anzeigen:

- Die betroffene Anwendung. Benutzer können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von Verstößen betroffen sind.
- Die Grafik zeigt alle Verstöße
- Zeitpunkt des Auftretens des Verstoßes
- Die Erkennungsmeldung für den Verstoß, in der die Gesamtzahl der eingegangenen Anfragen und der Prozentsatz der eingegangenen Anfragen angegeben sind, die über den erwarteten Anforderungen liegen
- Der akzeptierte Bereich der erwarteten Anforderungsraten reicht von der Anwendung ab

Bot-Erkennung

Das NetScaler Bot-Managementsystem verwendet verschiedene Techniken, um den eingehenden Bot-Verkehr zu erkennen. Die Techniken werden als Erkennungsregeln verwendet, um den Bot-Typ zu erkennen.

Konfiguration des Bot-Managements mithilfe der GUI

Benutzer können das NetScaler-Bot-Management konfigurieren, indem sie zuerst die Funktion auf der Appliance aktivieren. Weitere Informationen finden Sie unter Bot-Erkennung.

IP-Reputation

IP-Reputation ist ein Tool, das IP-Adressen identifiziert, die unerwünschte Anfragen senden. Mithilfe der IP-Reputationsliste können Sie Anfragen ablehnen, die von einer IP-Adresse mit einem schlechten Ruf kommen.

IP-Reputation mithilfe der GUI konfigurieren

Diese Konfiguration ist eine Voraussetzung für die Bot-IP-Reputationsfunktion. Weitere Informationen finden Sie unter IP-Reputation.

Automatisches Update für Bot-Signaturen

Die statische Bot-Signaturtechnik verwendet eine Signatur-Suchtabelle mit einer Liste guter und schlechter Bots. Weitere Informationen finden Sie unter Automatisches Signaturupdate.

Die zehn besten Adressen von NetScaler Web App Firewall und OWASP — 2021

Das Open Web Application Security Project (OWAP) hat die OWASP Top 10 für 2021 für die Sicherheit von Webanwendungen veröffentlicht. Diese Liste dokumentiert die häufigsten Sicherheitslücken in Webanwendungen und ist ein guter Ausgangspunkt für die Bewertung der Websicherheit. In diesem Abschnitt wird erklärt, wie Sie die NetScaler Web App Firewall konfigurieren, um diese Fehler zu beheben. WAF ist als integriertes Modul in NetScaler (Premium Edition) und einer kompletten Palette von Appliances verfügbar.

Das vollständige OWASP Top 10-Dokument ist unter OWASPTop Ten verfügbar.

Die 10 besten OWASP 2021	Funktionen der NetScaler Web App Firewall
A 1:2021 Kaputte Zugangskontrolle	AAA, Autorisierungssicherheitsfunktionen im AAA-Modul von NetScaler, Formularschutz und Cookie-Manipulationsschutz, StartUrl und ClosureUrl
A 2:2021 - Kryptografische Fehler	Kreditkartenschutz, Safe Commerce, Cookie-Proxying und Cookie-Verschlüsselung
A 3:2021 - Injektion	Verhinderung von Injektionsangriffen (SQL oder andere benutzerdefinierte Injektionen wie OS Command Injection, XPath Injection und LDAP-Injection), Signaturfunktion zur automatischen Aktualisierung

Die 10 besten OWASP 2021	Funktionen der NetScaler Web App Firewall
A 5:2021 Fehlkonfiguration der Sicherheit	Dieser Schutz umfasst WSI-Prüfungen, XML-Nachrichtenvalidierung und XML-SOAP-Fehlerfilterprüfung
A 6:2021 — Sicherheitslücke und veraltete Komponenten	Berichte über Sicherheitslücken, Vorlagen für die Anwendungs-Firewall und benutzerdefinierte Signaturen
A 7:2021 — Fehler bei Identifizierung und Authentifizierung	AAA, Schutz vor Cookie-Manipulation, Cookie-Proxying, Cookie-Verschlüsselung, CSRF-Tagging, SSL verwenden
A 8:2021 — Fehler bei der Software- und Datenintegrität	XML-Sicherheitsprüfungen, GWT-Inhaltstyp, benutzerdefinierte Signaturen, Xpath für JSON und XML
A 9:2021 — Fehler bei der Sicherheitsprotokollierung und Überwachung	Benutzerkonfigurierbares benutzerdefiniertes Protokollierungs-, Verwaltungs- und Analysesystem

A 1:2021 Kaputte Zugangskontrolle

Einschränkungen dessen, was authentifizierte Benutzer tun dürfen, werden oft nicht ordnungsgemäß durchgesetzt. Angreifer können diese Sicherheitslücken ausnutzen, um auf nicht autorisierte Funktionen und Daten zuzugreifen, z. B. auf Konten anderer Benutzer zuzugreifen, vertrauliche Dateien einzusehen, Daten anderer Benutzer zu ändern und Zugriffsrechte zu ändern.

NetScaler Web App Firewall-Schutzmaßnahmen

- Die AAA-Funktion, die Authentifizierung, Autorisierung und Prüfung für den gesamten Anwendungsverkehr unterstützt, ermöglicht es einem Site-Administrator, die Zugriffskontrollen mit der ADC-Appliance zu verwalten.
- Die Sicherheitsfunktion Autorisierung im AAA-Modul der ADC-Appliance ermöglicht es der Appliance, zu überprüfen, auf welche Inhalte auf einem geschützten Server sie jedem Benutzer Zugriff gewähren soll.
- Konsistenz von Formularfeldern: Wenn Objektreferenzen als versteckte Felder in Formularen gespeichert werden, können Sie mithilfe der Konsistenz von Formularfeldern überprüfen, ob diese Felder bei nachfolgenden Anfragen nicht manipuliert werden.

- Cookie-Proxying und Cookie-Konsistenz: Objektreferenzen, die in Cookie-Werten gespeichert sind, können mit diesen Schutzmaßnahmen validiert werden.
- URL-Prüfung mit URL-Schließung starten: Ermöglicht Benutzern den Zugriff auf eine vordefinierte Zulassungsliste von URLs. Die URL-Schließung erstellt eine Liste aller URLs, die während der Benutzersitzung in gültigen Antworten gesehen wurden, und ermöglicht automatisch den Zugriff darauf während dieser Sitzung.

A 2:2021 - Kryptografische Fehler

Viele Webanwendungen und APIs schützen sensible Daten wie Finanzen, Gesundheitswesen und personenbezogene Daten nicht ordnungsgemäß. Angreifer können solche schlecht geschützten Daten stehlen oder ändern, um Kreditkartenbetrug, Identitätsdiebstahl oder andere Verbrechen zu begehen. Sensible Daten können ohne zusätzlichen Schutz, z. B. Verschlüsselung im Ruhezustand oder bei der Übertragung, gefährdet werden und erfordern besondere Vorsichtsmaßnahmen, wenn sie mit dem Browser ausgetauscht werden.

NetScaler Web App Firewall-Schutzmaßnahmen

- Die Web Application Firewall schützt Anwendungen davor, sensible Daten wie Kreditkartendaten preiszugeben.
- Sensible Daten können im Safe Commerce-Schutz als sichere Objekte konfiguriert werden, um eine Offenlegung zu vermeiden.
- Alle sensiblen Daten in Cookies können durch Cookie-Proxying und Cookie-Verschlüsselung geschützt werden.

A 3:2021 - Injektion

Injektionsfehler wie SQL-, NoSQL-, OS- und LDAP-Injection treten auf, wenn nicht vertrauenswürdige Daten als Teil eines Befehls oder einer Abfrage an einen Interpreter gesendet werden. Die feindlichen Daten des Angreifers können den Interpreter dazu verleiten, unbeabsichtigte Befehle auszuführen oder ohne entsprechende Autorisierung auf Daten zuzugreifen.

XSS-Fehler treten auf, wenn eine Anwendung nicht vertrauenswürdige Daten ohne ordnungsgemäße Validierung oder Escaping in eine neue Webseite einfügt oder eine bestehende Webseite mithilfe einer Browser-API, die HTML oder JavaScript erstellen kann, mit vom Benutzer bereitgestellten Daten aktualisiert. XSS ermöglicht es Angreifern, Skripte im Browser des Opfers auszuführen, die Benutzersitzungen kapern, Websites verunstalten oder den Benutzer auf bösartige Websites umleiten können.

NetScaler Web App Firewall-Schutzmaßnahmen

- Die Funktion zur Verhinderung von SQL-Injection schützt vor häufigen Injection-Angriffen. Zum Schutz vor jeder Art von Injektionsangriffen, einschließlich XPath und LDAP, können benutzerdefinierte Injektionsmuster hochgeladen werden. Dies gilt sowohl für HTML- als auch für XML-Nutzlasten.
- Die Funktion zur automatischen Aktualisierung der Signatur hält die Injektionssignaturen auf dem neuesten Stand.
- Die Funktion zum Schutz von Feldformaten ermöglicht es dem Administrator, jeden Benutzerparameter auf einen regulären Ausdruck zu beschränken. Sie können beispielsweise erzwingen, dass ein PLZ-Feld nur ganze Zahlen oder sogar fünfstellige Ganzzahlen enthält.
- Die Konsistenz von Formularfeldern überprüft jedes übermittelte Benutzerformular anhand der Signatur des Benutzersitzungsformulars, um die Gültigkeit aller Formularelemente sicherzustellen.
- Pufferüberlaufprüfungen stellen sicher, dass die URL, Header und Cookies in den richtigen Grenzwerten sind, sodass Versuche, große Skripts oder Code einzufügen, blockiert werden.
- Der XSS-Schutz schützt vor gängigen XSS-Angriffen. Benutzerdefinierte XSS-Muster können hochgeladen werden, um die Standardliste der zulässigen Tags und Attribute zu ändern. Die ADC WAF verwendet eine weiße Liste zulässiger HTML-Attribute und -Tags, um XSS-Angriffe zu erkennen. Dies gilt sowohl für HTML- als auch für XML-Nutzlasten.
- ADC WAF blockiert alle Angriffe, die im OWASP XSS Filter Evaluation Cheat Sheet aufgeführt sind.
- Die Feldformatprüfung verhindert, dass ein Angreifer unangemessene Webformulardaten sendet, was ein potenzieller XSS-Angriff sein kann.
- Konsistenz von Formularfeldern.

A 5:2021 — Fehlkonfiguration der Sicherheit

Eine Fehlkonfiguration der Sicherheit ist das am häufigsten auftretende Problem. Dies ist häufig auf unsichere Standardkonfigurationen, unvollständige oder improvisierte Konfigurationen, offenen Cloud-Speicher, falsch konfigurierte HTTP-Header und ausführliche Fehlermeldungen mit vertraulichen Informationen zurückzuführen. Alle Betriebssysteme, Frameworks, Bibliotheken und Anwendungen müssen nicht nur sicher konfiguriert sein, sondern sie müssen auch rechtzeitig gepatcht und aktualisiert werden.

Viele ältere oder schlecht konfigurierte XML-Prozessoren werten externe Entitätsreferenzen in XML-Dokumenten aus. Externe Entitäten können verwendet werden, um interne Dateien mithilfe des Datei-URI-Handlers, interner Dateifreigaben, interner Portscans, Remotecodeausführung und Denial-of-Service-Angriffe offenzulegen.

NetScaler Web App Firewall-Schutzmaßnahmen

- Der von der Application Firewall generierte PCI-DSS-Bericht dokumentiert die Sicherheitseinstellungen auf dem Firewall-Gerät.
- Berichte der Scan-Tools werden in ADC-WAF-Signaturen konvertiert, um Sicherheitsfehlkonfigurationen zu behandeln.
- Die NetScaler Web App Firewall Web Application Firewall unterstützt Cenzic, IBM AppScan (Enterprise und Standard), Qualys, TrendMicro, WhiteHat und benutzerdefinierte Schwachstellen-Scan-Berichte.
- Zusätzlich zur Erkennung und Blockierung gängiger Anwendungsbedrohungen, die für Angriffe auf XML-basierte Anwendungen (d. h. Cross-Site Scripting, Befehlsinjektion usw.) angepasst werden können.
- Die NetScaler Web App Firewall Web Application Firewall umfasst eine Vielzahl von XML-spezifischen Sicherheitsvorkehrungen. Dazu gehören die Schemavalidierung zur gründlichen Überprüfung von SOAP-Nachrichten und XML-Payloads sowie eine leistungsstarke Prüfung von XML-Anhängen zum Blockieren von Anhängen, die schädliche ausführbare Dateien oder Viren enthalten.
- Automatische Methoden zur Überprüfung des Datenverkehrs blockieren XPath-Injection-Angriffe auf URLs und Formulare, die darauf abzielen, Zugriff zu erlangen.
- Die NetScaler Web App Firewall Web Application Firewall vereitelt auch verschiedene DoS-Angriffe, darunter externe Entitätsverweise, rekursive Expansion, übermäßige Verschachtelung und bösartige Nachrichten, die entweder lange oder viele Attribute und Elemente enthalten.

A 6:2021 — Anfällige und veraltete Komponenten

Komponenten wie Bibliotheken, Frameworks und andere Softwaremodule werden mit denselben Rechten wie die Anwendung ausgeführt. Wenn eine anfällige Komponente ausgenutzt wird, kann ein solcher Angriff zu schwerwiegenden Datenverlusten oder Serverübernahmen führen. Anwendungen und APIs, die Komponenten mit bekannten Sicherheitslücken verwenden, können die Anwendungsabwehr untergraben und verschiedene Angriffe und Auswirkungen ermöglichen.

NetScaler Web App Firewall-Schutzmaßnahmen

- Wir empfehlen, die Komponenten von Drittanbietern auf dem neuesten Stand zu halten.
- Sicherheitslücken-Scan-Berichte, die in ADC-Signaturen umgewandelt werden, können verwendet werden, um diese Komponenten virtuell zu patchen.
- Anwendungsfirewall-Vorlagen, die für diese anfälligen Komponenten verfügbar sind, können verwendet werden.

- Benutzerdefinierte Signaturen können an die Firewall gebunden werden, um diese Komponenten zu schützen.

A 7:2021 — Fehlerhafte Authentifizierung

Anwendungsfunktionen im Zusammenhang mit Authentifizierung und Sitzungsmanagement werden häufig falsch implementiert, sodass Angreifer Passwörter, Schlüssel oder Sitzungstoken kompromittieren oder andere Implementierungsfehler ausnutzen können, um vorübergehend oder dauerhaft die Identitäten anderer Benutzer anzunehmen.

NetScaler Web App Firewall-Schutzmaßnahmen

- Das NetScaler AAA-Modul führt die Benutzerauthentifizierung durch und bietet Single Sign-On-Funktionalität für Back-End-Anwendungen. Dies ist in die NetScaler AppExpert Policy-Engine integriert, um benutzerdefinierte Richtlinien auf der Grundlage von Benutzer- und Gruppeninformationen zu ermöglichen.
- Mithilfe von SSL-Offloading- und URL-Transformationsfunktionen kann die Firewall Websites auch dabei unterstützen, sichere Transportschichtprotokolle zu verwenden, um den Diebstahl von Sitzungstoken durch Netzwerk-Sniffing zu verhindern.
- Cookie-Proxying und Cookie-Verschlüsselung können eingesetzt werden, um den Diebstahl von Cookies vollständig zu verhindern.

A 8:2021 — Fehler bei der Software- und Datenintegrität

Eine unsichere Deserialisierung führt häufig zur Ausführung von Code aus der Ferne. Auch wenn Deserialisierungsfehler nicht zur Remotecodeausführung führen, können sie für Angriffe verwendet werden, darunter Replay-Angriffe, Injection-Angriffe und Angriffe zur Rechteeskalation.

NetScaler Web App Firewall-Schutzmaßnahmen

- JSON-Nutzlastinspektion mit benutzerdefinierten Signaturen.
- XML-Sicherheit: schützt vor XML Denial of Service (XDoS), XML SQL und Xpath Injection und Cross-Site Scripting, Formatprüfungen, Einhaltung von WS-I-Grundprofilen und Überprüfung von XML-Anhängen.
- Feldformatprüfungen sowie Cookie-Konsistenz und Feldkonsistenz können verwendet werden.

A 9:2021 — Fehler bei der Sicherheitsprotokollierung und Überwachung

Eine unzureichende Protokollierung und Überwachung in Verbindung mit einer fehlenden oder ineffektiven Integration in die Reaktion auf Vorfälle ermöglichen es Angreifern, Systeme weiter anzugreifen, ihre Persistenz aufrechtzuerhalten, auf mehr Systeme umzusteigen und Daten zu manipulieren, zu extrahieren oder zu zerstören. Die meisten Studien zeigen, dass die Zeit bis zur Entdeckung eines Verstoßes über 200 Tage beträgt, was in der Regel eher von externen Parteien als von internen Prozessen oder Überwachungen erkannt wird.

NetScaler Web App Firewall-Schutzmaßnahmen

- Wenn die Protokollaktion für Sicherheitsprüfungen oder Signaturen aktiviert ist, enthalten die resultierenden Protokollmeldungen Informationen über die Anfragen und Antworten, die die Anwendungsfirewall beim Schutz Ihrer Websites und Anwendungen beobachtet hat.
- Die Anwendungsfirewall bietet den Komfort, die integrierte ADC-Datenbank zu verwenden, um die Standorte zu identifizieren, die den IP-Adressen entsprechen, von denen bösartige Anfragen stammen.
- Ausdrücke im Standardformat (PI) bieten die Flexibilität, die in den Protokollen enthaltenen Informationen anzupassen, wobei die Option besteht, die spezifischen Daten hinzuzufügen, die in den von der Anwendungs-Firewall generierten Protokollmeldungen erfasst werden sollen.
- Die Anwendungsfirewall unterstützt CEF-Protokolle.

Referenzen

- HTML-SQL-Injektionsprüfung
- XML-SQL-Injektionsprüfung
- Den HTML Cross-Site Scripting Check über die Befehlszeile konfigurieren
- Siteübergreifende XML-Skriptprüfung
- Verwenden der Befehlszeile zur Konfiguration der Sicherheitsüberprüfung für den Pufferüberlauf
- Signaturobjekt hinzufügen oder entfernen
- Konfiguration oder Änderung eines Signature-Objekts
- Aktualisierung eines Signaturobjekts
- Integration von Snort-Regeln
- Bot-Erkennung
- Bereitstellen einer NetScaler VPX Instanz unter Microsoft Azure

URL-Schutzüberprüfungen

January 19, 2021

Der URL-Schutz prüft Anforderungs-URLs, um zu verhindern, dass Angreifer aggressiv versuchen, auf mehrere URLs zuzugreifen (kraftvolles Surfen) oder mithilfe einer URL eine bekannte Sicherheitslücke in Webserversoftware oder Website-Skripten auszulösen.

URL-Prüfung starten

August 19, 2021

Die Start-URL-Prüfung untersucht die URLs in eingehenden Anforderungen und blockiert den Verbindungsversuch, wenn die URL die angegebenen Kriterien nicht erfüllt. Um die Kriterien zu erfüllen, muss die URL mit einem Eintrag in der Liste Start-URL übereinstimmen, es sei denn, der Parameter URL-Schließung erzwingen ist aktiviert. Wenn Sie diesen Parameter aktivieren, ist ein Benutzer, der auf einen Link auf Ihrer Website klickt, mit dem Ziel dieses Links verbunden.

Der Hauptzweck der Start-URL-Prüfung besteht darin, wiederholte Versuche zu verhindern, auf zufällige URLs auf einer Website zuzugreifen (kraftvolles Surfen) durch Lesezeichen, externe Links oder das Springen zu Seiten, indem die URLs manuell eingegeben werden, um diesen Teil der Website zu erreichen. Erzwungenes Browsen kann verwendet werden, um einen Pufferüberlauf auszulösen, Inhalte zu finden, auf die Benutzer nicht direkt zugreifen sollen, oder eine Hintertür in sicheren Bereichen Ihres Webservers zu finden. Die Web App Firewall erzwingt den angegebenen Traversal- oder Logikpfad einer Website, indem nur Zugriff auf die URLs gewährt wird, die als Start-URLs konfiguriert sind.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Start URL Check ändern auf der Registerkarte Allgemein Sperren, Protokollieren, Statistiken, Lernaktionen und die folgenden Parameter aktivieren oder deaktivieren:

- **URL-Schließung erzwingen.** Ermöglichen Sie Benutzern den Zugriff auf jede Webseite Ihrer Website, indem Sie auf einen Hyperlink auf einer anderen Seite Ihrer Website klicken. Benutzer können zu jeder Seite Ihrer Website navigieren, die von der Startseite oder einer bestimmten Startseite aus erreicht werden kann, indem sie auf Hyperlinks klicken.
  Hinweis: Die URL-Schließfunktion ermöglicht es, jede Abfragezeichenfolge anzuhängen und mit der Aktion-URL eines Webformulars zu senden, das mit der HTTP-GET-Methode gesendet wird. Wenn Ihre geschützten Websites Formulare für den Zugriff auf eine SQL-Datenbank verwenden, stellen Sie sicher, dass Sie die SQL-Injection-Prüfung aktiviert und ordnungsgemäß konfiguriert haben.
- **Sitzungsloser URL-Abschluss.** Aus Sicht des Kunden funktioniert diese Art von URL-Schließung genauso wie die standardmäßige, sitzungsbewusste URL-Schließung, verwendet

aber ein in die URL eingebettetes Token anstelle eines Cookies, um die Aktivität des Benutzers zu verfolgen, was deutlich weniger Ressourcen verbraucht. Wenn sitzungslose URL-Schließung aktiviert ist, hängt die Web App Firewall ein as_url_id -Tag an alle URLs, die sich im URL-Abschluss befinden.

Hinweis: Wenn Sie sessionless (Sessionless URL Closure) aktivieren, müssen Sie auch den regulären URL-Closure aktivieren (URL-Closure
erzwingen), oder der sitzungslose URL-Closure funktioniert nicht.

- **Referer-Header validieren.** Stellen Sie sicher, dass der Referer-Header in einer Anfrage, die Webformulardaten von Ihrer geschützten Website anstelle einer anderen Website enthält. Diese Aktion überprüft, ob Ihre Website, kein externer Angreifer, die Quelle des Webformulars ist. Dadurch wird vor Cross-Site Request Forgeries (CSRF) geschützt, ohne dass Formular-Tagging erforderlich ist, was CPU-intensiver ist als Header-Prüfungen. Die Web App Firewall kann den HTTP-Referer-Header auf eine der folgenden vier Arten verarbeiten, je nachdem, welche Option Sie in der Dropdownliste auswählen:
  - **Off**— Validieren Sie den Referer-Header nicht.
  - **If-Present**—Validieren Sie den Referer-Header, wenn ein Referer-Header vorhanden ist. Wenn ein ungültiger Referer-Header gefunden wird, generiert die Anforderung eine Referer-Header-Verletzung. Wenn kein Referer-Header vorhanden ist, generiert die Anforderung keine Verweis-Header-Verletzung. Mit dieser Option kann die Web App Firewall Referer-Header-Validierung für Anforderungen durchführen, die einen Referer-Header enthalten, aber keine Anforderungen von Benutzern blockieren, deren Browser den Referer-Header nicht festlegen oder Webproxys oder Filter verwenden, die diesen Header entfernen.
  - **Always außer Start-URLs**—Validieren Sie den Referer-Header immer. Wenn kein Referer-Header vorhanden ist und die angeforderte URL nicht von der StartURL-Relaxationsregel ausgenommen wird, generiert die Anforderung eine Referer-Header-Verletzung. Wenn der Referer-Header vorhanden ist, aber ungültig ist, generiert die Anforderung eine Referer-Header-Verletzung.
  - **Always Except First Request**— Validieren Sie immer den Referer-Header. Wenn kein Referer-Header vorhanden ist, ist nur die URL zulässig, auf die zuerst zugegriffen wird. Alle anderen URLs sind ohne gültige Referer-Header gesperrt. Wenn der Referer-Header vorhanden ist, aber ungültig ist, generiert die Anforderung eine Referer-Header-Verletzung.

Eine Start-URL-Einstellung, **Closure URLs von Sicherheitsprüfungen**ausschließen, wird nicht im Dialogfeld Start URL Check ändern konfiguriert, sondern auf der Registerkarte Einstellungen des Profils konfiguriert. Wenn diese Einstellung aktiviert ist, weist die Web App Firewall darauf hin, keine weiteren formularbasierten Prüfungen (wie Cross-Site Scripting und SQL Injection-Prüfung) für URLs durchzuführen, die die URL-Schließungskriterien erfüllen.

> **Hinweis:**
>
> Obwohl die Referer-Header-Prüfung und die Start-URL-Sicherheitsprüfung dieselben Aktionseinstellungen verwenden, ist es möglich, die Referer-Header-Prüfung zu verletzen, ohne die Start-URL-Prüfung zu verletzen. Der Unterschied ist in den Protokollen sichtbar, die Verweiskopfverletzungen getrennt von Start-URL-Überprüfungsverletzungen protokollieren.

Die Referer-Header-Einstellungen (OFF, IF-Present, AlwaysExceptStartUrls und AlwaysExceptFirstRequest) sind in der Reihenfolge der am wenigsten restriktiven angeordnet und funktionieren wie folgt:

OFF:

- Referer Header wird nicht geprüft.

Wenn vorhanden:

- Anfrage hat keinen Referer-Header -> Anfrage ist erlaubt.
- Anfrage hat Referer-Header und die Referer-URL ist in URL-Schließung -> Anfrage ist erlaubt.
- Anfrage hat Referer-Header und die Referer-URL ist **nicht** in URL-Schließung -> Anfrage ist blockiert.

AlwaysExceptStartURLs:

- Anfrage hat keinen Referer-Header und die Anforderungs-URL ist eine Start-URL -> Anfrage ist erlaubt.
- Anfrage hat keinen Referer-Header und die Anforderungs-URL ist keine Start-URL ->Anforderung ist blockiert.
- Anfrage hat Referer-Header und die Referer-URL ist in URL-Schließung -> Anfrage ist erlaubt.
- Anfrage hat Referer-Header und die Referer-URL ist **nicht** in URL-Schließung -> Anfrage ist blockiert.

AlwaysExceptFirstRequest:

- Anfrage hat keinen Referer-Header und ist die erste Anforderungs-URL der Sitzung -> Anfrage ist erlaubt.
- Anfrage hat keinen Referer-Header und ist **nicht** die erste Anforderungs-URL der Sitzung -> Anfrage ist blockiert.
- Anfrage hat Referer-Header und ist entweder die erste Anforderungs-URL der Sitzung oder ist in URL-Schließung -> Anfrage ist erlaubt.
- Request hat Referer-Header und ist weder die erste Anforderungs-URL der Sitzung noch befindet sich in URL-Schließung -> Anfrage ist blockiert.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um die Start-URL-Prüfung zu konfigurieren:

- `set appfw profile <name> -startURLAction [block] [learn] [log] [stats] [none]`

- set appfw profile <name> -startURLClosure ([ON] | [OFF])
- set appfw profile <name> -sessionlessURLClosure ([ON] | [OFF])
- set appfw profile <name> -exemptClosureURLsFromSecurityChecks ([ON] | [OFF)
- set appfw profile <name> -RefererHeaderCheck ([OFF] | [if-present] | [AlwaysExceptStartURLs] | [AlwaysExceptFirstRequest])

Um Relaxationen für die Start-URL-Prüfung festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Prüfungen des Dialogfelds Start URL Check ändern auf Hinzufügen, um das Dialogfeld Start URL Check Relaxation hinzufügen zu öffnen, oder wählen Sie eine vorhandene Entspannung aus, und klicken Sie auf Öffnen, um das Dialogfeld URL Check Relaxation ändern zu öffnen. Beide Dialogfelder bieten die gleichen Optionen für die Konfiguration einer Entspannung.

Im Folgenden finden Sie Beispiele für Start-URL-Check-Relaxationen:

- Erlauben Sie den Zugriff auf die Homepage unter www.example.com:

```
^http://www[.]example[.]com$
<!--NeedCopy-->
```

- Benutzer können auf alle Webseiten im statischen HTML (.htm und .html), serveranalysierten HTML (.htp und .shtml), PHP (.php) und Microsoft ASP (.asp) unter www.example.com zugreifen:

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Benutzer können auf Webseiten mit Pfadnamen oder Dateinamen zugreifen, die Nicht-ASCII-Zeichen enthalten, unter www.example-español.com:

```
^http://www[.]example-espaxC3xB1ol[.]com/(([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*
([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

Hinweis: Im obigen Ausdruck wurde jede Zeichenklasse mit der Zeichenfolge x[0-9a-Fa-F][0-9A-Fa-f]gruppiert, die allen ordnungsgemäß konstruierten Zeichencodierungszeichenfolgen entspricht, aber keine streunenden Backslash-Zeichen zulässt, die nicht mit einer UTF-8-Zeichencodierungszeichenfolge verknüpft sind. Der doppelte umgekehrte Schrägstrich () ist ein maskierter umgekehrter Schrägstrich, der die Web App Firewall anweist, ihn als wörtlichen umgekehrten Schrägstrich zu interpretieren. Wenn Sie nur einen umgekehrten Schrägstrich enthalten, interpretiert die Web App Firewall stattdessen die folgende linke eckige

Klammer ([) als Literalzeichen anstelle des Öffnens einer Zeichenklasse, wodurch der Ausdruck unterbrochen wird.

- Ermöglichen Sie Benutzern den Zugriff auf alle Grafiken im Format GIF (.png), JPEG (.jpg und .jpeg) und PNG (.png) unter www.example.com:

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](gif|jpe?g|png)$
<!--NeedCopy-->
```

- Erlauben Sie Benutzern den Zugriff auf CGI- (.cgi) und PERL-Skripts (.pl), jedoch nur im CGI-BIN-Verzeichnis:

```
^http://www[.]example[.]com/CGI-BIN/[0-9A-Za-z][0-9A-Za-z_
   .-]*[.](cgi|pl)$
<!--NeedCopy-->
```

- Erlauben Sie Benutzern den Zugriff auf Microsoft Office und andere Dokumentdateien im Verzeichnis docsarchive:

```
^http://www[.]example[.]com/docsarchive/[0-9A-Za-z][0-9A-Za-z_
   -.]*[.](doc|xls|pdf|ppt)$
<!--NeedCopy-->
```

> **Hinweis:**
>
> Standardmäßig gelten alle Web App Firewall URLs als reguläre Ausdrücke.

Achtung: Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen/Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht wünschen, z. B. zum Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder zum Erlauben eines Angriffs, den die Start-URL-Prüfung sonst blockiert hätte.

> **Tipp**
>
> Sie können das *-und-* zur zulässigen Liste von SQL-Schlüsselwörtern für das URL-Benennungsschema hinzufügen. Zum Beispiel https://FQDN/bread-and-butter.

URL-Prüfung verweigern

May 11, 2023

URL-Prüfung verweigern untersucht und blockiert Verbindungen zu URLs, auf die häufig von Hackern und bösartigem Code zugegriffen wird. Diese Prüfung enthält eine Liste von URLs, die häufig Ziele von Hackern oder bösartigem Code sind und selten, wenn überhaupt, in legitimen Anfragen auftauchen. Sie können der Liste auch URLs oder URL-Muster hinzufügen. URL-Prüfung verweigern verhindert Angriffe auf verschiedene Sicherheitslücken, von denen bekannt ist, dass sie in Webserver-Software oder auf vielen Websites vorhanden sind.

URL-Prüfung verweigern hat Vorrang vor der Start-URL-Prüfung und verweigert somit böswillige Verbindungsversuche, selbst wenn eine Start-URL-Relaxation normalerweise das Fortfahren einer Anforderung ermöglichen würde.

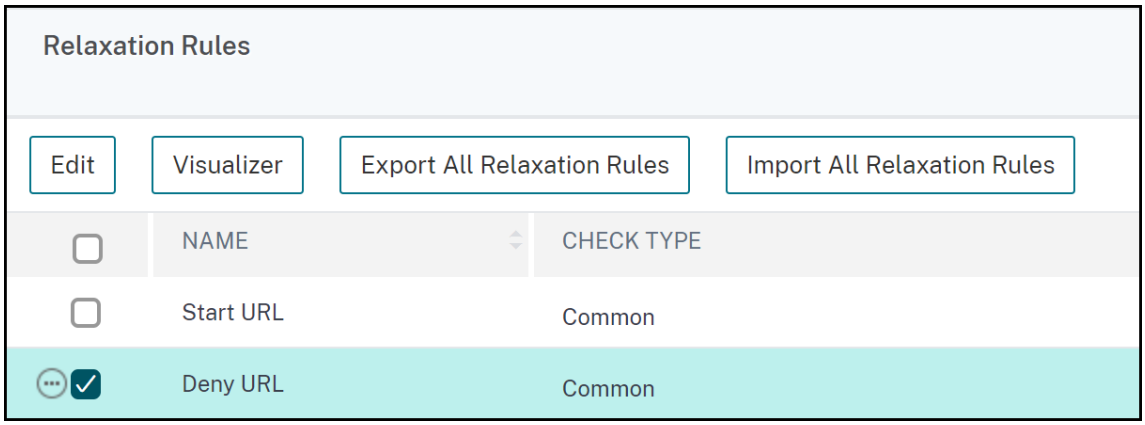
Im Dialogfeld “URL-Prüfung verweigern ändern” können Sie auf der Registerkarte “Allgemein” die Aktionen “Blockieren”, “Protokollieren” und “Statistiken” aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die Deny URL Check zu konfigurieren:

```
set appfw profile <name> -denyURLAction [\*\*block\*\*] [\*\*log\*\*]
    [\*\*stats\*\*] [\*\*none\*\*]
<!--NeedCopy-->
```

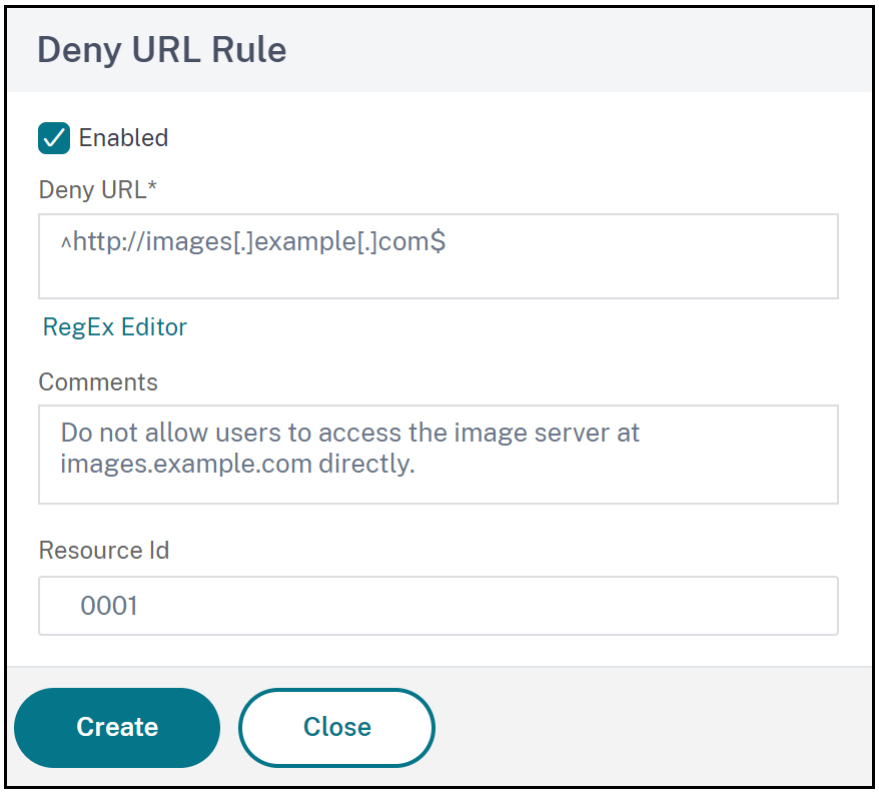
Sie können Ihre eigenen Verweigerungs-URLs nur in der NetScaler GUI erstellen und konfigurieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie ein Profil aus, für das Sie eine Verweigerungs-URL hinzufügen möchten, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie auf der Seite **Profil der NetScaler Web App Firewall** im Abschnitt **Erweiterte Einstellungen** die Option **Relaxationsregeln** aus.
4. Wählen Sie **URL verweigern** und klicken Sie auf **Bearbeiten**.



5. Klicken Sie auf der Seite **URL-Verweigern-Regeln** auf **Hinzufügen**.
6. Geben Sie die folgenden Details an und klicken Sie auf **Erstellen**.

- **URL verweigern** — Ein regulärer Ausdruck zum Definieren einer Verweigerungs-URL.
- **Kommentare** — Beschreibung des Ausdrucks.
- **Ressourcen-ID** — Eindeutige ID zur Identifizierung der URL-Verweigerungsregel.



7. Klicken Sie auf **Schließen**.
8. Klicken Sie auf der Seite **NetScaler Web App Firewall-Profil** auf **Fertig**.

Es folgen Beispiele für URL-Verweigern-Ausdrücke:

- Erlauben Sie Benutzern nicht, direkt auf den Bildserver unter images.example.com zuzugreifen:

```
^http://images[.]example[.]com$
<!--NeedCopy-->
```

- Benutzer dürfen nicht direkt auf CGI- (.cgi) - oder PERL- (.pl) -Skripts zugreifen:

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$
<!--NeedCopy-->
```

- Hier ist dieselbe Verweigerungs-URL, die geändert wurde, um Nicht-ASCII-Zeichen zu unterstützen:

```
^http://www[.]example[.]com/(([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f
   ])
```



```
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])*[.](cgi|pl)$
<!--NeedCopy-->
```

> **Achtung:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL oder das Muster definieren, die Sie blockieren möchten, und sonst nichts. Die unachtsame Verwendung von Platzhaltern und insbesondere der Kombination aus Meta-Zeichen/Platzhalterzeichen (.*) kann zu Ergebnissen führen, die Sie nicht wünschen, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten.

XML-Schutzüberprüfungen

January 19, 2021

Die XML-Schutzüberprüfungen untersuchen Anfragen für XML-basierte Angriffe aller Art.

> **Achtung:**
>
> Die XML-Sicherheitsprüfungen gelten nur für Inhalte, die mit einem HTTP-Content-Type-Header von text/xml gesendet werden. Wenn der Content-Type-Header fehlt oder auf einen anderen Wert eingestellt ist, werden alle XML-Sicherheitsprüfungen umgangen. Wenn Sie vorhaben, XML- oder Web 2.0-Webanwendungen zu schützen, müssen die Webmaster jedes Webservers, der diese Anwendungen hostet, sicherstellen, dass der richtige HTTP-Inhaltstyp-Header gesendet wird.

XML-Formatprüfung

January 19, 2021

Die XML-Formatprüfung untersucht das XML-Format eingehender Anforderungen und blockiert die Anforderungen, die nicht gut geformt sind oder die die Kriterien in der XML-Spezifikation für korrekt geformte XML-Dokumente nicht erfüllen. Einige dieser Kriterien sind:

- Ein XML-Dokument darf nur richtig codierte Unicode-Zeichen enthalten, die der Unicode-Spezifikation entsprechen.
- Es können keine speziellen XML-Syntaxzeichen wie <, > und &in das Dokument aufgenommen werden, außer wenn sie in XML-Markup verwendet werden.

- Alle Beginn-, End- und Leerelement-Tags müssen korrekt verschachtelt sein und keine fehlen oder überlappen.
- Bei XML-Element-Tags wird zwischen Groß- und Kleinschreibung unterschieden. Alle Anfangs- und End-Tags müssen genau übereinstimmen.
- Ein einzelnes Stammelement muss alle anderen Elemente im XML-Dokument enthalten.

Ein Dokument, das die Kriterien für wohlgeformte XML nicht erfüllt, erfüllt nicht die Definition eines XML-Dokuments. Streng genommen ist es kein XML. Allerdings erzwingen nicht alle XML-Anwendungen und Webdienste den XML-Standard, und nicht alle behandeln schlecht geformte oder ungültige XML korrekt. Unsachgemäße Verarbeitung eines schlecht geformten XML-Dokuments kann zu Sicherheitsverstößen führen. Der Zweck der XML-Formatprüfung besteht darin, einen böswilligen Benutzer daran zu hindern, eine schlecht geformte XML-Anforderung zu verwenden, um die Sicherheit Ihrer XML-Anwendung oder Web-Service zu verletzen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-Format ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren und Statistiken aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Formatprüfung zu konfigurieren:

- `set appfw profile <name> -xmlFormatAction [**block**] [**log**] [**stats**] [**none**]`

Sie können keine Ausnahmen für die XML-Formatprüfung konfigurieren. Sie können es nur aktivieren oder deaktivieren.

XML-Denial-of-Service-Prüfung

August 19, 2021

Die XML Denial-of-Service-Prüfung (XML DoS oder XDOs) untersucht eingehende XML-Anfragen, um festzustellen, ob sie mit den Merkmalen eines Denial-of-Service (DoS) -Angriffs übereinstimmen. Wenn es eine Übereinstimmung gibt, blockiert diese Anfragen. Der Zweck der XML-DoS-Prüfung besteht darin, zu verhindern, dass ein Angreifer XML-Anfragen verwendet, um einen Denial-of-Service-Angriff auf Ihren Webserver oder Ihre Website zu starten.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Denial-of-Service-Prüfung ändern auf der Registerkarte **Allgemein** die Aktionen Blockieren, Protokollieren, Statistiken und Lernen aktivieren oder deaktivieren:

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Denial-of-Service-Prüfung zu konfigurieren:

- `set appfw profile <name> -xmlDoSAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Um einzelne XML-Denial-of-Service-Regeln zu konfigurieren, müssen Sie die GUI verwenden. Wählen Sie auf der Registerkarte **Prüfungen** des Dialogfelds **Denial-of-Service-Überprüfung** ändern eine Regel aus, und klicken Sie auf **Öffnen**, um das Dialogfeld **Denial-of-Service ändern** für diese Regel zu öffnen. Die einzelnen Dialogfelder unterscheiden sich für die verschiedenen Regeln, sind aber einfach. Einige erlauben es Ihnen nur, die Regel zu aktivieren oder zu deaktivieren, andere ermöglichen es Ihnen, eine Zahl zu ändern, indem Sie einen neuen Wert in ein Textfeld eingeben.

> **Hinweis:**
>
> Das erwartete Verhalten der Learning Engine für Denial-of-Service-Angriffe basiert auf der konfigurierten Aktion. Wenn die Aktion als "Blockieren" festgelegt ist, lernt die Engine den konfigurierten Bind-Wert +1 und die XML-Analyse stoppt bei einer Verletzung. Wenn die konfigurierte Aktion nicht als "Block" festgelegt ist, lernt die Engine den tatsächlichen Wert für die Länge des eingehenden Verstoßes.

Die einzelnen XML-Denial-of-Service-Regeln lauten:

- Maximale Elementtiefe. Beschränken Sie die maximale Anzahl verschachtelter Ebenen in jedem einzelnen Element auf 256. Wenn diese Regel aktiviert ist und die Web App Firewall eine XML-Anforderung mit einem Element erkennt, das mehr als die maximale Anzahl zulässiger Ebenen aufweist, blockiert sie die Anforderung. Sie können die maximale Anzahl von Ebenen auf einen beliebigen Wert von 1 bis 65.535 ändern.
- Maximale Länge des Elementnamens. Beschränken Sie die maximale Länge jedes Elementnamens auf 128 Zeichen. Dies schließt den Namen innerhalb des erweiterten Namespace ein, der den XML-Pfad und den Elementnamen im folgenden Format enthält:

```
1  {
2  http://prefix.example.com/path/ }
3  target_page.xml
4  <!--NeedCopy-->
```

Der Benutzer kann die maximale Namenslänge auf einen beliebigen Wert zwischen einem (1) Zeichen und 65.535 ändern.

- Maximal # Elemente. Beschränken Sie die maximale Anzahl eines beliebigen Elementtyps pro XML-Dokument auf 65.535. Sie können die maximale Anzahl von Elementen auf einen beliebigen Wert zwischen 1 und 65.535 ändern.
- Maximal # Element Kinder. Beschränken Sie die maximale Anzahl von untergeordneten Elementen (einschließlich anderer Elemente, Zeicheninformationen und Kommentare), die jedes einzelne Element auf 65.535 haben darf. Sie können die maximale Anzahl von untergeordneten Elementen auf einen beliebigen Wert zwischen 1 und 65.535 ändern.

- Maximale Anzahl von Attributen Beschränken Sie die maximale Anzahl von Attributen, die jedes einzelne Element haben darf, auf 256. Sie können die maximale Anzahl von Attributen in einen beliebigen Wert zwischen 1 und 256 ändern.
- Maximale Länge von Attributnamen. Beschränken Sie die maximale Länge jedes Attributnamens auf 128 Zeichen. Sie können die maximale Länge des Attributnamens auf einen beliebigen Wert zwischen 1 und 2.048 ändern.
- Maximale Attributwert-Länge. Beschränken Sie die maximale Länge jedes Attributwerts auf 2048 Zeichen. Sie können die maximale Länge des Attributnamens auf einen beliebigen Wert zwischen 1 und 2.048 ändern.
- Maximale Länge der Zeichendaten Beschränken Sie die maximale Zeichendatenlänge für jedes Element auf 65.535. Sie können die Länge auf einen beliebigen Wert zwischen 1 und 65.535 ändern.
- Maximale Dateigröße Beschränken Sie die Größe jeder Datei auf 20 MB. Sie können die maximale Dateigröße auf einen beliebigen Wert ändern.
- Minimale Dateigröße. Erfordert, dass jede Datei mindestens 9 Byte lang ist. Sie können die minimale Dateigröße auf jede positive Ganzzahl ändern, die verschiedene Bytes repräsentiert.
- Maximale # Entity Expansions. Beschränken Sie die Anzahl der erlaubten Entitätenerweiterungen auf die angegebene Zahl. Standard: 1024.
- Maximale Entity-Erweiterungstiefe Beschränken Sie die maximale Anzahl verschachtelter Entitätenerweiterungen auf höchstens die angegebene Zahl. Standard: 32.
- Maximal # Namespaces. Beschränken Sie die Anzahl der Namespace-Deklarationen in einem XML-Dokument auf nicht mehr als die angegebene Zahl. Standard: 16.
- Maximale Namespace-URI-Länge. Begrenzen Sie die URL-Länge jeder Namespace-Deklaration auf nicht mehr als die angegebene Anzahl von Zeichen. Standard: 256.
- Anweisungen zur Blockverarbeitung. Sperren Sie alle speziellen Verarbeitungsanweisungen, die in der Anfrage enthalten sind. Diese Regel weist keine vom Benutzer veränderbaren Werte auf.
- Blockieren Sie DTD. Blockieren Sie alle Dokumenttypdefinitionen (DTD), die in der Anforderung enthalten sind. Diese Regel weist keine vom Benutzer veränderbaren Werte auf.
- Blockieren Sie externe Entitäten Blockieren Sie alle Verweise auf externe Entitäten in der Anforderung. Diese Regel weist keine vom Benutzer veränderbaren Werte auf.
- SOAP-Array-Prüfung Aktivieren oder deaktivieren Sie die folgenden SOAP-Array-Prüfungen:
  - **Maximale SOAP-Array-Größe.** Die maximale Gesamtgröße aller SOAP-Arrays in einer XML-Anforderung, bevor die Verbindung blockiert wird. Sie können diesen Wert ändern. Standard: 20000000.

- **Maximaler SOAP-Array-Rang.** Der maximale Rang oder die Dimensionen eines einzelnen SOAP-Arrays in einer XML-Anforderung, bevor die Verbindung blockiert wird. Sie können diesen Wert ändern. Standard: 16.

Site-übergreifende Scripting-Überprüfung von XML

May 11, 2023

Die XML-Cross-Site-Scripting-Prüfung untersucht die Benutzeranforderungen auf mögliche Cross-Site-Scripting-Angriffe in der XML-Payload. Findet es einen möglichen Cross-Site-Scripting-Angriff, blockiert es die Anfrage.

Um den Missbrauch der Skripts in Ihren geschützten Webdiensten zu verhindern, um die Sicherheit Ihrer Webdienste zu verletzen, blockiert die XML Cross-Site Scripting-Prüfung Skripts, die gegen dieselbe Ursprungsregel verstoßen, und besagt, dass Skripts auf keinem Server, sondern auf dem Server, auf dem sie sich befinden, zugreifen oder diese ändern dürfen. Jedes Skript, das gegen dieselbe Ursprungsregel verstößt, wird als siteübergreifendes Skript bezeichnet, und die Praxis, Skripts zum Zugriff auf oder Ändern von Inhalten auf einem anderen Server zu verwenden, wird als siteübergreifende Skripts bezeichnet. Der Grund, warum Cross-Site Scripting ein Sicherheitsproblem darstellt, besteht darin, dass ein Webserver, der Cross-Site Scripting ermöglicht, mit einem Skript angegriffen werden kann, das sich nicht auf diesem Webserver befindet, sondern auf einem anderen Webserver, z. B. einem, der dem Angreifer gehört und von diesem kontrolliert wird.

Die Web App Firewall bietet verschiedene Aktionsoptionen zur Implementierung des XML Cross-Site Scripting-Schutzes. Sie haben die Möglichkeit, die Aktionen **Block**, **Log**und **Stats** zu konfigurieren.

Die Web App Firewall XML Cross-Site Scripting Check wird anhand der Payload der eingehenden Anfragen durchgeführt, und Angriffszeichenfolgen werden identifiziert, auch wenn sie über mehrere Zeilen verteilt sind. Die Prüfung sucht nach Zeichenketten für Cross-Site-Scripting-Angriffe im **Element** und in den **Attributwerten** . Unter bestimmten Bedingungen können Sie Lockerungen anwenden, um die Sicherheitskontrolle zu Bypass. Die Protokolle und Statistiken können Ihnen helfen, die erforderlichen Lockerungen zu identifizieren.

Der CDATA Abschnitt der XML-Nutzlast könnte ein attraktiver Schwerpunkt für die Hacker sein, da die Skripts außerhalb des CDATA Abschnitts nicht ausführbar sind. Ein CDATA-Abschnitt wird für Inhalte verwendet, die ausschließlich als Zeichendaten behandelt werden sollen. Die HTML-Markup-Tag-Trennzeichen **<**, ****und ****/** veranlassen den Parser nicht, den Code als HTML-Elemente zu interpretieren. Das folgende Beispiel zeigt einen CDATA-Abschnitt mit einer Zeichenfolge für Cross-Site-Scripting-Angriffe:

```
1     <![CDATA[rn
```



```
2      <script language="Javascript" type="text/javascript">alert ("Got
          you")</script>rn
3      ]]>
4  <!--NeedCopy-->
```

Optionen für Aktionen

Eine Aktion wird angewendet, wenn die XML Cross-Site Scripting-Überprüfung in der Anfrage einen Cross-Site-Scripting-Angriff erkennt. Die folgenden Optionen stehen zur Optimierung des XML Cross-Site Scripting-Schutzes für Ihre Anwendung zur Verfügung:

- **Blockieren**— Die Aktion Blockieren wird ausgelöst, wenn die Cross-Site-Scripting-Tags in der Anfrage erkannt werden.
- **Log**— Generiert Protokollmeldungen, in denen die Aktionen angegeben sind, die bei der XML Cross-Site Scripting-Überprüfung ausgeführt wurden. Wenn der Block deaktiviert ist, wird für jede Stelle (ELEMENT, ATTRIBUTE), an der die Cross-Site-Scripting-Verletzung erkannt wurde, eine separate Lognachricht generiert. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
- **Statistiken**— Erfassen Sie Statistiken über Verstöße und Protokolle. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um zu sehen, ob Sie neue Entspannungsregeln konfigurieren oder die vorhandenen ändern müssen.

Regeln für Entspannung

Wenn Ihre Anwendung verlangt, dass Sie die Cross-Site Scripting-Überprüfung auf ein bestimmtes ELEMENT oder ATTRIBUTE in der XML-Payload Bypass, können Sie eine Relaxationsregel konfigurieren. Die Relaxationsregeln für den XML Cross-Site Scripting Check haben die folgenden Parameter:

- **Name**— Sie können literale Zeichenketten oder reguläre Ausdrücke verwenden, um den Namen des ELEMENTS oder des Attributs zu konfigurieren. Der folgende Ausdruck schließt alle ELEMENTE aus, die mit der Zeichenfolge name_ beginnen, gefolgt von einer Zeichenfolge aus Groß- oder Kleinbuchstaben oder Zahlen, die mindestens zwei und nicht mehr als fünfzehn Zeichen lang ist:

  ```
  ^name_[0-9A-Za-z]{ 2,15 } $
  ```


> **Hinweis**
>
> Bei den Namen wird Groß- und Kleinschreibung erkannt. Doppelte Einträge sind nicht zulässig, aber Sie können die Groß- und Kleinschreibung der Namen und Ortsunterschiede verwenden, um ähnliche Einträge zu erstellen. Zum Beispiel ist jede der folgenden Entspannungsregeln einzigartig:
>
> 1. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`
> 2. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 3. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 4. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`

- **Standort**— Sie können den Speicherort der Cross-Site Scripting Check-Ausnahme in Ihrer XML-Payload angeben. Die Option ELEMENT ist standardmäßig ausgewählt. Sie können es in ATTRIBUTEändern.
- **Kommentar**—Dies ist ein optionales Feld. Sie können eine bis zu 255 Zeichen lange Zeichenfolge verwenden, um den Zweck dieser Entspannungsregel zu beschreiben.

> **Warnung**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau den Namen definieren, den Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung regulärer Ausdrücke kann zu unerwünschten Ergebnissen führen, z. B. die Sperrung des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die XML Cross-Site Scripting-Überprüfung andernfalls blockiert hätte.

Konfiguration des XML Cross-Site Scripting-Checks über die Befehlszeile

Um XML Cross-Site Scripting zu konfigurieren, überprüfen Sie Aktionen und andere Parameter mithilfe der Befehlszeile.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um den XML Cross-Site Scripting Check zu konfigurieren:

```
> set appfw profile <name> -XMLcross-site scriptingAction (([block] [log] [
stats])| [none])
```


Um ein XML Cross-Site Scripting zu konfigurieren, überprüfen Sie die Relaxationsregel mithilfe der Befehlszeile.

Sie können Lockerungsregeln hinzufügen, um die Überprüfung von Cross-Site-Scripting-Skriptangriffen an einer bestimmten Stelle zu Bypass. Verwenden Sie den Befehl bind oder unbind, um die Relaxationsregelbindung wie folgt hinzuzufügen oder zu löschen:

```
> bind appfw profile <name> -XMLcross-site scripting <string> [isRegex ( REGEX | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] -comment <string> [-state ( ENABLED | DISABLED )]

> unbind appfw profile <name> -XMLcross-site scripting <String>
```

Beispiel:

```
> bind appfw profile test_pr -XMLcross-site scripting ABC
```

Nach dem Ausführen des obigen Befehls wird die folgende Relaxationsregel konfiguriert. Die Regel ist aktiviert, der Name wird als Literal behandelt (NOTREGEX) und ELEMENT wird als Standardspeicherort ausgewählt:

```
1)      XMLcross-site scripting:  ABC             IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

`> unbind appfw profile test_pr -XMLcross-site scripting abc`

ERROR: No such XMLcross-site scripting check

`> unbind appfw profile test_pr -XMLcross-site scripting ABC`

 Done
<!--NeedCopy-->
```

Konfiguration des XML Cross-Site Scripting-Checks mithilfe der GUI

In der GUI können Sie den XML Cross-Site Scripting-Check im Bereich für das mit Ihrer Anwendung verknüpfte Profil konfigurieren.

Um das XML Cross-Site Scripting zu konfigurieren oder zu ändern, überprüfen Sie dies mithilfe der GUI

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich Erweiterte Einstellungen auf **Sicherheitsprüfungen**.

In der Tabelle zur Sicherheitsüberprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsüberprüfungen angezeigt. Sie haben 2 Möglichkeiten für die Konfiguration:

a) Wenn Sie nur die Aktionen **Block**, **Log**und **Stats** für die **XML Cross-Site Scripting-Überprüfung**aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf **OK**klicken und dann auf Speichern und Schließen klicken, um den Bereich Sicherheitsprüfung zu schließen.

b) Sie können auf **XML Cross-Site Scripting**doppelklicken oder die Zeile auswählen und auf **Aktionseinstellungen**klicken, um die Aktionsoptionen anzuzeigen. Nachdem Sie eine der Aktionseinstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren.

Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern und schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

So konfigurieren Sie eine Relaxationsregel für XML Cross-Site Scripting mithilfe der GUI

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. **Doppelklicken Sie in der Tabelle Relaxation Rules auf den Eintrag**XML Cross-Site Scripting**, oder wählen Sie ihn aus und klicken Sie auf Bearbeiten.**
4. Führen Sie im Dialogfeld **Relaxationsregeln für XML Cross-Site Scripting** die Operationen **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren**oder **Deaktivieren** für Relaxationsregeln aus.

So verwalten Sie die Relaxationsregeln für XML Cross-Site Scripting mithilfe des Visualizers

Für eine konsolidierte Ansicht aller Relaxationsregeln können Sie die ZeileXML Cross-Site Scripting**in der Tabelle Relaxation Rules markieren und auf Visualizer klicken.** Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine vorhandene zu **bearbeiten** . Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

So zeigen Sie die Cross-Site Scripting-Muster über die GUI an oder passen sie an

Sie können die GUI verwenden, um die Standardliste der für das Cross-Site Scripting zulässigen Attribute oder zulässigen Tags anzuzeigen oder anzupassen. Sie können auch die Standardliste der Siteübergreifenden Scripting-Muster anzeigen oder anpassen.

Die Standardlisten sind **unter Web App Firewall** > **Signaturen** > **Standardsignaturen**angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, wird das Profil für die Verarbeitung der Cross-Site Scripting-Sicherheitsprüfung die im Objekt Standardsignaturen angegebene Standardliste für Cross-Site Scripting verwendet. Die im Standardsignaturobjekt angegebenen Tags, Attributes und Patterns sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese ändern oder ändern möchten, erstellen Sie eine Kopie des Default Signatures -Objekts, um ein benutzerdefiniertes

Signaturobjekt zu erstellen. Nehmen Sie Änderungen an den Listen „Zulässig“ oder „Abgelehnt“ im neuen benutzerdefinierten Signaturobjekt vor und verwenden Sie dieses Signaturobjekt in dem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten Listen für zulässige und abgelehnte Dateien verwenden möchten.

Weitere Hinweise zu Signaturen finden Sie unter http://support.citrix.com/proddocs/topic/ns-security-10-map/appfw-signatures-con.html.

Um standardmäßige Cross-Site-Scripting-Muster anzuzeigen:

1. Navigieren Sie zu **Web App Firewall** > **Signaturen**, wählen Sie ***Standardsignaturen**aus und klicken Sie auf **Bearbeiten**. Klicken Sie anschließend auf **SQL/Cross-Site-Scripting-Muster verwalten**.

Die Tabelle „ **SQL/Cross-Site Scripting-Pfade verwalten“ enthält die folgenden drei Zeilen, die sich auf Cross-Site Scripting** beziehen:

```
            xss/allowed/attribute

            xss/allowed/tag

            xss/denied/pattern
<!--NeedCopy-->
```

Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden Cross-Site-Scripting-Elemente (Tag, Attribut, Muster) anzuzeigen, die vom **Cross-Site** Scripting-Check der Web App Firewall verwendet werden.

So passen Sie Cross-Site-Scripting-Elementean: Sie können das benutzerdefinierte Signaturobjekt bearbeiten, um das zulässige Tag, die zulässigen Attribute und die abgelehnten Muster anzupassen. Sie können neue Einträge hinzufügen oder vorhandene entfernen.

1. **Navigieren Sie zu Web App Firewall** > **Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Bearbeiten**. Klicken Sie auf **SQL/Cross-Site-Scripting-Musterverwalten, um die Tabelle SQL/Cross-Site-Scripting-Pfade** verwalten anzuzeigen.
2. Wählen Sie die Cross-Site-Scripting-Zielzeile aus.

a) Klicken Sie auf **Elemente verwalten**, um das entsprechende Cross-Site-Scripting-Element **hinzuzufügen**, zu **bearbeiten** oder zu **entfernen** .

b) Klicken Sie auf **Entfernen**, um die ausgewählte Zeile zu entfernen.

> **Warnung**
>
> Seien Sie sehr vorsichtig, wenn Sie ein standardmäßiges Cross-Site-Scripting-Element entfernen oder ändern oder den Cross-Site-Scripting-Pfad löschen, um die gesamte Zeile zu entfernen. Die Signaturen, die Sicherheitsüberprüfung für HTML Cross-Site Scripting und die Sicherheitsüber-

> prüfung für XML Cross-Site Scripting verlassen sich auf diese Elemente, um Angriffe zu erkennen und Ihre Anwendungen zu schützen. Das Anpassen der Cross-Site-Scripting-Elemente kann Ihre Anwendung anfällig für Cross-Site-Scripting-Angriffe machen, wenn das erforderliche Pattern während der Bearbeitung entfernt wird.

Verwendung der Log-Funktion mit dem XML Cross-Site Scripting-Check

Wenn die Protokollaktion aktiviert ist, werden die Verstöße gegen die XML Cross-Site Scripting-Sicherheitsprüfung im Audit-Log als **Appfw_XML_Cross-Site** Scripting-Verstöße protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und verfolgen Sie die ns.logs im Ordner /var/log/, um auf die Protokollmeldungen zuzugreifen, die sich auf die Verstöße gegen XML Cross-Site Scripting beziehen:

```
> \*\*Shell\*\*

> \*\*tail -f /var/log/ns.log | grep APPFW_XML_cross-site scripting\*\*
<!--NeedCopy-->
```

Beispiel für eine Protokollmeldung zur Verletzung der Sicherheitsüberprüfung durch XML Cross-Site Scripting im systemeigenen Protokollformat mit Aktion <blocked>

```
Oct  7 01:44:34 <local0.warn> 10.217.31.98 10/07/2015:01:44:34 GMT ns
    0-PPE-1 : default APPFW APPFW_XML_cross-site scripting 1154 0 :
    10.217.253.69 3466-PPE1 - owa_profile http://10.217.31.101/FFC/login
    .html Cross-site script check failed for field script="Bad tag:
    script" <\*\*blocked\*\*>
<!--NeedCopy-->
```

Beispiel für eine Protokollmeldung zur Verletzung der Sicherheitsüberprüfung durch XML Cross-Site Scripting im CEF-Protokollformat, die die Aktion anzeigt <not blocked>

```
Oct  7 01:46:52 <local0.warn> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|APPFW_XML_cross-site scripting|4|src=10.217.30.17
    geolocation=Unknown spt=33141 method=GET request=http://
    10.217.31.101/FFC/login.html msg=Cross-site script check failed for
    field script="Bad tag: script" cn1=1607 cn2=3538 cs1=owa_profile cs2
    =PPE0 cs4=ERROR cs5=2015 act=\*\*not blocked\*\*
<!--NeedCopy-->
```

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die GUI enthält ein nützliches Tool (**Syslog Viewer**) zur Analyse der Logmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zur **Web App Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Security Checks**. **Markieren Sie die Zeile**XML Cross-Site Scripting**und klicken Sie auf Logs.** Wenn Sie direkt von der XML Cross-Site Scripting-Überprüfung des Profils aus auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen heraus und zeigt nur die Protokolle an, die sich auf diese Sicherheitsüberprüfungsverstöße beziehen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Prüfmeldungen auf den Link Syslog-Meldungen, um den Syslog-Viewer aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen ausgelöst werden können.
- Navigieren Sie zu **Web App Firewall** > **Richtlinien** > **Auditing**. Klicken Sie im Abschnitt **Prüfmeldungen** auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung.

Der XML-basierte Syslog-Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. **Um Protokollnachrichten für den**XML Cross-Site Scripting-Check**auszuwählen, filtern Sie, indem Sie in den Dropdownoptionen für Modul**APPFW**auswählen.** Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **Appfw_XML_Cross-Site Scripting** aktivieren und auf die Schaltfläche **Anwenden** klicken, werden im Syslog Viewer nur Protokollmeldungen angezeigt, die sich auf Verstöße gegen die Sicherheitsüberprüfung von XML Cross-Site Scripting beziehen.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollnachricht setzen, werden mehrere Optionen wie **Modul**, **Ereignistyp**, **Ereignis-ID**, **Client-IP** usw. unterhalb der Protokollmeldung angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Statistiken zu den Verstößen gegen XML Cross-Site Scripting

Wenn die Statistikaktion aktiviert ist, wird der Zähler für die XML Cross-Site Scripting-Überprüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Aktion Blockieren aktiviert ist, erhöht eine Anfrage für eine Seite, die drei Verstöße gegen XML Cross-Site Scripting enthält, den Statistikzähler um eins, da die Seite blockiert wird,

sobald der erste Verstoß erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikindikator für Verletzungen und Protokolle um drei, da jede Verletzung eine separate Protokollmeldung generiert.

Um XML Cross-Site Scripting anzuzeigen, überprüfen Sie die Statistiken mithilfe der Befehlszeile.

Geben Sie in der Befehlszeile Folgendes ein:

```
> **sh appfw stats**
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> **stat appfw profile** <profile name>
```

So zeigen Sie XML Cross-Site Scripting-Statistiken mithilfe der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall**.
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Scrollleiste, um die Statistiken zu Verstößen und Protokollen gegen XML Cross-Site Scripting einzusehen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Überprüfung der XML-SQL-Injektion

May 11, 2023

Die Prüfung der XML-SQL-Injektion untersucht die Benutzeranforderungen auf mögliche XML SQL Injection-Angriffe. Findet es injiziertes SQL in XML-Payloads, blockiert es die Anfragen.

Ein XML-SQL-Angriff kann Quellcode in eine Webanwendung einschleusen, sodass er interpretiert und als gültige SQL-Abfrage ausgeführt werden kann, um eine Datenbankoperation mit böswilliger Absicht auszuführen. Beispielsweise können XML-SQL-Angriffe gestartet werden, um unbefugten Zugriff auf den Inhalt einer Datenbank zu erhalten oder die gespeicherten Daten zu manipulieren. XML-SQL-Injection-Angriffe sind nicht nur häufig, sondern können auch sehr schädlich und kostspielig sein.

Die Unterteilung der Rechte der Datenbankbenutzer kann dazu beitragen, die Datenbank bis zu einem gewissen Grad zu schützen. Allen Datenbankbenutzern müssen nur die erforderlichen Rechte erteilt werden, um ihre beabsichtigten Aufgaben zu erledigen, sodass sie keine SQL-Abfragen ausführen können, um andere Aufgaben auszuführen. Beispielsweise darf ein schreibgeschützter Benutzer keine Datentabellen schreiben oder manipulieren. Der Web App Firewall XML SQL Injection Check überprüft alle XML-Anfragen, um besondere Schutzmaßnahmen gegen die Injektion von nicht autorisiertem SQL-Code zu bieten, der die Sicherheit gefährden könnte. Wenn die Web App Firewall unbefugten SQL-Code in einer XML-Anfrage eines Benutzers erkennt, kann sie die Anfrage blockieren.

Die NetScaler Web App Firewall überprüft das Vorhandensein von SQL-Schlüsselwörtern und Sonderzeichen, um den XML-SQL-Injection-Angriff zu identifizieren. Ein Standardsatz von Schlüsselwörtern und Sonderzeichen enthält bekannte Schlüsselwörter und Sonderzeichen, die häufig zum Starten von XML-SQL-Angriffen verwendet werden. Die Web App Firewall betrachtet drei Zeichen, ein einfaches gerades Anführungszeichen (‘), einen umgekehrten Schrägstrich () und ein Semikolon (;) als Sonderzeichen für die Verarbeitung von SQL-Sicherheitsprüfungen. Sie können neue Muster hinzufügen und den Standardsatz bearbeiten, um die XML-SQL-Prüfprüfung anzupassen.

Die Web App Firewall bietet verschiedene Aktionsoptionen zur Implementierung des XML-SQL-Injection-Schutzes. Sie können die Anfrage **blockieren**, in der Datei ns.log eine Nachricht mit Details zu den beobachteten Verstößen **protokollieren** und **Statistiken** sammeln, um die Anzahl der beobachteten Angriffe zu verfolgen.

Zusätzlich zu den Aktionen gibt es mehrere Parameter, die für die Verarbeitung von XML-SQL-Injection konfiguriert werden können. Sie können nach **SQL-Platzhalterzeichen**suchen. Sie können den XML-SQL-Injection-Typ ändern und eine der 4 Optionen (**sqlKeyword, sqlSplChar, sqlSplcharAndKeyword**, sqlSplcharOrKeyword**) auswählen, um anzugeben, wie die SQL-Schlüsselwörter und SQL-Sonderzeichen**bei der Verarbeitung der XML-Payload ausgewertet werden sollen. Der Parameter zur **Verarbeitung von XML-SQL-Kommentaren** bietet Ihnen die Möglichkeit, den Typ der Kommentare anzugeben, die bei der Erkennung von XML SQL Injection überprüft oder ausgenommen werden müssen.

Sie können Entspannungen einsetzen, um Fehlalarme zu vermeiden. Die Web App Firewall XML-SQL-Prüfung wird anhand der Payload der eingehenden Anfragen durchgeführt, und Angriffszeichenfolgen werden identifiziert, auch wenn sie über mehrere Zeilen verteilt sind. Die Prüfung sucht nach SQL-Injection-Zeichenketten im **Element** und den **Attributwerten** . Unter bestimmten Bedingungen können Sie Lockerungen anwenden, um die Sicherheitskontrolle zu Bypass. Die Protokolle und Statistiken können Ihnen helfen, die erforderlichen Lockerungen zu identifizieren.

Optionen für Aktionen

Eine Aktion wird angewendet, wenn die XML-SQL-Injection-Prüfung eine SQL-Injection-Angriffszeichenfolge in der Anfrage erkennt. Die folgenden Aktionen sind verfügbar, um einen optimierten XML-SQL-Injection-Schutz für Ihre Anwendung zu konfigurieren:

Block— Wenn Sie Block aktivieren, wird die Blockaktion nur ausgelöst, wenn die Eingabe der XML-SQL-Injection-Typspezifikation entspricht. Wenn **SqlSplCharAndKeyword** beispielsweise als XML-SQL-Injektionstyp konfiguriert ist, wird eine Anfrage nicht blockiert, wenn sie keine Schlüsselwörter enthält, selbst wenn SQL-Sonderzeichen in der Payload erkannt werden. **Eine solche Anfrage wird blockiert, wenn der XML-SQL-Injektionstyp entweder auf**sqlSplChar oder sqlSplcharOrKeyword**gesetzt ist.**

Protokoll — Wenn Sie die Protokollfunktionaktivieren, generiert die XML-SQL-Injection-Prüfung

Protokollmeldungen, in denen die Aktionen angegeben sind, die ausgeführt werden. Wenn der Block deaktiviert ist, wird für jede Stelle (**ELEMENT**, **ATTRIBUTE**), an der die XML-SQL-Verletzung erkannt wurde, eine separate Lognachricht generiert. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.

Statistiken— Wenn diese Option aktiviert ist, sammelt die Statistikfunktion Statistiken zu Verstößen und Protokollen. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um zu sehen, ob Sie neue Entspannungsregeln konfigurieren oder die vorhandenen ändern müssen.

XML-SQL-Parameter

Zusätzlich zu den Block-, Log- und Statistikaktionen können Sie die folgenden Parameter für die XML-SQL-Injection-Prüfung konfigurieren:

Suchen Sie nach XML-SQL-Platzhalterzeichen — Platzhalterzeichen können verwendet werden, um die Auswahl einer strukturierten Abfragesprache (SQL-SELECT) -Anweisung zu erweitern. Diese Platzhalteroperatoren können zusammen mit den Operatoren **LIKE** und **NOT LIKE** verwendet werden, um einen Wert mit ähnlichen Werten zu vergleichen. Die Prozentzeichen (%) und Unterstriche (_) werden häufig als Platzhalter verwendet. Das Prozentzeichen entspricht dem Sternchen-Platzhalterzeichen (*), das mit MS-DOS verwendet wird, und entspricht null, einem oder mehreren Zeichen in einem Feld. Der Unterstrich ähnelt dem MS-DOS-Fragezeichen (?) Platzhalterzeichen. Es stimmt mit einer einzelnen Zahl oder einem Zeichen in einem Ausdruck überein.

Sie können beispielsweise die folgende Abfrage verwenden, um eine Zeichenfolgensuche durchzuführen, um alle Kunden zu finden, deren Namen das D-Zeichen enthalten.

```
SELECT * from customer WHERE name like "%D%"
```

Im folgenden Beispiel werden die Operatoren kombiniert, um alle Gehaltswerte zu finden, die 0 als zweites und drittes Zeichen haben.

```
SELECT * from customer WHERE salary like '_00%
```

Verschiedene DBMS-Anbieter haben die Platzhalterzeichen um zusätzliche Operatoren erweitert. Die NetScaler Web App Firewall kann vor Angriffen schützen, die durch das Eingeben dieser Platzhalterzeichen gestartet werden. Die 5 Standard-Platzhalterzeichen sind Prozent (%), Unterstrich (_), Caret (^), öffnende eckige Klammer ([) und schließende eckige Klammer (]). Dieser Schutz gilt sowohl für HTML- als auch für XML-Profile.

Die Standard-Platzhalterzeichen sind eine Liste von Literalen, die in der ***Standardsignaturen angegeben sind**:

```
1 -  <wildchar type=" LITERAL" >%</wildchar>
2 -  <wildchar type=" LITERAL" >_</wildchar>
3 -  <wildchar type=" LITERAL" >^</wildchar>
4 -  <wildchar type=" LITERAL" >[</wildchar>
5 -  <wildchar type=" LITERAL" >]</wildchar>
6 <!--NeedCopy-->
```

Platzhalterzeichen in einem Angriff können PCRE sein, wie [^A-F]. Die Web App Firewall unterstützt auch PCRE-Platzhalter, aber die obigen Platzhalterzeichen reichen aus, um die meisten Angriffe zu blockieren.

> **Hinweis**
>
> Die **XML-SQL-Platzhalterprüfung** unterscheidet sich von der **XML-SQL-Sonderzeichenprüfung** . Diese Option muss mit Vorsicht verwendet werden, um Fehlalarme zu vermeiden.

Check Request mit SQL-Einschleusung-Typ— Die Web App Firewall bietet 4 Optionen, um die gewünschte Strenge für die SQL Injection-Prüfung basierend auf den individuellen Anforderungen der Anwendung zu implementieren. Die Anforderung wird mit der Spezifikation des Injektionstyps zur Erkennung von SQL-Verletzungen abgeglichen. Die 4 Optionen für den SQL-Einschleusung-Typ sind:

- **SQL-Sonderzeichen und Schlüsselwort**— Sowohl ein SQL-Schlüsselwort als auch ein SQL-Sonderzeichen müssen an der untersuchten Stelle vorhanden sein, um eine SQL-Verletzung auszulösen. Diese am wenigsten restriktive Einstellung ist auch die Standardeinstellung.
- **SQL-Sonderzeichen**— Mindestens eines der Sonderzeichen muss in der verarbeiteten Payload-Zeichenfolge vorhanden sein, um eine SQL-Verletzung auszulösen.
- **SQL-Schlüsselwort**— Mindestens eines der angegebenen SQL-Schlüsselwörter muss in der verarbeiteten Payload-Zeichenfolge vorhanden sein, um eine SQL-Verletzung auszulösen. Wählen Sie diese Option nicht ohne angemessene Berücksichtigung aus. Um Fehlalarme zu vermeiden, stellen Sie sicher, dass keines der Schlüsselwörter in den Eingaben erwartet wird.
- **SQL-Sonderzeichen oder Schlüsselwort**— Entweder das Schlüsselwort oder die Sonderzeichenfolge müssen in der Payload vorhanden sein, um die Sicherheitsüberprüfung auszulösen.

> **Tipp**
>
> Wenn Sie die Option SQL-Sonderzeichen auswählen, überspringt die Web App Firewall Zeichenfolgen, die keine Sonderzeichen enthalten. Da die meisten SQL-Server keine SQL-Befehle verarbeiten, denen kein Sonderzeichen vorangestellt ist, kann die Aktivierung dieser Option die Web App Firewall erheblich entlasten und die Verarbeitung beschleunigen, ohne dass Ihre geschützten Websites gefährdet werden.

Behandlung von SQL-Kommentaren— Standardmäßig analysiert und überprüft die Web App Firewall alle Kommentare in XML-Daten auf injizierte SQL-Befehle. Viele SQL-Server ignorieren alles in einem Kommentar, auch wenn ihm ein SQL-Sonderzeichen vorangestellt ist. Wenn Ihr XML-SQL-Server Kommentare ignoriert, können Sie zur schnelleren Verarbeitung die Web App Firewall so konfigurieren, dass Kommentare bei der Untersuchung von Anfragen für injiziertes SQL übersprungen werden. Die Optionen zur Behandlung von XML-SQL-Kommentaren sind:

- **ANSI**—Überspringt SQL-Kommentare im ANSI-Format, die normalerweise von UNIX-basierten SQL-Datenbanken verwendet werden.
- **Verschachtelt**— Verschachtelte SQL-Kommentare überspringen, die normalerweise von Microsoft SQL Server verwendet werden.
- **ANSI/verschachtelt**—Überspringen Sie Kommentare, die sowohl den ANSI- als auch den verschachtelten SQL-Kommentarstandards entsprechen. Kommentare, die nur dem ANSI-Standard oder nur dem verschachtelten Standard entsprechen, werden weiterhin auf injizierte SQL überprüft.
- **Alle Kommentare überprüfen**— Prüft die gesamte Anfrage nach injiziertem SQL, ohne etwas zu überspringen. Dies ist die Standardeinstellung.

> **Tipp**
>
> In den meisten Fällen dürfen Sie die Option Nested oder ANSI/Nested nicht wählen, es sei denn, Ihre Back-End-Datenbank läuft auf Microsoft SQL Server. Die meisten anderen Typen von SQL Server-Software erkennen verschachtelte Kommentare nicht. Wenn verschachtelte Kommentare in einer Anfrage erscheinen, die an einen anderen SQL-Servertyp gerichtet ist, deuten sie möglicherweise auf einen Versuch hin, die Sicherheit auf diesem Server zu verletzen.

Regeln zur Entspannung

Wenn Ihre Anwendung verlangt, dass Sie die XML-SQL-Injection-Prüfung für ein bestimmtes ELEMENT oder ATTRIBUT in der XML-Payload Bypass, können Sie eine Relaxationsregel konfigurieren. Die Relaxationsregeln für die XML-SQL-Injection-Prüfung haben die folgenden Parameter:

- **Name:** Sie können literale Zeichenketten oder reguläre Ausdrücke verwenden, um den Namen des **ELEMENTS** oder des **ATTRIBUTES**zu konfigurieren. Der folgende Ausdruck schließt alle **ELEMENTE** aus, die mit der Zeichenfolge **PurchaseOrder_** beginnen, gefolgt von einer Zahlenfolge, die mindestens zwei und nicht mehr als zehn Zeichen lang ist:

  Kommentar: „XML-SQL-Prüfung für Bestellelemente ausnehmen“

```
1     XMLSQLInjection:  "PurchaseOrder_[0-9A-Za-z]{
2  2,10 }
3  "
4
5     IsRegex:  REGEX          Location:  ELEMENT
```



```
6
7       State:  ENABLED
8   <!--NeedCopy-->
```

Hinweis: Bei den Namen wird zwischen Groß- und Kleinschreibung unterschieden. Doppelte Einträge sind nicht zulässig, aber Sie können die Groß- und Kleinschreibung der Namen und Ortsunterschiede verwenden, um ähnliche Einträge zu erstellen. Zum Beispiel ist jede der folgenden Entspannungsregeln einzigartig:

```
1   1)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX
2
3           Location:  ELEMENT       State:  ENABLED
4
5   2)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX
6
7           Location:  ELEMENT       State:  ENABLED
8
9   3)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX
10
11          Location:  ATTRIBUTE     State:  ENABLED
12
13  4)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX
14
15          Location:  ATTRIBUTE     State:  ENABLED
16  <!--NeedCopy-->
```

- **Ort**: Sie können den Speicherort der XML SQL Inspection-Ausnahme in Ihrer XML-Payload angeben. Die Option **ELEMENT** ist standardmäßig ausgewählt. Sie können es in **ATTRIBUTE**ändern.
- **Kommentar**: Dies ist ein optionales Feld. Sie können eine bis zu 255 Zeichen lange Zeichenfolge verwenden, um den Zweck dieser Entspannungsregel zu beschreiben.

> **Warnung**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau den Namen definieren, den Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung regulärer Ausdrücke kann zu unerwünschten Ergebnissen führen, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die XML SQL Injection-Inspektion andernfalls blockiert hätte.

Verwenden der Befehlszeile zur Konfiguration des XML SQL Injection Check

Gehen Sie wie folgt vor, um XML SQL Injection-Aktionen und andere Parameter mithilfe der Befehlszeile zu konfigurieren:

In der Befehlszeilenschnittstelle können Sie entweder den Befehl **set appfw profile oder den Befehl add appfw profileverwenden, um den XML-SQL-Injection-Schutz**zu konfigurieren. Sie können die Aktion (en) blockieren, protokollieren und Statistiken aktivieren. Wählen Sie den Typ des SQL-Angriffsmusters (Schlüsselwörter, Platzhalterzeichen, spezielle Zeichenketten) aus, das Sie in den Payloads erkennen möchten. Verwenden Sie den Befehl**unset appfw profile**, um die konfigurierten Einstellungen auf ihre Standardeinstellungen zurückzusetzen. Jeder der folgenden Befehle legt nur einen Parameter fest, aber Sie können mehrere Parameter in einen einzelnen Befehl aufnehmen:

- set appfw profile <name> **-XMLSQLInjectionAction** ([block] [log] [stats])| [none])
- set appfw profile <name> -XMLSQLInjectionCheckSQLWildChars (ON |OFF)
- set appfw profile <name> -XMLSQLInjectionType ([SQLKeyword] | [SQLSplChar] | [SQLSplCharANDKeyword] | [SQLSplCharORKeyword])
- set appfw profile <name> -XMLSQLInjectionParseComments ([checkall] | [ansi|nested] | [ansinested])

So konfigurieren Sie eine Relaxationsregel für SQL Injection mithilfe der Befehlszeile

Verwenden Sie den Befehl bind oder unbind, um Relaxationsregeln wie folgt hinzuzufügen oder zu löschen:

```
1 - bind appfw profile <name> -XMLSQLInjection <string> [isRegex (REGEX
    | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] - comment <string>
    [-state ( ENABLED | DISABLED )]
2 - unbind appfw profile <name> -XMLSQLInjection <String>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > bind appfw profile test_profile -XMLSQLInjection "PurchaseOrder_[0-9A
    -Za-z]{
2  2,15 }
3  " -isregex REGEX -location ATTRIBUTE
4
5 > unbind appfw profile test_profile - XMLSQLInjection "PurchaseOrder_
    [0-9A-Za-z]{
6  2,15 }
7  " -location ATTRIBUTE
8 <!--NeedCopy-->
```


Verwenden der GUI zur Konfiguration der XMLSQL-Injection-Sicherheitsprüfung

In der GUI können Sie die XML-SQL-Injection-Sicherheitsprüfung im Bereich für das Ihrer Anwendung zugeordnete Profil konfigurieren.

Um die XML-SQL-Injection-Prüfung mit der GUI zu konfigurieren oder zu ändern

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich Erweiterte Einstellungen auf **Sicherheitsprüfungen**.

In der Tabelle zur Sicherheitsüberprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsüberprüfungen angezeigt. Sie haben 2 Möglichkeiten für die Konfiguration:

a. Wenn Sie nur die Aktionen Block, Log und Stats für XML SQL Injection aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf OK klicken und dann auf Speichern und Schließen klicken, um den Bereich Sicherheitsüberprüfung zu schließen.

b. Wenn Sie zusätzliche Optionen für diese Sicherheitsüberprüfung konfigurieren möchten, doppelklicken Sie auf XML SQL Injection, oder wählen Sie die Zeile aus und klicken Sie auf **Aktionseinstellungen**, um die folgenden Optionen anzuzeigen:

AufSQL-Platzhalterzeichen prüfen— Betrachten Sie SQL-Platzhalterzeichen in der Nutzlast als Angriffsmuster.

Überprüfen Sie die Anforderung mit—Type der SQL-Einschleusung (SqlKeyword, SqlSplChar, SqlSplcharandKeyword oder SqlSplcharorKeyword), die überprüft werden soll.

SQL Comments Handling— Art der zu prüfenden Kommentare (Alle Kommentare prüfen, ANSI, Verschachtelt oder ANSI/verschachtelt).

Nachdem Sie eine der obigen Einstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsüberprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern** und **Schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

So konfigurieren Sie eine Relaxationsregel für XML-SQL-Injection mithilfe der GUI

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Doppelklicken Sie in der Tabelle Relaxation Rules auf den Eintrag **XML SQL Injection**, oder wählen Sie ihn aus und klicken Sie auf **Bearbeiten**.
4. Führen **Sie im Dialogfeld**Relaxationsregeln für XML SQL Injection**die Operationen Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren**oder **Deaktivieren** für Relaxationsregeln aus.

So verwalten Sie Relaxationsregeln für XML SQL Injection mithilfe des Visualizers

Für eine konsolidierte Ansicht aller Relaxationsregeln können Sie die Zeile **XML SQL Injection** in der Tabelle Relaxation Rules markieren und auf **Visualizer**klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine vorhandene zu **bearbeiten** . Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

Um die SQL Injection-Muster mithilfe der GUI anzuzeigen oder anzupassen:

Sie können die GUI verwenden, um die SQL-Muster anzuzeigen oder anzupassen.

Die Standard-SQL-Muster sind **unter Web App Firewall** > **Signaturen** > ***Standardsignaturen**angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, werden die im Objekt Standardsignaturen angegebenen Standard-SQL-Muster vom Profil für die Verarbeitung der XML-SQL-Injection-Sicherheitsprüfung verwendet. Die Regeln und Muster im Default Signatures-Objekt sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese Muster ändern oder ändern möchten, erstellen Sie ein benutzerdefiniertes Signaturobjekt, indem Sie eine Kopie des Standardsignaturobjekts erstellen und die SQL-Muster ändern. Verwenden Sie das benutzerdefinierte Signaturobjekt in dem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten SQL-Muster verwenden möchten.

Weitere Informationen finden Sie unter Signaturen.

So zeigen Sie SQL-Standardmuster an:

a. Navigieren Sie zu **Web App Firewall** > **Signaturen**, wählen Sie ***Standardsignaturen**aus und klicken Sie auf **Bearbeiten**. Klicken Sie anschließend auf **SQL/Cross-Site-Scripting-Muster verwalten**.

Die Tabelle „SQL/Cross-Site Scripting-Pfade verwalten“ enthält die folgenden vier Zeilen, die sich auf SQL Injection beziehen:

```
Injection (not_alphanum, SQL)/ Keyword

Injection (not_alphanum, SQL)/ specialstring

Injection (not_alphanum, SQL)/ transformrules/transform

Injection (not_alphanum, SQL)/ wildchar
<!--NeedCopy-->
```

b. Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden SQL-Muster (Schlüsselwörter, spezielle Zeichenketten, Transformationsregeln oder Platzhalterzeichen) anzuzeigen, die bei der SQL Injection-Prüfung der Web App Firewall verwendet werden.

Um SQL-Muster anzupassen: Sie können ein benutzerdefiniertes Signaturobjekt bearbeiten, um die SQL-Schlüsselwörter, Sonderzeichenfolgen und Platzhalterzeichen anzupassen. Sie können neue

Einträge hinzufügen oder vorhandene entfernen. Sie können die Transformationsregeln für die SQL-Spezialzeichenketten ändern.

a. Navigieren Sie zu **Web App Firewall** > **Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Bearbeiten**. Klicken Sie auf **SQL/Cross-Site-Scripting-Musterverwalten, um die Tabelle SQL/Cross-Site-Scripting-Pfade** verwalten anzuzeigen.

b. Wählen Sie die Ziel-SQL-Zeile aus.

i. Klicken Sie auf **Elemente verwalten**, um das entsprechende SQL-Element **hinzuzufügen**, zu **bearbeiten** oder zu **entfernen** .

ii. Klicken Sie auf **Entfernen**, um die ausgewählte Zeile zu entfernen.

> **Warnung**
>
> Sie müssen sehr vorsichtig sein, wenn Sie ein Standard-SQL-Element entfernen oder ändern oder den SQL-Pfad löschen, um die gesamte Zeile zu entfernen. Die Signaturregeln sowie die XML-SQL-Injection-Sicherheitsprüfung stützen sich auf diese Elemente, um SQL-Injection-Angriffe zu erkennen und Ihre Anwendungen zu schützen. Das Anpassen der SQL-Muster kann Ihre Anwendung anfällig für XML-SQL-Angriffe machen, wenn das erforderliche Muster während der Bearbeitung entfernt wird.

Verwendung der Log-Funktion mit der XML-SQL-Injection-Prüfung

Wenn die Protokollaktion aktiviert ist, werden die Verstöße gegen die **XML SQL Injection-Sicherheitsprüfung** im Audit-Log als **APPFW_XML_SQL-Verstöße** protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

Gehen Sie wie folgt vor, um über die Befehlszeile auf die Protokollmeldungen zuzugreifen:

Wechseln Sie zur Shell und verfolgen Sie die ns.logs im Ordner /var/log/, um auf die Protokollmeldungen zuzugreifen, die sich auf die Verstöße gegen XML Cross-Site Scripting beziehen:

```
> Shell

> tail -f /var/log/ns.log | grep APPFW_XML_SQL
<!--NeedCopy-->
```

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die GUI enthält ein nützliches Tool (Syslog Viewer) zur Analyse der Logmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Web App Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Security Checks**. Markieren Sie die Zeile **XML SQL Injection** und klicken Sie auf **Logs**. Wenn

Sie direkt von der XML-SQL-Injection-Prüfung des Profils aus auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen heraus und zeigt nur die Protokolle an, die sich auf diese Sicherheitsüberprüfungsverstöße beziehen.

- **Sie können den Syslog-Viewer auch aufrufen, indem Sie zu**System**> Auditing navigieren.** Klicken Sie im Abschnitt Prüfmeldungen auf den Link **Syslog-Meldungen, um den Syslog-Viewer** aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen ausgelöst werden können.
- Navigieren Sie zu **Web App Firewall** > **Richtlinien** > **Überwachung.** Klicken Sie im Abschnitt Prüfmeldungen auf den Link **Syslog-Meldungen, um den**Syslog-Viewer**aufzurufen, in dem alle Protokollmeldungen angezeigt werden, einschließlich anderer Protokolle von Verstößen gegen die Sicherheitsüberprüfung.

Der XML-basierte Syslog-Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. **Um Protokollnachrichten für die**XML-SQL-Injection-Prüfung**auszuwählen, filtern Sie, indem Sie in den Dropdown-Optionen für Modul**APPFW**auswählen.** Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_XML_SQL** aktivieren und auf die Schaltfläche **Anwenden** klicken, werden im Syslog-Viewer nur Protokollmeldungen angezeigt, die sich auf Verstöße gegen die **XML SQL Injection-Sicherheitsprüfung** beziehen.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollmeldung setzen, werden unter der Protokollmeldung mehrere Optionen wie **Modul**, **Ereignistyp, Ereignis-ID**und**Client-IP** angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Statistiken für die XML-SQL-Injection-Verstöße

Wenn die Statistikaktion aktiviert ist, wird der Zähler für die **XML-SQL-Injection-Prüfung** erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Block-Aktion aktiviert ist, erhöht eine Anfrage für eine Seite, die drei **XML-SQL-Injection-Verstöße** enthält, den Statistikzähler um eins, da die Seite blockiert wird, sobald der erste Verstoß erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikindikator für Verletzungen und Protokolle um drei, da jede Verletzung eine separate Protokollmeldung generiert.

Um XML SQL Injection anzuzeigen, überprüfen Sie die Statistiken mithilfe der Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:


```
> sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> stat appfw profile <profile name>
```

So zeigen Sie XML-SQL-Injection-Statistiken mithilfe der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall**.
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Scrollleiste, um die Statistiken zu Verstößen und Protokollen von **XML SQL Injection einzusehen** . Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

XML-Anlagenprüfung

January 19, 2021

Die XML-Anlagenprüfung prüft eingehende Anforderungen auf schädliche Anlagen und blockiert die Anforderungen, die Anlagen enthalten, die die Anwendungssicherheit verletzen könnten. Der Zweck der Überprüfung von XML-Anlagen besteht darin, zu verhindern, dass Angreifer eine XML-Anlage verwenden, um die Sicherheit auf Ihrem Server zu verletzen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-Anhang ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Lernen, Protokollieren, Statistiken und Lernen aktivieren oder deaktivieren:

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Anlagenprüfung zu konfigurieren:

- `set appfw profile <name> -xmlAttachmentAction [block] [learn] [log] [ stats] [none]`

Sie müssen die anderen Einstellungen für die Überprüfung der XML-Anlagen in der Benutzeroberfläche konfigurieren. Im Dialogfeld `Modify XML Attachment` Prüfen können Sie auf der Registerkarte Prüfen die folgenden Einstellungen konfigurieren:

- **Maximale Anlagengröße.** Zulassen von Anlagen, die nicht größer als die von Ihnen angegebene maximale Anlagengröße sind. Um diese Option zu aktivieren, aktivieren Sie zuerst das Kontrollkästchen Aktiviert, und geben Sie dann die maximale Anlagengröße in Byte in das`Size` Textfeld ein.
- **Anlageninhaltstyp.** Anhänge des angegebenen Inhaltstyps zulassen. Aktivieren Sie zum Aktivieren dieser Option zuerst das Kontrollkästchen Aktiviert, und geben Sie dann einen regulären Ausdruck ein, der dem Content-Type-Attribut der Anlagen entspricht, die Sie zulassen möchten.

- Sie können den URL-Ausdruck direkt in das Textfenster eingeben. In diesem Fall können Sie über dasRegex Tokens Menü eine Reihe nützlicher regulärer Ausdrücke am Cursor eingeben, anstatt sie manuell einzugeben.
- Sie können auf Regex-Editor klicken, um dasAdd Regular Expression Dialogfeld zu öffnen und es zum Erstellen des URL-Ausdrucks zu verwenden.

Interoperabilitätsprüfung von Webdiensten

January 19, 2021

Bei der WS-I-Prüfung (Web Services Interoperability) werden sowohl Anforderungen als auch Antworten auf die Einhaltung des WS-I-Standards untersucht und die Anforderungen und Antworten blockiert, die diesen Standard nicht erfüllen. Der Zweck der WS-I-Prüfung besteht darin, Anforderungen zu blockieren, die möglicherweise nicht mit anderen XML interagieren. Ein Angreifer kann Inkonsistenzen in der Interoperabilität verwenden, um einen Angriff auf Ihre XML-Anwendung zu starten.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Interoperabilitätsprüfung für Webdienste ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren, Statistiken und Lernen aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die Interoperabilitätsprüfung für Webdienste zu konfigurieren:

- `set appfw profile <name> -xmlWSIAction [block] ][log] [learn] [stats] [ none]`

Um einzelne Web Services Interoperabilitätsregeln zu konfigurieren, müssen Sie die GUI verwenden. Wählen Sie im Dialogfeld Interoperabilitätsprüfung für Webdienste auf der Registerkarte Prüfungen eine Regel aus, und klicken Sie auf Aktivieren oder Deaktivieren, um die Regel zu aktivieren oder zu deaktivieren. Sie können auch auf Öffnen klicken, um das Meldungsfeld Webdienst-Interoperabilitätsdetails für diese Regel zu öffnen. Im Meldungsfeld werden schreibgeschützte Informationen zur Regel angezeigt. Sie können keine dieser Regeln ändern oder andere Konfigurationsänderungen vornehmen.

Bei der WS-I-Prüfung werden die in WS-I Basic Profile 1.0 aufgeführten Regeln verwendet. WS-I bietet Best Practices für die Entwicklung interoperabler Web Services-Lösungen. WS-I-Prüfungen werden nur für SOAP-Nachrichten durchgeführt.

Eine Beschreibung der einzelnen WSI-Standardregeln finden Sie im Folgenden:

Regel	Beschreibung
BP1201	Der Nachrichtentext sollte ein soap:envelope mit Namespace sein.
R1000	Wenn ein ENVELOPE ein Fehler ist, darf das soap:Fault-Element NUR die untergeordneten Elemente faultcode, faultstring, faultactor und detail haben.
R1001	Wenn ein ENVELOPE ein Fehler ist, müssen die untergeordneten Elemente des Elements SOAP:Fault nicht qualifiziert sein.
R1003	Ein RECEIVER MUSS Fehlermeldungen akzeptieren, die eine beliebige Anzahl qualifizierter oder nicht qualifizierter Attribute aufweisen, einschließlich Null, die auf dem Detailelement angezeigt werden. Der Namespace von qualifizierten Attributen kann alles andere als der Namespace des qualifizierten Dokumentelements Envelope sein.
R1004	Wenn ein ENVELOPE ein faultcode-Element enthält, muss der Inhalt dieses Elements entweder einer der in SOAP 1.1 definierten Fehlercodes sein (ggf. zusätzliche Informationen im Detailelement liefern) oder ein Qname, dessen Namespace durch die spezifizierende Autorität des Fehlers gesteuert wird (in dieser Reihenfolge der Präferenz).
R1005	Ein ENVEL MUSS NICHT SOAP:EncodingStyle-Attribut für eines der Elemente enthalten, deren Namespace dem Namespace des qualifizierten Dokumentelements Envelope entspricht.
R1006	Ein ENVELOPE darf NICHT soap:encodingStyle-Attribute für ein Element enthalten, das ein untergeordnetes Element von soap:Body ist.

Regel	Beschreibung
R1007	Ein in einer rpc-literal-Bindung beschriebener ENVELOPE darf NICHT das soap:encodingStyle-Attribut für ein Element enthalten, das ein Enkelkind von soap:Body ist.
R1011	Ein ENVELOPE darf NICHT untergeordnete Elemente von soap:Envelope nach dem Element soap:Body haben.
R1012	Eine MESSAGE MUSS als UTF-8 oder UTF-16 serialisiert werden.
R1013	Ein ENVELOPE, der ein soap:mustUnderstand-Attribut enthält, DARF nur die lexikalischen Formulare 0 und 1 verwenden.
R1014	Die untergeordneten Elemente des soap:Body-Elements in einem ENVELOPE müssen namespace-qualifiziert sein.
R1015	Ein RECEIVER MUSS einen Fehler erzeugen, wenn ein Envelope auftritt, dessen Dokumentelement nicht SOAP:Envelope ist.
R1031	Wenn ein ENVELOPE ein faultcode-Element enthält, darf der Inhalt dieses Elements NICHT die SOAP 1.1-Punktnotation verwenden, um die Bedeutung des Fehlers zu verfeinern.
R1032	Die Elemente soap:Envelope, soap:Header und soap:Body in einem ENVELOPE dürfen NICHT Attribute im gleichen Namespace wie das des qualifizierten Dokumentelements Envelope haben
R1033	Ein ENVELOPE sollte NICHT die Namespace-Deklaration enthalten: `xmlns:xml=http://www.w3.org/XML/1998/namespace.`
R1109	Der Wert des SOAPAction HTTP-Header-Feldes in einer HTTP-Anforderung MESSAGE MUSS eine Zeichenfolge in Anführungszeichen sein.

Regel	Beschreibung
R1111	Eine INSTANCE SOLL einen 200-OK-HTTP-Statuscode für eine Antwortnachricht verwenden, die einen Envelope enthält, der kein Fehler ist.
R1126	Eine INSTANCE MUSS einen HTTP-Statuscode 500 Internal Server Error zurückgeben, wenn der Antwort-Envelope ein Fehler ist.
R1132	Eine HTTP-Anforderung MESSAGE MUSS die HTTP POST-Methode verwenden.
R1140	Eine Nachricht sollte mit HTTP/1.1 gesendet werden.
R1141	Eine MESSAGE MUSS mit HTTP/1.1 oder HTTP/1.0 gesendet werden.
R2113	Ein Envelope MUSS NICHT das soapenc:arrayType -Attribut enthalten.
R2211	Ein Envelope, der mit einer rpc-Literal Bindung beschrieben wurde, MUSS NICHT das xsi:nil -Attribut mit dem Wert 1 oder true für die Teile-Accessoren haben.
R2714	Bei unidirektionalen Operationen darf eine INSTANCE NICHT eine HTTP-Antwort zurückgeben, die einen Envelope enthält. Insbesondere muss der HTTP-Antwort-Entity-Body leer sein.
R2729	Ein Envelope, der mit einer rpc-Literal Bindung beschrieben wird, die eine Antwort ist, MUSS ein Wrapper-Element haben, dessen Name der entsprechende wsdl:Operationsname ist, der mit dem StringResponse versehen ist.
R2735	Ein Envelope, der mit einer rpc-Literal Bindung beschrieben wird, MUSS die Teilzugriffselemente für Parameter und Rückgabewerte in keinem Namespace platzieren.

Regel	Beschreibung
R2738	Ein Envelope MUSS alle soapbind:Header enthalten, die auf einer wsdl:input oder wsdl:output einer wsdl:operation einer wsdl:binding angegeben sind, die sie beschreibt.
R2740	Eine wsdl:Bindung in einer DESCRIPTION sollte ein soapbind:fault enthalten, der jeden bekannten Fehler beschreibt.
R2744	Eine HTTP-Anforderung MESSAGE MUSS ein SOAPAction-HTTP-Header-Feld mit einem in Anführungszeichen angegebenen Wert enthalten, der dem Wert des soapAction-Attributs von soapbind:operation entspricht, falls in der entsprechenden WSDL-Beschreibung vorhanden ist.

Überprüfung der XML-Nachrichtenüberprüfung

August 19, 2021

Die Überprüfung der XML-Nachrichtenüberprüfung prüft Anforderungen, die XML-Nachrichten enthalten, um sicherzustellen, dass sie gültig sind. Wenn eine Anforderung eine ungültige XML-Nachricht enthält, blockiert die Web App Firewall die Anforderung. Der Zweck der XML-Validierungsprüfung besteht darin, einen Angreifer daran zu hindern, speziell konstruierte ungültige XML-Nachrichten zu verwenden, um die Sicherheit Ihrer Anwendung zu verletzen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-Nachrichtenüberprüfung ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren und Statistiken aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Nachrichtenüberprüfungsprüfung zu konfigurieren:

- `set appfw profile <name> -xmlValidationAction [**block**] [**log**] [**stats**] [**none**]`

Sie müssen die GUI verwenden, um die anderen Einstellungen für die Überprüfung der XML-Gültigkeitsprüfung zu konfigurieren. Im Dialogfeld Überprüfung der XML-Nachrichtenüberprüfung

ändern können Sie auf der Registerkarte
Prüfungen die folgenden Einstellungen konfigurieren:

- **XML-Nachrichtenüberprüfung.** Verwenden Sie eine der folgenden Optionen, um die XML-Nachricht zu validieren:
  - **SOAP-Umschlag.** Überprüfen Sie nur den SOAP-Umschlag von XML-Nachrichten.
  - **WSDL.** Validieren von XML-Nachrichten mithilfe einer XML-SAAP-WSDL. Wenn Sie WSDL-Validierung wählen, müssen Sie in der Dropdownliste WSDL-Objekt eine WSDL auswählen. Wenn Sie mit einer WSDL überprüfen möchten, die noch nicht in die Web App Firewall importiert wurde, können Sie auf die Schaltfläche Importieren klicken, um das Dialogfeld WSDL-Importe verwalten zu öffnen und Ihre WSDL zu importieren. Weitere Informationen finden Sie unter WSDL .
    * Wenn Sie die gesamte URL validieren möchten, lassen Sie das Optionsfeld Absolut im Schaltflächenfeld Endpunktprüfung aktiviert. Wenn Sie nur den Teil der URL nach dem Host überprüfen möchten, aktivieren Sie das Optionsfeld Relativ.
    * Wenn Sie möchten, dass die Web App Firewall die WSDL strikt durchsetzen und keine zusätzlichen XML-Header zulassen, die nicht in der WSDL definiert sind, müssen Sie das Kontrollkästchen Zusätzliche Header zulassen, die nicht in der WSDL definiert sind.

      Achtung: Wenn Sie das Kontrollkästchen Zusätzliche Kopfzeilen
      zulassen, die nicht in der WSDL definiert sind, deaktivieren und Ihre WSDL nicht alle XML-Header definiert, die Ihre geschützte XML-Anwendung oder Web 2.0-Anwendung erwartet oder die ein Client sendet, können Sie den legitimen Zugriff auf Ihren geschützten Dienst sperren.
  - **XML-Schema.** Validieren von XML-Nachrichten mithilfe eines XML-Schemas. Wenn Sie die XML-Schemaüberprüfung wählen, müssen Sie in der Dropdownliste XML-Schemaobjekt ein XML-Schema auswählen. Wenn Sie ein XML-Schema überprüfen möchten, das noch nicht in die Web App Firewall importiert wurde, können Sie auf die Schaltfläche Importieren klicken, um das Dialogfeld XML-Schemaimporte verwalten zu öffnen und Ihre WSDL zu importieren. Weitere Informationen finden Sie unter WSDL .
- **Antwortvalidierung.** Standardmäßig versucht die Web App Firewall nicht, Antworten zu validieren. Wenn Sie Antworten von Ihrer geschützten Anwendung oder Website 2.0-Website validieren möchten, aktivieren Sie das Kontrollkästchen Antwort überprüfen. Wenn Sie dies tun, werden das Kontrollkästchen XML-Schema wiederverwenden, das in der Anforderungsüberprüfung angegeben wurde, und die Dropdownliste XML-Schemaobjekt aktiviert.
  - Aktivieren Sie das Kontrollkästchen XML-Schema wiederverwenden, um das für die Anforderungsvalidierung angegebene Schema auch zur Antwortvalidierung zu verwenden.
    Hinweis: Wenn Sie dieses Kontrollkästchen aktivieren, ist die Dropdownliste
    XML-Schemaobjekt ausgegraut.
  - Wenn Sie ein anderes XML-Schema für die Antwortüberprüfung verwenden möchten, ver-

wenden Sie die Dropdownliste XML-Schemaobjekt, um dieses XML-Schema auszuwählen oder hochzuladen.

XML-SOAP-Fehlerfilterprüfung

January 19, 2021

Die XML-SOAP-Fehlerfilterungsprüfung untersucht Antworten Ihrer geschützten Webdienste und filtert XML-SOAP-Fehler heraus. Dadurch wird verhindert, dass vertrauliche Informationen an Angreifer auslaufen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-SOAP-Fehlerfilterungsprüfung ändern auf der Registerkarte **Allgemein die** Aktionen Blockieren, Protokollieren und Statistiken sowie die Aktion Entfernen aktivieren oder deaktivieren, mit der SOAP-Fehler entfernt werden, bevor die Antwort an den Benutzer weitergeleitet wird.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-SOAP-Fehlerfilterungsprüfung zu konfigurieren:

```
set appfw profile <name> -XMLSOAPFaultAction [block] [log] [stats] [none]
```

Sie können keine Ausnahmen für die XML-SOAP-Fehlerfilterprüfung konfigurieren. Sie können es nur aktivieren oder deaktivieren.

JSON-Schutzprüfungen

May 11, 2023

NetScaler Web App Firewall schützt Ihre JSON-Anwendungen vor DoS-, SQL- oder Cross-Site-Scripting-Angriffen auf Inhaltsebene. Wenn es bei einer JSON-Anforderung zu einem DoS-, SQL- oder Cross-Site-Scripting-Angriff kommt, müssen Sie Ihre Anwendung schützen, indem Sie Grenzwerte für JSON-Strukturen wie Arrays und Zeichenketten konfigurieren.

> **Hinweis:**
>
> Die JSON-Sicherheitsprüfungen gelten nur für Inhalte, die mit einem JSON-Inhaltstype-Header gesendet werden. Wenn der Content-Type-Header fehlt oder auf einen anderen Wert gesetzt ist, werden alle JSON-Sicherheitsprüfungen umgangen. Wenn Sie Ihre JSON-Anwendungen schützen möchten, müssen die Webmaster jedes Webservers, der diese Anwendungen hostet,

> sicherstellen, dass ein geeigneter JSON-Inhaltstype-Header gesendet wird.
>
> Die Lernfunktion unterstützt JSON-SQL, Cross-Site-Scripting und DOS-Inhaltstypen nicht.

JSON-Denial-of-Service-Schutzprüfung

May 11, 2023

Die JSON-Denial-of-Service (DoS) -Prüfung untersucht eine eingehende JSON-Anforderung und prüft, ob Daten vorhanden sind, die den Merkmalen eines DoS-Angriffs entsprechen. Wenn die Anforderung JSON-Verstöße hatte, blockiert die Appliance die Anforderung, protokolliert die Daten, sendet eine SNMP-Warnung und zeigt auch eine JSON-Fehlerseite an. Der Zweck der JSON-DoS-Prüfung besteht darin, zu verhindern, dass ein Angreifer eine JSON-Anfrage sendet, um DoS-Angriffe auf Ihre JSON-Anwendungen oder Ihre Website zu starten.

Wenn ein Client eine Anforderung an eine NetScaler Appliance sendet, analysiert der JSON-Parser die Anforderungsnutzlast. Wenn eine Verletzung beobachtet wird, setzt die Appliance Einschränkungen für die JSON-Struktur durch. Die Einschränkung erzwingt eine Größenbeschränkung für die JSON-Anforderung. Wenn eine JSON-Verletzung festgestellt wurde, führt die Appliance daher eine Aktion aus und antwortet mit der JSON-Fehlerseite.

JSON-DoS-Regeln

Wenn die Appliance eine JSON-Anforderung erhält, erzwingt der JSON-DOS-Schutz die Größenbeschränkung für die folgenden DoS-Parameter in der Anforderungsnutzlast.

1. maximale Tiefe: Maximale Verschachtelung (Tiefe) des JSON-Dokuments. Diese Prüfung schützt vor Dokumenten mit übermäßiger Hierarchietiefe.
2. maximale Dokumentlänge: Maximale Dokumentlänge des JSON-Dokuments.
3. maximale Array-Länge: Maximale Array-Länge in einem beliebigen JSON-Objekt. Diese Prüfung schützt vor Arrays mit großen Längen.
4. maximale Stringlänge: Maximale Stringlänge im JSON. Diese Prüfung schützt vor Saiten mit großer Länge.
5. maximum object key count: Maximale Anzahl von Schlüsseln in einem beliebigen JSON-Objekt. Diese Prüfung schützt vor Objekten mit einer großen Anzahl von Schlüsseln.
6. maximale Objektschlüssellänge: Maximale Schlüssellänge in einem beliebigen JSON-Objekt. Diese Prüfung schützt vor Objekten mit großen Schlüsseln.

Es folgt eine Liste von JSON-DoS-Regeln, die während des JSON-Parsens validiert wurden.

1. JSONMaxContainerDepth. Diese Prüfung kann aktiviert werden, indem die JsonMaxContainerDepth-Prüfung konfiguriert wird und standardmäßig ist die Option OFF.

2. JSONMaxContainerDepth. Diese Prüfung kann durch die konfigurierbare Option jsonMaxContainerDepthCheck aktiviert/deaktiviert werden und der Standardwert kann mit der Option jsonMaxContainerDepth geändert werden. Sie können die Höchstwerte jedoch auf einen Wert zwischen 1 und 127 variieren. Standardwert: 5, Mindestwert: 1, Maximalwert: 127
3. JSONMaxDocumentLength. Diese Prüfung kann aktiviert werden, indem die JsonMaxDocumentLength-Prüfung konfiguriert wird und die Standardoption ist OFF.
4. JSONMaxDocumentLength. Diese Prüfung kann durch Konfigurieren der JsonMaxDocumentLength-Prüfung aktiviert werden, und die Standardlänge ist auf 20000000 Byte festgelegt. Mindestwert: 1, Maximalwert: 2147483647
5. JSONMaxObjectKeyCount. Die Regel überprüft, ob die Überprüfung der maximalen JSON-Objektschlüsselanzahl ein- oder ausgeschaltet ist. Mögliche Werte: ON, OFF, Standardwert: OFF
6. JSONMaxObjectKeyCount. Diese Prüfung kann aktiviert werden, indem die JsonMaxObjectKeyCount-Prüfung konfiguriert wird. Die Prüfung schützt vor Objekten mit einer großen Anzahl von Schlüsseln, und der Standardwert ist auf 1000 Byte festgelegt. Mindestwert: 0, Maximalwert: 2147483647
7. JSONMaxObjectKeyLength. Diese Prüfung kann durch Konfigurieren der JsonMaxObjectKeyLength-Prüfung aktiviert werden. Die Regel überprüft, ob die Überprüfung der maximalen JSON-Objektschlüssellänge ein- oder ausgeschaltet ist. Standardmäßig ist es ausgeschaltet.
8. JSONMaxObjectKeyLength. Der Scheck schützt vor Objekten mit großer Schlüssellänge. Standardwert: 128. Mindestwert: 1, Maximalwert: 2147483647
9. JSONMaxArrayLength. Die Regel überprüft, ob die Prüfung der maximalen JSON-Array-Länge EIN oder AUS ist. Standardmäßig ist es ausgeschaltet.
10. JSONMaxArrayLength. Die Prüfung schützt vor Arrays mit großen Längen. Standardmäßig ist der Wert auf 10000 festgelegt. Mindestwert: 1, Maximalwert: 2147483647
11. JSONMaxStringLength. Diese Prüfung kann durch Konfigurieren der JsonMaxStringLength-Prüfung aktiviert werden. Die Prüfung prüft, ob die maximale JSON-Stringlänge EIN oder AUS ist. Standardmäßig ist es ausgeschaltet.
12. JSONMaxStringLength. Der Scheck schützt vor Saiten mit großer Länge. Standardmäßig ist es auf 1000000 eingestellt. Mindestwert: 1, Maximalwert: 2147483647

Konfigurieren der JSON-DoS-Schutzprüfung

Um den JSON-DoS-Schutz zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Anwendungs-Firewall-Profil für JSON hinzufügen.
2. Legen Sie das Anwendungs-Firewall-Profil für JSON-DoS-Einstellungen

3. Konfigurieren Sie JSON-DoS-Variablen, indem Sie das Anwendungsfirewall-Profil binden

Anwendungs-Firewall-Profil für JSON-DoS-Schutz hinzufügen

Sie müssen zuerst ein Profil erstellen, das angibt, wie die Anwendungsfirewall Ihre JSON-Webinhalte vor JSON-DoS-Angriffen schützen muss.
Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Hinweis*:
>
> Wenn Sie den Profiltyp auf JSON festlegen, sind andere Prüfungen wie HTML oder XML nicht anwendbar.

Beispiel

```
add appfw profile profile1 -type JSON
```

Festlegen des Anwendungs-Firewall-Profils für JSON-DoS-Schutz

Sie müssen das Profil für eine oder mehrere JSON-DoS-Aktionen und das JSON-DoS-Fehlerobjekt konfigurieren, die im Anwendungs-Firewall-Profil festgelegt werden sollen.
Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <name> -JSONDoSAction [block] | [log] | [stats] | [none]
```

Blockieren — Blockieren Sie Verbindungen, die gegen diese Sicherheitsüberprüfung verstoßen.
Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.
Statistiken - Generieren Sie Statistiken für diese Sicherheitsüberprüfung.
Keine — Deaktiviert alle Aktionen für diese Sicherheitsüberprüfung.

> *Hinweis*:
>
> Um eine oder mehrere Aktionen zu aktivieren, geben Sie “set appfw profile -jsondosAction” ein, gefolgt von den zu aktivierenden Aktionen.

Beispiel

```
set appfw profile profile1 -JSONDoSAction block log stat
```

Konfigurieren von DoS-Variablen durch Bindung des Anwendungs-Firewall-

Um JSON-DoS-Schutz bereitzustellen, müssen Sie das Anwendungs-Firewall-Profil mit den JSON-DoS-Einstellungen binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile <name> -JSONDoSURL <expression> [-JSONMaxContainerDepthCheck
 ( ON | OFF )[-JSONMaxContainerDepth <positive_integer>]] [-JSONMaxDocumentLengthChec
 ( ON | OFF )[-JSONMaxDocumentLength <positive_integer>]] [-JSONMaxObjectKeyCountChec
 ( ON | OFF )[-SONMaxObjectKeyCount <positive_integer>]] [-JSONMaxObjectKeyLengthChec
 ( ON | OFF )[-JSONMaxObjectKeyLength <positive_integer>]] [-JSONMaxArrayLengthCheck
 ( ON | OFF )[-JSONMaxArrayLength <positive_integer>]] [-JSONMaxStringLengthCheck
 ( ON | OFF )[-JSONMaxStringLength <positive_integer>]]
```

Beispiel

```
bind appfw profile profile1 -JSONDoSURL ".*" -JSONMaxContainerDepthCheck ON
```

> *Hinweis*:
>
> Die JSON-DoS-Prüfungen sind nur anwendbar, wenn der Profiltyp als JSON ausgewählt ist. Außerdem werden SQL, Cross-Site Scripting, Feldformat und Formularfeldsignaturen bei JSON-Profilen auf Abfrageparameter angewendet.

JSON-Fehlerseite importieren

Wenn eine eingehende Anforderung einen DoS-Angriff hatte und Sie die Anforderung blockieren, zeigt die Appliance eine Fehlermeldung an. Um dies zu tun, müssen Sie die JSON-Fehlerseite importieren. Geben Sie in der Befehlszeile Folgendes ein:

```
import appfw jsonerrorpage <src> <name> [-comment <string>] [-overwrite]
```

Hierbei gilt:

src. URL (Protokoll, Host, Pfad und Name) für den Speicherort, an dem das importierte JSON-Fehlerobjekt gespeichert werden soll.

> *Hinweis*:
>
> Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, für den Zugriff eine Clientzertifikatauthentifizierung erforderlich ist Dies ist ein zwingendes Argument. Maximale Länge: 2047

Name. Name, der dem JSON-Fehlerobjekt auf dem NetScaler zugewiesen werden soll. Dies ist ein zwingendes Argument. Maximale Länge: 31
Kommentar. Kommentare, um Informationen über das JSON-Fehlerobjekt beizubehalten. Maximale Länge: 255
überschreiben. Überschreiben Sie jedes vorhandene JSON-Fehlerobjekt mit demselben Namen.

Beispiel-Konfiguration

```
Add appfw prof profjson - type JSON
Bind appfw prof profjson - JSONDoSURL ".*" -
    JSONMaxDocumentLengthCheck ON -JSONMaxDocumentLength 30 -
    JSONMaxContainerDepthCheck ON -JSONMaxContainerDepth 3
    JSONMaxObjectKeyCountCheck ON -JSONMaxObjectKeyCount 4 -
    JSONMaxObjectKeyLengthCheck ON -JSONMaxObjectKeyLength 10 -
    JSONMaxArrayLengthCheck ON -JSONMaxArrayLength 5 -
    JSONMaxStringLengthCheck ON -JSONMaxStringLength 30
<!--NeedCopy-->
```

Beispiel für Nutzlasten, Protokollmeldungen und Zähler:

JSONMaxDocumentLength Violation

JSONMaxDocumentLength: 30
Payload: {"a":"A","b":"B","c":"C","d":"D","e":"E"}

Protokollmeldung:

```
Document Length exceeds 20000000 May 29 20:23:32 <local0.info>
    10.217.31.243 05/29/2019:20:23:32 GMT 0-PPE-0 : default APPFW
    APPFW_JSON_DOS_MAX_DOCUMENT_LENGTH 136 0 : 10.217.32.134 114-PPE0 -
    profjson http://10.217.30.120/forms/login.html Document exceeds
    maximum document length (30). cn1=30467 cn2=115 cs1=profjson cs2=
    PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
1 0 6 as_viol_json_dos
2 0 3 as_viol_json_dos_max_document_length
3 0 6 as_log_json_dos
4 0 3 as_log_json_dos_max_document_length
5 0 6 as_viol_json_dos_profile appfw__(profile1)
6 0 3 as_viol_json_dos_max_document_length_profile appfw__(profile1)
7 0 6 as_log_json_dos_profile appfw__(profile1)
8 0 3 as_log_json_dos_max_document_length_profile appfw__(profile1)
<!--NeedCopy-->
```

JSONMaxContainerDepth Violation

JSONMaxContainerDepth: 3
Payload: {"a": {"b": {"c": {"d": { "e" : "f" }}}}}

Protokollmeldung:

```
May 29 19:33:59 <local0.info> 10.217.31.243 05/29/2019:19:33:59 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_CONTAINER_DEPTH 4626 0 : 10.217.31.247 22-PPE1 - profjson http://10.217.30.120/forms/login.html Document at offset (15) exceeds maximum container depth (3). cn1=30466 cn2=113 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
36 20999 7 1 0 as_viol_json_dos
37 0 6 1 0 as_viol_json_dos_max_container_depth
38 0 7 1 0 as_log_json_dos
39 0 6 1 0 as_log_json_dos_max_container_depth
40 0 7 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 6 1 0 as_viol_json_dos_max_container_depth_profile appfw__(profile1)
42 0 7 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 6 1 0 as_log_json_dos_max_container_depth_profile appfw__(profile1)
<!--NeedCopy-->
```

JSONMaxObjectKeyCount Violation

JSONMaxObjectKeyCount: 4

Payload: {“a”: ”A”, “b”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Protokollmeldung:

```
May 30 19:42:41 <local0.info> 10.217.31.243 05/30/2019:19:42:41 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_COUNT 457 0 : 10.217.32.134 219-PPE1 - profjson http://10.217.30.120/forms/login.html Object at offset (41) that exceeds maximum key count (4). cn1=30468 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
94 119105 15 1 0 as_viol_json_dos
95 0 4 1 0 as_viol_json_dos_max_object_key_count
96 0 15 1 0 as_log_json_dos
97 0 4 1 0 as_log_json_dos_max_object_key_count
98 0 15 1 0 as_viol_json_dos_profile appfw__(profile1)
```



```
99 0 4 1 0 as_viol_json_dos_max_object_key_count_profile appfw__(
    profile1)
100 0 15 1 0 as_log_json_dos_profile appfw__(profile1)
101 0 4 1 0 as_log_json_dos_max_object_key_count_profile appfw__(
    profile1)
<!--NeedCopy-->
```

JSONMaxObjectKeyLength Violation

JSONMaxObjectKeyLength: 10
Payload: {“a”: ”A”, “b1234567890”: “B”, “c”:“C”, “d” :“D”, ”e” : “E” }

Protokollmeldung:

```
May 31 20:26:10 <local0.info> 10.217.31.243 05/31/2019:20:26:10 GMT 0-
    PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_LENGTH 102 0 :
    10.217.32.134 89-PPE1 - profjson http://10.217.30.120/forms/login.
    html Object key(b1234567890) at offset (12) exceeds maximum key
    length (10). cn1=30469 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5
    =2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
242172 6 1 0 as_viol_json_dos
0 1 1 0 as_viol_json_dos_max_object_key_length
10 0 5 1 0 as_log_json_dos
11 0 1 1 0 as_log_json_dos_max_object_key_length
12 0 6 1 0 as_viol_json_dos_profile appfw__(profile1)
13 0 1 1 0 as_viol_json_dos_max_object_key_length_profile appfw__(
    profile1)
14 0 5 1 0 as_log_json_dos_profile appfw__(profile1)
15 0 1 1 0 as_log_json_dos_max_object_key_length_profile appfw__(
    profile1)
<!--NeedCopy-->
```

JSONMaxArrayLength Violation

JSONMaxArrayLength: 5
Payload: {“a”: ”A”, “c”:[”d”,”e”,”f”,”g”,”h”,”i”],”e”:[“E”,”e”]}

Protokollmeldung:


```
May 29 20:58:39 <local0.info> 10.217.31.243 05/29/2019:20:58:39 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_ARRAY_LENGTH 4650 0 : 10.217.32.134 153-PPE1 -profjson http://10.217.30.120/forms/login.html Array at offset (37) that exceeds maximum array length (5). cn1=30469 cn2=120 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
36 182293 10 1 0 as_viol_json_dos
37 0 1 1 0 as_viol_json_dos_max_array_length
38 0 10 1 0 as_log_json_dos 39 0 1 1 0 as_log_json_dos_max_array_length
40 0 10 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 1 1 0 as_viol_json_dos_max_array_length_profile appfw__(profile1)
42 0 10 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 1 1 0 as_log_json_dos_max_array_length_profile appfw__(profile1))
<!--NeedCopy-->
```

JSONMaxStringLength Violation

JSONMaxStringLength: 10

Payload: {“a”: ”A”, “c”:”CcCcCcCcCcCcCcCcCc”,”e”:[“E”,”e”]}

Protokollmeldung:

```
May 29 20:05:02 <local0.info> 10.217.31.243 05/29/2019:20:05:02 GMT 0-PPE-0 : default APPFW APPFW_JSON_DOS_MAX_STRING_LENGTH 134 0 : 10.217.32.134 80-PPE0 - profjson http://10.217.30.120/forms/login.html String(CcCcCcCcCcCcCc) at offset (27) that exceeds maximum string length (10). n1=30470 cn2=122 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

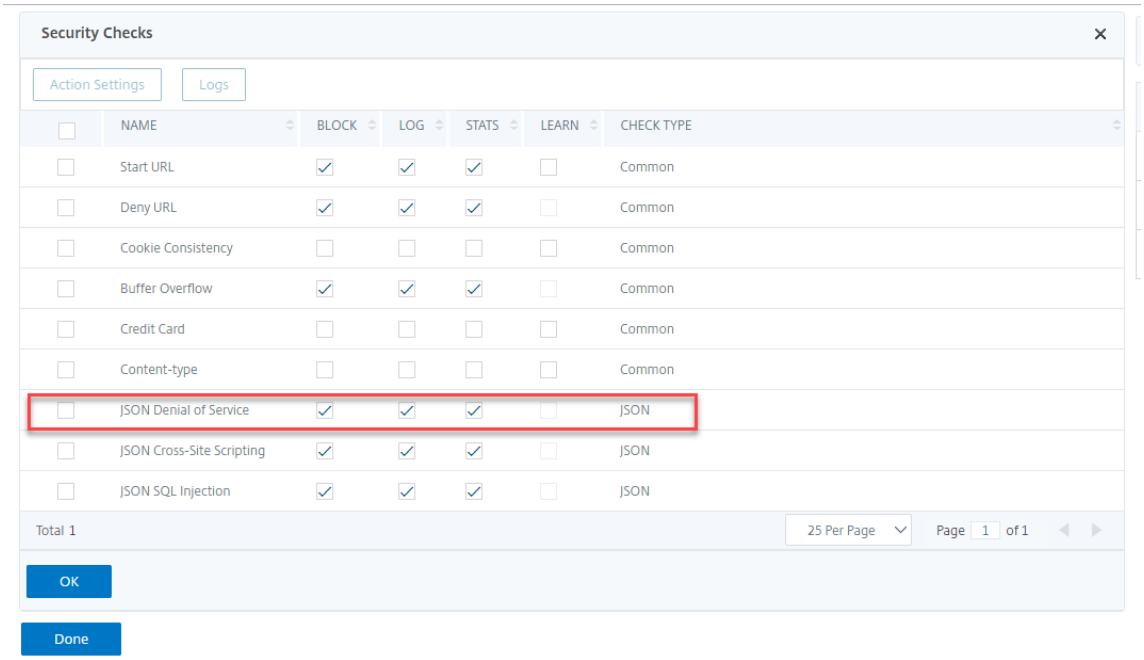
Zähler:

```
44 91079 3 1 0 as_viol_json_dos
45 0 1 1 0 as_viol_json_dos_max_string_length
46 0 3 1 0 as_log_json_dos
47 0 1 1 0 as_log_json_dos_max_string_length
48 0 3 1 0 as_viol_json_dos_profile appfw__(profile1)
49 0 1 1 0 as_viol_json_dos_max_string_length_profile appfw__(profile1)
50 0 3 1 0 as_log_json_dos_profile appfw__(profile1)
51 0 1 1 0 as_log_json_dos_max_string_length_profile appfw__(profile1
<!--NeedCopy-->
```

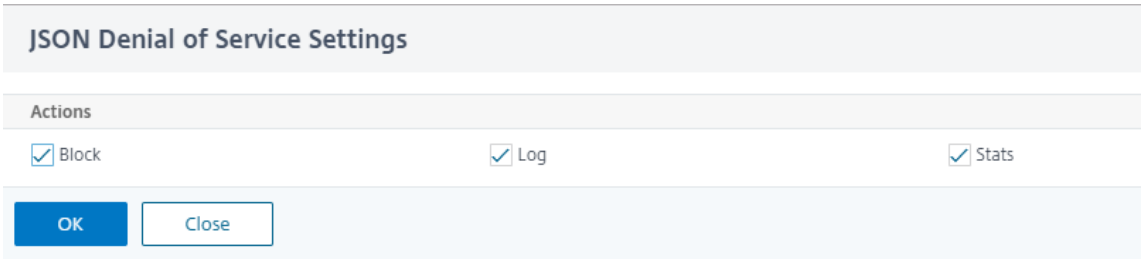

Konfigurieren Sie den JSON-DoS-Schutz mithilfe der GUI

Gehen Sie wie folgt vor, um die JSON-DoS-Schutzeinstellungen festzulegen.

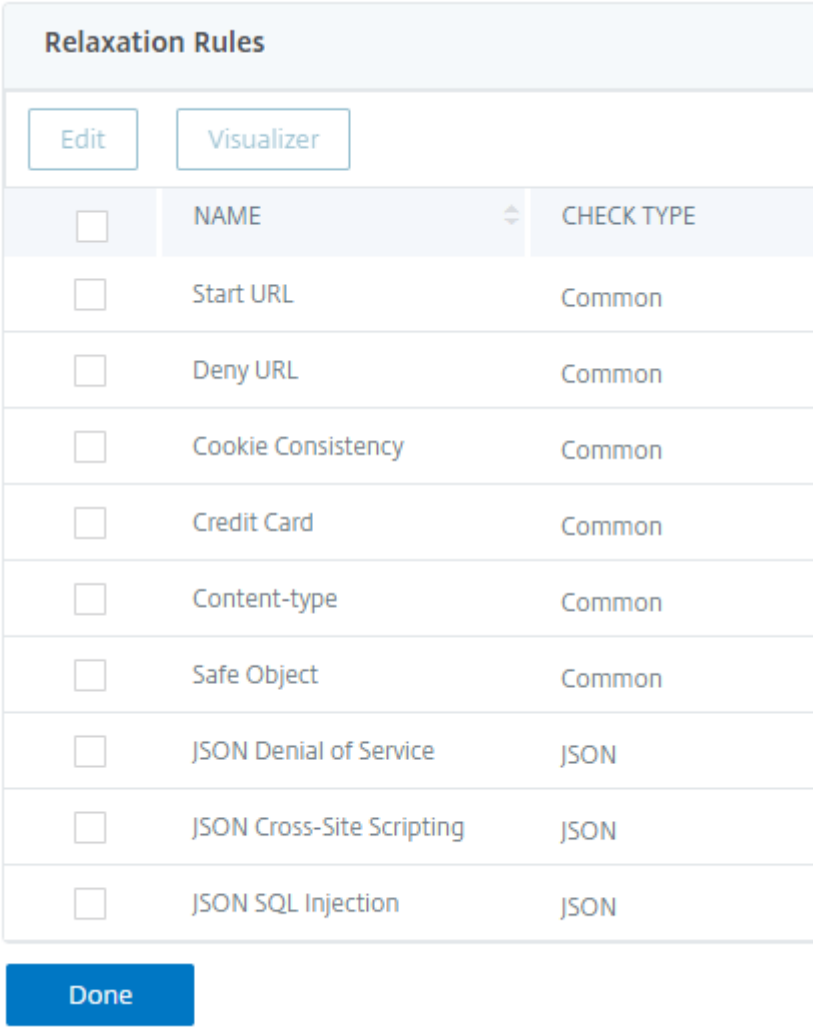
1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall Profilseiteunter Erweiterte Einstellungen auf Sicherheitsprüfungen**.
4. Gehen Sie im Abschnitt **Sicherheitsüberprüfungen** zu den **JSON-Denial-of-Service-Einstellungen** .
5. Klicken Sie neben dem Kontrollkästchen auf das Symbol der ausführbaren



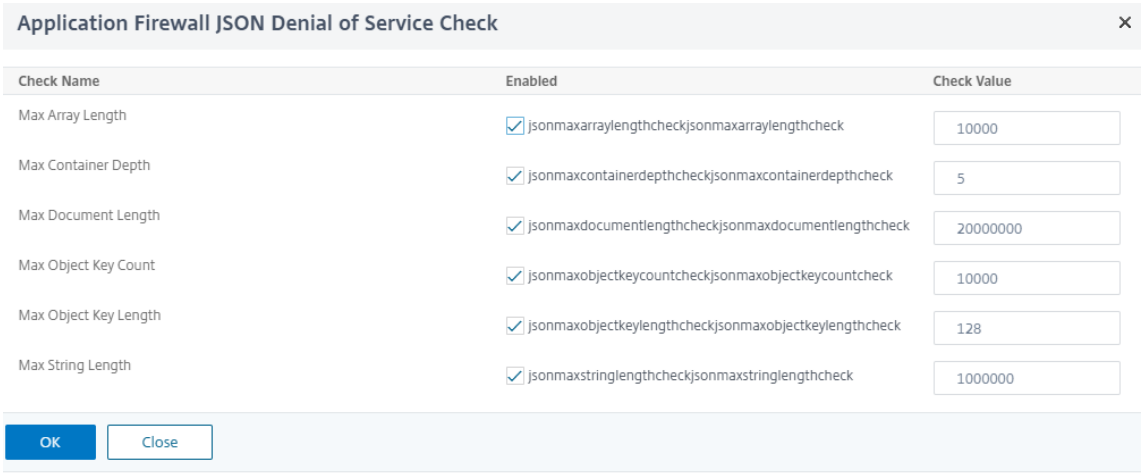
6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON-Denial-of-Service-Einstellungen** aufzurufen.
7. Wählen Sie die JSON-DoS-Aktion aus.
8. Klicken Sie auf **OK**.



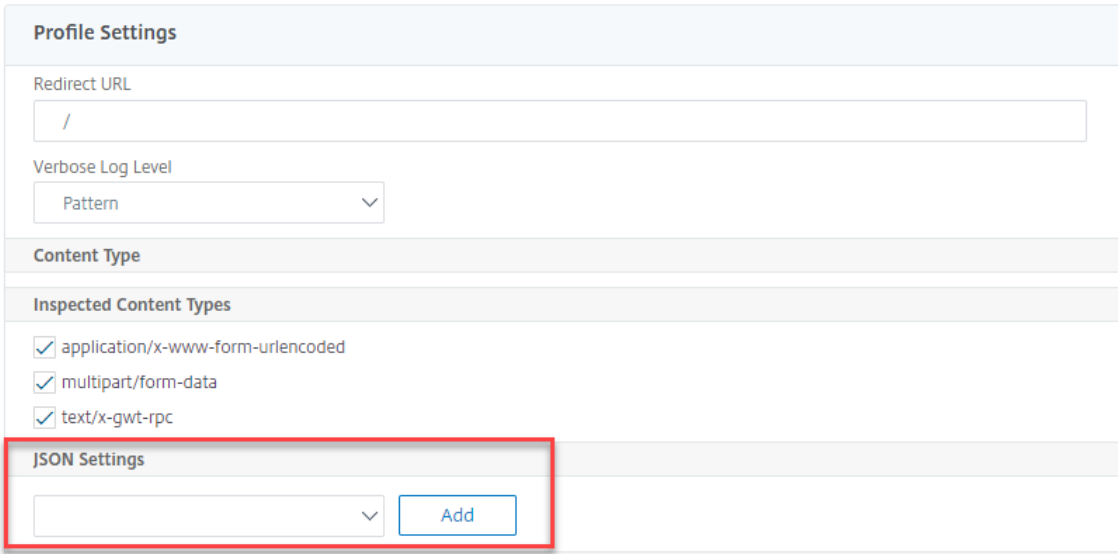
9. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Entspannungsregeln**.
10. Wählen Sie im Abschnitt **Entspannungsregeln** die **JSON-Denial-of-Service-Einstellungen aus** und klicken Sie auf **Bearbeiten**.



11. Legen **Sie in der Application Firewall JSON Denial of Service Check** die JSON-DoS-Validierungswerte fest.
12. Klicken Sie auf **OK**.

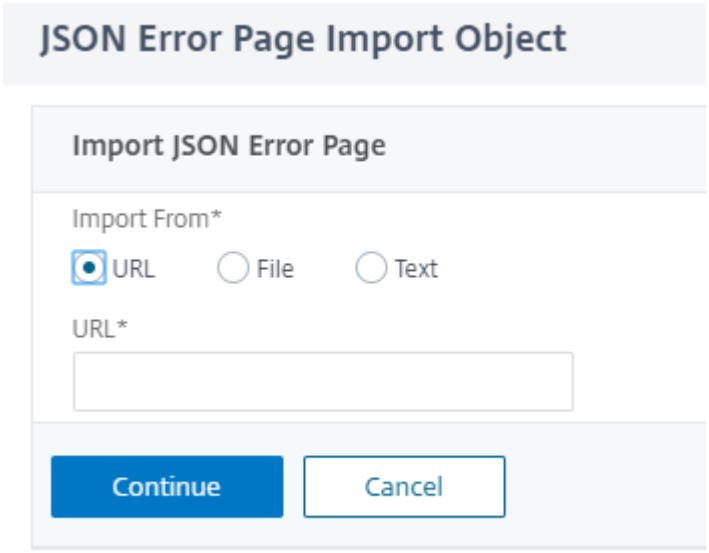


13. Klicken Sie auf der **NetScaler Web App Firewall Profilseite** unter **Erweiterte**Einstellungen auf Profileinstellungen**.
14. Gehen Sie im Abschnitt **Profileinstellungen** zum Unterabschnitt **JSON-Fehlereinstellungen**, um die **JSON-DoS-Fehlerseite** festzulegen.



15. Legen Sie auf der **Seite "Objekt importieren" der JSON-Fehlerseite** die folgenden Parameter fest:

    a) Importieren aus. Importieren Sie die Fehlerseite als Text, Datei oder URL.
    b) URL. URL, um den Benutzer auf die Fehlerseite umzuleiten.
    1 Datei. Wählen Sie eine Datei aus, die als JSON-DoS-Fehlerdatei importiert werden soll.
    c) Text. Geben Sie den Inhalt der JSON-Datei ein.
    d) Klicken Sie auf Weiter.
    e) Datei. Geben Sie den Dateinamen ein.
    f) Inhalt der Datei. Fügen Sie den Inhalt der Fehlerdatei hinzu.
    g) Klicken Sie auf **OK**.



16. Klicken Sie auf **OK**.
17. Klicken Sie auf **Fertig**.

JSON-SQL-Einschleusungsschutzprüfung

May 11, 2023

Eine eingehende JSON-Anforderung kann eine SQL-Einschleusung in Form von partiellen SQL-Abfragezeichenfolgen oder nicht autorisierten Befehlen im Code enthalten. Dies führt zum Diebstahl von Daten aus der JSON-Datenbank Ihrer Webserver. Nach Erhalt einer solchen Anfrage blockiert die Appliance eine solche Anfrage zum Schutz Ihrer Daten.

Stellen Sie sich ein Szenario vor, in dem ein Client eine JSON-SQL-Anforderung an eine NetScaler Appliance sendet, der JSON-Parser die Anforderungsnutzlast analysiert und wenn eine SQL-Einschleusung beobachtet wird, setzt die Appliance Einschränkungen für den JSON-SQL-Inhalt durch. Die Einschränkung erzwingt eine Größenbeschränkung für die JSON-SQL-Anforderung. Wenn eine JSON-SQL-Einschleusung beobachtet wird, führt die Appliance daher eine Aktion aus und antwortet mit der JSON-SQL-Fehlerseite.

Konfigurieren des JSON-SQL-Einschleusungsschutz

Um den JSON-SQL-Schutz zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie das Anwendungsfirewall-Profil als JSON hinzu.
2. Festlegen des Anwendungs-Firewall-Profils für JSON SQL Injection-Einstellungen

3. Konfigurieren Sie die JSON-SQL-Aktion, indem Sie das Anwendungs-Firewall-

Anwendungs-Firewall-Profil vom Typ JSON hinzufügen

Sie müssen zuerst ein Profil erstellen, das angibt, wie die Anwendungsfirewall Ihre JSON-Webinhalte vor JSON-SQL-Einschleusung-Angriffen schützen muss.
Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Hinweis*:
>
> Wenn Sie den Profiltyp auf JSON festlegen, sind andere Prüfungen wie HTML oder XML nicht anwendbar.

Beispiel

```
add appfw profile profile1 -type JSON
```

Konfigurieren der Aktion JSON SQL Injection

Sie müssen eine oder mehrere JSON SQL Injection-Aktionen konfigurieren, um Ihre Anwendung vor JSON-SQL-Einschleusung-Angriffen zu schützen.
Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <name> - JSONSQLInjectionAction [block] [log] [stats] [
none]
```

Die SQL-Einschleusung-Aktionen sind:
Blockieren — Verbindungen blockieren, die diese Sicherheitsüberprüfung verletzen.
Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.
Statistiken - Generieren Sie Statistiken für diese Sicherheitsüberprüfung.
Keine — Deaktiviert alle Aktionen für diese Sicherheitsüberprüfung.

Konfigurieren des Typs JSON SQL Injection

Um den Typ JSON SQL Injection in einem Anwendungs-Firewall-Profil zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <name> - JSONSQLInjectionType <JSONSQLInjectionType>
```

Beispiel

```
set appfw profile profile1 -JSONSQLInjectionType SQLKeyword
```


Wo die verfügbaren SQL Injection-Typen sind:
Verfügbare SQL-Einschleusung-Typen.
SQLSplChar. Sucht nach SQL-Sonderzeichen,
SqlKeyword. Sucht nach SQL-Schlüsselwörtern.
SQLSplCharANDKeyword. Prüft auf beides und blockiert, falls gefunden.
SQLSplCharORKeyword. . Sperrt, wenn ein SQL-Sonderzeichen oder ein SPL-Schlüsselwort gefunden
Mögliche Werte: SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword.

> *Hinweis*:
> Um eine oder mehrere Aktionen zu aktivieren, geben Sie “set appfw profile - jsonSqlInjectionAction” ein, gefolgt von den zu aktivierenden Aktionen.

Beispiel

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

Das folgende Beispiel zeigt eine Beispielnutzlast, die entsprechende Protokollnachricht und Statistikzähler:

```
Payload:
=======
{

  "test": "data",
  "username": "waf",
  "password": "select * from t1;",
  "details": {

    "surname": "test",
    "age": "23"
   }

 }


Log Message:
============
08/19/2019:08:49:46 GMT pegasus121 Informational 0-PPE-0 : default
   APPFW APPFW_JSON_SQL 6656 0 :  10.217.32.165 18402-PPE0 - profjson
   http://10.217.32.147/test.html SQL Keyword check failed for object
   value(with violation="select(;)") starting at offset(52) <blocked>
Counters:
========
   1  441083             1 as_viol_json_sql
```

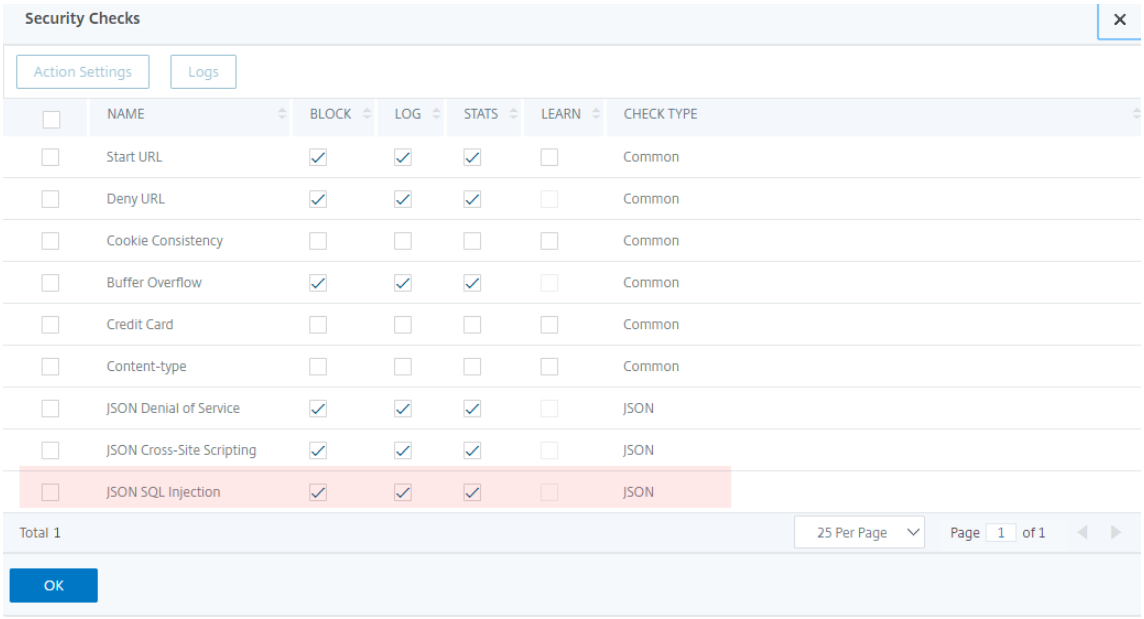


```
    3       0              1 as_log_json_sql
    5       0              1 as_viol_json_sql_profile appfw__(profjson)
    7       0              1 as_log_json_sql_profile appfw__(profjson)
<!--NeedCopy-->
```

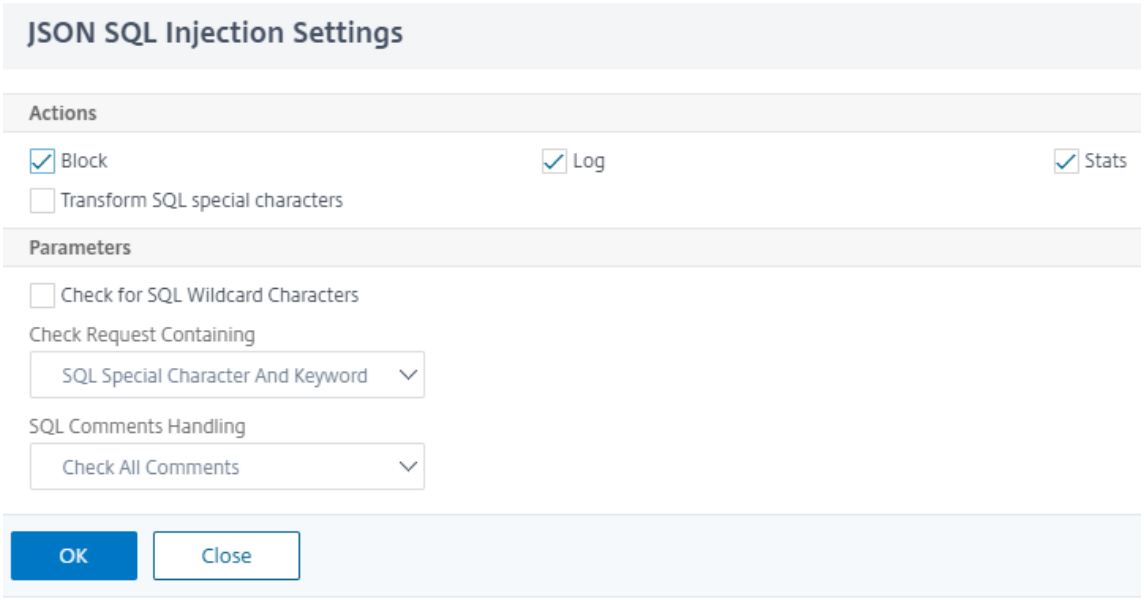
Konfigurieren Sie den JSON-SQL-Injection-Schutz mithilfe der GUI

Gehen Sie wie folgt vor, um die JSON-SQL-Einschleusung-Schutzeinstellungen festzulegen.

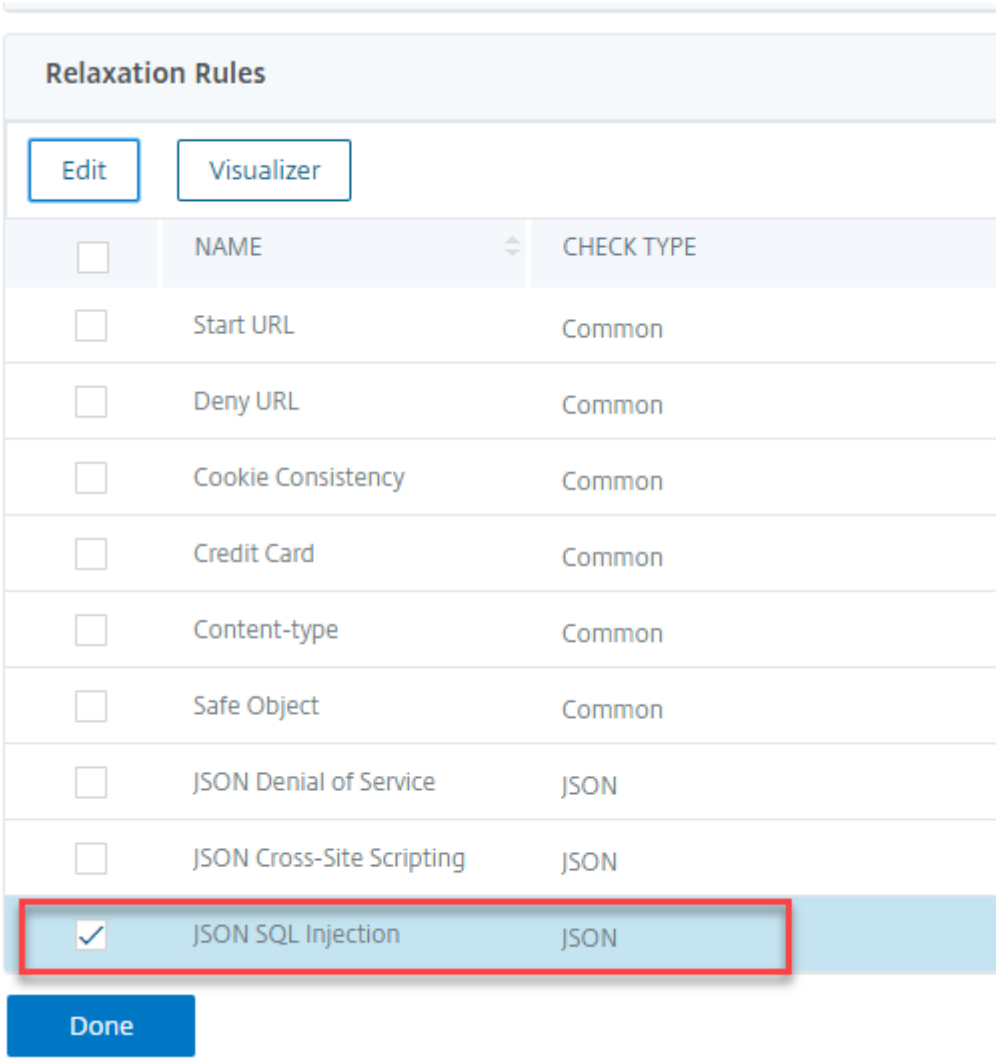
1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall-Profilseite** unter **ErweiterteEinstellungen auf Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu den **JSON-SQL-Einschleusung-Einstellungen** .
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.



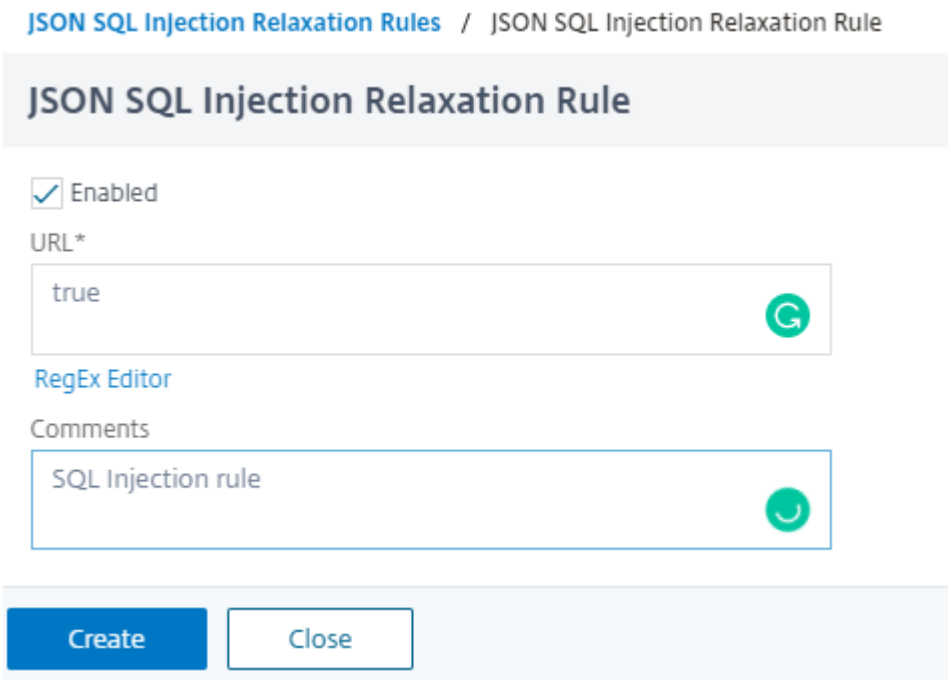
6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON SQL Injection Settings** aufzurufen.
7. Wählen Sie die **JSON SQL Injection-Aktionen** aus.
8. Klicken Sie auf **OK**.



9. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Entspannungsregeln**.
10. Wählen Sie im Abschnitt **Entspannungsregeln** die **JSON SQL Injection-Einstellungen** aus und klicken Sie auf **Bearbeiten**.



11. Geben Sie auf der Seite JSON SQL Injection Relaxation Rule die URL ein, an die die Anforderung gesendet werden muss. Alle an diese URL gesendeten Anfragen werden nicht blockiert.
12. Klicken Sie auf **Erstellen**.



Konfigurieren der Feinkornentspannung für den JSON-SQL-Einschleusungsschutz

Die Web App Firewall bietet Ihnen die Möglichkeit, einen bestimmten JSON-Schlüssel oder -Wert aus der JSON-basierten SQL Injection-Überprüfung zu lockern. Sie können mehrere Optionen zum Entspannen von JSON-Nutzlasten mithilfe von Feinkornrelaxierungsregeln konfigurieren.

Bisher bestand die einzige Möglichkeit, Lockerungen für JSON-Schutzprüfungen zu konfigurieren, darin, die gesamte URL anzugeben, wodurch die Überprüfung der gesamten URL umgangen würde.

Der JSON-basierte SQL-Sicherheitsschutz bietet Entspannung für Folgendes:

- Die wichtigsten Namen
- Die wichtigsten Werte

Mit der JSON-basierten SQL-Schutzprüfung können Sie Entspannungen konfigurieren, die bestimmte Muster zulassen und den Rest blockieren. Beispielsweise verfügt die Web App Firewall derzeit über einen Standardsatz von mehr als 100 SQL-Schlüsselwörtern. Da Hacker diese Schlüsselwörter bei SQL-Einschleusung-Angriffen verwenden können, kennzeichnet die Web App Firewall alle als potenzielle Bedrohungen. Wenn Sie ein oder mehrere Schlüsselwörter lockern möchten, die für den jeweiligen Standort als sicher gelten, können Sie eine Entspannungsregel konfigurieren, die die Sicherheitsüberprüfung Bypass und den Rest blockieren kann. Die in Relaxationen verwendeten Befehle haben optionale Parameter für Value Type und Value Expression. Sie können angeben, ob der Wertausdruck ein regulärer Ausdruck oder eine literale Zeichenfolge ist. Der Werttyp kann leer gelassen werden, oder Sie haben die Möglichkeit, Keyword oder Special String auszuwählen.

> **Hinweis:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Metazeichen- oder Platzhalterkombination mit Punkt-Sternchen (.*) kann zu Ergebnissen führen, die Sie nicht möchten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die JSON-SQL-Einschleusung-Prüfung sonst blockiert hätte.

Zu berücksichtigende Punkte

- Der Wertausdruck ist ein optionales Argument. Ein Feldname hat möglicherweise keinen Wertausdruck.
- Ein Schlüsselname kann an Ausdrücke mit mehreren Werten gebunden werden.
- Wertausdrücken muss ein Werttyp zugewiesen werden. Der Werttyp kann sein: 1) Schlüsselwort, 2) SpecialString.
- Sie können mehrere Entspannungsregeln pro Schlüsselname oder URL-Kombination festlegen.

Konfigurieren der JSON-Feinkorn-Entspannung für Befehlseinspritzangriffe mithilfe der Befehlsschnittstelle

Um die JSON-Dateikorn-Entspannungsregel zu konfigurieren, müssen Sie die Feinkornentspannungseinheiten an das Web App Firewall-Profil binden.

Geben Sie in der Befehlszeile Folgendes ein:

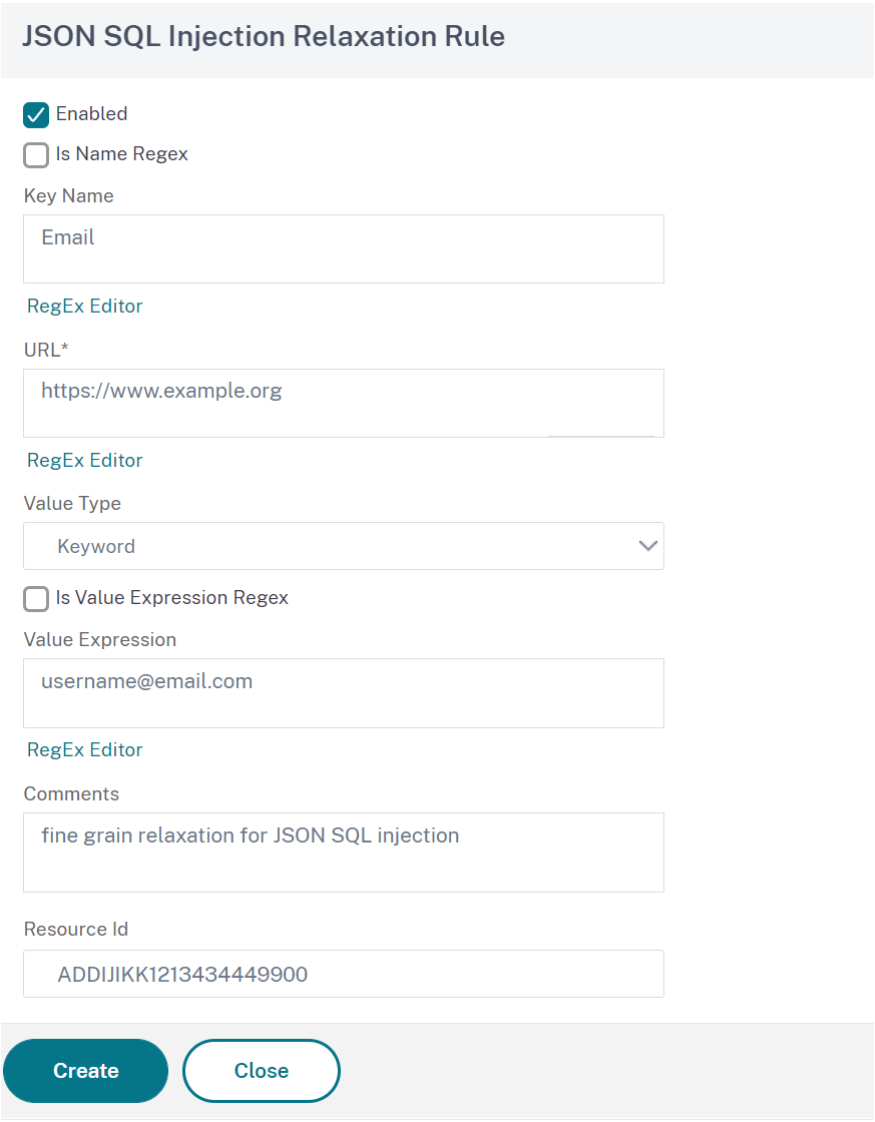
```
bind appfw profile <profile name> -jsoncmdURL <URL> -key <key name> -
    isregex <REGEX/NOTREGEX> -valueType <keyword/SpecialString> <value
    Expression> -isvalueRegex <REGEX/NOTREGEX>
<!--NeedCopy-->
```

Beispiel:

```
bind appfw profile appprofile1 -jsonsqlurl www.example.com -key
    stn_name  -isRegex NOTREGEX -valueType Keyword  “union”  -
    isvalueRegex NOTREGEX
<!--NeedCopy-->
```

Konfigurieren der Feinkornentspannungsregel für JSON-basierte Befehlseinschleusungsangriffe über die GUI

1. Navigieren Sie zu **Application Firewall > Profile**, wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Wählen Sie im Abschnitt **Relaxation Rules** einen **JSON SQL Injection-Datensatz** aus und klicken Sie auf **Bearbeiten**.
4. Klicken Sie im Schieberegler für **JSON SQL Injection Relaxation Rule** auf **Hinzufügen**
5. Legen Sie auf der Seite **JSON SQL Injection Relaxation Rule** die folgenden Parameter fest.
    a) Aktiviert
    b) Ist Name Regex
    c) Schlüsselname
    d) URL
    e) Werttyp
    f) Anmerkungen
    g) Ressourcen-ID
6. Klicken Sie auf **Erstellen**.



Überprüfung des JSON-Site-Scripting-Schutzes

May 11, 2023

Wenn eine eingehende JSON-Nutzlast schädliche Cross-Site-Scripting-Daten enthält, blockiert WAF die Anforderung. Die folgenden Verfahren erklären, wie Sie dies über CLI- und GUI-Schnittstellen konfigurieren können.

Konfigurieren des JSON-Site-Scripting-Schutzes

Um den JSON-Site-Scripting-Schutz zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie das Anwendungsfirewall-Profil als JSON hinzu.
2. Konfigurieren der JSON-Site-Scripting-Aktion zum Blockieren schädlicher Nutzdaten für Cross-Site Scripting

Anwendungs-Firewall-Profil vom Typ JSON hinzufügen

Sie müssen zuerst ein Profil erstellen, das angibt, wie die Anwendungsfirewall Ihre JSON-Webinhalte vor siteübergreifenden JSON-Skripting-Angriffen schützen muss.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> **Hinweis**:
>
> Wenn Sie den Profiltyp auf JSON festlegen, sind andere Prüfungen wie HTML oder XML nicht anwendbar.

Beispiel

```
add appfw profile profile1 -type JSON
```

Beispielausgabe für JSON-Site-Scripting-Verletzung

```
JSONcross-site scriptingAction: block log stats
Payload: {
 "username":"<a href="jAvAsCrIpT:alert(1)">X</a>","password":"xyz" }


Log message: Aug 19 06:57:33 <local0.info> 10.106.102.21
    08/19/2019:06:57:33 GMT  0-PPE-0 : default APPFW APPFW_JSON_cross-
    site scripting 58 0 :  10.102.1.98 12-PPE0 - profjson http://
    10.106.102.24/ Cross-site script check failed for object value(with
    violation="Bad URL: jAvAsCrIpT:alert(1)") starting at offset(12). <
    blocked>

Counters
    1  357000                  1 as_viol_json_xss
    3  0                       1 as_log_json_xss
    5  0                       1 as_viol_json_xss_profile appfw__(
       profjson)
    7  0                       1 as_log_json_xss_profile appfw__(
       profjson)

<!--NeedCopy-->
```


Konfigurieren der Aktion “JSON-Site-Scripting”

Sie müssen eine oder mehrere JSON-Site-Scripting-Aktionen konfigurieren, um Ihre Anwendung vor JSON-Cross-Site Scripting-Angriffen zu schützen.
Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <name> - JSONcross-site scriptingAction [block] [log] [
stats] [none]
```

Beispiel

```
set appfw profile profile1 -JSONcross-site scriptingAction block
```

Die verfügbaren Cross-Site-Scripting-Aktionen sind:
Blockieren — Verbindungen blockieren, die diese Sicherheitsüberprüfung verletzen.
Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.
Statistiken - Generieren Sie Statistiken für diese Sicherheitsüberprüfung.
Keine — Deaktiviert alle Aktionen für diese Sicherheitsüberprüfung.

> **Hinweis**:
> Um eine oder mehrere Aktionen zu aktivieren, geben Sie “set appfw profile - JsonCross-Site ScriptingAction” ein, gefolgt von den zu aktivierenden Aktionen.

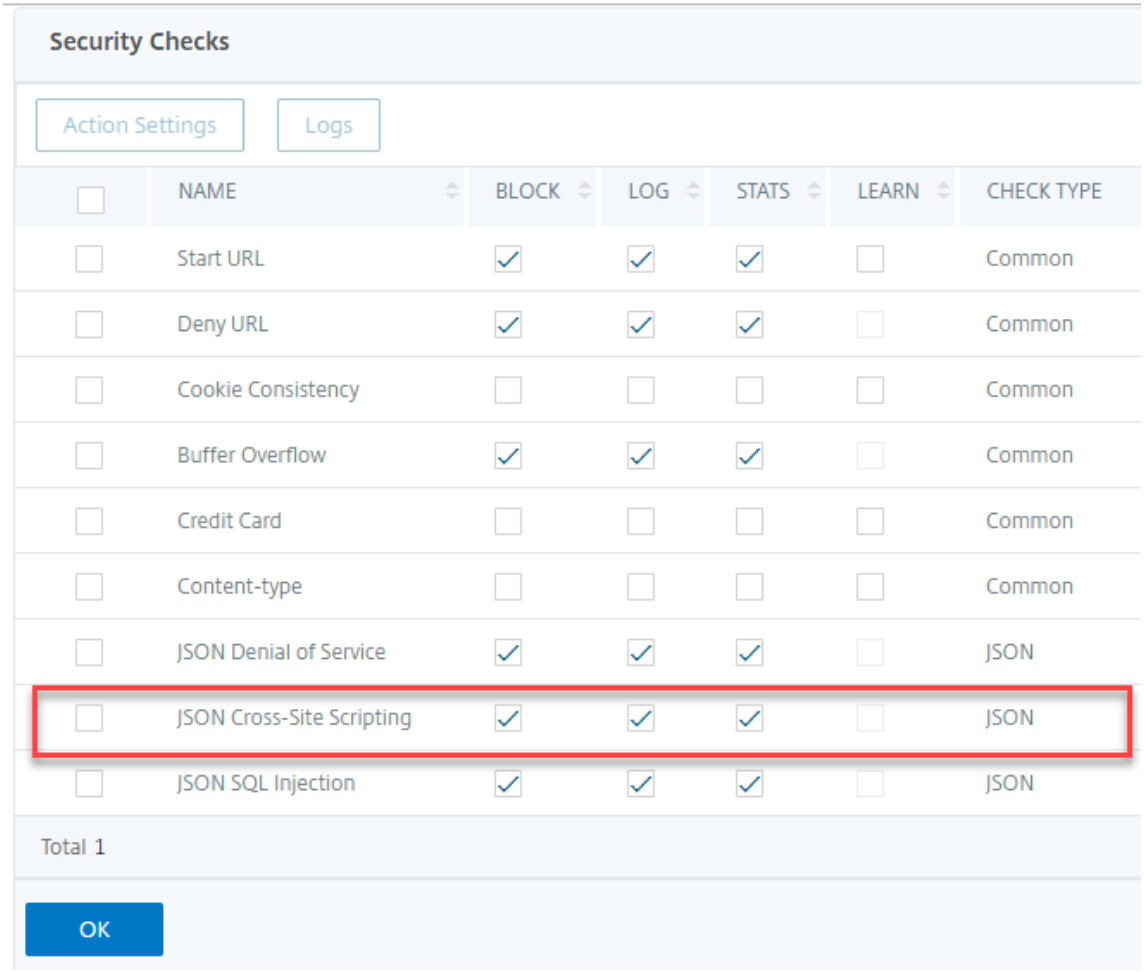
Beispiel

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

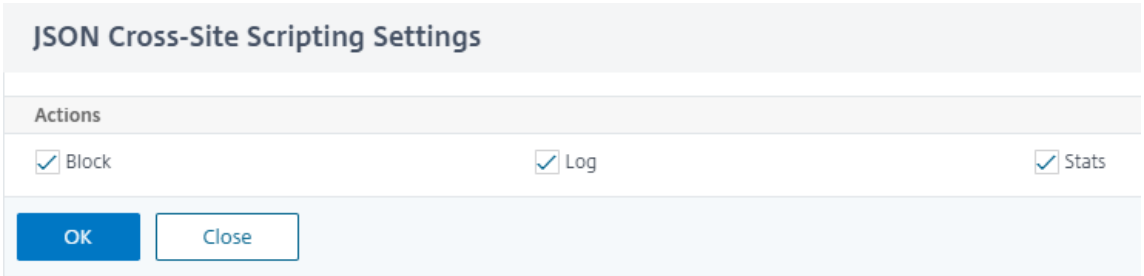
Konfigurieren Sie den JSON Cross Site Scripting (Cross-Site Scripting) -Schutz mithilfe der GUI

Gehen Sie wie folgt vor, um die Schutzeinstellungen für Cross Site Scripting (Cross-Site Scripting) festzulegen.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall-Profilseite** unter **ErweiterteEinstellungen auf Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsüberprüfungen** zu den Einstellungen für **JSON-Site-Scripting (Cross-Site-Scripting)** .
5. Klicken Sie neben dem Kontrollkästchen auf das Symbol der ausführbaren

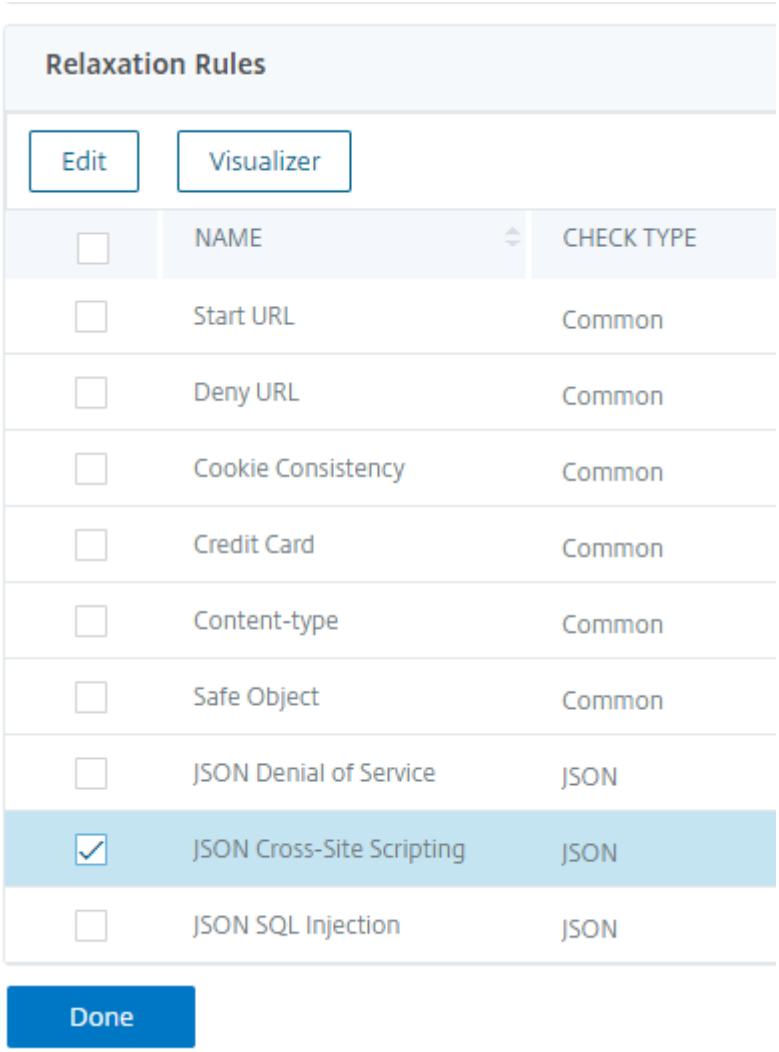


6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON-Site-Scripting-Einstellungen** aufzurufen.
7. Wählen Sie die Site-übergreifenden JSON-Skripting-Aktionen aus
8. Klicken Sie auf **OK**.

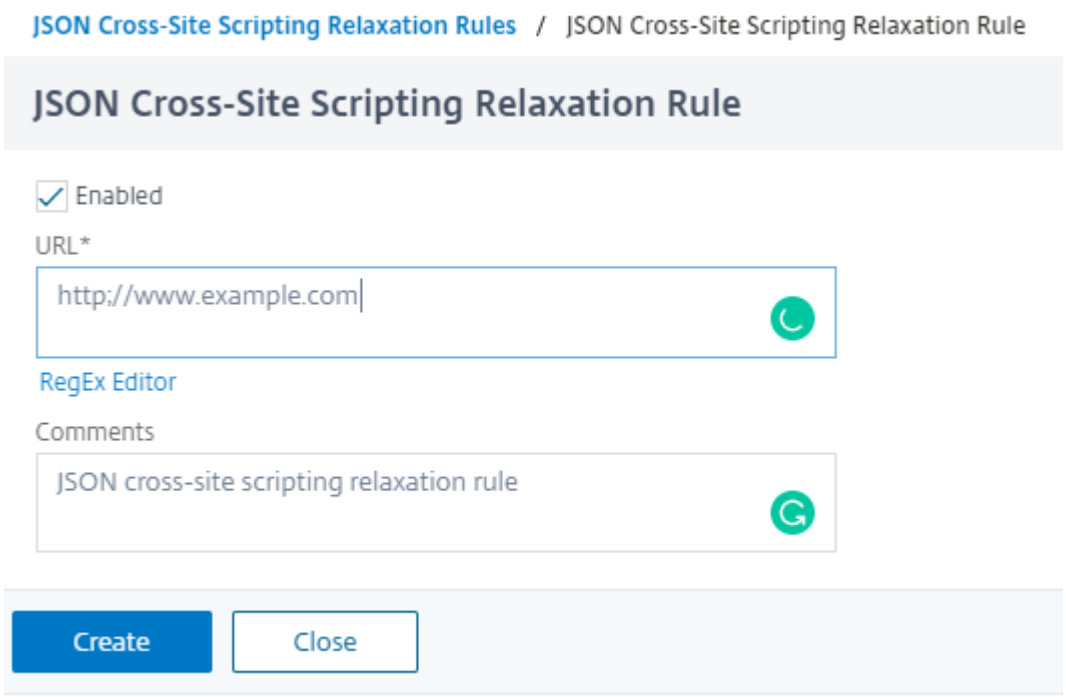


9. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Entspannungsregeln**.
10. Wählen Sie im Abschnitt **Entspannungsregeln** die JSON-Site-Scripting-Einstellungen aus und

klicken Sie auf **Bearbeiten**.



11. Klicken Sie auf der Seite **JSON-Site Scripting Relaxation Rule** auf **Hinzufügen**, um eine Relaxationsregel für JSON-Site Scripting hinzuzufügen.
12. Geben Sie die URL ein, an die die Anfrage gesendet werden muss. Alle an diese URL gesendeten Anfragen werden nicht blockiert.
13. Klicken Sie auf **Erstellen**.



Konfigurieren Sie feinkörnige Entspannung für JSON-basiertes Cross-Site Scripting

Die Web App Firewall bietet Ihnen die Möglichkeit, einen bestimmten JSON-Schlüssel oder -Wert aus der JSON-basierten Cross-Site Scripting (XSS) -Prüfung zu lockern. Sie können mehrere Optionen zum Entspannen von JSON-Nutzlasten mithilfe von Feinkornrelaxierungsregeln konfigurieren.
Bisher bestand die einzige Möglichkeit, Lockerungen für JSON-Schutzprüfungen zu konfigurieren, darin, die gesamte URL anzugeben, wodurch die Überprüfung der gesamten URL umgangen würde.
Der JSON-basierte SQL-Sicherheitsschutz bietet Entspannung für Folgendes:

- Die wichtigsten Namen
- Die wichtigsten Werte

Mit dem JSON-basierten Cross-Site Scripting (XSS) -Schutz können Sie Entspannungen konfigurieren, die bestimmte Muster zulassen und den Rest blockieren. Beispielsweise verfügt die Web App Firewall derzeit über einen Standardsatz von mehr als 100 SQL-Schlüsselwörtern. Da Hacker diese Schlüsselwörter bei SQL-Einschleusung-Angriffen verwenden können, kennzeichnet die Web App Firewall alle als potenzielle Bedrohungen. Wenn Sie ein oder mehrere Schlüsselwörter lockern möchten, die für den jeweiligen Standort als sicher gelten, können Sie eine Entspannungsregel konfigurieren, die die Sicherheitsüberprüfung Bypass und den Rest blockieren kann. Die in Relaxationen verwendeten Befehle haben optionale Parameter für Value Type und Value Expression. Sie können angeben, ob der Wertausdruck ein regulärer Ausdruck oder eine literale Zeichenfolge ist. Der Werttyp kann leer gelassen werden, oder Sie haben die Möglichkeit, Keyword oder Special String auszuwählen.

> **Hinweis:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Metazeichen- oder Platzhalterkombination mit Punkt-Sternchen (.*) kann zu Ergebnissen führen, die Sie nicht möchten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die JSON-SQL-Einschleusung-Prüfung sonst blockiert hätte.

Zu berücksichtigende Punkte

- Der Wertausdruck ist ein optionales Argument. Ein Feldname hat möglicherweise keinen Wertausdruck.
- Ein Schlüsselname kann an Ausdrücke mit mehreren Werten gebunden werden.
- Wertausdrücken muss ein Werttyp zugewiesen werden. Die Werttypen sind Tag, Attribut und Muster.
- Sie können mehrere Entspannungsregeln pro Schlüsselname/URL-Kombination festlegen.

Konfigurieren der JSON-Feinkorn-Entspannung für Cross-Site Scripting (XSS) -Injection-Angriffe mithilfe der Befehlsschnittstelle

Um die JSON-Dateikorn-Entspannungsregel zu konfigurieren, müssen Sie die Feinkornentspannungseinheiten an das Web App Firewall-Profil binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile <profile name> -jsonxssURL <URL> -key <key name> -
    isregex <REGEX/NOTREGEX> -valueType <keyword/SpecialString> <value
    Expression> -isvalueRegex <REGEX/NOTREGEX>
<!--NeedCopy-->
```

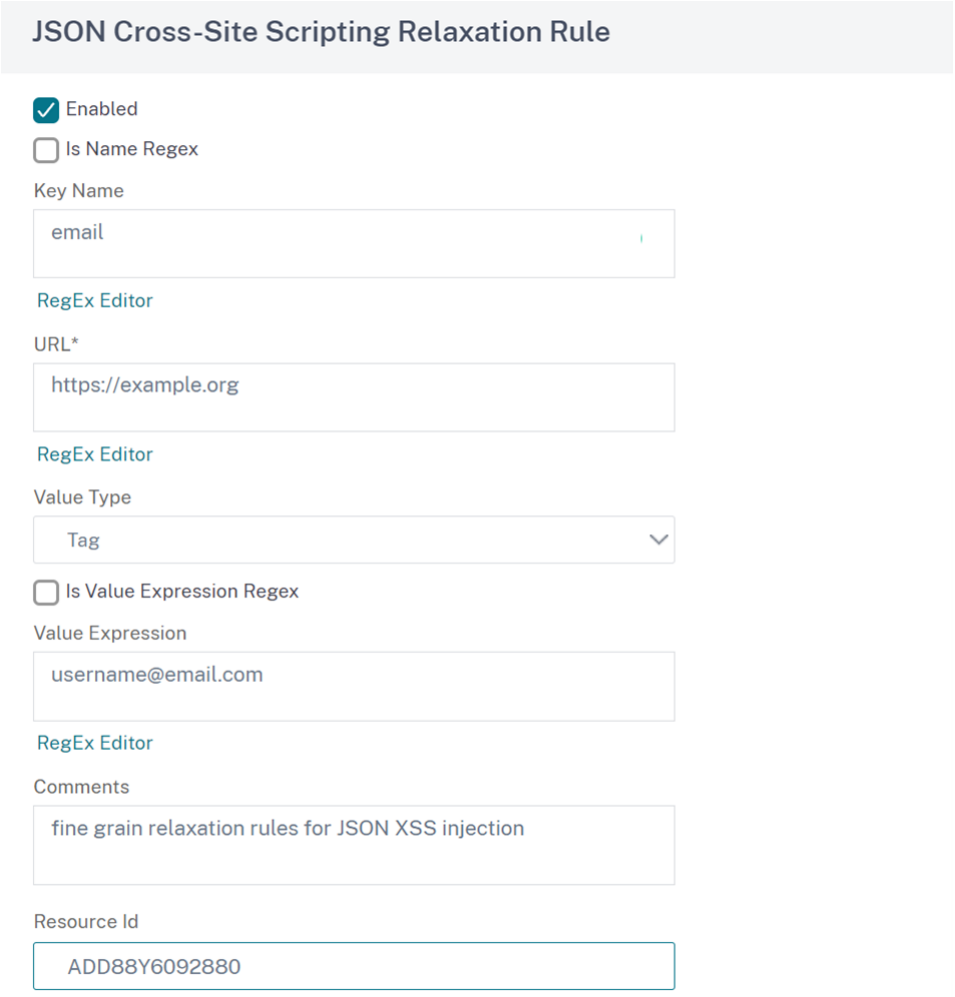
Beispiel:

```
bind appfw profile appprofile1 -jsonxssurl www.example.com -key name  -
    isRegex NOTREGEX -valueType Tag  “sname”  -isvalueRegex NOTREGEX
<!--NeedCopy-->
```

So konfigurieren Sie eine JSON-basierte Cross-Site Scripting (XSS) -Injection Feinkornentspannungsregel über die GUI

1. Navigieren Sie zu **Application Firewall > Profile**, wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.

2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Wählen Sie im Abschnitt **Relaxation Rules** einen JSON SQL Injection-Datensatz aus und klicken Sie auf **Bearbeiten**.
4. Klicken Sie im Schieberegler für **JSON-Site Scripting Relaxation Rules** auf **Hinzufügen**.
5. Legen Sie auf der **Seite Regel für die Entspannung von JSON-Site Scripting** die folgenden Parameter fest.
   a) Aktiviert
   b) Ist Name Regex
   c) Schlüsselname
   d) URL
   e) Werttyp
   f) Anmerkungen
   g) Ressourcen-ID
6. Klicken Sie auf **Erstellen**.



JSON-Befehlseinschleusungsprüfung

May 11, 2023

Die JSON-Befehlseinschleusungsprüfung untersucht den eingehenden JSON-Datenverkehr auf nicht autorisierte Befehle, die die Systemsicherheit beeinträchtigen oder das System modifizieren. Wenn bei der Untersuchung des Datenverkehrs schädliche Befehle erkannt werden, blockiert die Appliance die Anforderung oder führt die konfigurierte Aktion aus.

Bei einem Befehlseinschleusungsangriff zielt der Angreifer darauf ab, nicht autorisierte Befehle auf dem NetScaler-Betriebssystem oder dem Backend-Server auszuführen. Um dies zu erreichen, schleust der Angreifer Betriebssystembefehle über eine anfällige Anwendung ein. Die Back-End-Anwendung ist anfällig für Einschleusungsangriffe, wenn die Appliance eine Anfrage einfach ohne Sicherheitsüberprüfung weiterleitet. Daher ist es sehr wichtig, eine Sicherheitsüberprüfung zu konfigurieren, damit die NetScaler-Appliance Ihre Webanwendung schützen kann, indem sie unsichere Daten blockiert.

So funktioniert der Befehlseinschleusungsschutz

1. Bei einer eingehenden JSON-Anforderung untersucht WAF den Datenverkehr auf Schlüsselwörter oder Sonderzeichen. Wenn die JSON-Anforderung keine Muster enthält, die mit einem der verweigerten Schlüsselwörter oder Sonderzeichen übereinstimmen, ist die Anforderung zulässig. Andernfalls wird die Anforderung basierend auf der konfigurierten Aktion blockiert, verworfen oder umgeleitet.
2. Wenn Sie es vorziehen, ein Schlüsselwort oder ein Sonderzeichen von der Liste auszunehmen, können Sie eine Entspannungsregel erstellen, um die Sicherheitsüberprüfung unter bestimmten Bedingungen zu Bypass.
3. Sie können die Protokollierung aktivieren, um Protokollmeldungen zu generieren Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
4. Sie können die Statistikfunktion auch aktivieren, um statistische Daten zu Verstößen und Protokollen zu sammeln. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anforderungen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um festzustellen, ob Sie die neue Entspannungsregel konfigurieren oder die vorhandene ändern müssen.

Schlüsselwörter und Sonderzeichen, die für die Befehlseinschleusung verweigert werden

Zum Erkennen und Blockieren von JSON-Befehlseinschleusungsangriffen hat die Appliance über eine Reihe von Mustern (Schlüsselwörter und Sonderzeichen), die in der Standardsignaturdatei definiert sind. Es folgt eine Liste der blockierten Schlüsselwörter beim Erkennen von Befehlseinschleusungsverstößen

```
<commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>

<!--NeedCopy-->
```

In der Signaturdatei definierte Sonderzeichen sind:
`| ; & $ > < '\ ! >> ##`

Konfigurieren der JSON-Befehlseinschleusungsprüfung über die CLI

In der Befehlszeilenschnittstelle können Sie entweder den Befehl set appfw profile verwenden oder einen appfw-Profilbefehl hinzufügen, um die JSON-Befehlseinschleusungseinstellungen zu konfigurieren. Sie können die Block-, Protokoll- und Statistikaktionen aktivieren. Sie müssen auch den Befehlseinschleusungstyp wie Schlüsselwörter und Zeichenfolgenzeichen festlegen, die Sie in den Nutzdaten erkennen möchten.

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Hinweis:**
>
> Standardmäßig ist die Befehlseinschleusungsaktion auf “Protokollstatistiken blockieren” festgelegt. Außerdem wird der Standardeinschleusungsstyp des Befehls als festgelegt `CmdSplCharANDKeyWord`. Nach einem Upgrade ist für die vorhandenen Web-App-Firewall-Profile die Aktion auf “Keine” festgelegt.

Beispiel:

```
set appfw profile profile1 -JSONCMDInjectionAction block -JSONCMDInjectionType
 CmdSplChar
```

Dabei sind die verfügbaren JSON-Befehlseinschleusungsaktionen:

Keine — Deaktiviert den Befehlseinschleusungsschutz.
Log — Protokollieren von Befehlseinschleusungsverstößen für die Sicherheitsprüfung
Blockieren - blockiert Datenverkehr, der gegen die Befehlseinschleusungsüberprüfung verstößt.
Statistik - Generiert Statistiken für Sicherheitsverletzungen durch Befehlseinschleusung.

Dabei sind die verfügbaren JSON-Befehlseinschleusungstypen:

`Cmd SplChar` - Prüft Sonderzeichen
`CmdKeyWord` - Prüft Schlüsselwörter zur Befehlseinschleusung
`CmdSplCharANDKeyWord` - Dies ist die Standardaktion. Die Aktion prüft Sonderzeichen und Befehlseinschleusung. Schlüsselwörter und Blöcke nur, wenn beide vorhanden sind.
`CmdSplCharORKeyWord` - Überprüft Sonderzeichen und Befehlseinschleusungsschlüsselwörter und blockiert, wenn gefunden.

Konfigurieren der Entspannungsregeln für die JSON-Befehlseinschleusungsprüfung

Wenn Ihre Anwendung erfordert, dass Sie die JSON-Befehlseinschleusungsprüfung für ein bestimmtes ELEMENT oder ATTRIBUTE in der Nutzlast umgehen müssen, können Sie eine Entspannungsregel konfigurieren.

Die Entspannungsregeln für die JSON-Befehlseinschleusungsprüfung haben folgende Syntax.

```
bind appfw profile <profile name> -JSONCMDURL <expression> -comment <string
> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED )-state ( ENABLED |
DISABLED )
```

Beispiel für Relaxationsregel für Regex im Header

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/hello.html
```

Im Folgenden werden Anfragen von allen auf 1.1.1.1 gehosteten URLs gelockert:

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/*"
```

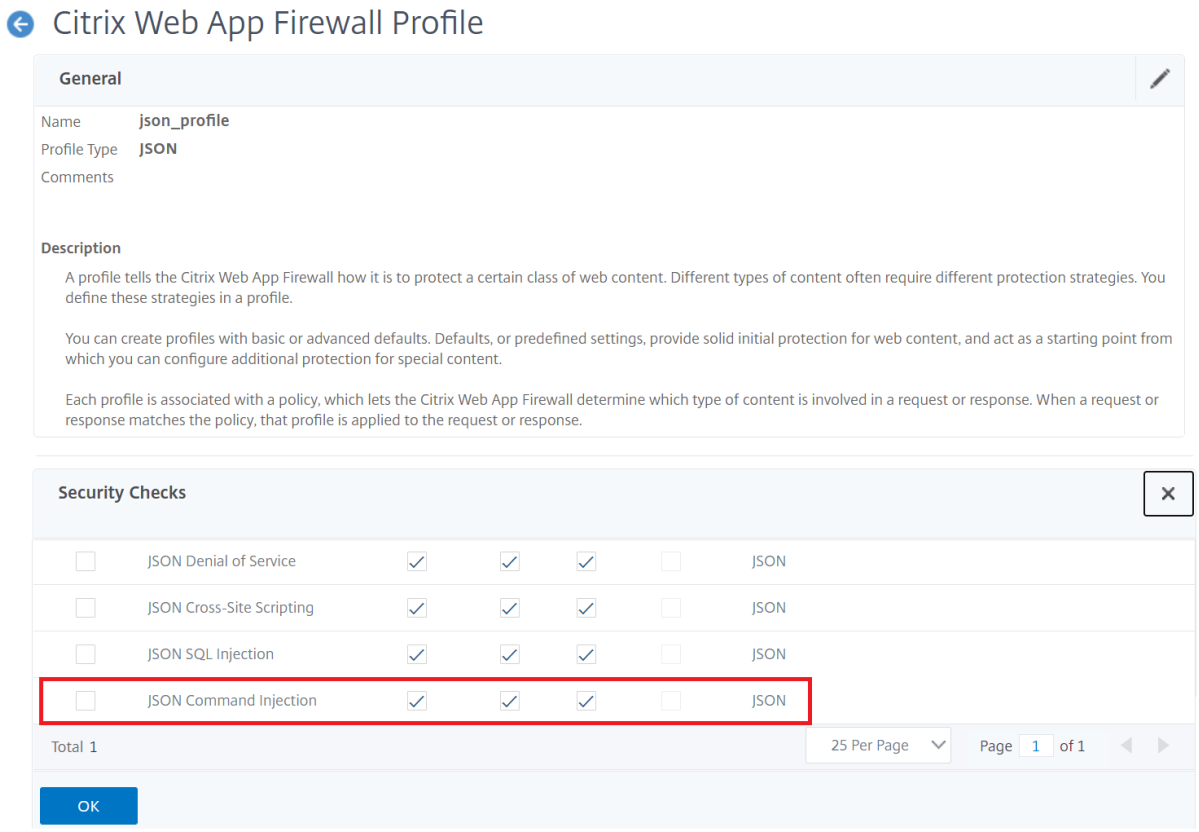
Um die Entspannung zu entfernen, verwenden Sie “unbind”.

```
unbind appfw profile abc_json -jsoncmDURL  " http://1.1.1.1/*"
```

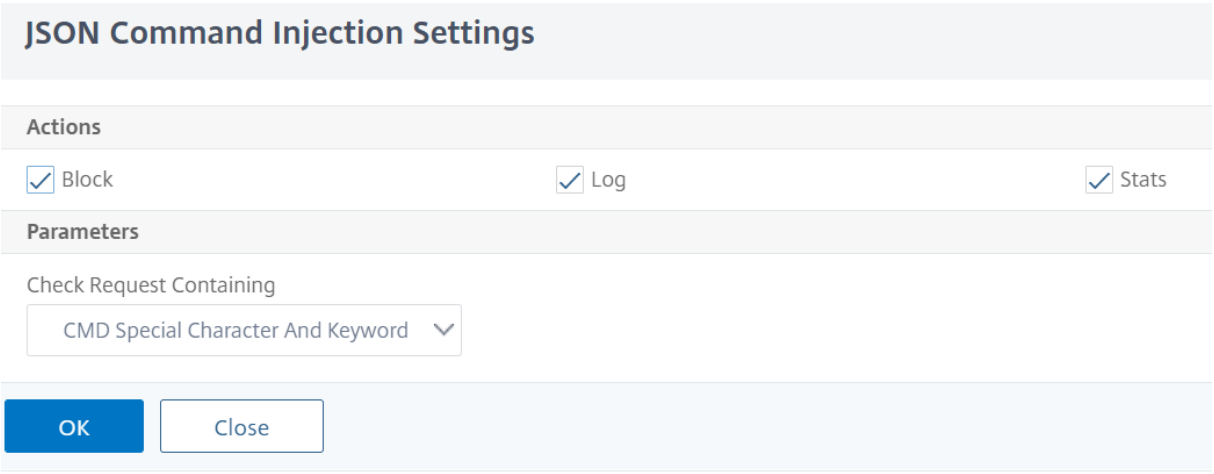
Konfigurieren der JSON-Befehlseinschleusungsprüfung über die GUI

Führen Sie die folgenden Schritte aus, um die JSON-Befehlseinschleusungsprüfung zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall und Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der **NetScaler Web App Firewall Profilseite** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.



1. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** die Option **JSON-Befehlseinschleusung** aus und klicken Sie auf**Aktion**.
2. Stellen Sie auf der Seite **JSON-Befehlseinschleusungseinstellungen** die folgenden Parameter ein
   a) Aktionen. Wählen Sie eine oder mehrere Aktionen für die Sicherheitsüberprüfung der JSON-Befehlseinschleusung aus.
   b) Überprüfen Sie die Anfrage enthält. Wählen Sie ein Befehlseinschleusungsmuster, um zu überprüfen, ob die eingehende Anforderung das Muster enthält.
3. Klicken Sie auf **OK**.



Anzeigen von Statistiken zum Befehlseinschleusungsdatenverkehr und -verletzungen

Auf der Seite " **NetScaler Web App Firewall Statistics** " werden Details zu Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format angezeigt.

So zeigen Sie Sicherheitsstatistiken mithilfe der Befehlszeilenschnittstelle an.

Geben Sie in der Befehlszeile Folgendes ein:

```
stat appfw profile profile1
```

Appfw-Profil Verkehrsstatistiken	Geschwindigkeit (/s)	Gesamt
Anfragen	0	0
Byte anfragen	0	0
Antworten	0	0
Antwort Byte	0	0
Bricht ab	0	0
Leitet	0	0
Langfristige Reaktionszeit (ms)	–	0
Letzte Reaktionszeit von Ave (ms)	–	0

Statistiken zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
Start-URL	0	0
URL verweigern	0	0
Referer-Header	0	0
Pufferüberlauf	0	0
Cookie-Konsistenz	0	0
Cookie-Entführung	0	0
CSRF-Formular-Tag	0	0
Site-übergreifendes HTML	0	0
HTML SQL injection	0	0
Feld-Format	0	0
Field consistency	0	0
Kreditkarte	0	0
Sicheres Objekt	0	0
Verstöße gegen die Signatur	0	0
Inhaltstyp	0	0
JSON-Denial-of-Service-Angriff	0	0
JSON-SQL-Einschleusung	0	0
JSON-Cross-Site Scripting	0	0
Dateiuploadtyp	0	0
Ableiten der XML-Nutzlast für Inhaltstypen	0	0
HTML-Befehlseinschleusung	0	0
XML-Format	0	0
XML-Denial-of-Service-Angriff (XDoS)	0	0
XML-Nachrichtenüberprüfung	0	0
Interoperabilität der Webdienste	0	0
XML SQL Injection	0	0

Statistiken zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
Site-übergreifende XML-Skrip	0	0
XML-Anhang	0	0
SOAP-Fehlerverletzungen	0	0
Generische XML-Verstöße	0	0
Verstöße insgesamt	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
Starten der URL-Protokolle	0	0
URL-Protokolle verweigern	0	0
Referer-Header-Protokolle	0	0
Pufferüberlauf-Protokolle	0	0
Protokolle zur Cookie-Konsistenz	0	0
Protokolle zur Cookie-Entführung	0	0
CSRF aus Tag-Protokollen	0	0
HTML-Cross-Site Scripting-Protokolle	0	0
HTML Cross-Site Scripting-Transformationsprotokolle	0	0
HTML SQL-Einschleusungsprotokolle	0	0
HTML SQL Transformationsprotokolle	0	0
Protokolle im Feldformat	0	0
Protokolle zur Feldkonsistenz	0	0
Kreditkarten	0	0
Protokolle zur Kreditkarten-Transformation	0	0
Sichere Objektprotokolle	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
Signatur-Protokolle	0	0
Inhalts-Typ-Protokolle	0	0
JSON-Denial-of-Service-Protokolle	0	0
JSON SQL-Einschleusungsprotokolle	0	0
JSON-Site-Scripting-Protokolle	0	0
Protokolle zum Hochladen von Dateien	0	0
Ableiten der XML-Nutzlast des Inhaltstyps L	0	0
JSON-CMD-Einschleusung	0	0
HTML-Befehlseinschleusungsprotokol	0	0
Protokolle im XML-Format	0	0
XML Denial of Service (XDoS) -Protokolle	0	0
Protokolle zur XML-Nachrichtenüberprüfung	0	0
WSI-Protokolle	0	0
XML SQL Injection-Protokolle	0	0
XML-Cross-Site Scripting-Protokolle	0	0
Protokolle für XML-Anhänge	0	0
SOAP-Fehlerlogs	0	0
Generische XML-Protokolle	0	0
Gesamtzahl der Protokollmeldungen	0	0

Statistikrate der Serverfehlerantwort (/s) | Gesamt |
|—|–|–|

HTTP Client Errors (4xx Resp) | 0 | 0|
HTTP Server Errors (5xx Resp) | 0 | 0 |

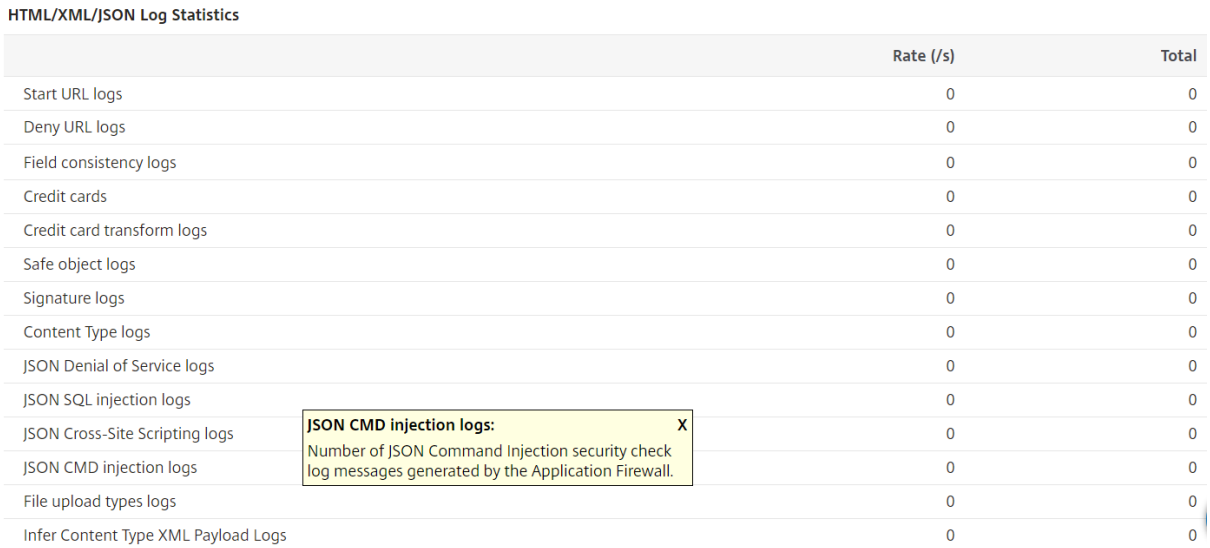
HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
JSON-Command Injection-	0	0
Protokolle im XML-Format	0	0

Anzeigen von JSON-Befehlseinschleusungsstatistiken über die NetScaler GUI

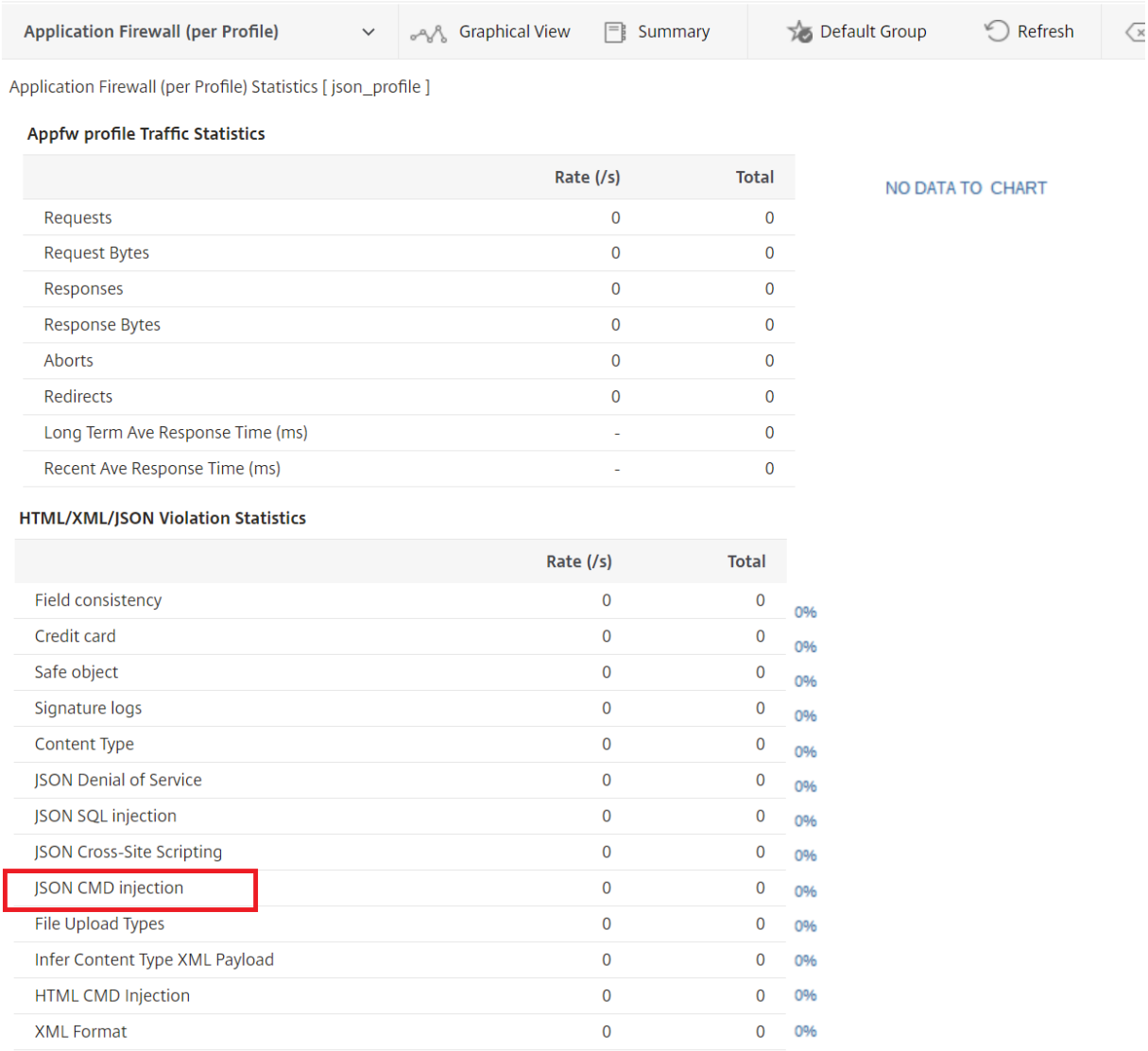
Führen Sie die folgenden Schritte aus, um Befehlseinschleusungsstatistiken anzuzeigen:

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Web App Firewall-Profil aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **NetScaler Web App Firewall Statistics** werden die Details zum JSON-Befehlseinschleusungsverkehr und Verstößen angezeigt.
4. Sie können die **Tabellarische Ansicht** wählen oder zur **grafischen Ansicht** wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.

JSON-Befehlseinschleusungverkehrsstatistiken



Statistiken zu JSON-Befehlseinschleusungsverstößen



Konfigurieren der feingesteuerten Lockerung für JSON-Befehlseinschleusungsprüfung

Die Web App Firewall bietet Ihnen die Möglichkeit, einen bestimmten JSON-Schlüssel oder -Wert aus der JSON-basierten Befehlseinschleusungsprüfung zu lockern. Sie können die Inspektion für ein oder mehrere Felder vollständig Bypass, indem Sie feingesteuert die Lockerungsregeln konfigurieren.

Bisher bestand die einzige Möglichkeit, Lockerungen für JSON-Schutzprüfungen zu konfigurieren, darin, die gesamte URL anzugeben, wodurch die Überprüfung der gesamten URL umgangen würde.

Der JSON-basierte Sicherheitsschutz gegen Befehlseinschleusung bietet Lockerungen für Folgendes:

- Die wichtigsten Namen
- Die wichtigsten Werte

Mit dem JSON-basierten Befehlseinschleusungsschutz können Sie Entspannungen konfigurieren, die bestimmte Muster zulassen und den Rest blockieren. Beispielsweise verfügt die Web App Firewall derzeit über einen Standardsatz von mehr als 100 SQL-Schlüsselwörtern. Da Hacker diese Schlüsselwörter bei Befehlseinschleusungsangriffen verwenden können, kennzeichnet die Web App Firewall alle als potenzielle Bedrohungen. Wenn Sie ein oder mehrere Schlüsselwörter lockern möchten, die für den jeweiligen Standort als sicher gelten, können Sie eine Entspannungsregel konfigurieren, die die Sicherheitsüberprüfung Bypass und den Rest blockieren kann. Die in Relaxationen verwendeten Befehle haben optionale Parameter für Value Type und Value Expression. Sie können angeben, ob der Wertausdruck ein regulärer Ausdruck oder eine literale Zeichenfolge ist. Der Werttyp kann leer gelassen werden, oder Sie haben die Möglichkeit, Keyword oder Special String auszuwählen.

> **Hinweis:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Metazeichen- oder Platzhalterkombination mit Punkt-Sternchen (.*) kann zu Ergebnissen führen, die Sie nicht möchten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die JSON-SQL-Einschleusung-Prüfung sonst blockiert hätte.

Zu berücksichtigende Punkte

- Der Wertausdruck ist ein optionales Argument. Ein Feldname hat möglicherweise keinen Wertausdruck.
- Ein Schlüsselname kann an Ausdrücke mit mehreren Werten gebunden werden.
- Wertausdrücken muss ein Werttyp zugewiesen werden. Der Werttyp kann sein: 1) Schlüsselwort, 2) SpecialString.
- Sie können mehrere Entspannungsregeln pro Schlüsselname/URL-Kombination festlegen.

Konfigurieren der JSON-Feinkorn-Entspannung für Befehlseinspritzangriffe mithilfe der Befehlsschnittstelle

Um die JSON-Dateikorn-Entspannungsregel zu konfigurieren, müssen Sie die Feinkornentspannungseinheiten an das Web App Firewall-Profil binden.

Geben Sie in der Befehlszeile Folgendes ein:

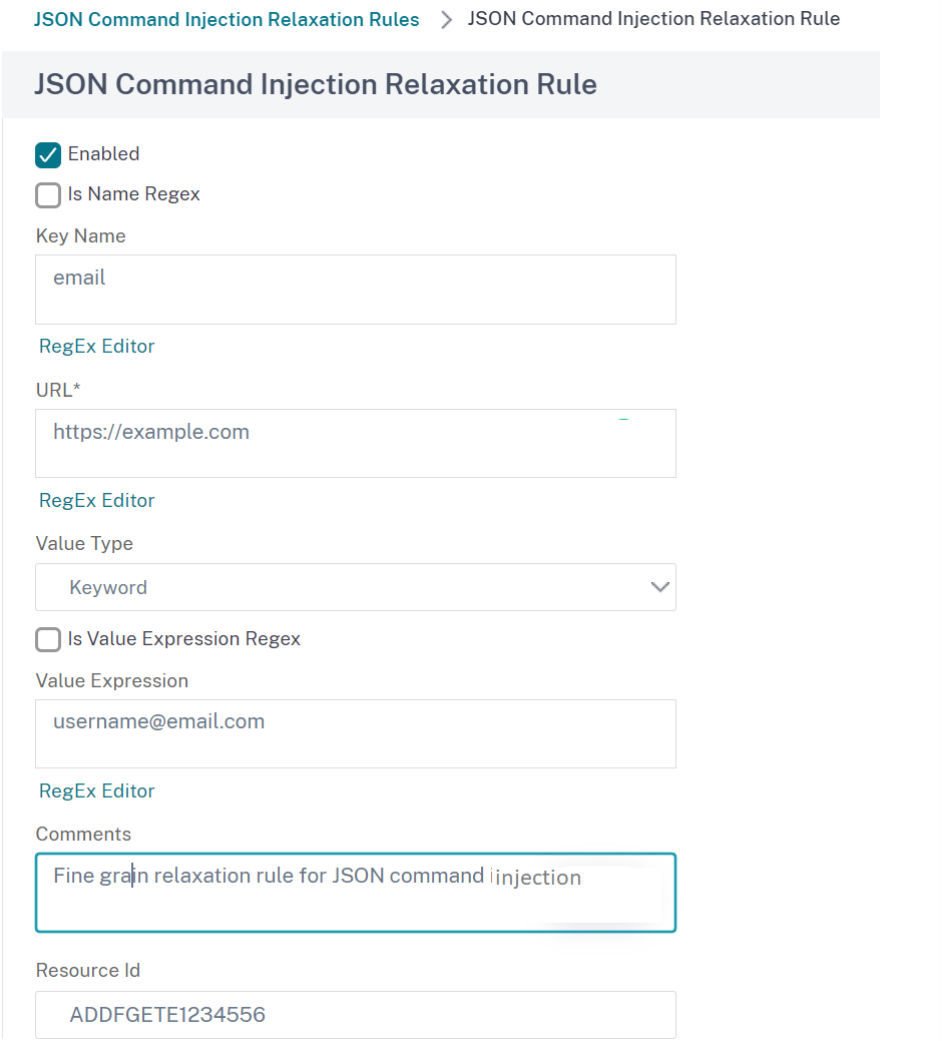
```
1 bind appfw profile <profile name> -jsoncmdURL <URL> -key <key name> -
     valueType <keyword/SpecialString> <value Expression>
2 <!--NeedCopy-->
```


Beispiel:

```
bind appfw profile appprofile1 -jsoncmdurl www.example.com -key blg_cnt -
isRegex NOTREGEX -valueType Keyword “cat” -isvalueRegex NOTREGEX
```

Konfigurieren der Feinkornentspannungsregel für JSON-basierte Befehlseinschleusungsangriffe über die GUI

1. Navigieren Sie zu **Application Firewall > Profile**, wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Wählen Sie im Abschnitt **Entspannungsregeln** einen **JSON Command Injection -Datensatz** aus und klicken Sie auf **Bearbeiten**.
4. Klicken Sie im Schieberegler für die **JSON-Befehlseinspritzung** auf **Hinzufügen**.
5. Legen Sie auf der Seite “ **Relaxationsregel für die JSON-Befehlseinschleusung** “
    a) Aktiviert
    b) Ist Name Regex
    c) Schlüsselname
    d) URL
    e) Werttyp
    f) Anmerkungen
    g) Ressourcen-ID
6. Klicken Sie auf **Erstellen**.



Verwaltung von Inhaltstypen

July 4, 2023

Webserver fügen einen Content-Type-Header mit einer MIME-/Type-Definition für jeden Inhaltstyp hinzu. Webserver stellen viele verschiedene Arten von Inhalten bereit. Beispielsweise wird Standard-HTML der MIME-Typ „text/html“ zugewiesen. JPG-Bildern wird der Inhaltstyp „“ oder „image/jpg“ zugewiesen. Ein normaler Webserver kann verschiedene Arten von Inhalten bereitstellen, die alle im Content Type-Header durch den zugewiesenen MIME/Typ definiert sind.

Viele Web App Firewall-Filterregeln sind darauf ausgelegt, einen bestimmten Inhaltstyp zu filtern. Die Filterregeln gelten für einen Inhaltstyp wie HTML und sind oft unangemessen, wenn ein anderer Inhaltstyp (z. B. Bilder) gefiltert wird. Daher versucht die Web App Firewall, den Inhaltstyp von Anfra-

gen und Antworten zu ermitteln, bevor sie sie filtert. Wenn ein Webserver oder Browser einer Anfrage oder Antwort keinen Content-Type-Header hinzufügt, wendet die Web App Firewall einen Standard-Inhaltstyp an und filtert den Inhalt entsprechend.

Der Standard-Inhaltstyp ist normalerweise „application/octet-stream“ mit der allgemeinsten MIME-/Typdefinition. Der MIME/Typ ist für jeden Inhaltstyp geeignet, den ein Webserver wahrscheinlich bereitstellen wird. Stellt der Web App Firewall jedoch nicht viele Informationen zur Verfügung, sodass sie die geeignete Filterung auswählen kann. Wenn ein geschützter Webserver so konfiguriert ist, dass er genaue Inhaltstyp-Header hinzufügt, können Sie dann ein Profil für den Webserver erstellen und ihm einen Standard-Inhaltstyp zuweisen. Dies wird getan, um sowohl die Geschwindigkeit als auch die Genauigkeit der Filterung zu verbessern.

Sie können auch eine Liste der zulässigen Anforderungsinhaltstypen für ein bestimmtes Profil konfigurieren. Wenn diese Funktion konfiguriert ist und die Web App Firewall eine Anfrage filtert, die keinem der zulässigen Inhaltstypen entspricht, blockiert sie die Anforderung.

Anfragen müssen immer entweder vom Typ „application/x-www-form-urlencoded“, „multipart/form-data“ oder „text/x-gwt-rpc“ sein. Die Web App Firewall blockiert jede Anfrage, für die ein anderer Inhaltstyp festgelegt wurde.

> **Hinweis**
>
> Sie können die Inhaltstypen „application/x-www-form-urlencoded“ oder „multipart/form-data“ nicht in die Liste der zulässigen Antwortinhaltstypen aufnehmen.

Um den Standardinhalt für Anfragen festzulegen, verwenden Sie die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> -requestContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp „text/html“ als Standard für das angegebene Profil festgelegt:

```
1 set appfw profile profile1 -requestContentType "text/html"
2 save ns config
3 <!--NeedCopy-->
```


Um den benutzerdefinierten Standardanforderungsinhalt zu entfernen, geben Sie Folgendes ein: Verwenden Sie die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `unset appfw profile <name> -requestContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Standard-Inhaltstyp „text/html“ für das angegebene Profil aufgehoben, sodass der Typ auf „application/octet-stream“ zurückgesetzt werden kann:

```
1 unset appfw profile profile1 -requestContentType "text/html"
2 save ns config
3 <!--NeedCopy-->
```

> **Hinweis**
>
> Verwenden Sie immer den letzten Inhaltstype-Header für die Verarbeitung und entfernen Sie alle verbleibenden Inhaltstype-Header, falls vorhanden, um sicherzustellen, dass der Back-End-Server eine Anfrage mit nur einem Inhaltstyp empfängt.
>
> *Um Anfragen zu blockieren, die umgangen werden können, fügen Sie eine Web App Firewall-Richtlinie mit der Regel HTTP.REQ.HEADER („content-type“) .COUNT.GT (1) ‘und einem Profil als appfw_block hinzu.*
>
> Wenn eine Anfrage ohne Content-Type-Header empfangen wird oder wenn die Anfrage einen Content-Type-Header ohne Wert hat, wendet die Web App Firewall den konfigurierten **RequestContentType-Wert** an und verarbeitet die Anfrage entsprechend.

Um den Standardinhalt der Antwort festzulegen, geben Sie Folgendes ein: Verwenden Sie die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> -responseContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp „text/html“ als Standard für das angegebene Profil festgelegt:


```
set appfw profile profile1 -responseContentType "text/html"
save ns config
<!--NeedCopy-->
```

Um den benutzerdefinierten Standardantwortinhalt zu entfernen, geben Sie Folgendes ein: Verwenden Sie die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `unset appfw profile <name> -responseContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Standard-Inhaltstyp „text/html“ für das angegebene Profil aufgehoben, sodass der Typ auf „application/octet-stream“ zurückgesetzt werden kann:

```
unset appfw profile profile1 -responseContentType "text/html"
save ns config
<!--NeedCopy-->
```

So fügen Sie mithilfe der Befehlszeilenschnittstelle einen Inhaltstyp zur Liste der zulässigen Inhaltstypen hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp „text/shtml“ zur Liste der zulässigen Inhaltstypen für das angegebene Profil hinzugefügt:

```
bind appfw profile profile1 -contentType "text/shtml"
save ns config
<!--NeedCopy-->
```


So entfernen Sie mithilfe der Befehlszeilenschnittstelle einen Inhaltstyp aus der Liste der zulässigen Inhaltstypen

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `unbind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp „text/shtml“ aus der Liste der zulässigen Inhaltstypen für das angegebene Profil entfernt:

```
unbind appfw profile profile1 -contentType "text/shtml"
save ns config
<!--NeedCopy-->
```

URL-codierte und aus mehreren Formularen bestehende Inhaltstypen verwalten

Mit der NetScaler Web App Firewall können Sie jetzt die Inhaltstypen Urlencoded und Multipart-Form für Formulare konfigurieren. Die Konfiguration des Inhaltstyps ähnelt der XML- und JSON-Liste. Basierend auf der Konfiguration klassifiziert die Web App Firewall die Anfragen und überprüft, ob URL-codierte oder aus mehreren Formularen bestehende Inhaltstypen vorliegen.

Um das Web App Firewall-Profil mit den Inhaltstypen Urlencoded und Multipart-Form zu konfigurieren, geben Sie
an der Befehlszeile Folgendes ein:

```
bind appfw profile p2 -contentType <string>
```

Beispiel:

```
bind appfw profile p2 -contentType UrlencodedFormContentType

bind appfw profile p2 -ContentType appfwmultipartform
```

Um die standardmäßigen und erlaubten Inhaltstypen mithilfe der GUI zu verwalten

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile**.
2. Wählen Sie im Detailbereich das zu konfigurierende Profil aus, und klicken Sie dann auf **Bearbeiten**. Das Dialogfeld **Web App Firewall-Profil konfigurieren** wird angezeigt.
3. Klicken Sie im Dialogfeld **Web App Firewall-Profil konfigurieren** auf die Registerkarte **Einstellungen** .
4. Scrollen Sie auf der Registerkarte **Einstellungen** etwa bis zur Hälfte nach unten zum Bereich Inhaltstyp.

5. Konfigurieren Sie im Bereich Inhaltstyp den standardmäßigen Inhaltstyp für Anfrage oder Antwort:
   - Um den Standard-Inhaltstyp für Anfragen zu konfigurieren, geben Sie die MIME-/Typdefinition des Inhaltstyps, den Sie verwenden möchten, in das Textfeld Standardanforderung ein.
   - Um den Standard-Inhaltstyp der Antwort zu konfigurieren, geben Sie die MIME-/Typdefinition des Inhaltstyps, den Sie verwenden möchten, in das Textfeld Standardantwort ein.
   - Um einen neuen zulässigen Inhaltstyp zu erstellen, klicken Sie auf **Hinzufügen**. Das Dialogfeld **Zulässigen Inhaltstyp hinzufügen** wird angezeigt.
   - Um einen vorhandenen zulässigen Inhaltstyp zu bearbeiten, wählen Sie diesen Inhaltstyp aus, und klicken Sie dann auf **Öffnen**. Das Dialogfeld **Zulässigen Inhaltstyp ändern** wird angezeigt.
6. Um die zulässigen Inhaltstypen zu verwalten, klicken Sie auf Zulässige Inhaltstypen verwalten.
7. Um einen neuen Inhaltstyp hinzuzufügen oder einen vorhandenen Inhaltstyp zu ändern, klicken Sie auf Hinzufügen oder Öffnen, und führen **Sie im Dialogfeld Zulässigen Inhaltstyp hinzufügen** oder **Zulässigen Inhaltstyp ändern** die folgenden Schritte aus.
   a) Aktivieren/deaktivieren Sie das Kontrollkästchen Aktiviert, um den Inhaltstyp in die Liste der zulässigen Inhaltstypen aufzunehmen oder aus dieser Liste auszuschließen.
   b) Geben Sie in das Textfeld Inhaltstyp einen regulären Ausdruck ein, der den Inhaltstyp beschreibt, den Sie hinzufügen oder den vorhandenen regulären Inhaltstyp ändern möchten.
   Inhaltstypen werden genauso formatiert wie MIME-Typbeschreibungen.

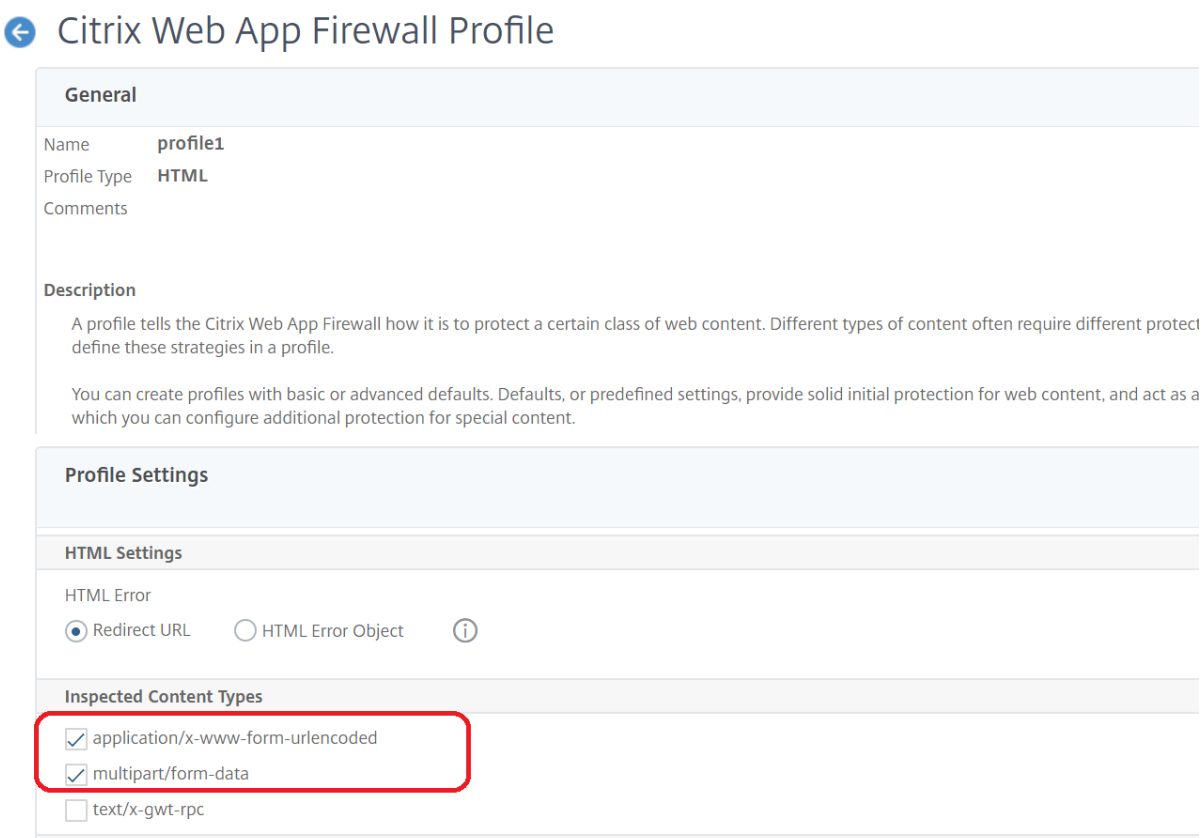
   > **Hinweis:**
   > Sie können jeden gültigen MIME-Typ in die Liste der zulässigen Inhaltstypen aufnehmen. Da viele Dokumenttypen aktive Inhalte und daher potenziell bösartige Inhalte enthalten können, müssen Sie Vorsicht walten lassen, wenn Sie MIME-Typen zu dieser Liste hinzufügen.

   c) Geben Sie eine kurze Beschreibung an, aus der der Grund für das Hinzufügen dieses bestimmten MIME-Typs zur Liste der zulässigen Inhaltstypen erklärt wird.
   d) Klicken Sie auf **Erstellen** oder **OK**, um Ihre Änderungen zu speichern.
8. Klicken Sie auf **Schließen**, um das Dialogfeld „Zulässige Inhaltstypen verwalten“ zu schließen und zur Registerkarte „ **Einstellungen** “ zurückzukehren.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So verwalten Sie die Inhaltstypen Urlencoded und MultiPart-Form mithilfe der NetScaler-GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile**.

2. Wählen Sie im Detailbereich das zu konfigurierende Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie auf der Seite **Web App Firewall-Profil konfigurierenim Abschnitt Erweiterte Einstellungendie Profileinstellungen** aus.
4. Stellen Sie im Abschnitt **Inspected Content Type** die folgenden Parameter ein:
   a) application/x-www-form-urlencoded. Markieren Sie das Kontrollkästchen, um den URL-codierten Inhaltstyp zu überprüfen.
   b) Mehrteile/Formulardaten. Wählen Sie das Häkchen aus, um den Inhaltstyp MultiPart-Form zu überprüfen.
5. Klicken Sie auf **OK**.



Profile

August 19, 2021

Ein Profil ist eine Sammlung von Sicherheitseinstellungen, die zum Schutz bestimmter Arten von Webinhalten oder bestimmten Teilen Ihrer Website verwendet werden. In einem Profil bestimmen

Sie, wie die Web App Firewall jeden ihrer Filter (oder Prüfungen) auf Anfragen an Ihre Websites und Antworten von ihnen anwendet. Die Web App Firewall unterstützt zwei Arten von Profilen: vier integrierte (Standard-) Profile, für die keine weitere Konfiguration erforderlich ist, und benutzerdefinierte Profile, die eine weitere Konfiguration erfordern.

Eingebaute Profile

Die vier integrierten Web App Firewall -Profile bieten einfachen Schutz für Anwendungen und Websites, die entweder keinen Schutz benötigen oder auf die Benutzer überhaupt nicht direkt zugreifen dürfen. Folgende Profiltypen sind:

- **APPFW_BYPASS.** Überspringt die gesamte Filterung der Web App Firewall und sendet den unveränderten Datenverkehr an die geschützte Anwendung oder Website oder an den Client.
- **APPFW_RESET.** Setzt die Verbindung zurück und erfordert, dass der Client seine Sitzung wiederherstellt, indem er eine bestimmte Startseite besucht.
- **APPFW_DROP.** Lässt den gesamten Datenverkehr zur oder von der geschützten Anwendung oder Website fallen und sendet keinerlei Antwort an den Kunden.
- **APPFW_BLOCK.** Blockiert den Datenverkehr zu oder von der geschützten Anwendung oder Website.

Sie verwenden die integrierten Profile genau wie benutzerdefinierte Profile, indem Sie eine Richtlinie konfigurieren, die den Datenverkehr auswählt, auf den Sie das Profil anwenden möchten, und dann das Profil Ihrer Richtlinie zuordnen. Da Sie keine integrierte Richtlinie konfigurieren müssen, bietet sie eine schnelle Möglichkeit, bestimmte Arten von Datenverkehr oder Datenverkehr zuzulassen oder zu blockieren, die an bestimmte Anwendungen oder Websites gesendet werden.

Benutzerdefinierte Profile

Benutzerdefinierte Profile sind Profile, die von Benutzern erstellt und konfiguriert werden. Im Gegensatz zu den Standardprofilen müssen Sie ein benutzerdefiniertes Profil konfigurieren, bevor es den Datenverkehr zu und von Ihren geschützten Anwendungen filtert.

Es gibt drei Arten von benutzerdefinierten Profilen:

- **HTML.** Schützt HTML-basierte Webseiten.
- **XML.** Schützt XML-basierte Webservices und Websites.
- **Web 2.0.** Schützt Web 2.0-Inhalte, die HTML- und XML-Inhalte wie ATOM-Feeds, Blogs und RSS-Feeds kombinieren.

Die Web App Firewall verfügt über eine Reihe von Sicherheitsprüfungen, die alle aktiviert oder deaktiviert werden können und in jedem Profil auf verschiedene Arten konfiguriert werden können. Jedes Profil verfügt außerdem über eine Reihe von Einstellungen, mit denen gesteuert wird, wie

verschiedene Inhaltstypen verarbeitet werden. Statt alle Sicherheitsprüfungen manuell zu konfigurieren, können Sie die Lernfunktion aktivieren und konfigurieren. Diese Funktion beobachtet den normalen Datenverkehr zu Ihren geschützten Websites für einen bestimmten Zeitraum und verwendet diese Beobachtungen, um Ihnen eine maßgeschneiderte Liste empfohlener Ausnahmen (*Entspannungen*) für einige Sicherheitskontrollen und zusätzliche Regeln für andere Sicherheitsprüfungen zu liefern.

Bei der Erstkonfiguration, sei es, ob Sie den Web App Firewall Wizard oder manuell verwenden, erstellen Sie normalerweise ein Allzweckprofil, um alle Inhalte auf Ihren Websites zu schützen, die nicht von einem spezifischeren Profil abgedeckt werden. Danach können Sie so viele spezifische Profile erstellen, wie Sie spezialisierte Inhalte schützen möchten.

Der Bereich Profile besteht aus einer Tabelle, die die folgenden Elemente enthält:

Name. Zeigt alle Web App Firewall Profile an, die in der Appliance konfiguriert sind.

Gebundene Signatur. Zeigt das Signaturobjekt an, das an das Profil in der vorherigen Spalte gebunden ist, sofern vorhanden.

Richtlinien. Zeigt die Web App Firewall Richtlinie an, die das Profil in der Spalte ganz links dieser Zeile aufruft, sofern vorhanden.

Kommentare. Zeigt den dem Profil zugeordneten Kommentar in der Spalte ganz links dieser Zeile an.

Profiltyp. Zeigt den Profiltyp an. Typen sind Built-in, HTML, XML und Web 2.0.

Über der Tabelle befindet sich eine Reihe von Schaltflächen und eine Dropdownliste, mit der Sie Informationen zu Ihren Profilen erstellen, konfigurieren, löschen und anzeigen können:

- **Add.** Fügen Sie der Liste ein neues Profil hinzu.
- **Bearbeiten.** Bearbeiten Sie das ausgewählte Profil.
- **Löschen.** Löschen Sie das ausgewählte Profil aus der Liste.
- **Statistik.** Zeigen Sie die Statistiken für das ausgewählte Profil an.
- **Aktion.** Dropdownliste, die zusätzliche Befehle enthält. Derzeit können Sie ein Profil importieren, das aus einer anderen Web App Firewall Konfiguration exportiert wurde.

Erstellen von Web App Firewall-Profilen

May 11, 2023

Sie können ein Web App Firewall-Profil auf zwei Arten erstellen: über die Befehlszeile und über die GUI. Das Erstellen eines Profils mit der Befehlszeile erfordert, dass Sie Optionen in der Befehlszeile angeben. Der Prozess ähnelt dem Konfigurieren eines Profils, und mit wenigen Ausnahmen nehmen die beiden Befehle dieselben Parameter an.

> **Hinweis**
>
> **Core-Profil**: Dieses Profil ist in Build 33.x und höher verfügbar. Es enthält begrenzte, aber grundlegende Sicherheitsprüfungen, die standardmäßig aktiviert sind, wohingegen bei den Profilen Basic und Advanced standardmäßig viele andere Sicherheitsprüfungen aktiviert sind. Das Kernprofil enthält die folgenden Sicherheitsüberprüfungen:
>
> - Grammatikbasierte SQL-Einschleusung
> - Grammatikbasierte CMD-Einschleusung
> - Cross-Site Scripting
> - Pufferüberlauf
> -
>
> **CVE-Profil**mit blockierten Schlüsselwörtern: Dieses Profil ist in Build 42.x und höher verfügbar. Verwenden Sie dieses Profil nur, um eine Signatur hinzuzufügen und zu binden. Es deaktiviert alle Prüfungen der NetScaler Web App Firewall mit Ausnahme der CVE-Prüfung.

Geben Sie beim Erstellen eines Profils eine der folgenden Optionen an: Basic, Advanced, Core oder CVE. Die Standardkonfiguration für die verschiedenen Sicherheitsüberprüfungen und -einstellungen, die Teil dieses Profils sind, wird angewendet. Sie können optional auch einen Kommentar hinzufügen. Nachdem Sie das Profil erstellt haben, müssen Sie es dann konfigurieren, indem Sie es im Datenbereich auswählen und dann auf **Bearbeiten**klicken.

Wenn Sie vorhaben, die Lernfunktion zu verwenden oder viele erweiterte Schutzmaßnahmen zu aktivieren und zu konfigurieren, müssen Sie erweiterte Standardeinstellungen wählen. Insbesondere wenn Sie planen, eine der SQL-Einschleusungstests, eine der Cross-Site-Scriptingprüfungen, jede Überprüfung, die Schutz vor Webformular-Angriffen bietet, oder die Cookie-Konsistenzprüfung zu konfigurieren, müssen Sie planen, die Lernfunktion zu verwenden. Sofern Sie bei der Konfiguration dieser Prüfungen nicht die richtigen Ausnahmen für Ihre geschützten Websites angeben, können diese den legitimen Datenverkehr blockieren. Es ist schwierig, alle Ausnahmen zu antizipieren, ohne zu weit gefasste Ausnahmen zu schaffen. Die Lernfunktion erleichtert diese Aufgabe erheblich. Andernfalls sind die grundlegenden Standardeinstellungen schnell und müssen den Schutz bieten, den Ihre Webanwendungen benötigen.

Es gibt drei Profiltypen:

- **HTML.** Schützt Standard-HTML-basierte Websites.
- **XML.** Schützt XML-basierte Webdienste und Websites.
- **Web 2.0 (HTML-XML).** Schützt Websites, die sowohl HTML- als auch XML-Elemente enthalten, wie ATOM-Feeds, Blogs und RSS-Feeds.

Es gibt auch ein paar Einschränkungen für den Namen, den Sie einem Profil geben können. Ein Profilname darf nicht mit dem Namen übereinstimmen, der einem anderen Profil oder einer anderen

Aktion in einer Funktion der NetScaler Appliance zugewiesen wurde. Bestimmte Aktions- oder Profilnamen werden integrierten Aktionen oder Profilen zugewiesen und können niemals für Benutzerprofile verwendet werden. Eine vollständige Liste der nicht zulässigen Namen finden Sie in den zusätzlichen Informationen zumWeb App Firewall-Profil. Wenn Sie versuchen, ein Profil mit einem Namen zu erstellen, der bereits für eine Aktion oder ein Profil verwendet wurde, wird eine Fehlermeldung angezeigt, und das Profil wird nicht erstellt.

So erstellen Sie ein Web App Firewall-Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw profile <name> [-defaults ( basic | advanced | core | cve)]`
- `set appfw profile <name> -type ( HTML | XML | HTML XML )`
- `set appfw profile <name> -comment "<comment>"`
- `save ns config`

Beispiel

Im folgenden Beispiel wird ein Profil mit dem Namen `pr-basic`mit grundlegenden Standardeinstellungen hinzugefügt und der Profiltyp HTML zugewiesen. Dies ist die geeignete Erstkonfiguration für ein Profil zum Schutz einer HTML-Website.

```
1 add appfw profile pr-basic -defaults basic -comment "Simple profile for
      websites."
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

So erstellen Sie ein Web App Firewall-Profil mit der GUI

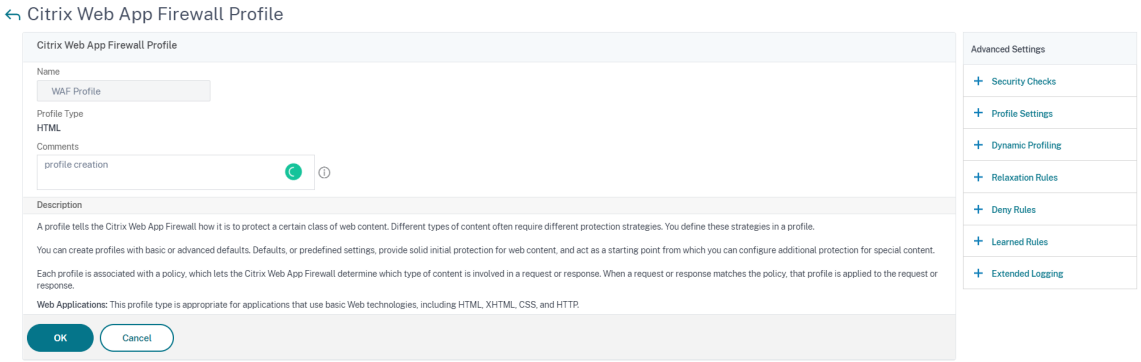
Führen Sie das folgende Verfahren aus, um ein Web App Firewall-Profil zu erstellen:

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **“Web App Firewall-Profil erstellen** “ die folgenden grundlegenden Parameter fest:
   a) Name
   b) Profiltyp
   c) Anmerkungen
   d) Standardwerte

e) Beschreibung

4. Klicken Sie auf **OK**.
5. Wählen Sie das von Ihnen erstellte Profil aus und klicken Sie auf **Bearbeiten**.
6. Führen Sie im Abschnitt **Erweiterte Einstellungen** die folgenden Konfigurationen aus:

   a) Sicherheitschecks
   b) Profil-Einstellungen
   c) Dynamische Profilerstellung
   d) Regeln für Entspannung
   e) Regeln verweigern
   f) Gelernte Regel
   g) Erweiterte Protokollierung



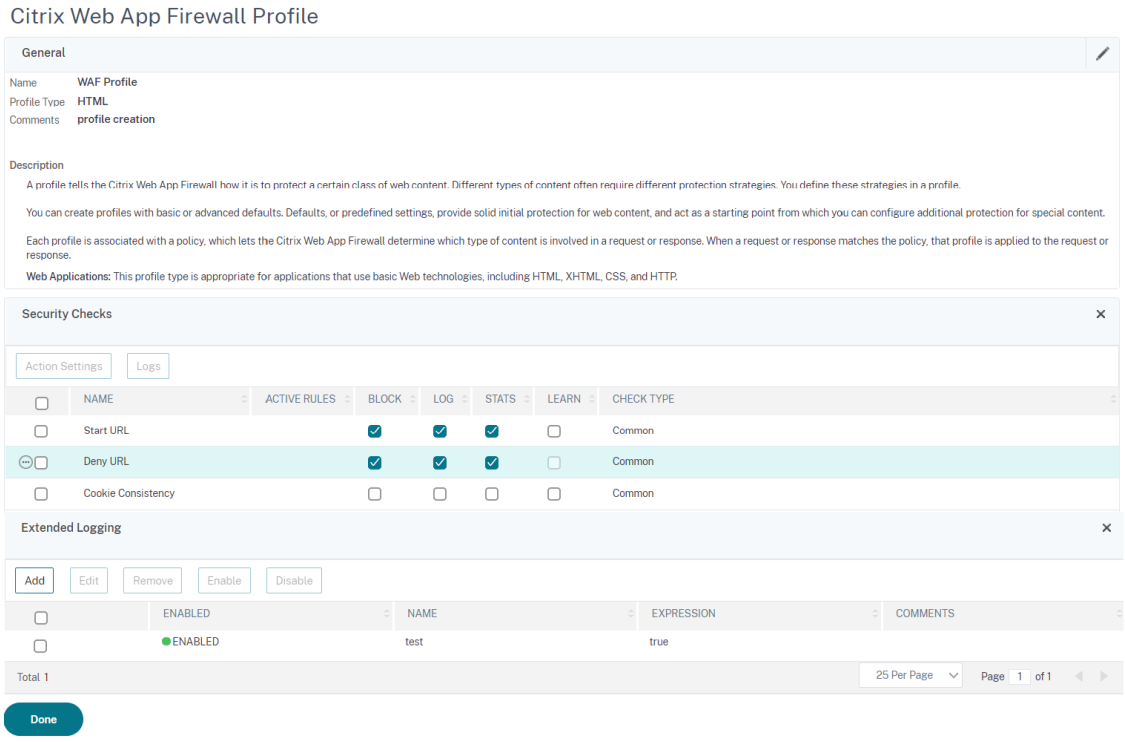
7. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** einen Sicherheitsschutz aus und klicken Sie auf **Aktionseinstellungen**.
8. Legen Sie auf der Seite “Sicherheitsprüfung” die Parameter fest.

   > **Hinweis:**
   >
   > Die Einstellung **Aktive Regel** ist nur für die Überprüfung von **HTML SQL Injection** verfügbar, um eine Entspannungsregel oder eine Verweigerungsregel für die SQL-Injection-P Weitere Informationen finden Sie unter Thema Entspannungs- und Verweigerungsregeln .

9. Klicken Sie auf **OK** und auf **Schließen**.
10. Legen Sie im Abschnitt **Profileinstellungen** die Profilparameter fest. Weitere Informationen finden Sie unter Konfigurieren der Einstellungen des Web App Firewall-Profils .
11. Wählen Sie im Abschnitt **Dynamische Profilerstellung** eine Sicherheitsprüfung aus, um dynamische Profileinstellungen hinzuzufügen. Weitere Informationen finden Sie unter Thema Dynamisches Profil .
12. Klicken Sie im Abschnitt **Entspannungsregeln** auf **Bearbeiten**, um eine Entspannungsregel

für eine Sicherheitsprüfung hinzuzufügen. Weitere Informationen finden Sie unter Entspannungsregel für Einzelheiten.

13. Fügen Sie im Abschnitt **Regeln ablehnen** eine Ablehnungsregel für die HTML-SQL-Injection-Prüfung hinzu. Weitere Informationen finden Sie unter Regeln für HTML-Ablehnung .
14. Legen Sie im Abschnitt **Gelernte Regel** die Lerneinstellungen fest. Weitere Informationen finden Sie unter Learning von Web App Firewall .
15. Klicken Sie im Abschnitt **Erweiterte Protokollierung** auf **Hinzufügen**, um sensible Daten zu maskieren. Weitere Informationen finden Sie unter Thema Erweiterte Protokollierung .
16. Klicken Sie auf **Fertig**und dann auf **Schließen**.



Konfigurieren von Regeln zum Erkennen gefälschter Konten

Die Erstellung eines gefälschten Kontos ist ein automatisierter Prozess zum Erstellen vieler Benutzerkonten, die nicht mit einer realen Person verknüpft sind, oder zum Erstellen von Benutzerkonten mit den Daten der realen Person ohne deren Zustimmung. Gefälschte Konten, die nicht legitime Benutzer erstellen, verwenden Registrierungsdetails, die nicht der wahren Identität einer Person entsprechen. Diese Konten werden erstellt, um Dienste, die von einer Webanwendung angeboten werden, für nicht legitime Zwecke wie Phishing-Angriffe, Verbreitung gefälschter Nachrichten, Scalping usw. zu missbrauchen. In den meisten Fällen werden diese Konten von Bots erstellt, die von böswilligen Benutzern ausgeführt werden.

Die NetScaler-Appliance wurde erweitert, um gefälschte Konten zu erkennen, indem Regeln zur Erkennung gefälschter Konten an ein Web App Firewall-Profil gebunden werden. Die Regel besteht aus Formular-URLs und Formularparametern für jede URL. Wenn eine eingehende Anfrage mit einem Ausdruck oder einer Formular-URL (Anmeldeseiten) übereinstimmt, die für eine Regel zur Erkennung gefälschter Konten konfiguriert ist, gilt die Auswertung für einen verdächtigen Anmeldeversuch und die Anforderungsdaten werden zur weiteren Überprüfung an den ADM-Server gesendet.

Führen Sie die folgenden Schritte aus, um die Erkennung gefälschter Konten mithilfe der Befehlsschnittstelle zu konfigurieren

1. Funktion zur Erkennung gefälschter Konten aktivieren
2. Regeln für gefälschte Konten binden

Funktion zur Erkennung gefälschter Konten aktivieren

Geben Sie in der Befehlszeile Folgendes ein:

```
add/set appfw profile <name> -FakeAccountDetection ( ON | OFF )
```

Beispiel:

```
add appfw profile profile1 -FakeAccountDetection ON
```

Regeln für gefälschte Konten binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile <name> -FakeAccount (string|expression)isFieldNameRegex
 (ON|OFF)-tag <TagExpression> ([-formUrl <FormURL>]| [-formExpression <
FormExpression>)])-state (ENABLED|DISABLED)
```

Hierbei gilt:

- `formUrl`: URL der HTTP-Formularaktion.
  formExpression: Zu bewertender Formausdruck.
- `fakeaccount`: Name des gefälschten Kontos.
  Tag: Tag-Ausdruck.
- `isFieldNameRegex`: Gibt an, ob fieldName Regex ist. Standardwert AUS.

Beispiel:

```
bind appfw profile profile1 -FakeAccount john -formURL  “/signup.php"-tag "
smith"
bind appfw profile profile2 -FakeAccount Will -formExpression "HTTP.REQ.
HEADER(\"Authorization\").CONTAINS(\"/test_accounts\").NOT && HTTP.REQ.URL.
CONTAINS(\"/login.php\")"-fieldName -tag "smith"
```

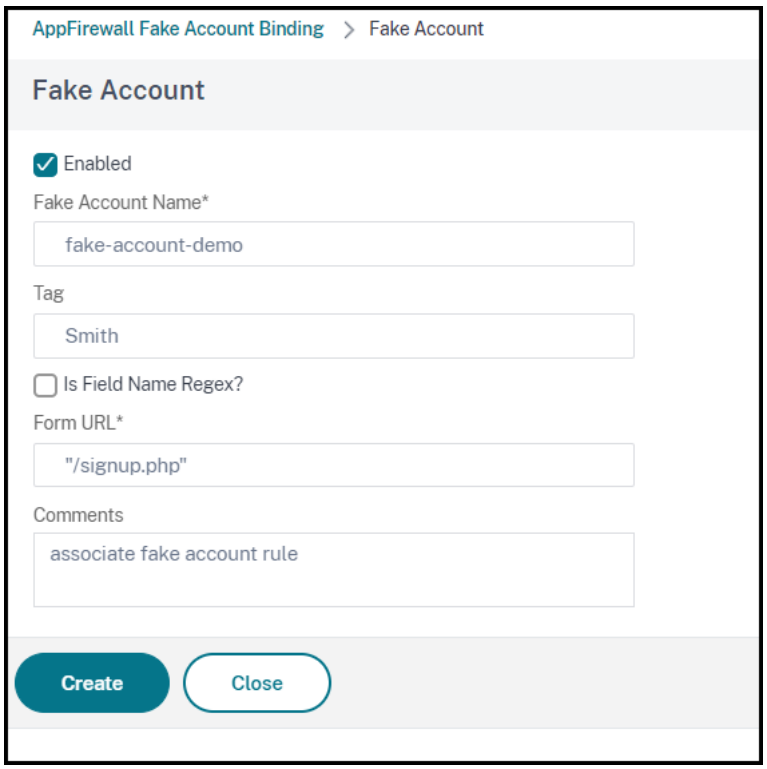

Beispieleingabe für eine HTTP-Post-Anfrage zur `example.com`-Anmeldeseite.

s.nein	Eingabe	Beispiel
1	Endpunkt-URL der HTTP-POST-Anforderung anmelden	`https://webapi.example.com/account/api/v1.0/contacts/`
2	E-Mail Feldname in der HTTP-Post-Anfrage	E-Mail-Adresse
3	Vorname Feldname in der HTTP-Post-Anfrage	Vorname
4	Nachname Feldname in der HTTP-Post-Anfrage	Nachname

Konfigurieren der Regel zur Erkennung gefälschter Konten der Web App Firewall über die GUI

Führen Sie die folgenden Schritte aus, um die Regel zur Erkennung gefälschter Konten über die GUI zu konfigurieren.

1. Navigieren Sie zu **Konfiguration** > **Sicherheit** > **NetScaler Web App Firewall** > **Profil**.
2. Wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der **Profilseite von NetScaler Web App Firewall** auf **Sicherheitsprüfungen** aus den **erweiterten Einstellungen**.
4. Wählen Sie im Abschnitt **Mit Citrix Cloud integrierte Prüfungen** eine Regel für gefälschte Konten aus und klicken Sie auf **Bearbeiten**.
5. Wählen Sie im **AppFirewall-Schieberegler für gefälschte Kontobindung** eine Regel zum Bearbeiten aus oder klicken Sie auf **Hinzufügen**.
6. Legen Sie auf der **Regelseite für gefälschte Konten** die folgenden Parameter fest:
   a) **Aktiviert**. Wählen Sie aus, um die Regel für gefälschte Konten zu aktivieren
   b) **Falscher Kontoname**. Name der Fake-Account-Regel.
   c) **Etikett**. Vorname im Formular zur Registrierung eines gefälschten Kontos.
   d) **Ist Feldname Regex?** Wählen Sie aus, ob das Formularfeld ein regulärer Ausdruck ist.
   e) **Formular-Ausdruck**. Regulärer Ausdruck, der das gefälschte Konto definiert.
   f) **Formular-URL**. Geben Sie die URL zur Erkennung gefälschter Konten ein
   g) **Kommentare**. Eine kurze Beschreibung der Regel zur Erkennung gefälschter Konten.
7. Klicken Sie auf **Erstellen**.



Erzwingen der HTTP-RFC-Konformität

May 11, 2023

NetScaler Web App Firewall prüft den eingehenden Datenverkehr auf HTTP-RFC-Konformität und legt jede Anforderung ab, die standardmäßig RFC-Verstöße aufweist. Es gibt jedoch bestimmte Szenarien, in denen die Appliance möglicherweise eine nicht RFC-Konformitätsanforderung Bypass oder blockieren muss. In solchen Fällen können Sie die Appliance so konfigurieren, dass solche Anfragen auf globaler oder Profilebene Bypass oder blockiert werden.

Blockieren oder Bypass Sie nicht RFC-konforme Anfragen auf globaler Ebene

Das HTTP-Modul identifiziert eine Anfrage als ungültig, wenn sie unvollständig ist und solche Anfragen nicht von der WAF bearbeitet werden können. Zum Beispiel fehlt eine eingehende HTTP-Anforderung, bei der ein Host-Header fehlt. Um solche ungültigen Anfragen zu blockieren oder zu Bypass, müssen Sie die Option `malformedReqAction` in den globalen Einstellungen der Anwendungs-Firewall konfigurieren.

Der Parameter ‘malformedReqAction’ überprüft die eingehende Anforderung auf ungültige Inhaltslänge, ungültige Chunked-Anforderung, keine HTTP-Version und unvollständigen Header.

> **Hinweis:**
>
> Wenn Sie die Blockoption im Parameter `malformedReqAction` deaktivieren, umgeht die Appliance die gesamte App-Firewall-Verarbeitung für alle Nicht-RFC-Konformitätsanforderungen und leitet die Anforderungen an das nächste Modul weiter.

So blockieren oder Bypass Sie ungültige HTTP-Anfragen ohne RFC-Beschwerde mithilfe der Befehlszeilenschnittstelle

Um ungültige Anfragen zu blockieren oder zu Bypass, geben Sie den folgenden Befehl ein:

```
set appfw settings -malformedreqaction <action>
```

Beispiel:

```
set appfw settings -malformedReqAction block
```

So zeigen Sie fehlerhafte Anforderungsaktionseinstellungen an

Um die Einstellungen für fehlerhafte Anforderungsaktionen anzuzeigen, geben Sie den folgenden Befehl ein:

```
show appfw settings
```

Ausgang:

```
1 DefaultProfile: APPFW_BYPASS UndefAction: APPFW_BLOCK SessionTimeout:
      900 LearnRateLimit: 400 SessionLifetime: 0
    SessionCookieName: citrix_ns_id ImportSizeLimit: 134217728
    SignatureAutoUpdate: OFF SignatureUrl:"https://s3.amazonaws.com/
    NSAppFwSignatures/SignaturesMapping.xml" CookiePostEncryptPrefix:
    ENC GeoLocationLogging: OFF CEFLogging: OFF EntityDecoding:
     OFF UseConfigurableSecretKey: OFF SessionLimit: 100000
    MalformedReqAction: block log stats
2  Done
3 <!--NeedCopy-->
```

So blockieren oder Bypass Sie ungültige HTTP-Anfragen ohne RFC-Beschwerde mithilfe der NetScaler GUI

1. Navigieren Sie zu **Sicherheit** > **NetScaler Web App Firewall**.
2. Klicken Sie auf der Seite **NetScaler Web App Firewall** unter **Einstellungen** auf **Engine-Einstellungen** ändern.
3. Wählen Sie auf der Seite **NetScaler Web App Firewall-Einstellungen konfigurieren** die Option **Fehlerhafte Anforderung protokollieren** als Blockieren, Log oder Statistik aus.

4. Klicken Sie auf **OK** und auf **Schließen**.

> **Hinweis:**
>
> Wenn Sie die Auswahl der Blockaktion aufheben oder keine fehlerhafte Anforderungsaktion auswählen, umgeht die Appliance die Anforderung, ohne den Benutzer zu verweilen.

Blockieren oder Umgehen von nicht RFC-konformen Anforderungen auf Profilebene

Andere nicht RFC-konforme Anforderungen können so konfiguriert werden, dass sie auf Profilebene blockiert oder umgangen werden. Sie müssen das RFC-Profil entweder im Block- oder Bypass-Modus konfigurieren. Durch diese Konfiguration wird jeder ungültige Datenverkehr, der mit dem Web App Firewall-Profil übereinstimmt, entweder umgangen oder entsprechend blockiert. Das RFC-Profil überprüft die folgenden Sicherheitsüberprüfungen:

- Ungültige GWT-RPC-Anfragen
- Ungültige Kopfzeilen für Inhaltstypen
- Ungültige Multipart-Anfragen
- Ungültige JSON-Anfragen
- Doppelte Cookie-Namen-Wert-Paarprüf

> **Hinweis:**
>
> Wenn Sie das Profil `RFC` in den Modus "Bypass" setzen, müssen Sie sicherstellen, dass Sie die Transformationsoption in den **HTML Cross-Site-Scripting-Einstellungen** und in den Abschnitten **HTML SQL Injection Settings** deaktivieren. Wenn Sie das `RFC`-Profil im Bypass-Modus aktivieren und festlegen, zeigt die Appliance eine Warnmeldung an: "Site-übergreifende Skripte umwandeln" und "SQL-Sonderzeichen transformieren" sind beide derzeit eingeschaltet. Empfehlen Sie es auszuschalten, wenn es mit verwendet wird `APPFW_RFC_BYPASS`.
>
> **Wichtig:**
>
> Außerdem zeigt die Appliance einen Warnhinweis an: "Appfw-Sicherheitsprüfungen sind möglicherweise nicht auf Anfragen anwendbar, die gegen RFC-Prüfungen verstoßen, wenn dieses Profil festgelegt wird. Das Aktivieren einer Transformationseinstellung wird nicht empfohlen, da Anfragen möglicherweise teilweise transformiert werden, die RFC-Verstöße enthalten.

So konfigurieren Sie ein RFC-Profil im Web App Firewall-Profil mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
set appfw profile <profile_name> -rfcprofile <rfcprofile_name
```


Beispiel

```
set appfw profile P1 -rfcprofile APPFW_RFC_BLOCK
```

> **Hinweis:**
>
> Standardmäßig ist das RFC-Profil im Blockmodus an das Web App Firewall-Profil gebunden.

So konfigurieren Sie ein RFC-Profil im Web App Firewall-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Web App Firewall-Profil** im Abschnitt **Erweiterte Einstellungen** auf **Profileinstellungen**.
4. Stellen Sie im Abschnitt **HTML-Einstellungen** das RFC-Profil auf den Modus APPFW_RFC_BYPASS ein.
   Das System zeigt eine Warnmeldung an: Appfw Security checks enabled ist möglicherweise nicht für Anforderungen anwendbar, die gegen RFC-Prüfungen verstößt, wenn dieses Profil eingestellt ist. Das Aktivieren einer Transformationseinstellung wird nicht empfohlen, da Anfragen teilweise transformiert werden können, die RFC-Verletzungen enthalten.

Konfigurieren von Web App Firewall-Profilen

May 11, 2023

Um ein benutzerdefiniertes Web App Firewall-Profil zu konfigurieren, konfigurieren Sie zunächst die Sicherheitsüberprüfungen, die im Web App Firewall-Assistenten als *tiefer Schutz**oder erweiterter Schutz* bezeichnet werden. Bestimmte Prüfungen erfordern eine Konfiguration, wenn Sie sie überhaupt verwenden möchten. Andere haben Standardkonfigurationen, die sicher, aber begrenzt sind. Ihre Websites benötigen oder profitieren möglicherweise von einer anderen Konfiguration, die mehr Funktionen bestimmter Sicherheitsüberprüfungen nutzt.

Nachdem Sie die Sicherheitsüberprüfungen konfiguriert haben, können Sie auch einige andere Einstellungen konfigurieren, die das Verhalten steuern, nicht einer einzigen Sicherheitsüberprüfung, sondern der Web App Firewall-Funktion. Die Standardkonfiguration reicht aus, um die meisten Websites zu schützen, aber Sie müssen sie überprüfen, um sicherzustellen, dass sie für Ihre geschützten Websites geeignet sind.

> **Hinweis:**
>
> Die Länge des Profilnamens und die gesamte Länge des Importobjektnamens können bis zu 127

> Zeichen festgelegt werden.

Weitere Informationen zu den Sicherheitsprüfungen der Web App Firewall finden Sie unter Erweiterter Schutz.

So konfigurieren Sie ein Web App Firewall-Profil mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> <arg1> [<arg2> ...]`

  Wobei:

  - `<arg1>` = ein Parameter und alle zugehörigen Optionen.
  - `<arg2>` = ein zweiter Parameter und alle zugehörigen Optionen.
  - … = zusätzliche Parameter und Optionen.

  Eine Beschreibung der Parameter, die beim Konfigurieren bestimmter Sicherheitsprüfungen verwendet werden sollen, finden Sie unter Erweiterter Schutz.

- `save ns config`

Beispiel

Das folgende Beispiel zeigt, wie das Blockieren für die Prüfungen HTML SQL Injection und HTML Cross-Site Scripting in einem Profil mit dem Namen `pr-basic`aktiviert wird. Dieser Befehl ermöglicht das Blockieren dieser Aktionen, ohne weitere Änderungen am Profil vorzunehmen.

```
1 set appfw profile pr-basic -crossSiteScriptingAction block -
     SQLInjectionAction block
2 <!--NeedCopy-->
```

Binden einer Entspannungsregel an ein Web App Firewall-Profil

Wenn eine Web App Firewall einen Verstoß erkennt, hat der Benutzer die Möglichkeit, die durch Relaxationsregeln angewendete Aktion zu Bypass. Die Entspannungsregel ist eine Ausnahme, die auf die erkannte Sicherheitsverletzung angewendet wird. Zum Beispiel schützen die Regeln zur Entspannung der Start-URL vor gewaltsamen Surfen. Bekannte Webserver-Schwachstellen, die von Hackern ausgenutzt werden, können erkannt und blockiert werden, indem eine Reihe von standardmäßigen Deny-URL-Regeln aktiviert wird. Häufig gestartete Angriffe wie Pufferüberlauf, SQL oder siteübergreifende Skripterstellung können ebenfalls leicht erkannt werden.

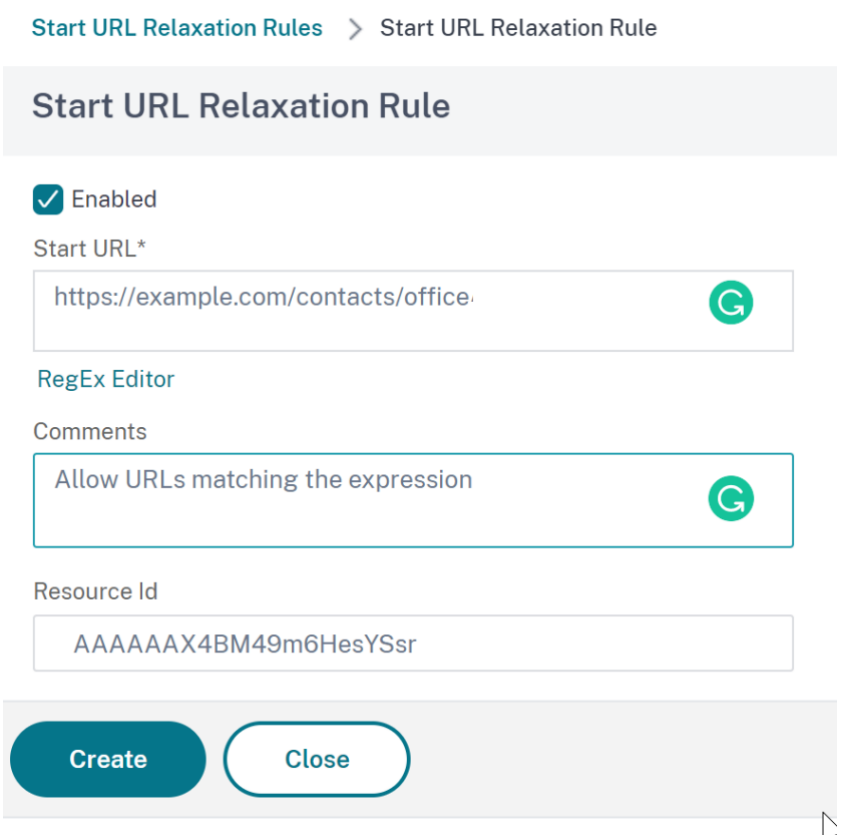
Bindung von Sicherheitsbefreiungs- oder Entspannungsregeln über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile <name> ((-startURL <expression> [-resourceId  <
    string>]) | -denyURL <expression> | (-fieldConsistency <string>   <
    formActionURL> [-isRegex ( REGEX | NOTREGEX )]) | (-
    cookieConsistency <string> [-isRegex ( REGEX | NOTREGEX )]) | (-
    SQLInjection <string> <formActionURL> [-isRegex ( REGEX | NOTREGEX )
    ] [-location <location>] [-valueType <valueType> <valueExpression
    >....
<!--NeedCopy-->
```

So binden Sie Sicherheitsbefreiungs- oder Lockerungsregeln über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der **Profilseite der NetScaler Web App Firewall** im Abschnitt **Erweiterte Einstellungen** auf **Entspannungsregeln** .
4. Klicken Sie im Abschnitt **Entspannungsregeln** auf **startURL** und dann auf **Bearbeiten**.
5. Klicken Sie auf der Seite **Regeln zur Entspannung der Start-URL** auf **Hinzufügen**.
6. Legen **Sie auf der Seite Regel zur Entspannung der Start-URL** die folgenden Parameter fest:
    a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um die Entspannungsregel zu aktivieren
    b) Startet die URL. Geben Sie den Wert für regulären Ausdruck
    c) Kommentare. Geben Sie eine kurze Beschreibung der Entspannungsregel an.
7. Klicken Sie auf **Erstellen** und **Schließen**.



So konfigurieren Sie ein Web App Firewall-Profil über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich das zu konfigurierende Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Konfigurieren Sie im Dialogfeld **Web App Firewall-Profil konfigurieren** auf der Registerkarte **Sicherheitsüberprüfungen** die Sicherheitsüberprüfungen.
   - Um eine Aktion für eine Prüfung zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie in der Liste das Kontrollkästchen für die Aktion.
   - Um die Parameter für die Sicherheitsüberprüfungen in der Liste zu konfigurieren, aktivieren Sie das Kontrollkästchen und klicken Sie auf **Aktive Einstellungen**.
   - Um die Protokolleinträge für die ausgewählte Sicherheitsüberprüfung zu überprüfen, aktivieren Sie das Kontrollkästchen und klicken Sie auf **Protokolle**. Mithilfe dieser Informationen können Sie die Sicherheitsüberprüfungen ermitteln, die mit Angriffen übereinstimmen, sodass Sie den Datenverkehr für die Sicherheitsüberprüfungen blockieren können. Sie können die Informationen auch verwenden, um zu ermitteln, welche Prüfungen mit legitimem Datenverkehr übereinstimmen, sodass Sie eine entsprechende Ausnahme kon-

figurieren können, um diese legitimen Verbindungen zuzulassen. Weitere Informationen zu den Protokollen finden Sie unter Protokolle, Statistiken und Berichte.

- Um eine Überprüfung vollständig zu deaktivieren, deaktivieren Sie in der Liste alle Kontrollkästchen rechts neben dieser Prüfung.

4. Konfigurieren Sie auf der Registerkarte **Einstellungen** die Profileinstellungen.
   - Um das Profil mit dem Satz von Signaturen zu verknüpfen, die Sie zuvor erstellt und konfiguriert haben, wählen Sie unter Allgemeine Einstellungen diesen Signatursatz in der Dropdownliste **Signaturen** aus.

     > **Hinweis:**
     >
     > Sie müssen die Bildlaufleiste auf der rechten Seite des Dialogfelds verwenden, um nach unten zu scrollen, um den Abschnitt Allgemeine Einstellungen anzuzeigen.

   - Um ein HTML- oder XML-Fehlerobjekt zu konfigurieren, wählen Sie das Objekt aus der entsprechenden Dropdownliste aus.

     > **Hinweis:**
     >
     > Sie müssen zuerst das Fehlerobjekt hochladen, das Sie im Bereich Importe verwenden möchten. Weitere Informationen zum Importieren von Fehlerobjekten finden Sie unter Importe.

   - Um den Standard-XML-Inhaltstyp zu konfigurieren, geben Sie die Inhaltstypzeichenfolge direkt in die Textfelder Standardanforderung und Standardantwort ein oder klicken Sie auf Zulässige Inhaltstypen verwalten, um die Liste der zulässigen Inhaltstypen zu verwalten »Mehr…..

5. Wenn Sie die Lernfunktion verwenden möchten, klicken Sie auf Lernen und konfigurieren Sie die Lerneinstellungen für das Profil, wie unter Konfigurieren und Verwenden der Lernfunktionbeschrieben.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Bereich **Profile** zurückzukehren.

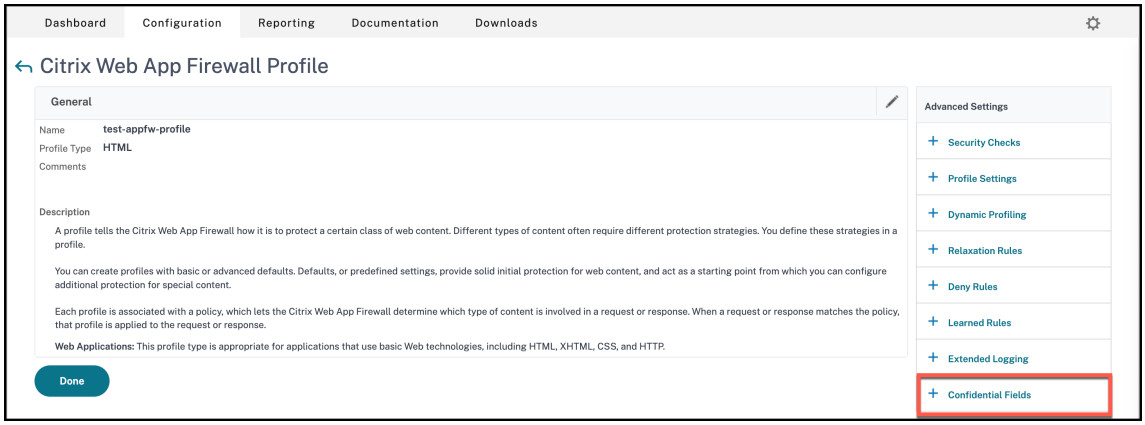
Vertrauliche Felder im WAF-Profil

> **Hinweis**
>
> Diese Funktion ist in Version 13.1 Build 27.x und höher verfügbar.

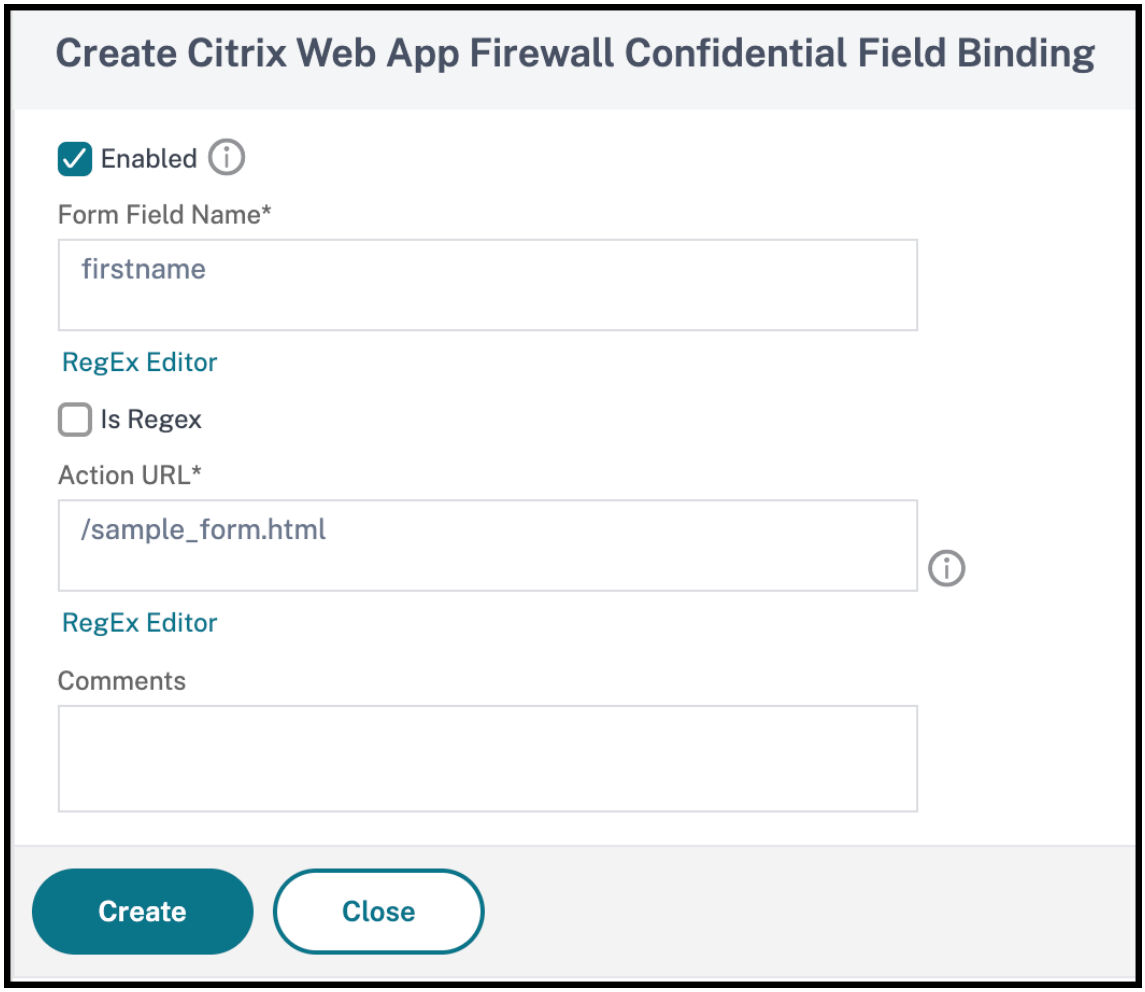
Sie können jetzt vertrauliche Felder in einem WAF-Profil hinzufügen. Diese Felder sind maskiert und werden nicht in den ADC-Protokollen erfasst, wenn ein Verstoß auftritt. Zuvor konnten Sie diese Felder nur mit Einstellungen hinzufügen. Weitere Informationen zum Hinzufügen vertraulicher Felder mithilfe von Einstellungen finden Sie unter Vertrauliche Felder.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.

2. Wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie in den erweiterten **Einstellungen** auf **Vertrauliche Felder**.



4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie Werte für die folgenden Parameter ein:
   - Name des Formularfelds*
   - URL der Aktion*
   - Anmerkungen



* steht für ein Pflichtfeld

6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Fertig**.

Profileinstellungen der Webanwendungs-Firewall

May 11, 2023

Im Folgenden sind die Profileinstellungen aufgeführt, die Sie auf der Appliance konfigurieren müssen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appfw profile <name> [-invalidPercentHandling <invalidPercentHandling
>] [-checkRequestHeaders ( ON | OFF )] [-URLDecodeRequestCookies ( ON |
 OFF )] [-optimizePartialReqs ( ON | OFF )] [-errorURL <expression>] [-
logEveryPolicyHit ( ON | OFF )] [-stripHtmlComments <stripHtmlComments>] [-
```



```
stripXmlComments ( none | all )] [-postBodyLimitSignature <positive_integer
>][-fileUploadMaxNum <positive_integer>][-canonicalizeHTMLResponse ( ON
| OFF )][-percentDecodeRecursively ( ON | OFF )] [-multipleHeaderAction
<multipleHeaderAction> ...][-inspectContentTypes <inspectContentTypes>
...][-semicolonFieldSeparator ( ON | OFF )]
```

Beispiel:

```
add appfw profile profile1 [-invalidPercentHandling secure_mode] [-checkRequestHeaders
 ON] [-URLDecodeRequestCookies OFF] [-optimizePartialReqs OFF]
```

Hierbei gilt:

InvalidPercentHandling — Konfiguriert die Methode für den Umgang mit prozentkodierten Namen und Werten.

Verfügbare Einstellungen funktionieren wie folgt:

asp_mode - Entfernt und analysiert ungültige Prozent für das Parsen.

Beispiel `curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz)` wird entfernt und der Rest des Inhalts wird überprüft und Maßnahmen für die SQLInjection-Überprüfung ergriffen.

secure_mode - Wir erkennen den ungültigen prozentualen codierten Wert und ignorieren ihn.

Beispiel `curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz)` wird erkannt, Zähler werden inkrementiert und der Inhalt wird so wie er ist an den Server weitergegeben.

apache_mode - Dieser Modus funktioniert ähnlich wie der sichere Modus.

> **Hinweis:**
>
> Ab Release 13.1 Build 45.x ist die Funktion `apache_mode` veraltet.

Mögliche Werte: apache_mode, asp_mode, secure_mode

Standardwert: secure_mode

OptimizePartialReqs — Bei AUS/AN (ohne sicheres Objekt) sendet eine NetScaler-Appliance die Teilanforderung an den Back-End-Server. Diese teilweise Antwort wurde an den Kunden zurückgesendet. OptimizePartialReqs ist sinnvoll, wenn das Safe-Objekt konfiguriert ist. Die Appliance sendet Anfragen nach vollständiger Antwort vom Server, wenn sie AUS ist, und fordert nur eine teilweise Antwort an, wenn sie EIN ist.

Verfügbare Einstellungen lauten wie folgt:

EIN - Teilweise Anfragen des Clients führen zu teilweisen Anfragen an den Back-End-Server.
OFF — Teilanfragen des Clients werden in vollständige Anfragen an den Backend-Server umgewandelt.

Mögliche Werte: ON, OFF
Standardwert: ON

URLDecodeRequestCookies. URL Dekodieren Sie Anforderungscookies, bevor Sie sie SQL- und Cross-Site-Scripting-Prüfungen unterziehen.

Mögliche Werte: ON, OFF
Standardwert: OFF

Unterschrift Post Body Limit (Byte). Schränkt die auf Signaturen untersuchte Anforderungsnutzlast (in Byte) mit dem Speicherort ein, der als "HTTP_POST_BODY" angegeben ist.

Standardwert: 8096
Mindestwert: 0
Maximalwert: 4294967295

Post-Body-Limit (Byte). Schränkt die von der Web Application Firewall überprüfte Anforderungsnutzlast (in Byte) ein.

Standardwert: 20000000
Minimalwert: 0
Maximalwert: 10 GB

Weitere Informationen zur Sicherheitseinstellung und ihrer GUI-Prozedur finden Sie unter Konfigurieren des Web App Firewall App-Firewall-Profils .

postBodyLimitAction. PostBodyLimit akzeptiert Fehlereinstellungen, wenn Sie die maximal zulässige Größe des HTTP-Bodys angeben. Um Fehlereinstellungen zu berücksichtigen, müssen Sie eine oder mehrere Post-Body Limit-Aktionen konfigurieren. Die Konfiguration ist auch für Anfragen anwendbar, bei denen der Übertragungscodierungs-Header in Chunked ist.

```
set appfw profile <profile_name> -PostBodyLimitAction block log stats
```

Wo,
Block - Diese Aktion blockiert eine Verbindung, die gegen die Sicherheitsprüfung verstößt und basiert auf der maximalen Größe des konfigurierten HTTP-Body (Post-Body-Limit). Sie müssen die Option immer aktivieren.

Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.

Statistiken - Generieren Sie Statistiken für diese Sicherheitsüberprüfung.

> **Hinweis:**
>
> Das Protokollformat für die Aktion "Post-Body-Limit" wurde nun geändert, um dem standardmäßigen Audit-Logging-Format zu folgen, zum Beispiel:
> `ns.log.4.gz:Jun 25 1.1.1.1. <local0.info> 10.101.10.100 06/25/2020:10:10:28 GMT 0-PPE-0 : default APPFW APPFW_POSTBODYLIMIT 1506 0 : <Netscaler IP>`


```
 4234-PPE0 - testprof ><URL> Request post body length(<Post Body Length
>)exceeds post body limit.
```

InspectQueryContentTypes Prüfen Sie Anforderungs- und Webformulare für injizierte SQL- und Cross-Site-Skripts für die folgenden Inhaltstypen.

```
set appfw profile p1 -inspectQueryContentTypes HTML XML JSON OTHER
```

Mögliche Werte: HTML, XML, JSON, OTHER

Standardmäßig ist dieser Parameter als “InspectQueryContentTypes: HTML JSON OTHER” für einfache und erweiterte appfw-Profile festgelegt.

Beispiel für Inspect-Abfrage-Inhaltstyp als XML:

```
1 > set appfw profile p1 -type XML
2 Warning: HTML, JSON checks except “InspectQueryContentTypes” & “
     Infer Content-Type XML Payload Action” will not be applicable when
     profile type is not HTML or JSON respectively.
3 <!--NeedCopy-->
```

Beispiel für Inspect-Abfrage-Inhaltstyp als HTML:

```
1 > set appfw profile p1 -type HTML
2 Warning: XML, JSON checks except “InspectQueryContentTypes” & “Infer
     Content-Type XML Payload Action” will not be applicable when
     profile type is not XML or JSON respectively
3 Done
4 <!--NeedCopy-->
```

Beispiel für Inspect-Abfrage-Inhaltstyp als JSON:

```
1 > set appfw profile p1 -type JSON
2 Warning: HTML, XML checks except “InspectQueryContentTypes” & “Infer
     Content-Type XML Payload Action will not be applicable when profile
     type is not HTML or XML respectively
3 Done
4 <!--NeedCopy-->
```

errorUrl Ausdruck. Die URL, die die NetScaler Web App Firewall als Fehler-URL verwendet. Maximale Länge: 2047

> **Hinweis:**
>
> Wenn die Fehler-URL mit der Signatur-URL vergleichbar ist, setzt die Appliance die Verbindung zurück, um Verletzungen in einer angeforderten URL zu blockieren.

LogEveryPolicyHit - Protokolliert jede Profilübereinstimmung, unabhängig von den Ergebnissen der Sicherheitsüberprüfungen.
Mögliche Werte: ON, OFF.
Standardwert: OFF.

stripXMLComments - Entfernen Sie XML-Kommentare, bevor Sie eine Webseite weiterleiten, die von einer geschützten Website als Antwort auf eine Benutzeranfrage gesendet wurde.
Mögliche Werte: none, all, exclude_script_tag.
Standardwert: keiner

postbodyLimitSignature - Maximal zulässige HTTP-Post-Body-Größe für die Signaturprüfung für den Ort HTTP_POST_BODY in den Signaturen, in Byte.
Die Wertänderungen können sich auf das CPU- und Latenzprofil auswirken.
Standardwert: 2048.
Minimaler Wert: 0
Maximalwert: 4294967295

FileUploadMaxNum - Maximal zulässige Anzahl von Datei-Uploads pro Anforderung zum Einreichen von Formularen. Die Maximaleinstellung (65535) ermöglicht eine unbegrenzte Anzahl von Uploads.
Standardwert: 65535
Mindestwert: 0
Maximalwert: 65535

CanonicalizeHTMLResponse - Führen Sie eine HTML-Entitätscodierung für alle Sonderzeichen in Antworten durch, die von Ihren geschützten Websites gesendet werden.
Mögliche Werte: ON, OFF
Standardwert: ON

PercentDecodeRecursive - Konfigurieren Sie, ob die Anwendungsfirewall prozentuale rekursive Dekodierung verwenden soll.
Mögliche Werte: ON, OFF
Standardwert: ON

MultipleHeaderAction - Eine oder mehrere Aktionen mit mehreren Headern. Verfügbare Einstellungen funktionieren wie folgt:

- Blockieren. Blockieren Sie Verbindungen, die mehrere Header haben.
- Loggen. Protokollieren Sie Verbindungen, die mehrere Header haben.
- KeepLast. Behalten Sie nur den letzten Header bei, wenn mehrere Header vorhanden sind.

inspectContentTypes — Eine oder mehrere InspectContentType Listen.

- application/x-www-form-urlencoded
- multipart/form-data
- text/x-gwt-rpc

Mögliche Werte: keine, application/x-www-form-urlencoded, multipart/form-data, text/x-gwt-rpc

SemicolonFieldSeparator - Erlaubt ‘;’ als Formularfeldtrennzeichen in URL-Abfragen und POST-Formularkörpern.
Mögliche Werte: ON, OFF
Standardwert: OFF

Ändern eines Web App Firewall-Profiltyps

May 11, 2023

Wenn Sie den falschen Profiltyp für ein Web App Firewall-Profil ausgewählt haben oder sich die Art des Inhalts auf der geschützten Website geändert hat, können Sie den Profiltyp ändern.

> **Hinweis:** Wenn Sie den Profiltyp ändern, gehen alle Konfigurationseinstellungen und erlernten Lockerungen oder Regeln für Funktionen verloren, die der neue Profiltyp nicht unterstützt. Wenn Sie beispielsweise den Profiltyp von Web 2.0 in XML ändern, gehen alle Konfigurationsoptionen für die Start-URL, die Formularfeld-Konsistenzprüfung und die anderen HTML-spezifischen Sicherheitsprüfungen verloren. Die Konfiguration für alle Optionen, die sowohl vom alten als auch vom neuen Profiltyp unterstützt werden, bleibt unverändert.

So ändern Sie einen Web App Firewall-Profiltyp mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Typ eines Profils mit dem Namen pr-basic von HTML in HTML-XML geändert, was dem Web 2.0-Typ in der GUI entspricht.

```
set appfw profile pr-basic -type HTML XML
save ns config
<!--NeedCopy-->
```

Um einen Web App Firewall-Profiltyp mithilfe der GUI zu ändern

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Richtlinien**.
2. Klicken Sie im Detailbereich auf **Aktion**und dann auf **Profiltyp ändern**.

3. Wählen **Sie im Dialogfeld Web App Firewall-Profiltyp ändern** in der Dropdownliste **Profiltyp** einen neuen Profiltyp aus.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Bereich **Profile** zurückzukehren.

Exportieren und Importieren eines Web App Firewall Profils

December 7, 2021

Sie können die gesamte Konfiguration eines Web App Firewall Profils (einschließlich aller gebundenen Objekte, wie HTML-Fehlerobjekt, XML-Fehlerobjekt, WSDL- oder XML-Schema, Signaturen usw.) über mehrere Appliances replizieren. Sie können ein Zielprofil auswählen und die Konfiguration exportieren, um sie im lokalen Dateisystem Ihres Computers zu speichern, oder Sie können die archivierte Konfiguration übertragen, um sie auf einem Server zu speichern. Ebenso können Sie das lokale Dateisystem Ihres Computers durchsuchen oder das Archiv vom Server importieren, um ein zuvor exportiertes Profil auszuwählen und in Ihre NetScaler Appliance zu importieren.

Die Option, die gesamte Profilkonfiguration zu exportieren und dann in eine andere Appliance zu importieren, kann in verschiedenen Anwendungsfällen nützlich sein. Sie können beispielsweise ein Web App Firewall Profil in einer Testbetteinrichtung konfigurieren, um zu testen und zu überprüfen, ob es wie erwartet funktioniert. Sobald Sie zufrieden sind, können Sie das Profil exportieren und die Profilkonfiguration in Ihre NetScaler Produktionen importieren. Diese Funktionalität ist auch nützlich, um Ihre Konfiguration zu sichern. Sie können das Profil exportieren, bevor Sie Änderungen vornehmen, sodass Sie die Konfiguration bei Bedarf problemlos in einen bekannten Zustand zurücksetzen können.

> **Hinweis:**
>
> Web App Firewall Profile, die aus einem Build exportiert und archiviert werden, können nicht auf einem System wiederhergestellt werden, auf dem ein anderer Build ausgeführt wird, da Änderungen in neueren Versionen zu Kompatibilitätsproblemen führen können. Wenn Sie versuchen, ein archiviertes Profil in einem anderen Build als dem, aus dem es exportiert wurde, wiederherzustellen, wird eine Fehlermeldung in ns.log protokolliert.

Die Export- und Importprofilfunktionalität ist sowohl in der GUI (GUI) als auch in der Befehlszeilenschnittstelle (CLI) verfügbar. Die GUI wird empfohlen, da sie einfach zu bedienende **Aktionsoptionen** bietet. Mit einem Klick auf eine Schaltfläche können Sie die gesamte Konfiguration eines Profils **exportieren oder importieren** .

Exportieren Web App Firewall Profilen mit der CLI

Wenn Sie ein Profil mit CLI **exportieren**, müssen Sie die Konfiguration **archivieren** und dann **exportieren** . Um ein Profil zu **importieren**, müssen Sie das Archiv in die NetScaler Appliance **im-**

portieren und dann den **Restore-Befehl** ausführen, um die Konfiguration zu extrahieren. Die folgenden CLI-Befehle können zum Exportieren, Importieren und Verwalten der Profilkonfigurationen verwendet werden.

CLI-Befehle zum Exportieren von Archiven:

- `archive appfw profile <name> <archivename> [-comment <string>]`
- `export appfw archive <name> <target>`

CLI-Befehle zum Importieren von Archiven:

- **`import`** `appfw archive <src> <name> [-comment <string>]`
- `restore appfw profile <archivename>`

CLI-Befehle zum Verwalten von Archiven:

- `show appfw archive`
- `rm appfw archive <name>`

Das Exportieren eines Profils von einer Appliance und das Importieren in eine andere erfordert fünf Schritte in CLI. Die ersten drei Schritte werden auf der Quell-Appliance ausgeführt, auf der die Profilkonfiguration ursprünglich erstellt wurde, und die nächsten 2 Schritte werden auf der Ziel-Appliance ausgeführt, auf der die Profilkonfiguration repliziert werden soll.

Profil aus der Quell-NetScaler Appliance exportieren:

Schritt 1: Erstellen Sie ein Archiv des konfigurierten Profils.

Schritt 2: Exportieren Sie das Archiv in das NetScaler Dateisystem.

Schritt 3: Verwenden Sie ein Dateiübertragungsprogramm wie scp, um die exportierte Archivdatei von der NetScaler Appliance A auf die NetScaler-Ziel-Appliance zu übertragen.

Profil in die NetScaler Ziel-Appliance importieren:

Schritt 4: Führen Sie den Importbefehl aus, um die archivierte Datei zu importieren. Sie können das Archiv aus dem lokalen Dateisystem Ihres NetScaler importieren oder das HTTP- oder HTTPS-Protokoll verwenden, um das Archiv von einem Server mit der URL zu importieren.

Schritt 5: Führen Sie den Restore-Befehl aus, um die Profilkonfiguration aus dem importierten Archiv wiederherzustellen

So exportieren Sie ein Web App Firewall Profil mit der Befehlszeilenschnittstelle:

Archivieren Sie zunächst die Konfiguration des Profils, und **exportieren** Sie das Archiv an einen Zielspeicherort. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
archive appfw profile <profileName> <archiveName>
```

Wobei:

- `<profileName>` ist der Name des Profils, das archiviert werden soll.

- <archiveName> ist der Name der zu erstellenden Archivdatei.

Ausführung des obigen Befehls erstellt 2 Instanzen der Archivdatei. Einer im Ordner /var/tmp und der andere im Ordner /var/archive/appfw.

```
export appfw archive <archiveName> <target>
```

Wobei:

- <archiveName> ist der Name des zu exportierenden Archivs. (Der gleiche Name wie im vorherigen Befehl.
- <target> ist ein Dateipfad, der mit local: als Präfix beginnt, gefolgt von<archiveName> .

Die Ausführung des Export-Befehls speichert die exportierte Archivdatei im Dateisystem Ihrer NetScaler Appliance im Ordner /var/tmp.

Beispiele:

```
> archive appfw profile test_pr archived_test_pr
```

```
> export appfw archive archived_test_pr local:dutA_test_pr
```

Nachdem die beiden oben genannten Befehle ausgeführt wurden, enthält der Ordner /var/tmp die archived_test_pr-Datei und die exportierte Kopie Duta_test_PR, die in ihrer Größe identisch sind. Über die Befehlszeilenschnittstelle können Sie in die Shell ablegen, um zu dem Ordner zu navigieren, um zu überprüfen, ob diese Dateien vorhanden sind.

Nach dem Exportieren der Archivdatei können Sie **scp** oder ein anderes solches Dateiübertragungsprogramm verwenden, um eine Kopie der Archivdatei von der NetScaler Appliance, auf der sie erstellt wurden, auf Ihre NetScaler-Ziel-Appliance zu übertragen.

Importieren von Web App Firewall Profilen mit der CLI

Nachdem Sie die archivierte Datei erfolgreich von der Quell-Appliance auf die Ziel-Appliance verschoben haben, können Sie das Archiv des Profils **importieren** und dann den **Wiederherstellungsbefehl** ausführen, um die Konfiguration des Profils auf der Ziel-Appliance zu replizieren.

Melden Sie sich bei der Ziel-Appliance an. Gehen Sie in die Shell und cd in den Ordner /var/tmp, um zu überprüfen, ob die Größe der scp'd Datei auf dieser Appliance mit der Größe der ursprünglichen archivierten Datei auf der Quell-Appliance übereinstimmt. Beenden Sie die Shell, um zur Befehlszeile zurückzukehren.

So importieren Sie ein Profil mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
import appfw archive <src> <name> [-comment <string>]
```

wobei

- <src> ist der Speicherort der Archivdatei, nachdem sie von der Quell-Appliance übertragen wurde, auf der sie erstellt wurde. Sie können ein lokales Dateisystem und einen Dateinamen verwenden. Wenn Sie das Archiv auf einem Server abgelegt haben, können Sie eine URL zum Importieren der archivierten Datei verwenden. Wenn der Pfad oder Dateiname Leerzeichen enthält, schließen Sie die URL in doppelte Anführungszeichen ein.
- <name> ist der Name der zu importierenden Archivdatei.
- <string> ist eine optionale Beschreibung des Zwecks des Archivs.

```
restore appfw profile <archiveName>
```

Beispiele:

A. Import aus lokaler Datei gefolgt von Wiederherstellung:

```
> import appfw archive local:dutA_test_pr dut2_test_pr
```

```
> restore appfw profile dut2_test_pr
```

B. Importieren von URL gefolgt von Wiederherstellung:

```
import appfw archive http://10.217.30.16/FFC/Profile_ImportExport/
dutA_test_pr.tgz my_archive
restore appfw profile my_archive
```

In diesem Beispiel wird das test_pr-Profil zusammen mit allen gebundenen Objekten (wie Signaturen, HTML-Fehlerseite, Relaxationsregeln usw.) auf der NetScaler Ziel-Appliance wiederhergestellt.

Sie können die folgenden CLI-Befehle verwenden, um auf Manpages für weitere Details zuzugreifen.

- manarchiv appfw Profil
- man export appfw archiv
- man import appfw archiv
- man wiederherstellen appfw Profil
- man show appfw archiv
- man rm appfw Archiv

Exportieren und Importieren von Web App Firewall Profilen mit der GUI

Die GUI ist einfacher zu verwenden als die CLI. Das Dienstprogramm führt sowohl Archivierungs- als auch Exportvorgänge durch, wenn Sie auf **Exportieren**klicken. Ebenso wird sowohl der Import als auch der Wiederherstellung ausgeführt, wenn Sie auf **Importieren**klicken. Die GUI kann auf das lokale Dateisystem des Computers zugreifen, von dem aus Sie auf das Dienstprogramm zugreifen. Sie können eine Kopie des Archivs exportieren und auf Ihrem lokalen Computer speichern. Sie können diese Kopie dann direkt in die Ziel-Appliance importieren, ohne die Archivdatei manuell von einer Appliance auf die andere übertragen zu müssen.

So exportieren Sie ein Web App Firewall Profil mit der GUI:

1. Navigieren Sie zu **Konfiguration** > **Sicherheit** > **Web App Firewall** > **Profile** .
2. Wählen Sie im Detailbereich ein zu exportierendes Profil aus. Klicken Sie auf **Aktionen** und wählen Sie **Exportieren** aus, um eine Kopie im lokalen Dateisystem Ihres Computers herunterzuladen und zu speichern.

So importieren Sie ein Web App Firewall Profil mit der GUI:

1. Navigieren Sie zu **Konfiguration** > **Sicherheit** > **Web App Firewall** > **Profile** .
2. Klicken Sie im Detailbereich auf **Aktionen**, und wählen Sie **Importieren** aus. Im Bereich Web App Firewall Profil importieren stehen Ihnen das Auswahlfeld Aus importieren 2 Optionen zur Verfügung:

URL: Sie können ein Archiv importieren, indem Sie eine **URL** angeben. Wenn diese Option ausgewählt ist, müssen Sie im **URL-Eingabefeld** einen absoluten Pfad für die archivierte Datei angeben.

Datei: Sie können ein Archiv aus der lokalen **Datei** importieren. Wenn diese Option ausgewählt ist, wird ein Auswahlfeld **Lokale Datei** angezeigt. Sie können die lokalen Dateien Ihres Computers durchsuchen, um die Zielarchivdatei auszuwählen.

Klicken Sie auf **Erstellen**, um das angegebene Archiv zu importieren. Beim erfolgreichen Abschluss des Importvorgangs wird die Profilkonfiguration auf der Ziel-Appliance erstellt.

Highlights

- Sie können die gesamte Konfiguration (einschließlich aller Importobjekte sowie konfigurierten Relaxationsregeln für das Profil) auf mehreren Appliances replizieren, ohne dass Sie Konfigurationsschritte wiederholen müssen, indem Sie die Export- und Importprofilfunktionalität verwenden.
- Die importierten Objekte, wie Signaturen, WSDL, Schema, Fehlerseite usw., sind in der archivierten TAR-Datei enthalten und auf der Ziel-Appliance repliziert.
- Angepasste Feldtypen sind in der archivierten TAR-Datei enthalten und auf der Ziel-Appliance repliziert.
- Die Richtlinienbindungen des archivierten Profils werden nicht repliziert, wenn die Konfiguration wiederhergestellt wird. Sie müssen die Richtlinie konfigurieren und sie an das Profil binden, nachdem Sie das Profil in die Appliance importiert haben.
- Der Name der Archivdatei kann bis zu 31 Zeichen lang sein. Wie bei Profilnamen muss ein Archivname mit einem alphanumerischen Zeichen oder Unterstrich beginnen und nur alphanumerische Zeichen und Unterstriche (_), Zahl (#), Punkt (.), Leerzeichen (), Doppelpunkt (:), at (@), Gleich (=) oder Bindestrich (-) enthalten.
- Kommentare, die mit dem Archiv verknüpft sind, müssen beschreibend genug sein, um den Zweck der archivierten Konfiguration zu vermitteln. Die maximal zulässige Länge für einen Kommentar beträgt 255 Zeichen.
- `clear config -force basic` Mit dem Befehl werden die archivierten Profile nicht entfernt.

- Die Import- und Exportprofilfunktionalität wird in Hochverfügbarkeitsbereitstellungen (HA) unterstützt.

Tipps zum Debuggen

- Überwachen Sie die Datei /var/log/ns.log während der Befehlsausführung, um festzustellen, ob Fehlermeldungen vorhanden sind.
- Zusätzliche Protokolle (_restore.log, remove.log, import.log) werden im Ordner /var/tmp/- generiert. Sie können beim Debuggen von Problemen während der entsprechenden Operationen helfen. Wenn diese Protokolle eine MB Größe erreichen, werden die Protokollmeldungen gelöscht, um die Protokolldatei auf ein Viertel der ursprünglichen Größe zu verkleinern.
- Wenn der Importbefehl fehlschlägt, wenn Sie die URL-Option anstelle des lokalen Dateisystems verwenden, stellen Sie sicher, dass DNS-Namensserver und Routeneinstellungen korrekt konfiguriert sind.
- Wenn Sie das HTTPS-Protokoll zum Importieren des Archivs verwenden, schlägt der Befehl möglicherweise fehl, wenn der HTTPS-Server Clientzertifikatauthentifizierung erfordert.

Einfache Fehlerbehebung mit Web Application Firewall-Protokollen

May 11, 2023

Bei einem Sicherheitsangriff ist es wichtig, eine detaillierte WAF-Protokollierung auf der Appliance zu erfassen. Dazu können Sie den Parameter “VerboseLogLevel” in einem Application Firewall-Profil konfigurieren.

Stellen Sie sich einen Internetverkehr mit einem Sicherheitsangriff vor. Wenn die Appliance den Datenverkehr empfängt, werden Details zu Verstößen wie HTTP-Headerdetails, Protokollmuster und Musternutzlastinformationen protokolliert und an den ADM-Server gesendet. Der ADM-Server überwacht die detaillierten Protokolle und zeigt sie zu Überwachungs- und Nachverfolgungszwecken auf der Seite Security Insight an.

Ausführliche Protokollierungsstufe mit der Befehlszeilenschnittstelle konfigurieren

Konfigurieren Sie den folgenden Befehl, um detaillierte WAF-Protokolle zu erfassen.
Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload|
patternPayloadHeader)
```


Beispiel

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

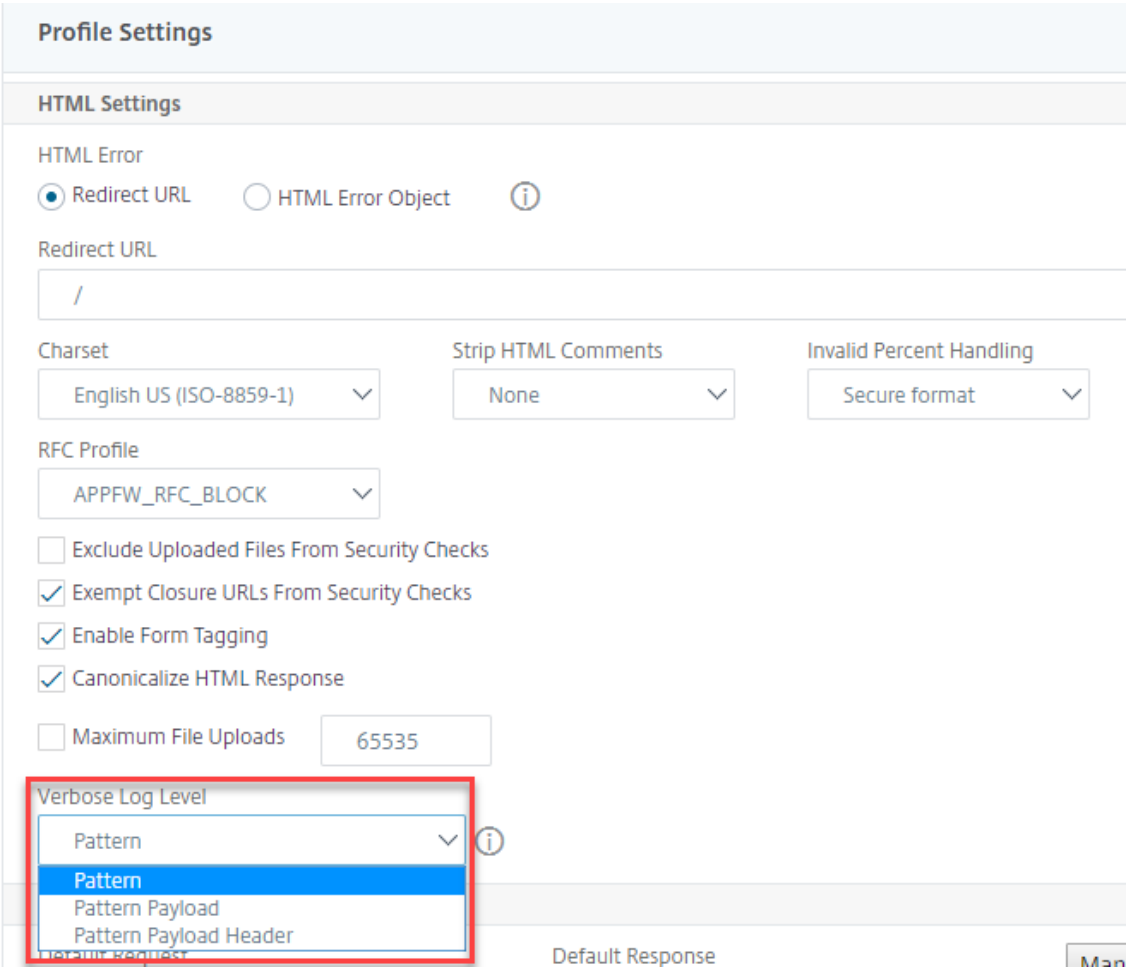
Die verfügbaren Protokollebenen sind:

1. Muster. Protokolliert nur Verletzungsmuster.
2. Pattern-Nutzlast. Protokolliert das Verletzungsmuster und 150 Byte zusätzliche Nutzlast des Feldelements.
3. Muster-Nutzlast-Header. Protokolliert das Verletzungsmuster, 150 Byte zusätzliche Nutzlast des Feldelements und HTTP-Header-Informationen.

Konfigurieren der ausführlichen Protokollebene mithilfe der NetScaler GUI

Führen Sie das folgende Verfahren aus, um den ausführlichen Protokollierungsgrad im WAF-Profil zu konfigurieren.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall Profilseite** unter **Erweiterte**Einstellungen auf Profileinstellungen**.
4. Wählen Sie im Abschnitt **Profileinstellungen** die detaillierte WAF-Protokollebene im Feld Ausführlicher Protokollierungsgrad aus.
5. Klicken Sie auf **OK** und **Fertig**.



Ausführliche Protokollierung für JSON-Sicherheitsprüfungen (SQL, CMD und Cross-Site Scripting)

Wenn ein eingehender Anforderungstyp JSON ist, können Sie den Parameter für die ausführliche Protokollebene konfigurieren, um detaillierte Verletzungsprotokolle wie Muster, Musternutzlast und HTTP-Header-Informationen zu erfassen. Die Protokolldetails werden dann an den NetScaler ADM-Server gesendet, um JSON-Verstöße zu überwachen und zu beheben. Die ausführliche Protokollnachricht wird nicht in der Datei ns.log gespeichert.

Die ausführliche Protokollierung für den Sicherheitsschutz von JSON-Inhaltstypen kann für die folgenden Arten von Verstößen konfiguriert werden:

- SQL Injection
- Cross-Site Scripting
- Befehlseinschleusung

Konfigurieren der ausführlichen Protokollierung für den JSON-Sicherheitsschutz mithilfe der CLI

Um detaillierte HTTP-Header-Informationen als Protokolle zu erfassen, können Sie den Parameter für die ausführliche Protokollierung im Web App Firewall-Profil konfigurieren. Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile_name> -VerboseLogLevel ( pattern |
   patternPayload | patternPayloadHeader )
<!--NeedCopy-->
```

Beispiel:

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

Die verfügbaren Protokollebenen sind:

Muster. Protokolliert nur Verletzungsmuster.

Pattern-Nutzlast. Protokolliert das Verletzungsmuster und 150 Byte zusätzliche JSON-Nutzlast.

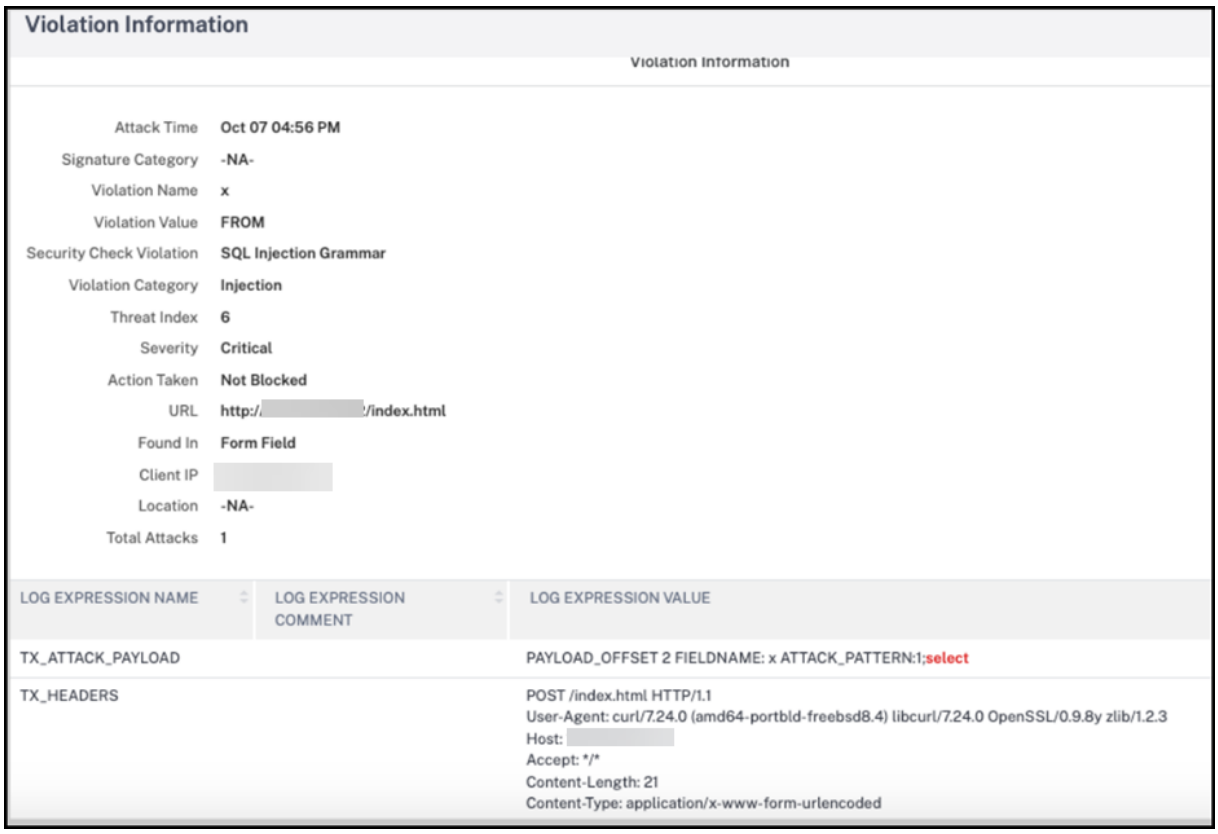
Muster-Nutzlast-Header. Protokolliert das Verletzungsmuster, 150 Byte zusätzliche JSON-Nutzlast und HTTP-Header-Informationen.

Konfigurieren der ausführlichen Protokollebene mithilfe der NetScaler GUI

Gehen Sie wie folgt vor, um die ausführliche Protokollebene für den JSON-Sicherheitsschutz zu konfigurieren.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit > Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall-Profilseite** unter **ErweiterteEinstellungen auf Sicherheitsprüfungen**.
4. Wählen Sie im Abschnitt **SicherheitsüberprüfungenJSON**aus und klicken Sie auf**Aktionseinstellungen**.
5. Legen Sie auf der Seite **JSON-Sicherheitseinstellungen** den Parameter **Verbose Logebene** fest.
6. Klicken Sie auf **OK** und **Fertig**.

Basierend auf den Details, die von der ausführlichen Protokollierung von NetScaler WAF JSON erfasst wurden, können die folgenden Verletzungsdetails auf dem NetScaler ADM-Server überprüft werden.



Schutz beim Hochladen von Dateien

August 4, 2023

Viele Angreifer versuchen, bösartigen Code, Viren oder Malware als Dateianhänge während der Multi-Formular-Übermittlung hochzuladen. Es ist wichtig, unser Netzwerk zu schützen und solche Bedrohungen zu überwinden. Um solche bösartigen Datei-Uploads zu verhindern, konfiguriert ein NetScaler-Administrator eine Reihe zulässiger Datei-Upload-Formate im WAF-Profil. Auf diese Weise beschränken Sie Dateiuploads auf bestimmte Formate und schützen die Appliance vor böswilligen Dateiuploads. Der Schutz funktioniert nur, wenn Sie die Option `ExcludeFileUploadFormChecks` im WAF-Profil deaktivieren.

So funktioniert das Hochladen von Dateien

Wenn Sie zulässige Datei-Upload-Formate konfigurieren, sieht die Komponenteninteraktion wie folgt aus:

- Kundenanfrage hat ein Formular mit einem Datei-Upload-Typ, zum Beispiel PDF.

- Im Rahmen der Sicherheitsüberprüfung überprüft die WAF die Nutzlast der Anfrage und validiert den Dateityp (basierend auf magischen Signaturnummern).
- Wenn der Dateityp kein unterstütztes Format hat, wird die entsprechende Aktion, die auf der Dateitypbindung basiert, angewendet.
- Um den Dateityp zu validieren, prüft die Appliance die Nutzdaten und prüft bei bekannten Offsets auf die bekannten magischen Zahlen. Jeder Dateityp hat eine Folge von magischen Zahlen, die den Dateityp validieren.

Konfigurieren Sie das Hochladen von Dateitypen mithilfe von NetScaler CLI

Um zulässige Dateiformate zu konfigurieren, verwendet die Appliance ein WAF-Profil, das an Dateiupload-Parameter gebunden ist.

1. Konfigurieren des Webanwendungs-Firewall-

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile_name> [-fileUploadTypesAction <fileUploadTypesAction
>]<fileUploadTypesAction> = ( none | block | log | stats )
```

Beispiel

```
set appfw profile profile1 -fileUploadTypesAction block
```

1. Binden Sie das Web Application Firewall-Profil mit Dateiupload-Parametern. Der Befehl bindet die angegebene Ausnahme (Entspannung) oder Regel an das angegebene Anwendungs-Firewall-Profil.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind appfw profile <profile_name> - fileUploadType <form_field > <form_action_url
> [-isNameRegex ( REGEX | NOTREGEX )] -fileType <fileType> ( pdf | msdoc |
text | image | any)
```

> **Hinweis:**
>
> Der Formularfeldname ist ein regulärer Ausdruckstyp. Der Standardwert ist `NOTREGEX`.

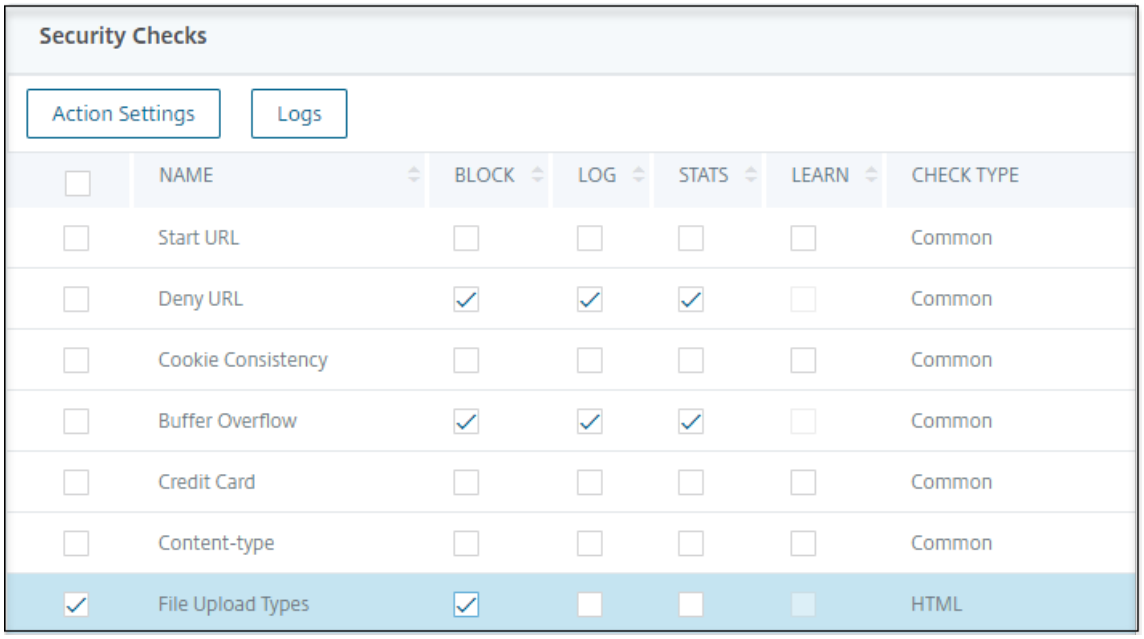
Beispiel

```
> bind appfw profile test -fileuploadType thefile "http://10.10.10.10/
fileupload_sample/upload.php"-isNameRegex NOTREGEX -filetype image
```

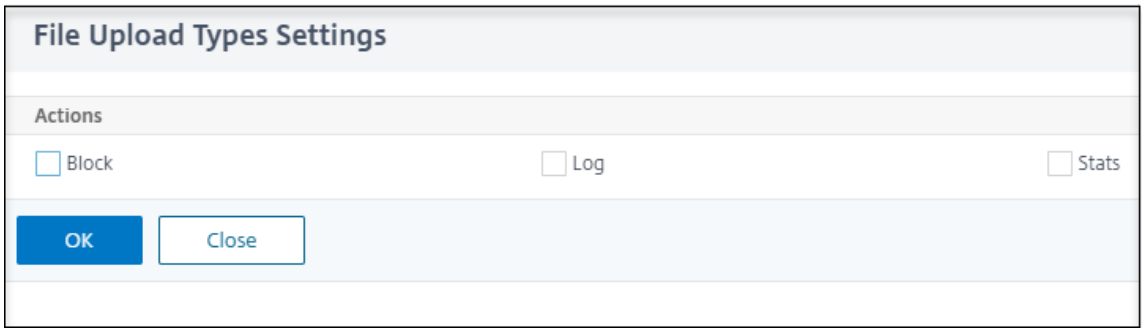
–>

Konfigurieren Sie den Sicherheitsschutz für das Hochladen von Dateien über die NetScaler GUI

1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite “Profile” auf **Hinzufügen**.
3. Klicken Sie auf der **NetScaler Web App Firewall-Profilseite** unter **ErweiterteEinstellungen auf Sicherheitsprüfungen**.
4. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** die Option **Datei-Upload-Typen** aus und klicken Sie auf **Aktionseinstellungen**.



5. Legen Sie auf der Seite **Einstellungen für Dateiuploadtypen** die Aktion zum Hochladen von Dateien fest.
6. Klicken Sie auf **OK**.



7. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** auf **OK** und **Fertig**.

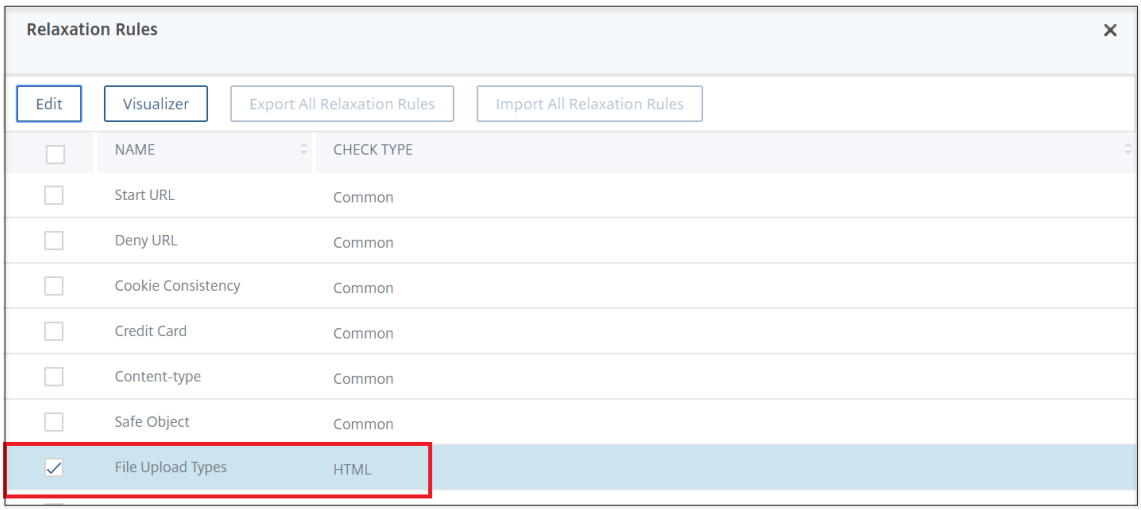
Konfigurieren Sie die Regel zum Hochladen von Dateien über die NetScaler GUI

Sie können den Sicherheitsschutz für das Hochladen von Dateien lockern, um Fehlalarme zu vermeiden. Beispielsweise blockiert die Appliance möglicherweise Dateiuploads, aber Sie können eine Ausnahmeregel hinzufügen, um Dateiuploads von bestimmten Websites zuzulassen. Auf diese Weise umgeht die Appliance die Sicherheitsüberprüfung für das angegebene Formularfeld und ermöglicht Benutzern das Hochladen von Dateien von der in der Aktions-URL genannten Website.

> **Hinweis:**
>
> Die Überprüfung des Datei-Uploads schlägt fehl, wenn die **Ausnahmeregel für Datei-Upload-Typen** nicht aktiviert ist.

Führen Sie die folgenden Schritte aus, um eine Ausnahmeregel zu erstellen.

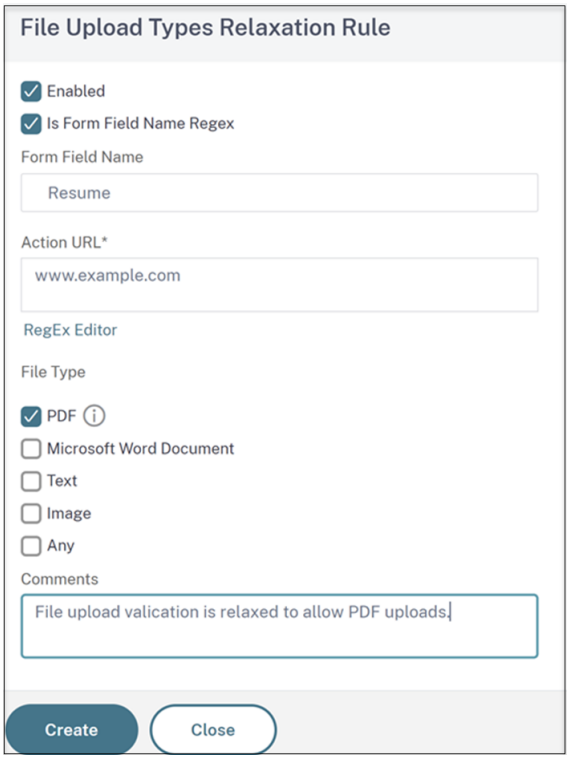
1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **NetScaler Web App Firewall** > **Profile**.
2. Klicken Sie auf der Seite “Profile” auf **Hinzufügen**.
3. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Ausnahmeregeln**.
4. Wählen Sie im Abschnitt **Ausnahmeregeln** die Option **Datei-Upload-Typen** aus und klicken Sie auf **Bearbeiten**.



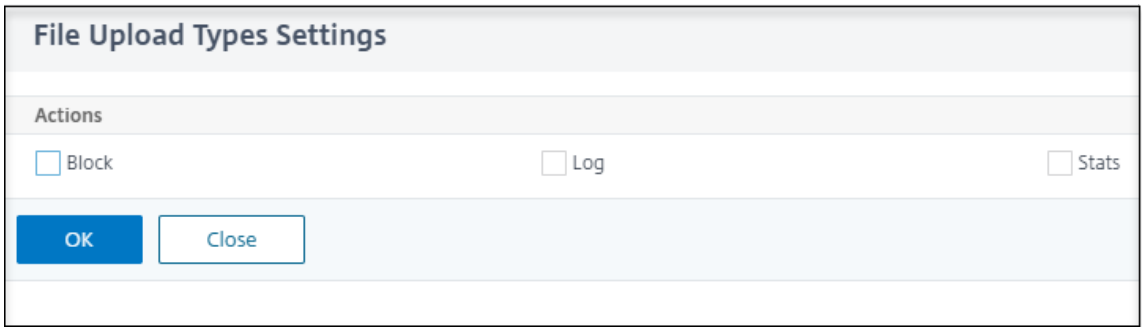
5. Klicken Sie auf der Seite **File Upload Types Relaxation Rule** auf **Hinzufügen**.
6. Legen Sie auf der Seite **File Upload Types Relaxation Rule** die folgenden Parameter fest:
   a) Aktiviert — Wählen Sie diese Option, um die Ausnahmeregel zu aktivieren.
   b) Is Form Field Name Regex — Wählen Sie diese Option, um ein Regex-Muster für den Formularfeldnamen zu aktualisieren.
   c) Formularfeldname — Geben Sie den Dateinamen ein, für den keine Sicherheitsüberprüfung erforderlich ist.

d) Aktions-URL — Die URL zur Einreichung von Formularen, die von den Sicherheitsprüfungen ausgenommen werden muss.
e) Dateityp — Unterstütztes Dateiformat, das hochgeladen werden kann.
f) Kommentare — Eine kurze Beschreibung des Datei-Uploads.

7. Klicken Sie auf **Erstellen**.



8. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** auf **OK** und **Fertig**.



Konfiguration und Verwendung der Lernfunktion

May 11, 2023

Die Lernfunktion ist ein Filter für sich wiederholende Muster, der Aktivitäten auf einer Website

oder Anwendung beobachtet, die durch die Web App Firewall geschützt ist, um festzustellen, was normale Aktivitäten auf dieser Website oder Anwendung ausmacht. Anschließend wird für jede Sicherheitsüberprüfung, die die Unterstützung der Lernfunktion beinhaltet, eine Liste mit bis zu 2.000 vorgeschlagenen Regeln oder Ausnahmen (Lockerungen) generiert. Benutzer finden es normalerweise einfacher, Entspannungen mithilfe der Lernfunktion zu konfigurieren, als die erforderlichen Entspannungen manuell einzugeben.

Die Sicherheitsüberprüfungen, die die Lernfunktion unterstützen, sind:

- URL-Prüfung starten
- Cookie-Konsistenzprüfung
- Form Field Consistency Check
- Field Formats Check
- CSRF Form Tagging Check
- HTML SQL Injection Check
- HTML Cross-Site Scripting Check
- XML-Denial-of-Service-Prüfung
- XML Attachment Check
- Interoperabilitätsprüfung der Webdienste

Sie führen zwei verschiedene Arten von Aktivitäten aus, wenn Sie die Lernfunktion verwenden. Zunächst aktivieren und konfigurieren Sie die Funktion für die Verwendung. Sie können den gesamten Datenverkehr zu Ihren geschützten Webanwendungen erfahren oder eine Liste von IP-Adressen (die Liste " *Trusted Learning Clients hinzufügen* " genannt) konfigurieren, aus der die Lernfunktion Empfehlungen generieren kann. Zweitens, nachdem die Funktion aktiviert wurde und eine bestimmte Menge an Traffic auf Ihre geschützten Websites verarbeitet hat, überprüfen Sie die Liste der vorgeschlagenen Regeln und Lockerungen (gelernte Regeln) und markieren jede mit einer der folgenden Bezeichnungen:

- **Bearbeiten und bereitstellen.** Die Regel wird in das Dialogfeld Bearbeiten gezogen, sodass Sie sie ändern können, und das geänderte Formular wird bereitgestellt.
- **Bereitstellen.** Die unveränderte gelernte Regel wird auf die Liste der Regeln oder Lockerungen für diese Sicherheitsüberprüfung gesetzt.
- **Überspringen.** Die gelernte Regel steht auf einer Liste von Regeln oder Lockerungen, die nicht eingesetzt werden. Die gelernte Regel wird beim Überspringen entfernt. Da sie jedoch nicht zu Entspannungen hinzugefügt werden, werden sie möglicherweise wieder gelernt.

Lernen wird nicht nur durchgeführt, wenn Entspannungen vorhanden sind, außer bei Feldformat-Regeln. Wenn Regeln übersprungen werden, werden sie nur aus der erlernten Datenbank entfernt. Da keine Entspannungen hinzugefügt werden, werden sie möglicherweise wieder gelernt. Wenn die Regeln bereitgestellt werden, werden sie aus der erlernten Datenbank entfernt und es werden auch Lockerungen für die Regeln hinzugefügt. Da Entspannungen hinzukommen, würden sie nicht wieder gelernt werden. Zum Schutz des Feldformats wird das Lernen unabhängig von Entspannungen

durchgeführt.

Sie können zwar die Befehlszeilenschnittstelle für die Grundkonfiguration der Lernfunktion verwenden, die Funktion ist jedoch hauptsächlich für die Konfiguration über den Web App Firewall-Assistenten oder die GUI konzipiert. Sie können die Lernfunktion nur eingeschränkt konfigurieren, indem Sie die Befehlszeile verwenden.

Der Assistent integriert die Konfiguration von Lernfunktionen in die Konfiguration der Web App Firewall als Ganzes und ist daher die einfachste Methode zur Konfiguration dieser Funktion auf einer neuen NetScaler Appliance oder bei der Verwaltung einer einfachen Web App Firewall-Konfiguration. Der GUI-Visualisierer und die manuelle Oberfläche bieten beide direkten Zugriff auf alle erlernten Regeln für alle Sicherheitsüberprüfungen und sind daher häufig vorzuziehen, wenn Sie erlernte Regeln für viele Sicherheitsüberprüfungen überprüfen müssen.

Die Lerndatenbank ist auf 20 MB begrenzt, was erreicht wird, nachdem pro Sicherheitsüberprüfung, für die Lernen aktiviert ist, etwa 2.000 gelernte Regeln oder Entspannungen generiert wurden. Wenn Sie gelernte Regeln nicht regelmäßig überprüfen und entweder genehmigen oder ignorieren und dieses Limit erreicht ist, wird ein Fehler im NetScaler-Protokoll protokolliert und es werden keine gelernten Regeln mehr generiert, bis Sie die bestehenden gelernten Regeln und Lockerungen überprüft haben.

Wenn das Lernen aufhört, weil die Datenbank ihre Größenbeschränkung erreicht hat, können Sie das Lernen neu starten, indem Sie entweder die vorhandenen gelernten Regeln und Lockerungen überprüfen oder die Lerndaten zurücksetzen. Nachdem erlernte Regeln oder Lockerungen genehmigt oder ignoriert wurden, werden sie aus der Datenbank entfernt. Nachdem Sie die Lerndaten zurückgesetzt haben, werden alle vorhandenen Lerndaten aus der Datenbank entfernt und auf ihre Mindestgröße zurückgesetzt. Wenn die Datenbank unter 20 MB fällt, wird das Lernen automatisch neu gestartet.

So konfigurieren Sie die Lerneinstellungen mit der Befehlszeilenschnittstelle

Geben Sie das zu konfigurierende Web App Firewall-Profil an, und geben Sie für jede Sicherheitsüberprüfung, die Sie in dieses Profil aufnehmen möchten, den Mindestschwellenwert oder den prozentualen Schwellenwert an. Der Mindestschwellenwert ist eine Ganzzahl, die die Mindestanzahl von Benutzersitzungen darstellt, die die Web App Firewall verarbeiten muss, bevor sie eine Regel oder Entspannung erlernt (Standard: 1). Der prozentuale Schwellenwert ist eine Ganzzahl, die den Prozentsatz der Benutzersitzungen darstellt, in denen die Web App Firewall ein bestimmtes Muster (URL, Cookie, Feld, Anlage oder Regelverletzung) beachten muss, bevor sie eine Regel oder Entspannung erfährt (Standard: 0). Verwenden Sie die folgenden Befehle:

- `set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThres`

<positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPerce <positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>] [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-XMLAttachmentPercentThreshold <positive_integer>]

- save ns config

Beispiel

Im folgenden Beispiel werden die Lerneinstellungen im Profil für die Sicherheitsüberprüfung von HTML SQL Injection aktiviert und konfiguriert. Dies ist eine geeignete Erstkonfiguration des Testbett-Lernens, bei der Sie die vollständige Kontrolle über den Datenverkehr haben, der an die Web App Firewall gesendet wird.

```
1 set appfw learningsettings pr-basic -SQLInjectionMinThreshold 10
2 set appfw learningsettings pr-basic -SQLInjectionPercentThreshold 70
3 save ns config
4 <!--NeedCopy-->
```

So setzen Sie die Lerneinstellungen mithilfe der Befehlszeilenschnittstelle auf die Standardeinstellungen zurück

Um jede benutzerdefinierte Konfiguration der Lerneinstellungen für das angegebene Profil und die Sicherheitsüberprüfung zu entfernen und die Lerneinstellungen auf ihre Standardeinstellungen zurückzusetzen, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- unset appfw learningsettings <profileName> [-startURLMinThreshold] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold] [-CSRFtagPercentThresh] [-fieldConsistencyMinThreshold] [-fieldConsistencyPercentThreshold] [-crossSiteScriptingMinThreshold] [-crossSiteScriptingPercentThreshold] [-SQLInjectionMinThreshold] [-SQLInjectionPercentThreshold] [-fieldFormatMinThreshold] [-fieldFormatPercentThreshold] [-XMLWSIMinThreshold] [-XMLWSIPercentThreshold] [-XMLAttachmentMinThreshold] [-XMLAttachmentPercen]
- save ns config

So zeigen Sie die Lerneinstellungen für ein Profil mithilfe der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
show appfw learningsettings <profileName>
```

So zeigen Sie nicht geprüfte gelernte Regeln oder Entspannungen für ein Profil mithilfe der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
show appfw learningdata <profileName> <securityCheck>
```

So entfernen Sie bestimmte nicht geprüfte gelernte Regeln oder Entspannungen mithilfe der Befehlszeilenschnittstelle aus der Lerndatenbank

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency
 <string> | (-fieldConsistency <string> <formActionURL>)| (-crossSiteScripting
 <string> <formActionURL>)| (-SQLInjection <string> <formActionURL>)| (-
fieldFormat <string><formActionURL>)| (-CSRFTag <expression> <CSRFFormOriginURL
>)| -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck
 <expression>)[-TotalXMLRequests]
```

Beispiel

Im folgenden Beispiel werden alle nicht überprüften gelernten Lockerungen für das Profil, die Sicherheitsüberprüfung HTML SQL Injection, entfernt, die für das **LastName-Formularfeld** gelten.

```
1 rm appfw learningdata pr-basic -SQLInjection LastName
2 <!--NeedCopy-->
```

So entfernen Sie alle nicht überprüften gelernten Daten mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
reset appfw learningdata
```


So exportieren Sie Lerndaten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
export appfw learningdata <profileName> <securitycheck>[-target <string>]
```

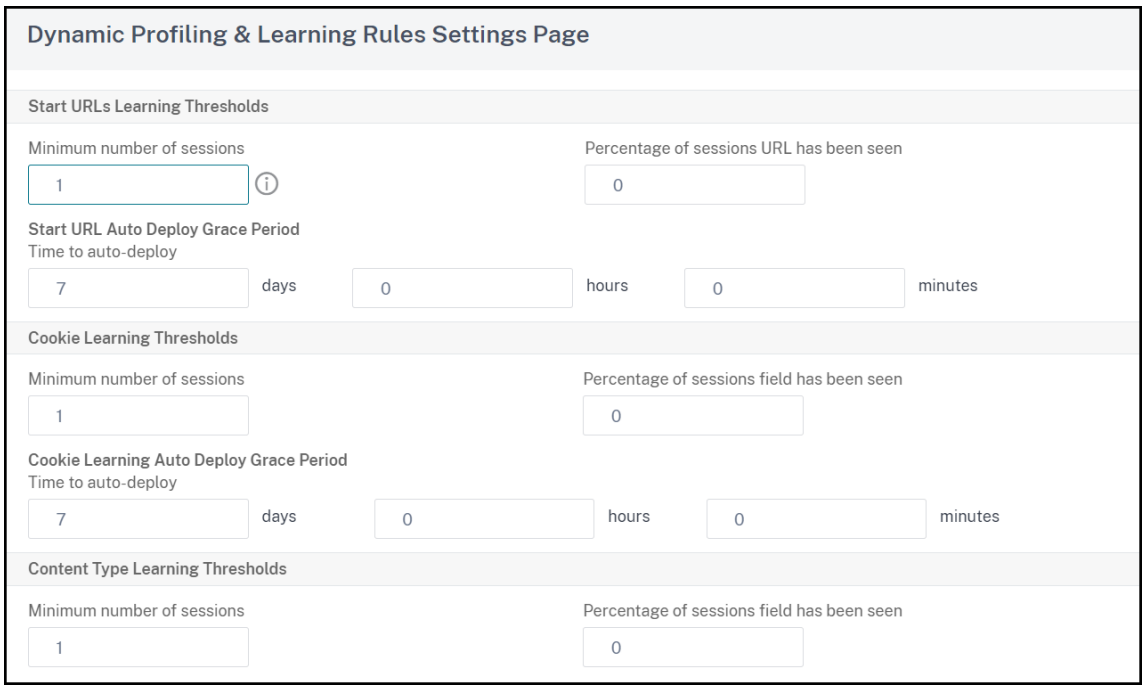
Beispiel

Im folgenden Beispiel werden gelernte Entspannungen für das Profil und die Sicherheitsüberprüfung der HTML SQL Injection in eine Datei im Format mit kommagetrennten Werten (CSV) im Verzeichnis /var/learnt_data/ unter dem im Parameter -target angegebenen Dateinamen exportiert.

```
1 export appfw learningdata pr-basic SQLInjection -target sqli_ld
2 <!--NeedCopy-->
```

So konfigurieren Sie die Lernfunktion mithilfe der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Gelernte Regeln** .
4. Wählen Sie im Abschnitt “ **Gelernte Regeln** “ eine Sicherheitsüberprüfung aus und klicken Sie auf **Einstellungen**.
5. Legen Sie auf der Seite **Einstellungen für die Sicherheitsprüfung** die folgenden Parameter fest:
   a) **Mindestzahlschwelle.** Je nachdem, welche Lerneinstellungen der Sicherheitsüberprüfung Sie konfigurieren, bezieht sich der Schwellenwert für die Mindestanzahl an Benutzersitzungen, die eingehalten werden müssen, auf die Mindestanzahl von zu beachtenden Anfragen oder auf die Mindestanzahl, wie oft ein bestimmtes Formularfeld eingehalten werden muss. bevor eine erlernte Entspannung erzeugt wird. Standard: 1
   b) **Prozentsatz des Schwellenwerts.** Je nachdem, welche Lerneinstellungen der Sicherheitsüberprüfung Sie konfigurieren, bezieht sich der Schwellenwert in Prozent auf den Prozentsatz der gesamten beobachteten Benutzersitzungen, die gegen die Sicherheitsüberprüfung verstoßen haben, auf den Prozentsatz der Anfragen oder auf den Prozentsatz, mit dem ein Formularfeld mit einem bestimmten Feldtyp übereinstimmte, vor erlernte Entspannung wird erzeugt. Standard: 0
6. Klicken Sie auf **OK** und auf **Schließen**.



7. Klicken Sie auf **Alle gelernten Daten** entfernen, um alle gelernten Daten zu entfernen und die Lernfunktion zurückzusetzen, sodass sie ihre Beobachtungen von Anfang an erneut starten muss.

   > **Hinweis:**
   >
   > Mit dieser Schaltfläche werden nur gelernte Empfehlungen entfernt, die nicht geprüft und entweder genehmigt oder übersprungen wurden. Erlernte Entspannungen, die akzeptiert und eingesetzt wurden, werden nicht beseitigt.

8. Um die Lernmaschine auf den Datenverkehr von einer bestimmten Gruppe von IPs zu beschränken, klicken Sie auf **Trusted Learning Clients**und fügen Sie die zu verwendenden IP-Adressen zur Liste hinzu.

   a) Um der Liste der vertrauenswürdigen Lernclients eine IP-Adresse oder einen IP-Adressbereich hinzuzufügen, klicken Sie auf **Hinzufügen**.
   b) Geben Sie im Dialogfeld **Trusted Learning Clients hinzufügen** im Listenfeld “Vertrauenswürdige Clients” die IP-Adresse oder einen IP-Adressbereich im CIDR-Format ein.
   c) Geben Sie im Textbereich Kommentare einen Kommentar ein, der diese IP-Adresse oder diesen Bereich beschreibt.
   d) Klicken Sie auf **Erstellen**, um Ihre neue IP-Adresse oder Ihren neuen Bereich zur Liste hinzuzufügen.
   e) Um eine vorhandene IP-Adresse oder einen Bereich zu ändern, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann auf **Öffnen**. Bis auf den Namen ist das angezeigte Dialogfeld identisch mit dem Dialogfeld **Trusted Learning Clients**

hinzufügen .

f) Um eine IP-Adresse oder einen Bereich zu deaktivieren oder zu aktivieren, diese jedoch in der Liste zu belassen, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann entsprechend auf **Deaktivieren oder Aktivieren**.

g) Um eine IP-Adresse oder einen Bereich vollständig zu entfernen, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann auf **Entfernen**.

9. Klicken Sie auf **Schließen**, um zur Seite Web App Firewall-Profil konfigurieren zurückzukehren.
10. Klicken Sie auf **Fertig**.

So überprüfen Sie gelernte Regeln oder Entspannungen mithilfe der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Gelernte Regeln** .
4. Wählen Sie im Abschnitt " **Gelernte Regeln** " eine Sicherheitsüberprüfung aus und klicken Sie auf **Einstellungen**.
5. Um die erlernten Daten hierarchisch als verzweigten Baum zu überprüfen, sodass Sie allgemeine Muster auswählen können, die vielen der erlernten Muster entsprechen, klicken Sie auf **Visualizer**.
6. Wenn Sie sich entschieden haben, tatsächlich erlernte Muster zu überprüfen, führen Sie die folgenden Schritte aus.
7. Wählen Sie die erste erlernte Entspannung aus und entscheiden Sie, wie Sie damit umgehen

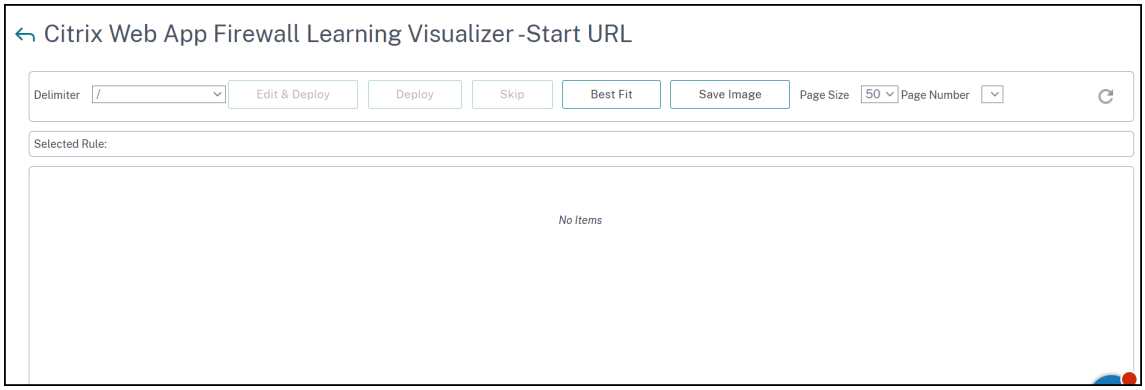
   a) Um die Entspannung zu ändern und dann zu akzeptieren, klicken Sie auf **Bearbeiten und bereitstellen**, bearbeiten Sie den regulären Entspannungsausdruck, und klicken Sie dann auf **OK**.

   b) Um die Entspannung ohne Änderungen zu akzeptieren, klicken Sie auf **Bereitstellen**.

   c) Um die Entspannung aus der Liste zu entfernen, ohne sie bereitzustellen, klicken Sie auf **Überspringen**.

   d) Wiederholen Sie den vorherigen Schritt, um jede weitere gelernte Entspannung zu überprüfen.

8. Klicken Sie auf **Schließen**, um zum Dialogfeld **Gelernte Regeln verwalten** zurückzukehren.
9. Klicken Sie auf **Fertig**.



Dynamisches Profiling

May 11, 2023

Die Lernfunktion ist ein Musterfilter, der Aktivitäten auf dem Backend-Server beobachtet und lernt. Basierend auf der Beobachtung generiert die Lernmaschine bis zu 2000 Regeln oder Ausnahmen (Entspannungen) für jede Sicherheitsüberprüfung. Um den Prozess zu automatisieren und die Entspannungsregeln automatisch bereitzustellen, verwendet die NetScaler-Appliance dynamische Profilerstellung.

Bei der dynamischen Profilerstellung zeichnet die Appliance die erlernten Daten für einen vordefinierten Schwellenwert auf und sendet eine SNMP-Warnung an den Benutzer. Wenn der Benutzer die Daten nicht innerhalb einer Nachfrist überspringt, stellt die Appliance sie automatisch als Entspannungsregel bereit. Früher musste der Benutzer die Relaxationsregeln manuell bereitstellen. Derzeit ist die dynamische Profilerstellung nur für die folgenden Sicherheitsüberprüfungen verfügbar:

1. HTML SQL injection
2. HTML-Cross-Site-Scripting
3. Feld-Format
4. Start-URL
5. Content-Typ
6. Feld-Formate
7. CSRF-Formular-Tagging
8. Cookie-Konsistenz
9. URL verweigern
10. Pufferüberlauf
11. Kreditkarte
12. Content-Typ-Schutz
13. JSON Cmd Injection protection

Betrachten Sie beispielsweise die Sicherheitsprüfung für HTML SQL Injection, die mit dynamischer Profilerstellung aktiviert ist. Sie können Lernen für eine Liste von IPs verwenden (die als Liste der vertrauenswürdigen Lernkunden bezeichnet wird), aus denen die Lernfunktion Empfehlungen generieren muss. Informationen zum Konfigurieren einer Liste vertrauenswürdiger Clients finden Sie unter Learning Trusted Clients Thema. Wenn der eingehende Verkehr Verstöße aufweist, wird er als gelernte Daten aufgezeichnet. Wenn die gelernten Daten in der Learning Engine aufgezeichnet werden, sendet die Appliance eine SNMP-Warnung an den Benutzer. Wenn der Benutzer ein falsches Positiv nicht erkennt und die erlernten Daten nicht innerhalb eines Kulanzzeitraums überspringt, stellt die Appliance diese automatisch als Relaxationsregel bereit.

> **Hinweis:**
> Nachdem Sie das dynamische Profil konfiguriert haben, müssen Sie die Appliance-Konfiguration regelmäßig auf die automatische Bereitstellung der Entspannungsregeln überprüfen und auf der Appliance speichern.

Konfigurieren der dynamischen Profilerstellung mit der NetScaler Befehlszeilenschnittstelle

Dynamische Profilerstellung ist für Start-URL, HTML Cross-Site Scripting, Feldformat oder HTML SQL Injection Sicherheitsüberprüfungen verfügbar. Um das dynamische Profiling zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

1. Konfigurieren Sie dynamisches Lernen
2. Konfigurieren der Nachfrist für die automatische Bereitstellung

Konfigurieren Sie dynamisches Lernen

Als ersten Schritt müssen Sie dynamisches Lernen auf Ihrer Appliance konfigurieren. Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile_name> dynamicLearning <security_checks>
```

Beispiel

```
set appfw profile test1 dynamicLearning SQLInjection CrossSiteScripting
fieldFormat startURL
```

Konfigurieren der Nachfrist für die automatische Bereitstellung

Sobald Sie die Funktion für bestimmte Sicherheitsüberprüfungen aktiviert haben, müssen Sie die Nachfrist für die automatische Bereitstellung konfigurieren.


```
set appfw learningsettings <profile name> -crossSiteScriptingAutoDeployGracePeriod
 <seconds>

set appfw learningsettings <profile name> fieldFormatAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> SQLInjectionAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> -startURLAutoDeployGracePeriod <
seconds>
```

Beispiel

```
set appfw learningsettings test1 -crossSiteScriptingAutoDeployGracePeriod 30

set appfw learningsettings test1 -startURLAutoDeployGracePeriod 7

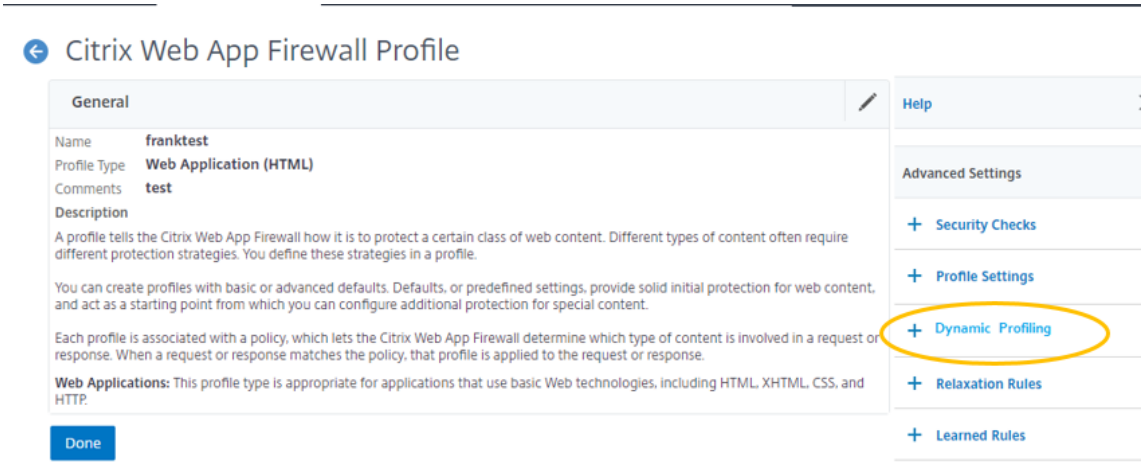
set appfw learningsettings test1 -fieldFormatAutoDeploymentGracePeriod 10

set appfw learning settings test1 -SQLInjectionAutoDeploymentGracePeriod 12
```

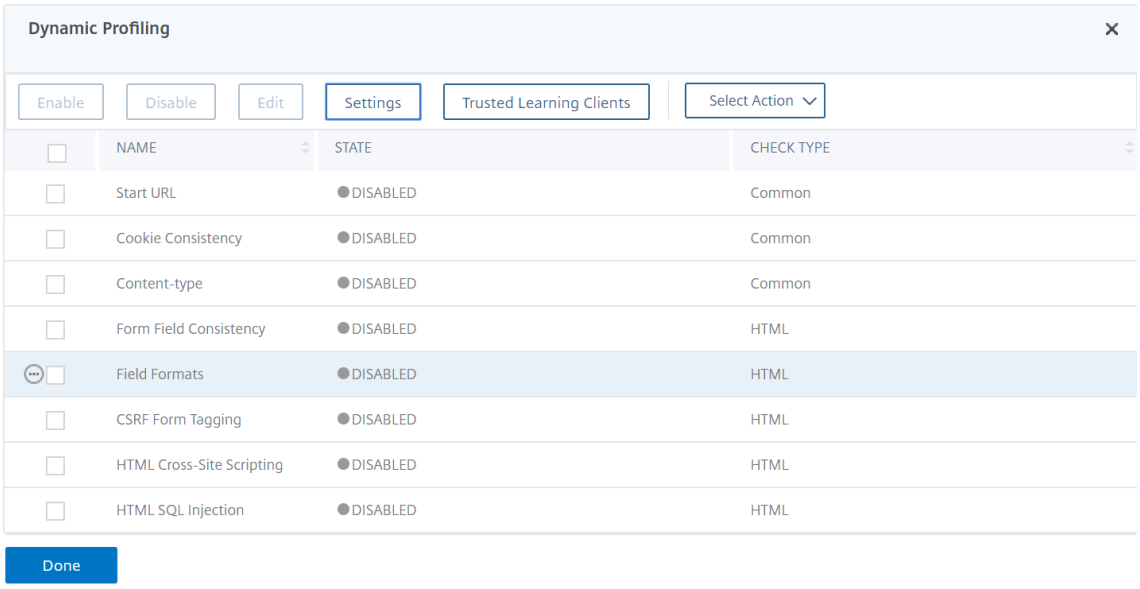
> **Hinweis:**
>
> Hier ist die Nachfrist für die automatische Bereitstellung in Minuten.

Konfigurieren der dynamischen Profilerstellung über die NetScaler GUI

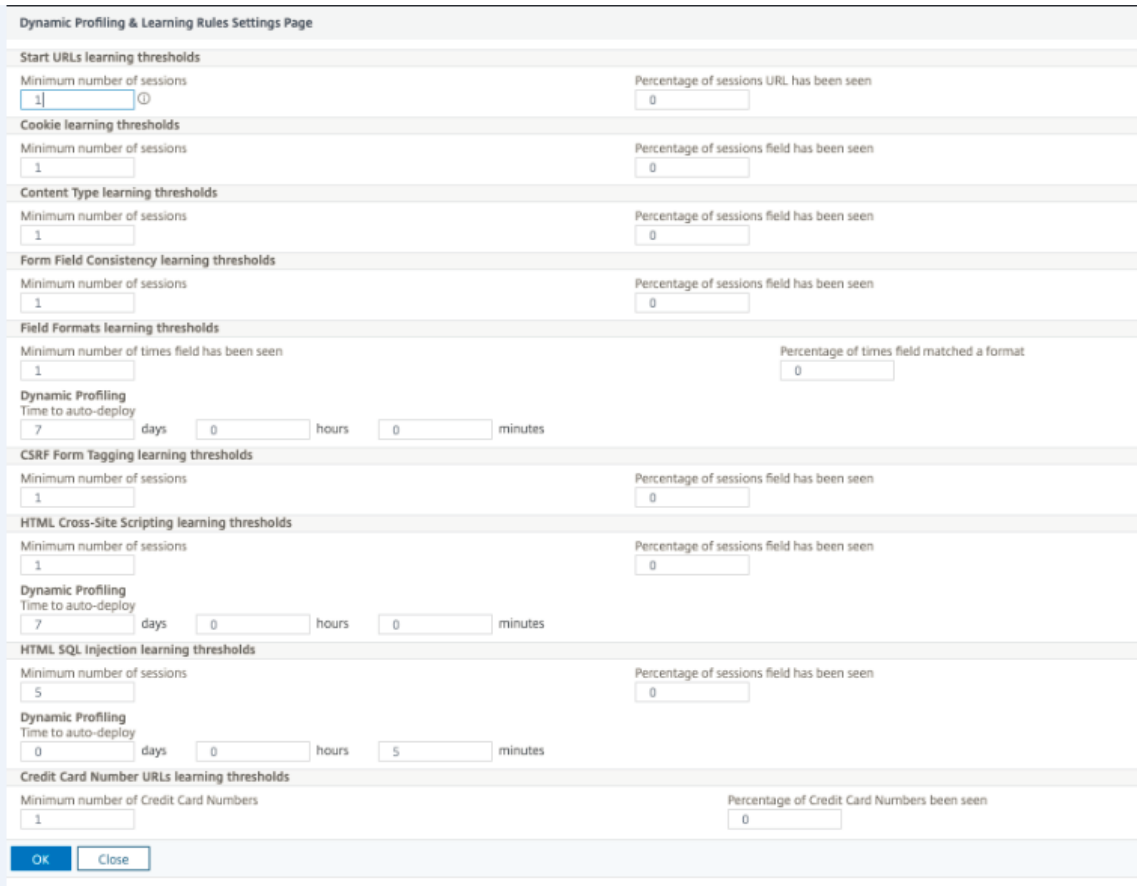
1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profil**.
2. Wählen Sie im Detailbereich ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Citrix Web App Profile** unter **Erweiterte Einstellungen** auf **Dynamisches Profiling**.



4. Wählen Sie im Abschnitt **Dynamic Profiling** eine Sicherheitsüberprüfung aus und klicken Sie auf **Bearbeiten**.



5. Legen Sie auf der Seite **Einstellungen für dynamische Profilerstellung und Lernen** die Nachfrist für die Sicherheitsüberprüfung fest.



6. Klicken Sie auf **OK** und **Fertig**.

Export und Import von Entspannungsregeln

Wenn Sie die dynamische Profilerstellung aktivieren, werden die gelernten Daten automatisch als Entspannungsregeln bereitgestellt. Darüber hinaus können Sie mit der Appliance auch die dynamischen Profilerstellungsregeln und regulären Entspannungsregeln exportieren. Sie können die Regeln aus der Staging-Umgebung exportieren und in die Produktionsumgebung importieren.

> **Hinweis:**
>
> Wenn Sie Regeln in die Produktionsumgebung importieren, müssen Sie sicherstellen, dass der Prozess additiv ist und die vorhandene Konfiguration nicht außer Kraft setzt.

Wie man Relaxationsregeln exportiert und importiert

Um die Entspannungsregeln zu exportieren und zu importieren, müssen Sie die folgenden Schritte ausführen:

1. Sie müssen zuerst die dynamischen Profiling-basierten Daten exportieren. Dazu steht die Exportoption für die Entspannungsregeln im WAF-Profil zur Verfügung. Wenn Sie diese Option auswählen, exportieren Sie die Regeln für die dynamische Profilerstellung und die regelmäßigen Entspannungsregeln. Sie können die Exportoption verwenden, um die Konfiguration als komprimiertes Bundle auf die Appliance herunterzuladen.
2. Nachdem Sie die Daten aus der Stagingumgebung exportiert haben, müssen Sie sie in eine andere NetScaler-Appliance importieren. Dazu müssen Sie die Importoption verwenden, die in den Entspannungsregeln des WAF-Profils verfügbar ist. Wenn Sie diese Option auswählen, importiert die Appliance die angegebenen Entspannungsregeln gebündelt und stellt sie im WAF-Profil der ausgewählten Appliance wieder her.

> **Hinweis:**
>
> Wenn Sie Relaxationsregeln in ein WAF-Profil importieren möchten, gibt es zwei Arten von Aktionen:
> Augment - Diese Aktion stellt sicher, dass der Import additiv ist und somit keine vorhandene Konfiguration außer Kraft gesetzt wird.
> Überschreiben — Diese Aktion überschreibt die bestehende Konfiguration mit der Konfiguration, die im komprimierten Exportpaket vorhanden ist.

Importieren Sie archivierte Relaxationsregeldatei mithilfe von CLI

Um die Entspannungsregeln zu importieren, müssen Sie das Archiv in die NetScaler-Appliance importieren und dann den Restore-Befehl ausführen, um die Konfiguration zu extrahieren. Der folgende

Satz von CLI-Befehlen kann zum Exportieren, Importieren und Verwalten der Konfigurationen verwendet werden.

Um die archivierte Datei vom bestimmten Speicherort zu importieren und wiederherzustellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
import appfw archive <src> <name> [-comment <string>]
```

Wo,
“src”: Gibt die Quelle der tar-Archivdatei im Formular an, <protocol>://<host>[:<port>][/<path>]
“name”: Gibt den Namen des Archivs an.
“ comment”: Kommentare, die mit diesem Archiv verknüpft sind.

```
restore appfw profile <archivename> [-relaxationRules] [-importProfileName <string>] [-matchUrlString <string>] [-replaceUrlString <string>] [-overwrite] [-augment]
```

Wobei
archivename: Zeigt die Quelle für das TAR-Archiv an. Dies ist ein zwingendes Argument.
“RelaxationRules”: Option zum Importieren aller appfw-Entspannungsregeln.

importProfileName: Gibt den Profilnamen an, der erstellt oder aktualisiert wurde, um die Entspannungsregeln während des Wiederherstellungsvorgangs zuzuordnen.
“ MatchUrlString”: Gibt die Action-URL-Zeichenfolge an, die in archivierten Relaxationsregeln übereinstimmt.

replaceUrlString: Zeigt die Zeichenfolge an, die in Aktion ersetzt werden soll, während Entspannungsregeln wiederhergestellt werden soll.

overwrite: Bestehende Regelaktion, um bestehende Entspannungsregeln zu bereinigen und während des Imports zu ersetzen.

augment: Bestehende Regelaktion zur Verstärkung von Relaxationsregeln während des Imports.

Beispiel:

```
import appfw archive local: dutA_test_pr.tgz demo
restore appfw profile dutA_test_pr
```

Exportieren Sie die archivierte Datei über die Befehlszeilenschnittstelle in die ausgewählte Appliance

Wenn Sie die Appfw-Entspannungsregeln mit CLI exportieren, müssen Sie die Konfiguration archivieren und dann exportieren.
Um die archivierte Datei zu archivieren und zu exportieren, geben Sie an der Eingabeaufforderung Folgendes ein:


```
archive appfw profile <name> <archivename> [-comment <string>]
```

Wobei
`archive name`: Zeigt die Quelle für das TAR-Archiv an. Dies ist ein zwingendes Argument.
`name`: Gibt den appfw-Profilnamen an, der die zu exportierenden Entspannungsregeln enthält

```
export appfw archive <name> <target>
```

Wo,
Name. Name des TAR-Archiv. Dies ist ein zwingendes Argument. Maximale Länge: 31
Ziel. Pfad zur zu exportierenden Datei. Dies ist ein zwingendes Argument. Maximale Länge: 2047

Beispiel:

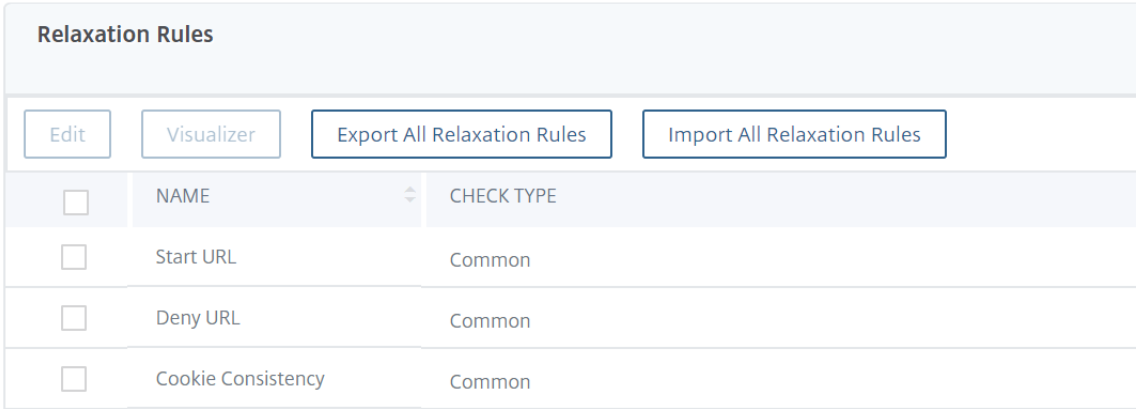
```
> archive appfw profile test_pr archived_test_pr
```

```
> export appfw archive archived_test_pr local:dutA_test_pr
```

So exportieren Sie Relaxationsregeln über die NetScaler GUI

Befolgen Sie die unten angegebenen Schritte, um Entspannungsregeln zu exportieren:

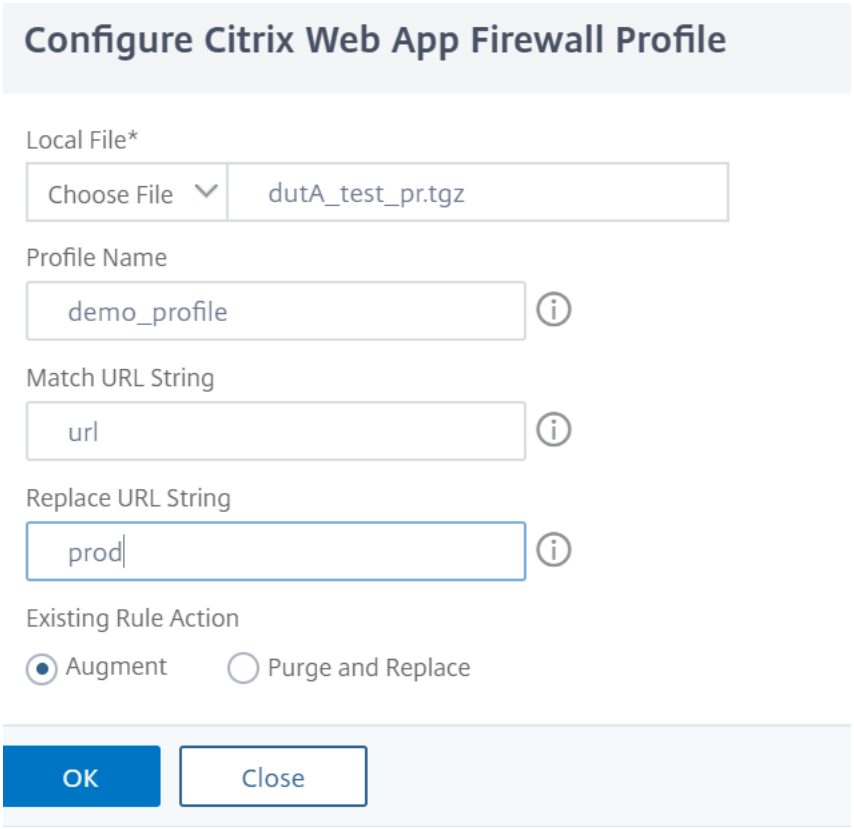
1. Navigieren Sie zu **Sicherheit** > **NetScaler Web App Firewall**.
2. Klicken Sie auf der Detailseite im Abschnitt **Konfigurationsübersicht** auf den Link **NetScaler Web App Firewall Profiles** .
3. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** unter **Erweiterte Einstellungen** auf den Link **Entspannungsregeln** .
4. Klicken Sie im Abschnitt **Entspannungsregeln** auf **Alle Entspannungsregeln exportieren**. Die Aktion gilt für alle Sicherheitsüberprüfungen und für diejenigen, bei denen dynamisches Lernen in diesem Profil aktiviert ist.



So importieren Sie Relaxationsregeln über die NetScaler GUI

Führen Sie die Schritte aus, um Entspannungsregeln zu importieren:

1. Navigieren Sie zu **Sicherheit** > **NetScaler Web App Firewall**.
2. Klicken Sie auf der Detailseite im Abschnitt " **Konfigurationsübersicht** " auf den Link **NetScaler Web App Firewall Profiles** .
3. Klicken Sie auf der Seite **NetScaler Web App Firewall Profile** unter **Erweiterte Einstellungen** auf den Link **Entspannungsregeln** .
4. Klicken Sie im Abschnitt **Entspannungsregeln** auf **Alle Entspannungsregeln importieren**.
5. Legen Sie auf der Seite **NetScaler Web App Firewall-Profil konfigurieren** die folgenden Parameter fest:
   a) Lokale Datei. Name der komprimierten archivierten Datei, die die Entspannungsregeln enthält.
   b) Name des Profils. Name des Profils, an das die Entspannungsregeln gebunden sind.
   c) Passende URL-Zeichenfolge. Teil der URL, der übereinstimmt.
   d) Ersetzen Sie den URL-String Teil der URL, der die URL-Zeichenfolge ersetzt.
   e) Bestehende Regelaktion. Wählen Sie aus, ob die Regel bestehende Regeln überschreiben oder die bestehenden Regeln erweitern muss.
6. Klicken Sie auf **OK**.



Ergänzende Informationen zu Profilen

May 11, 2023

Im Folgenden finden Sie zusätzliche Informationen zu bestimmten Aspekten von Web App Firewall-Profilen. In diesen Informationen wird erläutert, wie Sonderzeichen in eine Sicherheitsüberprüfungsregel oder Entspannung aufgenommen werden und wie Variablen beim Konfigurieren von Profilen verwendet werden.

Unterstützung von Konfigurationsvariablen

Anstatt statische Werte zu verwenden, können Sie zum Konfigurieren der Sicherheitsüberprüfungen und -einstellungen der Web App Firewall jetzt benannte NetScaler-Standardvariablen verwenden. Durch das Erstellen von Variablen können Sie Konfigurationen einfacher exportieren und dann in neue NetScaler Appliances importieren oder vorhandene NetScaler Appliances aus einem einzigen Satz von Konfigurationsdateien aktualisieren. Dies vereinfacht Updates, wenn Sie ein Testbett-Setup verwenden, um eine komplexe Web App Firewall-Konfiguration zu entwickeln, die auf Ihr lokales Netzwerk und Ihre Server abgestimmt ist, und diese Konfiguration dann auf Ihre NetScaler-Produktionsanlagen übertragen.

Sie erstellen Web App Firewall Konfigurationsvariablen auf die gleiche Weise wie alle anderen NetScaler Variablen, die nach den standardmäßigen NetScaler-Konventionen ausgeführt werden. Sie können eine benannte Ausdrucksvariable mithilfe der NetScaler-Befehlszeile oder der GUI erstellen.

Die folgenden URLs und Ausdrücke können mit Variablen anstelle von statischen Werten konfiguriert werden:

- **URL starten** (-starturl)
- **URL verweigern** (-denyurl)
- **Formularaktions-URL** für *Konsistenzprüfung von Formularfeldern* (-fieldconsistency)
- **Aktions-URL** für *XML SQL Injection Check* (-xmlSQLInjection)
- **Aktions-URL** für *XML-Cross-Site-Scripting Check* (-xmlcross-site scripting)
- **Formularaktions-URL** für *HTML SQL Injection Check* (-sqlInjection)
- **Formularaktions-URL** für *Field Format Check* (-fieldFormat)
- **Formularursprung-URL** und **Formularaktions-URL** für die *Prüfung auf websiteübergreifende Anforderungsfälschung (CSRF)* (-csrfTag)
- **Formularaktions-URL** für die *HTML Cross-Site Scripting Check* (-crossSiteScripting)
- **Safe Object** (-safeObject)
- **Aktions-URL** für *XML Denial-of-Service (XDoS)-Prüfung* (-XMLDoS)
- **URL** für die *Interoperabilitätsprüfung von Webdiensten* (-XMLWSIURL)
- <**URL** für die *XML-Validierungsprüfung* (-XMLValidationURL)

- **URL** für die *Überprüfung von XML-Anhängen* (-XMLAttachmentURL)

Weitere Informationen finden Sie unter Richtlinien und Ausdrücke.

Um eine Variable in der Konfiguration zu verwenden, schließen Sie den Variablennamen zwischen zwei bei (@) -Symbolen ein und verwenden sie dann genau so, wie Sie den statischen Wert, den sie ersetzt. Wenn Sie beispielsweise die Deny-URL-Prüfung über die grafische Benutzeroberfläche konfigurieren und die benannte Ausdrucksvariable myDenyURL zur Konfiguration hinzufügen möchten, geben Sie @myDenyURL@ in das Dialogfeld Verweigern-URL hinzufügen im Textbereich URL verweigern ein. Um dieselbe Aufgabe mithilfe der NetScaler-Befehlszeile auszuführen, geben Sie appfw profile <name> -denyURLAction @myDenyURL@ ein.

PCRE-Zeichencodierungsformat

Das NetScaler-Betriebssystem unterstützt nur die direkte Eingabe von Zeichen in den druckbaren ASCII-Zeichensatz — Zeichen mit Hexadezimalcodes zwischen HEX 20 (ASCII 32) und HEX 7E (ASCII 127). Um ein Zeichen mit einem Code außerhalb dieses Bereichs in Ihre Web App Firewall-Konfiguration aufzunehmen, müssen Sie seinen UTF-8-Hexadezimalcode als regulären PCRE-Ausdruck eingeben.

Für eine Reihe von Zeichentypen ist die Codierung mit einem regulären PCRE-Ausdruck erforderlich, wenn Sie sie als URL, Formularfeldname oder Safe-Object-Ausdruck in Ihre Web App Firewall-Konfiguration aufnehmen. Sie beinhalten:

- **Obere-ASCII-Zeichen.** Zeichen mit Kodierungen von HEX 7F (ASCII 128) bis HEX FF (ASCII 255). Abhängig von der verwendeten Zeichenzuordnung können sich diese Kodierungen auf Steuercodes, ASCII-Zeichen mit Akzenten oder anderen Modifikationen, nicht-lateinische Alphabet-Zeichen und Symbole beziehen, die nicht im ASCII-Basissatz enthalten sind. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken vorkommen.
- **Doppelbyte-Zeichen.** Zeichen mit Kodierungen, die zwei 8-Byte-Wörter verwenden. Doppelbyte-Zeichen werden hauptsächlich für die Darstellung von chinesischem, japanischem und koreanischem Text in elektronischer Form verwendet. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken vorkommen.
- **ASCII-Steuerzeichen.** Nicht druckbare Zeichen, die zum Senden von Befehlen an einen Drucker verwendet werden. Alle ASCII-Zeichen mit Hexadezimalcodes kleiner als HEX 20 (ASCII 32) fallen in diese Kategorie. Diese Zeichen dürfen jedoch niemals in einem URL- oder Formularfeldnamen vorkommen und würden selten, wenn überhaupt, in einem sicheren Objektausdruck vorkommen.

Die NetScaler Appliance unterstützt nicht den gesamten UTF-8-Zeichensatz, sondern nur die Zeichen in den folgenden acht Zeichensätzen:

- **Englisch US (ISO-8859-1).** Obwohl die Bezeichnung “English US” lautet, unterstützt die Web App Firewall alle Zeichen im ISO-8859-1-Zeichensatz, auch Latin-1-Zeichensatz genannt. Dieser Zeichensatz repräsentiert vollständig die meisten modernen westeuropäischen Sprachen und repräsentiert alle bis auf einige ungewöhnliche Zeichen im Rest.
- **Traditionelles Chinesisch (Big5).** Die Web App Firewall unterstützt alle Zeichen im BIG5-Zeichensatz, der alle traditionellen chinesischen Schriftzeichen (Ideogramme) enthält, die im modernen Chinesisch häufig verwendet werden, wie sie in Hongkong, Macau, Taiwan und von vielen Menschen chinesischer ethnischer Herkunft, die außerhalb des chinesischen Festlandes leben, gesprochen und geschrieben werden.
- **Chinesisch vereinfacht (GB2312).** Die Web App Firewall unterstützt alle Zeichen im GB2312-Zeichensatz, der alle im modernen Chinesisch gebräuchlichen vereinfachten chinesischen Schriftzeichen (Ideogramme) enthält, wie sie auf dem chinesischen Festland gesprochen und geschrieben werden.
- **Japanisch (SJIS).** Die Web App Firewall unterstützt alle Zeichen im Shift-JIS (SJIS) -Zeichensatz, der die meisten Zeichen (Ideogramme) enthält, die üblicherweise im modernen Japanisch verwendet werden.
- **Japanisch (EUC-JP).** Die Web App Firewall unterstützt alle Zeichen im EUC-JP-Zeichensatz, einschließlich aller Zeichen (Ideogramme), die üblicherweise im modernen Japanisch verwendet werden.
- **Koreanisch (EUC-KR).** Die Web App Firewall unterstützt alle Zeichen im EUC-KR-Zeichensatz, einschließlich aller Zeichen (Ideogramme), die üblicherweise im modernen Koreanisch verwendet werden.
- **türkisch (ISO-8859-9).** Die Web App Firewall unterstützt alle Zeichen im ISO-8859-9-Zeichensatz, der alle im modernen Türkisch verwendeten Buchstaben umfasst.
- **Unicode (UTF-8).** Die Web App Firewall unterstützt bestimmte zusätzliche Zeichen im UTF-8-Zeichensatz, einschließlich solcher, die im modernen Russisch verwendet werden.

Bei der Konfiguration der Web App Firewall geben Sie alle Nicht-ASCII-Zeichen als reguläre Ausdrücke im PCRE-Format ein, indem Sie den Hexadezimalcode verwenden, der diesem Zeichen in der UTF-8-Spezifikation zugewiesen ist. Symbolen und Zeichen innerhalb des normalen ASCII-Zeichensatzes, denen in diesem Zeichensatz einzelne, zweistellige Codes zugewiesen sind, werden im UTF-8-Zeichensatz dieselben Codes zugewiesen. Zum Beispiel das Ausrufezeichen (!) , dem der Hexadezimalcode 21 im ASCII-Zeichensatz zugewiesen ist, ist auch Hex 21 im UTF-8-Zeichensatz. Symbolen und Zeichen aus einem anderen unterstützten Zeichensatz sind paarweise Hexadezimalcodes im UTF-8-Zeichensatz zugewiesen. Zum Beispiel wird dem Buchstaben a mit einem akuten Akzent (á) der UTF-8-Code C3 A1 zugewiesen.

Die Syntax, die Sie verwenden, um diese UTF-8-Codes in der Konfiguration der Web App Firewall darzustellen, ist “xNN” für ASCII-Zeichen, “\ xNN\ xNN” für Nicht-ASCII-Zeichen, die in Englisch,

Russisch und Türkisch verwendet werden, und "\ xNN\ xNN\ xNN" für Zeichen, die in Chinesisch, Japanisch und Koreanisch verwendet werden. Zum Beispiel, wenn Sie eine! in einem regulären Ausdruck der Web App Firewall als UTF-8-Zeichen würden Sie\ x21 eingeben. Wenn Sie ein á einschließen möchten, geben Sie\ xC3\ xA1 ein.

> **Hinweis:**
>
> Normalerweise müssen Sie keine ASCII-Zeichen im UTF-8-Format darstellen, aber wenn diese Zeichen einen Webbrowser oder ein zugrunde liegendes Betriebssystem verwirren könnten, können Sie die UTF-8-Darstellung des Charakters verwenden, um diese Verwirrung zu vermeiden. Wenn eine URL beispielsweise ein Leerzeichen enthält, möchten Sie den Space möglicherweise als x20 codieren, um bestimmte Browser und Webserver-Software nicht zu verwechseln.

Im Folgenden finden Sie Beispiele für URLs, Formularfeldnamen und sichere Objektausdrücke, die Nicht-ASCII-Zeichen enthalten, die als reguläre Ausdrücke im PCRE-Format eingegeben werden müssen, um in die Konfiguration der Web App Firewall aufgenommen zu werden. Jedes Beispiel zeigt zuerst die tatsächliche URL, den Feldnamen oder die Ausdruckszeichenfolge, gefolgt von einem regulären Ausdruck im PCRE-Format.

- Eine URL mit erweiterten ASCII-Zeichen.

  Aktuelle URL: `http://www.josénuñez.com`

  Codierte URL: `^http://www\[.\]jos\xC3\xA9nu\xC3\xB1ez\[.\]com$`

- Eine weitere URL mit erweiterten ASCII-Zeichen.

  Aktuelle URL: `http://www.example.de/trömso.html`

  Codierte URL: `^http://www[.]example\[.]de/tr\xC3\xB6mso[.]html$`

- Ein Formularfeldname mit erweiterten ASCII-Zeichen.

  `Actual Name: nome_do_usuário`

  Codierter Name: `^nome_do_usu\xC3\xA1rio$`

- Ein sicherer Objektausdruck, der erweiterte ASCII-Zeichen enthält.

  Uncodierter Ausdruck [A-Z] {3,6} ¥[1-9][0-9]{6,6}

  Codierter Ausdruck: [A-Z] {3,6}\ xC2\ xA5[1-9][0-9]{6,6}

Sie können eine Reihe von Tabellen finden, die den gesamten Unicode-Zeichensatz und die passenden UTF-8-Kodierungen im Internet enthalten. Eine nützliche Website, die diese Informationen enthält, befindet sich unter der folgenden URL:

`http://www.utf8-chartable.de/unicode-utf8-table.pl`

Damit die Zeichen in der Tabelle auf dieser Website korrekt angezeigt werden, muss auf Ihrem Computer eine entsprechende Unicode-Schriftart installiert sein. Wenn Sie dies nicht tun, ist die visuelle

Anzeige des Charakters möglicherweise fehlerhaft. Selbst wenn Sie keine geeignete Schriftart zur Anzeige eines Zeichens installiert haben, sind die Beschreibung und die UTF-8- und UTF-16-Codes auf diesen Webseiten korrekt.

Invertierte PCRE-Ausdrücke

Zusätzlich zum übereinstimmenden Inhalt, der ein Muster enthält, können Sie auch Inhalt zuordnen, der kein Muster enthält, indem Sie einen invertierten PCRE-Ausdruck verwenden. Um einen Ausdruck umzukehren, fügen Sie einfach ein Ausrufezeichen (!) gefolgt von Leerraum als erstes Zeichen im Ausdruck.

> **Hinweis:** Wenn ein Ausdruck nur aus einem Ausrufezeichen besteht und nichts folgt, wird das Ausrufezeichen als Literalzeichen behandelt und nicht als Syntax, die einen invertierten Ausdruck angibt.

Die folgenden Web App Firewall Befehle unterstützen invertierte PCRE-Ausdrücke:

- Start-URL (URL)
- URL verweigern (URL)
- Konsistenz des Formularfeldes (Formularaktions-URL)
- Cookie-Konsistenz (Formularaktions-URL)
- Websiteübergreifende Anforderungsfälschung (CSRF) (Formularaktions-URL)
- HTML Cross-site Scripting (Formularaktions-URL)
- Feldformat (Formularaktions-URL)
- Feldtyp (Typ)
- Vertrauliches Feld (URL)

Hinweis: Wenn die Sicherheitsüberprüfung ein IsRegex-Flag oder -Kontrollkästchen enthält, muss sie auf YES gesetzt oder aktiviert sein, um reguläre Ausdrücke im Feld zu aktivieren. Andernfalls wird der Inhalt dieses Feldes als Literal behandelt und es werden keine regulären Ausdrücke (invertiert oder nicht) analysiert.

Unzulässige Namen für Web App Firewall-Profile

Die folgenden Namen werden integrierten Aktionen und Profilen auf der NetScaler Appliance zugewiesen und können nicht als Namen für ein vom Benutzer erstelltes Web App Firewall-Profil verwendet werden.

- AGRESSIVE
- ALLOW
- BASIC
- CLIENTAUTH
- COMPRESS

- CSSMINIFY
- DEFLATE
- DENY
- DNS-NOP
- DROP
- GZIP
- HTMLMINIFY
- IMGOPTIMIZE
- JSMINIFY
- MODERATE
- NOCLIENTAUTH
- NOCOMPRESS
- NONE
- NOOP
- NOREWRITE
- RESET
- SETASLEARNNSLOG_ACT
- SETNSLOGPARAMS_ACT
- SETSYSLOGPARAMS_ACT
- SETTMSESSPARAMS_ACT
- SETVPNPARAMS_ACT
- SET_PREAUTHPARAMS_ACT
- default_DNS64_action
- dns_default_act_Cachebypass
- dns_default_act_Drop
- nshttp_default_profile
- nshttp_default_strict_validation
- nstcp_default_Mobile_profile
- nstcp_default_XA_XD_profile
- nstcp_default_profile
- nstcp_default_tcp_interactive_stream
- nstcp_default_tcp_lan
- nstcp_default_tcp_lan_thin_stream
- nstcp_default_tcp_lfp
- nstcp_default_tcp_lfp_thin_stream
- nstcp_default_tcp_lnp
- nstcp_default_tcp_lnp_thin_stream
- nstcp_internal_apps

Benutzerdefinierter Fehlerstatus und Meldung für HTML-, XML- und JSON-Fehlerobjekt

May 11, 2023

Wenn die NetScaler Web App Firewall einen Verstoß erkennt, verarbeitet die Appliance das Fehlerszenario entweder mit einer Umleitungs-URL oder dem Fehlerobjekt (in das Profil importiert und aktiviert). Wenn das Szenario mit einer Fehlerobjektkonfiguration behandelt wird, liefert das WAF-Profil einen benutzerdefinierten Antwortstatuscode und eine benutzerdefinierte Meldung. Sie können die Antwortfehlerdetails für ein HTML-, XML- oder JSON-Fehlerobjekt im WAF-Profil anpassen.

> **Hinweis:**
>
> Standardmäßig werden der Fehlercode und die Fehlermeldung auf “200” und “OK” festgelegt, wenn die Einstellungen für Fehlerobjekte konfiguriert sind.

Beim Umgang mit Fehlerszenarien ist es wichtig, dass die Appliance mit dem entsprechenden HTTP-Antwortstatuscode und einer entsprechenden Meldung für die Behebung von Problemen antwortet. Durch die Bereitstellung einer benutzerdefinierten Fehlerstatusmeldung und eines benutzerdefinierten Fehlerstatuscodes kann die Appliance einen besseren Benutzereingriff ermöglichen, um ein Problem bei Auftreten eines Verstoßes zu beheben. Wenn Sie beispielsweise den Antwortfehlercode auf “404” und die Statusmeldung auf “Nicht gefunden” setzen, kann der Benutzer den Antwortstatuscode und die Nachricht überprüfen, um zu überprüfen, ob ein Verstoß aufgetreten ist. Dies kann dem Benutzer helfen, Antworten zu filtern, die das Fehlerobjekt enthalten

Konfigurieren Sie den benutzerdefinierten Statuscode und die Meldung für ein HTML-Fehlerobjekt in einem WAF-Profil über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set appfw profile <profile-name> -HTMLErrorStatusCode <value> -
    HTMLErrorStatusMessage <value> -useHTMLErrorObject ON
<!--NeedCopy-->
```

Beispiel:

```
set appfw profile profile_1 -HTMLErrorStatusCode 404 -HTMLErrorStatusMessage
  “Not Found”  -useHTMLErrorObject ON
```

Konfigurieren Sie den benutzerdefinierten Statuscode und die Meldung für das XML-Fehlerobjekt in einem WAF-Profil über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
1 set appfw profile <profile-name> -XMLErrorStatusCode <value> -
     XMLErrorStatusMessage <value>
2 <!--NeedCopy-->
```

Beispiel:

```
set appfw profile profile_1 -XMLErrorStatusCode 406 - XMLErrorStatusMessage
  “Not Acceptable”
```

Konfigurieren Sie den benutzerdefinierten Statuscode und die Meldung für das JSON-Fehlerobjekt in einem WAF-Profil über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set appfw profile <profile-name> -JSONErrorStatusCode <value> -
     JSONErrorStatusMessage <value>
2 <!--NeedCopy-->
```

Beispiel:

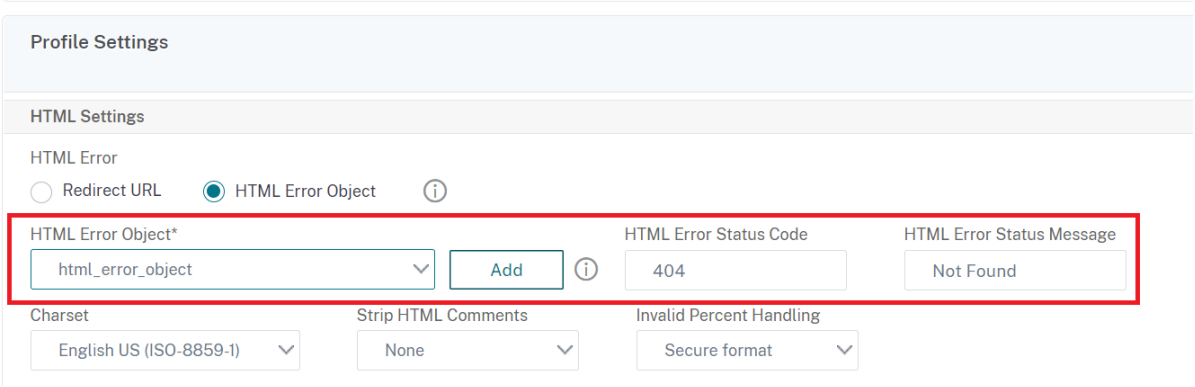
```
set appfw profile profile_1 -JSONErrorStatusCode 500 - JSONErrorStatusMessage
  “Internal Server Error”
```

Konfigurieren Sie den benutzerdefinierten Statuscode und die Nachricht für HTML-, JSON- oder XML-Fehlerobjekt in einem WAF-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Klicken Sie im Detailbereich auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Web App Firewall-Profil erstellen** im Abschnitt **Erweiterte Einstellungen** auf **Profileinstellungen**.
4. Legen Sie im Abschnitt **Profileinstellungen** die folgenden Parameter fest.

   a. HTML-Fehlerobjekt. Wählen Sie die Option zur Übergabe von Fehlerszenarien mit einem HTML-Fehlerobjekt aus. Importieren Sie das Fehlerobjekt aus einer URL, Datei oder einem Text.
   b. HTML-Fehlerstatuscode. Geben Sie einen benutzerdefinierten Fehlerstatuscode an.
   c. HTML-Fehlerstatusmeldung Geben Sie eine Kundenfehlermeldung ein.
5. Klicken Sie auf **OK** und **Fertig**.

> **Hinweis:**
>
> Das gleiche Verfahren gilt für benutzerdefinierte Fehlerobjekteinstellungen von JSON und XML.



Richtlinien

May 11, 2023

Ein Policy Label besteht aus einer Reihe von Richtlinien, anderen Richtlinienbezeichnungen und virtuellen serverspezifischen Richtlinienbanken. Die Web App Firewall wertet jede an das Richtlinienlabel gebundene Policy Label in der Reihenfolge ihrer Priorität aus. Wenn die Richtlinie übereinstimmt, filtert sie die Verbindung wie im zugehörigen Profil angegeben. Dann tut es alles, was der Goto -Parameter angibt, nämlich die Richtlinienbewertung zu beenden, zur nächsten Richtlinie zu wechseln oder zur Richtlinie mit der angegebenen Priorität zu wechseln. Wenn der Invoke-Parameter festgelegt ist, beendet er die Verarbeitung der aktuellen Policy Label und beginnt mit der Verarbeitung der angegebenen Policy Label oder des virtuellen Servers.

So erstellen Sie mithilfe der Befehlszeile ein Web App Firewall-Richtlinienlabel

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw policylabel <labelName> http_req`
- `save ns config`

Beispiel

Im folgenden Beispiel wird ein Policy Label mit dem Namen policylbl1 erstellt.

```
1 add appfw policylabel policylbl1 http_req
2 save ns config
3 <!--NeedCopy-->
```


So binden Sie eine Policy Label mithilfe der Befehlszeile an ein Richtlinienlabel

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw policylabel <labelName> <policyName> <priority> [<gotoPriorityExpressi >] [-invoke (<labelType> <labelName>)]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird die Policy1 mit der Priorität 1 an das Richtlinienlabel policylbl1 gebunden.

```
bind appfw policylabel policylbl1 policy1 1
save ns config
<!--NeedCopy-->
```

So konfigurieren Sie ein Web App Firewall-Richtlinienlabel über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Richtlinienbeschriftungen**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um ein neues Policy Label hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um ein vorhandenes Policy Label zu konfigurieren, wählen Sie das Policy Label aus und klicken dann auf **Öffnen**.

   Das Dialogfeld **Web App Firewall Policy Label erstellen** oder **Web App Firewall konfigurieren** wird geöffnet. Die Dialogfelder sind nahezu identisch.
3. Wenn Sie ein neues Richtlinienlabel erstellen, geben Sie im Dialogfeld Web App Firewall Policy Label erstellen einen Namen für Ihre neue Richtlinienbezeichnung ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und aus einem bis 127 Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), at (@), Gleichheit (=), Doppelpunkt (:) und Unterstrich (_) bestehen.
4. Wählen Sie **Richtlinie einfügen** aus, um eine neue Zeile einzufügen und eine Dropdownliste mit allen vorhandenen Web App Firewall -Richtlinien anzuzeigen.
5. Wählen Sie die Richtlinie aus, die Sie an das Policy Label binden möchten, oder wählen Sie Neue Richtlinie aus, um eine neue Richtlinie zu erstellen, und befolgen Sie die Anweisungen unter So erstellen und konfigurieren Sie eine Richtlinie über die grafische Benutzeroberfläche. Die ausgewählte oder erstellte Richtlinie wird in die Liste der global gebundenen Web App Firewall Richtlinien eingefügt.
6. Nehmen Sie zusätzliche Anpassungen vor.

- Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten neu generieren auswählen, um die Prioritäten gleichmäßig neu zu nummerieren.
- Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld Web App Firewall-Richtlinie konfigurieren zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.
- Um den Goto-Ausdruck festzulegen, doppelklicken Sie auf das Feld in der Spaltenüberschrift Goto Expression, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
- Um die Option Aufrufen festzulegen, doppelklicken Sie in der Spaltenüberschrift Aufrufen auf das Feld, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können

7. Wiederholen Sie die Schritte 5 bis 7, um zusätzliche Web App Firewall-Richtlinien, die Sie möchten, an die Policy Label zu binden.
8. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass Sie die Richtlinienbezeichnung erfolgreich erstellt oder geändert haben.

Richtlinien

May 11, 2023

Die Web App Firewall verwendet zwei Arten von Richtlinien: Firewallrichtlinien und Überwachungsrichtlinien. Firewall-Richtlinien steuern, welcher Datenverkehr an die Web App Firewall gesendet wird. Überwachungsrichtlinien steuern den Protokollserver, an den die Web App Firewall-Protokolle gesendet werden.

Firewall-Richtlinien können komplex sein, da die Richtlinienregel aus mehreren Ausdrücken in der NetScaler-Ausdruckssprache bestehen kann. Dabei handelt es sich um eine vollwertige objektorientierte Programmiersprache, die mit extremer Präzision genau definieren kann, welche Verbindungen gefiltert werden sollen. Da Firewallrichtlinien im Kontext der Web App Firewall funktionieren, müssen sie bestimmte Kriterien erfüllen, die damit zusammenhängen, wie die Web App Firewall funktioniert und welcher Datenverkehr von ihr angemessen gefiltert wird. Solange Sie diese Kriterien berücksichtigen, ähneln Firewallrichtlinien jedoch den Richtlinien für andere NetScaler-Funktionen. Die Anweisungen hier versuchen nicht, alle Aspekte des Schreibens von Firewall-Richtlinien zu behandeln, sondern bieten nur eine Einführung in die Richtlinien und behandeln die Kriterien, die nur für die Web App Firewall gelten.

Die Überwachung von Richtlinien ist einfach, da die Richtlinienregel immer ns_true lautet. Sie müssen

nur den Protokollserver angeben, an den Sie Protokolle senden möchten, die Protokollierungsstufen, die Sie verwenden möchten, und einige weitere Kriterien, die detailliert erläutert werden.

Richtlinien für Web App Firewall

May 11, 2023

Eine Firewall-Richtlinie ist eine Regel, die einem Profil zugeordnet ist. Die Regel ist ein Ausdruck oder eine Gruppe von Ausdrücken, die die Arten von Anforderungs-/Antwortpaaren definieren, die die Web App Firewall durch Anwenden des Profils filtern soll. Firewall-Richtlinienausdrücke sind in der NetScaler-Ausdruckssprache geschrieben, einer objektorientierten Programmiersprache mit speziellen Funktionen zur Unterstützung bestimmter NetScaler-Funktionen. Das Profil ist der Satz von Aktionen, die die Web App Firewall verwenden soll, um Anforderungs-/Antwortpaare zu filtern, die der Regel entsprechen.

Mithilfe von Firewall-Richtlinien können Sie verschiedenen Arten von Webinhalten unterschiedliche Filterregeln zuweisen. Nicht alle Webinhalte sind gleich. Eine einfache Website, die kein komplexes Scripting verwendet und auf private Daten zugreift und diese verarbeitet, erfordert möglicherweise nur das Schutzniveau eines Profils, das mit grundlegenden Standardeinstellungen erstellt wurde. Webinhalte, die JavaScript-erweiterte Webformulare enthalten oder auf eine SQL-Datenbank zugreifen, erfordern wahrscheinlich einen maßgeschneiderten Schutz. Sie können ein anderes Profil erstellen, um diesen Inhalt zu filtern und eine separate Firewall-Richtlinie zu erstellen, die bestimmen kann, welche Anfragen versuchen, auf diese Inhalte zuzugreifen. Dann verknüpfen Sie den Richtlinienausdruck mit einem von Ihnen erstellten Profil und binden die Richtlinie global, um sie in Kraft zu setzen.

Die Web App Firewall verarbeitet nur HTTP-Verbindungen und verwendet daher eine Teilmenge der gesamten NetScaler-Ausdruckssprache. Die Informationen hier beschränken sich auf Themen und Beispiele, die bei der Konfiguration der Web App Firewall nützlich sein dürften. Im Folgenden finden Sie Links zu weiteren Informationen und Verfahren für Firewall-Richtlinien:

- Anweisungen, die erklären, wie Sie eine Richtlinie erstellen und konfigurieren, finden Sie unter Erstellen und Konfigurieren von Web App Firewall-Richtlinien.
- Eine Prozedur, die ausführlich erklärt, wie eine Richtlinienregel (Ausdruck) erstellt wird, finden Sie unter So erstellen oder konfigurieren Sie eine Web App Firewall-Regel (Ausdruck).
- Eine Prozedur, die erklärt, wie Sie das Dialogfeld Ausdruck hinzufügen zum Erstellen einer Richtlinienregel verwenden, finden Sie unter So fügen Sie eine Firewallregel (Ausdruck) mithilfe des Dialogfelds Ausdruck hinzufügen hinzu.
- Eine Prozedur, die erklärt, wie Sie die aktuellen Bindungen für eine Richtlinie anzeigen, finden Sie unter Anzeigen der Bindungen einer Firewall-Richtlinie.
- Anweisungen, die erklären, wie Sie eine Web App Firewall-Richtlinie binden, finden Sie unter Binden von Web App Firewall-Richtlinien.

- Ausführliche Informationen zur Sprache der NetScaler-Ausdrücke finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis**
>
> Die Web App Firewall wertet die Richtlinien basierend auf den konfigurierten Prioritäts- und Gehe zu Ausdrücken aus. Am Ende der Richtlinienbewertung wird die letzte Richtlinie verwendet, die als wahr ausgewertet wird, und die Sicherheitskonfiguration des entsprechenden Profils wird zur Verarbeitung der Anforderung aufgerufen.
>
> Stellen Sie sich beispielsweise ein Szenario vor, in dem es 2 Richtlinien gibt.
>
> - Policy_1 ist eine generische Richtlinie mit expression=NS_True und hat ein entsprechendes Profile_1, das ein Basisprofil ist. Die Priorität ist auf 100 festgelegt.
> - Policy_2 ist spezifischer mit Expression=HTTP.REQ.URL.CONTAINS(“XYZ”) und hat ein entsprechendes profile_2, das ein fortgeschrittenes Profil ist. Der GoTo-Ausdruck ist auf NEXT und die Priorität auf 95 festgelegt, was im Vergleich zu Policy_1 eine höhere Priorität hat.
>
> Wenn in diesem Szenario die Zielzeichenfolge “XYZ” in der URL der verarbeiteten Anforderung erkannt wird, wird eine Übereinstimmung mit Policy_2 ausgelöst, da sie eine höhere Priorität hat, obwohl Policy_1 ebenfalls eine Übereinstimmung ist. Gemäß der GoTo-Ausdruckskonfiguration von Policy_2 wird die Richtlinienbewertung jedoch fortgesetzt und die nächste policy_1 wird ebenfalls verarbeitet. Am Ende der Richtlinienauswertung wird Policy_1 als wahr ausgewertet und die in Profile_1 konfigurierten grundlegenden Sicherheitsüberprüfungen werden aufgerufen.
>
> Wenn Policy_2 geändert wird und der GoTo-Ausdruck von **NEXT** in **END** geändert wird, löst die verarbeitete Anforderung, die die Zielzeichenfolge “XYZ” enthält, die Übereinstimmung mit Policy_2 aufgrund der Prioritätsüberlegung aus und gemäß der Konfiguration des GoTo-Ausdrucks endet die Richtlinienauswertung um dieser Punkt. Policy_2 wird als wahr ausgewertet und die in Profile_2 konfigurierten erweiterten Sicherheitsüberprüfungen werden aufgerufen.
>
> **NEXT**
> **END**
>
> Die Bewertung der Richtlinie wird in einem Durchgang abgeschlossen. Sobald die Richtlinienbewertung für die Anforderung abgeschlossen ist und die entsprechenden Profilaktionen aufgerufen werden, durchläuft die Anforderung keine weitere Runde der Richtlinienbewertung.

Erstellen und Konfigurieren von Web App Firewall-Richtlinien

May 11, 2023

Eine Firewall-Richtlinie besteht aus zwei Elementen: einer *Regel*und einem zugeordneten *Profil*. Die Regel wählt den HTTP-Datenverkehr aus, der den von Ihnen festgelegten Kriterien entspricht, und sendet diesen Datenverkehr zur Filterung an die Web App Firewall. Das Profil enthält die Filterkriterien, die die Web App Firewall verwendet.

Die Richtlinienregel besteht aus einem oder mehreren Ausdrücken in der Sprache für NetScaler Ausdrücke. Die Syntax von NetScaler Expressions ist eine leistungsstarke, objektorientierte Programmiersprache, mit der Sie den Datenverkehr, den Sie mit einem bestimmten Profil verarbeiten möchten, genau bestimmen können. Für Benutzer, die mit der Sprachsyntax für NetScaler-Ausdrücke nicht vertraut sind oder ihre NetScaler-Appliance über eine webbasierte Oberfläche konfigurieren möchten, bietet die GUI zwei Tools: das **Präfix-Menü** und das Dialogfeld **Ausdruck hinzufügen** . Beide helfen Ihnen beim Schreiben von Ausdrücken, die genau den Datenverkehr auswählen, den Sie verarbeiten möchten. Erfahrene Benutzer, die mit der Syntax vertraut sind, bevorzugen möglicherweise die NetScaler-Befehlszeile, um ihre NetScaler-Appliances zu konfigurieren.

> **Hinweis:**
>
> Zusätzlich zur Syntax der Standardausdrücke unterstützt das NetScaler-Betriebssystem aus Gründen der Abwärtskompatibilität die Syntax für klassische Ausdrücke von NetScaler auf NetScaler Classic- und NCore-Appliances und virtuellen Appliances. Klassische Ausdrücke werden auf NetScaler Cluster-Appliances und virtuellen Appliances nicht unterstützt. Aktuelle NetScaler Benutzer, die vorhandene Konfigurationen in den NetScaler Cluster migrieren möchten, müssen alle Richtlinien, die klassische Ausdrücke enthalten, in die Standardausdrucksyntax migrieren.

Ausführliche Informationen zu den Sprachen der NetScaler-Ausdrücke finden Sie unter Richtlinien und Ausdrücke.

Sie können eine Firewallrichtlinie mit der GUI oder der NetScaler Befehlszeile erstellen.

So erstellen und konfigurieren Sie eine Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw policy <name><rule> <profileName>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird eine Richtlinie mit dem Namen pl-blog mit einer Regel hinzugefügt, die den gesamten Datenverkehr zum oder vom Host blog.example.com abfängt und diese Richtlinie dem Profil pr-Blog zuordnet. Dies ist eine geeignete Richtlinie zum Schutz eines Blogs, das auf einem bestimmten Hostnamen gehostet wird.


```
add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com")" pr-blog
<!--NeedCopy-->
```

So erstellen und konfigurieren Sie eine Richtlinie mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Richtlinien**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Firewall-Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**. Die **Richtlinie “Web App Firewall erstellen** “ wird angezeigt.
   - Um eine vorhandene Firewall-Richtlinie zu bearbeiten, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Bearbeiten**.

   Die **Richtlinie “Web App Firewall erstellen** “ oder **“Web App Firewall konfigurieren** “ wird angezeigt.
3. Wenn Sie eine Firewall-Richtlinie **erstellen, geben Sie im Dialogfeld Web App Firewall App-Firewall-Richtlinie** erstellen im Textfeld Richtlinienname einen Namen für Ihre neue Richtlinie ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und aus einem bis 128 Buchstaben, Zahlen und den Symbolen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), at (@), Gleichheit (=), Doppelpunkt (:) und Unterstrich (_) bestehen.

   Wenn Sie eine vorhandene Firewall-Richtlinie konfigurieren, ist dieses Feld schreibgeschützt. Sie können es nicht ändern.
4. Wählen Sie in der Dropdown-Liste Profil das Profil aus, das Sie dieser Richtlinie zuordnen möchten. Sie können ein Profil erstellen, das mit Ihrer Richtlinie verknüpft wird, indem Sie auf Neu klicken, und Sie können ein vorhandenes Profil ändern, indem Sie auf Ändernklicken.
5. Erstellen Sie im Textbereich Ausdruck eine Regel für Ihre Richtlinie.
   - Sie können eine Regel direkt in den Textbereich eingeben.
   - Sie können auf Präfix klicken, um den ersten Begriff für Ihre Regel auszuwählen, und den Anweisungen folgen.
   - Sie können auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und damit die Regel zu erstellen.
6. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.

So erstellen oder konfigurieren Sie eine Web App Firewall-Regel (Ausdruck)

Die Richtlinienregel, auch *Ausdruck*genannt, definiert den Webverkehr, den die Web App Firewall mithilfe des mit der Richtlinie verknüpften Profils filtert. Wie andere NetScaler-Richtlinienregeln (oder *Ausdrücke*) verwenden die Web App Firewall-Regeln die Syntax von NetScaler-Ausdrücken. Diese Syntax ist leistungsstark, flexibel und erweiterbar. Es ist zu komplex, um es in diesen Anweisungen vollständig zu beschreiben. Sie können das folgende Verfahren verwenden, um eine einfache Firewall-Richtlinienregel zu erstellen, oder Sie können sie als Überblick über den Richtlinienerstellungsprozess lesen.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie im **Web App Firewall-Assistenten** oder in der NetScaler-GUI zum entsprechenden Speicherort, um Ihre Richtlinienregel zu erstellen:

   - Wenn Sie eine Richtlinie im **Web App Firewall-Assistenten** konfigurieren, klicken Sie im Navigationsbereich auf **Web App Firewall**, dann im Detailbereich auf **Web App Firewall Wizard**, und navigieren Sie dann zum Bildschirm „ **Regel angeben**“.
   - Wenn Sie eine Richtlinie manuell konfigurieren, erweitern Sie im Navigationsbereich **Web App Firewall**, **Richtlinien**und dann **Firewall**. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Richtlinie zu erstellen. Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.

2. Klicken Sie auf dem Bildschirm **Regel angeben** im Dialogfeld **Web App Firewall App-Firewall-Profil erstellen** oder im Dialogfeld **Web App Firewall App-Firewall-Profil konfigurieren** auf **Präfix**, und wählen Sie dann das Präfix für Ihren Ausdruck aus der Dropdown-Liste aus. Ihre Auswahlmöglichkeiten:

   - **HTTP.** Wählen Sie ein HTTP-Protokoll aus, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das Protokoll bezieht.
   - **SYS.** Wählen Sie geschützte Websites aus, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - **CLIENT.** Wählen Sie einen Kunden aus, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - **SERVER.** Wählen Sie einen Kunden aus, an den die Anfrage gesendet wurde und ob Sie einen Aspekt des Empfängers der Anfrage untersuchen möchten.

   Nachdem Sie ein Präfix ausgewählt haben, zeigt die Web App Firewall ein zweiteiliges Eingabeaufforderungsfenster an, in dem oben die möglichen nächsten Optionen angezeigt werden, und eine kurze Erklärung, was die ausgewählte Auswahl unten bedeutet.

3. Wähle dein nächstes Semester.

   Wenn Sie das HTTP-Protokoll als Präfix gewählt haben, wählen Sie nur REQ, das das Request/Response-Paar angibt. (Die Web App Firewall arbeitet bei der Anfrage und Antwort als Einheit statt auf jeder separat.) Wenn Sie ein anderes Präfix gewählt haben, sind Ihre Auswahl

vielfältiger. Um Hilfe zu einer bestimmten Auswahl zu erhalten, klicken Sie einmal auf diese Auswahl, um Informationen darüber im unteren Eingabeaufforderungsfenster anzuzeigen.

Wenn Sie entschieden haben, welchen Begriff Sie möchten, doppelklicken Sie darauf, um ihn in das **Ausdrucksfenster** einzufügen.

4. Geben Sie einen Zeitraum nach dem gerade gewählten Term ein. Sie werden dann aufgefordert, Ihren nächsten Begriff zu wählen, wie im vorherigen Schritt beschrieben. Wenn für einen Begriff die Eingabe eines Wertes erforderlich ist, geben Sie den entsprechenden Wert ein. Wenn Sie beispielsweise HTTP.REQ.HEADER (“”) wählen, geben Sie den Kopfzeilennamen zwischen den Anführungszeichen ein.
5. Wählen Sie weiterhin Begriffe aus den Eingabeaufforderungen aus und geben Sie alle benötigten Werte ein, bis Ihr Ausdruck beendet ist.

   Im Folgenden finden Sie einige Beispiele für Ausdrücke für bestimmte Zwecke.

   - **Spezifischer Webhost.** So stimmen Sie den Datenverkehr von einem bestimmten Webhost ab:

     ```
     1 HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
     2 <!--NeedCopy-->
     ```

     Ersetzen Sie für `shopping.example.com`den Namen des Webhosts, den Sie abgleichen möchten.

   - **Bestimmter Webordner oder -verzeichnis.** So stimmen Sie den Datenverkehr aus einem bestimmten Ordner oder Verzeichnis auf einem Webhost ab:

     ```
     1 HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
     2 <!--NeedCopy-->
     ```

     Ersetzen Sie für www.example.com den Namen des Webhosts. Ersetzen Sie für den Ordner den Ordner oder Pfad zu dem Inhalt, den Sie abgleichen möchten. Wenn sich Ihr Warenkorb beispielsweise in einem Ordner namens /solutions/orders befindet, ersetzen Sie diese Zeichenfolge durch Ordner.

   - **Bestimmte Art von Inhalt: GIF-Bilder.** So passen Sie Bilder im GIF-Format an:

     ```
     1 HTTP.REQ.URL.ENDSWITH(".png")
     2 <!--NeedCopy-->
     ```

     Um Bilder in anderen Formaten zu entsprechen, ersetzen Sie anstelle von .png eine andere Zeichenfolge.

   - **Spezifischer Inhaltstyp: Skripts.** So passen Sie alle CGI-Skripts an, die sich im CGI-BIN-Verzeichnis befinden:


```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
<!--NeedCopy-->
```

Um alle JavaScript mit .js-Erweiterungen abzugleichen:

```
HTTP.REQ.URL.ENDSWITH(".js")
<!--NeedCopy-->
```

Weitere Informationen zum Erstellen von Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Wenn Sie die Befehlszeile zum Konfigurieren einer Richtlinie verwenden, denken Sie daran, doppelte Anführungszeichen in NetScaler-Ausdrücken zu umgehen. Der folgende Ausdruck ist beispielsweise korrekt, wenn er in die GUI eingegeben wird:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
<!--NeedCopy-->
```

Wenn Sie jedoch in der Befehlszeile eingegeben werden, müssen Sie stattdessen den folgenden Befehl eingeben:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
<!--NeedCopy-->
```

So fügen Sie eine Firewallregel (Ausdruck) mithilfe des Dialogfelds Ausdruck hinzufügen hinzu

Das Dialogfeld **Ausdruck hinzufügen** (auch als Ausdrucksеditor bezeichnet) hilft Benutzern, die mit der Sprache der NetScaler-Ausdrücke nicht vertraut sind, eine Richtlinie zu erstellen, die dem Datenverkehr entspricht, den sie filtern möchten.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie im **Web App Firewall-Assistenten** oder in der NetScaler GUI zum entsprechenden Speicherort:
   - Wenn Sie eine Richtlinie im **Web App Firewall-Assistenten** konfigurieren, klicken Sie im Navigationsbereich auf **Web App Firewall**, dann im Detailbereich auf **Web App Firewall Wizard**, und navigieren Sie dann zum Bildschirm „ **Regel angeben**“.
   - Wenn Sie eine Richtlinie manuell konfigurieren, erweitern Sie im Navigationsbereich **Web App Firewall**, **Richtlinien**und dann **Firewall**. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Richtlinie zu erstellen. Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.

2. Klicken Sie auf dem Bildschirm **Regel angeben** im Dialogfeld **Web App-Firewall-Profil erstellen** oder im Dialogfeld **Web App Firewall-Profil konfigurieren** auf **Hinzufügen**.
3. Wählen **Sie im Dialogfeld Ausdruck hinzufügen** im Bereich Ausdruck konstruieren im ersten Listenfeld eines der folgenden Präfixe aus:
   - **HTTP.** Wählen Sie das HTTP-Protokoll, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht. Die Standardauswahl.
   - **SYS.** Wählen Sie geschützte Websites aus, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - **CLIENT.** Wählen Sie den Computer aus, der die Anfrage gesendet hat, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - **SERVER.** Wählen Sie den Computer aus, an den die Anfrage gesendet wurde, und prüfen Sie einen Aspekt des Empfängers der Anfrage.
4. Wählen Sie im zweiten Listenfeld Ihren nächsten Begriff aus. Die verfügbaren Begriffe unterscheiden sich je nach Auswahl, die Sie im vorherigen Schritt getroffen haben, da das Dialogfeld die Liste automatisch so anpasst, dass sie nur die Begriffe enthält, die für den Kontext gültig sind. Wenn Sie beispielsweise im vorherigen Listenfeld HTTP ausgewählt haben, ist REQ für Anfragen die einzige Wahl. Da die Web App Firewall Anfragen und zugehörige Antworten als eine einzige Einheit behandelt und beide filtert, müssen Sie keine spezifischen Antworten separat eingehen. Nachdem Sie Ihren zweiten Begriff gewählt haben, erscheint rechts neben dem zweiten ein drittes Listenfeld. Im Hilfefenster wird eine Beschreibung des zweiten Begriffs angezeigt, und im Fenster **Vorschauausdruck** wird Ihr Ausdruck angezeigt.
5. Wählen Sie im dritten Listenfeld den nächsten Begriff aus. Rechts erscheint ein neues Listenfeld, und das Hilfefenster ändert sich, um eine Beschreibung des neuen Begriffs anzuzeigen. Das Fenster **Vorschauausdruck** wird aktualisiert, um den Ausdruck so anzuzeigen, wie Sie ihn bis zu diesem Zeitpunkt angegeben haben.
6. Wählen Sie weiterhin Begriffe aus und wenn Sie dazu aufgefordert werden, Argumente auszufüllen, bis Ihr Ausdruck vollständig ist. Wenn Sie einen Fehler machen oder Ihren Ausdruck ändern möchten, nachdem Sie bereits einen Begriff ausgewählt haben, können Sie einfach einen anderen Begriff wählen. Der Ausdruck wird geändert, und alle Argumente oder mehr Begriffe, die Sie nach dem von Ihnen geänderten Begriff hinzugefügt haben, werden gelöscht.
7. Wenn Sie mit der Erstellung Ihres Ausdrucks fertig sind, klicken Sie auf **OK**, um das Dialogfeld **Ausdruck hinzufügen** zu schließen. Ihr Ausdruck wird in den **Ausdruckstextbereich** eingefügt.

Verbindliche Web App Firewall-Richtlinien

May 11, 2023

Nachdem Sie Ihre Web App Firewall-Richtlinien konfiguriert haben, binden Sie sie an Global oder

einen Bindungspunkt, um sie in Kraft zu setzen. Nach dem Binden wird jede Anfrage oder Antwort, die einer Web App Firewall-Richtlinie entspricht, durch das dieser Richtlinie zugeordnete Profil transformiert.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf jede positive Ganzzahl festlegen. Im NetScaler OS funktionieren die Richtlinienprioritäten in umgekehrter Reihenfolge — je höher die Zahl, desto niedriger die Priorität.

Da die Web App Firewall-Funktion nur die erste Richtlinie implementiert, der eine Anforderung entspricht, und keine zusätzlichen Richtlinien, denen sie möglicherweise ebenfalls entspricht, ist die Richtlinienpriorität wichtig, um die von Ihnen beabsichtigten Ergebnisse zu erzielen. Wenn Sie Ihrer ersten Richtlinie eine niedrige Priorität zuweisen (z. B. 1000), konfigurieren Sie die Web App Firewall so, dass sie nur ausgeführt wird, wenn andere Richtlinien mit einer höheren Priorität keiner Anfrage entsprechen. Wenn Sie Ihrer ersten Richtlinie eine hohe Priorität einräumen (z. B. 1), konfigurieren Sie die Web App Firewall so, dass sie zuerst ausgeführt wird, und überspringen alle anderen Richtlinien, die möglicherweise ebenfalls übereinstimmen. Sie können sich viel Raum lassen, um andere Richtlinien in beliebiger Reihenfolge hinzuzufügen, ohne Prioritäten neu zuweisen zu müssen, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen jeder Richtlinie festlegen, wenn Sie Ihre Richtlinien binden.

Weitere Informationen zum Binden von Richtlinien auf der NetScaler Appliance finden Sie unter “Richtlinien und Ausdrücke. “

So binden Sie eine Web App Firewall Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw global <policyName>`
- `bind appfw profile <profile_name> -crossSiteScripting data`

Beispiel

Das folgende Beispiel bindet die Richtlinie mit dem Namen pl-blog und weist ihr die Priorität 10 zu.

```
1 bind appfw global pl-blog 10
2 save ns config
3 <!--NeedCopy-->
```

Logausdrücke konfigurieren

Die Unterstützung von Protokollausdrücken für die Bindung der Web App Firewall wurde hinzugefügt, um HTTP-Header-Informationen zu protokollieren, wenn ein Verstoß auftritt.

Der Protokollausdruck ist an das Anwendungsprofil gebunden, und die Bindung enthält den Ausdruck, der ausgewertet und an die Protokollierungs-Frameworks gesendet werden muss, wenn ein Verstoß auftritt.

Der Protokolldatensatz zur Verletzung der Web App Firewall mit HTTP-Header-Informationen wird aufgezeichnet. Sie können einen benutzerdefinierten Protokollausdruck angeben, der bei der Analyse und Diagnose hilft, wenn Verstöße für den aktuellen Flow (Anforderung/Antwort) generiert werden.

Beispiel-Konfiguration

```
bind appfw profile <profile> -logexpression <string> <expression>
add policy expression headers "" HEADERS(100):"+HTTP.REQ.FULL_HEADER"
add policy expression body_100 ""BODY:"+HTTP.REQ.BODY(100)"
bind appfw profile test -logExpression log_body body_100
bind appfw profile test -logExpression log_headers  headers
bind appfw profile test -logExpression ""URL:"+HTTP.REQ.URL+" IP:"+
    CLIENT.IP.SRC"
<!--NeedCopy-->
```

Beispielprotokolle

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg= HEADERS(100)
    :POST /test/credit.html HTTP/1.1^M User-Agent: curl/7.24.0 (amd64-
    portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Host:
     10.217.222.44^M Accept: /^M Content-Length: 33^M Content-Type:
    application/x-www-form-urlencoded^M ^M  cn1=58 cn2=174 cs1=test cs2=
    PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=BODY:ata=
    asdadasdasdasddddddddddddddddd cn1=59 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=URL:/test/
    credit.html IP:10.217.222.128 cn1=60 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
```



```
<!--NeedCopy-->
```

```
Other violation logs
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_STARTURL|6|src=10.217.222.128 spt=26409 method=POST
    request=http://10.217.222.44/test/credit.html msg=Disallow Illegal
    URL. cn1=61 cn2=174 cs1=test cs2=PPE1 cs4=ALERT cs5=2017 act=not
    blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_SAFECOMMERCE|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=Maximum
    number of potential credit card numbers seen cn1=62 cn2=174 cs1=test
     cs2=PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

Hinweis

1. Es ist nur Auditlog-Unterstützung verfügbar. Unterstützung für Logstream und Visibility in Security Insight würden in zukünftigen Release-Versionen hinzugefügt.
2. Wenn Auditlogs generiert werden, können pro Lognachricht nur 1024 Byte an Daten generiert werden.
3. Wenn Log-Streaming verwendet wird, basieren die Grenzwerte auf der maximal unterstützten Größe des Log-Streams/den IPFIX-Protokollgrößenbeschränkungen. Die maximale Unterstützungsgröße für den Log-Stream ist größer als 1024 Byte.

So binden Sie eine Web App Firewall-Richtlinie mithilfe der GUI

1. Führen Sie einen der folgenden Schritte aus:
   - Navigieren Sie zu **Sicherheit** > **Web App Firewall**und klicken Sie im Detailbereich auf Web App Firewall Policy Manager.
   - Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Richtlinien** > **Firewall-Richtlinien**und klicken Sie im Detailbereich auf **Policy Manager**.
2. Wählen Sie im Dialogfeld **Web App Firewall Policy Manager** aus der Dropdownliste den Bindungspunkt aus, an den Sie die Richtlinie binden möchten. Es stehen folgende Optionen zur Auswahl:
   - **Global überschreiben.** Richtlinien, die an diesen Bindpunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen auf der NetScaler-Appliance und werden vor allen anderen Richtlinien angewendet.

- **LB Virtueller Server.** Richtlinien, die an einen virtuellen Lastausgleichsserver gebunden sind, werden nur auf den Datenverkehr angewendet, der von diesem virtuellen Lastausgleichsserver verarbeitet wird, und sie werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie LB Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Load-Balancing-Server auswählen, an den Sie diese Richtlinie binden möchten.
- **CS Virtueller Server.** Richtlinien, die an einen virtuellen Content Switching-Server gebunden sind, werden nur auf den Datenverkehr angewendet, der von diesem virtuellen Content Switching-Server verarbeitet wird, und sie werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie CS Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Content Switching-Server auswählen, an den Sie diese Richtlinie binden möchten.
- **Standard Global.** Richtlinien, die an diesen Bindpunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der NetScaler-Appliance.
- **Richtlinien-Etikett.** Richtlinien, die an ein Richtlinienlabel gebunden sind, verarbeiten den Datenverkehr, den das Richtlinienlabel an sie weiterleitet. Das Richtlinienlabel bestimmt die Reihenfolge, in der Richtlinien auf diesen Verkehr angewendet werden.
- **Keine.** Binden Sie die Richtlinie an keinen Bindungspunkt.

3. Klicken Sie auf **Weiter**. Eine Liste der vorhandenen Web App Firewall-Richtlinien wird angezeigt.
4. Wählen Sie die Richtlinie aus, die Sie binden möchten, indem Sie darauf klicken.
5. Nehmen Sie weitere Anpassungen an der Bindung vor.
   - Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten neu generieren auswählen, um die Prioritäten gleichmäßig neu zu nummerieren.
   - Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld **Web App Firewall-Richtlinie konfigurieren** zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.
   - Um den Goto-Ausdruck festzulegen, doppelklicken Sie auf das **Feld** in der Spaltenüberschrift Goto Expression, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
   - Um die Option Aufrufen festzulegen, doppelklicken Sie in der Spaltenüberschrift Aufrufen auf das Feld, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können
6. Wiederholen Sie die Schritte 3 bis 6, um weitere Web App Firewall-Richtlinien hinzuzufügen, die Sie global binden möchten.
7. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich gebunden wurde.

Die Bindungen einer Richtlinie anzeigen

May 11, 2023

Sie können schnell überprüfen, welche Bindungen für jede Firewall-Richtlinie vorhanden sind, indem Sie sich die Bindungen in der GUI ansehen.

So sehen Sie sich Bindungen für eine Web App Firewall-Richtlinie an

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Richtlinien > Firewall-Richtlinien**
2. Wählen Sie im Detailbereich die Richtlinie aus, die Sie überprüfen möchten, und klicken Sie dann auf Bindungen anzeigen. Das Meldungsfeld Binding Details for Policy: Policy wird mit einer Liste der Bindungen für die ausgewählte Richtlinie angezeigt.
3. Klicken Sie auf **Schließen**.

Zusätzliche Informationen zu den Web App Firewall-Richtlinien

May 11, 2023

Im Folgenden finden Sie zusätzliche Informationen zu bestimmten Aspekten der Web App Firewall-Richtlinien, die Systemadministratoren, die die Web App Firewall verwalten, möglicherweise kennen müssen.

Richtiges, aber unerwartetes Verhalten

Die Sicherheit von Webanwendungen und moderne Websites sind komplex. In einer Reihe von Szenarien kann eine NetScaler-Richtlinie dazu führen, dass sich die Web App Firewall in bestimmten Situationen anders verhält, als es ein Benutzer, der mit Richtlinien vertraut ist, normalerweise erwarten würde. Im Folgenden sind eine Reihe von Fällen aufgeführt, in denen sich die Web App Firewall unerwartet verhalten kann.

- **Anfrage mit einem fehlenden HTTP-Host-Header und einer absoluten URL.** Wenn ein Benutzer eine Anfrage sendet, ist die Anforderungs-URL in den meisten Fällen relativ. Das heißt, als Ausgangspunkt wird die Referer-URL verwendet, die URL, unter der sich der Browser des Benutzers befindet, wenn er die Anfrage sendet. Wenn eine Anfrage ohne Host-Header und mit einer relativen URL gesendet wird, wird die Anfrage normalerweise blockiert, sowohl weil sie gegen die HTTP-Spezifikation verstößt als auch weil eine Anfrage, die den Host nicht angibt, unter bestimmten Umständen einen Angriff darstellen kann. Wenn jedoch eine Anfrage mit

einer absoluten URL gesendet wird, auch wenn der Host-Header fehlt, umgeht die Anfrage die Web App Firewall und wird an den Webserver weitergeleitet. Obwohl eine solche Anforderung gegen die HTTP-Spezifikation verstößt, stellt sie keine mögliche Bedrohung dar, da eine absolute URL den Host enthält.

Richtlinien für die Prüfung

May 11, 2023

Überwachungsrichtlinien bestimmen, welche Nachrichten während einer Web App Firewall-Sitzung generiert und protokolliert werden. Die Nachrichten werden im SYSLOG-Format auf dem lokalen NSLOG-Server oder auf einem externen Protokollierungsserver protokolliert. Je nach der ausgewählten Protokollierungsstufe werden verschiedene Arten von Nachrichten protokolliert.

Um eine Überwachungsrichtlinie zu erstellen, müssen Sie zunächst entweder einen NSLOG-Server oder einen SYSLOG-Server erstellen. Anschließend erstellen Sie die Richtlinie und geben den Protokolltyp und den Server an, an den die Protokolle gesendet werden.

So erstellen Sie einen Auditing-Server mithilfe der Befehlszeilenschnittstelle

Sie können zwei verschiedene Arten von Überwachungsservern erstellen: einen NSLOG-Server oder einen SYSLOG-Server. Die Befehlsnamen sind unterschiedlich, aber die Parameter für die Befehle sind dieselben.

Um einen Auditing-Server zu erstellen, geben Sie an der Befehlszeile die folgenden Befehle ein:

- `add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird ein Syslog-Server mit dem Namen syslog1 an der IP 10.124.67.91 erstellt, wobei die Protokollstufen Notfall, Kritisch und Warnung, Log Facility auf LOCAL1 gesetzt sind, der alle TCP-Verbindungen protokolliert:

```
1 add audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning -logFacility
```



```
2 LOCAL1 -tcp ALL
3 save ns config
4 <!--NeedCopy-->
```

So ändern oder entfernen Sie einen Überwachungsserver mithilfe der Befehlszeilenschnittstelle

- Um einen Überwachungsserver zu ändern, geben Sie den <type> Befehl set audit, den Namen des Überwachungsservers und die zu ändernden Parameter mit ihren neuen Werten ein.
- Um einen Überwachungsserver zu entfernen, geben Sie den <type> Befehl rm audit und den Namen des Überwachungsservers ein.

Beispiel

Im folgenden Beispiel wird der Syslog-Server mit dem Namen syslog1 geändert, um Fehler und Warnungen zur Protokollebene hinzuzufügen:

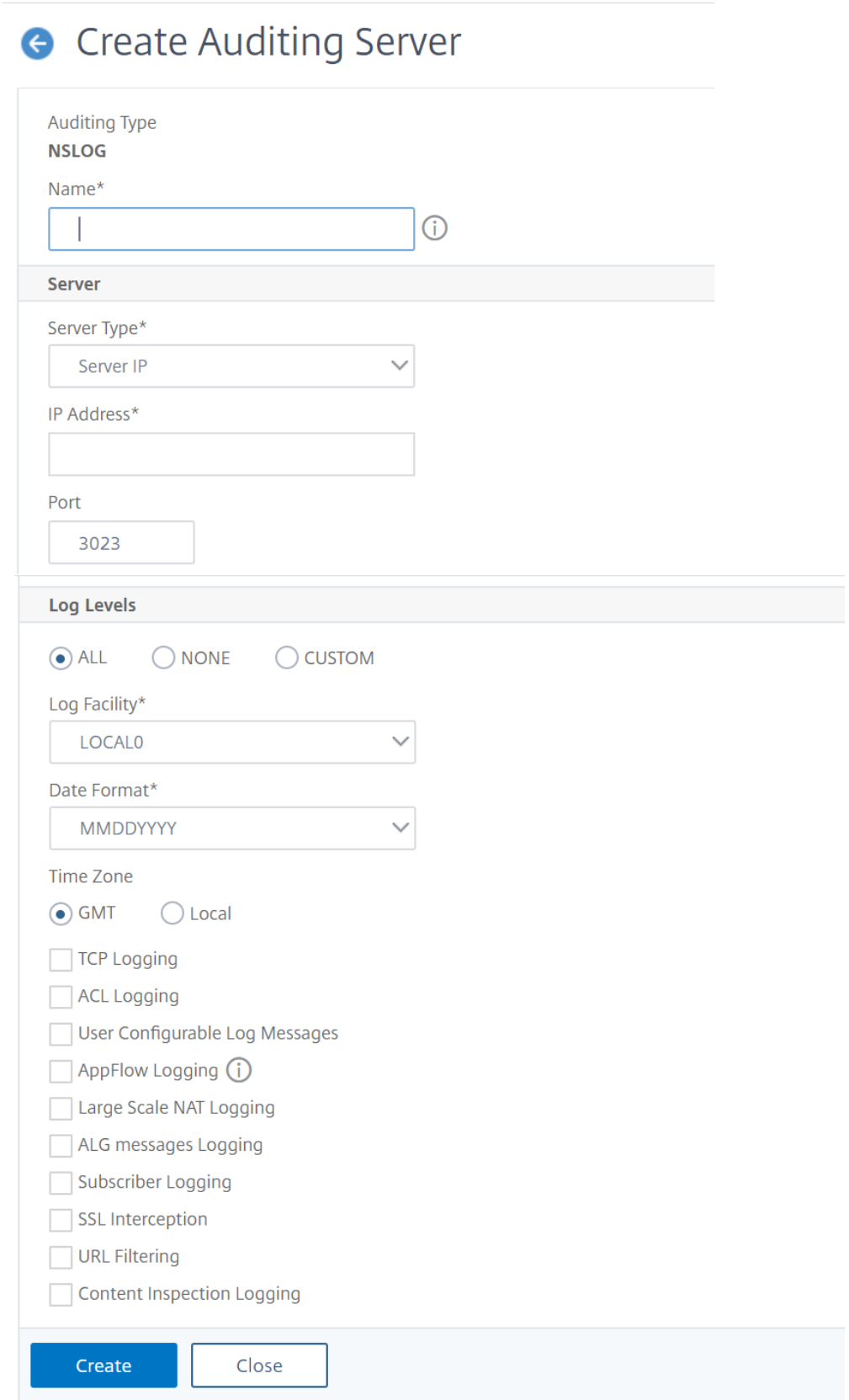
```
1 set audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning alert error
2 -logFacility LOCAL1 -tcp ALL
3 save ns config
4 <!--NeedCopy-->
```

So erstellen oder konfigurieren Sie einen Auditing-Server mithilfe der GUI

1. **Navigieren Sie zu**Sicherheit**>**NetScaler Web App Firewall**>**Richtlinien**>**Auditing**> Nslog.**
2. **Klicken Sie auf der Seite Nslog Auditing auf die Registerkarte Server.**
3. Führen Sie einen der folgenden Schritte aus:
   - Um einen neuen Auditing-Server hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen Überwachungsserver zu ändern, wählen Sie den Server aus, und klicken Sie dann auf **Bearbeiten**.
4. Stellen Sie auf der Seite „ **Auditing-Server erstellen** “ die folgenden Parameter ein:
   - Name
   - Server-Typ
   - IP-Adresse
   - Port
   - Ebenen protokollieren
   - Einrichtung zur Protokollierung

- Datumsformat
- Zeitzone
- TCP-Protokollierung
- ACL-Protokollierung
- Vom Benutzer konfigurierbare Protokollmeldungen
- AppFlow-Protokollierung
- NAT-Protokollierung in großem Maßstab
- Protokollierung von ALG-Nachrichten
- Abonnentenprotokollierung
- SSL-Abfangen
- URL-Filterung
- Protokollierung der Inhaltsprüfung

5. Klicken Sie auf **Erstellen** und **Schließen**.



So erstellen Sie mithilfe der Befehlszeilenschnittstelle eine Überwachungsrichtlinie

Sie können eine NSLOG-Richtlinie oder eine SYSLOG-Richtlinie erstellen. Der Typ der Richtlinie muss dem Servertyp entsprechen. Die Befehlsnamen für die beiden Richtlinientypen sind unterschiedlich, aber die Parameter für die Befehle sind dieselben.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add audit syslogPolicy <name> <-rule > <action>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird eine Richtlinie mit dem Namen syslogP1 erstellt, die den Web App Firewall-Verkehr auf einem Syslog-Server mit dem Namen syslog1 protokolliert.

```
add audit syslogPolicy syslogP1 rule "ns_true"action syslog1
save ns config
```

So konfigurieren Sie eine Überwachungsrichtlinie mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set audit syslogPolicy <name> [-rule <expression>] [-action <string>]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird die Richtlinie mit dem Namen syslogP1 geändert, um den Web App Firewall-Verkehr auf einem Syslog-Server namens syslog2 zu protokollieren.

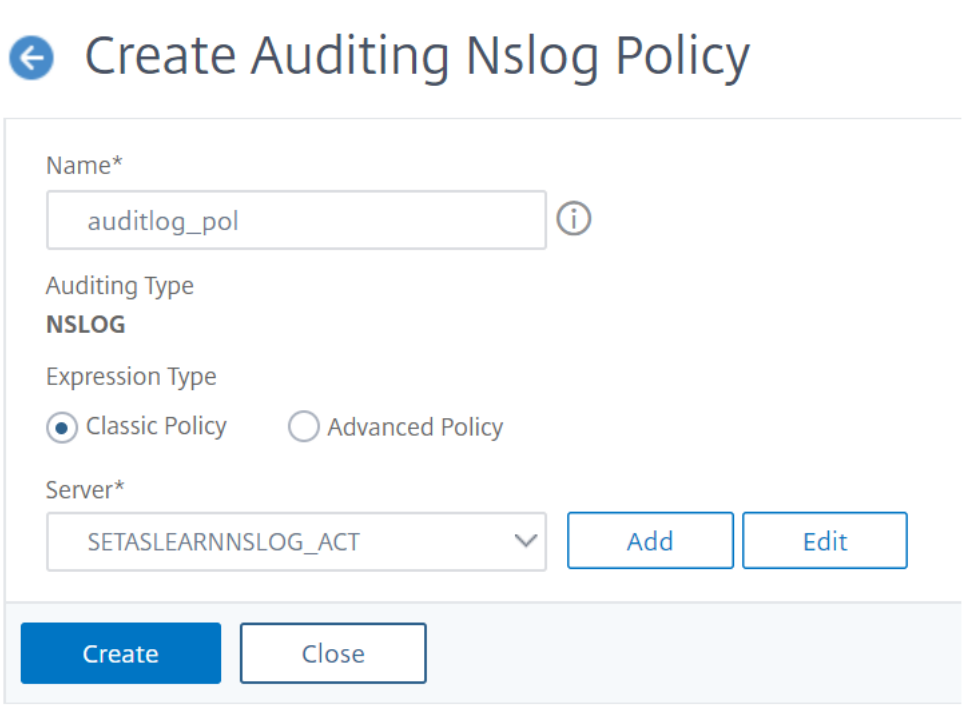
```
set audit syslogPolicy syslogP1 rule "ns_true"action syslog2
save ns config
```

So konfigurieren Sie eine Überwachungsrichtlinie mithilfe der GUI

1. Navigieren Sie zu **Sicherheit** > **NetScaler Web App Firewall** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Audit Nslog Policy**.
3. Klicken Sie auf der Seite Nslog Auditing auf **die Registerkarte Richtlinien** und führen Sie einen der folgenden Schritte aus:
    - Um eine neue Richtlinie hinzuzufügen, klicken Sie auf **Hinzufügen**.

- Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus und klicken dann auf **Bearbeiten**.

4. Stellen Sie auf der Seite „ **Auditing-NSlog-Richtlinie erstellen** “ die folgenden Parameter ein:
   - Name
   - Art der Prüfung
   - Ausdruck-Typ
   - Server
5. Klicken Sie auf **Erstellen**.



Importe

May 11, 2023

Verschiedene Funktionen der Web App Firewall verwenden externe Dateien, die Sie bei der Konfiguration in die Web App Firewall hochladen. Mithilfe der GUI verwalten Sie diese Dateien im Bereich Importe, der vier Registerkarten enthält, die den vier Dateitypen entsprechen, die Sie importieren können: HTML-Fehlerobjekte, XML-Fehlerobjekte, XML-Schemas und WSDL-Dateien (Web Services Description Language). Mit der NetScaler-Befehlszeile können Sie diese Dateitypen importieren, aber Sie können sie nicht exportieren.

HTML-Fehlerobjekt

Wenn die Verbindung eines Benutzers zu einer HTML- oder Web 2.0-Seite blockiert wird oder ein Benutzer nach einer nicht vorhandenen HTML- oder Web 2.0-Seite fragt, sendet die Web App Firewall eine HTML-basierte Fehlerantwort an den Browser des Benutzers. Bei der Konfiguration, welche Fehlerantwort die Web App Firewall verwenden muss, haben Sie zwei Möglichkeiten:

- Sie können eine Umleitungs-URL konfigurieren, die auf jedem Webserver gehostet werden kann, auf den Benutzer auch Zugriff haben. Wenn Sie beispielsweise eine benutzerdefinierte Fehlerseite auf Ihrem Webserver haben, 404.html, können Sie die Web App Firewall so konfigurieren, dass Benutzer auf diese Seite umgeleitet werden, wenn eine Verbindung blockiert wird.
- Sie können ein HTML-Fehlerobjekt konfigurieren, bei dem es sich um eine HTML-basierte Webseite handelt, die auf der Web App Firewall selbst gehostet wird. Wenn Sie diese Option wählen, müssen Sie das HTML-Fehlerobjekt in die Web App Firewall hochladen. Dies tun Sie im Bereich Importe auf der Registerkarte HTML-Fehlerobjekt.

Das Fehlerobjekt muss eine Standard-HTML-Datei sein, die außer den Anpassungsvariablen für das Web App Firewall-Fehlerobjekt keine Nicht-HTML-Syntax enthält. Es kann keine CGI-Skripts, serveranalysierten Code oder PHP-Code enthalten. Die Anpassungsvariablen ermöglichen es Ihnen, Informationen zur Fehlerbehebung in das Fehlerobjekt einzubetten, das der Benutzer erhält, wenn eine Anfrage blockiert wird. Die meisten Anfragen, die die Web App Firewall blockiert, sind zwar illegitim, aber selbst eine ordnungsgemäß konfigurierte Web App Firewall kann gelegentlich legitime Anfragen blockieren, insbesondere wenn Sie sie zum ersten Mal bereitstellen oder nachdem Sie erhebliche Änderungen an Ihren geschützten Websites vorgenommen haben. Durch das Einbetten von Informationen in die Fehlerseite stellen Sie dem Benutzer die Informationen zur Verfügung, die er dem technischen Support geben muss, damit alle Probleme behoben werden können.

Die Variablen zur Anpassung der Web App Firewall-Fehlerseite lauten wie folgt:

- $ {NS_TRANSACTION_ID}. Die Transaktions-ID, die die Web App Firewall dieser Transaktion zugewiesen hat.
- $ {NS_APPFW_SESSION_ID}. Die Web App Firewall-Sitzungs-ID.
- $ {NS_APPFW_VIOLATION_CATEGORY}. Die spezifische Sicherheitsüberprüfung oder Regel der Web App Firewall, gegen die verstoßen wurde.
- $ {NS_APPFW_VIOLATION_LOG}. Die detaillierte Fehlermeldung im Zusammenhang mit dem Verstoß.
- $ {Cookie Der Inhalt des angegebenen Cookies. Ersetzen Sie durch den Namen des spezifischen Cookie, das Sie auf der Fehlerseite anzeigen möchten. <CookieName> Wenn Sie mehrere Cookies haben, deren Inhalt Sie zur Fehlerbehebung anzeigen möchten, können Sie mehrere Instanzen dieser Anpassungsvariablen verwenden, jeweils mit dem entsprechenden Cookie-

Namen.

Hinweis: Wenn Sie das Blockieren für die Cookie-Konsistenzprüfung aktiviert haben, werden blockierte Cookies nicht auf der Fehlerseite angezeigt, da die Web App Firewall sie blockiert.

Um diese Variablen zu verwenden, betten Sie sie in den HTML- oder XML-Code des Fehlerseitenobjekts ein, als ob es sich um eine normale Textzeichenfolge handeln würde. Wenn das Fehlerobjekt dem Benutzer angezeigt wird, ersetzt die Web App Firewall für jede Anpassungsvariable die Informationen, auf die sich die Variable bezieht. Ein Beispiel für eine HTML-Fehlerseite, die benutzerdefinierte Variablen verwendet, ist unten dargestellt.

```
<!doctype html public "-//w3c//dtd html 4.0//en"> <html> <head> <
   title>Page Not Accessible</title> </head> <body> <h1>Page Not
   Accessible</h1> <p>The page that you accessed is not available. You
    can:</p> <ul> <li>return to the <b><a href="[homePage]">home page
   </a></b>, re-establish your session, and try again, or,</li> <li>
   report this incident to the help desk via <b><a href="mailto:[
   helpDeskEmailAddress]">email</a></b> or by calling [
   helpDeskPhoneNumber].</li> </ul> <p>If you contact the help desk,
   please provide the following information:</p> <table cellpadding=8
   width=80%> <tr><th align="right" width=30%>Transaction ID:</th><td
   align="left" valign="top" width=70%>${
 NS_TRANSACTION_ID }
 </td></tr> <tr><th align="right" width=30%>Session ID:</th><td align=
    "left" valign="top" width=70%>${
 NS_APPFW_SESSION_ID }
 </td></tr> <tr><th align="right" width=30%>Violation Category:</th><
    td align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_CATEGORY }
 </td></tr> <tr><th align="right" width=30%>Violation Log:</th><td
    align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_LOG }
 </td></tr> <tr><th align="right" width=30%>Cookie Name:</th><td align
    ="left" valign="top" width=70%>${
 COOKIE("[cookieName]") }
 </td></tr> </table> <body> <html>
<!--NeedCopy-->
```

Um diese Fehlerseite zu verwenden, kopieren Sie sie in einen Text- oder HTML-Editor. Ersetzen Sie die folgenden Variablen durch die entsprechenden lokalen Informationen, die in eckigen Klammern stehen, um sie von den NetScaler-Variablen zu unterscheiden. (Lassen Sie diese unverändert.):

- `[homePage]`. Die URL für die Homepage Ihrer Website.
- `[helpDeskEmailAddress]`. Die E-Mail-Adresse, die Benutzer verwenden sollen, um Blockiervorfälle zu melden.

- `[helpDeskPhoneNumber]`. Die Telefonnummer, die Benutzer anrufen sollen, um Blockiervorfälle zu melden.
- `[cookieName]`. Der Name des Cookie, dessen Inhalt Sie auf der Fehlerseite anzeigen möchten.

XML-Fehlerobjekt

Wenn die Verbindung eines Benutzers zu einer XML-Seite blockiert wird oder ein Benutzer nach einer nicht existierenden XML-Anwendung fragt, sendet die Web App Firewall eine XML-basierte Fehlerantwort an den Browser des Benutzers. Sie konfigurieren die Fehlerantwort, indem Sie im Bereich Importe auf der Registerkarte XML-Fehlerobjekt eine XML-basierte Fehlerseite in die Web App Firewall hochladen. Alle XML-Fehlerantworten werden auf der Web App Firewall gehostet. Sie können keine Umleitungs-URL für XML-Anwendungen konfigurieren.

> **Hinweis**:
> Sie können in einem XML-Fehlerobjekt dieselben Anpassungsvariablen wie in einem HTML-Fehlerobjekt verwenden.

XML-Schema

Wenn die Web App Firewall eine Validierungsprüfung für die Anfrage eines Benutzers für eine XML- oder Web 2.0-Anwendung durchführt, kann sie die Anforderung anhand des XML-Schemas oder des Design Type Document (DTD) für diese Anwendung validieren und jede Anforderung ablehnen, die nicht dem Schema oder der DTD entspricht. Sowohl ein XML-Schema als auch eine DTD sind Standard-XML-Konfigurationsdateien, die die Struktur eines bestimmten XML-Dokumenttyps beschreiben.

WSDL

Wenn die Web App Firewall eine Validierungsprüfung für die Anfrage eines Benutzers für einen XML-SOAP-basierten Webdienst durchführt, kann sie die Anforderung anhand der Web Services Type Definitionsdatei (WSDL) für diesen Webdienst validieren. Eine WSDL-Datei ist eine standardmäßige XML-SOAP-Konfigurationsdatei, die die Elemente eines bestimmten XML-SOAP-Webdienstes definiert.

Dateien importieren und exportieren

May 11, 2023

Sie können HTML- oder XML-Fehlerobjekte, XML-Schemas, DTDs und WSDLs mithilfe der GUI oder der Befehlszeile in die Web App Firewall importieren. Sie können jede dieser Dateien nach dem Import in einem webbasierten Textbereich bearbeiten, um kleine Änderungen direkt auf dem NetScaler

vorzunehmen, anstatt sie auf Ihrem Computer vornehmen und dann erneut importieren zu müssen. Schließlich können Sie mithilfe der GUI jede dieser Dateien auf Ihren Computer exportieren oder diese Dateien löschen.

> **Hinweis:**
>
> Sie können eine importierte Datei nicht mithilfe der Befehlszeile löschen oder exportieren.

So importieren Sie eine Datei mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `import appfw htmlerrorpage <src> <name>`
- `<save> ns config`

Beispiel

Im folgenden Beispiel wird ein HTML-Fehlerobjekt aus einer Datei namens error.html importiert und ihm der Name HtmlError zugewiesen.

```
1 import htmlerrorpage error.html HTMLError
2 save ns config
3 <!--NeedCopy-->
```

Um eine Datei mit der GUI zu importieren

Bevor Sie versuchen, ein XML-Schema, eine DTD- oder WSDL-Datei oder ein HTML- oder XML-Fehlerobjekt von einem Netzwerkspeicherort zu importieren, stellen Sie sicher, dass der NetScaler eine Verbindung zum Internet- oder LAN-Computer herstellen kann, auf dem sich die Datei befindet. Andernfalls können Sie die Datei oder das Objekt nicht importieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Importe**.
2. Navigieren Sie zu **Application Firewall** > **Importe**.
3. Wählen Sie im Bereich **Application Firewall-Importe** die Registerkarte für den Dateityp aus, den Sie importieren möchten, und klicken Sie dann auf **Hinzufügen**.

   Die Registerkarten lauten HTML-Fehlerseite, XML-Fehlerseite, XML-Schema oder WSDL. Der Upload-Vorgang ist aus Benutzersicht auf allen vier Tabs identisch.
4. Füllen Sie die Dialogfelder aus.
   - **Name**— Ein Name für das importierte Objekt.
   - **Importieren von**— Wählen Sie in der Dropdownliste den Speicherort der HTML-Datei, der XML-Datei, des XML-Schemas oder der WSDL aus, die Sie importieren möchten:

- **URL:** Eine Web-URL auf einer Website, auf die die Appliance zugreifen kann.
- **Datei:** Eine Datei auf einer lokalen oder Netzwerkfestplatte oder einem anderen Speichergerät.
- **Text:** Geben Sie den Text der benutzerdefinierten Antwort direkt in ein Textfeld in der GUI ein oder fügen Sie ihn ein.

Das dritte Textfeld ändert sich in den entsprechenden Wert. Die drei möglichen Werte sind unten angegeben.

- **URL**— Geben Sie die URL in das Textfeld ein.
- **Datei**— Geben Sie den Pfad und den Dateinamen der HTML-Datei direkt ein, oder klicken Sie auf Durchsuchen und suchen Sie nach der HTML-Datei.
- **Text**— Das dritte Feld wird entfernt, sodass ein Leerzeichen übrig bleibt.

5. Klicken Sie auf **Weiter**. Das Dialogfeld „Dateiinhalt“ wird angezeigt. Wenn Sie URL oder Datei ausgewählt haben, enthält das Textfeld Dateiinhalt die von Ihnen angegebene HTML-Datei. Wenn Sie Text ausgewählt haben, ist das Textfeld Dateiinhalt leer.
6. Wenn Sie Text ausgewählt haben, geben Sie den benutzerdefinierten Antwort-HTML-Code ein, den Sie importieren möchten, oder kopieren Sie ihn und fügen Sie ihn ein.
7. Klicken Sie auf **Fertig**.
8. Um ein Objekt zu löschen, wählen Sie das Objekt aus, und klicken Sie dann auf **Löschen**.

Um eine Datei mit der GUI zu exportieren

Bevor Sie versuchen, ein XML-Schema, eine DTD- oder WSDL-Datei oder ein HTML- oder XML-Fehlerobjekt zu exportieren, stellen Sie sicher, dass die Web App Firewall Appliance auf den Computer zugreifen kann, auf dem die Datei gespeichert werden soll. Andernfalls können Sie die Datei nicht exportieren.

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Importe**.
2. Wählen Sie im Bereich **Web App Firewall-Importe** die Registerkarte für den Dateityp aus, den Sie exportieren möchten.

   Der Exportvorgang ist aus Benutzersicht auf allen vier Tabs identisch.
3. Wählen Sie die Datei aus, die Sie exportieren möchten.
4. Erweitern Sie die Dropdownliste Aktion und wählen Sie **Exportieren**aus.
5. Wählen Sie im Dialogfeld **Datei speichern** und klicken Sie auf **OK**.
6. Navigieren **Sie im Dialogfeld Durchsuchen** zu dem lokalen Dateisystem und Verzeichnis, in dem Sie die exportierte Datei speichern möchten, und klicken Sie auf **Speichern**.

So bearbeiten Sie ein HTML- oder XML-Fehlerobjekt in der GUI

Sie bearbeiten den Text von HTML- und XML-Fehlerobjekten in der GUI, ohne sie zu exportieren und dann erneut zu importieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Importe**und wählen Sie dann die Registerkarte für den Dateityp aus, den Sie ändern möchten.
2. Navigieren Sie zu **Application Firewall** > **Importe**und wählen Sie dann die Registerkarte für den Dateityp aus, den Sie ändern möchten.
3. Wählen Sie die Datei aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

   Der Text des HTML- oder XML-Fehlerobjekts wird in einem Browser-Textbereich angezeigt. Sie können den Text ändern, indem Sie die standardmäßigen browserbasierten Bearbeitungstools und -methoden für Ihren Browser verwenden.

   Hinweis: Das Bearbeitungsfenster ist so konzipiert, dass Sie kleinere Änderungen an Ihrem HTML- oder XML-Fehlerobjekt vornehmen können. Um umfangreiche Änderungen vorzunehmen, ziehen Sie es möglicherweise vor, das Fehlerobjekt auf Ihren lokalen Computer zu exportieren und Standardtools zur Bearbeitung von HTML- oder XML-Webseiten zu verwenden.
4. Klicken Sie auf **OK**und dann auf **Schließen**.

Globale Konfiguration

January 19, 2021

Die globale Konfiguration der Web App Firewall wirkt sich auf alle Profile und Richtlinien aus. Die globalen Konfigurationselemente sind:

- **Motoreinstellungen.** Eine Sammlung globaler Einstellungen — Name des Sitzungscookies, Sitzungszeitüberschreitung, maximale Sitzungslebensdauer, Protokollkopfname, undefiniertes Profil, Standardprofil und Importgrößenbeschränkung —, die sich auf alle Verbindungen beziehen, die die Web App Firewall verarbeitet, anstatt auf eine bestimmte Teilmenge von Verbindungen.
- **Vertrauliche Felder.** Eine Reihe von Formularfeldern in Webformularen, die vertrauliche Informationen enthalten, die nicht in den Web App Firewall -Protokollen protokolliert werden dürfen. Formularfelder wie Kennwortfelder auf einer Anmeldeseite oder Kreditkartendaten in einem Warenkorb-Bestellformular werden normalerweise als vertrauliche Felder bezeichnet.
- **Feldtypen.** Die Liste der Webformularfeldtypen, die von der Sicherheitsprüfung Feldformate verwendet werden. Jeder dieser Feldtypen wird durch einen PCRE-konformen regulären Aus-

druck definiert, der den Datentyp und die minimale/maximale Länge der Daten definiert, die in diesem Formularfeldtyp zulässig sein müssen.

- **XML-Inhaltstypen.** Die Liste der Inhaltstypen, die als XML erkannt und XML-spezifischen Sicherheitsprüfungen unterzogen wurden. Jeder dieser Inhaltstypen wird durch einen PCRE-kompatiblen regulären Ausdruck definiert, der den exakten MIME-Typ definiert, der diesem Inhalt zugewiesen ist.
- **JSON-Inhaltstypen.** Die Liste der Inhaltstypen, die als JSON erkannt und JSON-spezifischen Sicherheitsprüfungen unterzogen wurden. Jeder dieser Inhaltstypen wird durch einen PCRE-kompatiblen regulären Ausdruck definiert, der den exakten MIME-Typ definiert, der diesem Inhalt zugewiesen ist.

Motoreinstellungen

May 11, 2023

Die Engine-Einstellungen wirken sich auf alle Anfragen und Antworten aus, die die NetScaler Web App Firewall verarbeitet. Im Folgenden sind die Einstellungen aufgeführt:

- **Cookie-Name**— Der Name des Cookies, das die NetScaler-Sitzungs-ID speichert.
- **Sitzungs-Timeout**— Die maximal zulässige Inaktivitätsdauer. Wenn eine Benutzersitzung für diesen Zeitraum keine Aktivität zeigt, wird die Sitzung beendet und der Benutzer muss sie wiederherstellen, indem er eine bestimmte Startseite aufruft.
- **Präfix für nachverschlüsselte Cookies**— Die Zeichenfolge, die dem verschlüsselten Teil aller verschlüsselten Cookies vorangeht.
- **Maximale Sitzungsdauer**— Die maximale Zeit in Sekunden, für die eine Sitzung live bleiben darf. Nach Ablauf dieses Zeitraums wird die Sitzung beendet und der Benutzer muss sie wiederherstellen, indem er eine bestimmte Startseite aufruft. Diese Einstellung darf nicht kleiner als das Sitzungs-Timeout sein. Um diese Einstellung zu deaktivieren, sodass es keine maximale Sitzungsdauer gibt, setzen Sie den Wert auf Null (0).
- **Name des Logging-Headers**— Der Name des HTTP-Headers, der die Client-IP für die Protokollierung enthält.
- **Undefiniertes Profil**— Das Profil, das angewendet wird, wenn die entsprechende politische Aktion als undefiniert bewertet wird.
- **Standardprofil**— Das Profil wird auf Verbindungen angewendet, die keiner Richtlinie entsprechen.
- **Importgrößenbeschränkung**— Die maximale Bytezahl aller in die Appliance importierten Dateien, einschließlich Signaturen, WSDLs, Schemas, HTML- und XML-Fehlerseiten. Wenn während eines Imports die Größe des importierten Objekts dazu führt, dass die Gesamtzahl aller importierten Dateien den konfigurierten Grenzwert überschreitet, schlägt der Im-

portvorgang fehl. Und die Appliance zeigt die folgende Fehlermeldung an: "*FEHLER: Import fehlgeschlagen — Überschreitung der konfigurierten Gesamtgrößenbeschränkung für die importierten Objekte*".

- **Begrenzung der Lernnachrichtenrate**— Die maximale Anzahl von Anfragen und Antworten pro Sekunde, die die Lernmaschine verarbeiten soll. Zusätzliche Anfragen oder Antworten, die dieses Limit überschreiten, werden nicht an die Learning Engine gesendet.
- **Proxyserver** - Ein Proxyserver ist ein Zwischenserver, der im Namen des Benutzers Daten aus dem Internet abruft. Es bietet eine zusätzliche Sicherheitsebene für Ihre Appliance. Die NetScaler-Appliance, für die die Proxyauthentifizierung aktiviert ist, authentifiziert sich beim Proxyserver, bevor sie die Updates aus dem Internet herunterlädt. Auf diese Weise werden die Appliances vor bösartigen Downloads geschützt. Konfigurieren Sie die folgenden Parameter:
  - **Proxyserver** — Die IP-Adresse des Proxyservers, von dem die neuesten AWS-Signaturen heruntergeladen werden.
  - **Proxyport** — Die Portnummer des Proxyservers, von dem die neuesten AWS-Signaturen heruntergeladen werden.
  - **Proxy-Benutzername** — Die Portnummer des Proxyservers, von dem die neuesten AWS-Signaturen heruntergeladen werden.
  - **Proxykennwort** — Passwort zur Authentifizierung beim Proxyserver zum Herunterladen von Signaturupdates.
- **Entitätsdekodierung**— Dekodieren Sie HTML-Entitäten, wenn Sie Web App Firewall-Prüfungen ausführen.
- **Fehlerhafte Anfrage protokollieren**— Aktiviert die Protokollierung von falsch formatierten HTTP-Anfragen.
- **Konfigurierbaren geheimen Schlüssel verwenden**— Verwenden Sie einen konfigurierbaren geheimen Schlüssel für Web App Firewall-Operationen. Dieser geheime Schlüssel wird zum Signieren und Überprüfen von Daten verwendet. Wenn „useConfigurableSecretKey" aktiviert ist, müssen Sie den im Parameter „set ns encryptionParams" aktivierten Schlüssel verwenden.
- **Gelernte Daten zurücksetzen**— Löscht alle gelernten Daten aus der Web App Firewall. Startet den Lernprozess neu, indem neue Daten gesammelt werden.

Zwei Einstellungen, *Gelernte Daten zurücksetzen* und *Automatische Signaturen*, sind an verschiedenen Stellen, je nachdem, ob Sie die NetScaler Web App Firewall über die Befehlszeilenschnittstelle oder die NetScaler GUI konfigurieren. Wenn Sie die Befehlszeilenschnittstelle verwenden, konfigurieren Sie "Gelernte Daten zurücksetzen" mithilfe des Befehls "appfw learning data". Dies benötigt keine Parameter und hat keine anderen Funktionen. Sie können die automatische Aktualisierung der Signatur im Befehl set appfw settings konfigurieren. Der Parameter -SignatureAutoUpdate aktiviert oder deaktiviert die automatische Aktualisierung der Signaturen, und -SignatureUrl konfiguriert die URL, die die aktualisierte Signaturdatei hostet.

Wenn Sie die NetScaler-GUI verwenden, konfigurieren Sie Reset Learned Data unter **Sicherheit > NetScaler Web App Firewall > Engine-Einstellungen**. Die Option **Gelernte Daten zurück-**

setzen befindet sich unten im Dialogfeld. Sie konfigurieren die automatische Aktualisierung von Signaturen für jeden Signatursatz unter **Sicherheit** > **NetScaler Web App Firewall** > **Signaturen**, indem Sie die Signaturdatei auswählen, mit der rechten Maustaste klicken und Einstellungen für **automatische**Updates auswählen.

Normalerweise sind die Standardwerte für die **Web App Firewall-Einstellungen** korrekt. Wenn die Standardeinstellungen jedoch zu Konflikten mit anderen Servern oder zu einer vorzeitigen Unterbrechung der Verbindung Ihrer Benutzer führen, müssen Sie sie ändern.

Das Sitzungslimit der **Web App Firewall** kann mit dem folgenden Befehl konfiguriert werden:

```
> set appfw settings -sessionLimit 500000

Done

Default value:100000   Max value:500000 per PE
<!--NeedCopy-->
```

So konfigurieren Sie die Engine-Einstellungen mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw settings [-sessionCookieName <name>] [-sessionTimeout <positiveInteger>] [-sessionLifetime <positiveInteger>][-clientIPLoggingHeader <headerName>] [-undefaction <profileName>] [-defaultProfile <profileName>] [-importSizeLimit <positiveInteger>] [-logMalformedReq (ON | OFF)] [-signatureAutoUpdate (ON | OFF)] [-signatureUrl <expression>] [-cookiePostEncryptPrefix <string>] [-entityDecoding (ON | OFF)] [-useConfigurableSecretKey (ON | OFF)][-learnRateLimit <positiveInteger>] [-proxyServer <proxy server ip>] [-proxyPort <proxy server port>] [-proxyUsername <username>] [-proxyPassword <password>]`
- `save ns config`

Beispiel

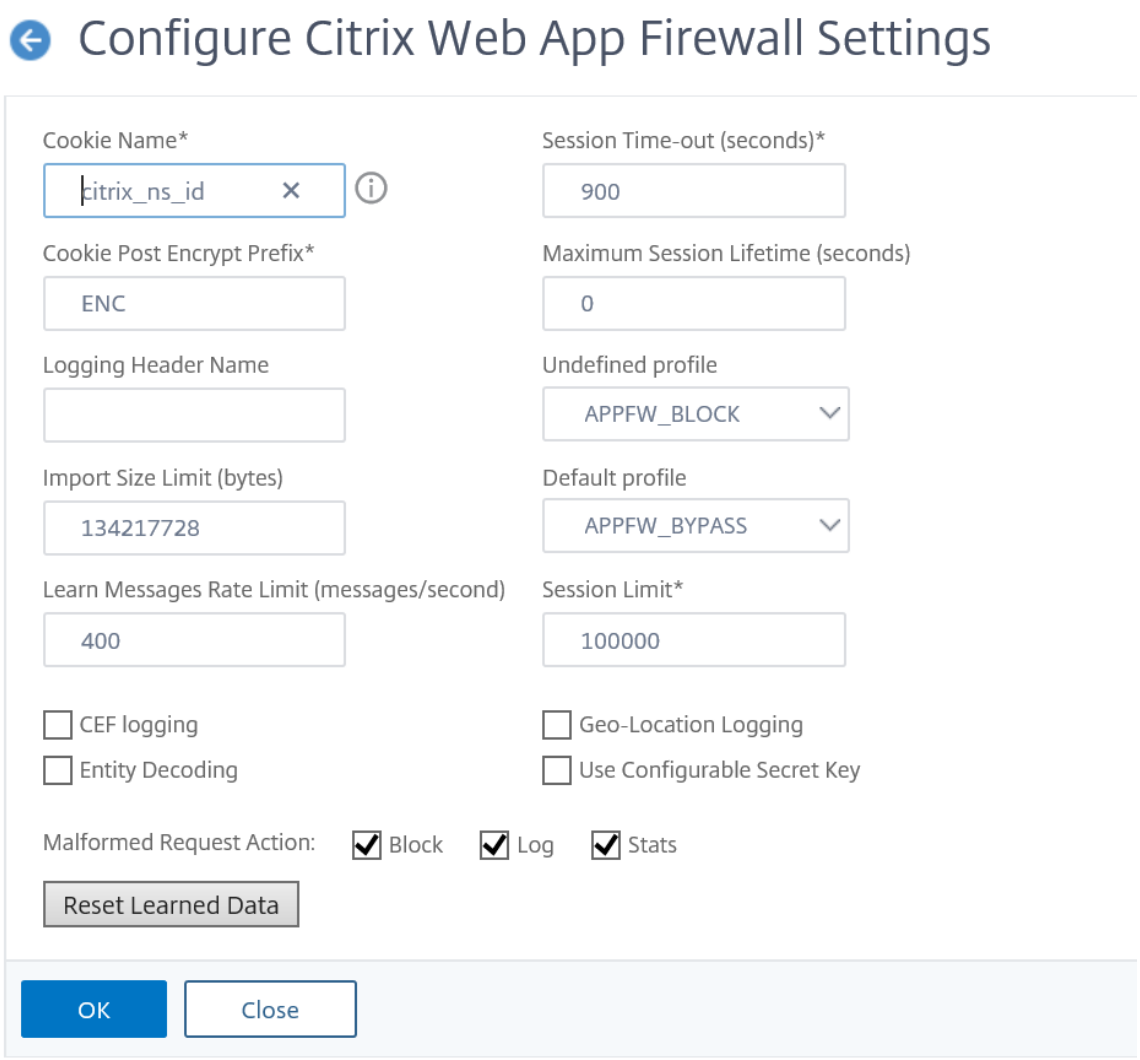
```
set appfw settings -sessionCookieName citrix-appfw-id -sessionTimeout
    3600
-sessionLifetime 14400 -clientIPLoggingHeader NS-AppFW-Client-IP -
    undefaction APPFW_RESET
-defaultProfile APPFW_RESET -importSizeLimit 4096 -proxyServer
    10.102.30.112 -proxyPort 3128 -proxyUsername defaultusername -
    proxyPassword defaultpassword
save ns config
```



```
<!--NeedCopy-->
```

So konfigurieren Sie die Engine-Einstellungen mithilfe der NetScaler-GUI

1. Navigieren Sie zu **Sicherheit** > **NetScaler Web App Firewall**
2. Klicken Sie im Detailbereich unter **Einstellungen auf**Engine-Einstellungen**ändern**.
3. Stellen Sie im Dialogfeld **Einstellungen der Web App Firewall Engine** die folgenden Parameter ein:
   - Name des Cookies
   - Sitzungs-Timeout
   - Präfix „Cookie Post Encrypt“
   - Maximale Sitzungsdauer
   - Name des Logging-Headers
   - Undefiniertes Profil
   - Standardprofil
   - Größenbeschränkung importieren
   - Ratenlimit für Lernnachrichten
   - Proxyserver
   - Proxy-Anschluss
   - Proxy-Benutzername
   - Proxy-Passwort
   - Entitätsdekodierung
   - Fehlerhafte Anfrage protokollieren
   - Geheimen Schlüssel verwenden
   - Erlernen Sie das Nachrichtenratenlimit
   - Automatische Aktualisierung von Signaturen
4. Klicken Sie auf **OK**.



Vertrauliche Felder

May 11, 2023

Sie können Webformularfelder als vertraulich festlegen, um die Informationen zu schützen, die Benutzer in sie eingeben. Normalerweise werden alle Informationen, die ein Benutzer in ein Webformular auf einem Ihrer geschützten Webserver eingibt, in den NetScaler-Protokollen protokolliert. Die Informationen, die in ein als vertraulich gekennzeichnetes Webformularfeld eingegeben werden, werden jedoch nicht protokolliert. Diese Informationen werden nur dort gespeichert, wo die Website so konfiguriert ist, dass sie solche Daten speichert, normalerweise in einer sicheren Datenbank.

Zu den gängigen Informationstypen, die Sie möglicherweise mit einer vertraulichen Feldbezeichnung schützen möchten, gehören:

- Kennwörter
- Kreditkartennummern, Validierungscodes und Ablaufdaten
- Sozialversicherungsnummern
- Steuer-Identifikationsnummern
- Heim-Adressen
- Private Telefonnummern

Zusätzlich zur bewährten Praxis kann die ordnungsgemäße Verwendung vertraulicher Feldbezeichnungen für die PCI-DSS-Konformität auf E-Commerce-Servern, die HIPAA-Konformität auf Servern, die medizinische Informationen in den USA verwalten, und die Einhaltung anderer Datenschutzstandards erforderlich sein.

> **Wichtig**:
>
> In den folgenden zwei Fällen funktioniert die Bezeichnung Vertrauliches Feld nicht wie erwartet:

- Wenn ein Webformular entweder ein vertrauliches Feld oder eine Aktions-URL mit mehr als 256 Zeichen enthält, wird die Feld- oder Aktions-URL in den NetScaler-Protokollen abgeschnitten.
- Bei bestimmten SSL-Transaktionen werden die Protokolle gekürzt, wenn entweder das vertrauliche Feld oder die Aktions-URL länger als 127 Zeichen ist.

In beiden Fällen maskiert die Web App Firewall eine fünfzehnstellige Zeichenfolge mit dem Buchstaben “x” anstelle der normalen achtstelligen Zeichenfolge. Um sicherzustellen, dass vertrauliche Informationen entfernt werden, muss der Benutzer Formularfeldnamen und Aktions-URL-Ausdrücke verwenden, die den ersten 256 oder (bei Verwendung von SSL) den ersten 127 Zeichen entsprechen.

Um Ihre Web App Firewall so zu konfigurieren, dass ein Webformularfeld auf einer geschützten Website vertraulich behandelt wird, fügen Sie dieses Feld der Liste Vertrauliche Felder hinzu. Sie können den Feldnamen als Zeichenfolge eingeben, oder Sie können einen PCRE-kompatiblen regulären Ausdruck eingeben, der ein oder mehrere Felder angibt. Sie können die Bezeichnung vertraulicher Felder aktivieren, wenn Sie das Feld hinzufügen, oder Sie können die Bezeichnung später ändern.

> **Hinweis**
>
> Ab Version 13.1 Build 27.x werden vertrauliche Felder auch in WAF-Profilen unterstützt. Weitere Informationen finden Sie unter Vertrauliche Felder im WAF-Profil.

So fügen Sie ein vertrauliches Feld mithilfe der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX )] [-comment "<string>"] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Beispiel

Im folgenden Beispiel werden alle Webformularfelder, deren Namen mit “Password” beginnen, zur Liste der vertraulichen Felder hinzugefügt.

```
add appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -isRegex
    REGEX -state ENABLED
save ns config
<!--NeedCopy-->
```

So ändern Sie ein vertrauliches Feld mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX ) ][-comment "<string>"] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird die Bezeichnung des vertraulichen Felds geändert, um einen Kommentar hinzuzufügen.

```
set appfw confidField Password "https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)" -comment "
    Protect password fields." -isRegex REGEX -state ENABLED
save ns config
<!--NeedCopy-->
```

So entfernen Sie ein vertrauliches Feld mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appfw confidField <fieldName> <url>`
- `save ns config`

So konfigurieren Sie ein vertrauliches Feld mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **Vertrauliche Felder verwalten**.
3. Führen Sie im Dialogfeld Vertrauliche Felder verwalten einen der folgenden Schritte aus:

- Um der Liste ein neues Formularfeld hinzuzufügen, klicken Sie auf Hinzufügen.
- Um eine vorhandene vertrauliche Feldbezeichnung zu ändern, wählen Sie das Feld aus, und klicken Sie dann auf **Bearbeiten**.
  Das Dialogfeld **Vertrauliche Felder der Web App Firewall** wird angezeigt.

  > **Hinweis**:
  > Wenn Sie eine vorhandene vertrauliche Feldbezeichnung auswählen und dann auf **Hinzufügen**klicken, werden im Dialogfeld **Vertrauliches Formularfeld erstellen** die Informationen für dieses vertrauliche Feld angezeigt. Sie können diese Informationen ändern, um Ihr neues vertrauliches Feld zu erstellen.

4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:
   - **Kontrollkästchen aktiviert.** Wählen oder deaktivieren Sie, um diese vertrauliche Feldbezeichnung zu aktivieren/deaktivieren
   - **Ist der Formularfeldname ein Kontrollkästchen für reguläre Ausdrücke.** Wählen oder deaktivieren Sie diese Option, um reguläre Ausdrücke im PCRE-Format im Formularfeldnamen zu aktivieren.
   - **Feldname.** Geben Sie eine Literalzeichenfolge oder einen regulären Ausdruck im PCRE-Format ein, der entweder einen bestimmten Feldnamen darstellt oder mehrere Felder mit Namen abgleicht, die einem Muster folgen.
   - **Aktions-URL.** Geben Sie eine literale URL oder einen regulären Ausdruck ein, der eine oder mehrere URLs der Webseite (n) definiert, auf denen sich die Webformulare befinden, die das vertrauliche Feld enthalten.
   - **Kommentare.** Geben Sie einen Kommentar ein. Optional.
5. Klicken Sie auf **Erstellen** oder **auf OK**.
6. Um eine vertrauliche Feldbezeichnung aus der Liste der vertraulichen Felder zu entfernen, wählen Sie die Liste der vertraulichen Felder aus, die Sie entfernen möchten. Klicken Sie dann auf Entfernen, um sie zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
7. Wenn Sie mit dem Hinzufügen, Ändern und Entfernen vertraulicher Feldbezeichnungen fertig sind, klicken Sie auf **Schließen**.

Beispiele

Im Folgenden finden Sie einige reguläre Ausdrücke, die Formularfeldnamen definieren, die für Sie nützlich sein könnten:

- `^passwd_ (Applies confidential-field status to all field names that begin with the “passwd_” string.)`
- `^((\[0-9a-zA-Z._-]*||\\x\[0-9A-Fa-f][0-9A-Fa-f])+-)?passwd_ (Applies confidential-field status to all field names that begin with the string passwd_, or that contain the string -passwd_ after another string that`


```
might contain non-ASCII special characters.)
```

Im Folgenden finden Sie einige reguläre Ausdrücke, die bestimmte URL-Typen definieren, die Sie möglicherweise nützlich finden. Ersetzen Sie die in den Beispielen gezeigten Webhosts und Domain (s) durch Ihre eigenen Webhosts.

- Wenn das Webformular auf mehreren Webseiten auf dem Webhost www.example.com erscheint, aber alle diese Webseiten logon.pl heißen? können Sie den folgenden regulären Ausdruck verwenden:

```
1 https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_.-]*/)*logon
     [.]pl?
2 <!--NeedCopy-->
```

- Wenn das Webformular auf mehreren Webseiten auf dem Webhost www.example-español.com erscheint, der das Sonderzeichen n-Tilde (ñ) enthält, können Sie den folgenden regulären Ausdruck verwenden, der das n-Tilde-Sonderzeichen als codierte UTF-8-Zeichenfolge darstellt, die C3 B1 enthält, den Hexadezimalcode, der diesem zugewiesen ist Zeichen im UTF-8-Zeichensatz:

```
1 https?://www[.]example-espa\xC3\xB1ol[.]com/([0-9A-Za-z][0-9A-Za-
     z_.-]\*/)\* logon[.]pl?
2 <!--NeedCopy-->
```

- Wenn das Webformular, das query.pl enthält, auf mehreren Webseiten auf verschiedenen Hosts innerhalb der Domäne example.com angezeigt wird, können Sie den folgenden regulären Ausdruck verwenden:

```
1 https?://([0-9A-Za-z][0-9A-Za-z_-.]*[.])\*example[.]com/([0-9A-Za
     -z][0-9A-Za-z_-.]\*/)*logon[.]pl?
2 <!--NeedCopy-->
```

- Wenn das Webformular, das query.pl enthält, auf mehreren Webseiten auf verschiedenen Hosts in verschiedenen Domänen angezeigt wird, können Sie den folgenden regulären Ausdruck verwenden:

```
1 https?://([0-9A-Za-z][0-9A-Za-z_-.]\*[.])\*[0-9A-Za-z][0-9A-Za-z_
     -.]+[.][a-z]{
2 2,6 }
3 /([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon[.]pl?
4 <!--NeedCopy-->
```

- Wenn das Webformular auf mehreren Webseiten auf dem Webhost www.example.com erscheint, aber alle diese Webseiten logon.pl heißen? können Sie den folgenden regulären Ausdruck verwenden:


```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon
   [.]pl?
<!--NeedCopy-->
```

Feldtypen

August 19, 2021

Ein Feldtyp ist ein regulärer Ausdruck im PCRE-Format, der ein bestimmtes Datenformat und minimale/maximale Datenlängen für ein Formularfeld in einem Webformular definiert. Feldtypen werden in der Feldformat-Prüfung verwendet.

Die Web App Firewall enthält mehrere Standardfeldtypen, die sind:

- integer. Eine Zeichenfolge beliebiger Länge, die nur aus Zahlen besteht, ohne Dezimalzeichen und mit einem optionalen vorangegangenen Minuszeichen (-).
- alpha. Eine Zeichenfolge beliebiger Länge, die nur aus Buchstaben besteht.
- alphanum. Eine Zeichenfolge beliebiger Länge, bestehend aus Buchstaben und/oder Zahlen.
- nohtml. Eine Zeichenfolge beliebiger Länge, die aus Zeichen besteht, einschließlich Satzzeichen und Leerzeichen, die keine HTML-Symbole oder Abfragen enthält.
- any. Irgendwas.

  > **Wichtig:**
  >
  > Wenn Sie den beliebigen Feldtyp als Standardfeldtyp oder einem Feld zuweisen, können aktive Skripts, SQL-Befehle und andere möglicherweise gefährliche Inhalte an Ihre geschützten Websites und Anwendungen in diesem Formularfeld gesendet werden. Sie müssen den Typ jeden Typ sparsam verwenden, wenn Sie ihn überhaupt benutzen.

Sie können auch eigene Feldtypen zur Liste Feldtypen hinzufügen. Sie können beispielsweise einen Feldtyp für eine Sozialversicherungsnummer, eine Postleitzahl oder eine Telefonnummer in Ihrem Land hinzufügen. Sie können auch einen Feldtyp für eine Kundenidentifikationsnummer oder eine Kreditkartennummer hinzufügen.

Um der Liste Feldtypen einen Feldtyp hinzuzufügen, geben Sie den Feldnamen als Literalzeichenfolge oder regulären Ausdruck im PCRE-Format ein.

So fügen Sie einen Feldtyp mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Liste Feldtypen ein Feldtyp namens SSN hinzugefügt, der US-Sozialversicherungsnummern entspricht, und die Priorität auf 1 festgelegt.

```
add appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1
save ns config
<!--NeedCopy-->
```

So ändern Sie einen Feldtyp mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Feldtyp so geändert, dass ein Kommentar hinzugefügt wird.

```
set appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1 -comment "US Social Security Number"
save ns config
<!--NeedCopy-->
```


So entfernen Sie einen Feldtyp mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `>rm appfw fieldType <name>`
- `save ns config`

So konfigurieren Sie einen Feldtyp mit der GUI

1. Navigieren Sie zu Sicherheit > Application Firewall.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Feldtypen verwalten**.
3. **Führen Sie im Dialogfeld Feldtypen verwalten** eine der folgenden Aktionen aus:
   - Um der Liste einen neuen Feldtyp hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen Feldtyp zu ändern, wählen Sie den Feldtyp aus, und klicken Sie dann auf **Bearbeiten**.
     Das Dialogfeld **Feldtyp konfigurieren** wird angezeigt.

   > **Hinweis:**
   >
   > Wenn Sie eine vorhandene Feldtypbezeichnung auswählen und dann auf **Hinzufügen**klicken, werden im Dialogfeld die Informationen für diesen Feldtyp angezeigt. Sie können diese Informationen ändern, um den neuen Feldtyp zu erstellen.

4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:
   - Name
   - Regulärer Ausdruck
   - Priorität
   - Kommentar
5. Klicken Sie auf Erstellen oder OK.
6. Um einen Feldtyp aus der Liste Feldtypen zu entfernen, wählen Sie die zu entfernende Feldtypliste aus, klicken Sie dann auf **Entfernen**, um ihn zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
7. Wenn Sie mit dem Hinzufügen, Ändern und Entfernen von Feldtypen fertig sind, klicken Sie auf **Schließen**.

Beispiele

Im Folgenden finden Sie einige reguläre Ausdrücke für Feldtypen, die Sie möglicherweise nützlich finden:

`^[1-9][0-9]{ 2,2 } -[0-9 } { 2,2 } -[0-9]{ 4,4 } $` US-Sozialversicherungsnummern

`^\[A-C\]\[0-9\]{ 7,7 } $` Kalifornien Führerscheinnummern

`^+[0-9]{ 1,3 } [0-9()-]{ 1,40 } $` Internationale Telefonnummern mit Ländervorwahl

`^[0-9]{ 5,5 } -[0-9]{ 4,4 } $` US-Postleitzahlennummern

`^[0-9A-Za-z][0-9A-Za-z.+_-]{ 0,25 } @([0-9A-Za-z][0-9A-Za-z_-]*[.]){ 1,4 } [A-Za-z]{ 2,6 } $` E-Mail-Adressen

XML-Inhaltstypen

February 16, 2021

Standardmäßig behandelt die Web App Firewall Dateien, die bestimmten Namenskonventionen folgen, als XML. Sie können die Web App Firewall so konfigurieren, dass Webinhalte auf zusätzliche Zeichenfolgen oder Muster untersucht werden, die darauf hindeuten, dass es sich bei diesen Dateien um XML-Dateien handelt. Dadurch kann sichergestellt werden, dass die Web App Firewall alle XML-Inhalte auf Ihrer Site erkennt, selbst wenn bestimmte XML-Inhalte nicht den normalen XML-Namenskonventionen entsprechen. Dadurch wird sichergestellt, dass XML-Inhalte XML-Sicherheitsprüfungen unterzogen werden.

Um die XML-Inhaltstypen zu konfigurieren, fügen Sie der Liste XML-Inhaltstypen die entsprechenden Muster hinzu. Sie können einen Inhaltstyp als Zeichenfolge eingeben oder einen PCRE-kompatiblen regulären Ausdruck eingeben, der eine oder mehrere Zeichenfolgen angibt. Sie können auch die vorhandenen XML-Inhaltstypen Muster ändern.

So fügen Sie mit der Befehlszeilenschnittstelle ein XML-Inhaltstypmuster hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw XMLContentType <XMLContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird das Muster hinzugefügt. */xml in die Liste XML-Inhaltstypen und bezeichnet sie als regulären Ausdruck.

```
1 add appfw XMLContentType ".*/xml" -isRegex REGEX
2 <!--NeedCopy-->
```


So entfernen Sie ein XML-Inhaltstypmuster mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appfw XMLContentType <XMLContenttypevalue>`
- `save ns config`

So konfigurieren Sie die XML-Inhaltstypliste mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** .
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **XML-Inhaltstypen verwalten**.
3. **Führen Sie im Dialogfeld XML-Inhaltstypen verwalten** eine der folgenden Aktionen aus:
   - Um einen neuen XML-Inhaltstyp hinzuzufügen, klicken Sie auf Hinzufügen.
   - Um einen vorhandenen XML-Inhaltstyp zu ändern, wählen Sie diesen Typ aus, und klicken Sie dann auf Bearbeiten.
     Das Dialogfeld XML-Inhaltstyp der Web App Firewall konfigurieren wird angezeigt. Hinweis: Wenn Sie ein vorhandenes XML-Inhaltstypmuster auswählen und dann auf Hinzufügen klicken, werden im Dialogfeld die Informationen für dieses Muster für den XML-Inhaltstyp angezeigt. Sie können diese Informationen ändern, um Ihr neues XML-Inhaltstypmuster zu erstellen.
4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:
   - **IsRegex.** Aktivieren oder deaktivieren Sie diese Option, um reguläre Ausdrücke im Formularfeldnamen im PCRE-Format zu aktivieren.
   - **XML-Inhaltstyp** Geben Sie eine Literalzeichenfolge oder einen regulären Ausdruck im PCRE-Format ein, der dem XML-Inhaltstypmuster entspricht, das Sie hinzufügen möchten.
5. Klicken Sie auf **Erstellen**.
6. Um ein XML-Inhaltstypmuster aus der Liste zu entfernen, wählen Sie es aus, klicken Sie dann auf **Entfernen**, um es zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
7. Wenn Sie mit dem Hinzufügen und Entfernen von XML-Inhaltstypmustern fertig sind, klicken Sie auf **Schließen**.

JSON-Inhaltstypen

February 16, 2021

Standardmäßig behandelt die Web App Firewall Dateien mit dem Inhaltstyp application/json als JSON-Dateien. Die Standardeinstellung ermöglicht es der Web App Firewall, JSON-Inhalte in Anfragen und Antworten zu erkennen und diesen Inhalt entsprechend zu handhaben.

Sie können die Web App Firewall so konfigurieren, dass Webinhalte auf zusätzliche Zeichenfolgen oder Muster untersucht werden, die darauf hindeuten, dass es sich bei diesen Dateien um

JSON-Dateien handelt. Dadurch kann sichergestellt werden, dass die Web App Firewall alle JSON-Inhalte auf Ihrer Site erkennt, selbst wenn bestimmte JSON-Inhalte nicht den normalen JSON-Namenskonventionen entsprechen, wodurch sichergestellt wird, dass JSON-Inhalte JSON-Sicherheitsprüfungen unterzogen werden.

Um die JSON-Inhaltstypen zu konfigurieren, fügen Sie der Liste JSON-Inhaltstypen die entsprechenden Muster hinzu. Sie können einen Inhaltstyp als Zeichenfolge eingeben oder einen PCRE-kompatiblen regulären Ausdruck eingeben, der eine oder mehrere Zeichenfolgen angibt. Sie können auch die vorhandenen JSON-Inhaltstypenmuster ändern.

So fügen Sie ein JSON-Inhaltstypmuster mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw JSONContentType <JSONContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird das Muster hinzugefügt. */json in die Liste JSON-Inhaltstypen und bezeichnet sie als regulären Ausdruck.

```
1 add appfw JSONContentType ".*/json" -isRegex REGEX
2 <!--NeedCopy-->
```

So konfigurieren Sie die JSON-Inhaltstypliste mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **JSON-Inhaltstypen verwalten**.
3. Führen Sie im Dialogfeld JSON-Inhaltstypen verwalten eine der folgenden Aktionen aus:
   - Um einen neuen JSON-Inhaltstyp hinzuzufügen, klicken Sie auf Hinzufügen.
   - Um einen vorhandenen JSON-Inhaltstyp zu ändern, wählen Sie diesen Typ aus, und klicken Sie dann auf Bearbeiten.
     Das Dialogfeld Web App Firewall JSON-Inhaltstyp konfigurieren wird angezeigt.
     Hinweis: Wenn Sie ein vorhandenes JSON-Inhaltstypmuster auswählen und dann auf Hinzufügen klicken, werden im Dialogfeld die Informationen für dieses JSON-Inhaltstypmuster angezeigt. Sie können diese Informationen ändern, um Ihr neues JSON-Inhaltstypmuster zu erstellen.
4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:

- **IsRegex.** Aktivieren oder deaktivieren Sie diese Option, um reguläre Ausdrücke im Formularfeldnamen im PCRE-Format zu aktivieren.
- **JSON-Inhaltstyp** Geben Sie eine Literalzeichenfolge oder einen regulären Ausdruck im PCRE-Format ein, der dem JSON-Inhaltstypmuster entspricht, das Sie hinzufügen möchten.

5. Klicken Sie auf **Erstellen** oder **OK**.
6. Um ein JSON-Inhaltstypmuster aus der Liste zu entfernen, wählen Sie es aus, klicken Sie dann auf **Entfernen**, um es zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
7. Wenn Sie mit dem Hinzufügen und Entfernen von XML-Inhaltstypmustern fertig sind, klicken Sie auf **Schließen**.

Statistiken und Berichte

May 11, 2023

Die in den Protokollen und Statistiken gepflegten und in den Berichten angezeigten Informationen enthalten wichtige Hinweise zum Konfigurieren und Verwalten der Web App Firewall.

Die Statistiken der Web App Firewall

Wenn Sie die Statistikaktion für Web App Firewall-Signaturen oder Sicherheitsprüfungen aktivieren, speichert die Web App Firewall Informationen über Verbindungen, die dieser Signatur oder Sicherheitsprüfung entsprechen. Sie können die gesammelten Statistikinformationen auf der Registerkarte **Überwachung** anzeigen, indem Sie im Listenfeld “Gruppe auswählen” eine der folgenden Optionen auswählen:

- **Web App Firewall.** Eine Zusammenfassung aller Statistikinformationen, die von Ihrer Web App Firewall-Appliance für alle Profile gesammelt wurden.
- **Web App Firewall (pro Profil).** Die gleichen Informationen, aber pro Profil angezeigt und nicht zusammengefasst.

Sie können diese Informationen verwenden, um zu überwachen, wie Ihre Web App Firewall funktioniert, und um festzustellen, ob bei einer Signatur oder Sicherheitsprüfung abnormale Aktivitäten oder ungewöhnliche Treffermengen vorliegen. Wenn Sie ein solches Muster abnormaler Aktivitäten sehen, können Sie die Protokolle auf diese Signatur oder Sicherheitsprüfung überprüfen, um Korrekturmaßnahmen zu diagnostizieren und zu ergreifen.

Entspannung traf den statistischen Zähler

Basierend auf der Entspannung, die auf den verletzten Verkehr angewendet wird, können Sie auch statistische Details anzeigen, wie oft ein Verstoß auf der Appliance auftritt, die Anzahl der zum Zeitpunkt des Verstoßes angewendeten Entspannungsregeln und den zuletzt angewendeten Zeitstempel. Dadurch kann die zentralisierte Lern-Engine automatisch ungenutzte oder redundante Entspannungsbindungen löschen. Weitere Informationen finden Sie unter Thema WAF Learn Engine .

Der statistische Zähler für die Entspannungstreffer ist nur für die folgenden Sicherheitsprüfungen verfügbar.

- Cross-Site Scripting
- SQL Injection
- Cookie-Konsistenz
- JSON SQL
- JSON-Cross-Site Scripting
- JSON-DoS
- JSON-CMD-Injection
- Site-übergreifende Fälschung
- Feld-Format
- Starturl
- Denyurl
- Content-Typ-Schutz

So zeigen Sie Statistiken für Trefferindikatoren für Relationsregel über die Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:

```
stat appfw profile p1
```

Beispiel:

```
stat appfw profile p1 -fullvalues
```

Starturl-Regel-Statistik

Regel	Hits	Bewerten	letzte Treffer-Zeit
87a4…51177	0	0	Do… 1970
5b83…dc12a	0	0	Do… 1970
12345	0	0	Do… 1970

So zeigen Sie Statistiken für Relaxationsregel an, indem Sie die GUI verwenden

Führen Sie die folgenden Schritte aus, um die Trefferzählerstatistiken der Entspannungsregel anzuzeigen

1. Navigieren Sie zu **Sicherheit > NetScaler Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein **Web App Firewall-Profil** aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **NetScaler Web App Firewall-Statistiken** werden die Statistikdetails angezeigt.
4. Sie können die Tabellarische Ansicht wählen oder zur grafischen Ansicht wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.

Die Web App Firewall-Berichte

Die Web App Firewall-Berichte enthalten Informationen über Ihre Web App Firewall-Konfiguration und zum Umgang mit dem Datenverkehr für Ihre geschützten Websites.

Der PCI-DSS-Bericht

Der Payment Card Industry (PCI) Data Security Standard (DSS), Version 1.2, besteht aus 12 Sicherheitskriterien, die die meisten Kreditkartenunternehmen von Unternehmen, die Online-Zahlungen mit Kredit- und Debitkarten akzeptieren, erfüllen müssen. Die Kriterien sollen Identitätsdiebstahl, Hacking und andere Arten von Betrug verhindern. Wenn ein ISP die PCI-DSS-Kriterien nicht erfüllt, verliert der ISP oder Händler möglicherweise die Berechtigung, Kreditkartenzahlungen über die Website anzunehmen.

ISPs und Online-Händler beweisen, dass sie PCI DSS einhalten, indem sie ein Audit von einem PCI DSS Qualified Security Assessor (QSA) -Unternehmen durchführen lassen. Der PCI-DSS-Bericht soll sie sowohl vor als auch während des Audits unterstützen. Vor dem Audit wird angezeigt, welche Web App Firewall-Einstellungen für PCI DSS relevant sind, wie sie konfiguriert werden müssen und (am wichtigsten), ob Ihre aktuelle Web App Firewall-Konfiguration dem Standard entspricht. Während der Prüfung kann der Bericht verwendet werden, um die Einhaltung relevanter PCI-DSS-Kriterien nachzuweisen.

Der PCI-DSS-Bericht besteht aus einer Liste der Kriterien, die für Ihre Web App Firewall-Konfiguration relevant sind. Unter jedem Kriterium listet es Ihre aktuellen Konfigurationsoptionen auf, gibt an, ob Ihre aktuelle Konfiguration dem PCI-DSS-Kriterium entspricht, und erklärt, wie Sie die Web App Firewall so konfigurieren, dass Ihre geschützten Websites das Kriterium erfüllen.

Der PCI-DSS-Bericht befindet sich unter **System > Berichte**. Um den Bericht als Adobe PDF-Datei zu **erstellen, klicken Sie auf PCI DSS-Bericht**erstellen. Abhängig von Ihren Browsereinstellungen wird der Bericht im Popup-Fenster angezeigt oder Sie werden aufgefordert, ihn auf Ihrer Festplatte zu speichern.

> **Hinweis:**
>
> Um diese und andere Berichte anzuzeigen, muss das Adobe Reader-Programm auf Ihrem Computer installiert sein.

Der PCI-DSS-Bericht besteht aus den folgenden Abschnitten:

- **Beschreibung.** Eine Beschreibung des PCI-DSS-Compliance-Zusammenfassungsberichts.
- **Firewall-Lizenz und Featurestatus** Zeigt an, ob die Web App Firewall auf Ihrer NetScaler-Appliance lizenziert und aktiviert ist.
- **Zusammenfassung der Geschäftsführung.** Eine Tabelle, die die PCI-DSS-Kriterien auflistet und Ihnen mitteilt, welche dieser Kriterien für die Web App Firewall relevant sind.
- **Detaillierte PCI-DSS-Kriterieninformationen.** Für jedes PCI-DSS-Kriterium, das für Ihre Web App Firewall-Konfiguration relevant ist, enthält der PCI-DSS-Bericht einen Abschnitt, der Informationen darüber enthält, ob Ihre Konfiguration konform ist, und wenn dies nicht der Fall ist, wie Sie sie einhalten können.
- **Konfiguration.** Daten für einzelne Profile, auf die Sie entweder zugreifen, indem Sie oben im Bericht auf Web App Firewall-Konfiguration oder direkt im Bereich Berichte klicken. Der Bericht zur Konfiguration der Web App Firewall entspricht dem PCI-DSS-Bericht, wobei die PCI-DSS-spezifische Zusammenfassung weggelassen wird.

Der Konfigurationsbericht der Web App Firewall

Der Bericht zur Konfiguration der Web App Firewall befindet sich unter **System > Berichte**. Um es anzuzeigen, klicken Sie auf **Web App Firewall-Konfigurationsbericht generieren**. Abhängig von Ihren Browsereinstellungen wird der Bericht im Popup-Fenster angezeigt oder Sie werden aufgefordert, ihn auf Ihrer Festplatte zu speichern.

Der Bericht zur Web App Firewall-Konfiguration beginnt mit einer Zusammenfassungsseite, die aus den folgenden Abschnitten besteht:

- **Web App Firewall-Richtlinien.** Eine Tabelle, in der Ihre aktuellen Web App Firewall-Richtlinien aufgeführt sind und den Richtliniennamen, den Inhalt der Richtlinie, die Aktion (oder das Profil), mit der sie verknüpft ist, und globale Bindungsinformationen anzeigen.
- **Web App Firewall App-Firewall-Profile.** Eine Tabelle, die Ihre aktuellen Web App Firewall-Profile auflistet und angibt, mit welcher Richtlinie jedes Profil verknüpft ist. Wenn ein Profil keiner Richtlinie zugeordnet ist, wird in der Tabelle an diesem Speicherort INAKTIV angezeigt.

Um alle Berichtsseiten für alle Richtlinien herunterzuladen, klicken Sie oben auf der Seite Profilübersicht auf **Alle Profile herunterladen**. Sie zeigen die Berichtsseite für jedes einzelne Profil an, indem Sie dieses Profil in der Tabelle unten auf dem Bildschirm auswählen. Die Profilseite für ein einzelnes

Profil zeigt an, ob jede Prüfaktion für jede Prüfung aktiviert oder deaktiviert ist, und die anderen Konfigurationseinstellungen für die Prüfung.

Um eine PDF-Datei mit der PCI-DSS-Berichtsseite für das aktuelle Profil **herunterzuladen, klicken Sie oben auf der Seite auf Aktuelles Profil** herunterladen. Um zur Seite Profilübersicht zurückzukehren, klicken Sie auf **Web App Firewall-Profile**. Um zur Hauptseite zurückzukehren, klicken Sie auf **Home**. Sie können den PCI-DSS-Bericht jederzeit **aktualisieren**, indem Sie in der oberen rechten Ecke des Browsers auf Aktualisieren klicken.

Web App Firewall Protokolle

September 1, 2023

Die Web App Firewall generiert Protokollmeldungen für die Nachverfolgung der Konfiguration, den Richtlinienaufruf und Details zu Verstößen gegen Sicherheitsüberprüfungen.

Wenn Sie die Protokollaktion für Sicherheitsprüfungen oder Signaturen aktivieren, enthalten die daraus resultierenden Protokollmeldungen Informationen über die Anforderungen und Antworten, die die Web App Firewall beim Schutz Ihrer Sites und Anwendungen beobachtet hat. Die wichtigsten Informationen sind die Maßnahmen, die die Web App Firewall ergriffen hat, wenn eine Signatur oder eine Verletzung der Sicherheitsüberprüfung festgestellt wurde. Für einige Sicherheitsüberprüfungen kann die Protokollnachricht nützliche Informationen liefern, z. B. den Standort des Benutzers oder ein erkanntes Muster, das eine Verletzung ausgelöst hat. Ein übermäßiger Anstieg der Anzahl von Nachrichten über Verstöße in den Protokollen kann auf einen Anstieg böswilliger Anfragen hinweisen. In der Meldung werden Sie darauf hingewiesen, dass Ihre Anwendung möglicherweise angegriffen wird, um eine bestimmte Sicherheitsanfälligkeit auszunutzen, die durch den Schutz der Web App Firewall erkannt und vereitelt wird.

> **Hinweis:**
>
> Wenn Sie die Protokolle der NetScaler Web App Firewall von den Systemprotokollen trennen möchten, müssen Sie einen externen SYSLOG-Server verwenden.

NetScaler (Native) Formatprotokolle

Die Web App Firewall verwendet standardmäßig die NetScaler-Formatprotokolle (auch als native Formatprotokolle bezeichnet). Diese Protokolle haben dasselbe Format wie die von anderen NetScaler-Funktionen generierten. Jedes Protokoll enthält die folgenden Felder:

- Zeitstempel. Datum und Uhrzeit, an dem die Verbindung hergestellt wurde.
- Schweregrad. Schweregrad des Protokolls.
- Modul. NetScaler-Modul, das den Protokolleintrag generiert hat.

- Event-Typ. Art des Ereignisses, wie Unterschriftenverletzung oder Verletzung der Sicherheitsüberprüfung.
- Ereignis-ID. Dem Ereignis zugewiesene ID.
- Client-IP. IP-Adresse des Benutzers, dessen Verbindung protokolliert wurde.
- Transaktions-ID. ID, die der Transaktion zugewiesen wurde, die das Protokoll verursacht hat.
- Sitzungs-ID. ID, die der Benutzersitzung zugewiesen wurde, die das Protokoll verursacht hat.
- Botschaft. Die Protokollnachricht. Enthält Informationen zur Identifizierung der Signatur oder Sicherheitsüberprüfung, die den Protokolleintrag ausgelöst hat.

Sie können nach jedem dieser Felder oder einer beliebigen Kombination von Informationen aus verschiedenen Feldern suchen. Ihre Auswahl ist nur durch die Funktionen der Tools begrenzt, die Sie zum Anzeigen der Protokolle verwenden. Sie können die Web App Firewall-Protokollmeldungen in der GUI beobachten, indem Sie auf den NetScaler Syslog-Viewer zugreifen, oder Sie können manuell eine Verbindung zur NetScaler-Appliance herstellen und über die Befehlszeilenschnittstelle auf Protokolle zugreifen, oder Sie können in die Shell wechseln und die Protokolle direkt aus `/var/log/folder` verfolgen.

Beispiel einer Protokollmeldung im nativen Format

```
1 Jun 22 19:14:37 <local0.info> 10.217.31.98 06/22/2015:19:14:37 GMT ns
     0-PPE-1 :
2 default APPFW APPFW_cross-site scripting 60 0 :  10.217.253.62 616-PPE1
     y/3upt2K8ySWWId3Kavbxyni7Rw0000
3 pr_ffc http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
4 12345&drinking_pref=on&text_area=%3Cscript%3E%0D%0A&loginButton=
     ClickToLogin&as_sfid=
5 AAAAAAWEXcNQLlSokNmqaYF6dvfqlChNzSMsdyO9JXOJomm2v
6 BwAMOqZIChv21EcgBc3rexIUcfm0vckKlsgoOeC_BArx1Ic4NLxxkWMtrJe4H7SOfkiv9NL7AG4juPIan

7 %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c Cross-site script
     check failed for
8 field text_area="Bad tag: script" <blocked>
9 <!--NeedCopy-->
```

Common Event Format (CEF) -Protokolle

Die Web App Firewall unterstützt auch CEF-Protokolle. CEF ist ein offener Protokollverwaltungsstandard, der die Interoperabilität sicherheitsrelevanter Informationen von verschiedenen Sicherheits- und Netzwerkgeräten und -anwendungen verbessert. Mit CEF können Kunden ein allgemeines Ereignisprotokollformat verwenden, sodass Daten einfach erfasst und für die Analyse durch ein Unternehmensverwaltungssystem aggregiert werden können. Die Protokollnachricht ist in verschiedene Felder unterteilt, sodass Sie die Nachricht einfach analysieren und Skripte schreiben können, um wichtige Informationen zu identifizieren.

Analysieren der CEF-Protokollnachricht

Neben Datum, Zeitstempel, Client-IP, Protokollformat, Appliance, Unternehmen, Build-Version, Modul- und Sicherheitsüberprüfungsinformationen enthalten die CEF-Protokollmeldungen der Web App Firewall die folgenden Details:

- src — Quell-IP-Adresse
- spt — Quell-Portnummer
- Anfrage — URL anfragen
- act — action (zum Beispiel blockiert, transformiert)
- msg — message (Meldung zur beobachteten Verletzung der Sicherheitsüberprüfung)
- Offset — stellt die Bytes vom Anfang der Datei dar.
- cn1 — Ereignis-ID
- cn2 — HTTP-Transaktion-ID
- cs1 — Profilname
- cs2 — PPE ID (zum Beispiel PPE1)
- cs3 — Sitzungs-ID
- cs4 — Schweregrad (zum Beispiel INFO, ALERT)
- cs5 — Ereignisjahr
- cs6 - Kategorie “Signatur-Verstoß”
- method — Methode (zum Beispiel GET/POST)

Betrachten Sie beispielsweise die folgende Protokollnachricht im CEF-Format, die generiert wurde, als ein Verstoß gegen die Start-URL ausgelöst wurde:

```
1 Jun 12 23:37:17 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0
2 |APPFW|APPFW_STARTURL|6|src=10.217.253.62 spt=47606 method=GET
3 request=http://aaron.stratum8.net/FFC/login.html msg=Disallow Illegal
     URL. cn1=1340
4 cn2=653 cs1=pr_ffc cs2=PPE1 cs3=EsdGd3VD0OaaURLcZnj05Y6DOmE0002 cs4=
     ALERT cs5=2015
5 act=blocked
6 <!--NeedCopy-->
```

Die obige Nachricht kann in verschiedene Komponenten unterteilt werden. Weitere Informationen finden Sie in der Tabelle mit den CEP-Protokollkomponenten .

Beispiel für eine Anforderungsprüfung Verletzung im CEF-Protokollformat: Anforderung ist nicht blockiert

```
1 Jun 13 00:21:28 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0|APPFW|
2 APPFW_FIELDCONSISTENCY|6|src=10.217.253.62 spt=761 method=GET request=
3 http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
```



```
123456789234&drinking_pref=on&text_area=&loginButton=ClickToLogin&
    as_sfid
=
    AAAAAAWIahZuYoIFbjBhYMP05mJLTwEfIY0a7AKGMg3jIBaKmwtK4t7M7lNxOgj7Gmd3SZc8KUj6CF

7W5kIWDRHN8PtK1Zc-txHkHNx1WknuG9DzTuM7t1THhluevXu9I4kp8%3D&as_fid=
    feeec8758b4174
0eedeeb6b35b85dfd3d5def30c msg=Field consistency check failed for field
     passwd cn1=1401
cn2=707 cs1=pr_ffc cs2=PPE1 cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=
    ALERT cs5=2015 act=
not blocked
<!--NeedCopy-->
```

Beispiel für eine Verletzung der Antwortprüfung im CEF-Format: Antwort wird transformiert

```
Jun 13 00:25:31 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SAFECOMMERCE|6|src=10.217.253.62 spt=34041 method=GET request=
http://aaron.stratum8.net/FFC/CreditCardMind.html msg=Maximum number of
     potential credit
card numbers seen cn1=1470 cn2=708 cs1=pr_ffc cs2=PPE1
cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Beispiel für eine Verletzung der anforderungsseitigen Signatur im CEF-Format: Anfrage ist blockiert

```
Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method=GET request=
http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=Signature
    violation rule ID 807:
web-cgi /wwwboard/passwd.txt access  cn1=140 cn2=841 cs1=pr_ffc cs2=
    PPE0
cs3=OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
    blocked
<!--NeedCopy-->
```

Beispiel für einen Verstoß gegen die Antwortprüfung im CEF-Format für einen Offset:

```
Jan 24 10:00:00 <local0.warn> 10.175.4.47 CEF:0|Citrix|NetScaler|NS13
    .0|APPFW|APPFW_XML_ERR_NOT_WELLFORMED|4|src=5.31.100.129 spt=20644
    method=GET request=https://wifiuae.duwifi.ae/publishApplications/en
    /5dafe3e74fa8015599009bc1/images/fallback_photo.svg msg=XML Format
    check failed: Message is not a well-formed XML.Error string is '
```



```
      unclosed token'. Offset:-517597 cn1=547290214 cn2=974226675 cs1=
      WIFI_UAE_AppFw cs2=PPE0 cs4=ERROR cs5=2023 act=blocked
<!--NeedCopy-->
```

In diesem Beispiel trat die XML_ERR_NOT_WELLFORMED-Verletzung aufgrund von auf `unclosed token`. Dieser Verstoß liegt an der Position 517597 vom Anfang der Datei an.

Protokollieren der Geolocation in den Verstoßmeldungen der Web App Firewall

Die Protokolldetails identifizieren den Ort, von dem Anforderungen stammen, und helfen Ihnen, die Web App Firewall für die optimale Sicherheitsstufe zu konfigurieren. Um Sicherheitsimplementierungen wie Ratenbegrenzungen zu Bypass, die auf den IP-Adressen der Clients beruhen, können Malware oder nicht autorisierte Computer die Quell-IP-Adresse in Anfragen ständig ändern. Durch die Identifizierung der spezifischen Region, aus der Anfragen kommen, kann festgestellt werden, ob die Anfragen von einem gültigen Benutzer oder einem Gerät stammen, das versucht, Cyberangriffe zu starten. Wenn beispielsweise eine übermäßig große Anzahl von Anfragen aus einem bestimmten Bereich eingeht, kann leicht festgestellt werden, ob sie von Benutzern oder einem Schurkencomputer gesendet werden. Die Geolokalisierungsanalyse des empfangenen Datenverkehrs kann nützlich sein, um Angriffe wie Denial-of-Service-Angriffe (DoS) abzuwehren.

Die Web App Firewall bietet Ihnen die Möglichkeit, die integrierte NetScaler-Datenbank zu verwenden, um die Speicherorte zu identifizieren, die den IP-Adressen entsprechen, von denen böswillige Anfragen stammen. Sie können dann ein höheres Sicherheitsniveau für Anfragen von diesen Sites erzwingen. NetScaler-Standardsyntaxausdrücke (PI) bieten Ihnen die Flexibilität, standortbasierte Richtlinien zu konfigurieren, die zusammen mit der integrierten Standortdatenbank verwendet werden können, um den Firewallschutz anzupassen und so Ihren Schutz vor koordinierten Angriffen zu stärken, die von betrügerischen Clients in einer bestimmten Region ausgeführt werden.

Sie können die integrierte NetScaler-Datenbank oder eine andere Datenbank verwenden. Wenn die Datenbank keine Standortinformationen für die bestimmte Client-IP-Adresse enthält, zeigt das CEF-Protokoll die Geolocation als unbekannte Geolocation an.

> **Hinweis:**
>
> Die Geolocation-Protokollierung verwendet das Common Event Format (CEF). Standardmäßig sind `CEF logging` und `GeoLocationLogging` AUS. Sie müssen beide Parameter explizit aktivieren.

Beispiel für eine CEF-Protokollnachricht mit Geolokationsinformationen

```
June 8 00:21:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_STARTURL|6|src=10.217.253.62 geolocation=NorthAmerica.US.Arizona.
    Tucson.\*.\*
```



```
3 spt=18655 method=GET request=http://aaron.stratum8.net/FFC/login.html
4 msg=Disallow Illegal URL. cn1=77 cn2=1547 cs1=test_pr_adv cs2=PPE1
5 cs3=KDynjg1pbFtfhC/nt0rBU1o/Tyg0001 cs4=ALERT cs5=2015 act=not blocked
6 <!--NeedCopy-->
```

Beispiel einer Protokollnachricht mit Geolocation= Unknown

```
1 June 9 23:50:53 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0|
2 APPFW|APPFW_STARTURL|6|src=10.217.30.251 geolocation=Unknown spt=5086
3 method=GET request=http://aaron.stratum8.net/FFC/login.html msg=
     Disallow Illegal URL.
4 cn1=74 cn2=1576 cs1=test_pr_adv cs2=PPE2 cs3=
     PyR0eOEM4gf6GJiTyauiHByL88E0002
5 cs4=ALERT cs5=2015 act=not blocked
6 <!--NeedCopy-->
```

Konfigurieren der Protokollaktion und anderer Protokollparameter mithilfe der Befehlsschnittstelle

So konfigurieren Sie die Protokollaktion für eine Sicherheitsüberprüfung eines Profils über die Befehlszeile

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set appfw profile <name> SecurityCheckAction ([log] | [none])`
- `unset appfw profile <name> SecurityCheckAction`

Beispiele

```
set appfw profile pr_ffc StartURLAction log
```

```
unset appfw profile pr_ffc StartURLAction
```

So konfigurieren Sie die CEF-Protokollierung über die Befehlszeile

Die CEF-Protokollierung ist standardmäßig deaktiviert. Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die aktuelle Einstellung zu ändern oder anzuzeigen:

- `set appfw settings CEFLogging on`
- `unset appfw settings CEFLogging`
- `sh appfw settings | grep CEFLogging`

So konfigurieren Sie die Protokollierung der Kreditkartennummern über die Befehlszeile

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set appfw profile <name> -doSecureCreditCardLogging ([ON] | [OFF])`

- `unset appfw profile <name> -doSecureCreditCardLogging`

So konfigurieren Sie die Geolocation-Protokollierung über die Befehlszeile

1. Verwenden Sie den Befehl set, um GeoLocationLogging zu aktivieren. Sie können die CEF-Protokollierung gleichzeitig aktivieren. Verwenden Sie den Befehl unset, um die Geolocation-Protokollierung zu deaktivieren. Der Befehl show zeigt die aktuellen Einstellungen aller Web App Firewall-Parameter an, es sei denn, Sie schließen den Befehl grep ein, um die Einstellung für einen bestimmten Parameter anzuzeigen.
   - `set appfw settings GeoLocationLogging ON [CEFLogging ON]`
   - `unset appfw settings GeoLocationLogging`
   - `sh appfw settings | grep GeoLocationLogging`
2. Geben Sie die Datenbank an

   ```
   add locationfile /var/netscaler/inbuilt_db/Citrix_netscaler_InBuilt_GeoIP_DB
   .csv
   ```

   oder

   ```
   add locationfile <path to database file>
   ```

Anpassen der Web App Firewall-Protokolle

Standardformat-Ausdrücke (PI) geben Ihnen die Flexibilität, die in den Protokollen enthaltenen Informationen anzupassen. Sie haben die Möglichkeit, die spezifischen Daten, die Sie erfassen möchten, in die von der Web App Firewall generierten Protokollmeldungen aufzunehmen. Wenn Sie beispielsweise die AAA-TM-Authentifizierung zusammen mit den Sicherheitsüberprüfungen der Web App Firewall verwenden und die URL, auf die zugegriffen wird, die den Verstoß gegen die Sicherheitsüberprüfung ausgelöst hat, den Namen des Benutzers, der die URL angefordert hat, die Quell-IP-Adresse und den Quellport, von dem aus der Benutzer die Anfrage gesendet hat, wissen möchten, können Sie kann die folgenden Befehle verwenden, um benutzerdefinierte Protokollmeldungen anzugeben, die alle Daten enthalten:

```
1 > sh version
2 NetScaler NS12.1: Build 50.0013.nc, Date: Aug 28 2018, 10:51:08   (64-
     bit)
3  Done
4 <!--NeedCopy-->
```

```
1 > add audit messageaction custom1 ALERT 'HTTP.REQ.URL + " " + HTTP.REQ.
     USER.NAME + " " + CLIENT.IP.SRC + ":" + CLIENT.TCP.SRCPORT'
2 Warning: HTTP.REQ.USER has been deprecated. Use AAA.USER instead.
3  Done
4 <!--NeedCopy-->
```



```
> add appfw profile test_profile
 Done
<!--NeedCopy-->
```

```
> add appfw policy appfw_pol true test_profile -logAction custom1
 Done
<!--NeedCopy-->
```

Konfigurieren der Syslog-Richtlinie, um Web App Firewall-Protokolle zu trennen

Die Web App Firewall bietet Ihnen die Möglichkeit, die Sicherheitsprotokollmeldungen der Web App Firewall zu isolieren und in eine andere Protokolldatei umzuleiten. Dies kann wünschenswert sein, wenn die Web App Firewall viele Protokolle generiert, wodurch es schwierig wird, andere NetScaler-Protokollmeldungen anzuzeigen. Sie können diese Option auch verwenden, wenn Sie nur die Web App Firewall-Protokollmeldungen anzeigen möchten und die anderen Protokollmeldungen nicht sehen möchten.

Um die Web App Firewall-Protokolle in eine andere Protokolldatei umzuleiten, konfigurieren Sie eine Syslog-Aktion, um die Web App Firewall-Protokolle an eine andere Protokolleinrichtung zu senden. Sie können diese Aktion verwenden, wenn Sie die Syslog-Richtlinie konfigurieren und global für die Verwendung durch Web App Firewall binden.

> **Hinweise:**
>
> - Um Richtlinien der Web App Firewall global zu binden, können Sie den globalen Bindungsparameter “APPFW_GLOBAL” in den Befehlen “bind audit syslogGlobal” und “bind audit nslogGlobal” konfigurieren. Die global gebundenen Überwachungsprotokollrichtlinien können Protokollmeldungen im Protokollierungskontext der Web App Firewall auswerten.
> - Sie können Web Application Firewall-Protokolle nicht von einem lokalen Audit- oder SYSLOG-Server trennen, der auf NetScaler ausgeführt wird. Die Verwendung der Local2-Protokollfunktion führt dazu, dass sowohl Web Application Firewall- als auch IP-Reputation-Protokolle in derselben Protokolldatei empfangen werden.

Beispiel:

1. Wechseln Sie zur Shell und bearbeiten Sie mit einem Editor wie vi die Datei /etc/syslog.conf. Fügen Sie einen neuen Eintrag hinzu, um local2.* zu verwenden, um Protokolle an eine separate Datei zu senden, wie im folgenden Beispiel gezeigt:

   ```
   local2.\* /var/log/ns.log.appfw
   ```


2. Starten Sie den Syslog-Prozess neu. Sie können den Befehl grep verwenden, um die Syslog-Prozess-ID (PID) zu identifizieren, wie im folgenden Beispiel gezeigt:

   ```
   root@ns\## **ps -A | grep syslog**

   1063 ?? Ss 0:03.00 /usr/sbin/syslogd -b 127.0.0.1 -n -v -v -8 -C

   root@ns## **kill -HUP** 1063
   ```

3. Konfigurieren Sie über die Befehlszeilenschnittstelle entweder erweiterte oder klassische SYSLOG-Richtlinien mit Aktion und binden Sie sie als globale Web App Firewall-Richtlinie. Citrix empfiehlt Ihnen, die erweiterte SYSLOG-Richtlinie zu konfigurieren.

   Erweiterte SYSLOG-Richtlinienkonfiguration

   ```
   add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
   LOCAL2

   add audit syslogPolicy syspol1 true sysact1

   bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
    APPFW_GLOBAL
   ```

   Klassische SYSLOG-Richtlinienkonfiguration

   ```
   add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
   LOCAL2

   add audit syslogPolicy syspol1 ns_true sysact1

   bind appfw global syspol1 100
   ```

4. Alle Verstöße gegen die Sicherheitsüberprüfung der Web App Firewall werden jetzt in die Datei `/var/log/ns.log.appfw` umgeleitet. Sie können diese Datei verkürzen, um die Verstöße gegen die Web App Firewall anzuzeigen, die während der Verarbeitung des laufenden Datenverkehrs ausgelöst werden.

   ```
   root@ns## tail -f ns.log.appfw
   ```

Hinweise:

- Wenn Sie Protokolle an eine andere Protokolldatei auf der lokalen NetScaler Appliance senden möchten, können Sie auf dieser lokalen NetScaler Appliance einen Syslog-Server erstellen. Fügen Sie `syslogaction` zu der eigenen IP hinzu und konfigurieren Sie den ADC so, als würden Sie einen externen Server konfigurieren. Der ADC fungiert als Server zum Speichern Ihrer Logs. Zwei Aktionen können nicht mit derselben IP und demselben Port hinzugefügt werden. In `syslogaction` ist der Wert von IP standardmäßig auf `127.0.0.1` und der Wert von Port auf `514` festgelegt.
- Wenn Sie die Syslog-Richtlinie so konfiguriert haben, dass die Protokolle an eine

> andere Protokolleinrichtung umgeleitet werden, werden die Web App Firewall-Protokollmeldungen nicht mehr in der `/var/log/ns.log` Datei angezeigt.

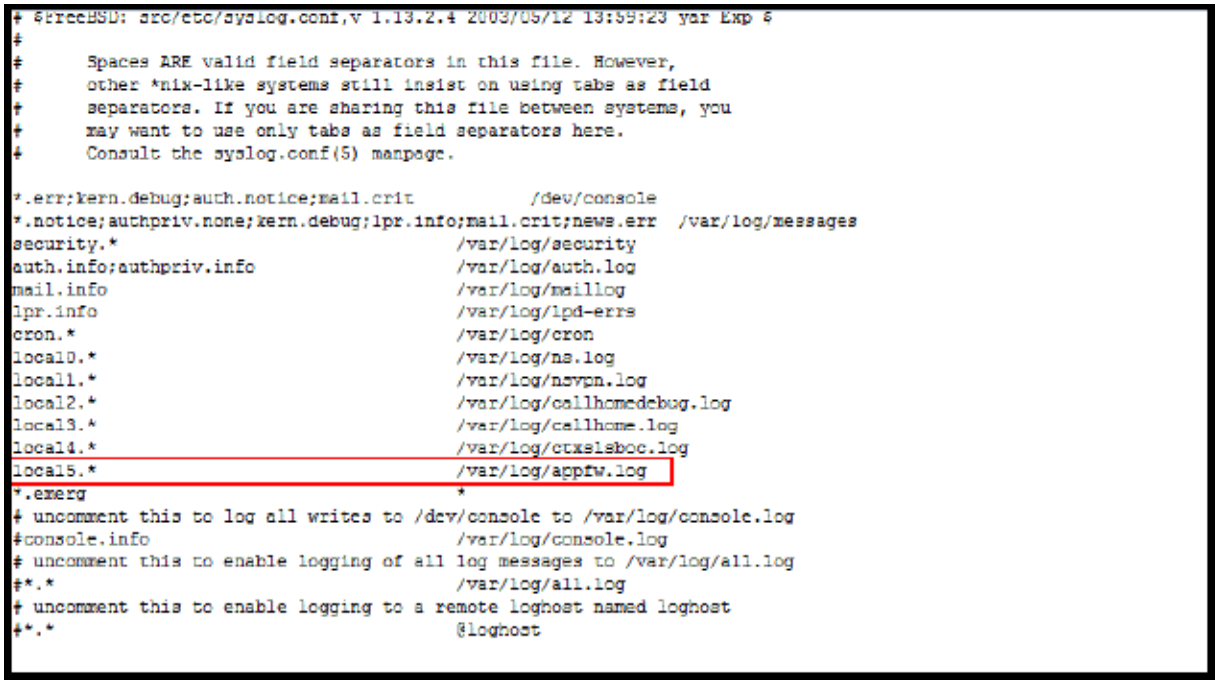
Senden der Application Firewall-Meldungen an einen separaten SYSLOG-Server

Um die Application Firewall-Meldungen an einen separaten SYSLOG-Server zu senden, müssen Sie die folgenden Schritte ausführen:

- Ein sicheres Dienstprogramm zur Dateiübertragung wie WinSCP
- Ein Dienstprogramm zum Öffnen einer SSH-Konsole für die Appliance wie PuTTY

Die folgenden Schritte sind erforderlich, um die Application Firewall-Meldungen an einen separaten SYSLOG-Server zu senden:

1. Melden Sie sich über WinSCP bei der NetScaler-Appliance an.
2. Aktualisieren Sie die Datei /etc/syslog.conf und fügen Sie der Datei folgende Zeile hinzu:
   `local5.* /var/log/appfw.log`

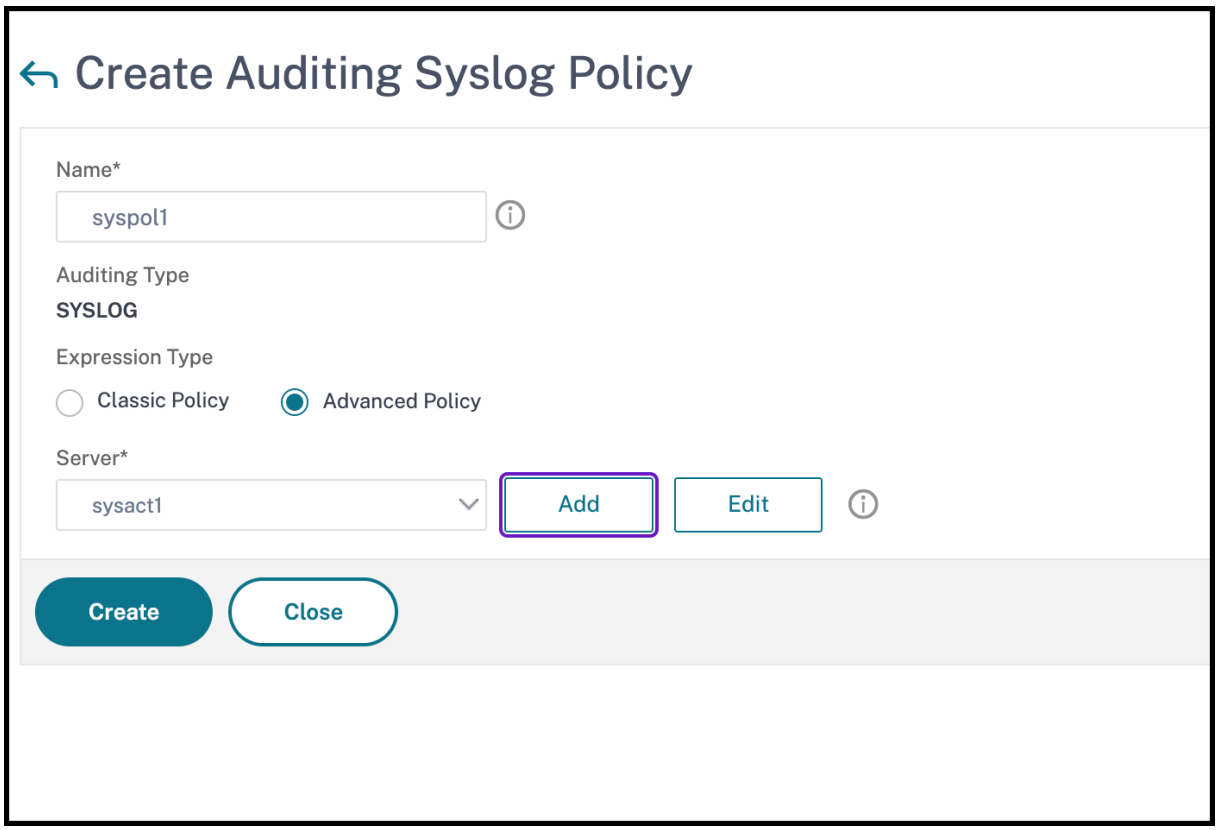


```
# $FreeBSD: src/etc/syslog.conf,v 1.13.2.4 2003/05/12 13:59:23 yar Exp $
#
#       Spaces ARE valid field separators in this file. However,
#       other *nix-like systems still insist on using tabs as field
#       separators. If you are sharing this file between systems, you
#       may want to use only tabs as field separators here.
#       Consult the syslog.conf(5) manpage.

*.err;kern.debug;auth.notice;mail.crit           /dev/console
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err  /var/log/messages
security.*                                      /var/log/security
auth.info;authpriv.info                         /var/log/auth.log
mail.info                                       /var/log/maillog
lpr.info                                        /var/log/lpd-errs
cron.*                                          /var/log/cron
local0.*                                        /var/log/ns.log
local1.*                                        /var/log/nsvpn.log
local2.*                                        /var/log/callhomedebug.log
local3.*                                        /var/log/callhome.log
local4.*                                        /var/log/ctxlsbcc.log
local5.*                                        /var/log/appfw.log
*.emerg                                         *
# uncomment this to log all writes to /dev/console to /var/log/console.log
#console.info                                   /var/log/console.log
# uncomment this to enable logging of all log messages to /var/log/all.log
#*.*                                            /var/log/all.log
# uncomment this to enable logging to a remote loghost named loghost
#*.*                                            @loghost
```

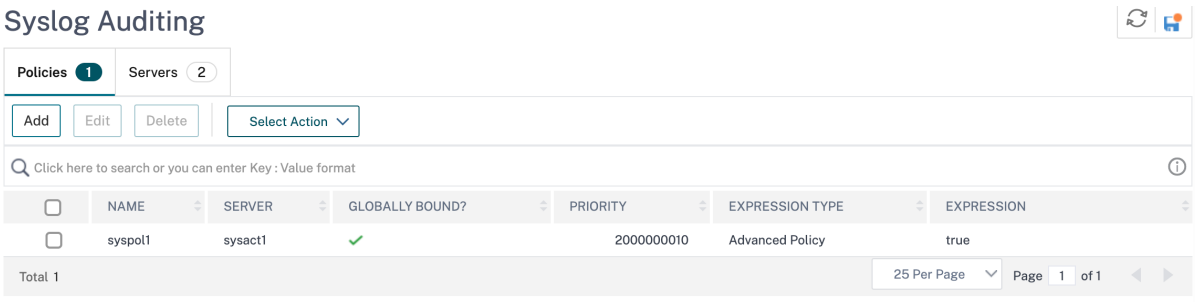
1. Führen Sie den folgenden Befehl über die Befehlszeilenschnittstelle aus, um die syslog PID neu zu starten:
   `kill -HUP <PID>`
2. Führen Sie den folgenden Befehl über die Befehlszeilenschnittstelle aus, um eine Syslog-Aktion wie sysact1 hinzuzufügen:
   `add audit syslogAction sysact1 127.0.0.1 -logLevel ALL -logFacility LOCAL5`

3. Führen Sie den folgenden Befehl aus, um die syspol1-Richtlinie hinzuzufügen, die den sysact1-Server verwendet:
   ```
   add audit syslogPolicy syspol1 ns_true sysact1
   ```
   Oder fügen Sie erweiterte Syslog-Richtlinien hinzu:
   ```
   add audit syslogPolicy syspol1 true sysact1
   ```



1. Führen Sie den folgenden Befehl aus, um die Anwendungs-Firewall-Richtlinie zu binden und sicherzustellen, dass sie in der Datei ns.conf gespeichert ist:
   ```
   bind appfw global syspol1 100
   ```
   Oder führen Sie den folgenden Befehl aus, um die Advanced Syslog-Richtlinie zu binden:

```
bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
APPFW_GLOBAL
```



Alle Verstöße gegen die Sicherheitsüberprüfung der Anwendungsfirewall werden an `/var/log/appfw.log` umgeleitet und werden nicht mehr in `ns.log` angezeigt. Sie können jetzt den Befehl tail ausführen und die neuesten Einträge in der anzeigen `/var/log/appfw.log`.

Web App Firewall-Protokolle anzeigen

Sie können die Protokolle anzeigen, indem Sie den Syslog-Viewer verwenden oder sich bei der NetScaler-Appliance anmelden, eine UNIX-Shell öffnen und den UNIX-Texteditor Ihrer Wahl verwenden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und schließen Sie die ns.logs im Ordner **/var/log/** an, um auf die Protokollmeldungen zuzugreifen, die sich auf Verstöße gegen die **Sicherheitsüberprüfung der Web App Firewall** beziehen:

- `Shell`
- `tail -f /var/log/ns.log`

Sie können den vi-Editor oder einen beliebigen Unix-Texteditor oder ein Textsuchwerkzeug verwenden, um die Protokolle nach bestimmten Einträgen anzuzeigen und zu filtern. Sie können den Befehl `grep` beispielsweise verwenden, um auf die Protokollmeldungen zuzugreifen, die sich auf die Kreditkartenverletzungen beziehen:

- `tail -f /var/log/ns.log | grep SAFECOMMERCE`

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die GUI enthält ein nützliches Tool (Syslog Viewer) zur Analyse der Logmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Um Protokollmeldungen für eine bestimmte Sicherheitsüberprüfung eines Profils anzuzeigen, navigieren Sie zu **Web App Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf Sicherheitsprüfungen. Markieren Sie die Zeile für die Zielsicherheitsprüfung und klicken Sie auf Protokolle. Wenn Sie direkt von der ausgewählten Sicherheitsüberprüfung des Profils auf die Protokolle zugreifen, filtert es die Protokollmeldungen heraus und zeigt nur die Protokolle an, die sich auf die Verletzungen für die ausgewählte Sicherheitsüberprüfung beziehen. Der Syslog-Viewer kann Web App Firewall-Protokolle im nativen Format und im CEF-Format anzeigen. Damit der Syslog-Viewer jedoch die zielprofilspezifischen Protokollmeldungen herausfiltern kann, müssen die Protokolle beim Zugriff über das Profil im CEF-Protokollformat vorliegen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link Syslog-Meldungen, um den Syslog-Viewer anzuzeigen, in dem alle Protokollmeldungen angezeigt werden, einschließlich aller Protokolle von Verstößen gegen die Sicherheitsüberprüfung der

Web App Firewall für alle Profile. Die Protokollmeldungen sind nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Verstöße gegen die Sicherheitsüberprüfung ausgelöst werden können.

- Navigieren Sie zu **Web App Firewall** > **Richtlinien** > **Auditing**. Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link Syslog-Meldungen, um den Syslog-Viewer anzuzeigen, in dem alle Protokollmeldungen einschließlich aller Protokolle von Sicherheitsüberprüfungen für alle Profile angezeigt werden.

Der HTML-basierte Syslog Viewer bietet die folgenden Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind:

- **Datei**— Die aktuelle Datei `/var/log/ns.log` ist standardmäßig ausgewählt, und die entsprechenden Meldungen werden im Syslog Viewer angezeigt. Eine Liste anderer Protokolldateien im /var/log-Verzeichnis ist in einem komprimierten.gz-Format verfügbar. Um eine archivierte Protokolldatei herunterzuladen und zu dekomprimieren, wählen Sie die Protokolldatei aus der Dropdown-Liste aus. Die Protokollmeldungen, die sich auf die ausgewählte Datei beziehen, werden dann im Syslog-Viewer angezeigt. Um die Anzeige zu aktualisieren, klicken Sie auf das Aktualisierungssymbol (ein Kreis aus zwei Pfeilen).
- **Modullistenfeld**—Sie können das NetScaler-Modul auswählen, dessen Protokolle Sie anzeigen möchten. Sie können es auf APPFW für Web App Firewall-Protokolle setzen.
- **Listenfeld Ereignisart**—Dieses Feld enthält eine Reihe von Kontrollkästchen zur Auswahl des Ereignistyps, an dem Sie interessiert sind. Um beispielsweise die Protokollmeldungen zu den Signaturverletzungen anzuzeigen, können Sie das Kontrollkästchen **APPFW_SIGNATURE_MATCH** aktivieren. In ähnlicher Weise können Sie ein Kontrollkästchen aktivieren, um die für Sie interessante Sicherheitsüberprüfung zu aktivieren. Sie können mehrere Optionen auswählen.
- **Schweregrad**—Sie können einen bestimmten Schweregrad auswählen, um nur die Protokolle für diesen Schweregrad anzuzeigen. Lassen Sie alle Kontrollkästchen leer, wenn Sie alle Protokolle sehen möchten.

  Um auf die Protokollmeldungen der Sicherheitsüberprüfung der Web App Firewall für eine bestimmte Sicherheitsüberprüfung zuzugreifen, filtern Sie, indem Sie in der Dropdown-Liste für Modul **APPFW** auswählen. Der Event-Typ zeigt eine Vielzahl von Optionen an, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_FIELDFORMAT** aktivieren und auf die Schaltfläche Übernehmen klicken, werden im Syslog Viewer nur Protokollnachrichten im Zusammenhang mit den Sicherheitsüberprüfungsverletzungen für Feldformate angezeigt. Wenn Sie die Kontrollkästchen **APPFW_SQL** und **APPFW_STARTURL** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog-Viewer nur Protokollmeldungen zu diesen beiden Verstößen gegen die Sicherheitsüberprüfung angezeigt.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollnachricht setzen, werden mehrere Op-

tionen wie **Module**, **EventType, EventID**oder**Message** unter der Protokollnachricht angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in den Protokollen hervorzuheben.

Highlights

- **Unterstützung des CEF-Protokollformats**— Die CEF-Protokollformat-Option bietet eine praktische Option zum Überwachen, Analysieren und Analysieren der Web App Firewall Protokollmeldungen, um Angriffe zu erkennen, konfigurierte Einstellungen zu optimieren, um Fehlalarme zu verringern und Statistiken zu sammeln.
- **Option zum Anpassen der Protokollnachricht**— Sie können erweiterte PI-Ausdrücke verwenden, um Protokollmeldungen anzupassen und die Daten, die Sie sehen möchten, in die Protokolle aufzunehmen.
- **Segregieren Sie Web App Firewall-spezifische Protokolle**— Sie haben die Möglichkeit, anwendungsfirewall-spezifische Protokolle zu filtern und in eine separate Protokolldatei umzuleiten.
- **Remote-Protokollierung**— Sie können die Protokollmeldungen an einen Remote-Syslog-Server umleiten.
- **Geolocation-Protokollierung**— Sie können die Web App Firewall so konfigurieren, dass sie die Geolocation des Bereichs einschließt, von dem aus die Anforderung empfangen wird. Eine eingebaute Geolokationsdatenbank ist verfügbar, aber Sie haben die Möglichkeit, eine externe Geolokationsdatenbank zu verwenden. Die NetScaler-Appliance unterstützt statische IPv4- und IPv6-Geolokationsdatenbanken.
- **Informationsreiche Protokollnachricht**— Im Folgenden finden Sie einige Beispiele für die Art der Informationen, die je nach Konfiguration in die Protokolle aufgenommen werden können:
  - Eine Web App Firewall-Richtlinie wurde ausgelöst.
  - Ein Verstoß gegen die Sicherheitsüberprüfung wurde ausgelöst.
  - Eine Anfrage wurde als missgebildet angesehen.
  - Eine Anfrage oder die Antwort wurde blockiert oder nicht blockiert.
  - Anforderungsdaten (wie SQL- oder Cross-Site-Scripting-Sonderzeichen) oder Antwortdaten (wie Kreditkartennummern oder sichere Objektzeichenfolgen) wurden transformiert.
  - Die Anzahl der Kreditkarten in der Antwort überschritt das konfigurierte Limit.
  - Die Kreditkartennummer und der Kreditkartentyp.
  - Die in den Signaturregeln konfigurierten Protokollzeichenfolgen und die Signatur-ID.
  - Geolokationsinformationen über die Quelle der Anfrage.
  - Maskierte (X) Benutzereingaben für geschützte vertrauliche Felder.

Maskieren Sie sensible Daten mit einem Regex-M

Die erweiterte Richtlinienfunktion (PI) `REGEX_REPLACE` in einem Protokollausdruck (gebunden an ein Web Application Firewall (WAF) -Profil) ermöglicht es Ihnen, sensible Daten in WAF-Protokollen zu maskieren. Sie können die Option verwenden, um Daten mithilfe eines Regex-Musters zu maskieren und ein Zeichen oder ein Zeichenfolgenmuster bereitzustellen, um die Daten zu maskieren. Sie können die PI-Funktion auch so konfigurieren, dass sie das erste Vorkommen oder alle Vorkommen des Regex-Musters ersetzt.

Standardmäßig bietet die GUI-Schnittstelle die folgende Maske:

- SSN
- Kreditkarte
- Kennwort
- Benutzername

Maskieren Sie sensible Daten in Web Application Firewall-

Sie können sensible Daten in WAF-Protokollen maskieren, indem Sie den erweiterten Richtlinienausdruck `REGEX_REPLACE` in dem an ein WAF-Profil gebundenen Protokollausdruck konfigurieren.
Um sensible Daten zu maskieren, müssen Sie die folgenden Schritte ausführen:

1. Hinzufügen eines Web Application Firewall-Profils
2. Binden Sie einen Protokollausdruck an das WAF-Profil

Hinzufügen eines Web Application Firewall-Profils

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appfw profile <name>
```

Beispiel:

```
Add appfw profile testprofile1
```

Binden eines Protokollausdrucks mit dem Web Application Firewall-Profil

Geben Sie an der Eingabeaufforderung Folgendes ein:

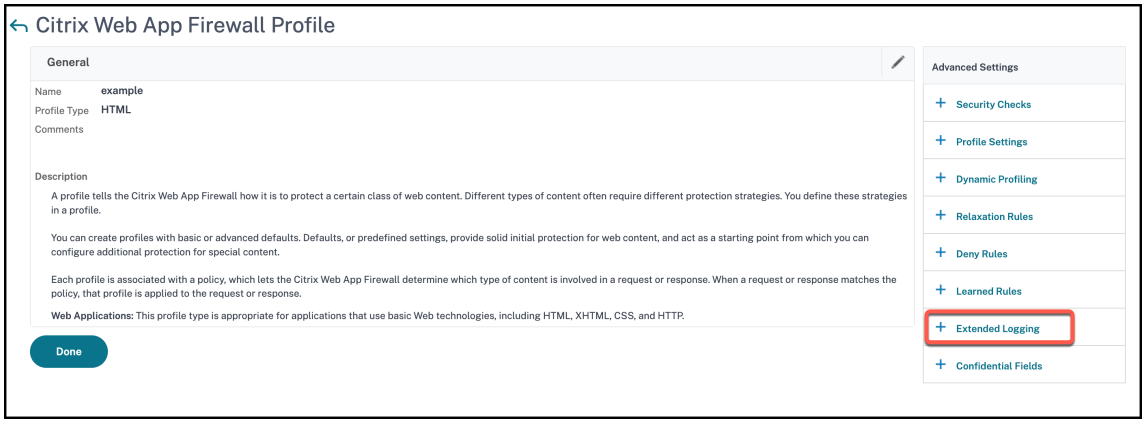
```
bind appfw profile <name> -logExpression <string> <expression> -comment <
string>
```

Beispiel:

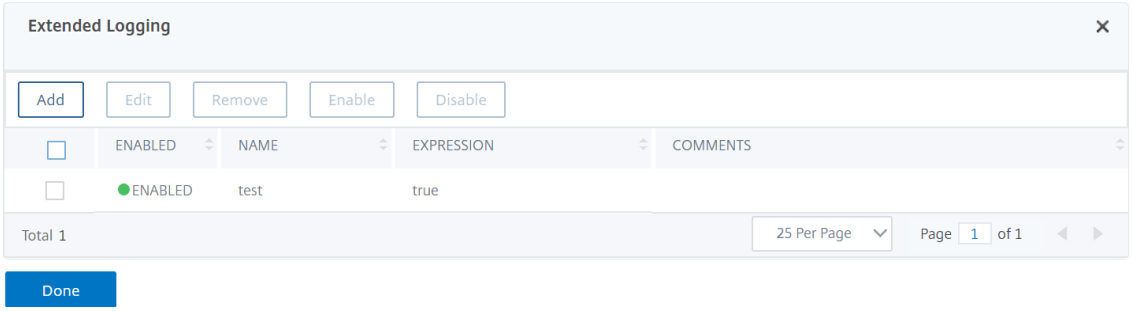
```
bind appfw profile testProfile -logExpression "MaskSSN""HTTP.REQ.BODY
(10000).REGEX_REPLACE(re!\b\d{ 3 } -\d{ 2 } -\d{ 4 } \b!, “xxx” , ALL)"-
comment "SSN Masked"
```


Maskieren Sie sensible Daten in Web Application Firewall-Protokollen über die NetScaler-GUI

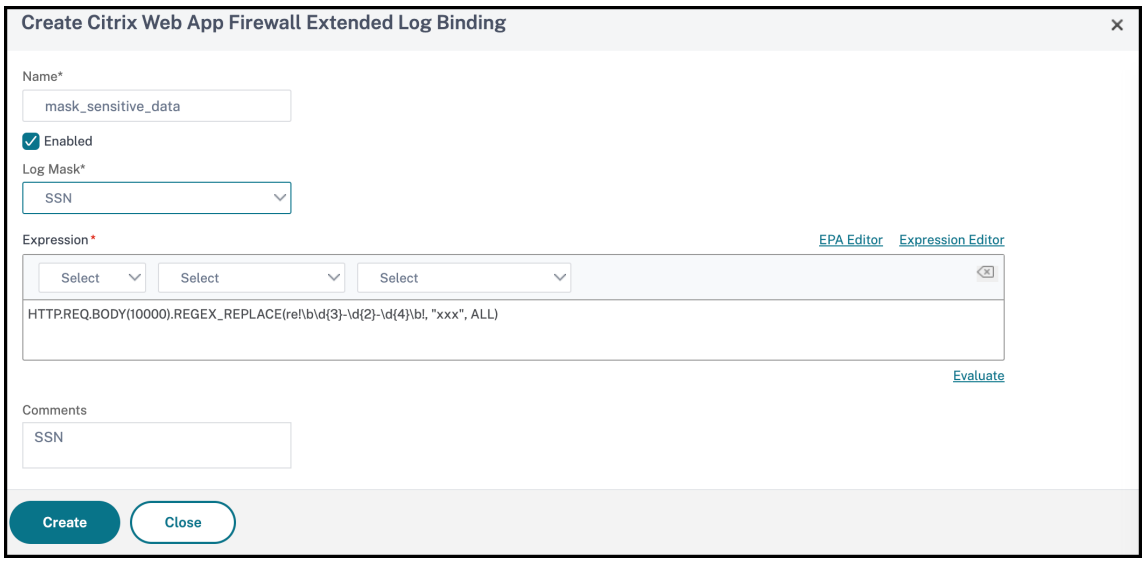
1. Erweitern Sie im Navigationsbereich **Sicherheit** > **NetScaler Web App Firewall** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Bearbeiten**.
3. Navigieren Sie auf der Seite **NetScaler Web App Firewall Profile** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Erweiterte Protokollierung**.



4. Klicken Sie im Abschnitt **Erweitertes Logging** auf **Hinzufügen**.



5. Legen Sie auf der Seite **Create NetScaler Web App Firewall Extended Log Binding** die folgenden Parameter fest:
   a) Name. Name des Protokollausdrucks.
   b) Aktiviert. Wählen Sie diese Option um sensible Daten zu maskieren.
   c) Log-Maske. Wählen Sie die zu maskierten Daten aus.
   d) Ausdruck. Geben Sie den erweiterten Richtlinienausdruck ein, mit dem Sie sensible Daten in WAF-Protokollen maskieren
   e) Kommentare. Kurze Beschreibung der Maskierung sensibler Daten.
6. Klicken Sie auf **Erstellen** und **Schließen**.



Anhänge

January 19, 2021

Das folgende ergänzende Material enthält zusätzliche Details zu komplexen oder peripheren Aufgaben der Web App Firewall.

PCRE-Zeichencodierungsformat

May 11, 2023

Das **NetScaler-Betriebssystem unterstützt nur die direkte** Eingabe von Zeichen im druckbaren ASCII-Zeichensatz — Zeichen mit Hexadezimalcodes zwischen HEX 20 (ASCII 32) und HEX 7E (ASCII 127). Um ein Zeichen mit einem Code außerhalb dieses Bereichs in Ihre Web App Firewall-Konfiguration aufzunehmen, müssen Sie seinen UTF-8-Hexadezimalcode als regulären PCRE-Ausdruck eingeben.

Viele Zeichentypen erfordern die Codierung mit einem regulären PCRE-Ausdruck, wenn Sie sie als URL, Formularfeldname oder Safe Object-Ausdruck in Ihre Web App Firewall-Konfiguration aufnehmen. Sie beinhalten:

- **Obere-ASCII-Zeichen.** Zeichen mit Kodierungen von HEX 7F (ASCII 128) bis HEX FF (ASCII 255). Abhängig von der verwendeten Zeichenzuordnung können sich diese Kodierungen auf Steuercodes, ASCII-Zeichen mit Akzenten oder anderen Modifikationen, nicht-lateinische Alphabet-

Zeichen und Symbole beziehen, die nicht im ASCII-Basissatz enthalten sind. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken vorkommen.

- **Doppelbyte-Zeichen.** Zeichen mit Kodierungen, die zwei 8-Byte-Wörter verwenden. Doppelbyte-Zeichen werden hauptsächlich für die Darstellung von chinesischem, japanischem und koreanischem Text in elektronischer Form verwendet. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken vorkommen.

  ASCII-Steuerzeichen. Nicht druckbare Zeichen, die zum Senden von Befehlen an einen Drucker verwendet werden. Alle ASCII-Zeichen mit Hexadezimalcodes kleiner als HEX 20 (ASCII 32) fallen in diese Kategorie. Diese Zeichen dürfen jedoch niemals in einem URL- oder Formularfeldnamen vorkommen und würden selten, wenn überhaupt, in einem sicheren Objektausdruck vorkommen.

Die NetScaler Appliance unterstützt nicht den gesamten UTF-8-Zeichensatz, sondern nur die Zeichen in den folgenden acht Zeichensätzen:

- **Englisch US (ISO-8859-1).** Obwohl das Etikett „English US“ lautet, unterstützt die Web App Firewall alle Zeichen des ISO-8859-1-Zeichensatzes, der auch als Latin-1-Zeichensatz bezeichnet wird. Dieser Zeichensatz repräsentiert vollständig die meisten modernen westeuropäischen Sprachen und repräsentiert alle bis auf einige ungewöhnliche Zeichen im Rest.
- **Traditionelles Chinesisch (Big5).** Die Web App Firewall unterstützt alle Zeichen im BIG5-Zeichensatz, der alle traditionellen chinesischen Schriftzeichen (Ideogramme) enthält, die im modernen Chinesisch häufig verwendet werden, wie sie in Hongkong, Macau, Taiwan und von vielen Menschen chinesischer ethnischer Herkunft, die außerhalb des chinesischen Festlandes leben, gesprochen und geschrieben werden.
- **Chinesisch vereinfacht (GB2312).** Die Web App Firewall unterstützt alle Zeichen im GB2312-Zeichensatz, der alle im modernen Chinesisch gebräuchlichen vereinfachten chinesischen Schriftzeichen (Ideogramme) enthält, wie sie auf dem chinesischen Festland gesprochen und geschrieben werden.
- **Japanisch (SJIS).** Die Web App Firewall unterstützt alle Zeichen im Shift-JIS (SJIS) - Zeichensatz, der die meisten Zeichen (Ideogramme) enthält, die üblicherweise im modernen Japanisch verwendet werden.
- **Japanisch (EUC-JP).** Die Web App Firewall unterstützt alle Zeichen im EUC-JP-Zeichensatz, einschließlich aller Zeichen (Ideogramme), die üblicherweise im modernen Japanisch verwendet werden.
- **Koreanisch (EUC-KR).** Die Web App Firewall unterstützt alle Zeichen im EUC-KR-Zeichensatz, einschließlich aller Zeichen (Ideogramme), die üblicherweise im modernen Koreanisch verwendet werden.

- **türkisch (ISO-8859-9).** Die Web App Firewall unterstützt alle Zeichen im ISO-8859-9-Zeichensatz, der alle im modernen Türkisch verwendeten Buchstaben umfasst.
- **Unicode (UTF-8).** Die Web App Firewall unterstützt bestimmte weitere Zeichen im UTF-8-Zeichensatz, einschließlich der Zeichen, die im modernen Russisch verwendet werden.

Bei der Konfiguration der Web App Firewall geben Sie alle Nicht-ASCII-Zeichen als reguläre Ausdrücke im PCRE-Format ein, indem Sie den Hexadezimalcode verwenden, der diesem Zeichen in der UTF-8-Spezifikation zugewiesen ist. Symbolen und Zeichen innerhalb des normalen ASCII-Zeichensatzes, dem in diesem Zeichensatz einstellige, zweistellige Codes zugewiesen sind, werden im UTF-8-Zeichensatz dieselben Codes zugewiesen. Zum Beispiel das Ausrufezeichen (!) , dem der Hexadezimalcode 21 im ASCII-Zeichensatz zugewiesen ist, ist auch Hex 21 im UTF-8-Zeichensatz. Symbolen und Zeichen aus einem anderen unterstützten Zeichensatz sind paarweise Hexadezimalcodes im UTF-8-Zeichensatz zugewiesen. Zum Beispiel wird dem Buchstaben a mit einem akuten Akzent (á) der UTF-8-Code C3 A1 zugewiesen.

Die Syntax, die Sie zur Darstellung dieser UTF-8-Codes in der Web App Firewall-Konfiguration verwenden, lautet „\ xNN“ für ASCII-Zeichen, „\ xNN\ xNN“ für Nicht-ASCII-Zeichen, die in Englisch, Russisch und Türkisch verwendet werden, und „\ xNN\ xNN\ xNN“ für Zeichen, die in Chinesisch, Japanisch und Koreanisch verwendet werden. Zum Beispiel, wenn Sie einen repräsentieren möchten! In einem regulären Ausdruck der Web App Firewall als UTF-8-Zeichen würden Sie\ x21 eingeben. Wenn Sie ein á einschließen möchten, geben Sie\ xC3\ xA1 ein.

> **Hinweis:**
>
> Normalerweise müssen Sie keine ASCII-Zeichen im UTF-8-Format darstellen, aber wenn diese Zeichen einen Webbrowser oder ein zugrunde liegendes Betriebssystem verwirren könnten, können Sie die UTF-8-Darstellung des Charakters verwenden, um diese Verwirrung zu vermeiden. Wenn eine URL beispielsweise ein Leerzeichen enthält, sollten Sie das Leerzeichen als\ x20 codieren, um bestimmte Browser und Webserversoftware nicht zu verwirren.

Im Folgenden finden Sie Beispiele für URLs, Formularfeldnamen und sichere Objektausdrücke, die Nicht-ASCII-Zeichen enthalten, die als reguläre Ausdrücke im PCRE-Format eingegeben werden müssen, um in die Konfiguration der Web App Firewall aufgenommen zu werden. Jedes Beispiel zeigt zuerst die tatsächliche URL, den Feldnamen oder die Ausdruckszeichenfolge, gefolgt von einem regulären Ausdruck im PCRE-Format.

- Eine URL mit erweiterten ASCII-Zeichen.

  Tatsächliche URL: `http://www.josénuñez.com`
  Verschlüsselte URL: `^http://www\[.\]jos\\xC3\\xA9nu\\xC3\\xB1ez\[.\]com$`

- Eine weitere URL mit erweiterten ASCII-Zeichen.

  Tatsächliche URL: `http://www.example.de/trömso.html`
  Verschlüsselte URL: `^http://www[.]example[.\]de/tr\xC3\xB6mso[.]html$`

Ein Formularfeldname mit erweiterten ASCII-Zeichen.

Aktueller Name: nome_do_usuário
Verschlüsselter Name: ^nome_do_usu\ xC3\ xA1rio$

- Ein sicherer Objektausdruck, der erweiterte ASCII-Zeichen enthält.

  Unkodierter Ausdruck [A-Z] {3,6} ¥[1-9\][0-9]{6,6}
  Kodierter Ausdruck: [A-Z] {3,6}\ xC2\ xA5 [1-9] [0-9] {6,6}

Sie können mehrere Tabellen finden, die den gesamten Unicode-Zeichensatz und passende UTF-8-Kodierungen im Internet enthalten. Eine nützliche Website, die diese Informationen enthält, ist in der folgenden Tabelle verfügbar.

http://www.utf8-chartable.de/unicode-utf8-table.pl

Damit die Zeichen in der Tabelle auf dieser Website korrekt angezeigt werden, muss auf Ihrem Computer eine entsprechende Unicode-Schriftart installiert sein. Wenn Sie dies nicht tun, ist die visuelle Anzeige des Charakters möglicherweise fehlerhaft. Auch wenn Sie keine entsprechende Schriftart installiert haben, um ein Zeichen anzuzeigen, sind die Beschreibung und die UTF-8- und UTF-16-Codes auf diesem Satz von Webseiten korrekt.

Whitehat-WASC-Signaturtypen für die WAF-Verwendung

May 11, 2023

Die NetScaler Web App Firewall akzeptiert und generiert Blockierungsregeln für alle Arten von Sicherheitslücken, die die Whitehat-Scanner generieren. Bestimmte Sicherheitslücken sind jedoch am besten auf eine Web App Firewall anwendbar. Im Folgenden finden Sie eine Liste dieser Sicherheitsanfälligkeiten, unterteilt danach, ob sie durch WASC 1.0-, WASC 2.0- oder Best Practices-Signaturtypen behoben wurden.

WASC 1.0-Signaturtypen

- Schmuggel von HTTP-Anfragen
- Aufteilung von HTTP-Antworten
- Schmuggel von HTTP-Antworten
- Null-Byte-Injektion
- Einbindung von Dateien aus der Ferne
- Missbrauch des URL-Redirectors

WASC 2.0-Signaturtypen

- Missbrauch von Funktionen
- Rohe Gewalt
- Spoofing von Inhalten
- Denial-of-Service-Angriff
- Verzeichnisindizierung
- Informationsleck
- Unzureichender Automatisierungsschutz
- Unzureichende Authentifizierung
- Unzureichende Autorisierung
- Unzureichender Sitzungsablauf
- LDAP-Injektion
- Fixierung der Sitzung

Bewährte Methoden

- Attribut „Automatisch vervollständigen“
- Unzureichende Cookie-Zugriffskontrolle
- Unzureichende Passwortstärke
- Ungültige Verwendung der HTTP-Methode
- Sitzungscookie, das kein HTTP ist
- Persistentes Sitzungscookie
- Personenbezogene Daten
- Gesicherte cache-HTTP-Nachrichten
- Unsicheres Session-Cookie

Streaming-Unterstützung für die Bearbeitung von Anfragen

May 11, 2023

Die NetScaler Web App Firewall unterstützt Streaming auf Anforderungsseite, um eine deutliche Leistungssteigerung zu erzielen Anstatt eine Anforderung zu puffern, untersucht die Appliance den eingehenden Datenverkehr auf Sicherheitsverletzungen wie SQL, Cross-Site Scripting, Feldkonsistenz und Feldformate. Wenn die Appliance die Verarbeitung der Daten für ein Feld abgeschlossen hat, wird die Anforderung an den Back-End-Server weitergeleitet, während die Appliance weiterhin andere Felder auswertet. Diese Datenverarbeitung verbessert die Verarbeitungszeit bei der Bearbeitung von Formularen erheblich.

Citrix empfiehlt, Streaming für Nutzlast-Inhalte mit mehr als 20 MB zu aktivieren. Außerdem muss der Back-End-Server die Chunked-Anforderungen akzeptieren, wenn das Streaming aktiviert ist.

> **Hinweis:**
>
> Die Aktion "Post-Body-Limit" ist immer auf "Blockieren" eingestellt und gilt sowohl für den Streaming- als auch für den Wenn der eingehende Datenverkehr größer als 20 MB ist, empfiehlt Citrix, den `PostBodyLimit` auf den erwarteten Wert zu konfigurieren.

Obwohl der Streaming-Prozess für die Benutzer transparent ist, sind aufgrund der folgenden Änderungen geringfügige Konfigurationsanpassungen erforderlich:

RegEx Pattern Match: Die RegEx-Musterübereinstimmung ist jetzt für zusammenhängende Zeichenfolgenübereinstimmungen auf 4K beschränkt.

Übereinstimmung mit Feldnamen: Das Lernmodul der Web App Firewall kann nur die ersten 128 Byte des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen hat, die eine identische Zeichenfolgenübereinstimmung für die ersten 128 Byte aufweisen, unterscheidet die Lernmaschine sie nicht. In ähnlicher Weise kann die eingesetzte Entspannungsregel versehentlich alle diese Felder lockern.

Das Entfernen von Leerräumen, die prozentuale Dekodierung, die Unicode-Dekodierung und die Zeichensatzkonvertierung werden während der Kanonisierung durchgeführt, um eine Sicherheitsüberprüfung zu ermöglichen. Das 128-Byte-Limit gilt für die kanonische Darstellung des Feldnamens im UTF-8-Zeichenformat. Die ASCII-Zeichen sind 1 Byte lang, aber die UTF-8-Darstellung der Zeichen in einigen internationalen Sprachen kann von 1 Byte bis 4 Byte reichen. Wenn jedes Zeichen in einem Namen 4 Byte für die Konvertierung in das UTF-8-Format benötigt, können nur die ersten 32 Zeichen im Namen durch die gelernte Regel unterschieden werden.

Feldkonsistenzprüfung: Wenn Sie die Feldkonsistenz aktivieren, werden alle Formulare in der Sitzung basierend auf dem von der Web App Firewall eingefügten "as_fid" -Tag gespeichert, ohne die "action_url" zu berücksichtigen.

- **Obligatorisches Formulartagging für Konsistenz im Formularfeld:** Wenn die Feldkonsistenzprüfung aktiviert ist, muss auch das Formulartag aktiviert sein Der Schutz vor Feldkonsistenz funktioniert möglicherweise nicht, wenn das Formulartagging ausgeschaltet ist.
- **Konsistenz von sitzungslosen Formularen:** Die Web App Firewall führt die Konvertierung von Formularen nicht mehr von "GET" nach "POST" durch, wenn der Parameter für die Feldkonsistenz ohne Sitzung aktiviert ist. Das Formulartag ist auch für die Konsistenz von Feldern ohne Sitzung erforderlich.
- **Manipulation von as_fid:** Wenn ein Formular nach der Manipulation von as_fid gesendet wird, wird eine Verletzung der Feldkonsistenz ausgelöst, selbst wenn kein Feld manipuliert wurde. Bei Nicht-Streaming-Anforderungen war dies zulässig, da die Formulare mithilfe der in der Sitzung gespeicherten "action_url" validiert werden können.

Signaturen: Die Signaturen haben jetzt die folgenden Spezifikationen:

- **Standort:** Es ist jetzt eine zwingende Anforderung, dass der Standort für jedes Muster angegeben werden muss. Alle Muster in der Regel **MÜSSEN** ein <Location>-Tag haben.
- **Schnelles Spiel:** Alle Signaturregeln müssen ein schnelles Übereinstimmungsmuster haben. Wenn es kein Fast-Match-Muster gibt, wird versucht, wenn möglich eines auszuwählen. Fast Match ist eine literale Zeichenfolge, PCRE kann aber für eine schnelle Übereinstimmung verwendet werden, wenn sie eine verwendbare Literalzeichenfolge enthält.
- **Veraltete Speicherorte:** Folgende Speicherorte werden in Signaturregeln nicht mehr unterstützt.
  - HTTP_ANY
  - HTTP_RAW_COOKIE
  - HTTP_RAW_HEADER
  - HTTP_RAW_RESP_HEADER
  - HTTP_RAW_SET_COOKIE

Cross-Site-Scripting/SQL Transform: Rohdaten werden für die Transformation verwendet, da die SQL-Sonderzeichen wie einfaches Anführungszeichen (‘), Backslash () und Semikolon (;)) sowie Cross-Site-Scripting-Tags identisch sind und keine Kanonisierung von Daten erfordern. Die Darstellung von Sonderzeichen wie HTML-Entity-Codierung, prozentuale Codierung oder ASCII wird für den Transformationsvorgang ausgewertet.

Die Web App Firewall prüft nicht mehr sowohl den Attributnamen als auch den Wert für die Cross-Site Scripting-Scripttransformation. Jetzt werden nur Cross-Site Scripting-Attributnamen umgewandelt, wenn Streaming aktiviert ist.

Verarbeitung von Cross-Site-Scripting-Tags: Im Rahmen der Streaming-Änderungen in NetScaler 10.5.e Build und höher wurde die Verarbeitung der Cross-Site-Scripting-Tags geändert. In früheren Versionen wurde das Vorhandensein einer offenen Klammer (<) oder einer schließenden Klammer (>) oder beiden (<>) als Cross-Site-Scripting-Verletzung gekennzeichnet. Das Verhalten hat sich ab Version 10.5.e geändert. Nur das Vorhandensein des Charakters in offener Klammer (<), or only the close bracket character (>) wird nicht mehr als Angriff betrachtet. Dies ist, wenn ein Charakter in offener Klammer (< is followed by a close bracket character (>), der Cross-Site-Scripting-Angriff markiert wird. Beide Zeichen müssen in der richtigen Reihenfolge (< followed by >) vorhanden sein, um die Cross-Site-Scripting-Verletzung auszulösen.

> **Hinweis:**
>
> **Meldung zur Änderung des SQL-Verstoßprotokolls:** Im Rahmen der Streaming-Änderungen in NetScaler ab Version 10.5.e verarbeiten wir die Eingabedaten jetzt in Blöcken. RegEx Pattern-Matching ist jetzt für zusammenhängende Zeichenfolgen auf 4K beschränkt. Mit dieser Änderung können die SQL-Verstoßprotokollmeldungen andere Informationen im Vergleich zu

> früheren Builds enthalten. Das Schlüsselwort und das Sonderzeichen in der Eingabe sind durch viele Byte getrennt. Die Appliance verfolgt die SQL-Schlüsselwörter und speziellen Zeichenfolgen bei der Verarbeitung der Daten, anstatt den gesamten Eingabewert zu puffern. Zusätzlich zum Feldnamen enthält die Protokollnachricht das SQL-Schlüsselwort, das SQL-Sonderzeichen oder sowohl das SQL-Schlüsselwort als auch das SQL-Sonderzeichen. Der Rest der Eingabe ist nicht mehr in der Protokollnachricht enthalten, wie im folgenden Beispiel gezeigt:
>
> **Beispiel:**
>
> In 10.5, wenn die Web App Firewall die SQL-Verletzung erkennt, ist möglicherweise die gesamte Eingabezeichenfolge in der folgenden Protokollmeldung enthalten:
>
> Die SQL-Schlüsselwortprüfung ist **text=”select a name from testbed1\;\(\;\)”.*<blocked>**
>
> In 11.0 protokollieren wir nur den Feldnamen, das Schlüsselwort und das Sonderzeichen (falls zutreffend) in der folgenden Protokollnachricht.
>
> SQL-Schlüsselwortprüfung für Feld fehlgeschlagen `text="select(;)"<blocked>`
>
> ****Diese Änderung gilt für Anfragen, die die Inhaltstypen **application/x-www-form-urlencoded, multipart/form-data oder text/x-gwt-rpc**enthalten.** **Protokollmeldungen, die während der Verarbeitung von **JSON** - oder **XML-Nutzdaten** generiert werden, sind von dieser Änderung nicht betroffen.

RAW POST Body: Die Inspektionen der Sicherheitskontrolle werden immer am RAW POST Körper durchgeführt.

Formular-ID: Die Web App Firewall hat das Tag “as_fid” eingefügt, bei dem es sich um einen berechneten Hash des Formulars handelt, das für die Benutzersitzung länger eindeutig ist. Es ist ein identischer Wert für ein bestimmtes Formular, unabhängig vom Benutzer oder der Sitzung.

Zeichensatz: Wenn eine Anforderung keinen Zeichensatz hat, wird der im Anwendungsprofil angegebene Standardzeichensatz bei der Verarbeitung der Anforderung verwendet.

Zähler:

Zähler mit dem Präfix “se” und “appfwreq” werden hinzugefügt, um die Streaming-Engine und die Streaming-Engine-Anforderungszähler zu verfolgen.

```
nsconsmg -d statswt0 -g se_err_

nsconsmg -d statswt0 -g se_tot_

nsconsmg -d statswt0 -g se_cur_

nsconsmg -d statswt0 -g appfwreq_err_

nsconsmg -d statswt0 -g appfwreq_tot_

nsconsmg -d statswt0 -g appfwreq_cur_
```


`_err counters`: zeigt das seltene Ereignis an, das erfolgreich gewesen sein muss, aber aufgrund eines Speicherzuweisungsproblems oder einer anderen Ressourcenkrise fehlgeschlagen ist.

`_tot counters`: immer größer werdende Zähler.

`_cur counters`: Zähler, die aktuelle Werte angeben, die sich basierend auf der Verwendung aus aktuellen Transaktionen ständig ändern.

Tipps:

- Die Sicherheitsüberprüfungen der Web App Firewall müssen genauso funktionieren wie zuvor.
- Für die Abwicklung der Sicherheitsüberprüfungen gibt es keine festgelegte Reihenfolge.
- Die Response-Side-Verarbeitung ist nicht betroffen und bleibt unverändert.
- Streaming ist nicht aktiviert, wenn ein clientloses VPN verwendet wird.

> **Wichtig:**
>
> **Berechnung der Cookie-Länge:** In Version 10.5.e wurde zusätzlich zu NetScaler Version 11.0 (in Builds vor 65.x) die Art der Verarbeitung des Cookie-Headers durch die Web App Firewall geändert. Die Appliance hat das Cookie einzeln ausgewertet, und wenn die Länge eines Cookies im Cookie-Header die konfigurierte Länge überschritt, wurde die Pufferüberlaufverletzung ausgelöst. Daher sind Anforderungen, die in der NetScaler 10.5-Version oder früheren Versionen blockiert wurden, möglicherweise zulässig. Die Länge des gesamten Cookie-Headers wird nicht für die Bestimmung der Cookie-Länge berechnet. In einigen Situationen kann die gesamte Cookie-Größe größer als der akzeptierte Wert sein, und der Server antwortet möglicherweise mit "400 Bad Request".
>
> **Hinweis:**
> Die Änderung wurde rückgängig gemacht. Das Verhalten von NetScaler Version 10.5.e bis Version 59.13xx.e und den nachfolgenden Builds ähnelt den Builds ohne Erweiterung von Version 10.5. Der gesamte rohe Cookie-Header wird jetzt bei der Berechnung der Länge des Cookies berücksichtigt. Umgebende Räume und die Semikolon-Zeichen (;), die die Name-Wert-Paare trennen, werden ebenfalls bei der Bestimmung der Cookie-Länge berücksichtigt.

Verfolgen Sie HTML-Anfragen mit Sicherheitsprotokollen

May 11, 2023

> **Hinweis:**
>
> Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

Die Fehlerbehebung erfordert die Analyse der in der Kundenanfrage erhaltenen Daten und kann eine Herausforderung sein. Vor allem, wenn viel Verkehr durch das Gerät fließt. Die Diagnose von Prob-

lemen kann die Funktionalität beeinträchtigen oder die Anwendungssicherheit erfordert möglicherweise eine schnelle Reaktion.

Der NetScaler isoliert den Datenverkehr für ein Web App Firewall-Profil und sammelt `nstrace` für die HTML-Anfragen. Die im Appfw-Modus `nstrace` gesammelten Informationen enthalten Anforderungsdetails mit Protokollnachrichten. Sie können im Trace „TCP-Stream folgen“ verwenden, um die Details der einzelnen Transaktion, einschließlich Header, Payload und der entsprechenden Lognachricht, auf demselben Bildschirm einzusehen.

So erhalten Sie einen umfassenden Überblick über Ihren Traffic. Eine detaillierte Ansicht der Anfrage, der Payload und der zugehörigen Protokolldatensätze kann hilfreich sein, um Verstöße gegen die Sicherheitsüberprüfung zu analysieren. Sie können das Muster, das den Verstoß auslöst, leicht identifizieren. Wenn das Muster zugelassen werden muss, können Sie entscheiden, ob Sie die Konfiguration ändern oder eine Relaxationsregel hinzufügen möchten.

Vorteile

1. **Datenverkehr für ein bestimmtes Profil isolieren**: Diese Erweiterung ist nützlich, wenn Sie den Datenverkehr nur für ein Profil oder für bestimmte Transaktionen eines Profils zur Problembehandlung isolieren. Sie müssen nicht mehr die gesamten im Trace gesammelten Daten durchsuchen oder spezielle Filter benötigen, um Anfragen, die Sie interessieren, zu isolieren, was bei hohem Datenverkehr mühsam sein kann. Sie können die Daten einsehen, die Sie bevorzugen.
2. **Daten für bestimmte Anfragen sammeln**: Der Trace kann für eine bestimmte Dauer gesammelt werden. Sie können die Nachverfolgung nur für einige Anfragen erfassen, um bei Bedarf bestimmte Transaktionen zu isolieren, zu analysieren und zu debuggen.
3. **Identifizieren Sie Resets oder Abbrüche**: Unerwartetes Schließen von Verbindungen ist nicht leicht sichtbar. Der im Modus —appfw gesammelte Trace erfasst einen Reset oder einen Abbruch, ausgelöst durch die Web App Firewall. Auf diese Weise können Sie ein Problem schneller isolieren, wenn Sie keine Meldung über einen Verstoß gegen die Sicherheitsüberprüfung sehen. Fehlerhafte Anfragen oder andere nicht RFC-konforme Anfragen, die von der Web App Firewall beendet wurden, sind jetzt einfacher zu identifizieren.
4. **Entschlüsselten SSL-Verkehr anzeigen: Der**HTTPS-Verkehr wird im Klartext erfasst, um die Fehlerbehebung zu erleichtern.
5. **Bietet einen umfassenden Überblick**: Ermöglicht es Ihnen, die gesamte Anfrage auf Paketebene, die Payload und die Protokolle zu überprüfen, um zu überprüfen, welche Sicherheitsüberprüfung ausgelöst wurde, und das Übereinstimmungsmuster in der Payload zu ermitteln. Wenn die Payload aus unerwarteten Daten, Junk-Strings oder nicht druckbaren Zeichen (Nullzeichen,\ r oder\ n usw.) besteht, sind diese im Trace leicht zu erkennen.
6. **Konfiguration ändern**: Das Debugging kann nützliche Informationen liefern, um zu entscheiden, ob das beobachtete Verhalten das richtige Verhalten ist oder ob die Konfiguration geändert werden muss.

7. **Verkürzte Reaktionszeit**: Durch ein schnelleres Debuggen des Zieldatenverkehrs kann die Reaktionszeit verbessert werden, sodass das NetScaler Engineering- und Support-Team Erklärungen oder Ursachenanalysen bereitstellen kann.

Weitere Informationen finden Sie unter Manuelle Konfiguration mithilfe des Themas der Befehlszeilenschnittstelle .

So konfigurieren Sie die Debug-Ablaufverfolgung für ein Profil mit der Befehlszeilenschnittstelle

Schritt 1. Aktiviere ns-Trace.

Sie können den Befehl show verwenden, um die konfigurierte Einstellung zu überprüfen.

- `set appfw profile <profile> -trace ON`

Schritt 2. Sammle Spuren. Sie können weiterhin alle Optionen verwenden, die für den `nstrace` Befehl gelten.

- `start nstrace -mode APPFW`

Schritt 3. Stoppen Sie die Spur.

- `stop nstrace`

Ort des Traces: Der`nstrace` wird in einem Ordner mit Zeitstempel gespeichert, der im Verzeichnis /var/nstrace erstellt wird und mit dem Befehl eingesehen werden kann. `wireshark` Sie können das nachverfolgen `/var/log/ns.log`, um die Protokollmeldungen mit Details zum Standort des neuen Trace zu sehen.

Tipps:

- Wenn die appfw-Modusoption verwendet wird, sammelt `nstrace` nur die Daten für ein oder mehrere Profile, für die das “nstrace” aktiviert wurde.
- Wenn Sie den Trace im Profil aktivieren, werden die Traces nicht automatisch erfasst, bis Sie explizit den Befehl „start ns trace“ ausführen, um den Trace zu sammeln.
- Die Aktivierung von Trace für ein Profil hat zwar möglicherweise keine negativen Auswirkungen auf die Leistung der Web App Firewall, aber Sie sollten diese Funktion möglicherweise nur für die Dauer aktivieren, für die Sie die Daten sammeln möchten. Es wird empfohlen, das —trace-Flag zu deaktivieren, nachdem Sie den Trace erfasst haben. Die Option verhindert das Risiko, versehentlich Daten aus Profilen abzurufen, für die Sie dieses Kennzeichen in der Vergangenheit aktiviert hatten.
- Die Block- oder Log-Aktion muss aktiviert sein, damit die Sicherheitsüberprüfung für den Transaktionsdatensatz in die aufgenommen werden kann `nstrace`.
- Resets und Abbrüche werden unabhängig von den Aktionen der Sicherheitsüberprüfungen protokolliert, wenn Trace für die Profile auf „On“ steht.

- Die Funktion ist nur für die Behebung der vom Client eingegangenen Anfragen geeignet. Die Traces im Modus —appfw beinhalten nicht die vom Server empfangenen Antworten.
- Sie können weiterhin alle Optionen verwenden, die für den `nstrace` Befehl gelten. Zum Beispiel

  ```
  start nstrace -tcpdump enabled -size 0 -mode appFW
  ```

- Wenn eine Anfrage mehrere Verstöße auslöst, enthält der Datensatz `nstrace` für diesen Datensatz alle entsprechenden Logmeldungen.
- Das CEF-Protokollnachrichtenformat wird für diese Funktion unterstützt.
- Signaturverstöße, die Block- oder Log-Aktionen für anforderungsseitige Überprüfungen auslösen, werden ebenfalls in die Protokollierung aufgenommen.
- Im Ablaufverfolgungsprotokoll werden nur HTML-Anforderungen (Nicht-XML) erfasst.

Web App Firewall-Unterstützung für Clusterkonfigurationen

May 11, 2023

> **Hinweis:**
>
> Die NetScaler Web App Firewall für Striped und teilweise Striped Konfigurationen wurde in der NetScaler 11.0-Version eingeführt.

Ein Cluster ist eine Gruppe von NetScaler-Appliances, die als einzelnes System konfiguriert und verwaltet werden. Jede Appliance im Cluster wird als Knoten bezeichnet. Abhängig von der Anzahl der Knoten, auf denen die Konfigurationen aktiv sind, werden Clusterkonfigurationen als gestreifte, teilweise gestreifte oder gepunktete Konfigurationen bezeichnet. Die Web App Firewall wird in allen Konfigurationen vollständig unterstützt.

Die beiden Hauptvorteile der Unterstützung Striped und teilweise Striped virtueller Server in Clusterkonfigurationen sind die folgenden:

1. Unterstützung für Sitzungs-Failover — Gestreifte und teilweise Striped virtuelle Serverkonfigurationen unterstützen Sitzungs-Failover. Die fortschrittlichen Sicherheitsfunktionen der Web App Firewall, wie das Schließen der Start-URL und die Konsistenzprüfung von Formularfeldern, verwalten und verwenden Sitzungen während der Transaktionsverarbeitung. Wenn in einer Hochverfügbarkeitskonfiguration oder in einer Spotte-Cluster-Konfiguration der Knoten, der den Web App Firewall-Verkehr verarbeitet, ausfällt, gehen alle Sitzungsinformationen verloren und der Benutzer muss die Sitzung erneut einrichten. In Striped virtuellen Serverkonfigurationen werden Benutzersitzungen über mehrere Knoten repliziert. Wenn ein Knoten ausfällt, wird

ein Knoten, auf dem das Replikat ausgeführt wird, Eigentümer. Sitzungsinformationen werden ohne sichtbare Auswirkungen auf den Benutzer verwaltet.

2. Skalierbarkeit — Jeder Knoten im Cluster kann den Datenverkehr verarbeiten. Mehrere Knoten des Clusters können die eingehenden Anfragen verarbeiten, die vom virtuellen Stripe-Server bedient werden. Dies verbessert die Fähigkeit der Web App Firewall, mehrere Anfragen gleichzeitig zu verarbeiten, wodurch die Gesamtleistung verbessert wird.

Sicherheitsprüfungen und Signaturschutz können bereitgestellt werden, ohne dass eine zusätzliche clusterspezifische Web App Firewall-Konfiguration erforderlich ist. Sie können die übliche Web App Firewall-Konfiguration auf dem CCO-Knoten (Configuration Coordinator) für die Weitergabe an alle Knoten vornehmen.

> **Hinweis:**
>
> Die Sitzungsinformationen werden auf mehrere Knoten repliziert, jedoch nicht auf allen Knoten in der Striped Konfiguration. Daher berücksichtigt die Failover-Unterstützung eine begrenzte Anzahl gleichzeitiger Ausfälle. Wenn mehrere Knoten gleichzeitig ausfallen, verliert die Web App Firewall möglicherweise die Sitzungsinformationen, falls ein Fehler auftritt, bevor die Sitzung auf einem anderen Knoten repliziert wird.

Highlights

- Die Web App Firewall bietet Skalierbarkeit, hohen Durchsatz und Unterstützung für Sitzungs-Failover in Cluster-Bereitstellungen.
- Alle Sicherheitsprüfungen und Signaturschutzmaßnahmen der Web App Firewall werden in allen Clusterkonfigurationen unterstützt.
- Charakterkarten werden für einen Cluster noch nicht unterstützt. Die Lernengine empfiehlt Feldtypen in erlernten Regeln für die Feldformat-Sicherheitsprüfung.
- Statistiken und gelernte Regeln werden aus allen Knoten in einem Cluster zusammengefasst.
- Distributed Hash Table (DHT) sorgt für das Zwischenspeichern der Sitzung und bietet die Möglichkeit, Sitzungsinformationen auf mehreren Knoten zu replizieren. Wenn eine Anfrage an den virtuellen Server geht, erstellt die NetScaler-Appliance Web App Firewall-Sitzungen im DHT und kann die Sitzungsinformationen auch vom DHT abrufen.
- Clustering ist mit den Lizenzen Advanced und Premium lizenziert. Diese Funktion ist mit der Standardlizenz nicht verfügbar.

Debuggen und Fehlerbehebung

January 21, 2021

Lesen Sie die folgenden Informationen zur Fehlerbehebung und zum Debuggen in Bezug auf die einzelnen Funktionen der Web App Firewall:

- Anwendungs-Firewall - Hohe CPU
- Speicher
- Fehler beim Hochladen großer Dateien
- Lernen
- Signaturen
- Ablaufverfolgungsprotokoll
- Sonstiges

Hohe CPU

May 11, 2023

Im Folgenden sind einige der aufgetretenen Debugging-Probleme im Zusammenhang mit Funktionen und hoher CPU-Auslastung sowie die bewährten Methoden aufgeführt, die Sie bei der Arbeit mit der Web App Firewall beachten sollten:

Überprüfen Sie die Richtlinientreffer, die Bindungen, die Netzwerkkonfiguration und die Konfiguration der Web App Firewall:

- Identifizieren Sie eine Fehlkonfiguration
- Identifizieren Sie den *vServer*, der den betroffenen Verkehr bedient

Überprüfen Sie die Protokolle in den folgenden Protokolldateien auf Sicherheitsverletzungen und aktuelle Konfigurationsänderungen:

- `/var/log/ns.log`
- `/var/nslog/import.log`
- `/var/nslog/aslearn.log`
- `tail -f /var/log/ns.log | grep APPFW_SIGNATURE_MATCH`

Beispiel:

```
1 Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
     .0|APPFW| APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method
     =GET request= http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=
     Signature violation rule ID 807: web-cgi /wwwboard/passwd.txt access
      cn1=140 cn2=841 cs1=pr_ffc cs2=PPE0 cs3=
     OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
     not blocked
2 <!--NeedCopy-->
```


Isolieren Sie den betroffenen Verkehr:

- Isolieren Sie das Profil
- Isolieren Sie die Sicherheitsüberprüfung
- Isolieren Sie die URL, den virtuellen Server und die Verkehrsparameter

Die konditionelle Verfolgung auf Profilebene hilft bei der Identifizierung von Datenverkehr und Verstößen:

- `set appfw profile <profile> -trace ON`
- `start nstrace -mode APPFW -size 0`
- `stop nstrace`

Hinweis: Stellen Sie sicher, dass der Trace mit der Option -size 0 erfasst wird.

Überprüfen Sie die Aktivitätsindikatoren für appfw, dht und IP-Reputation:

- `nsconmsg -g as_ -g appfwreq_ -g iprep -d current`

Bildschirmfenstergröße für Resets im Anschluss:

Appfw setzt die Fenstergröße auf 9845, wenn NetScaler die Verbindung aufgrund einer ungültigen HTTP-Nachricht zurücksetzt.

Beispiele:

- Falsch formatierte Anfrage empfangen — Verbindung zurückgesetzt
- Probleme im Zusammenhang mit hoher CPU-Auslastung
- Überprüfen Sie die Datenblätter auf die Systemgrenzen
- Überprüfen Sie, ob CPU-Auslastung, Appfw, DHT und speicherbezogene Aktivitäten vorliegen. Appfw-Sitzungen überwachen
- nsconmsg -g cc_cpu_use -g appfwreq -g als -g dht -g mem_as_obj -g MEM_AS_Component -d aktuell

Überwachen Sie den Speicher, der während des Zielzeitraums zugewiesen und von Web App Firewall-Komponenten und -Objekten freigegeben wurde. Es hilft dabei, den Schutz zu isolieren, was zu einer hohen CPU-Auslastung führt.

- Profiler-Ausgang
- Protokolle beobachten

Isolieren Sie die Appfw-Überprüfung, die zu einer hohen CPU-Auslastung führt:

- URL-Schließung starten
- Konsistenz der Formularfelder
- CSRF
- Cookie-Schutz
- Überprüfung des Referer-Headers

Stellen Sie sicher, dass das automatische Update von Signaturen nicht zu einer hohen CPU führt (Deaktivieren, um zu bestätigen).

Speicher

January 19, 2021

Im Folgenden finden Sie einige der bewährten Methoden, die Sie bei Problemen mit der Verwendung des Speichers der Web App Firewall beachten sollten:

Verwendung des Befehls nsconmsg:

- Suchen Sie nach globalen Speicherstatistiken, um festzustellen, dass genügend Speicher im System vorhanden ist und keine Speicherzuordnungsfehler auftreten, indem Sie den folgenden Befehl ausführen:

  ```
  * *- nsconmsg -d memstats
  ```

- Beachten Sie die aktuell zugewiesenen und maximalen Speichergrenzen für Appsecure, IP-Reputation, Cache und Komprimierung, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -d memstats | egrep -i APPSECURE|IPREP|CACHE|CMP
  ```

- Überprüfen Sie appfw, DHT, IP-Reputation Aktivitätszähler, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g as -g appfwreq_ -g iprep -d current
  ```

- Überprüfen Sie alle Fehlerindikatoren der Web App Firewall, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g as_ -g appfwreq_ -g iprep_ -d stats | grep err
  ```

- Überprüfen Sie alle Systemfehlerindikatoren, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g err -d current
  ```

- Prüfen Sie nach CPU-, APPFWREQ-, AS-und DHT-Leistungsindikatoren, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -d current
  ```

- Überprüfen Sie den konfigurierten Cache-Speicher, indem Sie den folgenden Befehl ausführen:
- `show cacheparameter`
- Überprüfen Sie den konfigurierten Speicher, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -d memstats | egrep -i CACHE
  ```


- Identifizieren der Speicherverteilung in Komponenten und Objekten der Web App Firewall:

AS_OBJ_-Speicher anzeigen:

```
nsconmsg -K newnslog -d stats | grep AS_OBJ | egrep -v AppFW_cpu0|total |
sort -k3
```

AS_COMPONENT_Speicher anzeigen:

```
nsconmsg -K newnslog -d stats | grep AS_COMPONENT | egrep -v AppFW_cpu0|
total | sort -k3
```

Überprüfen Sie die Anzahl der lebenden Sitzungen, indem Sie den folgenden Befehl ausführen:

Monitor/Plotten der aktiven Sitzung:

```
nsconmsg -g as_alive_sessions -d current
```

Monitor/Plot insgesamt zugewiesene, kostenlose, aktualisierte Sitzungen:

- `nsconmsg -g as_tot_alloc_sessions -g as_tot_free_sessions -d current`
- `nsconmsg -g as_tot_update_sessions -d current`

Reduzieren Sie bei Bedarf das Sitzungszeitlimit, um sicherzustellen, dass Sitzungslimits nicht verwendet werden, indem Sie den folgenden Befehl ausführen:

```
set appfwsettings -sessionTimeout <300>
```

Legen Sie bei Bedarf die maximale Lebensdauer der Sitzung fest, indem Sie den folgenden Befehl ausführen:

```
set appfwsettings -sessionLifetime <7200>
```

Überprüfen des zugewiesenen und genutzten Speichers

So überprüfen Sie den gesamten zugewiesenen Speicher und den verwendeten Speicher:

- Verwenden Sie den Befehl **nsconmsg —d memstats** . Beachten Sie das Feld **MEM_APPSECURE** .
- Verwenden Sie den Befehl **stat appfw**, um Informationen über den Verbrauch zu erhalten.

Die Web App Firewall löscht die Protokolle nach einer bestimmten Zeit oder Größe nicht automatisch.

- `All AppFw logs are archived in the */var/log/ns.log*` -Datei. Die Datei *ns.log* führt den Rollover-Task aus.

Weitere Informationen finden Sie unter folgendem Link:<http://support.citrix.com/article/CTX121898>

Erhöhen des Speichers der Web App Firewall:

- Es gibt keine CLI-Option, um den Speicher der Web App Firewall zu erhöhen. Der Web App Firewall -Speicher ist plattformspezifisch.
- Sie können die Option *nsapimgr* verwenden, um den Speicher zu erhöhen, dies wird jedoch nicht empfohlen.

Der maximal zulässige Speicher für die Web App Firewall wird von der Plattform bestimmt, und das Deaktivieren des IC wirkt sich nicht auf die Speicherzuweisung aus.

Fehler beim Hochladen großer Dateien

January 19, 2021

Wenn große Fehler beim Hochladen von Dateien auftreten, stellen Sie sicher, dass Sie Folgendes überprüfen:

— Falsch konfigurierte Anwendungsfirewall Postbody-Grenze
— Aktiviert das Scannen von Dateien, was zu einer erhöhten Verarbeitungszeit führt.
— Erledigen von Systemgrenzen.

Für Nutzlasten mit mehr als 20 MB empfiehlt Citrix, das Streaming auf dem Firewallprofil der Anwendung zu aktivieren. Außerdem müssen Sie sicherstellen, dass der Backend-Server Chunked Requests unterstützt, bevor Sie das Streaming aktivieren.

Seit Release 11.0 kann das Streaming-Flag auf Profilbasis aktiviert werden, um Puffern zu vermeiden, indem Sie den folgenden Befehl ausführen:

```
set appfw profile <profile name> -streaming on
```

Lernen

January 19, 2021

Im Folgenden finden Sie einige der empfohlenen Best Practices, wenn Probleme mit der Lernfunktionalität auftreten:

Aslearn Prozess:

- Stellen Sie sicher, dass der Prozess *aslearn* ausgeführt wird.
- Top-Befehlsausgabe prüfen
- Überprüfen Sie die Ausgabe von ps Befehl, indem Sie den folgenden Befehl ausführen:

  ```
  ps -ax | grep aslearn | grep -v "grep"
  ```


Beispiel:

```
root@ns# ps -ax | grep aslearn | grep -v "grep"
1439  ??  Ss     0:03.86 /netscaler/aslearn -start -f /netscaler/
   aslearn.conf
<!--NeedCopy-->
```

- Identifizieren Sie die letzten Konfigurationsbefehle, die vor dem beobachteten Problem ausgeführt wurden, indem Sie die Datei *ns.log* überprüfen:

  `/var/log/ns.log`

- Prüfen Sie aslearn Protokolle, um nach aslearn Nachrichten zu suchen:

  `/var/log/aslearn.log`

- Isolieren des Profils und der Sicherheitsüberprüfung, die durchgeführt wird
- Identifizieren Sie den GUI- und CLI-Befehl, der fehlschlägt, indem Sie den folgenden Befehl ausführen:

  `show appfw learningdata <profileName> <securityCheck>`

  Beispiele:

  - `show learningdata test_profile starturl`
  - `show learningdata test_profile crosssiteScripting`
  - `show learningdata test_profile sqLInjection`
  - `show learningdata test_profile csRFtag`
  - `show learningdata test_profile fieldformat`
  - `show learningdata test_profile fieldconsistency`

- Führen Sie die Integritätsprüfung von sqlite von der bsd Shell-Eingabeaufforderung durch:

  `nsshell ## sqlite3 /var/nslog/asl/<profile_name_in_lowercase>.db ' pragma integrity_check;`

  Beispiele:

```
root@ns# sqlite3 /var/nslog/asl/tsk0247284.db 'pragma
   integrity_check;'
ok
<!--NeedCopy-->
```

- Bereitstellen oder Entfernen von Regeln, um wieder mit dem Lernen zu beginnen:
  - Wenn 2000 Lernelemente (pro Schutz) erreicht sind, können Sie für diesen Schutz nicht mehr lernen.

  - Wenn eine Größe von 20 MB für die Datenbank erreicht wird, beenden Sie das Lernen für alle Schutzmaßnahmen
  - Neustart des aslearn-Prozesses

```
*/netscaler/aslearn -start -f/netscaler/aslearn.conf*
```

- Überprüfen Sie den Speicherplatz im Ordner /var, indem Sie Folgendes ausführen:

```
du -h /var
```

- Überprüfen Sie die Grenzwerte für Lernschwellenwerte, indem Sie den folgenden Befehl ausführen:

```
show appfwlearningsettings <profile_name> <securityCheck>
```

- Sammeln Sie gelernte Daten, indem Sie den folgenden Befehl ausführen:

```
export appfwlearningdata <profile_name> <securityCheck>
```

- Stellen Sie sicher, dass erlernte Daten in den Collector hochgeladen werden.

Signaturen

January 19, 2021

Erste Schritte mit Signaturen

So fügen Sie Signatur hinzu:

1. Wählen Sie die **Standardsignatur**aus, und klicken Sie auf **Hinzufügen**, um eine Kopie zu erstellen.
2. Geben Sie einen aussagekräftigen Namen. Das neue SIG-Objekt wird als Benutzerdefiniertes Objekt hinzugefügt.
3. Aktivieren Sie die Zielregeln, die Ihren spezifischen Anforderungen entsprechen.
   - Die Regeln sind standardmäßig deaktiviert.
   - mehr Regeln erfordern mehr Verarbeitung
4. Konfigurieren Sie die Aktionen:

   Block- und Protokollaktionen sind standardmäßig aktiviert. Statistik ist eine weitere Option
5. Legen Sie die Signatur fest, die von Ihrem Profil verwendet werden soll.

Tipps zur Verwendung von Signaturen

- Optimieren Sie den Verarbeitungsaufwand, indem Sie nur die Signaturen aktivieren, die zum Schutz Ihrer Anwendung anwendbar sind.
- Jedes Muster in der Regel muss übereinstimmen, um eine Signaturübereinstimmung auszulösen.
- Sie können eigene benutzerdefinierte Regeln hinzufügen, um eingehende Anforderungen zu überprüfen, um verschiedene Arten von Angriffen zu erkennen, wie SQL-Injection oder Cross-Site-Skripting-Angriffe.
- Sie können auch Regeln hinzufügen, um die Antworten zu überprüfen, um das Auslaufen vertraulicher Informationen wie Kreditkartennummern zu erkennen und zu blockieren.
- Fügen Sie mehrere Sicherheitsüberprüfungsbedingungen hinzu, um Ihre eigene benutzerdefinierte Prüfung zu erstellen.

Best Practices für die Verwendung von Signaturen

Im Folgenden finden Sie einige der bewährten Methoden, die Sie bei Problemen im Zusammenhang mit Signaturen befolgen können:

- Stellen Sie sicher, dass der Importbefehl sowohl für primäre als auch für sekundäre erfolgreich war.
- Überprüfen Sie, ob CLI- und GUI-Ausgaben konsistent sind.
- Überprüfen Sie ns.log, um Fehler beim Signaturimport und beim automatischen Update zu identifizieren.
- Überprüfen Sie, ob der DNS-Nameserver ordnungsgemäß konfiguriert ist.
- Überprüfen Sie die Inkompatibilität der Schemaversion.
- Überprüfen Sie, ob das Gerät nicht auf die Signaturaktualisierungs-URL zugreifen kann, die in AWS zur automatischen Aktualisierung gehostet wird.
- Überprüfen Sie, ob die Version nicht übereinstimmt zwischen der Standardsignatur und den vom Benutzer hinzugefügten Signaturen.
- Überprüfen Sie, ob die Versionsfehlung zwischen Signaturobjekten auf dem primären und sekundären Knoten übereinstimmt.
- Überwachen Sie die hohe CPU-Auslastung (deaktivieren Sie die automatische Aktualisierung, um ein Problem mit der Signaturaktualisierung auszuschließen).

Ablaufverfolgungsprotokoll

January 19, 2021

So zeichnen Sie Ablaufverfolgungsprotokolle auf:

1. Aktivieren Sie die Ablaufverfolgung für das Profil. Sie können den Befehl show verwenden, um die konfigurierte Einstellung zu überprüfen.

```
set appfw profile <profile> -trace ON
```

1. Beginnen Sie mit dem Sammeln von Trace. Sie können weiterhin alle Optionen verwenden, die für den Befehl nstrace gelten.

```
start nstrace -mode APPFW
```

1. Stoppen Sie das Sammeln der Trace

```
stop nstrace
```

Speicherort des Trace: Der nstrace wird in einem Zeitstempelordner gespeichert, der im Verzeichnis */var/nstrace* erstellt und mit Wireshark angezeigt werden kann. Sie können die Datei */var/log/ns.log* senden, um die Protokollmeldungen anzuzeigen, die Details zum Speicherort der neuen Ablaufverfolgung enthalten.

Vorteile von Trace-Protokollen:

- Datenverkehr für ein bestimmtes Profil isolieren
- Sammeln von Daten für bestimmte Anfragen
- Identifizieren von Zurücksetzungen oder Abbrüchen
- Entschlüsselten SSL-Datenverkehr anzeigen: HTTPS-Datenverkehr wird im Klartext erfasst, um die Fehlerbehebung zu erleichtern.
- Bietet umfassende Ansicht: Ermöglicht Ihnen, die gesamte Anforderung auf Paketebene zu betrachten, die Nutzlast zu überprüfen, Protokolle anzuzeigen, um zu überprüfen, welche Sicherheitsüberprüfungsverletzung ausgelöst wird, und das Übereinstimmungsmuster in der Nutzlast zu identifizieren. Wenn die Nutzlast aus unerwarteten Daten, Junk-Strings oder nicht druckbaren Zeichen (Nullzeichen, r oder n usw.) besteht, sind sie im Trace leicht zu erkennen.
- Beschleunigte Reaktionszeit: Schnelleres Debuggen im Zieldatenverkehr, um die Ursachenanalyse durchzuführen.

Sonstiges

August 19, 2021

Im Folgenden finden Sie die Lösungen für einige der Probleme, die bei der Verwendung der Web App Firewall auftreten können.

- Web App Firewall legt die Fenstergröße auf 9845 fest, wenn die Verbindung für ungültige HTTP-Nachrichten zurückgesetzt wird.

  — Fehlerhafte Anfrage empfangen - Verbindungszurücksetzung [Client/Server sendet ungültigen Header für Inhaltslänge]
  — Unbekannter Inhaltstyp in Anforderungsheadern

- Systemlimit: Die Anwendung erscheint eingefroren

  — Tritt auf, wenn die maximale Sitzungsgrenze erreicht ist. (100K)
  — Weniger Systemspeicher für den Betrieb.

  - IP-Reputation-Funktion funktioniert nicht
    — Der iprep-Prozess dauert etwa fünf Minuten, nachdem Sie die Reputation-Funktion aktiviert haben. Die IP-Reputationsfunktion funktioniert möglicherweise für diese Dauer nicht.

- Unerwartete Verletzungen der Web App Firewall, die ausgelöst werden

  — Sitzungszeitüberschreitung hat einen Standardwert von 900 Sekunden. Wenn Sitzungstimeout auf einen niedrigen Wert eingestellt ist, kann der Browser falsche Positive für Prüfungen auslösen, die auf Sitzungssitzung beruhen (z. B. CSRF, FFC). Überprüfen Sie die Sitzungszeitüberschreitung, und schauen Sie sich die Sitzungs-ID an (cs3 in CEF-Protokollen). Wenn die SessionID unterschiedlich ist, könnte das Sitzungstimeout der Grund sein.
  — Wenn Formular dynamisch durch Javascript generiert wird, kann es falsche FFC-Verletzungen auslösen.

- Leerer Feldname in FFC Verletzungsprotokollen (vor Version 11.0)

  Dies kann in Szenarien gesehen werden, in denen wir auf ein Formularfeld stoßen, das nicht in den Formularen in unserer Sitzung enthalten ist.

  Szenarien, in denen dies auftreten kann:

  — Die Sitzung hat das Timeout ab dem Zeitpunkt, an dem das Formular an den Client gesendet wurde und wann es empfangen wurde.
  — Das Formular wurde auf der Client-Seite mit einem Java-Skript generiert.

Referenzen

May 11, 2023

Weitere Informationen zu den Funktionen der Web App Firewall finden Sie in den folgenden Ressourcen.

- So ändert die NetScaler Web App Firewall den Datenverkehr von Anwendungen.
- Ablaufverfolgung und wie HTML-Anfragen über Web App Firewall Sicherheitsverletzung auf der NetScaler-Appliance protokolliert
- Schutz auf höchstem Niveau
- Entspannung der Sicherheit
- Informationen zum Konfigurieren und Bereitstellen einer Anwendung:
  - Anwendung
  - Firewall
  - Protokolle
- Artikel zur Signaturaktualisierung
- Bot-Verwaltung

Artikel zur Signaturwarnung

May 11, 2023

NetScaler Web App Firewall (WAF) kündigt Signaturupdates an, die Sie herunterladen und auf Ihre Appliance anwenden können. Wenn Sie einen Sicherheitsangriff entdecken, erhalten Sie eine E-Mail-Benachrichtigung über das neue Signatur-Update. Sie können die Signatur herunterladen und auf Ihre Appliance anwenden.

So erhalten Sie eine Signaturwarnungsbenachrichtigung

In diesem Artikel wird erläutert, wie Sie RSS-Feeds abonnieren, um Benachrichtigungen über neue Signaturaktualisierungen zu Sobald Sie abonniert sind, erhalten Sie regelmäßig RSS-Feeds, wenn neue Signaturen zum Herunterladen verfügbar sind.

> **Hinweis:**
>
> - Um Updates zu den Signaturen der Web App Firewall zu erhalten, müssen Sie die Funktion zur automatischen Signaturaktualisierung konfigurieren. Weitere Informationen finden Sie im Thema Autom. Signaturaktualisierung .
> - Um Updates zu neuen Bot-Signaturen zu erhalten, müssen Sie die Funktion zur automatischen Aktualisierung der Bot-Signatur konfigurieren. Weitere Informationen finden Sie im

> Thema Automatische Aktualisierung der Bot-Signatur .

Führen Sie die folgenden Schritte aus, um RSS-Feeds für neue Signaturaktualisierungenzu abonnieren:

1. Öffnen Sie das Thema Dokumentverlauf des Signaturwarnungsartikels in einem Webbrowser.
2. Klicken Sie oben rechts auf der Seite auf die Schaltfläche RSS und kopieren Sie die RSS-Feed-URL.
3. Fügen Sie die kopierte RSS-Feed-URL einem gewünschten RSS-Feed-Reader

Signatur-Update für August 2023

September 11, 2023

Für die in der Woche 2023-08-30 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Angriffen mit Sicherheitslücken zu schützen.

Signaturversion

Signaturversion 112 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, NetScaler 13.1 und NetScaler 14.1.

> **Hinweis:**
>
> Das Aktivieren der Signaturregeln für Postbody und Antworttext kann sich auf die Citrix ADC CPU

Überblick über Common Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste der Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	HÖHLEN-ID	Beschreibung
998632	CVE-2023-39526	WEB-MISC PrestaShop vor 8.0.5, 8.1.1 und 1.7.8.10 — Sicherheitsanfälligkeit beim Schreiben beliebiger Dateien über OUTFILE (CVE-2023-39526)

Signaturregel	HÖHLEN-ID	Beschreibung
998633	CVE-2023-39526	WEB-MISC PrestaShop vor 8.0.5, 8.1.1 und 1.7.8.10 — Sicherheitsanfälligkeit beim Schreiben beliebiger Dateien über DUMPFILE (CVE-2023-39526)
998634	CVE-2023-39143	WEB-MISC PaperCut NG/MF vor 22.1.3 — Sicherheitsanfälligkeit durch Pfaddurchquerung in Custom-ReportExampleServlet (CVE-2023-39143)
998635	CVE-2023-37979	WEB-WORDPRESS Ninja Forms Kontaktformular-Plugin bis zu 3.6.25 — Cross-Site-Scripting-Schwachstelle (CVE-2023-37979)
998636	CVE-2023-33652	WEB-MISC Sitecore — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2023-33652)
998637	CVE-2023-32563	WEB-MISC Ivanti Avalanche vor 6.4.1 — Sicherheitsanfälligkeit beim Hochladen beliebiger Dateien (CVE-2023-32563)
998638	CVE-2023-29357	WEB-MISC Microsoft SharePoint Server — Sicherheitsanfälligkeit im Zusammenhang mit Rechteerweiterungen über access_token/prooftoken (CVE-2023-29357)

Signaturregel	HÖHLEN-ID	Beschreibung
998639	CVE-2023-29357	WEB-MISC Microsoft SharePoint Server — Sicherheitsanfälligkeit bezüglich Rechteerweiterungen über Autorisierungsheader (CVE-2023-29357)
998640	CVE-2023-22480	WEB-MISC KubeOperator vor 3.16.4 — Sicherheitslücke bei unsachgemäßer Autorisierung (CVE-2023-22480)

Signatur-Update für August 2023

August 15, 2023

Für die in der Woche 2023-08-04 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 111 gilt für NetScaler VPX 11.1-, NetScaler 12.0-, Citrix ADC 12.1-, Citrix ADC 13.0- und NetScaler 13.1-Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC CPU auswirken.

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998641	CVE-2023-37580	WEB-MISC Zimbra Collaboration Suite — Mehrere Versionen — XSS-Sicherheitslücke (CVE-2023-37580)
998642	CVE-2023-35082	WEB-MISC MobileIron Core (Ivanti EPMM) vor 11.2 — Umgehung der Authentifizierung (CVE-2023-35082)
998643	CVE-2023-35078	WEB-MISC Ivanti EndPoint Manager Mobile — Umgehung der Authentifizierung (CVE-2023-35078)
998644	CVE-2023-34192	WEB-MISC Zimbra Collaboration Suite — Mehrere Versionen — XSS-Sicherheitslücke (CVE-2023-34192)
998645	CVE-2023-29382	WEB-MISC Zimbra Collaboration Suite — Mehrere Versionen — RCE über sfdc_preauth.jsp (CVE-2023-29382)

Signaturaktualisierung für Juli 2023

August 15, 2023

Für die in der Woche 2023-07-25 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 110 gilt für NetScaler 11.1-, NetScaler 12.0-, Citrix ADC 12.1-, Citrix ADC 13.0-, NetScaler 13.1- und NetScaler 14.1-Plattformen.

> **Hinweis:**
>
> Das Aktivieren der Signaturregeln für Postbody und Antworttext kann sich auf die NetScaler ADC CPU

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998646	CVE-2023-35036	WEB-MISC Progress MOVEit Transfer — Sicherheitslücke bei authentifizierter SQL-Injection durch X-siLock-FolderID-Schmuggel (CVE-2023-35036)
998647	CVE-2023-35036	WEB-MISC Progress MOVEit Transfer — Sicherheitsanfälligkeit durch authentifizierte SQL-Injection über X-SiLock-FolderID (CVE-2023-35036)
998648	CVE-2023-3460	WEB-WORDPRESS Ultimate Member Wordpress-Plugin vor 2.6.7 Unsachgemäße Rechteverwaltung (CVE-2023-3460)
998649	CVE-2023-33651	WEB-MISC Sitecore — Autorisierungsregeln umgehen Sicherheitslücke per MVC-Gerätesimulator (CVE-2023-33651)

Signaturregel	CVE-ID	Beschreibung
998650	CVE-2023-33157	WEB-MISC Microsoft SharePoint — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2023-33157)
998651	CVE-2023-30777	WEB-WORDPRESS WordPress-Plugin Erweiterte benutzerdefinierte Felder bis zu 6.1.5 — Reflektierte XSS-Sicherheitsanfälligkeit (CVE-2023-30777)
998652	CVE-2023-30545	WEB-MISC PrestaShop vor 8.0.4 und 1.7.8.9 — Schwachstelle beim Lesen beliebiger Dateien über LOAD_FILE (CVE-2023-30545)
998653	CVE-2023-2986	WEB-WORDPRESS Abandoned Cart Lite für WooCommerce-Plugin bis zu 5.14.2 Umgehung der Authentifizierung (CVE-2023-2986)
998654	CVE-2023-2982	WEB-WORDPRESS Wordpress-Plugin Soziale Anmeldung und Registrierung vor 7.6.4 — Umgehung der Authentifizierung (CVE-2023-2982)
998655	CVE-2023-29489	WEB-MISC cPanel vor 11.102.0.31 — XSS-Sicherheitsanfälligkeit (CVE-2023-29489)

Signaturregel	CVE-ID	Beschreibung
998656	CVE-2023-29300, CVE-2023-38203, CVE-2023-38204	WEB-MISC Adobe ColdFusion — Sicherheitslücke durch Deserialisierung nicht vertrauenswürdiger Daten (CVE-2023-29300, CVE-2023-38203, CVE-2023-38204)
998657	CVE-2023-29298, CVE-2023-38205	WEB-MISC Adobe ColdFusion in mehreren Versionen — Sicherheitsanfälligkeit zur Umgehung der Zugriffskontrolle über Restplay (CVE-2023-29298, CVE-2023-38205)
998658	CVE-2023-29298, CVE-2023-38205	WEB-MISC Adobe ColdFusion in mehreren Versionen — Sicherheitslücke zur Umgehung der Zugriffskontrolle über cfide (CVE-2023-29298, CVE-2023-38205)
998659	CVE-2023-28121	WEB-WORDPRESS WordPress-Plugin WooCommerce-Zahlungen bis zu 5.6.1 — Sicherheitsanfälligkeit durch Erhöhung von Berechtigungen (CVE-2023-28121)
998660	CVE-2023-27372	WEB-MISC SPIP bis zu 3.2.17, 4.0.0 bis 4.0.9, 4.1.0 bis 4.1.7, 4.2.0 Remotecodeausführung (CVE-2023-27372)

Signaturregel	CVE-ID	Beschreibung
998661	CVE-2023-27372	WEB-MISC SPIP bis zu 3.2.17, 4.0.0 bis 4.0.9, 4.1.0 bis 4.1.7, 4.2.0 Remotecodeausführung (CVE-2023-27372)
998662	CVE-2023-27350	WEB-MISC PaperCut NG — Sicherheitslücke durch Umgehung der Authentifizierung (CVE-2023-27350)
998663	CVE-2023-27067	WEB-MISC Sitecore bis zu 10.2 — Sicherheitsanfälligkeit durch Pfaddurchquerung (CVE-2023-27067)
998664	CVE-2023-26360	WEB-MISC Adobe ColdFusion 2018 vor Update 16 und 2021 vor Update 6 — Unsachgemäße Zugriffskontrolle (CVE-2023-26360)
998665	CVE-2023-26262	WEB-MISC Sitecore — Sicherheitslücke beim uneingeschränkten Hochladen von Sprachdateien (CVE-2023-26262)
998666	CVE-2023-2611	WEB-MISC Advantech r-SEEnet vor 2.4.23 — Sicherheitsanfälligkeit bei Verwendung von hartcodierten Anmeldeinformationen (CVE-2023-2611)
998667	CVE-2023-25804	WEB-MISC Roxy-WI vor 6.3.6.0 — Sicherheitsanfälligkeit durch Pfaddurchquerung (CVE-2023-25804)

Signaturregel	CVE-ID	Beschreibung
998668	CVE-2023-2575	WEB-MISC Advantech EKI-15XX — Sicherheitsanfälligkeit durch Stack-basierten Pufferüberlauf (CVE-2023-2575)
998669	CVE-2023-2574	WEB-MISC Advantech EKI-15XX — Sicherheitslücke beim Einschleusen von Betriebssystembefehlen (CVE-2023-2574)
998670	CVE-2023-2573	WEB-MISC Advantech EKI-15XX — Sicherheitslücke beim Einschleusen von Betriebssystembefehlen (CVE-2023-2573)
998671	CVE-2023-25690	WEB-MISC Apache HTTP Server 2.4.0 bis 2.4.55 — Sicherheitsanfälligkeit bezüglich Anforderungsschmuggel über Line Feed (CVE-2023-25690)
998672	CVE-2023-25690	WEB-MISC Apache HTTP Server 2.4.0 bis 2.4.55 — Sicherheitsanfälligkeit bei Anforderungsschmuggel via Carriage Return (CVE-2023-25690)
998673	CVE-2023-23489	WEB-WORDPRESS-Plugin Einfache digitale Downloads vor v3.1.0.2 — Sicherheitsanfälligkeit durch SQL-Injection (CVE-2023-23489)

Signaturregel	CVE-ID	Beschreibung
998674	CVE-2023-20887	WEB-MISC VMware Aria Operations for Networks — Sicherheitsanfälligkeit durch Befehlsinjektion (CVE-2023-20887)
998675	CVE-2023-1671	WEB-MISC Sophos Web Appliance vor 4.3.10.4 — Befehlsinjektion (CVE-2023-1671)
998676	CVE-2023-1196	WEB-WORDPRESS WordPress-Plugin Erweiterte benutzerdefinierte Felder vor 5.12.5 und 6.1.0 — Unvertrauenswürdige Deserialisierung (CVE-2023-1196)
998677	CVE-2023-1138	WEB-MISC Delta Electronics InfraSuite Device Master vor Version 1.0.5 — Offenlegung von Informationen per Bericht (CVE-2023-1138)
998678	CVE-2023-1138	WEB-MISC Delta Electronics InfraSuite Device Master vor 1.0.5 — Offenlegung von Informationen über ModuleConfig (CVE-2023-1138)
998679	CVE-2023-1137	WEB-MISC Delta Electronics InfraSuite Device Master vor 1.0.5 — Sicherheitslücke bei der Offenlegung von Informationen (CVE-2023-1137)

Signaturregel	CVE-ID	Beschreibung
998680	CVE-2023-0255	WEB-WORDPRESS-Plugin Aktiviert Media Replace vor Version 4.0.2 — Sicherheitsanfälligkeit beim Hochladen beliebiger Dateien (CVE-2023-0255)
998681	CVE-2022-36963	WEB-MISC SolarWinds-Plattform vor 2023.2 — Sicherheitsanfälligkeit durch Befehlsinjektion über TestCredentials (CVE-2022-36963)
998682	CVE-2022-29303	WEB-MISC Contec SolarView Compact vor 7.21 — Sicherheitslücke beim Einschleusen von Betriebssystembefehlen (CVE-2022-29303)
998683	CVE-2022-2185	WEB-MISC GitLab mehrere Versionen vor 14.10.5 und 15.1.1 — Sicherheitsanfälligkeit durch Fernausführung (CVE-2022-2185)
998684	CVE-2020-5284	WEB-MISC Next.js vor 9.3.2 — Sicherheitsanfälligkeit durch Pfaddurchquerung (CVE-2020-5284)

Signaturaktualisierung für Juli 2023

August 15, 2023

Für die in der Woche 2023-07-14 identifizierten Sicherheitslücken werden neue Signaturregeln gener-

iert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 109 gilt für NetScaler 11.1-, NetScaler 12.0-, Citrix ADC 12.1-, Citrix ADC 13.0-, NetScaler 13.1- und NetScaler 14.1-Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC CPU auswirken.

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998685	CVE-2023-36933	WEB-MISC Progress MOVEit Transfer mehrerer Versionen — Denial-of-Service-Schwachstelle (CVE-2023-36933)

Signaturaktualisierung für Juli 2023

August 15, 2023

Für die in der Woche 2023-07-12 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 108 gilt für NetScaler 11.1-, NetScaler 12.0-, Citrix ADC 12.1-, Citrix ADC 13.0-, NetScaler 13.1- und NetScaler 14.1-Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die

> Citrix ADC CPU auswirken.

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998686	CVE-2023-36934	WEB-MISC Progress MOVEit-Übertragung mehrerer Versionen — Sicherheitsanfälligkeit durch SQL-Injection (CVE-2023-36934)
998687	CVE-2023-36932	WEB-MISC Progress MOVEit Transfer mehrerer Versionen — Sicherheitsanfälligkeit durch SQL-Injection über rekursive Ordnerliste (CVE-2023-36932)

Signaturaktualisierung für Juni 2023

August 15, 2023

Für die in der Woche 2023-06-16 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 107 gilt für NetScaler 11.1-, NetScaler 12.0-, Citrix ADC 12.1-, Citrix ADC 13.0-, NetScaler 13.1- und NetScaler 14.1-Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die NetScaler CPU auswirken.

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998688	CVE-2023-35708	WEB-MISC Progress MOVEit Transfer mehrerer Versionen — Sicherheitsanfälligkeit durch nicht authentifizierte SQL-Injektion (CVE-2023-35708)
998689	CVE-2023-35036	WEB-MISC Progress MOVEit Transfer mehrerer Versionen — Sicherheitsanfälligkeit durch nicht authentifizierte SQL-Injection (CVE-2023-35036)

Signaturaktualisierung für Juni 2023

August 15, 2023

Für die in der Woche 2023-06-16 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 106 gilt für NetScaler 11.1-, NetScaler 12.0-, Citrix ADC 12.1-, Citrix ADC 13.0-, NetScaler 13.1- und NetScaler 14.1-Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die NetScaler CPU auswirken.

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998690	CVE-2023-34362	WEB-MISC Progress MOVEit überträgt mehrere Versionen — Sicherheitslücke in SQL Injection (CVE-2023-34362)
998691	CVE-2023-32243	WEB-WORDPRESS WordPress-Plugin Essentielle Addons für Elementor bis 5.7.1 — Sicherheitslücke bei der Eskalation von Rechten (CVE-2023-32243)
998692	CVE-2023-29084	WEB-MISC Zoho ManageEngine AdManager Plus vor 7181 — Sicherheitsanfälligkeit durch OS Command Injection (CVE-2023-29084)
998693	CVE-2023-29004	WEB-MISC Roxy-WI vor 6.3.9.0 — Absolute Path Traversal Vulnerability (CVE-2023-29004)
998694	CVE-2023-27351	WEB-MISC PaperCut NG — Sicherheitslücke zur Umgehung der Authentifizierung über /AutoSetup/SetStatus (CVE-2023-27351)
998695	CVE-2023-27351	WEB-MISC PaperCut NG — Sicherheitslücke zur Umgehung der Authentifizierung via /register oder /registerCreate (CVE-2023-27351)

Signaturregel	CVE-ID	Beschreibung
998696	CVE-2023-27351	WEB-MISC PaperCut NG — Sicherheitslücke zur Umgehung der Authentifizierung über /keepalive (CVE-2023-27351)
998697	CVE-2023-27350	WEB-MISC PaperCut NG — Sicherheitslücke durch Umgehung der Authentifizierung (CVE-2023-27350)
998698	CVE-2023-25812	WEB-MISC MinIO vor RELEASE.2023-02-17T17-52-43Z — Sicherheitslücke bei unsachgemäßer Wahrung von Berechtigungen (CVE-2023-25812)
998699	CVE-2023-25812	WEB-MISC MinIO vor RELEASE.2023-02-17T17-52-43Z — Sicherheitslücke bei unsachgemäßer Wahrung von Berechtigungen (CVE-2023-25812)
998700	CVE-2023-25803	WEB-MISC Roxy-WI vor 6.3.6.0 — Sicherheitslücke durch Path Traversal (CVE-2023-25803)
998701	CVE-2023-24031	WEB-MISC Zimbra Collaboration Suite vor 9.0.0 P30 — XSS-Sicherheitslücke über Clazz (CVE-2023-24031)
998702	CVE-2023-24031	WEB-MISC Zimbra Collaboration Suite vor 9.0.0 P30 — XSS-Sicherheitslücke über Altkey (CVE-2023-24031)

Signaturregel	CVE-ID	Beschreibung
998703	CVE-2023-24031	WEB-MISC Zimbra Collaboration Suite vor 9.0.0 P30 — XSS-Sicherheitslücke laut Titel (CVE-2023-24031)
998704	CVE-2023-24031	WEB-MISC Zimbra Collaboration Suite vor 9.0.0 P30 — XSS-Sicherheitslücke durch Zähler (CVE-2023-24031)
998705	CVE-2023-2338	WEB-MISC Pimcore vor v10.5.21 — Sicherheitslücke durch SQL-Injection (CVE-2023-2338)
998706	CVE-2023-2336	WEB-MISC Pimcore vor v10.5.21 — Path Traversal Vulnerability (CVE-2023-2336)
998707	CVE-2023-22973	WEB-MISC OpenEMR vor 7.0.0 - Lokale Dateieinbindung (LFI) (CVE-2023-22973)
998708	CVE-2023-21742	WEB-MISC Microsoft SharePoint — Sicherheitsanfälligkeit bei der Remote-Codeausführung (CVE-2023-21742)
998709	CVE-2023-20864	WEB-MISC VMware Aria Operations for Logs 8.10.2 — Sicherheitslücke bei Deserialisierung über ApproveMembership (CVE-2023-20864)
998710	CVE-2023-20864	WEB-MISC VMware Aria Operations for Logs 8.10.2 — Sicherheitslücke bei Deserialisierung über SetToken (CVE-2023-20864)

Signaturregel	CVE-ID	Beschreibung
998711	CVE-2023-20864	WEB-MISC VMware Aria Operations for Logs 8.10.2 — Sicherheitslücke bei Deserialisierung über ApplyMembership (CVE-2023-20864)
998712	CVE-2023-1578	WEB-MISC Pimcore vor v10.5.19 — Sicherheitslücke durch SQL-Injection (CVE-2023-1578)
998713	CVE-2023-1406	WEB-WORDPRESS JetEngine-Plugin vor 3.1.3.1 — Sicherheitslücke bei Remote-Codeausführung (CVE-2023-1406)
998714	CVE-2023-0315	WEB-MISC Froxlor Codeausführung per Fernzugriff (CVE-2023-0315)
998715	CVE-2022-45030	WEB-MISC rConfig 3.9.7 and Prior - SQL Injection Vulnerability (CVE-2022-45030)
998716	CVE-2022-43396	WEB-MISC Apache Kylin — Sicherheitslücke durch Befehlseinschleusung durch Konfigurationsüberschreibungen (CVE-2022-43396)
998717	CVE-2022-31700	WEB-MISC VMware Workspace ONE Access — Sicherheitslücke bei der Remote-Codeausführung über Multipart (CVE-2022-31700)

Signaturregel	CVE-ID	Beschreibung
998718	CVE-2022-31700	WEB-MISC VMware Workspace ONE Access — Sicherheitslücke bei der Remote-Codeausführung über JSON (CVE-2022-31700)
998719	CVE-2022-2884, CVE-2022-2992, CVE-2022-2865	WEB-MISC GitLab, mehrere Versionen — Sicherheitslücke bei der Remote-Codeausführung (CVE-2022-2884, CVE-2022-2992, CVE-2022-2865)
998720	CVE-2022-27926	WEB-MISC Zimbra Collaboration Suite vor 9.0.0 P24 — XSS-Sicherheitslücke (CVE-2022-27926)
998721	CVE-2022-0824	WEB-CGI Unsachgemäße Zugriffskontrolle zur Remote-Codeausführung in WebMin vor 1.990 mithilfe des Authentic-Themes (CVE-2022-0824)

Bot-Verwaltung

May 11, 2023

Manchmal besteht der eingehende Web-Traffic aus Bots und die meisten Organisationen leiden unter Bot-Attacken. Web- und mobile Anwendungen sind wichtige Umsatztreiber für Unternehmen, und die meisten Unternehmen sind von fortschrittlichen Cyberangriffen wie Bots bedroht.
Ein Bot ist ein Softwareprogramm, das bestimmte Aktionen automatisch wiederholt und viel schneller ausführt als ein Mensch. Bots können mit Webseiten interagieren, Formulare einreichen, Aktionen ausführen, Texte scannen oder Inhalte herunterladen. Sie können auf Social Media-Plattformen auf Videos zugreifen, Kommentare posten und twittern. Einige Bots, sogenannte Chatbots, können grundlegende Gespräche mit menschlichen Benutzern führen.

Ein Bot, der hilfreiche Dienste wie Kundenservice, automatisierter Chat und Suchmaschinen-Crawler erbringt, ist ein guter Bots. Gleichzeitig sind ein Bot, der Inhalte von einer Website kratzen oder herunterladen kann, Benutzeranmeldeinformationen, Spam-Inhalte stehlen und andere Arten von Cyberangriffen ausführen kann, schlechte Bots.
Da viele bösartige Bots bösartige Aufgaben ausführen, ist es wichtig, den Bot-Traffic zu verwalten und Ihre Webanwendungen vor Bot-Angriffen zu schützen. Mithilfe des NetScaler-Bot-Managements können Sie den eingehenden Bot-Traffic erkennen und Bot-Angriffe abwehren, um Ihre Webanwendungen zu schützen.
NetScaler Bot-Management hilft dabei, bösartige Bots zu identifizieren und Ihre Appliance vor fortschrittlichen Sicherheitsangriffen zu schützen. Es erkennt gute und schlechte Bots und identifiziert, ob eingehender Traffic ein Bot-Angriff ist. Durch den Einsatz von Bot-Management können Sie Angriffe abwehren und Ihre Webanwendungen schützen.

Die NetScaler Bot-Verwaltung bietet folgende Vorteile:

- **Verteidigen Sie sich gegen Bots, Skripts und Toolkits**. Bietet Bedrohungsabwehr in Echtzeit mithilfe statischer Signaturen und Geräte-Fingerprinting.
- **Neutralisieren Sie automatisierte einfache und fortgeschrittene Angriffe**. Verhindert Angriffe, wie App-Layer-DDoS, Kennwort-Spraying, Kennwort-Stuffing, Preis-Scraper und Inhalts-Scraper.
- **Schützen Sie Ihre APIs und Investitionen**. Schützt Ihre APIs vor ungerechtfertigtem Missbrauch und schützt Infrastrukturinvestitionen vor automatisiertem Verkehr.

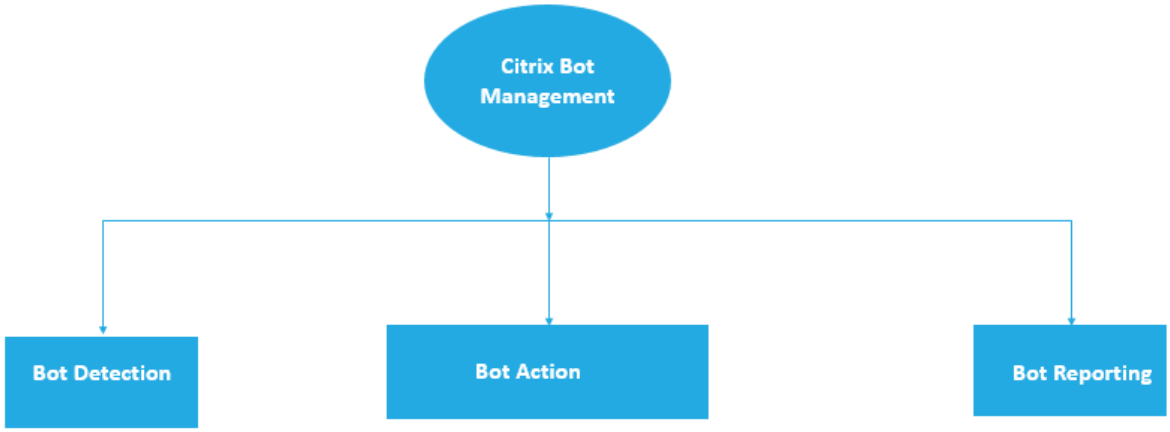
Einige Anwendungsfälle, in denen Sie von der Verwendung des NetScaler Bot-Managementsystems profitieren können, sind:

- Brute-Force-Anmeldung. Ein Webportal der Regierung wird ständig von Bots angegriffen, die versuchen, Benutzeranmeldungen mit Gewalt zu erzwingen. Das Unternehmen entdeckte den Angriff, indem es Webprotokolle durchsuchte und feststellte, dass bestimmte Benutzer immer wieder ausgewählt wurden, wobei schnelle Anmeldeversuche durchgeführt wurden und die Passwörter mithilfe eines Wörterbuchangriffs immer wieder erhöht wurden. Nach dem Gesetz müssen sie sich und ihre Nutzer schützen. Durch den Einsatz des NetScaler-Botmanagements können sie die Brute-Force-Anmeldung mithilfe von Geräte-Fingerprinting und Techniken zur Ratenbegrenzung verhindern.
- Blockieren Sie schlechte Bots und unbekannte Bots mit Fingerabdrücken Eine Web-Entität hat täglich 100.000 Besucher. Sie müssen den zugrunde liegenden Fußabdruck verbessern und geben ein Vermögen aus. In einem kürzlich durchgeführten Audit stellte das Team fest, dass 40 Prozent des Traffics von Bots, dem Scraping von Inhalten, der Auswahl von Nachrichten, der Überprüfung von Benutzerprofilen und mehr stammten. Sie möchten diesen Verkehr blockieren, um ihre Benutzer zu schützen und ihre Hosting-Kosten zu senken. Mithilfe des Bot-Managements können sie bekannte bösartige Bots blockieren und unbekannte Bots, die ihre Website manipulieren, Fingerabdrücke abdrücken. Indem sie diese Bots blockieren,

können sie den Bot-Verkehr um 90 Prozent reduzieren.

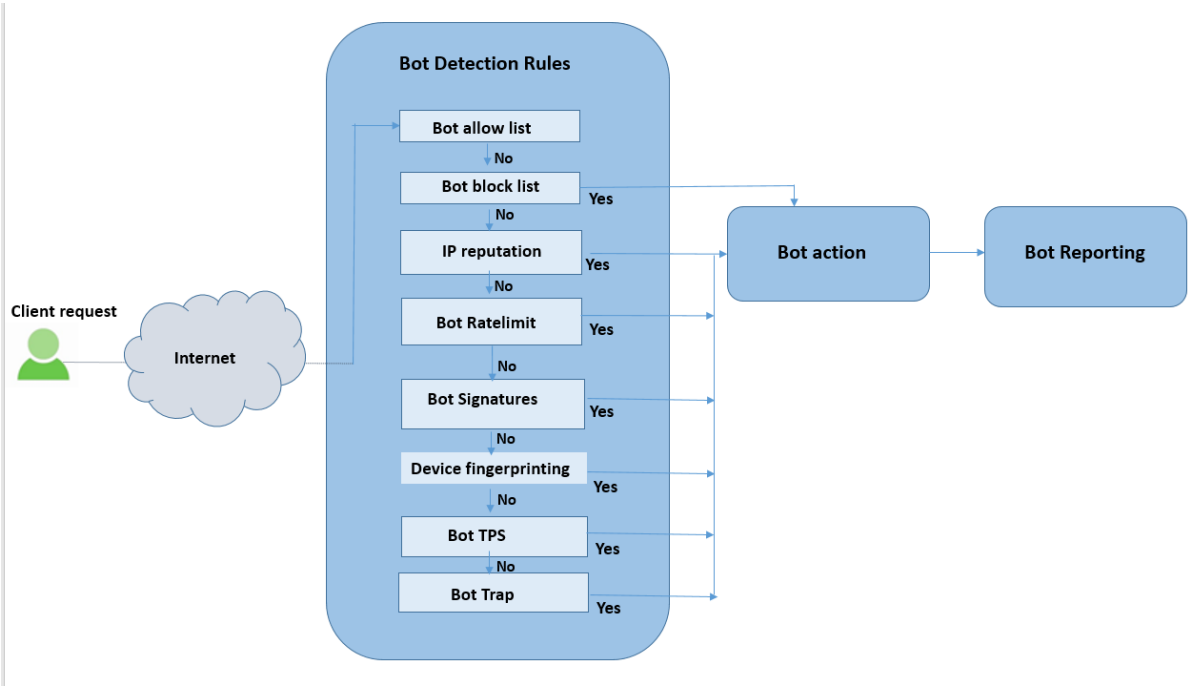
Was macht NetScaler Bot Management

Das NetScaler-Bot-Management hilft Unternehmen dabei, ihre Webanwendungen und öffentlichen Ressourcen vor fortschrittlichen Sicherheitsangriffen zu schützen. Wenn ein eingehender Datenverkehr ein Bot ist, erkennt das Bot-Managementsystem den Bot-Typ, weist eine Aktion zu und generiert Bot-Insights, wie im folgenden Diagramm gezeigt.



Wie funktioniert NetScaler Bot-Management

Das folgende Diagramm zeigt, wie die NetScaler Bot-Verwaltung funktioniert. Der Prozess umfasst acht Erkennungstechniken, die helfen, den eingehenden Datenverkehr als guten oder schlechten Bot zu erkennen. Standardmäßig sind gute Bots, die von Signaturen erkannt wurden, zulässig und schlechte Bots, die von Signaturen erkannt wurden, werden gelöscht.



1. Der Prozess beginnt mit der Aktivierung der Bot-Verwaltungsfunktion auf der Appliance.
2. Wenn ein Client eine Anfrage sendet, wertet die Appliance den Datenverkehr anhand der Bot-Richtlinienregeln aus. Wenn die eingehende Anfrage als Bot identifiziert wird, wendet die Appliance ein Bot-Erkennungsprofil an.
3. Sie müssen die standardmäßige oder benutzerdefinierte Bot-Signaturdatei an das Bot-Erkennungsprofil binden. Die Bot-Signaturdatei enthält eine Liste von Bot-Signaturregeln zur Identifizierung des eingehenden Bot-Typs.
4. Die Bot-Erkennungsregeln sind unter acht Erkennungskategorien in der Signaturdatei verfügbar. Die Kategorien sind Zulassungsliste, Sperrliste, statische Signatur, IP-Reputation, Geräte-Fingerabdruck und Ratenbegrenzung. Basierend auf dem Bot-Traffic wendet das System eine Erkennungsregel auf den Verkehr an.
5. Wenn der eingehende Bot-Traffic mit einem Eintrag in der Bot-Zulassungsliste übereinstimmt, umgeht das System andere Erkennungstechniken und die zugehörige Aktion protokolliert die Daten.
6. Bei anderen Erkennungstechniken als der Bot-Zulassungsliste wird die entsprechende Aktion angewendet, wenn eine eingehende Anforderung mit einer konfigurierten Regel übereinstimmt. Die möglichen Aktionen sind Drop, Redirect, Reset, Minderung und Log. CAPTCHA ist eine Minderungsaktion, die für IP-Reputation, Gerätefingerabdruck und TPS-Erkennungstechniken unterstützt wird.

Bot-Erkennung

August 4, 2023

Das NetScaler Bot-Managementsystem verwendet verschiedene Techniken, um den eingehenden Bot-Verkehr zu erkennen. Die Techniken werden als Erkennungsregeln verwendet, um den Bot-Typ zu erkennen. Die Techniken lauten wie folgt:

> **Hinweis:**
>
> Die Bot-Verwaltung unterstützt maximal 32 Konfigurations-Entitäten für Sperrlisten-, Positivlisten- und Ratenbegrenzungstechniken.

Liste zugelassener Bots — Eine benutzerdefinierte Liste von IP-Adressen (IPv4 und IPv6), Subnetzen (IPv4 und IPv6) und Richtlinienausdrücken, die als zulässige Liste umgangen werden können.

Bot-Blockliste — Eine benutzerdefinierte Liste von IP-Adressen (IPv4 und IPv6), Subnetzen (IPv4 und IPv6) und Richtlinienausdrücken, die für den Zugriff auf Ihre Webanwendungen gesperrt werden müssen.

IP-Reputation — Diese Regel erkennt, ob der eingehende Bot-Verkehr von einer bösartigen IP-Adresse stammt.

Gerätefingerabdruck — Diese Regel erkennt, ob der eingehende Bot-Verkehr die Geräte-Fingerabdruck-ID im Header der eingehenden Anfrage und in den Browserattributen eines eingehenden Client-Bot-Traffics enthält.

> **Einschränkung:**
>
> 1. JavaScript muss im Client-Browser aktiviert sein.
> 2. Funktioniert nicht für XML-Antworten.

Bot-Log-Ausdruck — Die Erkennungstechnik ermöglicht es Ihnen, zusätzliche Informationen als Protokollnachrichten zu erfassen. Die Daten können der Name des Benutzers sein, der die URL angefordert hat, die Quell-IP-Adresse und der Quellport, von dem der Benutzer die Anforderung oder Daten gesendet hat, die aus einem Ausdruck generiert wurden.

Ratenlimit — Diese Regelrate begrenzt mehrere Anfragen, die von demselben Client kommen.

Bot-Trap — Erkennt und blockiert automatisierte Bots, indem in der Kundenantwort eine Trap-URL angegeben wird. Die URL erscheint unsichtbar und nicht zugänglich, wenn der Client ein menschlicher Benutzer ist. Die Erkennungstechnik blockiert effektiv Angriffe von automatisierten Bots.

TPS — Erkennt eingehenden Traffic als Bots, wenn die maximale Anzahl von Anfragen und der prozentuale Anstieg der Anfragen das konfigurierte Zeitintervall überschreiten.

CAPTCHA — Diese Regel verwendet ein CAPTCHA zur Abwehr von Bot-Angriffen. Ein CAPTCHA ist eine Challenge-Response-Validierung, um festzustellen, ob der eingehende Verkehr von einem menschlichen Benutzer oder einem automatisierten Bot stammt. Die Validierung hilft dabei, automatisierte Bots zu blockieren, die Sicherheitsverletzungen für Webanwendungen verursachen. Sie können CAPTCHA als Bot-Aktion für IP-Reputation und Geräte-Fingerabdruck-Erkennungstechniken konfigurieren.

Lassen Sie uns nun sehen, wie Sie jede Technik konfigurieren können, um Ihren Bot-Traffic zu erkennen und zu verwalten.

So aktualisieren Sie Ihre Appliance auf NetScaler CLI-basierte Bot-Management-Konfiguration

Wenn Sie Ihre Appliance von einer älteren Version aktualisieren (NetScaler Version 13.0 Build 58.32 oder früher), müssen Sie die vorhandene Bot-Verwaltungskonfiguration zuerst nur einmal manuell in die NetScaler CLI-basierte Bot-Management-Konfiguration konvertieren. Führen Sie die folgenden Schritte aus, um Ihre Bot-Management-Konfiguration manuell zu konvertieren.

1. Stellen Sie nach dem Upgrade auf die neueste Version mithilfe des folgenden Befehls eine Verbindung zum Upgrade-Tool “upgrade_bot_config.py” her

   Geben Sie in der Befehlszeile Folgendes ein:

   ```
   shell "/var/python/bin/python /netscaler/upgrade_bot_config.py > /var/bot_upgrade_commands.txt"
   ```

2. Führen Sie die Konfiguration mit dem folgenden Befehl aus.

   Geben Sie in der Befehlszeile Folgendes ein:

   ```
   batch -f /var/bot_upgrade_commands.txt
   ```

3. Speichern Sie die aktualisierte Konfiguration.

```
save ns config
```

Konfigurieren der NetScaler CLI-basierten Bot-Verwaltung

Mit der Bot-Management-Konfiguration können Sie eine oder mehrere Bot-Erkennungstechniken an ein bestimmtes Bot-Profil binden.
Sie müssen die folgenden Schritte ausführen, um die NetScaler-basierte Bot-Verwaltung zu konfigurieren:

1. Bot-Management aktivieren
2. Botsignatur importieren
3. Bot-Profil hinzufügen

4. Bot-Profil binden
5. Bot-Richtlinie hinzufügen
6. Bind-Bot-Richtlinie
7. Konfigurieren Sie Bot-Einstellungen

> **Hinweis:**
>
> Wenn Sie Ihre Appliance von einer älteren Version upgraden, müssen Sie zuerst die vorhandene Bot-Management-Konfiguration manuell konvertieren. Weitere Informationen finden Sie unter Aktualisieren auf NetScaler CLI-basierte Bot-Verwaltungskonfiguration.

Bot-Management aktivieren

Bevor Sie beginnen können, stellen Sie sicher, dass die Bot-Verwaltungsfunktion auf der Appliance aktiviert ist. Wenn Sie über einen neuen NetScaler oder VPX verfügen, müssen Sie die Funktion aktivieren, bevor Sie sie konfigurieren. Wenn Sie eine NetScaler-Appliance von einer früheren Version auf die aktuelle Version aktualisieren, müssen Sie die Funktion aktivieren, bevor Sie sie konfigurieren. Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature Bot
```

Botsignatur importieren

Sie können die Standardsignatur-Bot-Datei importieren und an das Bot-Profil binden. Geben Sie in der Befehlszeile Folgendes ein:

```
import bot signature [<src>] <name> [-comment <string>] [-overwrite]
```

Ort:

`src` - Lokaler Pfadname oder URL (Protokoll, Host, Pfad und Dateiname). Maximale Länge: 2047.
> **Hinweis:**
>
> Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, für dessen Zugriff eine Client-Zertifikatsauthentifizierung erforderlich ist.

`name` - Name des Bot-Signaturdateiobjekts. Dies ist ein zwingendes Argument. Maximale Länge: 31

`comment` - Beschreibung des Signaturdateiobjekts. Maximale Länge: 255

`overwrite` - Aktion, die die bestehende Datei überschreibt.
> **Hinweis:**
>
> Verwenden Sie die Option `overwrite`, um den Inhalt der Signaturdatei zu aktualisieren. Verwenden Sie alternativ den Befehl `update bot signature <name>`, um die Signaturdatei auf der NetScaler-Appliance zu aktualisieren.

Beispiel

```
import bot signature http://www.example.com/signature.json signaturefile -
comment commentsforbot -overwrite
```

> **Hinweis:**
>
> Sie können die Option zum Überschreiben verwenden, um den Inhalt in der Signaturdatei zu aktualisieren. Sie können den Befehl `update bot signature <name>` auch verwenden, um die Signaturdatei in der NetScaler-Appliance zu aktualisieren.

Bot-Profil hinzufügen

Ein Bot-Profil ist eine Sammlung von Profileinstellungen zur Konfiguration der Bot-Verwaltung auf der Appliance. Sie können die Einstellungen für die Durchführung der Bot-Erkennung konfigurieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add bot profile <name> [-signature <string>] [-errorURL <string>] [-trapURL
 <string>] [-whiteList ( ON | OFF )] [-blackList ( ON | OFF )] [-rateLimit
( ON | OFF )] [-deviceFingerprint ( ON | OFF )] [-deviceFingerprintAction (
 none | log | drop | redirect | reset | mitigation )] [-ipReputation ( ON |
 OFF )] [-trap ( ON | OFF )]
```

Beispiel:

```
add bot profile profile1 -signature signature -errorURL http://www.example
.com/error.html -trapURL /trap.html -whitelist ON -blacklist ON -ratelimit
 ON -deviceFingerprint ON -deviceFingerprintAction drop -ipReputation ON -
trap ON
```

Bot-Profil binden

Nachdem Sie ein Bot-Profil erstellt haben, müssen Sie den Bot-Erkennungsmechanismus an das Profil binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind bot profile <name> | (-ipReputation [-category <ipReputationCategory>]
 [-enabled ( ON | OFF )] [-action ( none | log | drop | redirect | reset |
mitigation )] [-logMessage <string>]
```

Beispiel:

Das folgende Beispiel dient zur Bindung der IP-Reputationserkennungstechnik an ein bestimmtes Bot-Profil.


```
bind bot profile profile5 -ipReputation -category BOTNET -enabled ON -
action drop -logMessage message
```

Bot-Richtlinie hinzufügen

Sie müssen die Bot-Richtlinie zur Bewertung des Bot-Traffics hinzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add bot policy <name> -rule <expression> -profileName <string> [-undefAction
 <string>] [-comment <string>] [-logAction <string>]
```

Hierbei gilt:

Name- Name für die Bot-Richtlinie. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann geändert werden, nachdem die Bot-Richtlinie hinzugefügt wurde.

Rule— Ein Ausdruck, anhand dessen die Richtlinie bestimmt, ob das Bot-Profil auf die angegebene Anfrage angewendet werden soll. Dies ist ein zwingendes Argument. Maximale Länge: 1499

profileName— Name des Bot-Profils, das angewendet werden soll, wenn die Anfrage dieser Bot-Richtlinie entspricht. Dies ist ein zwingendes Argument. Maximale Länge: 127

undefAction- Aktion, die ausgeführt werden muss, wenn das Ergebnis der Politikbewertung nicht definiert ist (UNDEF). Ein UNDEF-Ereignis weist auf einen internen Fehlerzustand hin. Maximale Länge: 127

Comment- Beschreibung dieser Bot-Richtlinie. Maximale Länge: 255

logAction — Name der Protokollaktion, die für Anfragen verwendet werden soll, die dieser Richtlinie entsprechen. Maximale Länge: 127

Beispiel:

```
add bot policy pol1 -rule "HTTP.REQ.HEADER(\"header\").CONTAINS(\"custom
\")"- profileName profile1 -undefAction drop -comment commentforbotpolicy -
logAction log1
```

Binden Sie die Bot-Richtlinie global

Geben Sie in der Befehlszeile Folgendes ein:

```
bind bot global -policyName <string> -priority <positive_integer> [-gotoPriorityExpres
 <expression>][-type ( REQ_OVERRIDE | REQ_DEFAULT )] [-invoke (-labelType (
 vserver | policylabel )-labelName <string>)]
```


Beispiel:

```
bind bot global -policyName pol1 -priority 100 -gotoPriorityExpression NEXT
-type REQ_OVERRIDE
```

Binden Sie die Bot-Richtlinie an einen virtuellen Server

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )| <
serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>]
[-gotoPriorityExpression <expression>]
```

Beispiel:

```
bind lb vserver lb-server1 -policyName pol1 -priority 100 -gotoPriorityExpression
 NEXT -type REQ_OVERRIDE
```

Konfigurieren Sie Bot-Einstellungen

Sie können die Standardeinstellungen bei Bedarf anpassen.
Geben Sie in der Befehlszeile Folgendes ein:

```
1 set bot settings [-defaultProfile <string>] [-javaScriptName <string>]
     [-sessionTimeout <positive_integer>] [-sessionCookieName <string>]
     [-dfpRequestLimit <positive_integer>] [-signatureAutoUpdate ( ON |
     OFF )] [-signatureUrl <URL>] [-proxyServer <ip_addr|ipv6_addr|\*>]
     [-proxyPort <port|\*>]
2 <!--NeedCopy-->
```

Hierbei gilt:

`defaultProfile` — Profil, das verwendet werden soll, wenn eine Verbindung keiner Richtlinie entspricht. Die Standardeinstellung ist “ “, wodurch nicht übereinstimmende Verbindungen an den NetScaler zurückgesendet werden, ohne dass versucht wird, sie weiter zu filtern. Maximale Länge: 31

`javaScriptName` - Name des JavaScripts, das die BotNet-Funktion als Antwort verwendet. Muss mit einem Buchstaben oder einer Zahl beginnen und kann aus 1 bis 31 Buchstaben, Zahlen und den Bindestrichen (-) und Unterstrichen (_) bestehen. Die folgende Anforderung gilt nur für die NetScaler CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Cookie-Name” oder “mein Cookie-Name”). Maximale Länge: 31

`sessionTimeout` - Sitzungs-Timeout in Sekunden, nach deren Ablauf eine Benutzersitzung beendet wird.

`Minimum value` - 1, Maximalwert: 65535

`sessionCookieName` - Name des SessionCookies, den die BotNet-Funktion für das Tracking verwendet. Muss mit einem Buchstaben oder einer Zahl beginnen und kann aus 1 bis 31 Buchstaben, Zahlen und den Bindestrichen (-) und Unterstrichen (_) bestehen. Die folgende Anforderung gilt nur für die NetScaler CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Cookie-Name” oder “mein Cookie-Name”). Maximale Länge: 31

`dfpRequestLimit` — Anzahl der Anfragen, die ohne Bot-Sitzungscookie zugelassen werden sollen, wenn der Gerätefingerabdruck aktiviert ist. Mindestwert: 1, Maximalwert: 4294967295

`signatureAutoUpdate` - Flagge, die verwendet wird, um Bot-Signaturen für automatische Aktualisierungen zu aktivieren/deaktivieren. Mögliche Werte: ON, OFF.
Standardwert: OFF

`signatureUrl` - URL zum Herunterladen der Bot-Signaturzuordnungsdatei vom Server. Vorgabewert: `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`.
Maximale Länge: 2047

`proxyServer` - Proxy-Server-IP zum Abrufen aktualisierter Signaturen von AWS.

`proxyPort` - Proxy-Server-Port zum Abrufen aktualisierter Signaturen von AWS. Standardwert: 8080

`proxyUsername` - Benutzername zur Authentifizierung beim Proxyserver für das Herunterladen von Signaturaktualisierungen.

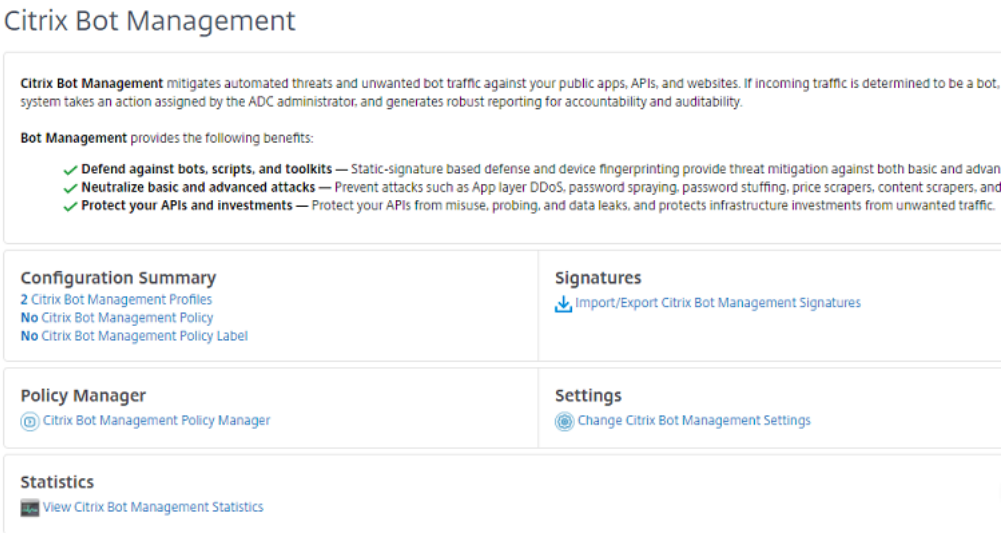
`proxyPassword` — Passwort zur Authentifizierung beim Proxyserver für das Herunterladen von Signaturaktualisierungen.

Beispiel:

```
set bot settings -defaultProfile profile1 -javaScriptName json.js -sessionTimeout
 1000 -sessionCookieName session -proxyServer 10.102.30.112 -proxyPort 3128
-proxyUsername defaultuser -proxyPassword defaultPassword
```

Konfigurieren der Bot-Verwaltung über die NetScaler-GUI

Sie können die NetScaler-Bot-Verwaltung konfigurieren, indem Sie zuerst die Funktion auf der Appliance aktivieren. Sobald Sie aktiviert haben, können Sie eine Bot-Richtlinie erstellen, um den eingehenden Traffic als Bot auszuwerten und den Traffic an das Bot-Profil zu senden. Dann erstellen Sie ein Bot-Profil und binden das Profil dann an eine Bot-Signatur. Alternativ können Sie auch die Standard-Bot-Signaturdatei klonen und die Signaturdatei verwenden, um die Erkennungstechniken zu konfigurieren. Nachdem Sie die Signaturdatei erstellt haben, können Sie sie in das Bot-Profil importieren.

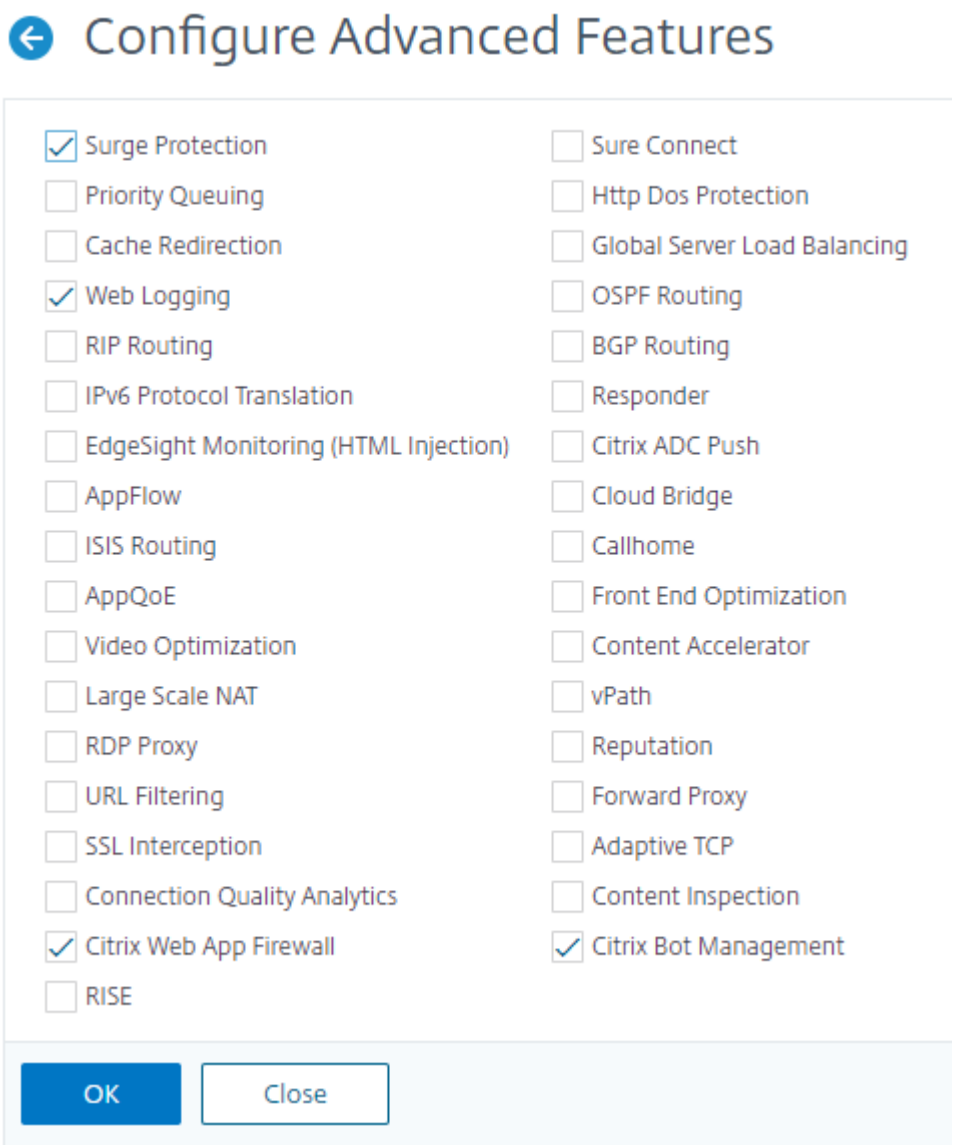


1. Bot-Management-Funktion aktivieren
2. Konfigurieren von Bot-Verwaltungseinstellungen
3. NetScaler-Bot-Standardsignatur klonen
4. NetScaler-Bot-Signatur importieren
5. Konfigurieren Sie Bot Einstellungen für die
6. Erstellen Sie ein Bot-Profil
7. Erstellen Sie Bot-Richtlinie

Bot-Management-Funktion aktivieren

Führen Sie die folgenden Schritte aus, um das Bot-Management zu aktivieren

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Wählen Sie auf der Seite „ **Erweiterte Funktionen konfigurieren** “ das Kontrollkästchen **Bot-Management** aus.
3. Klicken Sie auf **OK** und dann auf **Schließen**.



Konfigurieren der Bot-Verwaltungseinstellungen für die Geräte-Fingerabdruck-

Führen Sie den folgenden Schritt aus, um die Fingerabdrucktechnik des Geräts zu konfigurieren:

1. Navigieren Sie zu **Security** > **NetScaler Bot Management**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **NetScaler bot Management-Einstellungen ändern**.
3. Legen Sie in den **NetScaler bot-Verwaltungseinstellungen konfigurieren** die folgenden Parameter fest.
   a) Standardprofil. Wähle ein Bot-Profil aus.
   b) JavaScript-Name Name der JavaScript-Datei, die das Bot-Management in seiner Antwort

an den Client verwendet.

c) Sitzungstimeout. Timeout in Sekunden, nach dem die Benutzersitzung beendet wird.

d) Sitzungs-Cookie. Name des Sitzungscookies, das das Bot-Managementsystem zur Verfolgung verwendet.

e) Limit für Geräte-Fingerabdruck-Anfragen Anzahl der Anfragen, die ohne Bot-Sitzungscookie zugelassen werden sollen, wenn der Gerätefingerabdruck aktiviert ist.

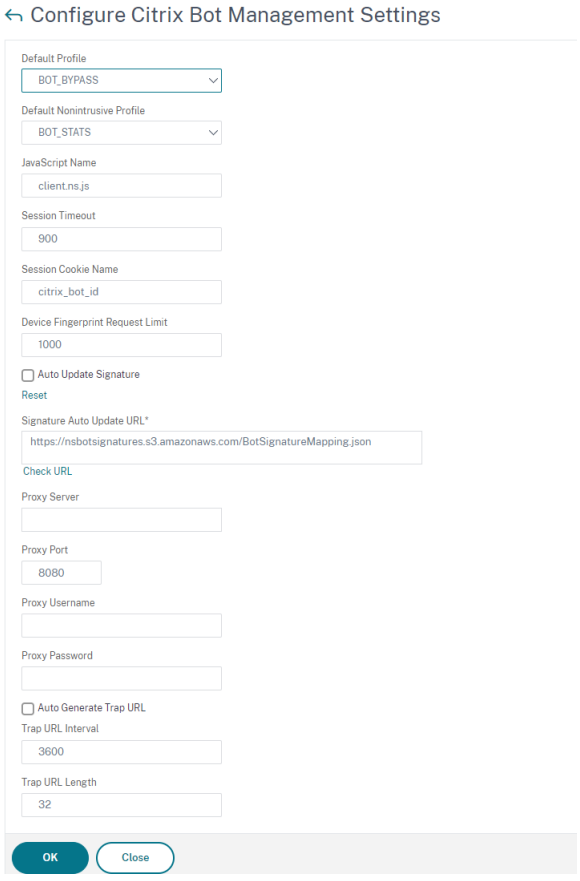
f) Proxyserver — IP-Adresse des Proxyservers, von dem die neuesten Signaturen hochgeladen werden.

g) Proxy-Port — Portnummer des Computers, von dem die neuesten Signaturen hochgeladen werden.

h) Proxy-Benutzername — Benutzername für die Authentifizierung des Proxyservers

i) Proxy-Passwort — Passwort für die Authentifizierung des Proxyservers.

> **Hinweis:**
>
> Die Felder Proxybenutzername und Proxy-Passwort sind aktiviert, wenn die Felder Proxy-Server und Proxy-Port konfiguriert sind.

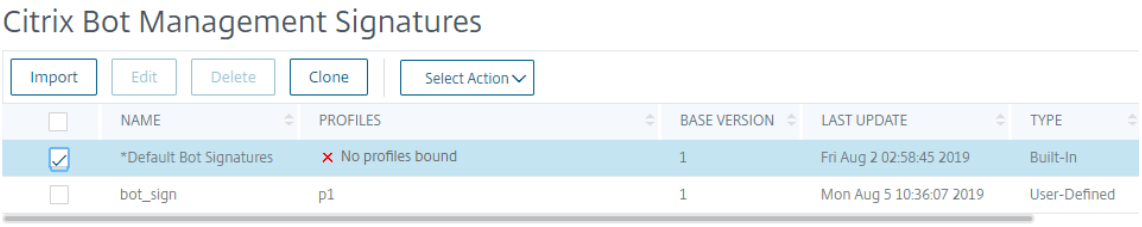


4. Klicken Sie auf **OK**.

Klonen der Bot-Signaturdatei

Führen Sie den folgenden Schritt aus, um die Bot-Signaturdatei zu klonen:

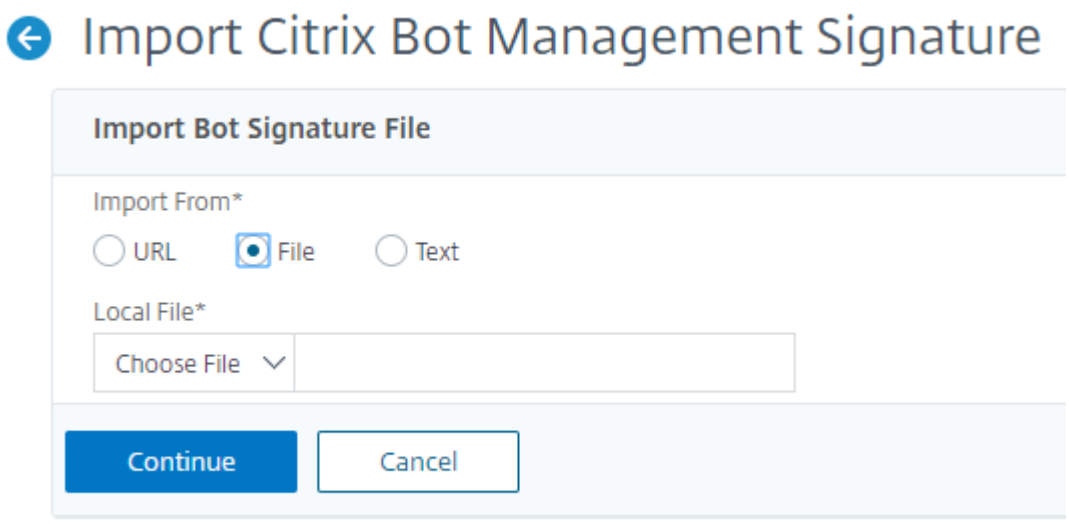
1. Navigieren Sie zu **Sicherheit** > **NetScaler Bot Management** und **Signatures**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Signatures** den Standard-Bot-Signaturdatensatz aus und klicken Sie auf **Klonen**.
3. Geben Sie auf der Seite **Bot-Signatur klonen** einen Namen ein und bearbeiten Sie die Signaturdaten.
4. Klicken Sie auf **Erstellen**.



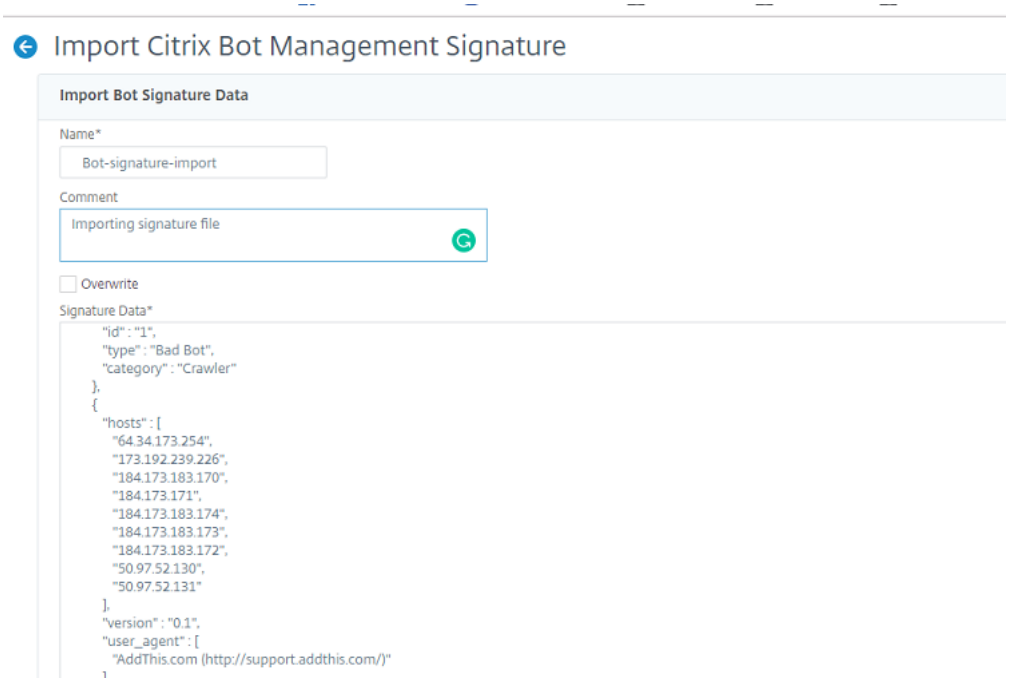
Importieren von Bot-Signatur

Wenn Sie eine eigene Signaturdatei haben, können Sie diese als Datei, Text oder URL importieren. Führen Sie die folgenden Schritte aus, um die Bot-Signaturdatei zu importieren:

1. Navigieren Sie zu **Sicherheit** > **NetScaler Bot Management** und **Signatures**.
2. Importieren Sie die Datei auf der Seite **NetScaler Bot Management Signatures** als URL, Datei oder Text.
3. Klicken Sie auf **Weiter**.



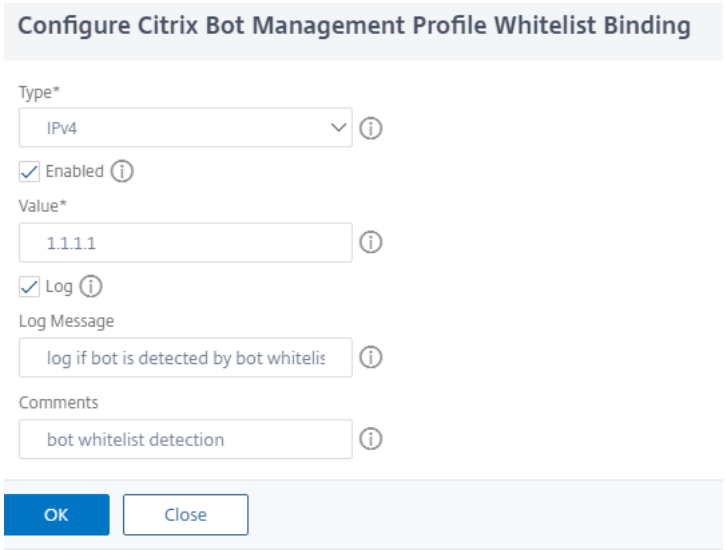
4. Stellen Sie auf der Seite NetScaler Bot Management Signature importieren die folgenden Parameter ein.
   a) Name — Name der Bot-Signaturdatei.
   b) Kommentar — Kurze Beschreibung der importierten Datei.
   c) Überschreiben — Aktivieren Sie das Kontrollkästchen, um das Überschreiben von Daten während der Dateiaktualisierung zuzulassen.
   d) Signaturdaten — Signaturparameter ändern
5. Klicken Sie auf **Fertig**.



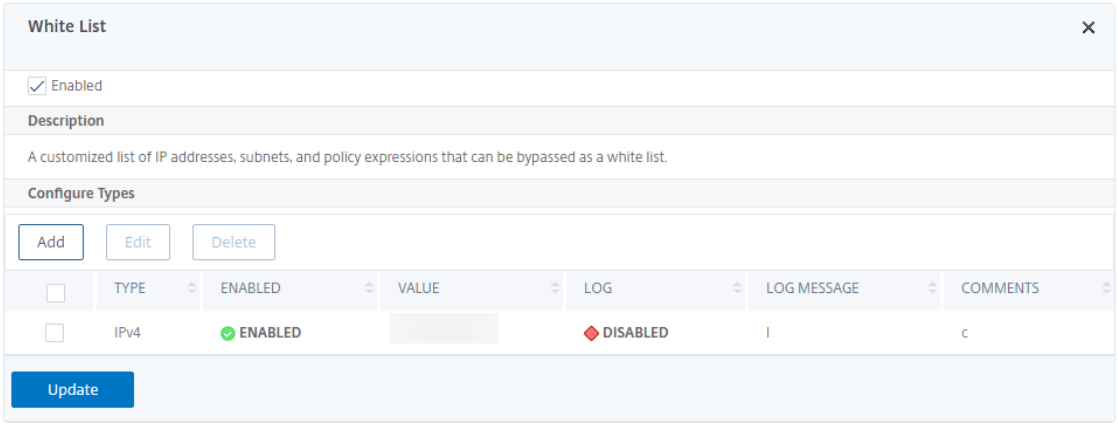
Konfigurieren der Bot-Positivliste über die NetScaler-GUI

Mit dieser Erkennungstechnik können Sie URLs umgehen, die Sie als Positivliste konfigurieren. Führen Sie den folgenden Schritt aus, um eine Positivliste zu konfigurieren:

1. Navigieren Sie zu **Sicherheit** > **NetScaler Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** eine Datei aus und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der Seite mit dem **NetScaler Bot Management-Profil** zum Abschnitt **Signature-instellungen** und klicken Sie auf **Positivliste**.
4. Stellen Sie im Abschnitt **Positivliste** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um die URLs der Zulassungsliste im Rahmen des Erkennungsprozesses zu validieren.
   b) Konfigurieren Sie Typen. Konfigurieren Sie eine URL für Positivlisten Die URL wird während der Bot-Erkennung umgangen. Klicken Sie auf Hinzufügen, um der Bot-Positivliste eine URL hinzuzufügen.
   c) Stellen Sie auf der Seite **Configure NetScaler Bot Management Profile Whitelist Binding** die folgenden Parameter ein:
      i. Typ. Der URL-Typ kann eine IPv4-Adresse, eine Subnetz-IP-Adresse oder eine IP-Adresse sein, die einem Richtlinienausdruck entspricht.
      ii. Aktiviert. Wählen Sie das Kontrollkästchen aus, um die URL zu validieren.
      iii. Wert. URL-Adresse.
      iv. Protokoll. Wählen Sie das Kontrollkästchen aus, um Protokolleinträge zu speichern.
      v. Nachricht protokollieren. Kurzbeschreibung des Protokolls.
      vi. Kommentare. Kurze Beschreibung der URL der Positivliste.
      vii. Klicken Sie auf **OK**.



5. Klicken Sie auf **Update**.
6. Klicken Sie auf **Fertig**.

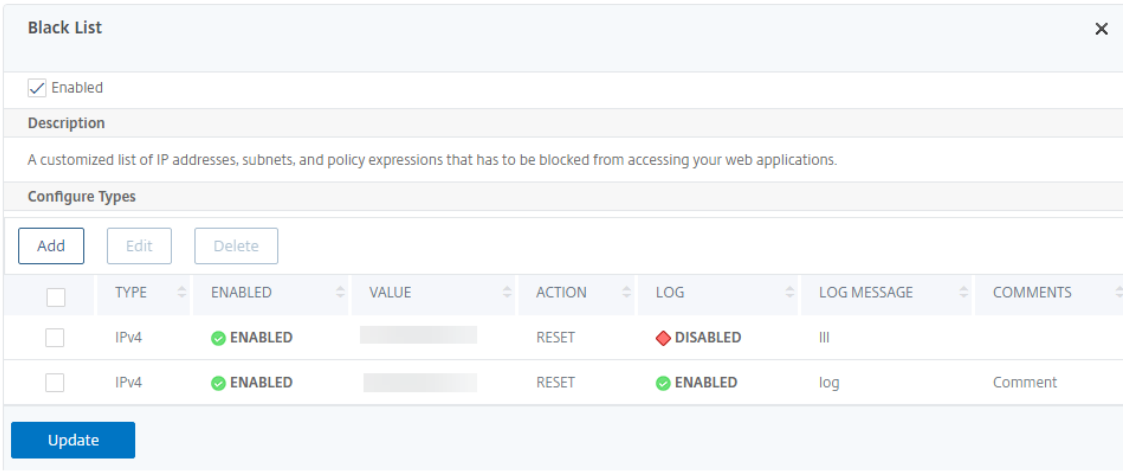


Konfigurieren Sie die Bot-Sperrliste über die NetScaler-GUI

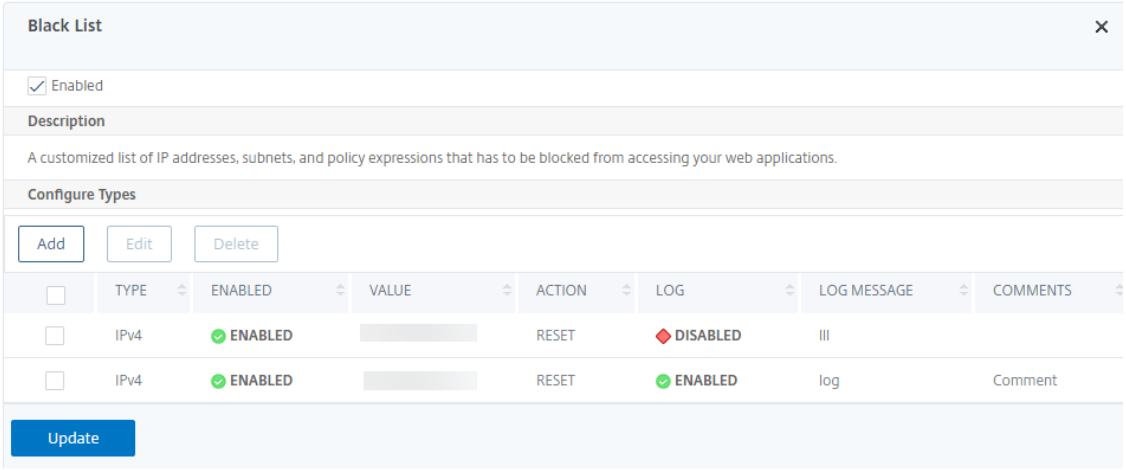
Mit dieser Erkennungstechnik können Sie die URLs löschen, die Sie als Sperrlisten-URLs konfigurieren. Führen Sie den folgenden Schritt aus, um eine Sperrlisten-URL zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **NetScaler Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** eine Signaturdatei aus und klicken Sie auf **Bearbeiten.**
3. Gehen Sie auf der Seite mit dem **NetScaler Bot Management-Profil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **Sperrliste**.
4. Stellen Sie im Abschnitt **Black List** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um Blocklisten-URLs im Rahmen des Erkennungsprozesses zu validieren.
   b) Konfigurieren Sie Typen. Konfigurieren Sie eine URL, um Teil des Erkennungsprozesses für Bot-Sperrlisten zu sein. Diese URLs werden während der Bot-Erkennung gelöscht. Klicken Sie auf Hinzufügen, um eine URL zur Bot-Sperrliste hinzuzufügen.
   c) Stellen Sie auf der Seite **Configure NetScaler Bot Management Profile Blacklist Binding** die folgenden Parameter ein.
      i. Typ. Der URL-Typ kann eine IPv4-Adresse, eine Subnetz-IP-Adresse oder eine IP-Adresse sein.
      ii. Aktiviert. Wählen Sie das Kontrollkästchen aus, um die URL zu validieren.
      iii. Wert. URL-Adresse.
      iv. Protokoll. Wählen Sie das Kontrollkästchen aus, um Protokolleinträge zu speichern.
      v. Nachricht protokollieren. Kurzbeschreibung des Logins.

vi. Kommentare. Kurze Beschreibung über die Sperrlisten-URL.
vii. Klicken Sie auf **OK**.



5. Klicken Sie auf **Update**.
6. Klicken Sie auf **Fertig**.



Konfigurieren Sie die IP-Reputation über die NetScaler-GUI

Die IP-Reputations-Bot-Technik verwendet die IP-Reputationsdatenbank und die Cloud-Dienstanbieter-Datenbank von Webroot, um zu überprüfen, ob es sich bei einer Clientanforderung um eine schädliche IP-Adresse oder eine Public Cloud- Als Teil der Bot-Kategorien wird konfiguriert und dann wird eine Bot-Aktion zugeordnet. Führen Sie die folgenden Schritte aus, um die Webroot IP-Reputation- und Cloud-Dienstanbieter-Datenbankkategorien zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **NetScaler bot-Verwaltung** und **Profile**.
2. Wählen Sie auf der Seite **NetScaler bot Management-Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.

3. Gehen Sie auf der Seite mit dem **NetScaler bot Management Profile** zum Abschnitt **Profile Settings** und klicken Sie auf **IP Reputation**.
4. Stellen Sie im Abschnitt **IP-Reputation** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um den eingehenden Bot-Verkehr im Rahmen des Erkennungsprozesses zu validieren.
   b) Kategorien konfigurieren. Sie können die IP-Reputationstechnik für eingehenden Bot-Verkehr in verschiedenen Kategorien verwenden. Basierend auf der konfigurierten Kategorie können Sie den Bot-Traffic löschen oder umleiten. Klicken Sie auf **Hinzufügen**, um eine schädliche Bot-Kategorie zu konfigurieren.
   c) Legen Sie auf der Seite **IP-Reputationsbindung des NetScaler bot-Verwaltungsprofils konfigurieren** die folgenden Parameter fest:
      i. Kategorie. Wählen Sie eine Webroot IP-Reputation-Bot-Kategorie aus, um eine Clientanfrage als schädliche IP-Adresse zu validieren.
         A. IP_BASED - Diese Kategorie prüft, ob die Client-IP-Adresse (IPv4 und IPv6) schädlich ist oder nicht.
         B. BOTNET - Diese Kategorie umfasst Botnet-C&C-Kanäle und infizierte Zombie-Maschinen, die vom Bot-Master gesteuert werden.
         C. SPAM_SOURCES — Diese Kategorie umfasst das Tunneln von Spam-Nachrichten über einen Proxy, anomale SMTP-Aktivitäten und Spam-Aktivitäten im Forum.
         D. SCANNER - Diese Kategorie umfasst alle Aufklärungsvorgänge wie Sonden, Host-Scan, Domain-Scan und Kennwort-Brute-Force-Angriffe.
         E. DOS — Diese Kategorie umfasst DOS, DDOS, anomale Synchronisationsflut und Erkennung anomaler Datenverkehr.
         F. REPUTATION - Diese Kategorie verweigert den Zugriff von IP-Adressen (IPv4 und IPv6), von denen derzeit bekannt ist, dass sie mit Malware infiziert sind. Zu dieser Kategorie gehören auch IP-Adressen mit einem durchschnittlich niedrigen Webroot Reputation Index. Durch die Aktivierung dieser Kategorie wird der Zugriff von identifizierten Quellen verhindert, um Malware-Verteilungspunkte zu kontaktieren.
         G. PHISHING — Diese Kategorie umfasst IP-Adressen (IPv4 und IPv6), die Phishing-Sites und andere Arten von Betrugsaktivitäten wie Anzeigenklickbetrug oder Spielbetrug hosten.
         H. PROXY — Diese Kategorie umfasst IP-Adressen (IPv4 und IPv6), die Proxy-Dienste bereitstellen.
         I. NETWORK - IPs, die Proxy- und Anonymisierungsdienste bereitstellen, einschließlich The Onion Router alias TOR oder Dark Net.
         J. MOBILE_THREATS - Diese Kategorie überprüft die Client-IP-Adresse (IPv4 und IPv6) mit der Liste der für mobile Geräte schädlichen Adressen.

ii. Kategorie. Wählen Sie eine Kategorie des Webroot Public Cloud-Dienstanbieters aus, um zu überprüfen, ob es sich bei einer Clientanforderung um eine Public Cloud-

A. AWS — Diese Kategorie prüft die Client-IP-Adresse mit einer Liste der Public Cloud-Adressen von AWS.
B. GCP — Diese Kategorie überprüft die Client-IP-Adresse mit der Liste der Public-Cloud-Adressen von der Google Cloud Platform.
C. AZURE — Diese Kategorie prüft die Clientadresse mit einer Liste der Public Cloud-Adressen von Azure.
D. ORACLE — Diese Kategorie prüft Client-IP-Adressen mit einer Liste der Public Cloud-Adressen von Oracle.
E. IBM — Diese Kategorie prüft die Client-IP-Adresse mit einer Liste der Public Cloud-Adressen von IBM.
F. SALESFORCE — Diese Kategorie überprüft die Client-IP-Adresse mit einer Liste der Public Cloud-Adressen von Salesforce.

Mögliche Werte für Webroot IP-Reputation Bot-Kategorie: IP, BOTNETS, SPAM_SOURCES, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, MOBILE_THREATS.

Mögliche Werte für die Kategorie der Webroot Public Cloud-Dienstanbieter: AWS, GCP, AZURE, ORACLE, IBM, SALESFORCE.

iii. Aktiviert. Aktivieren Sie das Kontrollkästchen, um die Erkennung der IP-Reputationssignatur zu validieren.

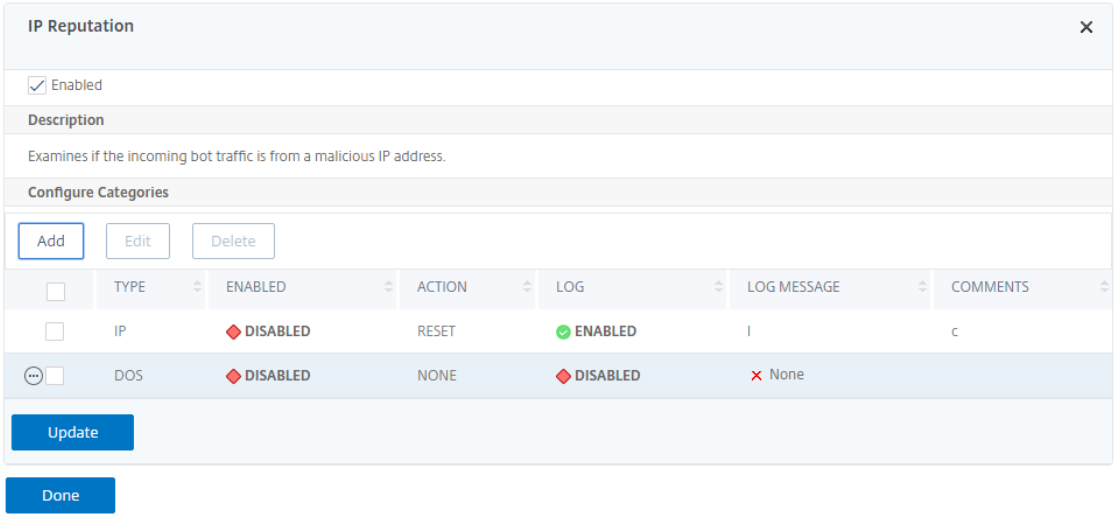
iv. Bot-Aktion. Basierend auf der konfigurierten Kategorie können Sie keine Aktion, keine Drop-, Umleitung- oder Minderungsaktion zuweisen.

v. Protokoll. Wählen Sie das Kontrollkästchen aus, um Protokolleinträge zu speichern.

vi. Nachricht protokollieren. Kurzbeschreibung des Protokolls.

vii. Kommentare. Kurze Beschreibung der Bot-Kategorie.

5. Klicken Sie auf **OK**.
6. Klicken Sie auf **Update**.
7. Klicken Sie auf **Fertig**.



> **Hinweis:**
>
> Wenn Sie die **IP-Reputation**deaktivieren, stellen Sie sicher, dass die Downloads gestoppt werden. Gehen Sie wie folgt vor, um die IP-Reputation-Downloads zu stoppen:
>
> 1. Navigieren Sie zu **Security > NetScaler bot Management > Change NetScaler bot Management Settings**.
> 2. Ändern Sie das **Default Nonintrusive Profile** in **BOT_BYPASS**.

Technik zur Begrenzung der Bot-Rate konfigurieren

Mit der Bot-Rate-Limit-Technik können Sie den Bot-Traffic innerhalb eines bestimmten Zeitrahmens basierend auf dem Standort Geolocation der Client-IP-Adresse, der Sitzung, dem Cookie oder der konfigurierten Ressource (URL) einschränken.
Durch die Konfiguration der Bot-Rate-Limit-Technik können Sie Folgendes sicherstellen:

- Blockieren Sie schädliche Bot-Aktivitäten.
- Reduzieren Sie die Verkehrsbelastung zu Webservern.

Bot-Ratenlimit mit NetScaler CLI konfigurieren

Geben Sie in der Befehlszeile Folgendes ein:

```
1 bind bot profile <name>... -ratelimit  -type <type> Geolocation -
    countryCode <countryName> -rate  <positive_integer> -timeSlice <
    positive_integer> [-action <action> ...] [-limitType ( BURSTY |
    SMOOTH )] [-condition <expression>] [-enabled ( ON | OFF )]
2 <!--NeedCopy-->
```

Hierbei gilt:

*SOURCE_IP - Ratenbegrenzung basierend auf der Client-IP-Adresse.

*SESSION - Ratenbegrenzung basierend auf dem konfigurierten Cookie-Namen.

*URL - Ratenbegrenzung basierend auf der konfigurierten URL.

*GEOLOCATION - Ratenbegrenzung basierend auf dem konfigurierten Ländernamen.

Possible values - SITZUNG, QUELL-IP, URL, GEOLOKALISIERUNG

Beispiel:

```
1  bind bot profile geo_prof -ratelimit -type Geolocation -countryCode IN
       -rate 100 -timeSlice 1000 -limitType SMOOTH -condition HTTP.REQ.
      HEADER("User-Agent").contains("anroid") -action log,drop -enabled
      on
2  <!--NeedCopy-->
```

Konfigurieren Sie das Bot-Ratenlimit über die NetScaler-GUI

Gehen Sie wie folgt vor, um die Technik zur Erkennung von Bot-Ratenlimits zu konfigurieren:

1. Navigieren Sie zu **Sicherheit > NetScaler Bot Management** und **Profiles**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der **NetScaler Bot Management-Profilseite** zum Abschnitt **Profileinstellungen** und klicken Sie auf **Rate Limit**.
4. Stellen Sie im Abschnitt **Rate Limit** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um den eingehenden Bot-Verkehr im Rahmen des Erkennungsprozesses zu validieren.
   b) Klicken Sie auf **Hinzufügen**, um Ratenlimit-Bindungen zu konfigurieren.
5. Stellen Sie auf der Seite **Configure NetScaler Bot Management Rate Limit** die folgenden Parameter ein.
   a) Typ — Ratenbegrenzung des Bot-Traffics auf der Grundlage der folgenden Parameter:
      i. Geolokalisierung — Ratenlimit basierend auf dem geografischen Standort des Benutzers.
      ii. source_IP — Ratenbegrenzung des Datenverkehrs basierend auf der Client-IP-Adresse.
      iii. Sitzung — Ratenbegrenzung des Bot-Traffics anhand des Sitzungs- oder Cookie-Namens.
      iv. URL — Ratenbegrenzung des Bot-Traffics basierend auf der konfigurierten URL.

b) Land — Wählen Sie eine Geolocation als Land oder Region aus.

c) Art des Ratenlimits — Schränkt die Art des Datenverkehrs auf der Grundlage der folgenden Typen ein.

- Bursty — Leitet alle Anfragen weiter, die innerhalb des festgelegten Schwellenwerts und des angegebenen Zeitraums liegen.
- Reibungslos — Leitet die Anfragen gleichmäßig über den angegebenen Zeitraum weiter.

d) Rate Limit Connection — Ermöglicht es Ihnen, mehrere Regeln für eine Bedingung zu erstellen.

e) Aktiviert — Wählen Sie das Kontrollkästchen aus, um den eingehenden Bot-Verkehr zu validieren.

f) Schwellenwert für Anfragen — Maximale Anzahl von Anfragen, die innerhalb eines bestimmten Zeitrahmens zulässig sind.

g) Zeitraum — Zeitrahmen in Millisekunden.

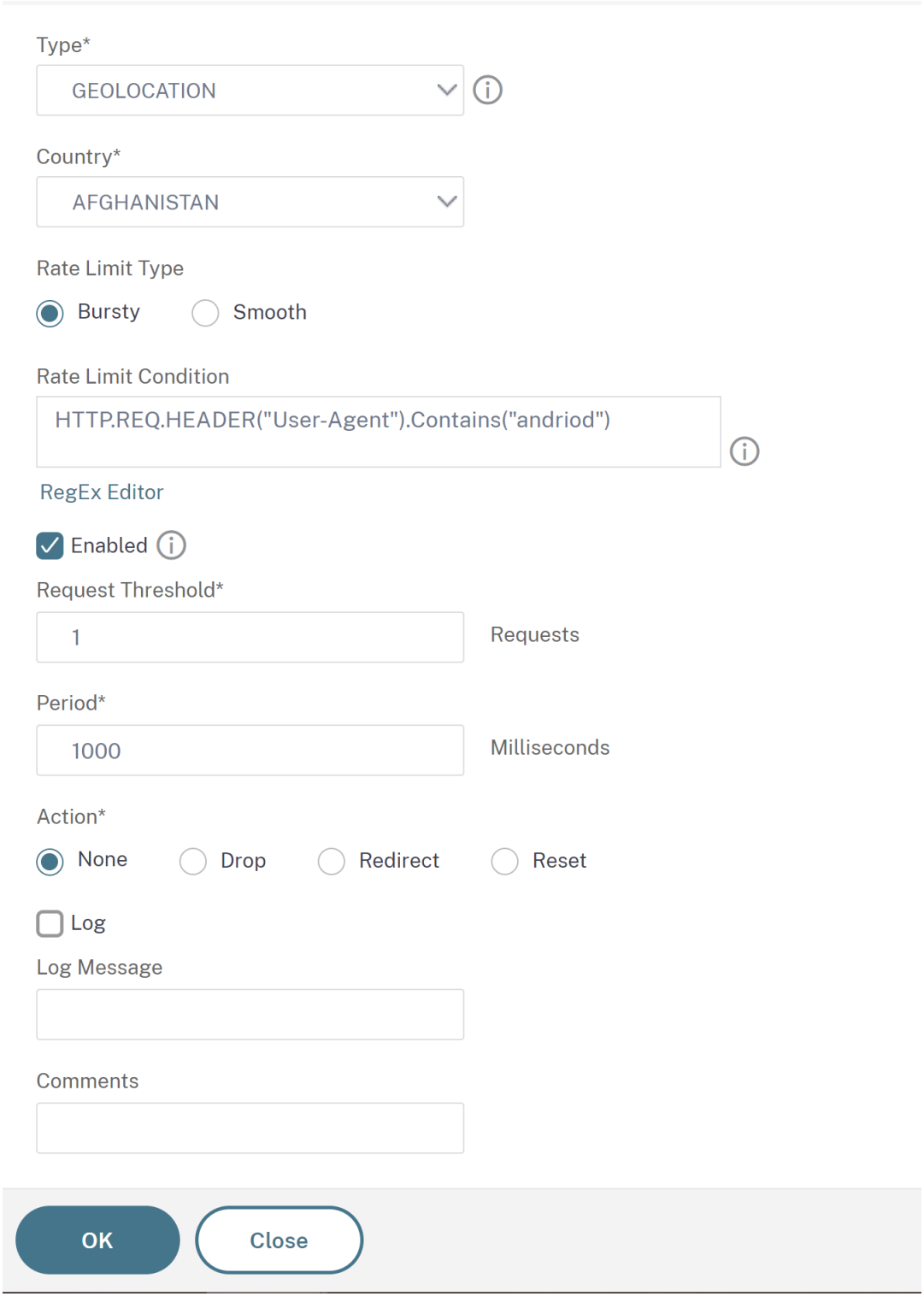
h) Aktion — Wählen Sie eine Bot-Aktion für die ausgewählte Kategorie aus.

i) Protokoll — Aktivieren Sie das Kontrollkästchen, um Protokolleinträge zu speichern.

j) Protokollnachricht — Kurze Beschreibung des Protokolls.

k) Kommentare — Kurze Beschreibung der Bot-Kategorie.

6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Update**.
8. Klicken Sie auf **Fertig**.

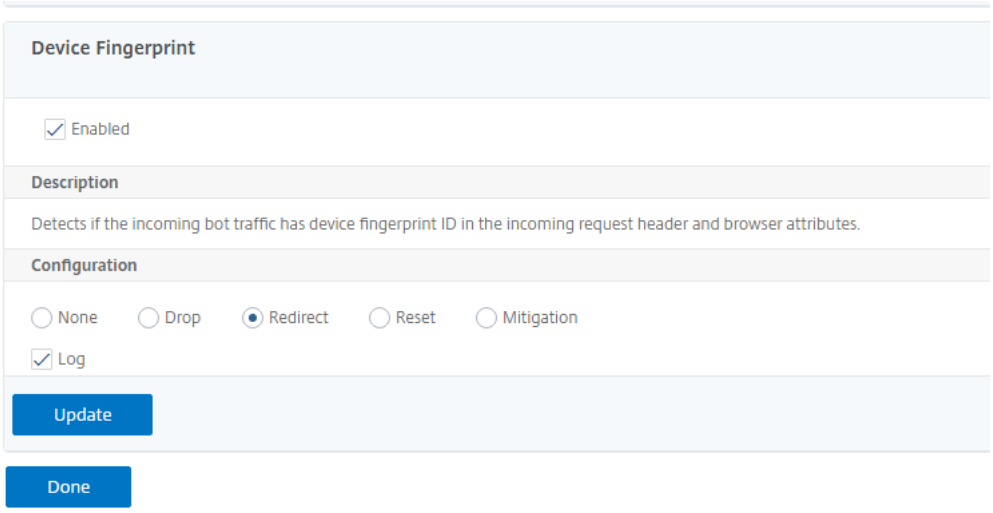


Konfigurieren Sie die Geräte-Fingerabdrucktechnik über die NetScaler-GUI

Diese Erkennungstechnik sendet eine Java-Skript-Herausforderung an den Client und extrahiert die Geräteinformationen. Basierend auf Geräteinformationen lässt die Technik den Bot-Verkehr fallen oder umgeht ihn. Folgen Sie den Schritten, um die Erkennungstechnik zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **NetScaler Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** eine Signaturdatei aus und klicken Sie auf **Bearbeiten.**
3. Gehen Sie auf der Seite mit dem **NetScaler Bot Management-Profil** zum Abschnitt **Signature-instellungen** und klicken Sie auf **Device Fingerprint**.
   Stellen Sie im Abschnitt **Gerätefingerabdruck** die folgenden Parameter ein:
   a) Enabled - Select to enable the rule.
   b) Configuration - Select one of the following options:
      i. None - Allows the traffic.
      ii. Drop - Drops the traffic.
      iii. Redirect - Redirects the traffic to error URL.
      iv. Mitigation, or CAPTCHA - Validates and allows the traffic.

      > **Note:**
      > During session replay attacks using the device fingerprint cookies, requests are dropped even if the device fingerprint configuration is set to **Mitigation**.
4. Klicken Sie auf **Update**.
5. Klicken Sie auf **Fertig**.



Konfigurieren der Geräte-Fingerabdruck-Technik für mobile (Android) -Anwendungen

Die Geräte-Fingerabdruck-Technik erkennt einen eingehenden Datenverkehr als Bot, indem ein JavaScript-Skript in die HTML-Antwort an den Client eingefügt wird. Wenn das JavaScript-Skript vom Browser aufgerufen wird, sammelt es Browser- und Client-Attribute und sendet eine Anfrage an die Appliance. Die Attribute werden untersucht, um festzustellen, ob es sich bei dem Traffic um einen Bot oder einen Menschen handelt.

Die Erkennungstechnik wird weiter erweitert, um Bots auf einer mobilen (Android) Plattform zu erkennen. Im Gegensatz zu Webanwendungen gilt im mobilen (Android) -Verkehr die Bot-Erkennung basierend auf dem JavaScript-Skript nicht. Um Bots in einem Mobilfunknetz zu erkennen, verwendet die Technik ein Bot Mobile SDK, das clientseitig in mobile Anwendungen integriert ist. Das SDK fängt den mobilen Verkehr ab, sammelt Gerätedetails und sendet die Daten an die Appliance. Auf der Appliance-Seite untersucht die Erkennungstechnik die Daten und bestimmt, ob die Verbindung von einem Bot oder einem Menschen stammt.

So funktioniert die Geräte-Fingerabdrucktechnik für die mobile Anwendung

In den folgenden Schritten wird der Workflow zur Bot-Erkennung erläutert, um festzustellen, ob eine Anfrage von einem mobilen Gerät von einem Menschen oder einem Bot stammt.

1. Wenn ein Benutzer mit einer mobilen Anwendung interagiert, zeichnet das Bot-SDK für Mobilgeräte das Verhalten des Geräts auf.
2. Der Client sendet eine Anfrage an die NetScaler-Appliance.
3. Beim Senden der Antwort fügt die Appliance ein Bot-Sitzungscookie mit Sitzungsdetails und Parametern ein, um Clientparameter zu erfassen.
4. Wenn die mobile Anwendung die Antwort erhält, validiert das in die mobile Anwendung integrierte NetScaler-Bot-SDK die Antwort, ruft die aufgezeichneten Fingerabdruckparameter des Geräts ab und sendet sie an die Appliance.
5. Die Technik zur Erkennung von Fingerabdrücken des Geräts auf der Appliance-Seite validiert die Gerätedetails und aktualisiert das Bot-Sitzungscookie, ob es sich um einen vermuteten Bot handelt oder nicht.
6. Wenn das Cookie abgelaufen ist oder der Fingerabdruckschutz des Geräts es vorzieht, Geräteparameter regelmäßig zu validieren und zu sammeln, wird der gesamte Vorgang oder die Herausforderung wiederholt.

Voraussetzung

Um mit der NetScaler-Technik zur Erkennung von Fingerabdrücken für mobile Anwendungen zu beginnen, müssen Sie das Bot Mobile SDK in Ihrer mobilen Anwendung herunterladen und installieren.

Konfigurieren Sie die Technik der Fingerabdruckerkennung für mobile (Android) -Anwendungen über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

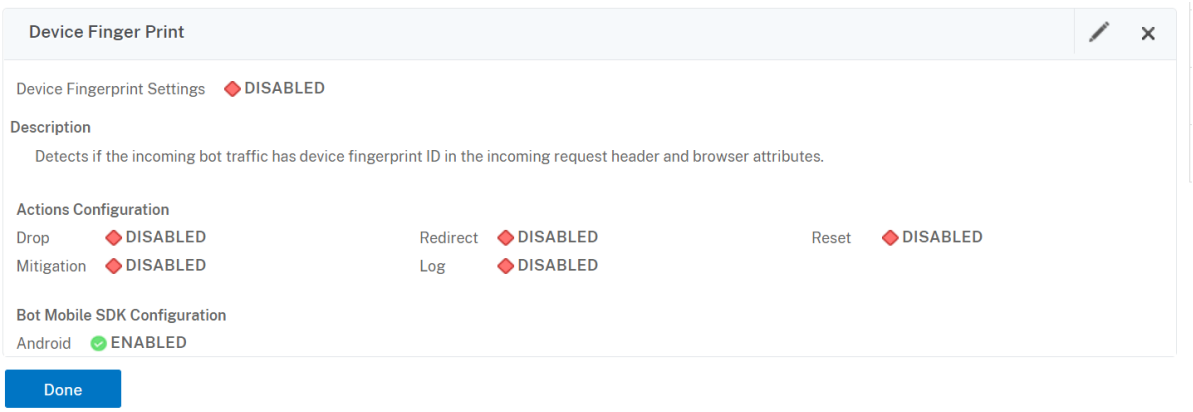
```
set bot profile <profile name> -deviceFingerprintMobile ( NONE | Android )
```

Beispiel:

```
set bot profile profile 1 -deviceFingerprintMobile Android
```

Konfigurieren Sie die Technik zur Erkennung von Geräte-Fingerabdrücken für mobile (Android) -Anwendungen über die GUI

1. Navigieren Sie zu **Sicherheit** > **NetScaler Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** eine Datei aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite mit dem **NetScaler Bot Management-Profil** unter **Profileinstellungen** auf **Device Fingerprint**.
4. Wählen **Sie im Abschnitt Configure Bot Mobile SDK** den Typ des mobilen Clients aus.
5. Klicken Sie auf **Aktualisieren** und **Fertig**.



Bot-Log-Ausdruck konfigurieren

Wenn der Client als Bot identifiziert wird, können Sie mit dem NetScaler-Bot-Management zusätzliche Informationen als Protokollnachrichten erfassen. Die Daten können der Name des Benutzers sein, der die URL angefordert hat, die Quell-IP-Adresse und der Quellport, von dem der Benutzer die Anforderung oder Daten gesendet hat, die aus einem Ausdruck generiert wurden. Um eine benutzerdefinierte Protokollierung durchzuführen, müssen Sie einen Protokollausdruck im Bot-Verwaltungsprofil konfigurieren.

Binden Sie den Log-Ausdruck im Bot-Profil über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

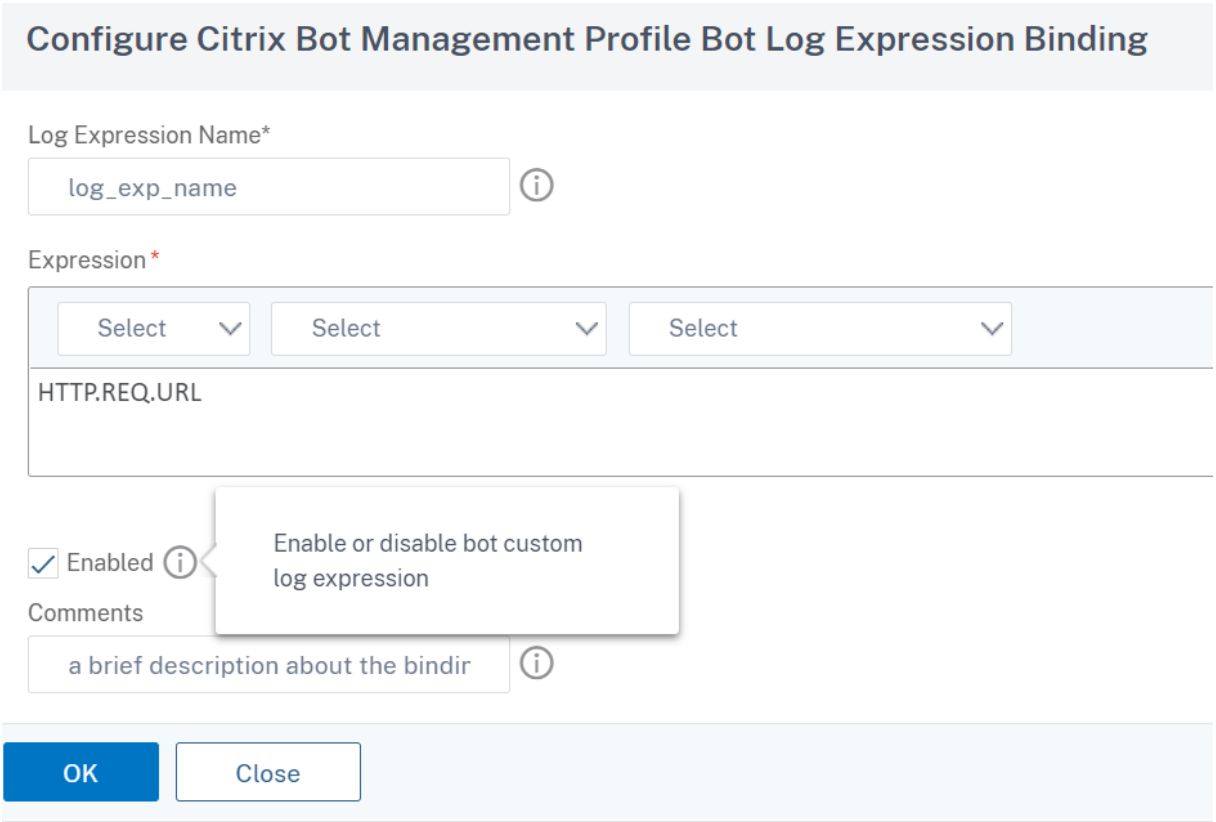
```
bind bot profile <name> (-logExpression -name <string> -expression <
    expression> [-enabled ( ON | OFF )]) -comment <string>
<!--NeedCopy-->
```

Beispiel:

```
bind bot profile profile1 -logExpression exp1 -expression HTTP.REQ.URL -
enabled ON -comment "testing log expression"
```

Binden Sie den Log-Ausdruck über die GUI an das Bot-Profil

1. Navigieren Sie zu **Sicherheit > NetScaler Bot Management > Profile**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** im Abschnitt **Profileinstellungen** die Option **Bot Log Expressions** aus.
3. Klicken Sie im Abschnitt Einstellungen für **Bot Log Expression Settings* auf **Hinzufügen**.
4. Stellen Sie auf der Seite **Configure NetScaler Bot Management Profile Bot Log Expression Binding** die folgenden Parameter ein.
   a) Name des Protokollausdrucks Name des Protokollausdrucks.
   b) Ausdruck. Geben Sie den Log-Ausdruck ein.
   c) Aktiviert. Aktivieren oder deaktivieren Sie die Bindung des Logausdrucks.
   d) Kommentare. Eine kurze Beschreibung zur Bindung des Bot-Log-Ausdrucks.
5. Klicken Sie auf**OK** und **Fertig**.



Konfigurieren der Bot-Trap-Technik

Die NetScaler-Bot-Trap-Technik fügt zufällig oder regelmäßig eine Trap-URL in die Serverantwort ein. Sie können auch eine Trap-URL-Liste erstellen und URLs dafür hinzufügen. Die URL erscheint unsichtbar und nicht zugänglich, wenn der Client ein menschlicher Benutzer ist. Wenn der Client jedoch ein automatisierter Bot ist, ist die URL zugänglich, und wenn darauf zugegriffen wird, wird der Angreifer als Bot kategorisiert und jede nachfolgende Anfrage des Bot wird blockiert. Die Trap-Technik blockiert effektiv Angriffe von Bots.

Die Trap-URL ist eine alphanumerische URL mit konfigurierbarer Länge und wird im konfigurierbaren Intervall automatisch generiert. Mit dieser Technik können Sie auch eine URL zum Einfügen von Traps für am häufigsten besuchte Sites oder häufig besuchte Sites konfigurieren. Auf diese Weise können Sie den Zweck festlegen, die Bot-Trap-URL für Anforderungen einzufügen, die der URL zum Einfügen von Traps entsprechen.

> **Hinweis:**
>
> Obwohl die Bot-Trap-URL automatisch generiert wird, ermöglicht Ihnen das NetScaler-Bot-

> Management weiterhin die Konfiguration einer benutzerdefinierten Trap-URL im Bot-Profil. Dies geschieht, um
> die Bot-Erkennungstechnik zu stärken und Angreifern den Zugriff auf die Trap-URL zu erschweren.

Um die Konfiguration der Bot-Trap abzuschließen, müssen Sie die folgenden Schritte ausführen.

1. Bot-Trap-URL aktivieren
2. Konfigurieren der Bot-Trap-URL im Bot-Profil
3. Binden Sie die URL zum Einfügen von Bot-Traps an
4. Konfigurieren Sie die Länge und das Intervall der Bot-Trap-URL in den Bot

Den URL-Schutz für Bot-Trap aktivieren

Bevor Sie beginnen können, müssen Sie sicherstellen, dass der URL-Schutz für die Bot-Trap auf der Appliance aktiviert ist. Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature Bot
```

Konfigurieren der Bot-Trap-URL im Bot-Profil

Sie können die Bot-Trap-URL konfigurieren und eine Trap-Aktion im Bot-Profil angeben.
Geben Sie in der Befehlszeile Folgendes ein:

```
add bot profile <name> -trapURL <string> -trap ( ON | OFF )-trapAction <
trapAction>
```

Hierbei gilt:

- `trapURL` ist die URL, die der Bot-Schutz als Trap-URL verwendet. Maximale Länge: 127
- `trap` dient dazu, die Bot-Trap-Erkennung zu aktivieren. Mögliche Werte: ON, OFF. Standardwert: OFF
- `trapAction` ist eine Aktion, die auf der Grundlage der Bot-Erkennung ergriffen werden muss. Mögliche Werte: NONE, LOG, DROP, REDIRECT, RESET, MITIGATION. Standardwert: NONE

Beispiel:

```
add bot profile profile1 -trapURL www.bottrap1.com trap ON -trapAction
RESET
```

Binden Sie die URL zum Einfügen von Bot-Traps an

Sie können die URL zum Einfügen von Bot-Traps konfigurieren und an das Bot-Profil binden.
Geben Sie in der Befehlszeile Folgendes ein:


```
bind bot profile <profile_name> trapInsertionURL -url <url> -enabled ON|OFF
-comment <comment>
```

Hierbei gilt:

URL — Das Regex-Muster der Anforderungs-URL, für das die Bot-Trap-URL eingefügt wird. Maximale Länge: 127

Beispiel:

```
bind bot profile profile1 trapInsertionURL -url www.example.com -enabled ON
-comment insert a trap URL randomly
```

Konfigurieren Sie die Länge und das Intervall der Bot-Trap-URL in den Bot

Sie können die Länge der Bot-Trap-URL konfigurieren und das Intervall festlegen, um die Bot-Trap-URL automatisch zu generieren.
Geben Sie in der Befehlszeile Folgendes ein:

```
set bot settings -trapURLAutoGenerate ( ON | OFF )-trapURLInterval <positive_integer
> -trapURLLength <positive_integer>
```

Hierbei gilt:

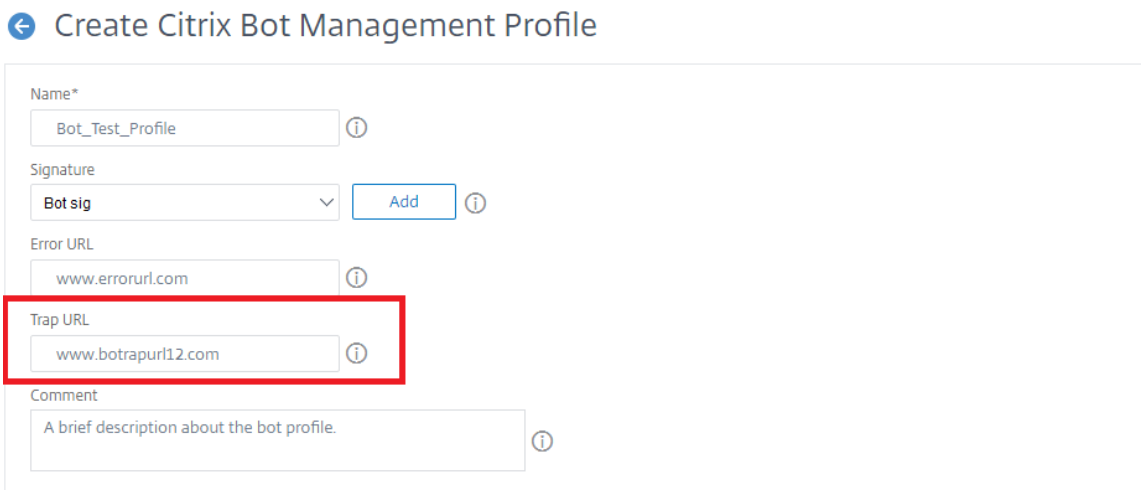
- trapURLInterval ist die Zeit in Sekunden, nach der die Bot-Trap-URL aktualisiert wird. Standardwert: 3600, Mindestwert: 300, Maximalwert: 86400
- trapURLLength. Länge der automatisch generierten Bot-Trap-URL. Standardwert: 32, Mindestwert: 10, Maximalwert: 255

Beispiel:

```
set bot settings -trapURLAutoGenerate ON -trapURLInterval 300 -trapURLLength
 60
```

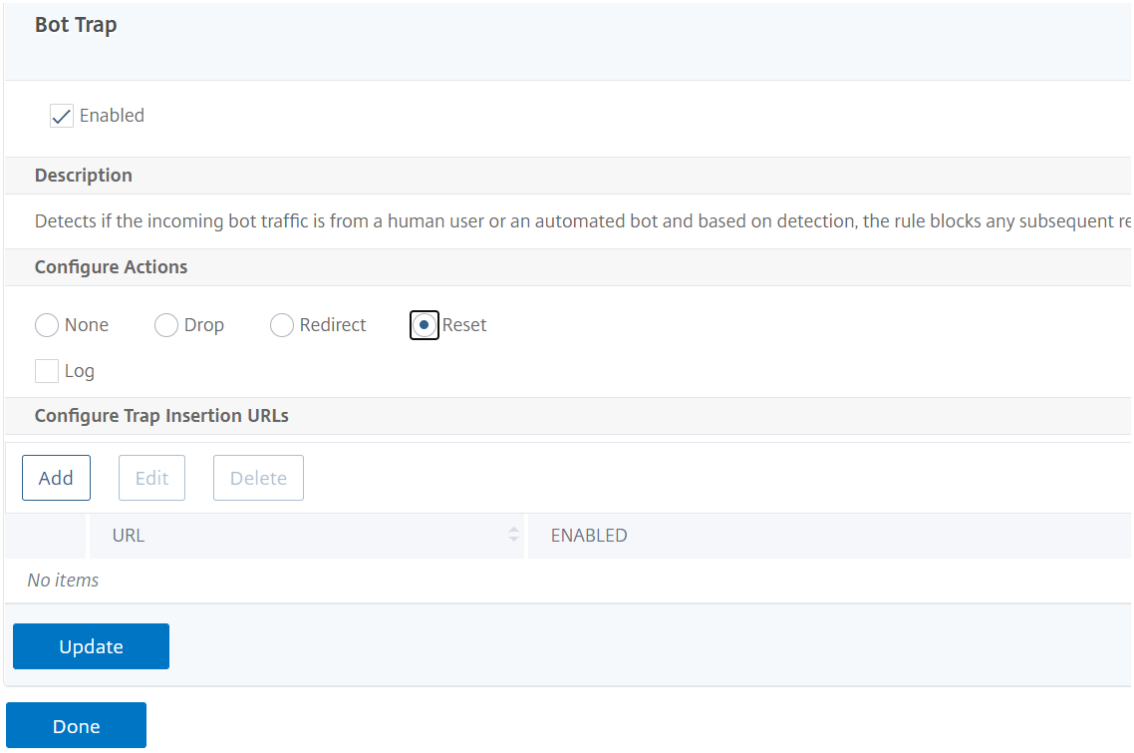
Konfigurieren Sie die Bot-Trap-URL über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Bot Management > Profile**.
2. Klicken Sie auf der Seite **NetScaler Bot Management Profiles** auf **Bearbeiten**, um die Bot-Trap-URL-Technik zu konfigurieren.
3. Geben Sie auf der Seite **NetScaler Bot Management-Profil erstellen** im Abschnitt Allgemein die Bot-Trap-URL ein.



4. Klicken Sie auf der Seite **NetScaler Bot Management-Profil erstellen** in den **Profileinstellungen** auf **Bot Trap**.
5. Stellen Sie im Abschnitt **Bot-Trap** die folgenden Parameter ein.

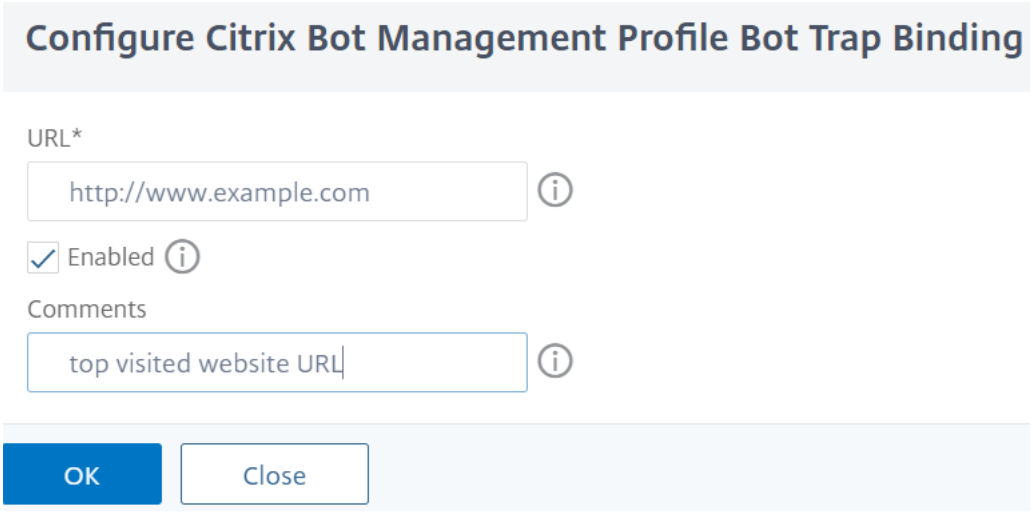
   a. Aktiviert. Wählen Sie das Kontrollkästchen, um die Bot-Trap-Erkennung zu aktivieren
   b. Beschreibung. Kurze Beschreibung der URL.
   c. Konfigurieren Sie Aktionen. Zu ergreifende Maßnahmen für Bot, die durch den Zugriff auf die Bot-Trap erkannt werden.



6. Klicken Sie im Abschnitt **Trap-Einfügungs-URLs konfigurieren** auf **Hinzufügen**.

7. Stellen Sie auf der Seite **Configure NetScaler Bot Management Profile Bot Trap Binding** die folgenden Parameter ein.

   a) Trap-URL. Geben Sie die zu bestätigende URL als URL zum Einfügen von Bot-Traps ein.
   b) Aktiviert. Aktiviert oder deaktiviert Bot-Trap-Einfüge-URL.
   c) Kommentar. Eine kurze Beschreibung der URL zum Einfügen von Traps.



8. Klicken Sie im Abschnitt **Signatureinstellungen** auf **Bot Trap**.
9. Stellen Sie im Abschnitt **Bot Trap** die folgenden Parameter ein:

   a) Aktiviert. Wählen Sie das Kontrollkästchen, um die Bot-Trap-Erkennung zu aktivieren.

   b) Stellen Sie im Abschnitt Konfigurieren die folgenden Parameter ein.

      i. Aktion. Zu ergreifende Maßnahmen für Bot, die durch den Zugriff auf die Bot-Trap erkannt werden.
      ii. Protokoll. Aktiviert oder deaktiviert die Protokollierung für die Bindung von Bot-Traps.

10. Klicken Sie auf **Aktualisieren** und **Fertig**.

Konfigurieren von Bot-Trap-URL-Einstellungen

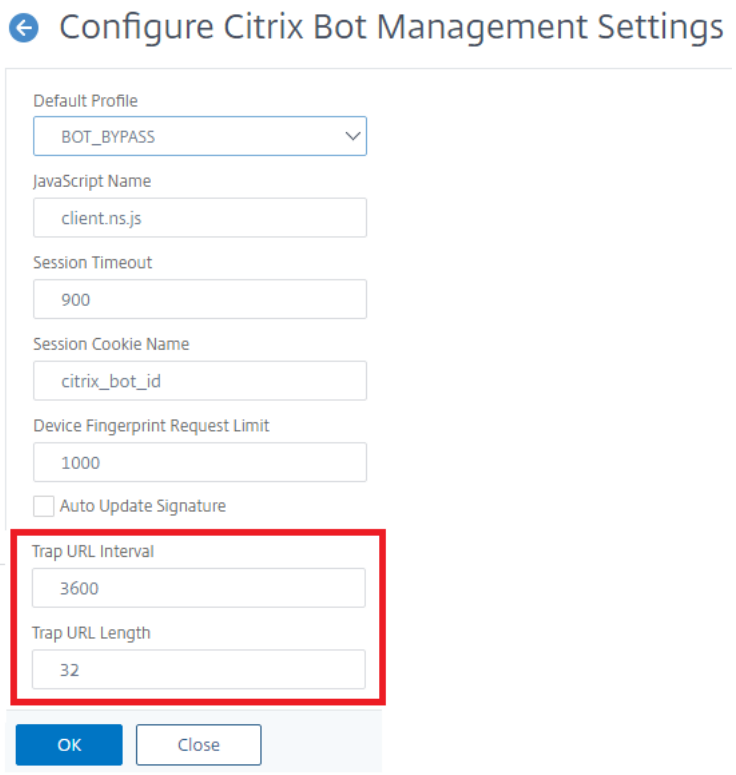
Führen Sie die folgenden Schritte aus, um die URL-Einstellungen für Bot-Trap zu konfigurieren

1. Navigieren Sie zu **Security > NetScaler Bot Management**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **NetScaler Bot Management-Einstellungen ändern**.
3. Stellen Sie unter **Configure NetScaler Bot Management Settings**die folgenden Parameter ein.

   a) Trap-URL-Intervall. Zeit in Sekunden, nach der die URL der Bot-Trap aktualisiert wird.

b) Länge der Trap-URL. Länge der automatisch generierten Bot-Trap-URL.

4. Klicken Sie auf **OK** und **Fertig**.



Ausdruck der Client-IP-Richtlinie zur Bot-Erkennung

Das NetScaler-Bot-Management ermöglicht es Ihnen jetzt, einen erweiterten Richtlinienausdruck zu konfigurieren, um die Client-IP-Adresse aus einem HTTP-Anforderungsheader, einem HTTP-Anforderungstext, einer HTTP-Anforderungs-URL oder mithilfe eines erweiterten Richtlinienausdrucks zu extrahieren. Die extrahierten Werte werden von einem Bot-Erkennungsmechanismus (wie TPS, Bot-Trap oder Ratenlimit) verwendet, um zu erkennen, ob es sich bei der eingehenden Anfrage um einen Bot handelt.

> **Hinweis:**
>
> Wenn Sie keinen Client-IP-Ausdruck konfiguriert haben, wird die Standard- oder vorhandene Quellclient-IP-Adresse für die Bot-Erkennung verwendet. Wenn ein Ausdruck konfiguriert ist, liefert das Auswertergebnis die Client-IP-Adresse, die für die Bot-Erkennung verwendet werden kann.

Sie können den Client-IP-Ausdruck konfigurieren und verwenden, um die tatsächliche Client-IP-Adresse zu extrahieren, wenn die eingehende Anforderung über einen Proxy-Server erfolgt und wenn die Client-IP-Adresse im Header vorhanden ist. Durch das Hinzufügen dieser Konfiguration kann die

Appliance den Bot-Erkennungsmechanismus verwenden, um Software-Clients und Servern mehr Sicherheit zu bieten.

Konfigurieren Sie den IP-Richtlinienausdruck des Clients im Bot-Profil über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add bot profile <name> [-clientIPExpression <expression>]
<!--NeedCopy-->
```

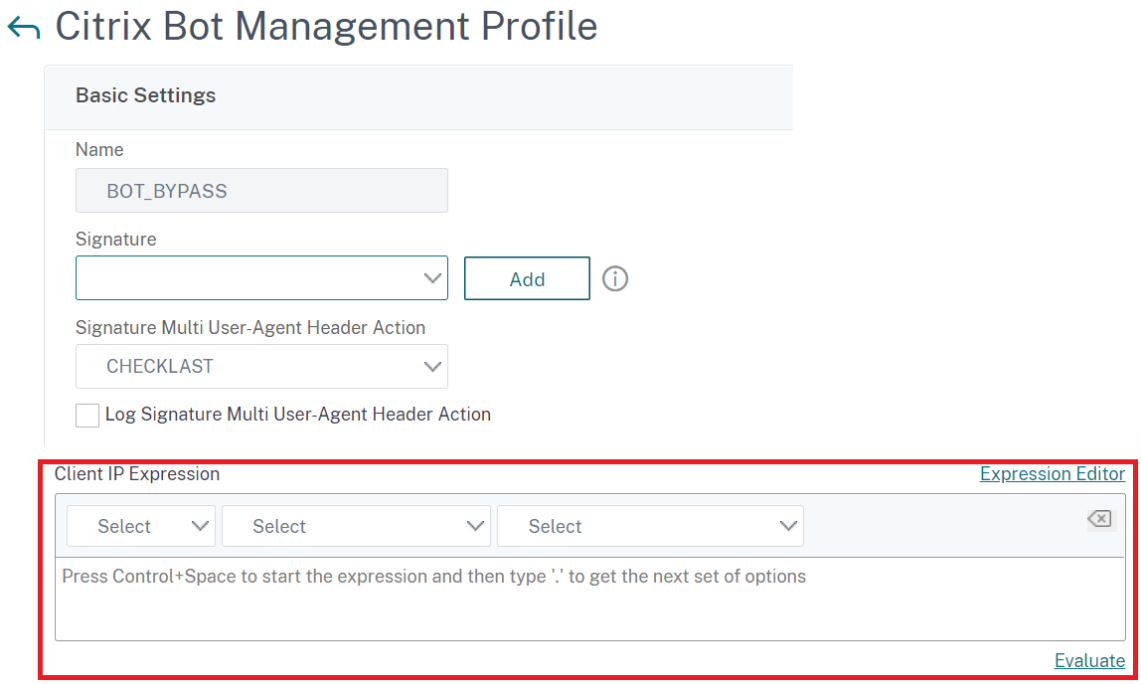
Beispiel:

```
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER("X-Forwarded-For")ALT CLIENT.IP.SRC.TYPECAST_TEXT_T'
```

```
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER("X-Forwarded-For")ALT CLIENT.IPv6.SRC.TYPECAST_TEXT_T'
```

Konfigurieren Sie den Ausdruck der Client-IP-Richtlinie im Bot-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Sicherheit > NetScaler Bot Management > Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **NetScaler Bot Management-Profil erstellen** den Client-IP-Ausdruck ein.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren von CAPTCHA für IP-Reputation und Gerätefingerabdruckerkennung

CAPTCHA ist ein Akronym, das für “Vollständig automatisierter öffentlicher Turing-Test, um Computer und Menschen voneinander zu unterscheiden” steht. CAPTCHA wurde entwickelt, um zu testen, ob ein eingehender Datenverkehr von einem menschlichen Benutzer oder einem automatisierten Bot stammt. CAPTCHA hilft dabei, automatisierte Bots zu blockieren, die Sicherheitsverletzungen für Webanwendungen verursachen. Im NetScaler verwendet CAPTCHA das Challenge-Response-Modul, um zu identifizieren, ob der eingehende Datenverkehr von einem menschlichen Benutzer und nicht von einem automatisierten Bot stammt.

Konfigurieren statischer Bot-Signaturen

Diese Erkennungstechnik ermöglicht es Ihnen, die Benutzeragent-Informationen aus den Browserdetails zu identifizieren. Basierend auf Benutzeragent-Informationen wird der Bot als schlechter oder guter Bot identifiziert und dann weisen Sie ihm eine Bot-Aktion zu.

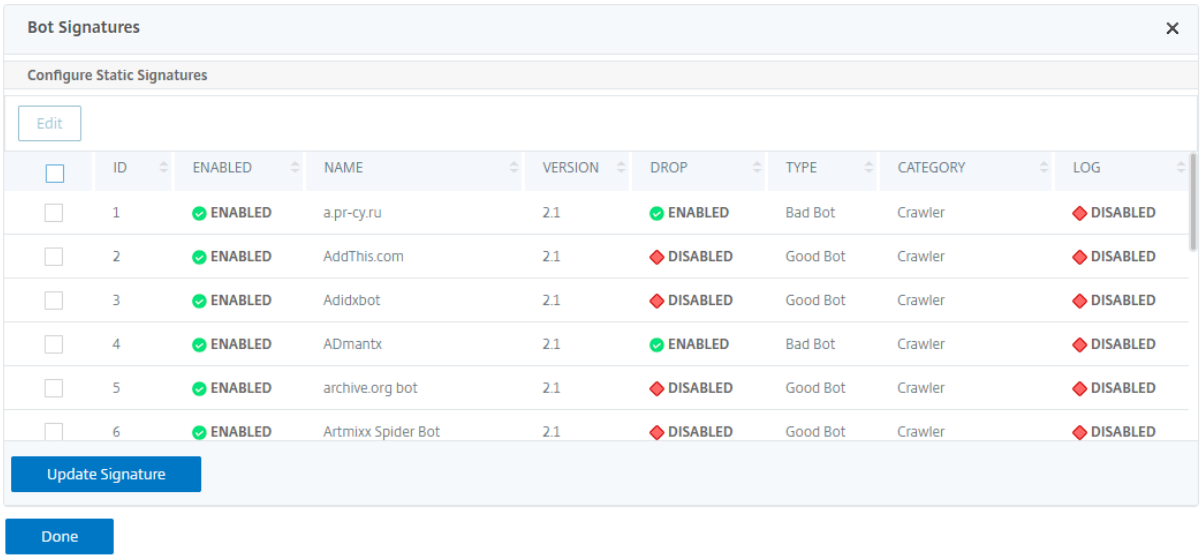
Gehen Sie wie folgt vor, um die statische Signaturtechnik zu konfigurieren:

1. Erweitern Sie im Navigationsbereich **Sicherheit > NetScaler Bot Management**Signaturen.
2. Wählen Sie auf der Seite **NetScaler Bot Management Signatures** eine Signaturdatei aus und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der **NetScaler Bot Management Signaturseite** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **Bot-Signaturen**.
4. Stellen Sie im Abschnitt **Bot-Signaturen** die folgenden Parameter ein:

a) Konfigurieren Sie statische Signaturen. Dieser Abschnitt enthält eine Liste der statischen Signaturdatensätze des Bot. Sie können einen Datensatz auswählen und auf **Bearbeiten** klicken, um ihm eine Bot-Aktion zuzuweisen.

b) Klicken Sie auf **OK**.

5. Klicken Sie auf **Signatur aktualisieren**.
6. Klicken Sie auf **Fertig**.



Abgrenzung der statischen Unterschrift Bot

NetScaler Bot Management schützt Ihre Webanwendung vor Bots. Statische Bot-Signaturen helfen dabei, gute und schlechte Bots basierend auf Anforderungsparametern wie User-Agent in der eingehenden Anforderung zu identifizieren.
Die Liste der Signaturen in der Datei ist riesig und es werden auch neue Regeln hinzugefügt und abgestandene werden regelmäßig entfernt. Als Administrator möchten Sie möglicherweise nach einer bestimmten Signatur oder einer Liste von Signaturen unter einer Kategorie suchen. Um Signaturen einfach zu filtern, bietet die Bot-Signaturseite eine verbesserte Suchfunktion. Mit der Suchfunktion können Sie Signaturregeln finden und ihre Eigenschaft basierend auf einem oder mehreren Signaturparametern wie Aktion, Signatur-ID, Entwickler und Signaturnamen konfigurieren.

Aktion — Wählen Sie eine Bot-Aktion aus, die Sie lieber für eine bestimmte Kategorie von Signaturregeln konfigurieren möchten. Im Folgenden sind die verfügbaren Aktionstypen aufgeführt:

- Ausgewählte aktivieren — Aktiviert alle ausgewählten Signaturregeln.
- Auswahl deaktivieren — Deaktiviert alle ausgewählten Signaturregeln.
- Auswahl löschen — Wählen Sie die Aktion „Löschen“ für alle ausgewählten Signaturregeln aus.
- Ausgewählt umleiten — Wendet die Aktion „Umleiten“ auf alle ausgewählten Signaturregeln an.
- Auswahl zurücksetzen — Wendet die Aktion „Zurücksetzen“ auf alle ausgewählten Signaturregeln an.

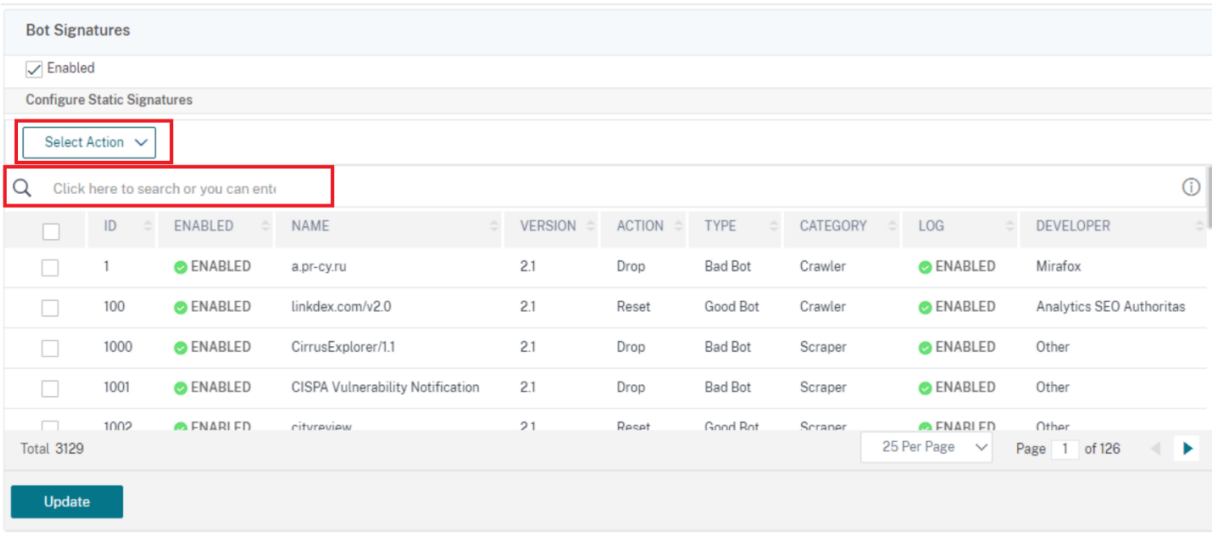
- Ausgewähltes Protokoll — Wendet die Aktion „Protokoll“ auf alle ausgewählten Signaturregeln an.
- Ausgewählte Option entfernen — Deaktiviert die Drop-Aktion für alle ausgewählten Signaturregeln.
- Ausgewählte Weiterleitung entfernen — Deaktiviert die Umleitungsaktion für alle ausgewählten Signaturregeln.
- Ausgewählte Zurücksetzung entfernen — Deaktiviert die Rücksetzaktion für alle ausgewählten Signaturregeln.
- Ausgewähltes Protokoll entfernen — Deaktiviert die Protokollaktion für alle ausgewählten Signaturregeln.

Kategorie — Wählen Sie eine Kategorie aus, um die Signaturregeln entsprechend zu filtern. Im Folgenden finden Sie eine Liste der Kategorien, die zum Sortieren von Signaturregeln verfügbar sind.

- Aktion — Sortiert anhand der Bot-Aktion.
- Kategorie — Sortiert nach Bot-Kategorie.
- Entwickler — Sortiert nach dem Herausgeber des Hostunternehmens.
- Aktiviert — Sortiert basierend auf aktivierten Signaturregeln.
- Id — Sortiert nach der ID der Signaturregel.
- Protokoll — Sortiert anhand von Signaturregeln, für die die Protokollierung aktiviert ist.
- Name — Sortiert nach dem Namen der Signaturregel.
- Typ — Sortiert nach Signaturtyp.
- Version — Sortiert nach der Version der Signaturregel.

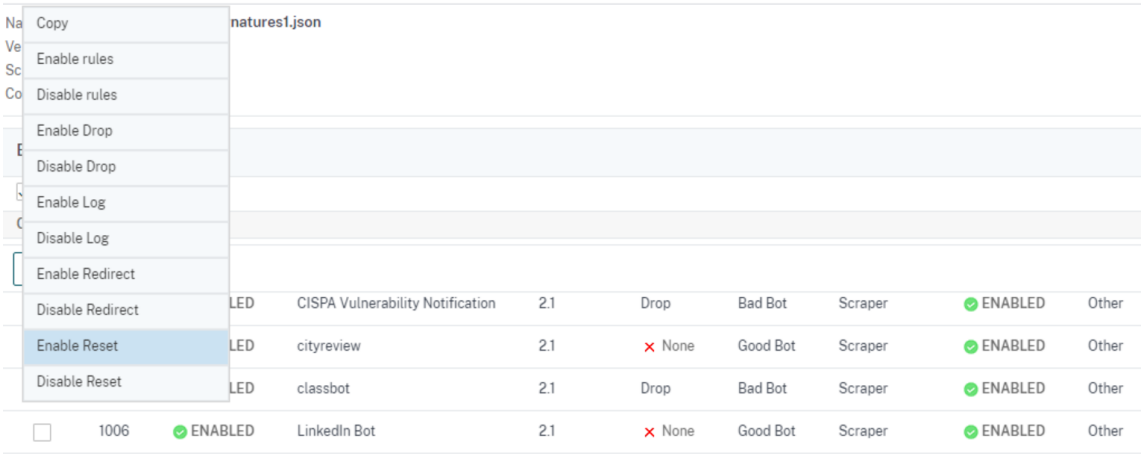
Suche nach Regeln für statische Unterschriften des Bot basierend auf Aktions- und Kategorietypen über die NetScaler-GUI

1. Navigieren Sie zu **Security > NetScaler Bot Management > Signature**.
2. Klicken Sie auf der Detailseite auf **Hinzufügen**.
3. Klicken Sie auf der Seite **NetScaler Bot Management Signatures** im Abschnitt **Statische Signatur** auf Bearbeiten.
4. Wählen **Sie im Abschnitt Statische Signatur konfigurieren** eine Signaturaktion aus der Dropdownliste aus.
5. Verwenden Sie die Suchfunktion, um eine Kategorie auszuwählen und die Regeln entsprechend zu filtern.
6. Klicken Sie auf **Update**.



Bearbeiten Sie die Eigenschaft der statischen Signaturregel des Bot über die NetScaler-GUI

1. Navigieren Sie zu **Security > NetScaler Bot Management > Signature**.
2. Klicken Sie auf der Detailseite auf **Hinzufügen**.
3. Klicken Sie auf der Seite **NetScaler Bot Management Signatures** im Abschnitt **Statische Signatur** auf Bearbeiten.
4. Wählen **Sie im Abschnitt Statische Signatur konfigurieren** eine Aktion aus der Dropdownliste aus.
5. Verwenden Sie die Suchfunktion, um eine Kategorie auszuwählen und die Regeln entsprechend zu filtern.
6. Wählen Sie aus der Liste der statischen Signaturen eine Signatur aus, um ihre Eigenschaft zu ändern.



7. Klicken Sie zum Bestätigen auf **OK**.

Funktionsweise von CAPTCHA in der NetScaler Bot-Verwaltung

In der NetScaler-Bot-Verwaltung wird die CAPTCHA-Validierung als Richtlinienaktion konfiguriert, die ausgeführt wird, nachdem die Bot-Richtlinie ausgewertet wurde. Die CAPTCHA-Aktion ist nur für IP-Reputation und Techniken zur Erkennung von Geräte-Fingerabdrücken verfügbar. Im Folgenden sind die Schritte aufgeführt, um zu verstehen, wie CAPTCHA funktioniert:

1. Wenn während der IP-Reputation oder der Erkennung von Geräte-Fingerabdruck-Bots eine Sicherheitsverletzung festgestellt wird, sendet die ADC-Appliance eine CAPTCHA-Herausforderung.
2. Der Client sendet die CAPTCHA-Antwort.
3. Die Appliance validiert die CAPTCHA-Antwort und wenn das CAPTCHA gültig ist, ist die Anforderung zulässig und wird an den Back-End-Server weitergeleitet.
4. Wenn die CATCHA-Antwort ungültig ist, sendet die Appliance eine neue CAPTCHA-Herausforderung, bis die maximale Anzahl von Versuchen erreicht ist.
5. Wenn die CAPTCHA-Antwort auch nach der maximalen Anzahl von Versuchen ungültig ist, löscht die Appliance die Anforderung oder leitet sie an die konfigurierte Fehler-URL um.
6. Wenn Sie die Protokollaktion konfiguriert haben, speichert die Appliance die Anforderungsdetails in der Datei ns.log.

Konfigurieren Sie die CAPTCHA-Einstellungen über die NetScaler-GUI

Die CAPTCHA-Aktion für das Bot-Management wird nur für IP-Reputation und Techniken zur Erkennung von Geräte-Fingerabdrücken unterstützt. Führen Sie die folgenden Schritte aus, um die **CAPTCHA-Einstellungen** zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > NetScaler Bot Management and Profiles**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der Seite mit dem **NetScaler Bot Management-Profil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **CAPTCHA.**
4. Klicken Sie im Abschnitt **CAPTCHA-Einstellungen** auf **Hinzufügen, um CAPTCHA-Einstellungen für das Profil zu konfigurieren** :
5. Stellen Sie auf der Seite **Configure NetScaler Bot Management CAPTCHA** die folgenden Parameter ein.
   a) URL. Bot-URL, für die die CAPTCHA-Aktion während der IP-Reputation und der Erkennung von Geräte-Fingerabdrücken angewendet wird.
   b) Aktiviert. Stellen Sie diese Option ein, um die CAPTCHA-Unterstützung zu aktivieren.

c) Gnade Zeit. Dauer bis zu dem keine neue CAPTCHA-Herausforderung gesendet wird, nachdem die aktuell gültige CAPTCHA-Antwort empfangen wurde.

d) Warte mal. Dauer, die die ADC-Appliance braucht, um zu warten, bis der Client die CAPTCHA-Antwort sendet.

e) Stummschaltung. Dauer, für die der Client, der eine falsche CAPTCHA-Antwort gesendet hat, warten muss, bis er es als nächstes versuchen darf. Während dieser Stummschaltung lässt die ADC-Appliance keine Anfragen zu. Reichweite: 60-900 Sekunden, Empfohlen: 300 Sekunden

f) Längenbegrenzung anfordern. Länge der Anfrage, für die die CAPTCHA-Herausforderung an den Kunden gesendet wird. Wenn die Länge größer als der Schwellenwert ist, wird die Anforderung gelöscht. Der Standardwert beträgt 10—3000 Byte.

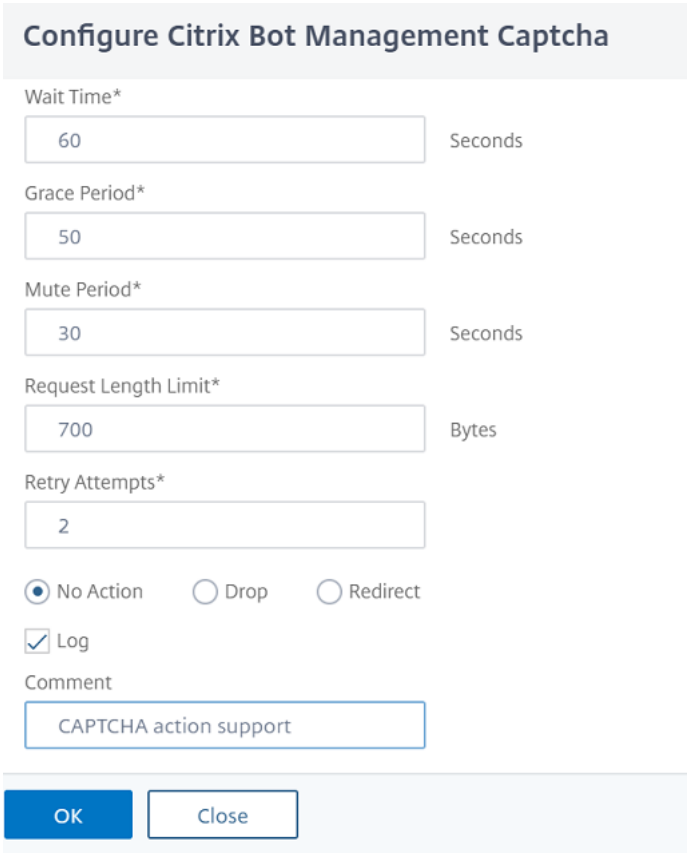
g) Versuche erneut versuchen. Anzahl der Versuche, die der Client erneut versuchen darf, die CAPTCHA-Herausforderung zu lösen. Reichweite: 1—10, Empfohlen: 5.

h) Es müssen keine Aktions-/Drop-/Umleitungsmaßnahmen ergriffen werden, wenn der Client die CAPTCHA-Validierung nicht besteht.

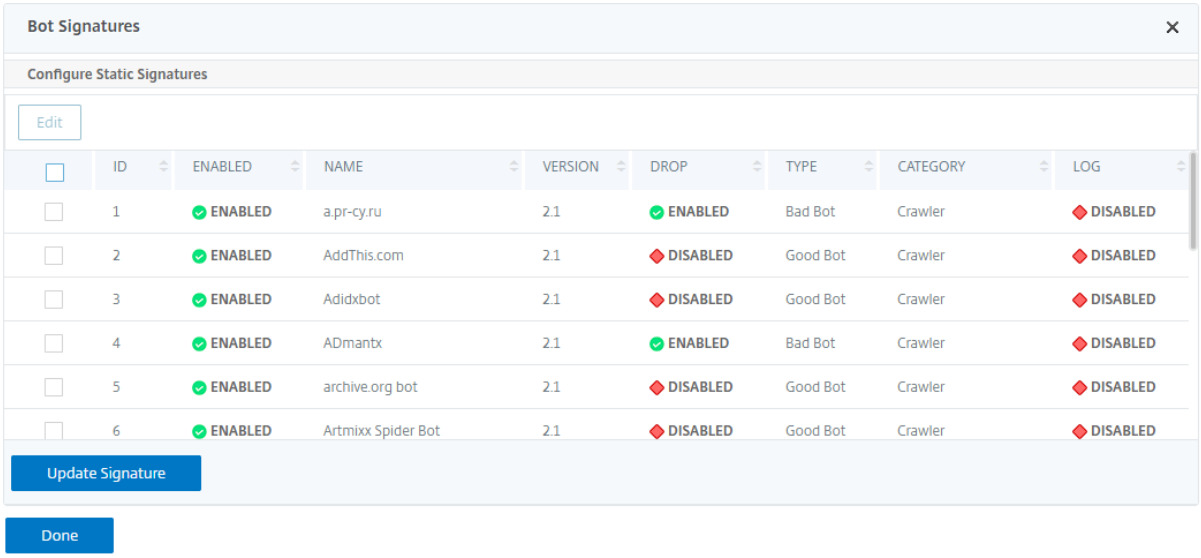
i) Protokoll. Stellen Sie diese Option ein, um Anforderungsinformationen vom Client zu speichern, wenn die Antwort CAPTCHA fehlschlägt. Die Daten werden in einer `ns.log`-Datei gespeichert.

j) Kommentar. Eine kurze Beschreibung der CAPTCHA-Konfiguration.

6. Klicken Sie auf **OK** und **Fertig**.



7. Navigieren Sie zu **Sicherheit > NetScaler Bot Management**Signaturen.
8. Wählen Sie auf der Seite **NetScaler Bot Management Signatures** eine Signaturdatei aus und klicken Sie auf **Bearbeiten**.
9. Gehen Sie auf der **NetScaler Bot Management Signaturseite** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **Bot-Signaturen**.
10. Stellen Sie im Abschnitt **Bot-Signaturen** die folgenden Parameter ein:
11. Konfigurieren Sie **statische Signaturen**. Wählen Sie einen statischen Bot-Signatureintrag aus und klicken Sie auf Bearbeiten, um ihm eine Bot-Aktion zuzuweisen.
12. Klicken Sie auf **OK**.
13. Klicken Sie auf **Signatur aktualisieren**.
14. Klicken Sie auf **Fertig**.



Automatisches Update für Bot-Signaturen

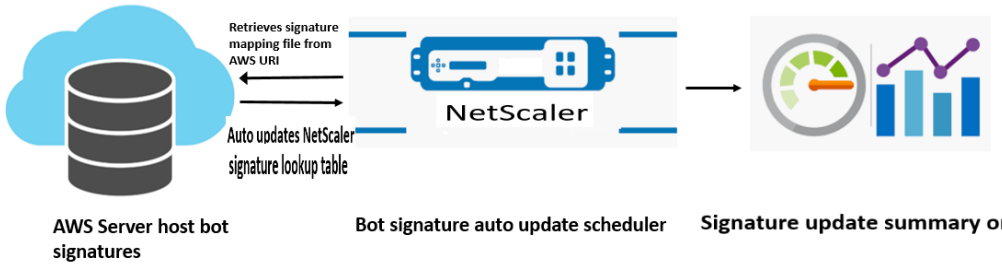
Die statische Bot-Signaturtechnik verwendet eine Signatur-Lookup-Tabelle mit einer Liste guter Bots und schlechter Bots. Die Bots werden basierend auf Benutzer-Agent-Zeichenfolgen und Domain-Namen kategorisiert. Wenn die Benutzer-Agent-Zeichenfolge und der Domänenname im eingehenden Bot-Verkehr mit einem Wert in der Nachschlagetabelle übereinstimmen, wird eine konfigurierte Bot-Aktion angewendet.
Die Bot-Signatur-Updates werden in der AWS-Cloud gehostet, und die Signatur-Lookup-Tabelle kommuniziert mit der AWS-Datenbank für Signaturaktualisierungen. Der Update-Scheduler für automatische Signaturen wird alle 1 Stunde ausgeführt, um die **AWS-Datenbank** zu überprüfen und die Signaturtabelle in der NetScaler-Appliance zu aktualisieren.

Die zu konfigurierende Signatur-Auto-Update-URL lautet: `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

> **Hinweis:**
>
> Sie können auch einen Proxyserver konfigurieren und Signaturen regelmäßig von der AWS-Cloud über den Proxy auf die Appliance aktualisieren. Für die Proxy-Konfiguration müssen Sie die Proxy-IP-Adresse und die Portadresse in den Bot-Einstellungen festlegen.

Wie das automatische Update der Bot-Signatur funktioniert

Das folgende Diagramm zeigt, wie die Bot-Signaturen aus der AWS-Cloud abgerufen, auf NetScaler aktualisiert und auf NetScaler ADM für eine Zusammenfassung der Signaturaktualisierung angezeigt werden.



Der Bot-Signatur-Auto-Update-Scheduler tut Folgendes:

1. Ruft die Zuordnungsdatei von der AWS-URI ab.
2. Überprüft die neuesten Signaturen in der Mapping-Datei mit den vorhandenen Signaturen in der ADC-Appliance.
3. Lädt die neuen Signaturen von AWS herunter und überprüft die Signaturintegrität.
4. Aktualisiert die vorhandenen Bot-Signaturen mit den neuen Signaturen in der Bot-Signaturdatei.
5. Generiert eine SNMP-Warnung und sendet die Signaturaktualisierungszusammenfassung an NetScaler ADM.

Konfigurieren Sie das automatische Update der Bot

Führen Sie die folgenden Schritte aus, um das automatische Update der Bot-Signatur zu konfigurieren:

Automatisches Update der Bot-Signatur aktivieren

Sie müssen die Option für die automatische Aktualisierung in den Bot-Einstellungen der ADC-Appliance aktivieren.
Geben Sie in der Befehlszeile Folgendes ein:

```
set bot settings -signatureAutoUpdate ON
```

Konfigurieren von Proxyservereinstellungen (optional)

Wenn Sie über einen Proxyserver auf die AWS-Signaturdatenbank zugreifen, müssen Sie den Proxyserver und den Port konfigurieren.

```
set bot settings -proxyserver -proxyport
```

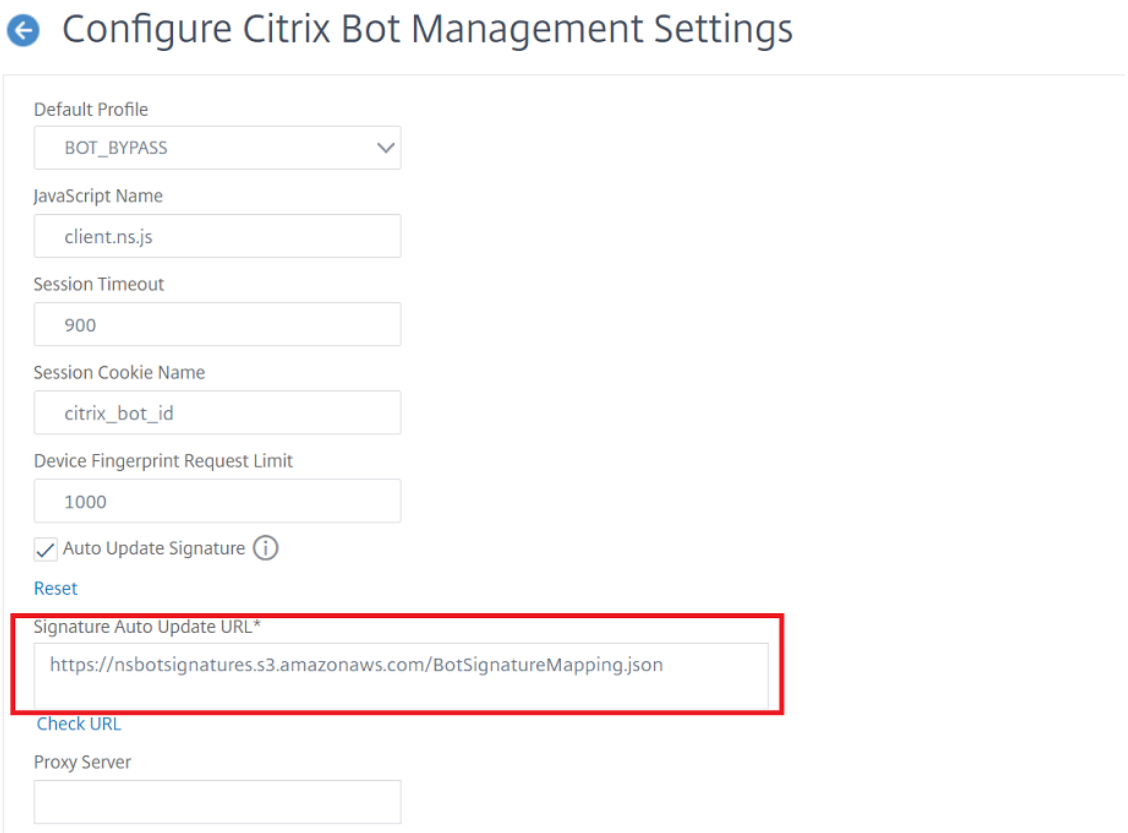
Beispiel:

```
set bot settings -proxy server 1.1.1.1 -proxyport 1356
```


Konfigurieren Sie das automatische Update der Bot-Signatur über die NetScaler-GUI

Führen Sie die folgenden Schritte aus, um das automatische Update für die Bot-Signatur

1. Navigieren Sie zu **Security > NetScaler Bot Management**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **NetScaler Bot Management-Einstellungen ändern**.
3. Aktivieren Sie in den **NetScaler Bot Management-Einstellungen konfigurieren** das Kontrollkästchen **Signatur automatisch aktualisieren**.



4. Klicken Sie auf **OK** und auf **Schließen**.

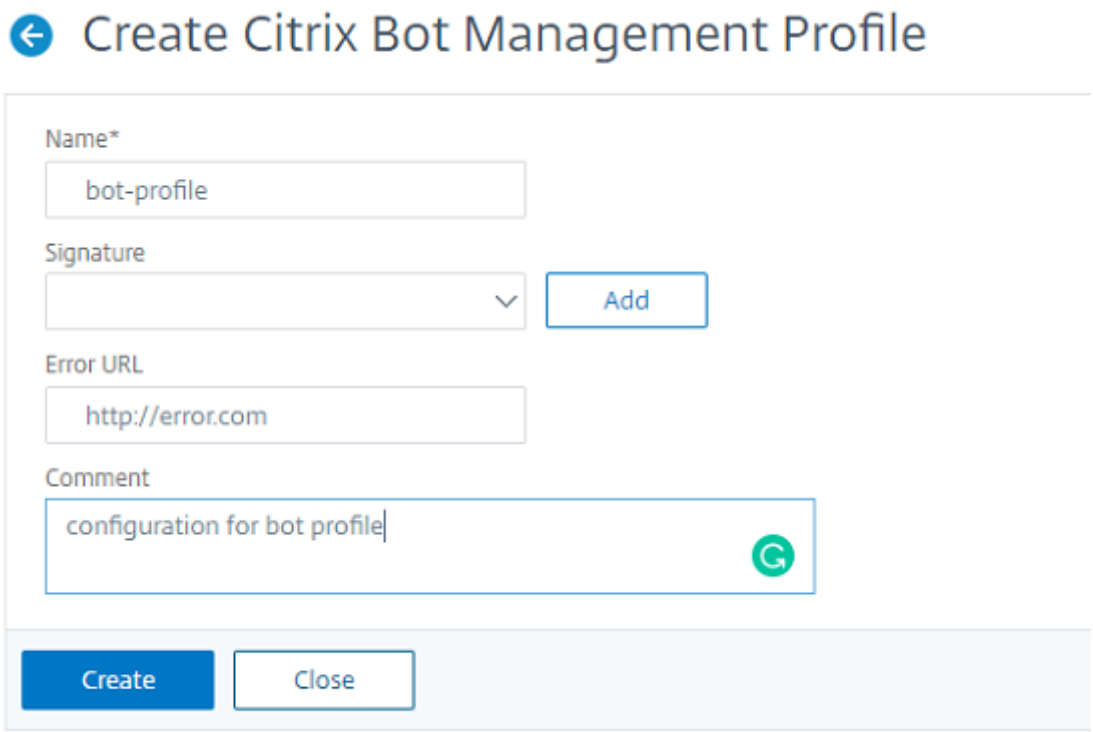
Erstellen Sie Bot-Management-Profil

Ein Bot-Profil ist eine Sammlung von Bot-Management-Einstellungen, die zur Erkennung des Bot-Typs verwendet werden. In einem Profil legen Sie fest, wie die Web App Firewall jeden ihrer Filter (oder Schecks) auf den Bot-Traffic auf Ihre Sites und Antworten von diesen anwendet.

Führen Sie die folgenden Schritte aus, um das Bot-Profil zu konfigurieren:

1. Navigieren Sie zu **Security** > **NetScaler Bot Management** > **Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.

3. Stellen Sie auf der Seite **NetScaler Bot Management Profile erstellen** die folgenden Parameter ein.
   a) Name. Name des Bot-Profils.
   b) Unterschrift. Name der Bot-Signaturdatei.
   c) Fehler-URL. URL für Weiterleitungen.
   d) Kommentar. Kurzbeschreibung des Profils.
4. Klicken Sie auf **Erstellen** und **Schließen**.



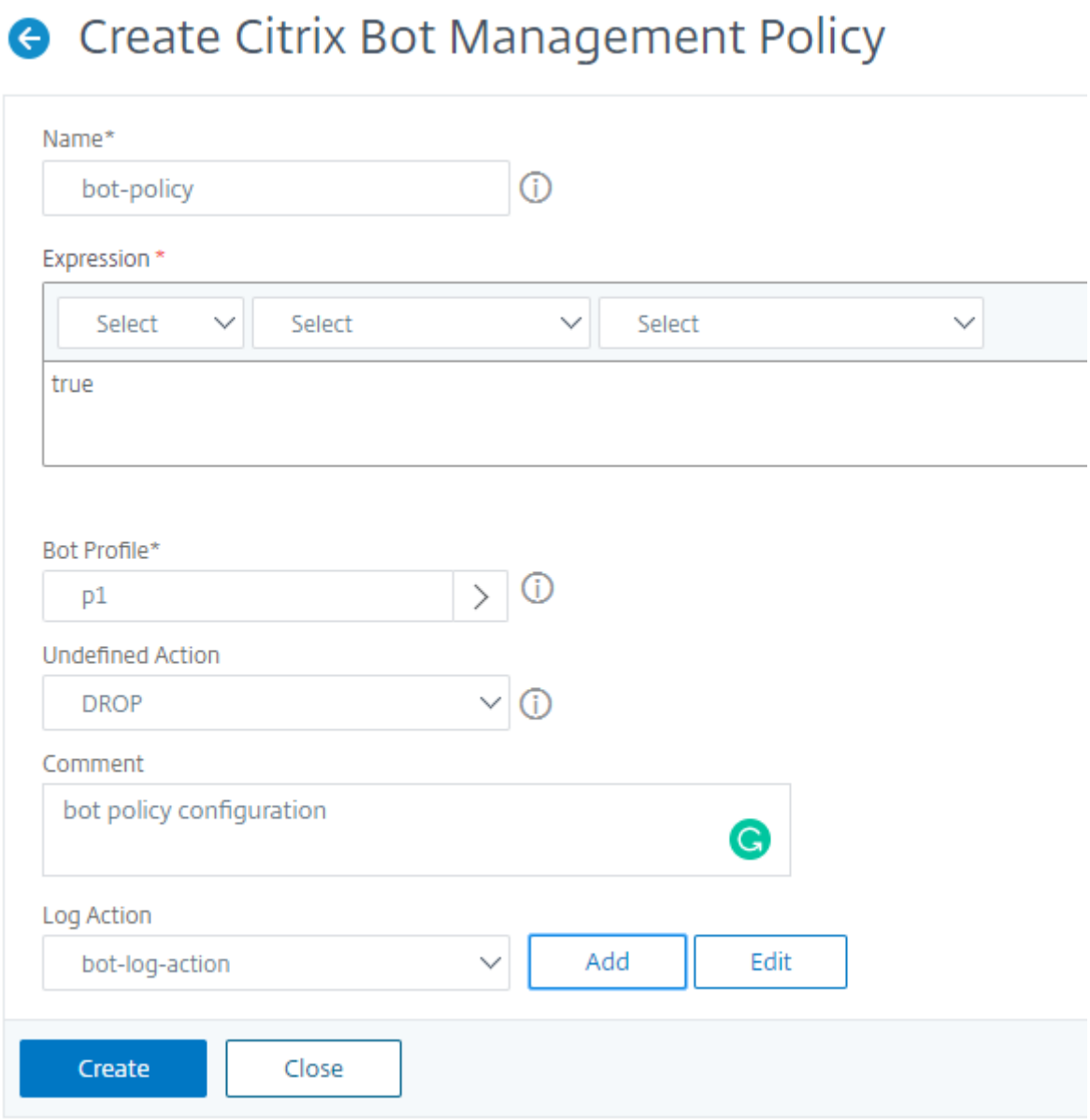
Erstellen Sie Bot-Richtlinie

Die Bot-Richtlinie steuert den Datenverkehr, der zum Bot-Verwaltungssystem fließt, und steuert auch die Bot-Protokolle, die an den Auditlog-Server gesendet werden. Folgen Sie dem Verfahren, um die Bot-Richtlinie zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **NetScaler Bot Management** > **Bot-Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite **Create NetScaler Bot Management Policy** die folgenden Parameter ein.
   a) Name. Name der Bot-Richtlinie.
   b) Ausdruck. Geben Sie den Richtlinienausdruck oder die Regel direkt in den Textbereich ein.
   c) Bot-Profil. Bot-Profil zur Anwendung der Bot-Richtlinie.

d) Undefinierte Aktion. Wählen Sie eine Aktion aus, die Sie lieber zuweisen möchten.
e) Kommentar. Kurze Beschreibung der Richtlinie.
f) Aktion protokollieren. Aktion der Überwachungsprotokollnachricht zum Protokollieren des Bot-Traffics. Weitere Informationen zur Aktion des Überwachungsprotokolls finden Sie unter Thema Audit-Protokollierung.

4. Klicken Sie auf **Erstellen** und **Schließen**.



Bot-Transaktionen pro Sekunde (TPS)

Die Bot-Technik “Transaktionen pro Sekunde” (TPS) erkennt eingehenden Traffic als Bot, wenn die Anzahl der Anfragen pro Sekunde (RPS) und der prozentuale Anstieg des RPS den konfigurierten Schwellenwert überschreiten. Die Erkennungstechnik schützt Ihre Webanwendungen vor automa-

tisierten Bots, die Web-Scraping-Aktivitäten, Brute-Forcing-Login und andere böswillige Angriffe verursachen können.

> **Hinweis:**
>
> Die Bot-Technik erkennt einen eingehenden Traffic nur als Bot, wenn beide Parameter konfiguriert sind und wenn beide Werte über das Schwellenwertlimit hinaus steigen.
> Betrachten wir ein Szenario, in dem die Appliance viele Anfragen von einer bestimmten URL erhält und Sie möchten, dass das NetScaler-Bot-Management erkennt, ob es einen Bot-Angriff gibt. Die TPS-Erkennungstechnik untersucht die Anzahl der Anfragen (konfigurierter Wert), die innerhalb von 1 Sekunde von der URL kommen, und den prozentualen Anstieg (konfigurierter Wert) der Anzahl der Anfragen, die innerhalb von 30 Minuten empfangen wurden. Wenn die Werte das Schwellenwertlimit überschreiten, wird der Verkehr als Bot betrachtet und die Appliance führt die konfigurierte Aktion aus.

Konfigurieren von Bot-Transaktionen pro Sekunde (TPS) -Technik

Um TPS zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie Bot TPS
2. Binden Sie TPS-Einstellungen an das Bot-Verwaltungsprofil

Binden Sie TPS-Einstellungen an das Bot-Verwaltungsprofil

Sobald Sie die Bot-TPS-Funktion aktiviert haben, müssen Sie die TPS-Einstellungen an das Bot-Verwaltungsprofil binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind bot profile <name>… (-tps [-type ( SourceIP | GeoLocation | RequestURL
 | Host )] [-threshold <positive_integer>] [-percentage <positive_integer
>] [-action ( none | log | drop | redirect | reset | mitigation )] [-
logMessage <string>])
```

Beispiel:

```
bind bot profile profile1 -tps -type RequestURL -threshold 1 -percentage
100000 -action drop -logMessage log
```

Aktivieren Sie die Bot-Transaktion pro Sekunde (TPS)

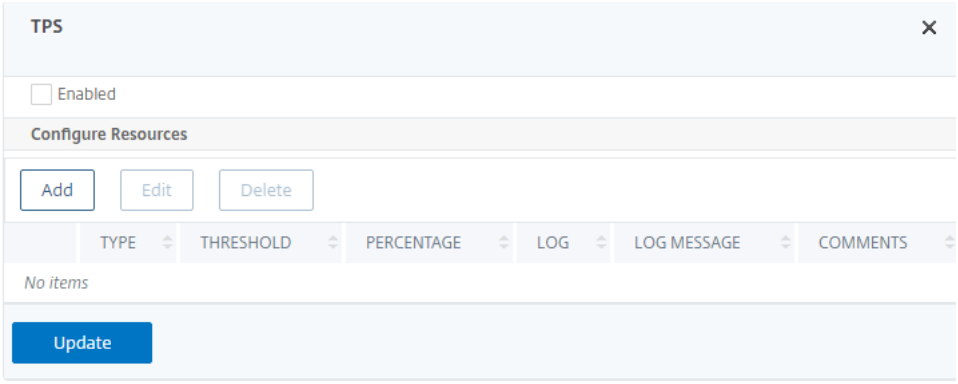
Bevor Sie beginnen können, müssen Sie sicherstellen, dass die Bot TPS-Funktion auf der Appliance aktiviert ist. Geben Sie in der Befehlszeile Folgendes ein:

```
set bot profile profile1 -enableTPS ON
```


Konfigurieren Sie Bot-Transaktionen pro Sekunde (TPS) über die NetScaler-GUI

Führen Sie die folgenden Schritte aus, um Bot-Transaktionen pro Sekunde zu konfigurieren:

1. Navigieren Sie zu **Sicherheit > NetScaler Bot Management > Profile**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **NetScaler Bot Management-Profil erstellen** im Abschnitt **Signature-instellungen** auf **TPS**.
4. Aktivieren Sie im Abschnitt **TPS** die Funktion und klicken Sie auf **Hinzufügen**.



5. Legen Sie auf der Seite **TPS-Bindung des NetScaler bot-Verwaltungsprofils konfigurieren** die folgenden Parameter fest.

   a) Typ — Die von der Erkennungstechnik zugelassenen Eingabetypen. Mögliche Werte: SOURCE IP, GEOLOCATION, HOST, URL.

   SOURCE_IP — TPS basierend auf der IP-Adresse des Clients.

   GEOLOCATION — TPS basierend auf dem geografischen Standort des Kunden.

   HOST - TPS basierend auf Clientanforderungen, die an eine bestimmte Back-End-Server-IP-Adresse weitergeleitet werden.

   URL — TPS basierend auf Clientanforderungen, die von einer bestimmten URL stammen.

   b) Fester Schwellenwert — Maximal zulässige Anzahl von Anfragen von einem TPS-Eingabetyp innerhalb eines Zeitintervalls von 1 Sekunde.

   c) Prozentualer Schwellenwert — Maximaler prozentualer Anstieg der Anfragen von einem TPS-Eingabetyp innerhalb eines 30-Minuten-Zeitintervalls.

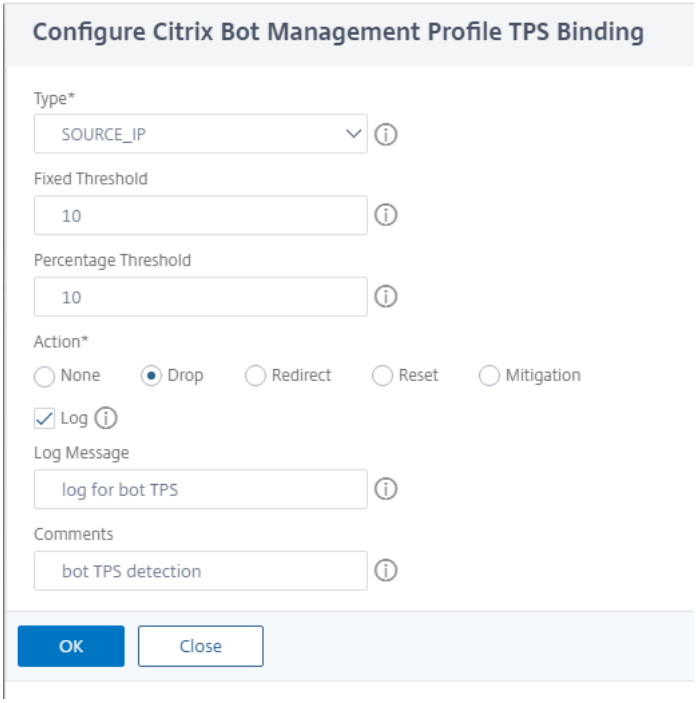
   d) Aktion — Aktion, die für einen Bot ergriffen werden muss, der durch die TPS-Bindung erkannt wurde.

   e) Protokoll — Aktiviert oder deaktiviert die Protokollierung für die TPS-Bindung.

f) Nachricht protokollieren. Meldung zum Log für Bot, die durch TPS-Bindung erkannt wurde. Maximale Länge: 255

g) Kommentare — Eine kurze Beschreibung der TPS-Konfiguration. Maximale Länge: 255

6. Klicken Sie auf **OK** und dann auf **Schließen**.



Bot-Erkennung basierend auf Maus- und Tastaturdynamik

Um Bots zu erkennen und Anomalien des Web-Scrapings zu mildern, verwendet das NetScaler Bot Management eine erweiterte Bot-Erkennungstechnik, die auf dem Verhalten von Maus und Tastatur basiert. Im Gegensatz zu herkömmlichen Bot-Techniken, die eine direkte menschliche Interaktion erfordern (z. B. die CAPTCHA-Validierung), überwacht die erweiterte Technik passiv die Maus und die Tastaturdynamik. Die NetScaler-Appliance sammelt dann die Benutzerdaten in Echtzeit und analysiert das Verhalten zwischen einem Menschen und einem Bot.

Die passive Bot-Erkennung mit Maus- und Tastaturdynamik hat gegenüber bestehenden Bot-Erkennungsmechanismen folgende Vorteile:

- Bietet eine kontinuierliche Überwachung während der gesamten Benutzersitzung und eliminiert einen einzelnen Checkpoint.
- Erfordert keine menschliche Interaktion und ist für Benutzer transparent.

So funktioniert die Bot-Erkennung mit Maus- und Tastaturdynamik

Die Bot-Erkennungstechnik mit Tastatur- und Mausdynamik besteht aus zwei Komponenten, einem Webseitenlogger und einem Bot-Detektor. Der Webseitenlogger ist ein JavaScript, das Tastatur- und Mausbewegungen aufzeichnet, wenn ein Benutzer eine Aufgabe auf der Webseite ausführt (z. B. ein Registrierungsformular ausfüllt). Der Logger sendet die Daten dann stapelweise an die NetScaler-Appliance. Die Appliance speichert die Daten dann als KM-Datensatz und sendet sie an den Bot-Detektor auf dem NetScaler ADM-Server, der analysiert, ob der Benutzer ein Mensch oder Bot ist.

Die folgenden Schritte erklären, wie die Komponenten miteinander interagieren:

1. Der NetScaler-Administrator konfiguriert den Richtlinienausdruck über das ADM StyleBook, CLI oder NITRO oder eine andere Methode.
2. Die URL wird im Bot-Profil festgelegt, wenn der Administrator die Funktion auf der Appliance aktiviert.
3. Wenn ein Client eine Anforderung sendet, verfolgt die NetScaler-Appliance die Sitzung und alle Anforderungen in der Sitzung.
4. Die Appliance fügt ein JavaScript (Webseitenlogger) in die Antwort ein, wenn die Anforderung mit dem konfigurierten Ausdruck im Bot-Profil übereinstimmt.
5. Das JavaScript sammelt dann die gesamte Tastatur- und Mausaktivität und sendet die KM-Daten in einer POST-URL (transient).
6. Die NetScaler-Appliance speichert die Daten und sendet sie am Ende der Sitzung an den NetScaler ADM-Server. Sobald die Appliance die vollständigen Daten einer POST-Anforderung erhalten hat, werden die Daten an den ADM-Server gesendet.
7. Der NetScaler ADM-Dienst analysiert die Daten und basierend auf der Analyse ist das Ergebnis auf der GUI des NetScaler ADM Service ADM-Dienstes verfügbar.

Der JavaScript-Logger zeichnet die folgenden Maus- und Tastaturbewegungen auf:

- Tastaturereignisse — alle Ereignisse
- Mausereignisse - Maus bewegen, Maus hoch, Maus runter
- Ereignisse in der Zwischenablage - einfügen
- Benutzerdefinierte Ereignisse — automatisches Ausfüllen, Abbrechen
- Zeitstempel jedes Ereignisses

Konfigurieren der Bot-Erkennung mit Maus- und Tastatur

Die NetScaler Bot-Verwaltungskonfiguration umfasst das Aktivieren oder Deaktivieren der Tastatur- und mausbasierten Erkennungsfunktion und konfiguriert die JavaScript-URL im Bot-Profil.
Führen Sie die folgenden Schritte aus, um die Bot-Erkennung mit Maus- und Tastaturdynamik zu konfigurieren

1. Tastatur- und mausbasierte Erkennung aktivieren

2. Konfigurieren Sie den Ausdruck, um zu entscheiden, wann das JavaScript in die HTTP-Antwort injiziert werden kann

Tastaturmausbasierte Bot-Erkennung aktivieren

Bevor Sie mit der Konfiguration beginnen, stellen Sie sicher, dass Sie die Tastatur- und mausbasierte Bot-Erkennungsfunktion auf der Appliance aktiviert haben.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add bot profile <name> -KMDetection ( ON | OFF )
2 <!--NeedCopy-->
```

Beispiel:

```
add bot profile profile1 -KMDetection ON
```

Bot-Ausdruck für das Einfügen von JavaScript konfigurieren

Konfigurieren Sie Bot-Ausdruck, um den Datenverkehr auszuwerten und JavaScript einzufügen. Das JavaScript wird nur eingefügt, wenn der Ausdruck als wahr ausgewertet wird.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 bind bot profile <name> -KMDetectionExpr -name <string> -expression <
     expression> -enabled ( ON | OFF ) - comment <string>
2 <!--NeedCopy-->
```

Beispiel:

```
bind bot profile profile1 -KMDetectionExpr -name test -expression http.req.
url.startswith("/testsite")-enabled ON
```

Konfigurieren Sie den in der HTTP-Antwort eingefügten JavaScript-Dateinamen für die tastaturmausbasierte

Um die Benutzeraktionsdetails zu erfassen, sendet die Appliance einen JavaScript-Dateinamen in der HTTP-Antwort. Die JavaScript-Datei sammelt alle Daten in einem KM-Datensatz und sendet sie an die Appliance.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set bot profile profile1 - KMJavaScriptName <string>
2 <!--NeedCopy-->
```


Beispiel:

```
set bot profile profile1 -KMJavaScriptName script1
```

Verhaltensgröße der Biometrie konfigurieren

Sie können die maximale Größe von Maus- und Tastaturverhaltensdaten konfigurieren, die als KM-Datensatz an die Appliance gesendet und vom ADM-Server verarbeitet werden können.

Geben Sie in der Befehlszeile Folgendes ein:

```
set bot profile profile1 -KMEventsPostBodyLimit <positive_integer>
<!--NeedCopy-->
```

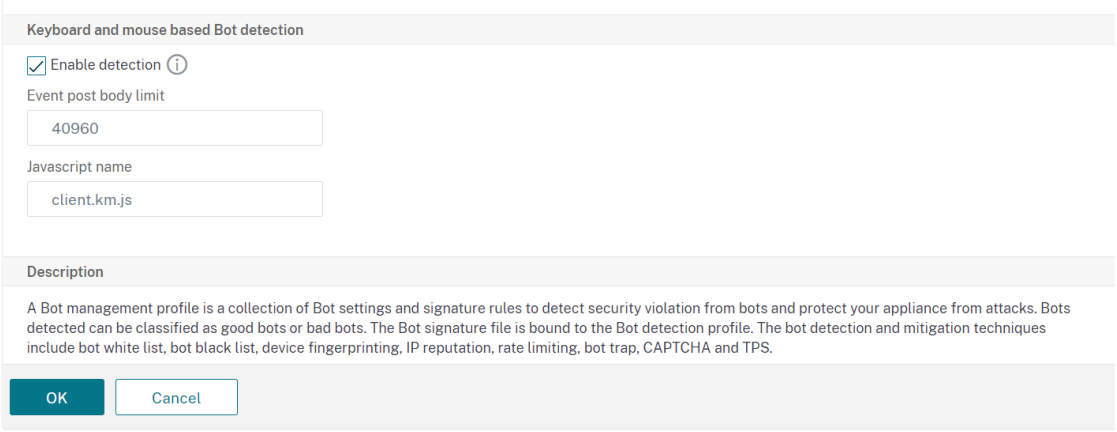
Beispiel:

```
set bot profile profile1 - KMEventsPostBodyLimit 25
```

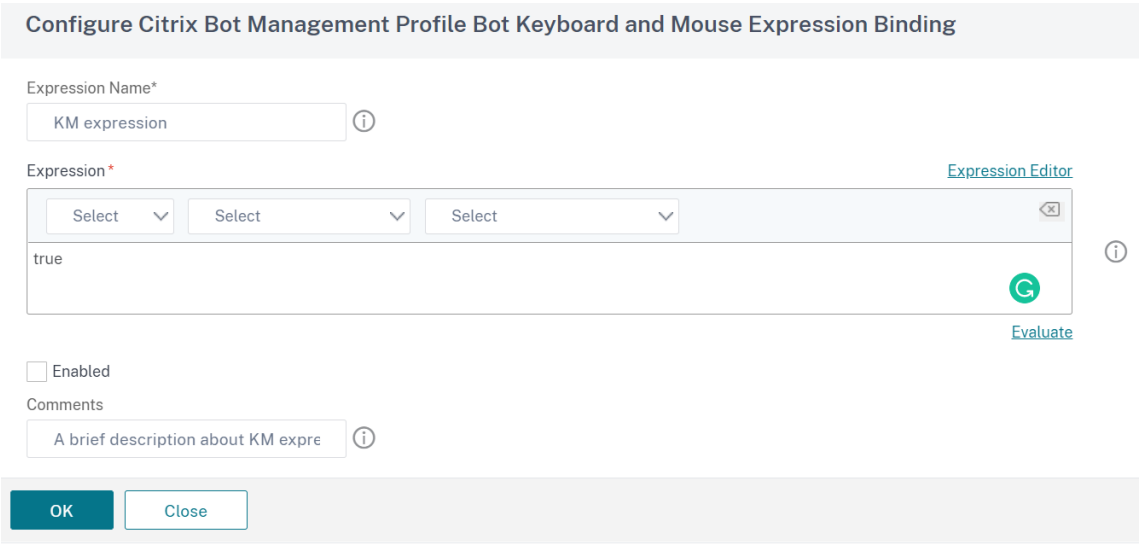
Nachdem Sie die NetScaler-Appliance so konfiguriert haben, dass JavaScript konfiguriert und Biometrie für das Verhalten von Tastatur und Maus erfasst werden, sendet die Appliance die Daten an den NetScaler ADM-Server. Weitere Informationen darüber, wie der NetScaler ADM-Server Bots aus der Verhaltensbiometrie erkennt, finden Sie unter Bot-Verstöße.

Konfigurieren von Tastatur- und Maus-Bot-Ausdruckseinstellungen über die GUI

1. Navigieren Sie zu **Sicherheit > NetScaler Bot Management and Profiles**.
2. Wählen Sie auf der Seite **NetScaler Bot Management Profiles** ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Stellen Sie im Abschnitt **Tastatur- und mausbasierte Bot-Erkennung** die folgenden Parameter ein:
   a) Aktivieren Sie die Erkennung. Wählen Sie das Kontrollkästchen aus, um das Verhalten der Bot-basierten Tastatur- und Mausdynamik zu erkennen.
   b) Grenzwert für das Ereignis nach dem Hauptteil Größe der Tastatur- und Mausdynamikdaten, die vom Browser gesendet werden, um von der NetScaler-Appliance verarbeitet zu werden.
4. Klicken Sie auf **OK**.



5. Gehen Sie auf der Seite **NetScaler bot Management Profile** zum Abschnitt **Profileinstellungen** und klicken Sie auf **Tastatur- und mausbasierte Bot-Ausdruckseinstellungen**.
6. Klicken Sie im Abschnitt **Einstellungen für Tastatur und Maus auf Bot Expression** Settings auf **Hinzufügen**.
7. Legen Sie auf der Seite **Configure NetScaler bot Management Profile Bot Keyboard and Mouse Expression Binding** die folgenden Parameter fest:
   a) Name des Ausdrucks. Name des Bot-Richtlinienausdrucks zur Erkennung von Tastatur- und Mausdynamik.
   b) Ausdruck. Ausdruck der Bot-Richtlinie.
   c) Aktiviert. Wählen Sie das Kontrollkästchen, um die Tastatur- und Bot-Tastatur- und Mausausdrucksbindung zu aktivieren.
   d) Kommentare. Eine kurze Beschreibung des Bot-Richtlinienausdrucks und seiner Bindung an das Bot-Profil.
   e) Klicken Sie auf **OK** und auf **Schließen**.
8. Klicken Sie im Abschnitt **Einstellungen für Tastatur- und mausbasierte Bot-Ausdrücke** auf **Aktualisieren**.



Umkehrende Protokollierung für Bot-Verkehr

Wenn eine eingehende Anfrage als Bot identifiziert wird, protokolliert die NetScaler-Appliance weitere HTTP-Header-Details zur Überwachung und Fehlerbehebung. Die ausführliche Protokollierungsfunktion des Bots ähnelt der ausführlichen Protokollierung im Web App Firewall-Modul.

Betrachten Sie einen eingehenden Verkehr von einem Kunden. Wenn der Client als Bot identifiziert wird, verwendet die NetScaler-Appliance die ausführliche Protokollierungsfunktion, um vollständige HTTP-Header-Informationen wie Domänenadresse, URL, User-Agent-Header und Cookie-Header zu protokollieren. Die Protokolldetails werden dann an den ADM-Server gesendet, um den Zweck zu überwachen und zu beheben. Die ausführliche Protokollnachricht wird nicht in der Datei “ns.log” gespeichert.

Konfigurieren Sie die ausführliche Bot-Protokollierung über die CLI

Um detaillierte HTTP-Header-Informationen als Protokolle zu erfassen, können Sie den ausführlichen Protokollierungsparameter im Bot-Profil konfigurieren. Geben Sie in der Befehlszeile Folgendes ein:

```
1 set bot profile <name> [-verboseLogLevel ( NONE | HTTP_FULL_HEADER ) ]
2 <!--NeedCopy-->
```

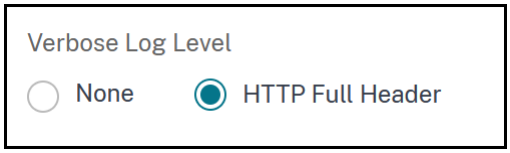
Beispiel:

```
set bot profile p1 -verboseLogLevel HTTP_FULL_HEADER
```

Konfigurieren Sie die ausführliche Bot-Protokollierung über die NetScaler-GUI

Folgen Sie dem Verfahren, um die ausführliche Protokollebene im Bot-Profil zu konfigurieren.

1. Navigieren Sie im Navigationsbereich zu **Security > NetScaler Bot Management**.
2. Klicken Sie auf der Seite **NetScaler Bot Management Profiles** auf **Hinzufügen**.
3. Wählen Sie auf der Seite **NetScaler Bot Management-Profil erstellen** die Option Ausführliches Log-Level als **HTTP Full Header** aus.
4. Klicken Sie auf **OK** und **Fertig**.



Eine Aktion für gefälschte Bot-Anfragen konfigurieren

Ein Angreifer könnte versuchen, sich als guter Bot auszugeben und Anfragen an Ihren Anwendungsserver zu senden. Solche Bots werden anhand der Bot-Signatur als Spoofed-Bots identifiziert. Konfigurieren Sie die folgenden Aktionen gegen gefälschte Bots, um Ihren Anwendungsserver zu schützen:

- DROP
- NONE
- REDIRECT
- RESET

Konfigurieren Sie eine Aktion für gefälschte Bot-Anfragen über die CLI

Führen Sie den folgenden Befehl aus, um eine Aktion für gefälschte Bot-Anfragen zu konfigurieren:

```
set bot profile <bot-profile-name> -spoofedReqAction <action> LOG
<!--NeedCopy-->
```

Beispiel:

```
set bot profile bot_profile -spoofedReqAction DROP LOG
<!--NeedCopy-->
```

In diesem Beispiel werden die Anfragen von gefälschten Bots verworfen und in einer NetScaler-Appliance protokolliert.

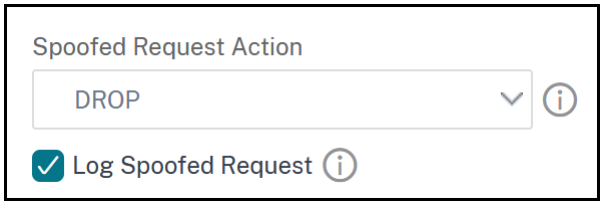
> **Tipp**
>
> Um Ereignisse von gefälschten Bots zu protokollieren, geben Sie LOG im Befehl an.

Konfigurieren Sie eine Aktion für gefälschte Bot-Anfragen über die GUI

Folgen Sie den Schritten, um eine Aktion für die gefälschten Bot-Anfragen zu konfigurieren:

1. Navigieren Sie zu **Security > NetScaler Bot Management**.
2. Klicken Sie auf der Seite **NetScaler Bot Management Profiles** auf **Hinzufügen**.
3. Wählen Sie eine Aktion aus der Liste der **gefälschten Anforderungsaktionen** aus.
4. Wählen Sie **Spoofed-Anfrage protokollieren**aus.

   Diese Aktion protokolliert die Ereignisse von gefälschten Bots.

5. Klicken Sie auf **Erstellen**.

Vom NetScaler bot Management gelöschte Header anfordern

Viele der Anforderungsheader im Zusammenhang mit dem Caching werden gelöscht, um jede Anforderung im Kontext einer Sitzung anzuzeigen. Ebenso löscht das Bot-Management diesen Header, wenn die Anfrage einen Codierungs-Header enthält, damit der Webserver komprimierte Antworten senden kann, sodass der Inhalt der unkomprimierten Serverantwort vom Bot-Management überprüft wird, um das JavaScript einzufügen.

Die Bot-Verwaltung löscht die folgenden Request-Header:

Bereich — Wird zur Wiederherstellung nach einer fehlgeschlagenen oder teilweisen Dateiübertragung verwendet.

If-Range — Ermöglicht einem Client, ein Teilobjekt abzurufen, wenn ein Teil dieses Objekts bereits in seinem Cache enthalten ist (bedingtes GET).

If-Modified-Since — Wenn das angeforderte Objekt seit der in diesem Feld angegebenen Zeit nicht geändert wurde, wird keine Entität vom Server zurückgegeben. Sie erhalten einen nicht modifizierten HTTP-304-Fehler.

If-None-Match — Ermöglicht effiziente Aktualisierungen zwischengespeicherter Informationen mit minimalem Aufwand.

Accept-Encoding — Welche Kodierungsmethoden sind für ein bestimmtes Objekt zulässig, z. B. gzip.

Bot-Verwaltung

May 11, 2023

Im Folgenden finden Sie einige der Problembehebungsszenarien, die in NetScaler Bot Management behandelt werden.

1. Wie geht man mit falsch positiven Fällen um?

   Sie können die Bot-Funktion „Liste zulassen“ verwenden, um falsch positive Fälle zu verwalten, und diese Transaktionen können umgangen werden.

2. Wie finde ich weitere Informationen über schlechten Bot-Traffic?

   Sie können die Audit-Logging-Funktion verwenden, um Details über den Traffic zu erhalten, der als schlechte Bots eingestuft wurde.

3. Warum sollten Sie den Standardsignaturnamen ändern?

   Sie können den Standardsignaturnamen ändern, wenn Konflikte an den von der NetScaler-Appliance bereitgestellten Endpunktressourcen festgestellt werden.

Bot-Verwaltung

May 11, 2023

1. Was ist NetScaler Bot-Management?

   NetScaler Bot Management erkennt und unterscheidet Traffic von guten Bots, schlechten Bots und menschlichen Clients. Die Bot-Management-Funktionalität schützt Ihre Webanwendungen vor schlechten Bots, indem eine konfigurierte Aktion auf eingehende Anfragen angewendet wird.

2. Warum muss NetScaler Bots für Ihre Webanwendung verwalten?

   Bösartige Bots machen 30% Ihres Internetverkehrs aus. Schädliche Bots wirken sich auf verschiedene Weise auf Webanwendungen aus, z. B. durch das Auslösen eines DoS-Angriffs, das Spammen von E-Mail-Adressen, das Verlangsamen der Anwendung mithilfe von Downloader-Programmen, das Herunterladen des Inhalts von Websites usw. Darüber hinaus können Bots einige der bekannten Erkennungsmechanismen leicht umgehen, die zu Verlust von Daten, Einnahmen und Reputation für Ihr Unternehmen führen.

3. Welche Techniken werden verwendet, um einen eingehenden Bot zu erkennen?

   Die Appliance verwendet Erkennungstechniken wie IP-Reputation, Ratenbegrenzung, Geräte-Fingerabdruck, TPS und Techniken zur Erkennung von Bot-Fallen. Darüber hinaus können Sie

eine angepasste Sperrliste auf der NetScaler GUI konfigurieren, um organisationsspezifische Bad Bots zu kategorisieren.

4. Was ist eine Bot-Signaturdatei und ihr Zweck?

   Die Bot-Signaturdatei enthält den Fußabdruck bekannter guter und schlechter Bots. Die Signaturdatei wird regelmäßig aktualisiert, um die neuesten Bot-Signaturen für einen besseren Bot-Schutz aufzunehmen.

5. Welche Art von NetScaler -Lizenz muss ich kaufen?

   Die Bot-Verwaltung ist mit der ADC Premium-Lizenz verfügbar.

6. Wo finde ich Bot-Protokolle zur Fehlerbehebung?

   NetScaler Überwachungsprotokolle bieten erkannte Bot-Details. Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

7. Gibt es eine automatische Update-Funktion für die Bot-Signaturdateien?

   Ja, die NetScaler Bot-Verwaltung unterstützt automatische Update-Funktionen.

8. Gibt es eine Voraussetzung für die Verwendung der Bot-IP-Reputationstechnik?

   Aktivieren Sie die IP-Reputationsfunktion, bevor Sie die IP-Reputation im Bot-Profil aktivieren und konfigurieren.

Bot Signatur Auto Update

May 11, 2023

Mit der automatischen Aktualisierungsfunktion für Bot-Signaturen erhalten Sie die neuesten Signaturen, die einen besseren Schutz und ein besseres Verkehrsmanagement vor guten und schlechten Bots bieten.

Die Signaturen werden stündlich automatisch aktualisiert, sodass nicht ständig nach der Verfügbarkeit des neuesten Updates gesucht werden muss. Wenn Sie die automatische Signaturaktualisierung aktiviert haben, stellt die NetScaler Appliance eine Verbindung zu dem Server her, auf dem die Signaturen gehostet werden, um zu überprüfen, ob eine neuere Version verfügbar ist.

Die neuesten in der Amazon-Cloud gehosteten Bot-Signaturen sind als Standard-Signatur-URL konfiguriert, um nach dem neuesten Update zu suchen. Damit die automatische Aktualisierungsfunktion funktioniert, müssen Sie auch den DNS-Server für den Zugriff auf die externe Site konfigurieren.

Signaturen aktualisieren

Alle benutzerdefinierten Signaturobjekte, die mit dem Standard-Signaturobjekt des Bot erstellt wurden, haben eine Version größer als Null. Wenn Sie die automatische Signaturaktualisierung aktivieren, werden alle Signaturen automatisch aktualisiert. Sie können die Standardaktion für Bot-Signaturen aktualisieren, indem Sie entweder eine Signatur oder eine Gruppe von Signaturen mithilfe der Suchfunktion in der NetScaler Bot-Management-GUI auswählen.

URL zur Aktualisierung der Bot-Signatur `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

Konfigurieren des automatischen Updates der Signatur

Um die automatische Signaturaktualisierung zu aktivieren, müssen Sie den folgenden Befehl ausführen:

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set bot settings SignatureAutoUpdate ON
2 <!--NeedCopy-->
```

Bot-Signaturwarnung

May 11, 2023

NetScaler Bot Management kündigt Signaturupdates an, die Sie herunterladen und auf Ihre Appliance anwenden können. Wenn Sie einen Bot-Angriff entdecken, erhalten Sie eine E-Mail-Benachrichtigung über das neue Signatur-Update. Sie können die Signatur herunterladen und auf Ihre Appliance anwenden.

Um Updates zu neuen Bot-Signaturen zu erhalten, müssen Sie die Funktion zur automatischen Signaturaktualisierung konfigurieren. Weitere Informationen finden Sie im Thema Automatische Aktualisierung der Bot-Signatur .

Bot-Signatur-Update für November 2020

May 11, 2023

Für die in der Woche 2020-11-11 identifizierten Bots werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 5 gilt für NetScaler 13.0-Plattform.

Neue Bot-Signaturen

Es folgt eine Liste der Regeln, der Kategorie und ihres Typs für Bot-Signaturen.

Kategorie	Bot-Typ	Anzahl der Unterschriften
Scraper	Good Bot	3
Marketing	Good Bot	23
Feed Fetcher	Good Bot	2
Tool	Bad Bot	3
Suchmaschine	Good Bot	34
Crawler	Good Bot	6
Nicht kategorisiert	Bad Bot	6
Viren-Scanner	Good Bot	1
Screenshot Creator	Good Bot	7
Scraper	Bad Bot	1
Tool	Good Bot	7

Bot-Signatur-Update für Januar 2021

May 11, 2023

Einige vorhandene Bot-Signaturen werden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Die Signaturversion 6 ist für NetScaler-Plattformen mit 13.0 61.x-Builds oder höher anwendbar.

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
143	Crawler	Good Bot
561	Scraper	Good Bot
857	Sitemonitor	Good Bot
892	Sitemonitor	Bad Bot
894	Sitemonitor	Bad Bot
980	Scraper	Bad Bot
1025	Sitemonitor	Bad Bot
1029	Feed Fetcher	Bad Bot
1030	Screenshot Creator	Bad Bot
1034	Tool	Bad Bot
1039	Marketing	Bad Bot
1042	Sitemonitor	Bad Bot
1047	Sitemonitor	Bad Bot
1053	Sitemonitor	Bad Bot
1072	Suchmaschine	Bad Bot
1073	Feed Fetcher	Bad Bot
1074	Nicht kategorisiert	Bad Bot
1078	Screenshot Creator	Bad Bot
1109	Marketing	Bad Bot
1132	Feed Fetcher	Bad Bot
1138	Marketing	Bad Bot
1150	Suchmaschine	Bad Bot
1164	Suchmaschine	Bad Bot
1167	Marketing	Bad Bot
1173	Tool	Bad Bot
1174	Marketing	Bad Bot
1176	Suchmaschine	Bad Bot
1178	Geschwindigkeitstester	Bad Bot
1185	Screenshot Creator	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1209	Nicht kategorisiert	Bad Bot
1244	Sitemonitor	Bad Bot
1251	Suchmaschine	Bad Bot
1254	Sitemonitor	Bad Bot
1256	Nicht kategorisiert	Bad Bot
1259	Tool	Bad Bot
1287	Suchmaschine	Bad Bot
1296	Suchmaschine	Bad Bot
1312	Nicht kategorisiert	Bad Bot
1316	Marketing	Bad Bot
1322	Sitemonitor	Bad Bot
1325	Screenshot Creator	Bad Bot
1328	Suchmaschine	Bad Bot
1330	Marketing	Bad Bot
1337	Tool	Bad Bot
1360	Suchmaschine	Bad Bot
1367	Suchmaschine	Bad Bot
1374	Tool	Bad Bot
1380	Nicht kategorisiert	Bad Bot
1388	Suchmaschine	Bad Bot
1400	Feed Fetcher	Bad Bot
1413	Nicht kategorisiert	Bad Bot
1420	Feed Fetcher	Bad Bot
1422	Sitemonitor	Bad Bot
1442	Nicht kategorisiert	Bad Bot
1447	Suchmaschine	Bad Bot
1460	Marketing	Bad Bot
1467	Tool	Bad Bot
1469	Tool	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1471	Suchmaschine	Bad Bot
1484	Nicht kategorisiert	Bad Bot
1493	Marketing	Bad Bot
1502	Sitemonitor	Bad Bot
1504	Nicht kategorisiert	Bad Bot
1506	Nicht kategorisiert	Bad Bot
1518	Nicht kategorisiert	Bad Bot
1520	Suchmaschine	Bad Bot
1531	Feed Fetcher	Bad Bot
1533	Nicht kategorisiert	Bad Bot
1540	Suchmaschine	Bad Bot
1556	Marketing	Bad Bot
1560	Nicht kategorisiert	Bad Bot
1564	Tool	Bad Bot
1570	Sitemonitor	Bad Bot
1575	Suchmaschine	Bad Bot
1586	Viren-Scanner	Bad Bot
1588	Nicht kategorisiert	Bad Bot
1594	Tool	Bad Bot
1619	Marketing	Bad Bot
1623	Tool	Bad Bot
1626	Suchmaschine	Bad Bot
1632	Feed Fetcher	Bad Bot
1648	Suchmaschine	Bad Bot
1652	Marketing	Bad Bot
1660	Marketing	Bad Bot
1713	Tool	Bad Bot
1719	Suchmaschine	Bad Bot
1722	Nicht kategorisiert	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1744	Nicht kategorisiert	Bad Bot
1754	Nicht kategorisiert	Bad Bot
1757	Nicht kategorisiert	Bad Bot
1762	Nicht kategorisiert	Bad Bot
1769	Nicht kategorisiert	Bad Bot
1771	Marketing	Bad Bot
1779	Tool	Bad Bot
1782	Tool	Bad Bot
1785	Geschwindigkeitstester	Bad Bot
1786	Tool	Bad Bot
1792	Sitemonitor	Bad Bot
1869	Tool	Bad Bot
1928	Marketing	Bad Bot
1942	Sitemonitor	Bad Bot
1949	Marketing	Bad Bot
1954	Marketing	Bad Bot
1964	Nicht kategorisiert	Bad Bot
1969	Suchmaschine	Bad Bot
2294	Suchmaschine	Bad Bot
2303	Nicht kategorisiert	Bad Bot
2308	Scraper	Bad Bot
2335	Marketing	Bad Bot
2374	Nicht kategorisiert	Bad Bot
2377	Nicht kategorisiert	Bad Bot
2385	Tool	Bad Bot
2389	Nicht kategorisiert	Bad Bot
2414	Nicht kategorisiert	Bad Bot
2421	Nicht kategorisiert	Bad Bot
2424	Nicht kategorisiert	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
2427	Nicht kategorisiert	Bad Bot
2429	Suchmaschine	Bad Bot
2437	Nicht kategorisiert	Bad Bot
2440	Suchmaschine	Bad Bot
2443	Nicht kategorisiert	Bad Bot
2453	Marketing	Bad Bot
2472	Marketing	Bad Bot
2474	Feed Fetcher	Bad Bot
2482	Nicht kategorisiert	Bad Bot
2500	Screenshot Creator	Bad Bot
2503	Nicht kategorisiert	Bad Bot
2507	Nicht kategorisiert	Bad Bot
2516	Tool	Bad Bot
2536	Marketing	Bad Bot
2543	Tool	Bad Bot
2548	Tool	Bad Bot
2557	Marketing	Bad Bot
2561	Nicht kategorisiert	Bad Bot
2572	Nicht kategorisiert	Bad Bot
2578	Nicht kategorisiert	Bad Bot
2584	Nicht kategorisiert	Bad Bot
2588	Nicht kategorisiert	Bad Bot
2592	Suchmaschine	Bad Bot
2600	Tool	Bad Bot
2606	Nicht kategorisiert	Bad Bot
2611	Nicht kategorisiert	Bad Bot
2622	Tool	Bad Bot
2625	Tool	Bad Bot
2631	Tool	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
2635	Tool	Bad Bot
2637	Screenshot Creator	Bad Bot
2641	Suchmaschine	Bad Bot
2655	Nicht kategorisiert	Bad Bot
2657	Marketing	Bad Bot
2663	Nicht kategorisiert	Bad Bot
2666	Tool	Bad Bot
2672	Feed Fetcher	Bad Bot
2674	Tool	Bad Bot
2681	Suchmaschine	Bad Bot
2684	Marketing	Bad Bot
2690	Nicht kategorisiert	Bad Bot
2704	Nicht kategorisiert	Bad Bot
2707	Nicht kategorisiert	Bad Bot
2714	Feed Fetcher	Bad Bot
2722	Nicht kategorisiert	Bad Bot
2726	Feed Fetcher	Bad Bot
2730	Screenshot Creator	Bad Bot
2736	Nicht kategorisiert	Bad Bot
2749	Nicht kategorisiert	Bad Bot
2753	Tool	Bad Bot
2756	Tool	Bad Bot
2760	Geschwindigkeitstester	Bad Bot
2780	Tool	Bad Bot
2785	Sitemonitor	Bad Bot
2789	Nicht kategorisiert	Bad Bot
2797	Tool	Bad Bot
2801	Tool	Bad Bot
2808	Tool	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
2810	Nicht kategorisiert	Bad Bot
2813	Nicht kategorisiert	Bad Bot
2816	Nicht kategorisiert	Bad Bot
2820	Link Checker	Bad Bot
2824	Link Checker	Bad Bot
2831	Screenshot Creator	Bad Bot
2843	Tool	Bad Bot
2846	Tool	Bad Bot
2849	Marketing	Bad Bot
2851	Nicht kategorisiert	Bad Bot
2855	Nicht kategorisiert	Bad Bot
2859	Tool	Bad Bot
2873	Nicht kategorisiert	Bad Bot
2875	Screenshot Creator	Bad Bot
2879	Nicht kategorisiert	Bad Bot
2881	Nicht kategorisiert	Bad Bot
2886	Sitemonitor	Bad Bot
2899	Nicht kategorisiert	Bad Bot
2916	Nicht kategorisiert	Bad Bot
2924	Tool	Bad Bot
2932	Marketing	Bad Bot
2935	Link Checker	Bad Bot
2939	Marketing	Bad Bot
2942	Nicht kategorisiert	Bad Bot
2955	Suchmaschine	Bad Bot
2960	Tool	Bad Bot
2964	Nicht kategorisiert	Bad Bot
2972	Marketing	Bad Bot
2978	Vulnerability Scanner	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
2980	Tool	Bad Bot
2985	Marketing	Bad Bot
2993	Nicht kategorisiert	Bad Bot
2999	Screenshot Creator	Bad Bot
3003	Feed Fetcher	Bad Bot
3005	Nicht kategorisiert	Bad Bot
3013	Nicht kategorisiert	Bad Bot
3016	Nicht kategorisiert	Bad Bot
3021	Suchmaschine	Bad Bot
3026	Nicht kategorisiert	Bad Bot
3030	Marketing	Bad Bot
3065	Marketing	Bad Bot
3068	Nicht kategorisiert	Bad Bot
3072	Marketing	Bad Bot
3077	Marketing	Bad Bot
3080	Nicht kategorisiert	Bad Bot
3086	Scraper	Bad Bot
3092	Suchmaschine	Bad Bot
3100	Nicht kategorisiert	Bad Bot
3104	Tool	Bad Bot
3111	Nicht kategorisiert	Bad Bot
3116	Sitemonitor	Bad Bot
3118	Tool	Bad Bot
3120	Marketing	Bad Bot
3122	Suchmaschine	Bad Bot
3126	Marketing	Bad Bot
3141	Tool	Bad Bot
3143	Nicht kategorisiert	Bad Bot
3145	Scraper	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3150	Nicht kategorisiert	Bad Bot
3173	Link Checker	Bad Bot
3176	Nicht kategorisiert	Bad Bot
3186	Geschwindigkeitstester	Bad Bot
3190	Scraper	Bad Bot
3203	Suchmaschine	Bad Bot
3216	Nicht kategorisiert	Bad Bot
3220	Tool	Bad Bot
3223	Link Checker	Bad Bot
3241	Nicht kategorisiert	Bad Bot
3245	Sitemonitor	Bad Bot
3285	Nicht kategorisiert	Bad Bot
3304	Marketing	Bad Bot
3307	Link Checker	Bad Bot
3316	Tool	Bad Bot
3326	Marketing	Bad Bot
3333	Suchmaschine	Bad Bot
3340	Suchmaschine	Bad Bot
3344	Marketing	Bad Bot
3350	Nicht kategorisiert	Bad Bot
3355	Marketing	Bad Bot
3365	Nicht kategorisiert	Bad Bot
3378	Nicht kategorisiert	Bad Bot
3388	Tool	Bad Bot
3396	Nicht kategorisiert	Bad Bot
3400	Nicht kategorisiert	Bad Bot
3421	Nicht kategorisiert	Bad Bot
3439	Nicht kategorisiert	Bad Bot
3447	Feed Fetcher	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3451	Tool	Bad Bot
3459	Screenshot Creator	Bad Bot
3469	Vulnerability Scanner	Bad Bot
3475	Nicht kategorisiert	Bad Bot
3485	Suchmaschine	Bad Bot
3493	Tool	Bad Bot
3502	Marketing	Bad Bot
3507	Suchmaschine	Bad Bot
3523	Nicht kategorisiert	Bad Bot
3535	Geschwindigkeitstester	Bad Bot
3549	Nicht kategorisiert	Bad Bot
3556	Nicht kategorisiert	Bad Bot
3561	Nicht kategorisiert	Bad Bot
3565	Nicht kategorisiert	Bad Bot
3572	Suchmaschine	Bad Bot
3578	Nicht kategorisiert	Bad Bot
3610	Suchmaschine	Bad Bot
3617	Nicht kategorisiert	Bad Bot
3621	Marketing	Bad Bot
3632	Tool	Bad Bot
3635	Marketing	Bad Bot
3653	Nicht kategorisiert	Bad Bot
3661	Suchmaschine	Bad Bot
3704	Nicht kategorisiert	Bad Bot
3707	Nicht kategorisiert	Bad Bot
3711	Nicht kategorisiert	Bad Bot
3730	Suchmaschine	Bad Bot
3740	Sitemonitor	Bad Bot
3759	Suchmaschine	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3764	Nicht kategorisiert	Bad Bot
3770	Nicht kategorisiert	Bad Bot

Bot-Signatur-Update für März 2021

May 11, 2023

Einige vorhandene Bot-Signaturen werden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Die Signaturversion 7 ist für NetScaler-Plattformen mit 13.0 61.x-Builds oder höher anwendbar.

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
278	Scraper	Good Bot
378	Scraper	Good Bot
379	Scraper	Good Bot
380	Scraper	Good Bot
381	Scraper	Good Bot
382	Scraper	Good Bot
383	Scraper	Good Bot
384	Scraper	Good Bot
385	Scraper	Good Bot
386	Scraper	Good Bot
387	Scraper	Good Bot
389	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
390	Scraper	Good Bot
391	Scraper	Good Bot
494	Scraper	Good Bot
627	Suchmaschine	Good Bot
660	Suchmaschine	Good Bot
3840	Crawler	Good Bot

Bot-Signatur-Update für August 2021

May 11, 2023

Neue Signaturen werden hinzugefügt und einige vorhandene Bot-Signaturen werden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Die Signaturversion 8 ist für NetScaler-Plattformen mit 13.0 61.x-Builds oder höher anwendbar.

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
236	Scraper	Good Bot
378	Scraper	Good Bot
381	Scraper	Good Bot
382	Scraper	Good Bot
390	Scraper	Good Bot
544	Scraper	Good Bot
702	Suchmaschine	Good Bot
979	Scraper	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3791	Geschwindigkeitstester	Good Bot
3797	Marketing	Good Bot
3800	Marketing	Good Bot
3824	Crawler	Bad Bot
3833	Suchmaschine	Good Bot
3849	Crawler	Good Bot
3871	Marketing	Good Bot
3963	Marketing	Good Bot
4027	Suchmaschine	Good Bot

Neue Bot-Signatur

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4028	Marketing	Good Bot
4029	Tool	Good Bot
4030	Scraper	Good Bot
4031	Scraper	Good Bot
4032	Nicht kategorisiert	Bad Bot
4033	Crawler	Good Bot
4034	Crawler	Good Bot
4035	Marketing	Good Bot
4036	Vulnerability Scanner	Good Bot
4037	Vulnerability Scanner	Good Bot
4038	Nicht kategorisiert	Bad Bot
4039	Tool	Good Bot
4040	Crawler	Good Bot
4041	Tool	Good Bot
4042	Crawler	Good Bot
4043	Screenshot Creator	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4044	Scraper	Bad Bot
4045	Scraper	Bad Bot
4046	Scraper	Bad Bot
4047	Nicht kategorisiert	Bad Bot
4048	Feed Fetcher	Good Bot
4049	Nicht kategorisiert	Bad Bot
4050	Crawler	Good Bot
4051	Crawler	Good Bot
4052	Tool	Good Bot
4053	Tool	Good Bot
4054	Scraper	Bad Bot
4055	Nicht kategorisiert	Good Bot
4056	Marketing	Good Bot
4057	Screenshot Creator	Good Bot
4058	Crawler	Good Bot
4059	Nicht kategorisiert	Bad Bot
4060	Suchmaschine	Good Bot
4061	Suchmaschine	Good Bot
4062	Suchmaschine	Good Bot
4063	Suchmaschine	Good Bot
4064	Tool	Good Bot
4065	Scraper	Good Bot
4066	Marketing	Good Bot
4067	Marketing	Good Bot
4068	Nicht kategorisiert	Bad Bot
4069	Nicht kategorisiert	Bad Bot
4070	Nicht kategorisiert	Bad Bot
4071	Tool	Good Bot
4072	Tool	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4073	Nicht kategorisiert	Bad Bot
4074	Nicht kategorisiert	Bad Bot
4075	Tool	Bad Bot
4076	Marketing	Good Bot
4077	Scraper	Good Bot
4078	Crawler	Good Bot
4079	Crawler	Good Bot
4080	Tool	Bad Bot
4081	Suchmaschine	Good Bot
4082	Tool	Good Bot
4083	Nicht kategorisiert	Bad Bot
4084	Nicht kategorisiert	Bad Bot
4085	Tool	Good Bot
4086	Tool	Good Bot
4087	Tool	Bad Bot
4088	Suchmaschine	Good Bot
4089	Marketing	Good Bot
4090	Tool	Good Bot
4091	Tool	Good Bot
4092	Tool	Good Bot
4093	Tool	Good Bot
4094	Nicht kategorisiert	Good Bot
4095	Sitemonitor	Good Bot
4096	Sitemonitor	Good Bot
4097	Sitemonitor	Good Bot
4098	Crawler	Good Bot
4099	Suchmaschine	Good Bot
4100	Suchmaschine	Good Bot
4101	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4102	Suchmaschine	Good Bot
4103	Marketing	Good Bot
4104	Marketing	Good Bot
4105	Marketing	Good Bot
4106	Marketing	Good Bot
4107	Marketing	Good Bot
4108	Marketing	Good Bot
4109	Suchmaschine	Good Bot
4110	Crawler	Good Bot
4111	Crawler	Good Bot
4112	Crawler	Good Bot
4113	Vulnerability Scanner	Good Bot
4114	Crawler	Good Bot
4115	Tool	Good Bot
4116	Nicht kategorisiert	Bad Bot
4117	Nicht kategorisiert	Bad Bot
4118	Nicht kategorisiert	Bad Bot
4119	Nicht kategorisiert	Bad Bot
4120	Marketing	Good Bot
4121	Marketing	Good Bot
4122	Marketing	Good Bot
4123	Marketing	Good Bot
4124	Marketing	Good Bot
4125	Marketing	Good Bot
4126	Marketing	Good Bot
4127	Marketing	Good Bot
4128	Marketing	Good Bot
4129	Marketing	Good Bot
4130	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4131	Tool	Good Bot
4132	Marketing	Good Bot
4133	Marketing	Good Bot
4134	Tool	Good Bot
4135	Marketing	Good Bot
4136	Marketing	Good Bot
4137	Marketing	Good Bot
4138	Marketing	Good Bot
4139	Marketing	Good Bot
4140	Marketing	Good Bot
4141	Marketing	Good Bot
4142	Marketing	Good Bot
4143	Marketing	Good Bot
4144	Marketing	Good Bot
4145	Suchmaschine	Good Bot
4146	Suchmaschine	Good Bot
4147	Suchmaschine	Good Bot
4148	Suchmaschine	Good Bot
4149	Suchmaschine	Good Bot
4150	Suchmaschine	Good Bot
4151	Suchmaschine	Good Bot
4152	Suchmaschine	Good Bot
4153	Suchmaschine	Good Bot
4154	Suchmaschine	Good Bot
4155	Suchmaschine	Good Bot
4156	Screenshot Creator	Good Bot
4157	Suchmaschine	Good Bot
4158	Suchmaschine	Good Bot
4159	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4160	Screenshot Creator	Good Bot
4161	Suchmaschine	Good Bot
4162	Suchmaschine	Good Bot
4163	Tool	Good Bot
4164	Suchmaschine	Good Bot
4165	Marketing	Good Bot
4166	Nicht kategorisiert	Bad Bot
4167	Tool	Bad Bot
4168	Geschwindigkeitstester	Good Bot
4169	Scraper	Bad Bot
4170	Tool	Good Bot
4171	Scraper	Bad Bot
4172	Webcrawler	Good Bot
4173	Tool	Good Bot
4174	Crawler	Good Bot
4175	Crawler	Good Bot
4176	Tool	Good Bot
4177	Suchmaschine	Good Bot
4178	Tool	Good Bot
4179	Webcrawler	Good Bot
4180	Tool	Good Bot
4181	Sitemonitor	Good Bot
4182	Sitemonitor	Good Bot
4183	Sitemonitor	Good Bot
4184	Sitemonitor	Good Bot
4185	Suchmaschine	Good Bot
4186	Tool	Good Bot
4187	Tool	Good Bot
4188	Screenshot Creator	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4189	Marketing	Good Bot
4190	Suchmaschine	Good Bot
4191	Suchmaschine	Good Bot
4192	Suchmaschine	Good Bot
4193	Suchmaschine	Good Bot
4194	Tool	Good Bot
4195	Suchmaschine	Bad Bot
4196	Tool	Good Bot
4197	Tool	Good Bot
4198	Marketing	Good Bot
4199	Marketing	Good Bot
4200	Vulnerability Scanner	Good Bot
4201	Tool	Good Bot
4202	Tool	Good Bot
4203	Nicht kategorisiert	Bad Bot
4204	Nicht kategorisiert	Bad Bot
4205	Suchmaschine	Good Bot
4206	Marketing	Good Bot
4207	Marketing	Good Bot
4208	Suchmaschine	Good Bot
4209	Suchmaschine	Good Bot
4210	Geschwindigkeitstester	Good Bot
4211	Tool	Good Bot
4212	Feed Fetcher	Good Bot
4213	Feed Fetcher	Good Bot
4214	Scraper	Bad Bot
4215	Tool	Good Bot
4216	Tool	Good Bot
4217	Tool	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4218	Scraper	Bad Bot
4219	Marketing	Good Bot
4220	Tool	Good Bot
4221	Tool	Bad Bot
4222	Sitemonitor	Good Bot
4223	Marketing	Good Bot
4224	Suchmaschine	Good Bot
4225	Suchmaschine	Good Bot
4226	Suchmaschine	Good Bot
4227	Marketing	Good Bot
4228	Marketing	Good Bot
4229	Tool	Good Bot
4230	Nicht kategorisiert	Bad Bot
4231	Screenshot Creator	Good Bot
4232	Tool	Good Bot
4233	Sitemonitor	Good Bot
4234	Sitemonitor	Good Bot
4235	Sitemonitor	Good Bot
4236	Sitemonitor	Good Bot
4237	Sitemonitor	Good Bot
4238	Sitemonitor	Good Bot
4239	Nicht kategorisiert	Bad Bot
4240	Marketing	Good Bot
4241	Marketing	Good Bot
4242	Marketing	Good Bot
4243	Marketing	Good Bot
4244	Marketing	Good Bot
4245	Marketing	Good Bot
4246	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4247	Suchmaschine	Good Bot
4248	Suchmaschine	Good Bot
4249	Screenshot Creator	Good Bot
4250	Suchmaschine	Good Bot
4251	Suchmaschine	Good Bot
4252	Crawler	Good Bot
4253	Crawler	Good Bot
4254	Crawler	Good Bot
4255	Tool	Good Bot
4256	Nicht kategorisiert	Good Bot
4257	Tool	Good Bot
4258	Crawler	Good Bot
4259	Crawler	Good Bot
4260	Tool	Good Bot
4261	Tool	Good Bot
4262	Tool	Good Bot
4263	Marketing	Good Bot
4264	Crawler	Bad Bot
4265	Suchmaschine	Good Bot
4266	Nicht kategorisiert	Good Bot
4267	Tool	Good Bot
4268	Tool	Good Bot
4269	Suchmaschine	Good Bot
4270	Suchmaschine	Good Bot
4271	Suchmaschine	Good Bot
4272	Suchmaschine	Good Bot
4273	Suchmaschine	Good Bot
4274	Suchmaschine	Good Bot
4275	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4276	Nicht kategorisiert	Bad Bot
4277	Nicht kategorisiert	Bad Bot
4278	Nicht kategorisiert	Bad Bot
4279	Marketing	Good Bot
4280	Crawler	Good Bot
4281	Nicht kategorisiert	Bad Bot
4282	Marketing	Good Bot
4283	Marketing	Good Bot
4284	Marketing	Good Bot
4285	Marketing	Good Bot
4286	Marketing	Good Bot
4287	Marketing	Good Bot
4288	Marketing	Good Bot
4289	Marketing	Good Bot
4290	Marketing	Good Bot
4291	Marketing	Good Bot
4292	Marketing	Good Bot
4293	Marketing	Good Bot
4294	Marketing	Good Bot
4295	Suchmaschine	Good Bot
4296	Suchmaschine	Good Bot
4297	Suchmaschine	Good Bot
4298	Suchmaschine	Good Bot
4299	Suchmaschine	Good Bot
4300	Suchmaschine	Good Bot
4301	Suchmaschine	Good Bot
4302	Suchmaschine	Good Bot
4303	Suchmaschine	Good Bot
4304	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4305	Suchmaschine	Good Bot
4306	Screenshot Creator	Good Bot
4307	Suchmaschine	Good Bot
4308	Suchmaschine	Good Bot
4309	Suchmaschine	Good Bot
4310	Suchmaschine	Good Bot
4311	Screenshot Creator	Good Bot
4312	Suchmaschine	Good Bot
4313	Suchmaschine	Good Bot
4314	Suchmaschine	Good Bot
4315	Suchmaschine	Good Bot
4316	Suchmaschine	Good Bot
4317	Suchmaschine	Good Bot
4318	Screenshot Creator	Good Bot
4319	Screenshot Creator	Good Bot
4320	Nicht kategorisiert	Bad Bot
4321	Nicht kategorisiert	Good Bot
4322	Crawler	Good Bot
4323	Tool	Good Bot
4324	Tool	Good Bot
4325	Tool	Good Bot
4326	Scraper	Bad Bot
4327	Suchmaschine	Good Bot
4328	Marketing	Good Bot
4329	Nicht kategorisiert	Bad Bot
4330	Sitemonitor	Good Bot
4331	Suchmaschine	Good Bot
4332	Suchmaschine	Good Bot
4333	Nicht kategorisiert	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4334	Scraper	Good Bot
4335	Marketing	Good Bot
4336	Marketing	Good Bot
4337	Tool	Good Bot
4338	Tool	Good Bot
4339	Tool	Good Bot
4340	Crawler	Good Bot
4341	Crawler	Good Bot
4342	Vulnerability Scanner	Good Bot
4343	Vulnerability Scanner	Good Bot
4344	Scraper	Good Bot
4345	Marketing	Good Bot
4346	Marketing	Good Bot
4347	Marketing	Good Bot
4348	Marketing	Good Bot
4349	Marketing	Good Bot
4350	Marketing	Good Bot
4351	Marketing	Good Bot
4352	Marketing	Good Bot
4353	Marketing	Good Bot
4354	Marketing	Good Bot
4355	Suchmaschine	Good Bot
4356	Suchmaschine	Good Bot
4357	Suchmaschine	Good Bot
4358	Suchmaschine	Good Bot
4359	Suchmaschine	Good Bot
4360	Suchmaschine	Good Bot
4361	Suchmaschine	Good Bot
4362	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4363	Suchmaschine	Good Bot
4364	Suchmaschine	Good Bot
4365	Screenshot Creator	Good Bot
4366	Suchmaschine	Good Bot
4367	Suchmaschine	Good Bot
4368	Suchmaschine	Good Bot
4369	Suchmaschine	Good Bot
4370	Screenshot Creator	Good Bot
4371	Suchmaschine	Good Bot
4372	Suchmaschine	Good Bot
4373	Suchmaschine	Good Bot
4374	Suchmaschine	Good Bot
4375	Suchmaschine	Good Bot
4376	Screenshot Creator	Good Bot
4377	Crawler	Good Bot
4378	Crawler	Good Bot
4379	Suchmaschine	Good Bot
4380	Suchmaschine	Good Bot
4381	Suchmaschine	Good Bot
4382	Suchmaschine	Good Bot
4383	Crawler	Good Bot
4384	Suchmaschine	Good Bot
4385	Tool	Good Bot
4386	Nicht kategorisiert	Good Bot
4387	Crawler	Good Bot
4388	Crawler	Good Bot
4389	Tool	Good Bot
4390	Tool	Good Bot
4391	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4392	Tool	Good Bot
4393	Tool	Good Bot
4394	Nicht kategorisiert	Good Bot
4395	Tool	Good Bot
4396	Sitemonitor	Good Bot
4397	Sitemonitor	Good Bot
4398	Tool	Bad Bot
4399	Tool	Bad Bot
4400	Tool	Bad Bot
4401	Tool	Bad Bot
4402	Tool	Bad Bot
4403	Tool	Bad Bot
4404	Suchmaschine	Good Bot
4405	Suchmaschine	Good Bot
4406	Suchmaschine	Good Bot
4407	Nicht kategorisiert	Good Bot

Aktualisierung der Bot-Signatur für September 2021

May 11, 2023

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 9 gilt für NetScaler-Plattformen mit 13.0 Builds 61.48 oder höher.

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
2	Crawler	Good Bot
5	Crawler	Good Bot
9	Crawler	Good Bot
45	Crawler	Good Bot
46	Crawler	Good Bot
48	Crawler	Good Bot
52	Crawler	Good Bot
60	Crawler	Good Bot
61	Crawler	Good Bot
63	Crawler	Good Bot
67	Crawler	Good Bot
71	Crawler	Good Bot
74	Crawler	Good Bot
75	Crawler	Good Bot
76	Crawler	Good Bot
78	Crawler	Good Bot
79	Crawler	Good Bot
80	Crawler	Good Bot
81	Crawler	Good Bot
82	Crawler	Good Bot
83	Crawler	Good Bot
84	Crawler	Good Bot
87	Crawler	Good Bot
90	Crawler	Good Bot
95	Crawler	Good Bot
96	Crawler	Good Bot
97	Crawler	Good Bot
100	Crawler	Good Bot
101	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
102	Crawler	Good Bot
103	Crawler	Good Bot
104	Crawler	Good Bot
107	Crawler	Good Bot
108	Crawler	Good Bot
110	Crawler	Good Bot
111	Crawler	Good Bot
114	Crawler	Good Bot
115	Crawler	Good Bot
123	Crawler	Good Bot
135	Crawler	Good Bot
136	Crawler	Good Bot
137	Crawler	Good Bot
140	Crawler	Good Bot
141	Crawler	Good Bot
143	Crawler	Good Bot
144	Crawler	Good Bot
145	Crawler	Good Bot
146	Crawler	Good Bot
147	Crawler	Good Bot
149	Crawler	Good Bot
152	Crawler	Good Bot
155	Crawler	Good Bot
156	Crawler	Good Bot
157	Crawler	Good Bot
158	Crawler	Good Bot
159	Crawler	Good Bot
160	Crawler	Good Bot
161	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
162	Crawler	Good Bot
163	Crawler	Good Bot
164	Crawler	Good Bot
165	Crawler	Good Bot
166	Crawler	Good Bot
167	Crawler	Good Bot
172	Crawler	Good Bot
173	Crawler	Good Bot
174	Crawler	Good Bot
176	Crawler	Good Bot
177	Crawler	Good Bot
180	Crawler	Good Bot
187	Crawler	Good Bot
197	Crawler	Good Bot
201	Crawler	Good Bot
202	Crawler	Good Bot
203	Crawler	Good Bot
206	Crawler	Good Bot
211	Feed Fetcher	Bad Bot
217	Feed Fetcher	Good Bot
219	Feed Fetcher	Good Bot
229	Scraper	Good Bot
235	Scraper	Good Bot
236	Scraper	Good Bot
237	Scraper	Good Bot
248	Scraper	Good Bot
250	Scraper	Good Bot
260	Scraper	Good Bot
263	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
265	Scraper	Good Bot
267	Scraper	Good Bot
268	Scraper	Good Bot
271	Scraper	Good Bot
272	Scraper	Good Bot
276	Scraper	Good Bot
277	Scraper	Good Bot
278	Scraper	Good Bot
279	Scraper	Good Bot
280	Scraper	Good Bot
281	Scraper	Good Bot
283	Scraper	Good Bot
285	Scraper	Good Bot
286	Scraper	Good Bot
287	Scraper	Good Bot
290	Scraper	Good Bot
292	Scraper	Good Bot
293	Scraper	Good Bot
342	Scraper	Good Bot
343	Scraper	Good Bot
344	Scraper	Good Bot
355	Scraper	Good Bot
357	Scraper	Good Bot
360	Scraper	Good Bot
362	Scraper	Good Bot
366	Scraper	Good Bot
370	Scraper	Good Bot
371	Scraper	Good Bot
372	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
373	Scraper	Good Bot
374	Scraper	Good Bot
376	Scraper	Good Bot
377	Scraper	Good Bot
380	Scraper	Good Bot
392	Scraper	Good Bot
393	Scraper	Good Bot
394	Scraper	Good Bot
396	Scraper	Good Bot
397	Scraper	Good Bot
414	Scraper	Good Bot
418	Scraper	Good Bot
419	Scraper	Good Bot
421	Scraper	Good Bot
422	Scraper	Good Bot
423	Scraper	Good Bot
424	Scraper	Good Bot
425	Scraper	Good Bot
426	Scraper	Good Bot
427	Scraper	Good Bot
428	Scraper	Good Bot
430	Scraper	Good Bot
432	Scraper	Good Bot
433	Scraper	Good Bot
434	Scraper	Good Bot
435	Scraper	Good Bot
441	Scraper	Good Bot
445	Scraper	Good Bot
446	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
451	Scraper	Good Bot
452	Scraper	Good Bot
454	Scraper	Good Bot
455	Scraper	Good Bot
456	Scraper	Good Bot
457	Scraper	Good Bot
458	Scraper	Good Bot
461	Scraper	Good Bot
465	Scraper	Good Bot
466	Scraper	Good Bot
469	Scraper	Good Bot
473	Scraper	Good Bot
474	Scraper	Good Bot
476	Scraper	Good Bot
477	Scraper	Good Bot
484	Scraper	Good Bot
485	Scraper	Good Bot
487	Scraper	Good Bot
488	Scraper	Good Bot
489	Scraper	Good Bot
490	Scraper	Good Bot
493	Scraper	Good Bot
494	Scraper	Good Bot
495	Scraper	Good Bot
497	Scraper	Good Bot
498	Scraper	Good Bot
499	Scraper	Good Bot
500	Scraper	Good Bot
505	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
506	Scraper	Good Bot
507	Scraper	Good Bot
512	Scraper	Good Bot
513	Scraper	Good Bot
514	Scraper	Good Bot
527	Scraper	Good Bot
533	Scraper	Good Bot
539	Scraper	Good Bot
540	Scraper	Good Bot
542	Scraper	Good Bot
544	Scraper	Good Bot
545	Scraper	Good Bot
546	Scraper	Good Bot
547	Scraper	Good Bot
548	Scraper	Good Bot
551	Scraper	Good Bot
552	Scraper	Good Bot
554	Scraper	Good Bot
556	Scraper	Good Bot
558	Scraper	Good Bot
560	Scraper	Good Bot
561	Scraper	Good Bot
566	Scraper	Good Bot
575	Scraper	Good Bot
578	Scraper	Good Bot
581	Scraper	Good Bot
591	Scraper	Good Bot
593	Scraper	Good Bot
595	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
600	Scraper	Good Bot
601	Scraper	Good Bot
602	Scraper	Good Bot
604	Scraper	Good Bot
605	Scraper	Good Bot
609	Scraper	Good Bot
610	Scraper	Good Bot
611	Scraper	Good Bot
612	Scraper	Good Bot
613	Scraper	Good Bot
615	Scraper	Good Bot
620	Suchmaschine	Good Bot
622	Suchmaschine	Good Bot
623	Suchmaschine	Good Bot
624	Suchmaschine	Good Bot
626	Suchmaschine	Good Bot
627	Suchmaschine	Good Bot
628	Suchmaschine	Good Bot
629	Suchmaschine	Good Bot
633	Suchmaschine	Good Bot
634	Suchmaschine	Good Bot
636	Suchmaschine	Good Bot
637	Suchmaschine	Good Bot
639	Suchmaschine	Good Bot
640	Suchmaschine	Good Bot
641	Suchmaschine	Good Bot
642	Suchmaschine	Good Bot
643	Suchmaschine	Good Bot
647	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
649	Suchmaschine	Good Bot
650	Suchmaschine	Good Bot
651	Suchmaschine	Good Bot
654	Suchmaschine	Good Bot
656	Suchmaschine	Good Bot
657	Suchmaschine	Good Bot
658	Suchmaschine	Good Bot
659	Suchmaschine	Good Bot
660	Suchmaschine	Good Bot
663	Suchmaschine	Good Bot
664	Suchmaschine	Good Bot
665	Suchmaschine	Good Bot
666	Suchmaschine	Good Bot
667	Suchmaschine	Good Bot
669	Suchmaschine	Good Bot
670	Suchmaschine	Good Bot
671	Suchmaschine	Good Bot
672	Suchmaschine	Good Bot
673	Suchmaschine	Good Bot
674	Suchmaschine	Good Bot
675	Suchmaschine	Good Bot
676	Suchmaschine	Good Bot
677	Suchmaschine	Good Bot
679	Suchmaschine	Good Bot
680	Suchmaschine	Good Bot
690	Suchmaschine	Good Bot
693	Suchmaschine	Good Bot
694	Suchmaschine	Good Bot
697	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
698	Suchmaschine	Good Bot
703	Suchmaschine	Good Bot
706	Suchmaschine	Good Bot
712	Suchmaschine	Good Bot
714	Suchmaschine	Good Bot
715	Suchmaschine	Good Bot
716	Suchmaschine	Good Bot
721	Suchmaschine	Good Bot
723	Suchmaschine	Good Bot
725	Suchmaschine	Good Bot
727	Suchmaschine	Good Bot
728	Suchmaschine	Good Bot
729	Suchmaschine	Good Bot
730	Suchmaschine	Good Bot
731	Suchmaschine	Good Bot
732	Suchmaschine	Good Bot
735	Suchmaschine	Good Bot
736	Suchmaschine	Good Bot
740	Suchmaschine	Good Bot
748	Suchmaschine	Good Bot
749	Suchmaschine	Good Bot
750	Suchmaschine	Good Bot
751	Suchmaschine	Good Bot
756	Suchmaschine	Good Bot
757	Suchmaschine	Good Bot
758	Suchmaschine	Good Bot
759	Suchmaschine	Good Bot
760	Suchmaschine	Good Bot
761	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
762	Suchmaschine	Good Bot
763	Suchmaschine	Good Bot
764	Suchmaschine	Good Bot
765	Suchmaschine	Good Bot
766	Suchmaschine	Good Bot
767	Suchmaschine	Good Bot
768	Suchmaschine	Good Bot
769	Suchmaschine	Good Bot
770	Suchmaschine	Good Bot
771	Suchmaschine	Good Bot
772	Suchmaschine	Good Bot
773	Suchmaschine	Good Bot
776	Suchmaschine	Good Bot
777	Suchmaschine	Good Bot
780	Suchmaschine	Good Bot
781	Suchmaschine	Good Bot
784	Suchmaschine	Good Bot
786	Suchmaschine	Good Bot
787	Suchmaschine	Good Bot
788	Suchmaschine	Good Bot
789	Suchmaschine	Good Bot
790	Suchmaschine	Good Bot
791	Suchmaschine	Good Bot
792	Suchmaschine	Good Bot
795	Suchmaschine	Good Bot
796	Suchmaschine	Good Bot
798	Suchmaschine	Good Bot
800	Suchmaschine	Good Bot
801	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
802	Suchmaschine	Good Bot
803	Suchmaschine	Good Bot
805	Suchmaschine	Good Bot
806	Suchmaschine	Good Bot
807	Suchmaschine	Good Bot
809	Suchmaschine	Good Bot
810	Suchmaschine	Good Bot
811	Suchmaschine	Good Bot
812	Suchmaschine	Good Bot
814	Suchmaschine	Good Bot
815	Suchmaschine	Good Bot
816	Suchmaschine	Good Bot
817	Suchmaschine	Good Bot
818	Suchmaschine	Good Bot
819	Suchmaschine	Good Bot
820	Suchmaschine	Good Bot
821	Suchmaschine	Good Bot
822	Suchmaschine	Good Bot
823	Suchmaschine	Good Bot
825	Suchmaschine	Good Bot
827	Suchmaschine	Good Bot
830	Suchmaschine	Good Bot
831	Suchmaschine	Good Bot
834	Suchmaschine	Good Bot
837	Suchmaschine	Good Bot
838	Suchmaschine	Good Bot
849	Sitemonitor	Good Bot
850	Sitemonitor	Good Bot
851	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
853	Sitemonitor	Good Bot
857	Sitemonitor	Good Bot
858	Sitemonitor	Good Bot
859	Sitemonitor	Good Bot
860	Sitemonitor	Good Bot
861	Sitemonitor	Good Bot
862	Sitemonitor	Good Bot
863	Sitemonitor	Good Bot
864	Sitemonitor	Good Bot
865	Sitemonitor	Good Bot
866	Sitemonitor	Good Bot
867	Sitemonitor	Good Bot
868	Sitemonitor	Good Bot
869	Sitemonitor	Good Bot
870	Sitemonitor	Good Bot
871	Sitemonitor	Good Bot
872	Sitemonitor	Good Bot
873	Sitemonitor	Good Bot
874	Sitemonitor	Good Bot
875	Sitemonitor	Good Bot
876	Sitemonitor	Good Bot
877	Sitemonitor	Good Bot
880	Sitemonitor	Good Bot
883	Sitemonitor	Good Bot
885	Sitemonitor	Good Bot
886	Sitemonitor	Good Bot
888	Sitemonitor	Good Bot
889	Sitemonitor	Good Bot
895	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
896	Sitemonitor	Good Bot
897	Sitemonitor	Good Bot
898	Sitemonitor	Good Bot
900	Sitemonitor	Good Bot
901	Sitemonitor	Good Bot
904	Sitemonitor	Good Bot
906	Sitemonitor	Good Bot
908	Sitemonitor	Good Bot
909	Sitemonitor	Good Bot
910	Sitemonitor	Good Bot
911	Sitemonitor	Good Bot
912	Sitemonitor	Good Bot
913	Sitemonitor	Good Bot
917	Sitemonitor	Good Bot
918	Sitemonitor	Good Bot
919	Sitemonitor	Good Bot
920	Sitemonitor	Good Bot
921	Sitemonitor	Good Bot
924	Sitemonitor	Good Bot
926	Sitemonitor	Good Bot
927	Sitemonitor	Good Bot
928	Sitemonitor	Good Bot
929	Sitemonitor	Good Bot
930	Sitemonitor	Good Bot
931	Sitemonitor	Good Bot
938	Sitemonitor	Good Bot
939	Sitemonitor	Good Bot
943	Sitemonitor	Bad Bot
958	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
959	Sitemonitor	Good Bot
960	Sitemonitor	Good Bot
963	Sitemonitor	Good Bot
984	Scraper	Good Bot
996	Scraper	Good Bot
997	Scraper	Good Bot
998	Scraper	Good Bot
1002	Scraper	Good Bot
1006	Scraper	Good Bot
1588	Nicht kategorisiert	Bad Bot
2561	Scraper	Bad Bot
2810	Crawler	Good Bot
3782	Marketing	Good Bot
3783	Suchmaschine	Good Bot
3788	Tool	Good Bot
3789	Tool	Good Bot
3790	Crawler	Good Bot
3792	Tool	Good Bot
3793	Tool	Good Bot
3794	Crawler	Good Bot
3796	Scraper	Good Bot
3798	Marketing	Good Bot
3799	Marketing	Good Bot
3801	Marketing	Good Bot
3802	Screenshot Creator	Good Bot
3803	Suchmaschine	Good Bot
3804	Screenshot Creator	Good Bot
3805	Suchmaschine	Good Bot
3806	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3807	Crawler	Good Bot
3808	Crawler	Good Bot
3809	Tool	Good Bot
3810	Scraper	Good Bot
3811	Tool	Good Bot
3813	Tool	Good Bot
3814	Crawler	Good Bot
3815	Nicht kategorisiert	Good Bot
3817	Tool	Good Bot
3818	Tool	Good Bot
3819	Tool	Good Bot
3820	Crawler	Good Bot
3821	Suchmaschine	Good Bot
3822	Marketing	Good Bot
3823	Nicht kategorisiert	Good Bot
3831	Scraper	Good Bot
3834	Suchmaschine	Good Bot
3835	Suchmaschine	Good Bot
3836	Nicht kategorisiert	Good Bot
3837	Nicht kategorisiert	Good Bot
3838	Nicht kategorisiert	Good Bot
3839	Marketing	Good Bot
3840	Crawler	Good Bot
3842	Crawler	Good Bot
3843	Crawler	Good Bot
3844	Marketing	Good Bot
3845	Marketing	Good Bot
3846	Marketing	Good Bot
3847	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3848	Nicht kategorisiert	Good Bot
3850	Tool	Good Bot
3851	Nicht kategorisiert	Good Bot
3852	Tool	Good Bot
3853	Vulnerability Scanner	Good Bot
3854	Crawler	Good Bot
3855	Crawler	Good Bot
3856	Tool	Good Bot
3861	Marketing	Good Bot
3862	Marketing	Good Bot
3863	Marketing	Good Bot
3864	Marketing	Good Bot
3865	Marketing	Good Bot
3866	Marketing	Good Bot
3867	Marketing	Good Bot
3868	Marketing	Good Bot
3869	Tool	Good Bot
3870	Marketing	Good Bot
3872	Marketing	Good Bot
3873	Suchmaschine	Good Bot
3874	Suchmaschine	Good Bot
3875	Suchmaschine	Good Bot
3876	Suchmaschine	Good Bot
3877	Screenshot Creator	Good Bot
3878	Suchmaschine	Good Bot
3879	Suchmaschine	Good Bot
3880	Screenshot Creator	Good Bot
3881	Screenshot Creator	Good Bot
3882	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3883	Suchmaschine	Good Bot
3884	Suchmaschine	Good Bot
3885	Suchmaschine	Good Bot
3886	Tool	Good Bot
3887	Crawler	Good Bot
3888	Crawler	Good Bot
3889	Nicht kategorisiert	Good Bot
3890	Marketing	Good Bot
3893	Crawler	Good Bot
3894	Tool	Good Bot
3895	Tool	Good Bot
3896	Suchmaschine	Good Bot
3897	Tool	Good Bot
3898	Tool	Good Bot
3899	Nicht kategorisiert	Good Bot
3901	Crawler	Good Bot
3903	Tool	Good Bot
3904	Suchmaschine	Good Bot
3905	Suchmaschine	Good Bot
3906	Suchmaschine	Good Bot
3912	Crawler	Good Bot
3918	Crawler	Good Bot
3919	Nicht kategorisiert	Good Bot
3920	Nicht kategorisiert	Good Bot
3921	Nicht kategorisiert	Good Bot
3922	Nicht kategorisiert	Good Bot
3923	Nicht kategorisiert	Good Bot
3924	Nicht kategorisiert	Good Bot
3925	Nicht kategorisiert	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3926	Marketing	Good Bot
3927	Marketing	Good Bot
3928	Marketing	Good Bot
3929	Tool	Good Bot
3930	Marketing	Good Bot
3931	Nicht kategorisiert	Good Bot
3932	Crawler	Good Bot
3933	Marketing	Good Bot
3934	Marketing	Good Bot
3935	Scraper	Good Bot
3936	Marketing	Good Bot
3937	Scraper	Good Bot
3938	Feed Fetcher	Good Bot
3940	Suchmaschine	Good Bot
3941	Crawler	Good Bot
3942	Scraper	Good Bot
3946	Feed Fetcher	Good Bot
3947	Crawler	Good Bot
3950	Viren-Scanner	Good Bot
3951	Marketing	Good Bot
3952	Marketing	Good Bot
3953	Marketing	Good Bot
3954	Marketing	Good Bot
3955	Marketing	Good Bot
3956	Marketing	Good Bot
3957	Marketing	Good Bot
3958	Marketing	Good Bot
3959	Marketing	Good Bot
3960	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3961	Marketing	Good Bot
3962	Marketing	Good Bot
3964	Marketing	Good Bot
3965	Marketing	Good Bot
3966	Marketing	Good Bot
3967	Marketing	Good Bot
3968	Marketing	Good Bot
3969	Marketing	Good Bot
3970	Suchmaschine	Good Bot
3971	Screenshot Creator	Good Bot
3972	Screenshot Creator	Good Bot
3973	Suchmaschine	Good Bot
3974	Suchmaschine	Good Bot
3975	Suchmaschine	Good Bot
3976	Suchmaschine	Good Bot
3977	Suchmaschine	Good Bot
3978	Screenshot Creator	Good Bot
3979	Suchmaschine	Good Bot
3980	Screenshot Creator	Good Bot
3981	Suchmaschine	Good Bot
3982	Suchmaschine	Good Bot
3983	Suchmaschine	Good Bot
3984	Suchmaschine	Good Bot
3985	Suchmaschine	Good Bot
3986	Suchmaschine	Good Bot
3987	Screenshot Creator	Good Bot
3988	Suchmaschine	Good Bot
3989	Suchmaschine	Good Bot
3990	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3991	Suchmaschine	Good Bot
3992	Suchmaschine	Good Bot
3993	Suchmaschine	Good Bot
3994	Suchmaschine	Good Bot
3995	Suchmaschine	Good Bot
3996	Suchmaschine	Good Bot
3997	Suchmaschine	Good Bot
3998	Suchmaschine	Good Bot
3999	Suchmaschine	Good Bot
4000	Screenshot Creator	Good Bot
4001	Suchmaschine	Good Bot
4002	Suchmaschine	Good Bot
4003	Suchmaschine	Good Bot
4004	Suchmaschine	Good Bot
4005	Screenshot Creator	Good Bot
4006	Crawler	Good Bot
4007	Marketing	Good Bot
4008	Marketing	Good Bot
4011	Tool	Good Bot
4012	Crawler	Good Bot
4013	Suchmaschine	Good Bot
4014	Tool	Good Bot
4015	Crawler	Good Bot
4016	Crawler	Good Bot
4017	Tool	Good Bot
4018	Tool	Good Bot
4019	Tool	Good Bot
4020	Tool	Good Bot
4021	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4024	Tool	Good Bot
4025	Suchmaschine	Good Bot
4026	Suchmaschine	Good Bot
4028	Marketing	Good Bot
4029	Tool	Good Bot
4030	Scraper	Good Bot
4031	Scraper	Good Bot
4035	Marketing	Good Bot
4037	Vulnerability Scanner	Good Bot
4042	Crawler	Good Bot
4043	Screenshot Creator	Good Bot
4048	Feed Fetcher	Good Bot
4052	Tool	Good Bot
4055	Nicht kategorisiert	Good Bot
4056	Marketing	Good Bot
4057	Screenshot Creator	Good Bot
4058	Crawler	Good Bot
4060	Suchmaschine	Good Bot
4061	Suchmaschine	Good Bot
4062	Suchmaschine	Good Bot
4063	Suchmaschine	Good Bot
4065	Scraper	Good Bot
4066	Marketing	Good Bot
4067	Marketing	Good Bot
4071	Tool	Good Bot
4076	Marketing	Good Bot
4078	Crawler	Good Bot
4079	Crawler	Good Bot
4081	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4082	Tool	Good Bot
4085	Tool	Good Bot
4086	Tool	Good Bot
4090	Tool	Good Bot
4091	Tool	Good Bot
4092	Tool	Good Bot
4093	Tool	Good Bot
4094	Nicht kategorisiert	Good Bot
4095	Sitemonitor	Good Bot
4096	Sitemonitor	Good Bot
4097	Sitemonitor	Good Bot
4098	Crawler	Good Bot
4099	Suchmaschine	Good Bot
4100	Suchmaschine	Good Bot
4101	Suchmaschine	Good Bot
4102	Suchmaschine	Good Bot
4103	Marketing	Good Bot
4104	Marketing	Good Bot
4105	Marketing	Good Bot
4106	Marketing	Good Bot
4107	Marketing	Good Bot
4108	Marketing	Good Bot
4109	Suchmaschine	Good Bot
4110	Crawler	Good Bot
4111	Crawler	Good Bot
4112	Crawler	Good Bot
4113	Vulnerability Scanner	Good Bot
4114	Crawler	Good Bot
4115	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4120	Marketing	Good Bot
4121	Marketing	Good Bot
4122	Marketing	Good Bot
4123	Marketing	Good Bot
4124	Marketing	Good Bot
4125	Marketing	Good Bot
4126	Marketing	Good Bot
4127	Marketing	Good Bot
4128	Marketing	Good Bot
4129	Marketing	Good Bot
4130	Marketing	Good Bot
4131	Tool	Good Bot
4132	Marketing	Good Bot
4133	Marketing	Good Bot
4134	Tool	Good Bot
4135	Marketing	Good Bot
4136	Marketing	Good Bot
4137	Marketing	Good Bot
4138	Marketing	Good Bot
4139	Marketing	Good Bot
4140	Marketing	Good Bot
4141	Marketing	Good Bot
4142	Marketing	Good Bot
4143	Marketing	Good Bot
4144	Marketing	Good Bot
4147	Suchmaschine	Good Bot
4148	Suchmaschine	Good Bot
4149	Suchmaschine	Good Bot
4150	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4151	Suchmaschine	Good Bot
4152	Suchmaschine	Good Bot
4153	Suchmaschine	Good Bot
4154	Suchmaschine	Good Bot
4155	Suchmaschine	Good Bot
4156	Screenshot Creator	Good Bot
4157	Suchmaschine	Good Bot
4158	Suchmaschine	Good Bot
4159	Suchmaschine	Good Bot
4160	Screenshot Creator	Good Bot
4161	Suchmaschine	Good Bot
4162	Suchmaschine	Good Bot
4163	Tool	Good Bot
4164	Suchmaschine	Good Bot
4168	Geschwindigkeitstester	Good Bot
4170	Tool	Good Bot
4172	Crawler	Good Bot
4173	Tool	Good Bot
4174	Crawler	Good Bot
4175	Crawler	Good Bot
4176	Tool	Good Bot
4177	Suchmaschine	Good Bot
4178	Tool	Good Bot
4179	Crawler	Good Bot
4180	Tool	Good Bot
4181	Sitemonitor	Good Bot
4182	Sitemonitor	Good Bot
4183	Sitemonitor	Good Bot
4184	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4185	Suchmaschine	Good Bot
4186	Tool	Good Bot
4187	Tool	Good Bot
4190	Suchmaschine	Good Bot
4191	Suchmaschine	Good Bot
4192	Suchmaschine	Good Bot
4193	Suchmaschine	Good Bot
4194	Tool	Good Bot
4196	Tool	Good Bot
4197	Tool	Good Bot
4198	Marketing	Good Bot
4199	Marketing	Good Bot
4200	Vulnerability Scanner	Good Bot
4201	Tool	Good Bot
4202	Tool	Good Bot
4205	Suchmaschine	Good Bot
4206	Marketing	Good Bot
4207	Marketing	Good Bot
4208	Suchmaschine	Good Bot
4209	Suchmaschine	Good Bot
4210	Geschwindigkeitstester	Good Bot
4211	Tool	Good Bot
4212	Feed Fetcher	Good Bot
4213	Feed Fetcher	Good Bot
4215	Tool	Good Bot
4216	Tool	Good Bot
4219	Marketing	Good Bot
4220	Tool	Good Bot
4222	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4223	Marketing	Good Bot
4224	Suchmaschine	Good Bot
4225	Suchmaschine	Good Bot
4226	Suchmaschine	Good Bot
4227	Marketing	Good Bot
4228	Marketing	Good Bot
4229	Tool	Good Bot
4231	Screenshot Creator	Good Bot
4232	Tool	Good Bot
4233	Sitemonitor	Good Bot
4234	Sitemonitor	Good Bot
4235	Sitemonitor	Good Bot
4236	Sitemonitor	Good Bot
4237	Sitemonitor	Good Bot
4238	Sitemonitor	Good Bot
4240	Marketing	Good Bot
4241	Marketing	Good Bot
4242	Marketing	Good Bot
4243	Marketing	Good Bot
4244	Marketing	Good Bot
4245	Marketing	Good Bot
4246	Marketing	Good Bot
4247	Suchmaschine	Good Bot
4248	Suchmaschine	Good Bot
4249	Screenshot Creator	Good Bot
4250	Suchmaschine	Good Bot
4251	Suchmaschine	Good Bot
4252	Crawler	Good Bot
4253	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4254	Crawler	Good Bot
4255	Tool	Good Bot
4256	Nicht kategorisiert	Good Bot
4257	Tool	Good Bot
4258	Crawler	Good Bot
4259	Crawler	Good Bot
4260	Tool	Good Bot
4261	Tool	Good Bot
4262	Tool	Good Bot
4265	Suchmaschine	Good Bot
4266	Nicht kategorisiert	Good Bot
4267	Tool	Good Bot
4268	Tool	Good Bot
4269	Suchmaschine	Good Bot
4270	Suchmaschine	Good Bot
4271	Suchmaschine	Good Bot
4272	Suchmaschine	Good Bot
4273	Suchmaschine	Good Bot
4274	Suchmaschine	Good Bot
4275	Suchmaschine	Good Bot
4279	Marketing	Good Bot
4280	Crawler	Good Bot
4282	Marketing	Good Bot
4283	Marketing	Good Bot
4284	Marketing	Good Bot
4285	Marketing	Good Bot
4286	Marketing	Good Bot
4287	Marketing	Good Bot
4288	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4289	Marketing	Good Bot
4290	Marketing	Good Bot
4291	Marketing	Good Bot
4292	Marketing	Good Bot
4293	Marketing	Good Bot
4294	Marketing	Good Bot
4295	Suchmaschine	Good Bot
4296	Suchmaschine	Good Bot
4297	Suchmaschine	Good Bot
4298	Suchmaschine	Good Bot
4299	Suchmaschine	Good Bot
4300	Suchmaschine	Good Bot
4301	Suchmaschine	Good Bot
4302	Suchmaschine	Good Bot
4303	Suchmaschine	Good Bot
4304	Suchmaschine	Good Bot
4305	Suchmaschine	Good Bot
4306	Screenshot Creator	Good Bot
4307	Suchmaschine	Good Bot
4308	Suchmaschine	Good Bot
4309	Suchmaschine	Good Bot
4310	Suchmaschine	Good Bot
4311	Screenshot Creator	Good Bot
4312	Suchmaschine	Good Bot
4313	Suchmaschine	Good Bot
4314	Suchmaschine	Good Bot
4315	Suchmaschine	Good Bot
4316	Suchmaschine	Good Bot
4317	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4318	Screenshot Creator	Good Bot
4319	Screenshot Creator	Good Bot
4321	Nicht kategorisiert	Good Bot
4322	Crawler	Good Bot
4323	Tool	Good Bot
4324	Tool	Good Bot
4325	Tool	Good Bot
4328	Marketing	Good Bot
4330	Sitemonitor	Good Bot
4331	Suchmaschine	Good Bot
4332	Suchmaschine	Good Bot
4335	Marketing	Good Bot
4336	Marketing	Good Bot
4337	Tool	Good Bot
4338	Tool	Good Bot
4339	Tool	Good Bot
4340	Crawler	Good Bot
4341	Crawler	Good Bot
4342	Vulnerability Scanner	Good Bot
4343	Vulnerability Scanner	Good Bot
4344	Scraper	Good Bot
4345	Marketing	Good Bot
4346	Marketing	Good Bot
4347	Marketing	Good Bot
4348	Marketing	Good Bot
4349	Marketing	Good Bot
4350	Marketing	Good Bot
4351	Marketing	Good Bot
4352	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4353	Marketing	Good Bot
4354	Marketing	Good Bot
4355	Suchmaschine	Good Bot
4356	Suchmaschine	Good Bot
4357	Suchmaschine	Good Bot
4358	Suchmaschine	Good Bot
4359	Suchmaschine	Good Bot
4360	Suchmaschine	Good Bot
4361	Suchmaschine	Good Bot
4362	Suchmaschine	Good Bot
4363	Suchmaschine	Good Bot
4364	Suchmaschine	Good Bot
4365	Screenshot Creator	Good Bot
4366	Suchmaschine	Good Bot
4367	Suchmaschine	Good Bot
4368	Suchmaschine	Good Bot
4369	Suchmaschine	Good Bot
4370	Screenshot Creator	Good Bot
4371	Suchmaschine	Good Bot
4372	Suchmaschine	Good Bot
4373	Suchmaschine	Good Bot
4374	Suchmaschine	Good Bot
4375	Suchmaschine	Good Bot
4376	Screenshot Creator	Good Bot
4377	Crawler	Good Bot
4378	Crawler	Good Bot
4379	Suchmaschine	Good Bot
4380	Suchmaschine	Good Bot
4381	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4382	Suchmaschine	Good Bot
4383	Crawler	Good Bot
4384	Suchmaschine	Good Bot
4385	Tool	Good Bot
4386	Nicht kategorisiert	Good Bot
4387	Crawler	Good Bot
4388	Crawler	Good Bot
4389	Tool	Good Bot
4390	Tool	Good Bot
4391	Tool	Good Bot
4392	Tool	Good Bot
4393	Tool	Good Bot
4394	Nicht kategorisiert	Good Bot
4395	Tool	Good Bot
4396	Sitemonitor	Good Bot
4397	Sitemonitor	Good Bot
4404	Suchmaschine	Good Bot
4405	Suchmaschine	Good Bot
4406	Suchmaschine	Good Bot
4407	Nicht kategorisiert	Good Bot

Bot-Signatur-Update für Oktober 2021

May 11, 2023

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 10 gilt für NetScaler-Plattformen mit 13.0 Builds von 76.31 oder höher.

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
71	Crawler	Good Bot
74	Crawler	Good Bot
75	Crawler	Good Bot
372	Scraper	Good Bot
373	Scraper	Good Bot
374	Scraper	Good Bot
375	Scraper	Good Bot
376	Scraper	Good Bot
377	Scraper	Good Bot
378	Scraper	Good Bot
379	Scraper	Good Bot
380	Scraper	Good Bot
381	Scraper	Good Bot
382	Scraper	Good Bot
383	Scraper	Good Bot
384	Scraper	Good Bot
385	Scraper	Good Bot
386	Scraper	Good Bot
387	Scraper	Good Bot
389	Scraper	Good Bot
390	Scraper	Good Bot
391	Scraper	Good Bot
639	Suchmaschine	Good Bot
702	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
703	Suchmaschine	Good Bot
1173	Tool	Good Bot
1174	Marketing	Good Bot
1176	Suchmaschine	Good Bot
1178	Geschwindigkeitstester	Good Bot
1185	Screenshot Creator	Good Bot
1209	Nicht kategorisiert	Good Bot
1531	Feed Fetcher	Good Bot
2586	Nicht kategorisiert	Good Bot
2674	Tool	Good Bot
2756	Tool	Good Bot
2758	Nicht kategorisiert	Good Bot
2759	Tool	Good Bot
2784	Tool	Good Bot
2952	Tool	Good Bot
3163	Tool	Good Bot
3554	Tool	Good Bot
3782	Marketing	Good Bot
3788	Tool	Good Bot
3789	Tool	Good Bot
3797	Marketing	Good Bot
3798	Marketing	Good Bot
3799	Marketing	Good Bot
3800	Marketing	Good Bot
3801	Marketing	Good Bot
3802	Screenshot Creator	Good Bot
3803	Suchmaschine	Good Bot
3804	Screenshot Creator	Good Bot
3805	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3861	Marketing	Good Bot
3862	Marketing	Good Bot
3863	Marketing	Good Bot
3864	Marketing	Good Bot
3865	Marketing	Good Bot
3866	Marketing	Good Bot
3867	Marketing	Good Bot
3868	Marketing	Good Bot
3869	Tool	Good Bot
3871	Marketing	Good Bot
3872	Marketing	Good Bot
3873	Suchmaschine	Good Bot
3874	Suchmaschine	Good Bot
3875	Suchmaschine	Good Bot
3876	Suchmaschine	Good Bot
3877	Screenshot Creator	Good Bot
3878	Suchmaschine	Good Bot
3879	Suchmaschine	Good Bot
3880	Screenshot Creator	Good Bot
3881	Screenshot Creator	Good Bot
3882	Suchmaschine	Good Bot
3883	Suchmaschine	Good Bot
3884	Suchmaschine	Good Bot
3885	Suchmaschine	Good Bot
3963	Marketing	Good Bot
4040	Crawler	Good Bot
4041	Tool	Good Bot
4120	Marketing	Good Bot
4122	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4123	Marketing	Good Bot
4124	Marketing	Good Bot
4125	Marketing	Good Bot
4133	Marketing	Good Bot
4134	Tool	Good Bot
4135	Marketing	Good Bot
4136	Marketing	Good Bot
4137	Marketing	Good Bot
4138	Marketing	Good Bot
4139	Marketing	Good Bot
4140	Marketing	Good Bot
4141	Marketing	Good Bot
4142	Marketing	Good Bot
4143	Marketing	Good Bot
4144	Marketing	Good Bot
4145	Suchmaschine	Good Bot
4146	Suchmaschine	Good Bot
4147	Suchmaschine	Good Bot
4148	Suchmaschine	Good Bot
4149	Suchmaschine	Good Bot
4150	Suchmaschine	Good Bot
4151	Suchmaschine	Good Bot
4152	Suchmaschine	Good Bot
4153	Suchmaschine	Good Bot
4154	Suchmaschine	Good Bot
4155	Suchmaschine	Good Bot
4156	Screenshot Creator	Good Bot
4157	Suchmaschine	Good Bot
4158	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4159	Suchmaschine	Good Bot
4160	Screenshot Creator	Good Bot
4161	Suchmaschine	Good Bot
4162	Suchmaschine	Good Bot
4163	Tool	Good Bot
4164	Suchmaschine	Good Bot
4209	Suchmaschine	Good Bot
4240	Marketing	Good Bot
4241	Marketing	Good Bot
4248	Suchmaschine	Good Bot
4249	Screenshot Creator	Good Bot
4250	Suchmaschine	Good Bot
4251	Suchmaschine	Good Bot
4282	Marketing	Good Bot
4283	Marketing	Good Bot
4284	Marketing	Good Bot
4285	Marketing	Good Bot
4286	Marketing	Good Bot
4287	Marketing	Good Bot
4288	Marketing	Good Bot
4289	Marketing	Good Bot
4290	Marketing	Good Bot
4291	Marketing	Good Bot
4292	Marketing	Good Bot
4293	Marketing	Good Bot
4294	Marketing	Good Bot
4295	Suchmaschine	Good Bot
4296	Suchmaschine	Good Bot
4297	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4298	Suchmaschine	Good Bot
4299	Suchmaschine	Good Bot
4300	Suchmaschine	Good Bot
4301	Suchmaschine	Good Bot
4302	Suchmaschine	Good Bot
4303	Suchmaschine	Good Bot
4304	Suchmaschine	Good Bot
4305	Suchmaschine	Good Bot
4306	Screenshot Creator	Good Bot
4307	Suchmaschine	Good Bot
4308	Suchmaschine	Good Bot
4309	Suchmaschine	Good Bot
4310	Suchmaschine	Good Bot
4311	Screenshot Creator	Good Bot
4312	Suchmaschine	Good Bot
4313	Suchmaschine	Good Bot
4314	Suchmaschine	Good Bot
4315	Suchmaschine	Good Bot
4316	Suchmaschine	Good Bot
4317	Suchmaschine	Good Bot
4318	Screenshot Creator	Good Bot
4319	Screenshot Creator	Good Bot
4337	Tool	Good Bot
4338	Tool	Good Bot
4345	Marketing	Good Bot
4346	Marketing	Good Bot
4347	Marketing	Good Bot
4348	Marketing	Good Bot
4349	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4350	Marketing	Good Bot
4351	Marketing	Good Bot
4352	Marketing	Good Bot
4353	Marketing	Good Bot
4354	Marketing	Good Bot
4355	Suchmaschine	Good Bot
4356	Suchmaschine	Good Bot
4357	Suchmaschine	Good Bot
4358	Suchmaschine	Good Bot
4359	Suchmaschine	Good Bot
4360	Suchmaschine	Good Bot
4361	Suchmaschine	Good Bot
4362	Suchmaschine	Good Bot
4363	Suchmaschine	Good Bot
4364	Suchmaschine	Good Bot
4365	Screenshot Creator	Good Bot
4366	Suchmaschine	Good Bot
4367	Suchmaschine	Good Bot
4368	Suchmaschine	Good Bot
4369	Suchmaschine	Good Bot
4370	Screenshot Creator	Good Bot
4371	Suchmaschine	Good Bot
4372	Suchmaschine	Good Bot
4373	Suchmaschine	Good Bot
4374	Suchmaschine	Good Bot
4375	Suchmaschine	Good Bot
4376	Screenshot Creator	Good Bot

Bot-Signatur-Update für November 2021

May 11, 2023

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 11 gilt für NetScaler-Plattformen mit 13.0 Builds von 76.31 oder höher.

Neue Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4408	Scraper	Good Bot
4409	Crawler	Bad Bot
4411	Marketing	Good Bot
4412	Marketing	Good Bot
4413	Marketing	Good Bot
4421	Screenshot Creator	Good Bot
4422	Crawler	Good Bot
4423	Tool	Bad Bot
4424	Sitemonitor	Good Bot
4425	Marketing	Good Bot
4426	Crawler	Bad Bot
4427	Scraper	Good Bot
4428	Scraper	Good Bot
4429	Screenshot Creator	Good Bot
4430	Viren-Scanner	Good Bot
4431	Sitemonitor	Good Bot
4432	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4433	Suchmaschine	Good Bot
4434	Suchmaschine	Good Bot
4435	Suchmaschine	Good Bot
4436	Marketing	Good Bot
4437	Marketing	Good Bot
4438	Scraper	Good Bot
4439	Scraper	Good Bot
4440	Scraper	Good Bot
4441	Feed Fetcher	Good Bot
4442	Marketing	Good Bot
4443	Scraper	Good Bot
4445	Nicht kategorisiert	Bad Bot
4446	Scraper	Good Bot
4450	Screenshot Creator	Good Bot
4451	Geschwindigkeitstester	Good Bot
4452	Suchmaschine	Good Bot
4466	Nicht kategorisiert	Good Bot
4467	Screenshot Creator	Good Bot
4468	Tool	Good Bot
4469	Nicht kategorisiert	Good Bot
4470	Tool	Good Bot
4472	Scraper	Good Bot
4473	Nicht kategorisiert	Good Bot
4474	Marketing	Good Bot
4476	Crawler	Good Bot
4477	Crawler	Good Bot
4478	Crawler	Good Bot
4479	Crawler	Good Bot
4480	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4481	Crawler	Good Bot
4482	Crawler	Good Bot
4483	Crawler	Good Bot
4484	Crawler	Good Bot
4485	Crawler	Good Bot
4486	Scraper	Good Bot
4487	Scraper	Good Bot
4488	Scraper	Good Bot
4489	Suchmaschine	Good Bot
4491	Tool	Good Bot
4492	Nicht kategorisiert	Bad Bot
4493	Crawler	Good Bot
4494	Tool	Good Bot
4496	Tool	Good Bot
4497	Crawler	Good Bot
4498	Nicht kategorisiert	Bad Bot
4499	Nicht kategorisiert	Bad Bot
4501	Marketing	Good Bot
4502	Marketing	Good Bot
4503	Marketing	Good Bot
4508	Nicht kategorisiert	Good Bot
4509	Nicht kategorisiert	Good Bot
4510	Nicht kategorisiert	Good Bot
4511	Nicht kategorisiert	Good Bot
4512	Tool	Good Bot
4513	Tool	Good Bot
4514	Tool	Good Bot
4515	Tool	Good Bot
4516	Nicht kategorisiert	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4518	Scraper	Bad Bot
4519	Screenshot Creator	Good Bot
4520	Marketing	Good Bot
4521	Nicht kategorisiert	Good Bot
4522	Tool	Good Bot
4523	Nicht kategorisiert	Bad Bot
4524	Nicht kategorisiert	Bad Bot
4525	Crawler	Good Bot
4526	Crawler	Good Bot
4527	Crawler	Good Bot
4528	Crawler	Good Bot
4529	Crawler	Good Bot
4530	Nicht kategorisiert	Bad Bot
4531	Marketing	Good Bot
4532	Marketing	Good Bot
4533	Marketing	Good Bot
4534	Marketing	Good Bot
4535	Marketing	Good Bot
4541	Marketing	Good Bot
4552	Nicht kategorisiert	Good Bot
4553	Tool	Bad Bot
4554	Tool	Bad Bot
4555	Tool	Good Bot
4556	Tool	Good Bot
4558	Scraper	Good Bot
4559	Crawler	Good Bot
4560	Crawler	Good Bot
4561	Sitemonitor	Good Bot
4562	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4563	Suchmaschine	Good Bot
1000000	Browser	Good Bot
1000001	Scraper	Bad Bot
1000002	Anwendung	Bad Bot
1000003	Browser	Good Bot
1000004	Scraper	Good Bot
1000005	Scraper	Good Bot
1000006	Crawler	Bad Bot
1000007	Browser	Bad Bot
1000008	Nicht kategorisiert	Bad Bot
1000009	Browser	Good Bot
1000010	Scraper	Bad Bot
1000011	Browser	Bad Bot
1000012	Browser	Good Bot
1000013	Browser	Bad Bot
1000014	Scraper	Good Bot
1000015	Scraper	Bad Bot
1000016	Scraper	Bad Bot
1000017	Browser	Good Bot
1000018	Browser	Bad Bot
1000019	Nicht kategorisiert	Bad Bot
1000020	Scraper	Good Bot
1000021	Browser	Bad Bot
1000022	Scraper	Good Bot
1000023	Scraper	Good Bot
1000024	Crawler	Good Bot
1000025	Browser	Bad Bot
1000026	Analysator	Good Bot
1000027	Analysator	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000028	Analysator	Good Bot
1000029	Analysator	Good Bot
1000030	Analysator	Good Bot
1000031	Browser	Good Bot
1000032	Analysator	Good Bot
1000033	Analysator	Good Bot
1000034	Browser	Bad Bot
1000035	Scraper	Good Bot
1000036	Scraper	Good Bot
1000037	Analysator	Good Bot
1000038	Analysator	Good Bot
1000039	Analysator	Good Bot
1000040	Analysator	Good Bot
1000041	Scraper	Good Bot
1000042	Analysator	Good Bot
1000043	Analysator	Good Bot
1000044	Crawler	Good Bot
1000045	Browser	Bad Bot
1000046	Browser	Bad Bot
1000047	Scraper	Good Bot
1000048	Browser	Bad Bot
1000049	Analysator	Good Bot
1000050	Browser	Bad Bot
1000051	Browser	Good Bot
1000052	Browser	Bad Bot
1000053	Scraper	Good Bot
1000054	Browser	Good Bot
1000055	Browser	Good Bot
1000056	Scraper	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000057	Crawler	Bad Bot
1000058	Scraper	Bad Bot
1000059	Analysator	Good Bot
1000060	Browser	Bad Bot
1000061	Browser	Bad Bot
1000062	Browser	Bad Bot
1000063	Scraper	Bad Bot
1000064	Scraper	Bad Bot
1000065	Scraper	Bad Bot
1000066	Anwendung	Bad Bot
1000067	Scraper	Bad Bot
1000068	Browser	Bad Bot
1000069	Scraper	Bad Bot
1000070	Scraper	Good Bot
1000071	Browser	Good Bot
1000072	Browser	Good Bot
1000073	Browser	Bad Bot
1000074	Browser	Bad Bot
1000075	Anwendung	Bad Bot
1000076	Scraper	Bad Bot

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
2	Crawler	Good Bot
5	Crawler	Good Bot
9	Crawler	Good Bot
30	Crawler	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
45	Crawler	Good Bot
46	Crawler	Good Bot
48	Crawler	Good Bot
52	Crawler	Good Bot
60	Crawler	Good Bot
61	Crawler	Good Bot
63	Crawler	Good Bot
67	Crawler	Good Bot
76	Crawler	Good Bot
78	Crawler	Good Bot
79	Crawler	Good Bot
80	Crawler	Good Bot
81	Crawler	Good Bot
82	Crawler	Good Bot
83	Crawler	Good Bot
84	Crawler	Good Bot
87	Crawler	Good Bot
90	Crawler	Good Bot
95	Crawler	Good Bot
96	Crawler	Good Bot
97	Crawler	Good Bot
100	Crawler	Good Bot
101	Crawler	Good Bot
102	Crawler	Good Bot
103	Crawler	Good Bot
104	Crawler	Good Bot
107	Crawler	Good Bot
108	Crawler	Good Bot
110	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
111	Crawler	Good Bot
114	Crawler	Good Bot
115	Crawler	Good Bot
123	Crawler	Good Bot
135	Crawler	Good Bot
136	Crawler	Good Bot
137	Crawler	Good Bot
140	Crawler	Good Bot
141	Crawler	Good Bot
143	Crawler	Good Bot
144	Crawler	Good Bot
145	Crawler	Good Bot
146	Crawler	Good Bot
147	Crawler	Good Bot
149	Crawler	Good Bot
152	Crawler	Good Bot
155	Crawler	Good Bot
156	Crawler	Good Bot
157	Crawler	Good Bot
158	Crawler	Good Bot
159	Crawler	Good Bot
160	Crawler	Good Bot
161	Crawler	Good Bot
162	Crawler	Good Bot
163	Crawler	Good Bot
164	Crawler	Good Bot
165	Crawler	Good Bot
166	Crawler	Good Bot
167	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
172	Crawler	Good Bot
173	Crawler	Good Bot
174	Crawler	Good Bot
176	Crawler	Good Bot
177	Crawler	Good Bot
180	Crawler	Good Bot
182	Crawler	Good Bot
187	Crawler	Good Bot
197	Crawler	Good Bot
201	Crawler	Good Bot
202	Crawler	Good Bot
203	Crawler	Good Bot
206	Crawler	Good Bot
217	Feed Fetcher	Good Bot
219	Feed Fetcher	Good Bot
229	Scraper	Good Bot
235	Scraper	Good Bot
236	Scraper	Good Bot
237	Scraper	Good Bot
248	Scraper	Good Bot
250	Scraper	Good Bot
252	Scraper	Good Bot
260	Scraper	Good Bot
263	Scraper	Good Bot
265	Scraper	Good Bot
267	Scraper	Good Bot
268	Scraper	Good Bot
271	Scraper	Good Bot
272	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
276	Scraper	Good Bot
277	Scraper	Good Bot
278	Scraper	Good Bot
279	Scraper	Good Bot
280	Scraper	Good Bot
281	Scraper	Good Bot
283	Scraper	Good Bot
285	Scraper	Good Bot
286	Scraper	Good Bot
287	Scraper	Good Bot
290	Scraper	Good Bot
292	Scraper	Good Bot
293	Scraper	Good Bot
338	Scraper	Good Bot
342	Scraper	Good Bot
343	Scraper	Good Bot
344	Scraper	Good Bot
351	Scraper	Good Bot
352	Scraper	Good Bot
353	Scraper	Good Bot
355	Scraper	Good Bot
357	Scraper	Good Bot
360	Scraper	Good Bot
362	Scraper	Good Bot
366	Scraper	Good Bot
370	Scraper	Good Bot
371	Scraper	Good Bot
392	Scraper	Good Bot
393	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
394	Scraper	Good Bot
396	Scraper	Good Bot
397	Scraper	Good Bot
414	Scraper	Good Bot
418	Scraper	Good Bot
419	Scraper	Good Bot
421	Scraper	Good Bot
422	Scraper	Good Bot
423	Scraper	Good Bot
424	Scraper	Good Bot
425	Scraper	Good Bot
426	Scraper	Good Bot
427	Scraper	Good Bot
428	Scraper	Good Bot
430	Scraper	Good Bot
432	Scraper	Good Bot
433	Scraper	Good Bot
434	Scraper	Good Bot
435	Scraper	Good Bot
441	Scraper	Good Bot
445	Scraper	Good Bot
446	Scraper	Good Bot
451	Scraper	Good Bot
452	Scraper	Good Bot
454	Scraper	Good Bot
455	Scraper	Good Bot
456	Scraper	Good Bot
457	Scraper	Good Bot
458	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
461	Scraper	Good Bot
465	Scraper	Good Bot
466	Scraper	Good Bot
469	Scraper	Good Bot
473	Scraper	Good Bot
474	Scraper	Good Bot
476	Scraper	Good Bot
477	Scraper	Good Bot
484	Scraper	Good Bot
485	Scraper	Good Bot
487	Scraper	Good Bot
488	Scraper	Good Bot
489	Scraper	Good Bot
490	Scraper	Good Bot
493	Scraper	Good Bot
494	Scraper	Good Bot
495	Scraper	Good Bot
497	Scraper	Good Bot
498	Scraper	Good Bot
499	Scraper	Good Bot
500	Scraper	Good Bot
505	Scraper	Good Bot
506	Scraper	Good Bot
507	Scraper	Good Bot
512	Scraper	Good Bot
513	Scraper	Good Bot
514	Scraper	Good Bot
527	Scraper	Good Bot
533	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
539	Scraper	Good Bot
540	Scraper	Good Bot
542	Scraper	Good Bot
544	Scraper	Good Bot
545	Scraper	Good Bot
546	Scraper	Good Bot
547	Scraper	Good Bot
548	Scraper	Good Bot
551	Scraper	Good Bot
552	Scraper	Good Bot
554	Scraper	Good Bot
556	Scraper	Good Bot
558	Scraper	Good Bot
560	Scraper	Good Bot
561	Scraper	Good Bot
566	Scraper	Good Bot
575	Scraper	Good Bot
578	Scraper	Good Bot
581	Scraper	Good Bot
582	Scraper	Good Bot
591	Scraper	Good Bot
593	Scraper	Good Bot
595	Scraper	Good Bot
600	Scraper	Good Bot
601	Scraper	Good Bot
602	Scraper	Good Bot
604	Scraper	Good Bot
605	Scraper	Good Bot
609	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
610	Scraper	Good Bot
611	Scraper	Good Bot
612	Scraper	Good Bot
613	Scraper	Good Bot
615	Scraper	Good Bot
620	Suchmaschine	Good Bot
622	Suchmaschine	Good Bot
623	Suchmaschine	Good Bot
624	Suchmaschine	Good Bot
626	Suchmaschine	Good Bot
627	Suchmaschine	Good Bot
628	Suchmaschine	Good Bot
629	Suchmaschine	Good Bot
633	Suchmaschine	Good Bot
634	Suchmaschine	Good Bot
636	Suchmaschine	Good Bot
637	Suchmaschine	Good Bot
640	Suchmaschine	Good Bot
641	Suchmaschine	Good Bot
642	Suchmaschine	Good Bot
643	Suchmaschine	Good Bot
647	Suchmaschine	Good Bot
649	Suchmaschine	Good Bot
650	Suchmaschine	Good Bot
651	Suchmaschine	Good Bot
654	Suchmaschine	Good Bot
656	Suchmaschine	Good Bot
657	Suchmaschine	Good Bot
658	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
659	Suchmaschine	Good Bot
660	Suchmaschine	Good Bot
663	Suchmaschine	Good Bot
664	Suchmaschine	Good Bot
665	Suchmaschine	Good Bot
666	Suchmaschine	Good Bot
667	Suchmaschine	Good Bot
669	Suchmaschine	Good Bot
670	Suchmaschine	Good Bot
671	Suchmaschine	Good Bot
672	Suchmaschine	Good Bot
673	Suchmaschine	Good Bot
674	Suchmaschine	Good Bot
675	Suchmaschine	Good Bot
676	Suchmaschine	Good Bot
677	Suchmaschine	Good Bot
679	Suchmaschine	Good Bot
680	Suchmaschine	Good Bot
690	Suchmaschine	Good Bot
693	Suchmaschine	Good Bot
694	Suchmaschine	Good Bot
697	Suchmaschine	Good Bot
698	Suchmaschine	Good Bot
702	Suchmaschine	Good Bot
706	Suchmaschine	Good Bot
712	Suchmaschine	Good Bot
713	Suchmaschine	Good Bot
714	Suchmaschine	Good Bot
715	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
716	Suchmaschine	Good Bot
721	Suchmaschine	Good Bot
723	Suchmaschine	Good Bot
725	Suchmaschine	Good Bot
727	Suchmaschine	Good Bot
728	Suchmaschine	Good Bot
729	Suchmaschine	Good Bot
730	Suchmaschine	Good Bot
731	Suchmaschine	Good Bot
732	Suchmaschine	Good Bot
735	Suchmaschine	Good Bot
736	Suchmaschine	Good Bot
740	Suchmaschine	Good Bot
748	Suchmaschine	Good Bot
749	Suchmaschine	Good Bot
750	Suchmaschine	Good Bot
751	Suchmaschine	Good Bot
756	Suchmaschine	Good Bot
757	Suchmaschine	Good Bot
758	Suchmaschine	Good Bot
759	Suchmaschine	Good Bot
760	Suchmaschine	Good Bot
761	Suchmaschine	Good Bot
762	Suchmaschine	Good Bot
763	Suchmaschine	Good Bot
764	Suchmaschine	Good Bot
765	Suchmaschine	Good Bot
766	Suchmaschine	Good Bot
767	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
768	Suchmaschine	Good Bot
769	Suchmaschine	Good Bot
770	Suchmaschine	Good Bot
771	Suchmaschine	Good Bot
772	Suchmaschine	Good Bot
773	Suchmaschine	Good Bot
776	Suchmaschine	Good Bot
777	Suchmaschine	Good Bot
780	Suchmaschine	Good Bot
781	Suchmaschine	Good Bot
784	Suchmaschine	Good Bot
786	Suchmaschine	Good Bot
787	Suchmaschine	Good Bot
788	Suchmaschine	Good Bot
789	Suchmaschine	Good Bot
790	Suchmaschine	Good Bot
791	Suchmaschine	Good Bot
792	Suchmaschine	Good Bot
795	Suchmaschine	Good Bot
796	Suchmaschine	Good Bot
798	Suchmaschine	Good Bot
800	Suchmaschine	Good Bot
801	Suchmaschine	Good Bot
802	Suchmaschine	Good Bot
803	Suchmaschine	Good Bot
805	Suchmaschine	Good Bot
806	Suchmaschine	Good Bot
807	Suchmaschine	Good Bot
809	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
810	Suchmaschine	Good Bot
811	Suchmaschine	Good Bot
812	Suchmaschine	Good Bot
814	Suchmaschine	Good Bot
815	Suchmaschine	Good Bot
816	Suchmaschine	Good Bot
817	Suchmaschine	Good Bot
818	Suchmaschine	Good Bot
819	Suchmaschine	Good Bot
820	Suchmaschine	Good Bot
821	Suchmaschine	Good Bot
822	Suchmaschine	Good Bot
823	Suchmaschine	Good Bot
825	Suchmaschine	Good Bot
827	Suchmaschine	Good Bot
830	Suchmaschine	Good Bot
831	Suchmaschine	Good Bot
834	Suchmaschine	Good Bot
837	Suchmaschine	Good Bot
838	Suchmaschine	Good Bot
849	Sitemonitor	Good Bot
850	Sitemonitor	Good Bot
851	Sitemonitor	Good Bot
853	Sitemonitor	Good Bot
857	Sitemonitor	Good Bot
858	Sitemonitor	Good Bot
859	Sitemonitor	Good Bot
860	Sitemonitor	Good Bot
861	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
862	Sitemonitor	Good Bot
863	Sitemonitor	Good Bot
864	Sitemonitor	Good Bot
865	Sitemonitor	Good Bot
866	Sitemonitor	Good Bot
867	Sitemonitor	Good Bot
868	Sitemonitor	Good Bot
869	Sitemonitor	Good Bot
870	Sitemonitor	Good Bot
871	Sitemonitor	Good Bot
872	Sitemonitor	Good Bot
873	Sitemonitor	Good Bot
874	Sitemonitor	Good Bot
875	Sitemonitor	Good Bot
876	Sitemonitor	Good Bot
877	Sitemonitor	Good Bot
880	Sitemonitor	Good Bot
881	Sitemonitor	Good Bot
883	Sitemonitor	Good Bot
885	Sitemonitor	Good Bot
886	Sitemonitor	Good Bot
888	Sitemonitor	Good Bot
889	Sitemonitor	Good Bot
895	Sitemonitor	Good Bot
896	Sitemonitor	Good Bot
897	Sitemonitor	Good Bot
898	Sitemonitor	Good Bot
900	Sitemonitor	Good Bot
901	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
904	Sitemonitor	Good Bot
906	Sitemonitor	Good Bot
908	Sitemonitor	Good Bot
909	Sitemonitor	Good Bot
910	Sitemonitor	Good Bot
911	Sitemonitor	Good Bot
912	Sitemonitor	Good Bot
913	Sitemonitor	Good Bot
917	Sitemonitor	Good Bot
918	Sitemonitor	Good Bot
919	Sitemonitor	Good Bot
920	Sitemonitor	Good Bot
921	Sitemonitor	Good Bot
924	Sitemonitor	Good Bot
926	Sitemonitor	Good Bot
927	Sitemonitor	Good Bot
928	Sitemonitor	Good Bot
929	Sitemonitor	Good Bot
930	Sitemonitor	Good Bot
931	Sitemonitor	Good Bot
934	Sitemonitor	Good Bot
938	Sitemonitor	Good Bot
939	Sitemonitor	Good Bot
958	Sitemonitor	Good Bot
959	Sitemonitor	Good Bot
960	Sitemonitor	Good Bot
963	Sitemonitor	Good Bot
984	Scraper	Good Bot
991	Scraper	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
996	Scraper	Good Bot
997	Scraper	Good Bot
998	Scraper	Good Bot
1002	Scraper	Good Bot
1006	Scraper	Good Bot
1622	Screenshot Creator	Good Bot
2810	Crawler	Good Bot
3432	Nicht kategorisiert	Bad Bot
3783	Suchmaschine	Good Bot
3784	Scraper	Bad Bot
3788	Tool	Good Bot
3790	Crawler	Good Bot
3791	Geschwindigkeitstester	Good Bot
3792	Tool	Good Bot
3793	Tool	Good Bot
3794	Crawler	Good Bot
3796	Scraper	Good Bot
3797	Marketing	Good Bot
3799	Marketing	Good Bot
3800	Marketing	Good Bot
3806	Tool	Good Bot
3807	Crawler	Good Bot
3808	Crawler	Good Bot
3809	Tool	Good Bot
3810	Scraper	Good Bot
3811	Tool	Good Bot
3812	Crawler	Good Bot
3813	Tool	Good Bot
3814	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3815	Nicht kategorisiert	Good Bot
3817	Tool	Good Bot
3818	Tool	Good Bot
3819	Tool	Good Bot
3820	Crawler	Good Bot
3821	Suchmaschine	Good Bot
3822	Marketing	Good Bot
3823	Nicht kategorisiert	Good Bot
3831	Scraper	Good Bot
3833	Suchmaschine	Good Bot
3834	Suchmaschine	Good Bot
3835	Suchmaschine	Good Bot
3836	Nicht kategorisiert	Good Bot
3838	Nicht kategorisiert	Good Bot
3839	Marketing	Good Bot
3840	Crawler	Good Bot
3842	Crawler	Good Bot
3843	Crawler	Good Bot
3844	Marketing	Good Bot
3845	Marketing	Good Bot
3846	Marketing	Good Bot
3847	Marketing	Good Bot
3848	Nicht kategorisiert	Good Bot
3849	Crawler	Good Bot
3850	Tool	Good Bot
3851	Nicht kategorisiert	Good Bot
3852	Tool	Good Bot
3853	Vulnerability Scanner	Good Bot
3854	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3855	Crawler	Good Bot
3856	Tool	Good Bot
3871	Marketing	Good Bot
3886	Tool	Good Bot
3887	Crawler	Good Bot
3888	Crawler	Good Bot
3889	Nicht kategorisiert	Good Bot
3890	Marketing	Good Bot
3893	Crawler	Good Bot
3894	Tool	Good Bot
3895	Tool	Good Bot
3896	Suchmaschine	Good Bot
3897	Tool	Good Bot
3898	Tool	Good Bot
3899	Nicht kategorisiert	Good Bot
3901	Crawler	Good Bot
3902	Tool	Good Bot
3903	Tool	Good Bot
3904	Suchmaschine	Good Bot
3905	Suchmaschine	Good Bot
3906	Suchmaschine	Good Bot
3907	Suchmaschine	Good Bot
3912	Crawler	Good Bot
3917	Nicht kategorisiert	Good Bot
3918	Crawler	Good Bot
3919	Nicht kategorisiert	Good Bot
3920	Nicht kategorisiert	Good Bot
3921	Nicht kategorisiert	Good Bot
3922	Nicht kategorisiert	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3923	Nicht kategorisiert	Good Bot
3924	Nicht kategorisiert	Good Bot
3925	Nicht kategorisiert	Good Bot
3926	Marketing	Good Bot
3927	Marketing	Good Bot
3928	Marketing	Good Bot
3929	Tool	Good Bot
3930	Marketing	Good Bot
3931	Nicht kategorisiert	Good Bot
3932	Crawler	Good Bot
3933	Marketing	Good Bot
3934	Marketing	Good Bot
3935	Scraper	Good Bot
3936	Marketing	Good Bot
3937	Scraper	Good Bot
3938	Feed Fetcher	Good Bot
3940	Suchmaschine	Good Bot
3941	Crawler	Good Bot
3942	Scraper	Good Bot
3946	Feed Fetcher	Good Bot
3947	Crawler	Good Bot
3950	Viren-Scanner	Good Bot
3951	Marketing	Good Bot
3952	Marketing	Good Bot
3953	Marketing	Good Bot
3954	Marketing	Good Bot
3955	Marketing	Good Bot
3956	Marketing	Good Bot
3957	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3958	Marketing	Good Bot
3959	Marketing	Good Bot
3960	Marketing	Good Bot
3961	Marketing	Good Bot
3962	Marketing	Good Bot
3963	Marketing	Good Bot
3964	Marketing	Good Bot
3965	Marketing	Good Bot
3966	Marketing	Good Bot
3967	Marketing	Good Bot
3968	Marketing	Good Bot
3969	Marketing	Good Bot
3970	Suchmaschine	Good Bot
3971	Screenshot Creator	Good Bot
3972	Screenshot Creator	Good Bot
3973	Suchmaschine	Good Bot
3974	Suchmaschine	Good Bot
3975	Suchmaschine	Good Bot
3976	Suchmaschine	Good Bot
3977	Suchmaschine	Good Bot
3978	Screenshot Creator	Good Bot
3979	Suchmaschine	Good Bot
3980	Screenshot Creator	Good Bot
3981	Suchmaschine	Good Bot
3982	Suchmaschine	Good Bot
3983	Suchmaschine	Good Bot
3984	Suchmaschine	Good Bot
3985	Suchmaschine	Good Bot
3986	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3987	Screenshot Creator	Good Bot
3988	Suchmaschine	Good Bot
3989	Suchmaschine	Good Bot
3990	Suchmaschine	Good Bot
3991	Suchmaschine	Good Bot
3992	Suchmaschine	Good Bot
3993	Suchmaschine	Good Bot
3994	Suchmaschine	Good Bot
3995	Suchmaschine	Good Bot
3996	Suchmaschine	Good Bot
3997	Suchmaschine	Good Bot
3998	Suchmaschine	Good Bot
3999	Suchmaschine	Good Bot
4000	Screenshot Creator	Good Bot
4001	Suchmaschine	Good Bot
4002	Suchmaschine	Good Bot
4003	Suchmaschine	Good Bot
4004	Suchmaschine	Good Bot
4005	Screenshot Creator	Good Bot
4006	Crawler	Good Bot
4007	Marketing	Good Bot
4008	Marketing	Good Bot
4011	Tool	Good Bot
4012	Crawler	Good Bot
4013	Suchmaschine	Good Bot
4014	Tool	Good Bot
4015	Crawler	Good Bot
4016	Crawler	Good Bot
4017	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4018	Tool	Good Bot
4019	Tool	Good Bot
4020	Tool	Good Bot
4021	Marketing	Good Bot
4024	Tool	Good Bot
4025	Suchmaschine	Good Bot
4026	Suchmaschine	Good Bot
4027	Suchmaschine	Good Bot
4028	Marketing	Good Bot
4029	Tool	Good Bot
4030	Scraper	Good Bot
4031	Scraper	Good Bot
4033	Crawler	Good Bot
4034	Crawler	Good Bot
4035	Marketing	Good Bot
4036	Vulnerability Scanner	Good Bot
4037	Vulnerability Scanner	Good Bot
4038	Nicht kategorisiert	Bad Bot
4039	Tool	Good Bot
4042	Crawler	Good Bot
4043	Screenshot Creator	Good Bot
4048	Feed Fetcher	Good Bot
4050	Crawler	Good Bot
4051	Crawler	Good Bot
4052	Tool	Good Bot
4053	Tool	Good Bot
4055	Nicht kategorisiert	Good Bot
4056	Marketing	Good Bot
4057	Screenshot Creator	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4058	Crawler	Good Bot
4060	Suchmaschine	Good Bot
4061	Suchmaschine	Good Bot
4062	Suchmaschine	Good Bot
4063	Suchmaschine	Good Bot
4064	Tool	Good Bot
4065	Scraper	Good Bot
4066	Marketing	Good Bot
4067	Marketing	Good Bot
4071	Tool	Good Bot
4076	Marketing	Good Bot
4077	Scraper	Good Bot
4078	Crawler	Good Bot
4079	Crawler	Good Bot
4081	Suchmaschine	Good Bot
4082	Tool	Good Bot
4085	Tool	Good Bot
4086	Tool	Good Bot
4087	Tool	Bad Bot
4088	Suchmaschine	Good Bot
4089	Marketing	Good Bot
4090	Tool	Good Bot
4091	Tool	Good Bot
4092	Tool	Good Bot
4093	Tool	Good Bot
4094	Nicht kategorisiert	Good Bot
4095	Sitemonitor	Good Bot
4096	Sitemonitor	Good Bot
4097	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4098	Crawler	Good Bot
4099	Suchmaschine	Good Bot
4100	Suchmaschine	Good Bot
4101	Suchmaschine	Good Bot
4102	Suchmaschine	Good Bot
4103	Marketing	Good Bot
4104	Marketing	Good Bot
4105	Marketing	Good Bot
4106	Marketing	Good Bot
4109	Suchmaschine	Good Bot
4110	Crawler	Good Bot
4111	Crawler	Good Bot
4112	Crawler	Good Bot
4113	Vulnerability Scanner	Good Bot
4114	Crawler	Good Bot
4115	Tool	Good Bot
4121	Marketing	Good Bot
4126	Marketing	Good Bot
4127	Marketing	Good Bot
4128	Marketing	Good Bot
4129	Marketing	Good Bot
4130	Marketing	Good Bot
4131	Tool	Good Bot
4132	Marketing	Good Bot
4165	Marketing	Good Bot
4168	Geschwindigkeitstester	Good Bot
4170	Tool	Good Bot
4172	Crawler	Good Bot
4173	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4174	Crawler	Good Bot
4175	Crawler	Good Bot
4176	Tool	Good Bot
4177	Suchmaschine	Good Bot
4178	Tool	Good Bot
4179	Crawler	Good Bot
4180	Tool	Good Bot
4181	Sitemonitor	Good Bot
4182	Sitemonitor	Good Bot
4183	Sitemonitor	Good Bot
4184	Sitemonitor	Good Bot
4185	Suchmaschine	Good Bot
4186	Tool	Good Bot
4187	Tool	Good Bot
4188	Screenshot Creator	Good Bot
4189	Marketing	Good Bot
4190	Suchmaschine	Good Bot
4191	Suchmaschine	Good Bot
4192	Suchmaschine	Good Bot
4193	Suchmaschine	Good Bot
4194	Tool	Good Bot
4196	Tool	Good Bot
4197	Tool	Good Bot
4198	Marketing	Good Bot
4199	Marketing	Good Bot
4200	Vulnerability Scanner	Good Bot
4201	Tool	Good Bot
4202	Tool	Good Bot
4205	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4209	Suchmaschine	Good Bot
4210	Geschwindigkeitstester	Good Bot
4211	Tool	Good Bot
4212	Feed Fetcher	Good Bot
4213	Feed Fetcher	Good Bot
4215	Tool	Good Bot
4216	Tool	Good Bot
4219	Marketing	Good Bot
4220	Tool	Good Bot
4222	Sitemonitor	Good Bot
4223	Marketing	Good Bot
4224	Suchmaschine	Good Bot
4225	Suchmaschine	Good Bot
4226	Suchmaschine	Good Bot
4227	Marketing	Good Bot
4228	Marketing	Good Bot
4229	Tool	Good Bot
4231	Screenshot Creator	Good Bot
4232	Tool	Good Bot
4233	Sitemonitor	Good Bot
4236	Sitemonitor	Good Bot
4242	Marketing	Good Bot
4243	Marketing	Good Bot
4244	Marketing	Good Bot
4245	Marketing	Good Bot
4246	Marketing	Good Bot
4247	Suchmaschine	Good Bot
4252	Crawler	Good Bot
4253	Crawler	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4254	Crawler	Good Bot
4255	Tool	Good Bot
4256	Nicht kategorisiert	Good Bot
4257	Tool	Good Bot
4258	Crawler	Good Bot
4259	Crawler	Good Bot
4260	Tool	Good Bot
4261	Tool	Good Bot
4262	Tool	Good Bot
4263	Marketing	Good Bot
4265	Suchmaschine	Good Bot
4266	Nicht kategorisiert	Good Bot
4267	Tool	Good Bot
4268	Tool	Good Bot
4269	Suchmaschine	Good Bot
4270	Suchmaschine	Good Bot
4271	Suchmaschine	Good Bot
4272	Suchmaschine	Good Bot
4273	Suchmaschine	Good Bot
4274	Suchmaschine	Good Bot
4275	Suchmaschine	Good Bot
4279	Marketing	Good Bot
4280	Crawler	Good Bot
4321	Nicht kategorisiert	Good Bot
4322	Crawler	Good Bot
4323	Tool	Good Bot
4324	Tool	Good Bot
4325	Tool	Good Bot
4327	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4328	Marketing	Good Bot
4330	Sitemonitor	Good Bot
4331	Suchmaschine	Good Bot
4334	Scraper	Good Bot
4335	Marketing	Good Bot
4336	Marketing	Good Bot
4339	Tool	Good Bot
4340	Crawler	Good Bot
4341	Crawler	Good Bot
4342	Vulnerability Scanner	Good Bot
4343	Vulnerability Scanner	Good Bot
4344	Scraper	Good Bot
4377	Crawler	Good Bot
4378	Crawler	Good Bot
4379	Suchmaschine	Good Bot
4380	Suchmaschine	Good Bot
4381	Suchmaschine	Good Bot
4382	Suchmaschine	Good Bot
4383	Crawler	Good Bot
4384	Suchmaschine	Good Bot
4385	Tool	Good Bot
4386	Nicht kategorisiert	Good Bot
4387	Crawler	Good Bot
4388	Crawler	Good Bot
4389	Tool	Good Bot
4390	Tool	Good Bot
4391	Tool	Good Bot
4392	Tool	Good Bot
4393	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4394	Nicht kategorisiert	Good Bot
4395	Tool	Good Bot
4396	Sitemonitor	Good Bot
4397	Sitemonitor	Good Bot
4404	Suchmaschine	Good Bot
4405	Suchmaschine	Good Bot
4406	Suchmaschine	Good Bot
4407	Nicht kategorisiert	Good Bot

Bot-Signatur-Update für März 2022

May 11, 2023

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 12 gilt für NetScaler-Plattformen mit 13.0 76.31 oder höheren Builds.

Neue Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4564	Marketing	Good Bot
4565	Marketing	Good Bot
4566	Marketing	Good Bot
4567	Marketing	Good Bot
4568	Marketing	Good Bot
4569	Nicht kategorisiert	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4570	Nicht kategorisiert	Bad Bot
4571	Crawler	Good Bot
4572	Crawler	Good Bot
4573	Nicht kategorisiert	Bad Bot
4574	Nicht kategorisiert	Bad Bot
4575	Marketing	Good Bot
4576	Marketing	Good Bot
4577	Marketing	Good Bot
4578	Marketing	Good Bot
4579	Marketing	Good Bot
4580	Marketing	Good Bot
4581	Marketing	Good Bot
4582	Marketing	Good Bot
4583	Screenshot Creator	Good Bot
4584	Suchmaschine	Good Bot
4585	Suchmaschine	Good Bot
4586	Screenshot Creator	Good Bot
4587	Nicht kategorisiert	Good Bot
4588	Geschwindigkeitstester	Good Bot
4589	Crawler	Good Bot
4590	Tool	Good Bot
4591	Tool	Good Bot
4592	Crawler	Bad Bot
4593	Suchmaschine	Good Bot
4594	Suchmaschine	Good Bot
4595	Suchmaschine	Good Bot
4596	Marketing	Good Bot
4597	Tool	Good Bot
4598	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4599	Marketing	Good Bot
4600	Marketing	Good Bot
4601	Marketing	Good Bot
4602	Suchmaschine	Good Bot
4603	Nicht kategorisiert	Good Bot
4604	Marketing	Good Bot
4605	Marketing	Good Bot
4606	Nicht kategorisiert	Bad Bot
4607	Nicht kategorisiert	Bad Bot
4608	Tool	Good Bot
4609	Nicht kategorisiert	Bad Bot
4610	Tool	Good Bot
4611	Tool	Good Bot
4612	Scraper	Good Bot
4613	Nicht kategorisiert	Good Bot
4614	Nicht kategorisiert	Good Bot
4615	Sitemonitor	Good Bot
4616	Crawler	Good Bot
4617	Sitemonitor	Good Bot
4618	Suchmaschine	Good Bot
4619	Marketing	Good Bot
4620	Marketing	Good Bot
4621	Suchmaschine	Good Bot
4622	Crawler	Good Bot
4623	Crawler	Good Bot
4624	Crawler	Good Bot
4625	Scraper	Good Bot
4626	Crawler	Good Bot
4627	Vulnerability Scanner	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4628	Tool	Good Bot
4629	Nicht kategorisiert	Bad Bot
4630	Nicht kategorisiert	Bad Bot
4631	Tool	Good Bot
4632	Feed Fetcher	Good Bot
4633	Crawler	Bad Bot
4634	Nicht kategorisiert	Good Bot
4635	Feed Fetcher	Good Bot
4636	Nicht kategorisiert	Good Bot
4637	Tool	Good Bot
4638	Tool	Good Bot
4639	Scraper	Bad Bot
4640	Nicht kategorisiert	Bad Bot
4641	Tool	Good Bot
4642	Crawler	Bad Bot
4643	Sitemonitor	Good Bot
4644	Sitemonitor	Good Bot
4645	Suchmaschine	Good Bot
4646	Suchmaschine	Good Bot
4647	Suchmaschine	Good Bot
4648	Suchmaschine	Good Bot
4649	Suchmaschine	Bad Bot
4650	Nicht kategorisiert	Good Bot

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
2554	Nicht kategorisiert	Bad Bot
3835	Suchmaschine	Good Bot
4027	Suchmaschine	Good Bot
4038	Nicht kategorisiert	Bad Bot
4085	Tool	Good Bot
4098	Crawler	Good Bot
4100	Suchmaschine	Good Bot
4220	Tool	Good Bot
4224	Suchmaschine	Good Bot
4281	Nicht kategorisiert	Bad Bot
4412	Marketing	Good Bot
4425	Marketing	Good Bot
4429	Screenshot Creator	Good Bot
4430	Viren-Scanner	Good Bot
4483	Crawler	Good Bot
4552	Nicht kategorisiert	Good Bot
4562	Suchmaschine	Good Bot
1000000	Browser	Good Bot
1000003	Browser	Good Bot
1000004	Scraper	Good Bot
1000005	Google_Crawler	Bad Bot
1000006	Browser	Bad Bot
1000007	Bot	Bad Bot
1000008	Browser	Bad Bot
1000009	Browser	Good Bot
1000010	Bot	Bad Bot
1000011	Browser	Bad Bot
1000012	Scraper	Good Bot
1000013	Scraper	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000014	Scraper	Bad Bot
1000015	Browser	Good Bot
1000016	Bot	Bad Bot
1000017	Browser	Bad Bot
1000018	Browser	Good Bot
1000019	Scraper	Good Bot
1000020	Scraper	Good Bot
1000021	Scraper	Good Bot
1000022	Google_Crawler	Good Bot
1000023	Browser	Bad Bot
1000024	Analysator	Good Bot
1000025	Analysator	Good Bot
1000026	Analysator	Good Bot
1000027	Analysator	Good Bot
1000028	Analysator	Good Bot
1000029	Browser	Good Bot
1000030	Analysator	Good Bot
1000031	Analysator	Good Bot
1000032	Browser	Bad Bot
1000033	Analysator	Good Bot
1000034	Browser	Bad Bot
1000035	Scraper	Good Bot
1000036	Scraper	Good Bot
1000037	Browser	Good Bot
1000038	Analysator	Good Bot
1000039	Analysator	Good Bot
1000040	Analysator	Good Bot
1000041	Analysator	Good Bot
1000042	Analysator	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000043	Analysator	Good Bot
1000044	Analysator	Good Bot
1000045	Google_App_Engine_Software	Good Bot
1000046	Google_Crawler	Good Bot
1000047	Browser	Bad Bot
1000048	Browser	Bad Bot
1000049	Analysator	Good Bot
1000050	Browser	Bad Bot
1000051	Browser	Good Bot
1000052	Browser	Bad Bot
1000053	Scraper	Good Bot
1000054	Google_Crawler	Bad Bot
1000055	Scraper	Bad Bot
1000056	Analysator	Good Bot
1000057	Browser	Bad Bot
1000058	Browser	Bad Bot
1000059	Browser	Bad Bot
1000060	Scraper	Bad Bot
1000061	Anwendung	Bad Bot
1000062	Scraper	Bad Bot
1000063	Scraper	Bad Bot
1000064	Scraper	Good Bot
1000065	Scraper	Bad Bot
1000066	Scraper	Bad Bot
1000067	Browser	Bad Bot
1000068	Scraper	Bad Bot
1000069	Browser	Bad Bot
1000070	Scraper	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000071	Anwendung	Bad Bot

Bot-Signatur-Update für August 2022

May 11, 2023

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 13 gilt für NetScaler-Plattformen mit 13.0 76.31 oder höheren Builds.

Neue Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4651	Marketing	Good Bot
4652	Nicht kategorisiert	Bad Bot
4653	Suchmaschine	Good Bot
4654	Tool	Good Bot
4655	Crawler	Good Bot
4656	Marketing	Good Bot
4657	Scraper	Good Bot
4658	Feed Fetcher	Good Bot
4659	Nicht kategorisiert	Bad Bot
4660	Tool	Good Bot
4661	Tool	Good Bot
4662	Nicht kategorisiert	Bad Bot
4663	Nicht kategorisiert	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4664	Marketing	Good Bot
4665	Nicht kategorisiert	Good Bot
4666	Nicht kategorisiert	Good Bot
4667	Feed Fetcher	Good Bot
4668	Nicht kategorisiert	Good Bot
4669	Tool	Good Bot
4670	Tool	Good Bot
4671	Suchmaschine	Good Bot
4672	Tool	Good Bot
4673	Nicht kategorisiert	Good Bot
4674	Nicht kategorisiert	Good Bot
4675	Nicht kategorisiert	Good Bot
4676	Marketing	Good Bot
4677	Scraper	Good Bot
4678	Marketing	Good Bot
4679	Crawler	Bad Bot
4680	Nicht kategorisiert	Good Bot
4681	Nicht kategorisiert	Good Bot
4682	Sitemonitor	Good Bot
4683	Sitemonitor	Good Bot
4684	Suchmaschine	Good Bot
4685	Suchmaschine	Good Bot
4686	Suchmaschine	Good Bot
4687	Suchmaschine	Good Bot
4688	Suchmaschine	Good Bot
4689	Suchmaschine	Good Bot
4690	Suchmaschine	Good Bot
4691	Suchmaschine	Good Bot
4692	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4693	Nicht kategorisiert	Good Bot
4694	Nicht kategorisiert	Bad Bot
4695	Crawler	Good Bot
4696	Crawler	Good Bot
4697	Crawler	Good Bot
4698	Suchmaschine	Good Bot
4699	Suchmaschine	Good Bot
4700	Suchmaschine	Good Bot
4701	Tool	Bad Bot
4702	Nicht kategorisiert	Good Bot
4703	Tool	Good Bot
4704	Tool	Good Bot
4705	Crawler	Good Bot
4706	Sitemonitor	Good Bot
4707	Suchmaschine	Good Bot
4708	Tool	Good Bot
4709	Vulnerability Scanner	Good Bot
4710	Vulnerability Scanner	Good Bot
4711	Crawler	Good Bot
4712	Crawler	Good Bot
4713	Crawler	Good Bot
4714	Scraper	Good Bot
4715	Tool	Good Bot
4716	Tool	Good Bot
4717	Suchmaschine	Bad Bot
4718	Nicht kategorisiert	Good Bot
4719	Tool	Good Bot
4720	Marketing	Good Bot
4721	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4722	Suchmaschine	Good Bot
4723	Nicht kategorisiert	Bad Bot
4724	Tool	Good Bot
4725	Suchmaschine	Good Bot
4726	Suchmaschine	Good Bot
4727	Tool	Good Bot
4728	Nicht kategorisiert	Bad Bot
4729	Sitemonitor	Good Bot
4730	Suchmaschine	Good Bot
4731	Suchmaschine	Good Bot
4732	Suchmaschine	Good Bot
4733	Suchmaschine	Good Bot
4734	Tool	Bad Bot
4735	Tool	Bad Bot
4736	Tool	Good Bot
4737	Marketing	Good Bot
4738	Tool	Good Bot
4739	Feed Fetcher	Good Bot
4740	Suchmaschine	Good Bot
4741	Nicht kategorisiert	Bad Bot
4742	Suchmaschine	Good Bot
4743	Crawler	Good Bot
4744	Tool	Good Bot
4745	Tool	Good Bot
4746	Marketing	Good Bot
4747	Nicht kategorisiert	Bad Bot
4748	Suchmaschine	Good Bot
4749	Suchmaschine	Good Bot
4750	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4751	Suchmaschine	Good Bot
4752	Suchmaschine	Good Bot

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3796	Scraper	Good Bot
3835	Suchmaschine	Good Bot
3935	Scraper	Good Bot
4027	Suchmaschine	Good Bot
4061	Suchmaschine	Good Bot
4100	Suchmaschine	Good Bot
4451	Geschwindigkeitstester	Good Bot
4562	Suchmaschine	Good Bot
4575	Marketing	Good Bot
4577	Marketing	Good Bot
4578	Marketing	Good Bot
4579	Marketing	Good Bot
4580	Marketing	Good Bot
4583	Screenshot Creator	Good Bot
4584	Suchmaschine	Good Bot
4585	Suchmaschine	Good Bot
4597	Tool	Good Bot
4599	Marketing	Good Bot
4601	Marketing	Good Bot
4623	Crawler	Good Bot
4630	Nicht kategorisiert	Bad Bot
4647	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000000	Browser	Good Bot
1000001	Anwendung	Bad Bot
1000002	Browser	Good Bot
1000003	Scraper	Good Bot
1000004	Browser	Good Bot
1000005	Browser	Bad Bot
1000006	Google Crawler	Bad Bot
1000007	Scraper	Bad Bot
1000008	Scraper	Good Bot
1000009	Browser	Bad Bot
1000010	Bot	Bad Bot
1000011	Bot	Bad Bot
1000012	Scraper	Bad Bot
1000013	Scraper	Bad Bot
1000014	Browser	Bad Bot
1000015	Browser	Good Bot
1000016	Browser	Bad Bot
1000017	Scraper	Good Bot
1000018	Scraper	Bad Bot
1000019	Scraper	Bad Bot
1000020	Scraper	Bad Bot
1000021	Browser	Good Bot
1000022	Scraper	Good Bot
1000023	Browser	Bad Bot
1000024	Bot	Bad Bot
1000025	Analysator	Good Bot
1000026	Scraper	Good Bot
1000027	Browser	Bad Bot
1000028	Browser	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000029	Scraper	Good Bot
1000030	Google Crawler	Good Bot
1000031	Browser	Bad Bot
1000032	Analysator	Good Bot
1000033	Bot	Bad Bot
1000034	Analysator	Good Bot
1000035	Analysator	Good Bot
1000036	Analysator	Good Bot
1000037	Analysator	Good Bot
1000038	Scraper	Good Bot
1000039	Analysator	Good Bot
1000040	Browser	Bad Bot
1000041	Browser	Bad Bot
1000042	Scraper	Good Bot
1000043	Browser	Good Bot
1000044	Analysator	Good Bot
1000045	Analysator	Good Bot
1000046	Analysator	Good Bot
1000047	Analysator	Good Bot
1000048	Analysator	Good Bot
1000049	Browser	Bad Bot
1000050	Google Crawler	Good Bot
1000051	Browser	Bad Bot
1000052	Browser	Bad Bot
1000053	Analysator	Good Bot
1000054	Browser	Good Bot
1000055	Scraper	Good Bot
1000056	Browser	Good Bot
1000057	Analysator	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000058	Google Crawler	Bad Bot
1000059	Scraper	Bad Bot
1000060	Browser	Bad Bot
1000061	Browser	Good Bot
1000062	Browser	Bad Bot
1000063	Browser	Bad Bot
1000064	Browser	Bad Bot
1000065	Scraper	Bad Bot
1000066	Anwendung	Bad Bot
1000067	Scraper	Bad Bot
1000068	Scraper	Bad Bot
1000069	Browser	Good Bot
1000070	Anwendung	Bad Bot

Bot-Signatur-Update für April 2023

May 11, 2023

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 14, gültig für NetScaler-Plattformen mit 13.0 76.31 oder späteren Versionen.

Neue Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4753	Tool	Bad Bot
4754	Nicht kategorisiert	Bad Bot
4755	Scraper	Good Bot
4756	Marketing	Good Bot
4757	Marketing	Good Bot
4758	Marketing	Good Bot
4759	Marketing	Good Bot
4760	Marketing	Good Bot
4761	Marketing	Good Bot
4762	Marketing	Good Bot
4763	Marketing	Good Bot
4764	Marketing	Good Bot
4765	Scraper	Bad Bot
4766	Scraper	Bad Bot
4767	Tool	Good Bot
4768	Scraper	Bad Bot
4769	Tool	Good Bot
4770	Scraper	Bad Bot
4771	Scraper	Bad Bot
4772	Scraper	Bad Bot
4773	Scraper	Bad Bot
4774	Scraper	Bad Bot
4775	Crawler	Good Bot
4776	Marketing	Good Bot
4777	Tool	Good Bot
4778	Tool	Good Bot
4779	Crawler	Good Bot
4780	Sitemonitor	Good Bot
4781	Sitemonitor	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4782	Sitemonitor	Good Bot
4783	Nicht kategorisiert	Good Bot
4784	Tool	Good Bot
4785	Tool	Good Bot
4786	Vulnerability Scanner	Good Bot
4787	Tool	Good Bot
4788	Marketing	Good Bot
4789	Marketing	Good Bot
4790	Marketing	Good Bot
4791	Nicht kategorisiert	Good Bot
4792	Nicht kategorisiert	Good Bot
4793	Nicht kategorisiert	Bad Bot
4794	Nicht kategorisiert	Bad Bot
4795	Tool	Good Bot
4796	Sitemonitor	Good Bot
4797	Sitemonitor	Good Bot
4798	Nicht kategorisiert	Good Bot
4799	Suchmaschine	Good Bot
4800	Suchmaschine	Good Bot
4801	Suchmaschine	Good Bot
4802	Nicht kategorisiert	Good Bot
4803	Tool	Bad Bot
4804	Scraper	Good Bot
4805	Marketing	Good Bot
4806	Crawler	Good Bot
4807	Crawler	Good Bot
4808	Vulnerability Scanner	Bad Bot
4809	Vulnerability Scanner	Good Bot
4810	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4811	Tool	Good Bot
4812	Nicht kategorisiert	Good Bot
4813	Nicht kategorisiert	Good Bot
4814	Sitemonitor	Good Bot
4815	Scraper	Bad Bot
4816	Suchmaschine	Good Bot
4817	Nicht kategorisiert	Good Bot
4818	Sitemonitor	Good Bot
4819	Suchmaschine	Good Bot
4820	Suchmaschine	Good Bot
4821	Suchmaschine	Good Bot
4822	Suchmaschine	Good Bot
4823	Suchmaschine	Good Bot
4824	Nicht kategorisiert	Good Bot
4825	Marketing	Good Bot
4826	Scraper	Good Bot
4827	Screenshot Creator	Good Bot
4828	Nicht kategorisiert	Bad Bot
4829	Nicht kategorisiert	Bad Bot
4830	Nicht kategorisiert	Bad Bot
4831	Nicht kategorisiert	Good Bot
4832	Nicht kategorisiert	Bad Bot
4833	Suchmaschine	Good Bot
4834	Suchmaschine	Good Bot
4835	Nicht kategorisiert	Good Bot
4836	Suchmaschine	Good Bot
4837	Tool	Good Bot
4838	Marketing	Good Bot
4839	Tool	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4840	Scraper	Good Bot
4841	Suchmaschine	Good Bot
4842	Sitemonitor	Good Bot
4843	Nicht kategorisiert	Bad Bot
4844	Suchmaschine	Good Bot
4845	Suchmaschine	Good Bot
4846	Crawler	Good Bot
4847	Marketing	Good Bot
4848	Tool	Good Bot
4849	Crawler	Good Bot
4850	Crawler	Good Bot
4851	Nicht kategorisiert	Bad Bot
4852	Suchmaschine	Good Bot
4853	Nicht kategorisiert	Good Bot
4854	Nicht kategorisiert	Good Bot
4855	Sitemonitor	Good Bot
4856	Tool	Good Bot
4857	Tool	Good Bot
4858	Scraper	Bad Bot
4859	Screenshot Creator	Good Bot
4860	Sitemonitor	Good Bot
4861	Sitemonitor	Good Bot
4862	Crawler	Good Bot
4863	Suchmaschine	Good Bot
4864	Suchmaschine	Good Bot
4865	Suchmaschine	Good Bot
4866	Suchmaschine	Good Bot
4867	Suchmaschine	Good Bot
4868	Marketing	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4869	Marketing	Good Bot
4870	Suchmaschine	Good Bot
4871	Nicht kategorisiert	Bad Bot
4872	Nicht kategorisiert	Bad Bot
4873	Nicht kategorisiert	Bad Bot
4874	Nicht kategorisiert	Bad Bot
4875	Nicht kategorisiert	Bad Bot
4876	Nicht kategorisiert	Bad Bot
4877	Nicht kategorisiert	Bad Bot
4878	Nicht kategorisiert	Bad Bot
4879	Nicht kategorisiert	Bad Bot
4880	Nicht kategorisiert	Good Bot
4881	Suchmaschine	Good Bot
4882	Nicht kategorisiert	Good Bot
4883	Tool	Good Bot
4884	Tool	Good Bot
4885	Tool	Good Bot
4886	Sitemonitor	Good Bot
4887	Sitemonitor	Good Bot
4888	Scraper	Bad Bot
4889	Marketing	Good Bot
4890	Nicht kategorisiert	Bad Bot
4891	Suchmaschine	Good Bot
4892	Suchmaschine	Good Bot
4893	Marketing	Good Bot
4894	Nicht kategorisiert	Bad Bot
4895	Nicht kategorisiert	Bad Bot
4896	Vulnerability Scanner	Good Bot
4897	Nicht kategorisiert	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4898	Nicht kategorisiert	Bad Bot
4899	Nicht kategorisiert	Bad Bot
4900	Crawler	Good Bot
4901	Crawler	Good Bot
4902	Vulnerability Scanner	Good Bot
4903	Tool	Good Bot
4904	Feed Fetcher	Good Bot
4905	Tool	Good Bot
4906	Crawler	Good Bot
4907	Nicht kategorisiert	Good Bot
4908	Nicht kategorisiert	Bad Bot
4909	Nicht kategorisiert	Good Bot
4910	Suchmaschine	Good Bot
4911	Suchmaschine	Good Bot
4912	Nicht kategorisiert	Good Bot
4913	Suchmaschine	Good Bot
4914	Crawler	Good Bot

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
3935	Scraper	Good Bot
4012	Crawler	Good Bot
4013	Suchmaschine	Good Bot
4027	Suchmaschine	Good Bot
4038	Nicht kategorisiert	Bad Bot
4071	Tool	Good Bot
4100	Suchmaschine	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
4220	Tool	Good Bot
4425	Marketing	Good Bot
4441	Feed Fetcher	Good Bot
4451	Geschwindigkeitstester	Good Bot
4563	Suchmaschine	Good Bot
4575	Marketing	Good Bot
4577	Marketing	Good Bot
4578	Marketing	Good Bot
4579	Marketing	Good Bot
4580	Marketing	Good Bot
4583	Screenshot Creator	Good Bot
4584	Suchmaschine	Good Bot
4585	Suchmaschine	Good Bot
4586	Screenshot Creator	Good Bot
4593	Suchmaschine	Good Bot
4597	Tool	Good Bot
4599	Marketing	Good Bot
4600	Marketing	Good Bot
4601	Marketing	Good Bot
4618	Suchmaschine	Good Bot
4633	Crawler	Bad Bot
4639	Scraper	Bad Bot
4647	Suchmaschine	Good Bot
4651	Marketing	Good Bot
4660	Tool	Good Bot
4687	Suchmaschine	Good Bot
4717	Suchmaschine	Bad Bot
4730	Suchmaschine	Good Bot
1000000	Browser	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000001	Anwendung	Bad Bot
1000002	Browser	Good Bot
1000003	Scraper	Good Bot
1000004	Browser	Good Bot
1000005	Browser	Bad Bot
1000006	Google_Crawler	Bad Bot
1000007	Scraper	Bad Bot
1000008	Scraper	Good Bot
1000009	Browser	Bad Bot
1000010	Bot	Bad Bot
1000011	Bot	Bad Bot
1000012	Scraper	Bad Bot
1000013	Scraper	Bad Bot
1000014	Browser	Bad Bot
1000015	Browser	Good Bot
1000016	Browser	Bad Bot
1000017	Scraper	Good Bot
1000018	Scraper	Bad Bot
1000019	Scraper	Bad Bot
1000020	Scraper	Bad Bot
1000021	Browser	Good Bot
1000022	Scraper	Good Bot
1000023	Browser	Bad Bot
1000024	Bot	Bad Bot
1000025	Analysator	Good Bot
1000026	Scraper	Good Bot
1000027	Browser	Bad Bot
1000028	Browser	Bad Bot
1000029	Scraper	Good Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000030	Google_Crawler	Good Bot
1000031	Browser	Bad Bot
1000032	Analysator	Good Bot
1000033	Bot	Bad Bot
1000034	Analysator	Good Bot
1000035	Analysator	Good Bot
1000036	Analysator	Good Bot
1000037	Analysator	Good Bot
1000038	Scraper	Good Bot
1000039	Analysator	Good Bot
1000040	Browser	Bad Bot
1000041	Browser	Bad Bot
1000042	Scraper	Good Bot
1000043	Browser	Good Bot
1000044	Analysator	Good Bot
1000045	Analysator	Good Bot
1000046	Analysator	Good Bot
1000047	Analysator	Good Bot
1000048	Analysator	Good Bot
1000049	Browser	Bad Bot
1000050	Google_Crawler	Good Bot
1000051	Browser	Bad Bot
1000052	Browser	Bad Bot
1000053	Analysator	Good Bot
1000054	Browser	Good Bot
1000055	Scraper	Good Bot
1000056	Browser	Good Bot
1000057	Analysator	Good Bot
1000058	Google_Crawler	Bad Bot

Bot-Signatur-ID	Bot-Kategorie	Bot-Typ
1000059	Scraper	Bad Bot
1000060	Browser	Bad Bot
1000061	Browser	Good Bot
1000062	Browser	Bad Bot
1000063	Browser	Bad Bot
1000064	Browser	Bad Bot
1000065	Scraper	Bad Bot
1000066	Anwendung	Bad Bot
1000067	Scraper	Bad Bot
1000068	Scraper	Bad Bot
1000069	Browser	Good Bot
1000070	Anwendung	Bad Bot

Cacheumleitung

May 11, 2023

In einer typischen Bereitstellung fragen verschiedene Clients Webserver wiederholt nach denselben Inhalten. Um den ursprünglichen Webserver bei der Verarbeitung jeder Anfrage zu entlasten, kann eine NetScaler-Appliance mit aktivierter Cache-Umleitung diesen Inhalt von einem Cache-Server statt vom Originalserver bereitstellen.

Die NetScaler-Appliance analysiert eingehende Anfragen, sendet Anfragen für zwischenspeicherbare Daten an Cache-Server und sendet nicht zwischenspeicherbare Anfragen und dynamische HTTP-Anfragen an Originalserver.

Die Cache-Umleitung ist eine richtlinienbasierte Funktion. Standardmäßig werden Anfragen, die einer Richtlinie entsprechen, an den Ursprungsserver gesendet, und alle anderen Anfragen werden an einen Cache-Server gesendet. Zu Test- oder Wartungszwecken sollten Sie die Richtlinienauswertung überspringen und alle Anfragen an den Cache oder an den Originalserver weiterleiten.

Sie können Content Switching mit Cache-Umleitung kombinieren, um selektive Inhalte zwischenzuspeichern und Inhalte von bestimmten Cacheservern für bestimmte Arten von angeforderten Inhalten bereitzustellen.

Eine NetScaler-Appliance, die für die Cache-Umleitung konfiguriert ist, kann am Rand eines Netzwerks, vor dem Originalserver oder an einer beliebigen Stelle im Netzwerk-Backbone bereitgestellt werden. In einer Edge-Bereitstellung, die häufig von Internet Service Providern (ISPs), Kabelunternehmen, Content Delivery Distribution Networks und Unternehmensnetzwerken verwendet wird, befindet sich die NetScaler-Appliance direkt vor den Clients. Bei einer serverseitigen Bereitstellung befindet sich die NetScaler-Appliance näher an den Originalservern.

Die Cache-Umleitung wird am häufigsten mit dem HTTP-Diensttyp verwendet, unterstützt aber auch das sichere HTTPS-Protokoll.

Richtlinien zur Cache-Umleitung

May 11, 2023

Ein virtueller Cache-Umleitungsserver wendet Cache-Umleitungsrichtlinien auf jede eingehende Anfrage an. Wenn eine Anfrage mit einer der konfigurierten Richtlinien übereinstimmt, wird sie standardmäßig als nicht zwischenspeicherbar betrachtet, und die NetScaler-Appliance sendet sie an den Originalserver. Andere Anfragen werden an einen Cache-Server gesendet. Dieses Verhalten kann umgekehrt werden, sodass Anfragen, die den konfigurierten Cache-Umleitungsrichtlinien entsprechen, an Cache-Server gesendet werden.

Die Appliance bietet eine Reihe von Richtlinien für die Cache-Umleitung. Wenn diese integrierten Richtlinien für Ihre Bereitstellung nicht ausreichen, können Sie benutzerdefinierte Cache-Umleitungsrichtlinien konfigurieren.

Hinweis: Nachdem Sie festgelegt haben, welche integrierten Cache-Umleitungsrichtlinien verwendet werden sollen, oder benutzerdefinierte Richtlinien erstellt haben, fahren Sie mit der Konfiguration der Cache-Umleitung fort. Um dieses Feature verwenden zu können, müssen Sie mindestens einen virtuellen Cache-Umleitungsserver konfigurieren, und für den normalen Betrieb müssen Sie mindestens eine Cache-Umleitungsrichtlinie an diesen virtuellen Server binden.

Integrierte Cache-Umleitungsrichtlinien

May 11, 2023

Die NetScaler-Appliance bietet integrierte Cache-Umleitungsrichtlinien, die typische Cache-Anforderungen verarbeiten. Diese Richtlinien basieren auf HTTP-Methoden, den URL- oder URL-Token der eingehenden Anforderung, der HTTP-Version oder den HTTP-Headern und ihren Werten in der Anforderung.

Integrierte Cache-Umleitungsrichtlinien können direkt an einen virtuellen Server gebunden werden und benötigen keine weitere Konfiguration.

Cache-Umleitungsrichtlinien verwenden zwei Arten von Appliance-Ausdruckssprachen, klassische und erweiterte Richtlinien. Weitere Informationen zu diesen Sprachen finden Sie unter Richtlinien und Ausdrücke.

Integrierte Richtlinien zur klassischen Cache-Umleitung

Integrierte Cacheumleitungsrichtlinien, die auf klassischen Ausdrücken basieren, werden *klassische Cacheumleitungsrichtlinien*genannt. Eine vollständige Beschreibung klassischer Ausdrücke und deren Konfiguration finden Sie unter Richtlinien und Ausdrücke.

Die klassischen Cache-Umleitungsrichtlinien bewerten grundlegende Merkmale des Datenverkehrs und anderer Daten. Beispielsweise können klassische Cache-Umleitungsrichtlinien bestimmen, ob eine HTTP-Anforderung oder -Antwort einen bestimmten Typ von Header oder URL enthält.

Die NetScaler-Appliance bietet die folgenden integrierten klassischen Cache-Umleitungsrichtlinien:

Integrierter Richtlinienname	Beschreibung
bypass-non-get	Umgehen Sie den Cache, wenn die Anforderung eine andere HTTP-Methode als GET verwendet.
bypass-cache-control	Umgehen Sie den Cache, wenn der Anforderungsheader ein Cache-Control enthält: No-Cache oder Cache-Control: No-Store-Header, oder wenn die HTTP-Anforderung einen Pragma-Header enthält.
bypass-dynamic-url	Umgehen Sie den Cache, wenn die URL andeutet, dass der Inhalt dynamisch ist, was durch das Vorhandensein einer der folgenden Erweiterungen angezeigt wird: cgi, asp, exe, cfm, ex, shtml oder htx. Bypass Sie auch den Cache, wenn die URL mit einem der folgenden Schritte beginnt: /cgi-bin/, /bin/ oder /exec/.
bypass-urltokens	Umgehen Sie den Cache, da die Anforderung dynamisch ist, wie durch eines der folgenden Token in der URL angegeben:? ,! oder =.

Integrierter Richtlinienname	Beschreibung
bypass-cookie	Umgehen Sie den Cache für jede URL, die einen Cookie-Header und eine andere Erweiterung als .png oder.jpg hat.

Integrierte Richtlinien für die erweiterte Richtlinien-Cache

Integrierte Cache-Umleitungsrichtlinien, die auf erweiterten Richtlinienausdrücken basieren, werden als *erweiterte Richtlinien für die Richtlinien-* Eine vollständige Beschreibung der erweiterten Richtlinienausdrücke und deren Konfiguration finden Sie unter Richtlinien und Ausdrücke.

Zusätzlich zu den gleichen Arten von Auswertungen, die mit klassischen Cache-Umleitungsrichtlinien durchgeführt werden, können Sie mit erweiterten Richtlinien-Cache-Umleitungsrichtlinien mehr Daten analysieren (z. B. den Hauptteil einer HTTP-Anforderung) und weitere Vorgänge in der Richtlinienregel konfigurieren (z. B. Ursprungs-Server).

NetScaler-Appliances bieten die folgenden zwei integrierten Aktionen für die erweiterten Richtlinien-Cache-Umleitungsrichtlinien:

- CACHE
- ORIGIN

Wie in ihren Namen angegeben, leiten sie die Anfrage an den Cache-Server bzw. den Ursprungsserver weiter.

Hinweis: Wenn Sie die integrierte Richtlinie für die erweiterte Richtlinien-Cache-Umleitung verwenden, können Sie die Aktion nicht ändern.

Die NetScaler-Appliance bietet die folgenden integrierten erweiterten Richtlinien für die Richtlinien-Cache-Umleitung:

Integrierter Richtlinienname	Beschreibung
bypass-non-get_adv	Umgehen Sie den Cache, wenn die Anforderung eine andere HTTP-Methode als GET verwendet.
bypass-cache-control_adv	Umgehen Sie den Cache, wenn der Anforderungsheader ein Cache-Control enthält: No-Cache oder Cache-Control: No-Store-Header, oder wenn die HTTP-Anforderung einen Pragma-Header enthält.

Integrierter Richtlinienname	Beschreibung
bypass-dynamic-url_adv	Umgehen Sie den Cache, wenn die URL andeutet, dass der Inhalt dynamisch ist, was durch das Vorhandensein einer der folgenden Erweiterungen angezeigt wird: cgi, asp, exe, cfm, ex, shtml oder htx. Bypass Sie auch den Cache, wenn die URL mit einem der folgenden Schritte beginnt: /cgi-bin/, /bin/ oder /exec/.
bypass-urltokens_adv	Umgehen Sie den Cache, da die Anforderung dynamisch ist, wie durch eines der folgenden Token in der URL angegeben:? ,! oder =.
bypass-cookie_adv	Umgehen Sie den Cache für jede URL, die einen Cookie-Header und eine andere Erweiterung als .png oder.jpg hat.

Anzeigen der integrierten Cache-Umleitungsrichtlinien

Sie können die verfügbaren Cache-Umleitungsrichtlinien über die Befehlszeile oder des Konfigurationsdienstprogramms anzeigen.

Zeigen Sie die integrierten Cache-Umleitungsrichtlinien über die CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
show cr policy [<policyName>]
```

Beispiel:

```
1 > show cr policy
2 1)       Cache-By-Pass RULE: NS_NON_GET          Policy:bypass-non-get
3 2)       Cache-By-Pass RULE: (NS_CACHECONTROL_NOSTORE ||
     NS_CACHECONTROL_NOCACHE || NS_HEADER_PRAGMA)    Policy:bypass-cache-
     control
4 3)       Cache-By-Pass RULE: (NS_EXT_CGI || NS_EXT_ASP || NS_EXT_EXE ||
      NS_EXT_CFM || NS_EXT_EX || NS_EXT_SHTML || NS_EXT_HTX) || (
     NS_URL_PATH_CGIBIN || NS_URL_PATH_EXEC || NS_URL_PATH_BIN)
     Policy:bypass-dynamic-url
5 4)       Cache-By-Pass RULE: NS_URL_TOKENS       Policy:bypass-
     urltokens
6 5)       Cache-By-Pass RULE: (NS_HEADER_COOKIE && NS_EXT_NOT_GIF &&
     NS_EXT_NOT_JPEG)     Policy:bypass-cookie
```



```
 Done
<!--NeedCopy-->
```

Zeigen Sie die integrierten Cache-Umleitungsrichtlinien über die GUI an

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Richtlinien. Die konfigurierten Cache-Umleitungsrichtlinien werden im Detailbereich angezeigt.
2. Wählen Sie eine der konfigurierten Richtlinien aus, um Details anzuzeigen.

Konfigurieren einer Cache-Umleitungsrichtlinie

May 11, 2023

Eine Cache-Umleitungsrichtlinie enthält einen Ausdruck (auch *Regel*genannt). Der Ausdruck stellt eine Bedingung dar, die ausgewertet wird, wenn die Clientanforderung mit der Richtlinie verglichen wird.

Sie konfigurieren keine expliziten Aktionen für Cache-Umleitungsrichtlinien.

Eine Cache-Umleitungsrichtlinie hat einen Namen und enthält einen erweiterten Richtlinienausdruck oder eine Reihe erweiterter Richtlinienausdrucksklauseln, die mithilfe logischer Operatoren kombiniert werden, und die folgenden integrierten Aktionen:

- CACHE
- ORIGIN

Weitere Informationen zu erweiterten Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

Hinzufügen einer Cache-Umleitungsrichtlinie mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Cache-Umleitungsrichtlinie hinzuzufügen und die Konfiguration zu überprüfen:

```
-  add cr policy <policyName> \*\*-rule\*\* <expression> -action<string
   > [-logAction<string>]

-  show cr policy [<policyName>]

<!--NeedCopy-->
```

Beispiele:

Richtlinie mit einem einfachen Ausdruck:

```
> add cr policy crpol1 -rule !(HTTP.REQ.URL.ENDSWITH(".jpeg")) -action origin
 Done
> show cr policy crpoll
    Policy: crpol1 Rule: !(HTTP.REQ.URL.ENDSWITH(".jpeg")) Action: ORIGIN
    Hits: 0
 Done

<!--NeedCopy-->
```

Richtlinie mit einem zusammengesetzten Ausdruck:

```
> add cr policy crpol11 -rule 'http.req.method.eq(post) && (HTTP.REQ.URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))'  -action cache
 Done
> show cr policy crpol11
    Policy: crpol11    Rule: http.req.method.eq(post) && (HTTP.REQ.URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))  Action: CACHE
    Hits: 0
 Done

<!--NeedCopy-->
```

Richtlinie, die einen Header auswertet:

```
> add cr policy crpol12 -rule http.req.header("If-Modified-Since").exists -action origin
 Done
> show cr policy crpol12
    Policy: crpol12    Rule: http.req.header("If-Modified-Since").exists   Action: ORIGIN
    Hits: 0
 Done

<!--NeedCopy-->
```


Ändern oder entfernen Sie eine Cache-Umleitungsrichtlinie über die CLI

- Um eine Cache-Umleitungsrichtlinie zu ändern, verwenden Sie den Befehl set cr policy, der genau dem Befehl add cr policy entspricht, mit der Ausnahme, dass Sie den Namen einer vorhandenen Richtlinie eingeben und nur die Parameter angeben müssen, die Sie ändern möchten.
- Um eine Richtlinie zu entfernen, verwenden Sie den `rm cr policy`-Befehl, der nur das Argument <name> akzeptiert. Wenn die Richtlinie an einen virtuellen Server gebunden ist, müssen Sie die Bindung aufheben, bevor Sie sie entfernen können.

Weitere Informationen zum Aufheben der Bindung einer Cache-Umleitungsrichtlinie finden Sie unter Aufheben der Bindung einer Richtlinie von einem virtuellen Cache-Umleitungsserver.

Konfigurieren einer Cache-Umleitungsrichtlinie mit einem einfachen Ausdruck mit der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Cache-Umleitungsrichtlinie erstellen** in das Textfeld **Name** den Namen der Richtlinie ein.
4. Wählen Sie in der Dropdownliste **Aktion** die entsprechende Aktion **CACHE** oder **ORIGIN** aus.
5. Klicken Sie im Bereich **Protokollieraktion** auf **Hinzufügen**. Geben Sie in das Dialogfeld **Aktion für Überwachungsnachricht erstellen** einen Namen ein.
    - Konfigurieren Sie die **Protokollebene**, indem Sie den entsprechenden Wert aus der Dropdownliste auswählen:
        - **EMERGENCY**
        - **ALERT**
        - **CRITICAL**
        - **ERROR**
        - **WARNING**
        - **NOTICE**
        - **INFORMATIONAL**
        - **DEBUG**
    - Geben Sie den Ausdruck im Bereich **Ausdruck** ein.
        - Ausdruckstyp-Allgemein
        - Flow Type -REQ
        - Protocol -HTTP
        - Qualifier -URL

- Operator - !=
- Wert - /.jpeg

- Klicken Sie auf **Erstellen**.

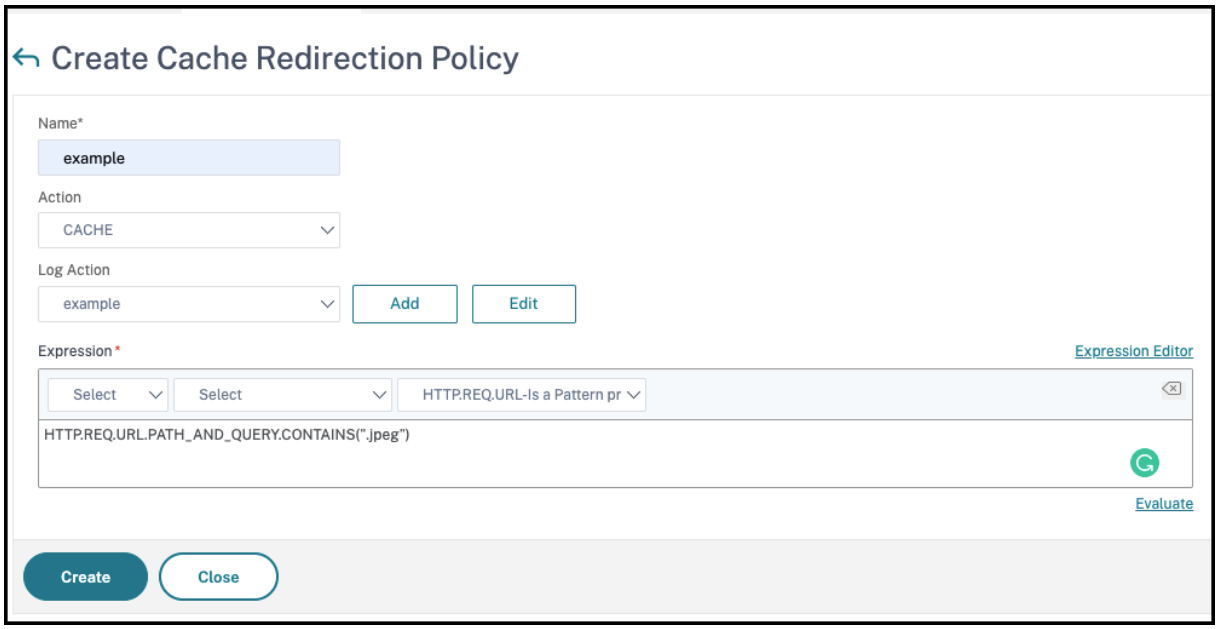
6. Um einen einfachen Ausdruck zu konfigurieren, geben Sie den Ausdruck ein. Es folgt ein Beispiel für einen Ausdruck, der in einer URL nach einer `.jpeg` Erweiterung sucht:

   - Ausdruckstyp-Allgemein
   - Flow Type -REQ
   - Protocol -HTTP
   - Qualifier -URL
   - Operator - !=
   - Wert - /.jpeg

   Der einfache Ausdruck im folgenden Beispiel prüft in einer Anfrage nach einem If-Modified-Since-Header:

   - Expression Type -General
   - Flow Type -REQ
   - Protocol -HTTP
   - Qualifier -HEADER
   - Operator -EXISTS
   - Header-Name -If-Modified-Since

7. Wenn Sie mit der Eingabe des Ausdrucks fertig sind, klicken Sie auf **Erstellen**.



Konfigurieren einer Cache-Umleitungsrichtlinie mit einem zusammengesetzten Ausdruck über die GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie in das Textfeld **Name** einen Namen für die Richtlinie ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrichsymbol beginnen und aus einem bis 127 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), bei (@), gleich (=) und Unterstrichen (_) bestehen. Sie sollten einen Namen wählen, der es anderen erleichtert, festzustellen, für welche Art von Inhalt diese Richtlinie erstellt wurde.
4. Wählen Sie in der Dropdownliste **Aktion** die entsprechende Aktion **CACHE** oder **ORIGIN** aus.
5. Klicken Sie im Bereich **Protokollieraktion** auf **Hinzufügen**. Geben Sie in das Dialogfeld **Aktion für Überwachungsnachricht erstellen** einen Namen ein.
   - Konfigurieren Sie die **Protokollebene**, indem Sie den entsprechenden Wert aus der Dropdownliste auswählen:
     - **EMERGENCY**
     - **ALERT**
     - **CRITICAL**
     - **ERROR**
     - **WARNING**
     - **NOTICE**
     - **INFORMATIONAL**
     - **DEBUG**
   - Geben Sie den Ausdruck im Bereich **Ausdruck** ein.
     - Ausdruckstyp-Allgemein
     - Flow Type -REQ
     - Protocol -HTTP
     - Qualifier -URL
     - Operator - !=
     - Wert - /.jpeg
   - Klicken Sie auf **Erstellen**.
6. Wählen Sie den Typ des zusammengesetzten Ausdrucks aus, den Sie erstellen möchten. Ihre Auswahlmöglichkeiten:
   - **Entsprechen Sie einem beliebigen Ausdruck**. Die Richtlinie stimmt mit dem Verkehr überein, wenn ein oder mehrere einzelne Ausdrücke mit dem Verkehr übereinstimmen.

- **Entspricht allen Ausdrücken**. Die Richtlinie stimmt nur dann mit dem Verkehr überein, wenn jeder einzelne Ausdruck mit dem Verkehr übereinstimmt.
- **Tabellarische Ausdrücke**. Schaltet die Liste Ausdrücke in ein tabellarisches Format mit drei Spalten um. In der Spalte ganz rechts platzieren Sie einen der folgenden Operatoren:
  - Der AND [&&] -Operator verlangt, dass eine Anfrage sowohl dem aktuellen Ausdruck als auch dem folgenden Ausdruck entspricht, um der Richtlinie zu entsprechen.
  - Der OR [||] -Operator verlangt, dass eine Anfrage entweder dem aktuellen Ausdruck oder dem folgenden Ausdruck oder beidem entspricht, um der Richtlinie zu entsprechen. Nur wenn die Anforderung nicht mit einem Ausdruck übereinstimmt, stimmt sie nicht mit der Richtlinie überein.

  Sie können Ausdrücke auch in verschachtelten Untergruppen gruppieren, indem Sie einen vorhandenen Ausdruck auswählen und auf einen der folgenden Operatoren klicken:

  - Der Operator BEGIN SUBGROUP [+ (], der die NetScaler-Appliance anweist, eine verschachtelte Untergruppe mit dem ausgewählten Ausdruck zu beginnen. (Um diesen Operator aus dem Ausdruck zu entfernen, klicken Sie auf - (.)
  - Der END SUBGROUP [+)] -Operator, der die NetScaler-Appliance anweist, die aktuelle verschachtelte Untergruppe mit dem ausgewählten Ausdruck zu beenden. (Um diesen Operator aus dem Ausdruck zu entfernen, klicken Sie auf -).)
- **Fortgeschrittene Freiform**. Schaltet den Ausdruckseditor vollständig aus und verwandelt die Ausdrucksliste in einen Textbereich, in den Sie einen zusammengesetzten Ausdruck eingeben können. Dies ist sowohl die leistungsstärkste als auch die schwierigste Methode zum Erstellen eines Richtlinienausdrucks und wird nur für diejenigen empfohlen, die mit der klassischen NetScaler Ausdruckssprache vertraut sind.

  Weitere Informationen zum Erstellen klassischer Ausdrücke im Textbereich Erweiterte Freiform finden Sie unter Konfigurieren klassischer Richtlinien und Ausdrücke.

  Achtung: Wenn Sie in den Bearbeitungsmodus für erweiterte Freiformausdrücke wechseln, können Sie nicht zu einem der anderen Modi zurückkehren. Wählen Sie diesen Ausdrucksbearbeitungsmodus nicht, es sei denn, Sie sind sicher, dass Sie ihn verwenden möchten.

7. Wenn Sie “Beliebiger Ausdruck anpassen”, “Alle Ausdrücke abgleichen” oder “Tabellarische Ausdrücke” gewählt haben, klicken Sie auf **Hinzufügen**, um das Dialogfeld Ausdruck hinzufügen anzuzeigen.

   Sie sollten den Ausdruckstyp für Cache-Umleitungsrichtlinien auf Allgemein festgelegt lassen.

8. Wählen Sie in der Dropdownliste Flow-Typ einen Flow-Typ für Ihren Ausdruck aus.

   Der Flusstyp bestimmt, ob die Richtlinie eingehende oder ausgehende Verbindungen untersucht. Sie haben zwei Möglichkeiten:

- **REQ**. Konfiguriert die NetScaler-Appliance für die Überprüfung eingehender Verbindungen oder Anfragen.
- **RES**. Konfiguriert die Appliance so, dass ausgehende Verbindungen oder Antworten untersucht werden.

9. Wählen Sie in der Dropdownliste Protokoll ein Protokoll für Ihren Ausdruck aus.

   Das Protokoll bestimmt die Art der Informationen, die die Richtlinie in der Anfrage oder Antwort untersucht. Je nachdem, ob Sie in der vorherigen Dropdownliste REQ oder RES gewählt haben, sind entweder alle vier oder nur drei der folgenden Optionen verfügbar:

   - **HTTP**. Konfiguriert die Appliance, um den HTTP-Header zu untersuchen.
   - **SSL**. Konfiguriert die Appliance für die Prüfung des SSL-Clientzertifikats. Nur verfügbar, wenn Sie REQ (Anfragen) in der vorherigen Dropdownliste gewählt haben.
   - **TCP**. Konfiguriert die Appliance für die Untersuchung des TCP-Headers.
   - **IP**. Konfiguriert die Appliance für die Überprüfung der Quell- oder Ziel-IP-Adresse.

10. Wählen Sie in der Dropdownliste Qualifier einen Qualifier für Ihren Ausdruck aus.

    Der Inhalt der Dropdownliste Qualifier hängt davon ab, welches Protokoll Sie gewählt haben. In der folgenden Tabelle werden die für jedes Protokoll verfügbaren Wahlmöglichkeiten beschrieben.

    Tabelle 1. Cache-Umleitungsrichtlinien-Qualifikatoren für jedes Protokoll verfügbar

Protokoll	Qualifier	Definition
HTTP	METHOD	In der Anforderung verwendete HTTP-Methode.
-	URL	Inhalt des URL-Headers.
-	URLTOKENS	URL-Token im HTTP-Header.
-	VERSION	HTTP-Version der Verbindung.
-	HEADER	Header-Teil der HTTP-Anforderung.
-	URLLEN	Länge des Inhalts des URL-Headers.
-	URLQUERY	Fragen Sie einen Teil des Inhalts des URL-Headers ab.
-	URLQUERYLEN	Länge des Abfrageabschnitts des URL-Headers.

Protokoll	Qualifier	Definition
SSL	CLIENT.CERT	SSL-Clientzertifikat als Ganzes.
-	CLIENT.CERT.SUBJECT	Inhalt des Felds Betreff des Client-Zertifikats.
-	CLIENT.CERT.ISSUER	Aussteller des Clientzertifikats.
-	CLIENT.CERT.SIGALGO	Im Clientzertifikat verwendeter Signaturalgorithmus.
-	CLIENT.CERT.VERSION	Version des Client-Zertifikats.
-	CLIENT.CERT.VALIDFROM	Datum, ab dem das Clientzertifikat gültig ist. (Das Startdatum.)
-	CLIENT.CERT.GÜLTIG FÜR	Datum, nach dem das Clientzertifikat nicht mehr gültig ist. (Das Enddatum.)
-	CLIENT.CERT.SERIALNUMBER	Seriennummer des Clientzertifikats.
-	CLIENT.CIPHER.TYPE	Im Clientzertifikat verwendete Verschlüsselungsmethode.
-	CLIENT.CIPHER.BITS	Anzahl signifikanter Bits im Verschlüsselungsschlüssel.
-	CLIENT.SSL.VERSION	SSL-Version des Clientzertifikats.
TCP	SOURCEPORT	Quellport der TCP-Verbindung.
-	DESTPORT	Zielport der TCP-Verbindung.
-	MSS	Maximale Segmentgröße (MSS) der TCP-Verbindung.
IP	SOURCEIP	Quell-IP-Adresse der Verbindung.

Protokoll	Qualifier	Definition
-	DESTIP	Ziel-IP-Adresse der Verbindung.

11. Wählen Sie den Operator für Ihren Ausdruck aus der Dropdownliste Operator aus.

    Ihre Wahl hängt von der Qualifikation ab, die Sie im vorherigen Schritt gewählt haben. Die vollständige Liste der Operatoren, die in dieser Dropdownliste erscheinen können, lautet:

    - == . Entspricht exakt der folgenden Textzeichenfolge.
    - != . Entspricht nicht der folgenden Textzeichenfolge.
      - . Ist größer als die folgende Ganzzahl.
    - CONTAINS . Enthält die folgende Textzeichenfolge.
    - CONTENTS . Der Inhalt der angegebenen Header-, URL- oder URL-Abfrage.
    - EXISTS . Der angegebene Header oder die angegebene Abfrage ist vorhanden.
    - NOTCONTAINS . Enthält nicht die folgende Textzeichenfolge.
    - NOTEXISTS . Der angegebene Header oder die angegebene Abfrage existiert nicht.

    Wenn Sie möchten, dass diese Richtlinie für Anfragen funktioniert, die an einen bestimmten Host gesendet werden, können Sie das Standardzeichen Gleichheitszeichen (==) beibehalten.

12. Wenn das Textfeld Wert sichtbar ist, geben Sie die entsprechende Zeichenfolge oder Zahl in das Textfeld ein.

    Wenn Sie beispielsweise möchten, dass diese Richtlinie Anforderungen auswählt, die an den Host shopping.example.com gesendet werden, geben Sie diese Zeichenfolge in das Textfeld Wert ein.

13. Wenn Sie HEADER als Qualifizierer gewählt haben, geben Sie die gewünschte Kopfzeile in das Textfeld Header-Name ein.
14. Klicken Sie auf **OK**, um Ihren Ausdruck zur Liste Ausdruck hinzuzufügen.
15. Wiederholen Sie die Schritte 4 bis 11, um weitere Ausdrücke zu erstellen.
16. Klicken Sie auf **Schließen**, um das Dialogfeld Ausdruck hinzufügen zu schließen und zum Dialogfeld **Cache-Umleitungsrichtlinie erstellen** zurückzukehren.
17. Wenn Sie mit der Eingabe des Ausdrucks fertig sind, klicken Sie auf **Erstellen**.

Konfigurationen für Cache-Umleitung

May 11, 2023

Abhängig von Ihrer Bereitstellung und Netzwerktopologie können Sie eine der folgenden Arten der Cache-Umleitung konfigurieren:

- **Durchsichtig** Ein transparenter Cache kann sich an verschiedenen Punkten entlang eines Netzwerk-Backbones befinden, um den Datenverkehr entlang der Lieferroute zu verringern. Im transparenten Modus fängt der virtuelle Cache-Umleitungsserver den gesamten Datenverkehr ab, der zur NetScaler-Appliance fließt, und wendet Cache-Umleitungsrichtlinien an, um zu bestimmen, ob Inhalte aus dem Cache oder vom Originalserver bereitgestellt werden sollen.
- **Proxy weiterleiten**. Ein Forward-Proxy-Cache-Server befindet sich am Rand eines Unternehmens-LAN und ist dem WAN zugewandt. Im Forward-Proxymodus löst der virtuelle Cache-Umleitungsserver den Hostnamen der eingehenden Anfrage mithilfe eines DNS-Servers auf und leitet Anfragen für Inhalte, die nicht zwischengespeichert werden können, an die aufgelösten Ursprungsserver weiter. Cachefähige Anfragen werden an die konfigurierten Cache-Server gesendet.
- **Reverse-Proxy**. Reverse-Proxy-Caches werden für bestimmte Ursprungsserver konfiguriert. Eingehender Datenverkehr, der an den Reverse-Proxy geleitet wird, kann entweder von einem Cache-Server bereitgestellt oder mit oder ohne Änderung der URL an den Ursprungsserver gesendet werden.

Konfigurieren der transparenten Umleitung

May 11, 2023

Wenn Sie die transparente Cache-Umleitung konfigurieren, wertet die NetScaler-Appliance den gesamten empfangenen Datenverkehr aus, um festzustellen, ob er zwischengespeichert werden kann. Dieser Modus reduziert den Datenverkehr entlang der Lieferroute und wird häufig verwendet, wenn sich der Cache-Server auf dem Backbone eines ISP oder Carriers befindet.

Standardmäßig werden zwischenspeicherbare Anfragen an einen Cache-Server und nicht zwischenspeicherbare Anfragen an den Ursprungsserver gesendet. Wenn die NetScaler-Appliance beispielsweise eine Anfrage empfängt, die an einen Webserver gerichtet ist, vergleicht sie die HTTP-Header in der Anfrage mit einer Reihe von Richtlinienausdrücken. Wenn die Anfrage nicht mit der Richtlinie übereinstimmt, leitet die Appliance die Anfrage an einen Cache-Server weiter. Wenn die Anforderung einer Richtlinie entspricht, leitet die Appliance die Anforderung unverändert an den Webserver weiter.

Weitere Informationen zum Ändern dieses Standardverhaltens finden Sie unter Direkte Richtlinientreffer auf den Cache anstelle des Ursprungs.

Um die transparente Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung und den Lastausgleich und konfigurieren Sie den Edge-Modus. Erstellen Sie dann einen virtuellen Cache-Umleitungsserver mit einer Wildcard-IP-Adresse (*), sodass dieser virtuelle Server über jede IP-Adresse, die die Appliance besitzt, Datenverkehr empfangen kann, der an die Appliance gesendet wird. Binden Sie an diesen virtuellen Server Richtlinien für die Cache-Umleitung, die die Arten von Anfragen beschreiben, die nicht zwischengespeichert werden sollten. Erstellen Sie dann einen virtuellen Lastausgleichsserver, der Datenverkehr vom virtuellen Cache-Umleitungsserver für zwischenspeicherbare Anfragen empfängt. Erstellen Sie schließlich einen Dienst, der einen physischen Cacheserver darstellt, und binden Sie ihn an den virtuellen Lastausgleichsserver.

Cache-Umleitung und Load Balancing aktivieren

October 8, 2021

Die Funktionen der Appliance-Cache-Umleitung und der Lastausgleich sind standardmäßig nicht aktiviert. Sie müssen aktiviert werden, bevor eine Konfiguration der Cache-Umleitung wirksam werden kann.

Aktivieren Sie die Cache-Umleitung und den Lastausgleich über die CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Cache-Umleitung und den Lastausgleich zu aktivieren und die Einstellungen zu überprüfen:


```
-  enable ns feature cr lb
-  show ns feature
<!--NeedCopy-->
```

Beispiel:

```
> enable ns feature cr lb
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   ON
 3)     Load Balancing                  LB                   ON
 4)     Content Switching               CS                   ON
 5)     Cache Redirection               CR                   ON
            ...
            ...
            ...

 23)    appliance Push                  push                 OFF
 Done
<!--NeedCopy-->
```

Aktivieren Sie die Cache-Umleitung und den Lastausgleich über die GUI

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Um die Cache-Umleitung zu aktivieren, klicken Sie im Detailbereich unter **Modi und Funktionen** auf **Erweiterte Funktionen konfigurieren**.
   a) Aktivieren Sie im Dialogfeld **Erweiterte Funktionen konfigurieren** das Kontrollkästchen neben der **Cache-Umleitung**, und klicken Sie dann auf **OK**.
   b) Im Dialogfeld “Funktionen aktivieren/deaktivieren?” klicken Sie auf Ja.
3. Um den Lastenausgleich zu aktivieren, klicken Sie im Detailbereich unter **Modi und Funktionen** auf **Grundfunktionen konfigurieren**.
   a) Aktivieren Sie im Dialogfeld **Grundfunktionen konfigurieren** das Kontrollkästchen neben dem Load Balancing, und klicken Sie dann auf **OK**.
   b) Im Dialogfeld “Funktionen aktivieren/deaktivieren?” klicken Sie auf Ja.

Edge-Modus konfigurieren

May 11, 2023

Bei der Bereitstellung am Rand eines Netzwerks lernt die NetScaler-Appliance dynamisch über die Server in diesem Netzwerk. Im Edge-Modus kann die Appliance dynamisch über bis zu 40.000 HTTP-Server und Proxy-TCP-Verbindungen für diese Server lernen.

Dieser Modus aktiviert die Erfassung von Statistiken für die dynamisch erlernten Dienste und wird in der Regel in transparenten Bereitstellungen für die Cache-Umleitung verwendet.

Aktivieren Sie den Edge-Modus mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den Edge-Modus zu aktivieren und die Einstellung zu überprüfen:

```
-  enable ns mode Edge
-  show ns mode
<!--NeedCopy-->
```

Beispiel:

```
> enable ns mode edge
 Done

> show ns mode

        Mode                          Acronym             Status
        -------                       -------             ------
          ...
          ...
          ...
 6)     MAC-based forwarding          MBF                 ON
 7)     Edge configuration            Edge                ON
 8)     Use Subnet IP                 USNIP               OFF
          ...
          ...
          ...
 16)    Bridge BPDUs                  BridgeBPDUs         OFF
 Done
<!--NeedCopy-->
```


Aktivieren Sie den Edge-Modus mithilfe der GUI

1. Erweitern Sie im Navigationsbereich System, und klicken Sie dann auf Einstellungen.
2. Klicken Sie im Detailbereich unter Modi und Funktionenauf Modi konfigurieren.
3. Aktivieren Sie im Dialogfeld Modi konfigurieren das Kontrollkästchen neben der Edge-Konfiguration, und klicken Sie dann auf OK.
4. In Funktion (en) aktivieren/deaktivieren? auf Ja.

Konfigurieren eines virtuellen Cache-Umleitungsservers

August 19, 2021

Standardmäßig leitet ein virtueller Cache-Umleitungsserver zwischenspeicherbare Anforderungen an den virtuellen Lastausgleichsserver für den Cache weiter und leitet nicht zwischenspeicherbare Anforderungen an den Ursprungsserver weiter (außer in einer Reverseproxy-Konfiguration, bei der nicht zwischenspeicherbare Anforderungen an einen virtuellen Lastenausgleichsserver gesendet werden). Es gibt drei Arten von virtuellen Cache-Umleitungsservern: transparent, Forward-Proxy und Reverse-Proxy.

Ein virtueller Server zur Cache-Umleitung verwendet eine IP-Adresse von * und eine Portnummer (in der Regel 80), die HTTP-Datenverkehr akzeptieren kann, der an jede IP-Adresse gesendet wird, die die Appliance repräsentiert. Daher können Sie nur einen virtuellen Server für die transparente Cache-Umleitung konfigurieren. Alle zusätzlichen virtuellen Cache-Umleitungsserver, die Sie konfigurieren, müssen Forward-Proxy- oder Reverse-Proxyumleitungsserver sein.

Hinzufügen eines virtuellen Cache-Umleitungsservers im transparenten Modus mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Cache-Umleitungsserver hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add cr vserver <name> <serviceType> [<IPAddress> <port> ] [-
     cacheType <cacheType>] [-redirect <redirect>]
2 -  show cr vserver [<name>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 add cr vserver Vserver-CRD-1 HTTP * 80 -cacheType TRANSPARENT -redirect
      POLICY
2 > show cr vserver Vserver-CRD-1
3         Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
```



```
4          State: UP  ARP:DISABLED
5          Client Idle Timeout: 180 sec
6          Down state flush: ENABLED
7          Disable Primary Vserver On Down : DISABLED
8          Default:        Content Precedence: RULE        Cache:
               TRANSPARENT
9          On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
10         Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
11  Done
12 <!--NeedCopy-->
```

Ändern oder Entfernen eines virtuellen Cache-Umleitungsservers mit der CLI

- Um einen virtuellen Server zu ändern, verwenden Sie den Befehl set cr vserver, der genauso aussieht wie mit dem Befehl add cr vserver, außer dass Sie den Namen eines vorhandenen virtuellen Servers eingeben.
- Um einen virtuellen Server zu entfernen, verwenden Sie den Befehl `rm cr vserver`, der nur das <name> Argument akzeptiert.

Hinzufügen eines virtuellen Cache-Umleitungsservers im transparenten Modus mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Cache-Umleitung) Werte für die folgenden Parameter an:
   - Name*—Name
   - Anschluss* — Anschluss

   * Ein erforderlicher Parameter
4. Wählen Sie in der Dropdownliste Protokoll ein unterstütztes Protokoll aus (z. B. **HTTP**). Wenn der virtuelle Server Datenverkehr an einem anderen Port als dem Standardport für das ausgewählte Protokoll empfangen soll, geben Sie einen neuen Wert in das Feld Port ein.
5. Klicken Sie auf die Registerkarte Erweitert.
6. Stellen Sie sicher, dass Cachetyp auf TRANSPARENT und Redirect auf POLICY festgelegt ist.
7. Klicken Sie auf Erstellenund dann auf Schließen. Im Bereich Cache-Umleitung Virtuelle Server wird der neue virtuelle Server angezeigt.

8. Wählen Sie den neuen virtuellen Cache-Umleitungsserver aus, um die Details seiner Konfiguration anzuzeigen.

Binden von Richtlinien an den virtuellen Cache-Umleitungsserver

January 19, 2021

Cache-Umleitungsrichtlinien werden nicht automatisch an den virtuellen Cache-Umleitungsserver gebunden. Ein richtlinienbasierter virtueller Cache-Umleitungsserver kann nur funktionieren, wenn Sie mindestens eine Richtlinie an ihn binden.

Binden von Richtlinien an einen virtuellen Cache-Umleitungsserver mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  bind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
> bind cr vserver Vserver-CRD-1 -policyName bypass-cache-control
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-dynamic-url
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-urltokens
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-cookie
 Done

> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: bypass-dynamic-url
```



```
3)      Cache bypass  Policy: bypass-urltokens
4)      Cache bypass  Policy: bypass-cookie
 Done
<!--NeedCopy-->
```

Binden einer benutzerdefinierten Richtlinie an einen virtuellen Cache-Umleitungsserver mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Klicken Sie auf den virtuellen Server, den Sie konfigurieren möchten, und klicken Sie auf Öffnen.
3. Wählen Sie auf der Registerkarte Richtlinien den Typ der Richtlinie aus, und klicken Sie dann auf Richtlinie einfügen.
4. Wählen Sie unter der Spalte Richtlinienname die Richtlinie aus, die Sie binden möchten.
5. Klicken Sie auf OK.

Aufheben der Bindung einer Richtlinie von einem virtuellen Cache-Umleitungsserver

May 11, 2023

Wenn Sie eine Richtlinie vom virtuellen Cache-Umleitungsserver trennen, wendet die NetScaler-Appliance die Richtlinie bei der Auswertung von Clientanforderungen nicht mehr an.

Entbinden Sie eine Richtlinie mit dem Befehl CLI von einem virtuellen Cache-Umleitungsserver

Geben Sie in der Befehlszeile Folgendes ein:

```
-  unbind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
unbind cr vserver Vserver-CR-1 -policyName bypass-non-get
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
```



```
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
 Done
<!--NeedCopy-->
```

Entbinden Sie eine benutzerdefinierte Richtlinie mithilfe der GUI von einem virtuellen Cache-Umleitungsserver

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Klicken Sie auf den virtuellen Server, den Sie konfigurieren möchten, und klicken Sie dann auf Öffnen.
3. Wählen Sie auf der Registerkarte Richtlinien unter Richtlinienname die Richtlinie aus, deren Bindung Sie aufheben möchten.
4. Klicken Sie auf Richtlinie aufheben, und klicken Sie dann auf OK.

Erstellen eines virtuellen Lastausgleichsservers

May 11, 2023

Der virtuelle Cache-Umleitungsserver auf der NetScaler-Appliance kann Anfragen entweder an eine Cache-Serverfarm senden, wenn die Anfrage zwischenspeicherbar ist, oder an die Original-Serverfarm, wenn die Anfrage nicht zwischenspeicherbar ist.

Jeder Cacheserver wird auf der Appliance durch einen Dienst dargestellt, der an einen virtuellen Lastausgleichsserver gebunden ist, der Anforderungen vom virtuellen Cache-Umleitungsserver empfängt und diese Anforderungen an die Server weiterleitet.

Weitere Informationen zum Konfigurieren von virtuellen Lastenausgleichs-Servern und anderen Konfigurationsoptionen finden Sie unter Load Balancing.

Erstellen eines virtuellen Lastausgleichsservers mit der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen virtuellen Lastausgleichsserver zu erstellen und die Konfiguration zu überprüfen:

```
-  add lb vserver <name> <serviceType> [<IPAddress>] [<port>]
```



```
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
> add lb vserver Vserver-LB-CR HTTP 10.102.20.30 80
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:00:08.470
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
 Done
<!--NeedCopy-->
```

Erstellen Sie mithilfe der GUI einen virtuellen Lastausgleichsserver

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an, wie hier gezeigt:

   - Name*-Name
   - IP-Adresse*- IP-Adresse
   - Hafen*-Anschluss

   * Ein erforderlicher Parameter
4. Wählen Sie in der Protokollliste ein unterstütztes Protokoll aus (z. B. **HTTP**). Wenn der virtuelle Server Datenverkehr an einem anderen Port als dem bekannten Port für das ausgewählte Protokoll empfangen soll, geben Sie einen neuen Wert in das Feld Port ein.

5. Klicken Sie auf Erstellenund dann auf Schließen. Im Bereich Load Balancing Virtual Servers wird der neue virtuelle Server angezeigt.

Konfigurieren eines HTTP-Dienstes

May 11, 2023

Auf der NetScaler-Appliance stellt ein Dienst einen physischen Server im Netzwerk dar. In der Konfiguration der transparenten Cache-Umleitung stellt der Dienst den Cache-Server dar. Cachefähige Anfragen werden vom virtuellen Cache-Umleitungsserver an den virtuellen Load-Balancing-Server gesendet, der wiederum jede Anfrage an den richtigen Dienst weiterleitet, der sie an den Cache-Server weiterleitet.

Konfigurieren Sie einen HTTP-Dienst mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen HTTP-Dienst zu erstellen und die Konfiguration zu überprüfen:

```
-  add service <name> <IP> <serviceType> <port> -cacheType <cacheType>
-  show service [<name>]
<!--NeedCopy-->
```

Beispiel:

```
> add service Service-HTTP-1 10.102.29.40 HTTP 80 -cacheType
   TRANSPARENT
 Done
> show service Service-HTTP-1
        Service-HTTP-1 (10.102.29.40:80) - HTTP
        State: DOWN
        Last state change was at Fri Jul  2 09:14:17 2010
        Time since last state change: 0 days, 00:00:13.820
        Server Name: 10.102.29.40
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): YES
        Idle timeout: Client: 180 sec   Server: 360 sec
        Client IP: DISABLED
```



```
18          Cache Type: TRANSPARENT Redirect Mode:
19          Cacheable: NO
20          SC: OFF
21          SP: ON
22          Down state flush: ENABLED
23
24  1)      Monitor Name: tcp-default
25                  State: DOWN     Weight: 1
26                  Probes: 3       Failed [Total: 3 Current: 3]
27                  Last response: Failure - Time out during TCP connection
                        establishment stage
28                  Response Time: N/A
29   Done
30  <!--NeedCopy-->
```

Ändern oder entfernen Sie einen Dienst über die CLI

- Um einen Dienst zu ändern, verwenden Sie den Befehl set service. Dies entspricht genau dem Befehl add service, außer dass Sie den Namen eines vorhandenen Dienstes eingeben.
- Um einen Dienst zu entfernen, verwenden Sie den Befehl `rm service`, der nur das <name>-Argument akzeptiert.

Fügen Sie über die GUI einen HTTP-Dienst hinzu

1. Navigieren Sie zu Traffic Management > Load Balancing > Services
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Service erstellen Werte für die folgenden Parameter an, wie hier gezeigt:
   - Dienstname* — Name
   - Server*—IP
   - Hafen* — Port

   * Ein erforderlicher Parameter
4. Wählen Sie in der Dropdownliste Protokoll* ein unterstütztes Protokoll aus (z. B. **HTTP**).
5. Klicken Sie auf Erstellenund dann auf Schließen.

Binden/Entbinden eines Dienstes/eines virtuellen Lastenausgleichsservers

August 19, 2021

Sie müssen einen Dienst an den virtuellen Lastausgleichsserver binden. Dadurch kann der Load Balancer die Anforderung an den Server weiterleiten, den der Dienst darstellt. Wenn sich Ihre Konfiguration ändert, können Sie die Bindung eines Diensts vom virtuellen Lastausgleichsserver aufheben.

Binden eines Dienstes an einen virtuellen Lastausgleichsserver mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
> bind lb vserver vserver-LB-CR service-HTTP-1
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:42:25.610
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
<!--NeedCopy-->
```


Aufheben der Bindung eines Dienstes von einem virtuellen Lastausgleichsserver mit der CLI

Um die Bindung eines Dienstes aufzuheben, verwenden Sie den Befehl `unbind lb vserver` anstelle von `bind lb vserver`.

Binden/Entbinden eines Dienstes von einem virtuellen Lastausgleichsserver mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server
2. Wählen Sie im Detailbereich den virtuellen Server aus, von dem Sie den Dienst binden/aufheben möchten, und klicken Sie dann auf Öffnen.
3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte Dienste in der Spalte Aktiv das Kontrollkästchen neben dem Dienstnamen.
4. Klicken Sie auf OK.

Deaktivieren der Einstellung “Proxy-Port verwenden” für transparentes Caching

May 11, 2023

Wenn die Option Quell-IP (USIP) für einen auf der NetScaler-Appliance konfigurierten Cache-Dienst deaktiviert ist, leitet die Appliance Client-Anforderungen an den Cache-Dienst weiter, indem sie eine geräteeigene Subnetz-IP-Adresse (SNIP) oder eine zugeordnete IP-Adresse (MIP) als Quell-IP-Adresse und einen zufälligen Port als Quellport verwendet. Der zufällig ausgewählte Port wird als Proxy-Port bezeichnet.

Wenn Sie jedoch einen vollständig transparenten Cache konfigurieren möchten (eine Cache-Konfiguration, bei der der Cache-Dienst die IP-Adresse und Portnummer des Clients empfängt), müssen Sie nicht nur die USIP-Option entweder global oder auf dem Cache-Dienst aktivieren, sondern auch die Einstellung Proxyport verwenden deaktivieren, entweder global oder im Cache-Dienst. Wenn Sie die Einstellung Proxy-Port verwenden deaktivieren, kann die Appliance den Quellport des Clients als Quellport verwenden, wenn sie eine Verbindung mit dem Cache-Dienst herstellt, und stellt eine vollständig transparente Cachekonfiguration sicher.

Weitere Informationen zum Konfigurieren der Option Proxyport verwenden global oder für einen Dienst finden Sie unter Konfigurieren des Quellports für serverseitige Verbindungen.

Weisen Sie der NetScaler-Appliance einen Portbereich zu

May 11, 2023

Die gemeinsame Nutzung der Client-IP-Adresse kann zu einem Konflikt führen, der dazu führt, dass Netzwerkgeräte wie Router, Cache-Server, Ursprungsserver und andere NetScaler-Appliances nicht in der Lage sind, die Appliance und damit den Client zu bestimmen, an den die Antwort gesendet werden soll.

Eine Methode zur Lösung dieses Problems besteht darin, der NetScaler-Appliance einen Quellportbereich zuzuweisen. Diese Zuteilung ermöglicht es Netzwerkgeräten, die NetScaler-Appliance, die die Anfrage gesendet hat, eindeutig zu identifizieren.

Weisen Sie einer NetScaler-Appliance mithilfe der CLI einen Quellportbereich zu

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns param -crPortRange <startPortNumber-endPortNumber>
```

Weisen Sie einer NetScaler-Appliance mithilfe der Appliance-GUI einen Quellportbereich zu

1. Klicken Sie im Navigationsbereich auf Systemund dann auf Einstellungen.
2. Klicken Sie in der Gruppe Einstellungen auf den Link Globale Systemeinstellungen ändern.
3. Geben Sie in der Gruppe Cache-Umleitungs-Portbereich den Portbereich für die Appliance an, indem Sie eine Portnummer für Startport und eine Portnummer für Endport eingeben.
4. Klicken Sie auf OK.

Aktivieren des Lastausgleichs virtueller Server, um Anfragen in den Cache umzuleiten

May 11, 2023

Wenn ein virtueller Lastausgleichsserver so konfiguriert ist, dass er eine bestimmte Kombination aus IP-Adresse und Port abhört, hat er Vorrang vor dem virtuellen Cache-Umleitungsserver für alle Anfragen, die für diese Kombination aus Adresse und Port bestimmt sind. Daher verarbeitet der virtuelle Cache-Umleitungsserver diese Anfragen nicht.

Wenn Sie diese Funktion außer Kraft setzen und den virtuellen Cache-Umleitungsserver entscheiden lassen möchten, ob die Anforderung aus dem Cache bedient werden soll oder nicht, konfigurieren Sie den jeweiligen virtuellen Lastausgleichsserver so, dass er zwischengespeichert werden kann.

Eine solche Konfiguration wird normalerweise verwendet, wenn ein ISP eine NetScaler-Appliance am Rand seines Netzwerks verwendet und der gesamte Datenverkehr durch die Appliance fließt.

Aktivieren Sie virtuelle Load-Balancing-Server, um Anfragen mithilfe der CLI an den Cache umzuleiten

Geben Sie in der Befehlszeile Folgendes ein:

```
-  set lb vserver <name> [-cacheable ( YES | NO)]
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-CR  - cacheable YES
> show lb vserver vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 01:05:51.510
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Cacheable: YES  PQ: OFF SC: OFF
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
<!--NeedCopy-->
```

Für eine transparente Cache-Umleitung fängt die Appliance den gesamten Datenverkehr ab und wertet jede Anfrage aus, um festzustellen, ob sie zwischengespeichert werden kann. Anfragen, die nicht zwischengespeichert werden können, werden unverändert an den Ursprungsserver gesendet.

Wenn Sie die transparente Cache-Umleitung verwenden, sollten Sie die Cache-Umleitung für virtuelle

Server, die den Datenverkehr immer an die Originalserver weiterleiten, für den Lastenausgleich deaktivieren.

Deaktivieren Sie das Caching für einen virtuellen Lastausgleichsserver mithilfe der CLI

Um das Caching für eine virtuelle Load-Balancing-Maschine zu deaktivieren, verwenden Sie den Befehl unset lb vserver anstelle von set lb vserver. Geben Sie den Wert KEIN Wert für den **zwischenspeicherbaren** Parameter an.

Aktivieren oder deaktivieren Sie virtuelle Load-Balancing-Server, um Anfragen mithilfe der GUI an den Cache umzuleiten

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, auf dem Sie das Caching aktivieren/deaktivieren möchten, und klicken Sie dann auf Öffnen.
3. Aktivieren/deaktivieren Sie auf der Registerkarte Erweitert das Kontrollkästchen Cache-Umleitung.
4. Klicken Sie auf OK.

Konfigurieren der Forward-Proxyumleitung

May 11, 2023

Ein Forward-Proxy ist eine zentrale Anlaufstelle für einen Kunden oder eine Gruppe von Kunden. In dieser Konfiguration leitet die NetScaler-Appliance Anfragen, die nicht zwischengespeichert werden können, an einen Ursprungsserver und zwischenspeicherbare Anfragen entweder an einen Forward-Proxycache oder an einen transparenten Cache weiter.

Wenn die Appliance als Forward-Proxy konfiguriert ist, müssen Benutzer ihre Browser so ändern, dass der Browser Anfragen an den Forward-Proxy und nicht an die Zielserver sendet.

Ein virtueller Forward-Proxy-Cache-Umleitungsserver auf der Appliance vergleicht die Anfrage mit einer Richtlinie für das Caching. Wenn die Anfrage nicht zwischenspeicherbar ist, fragt die Appliance einen virtuellen DNS-Lastausgleichsserver zur Auflösung des Ziels ab und sendet die Anfrage dann an den Ursprungsserver. Wenn die Anfrage zwischenspeicherbar ist, leitet die Appliance die Anfrage an einen virtuellen Lastausgleichsserver für den Cache weiter.

Die Appliance stützt sich auf einen Hostdomänennamen oder eine IP-Adresse im HOST-Header der Anfrage, um das angeforderte Ziel zu ermitteln. Wenn die Anfrage keinen HOST-Header enthält, fügt die Appliance einen HOST-Header ein, der auf der Ziel-IP-Adresse in der Anfrage basiert.

In der Regel fungiert die NetScaler-Appliance als Forward-Proxy in einem Unternehmens-LAN. In einer solchen Konfiguration befindet sich die Appliance am Rand eines Unternehmens-LAN und fängt Client-Anfragen ab, bevor sie an das WAN weitergeleitet werden. Durch die Konfiguration der Appliance im Forward-Proxy-Modus wird der Datenverkehr im WAN reduziert.

Um die Forward-Proxy-Cache-Umleitung zu konfigurieren, aktivieren Sie zunächst den Lastenausgleich und die Cache-Umleitung auf der Appliance. Konfigurieren Sie dann einen virtuellen DNS-Lastausgleichsserver und die zugehörigen Dienste. Konfigurieren Sie außerdem einen virtuellen Lastausgleichsserver und binden Sie an ihn die entsprechenden Dienste für den Cache. Konfigurieren Sie einen virtuellen Server für die Forward-Proxycache-Umleitung und binden Sie die virtuellen DNS- und Load-Balancing-Server daran. Sie müssen auch Caching-Richtlinien konfigurieren und sie an den virtuellen Cache-Umleitungsserver binden. Um das Setup abzuschließen, konfigurieren Sie die Client-Browser so, dass der Forward-Proxy verwendet wird.

Weitere Informationen zum Aktivieren der Cache-Umleitung und des Lastausgleichs auf der Appliance finden Sie unter Aktivieren der Cache-Umleitung und des Lastausgleichs.

Weitere Informationen zum Erstellen eines virtuellen Lastausgleichsservers finden Sie unter Erstellen eines virtuellen Lastausgleichsservers.

Weitere Informationen zur Konfiguration von Diensten, die den Cache-Server darstellen, finden Sie unter Konfigurieren eines HTTP-Dienstes.

Weitere Informationen zum Binden des Dienstes an einen virtuellen Server finden Sie unter Binden/Aufheben eines Dienstes an/von einem virtuellen Lastausgleichsserver.

Weitere Informationen zum Erstellen eines Forward-Proxy-Cache-Umleitungsservers finden Sie unter Konfigurieren eines virtuellen Cache-Umleitungsserversund Erstellen eines virtuellen Servers vom Typ TRANSPARENT oder FORWARD.

Weitere Informationen zum Binden von Cache-Umleitungsrichtlinien an den virtuellen Cache-Umleitungsserver finden Sie unter Konfigurieren einer Cache-Umleitungsrichtlinie.

Erstellen eines DNS-Diensts

May 11, 2023

Ein DNS-Dienst ist eine Darstellung eines physischen DNS-Servers im Netzwerk auf der NetScaler-Appliance. Ein virtueller DNS-Lastausgleichsserver sendet über einen solchen Dienst DNS-Anfragen an den DNS-Server im Netzwerk.

Erstellen Sie einen DNS-Dienst mithilfe der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um einen DNS-Dienst zu erstellen und die Konfiguration zu überprüfen:

```
-  add service <name> <IP> <serviceType> <port>
-  show service [<name>]
<!--NeedCopy-->
```

Beispiel:

```
add service Service-DNS-1 10.102.29.41 DNS 53
show service Service-DNS-1
        Service-DNS-1 (10.102.29.41:53) - DNS
        State: DOWN
        Last state change was at Fri Jul  2 10:14:32 2010
        Time since last state change: 0 days, 00:00:13.550
        Server Name: 10.102.29.41
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping-default
                State: DOWN     Weight: 1
                Probes: 3       Failed [Total: 3 Current: 3]
                Last response: Failure - Probe timed out.
                Response Time: 2000.0 millisec
 Done
<!--NeedCopy-->
```

Fügen Sie mithilfe der GUI einen DNS-Dienst hinzu

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.

3. Geben Sie im Dialogfeld Service erstellen Werte für die folgenden Parameter an, wie hier gezeigt:
    - Dienstname* — Name
    - Server* — IP
    - Hafen* — Port

* Ein erforderlicher Parameter

1. Wählen Sie in der Dropdownliste Protokoll* ein unterstütztes Protokoll aus (z. B. **DNS**).
2. Klicken Sie auf Erstellenund dann auf Schließen.

Erstellen eines virtuellen DNS-Lastausgleichsservers

August 19, 2021

Der virtuelle DNS-Server ermöglicht es dem Forward-Proxy, die DNS-Auflösung durchzuführen, bevor eine Clientanforderung an einen Ursprungsserver weitergeleitet wird. Der virtuelle DNS-Lastausgleichsserver ist dem DNS-Dienst zugeordnet, der den physischen DNS-Server im Netzwerk darstellt.

Erstellen eines virtuellen DNS-Lastausgleichsservers mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um einen virtuellen DNS-Lastausgleichsserver zu erstellen und die Konfiguration zu überprüfen:

```
-  add lb vserver <name> <serviceType>
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
> add lb vserver Vserver-DNS-1 DNS
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:00:08.10
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
```



```
13          Configured Method: LEASTCONNECTION
14          Mode: IP
15          Persistence: NONE
16  Done
17 <!--NeedCopy-->
```

Erstellen eines virtuellen DNS-Lastausgleichsservers mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) im Feld Name einen Namen für den virtuellen Server ein.
4. Wählen Sie in der Dropdownliste Protokoll* ein unterstütztes Protokoll (z. B. **DNS**) aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Im Bereich Virtuelle DNS-Server wird der neue virtuelle Server angezeigt.

Binden des DNS-Diensts an den virtuellen Server

August 19, 2021

Damit der DNS-Server auf DNS-Anforderungen antwortet, muss der Dienst, der den DNS-Server darstellt, an den virtuellen DNS-Server gebunden sein.

Binden Sie den DNS-Dienst an den virtuellen Lastausgleichsserver mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den DNS-Dienst an den virtuellen Lastausgleichsserver zu binden und die Konfiguration zu überprüfen:

```
1 -  bind lb vserver <name> <serviceName>
2 -  show lb vserver <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > bind lb vserver Vserver-DNS-1 Service-DNS-1
2  Done
3 > show lb vserver Vserver-DNS-1
4         Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
5         State: DOWN
6         Last state change was at Fri Jul  2 10:32:28 2010
7         Time since last state change: 0 days, 00:12:16.80
```



```
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE

1) Service-DNS-1 (10.102.29.41: 53) - DNS State: DOWN   Weight: 1
 Done
>
<!--NeedCopy-->
```

Entbinden eines DNS-Dienstes vom virtuellen Lastausgleichsserver mit der CLI

Verwenden Sie den`unbind lb vserver` Befehl anstelle von`bind lb vserver` .

Binden/Entbinden eines DNS-Dienstes eines virtuellen Lastausgleichsservers mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server
2. Wählen Sie im Detailbereich den virtuellen Server aus, an den Sie den DNS-Dienst binden/aufheben möchten, und klicken Sie dann auf Öffnen.
3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte Dienste in der Spalte Aktiv das Kontrollkästchen neben dem Dienstnamen.
4. Klicken Sie auf OK.

Konfigurieren eines Clientwebbrowsers für die Verwendung eines Forward-Proxy

May 11, 2023

Wenn Sie die NetScaler-Appliance als virtuellen Server für die Forward-Proxy-Cache-Umleitung im Netzwerk konfigurieren, müssen Sie den Client-Webbrowser so konfigurieren, dass er Anfragen an den Forward-Proxy sendet. Wenn Sie einen Forward-Proxy verwenden, erfolgt die einzige Route zu den Servern im Netzwerk normalerweise über den Forward-Proxy.

Informationen zur Konfiguration des Browsers für die Verwendung eines Forward-Proxys finden Sie in der Dokumentation Ihres Browsers. Geben Sie die IP-Adresse und die Portnummer des virtuellen

Forward-Proxy-Cache-Umleitungsservers für diese Konfiguration an.

Konfigurieren der Reverse-Proxyumleitung

March 2, 2023

Ein Reverse-Proxy befindet sich vor einem oder mehreren Webservern und schirmt den Ursprungsserver vor Clientanfragen ab. Oft ist ein Reverse-Proxy-Cache ein Frontend für alle Client-Anfragen an einen Server. Ein Administrator weist einem bestimmten Ursprungsserver einen Reverse-Proxy-Cache zu. Der Reverse-Proxy-Cache ist anders als transparente Proxy-Caches und Forward-Proxy-Caches, die häufig angeforderten Inhalte für alle Anfragen an einen Ursprungsserver zwischenspeichern, und die Wahl eines Servers basiert auf der Anforderung.

Im Gegensatz zu einem transparenten Proxy-Cache verfügt der Reverse-Proxy-Cache über eine eigene IP-Adresse und kann Zieldomänen und URLs in einer nicht zwischenspeicherbaren Anforderung durch neue Zieldomänen und URLs ersetzen.

Sie können die Reverse-Proxy-Cache-Umleitung auf der Seite des Originalservers oder am Rand eines Netzwerks bereitstellen. Bei der Bereitstellung auf dem Originalserver ist der virtuelle Reverse-Proxy-Cache-Umleitungsserver ein Frontend für alle Anfragen an den Originalserver.

Wenn die Appliance im Reverse-Proxy-Modus eine Anfrage empfängt, wertet der virtuelle Server für die Cache-Umleitung die Anfrage aus und leitet sie entweder an einen virtuellen Lastausgleichsserver für den Cache oder an einen virtuellen Lastausgleichsserver für den Ursprung weiter. Die eingehende Anfrage kann transformiert werden, indem der Host-Header oder die Host-URL geändert werden, bevor sie an den Backend-Server gesendet wird.

Um die Reverse-Proxy-Cache-Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung und den Lastausgleich. Konfigurieren Sie dann einen virtuellen Lastausgleichsserver und Dienste, um zwischenspeicherbare Anfragen an die Cache-Server zu senden. Konfigurieren Sie außerdem einen virtuellen Lastausgleichsserver und die zugehörigen Dienste für die Originalserver. Konfigurieren Sie dann einen virtuellen Server für die Reverse-Proxy-Cache-Umleitung und binden Sie die entsprechenden Cache-Umleitungsrichtlinien daran. Konfigurieren Sie abschließend die Zuordnungsrichtlinien und binden Sie sie an den virtuellen Server für die Reverse-Proxy-Cache-Umleitung.

Den Zuordnungsrichtlinien ist eine Aktion zugeordnet, die es dem virtuellen Cache-Umleitungsserver ermöglicht, alle nicht zwischenspeicherbaren Anforderungen an den virtuellen Lastausgleichsserver für den Ursprung weiterzuleiten.

Stellen Sie sicher, dass Sie das Standard-Cacheserver-Ziel erstellen.

Weitere Informationen zum Aktivieren der Cache-Umleitung und des Lastausgleichs auf der Appliance finden Sie unter Aktivieren der Cache-Umleitung und des Lastausgleichs.

Weitere Informationen zum Erstellen eines virtuellen Lastausgleichsservers finden Sie unter Erstellen eines virtuellen Lastausgleichsservers.

Weitere Informationen zur Konfiguration von Diensten, die den Cache-Server darstellen, finden Sie unter Konfigurieren eines HTTP-Dienstes.

Weitere Informationen zum Binden des Dienstes an einen virtuellen Server finden Sie unter Binden/Aufheben eines Dienstes an/von einem virtuellen Lastausgleichsserver.

Weitere Informationen zum Erstellen eines Reverse-Proxy-Cache-Umleitungsservers finden Sie unter Konfigurieren eines virtuellen Cache-Umleitungsserversund Erstellen eines virtuellen Servers vom Typ REVERSE.

Weitere Informationen zum Binden integrierter Cache-Umleitungsrichtlinien an den virtuellen Cache-Umleitungsserver finden Sie unter Binden von Richtlinien an den virtuellen Cache-Umleitungsserver.

Konfigurieren von Zuordnungsrichtlinien

Wenn eine eingehende Anfrage nicht zwischengespeichert werden kann, ersetzt der virtuelle Server für die Reverse-Proxy-Cache-Umleitung die Domäne und URL in der Anfrage durch die Domäne und URL eines Ziel-Ursprungsservers und leitet die Anfrage an den virtuellen Loadbalancing-Server für den Ursprung weiter.

Eine Zuordnungsrichtlinie ermöglicht es dem virtuellen Server mit Reverse-Proxy-Cache-Umleitung, die Zieldomäne und die URL zu ersetzen und die Anfrage an den virtuellen Load-Balancing-Server für den Ursprung weiterzuleiten.

Eine Zuordnungsrichtlinie muss zuerst die Domain und die URL übersetzen und dann die Anfrage an den virtuellen Ursprungsserver für den Lastausgleich weiterleiten.

Eine Zuordnungsrichtlinie kann eine Domain, ein URL-Präfix und ein URL-Suffix wie folgt zuordnen:

- Domainzuordnung: Sie können eine Domain ohne Präfix oder Suffix zuordnen. Die Domainzuordnung ist die Standardzuordnung für den virtuellen Server (z. B. die Zuordnung von www.mycompany.com zu www.myrealcompany.com).
- Präfixzuordnung: Sie können ein bestimmtes Muster mit einem Präfix als Teil der URL ersetzen (z. B. indem Sie www.mycompany.com/sports/index.html zu www.mycompany.com/news/index.html zuordnen).
- Suffixzuordnung: Sie können das Dateisuffix in der URL ersetzen (z. B. indem Sie www.mycompany.com/spor zu www.mycompany.com/sports/index.asp zuordnen).

Die Quell- und Zielzeichenfolgen, die zugeordnet werden, müssen ähnlich sein. Wenn Sie eine Quelldomäne angeben, müssen Sie eine Zieldomäne angeben, und wenn Sie ein Quellsuffix angeben, müssen Sie ein Zielsuffix angeben. In ähnlicher Weise muss die Ziel-URL auch eine exakte URL sein, wenn Sie eine genaue URL aus der Quelle angeben.

Nachdem Sie die Zuordnungsrichtlinien für den Reverse-Proxy-Modus konfiguriert haben, müssen Sie sie an den virtuellen Cache-Umleitungsserver binden.

Sie können Kombinationen aus Quell-URL, Ziel-URL sowie Quell- und Zieldomänen verwenden, um alle drei Arten der Domainzuordnung zu konfigurieren.

Konfigurieren Sie eine Zuordnungsrichtlinie für den Reverse-Proxy-Modus mithilfe der CLI

Geben Sie an der Befehlszeile den folgenden Befehl ein, um eine Policy-Map hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <
     string>] [-tu <string>]
2 -  show policy map [<mapPolicyName>]
3 <!--NeedCopy-->
```

Beispiel:

Der folgende Befehl ordnet eine Domäne in einer Client-Anfrage einer Zieldomäne zu:

```
1 > add policy map myMappingPolicy -sd www.mycompany.com -td www.
     myrealcompany.com
2  Done
3 > show policy map myMappingPolicy
4 1)      Name: myMappingPolicy
5         Source Domain: www.mycompany.com        Source Url:
6         Target Domain: www.myrealcompany.com    Target Url:
7  Done
8 <!--NeedCopy-->
```

Im Folgenden finden Sie ein Beispiel für die Zuordnung eines URL-Suffixes zu einem anderen URL-Suffix:

```
1 > add policy map myOtherMappingPolicy -sd www.mycompany.com -td www.
     myrealcompany.com -su /news.html -tu /realnews.html
2  Done
3 > show policy map myOtherMappingPolicy
4 1)      Name: myOtherMappingPolicy
5         Source Domain: www.mycompany.com        Source Url: /news.html
6         Target Domain: www.myrealcompany.com    Target Url: /realnews.
             html
7  Done
8 <!--NeedCopy-->
```


Konfigurieren Sie eine Zuordnungsrichtlinie für den Reverse-Proxy-Modus mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Zuordnungsrichtlinien**.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld “Kartenrichtlinie erstellen” Werte für die folgenden Parameter an, wie hier gezeigt:
   - Name*- mapPolicyName
   - Source Domain*-sd
   - Target Domain*-td
   - Source URL-su
   - Target URL-tu

   * Ein erforderlicher Parameter
4. Klicken Sie auf Erstellen und dann auf Schließen. Im Kartenbereich wird die neue Zuordnungsrichtlinie angezeigt.

Binden Sie die Zuordnungsrichtlinie mithilfe der CLI an den virtuellen Cache-Umleitungsserver

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Zuordnungsrichtlinie an den virtuellen Cache-Umleitungsserver zu binden und die Konfiguration zu überprüfen:

```
-  bind cr vserver <name> -policyName <string> [<targetVserver>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> bind cr vserver Vserver-CRD-3 -policyName myMappingPolicy Vserver-LB-
   CR
 Done
> show cr vserver Vserver-CRD-3
        Vserver-CRD-3 (10.102.29.50:88) - HTTP  Type: CONTENT
        State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default: Vserver-LB-CR  Content Precedence: RULE        Cache:
           REVERSE
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

```



```
1)      Policy:         Target: Vserver-LB-CR   Priority: 0     Hits: 0
1)      Map: myMappingPolicy Target: Vserver-LB-CR
 Done
<!--NeedCopy-->
```

Binden Sie die Zuordnungsrichtlinie mithilfe der GUI an den virtuellen Cache-Umleitungsserver

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, von dem Sie die Zuordnungsrichtlinie binden möchten, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Konfigurieren des virtuellen Servers**(Cache-Umleitung) auf der Registerkarte **Richtlinien** die Option **Zuordnung**aus, und klicken Sie dann auf **Richtlinie einfügen**.
4. Wählen Sie in der Spalte **Richtlinienname** die Richtlinie aus der Dropdownliste aus.
5. Klicken Sie in der Spalte **Ziel** auf den Abwärtspfeil, und wählen Sie dann den virtuellen Server aus der Dropdownliste aus.
6. Klicken Sie auf **OK**.

Selektive Cache-Umleitung

May 11, 2023

Die selektive Cache-Umleitung sendet Anfragen für bestimmte Inhaltstypen, z. B. Bilder, an einen Cache-Server oder eine Gruppe von Cache-Servern und sendet andere Inhaltstypen an einen anderen Cache-Server oder eine Gruppe von Cache-Servern. Sie können die erweiterte Cache-Umleitung in den Modi Transparent, Reverse-Proxy oder Forward-Proxy konfigurieren.

Bei der selektiven Cache-Umleitung fängt die NetScaler-Appliance eine Client-Anfrage ab und leitet Anfragen, die nicht zwischengespeichert werden können, an das ursprüngliche Ziel in der Client-Anfrage weiter. Bei zwischenspeicherbaren Anfragen sendet die Appliance die Anfragen an den Ziel-Cacheserver, der Inhalte eines bestimmten Inhaltstyps bereitstellen kann.

Bei der selektiven Cache-Umleitung müssen zusätzlich zu den Richtlinien für die Cache-Umleitung auch Richtlinien für den Inhaltswechsel konfiguriert werden. Die Appliance wertet zunächst die Cache-Umleitungsrichtlinien aus, die an den virtuellen Cache-Umleitungsserver gebunden sind. Wenn eine Anforderung einer Cache-Umleitungsrichtlinie entspricht, sendet der virtuelle Cache-Umleitungsserver die Anforderung an den Ursprungsserver oder einen virtuellen Lastausgleichsserver für den Ursprung. Wenn keine Cache-Umleitungsrichtlinien der Anfrage entsprechen, wertet die Appliance die Inhaltswechselrichtlinien aus, die an den virtuellen Cache-Umleitungsserver gebunden sind. Wenn eine Inhaltswechselrichtlinie der Anforderung entspricht, leitet der virtuelle

Server für die Cache-Umleitung die Anforderung an einen virtuellen Lastausgleichsserver für den Cache weiter.

Um die selektive Cache-Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung, den Lastenausgleich und den Content Switching auf der NetScaler-Appliance. Konfigurieren Sie dann einen virtuellen Lastausgleichsserver für den Cache und einen zugehörigen HTTP-Dienst. Konfigurieren Sie anschließend einen virtuellen Cache-Umleitungsserver und binden Sie sowohl die Cache-Umleitungs- als auch die Content-Switching-Richtlinien daran. Sobald Sie die Richtlinien gebunden haben, können Sie den virtuellen Server so konfigurieren, dass er entweder regelbasierten oder URL-basierten Richtlinien für den Inhaltswechsel Vorrang einräumt.

Wenn die Appliance für die Cache-Umleitung im transparenten Modus in einer Edge-Bereitstellungstopologie konfiguriert ist, sendet sie den gesamten zwischenspeicherbaren HTTP-Verkehr an eine transparente Cache-Farm. Clients greifen über die Appliance auf das Internet zu, die als Layer-4-Switch konfiguriert ist, der Datenverkehr auf Port 80 empfängt.

Die Appliance kann Anfragen für Bilder (z. B. GIF- und JPG-Dateien) an einen Server in der transparenten Cache-Farm und alle anderen Anfragen für statische Inhalte an andere Server in der Farm weiterleiten. Für diese Konfiguration konfigurieren Sie Richtlinien für den Content Switching, um Bilder an den Image-Cache und alle anderen zwischenspeicherbaren Inhalte an einen Standardcache zu senden.

Hinweis: Die hier beschriebene Konfiguration dient der transparenten selektiven Cache-Umleitung. Daher ist kein virtueller Lastausgleichsserver für den Ursprung erforderlich, wie dies bei einer Reverse-Proxy-Konfiguration der Fall wäre.

Um diese Art der selektiven Cache-Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung, den Lastenausgleich und den Content Switching. Konfigurieren Sie dann einen virtuellen Lastausgleichsserver für den Cache und konfigurieren Sie einen zugehörigen HTTP-Dienst. Konfigurieren Sie dann einen virtuellen Cache-Umleitungsserver und erstellen und binden Sie sowohl Cache-Umleitung als auch Content Switching-Richtlinien an diesen virtuellen Server.

Weitere Informationen zum Aktivieren der Cache-Umleitung und des Lastausgleichs auf der Appliance finden Sie unter Aktivieren der Cache-Umleitung und des Lastausgleichs.

Content Switching aktivieren

October 8, 2021

Um die selektive Cache-Umleitung zu konfigurieren, müssen Sie Content Switching aktivieren, nachdem Sie sowohl den Lastausgleich- als auch die Cache-Umleitungsfunktionen auf der Appliance aktiviert haben.

Aktivieren Sie die Content Switching über die CLI

Geben Sie an der Eingabeaufforderung ein:

```
-  enable ns feature CS

-  show ns feature
<!--NeedCopy-->
```

Beispiel:

```
> enable ns feature cs
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   ON
 3)     Load Balancing                  LB                   ON
 4)     Content Switching               CS                   ON
 5)     Cache Redirection               CR                   ON
          ...
          ...
          ...
 23)    appliance Push                  push                 OFF
 Done
<!--NeedCopy-->
```

Aktivieren Sie die Cache-Umleitung und den Lastausgleich über die GUI

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter Modi und Funktionen auf **Grundfunktionen konfigurieren**.
3. Aktivieren Sie im Dialogfeld **Grundfunktionen konfigurieren** das Kontrollkästchen neben **Content Switching** und klicken Sie dann auf **OK**.
4. Im Dialogfeld “Funktionen aktivieren/deaktivieren?” klicken Sie auf Ja.

Konfigurieren eines virtuellen Lastausgleichsservers für den Cache

May 11, 2023

Erstellen Sie einen virtuellen Lastausgleichsserver und einen HTTP-Dienst für jeden Typ von Cache-Server, der verwendet werden soll. Wenn Sie beispielsweise JPEG-Dateien von einem Cache-Server und GIF-Dateien von einem anderen Cache-Server bereitstellen und einen dritten Cache-Server für den Rest des Inhalts verwenden möchten, erstellen Sie einen HTTP-Dienst und einen virtuellen Server für jeden der drei Typen von Cache-Servern. Binden Sie dann jeden Dienst an seinen jeweiligen virtuellen Server.

Weitere Informationen zum Erstellen eines virtuellen Lastausgleichsservers finden Sie unter Erstellen eines virtuellen Lastausgleichsservers.

Weitere Informationen zur Konfiguration von Diensten, die den Cache-Server darstellen, finden Sie unter Konfigurieren eines HTTP-Dienstes.

Weitere Informationen zum Binden des Dienstes an einen virtuellen Server finden Sie unter Binden/Aufheben eines Dienstes an/von einem virtuellen Lastausgleichsserver.

Weitere Informationen zum Erstellen eines transparenten Proxy-Cache-Umleitungsservers finden Sie unter Konfigurieren eines virtuellen Cache-Umleitungsserversund Erstellen eines virtuellen Servers vom Typ TRANSPARENT.

Weitere Informationen zum Binden integrierter Cache-Umleitungsrichtlinien an den virtuellen Cache-Umleitungsserver finden Sie unter Binden von Richtlinien an den virtuellen Cache-Umleitungsserver.

Konfigurieren einer Cache-Umleitungsrichtlinie für einen bestimmten Inhaltstyp

Um Anfragen, die eine GIF- oder JPEG-Erweiterung enthalten, als zwischenspeicherbar zu identifizieren, konfigurieren Sie eine Cache-Umleitungsrichtlinie und binden sie an den virtuellen Cache-Umleitungsserver.

Hinweis: Wenn eine Anfrage mit einer Richtlinie übereinstimmt, leitet die NetScaler-Appliance sie an den Ursprungsserver weiter. Daher konfigurieren Sie im folgenden Verfahren Richtlinien, um Anforderungen abzugleichen, die
keine Erweiterungen .png oder .jpeg haben.

Um die Cache-Umleitung für einen bestimmten Inhaltstyp zu konfigurieren, konfigurieren Sie eine Richtlinie, die einen einfachen Ausdruck verwendet, wie unter Cache-Umleitungsrichtlinie konfigurierenbeschrieben.

Richtlinien für Content Switching konfigurieren

December 7, 2021

Sie müssen eine Content Switching-Richtlinie erstellen, um bestimmte Arten von Inhalten zu identifizieren, die an einen Server oder eine Farm weitergeleitet werden sollen, und andere Arten von Inhalten identifizieren, die von einem anderen Cacheserver oder einer anderen Farm bereitgestellt werden sollen. Sie können beispielsweise eine Richtlinie konfigurieren, um den Speicherort für Bilddateien mit den Erweiterungen.png und .jpeg zu bestimmen.

Bevor Sie die Content Switching-Richtlinie erstellen, müssen Sie eine Content Switching-Aktion definieren, um zu beschreiben, welcher virtuelle Lastausgleichsserver ausgewählt werden soll. Diese Aktion wird in der Content Switching-Richtlinie verwendet.

Nachdem Sie die Content Switching-Richtlinie definiert haben, binden Sie sie an einen virtuellen Content Switching-Server und geben einen virtuellen Lastausgleichsserver an. Anforderungen, die der Richtlinie entsprechen, werden an den benannten virtuellen Lastausgleichsserver weitergeleitet. Anforderungen, die nicht mit der Content Switching-Richtlinie übereinstimmen, werden an den standardmäßigen virtuellen Lastausgleichsserver für den Cache weitergeleitet.

Weitere Informationen zur Funktion zum Content Switching und zum Konfigurieren von Richtlinien zum Content Switching finden Sie unter Content Switching.

Sie müssen zuerst die Content Switching-Richtlinie erstellen und sie dann an den virtuellen Content Switching-Server binden.

Erstellen einer Content Switching-Richtlinie mithilfe des Befehls CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
- add cs action <name> [-targetLBVserver <string> | -targetVserver <
   string> | -targetVserverExpr <expression>]
- add cs policy <policyName> -rule <expression> [-action <string>]
- show cs policy [<policyName>]

<!--NeedCopy-->
```

Beispiele:

```
> add cs action action-CS-JPEG -targetLBVserver lbcachejpeg
Done
> show cs action action-CS-JPEG
    Name: action-CS-JPEG
    Target LB Vserver: lbcachejpeg
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0
Done

```



```
> add cs policy policy-CS-JPEG -rule 'HTTP.REQ.URL.SUFFIX == "jpeg"' -action action-CS-JPEG
Done
> show cs policy policy-CS-JPEG
    Policy: policy-CS-JPEG Rule: HTTP.REQ.URL.SUFFIX == "jpeg"
    Action: action-CS-JPEG

    HITS: 0
Done
>

> add cs action action-CS-GIF -targetLBVserver lbcachegif
Done
> show cs action action-CS-GIF
    Name: action-CS-GIF
    Target LB Vserver: lbcachegif
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0

Done
>
> add cs policy policy-CS-GIF -rule 'HTTP.REQ.URL.SUFFIX == "gif"' -action action-CS-GIF
Done
> show cs policy policy-CS-GIF
    Policy: policy-CS-GIF Rule: HTTP.REQ.URL.SUFFIX == "gif"
    Action: action-CS-GIF

    Hits: 0
Done
<!--NeedCopy-->
```

Erstellen Sie über die GUI eine regelbasierte Content Switching-Richtlinie

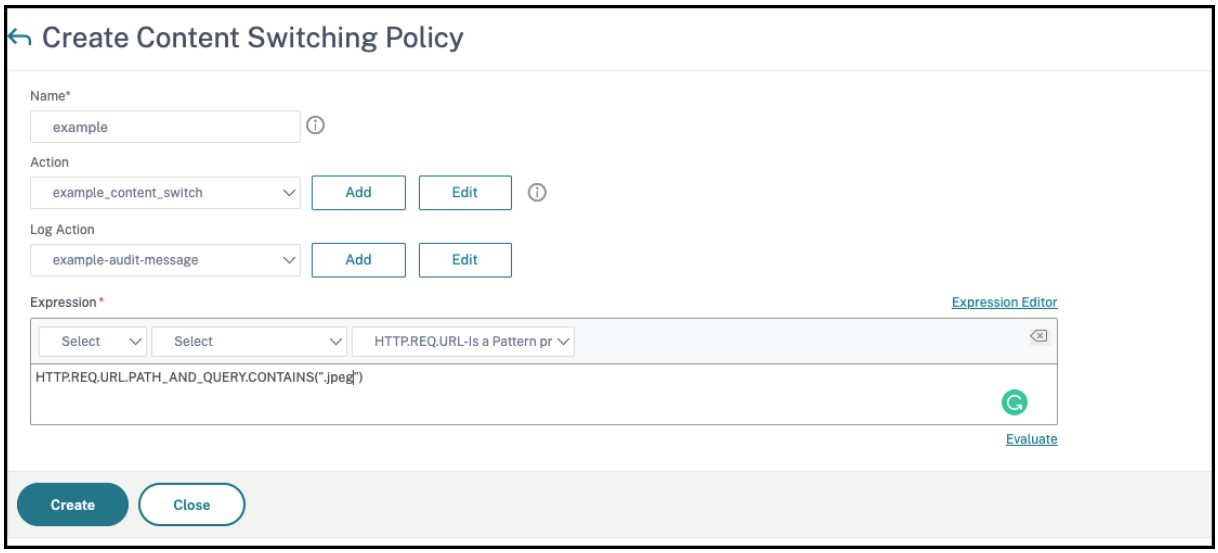
1. Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Content Switching-Policy erstellen** in das Textfeld **Name** einen Namen für die Richtlinie ein.
4. Klicken Sie auf der Registerkarte **Aktion** auf **Hinzufügen**, um eine Content-Switch-Aktion zu erstellen. Oder wählen Sie die verfügbare Aktion aus der Dropdownliste aus.

- Geben Sie auf der Registerkarte “Name” einen Namen für die Aktion “Inhalt mit” ein.
- Wählen Sie den virtuellen Server oder Ausdruck aus der Dropdownliste aus:
  - **Virtueller Loadbalancing-Server**
  - **Globaler Server-Loadbalancing-Server**
  - **Virtueller Authentifizierungsserver**
  - **NetScalar Gateway Virtueller Server**
  - **Ausdruck**
- Klicken Sie auf **Hinzufügen** oder **Bearbeiten**, um den **virtuellen Ziellastenausgleichsserver**zu konfigurieren.

5. Klicken Sie auf der Registerkarte **Protokollaktion** auf **Hinzufügen**, um eine Überwachungsnachrichtenaktion zu erstellen. Oder wählen Sie die verfügbare Überwachungsmeldungsaktion aus der Dropdownliste aus.
6. Wählen Sie im Bereich **Ausdruck** den erforderlichen Ausdruckstyp aus.
7. Wählen Sie im Dialogfeld **Ausdrucksеditor** die Ausdruckssyntax aus, die Sie verwenden möchten.

   Klicken Sie im Bereich **Ausdruck** auf **Auswerten**, um eine Ausdrucksauswertung auszuwerten. Der Evaluator wertet den von Ihnen eingegebenen Ausdruck aus, um zu überprüfen, ob er gültig ist, und zeigt eine Analyse der Auswirkung des Ausdrucks im **Ergebnisbereich** an.
8. Geben Sie Ihre Richtlinienausdrücke ein.

   Informationen zur Verwendung der erweiterten Syntax finden Sie unter Konfigurieren des erweiterten Richtlinienausdrucks: Erste Schritte.
9. Klicken Sie auf **Erstellen**. Die von Ihnen erstellte Richtlinie wird im Bereich **Content Switching-Richtlinien** angezeigt.



Binden Sie die Richtlinie zum Content Switching über die CLI an einen virtuellen Cache-Umleitungsserver

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Richtlinie für die Content Switching an einen virtuellen Cache-Umleitungsserver zu binden und die Konfiguration zu überprüfen:

```
-  bind cs vserver <name> (-lbvserver <string> | -vServer <string> (-
    policyName <string> [-targetLBVserver <string>] [-priority<
    positive_integer>] [-gotoPriorityExpression <expression>] [-type <
    type>] [-invoke (<labelType> <labelName>) ] )

-  show cs vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

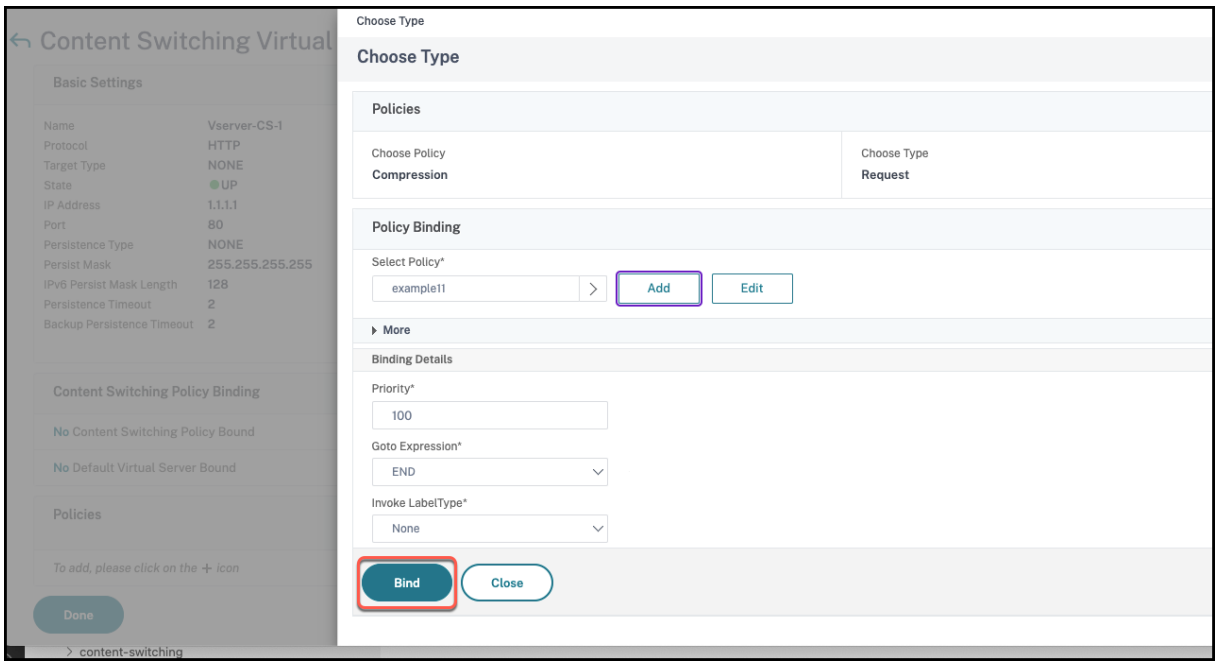
```
> bind cs vserver Vserver-CR-1 -policyName Policy-CS-JPEG -priority 100
 Done
> bind cs vserver Vserver-CR-1 -policyName Policy-CS-GIF -priority 200
 Done
> show cs vserver Vserver-CR-1
        Vserver-CR-1 (10.102.29.60:80) - HTTP   Type: CONTENT
        State: UP
        Last state change was at Fri Jul  2 12:53:45 2010
        Time since last state change: 0 days, 00:00:58.920
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow loggig: ENABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Cacheable: YES
        Vserver IP and Port insertion: OFF
        L2Conn: OFF    Case Sensitivity: ON
        Authentication: OFF
        401 Based Authentication: OFF
        Push: DISABLED  Push VServer:
        Push Label Rule: none
        HTTP Redirect Port: 0    Dtls:  OFF
        Persistence: NONE
        Listen Policy: NONE
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
```



```
29          Traffic Domain:  0
30
31 1)       Content-Switching Policy: Policy-CS-JPEG Priority: 100     Hits
       : 0
32 2)       Content-Switching Policy: Policy-CS-GIF Priority: 200     Hits:
        0
33  Done
34 >
35 <!--NeedCopy-->
```

Binden Sie die Richtlinie zum Content Switching über die GUI an einen virtuellen Cache-Umleitungsserver

1. Navigieren Sie zu **Verkehrsmanagement** > **Content Switching** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die Richtlinie binden möchten (z. B. **vServer-CS-1**), und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Content Switching Virtual Server** auf der Registerkarte **Richtlinien** unter **Erweiterte Einstellungen**auf Symbol **Hinzufügen**, wählen Sie dann Richtlinie und wählen Sie Typ aus der Dropdownliste **Richtlinie auswählen und Typ auswählen** aus.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Registerkarte **Richtlinienbindung** die verfügbare Richtlinie aus der Liste aus, und klicken Sie dann auf **Auswählen**, oder klicken Sie auf **Hinzufügen**, um eine neue Richtlinie zu erstellen, und klicken Sie dann auf **Erstellen**.
6. Klicken Sie auf **Binden**, um die Content Switching-Richtlinie an den virtuellen Server zu binden.
7. Klicke **Fertig**



Konfigurieren der Rangfolge für die Richtlinienbewertung

January 19, 2021

Sie können eine Content Switching-Richtlinie basierend auf einer Regel konfigurieren, bei der es sich um eine generische Konfiguration für verschiedene Inhaltstypen handelt, oder auf einer URL, die spezifischer ist und genau den Inhaltstyp definiert, der an einen bestimmten Cacheserver gesendet werden muss. Im Wesentlichen kann derselbe Inhalt entweder durch eine regelbasierte Richtlinie oder eine URL-basierte Richtlinie definiert werden.

Nachdem Sie Content Switching-Richtlinien eines beliebigen Typs an einen virtuellen Cache-Umleitungsserver gebunden haben, können Sie den virtuellen Server so konfigurieren, dass entweder regelbasierte oder URL-basierte Richtlinien Vorrang eingeräumt werden. Dies entscheidet wiederum, auf welche Server die jeweiligen Anfragen gerichtet sind.

Um die Priorität für die Richtlinienbewertung zu konfigurieren, verwenden Sie den Parameter precedence, der den Typ der Richtlinie (URL oder RULE) angibt, der Vorrang auf dem virtuellen Server zur Inhaltsumleitung hat.

Mögliche Werte: RULE, URL

Standardwert: RULE

Konfigurieren der Rangfolge für die Richtlinienbewertung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Priorität für die Richtlinienbewertung zu konfigurieren und die Konfiguration zu überprüfen:

```
-  set cr vserver <name> [-precedence (RULE | URL)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -precedence URL
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```

Konfigurieren der Rangfolge für die Richtlinienbewertung mit der GUI

1. Navigieren Sie zu Traffic Management > Content Switching > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die Priorität konfigurieren möchten (z. B. **vServer-CS-1**), und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld “Virtuellen Server konfigurieren (Content Switching)” auf der Registerkarte Erweitert neben Priorität auf Regel oder URL, und klicken Sie dann auf OK.

Verwalten eines virtuellen Cache-Umleitungsservers

January 19, 2021

Um einen virtuellen Cache-Umleitungsserver zu verwalten, müssen Sie Cache-Umleitungsstatistiken anzeigen. Möglicherweise müssen Sie Cache-Umleitungsserver aktivieren oder deaktivieren oder Richtlinientreffer in den Cache anstelle des Ursprungs leiten. Zu den administrativen Aufgaben gehören auch das Sichern eines virtuellen Cache-Umleitungsservers und das Verwalten von Clientverbindungen.

Statistiken zum virtuellen Server zur Cache-Umleitung anzeigen

January 19, 2021

Sie können Eigenschaften eines virtuellen Cache-Umleitungsservers und Statistiken über den Datenverkehr anzeigen, der einen virtuellen Cache-Umleitungsserver durchlaufen hat. Sie können auch die virtuellen Server und Richtlinien für die Cache-Umleitung anzeigen, die Sie für den Lastenausgleich von virtuellen Servern gebunden haben.

Um Statistiken für bestimmte virtuelle Cache-Umleitungsserver anzuzeigen, geben Sie mithilfe des Name-Parameters den Namen des virtuellen Servers an, für den Statistiken angezeigt werden sollen. Andernfalls werden Statistiken für alle virtuellen Cache-Umleitungsserver angezeigt. Maximale Länge: 127

Anzeigen von Statistiken für einen virtuellen Cache-Umleitungsserver mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat cr vserver [<name>]
```

Beispiel:

```
1  > stat cr vserver Vserver-CRD-1
2
3  Vserver Summary
4                            IP  port     Protocol        State
5  Vser...CRD-1         0.0.0.0    80         HTTP           UP
6
7  VServer Stats:
8                                          Rate (/s)
                                              Total
9  Requests                                       0
                         0
10 Responses                                      0
                         0
11 Request bytes                                  0
                         0
```



```
12 Response bytes                                          0
                          0
13
14  Done
15 >
16 <!--NeedCopy-->
```

Anzeigen von Statistiken für einen virtuellen Cache-Umleitungsserver mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie Statistiken anzeigen möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Statistiken.

Geben Sie den Servernamen aus, um grundlegende Statistiken für alle virtuellen Cache-Umleitungsserver anzuzeigen. Geben Sie den Servernamen ein, um detaillierte Statistiken für diesen virtuellen Server anzuzeigen, einschließlich Anzahl und Größe der Anforderungen und Antworten, die den virtuellen Server durchlaufen

Anzeigen der Statistiken eines virtuellen Cache-Umleitungsservers mit der Überwachungs- und Dashboard-Dienstprogramme

1. Um die Statistiken mit der Überwachungsdienstprogramme anzuzeigen, klicken Sie auf die Registerkarte Überwachung.
2. Wählen Sie im Dropdownmenü Gruppe auswählen die Option Virtuelle CR Server. Eine Liste der virtuellen Cache-Umleitungsserver wird angezeigt.
3. Um die Statistiken mit der Dashboard-Dienstprogramme anzuzeigen, klicken Sie auf die Registerkarte Dashboard.
4. Klicken Sie neben Statistisches Dienstprogramm auf Applet Client oder Webstart-Client.
5. Wählen Sie im Dropdownmenü Gruppe auswählen die Option Virtuelle CR Server. Das Dashboard zeigt zusammenfassende Statistiken für die virtuellen Server der Cache-Umleitung an.
6. Klicken Sie auf Diagramm, um ein Diagramm der virtuellen Serveraktivität anzuzeigen. Eine grafische Darstellung der Statistiken des virtuellen Servers wird angezeigt.

Aktivieren oder Deaktivieren eines virtuellen Cache-Umleitungsservers

May 11, 2023

Wenn Sie einen virtuellen Cache-Umleitungsserver erstellen, ist er standardmäßig aktiviert. Wenn Sie einen virtuellen Server mit Cache-Umleitung deaktivieren, ändert sich sein Status in OUT OF SER-

VICE und er leitet keine zwischenspeicherbaren Client-Anfragen mehr weiter. Die NetScaler-Appliance reagiert jedoch weiterhin auf ARP- und Ping-Anfragen für die IP-Adresse dieses virtuellen Servers.

Aktivieren oder deaktivieren Sie einen virtuellen Cache-Umleitungsserver mithilfe der CLI

Geben Sie in der Befehlszeile einen der folgenden Befehle ein:

```
-  enable cr vserver <name>
-  show cr vserver <name>
-  disable cr vserver <name>
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiele:

```
> enable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>

> disable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: OUT OF SERVICE  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

```



```
1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```

Aktivieren oder deaktivieren Sie einen virtuellen Cache-Umleitungsserver mithilfe der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Erweitern Sie im Navigationsbereich die Cache-Umleitung, und klicken Sie dann auf Virtuelle Server.
3. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie aktivieren oder deaktivieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Statistiken.
4. Klicken Sie im Dialogfeld Fortfahren auf Ja.

Direkte Richtlinienanfragen zum Cache anstelle des Ursprungswebservers

May 11, 2023

Wenn eine Anforderung mit einer Richtlinie übereinstimmt, leitet die NetScaler Appliance die Anforderung standardmäßig entweder direkt an den Ursprungsserver oder an einen virtuellen Lastausgleichsserver für den Ursprung weiter, je nachdem, wie Sie die Cache-Umleitung konfiguriert haben.

Sie können das Standardverhalten so ändern, dass, wenn eine Anforderung mit einer Richtlinie übereinstimmt, die Anforderung an einen virtuellen Lastausgleichsserver für den Cache weitergeleitet wird.

Um das Ziel für eine Richtlinienanforderung an den Ursprung oder den Cache zu ändern, verwenden Sie den `onPolicyMatch` Parameter, der angibt, wohin Anforderungen gesendet werden sollen, die der Cache-Umleitungsrichtlinie entsprechen.

Die gültigen Optionen sind:

1. `CACHE` - Leitt alle übereinstimmenden Anfragen an den Cache weiter.
2. `ORIGIN` - Leitt alle übereinstimmenden Anfragen an den Ursprungsserver weiter.

> **Hinweis:**
>
> Damit diese Option funktioniert, müssen Sie den Cache-Umleitungstyp als auswählen `POLICY`.

Mögliche Werte: CACHE, ORIGIN

Standardwert:ORIGIN

Ändern Sie das Ziel für eine Richtlinienanforderung mit der CLI in den Ursprung oder den Cache

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Ziel für einen Richtlinientreffer zu ändern und die Konfiguration zu überprüfen:

```
set cr vserver <name> [-onPolicyMatch (ORIGIN | CACHE)]
<!--NeedCopy-->
```

```
show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -onPolicyMatch CACHE
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Ändern Sie das Ziel eines Richtlinientreffens in den Ursprung oder den Cache, indem Sie die GUI verwenden

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Ziel für eine Richtlinienanforderung ändern möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Klicken **Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung)** auf **Erweitert**.
4. Wählen Sie **CACHE** oder **ORIGIN** aus der Dropdownliste **Umleiten zu** aus.

5. Klicken Sie auf **OK**.

Sichern eines virtuellen Cache-Umleitungsservers

August 19, 2021

Die Cache-Umleitung kann fehlschlagen, wenn der primäre virtuelle Server ausfällt oder übermäßigen Datenverkehr nicht verarbeiten kann. Sie können einen virtuellen Sicherungsserver angeben, der die Verarbeitung des Datenverkehrs übernimmt, wenn der primäre virtuelle Server ausfällt.

Um einen virtuellen Backup-Cache-Umleitungsserver anzugeben, verwenden Sie den Parameter BackupVServer, der den virtuellen Backup-Server angibt. Maximale Länge: 127

Angeben eines virtuellen Backup-Cache-Umleitungsservers mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Backup-Cache-Umleitungsserver anzugeben und die Konfiguration zu überprüfen:

```
-  set cr vserver <name> [-backupVServer <string>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -backupVServer Vserver-CRD-2
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```


Angeben eines virtuellen Backup-Cache-Umleitungsservers mit der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Ziel für eine Richtlinienanforderung ändern möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Wählen Sie in der Dropdownliste Virtueller Server sichern den virtuellen Server aus.
5. Klicken Sie auf OK.

Verwalten von Clientverbindungen für einen virtuellen Server

May 11, 2023

Sie können Timeouts auf einem virtuellen Cache-Umleitungsserver konfigurieren, sodass Clientverbindungen nicht auf unbestimmte Zeit geöffnet bleiben. Sie können Via-Header auch in Anfragen einfügen. Um möglicherweise die Netzwerküberlastung zu reduzieren, können Sie offene TCP-Verbindungen wiederverwenden. Sie können die verzögerte Bereinigung von virtuellen Serververbindungen mit Cache-Umleitung aktivieren oder deaktivieren.

Sie können die Appliance so konfigurieren, dass ICMP-Antworten an PING-Anforderungen gemäß Ihren Einstellungen gesendet werden. Stellen Sie für die IP-Adresse, die dem virtuellen Server entspricht, ICMP RESPONSE auf VSVR_CNTRLD und auf dem virtuellen Server ICMP VSERVER RESPONSE ein.

Die folgenden Einstellungen können auf einem virtuellen Server vorgenommen werden:

- Wenn Sie ICMP VSERVER RESPONSE auf allen virtuellen Servern auf PASSIVE setzen, reagiert die Appliance immer.
- Wenn Sie ICMP VSERVER RESPONSE auf allen virtuellen Servern auf ACTIVE setzen, reagiert die Appliance auch dann, wenn ein virtueller Server aktiv ist.
- Wenn Sie ICMP VSERVER RESPONSE bei einigen auf ACTIVE und bei anderen auf PASSIVE setzen, reagiert die Appliance auch dann, wenn ein auf ACTIVE gesetzter virtueller Server AKTIV ist.

Dieses Dokument enthält die folgenden Informationen:

- Client-Zeitlimit konfigurieren
- Fügen Sie Via-Header in die Anfragen ein
- TCP-Verbindungen wiederverwenden
- Konfiguration der verzögerten Verbindungsbereinigung

Client-Zeitlimit konfigurieren

Sie können den Ablauf von Clientanforderungen angeben, indem Sie einen Timeout-Wert für den virtuellen Cache-Umleitungsserver festlegen. Der Timeout-Wert ist die Anzahl der Sekunden, für die der virtuelle Cache-Umleitungsserver darauf wartet, eine Antwort auf die Clientanforderung zu erhalten.

Um einen Timeout-Wert zu konfigurieren, verwenden Sie den Parameter cltTimeout, der die Zeit in Sekunden angibt, nach der die NetScaler-Appliance alle inaktiven Client-Verbindungen schließt. Der Standardwert ist 180 Sekunden für HTTP/SSL-basierte Dienste und 9000 Sekunden für TCP-basierte Dienste.

Konfigurieren Sie das Client-Timeout mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um das Client-Zeitlimit zu konfigurieren und die Konfiguration zu überprüfen:

```
-  set cr vserver <name> [-cltTimeout <secs>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -cltTimeout 6000
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Konfigurieren Sie das Client-Timeout mithilfe der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.

2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Geben Sie im Textfeld Client-Zeitlimit (Sekunden) den Timeout-Wert in Sekunden ein.
5. Klicken Sie auf OK.

Fügen Sie Via-Header in die Anfragen ein

Ein Via-Header listet die Protokolle und Empfänger zwischen dem Start- und Endpunkt einer Anfrage oder Antwort auf und informiert den Server über Proxys, über die die Anfrage gesendet wurde. Sie können den virtuellen Server für die Cache-Umleitung so konfigurieren, dass er in jede HTTP-Anfrage einen Via-Header einfügt. Der via-Parameter ist standardmäßig aktiviert, wenn Sie einen virtuellen Server für die Cache-Umleitung erstellen.

Um das Einfügen von VIA-Headern in Client-Anfragen zu aktivieren oder zu deaktivieren, verwenden Sie den Parameter via, der den Status des Systems beim Einfügen eines Via-Headers in die HTTP-Anfragen angibt.

Mögliche Werte: ON, OFF

Standardwert: ON

Aktivieren oder deaktivieren Sie das Einfügen von VIA-Headern in Client-Anfragen mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
-  set cr vserver <name> [-via (ON|OFF)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -via ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
```



```
11          Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
12          Backup: Vserver-CRD-2
13
14  1)      Cache bypass  Policy: bypass-cache-control
15  2)      Cache bypass  Policy: Policy-CRD
16   Done
17  >
18  <!--NeedCopy-->
```

Aktivieren oder deaktivieren Sie das Einfügen von VIA-Headern in Client-Anfragen mithilfe der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Markieren Sie das Kontrollkästchen Via.
5. Klicken Sie auf OK.

TCP-Verbindungen wiederverwenden

Sie können die NetScaler-Appliance so konfigurieren, dass TCP-Verbindungen zu den Cache- und Originalservern über alle Client-Verbindungen hinweg wiederverwendet werden. Dies kann die Leistung verbessern, indem die Zeit gespart wird, die für den Aufbau einer Sitzung zwischen dem Server und der Appliance erforderlich ist. Die Wiederverwendungsoption ist standardmäßig aktiviert, wenn Sie einen virtuellen Cache-Umleitungsserver erstellen.

Um die Wiederverwendung von TCP-Verbindungen zu aktivieren oder zu deaktivieren, verwenden Sie den Wiederverwendungsparameter, der den Status der Wiederverwendung von TCP-Verbindungen zu den Cache- oder Ursprungsservern über alle Clientverbindungen angibt.

Mögliche Werte: ON, OFF

Standardwert: ON

Aktivieren oder deaktivieren Sie die Wiederverwendung von TCP-Verbindungen mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1  -  set cr vserver <name> [-reuse (ON|OFF)]
2  -  show cr vserver <name>
```



```
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -reuse ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Aktivieren oder deaktivieren Sie die Wiederverwendung von TCP-Verbindungen mithilfe der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Markieren Sie das Kontrollkästchen Wiederverwenden.
5. Klicken Sie auf OK.

Konfiguration der verzögerten Verbindungsbereinigung

Die Option down state flush führt eine verzögerte Bereinigung von Verbindungen auf einem virtuellen Cache-Umleitungsserver durch. Die Flush-Option im Down-State-Modus ist standardmäßig aktiviert, wenn Sie einen virtuellen Cache-Umleitungsserver erstellen.

Um die Option Downstate Flush zu aktivieren oder zu deaktivieren, legen Sie den Parameter downStateFlush fest.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

Aktivieren oder deaktivieren Sie die Down-State-Flush-Option mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die verzögerte Verbindungsbereinigung zu konfigurieren und die Konfiguration zu überprüfen:

```
-  set cr vserver <name> [-downStateFlush (ENABLED | DISABLED)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -downStateFlush ENABLED
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Aktivieren oder deaktivieren Sie die Wiederverwendung von TCP-Verbindungen mithilfe der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) auf die Registerkarte Erweitert.
4. Aktivieren Sie das Kontrollkästchen Down State Flush.
5. Klicken Sie auf OK.

Aktivieren Sie die externe Zustandsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server

September 18, 2023

In Public Clouds können Sie die NetScaler-Appliance als Lastausgleichsdienst der zweiten Ebene verwenden, wenn der native Load Balancer als erste Stufe verwendet wird. Der native Load Balancer kann ein Application Load Balancer (ALB) oder ein Netzwerklastenausgleichsmodul (NLB) sein. Die meisten Public Clouds unterstützen keine UDP Health Probes in ihren nativen Load Balancern. Wenn diese Server ausgefallen sind, wird ihr aktueller Status daher möglicherweise nicht aktualisiert. Infolgedessen wird der Datenverkehr bedingungslos an NetScaler gesendet, auch wenn die Anforderung nicht bearbeitet werden kann.
Um den Zustand solcher Anwendungen zu überwachen, unterstützt NetScaler HTTP- und TCP-Integritätsprüfungen.

Ein HTTP- oder TCP-Listener wird für einen virtuellen Content Switching-Server erstellt, wenn `probeProtocol` sowohl die als auch die `probePort` Parameter konfiguriert sind. Der Listener spiegelt den Status des virtuellen Servers wider. Der `ProbeSuccessResponseCode` Parameter gilt nur für HTTP und gibt die konfigurierte Zeichenfolge zurück, wenn der Test erfolgreich ist.

So aktivieren Sie die externe Integritätsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server mithilfe der CLI

Geben Sie an der Befehlszeile Folgendes ein:

```
1 add cr vserver <name> <serviceType> -ProbeProtocol <Http/TCP> -
     ProbePort <port-num> -ProbeSuccessResponseCode<http-code>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add cr vserver Vserver-CR-1 HTTP -ProbeProtocol HTTP -probeport 5000 -
     probesuccessResponseCode 200OK
2 <!--NeedCopy-->
```

So aktivieren Sie die externe Integritätsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Virtuelle Server**und erstellen Sie dann einen virtuellen Server.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Server zu erstellen.

3. Aktualisieren Sie im Bereich **Grundeinstellungen** die folgenden Details:
   a) Prüfprotokoll — Wählen Sie das Protokoll (HTTP oder TCP) der Sonde für die externe Zustandsprüfung des virtuellen Servers aus.
   b) Test Success Response Code — Geben Sie die Antwortzeichenfolge für eine erfolgreiche Prüfung ein. Dieser Parameter gilt nur für das HTTP-Protokoll.
      - Standardwert: 200ok
      - Maximale Länge: 63
   c) Probe Port — Geben Sie die Portnummer für die HTTP- oder TCP-Überwachung ein.
4. Klicken Sie auf **OK**.

N-Tier-Cache-Umleitung

May 11, 2023

Um große Mengen zwischengespeicherter Daten, in der Regel mehrere Gigabyte pro Sekunde, effizient zu verarbeiten, stellt ein Internetdienstanbieter (ISP) mehrere dedizierte Cacheserver bereit. Die Cache-Umleitungsfunktion der NetScaler-Appliance kann zur Lastverteilung der Cache-Server beitragen, aber eine einzelne Appliance oder mehrere Appliances bewältigen das große Datenverkehrsvolumen möglicherweise nicht effizient.

Sie können das Problem lösen, indem Sie die NetScaler-Appliances in zwei Ebenen (Layer) bereitstellen, wobei die Appliances in der oberen Ebene die Appliances auf der unteren Ebene ausgleichen und die Appliances auf der unteren Ebene die Cache-Server ausgleichen. Diese Anordnung wird als *n-Tier-Cache-Umleitung*bezeichnet.

Zu Zwecken wie Überwachung und Sicherheit muss ein ISP Kundendetails wie die IP-Adresse, die bereitgestellten Informationen und den Zeitpunkt der Interaktion verfolgen. Daher müssen Client-Verbindungen über eine NetScaler-Appliance vollständig transparent sein. Wenn Sie jedoch eine transparente Cache-Umleitung konfigurieren und die NetScaler-Appliances parallel bereitgestellt werden, muss die IP-Adresse des Clients von allen Appliances gemeinsam genutzt werden. Die gemeinsame Nutzung der Client-IP-Adresse führt zu einem Konflikt, der dazu führt, dass Netzwerkgeräte wie Router, Cache-Server, Ursprungsserver und andere NetScaler-Appliances nicht in der Lage sind, die Appliance und damit den Client zu bestimmen, an den die Antwort gesendet werden soll.

So wird die N-Tier-Cache-Umleitung implementiert

Um das Problem zu lösen, teilt die N-Tier-Cache-Umleitung der Appliance den Quellportbereich auf die Appliances der unteren Ebene auf und bezieht die Client-IP-Adresse in die Anfrage ein, die an die Cache-Server gesendet wird. Die NetScaler-Appliances der oberen Ebene sind so konfiguriert, dass

sie einen sitzungslosen Lastenausgleich durchführen, um eine unnötige Belastung der Appliances zu vermeiden.

Wenn die untergeordnete NetScaler-Appliance mit einem Cache-Server kommuniziert, verwendet sie eine zugeordnete IP-Adresse (MIP), um die Quell-IP-Adresse darzustellen. Daher kann der Cache-Server die Appliance identifizieren, von der er die Anfrage empfangen hat, und die Antwort an dieselbe Appliance senden.

Die untergeordnete NetScaler-Appliance fügt die Client-IP-Adresse in den Header der Anfrage ein, die an den Cache-Server gesendet wird. Die Client-IP im Header hilft der Appliance dabei, den Client zu bestimmen, an den das Paket weitergeleitet werden soll, wenn sie die Antwort von einem Cache-Server erhält, oder den Ursprungsserver im Falle eines Cache-Fehlers. Der Ursprungsserver bestimmt die zu sendende Antwort anhand der Client-IP, die in den Anforderungsheader eingefügt wurde.

Der Ursprungsserver sendet die Antwort an eine Appliance der oberen Ebene, einschließlich der Quellportnummer, von der der Originalserver die Anfrage empfangen hat. Der gesamte Quellportbereich, 1024 bis 65535, ist auf die NetScaler-Appliances der unteren Stufe verteilt. Jeder Appliance der unteren Stufe wird ausschließlich eine Gruppe von Adressen innerhalb des Bereichs zugewiesen. Diese Zuteilung ermöglicht es der Appliance der oberen Ebene, die NetScaler-Appliance der unteren Ebene, die die Anfrage an den Ursprungsserver gesendet hat, eindeutig zu identifizieren. Die Appliance der oberen Ebene kann die Antwort daher an die richtige Appliance der unteren Ebene weiterleiten.

Die NetScaler-Appliances der oberen Ebene sind für richtlinienbasiertes Routing konfiguriert, und die Routing-Richtlinien sind so definiert, dass sie die IP-Adresse der Ziel-Appliance anhand des Quellportbereichs bestimmen.

Für die Konfiguration von N-Tier CRD ist eine Einrichtung erforderlich

Das folgende Setup ist für das Funktionieren der n-Tier-Cache-Umleitung erforderlich:

Für jede NetScaler-Appliance der oberen Ebene:

- Aktivieren Sie den Layer-3-Modus.
- Definieren Sie Richtlinien für richtlinienbasierte Routen (PBRs), sodass der Datenverkehr entsprechend der Reichweite des Zielports weitergeleitet wird.
- Konfigurieren Sie einen virtuellen Lastausgleichsserver.
- Konfigurieren Sie den virtuellen Server so, dass er den gesamten vom Client kommenden Datenverkehr abhört. Stellen Sie den Diensttyp/das Protokoll auf ANY und die IP-Adresse auf ein Sternchen (*) ein.
- Aktivieren Sie den Sitzungslosen Lastenausgleich mit dem MAC-basierten Umleitungsmodus, um eine unnötige Belastung der NetScaler-Appliances der oberen Ebene zu vermeiden.
- Vergewissern Sie sich, dass die Option Proxyport verwenden aktiviert ist.
- Erstellen Sie einen Dienst für jede untergeordnete Appliance und binden Sie alle Dienste an den virtuellen Server.

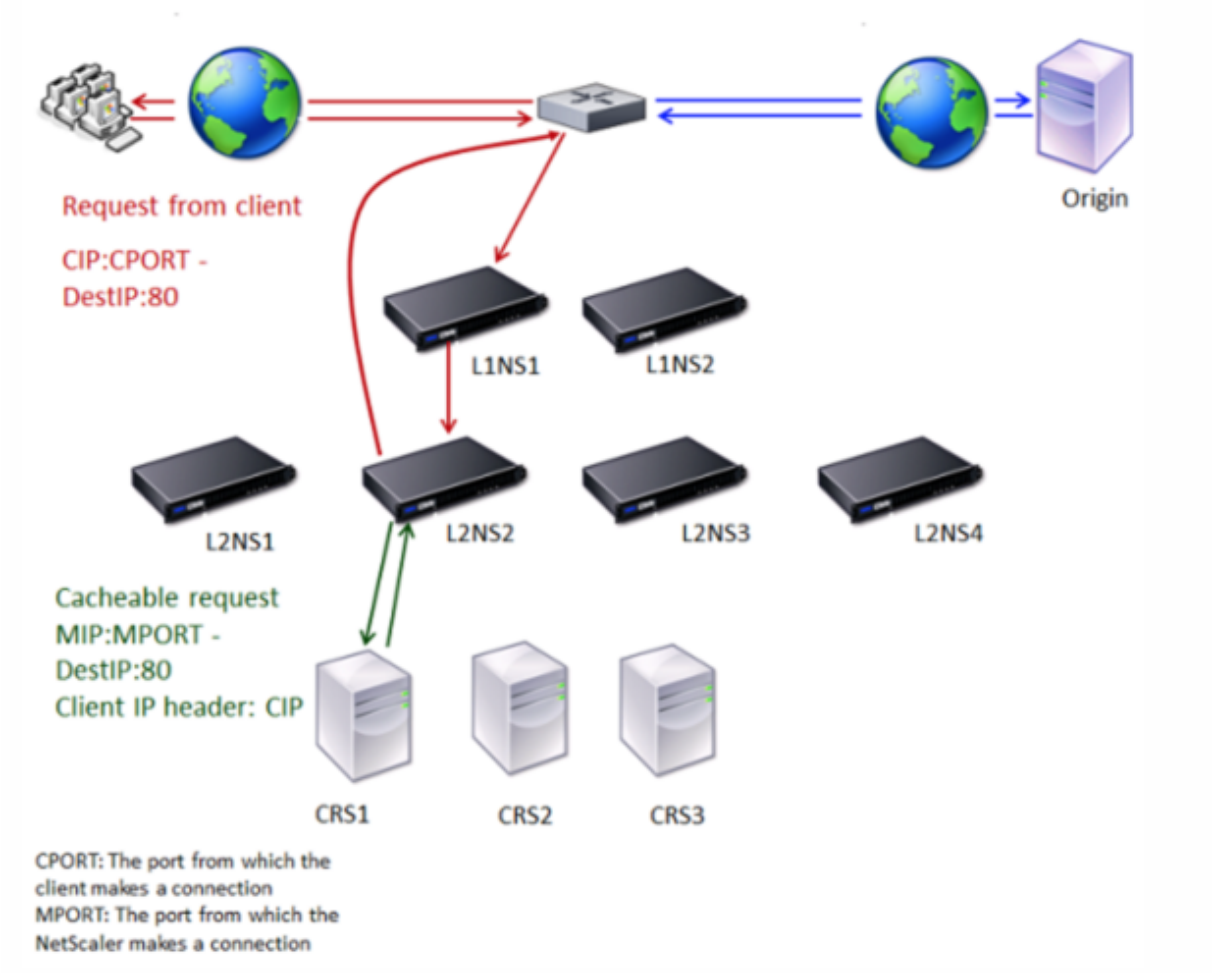
Für jede NetScaler-Appliance der unteren Stufe

- Konfigurieren Sie den Portbereich für die Cache-Umleitung auf der Appliance. Weisen Sie jeder Appliance der unteren Stufe einen exklusiven Bereich zu.
- Konfigurieren Sie einen virtuellen Lastausgleichsserver und aktivieren Sie die MAC-basierte Umleitung.
- Erstellen Sie einen Dienst für jeden Cache-Server, für den diese Appliance einen Lastenausgleich durchführen soll. Aktivieren Sie beim Erstellen des Dienstes das Einfügen der Client-IP in den Header. Binden Sie dann alle Dienste an den virtuellen Load-Balancing-Server.
- Konfigurieren Sie einen virtuellen Server für die Cache-Umleitung im transparenten Modus mit den folgenden Einstellungen:
  - Aktiviere die Origin USIP Option.
  - Fügen Sie einen Quell-IP-Ausdruck hinzu, um die Client-IP in den Header aufzunehmen.
  - Aktivieren Sie die Option Portbereich verwenden.

So funktioniert die N-Tier-Cache-Umleitung bei einem Cache-Treffer

Die folgende Abbildung zeigt, wie die Cache-Umleitung funktioniert, wenn eine Client-Anfrage zwischengespeichert werden kann und die Antwort von einem Cache-Server gesendet wird.

Abbildung 1. Cache-Umleitung bei einem Cache-Treffer



Zwei NetScaler-Appliances, L1NS1 und L1NS2, werden in der oberen Ebene bereitgestellt, und vier NetScaler-Appliances, L2NS1, L2NS2, L2NS3 und L2NS4, werden in der unteren Ebene bereitgestellt. Client A sendet eine Anfrage, die vom Router weitergeleitet wird. Die Cache-Server CRS1, CRS2 und CRS3 bearbeiten die Cache-Anfragen. Origin Server O bedient die ungecachten Anfragen.

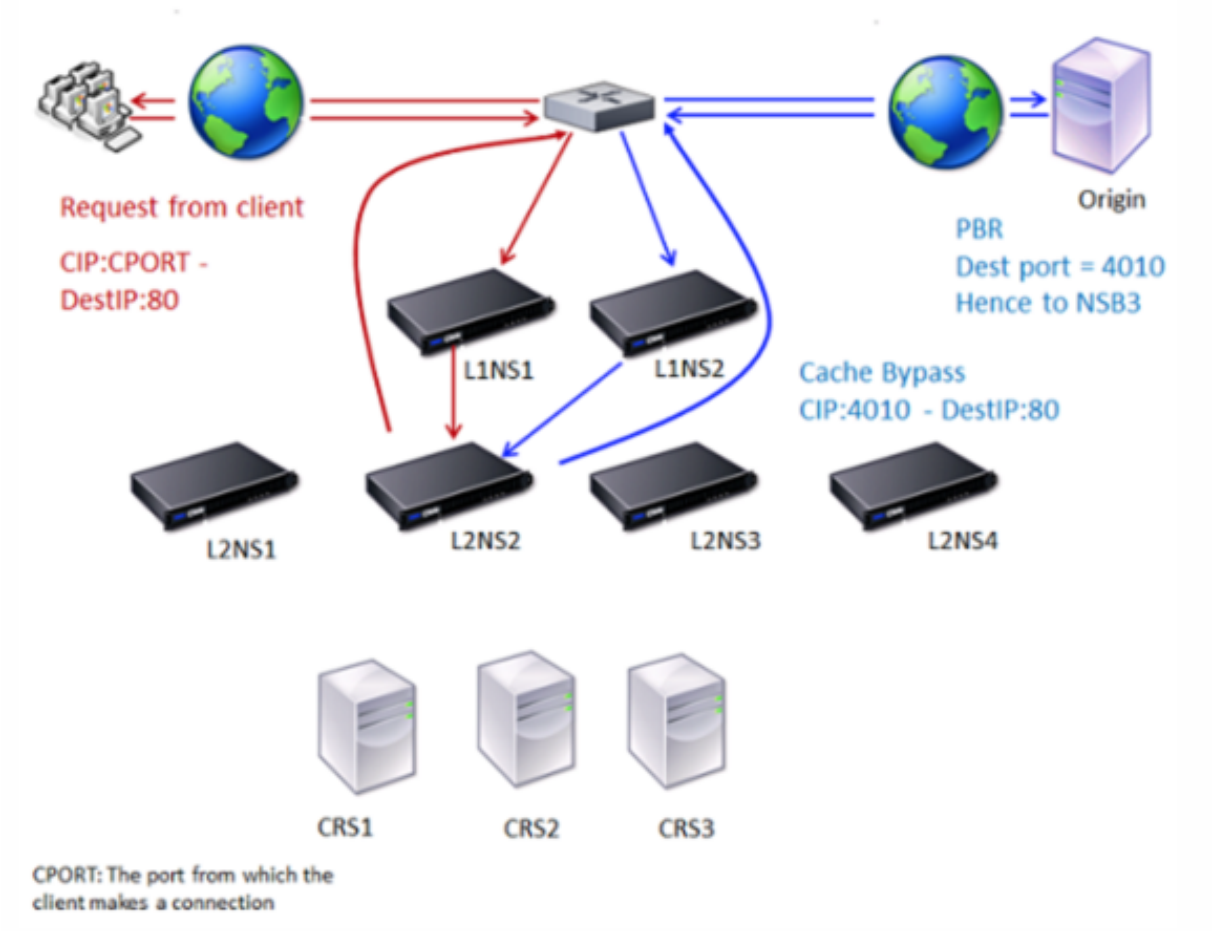
Verkehrsfluss

1. Der Client sendet eine Anfrage und der Router leitet sie an L1NS1 weiter.
2. L1NS1 verteilt die Anforderung auf L2NS2.
3. L2NS2 verteilt die Anforderung an den Cache-Server CRS1, und die Anfrage ist zwischenspeicherbar. L2NS2 schließt die Client-IP in den Anforderungsheader ein.
4. CRS1 sendet die Antwort an L2NS2, da L2NS2 bei der Verbindung zu CRS1 seinen MIP als Quell-IP-Adresse verwendet hat.
5. Mithilfe der Client-IP-Adresse im Anforderungsheader identifiziert L2NS2 den Client, von dem die Anfrage kam. L2NS2 sendet die Antwort direkt an den Router und vermeidet so eine unnötige Belastung der Appliance in der oberen Ebene.
6. Der Router leitet die Antwort an Client A weiter.

So funktioniert die N-Tier-Cache-Umleitung bei einem Cache-Bypass

Die folgende Abbildung zeigt, wie die Cache-Umleitung funktioniert, wenn eine Clientanfrage zur Antwort an einen Ursprungsserver gesendet wird.

Abbildung 2. Cache-Umleitung bei einem Cache-Bypass



Zwei NetScaler-Appliances, L1NS1 und L1NS2, werden in der oberen Ebene bereitgestellt, und vier NetScaler-Appliances, L2NS1, L2NS2, L2NS3 und L2NS4, werden in der unteren Ebene bereitgestellt. Client A sendet eine Anfrage, die vom Router weitergeleitet wird. Die Cache-Server CRS1, CRS2 und CRS3 bearbeiten die Cache-Anfragen. Origin Server O bedient die ungecachten Anfragen.

Verkehrsfluss

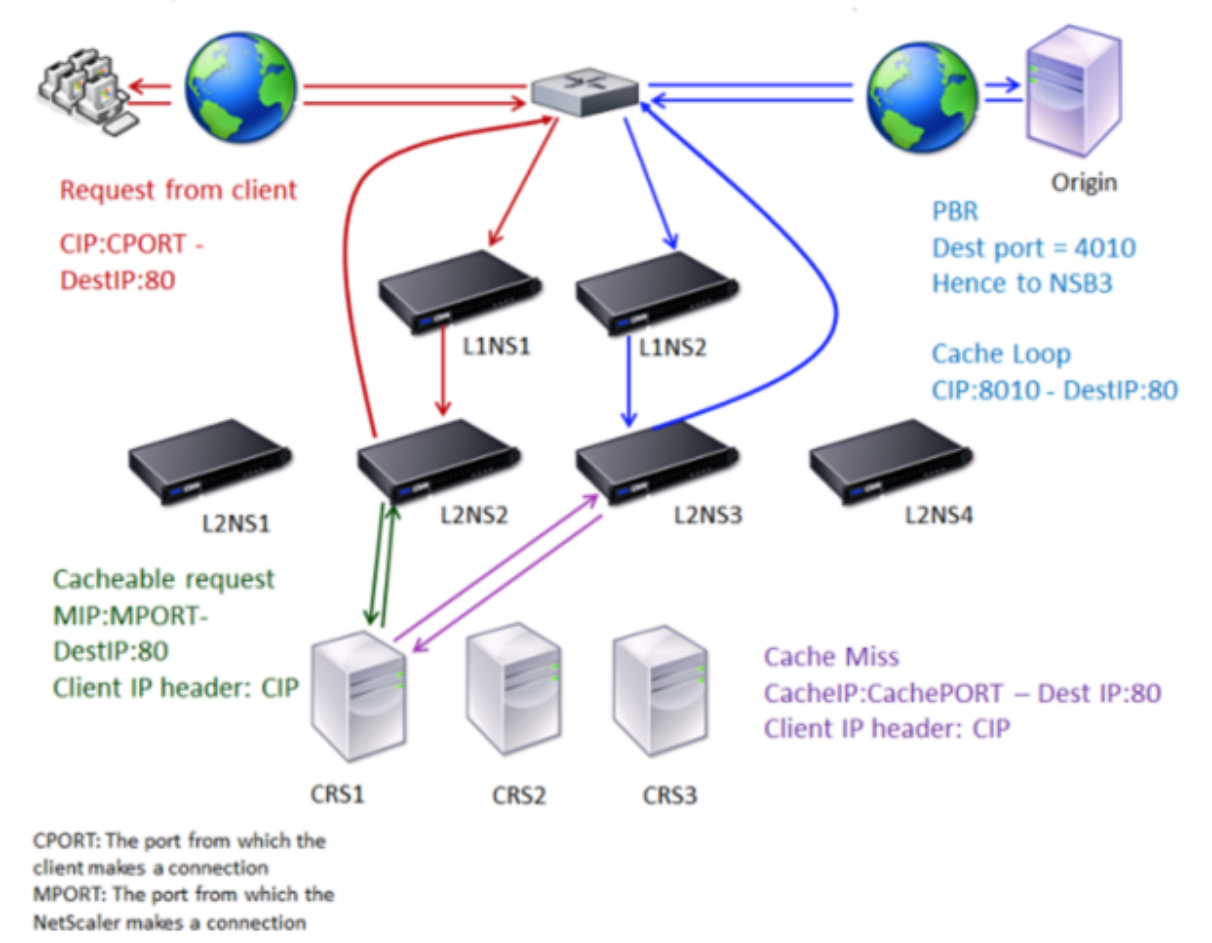
1. Der Client sendet eine Anfrage und der Router leitet sie an L1NS1 weiter.
2. L1NS1 verteilt die Anforderung auf L2NS2.
3. Die Anfrage ist nicht zwischenspeicherbar (Cache-Bypass). Daher sendet L2NS2 die Anfrage über den Router an den Ursprungsserver.
4. Der Ursprungsserver sendet die Antwort an eine Appliance der oberen Ebene, L1NS2.

5. Gemäß den PBR-Richtlinien leitet L1NS2 den Datenverkehr an die entsprechende Appliance der unteren Ebene, L2NS2, weiter.
6. L2NS2 verwendet die Client-IP-Adresse im Anforderungsheader, um den Client zu identifizieren, von dem die Anfrage kam, und sendet die Antwort direkt an den Router, wodurch eine unnötige Belastung der Appliance in der oberen Ebene vermieden wird.
7. Der Router leitet die Antwort an Client A weiter.

So funktioniert die N-Tier-Cache-Umleitung bei einem Cachefehler

Die folgende Abbildung zeigt, wie die Cache-Umleitung funktioniert, wenn eine Client-Anfrage nicht zwischengespeichert wird.

Abbildung 3. Cache-Umleitung im Falle eines Cache-Fehls



Zwei NetScaler-Appliances, L1NS1 und L1NS2, werden in der oberen Ebene bereitgestellt, und vier NetScaler-Appliances, L2NS1, L2NS2, L2NS3 und L2NS4, werden in der unteren Ebene bereitgestellt. Client A sendet eine Anfrage, die vom Router weitergeleitet wird. Die Cache-Server CRS1, CRS2 und CRS3 bearbeiten die Cache-Anfragen. Origin Server O bedient die ungecachten Anfragen.

Verkehrsfluss

1. Der Client sendet eine Anfrage und der Router leitet sie an L1NS1 weiter.
2. L1NS1 verteilt die Anforderung auf L2NS2.
3. L2NS2 verteilt die Anforderung an den Cache-Server CRS1, da die Anfrage zwischenspeicherbar ist.
4. CRS1 hat keine Antwort (Cachefehler). CRS1 leitet die Anfrage über die Appliance in der unteren Ebene an den Ursprungsserver weiter. L2NS3 fängt den Verkehr ab.
5. L2NS3 nimmt die Client-IP aus dem Header und leitet die Anfrage an den Ursprungsserver weiter. Der im Paket enthaltene Quellport ist der L2NS3-Port, von dem die Anfrage an den Ursprungsserver gesendet wird.
6. Der Ursprungsserver sendet die Antwort an eine Appliance der oberen Ebene, L1NS2.
7. Gemäß den PBR-Richtlinien leitet L1NS2 den Datenverkehr an die entsprechende Appliance der unteren Stufe, L2NS3, weiter.
8. L2NS3 leitet die Antwort an den Router weiter.
9. Der Router leitet die Antwort an Client A weiter.

Konfigurieren der NetScaler-Appliances der oberen Stufe

May 11, 2023

Konfigurieren Sie jede der NetScaler-Appliances der oberen Ebene wie folgt.

Konfigurieren Sie eine Appliance der oberen Ebene für die n-Tier-Cache-Umleitung mithilfe des Befehls CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add service \<name\>@ \<serviceIP\> \<serviceType\> \<port\>`

  Führen Sie diesen Befehl für jeden hinzuzufügenden Dienst aus.

- `add lb vserver \<name\>@ ANY \* \<port\> -persistenceType \<persistenceMethod \> -lbMethod \<lbMethod\> -m MAC -sessionless ENABLED -cltTimeout \< client\\_Timeout\\_Value\>`

- `bind lb vserver \<name\>@ \<serviceName\>`

  Führen Sie diesen Befehl für jeden Dienst aus, der gebunden werden soll.

- `enable ns mode l3`

- `add ns pbr \<name\> \<action\> -srcPort \<sourcePortNumber\> -destPort \<startPortNumber-endPortNumber\> -nexthop \<serviceIpAddress\> -protocol TCP`
- `apply ns pbrs`

  Führen Sie diesen Befehl aus, nachdem Sie alle erforderlichen PBRs hinzugefügt haben.

Konfigurieren Sie eine Appliance der oberen Ebene für die n-Tier-Cache-Umleitung mithilfe der GUI

1. L3-Modus aktivieren:
   a) Klicken Sie im Navigationsbereich auf Systemund dann auf Einstellungen.
   b) Klicken Sie in der Gruppe Einstellungen auf den Link Modi konfigurieren.
   c) Aktivieren Sie das Kontrollkästchen Layer-3-Modus (IP-Weiterleitung).
   d) Klicken Sie auf OK.
2. Konfigurieren Sie das richtlinienbasierte Routing (PBR):
   a) Navigieren Sie zu System > Netzwerk > PBRs.
   b) Klicken Sie im Bereich Policy-Based Routing (PBRs) auf Hinzufügen.
   c) Geben Sie einen Namen für den PBR ein.
   d) Wählen Sie die Aktion als Zulassen aus.
   e) Geben Sie in das Feld Next Hop die IP-Adresse des Dienstes ein, der eine Appliance der unteren Stufe darstellt.
   f) Wählen Sie in der Dropdownliste Protokoll die Option TCP aus.
   g) Geben Sie den Quellport und den Bereich des Zielports ein, der der hinzugefügten Appliance der niedrigeren Stufe entspricht.
   h) Klicken Sie auf Erstellen.
   i) Wählen Sie im Detailbereich den PBR aus und klicken Sie auf Anwenden.
   j) Wiederholen Sie die Schritte (i) bis Schritt (vii) für jedes untergeordnete Gerät.
3. Erstellen Sie einen Dienst für jede untergeordnete Appliance:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Services.
   b) Klicken Sie im Detailbereich auf “Hinzufügen”.
   c) Geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Das Protokoll sollte EIN BELIEBIGES sein.
   d) Klicken Sie auf Erstellen.
4. Konfigurieren Sie einen virtuellen Lastausgleichsserver:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
   b) Klicken Sie im Detailbereich auf “Hinzufügen”.
   c) Geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Das Protokoll sollte ANY sein und die IP-Adresse sollte * sein.
   d) Wählen Sie auf der Registerkarte Dienste die Dienste aus, die die NetScaler-Appliances der

unteren Stufe repräsentieren.

e) Wählen Sie auf der Registerkarte Erweitert den Umleitungsmodus als MAC-basiert aus und aktivieren Sie das Kontrollkästchen Sitzungslos.

f) Klicken Sie auf Erstellen.

Konfigurieren der NetScaler-Appliances der niedrigeren Stufe

May 11, 2023

Konfigurieren Sie jede der untergeordneten NetScaler-Appliances wie folgt.

Konfigurieren Sie eine untergeordnete Appliance für die n-Tier-Cache-Umleitung mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add service <name>@ <cacheServiceIP> <serviceType> <port> -cip ENABLED "ClientIP"-cachetype transparent`

  Wiederholen Sie dies für jeden Cache-Server.

- `add lb vserver <name>@ <serviceType> -m MAC`
- `bind lb vserver <name>@ <cacheServiceName>`

  Wiederholen Sie dies für jeden Cache-Server.

- `add cr vserver <name> <serviceType> * <port> -srcIPExpr "HTTP.REQ. HEADER("ClientIP")"-originusip ON -usePortRange ON`
- `set ns param-crPortRange <startPortNumber-endPortNumber>`

Konfigurieren Sie mithilfe der GUI eine Appliance der unteren Ebene für die n-Tier-Cache-Umleitung

1. Erstellen Sie einen Dienst für jeden Cache-Server. Um einen Service zu erstellen:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Services.
   b) Klicken Sie im Detailbereich auf Hinzufügen und geben Sie den Namen und das Protokoll an. Deaktivieren Sie das Kontrollkästchen Direkt adressierbar.
   c) Aktivieren Sie auf der Registerkarte Erweitert die Kontrollkästchen Override Global und das Kontrollkästchen Client-IP, und geben Sie dann in das Feld Header die Zeichenfolge ClientIP ein.
   d) Wählen Sie im Feld Cachetyp die Option Transparenter Cache aus.

e) Klicken Sie auf Erstellen.

2. Konfigurieren Sie einen virtuellen Lastausgleichsserver:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Virtual Services.
   b) Klicken Sie im Detailbereich auf Hinzufügen und geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Die IP-Adresse sollte ein Sternchen (*) sein.
   c) Wählen Sie auf der Registerkarte Dienste die Dienste aus, die die Cache-Server repräsentieren.
   d) Wählen Sie auf der Registerkarte Erweitert für Umleitungsmodus die Option MAC Based aus.
   e) Klicken Sie auf Erstellen.
3. Konfigurieren Sie einen virtuellen Server für die Cache-Umleitung:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Virtual Services.
   b) Klicken Sie im Detailbereich auf Hinzufügen und geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Die IP-Adresse sollte * sein.
   c) Wählen Sie für Cachetyp die Option Transparent aus.
   d) Wählen Sie auf der Registerkarte Erweitert im Feld Cache-Server den neuen virtuellen Load-Balancing-Server aus und aktivieren Sie die Kontrollkästchen Origin USIP und Use Port Range. Geben Sie in das Feld Quell-IP-Ausdruck HTTP.REQ.HEADER („ClientIp“) ein.
   e) Klicken Sie auf Erstellen.
4. Weisen Sie der Appliance einen Quellportbereich zu:
   a) Klicken Sie im Navigationsbereich auf Systemund dann auf Einstellungen.
   b) Klicken Sie in der Gruppe Einstellungen auf den Link Globale Systemeinstellungen ändern.
   c) Geben Sie in der Gruppe Cache-Umleitungs-Portbereich den Portbereich für die Appliance an, indem Sie eine Portnummer für Startport und eine Portnummer für Endport eingeben.
   d) Klicken Sie auf OK.

Übersetzen die Ziel-IP-Adresse einer Anfrage in die Ursprungs-IP-Adresse

May 11, 2023

Sie können den virtuellen Forward-Proxy-Cache-Umleitungsserver auf der NetScaler-Appliance so konfigurieren, dass die Ziel-IP-Adresse der Anfrage, die auf dem virtuellen Cache-Umleitungsserver landet, in die IP-Adresse des Originalservers übersetzt wird. Diese Übersetzung erfolgt unabhängig davon, ob die Anfrage an die zwischengespeicherten Server oder den Ursprungsserver gesendet wird. Bisher konnte der virtuelle Server für die Forward-Proxy-Cache-Umleitung in einer Service Provider-Umgebung nicht effektiv verwendet werden, um Datenverkehr über die Firewall zu senden, da die Cache-Umleitung mithilfe von Content Switching-Richtlinien eingeschränkt war. Der virtuelle Cache-

Umleitungsserver hat die ursprüngliche IP-Adresse nicht in die Ziel-IP übersetzt, als das Paket in den Cache gesendet wurde. Die Ziel-IP-Adresse war nur dann die des Ursprungsservers, wenn die Anfragen vom zwischengespeicherten Server bedient wurden.

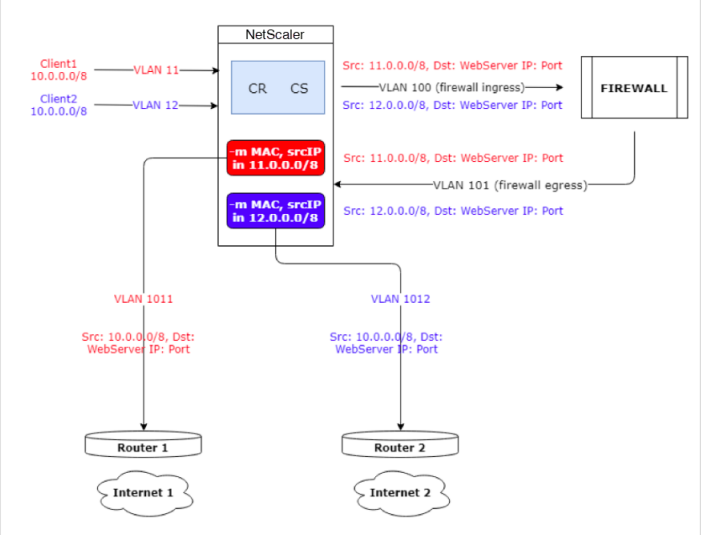
Hinweis: Die Übersetzung der Ziel-IP-Adresse einer Anfrage in die Ursprungs-IP-Adresse wird für einen virtuellen Server mit transparenter Cache-Umleitung nicht unterstützt. Für einen virtuellen Server mit transparenter Cache-Umleitung muss diese Option auf OFF gesetzt sein.

Anwendungsfall

In einer Bereitstellung, in der die NetScaler Appliance für die Forward-Proxy-Cache-Umleitung, Firewall und wiederverwendete Client-IP-Adressen konfiguriert ist, kann die Firewall die wiederverwendeten IP-Adressen nicht unterscheiden/verwenden. Daher müssen diese wiederverwendeten IP-Adressen in verschiedene IP-Adressen übersetzt werden. Um die wiederverwendeten IP-Adressen zu übersetzen, muss die NetScaler-Appliance Folgendes ausführen:

1. Fragen Sie einen virtuellen DNS-Lastausgleichsserver nach der Auflösung des Ziels ab.
2. Aktualisieren Sie die ursprüngliche IP-Adresse und die Portnummer im Ziel.
3. Senden Sie die Anfrage zurück an die Firewall.

Stellen Sie sich die folgende Bereitstellung vor, bei der eine NetScaler-Appliance für die Forward-Proxy-Cache-Umleitung, eine Firewall und zwei Router (Router 1 und Router 2) konfiguriert ist. Der Netzwerkverkehr fließt jeweils über Router 1 zu Internet 1 und über Router 2 zu Internet 2.



In diesem Beispiel kommen Eingabeanforderungen von Clients von zwei verschiedenen VLANs, VLAN11 oder VLAN12. Die Client-IP-Adresse (10.0.0.0) wird wiederverwendet.
Basierend auf den Richtlinien für die Cache-Umleitung und den Content Switching kann die Anfrage direkt an den Ursprungsserver oder an die Firewall gesendet werden.

- Wenn die Anfrage die Firewall Bypass und ins Internet gehen muss, wird basierend auf dem Eingabeanforderungs-VLAN entweder Router 1 oder Router 2 ausgewählt und die Anfrage wird an Internet 1 oder Internet 2 gesendet.
- Wenn die Anfrage die Firewall passieren muss, muss die Quell-IP der Anfrage in eine bestimmte IP-Adresse übersetzt werden. Die übersetzte IP-Adresse kann verwendet werden, um das VLAN zu identifizieren, über das die Anfrage eingegangen ist. Wenn die Eingabeanforderung beispielsweise von VLAN11 kommt, wird die Quell-IP-Adresse in 11.x.x.x übersetzt. Wenn die Anfrage von VLAN12 kommt, wird die Quell-IP-Adresse in 12.x.x.x übersetzt.

Nachdem die Firewall die Anfrage verarbeitet hat, wird die Anfrage an die Appliance zurückgesendet. Mithilfe der Kombination aus Listen-Policy und Netzprofilen übersetzt die Appliance dann die Quell-IP-Adresse zurück in die ursprüngliche IP-Adresse und sendet die Anfrage basierend auf der eingegebenen VLAN-ID an Router 1 oder Router 2.

Hinweis: Der Modus des virtuellen Lastausgleichsservers, der an den Cache gebunden ist, muss immer auf den MAC-Modus eingestellt sein. Der IP-Modus für diese Funktion ist zwar nicht blockiert, die Einstellung auf den IP-Modus führt jedoch zu unerwartetem Verhalten.

Um die Ziel-IP-Adresse und die Portnummer der Anfrage mithilfe der CLI in die Ursprungs-IP-Adresse zu übersetzen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cr vserver <vsname> -useoriginIpPortForCache <YES|NO>
<!--NeedCopy-->
```

Beispiel:

```
set cr vserver cvsrv1 -useoriginIpPortForCache YES
<!--NeedCopy-->
```

Wenn useOriginIPPortForCache auf Ja gesetzt ist und die Anfrage von den zwischengespeicherten Servern bedient werden muss, wird die Ziel-IP der Anfrage in die IP-Adresse des Ursprungsservers übersetzt.

Hinweis: Wenn useOriginipPortForCache aktiviert ist, setzen Sie den virtuellen Lastausgleichsserver, der an den Cache gebunden ist, immer auf den MAC-Modus.

Um die Ziel-IP-Adresse und den Port der Anfrage mithilfe der GUI in die Ursprungs-IP-Adresse zu übersetzen

1. Navigieren Sie zu **Traffic Management** > **Cache-Umleitung** > **Virtuelle Server** und klicken Sie auf **Hinzufügen**.

2. Geben Sie die Details des virtuellen Servers für die Cache-Umleitung an.
3. Wählen Sie **Origin-IP-Port für Cache verwenden** aus, um die Übersetzung der Ziel-IP-Adresse der Anfrage in die Ursprungs-IP-Adresse zu aktivieren.
4. Klicken Sie auf **OK**.

Clustering

May 11, 2023

> **Hinweis**
>
> Diese Funktion ist mit einer Lizenz für NetScaler Advanced oder Premium Edition verfügbar.

Ein NetScaler Cluster ist eine Gruppe von nCore Appliances, die als einzelnes Systemimage zusammenarbeiten. Jede Appliance des Clusters wird als Knoten bezeichnet. Der Cluster kann eine Appliance oder bis zu 32 NetScaler nCore-Hardware oder virtuelle Appliances als Knoten haben.

Der Client-Verkehr wird zwischen den Knoten verteilt, um eine hohe Verfügbarkeit, einen hohen Durchsatz und Skalierbarkeit zu gewährleisten.

Um einen Cluster zu erstellen, müssen Sie die folgenden Schritte ausführen:

- Fügen Sie die Appliances als Clusterknoten hinzu.
- Richten Sie die Kommunikation zwischen den Knoten ein.
- Richten Sie Links zu den Client- und Servernetzwerken ein.
- Konfigurieren Sie die Appliances und konfigurieren Sie die Verteilung des Client- und Serververkehrs.

Unterstützbarkeitsmatrix für NetScaler-Cluster

May 11, 2023

Das Clustering in der NetScaler-Appliance unterstützt eine breite Verbreitung von Funktionen in NetScaler-Konfigurationen.

Die folgende Tabelle listet die NetScaler-Funktionen auf und enthält den Supportabilitätsstatus für verschiedene NetScaler-Versionen von Clustersetups. Der Unterstützungsstatus einiger NetScaler-Funktionen in einem NetScaler BLX-Cluster unterscheidet sich von dem eines NetScaler Nicht-BLX-Clusters (MPX oder VPX, SDX ADC).

> **Wichtig**
>
> Der Eintrag Node-Level in der Tabelle gibt an, dass die Funktion nur auf einzelnen Clusterknoten unterstützt wird.

NetScaler Funktionen	12.1	13	13.0 NetScaler BLX-Cluster	NetScaler 13.1	13.1 NetScaler BLX-Cluster
SSL FIPS	No	No	No	No	No
SSL-Zertifikat-Paket	No	No	No	No	No
SSL-Interception	No	No	No	No	No
Content Switching-Aktionen	Ja	Ja	Ja	Ja	Ja
Richtlinienbasi Protokol-lierung für Content Switching-Richtlinien	Ja	Ja	Ja	Ja	Ja
Ratenlimit	Ja	Ja	Ja	Ja	Ja
Action-Analytik	Ja	Ja	No	Ja	No
GSLB	Ja	Ja	Ja	Ja	Ja
RTSP	Ja	Ja	Ja	Ja	Ja
DNSSEC	No	No	No	No	No
DNS64	No	No	No	No	No
FTP	Ja	Ja	No	Ja	No
TFTP	Ja	Ja	Ja	Ja	Ja
Spiegelung von Verbindun-gen	No	No	No	No	No

NetScaler Funktionen	12.1	13	13.0 NetScaler BLX-Cluster	NetScaler 13.1	13.1 NetScaler BLX-Cluster
Integriertes Caching	Knotenebene	Knotenebene	No	Knotenebene	No
Großer gemeinsam genutzter Cache	Knotenebene	Knotenebene	No	Knotenebene	No
Front-End-Optimierung	Knotenebene	Knotenebene	No	Knotenebene	No
Anwendungs-Firewall	Ja	Ja	No	Ja	No
HTTP-Denial-of-Service-Schutz (HDOSP)	Veraltet	Veraltet	Veraltet	Entfernt	Veraltet
Prioritätswarteschlange (PQ)	Knotenebene	Knotenebene	Veraltet	Entfernt	Veraltet
Sicherer Anschluss (SC)	Knotenebene	Knotenebene	Veraltet	Entfernt	Veraltet
AppQoE	Ja	Ja	No	Ja	No
Überlastungssc	Knotenebene	Knotenebene	Ja	Knotenebene	Ja
MPTCP	Ja	Ja	No	Ja	No
Gestreifte SNIPs	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.

NetScaler Funktionen	12.1	13	13.0 NetScaler BLX-Cluster	NetScaler 13.1	13.1 NetScaler BLX-Cluster
MSR	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.
IS-IS (IPv4 und IPv6)	Ja	Ja	No	Ja	No
Jumbo Frames	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	No	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	No
IP-IP-Tunneling	Ja	Ja	No	Ja	No
Link-Lastenausgleich	Ja	Ja	Ja	Ja	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.
FIS (Failover-Schnittstellensa	Ja	Ja	No	Ja	No
Link-Redundanz (LR)	Ja	Ja	No	Ja	No
NAT46	No	Ja	Ja	Ja	Ja
NAT64	No	Ja	Ja	Ja	Ja
RNAT6	Ja	Ja	Ja	Ja	Ja

NetScaler Funktionen	12.1	13	13.0 NetScaler BLX-Cluster	NetScaler 13.1	13.1 NetScaler BLX-Cluster
LSN/CGNAT	Ja	Ja	No	Ja	No
IPv6 ReadyLogo	Ja	Ja	No	Ja	No
Traffic-Domänen	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	No	Ja; Hinweis: Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	No
Routenüberwac	Ja	Ja	Ja	Ja	Ja
GRE Tunnelbau (CB)	No	No	No	No	No
Modus Schicht 2	Ja	Ja	No	Ja	No
Netzprofile	Ja	Ja	No	Ja	No
HTTPS-Callout	Ja	Ja	Ja	Ja	Ja
AAA-TM	Ja	Ja	No	Ja	No
AppFlow	Knotenebene	Knotenebene	No	Knotenebene	No
Web Insight	Ja	Ja	No	Ja	No
HDX Insight	Ja	Ja	No	Ja	No
VMAC/VRRP	Ja	Ja	No	Ja	No
NetScaler Push	No	No	No	No	No
Stateful Verbindungs-Failover	No	No	No	No	No
Ordnungsgemä Herunter-fahren	Ja	Ja	Ja	Ja	Ja

NetScaler Funktionen	12.1	13	13.0 NetScaler BLX-Cluster	NetScaler 13.1	13.1 NetScaler BLX-Cluster
DBS Autoscale	No	Ja	Ja	Ja	Ja
DSR mit TOS	No	No	Ja	Ja	Ja
Finer Startup-RR Control	Knotenebene	Knotenebene	No	Knotenebene	No
XML XSM	No	No	No	No	No
DHCP RA	No	No	No	Ja	No
Bridge-Gruppe	Ja	Ja	No	Ja	No
Netzwerkbrücke	No	No	No	No	No
Webinterface auf NetScaler (WIonNS)	Ja	Ja	No	Ja	No
EdgeSight-Überwachung	Veraltet	Veraltet	No	Veraltet	No
Metrik-Tabellen - Lokal	No	No	No	No	No
DNS-Caching	Knotenebene	Knotenebene	Knotenebene	Knotenebene	Knotenebene
Call Home	Knotenebene	Knotenebene	No	Knotenebene	No
{{page.gateway-onprem}} ICA-Proxymodus	Ja	Ja	No	Ja	No
{{page.gateway-onprem}} (SSL-VPN/vollständig VPN und clientloses VPN)	Knotenebene	Knotenebene	No	Knotenebene	No

NetScaler Funktionen	12.1	13	13.0 NetScaler BLX-Cluster	NetScaler 13.1	13.1 NetScaler BLX-Cluster
Citrix CloudBridge Connector	Ja	Ja	No	Ja	No
Richtlinienbasi Routing (PBR/PBR6)	Ja	Ja	No	Ja	No
IPv4 Policy Based Routing (PBR) mit virtuellem LLB-Server als Next Hop	No	Ja	No	Ja	No
IPv6 Policy Based Routing (PBR6) mit virtuellem LLB-Server als Next Hop	No	No	No	No	No
Bekanntheit der Abonnenten	No	No	No	No	No
Dynamisches Routing	Ja mit Unterstützung von v6-Protokollen (ospfv3, RIPng, ISIS6, BGP6)	Ja mit Unterstützung von v6-Protokollen (ospfv3, RIPng, ISIS6, BGP6)	Ja	Ja mit Unterstützung von v6-Protokollen (ospfv3, RIPng, ISIS6, BGP6)	Ja

NetScaler Funktionen	12.1	13	13.0 NetScaler BLX-Cluster	NetScaler 13.1	13.1 NetScaler BLX-Cluster
SYSLOG-TCP, Lastausgleich von Syslog-Servern, SNIP-Unterstützung und FQDN-Unterstützung für syslog	Ja	Ja	Ja	Ja	Ja
Bot-Verwaltung	No	Ja	No	Ja	No
VXLAN	No	No	No	No	No
NSVLAN	Ja	Ja	No	Ja	Ja

Außerdem werden die folgenden NetScaler-Konfigurationen unterstützt:

Lastausgleich, Lastausgleichs-Persistenz, DNS-Lastausgleich, SIP, MaxClient, Spillover (Verbindung und dynamisch). Überlauf basierend auf Bandbreite, DataStream, Komprimierungskontrolle, Inhaltsfilterung, TCP-Pufferung, Cache-Umleitung, Distributed Denial-of-Service (DDoS). Client-Keep-Alive, Grundnetzwerk (IPv4 und IPv6), OSPF (IPv4 und IPv6), RIP (IPv4 und IPv6), RIP (IPv4 und IPv6). VLAN, ICMP, Fragmentierung, MBF, ACL, Simple ACL, MSR, Pfad-MTU-Entdeckung, IP-IP, SNMP, Richtlinien (klassisch und fortgeschritten). Rewrite, Responder, HTTP-Callout, Webserver-Protokollierung, Audit-Protokollierung (NSLOG und syslog). USIP, Ortungsbefehle, NITRO API, AppExpert, KRPC.

Außerdem werden die folgenden NetScaler-Konfigurationen unterstützt:

Lastausgleich, Lastausgleichs-Persistenz, DNS-Lastausgleich, SIP, MaxClient, Spillover (Verbindung und dynamisch). Überlauf basierend auf Bandbreite, DataStream, Komprimierungskontrolle, Inhaltsfilterung, TCP-Pufferung, Cache-Umleitung, Distributed Denial-of-Service (DDoS). Client-Keep-Alive, Grundnetzwerk (IPv4 und IPv6), OSPF (IPv4 und IPv6), RIP (IPv4 und IPv6), RIP (IPv4 und IPv6). VLAN, ICMP, Fragmentierung, MBF, ACL, Simple ACL, MSR, Pfad-MTU-Entdeckung, IP-IP, SNMP, Richtlinien (klassisch und fortgeschritten). Rewrite, Responder, HTTP-Callout, Webserver-Protokollierung, Audit-Protokollierung (NSLOG und syslog). USIP, Ortungsbefehle, NITRO API, AppExpert, KRPC.

Voraussetzungen

July 24, 2023

NetScaler-Appliances (MPX, VPX, SDX ADC, BLX), die einem Cluster hinzugefügt werden sollen, müssen die folgenden Voraussetzungen erfüllen:

- Alle Appliances müssen über die gleiche Softwareversion und den gleichen Build verfügen.
- Alle Appliances müssen vom gleichen Plattformtyp sein. Das bedeutet, dass ein Cluster entweder alle Hardware-Appliances (NetScaler MPX) oder alle NetScaler VPX-Appliances oder alle NetScaler BLX-Appliances oder alle NetScaler SDX ADC-Instanzen haben muss.

  Hinweis:

  - Für einen Cluster von Hardware-Appliances (MPX) müssen die Appliances vom selben Modelltyp sein.
  - Für die Bildung des heterogenen Clusters müssen alle Appliances vom MPX-Plattformtyp sein.
  - Für einen Cluster von virtuellen Appliances (VPX) müssen die Appliances auf den folgenden Hypervisoren bereitgestellt werden: XenServer, Hyper-V, VMware ESX und KVM.
  - Informationen zum Einrichten eines Clusters von SDX NetScaler-Instanzen finden Sie unter Einrichten eines Clusters von NetScaler-Instanzen.
  - Jumbo-Frames werden auf einem NetScaler Cluster unterstützt, der aus NetScaler SDX-Instanzen besteht.
  - Sie können L3-Cluster von SDX-Instanzen erstellen.
  - Informationen zum Einrichten eines NetScaler BLX-Clusters finden Sie unter NetScaler BLX-Cluster.
- Appliances können zu verschiedenen Netzwerken gehören.
- Zunächst konfiguriert und mit einem gemeinsamen clientseitigen und serverseitigen Netzwerk verbunden werden.
- Für einen Cluster virtueller Appliances (NetScaler VPX oder NetScaler BLX oder NetScaler SDX ADC-Instanz) mit großen Konfigurationen wird empfohlen, 6 GB RAM für jeden Knoten des Clusters zu verwenden.

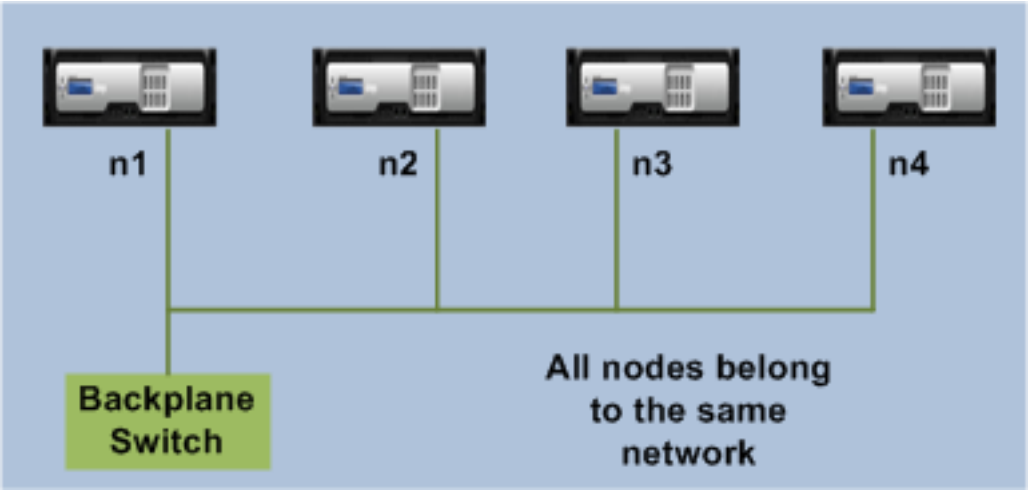
Cluster-Überblick

May 11, 2023

Ein NetScaler-Cluster wird gebildet, indem NetScaler-Appliances gruppiert werden. Basierend auf dem Netzwerkstandort der NetScaler-Appliances, die Sie den Cluster hinzufügen möchten, müssen Sie die folgenden Cluster-Setups kennen:

> **Hinweis**
>
> Sofern nicht anders angegeben, sind die Clusterfunktionen und -konfigurationen für L2- und L3-Cluster identisch.

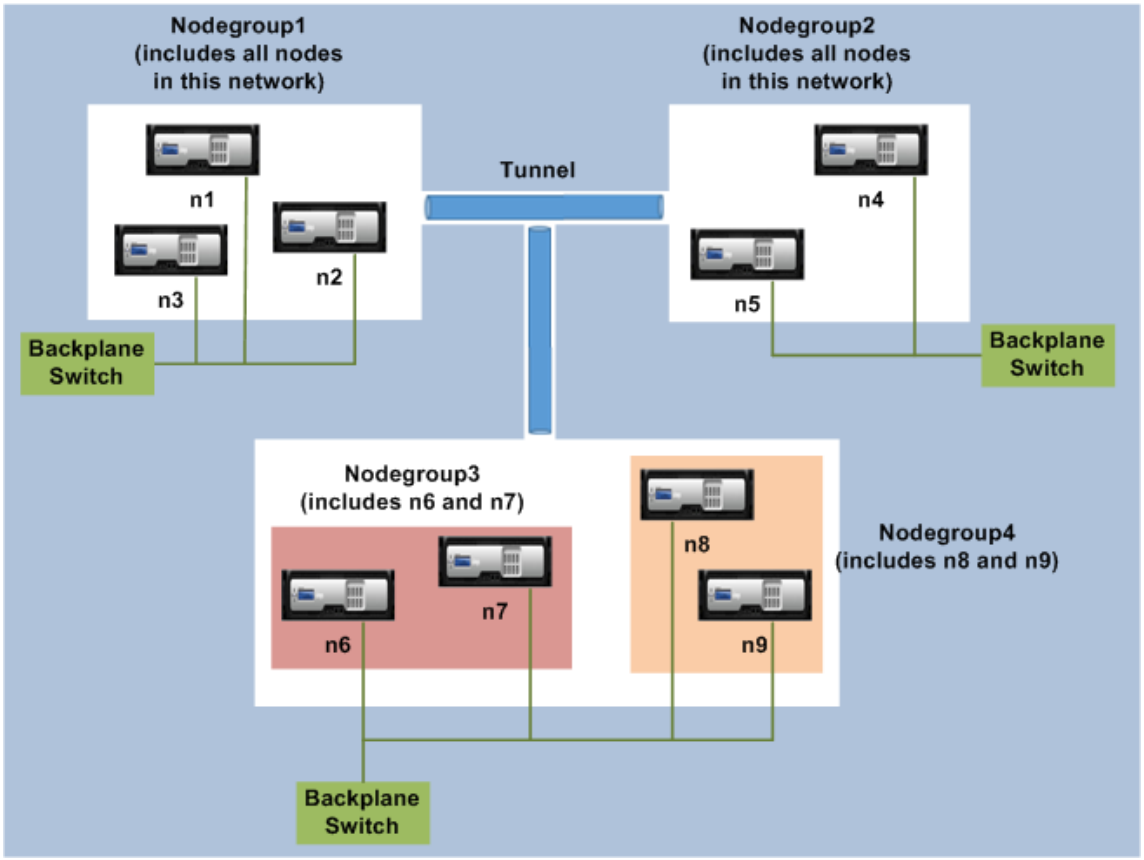
- **L2-Cluster:** In dieser Cluster-Bereitstellung gehören alle Clusterknoten demselben Netzwerk an.



- **L3-Cluster (auch als „Cluster im INC-Modus“ bezeichnet):** In dieser Cluster-Bereitstellung können Clusterknoten verschiedenen Netzwerken angehören. Die Clusterknoten eines bestimmten Netzwerks müssen in Knotengruppen gruppiert werden, die nur Knoten aus diesem Netzwerk enthalten. Aus der folgenden Abbildung sehen wir, dass sich die Knoten n1, n2, n3 im selben Netzwerk befinden und in Nodegroup1 gruppiert sind.

  Ähnlich gilt für die Knoten n4 und n5, die in Nodegroup2 gruppiert sind. Im dritten Netzwerk gibt es zwei Knotengruppen. Nodegroup3 umfasst n6 und n7 und Nodegroup4 umfasst n8 und n9.

  > **Hinweis**
  >
  > Wird ab NetScaler 11.0 unterstützt.

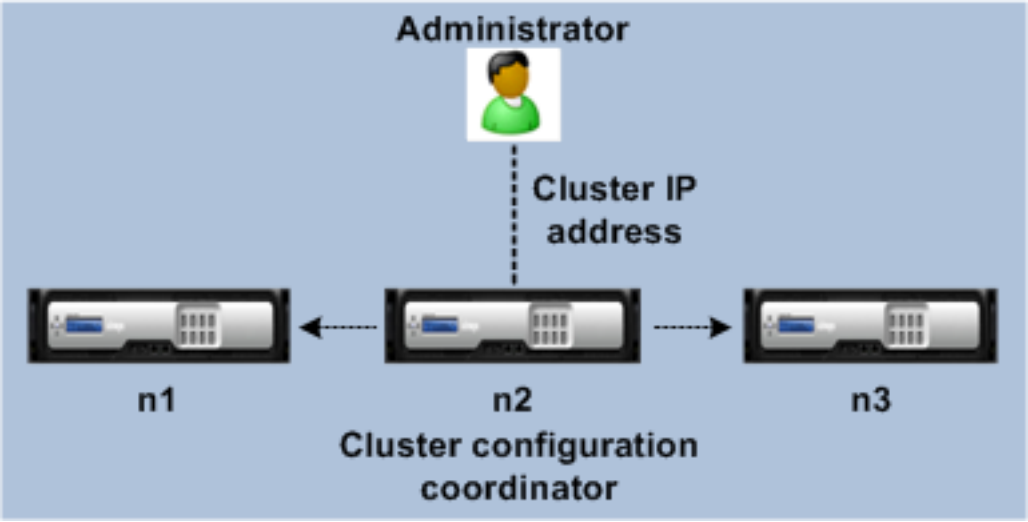


- **Sync-Status:** Der Befehl **show cluster** zeigt den Status des Clusterknotens an. Im Folgenden sind die Synchronisierungszustände für den Befehl **show cluster node** aufgeführt:
  - **Aktiviert:**Dieser Status zeigt, dass der Knoten in der Lage ist, eine Konfigurationssynchronisierung von anderen Knoten aus durchzuführen.
  - In**Bearbeitung:** Dies ist ein temporärer Status, der angezeigt wird, wenn der Knoten Konfigurationen von anderen Knoten synchronisiert.
  - **Erfolgreich:** Dieser Status steht für den Status der letzten Synchronisierung, die auf diesem Knoten stattgefunden hat.

Synchronisation über Clusterknoten hinweg

May 11, 2023

Alle Konfigurationen auf einem NetScaler-Cluster werden an der Cluster-IP-Adresse durchgeführt, die die Verwaltungsadresse des Clusters ist. Der Clusterknoten besitzt die Cluster-IP-Adresse, die als Clusterkonfigurationskoordinator (CCO) bezeichnet wird, wie in der folgenden Abbildung dargestellt:



Die Konfigurationen, die auf dem CCO verfügbar sind, werden automatisch an die anderen Clusterknoten weitergegeben, sodass alle Clusterknoten dieselben Konfigurationen haben.

- Mit NetScaler können nur wenige Konfigurationen auf einzelnen Clusterknoten über ihre NSIP-Adresse durchgeführt werden. In diesen Fällen müssen Sie die Konfigurationskonsistenz für alle Knoten im Cluster manuell sicherstellen. Diese Konfigurationen werden nicht über die anderen Clusterknoten verteilt. Weitere Informationen zu Operationen, die auf jedem Clusterknoten unterstützt werden, finden Sie unter Auf einzelnen Clusterknoten unterstützte Vorgänge.
- Die folgenden Befehle, wenn sie auf der Cluster-IP-Adresse ausgeführt werden, werden nicht an andere Clusterknoten weitergegeben:
  - **Abschaltung.** Schaltet nur den Konfigurationskoordinator herunter.
  - **neustarten.** Startet nur den Konfigurationskoordinator neu.
  - **RM-Cluster-Instanz.** Entfernt die Clusterinstanz von dem Knoten, auf dem Sie den Befehl ausführen.
- Für einen Befehl, der an andere Clusterknoten weitergegeben werden soll, gehen Sie wie folgt vor:
  - Das Quorum muss auf der Cluster-Instance konfiguriert werden.
  - Das Cluster-Quorum mit (n/2 + 1) der Clusterknoten muss größtenteils aktiv sein, damit der Cluster betriebsbereit ist.
  - Ein Cluster kann mit einer Mindestanzahl von Knoten ausgeführt werden, wenn die Mehrheitsregel (n/2 + 1) gelockert wird.

Wenn ein Knoten zu einem Cluster hinzugefügt wird, werden die Konfigurationen und die Dateien (SSL-Zertifikate, Lizenzen, DNS usw.), die auf dem CCO verfügbar sind, mit dem neu hinzugefügten Clusterknoten synchronisiert. Wenn ein vorhandener Clusterknoten, der absichtlich deaktiviert wurde oder ausgefallen ist, erneut hinzugefügt wird, vergleicht der Cluster die auf dem Knoten verfügbaren Konfigurationen mit den auf dem CCO verfügbaren Konfigurationen. Wenn die Konfigurationen nicht übereinstimmen, wird der Knoten mithilfe einer der folgenden Methoden synchronisiert:

- **Vollständige Synchronisation.** Wenn der Unterschied zwischen den Konfigurationen 255 Befehle übersteigt, werden alle Konfigurationen des CCO auf den Knoten angewendet, der dem Cluster wieder beitritt. Der Knoten bleibt während der Synchronisation betriebsbereit nicht verfügbar.
- **Inkrementelle Synchronisation.** Wenn der Unterschied zwischen den Konfigurationen kleiner oder gleich 255 Befehlen ist, werden nur die Konfigurationen, die nicht verfügbar sind, auf den Knoten angewendet, der dem Cluster wieder beitritt. Der Betriebszustand des Knotens bleibt davon unberührt.

> **Hinweis**
>
> Sie können die Konfigurationen und Dateien auch manuell synchronisieren. Weitere Informationen finden Sie unterClusterkonfigurationen synchronisieren und Clusterdateien synchronisieren.

Striped-, Teil-Striped- und Spotted-Konfigurationen

August 19, 2021

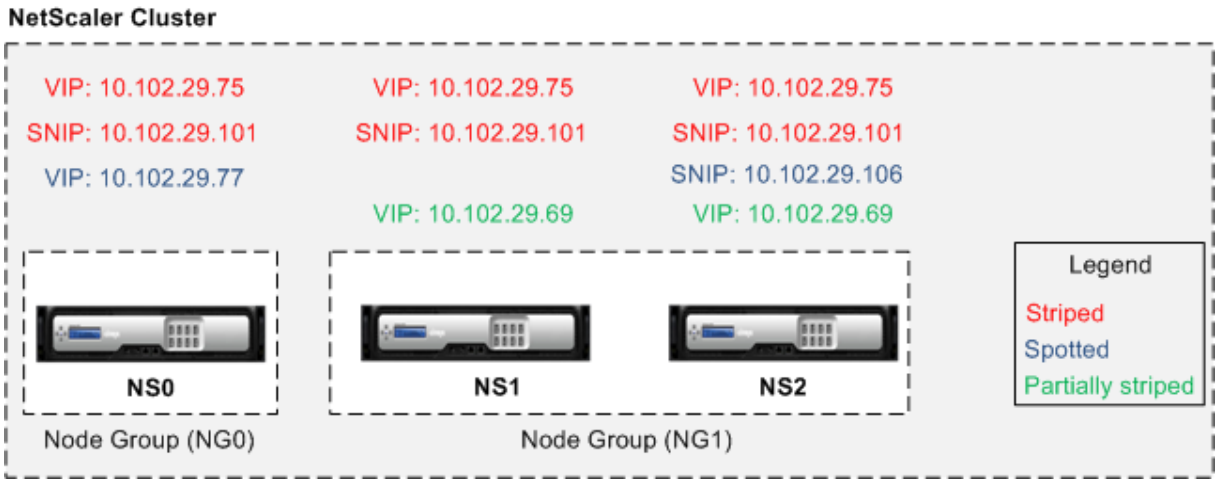
Aufgrund der Befehlsausbreitung haben alle Knoten in einem Cluster die gleichen Konfigurationen. Möglicherweise möchten Sie jedoch, dass einige Konfigurationen nur auf bestimmten Clusterknoten verfügbar sind. Obwohl Sie die Knoten, auf denen die Konfigurationen verfügbar sind, nicht einschränken können, können Sie die Knoten angeben, auf denen die Konfigurationen aktiv sind.

Beispiel:

- definieren Sie eine SNIP-Adresse, die nur auf einem Knoten aktiv ist, oder
- definieren Sie eine SNIP-Adresse, die auf allen Knoten aktiv ist, oder
- definieren Sie eine VIP-Adresse, die nur auf einem Knoten aktiv ist, oder
- eine VIP-Adresse definieren, die auf allen Knoten aktiv ist, oder
- Definieren Sie eine VIP-Adresse, die nur auf zwei Knoten eines 3-Knoten-Clusters aktiv ist

Abhängig von der Anzahl der Knoten, auf denen die Konfigurationen aktiv sind, werden Clusterkonfigurationen als gestreifte, teilweise gestreifte oder gepunktete Konfigurationen bezeichnet.

Abbildung 1. Cluster mit drei Knoten mit Striped-, Teil-Striped- und Spotted-Konfigurationen



Die folgende Tabelle enthält weitere Details zu den Konfigurationstypen:

Konfigurationstyp	Aktiv auf	Anwendbar für	Konfigurationen
Stripesetkonfiguration	Alle Clusterknoten	Alle Einträge	Es ist keine spezifische Konfiguration erforderlich, um eine Entität Striped zu erstellen. Standardmäßig werden alle Entitäten, die für eine Cluster-IP-Adresse definiert sind, auf allen Clusterknoten gestreift.
Teilweise gestreifte Konfiguration	Eine Teilmenge von Clusterknoten	Siehe Cluster-Knotengruppen.	Binden Sie die Entitäten, die teilweise gestreift werden sollen, an eine Knotengruppe. Die Konfiguration ist nur auf den Clusterknoten aktiv, die zur Knotengruppe gehören.

Konfigurationstyp	Aktiv auf	Anwendbar für	Konfigurationen
Spotted Konfiguration	Einzelner Clusterknoten	SNIP-Adresse, SNMP-Engine-ID, Hostname von Clusterknoten, Entitäten, die an eine Knotengruppe gebunden werden können	Eine Spotted-Konfiguration kann mit einem von zwei Ansätzen definiert werden. **SNIP-Adresse** Geben Sie beim Erstellen der SNIP-Adresse den Knoten an, auf dem die SNIP-Adresse aktiv sein soll, als Eigentümerknoten an. **Beispiel:** `add ns ip 10.102.29.106 255.255.255.0 -type SNIP -ownerNode 2` (vorausgesetzt, der NS2-ID ist 2). **Hinweis**: Sie können den Besitz einer Spotted-SNIP-Adresse zur Laufzeit nicht ändern. Um den Besitz zu ändern, müssen Sie zuerst die SNIP-Adresse löschen und sie erneut hinzufügen, indem Sie den neuen Besitzer angeben. **Entitäten, die an eine Knotengruppe gebunden werden können.** Durch Bindung der Entität an eine Knotengruppe mit einem einzelnen Mitglied.

Konfigurationstyp	Aktiv auf	Anwendbar für	Konfigurationen

Hinweis:

- Wenn Sie USIP deaktivieren, empfiehlt Citrix die Verwendung von Spotted-SNIP-Adressen. Sie können Striped SNIP-Adressen nur verwenden, wenn IP-Adressen fehlen. Die Verwendung von Striped-IP-Adressen kann zu ARP-Flussproblemen führen, wenn für die ARP-Auflösung keine Spotted-IP-Adressen im selben Subnetz vorhanden sind.
- Wenn Sie USIP aktivieren, empfiehlt Citrix, Striped SNIP-Adressen als Gateway für serverinitiierten Datenverkehr zu verwenden.

ARP-Besitzer-Unterstützung für Striped IP

In einem Cluster-Setup können Sie einen bestimmten Knoten so konfigurieren, dass er auf die ARP-Anforderung für eine Stripeset-IP antwortet. Der konfigurierte Knoten reagiert auf den ARP-Datenverkehr.

Ein neuer Parameter “ArPowner” wird in den Befehlen “IP hinzufügen, setzen und nicht gesetzt” eingeführt.

So aktivieren Sie den ARP-Besitzer auf einem Knoten mit der CLI.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip <ip_address> -arpOwner <node_id>
```

Hinweis:

Der ARP-Besitzerparameter wird nur im L2-Cluster unterstützt.

Unterstützung für Nachbarerkennungseigentümer für gestreifte IPv6-Adresse

In einem Cluster-Setup können Sie einen bestimmten Knoten als Neighbor Discovery (ND)-Besitzer für die Striped IPv6-Adresse konfigurieren, um die Link-Layer-Adresse zu bestimmen. Ein Client sendet eine Neighbor Solicitation (NS)-Nachricht an alle Knoten im Cluster-Setup. Der ND-Besitzer antwortet mit einer Neighbor Advertisement (NA)-Nachricht mit der Link-Layer-Adresse für die Striped IPv6-Adresse und dient dem Datenverkehr.

So aktivieren Sie ND-Besitzer auf einem Knoten über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add ns ip6 <IPv6Address> -ndOwner <node id>

set  ns ip6 <IPv6Address> -ndOwner <node id>
<!--NeedCopy-->
```

Beispiel:

```
add ns ip6 2001::21/64 -ndOwner 1

set ns ip6 2001::21/64 -ndOwner 1
<!--NeedCopy-->
```

So aktivieren Sie den ND-Besitzer auf einem Knoten mit der GUI

1. Navigieren Sie zu **System > Netzwerk > IPs**.
2. Wechseln Sie auf der **IPs-Seite** zur Registerkarte **IPv6s** und klicken Sie auf **Hinzufügen**.
3. Wählen **Sie auf der Seite IPv6 erstellen** eine der Knoten-IDs aus, die im Dropdownmenü **NDOwner im Cluster** aufgeführt sind.

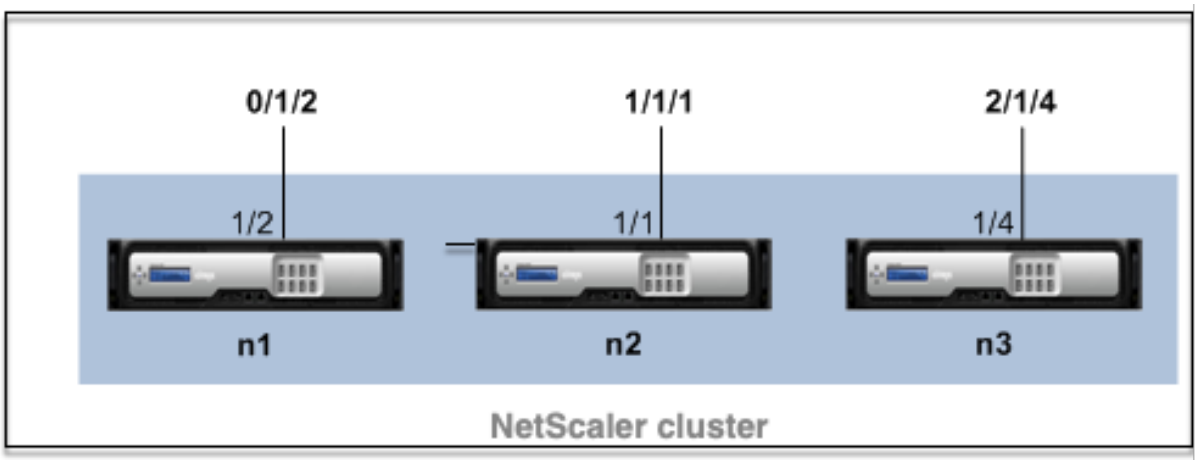
> **Hinweis:**
>
> Der ND-Besitzerparameter wird nur im L2-Cluster unterstützt.

Kommunikation in einem Cluster-Setup

May 11, 2023

Den Schnittstellen von NetScaler-Appliances, die einem Cluster hinzugefügt werden, ist eine Knoten-ID vorangestellt. Es hilft dabei, den Clusterknoten zu identifizieren, zu dem die Schnittstelle gehört. Daher wird aus der Schnittstellenkennung c/u, wobei c die Controller-Nummer und u die Einheitennummer ist, nun n/c/u, wobei n die Knoten-ID ist. In der folgenden Abbildung wird beispielsweise die Schnittstelle 1/2 des Knotens n1 als 0/1/2, die Schnittstelle 1/1 des Knotens n2 als 1/1/1 und die Schnittstelle 1/4 des Knotens n3 als 2/1/4 dargestellt.

Abbildung 1. Benennungskonvention für Schnittstellen in einem Cluster



- **Serverkommunikation**—
  Der Cluster kommuniziert mit dem Server über die physischen Verbindungen zwischen dem Clusterknoten und dem serverseitigen Verbindungsgerät. Die logische Gruppierung dieser physikalischen Verbindungen wird als Serverdatenebenebezeichnet.
- **Client-Kommunikation**— Der Cluster kommuniziert mit dem Client über die physischen Verbindungen zwischen dem Clusterknoten und dem clientseitigen Verbindungsgerät. Die logische Gruppierung dieser physischen Verbindungen wird als Client-Datenebene bezeichnet.
- **Kommunikation zwischen den Knoten**— Die Clusterknoten können auch miteinander kommunizieren. Die Art und Weise, wie sie kommunizieren, hängt davon ab, ob sich der Knoten im selben Netzwerk oder netzwerkübergreifend befindet.
  - Clusterknoten innerhalb desselben Netzwerks kommunizieren miteinander, indem sie die Cluster-Backplane verwenden. Die Backplane besteht aus einer Reihe von Schnittstellen, bei denen eine Schnittstelle jedes Knotens mit einem gemeinsamen Switch verbunden ist, der als Cluster-Backplane-Switch bezeichnet wird. Die verschiedenen Arten von Verkehr, der über die Backplane geleitet wird, die für die Kommunikation zwischen den Knoten verwendet wird, sind:
    * Node-zu-Knoten-Messaging (NNM)
    * Gelenkter Verkehr
    * Weitergabe und Synchronisation der Konfiguration
  - Jeder Knoten des Clusters verwendet eine spezielle MAC-Cluster-Backplane-Switch-Adresse, um über die Backplane mit anderen Knoten zu kommunizieren. Der Cluster-Spezial-MAC hat das Format: `0x02 0x00 0x6F <cluster_id> <node_id > <reserved>)`, wobei `cluster_id` die Cluster-Instanz-ID die Knotennummer der NetScaler-Appliance ist, die einem Cluster hinzugefügt wird. `node_id`

Die folgenden Abbildungen zeigen die Kommunikationsschnittstellen in L2-Clustern und L3-Clustern.

Abbildung 2. Cluster-Kommunikationsschnittstellen - L2-Cluster

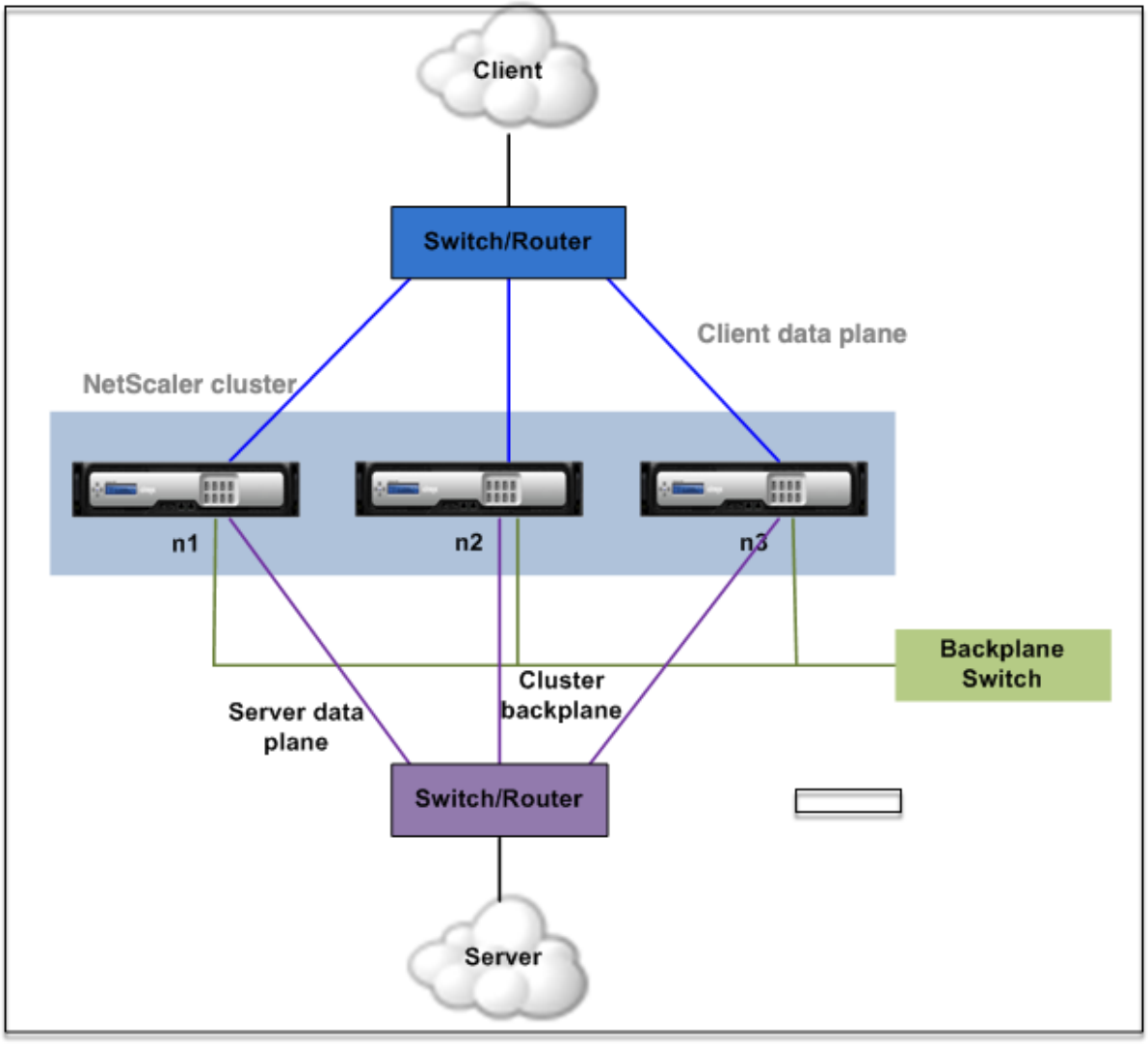
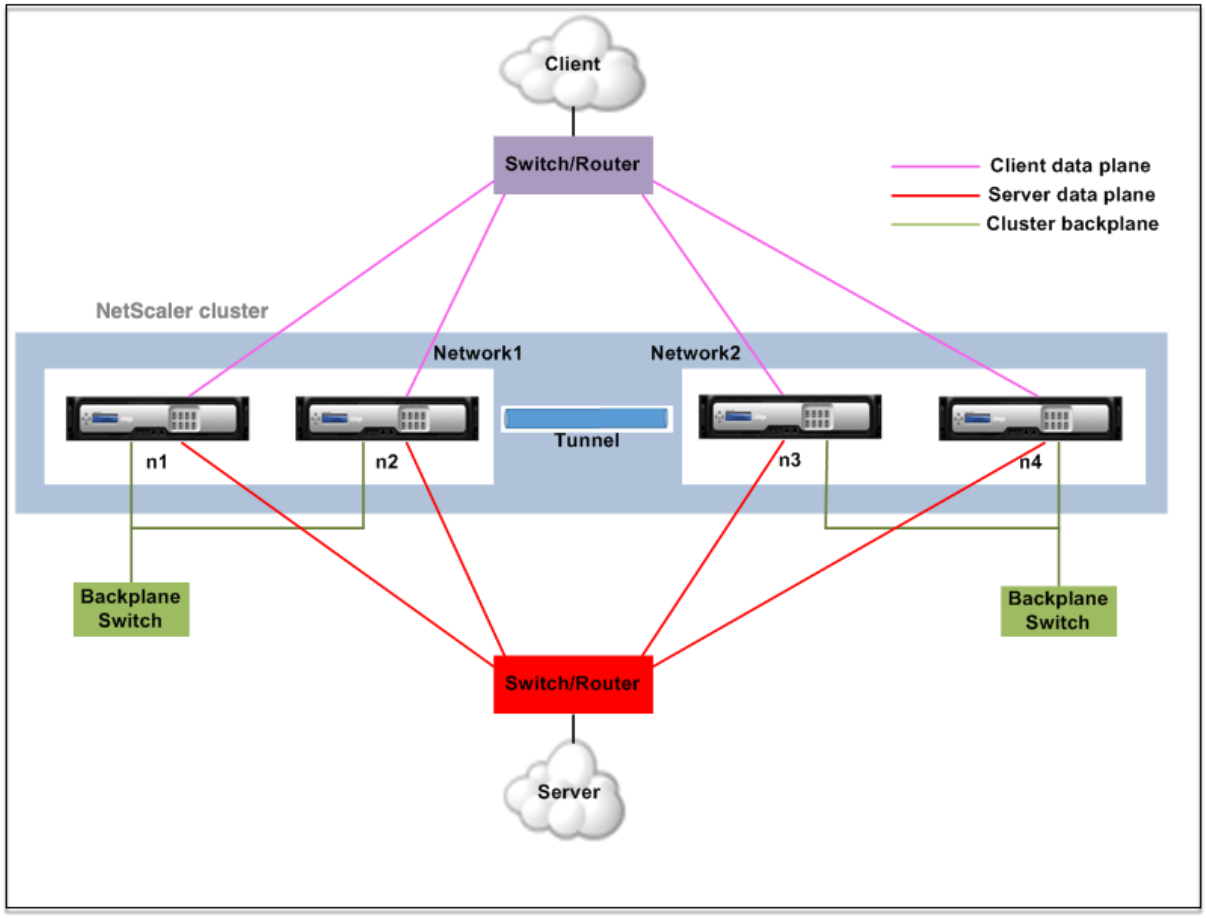


Abbildung 3. Cluster-Kommunikationsschnittstellen - L3-Cluster



Verkehrsverteilung in einem Cluster-Setup

May 11, 2023

In einem Cluster-Setup zeigen externe Netzwerke die Sammlung von NetScaler Appliances als einzelne Entität an. Daher muss der Cluster einen einzelnen Knoten auswählen, der den Datenverkehr empfangen muss. Der Cluster trifft diese Auswahl, indem er den Equal Cost Multiple Path (ECMP) oder den Mechanismus zur Verteilung des Datenverkehrs auf Cluster-Link-Aggregation verwendet. Der ausgewählte Knoten wird als Flow Receiver bezeichnet.

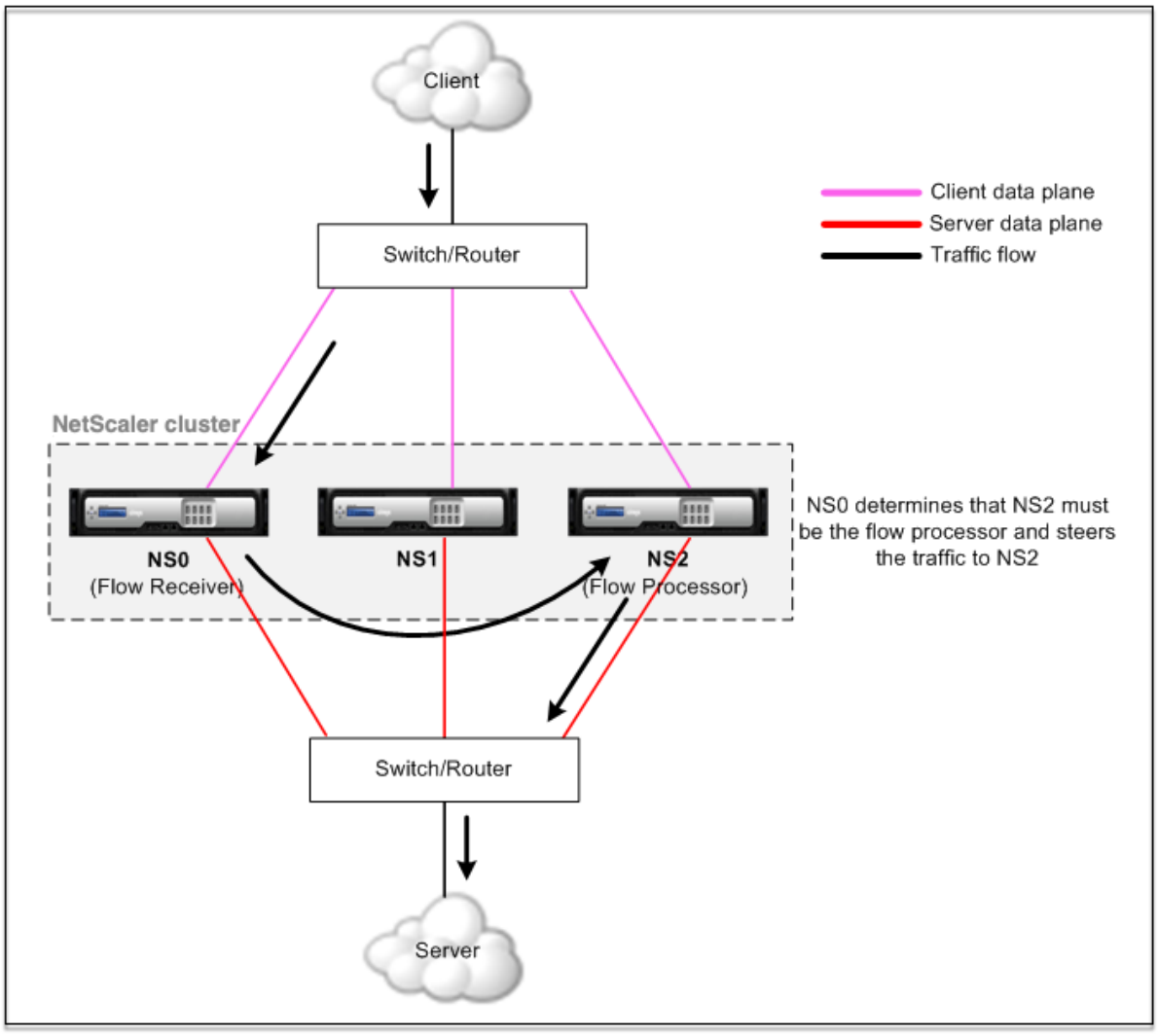
> **Hinweis**
>
> Für einen L3-Cluster (Knoten in verschiedenen Netzwerken) kann nur die ECMP-Verkehrsverteilung verwendet werden.

Der Flow-Empfänger erhält den Datenverkehr und bestimmt dann mithilfe der internen Clusterlogik den Knoten, der den Verkehr verarbeiten muss. Dieser Knoten wird als Flow-Prozessor bezeichnet. Der Flow-Empfänger leitet den Datenverkehr über die Backplane zum Flow-Prozessor, wenn sich der

Flow-Receiver und der Flow-Prozessor im selben Netzwerk befinden. Der Verkehr wird durch den Tunnel geleitet, wenn sich der Flow-Empfänger und der Flow-Prozessor in unterschiedlichen Netzwerken befinden.

> **Hinweis**
>
> - Der Flow-Empfänger und der Flow-Prozessor müssen Knoten sein, die Datenverkehr verarbeiten können.
> - Ab NetScaler 11 können Sie die Steuerung auf der Cluster-Backplane deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der Lenkung auf der Cluster-Backplane.

Abbildung 1. Datenverkehrsverteilung in einem Cluster



Die vorangehende Abbildung zeigt eine Client-Anfrage, die durch den Cluster fließt. Der Client sendet eine Anfrage an eine virtuelle IP-Adresse (VIP). Ein auf der Client-Datenebene konfigurierter Mechanismus zur Verkehrsverteilung wählt einen der Clusterknoten als Flow-Empfänger aus. Der Flussempfänger empfängt den Datenverkehr, bestimmt den Knoten, der den Datenverkehr verar-

beiten muss, und steuert die Anforderung an diesen Knoten (es sei denn, der Flow-Empfänger wählt sich selbst als Flow-Prozessor aus).

Der Flow-Prozessor stellt eine Verbindung mit dem Server her. Der Server verarbeitet die Anforderung und sendet die Antwort an die Subnetz-IP-Adresse (SNIP), die die Anforderung an den Server gesendet hat.

- Wenn es sich bei der SNIP-Adresse um eine gestreifte oder teilweise Striped-IP-Adresse handelt, wählt der auf der Serverdatenebene konfigurierte Verkehrsverteilungsmechanismus einen der Clusterknoten als Flow-Empfänger aus. Der Flow-Empfänger empfängt den Datenverkehr, bestimmt den Flow-Prozessor und leitet die Anfrage über die Cluster-Backplane an den Flow-Prozessor weiter.
- Wenn es sich bei der SNIP-Adresse um eine entdeckte IP-Adresse handelt, erhält der Knoten, dem die SNIP-Adresse gehört, die Antwort vom Server.

In einer asymmetrischen Cluster-Topologie (alle Clusterknoten sind nicht mit dem externen Switch verbunden) müssen Sie Linksets entweder ausschließlich oder in Kombination mit ECMP- oder Clusterlinkaggregation verwenden. Weitere Informationen finden Sie unter Verwenden von Linksets.

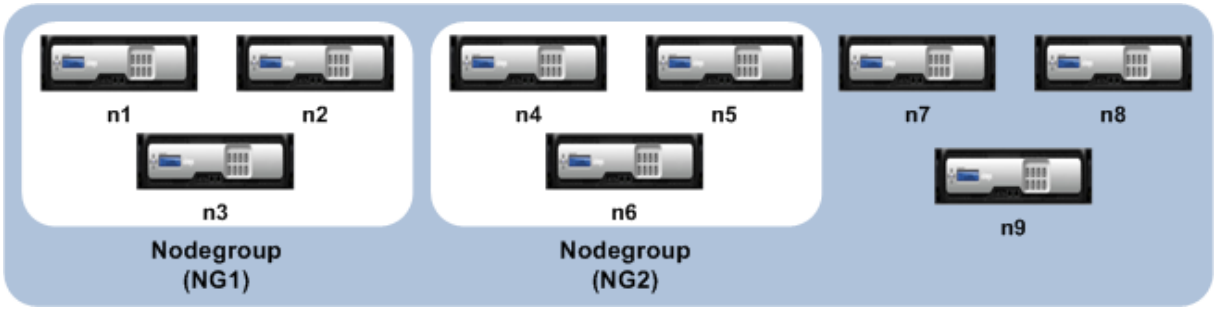
Clusterknotengruppen

May 11, 2023

> **Hinweis**
>
> Knotengruppen werden ab NetScaler 10.1 unterstützt.

Wie der Name schon sagt, ist eine Clusterknotengruppe eine Gruppe von Clusterknoten.

Abbildung 1. NetScaler-Cluster mit Knotengruppen



Die obige Abbildung zeigt einen Cluster mit den Knotengruppen NG1 und NG2, die jeweils 3 Clusterknoten enthalten. Der Cluster hat außerdem 3 Knoten, die keiner Knotengruppe angehören.

Eine Knotengruppe kann für Folgendes konfiguriert werden:

- Definieren von Spotted- und Teil-Striped-Konfigurationen. Weitere Informationen finden Sie unter Knotengruppen für Spotted und Partiell Striped Configurations.
- So konfigurieren Sie Redundanz von Knotengruppen. Weitere Informationen finden Sie unter Konfigurieren von Redundanz für Knotengruppen.
  Hinweis: Unterstützt ab NetScaler 10.5 Build 52.1115.e.
- Um einen L3-Cluster zu definieren (im INC-Modus auch Cluster genannt). In einem L3-Cluster können Clusterknoten aus verschiedenen Netzwerken stammen. Sie müssen Knoten, die zu einem Netzwerk gehören, in einer einzigen Knotengruppe gruppieren. Wenn beispielsweise n1, n2, n3 in netzwerk1 und n4, n5, n6 sind in netzwerk2, dann muss NG1 Knoten von netzwerk1 und NG2 müssen Knoten von netzwerk2 enthalten. Informationen zum Einrichten eines L3-Clusters finden Sie unter Erstellen eines NetScaler-Clusters.

> **Hinweis**
>
> - Wird ab NetScaler 11 unterstützt.
> - Die vorherigen Funktionen einer Knotengruppe schließen sich gegenseitig aus. Dies bedeutet, dass eine Knotengruppe nur eine der oben genannten Funktionen bereitstellen kann.

Cluster- und Knotenstatus

August 19, 2021

Damit ein Cluster funktionsfähig ist, müssen die meisten Knoten (n/2 + 1) operativ aktiv sein (der Betriebszustand ist ACTIVE).

> **Wichtig**
>
> Ab NetScaler Release 10.5 können Sie den Cluster so konfigurieren, dass er funktionsfähig ist, auch wenn die Mehrheitskriterien nicht erfüllt sind. Diese Konfiguration muss beim Erstellen eines Clusters durchgeführt werden.

Weitere Informationen zu den Status eines Clusterknotens finden Sie unter Status eines Clusterknotens.

Routing in einem Cluster

May 11, 2023

Das Routing in einem Cluster funktioniert ähnlich wie das Routing in einem eigenständigen System. Ein paar Punkte, die es zu beachten gilt:

- Alle Routing-Konfigurationen müssen von der Cluster-IP-Adresse aus durchgeführt werden, und die Konfigurationen werden an die anderen Clusterknoten weitergegeben.
- Routen sind auf die maximale Anzahl von ECMP-Routen begrenzt, die vom Upstream-Router unterstützt werden.
- Knotenspezifische Routing-Konfigurationen müssen mit dem Argument owner-node wie folgt durchgeführt werden:

```
  router ospf
    owner-node 0
      ospf router-id 97.131.0.1
    exit-owner-node
  !
<!--NeedCopy-->
```

Der folgende Befehl zeigt die konsolidierte Clusterkonfiguration für alle Knoten in VTYSH an.

```
show cluster-config
```

Der folgende Befehl zeigt den Clusterstatus auf jedem Knoten an.

```
show cluser node
```

IPv4-Routing im L2-Cluster

Der folgende Abschnitt enthält Beispielkonfigurationen, die Ihnen bei der Konfiguration von IPv4-OSPF- und BGP-Routing im L2-Cluster helfen.

Hinzufügen einer erkannten SNIP-Adresse und Aktivieren von dynamischem Routing

In der folgenden Konfiguration sind OSPF- und BGP-Routing aktiviert. Außerdem werden entdeckte SNIP-Adressen hinzugefügt und dynamisches Routing ist für diese SNIP-Adressen aktiviert.

```
en ns fea ospf bgp
add vlan 10
add ns ip 10.10.10.1 255.255.255.0 -dynamicrouting enabled -ownernode 1
add ns ip 10.10.10.2 255.255.255.0 -dynamicrouting enabled -ownernode 2
add ns ip 10.10.10.3 255.255.255.0 -dynamicrouting enabled -ownernode 3
bind vlan 10 -ipaddress 10.10.10.1 255.255.255.0
<!--NeedCopy-->
```

VTYSH IPv4-OSPF-Konfiguration

Um IPv4-OSPF im L2-Cluster zu konfigurieren, müssen Sie:

- Setzen Sie die Priorität auf Null.
- Konfigurieren Sie die Router-ID als Spott-Konfiguration.

> **Hinweis**
>
> Die OSPF-Konfigurationsrichtlinien für den L2-Cluster gelten auch für OSPFv3.

In der folgenden Beispielkonfiguration ist IPv4 OSPF konfiguriert.

```
       interface vlan10
        IP OSPF PRIORITY 0
        !
       router ospf
           owner-node 1
             ospf router-id 97.131.0.1
           exit-owner-node
           owner-node 2
             ospf router-id 97.131.0.2
           exit-owner-node
           owner-node 3
             ospf router-id 97.131.0.3
           exit-owner-node
       network 10.10.10.0/24 area 0
       redistribute kernel
        !
<!--NeedCopy-->
```

VTYSH IPv4-BGP-Konfiguration

In der folgenden VTYSH-Beispielkonfiguration ist IPv4-BGP konfiguriert.

```
     router bgp 100
       neighbor 10.10.10.10 remote-as 200
      owner-node 1
       neighbor 10.10.10.10 update-source 10.10.10.1
      exit-owner-node
      owner-node 2
       neighbor 10.10.10.10 update-source 10.10.10.2
      exit-owner-node
      owner-node 3
       neighbor 10.10.10.10 update-source 10.10.10.3
      exit-owner-node
     redistribute kernel
     !
<!--NeedCopy-->
```


> **Hinweis**
>
> Der Befehl update-source wird für jeden Nachbarn mit dem Argument owner-node in der folgenden Konfiguration verwendet, um eine Verbindung mit der richtigen Quell-IP herzustellen.

IPv6-Routing im L2-Cluster

Der folgende Abschnitt enthält Beispielkonfigurationen, die Ihnen bei der Konfiguration von IPv6-OSPF- und BGP-Routing im L2-Cluster helfen.

IPv6-Routing aktivieren

Bevor Sie IPv6-Routing in einem L2-Cluster konfigurieren, müssen Sie die IPv6-Funktion aktivieren.

Um IPv6-Routing mithilfe der CLI zu aktivieren,

Geben Sie in der Befehlszeile Folgendes ein:

- `enable ns fea ipv6pt`

Hinzufügen einer erkannten SNIP6-Adresse und Aktivieren von dynamischem Routing

In der folgenden Konfiguration sind OSPF- und BGP-Routing aktiviert. Außerdem werden entdeckte SNIP6-Adressen hinzugefügt und dynamisches Routing ist für diese SNIP6-Adressen aktiviert.

```
add ns ip6 3ffa::1/64 -dynamicrouting enabled -ownernode 1
add ns ip6 3ffa::2/64 -dynamicrouting enabled -ownernode 2
add ns ip6 3ffa::3/64 -dynamicrouting enabled -ownernode 3
add vlan 10
bind vlan 10 -ipaddress 3ffa::1/64
<!--NeedCopy-->
```

VTYSH IPv6-BGP-Konfiguration

In der folgenden VTYSH-Beispielkonfiguration ist IPv6-BGP konfiguriert.

```
  router bgp 100
   neighbor 3ffa::10 remote-as 200
     owner-node 1
      neighbor 3ffa::10 update-source 3ffa::1
     exit-owner-node
     owner-node-2
      neighbor 3ffa::10 update-source 3ffa::2
     exit-owner-node
```



```
9       owner-node-3
10       neighbor 3ffa::10 update-source 3ffa::3
11      exit-owner-node
12    no neighbor 3ffa::10 activate
13    address-family ipv6
14     redistribute kernel
15     neighbor 3ffa::10 activate
16    exit-address-family
17   !
18 <!--NeedCopy-->
```

Gelernte IPv6-Routen installieren

Der NetScaler-Cluster kann Routen verwenden, die von verschiedenen Routing-Protokollen gelernt wurden, nachdem Sie die Routen in der NetScaler-Cluster-Routingtabelle installiert haben.

Gehen Sie wie folgt vor, um erlernte IPv6-Routen in die interne Routingtabelle mithilfe der CLI zu installieren:

Geben Sie in der Befehlszeile Folgendes ein:

- `ns route-install ipv6 bgp`
- `ns route-install ipv6 ospf`
- `ns route-install default`

> **Hinweis**
>
> - Wenn Sie IPv4-Routen auf einem IPv6-Nachbarn austauschen müssen, müssen Sie den Befehl `no neighbor 3ffa::10 active` VTYSH aus der früheren Konfiguration entfernen.
> - Der `update-source` VTYSH-Befehl muss für jeden Besitzerknoten verwendet werden, um die richtige IPv6-Quell-IP anzugeben, während eine Verbindung zum BGP-Peer hergestellt wird, wie in der BGP-IPv4-Konfiguration angegeben.

Routing in einem L3-Cluster

Das Routing in einem L3-Cluster funktioniert nur, wenn die folgenden Konfigurationen auf der NetScaler-Appliance vorgenommen wurden.

- Aktivieren Sie das dynamische Routing für ein VLAN.

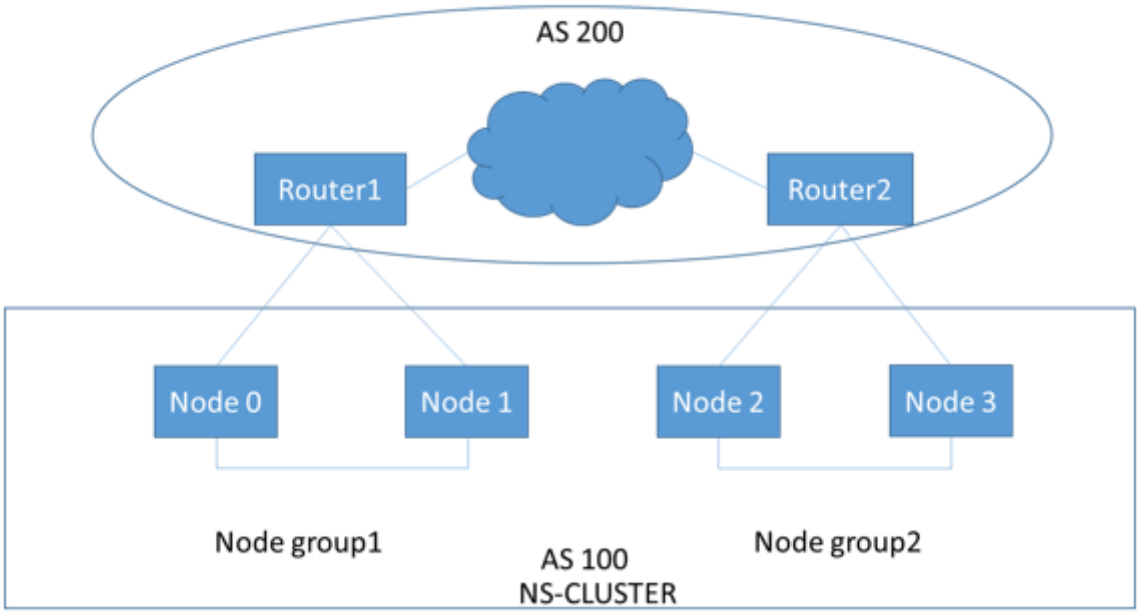
```
1  set vlan <id> -dynamicrouting enabled
2  <!--NeedCopy-->
```


- Um alle Clusterknoten zu erreichen, müssen VIP-, CLIP- und NetScaler-IP (NSIP) zusammen mit dem Befehl über Routing-Protokolle angekündigt werden. `set vlan`

Bereitstellungsszenario für BGP im L3-Cluster

Stellen Sie sich ein Beispiel vor, in dem alle Clusterknoten im AS 100-Netzwerk gruppiert sind und sich die Upstream-Router in einem anderen AS 200-Netzwerk befinden.

Die folgende Abbildung zeigt die AS 100- und AS 200-Bereitstellung in einem Cluster-Setup.



Bei dieser Bereitstellung kündigt CLIP den Upstream-Routern CCO an. Einige Clusterknoten unterbrechen den angekündigten Datenverkehr, da eine AS-Loop erkannt wird.

Um das Problem zu beheben, konfigurieren Sie den folgenden Befehl im VTYSH BGP-Router-Modus für jeden Nachbarn.

Geben Sie in der VTYSH-Befehlszeile Folgendes ein:

```
neighbor <peer_ip> allowas-in 1
```

Als bewährte Methode empfiehlt Citrix, eine der folgenden Optionen zu konfigurieren:

- Konfigurieren Sie Route-Maps, um nur die gewünschten Netzwerke zu ermitteln, z. B. Standardroute, NetScaler IP (NSIP) und NSIP-Subnetze auf Clusterknoten.
- Konfigurieren Sie Upstream-Routen, um nur gewünschte Netzwerke wie CLIP und NetScaler IP (NSIP) im Cluster anzukündigen.

IP-Adressierung für einen Cluster

May 11, 2023

Zusätzlich zu den Standardtypen von NetScaler-eigenen IP-Adressen — NetScaler NSIP, Virtual IP (VIP) und Subnet IP (SNIP) — kann eine geclusterte NetScaler-Appliance über eine Cluster-Management-IP-Adresse (CLIP) verfügen. Es kann auch Striped und gepunktete IP-Adressen enthalten.

- **CLIP-Adresse.** Eine IP-Adresse, die dem Cluster Coordinator Node (CCO) gehört. Die CLIP-Adresse kann in einem Cluster-Setup zwischen verschiedenen Knoten schwanken. Wenn der CLIP auf einen anderen Knoten des Clusters verschoben wird, wird dieser Knoten zum CCO. Der CCO ist die NetScaler-Appliance, die für Verwaltungsaufgaben im Cluster verantwortlich ist. Ein Netzwerkadministrator verwendet die CLIP-Adresse, um eine Verbindung zum Cluster herzustellen, um Konfigurations- und Verwaltungsaufgaben auszuführen, z. B. den Zugriff auf die einheitliche GUI, die Berichterstattung, die Verfolgung des Paketflusses und das Sammeln von Protokollen. Sie können mehrere CLIP-Adressen in einem Cluster in demselben oder in verschiedenen Netzwerken hinzufügen. Nur Konfigurationen, die auf dem CCO über die Cluster-IP-Adresse durchgeführt werden, werden an andere Knoten im Cluster weitergegeben.
- **Gestreifte IP-Adresse**. Eine logische IP-Adresse, die auf allen Knoten des Clusters verfügbar ist. Es kann sich entweder um eine VIP- oder eine SNIP-Adresse handeln.
- **Entdeckte IP-Adresse**. Eine logische IP (vorzugsweise SNIP-Adresse) ist nur auf einem Knoten verfügbar. Eine entdeckte IP-Adresse ist nur auf diesem Knoten sichtbar. Um den Aufwand für die Steuerung des Datenverkehrs zu minimieren, empfiehlt Citrix, für die Backend-Kommunikation mit dem Server eine entdeckte SNIP-Adresse zu verwenden.

Die folgende Tabelle enthält die Details der Konfigurationen.

IP-Adresse	NSIP	VIP	SNIP
Fleckig	Ja	Ja	Ja
Gestreift	Nein	Ja	Ja

Beispielsweise müssen Sie in einer Clustergruppe mit vier Knoten jeden Knoten mit einer gespotted SNIP-Adresse konfigurieren. Weitere Informationen zum Konfigurieren einer Spotted IP-Konfiguration finden Sie unter Striped, Partially Striped und Spotted Configurations.

Sie können eine SNIP-Adresse so definieren, dass sie nur auf einem Knoten aktiv ist oder auf allen Knoten aktiv ist. Wenn die virtuelle IP-Adresse und die Subnetz-IP-Adresse nur auf einem bestimmten Knoten verfügbar sind, handelt es sich um eine entdeckte Konfiguration. Die Konfiguration ist als Striped definiert, wenn die Subnetz-IP-Adresse und die IP-Adresse des virtuellen Servers auf allen

Knoten verfügbar sind. Spotted SNIP-Adressen helfen dabei, den Verkehr an Lenkung und Backplane zu reduzieren.

Bewährte Methoden für VLAN-Bindungen und Routenkonfiguration beim Hinzufügen eines Knotens zum Cluster

VLAN-IP-Bindungen

Wenn Sie ein VLAN an die entdeckte IP-Adresse binden, muss der NetScaler-Cluster mit den erkannten IP-Adressen im selben Subnetz auf allen Knoten konfiguriert werden. In einem Cluster mit zwei Knoten mit Knoten 0 und Knoten 1 können Sie beispielsweise die folgende Konfiguration haben:

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3 add vlan 100
4 bind vlan 100 -IPAddress 192.254.101.101 255.255.255.0
5 <!--NeedCopy-->
```

Routing-Konfiguration

Wenn eine Routing-Konfiguration mit der Spott-IP-Adresse als Standard-Gateway erforderlich ist, muss der ADC-Cluster mit den erkannten IP-Adressen im selben Subnetz auf allen Knoten konfiguriert werden. In einem Cluster mit zwei Knoten mit Knoten 0 und Knoten 1 können Sie beispielsweise die folgende Konfiguration haben:

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3
4 add route 192.254.102.0 255.255.255.0 192.254.101.103
5 <!--NeedCopy-->
```

> **Hinweis**
>
> In einem L3-Cluster-Setup wird nur die Spotted SNIP-Konfiguration unterstützt.

Konfigurieren von Layer-3-Clustering

May 11, 2023

Den L3-Cluster verstehen

Die Notwendigkeit, die Bereitstellung von Hochverfügbarkeit auszuweiten und die Skalierbarkeit des Client-Traffics in verschiedenen Netzwerken zu erhöhen, führte zur Einrichtung des L3-Clusters. Mit dem L3-Cluster können Sie NetScaler-Appliances in einzelnen Subnetzen gruppieren (L2-Cluster).

Der L3-Cluster wird auch als „Cluster im INC-Modus (Independent Network Configuration)“ bezeichnet. Bei der L3-Cluster-Bereitstellung werden die Clusterknoten im selben Netzwerk zu einer Knotengruppe gruppiert. Der L3-Cluster verwendet GRE-Tunneling, um die Pakete über Netzwerke zu steuern. Die Heartbeat-Nachrichten über die L3-Cluster werden weitergeleitet.

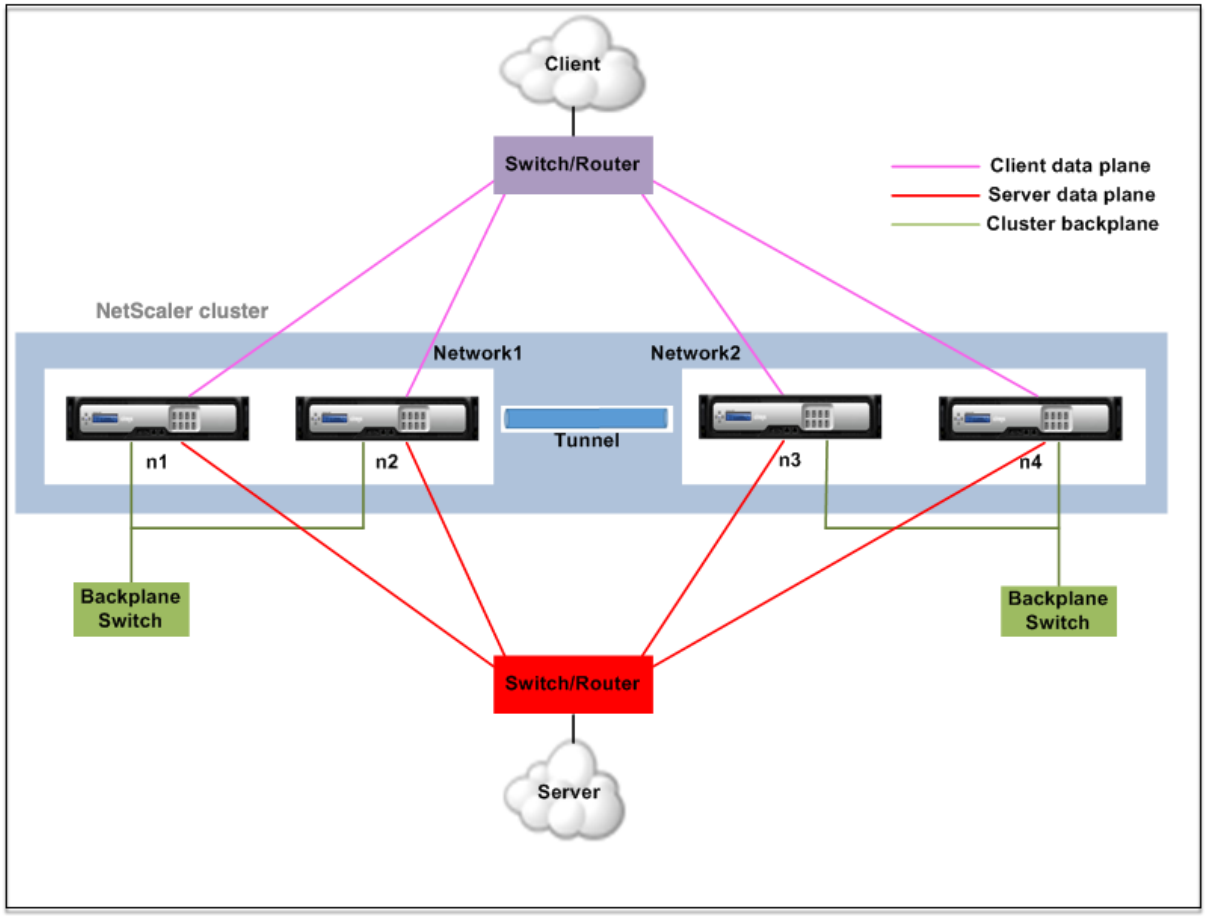
Dieses Dokument enthält die folgenden Details:

- Architektur
- Beispiel

Architektur

Die L3-Cluster-Architektur umfasst die folgenden Komponenten:

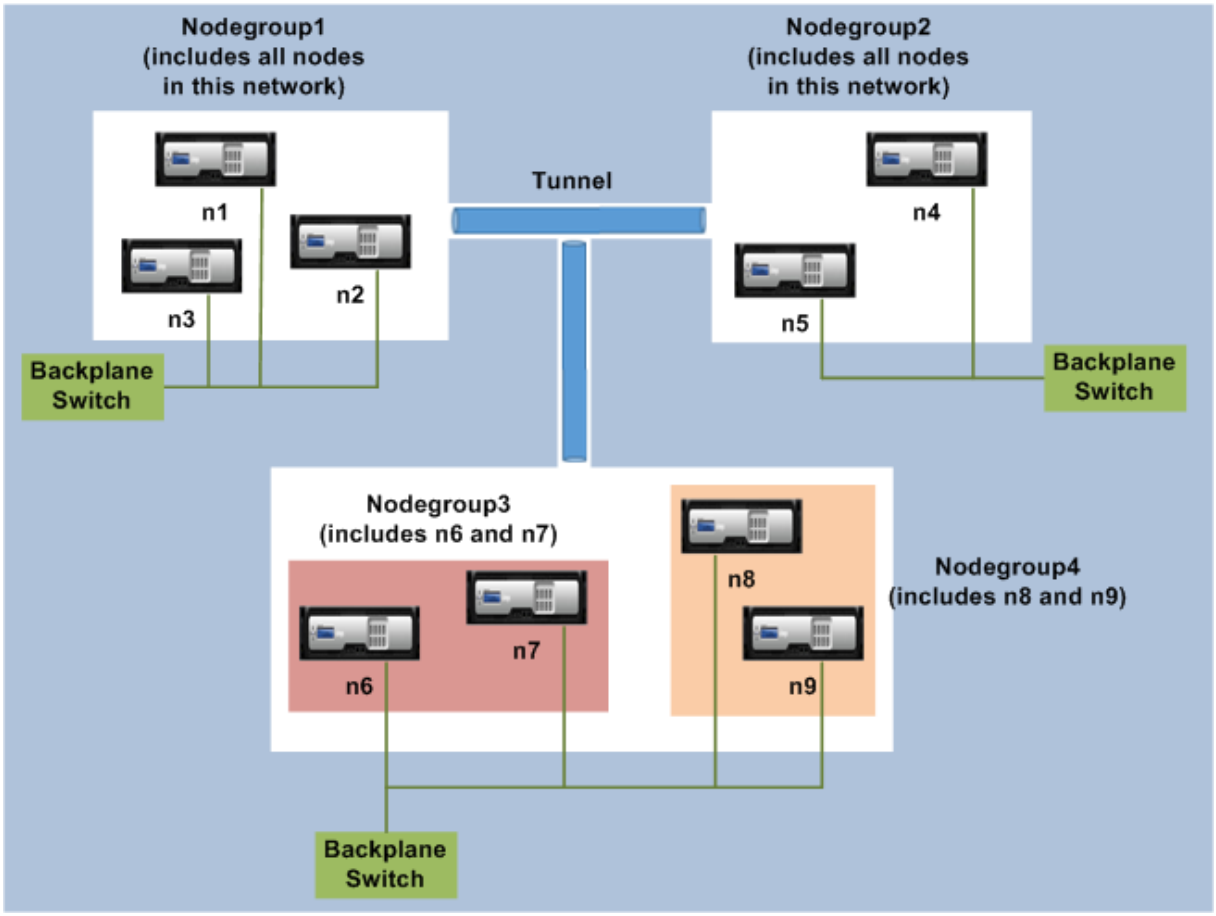
- **Knotengruppe**. Die Clusterknoten aus jedem Netzwerk (n1, n2) und (n3, n4) sind, wie in der folgenden Abbildung dargestellt, zu einer Knotengruppe gruppiert. Diese Knotengruppen sind an den Layer-3-Switch auf beiden Seiten des Netzwerks angeschlossen.
  - Der Cluster kommuniziert mit dem Client über die physischen Verbindungen zwischen dem Clusterknoten und dem clientseitigen Verbindungsgerät. Die logische Gruppierung dieser physischen Verbindungen wird als Client-Datenebene bezeichnet.
  - Der Cluster kommuniziert mit dem Server über die physischen Verbindungen zwischen dem Clusterknoten und dem serverseitigen Verbindungsgerät. Die logische Gruppierung dieser physikalischen Verbindungen wird als Serverdatenebenebezeichnet.
- **Schalter für die Rückwandplatine.** Clusterknoten innerhalb desselben Netzwerks kommunizieren miteinander, indem sie die Cluster-Backplane verwenden. Die Backplane besteht aus einer Reihe von Schnittstellen, bei denen eine Schnittstelle jedes Knotens mit einem gemeinsamen Switch verbunden ist, der als Cluster-Backplane-Switch bezeichnet wird.
- **GRE-Tunnel.** Die Pakete zwischen Knoten in einem L3-Cluster werden über einen unverschlüsselten GRE-Tunnel ausgetauscht, der die NSIP-Adressen der Quell- und Zielknoten für das Routing verwendet. Der Steuerungsmechanismus ändert sich für Knoten, die zu dem anderen Netzwerk gehören. Die Pakete werden durch einen GRE-Tunnel zum Knoten im anderen Subnetz geleitet, anstatt den MAC neu zu schreiben.



Beispiel

Stellen Sie sich ein Beispiel für eine L3-Cluster-Bereitstellung vor, die aus den folgenden Komponenten besteht:

- Drei NetScaler-Appliances (n1, n2 und n3) sind in Nodegroup1 gruppiert.
- In ähnlicher Weise sind die Knoten n4 und n5 in Nodegroup2 gruppiert. Im dritten Netzwerk gibt es zwei Knotengruppen. Nodegroup3 umfasst n6 und n7 und Nodegroup4 umfasst n8 und n9.
- Die NetScaler Appliances, die zu demselben Netzwerk gehören, werden zu einer Knotengruppe kombiniert.



Punkte, die vor der Konfiguration des L3-Clusters zu beachten sind

Beachten Sie die folgenden Punkte, bevor Sie den L3-Cluster auf einer NetScaler Appliance konfigurieren:

- Die Backplane ist bei der Konfiguration von L3-Subnetzen nicht erforderlich. Wenn die Rückwandplatine nicht angegeben ist, geht der Knoten nicht in den Ausfallzustand der Backplane über.

  > **Hinweis**
  >
  > Wenn Sie mehr als einen Knoten im selben L2-Netzwerk haben, muss die Backplane-Schnittstelle definiert werden. Wenn die Backplane-Schnittstelle nicht erwähnt wird, gehen die Knoten in den Status Backplane-Fail über.

- L2-Funktionen und Striped SNIPs werden im L3-Cluster nicht unterstützt.
- Die externe Verkehrsverteilung im L3-Cluster unterstützt nur Equal Cost Multiple Path (ECMP).
- Die ICMP-Fehler und die Fragmentierung werden nicht verarbeitet, wenn das Steering in einer L3-Cluster-Bereitstellung deaktiviert ist:

- Die Netzwerkentitäten (`route`, `route6`, `pbr`, und `pbr6`) müssen an die Konfigurationsknotengruppe gebunden sein.
- VLAN-, RNAT- und IP-Tunnel können nicht an eine Konfigurationsknotengruppe gebunden werden.
- Die Konfigurationsknotengruppe muss immer die Eigenschaft STRICT “YES” haben.
- Die Clusterknoten dürfen nicht mit dem Befehl “add cluster node” zu einer Konfigurationsknotengruppe hinzugefügt werden.
- Der Befehl `add cluster instance -INC enabled` löscht die Netzwerkentitäten (route, route6, PBR, pb6, RNAT, IP-Tunnel, ip6tunnel).
- Der `clear config extended`+ Befehl löscht die Entitäten (route, route6, PBR, pb6, RNAT, IP-Tunnel, ip6tunnel) in einem L3-Cluster nicht.

Konfigurieren des L3-Clusters

In einer L3-Clusterkonfiguration hat der Clusterbefehl verschiedene zu konfigurierende Attribute, die auf Knoten und Knotengruppen basieren. Die L3-Clusterkonfiguration umfasst neben IPv4-Profilen auch ein IPv6-Profil.

Das Konfigurieren eines L3-Clusters auf einer NetScaler Appliance besteht aus den folgenden Aufgaben:

- Erstellen einer Clusterinstanz
- Erstellen einer Knotengruppe im L3-Cluster
- Fügen Sie dem Cluster eine NetScaler Appliance hinzu und gruppieren Sie mit Knotengruppe
- Fügen Sie dem Knoten die Cluster-IP-Adresse hinzu
- Aktivieren Sie die Cluster-Instanz
- Speichern Sie die Konfiguration
- Fügen Sie einen Knoten zu einer vorhandenen Knotengruppe hinzu
- Erstellen einer Knotengruppe im L3-Cluster
- Gruppieren Sie neue Knoten zur neu erstellten Knotengruppe
- Fügen Sie den Knoten dem Cluster hinzu

Folgendes mithilfe der CLI konfigurieren

- **Um eine Cluster-Instance zu erstellen**

  ```
  add cluster instance <clid> -inc (<ENABLED|DISABLED>)[-processLocal <
  ENABLED | DISABLED]
  ```

- **Um eine Knotengruppe im L3-Cluster zu erstellen**

  ```
  add cluster nodegroup <name>
  ```


- **Um dem Cluster eine NetScaler Appliance hinzuzufügen und sie der Knotengruppe zuzuordnen**

  ```
  add cluster node <nodeid> <nodeip> -backplane <interface_name> node group <ng>
  ```

- **Um die Cluster-IP-Adresse auf diesem Knoten hinzuzufügen**

  ```
  add ns ip <IPAddress> <netmask> -type clip
  ```

- **Aktivieren Sie die Cluster-Instanz**

  ```
  enable cluster instance <clId>
  ```

- **Speichern Sie die Konfiguration**

  ```
  save ns config
  ```

- **Warmer Neustart der Appliance**

  ```
  reboot -warm
  ```

- **Um einen neuen Knoten zu einer vorhandenen Knotengruppe hinzuzufügen**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Um eine neue Knotengruppe im L3-Cluster zu erstellen**

  ```
  add cluster nodegroup <ng>
  ```

- **Um neue Knoten der neu erstellten Knotengruppe zuzuordnen**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **Um den Knoten mit dem Cluster zu verbinden**

```
1     join cluster  - clip <ip_addr> -password <password>
2
3     add cluster instance 1  - inc ENABLED  - processLocal  ENABLED
4
5        Done
6 <!--NeedCopy-->
```

> **Hinweis**
>
> Der Parameter „inc“ muss für einen L3-Cluster AKTIVIERT sein.

```
1     add cluster nodegroup ng1
2
3        Done
4
5     > add cluster node 0 1.1.1.1  - state ACTIVE -backplane 0/1/1  -
          nodegroup ng1
```



```
6
7          Done
8
9       > add ns ip 1.1.1.100 255.255.255.255  - type clip
10
11         Done
12
13      > enable cluster instance 1
14
15         Done
16
17      > save ns config
18
19         Done
20
21      > add cluster node 1 1.1.1.2  - state ACTIVE  - nodegroup ng1
22
23         Done
24
25      > add cluster nodegroup ng2
26
27         Done
28
29      > add cluster node 4 2.2.2.1  - state ACTIVE  - nodegroup ng2
30
31         Done
32
33      > add cluster node 5 2.2.2.2  - state ACTIVE  - nodegroup ng2
34
35         Done
36
37      > join cluster -clip 1.1.1.100 -password nsroot
38  <!--NeedCopy-->
```

Werbecluster-IP-Adresse eines L3-Clusters

Konfigurieren Sie die Cluster-IP-Adresse, die dem Upstream-Router bekannt gegeben wird, um die Clusterkonfiguration von jedem Subnetz aus zugänglich zu machen.Die Cluster-IP-Adresse wird von den auf einem Knoten konfigurierten dynamischen Routing-Protokollen als Kernel-Route angekündigt.

Die Ankündigung der Cluster-IP-Adresse besteht aus den folgenden Aufgaben:

- **Aktivieren Sie die Host-Route-Option der Cluster-IP-Adresse**.Die Host-Route-Option

überträgt die Cluster-IP-Adresse an eine ZeBOS-Routingtabelle, um die Kernelroute über dynamische Routing-Protokolle umzuverteilen.

- **Konfiguration eines dynamischen Routing-Protokolls auf einem Knoten**.Ein dynamisches Routingprotokoll gibt die Cluster-IP-Adresse an den Upstream-Router an. Weitere Informationen zum Konfigurieren eines dynamischen Routingprotokolls finden Sie unterKonfigurieren dynamischer Routen.

So aktivieren Sie die Host-Routenoption der Cluster-IP-Adresse mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
-  add nsip <IPAddress> <netmask> -hostRoute ENABLED

-  show nsip \<IPAddress\>

    > add ns ip 10.102.29.60 255.255.255.255 -hostRoute ENABLED

       Done
<!--NeedCopy-->
```

Spotted, partially striped configurations on L3 cluster

Die spotted und partially Striped Konfigurationen auf dem L3-Cluster unterscheiden sich geringfügig vom L2-Cluster. Die Konfiguration kann von Knoten zu Knoten unterschiedlich sein, da sich die Knoten in verschiedenen Subnetzen befinden. Die Netzwerkkonfigurationen können im L3-Cluster knotenspezifisch sein, daher müssen Sie die Spotted- oder teilweise Striped-Konfigurationen auf der Grundlage der unten genannten Parameter konfigurieren.

Führen Sie die folgenden Aufgaben aus, um gespernte, teilweise Striped Konfigurationen auf einer NetScaler Appliance über den L3-Cluster zu konfigurieren:

- Fügen Sie einer statischen IPv4-Routingtabelle eine Cluster-Besitzergruppe hinzu
- Eine Cluster-Besitzergruppe zu einer statischen IPv6-Routingtabelle hinzufügen
- Hinzufügen einer Cluster-Besitzergruppe zu einem IPv4-Policy-basierten Routing (PBR)
- Eine Cluster-Besitzergruppe zu einem IPv6-PBR hinzufügen
- Fügen Sie ein VLAN hinzu
- Binden Sie ein VLAN an eine bestimmte Besitzergruppe der Clusterknotengruppe

Folgendes mithilfe der CLI konfigurieren

- **Um eine Cluster-Besitzergruppe zu einer statischen IPv4-Routentabelle der NetScaler Appliance hinzuzufügen**


```
add route <network> <netmask> <gateway> -owner group <ng>
```

- **Um eine Cluster-Besitzergruppe zu einer statischen IPv6-Routentabelle der NetScaler Appliance hinzuzufügen**

  ```
  add route6 <network> -owner group <ng>
  ```

- **So fügen Sie einer IPv4-PBR eine Cluster-Besitzergruppe hinzu**

  ```
  add pbr <name> <action> -owner group <ng>
  ```

- **Um eine Cluster-Besitzergruppe zu einer IPv6-PBR hinzuzufügen**

  ```
  add pbr6 <name> <action> -owner group <ng>
  ```

- **Um ein VLAN hinzuzufügen**

  ```
  add vlan <id>
  ```

- **Um ein VLAN an eine bestimmte Besitzergruppe der Clusterknotengruppe zu binden**

  ```
  bind vlan <id> -ifnum - [IPAddress <ip_addr | ipv6_addr> [-owner group
  <ng>]
  ```

  Die folgenden Befehle sind Beispielbeispiele für Konfigurationen mit Punkten und teilweise Striped Konfigurationen, die mithilfe der CLI konfiguriert werden können.

```
1     > add route 10.102.29.0 255.255.255.0 10.102.29.2  - ownergroup ng2
2
3         Done
4
5     > add route6 fe80::9404:60ff:fedd:a464/64  - ownergroup ng1
6
7         Done
8
9     > add pbr pbr1 allow  - ownergroup ng1
10
11        Done
12
13    > add pbr6 pbr2 allow  - ownergroup ng2
14
15        Done
16
17    > add vlan 2
18
19        Done
20
21    > bind vlan 2  - ifnum 1/2  - [IPAddress 10.102.29.80 | fe80::9404:60
         ff:fedd:a464/64-ownergroup ng1
22
```



```
23          Done
24  <!--NeedCopy-->
```

Knotengruppe konfigurieren

In einem L3-Cluster werden die folgenden Befehle verwendet, um denselben Satz von Konfigurationen auf mehr als einer Knotengruppe zu replizieren:

Konfiguration von Folgendem mithilfe der CLU

- **Um der Routing-Tabelle der NetScaler Appliance eine statische IPv4-Route hinzuzufügen**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Beispielkonfiguration:

```
1  add route 0 0 10.102.53.1 -ownerGroup ng1
2
3  add route 0 0 10.102.53.1 -ownerGroup ng2
4  <!--NeedCopy-->
```

Sie definieren eine neue Knotengruppe ‘all’, um die vorherige Konfiguration zu unterstützen, und müssen die folgenden Befehle konfigurieren:

Folgendes mithilfe der CLI konfigurieren

- **Um dem Cluster eine neue Knotengruppe mit strikten Parametern hinzuzufügen**

  ```
  add cluster node group <name> -strict <YES | NO>
  ```

- **Um einen Clusterknoten oder eine Entität an die angegebene Knotengruppe zu binden**

  ```
  bind cluster nodegroup <name> -node <nodeid>
  ```

- **Um eine statische IPv4-Route zu allen Besitzergruppen hinzuzufügen**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Beispielkonfiguration:

```
1  add cluster nodegroup all -strict YES
2
3  bind cluster nodegroup all -node 1
4
5  bind cluster nodegroup all -node 2
6
7  add route 0 0 10.102.53.1 -ownerGroup all
```



```
<!--NeedCopy-->
```

Verkehrsverteilung in einem L3-Cluster

In einem Cluster-Setup zeigen externe Netzwerke die Sammlung von NetScaler Appliances als einzelne Entität an. Daher muss der Cluster einen einzelnen Knoten auswählen, der den Datenverkehr empfangen muss. Im L3-Cluster erfolgt diese Auswahl mit dem ECMP. Der ausgewählte Knoten wird als Flow Receiver bezeichnet.

> **Hinweis**
>
> Für einen L3-Cluster (Knoten in verschiedenen Netzwerken) kann nur die ECMP-Verkehrsverteilung verwendet werden.

Der Flow-Empfänger erhält den Datenverkehr und bestimmt dann mithilfe der internen Clusterlogik den Knoten, der den Verkehr verarbeiten muss. Dieser Knoten wird als Flow-Prozessor bezeichnet. Der Flow-Empfänger leitet den Datenverkehr über die Backplane zum Flow-Prozessor, wenn sich der Flow-Receiver und der Flow-Prozessor im selben Netzwerk befinden. Der Verkehr wird durch den Tunnel geleitet, wenn sich der Flow-Empfänger und der Flow-Prozessor in unterschiedlichen Netzwerken befinden.

> **Hinweis**
>
> - Der Flow-Empfänger und der Flow-Prozessor müssen Knoten sein, die Datenverkehr verarbeiten können.
> - Ab NetScaler 11 können Sie die Steuerung auf der Cluster-Backplane deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der Lenkung auf der Cluster-Backplane.

Die vorangehende Abbildung zeigt eine Client-Anfrage, die durch den Cluster fließt. Der Client sendet eine Anfrage an eine virtuelle IP-Adresse (VIP). Ein auf der Client-Datenebene konfigurierter Mechanismus zur Verkehrsverteilung wählt einen der Clusterknoten als Flow-Empfänger aus. Der Flussempfänger empfängt den Datenverkehr, bestimmt den Knoten, der den Datenverkehr verarbeiten muss, und steuert die Anforderung an diesen Knoten (es sei denn, der Flow-Empfänger wählt sich selbst als Flow-Prozessor aus). Wenn sich der Flow-Prozessor und der Flow-Empfänger in derselben Knotengruppe befinden, wird das Paket über die Backplane gesteuert. Und wenn sich der Flow-Prozessor und der Flow-Receiver in verschiedenen Knotengruppen befinden, wird das Paket über den gerouteten Pfad durch den Tunnel gesteuert.

Der Flow-Prozessor stellt eine Verbindung mit dem Server her. Der Server verarbeitet die Anforderung und sendet die Antwort an die Subnetz-IP-Adresse (SNIP), die die Anforderung an den Server gesendet hat. Da der SNIP im L3-Cluster immer ein Spotted SNIP ist, erhält der Knoten, dem die SNIP-Adresse gehört, die Antwort vom Server.

Einrichten eines NetScaler-Clusters

May 11, 2023

NetScaler Appliances, die Sie dem Cluster hinzufügen möchten, müssen die unter Voraussetzungen für Clusterknotenangegebenen Kriterien erfüllen. Bevor Sie einen Cluster tatsächlich einrichten, müssen Sie die Cluster-Grundlagen kennen. Weitere Informationen finden Sie unter Cluster-Übersicht.

Für die Bildung eines Clusters müssen Sie die Kommunikation zwischen Knoten einrichten, den Cluster erstellen (indem Sie die erste NetScaler Appliance hinzufügen) und dann die anderen Clusterknoten hinzufügen. Jeder dieser Schritte wird in den nachfolgenden Themen mit relevanten Details erklärt.

> **Hinweis**
>
> Es gibt zwar einige Unterschiede bei der Einrichtung eines L2- und L3-Clusters, aber es gibt auch viele Ähnlichkeiten. In den folgenden Themen wird die Einrichtung für beide Clustertypen erläutert und gleichzeitig die Konfigurationen hervorgehoben, die für L3-Cluster spezifisch sind.

Einrichten der Kommunikation zwischen Knoten

May 11, 2023

Die Knoten in einem Cluster-Setup kommunizieren miteinander, indem sie die folgenden Kommunikationsmechanismen zwischen den Knoten verwenden:

- Knoten, die sich innerhalb des Netzwerks befinden (dasselbe Subnetz), kommunizieren über die Cluster-Backplane miteinander. Die Backplane muss explizit eingerichtet werden. Im Folgenden finden Sie die detaillierten Schritte.
- Netzwerkübergreifend erfolgt die Steuerung der Pakete über einen GRE-Tunnel, und die andere Kommunikation von Knoten zu Knoten wird je nach Bedarf über die Knoten geleitet.

> **Wichtig**
>
> - Ab Version 11.0 aller Builds kann ein Cluster Knoten aus verschiedenen Netzwerken enthalten.
> - Ab Version 13.0 Build 58.3 wird GRE-Steering auf Fortville-NICs in einem L3-Cluster unterstützt.

Gehen Sie für jeden Knoten wie folgt vor, um die Cluster-Backplane einzurichten

1. Identifizieren Sie die Netzwerkschnittstelle, die Sie für die Backplane verwenden möchten.

2. Schließen Sie ein Ethernet- oder optisches Kabel von der ausgewählten Netzwerkschnittstelle an den Cluster-Backplane-Switch an.

Um beispielsweise die Schnittstelle 1/2 als Backplane-Schnittstelle für Knoten 4 zu verwenden, schließen Sie ein Kabel von der 1/2-Schnittstelle von Knoten 4 an den Backplane-Switch an.

Wichtige Punkte, die beim Einrichten der Cluster-Backplane zu beachten sind

- Verwenden Sie nicht die Verwaltungsschnittstelle (0/x) der Appliance als Backplane-Schnittstelle. In einem Cluster wird die Schnittstelle 0/1/x gelesen als:

  0 -> Knoten-ID 0
  1/x -> NetScaler-Schnittstelle

- Verwenden Sie keine Backplane-Schnittstellen für die Client- oder Serverdatenebenen.
- Citrix empfiehlt, den Link Aggregat-Kanal (LA) für die Cluster-Backplane zu verwenden.
- In einem Cluster mit zwei Knoten, in dem die Rückwandplatine Back-to-back verbunden ist, ist der Cluster unter einer der folgenden Bedingungen operativ DOWN:

  - Einer der Knoten wird neu gestartet.
  - Die Backplane-Schnittstelle eines der Knoten ist deaktiviert.

  Daher empfiehlt Citrix, dass Sie einen separaten Switch für die Backplane verwenden, damit der andere Clusterknoten und der Datenverkehr nicht beeinträchtigt werden. Sie können den Cluster nicht mit einem Back-to-Back-Link skalieren. Es kann zu Ausfallzeiten in der Produktionsumgebung kommen, wenn Sie die Clusterknoten skalieren.

- Die Backplane-Schnittstellen aller Knoten eines Clusters müssen an denselben Switch angeschlossen und an dasselbe L2-VLAN gebunden sein.
- Wenn Sie mehrere Cluster mit derselben Cluster-Instance-ID haben, stellen Sie sicher, dass die Backplane-Schnittstellen jedes Clusters an ein anderes VLAN gebunden sind.
- Die Backplane-Schnittstelle wird immer überwacht, unabhängig von den HA-Monitoring-Einstellungen dieser Schnittstelle.
- Der Zustand des MAC-Spoofings auf den verschiedenen Virtualisierungsplattformen kann sich auf den Steuerungsmechanismus auf der Cluster-Backplane auswirken. Stellen Sie daher sicher, dass der entsprechende Status konfiguriert ist:

  - XenServer - MAC-Spoofing deaktivieren
  - Hyper-V — MAC-Spoofing aktivieren
  - VMware ESX — MAC-Spoofing aktivieren (stellen Sie außerdem sicher, dass „Forged Transmits“ aktiviert ist)

- Die MTU für die Cluster-Backplane wird automatisch aktualisiert. Wenn Jumbo-Frames jedoch auf dem Cluster konfiguriert sind, muss die MTU der Cluster-Backplane explizit konfiguriert werden. Der Wert muss auf 78 + X festgelegt werden, wobei X die maximale MTU der Client- und Serverdatenebenen ist. Zum Beispiel, wenn die MTU einer Serverdatenebene 7500 und der Client-Datenebene 8922 beträgt. Die MTU einer Cluster-Backplane muss auf 78 + 8922 = 9000 festgelegt werden. Verwenden Sie den folgenden Befehl, um diese MTU festzulegen:

  ```
  > set interface <backplane_interface> -mtu <value>
  ```

- Die MTU für die Schnittstellen des Backplane-Switches muss größer oder gleich 1.578 Byte angegeben werden. Dies ist anwendbar, wenn der Cluster über Funktionen wie MBF, L2-Richtlinien, ACLs, Routing in CLAG-Bereitstellungen und vPath verfügt.

UDP-basierte Tunnelunterstützung für L2- und L3-Cluster

Ab NetScaler Version 13.0 Build 36.x können NetScaler L2- und L3-Cluster den Datenverkehr mithilfe von UDP-basiertem Tunneling steuern. Es ist für die Kommunikation zwischen den Knoten zwischen zwei Knoten in einem Cluster definiert. Mithilfe des Parameters „Tunnelmodus“ können Sie den GRE- oder UDP-Tunnelmodus über den Befehl zum Hinzufügen und Festlegen von Clusterknoten festlegen.

In einer L3-Cluster-Bereitstellung werden Pakete zwischen NetScaler-Knoten über einen unverschlüsselten GRE-Tunnel ausgetauscht, der die NSIP-Adressen der Quell- und Zielknoten für das Routing verwendet. Wenn dieser Austausch über das Internet erfolgt und kein IPSec-Tunnel vorhanden ist, ist das NSIPs im Internet verfügbar, was zu Sicherheitsproblemen führen kann.

> **Wichtig**
>
> Citrix empfiehlt Kunden, ihre eigene IPSec-Lösung einzurichten, wenn sie einen L3-Cluster verwenden.

Die folgende Tabelle hilft Ihnen dabei, die Tunnelunterstützung anhand verschiedener Bereitstellungen zu kategorisieren.

Lenkungstypen	AWS	Microsoft Azure	Vor Ort
MAC	Nicht unterstützt	Nicht unterstützt	Unterstützt
GRE Tunnel	Unterstützt	Nicht unterstützt	Unterstützt
UDP-Tunnel	Unterstützt	Unterstützt	Unterstützt

> **Wichtig**
>
> In einem L3-Cluster ist der Tunnelmodus standardmäßig auf GRE eingestellt.

Konfiguration eines UDP-basierten Tunnels

Sie können einen Clusterknoten hinzufügen, indem Sie die Parameter der Knoten-ID festlegen und den Status angeben. Konfigurieren Sie die Backplane, indem Sie den Schnittstellennamen angeben, und wählen Sie den Tunnelmodus Ihrer Wahl (GRE oder UDP).

CLI-Verfahren

Um den UDP-Tunnelmodus mithilfe der CLI zu aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

- `add cluster node <nodeId>@ [-state <state>] [-backplane <interface_name>] [-tunnelmode <tunnelmode>]`
- `set cluster node <nodeId>@ [-state <state>] [-tunnelmode <tunnelmode>]`

> **Hinweis**
>
> Mögliche Werte für den Tunnelmodus sind NONE, GRE, UDP.

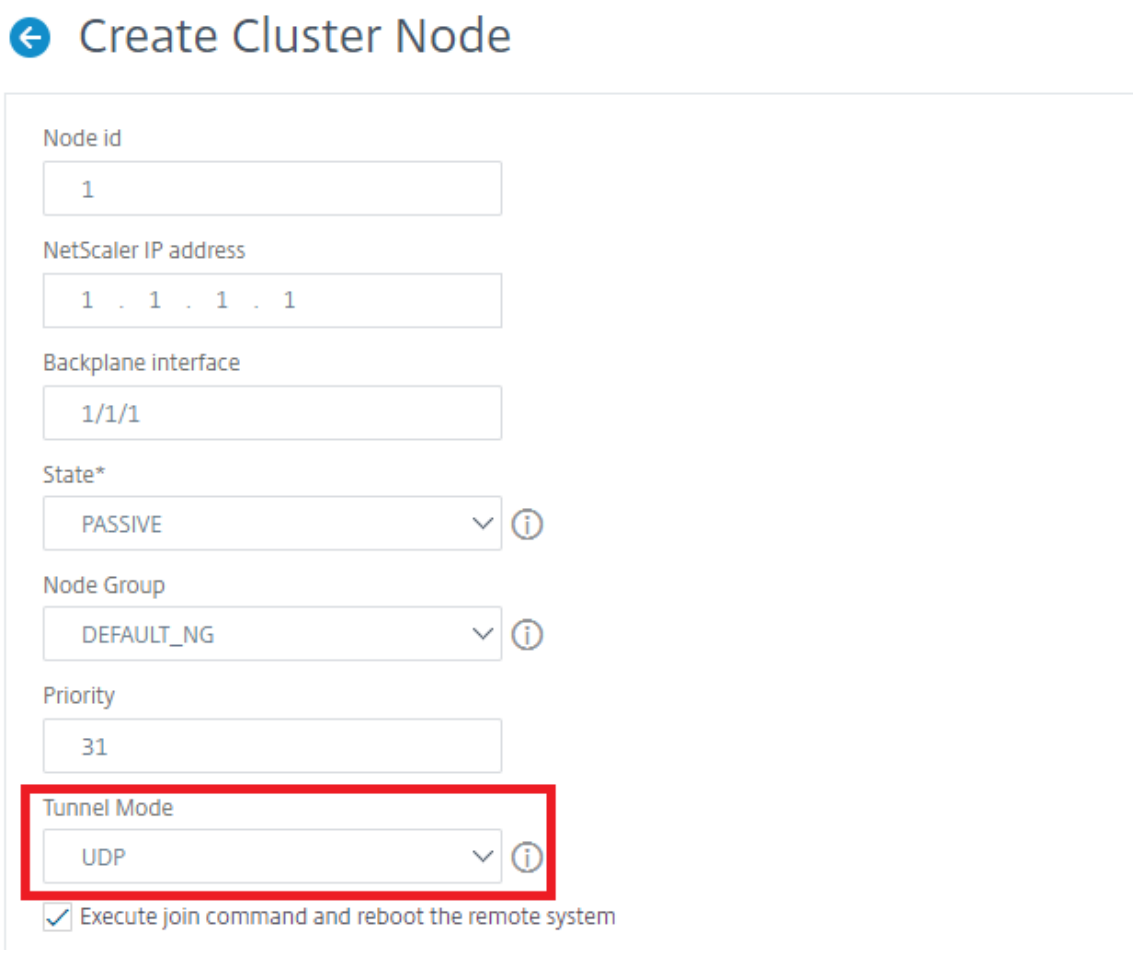
Beispiel

- `add cluster node 1 -state ACTIVE -backplane 1/1/1 -tunnelmode UDP`
- `set cluster node 1 -state ACTIVE -tunnelmode UDP`

GUI-Verfahren

Um den UDP-Tunnelmodus mithilfe der GUI zu aktivieren.

1. Navigieren Sie zu **System > Cluster > Knoten**.
2. Klicken Sie auf der Seite **Clusterknoten** auf **Hinzufügen**.
3. Stellen **Sie im Create Cluster Node**den Parameter **Tunnel Mode** auf UDP ein und klicken Sie auf **Create**.



4. Klicken Sie auf **Schließen**.

Erstellen eines NetScaler-Clusters

May 11, 2023

Um einen Cluster zu erstellen, nehmen Sie zunächst eine der NetScaler Appliances, die Sie dem Cluster hinzufügen möchten. Auf diesem Knoten müssen Sie die Clusterinstanz erstellen und die Cluster-IP-Adresse definieren. Dieser Knoten ist der erste Clusterknoten und wird als Cluster Configuration Coordinator (CCO) bezeichnet. Alle Konfigurationen, die auf der Cluster-IP-Adresse ausgeführt werden, werden auf diesem Knoten gespeichert und dann an die anderen Clusterknoten weitergegeben.

Die Verantwortung von CCO in einem Cluster ist nicht auf einen bestimmten Knoten festgelegt. Es kann sich im Laufe der Zeit ändern, abhängig von den folgenden Faktoren:

- Die Priorität des Knotens. Der Knoten mit der höchsten Priorität (niedrigste Prioritätsnummer) wird zum CCO gemacht. Wenn daher ein Knoten mit einer niedrigeren Prioritätsnummer als der

vorhandene CCO hinzugefügt wird, übernimmt der neue Knoten als CCO.

- Wenn der aktuelle CCO ausfällt, übernimmt der Knoten mit der nächstniedrigsten Prioritätsnummer als CCO. Wenn die Priorität nicht festgelegt ist oder mehrere Knoten mit der niedrigsten Prioritätsnummer vorhanden sind, wird der CCO aus einem der verfügbaren Knoten ausgewählt.

> **Hinweis:**
>
> Die Konfigurationen der Appliance (einschließlich SNIP-Adressen und VLANs) werden durch implizites Ausführen des `clear ns config extended` Befehls gelöscht. Das Standard-VLAN und das NSVLAN werden jedoch nicht von der Appliance gelöscht. Wenn Sie das NSVLAN auf dem Cluster haben möchten, stellen Sie daher sicher, dass es erstellt wurde, bevor die Appliance zum Cluster hinzugefügt wird. Für einen L3-Cluster (Clusterknoten in verschiedenen Netzwerken) werden Netzwerkkonfigurationen nicht von der Appliance gelöscht.
>
> **Wichtig:**
>
> HA Monitor (HAMON) in einem Cluster-Setup wird verwendet, um den Zustand einer Schnittstelle auf jedem Knoten zu überwachen. Der HAMON-Parameter muss auf jedem Knoten aktiviert sein, um den Zustand der Schnittstelle zu überwachen. Wenn der Betriebszustand der HAMON aktivierten Schnittstelle aus irgendeinem Grund ausfällt, wird der jeweilige Clusterknoten als fehlerfrei (NICHT AKTIV) gekennzeichnet und dieser Knoten kann den Datenverkehr nicht bedienen.

Erstellen Sie einen Cluster mithilfe der Befehlszeilenschnittstelle

- Melden Sie sich bei einer NetScaler-Appliance an (z. B. Appliance mit der NSIP-Adresse 10.102.29.60), die Sie dem Cluster hinzufügen möchten.
- Eine Clusterinstanz hinzufügen.

```
1  add cluster instance <clId> -quorumType <NONE | MAJORITY> -inc <
      ENABLED | DISABLED> -backplanebasedview <ENABLED | DISABLED>
2  <!--NeedCopy-->
```

- Mit der Option `-dfdretainl2params` können Sie die erweiterten L2-Header für den Backplane-Traffic hinzufügen.

  Geben Sie in der Befehlszeile Folgendes ein:

  `add cluster instance 1 -dfdretainl2params <ENABLED|DISABLED>`

  Der folgende Befehl zeigt den Status von `-dfdretainl2params`:

  `show cluster instance <clusterid>`

Verwenden Sie den folgenden Befehl, um den zu aktivieren oder zu deaktivieren –dfdretainl2params:

```
set cluster instance 1 -dfdretainl2params <ENABLED|DISABLED>
```

- Die Option –proxyarpstatus aktiviert oder deaktiviert die Proxy-ARP-Funktionalität für Cluster.

  Geben Sie in der Befehlszeile Folgendes ein:

  ```
  add cluster instance 1 -proxyarpstatus <ENABLED|DISABLED>
  ```

  Der folgende Befehl zeigt den Status von proxyarpstatus:

  ```
  show cluster instance <clusterid>
  ```

  Sie können den folgenden Befehl verwenden, um den zu aktivieren oder zu deaktivieren proxyarpstatus:

  ```
  set cluster instance 1 -proxyarpstatus <ENABLED|DISABLED>
  ```

> **Hinweis:**
>
> - Die Clusterinstanz-ID muss innerhalb eines LAN eindeutig sein.
> - Der –quorumType Parameter muss in den folgenden Szenarien auf MEHRHEIT und nicht auf NONE festgelegt werden:
>   - Topologies which do not have redundant links between cluster nodes. These topologies might be prone to network partition due to a single point of failure.
>   - During any cluster operations such as node addition or removal.
> - Stellen Sie für einen L3-Cluster sicher, dass der –inc Parameter auf ENABLED gesetzt ist. Der –inc Parameter muss für einen L2-Cluster deaktiviert sein.
> - Wenn der –backplanebasedview Parameter aktiviert ist, wird die Betriebsansicht (Satz von Knoten, die den Datenverkehr bedienen) basierend auf Heartbeats entschieden, die nur auf der Backplane-Schnittstelle empfangen werden. Standardmäßig ist dieser Parameter deaktiviert. Wenn dieser Parameter deaktiviert ist, hängt ein Knoten nicht vom Heartbeat-Empfang nur auf der Backplane ab.

1. [Nur für einen L3-Cluster] Erstellen Sie eine Knotengruppe. Im nächsten Schritt muss der neu hinzugefügte Clusterknoten dieser Knotengruppe zugeordnet werden.

   > **Hinweis:**
   >
   > Diese Knotengruppe umfasst alle oder eine Teilmenge der NetScaler Appliances, die zum selben Netzwerk gehören.

   ```
   add cluster nodegroup <name>
   <!--NeedCopy-->
   ```


2. Fügen Sie die NetScaler Appliance zum Cluster hinzu.

```
add cluster node <nodeId> <IPAddress> -state <state> -backplane <
   interface_name> -nodegroup <name>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für einen L3-Cluster:
>
> - Der Knotengruppenparameter muss auf den Namen der erstellten Knotengruppe festgelegt werden.
> - Der Backplane-Parameter ist obligatorisch für Knoten, die einer Knotengruppe mit mehr als einem Knoten zugeordnet sind, damit die Knoten innerhalb des Netzwerks miteinander kommunizieren können.

Beispiel:

Hinzufügen eines Knotens für einen L2-Cluster (alle Clusterknoten befinden sich im selben Netzwerk).

```
  add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
  <!--NeedCopy-->
```

Hinzufügen eines Knotens für einen L3-Cluster, der einen einzelnen Knoten aus jedem Netzwerk enthält. Hier müssen Sie die Rückwandplatine nicht einstellen.

```
  add cluster node 0 10.102.29.60 -state PASSIVE -nodegroup ng1
  <!--NeedCopy-->
```

Hinzufügen eines Knotens für einen L3-Cluster, der mehrere Knoten aus jedem Netzwerk umfasst. Hier müssen Sie die Backplane so einstellen, dass Knoten innerhalb eines Netzwerks miteinander kommunizieren können.

```
  add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
     -nodegroup ng1
  <!--NeedCopy-->
```

3. Fügen Sie die Cluster-IP-Adresse (z. B. 10.102.29.61) auf diesem Knoten hinzu.

```
add ns ip <IPAddress> <netmask> -type clip
<!--NeedCopy-->
```

Beispiel

```
add ns ip 10.102.29.61 255.255.255.255 -type clip
<!--NeedCopy-->
```


4. Aktivieren der Clusterinstanz

```
enable cluster instance <clId>
<!--NeedCopy-->
```

5. Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

6. Starten Sie die Appliance neu.

```
reboot -warm
<!--NeedCopy-->
```

   Überprüfen Sie die Cluster-Konfigurationen mit dem Befehl show cluster instance. Stellen Sie sicher, dass die Ausgabe des Befehls die NSIP-Adresse der Appliance als Knoten des Clusters anzeigt.

7. Nachdem der Knoten UP ist, melden Sie sich beim CLIP an und ändern Sie die RPC-Anmeldeinformationen für die Cluster-IP-Adresse und die Node-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

So erstellen Sie einen Cluster mit der GUI

1. Melden Sie sich bei einer Appliance an (z. B. einer Appliance mit der NSIP-Adresse 10.102.29.60), die Sie dem Cluster hinzufügen möchten.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich auf den Link **Cluster verwalten** .
4. Legen Sie im Dialogfeld Clusterkonfiguration die Parameter fest, die zum Erstellen eines Clusters erforderlich sind. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Textfeld.
5. Klicken Sie auf **Erstellen.**
6. Aktivieren Sie im Dialogfeld Clusterinstanz konfigurieren das Kontrollkästchen Clusterinstanz aktivieren.
7. Wählen Sie im Bereich Clusterknoten den Knoten aus und klicken Sie auf **Öffnen.**
8. Stellen Sie im Dialogfeld Clusterknoten konfigurieren den Status ein.
9. Klicken Sie auf **OK**und dann auf **Speichern.**
10. Starten Sie die Appliance neu.
11. Nachdem der Knoten UP ist, melden Sie sich beim CLIP an und ändern Sie die RPC-Anmeldeinformationen für die Cluster-IP-Adresse und die Node-IP-Adresse. Weitere

Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

Unterstützung des strikten Modus für den Synchronisierungsstatus des Clusters

Sie können jetzt einen Clusterknoten so konfigurieren, dass Fehler beim Anwenden der Konfiguration angezeigt werden. Ein neuer Parameter, "syncStatusStrictMode", wird sowohl im Befehl zum Hinzufügen als auch zum Festlegen der Clusterinstanz eingeführt, um den Status jedes Knotens in einem Cluster zu verfolgen. In der Standardeinstellung ist der Parameter `syncStatusStrictMode` deaktiviert.

So aktivieren Sie den strikten Modus mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set cluster instance <clID> [-syncStatusStrictMode (ENABLED | DISABLED)
   ]
<!--NeedCopy-->
```

Beispiel:

```
set cluster instance 1  -syncStatusStrictMode ENABLED
<!--NeedCopy-->
```

So zeigen Sie den Status des strikten Modus mithilfe der CLI an

```
    >show cluster instance
    1) Cluster ID: 1
        Dead Interval: 3 secs
        Hello Interval: 200 msecs
        Preemption: DISABLED
        Propagation: ENABLED
        Quorum Type: MAJORITY
        INC State: DISABLED
        Process Local: DISABLED
        Retain Connections: NO
        Heterogeneous: NO
        Backplane based view: DISABLED
        Cluster sync strict mode: ENABLED
        Cluster Status: ENABLED(admin), ENABLED(operational), UP

      WARNING(s):
        (1) - There are no spotted SNIPs configured on the cluster.
           Spotted SNIPs can help improve cluster performance
```



```
18
19          Member Nodes:
20          Node ID     Node IP      Health     Admin State  Operational
               State
21          -------     -------      ------     -----------
               -----------------
22      1)      1           192.0.2.20      UP         ACTIVE       ACTIVE(
           Configuration Coordinator)
23      2)      2           192.0.2.21      UP         ACTIVE       ACTIVE
24      3)      3           192.0.2.19*     UP         ACTIVE       ACTIVE
25  <!--NeedCopy-->
```

So zeigen Sie den Grund für einen Sync-Fehler eines Clusterknotens mithilfe der GUI an

1. Navigieren Sie zu **System > Cluster > Clusterknoten**.
2. Scrollen Sie auf der Seite **Clusterknoten** ganz nach rechts, um die Einzelheiten zum Grund des Synchronisationsfehlers der Clusterknoten anzuzeigen.

Hinzufügen eines Knotens zum Cluster

May 11, 2023

Sie können die Größe eines Clusters nahtlos auf maximal 32 Knoten skalieren. Wenn dem Cluster eine NetScaler-Appliance hinzugefügt wird, werden die Konfigurationen dieser Appliance gelöscht (indem intern der Befehl clear ns config -extended ausgeführt wird). Die SNIP-Adressen, **MTU-Einstellungen** der Backplane-Schnittstelle und alle VLAN-Konfigurationen (außer dem Standard-VLAN und NSVLAN) werden ebenfalls von der Appliance gelöscht.

Die Clusterkonfigurationen werden dann auf diesem Knoten synchronisiert. Während der Synchronisation kann es zu einem zeitweiligen Rückgang des Datenverkehrs kommen.

> **Wichtig**
>
> Bevor Sie einem Cluster eine NetScaler-Appliance hinzufügen:
>
> - Richten Sie die Backplane-Schnittstelle für den Knoten ein. Lesen Sie das vorherige Thema.
> - Überprüfen Sie, ob die auf der Appliance verfügbaren Lizenzen mit denen übereinstimmen, die im Konfigurationskoordinator verfügbar sind. Die Appliance wird nur hinzugefügt, wenn die Lizenzen übereinstimmen.
> - Wenn Sie das NSVLAN auf dem Cluster haben möchten, stellen Sie sicher, dass das NSVLAN auf der Appliance erstellt wurde, bevor es dem Cluster hinzugefügt wird.

- Citrix empfiehlt, den Knoten als passiven Knoten hinzuzufügen. Nachdem Sie den Knoten dem Cluster hinzugefügt haben, schließen Sie dann die knotenspezifische Konfiguration von der Cluster-IP-Adresse aus ab. Führen Sie den Befehl Force Cluster Sync aus, wenn der Cluster nur IP-Adressen erkannt hat. Und welches hat eine L3-VLAN-Bindung oder statische Routen.
- Wenn einem Cluster eine Appliance mit einem vorkonfigurierten Link Aggregat-Kanal (LA) hinzugefügt wird, ist der LA-Kanal weiterhin in der Clusterumgebung vorhanden. Der LA-Kanal wird von LA/x in NodeId/LA/x umbenannt, wobei LA/x die LA-Kanalkennung ist.

So fügen Sie dem Cluster über die Befehlszeilenschnittstelle einen Knoten hinzu

Hinweis

Wenn Sie einem Cluster-Setup einen Knoten hinzufügen und der Knoten über eine statische Standardroute verfügt, wird er dem Cluster-Koordinatorknoten (CCO) hinzugefügt. Wenn diese statische Standardroute auf ein falsches Gateway verweist, kann dies zu Ausfallzeiten der Dienste führen. Überprüfen Sie daher die statische Standardroute des neuen Knotens, bevor Sie ihn zum Cluster-Setup hinzufügen.

1. Melden Sie sich an der Cluster-IP-Adresse an und gehen Sie an der Befehlszeile wie folgt vor:
   - Fügen Sie die Appliance (z. B. 10.102.29.70) zum Cluster hinzu.

   Hinweis

   Für einen L3-Cluster:

   - Der Knotengruppenparameter muss auf eine Knotengruppe gesetzt werden, die Knoten desselben Netzwerks hat.
   - Wenn dieser Knoten zu demselben Netzwerk gehört wie der erste Knoten, der hinzugefügt wurde, konfigurieren Sie die Knotengruppe, die für diesen Knoten verwendet wurde.
   - Wenn dieser Knoten zu einem anderen Netzwerk gehört, erstellen Sie eine Knotengruppe und binden Sie diesen Knoten an die Knotengruppe.
   - Der Backplane-Parameter ist obligatorisch für Knoten, die einer Knotengruppe mit mehr als einem Knoten zugeordnet sind, damit die Knoten innerhalb des Netzwerks miteinander kommunizieren können.

```
add cluster node <nodeId> <IPAddress> -state <state> -backplane <
   interface_name> -nodegroup <name>

Example:

add cluster node 1 10.102.29.70 -state PASSIVE -backplane 1/1/1
<!--NeedCopy-->
```


- Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

2. Melden Sie sich an dem neu hinzugefügten Knoten an (z. B. 10.102.29.70) und verbinden Sie den Knoten mit dem Cluster.

```
join cluster -clip <ip_addr> -password <password>

Example:

join cluster -clip 10.102.29.61 -password nsroot
<!--NeedCopy-->
```

3. Konfigurieren Sie die folgenden Befehle auf dem CLIP.
   - Binden Sie VLAN an eine Schnittstelle

     ```
     bind vlan <id> -ifnum <interface_name>
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     bind vlan 1 -ifnum 2/1/2
     <!--NeedCopy-->
     ```

   - Fügt dem neu hinzugefügten Knoten eine entdeckte IP-Adresse hinzu

     ```
     add ns ip <IpAddress> <netmask> -ownerNode <positive_interger
        >
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2
     <!--NeedCopy-->
     ```

   - Überprüfen Sie das VLAN auf NSIP

     ```
     show vlan <id>
     <!--NeedCopy-->
     ```

     Beispiel:

     ```
     show vlan 1
     <!--NeedCopy-->
     ```


4. Führen Sie die folgenden Konfigurationen durch:
    - Wenn der Knoten zu einem Cluster hinzugefügt wird, der nur gescannte IPs hat, werden die Konfigurationen synchronisiert, bevor die erkannten IP-Adressen diesem Knoten zugewiesen werden. In solchen Fällen können L3-VLAN-Bindungen verloren gehen. Um diesen Verlust zu vermeiden, fügen Sie entweder eine Striped IP oder die L3-VLAN-Bindungen hinzu.
    - Definieren Sie die erforderlichen Spott-Konfigurationen.
    - Stellen Sie die MTU für die Backplane-Schnittstelle ein.
5. Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

6. Starten Sie die Appliance neu.

```
reboot -warm
<!--NeedCopy-->
```

7. Nachdem der Knoten UP ist und die Synchronisierung erfolgreich ist, ändern Sie die RPC-Anmeldeinformationen für den Knoten von der Cluster-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

```
set rpcNode <node-NSIP> -password <passwd>

Example:

set rpcNode 192.0.2.4 -password mypassword
<!--NeedCopy-->
```

8. Setzen Sie den Clusterknoten auf Aktiv.

```
set cluster node <nodeID> -state active.

Example:

set cluster node 1 -state active
<!--NeedCopy-->
```

So fügen Sie dem Cluster mithilfe der GUI einen Knoten hinzu

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten**.

3. Klicken Sie im Detailbereich auf **Hinzufügen**, um den neuen Knoten hinzuzufügen (z. B. 10.102.29.70).
4. Konfigurieren **Sie im Dialogfeld Clusterknoten erstellen** den neuen Knoten. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Textfeld.
5. Klicken Sie auf **Erstellen**. Wenn Sie aufgefordert werden, einen Warmneustart durchzuführen, klicken Sie auf **Ja.**
6. Nachdem der Knoten UP ist und die Synchronisierung erfolgreich ist, ändern Sie die RPC-Anmeldeinformationen für den Knoten von der Cluster-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.
7. Navigieren Sie zu **System > Cluster > Knoten > Bearbeiten**.
8. Ändern Sie den Status auf **AKTIV** und bestätigen Sie.

Um einen zuvor hinzugefügten Knoten mithilfe der GUI zum Cluster hinzuzufügen

Wenn Sie die CLI verwendet haben, um dem Cluster einen Knoten hinzuzufügen, den Knoten jedoch nicht mit dem Cluster verbunden haben, können Sie das folgende Verfahren verwenden.

> **Hinweis**
>
> Wenn ein Knoten dem Cluster beitritt, übernimmt er seinen Anteil am Datenverkehr vom Cluster, sodass eine bestehende Verbindung beendet werden kann.

1. Melden Sie sich bei dem Knoten an, den Sie dem Cluster hinzufügen möchten (z. B. 10.102.29.70).
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter Erste Schritte auf den Link Cluster beitreten.
4. Geben Sie im Dialogfeld “Mit vorhandenem Cluster verbinden” die Cluster-IP-Adresse und das `nsroot`-Kennwort des Konfigurationskoordinators ein. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Textfeld.
5. Klicken Sie auf **OK.**

Anzeigen der Details eines Clusters

August 19, 2021

Sie können die Details der Clusterinstanz und der Clusterknoten anzeigen, indem Sie sich bei der Cluster-IP-Adresse anmelden.

So zeigen Sie Details einer Clusterinstanz mit der CLI an

Melden Sie sich bei der Cluster-IP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cluster instance <clId>
```

> **Hinweis:**
>
> Wenn der vorhergehende Befehl von der NSIP-Adresse des Nicht-CCO-Knotens aus ausgeführt wird, zeigt der Befehl den Status des Clusters auf diesem Knoten an.

So zeigen Sie Details zu einem Clusterknoten mit der CLI an

Melden Sie sich bei der Cluster-IP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cluster node <nodeId>
```

So zeigen Sie Details einer Clusterinstanz über die GUI an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Erste Schritte**auf den Link **Cluster verwalten**, um die Details des Clusters anzuzeigen.

So zeigen Sie Details zu einem Clusterknoten mit der GUI an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten.**
3. Klicken Sie im Detailbereich auf den Knoten, für den Sie die Details anzeigen möchten.

Verteilen des Datenverkehrs auf Clusterknoten

May 11, 2023

Nachdem Sie den NetScaler-Cluster erstellt und die erforderlichen Konfigurationen durchgeführt haben, müssen Sie Equal Cost Multiple Path (ECMP) oder Cluster Link Aggregation (LA) auf der Client-Datenebene (für den Client-Verkehr) oder der Serverdatenebene (für den Server-Traffic) bereitstellen. Diese Mechanismen verteilen den externen Datenverkehr auf die Clusterknoten.

Richtliniengestützte Backplane-Steuerung

Das Policy-Based Backplane Steering (PBS) ist ein Mechanismus bei der Clusterbereitstellung, der den Datenverkehr zwischen den Clusterknoten auf der Grundlage der für den Flow definierten Hash-Methode steuert. Der Ablauf wird durch eine Kombination von L2- und L3-Parametern definiert, die der Access Control List (ACL) ähneln.

Die PBS unterstützt sowohl IPv4- als auch IPv6-Verkehr. Bei IPv6-Bereitstellungen unterstützt das Steering eine zusätzliche Option. `[dfdprefix <positive_integer>]` Es bietet die Flexibilität, denselben Flow-Prozessor für dasselbe IP-Präfix auszuwählen. Die Präfixoption wird nur für Quell-IP- oder Ziel-IP-Hashmethoden unterstützt.

> **Hinweis**
>
> Wenn der PBS-Mechanismus nicht zur Steuerung des Datenverkehrs verwendet wird, wird der Verkehr über die Standardmethode gesteuert.

Um die neuen ACL-Attribute zu konfigurieren, geben Sie in der CLI die folgenden Befehle ein:

CLI-Befehle für IPv4

- `add ns acl <aclname> <aclaction> [-type (classic | dfd)] [-dfdhash <dfdhash>]`
- `set ns acl <aclname> <aclaction> [-dfdhash <dfdhash>`
- `show ns acl [<aclname>][-type (classic | DFD)]`
- `apply ns acls [-type (classic | DFD)]`
- `clear ns acls [-type (classic | DFD)]`
- `renumber ns acls [-type (classic | DFD)]`

CLI-Befehle für IPv6

- `add ns acl6 <acl6name> <acl6action> [-type (classic | dfd)][-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `set ns acl6 <acl6name> <acl6action> [-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `show ns acl6 [<acl6name>][-type (classic | DFD)]`
- `apply ns acls6 [-type (classic | DFD)]`
- `clear ns acls6 [-type (classic | DFD)]`
- `renumber ns acls6 [-type (classic | DFD)]`

Im Folgenden sind die verschiedenen Arten von Hash-Methoden aufgeführt, die Sie angeben können, um das Paket an den Flow-Prozessor zu leiten:

- SIP-SPORT-TAUCHSPORT

- SIP
- EINTAUCHEN
- EIN SCHLUCK EINTAUCHEN
- SIPSPORT

Einschränkungen

1. Die Verteilung des Verkehrsflusses auf die Clusterknoten ist nicht gewährleistet, da der Flow-Prozessor durch die vom Administrator konfigurierten Regeln bestimmt wird.
2. Der L2-Modus wird nicht unterstützt.
3. Die Knotengruppen und Striped SNIPs werden nicht unterstützt, da es keine Bereitstellungsszenarien gibt.
4. MPTCP wird nicht unterstützt.
5. Unterstützung nur für TCP-, UDP- und ICMP-Verkehr.
6. Der Cluster-over-L3-Modus wird nicht unterstützt.
7. Lokaler Prozess auf Serviceebene wird nicht unterstützt.

Verwenden des Multiple-Pfads mit gleichem Kostenfaktor (ECMP)

August 19, 2021

Mithilfe des ECMP-Mechanismus (Equal Cost Multiple Path) für eine Clusterbereitstellung geben aktive Clusterknoten die IP-Adressen des virtuellen Servers an. Der Clusterknoten, der den angekündigten Datenverkehr empfängt, steuert den Datenverkehr zu dem Knoten, der den Datenverkehr verarbeiten muss. Es kann redundante Steuerungen in gepunkteten und teilweise gestreiften virtuellen Servern geben. Aus diesem Grund werden ab NetScaler 11 die IP-Adressen von gespotteten und teilweise gestreiften virtuellen Servern für die Besitzerknoten angekündigt, wodurch die redundante Steuerung reduziert wird.

Sie benötigen detaillierte Kenntnisse der Routingprotokolle, um ECMP verwenden zu können. Weitere Informationen finden Sie unter Konfigurieren dynamischer Routen. Weitere Informationen zum Routing in einem Cluster finden Sie unter Routing in einem Cluster.

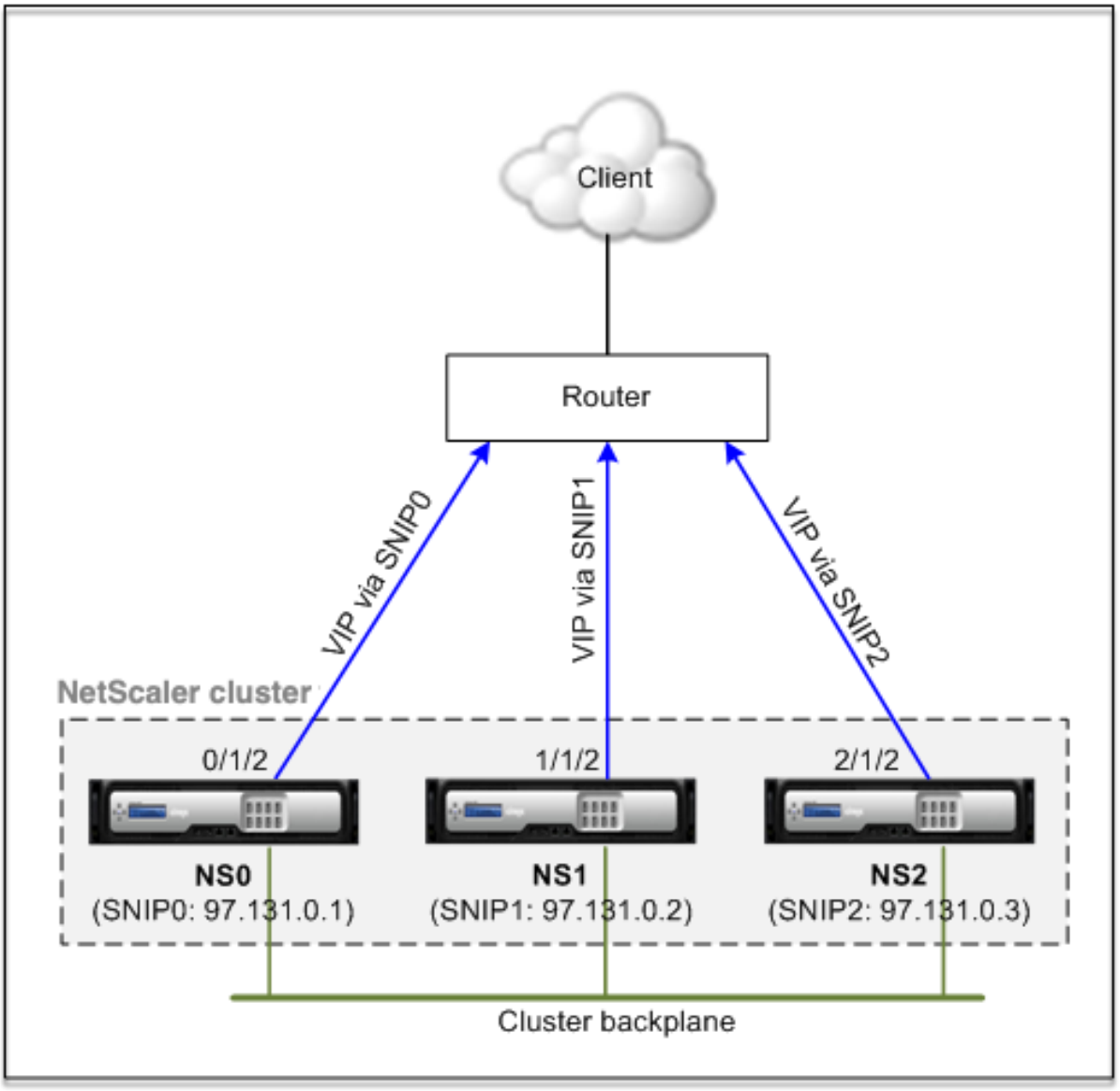
Um ECMP zu verwenden, müssen Sie zuerst Folgendes ausführen:

- Aktivieren Sie das erforderliche Routingprotokoll (OSPF, RIP, BGP oder ISIS) für die Cluster-IP-Adresse.
- Binden Sie die Schnittstellen und die gespotted IP-Adresse (mit aktiviertem dynamischem Routing) an ein VLAN.
- Konfigurieren Sie das ausgewählte Routingprotokoll und verteilen Sie die Kernel-Routen auf den ZeBOS mithilfe der VTYSH-Shell neu.

Führen Sie ähnliche Konfigurationen auf der Cluster-IP-Adresse und auf dem externen Verbindungsgerät durch.

> **Hinweis:**
>
> - Stellen Sie sicher, dass die Lizenzen auf dem Cluster dynamisches Routing unterstützen, andernfalls funktioniert ECMP nicht.
> - ECMP wird für virtuelle Platzhalterserver nicht unterstützt, da RHI eine VIP-Adresse benötigt, um Werbung für einen Router und virtuelle Platzhalterserver zu schalten. Da sie keine zugeordneten VIP-Adressen haben.

Abbildung 1. ECMP-Topologie



Wenn Sie den ECMP-Mechanismus für die Verkehrsverteilung in einer Clusterbereitstellung verwen-

den, kündigen die aktiven Cluster-Knoten die IP-Adressen des virtuellen Servers an den Upstream-Router an. Der ECMP-Router kann die VIP-Adresse über SNIP0, SNIP1 oder SNIP2 erreichen. Der Verkehrsfluss in Abbildung 1 wird wie folgt beschrieben:

1. Der Kunde sendet eine Anfrage an den im Cluster gehosteten VIP.
2. Der Upstream-Router, basierend auf den erlernten Routen der VIP, leitet das Paket an einen der Knoten weiter. Sagen wir NS1. Der Knoten NS1 ist der Flow Receiver.
3. Der Flow Receiver (NS1) bestimmt den Knoten, der den Datenverkehr verarbeiten muss, der als Flow Processor bezeichnet wird. Beispiel: Knoten NS2 ist der Flussprozessor.
4. Der Durchflussempfänger (NS1) mit SNIP1 (97.131.0.2) steuert die Anforderung mit SNIP2 (97.131.0.3) an den Flussprozessor (NS2).
5. Der Flow Processor (NS2) stellt eine Verbindung mit dem Server her.
6. Der Server verarbeitet die Anforderung und sendet die Antwort an die SNIP-Adresse, die die Anforderung an den Server gesendet hat.

Hinweise:

- Nur ACTIVE Knoten kündigen VIP-Routen an.
- INACTIVE Knoten kündigen keine VIP-Routen an.
- Alle ACTIVE Knoten kündigen gestreifte VIPs an.
- Nur ACTIVE Besitzerknoten kündigen Spotted- oder Teil-Striped-VIPs an.

So konfigurieren Sie ECMP auf dem Cluster mit der Befehlszeilenschnittstelle

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Aktivieren Sie das Routingprotokoll.

```
enable ns feature <feature>
```

Beispiel: Um das OSPF-Routingprotokoll zu aktivieren.

```
enable ns feature ospf
```

3. Fügen Sie ein VLANhinzu.

```
add vlan <id>
```

Beispiel

```
add vlan 97
```

4. Binden Sie die Schnittstellen der Clusterknoten an das VLAN.

```
bind vlan <id> -ifnum <interface_name>
```


Beispiel

```
bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Fügen Sie für jeden Knoten eine gespotted SNIP-Adresse hinzu, und aktivieren Sie dynamisches Routing.

```
add ns ip <SNIP> <netmask> -ownerNode <positive_integer> -
    dynamicRouting ENABLED
```

Beispiel

```
add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting
    ENABLED -type SNIP
add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting
    ENABLED -type SNIP
```

6. Binden Sie eine der Spotted-SNIP-Adressen an das VLAN. Wenn Sie eine Spotted-SNIP-Adresse an ein VLAN binden, werden alle anderen SNIP-Adressen, die auf dem Cluster in diesem Subnetz definiert sind, automatisch an das VLAN gebunden.

```
bind vlan <id> -IPAddress <SNIP> <netmask>
```

Beispiel

```
bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0
```

> **Hinweis:**
>
> Sie können NSIP-Adressen der Clusterknoten verwenden, anstatt SNIP-Adressen hinzuzufügen. Wenn ja, müssen Sie die Schritte 3 - 6 nicht ausführen.

7. Konfigurieren Sie das Routingprotokoll auf ZeBOS mit der VTYSH-Shell.

Beispiel:

So konfigurieren Sie ein OSPF-Routingprotokoll für die Knoten-IDs 0, 1 und 2.

```
vtysh
! interface vlan97 !
 router ospf   owner-node 0
ospf router-id 97.131.0.1   exit-owner-node
owner-node 1    ospf router-id 97.131.0.2
exit-owner-node
owner-node 2
```



```
8 ospf router-id 97.131.0.3   exit-owner-node   redistribute kernel
    network 97.0.0.0/8 area 0  !
```

> **Hinweis:**
>
> Für VIP-Adressen, die angekündigt werden sollen, wird die RHI-Einstellung mithilfe des Parameters vserverRHILevel wie folgt durchgeführt:

```
1 add ns ip <IPAddress> <netmask> -type VIP -vserverRHILevel <
    vserverRHILevel>
```

Für OSPF-spezifische RHI-Einstellungen gibt es weitere Einstellungen, die wie folgt durchgeführt werden können:

```
1 add ns ip <IPAddress> <netmask> -type VIP -ospfLSAType ( TYPE1 |
    TYPE5 ) -ospfArea <positive_integer>
```

Verwenden Sie den Befehl add ns ip6, um die vorherigen Befehle für IPv6-Adressen auszuführen.

8. Konfigurieren Sie ECMP auf dem externen Switch. Die folgenden Beispielkonfigurationen werden für den Cisco® Nexus 7000 C7010 Release 5.2 (1) Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

```
1 //For OSPF (IPv4 addresses) Global config: Configure terminal
    feature ospf    Interface config:  Configure terminal
    interface Vlan10      no shutdown      ip address 97.131.0.5/8
       Configure terminal  router ospf 1  network 97.0.0.0/8 area
    0.0.0.0  ---------------------------------
2
3 //For OSPFv3 (IPv6 addresses) Global config:  Configure terminal
    feature ospfv3    Configure terminal  interface Vlan10      no
    shutdown      ipv6 address use-link-local-only      ipv6 router
     ospfv3 1 area 0.0.0.0    Configure terminal  router ospfv3 1
```

Router-Monitoring-Clusterknoten in der ECMP-Bereitstellung

In einem Cluster-Setup können Sie auf einem Besitzerknoten mit einer SNIP-Adresskonfiguration nun die Option OwnerDownResponse deaktivieren. Standardmäßig ist die Option aktiviert, sodass der Knoten auf eine ICMP/ARP/ICMP6/ND6-Anforderung vom Upstream-Router reagieren kann. Sie können diese Option jetzt deaktivieren, damit der Router überwachen kann, ob ein Clusterknoten aktiv oder inaktiv ist. Wenn der Router eine Anforderung sendet und die Option deaktiviert ist, identifiziert er den Besitzerknoten als inaktiv und nicht für die Verkehrsverteilung verfügbar.

So konfigurieren Sie ECMP für die Verteilung statischer Routen mit der Befehlszeilenschnittstelle

```
add ns ip <ipddress> <netmask> -ownernode <node-id>  - ownerDownResponse
    disable
```

Anwendungsfall: ECMP mit BGP-Routing

January 19, 2021

So konfigurieren Sie ECMP mit BGP-Routingprotokoll:

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Aktivieren Sie das BGP-Routingprotokoll.

```
> enable ns feature bgp
```

3. Fügen Sie VLAN hinzu und binden Sie die erforderlichen Schnittstellen.

```
> add vlan 985
> bind vlan 985 -ifnum 0/0/1 1/0/1
```

4. Fügen Sie die gespotted IP-Adresse hinzu und binden Sie sie an das VLAN.

```
> add ns ip 10.100.26.14 255.255.255.0 -ownerNode 1 -
    dynamicRouting ENABLED
> add ns ip 10.100.26.15 255.255.255.0 -ownerNode 2 -
    dynamicRouting ENABLED
> bind vlan 985 -ipAddress 10.100.26.10 255.255.255.0
```

5. Konfigurieren Sie das BGP-Routing-Protokoll auf ZeBOS mit der VTYSH-Shell.

```
> vtysh conf t router bgp 65535 neighbor 10.100.26.1 remote-as
    65535
```

6. Konfigurieren Sie BGP am externen Switch. Die folgenden Beispielkonfigurationen werden für den Cisco® Nexus 7000 C7010 Release 5.2 (1) Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

```
> router bgp 65535 no synchronization
  bgp log-neighbor-changes neighbor 10.100.26.14 remote-as 65535
     neighbor 10.100.26.15 remote-as 65535 no auto-summary
  dont-capability-negotiate
```



```
4   dont-capability-negotiate
5   no dynamic-capability
```

Konfiguration des Cluster-ECMP mithilfe des Cisco Nexus 7000-Switches mit Routing-Protokoll

May 11, 2023

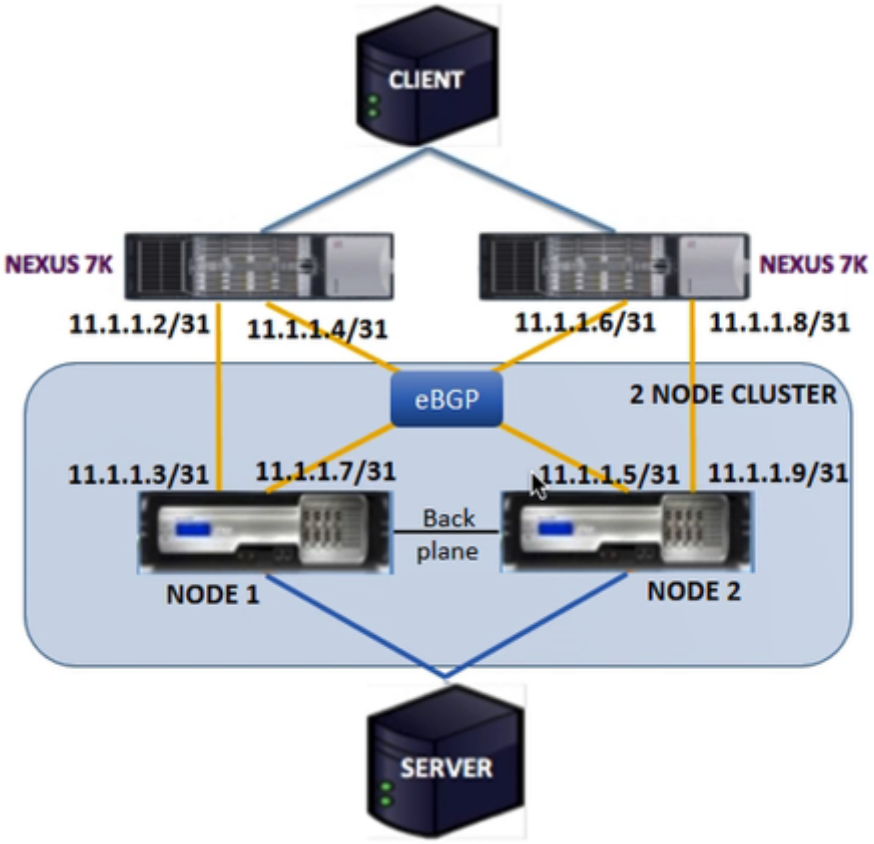
Mit ECMP über ein Cluster-Setup ist eine NetScaler-Appliance in der Lage, den Datenverkehr über ein Routing-Protokoll zu verarbeiten. Der ECMP-Mechanismus hilft bei der Bekanntgabe der IP-Adressen des virtuellen Servers über alle aktiven Clusterknoten.

Um ECMP verwenden zu können, müssen Sie zuerst das BGP-Protokoll auf der Cluster-IP-Adresse aktivieren. Binden Sie die Schnittstellen und die entdeckte IP-Adresse (mit aktiviertem dynamischem Routing) an ein VLAN. Konfigurieren Sie das ausgewählte Routing-Protokoll und verteilen Sie die Kernel-Routen auf dem ZeBOS mithilfe der VTYSH-Shell neu.

Anwendungsfall: Clustern Sie ECMP mithilfe eines Cisco Nexus 7000-Switches mit Routing-Protokoll

Stellen Sie sich ein Beispiel für eine Cluster-Bereitstellung mit einem Cisco Nexus 7000-Switch vor:

- Zwei NetScaler-Appliances (Node 1 und Node 2), die mit dem Nexus-Switch (Upstream) verbunden sind.
- Zwei Cisco Nexus 7000-Switches.
- Client und Server (leitet HTTP-Verkehr über den Nexus-Switch ab). Mit aktiviertem Hot Standby Router Protocol (HSRP) auf der Clientseite.



Voraussetzungen

Beachten Sie die folgenden Punkte, bevor Sie Clusterknoten auf einer NetScaler-Appliance konfigurieren.

1. Alle Appliances müssen vom gleichen Plattformtyp sein.
2. Das Border Gateway Protocol (BGP) muss auf den Clusterknoten aktiviert sein.

Konfiguration mithilfe der CLI auf einer NetScaler-Appliance

1. Melden Sie sich bei einer Appliance an (z. B. Appliance mit NSIP-Adresse 1.1.1.1)
2. So fügen Sie einen Clusterknoten hinzu.

```
1 add cluster node 0 1.1.1.2 -state ACTIVE -backplane 0/10/8
```

3. So fügen Sie die Cluster-IP-Adresse hinzu

```
1 add ns ip 1.1.1.10 255.255.255.254 -type clip
```

4. Speichern Sie die Konfiguration


```
save ns config
```

5. Warmer Neustart der Appliance

```
reboot -warm
```

6. So fügen Sie Knoten 1 mit CLIP hinzu

```
add cluster node 1 2.2.2.2 -state ACTIVE -backplane 1/10/8
```

7. So verbinden Sie einen Knoten mit dem Cluster

```
join cluster -clip 1.1.1.10 -password nsroot
```

8. Führen Sie die folgende Konfiguration auf CLIP durch
   - `enable ns feature bgp ospf DYNAMICROUTING`
   - `add ns ip 11.1.1.3 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`
   - `add ns ip 11.1.1.7 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`
   - `add ns ip 11.1.1.5 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`
   - `add ns ip 11.1.1.9 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`

Auf dem Cisco Nexus Router (11.1.1.2/31 und 11.1.1.4/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`

```
> interface vlan100
    no shutdown
    ip address 50.1.1.1/8
     hsrp 50
      ip 50.50.50.50

> interface Ethernet 4/15
```



```
8       ip address 11.1.1.2/31
9       no shutdown
10
11  >   interface Ethernet 4/19
12      ip address 11.1.1.4/31
13      no shutdown
14
15  >   interface Ethernet 4/22
16      switchport
17       switchport access vlan 100
```

Auf dem Cisco Nexus Router (11.1.1.6/31 und 11.1.1.8/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`

```
1   >   interface vlan100
2       no shutdown
3       no ip redirects
4       ip address 50.1.1.2/8
5        hsrp 50
6        ip 50.50.50.50
7
8   >   interface Ethernet 4/13
9       ip address 11.1.1.6/31
10      no shutdown
11
12  >   interface Ethernet 4/15
13      ip address 11.1.1.8/31
14      no shutdown
15
16  >   interface Ethernet 4/22
17      switchport
18      switchport access vlan 100
```

Für das BGP-Protokoll müssen Sie die folgenden Konfigurationen auf CLIP der NetScaler Appliance durchführen:

```
1  >  vtysh
2  ns# router bgp 1
3   redistribute kernel
```



```
 owner-node 0
 neighbor 11.1.1.2 remote-as 2
 neighbor 11.1.1.2 as-origination-interval 1
 neighbor 11.1.1.2 advertisement-interval 0
 neighbor 11.1.1.6 remote-as 2
 neighbor 11.1.1.6 as-origination-interval 1
 neighbor 11.1.1.6 advertisement-interval 0
owner-node 1
 neighbor 11.1.1.4 remote-as 2
 neighbor 11.1.1.4 as-origination-interval 1
 neighbor 11.1.1.4 advertisement-interval 0
 neighbor 11.1.1.8 remote-as 2
 neighbor 11.1.1.8 as-origination-interval 1
 neighbor 11.1.1.8 advertisement-interval 0
exit-owner-node
```

Durchführen der folgenden Konfigurationen auf dem Cisco Nexus-Router (11.1.1.3 und 11.1.1.5)

```
> ip access-list acl1
  10 permit ip 50.0.0.0/8 any
  route-map test permit
  match ip address acl1
 router bgp 2
  address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
 neighbor 11.1.1.3 remote-as 1
  address-family ipv4 unicast
  neighbor 11.1.1.5 remote-as 1
 address-family ipv4 unicast
```

Durchführen der folgenden Konfigurationen auf dem Cisco Nexus-Router (11.1.1.7 und 11.1.1.9)

```
> ip access-list acl1
   10 permit ip 50.0.0.0/8 any
  route-map test permit 1
   match ip address acl1
  router bgp 2
   address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
  neighbor 11.1.1.7 remote-as 1
   address-family ipv4 unicast
  neighbor 11.1.1.9 remote-as 1
   address-family ipv4 unicast
```


Für das OSPF-Protokoll müssen Sie die folgenden Konfigurationen auf CLIP der NetScaler Appliance durchführen:

```
> vtysh
ns# router osfp 1
redistribute kernel
owner-node 0
 network 15.1.1.2/31 area 0
 network 15.1.1.6/31 area 0
exit-owner-node

owner-node 1
 network 15.1.1.4/31 area 0
 network 15.1.1.8/31 area 0
exit-owner-node

route-map map2 permit 1
set metric 10
```

Auf dem Cisco Nexus Router (11.1.1.2/31 und 11.1.1.4/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

```
> route-map- map2 permit 1
   set metric 10

   interface Ethernet4/15
     ip address 15.1.1.2/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

   interface Ethernet4/19
     ip address 15.1.1.4/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

   router ospf 1
    router-id 1.1.1.1
    redistribute direct route-map map2
```

Auf dem Cisco Nexus Router (11.1.1.7/31 und 11.1.1.9/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

```
> route-map- map2 permit 1
    set metric 10

```



```
4     interface Ethernet4/13
5       ip address 15.1.1.6/31
6       ip router ospf 1 area 0.0.0.0
7       no shutdown
8
9      interface Ethernet4/15
10      ip address 15.1.1.8/31
11      ip router ospf 1 area 0.0.0.0
12      no shutdown
13
14     router ospf 1
15       router-id 1.1.1.2
16       redistribute direct route-map map2
```

Verwenden der Clusterlink-Aggregation

May 11, 2023

Die Cluster-Link-Aggregation ist eine Gruppe von Schnittstellen von Clusterknoten. Es ist eine Erweiterung der NetScaler Link Aggregation. Der einzige Unterschied besteht darin, dass die Schnittstellen in der Cluster-Link-Aggregation zwar von demselben Gerät stammen müssen, die Schnittstellen zwar von verschiedenen Knoten des Clusters stammen. Weitere Informationen zur Link-Aggregation finden Sie unter Konfigurieren der Link-Aggregation.

> **Wichtig**
>
> - Die Cluster-Link-Aggregation wird für einen Cluster von Hardware-Appliances (MPX) unterstützt.
> - Die Cluster-Link-Aggregation wird für einen Cluster von virtuellen (VPX) Appliances unterstützt, die auf ESX- und KVM-Hypervisoren bereitgestellt werden, mit den folgenden Einschränkungen:
> - Es müssen dedizierte Schnittstellen verwendet werden. Das bedeutet, dass die Schnittstellen nicht mit anderen virtuellen Maschinen geteilt werden dürfen.
> - Wenn ein Knoten INAKTIV wird, wird die entsprechende Cluster-LA-Schnittstelle als ausgeschaltet markiert, sodass der Datenverkehr nicht an einen INAKTIVEN Knoten gesendet wird.
> - Wenn ein Knoten AKTIV wird, wird die entsprechende Cluster-LA-Schnittstelle als eingeschaltet markiert.

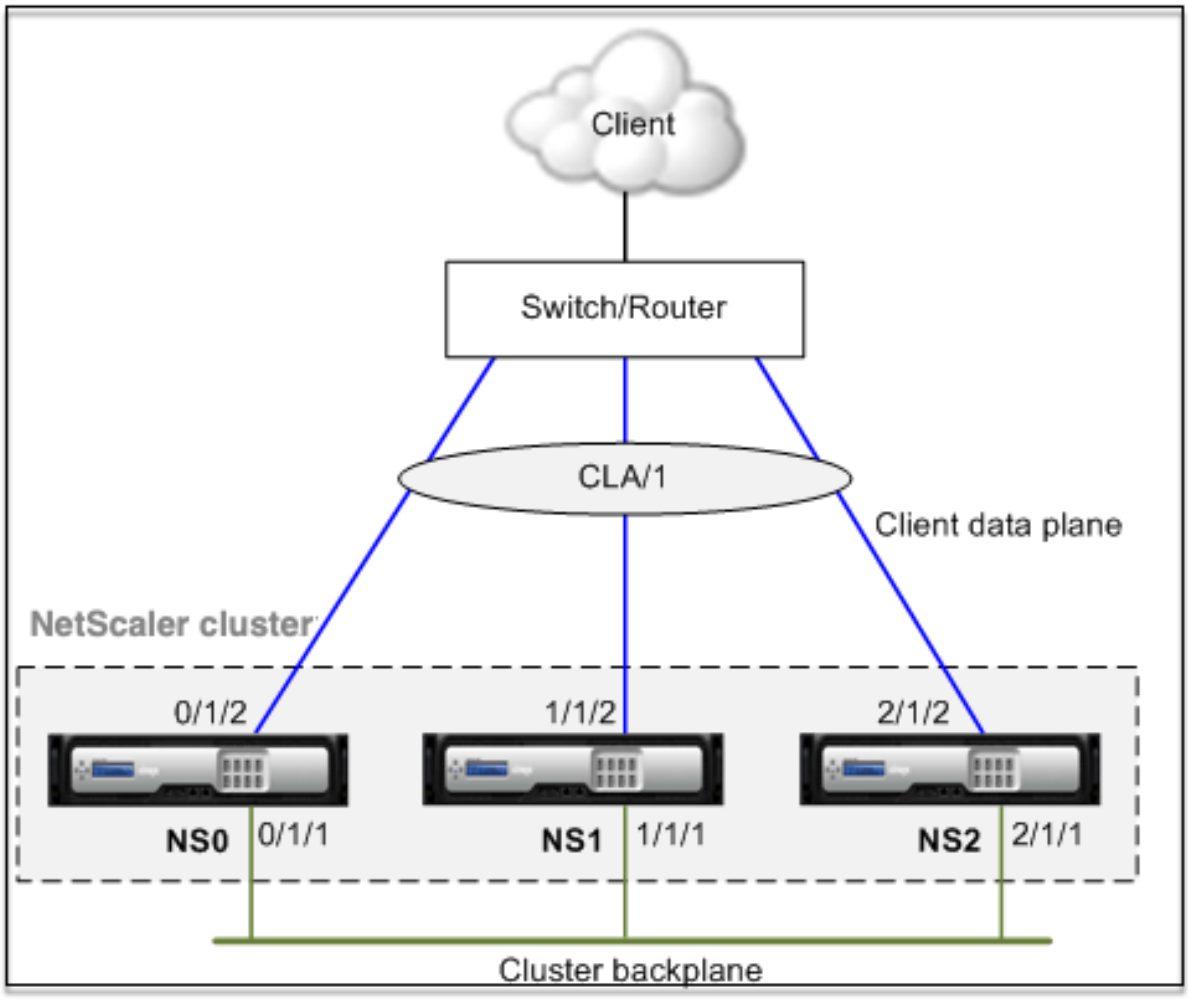
- Wenn die Cluster-Link-Aggregationsmitgliedsschnittstellen manuell deaktiviert werden oder wenn die Cluster-Link-Aggregation selbst manuell deaktiviert wird, wird die Fähigkeit zur Abschaltung der Schnittstelle nur durch den LACP-Timeout-Mechanismus erreicht.
- Jumbo MTU wird bei der LACP-Cluster-Link-Aggregation nicht unterstützt.

Hinweis: Die Cluster-Link-Aggregation wird auf VPX-Appliances, die auf XenServer, AWS und Hyper-V bereitgestellt werden, nicht unterstützt.

- Ab Version 12.0 wird die Cluster-Link-Aggregation auf NetScaler SDX-Appliances unterstützt.
- Die Anzahl der Schnittstellen, die an Cluster LA gebunden werden können, beträgt 16 (von jedem Knoten aus). Die maximale Anzahl von Schnittstellen in Cluster LA kann (16 * n) sein, wobei n die Anzahl der Knoten in einem Cluster ist. Die Gesamtzahl der Schnittstellen in Cluster LA hängt von der Anzahl der Schnittstellen für jeden Portkanal auf dem Upstream-Switch ab.
- Wenn eine NetScaler-Appliance Intel Fortville-Schnittstellen verwendet, kann die Umstellung eines Clusterknotens in den passiven Modus zu einem Ausfall mit CLAG für einige Sekunden führen. Das Problem tritt auf, weil LACP aktiviert ist, damit CLAG ordnungsgemäß funktioniert, und die Ausfallzeit von den NIC-LACP-Timern abhängt.

Stellen Sie sich beispielsweise einen Cluster mit drei Knoten vor, in dem alle drei Knoten mit dem Upstream-Switch verbunden sind. Ein Cluster-LA-Kanal (CLA/1) wird durch die Bindungsschnittstellen 0/1/2, 1/1/2 und 2/1/2 gebildet.

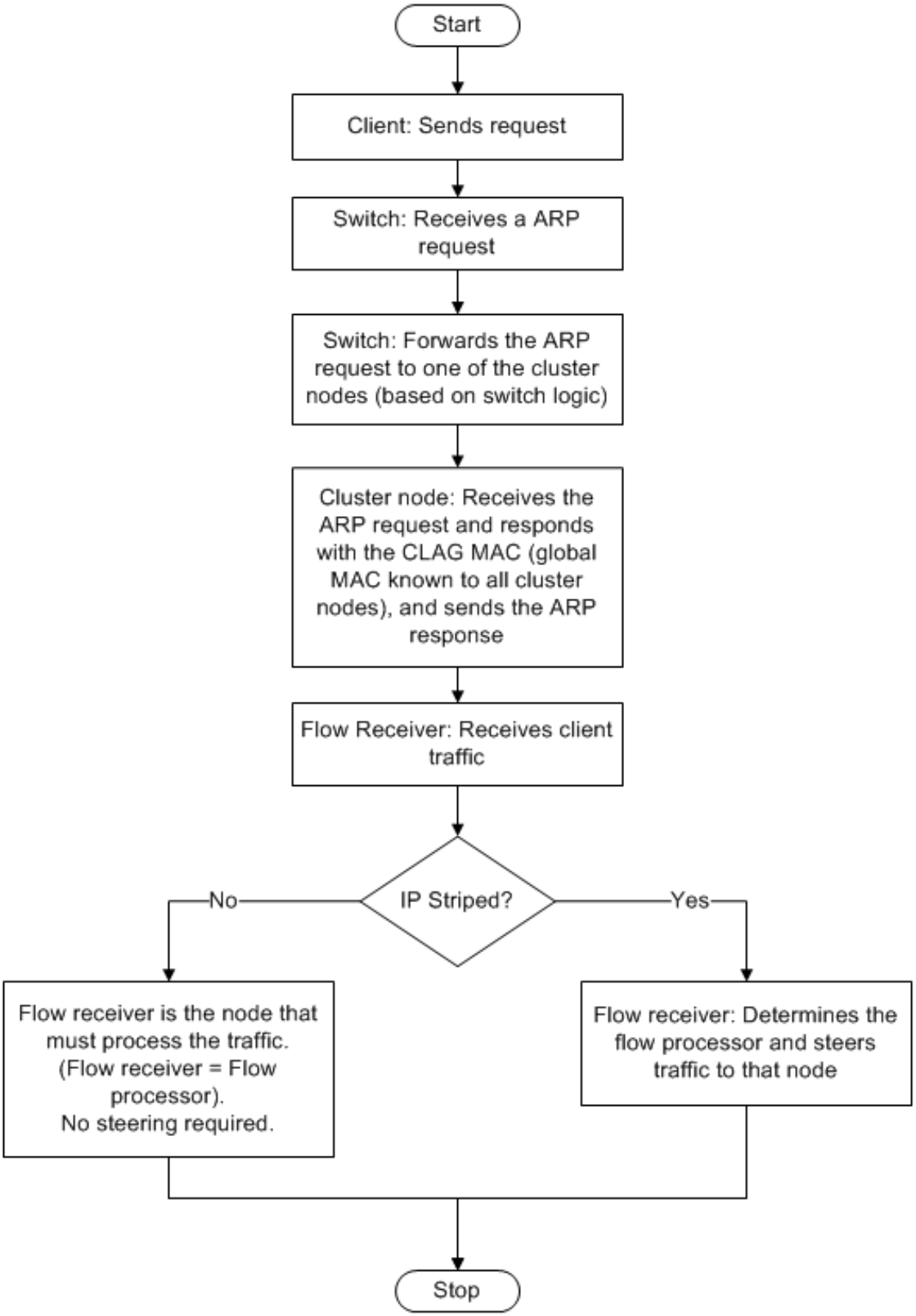
Abbildung 1. Topologie der Cluster-Link-Aggregation



Ein Cluster-LA-Kanal hat folgende Attribute:

- Jeder Kanal hat einen eindeutigen MAC, auf den sich die Clusterknoten einigen.
- Der Kanal kann sowohl die Schnittstellen lokaler als auch entfernter Knoten binden.
- In einem Cluster werden maximal vier Cluster-LA-Kanäle unterstützt.
- Backplane-Schnittstellen können nicht Teil eines Cluster-LA-Kanals sein.
- Wenn eine Schnittstelle an einen Cluster-LA-Kanal gebunden ist, haben die Kanalparameter Vorrang vor den Netzwerkschnittstellenparametern. Eine Netzwerkschnittstelle kann nur an einen Kanal gebunden werden.
- Der Verwaltungszugriff auf einen Clusterknoten darf nicht auf einem Cluster-LA-Kanal (z. B. CLA/1) oder seinen Mitgliedsschnittstellen konfiguriert werden. Dies liegt daran, dass, wenn der Knoten INAKTIV ist, die entsprechende Cluster-LA-Schnittstelle als ausgeschaltet markiert ist und daher den Verwaltungszugriff verliert.

Abbildung 2. Verkehrsverteilungsfluss mithilfe von Cluster LA



Unterstützung für Backup und Wiederherstellung von Cluster-LA auf NetScaler MPX

Sie können das Cluster-Setup von LA auf NetScaler MPX Backup und wiederherstellen. Die Cluster-LA-MAC-Adresse ist unabhängig von der physikalischen Schnittstellen-MAC-Adresse der Clusterknoten und kann sich nach dem Backup- und Wiederherstellungsprozess ändern. Der Cluster LA kann den Datenverkehr bedienen, nachdem ein Cluster-Wiederherstellungsprozess abgeschlossen ist. Weitere Informationen zum Backup und Wiederherstellen finden Sie unter Sichern und Wiederherstellen des Cluster-Setups

Statische Cluster-Link-Aggregation

August 19, 2021

Sie müssen einen statischen Cluster-LA-Kanal auf der Cluster-IP-Adresse und auf dem externen Verbindungsgerät konfigurieren. Konfigurieren Sie nach Möglichkeit den Upstream-Switch so, dass der Datenverkehr auf der Grundlage der IP-Adresse oder des Ports statt der MAC-Adresse verteilt wird.

So konfigurieren Sie einen statischen Cluster-LA-Kanal mit der CLI

1. Melden Sie sich bei der Cluster-IP-Adresse an.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass Sie den Cluster-LA Kanal für die Cluster-IP-Adresse konfigurieren, bevor Sie die Linkaggregation auf dem externen Switch konfigurieren. Andernfalls leitet der Switch den Datenverkehr zum Cluster weiter, obwohl der Cluster-LA-Kanal nicht konfiguriert ist. Dies kann zu Verkehrsverlust führen.

2. Erstellen Sie einen Cluster-LA-Kanal.

   ```
   add channel <id> -speed <speed>
   ```

   Beispiel

   ```
   add channel CLA/1 -speed 1000
   ```

   > **Hinweis:**
   >
   > Sie dürfen die Geschwindigkeit nicht als AUTO angeben. Vielmehr müssen Sie die Geschwindigkeit explizit als 10, 100, 1000 oder 10000 angeben. Nur Schnittstellen mit der Geschwindigkeit, die mit dem `<speed>` Attribut im Cluster-LA-Kanal übereinstimmt,

> werden der aktiven Verteilerliste hinzugefügt.

3. Binden Sie die erforderlichen Schnittstellen an den Cluster-LA-Kanal. Stellen Sie sicher, dass die Schnittstellen nicht für die Clusterrückwandplatine verwendet werden.

```
bind channel <id> <ifnum>
```

Beispiel

```
bind channel CLA/1 0/1/2 1/1/2 2/1/2
```

4. Überprüfen Sie die Konfigurationen.

```
show channel <id>
```

Beispiel

```
show channel CLA/1
```

> **Hinweis:**
>
> Sie können den Cluster-LA-Kanal mit dem `bind vlan` Befehl an ein VLAN binden. Die Schnittstellen des Kanals werden automatisch an das VLAN gebunden.

5. Konfigurieren Sie statische LA am externen Switch. Die folgenden Beispielkonfigurationen werden für das Cisco® Nexus 7000 C7010 Release 5.2 (1) bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

```
Global config:
Configure terminal

Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown

interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown
```


Dynamische Clusterlink-Aggregation

May 11, 2023

Der dynamische Cluster-LA-Kanal verwendet das Link Aggregation Control Protocol (LACP).

Sie müssen ähnliche Konfigurationen für die Cluster-IP-Adresse und auf dem externen Verbindungsgerät durchführen. Wenn möglich, konfigurieren Sie den Upstream-Switch so, dass der Datenverkehr basierend auf der IP-Adresse oder dem Port anstelle der MAC-Adresse verteilt wird.

> **Wichtige Punkte**
>
> - Aktivieren Sie LACP (indem Sie den LACP-Modus entweder als ACTIVE oder PASSIVE angeben).

```
>**Note**
>
> Make sure the LACP mode is not set as PASSIVE on both the NetScaler
   cluster and the external connecting device.
```

> - Geben Sie auf jeder Schnittstelle denselben LACP-Schlüssel an, der Teil des Kanals sein soll. Zum Erstellen eines Cluster-LA-Kanals kann der LACP-Schlüssel einen Wert von 5 bis 8 haben. Wenn Sie beispielsweise den LACP-Schlüssel an den Schnittstellen 0/1/2, 1/1/2 und 2/1/2 auf 5 setzen, wird CLA/1 erstellt. Die Schnittstellen 0/1/2, 1/1/2 und 2/1/2 werden automatisch an CLA/1 gebunden. Ebenso wird der CLA/2-Kanal erstellt, wenn Sie den LACP-Schlüssel auf 6 setzen.
> - Geben Sie den LAG-Typ als Cluster an.

So konfigurieren Sie einen dynamischen Cluster-LA-Kanal mithilfe der CLI

Geben Sie an der Cluster-IP-Adresse für jede Schnittstelle, die Sie dem Cluster-LA-Kanal hinzufügen möchten, Folgendes ein:

```
set interface <id> -lacpMode <lacpMode> -lacpKey <positive_integer> -
lagType CLUSTER<!--NeedCopy-->
```

Beispiel:

Konfigurieren eines Cluster-LA-Kanals CLA/1 mit 3 Schnittstellen.

```
> set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
```


> **Hinweis**
>
> Optional können Sie Link-Redundanz in einem Cluster mit LACPaktivieren.

Konfigurieren Sie dynamisches LA auf dem externen Switch. Die folgenden Beispielkonfigurationen sind für das Cisco® Nexus 7000 C7010 Version 5.2 (1) bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

```
Global config:
Configure terminal
feature lacp
Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown

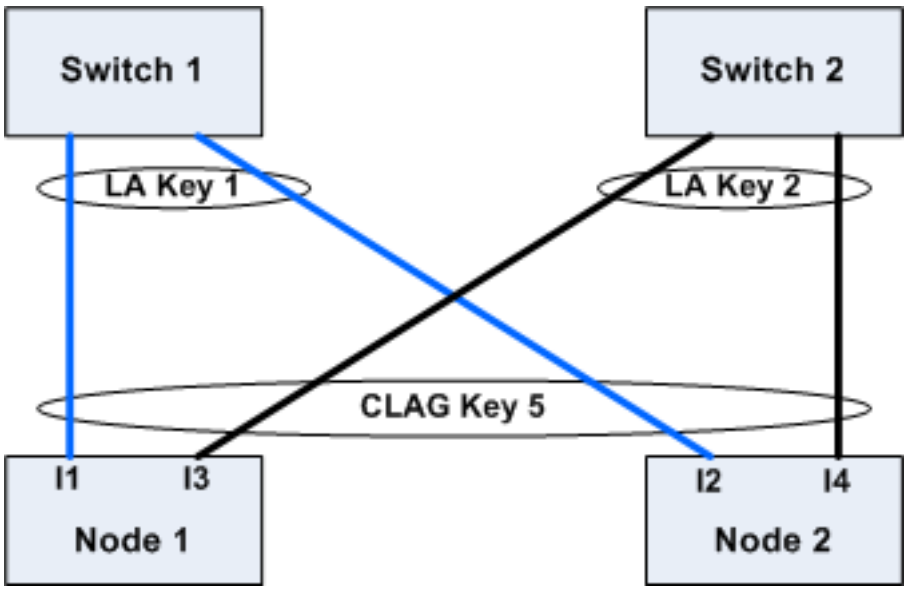
interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown
```

Verbindungsredundanz in einem Cluster mit LACP

May 11, 2023

Ein NetScaler-Cluster bietet Link-Redundanz für LACP, um sicherzustellen, dass alle Knoten über denselben Partnerschlüssel verfügen.

Um die Notwendigkeit einer Link-Redundanz zu verstehen, betrachten wir das Beispiel des folgenden Cluster-Setups zusammen mit den zugehörigen Fällen (wobei Fall 3 zu beachten ist):



In diesem Setup sind die Schnittstellen I1, I2, I3 und I4 mit KEY 5 an den LACP-Kanal gebunden. Auf der Partnerseite sind I1 und I2 mit Switch 1 verbunden, um mit KEY 1 einen einzigen LA-Kanal zu bilden. In ähnlicher Weise sind I3 und I4 mit Switch 2 verbunden, um mit KEY 2 einen einzigen LA-Kanal zu bilden.

Lassen Sie uns nun die folgenden Fälle betrachten, um die Notwendigkeit einer Link-Redundanz zu verstehen:

- **Fall 1: Switch 1 ist aktiv und Switch 2 ist ausgefallen**

  In diesem Fall würde Cluster LA auf beiden Knoten aufhören, LacPDUs von Key2 zu empfangen, und würde beginnen, LacPDUs von Key1 zu empfangen. Auf beiden Knoten ist Cluster LA mit KEY 1 und I1 verbunden und I2 ist UP und der Kanal auf beiden Knoten wäre UP.

- **Fall 2: Switch1 geht aus und Switch2 wird UP**

  In diesem Fall würde Cluster LA auf beiden Knoten aufhören, LacPDUs von Key1 zu empfangen, und würde beginnen, LacPDUs von Key2 zu empfangen. Auf beiden Knoten ist Cluster LA mit Key2 und I3 verbunden und I4 ist UP und der Kanal auf beiden Knoten wäre UP.

- **Fall 3: Sowohl Switch1 als auch Switch2 sind in Betrieb**

  In diesem Fall ist es möglich, dass Cluster LA auf Node1 Key1 als Partner wählt und Cluster LA auf Node2 Key2 als Partner wählt. Das bedeutet, dass I1 auf Node1 und I4 auf Node2 Datenverkehr empfangen, was unerwünscht ist. Dies kann passieren, weil sich die LACP-Staatsmaschine auf Knotenebene befindet und ihre Partner nach dem Prinzip „Wer zuerst kommt, mahlt zuerst“ auswählt.

  Um diese Probleme zu lösen, wird die Link-Redundanz von dynamischem Cluster-LA unterstützt. Um die Link-Redundanz auf einem Kanal oder einer Schnittstelle zu konfigurieren, müssen Sie sie aktivieren und optional den Schwellendurchsatz wie folgt angeben:


```
set channel CLA/1 -linkRedundancy ON -lrMinThroughput <positive_integer
>
```

Der Durchsatz der Partnerkanäle wird anhand des konfigurierten Schwellendurchsatzes überprüft. Der Partnerkanal, der den Schwellendurchsatz erfüllt, wird nach dem First-in-First-Out-Verfahren (FIFO) ausgewählt. Wenn keiner der Partnerkanäle den Schwellenwert erreicht oder wenn der Schwellendurchsatz nicht konfiguriert ist, wird der Partnerkanal mit der maximalen Anzahl von Links ausgewählt.

> **Hinweis**
>
> Der Schwellendurchsatz kann ab NetScaler 11 konfiguriert werden.

Verwenden des USIP-Modus im Cluster

May 11, 2023

Im Modus "Quell-IP" (USIP) leitet der Cluster oder die NetScaler Appliance jedes Paket mit der Client-IP-Adresse an den entsprechenden Back-End-Server weiter.

Verkehrsverteilung im USIP-Modus

Das Verhalten im USIP-Modus unterscheidet die Verteilung des Datenverkehrs über die Clientdatenebene und die Serverdatenebene in der ECMP- und CLAG-Bereitstellung. Der folgende Abschnitt enthält weitere Informationen zum Verhalten im USIP-Modus. Weitere Informationen zu CLAG im USIP-Modus finden Sie unter Verwenden der Cluster-Link-Aggregation.

USIP-Modus

Der Cluster verwendet die Client-IP, um die serverseitige Verbindung zu öffnen. Der Quellport wird möglicherweise basierend auf der `useproxyport` Einstellung beibehalten oder auch nicht.

USIP `useproxyport`-Szenarien

Der USIP `useproxyport` ist für den Verkehrsfluss EIN, der Quellport wird so ausgewählt, dass der umgekehrte Datenverkehr zum Flow-Prozessor hasht. Es gewährleistet eine einzelne Lenkung auf der Serverseite.

Der USIP `useproxyport` ist für den Verkehrsfluss AUS, der Quellport bleibt erhalten und daher gibt es eine doppelte Lenkung auf der Serverseite.

Wichtig

- Wenn USIP eingeschaltet ist, wird die Client-IP in der Back-End-Serververbindung verwendet, und die Verteilung des Datenverkehrs für die Reaktion ist über Clusterknoten hinweg erforderlich. Sie können die ECMP- oder CLAG-Bereitstellung für die Datenverkehrsverteilung serverseitig verwenden. In Ermangelung einer Datenverkehrsverteilung auf der Serverseite könnte der gesamte Rücklaufverkehr auf einem einzigen Clusterknoten landen, was zu Staus führt.
- Der `set rsskeytype -rsskey symmetric` Befehl wird verwendet, um die doppelte Lenkung auf eine einzelne Steuerung des Verkehrs in den `useproxyport` Off-Bereitstellungen zu reduzieren. Wo das 4-Tupel für die Verbindung für die Server- und Clientseite gleich bleibt. Zum Beispiel virtueller Server im Platzhaltermodus im MAC-Modus.

Einschränkungen

Die USIP funktioniert nicht, wenn der lokale Prozess deaktiviert ist.

Bereitstellung im USIP-Modus

Die folgende Abbildung zeigt eine Bereitstellung im USIP-Modus in einem Cluster-Setup.

Konfigurieren Sie Folgendes mit CLI

1. Aktivieren Sie das Routingprotokoll.

```
enable ns feature <feature>
```

Beispiel:

```
enable ns feature ospf
```

2. Fügen Sie für jeden Knoten eine gespotted SNIP-Adresse hinzu, und aktivieren Sie dynamisches Routing.

```
add ns ip <SNIP> <netmask> -dynamicRouting ( ENABLED | DISABLED )
    -ownerNode <positive_interger>  -ownerdownResponse ( YES | NO
    )
```

Beispiel

```
-  add ns ip 192.0.2.1 255.255.255.0 -dynamicRouting ENABLED  -
    ownerNode 0  -ownerDownResponse NO
```



```
2 - add ns ip 192.0.2.2 255.255.255.0 -dynamicRouting ENABLED -
    ownerNode 1 - ownerDownResponse NO
3 - add ns ip 192.0.2.3 255.255.255.0 -dynamicRouting ENABLED -
    ownerNode 2 - ownerDownResponse NO
```

3. Fügen Sie ein VLANhinzu.

```
1 add vlan <id>
```

Beispiel

```
1 add vlan 300
```

4. Binden Sie die Schnittstellen der Clusterknoten an das VLAN.

```
1 bind vlan <id> -ifnum <interface_name>
```

Beispiel

```
1 bind vlan 300 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Binden Sie eine der Spotted-SNIP-Adressen an das VLAN. Wenn Sie eine entdeckte SNIP-Adresse an ein VLAN binden, werden alle anderen gespotteten SNIP-Adressen, die im Cluster in diesem Subnetz definiert sind, automatisch an das VLAN gebunden.

```
1 bind vlan <id> -IPAddress <ip_addr | ipv6_addr> -netmask
```

Beispiel

```
1 bind vlan 300 - IPAddress 192.0.2.1 255.255.255.0
```

6. Konfigurieren Sie das Routingprotokoll auf ZeBOS mit der VTYSH-Shell. Konfigurieren Sie das OSPF-Routingprotokoll für Knoten-IDs 0, 1 und 2.

```
1  vtysh
2  configure terminal
3  ns block-sec-rtadv
4  router ospf
5  owner -node 0
6  router-id 192.0.2.1
7  exit-owner-node
8  owner-node 1
9  router-id 192.0.2.2
10 exit-owner-node
11 owner-node 2
```



```
router-id 192.0.2.3
exit-owner-node
network 192.0.2.0/24 area 0

default-information originate always
```

7. Führen Sie die folgenden Konfigurationen auf dem Router Cisco 3750 über die Befehlszeilenschnittstelle durch.

```
Configure terminal
feature ospf
interface vlan300
no shutdown
ip address 192.0.2.100/24
Configure terminal
router ospf 1
router-id 192.0.2.100
network 192.0.2.0 0.0.0.255 area 0
```

Hinweise

- Die Datenverkehrsverteilung auf Client und Server muss nicht identisch sein. Beispielsweise können Sie ECMP auf der Clientseite und CLAG serverseitig oder umgekehrt konfigurieren.
- Planen Sie für zusätzliche Kapazität der Backplane, da es im USIP-Einsatz mehr Lenkungsaufwand gibt.
- Die Konfiguration im Zusammenhang mit CLAG und Static Route (MSR) überwachen muss auf Serverseite gleich bleiben.
- Die Verkehrssteuerung befindet sich eher in den Bereitstellungen im USIP-Modus.

Verwalten des NetScaler Clusters

May 11, 2023

Nachdem Sie einen Cluster erstellt und den erforderlichen Mechanismus zur Verkehrsverteilung konfiguriert haben, kann der Cluster den Datenverkehr bereitstellen. Während der Lebensdauer des Clusters können Sie die folgenden Clusteraufgaben ausführen:

- Konfiguration von Knotengruppen
- Knoten eines Clusters deaktivieren
- Entdecken von NetScaler-Appliances

- Statistiken anzeigen
- Synchronisieren von Clusterkonfigurationen und Clusterdateien
- Synchronisieren der Uhrzeit zwischen den Knoten
- Aktualisierung oder Herabstufung der Software von Clusterknoten

Konfigurieren von Linksets

January 19, 2021

Linkset ist eine Gruppe von Schnittstellen von Clusterknoten, die zur selben Broadcast-Domäne gehören. In Linksets enthält jeder Knoten die Informationen darüber, welche Schnittstellen anderer Knoten mit derselben Broadcast-Domäne verbunden sind.

> **Hinweis:**
>
> Linksets sind eine obligatorische Konfiguration in den folgenden Szenarien:
>
> - Für Bereitstellungen, die eine MAC-basierte Weiterleitung (MBF) erfordern.
> - Für den Modus "-m MAC", der auf dem virtuellen Server zusammen mit dem globalen MBF-Modus aktiviert ist.
> - Verbesserung der Verwaltbarkeit von ACL- und L2-Richtlinien mit Schnittstellen. Sie definieren einen Linksatz der Schnittstellen und fügen ACL- und L2-Richtlinien basierend auf Linksets hinzu.

In einem Cluster-Setup verwenden die folgenden Funktionen MBF intern.

- Weiterleitungssitzung
- L2Conn
- MAC-Modus virtueller Server
- Transparenter Monitor
- LLB

Linksets müssen nur über die Cluster-IP-Adresse konfiguriert werden.

Betrachten Sie ein Beispiel mit einem Drei-Knoten-Cluster. In der folgenden Abbildung befinden sich die Schnittstellen 0/1/2, 1/1/2 und 2/1/2 in derselben Broadcast-Domäne und können daher als Linkset (LS/1) konfiguriert werden.

Abbildung 1. Linksetstopologie

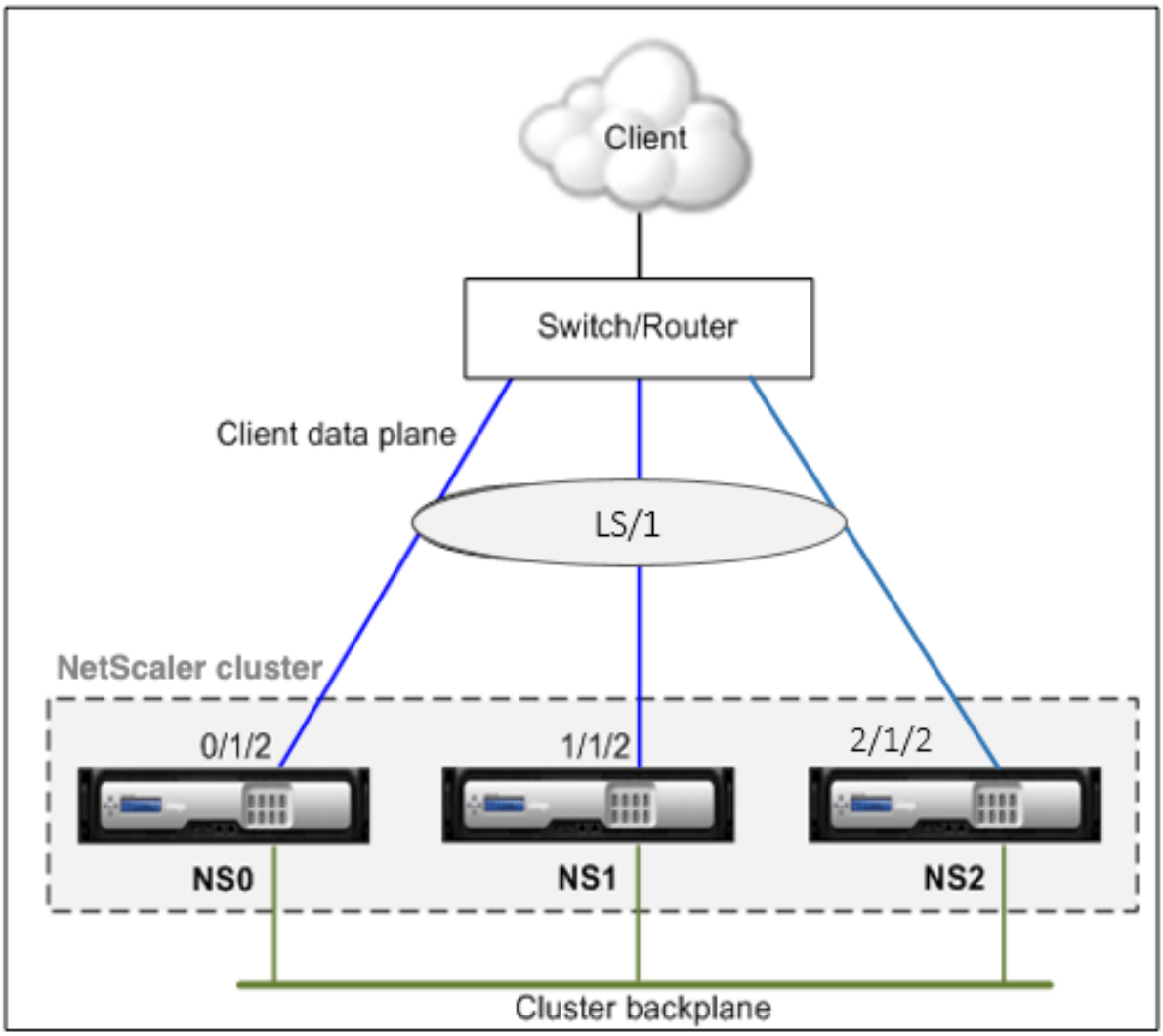
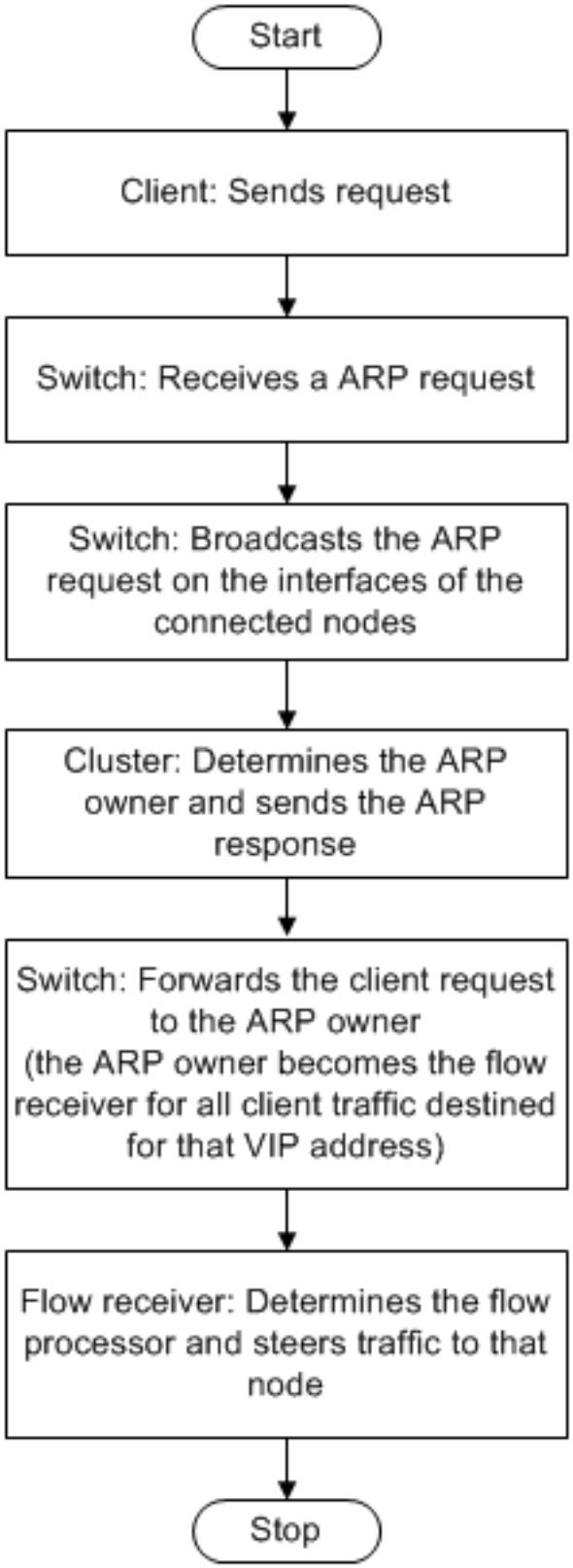


Abbildung 2. Verkehrsverteilungsfluss mit Linksets



So konfigurieren Sie ein Linkset mit der CLI

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Erstellen Sie einen Linksatz.

   “‘add linkset

   ```
   **Beispiel**

   ```add linkset LS/1<!--NeedCopy-->
   ```

3. Binden Sie die erforderlichen Schnittstellen an das Linkset. Stellen Sie sicher, dass die Schnittstellen nicht für die Cluster-Rückwandplatine verwendet werden.

   “‘bind linkset -ifnum ...

   ```
   **Beispiel**

   ```bind linkset LS/1 -ifnum 0/1/2 1/1/2 2/1/2<!--NeedCopy-->
   ```

4. Überprüfen Sie die Linkset-Konfigurationen.

   “‘show linkset

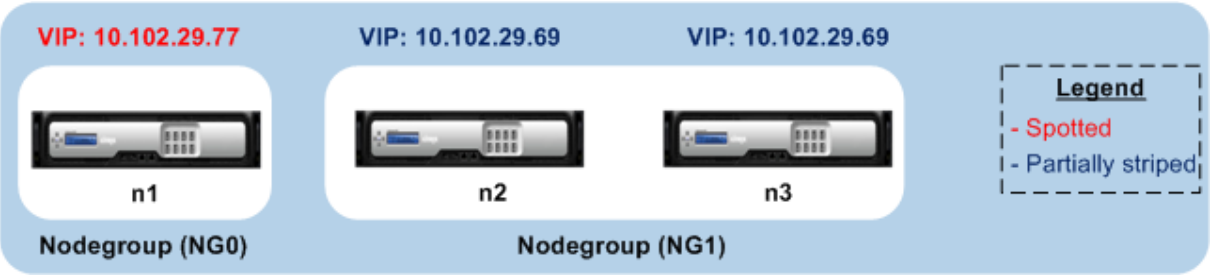
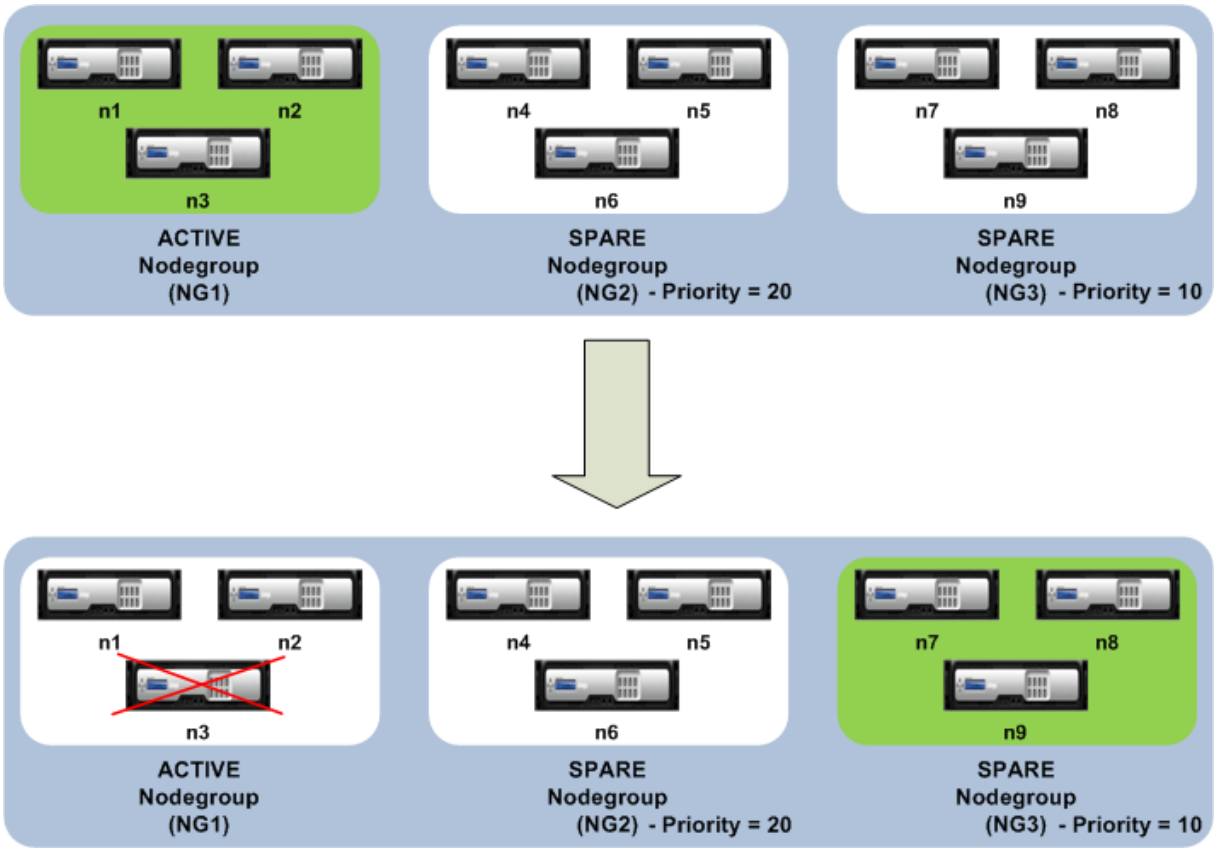
   ```
   **Beispiel**

   ```show linkset LS/1<!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > Sie können das Linkset mit dem `bind vlan` Befehl an ein VLAN binden. Die Schnittstellen des Linksets werden automatisch an das VLAN gebunden.

So konfigurieren Sie ein Linkset mit der GUI

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Netzwerk > Linksets**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Im Dialogfeld **Linkset erstellen**:
   - Geben Sie den Namen des Linksets an, indem Sie den Linkset-Parameter festlegen.
   - Geben Sie die Schnittstellen an, die dem Linkset hinzugefügt werden sollen, und klicken Sie auf Hinzufügen. Wiederholen Sie diesen Schritt für jede Schnittstelle, die Sie dem Linkset hinzufügen möchten.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.


   ```

# Knotengruppen für gepunktete und teilweise Striped Konfigurationen

May 11, 2023

Aufgrund des standardmäßigen Clusterverhaltens sind alle an der Cluster-IP-Adresse durchgeführten Konfigurationen auf allen Knoten des Clusters verfügbar. Es kann jedoch Fälle geben, in denen einige Konfigurationen nur auf bestimmten Clusterknoten verfügbar sein müssen.

Sie können diese Anforderung erfüllen, indem Sie eine Knotengruppe definieren, die die spezifischen Clusterknoten umfasst, und dann die Konfiguration an diese Knotengruppe binden. Es stellt sicher, dass die Konfiguration nur auf diesen Clusterknoten aktiv ist. Diese Konfigurationen werden als teilweise gestreift oder gepunktet bezeichnet (wenn nur ein einzelner Knoten aktiv ist). Weitere Informationen finden Sie unter Gestreifte, teilweise gestreifte und gepunktete Konfigurationen.

Betrachten Sie beispielsweise einen Cluster mit drei Knoten. Sie erstellen eine Knotengruppe NG0, die den Knoten n1 enthält, und eine weitere Knotengruppe NG1, die n2 und n3 umfasst. Binden Sie virtuelle Lastausgleichsserver 0,77 an NG0 und den virtuellen Lastausgleichsserver 0,69 an NG1.

Das bedeutet, dass der virtuelle Server 0.77 nur auf n1 aktiv ist und daher nur n1 den Traffic empfängt, der an 0.77 weitergeleitet wird. In ähnlicher Weise ist der virtuelle Server 0.69 nur auf den Knoten n2 und n3 aktiv und daher empfangen nur n2 und n3 Verkehr, der an 0.69 weitergeleitet wird.

Abbildung 1. NetScaler-Cluster mit Knotengruppen, die für punktuelle Konfigurationen und partielle Streifenkonfigurationen konfiguriert sind




Die Entitäten oder Konfigurationen, die Sie an eine Knotengruppe binden können, sind:

- Lastenausgleich, Content Switching, Cache-Umleitung, Authentifizierung, Autorisierung und Überwachung virtueller Server

  > **Hinweis**
  >
  > Virtuelle FTP-Lastausgleichsserver können nicht an Knotengruppen gebunden werden.

- Virtueller VPN-Server (unterstützt ab NetScaler 10.5 Build 50.10)
- Global Server Load Balancing (GSLB) -Sites und andere GSLB-Entitäten (unterstützt ab NetScaler 10.5 Build 52.11)
- Bezeichner und Stream-Bezeichner beschränken

 

# Verhalten von Knotengruppen

May 11, 2023

Aufgrund der Interoperabilität von Knotengruppen mit unterschiedlichen NetScaler-Funktionen und -Entitäten sind einige Verhaltensaspekte zu beachten. Knoten in einer Knotengruppe können ebenfalls gesichert werden. Lesen Sie weiter für weitere Informationen.

## Allgemeines Verhalten einer Clusterknotengruppe

- Eine Knotengruppe, an die Entitäten gebunden sind, kann nicht entfernt werden.
- Ein Clusterknoten, der zu einer Knotengruppe gehört, an die Entitäten gebunden sind, kann nicht entfernt werden.
- Eine Cluster-Instance mit Knotengruppen, an die Entitäten gebunden sind, kann nicht entfernt werden.
- Sie können keine Entität hinzufügen, die von einer anderen Entität abhängig ist. Es darf nicht Teil der Knotengruppe sein. Wenn Sie dies tun müssen, entfernen Sie zuerst die Abhängigkeit. Fügen Sie dann beide Entitäten zur Knotengruppe hinzu und ordnen Sie die Entitäten erneut zu.

  **Beispiele:**

  - Angenommen, Sie haben einen virtuellen Server, VS1, dessen Backup der virtuelle Server VS2 ist. Um VS1 zu einer Knotengruppe hinzuzufügen, stellen Sie zunächst sicher, dass VS2 als Backup-Server von VS1 entfernt wird. Binden Sie dann jeden Server einzeln an die Knotengruppe und konfigurieren Sie dann VS2 als Backup für VS1.
  - Angenommen, Sie haben einen virtuellen Content Switching-Server, CSVS1, dessen virtueller Zielserver für den Lastausgleich LBVS1 ist. Um CSVS1 zu einer Knotengruppe hinzuzufügen, entfernen Sie zuerst LBVS1 als Ziel. Binden Sie dann jeden Server einzeln an die Knotengruppe und konfigurieren Sie dann LBVS1 als Ziel.
  - Angenommen, Sie haben einen virtuellen Lastausgleichsserver, LBVS1, mit einer Richtlinie, die einen anderen virtuellen Lastausgleichsserver, LBVS2, aufruft. Um einen der virtuellen Server hinzuzufügen, entfernen Sie zunächst die Zuordnung. Binden Sie dann jeden Server einzeln an die Knotengruppe und ordnen Sie die virtuellen Server dann erneut zu.
- Sie können eine Entität nicht an eine Knotengruppe binden. Es hat keine Knoten und dafür ist die strikte Option aktiviert. Daher können Sie die Bindung des letzten Knotens einer Knotengruppe nicht aufheben, an den Entitäten gebunden sind und für den die Option Strict aktiviert ist.

 

- Die strikte Option kann nicht für eine Knotengruppe geändert werden, an die keine Knoten, aber Entitäten gebunden sind.

### Knoten in einer Knotengruppe sichern

Standardmäßig ist eine Knotengruppe so konzipiert, dass sie Backup-Knoten für Mitglieder einer Knotengruppe bereitstellt. Wenn ein Mitglied der Knotengruppe ausfällt, ersetzt ein Clusterknoten, der kein Mitglied der Knotengruppe ist, den ausgefallenen Knoten dynamisch. Dieser Knoten wird Ersatzknoten genannt.

> **Hinweis**
>
> Bei einer Knotengruppe mit nur einem Mitglied wird automatisch ein Backup-Knoten ausgewählt, wenn eine Entität an die Knotengruppe gebunden ist.

Wenn das ursprüngliche Mitglied der Knotengruppe auftaucht, wird der Ersatzknoten standardmäßig durch den ursprünglichen Mitgliedsknoten ersetzt.

Ab NetScaler 10.5 Build 50.10 ermöglicht Ihnen der NetScaler jedoch, dieses Ersatzverhalten zu ändern. Wenn Sie die Sticky-Option aktivieren, bleibt der Ersatzknoten auch dann erhalten, wenn der ursprüngliche Mitgliedsknoten erscheint. Der ursprüngliche Knoten übernimmt nur die Funktion, wenn der Ersatzknoten ausfällt.

Sie können die Backup-Funktion auch deaktivieren. Dazu müssen Sie die strikte Option aktivieren. In diesem Szenario wird beim Ausfall eines Knotengruppenmitglieds kein anderer Clusterknoten als Backup-Knoten übernommen. Der ursprüngliche Knoten ist weiterhin Teil der Knotengruppe, wenn er auftaucht. Diese Option stellt sicher, dass Entitäten, die an eine Knotengruppe gebunden sind, nur auf Knotengruppenmitgliedern aktiv sind.

> **Hinweis**
>
> Die Optionen Strict und Sticky können nur beim Erstellen einer Knotengruppe gesetzt werden.

## Konfiguration von Knotengruppen für gepunktete und teilweise Striped Konfigurationen

May 11, 2023

Um eine Knotengruppe für punktierte und teilweise Striped Konfigurationen zu konfigurieren, müssen Sie zunächst eine Knotengruppe erstellen und dann die erforderlichen Knoten an die Knotengruppe binden. Anschließend ordnen Sie dieser Knotengruppe die erforderlichen Entitäten zu. Die Entitäten, die an die Knotengruppe gebunden sind, gehören zu den folgenden:

 

- **Entdeckt** — Wenn an eine Knotengruppe gebunden ist, die einen einzelnen Knoten hat.
- **Teilweise gestreift** — Wenn an eine Knotengruppe gebunden ist, die mehr als einen Knoten hat.

**Einige Punkte, an die Sie sich erinnern sollten:**

- GSLB wird auf einem Cluster nur unterstützt, wenn GSLB-Sites an Knotengruppen gebunden sind, die einen einzelnen Cluster-Knoten haben. Weitere Informationen finden Sie unter Einrichten von GSLB in einem Cluster.
- NetScaler Gateway wird auf einem Cluster nur unterstützt, wenn die virtuellen VPN-Server an Knotengruppen gebunden sind, die über einen einzelnen Clusterknoten verfügen. Die Sticky-Option muss in der Knotengruppe aktiviert sein.
- In Versionen vor NetScaler 11 wird die Anwendungsfirewall nur auf einzelnen Clusterknoten unterstützt (Spotted-Konfiguration). Anwendungsfirewallprofile können nur virtuellen Servern zugeordnet werden, die an Knotengruppen gebunden sind, die über einen einzigen Clusterknoten verfügen. Das bedeutet, dass Sie bei der Bewerbung Folgendes nicht tun dürfen:
  - Binden Sie Anwendungs-Firewallprofile an Striped oder teilweise Striped virtuelle Server.
  - Binden Sie die Richtlinie an einen globalen Bindungspunkt oder an benutzerdefinierte Richtlinienlabels.
  - Trennen Sie einen virtuellen Server mit Anwendungs-Firewallprofilen von einer Knotengruppe.
- NetScaler 11 hat Anwendungsfirewall-Unterstützung für gestreifte und teilweise gestreifte Konfigurationen eingeführt. Weitere Informationen finden Sie unter Application Firewall-Unterstützung für Clusterkonfigurationen.

Überprüfen Sie die in einem Cluster unterstützten NetScaler Features, um die NetScaler-Versionen anzuzeigen, von denen GSLB, NetScaler Gateway und Application Firewall in einem Cluster unterstützt werden.

### So konfigurieren Sie eine Knotengruppe mit der Befehlszeilenschnittstelle

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Erstellen Sie eine Knotengruppe. Typ:

   ```
   add cluster nodegroup <name> -strict (YES | NO)<!--NeedCopy-->
   ```

   Beispiel

   ```
   1 add cluster nodegroup NG0 -strict YES
   ```

3. Binden Sie die erforderlichen Knoten an die Knotengruppe. Geben Sie den folgenden Befehl für jedes Mitglied der Knotengruppe ein:

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```


Beispiel

So binden Sie Knoten mit IDs 1, 5 und 6.

```
1 > bind cluster nodegroup NG0 -node 1
2 > bind cluster nodegroup NG0 -node 5
3 > bind cluster nodegroup NG0 -node 6
```

4. Binden Sie die Entität an die Knotengruppe. Geben Sie den folgenden Befehl einmal für jede Entität ein, die Sie binden möchten:

   ```
   bind cluster nodegroup <name> (-vServer <string> | -identifierName <
   string> | -gslbSite <string> -service <string>)<!--NeedCopy-->
   ```

   > **Hinweis**
   >
   > Die GSLBSite- und Serviceparameter sind ab NetScaler 10.5 verfügbar.

   Beispiel

   Zum Binden virtueller Server VS1 und VS2 und der Begrenzungskennung mit dem Namen identifiier1.

   ```
   1 > bind cluster nodegroup NG0 -vServer VS1
   2 > bind cluster nodegroup NG0 -vServer VS2
   3 > bind cluster nodegroup NG0 -identifierName identifier1
   ```

5. Überprüfen Sie die Konfigurationen, indem Sie die Details der Knotengruppe anzeigen. Typ:

   ```
   show cluster nodegroup <name><!--NeedCopy-->
   ```

   Beispiel

   ```
   1 > show cluster nodegroup NG0
   ```

So konfigurieren Sie eine Knotengruppe mit dem Konfigurationsdienstprogramm

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knotengruppen.**
3. Klicken Sie im Detailbereich auf **Hinzufügen.**
4. Konfigurieren **Sie im Dialogfeld Knotengruppe erstellen** die Knotengruppe:
   a) Klicken Sie unter **Clusterknoten**auf die Schaltfläche **Hinzufügen** .
      - In der Liste Verfügbar werden die Knoten angezeigt, die Sie an die Knotengruppe binden können, und in der Liste Konfiguriert werden die Knoten angezeigt, die an die Knotengruppe gebunden sind.

- Klicken Sie in der Liste Verfügbar auf das **Pluszeichen**, um den Knoten zu binden. Klicken Sie in ähnlicher Weise in der Liste „Konfiguriert“ auf das „ **-** “ -Zeichen, um die Bindung des Knotens aufzuheben.

b) Wählen Sie unter **Virtuelle Server**die Registerkarte aus, die dem Typ des virtuellen Servers entspricht, den Sie an die Knotengruppe binden möchten. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   - In der Liste Verfügbar werden die virtuellen Server angezeigt, die Sie an die Knotengruppe binden können, und in der Liste Konfiguriert werden die virtuellen Server angezeigt, die an die Knotengruppe gebunden sind.
   - Klicken Sie in der Liste Verfügbar auf das **Pluszeichen**, um den virtuellen Server zu binden. Klicken Sie auf das - Zeichen in der Liste Konfiguriert, um die Bindung des virtuellen Servers aufzuheben.

Konfiguration der Redundanz für Knotengruppen

May 11, 2023

> **Hinweis**
>
> Wird ab NetScaler 10.5 Build 52.1115.e unterstützt.

Knotengruppen können so konfiguriert werden, dass, wenn eine Knotengruppe ausfällt, eine andere Knotengruppe den Verkehr übernehmen und verarbeiten kann. Wenn beispielsweise eine Knotengruppe NG1 ausfällt, übernimmt NG2 die Leitung.

> **Hinweis**
>
> Diese Funktion kann zur Konfiguration der Rechenzentrumsredundanz verwendet werden, wobei jede Knotengruppe als Rechenzentrum konfiguriert wird.

Um diesen Anwendungsfall zu erreichen, müssen Clusterknoten logisch in Knotengruppen gruppiert werden, wobei einige Knotengruppen als ACTIVE und andere als SPARE konfiguriert werden müssen. Die aktive Knotengruppe mit der höchsten Priorität (d. h. der Nummer mit der niedrigsten Priorität) wird betriebsbereit gemacht und dient daher dem Verkehr. Wenn ein Knoten aus dieser operativ aktiven Knotengruppe ausfällt, wird die Knotenzahl dieser Knotengruppe mit der Knotenzahl der anderen aktiven Knotengruppen in der Reihenfolge ihrer Priorität verglichen. Wenn eine Knotengruppe eine höhere oder gleiche Knotenanzahl hat, wird diese Knotengruppe betriebsaktiv. Andernfalls werden die Ersatzknotengruppen überprüft.

> **Hinweis**
>
> - Zu einem bestimmten Zeitpunkt kann nur eine zustandsspezifische Knotengruppe aktiv

sein.

- Ein Clusterknoten erbt den Status der Knotengruppe. Wenn also ein Knoten mit dem Status „SPARE“ zur Knotengruppe mit dem Status „ACTIVE“ hinzugefügt wird, verhält sich der Knoten automatisch wie ein aktiver Knoten.
- Der Präemptionsparameter, der für die Cluster-Instance definiert ist, entscheidet, ob die anfängliche aktive Knotengruppe die Kontrolle übernimmt, wenn sie wieder aufgerufen wird.
- Eine Ersatzknotengruppe kann eine Knotengruppe aufnehmen und aktiven Verkehr hosten, wenn eine aktive Knotengruppe ausfällt.

Die folgende Abbildung zeigt ein Knotengruppen-Setup, bei dem die Knotengruppenredundanz definiert ist. NG1 ist zunächst die aktive Knotengruppe. Wenn einer der Knoten verloren geht, beginnt die Ersatzknotengruppe (NG3) mit der höchsten Priorität, den Verkehr zu bedienen.

Abbildung 1. NetScaler-Cluster mit konfigurierter Knotengruppenredundanz.



Konfiguration der Redundanz für Knotengruppen

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Erstellen Sie die aktive Knotengruppe und binden Sie die erforderlichen Cluster-Knoten.

```
1 > add cluster nodegroup NG1 -state ACTIVE
```



```
> bind cluster nodegroup NG1 -node n1
> bind cluster nodegroup NG1 -node n2
> bind cluster nodegroup NG1 -node n3
```

3. Erstellen Sie die Reserveknotengruppe und binden Sie die erforderlichen Knoten.

```
> add cluster nodegroup NG2 -state SPARE -priority 20
> bind cluster nodegroup NG2 -node n4
> bind cluster nodegroup NG2 -node n5
> bind cluster nodegroup NG2 -node n6
```

4. Erstellen Sie eine weitere Reserveknotengruppe und binden Sie die erforderlichen Knoten.

```
> add cluster nodegroup NG3 -state SPARE -priority 10
> bind cluster nodegroup NG3 -node n7
> bind cluster nodegroup NG3 -node n8
> bind cluster nodegroup NG3 -node n9
```

Deaktivieren der Lenkung auf der Cluster-Backplane

May 11, 2023

> **Hinweis**
>
> Wird ab NetScaler 11 unterstützt.

Das Standardverhalten eines NetScaler-Clusters besteht darin, den empfangenen Datenverkehr (Flow-Empfänger) an einen anderen Knoten (Flow-Prozessor) weiterzuleiten. Der Flow Processor muss dann den Verkehr verarbeiten. Dieser Vorgang, bei dem der Datenverkehr vom Flow-Empfänger zum Flow-Prozessor geleitet wird, erfolgt über die Cluster-Backplane und wird als Steering bezeichnet.

Bei Bedarf können Sie die Lenkung deaktivieren, sodass der Prozess lokal auf den Durchflussempfänger übertragen wird und der Durchflussempfänger somit zum Durchflussprozessor wird. Eine solche Konfiguration kann nützlich sein, wenn Sie eine Verbindung mit hoher Latenz haben.

> **Hinweis**
>
> Diese Konfiguration gilt nur für Striped virtuelle Server.

- Bei teilweise Striped virtuellen Servern wird der Datenverkehr zu einem Eigentümerknoten geleitet, wenn es sich bei dem Flow-Empfänger um einen Knoten handelt, der kein Eigentümer ist. Wenn der Flow-Empfänger jedoch ein Owner-Knoten ist, ist die Lenkung deaktiviert.

- Bei erkannten virtuellen Servern ist der Flow-Empfänger der Flow-Prozessor, sodass keine Steuerung erforderlich ist.

Einige Punkte, die Sie bei der Deaktivierung des Lenkmechanismus beachten sollten:

- Striped SNIPs werden nicht unterstützt, da die Lenkung deaktiviert ist.
- MPTCP und FTP funktionieren nicht.
- Der L2-Modus muss deaktiviert sein.
- Wenn USIP aktiviert ist, erreicht der Verkehr möglicherweise nicht denselben Knoten, da die Lenkung deaktiviert ist.
- Datenverkehr, der an die Cluster-IP-Adresse geleitet wird, wird an den Konfigurationskoordinator weitergeleitet.
- Wenn ein Knoten einem Cluster beitritt oder ihn verlässt, ist es möglich, dass mehr als 1/N Verbindungen betroffen sind. Dies liegt daran, dass eine Änderung der verfügbaren Knoten dazu führen kann, dass die Routen erneut gehasht werden. Infolgedessen wird der Verkehr an einen anderen Knoten weitergeleitet, und da die Steuerung nicht verfügbar ist, wird der Verkehr nicht verarbeitet.

Die Steuerung kann auf der Ebene einzelner virtueller Server oder auf globaler Ebene deaktiviert werden. Die globale Konfiguration hat Vorrang vor der Einstellung für den virtuellen Server.

- Deaktivierung der Backplane-Steuerung für alle Striped virtuellen Server

  Auf Cluster-Instanzebene konfiguriert. Der Datenverkehr, der für einen Striped virtuellen Server bestimmt ist, wird nicht über die Cluster-Backplane gesteuert.

  ```
  add cluster instance \<clId\> -processLocal ENABLED<!--NeedCopy-->
  ```

- Deaktivierung der Backplane-Steuerung für einen bestimmten Striped virtuellen Server

  Auf einem Striped virtuellen Server konfiguriert. Der für den virtuellen Server bestimmte Datenverkehr wird nicht über die Cluster-Backplane gesteuert.

  ```
  add lb vserver <name> <serviceType> -processLocal ENABLED<!--NeedCopy
  -->
  ```

Synchronisieren von Clusterkonfigurationen

May 11, 2023

NetScaler-Konfigurationen, die auf dem Konfigurationskoordinator verfügbar sind, werden mit den anderen Knoten des Clusters synchronisiert, wenn:

- Ein Knoten tritt dem Cluster bei
- Ein Knoten tritt dem Cluster wieder bei

- Ein neuer Befehl wird über die Cluster-IP-Adresse ausgeführt

Sie können auch die Konfigurationen, die auf dem Konfigurationskoordinator verfügbar sind (vollständige Synchronisierung), zwangsweise mit einem bestimmten Clusterknoten synchronisieren. Stellen Sie sicher, dass Sie jeweils einen Clusterknoten synchronisieren, da sonst der Cluster betroffen sein kann.

So synchronisieren Sie Cluster-Konfigurationen mithilfe der CLI:

Geben Sie an der Eingabeaufforderung der Appliance, auf der Sie die Konfigurationen synchronisieren möchten, Folgendes ein:

```
force cluster sync
```

So synchronisieren Sie Cluster-Konfigurationen mithilfe der GUI:

1. Melden Sie sich bei der Appliance an, auf der Sie die Konfigurationen synchronisieren möchten.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Utilities**auf Clustersynchronisierung erzwingen.
4. Klicken Sie auf **OK.**

Liste der Befehle anzeigen, die während der Clusterkonfigurationssynchronisierung fehlgeschlagen sind

In einem Cluster-Setup können Sie bei `syncStatusStrictMode` aktiviertem Sync-Status strikter Modus die Liste der Befehle anzeigen, die während einer Clustersynchronisierung fehlgeschlagen sind, auf einem Nicht-CCO-Knoten.

Sie können den Cluster-Synchronisationsstatus eines Nicht-CCO-Knotens ermitteln, indem Sie den `show node` Vorgang ausführen. `PARTIAL SUCCESS` Der Synchronisationsstatus zeigt an, dass einige Befehle auf dem Nicht-CCO-Knoten während der Clustersynchronisierung fehlgeschlagen sind.

So zeigen Sie die Liste der Befehle an, die auf einem Knoten während der Clustersynchronisierung mit CLI fehlgeschlagensind:

- `show cluster syncFailures`

Beispiel-Konfiguration

```
    > show cluster node

    1) Node ID: 1
            IP:                  10.102.201.24
            Backplane:           1/1/1
            Health:              UP
```



```
            Admin State:          ACTIVE
            Operational State:    ACTIVE(Configuration Coordinator)
            Sync State:           ENABLED
            Priority:             31
            Tunnel Mode:          NONE
            Node Group:           DEFAULT_NG
    2) Node ID: 2
            IP:                   10.102.201.62*
            Backplane:            2/1/1
            Health:               UP
            Admin State:          ACTIVE
            Operational State:    ACTIVE
            Sync State:           PARTIAL SUCCESS
    (Refer the files clus_sync_batch_status.log, sync_route_status.log
       and sync_clusdiff_status.log in /var/nssynclog directory for
       list of commands failed)
            Priority:             31
            Tunnel Mode:          NONE
            Node Group:           DEFAULT_NG
    3) Node ID: 3
            IP:                   10.102.201.64
            Backplane:            3/1/1
            Health:               UP
            Admin State:          ACTIVE
            Operational State:    ACTIVE
            Sync State:           PARTIAL SUCCESS
    (Refer the files clus_sync_batch_status.log, sync_route_status.log
       and sync_clusdiff_status.log in /var/nssynclog directory for
       list of commands failed)
            Priority:             31
            Tunnel Mode:          NONE
            Node Group:           DEFAULT_NG
    Done

    > show cluster syncFailures

    exec: add system user nsroot "********" -encrypted -externalAuth
       ENABLED -timeout 900 -logging ENABLED -maxsession 20 -
       allowedManagementInterface CLI API -devno 32768
    ERROR: Resource already exists
    --
    exec: set interface 2/LO/1 -autoneg ENABLED -haMonitor OFF -
       haHeartbeat OFF -mtu 1500 -ringtype Elastic -tagall OFF -
       trunkmode OFF -state ENABLED -lagtype NODE -lacpPriority 32768 -
       lacpTimeout LONG -throughput 0 -linkRedundancy OFF -
```



```
            bandwidthHigh 0 -bandwidthNormal 0 -intftype Loopback -svmCmd 0
            -ifnum 2/LO/1 -lldpmode NONE -lrsetPriority 1024
43      ERROR: Operation not allowed on loopback interface.
```

Synchronisieren der Zeit über Clusterknoten hinweg

August 19, 2021

Der Cluster verwendet ein Precision Time Protocol (PTP), um die Zeit über Clusterknoten hinweg zu synchronisieren. PTP verwendet Multicastpakete, um die Zeit zu synchronisieren. Wenn bei der Zeitsynchronisierung einige Probleme auftreten, müssen Sie PTP deaktivieren und NTP (Network Time Protocol) auf dem Cluster konfigurieren.

So aktivieren/deaktivieren Sie PTP mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
1  set ptp -state disable
```

So aktivieren/deaktivieren Sie PTP mit dem Konfigurationsdienstprogramm

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Dienstprogramme**auf **PTP-Einstellungen konfigurieren.**
4. Wählen Sie im Dialogfeld **PTP aktivieren/deaktivieren** aus, ob Sie PTP aktivieren oder deaktivieren möchten.
5. Klicken Sie auf **OK.**

Synchronisieren von Clusterdateien

October 8, 2021

Die im Konfigurationskoordinator verfügbaren Dateien werden Clusterdateien genannt. Diese Dateien werden automatisch auf den anderen Clusterknoten synchronisiert, wenn der Knoten zum Cluster hinzugefügt wird, und in regelmäßigen Abständen, während der Lebensdauer des Clusters. Außerdem können Sie die Clusterdateien manuell synchronisieren.

Wichtig: Das Entfernen von Zertifikaten oder Schlüsseldateien in einer Clusterumgebung schränkt die weitere Konfiguration auf der ADC-Appliance ein. Fügen Sie die Dateien wieder am selben Ort hinzu, um Konfigurationsänderungen vorzunehmen.

Die Verzeichnisse und Dateien aus dem Konfigurationskoordinator, die synchronisiert werden, sind:

- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/lesezeichen/
- /nsconfig/dns/
- /nsconfig/monitors/
- /nsconfig/nstemplates/
- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
- /nsconfig/inetd.conf
- /nsconfig/syslog.conf
- /nsconfig/snmpd.conf
- /nsconfig/ntp.conf
- /nsconfig/httpd.conf
- /nsconfig/sshd_config
- /nsconfig/hosts
- /nsconfig/enckey
- /var/nslw.bin/etc/krb5.conf
- /var/nslw.bin/etc/krb5.keytab
- /var/lib/gleich/db/
- /var/herunterladen/
- /var/wi/tomcat/webapps/
- /var/wi/tomcat/conf/catalina/localhost/
- /var/wi/java_home/lib/security/cacerts
- /var/wi/java_home/jre/lib/security/cacerts
- /nsconfig/lizenz/
- /nsconfig/rc.conf

> **Tipp**
>
> Dateien (Zertifikate und Schlüsseldateien), die manuell (oder über die Shell) in den Clusterkonfigurationskoordinator kopiert werden, sind auf den anderen Clusterknoten nicht automatisch verfügbar. Führen Sie den Befehl “Clusterdateien synchronisieren” von der Cluster-IP-Adresse aus, bevor Sie einen Befehl ausführen, der von diesen Dateien abhängt.

So synchronisieren Sie Clusterdateien über die Befehlszeile

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
sync cluster files <mode>
```

So synchronisieren Sie Clusterdateien mit dem Konfigurationsdienstprogramm

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Dienstprogramme**auf Clusterdateien synchronisieren.
4. Wählen Sie im Dialogfeld Clusterdateien **synchronisieren** die zu synchronisierenden Dateien in der Dropdownliste Modus aus.
5. Klicken Sie auf **OK.**

Anzeigen der Statistiken eines Clusters

January 19, 2021

Sie können die Statistiken einer Clusterinstanz und Clusterknoten anzeigen, um die Leistung zu bewerten oder den Betrieb des Clusters zu beheben.

So zeigen Sie die Statistiken einer Clusterinstanz mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
stat cluster instance <clId>
```

So zeigen Sie die Statistiken eines Clusterknotens mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
stat cluster node <nodeid>
```

> **Hinweis:**
>
> Der `stat cluster node <nodeid>` Befehl zeigt die Statistiken auf Clusterebene an, wenn Sie den Befehl von der Cluster-IP-Adresse aus ausführen. Wenn Sie jedoch von der NSIP-Adresse eines Clusterknotens aus ausführen, zeigt der Befehl Statistiken auf Knotenebene an.

So zeigen Sie die Statistiken einer Clusterinstanz mit dem Konfigurationsdienstprogramm an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich in der Mitte der Seite auf **Statistik.**

So zeigen Sie die Statistiken eines Clusterknotens mit dem Konfigurationsdienstprogramm an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten.**
3. Wählen Sie im Detailbereich einen Knoten aus, und klicken Sie auf **Statistik**, um die Statistiken des Knotens anzuzeigen. Um die Statistiken aller Knoten anzuzeigen, klicken Sie auf **Statistik**, ohne einen bestimmten Knoten auszuwählen.

Entdecken von NetScaler-Appliances

May 11, 2023

Sie können die Appliances ermitteln, die sich im selben Subnetz wie der aktuelle Knoten befinden. Die erforderlichen erkannten Appliances können dann selektiv zum Cluster hinzugefügt werden. Dieser Vorgang kann ausgeführt werden, um entweder einen Cluster zu erstellen oder um Knoten zu einem vorhandenen Cluster hinzuzufügen.

> **Hinweis**
>
> - Der Discover-Vorgang kann nur über das Konfigurationsprogramm ausgeführt werden.
> - Dieser Vorgang kann NetScaler-Appliances aus verschiedenen Netzwerken nicht erkennen.
> - Wenn Sie diesen Vorgang ausführen, um Knoten zu einem vorhandenen Cluster hinzuzufügen, werden die L3-VLAN-Konfigurationen vom Knoten gelöscht. Sie stellen sicher, dass Sie diese Konfigurationen definieren, sobald die Appliance dem Cluster hinzugefügt wurde.

Um Appliances mithilfe der GUI zu entdecken

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten.**
3. Klicken Sie im Detailbereich unten auf der Seite auf **Discover NetScalers**.
4. Stellen **Sie im Dialogfeld Discover NetScalers** die folgenden Parameter ein:

- **IP-Adressbereich** — Geben Sie den IP-Adressbereich an, in dem Sie Geräte erkennen möchten. Sie können beispielsweise nach allen NSIP-Adressen zwischen 10.102.29.4 und 10.102.29.15 suchen, indem Sie diese Option als 10.102.29.4 - 15 angeben.
- **Backplane-Schnittstelle** — Geben Sie die Schnittstellen an, die als Backplane-Schnittstelle verwendet werden sollen. Es ist ein optionaler Parameter. Wenn Sie diesen Parameter nicht angeben, müssen Sie ihn aktualisieren, nachdem der Knoten dem Cluster hinzugefügt wurde.

5. Klicken Sie auf **OK.**
6. Wählen Sie die Appliances aus, die Sie dem Cluster hinzufügen möchten.
7. Klicken Sie auf **OK.**

Deaktivieren eines Clusterknotens

August 19, 2021

Sie können einen Knoten vorübergehend aus einem Cluster entfernen, indem Sie die Clusterinstanz auf diesem Knoten deaktivieren. Ein deaktivierter Knoten wird nicht mit den Clusterkonfigurationen synchronisiert. Wenn der Knoten wieder aktiviert ist, werden die Clusterkonfigurationen automatisch synchronisiert. Weitere Informationen finden Sie unter Synchronisation über Clusterknotenhinweg.

Ein deaktivierter Knoten kann keinen Datenverkehr bereitstellen, und alle vorhandenen Verbindungen auf diesem Knoten werden beendet.

> **Hinweis:**
>
> Wenn die Konfigurationen eines deaktivierten Koordinatorknotens ohne Konfiguration geändert werden (über die NSIP-Adresse des Knotens), werden die Konfigurationen auf diesem Knoten nicht automatisch synchronisiert. Sie können die Konfigurationen wie unter Clusterkonfigurationen synchronisierenbeschrieben manuell synchronisieren.

So deaktivieren Sie einen Clusterknoten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung des Knotens, den Sie deaktivieren möchten, Folgendes ein:

```
disable cluster instance <clId>
```

> **Hinweis:**
>
> Führen Sie zum Deaktivieren des Clusters den Befehl
> disable cluster instance für die Cluster-IP-Adresse aus.

So deaktivieren Sie einen Clusterknoten mit dem Konfigurationsdienstprogramm

1. Navigieren Sie auf dem Knoten, den Sie deaktivieren möchten, zu **System > Cluster**, und klicken Sie auf **Cluster verwalten.**
2. Deaktivieren **Sie im Dialogfeld Clusterinstanz konfigurieren** das Kontrollkästchen Clusterinstanz **aktivieren**.

   > **Hinweis:**
   >
   > Um die Clusterinstanz auf allen Knoten zu deaktivieren, führen Sie das vorherige Verfahren für die Cluster-IP-Adresse aus.

Entfernen eines Clusterknotens

August 19, 2021

Wenn ein Knoten aus dem Cluster entfernt wird, werden die Clusterkonfigurationen vom Knoten gelöscht (indem intern der Befehl clear ns config -extended ausgeführt wird). Die SNIP-Adressen, **MTU-Einstellungen** der Backplane-Schnittstelle und alle VLAN-Konfigurationen (mit Ausnahme des Standard-VLAN und des NSVLAN) werden ebenfalls von der Appliance gelöscht.

> **Hinweis:**
>
> - Wenn der gelöschte Knoten der Clusterkonfigurationskoordinator (CCO) war, wird automatisch ein anderer Knoten als CCO ausgewählt, und die Cluster-IP-Adresse wird diesem Knoten zugewiesen. Alle aktuellen Cluster-IP-Adresssitzungen sind ungültig und Sie müssen eine neue Sitzung starten.
> - Um den gesamten Cluster zu löschen, müssen Sie jeden Knoten einzeln entfernen. Wenn Sie den letzten Knoten entfernen, werden die Cluster-IP-Adressen gelöscht.
> - Wenn ein aktiver Knoten entfernt wird, wird die Traffic Serving-Fähigkeit des Clusters um einen Knoten reduziert. Vorhandene Verbindungen auf diesem Knoten werden beendet.

So entfernen Sie einen Clusterknoten mit der CLI

Für NetScaler 10.1 und höher

1. Melden Sie sich bei der Cluster-IP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm cluster node <nodeId>

save ns config
```


2. Melden Sie sich am entfernten Knoten, der NSIP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
save ns config
```

> **Hinweis:**
>
> Wenn die Cluster-IP-Adresse vom Knoten aus nicht erreichbar ist, führen Sie den Befehl RM-Clusterinstanz-Befehl für die NSIP-Adresse dieses Knotens selbst aus.

Für NetScaler 10

1. Melden Sie sich bei dem Knoten an, den Sie aus dem Cluster entfernen möchten, und entfernen Sie den Verweis auf die Clusterinstanz.

```
rm cluster instance <clId>

save ns config
```

2. Melden Sie sich bei der Cluster-IP-Adresse an, und entfernen Sie den Knoten, von dem Sie die Clusterinstanz entfernt haben.

```
rm cluster node <nodeId>

save ns config
```

   Stellen Sie sicher, dass Sie den `rm cluster node` Befehl nicht vom lokalen Knoten ausführen. Dies führt zu inkonsistenten Konfigurationen zwischen dem CCO und dem Knoten.

So entfernen Sie einen Clusterknoten mit der GUI

Navigieren Sie auf der Cluster-IP-Adresse zu **System > Cluster > Knoten, wählen Sie den Knoten**aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen.**

Entfernen eines Knotens aus einem Cluster, der mit der Clusterverknüpfungsaggregation bereitgestellt wird

August 19, 2021

Um einen Knoten aus einem Cluster zu entfernen, der Clusterverknüpfungsaggregation als Verkehrsverteilungsmechanismus verwendet, müssen Sie sicherstellen, dass der Knoten passiv

ist, damit er keinen Datenverkehr empfängt, und entfernen Sie dann auf dem Upstream-Switch die entsprechende Schnittstelle aus dem Kanal.

Ausführliche Informationen zur Cluster-Link-Aggregation finden Sie unter Verwenden der Cluster-Link-Aggregation.

So entfernen Sie einen Knoten aus einem Cluster, der die Clusterverknüpfungsaggregation als Verkehrsverteilungsmechanismus verwendet

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Legen Sie den Status des Clusterknotens, den Sie entfernen möchten, auf PASSIVE fest.

```
set cluster node <nodeId> -state PASSIVE
```

3. Entfernen Sie auf dem Upstream-Switch die entsprechende Schnittstelle mit schaltspezifischen Befehlen aus dem Kanal.

> **Hinweis:**
>
> Sie müssen die Knotenschnittstelle auf dem Cluster-Link-Aggregationskanal nicht manuell entfernen. Es wird automatisch entfernt, wenn der Knoten im nächsten Schritt gelöscht wird.

4. Entfernen Sie den Knoten aus dem Cluster.

```
rm cluster node <nodeId>
```

Erkennen von Jumbo-Sonden auf einem Cluster

August 19, 2021

Wenn ein Jumbo-Frame auf einer Clusterschnittstelle aktiviert ist, muss die Backplane-Schnittstelle groß genug sein, um alle Pakete im Jumbo-Frame zu unterstützen. Dies wird erreicht, indem die Maximum Transmission Unit (MTU) der Rückwandplatine wie folgt eingestellt wird:

backplane_MTU = Maximum (alle Cluster-Schnittstelle MTUs) + 78

Um die vorangehende Konfiguration zu überprüfen, müssen Sie einen Jumbo-Prüfpunkt (der vorherigen Berechnungsgröße) an alle Peer-Knoten eines Cluster-Setups senden. Wenn der Prüfpunkt nicht erfolgreich ist, zeigt die Appliance eine Warnmeldung in der Ausgabe des Befehls Clusterinstanz anzeigen an.

Geben Sie im Befehlszeilenschnittstellenmodus den folgenden Befehl ein:


```
> show cluster instance
  Cluster ID: 1
  Dead Interval: 3 secs
  Hello Interval: 200 msecs
  Preemption: DISABLED
  Propagation: ENABLED
  Quorum Type: MAJORITY
  INC State: DISABLED
  Process Local: DISABLED
  Cluster Status: ENABLED(admin),    ENABLED(operational), UP
```

Warnung

Die MTU für eine Backplane-Schnittstelle muss groß genug sein, um alle Pakete im Rahmen zu verarbeiten. Es muss gleich <MTU_VAL> sein. Wenn der empfohlene Wert nicht vom Benutzer konfigurierbar ist, müssen Sie den MTU-Wert von Jumbo-Schnittstellen überprüfen.

Sl. no	Mitgliedsknoten	Integrität	Admin-Status	Betriebszustand
1	Node ID: 1; Node IP: 10.102.53.167	BEREIT	Aktiv	ACTIVE (Configuration Coordinator)
2	Node ID: 2; Node IP: 10.102.53.168	BEREIT	Aktiv	Aktiv

Routenüberwachung für dynamische Routen im Cluster

August 19, 2021

Sie können einen Routenmonitor verwenden, um einen Clusterknoten von der internen Routingtabelle abhängig zu machen, unabhängig davon, ob er eine dynamisch erlernte Route enthält oder nicht. Ein Routenmonitor auf jedem Knoten überprüft die interne Routingtabelle, um sicherzustellen, dass immer ein Routeneintrag zum Erreichen eines bestimmten Netzwerks vorhanden ist. Wenn der Routeneintrag nicht vorhanden ist, ändert sich der Status des Routenmonitors in DOWN.

Wenn in einer Clusterbereitstellung der clientseitige oder serverseitige Link eines Knotens ausfällt, wird der Datenverkehr zu diesem Knoten über die Peer-Knoten zur Verarbeitung gelenkt. Die Steuerung des Datenverkehrs wird implementiert, indem dynamisches Routing konfiguriert und statische ARP-Einträge hinzugefügt werden, die auf die spezielle MAC-Adresse jedes Knotens zeigen, auf allen Knoten. Wenn es in einer Clusterbereitstellung viele Knoten gibt, ist das Hinzufügen

und Verwalten von statischen ARP-Einträgen mit speziellen MAC-Adressen auf allen Knoten eine umständliche Aufgabe. Jetzt verwenden Knoten implizit spezielle MAC-Adressen für die Steuerung von Paketen. Daher müssen statische ARP-Einträge, die auf spezielle MAC-Adressen verweisen, nicht mehr zu den Clusterknoten hinzugefügt werden.

So binden Sie einen Clusterknoten mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
unbind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
```

Betrachten Sie ein Szenario, in dem Knoten 1 an den Routenmonitor 1.1.1.0 255.255.255.0 gebunden ist. Wenn eine dynamische Route fehlschlägt, wird Knoten 1 INAKTIV. Der Integritätsstatus steht im folgenden `show cluster node` Befehl nach Knoten-ID zur Verfügung.

```
Node ID: 1
IP:  10.102.169.96
Backplane:  1/1/2
Health: NOT UP
Reason(s): Route Monitor(s) of the node have failed
Route Monitor -  Network: 1.1.1.0   Netmask: 255.255.255.0   State:
    DOWN
```

Überwachen des Cluster-Setups mit SNMP MIB mit SNMP-Link

May 11, 2023

SNMP MIB ist eine gerätespezifische Information, die auf dem SNMP-Agenten zur Identifizierung einer NetScaler-Appliance konfiguriert ist. Es kann Informationen wie Appliance-Name, Administrator und Standort identifizieren. In einem Cluster-Setup können Sie jetzt die SNMP MIB in jedem Knoten konfigurieren, indem Sie den Parameter „OwnerNode“ in den Befehl set SNMP MIB aufnehmen. Ohne diesen Parameter gilt der Befehl set SNMP MIB nur für den Cluster Coordinator (CCO) -Knoten.

Um die MIB-Konfiguration für einen anderen Clusterknoten als den CCO anzuzeigen, fügen Sie den Parameter „OwnerNode“ in den Befehl show SNMP MIB ein.

Konfiguration von SNMP MIB auf CLIP

So konfigurieren und anzeigen Sie die MIB-Konfiguration auf CLIP mit der Befehlszeilenschnittstelle.

```
set snmp mib [-contact <string>] [-name <string>] [-location <string>]
      [-customID <string>] [-ownerNode <positive_integer>]
Done
show snmp mib [-ownerNode <positive_integer>]

 > set mib -contact John -name NS59 -location San Jose -customID 123 -
    ownerNode 3
Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun  7
           2016, 10:27:29
        sysUpTime:   124300
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  John
        sysName:     NS59
        sysLocation: San Jose
        sysServices: 72
        Custom ID: 123
 Done

> unset mib -contact -name -location -customID -ownerNode 3
 Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun 7
           2016, 10:27:29
        sysUpTime:   146023
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  WebMaster (default)
        sysName:     NetScaler
        sysLocation: POP (default)
        sysServices: 72
        Custom ID: Default
 Done
```


Cluster SNMP-Trap-Nachrichten

Beim Cluster-Setup müssen die SNMP-Trap-Alarmkonfigurationen über den CLIP vorgenommen werden. Die Befehle werden an jeden der Knoten weitergegeben.

Weitere Informationen zum Konfigurieren von SNMP finden Sie unter Konfigurieren des NetScaler zum Generieren von SNMP-Traps.

Im Folgenden sind die Cluster-spezifischen Traps aufgeführt, die verfügbar sind:

```
>sh snmp alarm | grep cluster
    CLUSTER-BACKPLANE-HB-MISSING N/A N/A 86400   ENABLED - ENABLED
    CLUSTER-CCO-CHANGE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-NODE-HEALTH N/A N/A 86400 ENABLED - ENABLED
    CLUSTER-NODE-QUORUM N/A N/A 86400 ENABLED - ENABLED
    CLUSTER-OVS-CHANGE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-PROP-FAILURE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-SYNC-FAILURE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-SYNC-PARTIAL-SUCCESS N/A N/A N/A ENABLED - ENABLED
    CLUSTER-VERSION-MISMATCH N/A N/A 86400 ENABLED - ENABLED
```

Überwachen von Fehlern bei der Befehlsausbreitung in einer Clusterbereitstellung

May 11, 2023

In einer Cluster-Bereitstellung können Sie den neuen Befehl „show prop status“ verwenden, um Probleme schneller zu überwachen und zu beheben. Die Probleme betrafen Fehler bei der Befehlsübertragung auf Nicht-CCO-Knoten. Dieser Befehl zeigt bis zu 20 der letzten Fehler bei der Befehlsübertragung auf allen Nicht-CCO-Knoten an. Sie können entweder die NetScaler Appliance CLI oder die GUI verwenden, um diesen Vorgang auszuführen. Sie können über die CLIP-Adresse oder über die NSIP-Adresse eines beliebigen Knotens in der Cluster-Bereitstellung auf sie zugreifen.

Ordnungsgemäßes Herunterfahren von Knoten

May 11, 2023

In einem Cluster-Setup gehen einige der vorhandenen Verbindungen (1/N-te Verbindungen, wobei N die Clustergröße ist) auf Clusterebene oder auf bestimmter virtueller Serverebene verloren. Dieses Verhalten wird beobachtet, wenn ein Knoten das System verlässt oder dem System beitritt. Um den

Verlust zu beheben, müssen Sie die bestehenden Verbindungen ordnungsgemäß handhaben. Eine reibungslose Handhabung erfolgt, indem die Option „Verbindungen im Cluster beibehalten“ in der CLIP-Adresse konfiguriert und im NSIP des Knotens ein Timeout-Intervall angegeben wird.

Der elegante Umgang mit Verbindungen ist in zwei Szenarien anwendbar:

1. Cluster-Upgrade
2. Neuer Knoten hinzugefügt

Ordnungsgemäßer Umgang mit Knoten beim Cluster-Upgrade

Um einen Cluster zu aktualisieren, müssen Sie jeweils einen Knoten aktualisieren. Bevor Sie einen Knoten aktualisieren, müssen Sie ihn in den passiven Zustand versetzen und ihn nach dem Upgrade in den aktiven Zustand versetzen. Um zu vermeiden, dass bestehende Verbindungen beim Upgrade des Knotens beendet werden, fahren Sie ihn ordnungsgemäß mit einem konfigurierten Timeout-Intervall herunter. Andernfalls wird 1/N (wobei N die Clustergröße ist) der Clusterverbindungen beendet.

> **Hinweis**
>
> Wenn bestehende Sitzungen nicht innerhalb des konfigurierten Timeout-Intervalls abgeschlossen werden, werden sie nach Ablauf der Nachfrist beendet.

Im Folgenden finden Sie die Schritte zur ordnungsgemäßen Handhabung von Knoten in einem Cluster-Upgrade-Szenario:

1. Stellen Sie sich ein Cluster-Setup mit fünf Knoten (n0, n1, n2, n3, n4) vor.
2. Bevor Sie einen Knoten herunterfahren, müssen Sie die Option „RetainConnectionsOnCluster“ konfigurieren. Es hilft, alle vorhandenen Verbindungen dieses Knotens auf Clusterebene oder virtueller Serverebene für ein bestimmtes Zeitintervall beizubehalten.

   Beispiel

   Auf CLIP

   “‘set cluster instance –retainConnectionsOnCluster YES

   ```
   ODER

   ```set lb vserver <vserver name>  - retainConnectionsOnCluster Yes
      <!--NeedCopy-->
   ```

3. Melden Sie sich nun an der NSIP-Adresse von Knoten n3 an und setzen Sie den Knoten n3 auf PASSIVE mit einem internen Timeout.

   Beispiel

   “‘set cluster node n3 –state PASSIVE –delay 60


   ```

```
1 ```saveconfig<!--NeedCopy-->
```

4. Schließen Sie nach Ablauf der Kulanzzeit alle Verbindungen, fahren Sie n3 herunter und starten Sie die NetScaler-Appliance neu.
5. Führen Sie ein Upgrade der Appliance durch. Stellen Sie dann, wenn die CLI mit der NSIP-Adresse der Appliance verbunden ist, den Knoten auf ACTIVE.

   Beispiel

   "'set cluster node n3 –state ACTIVE

   ```
   1 ```saveconfig<!--NeedCopy-->
   ```

6. Wiederholen Sie die Schritte 4—6 für alle Knoten im Cluster.
7. Nachdem alle Knoten aktualisiert und auf ACTIVE gesetzt wurden, setzen Sie die Option RetainConnectionsOnCluster von der CLIP-Adresse zurück.

   Beispiel

   "'set cluster instance -retainConnectionsOnCluster NO

   ```
   1 ODER
   2
   3 ```set lb vserver <vserver name>  - retainConnectionsOnCluster NO
       <!--NeedCopy-->
   ```

> **Hinweis**
>
> Wenn beim Upgrade eines Clusters ein Versionskonflikt auftritt, wird die Clusterpropagierung automatisch deaktiviert und es sind keine Befehle auf dem CLIP zulässig.

Anmutiger Umgang mit Knoten beim Hinzufügen eines neuen Knotens

Der elegante Umgang mit Knoten beschreibt, wie ein neuer Knoten zum vorhandenen NetScaler-Cluster hinzugefügt werden kann. Stellen Sie sich vor, Sie haben einen NetScaler-Cluster, der bereits Traffic bereitstellt. Und Sie möchten dem Cluster eine zusätzliche Appliance als Knoten hinzufügen, ohne die bestehenden Verbindungen zu beenden. Um das obige Szenario zu verwirklichen, legen Sie die Option fest, bestehende Verbindungen entweder auf globaler Ebene oder auf einer bestimmten virtuellen Serverebene beizubehalten. Wenn Sie fertig sind, speichern Sie die Konfiguration. Stellen Sie nun die Option zum Beibehalten von Verbindungen auf NEIN, damit bestehende Verbindungen von anderen Knoten dem neuen Knoten neu zugewiesen werden können.

Im Folgenden finden Sie die Schritte, um Knoten ordnungsgemäß zu behandeln, wenn ein Knoten neu hinzugefügt wurde:

1. Sie speichern die bestehende Konfiguration, in der die Option „RetainConnectionsOnCluster“ aktiviert ist. Auf diese Weise können Sie alle vorhandenen Verbindungen dieses Knotens auf Clusterebene oder virtueller Serverebene für ein bestimmtes Zeitintervall beibehalten.

   Auf CLIP

   ```
   1 set cluster instance x - retainConnectionsOnCluster YES
   ```

   ODER

   ```
   1 set lb vserver xxxx -retainConnectionsOnCluster Yes
   ```

2. Fügen Sie dem Cluster-Setup einen Knoten ‘n5’ hinzu.
3. Deaktivieren Sie die Option „RetainConnectionOnCluster“ auf „NEIN“, um bestehende Verbindungen von anderen Knoten auf den neu hinzugefügten Knoten n5 zu verteilen.

   Auf CLIP

   ```
   1 set cluster instance x - retainConnectionsOnCluster NO
   ```

   ODER

   ```
   1 set lb vserver xxxx -retainConnectionsOnCluster NO
   ```

> **Hinweis**
>
> Die Backplane-Steuerung hängt von der Art des Verkehrsverteilungsmechanismus (ECMP, CLAG und USIP) in einem Cluster-Setup ab. Die Erhöhung der Lenkung auf der Rückwandplatine hängt von der Verkehrsart ab.

Konfiguration des ordnungsgemäßen Herunterfahrens von Knoten in einem Cluster

Gehen Sie wie folgt vor, um das ordnungsgemäße Herunterfahren von Knoten in einem Cluster zu konfigurieren:

1. Konfigurieren Sie die Option „RetainConnectionsOnCluster“ auf globaler Ebene (Cluster).
2. Konfigurieren Sie die Option „RetainConnectionsOnCluster“ auf virtueller Serverebene.
3. Versetzen Sie den Knoten (beim Verlassen des Systems) in den passiven Zustand mit einem angemessenen Timeout-Intervall, das in der NSIP-Adresse des Knotens angegeben ist.
4. Überwachen Sie die bestehenden Verbindungen, um sicherzustellen, dass alle Transaktionen innerhalb der Übergangsfrist abgeschlossen werden.

So behalten Sie vorhandene Verbindungen auf globaler (Cluster-) Ebene über die Befehlszeilenschnittstelle

Sie können bestehende Verbindungen entweder auf globaler Ebene oder auf einer bestimmten virtuellen Serverebene beibehalten. Diese Option ist so konfiguriert, dass alle vorhandenen Verbindungen auf globaler Ebene beibehalten werden. Standardmäßig ist diese Option deaktiviert.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 - set cluster instance <clusterID> -retainConnectionsOnCluster YES
2
3 - set cluster instance 60 - retainConnectionsOnCluster YES
```

So behalten Sie vorhandene Verbindungen eines bestimmten virtuellen Servers im Cluster über die Befehlszeilenschnittstelle

Diese Option ist so konfiguriert, dass bestehende Verbindungen, die für einen virtuellen Lastausgleichsserver spezifisch sind, beibehalten werden. Um diese Verbindungen beizubehalten, aktivieren wir diese Option auf virtueller Serverebene. Standardmäßig ist diese Option deaktiviert.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 - set lb vserver <clusterID> -retainConnectionsOnCluster Yes
2
3 - set lb vserver v1 -retainConnectionsOnCluster Yes
```

So setzen Sie einen Clusterknoten mit der CLI auf den passiven Status

Um einen Clusterknoten mit einem angemessenen Timeout-Intervall in den passiven Zustand zu versetzen. Diese Einstellung wird im NSIP des Knotens vorgenommen, da die Propagierung während des Cluster-Upgrades deaktiviert ist.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 - set cluster node <clusterID> -state passive
2 -backplane <interface_name>@
3 -priority <positive_integer>
4 -delay <mins>
5
6 - set cluster node 4 -state PASSIVE -delay 60
7
8 - set cluster instance 60 - retainConnectionsOnCluster YES
9 - set lb vserver v1 -retainConnectionsOnCluster Yes
10 - set cluster node 4 -state PASSIVE -delay 60
```


> **Hinweis**
>
> Sie können auf einem Clusterknoten das folgende Verhalten beobachten, wenn dieser auf passiv gesetzt ist und eine von einem CLIP aus konfigurierte Verzögerungsoption verwendet wird:
>
> - Nach dem Timeout wird der Knoten vom NSIP des Knotens als passiv angezeigt.
> - Der Befehl **show cluster instance** auf CLIP zeigt den Knoten im CLIP als aktiv an. Wohingegen der Befehl **show cluster node** auf dem CLIP den Knoten als passiv anzeigt.

So konfigurieren Sie das ordnungsgemäße Herunterfahren von Knoten mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > System > Cluster** und klicken Sie auf **Cluster verwalten.**
2. Wählen Sie auf der Seite „ **Cluster verwalten** “ die Option „ **Verbindungen im Cluster beibehalten** “ aus.
3. Klicken Sie auf **OK**, und klicken Sie dann auf **Fertig**.

Ordnungsgemäßes Herunterfahren von Diensten

May 11, 2023

Ab NetScaler 12.1 Build 49.xx unterstützen NetScaler-Cluster das ordnungsgemäße Herunterfahren von Diensten. Um die Dienste ordnungsgemäß herunterzufahren, können Sie eine der folgenden Aufgaben ausführen.

- den Dienst explizit deaktivieren und
  - Stellen Sie eine Verzögerung (in Sekunden) ein.
  - Aktivieren Sie das ordnungsgemäße Herunterfahren.
- Fügen Sie dem Monitor einen TROFS-Code oder eine Zeichenfolge hinzu.

Weitere Informationen finden Sie unter Graceful Shutdown von Diensten.

So konfigurieren Sie ein ordnungsgemäßes Herunterfahren für einen Dienst mit der CLI

Nur mit der Option „Graceful“ deaktivieren:

Geben Sie in der Befehlszeile Folgendes ein:

```
disable service <name> [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```


Beispiel

```
disable service svc1 -graceFul YES
Done
sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE   Graceful (number of
                   active clients: 1)
                Last state change was at Wed Jul 25 10:46:29 2018
                Time since last state change: 0 days, 00:00:02.680
                ……….
                ……….
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 26           Failed [Total: 0
                                   Current: 0]
                                Last response: Success - TCP syn+ack
                                   received.
                                Response Time: 0.0 millisec
<!--NeedCopy-->
```

Mit Timeout und Graceful-Option deaktivieren:

Geben Sie in der Befehlszeile Folgendes ein:

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Beispiel

```
disable service svc1 2000 -graceFul YES

Done
> sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE (Graceful (number of active
                    clients: 1), Out Of Service in 1998 seconds)
                Last state change was at Wed Jul 25 10:49:08 2018
                Time since last state change: 0 days, 00:00:01.710
                ……….
                ……….
```



```
                  Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                 Passive: 0
                                Probes: 57           Failed [Total: 0
                                    Current: 0]
                                Last response: Success - TCP syn+ack
                                    received.
                                Response Time: 0.0 millisec
Done
<!--NeedCopy-->
```

Deaktivieren Sie die Dienstgruppe mit Timeout und Graceful-Option:

Geben Sie in der Befehlszeile Folgendes ein:

```
disable serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-delay
<secs>] [-graceFul ( YES | NO )]
Show service group <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
disable servicegroup sg -delay 2000 -graceFul yes
sh servicegroup sg
                sg - HTTP
                State: DISABLED                Effective State: OUT OF
                    SERVICE Monitor Threshold : 0
                Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                    kbits
                Use Source IP: NO
                Client Keepalive(CKA): NO
                ... ... ... .
                ... ... ...


                1)   200.200.10.21:80       Server Name: server3
                    Server ID: None Weight: 1
                                State:    GOING OUT OF SERVICE (learnt
                                    from node:2 )     Graceful (number
                                    of active clients: 6), Out Of
                                    Service in 1993 seconds
                                Last state change was at Mon Aug 13
                                    15:15:11 2018
                                ... ... ...
```



```
16
17                  2)   200.200.10.22:80       Server Name: server4
                       Server ID: None Weight: 1
18                                  State:    GOING OUT OF SERVICE (learnt
                                       from node:2 )     Graceful (number
                                       of active clients: 7), Out Of
                                       Service in 1993 seconds
19                                  Last state change was at Mon Aug 13
                                       15:15:11 2018
20 <!--NeedCopy-->
```

> **Hinweis**
> CLIP zeigt den aggregierten Wert aller aktiven Clientverbindungen von allen Clusterknoten an.

So konfigurieren Sie das ordnungsgemäße Herunterfahren für einen Dienst mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie den Dienst und klicken Sie in der Aktionsliste auf **Deaktivieren**. Geben Sie eine Wartezeit ein und wählen Sie Graceful aus.

So konfigurieren Sie einen TROFS-Code oder eine Zeichenfolge in einem Monitor mithilfe der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
1 add lb monitor <monitor-name> HTTP -trofsCode <respcode>
2 add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>
3 add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
4 <!--NeedCopy-->
```

So konfigurieren Sie einen TROFS-Code oder eine Zeichenfolge in einem Monitor mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Klicken Sie im Bereich Monitore auf Hinzufügen und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie Typ als HTTP aus und geben Sie einen TROFS-Code an.
   - Wählen Sie Typ als HTTP-ECV oder TCP-ECV aus, und geben Sie einen TROFS-String an.

IPv6-fähige Logo-Unterstützung für Cluster

August 19, 2021

Sie können Cluster-Appliances für die IPv6-Ready-Logo-Zertifizierung testen. Modifizierte Befehle zum Testen von IPv6-Kernprotokollen, z. B. für ND-Testfälle, Routeranforderungsverarbeitung und das Senden von Routenankündigungs- und Routerumleitungsnachrichten stehen in einem Cluster-Setup zur Verfügung. Im Folgenden sind die IPv6-Funktionalitäten zum Testen der IPv6-Kernprotokolle verfügbar.

Im Folgenden finden Sie die geänderten Funktionalitäten, die verfügbar sind, um IPv6-Core-Protokolle zu bestehen, wie ND-Testfälle, Router Solicitation-Verarbeitung und das Senden von Route-Werbung und Router-Umleitungsnachrichten in der Phase2-Testsuite IPv6ReadyLogo.

- Lokale SNIPs verknüpfen
- Adressenauflösung und Neighbor Unerreichbarkeit
- Router- und Präfixerkennung
- Routerumleitung
- DoDAD

Mit diesen geänderten Befehlen werden die folgenden Konfigurationen in einer Cluster-Appliance unterstützt.

Unterstützbare Konfigurationen zum Testen von IPv6-Kernprotokollen

Damit ein Cluster-Setup IPv6 Ready Logo-Testfälle bestehen kann, können Sie die folgenden Konfigurationen für die Cluster Management-IP-Adresse (CLIP) ausführen.

- global IP6 configuration
- basic IPv6 configuration
- weitere IPv6-Konfigurationen

Globale Konfiguration

Eine globale IPv6-Konfiguration ermöglicht es Ihnen, die globalen IPv6-Parameter (wie Relearning, RoutereDirection, NdBaseReachTime, NreTransLissionTime `natprefix`, td und doodad) so einzustellen, dass die grundlegende IPv6-Konfiguration ausgeführt wird.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ipv6 [-ralearning ( ENABLED | DISABLED )] [-routerRedirection (
    ENABLED | DISABLED )] [-ndBasereachTime<positive_integer>][-
    ndRetransmissionTime <positive_integer>] [-natprefix <ipv6_addr|*>[-
    td<positive_integer>]] [-doDAD ( ENABLED | DISABLED )]
```


Grundlegende IPv6-Konfiguration

Die grundlegende IPv6-Konfiguration ermöglicht es Ihnen, eine IPv6-Adresse zu erstellen und an eine VLAN-Schnittstelle zu binden. Sie können die folgenden Konfigurationen durchführen, um die IPv6-Core-Protokolle zu testen.

So fügen Sie dem Cluster-Setup über die Befehlszeilenschnittstelle ein VLAN hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add vlan <id>
```

So fügen Sie dem Cluster-Setup mit der CLI ein weiteres VLAN hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add vlan <id>
```

So binden Sie eine Schnittstelle mit der CLI an ein VLAN

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface_name>
```

So binden Sie eine Schnittstelle mit der CLI an ein VLAN

Mit diesem Befehl wird das globale Präfix als On-Link-Präfix in RA-Informationen für nachfolgende Router-Advertisements hinzugefügt. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface_name>
```

So fügen Sie die IPv6-SNIP-Adresse in einem VLAN mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

So fügen Sie die IPv6-Adresse im VLAN mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

So binden Sie die IPv6-Adresse mit der CLI an VLAN

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```


So binden Sie die IPv6-Adresse mit der CLI an VLAN

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```

So zeigen Sie die lokale IPv6-Adresse des Links an, die mit dem VLAN mit der CLI verbunden ist

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
sh VLAN
```

Beispiel 1

```
add vlan 2
add vlan 3
bind vlan 2 -ifnum 1/2
bind vlan 3 -ifnum 1/3
add ip6 fe80::9404:60ff:fedd:a464/64 -vlan 2 -scope link-local -type
    SNIP
add ip6 fe80::c0ee:7bff:fede:263f/64 -vlan 3 -scope link-local -type
    SNIP
add ip6 3ffe:501:ffff:100:9404:60ff:fedd:a464/64 -vlan 2
add ip6 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64 -vlan 3
bind vlan 2 -ipAddress 3ffe:501:ffff:100:9404:60ff:fedd:a464/64
bind vlan 3 -ipAddress 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64
```

Beispiel 2

```
sh vlan
1)      VLAN ID: 2      VLAN Alias Name:
        Interfaces : 1/6
        IPs :
             3ffe:501:ffff:100:2e0:edff:fe15:ea2a/64
3)      VLAN ID: 3      VLAN Alias Name:
        Link-local IPv6 addr: fe80::9404:60ff:fedd:a464/64
        Interfaces : 1/5
        IPs :
             3ffe:501:ffff:101:2e0:edff:fe15:ea2b/64
 Done
```


Mehr IPv6-Cluster-Konfiguration

Zum Testen von IPv6-Kernprotokollen können Sie die folgenden neuen oder geänderten IPv6-Konfigurationen verwenden.

So legen Sie VLAN-spezifische Router Advertisement-Parameter mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set nd6RAvariables -vlan <positive_integer> [-ceaseRouterAdv ( YES | NO )] [-sendRouterAdv ( YES | NO )] [-srcLinkLayerAddrOption ( YES | NO )][-onlyUnicastRtAdvResponse ( YES | NO )] [-managedAddrConfig ( YES | NO)] [-otherAddrConfig ( YES | NO )] [-currHopLimit <positive_integer>][-maxRtAdvInterval <positive_integer>] [-minRtAdvInterval<positive_integer>] [-linkMTU <positive_integer>] [-reachableTime<positive_integer>] [-retransTime <positive_integer>] [-defaultLifeTime<integer>]
```

So legen Sie die konfigurierbaren Parameter eines globalen On-Link-Präfixes über die Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-decrementPrefixLifeTimes ( YES | NO )] [-prefixValideLifeTime <positive_integer>] [-prefixPreferredLifeTime <positive_integer>]
```

So fügen Sie einem globalen On-Link-Präfix mit der CLI konfigurierbare Parameter hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-decrementPrefixLifeTimes ( YES | NO )]-prefixValideLifeTime <positive_integer>][-prefixPreferredLifeTime <positive_integer>]
```

So richten Sie einen On-Link zu den konfigurierbaren Parametern des IPv6-Präfixes mit der CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
help set onLinkIPv6Prefix
```

So binden Sie einen On-Link mit den konfigurierbaren Parametern des IPv6-Präfixes mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
help bind nd6RAvariables
```


So zeigen Sie Nd6raVariables mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
help sh nd6RAvariables
```

Beispiel

```
> sh nd6RAvariables
  1) Vlan : 1
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv: 198
     LinkMTU         : 0    ReachableTime  : 0          RetransTimer   : 0
     DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    : 0

  2) Vlan : 2
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv: 198
     LinkMTU         : 0    ReachableTime  : 0          RetransTimer   : 0
     DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    : 0
Done
>
> sh nd6Ravariables  -vlan 2
  1) Vlan : 2
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress: YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag: NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv: 198
     LinkMTU         : 0    ReachableTime  : 0          RetransTimer   : 0
```



```
23      DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    :
            0
24      Prefix :
25  3ffe:501:ffff:100::/64
26  Done
```

Verwalten von Cluster Heartbeat-Nachrichten

May 11, 2023

Die Verwaltung von Heartbeat-Nachrichten in einem Cluster ähnelt der Verwaltung in einer Hochverfügbarkeitskonfiguration (HA). Knoten können auf allen aktivierten Schnittstellen Heartbeat-Nachrichten an und voneinander senden und empfangen. Um einen erhöhten Datenverkehr aufgrund von Heartbeat-Meldungen zu vermeiden, können Sie jetzt die Heartbeat-Option auf Knotenschnittstellen deaktivieren. Die Heartbeat-Option auf der Backplane-Schnittstelle kann jedoch nicht deaktiviert werden, da sie für die Aufrechterhaltung der Konnektivität zwischen den Clusterknoten erforderlich ist.

Weitere Informationen zum Verwalten von Herzmeldungen finden Sie unter Verwalten von Heartbeat-Nachrichten für hohe Verfügbarkeit auf einer NetScaler Appliance.

So verwalten Sie Heartbeat-Meldungen auf einer Knotenschnittstelle mit der NetScaler CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1  set interface <ID> [-HAHeartBeat (ON | OFF)]
2  Show interface <ID>
```

Konfigurieren des Antwortstatus des Eigentümer

May 11, 2023

Sie können die OwnerDownResponse-Option auf einem Knoten konfigurieren, der über eine entdeckte SNIP-Adresse verfügt. Standardmäßig ist die Option aktiviert. Es ermöglicht der erkannten IP-Adresse, auf PING- oder ARP-Anfragen (vom Upstream-Router) zu antworten, wenn der Knoten inaktiv ist. Wenn Sie die Option deaktivieren, kann die IP-Adresse nicht auf die Router-Anforderungen reagieren, wenn der Besitzer-Knoten inaktiv ist.

Um zu erfahren, wie diese Funktion zur Überwachung statischer Routen in der ECMP-Bereitstellung verwendet wird, finden Sie unter Verwenden von Equal Cost Multiple Path (ECMP) .

So legen Sie den Antwortstatus des Besitzerknotens mit der NetScaler CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns ip <IPAddress> [-ownerNode <positive_integer>] [-
    ownerDownResponse (YES | NO )] [-td <positive_integer>]
```

Beispiel

```
add ns ip 2.2.2.2 255.255.255.0 -ownernode 6  - ownerdownResponse YES
```

So legen Sie den Antwortstatus des Besitzerknotens über die NetScaler GUI fest

1. Navigieren Sie zu **System > Netzwerk > IPs** und klicken Sie auf **Hinzufügen**, um eine entdeckte SNIP-Adresse zu erstellen.
2. Aktivieren oder deaktivieren Sie auf der Seite „ **IP-Adresse erstellen** “ das Kontrollkästchen **OwnerDownResponse** .

So bearbeiten Sie den Antwortstatus des Eigentümerknotens mithilfe der NetScaler-GUI

Navigieren Sie zu **System > Netzwerk > IPs**, wählen Sie eine IP-Adresse aus, und klicken Sie auf **Bearbeiten**, um das Kontrollkästchen **OwnerDownResponse**zu aktivieren oder zu deaktivieren.

Überwachung der Unterstützung für statische Routen (MSR) für inaktive Knoten in einer Spotted Cluster-Konfiguration

January 19, 2021

In einem Cluster, der mit der MSR-Option auf der Route aktiviert ist, können nur aktive Knoten auf eine statische Route untersuchen. Es kann ein Netzwerk erreichen, während inaktive und Reserveknoten keine Verbindung zur Route haben und nicht mit ihr nachforschen können. Sie können jetzt einen inaktiven oder Ersatzknoten konfigurieren, um PING und ARP Probe an IPv4-Route zu senden und ping6 und nd6 Probe an IPv6-Route zu senden. Sie können dies nur in einer Spotted Cluster-Konfiguration durchführen, in der die SNIP-Adresse aktiv ist und ausschließlich einem Knoten gehört.

VRRP-Interface-Bindung in einem aktiven Cluster mit einem einzigen Knoten

May 11, 2023

Wenn Sie ein Hochverfügbarkeits-Setup (HA) zu einem Cluster-Setup migrieren, müssen alle Konfigurationen kompatibel und im Cluster unterstützt werden können. Um dies zu erreichen, können Sie jetzt virtuelle Router-IDs (VRIDs und VRID6s) auf einer Knotenschnittstelle konfigurieren.

> **Wichtig**
>
> Derzeit unterstützt nur ein aktives Clustersystem mit einem Knoten VRIDs und VRID6s.

Anweisungen zum Konfigurieren von VRIDs und vRID6s finden Sie unter Konfigurieren von Virtual MAC-Adressen.

Um eine virtuelle Router-ID auf einem aktiven Cluster mit einem Knoten zu konfigurieren, fügen Sie die VRID oder VRID6 hinzu und binden Sie sie an die Cluster-Knoten-Schnittstelle.

So fügen Sie eine VRID mithilfe der NetScaler-CLI hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add vrID <ID>
```

So binden Sie eine VRID mit der NetScaler CLI an die Cluster-Knoten-Schnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
Bind vrid <ID> -ifnum <interface_name> | -trackifNum <interface_name

Add vrID 100
Bind vrid 100  - ifnum 1/1  1/2
done
```

So fügen Sie einen VRID6 mit der NetScaler CLI hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add vrID6 <ID>
```

So binden Sie einen VRID6 mit der CLI an eine Clusterknotenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
bind vrid6 <ID> -ifnum <interface_name> | -trackifNum <interface_name>

Add vrID6 100
```



```
Bind vrid6 100  - ifnum 1/1  1/2
Done
```

Setup- und Nutzungsszenarien

May 11, 2023

In diesem Abschnitt werden einige Szenarien erläutert, in denen der NetScaler-Cluster für verschiedene Funktionen und Netzwerktopologien eingerichtet und konfiguriert werden kann. Geben Sie Feedback, wenn Sie andere Szenarien dokumentieren möchten.

Erstellen eines Clusters mit zwei Knoten

January 19, 2021

Ein Cluster mit zwei Knoten stellt eine Ausnahme von der Regel dar, dass ein Cluster nur dann funktionsfähig ist, wenn mindestens (n/2 +1) Knoten, wobei n die Anzahl der Clusterknoten ist, in der Lage sind, Datenverkehr zu bedienen. Wenn dieselbe Formel auf einen Zwei-Knoten-Cluster angewendet wird, würde der Cluster fehlschlagen, wenn ein Knoten ausfällt (n/2 +1=2).

Ein Cluster mit zwei Knoten ist auch dann funktionsfähig, wenn nur ein Knoten den Datenverkehr bedienen kann.

Das Erstellen eines Clusters mit zwei Knoten entspricht dem Erstellen eines anderen Clusters. Sie fügen einen einen Knoten als Konfigurationskoordinator und den anderen Knoten als den anderen Clusterknoten hinzu.

> **Hinweis:**
>
> Die inkrementelle Konfigurationssynchronisierung wird in einem Cluster mit zwei Knoten nicht unterstützt. Es wird nur eine vollständige Synchronisation unterstützt.

Migrieren eines HA-Setups auf ein Cluster-Setup

May 11, 2023

Um ein vorhandenes Hochverfügbarkeits-Setup (HA) zu einem Cluster-Setup zu migrieren, müssen Sie zuerst die NetScaler-Appliances aus dem HA-Setup entfernen und eine Backup der HA-

Konfigurationsdatei erstellen. Anschließend können Sie die beiden Appliances verwenden, um einen Cluster zu erstellen und die gesicherte Konfigurationsdatei in den Cluster hochzuladen.

> **Hinweis**
>
> - Bevor Sie die gesicherte HA-Konfigurationsdatei in den Cluster hochladen, müssen Sie sie ändern, um sie clusterkompatibel zu machen. Lesen Sie den entsprechenden Schritt des Verfahrens.
> - Verwenden Sie den <backup_filename>Befehl **batch -f**, um die gesicherte Konfigurationsdatei hochzuladen.

Bei dem vorherigen Ansatz handelt es sich um eine grundlegende Migrationslösung, die zu Ausfallzeiten für die bereitgestellte Anwendung führt. Daher darf es nur in Bereitstellungen verwendet werden, bei denen die Anwendungsverfügbarkeit nicht berücksichtigt wird.

In den meisten Bereitstellungen ist die Verfügbarkeit der Anwendung jedoch von größter Bedeutung. In solchen Fällen müssen Sie den Ansatz verwenden, bei dem ein HA-Setup zu einem Cluster-Setup migriert werden kann, ohne dass es zu Ausfallzeiten kommt. Bei diesem Ansatz wird ein vorhandenes HA-Setup auf ein Cluster-Setup migriert, indem zuerst die sekundäre Appliance entfernt und diese Appliance verwendet wird, um einen Cluster mit einem Knoten zu erstellen. Sobald der Cluster betriebsbereit ist und den Datenverkehr bereitstellt, wird die primäre Appliance des HA-Setups zum Cluster hinzugefügt.

So konvertieren Sie ein HA-Setup mithilfe der Befehlszeilenschnittstelle in ein Cluster-Setup (ohne Ausfallzeiten)

Betrachten wir das Beispiel eines HA-Setups mit der primären Appliance (NS1) — 10.102.97.131 und der sekundären Appliance (NS2) — 10.102.97.132.

1. Stellen Sie sicher, dass die Konfigurationen des HA-Paares stabil sind.
2. Melden Sie sich bei einer der HA-Appliances an, rufen Sie die Shell auf und erstellen Sie eine Kopie der Datei ns.conf (z. B. ns_backup.conf).
3. Melden Sie sich bei der sekundären Appliance NS2 an und löschen Sie die Konfigurationen. Dieser Vorgang entfernt NS2 aus dem HA-Setup und macht es zu einer eigenständigen Appliance.

```
1 > clear ns config full
```

> **Hinweis**
>
> - Dieser Schritt ist erforderlich, um sicherzustellen, dass NS2 nicht anfängt, VIP-Adressen zu besitzen, da es sich um eine eigenständige Appliance handelt.
> - Zu diesem Zeitpunkt ist die primäre Appliance, NS1, noch aktiv und dient weiterhin

> dem Datenverkehr.

4. Erstellen Sie einen Cluster auf NS2 (jetzt keine sekundäre Appliance mehr), und konfigurieren Sie ihn als PASSIVE-Knoten.

```
> add cluster instance 1

> add cluster node 0 10.102.97.132 -state PASSIVE -backplane
   0/1/1

> add ns ip 10.102.97.133 255.255.255.255 -type CLIP

> enable cluster instance 1

> save ns config

> reboot -warm
```

5. Ändern Sie die gesicherte Konfigurationsdatei wie folgt:

   - Entfernen Sie die Features, die in einem Cluster nicht unterstützt werden. Eine Liste der nicht unterstützten Funktionen finden Sie unter NetScaler Features, die von einem Cluster unterstützt werden. Dies ist ein optionaler Schritt. Wenn Sie diesen Schritt nicht ausführen, schlägt die Ausführung nicht unterstützter Befehle fehl.
   - Entfernen Sie die Konfigurationen, die Schnittstellen haben, oder aktualisieren Sie die Schnittstellennamen von der c/u-Konvention auf die n/c/u-Konvention .

     Beispiel

     ```
     > add vlan 10 -ifnum 0/1
     ```

     muss geändert werden in

     ```
     > add vlan 10 -ifnum 0/0/1 1/0/1
     ```

   - Die Sicherungskonfigurationsdatei kann SNIP-Adressen haben. Diese Adressen sind auf allen Clusterknoten Striped. Es wird empfohlen, für jeden Knoten gepunktete IP-Adressen hinzuzufügen.

     Beispiel

     ```
     > add ns ip 1.1.1.1 255.255.255.0 -ownerNode 0

     > add ns ip 1.1.1.2 255.255.255.0 -ownerNode 1
     ```


- Aktualisieren Sie den Hostnamen, um den Besitzerknoten anzugeben.

  Beispiel

  ```
  > set ns hostname ns0 -ownerNode 0

  > set ns hostname ns1 -ownerNode 1
  ```

- Ändern Sie alle anderen relevanten Netzwerkkonfigurationen, die von gefleckten IPs abhängen. Zum Beispiel L3-VLAN, RNAT-Konfiguration, die SNIPs als NATIP verwendet, INAT-Regeln, die sich auf SNIPS/MIPS beziehen).

6. Gehen Sie auf dem Cluster wie folgt vor:

   - Nehmen Sie die topologischen Änderungen am Cluster vor, indem Sie die Cluster-Backplane, den Cluster-Link-Aggregationskanal usw. verbinden.
   - Wenden Sie Konfigurationen aus der gesicherten und geänderten Konfigurationsdatei über die Cluster-IP-Adresse auf den Konfigurationskoordinator an.

     ```
     > batch -f ns_backup.conf
     ```

   - Konfigurieren Sie externe Verkehrsverteilungsmechanismen wie ECMP oder Cluster-Link-Aggregation.

7. Verlagern Sie den Datenverkehr vom HA-Setup zum Cluster.

   - Melden Sie sich bei der primären Appliance NS1 an, und deaktivieren Sie alle Schnittstellen darauf.

     ```
     > disable interface <interface_id>
     ```

   - Melden Sie sich bei der Cluster-IP-Adresse an, und konfigurieren Sie NS2 als ACTIVE-Knoten.

     ```
     > set cluster node 0 -state ACTIVE
     ```

   > **Hinweis**
   >
   > Zwischen dem Deaktivieren der Schnittstellen und dem Aktivieren des Clusterknotens kann es zu einer geringen Ausfallzeit (in der Größenordnung von Sekunden) kommen.

8. Melden Sie sich bei der primären Appliance NS1 an und entfernen Sie sie aus dem HA-Setup.

   - Löschen Sie alle Konfigurationen. Dieser Vorgang entfernt NS1 aus dem HA-Setup und macht es zu einer eigenständigen Appliance.

     ```
     > clear ns config full
     ```


- Aktivieren Sie alle Schnittstellen.

```
> enable interface <interface_id>
```

9. Fügen Sie NS1 zum Cluster hinzu.
   - Melden Sie sich bei der Cluster-IP-Adresse an, und fügen Sie NS1 zum Cluster hinzu.

```
> add cluster node 1 10.102.97.131 -state PASSIVE -backplane
   1/1/1
```

   - Melden Sie sich bei NS1 an und verbinden Sie es mit dem Cluster, indem Sie die folgenden Befehle sequenziell ausführen:

```
> join cluster -clip 10.102.97.133 -password nsroot

> save ns config

> reboot -warm
```

10. Melden Sie sich bei NS1 an, und führen Sie die erforderlichen topologischen und Konfigurationsänderungen durch.
11. Melden Sie sich bei der Cluster-IP-Adresse an, und legen Sie NS1 als ACTIVE-Knoten fest.

```
> set cluster node 1 -state ACTIVE
```

Übergang zwischen einem L2- und L3-Cluster

May 11, 2023

> **Hinweis**
>
> Wird ab NetScaler 11 unterstützt.

Ein L2-Cluster ist ein Cluster, bei dem alle Knoten aus demselben Netzwerk stammen, und ein L3-Cluster kann Knoten aus verschiedenen Netzwerken enthalten. Sie können nahtlos von einem Clustertyp zum anderen wechseln, ohne dass es zu Ausfallzeiten für die Anwendungen kommt, die auf dem NetScaler bereitgestellt werden.

Umstellung eines Clusters von L2 auf L3

Sie können zu einem L3-Cluster wechseln, wenn der Cluster Knoten aus anderen Netzwerken enthalten soll.

Gehen Sie für die Cluster-IP-Adresse wie folgt vor:

1. Erstellen Sie eine Knotengruppe.

   Beispiel

   ```
   1 > add cluster nodegroup NG0
   ```

   Diese Knotengruppe wird im nächsten Schritt verwendet, um alle Knoten aus dem bestehenden L2-Cluster zu gruppieren.

2. Überführen Sie den L2-Cluster in einen L3-Cluster.

   Beispiel

   ```
   1 > set cluster instance 1 -inc ENABLED -nodegroup NG0
   ```

   Dieser Befehl erreicht den doppelten Zweck der Umstellung auf den L3-Cluster und das Hinzufügen aller Knoten des L2-Clusters zur Knotengruppe.

3. Jetzt können Sie dem Cluster weitere Knoten hinzufügen, wie unter Hinzufügen eines Knotens zum Clusterbeschrieben.

Übergang eines Clusters von L3 zu L2

Sie können zu einem L2-Cluster wechseln, wenn Sie Knoten behalten möchten, die zu einem einzigen Netzwerk gehören.

Gehen Sie für die Cluster-IP-Adresse wie folgt vor:

1. Entfernen Sie die Clusterknoten aus den Netzwerken, die Sie nicht behalten möchten.

   Beispiel

   ```
   1 > rm cluster node <nodeId>
   ```

2. Übergang des L3-Clusters zu einem L2-Cluster.

   Beispiel

   ```
   1 > set cluster instance 1 -inc DISABLED
   ```

   Der Cluster enthält jetzt nur Knoten eines einzelnen Netzwerks.

Einrichten von GSLB in einem Cluster

August 19, 2021

> **Hinweis:**
>
> Unterstützt ab NetScaler 10.5 Build 52.11.

Um GSLB in einem Cluster einzurichten, müssen Sie die verschiedenen GSLB-Entitäten an eine Knotengruppe binden. Die Knotengruppe muss über einen einzelnen Mitgliedsknoten verfügen.

> **Hinweise**
>
> - Wenn Sie die statische Proximity-GSLB-Methode konfiguriert haben, stellen Sie sicher, dass die statische Proximity-Datenbank auf allen Cluster-Knoten vorhanden ist. Dies geschieht standardmäßig, wenn die Datenbankdatei am Standardspeicherort verfügbar ist. Wenn die Datenbankdatei jedoch in einem anderen Verzeichnis als /var/netscaler/locdb/ gespeichert wird, müssen Sie die Datei manuell mit allen Cluster-Knoten synchronisieren.
> - Der `show gslb domain` Befehl wird in einem Cluster-Setup nicht unterstützt.

So richten Sie GSLB in einem Cluster mit der CLI ein:

Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie die folgenden Vorgänge an der Eingabeaufforderung aus:

1. Konfigurieren Sie die verschiedenen GSLB-Entitäten. Weitere Informationen finden Sie unter GSLB-Konfigurations-Entitäten.

   > **Hinweis:**
   >
   > Stellen Sie beim Erstellen der GSLB-Site sicher, dass Sie die Cluster-IP-Adresse und die IP-Adresse des öffentlichen Clusters angeben. Die IP-Adresse des öffentlichen Clusters wird nur benötigt, wenn der Cluster hinter einem NAT-Gerät bereitgestellt wird. Beim Konfigurieren einer GSLB-Site müssen Sie die Cluster-IP-Adresse desselben Standorts verwenden. Diese Parameter sind erforderlich, um die Verfügbarkeit der GSLB-Auto-Synchronisierungsfunktion zu gewährleisten.

   ```
   add gslb site <siteName> <siteType> <siteIPAddress> -publicIP <ip_addr>
    -clip <ip_addr> <publicCLIP><!--NeedCopy-->
   ```

2. Erstellen Sie eine Cluster-Knotengruppe.

   ```
   add cluster nodegroup <name> <name>@ [-strict ( YES | NO )] [-sticky (
   YES | NO )] [-state <state>] [-priority <positive_integer>]<!--NeedCopy
   -->
   ```

   > **Hinweis:**
   >
   > Aktivieren Sie die Sticky-Option, wenn Sie GSLB-basiert für VPN-Benutzer einrichten möchten.

3. Binden Sie einen einzelnen Clusterknoten an die Knotengruppe.


```
bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
```

4. Binden Sie die lokale GSLB-Site an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -gslbSite <string><!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass die IP-Adresse der lokalen GSLB-Site-IP-Adresse gestreift ist (verfügbar über alle Clusterknoten).

5. Binden Sie den ADNS- (oder ADNS-TCP-Dienst) oder den DNS- (oder DNS-TCP) Lastausgleichsserver an die Knotengruppe.

   So binden Sie den ADNS-Dienst:

   “‘bind cluster nodegroup -service

   ```
   **So binden Sie den virtuellen DNS-Lastausgleichsserver:**

   ```bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

6. Binden Sie den virtuellen GSLB-Server an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

7. [Optional] Um GSLB basierend auf VPN-Benutzern einzurichten, binden Sie den virtuellen VPN-Server an die GSLB-Knotengruppe.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

8. Überprüfen Sie die Konfigurationen.

   ```
   show gslb runningConfig<!--NeedCopy-->
   ```

So richten Sie GSLB in einem Cluster mit der GUI ein:

Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie die folgenden Vorgänge auf der Registerkarte Konfiguration aus:

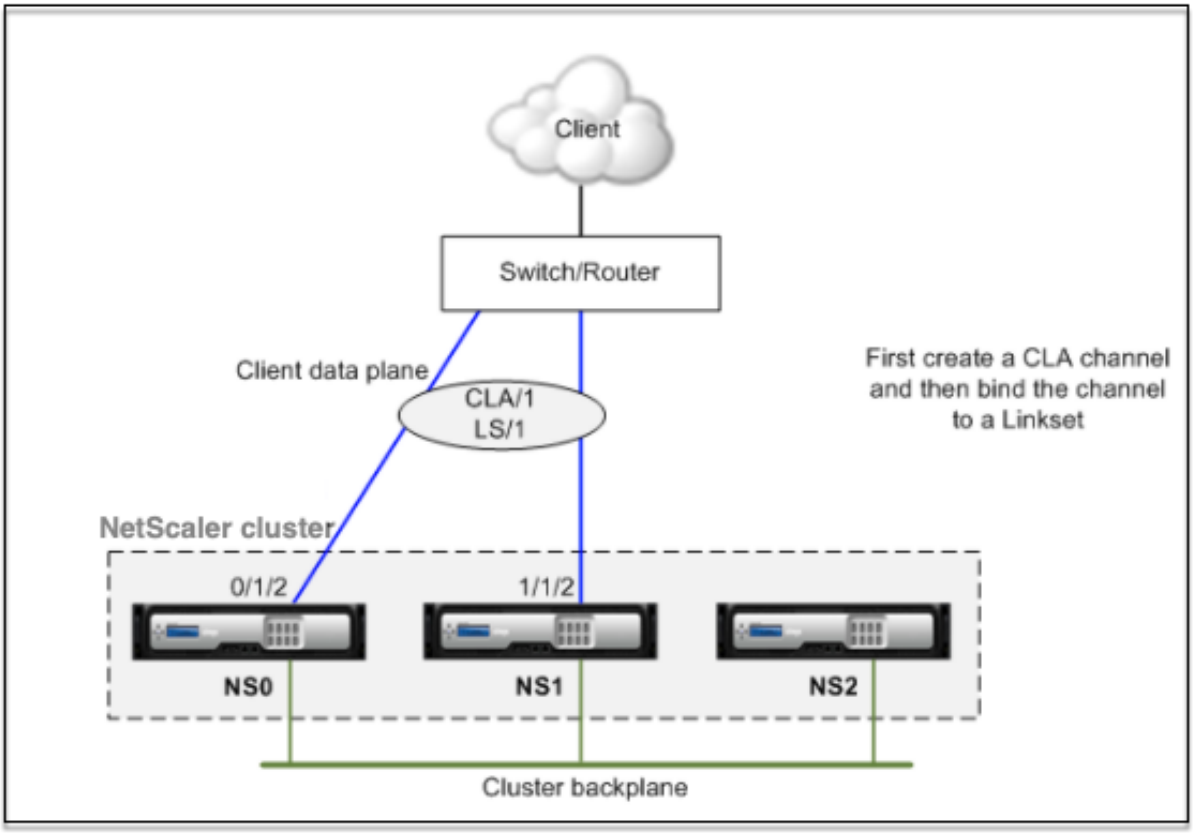
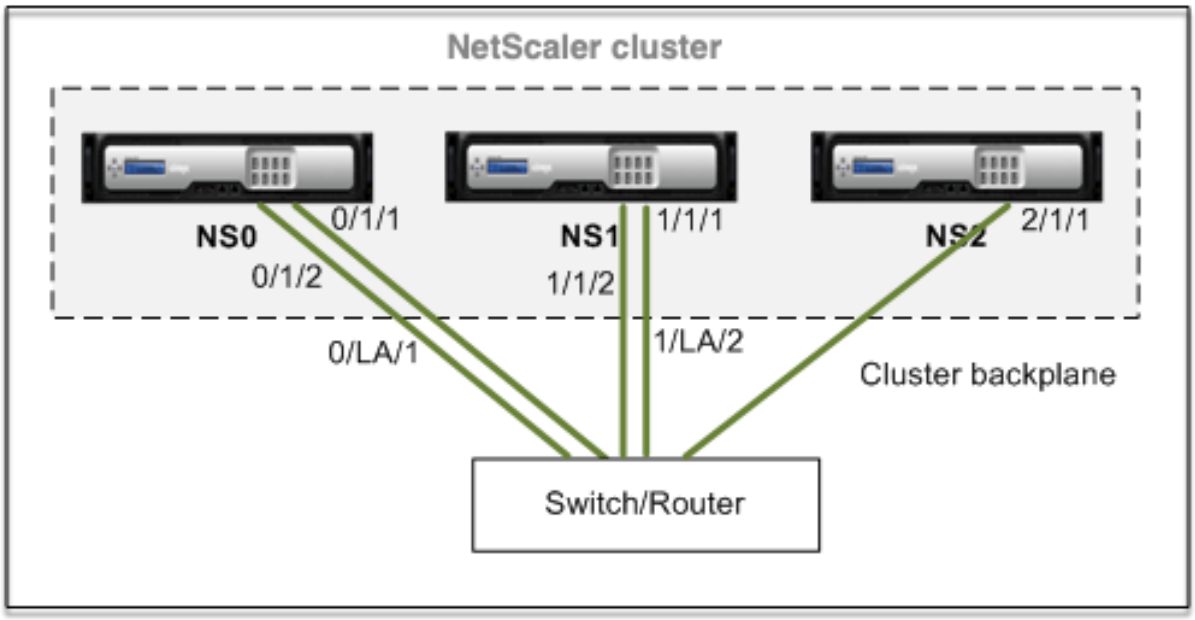
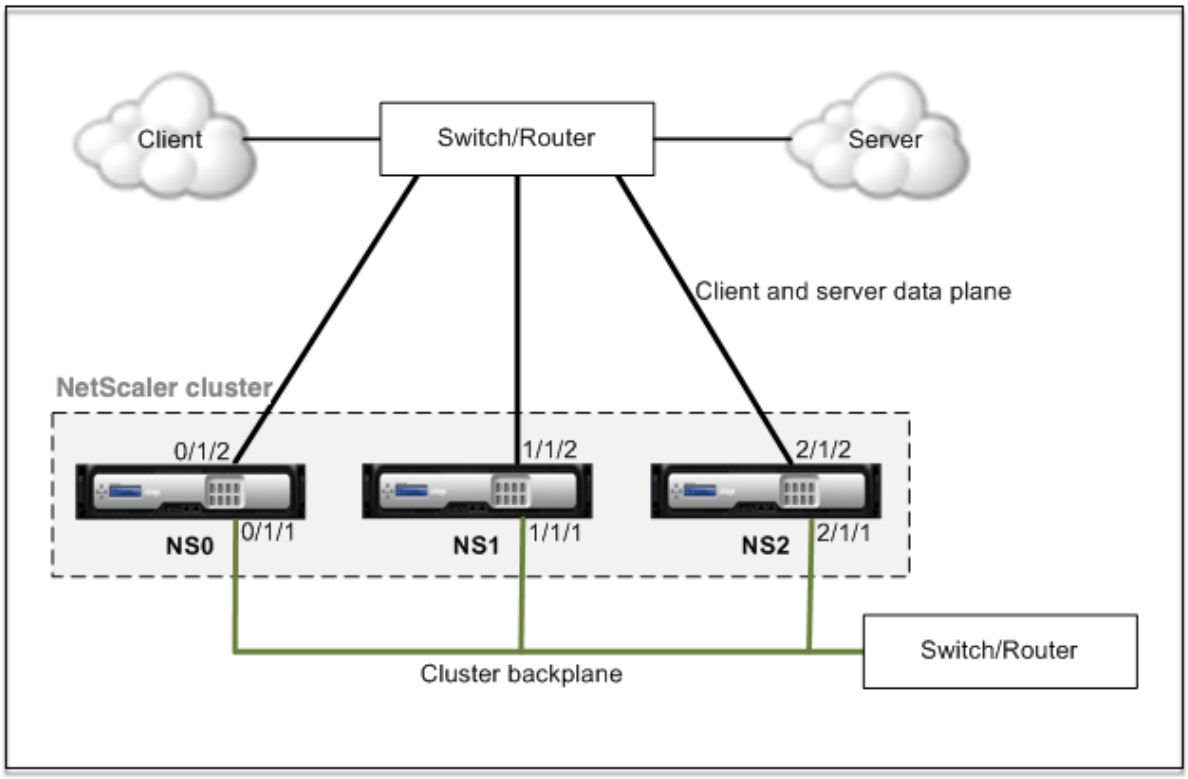
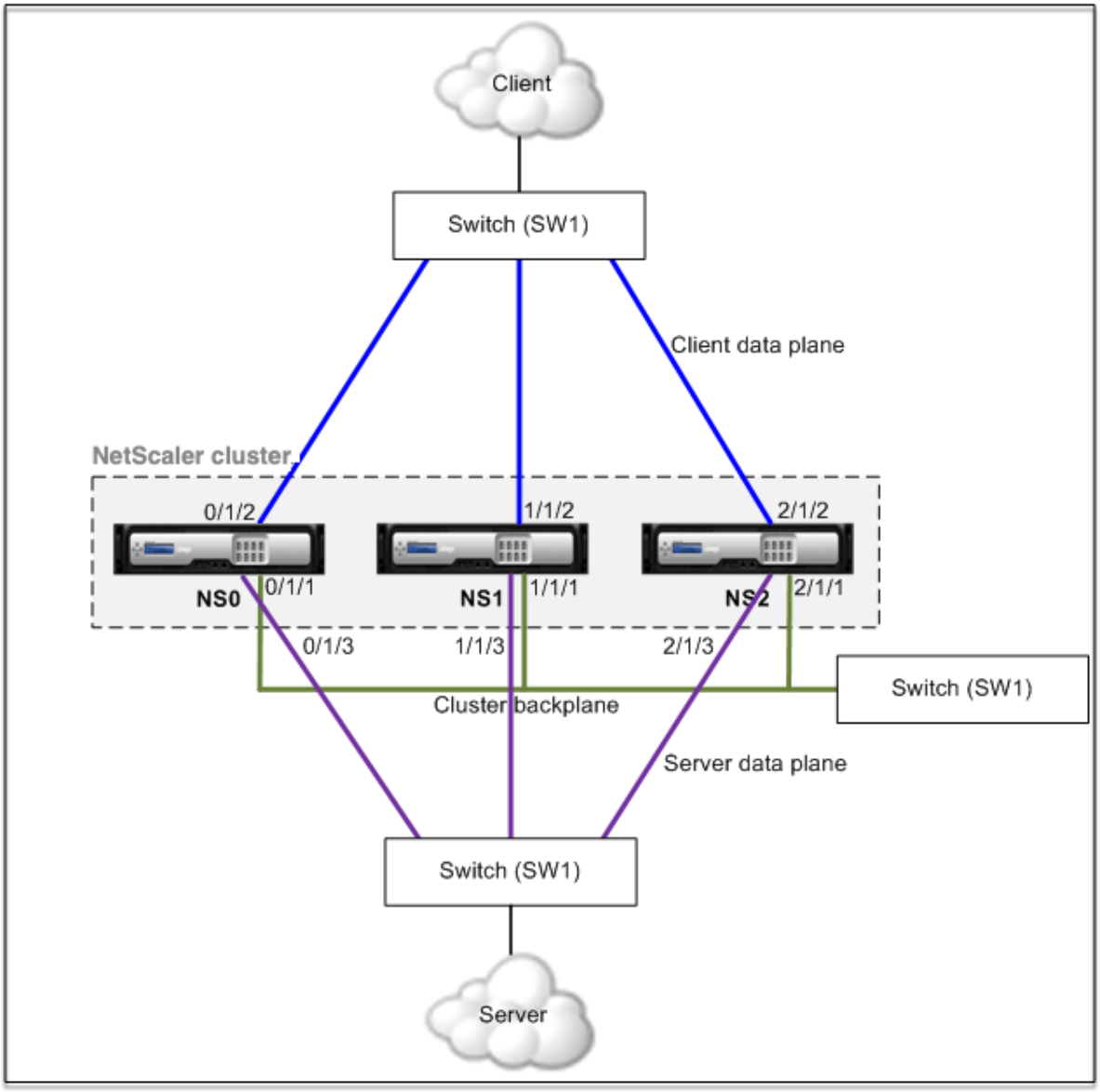
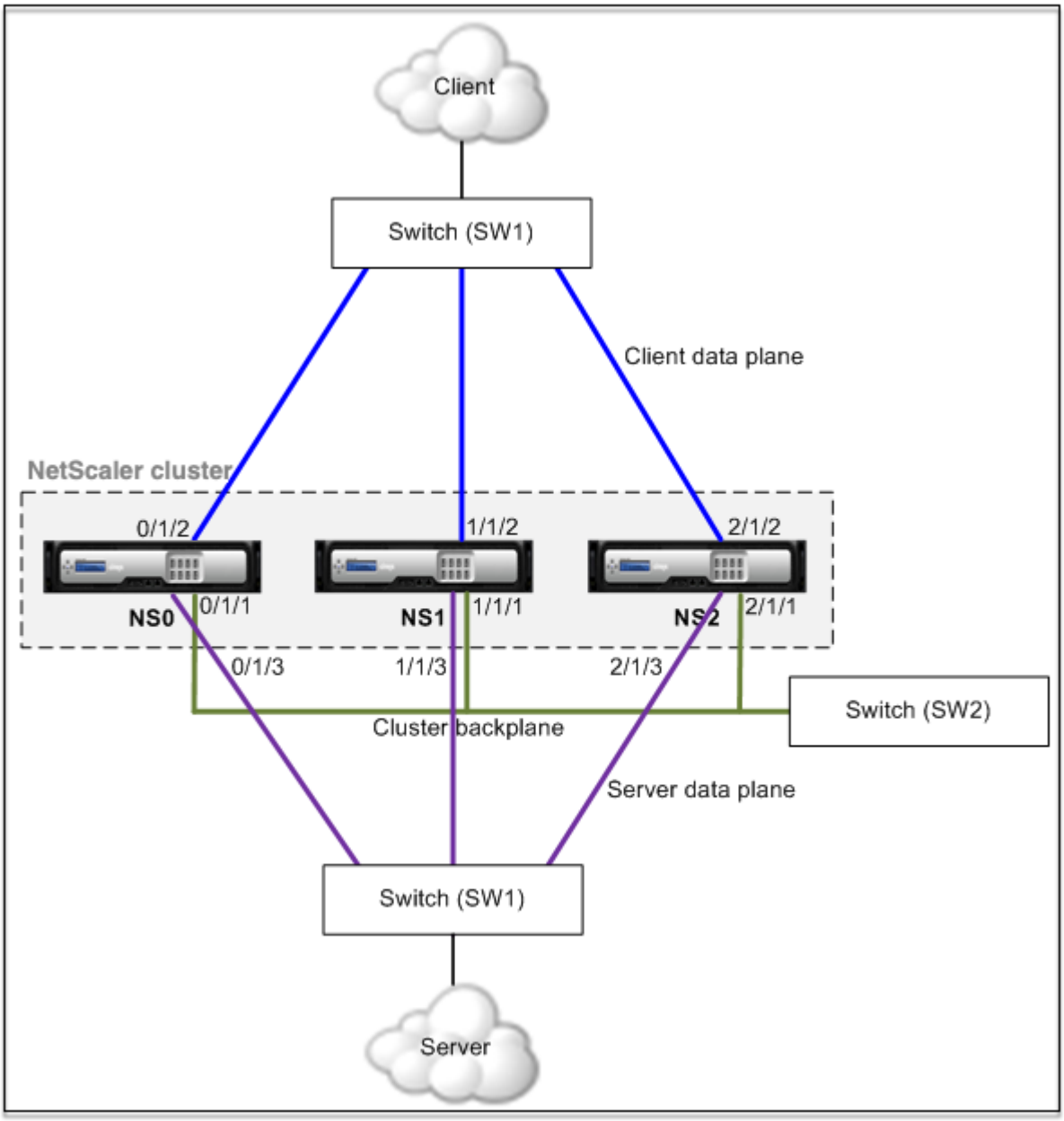
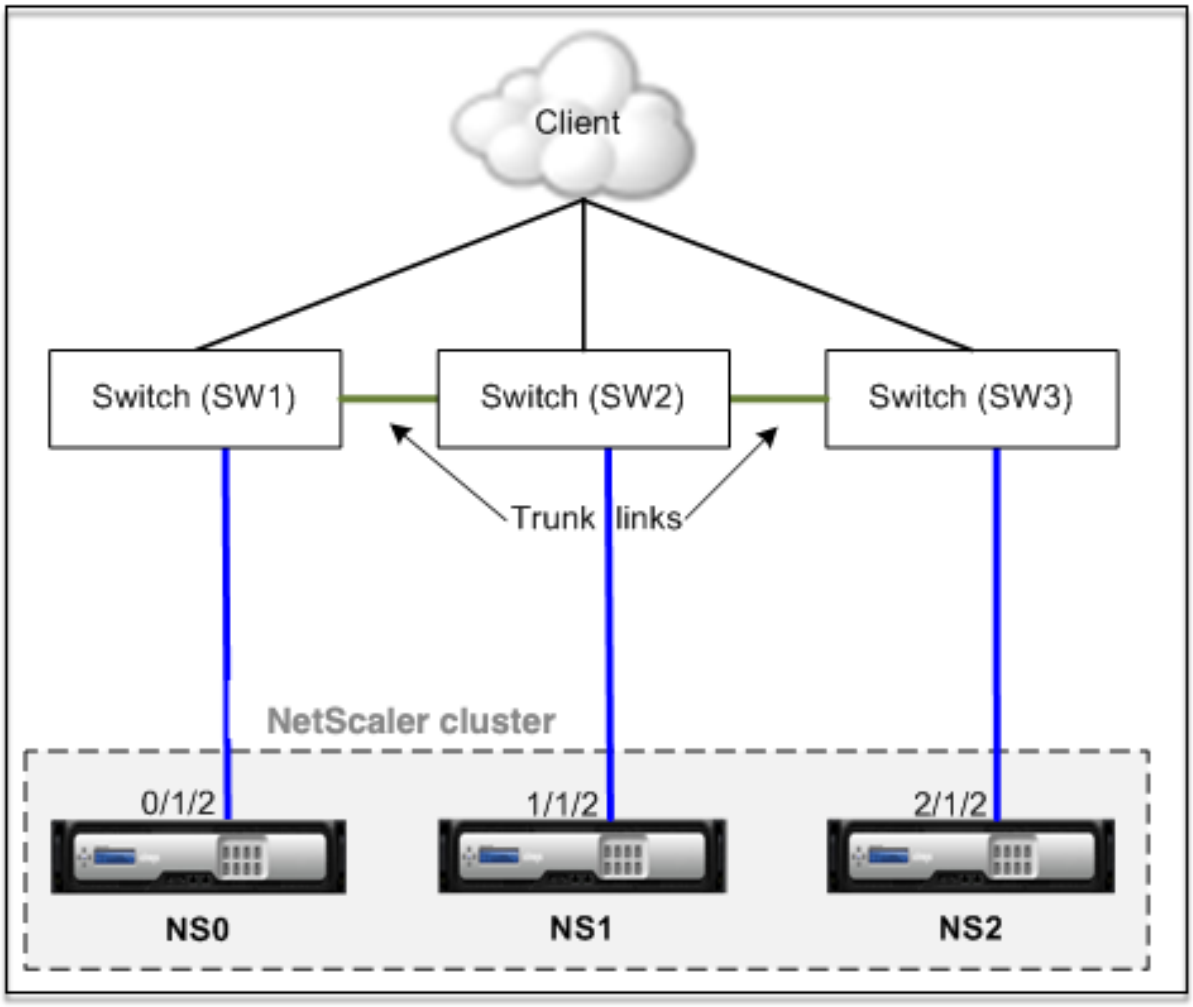
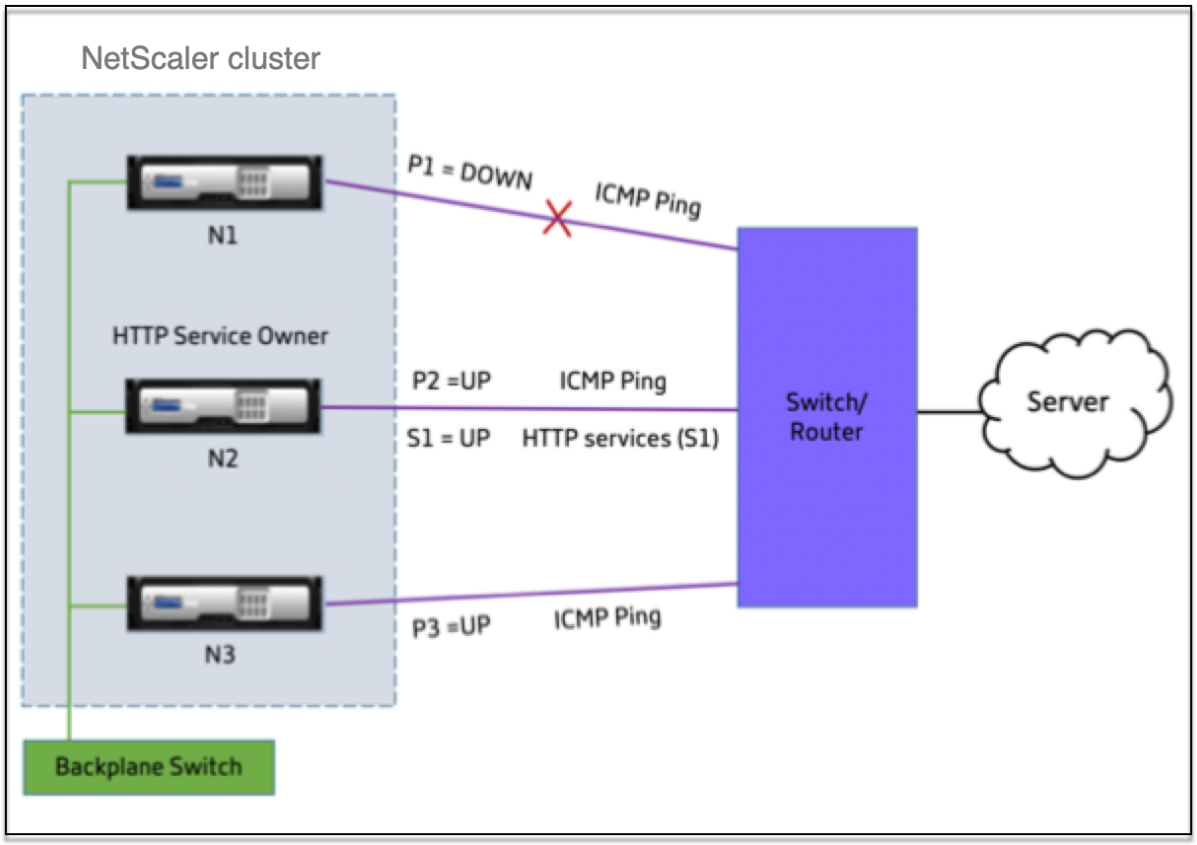
1. Konfigurieren Sie die GSLB-Entitäten.

   Navigieren Sie zu **Traffic Management > GSLB**, um die erforderlichen Konfigurationen durchzuführen.

2. Erstellen Sie eine Knotengruppe und führen Sie andere Knotengruppen-bezogene Konfigurationen durch.

   Navigieren Sie zu **System > Cluster > Knotengruppen**, um die erforderlichen Konfigurationen durchzuführen.

Die detaillierten Konfigurationen finden Sie in der Beschreibung des vorherigen CLI-Verfahrens.


   ```

### Unterstützung für GSLB-Topologie für übergeordnete und untergeordnete GSLB-Topologie in einem Cluster

Beginnend mit NetScaler 12.1 Build 49.xx wird GSLB Parent-Child-Topologie im Cluster unterstützt.

Weitere Informationen zur Eltern-Kind-Topologie finden Sie unter Bereitstellung von Eltern-Kind-Topologie unter Verwendung des MEP-Protokolls.

#### So richten Sie die übergeordnete und untergeordnete GSLB-Topologie in einem Cluster mit der Befehlszeilenschnittstelle ein

##### Übergeordnete Site

Führen Sie die folgende Konfiguration durch:

1. Erstellen Sie eine Cluster-Knotengruppe.

   ```
   add cluster nodegroup <name>
   ```

   Beispiel:

   ```
   add cluster nodegroup parentng
   ```

2. Binden Sie einen einzelnen Clusterknoten an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng -node n2
   ```

3. Binden Sie die lokale GSLB-Site an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng -gslbSite site1
   ```

4. Binden Sie den ADNS- (oder ADNS-TCP-Dienst) oder den DNS- (oder DNS-TCP) Lastausgleichsserver an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -service <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng - service ADNS
   ```

5. Binden Sie den virtuellen GSLB-Server an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -vServer <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng -vServce gslbvs1
   ```


Untergeordnete Site

Führen Sie die folgende Konfiguration durch:

1. Erstellen Sie eine Cluster-Knotengruppe.

   ```
   add cluster nodegroup <name>
   ```

   Beispiel:

   ```
   add cluster nodegroup childng
   ```

2. Binden Sie einen einzelnen Clusterknoten an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Beispiel:

   ```
   bind cluster nodegroup childng -node -n3
   ```

3. Binden Sie die lokale GSLB-Site an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup childng -gslbSite site1
   ```

> **Hinweis:**
>
> Damit übergeordnete und untergeordnete Standorte aggregierte Statistiken in metrikbasierten Lastausgleichsmethoden austauschen können, müssen Sie lokale GSLB-Dienste auf dem untergeordneten Standort hinzufügen. Die metrikbasierten Load Balancing-Methoden sind die geringste Verbindung, die geringste Bandbreite und die geringsten Pakete.

So richten Sie die übergeordnete und untergeordnete GSLB-Topologie in einem Cluster mit der GUI ein

1. Konfigurieren Sie die GSLB-Entitäten.

   Navigieren Sie zu **Traffic Management** > **GSLB**, um die erforderlichen Konfigurationen durchzuführen.

2. Erstellen Sie eine Knotengruppe.

   Navigieren Sie zu **System** > **Cluster** > **Knotengruppen**, um die erforderlichen Konfigurationen durchzuführen.

3. Wählen Sie auf der Seite “Knotengruppe” die Knotengruppe aus, an die Sie einen Knoten binden möchten, klicken Sie auf **“Bearbeiten”**und führen Sie die folgenden Aufgaben aus. Sie können diese Aufgaben auch ausführen, wenn Sie eine Knotengruppe hinzufügen.

- Binden Sie einen Knoten an die Knotengruppe.

  Klicken Sie in **Advance Settings**auf **Clusterknoten** und führen Sie die folgenden Aufgaben aus:

  - Klicken Sie im Abschnitt " **Clusterknoten** " auf **Kein Clusterknoten**.
  - Klicken **Sie in Clusterknoten**auswählen auf > und wählen Sie den Knoten aus, den Sie an die Knotengruppe binden möchten. Sie können auch einen Cluster-Knoten hinzufügen.

- Binden Sie die lokale GSLB-Site an die Knotengruppe.

  Klicken Sie in Advance Settings auf GSLB-Sites, und führen Sie die folgenden Aufgaben aus:

  - Klicken Sie im Abschnitt **GSLB Sites** auf Keine GSLB-Site.
  - Klicken **Sie auf der GSLB-Site**auswählen auf > und wählen Sie die GSLB-Site aus, die Sie an die Knotengruppe binden möchten. Sie können auch eine GSLB-Site hinzufügen.

- Binden Sie den virtuellen GSLB-Server an die Knotengruppe.

  Klicken Sie in **Advance Settings**auf **Virtual Servers** und führen Sie die folgende Aufgabe aus

  - Klicken Sie im Bereich " **Virtuelle Server** " auf +.
  - **Wählen Sie unter Choose Virtual Server**den Server aus, den Sie an die Knotengruppe binden möchten.

- Binden Sie den ADNS- (oder ADNS-TCP-Dienst) oder den DNS- (oder DNS-TCP) Lastausgleichsserver an die Knotengruppe.

  Klicken Sie in **Advance Settings**auf **Services** und führen Sie die folgenden Aufgaben aus:

  - Klicken Sie im Abschnitt " **Dienste** " auf **Kein Dienst**.
  - **Wählen Sie unter Dienst**auswählen den Dienst aus, den Sie an die Knotengruppe binden möchten. Sie können auch einen Dienst hinzufügen.

> **Hinweis:**
>
> Für untergeordnete Sites müssen Sie nur den Clusterknoten und den lokalen GSLB-Site an die Knotengruppe binden.

Verwenden der Cache-Umleitung in einem Cluster

May 11, 2023

Die Cache-Umleitung in einem Cluster funktioniert genauso wie auf einer eigenständigen NetScaler-Appliance. Der einzige Unterschied besteht darin, dass die Konfigurationen für die Cluster-IP-Adresse durchgeführt werden. Weitere Informationen zur Cache-Umleitung finden Sie unter Cache-Umleitung.

Punkte, die bei der Verwendung der Cache-Umleitung im transparenten Modus auf einem Cluster zu beachten sind:

- Stellen Sie vor der Konfiguration der Cache-Umleitung sicher, dass Sie alle Knoten mit dem externen Switch verbunden haben und dass Sie Linksets konfiguriert haben. Andernfalls werden Client-Anfragen verworfen.
- Wenn der MAC-Modus auf einem virtuellen Lastausgleichsserver aktiviert ist, stellen Sie sicher, dass der MBF-Modus auf dem Cluster aktiviert ist, indem Sie den Befehl enable ns mode MBF verwenden. Andernfalls werden die Anfragen direkt an den Ursprungsserver gesendet, anstatt an den Cache-Server gesendet zu werden.

Verwenden des L2-Modus in einem Cluster-Setup

January 19, 2021

> **Hinweis:**
>
> Unterstützt von NetScaler 10.5 und höher.

Um den L2-Modus in einem Cluster-Setup zu verwenden, müssen Sie Folgendes sicherstellen:

- Gefleckte IP-Adressen müssen bei Bedarf auf allen Knoten verfügbar sein.
- Linksets müssen verwendet werden, um mit dem externen Netzwerk zu kommunizieren.
- Asymmetrische Topologien oder asymmetrische Cluster-LA Gruppen werden nicht unterstützt.
- Cluster-LA-Gruppe wird empfohlen.
- Der Datenverkehr wird auf die Clusterknoten nur für Bereitstellungen verteilt, in denen Dienste vorhanden sind.

Verwenden des Cluster-LA Kanals mit Linksets

January 19, 2021

In einer asymmetrischen Cluster-Topologie sind einige Clusterknoten nicht mit dem Upstream-Netzwerk verbunden. In einem solchen Fall müssen Sie Linksets verwenden. Um die Leistung zu optimieren, können Sie die Schnittstellen, die mit dem Switch verbunden sind, als Cluster-LA-Kanal binden und dann den Kanal an einen Linkset binden.

Um zu verstehen, wie eine Kombination aus Cluster-LA-Kanal und Linksets verwendet werden kann, sollten Sie einen Cluster mit drei Knoten betrachten, für den der Upstream-Switch nur zwei Ports verfügbar ist. Sie können zwei Clusterknoten mit dem Switch verbinden und den anderen Knoten nicht verbunden lassen.

> **Hinweis:**
>
> In ähnlicher Weise können Sie auch eine Kombination aus ECMP und Linksets in einer asymmetrischen Topologie verwenden.

Abbildung 1. Linksets und Cluster-LA Kanaltopologie



So konfigurieren Sie Cluster LA-Channel und Linksets mit der CLI

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Binden Sie die angeschlossenen Schnittstellen an einen Cluster-LA-Kanal.

```
add channel CLA/1 -ifnum 0/1/2 1/1/2
```

3. Binden Sie den Cluster LA-Kanal an den Linkset.

```
add linkset LS/1 -ifnum CLA/1
```


Rückwandplatine auf LA-Kanal

January 19, 2021

In dieser Bereitstellung werden LA-Kanäle für die Cluster-Rückwandplatine verwendet.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit den Backplane-Schnittstellen als LA-Kanäle bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.

   a) Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:

   ```
   > create cluster instance 1
   > add cluster node 0 10.102.29.60 -state ACTIVE
   > enable cluster instance 1
   > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
   > save ns config
   > reboot -warm
   ```

   b) Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

   ```
   > add cluster node 1 10.102.29.70 -state ACTIVE
   ```



```
2 > add cluster node 2 10.102.29.80 -state ACTIVE
```

c) Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

2. Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

a) Erstellen Sie die LA-Kanäle für die Knoten NS0 und NS1.

```
1 > add channel 0/LA/1 -ifnum 0/1/1 0/1/2
2 > add channel 1/LA/2 -ifnum 1/1/1 1/1/2
```

b) Konfigurieren Sie die Rückwandplatine für die Clusterknoten.

```
1 > set cluster node 0 -backplane 0/LA/1
2 > set cluster node 1 -backplane 1/LA/2
3 > set cluster node 2 -backplane 2/1/1
```

Gemeinsame Schnittstellen für Client und Server und dedizierte Schnittstellen für Backplane

May 11, 2023

Es handelt sich um eine einarmige Bereitstellung des NetScaler-Clusters. Bei dieser Bereitstellung verwenden die Client- und Servernetzwerke dieselben Schnittstellen, um mit dem Cluster zu kommunizieren. Die Cluster-Backplane verwendet dedizierte Schnittstellen für die Kommunikation zwischen den Knoten.



- NS0 - NodeID: 0, NSIP: 10.102.29.60
- NS1 — NodeID: 1, NSIP: 10.102.29.70
- NS2 — NodeID: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit einer gemeinsamen Schnittstelle für Client und Server und einer anderen Schnittstelle für die Clusterrückwandplatine bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.
2. Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:

```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

3. Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
```



```
2 > add cluster node 2 10.102.29.80 -state ACTIVE -backplane
      2/1/1
```

4. Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

1. Erstellen Sie auf der Cluster-IP-Adresse VLANs für die Backplane-Schnittstellen sowie für die Client- und Serverschnittstellen.

   //For the backplane interfaces

```
1 > add vlan 10
2 > bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Für die Schnittstellen, die mit dem Client- und Server-Netzwerk verbunden sind.

```
1 > add vlan 20
2 > bind vlan 20 0/1/2 1/1/2 2/1/2
```

2. Erstellen Sie auf dem Switch VLANs für die Schnittstellen, die den Backplaneschnittstellen sowie den Client- und Serverschnittstellen entsprechen. Die folgenden Beispielkonfigurationen sind für den Cisco® Nexus 7000 C7010 Release 5.2 (1) -Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

   //Für die Backplane-Schnittstellen. Für jede Schnittstelle wiederholen…

```
1 > interface Ethernet2/47
2   switchport access vlan 100
3   switchport mode access
4   end
```

   //Für die Schnittstellen, die mit dem Client- und Server-Netzwerk verbunden sind. Für jede Schnittstelle wiederholen…

```
1 > interface Ethernet2/47
2   switchport access vlan 200
3   switchport mode access
4   end
```


Gemeinsamer Switch für Client, Server und Backplane

May 11, 2023

Bei dieser Bereitstellung verwenden Client, Server und Backplane dedizierte Schnittstellen auf demselben Switch, um mit dem NetScaler-Cluster zu kommunizieren.



- NS0 - NodeID: 0, NSIP: 10.102.29.60
- NS1 — NodeID: 1, NSIP: 10.102.29.70
- NS2 — NodeID: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit einem gemeinsamen Switch für Client, Server und Rück-

wandplatine bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.
2. Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:

```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

3. Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

4. Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

1. Erstellen Sie auf der Cluster-IP-Adresse VLANs für die Backplane-, Client- und Server-schnittstellen.

   //For the backplane interfaces

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //For the client-side interfaces

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //For the server-side interfaces


```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

2. Erstellen Sie auf dem Switch VLANs für die Schnittstellen, die den Backplaneschnittstellen sowie den Client- und Serverschnittstellen entsprechen. Die folgenden Beispielkonfigurationen sind für den Cisco® Nexus 7000 C7010 Release 5.2 (1) -Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

   //Für die Backplane-Schnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/47
  switchport access vlan 100
  switchport mode access
  end
```

   //Für die Client-Schnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/48
  switchport access vlan 200
  switchport mode access
  end
```

   //Für die Serverschnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/49
  switchport access vlan 300
  switchport mode access
  end
```

Gemeinsamer Switch für Client und Server und dedizierter Switch für Backplane

May 11, 2023

Bei dieser Bereitstellung verwenden die Clients und Server unterschiedliche Schnittstellen auf demselben Switch, um mit dem NetScaler-Cluster zu kommunizieren. Die Cluster-Backplane verwendet einen dedizierten Switch für die Kommunikation zwischen den Knoten.



- NS0 - NodeID: 0, NSIP: 10.102.29.60
- NS1 — NodeID: 1, NSIP: 10.102.29.70
- NS2 — NodeID: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit demselben Switch für die Clients und Server und einen anderen Switch für die Clusterrückwandplatine bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.
    - Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:


```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

- Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

- Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

2. Erstellen Sie auf der Cluster-IP-Adresse VLANs für die Backplane-, Client- und Serverschnittstellen.

   //For the backplane interfaces

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //For the client-side interfaces

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

   //For the server-side interfaces

```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

3. Erstellen Sie auf dem Switch VLANs für die Schnittstellen, die den Backplaneschnittstellen sowie den Client- und Serverschnittstellen entsprechen. Die folgenden Beispielkonfigurationen sind

für den Cisco® Nexus 7000 C7010 Release 5.2 (1) -Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

//Für die Backplane-Schnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/47
> switchport access vlan 100
> switchport mode access
> end
```

//Für die Client-Schnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/48
> switchport access vlan 200
> switchport mode access
> end
```

//Für die Serverschnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/49
> switchport access vlan 300
> switchport mode access
> end
```

Unterschiedliche Schalter für jeden Knoten

January 19, 2021

In dieser Bereitstellung ist jeder Clusterknoten mit einem anderen Switch verbunden, und zwischen den Switches werden Trunk-Links konfiguriert.



Die Clusterkonfigurationen sind die gleichen wie die anderen Bereitstellungsszenarien. Die meisten clientseitigen Konfigurationen werden auf den clientseitigen Switches durchgeführt.

Beispiel-Cluster-Konfigurationen

May 11, 2023

Das folgende Beispiel kann verwendet werden, um einen Cluster mit vier Knoten mit ECMP, Cluster LA oder Linksets zu konfigurieren.

1. Erstellen Sie den Cluster.
   - Melden Sie sich am ersten Knoten an.
   - Fügen Sie die Clusterinstanz hinzu.

```
1   > add cluster instance 1
```


- Fügen Sie dem Cluster den ersten Knoten hinzu.

```
1   > add cluster node 0 10.102.33.184 -backplane 0/1/1
```

- Aktivieren der Clusterinstanz

```
1   > enable cluster instance 1
```

- Fügen Sie die Cluster-IP-Adresse hinzu.

```
1   > add ns ip 10.102.33.185 255.255.255.255 -type CLIP
```

- Speichern Sie die Konfigurationen.

```
1   > save ns config
```

- Starten Sie die Appliance neu.

```
1   > reboot -warm
```

2. Fügen Sie dem Cluster die anderen drei Knoten hinzu.
   - Melden Sie sich an der Cluster-IP-Adresse an.
   - Fügen Sie dem Cluster den zweiten Knoten hinzu.

```
1   > add cluster node 1 10.102.33.187 -backplane 1/1/1
```

   - Fügen Sie dem Cluster den dritten Knoten hinzu.

```
1   > add cluster node 2 10.102.33.188 -backplane 2/1/1
```

   - Fügen Sie dem Cluster den vierten Knoten hinzu.

```
1   > add cluster node 3 10.102.33.189 -backplane 3/1/1
```

3. Verbinden Sie die hinzugefügten Knoten mit dem Cluster. Dieser Schritt gilt nicht für den ersten Knoten.
   - Melden Sie sich an jedem neu hinzugefügten Knoten an.
   - Verbinden Sie den Knoten mit dem Cluster.

```
1   > join cluster -clip 10.102.33.185 -password nsroot
```

   - Speichern Sie die Konfiguration.

```
1   > save ns config
```


- Starten Sie die Appliance neu.

```
> reboot -warm
```

4. Konfigurieren Sie den NetScaler-Cluster über die Cluster-IP-Adresse.

   // Lastausgleichsfunktion aktivieren

```
> enable ns feature lb
```

   // Hinzufügen eines virtuellen Load Balancing Servers

```
> add lb vserver first_lbvserver http
....
....
```

5. Konfigurieren Sie einen der folgenden Verkehrsverteilungsmechanismen (ECMP, Cluster LA oder Linkset) für den Cluster.

   ECMP

   - Melden Sie sich bei der Cluster-IP-Adresse an.
   - Aktivieren Sie das OSPF-Routingprotokoll.

```
> enable ns feature ospf
```

   - Fügen Sie ein VLANhinzu.

```
> add vlan 97
```

   - Binden Sie die Schnittstellen der Clusterknoten an das VLAN.

```
> bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
```

   - Fügen Sie auf jedem Knoten ein Spotted SNIP hinzu und aktivieren Sie dynamisches Routing darauf.

```
> add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 -
    dynamicRouting ENABLED
> add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 -
    dynamicRouting ENABLED
> add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 -
    dynamicRouting ENABLED
> add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 -
    dynamicRouting ENABLED
```


- Binden Sie eine der SNIP-Adressen an das VLAN.

```
1   > bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
```

- Konfigurieren Sie das Routing-Protokoll auf ZeBOS mit der VTYSH-Shell.

  Statischer Cluster LA

  - Melden Sie sich bei der Cluster-IP-Adresse an.
  - Fügen Sie einen Cluster-LA-Kanal hinzu.

```
1   > add channel CLA/1 -speed 1000
```

  - Binden Sie die Schnittstellen an den Cluster-LA-Kanal.

```
1   > bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
```

  - Führen Sie eine äquivalente Konfiguration auf dem Switch durch

    Dynamischer Cluster LA

    * Melden Sie sich bei der Cluster-IP-Adresse an.
    * Fügen Sie die Schnittstellen zum Cluster-LA-Kanal hinzu.

```
1   > set interface 0/1/5 -lacpmode active -lacpkey 5 -
      lagtype cluster
2   > set interface 1/1/5 -lacpmode active -lacpkey 5 -
      lagtype cluster
3   > set interface 2/1/5 -lacpmode active -lacpkey 5 -
      lagtype cluster
4   > set interface 3/1/5 -lacpmode active -lacpkey 5 -
      lagtype  cluster
```

    * Führen Sie eine äquivalente Konfiguration auf dem Switch durch

    Linksätze. Gehen Sie davon aus, dass der Knoten mit NodeID 3 nicht mit dem Switch verbunden ist. Sie müssen ein Linkset so konfigurieren, dass der nicht verbundene Knoten die anderen Knotenschnittstellen verwenden kann, um mit dem Switch zu kommunizieren.

a) Melden Sie sich bei der Cluster-IP-Adresse an.

b) Fügen Sie einen Linksatz hinzu.

```
1 > add linkset LS/1
```

c) Binden Sie die verbundenen Schnittstellen an das Linkset.


```
> bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
```

6. Aktualisieren Sie den Status der Clusterknoten auf ACTIVE.

```
> set cluster node 0 -state ACTIVE
> set cluster node 1 -state ACTIVE
> set cluster node 2 -state ACTIVE
> set cluster node 3 -state ACTIVE
```

Verwenden von VRRP in einem Cluster-Setup

August 19, 2021

Virtual Router Redundancy Protocol (VRRP) wird in einem Cluster-Setup für IPv4 und IPv6 unterstützt. Die beiden VRRP-Funktionen, die in einem Cluster-Setup unterstützt werden, sind schnittstellenbasiertes VRRP und IP-basiertes VRRP.

IP-basiertes VRRP

In IP-basiertem VRRP werden gestreifte VIP-Adressen, die an dieselbe VRID gebunden sind, auf allen Knoten eines Cluster-Setups konfiguriert. Diese VIP-Adressen sind auf allen Knoten aktiv

Einer der Clusterknoten fungiert als VRID-Besitzer und sendet die VRRP-Ankündigung an andere Knoten. Wenn der VRID-Besitzerknoten fehlschlägt, übernimmt ein anderer Knoten im Cluster den Besitz der VRID und beginnt mit dem Senden von VRRP-Ankündigungen. Sie können auch einen bestimmten Clusterknoten als Besitzer der VRID zuweisen.

> **Hinweis:**
>
> Citrix empfiehlt, die IP-basierte Methode für die VRRP-Bereitstellung im Cluster zu verwenden.

Konfigurieren von IP-basiertem VRRP für IPv4

Führen Sie die folgenden Aufgaben für ein Cluster-Setup zum Konfigurieren von IP-basiertem VRRP für IPv4 aus:

- **Fügen Sie eine VRID hinzu**. Eine VRID ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC-Adresse zu bilden. Die generische VMAC-Adresse hat die Form 00:00:5 e: 00:02: <VRID>.

- **(Optional) Weisen Sie einen Knoten als Besitzer der virtuellen MAC-Adresse**zu. Sie können den Ownernode-Parameter (beim Hinzufügen oder Ändern von VRID6) auf die ID des Clusterknotens festlegen, um ihn als Besitzer der virtuellen MAC-Adresse zuzuweisen. Wenn der zugewiesene Besitzerknoten fehlschlägt, wird einer der UP Clusterknoten dynamisch als Besitzer der virtuellen MAC-Adresse gewählt. Sie können den Besitzerknoten mit dem `set vrID <id> -ownerNode <positive_interger>` Befehl festlegen.
- **Binden Sie die VRID an die VIP-Adresse der Knoten**. Binden Sie die erstellte VRID an die gestreifte VIP-Adresse.

So fügen Sie eine VRID über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add vrid <ID> [-ownerNode <positive_integer>]
2 -  show vrid <ID>
```

So binden Sie die VRID mit der CLI an die VIP-Adresse

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set ns ip <IPv4Address> -vrid <ID><!--NeedCopy-->`
- `show vrid <ID><!--NeedCopy-->`

So fügen Sie eine VRID mit der GUI hinzu

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC** auf **Hinzufügen**.
2. Geben Sie auf der Seite **VMAC** erstellen einen Wert im Feld **Virtual Router ID** an, und klicken Sie dann auf **Erstellen** .

So binden Sie die VRID mit der GUI an eine VIP-Adresse

1. Navigieren Sie zu **System > Netzwerk > IPs**, wählen Sie auf der Registerkarte **IPv4s**eine VIP-Adresse aus und klicken Sie auf **Bearbeiten**.
2. Legen Sie während der Bearbeitung der VIP-Konfiguration den **Virtual Router ID-Parameter** fest.

```
1 > add vrid 90
2  Done
3 > set ns ip 192.0.2.90  - vrid 90
4  Done
```


Konfigurieren von IP-basiertem VRRP für IPv6

Führen Sie die folgenden Aufgaben für ein Cluster-Setup zum Konfigurieren von IP-basiertem VRRP für IPv6 aus:

- **Fügen Sie einen VRID6 hinzu**. Ein VRID6 ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC6-Adresse zu bilden. Die generische VMAC6-Adresse hat die Form 00:00:5 e: 00:02: <VRID6>.
- **(Optional) Weisen Sie einen Knoten als Besitzer der virtuellen MAC6-Adresse**zu. Sie können den Ownernode-Parameter (beim Hinzufügen oder Ändern von VRID6) auf die ID des Clusterknotens festlegen, um ihn als Besitzer der virtuellen MAC6-Adresse zuzuweisen. Wenn der zugewiesene Besitzerknoten fehlschlägt, wird einer der UP Clusterknoten dynamisch als Besitzer der virtuellen MAC6-Adresse gewählt.
- **Binden Sie den VRID6 an die VIP6-Adresse der Knoten**. Binden Sie den erstellten VRID6 an die gestreifte VIP6-Adresse.

So fügen Sie eine VRID6 über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add vrid6 <ID> [-ownerNode <positive_integer>]<!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

So binden Sie die VRID6 mit der CLI an die VIP6-Adresse

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set ns ip6 <IPv6Address> -vrid6 <ID><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

So fügen Sie eine VRID6 mit der GUI hinzu

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC6** auf **Hinzufügen** .
2. Geben Sie auf der Seite **Virtuellen MAC6 erstellen** einen Wert im Feld **Virtual Router ID** an, und klicken Sie dann auf **Erstellen** .

So binden Sie den VRID6 mit der GUI an eine VIP6-Adresse

1. Navigieren Sie zu **System > Netzwerk > IPs**, wählen Sie auf der Registerkarte **IPv6s**eine VIP-Adresse aus und klicken Sie auf **Bearbeiten**.

2. Legen Sie den **Virtual Router ID-Parameter** fest, während Sie die VIP6-Konfiguration bearbeiten.

```
> add vrid6 90
 Done
> set ns ip6 2001:db8::5001  - vrid6 90
 Done
```

Schnittstellenbasiertes VRRP

In der schnittstellenbasierten VRRP-Funktion wird dieselbe virtuelle MAC-Adresse auf beiden Knoten des Clusters konfiguriert. Diese virtuelle MAC-Adresse wird in GARP-Ankündigungen und ARP-Antworten für die auf einem Knoten konfigurierten IP-Adressen verwendet. Diese Funktion ist nützlich in einem Cluster-Setup mit zwei Knoten, das über externe Geräte/Router verfügt, die keine GARP-Ankündigungen akzeptieren.

> **Hinweis:**
>
> Die schnittstellenbasierte VRRP-Funktion ist nur für einen Cluster mit zwei Knoten anwendbar, bei dem ein Knoten im aktiven Zustand und der andere Knoten als Ersatz fungiert.

Bei der gleichen virtuellen MAC-Adresse auf beiden Clusterknoten bleibt die MAC-Adresse für die IP-Adressen auf dem neuen aktiven Knoten unverändert und die ARP-Tabellen auf den externen Geräten/Routern nicht aktualisiert werden müssen.

Konfigurieren von schnittstellenbasiertem VRRP für IPv4

Führen Sie die folgenden Aufgaben für ein Cluster-Setup aus, um schnittstellenbasiertes VRRP für IPv4 zu konfigurieren:

- **Fügen Sie eine VRID hinzu**. Eine VRID ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC-Adresse zu bilden.
- **Binden Sie die VRID an Knotenschnittstellen**. Binden Sie die Schnittstellen an die erstellte VRID. Die gebundenen Schnittstellen (im aktuellen aktiven Knoten) verwenden die virtuelle MAC-Adresse in GARP-Ankündigungen und ARP-Antworten für ihre IPv4-Adressen. Sie müssen die VRID den Schnittstellen beider Knoten des Active-Spare Cluster-Setups zuordnen. Dies liegt daran, dass im Gegensatz zu einer Hochverfügbarkeits-Konfiguration Schnittstellen-IDs in einem Cluster-Setup unterschiedlich sind.

So fügen Sie eine VRID über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
- add vrid <ID>
- show vrid <ID>
```

So binden Sie die VRID über die Befehlszeile an eine Schnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
- bind vrid <ID> -ifnum <interface_name>
- show vrid <ID>
```

So fügen Sie eine VRID hinzu und binden sie mit der GUI an Schnittstellen

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC** auf **Hinzufügen**.
2. Geben Sie auf der Seite **Virtuellen MAC erstellen** einen Wert im Feld **Virtuelle Router-ID*** an, binden Sie Schnittstellen im Abschnitt **Schnittstellen zuordnen**, und klicken Sie dann auf **Erstellen** .

```
> add vrid 300
 Done
> bind vrid 300 -ifnum 1/1/2 2/1/3
 Done
```

Konfigurieren von schnittstellenbasiertem VRRP für IPv6

Führen Sie die folgenden Aufgaben für ein Cluster-Setup aus, um schnittstellenbasiertes VRRP für IPv6 zu konfigurieren:

- **Fügen Sie einen VRID6 hinzu**. Ein VRID6 ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC6-Adresse zu bilden. Die generische VMAC6-Adresse hat die Form 00:00:5 e: 00:01: <VRID6>.
- **Binden Sie die VRID6 an Knotenschnittstellen**. Binden Sie die Schnittstellen an das erstellte VRID6. Die gebundenen Schnittstellen (im aktuellen aktiven Knoten) verwenden die virtuelle MAC6-Adresse in GARP-Ankündigungen und ARP-Antworten für ihre IPv6-Adressen. Sie müssen den VRID6 den Schnittstellen beider Knoten des Active-Spare Cluster-Setups zuordnen. Dies liegt daran, dass im Gegensatz zu einer Hochverfügbarkeits-Konfiguration Schnittstellen-IDs in einem Cluster-Setup unterschiedlich sind.

So fügen Sie eine VRID6 über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add vrid6 <ID>
2 -  show vrid6 <ID>
```

So binden Sie den VRID6 über die Befehlszeile an eine Schnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `bind vrid6 <ID> -ifnum <interface_name><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

So fügen Sie ein VRID6 hinzu und binden es mit der GUI an Schnittstellen

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC6** auf **Hinzufügen** .
2. Geben Sie auf der Seite **Virtuellen MAC6 erstellen** einen Wert im Feld **Virtuelle Router-ID** an, binden Sie Schnittstellen im Abschnitt **Schnittstellen zuordnen**, und klicken Sie dann auf **Erstellen** .

```
1 > add vrid6 100
2  Done
3 > bind vrid6 100 -ifnum 0/1/1 1/1/2 2/1/3
4  Done
```

Überwachen von Diensten in einem Cluster über die Pfadüberwachung

May 11, 2023

In einem Cluster-Setup wird die Eigentümerschaft für die Überwachungsdienste auf die Knoten verteilt. Daher überwachen verschiedene Knoten verschiedene Dienste. Der Knoten, der einen Dienst überwacht, wird als Dienstbesitzer bezeichnet. Nur der Dienstinhaber untersucht den Server, um den Status der ihm zugewiesenen Dienste zu überwachen. Es übermittelt außerdem den Status der Dienste an alle anderen Knoten innerhalb des Clusters. Der Nachteil der verteilten Überwachung besteht darin, dass die Netzwerkkonnektivität und der Verbindungsstatus zwischen allen Knoten und dem Server nicht bestimmt werden. Um diesen Nachteil zu überwinden, können Sie die Pfadüberwachung verwenden.

> **Hinweis**
>
> Sie können keinen Knoten auswählen, um einen Dienst zu überwachen. Die Auswahl der Knoten zur Überwachung eines Dienstes erfolgt über einen internen Mechanismus. Sie können den Eigentümerknoten zur Überwachung von Diensten sehen, indem Sie den Befehl `show service <service name>` und `show serviceGroup <service group name>` verwenden.

Die Pfadüberwachung überprüft die Netzwerkkonnektivität und den Verbindungsstatus zwischen einem Knoten und dem vom Server bereitgestellten Dienst. Ein Knoten sendet ICMP-Pings, um zu überprüfen, ob der Server erreichbar ist oder nicht.

So funktioniert die Pfadüberwachung

Stellen Sie sich ein Beispiel für einen NetScaler-Cluster vor, der aus den drei Knoten N1, N2 und N3 besteht. N2 ist der Dienstinhaber, der den Status der HTTP-Dienste (S1) überwacht. Es kündigt den Dienststatus an andere Knoten im Cluster an. Die Pfadüberwachung ist auf allen Knoten im Cluster für alle Dienste aktiviert. Jeder Knoten sendet nur einen ICMP-Ping an den Server. Der Dienstbesitzer sendet sowohl die HTTP-Dienstanforderung als auch einen ICMP-Ping. Jeder Knoten meldet seinen Status zur Pfadüberwachung an den Dienstinhaber.



Die folgenden zwei Parameter bestimmen den Dienststatus eines Knotens:

- S = vom Serviceinhaber ausgeschriebener Dienststatus
- P = Pfadüberwachungsstatus jedes Knotens

Ob ein Knoten einen Server erreichen kann oder nicht, bestimmt den Status der Pfadüberwachung für diesen Knoten.

Die folgende Tabelle zeigt den Dienststatus, der auf der Grundlage des Pfadüberwachungsstatus festgelegt wird, wenn der PathMonitorInDV-Parameter aktiviert oder deaktiviert ist.

Parameter	Status der Pfadüberwachung	Status des Dienstes
PathMonitorinDV = NEIN; Ist die Standardkonfiguration.	P1 = RUNTER	S1 = RUNTER
	P2 = HOCH	S1 = RUNTER
	P3 = HOCH	S1 = RUNTER
PathMonitorInDV = JA	P1 = RUNTER	S1 = RUNTER
	P2 = HOCH	S1 = HOCH
	P3 = HOCH	S1 = HOCH

In diesem Beispiel bestimmt der Dienstbesitzer den Dienststatus für alle Knoten auf der Grundlage des Knotens, dessen Pfadüberwachungsstatus auf DOWN gesetzt ist. Wenn der Pfadüberwachungsstatus für einen der Knoten DOWN ist, legt der Dienstbesitzer den Dienststatus für alle Knoten auf DOWN fest. Der Dienststatus für alle Knoten ist nur dann auf UP gesetzt, wenn der Pfadüberwachungsstatus für jeden Knoten UP ist.

Sie können die Pfadüberwachung für einzelne Knoten verwenden, indem Sie den Parameter PathMonitorInDV aktivieren. Dieser Parameter ermöglicht es dem Dienstbesitzer, den Dienststatus für jeden Knoten auf der Grundlage des Pfadüberwachungsstatus des jeweiligen Knotens festzulegen.

> **Hinweis**
>
> Wenn der PathMonitorInDV-Parameter gesetzt ist, können einige Funktionen wie die Persistenz nicht funktionieren.

Konfiguration der Pfadüberwachung

Die Pfadüberwachung ist für alle Dienste und Dienstgruppen anwendbar. Der Pfadüberwachungsparameter ist standardmäßig deaktiviert.

So aktivieren Sie die Pfadüberwachung für Dienste/Dienstgruppen mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <service name> <IP address> <service type> <port> [-pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]

add servicegroup <servicegroup name> <service type> [-pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Beispiel:

```
add service s1 1.1.1.1 HTTP 80 -pathMonitor YES
add servicegroup sg_1 HTTP -pathMonitor YES

add service s1 1.1.1.1 HTTP 80 -pathMonitor YES -pathMonitorIndv YES
add servicegroup sg_1 HTTP -pathMonitor YES -pathMonitorIndv YES
<!--NeedCopy-->
```

Sie können den Parameter zur Pfadüberwachung auch über den Befehl set wie folgt festlegen:

```
set service <service name> [-pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]
set servicegroup <servicegroup name> [-pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Beispiel:

```
set service s1 -pathMonitor YES
set servicegroup sg_1 -pathMonitor YES


set service s1 -pathMonitorIndv YES
set servicegroup sg_1 -pathMonitorIndv NO
<!--NeedCopy-->
```

Um die Pfadüberwachung für Dienste/Dienstgruppen mithilfe der GUI zu aktivieren

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.

   Navigieren Sie für Dienstgruppen zu **Traffic Management** > **Load Balancing** > **Service Groups**.

2. Wählen Sie im Bereich **Dienste/Dienstgruppen** einen Service/Dienstgruppe aus der Liste aus, und doppelklicken Sie dann, um ihn zu öffnen.

3. Klicken Sie auf der Registerkarte **Diensteinstellungen** auf **Bearbeiten**.
4. Wählen Sie **Path Monitoring**aus.
5. Wählen Sie **Individual Path Monitoring**, wenn Sie es anwenden möchten, und klicken Sie dann auf **OK**.

> **Hinweis**
>
> Sie können die Überwachung einzelner Pfade nur aktivieren, wenn Sie die Pfadüberwachung aktivieren.

Backup und Wiederherstellen des Clustersetups

May 11, 2023

Sie können den aktuellen Status eines NetScaler-Clusterknotens sichern. Später können Sie die gesicherten Dateien verwenden, um den Knoten auf denselben Clusterstatus zurückzusetzen. Als Vorsichtsmaßnahme müssen Sie diese Funktion verwenden, bevor Sie ein Upgrade auf den Clusterknoten durchführen.

Ein Cluster-Setup sichern

Sie können je nach den folgenden Bedingungen ein einfaches oder ein vollständiges Backup erstellen:

- Art der zu sichernden Daten.
- Häufigkeit, mit der Sie ein Backup erstellen.
- **Grundlegendes Backup.** Sichert nur Konfigurationsdateien. Möglicherweise möchten Sie diese Art der Backup häufig durchführen, da sich die gesicherten Dateien ständig ändern. Die gesicherten Dateien sind in der Tabelle aufgeführt.

Verzeichnis

Unterverzeichnis oder Dateien

/nsconfig/

- ns.conf
- Zebos.conf
- rc.netscaler
- snmpd.conf
- nsbefore.sh
- nsafter.sh
- inetd.conf

- ntp.conf
- syslog.conf
- newsyslog.conf
- crontab
- host.conf
- Gastgeber
- ttys
- sshd_config
- httpd.conf
- überwachen
- rc.conf
- ssh_config
- lokale Zeit
- Ausgabe
- issue.net

/var/

- herunterladen/*
- log/wicmd.log
- mit /tomcat/webapps/*
- wi/tomcat/logs/*
- wi/tomcat/conf/catalina/localhost/*
- nslw.bin/etc/krb.conf
- nslw.bin/etc/krb.keytab
- netscaler/locdb/*
- lib/likewise/db/*
- vpn/bookmark/*
- netscaler/crl
- Vorlagen/*
- Lerndaten/*

/netscaler/

- custom.html
- vsr.html
- **Vollständige Unterstützung.** Abgesehen von den Dateien, die durch ein einfaches Backup gesichert werden, sichert ein vollständiges Backup einige weniger häufig aktualisierte Dateien. Die Dateien, die bei Verwendung der vollständigen Sicherungsoption gesichert werden, sind in der Tabelle aufgeführt.

Verzeichnis

Unterverzeichnis oder Dateien

/nsconfig/

- ssl/*
- Lizenz/*
- Tipps/*

/var/

- netscaler/ssl/*
- wi/java_home/jre/lib/security/cacerts/*
- wi/java_home/lib/security/cacerts/*

> **Wichtig**
>
> Die Backup und Wiederherstellung funktionieren nicht, wenn CLAG in einem SDX-Cluster-Setup konfiguriert ist.

Das Backup wird als komprimierte TAR-Datei im Verzeichnis /var/ns_sys_backup/ gespeichert. Um Probleme zu vermeiden, die dadurch entstehen, dass kein Speicherplatz verfügbar ist, können Sie in diesem Verzeichnis maximal 50 Sicherungsdateien speichern. Sie können den Befehl rm system backup verwenden, um vorhandene Sicherungsdateien zu löschen, sodass Sie weitere Backups erstellen können.

Wenn Sie den Sicherungsvorgang auf einem CLIP eines Cluster-Setups ausführen, werden Sicherungsdateien auf jedem Clusterknoten erstellt.

So sichern Sie ein Cluster-Setup

Um das Cluster-Setup auf CLIP mithilfe der NetScaler-CLI zu sichern.

Führen Sie an der Eingabeaufforderung Folgendes aus:

- Speichern Sie die Konfiguration.

  ```
  save ns config<!--NeedCopy-->
  ```

- Erstellen Sie die Sicherungsdatei (einfach oder vollständig).

  “‘create system backup [][–level (basic | full)][-comment]

  ```
  **Beispiel**

  ```create system backup cluster-backup-1  -level basic<!--
     NeedCopy-->
  ```

Der vorherige Befehl erstellt auf jedem Clusterknoten eine Backup-TAR-Datei mit dem angegebenen Dateinamen. Beispielsweise wird die Datei Cluster-Backup-1.tgz auf jedem Clusterknoten erstellt.


  ```

> **Hinweis**
>
> Wenn der Dateiname nicht angegeben ist, werden Backup-TAR-Dateien auf jedem Clusterknoten mit der folgenden Namenskonvention erstellt:
>
> - `backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp>.tgz<!--NeedCopy-->`
> - `backup_<level>_<nsip_address of the cluster node 1>_<date-timestamp>.tgz<!--NeedCopy-->`
>
> Beispielsweise bei einem Cluster-Setup mit drei Knoten
>
> - `backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp>.tgz<!--NeedCopy-->` wird auf node0 erstellt
> - `backup _<level>_<nsip_address of the cluster node 1>_<date-timestamp>.tgz<!--NeedCopy-->` wird auf Node1 erstellt
> - `backup_<level>_<nsip_address of the cluster node 2>_<date-timestamp>.tgz<!--NeedCopy-->` wird auf Node2 erstellt

- Überprüfen Sie die erstellten Sicherungsdateien auf CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```

Ein Cluster-Setup wiederherstellen

Wenn ein Clusterknoten fehlerhaft wird, können Sie diesen Knoten durch einen neuen Knoten ersetzen. Sie können den neuen Knoten für einen Cluster einrichten, indem Sie eine Sicherungsdatei des fehlerhaften Knotens verwenden.

Wenn beispielsweise in einem Cluster-Setup mit drei Knoten Node1 fehlerhaft wird, können Sie diesen fehlerhaften Knoten durch einen neuen Knoten als Node1 ersetzen. Mit dem Wiederherstellungsvorgang können Sie eine der Sicherungsdateien des fehlerhaften Knotens auf dem neuen Knoten wiederherstellen.

> **Hinweis**
>
> Der Wiederherstellungsvorgang ist nicht erfolgreich, wenn die Sicherungsdatei umbenannt wird oder wenn der Inhalt der Datei geändert wird.

So stellen Sie einen Clusterknoten wieder her

So stellen Sie einen Clusterknoten mithilfe der CLI wieder her

Führen Sie an der Eingabeaufforderung Folgendes aus:

- Besorgen Sie sich eine Liste der auf CLIP verfügbaren Sicherungsdateien.


```
show system backup<!--NeedCopy-->
```

- Kopieren Sie die Backup-TAR-Datei in das Verzeichnis /var/ns_sys_backup des Clusterknotens, der wiederhergestellt werden soll.
- Fügen Sie die Backup-TAR-Datei zum Clusterknotenspeicher hinzu, indem Sie den folgenden Befehl auf dem Clusterknoten ausführen.

  “‘add system backup

  ```
  **Beispiel**

  ```add system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
  ```

  > **Hinweis**
  >
  > Der Befehl muss auf dem Clusterknoten ausgeführt werden, der wiederhergestellt werden soll.

- Stellen Sie den Clusterknoten wieder her, indem Sie die Sicherungsdatei angeben.

  “‘restore system backup

  ```
  **Beispiel**

  ```restore system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
  ```

  > **Hinweis**
  >
  > Der Befehl muss auf dem Clusterknoten ausgeführt werden, der wiederhergestellt werden soll.

- Starten Sie den Clusterknoten neu.

  reboot

  > **Hinweis**
  >
  > Der Befehl muss auf dem Clusterknoten ausgeführt werden, der wiederhergestellt werden soll.

Upgrade oder Downgrade des NetScaler-Clusters

May 11, 2023

Auf allen Knoten eines NetScaler-Clusters muss dieselbe Softwareversion ausgeführt werden. Um den Cluster zu aktualisieren oder herunterzustufen, müssen Sie daher jede NetScaler-Appliance des Clusters, jeweils einen Knoten nach dem anderen, aktualisieren oder downgraden.

Ein Knoten, der gerade aktualisiert oder heruntergestuft wird, wird nicht aus dem Cluster entfernt. Der Knoten bleibt Teil des Clusters und dient ununterbrochen dem Datenverkehr, mit Ausnahme der Ausfallzeit, wenn der Knoten nach dem Upgrade oder Downgrade neu gestartet wird.

Aufgrund einer Nichtübereinstimmung der Softwareversionen zwischen den Clusterknoten ist die Konfigurationspropagierung auf dem Cluster jedoch deaktiviert. Die Konfigurationspropagierung wird erst aktiviert, wenn alle Clusterknoten dieselbe Version aufweisen. Da die Konfigurationspropagierung während des Upgrades beim Downgrade eines Clusters deaktiviert ist, können Sie während dieser Zeit keine Konfigurationen über die Cluster-IP-Adresse durchführen.

Wichtig

- In einem Cluster-Setup mit maximaler Verbindung (MaxConn), der auf einen Wert ungleich Null festgelegt ist, schlagen CLIP-Verbindungen möglicherweise fehl, wenn eine der folgenden Bedingungen erfüllt ist:

```
- Upgrading the setup from NetScaler 13.0 76.x build to
  NetScaler 13.0 79.x build.
- Restarting the CCO node in a cluster setup running NetScaler
   13.0 76.x build.
```

  Problemumgehungen:

```
\- Vor dem Upgrade eines Cluster-Setups von NetScaler 13.0 76.
   x Build auf NetScaler 13.0 79.x Build muss der globale
   Parameter der maximalen Verbindung (MaxConn) auf Null
   gesetzt werden. Nach dem Upgrade des Setups können Sie den
   MaxConn-Parameter auf einen gewünschten Wert setzen und dann
    die Konfiguration speichern.
\- NetScaler 13.0 76.x Build ist nicht für Cluster-Setups
   geeignet. Citrix empfiehlt, den NetScaler 13.0 76.x Build
   nicht für ein Cluster-Setup zu verwenden.
```

- In einem Cluster-Setup stürzt eine NetScaler-Appliance möglicherweise ab, wenn:

```
- upgrading the setup from NetScaler 13.0 47.x or 13.0 52.x
  build to a later build, or
- upgrading the setup to NetScaler 13.0 47.x or 13.0 52.x
  build
```

  Problemumgehung: Führen Sie während des Upgrade-Vorgangs die folgenden Schritte aus:

```
\- Deaktivieren Sie alle Clusterknoten und aktualisieren Sie
   dann jeden Clusterknoten.
```



```
2 \-  Aktivieren Sie alle Clusterknoten, nachdem alle Knoten
      aktualisiert wurden.
```

Punkte, die vor dem Upgrade oder Herabstufen des Clusters zu beachten sind

- **WICHTIG:**

  Es ist wichtig, dass sowohl die Upgrade-Änderungen als auch Ihre Anpassungen auf eine aktualisierte NetScaler-Appliance angewendet werden. Wenn Sie benutzerdefinierte Konfigurationsdateien im Verzeichnis `/etc` haben, lesen Sie Überlegungen zum Upgrade für benutzerdefinierte Konfigurationsdateien, bevor Sie mit dem Upgrade fortfahren.

- Beim Upgrade oder Downgrade der Cluster-Softwareversion können keine Clusterknoten hinzugefügt werden.
- Sie können Konfigurationen auf Knotenebene über die NSIP-Adresse einzelner Knoten durchführen. Stellen Sie sicher, dass Sie auf allen Knoten die gleichen Konfigurationen ausführen, um sie synchron zu halten.
- Sie können den Befehl `start nstrace` nicht über die Cluster-IP-Adresse ausführen, wenn der Cluster aktualisiert wird. Sie können jedoch die Spur einzelner Knoten abrufen, indem Sie diesen Vorgang auf einzelnen Clusterknoten mit ihrer NSIP-Adresse ausführen.
- NetScaler 13.0 76.x Build ist nicht für Cluster-Setups geeignet. Citrix empfiehlt, den NetScaler 13.0 76.x Build nicht für ein Cluster-Setup zu verwenden.
- NetScaler 13.0 47.x- und 13.0 52.x-Builds sind nicht für ein Cluster-Setup geeignet. Dies liegt daran, dass die Kommunikation zwischen den Knoten in diesen Builds nicht kompatibel ist.
- Wenn ein Cluster aktualisiert wird, ist es möglich, dass auf den aktualisierten Knoten einige zusätzliche Funktionen aktiviert sind, die auf den noch nicht aktualisierten Knoten nicht verfügbar sind. Dies führt zu einer Warnung wegen Lizenzfehlanpassung, während der Cluster aktualisiert wird. Diese Warnung wird automatisch behoben, wenn alle Clusterknoten aktualisiert werden.

Wichtig

- Citrix empfiehlt, dass Sie warten, bis der vorherige Knoten aktiv ist, bevor Sie den nächsten Knoten aktualisieren oder herunterstufen.
- Citrix empfiehlt, dass der Clusterkonfigurationsknoten zuletzt aktualisiert/heruntergestuft werden muss, um mehrfache Unterbrechungen von Cluster-IP-Sitzungen zu vermeiden.

So aktualisieren oder downgraden Sie die Software der Clusterknoten

1. Stellen Sie sicher, dass der Cluster stabil ist und die Konfigurationen auf allen Knoten synchronisiert sind.
2. Greifen Sie über seine NSIP-Adresse auf jeden Knoten zu und führen Sie Folgendes aus:
   - Aktualisieren oder Herabstufen des Clusterknotens. Detaillierte Informationen zum Upgrade und Downgrade der Software einer Appliance finden Sie unter Upgrade und Downgrade einer NetScaler-Appliance.
   - Speichern Sie die Konfigurationen.
   - Starten Sie die Appliance neu.
3. Wiederholen Sie Schritt 2 für jeden der anderen Clusterknoten.

Auf einzelnen Clusterknoten unterstützte Vorgänge

May 11, 2023

In der Regel können NetScaler-Appliances, die Teil eines Clusters sind, nicht einzeln von ihrer NSIP-Adresse aus konfiguriert werden. Es gibt jedoch einige Operationen, die eine Ausnahme von dieser Regel darstellen. Wenn diese Operationen von der NSIP-Adresse aus ausgeführt werden, werden sie nicht an andere Clusterknoten weitergegeben.

Die Operationen sind:

- Clusterinstanz (setzen | rm | aktivieren | deaktivieren)
- Clusterknoten (gesetzt | rm)
- ns trace (starten | anzeigen | beenden)
- Schnittstelle (einstellen | aktivieren | deaktivieren)
- Route (hinzufügen | rm | setzen | löschen)
- ARP (hinzufügen | rm | senden -alles)
- Clustersynchronisierung erzwingen
- Clusterdateien synchronisieren
- NTP-Sync deaktivieren
- Speichern Sie ns Config
- reboot
- Abschaltung

Wenn Sie den Befehl beispielsweise `disable interface 1/1/1` von der NSIP-Adresse eines Clusterknotens aus ausführen, ist die Schnittstelle nur auf diesem Knoten deaktiviert. Da der Befehl nicht weitergegeben wird, bleibt die Schnittstelle 1/1/1 auf allen anderen Clusterknoten aktiviert.

Unterstützung für heterogene Cluster

May 11, 2023

Die NetScaler Appliance unterstützt einen heterogenen Cluster in einer Cluster-Bereitstellung. Ein heterogener Cluster umfasst Knoten mit unterschiedlicher NetScaler-Hardware, und Sie können eine Kombination verschiedener Plattformen im selben Cluster verwenden.

> **Wichtig**
>
> Die Bildung oder Unterstützbarkeit eines heterogenen Clusters ist möglich und nur auf MPX-Hardwareplattformen beschränkt.

Die Unterstützbarkeit und Bildung des heterogenen Clusters hängen von bestimmten NetScaler-Modellen ab. In der folgenden Tabelle sind die Plattformen aufgeführt, die bei der Bildung eines heterogenen Clusters mit der gleichen Anzahl von Paket-Engines unterstützt werden.

Anzahl der Paket-Engines	MPX-Hardwareplattformen	Unterstützte MPX-Hardwareplattformen zur Bildung eines heterogenen Clusters
5	MPX 11500	MPX 14020
7	MPX 11515	MPX 14040
9	MPX 11530	MPX 14060

In der folgenden Tabelle sind die Plattformen aufgeführt, die bei der Bildung eines heterogenen Clusters mit einer ungleichen Anzahl von Paket-Engines unterstützt werden.

Hardware-Plattformen	Unterstützte Hardwareplattformen zur Bildung eines heterogenen Clusters
MPX 150XX	MPX 140XX

Weitere Informationen zur Bildung einer heterogenen Clusterbereitstellung von NetScaler MPX-Appliances mit der unterschiedlichen Anzahl von Paket-Engines über verschiedene SSL-Chipsätze hinweg finden Sie im Abschnitt **Heterogene Clusterbereitstellungen** in der SSL-Offload-Konfiguration.

> **Hinweis**
>
> Vor Release 13.0 Build 47.x wird die folgende Fehlermeldung angezeigt, wenn Sie den Befehl "Cluster verbinden" von dem Knoten aus ausführen, der eine ungleiche Anzahl von Paket-Engines aufweist: "Nichtübereinstimmung der Anzahl aktiver PPEs zwischen CCO und lokalem Knoten".

Wichtige Hinweise

1. Die zusätzliche Management-CPU-Einstellung muss auf allen Clusterknoten identisch sein.
2. Der neu hinzugefügte Knoten muss auf den Datenebenen und der Backplane dieselbe Kapazität haben wie die vorhandenen Clusterknoten.
3. Wenn gemischte Plattformgeräte vorhanden sind, die verschiedene Chiffre unterstützen, würde sich der Cluster auf eine gemeinsame Chiffre Liste einigen.

FAQ

May 11, 2023

Eine Liste der häufig gestellten Fragen zum Clustering.

Wie viele NetScaler-Appliances können in einem einzigen NetScaler-Cluster enthalten sein?

Ein NetScaler-Cluster kann eine Appliance oder bis zu 32 NetScaler nCore Hardware oder virtuelle Appliances enthalten. Jeder dieser Knoten muss die unter Voraussetzungen für Clusterknotenangegebenen Kriterien erfüllen.

Kann eine NetScaler-Appliance Teil mehrerer Cluster sein?

Nein. Eine NetScaler Appliance kann nur zu einem Cluster gehören.

Was ist eine Cluster-IP-Adresse? Was ist seine Subnetzmaske?

Die Cluster-IP-Adresse ist die Verwaltungsadresse eines NetScaler-Clusters. Alle Clusterkonfigurationen müssen durchgeführt werden, indem über diese Adresse auf den Cluster zugegriffen wird. Die Subnetzmaske der Cluster-IP-Adresse ist auf 255.255.255.255 festgelegt.

Wie kann ich einen bestimmten Clusterknoten als Clusterkonfigurationskoordinator erstellen?

Um einen bestimmten Knoten manuell als Clusterkonfigurationskoordinator festzulegen, müssen Sie die Priorität dieses Knotens auf den niedrigsten numerischen Wert (höchste Priorität) setzen. Um das zu verstehen, betrachten wir einen Cluster mit drei Knoten, die die folgenden Prioritäten haben:

n1 - 29, n2 - 30, n3 - 31

Hier ist n1 der Konfigurationskoordinator. Wenn Sie n2 zum Konfigurationskoordinator machen möchten, müssen Sie seine Priorität auf einen Wert setzen, der niedriger als n1 ist, z. B. 28. Beim Speichern der Konfiguration wird n2 zum Konfigurationskoordinator.

> **Hinweis**
>
> n2 mit seinem ursprünglichen Prioritätswert von 30 wird zum Konfigurationskoordinator, wenn n1 ausfällt. Der Knoten mit dem nächstniedrigsten Prioritätswert wird ausgewählt, falls der Konfigurationskoordinator ausfällt.

Warum werden die Netzwerkschnittstellen eines Clusters in der 3-Tupel-Notation (n/u/c) statt in der regulären 2-Tupel-Notation (u/c) dargestellt?

Wenn eine NetScaler Appliance Teil eines Clusters ist, müssen Sie in der Lage sein, den Knoten zu identifizieren, zu dem die Schnittstelle gehört. Daher wurde die Namenskonvention für Netzwerkschnittstellen für Clusterknoten von u/c auf n/u/c geändert, wobei n die Knoten-ID bezeichnet.

Wie kann ich den Hostnamen für einen Clusterknoten festlegen?

Der Hostname eines Clusterknotens muss angegeben werden, indem der Befehl **set ns hostname** über die Cluster-IP-Adresse ausgeführt wird. Um beispielsweise den Hostnamen des Clusterknotens mit der ID 2 festzulegen, lautet der Befehl:

set ns hostname hostName1 -**ownerNode** 2

Kann ich NetScaler-Appliances automatisch erkennen, damit ich sie einem Cluster hinzufügen kann?

Ja. Mit dem Konfigurationsdienstprogramm können Sie Appliances ermitteln, die sich im selben Subnetz wie die NSIP-Adresse des Konfigurationskoordinators befinden. Weitere Informationen finden Sie unter Discovering NetScaler Appliances.

Ist die Traffic Serving-Funktion eines Clusters betroffen, wenn ein Knoten entfernt oder deaktiviert wird, neu gestartet oder heruntergefahren oder inaktiv gemacht wird?

Ja. Wenn einer dieser Vorgänge auf einem aktiven Knoten des Clusters ausgeführt wird, verfügt der Cluster über einen Knoten weniger, der den Datenverkehr abwickelt. Außerdem werden bestehende Verbindungen auf diesem Knoten beendet.

Ich habe mehrere eigenständige Appliances, von denen jede unterschiedliche Konfigurationen hat. Kann ich sie zu einem einzelnen Cluster hinzufügen?

Ja. Sie können Appliances mit unterschiedlichen Konfigurationen zu einem einzelnen Cluster hinzufügen. Wenn die Appliance jedoch zum Cluster hinzugefügt wird, werden die vorhandenen Konfigurationen gelöscht. Um die Konfigurationen zu verwenden, die auf den einzelnen Appliances verfügbar sind, müssen Sie:

1. Erstellen Sie eine einzige *.conf-Datei für alle Konfigurationen.
2. Bearbeiten Sie die Konfigurationsdatei, um Funktionen zu entfernen, die in einer Clusterumgebung nicht unterstützt werden.
3. Aktualisieren Sie die Benennungskonvention von Schnittstellen vom 2-Tupel-Format (u/c) auf das 3-Tupel-Format (n/u/c).
4. Wenden Sie die Konfigurationen mithilfe des Batch-Befehls auf den Konfigurationskoordinatorknoten des Clusters an.

Kann ich die Konfigurationen einer eigenständigen NetScaler-Appliance oder eines HA-Setups zum Cluster-Setup migrieren?

Nein. Wenn ein Knoten zu einem Cluster-Setup hinzugefügt wird, werden seine Konfigurationen implizit gelöscht, indem der Befehl **clear ns config** (mit der **erweiterten** Option) verwendet wird. Darüber hinaus werden die SNIP-Adressen und alle VLAN-Konfigurationen (außer Standard-VLAN und NSVLAN) gelöscht. Daher wird empfohlen, die Konfigurationen zu sichern, bevor Sie die Appliance zu einem Cluster hinzufügen. Bevor Sie die gesicherte Konfigurationsdatei für den Cluster verwenden, müssen Sie:

1. Bearbeiten Sie die Konfigurationsdatei, um Funktionen zu entfernen, die in einer Clusterumgebung nicht unterstützt werden.
2. Aktualisieren Sie die Benennungskonvention von Schnittstellen vom Format mit zwei Tupeln (x/y) auf das Format mit drei Tupeln (x/y/z).
3. Wenden Sie die Konfigurationen mithilfe des **Batch-Befehls** auf den Konfigurationskoordinatorknoten des Clusters an.

Sind Backplane-Schnittstellen Teil der L3-VLANs?

Ja, Backplane-Schnittstellen sind standardmäßig in allen L3-VLANs vorhanden, die im Cluster konfiguriert sind.

Wie kann ich einen Cluster konfigurieren, der Knoten aus verschiedenen Netzwerken enthält?

> **Hinweis**
>
> Wird ab NetScaler 11.0 unterstützt.

Ein Cluster, der Knoten aus verschiedenen Netzwerken enthält, wird als L3-Cluster bezeichnet (im INC-Modus manchmal als Cluster bezeichnet). In einem L3-Cluster müssen alle Knoten, die zu einem einzelnen Netzwerk gehören, in einer einzigen Knotengruppe gruppiert werden. Wenn ein Cluster aus jeweils zwei Knoten aus drei verschiedenen Netzwerken besteht, müssen Sie daher 3 Knotengruppen erstellen (eine für jedes Netzwerk) und jede dieser Knotengruppen den Knoten zuordnen, die zu diesem Netzwerk gehören. Informationen zur Konfiguration finden Sie in den Schritten zum Einrichten eines Clusters.

Wie kann ich das NSVLAN in einem Cluster konfigurieren/dekonfigurieren?

Führen Sie einen der folgenden Schritte aus:

- Um das NSVLAN in einem Cluster verfügbar zu machen, stellen Sie sicher, dass für jede Appliance dasselbe NSVLAN konfiguriert ist, bevor es zu einem Cluster hinzugefügt wird.
- Um das NSVLAN von einem Clusterknoten zu entfernen, entfernen Sie zuerst den Knoten aus dem Cluster und löschen Sie dann das NSVLAN aus der Appliance.

Ich habe einen Cluster eingerichtet, in dem einige NetScaler-Knoten nicht mit dem externen Netzwerk verbunden sind. Kann der Cluster immer noch normal funktionieren?

Ja. Der Cluster unterstützt einen Mechanismus namens Linksets, der es nicht verbundenen Knoten ermöglicht, Datenverkehr mithilfe der Schnittstellen verbundener Knoten zu verwalten. Die nicht verbundenen Knoten kommunizieren über die Cluster-Backplane mit den verbundenen Knoten. Weitere Informationen finden Sie unter Verwenden von Linksets.

Wie können Bereitstellungen, die eine MAC-basierte Weiterleitung (MBF) erfordern, in einem Cluster-Setup unterstützt werden?

Bereitstellungen, die MBF verwenden, müssen Linksets verwenden. Weitere Informationen finden Sie unter Verwenden von Linksets.

Kann ich Befehle von der NSIP-Adresse eines Cluster-Knotens ausführen?

Nein. Der Zugriff auf einzelne Clusterknoten über die NSIP-Adressen ist schreibgeschützt. Wenn Sie sich an der NSIP-Adresse eines Clusterknotens anmelden, können Sie daher nur die Konfigurationen und die Statistiken anzeigen. Sie können nichts konfigurieren. Es gibt jedoch einige Vorgänge, die Sie von der NSIP-Adresse eines Clusterknotens ausführen können. Weitere Informationen finden Sie unter Auf einzelnen Knoten unterstützte Vorgänge.

Kann ich die Konfigurationsverbreitung zwischen Clusterknoten deaktivieren?

Nein, Sie können die Weitergabe von Clusterkonfigurationen zwischen Clusterknoten nicht explizit deaktivieren. Während eines Software-Upgrades oder -Downgrades kann ein Versionskonflikt jedoch automatisch dazu führen, dass die Konfiguration nicht übereinstimmt.

Kann ich die NSIP-Adresse oder das NSVLAN einer NetScaler Appliance ändern, wenn sie Teil des Clusters ist?

Nein. Um solche Änderungen vorzunehmen, müssen Sie zuerst die Appliance aus dem Cluster entfernen, die Änderungen vornehmen und dann die Appliance dem Cluster hinzufügen.

Unterstützt der NetScaler-Cluster L2- und L3-VLANs?

Ja. Ein Cluster unterstützt VLANs zwischen Clusterknoten. Die VLANs müssen auf der Cluster-IP-Adresse konfiguriert werden.

- **L2-VLAN.** Sie können ein Layer2-VLAN erstellen, indem Sie Schnittstellen binden, die zu verschiedenen Knoten des Clusters gehören.
- **L3-VLAN.** Sie können ein Layer3-VLAN erstellen, indem Sie IP-Adressen binden, die zu verschiedenen Knoten des Clusters gehören. Die IP-Adressen müssen zu demselben Subnetz gehören. Stellen Sie sicher, dass eines der folgenden Kriterien erfüllt ist. Andernfalls können die L3-VLAN-Bindungen fehlschlagen.
  - Alle Knoten haben eine IP-Adresse im selben Subnetz wie das, das an das VLAN gebunden ist.
  - Der Cluster hat eine Striped-IP-Adresse und das Subnetz dieser IP-Adresse ist an das VLAN gebunden.

Wenn Sie einen Knoten zu einem Cluster hinzufügen, der nur über gescannte IPs verfügt, erfolgt die Synchronisierung, bevor diesem Knoten gescannte IP-Adressen zugewiesen werden. In solchen Fällen können L3-VLAN-Bindungen verloren gehen. Um diesen Verlust zu vermeiden, fügen Sie entweder eine Striped IP hinzu oder fügen Sie die L3-VLAN-Bindungen auf dem NSIP des neu hinzugefügten Knotens hinzu.

Wie kann ich SNMP auf einem NetScaler-Cluster konfigurieren?

SNMP überwacht den Cluster und alle Knoten des Clusters auf die gleiche Weise wie eine eigenständige Appliance. Der einzige Unterschied besteht darin, dass SNMP auf einem Cluster über die Cluster-IP-Adresse konfiguriert werden muss. Bei der Generierung hardwarespezifischer Traps sind zwei weitere Varbinds enthalten, um den Knoten des Clusters zu identifizieren: Knoten-ID und NSIP-Adresse des Knotens.

Welche Details muss ich zur Verfügung haben, wenn ich mich bei Clusterproblemen an den technischen Support wende?

Die NetScaler Appliance bietet einen **Clusterbefehl show techsupport -scope**, der Konfigurationsdaten, statistische Informationen und Protokolle aller Clusterknoten extrahiert. Führen Sie diesen Befehl für die Cluster-IP-Adresse aus.

Die Ausgabe dieses Befehls wird in einer Datei mit dem Namen *collector_cluster_ _P_ .tar.gz* <nsip_CCO><date-timestamp>gespeichert, die im Verzeichnis */var/tmp/support/cluster/* des Konfigurationskoordinators verfügbar ist.

Senden Sie dieses Archiv an den technischen Support, um das Problem zu beheben.

Kann ich Striped IP-Adressen als Standard-Gateway für Server verwenden?

Stellen Sie bei Cluster-Bereitstellungen sicher, dass das Standard-Gateway des Servers auf eine Striped-IP-Adresse verweist (wenn Sie eine NetScaler-eigene IP-Adresse verwenden). Bei LB-Bereitstellungen mit aktiviertem USIP muss das Standard-Gateway beispielsweise eine Striped SNIP-Adresse sein.

Kann ich die Routing-Konfigurationen eines bestimmten Clusterknotens von der Cluster-IP-Adresse aus anzeigen?

Ja. Sie können die für einen Knoten spezifischen Konfigurationen anzeigen und löschen, indem Sie beim Aufrufen der VTYSH-Shell den Eigentümerknoten angeben.

Um beispielsweise die Ausgabe eines Befehls auf den Knoten 0 und 1 anzuzeigen, lautet der Befehl wie folgt:

```
\> vtysh
ns# owner-node 0 1
ns(node-0 1)\# show cluster state
ns(node-0 1)\# exit-cluster-node
ns\#
```


Wie kann ich den Knoten angeben, für den ich die LACP-Systempriorität festlegen möchte?

> **Hinweis**
>
> Wird ab NetScaler 10.1 unterstützt.

In einem Cluster müssen Sie diesen Knoten mithilfe des Befehls **set lacp als Eigentümerknoten festlegen** .

Zum Beispiel: Um die LACP-Systempriorität für einen Knoten mit der ID 2 festzulegen:

```
set lacp -sysPriority 5 -ownerNode 2<!--NeedCopy-->
```

Wie werden IP-Tunnel in einem Cluster-Setup konfiguriert?

> **Hinweis**
>
> Wird ab NetScaler 10.1 unterstützt.

Die Konfiguration von IP-Tunneln in einem Cluster entspricht der Konfiguration auf einer eigenständigen Appliance. Der einzige Unterschied besteht darin, dass in einem Cluster-Setup die lokale IP-Adresse eine Striped SNIP-Adresse sein muss.

Wie kann ich einen Failover-Schnittstellensatz (FIS) auf den Knoten eines NetScaler-Clusters hinzufügen?

> **Hinweis**
>
> Wird ab NetScaler 10.5 unterstützt.

Geben Sie auf der Cluster-IP-Adresse die ID des Clusterknotens an, auf dem der FIS hinzugefügt werden muss. Verwenden Sie dazu den folgenden Befehl:

```
add fis <name> -ownerNode <nodeId>
```

> **Hinweise**
>
> - Der FIS-Name für jeden Clusterknoten muss eindeutig sein.
> - Ein Cluster-LA-Kanal kann zu einem FIS hinzugefügt werden. Sie stellen sicher, dass der Cluster-LA-Kanal über eine lokale Schnittstelle als Mitgliederschnittstelle verfügt.

Weitere Informationen zu FIS finden Sie unter Konfigurieren des Failover-Interface-Sets.

Wie werden Netzprofile in einem Cluster-Setup konfiguriert?

> **Hinweis**
>
> Wird ab NetScaler 10.5 unterstützt.

Sie können gesperrte IP-Adressen an ein Netzprofil binden. Dieses Netzprofil kann dann an einen virtuellen Server oder Dienst für den Spotted Load Balancing gebunden werden (der mithilfe einer Knotengruppe definiert wird). Die folgenden Empfehlungen müssen befolgt werden. Andernfalls werden die Netzprofilkonfigurationen nicht berücksichtigt und die USIP/USNIP-Einstellungen werden verwendet:

> **Hinweis**
>
> - Wenn der **strikte** Parameter der Knotengruppe auf **Ja**gesetzt ist, muss das Netzprofil mindestens eine IP-Adresse von jedem Knotengruppenmitglied enthalten.
> - Wenn der **strikte** Parameter der Knotengruppe auf **Nein**gesetzt ist, muss das Netzprofil mindestens eine IP-Adresse von jedem der Clusterknoten enthalten.

Wie kann ich WionNS in einem Cluster-Setup konfigurieren?

> **Hinweis**
>
> Wird ab NetScaler 11.0 Build 62.x unterstützt.

Um WionNS in einem Cluster zu verwenden, müssen Sie Folgendes tun:

1. Stellen Sie sicher, dass das Java-Paket und das WI-Paket auf allen Clusterknoten im selben Verzeichnis vorhanden sind.
2. Erstellen Sie einen virtuellen Lastausgleichsserver, für den die Persistenz konfiguriert ist.
3. Erstellen Sie Dienste mit IP-Adressen als NSIP-Adresse der einzelnen Clusterknoten, die Sie für den WI-Verkehr bereitstellen möchten. Dieser Schritt kann nur mit der NetScaler CLI konfiguriert werden.
4. Binden Sie die Dienste an den virtuellen Lastausgleichsserver.

> **Hinweis**
>
> Wenn Sie WIonNS über eine VPN-Verbindung verwenden, stellen Sie sicher, dass der virtuelle Loadbalancing-Server auf WIHOME eingestellt ist.

Kann der Cluster-LA-Kanal für den Verwaltungszugriff verwendet werden?

Nein. Der Verwaltungszugriff auf einen Clusterknoten darf nicht auf einem Cluster-LA-Kanal (z. B. CLA/1) oder seinen Mitgliedsschnittstellen konfiguriert werden. Dies liegt daran, dass, wenn der Knoten INAKTIV ist, die entsprechende Cluster-LA-Schnittstelle als ausgeschaltet markiert ist und daher den Verwaltungszugriff verliert.

Wie kommunizieren Clusterknoten miteinander und was sind die verschiedenen Arten von Datenverkehr, der durch die Backplane fließt?

Eine Backplane ist eine Reihe von Schnittstellen, bei denen eine Schnittstelle jedes Knotens mit einem gemeinsamen Switch verbunden ist, der als Cluster-Backplane-Switch bezeichnet wird. Die verschiedenen Arten von Datenverkehr, der über eine Backplane fließt, die für die Kommunikation zwischen den Knoten verwendet wird, sind:

- Node-zu-Knoten-Messaging (NNM)
- Gelenkter Verkehr
- Weitergabe und Synchronisation der Konfiguration

Jeder Knoten des Clusters verwendet eine spezielle MAC-Cluster-Backplane-Switch-Adresse, um über die Backplane mit anderen Knoten zu kommunizieren. Die spezielle Cluster-MAC hat die Form: **0x02 0x00 0x6F <cluster_id> <node_id> <reserved>**, wobei <cluster_id> die Cluster-Instanz-ID ist. <node_id> ist die Knotennummer der NetScaler Appliance, die einem Cluster hinzugefügt wird.

> **Hinweis**
>
> Die Menge an Datenverkehr, die von einer Backplane verarbeitet wird, hat einen vernachlässigbaren CPU-Overhead.

Was wird über den GRE-Tunnel für den Layer-3-Cluster geleitet?

Nur der gelenkte Datenverkehr läuft über den GRE-Tunnel. Die Pakete werden durch den GRE-Tunnel zum Knoten im anderen Subnetz geleitet.

Wie werden Node to Node Messaging (NNM) und Heartbeat-Nachrichten ausgetauscht und wie werden sie weitergeleitet?

Das NNM, Heartbeat-Nachrichten und das Cluster-Protokoll steuern den Datenverkehr nicht. Diese Nachrichten werden nicht durch den Tunnel gesendet, sondern direkt weitergeleitet.

Was sind die MTU-Empfehlungen für getunnelten Layer-3-Clusterverkehr?

Im Folgenden sind die Layer-3-Cluster-Empfehlungen von Jumbo MTU über den GRE-Tunnel aufgeführt:

- Die Jumbo-MTU kann zwischen den Clusterknoten auf dem L3-Pfad konfiguriert werden, um den GRE-Tunnel-Overhead zu berücksichtigen.
- Die Fragmentierung tritt nicht bei Paketen in voller Größe auf, die gesteuert werden müssen.
- Die Steuerung des Datenverkehrs funktioniert weiterhin, auch wenn Jumbo-Frames nicht erlaubt sind, aber aufgrund der Fragmentierung ist der Aufwand höher.

Wie wird der globale Hash-Schlüssel generiert und von allen Knoten gemeinsam genutzt?

Der `rsskey` für eine eigenständige Appliance wird beim Booten generiert. In einem Cluster-Setup enthält der erste Knoten den `rsskey` des Clusters. Jeder neue Knoten, der dem Cluster beitritt, synchronisiert den `rsskey`.

What is the need of `set rsskeytype -rsskey symmetric` command for *:*, USIP on, `useproxyport` off, topologies?

Es ist nicht clusterspezifisch, sondern gilt auch für eine eigenständige Appliance. Wenn USIP aktiviert ist und der Proxy-Port deaktiviert ist, reduziert der symmetrische `rsskey` sowohl die Core-zu-Core- (C2C)-Steuerung als auch die Knoten-zu-Knoten-Steuerung.

Welche Faktoren tragen zur Veränderung des CCO-Knotens bei?

Der erste Knoten, der zur Bildung eines Cluster-Setups hinzugefügt wird, wird zum CCO-Knoten (Configuration Coordinator). Die folgenden Faktoren tragen zur Änderung des CCO-Knotens im Cluster-Setup bei:

- Wenn der aktuelle CCO-Knoten aus dem Cluster-Setup entfernt wird
- Wenn der aktuelle CCO-Knoten abstürzt
- Wenn die Priorität des Nicht-CCO-Knotens geändert wird (eine niedrigere Priorität hat eine höhere Priorität)
- Unter dynamischen Bedingungen wie der Netzwerkerreichbarkeit zwischen den Knoten
- Wenn sich die Knotenzustände ändern — aktiv, sparsam und passiv. Aktive Knoten werden als CCO bevorzugt.
- Wenn sich die Konfiguration ändert und der Knoten mit der neuesten Konfiguration als CCO bevorzugt wird.

Fehlerbehebung beim NetScaler Cluster

May 11, 2023

Tritt in einem NetScaler-Cluster ein Fehler auf, besteht der erste Schritt bei der Fehlerbehebung darin, Informationen über die Clusterinstanz abzurufen. Sie können die Informationen abrufen, indem Sie die Befehle `show cluster instance clId` und `show cluster node nodeId` auf den jeweiligen Clusterknoten ausführen.

Wenn Sie das Problem mit den beiden oben genannten Methoden nicht finden können, können Sie eine der folgenden Methoden verwenden:

- **Identifizieren Sie die Ursache des Fehlers.** Versuchen Sie, den Cluster zu umgehen, um den Server zu erreichen. Wenn der Versuch erfolgreich ist, liegt das Problem wahrscheinlich beim Cluster-Setup.
- **Überprüfen Sie die kürzlich ausgeführten Befehle.** Führen Sie den Befehl history aus, um die zuletzt auf dem Cluster durchgeführten Konfigurationen zu überprüfen. Sie können auch die Datei ns.conf überprüfen, um die implementierten Konfigurationen zu überprüfen.
- **Überprüfen Sie die ns.log Dateien.** Verwenden Sie die Protokolldateien, die im Verzeichnis /var/log/ jedes Knotens verfügbar sind, um die ausgeführten Befehle, den Status der Befehle und die Statusänderungen zu identifizieren.
- **Überprüfen Sie die Newnslog-Dateien.** Verwenden Sie die `newnslog` Dateien, die im Verzeichnis /var/nslog/ jedes Knotens verfügbar sind, um die Ereignisse zu identifizieren, die auf den Clusterknoten aufgetreten sind. Sie können mehrere `newnslog` Dateien als eine einzige Datei anzeigen, indem Sie die Dateien in ein einzelnes Verzeichnis kopieren und dann den folgenden Befehl ausführen:

```
nsconmsg -K newnslog-node<id> -K     newnslog.node<id> -d current
```

Wenn Sie das Problem immer noch nicht lösen können, können Sie versuchen, die Pakete auf dem Cluster zu verfolgen oder den `techsupport -scope cluster` Befehl show zu verwenden. Sie können den Befehl verwenden, um den Bericht an das technische Support-Team zu senden.

Verfolgung der Pakete eines NetScaler Clusters

May 11, 2023

Das NetScaler-Betriebssystem bietet ein Hilfsprogramm namens *ns trace*, mit dem Sie einen Dump der Pakete abrufen können, die von einer Appliance empfangen und gesendet werden. Das Dienstprogramm speichert die Pakete in Ablaufverfolgungsdateien. Sie können diese Dateien verwenden, um Probleme im Paketfluss zu den Clusterknoten zu debuggen. Die Trace-Dateien müssen mit der Wireshark-Anwendung betrachtet werden.

Einige herausragende Aspekte des Dienstprogramms ns Trace sind:

- Kann so konfiguriert werden, dass Pakete selektiv mit klassischen Ausdrücken und Standardausdrücken verfolgt werden.
- Kann den Trace in mehreren Formaten erfassen: ns-Trace-Format (.cap) und TCP-Dump-Format (.pcap).
- Kann die Trace-Dateien aller Clusterknoten auf dem Konfigurationskoordinator aggregieren.
- Kann mehrere Trace-Dateien zu einer einzigen Trace-Datei zusammenführen (nur für.cap-Dateien).

Sie können das Dienstprogramm ns trace von der NetScaler-Befehlszeile oder der NetScaler-Shell aus verwenden.

So verfolgen Sie Pakete einer eigenständigen Appliance

Führen Sie den Befehl start ns trace auf der Appliance aus. <date-timestamp>Der Befehl erstellt Protokolldateien im Verzeichnis /var/nstrace/. Die Namen der Trace-Dateien haben die Form nstrace<id>.cap.

Sie können den Status anzeigen, indem Sie den Befehl show ns trace ausführen. Sie können die Verfolgung der Pakete beenden, indem Sie den Befehl stop ns trace ausführen.

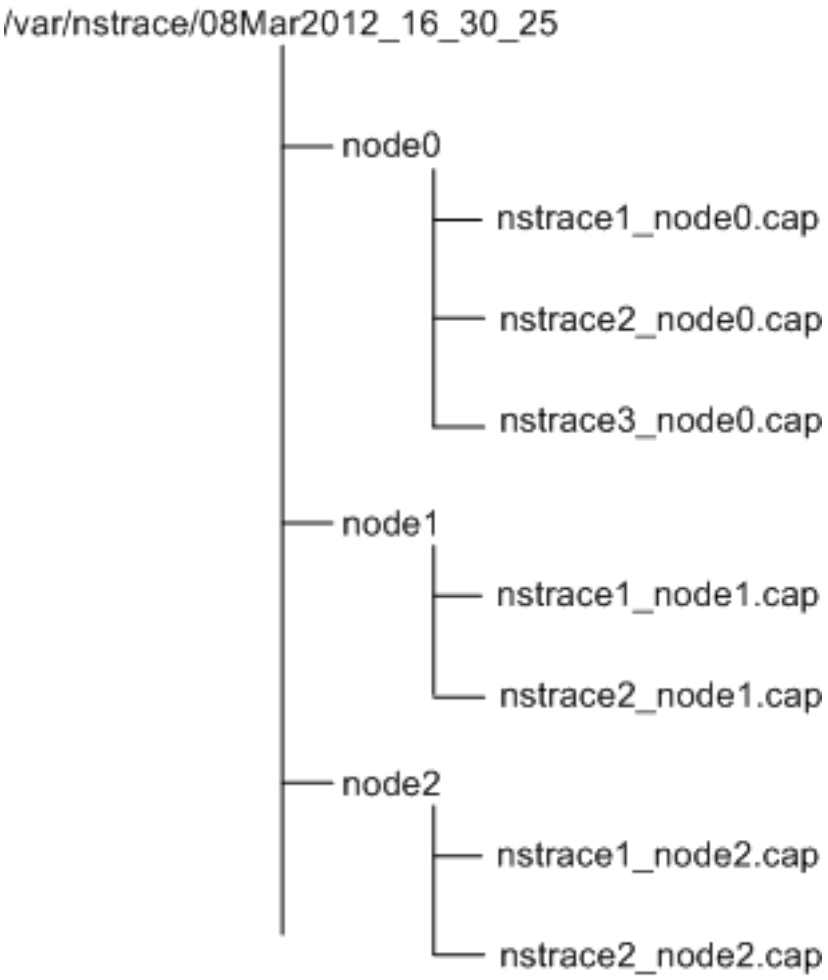
> **Hinweis**
>
> Sie können das Dienstprogramm ns trace auch von der NetScaler-Shell aus ausführen, indem Sie die
> Datei nstrace.sh ausführen. Es wird jedoch empfohlen, das Dienstprogramm ns trace über die NetScaler-Befehlszeilenschnittstelle zu verwenden.

So verfolgen Sie Pakete eines Clusters

Sie können die Pakete auf allen Clusterknoten verfolgen und alle Trace-Dateien auf dem Konfigurationskoordinator abrufen.

Führen Sie den Befehl start ns trace auf der Cluster-IP-Adresse aus. Der Befehl wird weitergegeben und auf allen Clusterknoten ausgeführt. Die Trace-Dateien werden in einzelnen Clusterknoten im Verzeichnis /var/nstrace/<date-timestamp> gespeichert. Die Namen der Trace-Dateien haben die Form nstrace<id>_node<id>.cap.

Sie können die Ablaufverfolgungsdateien jedes Knotens verwenden, um die Knoten Operationen zu debuggen. Wenn Sie jedoch die Trace-Dateien aller Clusterknoten an einem Ort haben möchten, müssen Sie den Befehl stop ns trace auf der Cluster-IP-Adresse ausführen. Die Trace-Dateien aller Knoten werden auf den Cluster-Konfigurationskoordinator im Verzeichnis<date-timestamp> /var/nstrace/ wie folgt heruntergeladen:



Mehrere Trace-Dateien zusammenführen

Sie können aus den Trace-Dateien eine einzelne Datei vorbereiten (wird nur unterstützt für. Cap-Dateien), die von den Clusterknoten abgerufen wurden. Die einzelnen Trace-Dateien geben Ihnen einen kumulativen Überblick über den Verlauf der Cluster-Pakete. Die Trace-Einträge in der einzelnen Trace-Datei werden nach der Uhrzeit sortiert, zu der die Pakete im Cluster empfangen wurden.

Um die Ablaufverfolgungsdateien zusammenzuführen, geben Sie in der NetScaler-Shell Folgendes ein:

```
1 > nstracemerge.sh -srcdir \<DIR\> -dstdir \<DIR\> -filename \<name\> -
    filesize \<num\>
```

Hierbei gilt:

- `srcdir` ist das Verzeichnis, aus dem die Trace-Dateien zusammengeführt werden. Alle Trace-Dateien in diesem Verzeichnis werden zu einer einzigen Datei zusammengeführt.
- `dstdir` ist das Verzeichnis, in dem die zusammengeführte Trace-Datei erstellt wird.

- `Filename` ist der Name der Trace-Datei, die erstellt wird.
- `Filesize` ist die Größe der Trace-Datei.

Beispiele

Im Folgenden finden Sie einige Beispiele für die Verwendung des Dienstprogramms ns trace zum Filtern von Paketen.

- So verfolgen Sie die Pakete auf den Backplane-Schnittstellen von drei Knoten:

  Mit klassischen Ausdrücken:

  ```
  1   > start nstrace -filter "INTF == 0/1/1 && INTF == 1/1/1 && INTF
        == 2/1/1"
  ```

  Verwendung von Standardausdrücken:

  ```
  1   > start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") &&
        CONNECTION.INTF.EQ("1/1/1") && CONNECTION.INTF.EQ("2/1/1")"
  ```

- Um die Pakete von einer Quell-IP-Adresse 10.102.34.201 oder von einem System zu verfolgen, dessen Quellport größer als 80 ist und der Dienstname nicht „s1" ist:

  Klassische Ausdrücke verwenden

  ```
  1   > start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME !=
        s1 && SOURCEPORT > 80)"
  ```

  Verwenden von Standardausdrücken

  ```
  1   > start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) || (
        CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.GT(80))"
  ```

> **Hinweis**
>
> Weitere Informationen zu Filtern, die in ns trace verwendet werden, finden Sie unter ns trace.

Erfassen von SSL-Sitzungsschlüsseln während einer Ablaufverfolgung

Wenn Sie den Befehl "start ns trace" ausführen, können Sie den neuen Parameter `capsslkeys` so festlegen, dass die SSL-Masterschlüssel für alle SSL-Sitzungen erfasst werden. Wenn Sie diesen Parameter angeben, wird zusammen mit dem Paket-Trace eine Datei mit dem Namen nstrace.sslkeys generiert. Diese Datei kann in Wireshark importiert werden, um den SSL-Verkehr in der entsprechenden Trace-Datei zu entschlüsseln.

Diese Funktion ähnelt Webbrowsern, die Sitzungsschlüssel exportieren, die später in Wireshark importiert werden können, um SSL-Verkehr zu entschlüsseln.

Vorteile der Verwendung von SSL-Sitzungsschlüsseln

Im Folgenden sind die Vorteile der Verwendung von SSL-Sitzungsschlüsseln aufgeführt:

1. Generiert kleinere Trace-Dateien, die die zusätzlichen Pakete, die durch den SSLPLAIN-Erfassungsmodus erstellt wurden, nicht enthalten.
2. Bietet die Möglichkeit, Klartext [SP (1] aus dem Trace anzuzeigen und zu wählen, ob die Masterschlüsseldatei gemeinsam genutzt werden soll oder ob vertrauliche Daten geschützt werden sollen, indem sie nicht gemeinsam genutzt werden.

Einschränkungen bei der Verwendung von SSL-Sitzungsschlüsseln

Im Folgenden sind die Einschränkungen bei der Verwendung von SSL-Sitzungsschlüsseln aufgeführt:

1. SSL-Sitzungen können nicht entschlüsselt werden, wenn die ersten Pakete der Sitzung nicht erfasst werden.
2. SSL-Sitzungen können nicht erfasst werden, wenn der FIPS-Modus (Federal Information Processing Standard) aktiviert ist.

So erfassen Sie SSL-Sitzungsschlüssel mithilfe der Befehlszeilenschnittstelle (CLI)

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um SSL-Sitzungsschlüssel in einer Ablaufverfolgungsdatei zu aktivieren oder zu deaktivieren und den Ablaufverfolgungsvorgang zu überprüfen.

```
1  > start nstrace -capsslkeys ENABLED
2  > show nstrace
3  Example
4  > start nstrace -capsslkeys ENABLED
5  > show nstrace
6        State:  RUNNING          Scope:  LOCAL           TraceLocation:
             "/var/nstrace/04May2016_17_51_54/..."
7        Nf:  24                  Time:  3600             Size:  164
                        Mode:  TXB NEW_RX
8        Traceformat:  NSCAP      PerNIC:  DISABLED       FileName:  04
            May2016_17_51_54 Link:  DISABLED
9        Merge:  ONSTOP           Doruntimecleanup:  ENABLED TraceBuffers:
              5000      SkipRPC:  DISABLED
10       SkipLocalSSH:  DISABLED  Capsslkeys:  ENABLED     InMemoryTrace:
             DISABLED
11   Done
```


So konfigurieren Sie SSL-Sitzungsschlüssel über die NetScaler GUI

1. Navigieren Sie zu **Konfiguration > System > Diagnose > Tools für den technischen Support** und klicken Sie auf **Neuen Trace starten**, um mit der Verfolgung verschlüsselter Pakete auf einer Appliance zu beginnen.
2. Aktivieren Sie auf der Seite **Start Trace** das Kontrollkästchen **Capture SSL Master Keys** .
3. Klicken Sie auf **OK** und **Fertig**.

Um die SSL-Masterschlüssel in Wireshark zu importieren

Navigieren Sie auf der Wireshark GUI zu **Bearbeiten > Voreinstellungen > Protokolle > SSL > (Pre) -Master-Secret Protokolldateiname und geben Sie die Masterschlüsseldateien** an, die von der Appliance erhalten wurden.

Problembehandlung häufiger Probleme

August 19, 2021

Beim Verbinden eines Knotens zum Cluster erhalte ich folgende Meldung: “FEHLER: Ungültiger Schnittstellenname/Nummer. “ Was muss ich tun, um diesen Fehler zu beheben?

Der genannte Fehler tritt auf, wenn Sie eine ungültige oder falsche Backplane-Schnittstelle angegeben haben, während Sie den Befehl ”Clusterknoten hinzufügen” zum Hinzufügen des Knotens verwendet haben. Um diesen Fehler zu beheben, überprüfen Sie die Schnittstelle, die Sie beim Hinzufügen des Knotens angegeben haben. Stellen Sie sicher, dass Sie die Verwaltungsschnittstelle der Appliance nicht als Backplane-Schnittstelle angegeben haben und dass das Bit <nodeId> der Schnittstelle mit der ID des Knotens übereinstimmt. Wenn die nodeID beispielsweise 3 ist, muss die Backplane-Schnittstelle 3/<c>/sein<u>.

Beim Verbinden eines Knotens zum Cluster erhalte ich folgende Meldung: “FEHLER: Clustering kann nicht aktiviert werden, da der lokale Knoten kein Mitglied des Clusters ist. “ Was muss ich tun, um diesen Fehler zu beheben?

Dieser Fehler tritt auf, wenn Sie versuchen, einen Knoten zu verbinden, ohne das NSIP des Knotens zum Cluster hinzuzufügen. Um diesen Fehler zu beheben, müssen Sie zuerst die NSIP-Adresse des Knotens dem Cluster hinzufügen hinzufügen, indem Sie den Befehl “ **Clusterknoten hinzufügen** “ verwenden und dann den Befehl “ **Cluster beitreten** “ ausführen.

Beim Verbinden eines Knotens zum Cluster erhalte ich folgende Meldung: “FEHLER: Verbindung verweigert. “ Was muss ich tun, um diesen Fehler zu beheben?

Dieser Fehler kann aus folgenden Gründen auftreten:

- **Verbindungsprobleme.** Der Knoten kann keine Verbindung zur Cluster-IP-Adresse herstellen. Versuchen Sie, die Cluster-IP-Adresse von dem Knoten zu pingen, dem Sie beitreten möchten.
- **Duplizierte Cluster-IP-Adresse.** Überprüfen Sie, ob die Cluster-IP-Adresse auf einem Nicht-Clusterknoten vorhanden ist. Wenn dies der Fall ist, erstellen Sie eine Cluster-IP-Adresse und versuchen Sie, dem Cluster wieder beizutreten.

Beim Verbinden eines Knotens mit dem Cluster erhalte ich die folgende Meldung: FEHLER: Lizenzkonflikt zwischen dem Konfigurationskoordinator und dem lokalen Knoten. Was muss ich tun, um diesen Fehler zu beheben?

Die Appliance, die Sie dem Cluster beitreten, muss über die gleichen Lizenzen wie der Konfigurationskoordinator verfügen. Dieser Fehler tritt auf, wenn die Lizenzen auf dem Knoten, dem Sie beitreten, nicht mit den Lizenzen auf dem Konfigurationskoordinator übereinstimmen. Um diesen Fehler zu beheben, führen Sie die folgenden Befehle auf beiden Knoten aus und vergleichen Sie die Ausgaben.

Von der Befehlszeile aus:

- `show ns hardware`
- `show ns license`

Aus der Schale:

- `nsconmsg -g feature -d stats`
- `ls /nsconfig/license`
- Anzeigen des Inhalts der Datei /var/log/license.log

Was muss ich tun, wenn die Konfigurationen eines Clusterknotens nicht mit den Clusterkonfigurationen synchronisiert sind?

Normalerweise werden die Konfigurationen automatisch zwischen allen Clusterknoten synchronisiert. Wenn Sie jedoch der Meinung sind, dass die Konfigurationen auf einem bestimmten Knoten nicht synchronisiert sind, müssen Sie die Synchronisierung erzwingen, indem Sie den Befehl force cluster sync von dem Knoten ausführen, den Sie synchronisieren möchten. Weitere Informationen finden Sie unter Clusterkonfigurationen synchronisieren.

Wenn Sie einen Clusterknoten konfigurieren, erhalte ich die folgende Meldung: “FEHLER: Sitzung ist schreibgeschützt; verbinden Sie sich mit der Cluster-IP-Adresse, um die Konfiguration zu ändern. “

Alle Konfigurationen auf einem Cluster müssen über die Cluster-IP-Adresse erfolgen, und die Konfigurationen werden an die anderen Clusterknoten weitergegeben. Alle Sitzungen, die über die NSIP-Adresse einzelner Knoten eingerichtet werden, sind schreibgeschützt.

Warum zeigt der Knotenstatus “INACTIVE” an, wenn der Knotenzustand “UP” anzeigt?

Ein fehlerweiter Knoten kann sich aus verschiedenen Gründen im Status INACTIVE befinden. Ein Scan der ns.log oder Fehlerzähler kann Ihnen helfen, den genauen Grund zu ermitteln.

Wie kann ich den Zustand eines Knotens auflösen, wenn sein Zustand NICHT UP anzeigt?

Knotenintegrität “**Nicht UP**” zeigt an, dass es einige Probleme mit dem Knoten gibt. Um die Ursache zu kennen, müssen Sie den Befehl **show cluster node** ausführen. Dieser Befehl zeigt die Knoteneigenschaften und den Grund für den Knotenfehler an.

Was muss ich tun, wenn der Zustand eines Knotens als NICHT UP angezeigt wird und der Grund darauf hinweist, dass Konfigurationsbefehle auf einem Knoten fehlgeschlagen sind?

Dieses Problem tritt auf, wenn einige Befehle nicht auf den Cluster-Knoten ausgeführt werden. In solchen Fällen müssen Sie sicherstellen, dass die Konfigurationen mit einer der folgenden Optionen synchronisiert werden:

- Wenn sich einige der Clusterknoten in diesem Zustand befinden, müssen Sie die Clustersynchronisierung auf diesen Knoten erzwingen. Weitere Informationen finden Sie unter Clusterkonfigurationen synchronisieren.
- Wenn sich alle Clusterknoten in diesem Zustand befinden, müssen Sie die Clusterinstanz auf allen Clusterknoten deaktivieren und aktivieren.

Wenn ich den Befehl set virtual server ausführe, erhalte ich die folgende Meldung: “Keine solche Ressource.” Was muss ich tun, um dieses Problem zu beheben?

Der Befehl **set vserver** wird beim Clustering nicht unterstützt. Die Befehle **“unset vserver”, “enable vserver”, “disable vserver”** und **rm vserver** werden ebenfalls nicht unterstützt. Der Befehl **show vserver** wird jedoch unterstützt.

Ich kann den Cluster nicht über eine Telnet-Sitzung konfigurieren. Was soll ich tun?

Über eine Telnet-Sitzung kann auf die Cluster-IP-Adresse nur im schreibgeschützten Modus zugegriffen werden. Daher können Sie keinen Cluster über eine Telnet-Sitzung konfigurieren.

Ich stelle einen signifikanten Zeitunterschied über die Clusterknoten fest. Was muss ich tun, um dieses Problem zu beheben?

Wenn PTP-Pakete aufgrund des Backplane-Switches verworfen werden oder wenn die physischen Ressourcen in einer virtuellen Umgebung zu stark beauftragen, wird die Zeit nicht synchronisiert.

Um die Zeiten zu synchronisieren, müssen Sie die folgenden Schritte für die Cluster-IP-Adresse ausführen:

1. PTP deaktivieren.

   sett ptp -state disable

2. Konfigurieren Sie Network Time Protocol (NTP) für den Cluster. Weitere Informationen finden Sie unter Einrichten der Uhrsynchronisation.

Was muss ich tun, wenn keine Verbindung zur Cluster-IP-Adresse und der NSIP-Adresse eines Clusterknotens besteht?

Wenn Sie nicht auf die Cluster-IP-Adresse oder den NSIP eines Clusterknotens zugreifen können, müssen Sie über die serielle Konsole auf die Appliance zugreifen. Wenn die NSIP-Adresse erreichbar ist, können Sie SSH von der Shell aus an die Cluster-IP-Adresse senden, indem Sie an der Shell-Eingabeaufforderung den folgenden Befehl ausführen:

“‘# ssh nsroot@

```
## Was muss ich tun, um einen Clusterknoten wiederherzustellen, der Verbindungsprobleme aufweist?

So stellen Sie einen Knoten mit Verbindungsproblemen wieder her:

1.  Deaktivieren Sie die Clusterinstanz auf diesem Knoten (da Sie keine Befehle vom NSIP eines Clusterknotens ausführen können).

1.  Führen Sie die zum Wiederherstellen des Knotens erforderlichen Befehle aus.

1.  Aktivieren Sie die Clusterinstanz auf diesem Knoten.

## Einige Knoten des Clusters haben zwei Standardrouten. Wie kann ich die zweite Standardroute vom Clusterknoten entfernen?

Um die zusätzliche Standardroute zu löschen, gehen Sie auf jedem Knoten mit der zusätzlichen Route folgendermaßen vor:

1.  Deaktivieren Sie die Clusterinstanz.
```



```
16
17      ```disable cluster instance <clId><!--NeedCopy-->
```

1. Entfernen Sie die Route.

   ```
   rm route <network> <netmask> <gateway><!--NeedCopy-->
   ```

2. Aktivieren Sie die Clusterinstanz.

   ```
   enable cluster instance <clId><!--NeedCopy-->
   ```

Die Clusterfunktionalität wird beeinträchtigt, wenn ein vorhandener Clusterknoten online geschaltet wird. Was muss ich tun, um dieses Problem zu beheben?

Wenn das RPC-Kennwort eines Knotens von der Cluster-IP-Adresse geändert wird, wenn dieser Knoten nicht im Cluster ist, besteht eine Nichtübereinstimmung bei RPC-Anmeldeinformationen, die die Clusterfunktionalität beeinträchtigen. Um dieses Problem zu lösen, verwenden Sie den Befehl set ns Rpc-Node, um das Kennwort auf dem NSIP des Knotens zu aktualisieren, der online ist.

Content Switching

May 11, 2023

Auf den heutigen komplexen Websites möchten Sie möglicherweise verschiedenen Benutzern unterschiedliche Inhalte präsentieren. Beispielsweise möchten Sie Benutzern aus dem IP-Bereich eines Kunden oder Partners den Zugriff auf ein spezielles Webportal gestatten. Möglicherweise möchten Sie Benutzern aus diesem Gebiet Inhalte präsentieren, die für ein bestimmtes geografisches Gebiet relevant sind. Vielleicht möchten Sie den Sprechern dieser Sprachen Inhalte in verschiedenen Sprachen präsentieren. Möglicherweise möchten Sie Inhalte präsentieren, die auf bestimmte Geräte wie Smartphones zugeschnitten sind, denjenigen, die die Geräte verwenden. Die NetScaler Content Switching-Funktion ermöglicht es der Appliance, Clientanforderungen auf mehrere Server basierend auf bestimmten Inhalten zu verteilen, die Sie diesen Benutzern präsentieren möchten.

Um Content Switching zu konfigurieren, erstellen Sie zunächst ein grundlegendes Content Switching-Setup und passen Sie es dann an Ihre Bedürfnisse an. Dies beinhaltet das Aktivieren der Content Switching-Funktion, das Einrichten des Lastausgleichs für den Server oder die Server, die jede Version des zu schaltenden Inhalts hosten, das Erstellen eines virtuellen Content Switching-Servers, das Erstellen von Richtlinien zur Auswahl, welche Anforderungen an welchen virtuellen Lastausgleichsserver gerichtet werden, und Binden der Richtlinien an den virtuellen Content Switching-Server. Sie können das Setup dann an Ihre Anforderungen anpassen, indem Sie Vorrang für Ihre Richtlinien festlegen, Ihr Setup schützen, indem Sie einen virtuellen Backupserver konfigurieren und die Leistung Ihres Setups verbessern, indem Sie Anfragen an einen Cache umleiten.

So funktioniert Content Switching

Content Switching ermöglicht es der NetScaler-Appliance, Anfragen, die an denselben Webhost gesendet werden, an verschiedene Server mit unterschiedlichem Inhalt weiterzuleiten. Sie können die Appliance beispielsweise so konfigurieren, dass Anfragen für dynamischen Inhalt (z. B. URLs mit dem Suffix von .asp, .dll oder .exe) an einen Server und Anfragen nach statischen Inhalten an einen anderen Server weitergeleitet werden. Sie können die Appliance so konfigurieren, dass Content Switching basierend auf TCP/IP-Headern und Nutzdaten durchgeführt wird.

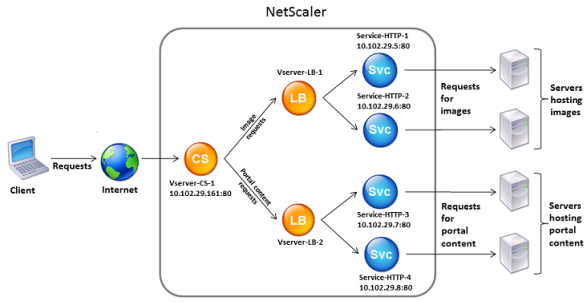
Sie können auch Content Switching verwenden, um die Appliance so zu konfigurieren, dass Anfragen basierend auf verschiedenen Clientattributen an verschiedene Server mit unterschiedlichen Inhalten umgeleitet werden. Einige dieser Client-Attribute sind:

- **Gerätetyp.** Die Appliance untersucht den Benutzeragenten oder den benutzerdefinierten HTTP-Header in der Clientanforderung auf den Gerätetyp, von dem die Anforderung stammt. Basierend auf dem Gerätetyp leitet es die Anforderung an einen bestimmten Webserver weiter. Wenn die Anfrage beispielsweise von einem Mobiltelefon stammt, wird die Anfrage an einen Server geleitet, der Inhalte bereitstellen kann, die der Benutzer auf dem Mobiltelefon anzeigen kann. Eine Anforderung von einem Computer wird an einen anderen Server gerichtet, der Inhalte bereitstellen kann, die für einen Computerbildschirm ausgelegt sind.
- **Sprache.** Die Appliance untersucht den HTTP-Header der Accept-Language in der Clientanforderung und bestimmt die Sprache, die vom Browser des Clients verwendet wird. Die Appliance sendet die Anforderung dann an einen Server, der Inhalte in dieser Sprache bereitstellt. Mithilfe der sprachbasierten Content Switching kann die Appliance beispielsweise jemanden senden, dessen Browser so konfiguriert ist, dass Inhalte auf Französisch mit der französischen Version einer Zeitung angefordert werden. Es kann jemand anderen, dessen Browser so konfiguriert ist, dass er Inhalte in englischer Sprache anfordert, an einen Server mit der englischen Version senden.
- **Plätzchen.** Die Appliance untersucht die HTTP-Anforderungsheader auf ein Cookie, das der Server zuvor gesetzt hat. Wenn es das Cookie findet, leitet es Anfragen an den entsprechenden Server weiter, der benutzerdefinierte Inhalte hostet. Wenn beispielsweise ein Cookie gefunden wird, das darauf hinweist, dass der Kunde Mitglied eines Kundenbindungsprogramms ist, wird die Anfrage an einen schnelleren Server oder einen mit speziellen Inhalten weitergeleitet. Wenn es kein Cookie findet oder wenn das Cookie anzeigt, dass der Benutzer kein Mitglied ist, wird die Anfrage an einen Server für die breite Öffentlichkeit gerichtet.
- **HTTP-Methode.** Die Appliance untersucht den HTTP-Header auf die verwendete Methode und sendet die Clientanforderung an den richtigen Server. Beispielsweise können GET-Anfragen für Bilder an einen Bildserver gerichtet werden, während POST-Anfragen an einen schnelleren Server geleitet werden können, der dynamische Inhalte verarbeitet.
- **Layer 3/4 Daten.** Die Appliance untersucht Anforderungen für die Quell- oder Ziel-IP, den Quell- oder Zielport oder andere Informationen, die in den TCP- oder UDP-Headern enthalten

sind, und leitet die Clientanforderung an den richtigen Server weiter. Beispielsweise können Anfragen von Quell-IPs, die Kunden gehören, an ein benutzerdefiniertes Webportal auf einem schnelleren Server oder eines mit speziellen Inhalten weitergeleitet werden.

Eine typische Content Switching-Bereitstellung besteht aus den im folgenden Diagramm beschriebenen Entitäten.

Abbildung 1. Content Switching Architektur



Eine Content Switching-Konfiguration besteht aus einem virtuellen Content Switching-Server, einem Load Balancing-Setup, bestehend aus virtuellen Servern und Diensten für den Lastenausgleich und Richtlinien für Content Switching. Um Content Switching zu konfigurieren, müssen Sie einen virtuellen Content Switching-Server konfigurieren und ihn Richtlinien und virtuellen Lastausgleichsservern zuordnen. Dieser Prozess erstellt eine*Content-Gruppe*eine Gruppe aller virtuellen Server und Richtlinien, die an einer bestimmten Content Switching-Konfiguration beteiligt sind.

Content Switching kann mit HTTP-, HTTPS-, TCP- und UDP-Verbindungen verwendet werden. Für HTTPS müssen Sie SSL-Offload aktivieren.

Wenn eine Anforderung den virtuellen Content Switching-Server erreicht, wendet der virtuelle Server die zugeordneten Content Switching-Richtlinien auf diese Anforderung an. Die Priorität der Richtlinie definiert die Reihenfolge, in der die an den virtuellen Content Switching-Server gebundenen Richtlinien ausgewertet werden. Wenn Sie erweiterte Richtlinienrichtlinien verwenden und eine Richtlinie an den virtuellen Server für die Content Switching binden, müssen Sie dieser Richtlinie eine Priorität zuweisen. Wenn Sie klassische NetScaler-Richtlinien verwenden, können Sie Ihren Richtlinien eine Priorität zuweisen, müssen dies jedoch nicht tun. Wenn Sie Prioritäten zuweisen, werden die Richtlinien in der von Ihnen festgelegten Reihenfolge ausgewertet. Wenn Sie dies nicht tun, wertet die NetScaler-Appliance Ihre Richtlinien in der Reihenfolge aus, in der sie erstellt wurden.

Zusätzlich zum Konfigurieren von Richtlinienprioritäten können Sie die Reihenfolge der Richtlinienbewertung mithilfe von Goto-Ausdrücken und Policy-Bank-Aufrufen ändern. Weitere Informationen zur erweiterten Richtlinienkonfiguration finden Sie unter Konfigurieren erweiterter Richtlinienrichtlinien.

Nachdem die Richtlinien ausgewertet wurden, leitet der virtuelle Content Switching-Server die Anforderung an den entsprechenden virtuellen Lastausgleichsserver weiter, der sie an den entsprechenden Dienst sendet.

Virtuelle Server für Content Switching können nur Anfragen an andere virtuelle Server senden. Wenn Sie einen externen Load Balancer verwenden, müssen Sie einen virtuellen Lastausgleichsserver dafür erstellen und den virtuellen Server als Dienst an den virtuellen Content Switching-Server binden.

Konfigurieren grundlegender Content Switching

May 11, 2023

Bevor Sie Content Switching konfigurieren, müssen Sie wissen, wie Content Switching eingerichtet ist und wie die Dienste und virtuellen Server verbunden sind.

Um ein grundlegendes, funktionales Content Switching-Setup zu konfigurieren, aktivieren Sie zunächst die Funktion zum Content Switching Erstellen Sie dann mindestens eine Content-Gruppe. Erstellen Sie für jede Content-Gruppe einen virtuellen Content Switching-Server, um Anfragen an eine Gruppe von Websites zu akzeptieren, die Content Switching verwenden. Erstellen Sie außerdem ein Lastausgleichs-Setup, das eine Gruppe virtueller Lastausgleichsserver umfasst, an die der virtuelle Content Switching-Server Anfragen weiterleitet. Um anzugeben, welche Anforderungen an welchen virtuellen Lastausgleichsserver weitergeleitet werden sollen, erstellen Sie mindestens zwei Content Switching-Richtlinien, eine für jeden Anforderungstyp, der umgeleitet werden soll. Wenn Sie die virtuellen Server und Richtlinien erstellt haben, binden Sie die Richtlinien an den virtuellen Server für die Content Switching. Sie können eine Richtlinie auch an mehrere virtuelle Content Switching-Server binden. Wenn Sie eine Richtlinie binden, geben Sie den virtuellen Lastausgleichsserver an, an den Anforderungen, die der Richtlinie entsprechen, gerichtet werden sollen.

Zusätzlich zum Binden einzelner Richtlinien an einen virtuellen Content Switching-Server können Sie Richtlinienbeschriftungen binden. Wenn Sie mehr Content-Gruppen erstellen, können Sie eine Policy Label oder ein Richtlinienlabel an mehr als einen der virtuellen Content Switching-Server binden.

> **Hinweis**
>
> Nachdem Sie eine Content-Gruppe erstellt haben, können Sie den virtuellen Content Switching-Server ändern, um die Konfiguration anzupassen.

Content Switching aktivieren

Um die Funktion zum Content Switching verwenden zu können, müssen Sie die Content Switching aktivieren. Sie können Content Switching-Entitäten konfigurieren, obwohl die Funktion Content Switching deaktiviert ist. Die Entitäten werden jedoch nicht funktionieren.

So aktivieren Sie Content Switching über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Content Switching zu aktivieren und die Konfiguration zu überprüfen:

```
enable ns feature CS

show ns feature
<!--NeedCopy-->
```

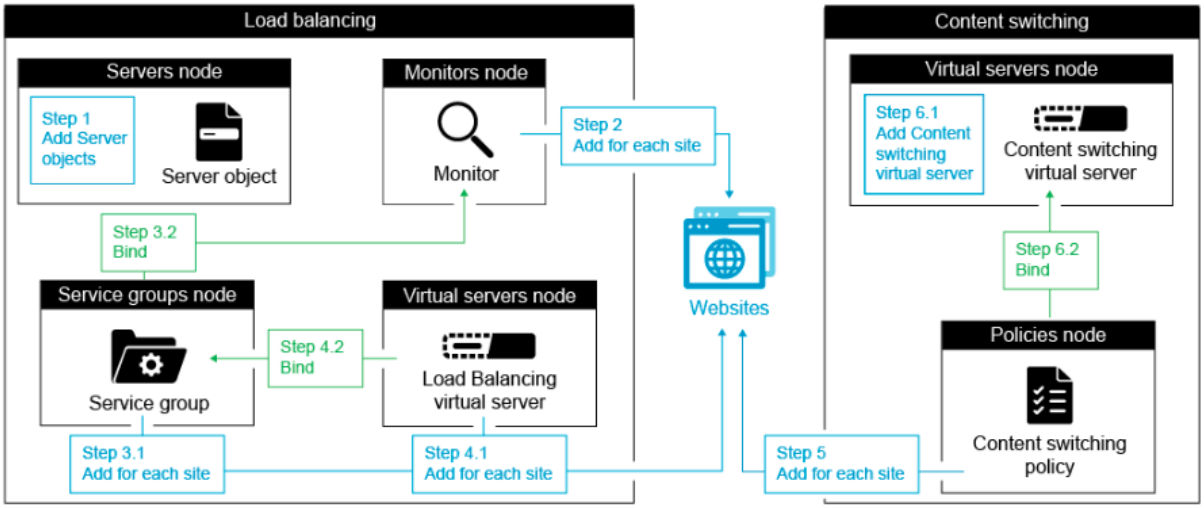
Beispiel:

```
> enable  feature ContentSwitch
    Done
> show feature

    Feature                         Acronym              Status
    -------                         -------              ------
1)     Web Logging                     WL                   OFF
2)     Surge Protection                SP                   ON
3)     Load Balancing                  LB                   ON
4)     Content Switching               CS                   ON
.
.
.
22)    Responder                       RESPONDER            ON
23)    NetScaler Push                  push                 OFF
Done
<!--NeedCopy-->
```

So aktivieren Sie Content Switching über die GUI

Navigieren Sie zu **System > Einstellungen** und wählen Sie in der Gruppe **Modi und Funktionen** die Option **Grundfunktionen konfigurieren**aus, und wählen Sie **Content Switching**aus.

Die folgende Abbildung veranschaulicht die schrittweise Konfiguration von Content Switching.



Erstellen von virtuellen Content Switching

Sie können virtueller Content Switching-Server hinzufügen, ändern und entfernen. Der Status eines virtuellen Servers ist bei der Erstellung DOWN, da der virtuelle Lastausgleichsserver noch nicht an ihn gebunden ist.

So erstellen Sie einen virtuellen Server über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver Vserver-CS-1 HTTP 10.102.29.161 80
<!--NeedCopy-->
```

So fügen Sie über die GUI einen virtuellen Content Switching-Server hinzu

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und fügen Sie einen virtuellen Server hinzu.
2. Geben Sie einen Namen für den virtuellen Server für die Content Switching an.

   > **Hinweis**

> Für jedes Protokoll gibt es einen anderen virtuellen Content Switching-Server. (Zum Beispiel HTTP und SSL).

3. Füllen Sie die entsprechenden Felder aus und klicken Sie auf **OK**.

Statistiken für virtuelle Content Switching-Server

In den Statistiken des virtueller Content Switching-Servers werden Informationen wie die Auswahl des virtuellen Servers, Anforderungsbytes, Antwortbytes, Gesamtzahl der empfangenen Pakete, Gesamtzahl der gesendeten Pakete, Überlaufschwelle, Überlaufauswahl, aktuell vom Client hergestellte Verbindungen und Auswahl des Backups des virtuellen Servers angezeigt.

Die Statistiken des virtuellen Servers zum Content Switching zeigen auch die zusammenfassenden Details des gebundenen virtuellen Standardlastausgleichsservers an.

So zeigen Sie Statistiken des virtuellen Content Switching-Servers über die CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
stat cs vserver <name>
<!--NeedCopy-->
```

Beispiel:

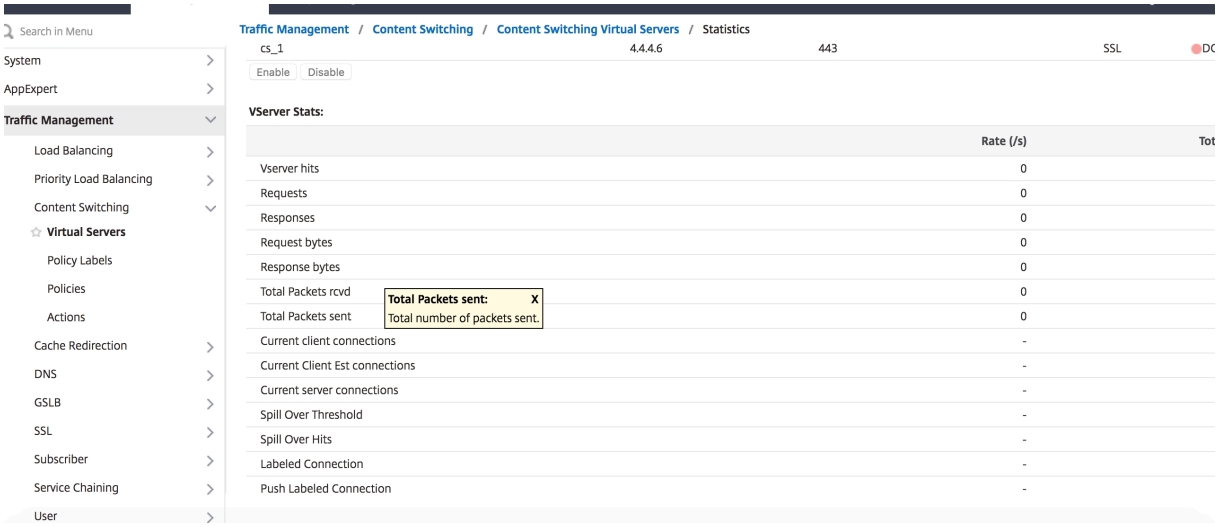
```
stat cs vserver CS_stats
<!--NeedCopy-->
```



```
Vserver Summary
                                IP  port     Protocol        State
CS_stats                   1.1.1.1    80         HTTP           UP

VServer Stats:
                                                  Rate (/s)                Total
Vserver hits                                              0                    0
Requests                                                  0                    0
Responses                                                 0                    0
Request bytes                                             0                    0
Response bytes                                            0                    0
Total Packets rcvd                                        0                    0
Total Packets sent                                        0                    0
Current client connections                               --                    0
Current Client Est connections                           --                    0
Current server connections                               --                    0
Spill Over Threshold                                     --                    0
Spill Over Hits                                          --                    0
Labeled Connection                                       --                    0
Push Labeled Connection                                  --                    0
Deferred Request                                          0                    0
Invalid Request/Response                                 --                    0
Invalid Request/Response Dropped                         --                    0
Vserver Down Backup Hits                                 --                    0
Current Multipath TCP sessions                           --                    0
Current Multipath TCP subflows                           --                    0
Apdex for client response times.                         --                 1.00
Average client TTLB                                      --                    0

 Done
```

So zeigen Sie Statistiken des virtuellen Content Switching-Servers über die GUI an

1. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server**.
2. Wählen Sie den virtuellen Server aus und klicken Sie auf **Statistiken**.



Konfigurieren eines Lastausgleichs-Setups für Content Switching

Der virtuelle Server für die Content Switching leitet alle Anfragen an einen virtuellen Lastausgleichsserver um. Sie müssen einen virtuellen Lastausgleichsserver für jede Version des Inhalts erstellen, der geswitcht wird. Dies gilt auch dann, wenn Ihr Setup nur einen Server für jede Version des Inhalts hat und Sie daher keinen Lastausgleich mit diesen Servern durchführen. Sie können auch den tatsächlichen Lastausgleich mit mehreren Servern mit Lastausgleich konfigurieren, die jede Version des Inhalts widerspiegeln. In beiden Szenarien muss dem virtuellen Content Switching-Server jeder Version des Inhalts, der geswitcht wird, über einen bestimmten virtuellen Lastausgleichsserver verfügen.

Der virtuelle Lastausgleichsserver leitet die Anforderung dann an einen Dienst weiter. Wenn nur ein Dienst an ihn gebunden ist, wählt er diesen Dienst aus. Wenn mehrere Dienste an ihn gebunden sind, verwendet es seine konfigurierte Lastausgleichsmethode, um einen Dienst für die Anforderung auszuwählen, und leitet diese Anforderung an den ausgewählten Dienst weiter.

Um ein grundlegendes Lastausgleichs-Setup zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- Erstellen von virtuellen Lastausgleichsservern
- Erstellen von Diensten
- Binden von Diensten an den virtuellen Lastausgleichsserver

Weitere Informationen zum Lastenausgleich finden Sie unter Funktionsweise des Lastenausgleichs. Ausführliche Anweisungen zum Einrichten einer grundlegenden Load Balancing-Konfiguration finden Sie unter Einrichten des grundlegenden Lastenausgleichs.

Konfigurieren einer Content Switching-Aktion

Sie geben den virtuellen Ziel-Lastausgleichsserver für eine Content Switching-Richtlinie an, wenn Sie die Richtlinie an den virtuellen Server für die Content Switching binden. Daher müssen Sie für jeden virtuellen Lastausgleichsserver eine Richtlinie konfigurieren, auf den der Datenverkehr geleitet werden soll.

Wenn Ihre Richtlinie zum Content Switching jedoch eine erweiterte Richtlinienregel verwendet, können Sie eine Aktion für die Richtlinie konfigurieren. In der Aktion können Sie den Namen des virtuellen Ziel-Lastausgleichsservers angeben oder einen anforderungsbasierten Ausdruck konfigurieren, der zur Laufzeit den Namen des virtuellen Lastausgleichsservers berechnet, an den die Anforderung gesendet werden soll. Der Aktionsausdruck muss in der erweiterten Richtlinie angegeben werden.

Die Ausdrucksoption kann die Größe Ihrer Content Switching-Konfiguration drastisch reduzieren, da Sie nur eine Richtlinie pro virtuellem Content Switching-Server benötigen. Content Switching-Richtlinien, die eine Aktion verwenden, können auch an mehrere virtuelle Server für die Content

Switching gebunden werden, da der virtuelle Ziel-Lastausgleichsserver nicht mehr in der Richtlinie zur Inhaltsvermittlung angegeben ist. Die Möglichkeit, eine einzelne Richtlinie an mehrere virtuelle Content Switching-Server zu binden, hilft dabei, die Größe Ihrer Content Switching-Konfiguration weiter zu reduzieren.

Nachdem Sie eine Aktion erstellt haben, erstellen Sie eine Richtlinie zum Content Switching und geben die Aktion in der Richtlinie an, damit die Aktion ausgeführt wird, wenn diese Richtlinie einer Anforderung entspricht.

> **Hinweis**
>
> Sie können auch für eine Richtlinie zum Content Switching, die eine erweiterte Richtlinienregel verwendet, den virtuellen Ziel-Lastausgleichsserver angeben, wenn Sie die Richtlinie an einen virtuellen Content Switching-Server binden, anstatt eine separate Aktion zu verwenden. Für domänenbasierte Richtlinien, URL-basierte Richtlinien und regelbasierte Richtlinien, die klassische Ausdrücke verwenden, ist eine Aktion nicht verfügbar. Daher geben Sie für diese Arten von Richtlinien den Namen des virtuellen Ziel-Lastausgleichsservers an, wenn Sie die Richtlinie an einen virtuellen Server für Content Switching binden.

Konfigurieren einer Aktion, die den Namen des virtuellen Ziel-Lastausgleichsservers angibt

Wenn Sie den Namen des virtuellen Ziel-Lastausgleichsservers in einer Content Switching-Aktion angeben möchten, benötigen Sie so viele Content Switching-Richtlinien wie virtuelle Ziel-Lastausgleichsserver. Entscheidungen Content Switching basieren in diesem Fall auf der Regel in der Content Switching-Richtlinie, und die Aktion gibt lediglich den virtuellen Ziel-Lastausgleichsserver an. Wenn eine Anforderung mit der Richtlinie übereinstimmt, wird die Anforderung an den angegebenen virtuellen Lastausgleichsserver weitergeleitet.

So erstellen und überprüfen Sie über die CLI eine Content Switching-Aktion, die den Namen des virtuellen Ziel-Lastausgleichsservers angibt

Geben Sie in der Befehlszeile Folgendes ein:

```
add cs action <name> -targetLBVserver <string> [-comment <string>]

show cs action <name>
<!--NeedCopy-->
```

Beispiel:

```
> add cs action mycsaction -targetLBVserver mylbvserver -comment "
    Forwards requests to mylbvserver."
 Done
```



```
> show cs action mycsaction
    Name: mycsaction
    Target LB Vserver: mylbvserver
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0
    Comment: "Forwards requests to mylbvserver."

 Done
>
<!--NeedCopy-->
```

So konfigurieren Sie über die GUI eine Content Switching-Aktion, die den Namen des virtuellen Ziel-Lastausgleichsservers angibt

1. Gehen Sie zu **Traffic Management > Content Switching > Aktionen**.
2. Konfigurieren Sie eine Content Switching-Aktion und geben Sie den Namen des virtuellen Ziel-Lastausgleichsservers an.

Konfigurieren einer Aktion, die einen Ausdruck für die Auswahl des Ziels zur Laufzeit angibt

Wenn Sie einen anforderungsbasierten Ausdruck konfigurieren, der den Namen des virtuellen Ziel-Lastausgleichsservers dynamisch berechnen kann, müssen Sie nur eine Content Switching-Richtlinie konfigurieren, um den entsprechenden virtuellen Server auszuwählen. Die Regel für die Richtlinie kann ein einfaches TRUE sein (die Richtlinie entspricht allen Anforderungen), da in diesem Fall Entscheidungen zum Content Switching auf dem Ausdruck in der Aktion basieren. Indem Sie einen Ausdruck in einer Aktion konfigurieren, können Sie die Größe Ihrer Content Switching-Konfiguration drastisch reduzieren.

Wenn Sie einen anforderungsbasierten Ausdruck für die Berechnung des Namens des virtuellen Ziel-Lastausgleichsservers zur Laufzeit konfigurieren, müssen Sie sorgfältig überlegen, wie die virtuellen Lastausgleichsserver in der Konfiguration benannt werden. Sie müssen in der Lage sein, ihre Namen mithilfe des anforderungsbasierten Richtlinienausdrucks in der Aktion abzuleiten.

Wenn Sie beispielsweise Anforderungen basierend auf dem URL-Suffix (Erweiterung der angeforderten Ressource) wechseln, können Sie beim Benennen der virtuellen Lastausgleichsserver die Konvention befolgen, das URL-Suffix an eine vorgegebene Zeichenfolge anzuhängen, `mylb_`z. Beispielsweise können virtuelle Lastenausgleichsserver für HTML-Seiten `mylb_html` und `mylb_pdf` PDF-Dateien benannt werden bzw. In diesem Fall lautet die Regel, die Sie in der Aktion zum Content Switching verwenden können, um den entsprechenden virtuellen Lastausgleichsserver auszuwählen `"mylb_"+HTTP.REQ.URL.SUFFIX`. Wenn der virtuelle Server für die Content Switching eine

Anforderung für eine HTML-Seite erhält, wird der Ausdruck zurückgegeben `mylb_html`, und die Anforderung wird auf den virtuellen Server umgestellt `mylb_html`.

So erstellen Sie über die CLI eine Content Switching-Aktion, die einen Ausdruck angibt

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Content Switching-Aktion zu erstellen, die einen Ausdruck angibt und die Konfiguration überprüft:

```
add cs action <name> -targetVserverExpr <expression>) [-comment <string
    >]

show cs action <name>
<!--NeedCopy-->
```

Beispiel:

```
> add cs action mycsaction1 -targetvserverExpr '"mylb_" + HTTP.REQ.URL.
    SUFFIX'
 Done
> show cs action mycsaction1
    Name: mycsaction1
    Target Vserver Expression: "mylb_" + HTTP.REQ.URL.SUFFIX
    Target LB Vserver: No_Target
                ...
 Done
>
<!--NeedCopy-->
```

So konfigurieren Sie eine Content Switching-Aktion, die über die GUI einen Ausdruck angibt

1. Gehen Sie zu **Traffic Management > Content Switching > Aktionen**.
2. Konfigurieren Sie eine Content Switching-Aktion und geben Sie einen Ausdruck an, der den Namen des virtuellen Ziel-Lastausgleichsservers dynamisch berechnet.

Konfigurieren von Richtlinien für Content Switching

Eine Content Switching-Richtlinie definiert eine Art von Anforderung, die an einen virtuellen Lastausgleichsserver gerichtet werden soll. Diese Richtlinien werden in der Reihenfolge der ihnen zugewiesenen Prioritäten oder (wenn Sie klassische NetScaler-Richtlinien verwenden und beim Binden keine Prioritäten zuweisen) in der Reihenfolge angewendet, in der die Richtlinien erstellt wurden.

> **Hinweis**
>
> **URL** - und **Domain-Parameter** sind veraltet und werden ab Version 13.1 nicht mehr unterstützt. Verwenden Sie die Standardrichtlinienausdrücke (Advanced). Das nspepi-Dienstprogramm kann bei der Konvertierung hilfreich sein.

Die Richtlinien:

- **Regelbasierte Richtlinien.** Die Appliance vergleicht eingehende Daten mit Ausdrücken, die in den Richtlinien angegeben sind. Sie erstellen regelbasierte Richtlinien, indem Sie entweder einen klassischen Ausdruck oder einen erweiterten Richtlinienausdruck verwenden. Sowohl klassische als auch erweiterte Richtlinien werden für regelbasierte Content Switching-Richtlinien unterstützt.

  > **Hinweis**
  >
  > Eine regelbasierte Richtlinie kann mit einer optionalen Aktion konfiguriert werden. Eine Richtlinie mit einer Aktion kann an mehrere virtuelle Server oder Richtlinienbeschriftungen gebunden sein.

  Wenn Sie beim Binden Ihrer Richtlinien an den virtuellen Content Switching-Server eine Priorität festlegen, werden die Richtlinien in der Reihenfolge ihrer Priorität ausgewertet. Wenn Sie beim Binden der Richtlinien keine spezifischen Prioritäten festlegen, werden die Richtlinien in der Reihenfolge ausgewertet, in der sie erstellt wurden.

Informationen zu klassischen Richtlinien und Ausdrücken von NetScaler finden Sie unter Konfigurieren klassischer Richtlinien und Ausdrücke. Informationen zu erweiterten Richtlinienrichtlinien finden Sie unter Konfigurieren erweiterter Richtlinienausdrücke.

So erstellen Sie eine Content Switching-Richtlinie mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add cs policy <policyName> -rule <RULEValue>

add cs policy <policyName> -rule <RULEValue> -action <actionName>
<!--NeedCopy-->
```

Beispiel:

```
add cs policy policy-CS-1 -rule "HTTP.REQ.URL.PATH.EQ("http://abcd.com
    ")"

add cs policy policy-CS-4 -rule "HTTP.REQ.HOSTNAME.EQ("example.com")"

add cs policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(24).EQ(10.217.84.0)"
```



```
6
7  add cs policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2009 Nov,GMT 2009 Dec)"
8
9  add cs policy-CS-3 -rule "http.req.method.eq(GET)" -action act1
10 <!--NeedCopy-->
```

So benennen Sie eine Content Switching-Richtlinie über die CLI um

Geben Sie in der Befehlszeile Folgendes ein:

```
1  rename cs policy <policyName> <newName>
2  <!--NeedCopy-->
```

Beispiel:

```
1  rename cs policy myCSPolicy myCSPolicy1
2  <!--NeedCopy-->
```

So benennen Sie eine Content Switching-Richtlinie über die GUI um

Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**, wählen Sie eine Richtlinie aus und wählen Sie in der Liste Aktion die Option Umbenennen aus.

So erstellen Sie über die GUI eine Content Switching-Richtlinie

1. Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**, und klicken Sie auf **Hinzufügen**.
2. Füllen Sie die entsprechenden Felder aus und klicken Sie auf **Erstellen**.

Konfigurieren von Content Switching-Policy Labels

Ein Policy Label ist ein benutzerdefinierter Bindepunkt, an den Richtlinien gebunden sind. Wenn ein Policy Label aufgerufen wird, werden alle an sie gebundenen Richtlinien in der Reihenfolge der Priorität ausgewertet, die Sie ihnen zugewiesen haben. Ein Policy Label kann eine oder mehrere Richtlinien enthalten, von denen jeder ein eigenes Ergebnis zugewiesen werden kann. Eine Übereinstimmung mit einer Policy Label im Richtlinienlabel kann dazu führen, dass mit der nächsten Policy Label fortgefahren wird, ein anderes Richtlinienlabel oder eine entsprechende Ressource aufgerufen wird oder die Richtlinienbewertung sofort beendet und die Kontrolle an die Policy Label zurückgegeben wird, die das Richtlinienlabel aufgerufen hat. Sie können nur Richtlinienbeschriftungen für erweiterte Richtlinienrichtlinien erstellen.

Ein Policy Label für den Content Switching besteht aus einem Namen, einem Labeltyp und einer Liste von Richtlinien, die an das Policy Label gebunden sind. Der Richtlinienbeschriftungstyp gibt das Protokoll an, das den an das Label gebundenen Richtlinien zugewiesen wurde. Sie muss mit dem Diensttyp des virtuellen Content Switching-Servers übereinstimmen, an den die Policy Label gebunden ist, die die Richtlinienbezeichnung aufruft. Beispielsweise können Sie TCP-Nutzlastrichtlinien nur an eine Policy Label vom Typ TCP binden. Das Binden von TCP-Payload-Richtlinien an ein Policy Label vom Typ HTTP wird nicht unterstützt.

Jede Policy Label in einer Richtlinienbezeichnung für den Content Switching ist entweder einem Ziel zugeordnet (was der Aktion entspricht, die anderen Arten von Richtlinien zugeordnet ist, z. B. Rewrite- und Responder-Richtlinien) oder einer GoToPriorityExpression-Option und einer Aufrufoption. Das heißt, für eine bestimmte Policy Label in einer Richtlinienbezeichnung für Content Switching können Sie ein Ziel angeben, oder Sie können die Option gotoPriorityExpression und die Aufrufoption festlegen. Wenn mehrere Richtlinien als wahr bewertet werden, wird nur das Ziel der letzten Richtlinie berücksichtigt, die als wahr bewertet wird.

Sie können entweder die NetScaler CLI oder die GUI verwenden, um Richtlinienbeschriftungen für den Content Switching zu konfigurieren. In der NetScaler CLI erstellen Sie zunächst ein Policy Label mithilfe des Befehls cs Policy Label hinzufügen. Dann binden Sie Richtlinien mithilfe des Befehls bind cs Policy Label an die Richtlinienbezeichnung, eine Policy Label nach der anderen. In der NetScaler GUI führen Sie beide Aufgaben in einem einzigen Dialogfeld aus.

So erstellen Sie über die CLI ein Policy Label für den Content Switching

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add cs policylabel <labelName> <cspolicylabelTypetype>`
2 <!--NeedCopy-->
```

Beispiel:

```
1 add cs policylabel testpollab http
2 <!--NeedCopy-->
```

So benennen Sie ein Policy Label für den Content Switching über die CLI um

Geben Sie in der Befehlszeile Folgendes ein:

```
1 rename cs policylabel <labelName> <newName>`
2 <!--NeedCopy-->
```

Beispiel:


```
rename cs policylabel oldPolicyLabelName newPolicyLabelName
<!--NeedCopy-->
```

So benennen Sie ein Policy Label für den Content Switching über die GUI um

Navigieren Sie zu **Traffic Management > Content Switching > Policy-Labels**, wählen Sie ein Policy Label aus und wählen Sie in der Liste Aktion die Option Umbenennen

So binden Sie eine Policy Label über die CLI an ein Richtlinienlabel für den Content Switching

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Policy Label an ein Richtlinienlabel zu binden und die Konfiguration zu überprüfen:

```
bind cs policylabel <labelName> <policyName> <priority>[-targetVserver
    <string>] | [-gotoPriorityExpression <expression>] | [-invoke <
    labeltype> <labelName>] ]

show cs policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
bind cs policylabel testpollab test_Pol 100 -targetVserver LBVIP
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 1
        Number of times invoked: 0
        Policy Name: test_Pol
        Priority: 100
        Target Virtual Server: LBVIP
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn eine Richtlinie mit einer Aktion konfiguriert ist, werden der virtuelle Zielserver (TargetVServer), zum Prioritätsausdruck (gotoPriorityExpression) und Parameter aufrufen (aufrufen) nicht erforderlich. Wenn eine Richtlinie nicht mit einer Aktion konfiguriert ist, müssen Sie mindestens einen der folgenden Parameter konfigurieren: targetVServer, gotoPriorityExpression und invoke.

So lösen Sie ein Policy Label über die CLI von einem Richtlinienlabel

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer Policy Label von einem Richtlinienlabel zu lösen und die Konfiguration zu überprüfen:

```
unbind cs policylabel <labelName> <policyName>

show cs policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
unbind cs policylabel testpollab test_Pol
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 0
        Number of times invoked: 0
<!--NeedCopy-->
```

So entfernen Sie ein Policy Label über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
rm cs policylabel <labelName>
<!--NeedCopy-->
```

So verwalten Sie ein Policy Label für Content Switching über die GUI

Navigieren Sie zu **Traffic Management > Content Switching > Richtlinienbeschriftungen**, konfigurieren Sie eine Richtlinienbezeichnung, binden Sie Richtlinien an das Label und geben Sie optional eine Priorität, einen GoToPriority-Ausdruck und eine Aufrufoption an.

Binden von Richtlinien an einen virtuellen Content Switching Server

Nachdem Sie den virtuellen Server und die Richtlinien für Content Switching erstellt haben, binden Sie jede Richtlinie an den virtuellen Content Switching-Server. Wenn Sie die Richtlinie an den virtuellen Server für die Content Switching binden, geben Sie den virtuellen Ziel-Lastausgleichsserver an.

> **Hinweis**
>
> Wenn Ihre Richtlinie Content Switching eine erweiterte Richtlinienregel verwendet, können Sie

> eine Aktion zum Content Switching für die Richtlinie konfigurieren. Wenn Sie eine Aktion konfigurieren, müssen Sie den virtuellen Ziel-Lastausgleichsserver angeben, wenn Sie die Aktion konfigurieren, und nicht, wenn Sie die Richtlinie an den virtuellen Server für die Content Switching binden. Weitere Informationen zum Konfigurieren einer Content Switching-Aktion finden Sie im Abschnitt
> Konfigurieren einer Content Switching-Aktion.

So binden Sie eine Richtlinie an einen virtuellen Content Switching-Server und wählen über die CLI einen virtuellen Ziel-Lastausgleichsserver aus

Geben Sie in der Befehlszeile Folgendes ein:

```
bind cs vserver <name>[-lbvserver<string> -targetLBVServer<string> -
    policyname <string> -priority <positive_integer>] [-
    gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )]
    [-invoke (<labelType> <labelName>)]
<!--NeedCopy-->
```

Beispiel:

```
bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -
    gotoPriorityExpression NEXT

bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -
    gotoPriorityExpression
'q.header("a").count' -flowtype REQUEST -invoke policylabel label1

bind cs vserver Vserver-CS-1 Vserver-LB-1 -policyname Policy-CS-1 -
    priority 20
<!--NeedCopy-->
```

> **Hinweis**
>
> Die Parameter, der virtuelle Ziel-Lastausgleichsserver (TargetVServer), gehen zum Prioritätsausdruck (gotoPriorityExpression) und die Aufrufmethode (aufrufen) können nicht verwendet werden, wenn eine Richtlinie eine Aktion hat.

So binden Sie eine Richtlinie an einen virtuellen Content Switching-Server und wählen über die GUI einen virtuellen Ziel-Lastausgleichsserver aus

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, öffnen Sie einen virtuellen Server, und binden Sie im Abschnitt

Content Switching-Richtlinienbindung eine Richtlinie an den virtuellen Server, und geben Sie einen virtuellen Ziel-Lastausgleichsserver an.

Konfigurieren der richtlinienbasierten Protokollierung für Content Switching

Sie können richtlinienbasierte Protokollierung für eine Richtlinie zum Content Switching konfigurieren. Mit der richtlinienbasierten Protokollierung können Sie ein Format für Protokollnachrichten angeben. Der Inhalt der Protokollnachricht wird mithilfe eines erweiterten Richtlinienausdrucks in der Richtlinie zum Content Switching definiert. Wenn die in der Richtlinie angegebene Aktion zum Content Switching ausgeführt wird, erstellt die NetScaler-Appliance die Protokollnachricht aus dem Ausdruck und schreibt die Nachricht in die Protokolldatei. Die richtlinienbasierte Protokollierung ist besonders nützlich, wenn Sie eine Konfiguration testen und Fehler beheben möchten, in der Content Switching-Aktionen den virtuellen Ziel-Lastausgleichsserver zur Laufzeit identifizieren.

> **Hinweis**
>
> Wenn mehrere an einen bestimmten virtuellen Server gebundene Richtlinien auf TRUE ausgewertet werden und mit einer Überwachungsnachrichtenaktion konfiguriert sind, führt die NetScaler-Appliance nicht alle Überwachungsmeldungsaktionen aus. Es führt nur die Aktion der Überwachungsnachricht aus, die für die Richtlinie konfiguriert ist, deren Content Switching-Aktion ausgeführt wird.

Um die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie zu konfigurieren, müssen Sie zunächst eine Auditbenachrichtigungsaktion konfigurieren. Weitere Informationen zum Konfigurieren einer Überwachungsnachrichtenaktion finden Sie unter Konfigurieren der NetScaler-Appliance für die Überwachungsprotokollierung. Nachdem Sie die Auditbenachrichtigungsaktion konfiguriert haben, geben Sie die Aktion in einer Content Switching-Richtlinie an.

So konfigurieren Sie die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie über die CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
set cs policy <policyName> -logAction <string>

show cs policy <policyName>
<!--NeedCopy-->
```

Beispiel:

```
> set cs policy cspol1 -logAction csLogAction
 Done
```



```
> show cs policy cspol1

    Policy: cspol1  Rule: TRUE  Action: csact1
    LogAction: csLogAction
    Hits: 0

1)  CS Vserver: csvs1
    Priority: 10
 Done
>
<!--NeedCopy-->
```

So konfigurieren Sie die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie über die GUI

Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**, öffnen Sie eine Richtlinie und wählen Sie in der Liste Protokollaktion eine Protokollaktion für die Richtlinie aus.

Überprüfung der Konfiguration

Um zu überprüfen, ob Ihre Content Switching-Konfiguration korrekt ist, müssen Sie die Content Switching-Entitäten anzeigen. Um den ordnungsgemäßen Betrieb zu überprüfen, nachdem Ihre Content Switching-Konfiguration bereitgestellt wurde, können Sie die Statistiken anzeigen, die beim Zugriff auf die Server generiert werden.

Anzeigen der Eigenschaften von virtuellen Content Switching-Servern

Sie können die Eigenschaften von virtuellen Content Switching-Servern anzeigen, die Sie auf der NetScaler-Appliance konfiguriert haben. Sie können die Informationen verwenden, um zu überprüfen, ob der virtuelle Server korrekt konfiguriert ist, und gegebenenfalls zur Fehlerbehebung. Zusätzlich zu Details wie Name, IP-Adresse und Port können Sie die verschiedenen Richtlinien, die an einen virtuellen Server gebunden sind, und seine Verkehrsverwaltungseinstellungen anzeigen.

Die Richtlinien für den Content Switching werden in der Reihenfolge ihrer Priorität angezeigt. Wenn mehr als eine Richtlinie dieselbe Priorität hat, werden sie in der Reihenfolge angezeigt, in der sie an den virtuellen Server gebunden sind.

> **Hinweis**
>
> Wenn Sie den virtuellen Server für die Content Switching so konfiguriert haben, dass Datenverkehr an einen virtuellen Lastausgleichsserver weitergeleitet wird, können Sie die Richtlinien für die Content Switching auch anzeigen, indem Sie die Eigenschaften des virtuellen Lastausgle-

> ichsservers anzeigen.

So zeigen Sie die Eigenschaften von virtuellen Content Switching-Servern über die CLI an

Um grundlegende Eigenschaften aller virtuellen Content Switching-Server in Ihrer Konfiguration oder detaillierte Eigenschaften eines bestimmten virtuellen Content Switching-Servers aufzulisten, geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
show cs vserver

show cs vserver <name>
<!--NeedCopy-->
```

Beispiel

```
1.
show cs vserver Vserver-CS-1
Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
Last state change was at Thu Jun 30 10:48:59 2011
Time since last state change: 6 days, 20:03:00.760
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
Default: Content Precedence: RULE
Vserver IP and Port insertion: OFF
Case Sensitivity: ON
Push: DISABLED Push VServer:
Push Label Rule: none

...
1) Policy : __ESNS_PREBODY_POLICY Priority:0
2) Policy : __ESNS_POSTBODY_POLICY Priority:0

1) Compression Policy Name: __ESNS_CMP_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

2) Rewrite Policy Name: __ESNS_REWRITE_POLICY Priority: 2147483647
GotoPriority Expression: END
```



```
Flowtype: REQUEST

3) Cache Policy Name: dfbx Priority: 10
GotoPriority Expression: END
Flowtype: REQUEST

4) Responder Policy Name: __ESNS_RESPONDER_POLICY Priority: 2147483647
GotoPriority Expression: END

1) Policy: wiki Target: LBVIP2 Priority: 25 Hits: 0
2) Policy: plain Target: LBVIP1 Priority: 90 Hits: 0
3) Policy: DispOrderTest2 Target: KerbAuthLBVS Priority: 91 Hits: 0
4) Policy: test_Pol Target: LBVIP1 Priority: 92 Hits: 0
5) Policy: PolicyNameTesting Target: LBVIP1 Priority: 100 Hits: 0
 Done
>

show cs vserver
1) Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
…
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED

2) apubendpt (10.111.111.1:80) - HTTP Type: CONTENT
State: UP
…
Client Idle Timeout: 180 sec
Down state flush: DISABLED
…

3) apubendpt1 (10.111.111.2:80) - HTTP Type: CONTENT
State: UP
…
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
…
<!--NeedCopy-->
```


Richtlinien für Content Switching anzeigen

Sie können die Eigenschaften der von Ihnen definierten Content Switching-Richtlinien anzeigen, z. B. den Namen, die Domäne und die URL oder den Ausdruck, und die Informationen verwenden, um Fehler in der Konfiguration zu finden oder um zu beheben, ob etwas nicht so funktioniert, wie es muss.

So zeigen Sie die Eigenschaften von Content Switching-Richtlinien über die CLI an

Um entweder die grundlegenden Eigenschaften aller Content Switching-Richtlinien in Ihrer Konfiguration oder die detaillierten Eigenschaften einer bestimmten Content Switching-Richtlinie aufzulisten, geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
show cs policy

show cs policy <PolicyName>
<!--NeedCopy-->
```

Beispiel:

```
show cs policy

show cs policy-CS-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften von Content Switching-Richtlinien über die GUI an

Navigieren Sie zu **Traffic Management** > **Content Switching** > **Richtlinien**, wählen Sie eine Richtlinie aus und wählen Sie in der Liste Aktion die Option **Bindungen anzeigen**aus.

Anzeigen einer Konfiguration eines virtuellen Content Switching-Servers mithilfe des Visualizers

Der Content Switching Visualizer ist ein Tool, mit dem Sie eine Content Switching-Konfiguration im grafischen Format anzeigen können. Sie können den Visualizer verwenden, um die folgenden Konfigurationselemente anzuzeigen:

- Eine Zusammenfassung der virtuellen Lastausgleichsserver, an die der virtuelle Content Switching-Server gebunden ist.
- Alle Dienste und Dienstgruppen, die an den virtuellen Lastausgleichsserver gebunden sind, und alle Monitore, die an die Dienste gebunden sind.
- Die Konfigurationsdetails eines beliebigen angezeigten Elements.

- Alle Richtlinien, die an den virtuellen Server für die Content Switching gebunden sind. Diese Richtlinien müssen keine Richtlinien für den Content Switching sein. Viele Arten von Richtlinien, wie z. B. Richtlinien zum Rewrite, können an einen virtuellen Content Switching-Server gebunden werden.

Nachdem Sie die verschiedenen Elemente in einem Content Switching- und Load-Balancing-Setup konfiguriert haben, können Sie die gesamte Konfiguration in eine Anwendungsvorlagendatei exportieren.

> **Hinweis**
>
> Der Visualizer benötigt eine grafische Oberfläche, sodass er nur über die GUI verfügbar ist.

So zeigen Sie eine Content Switching-Konfiguration mithilfe des Visualizers in der GUI an

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf **Visualizer**.
3. Im Fenster **Content Switching Visualizer** können Sie den sichtbaren Bereich wie folgt anpassen:
   - Klicken Sie auf die Symbole **Vergrößern** und **Verkleinern**, um den sichtbaren Bereich zu vergrößern oder zu verkleinern.
   - Klicken Sie auf das Symbol **Bild speichern**, um das Diagramm als Bilddatei zu speichern.
   - Beginnen Sie im Textfeld Suchen mit der Eingabe des Namens des gesuchten Elements. Wenn Sie genug Zeichen eingegeben haben, um das Objekt zu identifizieren, wird dessen Position hervorgehoben. Um die Suche einzuschränken, klicken Sie auf das Dropdown-Menü und wählen Sie den Elementtyp aus, nach dem Sie suchen möchten.
4. Um Konfigurationsdetails für Entitäten anzuzeigen, die an diesen virtuellen Server gebunden sind, können Sie Folgendes tun:
   - Um Richtlinien anzuzeigen, die an den virtuellen Server gebunden sind, wählen Sie in der Symbolleiste oben im Dialogfeld ein oder mehrere funktionsspezifische Richtliniensymbole aus. Wenn Richtlinienbeschriftungen konfiguriert sind, werden sie im Hauptansichtsbereich angezeigt.
   - Um die Konfigurationsdetails für einen gebundenen Dienst oder eine gebundene Dienstgruppe anzuzeigen, klicken Sie auf das Symbol für den Dienst, klicken Sie auf die Registerkarte Zugehörige Aufgaben und dann auf Mitgliederdienste anzeigen.
   - Um die Konfigurationsdetails für einen Monitor anzuzeigen, klicken Sie auf das Symbol für den Monitor, klicken Sie auf die Registerkarte **Zugehörige Aufgaben** und dann auf **Monitor anzeigen**.

5. Um detaillierte Statistiken für einen virtuellen Server in der Content Switching-Konfiguration anzuzeigen, klicken Sie auf den virtuellen Server, für den Sie Statistiken anzeigen möchten, klicken Sie dann auf die Registerkarte Zugehörige Aufgaben und dann auf **Statistiken**.
6. Um eine vergleichende Liste der Parameter anzuzeigen, deren Werte sich für einen virtuellen Lastausgleichsserver unterscheiden oder nicht über Service-Container hinweg definiert sind, klicken Sie auf das Symbol für einen Container, klicken Sie auf die Registerkarte **Zugehörige Aufgaben**, und klicken Sie dann auf **Service-Attribut-Diff**.
7. Um die Details zur Monitor-Bindung für die Dienste in einem Container anzuzeigen, klicken Sie im Dialogfeld "Service-Attribut-Diff" in der Spalte Gruppe für den Container auf **Details**. Mithilfe dieser Vergleichsliste können Sie ermitteln, welcher Service-Container die Konfiguration hat, die Sie auf alle Service-Container anwenden möchten.
8. Um die Anzahl der Anfragen anzuzeigen, die zu einem bestimmten Zeitpunkt von den virtuellen Servern in der Konfiguration pro Sekunde empfangen wurden, und die Anzahl der Auswahlen pro Sekunde zu einem bestimmten Zeitpunkt für Rewrite-, Responder- und Cache-Richtlinien, klicken Sie auf Statistiken anzeigen. Die statistischen Informationen werden auf den jeweiligen Knoten im Visualizer angezeigt. Diese Informationen werden nicht in Echtzeit aktualisiert. Es wird manuell aktualisiert. Um die Informationen zu aktualisieren, klicken Sie auf Statistiken aktualisieren.

   > **Hinweis**
   >
   > Diese Option ist nur für NetScaler NCore-Builds verfügbar.

9. Um Konfigurationsdetails für ein Element in ein Dokument oder eine Tabelle zu kopieren, klicken Sie auf das Symbol für dieses Element, klicken Sie auf Zugehörige Aufgaben, klicken Sie auf Eigenschaften kopieren, und fügen Sie die Informationen dann in ein Dokument ein.
10. Um die gesamte Konfiguration, die im Visualizer angezeigt wird, in eine Anwendungsvorlagendatei zu exportieren, klicken Sie auf das Symbol für den virtuellen Content Switching-Server, klicken Sie auf Verwandte Aufgaben und dann auf Vorlage erstellen. Beim Erstellen der Anwendungsvorlage können Sie Variablen in einigen Richtlinienausdrücken und -aktionen konfigurieren. Weitere Informationen zum Erstellen der Anwendungsvorlagendatei und zum Konfigurieren von Variablen für eine Vorlage finden Sie unter AppExpert.

Anpassen der grundlegenden Content Switching-Konfiguration

September 18, 2023

Nachdem Sie ein grundlegendes Content Switching-Setup konfiguriert haben, müssen Sie es möglicherweise an Ihre Anforderungen anpassen. Sie können virtuelle HTTP- und SSL-Content

Switching-Server so konfigurieren, dass sie mehrere Ports abhören, anstatt separate virtuelle Server zu erstellen. Wenn Sie Content Switching für ein bestimmtes virtuelles LAN konfigurieren möchten, können Sie einen virtuellen Content Switching-Server mit einer Listen-Richtlinie konfigurieren.

Unterstützung für mehrere Ports für virtuelle HTTP- und SSL-Typ-Content Switching-Server

Sie können NetScaler so konfigurieren, dass virtuelle HTTP- und SSL-Content Switching-Server auf mehreren Ports abhören, ohne separate virtuelle Server konfigurieren zu müssen. Diese Funktion ist besonders nützlich, wenn Sie eine Entscheidung zum Umschalten Content Switching auf einen Teil der URL und anderer L7-Parameter stützen möchten. Anstatt mehrere virtuelle Server mit derselben IP-Adresse und verschiedenen Ports zu konfigurieren, können Sie eine IP-Adresse konfigurieren und den Port als * angeben. Infolgedessen wird auch die Konfigurationsgröße reduziert.

So konfigurieren Sie einen virtuellen HTTP- oder SSL-Content Switching-Server für das Abhören mehrerer Ports mithilfe der Befehlszeile

Geben Sie an der Befehlszeile Folgendes ein:

```
add cs vserver \<name\> \<serviceType\> \<IPAddress\> Port \*
```

Beispiel

```
> add cs vserver cs1 HTTP 10.102.92.215 *
 Done
> sh cs vserver cs1
        cs1 (10.102.92.215:*) - HTTP    Type: CONTENT
        State: UP
        Last state change was at Tue May 20 01:15:49 2014
        Time since last state change: 0 days, 00:00:03.270
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Vserver IP and Port insertion: OFF
        L2Conn: OFF     Case Sensitivity: ON
        Authentication: OFF
        401 Based Authentication: OFF
        Push: DISABLED  Push VServer:
        Push Label Rule: none
```



```
21          IcmpResponse: PASSIVE
22          RHIstate:  PASSIVE
23          TD: 0
24   Done
25 <!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen HTTP- oder SSL-Content Switching-Server für das Abhören mehrerer Ports mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und erstellen Sie einen virtuellen Server vom Typ HTTP oder SSL.
2. Verwenden Sie ein Sternchen (*), um den Port anzugeben.

Konfigurieren von virtuellen Per-VLAN-Platzhalter-Servern

Wenn Sie Content Switching für den Datenverkehr in einem bestimmten VLAN konfigurieren möchten, können Sie einen virtuellen Platzhalterserver mit einer Listen-Richtlinie erstellen, die ihn auf die Verarbeitung des Datenverkehrs nur im angegebenen VLAN beschränkt.

So konfigurieren Sie einen virtuellen Platzhalterserver, der über die Befehlszeile ein bestimmtes VLAN abhört

Geben Sie an der Befehlszeile Folgendes ein:

```
1 add cs vserver \<name\> \<serviceType\> IPAddress `* Port *` -
     listenpolicy \<expression\> \[-listenpriority \<positive\_integer
     \>\]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add cs vserver Vserver-CS-vlan1 ANY * *
2 -listenpolicy "CLIENT.VLAN.ID.EQ(2)"  -listenpriority 10
3 <!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Platzhalterserver, der mithilfe des Konfigurationsdienstprogramms ein bestimmtes VLAN abhört

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und konfigurieren Sie einen virtuellen Server. Geben Sie eine Listenrichtlinie an, die darauf beschränkt, Datenverkehr nur im angegebenen VLAN zu verarbeiten.

Nachdem Sie diesen virtuellen Server erstellt haben, binden Sie ihn an einen oder mehrere Dienste, wie unter Basic Load Balancing einrichtenbeschrieben.

Konfigurieren der Microsoft SQL Server-Versionseinstellung

Sie können die Version von Microsoft® SQL Server® für einen virtuellen Content Switching-Server vom Typ MSSQL angeben. Die Versionseinstellung wird empfohlen, wenn Sie erwarten, dass einige Clients nicht dieselbe Version wie Ihr Microsoft SQL Server-Produkt ausführen. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht.

So stellen Sie den Versionsparameter von Microsoft SQL Server über die Befehlszeile ein

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Microsoft SQL Server-Versionsparameter für einen virtuellen Content Switching-Server festzulegen und die Konfiguration zu überprüfen:

- `set cs vserver \<name\> -mssqlServerVersion \<mssqlServerVersion\>`
- `show cs vserver \<name\>`

Beispiel

```
1 > set cs vserver myMSSQLcsvip -mssqlServerVersion 2008R2 Done > show cs
      vserver myMSSQLcsvip myMSSQLcsvip (192.0.2.13:1433) - MSSQL Type:
     CONTENT State: UP . . . . . MSsql Server Version: 2008R2 . . . . .
      . Done >
2 <!--NeedCopy-->
```

So legen Sie den Versionsparameter von Microsoft SQL Server mithilfe des Konfigurationsdienstprogramms fest

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MSSQL an.
2. Geben Sie **unter Erweiterte Einstellungen**die **Serverversion**an.

Aktivieren Sie die externe Zustandsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server

In Public Clouds können Sie die NetScaler-Appliance als Lastausgleichsdienst der zweiten Ebene verwenden, wenn der native Load Balancer als erste Stufe verwendet wird. Der native Load Balancer

kann ein Application Load Balancer (ALB) oder ein Netzwerklastenausgleichsmodul (NLB) sein. Die meisten Public Clouds unterstützen keine UDP Health Probes in ihren nativen Load Balancern. Wenn diese Server ausgefallen sind, wird ihr aktueller Status daher möglicherweise nicht aktualisiert. Infolgedessen wird der Datenverkehr bedingungslos an NetScaler gesendet, auch wenn die Anforderung nicht bearbeitet werden kann. Um den Zustand solcher Anwendungen zu überwachen, unterstützt NetScaler HTTP- und TCP-Integritätsprüfungen.

Ein HTTP- oder TCP-Listener wird für einen virtuellen Content Switching-Server erstellt, wenn `probeProtocol` sowohl die als auch die `probePort` Parameter konfiguriert sind. Der Listener spiegelt den Status des virtuellen Servers wider. Der Parameter ProbeSuccessResponseCode‘ gilt nur für HTTP und gibt die konfigurierte Zeichenfolge zurück, wenn der Test erfolgreich ist.

So aktivieren Sie die externe Integritätsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine externe TCP-Integritätsprüfung mit der Option TCPProbePort zu aktivieren:

```
add cs vserver <name> <protocol> <IPAddress> <port> -ProbeProtocol <
    Http/TCP> -ProbePort <port-num> -ProbeSuccessResponseCode<http-code>
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver Vserver-CS-1 HTTP 10.102.29.161 5002 -ProbeProtocol HTTP
    -probeport 5000 -probesuccessResponseCode 200OK
<!--NeedCopy-->
```

So aktivieren Sie die externe Integritätsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und erstellen Sie dann einen virtuellen Server.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Server zu erstellen.
3. Aktualisieren Sie im Bereich **Grundeinstellungen** die folgenden Details:
   a) Prüfprotokoll — Wählen Sie das Protokoll (HTTP oder TCP) der Sonde für die externe Zustandsprüfung des virtuellen Servers aus.
   b) Test Success Response Code — Geben Sie die Antwortzeichenfolge für eine erfolgreiche Prüfung ein. Dieser Parameter gilt nur für das HTTP-Protokoll.
      - Standardwert: 200ok
      - Maximale Länge: 63

c) Probe Port — Geben Sie die Portnummer für die HTTP- oder TCP-Überwachung ein.

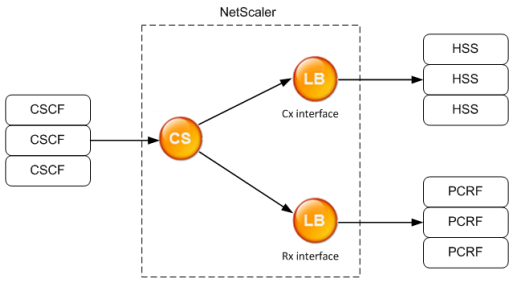
4. Klicken Sie auf **OK**.

Content Switching für das Diameter-Protokoll

May 11, 2023

Für den Datenverkehr im Diameter-Protokoll können Sie die NetScaler-Appliance (oder virtuelle Appliance) so konfigurieren, dass sie als Relay-Agent fungiert, der auf der Grundlage des Nachrichteninhalts (AVP-Wert in der Nachricht) ein Paket ausgleicht und an das entsprechende Ziel weiterleitet. Da die Appliance keine Verarbeitung auf Anwendungsebene durchführt, stellt sie Relaying-Dienste für alle Diameter-Anwendungen bereit, wie in den konfigurierten Content Switching-Richtlinien angegeben. Daher gibt die Appliance die Relay-Anwendungs-ID in der CEA-Nachricht (Capability Exchange Answer) an, wenn der Client eine Durchmesserverbindung herstellt. Sie müssen einen virtuellen Content Switching-Server, virtuelle Server für den Lastenausgleich und Dienste konfigurieren, die den Durchmesserknoten entsprechen. Wenn eine Anfrage den virtuellen Content Switching-Server erreicht, wendet der virtuelle Server die Content Switching-Richtlinien an, die mit dieser Art von Anfrage verknüpft sind. Nach der Auswertung der Richtlinien leitet der virtuelle Content Switching-Server die Anforderung an den entsprechenden virtuellen Lastausgleichsserver weiter, der sie an den entsprechenden Dienst sendet.

Eine Durchmesserschnittstelle stellt eine Verbindung zwischen den Knoten mit unterschiedlichen Durchmessern her. Die folgende Beispielbereitstellung verwendet Cx- und Rx-Schnittstellen. Eine Cx-Schnittstelle stellt eine Verbindung zwischen einem CSCF und einem HSS her. Eine Rx-Schnittstelle stellt eine Verbindung zwischen einem CSCF und einem PCRF her. Alle Nachrichten erreichen die NetScaler-Appliance. Je nachdem, ob die Nachricht für eine Cx- oder eine Rx-Schnittstelle bestimmt ist, und je nach den definierten Content Switching-Richtlinien wählt der NetScaler einen geeigneten Load-Balancing-Serverpool aus.



CSCF=Call Session Control Function
HSS=Home Subscriber Server
PCRF=Policy and Charging Rules Function

Beispielkonfiguration

1. Erstellen Sie für jede Entität einen Dienst, einen Load Balancing-Server, und binden Sie den Dienst an den virtuellen Server.

```
add service svc_pcrf[1-3] 1.1.1.1[1-3] DIAMETER 3868
add service svc_hss[1-3] 1.1.1.2[1-3] DIAMETER 3868
add lb vserver vs_rx DIAMETER -persistenceType DIAMETER -
    persistavpno 263
add lb vserver vs_cx DIAMETER -persistenceType DIAMETER -
    persistavpno 263
bind lb vserver vs_rx svc_pcrf[1-3]
bind lb vserver vs_cx svc_hss[1-3]
<!--NeedCopy-->
```

2. Erstellen Sie einen virtuellen Content Switching-Server und zwei Aktionen (eine für jeden virtuellen Load-Balancing-Server). Erstellen Sie zwei Content Switching-Richtlinien und binden Sie diese Richtlinien an den virtuellen Content Switching-Server, wobei Sie für jede Richtlinie eine Priorität angeben.

```
add cs vserver cs_diameter DIAMETER 10.1.1.10 3868
add cs action cx_action -targetLBVserver vs_cx
add cs action rx_action - targetLBvserver vs_rx
add cs policy cx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777216)" -action cx_action
add cs policy rx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777236)" -action rx_action
bind cs vserver cs_diameter -policyName rx_policy -priority 100
bind cs vserver cs_diameter -policyName cx_policy -priority 110
<!--NeedCopy-->
```

Schutz des Content Switching-Setups vor Ausfällen

May 11, 2023

Content Switching kann fehlschlagen, wenn der virtuelle Content Switching-Server AUSFÄLLT oder übermäßigen Datenverkehr nicht verarbeitet, oder aus anderen Gründen. Um die Wahrscheinlichkeit eines Fehlers zu verringern, können Sie die folgenden Maßnahmen ergreifen, um das Content Switching-Setup vor einem Ausfall zu schützen:

Konfiguration eines virtuellen Backup-Servers

Wenn der primäre virtuelle Content-Switching-Server als INAKTIV oder DEAKTIVIERT markiert ist, kann die NetScaler Appliance Anfragen an einen virtuellen Backup-Server für Content Switching weiterleiten. Es kann dem Kunden auch eine Benachrichtigung über den Ausfall oder die Wartung der Website senden. Der virtuelle Backup-Content-Switching-Server ist ein Proxy und für den Client transparent.

Bei der Konfiguration des virtuellen Backup-Servers können Sie den Konfigurationsparameter Primär deaktivieren bei Ausfall angeben, um sicherzustellen, dass der primäre virtuelle Server, wenn er wieder hochgefahren wird, der sekundäre Server bleibt, bis Sie ihn manuell zwingen, die Funktion des primären Servers zu übernehmen. Dies ist nützlich, wenn Sie sicherstellen möchten, dass alle Aktualisierungen der Datenbank auf dem Server für das Backup beibehalten werden, sodass Sie die Datenbanken synchronisieren können, bevor Sie den primären virtuellen Server wiederherstellen.

Sie können einen virtuellen Backup-Server für Content Switching konfigurieren, wenn Sie einen virtuellen Content Switching-Server erstellen oder wenn Sie die optionalen Parameter eines vorhandenen virtuellen Content Switching-Servers ändern. Sie können auch einen virtuellen Backup-Content-Switching-Server für einen vorhandenen virtuellen Backup-Content-Switching-Server konfigurieren und so kaskadierte virtuelle Server für den Backup Content Switching erstellen. Die maximale Tiefe virtueller Server mit kaskadierter Backup-Content-Switching-Funktion beträgt 10. Die Appliance sucht nach einem virtuellen Backup-Server für Content Switching, der aktiv ist, und greift auf diesen virtuellen Content Switching-Server zu, um die Inhalte bereitzustellen.

> **Hinweis**
>
> Wenn ein virtueller Content Switching-Server sowohl mit einem virtuellen Backup-Content-Switching-Server als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backup-Content-Switching-Server Vorrang vor der Umleitungs-URL. Die Weiterleitung wird verwendet, wenn die virtuellen Primär- und Backup-Server ausgefallen sind.

So richten Sie mithilfe der CLI einen virtuellen Backup-Content-Switching-Server ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver <name> -backupVserver <string> -disablePrimaryOnDown (ON
    |OFF)
<!--NeedCopy-->
```

Beispiel

```
set cs vserver Vserver-CS-1 -backupVserver Vserver-CS-2 -
    disablePrimaryOnDown ON
```



```
<!--NeedCopy-->
```

So richten Sie mithilfe der GUI einen virtuellen Backup-Content-Switching-Server ein

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie unter **Erweiterte Einstellungen**die Option **Schutz**aus und geben Sie einen **virtuellen Backup-Server**an.

Überschüssigen Datenverkehr auf einen virtuellen Backup-Server umleiten

Die Spillover-Option leitet neue Verbindungen, die an einem virtuellen Content Switching-Server ankommen, auf einen virtuellen Backup-Server für Content Switching um, wenn die Anzahl der Verbindungen zum virtuellen Content Switching-Server den konfigurierten Schwellenwert überschreitet. Der Schwellenwert wird dynamisch berechnet, oder Sie können den Wert festlegen. Die Anzahl der aufgebauten Verbindungen (in TCP) auf dem virtuellen Server wird mit dem Schwellenwert verglichen. Wenn die Anzahl der Verbindungen den Schwellenwert erreicht, werden neue Verbindungen zum virtuellen Backup-Content-Switching-Server umgeleitet.

Wenn die virtuellen Backup-Content-Switching-Server den konfigurierten Schwellenwert erreichen und die Last nicht aufnehmen können, leitet der primäre virtuelle Content Switching-Server alle Anfragen an die Umleitungs-URL um. Wenn auf dem primären virtuellen Content Switching-Server keine Umleitungs-URL konfiguriert ist, werden nachfolgende Anfragen verworfen.

So konfigurieren Sie einen virtuellen Content Switching-Server, um neue Verbindungen mithilfe der CLI an einen virtuellen Backup-Server umzuleiten

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver \<name\> -soMethod \<methodType\> -soThreshold \<
    thresholdValue\> -soPersistence \<persistenceValue\> -
    soPersistenceTimeout \<timeoutValue\>
<!--NeedCopy-->
```

Beispiel

```
set cs vserver Vserver-CS-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```


So richten Sie einen virtuellen Content Switching-Server so ein, dass er neue Verbindungen mithilfe der GUI an einen virtuellen Backup-Server umleitet

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie unter **Erweiterte Einstellungen**die Option **Schutz**aus und konfigurieren Sie Spillover.

Konfiguration einer Umleitungs-URL

Sie können eine Umleitungs-URL konfigurieren, um den Status der NetScaler-Appliance mitzuteilen, wenn ein virtueller Content Switching-Server vom Typ HTTP oder HTTPS AUSGEFALLEN oder DEAKTIVIERT ist. Diese URL kann lokal oder remote sein.

Umleitungs-URLs können absolute URLs oder relative URLs sein. Wenn die konfigurierte Umleitungs-URL eine absolute URL enthält, wird die HTTP-Weiterleitung an den konfigurierten Speicherort gesendet, unabhängig von der in der eingehenden HTTP-Anfrage angegebenen URL. Wenn die konfigurierte Umleitungs-URL nur den Domainnamen (relative URL) enthält, wird die HTTP-Weiterleitung an einen Standort gesendet, nachdem die eingehende URL an die in der Umleitungs-URL konfigurierte Domain angehängt wurde.

Citrix empfiehlt die Verwendung einer absoluten URL. Das heißt, eine URL, die auf/endet, zum Beispiel www.example.com/ statt einer relativen URL. Eine relative URL-Umleitung kann dazu führen, dass der Schwachstellen-Scanner einen Fehlalarm meldet.

> **Hinweis**
>
> Wenn ein virtueller Content Switching-Server sowohl mit einem virtuellen Backup-Server als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backup-Server Vorrang vor der Umleitungs-URL. Eine Umleitungs-URL wird verwendet, wenn die virtuellen Primär- und Backup-Server ausgefallen sind.

Wenn die Umleitung konfiguriert ist und der virtuelle Content Switching-Server nicht verfügbar ist, gibt die Appliance eine HTTP 302-Umleitung an den Browser des Benutzers aus.

Um mithilfe der CLI eine Umleitungs-URL für den Fall zu konfigurieren, dass der virtuelle Content Switching-Server nicht verfügbar ist

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver \<name\> -redirectURL \<URLValue\>
<!--NeedCopy-->
```


Beispiel

```
set cs vserver Vserver-CS-1 -redirectURL http://www.newdomain.com/
   mysite/maintenance
<!--NeedCopy-->
```

Um mithilfe der GUI eine Umleitungs-URL für den Fall zu konfigurieren, dass der virtuelle Content Switching-Server nicht verfügbar ist

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie unter **Erweiterte Einstellungen**die Option **Schutz**aus und geben Sie eine Umleitungs-URL an.

Konfiguration der Option zur Statusaktualisierung

Die Funktion zum Content Switching ermöglicht die Verteilung von Clientanfragen auf mehrere Server, basierend auf den spezifischen Inhalten, die den Benutzern präsentiert werden. Für ein effizientes Inhalts-Switching verteilt der virtuelle Content Switching-Server den Datenverkehr entsprechend dem Inhaltstyp auf die virtuellen Lastausgleichsserver, und die virtuellen Lastausgleichsserver verteilen den Datenverkehr gemäß der angegebenen Lastausgleichsmethode auf die physischen Server.

Für ein reibungsloses Verkehrsmanagement ist es wichtig, dass der virtuelle Content Switching-Server den Status der virtuellen Load-Balancing-Server kennt. Die Option zur Statusaktualisierung hilft dabei, den virtuellen Content Switching-Server als DOWN zu markieren, wenn der an ihn gebundene virtuelle Load-Balancing-Server als DOWN markiert ist. Ein virtueller Lastausgleichsserver wird als DOWN markiert, wenn alle an ihn gebundenen physischen Server als DOWN markiert sind.

Wenn die Statusaktualisierung deaktiviert ist:

Der Status des virtuellen Content Switching-Servers ist als AKTIV gekennzeichnet. Er bleibt aktiv, auch wenn kein virtueller Server für den gebundenen Lastausgleich aktiv ist.

Wenn die Statusaktualisierung aktiviert ist:

Wenn Sie einen virtuellen Content Switching-Server hinzufügen, wird sein Status zunächst als DOWN angezeigt. Wenn Sie einen virtuellen Load-Balancing-Server binden, dessen Status UP ist, wird der Status des virtuellen Content Switching-Servers in AKTIV geändert.

Wenn mehr als ein virtueller Lastausgleichsserver gebunden ist und einer von ihnen als Standard angegeben ist, spiegelt der Status des virtuellen Content Switching-Servers den Status des virtuellen Standardservers für den Lastausgleich wider.

Wenn mehr als ein virtueller Lastausgleichsserver gebunden ist, ohne dass einer von ihnen als Standard angegeben wurde, wird der Status des virtuellen Content Switching-Servers nur dann als AKTIV markiert, wenn alle virtuellen Server für den gebundenen Lastausgleich AKTIV sind.

So konfigurieren Sie die Option zur Statusaktualisierung mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add cs vserver \<name\> \<protocol\> \<ipAddress\> \<port\> -
   stateUpdate ENABLED
<!--NeedCopy-->
```

Beispiel

```
 add cs vserver csw_vserver HTTP 10.18.250.154 80 -stateupdate ENABLED
    -cltTimeout 180
<!--NeedCopy-->
```

So konfigurieren Sie die Option zur Statusaktualisierung mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Verkehrseinstellungen**und dann **Statusaktualisierung**aus.

Überspannungswarteschlange leeren

Wenn ein physischer Server eine Flut von Anfragen erhält, reagiert er nur langsam auf die Clients, die gerade mit ihm verbunden sind, was die Benutzer unzufrieden und verärgert macht. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Um solche Überlastungen zu vermeiden, bietet die NetScaler-Appliance Funktionen wie einen Überspannungsschutz, der die Geschwindigkeit steuert, mit der neue Verbindungen zu einem Dienst hergestellt werden können.

Die Appliance verbindet Multiplexing zwischen Clients und physischen Servern. Wenn die Appliance eine Client-Anfrage für den Zugriff auf einen Dienst auf einem Server empfängt, sucht sie nach einer bereits bestehenden Verbindung zum Server, die frei ist. Wenn eine freie Verbindung gefunden wird, wird diese Verbindung verwendet, um eine virtuelle Verbindung zwischen dem Client und dem Server herzustellen. Wenn keine bestehende freie Verbindung gefunden wird, stellt die Appliance eine neue Verbindung mit dem Server her und stellt eine virtuelle Verbindung zwischen dem Client und dem Server her. Wenn die Appliance jedoch keine neue Verbindung mit dem Server

herstellen kann, sendet sie die Clientanforderung an eine Überspannungswarteschlange. Wenn alle physischen Server, die an den virtuellen Load Balancing- oder Content-Switching-Server gebunden sind, die Obergrenze für Client-Verbindungen erreichen (maximaler Client-Wert, Überspannungsschutzschwelle oder maximale Kapazität des Dienstes), kann die Appliance keine Verbindung zu einem Server herstellen. Die Überspannungsschutzfunktion verwendet die Überspannungswarteschlange, um die Geschwindigkeit zu regulieren, mit der Verbindungen zu den physischen Servern geöffnet werden. Die Appliance verwaltet eine andere Überspannungswarteschlange für jeden Dienst, der an den virtuellen Server gebunden ist.

Die Länge einer Überspannungswarteschlange nimmt zu, wenn eine Anfrage eingeht, für die die Appliance keine Verbindung herstellen kann, und die Länge verringert sich, wenn eine Anfrage in der Warteschlange an den Server gesendet wird oder eine Anfrage ein Timeout erhält und aus der Warteschlange entfernt wird.

Wenn die Überspannungswarteschlange für einen Dienst oder eine Dienstgruppe zu lang wird, sollten Sie sie möglicherweise leeren. Sie können die Überspannungswarteschlange eines bestimmten Dienstes oder einer bestimmten Dienstgruppe oder aller Dienste und Dienstgruppen, die an einen virtuellen Lastausgleichsserver gebunden sind, leeren. Das Leeren einer Überspannungswarteschlange wirkt sich nicht auf die bestehenden Verbindungen aus. Nur die Anfragen in der Überspannungswarteschlange werden gelöscht. Für diese Anfragen muss der Kunde eine neue Anfrage stellen.

Sie können auch die Surge-Queue eines virtuellen Content Switching-Servers leeren. Wenn ein virtueller Content Switching-Server einige Anfragen an einen bestimmten virtuellen Lastausgleichsserver weiterleitet und der virtuelle Lastausgleichsserver auch einige andere Anfragen empfängt, werden beim Leeren der Überspannungswarteschlange des virtuellen Content Switching-Servers nur die von diesem virtuellen Content Switching-Server empfangenen Anforderungen geleert. Die anderen Anforderungen in der Überspannungswarteschlange des virtuellen Lastausgleichsservers werden nicht geleert.

> **Hinweis**
>
> Sie können die Anstiegswarteschlangen von Cache-Umleitungen, Authentifizierung, VPN oder virtuellen GSLB-Servern oder GSLB-Diensten nicht leeren.
> Verwenden Sie die Überspannungsschutzfunktion nicht, wenn die Option “Quell-IP (USIP) verwenden” aktiviert ist.

So leeren Sie eine Surge-Queue mit der CLI

Der Befehl flush ns SurgeQ funktioniert auf folgende Weise:

- Sie können den Namen eines Dienstes, einer Dienstgruppe oder eines virtuellen Servers angeben, dessen Überspannungswarteschlange geleert werden muss.

- Wenn Sie während der Ausführung des Befehls einen Namen angeben, wird die Überspannungswarteschlange der angegebenen Entität geleert. Wenn mehrere Entitäten denselben Namen haben, leert die Appliance die Überspannungswarteschlangen aller dieser Entitäten.
- Wenn Sie den Namen einer Dienstgruppe und einen Servernamen und einen Port angeben, während der Befehl ausgeführt wird, löscht die Appliance die Überspannungswarteschlange nur des angegebenen Dienstgruppenmitglieds.
- Sie können ein Dienstgruppenmitglied (<serverName> and <port>) nicht direkt angeben, ohne den Namen der Dienstgruppe (<name>) anzugeben, und Sie können keinen <port> ohne einen <serverName> angeben. Geben Sie <serverName> und <port> an, wenn Sie die Überspannungswarteschlange für ein bestimmtes Mitglied der Servicegruppe leeren möchten.
- Wenn Sie den Befehl ausführen, ohne Namen anzugeben, legt die Appliance die Überspannungswarteschlangen aller auf der Appliance vorhandenen Entitäten.
- Wenn ein Dienstgruppenmitglied mit einem Servernamen identifiziert wird, müssen Sie den Servernamen in diesem Befehl angeben. Sie können seine IP-Adresse nicht angeben.

Geben Sie in der Befehlszeile Folgendes ein:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>].
<!--NeedCopy-->
```

Beispiele

```
1. flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual
   server that is named SVC1ANZGB and has IP address as 10.10.10

2. flush ns surgeQ
The above command flushes all the surge queues on the appliance.
<!--NeedCopy-->
```

So leeren Sie eine Überspannungswarteschlange mit der GUI

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie in der Aktionsliste die Option **Flush Surge Queue**aus.

Verwalten eines Content Switching-Setups

May 11, 2023

Nachdem ein Content Switching-Setup konfiguriert wurde, sind möglicherweise regelmäßige Änderungen erforderlich. Wenn Betriebssysteme oder Software aktualisiert werden oder Hardware abgenutzt ist und ersetzt wird, müssen Sie möglicherweise Ihr Setup herunterfahren. Die Belastung Ihres Setups kann zunehmen und mehr Ressourcen erfordern. Sie können die Konfiguration auch ändern, um die Leistung zu verbessern.

Diese Aufgaben erfordern möglicherweise das Aufheben der Bindung von Richtlinien vom virtuellen Content Switching-Server oder das Deaktivieren oder Entfernen von virtuellen Content Switching-Servern. Nachdem Sie Ihr Setup geändert haben, müssen Sie möglicherweise Server erneut aktivieren und Richtlinien erneut binden. Möglicherweise möchten Sie auch Ihre virtuellen Server umbenennen.

Aufheben der Bindung von Richtlinien vom virtuellen Content Switching Server

Wenn Sie eine Content Switching-Richtlinie von ihrem virtuellen Server aufheben, schließt der virtuelle Server diese Richtlinie nicht mehr ein, wenn er festlegt, wohin Anfragen weitergeleitet werden sollen.

So lösen Sie eine Richtlinie über die CLI von einem virtuellen Content Switching-Server

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind cs vserver <name> -policyname <string>
```

Beispiel:

```
unbind cs vserver Vserver-CS-1 -policyname Policy-CS-1
```

So lösen Sie eine Richtlinie über die GUI von einem virtuellen Content Switching-Server

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie auf den Abschnitt **Richtlinien**, wählen Sie die Richtlinie aus und klicken Sie auf **Bindung aufheben**.

Virtuelle Server für Content Switching

Normalerweise entfernen Sie einen virtuellen Content Switching-Server nur, wenn Sie den virtuellen Server nicht mehr benötigen. Wenn Sie einen virtuellen Content Switching-Server entfernen, hebt die NetScaler-Appliance zuerst alle Richtlinien vom virtuellen Content Switching-Server auf und entfernt sie dann.

So entfernen Sie einen virtuellen Content Switching-Server über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
rm cs vserver <name>
```

Beispiel:

```
rm cs vserver Vserver-CS-1
```

So entfernen Sie einen virtuellen Content Switching-Server über die GUI

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus und klicken Sie auf **Löschen**.

Deaktivieren und erneute Aktivierung virtueller Server für Content Switching

Virtuelle Server für Content Switching sind standardmäßig aktiviert, wenn Sie sie erstellen. Sie können einen virtuellen Content Switching-Server für Wartungsarbeiten deaktivieren. Wenn Sie den virtuellen Server für die Content Switching deaktivieren, ändert sich der Status des virtuellen Content Switching-Servers in Out of Service. Während er außer Betrieb ist, reagiert der virtuelle Content Switching-Server nicht auf Anfragen.

So deaktivieren oder aktivieren Sie einen virtuellen Server über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `disable cs vserver <name>`
- `enable cs vserver <name>`

Beispiel:

```
disable cs vserver Vserver-CS-1
enable cs vserver Vserver-CS-1
```

So deaktivieren oder aktivieren Sie einen virtuellen Server über die GUI

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie in der **Aktionsliste** die Option **Aktivieren** oder **Deaktivieren** aus.

Umbenennen von virtuellen Content Switching-Servern

Sie können einen virtuellen Content Switching-Server umbenennen, ohne die Bindungen aufzuheben. Der neue Name wird automatisch an alle betroffenen Teile der NetScaler-Konfiguration weitergegeben.

So benennen Sie einen virtuellen Server über die CLI um

Geben Sie in der Befehlszeile Folgendes ein:

```
rename cs vserver <name> <newName>
```

Beispiel:

```
1 `rename cs vserver Vserver-CS-1 Vserver-CS-2`
```

So benennen Sie einen virtuellen Server mit der GUI um

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie in der Liste **Aktion** die Option **Umbenennen**aus.

Richtlinien für Content Switching verwalten

Sie können eine vorhandene Richtlinie ändern, indem Sie die Regeln konfigurieren oder die URL der Richtlinie ändern, oder Sie können eine Richtlinie entfernen. Sie können auch eine vorhandene erweiterte Content Switching-Richtlinie umbenennen. Sie können basierend auf der URL verschiedene Richtlinien erstellen. URL-basierte Richtlinien können von verschiedenen Typen sein, wie in der folgenden Tabelle beschrieben.

Weitere Informationen finden Sie unter Beispiele für URL-basierte Richtlinien.

> **Hinweis**
>
> Sie können regelbasierte Content Switching mithilfe klassischer Richtlinienausdrücke oder erweiterter Richtlinienausdrücke konfigurieren.

So ändern, entfernen oder benennen Sie eine Richtlinie über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set cs policy <policyName> [-domain <domainValue>] [-rule <ruleValue>] [-url <URLValue>]`
- `rm cs policy <policyName>`
- `rename cs policy <policyName> <newPolicyName>`

Beispiel:

```
set cs policy-CS-1 -domain "www.domainxyz.com"

set cs policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(22).EQ(10.100.148.0)"

set cs policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2010 Jun,GMT 2010 Jul)"

set cs policy-CS-1 -url /sports/*

rename cs policy-CS-1 Policy-CS-11

rm cs policy-CS-1
```

So ändern, entfernen oder benennen Sie eine Richtlinie über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**.
2. Wählen Sie die Richtlinie aus, löschen Sie sie, bearbeiten Sie sie oder klicken Sie in der Liste **Aktion** auf **Umbenennen** .

Verwaltung von Client-Verbindungen

May 11, 2023

Um eine effiziente Verwaltung der Client-Verbindungen zu gewährleisten, können Sie die virtuellen Content Switching-Server auf der NetScaler-Appliance so konfigurieren, dass sie die folgenden Funktionen verwenden:

- **Konfiguration der ICMP-Antwort.** Sie können die NetScaler-Appliance so konfigurieren, dass sie ICMP-Antworten auf PING-Anfragen gemäß Ihren Einstellungen sendet. Stellen Sie für die IP-Adresse, die dem virtuellen Server entspricht, ICMP RESPONSE auf VSVR_CNTRLD und auf dem virtuellen Server den virtuellen ICMP-Server RESPONSE ein.
  Die folgenden Einstellungen können auf einem virtuellen Server vorgenommen werden:
  - Wenn Sie den virtuellen ICMP-Server RESPONSE auf allen virtuellen Servern auf PASSIVE setzen, reagiert die NetScaler-Appliance immer.
  - Wenn Sie den virtuellen ICMP-Server RESPONSE auf allen virtuellen Servern auf ACTIVE setzen, reagiert die ADC-Appliance auch dann, wenn ein virtueller Server aktiv ist.
  - Wenn Sie den virtuellen ICMP-Server RESPONSE bei einigen auf ACTIVE und bei anderen auf PASSIVE setzen, reagiert die ADC-Appliance auch dann, wenn ein auf ACTIVE gesetzter virtueller Server AKTIV ist.

Umleiten von Clientanfragen an einen Cache

Die NetScaler Cache-Umleitungsfunktion leitet HTTP-Anforderungen an einen Cache um. Sie können den Aufwand für die Beantwortung von HTTP-Anfragen erheblich reduzieren und die Leistung Ihrer Website verbessern, indem Sie die Cache-Umleitungsfunktion ordnungsgemäß implementieren.

Ein Cache speichert häufig angeforderten HTTP-Inhalt. Wenn Sie die Cache-Umleitung auf einem virtuellen Server konfigurieren, sendet die NetScaler Appliance zwischenspeicherbare HTTP-Anforderungen an den Cache und nicht zwischenspeicherbare HTTP-Anforderungen an den Ursprungs-Webserver. Weitere Informationen zur Cache-Umleitung finden Sie unter "Cache-Umleitung.

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver \<name\> -cacheable \<Value\>
```

Beispiel

```
set cs vserver Vserver-CS-1 -cacheable yes
```

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter **Erweiterte Einstellungen**die Option **Verkehrseinstellungen**und anschließend **Cachefähig aus.**

Aktivierung der verzögerten Bereinigung von virtuellen Serververbindungen

Unter bestimmten Bedingungen können Sie die Einstellung Down-State-Flush so konfigurieren, dass bestehende Verbindungen beendet werden, wenn ein Dienst oder ein virtueller Server als DOWN markiert wird. Das Beenden vorhandener Verbindungen setzt Ressourcen frei und beschleunigt in bestimmten Fällen die Wiederherstellung überlasteter Load-Balancing-Setups.

So konfigurieren Sie die Einstellung zum Ausfallzustand auf einem virtuellen Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver \<name\> -downStateFlush \<Value\>
```


Beispiel

```
set cs vserver Vserver-CS-1 -downStateFlush enabled
<!--NeedCopy-->
```

So konfigurieren Sie die Flush-Einstellung für den Down-State-Flush auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter **Erweiterte Einstellungen**die Option **Traffic Settings**und dann **Down State Flush**aus.

Ports und Protokolle für die Umleitung umschreiben

Virtuelle Server und die an sie gebundenen Dienste verwenden möglicherweise verschiedene Ports. Wenn ein Dienst auf eine HTTP-Verbindung mit einer Umleitung reagiert, müssen Sie möglicherweise die NetScaler-Appliance so konfigurieren, dass der Port und das Protokoll geändert werden, um sicherzustellen, dass die Umleitung erfolgreich durchgeführt wird. Sie tun dies, indem Sie die Einstellung RedirectPortRewrite aktivieren und konfigurieren.

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver \<name\> -redirectPortRewrite \<Value\>
```

Beispiel

```
set cs vserver Vserver-CS-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Verkehrseinstellungen**und anschließend **Umschreiben**aus.

Einfügen der IP-Adresse und des Ports eines virtuellen Servers in den Anforderungsheader

Wenn Sie mehrere virtuelle Server haben, die mit verschiedenen Anwendungen auf demselben Dienst kommunizieren, müssen Sie die NetScaler-Appliance so konfigurieren, dass sie den HTTP-Anfragen, die an diesen Dienst gesendet werden, die IP-Adresse und Portnummer des entsprechenden virtuellen Servers hinzufügt. Mit dieser Einstellung können Anwendungen, die auf dem Dienst ausgeführt werden, den virtuellen Server identifizieren, der die Anforderung gesendet hat.

Wenn der primäre virtuelle Server ausgefallen ist und der virtuelle Backup-Server aktiv ist, werden die Konfigurationseinstellungen des virtuellen Backup-Servers zu den Clientanforderungen hinzugefügt. Wenn Sie möchten, dass dasselbe Header-Tag hinzugefügt wird, unabhängig davon, ob die Anfragen vom primären virtuellen Server oder vom virtuellen Backup-Server stammen, müssen Sie das erforderliche Header-Tag auf beiden virtuellen Servern konfigurieren.

> **Hinweis**
>
> Diese Option wird für virtuelle Wildcard-Server oder virtuelle Dummy-Server nicht unterstützt.

Um die IP-Adresse und den Port des virtuellen Servers mithilfe der CLI in die Clientanfragen einzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver \<name\> -insertVserverIPPort \<vServerIPPORT\>
```

Beispiel

```
1 set cs vserver Vserver-CS-1 -insertVserverIPPort 10.201.25.136:80
2 <!--NeedCopy-->
```

Um die IP-Adresse und den Port des virtuellen Servers mithilfe der GUI in die Clientanfragen einzufügen

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Traffic Settings** aus und wählen Sie in der Liste „IP-Porteinfügung virtueller Server“ die Option VIPADDR oder V6TOV4MAPPING aus und geben Sie im Wert für die IP-Porteinfügung des virtuellen Servers einen Portheader an.

Festlegen eines Timeout-Werts für inaktive Clientverbindungen

Sie können einen virtuellen Server so konfigurieren, dass alle inaktiven Client-Verbindungen nach Ablauf einer konfigurierten Timeout-Periode beendet werden. Wenn Sie diese Einstellung konfigurieren, wartet die NetScaler Appliance auf die angegebene Zeit und schließt die Clientverbindung, wenn sich der Client nach diesem Zeitpunkt im Leerlauf befindet.

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver \<name\> -cltTimeout \<Value\>
```

Beispiel

```
1 set cs vserver Vserver-CS-1 -cltTimeout 100
2 <!--NeedCopy-->
```

So legen Sie mithilfe der GUI einen Timeout-Wert für inaktive Client-Verbindungen fest

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter **Erweiterte Einstellungen**die Option **Traffic Settings**aus und geben Sie einen Wert für das **Client-Idle-Timeout** an.

Identifizieren von Verbindungen mit den 4-Tupel- und Layer-2-Verbindungsparametern

Sie können jetzt die L2Conn-Option für einen virtuellen Content Switching-Server einrichten. Bei eingestellter L2Conn-Option werden Verbindungen zum virtuellen Content Switching-Server durch die Kombination der Verbindungsparameter 4-Tupel (<source IP>:<source port>::\<destination IP\>:\<destination port\>) und Layer-2 identifiziert. Die Layer-2-Verbindungsparameter sind die MAC-Adresse, die VLAN-ID und die Kanal-ID.

So richten Sie die L2Conn-Option für einen virtuellen Content Switching-Server mithilfe der CLI ein

Geben Sie in der Befehlszeile die folgenden Befehle ein, um den Parameter L2Conn für einen virtuellen Content Switching-Server zu konfigurieren und die Konfiguration zu überprüfen:


```
1 -  set cs vserver \<name\> -l2Conn (**ON** | **OFF**)
2 -  show cs vserver \<name\>
```

Beispiel

```
1  > set cs vserver mycsvserver -l2Conn ON
2  Done
3  > show cs vserver mycsvserver
4       mycsvserver (192.0.2.56:80) - HTTP   Type: CONTENT
5       State: UP
6           . . .
7           . . .
8       L2Conn: ON Case Sensitivity: ON
9           . . .
10          . . .
11 Done
12 >
13 <!--NeedCopy-->
```

So stellen Sie die L2Conn-Option für einen virtuellen Content Switching-Server mithilfe der GUI ein

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Verkehrseinstellungen**und dann **Layer-2-Parameter**aus.

Persistenz-Unterstützung für den virtuellen Server mit Content Switching

May 11, 2023

Anwendungen bewegen sich von monolithischen Architekturen hin zu Microservices-Architekturen. Verschiedene Versionen derselben Anwendung können in der Microservices-Architektur koexistieren. Die NetScaler-Appliance muss die kontinuierliche Bereitstellung von Anwendungen unterstützen. Dies wird durch Plattformen erreicht, die Canary-Bereitstellungen durchführen (wie Spinnaker). Bei einer Continuous-Deployment-Setup wird eine neuere Version einer Anwendung automatisch bereitgestellt und schrittweise dem Client-Verkehr ausgesetzt, bis die Anwendung stabil ist und den

gesamten Datenverkehr aufnehmen kann. Außerdem müssen unterbrechungsfreie Dienste für den Kunden verfügbar sein.

Die NetScaler Content Switching-Funktion ermöglicht es NetScaler, der Appliance, Client-Anforderungen auf mehrere virtuelle Load-Balancing-Server zu verteilen, basierend auf den Richtlinien, die an den virtuellen Content Switching-Server gebunden sind.

Bei kontinuierlichen Bereitstellungen wird Content Switching verwendet, um den virtuellen Lastausgleichsserver auszuwählen, der verschiedene Versionen einer Anwendung bedient.

Beim Content Switching ändert sich die Auswahl eines virtuellen Lastausgleichsservers für eine bestimmte Anwendungsversion zur Laufzeit aufgrund der Änderung der Inhaltswechselrichtlinien. Wenn während dieser Umstellung einige Sitzungen mit älteren Versionen der Anwendung vorhanden sind, darf dieser Datenverkehr weiterhin nur von älteren Versionen bereitgestellt werden. Um diese Anforderung zu unterstützen, sorgt die NetScaler-Appliance für die Persistenz mehrerer Load Balancing-Gruppen hinter einem virtuellen Content Switching-Server. Der virtuelle Server Persistence for Content Switching ermöglicht den nahtlosen Übergang von Clients von einer Version zur anderen.

Unterstützte Persistenztypen auf virtuellen Content Switching-Servern

Die folgenden Persistenztypen werden auf virtuellen Content Switching-Servern unterstützt.

Persistenztyp	Beschreibung
Quell-IP	**QUELLE/IP.** Verbindungen von derselben Client-IP-Adresse sind Teil derselben Persistenzsitzung. Weitere Informationen finden Sie unter Persistenz der Quell-IP-Adresse.
HTTP-Cookie	**COOKIE-EINFÜGEN**. Verbindungen, die denselben HTTP-Cookie-Header haben, sind Teil derselben Persistenzsitzung. Das Format des Cookie, das die NetScaler-Appliance einfügt, ist: **NSC_ = wobei NSC_XXXX** <vid_str of CSvserver><vid_str of Lbvserver>die virtuelle Server-ID ist, die vom Namen des virtuellen Servers abgeleitet wird. Weitere Informationen finden Sie unter Persistenz von HTTP-Cookies.

Persistenztyp	Beschreibung
SSL-Sitzung ID	**SSL-SITZUNG**. Verbindungen mit derselben SSL-Sitzungs-ID sind Teil derselben Persistenzsitzung. Weitere Informationen finden Sie unter Persistenz der SSL-Sitzungs-ID.

Sie können einen Timeoutwert für Persistenz konfigurieren, der auf HTTP-Cookies basiert. Wenn Sie den Timeout-Wert auf 0 festlegen, gibt die ADC Appliance unabhängig von der verwendeten HTTP-Cookie-Version keine Ablaufzeit an. Die Ablaufzeit hängt dann von der Client-Software ab, und solche Cookies sind nur gültig, wenn die Software läuft.

Abhängig von der Art der Persistenz, die Sie konfiguriert haben, kann der virtuelle Server entweder 250.000 gleichzeitige persistente Verbindungen oder eine beliebige Anzahl persistenter Verbindungen unterstützen, bis die Grenzen liegen, die sich aus der Speichermenge auf Ihrer NetScaler-Appliance ergeben. Die folgende Tabelle zeigt, welche Arten von Persistenz in die einzelnen Kategorien fallen.

Persistenztyp	Anzahl der unterstützten gleichzeitigen persistenten Verbindungen
Quell-IP, SSL-Sitzungs-ID	250,000
HTTP-Cookie	Speicherbegrenzung. Wenn in CookieInsert das Timeout nicht 0 ist, ist die Anzahl der Verbindungen durch den Speicher begrenzt.

Einige Arten der Persistenz sind spezifisch für bestimmte Arten von virtuellen Servern. In der folgenden Tabelle sind die einzelnen Persistenztypen aufgeführt und es wird angegeben, welche Arten von Persistenz auf welchen virtuellen Servertypen unterstützt werden.

Persistenztyp	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEIP	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
PLÄTZCHEN EINFÜGEN	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
SSL-SITZUNG	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein

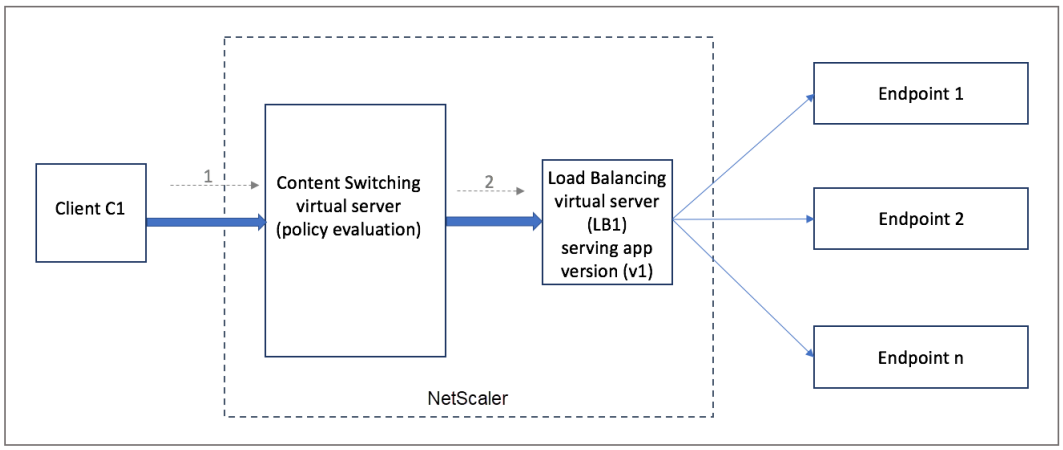
Unterstützung für Backup-Persistenz

Sie können den virtuellen Content Switching-Server so konfigurieren, dass er den Quell-IP-Persistenztyp als Backup-Persistenztyp verwendet, wenn der Cookie-Persistenztyp ausfällt. Es ist nützlich für Canary-Implementierungen in der Microservices-Architektur.
Wenn der Cookie-Persistenztyp fehlschlägt, greift die Appliance nur dann auf die Quell-IP-basierte Persistenz zurück, wenn der Clientbrowser in der Anfrage kein Cookie zurückgibt. Wenn der Browser jedoch ein Cookie zurückgibt (nicht unbedingt das Persistenz-Cookie), wird davon ausgegangen, dass der Browser Cookies unterstützt und daher keine Backup-Persistenz ausgelöst wird.
Sie können auch einen Timeout-Wert für die Backup-Persistenz festlegen. Timeout ist der Zeitraum, für den eine Persistenzsitzung aktiv ist.

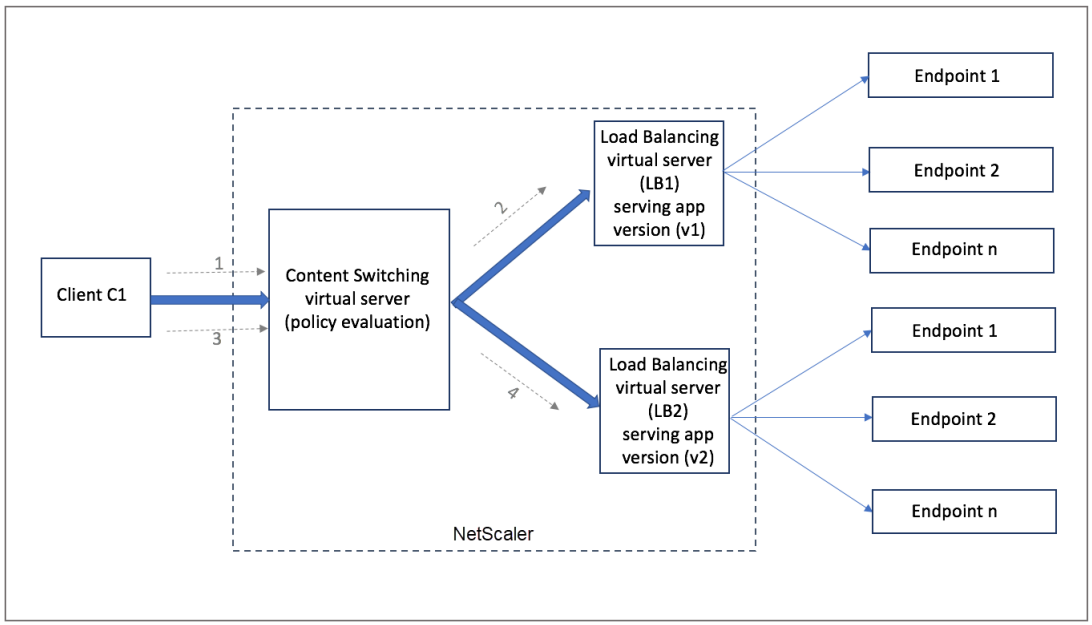
So funktioniert die Persistenz beim virtuellen Server für Content Switching

Szenario 1: Ein virtueller Content-Switching-Server ohne Persistenz

Das folgende Beispiel veranschaulicht die Bereitstellung mehrerer Versionen einer Anwendung mit einem virtuellen Content Switching-Server ohne Persistenz.



Wenn der Client C1 eine Anfrage an die Anwendung sendet, wird die Anforderung an den virtuellen Content Switching-Server in der NetScaler-Appliance gesendet. Der virtuelle Content Switching-Server wertet die Richtlinie aus und leitet die Anfrage an den virtuellen Load-Balancing-Server (LB1) weiter, der Version v1 der Anwendung bereitstellt.

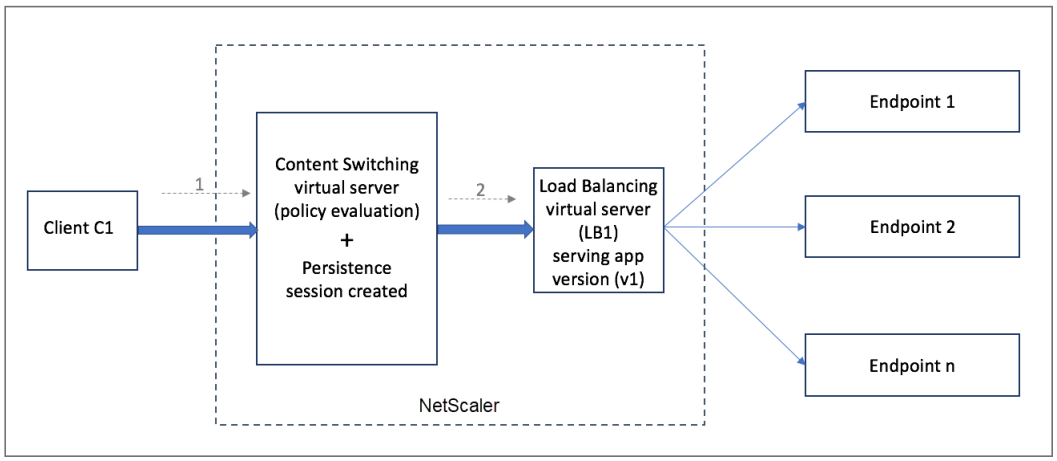


Stellen Sie sich vor, dass eine neue Version v2 der Anwendung bereitgestellt wird und einer Untergruppe von Benutzern zugänglich gemacht werden muss. Der neue virtuelle Load-Balancing-Server (LB2), der die v2-Version bereitstellt, ist durch die entsprechende Content Switching-Richtlinie an den virtuellen Content Switching-Server gebunden.

Wenn der Client C1 eine neue Anfrage sendet, wird die Richtlinie erneut ausgewertet und die Anfrage wird an den virtuellen Lastausgleichsserver LB2 weitergeleitet. Daher schlagen die Transaktionen für State-ful-Anwendungen fehl, wenn mehrere Versionen der Anwendung bereitgestellt werden.

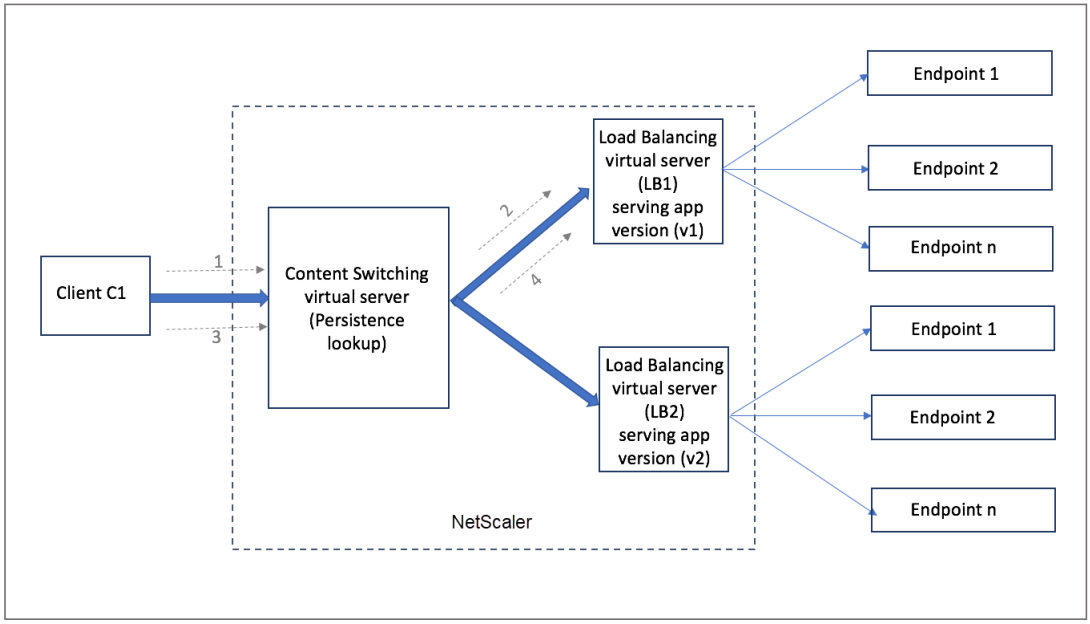
Szenario 2: Virtueller Content-Switching-Server mit Persistenz

Das folgende Beispiel veranschaulicht die Bereitstellung mehrerer Versionen der Anwendung mit einem virtuellen Content Switching-Server mit Persistenz.

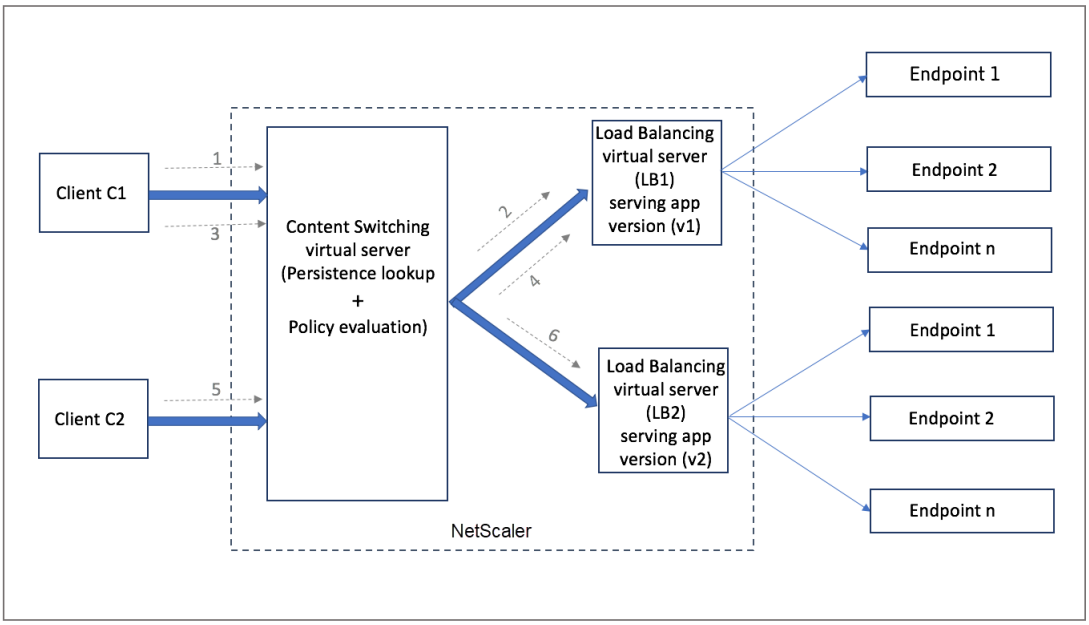


Wenn der Client C1 eine Anfrage an die Anwendung sendet, wird die Anforderung an den virtuellen

Content Switching-Server in der NetScaler-Appliance gesendet. Der virtuelle Content Switching-Server wertet die Richtlinie aus, erstellt einen Persistenz-Sitzungseintrag und leitet die Anfrage an den virtuellen Lastausgleichsserver LB1 weiter, der Version v1 der Anwendung bereitstellt.



Derselbe Client C1 fordert erneut die Anwendung an, und die Anforderung wird an den virtuellen Content Switching-Server in der NetScaler-Appliance gesendet. Es wird nach der Persistenzsitzung gesucht, und der virtuelle Lastausgleichsserver LB1 wird aus der vorhandenen Persistenzsitzung übernommen und die Anfrage wird an LB1 weitergeleitet. Mit dieser Lösung kommt es zu keiner Unterbrechung der bestehenden Transaktion, sodass der statusmäßige Charakter der Anwendung erhalten bleibt.



Betrachten wir einen neuen Kunden C2. Die neue Anforderung C2 wird im Rahmen der Richtlinienauswertung an die neuere Version der Anwendung gesendet, da für diesen Client keine Persistenzsitzung vorhanden ist. Dies führt zu einer erfolgreichen Einführung der neueren Version der Anwendung, ohne deren Statement zu beeinträchtigen.

Aufgrund der Persistenzunterstützung können Kunden mehrere Inhalte oder verschiedene Versionen der Anwendung nahtlos bereitstellen, ohne die bestehenden Transaktionen zu beeinträchtigen, insbesondere bei Stateful-Anwendungen. Ohne Beharrlichkeit im Bild ist das nicht möglich.

Konfigurieren Sie den Persistenztyp auf dem virtuellen Content Switching-Server mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set cs vserver <name> -PersistenceType <type> [-timeout <integer>]
<!--NeedCopy-->
```

Beispiel:

```
set cs vserver Vserver-CS-1 -persistenceType SOURCEIP -timeout 60
<!--NeedCopy-->
```

Konfigurieren Sie den Persistenztyp auf dem virtuellen Content Switching-Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server** und klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie in den **Grundeinstellungen**die Persistenzdetails.

Problembehandlung

September 18, 2023

Wenn die Funktion zum Content Switching nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf NetScaler-Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen zur Behebung von Problemen Content Switching

Optimale Ergebnisse erzielen Sie, wenn Sie die folgenden Ressourcen verwenden, um ein Problem mit dem Content Switching auf einer NetScaler-Appliance zu beheben:

- Konfigurationsdatei
- `newnslog` Datei, die generiert wurde, als das Problem auftrat
- Trace-Dateien
- Netzwerktopologiediagramm für das Netzwerk-Setup des Kunden
- NetScaler-Dokumentation, z. B. Versionshinweise, Knowledge Center-Artikel und Produktdokumentation.

Zusätzlich zu den oben genannten Ressourcen beschleunigen die folgenden Tools die Fehlerbehebung:

- Das `iehttpheaders` oder ein ähnliches Dienstprogramm
- Die Wireshark-Anwendung, die auf die NetScaler-Trace-Dateien zugeschnitten ist
- Ein SSH-Hilfsprogramm für den Befehlszeilenzugriff
- Ein HyperTerminal-Hilfsprogramm für den Zugriff auf die Konsole

Behebung von Problemen beim Umschalten von Inhalten

Die häufigsten Probleme Content Switching sind, dass die Funktion zum Content Switching überhaupt nicht oder nur sporadisch funktioniert und dass der Dienst nicht verfügbar ist.

- **Problem**

  Die Funktion Content Switching funktioniert nicht.

  Auflösung

  Überprüfen Sie die Konfiguration wie folgt:

  - Stellen Sie sicher, dass die Appliance für Content Switching lizenziert ist.
  - Stellen Sie sicher, dass die Funktion aktiviert ist.
  - Vergewissern Sie sich anhand der Konfigurationsdatei, dass gültige Content Switching-Richtlinien korrekt an die virtuellen Load Balancing-Server gebunden sind.

- **Problem**

  Der Kunde erhält die Antwort 503 — Service Unavailable.

  Auflösung

  - Überprüfen Sie die URL und die Richtlinienbindungen. Der Client erhält die 503-Antwort, wenn keine der von Ihnen konfigurierten Richtlinien ausgewertet wurde und kein virtueller Standardserver für den Lastausgleich definiert und an den virtuellen Content Switching-Server gebunden ist.

- Stellen Sie in der Konfiguration sicher, dass die Richtlinien und der Client auf die URL zugreift.
- Stellen Sie sicher, dass für jede Art von Anfrage die entsprechende Richtlinie bewertet wird. Wenn die Richtlinie nicht bewertet wurde, überprüfen Sie den Richtlinienausdruck und aktualisieren Sie ihn gegebenenfalls.
- Überprüfen Sie die URL und die HTTP-Anfrage- und Antwortheader. Dazu zeichnen Sie einen `HTTPHeader` Trace und, falls erforderlich, die Paket-Traces auf der Appliance und dem Client auf.

- **Problem**

  Zeitweise funktioniert die Funktion zum Content Switching nicht wie erwartet.

  Auflösung

  - Studieren Sie das Netzwerktopologiediagramm des Setups, falls verfügbar, um die verschiedenen Geräte zu verstehen, die zwischen dem Client und den Servern installiert sind.
  - Überprüfen Sie die Konfiguration und die Richtlinienbindungen. Stellen Sie sicher, dass die URL im Richtlinienausdruck mit der URL in der Client-Anfrage übereinstimmt.
  - Stellen Sie sicher, dass den Richtlinien entsprechende Prioritäten zugewiesen sind. Eine falsche Priorität oder Priorität, die einer Richtlinie zugewiesen wurde, kann zu Problemen führen.
  - Führen Sie die folgenden Befehle aus, um die Bindungen und Werte der Richtlinienauswahlzähler in der Befehlsausgabe zu überprüfen:

    ```
    show cs vserver \<CS VServer\>

    show cs policy \<CS Policy\>

    stat cs vserver \<CS VServer\>
    ```

  - Stellen Sie mithilfe eines `iehttpheaders` oder eines ähnlichen Hilfsprogramms fest, ob die HTTP-Header für die Anfragen oder Antworten Hinweise auf das Problem liefern.
  - Lesen Sie die Versionshinweise und die Artikel im Knowledge Center.
  - Wenn das Problem immer noch nicht behoben ist, wenden Sie sich mit den entsprechenden Daten an den technischen Support von Citrix, um weitere Untersuchungen durchzuführen.

DataStream

May 11, 2023

Die NetScaler DataStream-Funktion bietet einen intelligenten Mechanismus für den Anforderungswechsel auf der Datenbankebene, indem Anfragen auf der Grundlage der gesendeten SQL-Abfrage verteilt werden.

Bei der Bereitstellung vor Datenbankservern sorgt eine NetScaler-Appliance für eine optimale Verteilung des Datenverkehrs von den Anwendungsservern und Webservern. Administratoren können den Datenverkehr nach Informationen in der SQL-Abfrage und auf der Grundlage von Datenbanknamen, Benutzernamen, Zeichensätzen und Paketgröße segmentieren.

Sie können den Lastenausgleich so konfigurieren, dass Anfragen auf der Grundlage von Load-Balancing-Algorithmen umgeschaltet werden. Alternativ können Sie die Switching-Kriterien ausarbeiten, indem Sie den Content Switching so konfigurieren, dass eine Entscheidung auf der Grundlage eines SQL-Abfrageparameters getroffen wird. Sie können Monitore weiter konfigurieren, um den Status von Datenbankservern zu verfolgen.

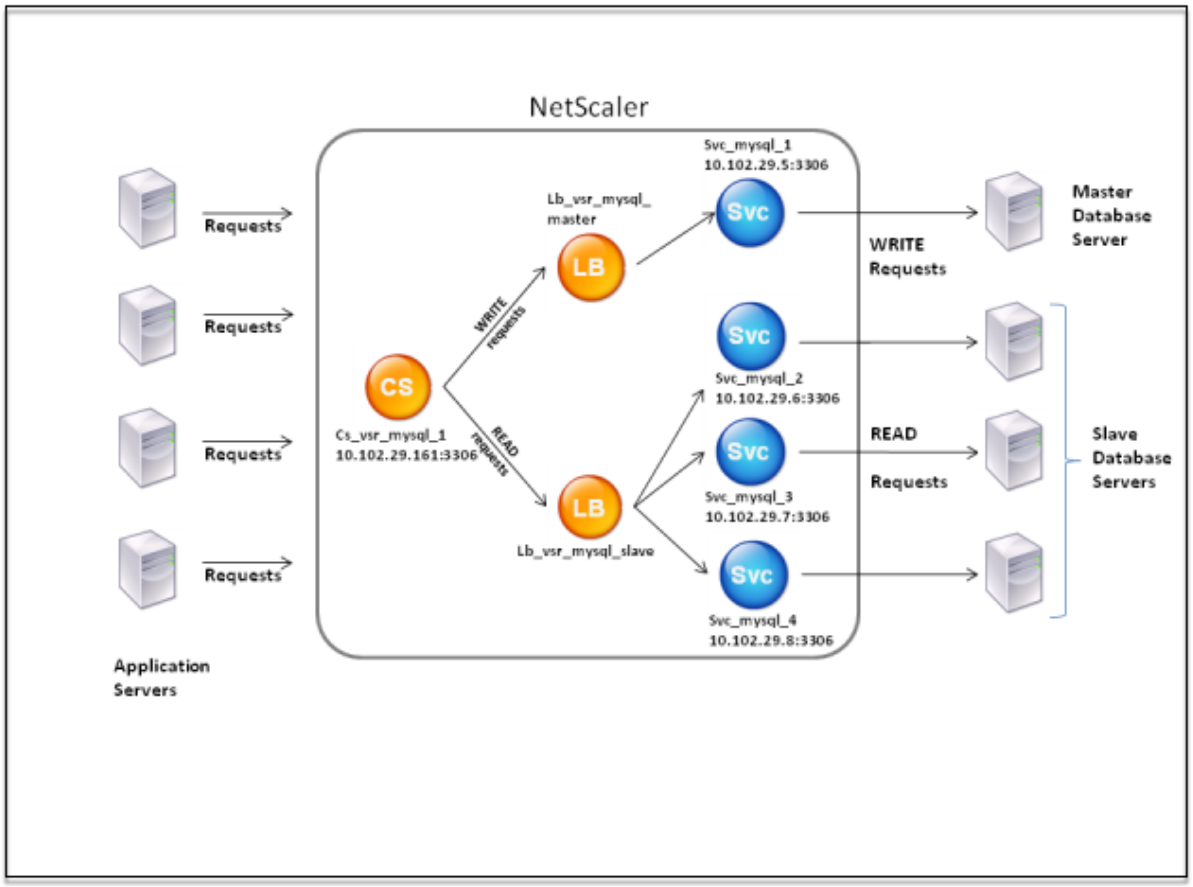
> **Hinweis**
>
> NetScaler DataStream wird nur für MySQL- und MS SQL-Datenbanken unterstützt. Informationen zur unterstützten Protokollversion, zu Zeichensätzen, speziellen Abfragen und Transaktionen finden Sie unter DataStream Reference.

So funktioniert DataStream

In DataStream wird die ADC-Appliance in einer Linie zwischen den Anwendungs- oder Webservern und den Datenbankservern platziert. Auf der Appliance werden die Datenbankserver durch Dienste repräsentiert.

Eine typische DataStream-Bereitstellung besteht aus den in der folgenden Abbildung beschriebenen Entitäten.

Abbildung 1. DataStream-Entitätsmodell



Wie in dieser Abbildung dargestellt, kann eine DataStream-Konfiguration aus folgenden Elementen bestehen:

- Ein optionaler virtueller Content Switching-Server (CS).
- Ein Lastausgleichs-Setup, das aus virtuellen Lastausgleichsservern (LB1 und LB2) besteht.
- Dienste (Svc1, Svc2, Svc3 und Svc4).
- Richtlinien für den Inhaltswechsel (optional).

Die Clients (Anwendungs- oder Webserver) senden Anfragen an die IP-Adresse eines virtuellen Content Switching-Servers (CS), der auf der NetScaler-Appliance konfiguriert ist. Die Appliance authentifiziert dann die Clients mithilfe der auf der Appliance konfigurierten Datenbank-Benutzeranmeldeinformationen. Der Content Switching Virtual Server (CS) wendet die zugehörigen Content Switching-Richtlinien auf die Anfragen an. Nach der Bewertung der Richtlinien leitet der Content Switching Virtual Server (CS) die Anfragen an den entsprechenden virtuellen Load-Balancing-Server (LB1 oder LB2) weiter. Anschließend verteilt der virtuelle Lastausgleichsserver die Anfragen auf der Grundlage des Load-Balancing-Algorithmus an die entsprechenden Datenbankserver (dargestellt durch Dienste auf der Appliance). Die NetScaler-Appliance verwendet dieselben Datenbankbenutzer-Anmeldeinformationen, um die Verbindung mit dem Datenbankserver zu authentifizieren.

Wenn kein virtueller Content Switching-Server auf der Appliance konfiguriert ist, senden die Clients (Anwendungs- oder Webserver) ihre Anfragen an einen virtuellen Lastausgleichsserver, der auf der Appliance konfiguriert ist. Die NetScaler-Appliance authentifiziert den Client mithilfe der auf der Appliance konfigurierten Datenbank-Benutzeranmeldeinformationen und verwendet dann dieselben Anmeldeinformationen, um die Verbindung mit dem Datenbankserver zu authentifizieren. Der virtuelle Lastausgleichsserver verteilt die Anfragen gemäß dem Load-Balancing-Algorithmus an die Datenbankserver. Der effektivste Load-Balancing-Algorithmus für den Datenbankwechsel ist die Methode mit der geringsten Verbindung.

DataStream verwendet Verbindungsmultiplexing, damit mehrere clientseitige Anfragen über dieselbe serverseitige Verbindung gestellt werden können. Die folgenden Verbindungseigenschaften werden berücksichtigt:

- Benutzername
- Database name
- Paket-Größe
- Zeichensatz

Konfigurieren von Datenbankbenutzern

August 19, 2021

In Datenbanken ist eine Verbindung immer statusbehaftet, was bedeutet, dass beim Herstellen einer Verbindung authentifiziert werden muss.

Konfigurieren Sie den Benutzernamen und das Kennwort Ihrer Datenbank auf der NetScaler Appliance. Wenn Sie beispielsweise einen Benutzer John in der Datenbank konfiguriert haben, müssen Sie den Benutzer John auch auf dem ADC konfigurieren. Durch das Hinzufügen von Datenbankbenutzernamen und Kennwörtern auf dem ADC werden sie der `nsconfig` Datei hinzugefügt.

> **Hinweis:**
>
> Bei Namen wird zwischen Groß- und Kleinschreibung unterschieden.

Der ADC verwendet diese Benutzeranmeldeinformationen, um die Clients zu authentifizieren und dann die Serververbindungen mit den Datenbankservern zu authentifizieren.

Hinzufügen eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
add db user <username> - password <password>
```

Beispiel:


```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Fügen Sie einen Datenbankbenutzer über die grafische Benutzeroberfläche hinzu

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, und konfigurieren Sie einen Datenbankbenutzer.

Wenn Sie das Kennwort des Datenbankbenutzers auf dem Datenbankserver geändert haben, müssen Sie das Kennwort des entsprechenden Benutzers zurücksetzen, der auf der ADC-Appliance konfiguriert ist.

Zurücksetzen des Kennworts eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Beispiel:

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Setzen Sie das Kennwort von Datenbankbenutzern über die grafische Benutzeroberfläche zurück

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus, und geben Sie neue Werte für das Kennwort ein.

Wenn ein Datenbankbenutzer nicht mehr auf dem Datenbankserver vorhanden ist, können Sie den Benutzer aus der ADC-Appliance entfernen. Wenn der Benutzer jedoch weiterhin auf dem Datenbankserver vorhanden ist und Sie den Benutzer aus der ADC-Appliance entfernen, wird jede Anforderung vom Client mit diesem Benutzernamen nicht authentifiziert. Daher wird die Anfrage nicht an den Datenbankserver weitergeleitet.

Entfernen eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
rm db user <username>
<!--NeedCopy-->
```


Beispiel:

```
rm db user nsdbuser
<!--NeedCopy-->
```

Entfernen eines Datenbankbenutzers mit der GUI

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus, und klicken Sie auf **Löschen**.

Konfigurieren eines Datenbankprofils

February 16, 2021

Ein Datenbankprofil ist eine benannte Sammlung von Parametern, die einmal konfiguriert, aber auf mehrere virtuelle Server angewendet wird, für die bestimmte Parametereinstellungen erforderlich sind. Nachdem Sie ein Datenbankprofil erstellt haben, binden Sie es an den virtuellen Lastausgleichs- oder Content Switching-Server. Sie können beliebig viele Profile erstellen.

Erstellen eines Datenbankprofils mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um ein Datenbankprofil zu erstellen und die Konfiguration zu überprüfen:

```
add db dbProfile <name> [-interpretQuery ( YES | NO )] [-stickiness (
    YES | NO )] [-kcdAccount <string>]

show db dbProfile
<!--NeedCopy-->
```

Beispiel:

```
> add dbProfile myDBProfile -interpretQuery YES -stickiness YES -
    kcdAccount mykcdaccnt
 Done
> show dbProfile myDBProfile
    Name: myDBProfile
    Interpret Query: YES
    Stickyness: YES
    KCD Account: mykcdaccnt
    Reference count: 0
```



```
9
10   Done
11 >
12 <!--NeedCopy-->
```

Erstellen eines Datenbankprofils mit der GUI

Navigieren Sie zu **System > Profile**, und konfigurieren Sie auf der Registerkarte **Datenbankprofile** ein Datenbankprofil.

Binden eines Datenbankprofils an einen virtuellen Lastenausgleichs- oder Content Switching-Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set (lb | cs) vserver <name> -dbProfileName <string>
2 <!--NeedCopy-->
```

Binden eines Datenbankprofils an einen virtuellen Lastenausgleichs- oder Content Switching-Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server oder Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **Profile**aus, und wählen Sie in der Liste **DB-Profil** ein Profil aus, das an den virtuellen Server gebunden werden soll. Um ein Profil zu erstellen, klicken Sie auf plus (+).

Load Balancing für DataStream konfigurieren

May 11, 2023

Bevor Sie ein Load-Balancing-Setup konfigurieren, müssen Sie die Load-Balancing-Funktion aktivieren. Erstellen Sie dann zunächst mindestens einen Dienst für jeden Datenbankserver in der Load Balancing-Gruppe. Wenn die Dienste konfiguriert sind, können Sie einen virtuellen Lastausgleichsserver erstellen und die Dienste an den virtuellen Server binden.

> **Hinweis**:
>
> Für Datenbanken kann der Lastenausgleich nur auf homogenen Datenbankservern (Datenbankservern, die genau dieselben Datenbanken enthalten) erfolgen. Für eine Konfiguration,

> die eindeutige Datenbanken auf verschiedenen Servern enthält, müssen Sie Content Switching verwenden. Wenn einige Ihrer Datenbankserver identische Inhalte hosten, können Sie den Lastenausgleich nur auf diesen Servern verwenden. Sie können dann Richtlinien für die Content Switching verwenden, um Anfragen an den virtuellen Lastausgleichsserver zu senden, der den Lastenausgleich für diese Datenbanken verwaltet.
>
> Die NetScaler-Appliance speichert derzeit den Datenbanknamen und die Anmeldeinformationen während der Datenbanksitzung. Wenn eine Abfrage an die Datenbank gestellt wird, verwendet sie diese Informationen, um eine Verbindung mit dem bestimmten Datenbankserver herzustellen.

Spezifische Parameterwerte für DataStream

- Protokoll

  Verwenden Sie den MYSQL-Protokolltyp für MySQL-Datenbanken und den MSSQL-Protokolltyp für MS SQL-Datenbanken, während Sie virtuelle Server und Dienste konfigurieren. Die MySQL- und TDS-Protokolle werden von den Clients verwendet, um mithilfe von SQL-Abfragen mit den jeweiligen Datenbankservern zu kommunizieren. Hinweise zum MySQL-Protokoll finden Sie unter http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Hinweise zum TDS-Protokoll finden Sie unter http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port, auf dem der virtuelle Server auf Clientverbindungen lauscht. Verwenden Sie Port 3306 für MySQL-Datenbankserver.

- Methode

  Es wird empfohlen, die Methode der geringsten Verbindung zu verwenden, um einen besseren Lastenausgleich und eine geringere Serverlast zu erzielen. Andere Methoden wie Round Robin, Least Response Time, Quell-IP-Hash, Quell-IP-Ziel-IP-Hash, Least Bandwidth, Least Packets und Source IP Source Port Hash werden jedoch ebenfalls unterstützt.

  Hinweis: Die URL-Hash-Methode wird für DataStream nicht unterstützt.

- Version von MS SQL Server

  Wenn Sie Microsoft SQL Server verwenden und erwarten, dass einige Clients eine andere Version als Ihr Microsoft SQL Server-Produkt ausführen, legen Sie den Parameter Serverversion für den virtuellen Load Balancing-Server fest. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht. Weitere Informationen zum Festlegen des Parameters “Serverversion” finden Sie unter Konfigurieren der Versionseinstellung MySQL und Microsoft SQL Server.

- MySQL-Serverversion

  Wenn Sie den MySQL-Server verwenden und erwarten, dass einige Clients eine andere Version als Ihr MySQL Server-Produkt ausführen, legen Sie den Parameter Serverversion für den virtuellen Lastausgleichsserver fest. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht. Weitere Informationen zum Festlegen des Parameters "Serverversion" finden Sie unter Konfigurieren der Versionseinstellung MySQL und Microsoft SQL Server.

Content Switching für DataStream konfigurieren

May 11, 2023

Sie können den Datenverkehr nach Informationen in der SQL-Abfrage basierend auf Datenbanknamen, Benutzernamen, Zeichensätzen und Paketgröße segmentieren.

Sie können Content Switching-Richtlinien mit erweiterten Richtlinienausdrücken konfigurieren, um Inhalte basierend auf Verbindungseigenschaften zu wechseln. Zum Beispiel Benutzername und Datenbankname, Befehlsparameter und die SQL-Abfrage zur Auswahl des Servers.

Die erweiterten Richtlinienausdrücke werten den Datenverkehr aus, der mit MySQL- und MS SQL-Datenbankservern verknüpft Verwenden Sie anforderungsbasierte Ausdrücke in erweiterten Richtlinienrichtlinien, um Anforderungswechselentscheidungen am Bindepunkt des virtuellen Servers für Content Switching zu Verwenden Sie antwortbasierte Ausdrücke (Ausdrücke, die mit MYSQL.RES beginnen), um Serverreaktionen auf benutzerkonfigurierte Integritätsmonitore auszuwerten.

Informationen zu erweiterten Richtlinienausdrücken finden Sie unter Erweiterte Richtlinienausdrücke: DataStream.

> **Hinweis:**
>
> Für Datenbanken kann der Lastenausgleich nur auf homogenen Datenbankservern (Datenbankservern, die genau dieselben Datenbanken enthalten) erfolgen. Für eine Konfiguration, die eindeutige Datenbanken auf verschiedenen Servern enthält, müssen Sie Content Switching verwenden. Wenn einige Ihrer Datenbankserver identische Inhalte hosten, können Sie den Lastenausgleich nur auf diesen Servern verwenden. Sie können dann Richtlinien für die Content Switching verwenden, um Anfragen an den virtuellen Lastausgleichsserver zu senden, der den Lastenausgleich für diese Datenbanken verwaltet.
>
> Die NetScaler-Appliance speichert derzeit den Datenbanknamen und die Anmeldeinformationen während der Datenbanksitzung. Wenn eine Abfrage an die Datenbank gestellt wird, ver-

> wendet sie diese Informationen, um eine Verbindung mit dem bestimmten Datenbankserver herzustellen.

Spezifische Parameterwerte für DataStream

- Protokoll

  Verwenden Sie den MYSQL-Protokolltyp für MySQL-Datenbanken und den MSSQL-Protokolltyp für MS SQL-Datenbanken, während Sie virtuelle Server und Dienste konfigurieren. Die MySQL- und TDS-Protokolle werden von den Clients verwendet, um mithilfe von SQL-Abfragen mit den jeweiligen Datenbankservern zu kommunizieren. Hinweise zum MySQL-Protokoll finden Sie unter http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Hinweise zum TDS-Protokoll finden Sie unter http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port, auf dem der virtuelle Server auf Clientverbindungen lauscht. Verwenden Sie Port 3306 für MySQL-Datenbankserver.

- MS SQL Serverversion

  Wenn Sie Microsoft SQL Server verwenden und erwarten, dass einige Clients eine andere Version als Ihr Microsoft SQL Server-Produkt ausführen, legen Sie den Serverversion-Parameter für den virtuellen Content Switching-Server fest. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht. Weitere Informationen zum Festlegen des Parameters “Serverversion” finden Sie unter Konfigurieren der Microsoft SQL Server-Versionseinstellung.

Konfigurieren von Monitoren für DataStream

August 19, 2021

Um den Status jedes Lastausgleichs-Datenbankservers in Echtzeit zu verfolgen, müssen Sie einen Monitor an jeden Dienst binden. Der Monitor ist so konfiguriert, dass er den Dienst testet, indem er regelmäßige Probes an den Dienst sendet, der manchmal als Durchführen einer Zustandsprüfung bezeichnet wird. Wenn der Monitor eine rechtzeitige Antwort auf seine Sonden erhält, markiert er den Dienst als UP. Wenn es keine rechtzeitige Antwort auf die angegebene Anzahl von Sonden erhält, markiert es den Dienst als DOWN.

Für DataStream müssen Sie die integrierten Monitore verwenden: MYSQL-ECV und MSSQL-ECV. Mit diesem Monitor können Sie eine SQL-Anfrage senden und die Antwort für eine Zeichenfolge

analysieren.

Bevor Sie Monitore für DataStream konfigurieren, müssen Sie Ihrer NetScaler er-Appliance Datenbank-Benutzeranmeldeinformationen hinzufügen. Informationen zum Konfigurieren von Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing-Setup.

Wenn Sie einen Monitor erstellen, wird eine TCP-Verbindung mit dem Datenbankserver hergestellt, und die Verbindung wird mithilfe des Benutzernamens authentifiziert, der beim Erstellen des Monitors angegeben wird. Anschließend können Sie eine SQL-Abfrage an den Datenbankserver ausführen und die Serverantwort auswerten, um zu überprüfen, ob sie mit der konfigurierten Regel übereinstimmt.

Die folgenden Beispiele sind für MySQL Server.

Beispiele:

Im folgenden Beispiel wird der Wert der Fehlermeldung ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon1 MYSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mysql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

Im folgenden Beispiel wird die Anzahl der Zeilen in der Antwort ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon4 MYSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mysql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

Im folgenden Beispiel wird der Wert einer bestimmten Spalte ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon3 MYSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mysql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Die folgenden Beispiele sind für MSSQL-Server.

Beispiele:

Im folgenden Beispiel wird der Wert der Fehlermeldung ausgewertet, um den Status des Servers zu bestimmen.


```
add lb monitor lb_mon1 MSSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mssql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

Im folgenden Beispiel wird die Anzahl der Zeilen in der Antwort ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon4 MSSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mssql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

Im folgenden Beispiel wird der Wert einer bestimmten Spalte ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon3 MSSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mssql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Anwendungsfall 1: Konfigurieren von DataStream für eine Primär-/Sekundärdatenbankarchitektur

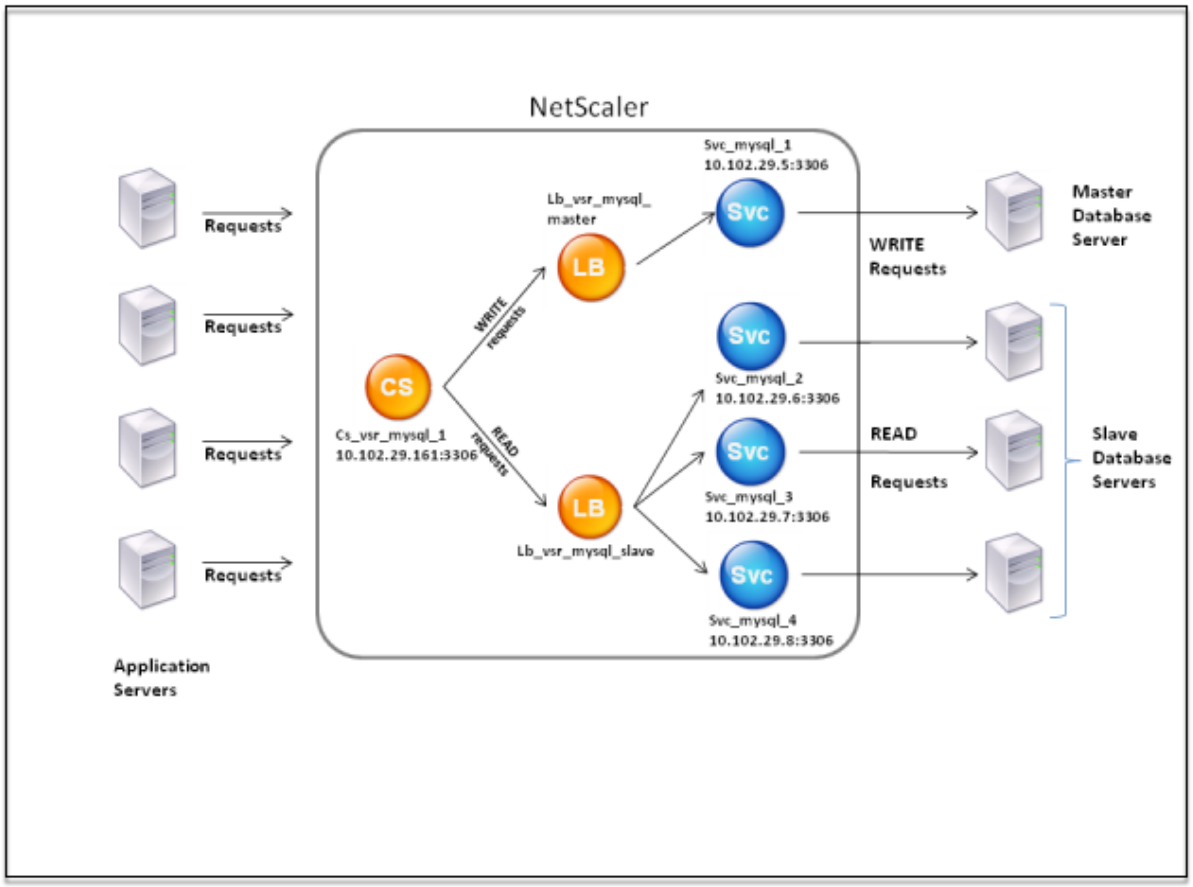
May 11, 2023

Ein häufig verwendetes Bereitstellungsszenario ist die primäre und sekundäre Datenbankarchitektur, bei der die Primärdatenbank alle Informationen in die sekundären Datenbanken repliziert

Bei der primären/sekundären Datenbankarchitektur möchten Sie möglicherweise, dass alle WRITE-Anforderungen an die Primärdatenbank und alle READ-Anforderungen an die sekundären Datenbanken gesendet werden.

Die folgende Abbildung zeigt die Entitäten und die Werte der Parameter, die Sie auf der Appliance konfigurieren müssen.

Abbildung 1. DataStream-Entitätsmodell für Primär-/Sekundärdatenbank-Setup



In diesem Beispielszenario wird ein Dienst (SVC_MySql_1) erstellt, um die Primärdatenbank darzustellen, und ist an einen virtuellen Lastausgleichsserver (LB_VSR_MySql_Primary) gebunden. Drei weitere Dienste (SVC_MySql_2, SVC_MySql_3 und SVC_MySql_4) werden erstellt, um die drei sekundären Datenbanken darzustellen, und sie sind an einen anderen virtuellen Lastausgleichsserver (LB_VSR_MySql_Secondary) gebunden.

Ein virtueller Content Switching-Server (CS_VSR_MySql_1) ist mit zugehörigen Richtlinien konfiguriert, um alle WRITE-Anforderungen an den virtuellen Lastausgleichsserver zu senden, lb_vsr_mysql_Primary. Alle READ-Anforderungen werden an den virtuellen Lastausgleichsserver LB_VSR_MySql_Secondary gesendet.

Wenn eine Anforderung den virtuellen Content Switching-Server erreicht, wendet der virtuelle Server die zugeordneten Content Switching-Richtlinien auf diese Anforderung an. Nach der Auswertung der Richtlinien leitet der virtuelle Content Switching-Server die Anforderung an den entsprechenden virtuellen Lastausgleichsserver weiter, der sie an den entsprechenden Dienst sendet.

In der folgenden Tabelle sind die Namen und Werte der Entitäten sowie die auf der NetScaler Appliance konfigurierte Richtlinie aufgeführt.

Typ der Entität	Name	IP-Adresse	Protokoll	Port	Ausdruck
Services	Svc_mysql_1	198.51.100.5	MYSQL	3306	Nicht verfügbar
	Svc_mysql_2	198.51.100.6	MYSQL	3306	Nicht verfügbar
	Svc_mysql_3	198.51.100.7	MYSQL	3306	Nicht verfügbar
	Svc_mysql_4	198.51.100.8	MYSQL	3306	Nicht verfügbar
Überwachung	lb_mon1	Nicht verfügbar	MYSQL-ECV	Nicht verfügbar	mysql.res.atleast_rows_cou
Virtuelle Lastenausgle-ichsserver	Lb_vsr_mysql_primary	198.51.100.201	MYSQL	3306	Nicht verfügbar
	Lb_vsr_mysql_	198.51.100.202	MYSQL	3306	Nicht verfügbar
Virtuelle Content Switching-Server	Cs_vsr_mysql_1	198.51.100.161	MYSQL	3306	Nicht verfügbar
Content Switching-Richtlinie	Cs_select	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	`MYSQL.REQ.QUERY.COMMAND.contains("select")`

Tabelle 1. Namen und Werte von Entitäten und Richtlinien

So konfigurieren Sie DataStream für ein Primär-/Sekundärdatenbank-Setup mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung

```
1 add db user user1 -password user1
2
3 add service Svc_mysql_1 198.51.100.5 mysql 3306
4
```



```
add service Svc_mysql_2 198.51.100.6 mysql 3306

add service Svc_mysql_3 198.51.100.7 mysql 3306

add service Svc_mysql_4 198.51.100.8 mysql 3306

add lb monitor lb_mon1 MYSQL-ECV -sqlQuery "select * from table1;" -
    evalrule "mysql.res.atleast_rows_count(1)" -database "NS" -userName
     "user1"

add lb vserver Lb_vsr_mysql_primary mysql 198.51.100.201 3306

add lb vserver Lb_vsr_mysql_secondary mysql 198.51.100.202 3306

bind lb vserver Lb_vsr_mysql_primary svc_mysql_1

bind lb vserver Lb_vsr_mysql_secondary svc_mysql_2

bind lb vserver Lb_vsr_mysql_secondary svc_mysql_3

bind lb vserver Lb_vsr_mysql_secondary svc_mysql_4

add cs vserver Cs_vsr_mysql_1 mysql 198.51.100.161 3306

add cs policy Cs_select  -rule "MYSQL.REQ.QUERY.COMMAND.contains("
    select")"

bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_primary

bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_secondary  -policy
    Cs_select  -priority 10

bind service Svc_mysql_1 -monitorName lb_mon1

bind service Svc_mysql_2 -monitorName lb_mon1

bind service Svc_mysql_3 -monitorName lb_mon1

bind service Svc_mysql_4 -monitorName lb_mon1
<!--NeedCopy-->
```


Anwendungsfall 2: Konfigurieren der Tokenmethode des Lastausgleichs für DataStream

May 11, 2023

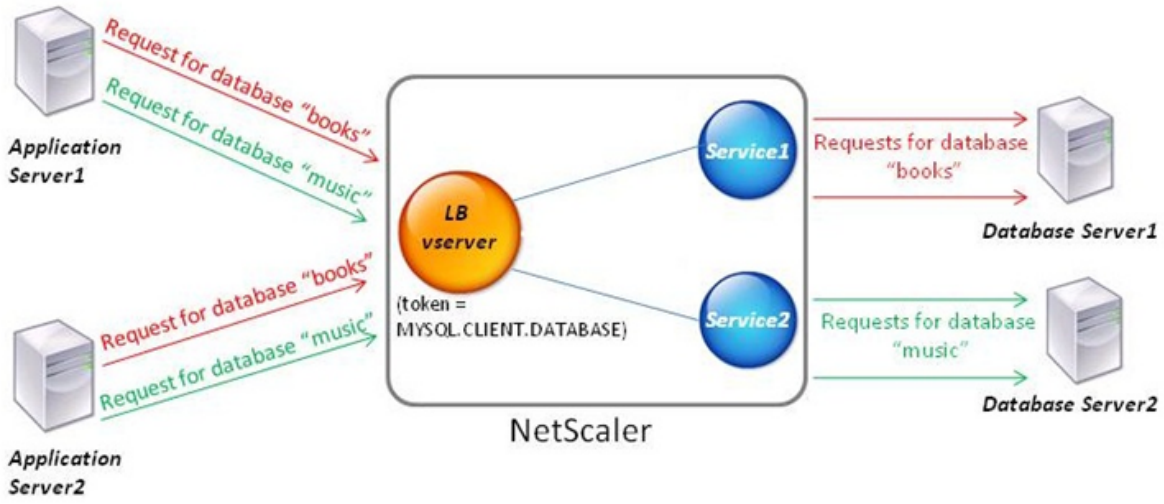
Sie können die Token-Methode für den Lastenausgleich für DataStream so konfigurieren, dass die Auswahl der Datenbankserver auf dem Wert des Tokens basiert, das aus den Client-Anforderungen (Anwendung oder Webserver) extrahiert wurde. Diese Token werden mithilfe von SQL-Ausdrücken definiert. Bei nachfolgenden Anfragen mit demselben Token sendet die NetScaler-Appliance die Anfragen an denselben Datenbankserver, der die erste Anfrage bearbeitet hat. Anfragen mit demselben Token werden an denselben Datenbankserver gesendet, bis das maximale Verbindungslimit erreicht ist oder der Sitzungseintrag abgelaufen ist.

Sie können die folgenden Beispiel-SQL-Ausdrücke verwenden, um Token zu definieren:

MySQL	MS SQL
MYSQL.REQ.QUERY.TEXT	MSSQL.REQ.QUERY.TEXT
MYSQL.REQ.QUERY.TEXT (n)	MSSQL. REQ.QUERY.TEXT (n)
MYSQL.REQ.QUERY.COMMAND	MSSQL.REQ.QUERY.COMMAND
MYSQL.CLIENT.USER	MSSQL.CLIENT.USER
MYSQL.CLIENT.DATABASE	MSSQL.CLIENT.DATABASE
MYSQL.CLIENT.CAPABILITIES	

Das folgende Beispiel zeigt, wie die NetScaler DataStream-Funktion funktioniert, wenn Sie die Token-Methode für den Lastenausgleich konfigurieren.

Abbildung 1. DataStream und die Token-Methode des Load Balancings



In diesem Beispiel ist das Token der Name der Datenbank. Eine Anfrage mit Token-Büchern wird an Datenbankserver1 gesendet und eine Anfrage mit Tokenmusik wird an Datenbankserver2 gesendet. Alle nachfolgenden Anfragen mit Token-Büchern werden an Datenbankserver1 und Anfragen mit Token-Musik an Datenbankserver2 gesendet. Diese Konfiguration bietet Pseudo-Persistenz mit den Datenbankservern.

Konfigurieren Sie dieses Beispiel mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add service Service1 192.0.2.9 MYSQL 3306

add service Service2 192.0.2.11 MYSQL 3306

add lb vserver token_lb_vserver MYSQL 192.0.2.15 3306 -lbmethod token -
    rule MYSQL.CLIENT.DATABASE

bind lb vserver token_lb_vserver Service1

bind lb vserver token_lb_vserver Service2
<!--NeedCopy-->
```

Konfigurieren Sie dieses Beispiel mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als **MYSQL**an.

2. Klicken Sie in den Abschnitt **Service** und konfigurieren Sie zwei Dienste, die das Protokoll als MYSQL angeben. Binden Sie diese Dienste an den virtuellen Server.
3. Klicken Sie **unter Erweiterte Einstellungen**auf **Methode** und wählen Sie in der Liste **Load Balancing-Methode** die Option **TOKEN** aus und geben Sie den Ausdruck als **MYSQL.CLIENT.DATABASE**an.

Anwendungsfall 3: Protokollieren von MSSQL-Transaktionen im transparenten Modus

May 11, 2023

Sie können die NetScaler-Appliance so konfigurieren, dass sie transparent zwischen MSSQL-Clients und -Servern arbeitet und nur Details aller Client-Server-Transaktionen protokolliert oder analysiert. Der transparente Modus ist so konzipiert, dass die NetScaler-Appliance nur MSSQL-Anfragen an den Server weiterleitet und dann die Antworten des Servers an die Clients weiterleitet. Während die Anfragen und Antworten die Appliance durchlaufen, protokolliert die Appliance die von ihnen gesammelten Informationen, wie in der Audit-Logging- oder AppFlow-Konfiguration angegeben, oder sammelt Statistiken, wie in der Action Analytics-Konfiguration angegeben. Sie müssen der Appliance keine Datenbankbenutzer hinzufügen.

Im transparenten Modus führt die NetScaler-Appliance für die Anfragen weder Load Balancing noch Content Switching noch Verbindungsmultiplexing durch. Es reagiert jedoch im Namen des Servers auf das Pre-Login-Paket eines Clients, sodass verhindert wird, dass während des Pre-Login-Handshakes eine Verschlüsselung vereinbart wird. Das Login-Paket und die nachfolgenden Pakete werden an den Server weitergeleitet.

Zusammenfassung der Konfigurationsaufgaben

Um MSSQL-Anfragen im transparenten Modus zu protokollieren oder zu analysieren, müssen Sie wie folgt vorgehen:

- Konfigurieren Sie die NetScaler-Appliance als Standard-Gateway für Clients und Server.
- Führen Sie auf der NetScaler-Appliance einen der folgenden Schritte aus:
  - **Konfigurieren Sie die Option „Quell-IP-Adresse (USIP) verwenden“ global:** Erstellen Sie einen virtuellen Lastausgleichsserver mit einer Platzhalter-IP-Adresse und der Portnummer, auf der die MSSQL-Server auf Anfragen warten (ein portspezifischer virtueller Wildcard-Server). Aktivieren Sie dann die USIP-Option global. Wenn Sie einen portspezifischen virtuellen Wildcard-Server konfigurieren, müssen Sie keine MSSQL-Dienste auf der Appliance erstellen. Die Appliance erkennt die Dienste anhand der Ziel-IP-Adresse in den Client-Anfragen.

  - **Wenn Sie die USIP-Option nicht global konfigurieren möchten:** Erstellen Sie MSSQL-Dienste, bei denen die USIP-Option für jeden von ihnen aktiviert ist. Wenn Sie Dienste konfigurieren, müssen Sie keinen portspezifischen virtuellen Wildcard-Server erstellen.
- Konfigurieren Sie Audit-Logging, AppFlow oder Action Analytics, um die Anfragen zu protokollieren oder Statistiken zu sammeln. Wenn Sie einen virtuellen Server konfigurieren, können Sie Ihre Richtlinien entweder an den virtuellen Server oder an den globalen Bindungspunkt binden. Wenn Sie keinen virtuellen Server konfigurieren, können Sie Ihre Richtlinien nur an den globalen Bindungspunkt binden.

Konfigurieren Sie den transparenten Modus mithilfe eines virtuellen Wildcard-Servers

Sie können den transparenten Modus konfigurieren, indem Sie einen portspezifischen virtuellen Wildcard-Server konfigurieren und den USIP-Modus (USIP) global aktivieren. Wenn ein Client seinem Standard-Gateway (der NetScaler-Appliance) eine Anfrage mit der IP-Adresse eines MSSQL-Servers im Ziel-IP-Adressheader sendet, überprüft die Appliance, ob die Ziel-IP-Adresse verfügbar ist. Wenn die IP-Adresse verfügbar ist, leitet der virtuelle Server die Anfrage an den Server weiter. Andernfalls wird die Anfrage verworfen.

Erstellen Sie einen virtuellen Wildcard-Server mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen virtuellen Wildcard-Server zu erstellen und die Konfiguration zu überprüfen:

```
add lb vserver <name> <serviceType> <IPAddress> <port>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> add lb vserver wildcardLbVs MSSQL * 1433
 Done
> show lb vserver wildcardLbVs
    wildcardLbVs (*:1433) - MSSQL   Type: ADDRESS
    State: UP
    . . .

 Done
>
<!--NeedCopy-->
```


Erstellen Sie mithilfe der GUI einen virtuellen Wildcard-Server

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und erstellen Sie einen virtuellen Server. Geben Sie MSSQL als Protokoll und * als IP-Adresse an.

Aktivieren Sie den Modus Use Source IP (USIP) global mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den USIP-Modus global zu aktivieren und die Konfiguration zu überprüfen:

```
enable ns mode USIP

show ns mode
<!--NeedCopy-->
```

Beispiel:

```
> enable ns mode USIP
 Done
> show ns mode

    Mode                                Acronym
       Status
    -------                             -------
       ------
                . . .
 3) Use Source IP                 USIP                          ON
                . . .
 Done
>
<!--NeedCopy-->
```

Aktivieren Sie den USIP-Modus global mithilfe der GUI

1. Navigieren Sie zu **System > Einstellungen** und wählen Sie unter Modi und Funktionen die Option **Modi konfigurieren**aus.
2. Wählen Sie **Quell-IP verwenden**aus.

Konfigurieren Sie den transparenten Modus mithilfe von MSSQL-Diensten

Sie können den transparenten Modus konfigurieren, indem Sie MSSQL-Dienste konfigurieren und USIP für jeden Dienst aktivieren. Wenn ein Client seinem Standard-Gateway (der NetScaler-

Appliance) eine Anfrage mit der IP-Adresse eines MSSQL-Servers im Ziel-IP-Adressheader sendet, leitet die Appliance die Anfrage an den Zielserver weiter.

Erstellen Sie einen MSSQL-Dienst und aktivieren Sie den USIP-Modus für den Dienst über die Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen MSSQL-Dienst mit aktiviertem USIP zu erstellen, und überprüfen Sie die Konfiguration:

```
add service <name> (<IP> | <serverName>) <serviceType> <port> -usip YES
    `

show service <name>
<!--NeedCopy-->
```

Beispiel

```
> add service myDBservice 192.0.2.0 MSSQL 1433 -usip YES
 Done
> show service myDBservice
    myDBservice (192.0.2.0:1433) - MSSQL
    State: UP
                . . .
    Use Source IP: YES      Use Proxy Port: YES
                . . .
 Done
>
<!--NeedCopy-->
```

Erstellen Sie einen MSSQL-Dienst mit aktivierter USIP über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und konfigurieren Sie einen Dienst.
2. Geben Sie das Protokoll als **MSSQL** an und wählen Sie **unter Einstellungen**die Option **Quell-IP verwenden**aus.

Anwendungsfall 4: Datenbankspezifischer Lastausgleich

May 11, 2023

Bei einer Datenbankserverfarm muss der Lastenausgleich nicht nur auf der Grundlage der Serverzustände, sondern auch anhand der Verfügbarkeit der Datenbank auf jedem Server erfolgen. Ein Dienst ist möglicherweise aktiv und ein Lastausgleichsgerät zeigt ihn möglicherweise als im Status UP an, aber die angeforderte Datenbank ist für diesen Dienst möglicherweise nicht verfügbar. Die Anfrage wird nicht bearbeitet, wenn eine Anfrage an einen Dienst weitergeleitet wird, für den die Datenbank nicht verfügbar ist. Daher muss ein Load-Balancing-Gerät die Verfügbarkeit einer Datenbank für jeden Dienst kennen. Und wenn es eine Load-Balancing-Entscheidung trifft, darf es nur die Dienste berücksichtigen, auf denen die Datenbank verfügbar ist.

Stellen Sie sich als Beispiel vor, dass die DatenbankServer1, server2 und server3 die Datenbanken mydatabase1 und mydatabase2 hosten. Wenn mydatabase1 auf Server2 nicht mehr verfügbar ist, muss das Load Balancing-Gerät über diese Statusänderung informiert sein. Es muss Anfragen für mydatabase1 nur auf Server1 und Server3 verteilen. Sobald mydatabase1 auf Server2 verfügbar ist, muss das Lastausgleichsgerät Server2 in die Lastausgleichsentscheidungen einbeziehen. In ähnlicher Weise muss das Gerät, wenn mydatabase2 auf Server3 nicht verfügbar ist, die Anforderungen für mydatabase2 nur auf Server1 und Server2 verteilen. Server3 darf nur dann in seine Load-Balancing-Entscheidungen einbezogen werden, wenn mydatabase2 verfügbar ist. Dieses Lastausgleichsverhalten muss für alle Datenbanken, die in der Serverfarm gehostet werden, konsistent sein.

Die NetScaler-Appliance implementiert dieses Verhalten, indem sie eine Liste aller Datenbanken abruft, die in einem Dienst aktiv sind. Um die Liste der aktiven Datenbanken abzurufen, verwendet die Appliance einen Monitor, der mit einer entsprechenden SQL-Abfrage konfiguriert ist. Wenn die angeforderte Datenbank für einen Dienst nicht verfügbar ist, schließt die Appliance den Dienst von Lastausgleichsentscheidungen aus, bis er verfügbar ist. Dieses Verhalten gewährleistet einen unterbrechungsfreien Service für Kunden.

> **Hinweis**
>
> Der datenbankspezifische Load Balancing wird nur für die Diensttypen MSSQL und MySQL unterstützt. Diese Unterstützung ist auch für die Bereitstellung von Microsoft SQL Server 2012 mit hoher Verfügbarkeit verfügbar.

Um einen datenbankspezifischen Load Balancing einzurichten, müssen Sie Folgendes konfigurieren:

- Aktivieren Sie die Lastausgleichsfunktion und konfigurieren Sie einen virtuellen Lastausgleichsserver vom Typ MSSQL oder MySQL.
- Konfigurieren Sie die Dienste, die die Datenbank hosten, und binden Sie die Dienste an den virtuellen Server. Der Monitor benötigt gültige Benutzeranmeldeinformationen, um sich am Datenbankserver anzumelden. Daher müssen Sie auf jedem der Server ein Datenbankbenutzerkonto konfigurieren und das Benutzerkonto dann der NetScaler-Appliance hinzufügen.
- Anschließend konfigurieren Sie einen MSSQL-ECV- oder MYSQL-ECV-Monitor und binden den Monitor an jeden Dienst.

- Schließlich müssen Sie die Konfiguration testen, um sicherzustellen, dass sie wie vorgesehen funktioniert. Bevor Sie diese Konfigurationsaufgaben ausführen, sollten Sie sich darüber im Klaren sein, wie der datenbankspezifische Lastenausgleich funktioniert.

So funktioniert der datenbankspezifische Load Balancing

Für den datenbankspezifischen Lastenausgleich konfigurieren Sie einen Monitor, der regelmäßig jeden Datenbankserver nach den Namen aller aktiven Datenbanken abfragt. Die NetScaler-Appliance speichert die Ergebnisse und aktualisiert die Datensätze regelmäßig auf der Grundlage der durch die Überwachung abgerufenen Informationen. Wenn ein Client eine bestimmte Datenbank abfragt, verwendet die Appliance die konfigurierte Load-Balancing-Methode, um einen Dienst auszuwählen, und überprüft dann ihre Datensätze, um festzustellen, ob die Datenbank für diesen Dienst verfügbar ist. Wenn aus den Datensätzen hervorgeht, dass die Datenbank nicht verfügbar ist, verwendet sie die konfigurierte Load-Balancing-Methode, um den nächsten verfügbaren Dienst auszuwählen, und wiederholt dann die Prüfung. Die Appliance leitet die Anfrage an den ersten verfügbaren Dienst weiter, auf dem die Datenbank aktiv ist.

Lastenausgleich aktivieren

Sie können Load Balancing-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Lastausgleichsfunktion deaktiviert ist. Die Entitäten funktionieren erst, wenn Sie die Funktion aktivieren.

Aktivieren Sie den Lastenausgleich mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen

```
enable ns feature LB

show ns feature
<!--NeedCopy-->
```

Beispiel:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                       Acronym             Status
        -------                       -------             ------
 1)     Web Logging                   WL                  OFF
 2)     Surge Protection              SP                  ON
```



```
3)     Load Balancing                LB                    ON
.
.
.
24)    NetScaler Push                push                  OFF
Done
<!--NeedCopy-->
```

Aktivieren Sie den Lastenausgleich mithilfe der GUI

Navigieren Sie zu **System > Einstellungen** und wählen **Sie unter Configure Basic Features**die Option **Load Balancing**aus.

Konfigurieren Sie einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich

Um einen virtuellen Server für den Lastenausgleich von Datenbanken auf der Grundlage der Verfügbarkeit zu konfigurieren, aktivieren Sie den datenbankspezifischen Load-Balancing-Parameter auf dem virtuellen Server. Durch die Aktivierung des Parameters wird die Load-Balancing-Logik geändert, sodass die NetScaler-Appliance die Ergebnisse der an den ausgewählten Dienst gesendeten Überwachungstests weiterleitet, bevor sie die Anfrage an diesen Dienst weiterleitet.

Konfigurieren Sie einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich mithilfe der CLI

Geben Sie an der Befehlszeile den folgenden Befehl ein, um einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name> <serviceType> <ipAddress> <port> -dbsLb ENABLED

show lb vserver <name>
<!--NeedCopy-->
```

Konfigurieren von Diensten

Nachdem Sie die Load-Balancing-Funktion aktiviert haben, müssen Sie mindestens einen Dienst für jeden Anwendungsserver erstellen, der in Ihr Load-Balancing-Setup aufgenommen werden soll. Die Dienste, die Sie konfigurieren, stellen die Verbindungen zwischen der NetScaler-Appliance und den Load Balancing-Servern bereit. Jeder Dienst hat einen Namen und gibt eine IP-Adresse, einen Port und den Datentyp an, der bereitgestellt wird.

Wenn Sie einen Dienst erstellen, ohne zuerst ein Serverobjekt zu erstellen, ist die IP-Adresse des Dienstes auch der Name des Servers, der den Dienst hostet. Wenn Sie Server lieber anhand des Namens als anhand der IP-Adresse identifizieren möchten, können Sie Serverobjekte erstellen und dann beim Erstellen eines Dienstes den Namen eines Servers anstelle seiner IP-Adresse angeben.

Konfigurieren von Datenbankbenutzern

In Datenbanken ist eine Verbindung immer statusbehaftet, was bedeutet, dass eine Verbindung, wenn sie hergestellt wird, authentifiziert werden muss.

Konfigurieren Sie Ihren Datenbankbenutzernamen und Ihr Passwort auf dem NetScaler. Wenn Sie beispielsweise einen Benutzer John in der Datenbank konfiguriert haben, müssen Sie den Benutzer John auch auf dem ADC konfigurieren. Dem ADC hinzugefügte Datenbankbenutzernamen und Passwörter werden der `nsconfig` Datei hinzugefügt.

> **Hinweis**
>
> Bei Namen wird zwischen Groß- und Kleinschreibung unterschieden.

Der ADC verwendet diese Benutzeranmeldeinformationen, um die Clients zu authentifizieren und dann die Serververbindungen mit den Datenbankservern zu authentifizieren.

Fügen Sie mithilfe der CLI einen Datenbankbenutzer hinzu

Geben Sie an der Eingabeaufforderung

```
add db user <username> - password <password>
<!--NeedCopy-->
```

Beispiel:

```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Fügen Sie einen Datenbankbenutzer über die grafische Benutzeroberfläche hinzu

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**und konfigurieren Sie einen Datenbankbenutzer.

Wenn Sie das Passwort des Datenbankbenutzers auf dem Datenbankserver geändert haben, müssen Sie das auf der NetScaler-Appliance konfigurierte Passwort des entsprechenden Benutzers zurücksetzen.

Setzen Sie das Passwort eines Datenbankbenutzers mithilfe der CLI zurück

Geben Sie an der Eingabeaufforderung

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Beispiel:

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Setzen Sie das Kennwort von Datenbankbenutzern über die grafische Benutzeroberfläche zurück

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus und geben Sie neue Werte für das Passwort ein.

Wenn auf dem Datenbankserver kein Datenbankbenutzer mehr vorhanden ist, können Sie den Benutzer aus der NetScaler-Appliance entfernen. Wenn der Benutzer jedoch weiterhin auf dem Datenbankserver existiert und Sie den Benutzer aus der ADC-Appliance entfernen, wird jede Anfrage des Clients mit diesem Benutzernamen nicht authentifiziert. Daher wird der Benutzername nicht an den Datenbankserver weitergeleitet.

Entfernen Sie einen Datenbankbenutzer mithilfe der CLI

Geben Sie an der Eingabeaufforderung

```
rm db user <username>
<!--NeedCopy-->
```

Beispiel:

```
rm db user nsdbuser
<!--NeedCopy-->
```

Entfernen Sie einen Datenbankbenutzer mithilfe der GUI

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus, und klicken Sie auf **Löschen**.

Konfigurieren Sie einen Monitor, um die Namen der aktiven Datenbanken abzurufen

Sie können einen Monitor erstellen, um die Liste aller aktiven Datenbanken auf einer Datenbankinstanz abzurufen. Der Monitor meldet sich mit gültigen Benutzeranmeldeinformationen am Datenbankserver an und führt eine entsprechende SQL-Abfrage aus. Die SQL-Abfrage, die Sie verwenden müssen, hängt von Ihrer SQL-Serverbereitstellung ab. In einem MSSQL-Datenbankspiegelungs-Setup können Sie beispielsweise die folgende Abfrage verwenden, um eine Liste der aktiven Datenbanken abzurufen, die auf einer Serverinstanz verfügbar sind.

```
select name from sys.databases where state=0
<!--NeedCopy-->
```

In einem MySQL-Datenbank-Setup können Sie die folgenden Abfragen verwenden, um eine Liste der aktiven Datenbanken abzurufen, die auf einer Serverinstanz verfügbar sind.

Datenbanken anzeigen:

Sie konfigurieren den Monitor auch so, dass er die Reaktion auf einen Fehler auswertet und die Ergebnisse speichert, falls kein Fehler auftritt. Wenn die Antwort einen Fehler enthält, markiert der Monitor den Dienst als DOWN. Die Appliance schließt den Dienst von Load-Balancing-Entscheidungen aus, bis kein Fehler mehr zurückgegeben wird.

> **Hinweis**
>
> Die datenbankspezifische Load-Balancing-Funktion wird nur für die Diensttypen MSSQL und MySQL unterstützt. Daher muss der Monitortyp MSSQL-ECV oder MYSQL-ECV sein.

Konfigurieren Sie einen Monitor, um die Namen aller aktiven Datenbanken abzurufen, die in einem Dienst über die Befehlszeilenschnittstelle gehostet werden

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Namen aller aktiven Datenbanken abzurufen, die auf einem Dienst gehostet werden, und um die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> <type> -userName <string> -sqlQuery <text>
    -evalRule <expression> -storedb ENABLED

show lb monitor <monitorName>
<!--NeedCopy-->
```

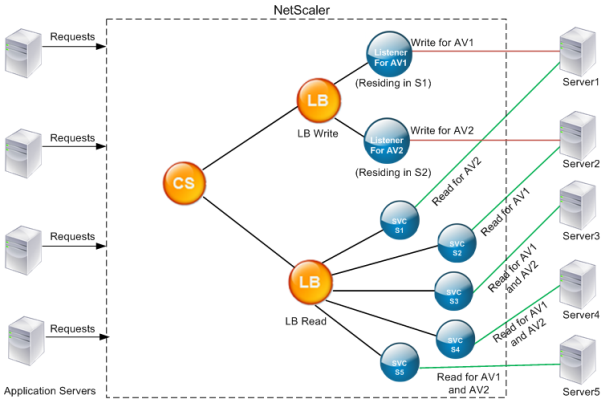
Konfigurieren Sie einen Monitor, um die Namen aller aktiven Datenbanken abzurufen, die in einem Dienst über die grafische Benutzeroberfläche gehostet werden

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore** und konfigurieren Sie einen Monitor vom Typ MSSQL-ECV oder MYSQL-ECV.

2. Geben Sie **unter Spezielle Parameter**einen Benutzernamen, eine Abfrage und eine Regel an. Für MSSQL-ECV muss die Abfrage beispielsweise „select name from sys.databases where state=0”) lauten, und eine Regel muss MSSQL.RES.TYPE.NE (ERROR) lauten. Für MYSQL-ECV muss die Abfrage „show databases“ lauten und eine Regel muss MYSQL.RES.TYPE.NE (ERROR) lauten.

Unterstützung für die Bereitstellung von Verfügbarkeitsgruppen für MSSQL

Stellen Sie sich das folgende Szenario vor, in dem der datenbankspezifische Lastenausgleich in einer Gruppenbereitstellung mit hoher Verfügbarkeit konfiguriert wird. S1 bis S5 sind die Dienste auf der ADC-Appliance. DB1 bis DB4 sind die Datenbanken auf den Servern, die durch die Dienste S1 bis S5 repräsentiert werden. AV1 und AV2 sind die Verfügbarkeitsgruppen. Jede Verfügbarkeitsgruppe enthält bis zu eine primäre Datenbankserverinstanz und bis zu vier sekundäre Datenbankserverinstanzen. Ein Dienst, der die Server in der Verfügbarkeitsgruppe repräsentiert, kann für eine Verfügbarkeitsgruppe primär und für eine andere Verfügbarkeitsgruppe sekundär sein. Jede Verfügbarkeitsgruppe enthält verschiedene Datenbanken und einen Listener, bei dem es sich um einen Dienst handelt. Alle Anfragen kommen auf dem Listener-Dienst an, der sich in der Primärdatenbank befindet. AVI enthält die Datenbanken DB1 und DB2. AV2 enthält die Datenbanken DB3 und DB4. L1 und L2 sind die Zuhörer auf AV1 bzw. AV2. S1 ist der primäre Dienst für AV1 und S2 ist der primäre Dienst für AV2.



Service	Liste der aktiven Datenbanken im Service
S1	DB1, DB2, DB3, DB4
S2	DB3, DB4
S3	DB3, DB4
S4	DB1, DB2
S5	DB1, DB2

Verfügbarkeitsgruppe	Datenbanken	Dienste, die die Server in der Verfügbarkeitsgruppe repräsentieren
AV1	DB1, DB2	S1, S4, S5
AV2	DB3, DB4	S1, S2, S3

Abfragen laufen wie folgt ab:

1. Bei einer READ-Abfrage für AV1 erfolgt ein Lastenausgleich zwischen S4 und S5. S1 ist der primäre Wert für AV1.
2. Eine WRITE-Abfrage für AV1 wird an L1 gerichtet.
3. Bei einer READ-Abfrage für AV2 erfolgt ein Lastenausgleich zwischen S1 und S3. S2 ist das Primärsystem für AV2.
4. Eine WRITE-Abfrage für AV1 wird an L2 gerichtet.

Beispiel-Konfiguration

1. Konfigurieren Sie virtuelle Server für Load Balancing und Content Switching.
   - `add lb vserver lbwrite -dbslb enabled`
   - `add lbvserver lbread MSSQL -dbslb enabled`
   - `add csvserver csv MSSQL 1.1.1.10 1433`
2. Konfigurieren Sie zwei Listener-Dienste, einen für jede Verfügbarkeitsgruppe, und fünf Dienste S1 bis S5, die die Datenbanken DB1 bis DB4 repräsentieren.
   - `add service L1 1.1.1.11 MSSQL 1433`
   - `add service L2 1.1.1.12 MSSQL 1433`
   - `add service s1 1.1.1.13 MSSQL 1433`
   - `add service s2 1.1.1.14 MSSQL 1433`
   - `add service s3 1.1.1.15 MSSQL 1433`
   - `add service s4 1.1.1.16 MSSQL 1433`
   - `add service s5 1.1.1.17 MSSQL 1433`
3. Binden Sie die Dienste an die virtuellen Load-Balancing-Server.
   - `bind lbvserver lbwrite L1`
   - `bind lbvserver lbwrite L2`
   - `bind lbvserver lbread s1`
   - `bind lbvserver lbread s2`
   - `bind lbvserver lbread s3`
   - `bind lbvserver lbread s4`
   - `bind lbvserver lbread s5`
4. Konfigurieren Sie Datenbankbenutzer.

- `add db user nsdbuser1 -password dd260427edf`
- `add db user nsdbuser2 -password ccd1234xyzw`

5. Konfigurieren Sie zwei Monitore, Monitor_l1 und Monitor_l2, für jeden Listener-Dienst, um die Liste der aktiven Datenbanken in dieser Verfügbarkeitsgruppe abzurufen. Fügen Sie einen Monitor hinzu, monitor1, um die Liste der Datenbanken für die sekundäre Datenbankserverinstanz abzurufen.
   - `add lb monitor monitor_L1 MSSQL-ECV -userName user1 -sqlQuery "SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_ b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address like '1.1.1.11'"-evalRule "MSSQL.RES.TYPE.NE(ERROR)" -storedb ENABLED`
   - `add lb monitor monitor_L2 MSSQL-ECV -userNameuser1 -sqlQuery "SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replicca b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address like '1.1.1.12'"-evalRule "MSSQL.RES.TYPE.NE(ERROR)"-storedb ENABLED`
   - `add lb monitor monitor1 MSSQL-ECV -userNameuser1 -sqlQuery "SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_states b ON a.replica_id=b.replica_id WHERE b.role = 2"-evalRule "MSSQL.RES.TYPE.NE(ERROR)"-storedb ENABLED`
6. Konfigurieren Sie Lese- und Schreibrechtlinien.
   - `add cs policy pol_write -rule "MSSQL.REQ.QUERY.TEXT.CONTAINS("insert")"`
   - `add cs policy pol_read -rule "MSSQL.REQ.QUERY.TEXT.CONTAINS("select")"`
7. Binden Sie die Richtlinien an den virtuellen Content Switching-Server.
   - `bind csvserver csv -targetLBVserver lbwrite -policyName pol_write -priority 11`
   - `bind csvserver csv -targetLBVserver lbread -policyName pol_read -priority 12`
8. Binden Sie Monitore an die Dienste. Binden Sie Monitore an die Dienste L1 und L2, um die Liste der aktiven Datenbanken für die Verfügbarkeitsgruppe abzurufen, für die sie der Listener ist. Binden Sie Monitore an alle Dienste, die an den schreibgeschützten virtuellen Server gebunden sind.
   - `bind service L1 -monitorName monitor_L1`

- bind service L2 -monitorName monitor_L2
- bind service s1 -monitorName monitor1
- bind service s2 -monitorName monitor1
- bind service s3 -monitorName monitor1
- bind service s4 -monitorName monitor1
- bind service s5 -monitorName monitor1

Konfigurationsbeispiele für den virtuellen MSSQL-Server

Um einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich zu konfigurieren, gehen Sie wie folgtvor:

```
add lb vserver DBSpecificLB1 MSSQL 192.0.2.10 1433 -dbsLb ENABLED

Done

show lb vserver DBSpecificLB1

DBSpecificLB1 (192.0.2.10:1433) - MSSQL Type: ADDRESS
. . .
DBS_LB: ENABLED

Done
<!--NeedCopy-->
```

Um Dienste zu konfigurieren:

Dienst hinzufügen msservice1 5.5.5.5 MSSQL 1433

So konfigurieren Sie einen Monitor zum Abrufen der Namen aller aktiven Datenbanken, die in einem Dienst gehostet werden, mithilfe der Befehlszeile:

```
add lb monitor mssql-monitor1 MSSQL-ECV -userName user1 -sqlQuery "
    select name from sys.databases where state=0" -evalRule "MSSQL.RES.
    TYPE.NE(ERROR)" -storedb EN

Done

show lb monitor mssql-monitor1

1)   Name.......: mssql-monitor1    Type......: MSSQL-ECV

...

Special parameters: Database.....:""
```



```
12
13 User name.....:"user1"
14
15 Query..:select name from sys.databases where state=0 EvalRule...:MSSQL.
       RES.TYPE.NE(ERROR)
16
17 Version...:70 STORE_DB...:ENABLED
18
19 Done
20 <!--NeedCopy-->
```

Konfigurationsbeispiele für den virtuellen MySQL-Server

Um einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich zu konfigurieren, gehen Sie wie folgtvor:

```
1 add lb vserver DBSpecificLB1 MYSQL 192.0.2.10 3306 -dbsLb ENABLED
2
3 Done
4
5 show lb vserver DBSpecificLB1
6
7 DBSpecificLB1 (192.0.2.10:3306) - MYSQL Type: ADDRESS
8
9 . . .
10
11 DBS_LB: ENABLED
12
13 Done
14 <!--NeedCopy-->
```

Um Dienste zu konfigurieren:

```
1 add service msservice1 5.5.5.5 MYSQL 3306
2 <!--NeedCopy-->
```

So konfigurieren Sie einen Monitor zum Abrufen der Namen aller aktiven Datenbanken, die in einem Dienst gehostet werden, mithilfe der Befehlszeile:

```
1 add lb monitor mysql-monitor1 MYSQL-ECV -userName user1 -sqlQuery "show
      databases" -evalRule "MYSQL.RES.TYPE.NE(ERROR)" -storedb ENABLED
2
3 Done
4
```



```
show lb monitor mysql-monitor1

1)     Name.......: mysql-monitor1  Type......: MYSQL-ECV  State....:
   ENABLED

...

Special parameters: Database.....:""

User name.....:"user1" Query..:show databases

EvalRule...:MYSQL.RES.TYPE.NE(ERROR) STORE_DB...:ENABLED

Done
<!--NeedCopy-->
```

DataStream-Referenz

May 11, 2023

Diese Referenz beschreibt die MySQL- und TDS-Protokolle, die Datenbankversionen, die Authentifizierungsmethoden und die Zeichensätze, die von der DataStream-Funktion unterstützt werden. Es beschreibt auch, wie der NetScaler mit Transaktionsanfragen und speziellen Abfragen umgeht, die den Status einer Verbindung ändern.

Sie können die NetScaler-Appliance auch so konfigurieren, dass sie Prüfprotokollmeldungen für die DataStream-Funktion generiert.

Unterstützte Datenbankversionen, Protokolle und Authentifizierungsmethoden

	MySQL-Datenbank	MS SQL-Datenbank
Datenbankversionen	MySQL-Datenbankversionen 4.1, 5.0, 5.1, 5.4, 5.5, 5.6	MS SQL-Datenbankversionen 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 (Kerberos-Authentifizierungsunterstützung)

	MySQL-Datenbank	MS SQL-Datenbank
Protokolle	MySQL Protokoll Version 10. Informationen zum MySQL-Protokoll finden Sie unter MySQL Client/Server Protocol	Tabular Data Stream (TDS) Protokoll Version 7.1 und höher. Informationen zum TDS-Protokoll finden Sie unter Tabular Data Stream Protocol
Authentifizierungsmethoden	Die native MySQL-Authentifizierung wird unterstützt.	Die SQL-Serverauthentifizierung und die Windows-Authentifizierung (Kerberos/NTLM) werden unterstützt.

Zeichensätze

Die DataStream-Funktion unterstützt nur den UTF-8-Zeichensatz.

Der vom Client beim Senden einer Anfrage verwendete Zeichensatz kann sich von dem Zeichensatz unterscheiden, der in den Antworten des Datenbankservers verwendet wird. Der Zeichensatz-Parameter wird zwar während des Verbindungsaufbaus gesetzt, kann aber jederzeit geändert werden, indem eine SQL-Abfrage gesendet wird. Der Zeichensatz ist mit einer Verbindung verknüpft, weshalb Anfragen für Verbindungen mit einem Zeichensatz nicht auf eine Verbindung mit einem anderen Zeichensatz gemultiplext werden können.

Die NetScaler-Appliance analysiert die vom Client gesendeten Abfragen und die vom Datenbankserver gesendeten Antworten.

Der einer Verbindung zugeordnete Zeichensatz kann nach dem ersten Handshake mithilfe der folgenden zwei Abfragen geändert werden:

```
SET NAMES <charset> COLLATION <collation>

SET CHARACTER SET <charset>
<!--NeedCopy-->
```

Transaktionen

In MySQL werden Transaktionen mithilfe des Verbindungsparameters AUTOCOMMIT oder der BEGIN:COMMIT-Abfragen identifiziert. Der AUTOCOMMIT-Parameter kann während des ersten

Handshakes oder nach dem Verbindungsaufbau mithilfe der Abfrage SET AUTOCOMMIT festgelegt werden.

Die NetScaler-Appliance analysiert jede Abfrage explizit, um den Beginn und das Ende einer Transaktion zu bestimmen.

Im MySQL-Protokoll enthält die Antwort zwei Flags, die angeben, ob es sich bei der Verbindung um eine Transaktion handelt: die Flags TRANSACTION und AUTOCOMMIT.

Wenn es sich bei der Verbindung um eine Transaktion handelt, wird das TRANSACTION-Flag gesetzt. Oder, wenn der AutoCommit-Modus OFF ist, ist das AUTOCOMMIT-Flag nicht gesetzt. Die ADC-Appliance analysiert die Antwort, und wenn entweder das TRANSACTION-Flag gesetzt ist oder das AUTOCOMMIT-Flag nicht gesetzt ist, führt sie kein Verbindungsmultiplexing durch. Wenn diese Bedingungen nicht mehr zutreffen, beginnt die ADC-Appliance mit dem Verbindungsmultiplexen.

> **Hinweis**
>
> Transaktionen werden auch für MS SQL unterstützt.

Besondere Anfragen

Es gibt spezielle Abfragen wie SET und PREPARE, die den Status der Verbindung ändern und möglicherweise das Umschalten von Anfragen unterbrechen. Daher müssen diese Abfragen anders behandelt werden.

Beim Empfang einer Anfrage mit speziellen Abfragen sendet die NetScaler-Appliance eine OK-Antwort an den Client und speichert die Anfrage auch in der Verbindung.

Wenn eine nicht spezielle Abfrage, wie INSERT und SELECT, zusammen mit einer gespeicherten Abfrage empfangen wird, sucht die ADC-Appliance nach der serverseitigen Verbindung, über die die gespeicherte Abfrage bereits an den Datenbankserver gesendet wurde. Wenn keine solchen Verbindungen bestehen, erstellt die ADC-Appliance eine Verbindung und sendet zuerst die gespeicherte Abfrage und dann die Anforderung mit der nicht speziellen Abfrage.

In den Spezialabfragen SET, USE db und INIT_DB ändert die Appliance ein Feld in der serverseitigen Verbindung, das der speziellen Abfrage entspricht. Diese Änderung führt zu einer besseren Wiederverwendung der serverseitigen Verbindung.

In jeder Verbindung werden nur 16 Abfragen gespeichert.

Im Folgenden finden Sie eine Liste der speziellen Abfragen, für die die ADC-Appliance ein modifiziertes Verhalten aufweist.

- SET-Abfrage

  Die SET-SQL-Abfragen definieren Variablen, die mit der Verbindung verknüpft sind. Diese Abfragen werden auch verwendet, um globale Variablen zu definieren, aber derzeit kann die ADC-

Appliance nicht zwischen lokalen und globalen Variablen unterscheiden. Für diese Abfrage verwendet die ADC-Appliance den Mechanismus „Speichern und Weiterleiten“.

- USE <db> query

  Mit dieser Abfrage kann der Benutzer die einer Verbindung zugeordnete Datenbank ändern. In diesem Fall analysiert die ADC-Appliance den gesendeten <db> Wert und ändert ein Feld in der serverseitigen Verbindung, um die neue zu verwendende Datenbank widerzuspiegeln.

- INIT_DB-Befehl

  Mit dieser Abfrage kann der Benutzer die einer Verbindung zugeordnete Datenbank ändern. In diesem Fall analysiert die ADC-Appliance den gesendeten <init_db> Wert und ändert ein Feld in der serverseitigen Verbindung, um die neue zu verwendende Datenbank widerzuspiegeln.

- COM_PREPARE

  Die ADC-Appliance stoppt die Anforderungsumschaltung beim Empfang dieses Befehls.

- Abfrage VORBEREITEN

  Diese Abfrage wird verwendet, um vorbereitete Anweisungen zu erstellen, die einer Verbindung zugeordnet sind. Für diese Abfrage verwendet die ADC-Appliance den Mechanismus „Speichern und Weiterleiten“.

Unterstützung für Audit-Log-Nachrichten

Sie können die NetScaler-Appliance jetzt so konfigurieren, dass sie Prüfprotokollmeldungen für die DataStream-Funktion generiert. Prüfprotokollmeldungen werden generiert, wenn clientseitige und serverseitige Verbindungen hergestellt, geschlossen oder unterbrochen werden. Die Kategorien von Nachrichten, die Sie protokollieren und anzeigen können, sind ERROR und INFO. Fehlermeldungen für clientseitige Verbindungen beginnen mit „CS“ und Fehlermeldungen für serverseitige Verbindungen beginnen mit „SS“. „ Zusätzliche Informationen werden bei Bedarf bereitgestellt. Protokollmeldungen für geschlossene Verbindungen (CS_CONN_CLOSED) enthalten beispielsweise nur die Verbindungs-ID. Protokollmeldungen für etablierte Verbindungen (CS_CONN_ESTD) enthalten jedoch Informationen wie Benutzername, Datenbankname und Client-IP-Adresse zusätzlich zur Verbindungs-ID.

Domain-Namenssystem

May 11, 2023

Hinweis: Ab Version 13.0 Build 41.x ist die NetScaler-Appliance im ADNS- und Proxy-Modus vollständig mit dem DNS-Flag-Tag 2019 kompatibel.

Sie können die NetScaler-Appliance so konfigurieren, dass sie als autorisierender Domänennamenserver (ADNS-Server) für eine Domäne fungiert. Fügen Sie die DNS-Ressourceneinträge hinzu, die zu der Domäne gehören, für die die Appliance autorisierend ist, und konfigurieren Sie die Ressourceneintragsparameter. Sie können die Appliance auch als Proxy-DNS-Server konfigurieren, der die Last einer Farm von DNS-Nameservern ausgleicht, die sich entweder innerhalb oder außerhalb Ihres Netzwerks befinden. Konfigurieren Sie die Appliance als Endresolver und Forwarder. Sie können DNS-Suffixe konfigurieren, die die Namensauflösung ermöglichen, wenn vollqualifizierte Domainnamen nicht konfiguriert sind. Die Appliance unterstützt auch die DNS ANY-Abfrage, die alle Datensätze abruft, die zu einer Domäne gehören.

Sie können die Appliance so konfigurieren, dass sie gleichzeitig als autorisierender DNS-Server für eine Domäne und als DNS-Proxyserver für eine andere Domäne fungiert. Wenn Sie die Appliance als autorisierenden DNS-Server oder DNS-Proxyserver für eine Zone konfigurieren, können Sie der Appliance ermöglichen, den TCP für Antwortgrößen zu verwenden, die die für das User Datagram Protocol (UDP) angegebene Größenbeschränkung überschreiten.

So funktioniert DNS auf dem NetScaler

Sie können die NetScaler-Appliance so konfigurieren, dass sie als ADNS-Server, DNS-Proxyserver, Endresolver und Weiterleitung fungiert. Sie können DNS-Ressourceneinträge auf der NetScaler-Appliance hinzufügen, einschließlich der folgenden Datensätze:

- Service (SRV) -Aufzeichnungen
- IPv6 (AAAA) -Aufzeichnungen
- Adresse (A) Aufzeichnungen
- Mail-Exchange (MX) -Datensätze
- Aufzeichnungen über kanonische Namen (CNAME)
- Pointer (PTR) -Aufzeichnungen
- Beginn der Behörde (SOA) -Aufzeichnungen
- Text (TXT) -Datensätze
- Name Authority Pointer (NAPTR) -Datensätze
- DNSKEY
- Datensätze für die Autorisierung der Zertifizierungsstelle (CAA)

Sie können den NetScaler auch so konfigurieren, dass der Lastenausgleich externer DNS-Nameserver erfolgt.

Die NetScaler-Appliance kann als Autorität für eine Domäne konfiguriert werden. Fügen Sie gültige SOA- und NS-Datensätze für die Domäne hinzu.

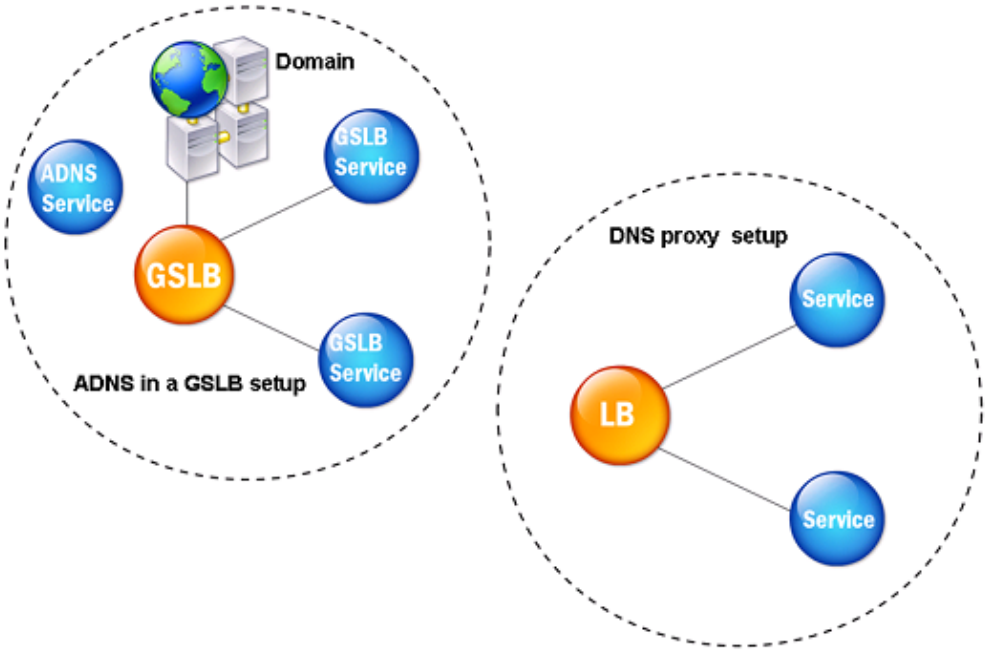
Ein ADNS-Server ist ein DNS-Server, der vollständige Informationen über eine Zone enthält.

Um die NetScaler-Appliance als ADNS-Server für eine Zone zu konfigurieren, müssen Sie einen ADNS-Dienst hinzufügen und dann die Zone konfigurieren. Dazu fügen Sie gültige SOA- und NS-

Records für die Domäne hinzu. Wenn ein Client eine DNS-Anforderung sendet, durchsucht die NetScaler-Appliance die konfigurierten Ressourceneinträge nach dem Domänennamen. Sie können den ADNS-Dienst für die Verwendung mit der Funktion NetScaler Global Server Load Balancing (GSLB) konfigurieren.

Sie können eine Subdomain delegieren, indem Sie NS-Datensätze für die Subdomain zur Zone der übergeordneten Domäne hinzufügen. Sie können dann den NetScaler für die Subdomain autorisierend machen, indem Sie für jeden der Subdomain-Namenserver einen “Glue-Record” hinzufügen. Wenn GSLB konfiguriert ist, trifft der NetScaler basierend auf seiner Konfiguration eine Entscheidung für den GSLB-Lastausgleich und antwortet mit der IP-Adresse des ausgewählten virtuellen Servers. Die folgende Abbildung zeigt die Entitäten in einem ADNS GSLB-Setup und einem DNS-Proxy-Setup.

Abbildung 1. DNS-Proxy-Entity



Die NetScaler-Appliance kann als DNS-Proxy fungieren. Das Zwischenspeichern von DNS-Datensätzen, was eine wichtige Funktion eines DNS-Proxys ist, ist standardmäßig auf der NetScaler-Appliance aktiviert. Durch das Zwischenspeichern kann die NetScaler-Appliance schnelle Antworten auf wiederholte Übersetzungen liefern. Erstellen Sie einen virtuellen DNS-Server mit Lastausgleich und DNS-Dienste, und binden Sie diese Dienste dann an den virtuellen Server.

Der NetScaler bietet zwei Optionen: minimale Lebenszeit (TTL) und maximale TTL für die Konfiguration der Lebensdauer der zwischengespeicherten Daten. Bei den zwischengespeicherten Daten tritt eine Zeitüberschreitung auf, wie in Ihren Einstellungen für diese beiden Optionen angegeben. Der NetScaler überprüft die TTL des DNS-Eintrags, der vom Server kommt. Wenn die TTL kleiner als die konfigurierte Mindest-TTL ist, wird sie durch die konfigurierte minimale TTL ersetzt. Wenn die TTL größer als die konfigurierte maximale TTL ist, wird sie durch die konfigurierte maximale TTL ersetzt.

Der NetScaler ermöglicht auch das Zwischenspeichern negativer Antworten für eine Domäne. Eine negative Antwort weist darauf hin, dass Informationen zu einer angeforderten Domäne nicht existieren oder dass der Server keine Antwort auf die Abfrage geben kann. Die Speicherung dieser Informationen wird als *negatives Caching*bezeichnet. Negatives Caching beschleunigt die Antworten auf Abfragen in einer Domäne und kann optional den Datensatztyp bereitstellen.

Eine negative Reaktion kann eine der folgenden sein:

- NXDOMAIN-Fehlermeldung - Wenn eine negative Antwort im lokalen Cache vorhanden ist, gibt NetScaler eine Fehlermeldung (NXDOMAIN) zurück. Wenn sich die Antwort nicht im lokalen Cache befindet, wird die Abfrage an den Server weitergeleitet, und der Server gibt einen NXDOMAIN-Fehler an den NetScaler zurück. Der NetScaler speichert die Antwort lokal im Cache und gibt dann die Fehlermeldung an den Client zurück.
- NODATA-Fehlermeldung - Der NetScaler sendet eine NODATA-Fehlermeldung, wenn der Domainname in der Abfrage gültig ist, Datensätze des angegebenen Typs jedoch nicht verfügbar sind.

Der NetScaler unterstützt die rekursive Auflösung von DNS-Anforderungen. Bei rekursiver Auflösung sendet der Resolver (DNS-Client) eine rekursive Abfrage nach einem Domänennamen an einen Nameserver. Wenn der abgefragte Nameserver für die Domäne autorisierend ist, antwortet er mit dem angeforderten Domainnamen. Andernfalls fragt der NetScaler die Nameserver rekursiv ab, bis der angeforderte Domänenname gefunden wurde.

Bevor Sie die rekursive Abfrageoption anwenden können, müssen Sie sie zuerst aktivieren. Sie können auch festlegen, wie oft der DNS-Resolver eine Auflösungsanfrage senden muss (DNS-Wiederholungen), falls eine DNS-Suche fehlschlägt.

Sie können den NetScaler als DNS-Weiterleitung konfigurieren. Ein Forwarder leitet DNS-Anfragen an externe Nameserver weiter. Mit dem NetScaler können Sie externe Nameserver hinzufügen und die Namensauflösung für Domänen außerhalb des Netzwerks bereitstellen. Mit dem NetScaler können Sie auch die Priorität der Namenssuche auf DNS oder Windows Internet Name Service (WINS) festlegen.

Ermöglichen Sie der ADC-Appliance, DNS zu verwenden, um den Hostnamen in die entsprechende IP-Adresse aufzulösen

Hinweis: Sie benötigen ein SSH-Dienstprogramm, um auf die Befehlszeilenschnittstelle (CLI) der Appliance zuzugreifen.

Standardmäßig kann die ADC-Appliance den Hostnamen nicht in die entsprechende IP-Adresse auflösen. Führen Sie die folgenden Aufgaben aus, um die Namensauflösung auf der Appliance zu aktivieren:

1. Definieren Sie Nameserver.
2. Definieren Sie ein DNS-Suffix.

Wichtige Hinweise

Führen Sie die DNS-Suche von der CLI aus. DNS-Lookups von der Shell-Eingabeaufforderung des FreeBSD-Betriebssystems schlagen fehl, weil der Eintrag in der Datei /etc/resolv.conf auf die 127.0.0.2 IP-Adresse verweist.

Die folgenden Befehle werden durch den Befehl `drill` in der FreeBSD-CLI der Appliance ersetzt, die mit dem Befehl `shell` erreichbar ist:

```
- host
- dig
- getent/MIP
- nslookup
<!--NeedCopy-->
```

Anstatt beispielsweise mit `dig www.google.com @8.8.8.8` den "A"-Datensatz "www.google.com" auf dem Namenserver "8.8.8.8" abzufragen, können Sie den Befehl `drill www.google.com @8.8.8.8` ausführen. Der Befehl `drill` zeigt das gleiche Ergebnis wie der Befehl `dig`.

```
root@lab# drill www.google.com @8.8.8.8
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 57980
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; www.google.com. IN A

;; ANSWER SECTION:
www.google.com. 300 IN A 142.250.187.196

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

```



```
;; Query time: 53 msec
;; SERVER: 8.8.8.8
;; WHEN: Thu Jun 9 11:04:55 2022
;; MSG SIZE rcvd: 48
<!--NeedCopy-->
```

Wenn die Appliance den DNS-Server nicht an seiner SNIP-Adresse anpingen kann, wird der Serverstatus als ausgefallen angezeigt. Ein erfolgreicher Ping ist wichtig, wenn sich das Gerät hinter einer Firewall befindet.

CLI-Konfiguration

Geben Sie in der Befehlszeile Folgendes ein:

```
add dns nameServer <Name_Server_IP_Address>
add dns suffix <DNS_Suffix>
<!--NeedCopy-->
```

Um die Konfiguration zu überprüfen, geben Sie Folgendes ein:

```
show dns nameServer
show dns suffix
<!--NeedCopy-->
```

Um die DNS-Auflösung zu testen, geben Sie:

```
show dns addrec <Host_Name>
<!--NeedCopy-->
```

GUI-Konfiguration

1. Navigieren Sie zu **Traffic Management > DNS > Nameserver > Hinzufügen**.
2. Geben **Sie im Dialogfeld Nameserver erstellen** die IP-Adresse des Nameservers ein und klicken Sie auf **Erstellen**.
3. Navigieren Sie zu **Traffic Management > DNS > DNS-Suffix > Hinzufügen**.
4. Geben **Sie im Dialogfeld DNS-Suffix erstellen** das DNS-Suffix ein, z. B. example.com, das für alle Host-Abfragen verwendet werden soll, und klicken Sie auf **Erstellen**.

Runder Robin DNS

Wenn ein Client eine DNS-Anforderung sendet, um den DNS-Ressourceneintrag zu finden, erhält er eine Liste von IP-Adressen, die auf den Namen in der DNS-Anforderung aufgelöst werden. Der Client

verwendet dann eine der IP-Adressen in der Liste, im Allgemeinen den ersten Datensatz oder die erste IP-Adresse. Daher wird ein einzelner Server für die gesamte TTL des Caches verwendet und ist überlastet, wenn viele Anfragen eingehen.

Wenn der NetScaler eine DNS-Anforderung erhält, antwortet er, indem er die Reihenfolge der Liste der DNS-Ressourceneinträge in einer Round-Robin-Methode ändert. Diese Funktion wird *Round-Robin-DNS*genannt. Round-Robin verteilt den Verkehr gleichmäßig zwischen Rechenzentren. Der NetScaler führt diese Funktion automatisch aus. Sie müssen dieses Verhalten nicht konfigurieren.

Funktioneller Überblick

Wenn der NetScaler als ADNS-Server konfiguriert ist, gibt er die DNS-Einträge in der Reihenfolge zurück, in der die Datensätze konfiguriert sind. Wenn der NetScaler als DNS-Proxy konfiguriert ist, gibt er die DNS-Einträge in der Reihenfolge zurück, in der er die Datensätze vom Server empfängt. Die Reihenfolge der im Cache vorhandenen Datensätze stimmt mit der Reihenfolge überein, in der Datensätze vom Server empfangen werden.

Der NetScaler ändert dann die Reihenfolge, in der Datensätze in der DNS-Antwort gesendet werden, in einer Round-Robin-Methode. Die erste Antwort enthält den ersten Datensatz in der Reihenfolge, die zweite Antwort enthält den zweiten Datensatz in der Folge, und die Reihenfolge wird in derselben Reihenfolge fortgesetzt. Daher können Clients, die denselben Namen anfordern, eine Verbindung zu verschiedenen IP-Adressen herstellen.

Beispiel für DNS-Round-Robin

Betrachten Sie als Beispiel für Round-Robin-DNS-Datensätze, die wie folgt hinzugefügt wurden:

```
1   add dns addRec ns1 1.1.1.1  add dns addRec ns1 1.1.1.2  add dns
       addRec ns1 1.1.1.3  add dns addRec ns1 1.1.1.4
2 <!--NeedCopy-->
```

Die Domain abc.com ist wie folgt mit einem NS-Datensatz verknüpft:

```
1   add dns nsrec abc.com. ns1
2 <!--NeedCopy-->
```

Wenn der NetScaler eine Abfrage für den A-Datensatz von ns1 erhält, werden die Adressdatensätze wie folgt in einer Round-Robin-Methode bedient. In der ersten DNS-Antwort wird 1.1.1.1 als erster Datensatz serviert:

```
1   ns1.                    1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4
```



```
<!--NeedCopy-->
```

In der zweiten DNS-Antwort wird die zweite IP-Adresse 1.1.1.2 als erster Datensatz serviert:

```
  ns1.                    1H IN A         1.1.1.2  ns1.
                         1H IN A         1.1.1.3  ns1.
                         1H IN A         1.1.1.4  ns1.
                         1H IN A         1.1.1.1
<!--NeedCopy-->
```

In der dritten DNS-Antwort wird die dritte IP-Adresse 1.1.1.2 als erster Datensatz serviert:

```
  ns1.                    1H IN A         1.1.1.3  ns1.
                         1H IN A         1.1.1.4  ns1.
                         1H IN A         1.1.1.1  ns1.
                         1H IN A         1.1.1.2
<!--NeedCopy-->
```

Konfiguration von DNS-Ressourceneinträgen

May 11, 2023

Sie konfigurieren Ressourceneinträge auf der Citrix® ADC Appliance, wenn Sie das Gerät als ADNS-Server für eine Zone konfigurieren. Sie können auch Ressourceneinträge auf der Appliance konfigurieren, wenn die Ressourceneinträge zu einer Zone gehören, für die die Appliance ein DNS-Proxyserver ist. Auf der Appliance können Sie die folgenden Datensatztypen konfigurieren:

- Aufzeichnungen über den Dienst
- AAAA-Datensätze
- Adressdatensätze
- Mail Exchange-Datensätze
- Namenserver-Datensätze
- Kanonische Aufzeichnungen
- Pointer Aufzeichnungen
- NAPTR-Aufzeichnungen
- Beginn der Autoritätsaufzeichnungen
- Textdatensätze
- Datensätze für die Autorisierung der Zertifizierungsstelle (CAA)

In der folgenden Tabelle sind die Datensatztypen aufgeführt, die Sie für einen Domänennameneintrag auf der NetScaler-Appliance konfigurieren können. Sie können beispielsweise maximal 25 IP-Adressen für einen Datensatz konfigurieren.

Tabelle 1. Datensatztyp und -nummer konfigurierbar

Datensatztyp	Anzahl der Datensätze
Adresse (A)	25
IPv6 (AAAA)	5
E-Mail-Austausch (MX)	12
Namenserver (NS)	16
Service (SRV)	8
Pointer (PTR)	20
Kanonischer Name (CNAME)	1
Start der Autorität (SOA)	1
Text (TXT)	20
Naming Authority Pointer (NAPTR)	20
Autorisierung der Zertifizierungsstelle (CAA)	20

> **Hinweis:**
>
> Die maximale Anzahl von IP-Adressen für einen bestimmten Hostnamen ist 25. Die Anzahl der verschiedenen Adressdatensätze kann jedoch mehr als 25 betragen.

Erstellen von SRV-Datensätzen für einen Dienst

May 11, 2023

Der SRV-Eintrag enthält Informationen zu den Diensten, die auf der NetScaler-Appliance verfügbar sind. Ein SRV-Datensatz enthält die folgenden Informationen:

- Name des Dienstes und des Protokolls
- Domänenname
- TTL
- DNS-Klasse
- Priorität des Ziels
- Gewicht von Datensätzen mit derselben Priorität
- Port des Dienstes
- Hostname des Dienstes.

Der NetScaler wählt zuerst den SRV-Datensatz mit der niedrigsten Prioritätseinstellung aus. Wenn ein Service mehrere SRV-Datensätze mit derselben Priorität hat, verwenden die Clients das Gewichtungsfeld, um zu bestimmen, welcher Host verwendet werden soll.

Fügen Sie mithilfe der CLI einen SRV-Datensatz hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen SRV-Datensatz hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add dns srvRec <domain> <target> -priority <positive_integer> -
     weight <positive_integer> -port <positive_integer> [-TTL <secs>]
2 -  sh dns srvRec <domain>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns srvRec _http._tcp.example.com nameserver1.com -priority 1 -
     weight 1 -port 80
2  Done
3 > show dns srvRec _http._tcp.example.com
4 1)      Domain Name : _http._tcp.example.com
5         Target Host : nameserver1.com
6         Priority : 1    Weight : 1
7         Port : 80       TTL : 3600 secs
8  Done
9 <!--NeedCopy-->
```

Ändern oder entfernen Sie einen SRV-Datensatz mithilfe der CLI

- Um einen SRV-Datensatz zu ändern, geben Sie Folgendes ein:
  - Der Befehl `set dns srvRec`
  - Der Name der Domain, für die der SRV-Eintrag konfiguriert ist
  - Der Name des Zielhosts, der den zugehörigen Dienst hostet
  - Die zu ändernden Parameter mit ihren neuen Werten
- Um einen SRV-Datensatz zu entfernen, geben Sie Folgendes ein:
  - Der Befehl `rm dns srvRec`
  - Der Name der Domain, für die der SRV-Eintrag konfiguriert ist
  - Der Name des Zielhosts, der den zugehörigen Dienst hostet

Konfigurieren Sie einen SRV-Datensatz mithilfe der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > SRV Records** und erstellen Sie einen SRV-Eintrag.

Erstellen von AAAA-Einträgen für einen Domainnamen

February 16, 2021

Ein AAAA-Ressourceneintrag speichert eine einzelne IPv6-Adresse.

Hinzufügen eines AAAA-Datensatzes mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen AAAA-Datensatz hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]
2 -  show dns aaaaRec <hostName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns aaaaRec www.example.com 2001:0db8:0000:0000:0000:0000:1428:57
     ab
2  Done
3 > show dns aaaaRec www.example.com
4 1)      Host Name : www.example.com
5         Record Type : ADNS              TTL : 5 secs
6         IPV6 Address : 2001:db8::1428:57ab
7  Done
8 <!--NeedCopy-->
```

Um einen AAAA-Eintrag und alle mit dem Domainnamen verbundenen IPv6-Adressen zu entfernen, geben Sie den `rm dns aaaaRec` Befehl und den Domänennamen ein, für den der AAAA-Eintrag konfiguriert ist. Um nur eine Teilmenge der IPv6-Adressen zu entfernen, die mit dem Domainnamen in einem AAAA-Eintrag verknüpft sind, geben Sie Folgendes ein:

- `rm dns aaaaRec` Befehl
- Der Domainname, für den der AAAA-Eintrag konfiguriert ist
- Die IPv6-Adressen, die Sie entfernen möchten

Hinzufügen eines AAAA-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > AAAA Records** und erstellen Sie einen AAAA-Eintrag.

Erstellen von Adressdatensätzen für einen Domänennamen

May 11, 2023

Adresseinträge (A) sind DNS-Einträge, die einen Domainnamen einer IPv4-Adresse zuordnen.

Sie können keine Adressdatensätze für einen Host löschen, der am Global Server Load Balancing (GSLB) teilnimmt. Der NetScaler löscht jedoch Adressdatensätze, die für GSLB-Domänen hinzugefügt wurden, wenn Sie die Domäne von einem virtuellen GSLB-Server trennen. Nur benutzerkonfigurierte Datensätze können manuell gelöscht werden. Sie können keinen Datensatz für einen Host löschen, auf den Datensätze wie NS, MX oder CNAME verweisen.

Fügen Sie mithilfe der CLI einen Adressdatensatz hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen Adressdatensatz hinzuzufügen und die Konfiguration zu überprüfen:

```
-  add dns addRec <hostName> <IPAddress> [-TTL <secs>]
-  show dns addRec <hostName>
<!--NeedCopy-->
```

Beispiel:

```
> add dns addRec ns.example.com 192.0.2.0
 Done
> show dns addRec ns.example.com
1)      Host Name : ns.example.com
        Record Type : ADNS                      TTL : 5 secs
        IP Address : 192.0.2.0
 Done
<!--NeedCopy-->
```

Um einen Adressdatensatz und alle mit dem Domainnamen verknüpften IP-Adressen zu entfernen, geben Sie den `rm dns addRec` Befehl und den Domainnamen ein, für den der Adressdatensatz konfiguriert ist. Um nur eine Teilmenge der IP-Adressen zu entfernen, die dem Domainnamen in einem Adressdatensatz zugeordnet sind, geben Sie Folgendes ein:

- `rm dns addRec` beherrschen

- Der Domainname, für den der Adressdatensatz konfiguriert ist
- Die IP-Adressen, die Sie entfernen möchten

Fügen Sie mithilfe der GUI einen Adressdatensatz hinzu

Navigieren Sie zu **Traffic Management > DNS > Einträge > Adressdatensätze** und erstellen Sie einen Adressdatensatz.

Erstellen von MX-Datensätzen für einen Mail-Exchange-Server

February 16, 2021

Mail Exchange (MX) -Datensätze werden verwendet, um E-Mail-Nachrichten über das Internet zu leiten. Ein MX-Eintrag enthält eine MX-Voreinstellung, die den zu verwendenden MX-Server angibt. Die MX-Voreinstellungswerte reichen von 0 bis 65536. Ein MX-Eintrag enthält eine eindeutige MX-Präferenznummer. Sie können die MX-Voreinstellung und die TTL-Werte für einen MX-Eintrag festlegen.

Wenn eine E-Mail-Nachricht über das Internet gesendet wird, sendet ein E-Mail-Übertragungs-Agent eine DNS-Abfrage, die den MX-Eintrag für den Domänennamen anfordert. Diese Abfrage gibt eine Liste der Hostnamen von Mail-Exchange-Servern für die Domäne zusammen mit einer Einstellungsnummer zurück. Wenn keine MX-Einträge vorhanden sind, wird die Anforderung für den Adressdatensatz dieser Domäne gestellt. Eine einzelne Domäne kann mehrere Mail-Exchange-Server haben.

Hinzufügen eines MX-Datensatzes mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen MX-Eintrag hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <
     secs>]
2 -  show dns mxRec <domain>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns mxRec example.com -mx mail.example.com -pref 1
2  Done
3 > show dns mxRec example.com
4 1)      Domain : example.com    MX Name : mail.example.com
5         Preference :   1        TTL : 5 secs
```



```
6   Done
7 <!--NeedCopy-->
```

Ändern oder Entfernen eines MX-Datensatzes mit der CLI

- Um einen MX-Record zu ändern, geben Sie den `set dns mxRec` Befehl, den Namen der Domäne, für die der MX-Eintrag konfiguriert ist, den Namen des MX-Records und die zu ändernden Parameter mit ihren neuen Werten ein.
- Um den TTL-Parameter auf seinen Standardwert festzulegen, geben Sie den `unset dns mxRec` Befehl, den Namen der Domäne, für die der MX-Eintrag konfiguriert ist, den Namen des MX-Records und -TTL ohne TTL-Wert ein. Sie können den `unset dns mxRec` Befehl verwenden, um nur den TTL-Parameter aufzuheben.
- Um einen MX-Eintrag zu entfernen, geben Sie den `rm dns mxRec` Befehl, den Namen der Domäne, für die der MX-Eintrag konfiguriert ist, und den Namen des MX-Records ein.

Hinzufügen eines MX-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > Mail Exchange-Datensätze** und erstellen Sie einen MX-Eintrag.

Erstellen von NS-Datensätzen für einen autorisierenden Server

February 16, 2021

NS-Einträge (Name Server) geben den autorisierenden Server für eine Domäne an. Sie können maximal 16 NS-Einträge konfigurieren. Sie können einen NS-Eintrag verwenden, um das Steuerelement einer Subdomäne an einen DNS-Server zu delegieren.

Erstellen eines NS-Datensatzes mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen NS-Datensatz zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add dns nsRec <domain> <nameServer> [-TTL <secs>]
2 -  show dns nsRec <domain>
3 <!--NeedCopy-->
```

Beispiel:


```
> add dns nsRec example.com nameserver1.example.com
 Done
> show dns nsRec example.com
1)      Domain : example.com    NameServer : nameserver1.example.com
        TTL : 5 sec
 Done
<!--NeedCopy-->
```

Um einen NS-Eintrag zu entfernen, geben Sie den `rm dns nsRec` Befehl, den Namen der Domäne, zu der der NS-Eintrag gehört, und den Namen des Nameservers ein.

Erstellen eines NS-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > Namenserver-Einträge** und erstellen Sie einen NS-Datensatz.

CNAME-Datensätze für eine Subdomain erstellen

May 11, 2023

Ein kanonischer Namenseintrag (CNAME-Eintrag) ist ein Alias für einen DNS-Namen. Diese Einträge sind nützlich, wenn mehrere Dienste den DNS-Server abfragen. Der Host, der über einen Adressdatensatz (A) verfügt, kann keinen CNAME-Datensatz haben.

Manchmal fordert eine NetScaler-Appliance im Proxymodus einen Adressdatensatz vom Cache statt vom Server an.

Fügen Sie mithilfe der CLI einen CNAME-Eintrag hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen CNAME-Eintrag zu erstellen und die Konfiguration zu überprüfen:

```
-  add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]
-  show dns cnameRec <aliasName>
<!--NeedCopy-->
```

Beispiel:

```
> add dns cnameRec www.example.com www.examplenw.com
 Done
> show dns cnameRec www.example.com
```



```
4          Alias Name      Canonical Name  TTL
5  1)      www.example.com        www.examplenw.com       5 secs
6   Done
7  <!--NeedCopy-->
```

Um einen CNAME-Eintrag für eine bestimmte Domain zu entfernen, geben Sie den `rm dns cnameRec` Befehl und den Alias des Domainnamens ein.

Fügen Sie mithilfe der GUI einen CNAME-Eintrag hinzu

Navigieren Sie zu **Traffic Management > DNS > Records > Canonical Records** und erstellen Sie einen CNAME-Eintrag.

CNAME-Einträge zwischenspeichern

Bei der Bereitstellung in einem Proxymodus sendet die ADC-Appliance die Abfrage für einen Adressdatensatz nicht immer an den Back-End-Server. Dieses Verhalten tritt auf, wenn für eine Antwort auf eine Anfrage nach einem Adressdatensatz eine teilweise CNAME-Kette im Cache vorhanden ist. Es gibt nur wenige Bedingungen, unter denen der ADC den teilweisen CNAME-Datensatz zwischenspeichert und die Abfrage aus dem Cache bereitstellt. Im Folgenden sind die Bedingungen aufgeführt:

- NetScaler muss in einem Proxymodus bereitgestellt werden.
- Die Antwort vom Backend-Server muss eine CNAME-Kette haben, für die der Datensatztyp des letzten Eintrags im Antwortabschnitt ein CNAME und der Fragetyp kein CNAME sein muss.
- Die Antwort vom Backend-Server darf keine No-Data- oder NX-Domain sein.
- Die Antwort des Backend-Servers muss eine verbindliche Antwort sein.

Erstellen von NAPTR-Datensätzen für Telekommunikationsdomäne

May 11, 2023

NAPTR (Naming Address Pointer) ist einer der am häufigsten verwendeten DNS-Einträge in der Telekommunikationsdomäne. NAPTR-Datensätze ordnen den Adressraum der Internettelefonie dem Internet-Adressraum zu. Sie ermöglichen es einem mobilen Gerät daher, eine Anfrage an den richtigen Server zu senden. Die Kombination von NAPTR-Datensätzen mit Service Records (SRV) ermöglicht die Verkettung mehrerer Datensätze, um komplexe Umschreibregeln zu bilden, die zu neuen Domainbezeichnungen oder Uniform Resource Identifiers (URIs) führen. Der DNS-Code für NAPTR ist 35.

NetScaler unterstützen NAPTR in zwei Modi: ADNS-Modus und Proxymodus. Im Proxymodus speichert der ADC die Antwort der Server im Cache und verwendet die zwischengespeicherten Datensätze, um zukünftige Abfragen zu verarbeiten. In NetScaler können maximal 20 NAPTR-Einträge für eine bestimmte Domäne hinzugefügt werden. NetScaler speichert die Antwort auf eine DNS-NAPTR-Datensatzabfrage im Cache. Alle nachfolgenden Anfragen für den NAPTR-Datensatz werden aus dem Cache bedient.

Erstellen Sie einen NAPTR-Datensatz mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen NAPTR-Datensatz hinzuzufügen und die Konfiguration zu überprüfen:

‘füge dns naptrRec hinzu [Flaggen][dienste](regexp|-replacement)\[-TTL]\‘

Entfernen Sie einen NAPTR-Datensatz mithilfe der CLU

```
rm dns naptrRec<domain> (<order> <preference> [-flags <string>] [-services
 <string>] (-regexp <expression> | -replacement <string>))| -recordId <
positive_integer>@)
```

Konfiguration eines NAPTR-Eintrags mithilfe der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > NAPTR-Einträge** und erstellen Sie einen NAPTR-Eintrag.

Erstellen von PTR-Datensätzen für IPv4- und IPv6-Adressen

February 16, 2021

Ein Zeigerdatensatz (PTR) übersetzt eine IP-Adresse in den Domänennamen. IPv4-PTR-Datensätze werden durch die Oktette einer IP-Adresse in umgekehrter Reihenfolge mit der Zeichenfolge in-addr.arpa dargestellt. am Ende angehängt. Beispielsweise ist der PTR-Eintrag für die IP-Adresse 1.2.3.4 4.3.2.1.in-addr.arpa.

IPv6-Adressen werden in umgekehrter Reihenfolge unter der Domäne IP6.ARPA zugeordnet. IPv6 Reverse-Maps verwenden eine Folge von Nibbles, die durch Punkte getrennt sind, mit dem Suffix .IP6.ARPA, wie in RFC 3596 definiert. Der Reverse-Lookup-Domänenname, der der Adresse 4321:0:1:2:3:4:567:89ab wäre z. B. b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.

Hinzufügen eines PTR-Datensatzes mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen PTR-Datensatz hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add dns ptrRec <reverseDomain> <domain> [-TTL <secs>]
2 -  show dns ptrRec <reverseDomain>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns ptrRec 0.2.0.192.in-addr.arpa example.com
2  Done
3 > show dns ptrRec 0.2.0.192.in-addr.arpa
4 1)      Reverse Domain Name : 0.2.0.192.in-addr.arpa
5         Domain Name : example.com              TTL : 3600 secs
6  Done
7 <!--NeedCopy-->
```

Um einen PTR-Eintrag zu entfernen, geben Sie den `rm dns ptrRec` Befehl und den Namen der umgekehrten Domäne ein, der dem PTR-Datensatz zugeordnet ist.

Hinzufügen eines PTR-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > PTR-Datensätze** und erstellen Sie einen PTR-Datensatz.

Erstellen von SOA-Datensätzen für autorisierende Informationen

February 16, 2021

Ein SOA-Eintrag (Start of Authority) wird nur an der Zonenspitze erstellt und enthält Informationen über die Zone. Der Datensatz enthält unter anderem den primären Nameserver, Kontaktinformationen (E-Mail) und standardmäßige (Mindest-) Time-to-Live-Werte (TTL) für Datensätze.

Erstellen eines SOA-Datensatzes mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen SOA-Datensatz hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add dns soaRec <domain> -originServer <originServerName> -contact <
     contactName>
```



```
-  sh dns soaRec <do main>
<!--NeedCopy-->
```

Beispiel:

```
> add dns soaRec example.com -originServer nameserver1.example.com -
   contact admin.example.com
 Done
> show dns soaRec example.com
1)      Domain Name : example.com
        Origin Server : nameserver1.example.com
        Contact : admin.example.com
        Serial No. : 100        Refresh : 3600 secs     Retry : 3 secs
        Expire : 3600 secs      Minimum : 5 secs        TTL : 3600 secs
 Done
<!--NeedCopy-->
```

Ändern oder Entfernen eines SOA-Datensatzes mit der CLI

- Um einen SOA-Eintrag zu ändern, geben Sie den`set dns soaRec` Befehl, den Namen der Domäne, für die der Datensatz konfiguriert ist, und die zu ändernden Parameter mit den neuen Werten ein.
- Um einen SOA-Eintrag zu entfernen, geben Sie den`rm dns soaRec` Befehl und den Namen der Domäne ein, für die der Datensatz konfiguriert ist.

Konfigurieren eines SOA-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > SOA-Einträge** und erstellen Sie einen SOA-Eintrag.

Erstellen von TXT-Datensätzen für beschreibendem Text

May 11, 2023

Domain-Hosts speichern TXT-Einträge zu Informationszwecken. Die RDATA-Komponente eines TXT-Eintrags, die aus einer oder mehreren Zeichenketten mit variabler Länge besteht, kann praktisch alle Informationen speichern, die ein Empfänger über die Domain benötigen könnte. Es kann auch Informationen über den Dienstanbieter, die Kontaktperson, E-Mail-Adressen und zugehörige Details enthalten. Der SPF-Schutz (Sender Policy Framework) war der prominenteste Anwendungsfall für den TXT-Datensatz.

Alle Konfigurationstypen (autorisierende DNS-, DNS-Proxy-, Endresolver- und Forwarder-Konfigurationen) auf der NetScaler-Appliance unterstützen TXT-Einträge. Sie können einer Domain maximal 20 TXT-Ressourceneinträge hinzufügen. Jeder Ressourcendatensatz wird mit einer eindeutigen, intern generierten Datensatz-ID gespeichert. Ein TXT-Ressourcendatensatz kann bis zu sechs Zeichenketten enthalten, von denen jede bis zu 255 Zeichen enthalten kann. Sie können die ID eines Datensatzes anzeigen und damit den Datensatz löschen. Sie können einen TXT-Ressourceneintrag jedoch nicht ändern.

Erstellen Sie einen TXT-Ressourcendatensatz mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen TXT-Ressourceneintrag zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add dns txtRec <domain> <string> ... [-TTL <secs>]
2 -  show dns txtRec [<domain> | -type <type>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns txtRec www.example.com "Contact: Mark" "Email: mark@example.
     com" -TTL 36000
2  Done
3 > show dns txtRec www.example.com
4 1)  Domain : www.example.com    Record id: 13783       TTL : 36000 secs
      Record Type : ADNS
5         "Contact: Mark"
6         "Email: mark@example.com"
7  Done
8 <!--NeedCopy-->
```

Teilen Sie die Zeichenfolge in einem TXT-Ressourcendatensatz mithilfe der CLI auf

Wenn Sie eine Zeichenfolge mit mehr als 255 Zeichen haben, können Sie die Zeichenketten unter Berücksichtigung der Beschränkung auf sechs Zeichenketten aufteilen. Jede Zeichenfolge kann 254 Byte lang sein.

```
1 add dns txtrec domain.com "string1" "string2" string3" "string4"
2 <!--NeedCopy-->
```

Beispiel:

```
1 add dns txtrec exampledomain.com "Contact: Evan" "Email: evan@example.
     com" "Contact: Mark" "Email: mark1@example.com"
```



```
<!--NeedCopy-->
```

Entfernen Sie einen TXT-Ressourcendatensatz mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen TXT-Ressourceneintrag zu entfernen und die Konfiguration zu überprüfen:

```
-  rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>)
-  show dns txtRec [<domain> | -type <type>]
<!--NeedCopy-->
```

Beispiel:
Sie können den Befehl `show dns txtRec` zuerst verwenden, um die Datensatz-ID des TXT-Ressourceneintrags anzuzeigen, den Sie entfernen möchten, wie hier gezeigt:

```
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 36865       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Evan"
        "Email: evan@example.com"
2)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Mark"
        "Email: mark1@example.com"
 Done
<!--NeedCopy-->
```

Die einfachere Methode zum Löschen eines TXT-Datensatzes besteht darin, die Datensatz-ID zu verwenden. Wenn Sie die Zeichenketten bereitstellen möchten, geben Sie sie in der Reihenfolge ein, in der sie im Datensatz gespeichert sind. Im folgenden Beispiel wird der TXT-Datensatz mithilfe seiner Datensatz-ID gelöscht.

```
>rm dns txtRec www.example.com -recordID 36865
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        "Contact: Mark"
        "Email: mark1@example.com"
 Done
<!--NeedCopy-->
```


Konfigurieren Sie einen TXT-Datensatz mithilfe der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > TXT Records** und erstellen Sie einen TXT-Eintrag.

Erstellen von CAA-Datensätze für einen Domainnamen

May 11, 2023

Certificate Authority Authorization (CAA) ist eine Art von DNS-Eintrag, mit dem die Domaininhaber angeben können, welche Certificate Authority (CA) SSL-Zertifikate für die Domain ausstellen kann.

Eine sichere Verbindung zu einem Dienst erfordert SSL-/TLS-Zertifikate, um die Identität des Hosts sicherzustellen und einen sicheren Kanal einzurichten. Das Fehlen von CAA-Einträgen kann ein Sicherheitsrisiko verursachen, da jeder eine Certificate Signing Request (CSR) für die Domain generieren und das Zertifikat von einer beliebigen Zertifizierungsstelle signieren lassen kann.

CAA-Einträge bieten einen Layer Schutz für Ihre Webpräsenz, indem sie es dem Domaininhaber ermöglichen, zu deklarieren, welche Zertifizierungsstellen ein Zertifikat für die Domain ausstellen dürfen. Wenn von einer nicht autorisierten Zertifizierungsstelle ein Zertifikat angefordert wird, informiert der CAA-Eintrag den Domaininhaber darüber. Wenn für eine Domain kein CAA-Eintrag vorhanden ist, kann jede Zertifizierungsstelle das Zertifikat für diese Domäne ausstellen.

Die NetScaler-Appliance unterstützt DNS-CAA-Datensätze in den folgenden Modi:

- **Proxy**: Die Appliance speichert CAA-Datensatzantworten von Back-End-Servern im Cache und beantwortet weitere Abfragen desselben Typs aus dem Cache.
- **ADNS**: Die Appliance reagiert auf DNS-Abfragen des CAA-Datensatztyps von den konfigurierten DNS-Datensätzen.

Hinweis:

> - Sie können maximal 20 CAA-Datensätze pro Domainnamen hinzufügen.
> - Rekursive Resolver- und Forwarder-Modi werden nicht unterstützt.

Einen CAA-Record mit der CLI hinzufügen

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 add dns caaRec <domain> <issuer-string> -tag <tag-string> -flag [None|
     Critical] [-TTL <secs>]
2 <!--NeedCopy-->
```

Beispiel:


```
> add dns caaRec newdomain string1 -tag Issue -flag None [-TTL 3600]
<!--NeedCopy-->
```

Befehlsdetails anzeigen

```
> show dns caaRec

1)  Domain : newdomain  ECS Subnet : None      Record id: 39423 TTL : 3600 secs Record Type : ADNS

Value: string1

Tag: issue

Flag: NONE

2)  Domain : test.com  ECS Subnet : None      Record id: 2572   TTL : 5 secs    Record Type : ADNS

Value: ca1.test.com

Tag: issue

Flag: NONE
<!--NeedCopy-->
```

Geben Sie den folgenden Befehl an der Eingabeaufforderung ein, um einen CAA-Datensatz zu entfernen:

```
rm dns caaRec <domain> <issuer-string> -tag <tag-string> | -recordId <positive_integer>@)
<!--NeedCopy-->
```

Beispiel:

```
rm dns caaRec newdomain -recordId 39423
<!--NeedCopy-->
```

> **Hinweis:**
>
> -recordId @ wird in einem Cluster nicht unterstützt.

Einen CAA-Record mit der GUI hinzufügen

Navigieren Sie zu **Traffic Management > DNS > Records > CAA Records** und erstellen Sie einen Adressdatensatz.

DNS-Statistiken anzeigen

May 11, 2023

Sie können die von der NetScaler-Appliance generierten DNS-Statistiken einsehen. Die DNS-Statistiken umfassen Laufzeit-, Konfigurations- und Fehlerstatistiken.

Zeigen Sie die Statistiken der DNS-Einträge mithilfe der CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
stat dns
```

Beispiel:

```
> stat dns
DNS Statistics

Runtime Statistics
Dns queries                             21
NS queries                               8
SOA queries                             18
.
.
.
Configuration Statistics
AAAA records                            17
A records                               36
MX records                               9
.
.
.
Error Statistics
Nonexistent domain                      17
No AAAA records                          0
No A records                            13
.
.
.
```



```
25 Done
26 <!--NeedCopy-->
```

Zeigen Sie die Statistiken der DNS-Einträge mithilfe der GUI an

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf **Statistiken**.

Konfigurieren einer DNS-Zone

May 11, 2023

Eine DNS-Zoneneinheit auf der NetScaler-Appliance erleichtert den Besitz einer Domain auf der Appliance. Eine Zone auf der Appliance ermöglicht es Ihnen auch, DNS-Sicherheitserweiterungen (DNSSEC) für die Zone zu implementieren oder die DNSSEC-Operationen der Zone von den DNS-Servern auf die Appliance auszulagern. DNSSEC-Zeichenoperationen werden für alle Ressourceneinträge in einer DNS-Zone ausgeführt. Wenn Sie also eine Zone signieren oder DNSSEC-Operationen für eine Zone auslagern möchten, müssen Sie die Zone zunächst auf der NetScaler-Appliance erstellen.

Erstellen Sie in den folgenden Szenarien eine DNS-Zone auf der Appliance:

- Die NetScaler-Appliance besitzt alle Datensätze in einer Zone, das heißt, die Appliance fungiert als autorisierender DNS-Server für die Zone. Die Zone muss erstellt werden, wobei der ProxyMode-Parameter auf NO gesetzt ist.
- Die NetScaler-Appliance besitzt nur eine Teilmenge der Datensätze in einer Zone. Alle anderen Ressourceneinträge in der Zone werden auf einer Reihe von Back-End-Nameservern gehostet. Die Appliance ist als DNS-Proxyserver für diese Backend-Server konfiguriert. Eine typische Konfiguration, bei der die NetScaler-Appliance nur eine Teilmenge der Ressourceneinträge in der Zone besitzt, ist eine GSLB-Konfiguration (Global Server Load Balancing). Die NetScaler-Appliance besitzt nur die GSLB-Domainnamen, während die Back-End-Nameserver alle anderen Datensätze besitzen. Die Zone muss erstellt werden, wobei der ProxyMode-Parameter auf YES gesetzt ist.
- Sie möchten DNSSEC-Operationen für eine Zone von Ihren autorisierenden DNS-Servern auf die Appliance auslagern. Die Zone muss erstellt werden, wobei der ProxyMode-Parameter auf YES gesetzt ist. Möglicherweise müssen Sie weitere Einstellungen für die Zone konfigurieren.

Im aktuellen Thema wird beschrieben, wie eine Zone für die ersten beiden Szenarien erstellt wird. Weitere Informationen zum Konfigurieren einer Zone zum Auslagern von DNSSEC-Vorgängen auf die Appliance finden Sie unter Auslagern von DNSSEC-Vorgängen auf die NetScaler Appliance.

> **Hinweis**
>
> Wenn die ADC-Appliance als autorisierender DNS-Server für eine Zone fungiert, müssen Sie die SOA-Einträge (Start of Authority) und Nameserver-Einträge (NS) für die Zone erstellen, bevor Sie die Zone erstellen. Wenn NetScaler als DNS-Proxyserver für eine Zone arbeitet, dürfen SOA- und NS-Einträge auf der NetScaler Appliance nicht erstellt werden. Weitere Informationen zum Erstellen von SOA- und NS-Datensätzen finden Sie unter Konfigurieren von DNS-Ressourceneinträgen.

Wenn Sie eine Zone erstellen, werden alle vorhandenen Domänennamen und Ressourceneinträge, die mit dem Namen der Zone enden, automatisch als Teil der Zone behandelt. Außerdem werden alle neuen Ressourceneinträge, die mit einem Suffix erstellt wurden, das dem Namen der Zone entspricht, implizit in der Zone enthalten.

Erstellen Sie mithilfe der CLI eine DNS-Zone auf der NetScaler-Appliance

Geben Sie an der Befehlszeile den folgenden Befehl ein, um der NetScaler-Appliance eine DNS-Zone hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add dns zone <zoneName> -proxyMode ( YES | NO )
2 -  show dns zone [<zoneName> | -type <type>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns zone example.com -proxyMode Yes
2  Done
3 > show dns zone example.com
4          Zone Name : example.com
5          Proxy Mode : YES
6 Done
7 <!--NeedCopy-->
```

Ändern oder entfernen Sie eine DNS-Zone mithilfe der CLI

- Um eine DNS-Zone zu ändern, geben Sie den `set dns zone` Befehl, den Namen der DNS-Zone und die zu ändernden Parameter mit ihren neuen Werten ein.
- Um eine DNS-Zone zu entfernen, geben Sie den `rm dns zone` Befehl und den Namen der DNS-Zone ein.

Konfigurieren Sie eine DNS-Zone mithilfe der GUI

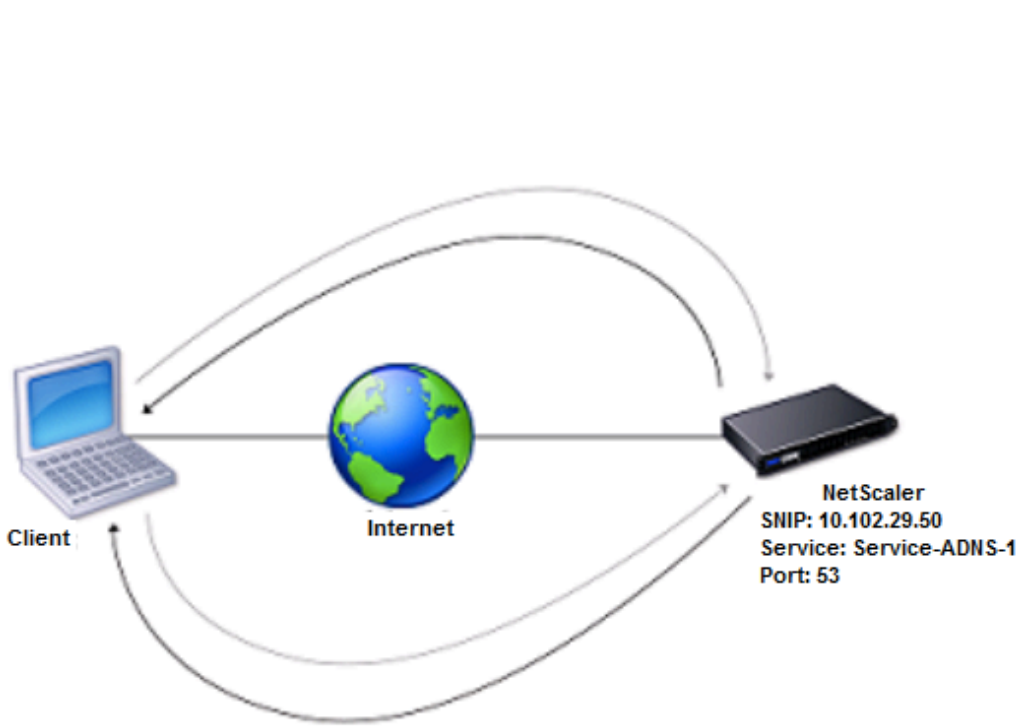
Navigieren Sie zu **Traffic Management > DNS > Zonen** und erstellen Sie eine DNS-Zone.

Konfigurieren von NetScaler als ADNS-Server

May 11, 2023

Sie können die ADC-Appliance so konfigurieren, dass sie als autorisierender Domainnamenserver (ADNS) für eine Domain fungiert. Als ADNS-Server für eine Domain löst der NetScaler DNS-Anfragen für alle Arten von DNS-Einträgen auf, die zur Domäne gehören. Um den NetScaler so zu konfigurieren, dass er als ADNS-Server für eine Domäne fungiert, müssen Sie einen ADNS-Dienst erstellen und NS- und Adressdatensätze für die Domäne auf dem NetScaler konfigurieren. Der ADNS-Dienst kann mithilfe der Subnetz-IP-Adresse (SNIP) oder einer separaten IP-Adresse konfiguriert werden. Das folgende Topologiediagramm zeigt eine Beispielkonfiguration und den Ablauf von Anfragen und Antworten.

Abbildung 1. NetScaler als ADNS



Die folgende Tabelle zeigt die Parameter, die für den ADNS-Dienst konfiguriert sind, der im vorherigen Topologiediagramm dargestellt ist.

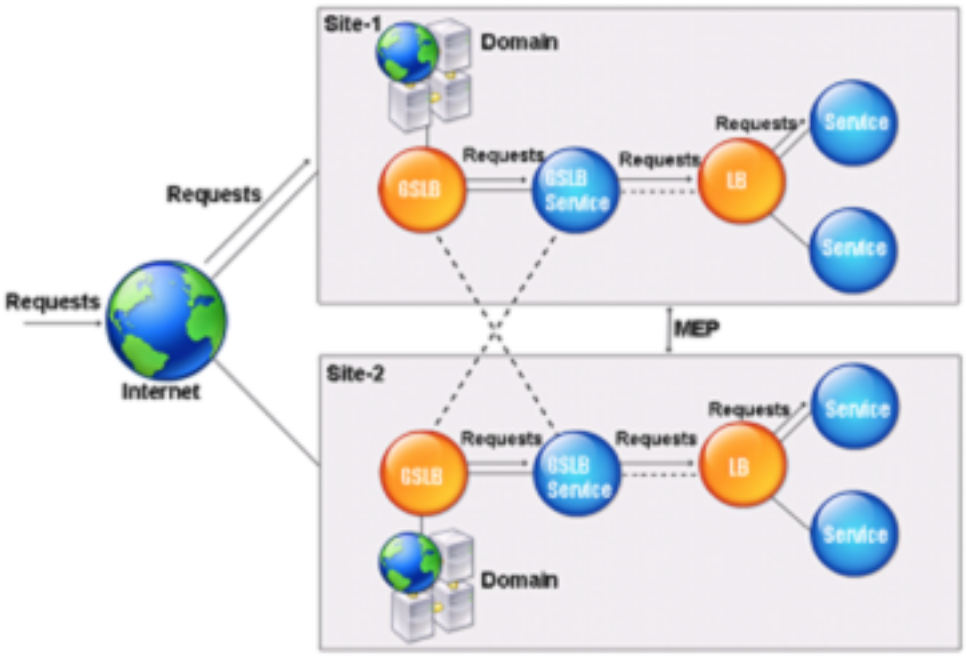
Entitätstyp	Name	IP-Adresse	Typ	Port
ADNS-Dienst	Service-ADNS-1	10.102.29.51	ADNS	53

Tabelle 1. Beispiel für eine ADNS-Dienstkonfiguration

Um ein ADNS-Setup zu konfigurieren, müssen Sie den ADNS-Dienst konfigurieren. Anweisungen zum Konfigurieren des ADNS-Dienstes finden Sie unter Lastenausgleich.

Während der DNS-Auflösung leitet der ADNS-Server den DNS-Proxy oder lokalen DNS-Server an, den NetScaler nach der IP-Adresse der Domäne abzufragen. Da der NetScaler für die Domain autorisierend ist, sendet er die IP-Adresse an den DNS-Proxy oder den lokalen DNS-Server. Das folgende Diagramm beschreibt die Platzierung und Rolle des ADNS-Servers in einer GSLB-Konfiguration.

Abbildung 2. GSLB-Entitätsmodell



Hinweis: Wenn Sie im ADNS-Modus SOA- und ADNS-Datensätze entfernen, funktioniert Folgendes nicht für die Domäne, die von der NetScaler: ANY-Abfrage gehostet wird (weitere Informationen zur ANY-Abfrage finden Sie unter DNS ANY-Abfrage) und negative Antworten wie NODATA und NXDOMAIN.

Erstellen eines ADNS-Dienstes

Ein ADNS-Dienst wird für den globalen Lastausgleich von Diensten verwendet. Weitere Informationen zum Erstellen eines GSLB-Setups finden Sie unter Globaler Server-Lastenausgleich. Sie können einen ADNS-Dienst hinzufügen, ändern, aktivieren, deaktivieren und entfernen. Anweisungen zum Erstellen eines ADNS-Dienstes finden Sie unter Konfigurieren von Diensten.

Hinweis: Sie können den ADNS-Dienst so konfigurieren, dass er SNIP oder eine neue IP-Adresse verwendet.

Wenn Sie einen ADNS-Dienst erstellen, reagiert NetScaler auf DNS-Abfragen an der konfigurierten ADNS-Dienst-IP und dem Port.

Sie können die Konfiguration überprüfen, indem Sie sich die Eigenschaften des ADNS-Dienstes ansehen. Sie können Eigenschaften wie Name, Status, IP-Adresse, Port, Protokoll und maximale Client-Verbindungen anzeigen.

Konfigurieren Sie das ADNS-Setup für die Verwendung von TCP

Standardmäßig verwenden einige Clients das User Datagram Protocol (UDP) für DNS, das ein Limit von 512 Byte für die Nutzlastlänge von UDP-Paketen festlegt. Um Payloads mit einer Größe von mehr als 512 Byte zu verarbeiten, muss der Client TCP verwenden. Um die DNS-Kommunikation über TCP zu aktivieren, müssen Sie die NetScaler-Appliance so konfigurieren, dass sie das TCP-Protokoll für DNS verwendet. Der NetScaler legt dann das Kürzungsbit in den DNS-Antwortpaketen fest. Das Kürzungsbit gibt an, dass die Antwort für UDP zu groß ist und dass der Client die Anfrage über eine TCP-Verbindung senden muss. Der Client verwendet dann das TCP-Protokoll auf Port 53 und öffnet eine neue Verbindung zum NetScaler. Der NetScaler überwacht Port 53 mit der IP-Adresse des ADNS-Dienstes, um die neuen TCP-Verbindungen vom Client zu akzeptieren.

Um NetScaler für die Verwendung des TCP-Protokolls zu konfigurieren, müssen Sie einen ADNS_TCP-Dienst konfigurieren. Anweisungen zum Erstellen eines ADNS_TCP-Dienstes finden Sie unter Lastenausgleich.

> **Wichtig**
>
> Um den NetScaler so zu konfigurieren, dass er UDP für DNS verwendet und TCP nur verwendet, wenn die Nutzlastlänge von UDP 512 Byte überschreitet, müssen Sie die ADNS- und ADNS_TCP-Dienste konfigurieren. Die IP-Adresse des ADNS_TCP-Dienstes muss mit der IP-Adresse des ADNS-Dienstes übereinstimmen.

DNS-Ressourceneinträge hinzufügen

Nachdem Sie einen ADNS-Dienst erstellt haben, können Sie DNS-Einträge hinzufügen. Anweisungen zum Hinzufügen von DNS-Datensätzen finden Sie unter Konfigurieren von DNS-Ressourceneinträgen.

ADNS-Dienste entfernen

Anweisungen zum Entfernen von Diensten finden Sie unter Lastenausgleich

Konfigurieren der Domänendelegierung

Bei der Domänendelegierung wird die Verantwortung für einen Teil des Domainbereichs einem anderen Nameserver zugewiesen. Daher wird bei der Domänendelegierung die Verantwortung für die Beantwortung der Anfrage an einen anderen DNS-Server delegiert. Die Delegierung verwendet NS-Datensätze.

Im folgenden Beispiel ist sub1.abc.com die Subdomain für abc.com. Das Verfahren beschreibt die Schritte zum Delegieren der Subdomain an den Nameserver ns2.sub1.abc.com und zum Hinzufügen eines Adressdatensatzes für ns2.sub1.abc.com.

Um die Domänendelegierung zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen, die in den folgenden Abschnitten beschrieben werden:

1. Erstellen Sie einen SOA-Eintrag für eine Domain.
2. Erstellen Sie einen NS-Eintrag, um einen Nameserver für die Domain hinzuzufügen.
3. Erstellen Sie einen Adressdatensatz für den Nameserver.
4. Erstellen Sie einen NS-Eintrag, um die Subdomain zu delegieren.
5. Erstellen Sie einen Glue-Datensatz für den Nameserver.

Erstellen eines SOA-Datensatzes

Anweisungen zum Konfigurieren von SOA-Datensätzen finden Sie unter Erstellen von SOA-Datensätzen für autoritative Informationen.

Erstellen eines NS-Datensatzes für einen Nameserver

Anweisungen zum Konfigurieren eines NS-Datensatzes finden Sie unter Erstellen von NS-Datensätzen für einen autoritativen Server. Wählen Sie in der Liste **Namensserver** den primären autoritativen Nameserver aus, z. B. ns1.abc.com.

Erstellen eines Adressdatensatzes

Anweisungen zum Konfigurieren von Adressdatensätzen finden Sie unter Erstellen von Adressdatensätzen für einen Domainnamen. Geben Sie in die Textfelder Hostname und IP-Adresse den Domänennamen für den DNS-Adressdatensatz und die IP-Adresse ein, z. B. ns1.abc.com bzw. 10.102.11.135.

Erstellen eines NS-Datensatzes für die Domänendelegierung

Anweisungen zum Konfigurieren von NS-Datensätzen finden Sie unter Erstellen von NS-Datensätzen für einen autoritativen Server. Wählen Sie in der Liste **Name Server** den primären autoritativen Nameserver aus, z. B. ns2.sub1.abc.com.

Erstellen Sie einen Glue-Datensatz

NS-Datensätze werden in der Regel unmittelbar nach dem SOA-Eintrag definiert (keine Einschränkung). Eine Domain muss mindestens zwei NS-Einträge haben. Wenn ein NS-Datensatz innerhalb einer Domain definiert ist, muss er einen passenden Adressdatensatz haben. Dieser Adressdatensatz wird als Glue-Datensatz bezeichnet. Glue-Datensätze beschleunigen DNS-Abfragen.

Anweisungen zum Hinzufügen von Glue-Datensätzen für eine Subdomain finden Sie im Verfahren zum Hinzufügen eines Address (A) -Datensatzes unter Konfigurieren von DNS-Ressourceneinträgen.

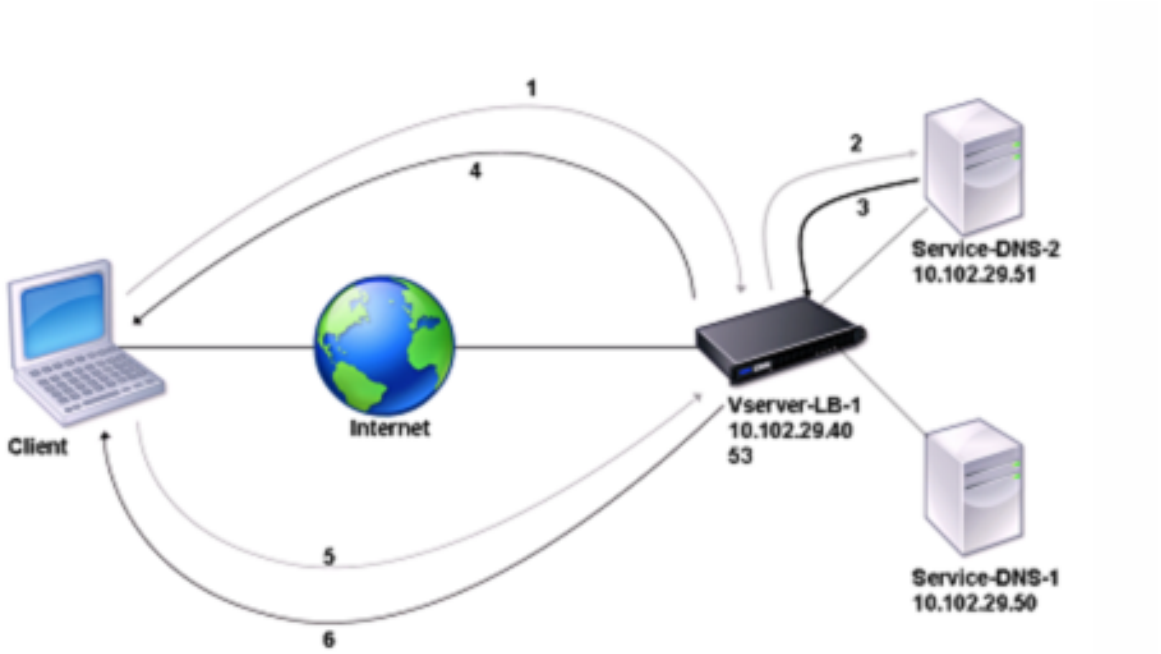
Anweisungen zum Konfigurieren von Adressdatensätzen finden Sie unter Erstellen von Adressdatensätzen für einen Domainnamen. Geben Sie in die Textfelder Hostname und IP-Adresse den Domänennamen für den DNS-Adressdatensatz und die IP-Adresse ein, z. B. ns2.sub1.abc.com bzw. 10.102.12.135.

Konfigurieren Sie die NetScaler-Appliance als DNS-Proxyserver

May 11, 2023

Als DNS-Proxyserver kann die ADC-Appliance als Proxy für einen einzelnen DNS-Server oder eine Gruppe von DNS-Servern fungieren. Der Fluss von Anfragen und Antworten wird im folgenden Topologiediagramm veranschaulicht.

Abbildung 1. NetScaler als DNS-Proxy



Standardmäßig speichert die NetScaler-Appliance Antworten von DNS-Nameservern im Cache. Wenn die Appliance eine DNS-Anfrage empfängt, sucht sie in ihrem Cache nach der abgefragten Domain. Wenn die Adresse der abgefragten Domäne in ihrem Cache vorhanden ist, gibt der NetScaler die entsprechende Adresse an den Client zurück. Andernfalls leitet es die Anfrage an einen DNS-Nameserver weiter, der die Verfügbarkeit der Adresse überprüft und sie an den NetScaler zurückgibt. Der NetScaler gibt die Adresse dann an den Client zurück.

Bei Anfragen für eine Domain, die zuvor zwischengespeichert wurde, stellt der NetScaler den Adressdatensatz der Domäne aus dem Cache bereit, ohne den konfigurierten DNS-Server abzufragen.

Die Appliance verwirft einen in ihrem Cache gespeicherten Datensatz, wenn der Time-to-Live (TTL)-Wert des Datensatzes den konfigurierten Wert erreicht. Ein Client, der einen abgelaufenen Datensatz anfordert, muss warten, bis der NetScaler den Datensatz vom Server abruft und seinen Cache aktualisiert. Um diese Verzögerung zu vermeiden, aktualisiert der NetScaler den Cache proaktiv, indem er den Datensatz vom Server abruft, bevor der Datensatz abläuft.

In der folgenden Tabelle sind Beispielnamen und die Werte der Entitäten aufgeführt, die auf dem NetScaler konfiguriert werden müssen.

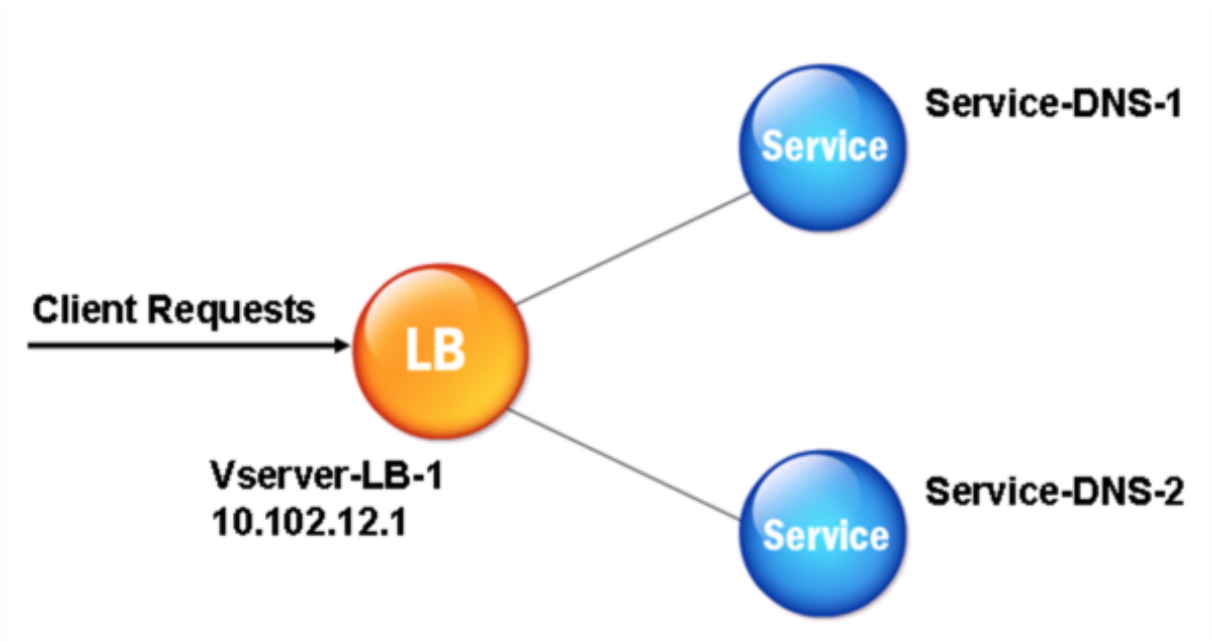
Tabelle 1. Beispiel für die Konfiguration einer DNS-Proxy-Entität

Entitätstyp	Name	IP-Adresse	Typ	Port
Virtueller LB-Server	Vserver-DNS-1	10.102.29.40	DNS	53
Services	Service-DNS-1	10.102.29.50	DNS	53

Entitätstyp	Name	IP-Adresse	Typ	Port
Services	Service-DNS-2	10.102.29.51	DNS	53

Das folgende Diagramm zeigt die Entitäten eines DNS-Proxys und die Werte der Parameter, die auf dem NetScaler konfiguriert werden sollen.

Abbildung 2. DNS-Proxy-Entity



> **Hinweis**
>
> Um die DNS-Proxyfunktion zu konfigurieren, müssen Sie wissen, wie Load Balancing-Dienste und virtuelle Server konfiguriert werden.

Erstellen eines virtuellen Lastausgleichsservers

Um einen DNS-Proxy auf dem NetScaler zu konfigurieren, konfigurieren Sie einen virtuellen Lastausgleichsserver vom Typ DNS. Um einen virtuellen DNS-Server für den Lastenausgleich einer Reihe von DNS-Servern zu konfigurieren, die rekursive Abfragen unterstützen, müssen Sie die Option Rekursion verfügbar aktivieren. Mit dieser Option wird das RA-Bit in den DNS-Antworten vom virtuellen DNS-Server auf ON gesetzt.

Anweisungen zum Erstellen eines virtuellen Lastenausgleichsservers finden Sie unter Load Balancing.

Erstellen von DNS-Diensten

Nachdem Sie einen virtuellen Lastausgleichsserver vom Typ DNS erstellt haben, müssen Sie DNS-Dienste erstellen. Sie können einen DNS-Dienst hinzufügen, ändern, aktivieren, deaktivieren und entfernen. Anweisungen zum Erstellen eines DNS-Dienstes finden Sie unter Load Balancing.

Binden eines virtuellen Lastausgleichsservers an DNS-Dienste

Um die DNS-Proxykonfiguration abzuschließen, müssen Sie die DNS-Dienste an den virtuellen Lastausgleichsserver binden. Anweisungen zum Binden eines Dienstes an einen virtuellen Lastausgleichsserver finden Sie unter Load Balancing.

Konfigurieren des DNS-Proxy-Setups für die Verwendung von TCP

Einige Clients verwenden das User Datagram Protocol (UDP) für die DNS-Kommunikation. UDP gibt jedoch eine maximale Paketgröße von 512 Byte an. Wenn die Payload-Länge 512 Byte überschreitet, muss der Client TCP verwenden. Wenn ein Client der NetScaler-Appliance eine DNS-Anfrage sendet, leitet die Appliance die Anfrage an einen der Nameserver weiter. Wenn die Antwort für ein UDP-Paket zu groß ist, setzt der Nameserver das Kürzungsbit in seiner Antwort an den NetScaler. Das Kürzungsbit gibt an, dass die Antwort für UDP zu groß ist und dass der Client die Anfrage über eine TCP-Verbindung senden muss. Die ADC-Appliance leitet die Antwort an den Client weiter, wobei das Kürzungsbit intakt ist. Es wartet darauf, dass der Client eine TCP-Verbindung mit der IP-Adresse des virtuellen DNS-Load-Balancing-Servers auf Port 53 initiiert. Der Client sendet die Anfrage über eine TCP-Verbindung. Die NetScaler-Appliance leitet die Anfrage dann an den Nameserver weiter und leitet die Antwort an den Client weiter.

Um den NetScaler so zu konfigurieren, dass er das TCP-Protokoll für DNS verwendet, müssen Sie einen virtuellen Lastausgleichsserver und Dienste konfigurieren, beide vom Typ DNS_TCP. Sie können Monitore vom Typ DNS_TCP konfigurieren, um den Status der Dienste zu überprüfen. Anweisungen zum Erstellen virtueller Server, Dienste und Monitore von DNS_TCP finden Sie unter Load Balancing.

Um die Datensätze proaktiv zu aktualisieren, verwendet NetScaler eine TCP-Verbindung zum Server, um die Datensätze abzurufen.

> **Wichtig**
>
> Um den NetScaler so zu konfigurieren, dass er UDP für DNS verwendet und TCP nur verwendet, wenn die Nutzlastlänge von UDP 512 Byte überschreitet, müssen Sie sowohl die DNS- als auch die DNS_TCP-Dienste konfigurieren. Die IP-Adresse des DNS_TCP-Dienstes muss mit der IP-Adresse des DNS-Dienstes übereinstimmen.

Time-to-Live-Werte für DNS-Einträge konfigurieren

Die TTL ist für alle DNS-Einträge mit demselben Domainnamen und Datensatztyp gleich. Wenn der TTL-Wert für einen der Datensätze geändert wird, spiegelt sich der neue Wert in allen Datensätzen desselben Domainnamens und -typs wider. Der Standard-TTL-Wert ist 3600 Sekunden. Das Minimum ist 0 und das Maximum ist 604800. Wenn ein DNS-Eintrag einen TTL-Wert hat, der kleiner als das Minimum oder größer als das Maximum ist, wird er als minimaler bzw. maximaler TTL-Wert gespeichert.

Minimale und maximale TTL mithilfe der CLI angeben

Geben Sie an der NetScaler-Befehlszeile die folgenden Befehle ein, um die minimale und maximale TTL anzugeben und die Konfiguration zu überprüfen:

```
-  set dns parameter [-minTTL <secs>] [-maxTTL <secs>]
-  show dns parameter
<!--NeedCopy-->
```

Beispiel:

```
> set dns parameter -minTTL 1200 -maxTTL 1800
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        Minimum TTL: 1200               Maximum TTL: 1800
            .
            .
            .
 Done
>
<!--NeedCopy-->
```

Minimale und maximale TTL mithilfe der GUI angeben

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter Einstellungen auf DNS-Einstellungen ändern.
3. Geben Sie im Dialogfeld DNS-Parameter konfigurieren unter TTL in den Textfeldern Minimum und Maximum die minimale bzw. maximale Lebensdauer (in Sekunden) ein, und klicken Sie dann auf OK.

Hinweis: Wenn die TTL abläuft, wird der Datensatz aus dem Cache gelöscht. Der NetScaler kontaktiert proaktiv die Server und ruft den DNS-Eintrag ab, kurz bevor der DNS-Eintrag abläuft.

DNS-Einträge leeren

Sie können alle im Cache vorhandenen DNS-Einträge löschen. Beispielsweise möchten Sie möglicherweise DNS-Einträge löschen, wenn ein Server nach Änderungen neu gestartet wird.

Alle Proxy-Datensätze mithilfe der CLI löschen

Geben Sie an der NetScaler Eingabeaufforderung Folgendes ein:

```
flush dns proxyRecords
```

Alle Proxy-Datensätze mithilfe der GUI löschen

1. Navigieren Sie zu **Traffic Management > DNS > Records**.
2. Klicken Sie im Detailbereich auf Flush Proxy Records.

DNS-Ressourceneinträge hinzufügen

Sie können DNS-Einträge zu einer Domäne hinzufügen, für die die NetScaler Appliance als DNS-Proxyserver konfiguriert ist. Informationen zum Hinzufügen von DNS-Datensätzen finden Sie unter Konfigurieren von DNS-Ressourceneinträgen.

Entfernen eines virtuellen DNS-Servers für Lastenausgleich

Informationen zum Entfernen eines virtuellen Lastenausgleichsservers finden Sie unter Load Balancing.

Begrenzen der Anzahl gleichzeitiger DNS-Anforderungen für eine Clientverbindung

Sie können die Anzahl gleichzeitiger DNS-Anfragen auf einer einzelnen Clientverbindung begrenzen, die durch das `<clientip:port>-<vserver ip:port>` Tupel gekennzeichnet ist. Gleichzeitige DNS-Anfragen sind die Anfragen, die die NetScaler-Appliance an die Nameserver weitergeleitet hat und für die die Appliance auf Antworten wartet. Durch die Begrenzung der Anzahl gleichzeitiger Anfragen auf einer Clientverbindung können Sie die Nameserver schützen, wenn ein feindlicher Client versucht, einen Distributed-Denial-of-Service (DDoS) -Angriff zu starten, indem er eine Flut von DNS-Anfragen sendet. Wenn das Limit für eine Clientverbindung erreicht ist, werden nachfolgende DNS-Anfragen für die Verbindung verworfen, bis die Anzahl der ausstehenden Anfragen das Limit unterschreitet. Dieses Limit gilt nicht für die Anfragen, die die NetScaler-Appliance aus ihrem Cache verarbeitet.

Der Standardwert für diesen Parameter ist 255. Dieser Standardwert ist in den meisten Szenarien ausreichend. Wenn die Nameserver unter normalen Betriebsbedingungen viele gleichzeitige DNS-Anfragen bearbeiten, können Sie entweder einen großen Wert oder einen Wert von Null (0) angeben. Ein Wert von 0 deaktiviert diese Funktion und gibt an, dass die Anzahl der DNS-Anfragen, die für eine einzelne Clientverbindung zulässig sind, unbegrenzt ist. Dieser Parameter ist ein globaler Parameter und gilt für alle virtuellen DNS-Server, die auf der NetScaler-Appliance konfiguriert sind.
Der Standardwert für diesen Parameter ist 255. Dieser Standardwert ist in den meisten Szenarien ausreichend. Wenn die Nameserver unter normalen Betriebsbedingungen viele gleichzeitige DNS-Anfragen bearbeiten, können Sie entweder einen großen Wert oder einen Wert von Null (0) angeben. Ein Wert von 0 deaktiviert diese Funktion und gibt an, dass die Anzahl der DNS-Anfragen, die für eine einzelne Clientverbindung zulässig sind, unbegrenzt ist. Dieser Parameter ist ein globaler Parameter und gilt für alle virtuellen DNS-Server, die auf der NetScaler-Appliance konfiguriert sind.
Der Standardwert für diesen Parameter ist 255. Dieser Standardwert ist in den meisten Szenarien ausreichend. Wenn die Nameserver unter normalen Betriebsbedingungen viele gleichzeitige DNS-Anfragen bearbeiten, können Sie entweder einen großen Wert oder einen Wert von Null (0) angeben. Ein Wert von 0 deaktiviert diese Funktion und gibt an, dass die Anzahl der DNS-Anfragen, die für eine einzelne Clientverbindung zulässig sind, unbegrenzt ist. Dieser Parameter ist ein globaler Parameter und gilt für alle virtuellen DNS-Server, die auf der NetScaler-Appliance konfiguriert sind.

Geben Sie die maximale Anzahl gleichzeitiger DNS-Anforderungen an, die für eine einzelne Clientverbindung zulässig sind, mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die maximale Anzahl gleichzeitiger DNS-Anfragen anzugeben, die für eine einzelne Clientverbindung zulässig sind, und überprüfen Sie die Konfiguration:

```
-  set dns parameter -maxPipeline <positive_integer>
-  show dns parameter
<!--NeedCopy-->
```

Beispiel:

```
> set dns parameter -maxPipeline 1000
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        .
        .
        .
        Max DNS Pipeline Requests: 1000
 Done
```



```
<!--NeedCopy-->
```

Geben Sie mithilfe der GUI die maximale Anzahl gleichzeitiger DNS-Anfragen an, die für eine einzelne Client-Verbindung zulässig sind

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf DNS-Einstellungen ändern.
3. Geben Sie im Dialogfeld DNS-Parameter konfigurieren einen Wert für Max. DNS-Pipelineanfragen an.
4. Klicken Sie auf OK.

Konfigurieren von NetScaler als End-Resolver

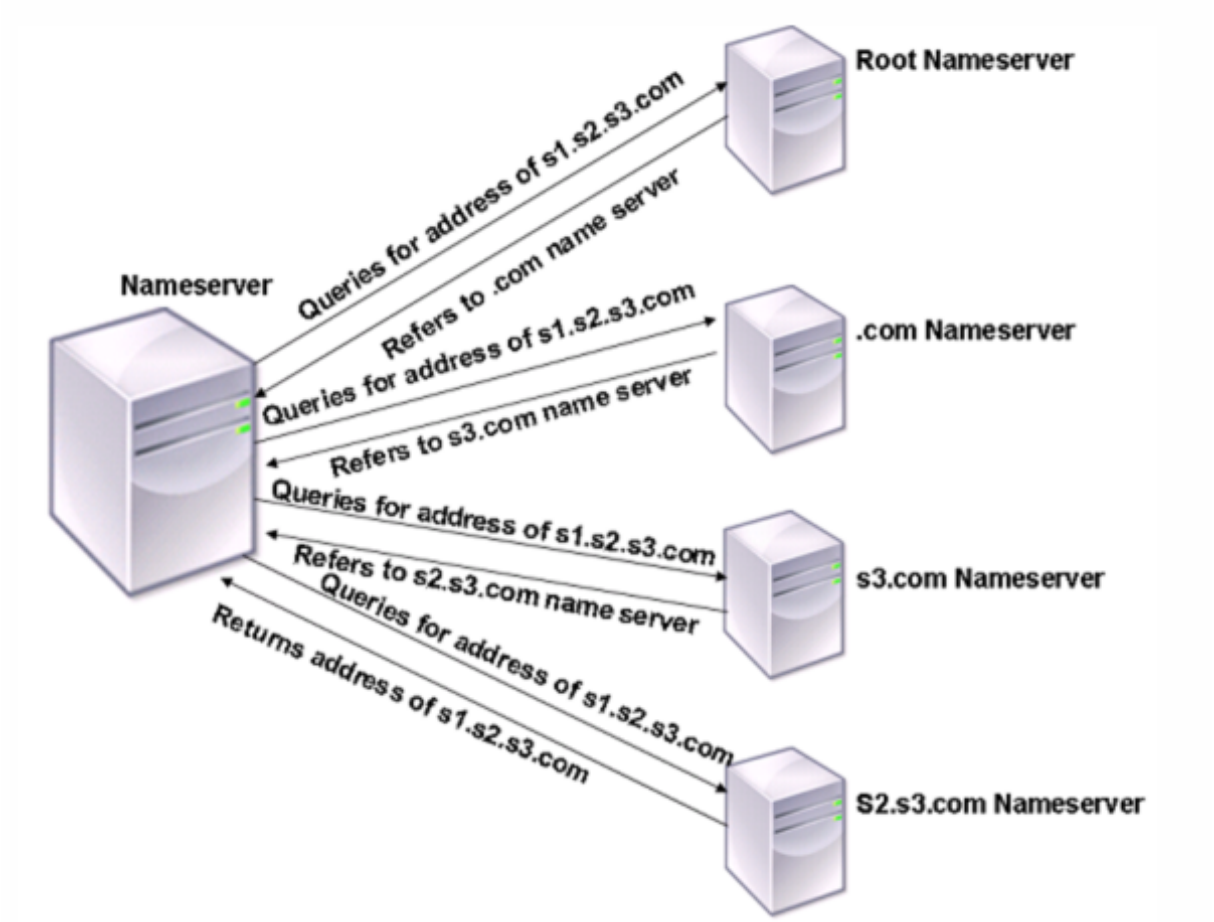
May 11, 2023

Ein Resolver ist eine Prozedur, die von einem Anwendungsprogramm aufgerufen wird, das einen Domänen-/Hostnamen in seinen Ressourceneintrag übersetzt. Der Resolver interagiert mit dem LDNS, das den Domainnamen sucht, um seine IP-Adresse zu erhalten. Der NetScaler kann eine End-to-End-Auflösung für DNS-Abfragen bereitstellen.

Bei rekursiver Auflösung fragt die NetScaler-Appliance verschiedene Nameserver rekursiv ab, um auf die IP-Adresse einer Domäne zuzugreifen. Wenn der NetScaler eine DNS-Anforderung empfängt, überprüft er seinen Cache auf den DNS-Eintrag. Wenn der Datensatz nicht im Cache vorhanden ist, fragt er die in der Datei ns.conf konfigurierten Root-Server ab. Der Stammnamenserver meldet sich mit der Adresse eines DNS-Servers, der detaillierte Informationen über die Domäne der zweiten Ebene enthält. Der Vorgang wird wiederholt, bis der erforderliche Datensatz gefunden wurde.

Wenn Sie die NetScaler-Appliance zum ersten Mal starten, werden 13 Root-Namenserver zur Datei ns.conf hinzugefügt. Die NS- und Adressdatensätze für die 13 Root-Server werden ebenfalls hinzugefügt. Sie können die Datei ns.conf ändern, aber der NetScaler erlaubt es Ihnen nicht, alle 13 Datensätze zu löschen. Es ist mindestens ein Namenservereintrag erforderlich, damit die Appliance die Namensauflösung durchführen kann. Das folgende Diagramm veranschaulicht den Prozess der Namensauflösung.

Abbildung 1. Rekursive Auflösung



Wenn der Namenserver in dem im Diagramm gezeigten Prozess eine Abfrage nach der Adresse von s1.s2.s3.com empfängt, überprüft er zuerst die Root-Nameserver auf s1.s2.s3.com. Ein Root-Namenserver meldet sich mit der Adresse des .com-Nameservers zurück. Wenn die Adresse von s1.s2.s3.com im Namenserver gefunden wird, antwortet er mit einer geeigneten IP-Adresse. Andernfalls fragt es andere Nameserver nach s3.com und dann nach s2.s3.com ab, um die Adresse von s1.s2.s3.com abzurufen. Auf diese Weise beginnt die Auflösung immer bei den Root-Nameservern und endet mit dem autorisierenden Nameserver der Domain.

> Hinweis
>
> Für rekursive Auflösungsfunktionen muss das Caching aktiviert sein.

Rekursive Auflösung aktivieren

Um die NetScaler-Appliance als Endresolver zu konfigurieren, müssen Sie die rekursive Auflösung auf der Appliance aktivieren. Sie müssen auch einen DNS-Namenserver mit der lokalen Option hinzufügen, damit das Feature funktioniert.

Rekursive Auflösung über die CLI aktivieren

Geben Sie an der Eingabeaufforderung folgende Befehle ein, um die rekursive Auflösung zu aktivieren und die Konfiguration zu überprüfen:

```
-  set dns parameter -recursion ENABLED
-  show dns parameter
<!--NeedCopy-->
```

Beispiel:

```
> set dns parameter -recursion ENABLED
 Done
> show dns parameter
        DNS parameters:
            .
            .
            .
        Recursive Resolution : ENABLED
            .
            .
            .
 Done
<!--NeedCopy-->
```

Rekursive Auflösung über die GUI aktivieren

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter Einstellungen auf DNS-Einstellungen ändern.
3. Aktivieren Sie im Dialogfeld DNS-Parameter konfigurieren das Kontrollkästchen Rekursion aktivieren, und klicken Sie dann auf OK.

Namenserver über die CLI hinzufügen (wenn die NetScaler-Appliance als Resolver fungiert)

Geben Sie in der Befehlszeile Folgendes ein:

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
<!--NeedCopy-->
```

Beispiel:

```
add dns nameServer 10.102.9.19 -local
show dns nameServer
1)  10.102.9.19 LOCAL -  State: UP  Protocol: UDP
```



```
4 Done
5 <!--NeedCopy-->
```

Lokal — Markieren Sie die IP-Adresse als eine, die zu einem lokalen rekursiven DNS-Server auf der NetScaler-Appliance gehört. Die Appliance löst rekursiv Abfragen auf, die an einer IP-Adresse eingehen, die als lokal markiert ist.
Damit die rekursive Auflösung funktioniert, muss auch der globale DNS-Parameter festgelegt werden.
`recursion`
Wenn kein Nameserver als lokal markiert ist, fungiert die Appliance als Stub-Resolver und gleicht die Nameserver aus.

Namenserver über die GUI hinzufügen

Navigieren Sie zu **Traffic Management** > **DNS** > **Nameserver**, und erstellen Sie einen Nameserver.

DNS Root Referral aktivieren

DNS Root Referral ist standardmäßig deaktiviert. Wenn aktiviert, antwortet die ADC-Appliance mit den Root Referral-Datensätzen.

Senden Sie ein Root Referral, wenn ein Client einen Domänennamen abfragt, der nicht mit den auf der NetScaler-Appliance konfigurierten/zwischengespeicherten Domänen zusammenhängt. Wenn die Einstellung deaktiviert ist, sendet die Appliance eine leere Antwort anstelle eines Root Referrals. Gilt für Domänen, für die die Appliance autorisierend ist. Deaktivieren Sie den Parameter, wenn die Appliance von einem Client angegriffen wird, der eine Flut von Abfragen für nicht verwandte Domänen sendet.

Root Referral über die CLI aktivieren

Geben Sie an der Eingabeaufforderung folgende Befehle ein, um die rekursive Auflösung zu aktivieren und die Konfiguration zu überprüfen:

```
1 -  set dns parameter -dnsrootReferral ENABLED
2 -  show dns parameter
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set dns parameter -recursion ENABLED
2  Done
3 > show dns parameter
4         DNS parameters:
```



```
5                .
6                .
7                .
8           DNS Root Referral : ENABLED
9                .
10               .
11               .
12  Done
13 <!--NeedCopy-->
```

Root Referral über die GUI aktivieren

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **DNS-Einstellungen ändern**.
3. Aktivieren Sie im Dialogfeld **DNS-Parameter konfigurieren** das Kontrollkästchen **Root Referral aktivieren**, und klicken Sie dann auf **OK**.

Anzahl der Wiederholungen festlegen

Konfigurieren Sie die ADC-Appliance so, dass sie eine vorkonfigurierte Anzahl von Versuchen (so genannte DNS-Wiederholungsversuche) ausführt, wenn sie keine Antwort von dem Server erhält, an den sie eine Abfrage sendet. Standardmäßig ist die Anzahl der DNS-Wiederholungen auf 5 festgelegt.

Legen Sie die Anzahl der DNS-Wiederholungsversuche über die CLI fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Anzahl der Wiederholungen festzulegen und die Konfiguration zu überprüfen:

```
1 -  set dns parameter -retries <positive_integer>
2 -  show dns parameter
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set DNS parameter -retries 3
2  Done
3 > show dns parameter
4         DNS parameters:
5         DNS retries: 3
6             .
7             .
8             .
```



```
 Done
<!--NeedCopy-->
```

Stellen Sie die Anzahl der Wiederholungen über die GUI ein

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter Einstellungen auf DNS-Einstellungen ändern.
3. Geben Sie im Dialogfeld DNS-Parameter konfigurieren im Textfeld DNS-Wiederholungen die Anzahl der DNS-Auflösungsanforderungen ein, und klicken Sie dann auf OK.

Konfigurieren Sie die NetScaler-Appliance als Forwarder

May 11, 2023

Ein Forwarder ist ein Server, der DNS-Anfragen an DNS-Server weiterleitet, die sich außerhalb des Netzwerks des Forwarder-Servers befinden. Abfragen, die lokal nicht gelöst werden können, werden an andere DNS-Server weitergeleitet. Ein Forwarder sammelt externe DNS-Informationen in seinem Cache, während er DNS-Abfragen auflöst. Um die NetScaler-Appliance als Forwarder zu konfigurieren, müssen Sie einen externen Nameserver hinzufügen.

Die NetScaler-Appliance ermöglicht es Ihnen, externe Nameserver hinzuzufügen, an die sie die Namensauflösungsanfragen weiterleiten kann, die lokal nicht gelöst werden können. Um die NetScaler-Appliance als Forwarder zu konfigurieren, müssen Sie die Nameserver hinzufügen, an die sie Abfragen zur Namensauflösung weiterleiten muss. Sie können die Suchpriorität angeben, um den Namensdienst anzugeben, den die NetScaler-Appliance für die Namensauflösung verwenden muss.

Informationen zur Konfiguration der NetScaler Appliance als Forwarder finden Sie unter Hinzufügen eines Namenservers (wenn die NetScaler Appliance als Forwarder fungiert) über die CLI.

> **Hinweis:**
>
> Die NetScaler-Appliance im Forwarder-Modus unterstützt TCP-, UDP- und UDP-TCP-Namenserver.
>
> - Wenn Sie einen TCP-Nameserver konfiguriert haben, sendet die NetScaler-Appliance die DNS-Anfrage über TCP.
> - Wenn Sie einen UDP-Namenserver konfiguriert haben, sendet die NetScaler Appliance die DNS-Anfrage über UDP.
> - Wenn Sie einen UDP-TCP-Nameserver konfiguriert haben, sendet die NetScaler-Appliance die DNS-Anfrage über UDP. Wenn jedoch das abgeschnittene Bit in der DNS-Antwort festgelegt ist, sendet die Appliance solche DNS-Anforderungen über TCP.

Hinzufügen eines Nameservers

Sie können einen Namenserver erstellen, indem Sie seine IP-Adresse angeben oder einen vorhandenen virtuellen Server als Namenserver konfigurieren.

- **IP-adressbasierter Namenserver** — Ein externer Namenserver, der für die Auflösung von Domänennamen kontaktiert werden muss Wenn mehrere IP-adressbasierte Nameserver auf der Appliance konfiguriert sind und der lokale Parameter auf keinem von ihnen festgelegt ist, werden eingehende DNS-Abfragen im Round-Robin-Modus auf alle Nameserver verteilt.
- **Virtueller serverbasierter Nameserver** — Ein virtueller DNS-Server, der im NetScaler konfiguriert ist. Führen Sie die folgenden Schritte aus, um eine genauere Kontrolle darüber zu erhalten, wie externe DNS-Namenserver den Lastenausgleich durchführen (z. B. wenn Sie eine andere Lastausgleichsmethode als Roundrobin verwenden möchten):
- Konfigurieren eines virtuellen DNS-Servers auf der Appliance
- Binden Sie die externen Nameserver als ihre Dienste
- Geben Sie in diesem Befehl den Namen des virtuellen Servers an.

Um die Konfiguration zu überprüfen, können Sie den Befehl `show dns nameServer` verwenden.

Um einen Nameserver zu entfernen, geben Sie in der NetScaler-CLI den `rm dns nameServer` Befehl gefolgt von der IP-Adresse des Nameservers ein.

Um die Details des DNS-Nameservers anzuzeigen, geben Sie in der NetScaler-CLI den `show dns nameServer` Befehl gefolgt von der IP-Adresse des Nameservers ein.

Fügen Sie über die CLI einen Namenserver hinzu (wenn die NetScaler-Appliance als Weiterleitung fungiert)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns nameServer ((<IP>) | <dnsVserverName>)
<!--NeedCopy-->
```

Oder

```
add dns nameServer ((<IP> | <dnsVserverName>) [-type <type>]
<!--NeedCopy-->
```

Beispiele:

```
add dns nameServer dnsVirtualNS

add dns nameServer 192.0.2.11 -type TCP

add dns nameServer 192.0.2.12 -type UDP_TCP
```



```
6
7
8  add dns nameServer 192.0.2.10
9  show dns nameServer 192.0.2.10
10
11 1) 192.0.2.10  -  State: UP  Protocol: UDP
12 Done
13 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn der Namenservertyp nicht angegeben ist, wird standardmäßig ein UDP-Namenserver erstellt. Um einen Namenserver vom Typ TCP oder UDP_TCP zu erstellen, müssen Sie den Typ angeben.
>
> Wenn Sie den Typ als UDP_TCP angeben, werden zwei Nameserver (ein UDP-Namenserver und ein TCP-Namenserver) für die angegebene IP-Adresse erstellt.

Namenserver über die CLI hinzufügen (wenn die NetScaler-Appliance als Resolver fungiert)

Geben Sie den Parameter `local` für einen rekursiven Resolver an. Aktivieren Sie die Rekursion mit dem Befehl `set dns parameter`.

Geben Sie in der Befehlszeile Folgendes ein:

```
1  add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
2  show dns nameServer
3  set dns parameter -recursion ENABLED
4  show dns parameter
5  <!--NeedCopy-->
```

Beispiel:

```
1  add dns nameServer 10.102.9.19 -local
2  show dns nameServer
3  1)  10.102.9.19 LOCAL -  State: UP  Protocol: UDP
4  Done
5  set dns parameter -recursion ENABLED
6  Done
7  show dns parameter
8          DNS parameters:
9              .
10             .
11             .
12         Recursive Resolution : ENABLED
```



```
13              .
14              .
15              .
16 Done
17 <!--NeedCopy-->
```

Lokal — Markieren Sie die IP-Adresse als eine, die zu einem lokalen rekursiven DNS-Server auf der NetScaler-Appliance gehört. Die Appliance löst rekursiv Abfragen auf, die an einer IP-Adresse eingehen, die als lokal markiert ist.
Damit die rekursive Auflösung funktioniert, muss auch der globale DNS-Parameter festgelegt werden.
`recursion`
Wenn kein Nameserver als lokal markiert ist, fungiert die Appliance als Stub-Resolver und gleicht die Nameserver aus.

Namenserver über die GUI hinzufügen

Navigieren Sie zu **Traffic Management** > **DNS** > **Nameserver**, und erstellen Sie einen Nameserver.

Festlegen der Priorität der DNS-Lookup

Sie können die Suchpriorität entweder auf DNS oder WINS festlegen. Diese Option wird im Betriebsmodus SSL VPN verwendet.

Setzen Sie die Suchpriorität über die CLI auf DNS

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Suchpriorität auf DNS festzulegen und die Konfiguration zu überprüfen:

```
1 -  set dns parameter -nameLookupPriority (DNS | WINS)
2 -  show dns parameter
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set dns parameter -nameLookupPriority DNS
2  Done
3 > show dns parameter
4              .
5              .
6              .
7         Name lookup priority : DNS
8              .
9              .
```



```
10                .
11  Done
12 <!--NeedCopy-->
```

Setzen Sie die Suchpriorität über die GUI auf DNS

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **DNS-Einstellungen ändern**.
3. Wählen **Sie im Dialogfeld DNS-Parameter konfigurieren** unter **Namen-Suchpriorität die**Option DNS oder WINS aus, und klicken Sie dann auf **OK**.

> **Hinweis**
>
> Wenn der virtuelle DNS-Server, den Sie konfiguriert haben, DOWN ist und Sie `-nameLookupPriority` auf DNS festlegen, versucht NetScaler nicht, die WINS-Suche zu starten. Wenn ein virtueller DNS-Server nicht konfiguriert oder deaktiviert ist, legen Sie den`-nameLookupPriority` auf WINS fest.

Deaktivieren und Aktivieren von Nameservern

Im folgenden Verfahren werden die Schritte zum Aktivieren oder Deaktivieren eines vorhandenen Namenservers beschrieben.

Aktivieren oder deaktivieren Sie einen Namenserver über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Namenserver zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
1 -  (enable | disable) dns nameServer <IPAddress>
2 -  show dns nameServer <IPAddress>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > disable dns nameServer 10.102.9.19
2  Done
3 > show dns nameServer 10.102.9.19
4 1)       10.102.9.19: LOCAL  -  State: OUT OF SERVICE
5  Done
6 <!--NeedCopy-->
```


Aktivieren oder deaktivieren Sie einen Namenserver über die GUI

1. Navigieren Sie zu **Traffic Management > DNS > Nameserver**.
2. Wählen Sie im Detailbereich den Namenserver aus, den Sie aktivieren oder deaktivieren möchten.
3. Klicken Sie auf **Aktivieren** oder **Deaktivieren**. Wenn ein Namenserver aktiviert ist, ist die Option **Deaktivieren** verfügbar. Wenn ein Namenserver deaktiviert ist, ist die Option **Aktivieren** verfügbar.

Konfigurieren von NetScaler als nicht-validierenden sicherheitsbewussten Stub-Resolver

May 11, 2023

Ab NetScaler 12.1 Build 49.xx fungiert NetScaler als nicht validierender, sicherheitsbewusster Stub-Resolver. Um diese Unterstützung zu aktivieren, wird das AD-Bit im DNS-Header gesetzt und das DO-Bit ist im OPT-Header deaktiviert. Wenn das AD-Bit gesetzt und das DO-Bit nicht gesetzt ist, validiert der Upstream-rekursive Resolver die DNSSEC-Antwort. Wenn die Validierung erfolgreich ist, reagiert der rekursive Resolver ohne DNSSEC-RRs. Wenn die DNSSEC-Validierung fehlschlägt, kehrt der rekursive Resolver mit einer SERVFAIL-Antwort zurück.

> **Wichtig:**
>
> Das AD-Bit ist standardmäßig im ADC-Forwarder gesetzt. Das AD-Bit ist nicht für DBS-initiierte Abfragen festgelegt.

Jumbo-Frames Unterstützung für DNS zur Handhabung von Reaktionen großer Größen

May 11, 2023

Ab NetScaler 12.1 Build 49.xx unterstützt DNS Jumbo-Frames für die Verarbeitung von UDP-Antworten mit mehr als 1.280 Byte. Bisher unterstützte die NetScaler-Appliance nur eine UDP-Paketgröße von nur bis zu 1.280 Byte.

Sie können die maximale UDP-Paketgröße festlegen, die die Appliance im Proxy-, ADNS- und Forwarder-Modus verarbeiten kann, indem Sie den Parameterwert Maximale UDP-Paketgröße konfigurieren. Wenn beispielsweise der Parameterwert Maximale UDP-Paketgröße auf 4096 festgelegt ist, kann die Appliance eine DNS-Antwort mit einer Größe von 4.096 Byte verarbeiten.

Wichtig

- Im Proxy-Modus wird die kleinste Größe zwischen der OPT-Nutzlastgröße der Clientanfrage und dem Wert für die maximale UDP-Paketgröße für das Senden von DNS-Abfragen an das Backend berücksichtigt. Wenn beispielsweise die OPT-Nutzlastgröße der Clientanfrage 3000 beträgt und der Wert für die maximale UDP-Paketgröße 4096 beträgt, werden 3.000 Byte große DNS-Abfragen an das Backend gesendet.

  Außerdem kann die Appliance vom Backend aus Antworten großer Größen empfangen und Antworten großer Größen verarbeiten.
- Im Forwarder-Modus legt die Appliance die OPT-Nutzlastgröße auf den Wert des Parameters UDP-Paketgröße fest.
- Wenn die DNS-Einträge lokal auf der Appliance sind, kann die Appliance Antwortgrößen erstellen, die so groß sind wie der Parameterwert Maximale UDP-Paketgröße. Diese Einstellung gilt für ADNS-, Proxy- und rekursive Resolver.

So konfigurieren Sie die maximale UDP-Paketgröße mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set dns parameter [-maxUDPPacketSize <positive_integer>]
<!--NeedCopy-->
```

Beispiel:

```
set dns parameter -maxUDPPacketSize 10000
<!--NeedCopy-->
```

Hinweis:

Der Mindest- und Höchstwert, den Sie für den Parameter Maximale UDP-Paketgröße festlegen können, sind 512 bzw. 16384. Der Standardwert ist 1280.

So konfigurieren Sie die maximale UDP-Paketgröße mit der GUI

1. Navigieren Sie zu **Traffic Management** > **DNS**.
2. Klicken Sie im Detailbereich auf **DNS-Einstellungen ändern**.
3. Geben Sie unter Maximale UDP-Paketgröße die maximale UDP-Paketgröße an.
4. Klicken Sie auf **OK**.

Konfigurieren der DNS-Protokollierung

May 11, 2023

Sie können die NetScaler-Appliance so konfigurieren, dass die DNS-Anforderungen und -Antworten protokolliert werden, die sie verarbeitet. Die Appliance protokolliert die DNS-Anfragen und -Antworten im SYSLOG-Format. Sie können entweder DNS-Anfragen oder DNS-Antworten oder beides protokollieren und die Syslog-Meldungen an einen Remote-Protokollserver senden. Die Protokollmeldungen können verwendet werden, um:

- Prüfen Sie die DNS-Antworten an den Kunden
- Prüfung von DNS-Clients
- Erkennen und verhindern Sie DNS-Angriffe
- Problembehandlung

Eine NetScaler-Appliance kann die folgenden Abschnitte in der DNS-Anforderung oder -Antwort basierend auf Ihrer Konfiguration protokollieren:

- Header-Abschnitt
- Abschnitt “Fragen”
- Abschnitt “Antwort”
- Abschnitt Autorität
- **Zusätzliche** Rubrik

DNS-Profile

Sie können ein DNS-Profil verwenden, um die verschiedenen DNS-Parameter zu konfigurieren, die der DNS-Endpunkt auf den DNS-Verkehr anwenden soll. Im Profil können Sie Protokollierung, Caching und negatives Caching aktivieren.

Wichtig: Seit der Version NetScaler 11.0 wurde die Aktivierung des DNS-Cachings mithilfe globaler DNS-Parameter eingestellt. Sie können das DNS-Caching mithilfe von DNS-Profilen aktivieren oder deaktivieren. Sie können jetzt das DNS-Caching für einen einzelnen virtuellen Server aktivieren, indem Sie das DNS-Caching in einem DNS-Profil aktivieren und das DNS-Profil auf den einzelnen virtuellen Server festlegen.

DNS-Profile unterstützen die folgenden Arten von DNS-Protokollierung:

- DNS-Abfrageprotokollierung
- Protokollierung des DNS-Antwortabschnitts
- Erweiterte DNS-Protokollierung
- DNS-Fehlerprotokollierung

Protokollierung von DNS-Abfragen

Sie können eine NetScaler-Appliance so konfigurieren, dass nur die DNS-Abfragen protokolliert werden, die von den DNS-Endpunkten auf der Appliance empfangen werden.

Hinweis: Wenn bei der Verarbeitung einer Abfrage Fehler auftreten, werden sie protokolliert, wenn diese Option im DNS-Profil festgelegt ist.

Es folgt ein Beispiel für eine Abfrageprotokollnachricht:

```
DNS DNS_QUERY 143 0 :  U:10.102.27.70#61297:10.102.27.73#53/22142/Q/
(RD)/NO/1/0/0/0#test.com./1#
<!--NeedCopy-->
```

Protokollierung des DNS-Antwortabschnitts

Sie können eine NetScaler-Appliance so konfigurieren, dass alle **Antwortabschnitte** in den DNS-Antworten protokolliert werden, die die Appliance an den Client sendet. Die Protokollierung des DNS-Antwortabschnitts ist nützlich, wenn der NetScaler als DNS-Resolver konfiguriert ist, oder in GLSB-Anwendungsfällen.

Es folgt ein Beispiel für ein DNS-Antwortabschnittsprotokoll:

```
DNS DNS_RESPONSE 6678 0 :  U:100.100.100.210#32776:100.100.100.10#
53/61373/Q/(RD,AA,RA,R)/NO/1/1/2/4#n1.citrix.com1./
28#ANS#AAAA/120/1111:2345:6789:ffab:abcd:effa:1234:3212##
<!--NeedCopy-->
```

Erweiterte DNS-Protokollierung

Um eine NetScaler-Appliance für die Protokollierung von Autorität und **zusätzlichen** Abschnitten in den DNS-Antworten zu konfigurieren, aktivieren Sie die erweiterte Protokollierung mit Protokollierung des Antwortabschnitts.

Hinweis: Wenn bei der Verarbeitung von Abfragen oder Antworten Fehler auftreten, werden die Fehler protokolliert, wenn diese Option im DNS-Profil festgelegt ist.

Es folgt ein Beispiel für eine Meldung, die protokolliert wird, wenn die Cache-Suche abgeschlossen ist und die Antwort in das Paket eingebettet ist:

```
DNS DNS_RESPONSE 2252 0 :  T:100.100.100.118#21411:100.100.100.10
#53/48537/Q/(RD,AA,CD,RA,R)/NO/1/1/2/6#a1.citrix.com1./1#ANS#A/
120/1.1.1.1##AUTH#citrix.com1/NS/120/n2.citrix.com1#n1.citrix.com1##ADD
   #n1.citrix.com1
/A/120/1.1.1.1#1.1.1.2##n1.citrix.com1/AAAA/120/
```



```
1111:2345:6789:ffab:abcd:effa:1234:3212##n2.citrix.com1/A/120/2.1.1.2
##n2.citrix.com1/AAAA/120/2222:faff:3212:8976:123:1241:64:ff9b##OPT
   /0/1280/DO##
<!--NeedCopy-->
```

DNS-Fehlerprotokollierung

Sie können eine NetScaler-Appliance so konfigurieren, dass die Fehler oder Fehler protokolliert werden, die bei der Verarbeitung einer DNS-Abfrage oder -Antwort auftreten. Für diese Fehler protokolliert die Appliance den DNS-Header, die **Fragenabschnitte** und die OPT-Datensätze.

Es folgt ein Beispiel für eine Nachricht, die protokolliert wird, wenn während der Verarbeitung einer DNS-Anforderung oder -Antwort ein Fehler auftritt:

```
DNS DNS_ERROR 149 0 :  U:10.102.27.70#27832:10.102.27.73#53/61153/Q/
(RD)/NO/1/0/0/0#test.com./1140#Packet Dropped
<!--NeedCopy-->
```

Policy-basierte Protokollierung

Sie können benutzerdefinierte Protokollierung basierend auf DNS-Ausdrücken konfigurieren, indem Sie die Richtlinien LogAction für DNS-Richtlinien, Rewrite oder Responder konfigurieren. Sie können angeben, dass die Protokollierung nur erfolgt, wenn eine bestimmte DNS-Richtlinie als true ausgewertet wird. Weitere Informationen finden Sie unter Konfigurieren der richtlinienbasierten Protokollierung für DNS.

Verstehen des NetScaler Syslog-Nachrichtenformats

Die NetScaler-Appliance protokolliert DNS-Anforderungen und -Antworten im folgenden Syslog-Format:

```
<transport> :<client IP>#<client ephemeral port>:<DNS endpoint IP>#<
   port>
 : <query id> /opcode/header flags/rcode/question section count/answer
    section count
/ auth section count / additional section count #<queried domain name>
/<queried type>#...
<!--NeedCopy-->
```

- **<transport>:**
  - T = TCP

  - U = UDP
- **<client IP>#< client ephemeral port >:** DNS-Client-IP-Adresse und Portnummer
- **<DNS endpoint IP>#<port>:** NetScaler DNS-Endpunkt-IP-Adresse und Portnummer
- **<query id>:**
  Abfrage-ID
- **<opcode>:** Betriebscode. Unterstützte Werte:
  - Q: Abfrage
  - I: umgekehrte Abfrage
  - S: Status
  - X0: nicht zugewiesen
  - N: benachrichtigen
  - U: aktualisieren
  - X1-10: nicht zugewiesene Werte
- **<header flags>:** Flags. Unterstützte Werte:
  - RD: Rekursion erwünscht
  - TC: abgeschnitten
  - AA: maßgebliche Antwort
  - CD: Scheck deaktiviert
  - AD: authentifizierte Daten
  - Z: nicht zugewiesen
  - RA: Rekursion verfügbar
  - R: Antwort
- **<rcode>:** Antwortcode. Unterstützte Werte:
  - NO: kein Fehler
  - F Formatfehler
  - S: Serverausfall
  - NX: nicht existierende Domäne
  - NI: nicht implementiert
  - R: Abfrage abgelehnt
  - YX: Name Existiert wenn es nicht darf
  - YXR: RR Set Existiert wenn es nicht darf
  - NXR: RR Set das existieren muss gibt es nicht
  - NAS: Server nicht maßgeblich für Zone
  - NA: Nicht autorisiert
  - NZ: Name nicht in der Zone enthalten
  - X1-5: nicht zugewiesen

- **/question section count/answer section count/auth section count/additional section count:** Fragenabschnitt, Autoritätsabschnittsanzahl und Anzahl **zusätzlicher** Abschnitte in DNS-Anforderung
- **<queried domain name>/<queried type>:** Abgefragte Domäne und abgefragter Typ in der DNS-Anforderung
- **#ANS#<record type>/<ttl>/.. #AUTH#<domain name>/<record type>/<ttl>.. #ADD#<domain name>/<record type>/<ttl>...:**

  In DNS-Antworten:

  Der Antwortbereich wird protokolliert, wenn die Protokollierung des Antwortbereichs im DNS-Profil aktiviert ist. Autorität und **Zusätzliche** Abschnitte werden protokolliert, wenn die erweiterte Protokollierung im DNS-Profil aktiviert ist. Das Protokollformat würde sich je nach Art des Datensatzes unterscheiden. Weitere Informationen finden Sie unter Grundlegendes zum Format der Datensatzprotokollierung.

  - ANS: answer section
  - AUTH: authority
  - ADD: **Additional** section
- **OPT/<edns version>/UDP max payload size/DO:** OPT-Datensatzformat im DNS-Protokoll
- **OPT/<EDNS version>/<UDP payload size>/<“DO”or empty based on whether DNSSEC OK bit is set or not>/<value of RDLEN>/ECS/<Q/R>/<option length>/<Family>/<Source Prefix-Length>/<Scope Prefix-Length>/<ECS Address>:**

  Wenn die DNS-Abfrage oder -Antwort die Option EDNS-Client-Subnetz (ECS) enthält, wird dies auch im OPT-Datensatzformat in der DNS-Protokolldatei protokolliert.

  Wenn eine DNS-Abfrage mit einer ECS-Option gesendet wird, die entweder eine IPv4- oder IPv6-Adresse enthält, wird die ECS-Option mit einer der folgenden Optionen protokolliert:

  - “ECS/Q” zeigt an, dass die Werte im Protokoll aus der Abfrage stammen
  - “ECS/R” zeigt an, dass die Werte im Protokoll aus der Antwort stammen.

  Der Wert von Scope Prefix-Length wird ebenfalls entsprechend eingestellt. In der DNS-Abfrage wird sie auf Null gesetzt, und für die Antwort wird sie auf den berechneten Wert festgelegt.

  In der folgenden Tabelle werden die protokollierten Details in verschiedenen Szenarien beschrieben:

Szenario	ECS-Option in der DNS-Abfrage festgelegt	ECS-Option in der DNS-Antwort festgelegt	Protokollierte Details
Sowohl Abfrageprotokollierung als auch erweiterte Protokollierung aktiviert	Ja	Ja	Die ECS-Option wird mit der Zeichenfolge “ECS/R/” protokolliert und die Scope-Präfix-Länge wird auf den berechneten Wert eingestellt.
Sowohl Abfrageprotokollierung als auch erweiterte Protokollierung aktiviert	Ja	Nein	Die ECS-Option wird mit der Zeichenfolge “ECS/Q” protokolliert und die Bereichspräfixlänge wird auf Null gesetzt.
Die Abfrageprotokollierung ist aktiviert, die erweiterte Protokollierung ist jedoch nicht aktiviert	Ja	Ja	Die ECS-Option wird mit der Zeichenfolge “ECS/Q/” protokolliert und die Scope-Präfix-Länge wird auf Null gesetzt.
Abfrageprotokollierung und erweiterte Protokollierung sind nicht aktiviert	Ja	Ja	Die ECS-Option ist nicht protokolliert.
Die Abfrageprotokollierung ist aktiviert, die erweiterte Protokollierung ist jedoch nicht aktiviert	Ja	Nein	Die ECS-Option wird mit der Zeichenfolge “ECS/Q/” protokolliert und die Scope-Präfix-Länge wird auf Null gesetzt.

Szenario	ECS-Option in der DNS-Abfrage festgelegt	ECS-Option in der DNS-Antwort festgelegt	Protokollierte Details
Die Abfrageprotokollierung ist nicht aktiviert, aber die erweiterte Protokollierung ist aktiviert	Ja	Ja	Die ECS-Option wird mit der Zeichenfolge “ECS/R/” protokolliert und die Scope-Präfix-Länge wird auf den berechneten Wert eingestellt.
Die Abfrageprotokollierung ist nicht aktiviert, aber die erweiterte Protokollierung ist aktiviert	Ja	Nein	Die ECS-Option ist nicht protokolliert.

Verstehen Sie das Datensatzprotokollformat

Es folgt ein Beispiel für das Datensatzprotokollierungsformat in einer Syslog-Meldung:

```
<domainname>/<record type>/ <record ttl> / <resource record data>#<
    resource record data>#......##
<!--NeedCopy-->
```

Es gilt:

Datensatztyp	Beispiel-Format	Ressourcen-Datensatzdaten/Format
Adresse (A)-Datensatz	A/5/1.1.1.1#1.1.1.2#1.1.1.3##	IPv4-Adresse
AAAA-Datensatz	AAAA/5/1::1#1::2#1::3##	IPv6-Adresse
SOA-Datensatz	SOA/3600/ns1.dnslogging.test./	Ursprungsserver, Kontakt und andere Details. Resource record format is: <originServer>/<contact>/<serial number>/<refresh rate>/<retry>/<expire>/<minimum>##

Datensatztyp	Beispiel-Format	Ressourcen-Datensatzdaten/Format
NS-Datensatz	NS/5/ns1.dnslogging.test	Hostname des Nameservers.
MX-Datensatz	#MX/5/10/host1.dnslogging.test	Präferenz gefolgt von Mail-Exchange-Server-Host
CNAME-Record-Protokollierung	CNAME/5/host1.dnslogging.test.##	Kanonischer Name
SRV-Datensatz	SRV/5/1/2/3/host1.dnslogging.t	Ressourcendatensatzformat: .## <priority>/<weight>/<port>/<target>#
TXT-Datensatz	TXT/5/dns+logging##	Die Daten umfassen alle Texte.
NAPTR-Datensatz	NAPTR/5/10/11////dnslogging#1	Ressourcendatensatzformat: ## <order>/<preference>/<flags>/<services>/<re expression>/<replacement string>#
DNSKEY-Datensatz	DNSKEY/5/1/3/5/AwEAAanP0K+i5	Ressourcendatensatzformat: <flags>/<protocol>/<algorithm>/<public key in base64 encoding>#
PTR-Datensatz	PTR/3600/test.com.#test4.com.	Domänenname

Einschränkungen der DNS-Protokollierung

Die DNS-Protokollierung hat die folgenden Einschränkungen:

- Wenn die Antwortprotokollierung aktiviert ist, werden nur die folgenden Datensatztypen protokolliert:
  - Adresse (A)-Datensatz
  - AAAA-Datensatz
  - SOA-Datensatz
  - NS-Datensatz
  - MX-Datensatz
  - CNAME-Datensatz
  - SRV-Datensatz
  - TXT-Datensatz
  - NAPTR-Datensatz
  - DNSKEY-Datensatz
  - PTR-Datensatz

Für alle anderen Datensatztypen werden nur L3/L4-Parameter, DNS-Header und Frage-Abschnitt protokolliert.

- RRSIG-Datensätze werden nicht protokolliert, selbst wenn die Antwortprotokollierung aktiviert ist.
- DNS64 wird nicht unterstützt.
- Proaktive DNS-Aktualisierungsanforderungen oder -antworten werden gemäß den Einstellungen im Standardprofil protokolliert.
- Wenn auf dem virtuellen Server die sitzungslose Option- und Antwortprotokollierung aktiviert ist, werden L3/L4-Parameter, der DNS-Header und der Abschnitt DNS-Frage anstelle der Antwort protokolliert.
- Die maximale Größe der Syslog-Nachricht beträgt 1024 Byte.
- Wenn Sie ein DNS-Profil für eine DNS-Richtlinie mit dem Aktionstyp Rewrite-Antwort festgelegt haben, protokolliert die NetScaler-Appliance die Abfrage oder die manipulierten Antworten nicht. Um die erforderlichen Informationen zu protokollieren, müssen Sie eine Aktion für eine Überwachungsnachricht in der DNS-Richtlinie verwenden.
- DNS-Transaktionen, die auf den DNS-Überwachungsverkehr zurückzuführen sind, werden nicht protokolliert.

Konfigurieren der DNS-Protokollierung

Es folgt eine Übersicht über die Konfiguration der DNS-Protokollierung:

1. Erstellen Sie eine Syslog-Aktion und aktivieren Sie DNS in der Aktion.
2. Erstellen Sie eine Syslog-Richtlinie und geben Sie die Syslog-Aktion in der Richtlinie an.
3. Binden Sie die Syslog-Richtlinie global, um die Protokollierung aller NetScaler-Systemereignisse zu ermöglichen. Oder binden Sie die Syslog-Richtlinie an einen bestimmten virtuellen Lastausgleichsserver.
4. Erstellen Sie ein DNS-Profil und definieren Sie eine der folgenden Protokollierungstypen, die Sie aktivieren möchten:
    - DNS-Abfrageprotokollierung
    - Protokollierung des DNS-Antwortabschnitts
    - Erweiterte DNS-Protokollierung
    - DNS-Fehlerprotokollierung
5. Konfigurieren Sie je nach Ihren Anforderungen eine der folgenden Optionen:
    - DNS-Dienst und virtueller Server für DNS
    - ADNS-Dienst
    - NetScaler als Spediteur
    - NetScaler als Resolver

6. Stellen Sie das erstellte DNS-Profil auf eine der DNS-Entitäten ein.

Konfigurieren Sie die DNS-Protokollierung für NetScaler, konfiguriert als DNS-Proxy über die CLI

1. Fügen Sie eine Syslog-Aktion hinzu und aktivieren Sie DNS in der Aktion. Geben Sie in der Befehlszeile Folgendes ein:

```
add audit syslogAction <name> (<serverIP> | -lbVserverName <string
    >) [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat <
    dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )]
     [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME |
    LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-
    appflowExport ( ENABLED |DISABLED )] [-lsn ( ENABLED | DISABLED
     )] [-alg ( ENABLED | DISABLED )] [-transport ( TCP | UDP )] [-
    tcpProfileName <string>] [-maxLogDataSizeToHold <
    positive_integer>] [-dns ( ENABLED | DISABLED)]
<!--NeedCopy-->
```

Beispiel:

```
add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
LOCAL_TIME -dns ENABLED
```

2. Erstellen Sie eine Syslog-Richtlinie und geben Sie die erstellte Syslog-Aktion in der Richtlinie an. Geben Sie in der Befehlszeile Folgendes ein:

```
add audit syslogPolicy <name> <rule> <action>
```

Beispiel:

```
add audit syslogPolicy syslogpol1 ns_true nssyslogact1
```

3. Binden Sie die Syslog-Richtlinie global. Geben Sie in der Befehlszeile Folgendes ein:

```
bind system global [<policyName> [-priority <positive_integer>]]
```

Beispiel:

```
bind system global syslogpol1
```

4. Erstellen Sie ein DNS-Profil und aktivieren Sie eine der folgenden Arten von Protokollen, die Sie konfigurieren möchten:

   - DNS-Abfrageprotokollierung
   - Protokollierung des DNS-Antwortabschnitts
   - Erweiterte DNS-Protokollierung

- DNS-Fehlerprotokollierung

Geben Sie in der Befehlszeile Folgendes ein:

```
add dns profile <dnsProfileName> [-dnsQueryLogging ( ENABLED | DISABLED
 )] [-dnsAnswerSecLogging ( ENABLED | DISABLED )] [-dnsExtendedLogging
 (ENABLED | DISABLED )] [-dnsErrorLogging ( ENABLED | DISABLED )] [-
cacheRecords ( ENABLED | DISABLED )] [-cacheNegativeResponses ( ENABLED
 | DISABLED )]
```

Beispiel:

```
add dns profile dnsprofile1 -dnsQueryLogging ENABLED
```

5. Konfigurieren Sie den Dienst vom Typ DNS. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   add service <name> <serverName> <serviceType> <port>
   ```

   Beispiel:

   ```
   add service svc1 10.102.84.140 dns 53
   ```

6. Konfigurieren Sie einen virtuellen Lastausgleichsserver des Diensttyps DNS.

   ```
   add lb vserver <name> <serviceType> <ip> <port>
   ```

   Beispiel:

   ```
   add lb vserver lb1 dns 100.100.100.10 53
   ```

7. Binden Sie den Dienst an den virtuellen Server. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   bind lb vserver <name> <serviceName>
   ```

   Beispiel:

   ```
   bind lb vserver lb1 svc1
   ```

8. Stellen Sie das erstellte DNS-Profil auf den virtuellen Server ein. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   set lb vserver <name> [ - dnsProfileName <string>]
   ```

   Beispiel:

   ```
   set lb vserver lb1 -dnsProfileName dnsprofile1
   ```

Beispiel-DNS-Protokollierungskonfiguration für NetScaler-Appliance, konfiguriert als DNS-Proxy

```
1 > add audit syslogAction nssyslogact1 10.102.151.136 -logLevel
2 CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -
      timeZone
```



```
LOCAL_TIME -dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```

Beispiel-DNS-Protokollierungskonfiguration für NetScaler-Appliance, konfiguriert als ADNS

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```

Beispiel-DNS-Protokollierungskonfiguration für NetScaler-Appliance, die als Forwarder konfiguriert ist

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
```



```
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add dns nameserver 8.8.8.8  - dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Beispiel einer DNS-Protokollierungskonfiguration für eine als Resolver konfigurierte NetScaler-Appliance

```
> add audit syslogAction nssyslogact1 10.102.151.136
-logLevel CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -
    logFacility LOCAL4
-timeZone LOCAL_TIME -dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> set dns parameter -recursion enABLED
Done
> add nameserver 1.1.1.100 -local dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Konfigurieren der richtlinienbasierten Protokollierung für DNS

Mit der richtlinienbasierten Protokollierung können Sie ein Format für Protokollnachrichten angeben. Der Inhalt einer Protokollnachricht wird mithilfe eines erweiterten Richtlinienausdrucks definiert. Wenn die in der Richtlinie angegebene Nachrichtenaktion ausgeführt wird, erstellt die NetScaler-Appliance die Protokollnachricht aus dem Ausdruck und schreibt die Nachricht in die Protokolldatei. Sie können die Appliance so konfigurieren, dass sie nur protokolliert wird, wenn eine bestimmte DNS-Richtlinie den Wert True ergibt.

> **Hinweis**
>
> Wenn Sie eine DNS-Richtlinie mit einem DNS-Profil für die Anforderungsseite festgelegt haben, protokolliert die NetScaler-Appliance nur die Abfrage.

Um die richtlinienbasierte Protokollierung für eine DNS-Richtlinie zu konfigurieren, müssen Sie zunächst eine Auditmeldungsaktion konfigurieren. Weitere Informationen zum Konfigurieren einer Überwachungsnachrichtenaktion finden Sie unter Konfigurieren der NetScaler Appliance für die Audit-Protokollierung. Geben Sie nach dem Konfigurieren der Auditmeldungsaktion die Meldungsaktion in einer DNS-Richtlinie an.

Konfigurieren Sie die richtlinienbasierte Protokollierung für eine DNS-Richtlinie über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die richtlinienbasierte Protokollierung für eine DNS-Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
1 -  add dns action <actionName> <actionType> [-IPAddress <ip_addr|
     ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
     ...] [-TTL <secs>] [-dnsProfileName <string>]
2 -  set dns policy <name> [<rule>] [-actionName <string>] [-logAction <
     string>]
3 -  show dns policy [<name>]
4 <!--NeedCopy-->
```

Beispiel 1:

Wenn Sie in einer GSLB-Bereitstellung mit unterschiedlichen IP-Adressen auf die Clientanforderungen aus einem bestimmten Subnetz antworten möchten, anstatt mit IP-Adressen zu antworten, die für allgemeine Zwecke verwendet werden (z. B. die IP-Adressen interner Benutzer), können Sie eine DNS-Richtlinie mit dem Aktionstyp als DNS-Ansicht konfigurieren. In diesem Fall können Sie die DNS-Protokollierung für die angegebene DNS-Aktion so konfigurieren, dass Sie die spezifischen Antworten protokollieren können.

```
1 > add dns profile dns_prof1 -dnsqueryLogging enABLED -
     dnsanswerSecLogging enABLED
2  Done
3 > add dns view dns_view1
4  Done
5 > add dns action dns_act1 viewName -view dns_view1  - dnsprofilename
     dns_prof1
6  Done
7 > add dns policy dns_pol1 "CLIENT.IP.SRC.APPLY_MASK(255.255.255.0).EQ
     (100.100.100.0)”
8 dns_act1
```



```
 Done
> bind dns global dns_pol1 100 -gotoPriorityExpression END -type
   REQ_DEFAULT
 Done
> bind gslb service site_1_svc -viewName dns_view1 123.1.1.1
 Done
> bind gslb service site_5_svc -view dns_view1 132.1.1.1
 Done
<!--NeedCopy-->
```

Hinweis: Wenn Sie in der vorherigen Konfiguration nach der Domäne abfragen, die auf einem virtuellen GSLB-Server konfiguriert ist, z. B. *sampletest.com*, werden alle internen Benutzer des Subnetzes 100.100.100.0/24 mit den IP-Adressen der DNS-Ansicht bedient und die Antworten werden protokolliert. Clientanforderungen für andere Subnetze werden nicht protokolliert.

Beispiel 2:

Wenn Sie nur die Abfragen für die Domäne *example.com*protokollieren möchten, können Sie ein DNS-Profil mit aktivierter Abfrageprotokollierung erstellen und das DNS-Profil auf eine DNS-Aktion mit dem
Aktionstyp NOOPfestlegen und dann eine DNS-Richtlinie erstellen und die DNS-Aktion festlegen. Zum Beispiel:

```
>add dns profile query_logging -dnsqueryLogging ENABLED
Done
>add dns action dns_act1 NOOP -dnsprofileName query_logging
Done
>add dns policy dns_pol1 DNS.REQ.QUESTION.DOMAIN.EQ("example.com")
   dns_act1
Done
<!--NeedCopy-->
```

Konfigurieren der Protokollaktion für die DNS-Richtlinie zum Protokollieren der Client-IP-Adresse

Die Protokollierungsaktion kann verwendet werden, um die Quell-IPs für die DNS-Abfragen mit dem folgenden Ausdruck zu protokollieren und als Teil der Protokollaktion in der DNS-Richtlinie zu verwenden.

```
> add audit messageaction log_act_custom INFORMATIONAL ""ClientIP:"
   CLIENT.IP.SRC" ECS IP:"+((DNS.REQ.OPT.ECS.IP).typecast_text_t ALT "
   NONE")"
Done
<!--NeedCopy-->
```


Der frühere Ausdruck erfasst sowohl die Quell-IP wie im IP-Header als auch die ECS-IP aus der DNS-ECS-Option, und jede davon kann bei Bedarf ausgeschlossen werden.

Beispiel einer DNS-Protokollierungskonfiguration für eine NetScaler-Appliance zum Protokollieren der Client

Wenn Sie die Protokollierung der DNS-Abfragen testen möchten, können Sie dies mit dem folgenden Ausdruck tun. Dadurch wird eine von 10 Abfragen protokolliert.

```
1 > add audit messageaction log_action_srcip_1of10 INFORMATIONAL ""
     OneOf10: Source IP : "+client.ip.src"
2 Done
3 > add responder policy logsrcip_1of10 "sys.random.mul(10).lt(1)" NOOP -
     logAction log_action_srcip_1of10
4 Done
5 <!--NeedCopy-->
```

DNS-Suffixe konfigurieren

May 11, 2023

Sie können DNS-Suffixe konfigurieren, die es der NetScaler-Appliance ermöglichen, nicht vollständig qualifizierte Domänennamen bei der Namensauflösung zu vervollständigen. Wenn beispielsweise bei der Auflösung eines nicht vollständig qualifizierten Domainnamens abc ein DNS-Suffix example.com konfiguriert ist, fügt die Appliance das Suffix an den Domainnamen an. Dann wird der Domainname aufgelöst. In diesem Fall würde es abc.example.com auflösen. Wenn keine DNS-Suffixe konfiguriert sind, fügt die Appliance den nicht vollständig qualifizierten Domainnamen einen Punkt an und löst den Domainnamen auf.

DNS-Suffixe erstellen

DNS-Suffixe haben Bedeutung und sind nur gültig, wenn der NetScaler als Endresolver oder Forwarder konfiguriert ist. Sie können ein Suffix mit bis zu 127 Zeichen angeben.

> **Hinweise:**
>
> - Die Reihenfolge der DNS-Suffixe ist wichtig. Die ADC-Appliance probiert die konfigurierten Suffixe in serieller Reihenfolge aus und stoppt, wenn sie eine erfolgreiche Antwort auf ein Suffix erhält.
> - Zu einem Zeitpunkt wird nur ein Domainname verarbeitet. Alle verfügbaren Suffixe werden

> an den Domainnamen angehängt, bis eine erfolgreiche Antwort eingeht.
> **Zum Beispiel:** Wenn der Domainname `www` ist und die Suffixe `abc.com` und `abc` sind. Die NetScaler-Appliance versucht zuerst `www.abc.com`. Wenn dies keine erfolgreiche Antwort zurückgibt, versucht die Appliance `www.abc`. Wenn `www.abc.com` eine erfolgreiche Antwort zurückgibt, versucht die Appliance nicht, das nächste Suffix zu verwenden.
> - Die Appliance verwendet alle Suffixe in der Reihenfolge, in der sie hinzugefügt wurden, bis sie eine erfolgreiche Antwort erhält.

DNS-Suffixe über die CLI erstellen

Geben Sie in der Befehlszeile die folgenden Befehle ein, um ein DNS-Suffix zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add dns suffix <dnsSuffix>
2 -  show dns suffix <dnsSuffix>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns suffix example.com
2  Done
3 > show dns suffix example.com
4 1)      Suffix: example.com
5 Done
6
7 <!--NeedCopy-->
```

Um ein DNS-Suffix mit der NetScaler-Befehlszeile zu entfernen, geben Sie an der Eingabeaufforderung den Befehl `rm dns suffix` und den Namen des DNS-Suffixes ein.

DNS-Suffixe über die GUI erstellen

Navigieren Sie zu **Traffic Management > DNS > DNS-Suffix** und erstellen Sie DNS-Suffixe.

DNS ANY Abfrage

May 11, 2023

Eine ANY-Abfrage ist eine Art von DNS-Abfrage, die alle für einen Domainnamen verfügbaren Datensätze abruft. Die ANY-Anfrage muss an einen Nameserver gesendet werden, der für eine Domain autorisierend ist.

Verhalten im ADNS-Modus

Im ADNS-Modus gibt die NetScaler-Appliance die in ihrem lokalen Cache gespeicherten Datensätze zurück. Wenn der Cache keine Datensätze enthält, gibt die Appliance die (negative) Antwort NXDOMAIN zurück.

Wenn der NetScaler die Domänendelegierungsdatensätze abgleichen kann, gibt er die NS-Einträge zurück. Andernfalls werden die NS-Einträge der Stammdomäne zurückgegeben.

Verhalten im DNS-Proxymodus

Im Proxymodus überprüft die NetScaler-Appliance ihren lokalen Cache. Wenn der Cache keine Datensätze enthält, leitet die Appliance die Abfrage an den Server weiter.

Verhalten für GSLB-Domänen (Global Server Load Balancing)

Wenn eine GSLB-Domäne auf der ADC-Appliance konfiguriert ist und eine ANY-Abfrage für die GSLB-Domäne (Standort) gesendet wird, gibt die Appliance die IP-Adresse des GSLB-Dienstes zurück. Es wählt diesen Dienst anhand einer Load-Balancing-Entscheidung aus. Wenn die Option Multiple IP Response (MIR) aktiviert ist, werden die IP-Adressen aller GSLB-Dienste gesendet.

Damit der NetScaler diese Datensätze zurückgibt, wenn er auf die ANY-Anfrage antwortet, müssen alle Datensätze, die einer GSLB-Domäne entsprechen, auf dem NetScaler konfiguriert werden.

> **Hinweis**
>
> Wenn Datensätze für eine Domäne zwischen dem NetScaler und einem Server verteilt werden, werden nur auf dem NetScaler konfigurierte Datensätze zurückgegeben.

Der NetScaler bietet die Möglichkeit, DNS-Ansichten und DNS-Richtlinien zu konfigurieren. Diese Ansichten und Richtlinien werden für die Durchführung des globalen Lastenausgleichs von Servern verwendet. Weitere Informationen finden Sie unter Globaler Server-Lastenausgleich.

Konfigurieren des negativen Caching von DNS-Datensätzen

May 11, 2023

Die NetScaler-Appliance unterstützt das Zwischenspeichern negativer Antworten für eine Domain. Eine negative Antwort weist darauf hin, dass Informationen zu einer angeforderten Domäne nicht existieren oder dass der Server keine Antwort auf die Abfrage geben kann. Die Speicherung dieser Informationen wird als negatives Cachingbezeichnet. Negatives Caching hilft dabei, Antworten auf Anfragen zu einer Domain zu beschleunigen.

> **Hinweis:**
>
> Negatives Caching wird nur unterstützt, wenn der Backend-Server als autorisierender DNS-Server (ADNS) für die abgefragte Domain konfiguriert ist.

Eine negative Reaktion kann eine der folgenden sein:

- NXDOMAIN-Fehlermeldung — Die autoritativen DNS-Server antworten mit der NXDOMAIN-Fehlermeldung, wenn für den abgefragten Domainnamen keine Datensätze auf dem Server konfiguriert sind. Diese Meldung impliziert, dass es sich bei der abgefragten Domain um einen ungültigen oder nicht existierenden Domainnamen handelt.
- NODATA-Fehlermeldung — Wenn der Domainname in der Abfrage gültig ist, aber Datensätze des angegebenen Typs nicht verfügbar sind, sendet die Appliance eine NODATA-Fehlermeldung.

Wenn negatives Caching aktiviert ist, speichert die Appliance die negative Antwort vom DNS-Server im Cache und verarbeitet nur die zukünftigen Anfragen aus dem Cache. Diese Aktion beschleunigt die Beantwortung von Abfragen und reduziert auch den Back-End-DNS-Verkehr. Negatives Caching kann in allen Bereitstellungen verwendet werden, d. h. wenn eine NetScaler Appliance als Proxy, Endresolver oder Weiterleitung fungiert.

Sie können negatives Caching mit einem DNS-Profil aktivieren oder deaktivieren, weitere Informationen finden Sie unter DNS-Profile. Standardmäßig ist das negative Zwischenspeichern im Standard-DNS-Profil (**default**-dns-profile) aktiviert, das standardmäßig an einen virtuellen DNS-Server oder im neu erstellten DNS-Profil gebunden ist.

Aktivieren oder deaktivieren Sie negatives Caching mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um das negative Caching zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
1 -  add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED
     )] [-cacheNegativeResponses (ENABLED | DISABLED )]
2 -  show dns profile [<dnsProfileName>]
3 <!--NeedCopy-->
```

Beispiel für ein Standard-DNS-Profil:

```
1 > sh dns profile default-dns-profile
2     1)   default-dns-profile
3         Query logging : DISABLED        Answer section logging :
             DISABLED
4         Extended logging : DISABLED     Error logging : DISABLED
5         Cache Records : ENABLED     Cache Negative Responses: ENABLED
6 Done
7 <!--NeedCopy-->
```


Beispiel für ein neu erstelltes DNS-Profil:

```
> add dnsprofile dns_profile1 -cacheRecords ENABLED -
    cacheNegativeResponses ENABLED
Done
> show dns profile dns_profile1
    1)   dns_profile1
        Query logging : DISABLED        Answer section logging :
           DISABLED
        Extended logging : DISABLED     Error logging : DISABLED
        Cache Records : ENABLED     Cache Negative Responses: ENABLED
Done
<!--NeedCopy-->
```

Geben Sie DNS-Parameter auf Dienst- oder virtueller Serverebene mithilfe der CLI an

Führen Sie an der Eingabeaufforderung folgende Schritte aus:

1. Konfigurieren Sie das DNS-Profil.

   ```
   add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED )]
    [-cacheNegativeResponses (ENABLED | DISABLED )]
   ```

2. Binden Sie das DNS-Profil an den Dienst oder den virtuellen Server.

   Um das DNS-Profil an den Dienst zu binden:

   ```
   set service <name> [-dnsProfileName <string>]
   ```

Beispiel:

```
>set service service1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```

Um das DNS-Profil an den virtuellen Server zu binden:

```
set lb vserver <name> [-dnsProfileName <string>]
```

Beispiel:

```
>set lb vserver lbvserver1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```


Geben Sie DNS-Parameter auf Service- oder virtueller Serverebene mithilfe der GUI an

1. Konfigurieren Sie das HTTP-Profil.

   Navigieren Sie zu **System** > **Profile**> **DNS-Profil**und erstellen Sie das DNS-Profil.

2. Binden Sie das HTTP-Profil an den Dienst oder den virtuellen Server.

   Navigieren Sie zu **Traffic Management** > **Load Balancing**> **Dienste/Virtuelle Server**und erstellen Sie das DNS-Profil, das an den Dienst oder den virtuellen Server gebunden sein muss.

Geschwindigkeitsbegrenzende negative Reaktion, die das Gerät ausgibt

Sie können einen Schwellenwert für negative Antworten festlegen, die von der NetScaler-Appliance aus dem Cache bereitgestellt werden. Wenn der Schwellenwert festgelegt ist, sendet die Appliance die Antwort aus dem Cache, bis der Schwellenwert erreicht ist. Sobald der Schwellenwert erreicht ist, verwirft die Appliance die Anfragen, anstatt mit einer NXDOMAIN-Antwort zu antworten.

Die Festlegung einer Ratenbegrenzung für negative Antworten hat die folgenden Vorteile.

- Sparen Sie die Ressourcen auf der NetScaler-Appliance.
- Beugen Sie böswilligen Abfragen für nicht existierende Domainnamen vor.

> **Hinweis:** Sie können einen Schwellenwert für negative Antworten nur für die Domänen festlegen, für die die ADC-Appliance als autorisierender Domainnamenserver konfiguriert ist. Sie können keinen Schwellenwert für zwischengespeicherte Datensätze festlegen, die von den autorisierenden Back-End-Nameservern empfangen werden.

Geschwindigkeitsbegrenzung negativer Antworten, die vom Cache mithilfe der CLI bereitgestellt werden

Geben Sie an der Eingabeaufforderung

```
set dns parameter -NXDOMainRateLimitThreshold <positive-integer>
<!--NeedCopy-->
```

Beispiel:

```
set dns parameter -NXDOMainRateLimitThreshold 1000
<!--NeedCopy-->
```

nxDomainRateLimitThreshold: Wenn dieser Parameter auf einen positiven Ganzzahlwert gesetzt ist, werden Antworten aus dem Cache bereitgestellt, bis dieser Schwellenwert (in Sekunden) erreicht ist. Sobald der Schwellenwert überschritten wird, werden die Anfragen verworfen. Der konfigurierte Schwellenwert gilt pro Paket-Engine.

Ratenbegrenzung der negativen Antwort, die vom Cache mithilfe der GUI ausgegeben wird

1. Navigieren Sie zu **Traffic Management > DNS** und klicken Sie auf **DNS-Einstellungen ändern**.
2. Geben Sie auf der Seite **DNS-Parameter konfigurieren** in das Feld **NXDOMAIN Rate Limit Threshold** den Schwellenwert ein, bis zu dem die Antworten aus dem Cache bereitgestellt werden müssen.

Hinweis: Der Wert im **NXDOMAIN Threshold Crossed** zeigt an, wie oft die Anforderungen gelöscht werden, nachdem der Schwellenwert erreicht wurde.

EDNS0-Clientsubnetzdaten zwischenspeichern, wenn sich die NetScaler-Appliance im Proxymodus befindet

May 11, 2023

Wenn im NetScaler Proxymodus ein Backend-Server, der ein EDNS0-Clientsubnetz (ECS) unterstützt, eine Antwort sendet, die die ECS-Option enthält, geht die NetScaler-Appliance wie folgt vor:

- Es leitet die Antwort so wie sie ist an den Kunden weiter und
- Speichert die Antwort zusammen mit den Client-Subnetzinformationen im Cache.

DNS-Anfragen, die aus demselben Subnetz derselben Domain stammen und für die der Server dieselbe Antwort senden würde, werden dann aus dem Cache bedient.

Hinweis:

- ECS-Caching ist standardmäßig deaktiviert. Aktivieren Sie das Zwischenspeichern von EDNS0-Client-Subnetzdaten im zugehörigen DNS-Profil.
- Die Anzahl der Subnetze, die Sie für eine Domain zwischenspeichern können, ist auf die verfügbaren Subnetz-IDs beschränkt, d. h. 1270 in der NetScaler-Appliance. Optional können Sie das Limit auf eine niedrigere Zahl setzen (Mindestwert: 1 ipv4/ipv6).

Zwischenspeichern von ECS-Antworten mithilfe der CLI aktivieren

Geben Sie in der Befehlszeile Folgendes ein:

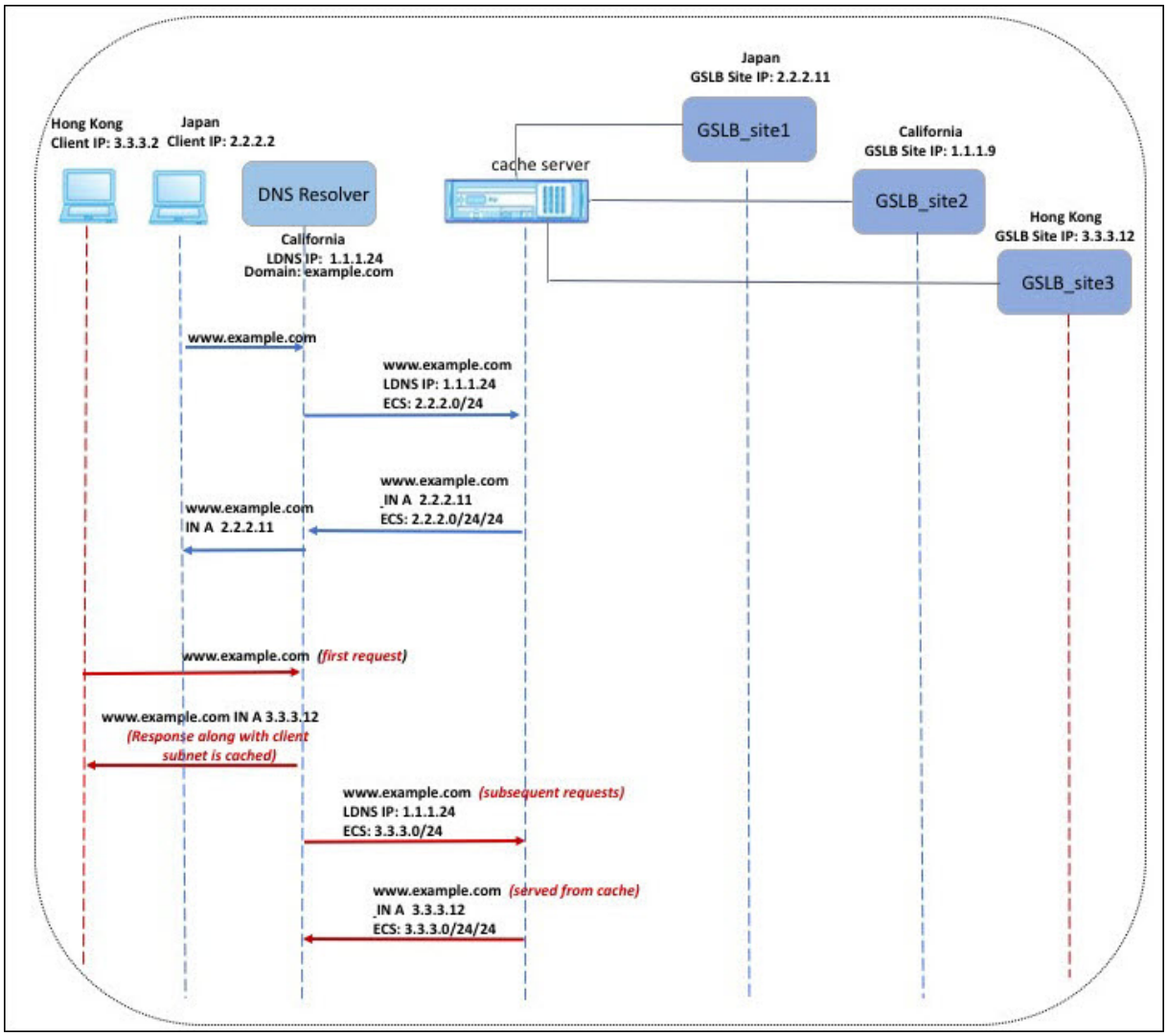
```
set dns profile <dnsProfileName> -cacheECSSubnet ( ENABLED | DISABLED )
```

Anzahl der Subnetze, die pro Domain zwischengespeichert werden können, mithilfe der CLI beschränken

Geben Sie in der Befehlszeile Folgendes ein:

```
set dns profile <dnsProfileName> -maxSubnetsPerDomain <positive_integer>
```


Beispiel:



In dem in der vorherigen Abbildung gezeigten Beispiel sendet der Client mit der IP-Adresse 2.2.2.2 eine Anfrage für www.example.com an den DNS-Resolver. Der DNS-Resolver sendet die folgende Antwort:

www.example.com IN A, IP ist 2.2.2.11 und ECS 2.2.2.0/24/24

Zu diesem Zeitpunkt werden die Antwort und die Client-Subnetz-ID (2.2.2.0/24) zwischengespeichert. Weitere Anfragen aus demselben Subnetz und derselben Domain werden aus dem Cache bedient.

Wenn die IP-Adresse des Clients beispielsweise 2.2.2.100 ist und die Abfrage für www.example.com erfolgt, wird die Abfrage aus dem Cache bereitgestellt und nicht an den Backend-Server gesendet.

Sicherheitserweiterungen für Domänennamen

May 11, 2023

DNS Security Extensions (DNSSEC) ist ein Standard der Internet Engineering Task Force (IETF). Es zielt darauf ab, Datenintegrität und Datenherkunftsauthentifizierung bei der Kommunikation zwischen Nameservern und Clients zu gewährleisten und gleichzeitig UDP-Antworten im Klartext zu übertragen. DNSSEC spezifiziert einen Mechanismus, der asymmetrische Schlüsselkryptografie und eine Reihe neuer Ressourceneinträge verwendet, die spezifisch für seine Implementierung sind.

Die DNSSEC-Spezifikation ist beschrieben in:

- RFC 4033, „Einführung und Anforderungen zur DNS-Sicherheit“
- RFC 4034, „Ressourceneinträge für die DNS-Sicherheitserweiterungen“
- RFC 4035, „Protokolländerungen für die DNS-Sicherheitserweiterungen“

Die betrieblichen Aspekte der Implementierung von DNSSEC innerhalb von DNS werden in RFC 4641, „DNSSEC Operational Practices“, erörtert.

Sie können DNSSEC auf dem NetScaler konfigurieren. Sie können Schlüssel für das Signieren von DNS-Zonen generieren und importieren. Sie können DNSSEC für Zonen konfigurieren, für die der NetScaler autorisiert ist. Sie können den ADC als DNS-Proxyserver für signierte Zonen konfigurieren, die auf einer Farm von Back-End-Nameservern gehostet werden. Wenn der ADC für eine Teilmenge der Datensätze autorisierend ist, die zu einer Zone gehören, für die der ADC als DNS-Proxyserver konfiguriert ist, können Sie die Teilmenge der Datensätze in die DNSSEC-Implementierung aufnehmen.

Konfigurieren von DNSSEC

May 11, 2023

Gehen Sie wie folgt vor, um DNSSEC zu konfigurieren:

1. Aktivieren Sie DNSSEC auf der NetScaler-Appliance.
2. Erstellen Sie einen Zonensignierschlüssel und einen Schlüsselsignierschlüssel für die Zone.
3. Füge die beiden Schlüssel zur Zone hinzu.
4. Unterschreibe die Zone mit den Schlüsseln.

Die NetScaler-Appliance fungiert nicht als DNSSEC-Resolver. DNSSEC auf dem ADC wird nur in den folgenden Bereitstellungsszenarien unterstützt:

1. ADNS — NetScaler ist das ADNS und generiert die Signaturen selbst.
2. Proxy — NetScaler fungiert als DNSSEC-Proxy. Es wird davon ausgegangen, dass der NetScaler in einem vertrauenswürdigen Modus vor den ADNS/LDNS-Servern platziert wird. Der ADC fungiert nur als Proxy-Caching-Entität und validiert keine Signaturen.

DNSSEC aktivieren und deaktivieren

Aktivieren Sie DNSSEC auf dem NetScaler, damit der ADC auf DNSSEC-fähige Clients reagiert. Standardmäßig ist DNSSEC aktiviert.

Sie können die DNSSEC-Funktion deaktivieren, wenn Sie nicht möchten, dass der NetScaler auf Clients mit DNSSEC-spezifischen Informationen reagiert.

Aktivieren oder deaktivieren Sie DNSSEC mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um DNSSEC zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
-  set dns parameter -dnssec ( ENABLED | DISABLED )
-  show dns parameter
<!--NeedCopy-->
```

Beispiel:

```
> set dns parameter -dnssec ENABLED
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
         .
         .
         .
         DNSEC Extension: ENABLED
        Max DNS Pipeline Requests: 255
 Done

<!--NeedCopy-->
```

Aktivieren oder deaktivieren Sie DNSSEC mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf DNS-Einstellungen ändern.
3. Aktivieren oder **deaktivieren Sie im Dialogfeld DNS-Parameter konfigurieren** das Kontrollkästchen **DNSSEC-Erweiterung aktivieren** .

DNS-Schlüssel für eine Zone erstellen

Für jede DNS-Zone, die Sie signieren möchten, müssen Sie zwei asymmetrische Schlüsselpaare erstellen. Ein Paar, der sogenannte Zone Signing Key (ZSK), wird verwendet, um alle Ressourcendaten-

sätze in der Zone zu signieren. Das zweite Paar wird als Key Signing Key (KSK) bezeichnet und wird verwendet, um nur die DNSKEY-Ressourceneinträge in der Zone zu signieren.

Wenn der ZSK und der KSK erstellt werden, wird der `suffix.key` an die Namen der öffentlichen Komponenten der Schlüssel angehängt. Das `suffix.private` wird an die Namen ihrer privaten Komponenten angehängt. Das Anhängen erfolgt automatisch.

Der NetScaler erstellt außerdem einen Delegation Signer (DS) -Datensatz und fügt das Suffix .ds an den Namen des Datensatzes an. Wenn es sich bei der übergeordneten Zone um eine signierte Zone handelt, müssen Sie den DS-Eintrag in der übergeordneten Zone veröffentlichen, um die Vertrauenskette einzurichten.

Wenn Sie einen Schlüssel erstellen, wird der Schlüssel im `/nsconfig/dns/` Verzeichnis gespeichert, aber er wird nicht automatisch in der Zone veröffentlicht. Nachdem Sie mithilfe des Befehls `create dns key` einen Schlüssel erstellt haben, müssen Sie den Schlüssel mithilfe des Befehls `add dns key` explizit in der Zone veröffentlichen. Das Generieren eines Schlüssels ist vom Prozess der Veröffentlichung des Schlüssels in einer Zone getrennt, sodass Sie alternative Methoden zum Generieren von Schlüsseln verwenden können. Sie können beispielsweise Schlüssel importieren, die von anderen Schlüsselgenerierungsprogrammen (z. B. `bind-keygen`) generiert wurden, indem Sie Secure FTP (SFTP) verwenden und dann die Schlüssel in der Zone veröffentlichen. Weitere Informationen zum Veröffentlichen eines Schlüssels in einer Zone finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.

Führen Sie die in diesem Thema beschriebenen Schritte aus, um einen Zonensignierungsschlüssel zu erstellen, und wiederholen Sie dann die Schritte zum Erstellen eines Schlüsselsignierungsschlüssels. Das Beispiel, das der Befehlssyntax folgt, erstellt zunächst ein Schlüsselpaar für die Zonensignierung für die Zone example.com. Das Beispiel verwendet dann den Befehl, um ein Schlüsselsignierschlüsselpaar für die Zone zu erstellen.

Ab Version 13.0 Build 61.x unterstützt die NetScaler-Appliance jetzt stärkere Kryptoalgorithmen wie RSASHA256 und RSASHA512, um eine DNS-Zone zu authentifizieren. Bisher wurde nur der RSASHA1-Algorithmus unterstützt.

Erstellen Sie einen DNS-Schlüssel mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
create dns key -zoneName <string> -keyType <keyType> -algorithm <algorithm>
 -keySize <positive_integer> -fileNamePrefix <string>
```

Beispiel:

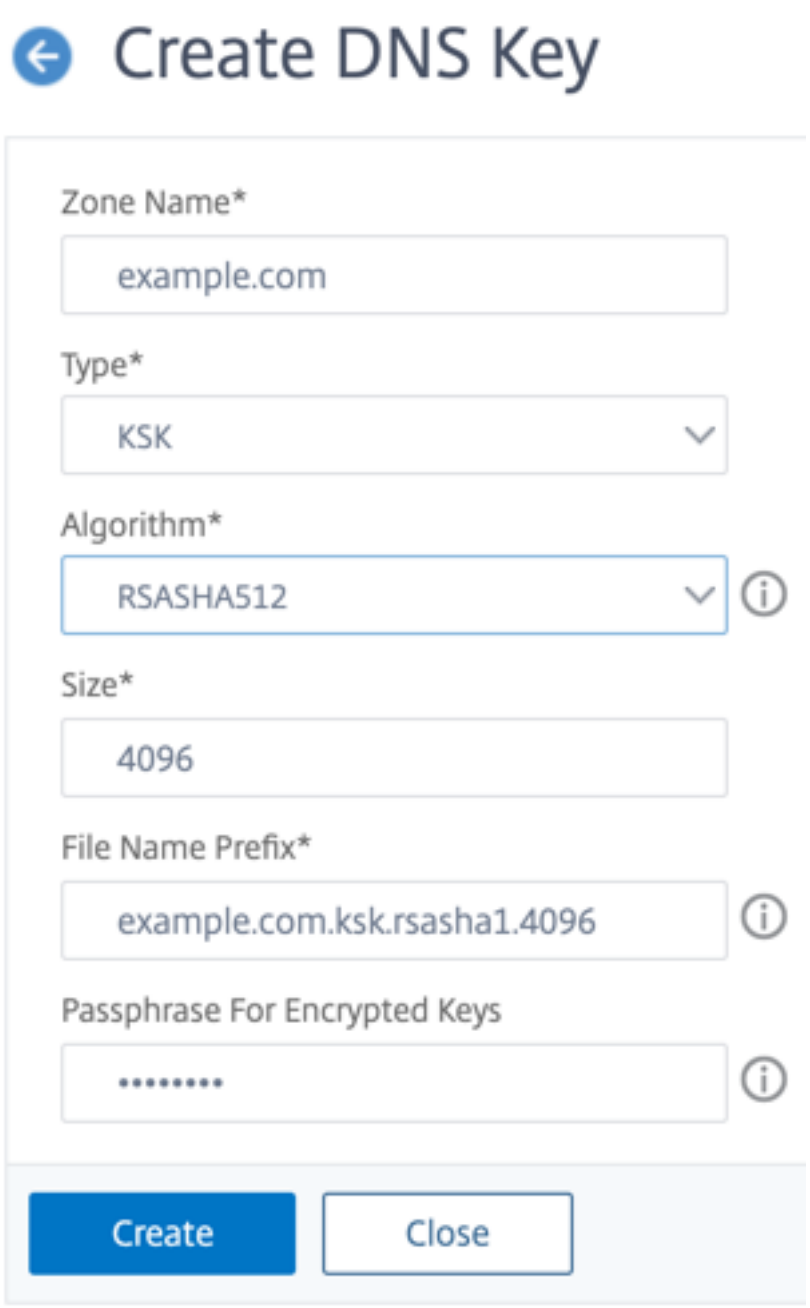
```
1 > create dns key -zoneName example.com -keyType zsk -algorithm
      RSASHA256 -keySize 1024 -fileNamePrefix example.com.zsk.rsasha1.1024
```



```
File Name: /nsconfig/dns/example.com.zsk.rsasha1.1024.key (public); /
    nsconfig/dns/example.com.zsk.rsasha1.1024.private (private); /
    nsconfig/dns/example.com.zsk.rsasha1.1024.ds (ds)
This operation may take some time, Please wait...
 Done
> create dns key -zoneName example.com -keyType ksk -algorithm
    RSASHA512 -keySize 4096 -fileNamePrefix example.com.ksk.rsasha1.4096
File Name: /nsconfig/dns/example.com.ksk.rsasha1.4096.key (public); /
    nsconfig/dns/example.com.ksk.rsasha1.4096.private (private); /
    nsconfig/dns/example.com.ksk.rsasha1.4096.ds (ds)
This operation may take some time, Please wait...
 Done
<!--NeedCopy-->
```

Erstellen Sie einen DNS-Schlüssel mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf **DNS-Schlüssel erstellen**.
3. Geben Sie Werte für die verschiedenen Parameter ein und klicken Sie auf **Erstellen**.



Hinweis: Um das Dateinamenpräfix eines vorhandenen Schlüssels zu ändern:

- Klicken Sie auf den Pfeil neben der Schaltfläche **Durchsuchen** .
- Klicken Sie entweder auf **Lokal** oder auf **Appliance** (je nachdem, ob der vorhandene Schlüssel auf Ihrem lokalen Computer oder im `/nsconfig/dns/` Verzeichnis auf der Appliance gespeichert ist)
- Navigieren Sie zum Speicherort des Schlüssels, und doppelklicken Sie dann auf den Schlüssel.
  Das Feld **Dateinamenpräfix** enthält nur das Präfix des vorhandenen Schlüssels. Ändern

Sie das Präfix entsprechend.

Veröffentlichen eines DNS-Schlüssels in einer Zone

Ein Schlüssel (Zonensignierungsschlüssel oder Schlüsselsignierschlüssel) wird in einer Zone veröffentlicht, indem der Schlüssel zur ADC-Appliance hinzugefügt wird. Ein Schlüssel muss in einer Zone veröffentlicht werden, bevor Sie die Zone signieren.

Bevor Sie einen Schlüssel in einer Zone veröffentlichen, muss der Schlüssel im Verzeichnis **/nsconfig/dns/** verfügbar sein. Wenn Sie den DNS-Schlüssel auf einem anderen Computer erstellt haben (z. B. mithilfe des Programms `bind-keygen`), stellen Sie sicher, dass der Schlüssel dem Verzeichnis `/nsconfig/dns/` hinzugefügt wird. Veröffentlichen Sie dann den Schlüssel in der Zone. Verwenden Sie die ADC-GUI, um den Schlüssel zum `/nsconfig/dns/` Verzeichnis hinzuzufügen. Oder verwenden Sie ein anderes Programm, um den Schlüssel in das Verzeichnis zu importieren, z. B. Secure FTP (SFTP).

Verwenden Sie den `add dns key` Befehl für jedes öffentlich-private Schlüsselpaar, das Sie in einer bestimmten Zone veröffentlichen möchten. Wenn Sie ein ZSK-Paar und ein KSK-Paar für eine Zone erstellt haben, verwenden Sie den `add dns key` Befehl, um zuerst eines der Schlüsselpaare in der Zone zu veröffentlichen. Wiederholen Sie den Befehl, um das andere Schlüsselpaar zu veröffentlichen. Für jeden Schlüssel, den Sie in einer Zone veröffentlichen, wird in der Zone ein DNSKEY-Ressourceneintrag erstellt.

Das Beispiel, das der Befehlssyntax folgt, veröffentlicht zuerst das Zonensignaturschlüsselpaar (das für die Zone example.com erstellt wurde) in der Zone. Das Beispiel verwendet dann den Befehl, um das Schlüsselpaar für die Signatur in der Zone zu veröffentlichen.

Veröffentlichen Sie einen Schlüssel in einer Zone mithilfe der CLI

Geben Sie an der Befehlszeile den folgenden Befehl ein, um einen Schlüssel in einer Zone zu veröffentlichen und die Konfiguration zu überprüfen:

```
1 -  add dns key <keyName> <publickey> <privatekey> [-expires <
     positive_integer> [<units>]] [-notificationPeriod <positive_integer>
      [<units>]] [-TTL <secs>]
2 -  show dns zone [<zoneName> | -type <type>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns key example.com.zsk example.com.zsk.rsasha1.1024.key example.
     com.zsk.rsasha1.1024.private
2  Done
```



```
> add dns key example.com.ksk example.com.ksk.rsasha1.4096.key example.com.ksk.rsasha1.4096.private
 Done
> show dns zone example.com
          Zone Name : example.com
          Proxy Mode : NO
          Domain Name : example.com
                  Record Types : NS SOA DNSKEY
          Domain Name : ns1.example.com
                  Record Types : A
          Domain Name : ns2.example.com
                  Record Types : A
 Done
<!--NeedCopy-->
```

Veröffentlichen Sie einen Schlüssel in einer DNS-Zone mithilfe der GUI

Navigieren Sie zu **Traffic Management > DNS > Keys**.

Hinweis: Um für den öffentlichen Schlüssel und den privaten Schlüssel einen Schlüssel hinzuzufügen, der auf Ihrem lokalen Computer gespeichert ist, klicken Sie auf den Pfeil neben der Schaltfläche **Durchsuchen**, klicken Sie auf **Lokal**, suchen Sie nach dem Speicherort des Schlüssels, und doppelklicken Sie dann auf den Schlüssel.

Einen DNS-Schlüssel konfigurieren

Sie können die Parameter eines Schlüssels konfigurieren, der in einer Zone veröffentlicht wurde. Sie können die Parameter Ablaufzeit, Benachrichtigungszeitraum und Time-to-Live (TTL) des Schlüssels ändern. Wenn Sie die Ablaufzeit eines Schlüssels ändern, signiert die Appliance automatisch erneut alle Ressourceneinträge in der Zone mit dem Schlüssel. Die erneute Signierung erfolgt, wenn die Zone mit dem bestimmten Schlüssel signiert ist.

Konfigurieren Sie einen Schlüssel mithilfe der CLI

Geben Sie an der Befehlszeile den folgenden Befehl ein, um einen Schlüssel zu konfigurieren und die Konfiguration zu überprüfen:

```
-  set dns key <keyName> [-expires <positive_integer> [<units>]] [-notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
-  show dns key [<keyName>]
<!--NeedCopy-->
```

Beispiel:


```
> set dns key example.com.ksk -expires 30 DAYS -notificationPeriod 3
   DAYS -TTL 3600
 Done
> show dns key example.com.ksk
1)      Key Name: example.com.ksk
        Expires: 30 DAYS        Notification: 3 DAYS    TTL: 3600
        Public Key File: example.com.ksk.rsasha1.4096.key
        Private Key File: example.com.ksk.rsasha1.4096.private
 Done
<!--NeedCopy-->
```

Konfigurieren Sie einen Schlüssel mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > DNS > Keys**.
2. Klicken Sie im Detailbereich auf den Schlüssel, den Sie konfigurieren möchten, und klicken Sie dann auf Öffnen.
3. Ändern Sie im Dialogfeld DNS-Schlüssel konfigurieren die Werte der folgenden Parameter wie gezeigt:
   - Läuft ab — Läuft ab
   - Meldezeitraum — notificationPeriod
   - TTL—TTL
4. Klicken Sie auf OK.

DNS-Zone signieren und abmelden

Um eine DNS-Zone zu sichern, müssen Sie die Zone mit den Schlüsseln signieren, die in der Zone veröffentlicht wurden. Wenn Sie eine Zone signieren, erstellt NetScaler für jeden Besitzernamen einen Next Secure (NSEC) -Ressourceneintrag. Anschließend verwendet es den Key Signing Key, um den DNSKEY-Ressourcendatensatz zu signieren. Schließlich verwendet es den ZSK, um alle Ressourcendatensätze in der Zone zu signieren, einschließlich der DNSKEY-Ressourcendatensätze und der NSEC-Ressourcendatensätze. Jeder Signiervorgang führt zu einer Signatur für die Ressourcendatensätze in der Zone. Die Signatur wird in einem neuen Ressourcendatensatz, dem RRSIG-Ressourcendatensatz, erfasst.

Nachdem Sie eine Zone signiert haben, speichern Sie die Konfiguration.

Signieren Sie eine Zone mit der CLI

Geben Sie an der Befehlszeile den folgenden Befehl ein, um eine Zone zu signieren und die Konfiguration zu überprüfen:

```
-  sign dns zone <zoneName> [-keyName <string> ...]
-  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
-  save config
<!--NeedCopy-->
```

Beispiel:

```
> sign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY RRSIG NSEC
         Domain Name : ns1.example.com
                 Record Types : A RRSIG NSEC
         Domain Name : ns2.example.com
                 Record Types : A RRSIG
         Domain Name : ns2.example.com
                 Record Types : RRSIG NSEC
Done
> save config
 Done
<!--NeedCopy-->
```

Die Signierung einer Zone mithilfe der CLI aufheben

Geben Sie an der Befehlszeile den folgenden Befehl ein, um die Signierung einer Zone aufzuheben und die Konfiguration zu überprüfen:

```
-  unsign dns zone <zoneName> [-keyName <string> ...]
-  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
<!--NeedCopy-->
```

Beispiel:

```
> unsign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
```



```
5           Proxy Mode : NO
6           Domain Name : example.com
7                   Record Types : NS SOA DNSKEY
8           Domain Name : ns1.example.com
9                   Record Types : A
10          Domain Name : ns2.example.com
11                  Record Types : A
12   Done
13  <!--NeedCopy-->
```

Signieren oder Aufheben der Signierung einer Zone mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > DNS > Zonen**.
2. Klicken Sie im Detailbereich auf die Zone, die Sie signieren möchten, und klicken Sie dann auf Anmelden/Abmelden.
3. Führen Sie im Dialogfeld DNS-Zone signieren/unsign (DNS-Zone signieren/unsign sign) einen der folgenden Schritte aus:
   - Um die Zone zu signieren, aktivieren Sie die Kontrollkästchen für die Schlüssel (Zonensignierungsschlüssel und Schlüsselsignierschlüssel), mit denen Sie die Zone signieren möchten.
     Sie können die Zone mit mehr als einem Zonensignierschlüssel oder einem Schlüsselsignierschlüsselpaar signieren.
   - Um die Zone zu signieren, deaktivieren Sie die Kontrollkästchen für die Schlüssel (Zonensignierungsschlüssel und Schlüsselsignierungsschlüssel), mit denen Sie die Zone entsignieren möchten.
     Sie können die Signierung der Zone mit mehr als einem Zonensignierungsschlüssel oder einem Schlüsselsignierungsschlüsselpaar aufheben.
4. Klicken Sie auf OK.

Zeigen Sie die NSEC-Datensätze für einen bestimmten Datensatz in einer Zone an

Sie können die NSEC-Datensätze einsehen, die der NetScaler automatisch für jeden Besitzernamen in der Zone erstellt.

Zeigen Sie den NSEC-Datensatz für einen bestimmten Datensatz in einer Zone mit der CLI an

Geben Sie in der Befehlszeile den folgenden Befehl ein, um den NSEC-Datensatz für einen bestimmten Datensatz in einer Zone anzuzeigen:

```
show dns nsecRec [<hostName> | -type (ADNS | PROXY | ALL)]
```

Beispiel:


```
> show dns nsecRec example.com
1)      Domain Name : example.com
        Next Nsec Name: ns1.example.com
        Record Types : NS SOA DNSKEY RRSIG NSEC
 Done
<!--NeedCopy-->
```

Zeigen Sie den NSEC-Datensatz für einen bestimmten Datensatz in einer Zone mithilfe der GUI an

1. Navigieren Sie zu **Traffic Management > DNS > Records > Next Secure Records**.
2. Klicken Sie im Detailbereich auf den Namen des Datensatzes, für den Sie den NSEC-Datensatz anzeigen möchten. Der NSEC-Datensatz für den ausgewählten Datensatz wird im Bereich Details angezeigt.

Entfernen Sie einen DNS-Schlüssel

Entfernen Sie einen Schlüssel aus der Zone, in der er veröffentlicht wurde, wenn der Schlüssel abgelaufen ist oder wenn der Schlüssel kompromittiert wurde. Wenn Sie einen Schlüssel aus der Zone entfernen, wird die Zone automatisch mit dem Schlüssel unsigniert. Das Entfernen des Schlüssels mit diesem Befehl entfernt nicht die Schlüsseldateien im Verzeichnis /nsconfig/dns/. Wenn die Schlüsseldateien nicht mehr benötigt werden, müssen sie explizit aus dem Verzeichnis entfernt werden.

Entfernen Sie mithilfe der CLI einen Schlüssel aus dem NetScaler

Geben Sie in der Befehlszeile den folgenden Befehl ein, um einen Schlüssel zu entfernen und die Konfiguration zu überprüfen:

```
-  rm dns key <keyName>
-  show dns key <keyName>
<!--NeedCopy-->
```

Beispiel:

```
> rm dns key example.com.zsk
 Done
> show dns key example.com.zsk
ERROR: No such resource [keyName, example.com.zsk]

<!--NeedCopy-->
```


Entfernen Sie mithilfe der GUI einen Schlüssel aus dem NetScaler

1. Navigieren Sie zu **Traffic Management > DNS > Keys**.
2. Klicken Sie im Detailbereich auf den Namen des Schlüssels, den Sie aus dem ADC entfernen möchten, und klicken Sie dann auf Entfernen.

Konfigurieren von DNSSEC, wenn NetScaler für eine Zone autoritativ ist

May 11, 2023

Wenn der NetScaler für eine bestimmte Zone autorisierend ist, werden alle Ressourceneinträge in der Zone auf dem ADC konfiguriert. Um die autoritative Zone zu signieren, müssen Sie die Zonensignierung und die Schlüsselsignierschlüssel für die Zone erstellen, die Schlüssel zum ADC hinzufügen und dann die Zone signieren. Weitere Informationen:

- DNS-Schlüssel für eine Zone erstellen
- Veröffentlichen eines DNS-Schlüssels in einer Zone
- Unterschreiben und unterschreiben Sie eine DNS-Zone.

Wenn auf dem ADC konfigurierte GSLB-Domänen zur Zone gehören, die signiert wird, werden die GSLB-Domainnamen zusammen mit den anderen Datensätzen, die zur Zone gehören, signiert.

Nachdem Sie eine Zone signiert haben, enthalten die Antworten auf Anfragen von DNSSEC-fähigen Clients die RRSIG-Ressourceneinträge zusammen mit den angeforderten Ressourceneinträgen. DNSSEC muss auf dem ADC aktiviert sein. Weitere Informationen zum Aktivieren von DNSSEC finden Sie unter Aktivieren und Deaktivieren von DNSSEC.

Nachdem Sie DNSSEC für die autorisierende Zone konfiguriert haben, müssen Sie die NetScaler Konfiguration speichern.

Konfigurieren von DNSSEC für eine Zone, für die NetScaler ein DNS-Proxyserver ist

May 11, 2023

Das Verfahren zum Signieren einer Zone, für die der NetScaler als DNS-Proxyserver konfiguriert ist, hängt davon ab, ob der ADC eine Teilmenge der Zoneninformationen besitzt, die den Back-End-Nameservern gehören. Ist dies der Fall, wird die Konfiguration als Konfiguration mit teilweisem Zonenbesitz betrachtet. Wenn der ADC keine Teilmenge der Zoneninformationen besitzt, wird die NetScaler-Konfiguration zur Verwaltung der Backend-Server als zonenlose DNS-Proxy-Serverkonfiguration betrachtet. Die grundlegenden DNSSEC-Konfigurationsaufgaben für beide

NetScaler-Konfigurationen sind dieselben. Das Signieren der Teilzone auf dem NetScaler erfordert jedoch einige zusätzliche Konfigurationsschritte.

Hinweis: Die Begriffe zonenlose Proxyserverkonfiguration und Teilzone werden nur im Zusammenhang mit der NetScaler-Appliance verwendet.

Wichtig: Bei der Konfiguration im Proxymodus führt der ADC keine Signaturüberprüfung für DNSSEC-Antworten durch, bevor der Cache aktualisiert wird.

Wenn Sie den ADC als DNS-Proxy für den Lastausgleich von DNSSEC-fähigen Resolvern (Servern) konfigurieren, müssen Sie bei der Konfiguration des virtuellen DNS-Servers die Option Rekursion Available aktivieren. Wenn eine DNSSEC-Anfrage eingeht, bei der das CD-Bit Checking Disabled (CD) gesetzt ist, wird die Anfrage an den Server weitergeleitet, wobei das CD-Bit beibehalten wird. Die Antwort vom Server wird nicht zwischengespeichert.

DNSSEC für eine zonenlose DNS-Proxyserverkonfiguration konfigurieren

Für eine zonenlose DNS-Proxyserverkonfiguration muss die Zonensignierung auf den Back-End-Nameservern durchgeführt werden. Auf dem NetScaler konfigurieren Sie den ADC als DNS-Proxyserver für die Zone. Erstellen Sie einen virtuellen Lastausgleichsserver mit dem Protokolltyp DNS. Konfigurieren Sie Dienste auf dem ADC so, dass sie die Nameserver repräsentieren. Binden Sie dann die Dienste an den virtuellen Lastausgleichsserver. Weitere Informationen zu diesen Konfigurationsaufgaben finden Sie unter Konfigurieren des NetScaler als DNS-Proxyserver.

Wenn ein Client dem ADC eine DNS-Anforderung mit dem DNSSEC OK (DO) -Bit sendet, überprüft der ADC seinen Cache auf die angeforderten Informationen. Wenn die Ressourceneinträge in seinem Cache nicht verfügbar sind, leitet der ADC die Anfrage an einen der DNS-Nameserver weiter. Anschließend leitet es die Antwort vom Nameserver an den Client weiter. Außerdem speichert der ADC die RRSIG-Ressourceneinträge zusammen mit der Antwort vom Nameserver im Cache. Nachfolgende Anfragen von DNSSEC-fähigen Clients werden vom Cache (einschließlich der RRSIG-Ressourceneinträge) gemäß dem Time-to-Live-Parameter (TTL) bedient. Wenn ein Client eine DNS-Anfrage sendet, ohne das DO-Bit zu setzen, antwortet der ADC nur mit den angeforderten Ressourceneinträgen. Es enthält nicht die RRSIG-Ressourceneinträge, die für DNSSEC spezifisch sind.

DNSSEC für eine Konfiguration mit teilweisem Zonenbesitz konfigurieren

In einigen ADC-Konfigurationen kann, obwohl die Autorität für eine Zone bei den Back-End-Nameservern liegt, eine Teilmenge der zu der Zone gehörenden Ressourceneinträge auf dem ADC konfiguriert werden. Der ADC besitzt nur diese Teilmenge von Datensätzen (oder ist für sie maßgebend). Eine solche Teilmenge von Datensätzen kann als *Teilzone* auf dem ADC betrachtet werden. Der ADC besitzt die Teilzone. Alle anderen Datensätze gehören den Back-End-Nameservern.

Eine typische partielle Zonenkonfiguration auf dem NetScaler wird angezeigt, wenn:

- Global Server Load Balancing (GSLB) -Domänen sind auf dem ADC konfiguriert
- Die GSLB-Domains sind Teil einer Zone, für die die Back-End-Nameserver maßgebend sind.

Das Signieren einer Zone, die nur eine Teilzone auf dem ADC umfasst, beinhaltet:

- Einbeziehen der partiellen Zoneninformationen in die Zonendateien des Back-End-Nameservers
- Signieren der Zone auf den Back-End-Nameservern
- Signieren der Teilzone auf dem ADC.

Derselbe Schlüsselsatz muss verwendet werden, um die Zone auf den Nameservern und die Teilzone auf dem ADC zu signieren.

Signieren Sie die Zone auf den Back-End-Nameservern

1. Nehmen Sie die Ressourceneinträge, die in der Teilzone enthalten sind, in die Zonendateien der Nameserver auf.
2. Erstellen Sie Schlüssel und verwenden Sie die Schlüssel, um die Zone auf den Back-End-Nameservern zu signieren.

Signieren Sie die Teilzone auf dem NetScaler

1. Erstellen Sie eine Zone mit dem Namen der Zone, die den Back-End-Nameservern gehört. Stellen Sie bei der Konfiguration der Teilzone den Parameter ProxyMode auf YES ein. Diese Zone ist die Teilzone, die die Ressourceneinträge enthält, die dem ADC gehören.

   Wenn der Name der Zone, die auf den Back-End-Nameservern konfiguriert ist, beispielsweise example.com lautet, müssen Sie auf dem ADC eine Zone mit dem Namen example.com erstellen. Setzen Sie den ProxyMode-Parameter auf YES. Weitere Informationen zum Hinzufügen einer Zone finden Sie unter Konfigurieren einer DNS-Zone.

   > **Hinweis**
   >
   > Fügen Sie keine SOA- und NS-Einträge für die Zone hinzu. Diese Datensätze müssen auf dem ADC für eine Zone vorhanden sein, für die der ADC maßgebend ist.

2. Importieren Sie die Schlüssel (von einem der Back-End-Nameserver) in den ADC und fügen Sie sie dann dem /nsconfig/dns/ -Verzeichnis hinzu. Weitere Informationen darüber, wie Sie einen Schlüssel importieren und zum ADC hinzufügen können, finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.

3. Signieren Sie die Teilzone mit den importierten Schlüsseln. Wenn Sie die Teilzone mit den Schlüsseln signieren, generiert der ADC RRSIG- und NSEC-Datensätze für die Ressourceneintragsgruppen bzw. einzelne Ressourceneinträge in der Teilzone. Weitere Informationen zum Signieren einer Zone finden Sie unter Signieren und Aufheben einer DNS-Zone.

DNSSEC für Domainnamen mit globalem Serverlastenausgleich (GSLB) konfigurieren

May 11, 2023

Wenn GSLB auf dem NetScaler konfiguriert ist und der ADC für die Zone, zu der die GSLB-Domänennamen gehören, autorisierend ist, werden alle GLSB-Domänennamen signiert, wenn die Zone signiert wird. Weitere Informationen zum Signieren einer Zone, für die der ADC autoritativ ist, finden Sie unter Konfigurieren von DNSSEC, wenn die NetScaler Appliance für eine Zone autoritativ ist.

Wenn die GSLB-Domains zu einer Zone gehören, für die die Back-End-Nameserver autorisierend sind, müssen Sie:

- Signieren Sie zuerst die Zone auf den Nameservern.
- Unterschreiben Sie dann die Teilzone auf dem ADC, um die DNSSEC-Konfiguration für die Zone abzuschließen.

Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Konfiguration des Teilzonenbesitzes.

Wartung der Zonen

May 11, 2023

Aus Sicht von DNSSEC beinhaltet die Zonenwartung die Übertragung von Zone Signing Keys und Key Signing Keys, wenn der Schlüsselablauf unmittelbar bevorsteht. Diese Zonenverwaltungsaufgaben müssen manuell ausgeführt werden. Die Zone wird automatisch neu signiert und erfordert keinen manuellen Eingriff.

Eine aktualisierte Zone erneut signieren

Wenn eine Zone aktualisiert wird (einen Datensatz hinzufügen oder einen vorhandenen Datensatz ändern), signiert die Appliance den neuen (oder geänderten) Datensatz automatisch erneut. Wenn eine Zone mehrere Zonensignierschlüssel enthält, signiert die Appliance den neuen (oder geänderten) Datensatz erneut mit dem Schlüssel, der zum Signieren der Zone verwendet wurde.

Übertragen Sie DNSSEC-Schlüssel

Hinweis: Manuelles Übertragen der DNSSEC-Schlüssel (KSK, ZSK), bevor sie ablaufen.

Auf dem NetScaler können Sie die Methoden Prepublish und Double Signature verwenden, um einen Rollover des Zone Signing Key und des Key Signing Key durchzuführen. Weitere Informationen zu diesen beiden Rollover-Methoden finden Sie in RFC 4641, „DNSSEC Operational Practices“.

In den folgenden Themen werden Befehle auf dem ADC den Schritten der in RFC 4641 beschriebenen Rollover-Verfahren zugeordnet.

Die Schlüsselablaufbenachrichtigung wird über ein SNMP-Trap namens dnskeyExpiry gesendet. Drei MIB-Variablen, DNSKeyName, DNSKeyTimeToExpire und DNSKeyUnitsOfExpiry werden zusammen mit dem SNMP-Trap DNSKeyExpiry gesendet. Weitere Informationen finden Sie in der *NetScaler SNMP OID Reference unter NetScaler 12.0 SNMP OID Reference.*

Schlüsselrollover für die Vorveröffentlichung

RFC 4641, „DNSSEC Operational Practices“, definiert vier Stufen für die Rollover-Methode vor dem Veröffentlichen von Schlüsseln: erster, neuer DNSKEY, neue RRSIGs und DNSKEY-Entfernung. Jede Phase ist mit einer Reihe von Aufgaben verknüpft, die Sie auf dem ADC ausführen müssen. Im Folgenden finden Sie die Beschreibungen der einzelnen Phasen und der Aufgaben, die Sie ausführen müssen. Das hier beschriebene Rollover-Verfahren kann sowohl für Key Signing Keys als auch für Zone Signing Keys verwendet werden.

- **Stufe 1: Anfänglich.** Die Zone enthält nur die Schlüsselsätze, mit denen die Zone aktuell signiert wurde. Der Status der Zone in der Anfangsphase ist der Zustand der Zone kurz bevor Sie mit dem Key-Rollover-Vorgang beginnen.

  Beispiel:

  Betrachten Sie den Schlüssel example.com.zsk1, mit dem die Zone example.com signiert ist. Die Zone enthält nur die RRSigs, die durch den Schlüssel example.com.zsk1 generiert wurden und dessen Ablauf fällig ist. Der Key Signing Key ist example.com.ksk1.

- **Stufe 2: Neuer DNSKEY.** Ein neuer Schlüssel wird erstellt und in der Zone veröffentlicht. Das heißt, der Schlüssel wird dem ADC hinzugefügt, aber die Zone wird erst mit dem neuen Schlüssel signiert, wenn die Pre-Roll-Phase abgeschlossen ist. In dieser Phase enthält die Zone den alten Schlüssel, den neuen Schlüssel und die vom alten Schlüssel generierten RRSIGs. Wenn der neue Schlüssel für die gesamte Dauer der Pre-Roll-Phase veröffentlicht wird, erhält der DNSKEY-Ressourceneintrag, der der neuen Schlüsselzeit entspricht, bis er an die sekundären Nameserver weitergegeben wird.

  Beispiel:

  Der Zone example.com wird ein neuer Schlüssel example.com.zsk2 hinzugefügt. Die Zone wird erst mit example.com.zsk2 signiert, wenn die Pre-Roll-Phase abgeschlossen ist. Die Zone example.com enthält DNSKEY-Ressourceneinträge sowohl für example.com.zsk1 als auch für example.com.zsk2.

NetScaler-Befehle:

Führen Sie die folgenden Aufgaben auf dem ADC aus:

- Erstellen Sie mit dem Befehl `create dns key` einen DNS-Schlüssel.

  Weitere Informationen zum Erstellen eines DNS-Schlüssels, einschließlich eines Beispiels, finden Sie unter Erstellen von DNS-Schlüsseln für eine Zone.

- Veröffentlichen Sie den neuen DNS-Schlüssel in der Zone mithilfe des`add dns key` Befehls.

  Weitere Informationen zum Veröffentlichen des Schlüssels in der Zone, einschließlich eines Beispiels, finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.

- **Stufe 3: Neue RRSIGs.** Die Zone ist mit dem neuen DNS-Schlüssel signiert und dann mit dem alten DNS-Schlüssel unsigniert. Der alte DNS-Schlüssel wird nicht aus der Zone entfernt und bleibt veröffentlicht, bis die vom alten Schlüssel generierten RRSIGs ablaufen.

  Beispiel:

  Die Zone ist mit example.com.zsk2 signiert und dann mit example.com.zsk1 unsigniert. Die Zone veröffentlicht weiterhin example.com.zsk1, bis die von example.com.zsk1 generierten RRSigs ablaufen.

  NetScaler-Befehle:

  Führen Sie die folgenden Aufgaben auf dem ADC aus:

  - Signieren Sie die Zone mit dem neuen DNS-Schlüssel, indem Sie den `sign dns zone` Befehl verwenden.
  - Heben Sie die Signatur der Zone mit dem alten DNS-Schlüssel mithilfe des`unsign dns zone` Befehls auf.

  Weitere Informationen zum Signieren und Aufheben einer Zone, einschließlich Beispielen, finden Sie unter Signieren und Aufheben der Unterzeichnung einer DNS-Zone.

- **Stufe 4: DNSKEY Entfernung.** Wenn die vom alten DNS-Schlüssel generierten RRSIGs ablaufen, wird der alte DNS-Schlüssel aus der Zone entfernt.

  Beispiel:

  Der alte DNS-Schlüssel example.com.zsk1 wird aus der Zone example.com entfernt.

  NetScaler-Befehle

  Auf dem ADC entfernen Sie den alten DNS-Schlüssel mit dem Befehl `rm dns key`. Weitere Informationen zum Entfernen eines Schlüssels aus einer Zone, einschließlich eines Beispiels, finden Sie unter Entfernen eines DNS-Schlüssels.

Doppelte Signaturschlüssel Rollover

RFC 4641, „DNSSEC Operational Practices“, definiert drei Stufen für die Schlüsselübergabe mit doppelter Signatur: erster, neuer DNSKEY und Entfernung von DNSKEY. Jede Phase ist mit einer Reihe von Aufgaben verknüpft, die Sie auf dem ADC ausführen müssen. Im Folgenden finden Sie die Beschreibungen der einzelnen Phasen und der Aufgaben, die Sie ausführen müssen. Das hier beschriebene Rollover-Verfahren kann sowohl für Key Signing Keys als auch für Zone Signing Keys verwendet werden.

- **Stufe 1: Anfänglich.** Die Zone enthält nur die Schlüsselsätze, mit denen die Zone aktuell signiert wurde. Der Status der Zone in der Anfangsphase ist der Zustand der Zone kurz bevor Sie mit dem Key-Rollover-Vorgang beginnen.

  Beispiel:

  Betrachten Sie den Schlüssel example.com.zsk1, mit dem die Zone example.com signiert ist. Die Zone enthält nur die RRSigs, die durch den Schlüssel example.com.zsk1 generiert wurden und dessen Ablauf fällig ist. Der Key Signing Key ist example.com.ksk1.

- **Stufe 2: Neuer DNSKEY.** Der neue Schlüssel wird in der Zone veröffentlicht und die Zone wird mit dem neuen Schlüssel signiert. Die Zone enthält die RRSigs, die durch den alten und den neuen Schlüssel generiert werden. Die Mindestdauer, für die die Zone beide Gruppen von RRSIGs enthalten muss, ist die Zeit, die benötigt wird, bis alle RRSIGs ablaufen.

  Beispiel:

  Der Zone example.com wird ein neuer Schlüssel example.com.zsk2 hinzugefügt. Die Zone ist mit example.com.zsk2 signiert. Die Zone example.com enthält jetzt die RRSigs, die aus beiden Schlüsseln generiert wurden.

  NetScaler-Befehle

  Führen Sie die folgenden Aufgaben auf dem ADC aus:

  - Erstellen Sie mit dem Befehl `create dns key` einen DNS-Schlüssel.

    Weitere Informationen zum Erstellen eines DNS-Schlüssels, einschließlich eines Beispiels, finden Sie unter Erstellen von DNS-Schlüsseln für eine Zone.

  - Veröffentlichen Sie den neuen Schlüssel in der Zone mithilfe des`add dns key` Befehls.

    Weitere Informationen zum Veröffentlichen des Schlüssels in der Zone, einschließlich eines Beispiels, finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.

  - Signieren Sie die Zone mit dem neuen Schlüssel, indem Sie den`sign dns zone` Befehl verwenden.

    Weitere Informationen zum Signieren einer Zone, einschließlich Beispielen, finden Sie unter Signieren und Aufheben einer DNS-Zone.

- **Stufe 3: DNSKEY Entfernung.** Wenn die vom alten DNS-Schlüssel generierten RRSIGs ablaufen, wird der alte DNS-Schlüssel aus der Zone entfernt.

  Beispiel:

  Der alte DNS-Schlüssel example.com.zsk1 wird aus der Zone example.com entfernt.

  NetScaler-Befehle:

  Auf dem ADC entfernen Sie den alten DNS-Schlüssel mit dem Befehl `rm dns key`.

  Weitere Informationen zum Entfernen eines Schlüssels aus einer Zone, einschließlich eines Beispiels, finden Sie unter Entfernen eines DNS-Schlüssels.

Offload von DNSSEC-Vorgängen an NetScaler

May 11, 2023

Für DNS-Zonen, für die Ihre DNS-Server autorisierend sind, können DNSSEC-Operationen auf die ADC-Appliance ausgelagert werden. In einer DNSSEC-Offloading-Bereitstellung sendet ein DNS-Server unsignierte Antworten. Der ADC signiert die Antwort dynamisch, bevor er sie an den Client weiterleitet. Der ADC speichert auch die signierte Antwort im Cache. Abgesehen von der Reduzierung der Belastung der DNS-Server bietet Ihnen die Auslagerung von DNSSEC-Operationen auf den ADC die folgenden Vorteile:

- Sie können Datensätze signieren, die die DNS-Server programmgesteuert generieren. Solche Datensätze können nicht durch routinemäßige Zonensigniervorgänge signiert werden, die auf den DNS-Servern ausgeführt werden.
- Sie können signierte Antworten an Kunden senden, auch wenn Sie DNSSEC auf Ihren Servern nicht implementiert haben.

Zum Einrichten der DNSSEC-Abladung müssen Sie einen virtuellen DNS-Lastausgleichsserver konfigurieren, Dienste konfigurieren, die die DNS-Server darstellen, und dann die Dienste an den virtuellen Server binden. Informationen zum Konfigurieren eines virtuellen DNS-Lastenausgleichsservers, zum Konfigurieren von Diensten und zum Binden der Dienste an den virtuellen Server finden Sie unter Konfigurieren einer DNS-Zone.

Erstellen Sie eine Zonen-Entity auf dem ADC für jede DNS-Zone, deren DNSSEC-Vorgänge Sie auslagern möchten. Für jede DNS-Zone müssen Sie die Parameter Proxymodus und DNSSEC-Offload aktivieren. Sie können optional die Generierung von NSEC-Datensätzen für eine ausgelastete Zone konfigurieren. Folgen Sie den Anweisungen in diesem Thema, um eine DNS-Zonenentität für DNSSEC-Offloading zu erstellen.

Um die Konfiguration abzuschließen, müssen Sie DNS-Schlüssel für die Zone generieren, die Schlüssel zur Zone hinzufügen und dann die Zone mit den Schlüsseln signieren. Dieser Prozess ist der gleiche

wie für normale DNSSEC. Informationen zum Erstellen von Schlüsseln, zum Hinzufügen von Schlüsseln zu einer Zone und zum Signieren der Zone finden Sie unter Sicherheitserweiterungen für Domänennamen.

Nachdem Sie DNS-Abladung konfiguriert haben, müssen Sie den DNS-Cache auf dem NetScaler leeren. Durch das Leeren des DNS-Cache wird sichergestellt, dass alle nicht signierten Datensätze im Cache entfernt und dann durch signierte Datensätze ersetzt werden. Informationen zum Löschen des DNS-Caches finden Sie unter Flush DNS-Datensätze.

Aktivieren der DNSSEC-Abladung für eine Zone mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um das DNSSEC-Offloading für eine Zone zu aktivieren und die Konfiguration zu überprüfen:

```
1 -  add dns zone <zoneName> -proxyMode YES -dnssecOffload ENABLED [-nsec
     ( ENABLED | DISABLED )
2 -  show dns zone
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns zone example.com -proxyMode YES -dnssecOffload ENABLED nsec
    ENABLED
2  Done
3 > show dns zone example.com
4      Zone Name : example.com
5      Proxy Mode : YES
6      DNSSEC Offload: ENABLED    NSEC: ENABLED
7  Done
8 <!--NeedCopy-->
```

Aktivieren Sie DNSSEC-Offloading für eine Zone mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > DNS > Zonen**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Zone auf dem NetScaler zu erstellen, klicken Sie auf Hinzufügen.
   - Doppelklicken Sie auf die Zone, um DNSSEC-Offloading für eine bestehende Zone zu konfigurieren.
3. Aktivieren Sie im Dialogfeld DNS-Zone erstellen oder DNS-Zone konfigurieren die Kontrollkästchen Proxymodus und DNSSEC-Offload.
4. Wenn der NetScaler NSEC-Datensätze für die Zone generieren soll, aktivieren Sie optional das Kontrollkästchen NSEC.

Unterstützung von Admin-Partitionen für DNSSEC

May 11, 2023

In einer partitionierten NetScaler-Appliance werden die generierten DNS-Schlüssel an den folgenden Speicherorten gespeichert:

- Standardpartition: /nsconfig/dns/
- Nichtstandardpartition: /nsconfig/partitions/<partitionname>/dns/

Sie können dem DNS-Schlüssel jetzt ein Passwort hinzufügen. Um dem DNS-Schlüssel ein Kennwort hinzuzufügen, müssen Sie zuerst das Kennwort im Befehl `create dns key` hinzufügen. Geben Sie dann dasselbe Kennwort in den Befehl `add dns key` ein, wenn Sie der ADC-Appliance den DNS-Schlüssel hinzufügen. Zum Beispiel:

```
create dns key -zoneName com -keytype ksK -algorithm rsASHA1 -keysize 4096
- fileNamePrefix com.ksk.rsasha1.4096 -password 1jsfd3Wa

add dns key com.zsk.4096 /nsconfig/dns/com.zsk.rsasha1.4096.private -
password 1jsfd3Wa
```

Hinweis:

- In einer partitionierten Standardumgebung werden die Schlüssel vom Standardspeicherort/nsconfig/dns/ gelesen. Wenn die Schlüssel jedoch an einem anderen Ort gespeichert sind, muss der Pfadname im `add dns key -private` Befehl angegeben werden. Beispiel: `add dns key -private <path name>`.
- Für eine nicht standardmäßige partitionierte Umgebung werden die Schlüssel vom Standardspeicherort gelesen `/nsconfig/partitions/<partitionname>/dns/`.

Unterstützung von Wildcard-DNS-Domänen

May 11, 2023

Wildcard-DNS-Domains werden verwendet, um Anfragen für nicht existierende Domains und Subdomains zu bearbeiten. Verwenden Sie in einer Zone Platzhalterdomänen, um Abfragen für alle nicht existierenden Domänen oder Subdomänen an einen bestimmten Server umzuleiten, anstatt für jede Domäne einen separaten Resource Record (RR) zu erstellen. Am häufigsten wird eine Platzhalter-DNS-Domäne verwendet, um eine Zone zu erstellen, mit der E-Mails aus dem Internet an ein anderes Mailsystem weitergeleitet werden können.

In der DNS-Auflösung unterstützen Wildcard-RRs die Wildcard-Domain. Die Platzhalter-RRs werden verwendet, um die Antworten auf Abfragen nach einem nicht existierenden Domainnamen zu syn-

thetisieren. Wenn Sie beispielsweise eine Anfrage gestellt haben `http://image.example.com`und die Subdomain „image“ nicht existiert, werden Sie möglicherweise zu example.com umgeleitet.

Ein Platzhalterdatensatz hat ein Sternchen (*) als Bezeichnung eines Domainnamens ganz links. Zum Beispiel `*.example.com`. Ein Sternchen an einer anderen Stelle im Domainnamen steht für einen Wildcard-DNS-Eintrag. **new**`.*.example.com` Ist beispielsweise kein gültiger Wildcard-DNS-Eintrag.

> **Hinweis**
>
> - Eine Wildcard-Domäne wird nur unterstützt, wenn die NetScaler-Appliance für die Zone autorisierend ist und als ADNS- oder DNS-Proxyserver konfiguriert ist.
> - Die Wildcard-Domain wird für NS- und SOA-Einträge nicht unterstützt.
> - Die Wildcard-Domain kann nicht angewendet werden, wenn sich die Abfrage in einer anderen Zone befindet.
> - Eine Wildcard-Domain kann nicht angewendet werden, wenn bekannt ist, dass der QNAME oder ein Name zwischen der Wildcard-Domain und dem QNAME existiert.

Beispiel-Konfiguration

```
add dns soaRec example.com -originServer n1.example.com -contact admin.
   example.com

add dns nsRec example.com n1.example.com

add dns nsRec example.com n2.example.com

add dns zone example.com  -proxyMode no

add dns addrec www.example.com 2.2.2.2

add dns addrec *.example.com 10.10.10.10

add dns addrec *.example.com 10.10.10.11

add dns aaaarec *.example.com 2001::1
<!--NeedCopy-->
```

In dem Beispiel wird ein Platzhalterdomänenname für einen A- und AAAA-Datensatz hinzugefügt.

Wenn eine Abfrage für einen Domainnamen eingeht, der in der Zone vorhanden ist, antwortet die NetScaler-Appliance mit der entsprechenden Antwort. Zum Beispiel für `www.example.com`, die Appliance antwortet im Beispiel mit 2.2.2.2.

Für einen nicht existierenden Domainnamen, der einem Platzhaltertyp entspricht, wird eine synthetisierte Antwort geliefert.

Im Beispiel antwortet die NetScaler-Appliance mit 10.10.10.10 und 10.10.10.11 für einen Domainnamen nonexist.example.com oder xyz.example.com.

Die Wildcard-Synthese ist für einen Domainnamen, der in der Zone existiert, nicht anwendbar.

Beispielsweise synthetisiert die NetScaler-Appliance für die Abfrage `www.example.com` und den Typ AAAA nicht mit Platzhaltern, da dies beim Typ A der Fall `www.example.com` ist. In dem Beispiel antwortet die NetScaler-Appliance mit einer NODATA-Antwort.

Auf eine Abfrage, sagen wir abc.example.com und geben Sie AAAA ein, antwortet die NetScaler-Appliance mit einer synthetisierten Antwort. Zum Beispiel für `www.example.com`, die Appliance antwortet im Beispiel mit 2001: :1.

Vermeiden von DNS-DDoS-Angriffe

May 11, 2023

DNS-Server sind eine der kritischsten Komponenten eines Netzwerks und müssen vor Angriffen geschützt werden. Eine der grundlegendsten Arten von DNS-Angriffen ist der DDoS-Angriff. Angriffe dieser Art nehmen zu und können zerstörerisch sein. Sie können Folgendes tun, um DDoS-Angriffe abzuwehren:

- Negative Aufzeichnungen löschen.
- Beschränken Sie die Gültigkeitsdauer (TTL) negativer Aufzeichnungen.
- Bewahren Sie NetScaler-Speicher auf, indem Sie den vom DNS-Cache verbrauchten Speicher einschränken.
- Bewahren Sie DNS-Einträge im Cache auf.
- Aktivieren Sie den DNS-Cache-Bypass.

Negative Datensätze löschen

Ein DNS-Angriff füllt den Cache mit negativen Einträgen (NXDOMAIN und NODATA). Daher werden Antworten auf legitime Anfragen nicht zwischengespeichert, sodass neue Anfragen zur DNS-Auflösung an einen Backend-Server gesendet werden. Die Antworten erfolgen daher verzögert.

Sie können jetzt die negativen DNS-Einträge aus dem DNS-Cache der NetScaler-Appliance löschen.

Leeren negativer Cache-Datensätze mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
flush dns proxyrecords -type (dnsRecordType | negRecType)NXDOMAIN | NODATA
```


Beispiel:

```
flush dns proxyrecords -negRecType NODATA
```

Leeren negativer Cache-Datensätze mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **DNS** > **Records**.
2. Klicken Sie im Detailbereich auf **Flush Proxy Records**.
3. Wählen Sie im Feld **Flush Type** die Option **Negative Records**aus.
4. Wählen Sie im Feld **Negative Records Type** entweder **NXDOMAIN** oder **NODATA**aus.

Schutz vor zufälligen Subdomain- und NXDOMAIN-Angriffen

Um zufällige Subdomain- und NXDOMAIN-Angriffe zu verhindern, können Sie den DNS-Cache-Speicher einschränken und die TTL-Werte für negative Datensätze anpassen.

Um die vom DNS-Cache verbrauchte Speichermenge zu begrenzen, geben Sie die maximale Cachegröße (in MB) sowie die Cachegröße (in MB) zum Speichern negativer Antworten an. Wenn eines der Grenzwerte erreicht ist, werden dem Cache keine weiteren Einträge hinzugefügt. Außerdem werden Syslog-Meldungen protokolliert, und wenn Sie SNMP-Traps konfiguriert haben, werden SNMP-Traps generiert. Wenn diese Grenzwerte nicht gesetzt sind, wird das Caching fortgesetzt, bis der Systemspeicher erschöpft ist.

Ein höherer TTL-Wert für negative Datensätze kann dazu führen, dass Datensätze gespeichert werden, die für eine lange Zeit nicht wertvoll sind. Ein niedrigerer TTL-Wert führt dazu, dass mehr Anfragen an den Backend-Server gesendet werden.

Die TTL des negativen Datensatzes wird auf einen Wert gesetzt, der der niedrigere Wert des TTL-Werts oder des „Expires“ -Werts des SOA-Datensatzes sein kann.

Hinweis:

- Diese Einschränkung wird pro Paket-Engine hinzugefügt. Wenn MaxCacheSize beispielsweise auf 5 MB festgelegt ist und die Appliance über 3 Paket-Engines verfügt, beträgt die gesamte Cachegröße 15 MB.
- Die Cachegröße für die negativen Datensätze muss kleiner oder gleich der maximalen Cachegröße sein.
- Wenn Sie das DNS-Cache-Speicherlimit auf einen Wert reduzieren, der unter der Menge der bereits zwischengespeicherten Daten liegt, bleibt die Cachegröße über dem Grenzwert, bis die Daten altern. Das heißt, es übersteigt TTL0 oder ist geleert (Befehl `flush dns proxyrecords` oder Flush Proxy Records in der NetScaler GUI).
- Informationen zum Konfigurieren von SNMP-Traps finden Sie unter Konfigurieren des NetScaler zum Generieren von SNMP-Traps.

Beschränken Sie den vom DNS-Cache belegten Speicher mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set dns parameter -maxCacheSize <MBytes> -maxNegativeCacheSize <MBytes>
```

Beispiel:

```
set dns parameter - maxCacheSize 100 -maxNegativeCacheSize 25
```

Beschränken Sie den vom DNS-Cache verbrauchten Speicher mithilfe der GUI

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **DNS**, klicken Sie auf **DNS-Einstellungen ändern**und stellen Sie die folgenden Parameter ein:

- Maximale Cachegröße in MB
- Maximale negative Cachegröße in MB

Schränken Sie die TTL negativer Datensätze mithilfe der CLI ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set dns parameter -maxnegcacheTTL <secs>
```

Beispiel:

```
set dns parameter -maxnegcacheTTL 360
```

Schränken Sie die TTL negativer Datensätze mithilfe der GUI ein

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **DNS**.
2. Klicken Sie auf **DNS-Einstellungen ändern** und legen Sie den Parameter **Max Negative Cache TTL in sec** fest.

DNS-Einträge im Cache aufbewahren

Ein Angriff kann den DNS-Cache mit unwichtigen Einträgen überfluten, kann aber dazu führen, dass die bereits zwischengespeicherten legitimen Datensätze geleert werden, um Platz für die neuen Einträge zu schaffen. Um zu verhindern, dass Angriffe den Cache mit ungültigen Daten füllen, können Sie die legitimen Datensätze auch dann beibehalten, wenn sie ihre TTL-Werte überschreiten.

Wenn Sie den CacheNoExpire-Parameter aktivieren, werden die derzeit im Cache befindlichen Datensätze beibehalten, bis Sie den Parameter deaktivieren.

Hinweis:

- Diese Option kann nur verwendet werden, wenn die maximale Cachegröße angegeben ist (MaxCacheSize-Parameter).
- Wenn MaxNegCacheTTL konfiguriert und CacheNoExpire aktiviert ist, hat CacheNoExpire Priorität.

Bewahren Sie DNS-Einträge mithilfe der CLI im Cache auf

Geben Sie in der Befehlszeile Folgendes ein:

```
set dns parameter -cacheNoExpire ( ENABLED | DISABLED)
```

Beispiel:

```
set dns parameter -cacheNoExpire ENABLED
```

Bewahren Sie DNS-Einträge mithilfe der GUI im Cache auf

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **DNS** und klicken Sie auf **DNS-Einstellungen ändern**.
2. Wählen Sie **Cache No Expire aus**.

DNS-Cache-Bypass aktivieren

Für eine bessere Sichtbarkeit und Kontrolle von DNS-Anfragen stellen Sie den CacheHitBypass-Parameter so ein, dass alle Anfragen an die Backend-Server weitergeleitet werden und der Cache erstellt, aber nicht verwendet werden kann. Nachdem der Cache erstellt wurde, können Sie den Parameter deaktivieren, sodass Anfragen aus dem Cache bearbeitet werden.

Aktivieren Sie den DNS-Cache-Bypass mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set dns parameter -cacheHitBypass ( ENABLED | DISABLED )
```

Beispiel:

```
set dns parameter -cacheHitBypass ENABLED
```

Aktivieren Sie den DNS-Cache-Bypass mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **DNS** und klicken Sie auf **DNS-Einstellungen ändern**.
2. Wählen Sie **Cache Hit Bypass**aus.

Den `Slowloris` Angriff verhindern

Eine DNS-Anfrage, die sich über mehrere Pakete erstreckt, stellt die potenzielle Gefahr eines `Slowloris` Angriffs dar. Die NetScaler-Appliance kann DNS-Abfragen, die in mehrere Pakete aufgeteilt sind, im Hintergrund löschen.

Sie können den `splitPktQueryProcessing` Parameter auf ALLOW oder DROP einer DNS-Abfrage setzen, wenn die Abfrage in mehrere Pakete aufgeteilt ist.

Hinweis: Diese Einstellung gilt nur für DNS-TCP.

Beschränken Sie die DNS-Abfragen mithilfe der CLI auf ein einzelnes Paket

Geben Sie in der Befehlszeile Folgendes ein:

```
set dns parameter -splitPktQueryProcessing ( ALLOW | DROP )
```

Beispiel:

```
set dns parameter -splitPktQueryProcessing DROP
```

Beschränken Sie DNS-Abfragen mithilfe der GUI auf ein einzelnes Paket

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **DNS** und klicken Sie auf **DNS-Einstellungen ändern**.
2. Wählen Sie im Feld **Verarbeitung von Split Packet Query Processing** die Option **ALLOW** oder **DROP**aus.

Sammeln Sie Statistiken der DNS-Antworten, die aus dem Cache bereitgestellt werden

Sie können Statistiken der DNS-Antworten sammeln, die aus dem Cache bereitgestellt werden. Verwenden Sie dann diese Statistiken, um einen Schwellenwert zu erstellen, ab dem mehr DNS-Verkehr verloren geht, und setzen Sie diesen Schwellenwert mit einer bandbreitenbasierten Richtlinie durch. Bisher war die Bandbreitenberechnung für einen virtuellen DNS-Lastausgleichsserver nicht korrekt, da die Anzahl der aus dem Cache abgegebenen Anfragen nicht gemeldet wurde.

Im Proxymodus werden die Statistiken für Anforderungsbytes, Antwortbytes, Gesamtzahl der empfangenen Pakete und Gesamtzahl der gesendeten Pakete kontinuierlich aktualisiert. Bisher wurden diese Statistiken nicht immer aktualisiert, insbesondere für einen virtuellen DNS-Lastausgleichsserver.

Im Proxymodus können Sie jetzt auch die Anzahl der DNS-Antworten ermitteln, die aus dem Cache bereitgestellt werden. Um diese Statistiken zu sammeln, wurden dem `stat lb vserver` < `DNSvirtualServerName`> Befehl die folgenden Optionen hinzugefügt:

- **Anfragen** — Gesamtzahl der Anfragen, die vom virtuellen DNS- oder DNS_TCP-Server empfangen wurden. Beinhaltet die an das Backend weitergeleiteten Anfragen und die aus dem Cache beantworteten Anfragen.
- **Vserver hits** — Gesamtzahl der Anfragen, die an das Backend weitergeleitet wurden. Die Anzahl der Anfragen, die aus dem Cache bedient werden, ist die Differenz zwischen der Gesamtzahl der Anfragen und der Anzahl der Anfragen, die vom virtuellen Server bedient werden.
- **Antworten** — Gesamtzahl der von diesem virtuellen Server gesendeten Antworten. Wenn ein virtueller DNS-LB-Server beispielsweise 5 DNS-Anfragen empfangen, 3 davon an das Backend weitergeleitet und 2 davon aus dem Cache bedient hat, würde der entsprechende Wert jeder dieser Statistiken wie folgt lauten:
  - **Vserver-Treffer**: 3
  - **Anfragen**: 5
  - **Antworten**: 5

Firewall-Lastausgleich

May 11, 2023

Der Firewall-Load-Balancing verteilt den Datenverkehr auf mehrere Firewalls und sorgt so für Fehlertoleranz und erhöhten Durchsatz. Der Firewall-Load-Balancing schützt Ihr Netzwerk durch:

- Verteilung der Last auf die Firewalls, wodurch ein einziger Fehlerpunkt vermieden wird und das Netzwerk skaliert werden kann.
- Erhöhung der Hochverfügbarkeit.

Die Konfiguration einer NetScaler-Appliance für den Firewall-Lastenausgleich ähnelt der Konfiguration des Lastenausgleichs, mit der Ausnahme, dass der empfohlene Diensttyp ANY ist, der empfohlene Monitortyp PING ist und der virtuelle Servermodus für den Lastausgleich auf MAC eingestellt ist.

Sie können den Firewall-Lastenausgleich in einer Sandwich-, Unternehmens- oder Mehr-Firewall-Umgebungskonfiguration einrichten. Die Sandwich-Umgebung wird für den Lastenausgleich von Datenverkehr, der von außen in das Netzwerk eingeht, und für den Datenverkehr, der das Netzwerk zum Internet verlässt, verwendet. Dazu werden zwei NetScaler-Appliances konfiguriert, eine auf jeder Seite einer Reihe von Firewalls. Sie konfigurieren eine Unternehmensumgebung für den Lastenausgleich von Datenverkehr, der das Netzwerk verlässt, in das Internet. Die Unternehmensumgebung beinhaltet die Konfiguration einer einzelnen NetScaler-Appliance zwischen dem internen Netzwerk und den Firewalls, die den Zugriff auf das Internet ermöglichen. Die Umgebung mit mehreren Firewalls wird für den Load-Balance-Verkehr verwendet, der von einer anderen Firewall kommt. Wenn der Firewall-Lastenausgleich auf beiden Seiten der NetScaler Appliance aktiviert ist, wird der Datenverkehr sowohl in ausgehender als auch in eingehender Richtung verbessert und eine

schnellere Verarbeitung des Datenverkehrs gewährleistet. Die Umgebung mit mehreren Firewalls beinhaltet die Konfiguration einer NetScaler-Appliance, die sich zwischen zwei Firewalls befindet.

Wichtig: Wenn Sie statische Routen auf der NetScaler-Appliance für die Ziel-IP-Adresse konfigurieren und den L3-Modus aktivieren, verwendet die NetScaler-Appliance ihre Routingtabelle, um den Datenverkehr weiterzuleiten, anstatt den Datenverkehr an den vServer mit dem Load Balancing zu senden.

Hinweis: Damit FTP funktioniert, sollte auf der NetScaler-Appliance ein zusätzlicher virtueller Server oder Dienst mit IP-Adresse und Port als * bzw. 21 und als Diensttyp als FTP konfiguriert werden. In diesem Fall verwaltet die NetScaler-Appliance das FTP-Protokoll, indem sie die FTP-Steuerverbindung akzeptiert, die Payload ändert und die Datenverbindung verwaltet — alles über dieselbe Firewall.

Der Firewall-Load Balancing unterstützt nur einige der Load-Balancing-Methoden, die auf der NetScaler-Appliance unterstützt werden. Außerdem können Sie nur einige Arten von Persistenz und Monitoren konfigurieren.

Methoden zum Firewall-Lastenausgleich

Die folgenden Load-Balancing-Methoden werden für den Firewall-Lastenausgleich unterstützt.

- Geringste Verbindungen
- Runde Robin
- Am wenigsten Pakete
- Geringste Bandbreite
- Quell-IP-Hash
- Ziel-IP-Hash
- Quell-IP-Ziel-IP-Hash
- Quell-IP-Quellport-Hash
- Methode mit der geringsten Reaktionszeit (LRTM)
- Benutzerdefinierte Last

Firewall-Persistenz

Nur auf SOURCEIP, DESTIP und SOURCEIPDESTIP basierende Persistenz wird für den Firewall-Lastenausgleich unterstützt.

Überwachung des Firewall-Servers

Beim Firewall-Lastenausgleich werden nur PING und transparente Monitore unterstützt. Sie können einen PING-Monitor (Standard) an den Backend-Dienst binden, der die Firewall darstellt. Wenn eine Firewall so konfiguriert ist, dass sie nicht auf Ping-Pakete reagiert, können Sie transparente Monitore konfigurieren, um Hosts auf der vertrauenswürdigen Seite mithilfe einzelner Firewalls zu überwachen.

Sandwich-Umgebung

May 11, 2023

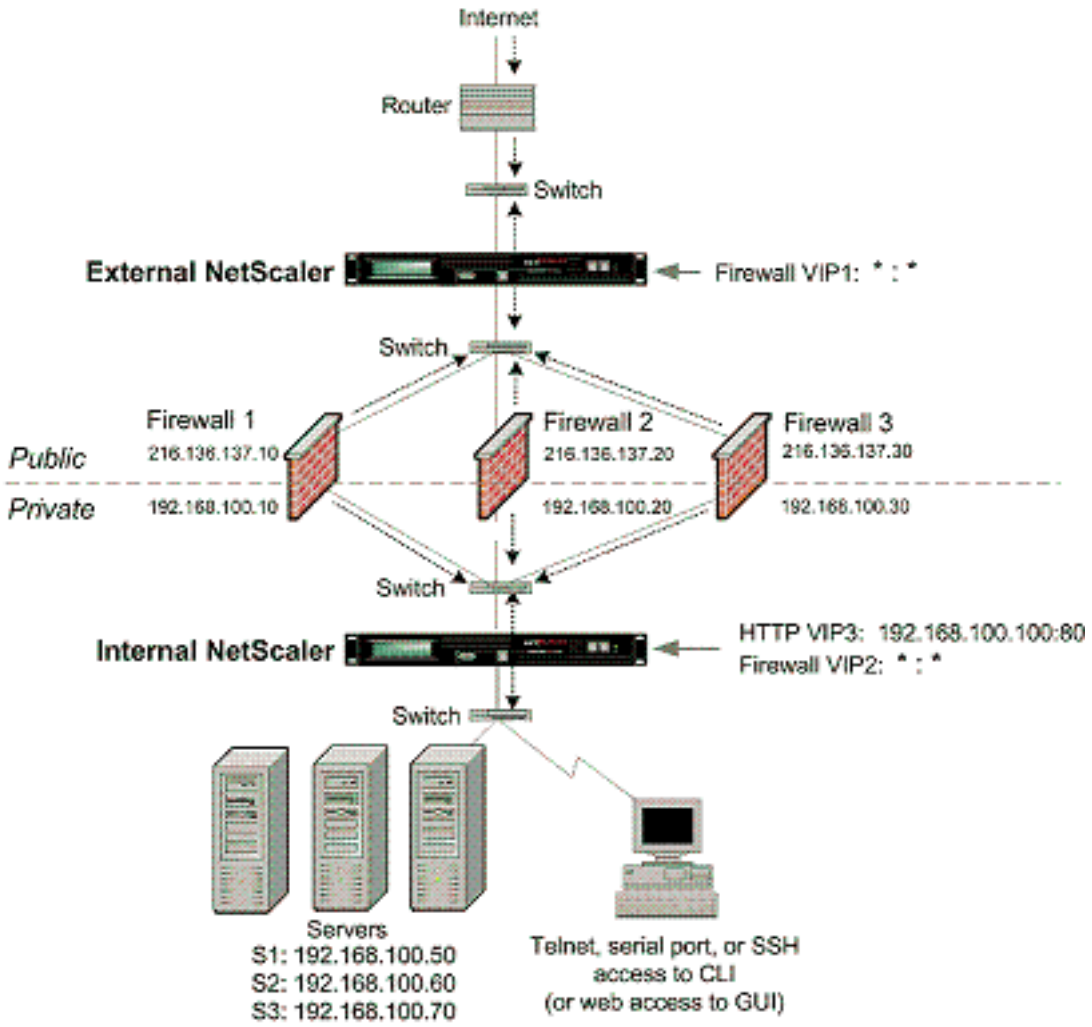
Eine NetScaler-Bereitstellung in einem Sandwichmodus kann den Netzwerkverkehr über Firewalls in beide Richtungen ausgleichen: Ingress (Datenverkehr, der von außen in das Netzwerk gelangt, z. B. das Internet) und Egress (Datenverkehr, der das Netzwerk verlässt und ins Internet gelangt).

In diesem Setup befindet sich ein NetScaler auf jeder Seite einer Reihe von Firewalls. Der NetScaler, der zwischen den Firewalls und dem Internet platziert wird und als externer NetScaler bezeichnet wird, der den eingehenden Datenverkehr verarbeitet, wählt auf der Grundlage der konfigurierten Methode die beste Firewall aus. Der NetScaler zwischen den Firewalls und dem privaten Netzwerk, der sogenannte interne NetScaler, verfolgt die Firewall, von der das erste Paket für eine Sitzung empfangen wird. Anschließend wird sichergestellt, dass alle nachfolgenden Pakete für diese Sitzung an dieselbe Firewall gesendet werden.

Der interne NetScaler kann als regulärer Traffic Manager konfiguriert werden, um den Datenverkehr auf den privaten Netzwerkservern zu verteilen. Diese Konfiguration ermöglicht auch, dass der vom privaten Netzwerk ausgehende Datenverkehr (ausgehender Datenverkehr) über die Firewalls verteilt wird.

Das folgende Diagramm zeigt die Load-Balancing-Umgebung der Sandwich-Firewall.

Abbildung 1. Firewall-Lastenausgleich (Sandwich)



Der Diensttyp ANY konfiguriert den NetScaler so, dass er den gesamten Datenverkehr akzeptiert.

Um die Vorteile von HTTP und TCP nutzen zu können, konfigurieren Sie den Dienst und den virtuellen Server mit dem Typ HTTP oder TCP. Damit FTP funktioniert, konfigurieren Sie den Dienst mit dem Typ FTP.

Konfiguration des externen NetScaler in einer Sandwich-Umgebung

Führen Sie die folgenden Aufgaben aus, um den externen NetScaler in einer Sandwichumgebung zu konfigurieren:

- Aktivieren Sie die Lastausgleichsfunktion.
- Konfigurieren Sie einen Platzhalterdienst für jede Firewall.
- Konfigurieren Sie einen Monitor für jeden Wildcard-Dienst.
- Konfigurieren Sie einen virtuellen Wildcard-Server für Datenverkehr aus dem Internet.
- Konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus.
- Binden Sie Dienste an den virtuellen Wildcard-Server.

- Speichern und überprüfen Sie die Konfiguration.

Aktivieren der Load Balancing-Funktion

So aktivieren Sie Load Balancing mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Beispiel:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                       Acronym             Status
        -------                       -------             ------
 1)     Web Logging                   WL                  OFF
 2)     Surge Protection              SP                  ON
 3)     Load Balancing                LB                  ON
 .
 .
 .
 24)    NetScaler Push                push                OFF
 Done
<!--NeedCopy-->
```

So aktivieren Sie Load Balancing mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen** und wählen **Sie unter Configure Basic Features**die Option **Load Balancing**aus.

Einen Platzhalterdienst für jede Firewall konfigurieren

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <serverName> ANY *
```



```
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Services** und fügen Sie einen Dienst hinzu. Geben Sie **ANY** im Feld **Protokoll** und * im Feld Port an.

Einen Monitor für jeden Wildcard-Dienst konfigurieren

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um die Hosts auf der vertrauenswürdigen Seite mithilfe einzelner Firewalls zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht die Konnektivität nur zwischen der NetScaler-Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, das die im Monitor angegebene Ziel-IP-Adresse besitzt. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der Geräte mit dem nächsten Hop von dieser Firewall ausgefallen ist, schließt die Appliance die Firewall beim Load Balancing ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der Geräte für den nächsten Hop ausgefallen ist. Durch das Binden eines transparenten Monitors wird der Dienst als DOWN markiert, wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, und die Firewall wird nicht einbezogen, wenn die Appliance den Firewall-Lastausgleich durchführt.

Die Bindung eines transparenten Monitors hat Vorrang vor dem PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```


Beispiel:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
To bind a PING monitor, type the following command:
bind monitor PING fw-svc1
<!--NeedCopy-->
```

So erstellen und binden Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**und erstellen Sie dann einen transparenten Monitor und binden Sie ihn.

Konfigurieren Sie einen virtuellen Wildcard-Server für Datenverkehr aus dem Internet

So konfigurieren Sie einen virtuellen Wildcard-Server für Datenverkehr aus dem Internet mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Wildcard-Server für Datenverkehr aus dem Internet mithilfe des Konfigurationsprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und erstellen Sie einen virtuellen Wildcard-Server. Geben Sie **ANY** im Feld **Protokoll** und * im Feld Port an.

Konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus

So konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und wählen Sie den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB-1).
2. Bearbeiten Sie den Abschnitt **Grundeinstellungen** und klicken Sie auf **Mehr**.
3. Wählen Sie in der Dropdownliste **Umleitungsmodus** die Option **MAC Based**aus.

Binden Sie Dienste an den virtuellen Wildcard-Server

So binden Sie einen Dienst mithilfe der Befehlszeilenschnittstelle an den virtuellen Wildcard-Server

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Dienst mithilfe des Konfigurationsdienstprogramms an den virtuellen Wildcard-Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und wählen Sie den virtuellen Server aus, für den Sie den Dienst binden möchten.
2. Klicken Sie in den Abschnitt **Dienste** und wählen Sie einen Dienst aus, den Sie binden möchten.

Speichern und überprüfen Sie die Konfiguration

Speichern Sie die Konfiguration, wenn Sie die Konfigurationsaufgaben abgeschlossen haben. Stellen Sie sicher, dass die Einstellungen korrekt sind.

So speichern und überprüfen Sie die Konfiguration mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

```
save ns config
show vserver
<!--NeedCopy-->
```

Beispiel:

```
save config
sh lb vserver FWLBVIP1
FWLBVIP1 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 06:40:14 2010
        Time since last state change: 0 days, 00:00:11.240
        Effective State: UP  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: SRCIPDESTIPHASH
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw_svc_1 (10.102.29.251: *) - ANY State: UP  Weight: 1
2) fw_svc_2 (10.102.29.18: \*) - ANY State: UP   Weight: 1
 Done
show service fw-svc1
        fw-svc1 (10.102.29.251:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 10:04:50 2010
        Time since last state change: 0 days, 00:00:38.120
        Server Name: 10.102.29.251
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
```



```
30          Access Down Service: NO
31          TCP Buffering(TCPB): YES
32          HTTP Compression(CMP): NO
33          Idle timeout: Client: 120 sec   Server: 120 sec
34          Client IP: DISABLED
35          Cacheable: NO
36          SC: OFF
37          SP: OFF
38          Down state flush: ENABLED
39
40  1)      Monitor Name: monitor-HTTP-1
41                  State: DOWN     Weight: 1
42                  Probes: 5       Failed [Total: 5 Current: 5]
43                  Last response: Failure - Time out during TCP connection
                        establishment stage
44                  Response Time: 2000.0 millisec
45  2)      Monitor Name: ping
46                  State: UP       Weight: 1
47                  Probes: 3       Failed [Total: 0 Current: 0]
48                  Last response: Success - ICMP echo reply received.
49                  Response Time: 1.415 millisec
50   Done
51  <!--NeedCopy-->
```

Konfiguration des internen NetScaler in einer Sandwich-Umgebung

Führen Sie die folgenden Aufgaben aus, um den internen NetScaler in einer Sandwichumgebung zu konfigurieren

Für Datenverkehr vom Server (Egress)

- Aktivieren Sie die Lastausgleichsfunktion.
- Konfigurieren Sie einen Platzhalterdienst für jede Firewall.
- Konfigurieren Sie einen Monitor für jeden Wildcard-Dienst.
- Konfigurieren Sie einen virtuellen Platzhalterserver, um den an die Firewalls gesendeten Datenverkehr auszugleichen.
- Konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus.
- Binden Sie Firewalldienste an den virtuellen Platzhalterserver.

Für Datenverkehr über private Netzwerkserver

- Konfigurieren Sie einen Dienst für jeden virtuellen Server.
- Konfigurieren Sie für jeden Dienst einen Monitor.

- Konfigurieren Sie einen virtuellen HTTP-Server, um den an die Server gesendeten Datenverkehr auszugleichen.
- Binden Sie HTTP-Dienste an den virtuellen HTTP-Server.
- Speichern und überprüfen Sie die Konfiguration.

Aktivieren der Load Balancing-Funktion

Sie können Load Balancing-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Lastausgleichsfunktion deaktiviert ist. Sie funktionieren jedoch erst, wenn Sie die Funktion aktivieren.

So aktivieren Sie Load Balancing mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen

```
enable ns feature LB
show ns feature
<!--NeedCopy-->
```

Beispiel:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                       Acronym             Status
        -------                       -------             ------
 1)     Web Logging                   WL                  OFF
 2)     Surge Protection              SP                  ON
 3)     Load Balancing                LB                  ON
 .
 .
 .
 24)    NetScaler Push                push                OFF
 Done
<!--NeedCopy-->
```

So aktivieren Sie Load Balancing mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen** und wählen Sie unter Configure Basic Features die Option **Load Balancing**aus.

Einen Platzhalterdienst für jede Firewall konfigurieren

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Services** und fügen Sie einen Dienst hinzu. Geben Sie **ANY** im Feld **Protokoll** und * im Feld Port an.

Einen Monitor für jeden Wildcard-Dienst konfigurieren

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um die Hosts auf der vertrauenswürdigen Seite mithilfe einzelner Firewalls zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht die Konnektivität nur zwischen der NetScaler-Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, das die im Monitor angegebene Ziel-IP-Adresse besitzt. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der Geräte mit dem nächsten Hop von dieser Firewall ausgefallen ist, schließt die Appliance die Firewall beim Load Balancing ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der Geräte für den nächsten Hop ausgefallen ist. Durch das Binden eines transparenten Monitors wird der Dienst als DOWN markiert, wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, und die Firewall wird nicht einbezogen, wenn die Appliance den Firewall-Lastausgleich durchführt.

Die Bindung eines transparenten Monitors hat Vorrang vor dem PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

So erstellen und binden Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore** und erstellen Sie einen Monitor.
2. Geben **Sie im Dialogfeld Monitor erstellen** die erforderlichen Parameter ein und wählen Sie **Transparent**aus.

Konfigurieren Sie einen virtuellen Platzhalterserver, um den an die Firewalls gesendeten Datenverkehr auszugleichen

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Wildcard-Server für Datenverkehr aus dem Internet mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und erstellen Sie einen virtuellen Wildcard-Server.

2. Geben Sie **ANY** im Feld Protokoll und ***** im Feld Port an.

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf "Hinzufügen".
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an, wie hier gezeigt:
   - Name—Name
4. Wählen Sie unter Protokoll BELIEBIG und unter IP-Adresse und Port die Option * aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der virtuelle Server, den Sie erstellt haben, wird im Bereich Load Balancing Virtual Servers angezeigt.

Konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus

So konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und wählen Sie den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB-1).
2. Bearbeiten Sie den Abschnitt **Grundeinstellungen** und klicken Sie auf **Mehr**.
3. Wählen Sie in der Dropdownliste **Umleitungsmodus** die Option **MAC Based**aus.

Binden Sie Firewalldienste an den virtuellen Platzhalterserver

So binden Sie Firewalldienste mithilfe der Befehlszeilenschnittstelle an den virtuellen Platzhalterserver

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie Firewalldienste mithilfe des Konfigurationsdienstprogramms an den virtuellen Platzhalterserver

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und wählen Sie einen virtuellen Server aus.
2. Klicken Sie in den Abschnitt Service und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Einen Dienst für jeden virtuellen Server konfigurieren

So konfigurieren Sie einen Dienst für jeden virtuellen Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
<!--NeedCopy-->
```

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und konfigurieren Sie einen Dienst für jeden virtuellen Server.
2. Geben Sie **HTTP** im Feld **Protokoll** an und wählen Sie unter **Verfügbare Monitore** die Option **HTTP**aus.

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Service erstellen Werte für die folgenden Parameter an, wie hier gezeigt:
   - Dienstname — Name
   - Server — ServerName
   - Port-Anschluss
4. Geben Sie unter Protokoll den Wert HTTP an. Wählen Sie unter Verfügbare Monitore die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der von Ihnen erstellte Dienst wird im Bereich Dienste angezeigt.

Einen Monitor für jeden Dienst konfigurieren

So binden Sie einen Monitor mithilfe der Befehlszeilenschnittstelle an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Monitor mithilfe des Konfigurationsdienstprogramms an einen Dienst

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, doppelklicken Sie auf einen Dienst und fügen Sie einen Monitor hinzu.

Konfigurieren Sie einen virtuellen HTTP-Server, um den an die Server gesendeten Datenverkehr auszugleichen

So konfigurieren Sie einen virtuellen HTTP-Server für den Ausgleich des Datenverkehrs, der über die Befehlszeilenschnittstelle an die Server gesendet wird

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```


Beispiel:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen HTTP-Server so, dass er den mit dem Konfigurationsdienstprogramm an die Server gesendeten Datenverkehr ausgleicht

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtual Services**und konfigurieren Sie einen virtuellen HTTP-Server.
2. Geben Sie **HTTP** im Feld **Protokoll** an.

So konfigurieren Sie einen virtuellen HTTP-Server so, dass er den mit dem Konfigurationsdienstprogramm an die Server gesendeten Datenverkehr ausgleicht

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an, wie hier gezeigt:
   - Name—Name
   - **IP-Adresse — IP-Adresse**
     Hinweis: Wenn der virtuelle Server IPv6 verwendet, aktivieren Sie das IPv6-Kontrollkästchen und geben Sie die Adresse im IPv6-Format ein (z. B. 1000:0000:0000:0000:0005:0600:700 a:888b).
   - Port-Anschluss
4. Wählen Sie unter Protokoll die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der virtuelle Server, den Sie erstellt haben, wird im Bereich Load Balancing Virtual Servers angezeigt.

Speichern und überprüfen Sie die Konfiguration

Speichern Sie die Konfiguration, wenn Sie die Konfigurationsaufgaben abgeschlossen haben. Sie sollten auch überprüfen, ob die Einstellungen korrekt sind.

So speichern und überprüfen Sie die Konfiguration mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

- `save ns config`
- `show vserver`

Beispiel:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
```



```
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
 Done
<!--NeedCopy-->
```

So speichern und überprüfen Sie die Konfiguration mit dem Konfigurationsdienstprogramm

1. Klicken Sie im **Detailbereich** auf **Speichern**.
2. Klicken **Sie im Dialogfeld „Konfiguration speichern** “ auf **Ja**.
3. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
4. Wählen Sie im **Detailbereich** den virtuellen Server aus, den Sie in Schritt 5 erstellt haben.
5. Stellen Sie sicher, dass die im **Detailbereich** angezeigten Einstellungen korrekt sind.
6. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
7. Wählen Sie im **Detailbereich** die Dienste aus, die Sie in Schritt 5 erstellt haben.
8. Stellen Sie sicher, dass die im **Detailbereich** angezeigten Einstellungen korrekt sind.

Überwachung eines Firewall-Load-Balancing-Setups in einer Sandwich-Umgebung

Nachdem die Konfiguration ausgeführt wurde, sollten Sie die Statistiken für jeden Dienst und virtuellen Server anzeigen, um nach möglichen Problemen zu suchen.

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der NetScaler-Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der eingegangenen Anfragen

- Rate der Treffer

So zeigen Sie Statistiken zu virtuellen Servern mit der Befehlszeilenschnittstelle an

Um eine Zusammenfassung der Statistiken für alle derzeit auf dem NetScaler konfigurierten virtuellen Server oder für einen einzelnen virtuellen Server anzuzeigen, geben Sie an der Befehlszeile Folgendes ein:

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Beispiel:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done

<!--NeedCopy-->
```

So zeigen Sie Statistiken zu virtuellen Servern mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server > Statistik**.
2. Wenn Sie die Statistiken für nur einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf **Statistik**.

Statistiken eines Dienstes anzeigen

Sie können die Rate von Anfragen, Antworten, Anforderungsbytes, Antwortbytes, aktuellen Clientverbindungen, Anforderungen in Surge-Warteschlange, aktuellen Serververbindungen usw.

mithilfe der Dienststatistik anzeigen.

So zeigen Sie die Statistiken eines Dienstes mit der Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines Dienstes mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services > Statistik**.
2. Wenn Sie die Statistiken nur für einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf **Statistiken**.

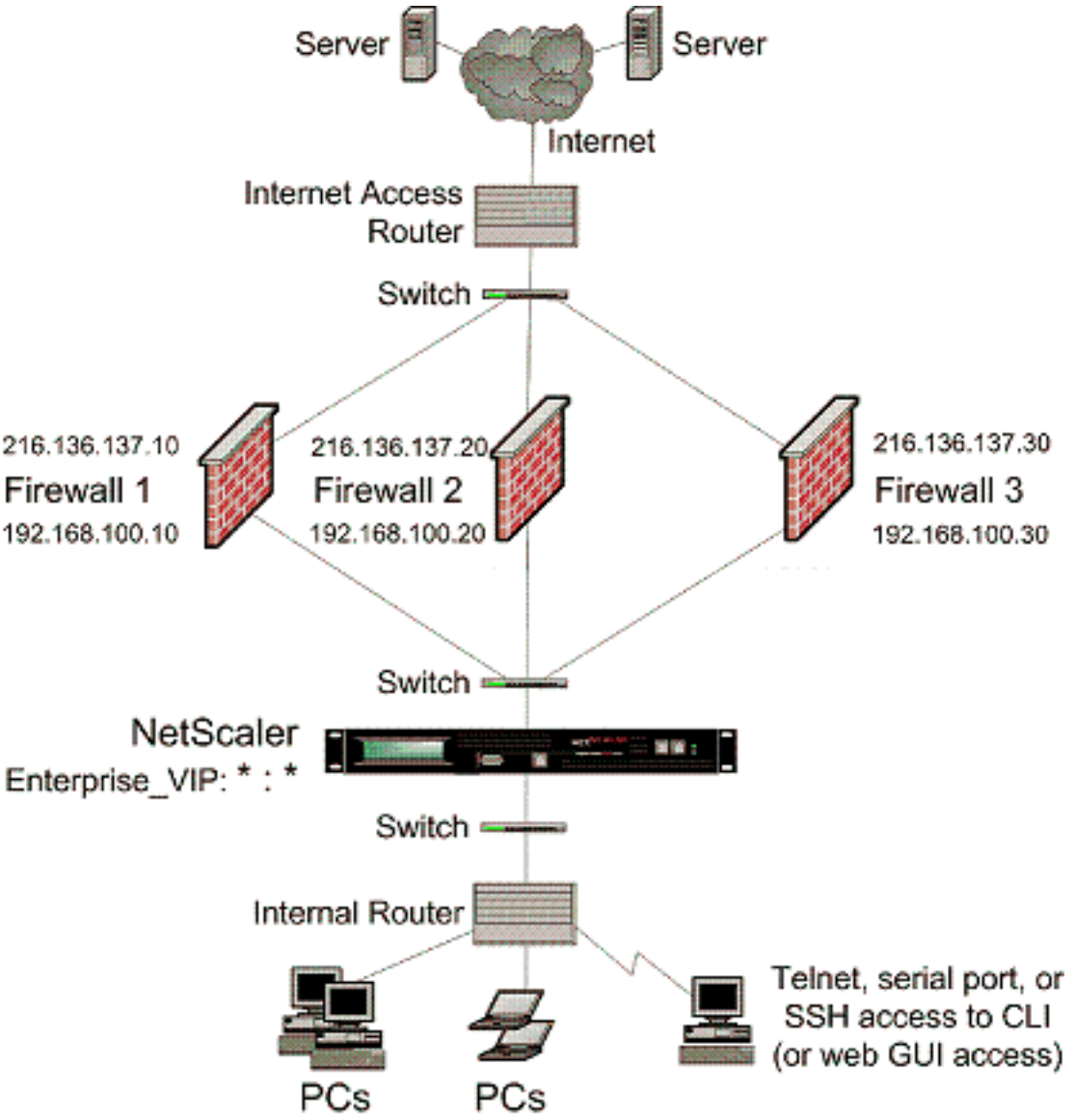
Unternehmens-Umgebung

May 11, 2023

Im Unternehmens-Setup wird der NetScaler zwischen den Firewalls platziert, die mit dem öffentlichen Internet und dem internen privaten Netzwerk verbunden sind, und verarbeitet den ausgehenden Datenverkehr. Der NetScaler wählt die beste Firewall basierend auf der konfigurierten Load Balancing-Richtlinie aus.

Das folgende Diagramm zeigt die Unternehmens-Firewall-Lastausgleichsumgebung

Abbildung 1. Firewall-Lastenausgleich (Enterprise)



Der Diensttyp ANY konfiguriert den NetScaler so, dass er den gesamten Datenverkehr akzeptiert.

Um die Vorteile im Zusammenhang mit HTTP und TCP in Anspruch zu nehmen, konfigurieren Sie den Dienst und den vserver mit dem Typ HTTP oder TCP. Damit FTP funktioniert, konfigurieren Sie den Dienst mit dem Typ FTP.

Konfiguration des NetScaler in einer Unternehmensumgebung

Führen Sie die folgenden Aufgaben aus, um einen NetScaler in einer Unternehmensumgebung zu konfigurieren.

Für Datenverkehr vom Server (Egress)

- Aktivieren Sie die Lastausgleichsfunktion.

- Konfigurieren Sie einen Platzhalterdienst für jede Firewall.
- Konfigurieren Sie einen Monitor für jeden Wildcard-Dienst.
- Konfigurieren Sie einen virtuellen Platzhalterserver, um den an die Firewalls gesendeten Datenverkehr auszugleichen.
- Konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus.
- Binden Sie Firewalldienste an den virtuellen Platzhalterserver.

Für Datenverkehr über private Netzwerkserver

- Konfigurieren Sie einen Dienst für jeden virtuellen Server.
- Konfigurieren Sie für jeden Dienst einen Monitor.
- Konfigurieren Sie einen virtuellen HTTP-Server, um den an die Server gesendeten Datenverkehr auszugleichen.
- Binden Sie HTTP-Dienste an den virtuellen HTTP-Server.
- Speichern und überprüfen Sie die Konfiguration.

Im folgenden Konfigurationsbeispiel wird einer der Firewall-Server im Netzwerk-Topologie-Diagramm (Abbildung 1) betrachtet.

Aktivieren der Load Balancing-Funktion

Sie können Load Balancing-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Load Balancing-Funktion deaktiviert ist. Sie funktionieren jedoch erst, wenn Sie die Funktion aktivieren.

So aktivieren Sie Load Balancing mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen

- enable ns feature LB
- show ns feature

Beispiel:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
```



```
12  .
13  24)    NetScaler Push                  push                  OFF
14  Done
15 <!--NeedCopy-->
```

So aktivieren Sie Load Balancing mit dem Konfigurationsdienstprogramm

Navigieren Sie zu System > Einstellungen und wählen Sie unter Configure Basic Featuresdie Option Load Balancingaus.

Einen Platzhalterdienst für jede Firewall konfigurieren

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add service <name> <serverName> ANY *
2 <!--NeedCopy-->
```

Beispiel:

```
1 add service Service-HTTP-1 192.168.100.10 ANY *
2 <!--NeedCopy-->
```

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Service erstellen Werte für die folgenden Parameter an, wie hier gezeigt:
   - Dienstname — Name
   - Server — ServerName
4. Wählen Sie unter Protokoll ANY und unter Port die Option * aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der von Ihnen erstellte Dienst wird im Bereich Dienste angezeigt.

Einen Monitor für jeden Wildcard-Dienst konfigurieren

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um Hosts auf der vertrauenswürdigen Seite durch einzelne Firewalls zu

überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht die Konnektivität nur zwischen der NetScaler-Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, das die im Monitor angegebene Ziel-IP-Adresse besitzt. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der Geräte mit dem nächsten Hop von dieser Firewall ausgefallen ist, schließt die Appliance die Firewall beim Load Balancing ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der Geräte für den nächsten Hop ausgefallen ist. Durch das Binden eines transparenten Monitors wird der Dienst als DOWN markiert, wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, und die Firewall wird nicht einbezogen, wenn die Appliance den Firewall-Lastausgleich durchführt.

Das Binden eines transparenten Monitors überschreibt den PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -destport 80 -
    transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

So erstellen und binden Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Monitor erstellen die Werte wie folgt an:
    - Vorname*
    - Typ*—Typ

- Ziel-IP
- Transparente

-* Ein erforderlicher Parameter

4. Klicken Sie auf Erstellenund dann auf Schließen. Wählen Sie im Bereich Monitore den Monitor aus, den Sie gerade konfiguriert haben, und stellen Sie sicher, dass die am unteren Bildschirmrand angezeigten Einstellungen korrekt sind.

Konfigurieren Sie einen virtuellen Platzhalterserver, um den an die Firewalls gesendeten Datenverkehr auszugleichen

Der Datenverkehr, der durch Firewalls fließt, ist für verschiedene Proxys oder Server gedacht, die sich hinter den Firewalls befinden. Diese Proxys oder Server können unterschiedliche IP-Adressen und Ports haben. Damit der Datenverkehr transparent durch die Firewalls geleitet wird, müssen die IP-Adresse und der Port des virtuellen Servers Load Balancing der Firewalls auf * gesetzt werden, um Datenverkehr für jede IP-Adresse und jeden Port zu akzeptieren.

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an, wie hier gezeigt:
   - Name—Name
4. Wählen Sie unter Protokoll BELIEBIG und unter IP-Adresse und Port die Option * aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der virtuelle Server, den Sie erstellt haben, wird im Bereich Load Balancing Virtual Servers angezeigt.

Konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus

So konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Klicken Sie auf der Registerkarte Erweitert unter Umleitungsmodus auf MAC-basiert.
4. Klicken Sie auf OK.

Binden Sie Firewalldienste an den virtuellen Platzhalterserver

So binden Sie Firewalldienste mithilfe der Befehlszeilenschnittstelle an den virtuellen Platzhalterserver

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie Firewalldienste mithilfe des Konfigurationsdienstprogramms an den virtuellen Platzhalterserver

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Serverund wählen Sie einen virtuellen Server aus.

2. Klicken Sie in den Abschnitt Service und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Einen Dienst für jeden virtuellen Server konfigurieren

So konfigurieren Sie einen Dienst für jeden virtuellen Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 192.168.100.10 HTTP 80
<!--NeedCopy-->
```

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Service erstellen Werte für die folgenden Parameter an, wie hier gezeigt:
   - Dienstname — Name
   - Server — ServerName
   - Port-Anschluss
4. Geben Sie unter Protokoll den Wert HTTP an. Wählen Sie unter Verfügbare Monitore die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der von Ihnen erstellte Dienst wird im Bereich Dienste angezeigt.

Einen Monitor für jeden Dienst konfigurieren

So binden Sie einen Monitor mithilfe der Befehlszeilenschnittstelle an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Beispiel:


```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Monitor mithilfe des Konfigurationsdienstprogramms an einen Dienst

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Öffnen Sie den Dienst, und fügen Sie einen Monitor hinzu.

Konfigurieren Sie einen virtuellen HTTP-Server, um den an die Server gesendeten Datenverkehr auszugleichen

So konfigurieren Sie einen virtuellen HTTP-Server für den Ausgleich des Datenverkehrs, der über die Befehlszeilenschnittstelle an die Server gesendet wird

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen HTTP-Server so, dass er den mit dem Konfigurationsdienstprogramm an die Server gesendeten Datenverkehr ausgleicht

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an, wie hier gezeigt:
   - Name—Name
   - IP-Adresse — IPAddress
     Hinweis: Wenn der virtuelle Server IPv6 verwendet, aktivieren Sie das Kontrollkästchen IPv6, und geben Sie die Adresse im IPv6-Format ein (z. B. **1000:0000:0000:0000:0005:0600:700a:888b**).
   - Port-Anschluss
4. Wählen Sie unter Protokoll die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der virtuelle Server, den Sie erstellt haben, wird im Bereich Load Balancing Virtual Servers angezeigt.

Binden Sie HTTP-Dienste an den virtuellen HTTP-Server

So binden Sie HTTP-Dienste mithilfe der Befehlszeilenschnittstelle an den virtuellen Platzhalterserver

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie HTTP-Dienste mithilfe des Konfigurationsdienstprogramms an den virtuellen Platzhalterserver

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Serverund wählen Sie einen virtuellen Server aus.
2. Klicken Sie in den Abschnitt Service und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Speichern und überprüfen Sie die Konfiguration

Speichern Sie die Konfiguration, wenn Sie die Konfigurationsaufgaben abgeschlossen haben. Sie sollten auch überprüfen, ob die Einstellungen korrekt sind.

So speichern und überprüfen Sie die Konfiguration mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

- Speichern Sie ns Config
- vserver anzeigen

Beispiel:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
```



```
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (192.168.100.10: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (192.168.100.10:\*) - ANY
        State: UP
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 192.168.100.10
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: UP     Weight: 1
                Probes: 9       Failed [Total: 0 Current: 0]
                Last response: Success - HTTP response code 200
       received
                Response Time: 100.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
 Done
```



```
<!--NeedCopy-->
```

So speichern und überprüfen Sie die Konfiguration mit dem Konfigurationsdienstprogramm

1. Klicken Sie im Detailbereich auf Speichern.
2. Klicken Sie im Dialogfeld Konfiguration speichern auf Ja.
3. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
4. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie in Schritt 5 erstellt haben, und stellen Sie sicher, dass die im Detailbereich angezeigten Einstellungen korrekt sind.
5. Navigieren Sie zu Traffic Management > Load Balancing > Services.
6. Wählen Sie im Detailbereich den Dienst aus, den Sie in Schritt 5 erstellt haben, und stellen Sie sicher, dass die im Bereich Details angezeigten Einstellungen korrekt sind.

Überwachen einer Firewall-Lastausgleichseinrichtung in einer Unternehmensumgebung

Nachdem die Konfiguration ausgeführt wurde, sollten Sie die Statistiken für jeden Dienst und virtuellen Server anzeigen, um nach möglichen Problemen zu suchen.

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der NetScaler-Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der eingegangenen Anfragen
- Rate der Treffer

So zeigen Sie Statistiken zu virtuellen Servern mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein, um eine Zusammenfassung der Statistiken für alle virtuellen Server anzuzeigen, die derzeit auf der NetScaler-Appliance konfiguriert sind, oder für einen einzelnen virtuellen Server:


```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Beispiel:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                       vsvrIP  port     Protocol        State    Req/s
                            Hits/s
One                         *    80         HTTP           UP      5/s
        0/s
Two                         *     0          TCP         DOWN      0/s
        0/s
Three                       *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done


<!--NeedCopy-->
```

So zeigen Sie Statistiken zu virtuellen Servern mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server > Statistik.
2. Wenn Sie die Statistiken für nur einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf Statistik.

Statistiken eines Dienstes anzeigen

Aktualisiert: 2013-08-28

Sie können die Rate von Anfragen, Antworten, Anforderungsbytes, Antwortbytes, aktuellen Clientverbindungen, Anforderungen in Surge-Warteschlange, aktuellen Serververbindungen usw. mithilfe der Dienststatistik anzeigen.

So zeigen Sie die Statistiken eines Dienstes mit der Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:


```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines Dienstes mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu Traffic Management > Load Balancing > Services > Statistik.
2. Wenn Sie die Statistiken nur für einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf Statistiken.

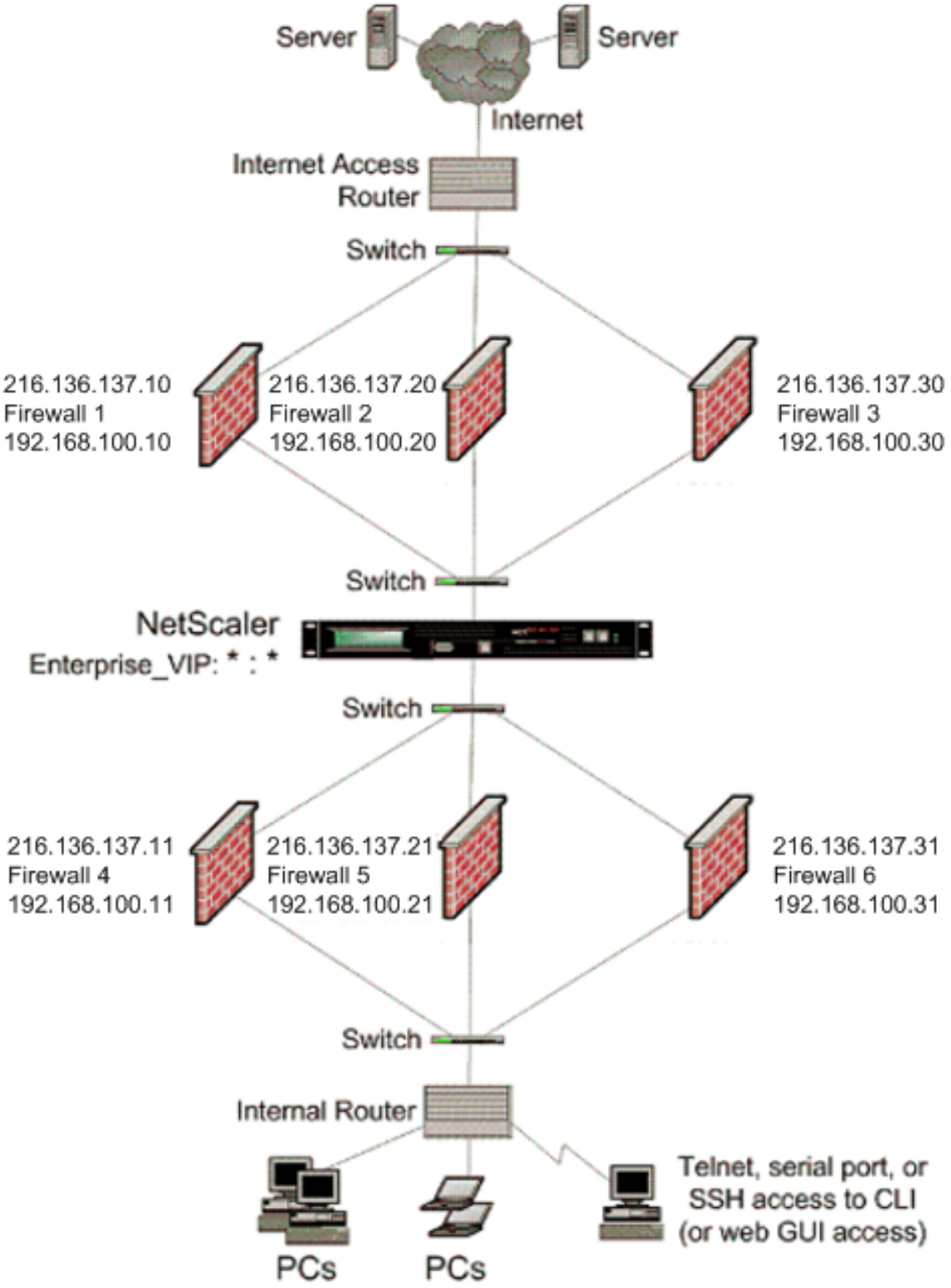
Mehrfach-Firewall-Umgebung

May 11, 2023

In einer Umgebung mit mehreren Firewalls wird die NetScaler-Appliance zwischen zwei Gruppen von Firewalls platziert, wobei der externe Satz eine Verbindung zum öffentlichen Internet herstellt und der interne Satz eine Verbindung zum internen privaten Netzwerk herstellt. Das externe Set verarbeitet normalerweise den ausgehenden Verkehr. Diese Firewalls implementieren hauptsächlich Zugriffskontrolllisten, um den Zugriff auf externe Ressourcen zu ermöglichen oder zu verweigern. Das interne Set verarbeitet normalerweise den eingehenden Verkehr. Diese Firewalls implementieren Sicherheitsmaßnahmen, um das Intranet vor böswilligen Angriffen zu schützen, und sorgen nicht nur für einen Lastenausgleich des eingehenden Datenverkehrs. In der Umgebung mit mehreren Firewalls können Sie den Datenverkehr, der von einer anderen Firewall kommt, ausgleichen. Standardmäßig erfolgt für den von einer Firewall kommenden Datenverkehr kein Lastausgleich auf der anderen Firewall über eine NetScaler-Appliance. Wenn der Firewall-Lastenausgleich auf beiden Seiten von NetScaler aktiviert ist, wird der Datenverkehr sowohl in ausgehender als auch in eingehender Richtung verbessert und eine schnellere Verarbeitung des Datenverkehrs gewährleistet.

Die folgende Abbildung zeigt eine Load-Balancing-Umgebung mit mehreren Firewalls

Abbildung 1. Firewall-Load-Balancing (mehrere Firewalls)



Mit einer Konfiguration wie der in Abbildung 1 gezeigten können Sie den NetScaler so konfigurieren, dass der Datenverkehr über eine interne Firewall lastenverteilt wird, auch wenn der Lastenausgleich

durch eine externe Firewall erfolgt. Wenn diese Funktion beispielsweise konfiguriert ist, wird der von den externen Firewalls (Firewalls 1, 2 und 3) kommende Datenverkehr auf die internen Firewalls (Firewalls 4, 5 und 6) verteilt und umgekehrt.

Der Firewall-Lastenausgleich wird nur für virtuelle LB-Server im MAC-Modus unterstützt.

Der Diensttyp ANY konfiguriert den NetScaler so, dass er den gesamten Datenverkehr akzeptiert.

Um die Vorteile von HTTP und TCP nutzen zu können, konfigurieren Sie den Dienst und den virtuellen Server mit dem Typ HTTP oder TCP. Damit FTP funktioniert, konfigurieren Sie den Dienst mit dem Typ FTP.

Konfiguration des NetScaler in einer Umgebung mit mehreren Firewalls

Um eine NetScaler-Appliance in einer Umgebung mit mehreren Firewalls zu konfigurieren, müssen Sie die Lastausgleichsfunktion aktivieren, einen virtuellen Server für den Lastausgleich des ausgehenden Datenverkehrs über die externen Firewalls konfigurieren, einen virtuellen Server für den Lastausgleich des eingehenden Datenverkehrs über die internen Firewalls konfigurieren und den Firewall-Lastenausgleich auf der NetScaler-Appliance aktivieren. Um einen virtuellen Server für den Lastenausgleich des Datenverkehrs über eine Firewall in einer Umgebung mit mehreren Firewalls zu konfigurieren, müssen Sie:

1. Einen Platzhalterdienst für jede Firewall konfigurieren
2. Einen Monitor für jeden Wildcard-Dienst konfigurieren
3. Konfigurieren Sie einen virtuellen Platzhalterserver, um den an die Firewalls gesendeten Datenverkehr auszugleichen
4. Konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus
5. Binden Sie Firewalldienste an den virtuellen Platzhalterserver

Aktivierung der Load-Balancing-Funktion

Um Load Balancing-Entitäten wie Dienste und virtuelle Server zu konfigurieren und zu implementieren, müssen Sie die Lastausgleichsfunktion auf dem NetScaler-Gerät aktivieren.

So aktivieren Sie den Lastenausgleich mithilfe der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen

```
enable ns feature <featureName>
show ns feature
<!--NeedCopy-->
```

Beispiel:


```
enable ns feature LoadBalancing
Done
show ns feature
Feature Acronym Status
------- ------- ------
1) Web Logging WL OFF
2) Surge Protection SP ON
3) Load Balancing LB ON
.
.
.
24) NetScaler Push push OFF
Done
<!--NeedCopy-->
```

Um den Lastenausgleich mithilfe der GUI zu aktivieren, gehen Sie wie folgt vor:

1. Erweitern Sie im Navigationsbereich System, und klicken Sie dann auf Einstellungen.
2. Klicken Sie im Bereich Einstellungen unter Modi und Funktionen auf Grundfunktionen ändern.
3. Aktivieren Sie im Dialogfeld „Grundfunktionen konfigurieren“ das Kontrollkästchen Load Balancing, und klicken Sie dann auf Ok.

Konfiguration eines Wildcard-Dienstes für jede Firewall

Um Datenverkehr von allen Protokollen zu akzeptieren, müssen Sie den Wildcard-Dienst für jede Firewall konfigurieren, indem Sie die Unterstützung für alle Protokolle und Ports angeben.

Um mit der CLI einen Wildcard-Dienst für jede Firewall zu konfigurieren, gehen Sie wie folgt vor:

Geben Sie an der Befehlszeile den folgenden Befehl ein, um die Unterstützung für alle Protokolle und Ports zu konfigurieren:

```
add service <name>@ <serverName> <serviceType> <port_number>
<!--NeedCopy-->
```

Beispiel:

```
add service fw-svc1 10.102.29.5 ANY *
<!--NeedCopy-->
```

Um mit der GUI einen Wildcard-Dienst für jede Firewall zu konfigurieren, gehen Sie wie folgt vor:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.

2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld „Dienste erstellen“ Werte für die folgenden Parameter an, wie hier gezeigt:
   - Dienstname — Name
   - Server — ServerName

   -* Ein erforderlicher Parameter
4. Wählen Sie unter Protokoll die Option Beliebig und unter Port die Option * aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der von Ihnen erstellte Dienst wird im Bereich Dienste angezeigt.

Konfiguration eines Monitors für jeden Dienst

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um Hosts auf der vertrauenswürdigen Seite durch einzelne Firewalls zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht die Konnektivität nur zwischen der NetScaler-Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, das die im Monitor angegebene Ziel-IP-Adresse besitzt. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der Geräte mit dem nächsten Hop von dieser Firewall ausgefallen ist, schließt die Appliance die Firewall beim Load Balancing ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der Geräte für den nächsten Hop ausgefallen ist. Durch das Binden eines transparenten Monitors wird der Dienst als DOWN markiert, wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, und die Firewall wird nicht einbezogen, wenn die Appliance den Firewall-Lastausgleich durchführt.

Das Binden eines transparenten Monitors überschreibt den PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Beispiel:


```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

Die NetScaler-Appliance lernt die Server-L2-Parameter vom Monitor, der an den Dienst gebunden ist. Konfigurieren Sie für UDP-ECV-Monitore eine Empfangszeichenfolge, damit die Appliance die L2-Parameter des Servers lernen kann. Wenn die Empfangszeichenfolge nicht konfiguriert ist und der Server nicht reagiert, lernt die Appliance die L2-Parameter nicht, aber der Dienst ist auf UP eingestellt. Der Traffic für diesen Dienst ist schwarz.

Um eine Empfangszeichenfolge mit der CLI zu konfigurieren:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )] [-send <string>] [-recv <string>]
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor monitor-udp-1 udp-ecv -destip 10.10.10.11 -transparent
    YES  - send "test message"  - recv "site_is_up"
<!--NeedCopy-->
```

Um einen transparenten Monitor mithilfe der GUI zu erstellen und zu binden:

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld „Monitor erstellen“ Werte für die folgenden Parameter an, wie in der Abbildung gezeigt:
   - Vorname*
   - Typ*—Typ
   - Ziel-IP
   - Transparente

   -* Ein erforderlicher Parameter
4. Klicken Sie auf Erstellenund dann auf Schließen. Wählen Sie im Bereich Monitore den Monitor aus, den Sie gerade konfiguriert haben, und stellen Sie sicher, dass die am unteren Bildschirmrand angezeigten Einstellungen korrekt sind.

Konfiguration eines virtuellen Servers zur Lastverteilung des an die Firewalls gesendeten Datenverkehrs

Um jede Art von Datenverkehr auszubalancieren, müssen Sie einen virtuellen Wildcard-Server konfigurieren, der das Protokoll und den Port als beliebigen Wert angibt.

Gehen Sie wie folgt vor, um einen virtuellen Server so zu konfigurieren, dass er den an die Firewalls gesendeten Datenverkehr mithilfe der CLI ausgleicht:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add lb vserver <name>@ <serviceType> <IPAddress> <port_number>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

Gehen Sie wie folgt vor, um einen virtuellen Server so zu konfigurieren, dass er den an die Firewalls gesendeten Datenverkehr mithilfe der GUI ausgleicht:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Wählen Sie unter Protokoll die Option Beliebig und unter IP-Adresse und Port die Option * aus.
4. Klicken Sie auf Erstellenund dann auf Schließen. Der virtuelle Server, den Sie erstellt haben, wird im Bereich Load Balancing Virtual Servers angezeigt.

Konfiguration des virtuellen Servers für den MAC-Rewrite-Modus

Um den virtuellen Server so zu konfigurieren, dass er die MAC-Adresse für die Weiterleitung des eingehenden Datenverkehrs verwendet, müssen Sie den MAC-Rewrite-Modus aktivieren.

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mithilfe der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```


So konfigurieren Sie den virtuellen Server im MAC-Rewrite-Modus mithilfe der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB1), und klicken Sie dann auf Öffnen.
3. Klicken Sie auf der Registerkarte Erweitert unter dem Modus Umleitungsmodus auf Öffnen.
4. Klicken Sie auf OK.

Firewalldienste an den virtuellen Server binden

Um auf einen Dienst auf der NetScaler-Appliance zuzugreifen, müssen Sie ihn an einen virtuellen Wildcard-Server binden.

Gehen Sie wie folgt vor, um Firewalldienste mithilfe der CLI an den virtuellen Server zu binden:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind lb vserver <name>@ <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Gehen Sie wie folgt vor, um Firewalldienste mithilfe der GUI an den virtuellen Server zu binden:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB1), und klicken Sie dann auf Öffnen.
3. Aktivieren Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) auf der Registerkarte Dienste das Kontrollkästchen Aktiv neben dem Dienst, den Sie an den virtuellen Server binden möchten (z. B. Service-HTTP-1).
4. Klicken Sie auf OK.

Konfiguration des Lastausgleichs mit mehreren Firewalls auf der NetScaler-Appliance

Um den Datenverkehr auf beiden Seiten eines NetScaler mithilfe des Firewall-Lastenausgleichs auszugleichen, müssen Sie den Lastausgleich für mehrere Firewalls mithilfe des vServerSpecificMac-Parameters aktivieren.

So konfigurieren Sie den Lastenausgleich mit mehreren Firewalls mithilfe der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:


```
set lb parameter -vServerSpecificMac <status>
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -vServerSpecificMac ENABLED
<!--NeedCopy-->
```

Um den Lastenausgleich mit mehreren Firewalls mithilfe der GUI zu konfigurieren, gehen Sie wie folgt vor:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. Load Balancing-Parameter konfigurieren).
3. Aktivieren Sie im Dialogfeld „Load Balancing-Parameter festlegen“ das Kontrollkästchen Virtual Server Specific MAC.
4. Klicken Sie auf OK.

Konfiguration speichern und überprüfen

Speichern Sie die Konfiguration, wenn Sie die Konfigurationsaufgaben abgeschlossen haben. Sie sollten auch überprüfen, ob die Einstellungen korrekt sind.

Um die Konfiguration mit der CLI zu speichern und zu überprüfen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen transparenten Monitor zu konfigurieren und die Konfiguration zu überprüfen:

- Speichern Sie ns Config
- vserver anzeigen

Beispiel:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
```



```
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.275 millisec
 Done
<!--NeedCopy-->
```

Um die Konfiguration mit der GUI zu speichern und zu überprüfen:

1. Klicken Sie im Detailbereich auf Speichern.

2. Klicken Sie im Dialogfeld Konfiguration speichern auf Ja.
3. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
4. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie in Schritt 5 erstellt haben, und stellen Sie sicher, dass die im Detailbereich angezeigten Einstellungen korrekt sind.
5. Navigieren Sie zu Traffic Management > Load Balancing > Services.
6. Wählen Sie im Detailbereich den Dienst aus, den Sie in Schritt 5 erstellt haben, und stellen Sie sicher, dass die im Bereich Details angezeigten Einstellungen korrekt sind.

Überwachung eines Firewall-Load-Balancing-Setups in einer Umgebung mit mehreren Firewalls

Nachdem die Konfiguration ausgeführt wurde, sollten Sie die Statistiken für jeden Dienst und virtuellen Server anzeigen, um nach möglichen Problemen zu suchen.

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der NetScaler-Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der eingegangenen Anfragen
- Rate der Treffer

So zeigen Sie Statistiken zu virtuellen Servern mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein, um eine Zusammenfassung der Statistiken für alle virtuellen Server anzuzeigen, die derzeit auf der NetScaler-Appliance konfiguriert sind, oder für einen einzelnen virtuellen Server:

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Beispiel:


```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done


<!--NeedCopy-->
```

So zeigen Sie virtuelle Serverstatistiken mithilfe der GUI an:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server > Statistik.
2. Wenn Sie die Statistiken für nur einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf Statistik.

Statistiken eines Dienstes anzeigen

Sie können die Rate von Anfragen, Antworten, Anforderungsbytes, Antwortbytes, aktuellen Clientverbindungen, Anforderungen in Surge-Warteschlange, aktuellen Serververbindungen usw. mithilfe der Dienststatistik anzeigen.

So zeigen Sie die Statistiken eines Dienstes mithilfe der Befehlszeilenschnittstelle an:

Geben Sie in der Befehlszeile Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```


Gehen Sie wie folgt vor, um die Statistiken eines Dienstes mithilfe der GUI einzusehen:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services > Statistik.
2. Wenn Sie die Statistiken nur für einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf Statistiken.

Globaler Serverlastausgleich

May 11, 2023

> **Hinweise:**
>
> - Ab Version 13.0 Build 41.x entsprechen Global Server Load Balancing (GSLB) Bereitstellungen, die die NetScaler Appliance verwenden, vollständig dem DNS-Flaggentag 2019.
> - Die GSLB-Funktion ist in den NetScaler Advance- und Premium Edition-Lizenzen enthalten. Die NetScaler-Optionslizenz wird von der Standard Edition unterstützt.

Für GSLB konfigurierte NetScaler-Appliances bieten Disaster Recovery und stellen die kontinuierliche Verfügbarkeit von Anwendungen sicher, indem sie vor Ausfallpunkten in einem WAN schützen. GSLB verteilt die Last zwischen den Rechenzentren, indem Kundenanfragen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder im Falle eines Ausfalls an die verbleibenden Rechenzentren weitergeleitet werden.

In einer typischen Konfiguration sendet ein lokaler DNS-Server Clientanfragen an einen virtuellen GSLB-Server, an den GSLB-Dienste gebunden sind. Ein GSLB-Dienst identifiziert einen virtuellen Load-Balancing- oder Content-Switching-Server, der sich am lokalen Standort oder an einem Remote-Standort befinden kann. Wenn der virtuelle GSLB-Server einen virtuellen Load Balancing- oder Content-Switching-Server an einem Remote-Standort auswählt, sendet er die IP-Adresse des virtuellen Servers an den DNS-Server. Der DNS-Server sendet es an den Client. Der Client sendet die Anfrage dann erneut an den neuen virtuellen Server mit der neuen IP.

Die GSLB-Entitäten, die Sie konfigurieren müssen, sind die GSLB-Sites, die GSLB-Dienste, die virtuellen GSLB-Server, virtuelle Load Balancing- oder Content-Switching-Server und autoritative DNS (ADNS) -Dienste. Sie müssen MEP auch konfigurieren. Sie können auch DNS-Ansichten konfigurieren, um verschiedenen Teilen Ihres Netzwerks Clients zugänglich zu machen, die von verschiedenen Standorten aus auf das Netzwerk zugreifen.

> **Hinweis:**
>
> Um die GSLB-Funktionen in vollem Umfang nutzen zu können, verwenden Sie ADC-Appliances für Load Balancing oder Content Switching in jedem Rechenzentrum, sodass Ihre GSLB-Konfiguration das proprietäre MEP zum Austausch von Standortmetriken verwenden kann.

So funktioniert GSLB

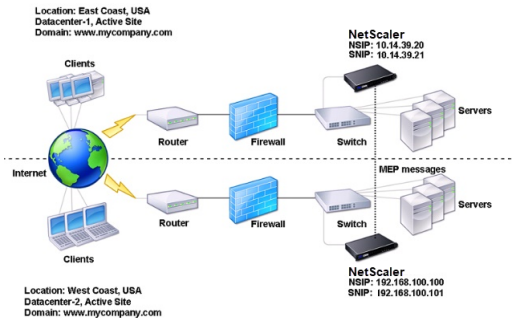
Bei normalem DNS erhält ein Client, wenn er eine DNS-Anfrage (Domain Name System) sendet, eine Liste der IP-Adressen der Domain oder des Dienstes. Im Allgemeinen wählt der Client die erste IP-Adresse in der Liste aus und initiiert eine Verbindung mit diesem Server. Der DNS-Server verwendet eine Technik namens DNS-Round-Robin, um die IPs auf der Liste zu durchsuchen. Es sendet die erste IP-Adresse an das Ende der Liste und erhöht die anderen, nachdem es auf jede DNS-Anfrage geantwortet hat. Diese Technik gewährleistet eine gleichmäßige Verteilung der Last, unterstützt jedoch keine Notfallwiederherstellung, einen auf der Last oder Nähe der Server basierenden Lastausgleich oder Persistenz.

Wenn Sie GSLB auf ADC-Appliances konfigurieren und MEP aktivieren, wird die DNS-Infrastruktur verwendet, um den Client mit dem Rechenzentrum zu verbinden, das die festgelegten Kriterien am besten erfüllt. Die Kriterien können Folgendes bezeichnen:

- Am wenigsten ausgelastetes Rechenzentrum
- Nächstgelegenes Rechenzentrum
- Rechenzentrum, das am schnellsten auf Anfragen vom Standort des Kunden reagiert
- Eine Kombination aus diesen Metriken und SNMP-Metriken.

Eine Appliance verfolgt den Standort, die Leistung, Auslastung und Verfügbarkeit jedes Rechenzentrums. Es verwendet diese Faktoren, um das Rechenzentrum auszuwählen, an das die Client-Anfrage gesendet werden soll.

Die folgende Abbildung zeigt eine grundlegende GSLB-Topologie.



Eine GSLB-Konfiguration besteht aus einer Gruppe von GSLB-Entitäten auf jeder Appliance in der Konfiguration. Zu diesen Entitäten gehören GSLB-Sites, GSLB-Dienste, GSLB-Dienstgruppen, virtuelle GSLB-Server, Load-Balancing-Server, Content-Switching-Server und ADNS-Dienste.

GSLB-Bereitstellungstypen

May 11, 2023

NetScaler-Appliances, die für Global Server Load Balancing (GSLB) konfiguriert sind, ermöglichen die Notfallwiederherstellung und stellen die kontinuierliche Verfügbarkeit von Anwendungen sicher, indem sie vor Ausfallpunkten in einem Wide Area Network (WAN) schützen. GSLB kann die Last zwischen den Rechenzentren verteilen, indem Kundenanfragen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder im Falle eines Ausfalls an die verbleibenden Rechenzentren weitergeleitet werden.

Im Folgenden sind einige der typischen GSLB-Bereitstellungstypen aufgeführt:

- Aktiv-Aktiv-Sitebereitstellung
- Aktiv-Passiv-Sitebereitstellung
- Bereitstellung einer übergeordneten und untergeordneten Topologie

Aktiv-Aktiv-Sitebereitstellung

May 11, 2023

Ein aktiv-aktiver Standort besteht aus mehreren aktiven Rechenzentren. Die Client-Anforderungen werden auf die aktiven Rechenzentren verteilt. Dieser Bereitstellungstyp kann verwendet werden, wenn Sie eine globale Verteilung des Datenverkehrs in einer verteilten Umgebung benötigen.

Alle Sites in einer Aktiv-Aktiv-Bereitstellung sind aktiv, und alle Dienste für eine bestimmte Anwendung/Domäne sind an denselben virtuellen GSLB-Server gebunden. Sites tauschen Metriken über das Metrics Exchange Protocol (MEP) aus. Zu den zwischen den Standorten ausgetauschten Standortmetriken gehören der Status jedes virtuellen Load-Balancing- und Content-Switching-Servers, die aktuelle Anzahl der Verbindungen, die aktuelle Paketrate und die aktuelle Bandbreitennutzung. Die NetScaler Appliance benötigt diese Informationen, um den Lastenausgleich zwischen den Standorten durchzuführen.

Eine aktive und aktive Bereitstellung kann maximal 32 GSLB-Standorte umfassen, da MEP nicht mehr als 32 Standorte synchronisieren kann. In diesem Bereitstellungstyp sind keine Backup-Sites konfiguriert.

Die NetScaler Appliance sendet Clientanforderungen an den entsprechenden GSLB-Site gemäß der in der GSLB-Konfiguration angegebenen GSLB-Methode.

Für eine aktiv-aktive Bereitstellung können Sie die folgenden GSLB-Methoden konfigurieren.

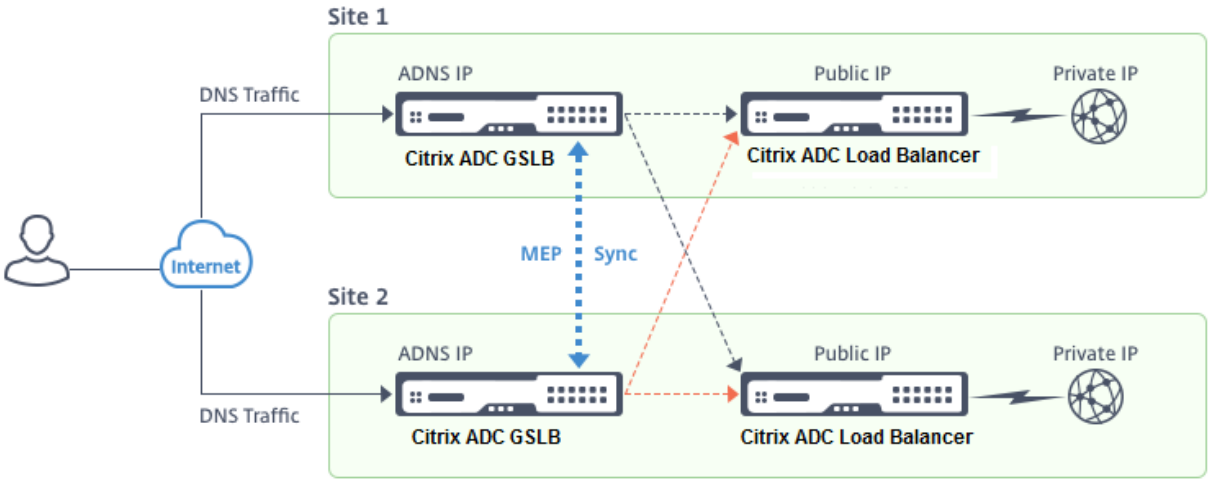
- Runde Robin
- Geringste Verbindungen
- Kleinste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete

- Quell-IP-Hash
- Benutzerdefinierte Last
- Roundtrip-Zeit (RTT)
- Statische Nähe

> Hinweis:
>
> - Wenn MEP deaktiviert ist, werden die folgenden GSLB-Methoden standardmäßig auf die Round Robin-Methode eingestellt.
> - RTT
> - Kleinste Verbindungen
> - Kleinste Bandbreite
> - Kleinste Pakete
> - Kleinste Reaktionszeit
> - Bei der statischen Näherungsmethode GLSB sendet die Appliance die Anforderung an die IP-Adresse des Standorts, die den Näherungskriterien am besten entspricht.
> - Bei der Round Trip Time-Methode dienen die Werte für die dynamische Roundtrip Time (RTT) dazu, die IP-Adresse der Site mit der besten Leistung auszuwählen. RTT ist ein Maß für die Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource.

GSLB Aktiv-Aktiv-Rechenzentrum-Topologie

Im Diagramm sind Standort 1 und Standort 2 aktive GLSB-Sites.



Wenn der Client eine DNS-Anforderung sendet, landet er an einem der aktiven Sites.

Wenn Standort 1 die Clientanforderung empfängt, wählt der virtuelle GSLB-Server an Standort 1 einen virtuellen Load Balancing- oder Content-Switching-Server aus und sendet die IP-Adresse des virtuellen Servers an den DNS-Server, der sie an den Client sendet. Der Client sendet die Anfrage dann erneut an den neuen virtuellen Server unter der neuen IP-Adresse.

Da beide Standorte aktiv sind, bewertet der GSLB-Algorithmus die Dienste an beiden Standorten, wenn er eine Auswahl trifft, die durch die konfigurierte GSLB-Methode bestimmt wird.

Aktiv-Passiv-Standortbereitstellung

August 19, 2021

Ein aktiv-passiver Standort besteht aus einem aktiven und einem passiven Rechenzentrum. Dieser Bereitstellungstyp ist ideal für die Notfallwiederherstellung.

Bei dieser Art der Bereitstellung sind einige Sites (Remotesites) nur für die Notfallwiederherstellung reserviert. Diese Sites nehmen nicht an einer Entscheidungsfindung teil, bis alle aktiven Sites DOWN sind. Ein passiver Standort wird erst betriebsbereit, wenn ein Notfallereignis ein Failover auslöst.

Nachdem Sie das primäre Rechenzentrum konfiguriert haben, replizieren Sie die Konfiguration für das Backupdatenzentrum und legen Sie es als passiven GSLB-Standort fest, indem Sie einen virtuellen GSLB-Server an diesem Standort als virtuellen Backupserver festlegen.

Eine aktive und passive Bereitstellung kann maximal 32 GSLB-Sites umfassen, da MEP nicht mehr als 32 Sites synchronisieren kann.

Für eine aktiv-passive Bereitstellung können Sie die folgenden GSLB-Methoden konfigurieren.

- Runde Robin
- Geringste Verbindungen
- Kleinste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete
- Quell-IP-Hash
- Benutzerdefinierte Last
- Roundtrip-Zeit (RTT)
- Statische Nähe

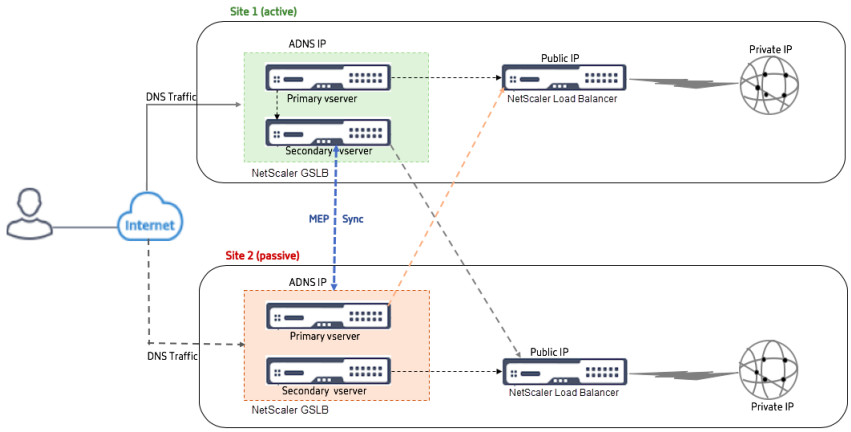
Hinweis:

- Wenn MEP deaktiviert ist, werden die folgenden Algorithmusmethoden standardmäßig Round Robin verwendet.
  - RTT
  - Geringste Verbindungen
  - Geringste Bandbreite
  - Am wenigsten Pakete
  - Kleinste Reaktionszeit

- Bei der statischen Näherungsmethode GLSB sendet die Appliance die Anforderung an die IP-Adresse des Standorts, die den Näherungskriterien am besten entspricht.
- Bei der Round Trip Time -Methode werden die Werte der dynamischen Round Trip Time (RTT) die IP-Adresse des am besten ausführenden Standorts ausgewählt. RTT ist ein Maß für die Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource.

Aktiv-passives GSLB-Rechenzentrumtopologie

Im Diagramm ist Standort 1 ein aktiver Standort und Standort 2 ein passiver Standort mit derselben Konfiguration wie Standort 1.



Wenn Standort 1 ausfällt, wird Standort 2 betriebsbereit.

Wenn der Client eine DNS-Anforderung sendet, kann die Anforderung an jedem der Sites landen. Die Dienste werden jedoch nur von der aktiven Site (Site1) ausgewählt, solange sie UP ist.

Dienste vom passiven Standort (Standort 2) werden nur ausgewählt, wenn der aktive Standort (Standort 1) DOWN ist.

Bereitstellung von Übergeordnet-Untergeordnet-Topologie mit MEP-Protokoll

May 11, 2023

NetScaler GSLB bietet Global Server Load Balancing und Notfallwiederherstellung, indem Mesh-Verbindungen zwischen allen beteiligten Sites hergestellt und intelligente Entscheidungen für den Lastenausgleich getroffen werden. Jede Site kommuniziert mit den anderen, um Server- und Netzwerkmetriken über das Metric Exchange Protocol (MEP) in regelmäßigen Abständen auszutauschen.

Mit der Zunahme der Anzahl der Peersites nimmt das Volumen des MEP-Verkehrs jedoch aufgrund der Mesh-Topologie exponentiell zu. Um dies zu umgehen, können Sie eine Übergeordnet-Untergeordnet-Topologie verwenden. Die übergeordnete und untergeordnete Topologie unterstützt auch größere Bereitstellungen. Zusätzlich zu den 32 übergeordneten Sites können Sie 1024 untergeordnete Sites konfigurieren.

Die übergeordnete und untergeordnete GSLB-Topologie ist ein zweistufiges hierarchisches Design mit den folgenden Merkmalen:

- Auf der obersten Ebene befinden sich übergeordnete Sites, die Peer-Beziehungen zu anderen Eltern haben.
- Jeder Elternteil kann mehrere untergeordnete Sites haben.
- Jede übergeordnete Site tauscht Integritätsinformationen mit den untergeordneten Sites und mit anderen übergeordneten Sites aus.
- Eine untergeordnete Site kommuniziert nur mit ihrer übergeordneter Site.
- In einer Übergeordnet-Untergeordnet-Beziehung für GSLB antwortet nur die übergeordnete Site auf ADNS-Abfragen. Die untergeordneten Sites fungieren als normale Lastausgleichssites.
- Konfigurieren Sie einen ADNS-Dienst oder virtuellen DNS-Lastausgleichsserver nur für die übergeordneten Site.
- Eine übergeordnete Site kann eine normale GSLB-Konfiguration haben, d. h. Dienste von lokalen und allen Remotesites, aber eine untergeordnete Site kann nur lokale Dienste haben. Außerdem sind nur für die übergeordneten Sites virtuelle GSLB-Server konfiguriert.

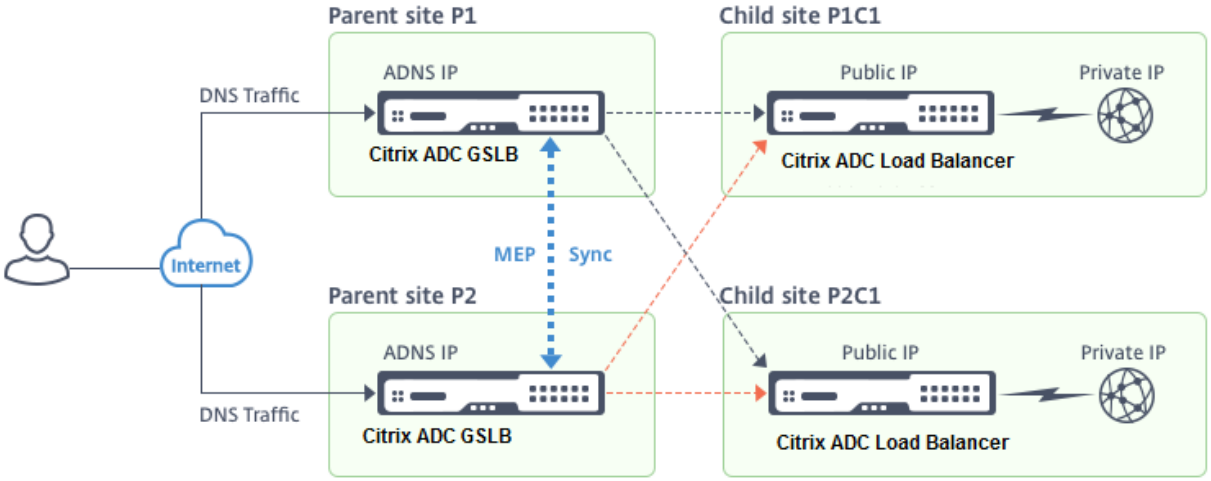
> **Hinweis**
>
> - In einer übergeordneten und untergeordneten Topologie wird der Austausch von Standortmetriken von der unteren von zwei IP-Adressen initiiert. Ab NetScaler Release 11.1 Build 51.x initiieren die übergeordneten Sites jedoch Verbindungen zu den untergeordneten Sites und nicht umgekehrt. Weil die übergeordneten Sites Informationen zu allen untergeordneten Sites im GSLB-Setup enthalten.

- In einer Übergeordnet-Übergeordnet-Verbindung wird der Austausch von Standortmetriken immer noch von der unteren IP von zwei IP-Adressen initiiert.
- In einer Übergeordnet-Untergeordnet-Topologie müssen GSLB-Dienste nicht immer auf einer untergeordneten Site konfiguriert werden. Wenn Sie jedoch über mehr Konfigurationen wie Clientauthentifizierung, Einfügen von Client-IP-Adressen oder andere SSL-spezifische Anforderungen verfügen, müssen Sie für die untergeordnete Site einen expliziten GSLB Service hinzufügen und ihn entsprechend konfigurieren.
- In einer übergeordneten und untergeordneten Topologie können sich der übergeordnete Standort und der untergeordnete Standort auf unterschiedlichen NetScaler-Softwareversionen befinden. Um jedoch die GSLB-Option AutomaticConfigSync verwenden zu können, um die Konfiguration zwischen den übergeordneten Standorten zu synchronisieren, müssen sich

alle übergeordneten Sites auf den SameNetScaler-Softwareversionen befinden. Wenn Sie die Option AutomaticConfigSync nicht verwenden, können sich die übergeordnete Site und die untergeordnete Site auf unterschiedlichen NetScaler-Softwareversionen befinden. Stellen Sie jedoch sicher, dass Sie keine der neuen Funktionen der neuesten Version verwenden. Dies gilt im Allgemeinen auch für zwei NetScaler-Knoten, die an GSLB teilnehmen.

Grundlegende Übergeordnet-Untergeordnet-Topologie

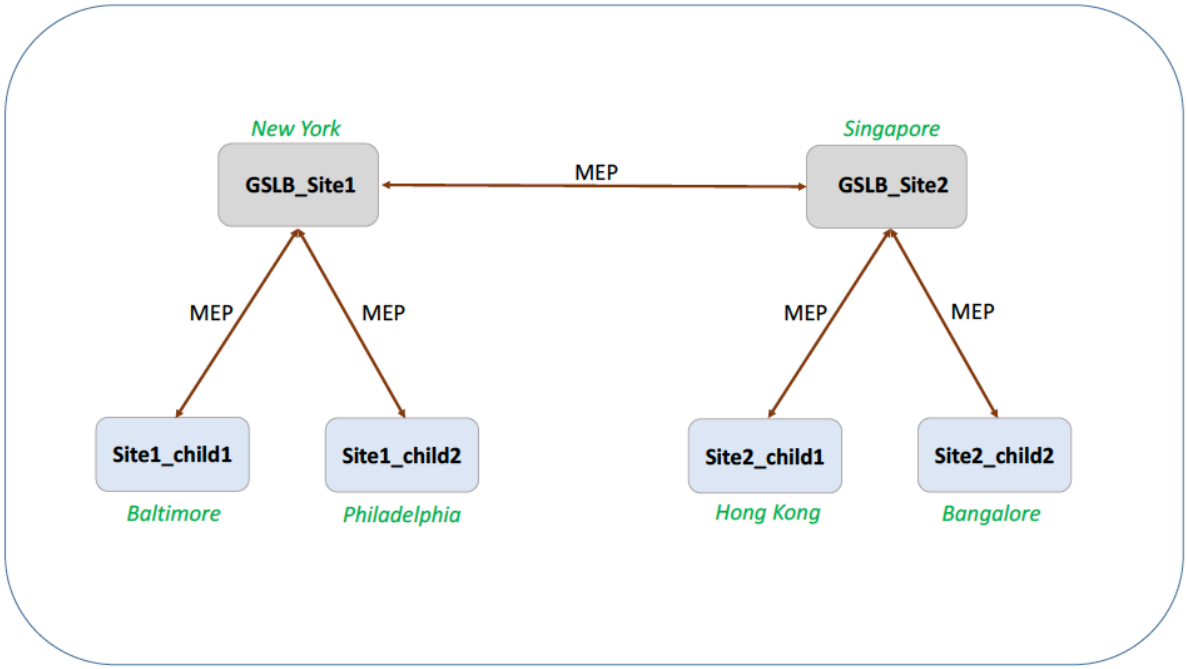
Im Diagramm sind SiteP1 und SiteP2 übergeordnete Sites in einer Peer-Beziehung. Site P1C1 und P2C1 sind die untergeordneten Sites von P1 bzw. P2.



Einrichten einer Übergeordnet-Untergeordnet-Konfiguration für GSLB

Wenn Sie eine Firewall für eine GSLB-Site konfiguriert haben, stellen Sie sicher, dass Port 3011 geöffnet ist.

Das folgende Diagramm zeigt ein Beispiel für eine Übergeordnet-Untergeordnet-Konfiguration.



- Die Konfiguration einer untergeordneten Site umfasst die untergeordnete Site und deren übergeordnete Site, aber keine anderen übergeordneten oder untergeordneten Sites.
- Netzwerkmetriken wie RTT- und Persistenzsitzungsinformationen werden nur über die übergeordneten Sites hinweg synchronisiert. Daher sind Parameter wie nwMetricExchange und sessionExchange standardmäßig auf allen untergeordneten Sites deaktiviert.
- Um die korrekte Übergeordnet-Untergeordnet-Konfiguration zu überprüfen, überprüfen Sie den Status aller GSLB Services, die an die übergeordneten Sites gebunden sind.

So richten Sie über die CLI eine Übergeordnet-Untergeordnet-Konfiguration für GSLB ein:

1. Konfigurieren Sie für jede übergeordnete Site alle untergeordneten Sites, die übergeordneten Peer-Sites und die untergeordneten Sites, die mit den Peer-Sites verknüpft sind:

   Verwenden Sie beim Hinzufügen einer übergeordneten Site den folgenden Befehl:

   ```
   add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
       ipv6_addr|*>]
   <!--NeedCopy-->
   ```

   Verwenden Sie beim Hinzufügen einer untergeordneten Site den folgenden Befehl:

   ```
   add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
       ipv6_addr|*>] [-parentSite <string>]
   <!--NeedCopy-->
   ```

2. Konfigurieren Sie für untergeordneten Sites die jeweilige untergeordnete Site und ordnen Sie die untergeordnete Site auch der übergeordneten Site zu:

> **Hinweis:**
>
> Konfigurieren Sie die übergeordnete Site und die Verknüpfung mit der untergeordneten Sie korrekt. Sie müssen beispielsweise site1_child1 mit GSLB_Site1 konfigurieren. Sie können site1_child1 nicht mit GSLB_Site2 konfigurieren.

Verwenden Sie den folgenden Befehl, um die übergeordnete Site zu konfigurieren, mit der die untergeordnete Site verknüpft ist:

```
1 add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
     ipv6_addr|*>]
2 <!--NeedCopy-->
```

Verwenden Sie den folgenden Befehl, um eine untergeordnete Site hinzuzufügen und sie der übergeordneten Site zuzuordnen:

```
1 add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
     ipv6_addr|*>] [-parentSite <string>]
2 <!--NeedCopy-->
```

Ein vollständiges Beispiel für eine Übergeordnet-Untergeordnet-Konfiguration über die Befehlszeilenschnittstelle finden Sie unter Beispiel einer vollständigen Übergeordnet-Untergeordnet-Konfiguration über die CLI.

> **Hinweis**
>
> Wenn die IP-Adresse des virtuellen Lastausgleichsservers eine private IP-Adresse ist und sich die öffentliche IP-Adresse von dieser IP-Adresse unterscheidet, müssen Sie einen GSLB Service für den lokalen virtuellen Lastausgleichsserver für die untergeordneten Site konfigurieren. Dies ist für die Statistikerfassung zwischen der übergeordneten und der untergeordneten Site erforderlich.
>
> Geben Sie für die untergeordnete Site an der Eingabeaufforderung Folgendes ein:
>
> `add gslb service <name> <private IP/lb vserver IP> http 80 -sitename <childsite name> -publicip <public IP of LB vserver>`
>
> **Beispiel:**
>
> `add gslb service Service-GSLB 192.168.1.3 http 80 -GSLB_Site11 site 11_lb1 172.16.1.1`
>
> Wobei 192.168.1.3 eine private IP-Adresse des virtuellen Lastausgleichsservers und 172.16.1.1 eine öffentliche IP-Adresse des virtuellen Lastausgleichsservers ist.

Backup einer übergeordneten Site

Hinweis: Diese Funktion wurde in NetScaler Release 11.1 Build 51.x eingeführt. Um die Topologie der übergeordneten Backupsite zu verwenden, stellen Sie sicher, dass die übergeordnete Site und die untergeordneten Sites auf NetScaler 11.1 Build 51.x und höher sind.

Die Topologie der übergeordneten Backupsite ist in Szenarien nützlich, in denen viele untergeordnete Sites einer übergeordneten Site zugeordnet sind. Wenn diese übergeordnete Site DOWN ist, sind alle untergeordneten Sites nicht mehr verfügbar. Um dies zu verhindern, können Sie jetzt eine übergeordnete Backupsite konfigurieren, zu der die untergeordneten Sites eine Verbindung herstellen können, wenn die ursprüngliche übergeordnete Site DOWN ist. Die übergeordnete Site sendet die übergeordnete Backupliste über die MEP-Nachrichten an die untergeordneten Sites.

Wenn eine übergeordnete Site DOWN ist, erfahren die anderen übergeordneten Sites in der GSLB über MEP, dass eine bestimmte übergeordnete Site DOWN ist, da MEP für diese übergeordnete Site DOWN ist. Die anderen übergeordneten Sites im GSLB-Setup suchen die Backupkette des Peer-Parent. Die übergeordnete Site mit der höchsten Präferenz übernimmt die untergeordneten Sites der übergeordneten Site, die DOWN ist. Das neue übergeordnete Objekt stellt dann eine Verbindung mit der untergeordneten Site her. Eine untergeordnete Site kann die Verbindung annehmen oder ablehnen, nachdem sie die vorhandenen Verbindungen und die Informationen in der Backupliste ausgewertet hat. Es dauert einige Sekunden, bis die übergeordnete Backupsite die untergeordneten Sites übernommen hat.
Wenn die ursprüngliche übergeordnete Site wieder in Betrieb ist, versucht sie, Verbindungen zu ihren untergeordneten Sites herzustellen, die zu einer anderen übergeordneten Site migriert wurden. Wenn ein Verbindungsversuch erfolgreich ist, wird die untergeordnete Site wieder ihrer ursprünglichen übergeordneten Site zugewiesen.

Hinweis:

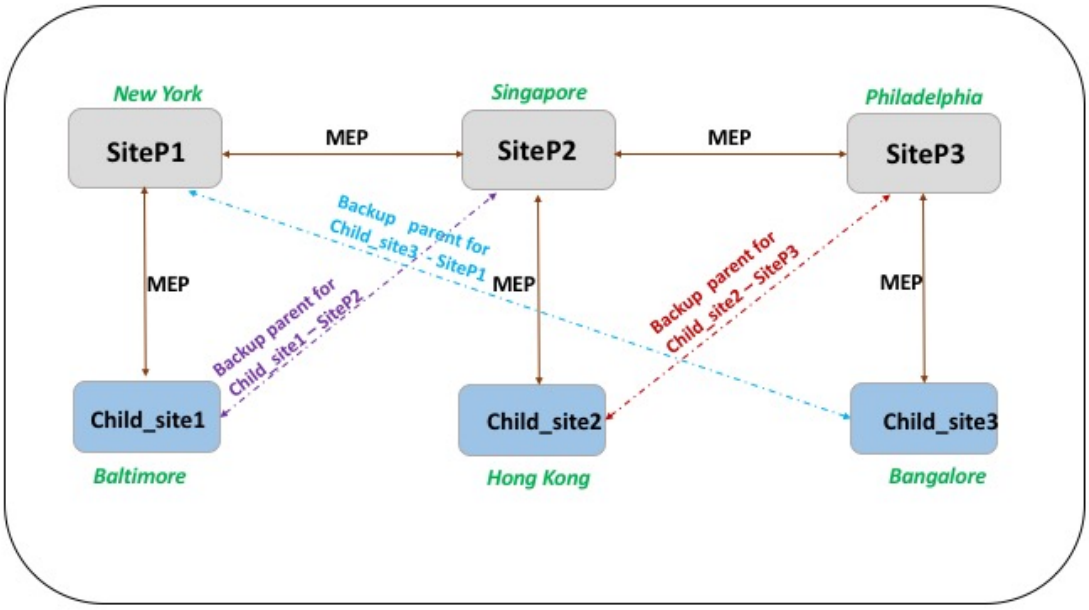
- Nur übergeordnete Sites können als Backups konfiguriert werden, und diese Konfiguration kann nur in der übergeordneten Site durchgeführt werden.
- Alle untergeordneten Sites verwenden die übergeordnete Backupgruppe.
- Die Synchronisierung erfolgt nur auf den übergeordneten Sites. Die Konfiguration der untergeordneten GSLB-Sites ist von der Synchronisierung nicht betroffen. Dies liegt daran, dass die übergeordnete Site und die untergeordneten Sitekonfigurationen nicht identisch sind. Die Konfiguration der untergeordneten Sites besteht nur aus den Details ihrer eigenen und ihrer übergeordneten Site. Außerdem müssen GSLB-Dienste nicht immer in den untergeordneten Sites konfiguriert werden.

Betrachten Sie die in der folgenden Abbildung gezeigte Konfiguration:

- SiteP1, SiteP2 und SiteP3 sind die übergeordneten Sites.
- child_site1, child_site2 und child_site3 sind die untergeordneten Sites von siteP1, siteP2 und siteP3.

- Backup der übergeordneten Sites;
  - SiteP1-Backup-Übergeordnet— SiteP2 (höhere Präferenz) und SiteP3
  - SiteP2 Backup-Übergeordnet— SiteP3 (höhere Präferenz) und siteP1
  - SiteP3 Backup-Übergeordnet— SiteP1 (höhere Präferenz) und SiteP2

Hinweis: Zur Veranschaulichung zeigt die Abbildung nur ein übergeordnetes Backupobjekt für jede übergeordnete Site.



Die folgende Liste fasst das Verhalten der übergeordneten und untergeordneten Sites in verschiedenen Szenarien zusammen:

- Szenario 1: SiteP1 geht DOWN.
  - SiteP2 und SiteP3 erkennen, dass die MEP-Verbindung von SiteP1 DOWN ist. SiteP2 ist in der Einstellungsliste von Backup-Übergeordnet für SiteP1 höher und versucht daher, eine Verbindung zu child_Site1 herzustellen. SiteP3 geht davon aus, dass child_site1 jetzt die untergeordnete Site der übergeordneter SiteP2 ist.
  - SiteP2 sendet Child_Site1 die Liste von Backup-Übergeordnet von SiteP1 (SiteP2 und SiteP3) an child_Site1. child_site1 verwendet die Liste, um zu entscheiden, ob die Verbindung von SiteP2 akzeptiert oder abgelehnt werden soll. Es akzeptiert die Verbindung und wird untergeordnet zu SiteP2.
  - Wenn SiteP1 wieder aktiv ist, sendet sie child_Site1 eine Verbindungsanfrage. Die neue Anforderung hat Vorrang und child_Site 1 migriert zu SiteP1.
- Szenario 2: Nur die MEP-Verbindung zwischen SiteP1 und SiteP2 ist DOWN. child_site1 lehnt die Verbindungsanfrage von SiteP2 ab, da das übergeordnete Objekt, SiteP1, immer noch UP ist.

- Szenario 3: SiteP3 und Child_Site1 erkennen, dass SiteP1 DOWN ist und die MEP-Verbindung zwischen SiteP3 und SiteP2 ebenfalls DOWN ist. SiteP2 erkennt jedoch, dass SiteP1 aktiv ist und die MEP-Verbindung zwischen SiteP1 und SiteP2 UP ist.
  - SiteP2 ergreift keine Maßnahmen.
  - SiteP3 überprüft die Backupliste von SiteP1 und stellt fest, dass SiteP2 eine höhere Präferenz als SiteP3 hat. Aber SiteP2 ist DOWN, also versucht SiteP3 eine Verbindung mit child_site1 herzustellen. child_site1 hat erkannt, dass SiteP1 DOWN ist und akzeptiert daher die Verbindungsanfrage von SiteP3.
  - Jetzt geht die Verbindung zwischen SiteP1 und SiteP2 DOWN. SiteP2 überprüft die Backupliste von SiteP1 und findet sich als das am meisten bevorzugte Backup wieder, sodass es versucht, eine Verbindung zu child_Site1 herzustellen. child_site1 wertet die neue Verbindungsanforderung basierend auf der Liste von SiteP1 aus und findet SiteP2 als das am meisten bevorzugte Backup, sodass es von SiteP3 auf SiteP2 migriert.

So konfigurieren Sie eine übergeordneten Backupsite über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb site <sitename> -backupParentlist <bkp_site1> <bkp_site2> … <
   bkp_site5>
<!--NeedCopy-->
```

<sitename> ist die aktuelle übergeordnete Site.

Beispiel:

Für die übergeordneten Site (SiteP1) werden die Sites (SiteP2 und SiteP3) als übergeordnete Backupsites konfiguriert.

```
set gslb site SiteP1 -backupParentlist SiteP2 SiteP3
<!--NeedCopy-->
```

Hinweis:

- Sie können keine neue Site als übergeordnetes Backupobjekt hinzufügen. Sie müssen zuerst alle Sites hinzufügen und dann die Site als übergeordnetes Backupobjekt konfigurieren.
- Um ein übergeordnetes Backupobjekt zu entfernen, müssen Sie den Befehl unset verwenden, mit dem alle Sites aufgehoben werden, die zuvor als übergeordnete Backupsites konfiguriert wurden.

So konfigurieren Sie eine übergeordnete Backupsite über die GUI

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Sites**.
2. Fügen Sie eine neue Site hinzu oder wählen Sie eine vorhandene Site aus.
3. Wählen Sie beim Erstellen oder Konfigurieren der GSLB-Site das Optionsfeld **Backup Parent Sites** .

GSLB-Konfigurationseinheiten

May 11, 2023

Eine GSLB-Konfiguration besteht aus einer Gruppe von GSLB-Entitäten auf jeder Appliance in der Konfiguration. Zu diesen Entitäten gehören die Folgenden:

- GSLB-Websites
- GSLB-Dienste
- Virtuelle GSLB Server
- Virtuelle Loadbalancing- oder Content Switching-Server
- ADNS-Dienste
- DNS-VIPs

GSLB-Websites

Ein typisches GSLB-Setup besteht aus Rechenzentren, von denen jedes über verschiedene Netzwerkgeräte verfügt, bei denen es sich möglicherweise um NetScaler-Appliances handelt oder auch nicht. Die Rechenzentren werden GSLB-Standorte genannt. Jede GSLB-Site wird von einer NetScaler-Appliance verwaltet, die sich lokal auf dieser Site befindet. Jede dieser Appliances behandelt ihren eigenen Standort als lokalen Standort und alle anderen Standorte, die von anderen Appliances verwaltet werden, als Remote-Standorte.

Wenn die Appliance, die einen Standort verwaltet, die einzige NetScaler-Appliance in diesem Rechenzentrum ist, dient die auf dieser Appliance gehostete GSLB-Site als Platzhalter für die Buchhaltung zu Prüfungszwecken, da keine Metriken erfasst werden können. In der Regel ist dies der Fall, wenn die Appliance nur für GSLB verwendet wird und andere Produkte im Rechenzentrum für den Loadbalancing oder Content Switching verwendet werden.

Beziehungen zwischen GSLB-Standorten

Das Konzept der Websites ist für NetScaler GSLB-Implementierungen von zentraler Bedeutung. Sofern nicht anders angegeben, gehen Websites untereinander eine Beziehung zu Gleichaltrigen ein. Diese Beziehung wird zuerst für den Austausch von Gesundheitsinformationen und dann für die

Verteilung der Last verwendet, die durch den ausgewählten Algorithmus bestimmt wird. In vielen Situationen ist jedoch eine Peer-Relation zwischen allen GSLB-Standorten nicht wünschenswert. Gründe für das Fehlen einer All-Peer-Implementierung könnten sein:

- Um GSLB-Standorte klar zu trennen. Zum Beispiel, um Websites, die an der Lösung von DNS-Abfragen beteiligt sind, von den Websites für das Verkehrsmanagement zu trennen.
- Um das Volumen des Metric Exchange Protocol (MEP) -Datenverkehrs zu reduzieren, der mit zunehmender Anzahl von Peer-Sites exponentiell zunimmt.

Diese Ziele können durch die Nutzung von GSLB-Websites für Eltern und Kinder erreicht werden.

GSLB-Dienste

Ein GSLB-Dienst ist normalerweise eine Darstellung eines virtuellen Lastausgleichs- oder Content-Switching-Servers, obwohl er jede Art von virtuellem Server darstellen kann. Der GSLB-Dienst identifiziert die IP-Adresse, die Portnummer und den Diensttyp des virtuellen Servers. GSLB-Dienste sind an virtuelle GSLB-Server auf den NetScaler-Appliances gebunden, die die GSLB-Sites verwalten. Ein GSLB-Dienst, der an einen virtuellen GSLB-Server im selben Rechenzentrum gebunden ist, ist lokal auf dem virtuellen GSLB-Server. Ein GSLB-Dienst, der an einen virtuellen GSLB-Server in einem anderen Rechenzentrum gebunden ist, ist von diesem virtuellen GSLB-Server entfernt.

> **Hinweis**
>
> Websites und Dienste sind von Natur aus miteinander verknüpft, um auf die Nähe zwischen den beiden hinzuweisen. Das heißt, alle Dienste müssen zu einem Standort gehören und aus Gründen der Nähe wird davon ausgegangen, dass sie sich am selben Standort wie der GSLB-Standort befinden. Ebenso sind Dienste und virtuelle Server verknüpft, sodass die Logik mit den verfügbaren Ressourcen verknüpft ist.

Virtuelle GSLB Server

An einen virtuellen GSLB-Server sind ein oder mehrere GSLB-Dienste gebunden, und der Datenverkehr wird zwischen diesen Diensten lastenausgeglichen. Es wertet die konfigurierten GSLB-Methoden (Algorithmen) aus, um den geeigneten Dienst auszuwählen, an den eine Client-Anfrage gesendet werden soll. Da die GSLB-Dienste entweder lokale Server oder Remote-Server darstellen können, hat die Auswahl des optimalen GSLB-Dienstes für eine Anfrage den Effekt, dass das Rechenzentrum ausgewählt wird, das die Client-Anfrage bearbeiten soll.

Die Domäne, für die der globale Serverlastenausgleich konfiguriert ist, muss an den virtuellen GSLB-Server gebunden sein, da ein oder mehrere an den virtuellen Server gebundene Dienste Anfragen für diese Domäne bearbeiten.

Im Gegensatz zu anderen virtuellen Servern, die auf einer NetScaler Appliance konfiguriert sind, hat ein virtueller GSLB-Server keine eigene virtuelle IP-Adresse (VIP).

Virtuelle Loadbalancing- oder Content Switching-Server

Ein virtueller Loadbalancing- oder Content-Switching-Server steht für einen oder mehrere physische Server im lokalen Netzwerk. Clients senden ihre Anfragen an die virtuelle IP-Adresse (VIP) des virtuellen Loadbalancing- oder Content Switching-Servers, und der virtuelle Server verteilt die Last auf die physischen Server. Nachdem ein virtueller GSLB-Server einen GSLB-Dienst auswählt, der entweder einen lokalen oder einen Remote-Lastausgleich oder einen virtuellen Content Switching-Server darstellt, sendet der Client die Anforderung an die VIP-Adresse dieses virtuellen Servers.

Weitere Informationen zum Lastenausgleich oder zum Content Switching von virtuellen Servern und Diensten finden Sie unter Load Balancing oder Content Switching.

ADNS-Dienste

Ein ADNS-Dienst ist eine spezielle Art von Dienst, der nur auf DNS-Anfragen für Domänen reagiert, für die die NetScaler Appliance autoritativ ist. Wenn ein ADNS-Dienst konfiguriert ist, besitzt die Appliance die IP-Adresse des ADNS-Dienstes und gibt sie bekannt. Beim Empfang einer DNS-Anfrage durch einen ADNS-Dienst sucht die Appliance nach einem virtuellen GSLB-Server, der an diese Domain gebunden ist. Wenn ein virtueller GSLB-Server an die Domain gebunden ist, wird er nach der besten IP-Adresse abgefragt, an die die DNS-Antwort gesendet werden soll.

DNS-VIPs

Eine virtuelle DNS-IP ist eine virtuelle IP-Adresse (VIP), die einen virtuellen DNS-Loadbalancing-Server auf der NetScaler Appliance darstellt. DNS-Anforderungen für Domänen, für die die NetScaler Appliance autorisierend ist, können an eine DNS-VIP gesendet werden.

GSLB-Methoden

May 11, 2023

Im Gegensatz zu herkömmlichen DNS-Servern, die einfach mit den IP-Adressen der konfigurierten Server antworten, antwortet eine für GSLB konfigurierte NetScaler-Appliance mit den IP-Adressen der Dienste, die durch die konfigurierte GSLB-Methode bestimmt werden. Standardmäßig ist der virtuelle GSLB-Server auf die Methode mit der geringsten Verbindung eingestellt. Wenn alle GSLB-Dienste ausgefallen sind, antwortet die Appliance mit den IP-Adressen aller konfigurierten GSLB-Dienste.

GSLB-Methoden sind Algorithmen, die der virtuelle GSLB-Server verwendet, um den GSLB-Dienst mit der besten Leistung auszuwählen. Nachdem der Hostname in der Webadresse aufgelöst wurde, sendet der Client den Datenverkehr direkt an die aufgelöste Dienst-IP-Adresse.

Die NetScaler Appliance bietet die folgenden GSLB-Methoden:

- Runde Robin
- Geringste Verbindungen
- Kleinste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete
- Quell-IP-Hash
- Benutzerdefinierte Last
- Roundtrip-Zeit (RTT)
- Statische Nähe

Damit GSLB-Methoden mit einer Remote-Site funktionieren, muss entweder MEP aktiviert sein oder explizite Monitore müssen an die Remotedienste gebunden sein. Wenn MEP deaktiviert ist, sind die Methoden RTT, Least Connections, Least Bandwidth, Least Packets und Least Response Time standardmäßig Round Robin.

Die Methoden Static Proximity und RTT Load Balancing sind spezifisch für GSLB.

Angeben einer anderen GSLB-Methode als statische Nähe oder dynamische RTT

Informationen zum Round-Robin, zu den kleinsten Verbindungen, der kleinsten Reaktionszeit, der geringsten Bandbreite, den kleinsten Paketen, dem Quell-IP-Hash oder zur benutzerdefinierten Load-Methode finden Sie unter Load Balancing.

So ändern Sie die GSLB-Methode mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver <name> -lbMethod GSLBMethod
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -lbMethod ROUNDROBIN
<!--NeedCopy-->
```

So ändern Sie die GSLB-Methode mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen GSLB-Server aus und klicken Sie auf **Öffnen**.
3. Wählen Sie im Dialogfeld Virtuellen GSLB-Server konfigurieren auf der Registerkarte Methode und Persistenz unter Methode eine Methode aus der Liste Methode auswählen aus.

4. Klicken Sie auf **OK**, und stellen Sie sicher, dass die ausgewählte Methode unten unter Details angezeigt wird.

GSLB-Algorithmen

May 11, 2023

Die folgenden Algorithmen werden für GSLB unterstützt.

- **Round Robin**: Wenn ein virtueller GSLB-Server für die Verwendung der Round-Robin-Methode konfiguriert ist, rotiert er kontinuierlich eine Liste der Dienste, die an ihn gebunden sind. Wenn der virtuelle Server eine Anforderung empfängt, weist er die Verbindung dem ersten Dienst in der Liste zu und verschiebt diesen Dienst dann an das Ende der Liste.
- **Geringste Antwortzeit**: Wenn der virtuelle GSLB-Server für die Verwendung der Methode mit der geringsten Antwortzeit konfiguriert ist, wählt er den Dienst mit dem niedrigsten Wert aus. Wobei niedrigster Wert = aktuell aktive Verbindungen X durchschnittliche Reaktionszeit.

  Sie können diese Methode nur für HTTP- und Secure Sockets Layer (SSL) -Dienste konfigurieren. Die Antwortzeit (auch Time to First Byte oder TTFB genannt) ist das Zeitintervall zwischen dem Senden eines Anforderungspakets an einen Dienst und dem Empfang des ersten Antwortpakets vom Dienst. Die NetScaler Appliance verwendet den Antwortcode 200, um den TTFB zu berechnen.
- **Geringste Verbindungen**: Wenn ein virtueller GSLB-Server so konfiguriert ist, dass er den GSLB-Algorithmus (oder die Methode) mit der geringsten Verbindung verwendet, wählt er den Dienst mit den wenigsten aktiven Verbindungen aus. Dies ist die Standardmethode, da sie in den meisten Fällen die beste Leistung bietet.
- **Geringste Bandbreite**: Ein virtueller GSLB-Server, der für die Verwendung der Methode mit der geringsten Bandbreite konfiguriert ist, wählt den Dienst aus, der derzeit den geringsten Datenverkehr bedient, gemessen in Megabit pro Sekunde (Mbit/s).
- **Wenigste Pakete**: Ein virtueller GSLB-Server, der für die Verwendung der Methode mit den wenigsten Paketen konfiguriert ist, wählt den Dienst aus, der in den letzten 14 Sekunden die wenigsten Pakete empfangen hat.
- **Quell-IP-Hash**: Ein virtueller GSLB-Server, der für die Verwendung der Quell-IP-Hashmethode konfiguriert ist, verwendet den Hashwert der IPv4- oder IPv6-Adresse des Clients, um einen Dienst auszuwählen. Um alle Anforderungen von Quell-IP-Adressen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver weiterzuleiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den netMask-Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

- **Benutzerdefinierte Last**: Benutzerdefinierter Lastausgleich wird für Serverparameter wie CPU-Auslastung, Arbeitsspeicher und Reaktionszeit durchgeführt. Bei Verwendung der benutzerdefinierten Lademethode wählt die NetScaler Appliance normalerweise einen Dienst aus, der keine aktiven Transaktionen verarbeitet. Wenn alle Dienste im GSLB-Setup aktive Transaktionen verarbeiten, wählt die Appliance den Dienst mit der geringsten Last aus. Ein spezieller Monitortyp, der als Lastmonitor bezeichnet wird, berechnet die Last für jeden Dienst im Netzwerk. Die Lastmonitore markieren nicht den Status eines Dienstes, aber sie nehmen Dienste aus der GSLB-Entscheidung heraus, wenn diese Dienste nicht UP sind.
- **Statische Nähe**: GSLB verwendet eine IP-basierte statische Proximity-Datenbank, um die Nähe zwischen dem lokalen DNS-Server des Clients und den GSLB-Sites zu ermitteln. Die NetScaler-Appliance antwortet mit der IP-Adresse eines Standorts, der die Näherungskriterien am besten erfüllt.
- **Roundtrip-Zeit**: RTT ist ein Maß für die Zeit oder Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource. Die NetScaler Appliance untersucht den lokalen DNS-Server des Clients und sammelt RTT-Metrikinformationen. Die Appliance verwendet dann diese Metrik, um ihre Lastausgleichsentscheidung zu treffen. Der globale Serverlastenausgleich überwacht den Echtzeitstatus des Netzwerks und leitet die Clientanforderung dynamisch an das Rechenzentrum mit dem niedrigsten RTT-Wert weiter.
- **API-Methode**: GSLB verwendet eine REST-API, um den GSLB-Dienst mit der besten Leistung zu ermitteln. Wenn GSLB in der API-Methode eine DNS-Anforderung von einem Client empfängt, wertet es die Anforderung anhand der angegebenen Regel aus.

Weitere Informationen finden Sie unter Load Balancing.

Statische Nähe

May 11, 2023

Die statische Proximity-Methode für GSLB verwendet eine auf IP-Adressen basierende statische Proximity-Datenbank, um die Nähe zwischen dem lokalen DNS-Server des Clients und den GSLB-Standorten zu ermitteln. Die NetScaler-Appliance antwortet mit der IP-Adresse eines Standorts, der die Näherungskriterien am besten erfüllt.

Wenn zwei oder mehr GSLB-Standorte an verschiedenen geografischen Standorten denselben Inhalt bereitstellen, verwaltet die NetScaler-Appliance eine Datenbank mit IP-Adressbereichen und verwendet die Datenbank für Entscheidungen über die GSLB-Websites, an die eingehende Clientanfragen weitergeleitet werden sollen.

Damit die statische Proximity-Methode funktioniert, müssen Sie entweder die NetScaler-Appliance so konfigurieren, dass sie eine vorhandene statische Proximity-Datenbank verwendet, die über

eine Standortdatei gefüllt wird, oder der statischen Proximity-Datenbank benutzerdefinierte Einträge hinzufügen. Nachdem Sie benutzerdefinierte Einträge hinzugefügt haben, können Sie deren Standortqualifikatoren festlegen. Nachdem Sie die Datenbank konfiguriert haben, können Sie die statische Nähe als GSLB-Methode angeben.

Weitere Informationen zum Konfigurieren der statischen Nähe finden Sie unter Konfigurieren der statischen Nähe.

Dynamische Roundtrip-Zeitmethode

May 11, 2023

Dynamic Round Trip Time (RTT) ist ein Maß für die Zeit oder Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource. Um dynamisches RTT zu messen, untersucht die NetScaler-Appliance den lokalen DNS-Server des Clients und sammelt RTT-Metrikinformationen. Die Appliance verwendet dann diese Metrik, um ihre Lastausgleichsentscheidung zu treffen. Der globale Serverlastenausgleich überwacht den Echtzeitstatus des Netzwerks und leitet die Clientanforderung dynamisch an das Rechenzentrum mit dem niedrigsten RTT-Wert weiter.

Wenn die DNS-Anfrage eines Clients für eine Domain an die NetScaler-Appliance geht, die als autorisierender DNS für diese Domäne konfiguriert ist, verwendet die Appliance den RTT-Wert, um die IP-Adresse der Site mit der besten Leistung auszuwählen, um sie als Antwort auf die DNS-Anfrage zu senden.

Die NetScaler-Appliance verwendet verschiedene Mechanismen wie ICMP Echo Request or Reply (PING), UDP und TCP, um die RTT-Metriken für Verbindungen zwischen dem lokalen DNS-Server und den teilnehmenden Websites zu sammeln. Die Appliance sendet zunächst eine Ping-Sonde, um den RTT zu ermitteln. Wenn die Ping-Prüfung fehlschlägt, wird eine DNS-UDP-Prüfung verwendet. Wenn diese Prüfung ebenfalls fehlschlägt, verwendet die Appliance eine DNS-TCP-Sonde.

Diese Mechanismen werden auf der NetScaler-Appliance als Load Balancing Monitors dargestellt und sind leicht zu erkennen, da sie das Präfix „ldns“ verwenden. Die drei Monitore sind in ihrer Standardreihenfolge:

- `ldns-ping`
- `ldns-dns`
- `ldns-tcp`

Diese Monitore sind in die Appliance integriert und auf sichere Standardeinstellungen eingestellt. Sie sind jedoch wie jeder andere Monitor der Appliance anpassbar.

Sie können die Standardreihenfolge ändern, indem Sie sie explizit als GSLB-Parameter festlegen. Um

beispielsweise die Reihenfolge als DNS-UDP-Abfrage festzulegen, gefolgt von PING und dann TCP, geben Sie den folgenden Befehl ein:

```
set gslb parameter -ldnsprobeOrder DNS PING TCP
<!--NeedCopy-->
```

Sofern sie nicht angepasst wurden, führt die NetScaler-Appliance UDP- und TCP-Untersuchungen an Port 53 durch. Im Gegensatz zu normalen Load Balancing-Monitoren müssen die Tests jedoch nicht erfolgreich sein, um gültige RTT-Informationen bereitzustellen. ICMP-Portmeldungen, TCP-Resets und DNS-Fehlerantworten, die normalerweise einen Ausfall darstellen würden, sind für die Berechnung des RTT-Werts akzeptabel.

Sobald die RTT-Daten kompiliert wurden, verwendet die Appliance das proprietäre Metrics Exchange Protocol (MEP), um RTT-Werte zwischen den teilnehmenden Standorten auszutauschen. Nach der Berechnung der RTT-Metriken sortiert die Appliance die RTT-Werte, um das Rechenzentrum mit der besten (kleinsten) RTT-Metrik zu identifizieren. „

Wenn RTT-Informationen nicht verfügbar sind (z. B. wenn der lokale DNS-Server eines Clients zum ersten Mal auf die Site zugreift), wählt die NetScaler-Appliance mithilfe der Round-Robin-Methode einen Standort aus und leitet den Client an die Site weiter.

Um die dynamische Methode zu konfigurieren, konfigurieren Sie den virtuellen GSLB-Server der Site für dynamisches RTT. Sie können auch das Intervall festlegen, in dem lokale DNS-Server auf einen anderen Wert als den Standardwert überprüft werden.

Konfigurieren Sie einen virtuellen GSLB-Server für dynamisches RTT

Um einen virtuellen GSLB-Server für dynamisches RTT zu konfigurieren, geben Sie die RTT-Load-Balancing-Methode an.

Die NetScaler-Appliance überprüft regelmäßig die Timing-Informationen für einen bestimmten lokalen Server. Wenn eine Änderung der Latenz den konfigurierten Toleranzfaktor überschreitet, aktualisiert die Appliance ihre Datenbank mit den neuen Timing-Informationen und sendet den neuen Wert an andere GSLB-Standorte, indem sie einen MEP-Austausch durchführt. Der Standard-Toleranzfaktor ist 5 Millisekunden (ms).

Der RTT-Toleranzfaktor muss in der gesamten GSLB-Domäne gleich sein. Wenn Sie es für einen Standort ändern, müssen Sie identische RTT-Toleranzfaktoren auf allen NetScaler-Appliances konfigurieren, die in der GSLB-Domäne bereitgestellt werden.

So konfigurieren Sie einen virtuellen GSLB-Server für dynamisches RTT mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
set gslb vserver <name> -lbMethod RTT -tolerance <value>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -lbMethod RTT -tolerance 10
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen GSLB-Server für dynamisches RTT mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server** und doppelklicken Sie auf den virtuellen Server.

Stellen Sie das Prüfintervall der lokalen DNS-Server ein

Die NetScaler-Appliance verwendet verschiedene Mechanismen wie ICMP Echo Request or Reply (PING), TCP und UDP, um RTT-Metriken für Verbindungen zwischen dem lokalen DNS-Server und den teilnehmenden GSLB-Sites abzurufen. Standardmäßig verwendet die Appliance einen Ping-Monitor und überprüft den lokalen DNS-Server alle 5 Sekunden. Die Appliance wartet dann 2 Sekunden auf die Antwort. Wenn innerhalb dieser Zeit keine Antwort eingeht, verwendet es den TCP-DNS-Monitor für die Untersuchung.

Sie können jedoch das Zeitintervall für die Untersuchung des lokalen DNS-Servers an Ihre Konfiguration anpassen.

So ändern Sie das Prüfintervall mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb monitor <monitorName> <type> -interval <integer> <units> -
    resptimeout <integer> <units>
<!--NeedCopy-->
```

Beispiel:

```
set lb monitor ldns-tcp LDNS-TCP -interval 10 sec -resptimeout 5 sec
<!--NeedCopy-->
```


So ändern Sie das Prüfintervall mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**und doppelklicken Sie auf den Monitor, den Sie ändern möchten (z. B. Ping).

API-Methode

June 2, 2023

Sie können die API-Methode verwenden, um den GSLB-Dienst mit der besten Leistung zu ermitteln. Die API-Methode für GSLB verwendet eine REST-API, um den GSLB-Dienst mit der besten Leistung zu ermitteln.

Wenn GSLB in der API-Methode eine DNS-Anforderung von einem Client empfängt, wertet es die Anforderung anhand der angegebenen Regel aus. Wenn GSLB auf den HTTP-Callout-Ausdruck SYS.HTTP_CALLOUT (<name>) stößt, ruft es eine REST-API-Anfrage an einen HTTP-Callout-Agent auf. GSLB verwendet die Antwort des HTTP-Callout-Agents, um den Dienst mit der besten Leistung zu ermitteln. In der DNS-Antwort gibt GSLB die IP-Adresse des Dienstes mit der besten Leistung an den Client zurück.

So konfigurieren Sie eine GSLB-API-Methode mithilfe der CLI

Gehen Sie wie folgt vor, um die GSLB-API-Methode zu konfigurieren:

1. Konfigurieren Sie ein HTTP-Callout.

   Weitere Informationen finden Sie unter Konfigurieren eines HTTP-Callouts.

   Geben Sie in der Befehlszeile Folgendes ein:

```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-
    port <port>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod (GET | POST)] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)
    > ...] [-bodyExpr <string>] [-fullReqExpr <string>] [-scheme (
    http | https)] [-resultExpr <string>] [-cacheForSecs <secs>] [-
    comment <string>]
<!--NeedCopy-->
```

   Beispiel:

```
add policy httpCallout GSLB_Method_API -IPAddress 208.111.39.237 -
    port 443 -returnType TEXT -hostExpr  "\" hopx.gslb.com\ ""  -
    urlStemExpr  "\" /zones/1/customers/92395/apps/6/decision\ ""
```



```
    -headers Authorization( “Basic 19fbe6db-4332-4e3f-a8bc-
    ee47bdc726f8") -parameters ip(DNS.REQ.OPT.ECS.IP.
    TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme
    https -resultExpr  “HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
    XPATH_JSON(xp%/providers/Val[1]/provider%)”  -cacheForSecs 30
<!--NeedCopy-->
```

2. Geben Sie die API-Methode für den Lastenausgleich an. GSLB wertet die DNS-Anfrage anhand der angegebenen Regel aus.

   Geben Sie in der Befehlszeile Folgendes ein:

```
add gslb vserver <name> <serviceType>  [-lbMethod <lbMethod>] [-
    backupLBMethod <backupLBMethod>] -rule <expression>
<!--NeedCopy-->
```

   Beispiel:

```
add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN
     -rule  “sys.http_callout(GSLB_Method_API)”
<!--NeedCopy-->
```

Beispielkonfiguration für die Integration von GSLB und ITM mit API als LB-Methode

Diese Konfiguration ermöglicht es GSLB, die Aspekte der Internetsichtbarkeit des Intelligent Traffic Management (ITM) von Citrix zu verwenden, um den GSLB-Dienst mit der besten Leistung zu ermitteln.

```
/* Enable ns features */

enable ns feature lb gslb cs

/* This is a named expression that is used in the HTTP callout, used
    for result expression. */

add policy expression exp1 "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
    XPATH_JSON(xp%/providers/Val[1]/provider%)"

/* This is a named expression that is used in HTTP callout, used for
    host expression. */

add policy expression exp2 ""hopx.cedexis.com""

/* This is the HTTP callout configured to request the ITM for the GSLB
    decision. */
```



```
14
15 add policy httpCallout ITM_OpenMix_API -IPAddress 208.111.39.237 -port
       80 -returnType TEXT -hostExpr exp2 -urlStemExpr ""/zones/1/customers
       /61770/apps/3/decision"" -headers Authorization("Basic a310697a-1d69
       -48bf-8f36-55742a8e894e") -parameters ip(DNS.REQ.OPT.ECS.IP.
       TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme http -
       resultExpr exp1 -cacheForSecs 30
16
17 /* Add service 1 */
18 add service sg1 98.136.103.24 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
        -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
       svrTimeout 360 -CKA NO -TCPB NO -CMP NO
19
20 /* Add service 2 */
21 add service sg2 172.217.194.113 HTTP 80 -gslb NONE -maxClient 0 -maxReq
        0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180
       -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
22
23 /* Add ADNS service */
24
25 add service adns1 10.102.217.106 ADNS 53 -gslb NONE -maxClient 0 -
       maxReq 0 -cip DISABLED -usip NO -useproxyport NO -sp OFF -cltTimeout
        120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO
26
27 /* Add lb vserver 1 for service 1 */
28 add lb vserver lbvs1 HTTP 10.102.217.116 80 -persistenceType NONE -
       cltTimeout 180
29
30 /* Add lb vserver 2 for service 2 */
31 add lb vserver lbvs2 HTTP 10.102.217.117 80 -persistenceType NONE -
       cltTimeout 180
32
33 /* Bind service 1 to lb vserver 1 */
34
35 bind lb vserver lbvs1 sg1
36
37 /* Bind service 2 to lb vserver 2 */
38
39 bind lb vserver lbvs2 sg2
40
41 /* Configure API GSLB method on GSLB virtual server to call the HTTP
       callout. This HTTP callout requests the ITM for the GSLB decision
       and returns GSLB service name, which should serve the request. */
42
43 add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN -
```



```
    rule "sys.http_callout(ITM_OpenMix_API)" -tolerance 0 -ECS ENABLED
44
45 /* Add GSLB site */
46
47 add gslb site site1 10.102.217.106 -publicIP 10.102.217.106
48
49 /* Add GSLB service 1 */
50
51 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai_1
    10.102.217.116 HTTP 80 -publicIP 10.102.217.116 -publicPort 80 -
    maxClient 0 -siteName site1 -sitePersistence HTTPRedirect -
    sitePrefix gs2. -cltTimeout 180 -svrTimeout 360 -downStateFlush
    ENABLED
52
53 /* Add GSLB service 2 */
54
55 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai 10.102.217.117
    HTTP 80 -publicIP 10.102.217.117 -publicPort 80 -maxClient 0 -
    siteName site1 -sitePersistence HTTPRedirect -sitePrefix gs1. -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
56
57 /* Bind the GSLB service 1 to GSLB server 1 */
58 bind gslb vserver vs1 -serviceName
    aws_ec2_ap_south_1_asia_pacific_mumbai_1
59
60 /* Bind the GSLB service 2 to GSLB server 2 */
61 bind gslb vserver vs1 -serviceName
    aws_ec2_ap_south_1_asia_pacific_mumbai
62
63 /* Bind a domain name to the GSLB virtual server */
64 bind gslb vserver vs1 -domainName testruchit104.com -TTL 5
65
66 <!--NeedCopy-->
```

Statische Nähe konfigurieren

May 11, 2023

Damit die statische Proximity-Methode funktioniert, müssen Sie entweder die NetScaler-Appliance so konfigurieren, dass sie eine vorhandene statische Proximity-Datenbank verwendet, die über eine Standortdatei gefüllt wird, oder der statischen Proximity-Datenbank benutzerdefinierte Einträge hinzufügen. Nachdem Sie benutzerdefinierte Einträge hinzugefügt haben, können Sie deren

Standortqualifikatoren festlegen. Nachdem Sie die Datenbank konfiguriert haben, können Sie die statische Nähe als GSLB-Methode angeben.

Dieses Dokument enthält die folgenden Informationen:

- Hinzufügen einer Standortdatei zur Erstellung einer statischen Proximity-Datenbank
- Hinzufügen benutzerdefinierter Einträge zu einer statischen Proximity-Datenbank
- Einstellung der Standortqualifikatoren
- Angabe der Proximity-Methode
- Statische GSLB-Näherungsdatenbank synchronisieren

Hinzufügen einer Standortdatei zum Erstellen einer statischen Proximitydatenbank

June 19, 2023

Eine statische Näherungsdatenbank ist eine UNIX-basierte ASCII-Datei. Einträge, die aus einer Standortdatei zu dieser Datenbank hinzugefügt wurden, werden als statische Einträge bezeichnet. Es kann nur eine Standortdatei auf eine NetScaler-Appliance geladen werden. Durch das Hinzufügen einer neuen Standortdatei wird die vorhandene Datei überschrieben. Die Anzahl der Einträge in der statischen Näherungsdatenbank wird durch den konfigurierten Speicher in der NetScaler-Appliance begrenzt.

Die statische Näherungsdatenbank kann im Standardformat oder in einem Format erstellt werden, das aus kommerziell konfigurierten Datenbanken Dritter (wie www.maxmind.com und www.ip2location.com) abgeleitet ist.

Die NetScaler-Appliance enthält die folgenden zwei IP-Geolocation-Datenbankdateien. Dies sind GeoLite2-Dateien, die von MaxMind veröffentlicht wurden.

- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4
- Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6

Diese Datenbankdateien sind in einem von der NetScaler-Appliance unterstützten Format im Verzeichnis /var/netscaler/inbuilt_db verfügbar.

Sie können diese IP-Geolokalisierungsdatenbanken als Standortdatei für die statische Näherungsbasierte GSLB-Methode oder in standortbasierten Richtlinien verwenden.

Diese Datenbanken unterscheiden sich in den Details, die sie bereitstellen. Es gibt keine strikte Durchsetzung des Datenbankdateiformats, außer dass die Standarddatei über Format-Tags verfügt. Bei den

Datenbankdateien handelt es sich um ASCII-Dateien, die ein Komma als Feldtrennzeichen verwenden. Es gibt Unterschiede in der Struktur der Felder und der Darstellung von IP-Adressen in den Sites.

Der Formatparameter beschreibt die Struktur der Datei für die NetScaler-Appliance. Wenn Sie einen falschen Wert für die Formatoption angeben, können die internen Daten beschädigt werden.

> **Hinweis**
>
> - Wenn das Verzeichnis /var/netscaler/inbuilt_db/ nach einem Upgrade die Datenbankdatei (Citrix_Netscaler_InBuilt_GeoIP_DB.csv) aus den früheren NetScaler-Softwareversionen enthält, wird die Datei beibehalten.
> - Der Standardspeicherort der Datenbankdatei ist /var/netscaler/locdb, und bei einem Hochverfügbarkeitssetup (HA) muss eine identische Kopie der Datei auf beiden NetScaler-Appliances am selben Speicherort vorhanden sein.
> - Wenn die Standortdatei an einem anderen Ort als dem Standardspeicherort gespeichert ist, geben Sie den Pfad der Standortdatei an.
> - Für Admin-Partitionen lautet der Standardpfad: /var/partitions/<partitionName> /netscaler/locdb.
> - Einige Datenbanken enthalten kurze Ländernamen gemäß ISO-3166 und lange Ländernamen. Der NetScaler verwendet Kurznamen beim Speichern und Abgleichen von Qualifizierern.
> - Um eine statische Näherungsdatenbank zu erstellen, melden Sie sich bei der UNIX-Shell der NetScaler-Appliance an und erstellen Sie mit einem Editor eine Datei mit den Standortdetails in einem der von NetScaler unterstützten Formate.
> - Die NetScaler-Appliance wird mit der GeoLite2-Datenbank (IPv4 und IPv6) ausgeliefert, NetScaler verwaltet oder aktualisiert die MaxMind GeoLite2-Datenbank jedoch nicht regelmäßig. Bei Bedarf können Sie die GeoLite2-Datenbank von www.maxmind.com abrufen und in das NetScaler-Datenbankformat konvertieren. Weitere Informationen finden Sie unter Skript zum Konvertieren des MaxMind GeoLite2-Datenbankformats in das NetScaler-Datenbankformat.

So fügen Sie eine statische Standortdatei mit der CLI hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add locationFile <locationFile> [-format <format>]
-  show locationFile
<!--NeedCopy-->
```

Beispiel:

```
add locationFile /var/netscaler/locdb/nsgeo1.0 -format netscaler
Done
```



```
3
4 show locationFile
5 Location File: /var/netscaler/locdb/nsgeo1.0
6 Format: netscaler
7  Done
8 >
9 <!--NeedCopy-->
```

Beispiel:

```
1 add locationFile /var/netscaler/inbuilt_db/
     Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4 -format netscaler
2
3 add locationFile6 /var/netscaler/inbuilt_db/
     Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6 -format netscaler
4 <!--NeedCopy-->
```

So fügen Sie eine statische Standortdatei mit der GUI hinzu:

1. Navigieren Sie zu **AppExpert** > **Standort**, und klicken Sie auf die Registerkarte **Statische Datenbank** .
2. Klicken Sie auf **Hinzufügen**, um eine statische Standortdatei hinzuzufügen.

Sie können eine importierte Standortdateidatenbank anzeigen, indem **Sie das Dialogfeld Datenbank anzeigen** im Konfigurationsdienstprogramm verwenden. Es gibt kein CLI-Äquivalent.

So zeigen Sie eine statische Standortdatei mit der GUI an:

1. Navigieren Sie zu **AppExpert** > **Standort**, und klicken Sie auf die Registerkarte **Statische Datenbank** .
2. Wählen Sie eine Datei mit statischem Speicherort aus, und klicken Sie in der Liste **Aktion** auf **Datenbank anzeigen**.

So konvertieren Sie eine Standortdatei in das NetScaler-Format:

Wenn Sie eine Standortdatei hinzufügen, wird sie standardmäßig im NetScaler-Format gespeichert. Sie können eine Standortdatei anderer Formate in das NetScaler-Format konvertieren.

> **Hinweis**: Auf die Option `nsmap` kann nur über die Befehlszeilenschnittstelle zugegriffen werden. Die Konvertierung ist nur in das NetScaler-Format möglich.

Um das statische Datenbankformat zu konvertieren, geben Sie an der CLI-Eingabeaufforderung den folgenden Befehl ein:

```
1 nsmap -f <inputFileFormat> -o <outputFileName> <inputFileName>
2 <!--NeedCopy-->
```

Beispiel:


```
1  nsmap -f ip-country-region-city -o nsfile.ns ip-country-region-city.
       csv
2  <!--NeedCopy-->
```

Skript zum Konvertieren des MaxMind GeoLite2-Datenbankformats in das NetScaler-Datenbankformat

MaxMind GeoIP-Datenbank kann nicht direkt in NetScaler verwendet werden. Die MaxMind GeoIP-Datenbank muss in das NetScaler-Format konvertiert und dann für die IP-Siteerkennung in der statischen GSLB-Näherungsmethode und anderen Funktionen wie Richtlinien geladen werden.
Sie können ein Skript verwenden, um das GeoLite2-Datenbankformat in das NetScaler-Datenbankformat zu konvertieren. Dieses Skript kann verwendet werden, um sowohl IPv4- als auch IPv6-Dateien zu konvertieren.
Das Skript ist an folgendem Ort verfügbar: https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format

Schritte zum Konvertieren der GeoIP2-Datenbank in das NetScaler-Format

1. Laden Sie die GeoLite2 City- oder GeoLite2-Länderdatenbank im.csv-Format von herunter https://dev.maxmind.com/geoip/geoip2/geolite2/.
2. Kopieren Sie die Datei in ein NetScaler-Verzeichnis (z. B. /var). Entpacken Sie die Datei mit dem folgenden Shell-Befehl, der ein Verzeichnis mit demselben Namen erstellen würde.

   ```
   tar -xf <filename>
   ```

3. Laden Sie das Skript Convert_GeoIPDB_to_NetScaler_Format.pl von https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format herunter und kopieren Sie es in das in Schritt #2 erstellte Verzeichnis.
4. Führen Sie den folgenden Befehl aus, um die zulässigen Optionen für die Skriptausführung zu überprüfen:

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -help
   ```

   Verschiedene Optionen sind verfügbar:

   - <filename> IPv4-Ausgabedatei. Standardname der Ausgabedatei: Netscaler_Maxmind_GeoIP_DB_IP
   - -p <filename> IPv6-Ausgabedatei. Standardname der Ausgabedatei: Netscaler_Maxmind_GeoIP_DI
   - -logfile <filename> Datei mit einer Liste von Ereignissen/Nachrichten
   - -debug Druckt alle Nachrichten auf STDOUT

5. Führen Sie den folgenden Befehl aus, um das GeoLite2-Datenbankformat in das NetScaler-Datenbankformat zu konvertieren.

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl
   ```

   > **Hinweis:** Der Vorgang kann bis zu 5 Minuten dauern.

   Die im Skript verwendeten Standarddateinamen sind die der MaxMind GeoLite2 City-basierten Datenbank. Wenn Sie die GeoLite2-Länderdatenbank heruntergeladen haben, müssen Sie die Eingabedateinamen entsprechend der Liste angeben.

   - `-b <filename>` Name der zu konvertierenden IPv4-Blockdatei. Standarddateiname: GeoLite2-City-Blocks-IPv4.csv
   - `-i <filename>` Name der zu konvertierenden IPv6-Blockdatei. Standarddateiname: GeoLite2-City-Blocks-IPv6.csv
   - `-l <filename>` Name der zu konvertierenden Standortdatei. Standarddateiname: GeoLite2-City-Locations-en.csv

   Beispiel:

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -b GeoLite2-City-Blocks-IPv4.csv -i GeoLite2-City-Blocks-IPv6.csv -l  GeoLite2-City-Locations-en.csv
   <!--NeedCopy-->
   ```

   Im Folgenden sind die Ausgabedateien aufgeführt, die nach der Ausführung des Skripts generiert wurden

   - Netscaler_Maxmind_GeoIP_DB_IPv4.csv
   - Netscaler_Maxmind_GeoIP_DB_IPv6.csv

6. Sobald die Konvertierung der Datenbank in das NetScaler-Format abgeschlossen ist, verwenden Sie den folgenden Befehl, um sie zu verwenden.

   ```
   add locationFile <locationFile>
   ```

Fügen Sie eine statische Datenbankdatei eines Drittanbieters auf einer NetScaler-Appliance hinzu

Führen Sie die folgenden Schritte aus, um eine statische Datenbankdatei eines Drittanbieters auf einer NetScaler-Appliance hinzuzufügen.

1. Besorgen Sie sich die Standortdatenbankdatei von einem Drittanbieter, z. B. www.maxmind.com.

   > **Hinweis:**
   >
   > Wenn Sie die Standortdatenbankdatei von www.maxmind.com herunterladen, können Sie

> sie mit dem leicht verfügbaren Skript in das NetScaler-Datenbankformat konvertieren. Informationen zur Verwendung des Skripts finden Sie unter Skript zum Konvertieren des MaxMind GeoLite2-Datenbankformats in das NetScaler-Datenbankformat.
>
> Bei Standortdatenbanken, die von anderen Drittanbietern heruntergeladen wurden, müssen Sie sie in das NetScaler-Datenbankformat konvertieren, bevor Sie sie einer NetScaler-Appliance hinzufügen.

2. Führen Sie den folgenden Befehl aus, um eine statische Standortdatei hinzuzufügen:

```
add location file <locationfile Name>
<!--NeedCopy-->
```

> **Hinweis:**
>
> - Wenn die Standortdatenbankdatei nicht am Standardspeicherort **/var/netscaler/locdb** abgelegt wird, muss `<locationfile Name>` den Speicherort der Datei zusammen mit dem Dateinamen enthalten.
> - Bevor Sie den Befehl `add location file <locationfile Name>` ausführen:
>   - Make sure that the location database file is present in one of the directories of the NetScaler appliance.
>   - Run the `sync HA files` command on the high availability setup and the `sync cluster files` command in a cluster setup. These commands ensure that the location database file is copied to the secondary appliance of the high availability pair and peer nodes of the cluster.

3. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Standortdatenbank geladen ist:

```
show location parameter
<!--NeedCopy-->
```

Dieser Befehl zeigt die Parameter an, z. B. die Anzahl der statischen Einträge. Es können maximal 3M-1-Einträge (3 Millionen minus eins) geladen werden. Wenn die Datenbank geladen wird, wird der Befehl `Loading: In progress` angezeigt. Nach Abschluss des Ladevorgangs wird der Befehl `Loading: Idle` angezeigt. Wenn die Datenbank nicht richtig geladen wurde, zeigt dieser Befehl auch eine Fehlermeldung an.

4. Führen Sie den folgenden Befehl aus, um den Standort der GSLB-Site anzuzeigen:

```
show gslb service
<!--NeedCopy-->
```


> **Hinweis**
>
> - Wenn die Datenbank korrekt geladen wurde, wird der Standort der GSLB-Sites automatisch in die Datenbank eingetragen.
> - Sie können in der Konfiguration auf der Appliance nur eine Standortdatei angeben.
> - Wenn keine Übereinstimmung für eine eingehende IP-Adresse gefunden wird, wird die Anforderung mit der Round-Robin-Methode verarbeitet.

5. Führen Sie den folgenden Befehl aus, um die GSLB-Methode auf der Appliance zu konfigurieren:

```
set gslb vserver GSLBVserverName -lbMethod MethodType
<!--NeedCopy-->
```

Benutzerdefinierte Einträge zu einer statischen Proximitydatenbank hinzufügen

May 11, 2023

Benutzerdefinierte Einträge haben Vorrang vor statischen Einträgen in der Proximity-Datenbank. Sie können maximal 3000 benutzerdefinierte Einträge hinzufügen. Bei einem benutzerdefinierten Eintrag kennzeichnen Sie alle ausgelassenen Qualifikationsmerkmale mit einem Sternchen (*) und setzen Sie den Parameter in doppelte Anführungszeichen, falls Qualifikationsmerkmale einen Punkt oder ein Leerzeichen im Namen haben. Die ersten 31 Zeichen werden für jedes Qualifikationsmerkmal bewertet. Sie können auch den Längen- und Breitengrad der geografischen Position des IP-Adressbereichs angeben, um einen Dienst mit der GSLB-Methode für statische Nähe auszuwählen.

So fügen Sie benutzerdefinierte Einträge mithilfe der Befehlszeilenschnittstelle hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um der statischen Proximity-Datenbank einen benutzerdefinierten Eintrag hinzuzufügen und die Konfiguration zu überprüfen.

```
add location < IPfrom> < IPto> <preferredLocation> [-longitude <integer
    >[-latitude <integer>]]
show location
<!--NeedCopy-->
```

Beispiel:

```
> add location 192.168.100.1 192.168.100.100 *.us.ca.mycity
Done
<!--NeedCopy-->
```



```
> show location
1) IP from 192.168.100.1    IP to 192.168.100.100
Continent.Country.REgion.City.ISP.Organization =
North America.us.ca.mycity.*.
Coordinated: Not specified
Done
<!--NeedCopy-->
```

Parameter für das Hinzufügen benutzerdefinierter Einträge

- **Von IP-Adresse**: Erste IP-Adresse im Bereich, die in punktierter Dezimalschreibweise angegeben ist.

  Dies ist ein zwingendes Argument.

- **An IP-Adresse**: Letzte IP-Adresse in dem Bereich, der in punktierter Dezimalschreibweise angegeben ist.

  Dies ist ein zwingendes Argument.

- **Standortname**: Eine Reihe von Qualifikationsmerkmalen in punktierter Schreibweise beschreibt die geografische Position des IP-Adressbereichs. Jedes Qualifikationsmerkmal ist spezifischer als das vorhergehende, wie in continent.country.region.city.isp.organization. Zum Beispiel „na.us.ca.San Jose.ATT.Citrix“.

  Dies ist ein zwingendes Argument. Maximale Länge: 197

  > **Hinweis:**
  >
  > Ein Qualifikationsmerkmal, das einen Punkt (.) oder ein Leerzeichen () enthält, muss in doppelte Anführungszeichen gesetzt werden.

- **Längengrad**: Der numerische Wert in Grad gibt den Längengrad der geografischen Position des IP-Adressbereichs an.
  Maximalwert: 180

- **Breitengrad**: Der numerische Wert in Grad gibt den Breitengrad der geografischen Position des IP-Adressbereichs an.
  Maximalwert: 180

  > **Hinweis:**
  >
  > Längen- und Breitengradparameter werden verwendet, um einen Dienst mit der GSLB-Methode für statische Nähe auszuwählen. Wenn sie nicht angegeben sind, basiert die Auswahl auf den für den Standort angegebenen Qualifikationsmerkmalen.

So fügen Sie mithilfe des Konfigurationsdienstprogramms benutzerdefinierte Einträge hinzu

Navigieren Sie zu **AppExpert** > **Standort**, klicken Sie auf die Registerkarte **Benutzerdefinierte Einträge** und fügen Sie die benutzerdefinierten Einträge hinzu.

Festlegen von Standortkennzeichnungen

May 11, 2023

Die zur Implementierung der statischen Nähe verwendete Datenbank enthält den Standort der GSLB-Standorte. Jeder Standort hat einen IP-Adressbereich und bis zu sechs Qualifizierer für diesen Bereich. Die Qualifikationszeichen sind wörtliche Zeichenfolgen und werden zur Laufzeit in einer vorgeschriebenen Reihenfolge verglichen. Jeder Standort muss mindestens einen Qualifier haben. Die Qualifier-Labels definieren die Bedeutung der Qualifier (Kontext), die benutzerdefiniert sind. NetScaler hat zwei eingebaute Kontexte:

Geografischer Kontext, der die folgenden Qualifier-Labels hat:

- Qualifier 1 — “Kontinent”
- Qualifikationsspiel 2 — “Land”
- Qualifier 3 — “Staat”
- Qualifikationsspiel 4 — “Stadt”
- Qualifikationsspiel 5 — “ISP”
- Qualifier 6 — “Organisation”

Benutzerdefinierte Einträge, die die folgenden Qualifier-Labels haben:

- Qualifikationsspiel 1 — “Qualifikationsspiel 1”
- Qualifikationsspiel 2 — “Qualifikationsspiel 2”
- Qualifikationsspiel 3 — “Qualifikationsspiel 3”
- Qualifikationsspiel 4 — “Qualifikationsspiel 4”
- Qualifikationsspiel 5 — “Qualifikationsspiel 5”
- Qualifikationsspiel 6 — “Qualifikationsspiel 6”

Wenn der geografische Kontext ohne Kontinentkennzeichen festgelegt ist, wird Kontinent vom Land abgeleitet. Sogar die eingebauten Qualifier-Labels basieren auf dem Kontext, und die Beschriftungen können geändert werden. Diese Qualifier-Labels geben die Standorte an, die den IP-Adressen zugeordnet sind, die für statische Näherungsentscheidungen verwendet werden.

Um eine statische Proximity-basierte Entscheidung zu treffen, vergleicht die NetScaler-Appliance die von der IP-Adresse des lokalen DNS-Server-Resolvers abgeleiteten Standortattribute (Qualifikatoren)

mit den Standortattributen der teilnehmenden Sites. Wenn nur eine Site übereinstimmt, gibt die Appliance die IP-Adresse dieser Site zurück. Wenn es mehrere Übereinstimmungen gibt, ist die ausgewählte Site das Ergebnis eines Round Robin auf den übereinstimmenden GSLB-Sites. Wenn es keine Übereinstimmung gibt, ist die ausgewählte Site das Ergebnis eines Round Robin auf allen konfigurierten Standorten. Eine Seite, die keine Qualifikationsspiele hat, wird als Spiel betrachtet.

Mit den GEO-Regeln für den standortbasierten Richtlinienausdruck können Sie Platzhalterübereinstimmungen überprüfen. Diese Funktion prüft, ob Platzhalterqualifizierer mit anderen Qualifikationszeichen übereinstimmen, einschließlich Nicht-Platzhalter oder nicht. Die Platzhalterübereinstimmung erfolgt mithilfe des Attributs `matchWildcardtoany`, das dem Befehl `set locationParameter` hinzugefügt wurde.

Das Attribut `matchWildcardtoany` kann auf die folgenden Werte festgelegt werden:

- **Ja:** Wildcard-Qualifikationsspiele entsprechen allen anderen Qualifikationsspielen.
- **Nein:** Platzhalter-Qualifikationsspiele stimmen nicht mit Nicht-Wildcard-Qualifikationsspielen überein, sondern stimmen mit anderen Platzhalter-Qualifikationsspielen überein. Die Standardoption ist " **Nein**".
- **Ausdruck:** Platzhalterqualifikatoren in einem Ausdruck entsprechen jedem Qualifier an einer LDNS-Position, aber Platzhalterqualifikatoren an der LDNS-Position entsprechen nicht den Platzhalterkennungszeichen in einem Ausdruck, bei dem es sich nicht um Platzhalter handelt.

Beispiel:

```
add dns policy1 "CLIENT.IP.SRC.MATCHES_LOCATION("Continent.country
    \*.\*.\*.\* \ ")"  <action>
<!--NeedCopy-->
```

So stellen Sie die Standortparameter über die CLI ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set locationparameter -context <context> -q1label <string> [-q2label <
    string>] [-q3label <string>] [-q4label <string>] [-q5label <string>]
     [-q6label <string>] -matchWildcardtoany [Yes | No | Expression]
<!--NeedCopy-->
```

Beispiel:

```
set locationparameter -context custom -q1label asia -matchWildcardtoany
    Yes
<!--NeedCopy-->
```


So stellen Sie die Standortparameter über die GUI ein

1. Navigieren Sie zu **Traffic Management > GSLB > Datenbank und Einträge**.
2. Klicken Sie unter **Einstellungen**auf **Standortparameter ändern**.
3. Legen Sie auf der Seite **Standortparameter konfigurieren** die Standortparameter fest.

Konfigurationsbeispiel (mit CLI)

Erwägen Sie die folgende Netzwerkkonfiguration:

- Name des virtuellen GSLB-Servers: gv1
- IP-Adresse des virtuellen GSLB-Servers: 1.1.1.2
- GSLB-Dienst: gsvc1 an gv1 gebunden
- Speicherort DB-Dateiname: sample.csv
- Geolokalisierungsqualifizierer: Die Qualifizierer 1 und 2 sind konfiguriert. Rest ist so eingestellt, dass es mit dem Platzhalter übereinstimmt.
  - Qualifikationsspiel 1 — Asien
  - Qualifikationsspiel 2 — IR
  - Qualifikationsspiel 3-*
  - Qualifikationsspiel 4-*
  - Qualifikationsspiel 5-*
  - Qualifikationsspiel 6-*
- DNS-Richtlinie — Die Richtlinie pol1 ist so eingestellt, dass die Pakete verworfen werden, wenn es eine Übereinstimmung gibt.

Stellen Sie den Standortparameter ein und konfigurieren Sie die DNS-Richtlinie wie folgt:

```
set locationParameter -q2label Country_Code -q3label Subdivision_1_Name
    -q4label Subdivision_2_Name -q5label City

add locationFile "/var/netscaler/inbuilt_db/sample.csv"

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0

add dns policy pol1 "CLIENT.IP.SRC.MATCHES_LOCATION("Asia.IR
   .\*.\*.\*.\*")||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SY.\*.\*.\*.\*"
   )||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SD.\*.\*.\*.\*")||CLIENT.IP.
   SRC.MATCHES_LOCATION("Asia.KP.\*.\*.\*.\*")||CLIENT.IP.SRC.
   MATCHES_LOCATION("North America.CU.\*.\*.\*.\*")||CLIENT.IP.SRC.
   MATCHES_LOCATION("Europe.UA.Crimea.\*.\*.\*.\*")"
   dns_default_act_Drop

bind dns global pol1 1 -gotoPriorityExpression 65535 -type REQ_DEFAULT

```



```
add gslb service gsvc1 1.1.1.2 HTTP 80 -publicIP 1.1.1.2 -publicPort 80
     -maxClient 0 -healthMonitor NO -siteName s1 -cltTimeout 180 -
    svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver gv1 -serviceName gsvc1

bind gslb vserver gv1 -domainName www.gslbnew.com -TTL 5
<!--NeedCopy-->
```

Fügen Sie der Location-DB-Datei die folgenden Clienteinträge hinzu. In diesem Beispiel lautet der DB-Dateiname des Speicherorts sample.csv:

```
10.106.24.170,10.106.24.190,,,,,,,8.0000,47.0000

10.102.82.170,10.102.82.190,Asia,,,,,,-73.9924,40.7553

10.106.24.140,10.106.24.150,,IR,,,,,51.4231,35.6961
<!--NeedCopy-->
```

Gemäß der vorherigen Konfiguration haben die Clients zwischen 10.106.24.170 und 10.106.24.190 keine Platzhalterqualifizierer definiert. Die Clients zwischen 10.106.24.140 und 10.106.24.150 haben den Qualifizierer 2 als IR.

Setzen Sie den Match-Platzhalter-Qualifizierer auf NEIN:

```
set locationparameter -matchWildcardtoany no
<!--NeedCopy-->
```

Wenn der Übereinstimmungs-Platzhalter-Qualifizierer auf NEIN festgelegt ist, stimmen die Platzhalter-Qualifizierer nur mit den definierten Platzhalter-Qualifizierern überein. Es stimmt nicht mit anderen Nicht-Wildcard-Qualifizierern überein.

- Die DNS-Abfragen, die 10.106.24.147 kommen, entsprechen dem definierten Platzhalter-Qualifizierer (Qualifizierer 2 = IR). Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Wenn Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem Client 10.106.24.147 ausführen, zeigt die Ausgabe, dass die Server nicht erreichbar waren.

  ```
  root@ns#  dig @10.102.82.13 www.gslbnew.com

  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  ; (1 server found)
  ;; global options: +cmd
  ;; connection timed out; no servers could be reached
  <!--NeedCopy-->
  ```


- Die DNS-Abfragen von 10.106.24.180 stimmen nicht mit den definierten Qualifizierern überein. Die DNS-Richtlinie tritt nicht in Kraft und die Abfragen werden verarbeitet.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem 10.106.24.180-Client aus. Die Ausgabe zeigt die IP-Adresse des virtuellen GSLB-Servers.

```
root@ns# dig @10.102.82.13 www.gslbnew.com

; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gslbnew.com. IN    A

;; ANSWER SECTION:
www.gslbnew.com.    5   IN  A   1.1.1.2

;; Query time: 12 msec
;; SERVER: 10.102.82.13#53(10.102.82.13)
;; WHEN: Tue Mar 29 22:46:40 UTC 2022
;; MSG SIZE  rcvd: 60
<!--NeedCopy-->
```

Setzen Sie den Match-Platzhalter-Qualifizierer auf Ja:

```
set locationparameter -matchWildcardtoany yes
<!--NeedCopy-->
```

Wenn der Match-Platzhalter-Qualifizierer auf Ja festgelegt ist, stimmen die Platzhalter-Qualifizierer mit allen Platzhaltern überein (definierter und Nicht-Platzhalter-Qualifizierer).

- Die DNS-Abfragen, die 10.106.24.147 kommen, entsprechen dem definierten Qualifizierer (Qualifizierer 2 = IR). Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem Client 10.106.24.147 aus. Die Ausgabe zeigt, dass Server nicht erreichbar waren.

```
root@ns#  dig @10.102.82.13 www.gslbnew.com
```



```
2
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
7   <!--NeedCopy-->
```

- Die Abfragen von 10.106.24.180 stimmen mit den Nicht-Wildcard-Qualifizierern überein. Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem 10.106.24.180-Client aus. Die Ausgabe zeigt, dass Server nicht erreichbar waren.

```
1   root@ns# dig @10.102.82.13 www.gslbnew.com
2
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
7   <!--NeedCopy-->
```

Stellen Sie den Match-Platzhalter-Qualifizierer auf Ausdruck:

```
1 set locationparameter -matchWildcardtoany expression
2 <!--NeedCopy-->
```

Wenn der Übereinstimmungs-Platzhalter-Qualifizierer auf Ausdruck festgelegt ist, stimmen die Platzhalter-Qualifizierer entweder mit dem in der DNS-Richtlinie verfügbaren Qualifizierer oder mit den in der Speicherort-DB-Datei verfügbaren Qualifizierern überein.

- Die DNS-Abfragen, die 10.106.24.147 kommen, stimmen mit den definierten Platzhalter-Qualifizierern in der DNS-Richtlinie überein. Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem Client 10.106.24.147 aus. Die Ausgabe zeigt, dass Server nicht erreichbar waren.

```
1   root@ns#  dig @10.102.82.13 www.gslbnew.com
2
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
7   <!--NeedCopy-->
```


- Die Abfragen von 10.106.24.180 stimmen nicht mit den Qualifizierern in der DNS-Richtlinie überein. Daher tritt die DNS-Richtlinie nicht in Kraft und die Abfragen werden verarbeitet.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem 10.106.24.180-Client aus. Die Ausgabe zeigt die IP-Adresse des virtuellen GSLB-Servers.

```
root@ns# dig @10.102.82.13 www.gslbnew.com

; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gslbnew.com.  IN   A

;; ANSWER SECTION:
www.gslbnew.com.    5   IN  A   1.1.1.2

;; Query time: 12 msec
;; SERVER: 10.102.82.13#53(10.102.82.13)
;; WHEN: Tue Mar 29 22:46:40 UTC 2022
;; MSG SIZE  rcvd: 60
<!--NeedCopy-->
```

Angeben der Näherungsmethode

January 19, 2021

Wenn Sie die statische Näherungsdatenbank konfiguriert haben, können Sie die statische Nähe als GLSB-Methode angeben.

So legen Sie die statische Nähe mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die statische Nähe zu konfigurieren und die Konfiguration zu überprüfen:


```
set gslb vserver <name> -lbMethod STATICPROXIMITY
show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -lbMethod STATICPROXIMITY
show gslb vserver
<!--NeedCopy-->
```

So legen Sie die statische Nähe mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server, und doppelklicken Sie auf den virtuellen Server.
2. Klicken Sie auf den Abschnitt **Methode**, und wählen Sie in der Dropdownliste **Methode wählen** die Option **STATICPROXIMITY** aus.

GSLB statische Näherungsdatenbank synchronisieren

January 19, 2021

Für die Synchronisierung einer statischen GSLB-Datenbank (Global Server Load Balancing, Global Server Load Balancing, Global Server Load Balancing, GSLB) muss einer der Sites als Master-GSLB-Knoten identifiziert werden. Jeder Standort in der Topologie kann als Master-Knoten bezeichnet werden. Der Rest der GSLB-Knoten wird automatisch als Slave-Knoten bezeichnet.

Durch das Synchronisieren statischer GSLB-Näherungsdatenbanken werden die Dateien im Verzeichnis /var/netscaler/locdb über die Slave-Knoten hinweg synchronisiert. Während des Synchronisierungsprozesses ruft der Master-Knoten die laufende Konfiguration von jedem der Slave-Knoten ab und vergleicht sie mit der Konfiguration auf dem Master-Knoten. Der Master-GSLB-Knoten verwendet das rsync-Programm, um die statische Näherungsdatenbank über die Slave-Knoten hinweg zu synchronisieren. Um den Synchronisierungsvorgang zu beschleunigen, nimmt das rsync-Programm nur genügend Änderungen vor, um die Unterschiede zwischen den beiden Dateien zu beseitigen. Der Synchronisierungsvorgang kann nicht zurückgesetzt werden.

Im folgenden Beispiel wird Site2, eine Slave-Site, mit Mastersite Site1 synchronisiert. Der Administrator gibt den Befehl **sync gslb config** auf Site1 ein:

```
sync gslb config -nowarn
Sync Time: Feb 24 2014 14:56:16
Retrieving local site info: ok
```



```
Retrieving all participating gslb sites info:
0 bytes in 0 blocks
ok
site1[Master]:
        Getting Config: ok
site2[Slave]:
        Syncing gslb static proximity database: ok
        Getting Config: ok
        Comparing config: ok
        Applying changes: ok
 Done
<!--NeedCopy-->
```

Konfigurieren der Site-zu-Site-Kommunikation

May 11, 2023

Die GSLB-Kommunikation zwischen Standorten erfolgt zwischen den RPC-Knoten (Remote Procedure Call), die den kommunizierenden Standorten zugeordnet sind. Ein Master-GSLB-Standort stellt Verbindungen zu Slave-Standorten her, um GSLB-Konfigurationsinformationen zu synchronisieren und Standortmetriken auszutauschen.

Ein RPC-Knoten wird automatisch erstellt, wenn eine GSLB-Site erstellt wird, und ihm werden ein intern generierter Benutzername und ein Passwort zugewiesen. Die NetScaler-Appliance verwendet diesen Benutzernamen und dieses Kennwort, um sich während des Verbindungsaufbaus an Remote-GSLB-Sites zu authentifizieren. Für einen RPC-Knoten sind keine Konfigurationsschritte erforderlich, Sie können jedoch ein Passwort Ihrer Wahl angeben, die Sicherheit erhöhen, indem Sie die Informationen, die GSLB-Sites austauschen, verschlüsseln und eine Quell-IP-Adresse für den RPC-Knoten angeben.

Die Appliance benötigt eine NetScaler-eigene IP-Adresse, die als Quell-IP-Adresse für die Kommunikation mit anderen GSLB-Sites verwendet werden kann. Standardmäßig verwenden die RPC-Knoten entweder eine Subnetz-IP-Adresse (SNIP), aber Sie können eine IP-Adresse Ihrer Wahl angeben.

In den folgenden Themen werden das Verhalten und die Konfiguration von RPC-Knoten auf der NetScaler-Appliance beschrieben:

Das Passwort eines RPC-Knotens ändern

Citrix empfiehlt Ihnen, die Kommunikation zwischen Websites in Ihrem GSLB-Setup zu sichern, indem Sie das Passwort jedes RPC-Knotens ändern. Nachdem Sie das Passwort für den RPC-Knoten

der lokalen Site geändert haben, müssen Sie die Änderung manuell an den RPC-Knoten an jedem der Remote-Sites weitergeben.

Das Passwort wird in verschlüsselter Form gespeichert. Sie können überprüfen, ob sich das Passwort geändert hat, indem Sie den Befehl show RpcNode verwenden, um die verschlüsselte Form des Passworts vor und nach der Änderung zu vergleichen.

> **Hinweis:** GSLB verwendet ein internes Benutzerkonto. Zur Erhöhung der Sicherheit empfiehlt Citrix, dass Sie auch das interne Benutzerkontokennwort ändern. Das Kennwort des internen Benutzerkontos wird durch das RPC-Knotenkennwort geändert.

So ändern Sie das Passwort eines RPC-Knotens mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile die folgenden Befehle ein, um das Passwort eines RPC-Knotens zu ändern:

```
set ns rpcNode <IPAddress> {
 -password }

show ns rpcNode
<!--NeedCopy-->
```

Beispiel:

```
> set rpcNode 192.0.2.4 -password mypassword
 Done
> show rpcNode
.
.
.
2)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
    SrcIP:  *               Secure:  OFF
Done
>

<!--NeedCopy-->
```

So löschen Sie das Passwort eines RPC-Knotens mithilfe der Befehlszeilenschnittstelle

Um das Passwort eines RPC-Knotens mithilfe der CLI zu deaktivieren, geben Sie den Befehl unset RpcNode, die IP-Adresse des RPC-Knotens und den Kennwortparameter ohne Wert ein.

So ändern Sie das Passwort eines RPC-Knotens mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu System > Netzwerk > RPC, wählen Sie den RPC-Knoten aus und ändern Sie das Passwort.

Verschlüsseln Sie den Austausch von Site-Metriken

Sie können die Informationen, die zwischen GSLB-Sites ausgetauscht werden, sichern, indem Sie die sichere Option für die RPC-Knoten im GSLB-Setup festlegen. Wenn die sichere Option gesetzt ist, verschlüsselt die NetScaler-Appliance die gesamte Kommunikation, die vom Knoten an andere RPC-Knoten gesendet wird.

Um den Austausch von Site-Metriken mithilfe der Befehlszeilenschnittstelle zu verschlüsseln

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den Austausch von Site-Metriken zu verschlüsseln und die Konfiguration zu überprüfen:

```
set ns rpcNode <IPAddress> [-secure ( YES | NO )]
show rpcNode
<!--NeedCopy-->
```

Beispiel:

```
> set rpcNode 192.0.2.4 -secure YES
 Done
>
> show rpcNode
.
.
.
3)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e SrcIP:
    192.0.2.3     Secure:  ON
 Done
>
<!--NeedCopy-->
```

So deaktivieren Sie den sicheren Parameter mithilfe der Befehlszeilenschnittstelle

Um den sicheren Parameter mithilfe der CLI zu deaktivieren, geben Sie den Befehl unset RpcNode, die IP-Adresse des RPC-Knotens und den sicheren Parameter ohne Wert ein.

So verschlüsseln Sie den Austausch von Site-Metriken mithilfe des NetScaler-Konfigurationsprogramms

1. Navigieren Sie zu System > Netzwerk > RPC und doppelklicken Sie auf einen RPC-Knoten.
2. Wählen Sie die Option **Sicher** und klicken Sie auf **OK**.

Quell-IP-Adresse für einen RPC-Knoten konfigurieren

Standardmäßig verwendet die NetScaler-Appliance eine NetScaler-eigene Subnetz-IP-Adresse (SNIP) als Quell-IP-Adresse für einen RPC-Knoten. Sie können die Appliance jedoch so konfigurieren, dass sie eine bestimmte SNIP-Adresse verwendet. Wenn eine SNIP-Adresse nicht verfügbar ist, kann die GSLB-Site nicht mit anderen Websites kommunizieren. In einem solchen Szenario müssen Sie entweder die NSIP-Adresse oder eine virtuelle IP-Adresse (VIP) als Quell-IP-Adresse für einen RPC-Knoten konfigurieren. Eine VIP-Adresse kann nur dann als Quell-IP-Adresse eines RPC-Knotens verwendet werden, wenn der RPC-Knoten ein Remote-Knoten ist. Wenn Sie eine VIP-Adresse als Quell-IP-Adresse konfigurieren und die VIP-Adresse entfernen, verwendet die Appliance eine SNIP-Adresse.

> **Hinweis**
>
> Ab NetScaler 11.0.64.x können Sie die Appliance so konfigurieren, dass sie die GSLB-Site-IP-Adresse als Quell-IP-Adresse für einen RPC-Knoten verwendet.

So geben Sie mithilfe der Befehlszeilenschnittstelle eine Quell-IP-Adresse für einen RPC-Knoten an

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Quell-IP-Adresse für einen RPC-Knoten zu ändern und die Konfiguration zu überprüfen:

```
set ns rpcNode <IPAddress> [-srcIP <ip_addr|ipv6_addr|*>]
show ns rpcNode
<!--NeedCopy-->
```

Beispiel:

```
set rpcNode 192.0.2.4 -srcIP 192.0.2.3
Done
show rpcNode
<!--NeedCopy-->
```

```
IPAddress: 192.0.2.4 Password: d336004164d4352ce39e SrcIP: 192.0.2.3
    Secure: OFF
Done
<!--NeedCopy-->
```


So deaktivieren Sie den Quell-IP-Adressparameter mithilfe der Befehlszeilenschnittstelle

Um den Quell-IP-Adressparameter mithilfe der CLI zu deaktivieren, geben Sie den unset RpcNodeCommand, die IP-Adresse des RPC-Knotens und den Parameter srcIP ohne Wert ein.

So geben Sie mithilfe des NetScaler-Konfigurationsprogramms eine Quell-IP-Adresse für einen RPC-Knoten an

1. Navigieren Sie zu System > Netzwerk > RPC und doppelklicken Sie auf einen RPC-Knoten.
2. Geben Sie im Feld Quell-IP-Adresse die IP-Adresse ein, die der RPC-Knoten als Quell-IP-Adresse verwenden soll, und klicken Sie auf OK.

> **Wichtig**
>
> Die Quell-IP-Adresse kann nicht zwischen den an GSLB teilnehmenden Standorten synchronisiert werden, da die Quell-IP-Adresse für einen RPC-Knoten für jede NetScaler-Appliance spezifisch ist. Nachdem Sie eine Synchronisierung erzwungen haben (mit dem Befehl sync gslb config —ForceSync oder durch Auswahl der Option ForceSync in der GUI), müssen Sie die Quell-IP-Adressen auf den anderen NetScaler Appliances manuell ändern.

Konfigurieren des Metrikaustauschprotokoll

September 1, 2023

Die Rechenzentren in einem GSLB-Setup tauschen Metriken miteinander über das Metrics Exchange Protocol (MEP) aus, ein proprietäres Protokoll für die NetScaler-Appliance. Der Austausch der metrischen Informationen beginnt, wenn Sie eine GSLB-Site erstellen. Diese Metriken umfassen Last-, Netzwerk- und Persistenzinformationen.

MEP ist für die Zustandsprüfung von Rechenzentren erforderlich, um deren Verfügbarkeit sicherzustellen. Eine Verbindung zum Austausch von Netzwerkmetriken (Round-Time) kann von jedem der am Austausch beteiligten Rechenzentren initiiert werden. Eine Verbindung zum Austausch von Standortmetriken wird jedoch immer von dem Rechenzentrum mit der niedrigeren IP-Adresse initiiert. Standardmäßig verwendet das Rechenzentrum eine Subnetz-IP-Adresse (SNIP), um eine Verbindung zur IP-Adresse eines anderen Rechenzentrums herzustellen. Sie können jedoch eine bestimmte SNIP-, virtuelle IP-Adresse (VIP) oder die NSIP-Adresse als Quell-IP-Adresse für den Metrikenaustausch konfigurieren. Der Kommunikationsprozess zwischen GSLB-Sites verwendet den TCP-Port 3011 oder 3009, daher muss dieser Port auf Firewalls geöffnet sein, die sich zwischen den NetScaler-Appliances befinden.

Hinweis: Sie können eine SNIP- oder eine GSLB-Site-IP-Adresse als Quell-IP-Adresse für den Metrikaustausch konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Quell-IP-Adresse für

einen RPC-Knoten.

Wenn die Quell- und Zielsites (der Standort, der eine MEP-Verbindung initiiert, bzw. der Standort, der die Verbindungsanforderung empfängt) sowohl private als auch öffentliche IP-Adressen konfiguriert haben, tauschen die Sites MEP-Informationen mithilfe der öffentlichen IP-Adressen aus.

Sie können Monitore auch binden, um den Zustand der Remote-Dienste zu überprüfen, wie unter "Überwachung von GSLB-Diensten beschrieben. " Wenn Monitore gebunden sind, steuert der Metrikaustausch nicht den Status des Remote-Dienstes. Wenn ein Monitor an einen Remote-Service gebunden ist und der Metrikaustausch aktiviert ist, steuert der Monitor den Systemstatus. Durch die Bindung der Monitore an den Remote-Service kann die NetScaler-Appliance mit einem Lastenausgleichsgerät interagieren, das nicht von NetScaler stammt. Die NetScaler-Appliance kann Geräte überwachen, die nicht von NetScaler stammen, kann auf ihnen jedoch keinen Lastenausgleich durchführen, es sei denn, die Monitore sind an alle GSLB-Dienste gebunden und es werden nur statische Lastausgleichsmethoden (wie Round Robin, statische Nähe oder Hash-basierte Methoden) verwendet.

Mit NetScaler Version 11.1.51.x oder höher können Sie zur Vermeidung unnötiger Dienstunterbrechungen eine Zeitverzögerung festlegen, um GSLB-Dienste als DOWN zu kennzeichnen, wenn eine MEP-Verbindung ausfällt.

MEP-Status in einem Hochverfügbarkeits-Setup

In einem Hochverfügbarkeits-Setup stellt der primäre Knoten Verbindungen zu den Remote-Sites her und der MEP-Status wird nicht vom primären Knoten zu den sekundären Knoten synchronisiert. Daher bleibt der MEP-Status im sekundären Knoten DOWN. Wenn der sekundäre Knoten zum primären Knoten wird, stellt er MEP-Verbindungen mit dem neuen GSLB-Standort her und aktualisiert den MEP-Status entsprechend.

Den Austausch von Site-Metriken aktivieren

Zu den zwischen den GSLB-Standorten ausgetauschten Standortmetriken gehören der Status jedes virtuellen Load-Balancing- oder Content-Switching-Servers, die aktuelle Anzahl der Verbindungen, die aktuelle Paketrate und Informationen zur aktuellen Bandbreitennutzung.

Die NetScaler-Appliance benötigt diese Informationen, um den Lastenausgleich zwischen den Standorten durchzuführen. Das Austauschintervall der Standortmetrik beträgt 1 Sekunde. Ein GSLB-Remote-Dienst muss an einen lokalen virtuellen GSLB-Server gebunden sein, um den Austausch von Standortmetriken mit dem Remotedienst zu ermöglichen.

So aktivieren oder deaktivieren Sie den Austausch von Site-Metriken mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile die folgenden Befehle ein, um Site Metric Exchange zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
set gslb site <siteName> -metricExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Beispiel:

```
set gslb site Site-GSLB-East-Coast -metricExchange ENABLED
set gslb site Site-GSLB-East-Coast -metricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie den Austausch von Site-Metriken mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**und wählen Sie die Site aus.
2. Wählen **Sie im Dialogfeld GSLB-Site konfigurieren** die Option **Metric Exchange** aus.

Austausch von Netzwerkmetriken aktivieren

Wenn Ihre GSLB-Sites die Load-Balancing-Methode (Round-Time, RTT) verwenden, können Sie den Austausch von RTT-Informationen über den lokalen DNS-Dienst des Clients aktivieren oder deaktivieren. Diese Informationen werden alle 5 Sekunden ausgetauscht.

Weitere Informationen zum Ändern der GSLB-Methode in eine auf RTT basierende Methode finden Sie unter GSLB-Methoden.

So aktivieren oder deaktivieren Sie den Austausch von Netzwerkmetrikinformationen mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den Informationsaustausch über Netzwerkmetriken zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
set gslb site <siteName> -nwmetricExchange (ENABLED|DISABLED)
show gslb site <<siteName>
<!--NeedCopy-->
```

Beispiel:


```
set gslb site Site-GSLB-East-Coast -nwmetricExchange ENABLED
set gslb site Site-GSLB-East-Coast -nwmetricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie den Informationsaustausch über Netzwerkmetriken mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites.**
2. Wählen **Sie im Dialogfeld GSLB-Site konfigurieren** die Option **Network Metric Exchange** aus.

Konfiguration einer Zeitverzögerung für die GSLB-Dienste, die als DOWN markiert werden, wenn eine MEP-Verbindung unterbrochen wird

Wenn sich der Status einer MEP-Verbindung zu einem Remote-Site in DOWN ändert, wird der Status aller GSLB-Dienste an diesem Remote-Site als DOWN markiert, obwohl die Site möglicherweise nicht wirklich DOWN ist.

Sie können jetzt eine Verzögerung festlegen, damit die MEP-Verbindung wieder hergestellt werden kann, bevor die Website als DOWN markiert wird. Wenn die MEP-Verbindung vor Ablauf der Verzögerung wieder hergestellt wird, sind die Dienste nicht betroffen.

Wenn Sie beispielsweise die Verzögerung auf 10 setzen, bleiben die GSLB-Dienste AKTIV, bis die MEP-Verbindung 10 Sekunden lang NICHT verfügbar war. Nach dieser Dauer werden die GSLB-Dienste als DOWN markiert. Wenn die MEP-Verbindung jedoch innerhalb der 10 Sekunden wieder aktiv ist, bleiben die GSLB-Dienste im UP-Status.

> **Hinweis:**
>
> Diese Verzögerung gilt nur für Dienste, die nicht an einen Monitor gebunden sind. Die Verzögerung wirkt sich nicht auf die Triggermonitore aus.

So stellen Sie mithilfe der Befehlszeilenschnittstelle eine Zeitverzögerung ein

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set gslb parameter** - GSLBSvcStateDelayTime <sec>
<!--NeedCopy-->
```

Beispiel:

Setze den GSLB-Parameter - gslbsvcStateDelayTime 10

> **Hinweis**
>
> Wenn Sie in einer hierarchischen Bereitstellung (übergeordnete und untergeordnete Topologie) den GSLB-Dienst sowohl auf der übergeordneten als auch auf der untergeordneten Site konfigurieren, legen Sie den GSLB-Parameter sowohl auf der übergeordneten als auch auf der untergeordneten Site fest. Wenn Sie den GSLB-Dienst nicht auf der untergeordneten Site konfigurieren, legen Sie den GSLB-Parameter nur auf der übergeordneten Site fest.

So stellen Sie mit der GUI eine Zeitverzögerung ein

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **GSLB-Einstellungen ändern**.
2. Geben Sie im Feld **GSLB-Dienststatus-Verzögerungszeit (Sekunden)** die Zeitverzögerung in Sekunden ein.

Konfigurieren Sie eine Lernzeit für GSLB-Dienste, wenn der MEP-Verbindungsstatus auftaucht, um Klappen bei GSLB-Diensten zu vermeiden

Wenn ein Knoten neu gestartet wird oder während des HA-Failovers, wird das System initialisiert. Dann muss der Knoten aktuelle Informationen über die konfigurierten lokalen und untergeordneten Dienste erfahren, um den Dienststatus über MEP an Remote-Knoten zu kommunizieren. Der Knoten braucht einige Zeit, um die richtigen Informationen zu erfahren. Wenn ein Peer-Knoten eine Verbindung zu diesem Knoten herstellt und ein Update anfordert, sendet der Knoten möglicherweise einen falschen Dienststatus und Statistiken. Diese falschen Informationen können zu Service-Flap und anderen funktionalbezogenen Problemen auf den Remote-Peer-Knoten führen. Um dieses Szenario zu vermeiden, können Sie jetzt eine Lernzeit für den lokalen und untergeordneten GSLB Service festlegen.

Wenn ein Lern-Timeout konfiguriert ist, erhält die GSLB-Site etwas Pufferzeit (Lern-Timeout), um die richtigen Statistiken über ihren lokalen und untergeordneten Service zu erfahren. Wenn sich ein Dienst in einer Lernphase befindet, erhält die Remote-GSLB-Site diese Informationen im MEP-Update und berücksichtigt nicht den primären Standortstatus und die Statistiken, die von MEP für diesen Dienst erhalten wurden.

GSLB-Dienste treten in einem der folgenden Szenarien in die Lernphase ein.

- NetScaler-Appliance wird neu gestartet
- Ein Failover mit hoher Verfügbarkeit ist aufgetreten
- Owner-Knoten in einem Cluster GSLB-Setup wird geändert
- MEP ist auf einem lokalen Knoten aktiviert
- Die GSLB-Site kommt aus dem Inselszenario heraus. Eine GSLB-Site wird zur Insel, wenn sie mit keiner anderen Site verbunden ist.

In einer Eltern-Kind-Bereitstellung verschiebt das übergeordnete Backup-Element (falls konfiguriert) die GSLB-Dienste der übernommenen untergeordneten Website selektiv in die Lernphase, in der das primäre Elternteil NACH UNTEN geht.

So legen Sie eine Lernzeit für den Service-Status mit der CLI fest

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set gslb parameter - SvcStateLearningTime <sec>
<!--NeedCopy-->
```

Sie können “SvcStateLearningTime” in Sekunden einstellen. Der Standardwert ist 0 und der Maximalwert beträgt 3600. Dieser Parameter ist nur anwendbar, wenn Monitore nicht an GSLB-Dienste gebunden sind.

Beispiel:

```
set gslb parameter - SvcStateLearningTime 10
<!--NeedCopy-->
```

So legen Sie eine Lernzeit für den Service-Status mit der GUI fest

1. Navigieren Sie zu **Konfiguration > Traffic Management > GSLB > Dashboard > GSLB-Einstellungen ändern**.

   Die Seite **GSLB-Parameter festlegen** wird angezeigt.

2. Geben Sie im Feld **GSLB Service State Learning Time (Sekunden)** die Lernzeit in Sekunden ein.

Persistenzinformationsaustausch aktivieren

Sie können die NetScaler-Appliance so konfigurieren, dass sie persistente Verbindungen bereitstellt, sodass eine Client-Übertragung an einen beliebigen virtuellen Server in einer Gruppe an einen Server weitergeleitet werden kann, der vorherige Übertragungen von demselben Client empfangen hat.

Sie können den Austausch von Persistenzinformationen an jeder Site aktivieren oder deaktivieren. Diese Informationen werden alle 5 Sekunden zwischen NetScaler Appliances ausgetauscht, die an GSLB teilnehmen.

Weitere Informationen zum Konfigurieren von Persistenz finden Sie unter Persistente Verbindungen konfigurieren.

So aktivieren oder deaktivieren Sie den Persistenzinformationsaustausch mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den Austausch von Persistenzinformationen zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
set gslb site <siteName> -sessionExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Beispiel:

```
set gslb site Site-GSLB-East-Coast -sessionExchange  ENABLED
set gslb site Site-GSLB-East-Coast -sessionExchange  DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie den Austausch von Persistenzinformationen mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**und doppelklicken Sie auf die Site.
2. Aktivieren oder **deaktivieren Sie im Dialogfeld GSLB-Site konfigurieren** das Kontrollkästchen **Persistence Session Entry Exchange** .

Konfigurieren von GSLB mit einem Assistenten

August 19, 2021

Sie können nun einen Assistenten verwenden, um die GSLB-Bereitstellungstypen zu konfigurieren: active-active, active-passive und übergeordnet-child.

Dieser Assistent ist in der GUI verfügbar. Um auf den Assistenten zuzugreifen, navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** und klicken Sie auf **Erste Schritte** .

Sie können diesen Assistenten auch über das GSLB-Dashboard aufrufen. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **GSLB** > **Dashboard**, und klicken Sie auf **GSLB konfigurieren** .

Hinweis: Sie können die GSLB-Entitäten auch einzeln konfigurieren.

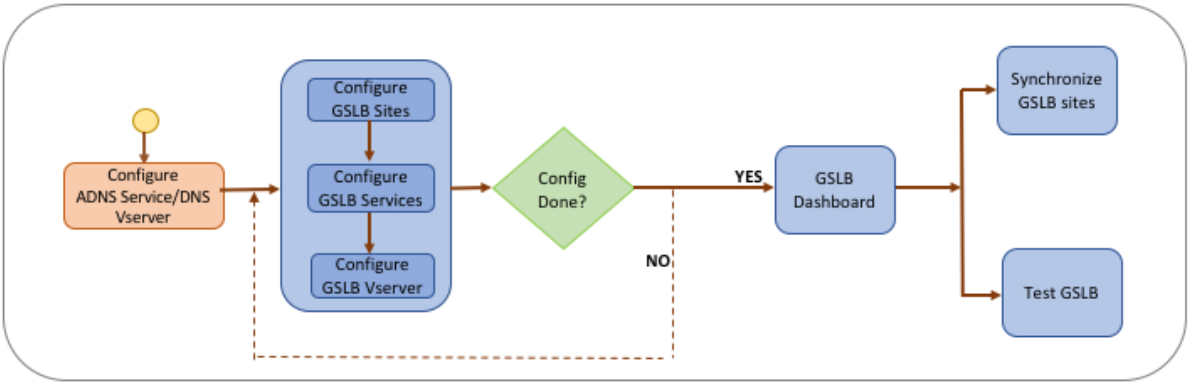
- Active-Active-Sitekonfiguration
- Aktiv-Passiv-Standort-Konfigurationon
- Konfiguration der übergeordneten und untergeordneten Topologie

> **Wichtig**
>
> Diese Funktion wird in der Hochverfügbarkeitsbereitstellung und nicht in Adminpartitions- und Clusterbereitstellungen unterstützt.

Active-Active-Site konfigurieren

May 11, 2023

Die folgende Abbildung zeigt den Arbeitsablauf einer aktiven GSLB-Site-Konfiguration.



Bevor Sie mit der Konfiguration einer aktiv aktiven Site beginnen, stellen Sie sicher, dass Sie für jede Serverfarm oder jedes Rechenzentrum eine Standardkonfiguration für den Lastenausgleich konfiguriert haben.

Um die GSLB-Konfiguration auf allen GSLB-Sites im Deployment zu synchronisieren, müssen Sie außerdem Folgendes sicherstellen:

- Lokale GLSB-Sites werden auf allen Appliances in der GSLB-Konfiguration konfiguriert.
- Sie haben den Verwaltungszugriff auf alle GSLB-Sites in der Konfiguration aktiviert.
- Sie haben die Firewall so konfiguriert, dass sie die automatische Synchronisation und MEP-Verbindungen akzeptiert.
- Auf den Master- und Slave-NetScaler-Appliances werden dieselben NetScaler-Softwareversionen ausgeführt.
- Alle NetScaler-Appliances, die als Standorte teilnehmen, sollten dieselbe NetScaler-Softwareversion haben (die Standorte stehen nicht in einer Master-Slave-Beziehung).
- Das Passwort für den RPC-Knoten ist für alle GSLB-Sites in der GSLB-Konfiguration identisch.

So konfigurieren Sie eine aktive und aktive Site mithilfe des Assistenten

Gehen Sie auf der Registerkarte Konfiguration wie folgt vor:

1. Navigieren Sie zu **Traffic Management** > **GSLB**und klicken Sie dann auf **Get Started**.
2. Wenn Sie keinen ADNS-Dienst oder keinen virtuellen DNS-Server für die Site konfiguriert haben, können Sie dies jetzt tun.
   a) Klicken Sie auf **Ansicht** und dann auf **Hinzufügen**.
   b) Geben Sie den Dienstnamen und die IP-Adresse ein und wählen Sie das Protokoll (ADNS/ADNS_TCP) aus, über das die Daten mit dem Dienst ausgetauscht werden.
3. Wählen Sie **Active-Active Site**aus.
4. Geben Sie den vollqualifizierten Domainnamen ein und geben Sie den Zeitraum an, für den der Datensatz von DNS-Proxys zwischengespeichert werden muss.
5. Konfigurieren Sie die GSLB-Sites. Jeder Standort muss mit einem lokalen GSLB-Site konfiguriert werden, und die Konfiguration jedes Standorts muss alle anderen Standorte als Remote-GSLB-Sites beinhalten. Es kann nur einen lokalen Standort geben und alle anderen Standorte sind Remote-Sites.
   a) Geben Sie die Site-Details wie den Site-Namen und die Site-IP-Adresse ein.
   b) Wählen Sie entweder den Site-Typ REMOTE oder LOCAL aus.
   c) Ändern Sie optional das RPC-Passwort und sichern Sie es gegebenenfalls.
   d) Wenn ein Monitor an den GSLB-Dienst gebunden werden soll, wählen Sie die Bedingung aus, unter der der Monitor den Dienst überwachen soll. Dies wird erst wirksam, wenn ein Monitor an die Dienste gebunden ist. Die möglichen Bedingungen sind:
      - **IMMER**. Überwachen Sie den GSLB-Dienst jederzeit.
      - **MEP schlägt fehl**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
      - **MEP schlägt fehl und die Service-ID ist ausgefallen.** Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der über den Metrikaustausch aktualisiert wurde, ist INAKTIV.
6. Konfigurieren Sie die GSLB-Dienste. Um eine aktiv-aktive Site zu erstellen, müssen Sie mindestens zwei GSLB-Dienste hinzufügen.
   a) Geben Sie die Dienstdetails ein, z. B. den Dienstnamen, den Diensttyp und die Portnummer.
   b) Ordnen Sie den Dienst einem Standort (lokal oder remote) zu, indem Sie den GSLB-Standort auswählen, zu dem der GSLB-Dienst gehört.
   c) Wählen Sie bei Bedarf den Monitor aus, der an den Dienst gebunden werden muss, wenn MEP ausfällt. Der Dienst kann ein vorhandener Server sein, oder Sie können einen neuen Server oder einen virtuellen Server erstellen.
   d) Um einen vorhandenen Server zuzuordnen, wählen Sie den Servernamen aus. Die Dienst-IP-Adresse wird automatisch aufgefüllt.
      - Wenn sich die öffentliche IP-Adresse von der Server-IP unterscheidet, was in einer NAT-Umgebung vorkommen kann, geben Sie die öffentliche IP-Adresse und die Portnummer des öffentlichen Port ein.

- Um einen neuen Server zuzuordnen, erstellen Sie einen Server, indem Sie die Server-IP-Details und seine öffentliche IP-Adresse sowie die öffentliche Portnummer eingeben.
- Um einen virtuellen Server zuzuordnen, wählen Sie einen bereits vorhandenen virtuellen Server aus oder klicken Sie auf + und fügen Sie einen neuen virtuellen Server hinzu. Dieser vserver ist der vserver für den Lastenausgleich, mit dem dieser GSLB-Dienst verknüpft wird.

7. Konfigurieren Sie die virtuellen GSLB-Server.
   a) Geben Sie den Namen des virtuellen GSLB-Servernamens ein und wählen Sie den DNS-Datensatztyp aus.
   b) Klicken Sie im Feld **Dienst auswählen** auf **>** und wählen Sie die GSLB-Dienste aus, die an den virtuellen GSLB-Server gebunden werden sollen.
   c) Klicken Sie im Feld **Domänenbindung** auf **, um die Domain auszuwählen, die an diesen virtuellen GSLB-Server gebunden werden soll.
   d) Wählen Sie die GSLB-Methode, um den GSLB-Dienst mit der besten Leistung auszuwählen. Die Standardwerte für die GSLB-Methode, die Sicherungsmethode und das dynamische Gewicht werden standardmäßig automatisch ausgefüllt. Sie können sie bei Bedarf ändern.
      - Wenn Sie sich für die **algorithmusbasierte** Methode entscheiden, wählen Sie die primäre Methode und die Backup-Methode aus und geben Sie auch die Option für die dynamische Gewichtung an.
      - Wenn Sie die Methode **Static Proximity** wählen, wählen Sie die Backup-Methode und die dynamische Gewichtungsmethode. Geben Sie außerdem den Speicherort der Datenbankdatei an, indem Sie auf das Symbol > klicken, oder fügen Sie einen neuen Speicherort hinzu, indem Sie im Feld Standortdatenbank auswählen auf **+** klicken.
      - Wenn Sie sich für die Methode **Dynamic Proximity (RTT)** entscheiden, wählen Sie die Backup-Methode und geben Sie die Option für die dynamische Gewichtung und den Wert für die Hin- und Rückflugzeit an, auf dessen Grundlage der Dienst mit der besten Leistung ausgewählt werden soll.
8. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
9. Wenn Sie die GSLB-Site-Konfiguration geändert haben, klicken Sie im Dashboard auf **GSLB automatisch synchronisieren**, um die Konfiguration mit anderen Sites im GSLB-Setup zu synchronisieren.
   - Stellen Sie vor der Synchronisierung sicher, dass die Konfiguration der lokalen Site Informationen über die Remote-Sites enthält. Damit die Synchronisation erfolgreich ist, muss die lokale Site außerdem auf den anderen NetScaler-Appliances konfiguriert werden.
   - Wenn die Echtzeitsynchronisierung aktiviert ist, müssen Sie nicht auf **GSLB automatisch**

synchronisierenklicken. Die Synchronisation erfolgt automatisch. Gehen Sie wie folgt vor, um die Echtzeitsynchronisierung zu aktivieren:

a) Navigieren Sie zu **Traffic Management** > **GSLB** > **Dashboard** und klicken Sie auf **GSLB-Einstellungen ändern**.

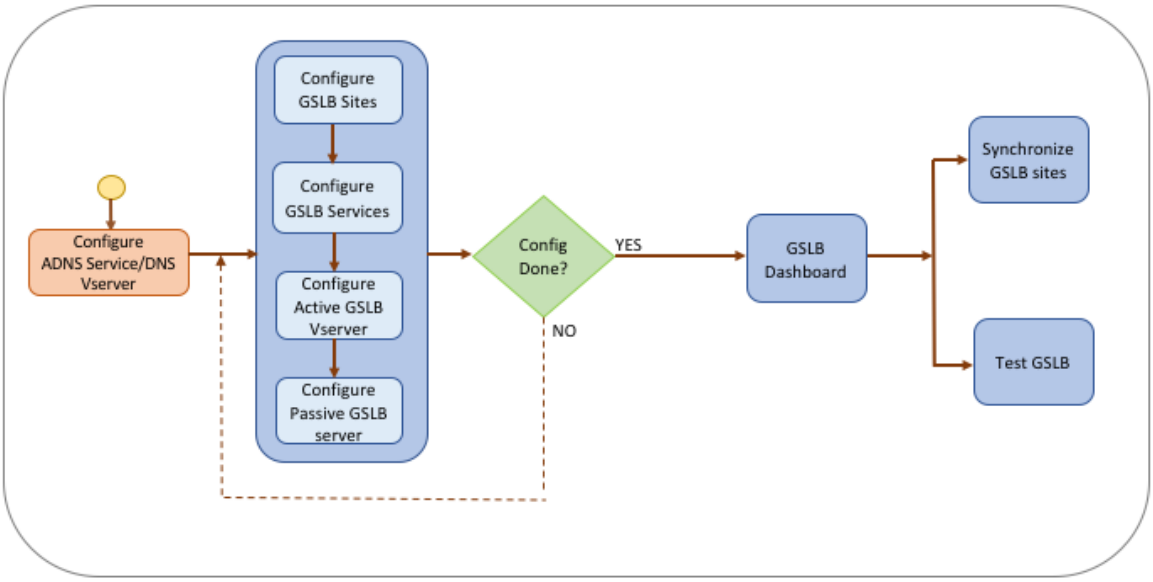
b) Markieren Sie das Kontrollkästchen **Automatische Konfigurationssynchronisierung** .

10. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

Aktiv-Passiv-Site konfigurieren

May 11, 2023

Die folgende Abbildung zeigt den Arbeitsablauf bei der Konfiguration des aktiv/passiven Standorts.



Bevor Sie mit der Konfiguration einer aktiv/passiven Site beginnen, stellen Sie sicher, dass Sie für jede Serverfarm oder jedes Rechenzentrum eine Standardkonfiguration für den Lastenausgleich konfiguriert haben.

Um die GSLB-Konfiguration auf allen GSLB-Sites im Deployment zu synchronisieren, müssen Sie außerdem Folgendes sicherstellen:

- Lokale GLSB-Sites werden auf allen Appliances in der GSLB-Konfiguration konfiguriert.
- Sie haben den Verwaltungszugriff auf alle GSLB-Sites in der Konfiguration aktiviert.

- Sie haben die Firewall so konfiguriert, dass sie die automatische Synchronisation und MEP-Verbindungen akzeptiert.
- Auf den Master- und Slave-NetScaler-Appliances werden dieselben NetScaler-Softwareversionen ausgeführt.
- Alle NetScaler-Appliances, die als Standorte teilnehmen, sollten dieselbe NetScaler-Softwareversion haben (die Standorte stehen nicht in einer Master-Slave-Beziehung).
- Das Passwort für den RPC-Knoten ist für alle GSLB-Sites in der GSLB-Konfiguration identisch.

So konfigurieren Sie eine aktiv/passive Site mithilfe des Assistenten

Gehen Sie auf der Registerkarte Konfiguration wie folgt vor:

1. Navigieren Sie zu **Traffic Management** > **GSLB**und klicken Sie dann auf **Get Started**.
2. Wenn Sie keinen ADNS-Dienst oder keinen virtuellen DNS-Server für die Site konfiguriert haben, können Sie dies jetzt tun.
   a) Klicken Sie auf **Ansicht** und dann auf **Hinzufügen**.
   b) Geben Sie den Dienstnamen und die IP-Adresse ein und wählen Sie das Protokoll (ADNS/ADNS_TCP) aus, über das die Daten mit dem Dienst ausgetauscht werden.
3. Wählen Sie **Active-Passive Site**aus.
4. Geben Sie den vollqualifizierten Domainnamen ein und geben Sie den Zeitraum an, für den der Datensatz von DNS-Proxys zwischengespeichert werden muss.
5. Konfigurieren Sie die GSLB-Sites. Jeder Standort muss mit einem lokalen GSLB-Site konfiguriert werden, und die Konfiguration jedes Standorts muss alle anderen Standorte als Remote-GSLB-Sites beinhalten. Es kann nur einen lokalen Standort geben und alle anderen Standorte sind Remote-Sites.
   a) Geben Sie die Site-Details wie den Site-Namen und die Site-IP-Adresse ein.
   b) Wählen Sie entweder den Site-Typ REMOTE oder LOCAL aus.
   c) Ändern Sie optional das RPC-Passwort und sichern Sie es gegebenenfalls.
   d) Wenn ein Monitor an den GSLB-Dienst gebunden werden soll, wählen Sie die Bedingung aus, unter der der Monitor den Dienst überwachen soll. Dies wird erst wirksam, wenn ein Monitor an die Dienste gebunden ist. Die möglichen Bedingungen sind:
      - **IMMER**. Überwachen Sie den GSLB-Dienst jederzeit.
      - **MEP schlägt fehl**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
      - **MEP schlägt fehl und die Service-ID ist ausgefallen.** Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der über den Metrikaustausch aktualisiert wurde, ist INAKTIV.
6. Konfigurieren Sie die GSLB-Dienste.
   a) Geben Sie die Dienstdetails ein, z. B. den Dienstnamen, den Diensttyp und die Portnummer.

b) Ordnen Sie den Dienst einem Standort (lokal oder remote) zu, indem Sie den GSLB-Standort auswählen, zu dem der GSLB-Dienst gehört.
c) Wählen Sie bei Bedarf den Monitor aus, der an den Dienst gebunden werden muss, wenn MEP ausfällt. Der Dienst kann ein vorhandener Server sein, oder Sie können einen neuen Server oder einen virtuellen Server erstellen.
d) Um einen vorhandenen Server zuzuordnen, wählen Sie den Servernamen aus. Die Dienst-IP-Adresse wird automatisch aufgefüllt.
   - Wenn sich die öffentliche IP-Adresse von der Server-IP unterscheidet, was in einer NAT-Umgebung vorkommen kann, geben Sie die öffentliche IP-Adresse und die Portnummer des öffentlichen Port ein.
   - Um einen neuen Server zuzuordnen, erstellen Sie einen Server, indem Sie die Server-IP-Details und seine öffentliche IP-Adresse sowie die öffentliche Portnummer eingeben.
   - Um einen virtuellen Server zuzuordnen, wählen Sie einen bereits vorhandenen virtuellen Server aus oder klicken Sie auf **+** und fügen Sie einen neuen virtuellen Server hinzu. Dieser vserver ist der vserver für den Lastenausgleich, mit dem dieser GSLB-Dienst verknüpft wird.

7. Konfigurieren Sie die virtuellen GSLB-Backup-Server. Die virtuellen GSLB-Backup-Server werden erst betriebsbereit, wenn auf die primären virtuellen GSLB-Server nicht zugegriffen werden kann oder sie aus irgendeinem Grund als DOWN markiert sind.
   a) Geben Sie den Namen des virtuellen GSLB-Servernamens ein und wählen Sie den DNS-Datensatztyp aus.
   b) Klicken Sie in **Service Binding** auf **und wählen Sie die GSLB-Dienste aus, die an den virtuellen GSLB-Server gebunden werden müssen.
   c) Wählen Sie die GSLB-Methode, um den GSLB-Dienst mit der besten Leistung auszuwählen. Die Standardwerte für die GSLB-Methode, die Sicherungsmethode und das dynamische Gewicht werden standardmäßig automatisch ausgefüllt. Sie können sie bei Bedarf ändern.
      - Wenn Sie die **algorithmusbasierte** Methode wählen, wählen Sie die Primär- und die Backup-Methode aus.
      - Wenn Sie die Methode **Static Proximity** wählen, wählen Sie die Sicherungsmethode und geben Sie den Speicherort der Datenbankdatei an.
      - Wenn Sie die **Dynamic Proximity (RTT)** -Methode wählen, wählen Sie die Backup-Methode und geben Sie das Service-Gewicht und den RTT-Wert an, auf deren Grundlage der Dienst mit der besten Leistung ausgewählt werden soll.

8. Konfigurieren Sie die virtuellen GSLB-Server.
   a) Geben Sie den Namen des virtuellen GSLB-Servernamens ein und wählen Sie den DNS-Datensatztyp aus.
   b) Klicken Sie im Feld **Dienst auswählen** auf **>** und wählen Sie die GSLB-Dienste aus, die an

den virtuellen GSLB-Server gebunden werden sollen.

c) Klicken Sie im Feld **Domänenbindung** auf **, um die Domain auszuwählen, die an diesen virtuellen GSLB-Server gebunden werden soll.

d) Wählen Sie die GSLB-Methode, um den GSLB-Dienst mit der besten Leistung auszuwählen. Die Standardwerte für die GSLB-Methode, die Sicherungsmethode und das dynamische Gewicht werden standardmäßig automatisch ausgefüllt. Sie können sie bei Bedarf ändern.

- Wenn Sie sich für die **algorithmusbasierte** Methode entscheiden, wählen Sie die primäre Methode und die Backup-Methode aus und geben Sie auch die Option für die dynamische Gewichtung an.
- Wenn Sie die Methode **Static Proximity** wählen, wählen Sie die Backup-Methode und die dynamische Gewichtungsmethode. Geben Sie außerdem den Speicherort der Datenbankdatei an, indem Sie auf das Symbol **** klicken, oder fügen Sie einen neuen Speicherort hinzu, indem Sie im Feld Standortdatenbank auswählen auf **+** klicken.
- Wenn Sie sich für die Methode **Dynamic Proximity (RTT)** entscheiden, wählen Sie die Backup-Methode und geben Sie die Option für die dynamische Gewichtung und den Wert für die Hin- und Rückflugzeit an, auf dessen Grundlage der Dienst mit der besten Leistung ausgewählt werden soll.

9. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
10. Wenn Sie die GSLB-Site-Konfiguration geändert haben, klicken Sie im Dashboard auf **GSLB automatisch synchronisieren**, um die Konfiguration mit anderen Sites im GSLB-Setup zu synchronisieren.
    - Stellen Sie vor der Synchronisierung sicher, dass die Konfiguration der lokalen Site Informationen über die Remote-Sites enthält. Damit die Synchronisation erfolgreich ist, muss die lokale Site außerdem auf den anderen NetScaler-Appliances konfiguriert werden.
    - Wenn die Echtzeitsynchronisierung aktiviert ist, müssen Sie nicht auf **GSLB automatisch synchronisieren**klicken. Die Synchronisation erfolgt automatisch. Gehen Sie wie folgt vor, um die Echtzeitsynchronisierung zu aktivieren:
      a) Navigieren Sie zu **Traffic Management** > **GSLB** > **Dashboard** und klicken Sie auf **GSLB-Einstellungen ändern**.
      b) Markieren Sie das Kontrollkästchen **Automatische Konfigurationssynchronisierung** .
11. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

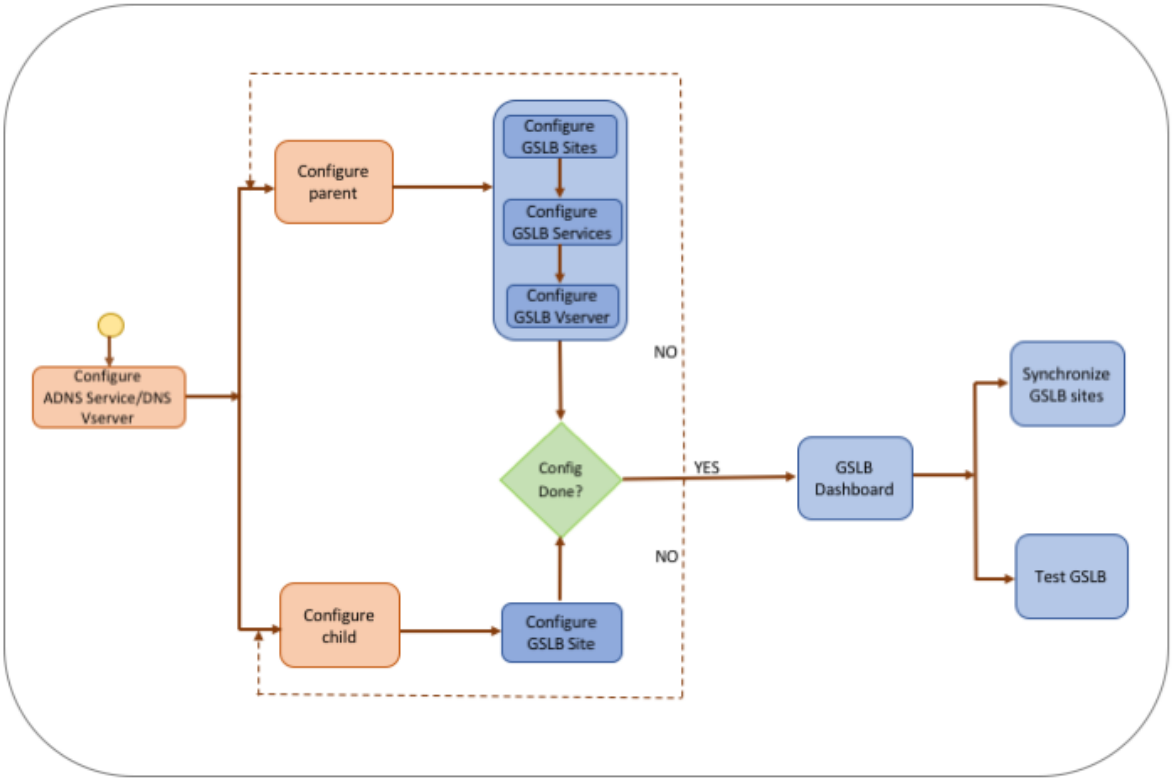
> **Hinweis**
>
> Weitere Informationen zum Konfigurieren von GSLB-Entitäten eines aktiv-passiven GSLB-Setups für Disaster Recovery finden Sie unter Konfigurieren von GSLB für Disaster Recovery.

Konfigurieren der Eltern-Kind-Topologie

May 11, 2023

In einer Eltern-Kind-Topologie befinden sich auf der obersten Ebene übergeordnete Standorte, die Beziehungen zu Gleichaltrigen zu anderen Elternteilen unterhalten. Jeder Elternteil kann mehrere Websites für Kinder haben, und jeder Elternstandort tauscht Gesundheitsinformationen mit den Websites seiner Kinder und mit Websites anderer Eltern aus. Ein untergeordneter Standort kommuniziert jedoch nur mit seinem übergeordneten Standort.

Die folgende Abbildung zeigt den Arbeitsablauf einer GSLB-Topologiekonfiguration mit übergeordnetem und untergeordnetem System.



Bevor Sie mit der Konfiguration der Bereitstellung der übergeordneten und untergeordneten Topologie beginnen, stellen Sie sicher, dass Sie für jede Serverfarm oder jedes Rechenzentrum eine Standardkonfiguration für den Lastenausgleich konfiguriert haben.

Um die GSLB-Konfiguration auf allen GSLB-Sites im Deployment zu synchronisieren, müssen Sie außerdem Folgendes sicherstellen:

- Lokale GLSB-Sites werden auf allen Appliances in der GSLB-Konfiguration konfiguriert.
- Sie haben den Verwaltungszugriff auf alle GSLB-Sites in der Konfiguration aktiviert.
- Sie haben die Firewall so konfiguriert, dass sie die automatische Synchronisation und MEP-Verbindungen akzeptiert.
- Alle NetScaler-Appliances, die als Standorte teilnehmen, sollten dieselbe NetScaler-Softwareversion haben (die Standorte stehen nicht in einer Master-Slave-Beziehung).
- Das Passwort für den RPC-Knoten ist für alle GSLB-Sites in der GSLB-Konfiguration identisch.

So konfigurieren Sie mithilfe des Assistenten eine Bereitstellung mit übergeordnetem Kind

Gehen Sie auf der Registerkarte Konfiguration wie folgt vor:

1. Navigieren Sie zu **Traffic Management** > **GSLB**und klicken Sie dann auf **Get Started**.
2. Wenn Sie keinen ADNS-Server oder keinen virtuellen DNS-Server für die Site konfiguriert haben, können Sie dies jetzt tun.
   a) Klicken Sie auf **Ansicht** und dann auf **Hinzufügen**.
   b) Geben Sie den Dienstnamen und die IP-Adresse ein und wählen Sie das Protokoll (ADNS/ADNS_TCP) aus, über das die Daten mit dem Dienst ausgetauscht werden.
3. Wählen Sie **Parent-Child-Topologie**aus.
4. Wählen Sie im Feld Wählen Sie den Site-Typ aus;
   - **Übergeordneter** Standort — Bei der Konfiguration des übergeordneten Standorts müssen Sie die zugehörigen untergeordneten Standorte und auch die anderen übergeordneten Standorte im GSLB-Setup konfigurieren.
   - **Child** — Bei der Konfiguration des untergeordneten Standorts müssen Sie nur den untergeordneten Standort und seinen übergeordneten Standort konfigurieren.

So konfigurieren Sie eine übergeordnete Site

1. Geben Sie den vollqualifizierten Domainnamen ein und geben Sie den Zeitraum an, für den der Datensatz von DNS-Proxys zwischengespeichert werden muss.
2. Konfigurieren Sie die GSLB-Sites. Jeder Standort muss mit einem lokalen GSLB-Site konfiguriert werden, und die Konfiguration jedes Standorts muss alle anderen Standorte als Remote-GSLB-Sites beinhalten. Es kann nur eine lokale Site geben. Alle anderen Standorte sind Remote-Sites. Wenn die angegebene Site-IP-Adresse der Appliance gehört (z. B. eine MIP- oder SNIP-Adresse), handelt es sich bei der Site um einen lokalen Standort. Andernfalls handelt es sich um eine Remote-Site.
3. Geben Sie die Site-Details wie den Site-Namen und die Site-IP-Adresse ein.

a) Wählen Sie den Site-Typ aus.
b) Ändern Sie optional das RPC-Passwort und sichern Sie es gegebenenfalls.
c) Wenn ein Monitor an den GSLB-Dienst gebunden werden soll, wählen Sie die Bedingung aus, unter der der Monitor den Dienst überwachen soll. Dies wird erst wirksam, wenn ein Monitor an die Dienste gebunden ist. Die möglichen Bedingungen sind:
   - **Always**. Überwachen Sie den GSLB-Dienst jederzeit.
   - **MEP schlägt fehl**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
   - **MEP schlägt fehl und der Dienst ist AUSGEFALLEN.** Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der über den Metrikaustausch aktualisiert wurde, ist INAKTIV.

4. Konfigurieren Sie die GSLB-Dienste.
   a) Geben Sie die Dienstdetails wie Dienstname, Diensttyp und Portnummer ein.
   b) Ordnen Sie den Dienst einem Standort (lokal oder remote) zu, indem Sie den GSLB-Standort auswählen, zu dem der GSLB-Dienst gehört.
   c) Wählen Sie bei Bedarf den Monitor aus, der an den Dienst gebunden werden muss, wenn MEP ausfällt. Der Dienst kann ein vorhandener Server sein, oder Sie können einen neuen Server oder einen virtuellen Server erstellen.
      - Um einen vorhandenen Server zuzuordnen, wählen Sie den Servernamen aus. Die Dienst-IP-Adresse wird automatisch ausgefüllt.
      - Um einen neuen Server zuzuordnen, erstellen Sie einen Server, indem Sie die Server-IP-Details und seine öffentliche IP-Adresse sowie die öffentliche Portnummer eingeben.
      - Um einen virtuellen Server zuzuordnen, wählen Sie einen bereits vorhandenen virtuellen Server aus oder klicken Sie auf **+** und fügen Sie einen neuen virtuellen Server hinzu. Dieser vserver ist der vserver für den Lastenausgleich, dem dieser GSLB-Dienst zugeordnet wird. Wenn sich die öffentliche IP-Adresse von der Server-IP unterscheidet, was in einer NAT-Umgebung vorkommen kann, geben Sie die öffentliche IP-Adresse und die öffentliche Portnummer ein.

5. Konfigurieren Sie die virtuellen GSLB-Server.
   a) Geben Sie den Namen des virtuellen GSLB-Servernamens ein und wählen Sie den DNS-Datensatztyp aus.
   b) Klicken Sie im Feld **Dienst auswählen** auf **>** und wählen Sie die GSLB-Dienste aus, die an den virtuellen GSLB-Server gebunden werden sollen.
   c) Klicken Sie im Feld **Domänenbindung** auf **, um den Domainnamen anzuzeigen, der an den virtuellen GSLB-Server gebunden ist.
   d) Wählen Sie die GSLB-Methode, um den GSLB-Dienst mit der besten Leistung auszuwählen. Die Standardwerte für die GSLB-Methode, die Backup-Methode und das dynamische Gewicht werden standardmäßig automatisch aufgefüllt. Sie können sie bei Bedarf

ändern.

- Wenn Sie sich für die **algorithmusbasierte** Methode entscheiden, wählen Sie die primäre Methode und die Backup-Methode aus und geben Sie auch die Option für die dynamische Gewichtung an.
- Wenn Sie die Methode **Static Proximity** wählen, wählen Sie die Backup-Methode und die dynamische Gewichtungsmethode. Geben Sie außerdem den Speicherort der Datenbankdatei an, indem Sie auf das Symbol **** klicken, oder fügen Sie einen neuen Speicherort hinzu, indem Sie im Feld Standortdatenbank auswählen auf **+** klicken.
- Wenn Sie die **Dynamic Proximity (RTT)** -Methode wählen, wählen Sie die Backup-Methode und geben Sie das Service-Gewicht und den RTT-Wert an, auf deren Grundlage der Dienst mit der besten Leistung ausgewählt werden soll.

6. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
7. Wenn Sie die Konfiguration der übergeordneten GSLB-Website geändert haben, klicken Sie auf **GSLB automatisch synchronisieren, um die Konfiguration mit den anderen übergeordneten Sites im GSLB-Setup** zu synchronisieren. In einer Parent-Child-Topologie wird die Synchronisation für die untergeordneten Sites übersprungen.
   - Stellen Sie vor der Synchronisierung sicher, dass die Konfiguration der lokalen Site Informationen über die Remote-Sites enthält.
   - Wenn die Echtzeitsynchronisierung aktiviert ist, müssen Sie nicht auf **GSLB automatisch synchronisieren**klicken. Die Synchronisation erfolgt automatisch. Gehen Sie wie folgt vor, um die Echtzeitsynchronisierung zu aktivieren:
     a) Navigieren Sie zu **Traffic Management** > **GSLB** > **Dashboard** und klicken Sie auf **GSLB-Einstellungen ändern**.
     b) Markieren Sie das Kontrollkästchen **Automatische Konfigurationssynchronisierung** .
8. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

So konfigurieren Sie eine untergeordnete Site

1. Konfigurieren Sie die GSLB-Sites.
   a) Geben Sie die Site-Details wie den Site-Namen und die Site-IP-Adresse ein.
   b) Wählen Sie den Site-Typ aus.
   c) Ändern Sie optional das RPC-Passwort und sichern Sie es gegebenenfalls. 4. Wenn ein Monitor an den GSLB-Dienst gebunden ist, wählen Sie die Bedingung aus, unter der der Monitor den Dienst überwachen soll. Die möglichen Bedingungen sind:
      - **Always**. Überwachen Sie den GSLB-Dienst jederzeit.

- **MEP schlägt fehl**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
- **MEP schlägt fehl und der Dienst ist AUSGEFALLEN.** Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der über den Metrikaustausch aktualisiert wurde, ist INAKTIV.

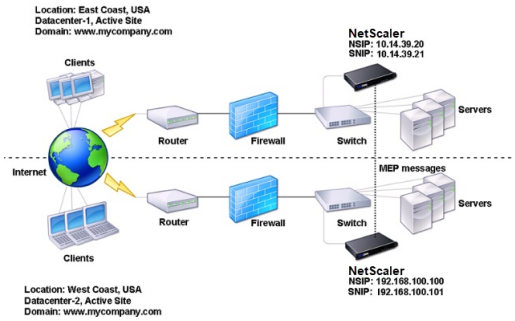
2. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
3. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

GSLB-Entitäten einzeln konfigurieren

May 11, 2023

Der globale Serverlastenausgleich wird verwendet, um den Datenverkehr zu einer Website zu verwalten, die auf zwei separaten Serverfarmen gehostet wird, die sich idealerweise an unterschiedlichen geografischen Standorten befinden. Stellen Sie sich beispielsweise eine Website, www.mycompany.com, vor, die auf zwei geografisch getrennten Serverfarmen oder Rechenzentren gehostet wird. Beide Serverfarmen verwenden NetScaler-Appliances. Die NetScaler-Appliances in diesen Serverfarmen sind im einarmigen Modus eingerichtet und fungieren als autorisierende DNS-Server für die Domain www.mycompany.com. Die folgende Abbildung veranschaulicht diese Konfiguration.

Abbildung 1. Grundlegende GSLB-Topologie



Um ein solches GSLB-Setup zu konfigurieren, müssen Sie zunächst ein Standard-Load-Balancing-Setup für jede Serverfarm oder jedes Rechenzentrum konfigurieren. Auf diese Weise können Sie die Last auf die verschiedenen Server in jeder Serverfarm verteilen. Konfigurieren Sie dann beide NetScaler-Appliances als autoritative DNS-Server (ADNS). Erstellen Sie als Nächstes eine GSLB-Site für jede Serverfarm, konfigurieren Sie virtuelle GSLB-Server für jeden Standort, erstellen Sie GLSB-Dienste und binden Sie die GSLB-Dienste an die virtuellen GSLB-Server. Binden Sie abschließend

die Domain an die virtuellen GSLB-Server. Die GSLB-Konfigurationen auf den beiden Appliances an den beiden verschiedenen Sites sind identisch, obwohl die Lastausgleichs-Konfigurationen für jeden Standort spezifisch für diesen Standort sind.

Hinweis: Informationen zum Konfigurieren einer GSLB-Site in einem NetScaler Cluster-Setup finden Sie unter Einrichten von GSLB in einem Cluster.

Konfigurieren eines Standard-Lastausgleichs

Ein virtueller Lastausgleichsserver verteilt die Last auf verschiedene physische Server im Rechenzentrum. Diese Server werden als Dienste auf der NetScaler Appliance dargestellt, und die Dienste sind an den virtuellen Lastausgleichsserver gebunden.

Weitere Informationen zum Konfigurieren eines grundlegenden Load Balancing-Setups finden Sie unter Load Balancing.

Konfigurieren eines autoritativen DNS-Dienstes

May 11, 2023

Wenn Sie die NetScaler-Appliance als autoritativen DNS-Server konfigurieren, akzeptiert sie DNS-Anfragen vom Client und antwortet mit der IP-Adresse des Rechenzentrums, an das der Client Anfragen senden soll.

Hinweis: Damit die NetScaler Appliance autorisierend ist, müssen Sie auch SOA- und NS-Datensätze erstellen. Weitere Informationen zu SOA- und NS-Datensätzen finden Sie unter Domänennamensystem.

So erstellen Sie einen ADNS-Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen ADNS-Dienst zu erstellen und die Konfiguration zu überprüfen:

```
add service <name> <IP>@ ADNS <port>

show service <name>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-ADNS-1 10.14.39.21 ADNS 53

```



```
show service Service-ADNS-1
<!--NeedCopy-->
```

So ändern Sie einen ADNS-Dienst mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set service <name> <IPAddress> ADNS <port>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

So entfernen Sie einen ADNS-Dienst mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm service <name>
<!--NeedCopy-->
```

Beispiel:

```
rm service Service-ADNS-1
<!--NeedCopy-->
```

So konfigurieren Sie einen ADNS-Dienst mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
2. Fügen Sie einen neuen ADNS-Dienst hinzu, oder wählen Sie einen vorhandenen Dienst aus, und bearbeiten Sie dessen Einstellungen.

Konfigurieren einer grundlegenden GSLB-Site

May 11, 2023

Eine GSLB-Site stellt ein Rechenzentrum in Ihrem Netzwerk dar und ist eine logische Gruppierung von virtuellen GSLB-Servern, -Diensten und anderen Netzwerkentitäten. In der Regel gibt es in einem GSLB-Setup viele GSLB-Websites, die so ausgestattet sind, dass sie einem Kunden dieselben

Inhalte zur Verfügung stellen. Diese sind normalerweise geografisch getrennt, um sicherzustellen, dass die Domain auch dann aktiv ist, wenn eine Website vollständig ausfällt. Alle Sites in der GSLB-Konfiguration müssen auf jeder NetScaler-Appliance konfiguriert werden, die eine GSLB-Site hostet. Mit anderen Worten, an jedem Standort konfigurieren Sie den lokalen GSLB-Standort und jeden Remote-GSLB-Standort.

Sobald GSLB-Sites für eine Domäne erstellt wurden, sendet die NetScaler-Appliance Clientanfragen an die entsprechende GSLB-Site, die durch die konfigurierten GSLB-Algorithmen bestimmt wird.

So erstellen Sie eine GSLB-Site mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine GSLB-Site zu erstellen und die Konfiguration zu überprüfen:

```
add gslb site <siteName> <siteIPAddress>
show gslb site <siteName>
<!--NeedCopy-->
```

Beispiel:

```
add gslb site Site-GSLB-East-Coast 10.14.39.21
show glsb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So ändern oder entfernen Sie eine GSLB-Site mithilfe der Befehlszeilenschnittstelle

- Um eine GSLB-Site zu ändern, verwenden Sie den Befehl set gslb site. Dieser Befehl entspricht der Verwendung des Befehls add gslb site, außer dass Sie den Namen einer vorhandenen GSLB-Site eingeben.
- Um einen Site-Parameter zu deaktivieren, verwenden Sie den Befehl unset gslb site, gefolgt vom SiteName-Wert und dem Namen des Parameters, der auf den Standardwert zurückgesetzt werden soll.
- Um eine GSLB-Site zu entfernen, verwenden Sie den Befehl rm gslb site, der <name> nur das Argument akzeptiert.

So konfigurieren Sie eine einfache GSLB-Site mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites.**
2. Fügen Sie eine neue GSLB-Site hinzu oder wählen Sie eine bestehende GSLB-Site aus und bearbeiten Sie deren Einstellungen.

Um die Statistiken einer GSLB-Site mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat gslb site <siteName>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

Um die Statistiken einer GSLB-Site mithilfe des Konfigurationsprogramms anzuzeigen

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites.**
2. Wählen Sie die GSLB-Site aus, und klicken Sie auf **Statistiken**.

Konfigurieren eines GSLB-Dienstes

January 19, 2021

Ein GSLB-Dienst ist eine Darstellung eines virtuellen Lastausgleichs- oder Content Switching-Servers. Ein lokaler GSLB-Dienst stellt einen lokalen Lastenausgleich oder einen virtuellen Content Switching-Server dar. Ein Remote-GSLB-Dienst stellt einen Lastenausgleich oder einen virtuellen Content Switching-Server dar, der an einem der anderen Sites im GSLB-Setup konfiguriert ist. An jedem Standort im GSLB-Setup können Sie einen lokalen GSLB-Dienst und eine beliebige Anzahl von GSLB-Remote-Diensten erstellen.

> **Wichtig**:
>
> Wenn sich der virtuelle Lastausgleichsserver entweder in einem GSLB-Knoten selbst befindet oder sich in einem untergeordneten Knoten (in der Eltern-Kind-Bereitstellung) befindet und keine Monitore an den GSLB-Dienst gebunden sind, stellen Sie sicher, dass Folgendes:
>
> Die IP-Adresse des GLSB-Dienstes, die Portnummer und das Protokoll übereinstimmen der virtuelle Server, den der Dienst darstellt. Andernfalls wird der Dienststatus als DOWN markiert.

So erstellen Sie einen GSLB-Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen GSLB-Dienst zu erstellen und die Konfiguration zu überprüfen:


```
add gslb service <serviceName> <serverName | IP> <serviceType> <port>-
    siteName <string>
show gslb service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
add gslb service Service-GSLB-1 10.14.39.14 HTTP 80  - siteName Site-
    GSLB-East-Coast
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

So ändern oder entfernen Sie einen GSLB-Dienst mit der Befehlszeilenschnittstelle

- Um einen GSLB-Dienst zu ändern, verwenden Sie den<serviceName> Befehl set gslb service. Geben Sie für diesen Befehl den Namen des GSLB-Dienstes an, dessen Konfiguration Sie ändern möchten. Sie können die vorhandenen Werte der von Ihnen angegebenen Parameter ändern oder standardmäßig festlegen. Sie können den Wert von mehr als einem Parameter im selben Befehl ändern. Weitere Informationen zu den Parametern finden Sie im Befehl add gslb service. Beispiel

  ```
  > set gslb service SKP_GSLB_NOTCNAME_SVC2 -maxBandWidth 25 -
      maxClient 8
  Done
  > sh gslb service SKP_GSLB_NOTCNAME_SVC2
  SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
  ...
  Max Conn: 8  Max Bandwidth: 25 kbits
  <!--NeedCopy-->
  ```

- Um einen Parameter auf seinen Standardwert zurückzusetzen, können Sie den<serviceName > Befehl unset gslb service und die zu löschenden Parameter verwenden. Beispiel

  ```
  > unset gslb service SKP_GSLB_NOTCNAME_SVC2 maxBandWidth
  Done
  > sh gslb service SKP_GSLB_NOTCNAME_SVC2
  SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
  ...
  Max Conn: 8  Max Bandwidth: 0 kbits
  <!--NeedCopy-->
  ```

- Um einen GSLB-Dienst zu entfernen, verwenden Sie den<serviceName> Befehl rm gslb service.

So erstellen Sie einen GSLB-Dienst mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Fügen Sie einen neuen GSLB-Dienst hinzu, oder wählen Sie einen vorhandenen Dienst aus und bearbeiten Sie dessen Einstellungen.

So zeigen Sie die Statistiken eines GSLB-Diensts mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat gslb service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb service Service-GSLB-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines GSLB-Diensts mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Wählen Sie den GSLB-Dienst aus, und klicken Sie auf **Statistiken**.

Konfigurieren einer GSLB-Dienstgruppe

May 11, 2023

Mit der Dienstgruppe können Sie eine Gruppe von Diensten so einfach wie einen einzigen Dienst verwalten. Wenn Sie eine Option für eine Dienstgruppe aktivieren oder deaktivieren, wird die Option für alle Mitglieder der Dienstgruppe aktiviert oder deaktiviert. Sie können diese Funktion beispielsweise auf Optionen wie Kompression, Zustandsüberwachung und ordnungsgemäßes Herunterfahren anwenden.

Nachdem Sie eine Dienstgruppe erstellt haben, können Sie einen der folgenden Schritte ausführen:

- Binden Sie die Dienstgruppe an einen virtuellen Server.
- Fügen Sie der Dienstgruppe Dienste hinzu.
- Binden Sie Monitore an die Dienstgruppen.

> **Wichtig**
>
> Wenn sich der virtuelle Lastausgleichsserver entweder in einem GSLB-Knoten selbst oder in

> einem untergeordneten Knoten (in der Übergeordnet-Untergeordnet-Bereitstellung) befindet und keine Monitore an den GSLB Service gebunden sind, stellen Sie Folgendes sicher: IP-Adresse, Portnummer und Protokoll
>
> der GLSB-Dienstgruppe stimmen mit dem virtuellen Server überein, um den der Dienst handelt vertretend. Ansonsten ist der Dienstzustand als DOWN gekennzeichnet.

Der NetScaler unterstützt die folgenden Typen von GSLB-Dienstgruppen.

- IP-Adressbasierte Dienstgruppen
- Auf Domainnamen basierende Dienstgruppen
- Auf Domainnamen basierende Autoscale-Dienstgruppen

GSLB Domainnamen basierte Autoscale-Dienstgruppen

Die NetScaler Hybrid- und Multi-Cloud Global Server Load Balancing (GSLB) -Lösung ermöglicht es Kunden, den Anwendungsverkehr auf mehrere Rechenzentren in Hybrid Clouds, mehreren Clouds und on-premises zu verteilen. Die NetScaler GSLB-Lösung unterstützt verschiedene Load Balancing-Lösungen wie den NetScaler Load Balancer, Elastic Load Balancing (ELB) für AWS und andere Load Balancer von Drittanbietern. Darüber hinaus führt die GSLB-Lösung einen globalen Lastausgleich durch, auch wenn die GSLB- und Load-Balancing-Schichten unabhängig verwaltet werden.

In Cloud-Bereitstellungen erhalten Benutzer einen Domänennamen als Referenz, wenn sie zu Verwaltungszwecken auf die Load Balancing-Lösung zugreifen. Es wird empfohlen, dass externe Entitäten nicht die IP-Adressen verwenden, in die diese Domainnamen auflösen. Außerdem werden die Load-Balancing-Schichten basierend auf der Last nach oben oder unten skaliert, und es wird nicht garantiert, dass die IP-Adressen statisch sind. Daher wird empfohlen, den Domänennamen anstelle von IP-Adressen zu verwenden, um auf die Endpunkte des Lastenausgleichs zu verweisen. Dies erfordert, dass die GSLB-Dienste unter Verwendung des Domainnamens anstelle von IP-Adressen referenziert werden, und es muss alle IP-Adressen verbrauchen, die für den Domänennamen der Lastausgleichsschicht zurückgegeben werden, und eine Repräsentation dafür in GSLB haben.

Um Domänennamen anstelle von IP-Adressen zu verwenden, wenn Sie auf die Lastausgleichs-Endpunkte verweisen, können Sie die auf Domänennamen basierenden Dienstgruppen für GSLB verwenden.

Überwachen Sie auf GSLB-Domänennamen

Die NetScaler-Appliance verfügt über zwei integrierte Monitore, die TCP-basierte Anwendungen überwachen; `tcp-default` und `ping-default`. Der `tcp-default` Monitor ist an alle TCP-Dienste gebunden und der `ping-default` Monitor ist an alle Nicht-TCP-Dienste gebunden. Die eingebauten Monitore sind standardmäßig an die GSLB-Dienstgruppen gebunden. Es wird jedoch empfohlen, einen anwendungsspezifischen Monitor an die GSLB-Dienstgruppen zu binden.

Empfehlung für die Einstellung der Trigger-Monitor-Option auf MEPDOWN

Die Option Trigger-Monitore kann verwendet werden, um anzugeben, ob die GSLB-Site die Monitore immer verwenden muss, oder Monitore verwenden, wenn das Metrikaustauschprotokoll (MEP) DOWN ist.

Die Option Monitore auslösen ist standardmäßig auf IMMER eingestellt.

Wenn die Option Monitore auslösen auf IMMER gesetzt ist, löst jeder GSLB-Knoten die Monitore unabhängig voneinander aus. Wenn jeder GSLB-Knoten die Monitore unabhängig auslöst, arbeitet jeder GSLB-Knoten möglicherweise mit einem anderen Satz von GSLB-Diensten. Dies kann zu Abweichungen bei den DNS-Antworten für die DNS-Anforderungen führen, die auf diesen GSLB-Knoten landen. Wenn jeder GSLB-Knoten unabhängig überwacht, erhöht sich außerdem die Anzahl der Monitor-Prüfpunkte, die die Load Balancer-Einheit erreichen. Die Persistenzeinträge werden auch über die GSLB-Knoten hinweg inkompatibel.

Daher wird empfohlen, dass die Option Monitore auslösen in der GSLB-Siteeinheit auf MEPDOWN festgelegt ist. Wenn die Option Monitore auslösen auf MEPDOWN festgelegt ist, liegt die Domänenauflösung und die Überwachung des Lastausgleichs beim lokalen GSLB-Knoten. Wenn die Option Monitore auslösen auf MEPDOWN gesetzt ist, erfolgt die Load-Balancing-Domänenauflösung und die anschließende Überwachung durch den lokalen GSLB-Knoten einer GSLB-Dienstgruppe. Die Ergebnisse werden dann mithilfe des Metrik-Austauschprotokolls (MEP) an alle anderen an GSLB teilnehmenden Knoten weitergegeben.

Wenn der Satz von IP-Adressen, die einer Load Balancing-Domäne zugeordnet sind, aktualisiert wird, wird er außerdem über MEP benachrichtigt.

Einschränkungen von GSLB-Dienstgruppen

- Bei einer Load Balancing-Domäne ist die IP-Adresse, die in der DNS-Antwort zurückgegeben wird, im Allgemeinen die öffentliche IP-Adresse. Die private IP-Adresse kann nicht dynamisch angewendet werden, wenn die Load-Balancing-Domäne aufgelöst wird. Daher sind der öffentliche IP-Port und der private IP-Port für die IP-Portbindungen der GSLB-Domänennamen, die auf Autoscale-Dienstgruppen basieren, identisch. Diese Parameter können nicht explizit für die auf Domänennamen basierenden Autoscale-Dienstgruppen festgelegt werden.
- Sitepersistenz, DNS-Ansichten und Clustering werden für GSLB-Dienstgruppen nicht unterstützt.

Konfigurieren und Verwalten von GSLB-Dienstgruppen über die CLI

So fügen Sie eine GSLB-Dienstgruppe hinzu:

```
add gslb serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (
    DISABLED | DNS )] -siteName <string>
```



```
<!--NeedCopy-->
```

Beispiel:

```
add gslb serviceGroup Service-Group-1 http -autoScale DNS -siteName
    Site1
<!--NeedCopy-->
```

So binden Sie eine GSLB-Dienstgruppe an einen virtuellen Server:

```
bind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName
    >@ | (-monitorName <string>@))
<!--NeedCopy-->
```

Beispiel:

```
bind gslb serviceGroup Service-Group-1 203.0.113.2
bind gslb serviceGroup Service-Group-1 S1 80
bind gslb serviceGroup** Service-Group-1 -monitorName Mon1
<!--NeedCopy-->
```

So trennen Sie die Bindung einer GSLB-Dienstgruppe an einen virtuellen Server:

```
unbind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <
    serverName>@ | -monitorName <string>@)
<!--NeedCopy-->
```

Beispiel:

```
unbind gslb serviceGroup Service-Group-1 -monitorName Mon1
<!--NeedCopy-->
```

So legen Sie Parameter für eine GSLB-Dienstgruppe fest:

```
set gslb serviceGroup <serviceGroupName>@ [(<serverName>@ <port> [-
    weight <positive_integer>] [-hashId <positive_integer>] [-publicIP <
    ip_addr|ipv6_addr|*>] [-publicPort <port>]) | -maxClient <
    positive_integer> | -cip ( ENABLED | DISABLED ) | <cipHeader> | -
    cltTimeout <secs> | -svrTimeout <secs> | -maxBandwidth <
    positive_integer> | -monThreshold <positive_integer> | -
    downStateFlush ( ENABLED | DISABLED )] [-monitorName <string> -
    weight <positive_integer>] [-healthMonitor ( YES | NO )] [-comment <
    string>] [-appflowLog ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

So heben Sie die Einstellung von Parametern aus einer GSLB-Dienstgruppe auf:


```
unset gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port> [-
    weight] [-hashId] [-publicIP] [-publicPort]] [-maxClient] [-cip] [-
    cltTimeout] [-svrTimeout] [-maxBandwidth] [-monThreshold] [-
    appflowLog] [-monitorName] [-weight] [-healthMonitor] [-cipHeader]
    [-downStateFlush] [-comment]
<!--NeedCopy-->
```

So aktivieren Sie eine GSLB-Dienstgruppe

```
enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

Beispiel:

```
enable gslb serviceGroup SG1 S1 80
<!--NeedCopy-->
```

So deaktivieren Sie eine GSLB-Dienstgruppe

```
disable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-
    delay <secs>] [-graceFul ( YES /| NO )]
<!--NeedCopy-->
```

Beispiel:

```
disable gslb serviceGroup SRG2 S1 80
<!--NeedCopy-->
```

> **Hinweis**
>
> Die zu deaktivierende Dienstgruppe muss eine DBS-Dienstgruppe und keine Autoscale-Dienstgruppe sein.

So entfernen Sie eine GSLB-Dienstgruppe:

```
rm gslb serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
rm gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken einer GSLB-Dienstgruppe an:


```
stat gslb serviceGroup [<serviceGroupName>]
<!--NeedCopy-->
```

Beispiel:

```
stat gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften einer GSLB-Dienstgruppe an:

```
show gslb serviceGroup [<serviceGroupName>  -includeMembers]
<!--NeedCopy-->
```

Beispiel:

```
show gslb serviceGroup SG1
show gslb serviceGroup -includeMembers
<!--NeedCopy-->
```

Mitglieder der GSLB-Dienstgruppe aktivieren oder deaktivieren

Sie können ein einzelnes Mitglied einer GSLB-Dienstgruppe (DNS-basiert) selektiv aktivieren oder deaktivieren, anstatt die gesamte Dienstgruppe zu aktivieren oder zu deaktivieren. Diese Funktion ist sowohl in Dienstgruppen mit automatischer Skalierung als auch in Dienstgruppen ohne automatische Skalierung verfügbar. Daher wird die Verwaltung einer GSLB-Dienstgruppe erleichtert.

Sie müssen beispielsweise den Datenverkehr zu einem bestimmten Server auf einer GSLB-Site vermeiden. Nehmen wir an, 10 GSLB-Dienste oder -Server (S1 bis S10) sind an eine Dienstgruppe (SG1) gebunden. Sie möchten nur den Dienst 5 (S5) deaktivieren, d. h. den Datenverkehr zum Server 5 vermeiden. Ohne diese Funktion müssen Sie die Dienste S1 bis S4 und die Dienste S6 bis S10 separat binden. Dieser Vorgang wird in einer großen GSLB-Dienstgruppe langwierig, in der Sie eine große Anzahl von Diensten deaktivieren oder aktivieren müssen. Mit dieser Funktion können Sie Dienst 5 (S5) direkt deaktivieren, ohne andere Dienste in der Dienstgruppe zu beeinträchtigen.

So aktivieren Sie ein GSLB-Dienstgruppenmitglied mithilfe von CLI:

```
enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

> **Hinweis:**
>
> Um eine GSLB-Dienstgruppe zu aktivieren, geben Sie nur den Namen der Dienstgruppe an. Um ein Mitglied einer Dienstgruppe zu aktivieren, geben Sie zusätzlich zum GSLB-

> Dienstgruppennamen den Namen des Servers, der den Dienst hostet, und die Portnummer des Dienstes an.

Beispiel:

```
enable gslb serviceGroup http_svc_group 10.102.27.153 80
<!--NeedCopy-->
```

So deaktivieren Sie eine GSLB-Dienstgruppe oder ein Mitglied der GSLB-Dienstgruppe über die CLI:

```
disable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```

Beispiel:

```
disable gslb serviceGroup http_svc_group 10.102.27.153 80
<!--NeedCopy-->
```

> **Hinweis:**
>
> Um eine GSLB-Dienstgruppe zu deaktivieren, geben Sie nur den Namen der Dienstgruppe an. Um ein Mitglied einer Dienstgruppe zu deaktivieren, geben Sie zusätzlich zum GSLB-Dienstgruppennamen den Namen des Servers, der den Dienst hostet, und die Portnummer des Dienstes an.

Änderungen an den vorhandenen GSLB CLI-Befehlen

Im Folgenden sind die Änderungen aufgeführt, die nach der Einführung der GSLB-Dienstgruppen an den vorhandenen GSLB-Befehlen vorgenommen werden:

- `bind gslb vserver` - Der Name der Dienstgruppe wird zum Befehl bind hinzugefügt.

  Beispiel:

  ```
  bind gslb vserver <name> ((-serviceName <string> [-weight <
      positive_integer>] ) | <serviceGroupName>@ | | (-domainName <
      string> [-TTL <secs>] [-backupIP<ip_addr|ipv6_addr|*>] [-
      cookieDomain <string>] [-cookieTimeout <mins>][-sitedomainTTL
      <secs>]) | (-policyName <string>@ [-priority<positive_integer
      >] [-gotoPriorityExpression <expression>] [-type REQUEST |
      RESPONSE )]))
  <!--NeedCopy-->
  ```

- `unbind gslb vserver` - Die Dienstgruppe wurde zum Befehl unbind hinzugefügt.

  Beispiel:


```
unbind gslb vserver <name> (-serviceName <string> <
    serviceGroupName> @ /(-domainName <string> [-backupIP] [-
    cookieDomain]) | -policyName <string>@)
<!--NeedCopy-->
```

- `show gslb site` - Wenn dieser Befehl ausgeführt wird, werden auch die GSLB-Dienstgruppen angezeigt.
- `show gslb vs` - Wenn dieser Befehl ausgeführt wird, werden die GSLB-Dienstgruppen angezeigt.
- `stat gslb vs` - Wenn dieser Befehl ausgeführt wird, werden auch die Statistiken der GSLB-Dienstgruppen angezeigt.
- `show lb monitor bindings` - Wenn dieser Befehl ausgeführt wird, werden auch die GSLB-Dienstgruppenbindungen angezeigt.

Konfigurieren von GSLB-Dienstgruppen über die GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Service Groups**.
2. Erstellen Sie eine Dienstgruppe und setzen Sie den AutoScale-Modus auf DNS.

Konfigurieren der Sitepersistenz für die GSLB-Dienstgruppen

Sie können die Sitepersistenz für die auf IP-Adressen und Domänennamen basierenden Dienstgruppen konfigurieren. Sitepersistenz wird für Domänennamen-basierte Autoscale-Dienstgruppen nicht unterstützt.

So stellen Sie die Sitepersistenz basierend auf HTTP-Cookies über die CLI ein

- Für die Persistenz des Verbindungsproxys müssen Sie das Site-Präfix nicht festlegen.

  Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb service group <serviceGroupName> [-sitePersistence <
    sitePersistence>]
<!--NeedCopy-->
```

- Für die Persistenz der HTTP-Umleitung müssen Sie zuerst das Standortpräfix für ein Mitglied der Dienstgruppe festlegen und dann den `HTTPRedirect` Persistenzparameter für die Dienstgruppe festlegen.

  Geben Sie in der Befehlszeile Folgendes ein:


```
set gslb servicegroup <serviceGroupName>  <serviceGroup member
   name|Ip> <port>  [-sitePrefix <string>]

set gslb servicegroup <serviceGroupName> [-sitePersistence <
   sitePersistence>]
<!--NeedCopy-->
```

Beispiele:

- Persistenz des Verbindungsproxys

```
set gslbservicegroup sg1 -sitePersistence connectionProxy
<!--NeedCopy-->
```

- Beständigkeit der HTTP-Umleitung

```
set gslb servicegroup sg2 test1 80 -sitePrefix vserver-GSLB-1

set gslb servicegroup sg2 -sitePersistence HTTPRedirect
<!--NeedCopy-->
```

So legen Sie die Sitepersistenz basierend auf Cookies über die GUI fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services Groups** und wählen Sie die Dienstgruppe aus, die Sie für die Sitepersistenz konfigurieren möchten (z. B. ServiceGroup-GSLB-1).
2. Klicken Sie auf den Abschnitt **Sitepersistenz** und legen Sie die Persistenz fest, die Ihren Anforderungen entspricht.

> **Tipp**
>
> Informationen zum Bereitstellungsszenario und zur Beispielkonfiguration von GSLB-Dienstgruppen finden Sie in den folgenden Themen:
>
> - Anwendungsfall: Bereitstellung einer auf Domänennamen basierenden Autoscale-Dienstgruppe
> - Anwendungsfall: Bereitstellung der IP-adressbasierten Autoscale-Dienstgruppe

Konfigurieren eines virtuellen GSLB-Servers

May 11, 2023

Ein virtueller GSLB-Server ist eine Entität, die einen oder mehrere GSLB-Dienste repräsentiert und den Datenverkehr zwischen ihnen ausgleicht. Es wertet die konfigurierten GSLB-Methoden oder -Algorithmen aus, um einen GSLB-Dienst auszuwählen, an den die Client-Anfrage gesendet werden soll.

> **Hinweis**
>
> Eine GSLB-Serverprotokollanforderung besteht hauptsächlich darin, eine Beziehung zwischen dem virtuellen Server und den Diensten herzustellen, die an den virtuellen Server gebunden sind. Dadurch bleiben CLI/APIs auch für andere Arten von virtuellen Servern konsistent. Der Parameter Service Type auf einem Dienst oder einem virtuellen Server wird bei der Verarbeitung der DNS-Anfragen nicht verwendet. Es wird stattdessen während der Persistenz der Website, der Überwachung und der Suche über MEP referenziert.

So erstellen Sie einen virtuellen GSLB-Server über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile die folgenden Befehle ein, um einen virtuellen GSLB-Server hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add gslb vserver <name> <serviceType> -ipType (IPv4 | IPv6)
2 -  show gslb vserver <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add gslb vserver Vserver-GSLB-1 HTTP -ipType IPv4
2 add gslb vserver Vserver-GSLB-2 HTTP -ipType IPv6
3 show gslb vserver Vserver-GSLB-1
4 show gslb vserver Vserver-GSLB-2
5 <!--NeedCopy-->
```

So ändern oder entfernen Sie einen virtuellen GSLB-Server über die Befehlszeilenschnittstelle

- Verwenden Sie den Befehl `set gslb vserver`, um einen virtuellen GSLB-Server zu ändern. Dieser Befehl funktioniert ähnlich wie der Befehl `add gslb vserver`, außer dass Sie den Namen eines vorhandenen virtuellen GSLB-Servers eingeben.
- Um einen Parameter auf seinen Standardwert zurückzusetzen, können Sie den Befehl `unset gslb vserver` verwenden, gefolgt vom Wert vserverName und dem Namen des Parameters, der zurückgesetzt werden soll.
- Um einen virtuellen GSLB-Server zu entfernen, verwenden Sie den Befehl `rm gslb vserver`, der nur das Argument “name” akzeptiert.

So konfigurieren Sie einen virtuellen GSLB-Server mit dem Konfigurationsprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Fügen Sie einen neuen virtuellen GSLB-Server hinzu, oder wählen Sie einen vorhandenen virtuellen GSLB-Server aus und bearbeiten Sie seine Einstellungen.

So können Sie die Statistiken eines virtuellen GSLB-Servers über die Befehlszeilenschnittstelle anzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

So können Sie die Statistiken eines virtuellen GSLB-Servers über das Konfigurationsprogramm anzeigen

Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, wählen Sie den virtuellen Server aus und klicken Sie auf **Statistik**.

Statistiken für virtuelle GSLB-Server

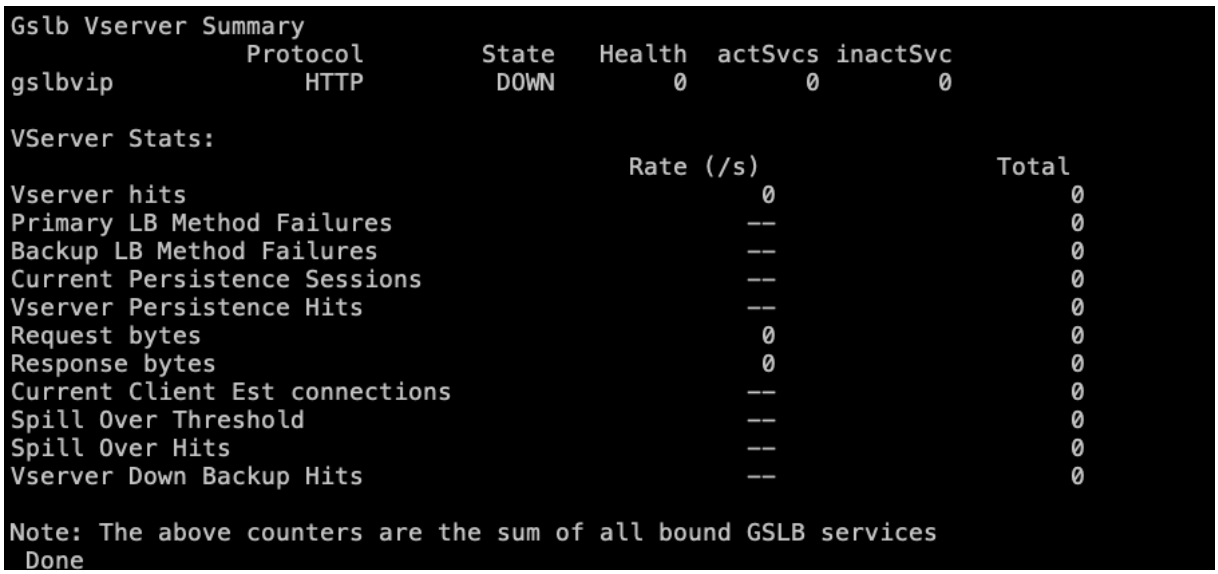
Ab NetScaler Version 12.1 Build 51.xx und höher zeigen die Statistiken des virtuellen GSLB-Servers zusätzlich zu Details wie: virtuelle Server-Treffer, aktuelle Persistenzsitzung, Anforderungsbytes, Antwortbytes, Spillover-Schwellenwert, Spillover-Treffer, aktuelle Client-Verbindungen und Backup-Treffer für den Ausfall des virtuellen Servers.

- **Fehler bei der primären LB-Methode**: Häufigkeit, mit der die primäre GSLB-Methode ausgefallen ist.
- **Fehler bei der Backup-LB-Methode**: Häufigkeit, mit der die Backup-GSLB-Methode ausgefallen ist.
- **Vserver-Persistenz-Treffer**: Gibt an, wie oft die Anfrage über die Persistenzsitzungen bedient wird.

Die Statistiken des virtuellen GSLB-Servers zeigen auch die Statistiken der an den virtuellen Server gebundenen Dienstgruppenmitglieder an.

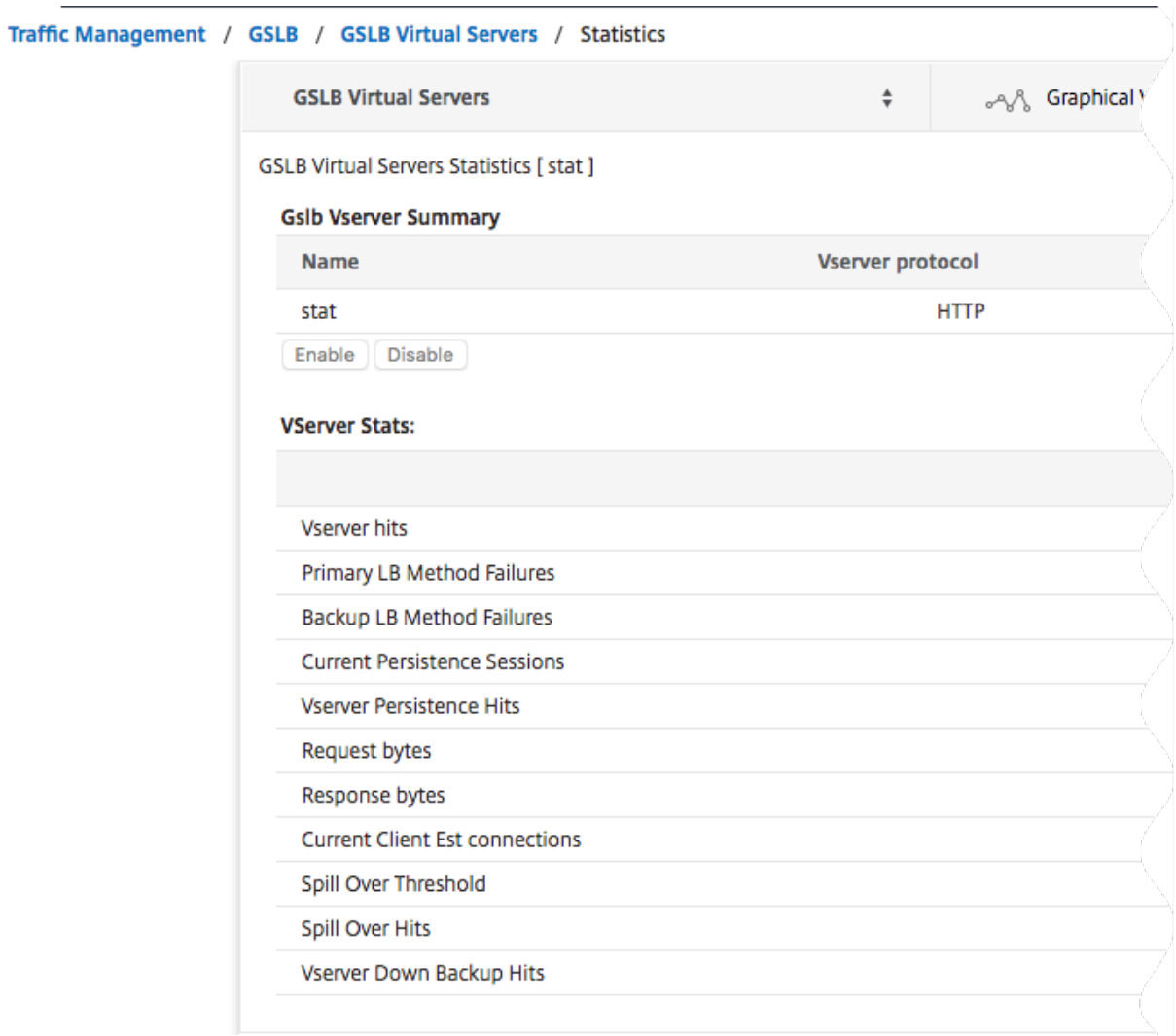
> **Hinweis:**
> Die primäre Methode oder die Backup-Methode kann fehlschlagen, wenn die primäre Methode statische Nähe und die Backup-Methode RTT ist. Wenn in diesem Szenario kein Standort vorhanden ist, der der LDNS-IP entspricht, schlägt die statische Nähe fehl und es wird versucht, die Backup-Methode zu verwenden. Die Statistiken werden auf der Grundlage der folgenden Informationen aktualisiert:
>
> - Wenn die Backup-Methode erfolgreich ist, werden nur die Fehlerstatistiken der primären Methode erhöht.
> - Wenn die RTT-Berechnung nicht erfolgreich ist, schlägt auch die Backup-Methode fehl. In diesem Fall werden die Fehlerstatistiken sowohl bei der Primär- als auch bei der Backup-Methode erhöht.
>
> Wenn die Backup-Methode fehlschlägt, wird die letzte Methode des Round-Robin-Verfahrens verwendet.

Das folgende Bild ist ein Beispiel für virtuelle GSLB-Serverstatistiken aus der CLI.



```
Gslb Vserver Summary
                Protocol        State   Health  actSvcs inactSvc
gslbvip             HTTP         DOWN        0        0        0

VServer Stats:
                                        Rate (/s)                Total
Vserver hits                                 0                       0
Primary LB Method Failures                  --                       0
Backup LB Method Failures                   --                       0
Current Persistence Sessions                --                       0
Vserver Persistence Hits                    --                       0
Request bytes                                0                       0
Response bytes                               0                       0
Current Client Est connections              --                       0
Spill Over Threshold                        --                       0
Spill Over Hits                             --                       0
Vserver Down Backup Hits                    --                       0

Note: The above counters are the sum of all bound GSLB services
 Done
```

Das folgende Bild ist ein Beispiel für Statistiken über virtuelle GSLB-Server von der GUI.



GSLB-Servicestatistik

Wenn Sie den Befehl `stat gslb service` von der Befehlszeile aus ausführen oder im Konfigurationsprogramm auf den **Link Statistik** klicken, werden die folgenden Details des Dienstes angezeigt:

- **Bytes anfordern.** Gesamtzahl der auf diesem Dienst oder virtuellen Server empfangenen Anforderungsbytes.
- **Antwortbytes.** Anzahl der Antwortbytes, die von diesem Dienst oder virtuellen Server empfangen wurden.
- **Der aktuelle Client hat Verbindungen hergestellt.** Anzahl der Client-Verbindungen im Status ETABLIERT.
- **Aktuelle Auslastung des Dienstes.** Auslastung des Dienstes (Wird anhand des an den Dienst gebundenen Lastmonitors berechnet).

Die Daten der Anzahl der Anfragen und Antworten sowie die Anzahl der aktuellen Client- und

Serververbindungen werden möglicherweise nicht angezeigt oder nicht mit den Daten des entsprechenden virtuellen Lastausgleichsservers synchronisiert.

Löschen der virtuellen GSLB-Server- oder Servicestatistiken

Hinweis: Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

Sie können jetzt die Statistiken eines virtuellen GSLB-Servers und -Dienstes löschen. NetScaler bietet die folgenden zwei Optionen zum Löschen der Statistiken:

- **Basic**: Löscht die Statistiken, die für den virtuellen Server spezifisch sind, behält jedoch die Statistiken bei, die vom gebundenen GLSB-Dienst bereitgestellt wurden.
- **Vollständig**: Löscht sowohl den virtuellen Server als auch die gebundenen GSLB-Dienststatistiken.

So löschen Sie die Statistiken eines virtuellen GSLB-Servers über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
stat gslb vserver <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb vserver Vserver-GSLB-1 - clearstats basic
<!--NeedCopy-->
```

So löschen Sie die Statistiken eines GSLB-Dienstes über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
stat gslb service <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb service service-GSLB-1 - clearstats basic
<!--NeedCopy-->
```

So löschen Sie die Statistiken eines virtuellen GSLB-Servers über das Konfigurationsprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie den virtuellen GSLB-Server aus, klicken Sie auf **Statistik**und dann auf **Löschen**.
3. Wählen Sie in der Dropdownliste **Löschen** die Option **Einfach** oder **Vollständig**aus, und klicken Sie dann auf **OK**.

So löschen Sie die Statistiken eines GSLB-Dienstes über das Konfigurationsprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Wählen Sie den GSLB-Dienst aus, klicken Sie auf **Statistik**und dann auf **Löschen**.
3. Wählen Sie in der Dropdownliste **Löschen** die Option **Einfach** oder **Vollständig**aus, und klicken Sie dann auf **OK**.

Virtuelle GSLB-Server aktivieren und deaktivieren

Wenn Sie einen virtuellen GSLB-Server erstellen, ist er standardmäßig aktiviert. Wenn Sie den virtuellen GSLB-Server deaktivieren, trifft die NetScaler-Appliance nach Erhalt einer DNS-Anfrage keine GSLB-Entscheidung auf der Grundlage der konfigurierten GSLB-Methode. Stattdessen enthält die Antwort auf die DNS-Abfrage die IP-Adressen aller Dienste, die an den virtuellen Server gebunden sind.

So aktivieren oder deaktivieren Sie einen virtuellen GSLB-Server über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
enable gslb vserver <name>@

disable gslb vserver <name>@
<!--NeedCopy-->
```

Beispiel:

```
enable gslb vserver Vserver-GSLB-1
disable gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie einen virtuellen GSLB-Server über das Konfigurationsprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus, und wählen Sie in der Liste **Aktion** die Option **Aktivieren** oder **Deaktivieren** aus.

Anwendungsfälle — virtueller GSLB-Server

Im Folgenden sind einige Anwendungsfälle aufgeführt, in denen Sie virtuelle GSLB-Server konfigurieren können:

- Konfigurieren Sie den virtuellen GSLB-Server, um das GSLB-Setup vor einem Ausfall zu schützen
- Persistenz in GSLB konfigurieren
- Konfigurieren Sie die GSLB-API-Methode

Binden von GSLB-Diensten an einen virtuellen GSLB-Server

January 19, 2021

Sobald die GSLB-Dienste und der virtuelle Server konfiguriert sind, müssen relevante GSLB-Dienste an den virtuellen GSLB-Server gebunden werden, um die Konfiguration zu aktivieren.

So binden Sie einen GSLB-Dienst mit der Befehlszeilenschnittstelle an einen virtuellen GSLB-Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen GSLB-Dienst an einen virtuellen GSLB-Server zu binden und die Konfiguration zu überprüfen:

```
bind gslb vserver <name> -serviceName <string>

show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
bind gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

So heben Sie die Bindung eines GSLB-Diensts von einem virtuellen GSLB-Server mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind gslb vserver <name> -serviceName <string>
<!--NeedCopy-->
```

So binden Sie GSLB-Dienste mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf einen virtuellen Server.

2. Klicken Sie in den Abschnitt **Domänen**, konfigurieren Sie eine Domäne und binden Sie die Domäne.

Binden einer Domäne an einen virtuellen GSLB-Server

May 11, 2023

Um eine NetScaler-Appliance zum autoritativen DNS-Server für eine Domäne zu machen, müssen Sie die Domäne an den virtuellen GSLB-Server binden. Wenn Sie eine Domäne an einen virtuellen GSLB-Server binden, fügt die NetScaler-Appliance einen Adressdatensatz für die Domäne hinzu, der den Namen des virtuellen GSLB-Servers enthält. Die Einträge für den Start von Autorität (SOA) und Nameserver (NS) für die GSLB-Domäne müssen manuell hinzugefügt werden.

Weitere Informationen zum Konfigurieren von SOA- und NS-Datensätzen finden Sie unter Domänennamensystem.

So binden Sie eine Domäne über die Befehlszeilenschnittstelle an einen virtuellen GSLB-Server

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Domäne an einen virtuellen GSLB-Server zu binden und die Konfiguration zu überprüfen:

```
bind gslb vserver <name> -domainName <string>
show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
bind gslb vserver Vserver-GSLB-1 -domainName www.mycompany.com
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

So trennen Sie die Bindung einer GSLB-Domäne von einem virtuellen GSLB-Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind gslb vserver <name> -domainName <string>
<!--NeedCopy-->
```


So binden Sie eine Domäne mithilfe des Konfigurationsdienstprogramms an einen virtuellen GSLB-Server

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie im Bereich GSLB Virtual Servers den virtuellen GSLB-Server aus, an den Sie die Domäne binden möchten (z. B. vServer-GSLB-1), und klicken Sie auf Öffnen.
3. Führen Sie im Dialogfeld Virtuellen GSLB-Server konfigurieren auf der Registerkarte Domänen eine der folgenden Aktionen aus:
   - Um eine neue Domain zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine bestehende Domain zu ändern, wählen Sie die Domain aus und klicken Sie dann auf **Öffnen**.
4. Geben Sie im Dialogfeld GSLB-Domäne erstellen oder GSLB-Domäne konfigurieren Werte für die folgenden Parameter an, wie hier gezeigt:
   - Domainname* — Domainname (z. B. www.mycompany.com)

   * Ein erforderlicher Parameter
5. Klicken Sie auf Erstellen.
6. Klicken Sie auf OK.

Um die Statistiken einer Domain mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat gslb domain <name>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb domain www.mycompany.com
<!--NeedCopy-->
```

Hinweis: Um Statistiken für eine bestimmte GSLB-Domäne anzuzeigen, geben Sie den Namen der Domäne genau so ein, wie er der NetScaler-Appliance hinzugefügt wurde. Wenn Sie den Domainnamen nicht oder einen falschen Domainnamen angeben, werden Statistiken für alle konfigurierten GSLB-Domains angezeigt.

So können Sie die Statistiken einer Domain mithilfe des Konfigurationsprogramms einsehen

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.

2. Wählen Sie im Bereich GSLB Virtual Servers den virtuellen GSLB-Server aus (z. B. vServer-GSLB-1) und klicken Sie auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen GSLB-Server konfigurieren auf der Registerkarte Domänen die Domäne aus, und klicken Sie dann auf **Statistik s.**

Um die Konfigurationsdetails der Entitäten, die an eine GSLB-Domäne gebunden sind, mithilfe der Befehlszeile anzuzeigen

Hinweis: Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

Geben Sie in der Befehlszeile Folgendes ein:

```
show gslb domain <name>
<!--NeedCopy-->
```

Beispiel:

```
show gslb domain gslb1.com
       gslb1.com
       gvs1 - HTTP    state: DOWN
       DNS Record Type: A
       Configured Method: LEASTCONNECTION
       Backup Method: ROUNDROBIN
       Persistence Type: NONE
       Empty Down Response: DISABLED
       Multi IP Response: DISABLED
       Dynamic Weights: DISABLED

       gsvc1 (10.102.239.165: 80)- HTTP State: DOWN    Weight: 1
              Dynamic Weight: 0    Cumulative Weight: 1
              Effective State: DOWN
              Threshold : BELOW

              Monitor Name : http
                     State: DOWN   Weight: 1
                     Probes: 144   Failed [Total: 144 Current: 144]
                     Last response: Failure - TCP syn sent, reset
                        received.
                     Response Time: 2000 millisec

       gsvc2 (10.102.239.179: 80)- HTTP State: DOWN    Weight: 1
              Dynamic Weight: 0    Cumulative Weight: 1
              Effective State: DOWN
              Threshold : BELOW

```



```
28                Monitor Name : http-ecv
29                       State: DOWN   Weight: 1
30                       Probes: 141   Failed [Total: 141 Current: 141]
31                       Last response: Failure - TCP syn sent, reset
                            received.
32                       Response Time: 2000 millisec
33 Done
34 <!--NeedCopy-->
```

Um die Konfigurationsdetails der Entitäten anzuzeigen, die an eine GSLB-Domäne gebunden sind, mithilfe des Konfigurationsdienstprogramms

Hinweis: Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server** und doppelklicken Sie auf einen virtuellen Server.
2. Klicken Sie auf das Feld unter dem Bereich **Domains** .
3. Wählen Sie im Dialogfeld **GSLB-Domänenbindung für virtuelle Server** eine Domäne aus, und klicken Sie dann auf **Bindungen anzeigen** .

Beispiel für eine GSLB-Setup und -Konfiguration

May 11, 2023

Eine Organisation verfügt über ein geografisch verteiltes Netzwerk und drei Rechenzentren in den Vereinigten Staaten, Mexiko und Kolumbien. In der Konfiguration, die sich auf diese Standorte bezieht, werden diese jeweils als US, MX und CO bezeichnet. An jedem Standort verfügt das Unternehmen über eine Serverfarm, die dieselben Inhalte bereitstellt, und das Setup funktioniert wie erwartet. Die NetScaler-Appliance an jedem Standort wird über einen virtuellen Server mit dem HTTP-Protokoll auf Port 80 konfiguriert.

Die Organisation hat das GSLB-Setup implementiert, indem an jedem Standort eine Standort-ID hinzugefügt wurde. Die Site-ID enthält einen Site-Namen und eine IP-Adresse, die der NetScaler-Appliance gehören und für die GSLB-Kommunikation verwendet werden.
Jeder Standort hat einen lokalen Standort für die Appliance. Außerdem verfügt jeder Standort über zwei Standorte, die von der lokalen Appliance entfernt sind. Auf jeder Site wird ein virtueller GSLB-Server mit demselben Namen erstellt. Dieser virtuelle Server identifiziert die Website der Organisation weltweit und ihm ist keine IP-Adresse zugeordnet.
Im Setup sind auch GSLB-Dienste konfiguriert, die auf die virtuellen Lastausgleichsserver verweisen,

die auf jeder GSLB-Website konfiguriert sind, indem die IP-Adresse, das Protokoll und die Portnummer des jeweiligen virtuellen Servers angegeben werden. Diese Dienste sind an den virtuellen GSLB-Server gebunden.

Hinweis: Im folgenden Verfahren verwenden die Befehle private IP-Adressen für die GSLB-Sites. Stellen Sie für öffentliche Websites und GSLB-Dienste sicher, dass Sie öffentliche IP-Adressen für diese Websites verwenden.

In der folgenden Tabelle sind die im Beispiel verwendeten IP-Adressen und Standorte aufgeführt:

IP-Adresse	Standort
10.3.1.101	Site-IP des lokalen NetScaler.
172.16.1.101	Standort-IP des Remote-Standorts Site-MX.
192.168.1.101	Standort-IP des entfernten Standorts Site-co.
172.16.1.100	Dienst-IP des Remote-Standorts Site-MX.
10.3.1.100	Dienst-IP des lokalen NetScaler.
192.168.1.100	Dienst-IP des Remote-Standorts Site-co.

Wenn Sie eine GSLB-Site hinzufügen und die Site nur über das Internet kommuniziert, verwenden Sie das Feld „Öffentliche IP“. Zum Beispiel, wenn zwischen den GSLB-Standorten keine VPN-Konnektivität von Standort zu Standort besteht.

So konfigurieren Sie das GSLB-Setup mit NetScaler-Appliances mithilfe der CLI-Befehle

1. Aktivieren Sie die GSLB-Funktion, falls dies noch nicht geschehen ist.

```
enable ns feature gslb
<!--NeedCopy-->
```

2. Identifizieren Sie ein SNIP, das zum Hinzufügen einer lokalen GSLB-Site dient.
3. Fügen Sie die GSLB-Site für die lokale NetScaler-Appliance hinzu.

```
add gslb site site-US 10.3.1.101
<!--NeedCopy-->
```

4. Fügen Sie die GSLB-Sites für die Remote-NetScaler-Appliances hinzu.

```
add gslb site site-MX 172.16.1.101
add gslb site site-CO 192.168.1.101
```



```
<!--NeedCopy-->
```

5. Fügen Sie den virtuellen GSLB-Server hinzu, der auf einen Dienst verweist, der im GSLB-Setup verwendet wird:

```
add gslb vserver gslb-lb HTTP
<!--NeedCopy-->
```

6. Fügen Sie die GSLB-Dienste für jede Site hinzu, die am GSLB-Setup teilnimmt:

```
add gslb service gslb_SVC30 172.16.1.100 HTTP 80 -siteName site-MX
add gslb service gslb_SVC10 10.3.1.100 HTTP 80 -siteName site-US
add gslb service gslb_SVC20 192.168.1.100 HTTP 80 -siteName site-
   CO
<!--NeedCopy-->
```

7. Binden Sie die GSLB-Dienste an den virtuellen GSLB-Server:

```
bind gslb vserver gslb-lb -serviceName gslb_SVC10
bind gslb vserver gslb-lb -serviceName gslb_SVC20
bind gslb vserver gslb-lb -serviceName gslb_SVC30
<!--NeedCopy-->
```

8. Binden Sie die Domain an den virtuellen GSLB-Server.

```
bind gslb vserver gslb-lb -domainName www.mycompany.com -TTL 30
<!--NeedCopy-->
```

9. Fügen Sie einen ADNS-Dienst hinzu, der die DNS-Abfragen überwacht.

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

Synchronisieren der Konfiguration in einem GSLB-Setup

May 11, 2023

In der Regel verfügt ein GSLB-Setup über einige Rechenzentren, wobei für jedes Rechenzentrum ein GSLB-Site konfiguriert ist. Konfigurieren Sie in jedem NetScaler, der an GSLB teilnimmt, einen GSLB-Standort als lokalen Standort und die anderen als Remote-Sites. Wenn Sie zu einem späteren Zeitpunkt einen anderen GSLB-Site hinzufügen, müssen Sie sicherstellen, dass die Konfiguration über

alle GSLB-Sites hinweg identisch ist. Sie können die GSLB-Konfigurationssynchronisierungsoption des NetScaler verwenden, um die Konfiguration über die GSLB-Sites hinweg zu synchronisieren.

Die NetScaler Appliance, von der Sie die Synchronisierungsoption verwenden, wird als “Hauptsitz” und die GSLB-Sites bezeichnet, auf denen die Konfiguration als “untergeordnete Websites” kopiert wird. Wenn Sie eine GSLB-Konfiguration synchronisieren, werden die Konfigurationen auf allen GSLB-Sites, die am GSLB-Setup teilnehmen, ähnlich der Konfiguration auf der Hauptsite vorgenommen.

Die Synchronisierung erfolgt nur auf den übergeordneten Sites. Die Synchronisierung hat keinen Einfluss auf die Konfiguration der untergeordneten GSLB-Websites. Dies liegt daran, dass die übergeordnete Site und die untergeordneten Sitekonfigurationen nicht identisch sind. Die Konfiguration der untergeordneten Sites besteht nur aus den Details ihrer eigenen und ihrer übergeordneten Site. Außerdem müssen GSLB-Dienste nicht immer in den untergeordneten Sites konfiguriert werden.

- Der Hauptknoten findet die Unterschiede zwischen der Konfiguration des Hauptknotens und des untergeordneten Knotens und ändert die Konfiguration des untergeordneten Knotens, um ihn dem Hauptknoten ähnlich zu machen.

  Wenn Sie eine Synchronisation erzwingen (verwenden Sie die Option “Sync erzwingen”), löscht die Appliance die GSLB-Konfiguration aus dem untergeordneten Knoten und konfiguriert dann den Untergebenen so, dass er dem Hauptknoten ähnelt.

- Wenn während der Synchronisation ein Befehl fehlschlägt, wird die Synchronisation nicht abgebrochen, und die Fehlermeldung wird in einer **ERR-Datei** im Verzeichnis **/var/netscaler/gslb** protokolliert.

- Die Synchronisierung erfolgt nur auf den übergeordneten Sites. Die Synchronisierung hat keinen Einfluss auf die Konfiguration der untergeordneten GSLB-Websites. Dies liegt daran, dass die übergeordnete Site und die untergeordneten Sitekonfigurationen nicht identisch sind. Die Konfiguration der untergeordneten Sites besteht nur aus den Details ihrer eigenen und ihrer übergeordneten Site. Außerdem müssen GSLB-Dienste nicht immer in den untergeordneten Sites konfiguriert werden.

- Wenn Sie die interne Benutzeranmeldung deaktivieren, verwendet die GSLB Auto-Synchronisierung die SSH-Schlüssel, um die Konfiguration zu synchronisieren. Um jedoch die automatische GSLB-Synchronisierung in der Partitionsumgebung verwenden zu können, müssen Sie die interne Benutzeranmeldung aktivieren und sicherstellen, dass der Partitionsbenutzername in den lokalen und Remote-GSLB-Sites identisch ist.

> **Hinweis**
>
> - Konfigurieren Sie auf dem RPC-Knoten des Remote-GSLB-Sites die Firewall so, dass sie Autosync-Verbindungen akzeptiert, indem Sie die Remote-Site-IP (Cluster-IP-Adresse für Cluster-Setup) und den Port (3010 für RPC und 3008 für sicheren RPC) angeben. Wenn sich die Standardroute zum Erreichen der Remote-Standorte wie in den meisten Fällen im Ver-

> waltungssubnetz befindet, wird NSIP als Quell-IP-Adresse verwendet.
>
> Um eine andere Quell-IP-Adresse zu konfigurieren, müssen Sie die GSLB-Site-IP-Adresse und das SNIP in einem anderen Subnetz haben. Außerdem müssen Sie über ein IP-Subnetz der GSLB-Standort-IP-Adresse eine explizite Route zur IP-Adresse des Remote-Standorts definiert haben.
>
> Zur Erhöhung der Sicherheit empfiehlt Citrix, dass Sie die Kennwörter für das interne Benutzerkonto und den RPC-Knoten ändern. Das Kennwort des internen Benutzerkontos wird durch das RPC-Knotenkennwort geändert. Weitere Informationen finden Sie unter Ändern eines RPC-Knotenkennworts.

Wenn Sie die Option saveconfig verwenden, speichern die Sites, die am Synchronisierungsprozess teilnehmen, ihre Konfiguration automatisch auf folgende Weise:

Konfigurieren Sie auf dem RPC-Knoten des Remote-GSLB-Sites die Firewall so, dass sie Autosync-Verbindungen akzeptiert, indem Sie die Remote-Site-IP (Cluster-IP-Adresse für Cluster-Setup) und den Port (3010 für RPC und 3008 für sicheren RPC) angeben. Wenn sich die Standardroute zum Erreichen der Remote-Standorte wie in den meisten Fällen in einem Verwaltungssubnetz befindet, wird NSIP als Quell-IP-Adresse verwendet.

Um eine andere Quell-IP-Adresse zu konfigurieren, müssen Sie die GSLB-Site-IP-Adresse und das SNIP in einem anderen Subnetz haben. Außerdem müssen Sie über das IP-Subnetz der GSLB-Site eine explizite Route zur IP-Adresse des Remote-Standorts definiert haben. Die Quell-IP-Adresse kann nicht über die an GSLB beteiligten Sites synchronisiert werden, da die Quell-IP-Adresse für einen RPC-Knoten für jede NetScaler Appliance spezifisch ist. Daher müssen Sie, nachdem Sie eine Synchronisation erzwungen haben (mithilfe des Befehls sync gslb config -ForceSync oder durch Auswahl der ForceSync-Option in der GUI), die Quell-IP-Adressen der anderen NetScaler-Appliances manuell ändern. Port 22 ist auch für die Synchronisierung der Datenbankdateien mit dem Remotestandort erforderlich.

Verbesserung der Zeit für die Konfigurationssynchronisierung auf allen GSLB-Sites

Konfigurieren Sie die TCP-Profileinstellungen an der Eingabeaufforderung wie folgt:

```
1 set tcpprofile nstcp_internal_apps -bufferSize 4194304 -sendBuffsize
     4194304 -tcpmode ENDPOINT
2 <!--NeedCopy-->
```

Einschränkungen der Synchronisation

- Auf der Hauptwebsite müssen die Namen der Remote-GSLB-Sites mit den Namen der Sites identisch sein, die auf den NetScaler Appliances konfiguriert sind, die diese Websites hosten.
- Während der Synchronisation können Verkehrsstörungen auftreten.

- NetScaler wird getestet, um bis zu 200.000 Zeilen der Konfiguration zu synchronisieren.
- Die Synchronisierung kann fehlschlagen:
  - Wenn die Überlaufmethode von CONNECTION in DYNAMIC CONNECTION geändert wird.
  - Wenn Sie das Standortpräfix der GSLB-Dienste austauschen, die an einen virtuellen GSLB-Server auf dem Hauptknoten gebunden sind, und versuchen Sie dann zu synchronisieren.
  - Wenn die RPC-Knotenkennwörter für NSIP- und Loopback-IP-Adresse unterschiedlich sind.
  - Wenn Sie die Synchronisierung auf GSLB-Sites durchführen, die in verschiedenen Partitionen derselben NetScaler Appliance konfiguriert sind.
- Wenn Sie die GSLB-Sites als Hochverfügbarkeitspaare (HA) konfiguriert haben, müssen die RPC-Knotenkennwörter von primären und sekundären Knoten identisch sein.
- Wenn Sie eine GLSB-Entität umbenennen, die Teil Ihrer GSLB-Konfiguration ist (verwenden Sie den Befehl “show gslb runningConfig”, um die GSLB-Konfiguration anzuzeigen). Sie müssen die Option Sync erzwingen verwenden, um die Konfiguration mit anderen GSLB-Sites zu synchronisieren.

> **Hinweis:**
>
> - Bei der inkrementellen Synchronisation müssen Sie die Option Sync erzwingen nicht verwenden, um die Konfiguration mit anderen GSLB-Sites zu synchronisieren. Dies gilt ab NetScaler Release 13.0 Build 79.x ab.

Hinweis: Um die Einschränkungen aufgrund einiger Einstellungen in der GSLB-Konfiguration zu überwinden, können Sie die Option “Synchronisierung erzwingen” verwenden. Wenn Sie jedoch die Option Force Sync verwenden, werden die GSLB-Entitäten entfernt und wieder zur Konfiguration hinzugefügt, und die GSLB-Statistiken werden auf Null zurückgesetzt. Daher wird der Verkehr während der Konfigurationsänderung unterbrochen.

Punkte, die Sie beachten sollten, bevor Sie mit der Synchronisation eines GSLB-Setups beginnen

Bevor Sie die Synchronisierung eines GSLB-Setups starten, stellen Sie sicher, dass:

- Auf allen GSLB-Sites einschließlich des Hauptstandorts müssen Verwaltungszugriff und SSH für die IP-Adresse der entsprechenden GSLB-Site aktiviert sein. Die IP-Adresse eines GSLB-Sites muss eine IP-Adresse sein, die der NetScaler Appliance gehört. Weitere Informationen zum Hinzufügen der IP-Adressen der GSLB-Site und zum Aktivieren des Verwaltungszugriffs finden Sie unter “Konfigurieren einer grundlegenden GSLB-Site”.
- Die GSLB-Konfiguration auf der NetScaler Appliance, die als Hauptstandort angesehen wird, ist vollständig und geeignet, um auf allen Standorten kopiert zu werden.
- Wenn Sie die GSLB-Konfiguration zum ersten Mal synchronisieren, müssen alle an GSLB teilnehmenden Websites über die GSLB-Standorteinheit ihrer jeweiligen lokalen Sites verfügen.

- Sie synchronisieren keine Sites, die nach Entwurf nicht über die gleiche Konfiguration verfügen.
- Der Hauptstandort und die untergeordneten Sites führen dieselben NetScaler-Versionen aus. Ab Version 12.1, Build 50.x, sucht die Appliance auf Haupt- und Unterstandorten nach der Firmware-Version, bevor die Synchronisierung initiiert wird. Wenn die Haupt- und die untergeordneten Websites verschiedene Versionen ausführen, wird die Synchronisierung für diesen Remote-Standort abgebrochen, um zu vermeiden, dass inkompatible Änderungen über die Versionen hinweg vorgenommen werden. Außerdem wird eine Fehlermeldung mit den Standortdetails angezeigt, auf denen die Synchronisation abgebrochen wurde.

  Die folgenden Abbildungen zeigen beispielhafte Fehlermeldungen von der CLI und der GUI.

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------------
        Site Name               Status          Reason
-------------------------------------------------------------------------------------------------------------------
        s2                      Failure         Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                      Success         All Done
        s3                      Success         All Done
Done
>
```

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------------
        Site Name               Status          Reason
-------------------------------------------------------------------------------------------------------------------
        s2                      Failure         Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                      Success         All Done
        s3                      Success         All Done
Done
>
```

Wichtig

Die folgenden Verzeichnisse werden im Rahmen der GSLB-Konfigurationssynchronisierung synchronisiert.

- /var/netscaler/locdb/
- /var/netscaler/ssl/
- /var/netscaler/inbuilt_db/

Manuelle Synchronisation zwischen Standorten, die an GSLB teilnehmen

May 11, 2023

Die manuelle Synchronisation der GSLB-Konfiguration zwischen dem Master-Site und den Slave-Standorten erfolgt auf folgende Weise:

- Der Master-Site erkennt die Unterschiede zwischen der Konfiguration seiner eigenen Site und der Slave-Site.
- Die Master-Site wendet den Unterschied in der Konfiguration auf die Slave-Site an.
- Die Master-Site führt die Konfigurationssynchronisierung mit allen Slave-Sites im GSLB-Setup durch und schließt den Synchronisationsprozess ab.

Wichtig: Nachdem eine GSLB-Konfiguration synchronisiert wurde, kann die Konfiguration auf keiner der GSLB-Sites rückgängig gemacht werden. Führen Sie die Synchronisation nur durch, wenn Sie sicher sind, dass der Synchronisationsprozess die Konfiguration auf der Remote-Site nicht überschreibt. Eine Standortsynchronisierung ist unerwünscht, wenn die lokalen und die Remote-Standorte von Natur aus unterschiedliche Konfigurationen haben, was zu einem Ausfall des Standorts führt. Wenn einige Befehle fehlschlagen und einige Befehle erfolgreich sind, werden die erfolgreichen Befehle nicht rückgängig gemacht.

Wichtige Hinweise

- Wenn Sie eine Synchronisation erzwingen (verwenden Sie die Option „Synchronisierung erzwingen“), löscht die NetScaler-Appliance die GSLB-Konfiguration von der Slave-Site. Anschließend konfiguriert die Master-Site die Slave-Site so, dass sie ihrer eigenen Site ähnelt.
- Wenn während der Synchronisation ein Befehl fehlschlägt, wird die Synchronisation nicht abgebrochen. Die Fehlermeldungen werden in einer .err-Datei im Verzeichnis /var/netscaler/gslb protokolliert.
- Wenn Sie die `saveconfig` Option verwenden, speichern die am Synchronisierungsprozess beteiligten Sites ihre Konfiguration automatisch auf folgende Weise:
  - Die Master-Site speichert ihre Konfiguration unmittelbar bevor sie den Synchronisationsprozess einleitet.
  - Die Slave-Sites speichern ihre Konfiguration, nachdem der Synchronisationsprozess abgeschlossen ist. Eine Slave-Site speichert ihre Konfiguration nur, wenn der Konfigurationsunterschied erfolgreich auf sie angewendet wurde. Wenn die Synchronisation auf einer Slave-Site fehlschlägt, müssen Sie die Ursache des Fehlers manuell untersuchen und Abhilfemaßnahmen ergreifen.

Um eine GSLB-Konfiguration mit der CLI zu synchronisieren:

Geben Sie an der Befehlszeile die folgenden Befehle ein, um GSLB-Sites zu synchronisieren und die Konfiguration zu überprüfen:

```
sync gslb config [-preview | -forceSync <string> | -nowarn | -
   saveconfig] [-debug]
show gslb syncStatus
<!--NeedCopy-->
```

Beispiel:

```
sync gslb config

[WARNING]: Syncing config may cause configuration loss on other site.

Please confirm whether you want to sync-config (Y/N)? [N]:y

Sync Time: Dec 9 2011 10:56:9

Retrieving local site info: ok

Retrieving all participating gslb sites info: ok

Gslb_site1[Master]:

Getting Config: ok

Gslb_site2[Slave]:

Getting Config: ok

Comparing config: ok

Applying changes: ok

Done
<!--NeedCopy-->
```

So synchronisieren Sie eine GSLB-Konfiguration mithilfe der GUI:

1. Navigieren Sie zu **Traffic Management > GSLB > Dashboard**.
2. Klicken Sie auf **Auto Synchronization GSLB** und wählen Sie **ForceSYN**aus.
3. Wählen Sie unter **GSLB-Site-Name**die GSLB-Sites aus, die mit der Master-Knotenkonfiguration synchronisiert werden sollen.

Vorschau der GSLB-Synchronisation

In der Vorschau des GSLB-Synchronisierungsvorgangs können Sie die Unterschiede zwischen dem Masterknoten und den einzelnen Slave-Knoten erkennen. Wenn es Abweichungen gibt, können Sie eine Fehlerbehebung durchführen, bevor Sie die GSLB-Konfiguration synchronisieren.

Um eine Vorschau der GSLB-Synchronisationsausgabe mit der CLI anzuzeigen:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
sync gslb config -preview
<!--NeedCopy-->
```

Um eine Vorschau der GSLB-Synchronisationsausgabe mithilfe der GUI anzuzeigen:

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard**.
2. Klicken Sie auf **Automatische Synchronisation GSLB** und wählen Sie **Vorschau**.
3. Klicken Sie auf **Ausführen**.
   In einem Fortschrittsfenster werden alle Abweichungen in der Konfiguration angezeigt.

Debuggen der während des Synchronisierungsprozesses ausgelösten Befehle

Sie können den Status (Erfolg oder Misserfolg) jedes Befehls einsehen, der während des Synchronisationsprozesses ausgelöst wurde, und die entsprechenden Fehler beheben.

So debuggen Sie die GSLB-Synchronisationsbefehle mithilfe der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
sync gslb config -debug
<!--NeedCopy-->
```

So debuggen Sie die GSLB-Synchronisationsbefehle mithilfe der GUI:

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard**.
2. Klicken Sie auf **Automatische Synchronisation GSLB** und wählen Sie **Debug**aus.
3. Klicken Sie auf **Ausführen**. Ein Fortschrittsfenster zeigt den Status jedes Befehls an, der während der Synchronisation ausgelöst wurde.

Echtzeit-Synchronisation zwischen Websites, die an GSLB teilnehmen

May 11, 2023

Sie können den `AutomaticConfigSync` Parameter verwenden, um die GSLB-Konfiguration des Hauptstandorts in Echtzeit automatisch mit allen untergeordneten Standorten zu synchronisieren. Sie müssen die AutoSync-Option nicht manuell auslösen, um die Konfiguration zu synchronisieren.

Sie können die GSLB-Konfiguration des Hauptstandorts automatisch mit allen untergeordneten Sites synchronisieren, indem Sie eine inkrementelle Synchronisierung oder eine vollständige Synchronisierung verwenden. Mit dem `GSLBSyncMode` Parameter können Sie den Synchronisationsmodus wählen.

> Hinweis:
>
> Ab NetScaler Release 13.0 Build 79.x wird die inkrementelle Synchronisation der GSLB-Synchronisation unterstützt. Standardmäßig wird die Synchronisation mittels inkrementeller Synchronisation durchgeführt. Inkrementelle Synchronisierung kann durch Aktivieren des `IncrementalSync` Parameters durchgeführt werden. Einzelheiten finden Sie unter Inkrementelle Synchronisierung der GSLB-Konfiguration.

Best Practices für die Verwendung der Echtzeitsynchronisierungsfunktion

- Es wird empfohlen, dass alle als Standorte teilnehmenden NetScaler-Appliances über die SameNetScaler-Softwareversion verfügen.
- Um das RPC-Knotenkennwort zu ändern, ändern Sie zuerst das Kennwort auf der untergeordneten Website und dann auf der Hauptwebsite.
- Konfigurieren Sie lokale GSLB-Sites auf jedem Standort, der an GSLB beteiligt ist.
- Aktivieren Sie AutomaticConfigSync auf einer der Sites, an denen die Konfiguration durchgeführt wird. Diese Seite wird schließlich mit anderen GSLB-Sites synchronisiert.
- Wenn eine neue Konfiguration vorliegt oder Änderungen an der vorhandenen Konfiguration vorgenommen werden, überprüfen Sie den Status mithilfe des `show gslb syncStatus` Befehls, um zu bestätigen, ob die Änderungen an allen Standorten synchronisiert wurden oder ob ein Fehler aufgetreten ist.
- Die RSYNC-Portüberwachung muss aktiviert sein.

So aktivieren Sie die Echtzeitsynchronisierung mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb parameter [ - automaticConfigSync (ENABLED | DISABLED)] [-
    MEPKeepAliveTimeout <secs>]  [-GSLBSyncMode ( IncrementalSync |
    FullSync )] [-GSLBSyncLocFiles ( ENABLED | DISABLED)] [-
    GslbConfigSyncMonitor ( ENABLED | DISABLED )] [-GSLBSyncInterval <
    secs>] [-GSLBSyncSaveConfigCommand ( ENABLED | DISABLED )]
<!--NeedCopy-->
```


Beispiel:

```
set gslb parameter  - automaticConfigSync ENABLED
<!--NeedCopy-->
```

Die Echtzeitsynchronisierung bietet die folgenden konfigurierbaren Parameter:

- **gslbSyncMode -Modus**, in dem die Konfiguration vom Hauptstandort zu Remote-Standorten synchronisiert wird.
  - Mögliche Werte: IncrementalSync, FullSync
  - Standardwert: IncrementalSync
- **gslbSynclocFiles**—Während der GSLB-Konfigurationssynchronisation werden die Änderungen an den Speicherort DB-Dateien standardmäßig erkannt und automatisch synchronisiert. Da sich die Speicherort-DB-Verzeichnisse nicht häufig ändern, können Administratoren die automatische Synchronisierung der Speicherort-DB-Dateien deaktivieren. Stattdessen müssen Administratoren die DB-Dateien des Speicherorts manuell auf die untergeordneten GSLB-Websites kopieren. Das Synchronisieren von StandortdB-Dateien benötigt viel Zeit. Dadurch wird die gesamte Synchronisationszeit reduziert.

  Beispiel zum Deaktivieren der automatischen Synchronisierung der Speicherort-DB-Dateien:

  ```
  set gslb parameter -GSLBSyncMode IncrementalSync -
     GSLBSyncLocFiles DISABLED
  <!--NeedCopy-->
  ```

- **GSLBConfigSyncMonitor**— Aktivieren Sie den Parameter GSLB Config Sync Monitor, um den Status des RSYNC-Ports der untergeordneten Standorte zu überwachen, bei dem es sich um den SSH-Port 22 auf der Remote-GSLB-Site-IP-Adresse handelt. Wenn der Monitor den untergeordneten Standortstatus als DOWN anzeigt, wird der RSYNC-Vorgang zu dieser Site übersprungen. Dies reduziert die Verzögerungen bei der Synchronisation, die durch den Versuch verursacht werden, eine Verbindung zu den Remote-Standorten herzustellen, die DOWN sind.

  Beispiel zum Aktivieren der RSYNC-Portüberwachung in der CLI:

  ```
  set gslb parameter -GSLBSyncMode IncrementalSync -
     GslbConfigSyncMonitor ENABLED
  <!--NeedCopy-->
  ```

- **gslbSyncInterval**—Legt das Zeitintervall (in Sekunden) fest, in dem die GSLB-Konfigurationssynchronisation stattfindet. Standardmäßig synchronisiert die Funktion zur automatischen GSLB-Konfiguration die GSLB-Konfiguration automatisch alle 10 Sekunden. Sie können das Zeitintervall auf einen beliebigen Wert ändern. Verzichten Sie darauf, dies auf einen niedrigeren Wert zu setzen, z.

B. nicht weniger als 5 Sekunden. Weil eine häufige Synchronisierung den CPU-Verbrauch des Managements erhöhen kann.

> Hinweis:
>
> In einem Setup der Admin-Partition kann das Zeitintervall nur in der Standardpartition festgelegt werden, da es sich um einen globalen Parameter handelt.

Beispiel zum Festlegen des Synchronisierungsintervalls:

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
   IncrementalSync -GSLBSyncInterval 7
<!--NeedCopy-->
```

- **gslbSyncSaveConfigCommand**—Aktivieren Sie diesen Parameter, um den `save ns config` Befehl mit untergeordneten Sites zu synchronisieren, wenn die `AutomaticConfigSync` Option aktiviert ist.

  Beispiel zum Aktivieren der Synchronisierung des Befehls "Konfiguration speichern":

```
set gslb parameter -AutomaticConfigSync ENABLED -
   GSLBSyncSaveConfigCommand ENABLED
<!--NeedCopy-->
```

  Der `save ns config` Befehl wird in bestimmten Szenarien wie folgt nicht mit untergeordneten Sites synchronisiert:

  - Die untergeordnete Site ist ausgefallen oder nicht erreichbar, wenn die Konfiguration auf der Hauptwebsite gespeichert wird.
  - Die Konfiguration an einer untergeordneten Site ist fehlgeschlagen.

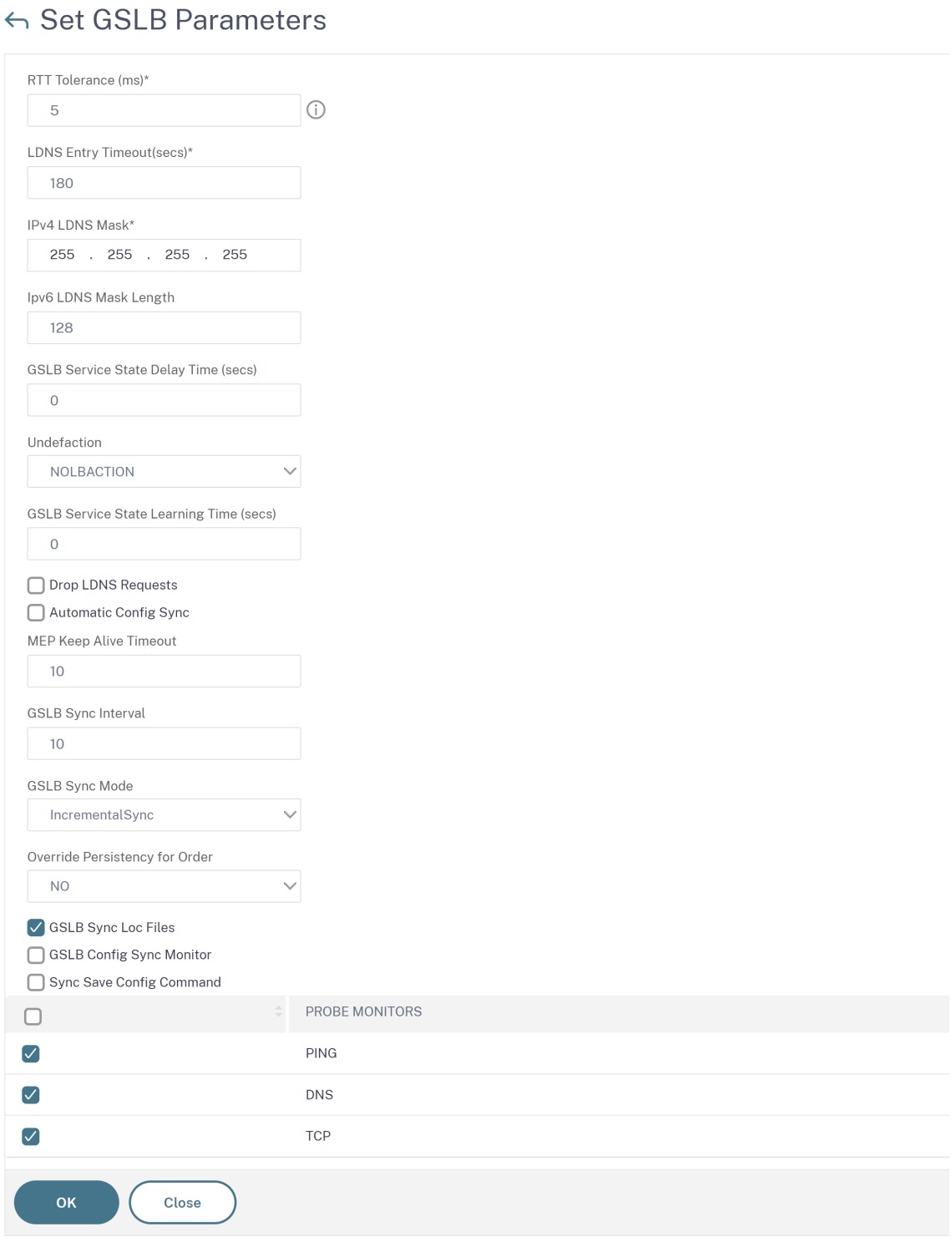
So aktivieren Sie die Echtzeitsynchronisierung über die GUI

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **GSLB-Einstellungen ändern**.
2. Auf der Seite **GSLB-Parameter festlegen** können Sie Folgendes ausführen:
   - Um die GSLB-Konfiguration in Echtzeit automatisch zu synchronisieren, wählen Sie **Automatic ConfigSync**.

   Hinweis: Diese Option muss nur an dem Standort aktiviert werden, an dem die Konfiguration ausgeführt wird.

   - Um das Intervall für die automatische GSLB-Konfiguration einzustellen, geben Sie die Zeit in Sekunden in das Feld **GSLB-Synchronisierungsintervall** ein.
   - Um die RSYNC-Portüberwachung zu aktivieren, aktivieren Sie das Kontrollkästchen **GSLB Config Sync Monitor** .

- Deaktivieren Sie das Kontrollkästchen **GSLB Sync Loc Files, um die automatische Synchronisierung der Speicherort DB-Dateien** zu deaktivieren.
- Um die Synchronisierung des `save ns config` Befehls mit den untergeordneten Sites zu ermöglichen, aktivieren Sie das Kontrollkästchen **Konfigurationsbefehl speichern synchronisieren** .



Informationen zu den folgenden Themen finden Sie unter Manuelle Synchronisierung zwischen Websites, die an GSLB teilnehmen.

- Vorschau der GSLB-Synchronisation
- Debuggen der während des Synchronisationsvorgangs ausgelösten Befehle

Wichtige Hinweise

- Die konsolidierte Protokolldatei, die sich auf die Echtzeitsynchronisation bezieht, wird im Verzeichnis /var/netscaler/gslb/periodic_sync.log gespeichert.
- Die Standardkonfigurationsdatei wird im Verzeichnis /var/netscaler/gslb_sync/ gespeichert.
- Die Hauptwebsite verwendet die folgende Verzeichnisstruktur:
  - Die Hauptwebsite speichert alle ihre Dateien im Verzeichnis /var/netscaler/gslb_sync/master.
  - Die Hauptwebsite speichert ihre Konfigurationsdatei, die mit den untergeordneten Sites synchronisiert werden muss, im Verzeichnis /var/netscaler/gslb_sync/master/gslbconf/.
  - Die Statusdateien, die von allen untergeordneten Sites abgerufen werden, werden im Verzeichnis /var/netscaler/gslb_sync/master/slavestatus/ gespeichert.
- Die untergeordnete Site verwendet die folgende Verzeichnisstruktur:
  - Die untergeordnete Site nimmt die neueste Konfigurationsdatei ab, die aus dem Verzeichnis /var/netscaler/gslb_sync/slave/gslbconf angewendet werden soll.
  - Die untergeordnete Site speichert ihre Statusdatei im Verzeichnis /var/netscaler/gslb_sync/slave/gslbst
- In einem Admin-Partitions-Setup wird dieselbe Verzeichnisstruktur am Speicherort beibehalten: /var/partitions/`partition name`/netscaler/gslb_sync.
- Die Uhren auf allen Standorten müssen genau auf einen Echtzeitstandard wie Coordinated Universal Time (UTC) eingestellt sein.

Inkrementelle Synchronisation der GSLB-Konfiguration

Die automatische GSLB-Konfigurationssynchronisierungsfunktion prüft im Intervall alle 10 Sekunden auf die Konfigurationsänderungen am Hauptstandort und führt eine Synchronisation durch. Dieser Wert des Synchronisierungsintervalls ist konfigurierbar.

Bei der inkrementellen Synchronisation werden nur die Konfigurationen, die sich am Hauptstandort zwischen der letzten Synchronisation und dem anschließenden Synchronisierungsintervall (10 Sekunden) geändert haben, an allen untergeordneten Standorten synchronisiert. Die inkrementelle Synchronisation ist das Standardverhalten. Wenn Sie nur die inkrementellen Konfigurationen drücken, wird die Größe der Konfigurationsdatei und damit die Synchronisationszeit erheblich reduziert. Wenn eine inkrementelle Synchronisation fehlschlägt, führt das System automatisch eine vollständige Konfigurationssynchronisation durch.

Die inkrementelle Synchronisation wird auf folgende Weise durchgeführt:

- Die Haupt-Site verschiebt die Konfigurationsdatei, die nur aus den neuesten Änderungen besteht, an alle untergeordneten Websites. Die letzte Änderung bezieht sich auf die Konfigurationen, die sich zwischen der letzten Synchronisation und dem anschließenden Synchronisierungsintervall (10 Sekunden) geändert haben.
- Jede untergeordnete Website wendet die letzte Änderung auf ihre eigene Website an.
- Inkrementelle Synchronisation wird nicht auf den untergeordneten Standorten versucht, die sich im Zustand DOWN befinden. Wenn die Site wieder nach oben kommt, wird erneut die Synchronisierung durchgeführt.
- Die untergeordnete Site generiert bei jedem Schritt Statusprotokolle und kopiert sie in eine Datei an einem bestimmten Speicherort.
- Die Haupt-Site ruft die Statusprotokolldateien vom angegebenen Speicherort ab.
- Die Hauptwebsite erstellt eine Protokolldatei mit Protokollen, die von allen untergeordneten Websites kombiniert werden.
- Diese kombinierte Protokolldatei wird in der Datei "/var/netscaler/gslb/periodic_sync.log" gespeichert.

Weitere Informationen zu den Verzeichnissen, in denen die Konfigurationsdateien gespeichert sind, finden Sie im Abschnitt Verweist auf Hinweis .

So aktivieren Sie die inkrementelle Synchronisation der GSLB-Konfiguration mit der CLI

```
set gslb parameter -AutomaticConfigSync (ENABLED | DISABLED) -
    GSLBSyncMode (IncrementalSync | FullSync) -GslbConfigSyncMonitor (
    ENABLED | DISABLED) -GSLBSyncInterval <secs> -GSLBSyncLocFiles (
    ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
    IncrementalSync
<!--NeedCopy-->
```

So aktivieren Sie die inkrementelle GSLB-Synchronisation mit der GUI

1. Navigieren Sie zu **Traffic Management > GSLB > Dashboard > GSLB-Einstellungen ändern**.
2. Wählen Sie auf der Seite **GSLB-Parameter festlegen** im Dropdown-Menü **GSLB Sync Modedie Option IncrementalSync** .

Vollständige Synchronisation der GSLB-Konfiguration

Immer wenn es eine Konfigurationsänderung am Hauptstandort gibt, wird die vollständige GSLB-laufende Konfiguration auf dem Hauptstandort an alle untergeordneten Standorte weitergeleitet. Selbst wenn die inkrementelle Synchronisation konfiguriert ist, wird eine vollständige Synchronisation durchgeführt, wenn der Hauptstandort den Konfigurationsstatus des untergeordneten Standorts nicht kennt. Einige dieser Szenarien lauten wie folgt:

- Aktivieren Sie zum ersten Mal die Funktion zur automatischen GSLB-Konfigurationssynchronisierung.
- Starten Sie die NetScaler-Appliance neu.
- Die GSLB-Bereitstellung verfügt über mehrere Hauptstandorte, und eine andere Hauptwebsite wird zur aktiven Hauptwebsite.
- Fügen Sie der GSLB-Bereitstellung eine neue untergeordnete Site hinzu.

Die vollständige Synchronisation der GSLB-Konfiguration erfolgt auf folgende Weise:

- Die Haupt-Site verschiebt ihre neueste Konfigurationsdatei an alle untergeordneten Sites.
- Jede untergeordnete Site vergleicht ihre eigene Konfiguration mit der neuesten Konfigurationsdatei, die vom Hauptstandort gesendet wird. Die untergeordnete Site identifiziert den Unterschied in der Konfiguration und wendet die Delta-Konfiguration für einen eigenen Standort an.
- Die untergeordnete Site generiert bei jedem Schritt Statusprotokolle und kopiert sie in eine Datei an einem bestimmten Speicherort.
- Die Haupt-Site ruft die Statusprotokolldateien vom angegebenen Speicherort ab.
- Die Hauptwebsite erstellt eine Protokolldatei mit Protokollen, die von allen untergeordneten Websites kombiniert werden.
- Diese kombinierte Protokolldatei wird in der Datei “/var/netscaler/gslb/periodic_sync.log” gespeichert.

Wenn Sie versuchen, eine Site manuell (mit dem `sync gslb config` Befehl) zu synchronisieren, während sie automatisch synchronisiert wird, wird eine Fehlermeldung “Sync in Bearbeitung” angezeigt. Die automatische Synchronisierung kann nicht für einen Standort ausgelöst werden, der derzeit manuell synchronisiert wird.

> **Achtung:**
>
> Ab NetScaler 12.1 Build 49.37 werden SNMP-Traps generiert, wenn Sie die GSLB-Konfiguration synchronisieren. Bei der Echtzeitsynchronisierung wird der Synchronisationsstatus im ersten SNMP-Trap als Ausfall erfasst. Sie können diesen Status ignorieren, da unmittelbar nach der ersten Trap automatisch eine zweite SNMP-Trap mit dem tatsächlichen Synchronisationsstatus generiert wird. Wenn die Synchronisierung jedoch auch im zweiten Versuch fehlgeschlagen ist, wird SNMP-Trap nicht generiert, da sich der Synchronisationsstatus nicht vom vorherigen Synchronisationsstatus geändert hat.

Weitere Informationen zum Konfigurieren der NetScaler-Appliance zum Generieren von Traps finden Sie unter Konfigurieren des NetScaler zum Generieren von SNMP-Traps.

So aktivieren Sie die vollständige GSLB-Synchronisation mit der CLI

```
set gslb parameter -GSLBSyncMode (IncrementalSync | FullSync)
<!--NeedCopy-->
```

Beispiel:

```
set gslb parameter -GSLBSyncMode FullSync
<!--NeedCopy-->
```

So aktivieren Sie die inkrementelle GSLB-Synchronisation mit der GUI:

1. Navigieren Sie zu **Traffic Management > GSLB > Dashboard > GSLB-Einstellungen ändern**.
2. Wählen **Sie auf der Seite GSLB-Parameter festlegen** im Dropdownmenü **GSLB-Synchronisierungsmodus die Option FullSyncMode** aus.

Mehrere Hauptstandorte in einer GSLB-Bereitstellung

Die NetScaler-Appliance unterstützt mehrere Hauptstandorte in einer aktiv-passiven Bereitstellung. Es wird empfohlen, zwei Hauptstandorte in einer GSLB-Bereitstellung zu haben, um den Ausfall des GSLB-Hauptstandorts zu bewältigen. Zwei Hauptstandorte können einen einzelnen Ausfallpunkt der GSLB-Konfigurationssynchronisation vermeiden. Zu jeder Zeit kann nur ein Hauptstandort die GSLB-Konfiguration vom Benutzer aktiv verarbeiten. Wenn die Konfigurationsänderungen gleichzeitig an mehreren Hauptstandorten durchgeführt werden, kann dies zu Konfigurationsinkonsistenz oder Konfigurationsverlusten führen. Daher wird empfohlen, Konfigurationsänderungen von jeweils nur einem Hauptstandort aus durchzuführen und den anderen Hauptstandort als Backup zu verwenden, wenn der aktive Hauptstandort ausfällt.

> Hinweis:
>
> Wenn mehrere Hauptstandorte in einer GSLB-Bereitstellung verwendet werden, muss die RSYNC-Überwachung aktiviert sein.

Führen Sie den folgenden Befehl aus, um einen GSLB-Knoten als einen der Hauptstandorte für die GSLB-Konfigurationssynchronisation zu erstellen:

```
set gslb parameter -automaticConfigSync Enabled
<!--NeedCopy-->
```

GSLB-Synchronisationsstatus und Zusammenfassung anzeigen

December 7, 2021

Nachdem die GSLB-Konfiguration über die GSLB-Sites synchronisiert wurde, können Sie den detaillierten Status und die Zusammenfassung des letzten GSLB-Synchronisierungsvorgangs anzeigen. Dies gilt sowohl für die manuelle als auch für die Echtzeitsynchronisation GSLB.

So zeigen Sie den GSLB-Synchronisationsstatus oder die Zusammenfassung mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show gslb sync status
<!--NeedCopy-->
```

oder

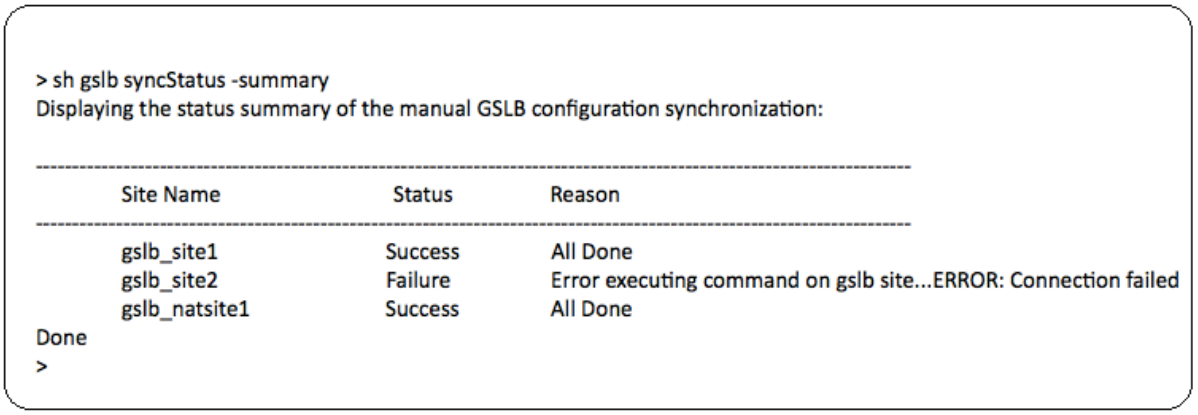
```
show gslb syncStatus -summary
<!--NeedCopy-->
```

Beispiel-Konfigurationsausgabe für die manuelle GSLB-Synchronisierung

Die folgende Ausgabe zeigt den Status der manuellen GSLB-Konfigurationssynchronisierung an.

```
> sh gslb syncStatus
Displaying the status of the manual GSLB configuration synchronization:

gslb_site1[Master]:
        Getting Config:  ok
gslb_site2[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
gslb_natsite1[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
 Done
>
```


Die folgende Ausgabe zeigt die Statusübersicht der manuellen GSLB-Konfigurationssynchronisierung an.



```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------
        Site Name                Status          Reason
-------------------------------------------------------------------------------------------------------
        gslb_site1               Success         All Done
        gslb_site2               Failure         Error executing command on gslb site...ERROR: Connection failed
        gslb_natsite1            Success         All Done
Done
>
```

Beispiel-Konfigurationsausgabe für GSLB-Echtzeitsynchronisation

Die folgende Ausgabe zeigt den Status der Echtzeit-GSLB-Konfigurationssynchronisierung für die Master Site an:

```
> sh gslb syncStatus
Displaying the status of the real time GSLB configuration
    synchronization as master node:

site2[Master]:
                New GSLB configuration detected at Fri Jan 23 20:54:24
                    2020
                Fetching current configuration: Done
                Updating default.conf file: Done
site1[Slave]:
                Syncing gslb static proximity database to node site1:
                    Done
                Syncing inbuilt GSLB static proximity database to node
                    site1: Done
                Syncing ssl certificates, keys and CRLS to node site1:
                    Done
                Syncing current configuration to site1: Done
                Pulling status files from site1: Status file not
                    available yet(Sync in progress)
                Pulling status files from site1: Done
                site1 received new configuration from 10.102.217.205 in
                     file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                    conf
                Firing set gslb parameter -startConfigSync ENABLED
```



```
                    command: Done
17                  Fetching running GSLB Config: Done
18                  Comparing config: Done
19                  Applying changes: Done
20                  Firing set gslb parameter -startConfigSync DISABLED
                        command: Done
21                  Updating default.conf file: Done
22  Done
23  <!--NeedCopy-->
```

Die folgende Ausgabe zeigt den Status der Echtzeit-GSLB-Konfigurationssynchronisierung für die Slave-Site an:

```
1   > sh gslb syncStatus
2   Displaying the status of the real time GSLB configuration
        synchronization as slave node:
3
4                   site1 received new configuration from 10.102.217.205 in
                         file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                        conf
5                   Firing set gslb parameter -startConfigSync ENABLED
                        command: Done
6                   Fetching running GSLB Config: Done
7                   Comparing config: Done
8                   Applying changes: Done
9                   Firing set gslb parameter -startConfigSync DISABLED
                        command: Done
10                  Updating default.conf file: Done
11  Done
12  <!--NeedCopy-->
```

Die folgende Ausgabe zeigt die Statusübersicht der Echtzeit-GSLB-Konfigurationssynchronisierung für die Master Site an:

```
1   > sh gslb syncStatus -summary
2   Displaying the status summary of the real time GSLB configuration
        synchronization as master node:
3
4   ------------------------------------------------------------------------------

5                   Site Name                                   Status
                                    Reason
6   ------------------------------------------------------------------------------

7                   site2                                       Success
```



```
                                  All Done
8                 site1                                     Success
                                  All Done
9
10 Done
11 <!--NeedCopy-->
```

Die folgende Ausgabe zeigt die Statusübersicht der Echtzeit-GSLB-Konfigurationssynchronisierung für Slave-Site an:

```
1  > sh gslb syncStatus  -summary
2  Displaying the status summary of the real time GSLB configuration
       synchronization as slave node:
3
4  ------------------------------------------------------------------------------

5                 Site Name                                 Status
                                   Reason
6  ------------------------------------------------------------------------------

7                 site1                                     Success
                                  All Done
8
9  Done
10 <!--NeedCopy-->
```

So zeigen Sie den GSLB-Synchronisationsstatus oder die Zusammenfassung mit der GUI an

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard**.
2. Klicken Sie bei Bedarf auf **Synchronisationsübersicht anzeigen oder Synchronisationsstatus** anzeigen.

SNMP-Traps für die GSLB-Konfigurationssynchronisation

May 11, 2023

Ab NetScaler 12.1 Build 49.xx generiert die NetScaler-Appliance SNMP-Traps sowohl für lokale als auch für Remote-Sites, wenn Sie die GSLB-Konfiguration synchronisieren. SNMP-Traps werden sowohl für die manuelle Synchronisation als auch für die Echtzeitsynchronisierung generiert.

Wenn Sie die GSLB-Konfiguration zum ersten Mal synchronisieren, werden SNMP-Traps generiert. Bei den nachfolgenden Synchronisationsversuchen werden die SNMP-Traps nur generiert, wenn sich der

Synchronisationsstatus gegenüber dem vorherigen Synchronisationsstatus ändert. Außerdem werden die SNMP-Traps nur für Sites generiert, für die sich der Synchronisationsstatus gegenüber dem vorherigen Status geändert hat.

Stellen Sie sich beispielsweise vor, dass die erste GSLB-Konfigurationssynchronisierung erfolgreich war. Wenn Sie die Konfiguration zum zweiten Mal synchronisieren und die Synchronisation erneut erfolgreich ist, werden keine SNMP-Traps generiert, da der Status nicht geändert wird. Schlägt die Synchronisation jedoch beim dritten Versuch für eine der Sites fehl, wird ein SNMP-Trap nur für diese Site generiert.

In einem Hochverfügbarkeits- und Cluster-Setup generiert die Appliance die SNMP-Traps, wenn Sie die GSLB-Konfiguration vom neuen Knoten aus synchronisieren, unabhängig vom vorherigen Synchronisationsstatus. Wenn die SNMP-Trap-Option zuvor deaktiviert und dann aktiviert wurde, werden SNMP-Traps ab diesem Zeitpunkt unabhängig vom vorherigen Synchronisationsstatus generiert.

Die SNMP-Traps der GSLB-Konfigurationssynchronisation enthalten folgende Details:

- Name der GSLB-Site, für die die SNMP-Trap gesendet wird.
- Synchronisationsstatus der GSLB-Konfiguration: Erfolg oder Misserfolg.
- GSLB-Konfigurationssynchronisierungsmodus: Inkrementelle Synchronisierung oder Vollsynchronisierung.
- (Optional) Detaillierte Informationen zu den SNMP-Fallen.

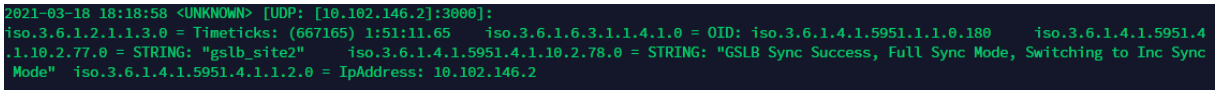
Die SNMP-Traps werden in den folgenden Szenarien generiert:

- Der GSLB-Synchronisationsstatus für eine GSLB-Site wechselt von Erfolg zu Failure und umgekehrt.
- Der GSLB-Synchronisationsmodus wechselt von der inkrementellen Synchronisation zur vollständigen Synchronisation und umgekehrt.

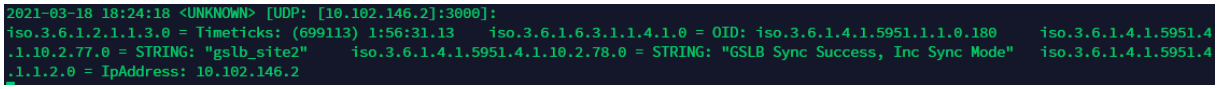
> Hinweis:
>
> Selbst wenn die inkrementelle Synchronisation aktiviert ist und die vollständige Synchronisation aus irgendeinem Grund auf einer GSLB-Site durchgeführt wird, wird der Grund für die vollständige Synchronisierung im Abschnitt “Detaillierte Informationen” der Fallenmeldung erwähnt. Zum Beispiel, wenn der GSLB-Konfiguration eine neue GSLB-Site hinzugefügt wird.

Beispiel für SNMP-Trap-Nachrichten

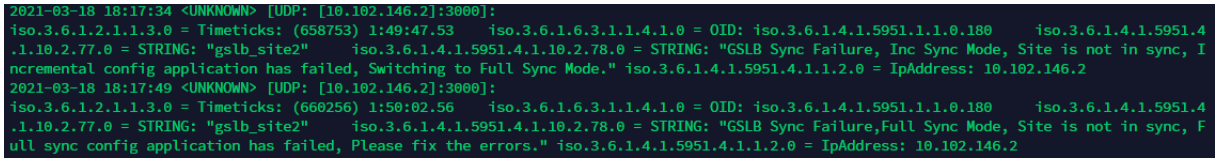
Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati
im Vollsynchronisierungsmodus erfolgreich ist.



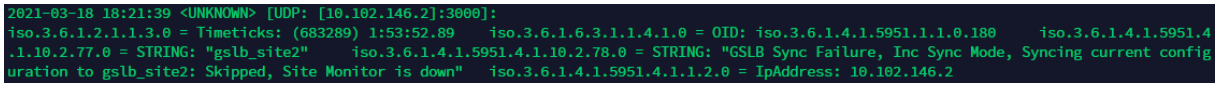
Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati
im inkrementellen Synchronisierungsmodus erfolgreich ist.



Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati
im inkrementellen Synchronisierungsmodus fehlgeschlagen ist. Die Fehlermeldung zeigt an, dass Sie die Fehler manuell beheben müssen, um die Synchronisation abzuschließen.



Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati
im inkrementellen Synchronisierungsmodus fehlgeschlagen ist. Es gibt auch den Grund für den Synchronisierungsfehler an, dh der Site-Monitor ist DOWN.



GSLB-Dashboard

January 19, 2021

Sie können den Gesamtstatus der GSLB-Sites, die an GSLB teilnehmen, auf dem GSLB-Dashboard anzeigen.

Sie können über das Dashboard auf die GSLB-Einstellungen zugreifen. Sie können den GSLB-Konfigurationsassistenten auch über das Dashboard starten. Darüber hinaus können Sie die Synchronisierung durchführen und das GSLB-Setup über das Dashboard testen.

Um auf das GSLB-Dashboard zuzugreifen, navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard** .

Überwachen von GSLB-Diensten

May 11, 2023

Wenn Sie einen Remotedienst an einen virtuellen GSLB-Server binden, tauschen die GSLB-Standorte metrische Informationen aus, einschließlich metrischer Netzwerkinformationen, bei denen es sich um die Roundtrip-Time- und Persistenzinformationen handelt.

Wenn eine Metric Exchange-Verbindung zwischen einem der teilnehmenden Standorte kurzzeitig unterbrochen wird, wird der Remote-Site als DOWN markiert, und an den verbleibenden Standorten, die aktiv sind, wird ein Lastenausgleich durchgeführt. Wenn Metric Exchange für einen Standort NICHT verfügbar ist, werden auch die Remote-Dienste, die zu dieser Site gehören, als NICHT VERFÜGBAR markiert.

Die NetScaler Appliance bewertet regelmäßig den Status der Remote-GSLB-Dienste, indem sie entweder MEP oder Monitore verwendet, die explizit an die Remotedienste gebunden sind. Es ist nicht erforderlich, explizite Monitore an lokale Dienste zu binden, da der Status des lokalen GSLB-Dienstes standardmäßig mithilfe des MEP aktualisiert wird. Sie können jedoch explizite Monitore an einen Remotedienst binden. Wenn Monitore explizit gebunden sind, wird der Status des Remotedienstes nicht vom Metrikaustausch gesteuert.

Wenn Sie einen Monitor an einen Remote-GSLB-Dienst binden, verwendet die NetScaler-Appliance standardmäßig den vom Monitor gemeldeten Status des Dienstes. Sie können die NetScaler-Appliance jedoch so konfigurieren, dass Monitore zur Bewertung von Diensten in den folgenden Situationen verwendet werden:

- Verwenden Sie immer Monitore (Standardeinstellung).
- Verwenden Sie Monitore, wenn MEP ausgeschaltet ist.
- Verwenden Sie Monitore, wenn Remotedienste und MEP AUSGESCHALTET sind.

Die zweite und dritte der oben genannten Einstellungen ermöglichen es der Appliance, die Überwachung zu beenden, wenn MEP eingeschaltet ist. In einem hierarchischen GSLB-Setup stellt eine GSLB-Website dem MEP beispielsweise Informationen über ihre untergeordneten Standorte zur Verfügung. Ein solcher Zwischenstandort kann den Status des untergeordneten Standorts aufgrund von Netzwerkproblemen als DOWN bewerten, obwohl der tatsächliche Status des Standorts UP ist. In diesem Fall können Sie Monitore an die Dienste des übergeordneten Standorts binden und MEP deaktivieren, um den aktuellen Status des Remotedienstes zu ermitteln. Mit dieser Option können Sie steuern, wie die Zustände der Remotedienste bestimmt werden.

Um Monitore zu verwenden, erstellen Sie sie zunächst und binden Sie sie dann an GSLB-Dienste.

Monitor-Trigger konfigurieren

Sie können eine GSLB-Site so konfigurieren, dass sie immer Monitore verwendet (Standard), Monitore verwendet, wenn MEP ausgefallen ist, oder Monitore verwendet, wenn sowohl der Remotedienst als auch das MEP ausgefallen sind. In den beiden letztgenannten Fällen beendet die NetScaler-Appliance die Überwachung, wenn MEP in den Status UP zurückkehrt.

So konfigurieren Sie die Monitorauslösung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
set gslb site <siteName>  -triggerMonitor (ALWAYS | MEPDOWN |
   MEPDOWN_SVCDOWN)
<!--NeedCopy-->
```

Beispiel:

```
set gslb site Site-GSLB-North-America  -triggerMonitor Always
<!--NeedCopy-->
```

So konfigurieren Sie die Monitorauslösung mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**und doppelklicken Sie auf die Site.
2. Wählen Sie in der Dropdownliste **Trigger Monitors** eine Option aus, wann die Überwachung ausgelöst werden soll.

Monitore hinzufügen oder entfernen

Um einen Monitor hinzuzufügen, geben Sie den Typ und den Port an. Sie können einen Monitor, der an einen Dienst gebunden ist, nicht entfernen. Sie müssen zuerst den Monitor vom Dienst trennen.

So fügen Sie einen Monitor mithilfe der Befehlszeilenschnittstelle hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen Monitor zu erstellen und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> -type <monitorType> -destPort <portNumber>

show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor monitor-HTTP-1 -type HTTP -destPort 80
show lb monitor monitor-HTTP-1
<!--NeedCopy-->
```

So entfernen Sie einen Monitor mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
rm lb monitor <monitorName>
<!--NeedCopy-->
```

So fügen Sie mithilfe des Konfigurationsdienstprogramms einen Monitor hinzu

Navigieren Sie zu
Traffic Management > Load Balancing > Monitore und fügen Sie einen Monitor hinzu oder löschen Sie ihn.

Monitore an einen GSLB-Dienst binden

Sobald Sie Monitore erstellt haben, müssen Sie sie an GSLB-Dienste binden. Wenn Sie Monitore an die Dienste binden, können Sie ein Gewicht für den Monitor angeben. Nachdem Sie einen oder mehrere gewichtete Monitore gebunden haben, können Sie einen Monitorschwellenwert für den Dienst konfigurieren. Durch diesen Schwellenwert wird der Dienst heruntergefahren, wenn die Summe der gebundenen Monitorgewichte den Schwellenwert unterschreitet.

Hinweis: Im Konfigurationsprogramm können Sie sowohl das Gewicht als auch den Überwachungsschwellenwert festlegen, während Sie den Monitor binden. Wenn Sie die Befehlszeile verwenden, müssen Sie einen separaten Befehl ausführen, um den Überwachungsschwellenwert des Dienstes festzulegen.

So binden Sie den Monitor mithilfe der Befehlszeilenschnittstelle an den GSLB-Dienst

Geben Sie in der Befehlszeile Folgendes ein:

```
bind monitor <name> <serviceName> [ -state (Enabled | Disabled) ] -
    weight <positiveInteger>
<!--NeedCopy-->
```

Beispiel:

```
bind monitor monitor-HTTP-1 service-GSLB-1 -state enabled -weight 2
<!--NeedCopy-->
```

So legen Sie den Überwachungsschwellenwert für einen GSLB-Dienst mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:


```
set gslb service <ServiceName> -monThreshold <PositiveInteger>
<!--NeedCopy-->
```

Beispiel:

```
set gslb service service-GSLB-1 -monThreshold 9
<!--NeedCopy-->
```

So binden Sie den Monitor mithilfe des Konfigurationsdienstprogramms an den GSLB-Dienst

1. Navigieren Sie zu Traffic Management > GSLB > Services.
2. Klicken Sie auf den Abschnitt **Monitor** und binden Sie den Monitor an den GSLB-Dienst.

So legen Sie den Überwachungsschwellenwert für einen GSLB-Dienst mithilfe des Konfigurationsdienstprogramms fest

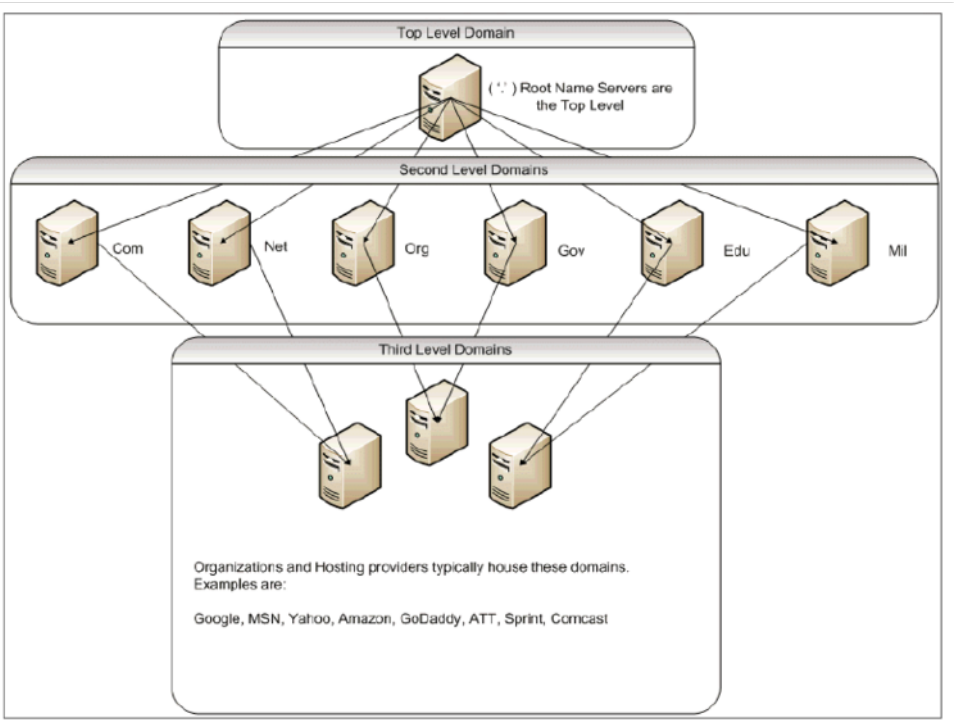
1. Navigieren Sie zu Traffic Management > GSLB > Services.
2. Klicken Sie auf den Abschnitt **Schwellenwert überwachen** und geben Sie einen Schwellenwert ein.

Wie das Domänennamensystem GSLB unterstützt

May 11, 2023

Das Domänennamensystem (DNS) wird als verteilte Datenbank betrachtet, die die Client/Server-Architektur verwendet. Nameserver sind die Server in der Architektur, und die Resolver sind die Clients, bei denen es sich um Bibliotheksroutinen handelt, die auf einem Betriebssystem installiert sind und Abfragen über das Netzwerk erstellen und senden.

Die logische Hierarchie des DNS ist im folgenden Diagramm dargestellt:



> Hinweis:
>
> Die Stammserver der zweiten Ebene sind dafür verantwortlich, Name-Server-zu-Adress-Zuordnungen für Name-Server-Delegationen innerhalb der Domänen .com, .net, .org, .gov usw. zu pflegen. Jede Domäne innerhalb der Domänen der zweiten Ebene ist für die Pflege von Nameserver-zu-Adress-Zuordnungen für die untergeordneten Organisationsdomänen verantwortlich. Auf Organisationsebene werden die einzelnen Hostadressen für www, FTP und andere Dienste, die Hosts bereitstellen, aufgelöst.

Delegation

Der Hauptzweck der aktuellen DNS-Topologie besteht darin, die Aufrechterhaltung aller Adressaufzeichnungen in einer Behörde zu verringern. Dies ermöglicht die Delegation eines Organisationsnamenraums an diese bestimmte Organisation. Die Organisation kann ihren Raum dann weiter an Subdomains innerhalb der Organisation delegieren. Unter citrix.com können Sie beispielsweise Subdomains namens `sales.citrix.comeducation.citrix.com`, und erstellen `support.citrix.com`. Die entsprechenden Abteilungen können ihre eigenen Nameserver verwalten, die für ihre Subdomain autoritativ sind, und dann ihren eigenen Satz von Hostnamen verwalten, um Zuordnungen zu adressieren. Keine einzige Abteilung ist für die Pflege aller Citrix Adressdatensätze verantwortlich. Jede Abteilung kann Adressen ändern und Topologien ändern und nicht mehr Arbeit in der übergeordneten Domäne oder Organisation auferlegen.

Vorteile der hierarchischen Topologie

Einige der Vorteile der hierarchischen Topologie sind:

- Skalierbarkeit
- Hinzufügen von Caching-Funktionen zu Nameservern auf jeder Ebene, wo eine DNS-Anfrage von einem Host bedient wird, der für eine bestimmte Domäne nicht autoritativ ist, aber die Antwort auf die Abfrage beitragen und die Staus- und Antwortzeit verkürzt.
- Das Caching erzeugt auch Redundanz und Ausfallsicherheit gegenüber Serverausfällen. Wenn ein Nameserver ausfällt, ist es weiterhin möglich, dass Datensätze von anderen Servern bereitgestellt werden können, die kürzlich zwischengespeicherte Kopien derselben Datensätze enthalten.

Resolver

Resolver sind die Clientkomponente im DNS-System. Programme, die auf einem Host ausgeführt werden, die Informationen aus dem Domänennamenbereich benötigen, verwenden den Resolver. Der Resolver behandelt:

- Abfragen eines Nameservers.
- Interpretieren von Antworten (dies können Ressourceneinträge oder ein Fehler sein).
- Rückgabe der Informationen an die Programme, die sie angefordert haben.

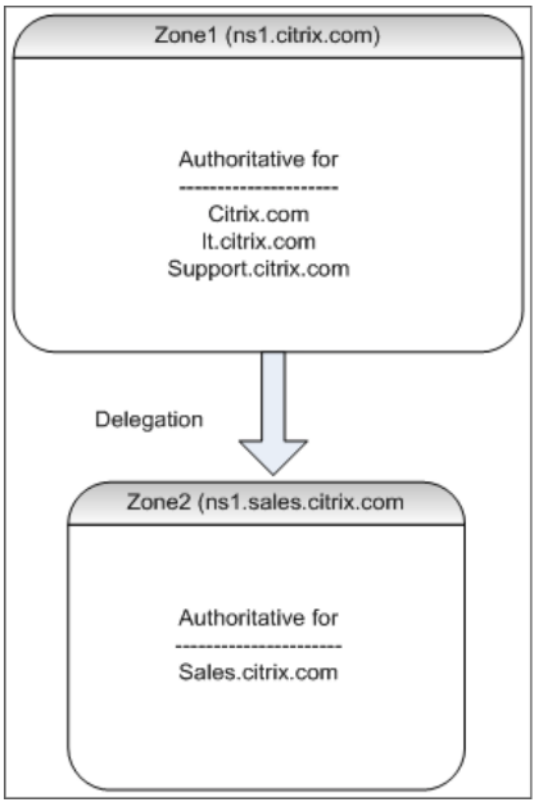
Der Resolver besteht aus einer Reihe von Bibliotheksroutinen, die in Programme wie Telnet, FTP und Ping kompiliert werden. Es sind keine getrennten Prozesse. Die Resolver können eine Anfrage zusammenstellen, senden und auf eine Antwort warten. Und senden Sie es erneut (möglicherweise an einen sekundären Nameserver), wenn es nicht innerhalb einer bestimmten Zeit beantwortet wird. Diese Arten von Resolvern werden als Stub-Resolver bezeichnet. Einige Resolver verfügen über die zusätzliche Funktionalität, um Datensätze zu zwischenspeichern und die Zeit zu leben (TTL). In Windows ist diese Funktionalität über den DNS-Clientdienst verfügbar, der über die Konsole “services.msc” sichtbar ist.

Namen-Server

Nameserver speichern im Allgemeinen vollständige Informationen über einen bestimmten Teil eines Domänennamenraums (Zone genannt). Der Nameserver soll dann die Berechtigung für diese Zone haben. Sie können auch für mehrere Zonen maßgeblich sein.

Der Unterschied zwischen einer Domäne und einer Zone ist subtil. Eine Domäne ist der vollständige Satz von Entitäten einschließlich ihrer Subdomains, während eine Zone nur die Informationen innerhalb einer Domäne ist, die nicht an einen anderen Nameserver delegiert wird. Ein Beispiel für eine Zone ist `citrix.com`, während es `sales.citrix.com` sich um eine separate Zone handelt, wenn diese Zone an einen anderen Nameserver innerhalb der Subdomäne delegiert wird. In diesem Fall

kann die primäre Citrix Zone `citrix.comit.citrix.com`, und enthalten `support.citrix.com`. Da der delegiert `sales.citrix.com` wird, ist es nicht Teil der Zone, über die der `citrix.com` Nameserver autoritativ ist. Das folgende Diagramm zeigt die beiden Zonen.

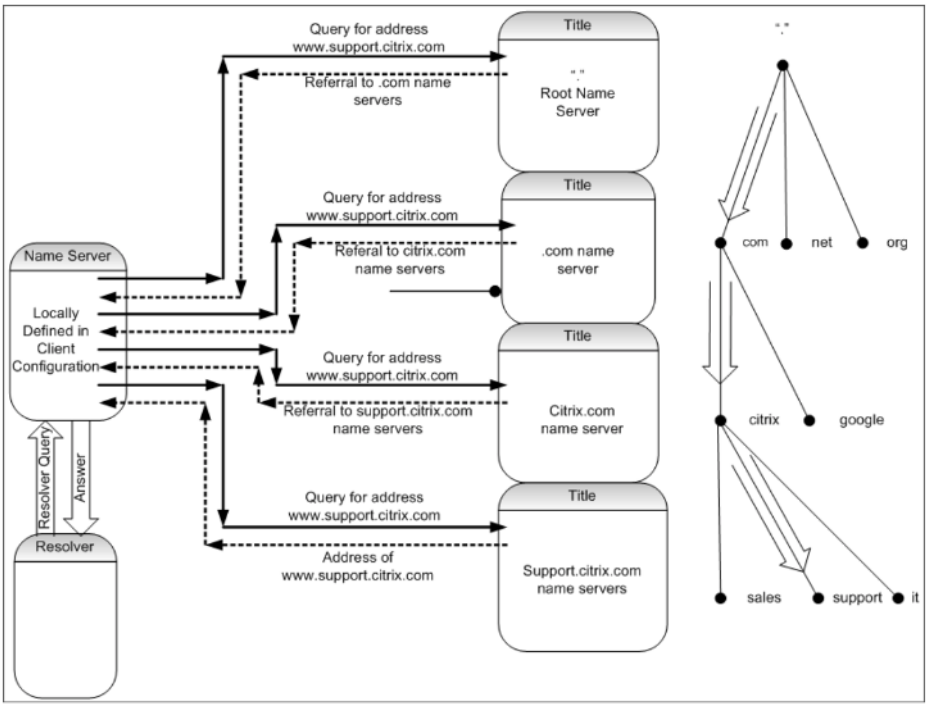


Um eine Subdomain ordnungsgemäß zu delegieren, müssen Sie verschiedenen Nameservern die Berechtigung für die Subdomain zuweisen. Im vorhergehenden Beispiel enthält der `ns1.citrix.com` keine Informationen über die `sales.citrix.com` Subdomain. Stattdessen enthält es Zeiger auf die Name-Server, die für die `ns1.sales.citrix.com` Subdomain autoritativ sind.

Stammnameserver und Abfrageauflösung

Root-Name-Server kennen die IP-Adressen aller Name-Server, die für die Domänen der zweiten Ebene autoritativ sind. Wenn ein Nameserver keine Informationen über eine bestimmte Domäne in seinen eigenen Datendateien hat, muss er sich nur an einen Stammserver wenden, um den richtigen Zweig der **DNS-Baumstruktur** zu durchqueren, um schließlich zur angegebenen Domäne zu gelangen. Dies beinhaltet eine Reihe von Anfragen an mehrere Nameserver, um beim Traversal des Baums zu helfen, den nächsten autoritativen Nameserver zu finden, der zur weiteren Lösung kontaktiert werden muss.

Das folgende Diagramm zeigt eine typische DNS-Anforderung, vorausgesetzt, dass während der Durchquerung kein zwischengespeicherter Datensatz für den angeforderten Namen vorhanden ist. Im folgenden Beispiel wird ein Mock Up der Citrix Domäne verwendet.



Rekursive und nicht rekursive Abfragen

Das vorhergehende Beispiel veranschaulicht die beiden Arten von Abfragen, die auftreten können.

- Rekursive Abfrage: Die Abfrage zwischen dem Resolver und dem lokal konfigurierten Name-Server ist rekursiv. Dies bedeutet, dass der Name-Server die Abfrage erhält und nicht auf den Resolver reagiert, bis die Abfrage vollständig beantwortet wurde oder ein Fehler zurückgegeben wird. Wenn der Nameserver eine Verweisung an die Abfrage erhält, folgt der Name-Server der Überweisung, bis der Name-Server die zurückgegebene Antwort (IP-Adresse) schließlich erhält.
- Nicht rekursive Abfrage: Die Abfrage, die der lokal konfigurierte Name-Server an den nachfolgenden autoritativen Nameserver auf Domänenebene stellt, ist nicht rekursiv (oder iterativ). Jede Anfrage wird sofort entweder mit einer Verweisung an einen autoritativen Server auf niedrigerer Ebene oder mit der Antwort auf die Abfrage beantwortet, wenn der abgefragte Name-Server die Antwort in seinen Datendateien oder seinem Cache enthält.

Zwischenspeichern

Obwohl der Lösungsprozess involviert ist und möglicherweise kleine Anfragen an mehrere Hosts erfordert, ist er schnell. Einer der Faktoren, der die Geschwindigkeit der DNS-Auflösung erhöht, ist das Caching. Jedes Mal, wenn ein Name-Server eine rekursive Abfrage erhält, muss er möglicherweise mit anderen Servern kommunizieren, um schließlich zum richtigen autoritativen Server für die spezifische Anforderung zu gelangen. Es speichert alle Informationen, die es zur späteren Bezugnahme

erhält. Wenn der nächste Client eine ähnliche Anfrage stellt, z. B. einen anderen Host, aber in derselben Domäne, kennt er bereits den Name-Server, der für diese Domäne autoritativ ist, und kann eine Anfrage direkt dorthin senden, anstatt am Root-Name-Server zu starten.

Caching kann auch für negative Antworten auftreten, z. B. für Abfragen nach Hosts, die nicht existieren. In diesem Fall darf der Server den autoritativen Nameserver nicht nach der angeforderten Domäne abfragen, um herauszufinden, dass der Host nicht existiert. Um Zeit zu sparen, prüft der Name-Server einfach den Cache und antwortet mit dem negativen Datensatz zurück.

Nameserver zwischenspeichern Datensätze nicht auf unbestimmte Zeit, sonst können Sie die IP-Adressen niemals aktualisieren. Um Synchronisationsprobleme zu vermeiden, enthalten DNS-Antworten eine Time to live (TTL). In diesem Feld wird das Zeitintervall beschrieben, für das der Cache einen Datensatz speichern kann, bevor er ihn verwerfen und beim autoritativen Nameserver nach aktualisierten Datensätzen suchen muss. Wenn sich die Datensätze nicht geändert haben, ermöglicht die Verwendung von TTL auch schnelle dynamische Antworten von Geräten, die GSLB ausführen.

Arten von Ressourceneintrags

Verschiedene RFCs bieten eine umfassende Liste der DNS-Ressourceneinzeichnungstypen und deren Beschreibung. In der folgenden Tabelle sind die gängigen Ressourcendatensatztypen aufgeführt.

Typ des Ressourceneintrags	Beschreibung	RFC
A	Eine Host-Adresse	RFC 1035
NS	Ein autoritativer Nameserver	RFC 1035
MD	Ein E-Mail-Ziel (Obsolete - benutze MX)	RFC 1035
MF	Ein Mail-Forwarder (Obsolet - benutze MX)	RFC 1035
CNAME	Der kanonische Name für einen Alias	RFC 1035
SOA	Markiert den Beginn einer Autoritätszone	RFC 1035
WKS	Eine bekannte Leistungsbeschreibung	RFC 1035
PTR	Ein Domainnamen-Zeiger	RFC 1035
HINFO	Hostinformationen	RFC 1035

Typ des Ressourceneintrags	Beschreibung	RFC
MINFO	Informationen zu Postfächern oder Maillisten	RFC 1035
MX	Mail-Austausch	RFC 1035
TXT	Text-Zeichenfolgen	RFC 1035
AAAA	IP6-Adresse	RFC 3596
SRV	Server-Auswahl	RFC 2782]

Wie GSLB DNS unterstützt

GSLB verwendet Algorithmen und Protokolle, die entscheiden, welche IP-Adresse für eine DNS-Abfrage gesendet werden muss. GSLB-Sites sind geografisch verteilt, und an jedem Standort befindet sich ein autoritativer DNS-Nameserver, der als Dienst auf der NetScaler-Appliance ausgeführt wird. Alle Nameserver an den verschiedenen beteiligten Standorten sind für dieselbe Domain maßgeblich. Jede der GSLB-Domänen ist eine Subdomain, für die eine Delegation konfiguriert ist. Daher sind die GSLB-Name-Server autoritativ und können einen der verschiedenen Load Balancing-Algorithmen verwenden, um zu entscheiden, welche IP-Adresse zurückgegeben werden soll.

Eine Delegation wird erstellt, indem ein Name-Server-Datensatz für die GSLB-Domäne in den übergeordneten Domänen-Datenbankdateien und einen nachfolgenden Adressdatensatz für die Nameserver hinzugefügt wird, die für die Delegierung verwendet werden. Wenn Sie beispielsweise GSLB für verwenden möchten `www.citrix.com`, kann die folgende Bind SOA-Datei verwendet werden, um Anfragen an Nameserver `www.citrix.com` zu delegieren: Netscaler1 und Netscaler2.

```
1  ##############################################################################
2  @ IN SOA citrix.com. hostmaster.citrix.com. (
3  1 ; serial
4  3h ; refresh
5  1h ; retry
6  1w ; expire
7  1h ) ; negative caching TTL
8  IN NS ns1
9  IN NS ns2
10 IN MX 10 mail
11
12 ns1   IN A 10.10.10.10
13 ns2   IN A 10.10.10.20
14 mail  IN A 10.20.20.50
```



```
15
16 ### Old Configuration if www was not delegated to a GSLB name server
17 www IN A 10.20.20.50
18
19 ### Updated Configuration
20 Netscaler1 IN A xxx.xxx.xxx.xxx
21 Netscaler2 IN A yyy.yyy.yyy.yyy
22 www IN NS Netscaler1.citrix.com.
23 www IN NS Netscaler2.citrix.com.
24 ###
25 IN MX 20 mail2
26 mail2 IN A 10.50.50.20
27 ################################################################################
28
29 <!--NeedCopy-->
```

Das Verständnis von BIND ist keine Voraussetzung für die Konfiguration von DNS. Alle konformen DNS-Server-Implementierungen verfügen über eine Methode, um die äquivalente Delegation zu erstellen. Microsoft DNS-Server können mithilfe der Anweisungen unter Zonendelegation erstellen für die Delegation konfiguriert werden.

Was GSLB auf der NetScaler-Appliance von der Verwendung des Standard-DNS-Dienstes für die Verteilung des Datenverkehrs unterscheidet, ist, dass die NetScaler GSLB-Sites Daten mithilfe eines proprietären Protokolls namens Metric Exchange Protocol (MEP) austauschen. Mit MdEP können die GSLB-Sites Informationen über alle anderen Websites aufbewahren. Wenn eine DNS-Anfrage eingegangen ist, berücksichtigt der Abgeordnete die GSLB-Metriken, um Informationen wie die folgenden zu ermitteln:

- Site mit der geringsten Anzahl aktueller Verbindungen
- Site, die dem LDNS-Server am nächsten liegt und die Anfrage basierend auf Round-Trip-Zeiten (RTT) gesendet hat.

Es gibt mehrere Load Balancing-Algorithmen, die verwendet werden können, aber GSLB ist ein DNS, wobei das Gehirn darunter dem Nameserver (gehostet auf der NetScaler-Appliance) mitteilt, welche Adresse basierend auf Metriken der teilnehmenden Sites gesendet werden muss.

Weitere Vorteile, die GSLB bietet, sind die Fähigkeit, Persistenz (oder Site-Affinität) aufrechtzuerhalten. Antworten auf die eingehenden DNS-Abfragen können mit der Quell-IP-Adresse verglichen werden, um festzustellen, ob diese Adresse in der jüngsten Vergangenheit an eine bestimmte Site weitergeleitet wurde. In diesem Fall wird dieselbe Adresse in der DNS-Antwort gesendet, um sicherzustellen, dass die Clientsitzung beibehalten wird.

Eine andere Form der Persistenz wird auf Standortebene durch Verwendung von HTTP-Weiterleitungen oder HTTP-Proxy erhalten. Diese Formen der Persistenz treten auf, nachdem die DNS-Reaktion aufge-

treten ist. Wenn Sie also eine HTTP-Anfrage auf einer Website erhalten, die ein Cookie enthält, um die Anfrage an eine andere teilnehmende Website zu leiten, können Sie entweder mit einer Weiterleitung antworten oder die Anfrage an die entsprechende Website stellen.

Metrisches Austauschprotokoll

Metric Exchange Protocol (MEP) wird verwendet, um die in GSLB-Berechnungen verwendeten Daten über Standorte hinweg freizugeben. Mithilfe von MEP-Verbindungen tauschen Sie drei Arten von Daten aus. Diese Verbindungen müssen über TCP-Port 3011 nicht sicher sein oder können mit SSL über TCP-Port 3009 sicher sein.

Die folgenden drei Arten von Daten werden ausgetauscht und haben ihre eigenen Intervalle und Austauschmethoden.

- **Austausch von Standortmetrik:** Dies ist ein Polling-Exchange-Modell. Wenn Site1 beispielsweise eine Konfiguration für Site2-Dienste hat, fragt jede zweite Site1 Site2 nach dem Status der GSLB-Dienste. Site2 antwortet mit dem Status und anderen Ladedetails.
- **Austausch von Netzwerkmetriken:** Dies ist der LDNS-RTT-Informationsaustausch, der im dynamischen Proximity-Load Balancing-Algorithmus verwendet wird. Dies ist ein Push-Exchange-Modell. Alle fünf Sekunden leitet jede Site ihre Daten an andere teilnehmende Websites weiter.
- **Persistenzaustausch:** Dies ist für den Sourceip-Persistenzaustausch. Dies ist auch ein Push-Exchange-Modell. Alle fünf Sekunden leitet jede Site ihre Daten an andere teilnehmende Websites weiter.

Standardmäßig werden Website-Dienste über den Abgeordneten nur basierend auf Abfrageinformationen überwacht. Wenn Sie Monitore basierend auf dem Monitorintervall binden, wird der Status aktualisiert und Sie können die Häufigkeit der Updates steuern, indem Sie das Überwachungsintervall entsprechend einstellen.

Prioritätsauftrag für GSLB-Dienste

May 11, 2023

Mit der Funktion “Prioritätsreihenfolge für Dienste” können Sie die Reihenfolge von Diensten oder Dienstgruppen basierend auf den Auswahleinstellungen für den Lastausgleich priorisieren. Sie können die Prioritätsreihenfolge konfigurieren, wenn Sie Folgendes tun:

- Binden Sie einen Dienst an einen virtuellen GSLB-Server.
- Binden Sie eine Dienstgruppe an einen virtuellen GSLB-Server.
- Binden Sie ein Dienstgruppenmitglied an die GSLB-Dienstgruppe.

Derzeit können Sie die Prioritätsreihenfolge für Dienste mithilfe der folgenden Methoden konfigurieren. Diese Ansätze haben jedoch die folgenden Einschränkungen:

- Konfigurieren einer virtuellen Backupserverkette: Die Anzahl der Konfigurationszeilen ist hoch, und Sie müssen den Befehl `show` mehrmals ausführen, um den Status aller GSLB-Dienste für jeden virtuellen Server zu ermitteln.
- Konfigurieren des bevorzugten Speicherorts: Sie müssen Standorteinträge für alle Ihre Anwendungsendpunkte erstellen.

Die Prioritätsreihenfolge für Dienste behebt die vorherigen Einschränkungen mit weniger Konfigurationsbefehlen und hilft Ihnen, die bevorzugte Standortkonfiguration zu erreichen, ohne dass die IP-Adressen aller GSLB-Dienste standortbezogen dargestellt werden müssen.

Prioritätsreihenfolge für GSLB-Dienste konfigurieren

Um die Prioritätsreihenfolge für GSLB-Dienste zu konfigurieren, wird der Parameter `-order <number>` zu den Bindungsbefehlen hinzugefügt.

> **Hinweis:**
>
> Die niedrigste Auftragsnummer hat die höchste Priorität.

Befehl:

```
bind gslb vserver <vservername> -servicename/servicegroupname <servicename/servicegroupname> -order <number>
```

Stellen Sie sich beispielsweise eine Reihe von Diensten vor, die an einen virtuellen GSLB-Server (gv1) gebunden sind. Mit dem Parameter
`- order <number>` können Sie die Reihenfolge der Auswahl der Dienste wie folgt priorisieren:

- Set 1 (s1, s2) bound to gv1 – order 1
- Set 2 (s3, s4) bound to gv1 – order 2
- Set 3 (s5, s6) bound to gv1 – order 3

Nachdem Sie die Dienste an gv1 gebunden haben und gv1 den Clientverkehr empfängt, ist die Reihenfolge der Auswahl der Dienste wie folgt:

- Der virtuelle Server (gv1) wählt die Dienste in Satz 1 (s1 und s2) mit der laufenden Nummer 1 aus, da diesem Set die niedrigste Ordnungsnummer zugewiesen ist. Standardmäßig hat die niedrigste Auftragsnummer die höchste Priorität.
- Wenn alle Dienste in Satz 1 DOWN sind, wählt gv1 Satz 2 (s3 und s4) mit der laufenden Nummer 2.
- Wenn alle Dienste in Satz 1 und Satz 2 ausgefallen sind, wählt gv1 Satz 3 (s5 und s6) mit der laufenden Nummer 3.

Konfigurieren der Prioritätsreihenfolge für GSLB-Dienste mithilfe der CLI

Um die Prioritätsreihenfolge für die GSLB-Dienste zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

1. GSLB-Sites hinzufügen.

```
add gslb site site1 1.1.1.1
add gslb site site2 1.1.1.2
```

2. Fügen Sie einen virtuellen GSLB-Server hinzu.

```
add gslb vserver gv1 HTTP
```

3. GSLB-Dienste hinzufügen.

```
add gslb service gsvc1 1.1.1.3 http 80 -sitename site1
add gslb service gsvc2 1.1.1.4 http 80 -sitename site2
add gslb service gsvc3 1.1.1.5 http 80 -sitename site1
add gslb service gsvc4 1.1.1.6 http 80 -sitename site2
add gslb service gsvc5 1.1.1.7 http 80 -sitename site1
add gslb service gsvc6 1.1.1.8 http 80 -sitename site2
```

4. Legen Sie die Bestellnummer fest und binden Sie die Dienste an den virtuellen GSLB-Server.

```
bind gslb vserver gv1 gsvc1 -order 1
bind gslb vserver gv1 gsvc2 -order 1
bind gslb vserver gv1 gsvc3 -order 2
bind gslb vserver gv1 gsvc4 -order 2
bind gslb vserver gv1 gsvc5 -order 3
bind gslb vserver gv1 gsvc6 -order 3
```

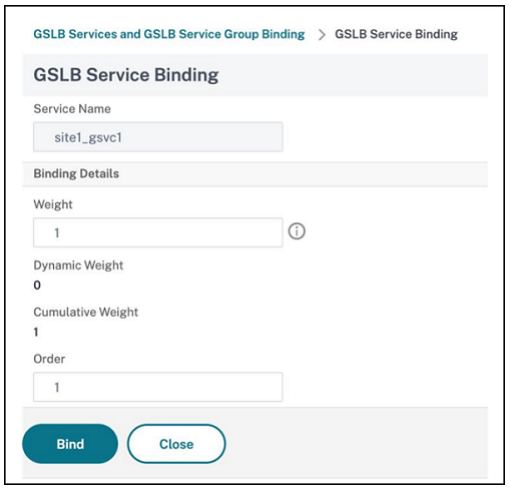
Konfigurieren der Prioritätsreihenfolge für GSLB-Dienste über die GUI

Voraussetzungen:

- Sie haben GSLB-Sites erstellt.
- Sie haben einen virtuellen GSLB-Server erstellt.
- Sie haben GSLB-Dienste erstellt.

Gehen Sie wie folgt vor, um die Prioritätsreihenfolge für GSLB-Dienste zu konfigurieren und sie an den virtuellen GSLB-Server zu binden:

1. Navigieren Sie zu**Traffic Management > GSLB > Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server.
2. Klicken Sie in **GSLB Virtual Server** im Abschnitt **GSLB-Dienste und GSLB-Dienstgruppenbindung** auf **GSLB Virtual Server to GSLB Service Bindings**.
3. Klicken Sie im Dialogfeld **GSLB-Dienste und GSLB-Dienstgruppenbindung** auf **Bindung hinzufügen**.
4. Wählen Sie im Dialogfeld **GSLB Service Binding** einen Dienst aus.
5. Geben Sie eine Zahl in das Feld **Reihenfolge**ein, um die Prioritätsreihenfolge für den Dienst festzulegen.



6. Klicken Sie auf**Binden**.
7. Wiederholen Sie die Schritte 1—6, um unterschiedliche Prioritätsreihenfolgennummern für verschiedene Dienste zu konfigurieren

Konfigurieren der Prioritätsreihenfolge für GSLB-Dienste mithilfe von LB

Standardmäßig hat die niedrigste Auftragsnummer die höchste Priorität. Sie können dieses Standardverhalten jedoch mithilfe der neuen LB-Aktion und der Richtlinienbefehle aufschieben. Sie können die Reihenfolge der Serviceauswahl basierend auf dem eingehenden Clientverkehr oder den Kundendaten konfigurieren.

Stellen Sie sich beispielsweise eine Reihe von Diensten vor, die an einen virtuellen GSLB-Server (gv1) gebunden sind. Mit dem Parameter – `order <number>` haben Sie die Prioritätsreihenfolge für Dienste wie folgt konfiguriert:

- Set 1 (s1, s2) bound to gv1 – order 1
- Set 2 (s3, s4) bound to gv1 – order 2
- Set 3 (s5, s6) bound to gv1 – order 3

Standardmäßig hat die niedrigste Auftragsnummer die höchste Priorität. Daher ist die standardmäßige Prioritätsreihenfolge der Präferenz 1, 2 und 3 für Dienste in Set 1, Set2 bzw. Set3. Für einen bestimmten Client-Traffic möchten Sie jedoch die Prioritätsreihenfolge auf 3, 1 und 2 ändern. Um dies zu erreichen, können Sie eine LB-Richtlinie hinzufügen und an gv1 binden.

Ein LB-Richtlinienbefehl besteht aus zwei Elementen: einer Regel und einer Aktion. Die Regel ist mit einer Aktion verknüpft, die ausgeführt wird, wenn eine Anforderung mit der Regel übereinstimmt.

> **Hinweis:**
>
> Die LB-Richtlinienbefehle gelten sowohl für die LB- als auch für die GSLB-Konfiguration und gelten für die Anforderungen, die von der NetScaler-Appliance verarbeitet werden.

LB-Aktion

Ausdruck:

```
add lb action <name> <type> <string>
```

Beispiel:

```
add lb action act1 -type SELECTIONORDER -value 3 2 1
```

Parameter:

- `name`: Name der Aktion.
- `type`: Art der Aktion.
- `string`: Wert für die angegebene Aktion.

LB-Richtlinie

Ausdruck:

```
add lb policy <name> <rule> <action> <undefaction>
```

Beispiel:

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

Parameter:

- `name`: Name der Richtlinie.
- `rule`: Eine Regel besteht aus einem oder mehreren Ausdrücken. Die Regel ist mit einer Aktion verknüpft, die ausgeführt wird, wenn die Anforderung mit der Regel übereinstimmt.
- `action`: DROP, NOLBACTION und RESET werden unterstützt.

- `undefaction`: Die NetScaler-Appliance generiert ein undefiniertes Ereignis (UNDEF-Ereignis), wenn eine Anforderung nicht mit einer Richtlinie übereinstimmt. Sie können den Befehl `set lb param -undefAction <action>` verwenden, um die undefinierte Aktion festzulegen. Sie können diese Aktionen einem undefinierten Ereignis zuweisen: DROP, NOLBACTION und RESET.

Betrachten wir ein Beispiel, in dem Sie eine LB-Aktion, eine LB-Richtlinie, hinzufügen und die Richtlinie wie folgt an einen virtuellen GSLB-Server (gv1) binden:

```
add lb action act1 -type SELECTIONORDER -value 3 1 2

add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1

bind gslb vserver gv1 -policyName pol1 -priority 20 - gotoPriorityExpression
 END -type REQUEST
```

Die Regel wählt den Clientdatenverkehr aus, der der IP-Adresse entspricht `8.8.8.8`, und sendet diesen Datenverkehr an gv1. Der Aktionstyp LB (`SELECTIONORDER`) definiert die Auswahlreihenfolge für Dienste. Nachdem Sie die LB-Richtlinie an gv1 gebunden haben und wenn gv1 den Clientdatenverkehr von der IP-Adresse empfängt`8.8.8.8`, werden die Dienste in der folgenden Reihenfolge ausgewählt:

1. Der virtuelle Server (gv1) wählt Dienste in Satz 3 (s5 und s6) mit der Prioritätsreihenfolge 3 aus.
2. Wenn alle Dienste in Satz 3 DOWN sind, wählt gv1 Satz 1 (s1 und s2) mit der Prioritätsreihenfolge 2 aus.
3. Wenn alle Dienste in Satz 3 und Satz 2 ausgefallen sind, wählt gv1 Satz 1 (s1 und s2) mit der Reihenfolge 1.

Konfigurieren der Prioritätsreihenfolge für GSLB-Dienste mit LB-Richtlinienbefehlen mithilfe der CLI

Um die Prioritätsreihenfolge für GSLB-Dienste über LB-Richtlinienbefehle zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

1. Fügt eine LB-Aktion hinzu.

   ```
   add lb action act1 -type SELECTIONORDER -value 3 1 2
   ```

2. Eine LB-Richtlinie hinzufügen.

   ```
   add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
   ```

3. GSLB-Sites hinzufügen.

   ```
   add gslb site site1 1.1.1.1

   add gslb site site2 1.1.1.2
   ```


4. Fügen Sie einen virtuellen GSLB-Server hinzu.

```
add gslb vserver gv1 HTTP
```

5. Binden Sie die LB-Richtlinie an den virtuellen GSLB-Server.

```
bind gslb vserver gv1 -policyName pol1 -priority 20 - gotoPriorityExpression
 END -type REQUEST
```

6. GSLB-Dienste hinzufügen.

```
add gslb service gsvc1 1.1.1.3 http 80 -sitename site1

add gslb service gsvc2 1.1.1.4 http 80 -sitename site2

add gslb service gsvc3 1.1.1.5 http 80 -sitename site1

add gslb service gsvc4 1.1.1.6 http 80 -sitename site2

add gslb service gsvc5 1.1.1.7 http 80 -sitename site1

add gslb service gsvc6 1.1.1.8 http 80 -sitename site2
```

7. Legen Sie die Reihenfolge fest und binden Sie die Dienste an den virtuellen GSLB-Server.

```
bind gslb vserver gv1 gsvc1 -order 1

bind gslb vserver gv1 gsvc2 -order 1

bind gslb vserver gv1 gsvc3 -order 2

bind gslb vserver gv1 gsvc4 -order 2

bind gslb vserver gv1 gsvc5 -order 3

bind gslb vserver gv1 gsvc6 -order 3
```

Konfigurieren der Prioritätsreihenfolge für GSLB-Dienste mit den Befehlen der LB-Richtlinie über die GUI

Voraussetzungen:

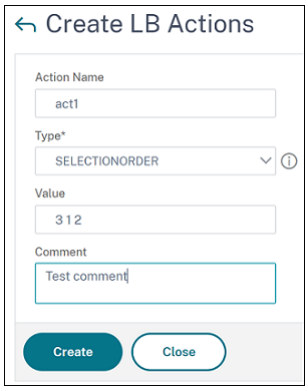
- Sie haben GSLB-Sites erstellt.
- Sie haben einen virtuellen GSLB-Server erstellt.
- Sie haben Dienste erstellt.

Schritt 1 — Erstellen einer LB-Aktion:

1. Navigieren Sie zu **AppExpert > LB > Aktionen**.
2. Klicken Sie in**LB-Aktionen**auf**Hinzufügen**.
3. Geben**Sie im Dialogfeld LB-Aktionen erstellen** Werte für die folgenden Parameter an:

- **Name der Aktion**: act1
- **Typ**: SELECTIONORDER
- **Wert**: 3 1 2

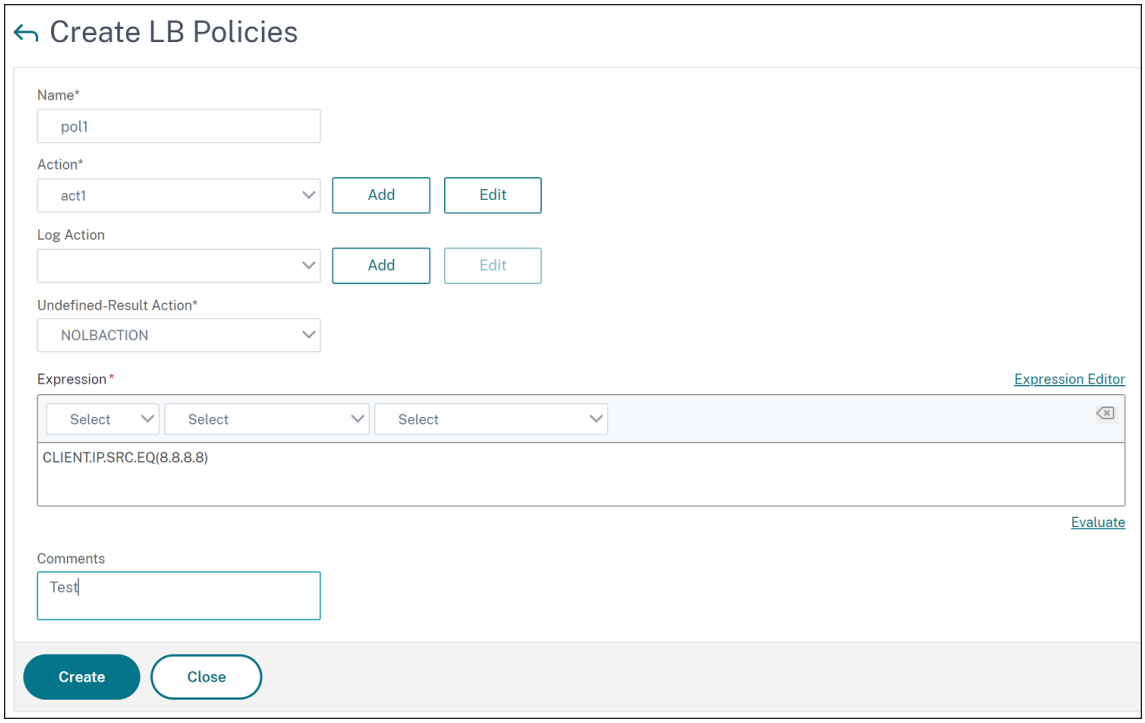
  > **Hinweis:**
  >
  > Die Zahlen im Feld **Wert**sind durch ein Leerzeichen getrennt.



4. Klicken Sie auf **Erstellen**.

Schritt 2 — Erstellen einer LB-Richtlinie:

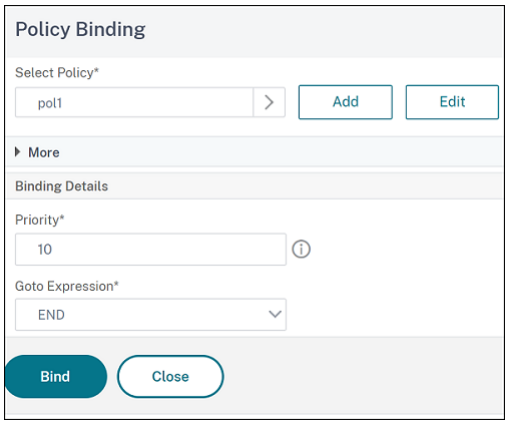
1. Navigieren Sie zu **AppExpert > LB > Richtlinien**.
2. Klicken Sie in den**LB-Richtlinien**auf**Hinzufügen**.
3. Geben**Sie im Dialogfeld LB-Richtlinien erstellen** Werte für die folgenden Parameter an:
   - **Vorname**: pol 1
   - **Aktion**: act 1
   - **Aktion mit undefiniertem Ergebnis**: NOLBACTION
   - **Ausdruck**: CLIENT.IP.SRC.EQ (8.8.8.8)



4. Klicken Sie auf**Erstellen**.

Schritt 3 — Binden Sie die LB-Richtlinie an den virtuellen GSLB-Server:

1. Navigieren Sie zu**Traffic Management > GSLB > Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server.
2. Klicken Sie in **GSLB Virtual Server**im Abschnitt **Erweiterte Einstellungen** auf**Richtlinien**.
3. Klicken Sie im Abschnitt**Richtlinien**auf **GSLB Virtual Server LB-Richtlinienbindung**.
4. Geben Sie im Dialogfeld **Richtlinienbindung** Werte für die folgenden Parameter an:
   - **Wählen Sie Policy**: pol 1
   - **Priorität**: 10
   - **Gehe zu Expression**: END



5. Klicken Sie auf **Bind**.

Schritt 4 — Prioritätsreihenfolge für GSLB-Dienste konfigurieren:

Informationen zum Konfigurieren der Prioritätsreihenfolge für GSLB finden Sie im Abschnitt **Konfigurieren der Prioritätsreihenfolge für GSLB-Dienste über die GUI**.

Persistenzeinstellungen für Dienste

Wenn Persistenz für einen Dienst konfiguriert ist, wird standardmäßig immer Persistenz bevorzugt.

Stellen Sie sich zum Beispiel einen Dienst mit konfigurierter Persistenz und Prioritätsreihenfolge 1 vor. Wenn ein Dienst mit der Prioritätsreihenfolge 0 AKTIV ist, wird immer der Dienst mit der Prioritätsreihenfolge 1 bevorzugt.

Sie können dieses Standardverhalten jedoch mit dem folgenden CLI-Befehl überschreiben:

```
set gslb param -overridePersistencyforOrder<YES/NO>
```

Betrachten wir das folgende Beispiel:

Eine Reihe von Diensten ist an einen virtuellen GSLB-Server (gv1) mit der folgenden Prioritätsreihenfolge gebunden:

- Set 1 (s1, s2) bound to gv1 – order 1
- Set 2 (s3, s4) bound to gv1 – order 2

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Persistenz zu überschreiben:

```
set gslb parameter -overridePersistencyforOrder YES
```

Wenn Satz 1 (Dienste mit Persistenz sind konfiguriert) DOWN ist, dann behandeln Set 2 Dienste alle Anforderungen, bis die Dienste von Satz 1 UP sind. Ein Persistenzeintrag für Priorität 2 wird erstellt.

Nehmen wir an, dass die Set-1-Dienste nach einiger Zeit aktiv sind. Jetzt sind sowohl Set 1- als auch Set 2-Dienste UP, um die Anforderungen zu bearbeiten. In diesem Szenario werden neue Lastausgleichsentscheidungen getroffen, da Dienstleistungen mit höherem Auftrag in Betrieb sind. Der Persistenzeintrag wird mit einem neuen Load-Balancing-Eintrag überschrieben.

Priorität umschalten

Mit der Funktion zum Umschalten der Priorität können Sie während des Versionsupgrades für einen Dienst mit einer höheren Priorität den gesamten Datenverkehr auf einen Dienst mit niedriger Priorität umschalten. Sie können die folgenden Befehle verwenden, um die Priorität umzuschalten:

- `set gslb vserver -toggleorder <Ascending/Descending>`
- `set gslb vserver v1 -orderthreshold 80`

Betrachten wir zum Beispiel, dass es zwei Dienste mit den folgenden Prioritäten gibt:

- Service 1- order 0
- Service 2 – order 1

Standardmäßig verarbeitet Dienst 1 den gesamten Datenverkehr. Wenn Dienst 1 aktualisiert werden muss, muss der Datenverkehr zu Dienst 2 umgeleitet werden.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Priorität umzuschalten:

```
set gslb vserver -toggleorder Descending
```

Standardmäßig hat 0 eine höhere Priorität. Nach dem Umschalten der Priorität wird 1 jedoch als höhere Priorität betrachtet. Wenn für den Dienst ein Persistenzeintrag vorhanden ist, wird das Verhalten der Persistenzeinstellung wie im Abschnitt**Persistenzeinstellungen für Dienste** erläutert.

Upgradeempfehlungen für die GSLB-Bereitstellung

May 11, 2023

Dieser Abschnitt enthält Empfehlungen zur Reihenfolge, in der GSLB-Knoten in verschiedenen GSLB-Setups aktualisiert werden müssen. Es befasst sich auch mit einigen FAQs.

Hinweis: Die NetScaler-Appliance, von der aus die GSLB-Synchronisierung gestartet wird, wird als “Hauptsitz” und die GSLB-Sites bezeichnet, auf denen die Konfiguration als “untergeordnete Standorte” kopiert wird.

Bevor Sie mit dem Upgrade-Prozess beginnen, lesen Sie die in den folgenden Themen genannten Voraussetzungen:

- Voraussetzungen
- Aktualisieren Sie ein Paar mit hoher Verfügbarkeit.
- Aktualisieren Sie einen Cluster.

Zu beachtende Punkte beim Upgrade von GSLB-Setups

- Aktualisieren Sie in einem HA-Setup zuerst die untergeordneten Standorte und dann die Hauptwebsite.
- In einem HA-Setup werden Dienststatus möglicherweise nicht von einem älteren Build-Primärknoten zu einem neueren sekundären Build-Knoten weitergegeben. Wenn die Builds jedoch aus verschiedenen Versionen bestehen, aber dieselbe HA-Version haben, wird der Dienststatus möglicherweise weiterhin verbreitet.

- Wenn GSLB in einem Cluster konfiguriert ist, aktualisieren Sie zuerst die Nicht-Besitzer-Knoten, und aktualisieren Sie dann den Eigentümerknoten. Wenn sich ein Standort oder mehrere Standorte in einem Cluster befinden, folgen Sie an jeder Site dieselbe Upgrade-Sequenz.
- Aktivieren Sie neue GSLB-Funktionen erst, nachdem Sie alle Knoten auf einen neueren Build aktualisiert haben.
- Aktualisieren Sie alle GSLB-Knoten auf den neuesten Build. Es gibt keine funktionalen Auswirkungen auf die verfügbaren Funktionen, wenn einige der GSLB-Knoten eine ältere Version verwenden und einige der GSLB-Knoten auf eine neuere Version aktualisiert werden.

FAQ

- **Werden GSLB-Dienstzustände propagiert, wenn Instanzen verschiedene Softwareversionen ausführen?**

  GSLB MEP ist funktionsfähig, wenn Instanzen, die auf verschiedenen Versionen und GSLB-Dienstzuständen ausgeführt werden, über GSLB-Sites verteilt werden. Es gibt keine Auswirkungen auf die MEP-Kommunikation, wenn Instanzen nach einem Upgrade verschiedene Versionen ausführen.

- **Ist es empfehlenswert, während eines Upgrades Konfigurationsänderungen vorzunehmen?**

  Wenn in einem GSLB-Setup ein Hauptstandort aktualisiert wird, wird nicht empfohlen, Konfigurationsänderungen an anderen GSLB-Knoten vorzunehmen.

Zugehörige Ressourcen

Die folgenden Ressourcen enthalten Informationen zum Upgrade einer NetScaler-Instanz mithilfe von NetScaler ADM:

- 10 Möglichkeiten, wie NetScaler ADM Service einfachere NetScaler-Upgrades unterstützt
- Verwenden Sie den NetScaler ADM Service, um NetScaler-Instanzen zu aktualisieren
- Verwenden Sie NetScaler ADM-Software, um NetScaler Instanzen zu aktualisieren

Anwendungsfall: Bereitstellung einer Domänennamen-basierten Autoscale-Dienstgruppe

May 11, 2023

> **Tipp**
>
> Informationen zu den GSLB-Dienstgruppen finden Sie unter Konfigurieren einer GSLB-Dienstgruppe

Bereitstellungsszenario

Zwei Rechenzentren werden in zwei AWS-Regionen bereitgestellt, eines in Sydney und eines in North Virginia. Ein weiteres Rechenzentrum wird in Azure bereitgestellt. Ein AWS-ELB in jeder AWS-Region wird für den Lastenausgleich der Anwendungsserver verwendet. ALB wird für Azure verwendet, um den Lastenausgleich des Anwendungsservers durchzuführen. Die NetScaler-Appliances werden für GSLB für die ELBs und ALB mithilfe einer auf GSLB-Domänennamen basierenden Autoscale-Dienstgruppe konfiguriert.

> **Wichtig**
>
> Sie müssen die erforderlichen Sicherheitsgruppen in AWS konfigurieren und sie an die GSLB-Instance anhängen. Port 53 muss in den Regeln für eingehende und ausgehende Sicherheitsgruppen zugelassen sein. Außerdem müssen die Ports (3009 oder 3011, je nach sicherer MEP-Konfiguration) für die MEP-Kommunikation geöffnet sein. Für die Anwendungsüberwachung müssen die entsprechenden Ports in den Regeln für ausgehende Verbindungen der Sicherheitsgruppe zugelassen sein.

Die Konfigurationsschritte für das obige Bereitstellungsszenario und die entsprechenden CLI-Befehle lauten wie folgt:

1. Erstellen Sie Rechenzentren (vertreten durch GSLB-Sites).

   ```
   add gslb site aws-sydney 192.0.2.2

   add gslb site aws-nvirginia 198.51.100.111

   add gslb site alb-southindia 203.0.113.6
   ```

2. Fügen Sie einen Nameserver mit der DNS-Gateway-IP-Adresse hinzu, zu der der GSLB-Knoten hinzugefügt wird. Dies muss in allen Rechenzentren erfolgen.

   ```
   add dns nameServer 8.8.8.8
   ```

3. Fügen Sie Server für ELB und ALB hinzu.

   ```
   add server aws-sydney_server lb-sydney-1052691850.ap-southeast-2.elb.
   amazonaws.com

   add server aws-nvirginia_server LB-nvirginia-860559595.us-east-1.elb.
   amazonaws.com

   add server alb-southindia_server alb.southindia.cloudapp.azure.com
   ```


4. Fügen Sie GSLB-Autoscale-Dienstgruppen für jeden ELB und ALB hinzu und binden Sie jeden Server an die jeweilige Dienstgruppe.

   ```
   add gslb serviceGroup aws-nvirginia_sg HTTP -autoScale DNS -siteName aws-nvirginia

   add gslb serviceGroup aws-sydney_sg HTTP -autoScale DNS -siteName aws-sydney

   add gslb serviceGroup alb-southindia_sg HTTP -autoScale DNS -siteName alb-southindia

   bind gslb serviceGroup aws-nvirginia_sg aws-nvirginia_server 80

   bind gslb serviceGroup aws-sydney_sg aws-sydney_server 80

   bind gslb serviceGroup alb-southindia_sg alb-southindia_server 80
   ```

5. Fügen Sie einen virtuellen GSLB-Server hinzu, und binden Sie die Anwendungsdomäne und die Dienstgruppen an diesen virtuellen Server.

   ```
   add gslb vserver gv1 HTTP

   bind gslb vserver gv1 -serviceGroupName aws-nvirginia_sg

   bind gslb vserver gv1 -serviceGroupName aws-sydney_sg

   bind gslb vserver gv1 -serviceGroupName alb-southindia_sg
   ```

Anwendungsfall: Bereitstellung einer IP-Adressbasierten GSLB-Dienstgruppe

August 19, 2021

> **Tipp**
>
> Informationen zu den GSLB-Dienstgruppen finden Sie unter Konfigurieren einer GSLB-Dienstgruppe.

Bereitstellungsszenario

Wenn mehrere Anwendungen auf demselben Anwendungsserver gehostet werden, sollte die GSLB diese Anwendungen untersuchen, um zu sehen, ob die Anwendungen reagieren oder nicht. Wenn eine Anwendung nicht antwortet, muss der Benutzer an den Server weitergeleitet werden, auf dem die Anwendung UP ist. Wenn eine der Anwendungen DOWN ist, sollte der Server nicht mit DOWN gekennzeichnet werden, da die anderen Anwendungen UP sind.

Im folgenden Beispiel werden mehrere Anwendungen (HTTPS) auf einem Server in jeder GSLB-Site gehostet und daher alle diese Anwendungen auf eine IP-Adresse der jeweiligen Site aufgelöst.

Mit den GSLB-Dienstgruppen können Sie denselben Server mit einer IP-Adresse und einem Port haben, der an mehrere Dienstgruppen gebunden ist, wobei jede Dienstgruppe eine andere Anwendung darstellt.

Ein anwendungsspezifischer Monitor ist an die Dienstgruppen gebunden, die die Dienstgruppe als DOWN kennzeichnen, wenn die Anwendung DOWN ist. Wenn also eine Anwendung DOWN ist, wird nur diese Anwendung aus dem Setup und nicht vom Server entfernt.

```
```
add gslb serviceGroup app1_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app2_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app1_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add gslb serviceGroup app2_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add lb monitor http_app2 HTTP -respCode 200 -httpRequest "GET /testsite
    /app2.html"

add lb monitor http_app1 HTTP -respCode 200 -httpRequest "GET /testsite
    /app1.html"

bind gslb serviceGroup app1_site1 192.0.2.140 80

bind gslb serviceGroup app1_site1 -monitorName http_app1

bind gslb serviceGroup app2_site1 192.0.2.140 80

bind gslb serviceGroup app2_site1 -monitorName http_app2

bind gslb serviceGroup app1_site2 192.0.2.142 80

bind gslb serviceGroup app1_site2 -monitorName http_app1

bind gslb serviceGroup app2_site2 192.0.2.142 80

bind gslb serviceGroup app2_site2 -monitorName http_app2
```

 
```

```
<!--NeedCopy--> ```
```

Anleitungsartikel

August 19, 2021

Die GSLB-Anleitungen enthalten Informationen über einige der wichtigen GSLB-Konfigurationen wie das Anpassen der GSLB-Konfiguration, das Konfigurieren von persistenten Verbindungen, die Notfallwiederherstellung usw.

Anpassen Ihrer GSLB-Konfiguration

Persistente Verbindungen konfigurieren

Verwalten von Clientverbindungen

Konfigurieren von GSLB für Nähe

Schützen des GSLB-Setups vor Fehlern

Konfigurieren von GSLB für Disaster Recovery

Überschreiben des statischen Näherungsverhaltens durch Konfigurieren bevorzugter Speicherorte

Konfigurieren der GSLB-Dienstauswahl über Content Switching

Konfigurieren des globalen Server-Lastausgleichs für DNS-Abfragen mit NAPTR-Einträgen

Verwenden der EDNS0-Client-Subnetzoption für den globalen Server-Lastausgleich

Beispiel für eine vollständige übergeordnete und untergeordnete Konfiguration mithilfe des Metriks-Exchange-Protokolls

Anpassen der GSLB-Konfiguration

May 11, 2023

Sobald Ihre grundlegende GSLB-Konfiguration betriebsbereit ist, können Sie sie anpassen, indem Sie die Bandbreite eines GSLB-Dienstes ändern, CNAME-basierte GSLB-Dienste, statische Nähe, dynamisches RTT, persistente Verbindungen oder dynamische Gewichtungen für Dienste konfigurieren oder die GSLB-Methode ändern.

Sie können auch die Überwachung für GSLB-Dienste konfigurieren, um deren Status zu ermitteln.

Diese Einstellungen hängen von Ihrer Netzwerkbereitstellung und den Arten von Clients ab, von denen Sie erwarten, dass sie eine Verbindung zu Ihren Servern herstellen.

Ändern Sie die maximale Verbindung oder die maximale Bandbreite für einen GSLB-Dienst

Sie können die Anzahl der neuen Clients einschränken, die gleichzeitig eine Verbindung zu einem virtuellen Load-Balancing- oder Content-Switching-Server herstellen können, indem Sie die maximale Anzahl von Clients und/oder die maximale Bandbreite für den GSLB-Dienst konfigurieren, der den virtuellen Server darstellt.

So ändern Sie die maximale Client-Anzahl oder Bandbreite eines GSLB-Dienstes mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile den folgenden Befehl ein, um die maximale Anzahl von Clientverbindungen oder die maximale Bandbreite eines GSLB-Dienstes zu ändern und die Konfiguration zu überprüfen:

```
set gslb service <serviceName> [-maxClients <positive_integer>] [-
   maxBandwidth <positive_integer>]
show gslb service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
set glsb service Service-GSLB-1  -maxBandwidth 100  -maxClients 100
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

So ändern Sie die maximale Anzahl der Clients oder die maximale Bandbreite eines GSLB-Dienstes mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**und doppelklicken Sie auf einen Dienst.
2. Klicken Sie in den Abschnitt **Weitere Einstellungen** und stellen Sie die folgenden Parameter ein:
   - Max Kunden — Max Kunden
   - Maximale Bandbreite — Maximale Bandbreite

Erstellen Sie CNAME-basierte GSLB-Dienste

Um einen GSLB-Dienst zu konfigurieren, können Sie die IP-Adresse des Servers oder einen kanonischen Namen des Servers verwenden. Wenn Sie mehrere Dienste (wie einen FTP- und einen Webserver, die jeweils auf unterschiedlichen Ports laufen) von einer einzigen IP-Adresse aus ausführen

oder mehrere HTTP-Dienste auf demselben Port mit unterschiedlichen Namen auf demselben physischen Host ausführen möchten, können Sie kanonische Namen (CNAMES) für die Dienste verwenden.

Sie können beispielsweise zwei Einträge im DNS als ftp.example.com und www.example.com für FTP-Dienste und HTTP-Dienste auf derselben Domain, example.com, haben. CNAME-basierte GSLB-Dienste sind in einer mehrstufigen Domain-Resolver-Konfiguration oder beim mehrstufigen Domain-Load-Balancing nützlich. Die Konfiguration eines CNAME-basierten GSLB-Dienstes kann auch hilfreich sein, wenn sich die IP-Adresse des physischen Servers wahrscheinlich ändert.

Wenn Sie CNAME-basierte GSLB-Dienste für eine GSLB-Domäne konfigurieren und eine Anfrage für die GSLB-Domäne gesendet wird, stellt die NetScaler-Appliance einen CNAME anstelle einer IP-Adresse bereit. Wenn der A-Eintrag für diesen CNAME-Eintrag nicht konfiguriert ist, muss der Client die CNAME-Domäne nach der IP-Adresse abfragen. Wenn der A-Datensatz für diesen CNAME-Eintrag konfiguriert ist, stellt die NetScaler-Appliance dem CNAME den entsprechenden A-Datensatz (IP-Adresse) zur Verfügung. Die NetScaler-Appliance verarbeitet die endgültige Auflösung der DNS-Abfrage, die durch die GSLB-Methode bestimmt wird. Die CNAME-Einträge können auf einer anderen NetScaler-Appliance oder auf einem Drittanbietersystem verwaltet werden.

In einem auf IP-Adressen basierenden GSLB-Dienst wird der Status eines Dienstes durch den Status des Servers bestimmt, den er repräsentiert. Bei einem CNAME-basierten GSLB-Dienst ist der Status jedoch standardmäßig auf UP gesetzt. Die IP-Adresse des virtuellen Servers (VIP) oder das Metric Exchange Protocol (MEP) werden nicht zur Bestimmung seines Status verwendet. Wenn ein Desktop-basierter Monitor an einen CNAME-basierten GSLB-Dienst gebunden ist, wird der Status des Dienstes anhand des Ergebnisses der Monitoruntersuchungen bestimmt.

Sie können einen CNAME-basierten GSLB-Dienst nur an einen virtuellen GSLB-Server binden, der den DNS-Datensatztyp als CNAME hat. Außerdem kann eine NetScaler-Appliance höchstens einen GSLB-Dienst mit einem bestimmten CNAME-Eintrag enthalten.

Im Folgenden sind einige der Funktionen aufgeführt, die für einen CNAME-basierten GSLB-Dienst unterstützt werden:

- Die auf GSLB-Richtlinien basierende Seitenaffinität wird unterstützt, wobei der CNAME der bevorzugte Standort ist.
- Die Quell-IP-Persistenz wird unterstützt. Der Persistenzeintrag enthält die CNAME-Informationen anstelle der IP-Adresse und des Port des ausgewählten Dienstes.

Im Folgenden sind die Einschränkungen von CNAME-basierten GSLB-Diensten aufgeführt:

- Die Persistenz der Website wird nicht unterstützt, da der Dienst, auf den ein CNAME verweist, an jedem Standort eines Drittanbieters vorhanden sein kann.
- Die Antwort mit mehreren IP-Adressen wird nicht unterstützt, da eine Domain nicht mehrere CNAME-Einträge haben kann.
- Source IP Hash und Round Robin sind die einzigen unterstützten Load-Balancing-Methoden. Die Methode Static Proximity wird nicht unterstützt, da ein CNAME nicht mit einer IP-Adresse

verknüpft ist und die statische Nähe nur anhand der IP-Adressen aufrechterhalten werden kann.

Hinweis: Die Empty-Down-Response-Funktion sollte auf dem virtuellen GSLB-Server aktiviert sein, an den Sie den CNAME-basierten GSLB-Dienst binden. Wenn Sie die Empty-Down-Response-Funktion aktivieren und ein virtueller GSLB-Server AUSGEFALLEN oder deaktiviert ist, enthält die Antwort auf eine DNS-Anfrage für die an diesen virtuellen Server gebundenen Domänen anstelle eines Fehlercodes einen leeren Datensatz ohne IP-Adressen.

So erstellen Sie einen CNAME-basierten GSLB-Dienst mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add gslb service <serviceName> -cnameEntry <string> -siteName <string>
<!--NeedCopy-->
```

Beispiel:

```
add gslb service Service-GSLB-1 -cnameEntry transport.mycompany.com -
    siteName Site-GSLB-East-Coast
add gslb service Service-GSLB-2 -cnameEntry finance.mycompany.com -
    siteName Site-GSLB-West-Coast
<!--NeedCopy-->
```

So erstellen Sie einen CNAME-basierten GSLB-Dienst mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Erstellen Sie einen Dienst und setzen Sie den **Typ auf Canonical Name**Based.

Konfigurieren Sie den Übergang zum Out-of-Service State (TROFS) in GSLB

Wenn Sie die Persistenz auf einem virtuellen GSLB-Server konfigurieren, an den ein Dienst gebunden ist, verarbeitet der Dienst auch nach seiner Deaktivierung weiterhin Anfragen vom Client und akzeptiert nur neue Anfragen oder Verbindungen, um die Persistenz zu wahren. Nach einer konfigurierten Zeit, der sogenannten Phase des ordnungsgemäßen Herunterfahrens, werden keine neuen Anfragen oder Verbindungen an den Dienst weitergeleitet, und alle bestehenden Verbindungen werden geschlossen.

Wenn Sie einen Dienst deaktivieren, können Sie mithilfe des Arguments delay einen Zeitraum für das reibungslose Herunterfahren in Sekunden angeben. Wenn der Dienst während der Phase des ordnungsgemäßen Herunterfahrens an einen virtuellen Server gebunden ist, wird sein Status als Außer Betrieb angezeigt.

Dynamische Gewichte für Dienste konfigurieren

In einem typischen Netzwerk gibt es Server, die eine höhere Kapazität für den Datenverkehr haben als andere. Bei einer regulären Load-Balancing-Konfiguration wird die Last jedoch gleichmäßig auf alle Dienste verteilt, obwohl verschiedene Dienste Server mit unterschiedlichen Kapazitäten darstellen.

Um Ihre GSLB-Ressourcen zu optimieren, können Sie dynamische Gewichte auf einem virtuellen GSLB-Server konfigurieren. Die dynamischen Gewichtungen können entweder auf der Gesamtzahl der an den virtuellen Server gebundenen Dienste oder auf der Summe der Gewichte der einzelnen Dienste basieren, die an den virtuellen Server gebunden sind. Die Verkehrsverteilung basiert dann auf den für die Dienste konfigurierten Gewichtungen.

Wenn dynamische Gewichte auf dem virtuellen GSLB-Server konfiguriert sind, werden Anfragen gemäß der Load-Balancing-Methode, dem Gewicht des GSLB-Dienstes und dem dynamischen Gewicht verteilt. Das Produkt aus dem Gewicht des GSLB-Dienstes und dem dynamischen Gewicht wird als kumuliertes Gewicht bezeichnet. Wenn das dynamische Gewicht auf dem virtuellen GSLB-Server konfiguriert ist, werden Anfragen daher auf der Grundlage der Load-Balancing-Methode und des kumulierten Gewichts verteilt.

Wenn die dynamische Gewichtung für einen virtuellen Server deaktiviert ist, wird der numerische Wert auf 1 gesetzt. Dadurch wird sichergestellt, dass das kumulierte Gewicht zu jeder Zeit eine Ganzzahl ungleich Null ist.

Die dynamische Gewichtung kann auf der Gesamtzahl der aktiven Dienste basieren, die an virtuelle Load-Balancing-Server gebunden sind, oder auf den den Diensten zugewiesenen Gewichtungen.

Stellen Sie sich eine Konfiguration mit zwei GSLB-Sites vor, die für eine Domain konfiguriert sind und jeder Standort über zwei Dienste verfügt, die den Client bedienen können. Wenn ein Dienst an einem Standort ausfällt, muss der andere Server an diesem Standort doppelt so viel Traffic verarbeiten wie ein Dienst am anderen Standort. Wenn die dynamische Gewichtung auf der Anzahl der aktiven Dienste basiert, hat die Site, auf der beide Dienste aktiv sind, das Doppelte der Site, auf der ein Dienst ausgefallen ist, und erhält daher doppelt so viel Traffic.

Ziehen Sie alternativ eine Konfiguration in Betracht, bei der die Dienste am ersten Standort Server darstellen, die doppelt so leistungsstark sind wie Server am zweiten Standort. Wenn dynamisches Gewicht auf den Gewichten basiert, die den Diensten zugewiesen sind, kann doppelt so viel Datenverkehr an die erste Site gesendet werden wie an die zweite.

Hinweis: Weitere Informationen zum Zuweisen von Gewichtungen zu Lastenausgleichsdiensten finden Sie unter Zuweisen von Gewichten zu Diensten.

Betrachten Sie als Veranschaulichung der Berechnung der dynamischen Gewichtung einen virtuellen GSLB-Server, der über einen GSLB-Dienst gebunden ist. Der GSLB-Dienst stellt einen virtuellen Lastausgleichsserver dar, an den wiederum zwei Dienste gebunden sind. Das dem GSLB-Dienst zugewiesene Gewicht beträgt 3. Die den beiden Diensten zugewiesenen Gewichte sind 1 bzw. 2. In

diesem Beispiel, wenn das dynamische Gewicht auf Folgendes eingestellt ist:

- **Deaktiviert: Das**kumulative Gewicht des virtuellen GSLB-Servers ist das Produkt aus der dynamischen Gewichtung (deaktiviert = 1) und dem Gewicht des GSLB-Dienstes (3), sodass das kumulierte Gewicht 3 ist.
- **SERVICECOUNT**: Die Anzahl ist die Summe der Anzahl der Dienste, die an die virtuellen Load-Balancing-Server gebunden sind, die dem GSLB-Dienst entsprechen (2), und das kumulierte Gewicht ist das Produkt aus der dynamischen Gewichtung (2) und der Gewichtung des GSLB-Dienstes (3), also 6.
- **SERVICEWEIGHT**: Das dynamische Gewicht ist die Summe der Gewichte der Dienste, die an die virtuellen Load-Balancing-Server gebunden sind, die dem GSLB-Dienst entsprechen (3), und das kumulierte Gewicht ist das Produkt aus der dynamischen Gewichtung (3) und der Gewichtung des GSLB-Dienstes (3), also 9.

Hinweis: Dynamische Gewichtungen sind nicht anwendbar, wenn virtuelle Content Switching-Server konfiguriert sind.

So konfigurieren Sie einen virtuellen GSLB-Server für die Verwendung dynamischer Gewichtungen mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver <name> -dynamicWeight SERVICECOUNT | SERVICEWEIGHT
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -dynamicWeight SERVICECOUNT
<!--NeedCopy-->
```

So richten Sie den virtuellen GSLB-Server mithilfe des Konfigurationsdienstprogramms so ein, dass er dynamische Gewichtungen verwendet

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server und doppelklicken Sie auf den virtuellen GSLB-Server, dessen Methode Sie ändern möchten (z. B. vServer-GSLB-1).
2. Klicken Sie auf den Abschnitt **Methode** und wählen Sie in der Dropdownliste **Dynamic Weight** die Option **SERVICECOUNT oder**SERVICEWEIGHT**aus.

So konfigurieren Sie die Persistenz in GSLB

May 11, 2023

Persistenz stellt sicher, dass eine Reihe von Clientanfragen für einen bestimmten Domainnamen an dasselbe Rechenzentrum gesendet wird, anstatt einen Lastenausgleich vorzunehmen. Wenn Persistenz für eine bestimmte Domäne konfiguriert ist, hat sie Vorrang vor der konfigurierten GSLB-Methode. Sie können Persistenz für Bereitstellungen verwenden, bei denen Informationen zu einer Client-Transaktion lokal auf einer Instance gespeichert werden, die die ersten Anfragen bearbeitet hat. Zum Beispiel die Bereitstellungen für E-Commerce, die einen Einkaufswagen verwenden, bei denen der Server den Verbindungsstatus aufrechterhalten muss, um die Transaktion verfolgen zu können. Die NetScaler-Appliance wählt ein Rechenzentrum aus, um eine Client-Anfrage zu verarbeiten. Wenn die Persistenz aktiviert ist, leitet es dieselbe IP-Adresse des ausgewählten Rechenzentrums für alle nachfolgenden DNS-Anfragen (Domain Name System) weiter. Wenn eine Persistenzsitzung auf ein ausfallendes Rechenzentrum verweist, verwendet die NetScaler-Appliance die konfigurierte GSLB-Methode, um ein neues Rechenzentrum auszuwählen. Es wird dann für nachfolgende Anfragen des Clients persistent.
Für die Persistenz in GSLB muss derselbe Satz von Persistenz-Identifikatoren (PersistID) auf den virtuellen GSLB-Servern in allen Rechenzentren konfiguriert werden. Das GSLB-Modul verwendet den Persistenz-Identifier, um einen virtuellen GSLB-Server eindeutig zu identifizieren. Wenn die Quell-IP-Persistenz auf dem virtuellen GSLB-Server aktiviert ist, werden die Persistenzsitzungen auch im Rahmen des Metrikaustauschs ausgetauscht. Damit die NetScaler-Appliance standortübergreifende Persistenz unterstützt, muss die persistenzbezogene Konfiguration an allen teilnehmenden GSLB-Sites vorgenommen werden. Citrix empfiehlt die Persistenz in GSLB für statusorientierte Anwendungen, bei denen die Clients für die nachfolgenden Anfragen erneut eine Verbindung zu derselben Anwendungsinstanz herstellen müssen.

Sie können Persistenz in GSLB auf folgende Weise erreichen:

- Persistenz auf dem virtuellen GSLB-Server
- Persistenz der Website auf GSLB-Diensten

Persistenz auf dem virtuellen GSLB-Server

Die Persistenz auf dem virtuellen GSLB-Server wird während der DNS-Anfragen verwendet. Die Quell-IP-Adresse der DNS-Anfrage wird verwendet, um eine Persistenzsitzung zwischen dem Client und dem Rechenzentrum zu erstellen. DNS-Clients sind in der Regel lokale DNS- (LDNS) oder DNS-Gateways, die eine Reihe von Clients, die hinter ihnen sitzen, als Proxy verwenden (bei ISPs). Die Persistenz auf einem virtuellen GSLB-Server ist unabhängig vom Anwendungsprotokoll.
Im Allgemeinen werden mehrere DNS-Gateways oder Local Domain Name Server (LDNS) im Client-Netzwerk konfiguriert. Citrix empfiehlt Ihnen, eine geeignete Persistenzmaske zu konfigurieren, da der Client für die nachfolgenden DNS-Anfragen unabhängig von den Upstream-LDNS-Geräten, die für die Verbindung mit der ADC-Appliance verwendet werden, in demselben Rechenzentrum bestehen kann, das die früheren Anfragen bearbeitet hat. Nachdem die Persistenzsitzung für eine LDNS-IP-Adresse erstellt wurde, erhalten alle Endclients, die über dieses LDNS eine Verbindung herstellen,

dieselbe IP-Adresse des Rechenzentrums.

Persistenz der Website auf GSLB-Diensten

Die Persistenz der Website wird während der Bearbeitung der Anwendungsanfragen wirksam. Die Persistenz der Website funktioniert nur für HTTP- und HTTPS-Verkehr, da die Persistenz mithilfe von HTTP-Cookies erreicht wird. Da Cookies auf HTTP-Clients (Browsern) verwaltet werden, erhalten Sie Einblick in die Clients, die sich hinter den DNS-Gateways befinden. Wenn Sie Cookies verwenden, um die Persistenz für Clients zu erreichen, werden auf der ADC-Appliance für jeden eingehenden Client keine Ressourcen verbraucht. Wenn Sie einen GSLB-Dienst mit einer Verzögerungszeit herunterfahren, geht der Dienst in den Status „Transition to Out of Service“ (TROFS) über. Persistenz wird unterstützt, solange sich der Dienst im UP- oder TROFS-Status befindet. Das heißt, wenn derselbe Client innerhalb der angegebenen Verzögerungszeit eine Anfrage für denselben Dienst sendet, nachdem ein Dienst als TROFS markiert wurde, bearbeitet derselbe GSLB-Standort (Rechenzentrum) die Anfrage.

Wenn Sie über einen Alias auf eine Anwendung zugreifen, stellen Sie sicher, dass der CNAME-Datensatz auch auf der NetScaler-Appliance konfiguriert ist. In einer übergeordneten und untergeordneten Topologie funktioniert die Site-Persistenz nicht, wenn Sie über einen Alias auf eine Anwendung zugreifen.

> Hinweis
>
> Wenn der Verbindungsproxy als Site-Persistenzmethode angegeben ist und Sie auch die Persistenz auf virtuellen LB-Servern konfigurieren möchten, wird die Quell-IP-Persistenz nicht empfohlen. Wenn die Verbindung über einen Proxy übertragen wird, wird eine IP-Adresse verwendet, die der ADC-Appliance gehört, und nicht die tatsächliche IP-Adresse des Clients.
> Konfigurieren Sie eine geeignete Persistenz, die die Quell-IP der HTTP (S) -Anfrage nicht verwendet, um den Client zu identifizieren, z. B. Cookie-Persistenz oder regelbasierte Persistenz.

Konfigurieren Sie die Persistenz basierend auf der Quell-IP-Adresse

Wenn die Quell-IP-Persistenz auf dem virtuellen GSLB-Server konfiguriert ist, werden Persistenzsitzungen für die Quell-IP-Adresse der DNS-Anfrage erstellt. Abhängig von der ECS-Funktion (Extended Client Subnet) wird die Quell-IP-Adresse der DNS-Anfrage aus einer der folgenden Quellen übernommen:

- Die Quell-IP im IP-Header des eingehenden DNS-Request-Pakets
- Die Option ECS in der DNS-Anfrage Weitere Informationen zu ECS finden Sie unter Verwenden der EDNS0-Client-Subnetzoption für den globalen Server-Lastenausgleich.

Persistenzsitzungen für einen Client dauern bis zum Persistenz-Timeout. Nach Ablauf des Timeouts werden bestehende Persistenzsitzungen gelöscht. Für nachfolgende Anfragen wird eine neue

GSLB-Entscheidung getroffen und möglicherweise eine andere GSLB-Dienst-IP-Adresse ausgewählt. Die Quell-IP-Persistenz auf dem virtuellen GSLB-Server und die Site-Persistenz auf dem GSLB-Dienst ergänzen sich gegenseitig. Wenn die Quell-IP-Persistenz auf dem virtuellen GSLB-Server deaktiviert ist, wählt der virtuelle GSLB-Server jedes Mal, wenn der DNS versucht, die Auflösung vorzunehmen, einen anderen GSLB-Dienst aus. Der Client stellt auch eine Verbindung zu einem anderen GSLB-Dienst her und das Rechenzentrum, das die Anwendungsanforderung empfängt, stellt die Verbindung zu dem Rechenzentrum her, das den Client zuerst bedient hat. Dies könnte zu einer gewissen Latenz führen. Durch die Aktivierung der Quell-IP-Persistenz auf dem virtuellen GSLB-Server können also häufige Mehrfachsprünge für Anwendungsanfragen vermieden werden. Wenn die Quell-IP-Persistenzsitzung abgelaufen ist und der Client danach wieder eine Verbindung herstellt, verbindet die Site-Persistenz den Client wieder mit dem Rechenzentrum, das den Client ursprünglich bedient hatte. Wenn der Client eine Verbindung über ein DNS-Gateway herstellt, das nicht in den konfigurierten Persistenzmaskenbereich fällt, hilft die Standortpersistenz den Clients außerdem, sich an das Rechenzentrum zu halten, das die erste Anfrage bearbeitet hat.

So konfigurieren Sie die Persistenz basierend auf der Quell-IP-Adresse über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver <name> -persistenceType (SOURCEIP|NONE) -persistenceId
    <positive_integer> [-persistMask <netmask>] - [timeout <mins>]
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -persistenceType SOURCEIP -
   persistenceId 23 -persistMask 255.255.255.255 - timeout 2
<!--NeedCopy-->
```

So konfigurieren Sie die Persistenz auf der Grundlage der Quell-IP-Adresse mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtual Servers** und doppelklicken Sie auf den virtuellen GSLB-Server, dessen Methode Sie ändern möchten (z. B. vServer-GSLB-1).
2. Klicken Sie auf den Abschnitt **Persistenz** und wählen Sie in der Dropdownliste **Persistenz** die Option **SOURCEIP aus und legen Sie die folgenden** Parameter fest:
   - Persistenz-ID — Persistence-ID
   - Auszeit — Auszeit
   - IPv4-Netzmaske oder IPv6-Maskenlänge — PersistMask

Konfigurieren Sie die Persistenz der Website auf der Grundlage von HTTP-Cookies

Die Persistenz der Website wird mithilfe von HTTP-Cookies (bekannt als „Site-Cookie“) erreicht, um den Client erneut mit demselben Server zu verbinden. Wenn die GSLB-Appliance auf eine Client-DNS-Anfrage reagiert, indem sie die IP-Adresse der ausgewählten GSLB-Site sendet, sendet der Client eine HTTP-Anfrage an diese GSLB-Site. Der Anwendungsendpunkt auf dieser GSLB-Site fügt dem HTTP-Header ein Site-Cookie hinzu, und die Seitenpersistenz ist wirksam.
Wenn der Client eine DNS-Anfrage sendet, nachdem der Client-Cache abgelaufen ist, wird die DNS-Anfrage möglicherweise an eine andere GSLB-Site weitergeleitet. Die neue GSLB-Site verwendet das im Client-Request-Header enthaltene Site-Cookie, um die Persistenz zu implementieren. Die Funktion „Site-Persistenz“ wird unter den folgenden Bedingungen aktiv:

- Wenn der Domainname im Host-Header mit einer der GSLB-Domänen übereinstimmt
- Wenn die Site-Persistenz im GSLB-Dienst aktiviert ist, stellt dies den virtuellen Server dar, der den Anwendungsdatenverkehr empfängt.

Das Site-Cookie enthält Informationen über den ausgewählten GSLB-Dienst, zu dem der Client eine persistente Verbindung hat. Wenn der GSLB-Dienst, auf den das Cookie verweist, INAKTIV ist oder aus der GLSB-Konfiguration entfernt wurde, verarbeitet der virtuelle Server, der den Verkehr empfängt, den Verkehr weiter. Der Ablauf des Cookie basiert auf dem Cookie-Timeout, das auf der NetScaler-Appliance konfiguriert wurde. Wenn die Namen der virtuellen Server nicht auf allen Sites identisch sind, müssen Sie die Persistenz-ID verwenden. Die eingefügten Cookies entsprechen RFC 2109.

NetScaler unterstützt zwei Arten von Site-Persistenz:

- Verbindungs-Proxy
- HTTP-Weiterleitung

Verbindungs-Proxy

Im Verbindungs-Proxy-Modus der Site-Persistenz führt das Rechenzentrum, das die nachfolgende Anwendungsanforderung empfängt, die folgenden Aufgaben aus, um eine Verbindung herzustellen:

1. Stellt eine Verbindung zur GSLB-Site her, die das Site-Cookie eingefügt hat.
2. leitet die Client-Anfrage an die ursprüngliche Site weiter.

> **Hinweis:**
>
> Der Proxyserver stellt mithilfe der folgenden Details eine Verbindung mit der ursprünglichen Site her:
>
> - Das SNIP der neuen Site ist die Quell-IP-Adresse.
> - Die öffentliche IP-Adresse des GSLB-Dienstes der ursprünglichen Site ist die Ziel-IP-Adresse.

> - Ein kurzlebiger Port ist der Quellport und der GSLB-Serviceport ist der Zielport.
> - Verwendet je nach GSLB-Diensttyp entweder HTTP- oder HTTPS-Protokolle.

3. Erhält eine Antwort von der ursprünglichen GSLB-Site.
4. Leitet diese Antwort an den Client zurück.
5. Schließt die Verbindung.

HTTP-Weiterleitung

Wenn die GSLB-Konfiguration die HTTP-Weiterleitungspersistenz verwendet, leitet die neue Site die Anfrage an die Site weiter, die das Cookie ursprünglich eingefügt hat. Der Domainname in der Weiterleitungs-URL ist die Site-Domain. Stellen Sie sicher, dass sowohl Cookies als auch SSL-Zertifikate sowohl für die GSLB-Domain als auch für die Site-Domain gelten. Um Cookies sowohl für die GSLB als auch für die Site-Domain anzuwenden, muss die Cookie-Domäne die Site-zu-GSLB-Domäne sein. Um SSL-Zertifikate sowohl auf die GSLB- als auch auf die Site-Domain anzuwenden, muss es sich bei dem an den virtuellen SSL-Server gebundenen Zertifikat um ein Wildcard-Zertifikat handeln.

Der Verbindungsproxy wird aktiviert, wenn die folgenden Bedingungen erfüllt sind:

- Anfragen werden für eine Domain gesendet, die an GSLB teilnimmt. Die Domain wird aus dem URL/Host-Header abgerufen.
- Für den lokalen GSLB-Dienst ist der Verbindungsproxy aktiviert.
- Die Anfrage enthält ein gültiges Cookie, das die IP-Adresse eines aktiven Remote-GSLB-Dienstes enthält.

> **Hinweis**
>
> In einer GSLB-Parent-Child-Konfiguration funktioniert der Verbindungsproxy wie vorgesehen, auch wenn ein GSLB-Dienst nicht auf einer untergeordneten Site konfiguriert ist. Wenn Sie jedoch über eine zusätzliche Konfiguration wie Clientauthentifizierung, Client-IP-Adresseneinfügung oder andere SSL-spezifische Anforderungen verfügen, müssen Sie einen expliziten GSLB-Dienst auf der Site hinzufügen und entsprechend konfigurieren.
>
> Weitere Informationen zur Eltern-Kind-Topologie finden Sie unter Bereitstellung von Eltern-Kind-Topologie mit dem MEP-Protokoll.

So legen Sie die Persistenz basierend auf HTTP-Cookies über die Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb service <serviceName> -sitePersistence (ConnectionProxy [-
    sitePrefix <prefix>] | HTTPredirect -sitePrefix <prefix>)
<!--NeedCopy-->
```


Beispiel:

```
set gslb service service-GSLB-1 -sitePersistence ConnectionProxy
set gslb service service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
<!--NeedCopy-->
```

Um die Persistenz auf der Grundlage von Cookies mithilfe der GUI einzustellen

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services** und wählen Sie den Dienst aus, den Sie für die Site-Persistenz konfigurieren möchten (z. B. Service-GSLB-1).
2. Klicken Sie auf den Abschnitt **Site Persistence** und stellen Sie die Persistenz auf der Grundlage von Cookies ein.

Verwalten von Clientverbindungen

May 11, 2023

Um die Verwaltung von Clientverbindungen zu erleichtern, können Sie die verzögerte Bereinigung von Verbindungen zum virtuellen Server aktivieren. Sie können dann den lokalen DNS-Verkehr verwalten, indem Sie DNS-Richtlinien konfigurieren.

Aktivieren Sie die verzögerte Bereinigung von virtuellen Serververbindungen

Der Status eines virtuellen Servers hängt von den Zuständen der an ihn gebundenen Dienste ab, und der Status jedes Dienstes hängt von den an ihn gebundenen Monitoren ab. Wenn ein Server langsam oder ausfällt, prüft die Überwachung ein Timeout und der Dienst, der den Server repräsentiert, wird als DOWN markiert. Ein virtueller Server wird nur dann als DOWN markiert, wenn alle an ihn gebundenen Dienste als DOWN gekennzeichnet sind. Sie können Dienste und virtuelle Server so konfigurieren, dass sie entweder alle Verbindungen beenden, wenn sie ausfallen, oder die Verbindung zulassen. Die letztere Einstellung ist für Situationen gedacht, in denen ein Dienst aufgrund eines langsamen Servers als DOWN markiert ist.

Wenn Sie die Down-Status-Flush-Option konfigurieren, führt die NetScaler-Appliance eine verzögerte Bereinigung der Verbindungen zu einem ausgefallenen GSLB Service durch.

So ermöglichen Sie die verzögerte Bereinigung virtueller Serververbindungen über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die verzögerte Verbindungsbereinigung zu konfigurieren und die Konfiguration zu überprüfen:

```
set gslb service <name> -downStateFlush (ENABLED | DISABLED)
show gslb service <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb service Service-GSLB-1 -downStateFlush ENABLED
Done

show gslb service Service-GSLB-1
Done
<!--NeedCopy-->
```

So aktivieren Sie die verzögerte Bereinigung virtueller Serververbindungen mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services** und doppelklicken Sie auf den Dienst.
2. Klicken Sie auf den Abschnitt **Andere Einstellungen** und wählen Sie die Option **Down State Flush** aus.

Verwalten Sie den lokalen DNS-Verkehr mithilfe von DNS-Richtlinien

Sie können DNS-Richtlinien verwenden, um Site-Affinität zu implementieren, indem Sie den Datenverkehr von der IP-Adresse eines lokalen DNS-Resolvers oder Netzwerks zu einer vordefinierten Ziel-GSLB-Site leiten. Dies wird konfiguriert, indem DNS-Richtlinien mit DNS-Ausdrücken erstellt und die Richtlinien global auf der NetScaler-Appliance gebunden werden.

DNS-Ausdrücke

Die NetScaler-Appliance bietet bestimmte vordefinierte DNS-Ausdrücke, die zum Konfigurieren von Aktionen für eine Domäne verwendet werden können. Solche Aktionen können beispielsweise bestimmte Anfragen löschen, eine bestimmte Ansicht für eine bestimmte Domain auswählen oder bestimmte Anfragen an einen bestimmten Standort umleiten.

Diese DNS-Ausdrücke (auch *Regeln*genannt) werden kombiniert, um DNS-Richtlinien zu erstellen, die dann global an die NetScaler-Appliance gebunden sind.

Es folgt die Liste der vordefinierten DNS-Qualifizierer, die auf der NetScaler-Appliance verfügbar sind:

- CLIENT.UDP.DNS.DOMAIN.EQ (“Domainname”)
- CLIENT.UDP.DNS.IS_AREC
- CLIENT.UDP.DNS.IS_AAAAREC
- CLIENT.UDP.DNS.IS_SRVREC
- CLIENT.UDP.DNS.IS_MXREC
- CLIENT.UDP.DNS.IS_SOAREC
- CLIENT.UDP.DNS.IS_PTRREC
- CLIENT.UDP.DNS.IS_CNAME
- CLIENT.UDP.DNS.IS_NSREC
- CLIENT.UDP.DNS.IS_ANYREC

Der DNS-Ausdruck CLIENT.UDP.DNS.DOMAIN kann mit Zeichenfolgenausdrücken verwendet werden. Wenn Sie Domainnamen als Teil des Ausdrucks verwenden, müssen diese mit einem Punkt (.) enden. Zum Beispiel CLIENT.UDP.DNS.DOMAIN.ENDSWITH(“abc.com.”)

So erstellen Sie einen Ausdruck mithilfe des Konfigurationsdienstprogramms

1. Klicken Sie auf das Symbol neben dem Textfeld Ausdruck. Klicken Sie auf Hinzufügen. (Lassen Sie die Dropdownlistenfelder Flow-Typ und Protokoll leer.) Befolgen Sie diese Schritte, um eine Regel zu erstellen.
2. Wählen Sie im Feld Qualifier einen Qualifier aus (z. B. LOCATION).
3. Wählen Sie im Feld Operator einen Operator aus (z. B. ==).
4. Geben Sie im Feld Wert einen Wert ein (z. B. Asien, Japan…).
5. Klicken Sie auf OK. Klicken Sie auf Erstellen und auf Schließen. Die Regel wird erstellt.
6. Klicken Sie auf OK.

Konfigurieren von DNS-Aktionen

Eine DNS-Richtlinie enthält den Namen einer DNS-Aktion, die ausgeführt werden soll, wenn die Richtlinienregel auf TRUE ausgewertet wird. Eine DNS-Aktion kann eine der folgenden Aktionen ausführen:

- Senden Sie dem Client eine IP-Adresse, für die Sie eine DNS-Ansicht konfiguriert haben. Weitere Informationen zu DNS-Ansichten finden Sie unter Hinzufügen von DNS-Ansichten.
- Senden Sie dem Client die IP-Adresse eines GSLB-Dienstes, nachdem Sie auf eine Liste der bevorzugten Speicherorte verwiesen haben, die das statische Näherungsverhalten außer Kraft setzen. Weitere Informationen zu bevorzugten Standorten finden Sie unter Überschreiben des statischen Näherungsverhaltens durch Konfigurieren bevorzugter Standorte.
- Senden Sie dem Client eine bestimmte IP-Adresse, die durch die Auswertung der DNS-Abfrage oder -Antwort (DNS-Antwort-Rewrite) bestimmt wird.

- Leiten Sie eine Anforderung an den Nameserver weiter, ohne eine Suche im DNS-Cache der Appliance durchzuführen.
- Schenken Sie eine Anfrage.

Sie können keine DNS-Aktion erstellen, um eine DNS-Anforderung zu löschen oder den DNS-Cache auf der Appliance zu umgehen. Wenn Sie eine DNS-Anforderung löschen möchten, verwenden Sie die integrierte Aktion DNS_Default_ACT_Drop. Wenn Sie den DNS-Cache Bypass möchten, verwenden Sie die integrierte Aktion dns_default_act_cacheBypass. Beide Aktionen sind zusammen mit benutzerdefinierten Aktionen in den Dialogfeldern DNS-Richtlinie erstellen und DNS-Richtlinie konfigurieren verfügbar. Diese eingebauten Aktionen können nicht geändert oder entfernt werden.

So konfigurieren Sie eine DNS-Aktion über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine DNS-Aktion zu konfigurieren und die Konfiguration zu überprüfen:

```
add dns action <actionName> <actionType> (-IPAddress <ip_addr |
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...) [-TTL <secs>]

show dns action [<actionName>]
<!--NeedCopy-->
```

Beispiele

Beispiel 1: Konfigurieren des Rewrites von DNS-Antworten. Die folgende DNS-Aktion sendet dem Client eine vorkonfigurierte IP-Adresse, wenn die Richtlinie, an die die Aktion gebunden ist, als wahr ausgewertet wird:

```
add dns action dns_act_response_rewrite Rewrite_Response -IPAddress
    192.0.2.20 192.0.2.56 198.51.100.10
 Done

show dns action dns_act_response_rewrite
1) ActionName: dns_act_response_rewrite ActionType: Rewrite_Response
     TTL: 3600              IPAddress: 192.0.2.20 192.0.2.56
    198.51.100.10
 Done
<!--NeedCopy-->
```

Beispiel 2: Konfigurieren einer DNS-View-basierten Antwort. Die folgende DNS-Aktion sendet dem Client eine IP-Adresse, für die Sie eine DNS-Ansicht konfiguriert haben:


```
add dns action send_ip_from_view_internal_ip ViewName -viewName
   view_internal_ip
Done

show dns action send_ip_from_view_internal_ip
1)  ActionName:  send_ip_from_view_internal_ip ActionType:  ViewName
      ViewName:  view_internal_ip
 Done
<!--NeedCopy-->
```

Beispiel 3: Konfigurieren einer Antwort basierend auf einer bevorzugten Standortliste. Die folgende DNS-Aktion sendet dem Client die IP-Adresse, die dem bevorzugten Standort entspricht, den er aus der angegebenen Liste von Standorten auswählt:

```
add dns action send_preferred_location GslbPrefLoc -preferredLocList NA
   .tx.ns1.\*.\*.* NA.tx.ns2.\*.\*.* NA.tx.ns3.\*.\*.*
Done

show dns action  send_preferred_location
1)  ActionName:  send_preferred_location ActionType:  GslbPrefLoc
   PreferredLocList:  "NA.tx.ns1.\*.\*.\*" "NA.tx.ns2.\*.\*.\*" "NA.tx.
   ns3.\*.\*.*"
 Done
<!--NeedCopy-->
```

So konfigurieren Sie eine DNS-Aktion mithilfe des NetScaler-Konfigurationsdienstprogramms

1. Navigieren Sie zu Traffic Management > DNS > Aktionen, erstellen oder bearbeiten Sie eine DNS-Aktion.
2. Legen Sie im Dialogfeld DNS-Aktion erstellen oder DNS-Aktion konfigurieren die folgenden Parameter fest:
   - Aktionsname (kann für eine bestehende DNS-Aktion nicht geändert werden)
   - Typ (kann für eine vorhandene DNS-Aktion nicht geändert werden)

     Um den

     Type -Parameter festzulegen, führen Sie einen der folgenden Schritte aus:
     - Um eine DNS-Aktion zu erstellen, die einer DNS-Ansicht zugeordnet ist, wählen Sie Name anzeigen aus. Wählen Sie dann aus der Liste Name der Ansicht die DNS-Ansicht aus, die Sie in der Aktion verwenden möchten.
     - Um eine DNS-Aktion mit einer Liste bevorzugter Standorte zu erstellen, wählen Sie Bevorzugte Standortliste aus. Geben Sie unter Bevorzugter Standort einen Standort

ein und klicken Sie dann auf Hinzufügen. Fügen Sie so viele DNS-Standorte hinzu, wie Sie möchten.

- Um eine DNS-Aktion zum Rewrite einer DNS-Antwort auf der Grundlage einer Richtlinienbewertung zu konfigurieren, wählen Sie Rewrite-Antwort aus. Geben Sie unter IP-Adresse eine IP-Adresse ein und klicken Sie dann auf Hinzufügen. Fügen Sie so viele IP-Adressen hinzu, wie Sie möchten.

- TTL (gilt nur für den Aktionstyp Rewrite-Antwort)

Konfigurieren von DNS-Richtlinien

DNS-Richtlinien arbeiten in einer Standortdatenbank, die statische und benutzerdefinierte IP-Adressen verwendet. Die Attribute der eingehenden lokalen DNS-Anforderung werden als Teil eines Ausdrucks definiert, und die Ziel-Site wird als Teil einer DNS-Richtlinie definiert. Beim Definieren von Aktionen und Ausdrücken können Sie ein Paar einfacher Anführungszeichen (‘’) als Platzhalterqualifizierer verwenden, um mehr als eine Position anzugeben. Wenn eine DNS-Richtlinie konfiguriert ist und eine GSLB-Anforderung empfangen wird, wird zuerst die benutzerdefinierte IP-Adressdatenbank nach einem Eintrag abgefragt, der die Standortattribute für die Quelle definiert:

- Wenn eine DNS-Abfrage von einem LDNS stammt, werden die Eigenschaften des LDNS anhand der konfigurierten Richtlinien bewertet. Wenn sie übereinstimmen, wird eine entsprechende Aktion (Site-Affinität) ausgeführt. Wenn die LDNS-Eigenschaften mit mehr als einem Standort übereinstimmen, ist die Anforderung ein Lastausgleich zwischen den Standorten, die den LDNS-Eigenschaften entsprechen.
- Wenn der Eintrag in der benutzerdefinierten Datenbank nicht gefunden wird, wird die statische IP-Adressdatenbank nach einem Eintrag abgefragt, und wenn es eine Übereinstimmung gibt, wird die obige Richtlinienbewertung wiederholt.
- Wenn der Eintrag weder in den benutzerdefinierten noch in den statischen Datenbanken gefunden wird, wird die beste Site ausgewählt und in der DNS-Antwort auf der Grundlage der konfigurierten Lastausgleichsmethode gesendet.

Die folgenden Einschränkungen gelten für DNS-Richtlinien, die auf der NetScaler-Appliance erstellt wurden.

- Maximal 64 Richtlinien werden unterstützt.
- DNS-Richtlinien gelten global für die NetScaler-Appliance und können nicht auf einen bestimmten virtuellen Server oder eine bestimmte Domäne angewendet werden.
- Eine domäne- oder virtuelle Server-spezifische Bindung von Richtlinien wird nicht unterstützt.

Sie können DNS-Richtlinien verwenden, um Clients, die einem bestimmten IP-Adressbereich entsprechen, an eine bestimmte Site weiterzuleiten. Wenn Sie beispielsweise ein GSLB-Setup mit mehreren geografisch getrennten GSLB-Sites haben, können Sie alle Clients, deren IP-Adresse innerhalb eines bestimmten Bereichs liegt, an ein bestimmtes Rechenzentrum weiterleiten.

Sowohl TCP-basierter als auch UDP-basierter DNS-Verkehr kann ausgewertet werden. Richtlinienausdrücke sind für UDP-basierten DNS-Verkehr auf dem Server und sowohl für UDP-basierten DNS-Verkehr als auch für TCP-basierten DNS-Verkehr auf der Clientseite verfügbar. Darüber hinaus können Sie Ausdrücke konfigurieren, um Abfragen und Antworten auszuwerten, die nur die folgenden DNS-Fragetypen (oder QTYPE-Werte) beinhalten:

- A
- AAAA
- NS
- SRV
- PTR
- CNAME
- SOA
- MX
- ANY

Die folgenden Antwortcodes (RCODE-Werte) werden ebenfalls unterstützt:

- NOERROR - Kein Fehler
- FORMERR - Formatfehler
- SERVFAIL - Serverausfall
- NXDOMAIN — Nicht existierende Domäne
- NOTIMP - Abfragetyp nicht implementiert
- ABGELEHNT - Abfrage abgelehnt

Sie können Ausdrücke zur Auswertung des DNS-Datenverkehrs konfigurieren. Ein DNS-Ausdruck beginnt mit den Präfixen DNS.REQ oder DNS.RES. Zur Auswertung der abgefragten Domäne, des Abfragetyps und des Trägerprotokolls stehen Funktionen zur Verfügung. Weitere Informationen zu DNS-Ausdrücken finden Sie unter “Ausdrücke zum Auswerten einer DNS-Nachricht und Identifizierung ihres Carrier-Protokolls” unter “Richtlinienkonfiguration und Referenz”.

So fügen Sie mit der Befehlszeilenschnittstelle eine DNS-Richtlinie hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine DNS-Richtlinie zu erstellen und die Konfiguration zu überprüfen:

```
add dns policy <name> <rule> <actionName>
show dns policy <name>
<!--NeedCopy-->
```

Beispiel:

```
> add dns policy-GSLB-1 'CLIENT.UDP.DNS.DOMAIN.EQ("domainname")'
   my_dns_action
```



```
 Done
> show dns policy-GSLB-1
    Name: policy-GSLB-1
    Rule: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")
    Action Name: my_dns_action
    Hits: 0
    Undef Hits: 0

 Done
<!--NeedCopy-->
```

So entfernen Sie eine konfigurierte DNS-Richtlinie über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
rm dns policy <name>
<!--NeedCopy-->
```

So konfigurieren Sie eine DNS-Richtlinie mithilfe des NetScaler-Konfigurationsdienstprogramms

1. Navigieren Sie zu Traffic Management > DNS > Richtlinien und erstellen Sie eine DNS-Richtlinie.
2. Legen Sie im Dialogfeld DNS-Richtlinie erstellen oder DNS-Richtlinie konfigurieren die folgenden Parameter fest:
   - Richtlinienname (kann für eine bestehende Richtlinie nicht geändert werden)
   - Aktion
   - Ausdruck

     Um einen Ausdruck anzugeben, gehen Sie wie folgt vor:

     a) Klicken Sie auf Hinzufügen, und wählen Sie dann im angezeigten Dropdown-Feld das Ausdruckselement aus, mit dem Sie den Ausdruck beginnen möchten. Eine zweite Liste wird angezeigt. Die Liste enthält eine Reihe von Ausdruckselementen, die Sie unmittelbar nach dem ersten Ausdruckselement verwenden können.

     b) Wählen Sie in der zweiten Liste das gewünschte Ausdruckselement aus, und geben Sie dann eine Periode ein.

     c) Wenn Sie nach jeder Auswahl einen Zeitraum eingeben, wird der nächste Satz gültiger Ausdruckselemente in einer Liste angezeigt. Wählen Sie Ausdruckselemente aus und geben Sie Argumente für Funktionen ein, bis Sie den gewünschten Ausdruck haben.
3. Klicken Sie auf Erstellen oder OKund dann auf Schließen.

Binden von DNS-Richtlinien

DNS-Richtlinien sind global an die NetScaler-Appliance gebunden und für alle konfigurierten virtuellen GSLB-Server verfügbar. Obwohl DNS-Richtlinien global gebunden sind, kann die Richtlinienausführung auf einen bestimmten virtuellen GSLB-Server beschränkt werden, indem die Domäne im Ausdruck angegeben wird.

Hinweis: Obwohl der globale Befehl bind dns REQ_OVERRIDE und RES_OVERRIDE als gültige Bindepunkte akzeptiert, sind diese Bindungspunkte redundant, da DNS-Richtlinien nur global gebunden werden können. Binden Sie Ihre DNS-Richtlinien nur an die Bindungspunkte REQ_DEFAULT und RES_DEFAULT.

So binden Sie eine DNS-Richtlinie global über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine DNS-Richtlinie global zu binden und die Konfiguration zu überprüfen:

```
bind dns global <policyName> <priority> [-gotoPriorityExpression <
    string>] [-type <type>]
show dns global -type <type>
<!--NeedCopy-->
```

Beispiel:

```
bind dns global policy-GSLB-1 10 -gotoPriorityExpression END
 Done
show dns global -type REQ_DEFAULT
1)  Policy Name: policy-GSLB-1
    Priority: 10
    GotoPriorityExpression: END
 Done
<!--NeedCopy-->
```

So binden Sie eine DNS-Richtlinie mithilfe des Konfigurationsdienstprogramms global

1. Navigieren Sie zu Traffic Management > DNS > Richtlinien.
2. Klicken Sie im Detailbereich auf Globale Bindungen.
3. Klicken Sie im Dialogfeld DNS-Richtlinie (n) an Global binden/aufheben auf Richtlinie einfügen.
4. Wählen Sie in der Spalte Richtlinienname aus der Liste die Richtlinie aus, die Sie binden möchten. Alternativ klicken Sie in der Liste auf Neue Richtlinie, und erstellen Sie dann eine DNS-Richtlinie, indem Sie Parameter im Dialogfeld DNS-Richtlinie erstellen festlegen.

5. Um eine Richtlinie zu ändern, die bereits global gebunden ist, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld DNS-Richtlinie konfigurieren die Richtlinie, und klicken Sie dann auf OK.
6. Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie aufheben.
7. Um die einer Richtlinie zugewiesene Priorität zu ändern, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
8. Um zugewiesene Prioritäten erneut zu generieren, klicken Sie auf Prioritäten neu generieren. Die Prioritätswerte werden so geändert, dass sie bei 100 beginnen, mit Schritten von 10, ohne die Reihenfolge der Auswertung zu beeinflussen.
9. Klicken Sie auf OK.

So zeigen Sie die globalen Bindungen einer DNS-Richtlinie über die Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

```
show dns global
```

So zeigen Sie die globalen Bindungen einer DNS-Richtlinie mithilfe des Konfigurationsdienstprogramms an

1. Navigieren Sie zu **Traffic Management** > **DNS** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**. Die globalen Bindungen aller DNS-Richtlinien werden in diesem Dialogfeld angezeigt.

Hinzufügen von DNS-Ansichten

Sie können DNS-Ansichten konfigurieren, um verschiedene Clienttypen zu identifizieren und einer Gruppe von Clients, die nach derselben GSLB-Domäne fragen, eine geeignete IP-Adresse bereitzustellen. DNS-Ansichten werden mithilfe von DNS-Richtlinien konfiguriert, die die an den Client zurückgesendeten IP-Adressen auswählen.

Wenn Sie beispielsweise GSLB für die Domäne Ihres Unternehmens konfiguriert haben und den Server im Netzwerk Ihres Unternehmens gehostet haben, können Clients, die im internen Netzwerk Ihres Unternehmens nach der Domäne fragen, die interne IP-Adresse des Servers anstelle der öffentlichen IP-Adresse erhalten. Clients, die DNS für die Domain aus dem Internet abfragen, können andererseits die öffentliche IP-Adresse der Domain erhalten.

Um eine DNS-Ansicht hinzuzufügen, weisen Sie ihr einen Namen mit bis zu 31 Zeichen zu. Das Hauptzeichen muss eine Zahl oder ein Buchstabe sein. Die folgenden Zeichen sind ebenfalls zulässig: @ _ -. (Zeitraum): (Doppelpunkt) # und Raum (). Nachdem Sie die Ansicht hinzugefügt haben, konfigurieren Sie eine Richtlinie, um sie Clients und einem Teil des Netzwerks zuzuordnen, und

binden die Richtlinie global. Informationen zum Konfigurieren und Binden einer DNS-Richtlinie finden Sie unter **Verwalten des lokalen DNS-Datenverkehrs mithilfe von DNS-Richtlinien**.

So fügen Sie über die Befehlszeile eine DNS-Ansicht hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine DNS-Ansicht zu erstellen und die Konfiguration zu überprüfen:

```
1 add dns view <viewName>
2 show dns view <viewName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add dns view PrivateSubnet
2 show dns view PrivateSubnet
3 <!--NeedCopy-->
```

So entfernen Sie eine DNS-Ansicht über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
1 rm dns view <viewName>
2 <!--NeedCopy-->
```

So fügen Sie mithilfe des Konfigurationsdienstprogramms eine DNS-Ansicht hinzu

Navigieren Sie zu Traffic Management > DNS > Ansichten und fügen Sie eine DNS-Ansicht hinzu.

Weitere Informationen zum Erstellen einer DNS-Richtlinie und zum globalen Binden von DNS-Richtlinien finden Sie unter **Verwalten des lokalen DNS-Datenverkehrs mithilfe von DNS-Richtlinien**.

Konfigurieren von GSLB für Proximity

May 11, 2023

Wenn Sie GSLB für Proximity konfigurieren, werden Clientanfragen an das nächstgelegene Rechenzentrum weitergeleitet. Der Hauptvorteil der proximitätsbasierten GSLB-Methode sind schnellere Reaktionszeiten, die sich aus der Auswahl des nächstgelegenen verfügbaren Rechenzentrums ergeben.

Eine solche Bereitstellung ist entscheidend für Anwendungen, die schnellen Zugriff auf große Datenmengen benötigen.

Sie können GSLB für die Nähe auf der Grundlage der Roundtrip-Zeit (RTT), der statischen Nähe oder einer Kombination aus beiden konfigurieren.

Konfigurieren Sie die Methode Dynamic Round Trip Time (RTT)

Dynamic Round Trip Time (RTT) ist ein Maß für die Zeit oder Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource. Um dynamisches RTT zu messen, untersucht die NetScaler-Appliance den lokalen DNS-Server des Clients und sammelt RTT-Metrikinformationen. Die Appliance verwendet dann diese Metrik, um ihre Lastausgleichsentscheidung zu treffen. Der globale Serverlastenausgleich überwacht den Status des Netzwerks in Echtzeit und leitet die Client-Anfrage dynamisch an das Rechenzentrum mit dem niedrigsten RTT-Wert weiter.

Um GSLB für die Methode „Proximity with dynamic“ zu konfigurieren, müssen Sie zuerst das grundlegende GSLB-Setup und dann das dynamische RTT konfigurieren.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie dann für die lokale Site einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie eine grundlegende GSLB-Setup konfiguriert haben, konfigurieren Sie die dynamische RTT-Methode.

Weitere Informationen zur Konfiguration des virtuellen GSLB-Servers für die Verwendung der dynamischen RTT-Methode für den Lastenausgleich finden Sie unter Konfigurieren von dynamischem RTT.

Statische Nähe konfigurieren

Die statische Proximity-Methode für GSLB verwendet eine auf IP-Adressen basierende statische Proximity-Datenbank, um die Nähe zwischen dem lokalen DNS-Server des Clients und den GSLB-Standorten zu ermitteln. Die NetScaler-Appliance antwortet mit der IP-Adresse eines Standorts, der die Näherungskriterien am besten erfüllt.

Wenn zwei oder mehr GSLB-Standorte an verschiedenen geografischen Standorten denselben Inhalt bereitstellen, verwaltet die NetScaler-Appliance eine Datenbank mit IP-Adressbereichen und verwen-

det die Datenbank für Entscheidungen über die GSLB-Websites, an die eingehende Clientanfragen weitergeleitet werden sollen.

Um GSLB für Näherung mit statischer Nähe zu konfigurieren, müssen Sie zuerst die grundlegende GSLB-Setup konfigurieren und dann statische Nähe konfigurieren.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie dann für die lokale Site einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie eine grundlegende GSLB-Setup konfiguriert haben, konfigurieren Sie die statische Nähe.

Weitere Informationen zur Konfiguration des virtuellen GSLB-Servers für die Verwendung der statischen Nähe für den Lastenausgleich finden Sie unter Konfigurieren der statischen Nähe.

Konfigurieren der statischen Nähe und dynamischen RTT

Sie können den virtuellen GSLB-Server so konfigurieren, dass er eine Kombination aus statischer Nähe und dynamischem RTT verwendet, wenn einige Kunden aus einem internen Netzwerk wie einer Zweigstelle kommen. Sie können GSLB so konfigurieren, dass die von der Zweigstelle oder einem anderen internen Netzwerk kommenden Clients an einen bestimmten GSLB-Standort weitergeleitet werden, der sich geografisch in der Nähe des Client-Netzwerks befindet. Für alle anderen Anfragen können Sie dynamisches RTT verwenden.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie dann für die lokale Site einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie ein grundlegendes GSLB-Setup konfiguriert haben, konfigurieren Sie den virtuellen GSLB-Server so, dass er statische Nähe für den gesamten Datenverkehr verwendet, der von einem internen Netzwerk stammt, und verwenden Sie dann den dynamischen RTT für den gesamten anderen Datenverkehr.

Weitere Informationen zur Konfiguration der statischen Nähe finden Sie unter Konfigurieren der statischen Nähe und weitere Informationen zur Konfiguration von dynamischem RTT finden Sie unter Konfigurieren von dynamischem RTT.

Schützen des GSLB-Setups vor Ausfällen

May 11, 2023

Sie können Ihr GSLB-Setup vor dem Ausfall einer GSLB-Site oder eines virtuellen GSLB-Servers schützen, indem Sie Folgendes konfigurieren:

- Ein virtueller GSLB-Server
- Eine NetScaler Appliance, um mit mehreren IP-Adressen zu antworten
- Eine Backup-IP-Adresse für eine GSLB-Domäne

Sie können überschüssigen Datenverkehr auch auf einen virtuellen Backup-Server umleiten, indem Sie Spillover verwenden.

Konfigurieren Sie einen virtuellen GSLB-Backup-Server

Durch die Konfiguration einer Backup-Entität für einen virtuellen GSLB-Server wird sichergestellt, dass der DNS-Verkehr zu einer Site nicht unterbrochen wird, wenn der virtuelle GSLB-Server ausfällt. Die Backup-Entität kann ein anderer virtueller GSLB-Server oder eine Backup-IP-Adresse sein. Wenn eine Backupeinheit konfiguriert ist, verarbeitet die Backupeinheit DNS-Anforderungen, wenn der primäre virtuelle GSLB-Server ausfällt. Um anzugeben, was passieren muss, wenn der primäre virtuelle GSLB-Server erneut angezeigt wird, können Sie die Sicherungseinheit so konfigurieren, dass sie den Datenverkehr fortsetzt, bis Sie den primären virtuellen Server manuell die Übernahme aktivieren (mit der Option DisablePrimaryOnDown).

Hinweis: Sie können eine einzelne Backup-Entität als Backup für mehrere virtuelle GSLB-Server konfigurieren.

So konfigurieren Sie einen virtuellen GSLB-Backupserver mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen GSLB-Server als virtuellen Sicherungsserver zu konfigurieren und die Konfiguration zu überprüfen:

```
set gslb vserver <name> -backupVServer <name> [-disablePrimaryOnDown (
    ENABLED | DISABLED)]

show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2 -
    disablePrimaryOnDown ENABLED
```



```
show gslb vserver vserver-GSLB-1
<!--NeedCopy-->
```

So richten Sie den virtuellen GSLB-Server mithilfe des Konfigurationsdienstprogramms als virtuellen Backup-Server ein

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server.
2. Wählen Sie den Abschnitt **Virtuellen Server Backup** und den virtuellen Backup-Server wählen.

Konfigurieren eines GSLB-Setups für die Reaktion mit mehreren IP-Adressen

Eine typische DNS-Antwort enthält die IP-Adresse des am besten leistungsfähigen GSLB-Dienstes. Wenn Sie jedoch mehrere IP-Antworten (MIR) aktivieren, sendet die NetScaler Appliance den besten GSLB Service als ersten Datensatz in der Antwort und fügt die verbleibenden aktiven Dienste als zusätzliche Datensätze hinzu. Wenn MIR deaktiviert ist (Standardeinstellung), sendet die NetScaler Appliance den besten Service als einzigen Datensatz als Antwort.

So konfigurieren Sie einen virtuellen GSLB-Server für mehrere IP-Antworten mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen virtuellen GSLB-Server für mehrere IP-Antworten zu konfigurieren und die Konfiguration zu überprüfen:

```
set gslb vserver<name> -MIR (ENABLED | DISABLED)
-  show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -MIR ENABLED
 show gslb vserver <vserverName>
<!--NeedCopy-->
```

So richten Sie mithilfe des Konfigurationsdienstprogramms einen virtuellen GSLB-Server für mehrere IP-Antworten ein

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server, für den Sie einen virtuellen Backupserver konfigurieren möchten (z. B. vServer-GSLB-1).

2. Aktivieren Sie auf der Registerkarte **Erweitert** unter Wenn dieser virtuelle Server “UP” ist, das Kontrollkästchen Alle “aktiven” Dienst-IP als Antwort (MIR) senden, und wählen Sie **OK**aus.

Konfigurieren eines virtuellen GSLB-Servers für die Reaktion mit einem leeren Adressdatensatz bei DOWN

Eine DNS-Antwort kann entweder die IP-Adresse der angeforderten Domain oder eine Antwort enthalten, die besagt, dass die IP-Adresse der Domain dem DNS-Server nicht bekannt ist. In diesem Fall wird die Anfrage an einen anderen Nameserver weitergeleitet. Dies sind die einzig möglichen Antworten auf eine DNS-Anfrage.

Wenn ein virtueller GSLB-Server deaktiviert ist oder sich in einem DOWN-Status befindet, enthält die Antwort auf eine DNS-Anfrage für die an diesen virtuellen Server gebundene GSLB-Domäne die IP-Adressen aller Dienste, die an den virtuellen Server gebunden sind. Sie können den virtuellen GSLB-Server jedoch so konfigurieren, dass er in diesem Fall eine leere Down-Antwort (EDR) sendet. Wenn diese Option aktiviert ist, enthält eine DNS-Antwort von einem virtuellen GSLB-Server, der sich im Status DOWN befindet, keine IP-Adresseinträge, aber der Antwortcode ist erfolgreich. Dadurch wird verhindert, dass Clients versuchen, eine Verbindung zu GSLB-Sites herzustellen, die ausgefallen sind.

Hinweis: Sie müssen diese Einstellung für jeden virtuellen Server konfigurieren, auf den sie angewendet werden soll.

So konfigurieren Sie einen virtuellen GSLB-Server für leere Down-Antworten mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver<name> -EDR (ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
> set gslb vserver vserver-GSLB-1 -EDR ENABLED
 Done
<!--NeedCopy-->
```

So richten Sie mithilfe des Konfigurationsdienstprogramms einen virtuellen GSLB-Server für leere Down-Antworten ein

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server, für den Sie einen virtuellen Backupserver konfigurieren möchten (z. B. vServer-GSLB-1).

2. Aktivieren Sie auf der Registerkarte Erweitert unter Wenn dieser virtuelle Server “Nicht” ist, das Kontrollkästchen Die IP-Adresse in Antwort (EDR) keinen Dienst senden.
3. Klicken Sie auf **OK**.

Konfigurieren Sie eine Backup-IP-Adresse für eine GSLB-Domain

Sie können eine Backup-Site für Ihre GSLB-Konfiguration konfigurieren. Wenn bei dieser Konfiguration alle primären Standorte NACH UNTEN gehen, wird die IP-Adresse der Backup-Site in der DNS-Antwort angegeben.

Wenn ein virtueller GSLB-Server aktiv ist, sendet dieser virtuelle Server in der Regel eine DNS-Antwort mit einer der aktiven Site-IP-Adressen, die von der konfigurierten GSLB-Methode ausgewählt wurde. Wenn alle konfigurierten primären Standorte auf dem virtuellen GSLB-Server inaktiv sind (im Status DOWN), sendet der autoritative Domänennamensystem (ADNS) -Server oder der DNS-Server eine DNS-Antwort mit der IP-Adresse des Backup-Site.

Hinweis: Wenn eine Backup-IP-Adresse gesendet wird, wird die Persistenz nicht berücksichtigt.

So legen Sie mithilfe der Befehlszeilenschnittstelle eine Backup-IP-Adresse für eine Domain fest

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Backup-IP-Adresse festzulegen und die Konfiguration zu überprüfen:

```
set gslb vserver <name> -domainName <string> -backupIP <IPAddress>
show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -domainName www.abc.com -backupIP
   10.102.29.66
show gslb vserver vserver-GSLB-1
<!--NeedCopy-->
```

So legen Sie mithilfe des Konfigurationsdienstprogramms eine Backup-IP-Adresse für eine Domain fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtual Servers** und doppelklicken Sie auf den virtuellen GSLB-Server, an den Sie die Backup-Domäne binden möchten (z. B. vServer-GSLB-1).
2. Klicken Sie auf den Abschnitt **Domains**, konfigurieren Sie die GSLB-Domain und geben Sie die IP-Adresse der Backup-Domain im Feld **Backup-IP** an.

Überschüssigen Datenverkehr auf einen virtuellen Backup-Server umleiten

Sobald die Anzahl der Verbindungen zu einem primären virtuellen GSLB-Server den konfigurierten Schwellenwert überschreitet, können Sie die Spillover-Option verwenden, um neue Verbindungen an einen virtuellen Backup-GSLB-Server umzuleiten. Dieser Schwellenwert kann dynamisch berechnet oder manuell festgelegt werden. Sobald die Anzahl der Verbindungen zum primären virtuellen Server unter den Schwellenwert fällt, nimmt der primäre virtuelle GSLB-Server die Bearbeitung von Clientanfragen wieder auf.

Sie können die Persistenz mit Spillover konfigurieren. Wenn die Persistenz konfiguriert ist, werden neue Clients auf den virtuellen Backup-Server umgeleitet, sofern dieser Client nicht bereits mit einem primären virtuellen Server verbunden ist. Wenn die Persistenz konfiguriert ist, werden Verbindungen, die an den virtuellen Backup-Server umgeleitet wurden, nicht zurück zum primären virtuellen Server verschoben, nachdem die Anzahl der Verbindungen zum primären virtuellen Server unter den Schwellenwert gefallen ist. Stattdessen verarbeitet der virtuelle Backup-Server diese Verbindungen weiter, bis sie vom Benutzer beendet werden. In der Zwischenzeit akzeptiert der primäre virtuelle Server neue Clients.

Der Schwellenwert kann anhand der Anzahl der Verbindungen, der Bandbreite und des Zustands der Dienste gemessen werden.

Wenn der virtuelle Backup-Server den konfigurierten Schwellenwert erreicht und keine zusätzliche Last aufnehmen kann, leitet der primäre virtuelle Server alle Anfragen an die angegebene Umleitungs-URL um. Wenn auf dem primären virtuellen Server keine Umleitungs-URL konfiguriert ist, werden nachfolgende Anfragen verworfen.

Die Spillover-Funktion verhindert, dass der GSLB-Remote-Backup-Dienst (Backup-GSLB-Site) mit Client-Anfragen überflutet wird, wenn der primäre virtuelle GSLB-Server ausfällt. Dies tritt auf, wenn ein Monitor an einen GSLB-Remote-Dienst gebunden ist und der Dienst aufgrund eines Fehlers in den Status DOWN versetzt wird. Aufgrund der Spillover-Funktion behält der Monitor den Status des Remote-GSLB-Dienstes jedoch weiterhin bei.

Im Rahmen der Lösung dieses Problems werden zwei Staaten für einen GSLB-Dienst beibehalten, der Primärstaat und der effektive Staat. Der Primärstatus ist der Status des primären virtuellen Servers und der effektive Status ist der kumulative Status der virtuellen Server (Primär- und Backup-Kette). Der effektive Status wird auf UP gesetzt, wenn einer der virtuellen Server in der Kette der virtuellen Server in Betrieb ist. Eine Flagge, die anzeigt, dass der primäre VIP den Schwellenwert erreicht hat, ist ebenfalls vorhanden. Der Schwellenwert kann entweder anhand der Anzahl der Verbindungen oder der Bandbreite gemessen werden.

Ein Dienst wird für GSLB nur in Betracht gezogen, wenn sein Primärstatus UP ist. Der Datenverkehr wird nur dann an den GSLB-Backupdienst weitergeleitet, wenn alle primären virtuellen Server heruntergefahren sind. In der Regel haben solche Bereitstellungen nur einen Sicherungs-GSLB-Dienst.

Das Hinzufügen von primären und effektiven Zuständen zu einem GSLB-Dienst hat folgende

Auswirkungen:

- Wenn die Quell-IP-Persistenz konfiguriert ist, wird der lokale DNS nur dann an die zuvor ausgewählte Site weitergeleitet, wenn der primäre virtuelle Server an der ausgewählten Site aktiv ist und den Schwellenwert unterschreitet. Persistenz kann im Round-Robin-Modus ignoriert werden.
- Wenn die Cookie-basierte Persistenz konfiguriert ist, werden Clientanforderungen nur dann umgeleitet, wenn der primäre virtuelle Server auf dem ausgewählten Standort UP ist.
- Wenn der primäre virtuelle Server seine Sättigung erreicht hat und die Backup-VIPs nicht vorhanden oder heruntergefahren sind, wird der effektive Status auf DOWN festgelegt.
- Wenn externe Monitore an einen virtuellen HTTP-HTTPS-Server gebunden sind, entscheidet der Monitor den Primärzustand.
- Wenn kein virtueller Backupserver auf dem primären virtuellen Server vorhanden ist und der primäre virtuelle Server seinen Schwellenwert erreicht hat, wird der effektive Status auf DOWN festgelegt.

So konfigurieren Sie den virtuellen Backup-GSLB-Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den virtuellen GSLB-Server zu konfigurieren und die Konfiguration zu überprüfen:

```
set gslb vserver <name> -soMethod <method> -soThreshold <threshold> -
    soPersistence ( \*\*ENABLED\*\* | \*\*DISABLED\*\* ) -
    soPersistenceTimeout <timeout>
show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -soMethod CONNECTION -soThreshold 1000
    -soPersistence ENABLED -soPersistenceTimeout 2
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Backup-GSLB-Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen Server, den Sie als Backup konfigurieren möchten (z. B. vServer-LB-1).
2. Klicken Sie auf den Abschnitt **SpillOver**, und legen Sie die folgenden Parameter fest:
   - Methode — Irgendeine Methode
   - Schwellenwert — SoSchwellenwert

- Persistenz-Timeout (min) — soPersistenceTimeout

3. Wählen Sie die Option Persistenz aus, und klicken Sie auf **OK**.

Konfigurieren von GSLB für Disaster Recovery

May 11, 2023

Disaster Recovery-Funktionen sind von entscheidender Bedeutung, da Ausfallzeiten kostspielig sind. Eine für GSLB konfigurierte NetScaler-Appliance leitet den Datenverkehr an das am wenigsten ausgelastete oder das leistungsstärkste Rechenzentrum weiter. Diese Konfiguration, die als aktiv-aktives Setup bezeichnet wird, verbessert nicht nur die Leistung, sondern bietet auch eine sofortige Notfallwiederherstellung, indem Datenverkehr an andere Rechenzentren weitergeleitet wird, wenn ein Rechenzentrum, das Teil des Setups ist, ausfällt. Alternativ können Sie ein GSLB-Setup im aktiven Standby-Modus nur für die Notfallwiederherstellung konfigurieren.

Konfigurieren Sie GSLB für die Notfallwiederherstellung in einem Active-Standby-Rechenzentrums-Setup

Ein herkömmliches Disaster-Recovery-Setup umfasst ein aktives Rechenzentrum und ein Standby-Rechenzentrum. Das Standby-Rechenzentrum ist ein Remote-Standort. Tritt aufgrund eines Katastrophenereignisses ein Failover auf, das dazu führt, dass das primäre aktive Rechenzentrum inaktiv ist, wird das Standby-Rechenzentrum betriebsbereit.

Die Konfiguration der Notfallwiederherstellung in einem Rechenzentrum mit aktivem Standby-Modus umfasst die folgenden Aufgaben.

- Erstellen Sie das aktive Rechenzentrum.
  - Fügen Sie eine lokale GSLB-Site hinzu.
  - Fügen Sie einen GSLB-vserver hinzu, der das aktive Rechenzentrum darstellt.
  - Binden Sie die Domain an den virtuellen GSLB-Server.
  - Fügen Sie gslb-Dienste hinzu und binden Sie die Dienste an den aktiven virtuellen GSLB-Server.
- Erstellen Sie das Standby-Rechenzentrum.
  - Fügen Sie eine Remote-GSLB-Site hinzu.
  - Fügen Sie einen gslb-vserver hinzu, der das Standby-Rechenzentrum darstellt.
  - Fügen Sie gslb-Dienste hinzu, die das Standby-Rechenzentrum darstellen, und binden Sie die Dienste an den Standby-GSLB-vserver.
  - Benennen Sie das Standby-Rechenzentrum, indem Sie den virtuellen GSLB-Standby-Server als virtuellen Backup-Server für den aktiven virtuellen GSLB-Server konfigurieren.

Nachdem Sie das primäre Rechenzentrum konfiguriert haben, replizieren Sie die Konfiguration für das Backupdatenzentrum und legen Sie es als Standby GSLB-Site fest, indem Sie einen virtuellen GSLB-Server an diesem Standort als virtuellen Backupserver festlegen.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

So weisen Sie die Standby GSLB-Site mit der Befehlszeilenschnittstelle aus

Geben Sie sowohl am aktiven Standort als auch am Remote-Standort an der Befehlszeile Folgendes ein:

```
set gslb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2
<!--NeedCopy-->
```

So konfigurieren Sie die Standby-Site mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server und doppelklicken Sie auf den virtuellen GSLB-Server für den primären Standort.
2. Klicken Sie auf den Abschnitt **Virtuellen Backup-Server** und wählen Sie einen virtuellen Backup-Server aus.

Sobald der primäre virtuelle Server aktiv wird, beginnt er standardmäßig, Datenverkehr zu empfangen. Wenn Sie jedoch möchten, dass der Datenverkehr auch dann an den virtuellen Backup-Server weitergeleitet wird, wenn der primäre virtuelle Server aktiv wird, verwenden Sie die Option „Primär deaktivieren bei Ausfall“.

Konfiguration für Disaster Recovery in einem aktiven Rechenzentrums-Setup

Eine aktiv-aktive GSLB-Bereitstellung, bei der beide GSLB-Standorte aktiv sind, beseitigt jedes Risiko, das mit einem Standby-Rechenzentrum einhergehen kann. Mit einer solchen Einrichtung können Web- oder Anwendungsinhalte an geografisch getrennten Orten gespiegelt werden. Dadurch wird sichergestellt, dass Daten in jedem verteilten Rechenzentrum konsistent verfügbar sind.

Um GSLB für die Notfallwiederherstellung in einem aktiven Rechenzentrum zu konfigurieren, müssen Sie zuerst das grundlegende GSLB-Setup im ersten Rechenzentrum konfigurieren und dann alle anderen Rechenzentren konfigurieren.

Erstellen Sie zunächst mindestens zwei GSLB-Sites. Erstellen Sie dann für die lokale Site einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server an der lokalen Site. Erstellen Sie schließlich am lokalen Standort einen virtuellen Lastausgleichsserver mit derselben virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Nachdem Sie das erste Rechenzentrum konfiguriert haben, replizieren Sie die Konfiguration für andere Rechenzentren, die Teil der Einrichtung sind.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Konfigurieren für Disaster Recovery mit gewichtetem Round Robin

Wenn Sie GSLB für die Verwendung der gewichteten Round-Robin-Methode konfigurieren, werden den GSLB-Diensten Gewichtungen hinzugefügt und der konfigurierte Prozentsatz des eingehenden Datenverkehrs wird an jeden GSLB-Standort gesendet. Sie können Ihr GSLB-Setup beispielsweise so konfigurieren, dass 80 Prozent des Traffics an eine Site und 20 Prozent des Traffics an eine andere weitergeleitet werden. Nachdem Sie dies getan haben, sendet die NetScaler-Appliance für jede Anfrage, die sie an den zweiten Standort sendet, vier Anfragen an den ersten Standort.

Um die gewichtete Round-Robin-Methode einzurichten, erstellen Sie zunächst zwei GSLB-Standorte, lokal und remote. Erstellen Sie als Nächstes für die lokale Site einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Konfigurieren Sie die GSLB-Methode als Round-Robin-Methode. Erstellen Sie als Nächstes ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Jedem Dienst, der einen physischen Server im Netzwerk darstellt, sind Gewichtungen zugeordnet. Daher wird dem GSLB-Dienst ein dynamisches Gewicht zugewiesen, das sich aus der Summe der Gewichte aller an ihn gebundenen Dienste ergibt. Der Verkehr wird dann auf die GSLB-Dienste aufgeteilt, basierend auf dem Verhältnis des dynamischen Gewichts des jeweiligen Dienstes zum Gesamtgewicht. Sie können anstelle des dynamischen Gewichts auch individuelle Gewichte für jeden GSLB-Service konfigurieren.

Wenn den Diensten keine Gewichtungen zugeordnet sind, können Sie den virtuellen GSLB-Server so konfigurieren, dass die Anzahl der an ihn gebundenen Dienste verwendet wird, um die Gewichtung dynamisch zu berechnen.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie ein grundlegendes GSLB-Setup konfiguriert haben, müssen Sie die gewichtete Round-Robin-Methode so konfigurieren, dass der Datenverkehr auf die konfigurierten GSLB-Sites aufgeteilt

wird, entsprechend den für die einzelnen Dienste konfigurierten Gewichtungen.

So konfigurieren Sie einen virtuellen Server, um Diensten Gewichtungen zuzuweisen, indem Sie die Befehlszeilenschnittstelle verwenden

Geben Sie an der Befehlszeile einen der folgenden Befehle ein, je nachdem, ob Sie einen neuen virtuellen Lastausgleichsserver erstellen oder einen vorhandenen konfigurieren möchten:

```
add lb vserver <name>@ -weight <WeightValue> <ServiceName>
set lb vserver <name>@ -weight <WeightValue> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
set lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
<!--NeedCopy-->
```

So legen Sie das dynamische Gewicht mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver <name> -dynamicWeight DynamicWeightType
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -dynamicWeight ServiceWeight
<!--NeedCopy-->
```

So fügen Sie Gewichtungen zu den GSLB-Diensten mithilfe der Befehlszeilenschnittstelle hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver <name> -serviceName GSLBServiceName -weight
   WeightValue
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1 -weight 1
<!--NeedCopy-->
```


So konfigurieren Sie einen virtuellen Server, um Diensten Gewichte zuzuweisen, indem Sie das Konfigurationsprogramm verwenden

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtual Servers und doppelklicken Sie auf den virtuellen Server (z. B. vServer-LB-1).
2. Klicken Sie auf den Abschnitt Dienste und legen Sie das Gewicht eines Dienstes fest.

So fügen Sie Gewichtungen zu den GSLB-Diensten mithilfe des Konfigurationsdienstprogramms hinzu

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server und doppelklicken Sie auf den virtuellen Server (z. B. vServer-GSLB-1)
2. Klicken Sie auf den Abschnitt Dienste und legen Sie das Gewicht des Dienstes im Feld Gewicht fest.

So legen Sie das dynamische Gewicht mithilfe des Konfigurationsprogramms fest

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server und doppelklicken Sie auf den virtuellen Server (z. B. vServer-GSLB-1).
2. Klicken Sie auf den Abschnitt **Methode** und wählen Sie in der Dropdownliste **Dynamic Weight** die Option **SERVICEWEIGHT**aus.

Konfiguration für Disaster Recovery mit Data Center Persistence

Die Persistenz des Rechenzentrums ist für Webanwendungen erforderlich, bei denen eine Verbindung mit demselben Server aufrechterhalten werden muss, anstatt die Anforderungen mit einem Lastenausgleich zu versehen. In einem E-Commerce-Portal ist beispielsweise die Aufrechterhaltung einer Verbindung zwischen dem Client und demselben Server von entscheidender Bedeutung. Für solche Anwendungen kann die Persistenz der HTTP-Weiterleitung in einem Active-Active-Setup konfiguriert werden.

Um GSLB für die Notfallwiederherstellung mit Rechenzentrumspersistenz zu konfigurieren, müssen Sie zuerst die grundlegende GSLB-Setup konfigurieren und dann die HTTP-Umleitungspersistenz konfigurieren.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie als Nächstes für die lokale Site einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie als Nächstes ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie als Nächstes einen virtuellen Lastausgleichsserver mit derselben virtuellen Server-IP-Adresse wie der GSLB-Dienst. Duplizieren Sie abschließend die vorherigen Schritte für die Remotekonfiguration oder konfigurieren Sie die NetScaler Appliance, um Ihre GSLB-Konfiguration automatisch zu synchronisieren.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie eine grundlegende GSLB-Setup konfiguriert haben, konfigurieren Sie die Priorität der HTTP-Umleitung, um die Persistenz des Rechenzentrums zu aktivieren.

So konfigurieren Sie die HTTP-Weiterleitung mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die HTTP-Weiterleitung zu konfigurieren und die Konfiguration zu überprüfen:

```
set gslb service <serviceName> -sitePersistence <sitePersistence> -
   sitePrefix <string>
show gslb service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
set gslb service Service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

So konfigurieren Sie die HTTP-Weiterleitung mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu Traffic Management > GSLB > Services und doppelklicken Sie auf den GSLB-Dienst, der konfiguriert werden soll.
2. Klicken Sie auf den Abschnitt **Site Persistence**, wählen Sie die Option **HttpRedirect aus und geben Sie im Textfeld Site Prefixdas Site-Präfix** ein (z. B. vServer-GSLB-1).

> **Hinweis**
>
> Wenn die Standortpersistenz nicht konfiguriert ist und ein virtueller Lastausgleichsserver, der als lokaler GSLB-Dienst konfiguriert ist, DOWN ist, werden die HTTP-Anforderungen mithilfe einer 302-Umleitung an andere fehlerfreie GSLB-Sites umgeleitet.

Überschreiben des statischen Proximityverhaltens durch Konfigurieren bevorzugter Standorte

May 11, 2023

Möglicherweise möchten Sie den Datenverkehr von einem lokalen DNS-Server (LDNS) oder Netzwerk an einen anderen GSLB-Dienst als den GSLB-Dienst weiterleiten, den die statische Proximity-Methode für diesen Verkehr auswählt. Das heißt, Sie haben einen
bevorzugten Standort für diesen Verkehr. Um die statische Näherungsmethode durch bevorzugte Standorte zu überschreiben, können Sie wie folgt vorgehen:

1. Konfigurieren Sie eine DNS-Aktion, die aus einer Liste der bevorzugten Speicherorte besteht. Weitere Informationen zum Konfigurieren einer DNS-Aktion finden Sie unter Konfigurieren einer DNS-Aktion.
2. Konfigurieren Sie eine DNS-Richtlinie, um den Datenverkehr zu identifizieren, der vom LDNS-Server oder Netzwerk eintrifft, für den Sie die statische Nähe überschreiben möchten, und wenden Sie die Aktion in der Richtlinie an.
3. Binden Sie die Richtlinie an den globalen Anforderungsbindungspunkt.

In der DNS-Aktion können Sie eine Liste mit bis zu 8 bevorzugten Standorten konfigurieren. Die Positionen müssen in der punktierten Qualifier-Notation angegeben werden. Dies ist die Schreibweise, in der Sie der statischen Proximity-Datenbank benutzerdefinierte Standorte hinzufügen. Die Speicherorte können Platzhalter für Kriterien enthalten, die Sie weglassen möchten. Informationen zur gepunkteten Qualifikator-Notation für Standorte finden Sie unter Benutzerdefinierte Einträge zu einer statischen Proximity-Datenbank hinzufügen. Bei der Eingabe der bevorzugten Positionen müssen Sie diese in absteigender Reihenfolge der Priorität eingeben.

Wenn eine Richtlinie als
TRUE ausgewertet wird, ordnet die NetScaler-Appliance die bevorzugten Standorte in Prioritätsreihenfolge den Standorten der GSLB-Dienste zu. Es gibt die folgenden zwei Arten von Spielen:

- Wenn alle Qualifikationsspiele an einem bevorzugten Ort, die keine Wildcard haben, mit den entsprechenden Qualifikationsspielen am Standort eines GSLB-Dienstes übereinstimmen, gilt das Spiel als perfekt. Beispielsweise passt ein GSLB-Servicestandort *.* oder Europe.UK.*.* perfekt zum bevorzugten Standort *.UK.*.*.
- Wenn nur eine Teilmenge der Qualifikationsspiele, bei denen es sich nicht um Wildcards handelt, übereinstimmt, wird das Spiel als Teilspiel betrachtet. Beispielsweise entspricht ein GSLB-Servicestandort von Europe.eg teilweise dem bevorzugten Standort Europe.uk.

Wenn eine DNS-Richtlinie als
TRUE ausgewertet wird, wird der folgende Algorithmus verwendet, um einen GSLB-Dienst auszuwählen:

1. Die Appliance bewertet den bevorzugten Standort mit der höchsten Priorität und geht in der Prioritätsreihenfolge nach unten, bis eine perfekte Übereinstimmung zwischen einem bevorzugten Standort und dem Standort eines GSLB-Dienstes gefunden wurde.

   Wenn eine perfekte Übereinstimmung gefunden wird, überprüft das Gerät, ob der entsprechende GSLB-Dienst verfügbar ist. Wenn es aktiv ist, gibt es die IP-Adresse des GSLB-Dienstes in der

DNS-Antwort zurück. Wenn mehrere perfekte Übereinstimmungen gefunden werden (was passieren kann, wenn ein oder mehrere Platzhalter an einem bevorzugten Ort verwendet werden), überprüft die Appliance den Status der entsprechenden GSLB-Dienste und verteilt die laufenden GSLB-Dienste.

2. Wenn für keinen der bevorzugten Standorte eine perfekte Übereinstimmung gefunden wird, kehrt das Gerät zu dem bevorzugten Standort mit der höchsten Priorität zurück und geht in der Prioritätsreihenfolge nach unten, bis eine teilweise Übereinstimmung zwischen einem bevorzugten Standort und dem Standort eines GSLB-Dienstes gefunden wird.

   Wenn eine teilweise Übereinstimmung gefunden wird, überprüft die Appliance, ob der entsprechende GSLB-Dienst aktiv ist. Wenn es aktiv ist, gibt es die IP-Adresse des GSLB-Dienstes in der DNS-Antwort zurück. Wenn mehrere teilweise Übereinstimmungen gefunden werden, überprüft die Appliance den Status jedes der entsprechenden GSLB-Dienste und gleicht den Lastausgleich der laufenden GSLB-Dienste aus.

3. Wenn keine der perfekten oder teilweisen Übereinstimmungen verfügbar sind, gleicht die Appliance alle anderen verfügbaren GSLB-Dienste aus.

   Auf diese Weise implementiert die Appliance eine Art von Site-Affinität für den Datenverkehr, die der DNS-Richtlinie entspricht.

Beispiel

Stellen Sie sich eine GSLB-Konfiguration vor, die aus den folgenden acht GSLB-Diensten besteht:

- Asien.in
- Asien.jpn
- Asia.hk
- Europe.uk
- Europe.ru
- Europa.eg
- Afrika.sd
- Afrika.ZMB

Beachten Sie außerdem die folgende DNS-Aktion und Richtlinienkonfiguration:

```
1 > add dns action prefLoc11 GslbPrefLoc -preferredLocList "Asia.HK" "
     Europe.UK"
2  Done
3 > add dns policy dnsPolPrefLoc "CLIENT.IP.SRC.MATCHES_LOCATION("\*.ZMB
     .\*.*")" prefLoc11
4  Done
5 <!--NeedCopy-->
```


Wenn die Appliance eine Anfrage vom Standort
.*ZMB*empfängt..*, die bevorzugten Standorte werden wie folgt bewertet:

1. Die Appliance versucht, einen GSLB-Dienst zu finden, dessen Standort perfekt zu Asia.hk passt, dem bevorzugten Standort mit der höchsten Priorität. Es stellt fest, dass der GSLB-Service bei Asia.hk perfekt passt. Wenn der GSLB-Dienst aktiv ist, sendet er dem Client die IP-Adresse des GSLB-Dienstes.
2. Wenn der GSLB-Dienst auf Asia.hk nicht verfügbar ist, versucht die Appliance, eine perfekte Lösung für den zweitbevorzugten Standort, Europe.uk, zu finden. Es stellt fest, dass der GSLB-Service bei Europe.uk perfekt zusammenpasst. Wenn der GSLB-Dienst aktiv ist, sendet er dem Client die IP-Adresse des Dienstes.
3. Wenn der GSLB-Dienst auf Europe.uk nicht verfügbar ist, kehrt er zum bevorzugten Standort mit der höchsten Priorität, Asia.hk, zurück und sucht nach Teilübereinstimmungen. Für Asia.hk wurde festgestellt, dass Asia.in und Asia.JPN teilweise übereinstimmen. Wenn nur einer der entsprechenden GSLB-Dienste aktiv ist, sendet er dem Client die IP-Adresse des Dienstes. Wenn beide Standorte verfügbar sind, erfolgt ein Lastenausgleich zwischen den beiden Diensten.
4. Wenn alle Teilübereinstimmungen für Asia.hk ausgefallen sind, sucht die Appliance nach Teilübereinstimmungen für Europe.uk. Es wurde festgestellt, dass Europe.ru und Europe.eg teilweise mit dem bevorzugten Standort übereinstimmen. Wenn nur einer der entsprechenden GSLB-Dienste aktiv ist, sendet er dem Client die IP-Adresse des Dienstes. Wenn beide Standorte verfügbar sind, erfolgt ein Lastenausgleich zwischen den beiden Diensten.
5. Wenn alle Teilspiele für Europe.uk ausgefallen sind, gleicht die Appliance alle anderen verfügbaren GSLB-Dienste aus. Im aktuellen Beispiel gleicht die Appliance-Lastverteilung Africa.sd und Africa.zmb aus, da die verbleibenden sechs GSLB-Dienste als ausgefallen wurden.

Konfigurieren der GSLB-Dienstauswahl über Content Switching

August 19, 2021

In einer typischen GSLB-Bereitstellung können Sie die Auswahl eines Satzes von GSLB-Diensten priorisieren, die an einen virtuellen GSLB-Server gebunden sind. Folgende Aktionen können jedoch nicht durchgeführt werden:

- Beschränken Sie die Auswahl eines GSLB-Dienstes aus einer Teilmenge von GSLB-Diensten, die an einen virtuellen GSLB-Server für die angegebene Domäne gebunden sind.
- Wenden Sie unterschiedliche Load Balancing-Methoden auf die verschiedenen Teilmengen von GSLB-Diensten in der Bereitstellung an.
- Wenden Sie Spillover-Richtlinien auf eine Teilmenge von GSLB-Diensten an, und Sie können kein Backup für eine Teilmenge von GSLB-Diensten haben.

- Konfigurieren Sie eine Teilmenge von GSLB-Diensten, um unterschiedliche Inhalte bereitzustellen. Das heißt, Sie können nicht zwischen Servern auf verschiedenen GSLB-Sites wechseln. Die GSLB-Konfiguration setzt voraus, dass die Server denselben Inhalt enthalten.
- Definieren Sie einen GSLB-Teilsatz mit unterschiedlichen Prioritäten und geben Sie eine Reihenfolge an, in der die Dienste in der Teilmenge auf eine Anforderung angewendet werden.

Sie können nun eine Content Switching-Richtlinie (CS) konfigurieren, um die GSLB-Bereitstellung anzupassen. Konfigurieren Sie zunächst einen Satz von GSLB-Diensten und binden Sie ihn an einen virtuellen GSLB-Server. Konfigurieren Sie dann einen virtuellen CS Server vom Zieltyp GSLB, definieren Sie eine CS-Richtlinie und -Aktion mit dem virtuellen GSLB-Server als virtuellen Zielserver und binden Sie die CS-Richtlinie an den virtuellen CS Server.

> **Wichtig**
>
> - Nur CS-Richtlinien mit DNS-basierten Ausdrücken können an einen virtuellen CS Server vom Zieltyp GSLB gebunden werden.
> - Wenn ein GLSB-Dienst über einen virtuellen GSLB-Server an einen virtuellen CS Server gebunden ist, können Sie keinen anderen virtuellen GSLB-Server binden, der mit demselben GSLB-Dienst an den virtuellen CS Server gebunden ist.

Beispiel
Betrachten Sie eine GLSB-Bereitstellung, die zwei GSLB-Sites enthält. An jedem Standort sind vier GSLB-Dienste (S-1, S-2, S-3 und S-4) an den virtuellen GSLB-Server VS-1 gebunden. Sie können einen virtuellen CS-Server (Content Switching) vom Zieltyp GSLB konfigurieren und eine CS-Richtlinie und -Aktion mit VS-1 als virtuellen Zielserver definieren, sodass Anfragen für Inhalte in Englisch nur von S-1 und S-2 bedient werden und Anforderungen für Inhalte in der lokalen Sprache nur von S-3 und S-4 bedient werden.

Sie können S-1 Priorität einräumen, indem Sie einen virtuellen Backupserver für VS-1 konfigurieren und S-2 an den virtuellen Backupserver binden. S-1 bedient die Client-Anfragen. Wenn der Server S-1 ausfällt, erfüllt S-2 die Anforderungen. Wenn sowohl S-1 als auch S-2 ausgefallen sind, erhalten Clients eine leere Antwort.

So konfigurieren Sie die GSLB-Dienstauswahl über Content Switching:

1. Konfigurieren Sie GSLB. Anweisungen finden Sie unter Konfigurieren des globalen Server-Lastenausgleichs.
2. Konfigurieren Sie einen virtuellen Content Switching-Server (CS) des Zieltyps GSLB. Weitere Informationen finden Sie unter Erstellen virtueller Server mit Content Switching.
3. Konfigurieren von Content Switching-Richtlinien (CS). Weitere Informationen finden Sie unter Content Switching-Richtlinien konfigurieren.
4. Konfigurieren Sie CS-Aktionen, die einen virtuellen GSLB-Server als virtuellen Zielserver festlegen. Weitere Informationen finden Sie unter Konfigurieren einer Content Switching-Aktion.
5. Binden Sie die CS-Richtlinien an den virtuellen CS Server. Weitere Informationen finden Sie

unter Binden von Richtlinien an einen virtuellen Content Switching-Server.

6. Binden Sie die Domäne an den virtuellen CS Server anstelle des virtuellen GSLB-Servers.

Beispielkonfiguration

Die folgende Beispielkonfiguration sendet Anforderungen vom Client mit der IP-Adresse 5.5.5.5 an SERVICE_GSLB1 und SERVICE_GSLB2. SERVICE_GSLB1 hat eine höhere Priorität als SERVICE_GSLB2, und SERVICE_GSLB2 bedient die Client-Anforderungen nur, wenn SERVICE_GSLB1 heruntergefahren ist. Wenn sowohl SERVICE_GSLB1 als auch SERVICE_GSLB2 ausgefallen sind, werden SERVICE_GSLB3 und SERVICE_GSLB4 nicht berücksichtigt, und eine leere Antwort wird an den Client gesendet.

```
add cs vs CSVSERVER_GSLB http  -targettype GSLB
Done
add gslb vs VSERVER_GSLB1 http
Done
add gslb vs VSERVER_GSLB2 http
Done
add gslb vs VSERVER_GSLB_BACKUP1 http
Done
set gslb vs VSERVER_GSLB1 -backupvserver VSERVER_GSLB_BACKUP1
Done
add gslb service SERVICE_GSLB1 1.1.1.1 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB2 1.1.1.2 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB3 1.1.1.3 HTTP 80 -sitename site2
Done
add gslb service SERVICE_GSLB4 1.1.1.4 HTTP 80 -sitename site2
Done
bind gslb vs VSERVER_GSLB1 -servicename SERVICE_GSLB1
Done
bind gslb vs VSERVER_GSLB_BACKUP1 -servicename SERVICE_GSLB2
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB3
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB4
Done
add cs action a1 -targetvserver VSERVER_GSLB1
Done
add cs policy p1 -rule "CLIENT.IP.SRC.EQ(5.5.5.5)" -action a1
Done
bind cs vs CSVSERVER_GSLB -domainName www.abc.com
Done
bind cs vs CSVSERVER_GSLB -policyname p1 -priority 1
```



```
Done
add cs action a2 -targetvserver VSERVER_GSLB2
Done
add cs policy p2 -rule "CLIENT.IP.SRC.EQ(6.6.6.6)" -action a2
Done
bind cs vs CSVSERVER_GSLB -policyname p2 -priority 2
Done
<!--NeedCopy-->
```

Zuordnen eines virtuellen Zielserverausdrucks zu einer GSLB-Content Switching-Aktion

Sie können nun einen virtuellen Zielserverausdruck einer GSLB-Content Switching-Aktion zuordnen. Dadurch kann der virtuelle GSLB-Content Switching-Server Richtlinienausdrücke verwenden, um den Namen des virtuellen GSLB Zielservers während der Verarbeitung der DNS-Anforderungen zu erstellen.

So konfigurieren Sie eine Content Switching-Aktion, die einen Ausdruck mit der CLI angibt

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Content Switching-Aktion so zu konfigurieren, dass die HTTP-Callout-Antwort abgerufen wird.

```
add cs action <name> -targetVserverExpr <expression>
<!--NeedCopy-->
```

Beispiel:

```
add cs action csact_GSLB_VServer -targetVserverExpr "SYS.HTTP_CALLOUT(
   GSLB_Method_API)"
<!--NeedCopy-->
```

So konfigurieren Sie eine Content Switching-Aktion, die einen Ausdruck mit der GUI angibt

1. Navigieren Sie zu **Traffic Management > Content Switching > Aktionen**.
2. Konfigurieren Sie eine Content Switching-Aktion, und geben Sie einen **Ausdruck** an, der den Namen des virtuellen Zielservers für den Lastenausgleich dynamisch berechnet.

Konfigurieren von GSLB für DNS-Abfragen mit NAPTR-Datensätzen

May 11, 2023

In einer typischen GSLB-Bereitstellung (Global Server Load Balancing) empfängt die NetScaler-Appliance DNS-Abfragen für A/AAAA-Einträge, wählt den am besten geeigneten GSLB-Dienst gemäß der konfigurierten Load-Balancing-Methode aus und gibt die IP-Adresse des Dienstes als Antwort auf die DNS-Anfrage zurück. Sie können die Appliance jetzt so konfigurieren, dass sie DNS-Abfragen für NAPTR-Einträge empfängt und mit der Liste der für eine Domäne konfigurierten Dienste antwortet. Die Appliance überwacht auch den Zustand der Dienste und stellt in der Antwort nur eine Liste der Dienste bereit, die aktiv sind.

Beispiel:

In Telco-Bereitstellungen können Sie eine NetScaler-Appliance so konfigurieren, dass sie DNS-Abfragen mit NAPTR-Einträgen von Clients wie Mobile Management Entities (MMEs) empfängt, die die Rolle eines DNS-Resolvers spielen, um alle Dienste zu ermitteln, die vom Domainnamen angeboten werden. Die Appliance beantwortet die Anfrage mit NAPTR-Datensätzen für alle verfügbaren Dienste. Die MME kann diese NAPTR-Antwort verwenden, um das S-NAPTR-Verfahren auszuführen, um die Knoten auf der Grundlage des angebotenen Dienstes, der Colocation, der topologischen Nähe usw. auszuwählen.

Wenn mehrere Knoten für die Auswahl in Frage kommen, kann die MME das Präferenzfeld im NAPTR-Datensatz der NetScaler-Appliance verwenden, um den Knoten zu bestimmen.

NAPTR-Datensatzformat

Während eine NetScaler-Appliance auf eine DNS-Anfrage mit einem NAPTR-Eintrag antwortet, erstellt sie für jeden GSLB-Dienst einen NAPTR-Antwortdatensatz.

In der folgenden Tabelle sind die Dateien im NAPTR-Datensatz aufgeführt:

Feld	
Domäne	Die GSLB-Domain
TTL	Die Zeit, für die der NAPTR-Datensatz zwischengespeichert werden kann.
Klasse	Die Klasse des Rekords. In der Standardeinstellung ist dieser Wert auf IN gesetzt.
Typ	Der DNS-Eintragstyp.
Bestellung	Gibt die Reihenfolge an, in der der NAPTR-Datensatz verarbeitet werden MUSS. Sie können die Reihenfolge im GSLB-Service angeben. Andernfalls ist es auf 1 gesetzt.

Feld	
Präferenz	Gibt die Reihenfolge an, in der NAPTR-Datensätze mit gleichen „Ordnungswerten“ verarbeitet werden SOLLEN, wobei niedrige Zahlen vor hohen Zahlen verarbeitet werden sollen. Wenn die Bestellung nicht im GSLB-Service angegeben ist, wird sie auf 1 gesetzt.
Flags	Steuert die Aspekte des Umschreibens und der Interpretation der Felder im Datensatz. Die NetScaler-Appliance legt diesen Wert auf A fest.
Service	Gibt die verfügbaren Dienste an.
Regulärer Ausdruck	Reguläre Ausdrücke werden nicht unterstützt, daher ist dieser Wert auf NULL gesetzt.
Ersatz	Der Domainname des Knotens, der die Dienste hostet.

Konfigurationsprozedur

Ausführliche Anweisungen zur GSLB-Konfiguration finden Sie unter Konfigurieren des globalen Server-Lastenausgleichs (GSLB). Stellen Sie sicher, dass Sie Folgendes tun:

- Stellen Sie beim Hinzufügen des virtuellen GSLB-Servers die folgenden Parameter ein:
  - Diensttyp: BELIEBIG
  - DNS-Datensatztyp: NAPTR
  - LB-Methode: CUSTOMLOAD

Beispiel:

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD
<!--NeedCopy-->
```

- Stellen Sie beim Hinzufügen einer GSLB-Site den Parameter *NaptrReplacementSuffix* auf den Domainnamen ein, den Sie in die NAPTR-Datensätze einbetten möchten.

Beispiel:

```
add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com
<!--NeedCopy-->
```


- Stellen Sie beim Hinzufügen des GSLB-Dienstes die folgenden Parameter ein:
  - Naptr-Ersatz
  - NAPTR-Bestellung
  - NAPTR-Dienste
  - Naptr-Domäne TTL
  - Naptr-Präferenz

Beispiel-Konfiguration

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD

Done

add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com

Done

add gslb service sgw1 3.3.3.13 ANY *  -siteName site1 -naptrreplacement
    sgw1.site1. -naptrOrder 2 -naptrServices x-3gpp-sgw:x-s5-gtp -
   naptrDomainTTL 20 -naptrPreference   200

Done

add gslb service sgw2 3.3.3.11 ANY *  -siteName site1 -naptrreplacement
    sgw2.site1. -naptrOrder 5 -naptrServices x-3gpp-sgw:x-s5-gtp  -
   naptrDomainTTL 20  naptrPreference  100

Done

add gslb service sgw3 3.3.3.12 ANY *  -siteName site2 -naptrreplacement
    sgw3.site1. -naptrOrder 10 -naptrServices x-3gpp-sgw:x-s5-gtp  -
   naptrDomainTTL 20 naptrPreference   300

bind gslb vserver gslb_vs -serviceName sgw1

Done

bind gslb vserver gslb_vs -serviceName sgw2

Done

bind gslb vserver gslb_vs -serviceName sgw3

```



```
Done

bind gslb service sgw1 -monitorName ping

Done

bind gslb service sgw2 -monitorName ping

Done

bind gslb service sgw3 -monitorName ping

Done

bind gslb vserver gslb_vs -domainName gslb.com -TTL 5

Done
<!--NeedCopy-->
```

> **Hinweis**
>
> DNS-Abfragen mit NAPTR-Einträgen werden in der übergeordneten und untergeordneten Konfiguration nicht unterstützt.

Konfigurieren von GSLB für Platzhalter-Domäne

July 8, 2022

Sie können eine Platzhalter-DNS-Domäne an einen virtuellen GSLB-Server binden. Benutzer, die auf die Anwendungen hinter einer Wildcard-Domäne zugreifen, werden an das optimale Rechenzentrum weitergeleitet, das diese Anwendungen hostet. Die Platzhalterdomäne verarbeitet Anforderungen für nicht vorhandene Domänen und Unterdomänen. Weitere Informationen zu Platzhalter-Domänen finden Sie unter Unterstützen von Platzhalter-DNS-Domänen. Weitere Informationen zu DNS-Zonen finden Sie unter Konfigurieren einer DNS-Zone.

Um GSLB für eine Platzhalterdomäne zu konfigurieren, müssen Sie zunächst das grundlegende GSLB-Setup konfigurieren. Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

So konfigurieren Sie ein GSLB-Setup für Platzhalterdomäne mit der CLI

Führen Sie die folgenden Schritte aus, um ein GSLB-Setup für eine Wildcard-Domain

1. Erstellen Sie die GSLB-Sites.

```
add gslb site site1 10.0.1.10
add gslb site site2 20.0.1.10
<!--NeedCopy-->
```

2. Fügen Sie die GSLB-Dienste für jede am GSLB-Setup beteiligte Site hinzu.

```
add gslb service svc1 -sitename site1 10.0.1.10  http 80
add gslb service svc2 -sitename site1 10.0.1.10  http 80
add gslb service svc3 -sitename site2 20.0.1.10  http 80
add gslb service svc4 -sitename site2 20.0.1.10  http 80
<!--NeedCopy-->
```

3. Fügen Sie den virtuellen GSLB-Server hinzu, der auf einen im GSLB-Setup verwendeten Dienst verweist.

```
add gslb vserver gslb_vs http
<!--NeedCopy-->
```

4. Fügen Sie einen ADNS-Dienst hinzu, der die DNS-Abfragen überwacht.

```
add service adns_udp 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

5. Binden Sie die GSLB-Dienste an den virtuellen GSLB-Server.

```
bind gslb vserver gslb_vs -service svc1
bind gslb vserver gslb_vs -service svc2
bind gslb vserver gslb_vs -service svc3
bind gslb vserver gslb_vs -service svc4
<!--NeedCopy-->
```

6. Erstellen Sie eine Zone.

```
add dns soaRec test.com -originServer n1.test.com -contact n1.test
    .com
add dns nsrec test.com n1.test.com
add dns nsrec test.com n2.test.com
add dns zone test.com -proxymode no
<!--NeedCopy-->
```

7. Binden Sie den Domänennamen an den virtuellen GSLB-Server.

```
bind gslb vserver gslb_vs -domainName *.test.com
<!--NeedCopy-->
```


Verwenden Sie die EDNS0-Clientsubnetzoption für Global Server Load Balancing

May 11, 2023

EDNS Client Subnet (ECS) ist eine DNS-Header-Erweiterung (Domain Name Server), die die Details des Client-Subnetzes bereitstellt. Sie können diese Details verwenden, um die Genauigkeit von NetScaler Global Server Load Balancing (GSLB) zu verbessern, indem Sie den Netzwerkstandort des Clients und nicht den Standort des DNS-Resolvers verwenden, um die topologische Nähe des Clients zu bestimmen.

> **Hinweis**
>
> NetScaler unterstützt nur EDNS0.

Wichtig:

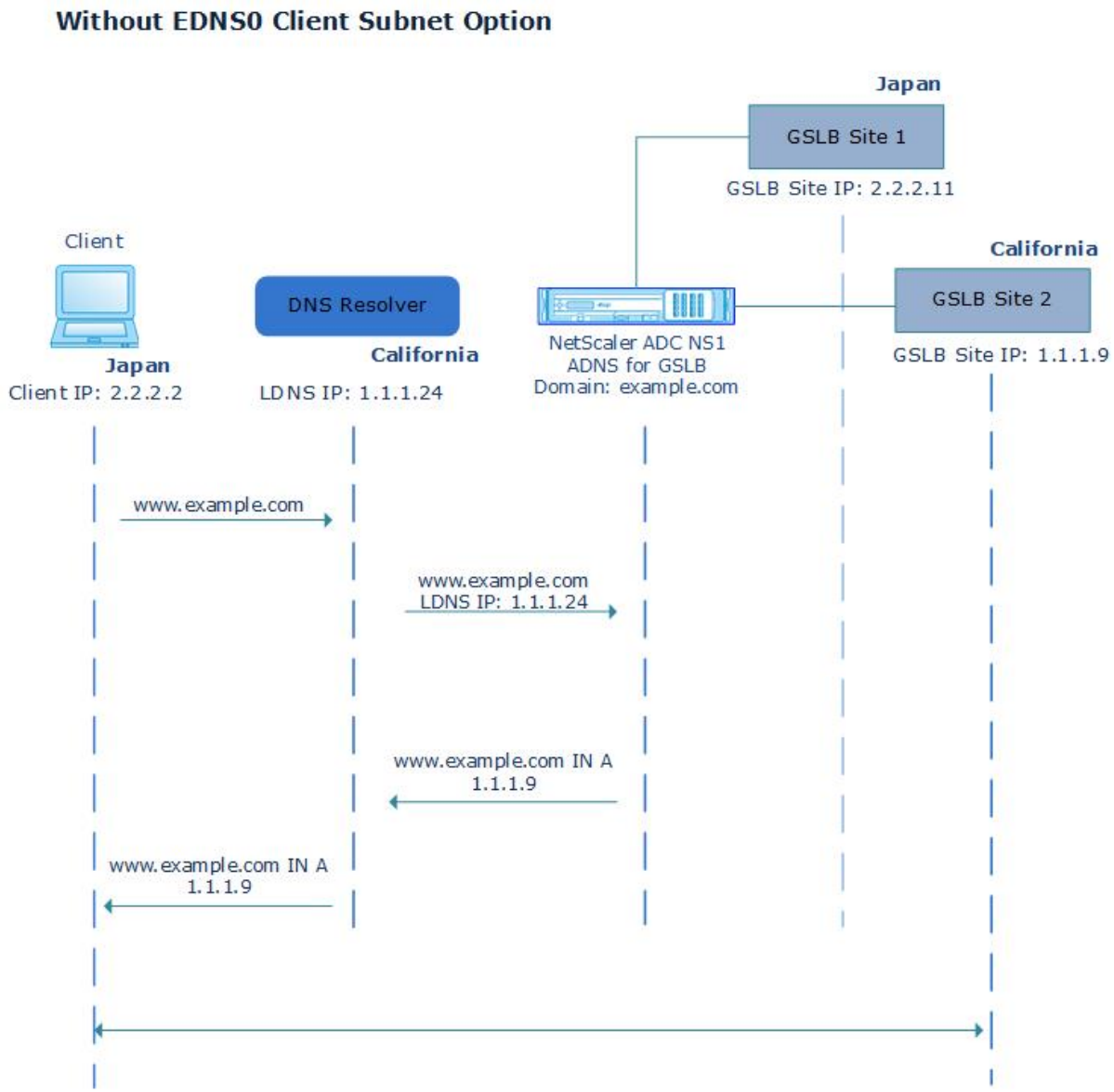
> Stellen Sie sicher, dass der Local Domain Name Server (LDNS) in Ihrer Bereitstellung das EDNS0-Clientsubnetz unterstützt, sodass die eingehenden DNS-Abfragen die EDNS0-Clientsubnetzoption enthalten und die NetScaler-Appliance bei der Verarbeitung der DNS-Anfrage die ECS-Adresse verwendet.

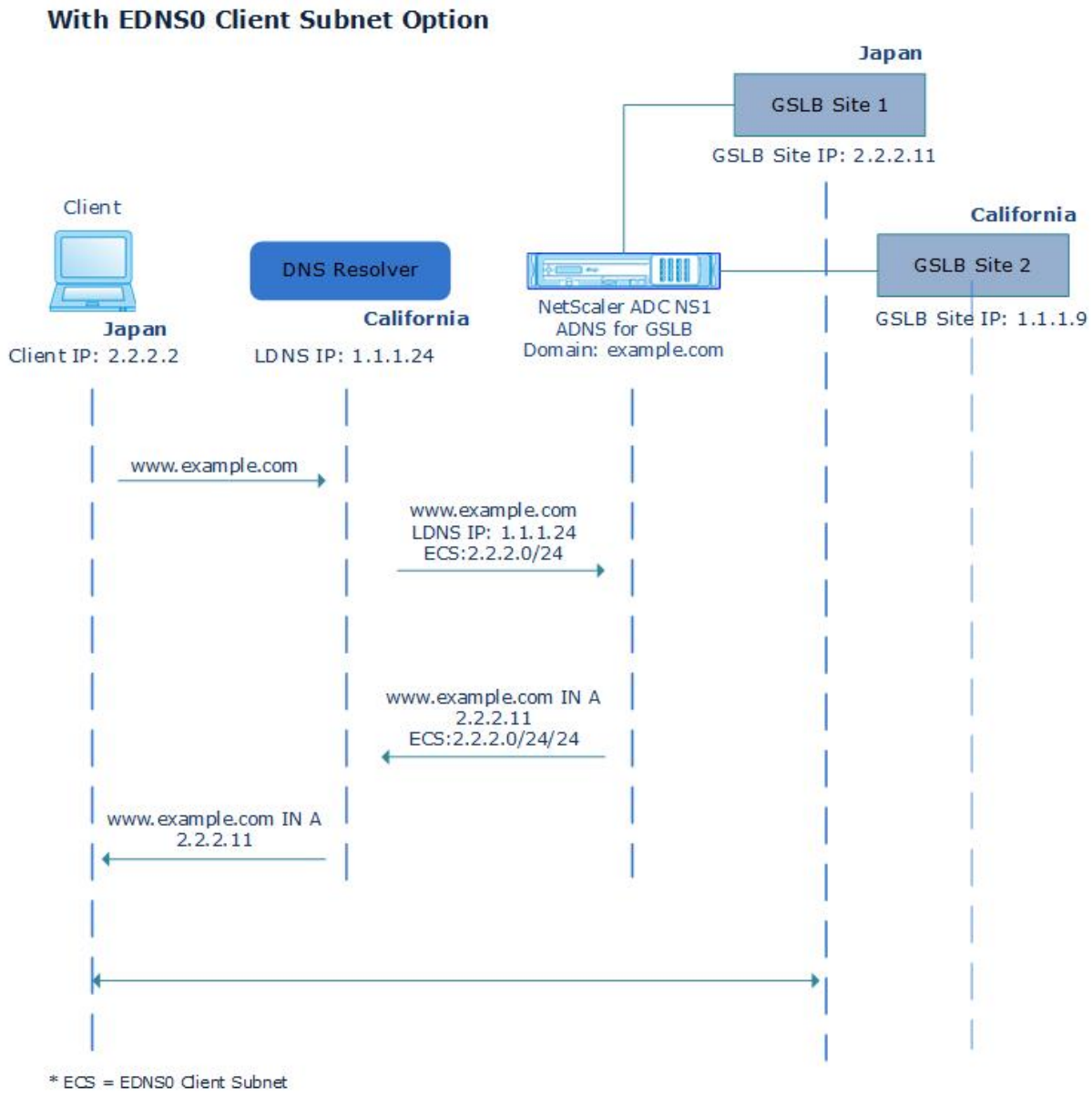
Die NetScaler-Appliance verwendet die LDNS-IP-Adresse zur Bestimmung der topologischen Nähe des Clients und führt GSLB aus, wenn Sie proximitätsbasierte Lastausgleichsmethoden wie statische Nähe oder dynamische Round-Trip-Time (RTT) verwenden. Dies passiert in einer typischen GSLB-Bereitstellung. Wenn jedoch ein zentraler DNS-Resolver wie Google DNS oder OpenDNS an der Bereitstellung beteiligt ist, sendet die NetScaler-Appliance die DNS-Anfrage an ein Rechenzentrum in der Nähe des zentralen DNS-Resolvers, das sich möglicherweise nicht in der Nähe des Clients befindet. In einer typischen NetScaler-GSLB-Bereitstellung, bei der die statische Proximity-Load-Balancing-Methode verwendet wird, wird beispielsweise eine Endbenutzeranfrage aus Japan an ein Rechenzentrum in Japan und eine Endbenutzeranfrage aus Kalifornien an ein Rechenzentrum in Kalifornien gesendet. Wenn jedoch ein zentraler DNS-Resolver beteiligt ist, sendet die NetScaler-Appliance möglicherweise eine Anfrage von Japan an ein Rechenzentrum in Kalifornien.

Sie können die ECS-Option in Bereitstellungen verwenden, in denen die NetScaler-Appliance als Authoritative DNS (ADNS) -Server für eine GSLB-Domäne konfiguriert ist. Wenn Sie statische Nähe als Lastausgleichsmethode verwenden, können Sie das IP-Subnetz im EDNS-Header anstelle der LDNS-IP-Adresse verwenden. Dies hilft, die geografische Nähe des Kunden zu bestimmen. Bei der Bereitstellung im Proxymodus leitet die NetScaler-Appliance eine ECS-fähige DNS-Abfrage unverändert an die Backend-Server weiter. Die Appliance speichert keine ECS-fähigen DNS-Antworten.

> **Hinweis**

> Die ECS-Option gilt nicht für alle anderen Bereitstellungsmodi, wie z. B. den ADNS-Modus für Nicht-GSLB-Domänen, den Resolver-Modus und den Forwarder-Modus. Die ECS-Option wird von der NetScaler-Appliance in den oben genannten Modi ignoriert. Außerdem ist ECS standardmäßig für die GSLB-Bereitstellung deaktiviert.





Gehen Sie wie folgt vor, um die EDNS0-Client-Subnetzoption mithilfe der Befehlszeilenschnittstelle zu aktivieren:

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver <vserver_name> **-ECS ENABLED

set gslb vserver vserver-GSLB-1 -ECS ENABLED
<!--NeedCopy-->
```


Adressvalidierung

Sie können einen virtuellen GSLB-Server konfigurieren, um zu überprüfen, ob die von der EDNS0-Client-Subnetzoption (ECS) der DNS-Abfrage zurückgegebene Adresse keine private oder nicht routbare IP-Adresse ist. Wenn die Adressüberprüfung aktiviert ist, ignoriert die NetScaler-Appliance die ECS-Adresse in der DNS-Abfrage, sofern sie in der folgenden Tabelle aufgeführt ist, und verwendet stattdessen die LDNS-IP-Adresse für den globalen Serverlastenausgleich.

> **Hinweis**
>
> Standardmäßig ist die Adressüberprüfung deaktiviert.

Art der Adresse	Adresse	Beschreibung
IPV4	10.0.0.0/8	Für den privaten Gebrauch
	172.16.0.0/12	Für den privaten Gebrauch
	192.168.0.0/16	Für den privaten Gebrauch
	0.0.0.0/8	Bezieht sich auf den Host im Netzwerk
	100.64.0.0/10	Gemeinsamer Adressraum
	127.0.0.0/8	Loopback-Adresse
	169.254.0.0/16	Link Lokale IPv4-Adresse, wie in RFC 3927 definiert
	192.0.0.0/24	Wird für IETF-Protokollzuweisungen verwendet, beinhaltet den privaten Bereich 192.168.0.0/16
	192.0.2.0/24	Wird zu Dokumentationszwecken verwendet
	192.88.99.0/24	Wird für 6to4 Relay Anycast verwendet
	198.18.0.0/15	Wird bei Geräte-Benchmark-Tests verwendet
	198.51.100.0/24	Wird zu Dokumentationszwecken verwendet

Art der Adresse	Adresse	Beschreibung
	203.0.113.0/24	Wird zu Dokumentationszwecken verwendet
	240.0.0.0/4	Wird als reserviert verwendet
	255.255.255.255/32	Wird für die Übertragung verwendet
IPv6	::1/128	Loopback-Adresse
	::/128	nicht spezifizierte Adresse
	::ffff:0:0/96	IPv4-zugeordnete Adresse
	100::/64	Adressblock nur verwerfen
	2001::/23	Wird für IETF-Protokollzuweisungen verwendet
	2001::/32	TEREDO
	2001:2::/48	Wird für Benchmarking verwendet
	2001:db8::/32	Wird zu Dokumentationszwecken verwendet
	2001:10::/28	ORCHIDEE
	2002::/16	Wird für 6to4 Relay Anycast verwendet
	fc00::/7	Einzigartig — lokal
	fe80::/10	Lokale Unicast-Adressen verknüpfen

So aktivieren Sie die Adressüberprüfung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set gslb vserver <vserver_name> -ecsAddrValidation ENABLED

set gslb vserver vserver-GSLB-1 -ecsAddrValidation ENABLED
```



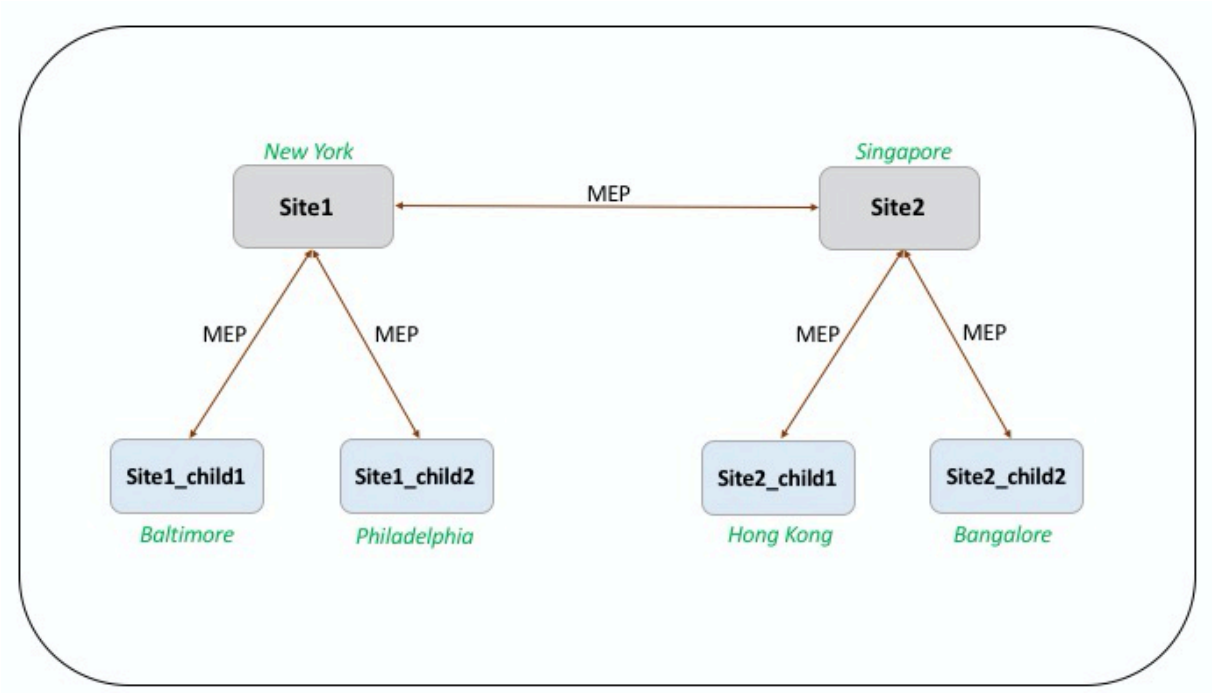
```
<!--NeedCopy-->
```

Beispiel für eine vollständige Parent-Child-Konfiguration mit dem Metrics Exchange Protocol

August 19, 2021

Betrachten Sie die folgende übergeordnete und untergeordnete Topologie, in der die GSLB-Sites global verteilt sind.

- Site1 und Site2 sind die übergeordneten Sites.
- Site1_Child1 und Site1_Child2 sind die untergeordneten Sites von Site1.
- Site2_Child1 und Site2_Child2 sind die untergeordneten Sites von Site2.



Die folgenden Befehle veranschaulichen die vollständige Konfiguration der über-/untergeordneten Topologie.

site1

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site2 10.106.24.164 -publicIP 10.106.24.164

```



```
add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
    publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
    site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
     10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
    publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
    site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
     10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
    appflowLog DISABLED

bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1

bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1

bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1

bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1

bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
<!--NeedCopy-->
```


site1_child1

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1
<!--NeedCopy-->
```

Sie können die folgenden Befehle für die Konfiguration des Lastenausgleichs hinzufügen:

```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.132 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site1_child2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

You can add the following commands for load balancing configuration:

add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.68 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```


site2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site2 10.106.24.164 -publicIP 10.106.24.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
    publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
    site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
     10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
    publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
    site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
     10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
    appflowLog DISABLED

bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1

bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1

```



```
bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1

bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1

bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
<!--NeedCopy-->
```

site2_child1

```
add gslb site site2 10.106.24.164 -publicIP 10.106.24.164

add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2
<!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.106.24.134 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site2_child2

```
add gslb site site2 10.106.24.164 -publicIP 10.106.24.164

add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2
<!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO
```



```
2
3 add lb vserver lb1 HTTP 10.106.24.68 80 -persistenceType NONE -
     cltTimeout 180
4
5 bind lb vserver lb1 svc1
6 \`\`\`
7 <!--NeedCopy-->
```

Link-Lastenausgleich

May 11, 2023

Link Load Balancing (LLB) gleicht den ausgehenden Verkehr über mehrere Internetverbindungen aus, die von verschiedenen Dienstanbietern bereitgestellt werden. LLB ermöglicht es der NetScaler-Appliance, den Datenverkehr zu überwachen und zu steuern, sodass Pakete nahtlos über die bestmögliche Verbindung übertragen werden. Anders als beim Server-Load-Balancing, wo ein Service einen Server darstellt, steht bei LLB ein Service für einen Router oder den nächsten Hop. Ein Link ist eine Verbindung zwischen der NetScaler-Appliance und dem Router.

Um den Link-Load-Balancing zu konfigurieren, konfigurieren viele Benutzer zunächst ein Basis-Setup mit Standardeinstellungen. Ein grundlegendes Setup umfasst Dienste, virtuelle Server, Monitore, Routen, eine LLB-Methode und Persistenz (optional). Sobald ein Basis-Setup betriebsbereit ist, können Sie es an Ihre Umgebung anpassen.

Load-Balancing-Methoden, die auf LLB anwendbar sind, sind Round-Robin-Verfahren, Ziel-IP-Hash, geringste Bandbreite und geringste Pakete. Sie können optional die Persistenz für Verbindungen konfigurieren, die auf einem bestimmten Link aufrechterhalten werden. Die verfügbaren Persistenztypen basieren auf der Quell-IP-Adresse, auf der Ziel-IP-Adresse und auf der Quell- und Ziel-IP-Adresse. PING ist der Standardmonitor, es wird jedoch empfohlen, einen transparenten Monitor zu konfigurieren.

Sie können Ihre Einrichtung anpassen, indem Sie Reverse NAT (RNAT) und Backup-Links konfigurieren.

Konfigurieren eines Basic LLB-Setups

May 11, 2023

Um LLB zu konfigurieren, erstellen Sie zunächst Dienste, die jeden Router für die Internet Service Provider (ISPs) repräsentieren. Ein PING-Monitor ist standardmäßig an jeden Dienst gebunden. Das Anbinden eines transparenten Monitors ist optional, wird aber empfohlen. Anschließend erstellen

Sie einen virtuellen Server, binden die Dienste an den virtuellen Server und konfigurieren eine Route für den virtuellen Server. Die Route identifiziert den virtuellen Server als Gateway zu den physischen Routern, die durch die Dienste repräsentiert werden. Der virtuelle Server wählt einen Router mithilfe der von Ihnen angegebenen Load-Balancing-Methode aus. Optional können Sie die Persistenz konfigurieren, um sicherzustellen, dass der gesamte Datenverkehr für eine bestimmte Sitzung über einen bestimmten Link gesendet wird.

Gehen Sie wie folgt vor, um ein grundlegendes LLB-Setup zu konfigurieren:

- Konfigurieren von Diensten
- Einen virtuellen LLB-Server konfigurieren und einen Dienst binden
- Konfiguration der LLB-Methode und Persistenz
- Eine LLB-Route konfigurieren
- Erstellen und binden Sie einen transparenten Monitor

Konfigurieren von Diensten

Ein Standardmonitor (PING) wird beim Erstellen des Dienstes automatisch an einen Servicetyp von ANY gebunden, Sie können jedoch den Standardmonitor durch einen transparenten Monitor ersetzen, wie unter Erstellen und Binden eines transparenten Monitorsbeschrieben.

So erstellen Sie einen Dienst mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <IP> <serviceType> <port>

show service <name>
<!--NeedCopy-->
```

Beispiel:

```
add service ISP1R_svc_any 10.10.10.254 any *
show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: DOWN
        Last state change was at Tue Aug 31 04:31:13 2010
        Time since last state change: 2 days, 05:34:18.600
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
```



```
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 244705  Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

So erstellen Sie Dienste mithilfe des Konfigurationsprogramms

Navigieren Sie zu Traffic Management > Load Balancing > Servicesund erstellen Sie einen Dienst.

So erstellen Sie Dienste mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an:
   - Dienstname* — Name
   - Server—IP
   - protocol* — ServiceType (Wählen Sie ANY aus der Dropdownliste aus.)
   - Hafen* — Port

Ein erforderlicher Parameter

1. Klicken Sie auf Erstellen.
2. Wiederholen Sie die Schritte 2-4, um einen weiteren Dienst zu erstellen.
3. Klicken Sie auf Schließen.
4. Wählen Sie im Bereich Dienste die Dienste aus, die Sie gerade konfiguriert haben, und überprüfen Sie, ob die unten auf dem Bildschirm angezeigten Einstellungen korrekt sind.

Einen virtuellen LLB-Server konfigurieren und einen Dienst binden

Nachdem Sie einen Dienst erstellt haben, erstellen Sie einen virtuellen Server und binden Sie Dienste an den virtuellen Server. Die standardmäßige LB-Methode der geringsten Verbindungen wird in LLB nicht unterstützt. Informationen zum Ändern der LB-Methode finden Sie unter Konfigurieren der LLB-Methode und Persistenz.

So erstellen Sie einen virtuellen Link-Lastausgleichsserver und binden einen Dienst mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <serviceType>

bind lb vserver < name> <serviceName>

show lb vserver < name>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver LLB-vip any
bind lb vserver LLB-vip ISP1R_svc_any
sh lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Thu Sep  2 10:51:32 2010
        Time since last state change: 0 days, 17:51:46.770
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
        Persistence: NONE
        Connection Failover: DISABLED

1) ISP1R_svc_any (10.10.10.254: *) - ANY State: DOWN    Weight: 1
 Done
<!--NeedCopy-->
```


Um einen virtuellen Link-Load-Balancing-Server zu erstellen und einen Dienst mithilfe des Konfigurationsprogramms zu binden

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und erstellen Sie einen virtuellen Server für den Link-Lastenausgleich. Geben Sie **ANY** im Feld **Protokoll** an.
2. Wählen Sie in der Dropdownliste **IP-Adresstyp** die gewünschte Option aus. Wählen Sie **Nicht adressierbar** aus, um einen virtuellen Server zu erstellen, auf den nicht direkt zugegriffen werden kann.
3. Aktivieren Sie auf der Registerkarte **Dienste** in der Spalte **Aktiv** das Kontrollkästchen für den Dienst, den Sie an den virtuellen Server binden möchten.

Konfiguration der LLB-Methode und Persistenz

Standardmäßig verwendet die NetScaler-Appliance die Methode mit den wenigsten Verbindungen, um den Dienst für die Umleitung jeder Client-Anfrage auszuwählen. Sie sollten die LLB-Methode jedoch auf eine der unterstützten Methoden festlegen. Sie können auch die Persistenz konfigurieren, sodass verschiedene Übertragungen von demselben Client an denselben Server weitergeleitet werden.

Um die LLB-Methode und/oder Persistenz mithilfe der Befehlszeilenschnittstelle zu konfigurieren

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set lb vserver <name> -lbMethod <lbMethod> -persistenceType <
   persistenceType>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver LLB-vip -lbmethod ROUNDROBIN -persistencetype SOURCEIP

show lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 00:52:21.200
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
```



```
12          No. of Bound Services :  0 (Total)       0 (Active)
13          Configured Method: ROUNDROBIN
14          Mode: IP
15          Persistence: SOURCEIP
16       Persistence Mask: 255.255.255.255       Persistence v6MaskLength:
             128   Persistence Timeout: 2 min
17          Connection Failover: DISABLED
18 <!--NeedCopy-->
```

So konfigurieren Sie die Link-Load-Balancing-Methode und/oder die Persistenz mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server und wählen Sie den virtuellen Server aus, für den Sie die Load-Balancing-Methode und/oder die Persistenzeinstellungen konfigurieren möchten.
2. Wählen Sie im Abschnitt **Erweiterte Einstellungen** die Option Methode aus und konfigurieren Sie die Load-Balancing-Methode.
3. Wählen Sie im Abschnitt **Erweiterte Einstellungen** die Option **Persistenz** aus und konfigurieren Sie die Persistenzparameter.

Eine LLB-Route konfigurieren

Nachdem Sie die IPv4- oder IPv6-Dienste, virtuellen Server, LLB-Methoden und Persistenz konfiguriert haben, konfigurieren Sie eine IPv4- oder IPv6-LLB-Route für das Netzwerk, wobei Sie den virtuellen LLB-Server als Gateway angeben. Eine Route ist eine Sammlung von Links, die über einen Lastenausgleich verfügen. Anfragen werden an die IP-Adresse des virtuellen LLB-Servers gesendet, die als Gateway für den gesamten ausgehenden Verkehr fungiert und den Router anhand der konfigurierten LLB-Methode auswählt.

So konfigurieren Sie eine IPv4-LLB-Route mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lb route <network> <netmask> <gatewayName>
2
3 show lb route [<network> <netmask>]
4 <!--NeedCopy-->
```

Beispiel:

```
1 add lb route 0.0.0.0 0.0.0.0 LLB-vip
2 show lb route 0.0.0.0 0.0.0.0
```



```
3         Network          Netmask        Gateway/VIP              Flags
4       -----------      -------------   --------------           --------
5 1)      0.0.0.0          0.0.0.0        LLB-vip                UP
6 <!--NeedCopy-->
```

So konfigurieren Sie eine IPv6-LLB-Route mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lb route6 <network> <gatewayName>
2
3 show lb route6
4 <!--NeedCopy-->
```

Beispiel:

```
1 add lb route6 ::/0 llb6_vs show lb route6 Network VIP Flags -----------
      --------- -------- 1) ::/0 llb6_vs UP
2 <!--NeedCopy-->
```

So konfigurieren Sie eine LLB-Route mithilfe des Konfigurationsprogramms

Navigieren Sie zu System > Netzwerk > Routen, wählen Sie **LLB**aus und konfigurieren Sie die LLB-Route.

Hinweis: Wählen Sie LLBV6, um eine IPV6-Route zu konfigurieren.

So konfigurieren Sie eine LLB-Route mithilfe des Konfigurationsprogramms

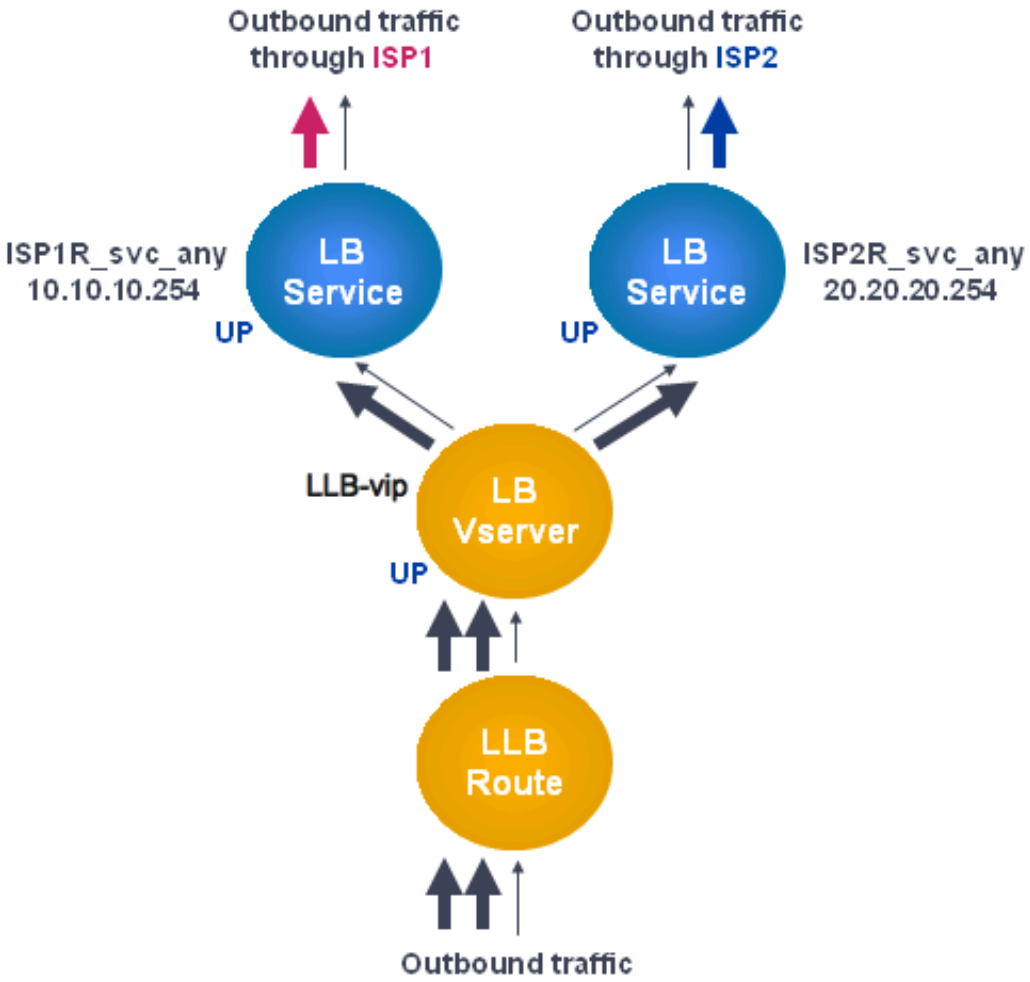
1. Navigieren Sie zu System > Netzwerk > Routen.
2. Wählen Sie im Detailbereich eine der folgenden Optionen aus:
   - Klicken Sie auf LLB, um eine IPv4-Route zu konfigurieren.
   - Klicken Sie auf LLBV6, um eine IPv4-Route zu konfigurieren.
3. Stellen Sie im Dialogfeld LB-Route erstellen oder LB-IPV6-Route erstellen die folgenden Parameter ein:
   - Netzwerk*
   - Netmask* — Erforderlich für IPV4-Routen.
   - Gatewayname* — Gatewayname

     * Ein erforderlicher Parameter

4. Klicken Sie auf Erstellenund dann auf Schließen. Die Route, die Sie gerade erstellt haben, wird auf der Registerkarte LLB oder LLB6 im Bereich Routen angezeigt.

Das folgende Diagramm zeigt eine grundlegende LLB-Einrichtung. Für jeden der beiden Links (ISPs) ist ein Dienst konfiguriert, und PING-Monitore sind standardmäßig an diese Dienste gebunden. Basierend auf der konfigurierten LLB-Methode wird ein Link ausgewählt.

Abbildung 1. Grundlegende LLB-Setup



Hinweis

Wenn Ihr Internetdienstanbieter eine IPv6-Adresse bereitgestellt hat, ersetzen Sie den IPv4-Dienst in der obigen Abbildung durch einen IPv6-Dienst.

Erstellen und binden Sie einen transparenten Monitor

Sie erstellen einen transparenten Monitor, um den Zustand von Upstream-Geräten wie Routern zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht die Konnektivität nur zwischen der NetScaler-Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, das die im Monitor angegebene Ziel-IP-Adresse besitzt. Wenn kein transparenter Monitor konfiguriert ist und der Status des Routers AKTIV ist, aber eines der nächsten Hop-Geräte dieses Routers ausgefallen ist, bezieht die Appliance den Router mit ein, führt den Lastenausgleich durch und leitet das Paket an den Router weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der Geräte für den nächsten Hop ausgefallen ist. Wenn eines der Geräte (einschließlich des Routers) ausgefallen ist, wird der Dienst als DOWN markiert und der Router wird nicht einbezogen, wenn die Appliance den Link-Load-Balancing durchführt.

So erstellen Sie einen transparenten Monitor mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> <type> -destIP <ip_addr|*> -transparent
   YES

show lb monitor [<monitorName>]
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor monitor-1 PING -destIP 10.10.10.11 -transparent YES
> show lb monitor monitor-1
1)   Name.......: monitor-1  Type......:      PING   State....:
   ENABLED
Standard parameters:
  Interval.........:           5 sec   Retries...........:
                    3
  Response timeout.:           2 sec   Down time.........:
     30 sec
  Reverse..........:              NO   Transparent.......:
                  YES
  Secure...........:              NO   LRTM..............:
     ENABLED
  Action...........:   Not applicable   Deviation.........:
     0 sec
  Destination IP...:      10.10.10.11
  Destination port.:    Bound service
  Iptunnel.........:              NO
```



```
13   TOS..............:                NO   TOS ID............:
                        0
14   SNMP Alert Retries:                0     Success Retries..:
                        1
15   Failure Retries..:                 0
16 <!--NeedCopy-->
```

So erstellen Sie einen transparenten Monitor mithilfe des Konfigurationsprogramms

Navigieren Sie zu Traffic Management > Load Balancing > Monitore und konfigurieren Sie einen transparenten Monitor.

So erstellen Sie einen transparenten Monitor mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.
2. Klicken Sie im Bereich Monitore auf Hinzufügen.
3. Stellen Sie im Dialogfeld „Monitor erstellen“ die folgenden Parameter ein:
   - Vorname*
   - Typ*
   - Ziel-IP
   - Transparente

     * Ein erforderlicher Parameter
4. Klicken Sie auf Erstellenund dann auf Schließen.
5. Wählen Sie im Bereich Monitore den Monitor aus, den Sie gerade konfiguriert haben, und überprüfen Sie, ob die im Detailbereich angezeigten Einstellungen korrekt sind.

So binden Sie einen Monitor mithilfe des Konfigurationsdienstprogramms an einen Dienst

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Wählen Sie auf der Registerkarte **Monitore** unter **Verfügbar**den Monitor aus, den Sie an den Dienst binden möchten, und klicken Sie dann auf **Hinzufügen**.

So binden Sie einen Monitor mithilfe der Befehlszeilenschnittstelle an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:


```
bind lb monitor <monitorName> <serviceName>

show service <name>
<!--NeedCopy-->
```

Beispiel:

```
bind lb monitor monitor-HTTP-1 ISP1R_svc_any
 Done
> show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: UP
        Last state change was at Thu Sep  2 10:51:07 2010
        Time since last state change: 0 days, 18:41:55.130
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: UP  Weight: 1
                Probes: 1256       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

So binden Sie einen Monitor mithilfe des Konfigurationsdienstprogramms an einen Dienst

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Wählen Sie im Detailbereich einen Dienst aus, an den Sie einen Monitor binden möchten, und klicken Sie dann auf Öffnen.

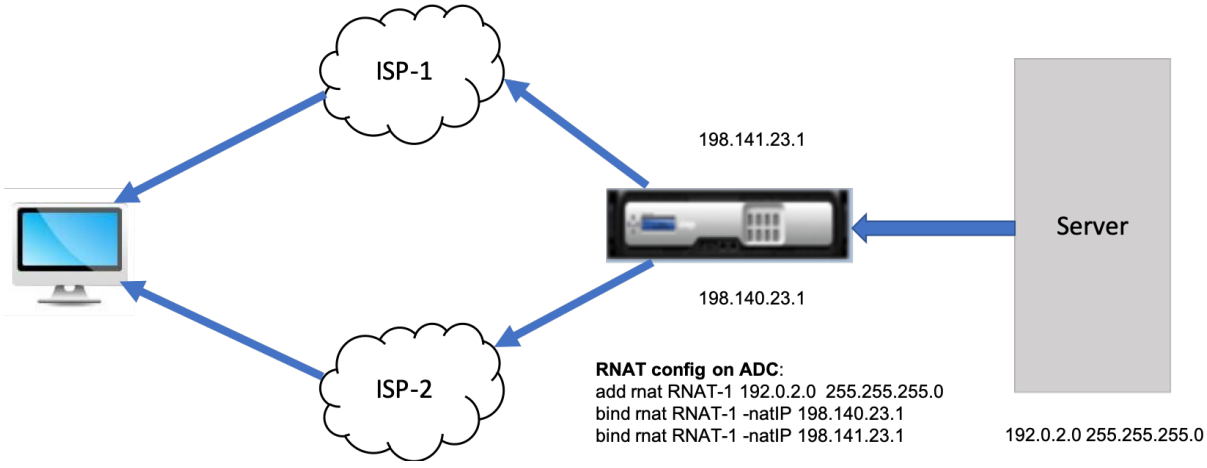
3. Wählen Sie im Dialogfeld Dienst konfigurieren auf der Registerkarte Monitore unter Verfügbar den Monitor aus, den Sie an den Dienst binden möchten, und klicken Sie dann auf Hinzufügen.
4. Klicken Sie auf OK.
5. Wählen Sie im Bereich Dienste den Dienst aus, den Sie gerade konfiguriert haben, und überprüfen Sie, ob die im Detailbereich angezeigten Einstellungen korrekt sind.

RNAT mit LLB konfigurieren

May 11, 2023

Sie können ein LLB-Setup für die umgekehrte Netzwerkadressübersetzung (RNAT) für ausgehenden Verkehr konfigurieren. Es stellt sicher, dass der Rückkehr-Netzwerkverkehr für einen bestimmten Flow über denselben Pfad geleitet wird. Konfigurieren Sie zuerst die grundlegende LLB, wie unter Konfigurieren eines grundlegenden LLB-Setupsbeschrieben, und konfigurieren Sie dann RNAT wie unter RNAT konfigurierenbeschrieben. Aktivieren Sie dann den Modus “Subnetz-IP (USNIP) verwenden”.

In der folgenden Abbildung verwendet die NetScaler-Appliance LLB, um ausgehenden Datenverkehr an verschiedene Links weiterzuleiten. Während des RNAT-Vorgangs ersetzt die ADC-Appliance die Quell-IP-Adressen des ausgehenden Datenverkehrs durch die öffentliche NAT-IP-Adresse (198.141.23.1), um den Datenverkehr über ISP-1 weiterzuleiten. In ähnlicher Weise ersetzt die ADC-Appliance die Quell-IP-Adressen durch 198.140.23.1, um den Datenverkehr über ISP-2 weiterzuleiten.



So fügen Sie SNIPs für ISP-Router mithilfe der CLI hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add NS IP <subnet of first ISP in the IP router> <subnet mask> -type
    SNIP
2
```



```
add NS IP <subnet of second ISP in the IP router> <subnet mask> -type
    SNIP
<!--NeedCopy-->
```

Beispiel:

```
add ns ip 198.140.23.1 255.255.255.0 -type snip

add ns ip 198.141.23.1 255.255.255.0 -type snip
<!--NeedCopy-->
```

So konfigurieren Sie RNAT mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ …

show rnat <name>
<!--NeedCopy-->
```

Beispiel:

```
add rnat RNAT-1 192.0.2.0 255.255.255.0
bind rnat RNAT-1 -natIP 198.140.23.1
bind rnat RNAT-1 -natIP 198.141.23.1

> show rnat RNAT-1
    1) RNAT Name: RNAT-1     Network: 192.0.2.0      Netmask:
       255.255.255.0     Traffic Domain: 0
        UseProxyPort: ENABLED

        NatIP: 198.140.23.1
        NatIP: 198.141.23.1
<!--NeedCopy-->
```

So konfigurieren Sie RNAT mithilfe der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **NATs.**
2. Klicken Sie auf der Registerkarte **RNAT** auf **RNAT konfigurieren**.
3. Geben Sie das Netzwerk an, in dem RNAT ausgeführt werden soll.

> **Hinweis**
>
> Sie können RNAT auch mithilfe von Zugriffssteuerungslisten (Access Control Lists, ACLs) konfigurieren. Weitere Informationen finden Sie unter RNAT konfigurieren .

So aktivieren Sie den Subnetz-IP-Modus verwenden mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns mode USNIP

show ns mode
<!--NeedCopy-->
```

Beispiel:

```
enable ns mode USNIP

show ns mode
        Mode                            Acronym             Status
        -------                         -------             ------
 1)     Fast Ramp                       FR                  ON
 2)     … .
 8)     Use Subnet IP                   USNIP               ON
 9)     …
<!--NeedCopy-->
```

So aktivieren Sie den Modus „Subnetz-IP verwenden“ mithilfe der GUI

1. Navigieren Sie zu **System** > **Einstellungen** und klicken Sie unter **Modi und Funktionen**auf **Modi konfigurieren**.
2. Wählen **Sie im Dialogfeld Modi konfigurieren** die Option **Subnetz-IP verwenden** aus, und klicken Sie dann auf **OK** .

Eine Backup-Route konfigurieren

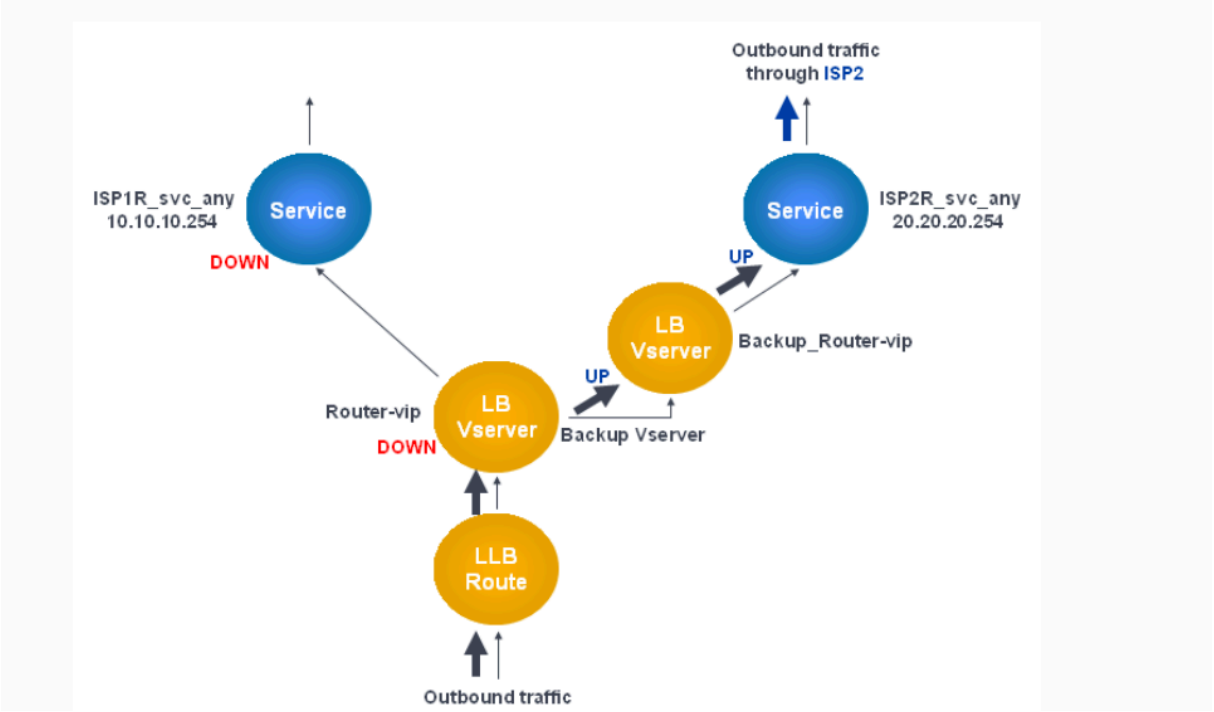
May 11, 2023

Um eine Unterbrechung der Dienste zu verhindern, wenn die primäre Route ausfällt, können Sie eine Backup-Route konfigurieren. Nach der Konfiguration der Backuproute verwendet die NetScaler Appliance diese automatisch, wenn die primäre Route fehlschlägt. Erstellen Sie zunächst einen

primären virtuellen Server, wie unter Konfigurieren eines virtuellen LLB-Servers und Binden eines Dienstesbeschrieben. Um eine Backuproute zu konfigurieren, erstellen Sie einen sekundären virtuellen Server, der einem primären virtuellen Server ähnlich ist, und weisen Sie diesen virtuellen Server als virtuellen Backupserver (Route) an.

In der folgenden Abbildung ist **Router-VIP** der primäre virtuelle Server, und **Backup_Router-VIP** ist der sekundäre virtuelle Server, der als virtueller Backup-Server bezeichnet wird.

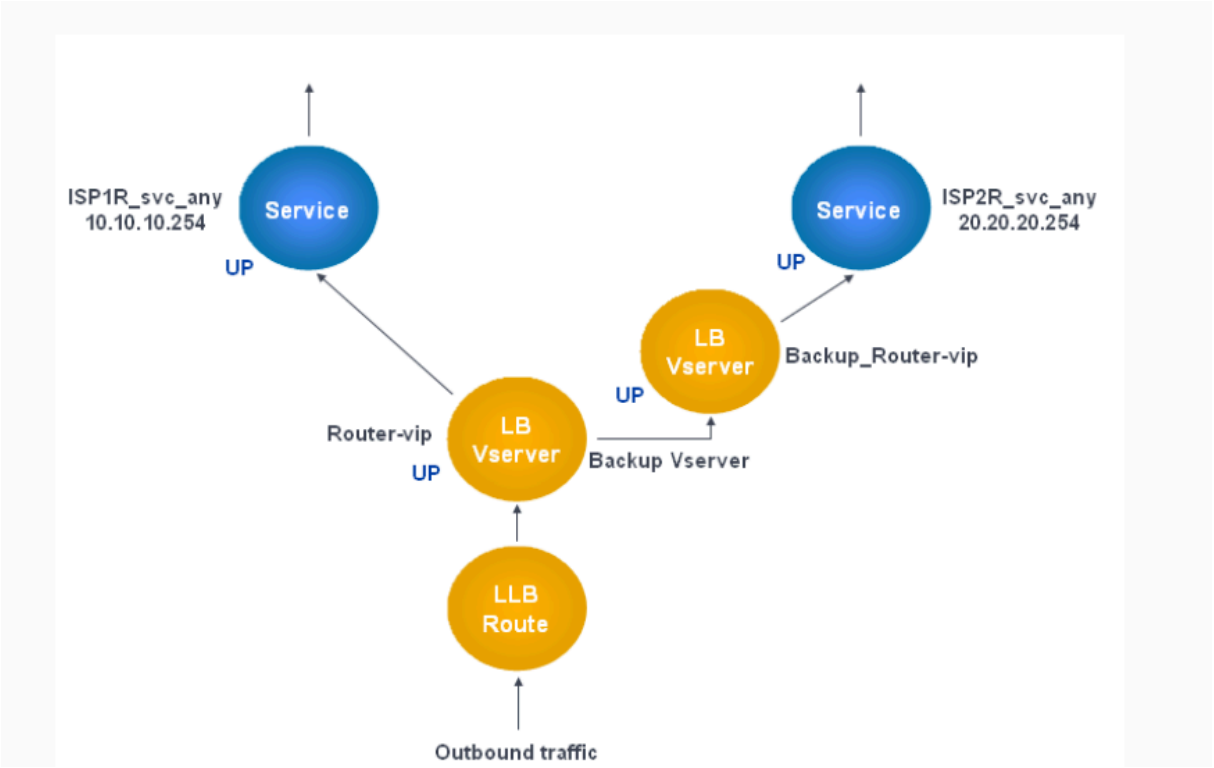
Abbildung 1. Einrichtung der Backup-Route



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst in der vorherigen Abbildung durch einen IPv6-Dienst.

Standardmäßig wird der gesamte Verkehr über die primäre Route gesendet. Wenn die primäre Route jedoch ausfällt, wird der gesamte Datenverkehr auf die Backup-Route umgeleitet, wie in der folgenden Abbildung dargestellt.

Abbildung 2. Routing im Betrieb sichern



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst in der vorherigen Abbildung durch einen IPv6-Dienst.

So legen Sie den sekundären virtuellen Server mithilfe der Befehlszeilenschnittstelle als virtuellen Backupserver fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Router-vip -backupVServer Backup_Router-vip
> show lb vserver Router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 03:09:45.600
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       1 (Active)
```



```
12          Configured Method: ROUNDROBIN
13          Mode: IP
14          Persistence: DESTIP     Persistence Mask: 255.255.255.255
                      Persistence v6MaskLength: 128   Persistence Timeout: 2
                min
15          Backup: Router2-vip
16          Connection Failover: DISABLED
17   Done
18  <!--NeedCopy-->
```

So legen Sie den sekundären virtuellen Server mithilfe des Konfigurationsdienstprogramms als virtuellen Backup-Server fest

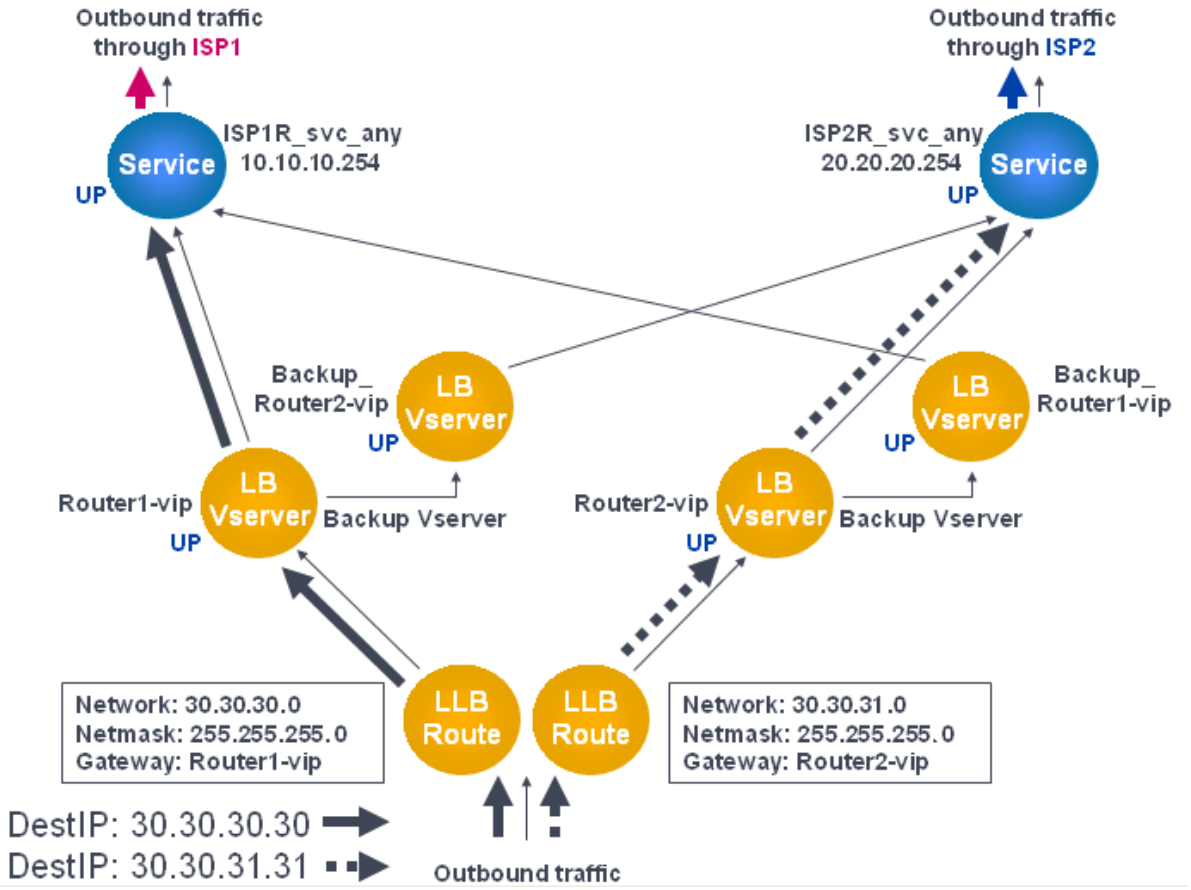
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und wählen Sie den sekundären virtuellen Server aus, für den Sie den virtuellen Backup-Server konfigurieren möchten.
2. Wählen **Sie im Dialogfeld Load Balancing Virtual Server** unter **Advanced**die Option **Schutz**aus.
3. Wählen Sie in der Dropdownliste **Virtueller Sicherungsserver** den sekundären virtuellen Backupserver aus, und klicken Sie dann auf **OK**.

Resilientes LLB-Bereitstellungsszenario

February 16, 2021

Im folgenden Diagramm gibt es zwei Netzwerke: 30.30.30.0 und 30.30.31.0. Der Link-Lastausgleich wird basierend auf der Ziel-IP-Adresse konfiguriert. Zwei Routen sind mit Gateways **Router1-VIP** und **Router2-VIP** konfiguriert. **Router1-VIP** ist als Backup für **Router2-VIP** und umgekehrt konfiguriert. Der gesamte Datenverkehr mit der Ziel-IP, die als 30.30.30.30 angegeben ist, wird über **Router1-VIP** gesendet und der Datenverkehr mit der als 30.30.31.31 angegebenen Ziel-IP wird über **Router2-VIP** gesendet.

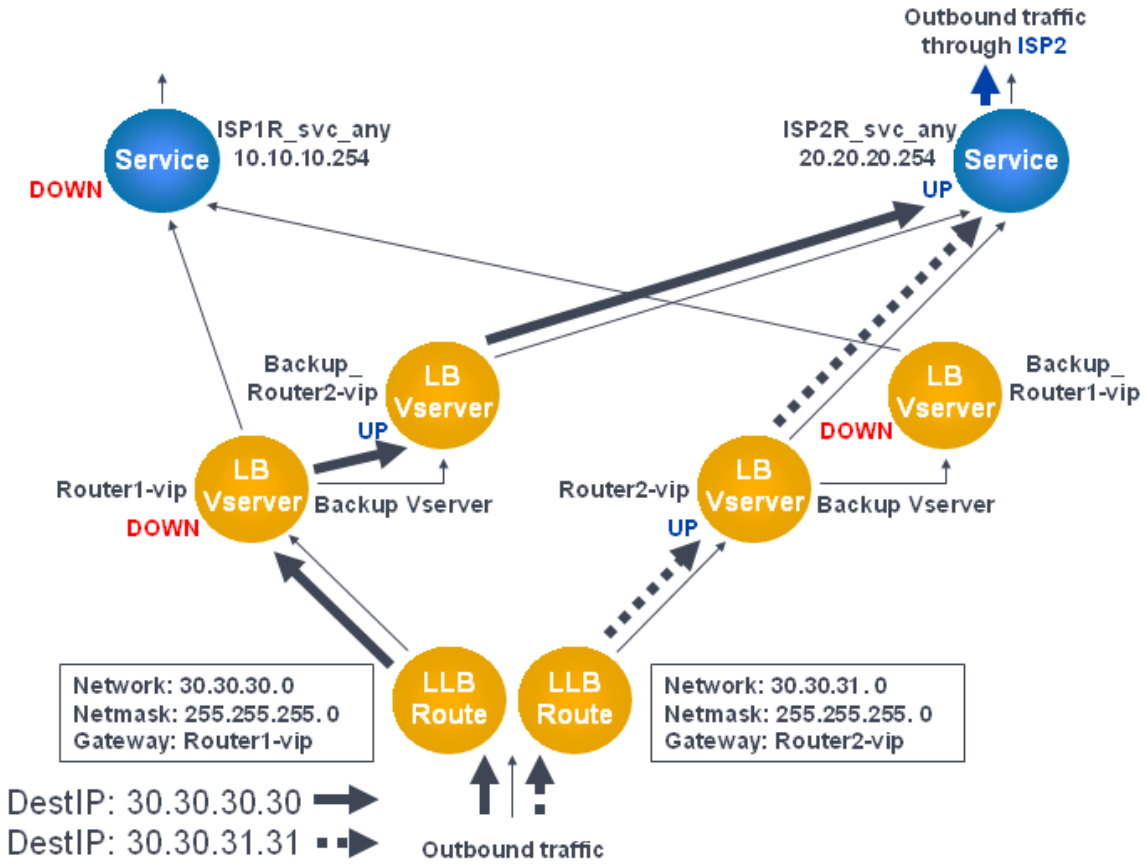
Abbildung 1. Resilient LLB-Bereitstellungs-Setup



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst durch einen IPv6-Dienst in der vorherigen Abbildung.

Wenn jedoch eines der Gateways (**Router1-VIP** oder **Router2-VIP**) DOWN ist, wird der Datenverkehr über den Backup-Router weitergeleitet. Im folgenden Diagramm ist **Router1-VIP** für ISP1 DOWN, sodass der gesamte Datenverkehr mit der Ziel-IP, die als 30.30.30.30 angegeben ist, ebenfalls über ISP2 gesendet wird.

Abbildung 2. Resilient LLB-Bereitstellungsszenario



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst durch einen IPv6-Dienst in der vorherigen Abbildung.

Überwachen Sie ein LLB-Setup

May 11, 2023

Nachdem die Konfiguration eingerichtet und ausgeführt wurde, können Sie die Statistiken für jeden Dienst und virtuellen Server einsehen, um nach möglichen Problemen zu suchen.

Sehen Sie sich die Statistiken eines virtuellen Servers an

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der NetScaler-Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen. Sie können auch den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der eingegangenen Anfragen
- `Rate of hits`

Zeigen Sie virtuelle Serverstatistiken mithilfe der CLI an

Um eine Zusammenfassung der Statistiken für alle derzeit auf dem NetScaler konfigurierten virtuellen Server oder für einen einzelnen virtuellen Server anzuzeigen, geben Sie an der Befehlszeile Folgendes ein:

```
stat lb vserver -detail] [<name>]
<!--NeedCopy-->
```

Beispiel:

```
stat lb vserver -detail
Virtual Server(s) Summary
                      vsvrIP  port     Protocol        State    Req/s
                           Hits/s
One                         *    80         HTTP           UP      5/s
        0/s
Two                         *     0          TCP         DOWN      0/s
        0/s
Three                       *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done
<!--NeedCopy-->
```

Zeigen Sie virtuelle Serverstatistiken mithilfe der GUI an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server > Statistik**.
2. Wenn Sie die Statistiken für nur einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf Statistik.

Sehen Sie sich die Statistiken eines Dienstes an

Sie können die Rate der Anfragen, Antworten, Anforderungsbytes, Antwortbytes, aktuelle Clientverbindungen, Anfragen in der Überspannungswarteschlange, aktuelle Serververbindungen usw. mithilfe der Dienststatistiken anzeigen.

Sehen Sie sich die Statistiken eines Dienstes mithilfe der CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Zeigen Sie die Statistiken eines Dienstes über die GUI an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services > Statistik**.
2. Wenn Sie die Statistiken nur für einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf Statistiken.

Lastausgleich

May 11, 2023

Die Lastenausgleichsfunktion verteilt Benutzeranfragen für Webseiten und andere geschützte Anwendungen auf mehrere Server, die alle denselben Inhalt hosten (oder spiegeln). Sie verwenden den Lastenausgleich in erster Linie, um Benutzeranforderungen an stark genutzte Anwendungen zu verwalten, schlechte Leistung und Ausfälle zu vermeiden und sicherzustellen, dass Benutzer auf Ihre geschützten Anwendungen zugreifen können. Der Lastenausgleich bietet auch Fehlertoleranz. Wenn ein Server, der eine geschützte Anwendung hostet, nicht verfügbar wird, verteilt die Funktion Benutzeranfragen an die anderen Server, die dieselbe Anwendung hosten.

Sie können die Lastenausgleichsfunktion konfigurieren:

- Verteilen Sie alle Anforderungen für eine bestimmte geschützte Website, Anwendung oder Ressource zwischen zwei oder mehr identisch konfigurierten Servern.

- Verwenden Sie einen der verschiedenen Algorithmen, um zu ermitteln, welcher Server jede eingehende Benutzeranforderung empfangen muss, wobei die Entscheidung auf verschiedene Faktoren beruht, z. B. welcher Server über die wenigsten aktuellen Benutzerverbindungen verfügt oder welcher Server die geringste Last hat.

Die Lastausgleichsfunktion ist ein Kernmerkmal der NetScaler Appliance. Die meisten Benutzer richten zunächst eine funktionierende Grundkonfiguration ein und passen dann verschiedene Einstellungen an, einschließlich der Persistenz für Verbindungen. Darüber hinaus können Sie Funktionen konfigurieren, um die Konfiguration vor Fehlern zu schützen, Clientdatenverkehr zu verwalten, Server zu verwalten und zu überwachen und eine umfangreiche Bereitstellung zu verwalten.

So funktioniert Load Balancing

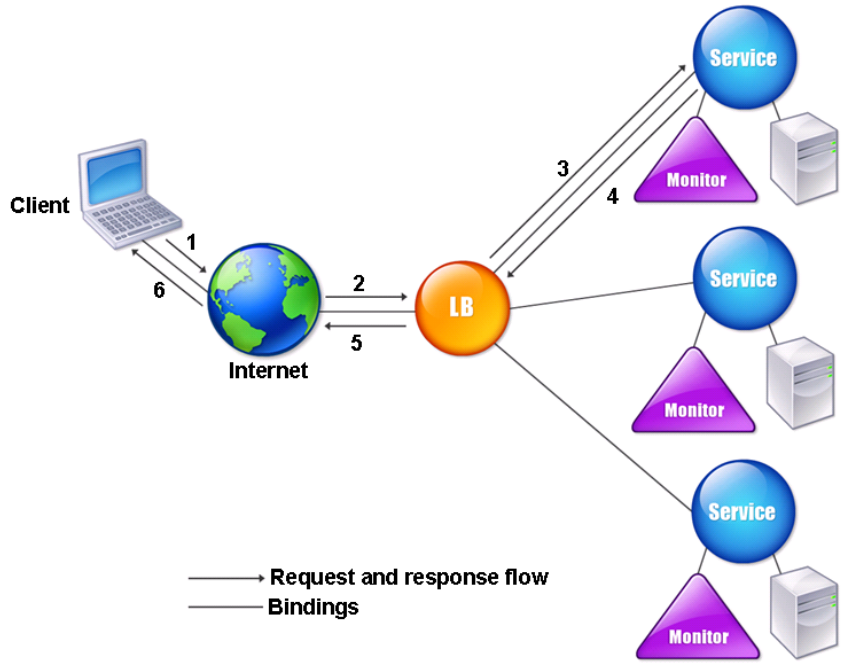
May 11, 2023

In einem grundlegenden Load-Balancing-Setup senden Clients ihre Anfragen an die IP-Adresse eines virtuellen Servers, der auf der NetScaler-Appliance konfiguriert ist. Der virtuelle Server verteilt sie an die Anwendungsserver mit Lastenausgleich nach einem voreingestellten Muster, dem sogenannten Lastausgleichsalgorithmus. Manchmal möchten Sie dem virtuellen Lastenausgleichsserver möglicherweise eine Platzhalteradresse anstelle einer bestimmten IP-Adresse zuweisen. Anweisungen zum Angeben eines globalen HTTP-Ports auf der Appliance finden Sie unter **Globale HTTP-Ports**.

Grundlagen des Lastenausgleichs

Ein Lastenausgleichs-Setup umfasst einen virtuellen Lastausgleichsserver und mehrere Anwendungsserver mit Lastausgleich. Der virtuelle Server empfängt eingehende Clientanforderungen, verwendet den Load-Balancing-Algorithmus, um einen Anwendungsserver auszuwählen, und leitet die Anfragen an den ausgewählten Anwendungsserver weiter. Die folgende Konzeptzeichnung zeigt eine typische Load-Balancing-Implementierung. Eine weitere Variante beinhaltet die Zuweisung eines globalen HTTP-Ports.

Abbildung 1. Lastenausgleich-Architektur



Der virtuelle Lastausgleichsserver kann mehrere Algorithmen (oder Methoden) verwenden, um zu bestimmen, wie die Last auf die von ihm verwaltlichen Lastausgleichsserver verteilt werden kann. Die Standardmethode für den Lastenausgleich ist die geringste Verbindungsmethode, bei der die NetScaler Appliance jede eingehende Clientverbindung an den Anwendungsserver mit Lastenausgleich weiterleitet, der derzeit die wenigsten aktiven Benutzerverbindungen aufweist.

Die Entitäten, die Sie in einem typischen NetScaler-Load-Balancing-Setup konfigurieren, sind:

- **Virtueller Lastausgleichsserver.** Die Kombination aus IP-Adresse, Port und Protokoll, an die ein Client Verbindungsanfragen für eine bestimmte Website oder Anwendung mit Lastausgleich sendet. Wenn die Anwendung über das Internet zugänglich ist, ist die IP-Adresse des virtuellen Servers (VIP) eine öffentliche IP-Adresse. Wenn die Anwendung nur vom LAN oder WAN aus zugänglich ist, ist der VIP normalerweise eine private (nicht routfähige ICANN-IP-Adresse).
- **Bedienung.** Die Kombination aus IP-Adresse, Port und Protokoll, die verwendet wird, um Anfragen an einen bestimmten Anwendungsserver mit Lastenausgleich weiterzuleiten. Ein Dienst kann eine logische Darstellung des Anwendungsservers selbst oder einer Anwendung sein, die auf einem Server ausgeführt wird, der mehrere Anwendungen hostet. Nachdem Sie einen Dienst erstellt haben, binden Sie ihn an einen virtuellen Lastausgleichsserver.
- **Serverobjekt.** Eine virtuelle Entität, mit der Sie einem physischen Server einen Namen zuweisen können, anstatt den Server anhand seiner IP-Adresse zu identifizieren. Wenn Sie ein

Serverobjekt erstellen, können Sie seinen Namen anstelle der IP-Adresse des Servers angeben, wenn Sie einen Dienst erstellen. Andernfalls müssen Sie die IP-Adresse des Servers angeben, wenn Sie einen Dienst erstellen, und die IP-Adresse wird zum Namen des Servers.

- **Überwachen.** Eine Entität auf der NetScaler-Appliance, die einen Dienst verfolgt und sicherstellt, dass er ordnungsgemäß funktioniert. Der Monitor untersucht in regelmäßigen Abständen jeden Dienst, dem Sie ihn zuweisen, oder führt eine Integritätsprüfung durch. Wenn der Dienst nicht innerhalb der durch das Timeout angegebenen Zeit reagiert und eine bestimmte Anzahl von Integritätsprüfungen fehlschlägt, wird dieser Dienst als INAKTIV markiert. Die NetScaler-Appliance überspringt diesen Dienst dann beim Lastenausgleich, bis die Probleme behoben sind, die dazu geführt haben, dass der Dienst nicht mehr reagiert hat.

Die virtuellen Server, Dienste und Anwendungsserver mit Lastausgleich in einem Load-Balancing-Setup können entweder IP-Adressen der Internetprotokollversion 4 (IPv4) oder der Internetprotokollversion 6 (IPv6) verwenden. Sie können IPv4- und IPv6-Adressen in einem einzigen Load-Balancing-Setup kombinieren.

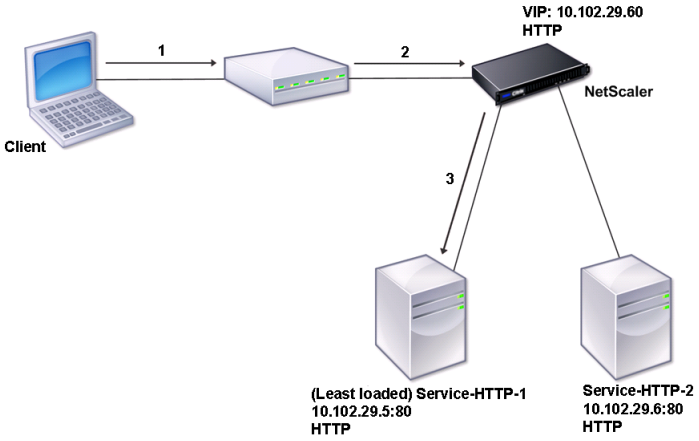
Variationen der Load-Balancing-Setup finden Sie in den folgenden Anwendungsfällen:

- Konfiguration des Load Balancings im direkten Serverrückgabemodus
- Konfiguration von LINUX-Servern im DSR-Modus
- Konfiguration des DSR-Modus bei Verwendung von TOS
- Konfiguration des Load Balancings im DSR-Modus mithilfe von IP over IP
- Konfiguration des Load Balancings im Einarm-Modus
- Konfiguration des Load Balancings im Inline-Modus
- Lastverteilung der Server des Intrusion Detection Systems
- Load Balance-Remotedesktopprotokollserver

Die Topologie verstehen

In einem Load-Balancing-Setup befindet sich der Lastausgleichsserver logisch zwischen dem Client und der Serverfarm und verwaltet den Datenverkehr zu den Servern in der Serverfarm. Auf der NetScaler-Appliance werden die Anwendungsserver durch virtuelle Entitäten repräsentiert, die als Dienste bezeichnet werden. Das folgende Diagramm zeigt die Topologie einer grundlegenden Load-Balancing-Konfiguration.

Abbildung 2. Grundlegende Load Balancing-Topologie

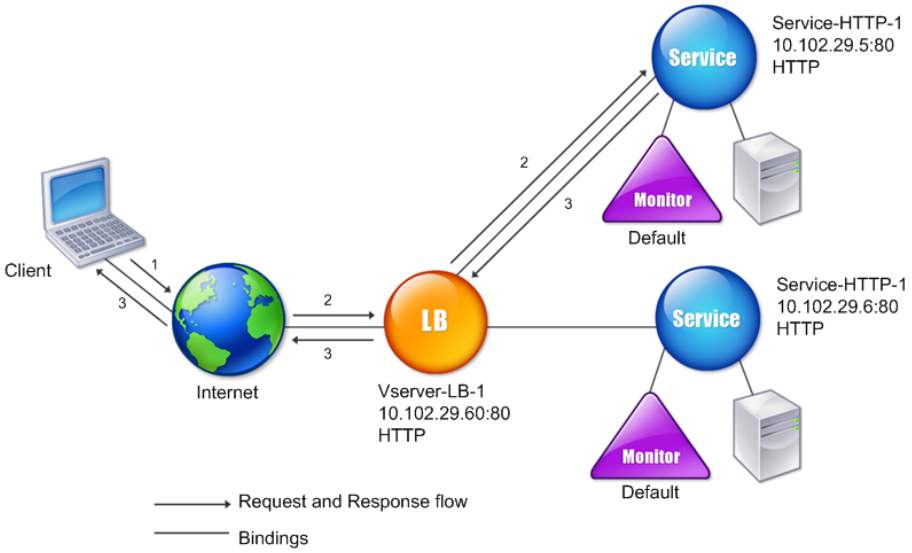


Im Diagramm wird der Lastenausgleich verwendet, um den Datenfluss zu den Servern zu verwalten. Der virtuelle Server wählt den Dienst aus und weist ihn der Bearbeitung von Clientanforderungen zu. Stellen Sie sich ein Szenario vor, in dem die Dienste Service-HTTP-1 und Service-HTTP-2 erstellt und an den virtuellen Server mit dem Namen vServer-LB-1 gebunden werden. vServer-LB-1 leitet die Client-Anfrage entweder an Service-HTTP-1 oder Service-HTTP-2 weiter. Die NetScaler-Appliance verwendet die Methode zum Lastausgleich mit der geringsten Verbindungslast, um den Dienst für jede Anforderung auszuwählen. In der folgenden Tabelle sind die Namen und Werte der grundlegenden Entitäten aufgeführt, die auf der Appliance konfiguriert werden müssen.

Entität	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.60	80	HTTP
Services	Service-HTTP-1	10.102.29.5	80	HTTP
	Service-HTTP-2	10.102.29.6	80	HTTP
Monitore	Standard	Ohne	Ohne	Ohne

Das folgende Diagramm zeigt die Beispielwerte für den Lastausgleich und die obligatorischen Parameter, die in der vorherigen Tabelle beschrieben sind.

Abbildung 3. Load Balancing Entity Modell



Verwendung von Platzhaltern anstelle von IP-Adressen und Ports

Manchmal müssen Sie möglicherweise einen Platzhalter für die IP-Adresse oder den Port eines virtuellen Servers oder für den Port eines Dienstes verwenden. Die folgenden Fälle erfordern möglicherweise die Verwendung eines Platzhalters:

- Wenn die NetScaler Appliance als transparenter Durchgang konfiguriert ist, muss der gesamte Datenverkehr akzeptiert werden, der an sie gesendet wird, unabhängig von der IP oder dem Port, an den sie gesendet wird.
- Wenn ein oder mehrere Dienste Ports abhören, die nicht bekannt sind.
- Wenn ein oder mehrere Dienste im Laufe der Zeit die Ports ändern, auf denen sie abhören.
- Wenn Sie das Limit für die Anzahl der IP-Adressen und Ports erreichen, die Sie auf einer einzelnen NetScaler-Appliance konfigurieren können.
- Wenn Sie virtuelle Server erstellen möchten, die den gesamten Datenverkehr in einem bestimmten virtuellen LAN überwachen.

Wenn ein mit Platzhalter konfigurierter virtueller Server oder Dienst Datenverkehr empfängt, ermittelt die NetScaler Appliance die tatsächliche IP-Adresse oder den tatsächlichen Port und erstellt Datensätze für den Dienst und den zugehörigen Lastausgleichsanwendungsserver. Diese dynamisch erstell-

ten Datensätze werden als dynamisch erlernte Server- und Dienstdatensätze bezeichnet.

Beispielsweise kann eine Firewall-Load-Balancing-Konfiguration Platzhalter sowohl für die IP-Adresse als auch für den Port verwenden. Wenn Sie einen Platzhalter-TCP-Service an diesen Typ eines virtuellen Lastausgleichsservers binden, empfängt und verarbeitet der virtuelle Server den gesamten TCP-Datenverkehr, der keinem anderen Dienst oder virtuellen Server entspricht.

In der folgenden Tabelle werden einige der verschiedenen Arten von Platzhalterkonfigurationen beschrieben und wann sie verwendet werden müssen.

IP	Port	Protokoll	Beschreibung
*	*	TCP	Ein allgemeiner virtueller Wildcard-Server, der Datenverkehr akzeptiert, der an eine beliebige IP-Adresse und Port der NetScaler Appliance gesendet wird. Bei Verwendung eines virtuellen Platzhalterservers lernt die Appliance dynamisch die IP und den Port jedes Dienstes und erstellt die erforderlichen Datensätze, während sie den Datenverkehr verarbeitet.

IP	Port	Protokoll	Beschreibung
*	*	TCP	Ein virtueller Firewall-Lastenausgleichsserver. Sie können Firewalldienste an diesen virtuellen Server binden, und die NetScaler-Appliance leitet den Datenverkehr über die Firewall zum Ziel weiter.
IP-Adresse	*	TCP, UDP und ANY	Ein virtueller Server, der den gesamten Datenverkehr akzeptiert, der an die angegebene IP-Adresse gesendet wird, unabhängig vom Port. Sie müssen explizit an diesen virtuellen Server die Dienste binden, zu denen der Datenverkehr umgeleitet wird. Es lernt sie nicht dynamisch.

IP	Port	Protokoll	Beschreibung
			Hinweis: Sie konfigurieren keine Dienste oder virtuelle Server für einen globalen HTTP-Port. In diesem Fall konfigurieren Sie einen bestimmten Port als globalen HTTP-Port (setzen Sie beispielsweise ns param -HttpPort 80). Die Appliance akzeptiert dann den gesamten Datenverkehr, der der Portnummer entspricht, und verarbeitet ihn als HTTP-Verkehr. Die Appliance lernt dynamisch und erstellt Dienste für diesen Verkehr.

IP	Port	Protokoll	Beschreibung
*	Port	SSL, SSL_TCP	Ein virtueller Server, der den gesamten Datenverkehr akzeptiert, der an eine beliebige IP-Adresse an einem bestimmten Port gesendet wird. Wird für globales transparentes SSL-Offloading verwendet. Die gesamte SSL-, HTTP- und TCP-Verarbeitung, die normalerweise für einen Dienst desselben Protokolltyps ausgeführt wird, wird auf den Datenverkehr angewendet, der an diesen bestimmten Port gerichtet ist. Die Appliance verwendet den Port, um dynamisch die IP des Dienstes zu erlernen, den sie verwenden muss. Wenn —cleartext nicht angegeben ist, verwendet die NetScaler Appliance End-to-End-SSL.

IP	Port	Protokoll	Beschreibung
*	Port	Nicht zutreffend	Alle anderen virtuellen Server, die Datenverkehr zum Port akzeptieren können. Sie binden Dienste nicht an diese virtuellen Server. Die NetScaler Appliance lernt sie dynamisch.

Hinweis: Wenn Sie Ihre NetScaler Appliance als transparenten Durchgang konfiguriert haben, der globale (Platzhalter-) Ports verwendet, möchten Sie möglicherweise den Edge-Modus aktivieren. Weitere Informationen finden Sie unter “Edge-Modus konfigurieren. “

Die NetScaler Appliance versucht, virtuelle Server und Dienste zu finden, indem sie zunächst eine exakte Übereinstimmung versucht. Wenn keine gefunden wird, wird auf der Grundlage von Platzhaltern in der folgenden Reihenfolge weiter nach einem Treffer gesucht:

1. Spezifische IP-Adresse und spezifische Portnummer
2. Spezifische IP-Adresse und ein * (Wildcard) Port
3. • (Wildcard-) IP-Adresse und ein bestimmter Port
4. • (Platzhalter-) IP-Adresse und ein * (Platzhalter) Port

Wenn die Appliance einen virtuellen Server nicht nach IP-Adresse oder Portnummer auswählen kann, sucht sie in der folgenden Reihenfolge nach einem virtuellen Server, der auf dem in der Anforderung verwendeten Protokoll basiert:

1. HTTP
2. TCP
3. ANY

Konfiguration globaler HTTP-Ports

Sie konfigurieren keine Dienste oder virtuellen Server für einen globalen HTTP-Port. Stattdessen konfigurieren Sie einen bestimmten Port, indem Sie den Befehl set ns param verwenden. Nach der Konfiguration dieses Port akzeptiert die NetScaler-Appliance den gesamten Datenverkehr, der der Portnummer entspricht, und verarbeitet ihn als HTTP-Verkehr, wobei sie dynamisch lernt und Dienste für diesen Verkehr erstellt.

Sie können mehr als eine Portnummer als globalen HTTP-Port konfigurieren. Wenn Sie in einem einzigen Befehl set ns param mehr als eine Portnummer angeben, trennen Sie die Portnummern durch ein einzelnes Leerzeichen. Wenn ein oder mehrere Ports bereits als globale HTTP-Ports angegeben wurden und Sie einen oder mehrere Ports hinzufügen möchten, ohne die aktuell konfigurierten Ports zu entfernen, müssen Sie im Befehl alle aktuellen und neuen Portnummern angeben. Bevor Sie Portnummern hinzufügen, verwenden Sie den Befehl show ns param, um die aktuell konfigurierten Ports anzuzeigen.

So konfigurieren Sie einen globalen HTTP-Port mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen globalen HTTP-Port zu konfigurieren und die Konfiguration zu überprüfen:

```
set ns param  -httpPort <port>

show ns param
<!--NeedCopy-->
```

Beispiel 1: Konfiguration eines Port als globalen HTTP-Port

In diesem Beispiel ist Port 80 als globaler HTTP-Port konfiguriert.

```
set ns param -httpPort 80
Done
show ns param
         Global configuration settings:
                           HTTP port(s): 80
                       Max connections: 0
            Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
         Persistence Cookie Secure Flag: ENABLED
         ...
         ...
<!--NeedCopy-->
```

Beispiel 2: Hinzufügen von Ports, wenn ein oder mehrere globale HTTP-Ports bereits konfiguriert sind**

In diesem Beispiel wird Port 8888 zur globalen HTTP-Portliste hinzugefügt. Port 80 ist bereits als globaler HTTP-Port konfiguriert.


```
> show ns param
        Global configuration settings:
                            HTTP port(s): 80
                        Max connections: 0
           Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576
        ...
        ...
 Done
> set ns param -httpPort 80 8888
 Done
>  show ns param

        Global configuration settings:
                            HTTP port(s): 80,8888
                        Max connections: 0
           Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576

        ...
        ...
 Done
>
<!--NeedCopy-->
```

So konfigurieren Sie einen globalen HTTP-Port mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **System > Einstellungen > HTTP-Parameter ändern**, und fügen Sie dann eine HTTP-Portnummer hinzu.

Einrichten des grundlegenden Lastenausgleichs

August 15, 2023

Bevor Sie Ihr erstes Load-Balancing-Setup konfigurieren, aktivieren Sie die Load-Balancing-Funktion.

Erstellen Sie dann zunächst mindestens einen Dienst für jeden Server in der Load Balancing-Gruppe. Wenn die Dienste konfiguriert sind, können Sie einen virtuellen Lastausgleichsserver erstellen und jeden Dienst an den virtuellen Server binden. Damit ist die Ersteinrichtung abgeschlossen. Bevor Sie mit der weiteren Konfiguration fortfahren, überprüfen Sie Ihre Konfiguration, um sicherzustellen, dass jedes Element ordnungsgemäß konfiguriert wurde und wie erwartet funktioniert.

Load Balancing aktivieren

Sie können Load Balancing-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Load Balancing-Funktion deaktiviert ist. Sie funktionieren jedoch erst, wenn Sie die Funktion aktivieren.

So aktivieren Sie den Lastenausgleich mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen

- enable ns feature LB
- show ns feature

Beispiel

```
> enable ns feature LoadBalancing

 Done

> show ns feature


        Feature                         Acronym             Status

        -------                         -------             ------

 1)     Web Logging                     WL                  OFF

 2)     Surge Protection                SP                  ON

 3) Load Balancing LB ON

 .

 .

```



```
23      .
24
25      24)    NetScaler Push                  push                  OFF
26
27      Done
28  <!--NeedCopy-->
```

So aktivieren Sie den Lastenausgleich mithilfe der GUI

Navigieren Sie zu **System** > **Einstellungen** und wählen Sie unter **Grundfunktionen konfigurieren**die Option **Load Balancing**aus.

Konfiguration eines Serverobjekts

Erstellen Sie einen Eintrag für Ihren Server auf der NetScaler-Appliance. Die NetScaler-Appliance unterstützt auf IP-Adressen basierende Server und domänenbasierte Server. Wenn Sie einen IP-adressbasierten Server erstellen, können Sie beim Erstellen eines Dienstes den Namen des Servers anstelle seiner IP-Adresse angeben. Informationen zum Einrichten von DNS für einen domänenbasierten Server finden Sie unter Domänennamensystem.

So erstellen Sie ein Serverobjekt mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  add server `<name>`@ `<IPAddress>`@ | `<domain>`
2  <!--NeedCopy-->
```

Beispiel für das Hinzufügen eines auf IP-Adressen basierenden Nameservers:

```
1  add server web_serv 10.102.27.150
2  <!--NeedCopy-->
```

Beispiel für das Hinzufügen eines domänenbasierten Servers:

```
1  add server web_serv test.com
2  <!--NeedCopy-->
```

So erstellen Sie ein Serverobjekt mithilfe der GUI

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Server**und fügen Sie ein Serverobjekt hinzu.

Dienste konfigurieren

Nachdem Sie die Load-Balancing-Funktion aktiviert haben, müssen Sie mindestens einen Dienst für jeden Anwendungsserver erstellen, der in Ihr Load-Balancing-Setup aufgenommen werden soll. Die Dienste, die Sie konfigurieren, stellen die Verbindungen zwischen der NetScaler-Appliance und den Load Balancing-Servern bereit. Jeder Dienst hat einen Namen und gibt eine IP-Adresse, einen Port und den Datentyp an, der bereitgestellt wird.

Wenn Sie einen Dienst erstellen, ohne zuerst ein Serverobjekt zu erstellen, ist die IP-Adresse des Dienstes auch der Name des Servers, der den Dienst hostet. Wenn Sie Server lieber anhand des Namens als anhand der IP-Adresse identifizieren möchten, können Sie Serverobjekte erstellen und dann beim Erstellen eines Dienstes den Namen eines Servers anstelle seiner IP-Adresse angeben.

Wenn Sie einen Dienst erstellen, der UDP als Transportschichtprotokoll verwendet, wird automatisch ein Ping-Monitor an den Dienst gebunden. Ein Ping-Monitor ist der grundlegendste der eingebauten Monitore. Wenn Sie einen Dienst erstellen, der TCP als Transportschichtprotokoll verwendet, wird automatisch ein TCP_Default-Monitor an den Dienst gebunden. Wenn Sie eine Strategie für die Verwaltung Ihres Load-Balancing-Setups entwickeln, entscheiden Sie sich möglicherweise dafür, einen anderen Monitortyp oder mehrere Monitore an den Dienst zu binden.

Einen Dienst erstellen

Bevor Sie einen Dienst erstellen, müssen Sie sich mit den verschiedenen Diensttypen und deren Verwendung vertraut machen. In der folgenden Liste werden die Arten von Diensten beschrieben, die auf der NetScaler-Appliance unterstützt werden.

HTTP

Wird für Server mit Lastenausgleich verwendet, die HTTP-Verkehr akzeptieren, wie z. B. Standardwebsites und Webanwendungen. Der HTTP-Diensttyp ermöglicht es der NetScaler-Appliance, Komprimierung, Inhaltsfilterung, Caching und Client-Keep-Alive-Unterstützung für Ihre Layer-7-Webserver bereitzustellen. Dieser Diensttyp unterstützt auch das Einfügen von IP-Ports für virtuelle Server, das Umschreiben von Umleitungsporten, Web 2.0-Push und Unterstützung für die URL-Umleitung.

Da HTTP ein TCP-basiertes Anwendungsprotokoll ist, können Sie den TCP-Diensttyp auch für Webserver verwenden. Wenn Sie dies tun, kann die NetScaler-Appliance jedoch nur Layer-4-Lastenausgleich durchführen. Es kann keine der zuvor beschriebenen Layer-7-Unterstützungen bereitstellen.

SSL

Wird für Server verwendet, die HTTPS-Verkehr akzeptieren, wie z. B. E-Commerce-Websites und Warenkorbanwendungen. Der SSL-Diensttyp ermöglicht es der NetScaler-Appliance, SSL-Verkehr für Ihre sicheren Webanwendungen zu verschlüsseln und zu entschlüsseln (SSL-Offloading durchzuführen). Es unterstützt auch HTTP-Persistenz, Inhaltswechsel, Umschreiben, Einfügen von IP-Ports für virtuelle Server, Web 2.0-Push und URL-Umleitung.

Sie können auch die Diensttypen SSL_BRIDGE, SSL_TCP oder TCP verwenden. Wenn Sie dies tun, führt die Appliance jedoch nur den Layer-4-Lastenausgleich durch. Es kann kein SSL-Offloading oder keine der beschriebenen Layer-7-Unterstützungen bereitstellen.

FTP

Wird für Server verwendet, die FTP-Verkehr akzeptieren. Der FTP-Diensttyp ermöglicht es der NetScaler-Appliance, bestimmte Details des FTP-Protokolls zu unterstützen.

Sie können auch TCP- oder ANY-Servicetypen für FTP-Server verwenden.

TCP

Wird für Server verwendet, die viele verschiedene Arten von TCP-Verkehr akzeptieren oder die eine Art von TCP-Verkehr akzeptieren, für die kein spezifischerer Diensttyp verfügbar ist.

Sie können für diese Server auch den ANY-Servicetyp verwenden.

SSL_TCP

Wird für Server verwendet, die SSL-Verkehr ohne HTTP akzeptieren, um SSL-Offloading zu unterstützen.

Sie können für diese Dienste auch den TCP-Diensttyp verwenden. Wenn Sie dies tun, führt die NetScaler-Appliance sowohl den Layer-4-Lastenausgleich als auch das SSL-Offloading durch.

UDP

Wird für Server verwendet, die UDP-Verkehr akzeptieren. Sie können auch den Servicetyp ANY verwenden.

SSL_BRIDGE

Wird für Server verwendet, die SSL-Verkehr akzeptieren, wenn Sie nicht möchten, dass die NetScaler-Appliance SSL-Offloading durchführt. Alternativ können Sie den Diensttyp SSL_TCP verwenden.

NNTP

Wird für Server verwendet, die Network News Transfer Protocol (NNTP) -Traffic akzeptieren, in der Regel Usenet-Sites.

DNS

Wird für Server verwendet, die DNS-Verkehr akzeptieren, in der Regel Nameserver. Mit dem DNS-Diensttyp validiert die NetScaler-Appliance das Paketformat jeder DNS-Anfrage und -Antwort. Es kann auch DNS-Antworten zwischenspeichern. Sie können DNS-Richtlinien auf DNS-Dienste anwenden.

Sie können für diese Dienste auch den UDP-Servicetyp verwenden. Wenn Sie dies jedoch tun, kann die NetScaler-Appliance nur Layer-4-Lastenausgleich durchführen. Es kann keine Unterstützung für DNS-spezifische Funktionen bieten.

ANY

Wird für Server verwendet, die jede Art von TCP-, UDP- oder ICMP-Verkehr akzeptieren. Der ANY-Parameter wird hauptsächlich beim Firewall-Lastenausgleich und beim Link-Load-Balancing verwendet.

SIP-UDP

Wird für Server verwendet, die UDP-basierten SIP-Verkehr (Session Initiation Protocol) akzeptieren. SIP initiiert, verwaltet und beendet Multimedia-Kommunikationssitzungen und hat sich zum Standard für Internettelefonie (VoIP) entwickelt.

Sie können für diese Dienste auch den UDP-Servicetyp verwenden. In diesem Fall führt die NetScaler Appliance jedoch nur Layer 4 Lastenausgleich aus. SIP-spezifische Funktionen können nicht unterstützt werden.

DNS-TCP

Wird für Server verwendet, die DNS-Verkehr akzeptieren, wobei die NetScaler-Appliance als Proxy für TCP-Verkehr fungiert, der an DNS-Server gesendet wird. Bei Diensten des DNS-TCP-Diensttyps überprüft die NetScaler-Appliance das Paketformat jeder DNS-Anfrage und -Antwort und kann DNS-Antworten wie beim DNS-Diensttyp zwischenspeichern.

Sie können für diese Dienste auch den TCP-Diensttyp verwenden. Wenn Sie dies jedoch tun, führt die NetScaler-Appliance nur den Layer-4-Lastenausgleich für externe DNS-Nameserver durch. Es kann keine Unterstützung für DNS-spezifische Funktionen bieten.

RTSP

Wird für Server verwendet, die RTSP-Verkehr (Real Time Streaming Protocol) akzeptieren. RTSP bietet die Bereitstellung von Multimedia- und anderen Streaming-Daten. Wählen Sie diesen Typ aus, um Audio-, Video- und andere Arten von gestreamten Medien zu unterstützen.

Sie können für diese Dienste auch den TCP-Diensttyp verwenden. In diesem Fall führt die NetScaler Appliance jedoch nur Layer 4 Lastenausgleich aus. Es kann den RTSP-Stream nicht analysieren oder RTSPID-Persistenz oder RTSP NAT unterstützen.

DHCPRA

Wird für Server verwendet, die DHCP-Verkehr akzeptieren. Der DHCPRA-Diensttyp kann verwendet werden, um DHCP-Anfragen und -Antworten zwischen VLANs weiterzuleiten.

DURCHMESSER

Wird für den Lastenausgleich Diameter-Datenverkehrs zwischen mehreren Diameter-Servern verwendet. Diameter verwendet ein nachrichtenbasiertes Load Balancing.

SSL_DURCHMESSER

Wird für den Lastenausgleich Diameter-Datenverkehrs über SSL verwendet.

Dienste werden als DEAKTIVIERT gekennzeichnet, bis die NetScaler-Appliance eine Verbindung zum zugehörigen Lastausgleichsserver herstellt und überprüft, ob dieser betriebsbereit ist. Zu diesem Zeitpunkt wird der Dienst als AKTIVIERT gekennzeichnet. Danach überwacht die NetScaler-Appliance regelmäßig den Status der Server und versetzt alle Server, die nicht auf Überwachungstests (sogenannte Integritätsprüfungen) reagieren, wieder in den Status DEAKTIVIERT, bis sie reagieren.

Hinweis: Sie können eine Reihe von Diensten mit einem einzigen CLI-Befehl oder demselben Dialogfeld erstellen. Die Namen im Bereich variieren je nach Zahl, die als Suffix/Präfix verwendet wird. Zum Beispiel service1, service2 usw. Im Konfigurationsprogramm können Sie einen Bereich nur im letzten Oktett der IP-Adresse angeben. Dies ist der vierte Bereich bei einer IPv4-Adresse und der achte bei einer IPv6-Adresse. Über die Befehlszeile können Sie den Bereich in einem beliebigen Oktett der IP-Adresse angeben.

QUIC

Wird von Load-Balancing-Servern verwendet, die UDP-basierten QUIC-Videoverkehr akzeptieren. Der Dienst ermöglicht es der NetScaler-Appliance, den verschlüsselten ABR-Videoverkehr über das UDP-Protokoll zu optimieren.

So erstellen Sie einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> <serviceType> <port>

add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

Um einen Dienst mithilfe der GUI zu erstellen

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an:
   - Dienstname — Name
   - Server — ServerName
   - Protokoll — Diensttyp
   - Port-Anschluss
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Der von Ihnen erstellte Dienst wird im Bereich Dienste angezeigt.

Einen virtuellen Server erstellen

Nachdem Sie Ihre Dienste erstellt haben, müssen Sie einen virtuellen Server erstellen, der den Datenverkehr für die Websites, Anwendungen oder Server mit Lastausgleich akzeptiert. Sobald der Lastausgleich konfiguriert ist, stellen Benutzer über die IP-Adresse oder den FQDN des virtuellen Servers eine Verbindung zu der Website, Anwendung oder dem Server mit Lastausgleich her.

> **Hinweise:**
>
> - Virtuelle Servernamen mit dem Präfix „app_“ erscheinen nicht in der GUI, obwohl sie in der Datei ns.conf vorhanden sind und angezeigt werden, wenn Sie den Befehl show ausführen. Virtuelle Servernamen mit dem Präfix „app“ werden jedoch in der GUI angezeigt.
> - Der virtuelle Server wird als DOWN bezeichnet, bis Sie die von Ihnen erstellten Dienste an ihn binden und bis der NetScaler eine Verbindung zu diesen Diensten herstellt und überprüft, ob sie betriebsbereit sind. Nach der Überprüfung wird der virtuelle Server als UP bezeichnet.
> - Wenn Sie möchten, dass der virtuelle Server alle Ports abhört, verwenden Sie anstelle des spezifischen Port ein Platzhalterzeichen (*).

> **Example:** `add lb vserver v1 TCP 1.11.1.1 *`.

So erstellen Sie einen virtuellen Server über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

So erstellen Sie einen virtuellen Server über die GUI

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und erstellen Sie dann einen virtuellen Server.

Dienste an den virtuellen Server binden

Hinweis: Ein Dienst kann an maximal 500 virtuelle Server gebunden werden.

Nachdem Sie Dienste und einen virtuellen Server erstellt haben, müssen Sie die Dienste an den virtuellen Server binden. Normalerweise sind Dienste an virtuelle Server desselben Typs gebunden, aber Sie können bestimmte Arten von Diensten an bestimmte verschiedene Arten von virtuellen Servern binden, wie unten gezeigt.

Virtueller Servertyp	Servicetyp	Kommentar
HTTP	SSL	Normalerweise würden Sie einen SSL-Dienst an einen virtuellen HTTP-Server binden, um die Verschlüsselung durchzuführen.
SSL	HTTP	Normalerweise würden Sie einen HTTP-Dienst an einen virtuellen SSL-Server binden, um SSL-Offloading durchzuführen.

Virtueller Servertyp	Servicetyp	Kommentar
SSL_TCP	TCP	Normalerweise würden Sie einen TCP-Dienst an einen virtuellen SSL_TCP-Server binden, um SSL-Offloading für andere TCP-Server durchzuführen (SSL-Entschlüsselung ohne Inhaltserkennung).

Der Status der an einen virtuellen Server gebundenen Dienste bestimmt den Status des virtuellen Servers: Wenn alle gebundenen Dienste DOWN sind, wird der virtuelle Server als DOWN markiert, und wenn einer der gebundenen Dienste UP oder OUT OF SERVICE ist, ist der Status des virtuellen Servers UP.

So binden Sie einen Dienst mithilfe der CLI an einen virtuellen Lastausgleichsserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> <serviceName>

bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Dienst mithilfe der GUI an einen virtuellen Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management**> **Load Balancing** > **Virtuelle Server**und wählen Sie einen virtuellen Server aus.
2. Klicken Sie in den Abschnitt **Service** und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Überprüfen der Konfiguration

Nach Abschluss der Basiskonfiguration können Sie die Eigenschaften jedes Dienstes und des virtuellen Lastenausgleichsservers in Ihrem Load Balancing-Setup anzeigen, um zu überprüfen, ob jeder korrekt konfiguriert ist. Nachdem die Konfiguration ausgeführt wurde, können Sie die Statistiken für jeden Dienst und den virtuellen Lastenausgleichsserver anzeigen, um nach möglichen Problemen zu suchen.

Anzeigen der Eigenschaften eines Serverobjekts

Sie können Eigenschaften wie den Namen, den Status und die IP-Adresse jedes Serverobjekts in Ihrer NetScaler-Appliance-Konfiguration anzeigen.

So können Sie die Eigenschaften von Serverobjekten mithilfe der Befehlszeilenschnittstelle anzeigen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show server <serverName>

show server server-1
<!--NeedCopy-->
```

So können Sie die Eigenschaften von Serverobjekten mithilfe des Konfigurationsprogramms anzeigen

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Server**. Die Parameterwerte der verfügbaren Server werden im Detailbereich angezeigt.

Eigenschaften eines virtuellen Servers anzeigen

Sie können Eigenschaften wie den Namen, den Status, den effektiven Status, die IP-Adresse, den Port, das Protokoll, die Methode und die Anzahl der gebundenen Dienste für Ihre virtuellen Server anzeigen. Wenn Sie mehr als die grundlegenden Load-Balancing-Einstellungen konfiguriert haben, können Sie die Persistenzeinstellungen für Ihre virtuellen Server, alle an sie gebundenen Richtlinien sowie alle virtuellen Cache-Umleitungs- und Content-Switching-Server einsehen, die an die virtuellen Server gebunden wurden.

So können Sie die Eigenschaften eines virtuellen Load-Balancing-Servers mithilfe der CLI anzeigen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lb vserver <name>

show lb vserver Vserver-LB-1
<!--NeedCopy-->
```


So können Sie die Eigenschaften eines virtuellen Load-Balancing-Servers mithilfe der GUI anzeigen

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server, um seine Eigenschaften unten im Detailbereich anzuzeigen.
3. Um die Cache-Umleitung und die virtuellen Server mit Content Switching anzuzeigen, die an diesen virtuellen Server gebunden sind, klicken Sie auf **CS/CR-Bindungen anzeigen**.

Anzeigen der Eigenschaften eines Dienstes

Sie können den Namen, den Status, die IP-Adresse, den Port, das Protokoll, die maximale Client-Verbindung, die maximalen Anfragen pro Verbindung und den Servertyp der konfigurierten Dienste einsehen und diese Informationen verwenden, um Fehler in der Dienstkonfiguration zu beheben.

Um die Eigenschaften von Diensten mithilfe der CLI anzuzeigen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show service <name>

show service Service-HTTP-1
<!--NeedCopy-->
```

Um die Eigenschaften von Diensten mithilfe der GUI anzuzeigen

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**. Die Details der verfügbaren Dienste werden im Bereich Dienste angezeigt.

Die Bindungen eines Dienstes anzeigen

Sie können die Liste der virtuellen Server einsehen, an die der Dienst gebunden ist. Die Bindungsinformationen enthalten auch den Namen, die IP-Adresse, den Port und den Status der virtuellen Server, an die die Dienste gebunden sind. Sie können die Bindungsinformationen verwenden, um jedes Problem mit der Bindung der Dienste an virtuelle Server zu beheben.

Um die Bindungen eines Dienstes mithilfe der CLI anzuzeigen

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show service bindings <name>

show service bindings Service-HTTP-1
<!--NeedCopy-->
```

Um die Bindungen eines Dienstes mithilfe der GUI anzuzeigen

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
2. Wählen Sie im Detailbereich den Dienst aus, dessen Bindungsinformationen Sie anzeigen möchten.
3. Klicken Sie auf der Registerkarte **Aktion** auf **Bindungen anzeigen**.

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der NetScaler-Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der eingegangenen Anfragen
- Rate der Treffer

So zeigen Sie virtuelle Serverstatistiken mithilfe der CLI an

Um eine Zusammenfassung der Statistiken für alle derzeit auf der Appliance konfigurierten virtuellen Server oder für einen einzelnen virtuellen Server anzuzeigen, geben Sie an der Befehlszeile Folgendes ein:

```
stat lb vserver [`<name>`]
<!--NeedCopy-->
```

Beispiel:

```
stat lb vserver server-1
<!--NeedCopy-->
```


Die folgende Abbildung zeigt eine Beispielstatistik.


```
> stat lbvserver
[
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
vserver1        10.102.20.200    80          SSL         DOWN      0/s

lb1               203.1.113.5   443         DTLS         DOWN      0/s

vicap                       *     0          TCP         DOWN      0/s

lbicap                2.2.3.4  1344          TCP         DOWN      0/s

app_...stest          0.0.0.0     0         HTTP         DOWN      0/s

app_...ttest          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...test1          0.0.0.0     0         HTTP         DOWN      0/s

app_...1test          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...est12          0.0.0.0     0         HTTP         DOWN      0/s

app_...sting          0.0.0.0     0         HTTP         DOWN      0/s

test                  2.2.2.2    80         HTTP         DOWN      0/s

shar...lt-lb          0.0.0.0     0         HTTP         DOWN      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ts-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ns-lb          0.0.0.0     0         HTTP           UP      0/s

shar...as-lb          0.0.0.0     0         HTTP           UP      0/s

forward-vs            0.0.0.0     0          TCP         DOWN      0/s

tcpcs                 0.0.0.0     0          TCP         DOWN      0/s

test124               0.0.0.0     0          SSL         DOWN      0/s

testssl               0.0.0.0     0          SSL         DOWN      0/s
```


So zeigen Sie Statistiken über virtuelle Server mit der GUI an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wenn Sie die Statistiken nur für einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus, dessen Statistiken Sie anzeigen möchten.
3. Klicken Sie im Detailbereich auf **Statistiken**.

Statistiken eines Dienstes anzeigen

Sie können die Rate der Anfragen, Antworten, Anforderungsbytes, Antwortbytes, aktuelle Clientverbindungen, Anfragen in der Überspannungswarteschlange, aktuelle Serververbindungen usw. mithilfe der Dienststatistiken anzeigen.

So zeigen Sie die Statistiken eines Dienstes mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Um die Statistiken eines Dienstes mithilfe der GUI anzuzeigen

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
2. Wählen Sie im Detailbereich den Dienst aus, dessen Statistiken Sie anzeigen möchten (z. B. Service-HTTP-1).
3. Klicken Sie auf **Statistiken**. Die Statistiken werden in einem neuen Fenster angezeigt.

Lastenausgleich virtueller Server und Dienststatus

August 19, 2021

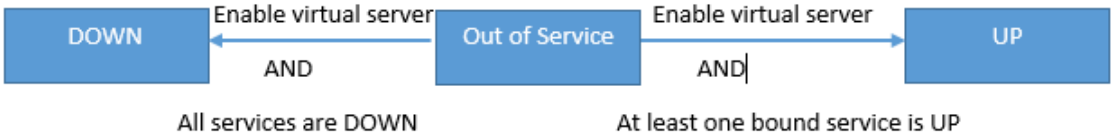
Ein virtueller Lastausgleichsserver, der keinen virtuellen Backup-Server hat, kann je nach Status der an ihn gebundenen Dienste und ob er administrativ deaktiviert ist, die folgenden Status annehmen:

- **UP**: Mindestens einer der an den virtuellen Server gebundenen Dienste ist UP.

- **DOWN**: Alle an den virtuellen Server gebundenen Dienste sind DOWN, oder die Lastausgleichsfunktion ist nicht aktiviert.
- **Out of Service (OFS)**: Wenn Sie den virtuellen Server administrativ deaktivieren, wechselt er in den OFS-Status, aber sein effektiver Status ist DOWN. Der Administrator kann den Übergang zum OFS-Status vom Status DOWN oder UP oder in den Status DOWN oder UP aus dem OFS-Status steuern.

Der Status und der effektive Status eines virtuellen Servers sind identisch, wenn ein virtueller Backupserver nicht konfiguriert ist. Wenn jedoch ein virtueller Backup-Server oder eine Kette virtueller Backup-Server konfiguriert wird, wird der effektive Status von den Status der Dienste abgeleitet, die an den primären virtuellen Server und die virtuellen Backup-Server gebunden sind. Wenn einer der virtuellen Backupserver in der Kette UP ist, ist der effektive Status des primären virtuellen Servers UP, selbst wenn alle an den primären virtuellen Server gebundenen Dienste DOWN sind.

Die folgenden Diagramme zeigen die Bedingungen, unter denen ein virtueller Server von einem Status in einen anderen übergeht.



Ein Dienst kann die folgenden Zustände annehmen:

- **UP:** Wenn Prüfpunkte von allen Monitoren, die an den Dienst gebunden sind, erfolgreich sind.
- **DOWN**: Wenn Monitorprüfungen an den Dienst nicht innerhalb der konfigurierten Frist beant-

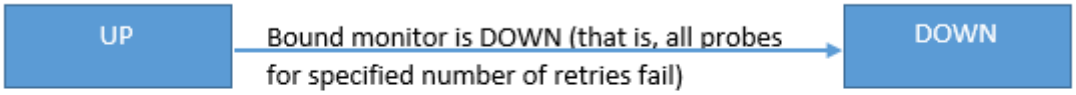
wortet werden.

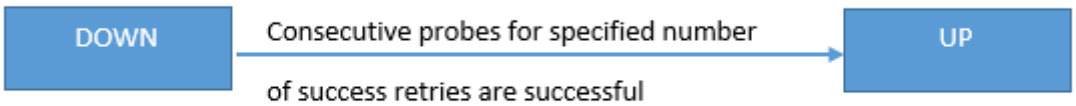
- **OUT OF SERVICE**: Wenn Sie den Dienst administrativ deaktivieren oder wenn Sie den Dienst ordnungsgemäß herunterfahren und keine aktiven Transaktionen für den Dienst vorhanden sind
- **GOING OUT OF SERVICE (TROFS)**: Wenn Sie den Dienst administrativ mit Verzögerung deaktivieren oder den Dienst ordnungsgemäß herunterfahren und aktive Transaktionen für den Dienst vorhanden sind. Weitere Informationen finden Sie unter Graceful Herunterfahren von Diensten.
- **DOWN WHEN OUT OF SERVICE (TROFS_DOWN)[]** Eine Überwachungssonde schlägt fehl, während der Dienst den Status “GOING OUT OF SERVICE” hat.

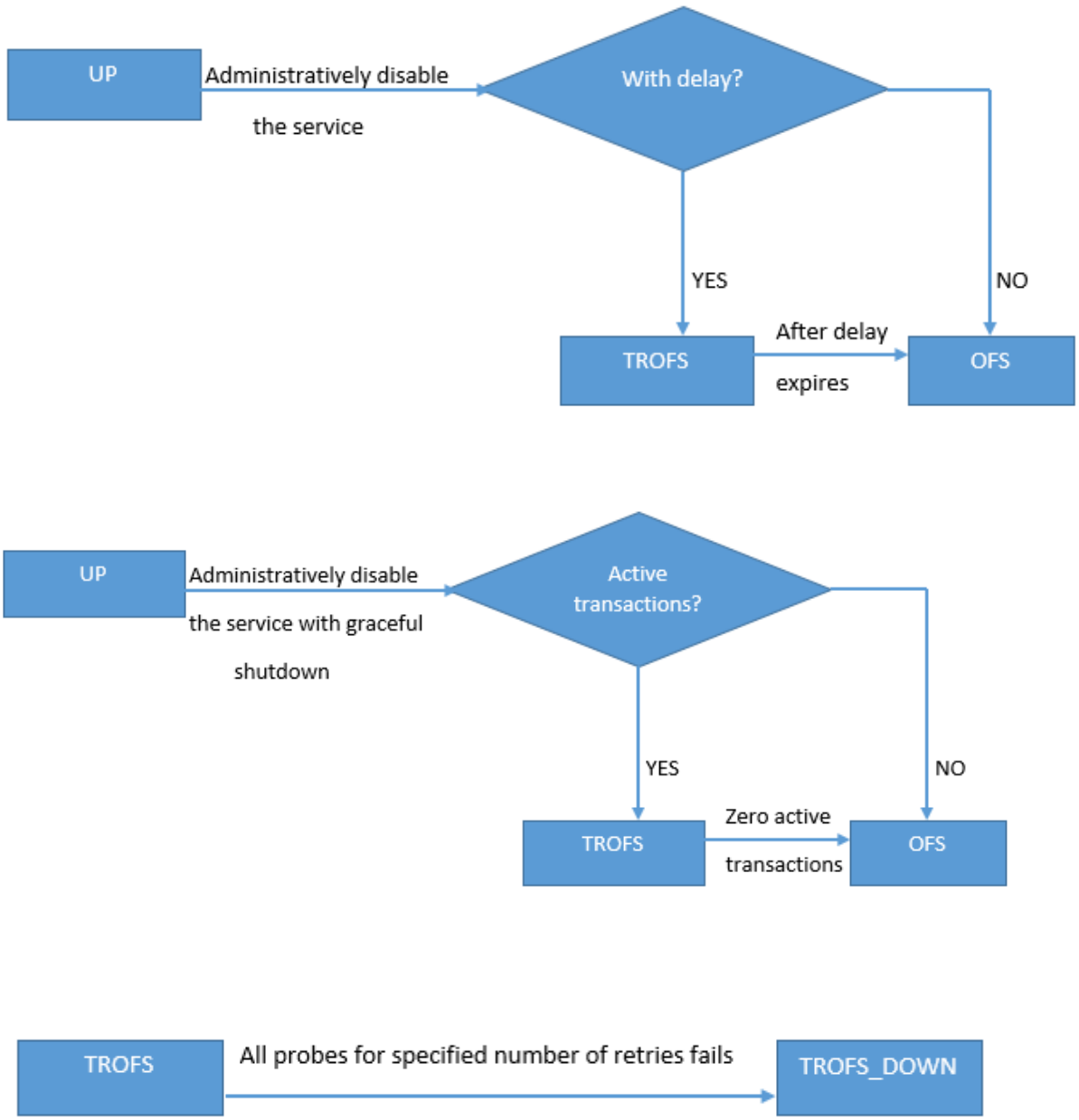
Ein Dienst beim Übergang von UP zu OFS befindet sich im Status GOING OUT OF SERVICE. Ein Dienst, der von DOWN zu OFS wechselt, befindet sich im Zustand DOWN WHEN GOING OUT OF SERVICE. Wenn ein Dienst z. B. DOWN ist und Sie ihn mit Verzögerung deaktivieren, wechselt der Dienst zu DOWN WHEN GOING OUT OF SERVICE und dann in den Zustand OUT OF SERVICE. Wenn ein Dienst UP ist und Sie ihn mit Verzögerung deaktivieren, wechselt der Dienst zu GOING OUT OF SERVICE. Wenn während dieser Zeit eine Überwachungssonde zum Server ausfällt, wechselt der Dienst zu DOWN WHEN GOING OUT OF SERVICE und tritt nach Ablauf der Verzögerungszeit in den OFS-Zustand ein.

> **Hinweis:**
>
> Sie können Spillover auf einen virtuellen Backup-Server konfigurieren, indem Sie den Parameter HealthThreshold auf einen positiven Wert ungleich Null setzen. Wenn dann ein einzelner Dienst, der an den primären virtuellen Server gebunden ist, in den Zustand DOWN WHEN GOING OUT OF SERVICE wechselt und der Integritätsschwellenwert nicht erreicht wird, wird der primäre virtuelle Server mit DOWN markiert, und neue Verbindungen werden an den virtuellen Backupserver weitergeleitet.

Die folgenden Diagramme zeigen die Bedingungen, unter denen ein Dienst von einem Status in einen anderen übergeht.







Unterstützung für Lastausgleichsprofil

June 19, 2023

Eine Load Balancing-Konfiguration hat viele Parameter, so dass das Festlegen der gleichen Parameter auf mehreren virtuellen Servern mühsam werden kann. Ab Release 11.1 erleichtert ein Load Balancing (LB) Profil diese Aufgabe. Sie können jetzt Lastausgleichsparameter in einem Profil festlegen und

dieses Profil virtuellen Servern zuordnen, anstatt diese Parameter auf jedem virtuellen Server festzulegen.

Die folgenden Parameter werden derzeit in einem LB-Profil unterstützt:

- `HTTPonlyflag`— Schließe das HttpOnly-Attribut in Persistenz-Cookies ein Das Attribut HttpOnly beschränkt den Umfang eines Cookies auf HTTP-Anforderungen und hilft dabei, das Risiko von Cross-Site-Skripting-Angriffen zu verringern.
- UseSecuredPersistenceCookie — Verschlüsseln Sie die Persistenz-Cookie-Werte mithilfe des SHA2-Hash-Algorithmus.
- `Cookiepassphrase`— Geben Sie die Passphrase an, die verwendet wird, um einen gesicherten Persistenz-Cookie-Wert zu erzeugen.
- DBS_LB — Aktiviert den datenbankspezifischen Lastausgleich für MySQL - und MSSQL-Diensttypen.
- Cl_process_local — Pakete, die für einen virtuellen Server in einem Cluster bestimmt sind, werden nicht gesteuert. Aktivieren Sie die Option für den Antwortmodus für einzelne Paketanfragen oder wenn das Upstream-Gerät einen richtigen RSS für die verbindungsbasierte Verteilung ausführt.
- lbhashalgorithm: Geben Sie den Hashing-Algorithmus an, der für die folgenden hashbasierten Load Balancing-Methoden verwendet werden soll:
  - URL-Hash-Methode
  - Domain-Hash-Methode
  - Ziel-IP-Hash-Methode
  - Quell-IP-Hash-Methode
  - Quell-IP-Ziel-IP-Hashmethode
  - Quell-IP-Quellport-Hash-Methode
  - Anruf-ID-Hash-Methode
  - Token-Methode

  Mögliche Werte: DEFAULT, PRAC, JARH
  Standardwert: DEFAULT
- LBHashfinger: Geben Sie die Anzahl der Finger an, die in PRAC- und JARH-Algorithmen für hashbasierte LB-Methoden verwendet werden sollen. Die Erhöhung der Anzahl der Finger ermöglicht eine bessere Verteilung des Datenverkehrs auf Kosten des zusätzlichen Speichers.

  Standardwert: 256
  Minimaler Wert: 1
  Maximaler Wert: 1024
- ProximityFromSelf-aktivieren Sie, um die Loopback-IP-Adresse des Netscalers anstelle der IP-Adresse des Clients zu verwenden, um den nächstgelegenen Serverstandort für den statischen

Proximity-Load-Balancing oder die GSLB-Entscheidung abzurufen.

> **Hinweis**
>
> Sie können DBS_LB und CL_Process_Local-Parameter auf einem virtuellen Server und im Profil festlegen. Wenn Sie diese Parameter auf einem virtuellen Server aktivieren und dann ein Profil für diesen virtuellen Server festlegen, werden die Parameter in der Ausgabe des `"show lb vserver"` Befehls für diesen virtuellen Server als deaktiviert angezeigt. Überprüfen Sie das Profil, um den aktuellen Status dieser Parameter zu sehen. Wenn Sie ein Profil für einen virtuellen Server festlegen und dann aufheben, werden die Parameter mit Standardwerten für diesen virtuellen Server festgelegt.

So erstellen Sie ein LB-Profil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb profile <lbprofilename> -dbsLb ( ENABLED | DISABLED ) -
    processLocal ( ENABLED | DISABLED ) -httpOnlyCookieFlag ( ENABLED |
    DISABLED ) -cookiePassphrase -useSecuredPersistenceCookie ( ENABLED
    | DISABLED ) -lbHashAlgorithm <lbHashAlgorithm> -lbHashFingers <
    positive_integer>- proximityFromSelf <NO/YES>
<!--NeedCopy-->
```

Beispiel:

```
> sh lb profile p1
LB Profile name:  p1
DBS LB : DISABLED   Process Local: DISABLED
Persistence Cookie HttpOnly Flag: ENABLED
Use Encrypted Persistence Cookie: DISABLED
Proximity From Self: ENABLED
No of vservers bound: 0
Store MQTT clientid and username in transactional logs: NO
Hash LB algorithm used in LB decision: DEFAULT
Number of fingers for Hash LB algorithm: 256
Done

<!--NeedCopy-->
```

So erstellen Sie ein LB-Profil mithilfe der GUI

Navigieren Sie zu **System** > **Profile** > **LB-Profil**und fügen Sie ein Profil hinzu.

So verknüpfen Sie ein LB-Profil mit einem virtuellen LB-Server mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -lbprofilename <string>
<!--NeedCopy-->
```

Beispiel

```
set lbvserver lbvip1 -lbprofile p1

Done

sh lb vserver lbvip1

lbvip1 (203.0.113.1:80) - HTTP       Type: ADDRESS
State: UP
Last state change was at Wed May 25 12:36:20 2016
Time since last state change: 0 days, 00:01:26.140
Effective State: UP  ARP:DISABLED
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: ENABLED
Port Rewrite : DISABLED
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION      BackupMethod: ROUNDROBIN
Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED  Push VServer:
Push Multi Clients: NO
Push Label Rule: none
L2Conn: OFF
Skip Persistency: None
Listen Policy: NONE
IcmpResponse: PASSIVE
RHIstate: PASSIVE
New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
Mac mode Retain Vlan: DISABLED
DBS_LB: DISABLED
Process Local: DISABLED
Traffic Domain: 0
LB Profile: p1
Done
<!--NeedCopy-->
```


So verknüpfen Sie ein LB-Profil mit einem virtuellen LB-Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie in **den Erweiterten Einstellungen**auf **Profile**.
4. Wählen Sie in der Liste **LB-Profil** das Profil aus, das mit diesem virtuellen Server verknüpft werden soll.

So konfigurieren Sie den Parameter Proximity from Self im Load Balancing-Profil mithilfe der GUI

Konfigurieren Sie den Parameter Proximity from Self im Profil so, dass der Parameter für die Entität aktiviert wird, wenn das Profil an die Entität angehängt wird.

1. Navigieren Sie zu **System** > **Profil** > **LB-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie **Proximity von Self aus**.
4. Klicken Sie auf **OK**.

Load Balancing-Algorithmen

May 11, 2023

Der Load-Balancing-Algorithmus definiert die Kriterien, anhand derer die NetScaler-Appliance den Dienst auswählt, an den jede Client-Anfrage umgeleitet werden soll. Verschiedene Load-Balancing-Algorithmen verwenden unterschiedliche Kriterien. Beispielsweise wählt der Algorithmus mit der geringsten Verbindung den Dienst mit den wenigsten aktiven Verbindungen aus, während der Round-Robin-Algorithmus eine laufende Warteschlange mit aktiven Diensten verwaltet, jede Verbindung an den nächsten Dienst in der Warteschlange verteilt und diesen Dienst dann an das Ende der Warteschlange sendet.

Einige Load-Balancing-Algorithmen eignen sich am besten für den Verkehr auf Websites, andere für die Verwaltung des Datenverkehrs zu DNS-Servern und andere für die Verwaltung komplexer Webanwendungen, die im E-Commerce oder in Unternehmens-LANs oder WANs verwendet werden. In der folgenden Tabelle sind alle Load-Balancing-Algorithmen aufgeführt, die die NetScaler-Appliance unterstützt, mit einer kurzen Beschreibung ihrer Funktionsweise.

Name	Serverauswahl basierend auf
GERINGSTE VERBINDUNG	Welcher Dienst hat derzeit die wenigsten Client-Verbindungen. Dies ist der Standard-Load-Balancing-Algorithmus.
ROUNDROBIN	Welcher Dienst steht ganz oben auf einer Liste von Diensten. Nachdem dieser Dienst für eine Verbindung ausgewählt wurde, wird er an das Ende der Liste verschoben.
GERINGSTE REAKTIONSZEIT	Welcher Server mit Lastausgleich hat derzeit die schnellste Reaktionszeit.
URL-HASH	Ein Hash der Ziel-URL.
DOMAIN-HASH	Ein Hash der Zieldomain.
DESTINATIONIPHASH	Ein Hash der Ziel-IP-Adresse.
SOURCEIPHASH	Ein Hash der Quell-IP-Adresse.
SRCIPDESTIPHASH	Ein Hash der Quell- und Ziel-IP-Adressen.
CALLIDHASH	Ein Hash der Anruf-ID im SIP-Header.
SCRIPT SRCPORTHASH	Ein Hash der IP-Adresse und des Port des Clients.
LEASTBANDWIDTH	Welcher Dienst hat derzeit die wenigsten Bandbreitenbeschränkungen.
LEASTPACKETS	Welcher Dienst empfängt derzeit die wenigsten Pakete.
BENUTZERDEFINIERTE LADUNG	Daten von einem Lastmonitor.
WERTMARKE	Das konfigurierte Token.
LRTM	Die wenigsten aktiven Verbindungen und die niedrigste durchschnittliche Reaktionszeit.

Abhängig vom Protokoll des Dienstes, bei dem es sich um einen Lastenausgleich handelt, richtet die NetScaler-Appliance jede Verbindung zwischen Client und Server so ein, dass sie für ein anderes Zeitintervall besteht. Dies wird als Load-Balancing-Granularität bezeichnet. Es gibt drei Typen: anforderungsbasierte, verbindungsbasierte und zeitbasierte Granularität. In der folgenden Tabelle werden die einzelnen Granularitätstypen beschrieben und wann sie verwendet werden.

Granularität	Arten von Load Balanced-Diensten	Spezifiziert
Auf Anfrage	HTTP oder HTTPS	Für jede HTTP-Anfrage wird unabhängig von TCP-Verbindungen ein neuer Dienst ausgewählt. Wie bei allen HTTP-Anfragen wird die Verbindung geschlossen, nachdem der Webserver die Anfrage erfüllt hat.
Verbindungsbasiert	TCP und TCP-basierte Protokolle außer HTTP	Für jede neue TCP-Verbindung wird ein Dienst ausgewählt. Die Verbindung bleibt bestehen, bis sie entweder vom Dienst oder vom Client beendet wird.
Zeitbasiert	UDP und andere IP-Protokolle	Für jedes UDP-Paket wird ein neuer Dienst ausgewählt. Bei Auswahl eines Dienstes wird eine Sitzung zwischen dem Dienst und einem Client für einen bestimmten Zeitraum erstellt. Wenn die Zeit abgelaufen ist, wird die Sitzung gelöscht und ein neuer Dienst für zusätzliche Pakete ausgewählt, selbst wenn diese Pakete vom selben Client stammen.

Beim Start eines virtuellen Servers oder wenn sich der Status eines virtuellen Servers ändert, kann der virtuelle Server zunächst die Round-Robin-Methode verwenden, um die Client-Anfragen auf die physischen Server zu verteilen. Diese Art der Verteilung, die als *Startup-Round-Robin bezeichnet wird, trägt dazu bei,* unnötige Belastung eines einzelnen Servers zu vermeiden, wenn die ersten Anfragen bearbeitet werden. Nachdem der virtuelle Server beim Start die Round-Robin-Methode verwendet hat, wechselt er zu der auf dem virtuellen Server angegebenen Load-Balancing-Methode.

Der Startup RR Factor funktioniert auf folgende Weise:

- Wenn der Startup-RR-Faktor auf Null gesetzt ist, wechselt die Appliance je nach Anforderungsrate zur angegebenen Load-Balancing-Methode.
- Wenn der Start-RR-Faktor eine andere Zahl als Null ist, verwendet die Appliance die Round-Robin-Methode für die angegebene Anzahl von Anfragen, bevor sie zur angegebenen Load-Balancing-Methode wechselt.
- Standardmäßig ist der Startup RR Factor auf Null gesetzt.

Hinweis: Sie können den Start-RR-Faktor nicht für einen einzelnen virtuellen Server festlegen. Der von Ihnen angegebene Wert gilt für alle virtuellen Server auf der NetScaler-Appliance.

So legen Sie den Round-Robin-Faktor beim Starten mithilfe der CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb parameter -startupRRFactor <positive_integer>
```

Beispiel

```
set lb parameter -startupRRFactor 25000
```

So legen Sie den Round-Robin-Faktor beim Starten mithilfe der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Lastenausgleichsparameter konfigurieren**, und legen Sie den Start-RR-Faktor fest.

Kleinste Verbindungsmethode

May 11, 2023

Wenn ein virtueller Server so konfiguriert ist, dass er den Algorithmus (oder die Methode) für den Lastenausgleich mit den wenigsten Verbindungen verwendet, wählt er den Dienst mit den wenigsten aktiven Verbindungen aus. Dies ist die Standardmethode, da sie in den meisten Fällen die beste Leistung bietet.

Für TCP-, HTTP-, HTTPS- und SSL_TCP-Dienste nimmt die NetScaler-Appliance die folgenden Verbindungstypen in ihre Liste der vorhandenen Verbindungen auf:

- **Aktive Verbindungen zu einem Dienst.** Verbindungen, die Anfragen darstellen, die ein Client an den virtuellen Server gesendet hat und die der virtuelle Server an einen Dienst weitergeleitet hat. Bei HTTP- und HTTPS-Diensten stellen aktive Verbindungen nur die HTTP- oder HTTPS-Anfragen dar, die noch keine Antwort erhalten haben.

- **Wartende Verbindungen in der Überspannungswarteschlange.** Alle Verbindungen zum virtuellen Server, die in einer Warteschlange warten und noch nicht an einen Dienst weitergeleitet wurden. In der Überspannungswarteschlange können sich aus einem der folgenden Gründe jederzeit Verbindungen aufbauen:
  - Ihre Dienste haben Verbindungslimits, und alle Dienste in Ihrer Load-Balancing-Konfiguration haben dieses Limit.
  - Die Überspannungsschutzfunktion ist konfiguriert und wurde durch einen Anstieg der Anfragen an den virtuellen Server aktiviert.
  - Der Load-Balancing-Server hat ein internes Limit erreicht und öffnet daher keine neuen Verbindungen. (Beispielsweise ist das Verbindungslimit eines Apache-Servers erreicht.)

Wenn ein virtueller Server die Methode der geringsten Verbindung verwendet, betrachtet er die wartenden Verbindungen als zum jeweiligen Dienst gehörend. Daher werden keine neuen Verbindungen zu diesen Diensten geöffnet.

Bei UDP-Diensten umfassen die Verbindungen, die der Algorithmus mit der geringsten Verbindung berücksichtigt, alle Sitzungen zwischen dem Client und einem Dienst. Diese Sitzungen sind logische, zeitbasierte Einheiten. Wenn das erste UDP-Paket in einer Sitzung eintrifft, erstellt die NetScaler-Appliance eine Sitzung zwischen der Quell-IP-Adresse und dem Port sowie der Ziel-IP-Adresse und dem Port.

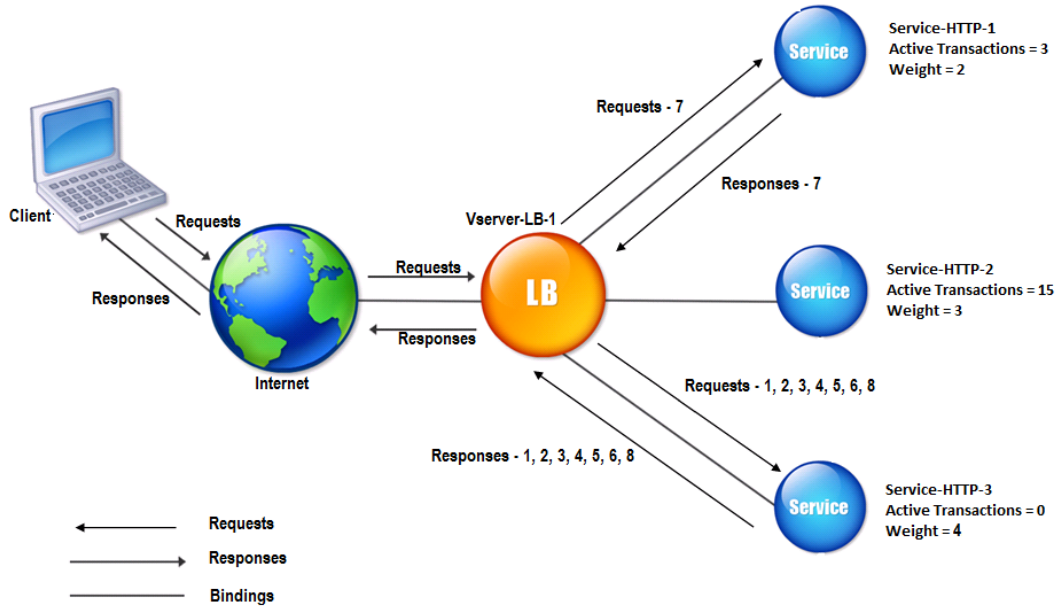
Für RTSP-Verbindungen (Real-Time Streaming Protocol) verwendet die NetScaler-Appliance die Anzahl der aktiven Kontrollverbindungen, um die niedrigste Anzahl von Verbindungen zu einem RTSP-Dienst zu ermitteln.

Das folgende Beispiel zeigt, wie ein virtueller Server einen Dienst für den Lastenausgleich auswählt, indem er die Methode der geringsten Verbindung verwendet. Betrachten Sie die folgenden drei Dienste:

- Service-HTTP-1 verarbeitet 3 aktive Transaktionen.
- Service-HTTP-2 verarbeitet 15 aktive Transaktionen.
- Service-HTTP-3 verarbeitet keine aktiven Transaktionen.

Das folgende Diagramm zeigt, wie die NetScaler-Appliance eingehende Anfragen weiterleitet, wenn die Methode mit der geringsten Verbindung verwendet wird.

Abbildung 1. Mechanismus der Load-Balancing-Methode mit den wenigsten Verbindungen



In diesem Diagramm wählt der virtuelle Server den Dienst für jede eingehende Verbindung aus, indem er den Server mit den wenigsten aktiven Transaktionen auswählt.

Verbindungen werden wie folgt weitergeleitet:

- Service-HTTP-3 empfängt die erste Anforderung, da es keine aktiven Transaktionen verarbeitet.

  Hinweis: Der Dienst ohne aktive Transaktion wird zuerst ausgewählt.

- Service-HTTP-3 empfängt die zweite und dritte Anforderung, da der Dienst die nächstgeringste Anzahl von aktiven Transaktionen hat.
- Service-HTTP-1 erhält die vierte Anforderung, da Service-HTTP-1 und Service-HTTP-3 die gleiche Anzahl aktiver Transaktionen haben, der virtuelle Server verwendet die Round-Robin-Methode, um zwischen ihnen zu wählen.
- Service-HTTP-3 empfängt die fünfte Anforderung.
- Service-http-1 empfängt die sechste Anforderung usw., bis sowohl Service-http-1 als auch Service-http-3 dieselbe Anzahl von Anforderungen verarbeiten wie Service-http-2. Dann beginnt die NetScaler Appliance mit der Weiterleitung von Anfragen an Service-HTTP-2, wenn es sich um den am wenigsten geladenen Dienst handelt oder in der Round-Robin-Warteschlange an der Reihe ist.

  Hinweis: Wenn Verbindungen zu Service-HTTP-2 geschlossen werden, werden möglicherweise neue Verbindungen erhalten, bevor jeder der beiden anderen Dienste 15 aktive Transaktionen

aufweist.

In der folgenden Tabelle wird erläutert, wie Verbindungen in dem zuvor beschriebenen Load Balancing-Setup mit drei Diensten verteilt werden.

Eingehende Verbindung	Ausgewählter Dienst	Aktuelle Anzahl aktiver Verbindungen	Bemerkungen
Request-1	Service-HTTP-3; (N = 0)	1	Service-HTTP-3 hat die wenigsten aktiven Verbindungen.
Request-2	Service-HTTP-3; (N = 1)	2	Service-HTTP-3 hat die wenigsten aktiven Verbindungen.
Request-3	Service-HTTP-3; (N = 2)	3	-
Request-4	Service-HTTP-1; (N = 3)	4	Service-HTTP-1 und Service-HTTP-3 haben dieselbe Anzahl aktiver Verbindungen.
Request-5	Service-HTTP-3; (N = 3)	4	Service-HTTP-1 und Service-HTTP-3 haben dieselbe Anzahl aktiver Verbindungen.
Request-6	Service-HTTP-1; (N = 4)	5	-
Request-7	Service-HTTP-3; (N = 4)	5	-
Request-8	Service-HTTP-1; (N = 5)	6	-

Service-HTTP-2 wird für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt und die aktuellen Verbindungen zu ihm geschlossen werden oder wenn die anderen Dienste (Service-HTTP-1 und Service-HTTP-3) jeweils 15 oder mehr Verbindungen haben.

Die NetScaler-Appliance kann auch die Methode mit der geringsten Verbindung verwenden, wenn Diensten Gewichtungen zugewiesen werden. Es wählt einen Dienst aus, indem es den Wert (Nw) des folgenden Ausdrucks verwendet:

Nw = (Anzahl der aktiven Transaktionen) * (10000/Gewicht)

Das folgende Beispiel zeigt, wie die NetScaler-Appliance einen Dienst für den Lastenausgleich auswählt, indem sie die Methode der geringsten Verbindung verwendet, wenn Diensten Gewichtungen zugewiesen werden. Nehmen wir im vorherigen Beispiel an, Service-HTTP-1 wird eine Gewichtung von 2 zugewiesen, Service-HTTP-2 wird eine Gewichtung von 3 zugewiesen und Service-HTTP-3 wird eine Gewichtung von 4 zugewiesen. Verbindungen werden wie folgt weitergeleitet:

- Service-HTTP-3 erhält die erste, da der Dienst keine aktiven Transaktionen verarbeitet.

  Hinweis: Wenn die Dienste keine aktiven Transaktionen abwickeln, verwendet die NetScaler Appliance die Round-Robin-Methode unabhängig von den Gewichten, die jedem der Dienste zugewiesen sind.

- Service-HTTP-3 erhält die zweite, dritte, vierte, fünfte, sechste und siebte Anforderung, da der Dienst den niedrigsten Nw-Wert aufweist.
- Service-HTTP-1 empfängt die achte Anforderung. Da Service-HTTP-1 und Service-HTTP-3 jetzt denselben Nw-Wert haben, führt die Appliance Load Balancing auf Round-Robin-Weise durch. Daher erhält Service-HTTP-3 die neunte Anforderung.

In der folgenden Tabelle wird erläutert, wie Verbindungen für das zuvor beschriebene Drei-Service-Load Balancing-Setup verteilt werden.

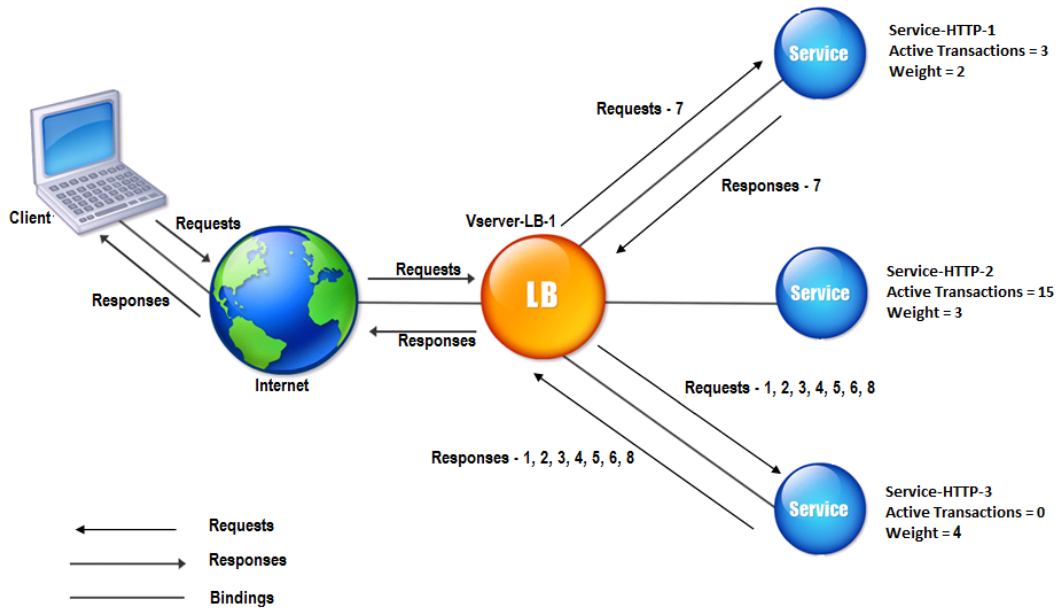
Anfrage erhalten	Ausgewählter Dienst	Aktueller Nw-Wert (Anzahl der aktiven Transaktionen) * (10000/Gewicht)	Bemerkungen
Request-1	service-HTTP-3; (Jetzt = 0)	Nw = 2500	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-2	service-HTTP-3; (Nw = 2500)	Neu = 5000	
Request-3	Service-HTTP-3; (Nw = 5000)	Nw = 7500	
Request-4	Service-HTTP-3; (Jetzt = 7500)	Neu = 10000	
Request-5	Service-HTTP-3; (Nw = 10000)	Nw = 12500	
Request-6	Service-HTTP-3; (Nw = 12500)	Nw = 15000	

Anfrage erhalten	Ausgewählter Dienst	Aktueller Nw-Wert (Anzahl der aktiven Transaktionen) * (10000/Gewicht)	Bemerkungen
Request-7	Service-HTTP-1; (Nw = 15000)	Neu = 20000	Service-HTTP-1 und Service-HTTP-3 haben dieselben Nw-Werte
Request-8	Service-HTTP-3; (Nw = 15000)	Nw = 17500	

Service-HTTP-2 wird für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn der Nw-Wert anderer Dienste (Service-HTTP-1 und Service-HTTP-3) 50000 beträgt.

Das folgende Diagramm zeigt, wie die NetScaler-Appliance die Methode der geringsten Verbindung verwendet, wenn den Diensten Gewichtungen zugewiesen werden.

Abbildung 2. Mechanismus der Load Balancing-Methode Lost Connections, wenn Gewichtungen zugewiesen werden



Informationen zum Konfigurieren der kleinsten Verbindungsmethode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

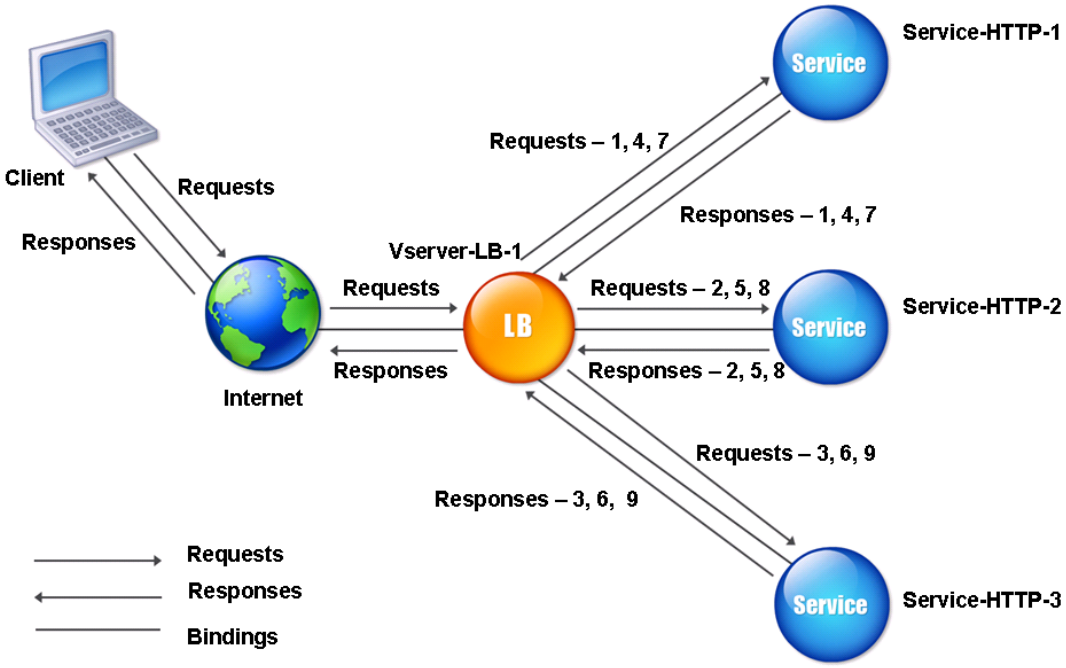
Round-Robin-Methode

May 11, 2023

Wenn ein virtueller Lastausgleichsserver für die Verwendung der Round-Robin-Methode konfiguriert ist, rotiert er kontinuierlich eine Liste der Dienste, die an ihn gebunden sind. Wenn der virtuelle Server eine Anforderung empfängt, weist er die Verbindung dem ersten Dienst in der Liste zu und verschiebt diesen Dienst dann an das Ende der Liste.

Das folgende Diagramm zeigt, wie die NetScaler Appliance die Round-Robin-Methode mit einem Load-Balancing-Setup verwendet, das drei Loadbalancing-Server und die zugehörigen Dienste enthält.

Abbildung 1. Funktionsweise der Round-Robin-Load Balancing-Methode



Wenn Sie jedem Dienst ein anderes Gewicht zuweisen, führt die NetScaler Appliance die gewichtete Round-Robin-Verteilung eingehender Verbindungen durch. Dies geschieht, indem die niedriger gewichteten Dienste in geeigneten Intervallen übersprungen werden.

Nehmen wir zum Beispiel an, dass Sie ein Load-Balancing-Setup mit drei Diensten haben. Sie legen Service-HTTP-1 auf eine Gewichtung von 2, Service-HTTP-2 auf eine Gewichtung von 3 und Service-HTTP-3 auf eine Gewichtung von 4 fest. Die Dienste sind an vServer-LB-1 gebunden, das für die Ver-

wendung der Round-Robin-Methode konfiguriert ist. Mit diesem Setup werden eingehende Anfragen wie folgt zugestellt:

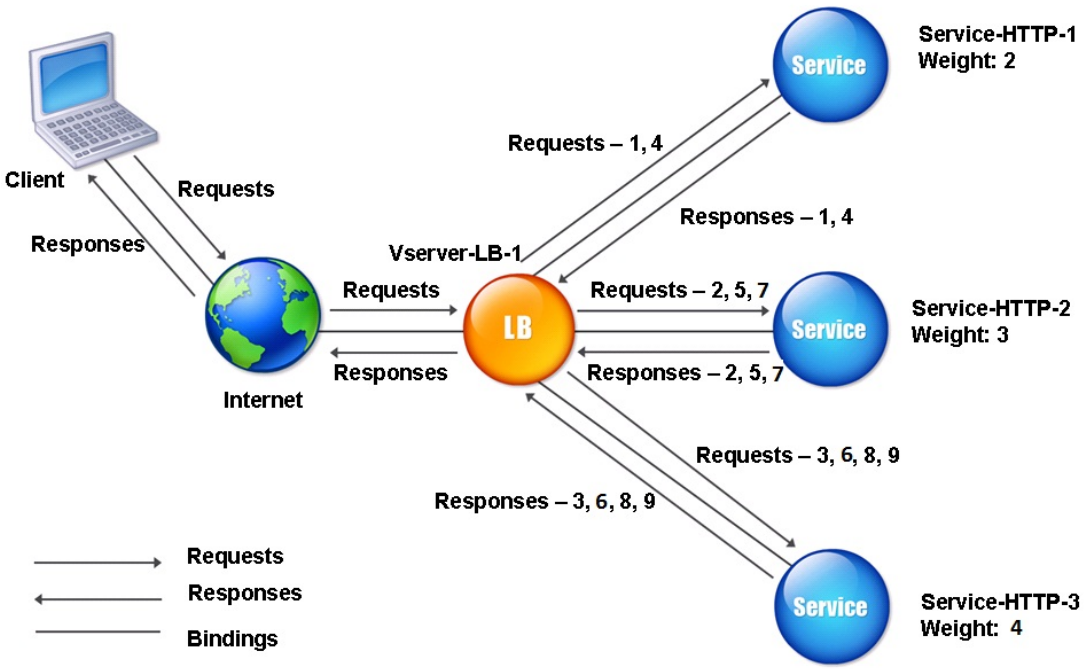
- Service-HTTP-1 empfängt die erste Anfrage.
- Service-HTTP-2 empfängt die zweite Anfrage.
- Service-HTTP-3 empfängt die dritte Anfrage.
- Service-HTTP-1 empfängt die vierte Anforderung.
- Service-HTTP-2 empfängt die fünfte Anforderung.
- Service-HTTP-3 empfängt die sechste Anfrage.
- Service-HTTP-2 empfängt die siebte Anfrage.
- Service-HTTP-3 empfängt sowohl die achte als auch die neunte Anfrage.

> **Hinweis**:
>
> Sie können auch Gewichtungen für Dienste konfigurieren, um zu verhindern, dass mehrere Dienste denselben Server verwenden und den Server überlasten.

Dann beginnt ein neuer Zyklus, der dasselbe Muster verwendet.

Das folgende Diagramm veranschaulicht die gewichtete Round-Robin-Methode.

Abbildung 2. Wie die Round Robin Load Balancing-Methode Gewichtete Dienste unterstützt



Informationen zum Konfigurieren der Round-Robin-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Methode der geringsten Reaktionszeit

May 11, 2023

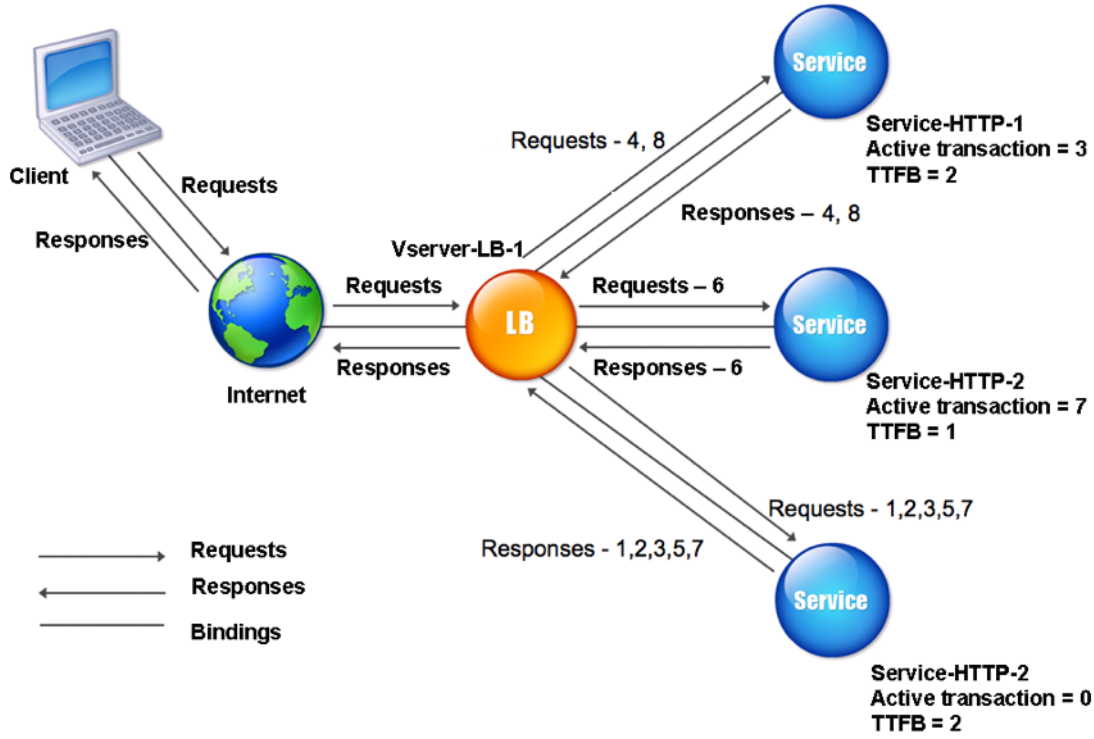
Wenn der virtuelle Load Balancing-Server so konfiguriert ist, dass er die Methode mit der geringsten Antwortzeit verwendet, wählt er den Dienst mit den wenigsten aktiven Verbindungen und der niedrigsten durchschnittlichen Antwortzeit aus. Sie können diese Methode nur für virtuelle HTTP- und Secure Sockets Layer (SSL) -Lastausgleichsserver konfigurieren. Die Antwortzeit (auch Time to First Byte oder TTFB genannt) ist das Zeitintervall zwischen dem Senden eines Anforderungspakets an einen Dienst und dem Empfang des ersten Antwortpakets vom Dienst. Die NetScaler Appliance verwendet den Antwortcode 200, um den TTFB zu berechnen.

Das folgende Beispiel zeigt, wie ein virtueller Server einen Dienst für den Lastenausgleich auswählt, indem er die Methode mit der geringsten Antwortzeit verwendet. Betrachten Sie die folgenden drei Dienste:

- Service-HTTP-1 verarbeitet drei aktive Transaktionen und TTFB dauert zwei Sekunden.
- Service-HTTP-2 verarbeitet sieben aktive Transaktionen und TTFB ist eine Sekunde.
- Service-HTTP-3 verarbeitet keine aktiven Transaktionen und TTFB dauert zwei Sekunden.

Das folgende Diagramm zeigt, wie die NetScaler-Appliance die Methode mit der geringsten Antwortzeit verwendet, um die Verbindungen weiterzuleiten.

Abbildung 1. Funktionsweise der Load Balancing-Methode für die geringste Antwortzeit



Der virtuelle Server wählt einen Dienst aus, indem die Anzahl der aktiven Transaktionen mit dem TTFB für jeden Dienst multipliziert und dann den Dienst mit dem niedrigsten Ergebnis ausgewählt wird. Für das oben gezeigte Beispiel leitet der virtuelle Server Anfragen wie folgt weiter:

- Service-HTTP-3 empfängt die erste Anforderung, da der Dienst keine aktiven Transaktionen verarbeitet.
- Service-HTTP-3 erhält auch die zweite und dritte Anforderung, da das Ergebnis der niedrigste der drei Dienste ist.
- Service-HTTP-1 empfängt die vierte Anforderung. Da Service-HTTP-1 und Service-HTTP-3 dasselbe Ergebnis haben, wählt die NetScaler-Appliance zwischen ihnen, indem sie die Round-Robin-Methode anwendet.
- Service-HTTP-3 empfängt die fünfte Anforderung.
- Service-HTTP-2 empfängt die sechste Anfrage, da es zu diesem Zeitpunkt das niedrigste Ergebnis hat.
- Da Service-http-1, Service-http-2 und Service-http-3 zu diesem Zeitpunkt alle dasselbe Ergebnis haben, wechselt die Appliance zur Roundrobin-Methode und verteilt weiterhin Verbindungen mit dieser Methode.

In der folgenden Tabelle wird erläutert, wie Verbindungen in dem zuvor beschriebenen Load Balancing-Setup mit drei Diensten verteilt werden.

Anfrage erhalten	Ausgewählter Dienst	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-1	Service-HTTP-3; (N = 0)	N = 2	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-3	Service-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-4	Service-HTTP-1; (N = 6)	N = 8	Service-HTTP-1 und Service-HTTP-3 haben dieselben N-Werte. Die Appliance verwendet die Round-Robin-Methode, um die Anfragen zu verteilen.
Request-5	Service-HTTP-3; (N = 6)	N = 8	Service-HTTP-1 und Service-HTTP-3 haben dieselben N-Werte.
Request-6	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 hat den niedrigsten N-Wert.

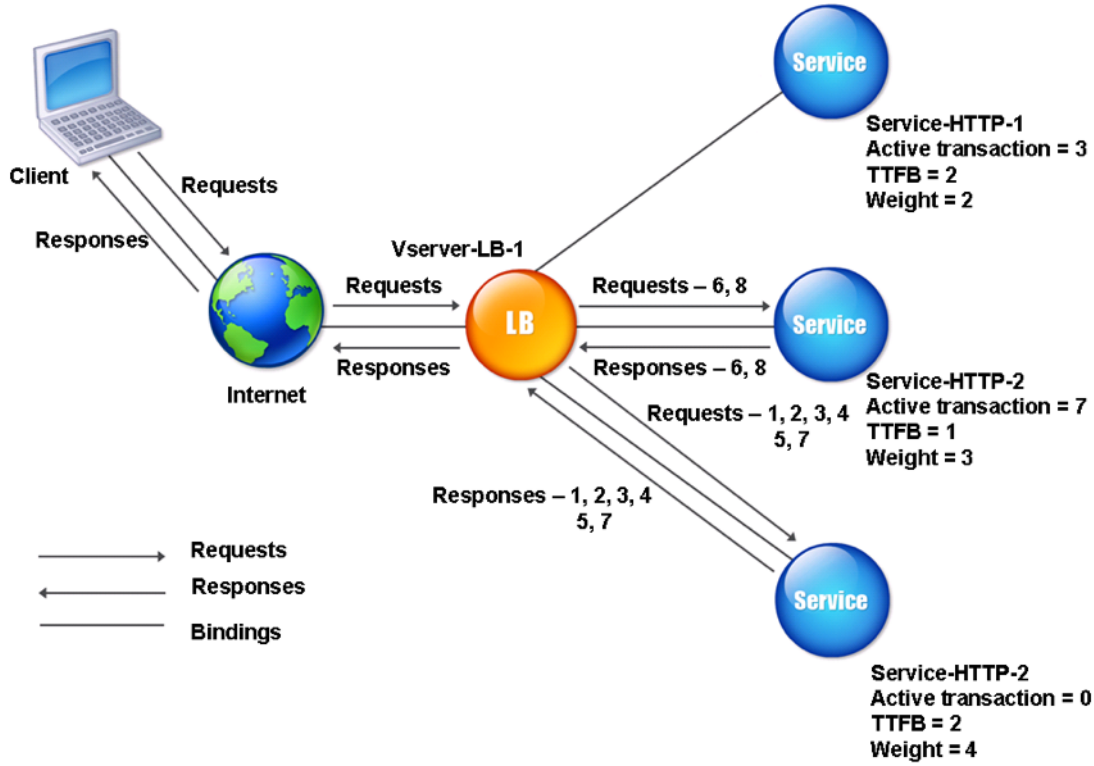
Anfrage erhalten	Ausgewählter Dienst	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-7	Service-HTTP-3; (N = 8)	N = 10	Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte. Die NetScaler-Appliance verwendet die Round-Robin-Methode, um die Anfragen zu verteilen.
Request-8	Service-HTTP-1; (N = 8)	N = 10	Service-HTTP-1 und Service-HTTP-2 haben dieselben N-Werte, die Appliance verwendet die Round-Robin-Methode, um die Anfragen zu verteilen.

Service-HTTP-1 wird erneut für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn sein N-Wert niedriger ist als der der anderen Dienste (Service-HTTP-2 und Service-HTTP-3).

Auswahl der Dienstleistungen bei der Gewichtserteilung

Das folgende Diagramm zeigt, wie die NetScaler-Appliance die Methode mit der geringsten Reaktionszeit verwendet, wenn Gewichtungen zugewiesen werden.

Abbildung 2. Funktionsweise der Load Balancing-Methode für die geringste Antwortzeit bei Zuweisung von Gewichten



Der virtuelle Server wählt einen Dienst mithilfe des Wertes (Nw) im folgenden Ausdruck aus:

Nw = (N) * (10000/Gewicht), wobei N = (Anzahl der aktiven Transaktionen * TTFB)

Angenommen, Service-HTTP-1 wird eine Gewichtung von 2 zugewiesen, Service-HTTP-2 wird Gewicht von 3 zugewiesen und Service-HTTP-3 wird Gewicht von 4 zugewiesen.

Die NetScaler-Appliance verteilt Anfragen wie folgt:

- Service-HTTP-3 empfängt die erste Anforderung, da es keine aktiven Transaktionen verarbeitet.

  Wenn die Dienste keine aktiven Transaktionen abwickeln, wählt die Appliance sie unabhängig von den ihnen zugewiesenen Gewichten aus.
- Service-http-3 empfängt die zweite, dritte, vierte und fünfte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die sechste Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-3 empfängt die siebte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.

Service-HTTP-1 hat das niedrigste Gewicht und daher den höchsten Nw-Wert, so dass der virtuelle Server ihn nicht für den Lastenausgleich auswählt.

In der folgenden Tabelle wird erläutert, wie Verbindungen in dem zuvor beschriebenen Load Balancing-Setup mit drei Diensten verteilt werden.

Anfrage erhalten	Ausgewählter Dienst	Aktueller neuer Wert = (N) * (10000/Gewicht)	Bemerkungen
Request-1	service-HTTP-3; (Jetzt = 0)	Neu = 5000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-2	service-HTTP-3; (Nw = 5000)	Neu = 10000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-3	Service-HTTP-3; (Nw = 10000)	Nw = 15000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-4	Service-HTTP-3; (Nw = 15000)	Neu = 20000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-5	Service-HTTP-3; (Jetzt = 20000)	Neu = 25000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-6	service-HTTP-2; (Jetzt = 23333.34)	Jetzt = 26666.67	Service-HTTP-2 hat den niedrigsten Nw-Wert.
Request-7	Service-HTTP-3; (Jetzt = 25000)	Nw = 30000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-8	service-HTTP-2; (Jetzt = 26666.67)	Neu = 30000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Service-HTTP-1 wird für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn sein Nw-Wert niedriger ist als bei anderen Diensten (Service-HTTP-2 und Service-HTTP-3).

So konfigurieren Sie die Load-Balancing-Methode mit der geringsten Reaktionszeit mithilfe der CLI

Geben Sie in der Befehlszeile ein;

```
set lb vserver <name> -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

So konfigurieren Sie die Load-Balancing-Methode mit der geringsten Reaktionszeit mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **LEASTRESPONSETIME**aus.

Weitere Informationen zum Konfigurieren von Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

LRTM-Methode

May 11, 2023

Hinweis: LRTM steht für Least Response Time Method Using Monitore (LRTM).

Wenn ein virtueller Lastausgleichsserver für die Verwendung der LRTM-Methode konfiguriert ist, verwendet er die vorhandene Überwachungsinfrastruktur, um die schnellste Reaktionszeit zu erzielen. Der virtuelle Load-Balancing-Server wählt dann den Dienst mit der geringsten Anzahl aktiver Transaktionen und der niedrigsten Antwortzeit aus. Bevor Sie die LRTM-Methode verwenden, müssen Sie anwendungsspezifische Monitore an jeden Dienst binden und den LRTM-Modus auf diesen Monitoren aktivieren. Die NetScaler-Appliance trifft dann Entscheidungen zum Lastenausgleich auf der Grundlage der Antwortzeiten, die sie anhand von Überwachungstests berechnet.

Sie können die LRTM-Methode auch verwenden, um Nicht-HTTP- und Nicht-HTTPS-Dienste auszubalancieren. Sie können diese Methode auch verwenden, wenn mehrere Monitore an einen Dienst gebunden sind. Jeder Monitor bestimmt die Reaktionszeit anhand des Protokolls, das er für den Dienst misst, an den er gebunden ist. Der virtuelle Server berechnet dann eine durchschnittliche Antwortzeit für diesen Dienst, indem die Ergebnisse gemittelt werden.

In der folgenden Tabelle wird zusammengefasst, wie die Reaktionszeiten für die verschiedenen Monitore berechnet werden.

Überwachung	Berechnung der Reaktionszeit
PING	Zeitunterschied zwischen der ICMP ECHO-Anfrage und der ICMP ECHO-Antwort.
TCP	Zeitunterschied zwischen der SYN-Anfrage und der SYN+ACK-Antwort.
HTTP	Zeitunterschied zwischen der HTTP-Anfrage (nachdem die TCP-Verbindung hergestellt wurde) und der HTTP-Antwort.
TCP-ECV	Zeitunterschied zwischen dem Zeitpunkt, zu dem die Daten-Sendezeichenfolge gesendet wird und der Datenempfangszeichenfolge zurückgegeben wird. Es wird davon ausgegangen, dass ein TCP-ECV-Monitor ohne die Sende- und Empfangszeichenfolgen eine falsche Konfiguration hat.
HTTP-ECV	Zeitunterschied zwischen der HTTP-Anfrage und der HTTP-Antwort.
UDP-ECV	Zeitunterschied zwischen der Sendezeichenfolge des UDP und der Empfangszeichenfolge. Ein UDP-ECV-Monitor ohne Empfangszeichenfolge wird als falsch konfiguriert.
DNS	Zeitunterschied zwischen einer DNS-Anfrage und der DNS-Antwort.
TCPS	Zeitunterschied zwischen einer SYN-Anfrage und dem Abschluss des SSL-Handshakes.
FTP	Zeitunterschied zwischen dem Senden des Benutzernamens und dem Abschluss der Benutzerauthentifizierung.
HTTPS (überwacht HTTPS-Anfragen)	Der Zeitunterschied ist der gleiche wie für den HTTP-Monitor.
HTTPS-ECV (überwacht HTTPS-Anfragen)	Der Zeitunterschied ist der gleiche wie beim HTTP-ECV-Monitor

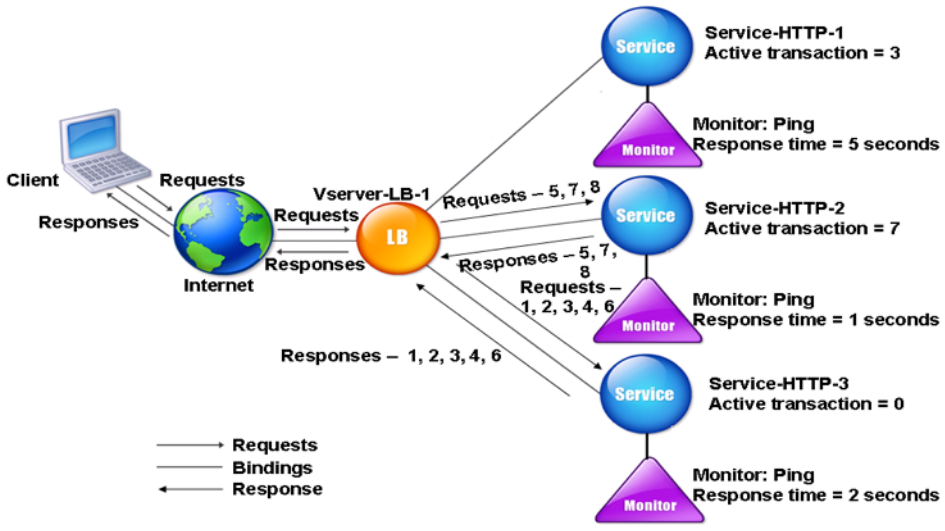
Überwachung	Berechnung der Reaktionszeit
USER	Zeitunterschied zwischen dem Zeitpunkt, zu dem eine Anfrage an den Dispatcher gesendet wird, und dem Zeitpunkt, zu dem die Antwort des Dispatchers empfangen wird.

Das folgende Beispiel zeigt, wie die NetScaler-Appliance mithilfe der LRTM-Methode einen Dienst für den Lastenausgleich auswählt. Betrachten Sie die folgenden drei Dienste:

- Service-HTTP-1 verarbeitet 3 aktive Transaktionen und die Antwortzeit beträgt fünf Sekunden.
- Service-HTTP-2 verarbeitet 7 aktive Transaktionen und die Antwortzeit beträgt eine Sekunde.
- Service-HTTP-3 verarbeitet keine aktiven Transaktionen und die Antwortzeit beträgt zwei Sekunden.

Das folgende Diagramm veranschaulicht den Prozess, dem die NetScaler-Appliance folgt, wenn sie Anfragen weiterleitet.

Abbildung 1. Funktionsweise der LRTM-Methode



Der virtuelle Server wählt einen Dienst mithilfe des Wertes (N) im folgenden Ausdruck aus:

N = (Anzahl der aktiven Transaktionen * Reaktionszeit, die vom Monitor bestimmt wird)

Der virtuelle Server stellt Anfragen wie folgt aus:

- Service-HTTP-3 erhält die erste Anforderung, da dieser Dienst keine aktive Transaktion verarbeitet.

- Service-HTTP-3 erhält die zweite, dritte und vierte Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Service-HTTP-2 empfängt die fünfte Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Da sowohl Service-HTTP-2 als auch Service-HTTP-3 derzeit denselben N-Wert haben, wechselt die NetScaler Appliance zur Round-Robin-Methode. Daher erhält Service-HTTP-3 die sechste Anfrage.
- Service-HTTP-2 empfängt die siebte und achte Anforderung, da dieser Dienst den niedrigsten N-Wert hat.

Service-HTTP-1 wird für den Lastenausgleich nicht berücksichtigt, da es im Vergleich zu den beiden anderen Diensten stärker ausgelastet ist (hat den höchsten N-Wert). Wenn Service-HTTP-1 jedoch seine aktiven Transaktionen abschließt, berücksichtigt die NetScaler-Appliance diesen Dienst erneut für den Lastenausgleich.

Die folgende Tabelle fasst zusammen, wie N für die Dienste berechnet wird.

Anfrage erhalten	Ausgewählter Dienst	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-1	Service-HTTP-3; (N = 0)	N = 2	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-3	Service-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-4	Service-HTTP-3; (N = 6)	N = 8	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-5	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 hat den niedrigsten N-Wert.

Anfrage erhalten	Ausgewählter Dienst	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-6	Service-HTTP-3; (N = 8)	N = 10	Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte. NetScaler Appliance wechselt zur Round-Robin-Methode und wählt Service-HTTP-3
Request-7	Service-HTTP-2; (N = 8)	N = 9	Service-HTTP-2 hat den niedrigsten N-Wert.
Request-8	Service-HTTP-2; (N = 9)	N = 10	Service-HTTP-2 hat den niedrigsten N-Wert.

Service-HTTP-1 wird erneut für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn sein N-Wert niedriger ist als der der anderen Dienste (Service-HTTP-2 und Service-HTTP-3).

Auswahl der Dienstleistungen bei der Gewichtserteilung

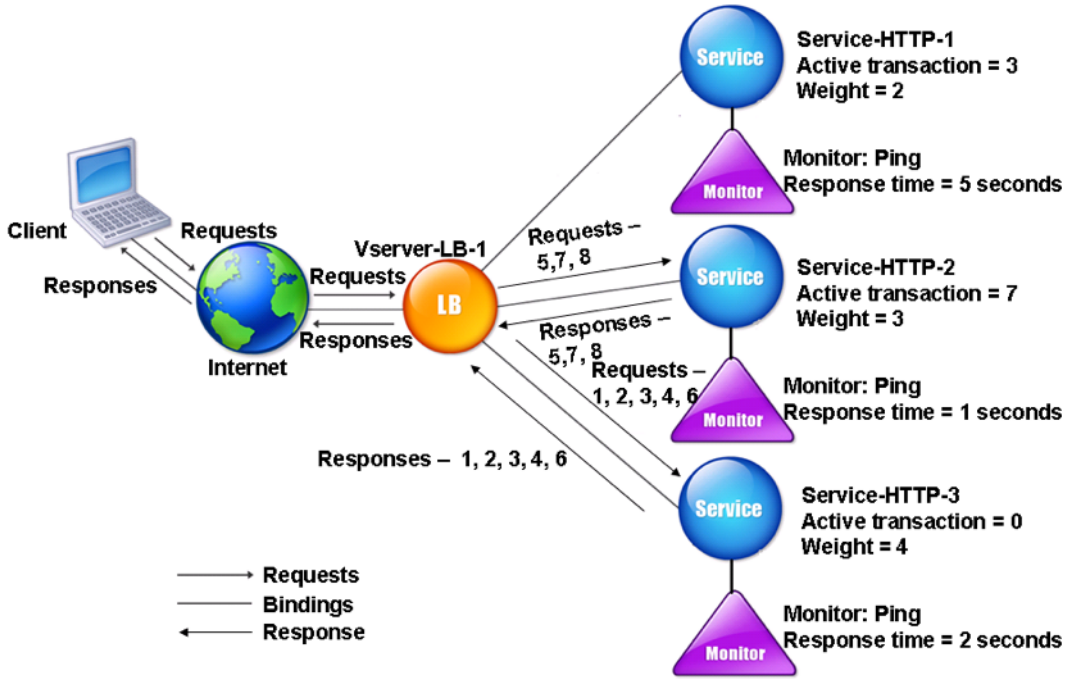
Die NetScaler-Appliance führt auch einen Lastenausgleich durch, indem sie die Anzahl der aktiven Transaktionen, die Reaktionszeit und die Gewichtungen verwendet, wenn Diensten unterschiedliche Gewichtungen zugewiesen werden. Die NetScaler-Appliance wählt den Dienst aus, indem sie den Wert (Nw) im folgenden Ausdruck verwendet:

Nw = (N) * (10000/Gewicht)

Wobei N = (Anzahl der aktiven Transaktionen * Reaktionszeit, die vom Monitor bestimmt wird)

Das folgende Diagramm zeigt, wie der virtuelle Server die LRTM-Methode verwendet, wenn Gewichte zugewiesen werden.

Abbildung 2. Funktionsweise der Load Balancing-Methode für die geringste Antwortzeit bei Zuweisung von Gewichten



In diesem Beispiel wird Service-http-1 eine Gewichtung von 2 zugewiesen, Service-http-2 wird eine Gewichtung von 3 zugewiesen und Service-http-3 wird die Gewichtung 4 zugewiesen.

Die NetScaler Appliance übermittelt Anfragen wie folgt:

- Service-HTTP-3 empfängt die erste Anforderung, da es keine aktiven Transaktionen verarbeitet.
- Service-http-3 empfängt die zweite, dritte, vierte und fünfte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die sechste Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-3 empfängt die siebte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achten Anfragen, da dieser Dienst den niedrigsten Nw-Wert hat.

Service-HTTP-1 hat das niedrigste Gewicht und den höchsten Nw-Wert, sodass die NetScaler-Appliance es nicht für den Lastenausgleich auswählt.

In der folgenden Tabelle wird zusammengefasst, wie Nw für verschiedene Monitore berechnet wird.

Anfrage erhalten	Ausgewählter Dienst	Aktueller Neuwert (N) * (10000/Gewicht)	Bemerkungen
Request-1	service-HTTP-3; (Jetzt = 0)	Neu = 5000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-2	service-HTTP-3; (Nw = 5000)	Neu = 10000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-3	Service-HTTP-3; (Nw = 10000)	Nw = 15000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-4	Service-HTTP-3; (Nw = 15000)	Neu = 20000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-5	Service-HTTP-3; (Jetzt = 20000)	Neu = 25000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-6	service-HTTP-2; (Jetzt = 23333.34)	Jetzt = 26666.67	Service-HTTP-2 hat den niedrigsten Nw-Wert.
Request-7	Service-HTTP-3; (Jetzt = 25000)	Nw = 30000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-8	service-HTTP-2; (Jetzt = 26666.67)	Neu = 30000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Service-HTTP-1 wird für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn sein Nw-Wert niedriger ist als bei anderen Diensten (Service-HTTP-2 und Service-HTTP-3).

So konfigurieren Sie die LRTM-Load-Balancing-Methode mithilfe der CLI

Geben Sie in der Befehlszeile ein;

```
set lb vserver <name> [-lbMethod <lbMethod>]
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod LRTM
<!--NeedCopy-->
```

So konfigurieren Sie die LRTM-Load-Balancing-Methode mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **LRTM**aus.

So aktivieren Sie die LRTM-Option in Monitoren mithilfe der CLI

Geben Sie in der Befehlszeile ein;

```
set lb monitor <monitorName> <type> [-LRTM ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Beispiel:

```
set lb monitor monitor-HTTP-1 HTTP -LRTM ENABLED
<!--NeedCopy-->
```

So aktivieren Sie die LRTM-Option in Monitoren mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**und öffnen Sie einen Monitor.
2. Wählen Sie unter Erweiterte Parameter die Option **LRTM (Least Reaktionszeit using Monitoring)**aus.

Weitere Informationen zum Konfigurieren von Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Hashing-Methoden

May 11, 2023

Load Balancing-Methoden, die auf Hashes bestimmter Verbindungsinformationen oder Header-Informationen basieren, stellen die meisten Load Balancing-Methoden der NetScaler Appliance dar. Hashes sind kürzer und einfacher zu verwenden als die Informationen, auf denen sie basieren,

während genügend Informationen beibehalten werden, um sicherzustellen, dass keine zwei verschiedenen Informationsstücke denselben Hash generieren und daher miteinander verwechselt werden.

Sie können die Hashing-Load Balancing-Methoden in einer Umgebung verwenden, in der ein Cache eine breite Palette von Inhalten aus dem Internet oder bestimmten Ursprungsservern bereitstellt. Caching-Anforderungen reduzieren die Anforderungs- und Antwortlatenz und gewährleistet eine bessere Ressourcenauslastung (CPU), wodurch das Caching auf stark genutzten Websites und Anwendungsservern populär wird. Da diese Sites auch vom Lastenausgleich profitieren, sind Hashing-Load Balancing-Methoden sehr nützlich.

Die NetScaler-Appliance bietet die folgenden Hashing-Methoden:

- URL-Hash-Methode
- Domain-Hash-Methode
- Ziel-IP-Hash-Methode
- Quell-IP-Hash-Methode
- Quell-IP-Ziel-IP-Hashmethode
- Quell-IP-Quellport-Hash-Methode
- Anruf-ID-Hash-Methode
- Token-Methode

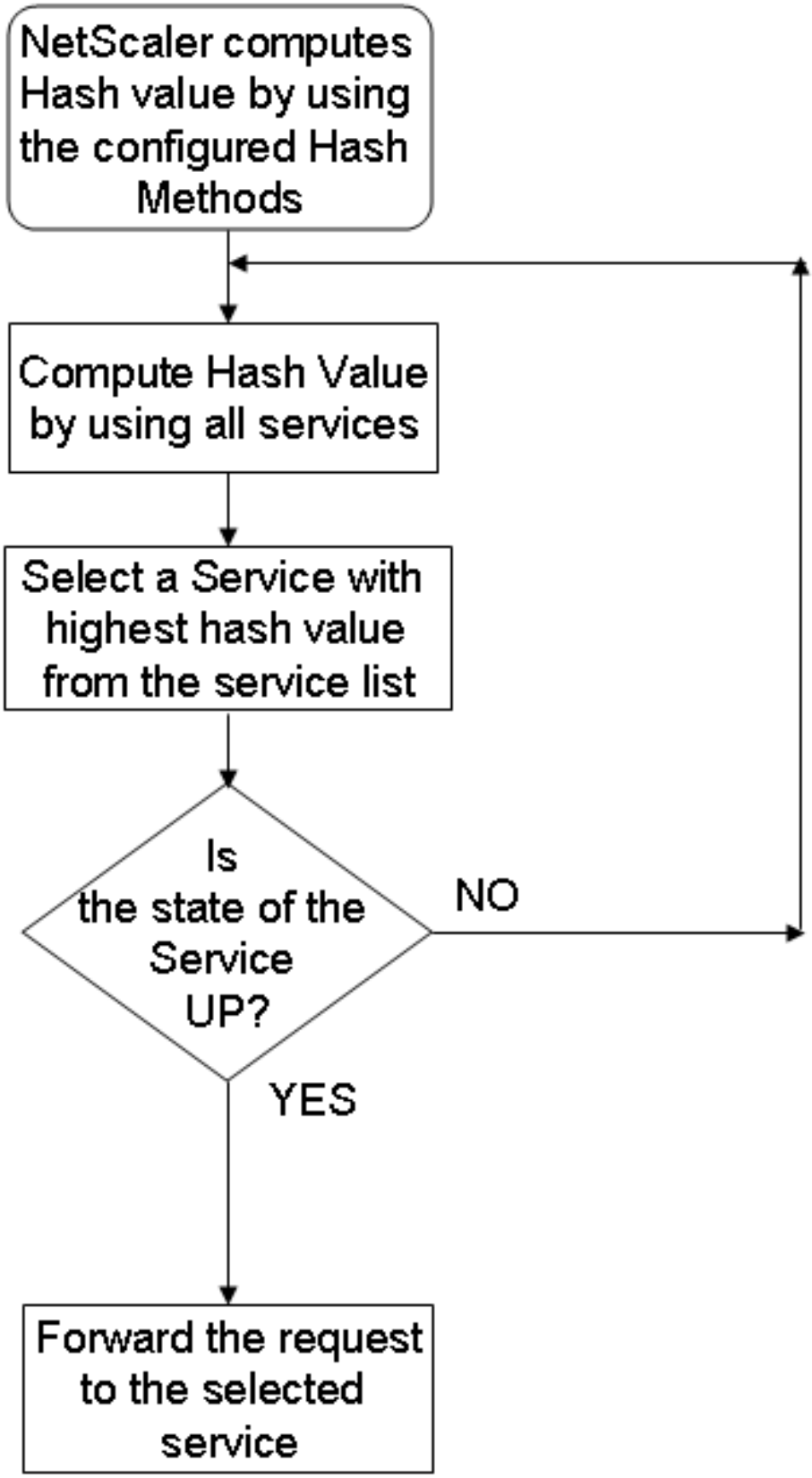
Die meisten Hashing-Algorithmen berechnen zwei Hash-Werte:

- Ein Hash der IP-Adresse und des Ports des Dienstes.
- Ein Hash der eingehenden URL, des Domainnamens, der Quell-IP-Adresse, der Ziel-IP-Adresse oder der Quell- und Ziel-IP-Adressen, abhängig von der konfigurierten Hash-Methode.

Die NetScaler Appliance generiert dann einen neuen Hash-Wert, indem beide Hash-Werte verwendet werden. Schließlich leitet es die Anforderung an den Dienst mit dem höchsten Hashwert weiter. Da die Appliance für jede Anforderung einen Hashwert berechnet und den Dienst auswählt, der die Anforderung verarbeitet, füllt sie einen Cache. Nachfolgende Anforderungen mit demselben Hash-Wert werden an denselben Dienst gesendet. Das folgende Flussdiagramm veranschaulicht diesen Prozess.

> Hinweis
>
> Ab NetScaler Release 13.0 Build 79.x werden konsistente Hashing-Algorithmen von Prime Re-Shuffled Assisted CARP (PRAC) und Jump Table Assisted Ring Hash (JARH) unterstützt. Die konsistenten Hashing-Algorithmen sorgen für minimale Unterbrechungen, wenn Dienste zu Ihrem Load Balancing-Setup oder während eines Service Flap-Ereignisses im Load Balancing-Setup hinzugefügt oder aus diesem gelöscht werden. Weitere Informationen finden Sie unter Konsistente Hashing-Algorithmen.

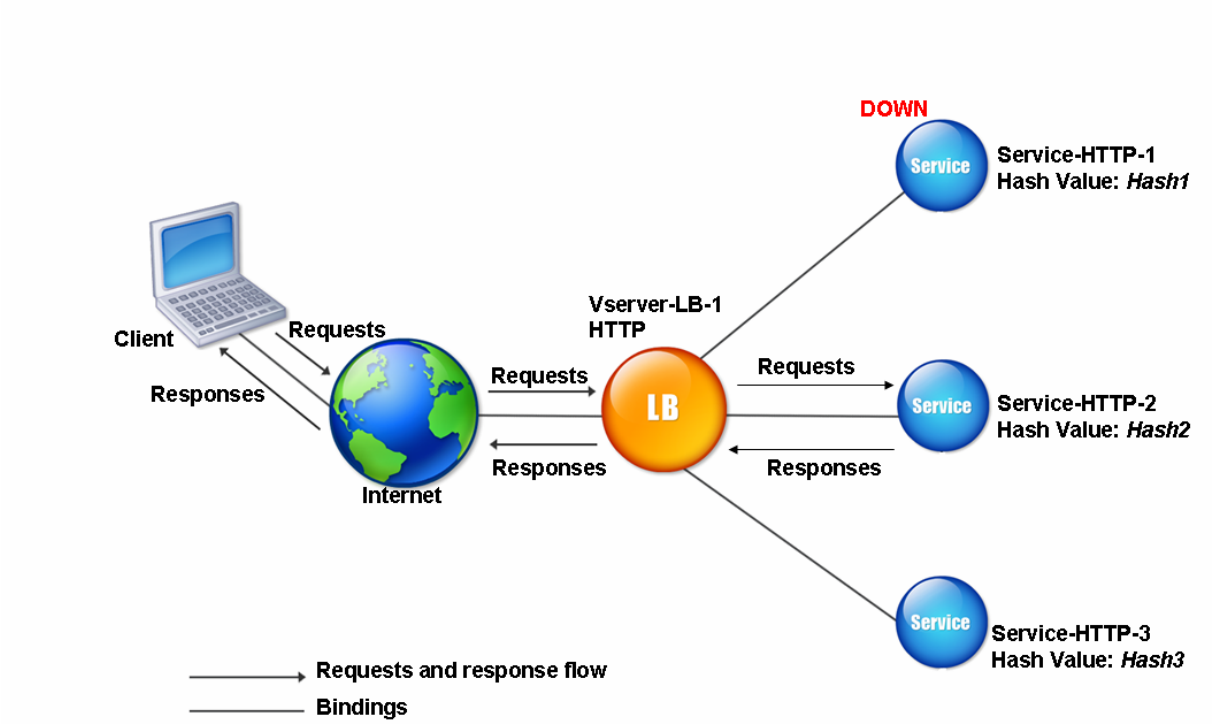
Abbildung 1. Wie die Hashing-Methoden Anforderungen verteilen



Hashing-Methoden können auf IPv4- und IPv6-Adressen angewendet werden.

Stellen Sie sich ein Szenario vor, in dem drei Dienste (Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3) an einen virtuellen Server gebunden sind, eine beliebige Hash-Methode konfiguriert ist und der Hashwert Hash1 ist. Wenn die konfigurierten Dienste aktiv sind, wird die Anfrage an Service-HTTP-1 gesendet. Wenn Service-HTTP-1 ausgefallen ist, berechnet die NetScaler-Appliance den Hashwert für das letzte Protokoll der Anzahl der Dienste. Die Appliance wählt dann den Dienst mit dem höchsten Hashwert aus, z. B. service-HTTP-2. Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 2. Entitätsmodell für Hashing-Methoden



> Hinweis
>
> Wenn die NetScaler Appliance einen Dienst nicht mithilfe einer Hashing-Methode auswählen kann, wird standardmäßig die kleinste Verbindungsmethode verwendet, um einen Dienst für die eingehende Anforderung auszuwählen. Passen Sie Server-Pools an, indem Sie Dienste in Zeiten mit geringem Datenverkehr entfernen, damit die Caches neu aufgefüllt werden können, ohne die Leistung Ihres Lastenausgleichs-Setups zu beeinträchtigen.

Konsistente Hashing-Algorithmen

Die konsistenten Hashing-Algorithmen werden verwendet, um zustandslos Persistenz zu erreichen. Die hashbasierten LB-Methoden verwenden einen der folgenden drei konsistenten Hashing-Algorithmen:

- **Cache-Array-Routing-Protokoll (CARP)**

  Der CARP-Algorithmus wird zum Lastenausgleich von HTTP-Anfragen auf mehreren Proxy-Cache-Servern verwendet. Dieser Algorithmus ist standardmäßig aktiviert.

- **Prime Re-Shuffled Assisted CARP (PRAC)**

  Die NetScaler Appliance verwendet den proprietären PRAC-Algorithmus, um eine einheitliche Verkehrsverteilung bereitzustellen.

- **Sprungtisch Assisted Ring Hash (JARH)**

  Die NetScaler Appliance verwendet den proprietären JARH-Algorithmus, um eine Konsistenz und einheitliche Verteilung des Datenverkehrs zu gewährleisten. Dieser Algorithmus verwendet Hash-Finger. Eine höhere Anzahl von Finger sorgt für eine bessere Verkehrsverteilung. Die Erhöhung der Anzahl der Finger erhöht jedoch auch die Speicherauslastung.

So wählen Sie den konsistenten Hashing-Algorithmus mit CLI aus

```
set lb parameter [-lbHashAlgorithm [DEFAULT|JARH|PRAC] [-lbHashFingers
   <positive_integer>]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -lbHashAlgorithm JARH -lbHashFingers 10
<!--NeedCopy-->
```

ARGUMENTE:

- **lbhashalgorithm**-Geben Sie den Hashing-Algorithmus an, der für die folgenden Hash-basierten Load Balancing-Methoden verwendet werden soll:
  - URL-Hash-Methode
  - Domain-Hash-Methode
  - Ziel-IP-Hash-Methode
  - Quell-IP-Hash-Methode
  - Quell-IP-Ziel-IP-Hashmethode
  - Quell-IP-Quellport-Hash-Methode
  - Anruf-ID-Hash-Methode
  - Token-Methode

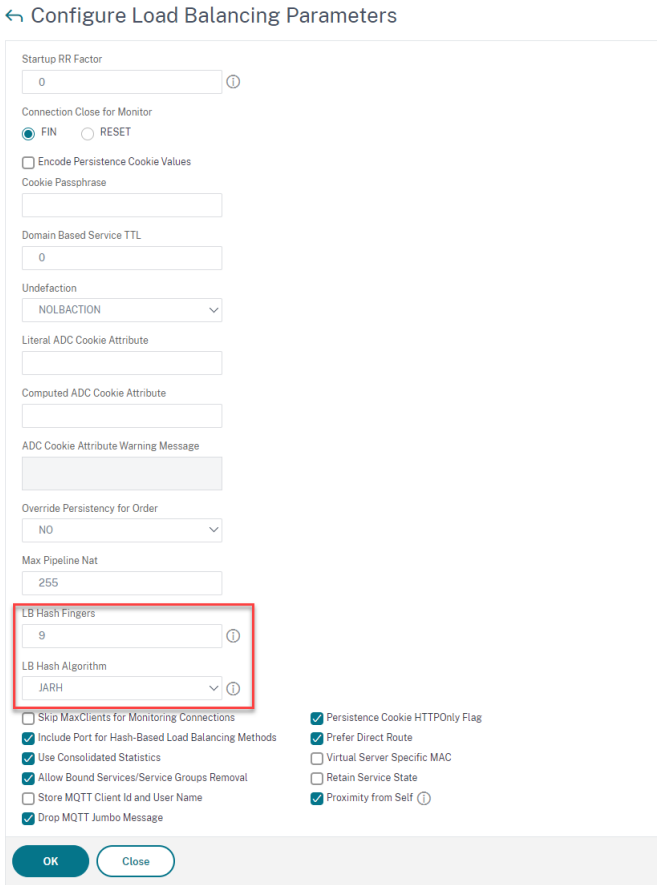
  Mögliche Werte: DEFAULT, PRAC, JARH
  Standardwert: DEFAULT

- **lbHashFingers**-Geben Sie die Anzahl der Finger an, die in PRAC- und JARH-Algorithmen für hashbasierte LB-Methoden verwendet werden sollen. Die Erhöhung der Anzahl der Finger ermöglicht eine bessere Verteilung des Datenverkehrs auf Kosten des zusätzlichen Speichers.

  Standardwert: 256
  Minimaler Wert: 1
  Maximaler Wert: 1024

So wählen Sie den konsistenten Hashing-Algorithmus mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter ändern**.
2. Geben **Sie im Bereich Load Balancing-Parameter konfigurieren** die entsprechenden Werte für die folgenden Felder ein, basierend auf Ihrer Anforderung:
   - LB Hash Finger
   - Wählen Sie im Feld **LB Hash Algorithm** den konsistenten Hashing-Algorithmus aus dem Dropdownmenü aus.



Die URL-Hash-Methode

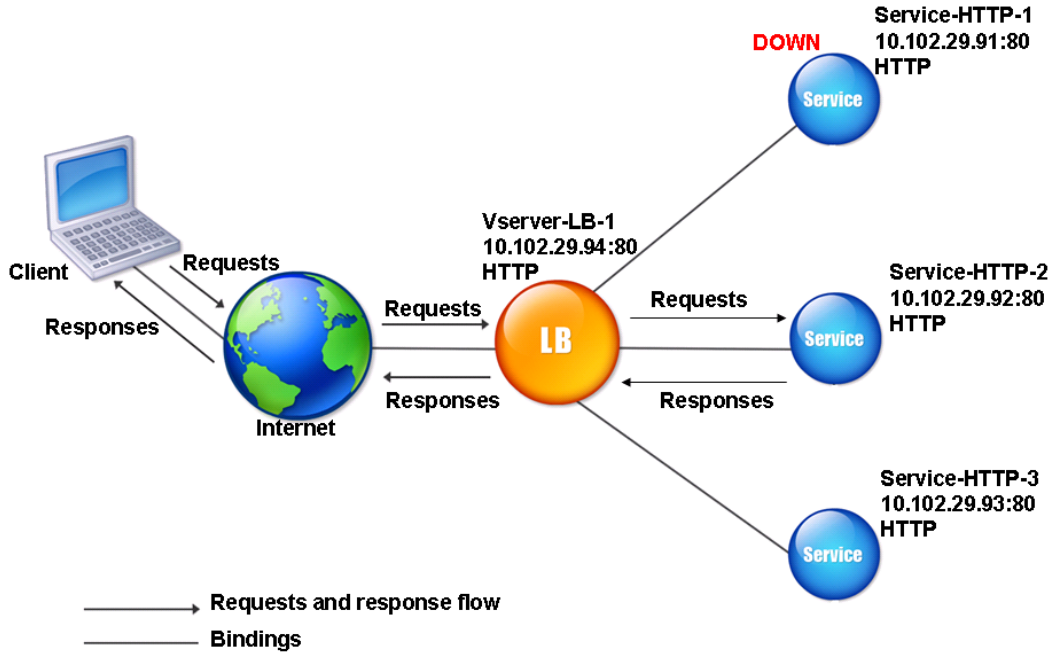
Wenn Sie die NetScaler-Appliance so konfigurieren, dass sie die URL-Hash-Methode für den Lastenausgleich der Dienste verwendet, generiert die Appliance für die Auswahl eines Dienstes einen Hashwert der HTTP-URL, die in der eingehenden Anfrage vorhanden ist. Wenn der durch den Hashwert ausgewählte Dienst DOWN ist, verfügt der Algorithmus über eine Methode, um einen anderen Dienst aus der Liste der aktiven Dienste auszuwählen. Die Appliance speichert den Hashwert der URL im Cache, und wenn sie nachfolgende Anfragen empfängt, die dieselbe URL verwenden, leitet sie diese an denselben Dienst weiter. Wenn die Appliance eine eingehende Anfrage nicht analysieren kann, verwendet sie die Round-Robin-Methode für den Lastenausgleich anstelle der URL-Hash-Methode.

Zur Generierung des Hashwerts verwendet die Appliance einen bestimmten Algorithmus und berücksichtigt einen Teil der URL. Standardmäßig berücksichtigt die Appliance die ersten 80 Byte der URL. Wenn die URL weniger als 80 Byte lang ist, wird die vollständige URL verwendet. Sie können eine andere Länge angeben. Die Hash-Länge kann zwischen 1 Byte und 4096 Byte liegen. Wenn lange URLs verwendet werden, bei denen nur wenige Zeichen unterschiedlich sind, empfiehlt es sich, die Hash-Länge so hoch wie möglich zu gestalten, um eine gleichmäßigere Lastverteilung sicherzustellen.

Betrachten Sie ein Szenario, in dem drei Dienste, service-http-1, service-http-2 und service-http-3, an einen virtuellen Server gebunden sind und die auf dem virtuellen Server konfigurierte Lastausgleichsmethode die URL-Hash-Methode ist. Der virtuelle Server erhält eine Anforderung und der Hashwert der URL ist U1. Appliance wählt Service-HTTP-1 aus. Wenn Service-HTTP-1 auf DOWN festgelegt ist, wählt die Appliance Service-HTTP-2 aus.

Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 3. So funktioniert URL-Hashing



Wenn sowohl Service-HTTP-1 als auch Service-HTTP-2 DOWN sind, sendet die Appliance Anfragen mit dem Hashwert U1 an Service-HTTP-3.

Wenn Service-HTTP-1 und Service-HTTP-2 ausgefallen sind, werden Anforderungen, die den Hash-URL1 generieren, an Service-HTTP-3 gesendet. Wenn diese Dienste UP sind, werden die Anfragen, die den Hash-URL1 erzeugen, auf folgende Weise verteilt:

- Wenn der Service-HTTP-2 hochgeladen ist, wird die Anforderung an Service-HTTP-2 gesendet.
- Wenn der Service-HTTP-1 aktiv ist, wird die Anfrage an Service-HTTP-1 gesendet.
- Wenn Service-HTTP-1 und Service-HTTP-2 gleichzeitig hochgeladen sind, wird die Anforderung an Service-HTTP-1 gesendet.

Informationen zum Konfigurieren der URL-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält. Wählen Sie die Load Balancing-Methode als URL-Hash aus, und legen Sie die Hashlänge auf die Anzahl der Bytes fest, die zum Generieren des Hash-Werts verwendet werden sollen.

Die Domain-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Domain-Hash-Methode konfiguriert ist, verwendet den Hashwert des Domainnamens in der HTTP-Anfrage, um einen Dienst auszuwählen.

Der Domainname wird entweder von der eingehenden URL oder dem Host-Header der HTTP-Anfrage übernommen. Wenn der Domainname sowohl in der URL als auch im Host-Header erscheint, bevorzugt die Appliance die URL.

Wenn Sie das Hashing für Domainnamen konfigurieren und eine eingehende HTTP-Anfrage keinen Domainnamen enthält, verwendet die NetScaler-Appliance standardmäßig die Round-Robin-Methode für diese Anfrage.

Die Hashwertberechnung verwendet die Namenslänge oder den Hashlängenwert, je nachdem, welcher Wert kleiner ist. Standardmäßig berechnet die NetScaler-Appliance den Hashwert aus den ersten 80 Byte des Domainnamens. Um bei der Berechnung des Hash-Werts eine andere Anzahl von Bytes im Domänennamen anzugeben, können Sie den Parameter hashlength (HashLength im Konfigurationsdienstprogramm) auf einen Wert von 1 bis 4096 (Byte) festlegen.

Informationen zum Konfigurieren der Domänen-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Ziel-IP-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Ziel-IP-Hash-Methode konfiguriert ist, verwendet den Hashwert der Ziel-IP-Adresse, um einen Server auszuwählen. Sie können die Ziel-IP-Adresse maskieren, um anzugeben, welcher Teil davon in der Hashwertberechnung verwendet werden soll, sodass Anforderungen, die von verschiedenen Netzwerken stammen, aber für dasselbe Subnetz bestimmt sind, alle an denselben Server gerichtet werden. Diese Methode unterstützt IPv4- und IPv6-basierte Zielserver.

Diese Load-Balancing-Methode eignet sich für die Verwendung mit der Cache-Umleitungsfunktion.

Um die Ziel-IP-Hash-Methode für einen IPv4-Zielserver zu konfigurieren, legen Sie den NetMask-Parameter fest. Um diese Methode für einen IPv6-Zielserver zu konfigurieren, verwenden Sie den Parameter v6NetMaskLen. Im Konfigurationsdienstprogramm werden Textfelder zum Festlegen dieser Parameter angezeigt, wenn Sie die **Ziel-IP-Hash-Methode**auswählen.

Informationen zum Konfigurieren der Ziel-IP-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Quell-IP-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Quell-IP-Hash-Methode konfiguriert ist, verwendet den Hashwert der Client-IPv4- oder IPv6-Adresse, um einen Dienst auszuwählen. Um alle Anforderungen von Quell-IP-Adressen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver weiterzuleiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den netMask-Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

Informationen zum Konfigurieren der Quell-IP-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die IP-Hash-Methode des Quell-IP-Ziels

Ein virtueller Lastausgleichsserver, der für die Verwendung der Quell-IP-Ziel-Hash-Methode konfiguriert ist, verwendet den Hashwert der Quell- und Ziel-IP-Adressen (IPv4 oder IPv6), um einen Dienst auszuwählen. Hashing ist symmetrisch. Der Hashwert ist unabhängig von der Reihenfolge der Quell- und Ziel-IPs gleich. Dadurch wird sichergestellt, dass alle Pakete, die von einem bestimmten Client zum selben Ziel fließen, an denselben Server weitergeleitet werden.

Um alle Anforderungen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver zu leiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den netMask-Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

Informationen zum Konfigurieren der IP-Ziel-IP-Hash-Methode des Quell-IP-Ziels finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Quell-IP-Quellport-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Hash-Methode des Quell-IP-Quellports konfiguriert ist, verwendet den Hashwert der Quell-IP (entweder IPv4 oder IPv6) und des Quellports, um einen Dienst auszuwählen. Dadurch wird sichergestellt, dass alle Pakete auf einer bestimmten Verbindung an denselben Dienst weitergeleitet werden.

Diese Methode wird bei der Verbindungsspiegelung und beim Lastenausgleich der Firewall verwendet. Weitere Informationen zur Verbindungsspiegelung finden Sie unter Verbindungs-Failover.

Um alle Anforderungen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver zu leiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den netMask-Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

Informationen zum Konfigurieren der Hash-Methode für Quell-IP-Quellport finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Call-ID-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Anruf-ID-Hash-Methode konfiguriert ist, verwendet den Hashwert der Anruf-ID im SIP-Header, um einen Dienst auszuwählen. Pakete für eine bestimmte SIP-Sitzung werden daher immer an denselben Proxyserver geleitet.

Diese Methode ist für den SIP-Lastenausgleich anwendbar. Weitere Informationen zum SIP-Lastenausgleich finden Sie unter Überwachen von SIP-Diensten.

Informationen zum Konfigurieren der Call-ID-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Methode der geringsten Bandbreite

May 11, 2023

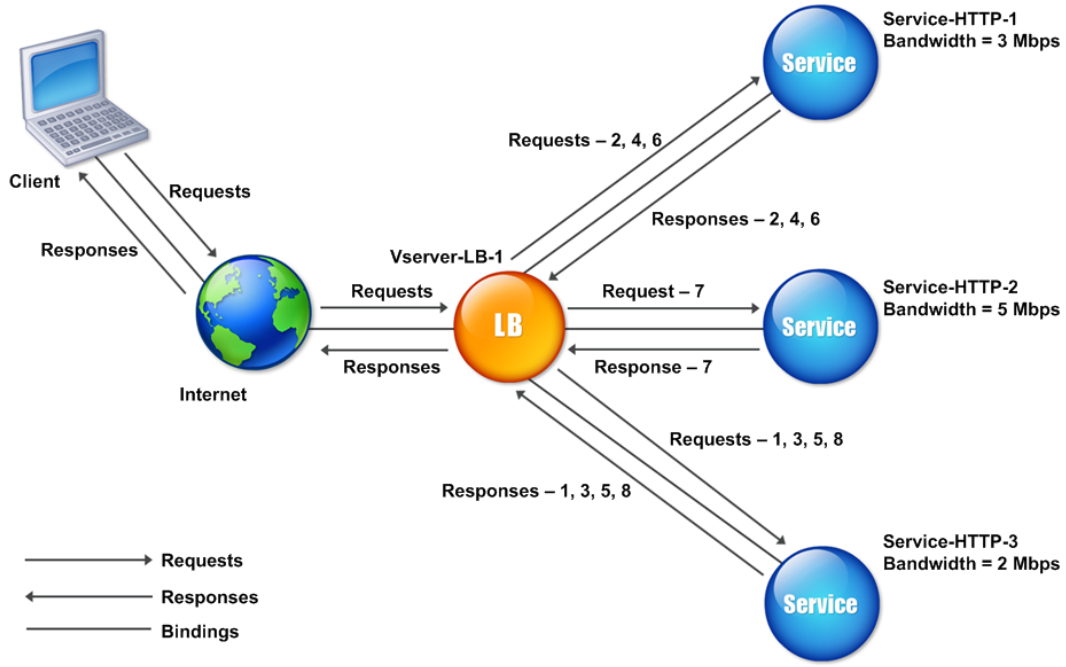
Ein virtueller Lastausgleichsserver, der für die Verwendung der Methode mit der geringsten Bandbreite konfiguriert ist, wählt den Dienst aus, der derzeit die geringste Menge an Datenverkehr, gemessen in Megabit pro Sekunde (Mbit/s), bereitstellt. Das folgende Beispiel zeigt, wie der virtuelle Server einen Dienst für den Lastenausgleich auswählt, indem er die Methode mit der geringsten Bandbreite verwendet.

Stellen Sie sich drei Dienste vor: Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3.

- Service-HTTP-1 hat eine Bandbreite von 3 Mbit/s.
- Service-HTTP-2 hat eine Bandbreite von 5 Mbit/s.
- Service-HTTP-3 hat eine Bandbreite von 2 Mbit/s.

Das folgende Diagramm zeigt, wie der virtuelle Server die Methode mit der geringsten Bandbreite verwendet, um Anfragen an die drei Dienste weiterzuleiten.

Abbildung 1. Funktionsweise der Load Balancing-Methode der geringsten Bandbreite



Der virtuelle Server wählt den Dienst mithilfe des Bandbreitenwerts (N) aus. Dies ist die Summe der Anzahl der Bytes, die in den letzten 14 Sekunden übertragen und empfangen wurden. Wenn für jede Anfrage 1 Mbit/s Bandbreite erforderlich ist, stellt die NetScaler-Appliance Anfragen wie folgt bereit:

- Service-HTTP-3 empfängt die erste Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Da Service-HTTP-1 und Service-HTTP-3 jetzt denselben N-Wert haben, wechselt der virtuelle Server abwechselnd zwischen ihnen zur Round-Robin-Methode für diese Server. Service-http-1 empfängt die zweite Anforderung, Service-http-3 erhält die dritte Anforderung, Service-http-1 erhält die vierte Anforderung, Service-http-3 erhält die fünfte Anforderung und Service-http-1 erhält die sechste Anforderung.
- Da Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 jetzt alle denselben N-Wert haben, enthält der virtuelle Server Service-HTTP-2 in die Round-Robin-Liste. Daher erhält Service-http-2 die siebte Anforderung, Service-http-3 erhält die achte Anforderung usw.

In der folgenden Tabelle wird zusammengefasst, wie N berechnet wird.

Anfrage erhalten	Ausgewählter Dienst	Aktueller N-Wert	Bemerkungen
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-1; (N = 3)	N = 4	Service-HTTP-1 und Service-HTTP-3 haben dieselben N-Werte.
Request-3	Service-HTTP-3; (N = 3)	N = 4	Service-HTTP-1 und Service-HTTP-3 haben dieselben N-Werte.
Request-4	Service-HTTP-1; (N = 4)	N = 5	-
Request-5	Service-HTTP-3; (N = 4)	N = 5	-
Request-6	Service-HTTP-1; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte.
Request-7	Service-HTTP-2; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte.
Request-8	Service-HTTP-3; (N = 5)	N = 6	-

Hinweis: Wenn Sie die RTSP-NAT-Option auf dem virtuellen Server aktivieren, verwendet die NetScaler Appliance die Anzahl der ausgetauschten Daten und Kontrollbytes, um die Bandbreitenauslastung für RTSP-Dienste zu bestimmen. Weitere Informationen zur RTSP-NAT-Option finden Sie unter RTSP-Verbindungen verwalten.

Die NetScaler Appliance führt außerdem Lastenausgleich durch, indem Bandbreite und Gewichte verwendet werden, wenn den Diensten unterschiedliche Gewichtungen zugewiesen werden. Es wählt einen Dienst aus, indem der Wert (Nw) im folgenden Ausdruck verwendet wird:

Nw = (N) * (10000/Gewicht)

Nehmen wir wie im vorherigen Beispiel an, dass Service-HTTP-1 eine Gewichtung von 2, Service-HTTP-2 eine Gewichtung von 3 zugewiesen wird und Service-HTTP-3 eine Gewichtung von 4 zugewiesen wird. Die NetScaler Appliance übermittelt Anfragen wie folgt:

- Service-HTTP-3 empfängt die erste zweite, dritte, vierte und fünfte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-1 empfängt die sechste Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-3 empfängt die siebte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.

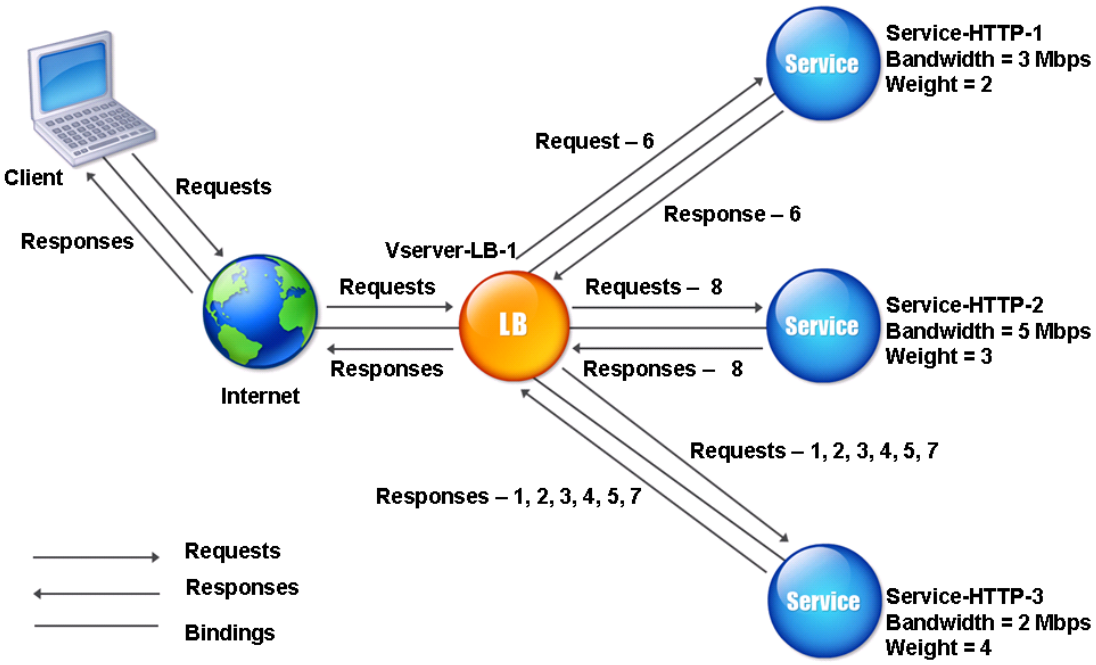
In der folgenden Tabelle wird zusammengefasst, wie Nw berechnet wird.

Anfrage erhalten	Ausgewählter Dienst	Aktueller Neuwert (Anzahl der aktiven Transaktionen) * (10000 /Gewicht)	Bemerkungen
Request-1	Service-HTTP-3; (Nw = 5000)	Neu = 5000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-2	Service-HTTP-3; (Nw = 5000)	Nw = 7500	-
Request-3	Service-HTTP-3; (Jetzt = 7500)	Neu = 10000	-
Request-4	Service-HTTP-3; (Nw = 10000)	Nw = 12500	-
Request-5	Service-HTTP-3; (Nw = 12500)	Nw = 15000	-
Request-6	Service-HTTP-1; (Nw = 15000)	Neu = 20000	Service-HTTP-1 und Service-HTTP-3 haben den gleichen Nw-Wert.
Request-7	Service-HTTP-3; (Nw = 15000)	Nw = 17500	Service-HTTP-1 und Service-HTTP-3 haben den gleichen Nw-Wert.

Anfrage erhalten	Ausgewählter Dienst	Aktueller Neuwert (Anzahl der aktiven Transaktionen) * (10000 /Gewicht)	Bemerkungen
Request-8	Service-HTTP-2; (Nw = 16666,67)	Neu = 20000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Das folgende Diagramm zeigt, wie der virtuelle Server die Methode mit der geringsten Bandbreite verwendet, wenn den Diensten Gewichtungen zugewiesen werden.

Abbildung 2. Funktionsweise der Load Balancing-Methode mit der geringsten Bandbreite bei Zuweisung von Gewichten



Informationen zum Konfigurieren der Methode mit der geringsten Bandbreite finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Methode der kleinsten Pakete

May 11, 2023

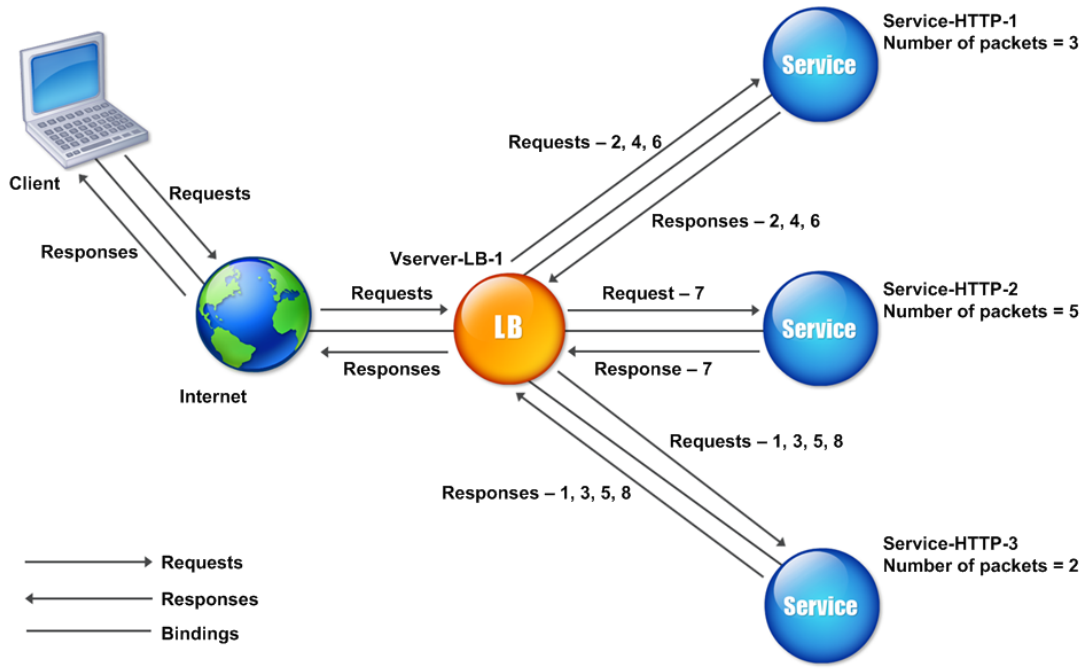
Ein virtueller Lastausgleichsserver, der für die Verwendung der Methode mit den wenigsten Paketen konfiguriert ist, wählt den Dienst aus, der in den letzten 14 Sekunden die wenigsten Pakete empfangen hat.

Betrachten Sie beispielsweise drei Dienste, Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3.

- Service-HTTP-1 hat in den letzten 14 Sekunden drei Pakete bearbeitet.
- Service-HTTP-2 hat in den letzten 14 Sekunden fünf Pakete verarbeitet.
- Service-HTTP-3 hat in den letzten 14 Sekunden zwei Pakete bearbeitet.

Das folgende Diagramm veranschaulicht, wie die NetScaler Appliance für jede empfangene Anforderung die Methode der wenigsten Pakete verwendet, um einen Dienst auszuwählen.

Abbildung 1. So funktioniert die Loadbalancing-Methode mit den wenigsten Paketen



Die NetScaler Appliance wählt einen Dienst anhand der Anzahl der Pakete (N) aus, die von jedem Dienst in den letzten 14 Sekunden übertragen und empfangen wurden. Mit dieser Methode übermittelt es Anfragen wie folgt:

- Service-HTTP-3 empfängt die erste Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Da Service-HTTP-1 und Service-HTTP-3 jetzt den gleichen N-Wert haben, wechselt der virtuelle Server zur Round-Robin-Methode. Service-http-1 erhält daher die zweite Anforderung, Service-http-3 erhält die dritte Anforderung, Service-http-1 erhält die vierte Anforderung, Service-http-3 erhält die fünfte Anforderung und Service-http-1 erhält die sechste Anforderung.
- Da Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 jetzt alle den gleichen N-Wert haben, wechselt der virtuelle Server auch zur Round-Robin-Methode für Service-HTTP-2, einschließlich dieser in der Round-Robin-Liste. Daher erhält Service-http-2 die siebte Anforderung, Service-http-3 erhält die achte Anforderung usw.

In der folgenden Tabelle wird zusammengefasst, wie N berechnet wird.

Anfrage erhalten	Ausgewählter Dienst	Aktueller N-Wert	Bemerkungen
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-1; (N = 3)	N = 4	Service-HTTP-1 und Service-HTTP-3 haben dieselben N-Werte.
Request-3	Service-HTTP-3; (N = 3)	N = 4	Service-HTTP-1 und Service-HTTP-3 haben dieselben N-Werte.
Request-4	Service-HTTP-1; (N = 4)	N = 5	-
Request-5	Service-HTTP-3; (N = 4)	N = 5	-
Request-6	Service-HTTP-1; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte.
Request-7	Service-HTTP-2; (N = 5)	N = 6	Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte.

Anfrage erhalten	Ausgewählter Dienst	Aktueller N-Wert	Bemerkungen
Request-8	Service-HTTP-3; (N = 5)	N = 6	-

Hinweis: Wenn Sie die Option RTSP NAT auf dem virtuellen Server aktivieren, berechnet die Appliance die Anzahl der Daten- und Steuerpakete, um die Anzahl der Pakete für RTSP-Dienste zu berechnen. Weitere Informationen zur RTSP-NAT-Option finden Sie unter RTSP-Verbindungen verwalten.

Die NetScaler Appliance führt außerdem Lastenausgleich durch, indem die Anzahl der Pakete und Gewichte verwendet wird, wenn jedem Dienst ein anderes Gewicht zugewiesen wird. Es wählt einen Dienst aus, indem der Wert (Nw) im folgenden Ausdruck verwendet wird:

Nw = (N) * (10000/Gewicht)

Nehmen wir wie im vorherigen Beispiel an, dass Service-HTTP-1 eine Gewichtung von 2, Service-HTTP-2 eine Gewichtung von 3 zugewiesen wird und Service-HTTP-3 eine Gewichtung von 4 zugewiesen wird. Die NetScaler Appliance übermittelt Anfragen wie folgt:

- Service-HTTP-3 empfängt die erste zweite, dritte, vierte und fünfte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-1 empfängt die sechste Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-3 empfängt die siebte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.

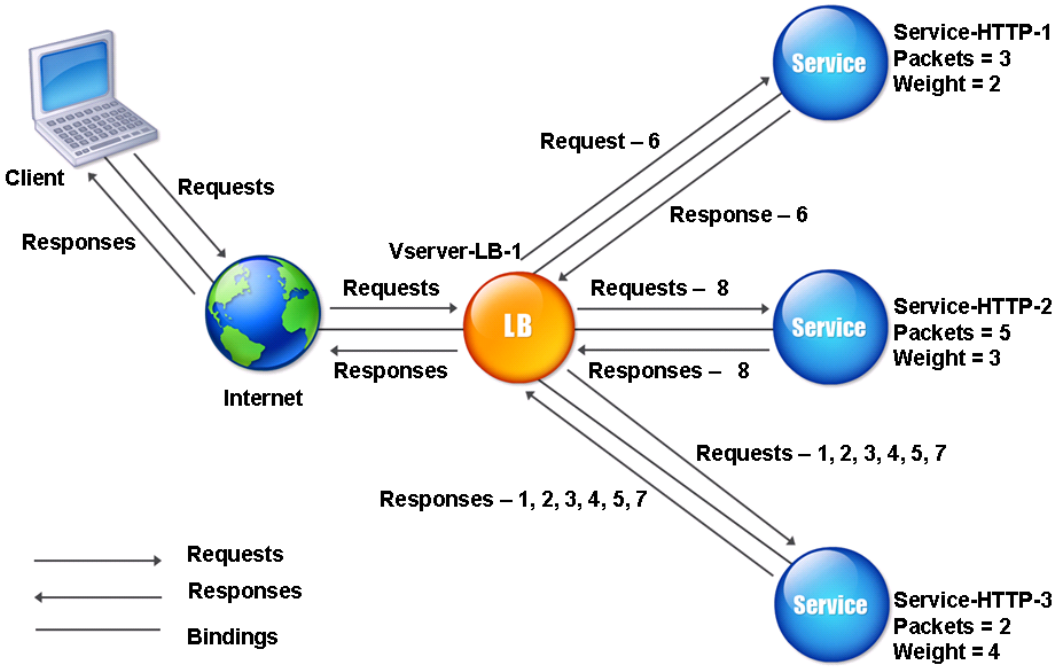
In der folgenden Tabelle wird zusammengefasst, wie Nw berechnet wird.

Anfrage erhalten	Ausgewählter Dienst	Aktueller Neuwert (Anzahl der aktiven Transaktionen) * (10000//Gewicht)	Bemerkungen
Request-1	Service-HTTP-3; (Nw = 5000)	Neu = 5000	Service-HTTP-3 hat den niedrigsten Nw-Wert.
Request-2	Service-HTTP-3; (Nw = 5000)	Nw = 7500	-
Request-3	Service-HTTP-3; (Nw = 7500)	Neu = 10000	-
Request-4	Service-HTTP-3; (Nw = 10000)	Nw = 12500	-
Request-5	Service-HTTP-3; (Nw = 12500)	Nw = 15000	-

Anfrage erhalten	Ausgewählter Dienst	Aktueller Neuwert (Anzahl der aktiven Transaktionen) * (10000//Gewicht)	Bemerkungen
Request-6	Service-HTTP-1; (Nw = 15000)	Neu = 20000	Service-HTTP-1 und Service-HTTP-3 haben den gleichen Nw-Wert.
Request-7	Service-HTTP-3; (Nw = 15000)	Nw = 17500	Service-HTTP-1 und Service-HTTP-3 haben den gleichen Nw-Wert.
Request-8	Service-HTTP-2; (Nw = 16666,67)	Neu = 20000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Das folgende Diagramm zeigt, wie der virtuelle Server die Methode der kleinsten Pakete verwendet, wenn Gewichte zugewiesen werden.

Abbildung 2. So funktioniert die Methode “Least Packets”, wenn Gewichte zugewiesen werden



Informationen zum Konfigurieren der Methode der kleinsten Pakete finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

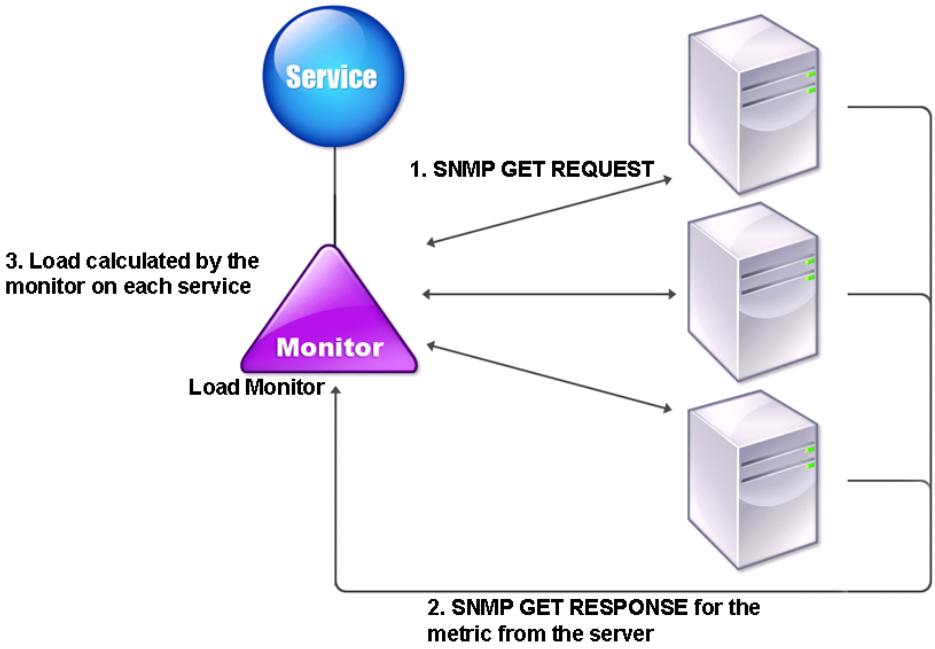
Benutzerdefinierte Lademethode

May 11, 2023

Ein benutzerdefinierter Lastenausgleich wird für Serverparameter wie CPU-Auslastung, Arbeitsspeicher und Antwortzeit durchgeführt. Bei Verwendung der benutzerdefinierten Lademethode wählt die NetScaler Appliance normalerweise einen Dienst aus, der keine aktiven Transaktionen verarbeitet. Wenn alle Dienste im Load Balancing-Setup aktive Transaktionen verarbeiten, wählt die Appliance den Service mit der kleinsten Last aus. Ein spezieller Monitortyp, der als Lastmonitor bezeichnet wird, berechnet die Last für jeden Dienst im Netzwerk. Die Lastüberwachungen markieren nicht den Status eines Dienstes, aber sie nehmen Dienste aus der Lastausgleichsentscheidung heraus, wenn diese Dienste nicht UP sind.

Weitere Informationen zu Lastmonitoren finden Sie unter Grundlegendes zu Lastmonitoren. Das folgende Diagramm veranschaulicht, wie ein Lastmonitor funktioniert.

Abbildung 1. So funktionieren Lastmonitore



Der Lastmonitor berechnet mithilfe von SNMP-Sonden die Belastung jedes Dienstes, indem er eine SNMP GET-Anfrage an den Dienst sendet. Diese Anforderung enthält eine oder mehrere Objekt-IDs (OIDs). Der Dienst antwortet mit einer SNMP-GET-Antwort mit Metriken, die den SNMP-OIDs entsprechen. Der Lastmonitor berechnet anhand der Antwortmetriken die Belastung des Dienstes.

Der Lastmonitor berechnet die Last auf einem Dienst mithilfe der folgenden Parameter:

- Metrikwerte, die über SNMP-Prüfpunkte abgerufen werden, die als Tabellen in der NetScaler-Appliance vorhanden sind.
- Für jede Metrik festgelegter Schwellenwert.
- Jeder Metrik zugewiesenes Gewicht.

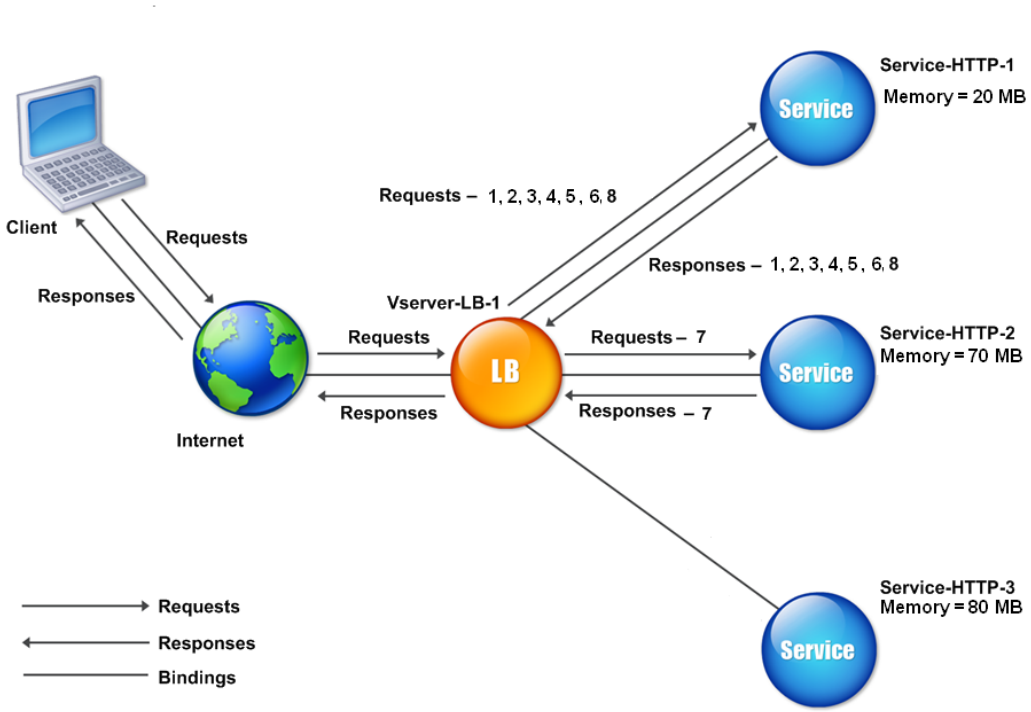
Betrachten Sie beispielsweise drei Dienste, Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3.

- Service-HTTP-1 verwendet 20 MB Speicher.
- Service-HTTP-2 verwendet 70 MB Arbeitsspeicher.
- Service-HTTP-3 verwendet 80 MB Speicher.

Die Server mit Lastausgleich können Metriken wie die CPU- und Speichernutzung an die Dienste exportieren, die sie wiederum dem Load Monitor zur Verfügung stellen können. Der Load Monitor sendet eine SNMP-GET-Anfrage mit den OIDs 1.3.6.1.4.1.5951.4.1.1.41.1.5, 1.3.6.1.4.1.5951.4.1.1.41.1.4 und

1.3.6.1.4.1.5951.4.1.1.41.1.3 an die Dienste. SNMP-OIDs vom Typ STRING werden nicht unterstützt, da Sie die Last nicht mithilfe einer STRING-OID berechnen können. Lasten können mithilfe anderer Datentypen wie INT und Gauge32 berechnet werden. Die drei Dienste antworten auf die Anfrage. Die NetScaler-Appliance vergleicht die exportierten Metriken und wählt dann Service-HTTP-1 aus, da sie über mehr verfügbaren Speicher verfügt. Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 2. So funktioniert die benutzerdefinierte Lademethode



Wenn jede Anforderung 10 MB Speicher verwendet, stellt die NetScaler-Appliance Anfragen wie folgt bereit:

- Service-HTTP-1 empfängt die erste, zweite, dritte, vierte und fünfte Anfrage, da dieser Dienst den niedrigsten N-Wert hat.
- Service-HTTP-1 und Service-HTTP-2 haben jetzt dieselbe Last, sodass der virtuelle Server für diese Server zur Round-Robin-Methode zurückkehrt. Daher erhält Service-HTTP-2 die sechste Anforderung, und Service-HTTP-1 empfängt die siebte Anforderung.
- Da Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 jetzt alle dieselbe Last haben, kehrt der virtuelle Server auch auf die Round-Robin-Methode für Service-HTTP-3 zurück. Daher erhält Service-HTTP-3 die achte Anforderung.

In der folgenden Tabelle wird zusammengefasst, wie N berechnet wird.

Anfrage erhalten	Dienst ausgewählt	Aktueller N-Wert (Anzahl der aktiven Transaktionen)	Bemerkungen
Request-1	Service-HTTP-1; (N = 20)	N = 30	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-1; (N = 30)	N = 40	-
Request-3	Service-HTTP-1; (N = 40)	N = 50	-
Request-4	Service-HTTP-1; (N = 50)	N = 60	-
Request-5	Service-HTTP-1; (N = 60)	N = 70	-
Request-6	Service-HTTP-1; (N = 70)	N = 80	Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte.
Request-7	Service-HTTP-2; (N = 70)	N = 80	Service-HTTP-3 haben dieselben N-Werte.
Request-8	Service-HTTP-1; (N = 80)	N = 90	Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 haben dieselben N-Werte.

Wenn den Diensten unterschiedliche Gewichte zugewiesen werden, berücksichtigt der benutzerdefinierte Lastalgorithmus sowohl die Belastung der einzelnen Dienste als auch die jedem Dienst zugewiesene Gewichtung. Es wählt einen Dienst aus, indem der Wert (Nw) im folgenden Ausdruck verwendet wird:

Nw = (N) * (10000/Gewicht)

Nehmen wir wie im vorherigen Beispiel an, Service-HTTP-1 wird eine Gewichtung von 4 zugewiesen, Service-HTTP-2 wird eine Gewichtung von 3 zugewiesen und Service-HTTP-3 wird eine Gewichtung von 2 zugewiesen. Wenn jede Anforderung 10 MB Speicher verwendet, stellt die NetScaler-Appliance Anfragen wie folgt bereit:

- Service-HTTP-1 empfängt die erste, zweite, dritte, vierte, fünfte, sechste, siebte und achte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die neunte Anfrage, da dieser Dienst den niedrigsten Nw-Wert hat.

Service-HTTP-3 hat den höchsten Nw-Wert und wird daher für den Lastenausgleich nicht berücksichtigt.

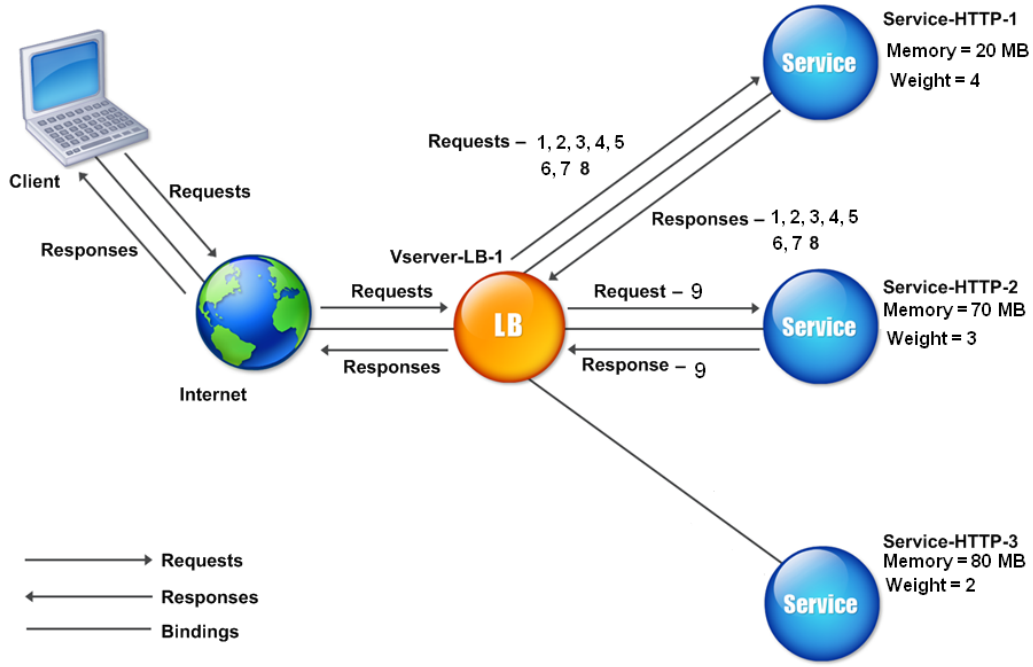
In der folgenden Tabelle wird zusammengefasst, wie Nw berechnet wird.

Anfrage erhalten	Dienst ausgewählt	Aktueller Neuwert (Anzahl der aktiven Transaktionen) * (10000 /Gewicht)	Bemerkungen
Request-1	Service-HTTP-1; (Jetzt = 50000)	Nw = 75000	Service-HTTP-1 hat den niedrigsten Nw-Wert.
Request-2	Service-HTTP-1; (Nw = 5000)	Neu = 100000	-
Request-3	Service-HTTP-1; (Nw = 15000)	Nw = 125000	-
Request-4	Service-HTTP-1; (Nw = 20000)	Neu = 150000	-
Request-5	service-HTTP-1; (Jetzt = 23333.34)	Nw = 175000	-
Request-6	Service-HTTP-1; (Jetzt = 25000)	Neu = 200000	-
Request-7	service-HTTP-1; (Jetzt = 23333.34)	Neu = 225000	-
request-8|service-HTTP-1; (Nw = 25000) |Nw = 250000||-| |Request-9|service-HTTP-2; (Nw = 233333.34) |Nw = 266666.67|Service-HTTP-2 hat den niedrigsten
Nw-Wert.

Service-HTTP-1 wird für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn der Nw-Wert anderer Dienste (Service-HTTP-2 und Service-HTTP-3) 400.000 beträgt.

Das folgende Diagramm zeigt, wie die NetScaler-Appliance die benutzerdefinierte Lademethode verwendet, wenn Gewichte zugewiesen werden.

Abbildung 3. Funktionsweise der benutzerdefinierten Lademethode beim Zuweisen von Gewichten



Informationen zum Konfigurieren der benutzerdefinierten Lademethode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Methode der statischen Nähe

June 19, 2023

Wenn ein virtueller Server für die Verwendung der statischen Näherungsmethode konfiguriert ist, wählt er den Dienst aus, der den Näherungskriterien am besten entspricht.

Damit die statische Proximity-Methode funktioniert, müssen Sie entweder die NetScaler-Appliance so konfigurieren, dass sie eine vorhandene statische Proximity-Datenbank verwendet, die über eine Standortdatei gefüllt wird, oder der statischen Proximity-Datenbank benutzerdefinierte Einträge hinzufügen. Nachdem Sie benutzerdefinierte Einträge hinzugefügt haben, können Sie deren Standortqualifikatoren festlegen. Nach der Konfiguration der Datenbank können Sie die statische Nähe als Load-Balancing-Methode angeben.

Weitere Informationen finden Sie in den folgenden Themen.

- Hinzufügen einer Standortdatei zur Erstellung einer statischen Proximity-Datenbank

- Hinzufügen benutzerdefinierter Einträge zu einer statischen Proximity-Datenbank
- Einstellung der Standortqualifikatoren
- Angabe der Methode Static Proximity

Angabe der Proximity-Methode

Wenn Sie die statische Proximity-Datenbank konfiguriert haben, können Sie statische Nähe als GLSB-Methode angeben.

So geben Sie die statische Nähe mithilfe der Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile die folgenden Befehle ein, um die statische Nähe zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -lbMethod STATICPROXIMITY

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod STATICPROXIMITY

show lb vserver
<!--NeedCopy-->
```

Um die statische Nähe mithilfe der GUI zu spezifizieren

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server** und wählen Sie den virtuellen Server aus.
2. Klicken Sie auf **Bearbeiten** und erweitern Sie den Abschnitt **Methode** .
3. Wählen Sie in der Liste der **Load Balancing-Methoden** die Option **STATICPROXIMITY**aus.

> **Hinweis**
>
> Aktivieren Sie den Parameter proximityFromSelf, um die Loopback-IP-Adresse des Netscalers anstelle der IP-Adresse des Clients zu verwenden, um den nächstgelegenen Serverstandort für den statischen Proximity-Load-Balancing oder die GSLB-Entscheidung abzurufen.

Token-Methode

May 11, 2023

Ein virtueller Lastausgleichsserver, der für die Verwendung der Token-Methode konfiguriert ist, stützt seine Auswahl eines Dienstes auf dem Wert eines Datensegments, das aus der Clientanforderung extrahiert wurde. Das Datensegment wird als Token bezeichnet. Sie konfigurieren den Ort und die Größe des Tokens. Für nachfolgende Anforderungen mit demselben Token wählt der virtuelle Server denselben Dienst aus, der die ursprüngliche Anforderung verarbeitet hat.

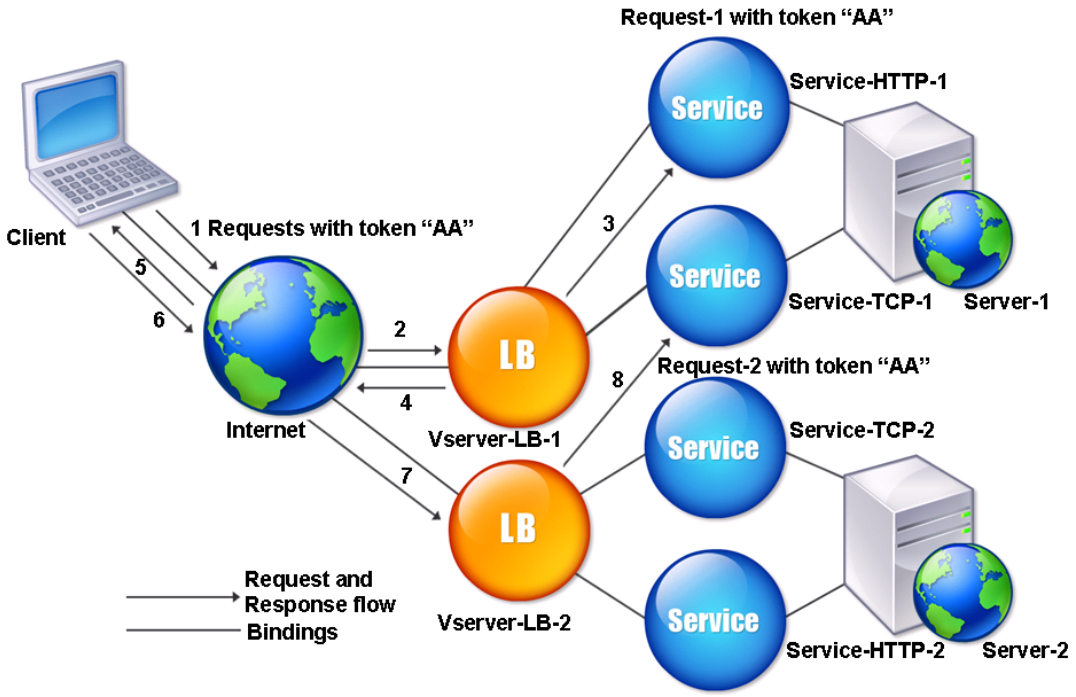
Diese Methode ist inhaltsbewusst. Es funktioniert unterschiedlich für TCP-, HTTP- und HTTPS-Verbindungen. Bei HTTP- oder HTTPS-Diensten befindet sich das Token in den HTTP-Headern, der URL oder im BODY. Um das Token zu finden, geben oder erstellen Sie einen klassischen oder erweiterten Ausdruck. Weitere Informationen zu klassischen oder erweiterten Ausdrücken finden Sie unter Richtlinienkonfiguration und Referenz.

Bei HTTP-Diensten sucht der virtuelle Server nach dem konfigurierten Token in den ersten 24 Kilobyte (KB) der TCP-Nutzlast. Bei Nicht-HTTP-Diensten (TCP, SSL und SSL_TCP) sucht der virtuelle Server in den ersten 16 Paketen nach dem konfigurierten Token, wenn die Gesamtgröße der 16 Pakete weniger als 24 KB beträgt. Wenn die Gesamtgröße der 16 Pakete jedoch mehr als 24 KB beträgt, sucht die Appliance in den ersten 24 KB der Payload nach dem Token. Sie können diese Lastausgleichsmethode für virtuelle Server verschiedener Typen verwenden, um sicherzustellen, dass Anfragen, die dasselbe Token verwenden, unabhängig vom verwendeten Protokoll an die entsprechenden Dienste weitergeleitet werden.

Stellen Sie sich zum Beispiel ein Load-Balancing-Setup vor, das aus Servern besteht, die Webinhalte enthalten. Sie möchten die NetScaler-Appliance so konfigurieren, dass sie im URL-Abfrageteil der Anfrage nach einer bestimmten Zeichenfolge (dem Token) sucht. Server-1 hat zwei Dienste, Service-HTTP-1 und Service-TCP-1, und Server-2 hat zwei Dienste, Service-HTTP-2 und Service-TCP-2. Die TCP-Dienste sind an vServer-LB-2 gebunden, und die HTTP-Dienste sind an vServer-LB-1 gebunden.

Wenn vServer-LB-1 eine Anfrage mit dem Token AA empfängt, wählt es den Dienst Service-HTTP-1 (gebunden an Server-1) aus, um die Anfrage zu verarbeiten. Wenn vServer-LB-2 eine andere Anfrage mit demselben Token (AA) empfängt, leitet es diese Anfrage an den Dienst Service-TCP-1 weiter. Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 1. Funktionsweise der Token-Methode



So konfigurieren Sie die Token-Load Balancing-Methode mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Token-Load-Balancing-Methode zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -lbMethod TOKEN -rule <rule> -datalength <length>
    -dataoffset <offset>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver LB-VServer-1 -lbMethod TOKEN -rule 'AA' -datalength 2 -
   dataoffset 25

show lb vserver LB-VServer-1
<!--NeedCopy-->
```


So konfigurieren Sie die Token-Load-Balancing-Methode mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Klicken Sie in den Erweiterten Einstellungen auf Methode
3. Wählen Sie in der Liste Load Balancing Method die Option Token aus, und geben Sie einen Ausdruck an.

Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält

May 11, 2023

Nachdem Sie einen Load-Balancing-Algorithmus für Ihr Load-Balancing-Setup ausgewählt haben, müssen Sie die NetScaler-Appliance so konfigurieren, dass sie diesen Algorithmus verwendet. Sie können es mithilfe der CLI oder mithilfe des Konfigurationsprogramms konfigurieren.

Hinweis:

Die Token-Methode ist richtlinienbasiert und erfordert mehr Konfiguration als hier beschrieben. Informationen zum Konfigurieren der Token-Methode finden Sie unter Token-Methode.

Bei einigen hash-basierten Methoden können Sie eine IP-Adresse maskieren, um Anforderungen zu demselben Subnetz an denselben Server zu leiten. Weitere Informationen finden Sie unter Hashing-Methoden.

So legen Sie die Load Balancing-Methode mit der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -lbMethod <method>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod LeastConnection
<!--NeedCopy-->
```


So legen Sie die Load-Balancing-Methode mithilfe des Konfigurationsprogramms fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf **Methode**, und wählen Sie in der Liste Load Balancing Method eine Methode aus.

Persistenz und persistente Verbindungen

May 11, 2023

Ein zustandsloses Lastenausgleichsprotokoll wie HTTP unterbricht die Pflege von Statusinformationen über Clientverbindungen, wenn die Persistenz nicht konfiguriert ist. Verschiedene Übertragungen desselben Clients können an verschiedene Server weitergeleitet werden, obwohl alle Übertragungen Teil derselben Sitzung sind. Sie können die Persistenz auf einem virtuellen Lastenausgleichsserver konfigurieren, der bestimmte Arten von Webanwendungen wie Einkaufswagen-Anwendungen verarbeitet.

Bevor Sie Persistenz konfigurieren können, müssen Sie die verschiedenen Arten von Persistenz verstehen, wie sie verwendet werden und welche Auswirkungen sie haben. Anschließend müssen Sie die NetScaler Appliance so konfigurieren, dass sie dauerhafte Verbindungen für die Websites und Webanwendungen bereitstellt, die sie benötigen.

Sie können auch die Backup-Persistenz konfigurieren, die wirksam wird, wenn der primäre Persistenztyp, der für einen virtuellen Lastausgleichsserver konfiguriert ist, fehlschlägt. Sie können Persistenzgruppen so konfigurieren, dass eine Clientübertragung an einen beliebigen virtuellen Server in einer Gruppe an einen Server weitergeleitet werden kann, der frühere Übertragungen vom selben Client empfangen hat.

Informationen zur Persistenz beim RADIUS-Lastenausgleich finden Sie unter Konfigurieren des RADIUS-Lastenausgleichs mit Persistenz.

Über Persistence

May 11, 2023

Sie können zwischen verschiedenen Arten von Persistenz für einen bestimmten virtuellen Lastenausgleichsserver wählen, der dann alle Verbindungen vom selben Benutzer an Ihre Einkaufswagenanwendung, webbasierte E-Mail oder andere Netzwerkanwendung an denselben Dienst weiterleitet. Die Persistenzsitzung bleibt für die von Ihnen angegebene Zeit in Kraft.

Wenn ein an einer Persistenzsitzung teilnehmender Server heruntergefahren wird, verwendet der virtuelle Lastausgleichsserver die konfigurierte Lastenausgleichsmethode, um einen neuen Dienst auszuwählen, und richtet eine neue Persistenzsitzung mit dem von diesem Dienst vertretenen Server ein. Wenn der Server AUSSER BETRIEB geht, verarbeitet er weiterhin bestehende Persistenzsitzungen, aber der virtuelle Server leitet keinen neuen Datenverkehr an ihn weiter. Nach Ablauf der Shutdown-Phase stellt der virtuelle Server die Weiterleitung von Verbindungen von vorhandenen Clients zum Dienst ein, schließt bestehende Verbindungen und leitet diese Clients bei Bedarf an neue Dienste weiter.

Je nach dem von Ihnen konfigurierten Persistenztyp untersucht die NetScaler-Appliance möglicherweise die Quell-IPs, Ziel-IPs, SSL-Sitzungs-IDs, Host- oder URL-Header oder eine Kombination dieser Dinge, um jede Verbindung der richtigen Persistenzsitzung zuzuordnen. Es kann auch die Persistenz auf einem Cookie basieren, das vom Webserver ausgegeben wird, auf einem willkürlich zugewiesenen Token oder auf einer logischen Regel. Fast alles, was es der Appliance ermöglicht, Verbindungen mit der richtigen Persistenzsitzung abzugleichen, und wird als Grundlage für Persistenz verwendet.

In der folgenden Tabelle werden die Persistenztypen zusammengefasst, die auf der NetScaler Appliance verfügbar sind.

Persistenz-Typ	Beschreibung
Quell-IP	QUELLE/IP. Verbindungen von derselben Client-IP-Adresse sind Teil derselben Persistenzsitzung.
HTTP-Cookie	PLÄTZCHEN/EINFÜGEN. Verbindungen, die denselben HTTP-Cookie-Header haben, sind Teil derselben Persistenzsitzung.
SSL-Sitzung ID	SSLSESSION. Verbindungen mit derselben SSL-Sitzungs-ID sind Teil derselben Persistenzsitzung.
URL Passive	URL/PASSIV. Verbindungen zu derselben URL werden als Teile derselben Persistenzsitzung behandelt.
Benutzerdefinierte Server-ID	BENUTZERDEFINIERTE SERVER-ID. Verbindungen mit demselben HTTP-HOST-Header werden als Teile derselben Persistenzsitzung behandelt.
Ziel-IP	DESTIP. Verbindungen zu derselben Ziel-IP werden als Teile derselben Persistenzsitzung behandelt.

Persistenz-Typ	Beschreibung
Quell- und Ziel-IPs	SKRIPTSPITZE. Verbindungen, die sowohl von derselben Quell-IP als auch von derselben Ziel-IP ausgehen, werden als Teile derselben Persistenzsitzung behandelt.
SIP-Anruf-ID	KALLID. Verbindungen, die dieselbe Anruf-ID im SIP-Header haben, werden als Teile derselben Persistenzsitzung behandelt.
RTSP-Sitzungs-ID	RTSPSID. Verbindungen mit derselben RTSP-Sitzungs-ID werden als Teile derselben Persistenzsitzung behandelt.
Benutzerdefinierte Regel	REGEL. Verbindungen, die einer benutzerdefinierten Regel entsprechen, werden als Teile derselben Persistenzsitzung behandelt.

Tabelle 1. Arten der Persistenz

Abhängig von der Art der Persistenz, die Sie konfiguriert haben, kann der virtuelle Server entweder 250.000 gleichzeitige persistente Verbindungen oder eine beliebige Anzahl persistenter Verbindungen unterstützen, bis die Grenzen liegen, die sich aus der RAM-Größe Ihrer NetScaler-Appliance ergeben. Die folgende Tabelle zeigt, welche Arten von Persistenz in die einzelnen Kategorien fallen.

Persistenz-Typ	Anzahl der unterstützten gleichzeitigen persistenten Verbindungen
Quell-IP, SSL-Sitzungs-ID, Regel, Ziel-IP, Quell-IP/Ziel-IP, SIP-Anruf-ID, RTSP-Sitzungs-ID	250 K
Cookie, URL-Server-ID, benutzerdefinierte Server-ID	Speicherbegrenzung. Wenn in CookieInsert ein Timeout nicht 0 ist, wird die Anzahl der Verbindungen durch den Speicher begrenzt.

Tabelle 2. Persistenztypen und Anzahl der unterstützten gleichzeitigen Verbindungen

Einige Arten der Persistenz sind spezifisch für bestimmte Arten von virtuellen Servern. In der folgenden Tabelle sind die einzelnen Persistenztypen aufgeführt und es wird angegeben, welche Arten von Persistenz auf welchen virtuellen Servertypen unterstützt werden.

Persistenz-Typ	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEI	JA	JA	JA	JA	JA	JA	NEIN	NEIN
PLÄTZCHEN EINFÜ-GEN	JA	JA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
SSL-SITZUNG	NEIN	JA	NEIN	NEIN	JA	JA	NEIN	NEIN
URL PASSIV	JA	JA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
BENUTZE SERVER-ID	JA	JA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
REGEL	JA	JA	JA	NEIN	NEIN		NEIN	NEIN
SRCIPDE	JA	JA	JA	JA	JA	JA	NEIN	NEIN
DESTIP	JA	JA	JA	JA	JA	JA	NEIN	NEIN
KALLID	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA
RTSPID	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	NEIN

Tabelle 3. Beziehung des Persistenztyps zum virtuellen Servertyp

Persistenz der Quell-IP-Adresse

May 11, 2023

Wenn die Quell-IP-Persistenz konfiguriert ist, verwendet der virtuelle Lastausgleichsserver die konfigurierte Lastausgleichsmethode, um einen Dienst für die erste Anforderung auszuwählen, und verwendet dann die Quell-IP-Adresse (Client-IP-Adresse), um nachfolgende Anfragen von diesem Client zu identifizieren und an denselben Dienst zu senden. Sie können einen Timeout-Wert festlegen, der die maximale Inaktivitätsdauer für die Sitzung angibt. Wenn der Timeout-Wert abgelaufen ist, wird die Sitzung verworfen und der konfigurierte Load-Balancing-Algorithmus wird verwendet, um einen neuen Server auszuwählen.

Achtung: Unter bestimmten Umständen kann die Verwendung von Persistenz basierend auf Quell-IP-Adresse Ihre Server überlasten. Alle Anfragen an eine einzelne Website oder Anwendung werden über das einzelne Gateway zur NetScaler Appliance weitergeleitet, obwohl sie dann an mehrere Standorte

umgeleitet werden. In mehreren Proxy-Umgebungen haben Clientanfragen häufig unterschiedliche Quell-IP-Adressen, selbst wenn sie vom selben Client gesendet werden, was zu einer schnellen Multiplikation von Persistenzsitzungen führt, in denen eine einzelne Sitzung erstellt werden muss. Dieses Problem wird als Mega Proxy Problem bezeichnet. Sie können HTTP-Cookie-basierte Persistenz anstelle der Quell-IP-basierten Persistenz verwenden, um dies zu verhindern.

Informationen zum Konfigurieren der Persistenz basierend auf der Quell-IP-Adresse finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Hinweis: Wenn der gesamte eingehende Datenverkehr hinter einem NAT (Network Address Translation) -Gerät oder -Proxy stammt, scheint der Datenverkehr für die NetScaler Appliance von einer einzigen Quell-IP-Adresse zu stammen. Dadurch wird verhindert, dass die Quell-IP-Persistenz ordnungsgemäß funktioniert. In diesem Fall müssen Sie einen anderen Persistenztyp auswählen.

Persistenz von HTTP-Cookies

May 11, 2023

Wenn die HTTP-Cookie-Persistenz konfiguriert ist, setzt die NetScaler-Appliance ein Cookie in den HTTP-Headern der ersten Client-Anfrage. Das Cookie enthält die IP-Adresse und den Port des Dienstes, der vom Load-Balancing-Algorithmus ausgewählt wurde. Wie bei jeder HTTP-Verbindung schließt der Client dieses Cookie dann bei allen nachfolgenden Anfragen ein.

Wenn die NetScaler-Appliance das Cookie erkennt, leitet sie die Anfrage an die Dienst-IP und den Port im Cookie weiter und sorgt so für die Persistenz der Verbindung. Sie können diese Art der Persistenz mit virtuellen Servern vom Typ HTTP oder HTTPS verwenden. Dieser Persistenztyp verbraucht keine Appliance-Ressourcen und kann daher eine unbegrenzte Anzahl persistenter Clients aufnehmen.

Hinweis: Wenn der Webbrowser des Clients so konfiguriert ist, dass er Cookies ablehnt, funktioniert die auf HTTP-Cookie basierende Persistenz nicht. Es kann ratsam sein, einen Cookie-Check auf der Website zu konfigurieren und Kunden, die Cookies anscheinend nicht ordnungsgemäß speichern, zu warnen, dass sie Cookies für die Website aktivieren müssen, wenn sie sie verwenden möchten.

Das Cookie-Format, das von der NetScaler Appliance eingefügt wird, lautet:

```
NSC_XXXX=<ServiceIP ><ServicePort>
```

Es gilt:

- NSC_XXXX ist die virtuelle Server-ID, die vom Namen des virtuellen Servers abgeleitet wird.
- ServiceIP und ServicePort sind codierte Repräsentationen der Dienst-IP-Adresse bzw. des Serviceports. Die IP-Adresse und der Port werden separat codiert.

Sie können einen Timeoutwert für diesen Persistenztyp festlegen, um einen Inaktivitätszeitraum für die Sitzung anzugeben. Wenn die Verbindung für den angegebenen Zeitraum inaktiv war, verwirft

die NetScaler Appliance die Persistenzsitzung. Jede nachfolgende Verbindung von demselben Client führt dazu, dass ein neuer Server basierend auf der konfigurierten Lastausgleichsmethode ausgewählt wird und eine neue Persistenzsitzung eingerichtet wird.

Hinweis: Wenn Sie den Timeout-Wert auf 0 setzen, gibt die NetScaler-Appliance keine Ablaufzeit an, sondern setzt ein Sitzungscookie, das nicht gespeichert wird, wenn der Browser des Clients heruntergefahren wird.

Standardmäßig setzt die NetScaler-Appliance HTTP-Cookies der Version 0, um maximale Kompatibilität mit Clientbrowsern zu gewährleisten. (Nur bestimmte HTTP-Proxys verstehen die Cookies der Version 1, die am häufigsten verwendeten Browser nicht.) Sie können die Appliance so konfigurieren, dass sie HTTP-Version 1-Cookies setzt, um RFC2109 zu entsprechen. Bei HTTP-Cookies der Version 0 fügt die Appliance das Ablaufdatum und die Uhrzeit des Cookies als absolute koordinierte Weltzeit (GMT) ein. Dieser Wert wird als Summe der aktuellen GMT-Zeit auf der Appliance und des Timeout-Werts berechnet. Für HTTP-Version 1-Cookies fügt die Appliance eine relative Ablaufzeit ein, indem sie das „Max-Age“ -Attribut des HTTP-Cookies festlegt. In diesem Fall berechnet der Browser des Clients die tatsächliche Ablaufzeit.

Informationen zum Konfigurieren der Persistenz basierend auf einem von der Appliance eingefügten Cookie finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Im HTTP-Cookie legt die Appliance standardmäßig das `HTTPOnly` Flag fest, um anzuzeigen, dass das Cookie nicht skriptfähig ist und der Clientanwendung nicht bekannt gegeben werden darf. Daher kann ein clientseitiges Skript nicht auf das Cookie zugreifen, und der Client ist nicht anfällig für siteübergreifende Skripterstellung.

Bestimmte Browser unterstützen das `HTTPOnly` Flag jedoch nicht und geben das Cookie daher möglicherweise nicht zurück. Infolgedessen ist die Beharrlichkeit gebrochen. Für Browser, die das Flag nicht unterstützen, können Sie das `HTTPOnly` Flag im Persistenz-Cookie weglassen.

So ändern Sie die `HTTPOnly` Flag-Einstellung mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb parameter -httpOnlyCookieFlag (ENABLED|DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
>  set lb parameter -httpOnlyCookieFlag disabled
   Done
> show lb parameter
  Global LB parameters:
       Persistence Cookie HttpOnly Flag: DISABLED
       Use port for hash LB: YES
```



```
 Done
<!--NeedCopy-->
```

So ändern Sie die HTTPOnly Flag-Einstellung mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing Parameter konfigurieren**, und wählen oder deaktivieren Sie das Flag “ **Persistenz-Cookie HttpOnly**”.

Verschlüsseln des Cookies

Ab Version 10.5 Build 55.8 können Sie das Cookie zusätzlich zu jeder beliebigen SSL-Verschlüsselung verschlüsseln.

Um das Cookie mithilfe der Befehlszeilenschnittstelle zu verschlüsseln, geben Sie in der Befehlszeile Folgendes ein

```
set lb parameter -UseEncryptedPersistenceCookie ENABLED -
   cookiePassphrase test
<!--NeedCopy-->
```

Um das Cookie mithilfe des Konfigurationsprogramms zu verschlüsseln

1. **Navigieren Sie zu**Traffic Management**>**Load Balancing-Parameter ändern**, wählen Sie „**Verschlüsseln von Persistenz-Cookie-Werten“ und geben Sie eine Passphrase in das Feld Cookie-Passphrase**ein.**

Persistenz der SSL-Sitzungs-ID

May 11, 2023

Wenn die SSL-Sitzungs-ID-Persistenz konfiguriert ist, verwendet die NetScaler Appliance die SSL-Sitzungs-ID, die Teil des SSL-Handshake-Prozesses ist, um eine Persistenzsitzung zu erstellen, bevor die erste Anforderung an einen Dienst weitergeleitet wird. Der virtuelle Lastausgleichsserver leitet nachfolgende Anforderungen mit derselben SSL-Sitzungs-ID an denselben Dienst weiter. Diese Art der Persistenz wird für SSL-Brückendienste verwendet.

Hinweis:

Es gibt zwei Probleme, die Benutzer berücksichtigen müssen, bevor sie sich für diese Art von Persistenz entscheiden. Erstens verbraucht dieser Persistenztyp Ressourcen auf der NetScaler Appliance,

wodurch die Anzahl der gleichzeitig unterstützten Persistenzsitzungen begrenzt wird. Wenn Sie erwarten, mehrere Persistenzsitzungen zu unterstützen, sollten Sie möglicherweise eine andere Art von Persistenz wählen.

Zweitens, wenn der Client und der Server mit Lastausgleich die Sitzungs-ID während ihrer Transaktionen neu verhandeln müssen, wird die Persistenz nicht beibehalten, und eine neue Persistenzsitzung wird erstellt, wenn die nächste Anforderung des Clients empfangen wird. Dies kann dazu führen, dass die Aktivitäten des Kunden auf der Website unterbrochen werden und der Client möglicherweise aufgefordert wird, sich erneut zu authentifizieren oder die Sitzung neu zu starten. Dies kann auch zu einer großen Anzahl verlassener Sitzungen führen, wenn das Timeout auf einen zu großen Wert eingestellt ist.

Informationen zum Konfigurieren der Persistenz basierend auf der SSL-Sitzungs-ID finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

> **Hinweis**
>
> SSL-Sitzungs-ID-Persistenz wird bei Sitzungstickets nicht unterstützt.

Sichern Sie die Persistenzunterstützung für SSL-Sitzungs-ID

Ab NetScaler Version 12.0 Build 56.20 wird die Quell-IP-Persistenz als Backuppersistenztyp für die SSL-Sitzungs-ID-Persistenz unterstützt. Wenn der Client und der Load-Balancing-Server die Sitzung neu aushandeln und die Quell-IP-Persistenz als Backup-Persistenz konfiguriert ist, werden Clientanfragen an denselben Server weitergeleitet.

Um die Backup-Persistenz für die SSL-Sitzungs-ID zu unterstützen, erstellt die NetScaler-Appliance Sitzungseinträge sowohl für die Quell-IP als auch für die SSL-Sitzungs-ID, wenn eine Clientanfrage zum ersten Mal empfangen wird. Für die nachfolgenden Anfragen, die dieselbe Sitzungs-ID enthalten, wird die SSL-Sitzungs-ID verwendet. Wenn der Client und der Server mit Lastenausgleich die Sitzung neu verhandeln, wird die Clientanforderung mit der Quell-IP-Persistenz an denselben Server weitergeleitet und ein neuer SSL-Sitzungs-ID-Persistenzeintrag erstellt.

Informationen zum Konfigurieren der Backup-Persistenz finden Sie unter Konfigurieren der Backuppersistenz.

Diameter-AVP-Nummer-Persistenz

May 11, 2023

Sie können Persistenz verwenden, die auf der AVP-Nummer (Attribute-Value Pair) einer Diameter-Nachricht basiert, um persistente Diameter-Sitzungen zu erstellen. Wenn die NetScaler-Appliance

den AVP in der Diameter-Nachricht findet, erstellt sie eine Persistenzsitzung, die auf dem Wert des AVP basiert. Alle nachfolgenden Nachrichten, die dem Wert des AVP entsprechen, werden an den zuvor ausgewählten Server weitergeleitet. Wenn der Wert des AVP nicht mit der Persistenzsitzung übereinstimmt, wird eine neue Sitzung für den neuen Wert erstellt.

Hinweis: Wenn die AVP-Nummer nicht in Diameter-Basisprotokoll RFC 6733 definiert ist und die Nummer in einem gruppierten AVP verschachtelt ist, müssen Sie eine Folge von AVP-Nummern (maximal 3) in übergeordneter und untergeordneter Reihenfolge definieren. Wenn beispielsweise die persistente AVP-Nummer X innerhalb von AVP Y verschachtelt ist, das in Z verschachtelt ist, definieren Sie die Liste als Z Y X.

So konfigurieren Sie die Diameter-basierte Persistenz auf einem virtuellen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set lb vserver <name> -PersistenceType <type-> persistAVPno <
   positive_integer>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver diameter_vs -persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Benutzerdefinierte Server-ID-Persistenz

May 11, 2023

Bei der Persistenzmethode Custom Server ID wird die in der Clientanforderung angegebene Server-ID verwendet, um die Persistenz aufrechtzuerhalten. Damit diese Art der Persistenz funktioniert, müssen Sie zunächst eine Server-ID für die Dienste festlegen. Die NetScaler Appliance überprüft die URL der Clientanforderung und stellt eine Verbindung mit dem Server her, der der angegebenen Server-ID zugeordnet ist. Der Dienstanbieter muss sicherstellen, dass die Benutzer die Server-IDs kennen, die in ihren Anfragen für bestimmte Dienste bereitgestellt werden sollen.

Wenn Ihre Website beispielsweise verschiedene Datentypen wie Bilder, Text und Multimedia von verschiedenen Servern bereitstellt, können Sie jedem Server eine Server-ID zuweisen. Auf der NetScaler-Appliance geben Sie diese Server-IDs für die entsprechenden Dienste an und konfigurieren die benutzerdefinierte Server-ID-Persistenz auf dem entsprechenden virtuellen Load-Balancing-

Server. Beim Senden einer Anfrage fügt der Client die Server-ID in die URL ein, die den erforderlichen Datentyp angibt.

So konfigurieren Sie die Persistenz benutzerdefinierter Server-IDs:

- Weisen Sie in Ihrem Load-Balancing-Setup jedem Dienst, für den Sie die benutzerdefinierte Server-ID verwenden möchten, eine Server-ID zu, um die Persistenz aufrechtzuerhalten. Alphanumerische Server-IDs sind zulässig.
- Geben Sie Regeln in der standardmäßigen Syntaxausdruckssprache an, um die URL-Abfragen für die Server-ID zu untersuchen und den Datenverkehr an den entsprechenden Server weiterzuleiten.
- Konfigurieren Sie die benutzerdefinierte Server-ID-Persistenz.

Hinweis: Der Wert für das Persistenz-Timeout hat keinen Einfluss auf den Persistenztyp Benutzerdefinierte Server-ID. Die maximale Anzahl persistenter Clients ist unbegrenzt, da dieser Persistenztyp keine Clientinformationen speichert.

Beispiel:

Weisen Sie in einem Load-Balancing-Setup mit zwei Diensten Service-1 die Server-ID 2345-photo-56789 und Service-2 die Server-ID 2345-drawing-abb123 zu. Binden Sie diese Dienste an einen virtuellen Server namens Web11.

```
1 set service Service-1 10.102.29.5 -CustomServerID 2345-photo-56789
2
3 set service Service-2 10.102.29.6 -CustomServerID 2345-drawing-abb123
4 <!--NeedCopy-->
```

Aktivieren Sie auf dem virtuellen Server Web11 die benutzerdefinierte Server-ID-Persistenz.

Erstellen Sie den folgenden Ausdruck, damit alle URL-Abfragen, die die Zeichenfolge „sid=“ enthalten, untersucht werden.

HTTP.REQ.URL.AFTER_STR („sid=“)

Beispiel:

```
1 set lb vserver Web11 -persistenceType customserverID -rule "HTTP.REQ.
     URL.AFTER_STR("sid=")"
2
3 bind lb vserver Web11 Service-[1-2]
4 <!--NeedCopy-->
```

Wenn ein Client eine Anfrage mit der folgenden URL an die IP-Adresse von Web11 sendet, leitet die Appliance die Anfrage an Service-2 weiter und berücksichtigt die Persistenz.

Beispiel:


```
http://www.example.com/index.asp?&sid=2345-drawing-abb123
```

Weitere Informationen zu Standardsyntaxrichtlinienausdrücken finden Sie in der Richtlinienkonfiguration und -referenz.

So konfigurieren Sie die Persistenz der benutzerdefinierten Server-ID mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie den Dienst und legen Sie eine Server-ID fest.
3. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie den virtuellen Server.
4. Wählen Sie unter Erweiterte Einstellungen die Option Persistenz aus.
5. Wählen Sie CUSTOMESERVERID, und geben Sie einen Ausdruck an.

Persistenz der IP-Adresse

May 11, 2023

Sie können die Persistenz auf Ziel-IP-Adressen oder sowohl auf Quell-IP-Adressen als auch auf Ziel-IP-Adressen stützen.

Persistenz basierend auf Ziel-IP-Adressen

Wenn die NetScaler Appliance eine Anforderung von einem neuen Client empfängt, erstellt sie eine Persistenzsitzung basierend auf der IP-Adresse des vom virtuellen Server ausgewählten Dienstes (der Ziel-IP-Adresse). Später leitet es Anfragen an dieselbe Ziel-IP an denselben Dienst weiter. Diese Art der Persistenz wird beim Link-Load-Balancing verwendet. Weitere Informationen zum Link-Lastenausgleich finden Sie unter Link Load Balancing.

Der Timeout-Wert für die Ziel-IP-Persistenz entspricht dem für die Persistenz der Quell-IP-Persistenz, beschrieben unter Persistenz basierend auf Quell-IP-Adresse.

Informationen zum Konfigurieren der Persistenz basierend auf der Ziel-IP-Adresse finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Persistenz basierend auf Quell- und Ziel-IP-Adressen

Wenn die NetScaler Appliance eine Anforderung erhält, erstellt sie eine Persistenzsitzung, die sowohl auf der IP-Adresse des Clients (der Quell-IP-Adresse) als auch auf der IP-Adresse des vom virtuellen

Server ausgewählten Dienstes (der Ziel-IP-Adresse) basiert. Später leitet es Anfragen von derselben Quell-IP und an dieselbe Ziel-IP an denselben Dienst weiter.

Der Timeout-Wert für die Ziel-IP-Persistenz entspricht dem für die Persistenz der Quell-IP-Persistenz, beschrieben unter Persistenz basierend auf Quell-IP-Adresse.

Informationen zum Konfigurieren der Persistenz basierend auf Quell- und Ziel-IP-Adressen finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

SIP-Anruf-ID-Persistenz

May 11, 2023

Bei der SIP-Anruf-ID-Persistenz wählt die NetScaler-Appliance einen Dienst auf der Grundlage der Anruf-ID im SIP-Header aus. Dadurch kann es Pakete für eine bestimmte SIP-Sitzung an denselben Dienst und damit an denselben Lastausgleichsserver weiterleiten. Dieser Persistenztyp ist speziell für den SIP-Lastenausgleich anwendbar. Weitere Informationen zum SIP-Lastenausgleich finden Sie unter Überwachen von SIP-Diensten.

Informationen zum Konfigurieren der Persistenz basierend auf SIP-Anruf-ID finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

RTSP-Sitzungs-ID-Persistenz

May 11, 2023

Wenn die NetScaler Appliance eine Anforderung von einem neuen Client empfängt, erstellt sie eine Persistenzsitzung basierend auf der RTSP- Sitzungs-ID (Real-Time Streaming Protocol) im RTSP-Paket-Header und leitet die Anforderung dann an den RTSP-Dienst weiter, der vom konfigurierten Load Balancing ausgewählt wurde -Methode. Es leitet nachfolgende Anforderungen, die dieselbe Sitzungs-ID enthalten, an denselben Dienst weiter. Dieser Persistenztyp ist speziell für den SIP-Lastenausgleich anwendbar. Weitere Informationen zum SIP-Lastenausgleich finden Sie unter Überwachen von SIP-Diensten.

Hinweis: Die Persistenz der RTSP-Sitzungs-ID ist standardmäßig auf virtuellen RTSP-Servern konfiguriert, und Sie können diese Einstellung nicht ändern.

Manchmal geben verschiedene RTSP-Server dieselben Sitzungs-IDs aus. In diesem Fall können keine eindeutigen Sitzungen zwischen dem Client und dem RTSP-Server erstellt werden, indem nur die RTSP-Sitzungs-ID verwendet wird. Wenn Sie mehrere RTSP-Server haben, die möglicherweise dieselben Sitzungs-IDs ausgeben, können Sie die Appliance so konfigurieren, dass die IP-Adresse und den

Port des Servers an die Sitzungs-ID angehängt wird und ein eindeutiges Token erstellen, mit dem die Persistenz festgestellt werden kann. Dies wird als Sitzungs-ID-Zuordnung bezeichnet.

Informationen zum Konfigurieren von Persistenz basierend auf RTSP-Sitzungs-IDs finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Wichtig: Wenn Sie die Session-ID-Zuordnung verwenden müssen, müssen Sie den folgenden Parameter festlegen, wenn Sie jeden Service innerhalb der Load Balancing-Einrichtung konfigurieren. Stellen Sie außerdem sicher, dass keine nicht persistenten Verbindungen über den virtuellen RTSP Server weitergeleitet werden.

URL-passive Persistenz konfigurieren

May 11, 2023

Bei der passiven URL-Persistenz extrahiert die NetScaler-Appliance, wenn sie eine Anforderung von einem Client empfängt, die IP-Adress-Portinformationen des Servers (ausgedrückt als einzelne Hexadezimalzahl) aus der Clientanforderung.

Die passive URL-Persistenz erfordert die Konfiguration eines erweiterten Ausdrucks, der das Abfrageelement angibt, das die IP-Adressen-Port-Informationen des Servers enthält. Weitere Informationen zu klassischen und erweiterten Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

Mit dem folgenden Ausdruck wird die Appliance so konfiguriert, dass Anforderungen für URL-Abfragen untersucht werden, die die Zeichenfolge urlp= enthalten, die Server-IP-Adressen-Port-Informationen extrahiert, sie aus einer hexadezimalen Zeichenfolge in eine IP- und Portnummer konvertiert und die Anforderung an den Dienst weitergeleitet, der mit dieser IP-Adresse und Portnummer.

HTTP.REQ.URL.AFTER_STR(“urlp=”)

Wenn die passive URL-Persistenz aktiviert ist und der vorherige Ausdruck konfiguriert ist, wird eine Anforderung mit der folgenden URL- und Server-IP-Adressen-Port-Zeichenfolge an 10.102.29.10:80 weitergeleitet.

```
http://www.example.com/index.asp?&urlp=0A661D0A0050
```

Der Persistenz-Timeout-Wert hat keinen Einfluss auf diesen Persistenztyp. Die Persistenz bleibt erhalten, solange die IP-Adressen-Portinformationen des Servers aus Clientanforderungen extrahiert werden können. Dieser Persistenztyp verbraucht keine Appliance-Ressourcen, so dass er eine unbegrenzte Anzahl persistenter Clients aufnehmen kann.

Um die passive URL-Persistenz zu konfigurieren, konfigurieren Sie zunächst die Persistenz wie unter Persistenztypen konfigurieren beschrieben, die keine Regel erfordern. Sie setzen den Persistenztyp auf URLPASSIVE. Sie führen dann die folgenden Verfahren aus.

So konfigurieren Sie die passive URL-Persistenz mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

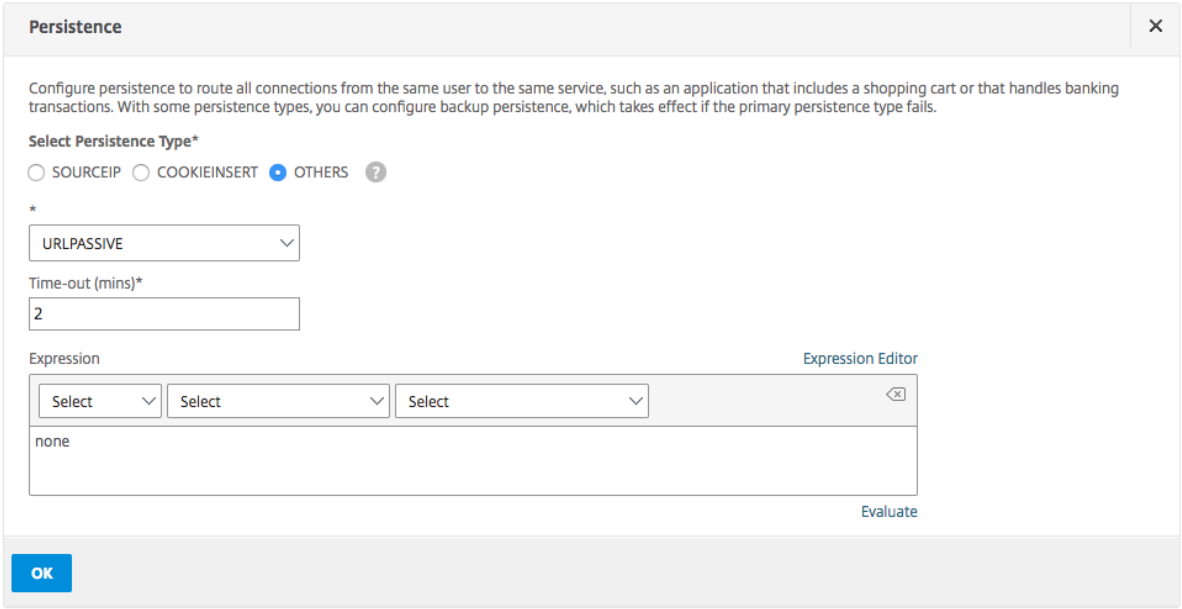
```
set lb vserver <vserverName>  [-persistenceType <persistenceType>]  [-rule <expression>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver LB-VServer-1 -persistenceType URLPASSIVE  -rule HTTP.REQ.URL.AFTER_STR( “urlp=” )
<!--NeedCopy-->
```

So konfigurieren Sie die Persistenz auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Wählen Sie im Abschnitt Persistenz den Persistenztyp aus, der Ihren Anforderungen entspricht. Der am besten geeignete Persistenztyp für den virtuellen Server ist als Optionsschaltflächen verfügbar. Andere Persistenztypen, die für den bestimmten virtuellen Servertyp gelten, können aus der Liste Andere ausgewählt werden.



> **Hinweis:**
>
> Vor NetScaler Release 12.0 Build 56.20 sind alle Persistenztypen in einer einzigen Persistence-Dropdownliste ohne Optionsschaltflächen verfügbar.

Persistenz basierend auf benutzerdefinierten Regeln konfigurieren

May 11, 2023

> **Warnung:**
>
> Die Verwendung klassischer Ausdrücke für die Persistenzregel in der Lastausgleichsfunktion wurde entfernt und ist ab Version 13.1 für die Filterregel auf der NetScaler-Appliance nicht mehr verfügbar. Citrix empfiehlt, diese Richtlinienausdrücke nicht über die NetScaler-Befehlszeilenschnittstelle, die NetScaler GUI oder die Nitro-Automatisierung zu verwenden. Weitere Informationen finden Sie in Tabelle 1 und Tabelle 2 auf der Seite Classic Policy Deprecation FAQ .

Wenn eine regelbasierte Persistenz konfiguriert ist, erstellt die NetScaler-Appliance eine Persistenzsitzung basierend auf dem Inhalt der übereinstimmenden Regel, bevor sie die Anforderung an den Dienst leitet, der von der konfigurierten Lastausgleichsmethode ausgewählt wurde. Später leitet es alle Anfragen, die mit der Regel übereinstimmen, an denselben Dienst weiter. Sie können regelbasierte Persistenz für Dienste vom Typ HTTP, SSL, RADIUS, ANY, TCP und SSL_TCP konfigurieren.

Regelbasierte Persistenz erfordert einen klassischen oder erweiterten Richtlinienausdruck. Sie können einen klassischen Ausdruck verwenden, um Anforderungskopfzeilen auszuwerten, oder Sie können einen erweiterten Richtlinienausdruck verwenden, um Anforderungskopfzeilen, Webformulardaten in einer Anforderung, Antwort-Header oder Antwortkörper auszuwerten. Sie können beispielsweise einen klassischen Ausdruck verwenden, um die Persistenz basierend auf dem Inhalt des HTTP-Host-Headers zu konfigurieren. Sie können auch einen erweiterten Richtlinienausdruck verwenden, um die Persistenz basierend auf Anwendungssitzungsinformationen in einem Antwort-Cookie oder einem benutzerdefinierten Header zu konfigurieren. Weitere Informationen zum Erstellen und Verwenden klassischer und erweiterter Richtlinienausdrücke finden Sie unter Richtlinien und Ausdrücke.

Die Ausdrücke, die Sie konfigurieren können, hängen von der Art des Dienstes ab, für den Sie regelbasierte Persistenz konfigurieren. Beispielsweise sind bestimmte RADIUS-spezifische Ausdrücke für andere Protokolle als RADIUS nicht zulässig, und TCP-Options-basierte Ausdrücke sind für andere Diensttypen als den Typ ANY nicht zulässig. Für TCP- und SSL_TCP-Diensttypen können Sie Ausdrücke verwenden, die TCP/IP-Protokolldaten, Layer-2-Daten, TCP-Optionen und TCP-Nutzlasten auswerten.

Hinweis: Für einen Anwendungsfall, der die Konfiguration regelbasierter Persistenz auf Basis von Financial Information Exchange (“FIX”) -Protokolldaten beinhaltet, die über TCP übertragen werden, finden Sie unter Konfigurieren regelbasierter Persistenz basierend auf einem Name-Wert-Paar in einem TCP-Byte-Stream.

Regelbasierte Persistenz kann verwendet werden, um die Persistenz mit Entitäten wie Citrix SD-WAN-Appliances, Citrix SD-WAN SD-WAN-Plug-Ins, Cache-Servern und Anwendungsservern aufrechtzuer-

halten.

Hinweis: Auf einem beliebigen virtuellen Server können Sie keine regelbasierte Persistenz für die Antworten konfigurieren.

Um die Persistenz basierend auf einer benutzerdefinierten Regel zu konfigurieren, konfigurieren Sie zunächst die Persistenz wie unter Persistenztypen konfigurieren beschrieben, die keine Regel erfordern, und legen den Persistenztyp auf REGEL fest. Sie können dann die folgenden Verfahren ausführen. Sie können die regelbasierte Persistenz mit dem Konfigurationsdienstprogramm oder der CLI konfigurieren.

So konfigurieren Sie die Persistenz basierend auf benutzerdefinierten Regeln über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

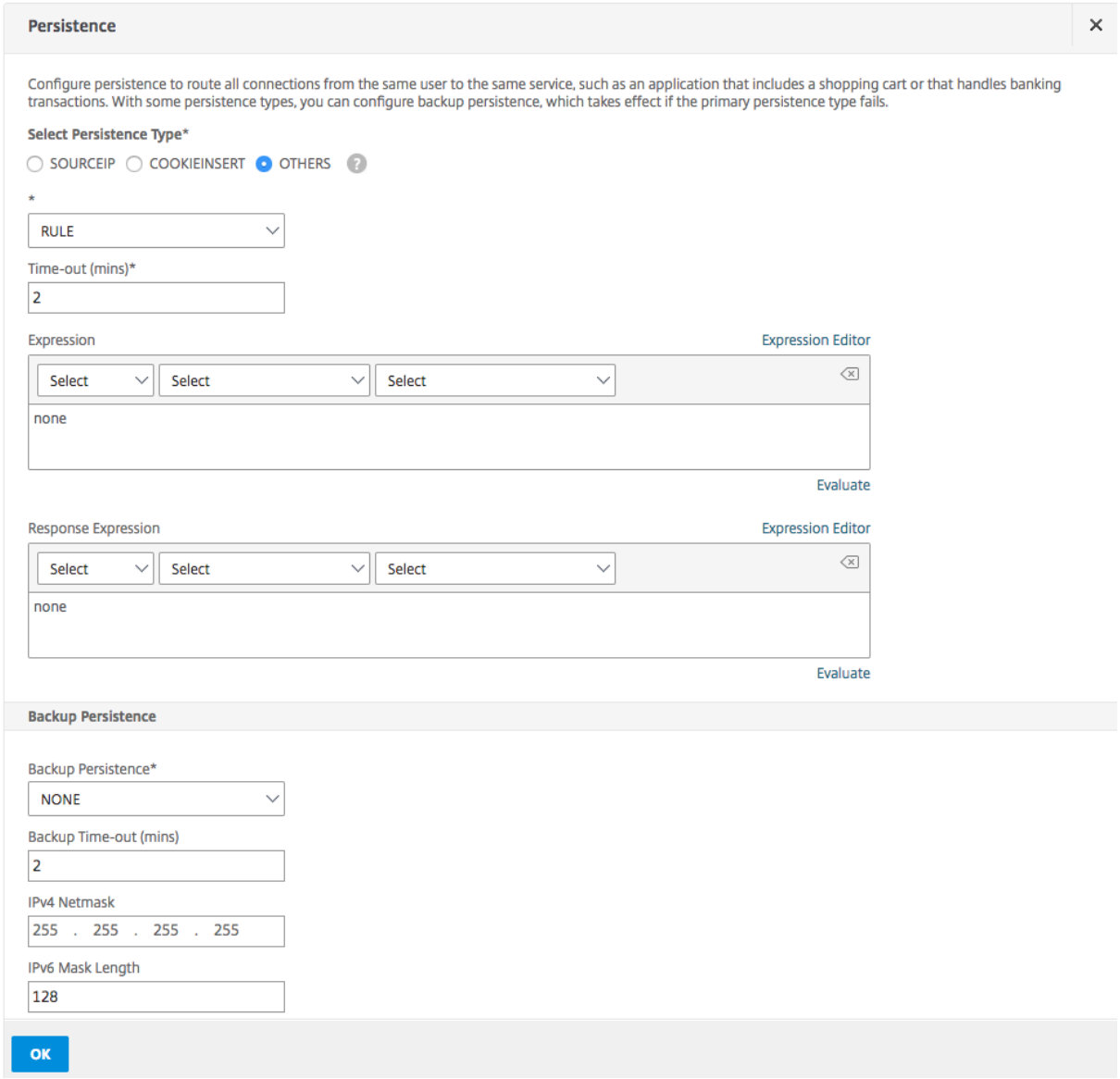
```
set lb vserver <vserverName> [-rule <expression>][-resRule <expression
    >]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vsvr_name -rule http.req.header("cookie").value(0).
    typecast_nvlist_t('=',';').value("server")

set lb vserver vsvr_name -resrule http.res.header("set-cookie").value
    (0).typecast_nvlist_t('=',';').value("server")

<!--NeedCopy-->
```

So konfigurieren Sie die Persistenz basierend auf benutzerdefinierten Regeln über die GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Wählen Sie im Abschnitt Persistenz den Persistenztyp aus, der Ihren Anforderungen entspricht. Der am besten geeignete Persistenztyp für den virtuellen Server ist als Optionsschaltflächen verfügbar. Andere Persistenztypen, die für den bestimmten virtuellen Servertyp gelten, können aus der Liste Andere ausgewählt werden.



> **Hinweis**
>
> Vor NetScaler Release 12.0 Build 56.20 sind alle Persistenztypen in einer einzigen Persistence-Dropdownliste ohne Optionsschaltflächen verfügbar.

Beispiel: Klassischer Ausdruck für eine Anforderungsnutzlast

Der folgende klassische Ausdruck erstellt eine Persistenzsitzung basierend auf dem Vorhandensein eines User-Agent-HTTP-Headers, der die Zeichenfolge “MyBrowser” enthält, und leitet alle nachfolgenden Clientanforderungen, die diesen Header und diese Zeichenfolge enthalten, an denselben Server weiter, der für die ursprüngliche Anforderung ausgewählt wurde.

```
1 http header User-Agent contains MyBrowser
```



```
<!--NeedCopy-->
```

Beispiel: Erweiterter Richtlinienausdruck für einen Anforderungskopf

Der folgende erweiterte Richtlinienausdruck macht dasselbe wie der vorherige klassische Ausdruck.

HTTP.REQ.HEADER (User-Agent) .CONTAINS (MyBrowser)

Beispiel: Erweiterte Richtlinie Ausdruck für ein Response-Cookie

Der folgende Ausdruck untersucht Antworten auf “Server” -Cookies und leitet dann alle Anfragen, die dieses Cookie enthalten, an denselben Server weiter, der für die ursprüngliche Anforderung ausgewählt wurde.

HTTP.RES.HEADER(“SET-COOKIE”).VALUE(0).TYPECAST_NVLIST_T(‘=’,’;’).VALUE(“server”)

Persistenztypen konfigurieren, für die keine Regel erforderlich ist

June 19, 2023

Um die Persistenz zu konfigurieren, müssen Sie zuerst einen virtuellen Lastausgleichsserver einrichten, wie unter Basic Load Balancing einrichtenbeschrieben. Anschließend konfigurieren Sie die Persistenz auf dem virtuellen Server.

So konfigurieren Sie die Persistenz auf einem virtuellen Server mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Persistenz zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -PersistenceType <type> [-timeout <integer>]

show lb vserver
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -persistenceType SOURCEIP -timeout 60

show lb vserver
<!--NeedCopy-->
```

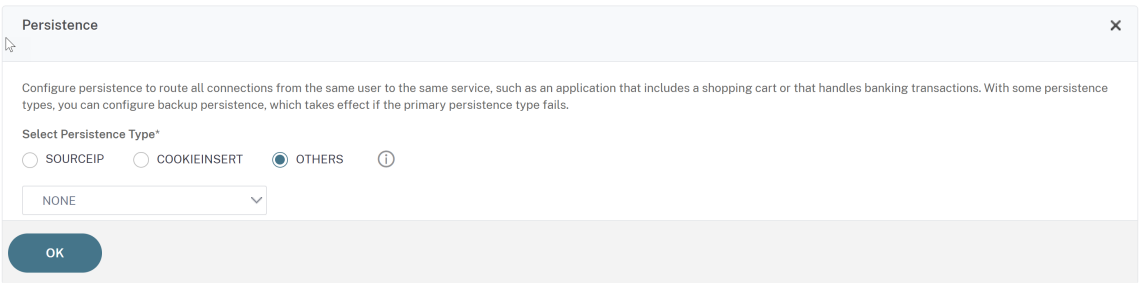

Timeout ist der Zeitraum, für den eine Persistenzsitzung aktiv ist. Die Timeout-Standard- und Mindestwerte (in Minuten) variieren je nach Persistenztyp, wie in der folgenden Tabelle aufgeführt.

Persistenztyp	Standardwert	Minimum	Maximum
Cookieeinfügen/Gruppe Cookie einfügen	2	0	1440
Andere Persistenztypen	2	2	1440

> **Hinweis**
>
> - Der Persistenztyp „Gruppen-Cookieeinfügung“ kann für die Load-Balancing-Gruppe festgelegt werden.
> - Für IP-basierte Persistenz können Sie auch den Parameter persistMask festlegen.
> - Der Persistenztyp ist standardmäßig auf NONE gesetzt.

So konfigurieren Sie die Persistenz auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Wählen Sie im Abschnitt Persistenz den Persistenztyp aus, der Ihren Anforderungen entspricht. Der am besten geeignete Persistenztyp für den virtuellen Server ist als Optionsschaltflächen verfügbar. Andere Persistenztypen, die für den bestimmten virtuellen Servertyp gelten, können aus der Liste **Andere** ausgewählt werden.



> **Hinweis** Vor NetScaler Release 12.0 Build 56.20 sind alle Persistenztypen in einer einzigen Persistenz-Dropdownliste ohne Optionsfelder verfügbar.

Konfigurieren der Backup-Persistenz

December 7, 2021

Sie können einen virtuellen Server so konfigurieren, dass er den Persistenztyp der Quell-IP verwendet, wenn der primäre Persistenztyp fehlschlägt.

In der folgenden Tabelle werden die Kombinationen von primären und sekundären Backup-Persistenztypen sowie die Bedingungen beschrieben, bei denen die Backup-Persistenz verwendet wird.

Primäre Persistenz	Backup-Persistenz	Wenn die primäre Persistenzsuche fehlschlägt…
CookieInsert	Quell-IP	Die Appliance greift nur dann auf Source-IP-basierte Persistenz zurück, wenn der Client-Browser in der Anforderung kein Cookie zurückgibt. Wenn der Browser jedoch ein Cookie zurückgibt (nicht notwendigerweise das Persistenz-Cookie), wird davon ausgegangen, dass der Browser Cookies unterstützt und somit Backup-Persistenz nicht ausgelöst wird.
Regel	Quell-IP	Die Appliance verwendet Source-IP-basierte Persistenz, wenn der in der Regel angegebene Parameter in der eingehenden Anforderung fehlt.

Hinweis:

- Wenn der primäre Persistenztyp HTTP-Cookie-basierte Persistenz ist und der Backup-Persistenztyp Quell-IP-basiert ist, können Sie einen Timeout-Wert für die Backup-Persistenz festlegen. Anweisungen finden Sie unter Festlegen eines Timeout-Werts für Idle Clientverbindungen.
- Sie können keinen Timeout-Wert für die Backup-Persistenz festlegen, wenn die primäre Persistenz auf Regel basiert, da in diesem Fall der Timeout-Wert für die sekundäre Persistenz mit dem für die primäre Persistenz übereinstimmen muss. Daher laufen die primären und

> sekundären zur gleichen Zeit ab.

So legen Sie die Backup-Persistenz für einen virtuellen Server mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -persistenceType <PersistenceType> -
    persistenceBackup <BackupPersistenceType>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -persistenceType CookieInsert -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1  - persistenceType RULE  - rule http.req.
    header("User-Agent").value(0).contains("MyBrowser")  -
    persistenceBackup SOURCEIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP
<!--NeedCopy-->
```

So legen Sie die Backup-Persistenz für einen virtuellen Server mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen Persistenz**aus, und geben Sie einen Backup-Persistenztyp an.

Hinweis: Die primäre Persistenz muss auf COOKIEINSERT, RULE oder SSLSESSION festgelegt sein.

Persistenzgruppen konfigurieren

August 19, 2021

Wenn Sie über Server mit Lastenausgleich verfügen, die verschiedene Arten von Verbindungen verarbeiten (z. B. Webserver, die Multimedia hosten), können Sie eine virtuelle Servergruppe so konfigurieren, dass diese Verbindungen verarbeitet werden. Um eine virtuelle Servergruppe zu erstellen, binden Sie verschiedene Typen von virtuellen Servern, einen für jeden Verbindungstyp, den Ihre Server mit Lastausgleich akzeptieren, in eine einzelne Gruppe. Anschließend konfigurieren Sie einen Persistenztyp für die gesamte Gruppe.

Sie können entweder Quell-IP-basierte Persistenz oder HTTP-Cookie-basierte Persistenz für Persistenzgruppen konfigurieren. Nachdem Sie die Persistenz für die gesamte Gruppe festgelegt haben, können Sie sie nicht für einzelne virtuelle Server in der Gruppe ändern. Wenn Sie die Persistenz für eine Gruppe konfigurieren und der Gruppe dann einen neuen virtuellen Server hinzufügen, wird die Persistenz des neuen virtuellen Servers so geändert, dass sie mit der Persistenzeinstellung der Gruppe übereinstimmt.

Wenn die Persistenz auf einer Gruppe virtueller Server konfiguriert ist, werden Persistenzsitzungen für anfängliche Anforderungen erstellt, und nachfolgende Anforderungen werden an denselben Dienst wie die Erstanforderung weitergeleitet, unabhängig vom virtuellen Server in der Gruppe, der jede Clientanforderung empfängt.

Wenn Sie einen virtuellen Server mit Persistenzsitzungen zu einer Lastausgleichsgruppe mit einem anderen Persistenztyp hinzufügen, werden die vorhandenen persistenten Sitzungen, die für einen alten Persistenztyp spezifisch sind, gelöscht. Die persistenten Sitzungen entscheiden, ob der Datenverkehr auf denselben virtuellen Server oder auf einen anderen Server übertragen werden muss. Daher sind bestehende Verbindungen nicht betroffen.

Der Persistenztyp einer Lastausgleichsgruppe wird unabhängig vom Protokolltyp des virtuellen Servers auf alle an diese Gruppe gebundenen virtuellen Server angewendet. Eine Load Balancing-Gruppe unterstützt die folgenden Persistenztypen:

- sourceIP
- CookieInsert
- Regel

Einige virtuelle Server unterstützen nur bestimmte Persistenzarten. Beispielsweise kann ein virtueller Server vom Typ SSL_BRIDGE nur den sourceIP-Persistenztyp für eine LB-Gruppe verwenden.

Wenn Sie HTTP-Cookie-basierte Persistenz konfigurieren, wird das Domänenattribut des HTTP-Cookies gesetzt. Diese Einstellung bewirkt, dass die Clientsoftware das HTTP-Cookie in Clientanforderungen hinzufügt, wenn verschiedene virtuelle Server unterschiedliche öffentliche Hostnamen haben. Weitere Informationen zum Persistenztyp von CookieInsert finden Sie unter Persistenz basierend auf HTTP-Cookies.

So erstellen Sie eine Persistenzgruppe virtueller Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb group <vServerGroupName> <vServerName> -persistenceType <
   PersistenceType>
<!--NeedCopy-->
```

Beispiel:

```
bind lb group Vserver-Group-1 Vserver-LB-1 -persistenceType
   CookieInsert
<!--NeedCopy-->
```

So ändern Sie eine virtuelle Servergruppe mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Persistency Groups**, erstellen Sie eine Persistenzgruppe und geben Sie die virtuellen Server an, die Teil dieser Gruppe sein müssen.

So ändern Sie eine virtuelle Servergruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb group <vServerGroupName> -PersistenceBackup <
   BackupPersistenceType> -persistMask <SubnetMaskAddress>
<!--NeedCopy-->
```

Beispiel:

```
set lb group vserver-Group-1 -PersistenceBackup SourceIP -persistMask
   255.255.255.255
<!--NeedCopy-->
```

Freigabe persistenter Sitzungen zwischen virtuellen Servern

May 11, 2023

In einigen Kundenumgebungen (Telekommunikation und ISP) wickelt ein einziger Server sowohl die Steuerung als auch den Datenverkehr ab. Für eine bestimmte Client-IP-Adresse müssen sowohl

die Steuerung als auch der Datenverkehr an denselben Backend-Server geleitet werden. Dazu ist ein virtueller Server für die Verarbeitung des Client-Authentifizierungsverkehrs erforderlich, und in der Regel wird darauf eine regelbasierte Persistenz konfiguriert. Zum Beispiel radius.req.avp (8) .value.typecast_text_t'. Der zweite virtuelle Server für die Abwicklung des Datenverkehrs. Normalerweise ist SourceIP Persistenz darauf konfiguriert.

Zuvor waren Persistenzeinträge lokal für den virtuellen Server. Wenn Sie Persistenz auf mehrere virtuelle Server anwenden mussten, mussten Sie den virtuellen Server einer Load Balancing-Gruppe hinzufügen und dann einen gemeinsamen Persistenztyp auf die Gruppe anwenden. Diese Anforderung kann nicht erfüllt werden, da alle virtuellen Server, die an eine Lastausgleichsgruppe gebunden sind, die für die Gruppe konfigurierte Persistenz geerbt haben.

Mit der Funktion "Persistenzfreigabe zwischen virtuellen Servern" können Sie den neuen `useVserverPersistency` Parameter für eine Lastausgleichsgruppe festlegen, damit der virtuelle Server in der Gruppe seine eigenen Persistenzparameter verwenden kann, anstatt sie von den Gruppeneinstellungen zu erben. Sie können auf jedem virtuellen Server eine separate regelbasierte Persistenz konfigurieren.

Optional können Sie einen der virtuellen Server in der Gruppe auch als virtuellen Hauptserver festlegen. Wenn ein virtueller Server als virtueller Hauptserver bezeichnet wird, erstellt nur dieser virtuelle Server die Persistenzeinträge, die von allen virtuellen Servern in der Gruppe verwendet werden. Wenn der virtuelle Hauptserver ausgefallen ist, erstellt die NetScaler Appliance keine Persistenzeinträge.

Hinweis: Die Persistenzfreigabe auf den virtuellen Servern wird nur für regelbasierte Persistenzmethoden unterstützt. Konfigurieren Sie kompatible regelbasierte Persistenzparameter auf den virtuellen Servern des Mitglieds.

Beispiel:

Angenommen, v1 und v2 sind an eine Lastausgleichsgruppe gebunden, v1 ist ein virtueller Server vom Typ RADIUS und v2 ist ein virtueller Server vom Typ HTTP. 'Radius.req.avp (8) .value.typecast_text_t' Persistenz ist auf v1 konfiguriert und 'client.ip.src' ist auf v2 konfiguriert.

Wenn Datenverkehr durch den virtuellen RADIUS-Server v1 fließt, erstellt er einen dauerhaften Eintrag basierend auf der ausgewerteten Regelzeichenfolge. Später, wenn der Datenverkehr den virtuellen Server des HTTP-Typs v2 erreicht, sucht v2 nach den Persistenzeinträgen in der Load Balancing-Gruppe und leitet den Datenverkehr mit derselben Persistenzsitzung auf denselben Back-End-Server weiter.

Konfigurieren der Freigabe von persistenten Sitzungen

Um Persistenzparameter über den virtuellen Server in einer Load Balancing-Gruppe freizugeben, müssen Sie zuerst den UsevServerPersistency-Parameter aktivieren und dann einen der virtuellen Server in der Gruppe als Hauptserver festlegen.

So aktivieren Sie den Parameter UseVServerPersistency mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb group <name> -useVserverPersistency ( ENABLED)
<!--NeedCopy-->
```

Beispiel:

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

So aktivieren Sie den UseVServerPersistency-Parameter mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastausgleich** > **Persistenzgruppen** .
2. Klicken Sie auf **Hinzufügen**, um eine neue Gruppe hinzuzufügen, oder wählen Sie eine vorhandene Gruppe aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Vserver-Persistenz verwenden**aus.

So weisen Sie einen virtuellen Server mit der Befehlszeilenschnittstelle als virtuellen Hauptserver aus

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb group <name> -useVserverPersistency ( ENABLED ) -masterVserver <
    string>
<!--NeedCopy-->
```

Beispiel:

```
set lb group lb_grp1 -useVserverPersistency ENABLED  - masterVserver vs1
<!--NeedCopy-->
```

So weisen Sie einen virtuellen Server mit der GUI als virtuellen Hauptserver aus

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastausgleich** > **Persistenzgruppen** .
2. Klicken Sie auf **Hinzufügen**, um eine neue Gruppe hinzuzufügen, oder wählen Sie eine vorhandene Gruppe aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Vserver-Persistenz verwenden**aus.

4. Klicken Sie im Feld **Name des virtuellen Servers** auf **+**, um den virtuellen Server der Gruppe hinzuzufügen. Sie können den verfügbaren virtuellen Server auswählen oder einen virtuellen Server erstellen.
5. Klicken Sie auf **Erstellen**, wenn Sie eine neue Gruppe hinzufügen, oder auf **Schließen**, wenn Sie eine vorhandene Gruppe ändern.
6. Wählen Sie die Gruppe aus, für die Sie den UsevServerPersistency-Parameter aktiviert haben, und klicken Sie auf **Bearbeiten**, um einen virtuellen Server als Hauptserver zum Erstellen von Persistenzeinträgen festzulegen.
7. Wählen Sie aus der Liste **Master vServer** den virtuellen Server aus, der als virtueller Hauptserver bezeichnet werden muss.

Argumente

vServer-Persistenz verwenden

Erlauben Sie den virtuellen Servern in einer Gruppe, ihre eigenen Persistenzparameter zu verwenden, um persistente Sitzungen zu erstellen, anstatt die Persistenzeinstellungen von den Gruppeneinstellungen zu erben. Wenn dieser Parameter aktiviert ist, kann die Persistenz für die Load Balancing-Gruppe nicht festgelegt werden.

Wenn dieser Parameter deaktiviert ist, erben die virtuellen Server der Gruppe die Persistenzparameter aus den Gruppeneinstellungen.

Wenn dieser Parameter in der Load Balancing-Gruppe aktiviert ist, löscht die NetScaler-Appliance alle entsprechenden Persistenzeinträge der Gruppe und der virtuellen Mitgliedsserver.

Mögliche Werte: ENABLED, DISABLED

Standard: DEAKTIVIERT

Beispiel:

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

MasterVServer

Bestimmen Sie einen virtuellen Server als virtuellen Hauptserver in seiner Load Balancing-Gruppe. Nach der Bezeichnung kann nur der virtuelle Hauptserver die von der Gruppe verwendeten persistenten Einträge erstellen.

Hinweis: Dieser Parameter kann nur festgelegt werden, wenn der Parameter UseVServerPersistency aktiviert ist.

Beispiel:


```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Beispielkonfiguration für die gemeinsame Nutzung persistenter Sitzungen mithilfe der Befehlszeilenschnittstelle

Die virtuellen Server werden erstellt

```
add lb vs vs1 http 10.1.10.11 80 -persistence rule -rule 'client.ip.src'

add lb vs vs2 radius 10.2.2.2 1812 -persistenceType rule -rule 'Radius.req.avp(8).value.typecast_text_t'
<!--NeedCopy-->
```

Die Gruppen werden erstellt.

```
add lb group lb_grp1 -persistenceType NONE -useVserverPersistency ENABLED
<!--NeedCopy-->
```

Ein virtueller Server in einer Gruppe wird als virtueller Hauptserver bezeichnet.

```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Die virtuellen Server sind an die Gruppe gebunden.

```
bind lb group lb_grp1 vs1
bind lb group lb_grp1 vs2
<!--NeedCopy-->
```

Weitere Informationen finden Sie unter Einrichten des Basis-Lastenausgleichs und Konfigurieren von Persistenzgruppen.

RADIUS-Lastausgleichs mit Persistenz konfigurieren

May 11, 2023

Die heutige komplexe Netzwerkumgebung erfordert häufig die Koordination einer Lastausgleichskonfiguration mit hoher Kapazität mit robuster Authentifizierung und Autorisierung. Anwendungsbenutzer können sich über mobile Zugangspunkte wie DSL- oder Kabelverbindungen für

Verbraucher, WiFi oder sogar DFÜ-Knoten mit einem VPN verbinden. Diese Verbindungen verwenden normalerweise dynamische IPs, die sich während der Verbindung ändern können.

Wenn Sie den RADIUS-Lastenausgleich auf der NetScaler-Appliance so konfigurieren, dass persistente Clientverbindungen zu RADIUS-Authentifizierungsservern unterstützt werden, verwendet die Appliance die Benutzeranmeldung oder das angegebene RADIUS-Attribut anstelle der Client-IP als Sitzungs-ID und leitet alle mit dieser Benutzersitzung verknüpften Verbindungen und Datensätze an denselben RADIUS-Server weiter. Benutzer können sich daher von mobilen Zugangsstandorten aus bei Ihrem VPN anmelden, ohne dass Verbindungsabbrüche auftreten, wenn sich die Client-IP oder der WiFi-Zugangspunkt ändert.

Um den RADIUS-Lastausgleich mit Persistenz zu konfigurieren, müssen Sie zuerst die RADIUS-Authentifizierung für Ihr VPN konfigurieren. Informationen und Anweisungen finden Sie im Kapitel Authentifizierung, Autorisierung, Auditing (AAA) in AAA Application Traffic. Wählen Sie auch entweder die Funktion Load Balancing oder Content Switching als Grundlage für Ihre Konfiguration und stellen Sie sicher, dass die von Ihnen gewählte Funktion aktiviert ist. Der Konfigurationsprozess mit beiden Funktionen ist fast identisch.

Anschließend konfigurieren Sie entweder zwei virtuelle Load-Balancing-Server oder zwei Content-Switching-Server, von denen einer für den RADIUS-Authentifizierungsverkehr und der andere für den RADIUS-Abrechnungsverkehr zuständig ist. Als Nächstes konfigurieren Sie zwei Dienste, einen für jeden virtuellen Lastausgleichsserver, und binden jeden virtuellen Lastausgleichsserver an seinen Dienst. Schließlich erstellen Sie eine Load-Balancing-Persistenzgruppe und legen den Persistenztyp auf RULE fest.

Aktivierung der Load Balancing- oder Content Switching-Funktion

Um die Load Balancing- oder Content Switching-Funktion verwenden zu können, müssen Sie zunächst sicherstellen, dass die Funktion aktiviert ist. Wenn Sie eine neue NetScaler Appliance konfigurieren, die noch nicht konfiguriert wurde, sind beide Funktionen bereits aktiviert, sodass Sie zum nächsten Abschnitt springen können. Wenn Sie eine NetScaler Appliance mit einer vorherigen Konfiguration konfigurieren und Sie nicht sicher sind, ob die von Ihnen verwendete Funktion aktiviert ist, müssen Sie dies jetzt tun.

- Anweisungen zum Aktivieren der Lastenausgleichsfunktion finden Sie unter Load Balancing aktivieren.
- Anweisungen zum Aktivieren der Content Switching-Funktion finden Sie unter Aktivieren des Inhaltswechsels

Konfigurieren virtueller Server

Nachdem Sie die Load-Balancing- oder Content-Switching-Funktion aktiviert haben, müssen Sie als Nächstes zwei virtuelle Server konfigurieren, um die RADIUS-Authentifizierung zu unterstützen:

- **Virtueller RADIUS-Authentifizierungsserver.** Dieser virtuelle Server und der zugehörige Dienst verarbeiten den Authentifizierungsdatenverkehr zu Ihrem RADIUS-Server. Der Authentifizierungsdatenverkehr besteht aus Verbindungen, die mit Benutzern verbunden sind, die sich bei Ihrer geschützten Anwendung oder VPN (Virtual Private Network) anmelden.
- **RADIUS Accounting Virtual Server.** Dieser virtuelle Server und der zugehörige Service verarbeiten Buchhaltungsverbindungen zu Ihrem RADIUS-Server. Accounting Traffic besteht aus Verbindungen, die die Aktivitäten eines authentifizierten Benutzers in Ihrer geschützten Anwendung oder VPN verfolgen.

Wichtig: Sie müssen entweder ein Paar virtueller Load-Balancing-Server oder ein Paar von virtuellen Content Switching-Servern erstellen, die Sie in Ihrer RADIUS-Persistenzkonfiguration verwenden können. Sie können virtuelle Servertypen nicht mischen.

So konfigurieren Sie einen virtuellen Lastausgleichsserver mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Lastausgleichsserver zu erstellen und die Konfiguration zu überprüfen:

```
1 add lb vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
     <rule>
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Um einen vorhandenen virtuellen Lastenausgleichsserver zu konfigurieren, ersetzen Sie den vorhergehenden `add lb virtual server` Befehl durch den `set lb vserver` Befehl, der dieselben Argumente annimmt.

So konfigurieren Sie einen virtuellen Content Switching-Server über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Content Switching Server zu erstellen und die Konfiguration zu überprüfen:

```
1 add cs vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
     <rule>
2
3 show cs vserver <name>
4 <!--NeedCopy-->
```

Um einen vorhandenen virtuellen Content Switching-Server zu konfigurieren, ersetzen Sie den vorherigen `add cs vserver` Befehl durch den `set cs vserver` Befehl, der dieselben Argumente annimmt.

Beispiel:

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Load-Balancing- oder Content-Switching-Server mithilfe des Konfigurationsprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** oder navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server>**und konfigurieren Sie einen virtuellen Server.

Dienste konfigurieren

Nachdem Sie Ihre virtuellen Server konfiguriert haben, müssen Sie als Nächstes zwei Dienste konfigurieren, einen für jeden der von Ihnen erstellten virtuellen Server.

Hinweis: Nach der Konfiguration befinden sich diese Dienste im Status DEAKTIVIERT, bis die NetScaler Appliance eine Verbindung mit den Authentifizierungs- und Accounting-IPs Ihres RADIUS-Servers herstellen und deren Status überwachen kann. Anweisungen finden Sie unter Dienste konfigurieren.

Binden virtueller Server an Dienste

Nach der Konfiguration Ihrer Dienste müssen Sie als Nächstes jeden der von Ihnen erstellten virtuellen Server an den entsprechenden Dienst binden.Anweisungen finden Sie unter Binding Services an den virtuellen Server.

Konfigurieren einer Persistenzgruppe für Radius

Nachdem Sie Ihre virtuellen Load-Balancing-Server an die entsprechenden Dienste gebunden haben, müssen Sie Ihre RADIUS-Load-Balancing-Konfiguration einrichten, um die Persistenz zu unterstützen. Dazu konfigurieren Sie eine Load Balancing-Persistenzgruppe, die Ihre virtuellen

RADIUS-Loadbalancing-Server und -Dienste enthält, und konfigurieren diese Load Balancing-Persistenzgruppe so, dass sie regelbasierte Persistenz verwendet. Eine Persistenzgruppe ist erforderlich, da die virtuellen Authentifizierungs- und Buchhaltungsserver unterschiedlich sind und sowohl die Authentifizierungs- als auch die Buchhaltungsnachricht für einen einzelnen Benutzer denselben RADIUS-Server erreichen sollten. Persistenzgruppe ermöglicht es, dieselbe Sitzung für beide virtuellen Server zu verwenden. Anweisungen finden Sie unter Konfigurieren von Persistenzgruppen.

Konfigurieren von RADIUS Shared Secret

Ab Version 12.0 unterstützt eine NetScaler-Appliance RADIUS Shared Secret. Ein RADIUS-Client und ein Server kommunizieren miteinander über einen gemeinsamen Schlüssel, der auf dem Client und auf dem Server konfiguriert ist. Transaktionen zwischen einem RADIUS-Client und Server werden mithilfe eines Shared Secret authentifiziert. Dieses Geheimnis wird auch verwendet, um einige der Informationen im RADIUS-Paket zu verschlüsseln.

Szenarien zur Überprüfung gemeinsam genutzter geheimer Schlüssel in RADIUS

Die Validierung des **freigegebenen geheimen RADIUS-Schlüssels** erfolgt in den folgenden Szenarien:

- Der**gemeinsame geheime RADIUS-Schlüssel ist sowohl für den Radius-Client als auch für den RADIUS-Server konfiguriert:** Die NetScaler-Appliance verwendet den geheimen RADIUS-Schlüssel sowohl für die Clientseite als auch für die Serverseite. Wenn die Überprüfung erfolgreich ist, lässt die Appliance die RADIUS-Nachricht durchgehen. Andernfalls wird die RADIUS-Nachricht gelöscht.
- Der**gemeinsame geheime RADIUS-Schlüssel ist weder für den Radius-Client noch für den RADIUS-Server konfiguriert: Die** NetScaler-Appliance verwirft die RADIUS-Nachricht, da die Validierung des gemeinsam genutzten geheimen Schlüssels auf einem Knoten, für den kein Radkey konfiguriert ist, nicht durchgeführt werden kann.
- Der**gemeinsame geheime RADIUS-Schlüssel ist nicht sowohl für den RADIUS-Client als auch für den RADIUS-Server konfiguriert:** Die NetScaler-Appliance umgeht die Überprüfung des geheimen RADIUS-Schlüssels und lässt die RADIUS-Nachrichten passieren.

Sie können einen standardmäßigen gemeinsamen Schlüssel für RADIUS oder pro Client oder Subnetz konfigurieren. Es wird empfohlen, einen gemeinsamen geheimen RADIUS-Schlüssel für alle Bereitstellungen hinzuzufügen, für die die RADIUS-Richtlinie konfiguriert ist. Die Appliance verwendet die Quell-IP-Adresse des RADIUS-Pakets, um zu entscheiden, welcher gemeinsame Schlüssel verwendet werden soll. Sie können einen RADIUS-Client und Server und den entsprechenden Shared Secret wie folgt konfigurieren:

Geben Sie an der CLI-Eingabeaufforderung Folgendes ein:


```
add radiusNode <clientPrefix/Subnet> -radKey <Shared_secret_key>
<!--NeedCopy-->
```

Argumente

IP-Adresse

IP-Adresse oder Subnetz des RADIUS-Clients im CIDR-Format. Die Appliance verwendet die Quell-IP-Adresse eines eingehenden Anforderungspakets, um der Client-IP-Adresse zu entsprechen. Anstatt eine Client-IP-Adresse zu konfigurieren, können Sie die Client-Netzwerkadresse konfigurieren. Das längste Präfix wird abgeglichen, um den gemeinsamen Schlüssel für eine eingehende Clientanfrage zu identifizieren.

Radkey

Gemeinsamer geheimer Schlüssel zwischen dem Client, der NetScaler-Appliance und dem Server. Maximale Länge: 31

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add service radius_auth_service1 192.168.41.68 RADIUS 1812

add service radius_acct_service1 192.168.41.70 RADIUS 1813

bind lb vserver radius_auth_vs1 radius_auth_service1

bind lb vserver radius_acct_vs1 radius_acct_service[1-3]

add radiusNode 192.168.41.0/24 -radKey  serverkey123

add radiusNode 203.0.113.0/24 -radkey clientkey123
<!--NeedCopy-->
```

Ein gemeinsam genutzter geheimer Schlüssel muss sowohl für einen RADIUS-Client als auch für einen RADIUS-Server konfiguriert werden. Der Befehl ist derselbe. Das Subnetz bestimmt, ob der gemeinsame geheime Schlüssel für einen Client oder für einen Server bestimmt ist.

Wenn das angegebene Subnetz beispielsweise ein Client-Subnetz ist, gilt der gemeinsame Schlüssel für den Client. Wenn das angegebene Subnetz ein Serversubnetz ist (192.168.41.0/24 im vorherigen

Beispiel), ist das Shared Secret für den Server.

Ein Subnetz von 0.0.0.0/0 bedeutet, dass es der Standardgeheimnis für alle Clients und Server ist.

> **Hinweis:**
>
> Nur die PAP- und CHAP-Authentifizierungsmethoden werden mit RADIUS Shared Secret unterstützt.

Persistenzsitzungen anzeigen

May 11, 2023

Sie können die verschiedenen Persistenzsitzungen einsehen, die global oder für einen bestimmten virtuellen Server gültig sind.

> **Hinweis**: Eine NetScaler NCore-Appliance verwendet mehrere CPU-Kerne für die Paketbehandlung. Der CPU-Kern besitzt jede Sitzung auf der Appliance. Wenn die Appliance eine Anforderung erhält, für die keine Sitzung existiert, wird eine Sitzung erstellt, und einer der Kerne wird als Eigentümer dieser Sitzung bezeichnet.
>
> Nachfolgende Anforderungen, die zu dieser Sitzung gehören, kommen möglicherweise nicht immer an und werden vom Eigentümerkern behandelt. In diesem Fall stellt Inter-Core Messaging sicher, dass die Sitzungsinformationen auf dem Owner-Core immer aktuell sind.

Wenn jedoch ein Kern eine Anforderung empfängt, die zu einer Persistenzsitzung gehört, die einem anderen Kern gehört, aktualisiert das Inter-Core-Messaging den Timeout-Wert für die Persistenzsitzung nicht.

In der Ausgabe von sukzessive run show lb persistentSessions -Befehlen, die nur Timeout-Werte von Besitzerkernen anzeigen, kann der Timeout-Wert für eine Persistenzsitzung auf 0 (Null) abnehmen, selbst wenn die Persistenzsitzung aktiv bleibt.

So zeigen Sie Persistenzsitzungen mit der Befehlszeilenschnittstelle an

Um Persistenzsitzungen für alle virtuellen Server anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lb persistentSessions [<vServer>]
<!--NeedCopy-->
```

Geben Sie an der Eingabeaufforderung Folgendes ein, um Persistenzsitzungen für einen virtuellen Server anzuzeigen:


```
show lb persistentSessions <vServername>
<!--NeedCopy-->
```

Beispiel:

```
show lb persistentSessions myVserver
<!--NeedCopy-->
```

So zeigen Sie Persistenzsitzungen mit der GUI an

Navigieren Sie zu **Traffic Management** > **Persistente Sitzungen für virtuelle Server**.

Persistenzsitzungen löschen

May 11, 2023

Möglicherweise müssen Sie Persistenzsitzungen von der NetScaler-Appliance löschen, wenn das Timeout für Sitzungen nicht erreicht wird. Sie haben folgende Optionen:

- Löschen Sie alle Sitzungen für alle virtuellen Server gleichzeitig.
- Löscht alle Sitzungen für einen bestimmten virtuellen Server auf einmal.
- Löscht eine bestimmte Sitzung, die einem bestimmten virtuellen Server zugeordnet ist.

So löschen Sie eine Persistenzsitzung mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um Persistenzsitzungen zu löschen und die Konfiguration zu überprüfen:

```
clear lb persistentSessions [<vServer> [-persistenceParam <string>]]

show persistentSessions <vServer>
<!--NeedCopy-->
```

Beispiele:

Beispiel 1 löscht alle Persistenzsitzungen für den Lastenausgleich des virtuellen Servers lbvip1.

Beispiel 2 zeigt zuerst die Persistenzsitzungen für den Lastenausgleich des virtuellen Servers lbvip1 an, löscht die Sitzung mit dem Persistenzparameter xls und zeigt dann die Persistenzsitzungen an, um zu überprüfen, ob die Sitzung gelöscht wurde.

Beispiel 1:


```
> clear persistentSessions lbvip1
 Done
> show persistentSessions
 Done
>
<!--NeedCopy-->
```

Beispiel 2:

```
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    xls
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
> clear persistentSessions lbvip1 -persistenceParam xls
 Done
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
>
<!--NeedCopy-->
```

So löschen Sie Persistenzsitzungen mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Persistente Sitzungen löschen**.

Persistenzeinstellungen für überlastete Dienste überschreiben

May 11, 2023

Wenn ein Dienst ausgelastet ist oder anderweitig nicht verfügbar ist, wird der Dienst für Clients herabgesetzt. In diesem Fall müssen Sie möglicherweise die NetScaler Appliance so konfigurieren, dass die Anforderungen, die sonst in die Persistenzsitzung aufgenommen würden, die mit dem überladenen Dienst verknüpft ist, vorübergehend an andere Dienste weiterleitet. Mit anderen Worten, Sie müssen möglicherweise die Persistenzeinstellung überschreiben, die für den virtuellen Lastausgleichsserver konfiguriert ist. Sie können diese Funktionalität erreichen, indem Sie den Parameter Skippersistency festlegen. Wenn dieser Skippersistence-Parameter festgelegt ist und der virtuelle Server neue Verbindungen für einen überlasteten Dienst erhält, passiert Folgendes.

- Der virtuelle Server ignoriert alle vorhandenen Persistenzsitzungen, die mit diesem Dienst verknüpft sind, bis der Dienst in einen Status zurückkehrt, in dem er Anfragen annehmen kann.
- Persistenzsitzungen, die mit anderen Diensten verknüpft sind, sind nicht betroffen.

Diese Funktion ist nur für virtuelle Server verfügbar, deren Typ ANY oder UDP ist.

In Branch Repeater Lastausgleich-Konfigurationen müssen Sie auch einen Lastmonitor konfigurieren und ihn an den Dienst binden. Der Monitor nimmt den Dienst aus nachfolgenden Lastausgleichsentscheidungen heraus, bis die Last auf dem Dienst unter den konfigurierten Schwellenwert gebracht wird. Informationen zum Konfigurieren eines Lastmonitors für Ihren virtuellen Server finden Sie unter Grundlegendes zu Lastmonitoren.

Sie können den virtuellen Server so konfigurieren, dass er eine der folgenden Aktionen mit den Anforderungen durchführt, die andernfalls Teil der Persistenzsitzung wären:

- **Senden Sie jede Anfrage an einen der anderen Dienste.** Der virtuelle Server trifft eine Lastenausgleichsentscheidung und sendet jede Anforderung basierend auf der Load Balancing-Methode an einen der anderen Dienste. Wenn alle Dienste überlastet sind, werden Anforderungen gelöscht, bis ein Dienst verfügbar ist.

  Sowohl Wildcard- als auch IP-Adressserver unterstützen diese Option. Diese Aktion ist für alle Bereitstellungen geeignet, auch für Bereitstellungen, bei denen der virtuelle Server den Lastenausgleich von Branch Repeater-Appliances oder Firewalls durchführt.

- **Umgehen Sie die Konfiguration des virtuellen Serverdienstes.** Der virtuelle Server trifft keine Lastausgleichsentscheidung. Stattdessen überbrückt es einfach jede Anforderung an einen physischen Server basierend auf der Ziel-IP-Adresse in der Anforderung.

  Nur virtuelle Wildcard-Server vom Typ ANY und UDP unterstützen die Umgehungsoption. Virtuelle Wildcard-Server haben eine Kombination *aus* IP und Port. Diese Aktion eignet sich für Bereitstellungen, in denen Sie den virtuellen Server zum Lastenausgleich von Branch Repeater-Appliances oder Firewalls verwenden. In diesen Bereitstellungen leitet die NetScaler Appliance zunächst eine Anforderung an eine Branch Repeater-Appliance oder eine Firewall weiter und leitet die verarbeitete Antwort dann an einen physischen Server weiter. Der virtuelle Server sendet Anfragen unter den folgenden Bedingungen direkt an seine Ziel-IP-Adressen.

  - Sie konfigurieren den virtuellen Server so, dass er die Konfiguration des virtuellen Server-Servers für überladene Dienste Bypass.
  - Die Branch Repeater Appliance oder Firewall wird überlastet.

  Der virtuelle Server sendet Anfragen direkt an seine Ziel-IP-Adressen, bis die Branch Repeater Appliance oder Firewall Anfragen annehmen kann.

So überschreiben Sie Persistenzeinstellungen für überlastete Dienste über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um Persistenzeinstellungen für überladene Dienste außer Kraft zu setzen und die Konfiguration zu überprüfen:

```
set lb vserver <name> -skippersistency <skippersistency>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel

```
> set lb vserver mylbvserver -skippersistency ReLb
 Done
> show lb vserver mylbvserver
    mylbvserver (\*:\*) - ANY Type: ADDRESS
       . . .
       . . .
 Skip Persistency: ReLb
       . . .
 Done
>
<!--NeedCopy-->
```

So überschreiben Sie Persistenzeinstellungen für überlastete Dienste über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und wählen Sie den virtuellen Server vom Typ UDP oder ANY aus.
2. Wählen Sie im Bereich Erweiterte Einstellungen die Option Verkehrseinstellungen aus, und geben Sie den Typ der Persistenz überspringen an.

Problembehandlung

May 11, 2023

- **Die Statistiken der NetScaler VPX-Appliance zeigen, dass die Appliance das Sitzungspersistenzlimit erreicht hat. Daher schlagen Persistenzsitzungen fehl. Ist es möglich, das Persistenzlimit für Sitzungen zu erhöhen?**

Ursache: Die NetScaler-Appliance hat das Systemlimit von 250.000 Persistenzsitzungen für einen Kern.

Lösung: Um dieses Problem zu beheben, können Sie eine der folgenden Aufgaben ausführen:

- Reduzieren Sie den Timeout-Wert für Persistenz
- Erhöhen Sie die Anzahl der Kerne für die Appliance

- **Nach der Konfiguration der Cookie Insert Persistenz auf der NetScaler-Appliance berichten die Benutzer, dass die Verbindungen einige Zeit einwandfrei funktionieren, dann aber unterbrochen werden. Welche bewährte Methode sollte ich bei der Konfiguration der Persistenz befolgen?**

  Ursache: Standardmäßig beträgt der Timeout-Wert für die Persistenz von Cookie Insert 120 Sekunden.

  Lösung: Wenn Sie die Persistenz für Anwendungen konfigurieren, für die die Leerlaufzeit nicht bestimmt werden kann, setzen Sie den Wert für das Persistenz-Timeout von Cookie Insert auf 0. Mit dieser Einstellung tritt bei der Verbindung kein Timeout auf.

- **Nachdem ich einen virtuellen HTTP-Server auf der NetScaler-Appliance konfiguriert habe, muss ich sicherstellen, dass ein Benutzer für den angeforderten Inhalt immer eine Verbindung zu demselben Server herstellt. Deshalb habe ich die SourceIP-Persistenz konfiguriert. Wenn Sie nun den Timeout-Wert für Persistenz erhöhen, wird Latenz eingeführt. Wie kann ich den Timeout-Wert erhöhen, ohne die Leistung zu beeinträchtigen?**

  Lösung: Erwägen Sie, die Cookie Insert Persistenz zu verwenden, wobei der Timeout-Wert auf 0 gesetzt ist. Diese Einstellung ermöglicht langfristige Persistenzeinstellungen, da die Appliance keine Zeit für das Ablaufen des Cookie angibt.

- **Nach der Konfiguration der Cookie Insert Persistenz auf der NetScaler-Appliance funktioniert sie erwartungsgemäß, wenn Clients aus derselben Zeitzone auf den Inhalt zugreifen. Wenn jedoch ein Client aus einer anderen Zeitzone versucht, eine Verbindung herzustellen, wird die Verbindung sofort unterbrochen.**

  Ursache: Die zeitbasierte Persistenz beim Einfügen von Cookies funktioniert erwartungsgemäß, wenn ein Client aus derselben Zeitzone eine Verbindung herstellt. Wenn sich der Clientcomputer und die NetScaler Appliance jedoch in verschiedenen Zeitzonen befinden, ist das Cookie ungültig. Wenn beispielsweise ein Client in der EST-Zeitzone um 11:00 Uhr EST ein Cookie an eine NetScaler Appliance in der PST-Zeitzone sendet, erhält die Appliance das Cookie um 14:00 Uhr PST. Aufgrund des Zeitunterschieds ist das Cookie nicht gültig und die Verbindung ist sofort Timeout.

  Lösung: Setzen Sie den Timeout-Wert für die Cookie Insert Persistenz auf 0.

- **Eine NetScaler-Appliance wird für den Lastenausgleich von Anwendungsservern verwendet, z. B. Oracle Weblogic Server. Um sicherzustellen, dass Clients persistente**

Verbindungen zu diesen Servern erhalten, ist die SourceIP-Persistenz konfiguriert. Es funktioniert wie erwartet, wenn eine Verbindung von einem Computer aus hergestellt wird. Wenn Thin Clients jedoch versuchen, eine Verbindung über einen Terminalserver herzustellen, empfängt die Appliance daraufhin Anfragen von mehreren Clients von derselben IP-Adresse (der IP-Adresse des Terminalservers). Daher werden die Verbindungen von allen Thin Clients an denselben Anwendungsserver geleitet. Ist es möglich, die Persistenz für Anfragen von einzelnen Thin Clients basierend auf der Client-IP-Adresse zu konfigurieren?

Ursache: Die NetScaler-Appliance empfängt Anfragen vom Terminalserver und die Quell-IP-Adresse der Anfrage bleibt unverändert. Daher kann die Appliance nicht zwischen den von den Thin Clients empfangenen Anfragen unterscheiden und die Persistenz entsprechend den Anfragen von Thin Clients bereitstellen.

Lösung: Um dieses Problem zu vermeiden, können Sie die Regelpersistenz auf der Grundlage eines eindeutigen Parameterwerts für jeden Thin Client konfigurieren.

- **Die NetScaler-Appliance wird für den Lastenausgleich von Webinterface-Servern verwendet. Beim Zugriff auf die Server erhält der Benutzer die Fehlermeldung „State Error“. Wenn einer der Webinterface-Server heruntergefahren wird oder nicht verfügbar ist, erhalten einige Benutzer außerdem eine Fehlermeldung.**

  Ursache: Mangelnde Persistenz auf den Webinterface-Servern kann zu Fehlermeldungen führen, wenn ein Benutzer versucht, eine Verbindung zum Server herzustellen.

  Lösung: Citrix empfiehlt, dass Sie die Cookie-Insert-Persistenzmethode auf der NetScaler Appliance beim Lastenausgleich von Webinterface-Servern angeben.

Cookie-Attribute in ADC-generierten Cookies einfügen

May 11, 2023

Die Webadministratoren können andere Cookie-Attribute in die von der NetScaler Appliance generierten Cookies einfügen. Diese zusätzlichen Cookie-Attribute helfen bei der Durchsetzung der erforderlichen Richtlinien für die von ADC generierten Cookies basierend auf dem Anwendungszugriffsmuster.

Die folgenden Funktionen verwenden die von ADC generierten Cookies, um Persistenz zu erreichen.

- Persistenz von Load-Balancing-Cookies
- Persistenz von Cookies für Lastausgleichsgruppen
- Persistenz der GSLB-Site
- Cookie-Persistenz beim Content Switching

Sie können mit den folgenden Parametern andere Cookie-Attribute in die von ADC generierten Cookies einfügen:

- **literalAdcCookieAttribute:** Hängen Sie andere Cookie-Attribute als String an das von ADC generierte Cookie an.
- **ComputedADCCookieAttribute:** Verwenden Sie eine ADC ns-Variable, um Cookie-Attribute an das von ADC generierte Cookie anzuhängen, basierend auf den Client- oder Serverattributen, z. B.

> **Hinweis**
>
> Sie können nicht sowohl das Literal ADC Cookie-Attribut als auch das berechnete ADC-Cookie-Attribut gleichzeitig für den Load-Balancing-Parameter oder in einem einzigen Load-Balancing-Profil konfigurieren.

Anwendungsfall: SameSite-Cookie-Attribut konfigurieren

Jedem Cookie ist eine Domain zugeordnet. Wenn die Domain eines Cookies mit der Website-Domain in der Adressleiste des Benutzers übereinstimmt, wird dies als Kontext derselben Website (oder eines Erstanbieters) betrachtet. Wenn die mit einem Cookie verknüpfte Domain mit einem externen Dienst übereinstimmt und nicht mit der Website in der Adressleiste des Benutzers, wird dies als seitenübergreifender (oder Drittanbieter-) Kontext betrachtet.

Das **SameSite-Attribut** gibt dem Browser an, ob das Cookie für den standortübergreifenden Kontext oder nur für den Kontext derselben Website verwendet werden kann. Wenn eine Anwendung beabsichtigt, im standortübergreifenden Kontext zugegriffen zu werden, kann sie dies nur über die HTTPS-Verbindung tun. Einzelheiten finden Sie unter RFC6265.

Bis Februar 2020 wurde die **SameSite-Eigenschaft** nicht explizit in NetScaler festgelegt. Der Browser verwendete den Standardwert „Keine“ und hatte keine Auswirkungen auf die NetScaler-Bereitstellungen.

Mit dem Upgrade bestimmter Browser wie Google Chrome 80 ändert sich jedoch das standardmäßige domänenübergreifende Verhalten von Cookies. Das **SameSite-Attribut** kann auf einen der folgenden Werte festgelegt werden. Der Standardwert für Google Chrome ist auf Lax festgelegt.

- **Keine:** Zeigt an, dass der Browser ein Cookie im seitenübergreifenden Kontext nur für sichere Verbindungen verwendet.
- **Lax:** Zeigt an, dass der Browser ein Cookie für Anfragen im Kontext derselben Website verwendet. Im Cross-Site-Kontext können nur sichere HTTP-Methoden wie GET-Request das Cookie verwenden.
- **Streng:** Verwenden Sie das Cookie nur im Kontext derselben Site.

Wenn das Cookie kein SameSite-Attribut enthält, übernimmt Google Chrome die Funktionalität von SameSite = Lax.

> **Hinweis**
>
> Für bestimmte Versionen anderer Browser ist der Standardwert für das SameSite-Attribut möglicherweise auf **Keine**festgelegt. In einigen Browser-Versionen kann “SameSite = none” anders behandelt werden. Die folgenden Browser lehnen beispielsweise ein Cookie mit „SameSite = none“ ab:
>
> - Versionen von Chrome von Chrome 51 bis Chrome 66 (an beiden Enden inklusive)
> - Versionen des UC-Browsers auf Android vor Version 12.13.2

Konfigurieren von ADC-generierten Cookies

Um von ADC generierte Cookie-Attribute zu konfigurieren, müssen Sie Folgendes ausführen:

1. Erstellen eines virtuellen Lastausgleichsservers
2. Legen Sie die ADC-Cookie-Attribute für den virtuellen Load-Balancing-Server entweder über LB-Parameter oder über das LB-Profil fest.
3. Wenn Sie ein LB-Profil verwenden, legen Sie das LB-Profil auf einen virtuellen Lastausgleichsserver fest.
4. Wenn Sie sich dafür entscheiden, das berechnete ADC-Cookie-Attribut zu verwenden, konfigurieren Sie die entsprechende Rewrite-Richtlinie.

> **Hinweis**
>
> Wenn ein LB-Profil an einen virtuellen LB-Server gebunden ist, wird die Profilparameterkonfiguration anstelle der globalen LB-Parameterkonfiguration berücksichtigt.

Sie können die vom ADC generierten Cookie-Attribute auf folgende Weise festlegen:

- Festlegen der ADC-Cookie-Attribute in Lastenausgleichsparametern
- Festlegen der ADC-Cookie-Attribute im Load Balancing-Profil

Festlegen der ADC-Cookie-Attribute in den Lastenausgleichsparametern über die Befehlszeilenschnittstelle

Um eine Richtlinie einheitlich auf von ADC generierte Cookies aller auf der NetScaler Appliance konfigurierten Anwendungen anzuwenden, können Sie das ADC-Cookie-Attribut in den globalen LB-Parametern festlegen.

Die Einstellung **Literal ADC Cookie Attribut** ermöglicht es Ihnen, die Cookie-Attribute bedingungslos in das von ADC generierte Cookie einzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set lb parameter -LiteralADCCookieAttribute <string>
2 <!--NeedCopy-->
```


Beispiel:

```
set lb parameter -LiteralADCCookieAttribute SameSite=None
<!--NeedCopy-->
```

Mit der Einstellung **„Berechnetes ADC-Cookie-Attribut“** können Sie die Cookie-Attribute basierend auf den Client- oder Serverattributen unter bestimmten Bedingungen in das von ADC generierte Cookie einfügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb parameter -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

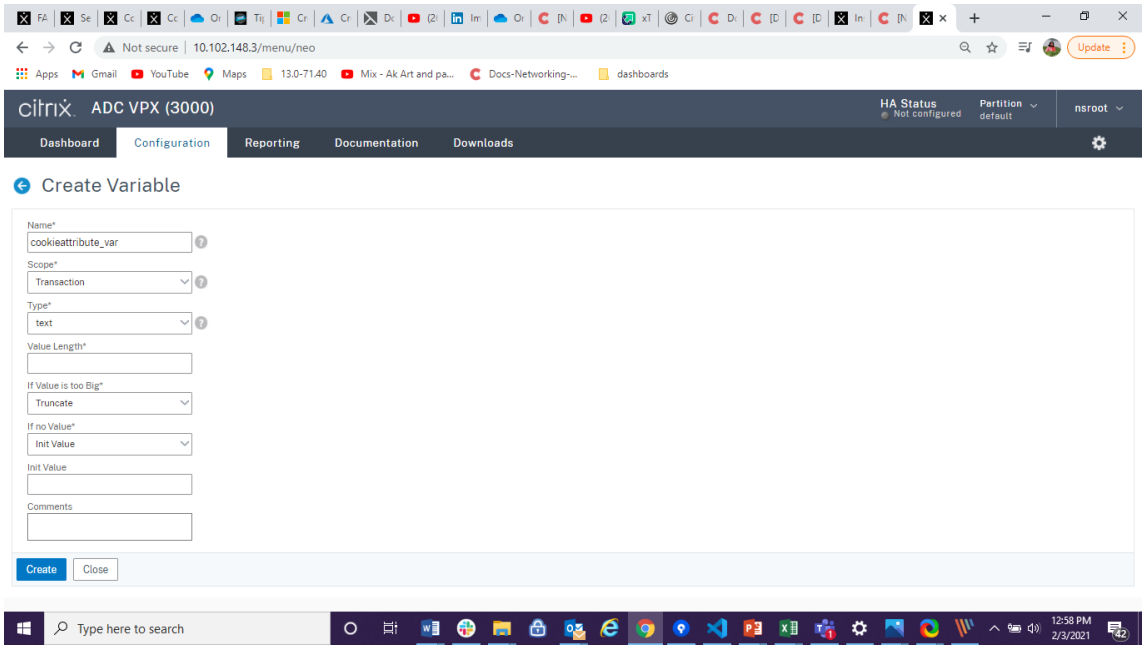
Beispiel:

```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
add rewrite policy append_samesite_attribute true samesiteassign

bind rewrite global exception_samesite_attribute 90 110 -type
    RES_OVERRIDE
bind rewrite global append_samesite_attribute 100 110 -type
    RES_OVERRIDE
<!--NeedCopy-->
```

Variablen mithilfe der GUI konfigurieren

1. Navigieren Sie zu **AppExpert > Variablen**und klicken Sie auf **Hinzufügen**.

2. Wählen **Sie auf der Seite “Variable erstellen** “ im Dropdownmenü **Geltungsbereich** als **Transaktion** und als **Texteingeben** aus.

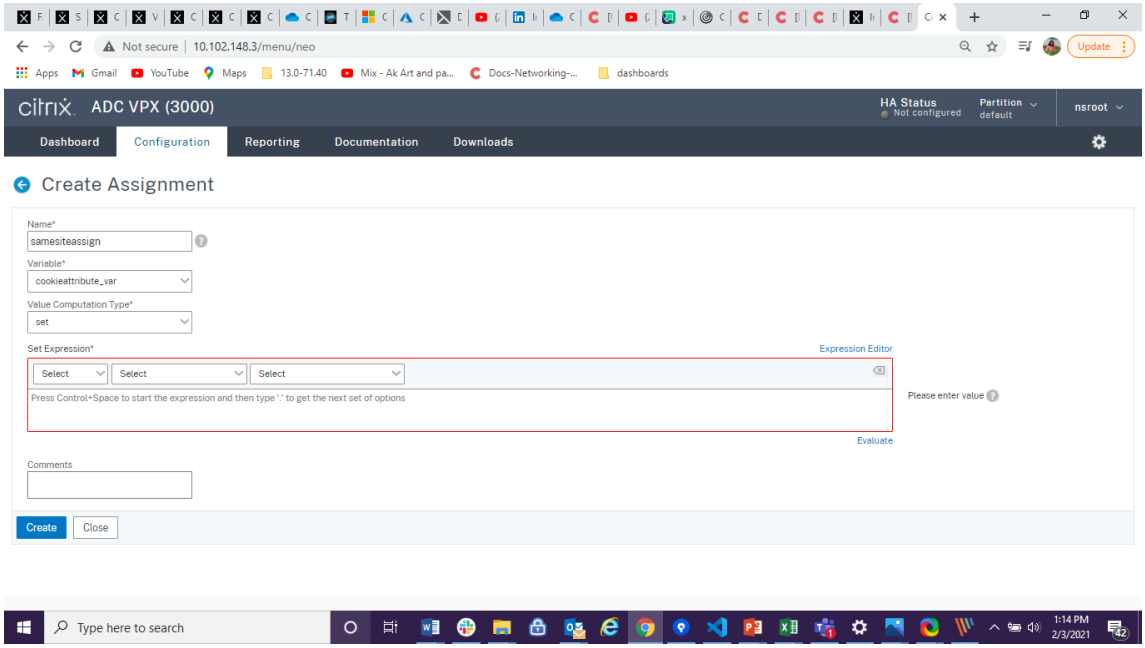


3. Geben Sie weitere Details ein und klicken Sie auf **Erstellen**.

Erstellen Sie eine Aufgabe mithilfe der GUI

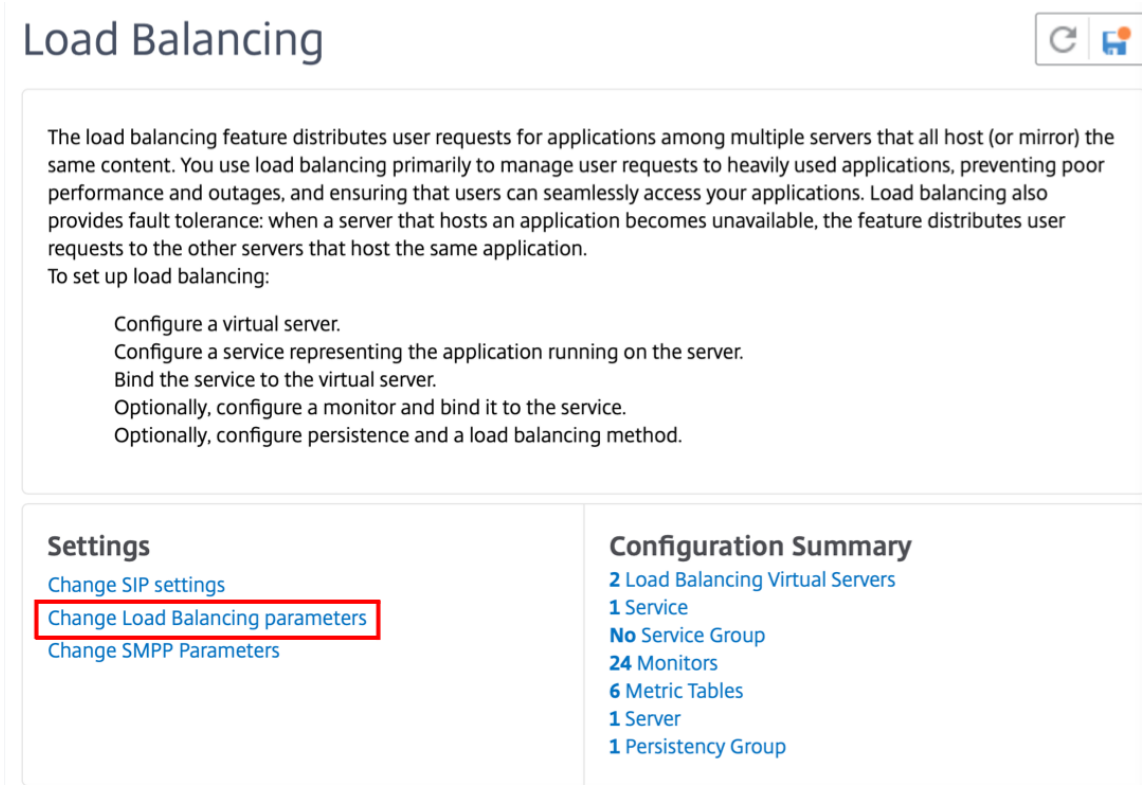
Nachdem Sie eine Variable konfiguriert haben, können Sie einen Wert zuweisen oder die Operation angeben, die an der Variablen ausgeführt werden soll, indem Sie eine Zuweisung erstellen.

1. Navigieren Sie zu **AppExpert > Zuweisungen**und klicken Sie auf **Hinzufügen**.
2. Geben **Sie auf der Seite Zuweisung erstellen** die Details ein und klicken Sie auf **Erstellen**.



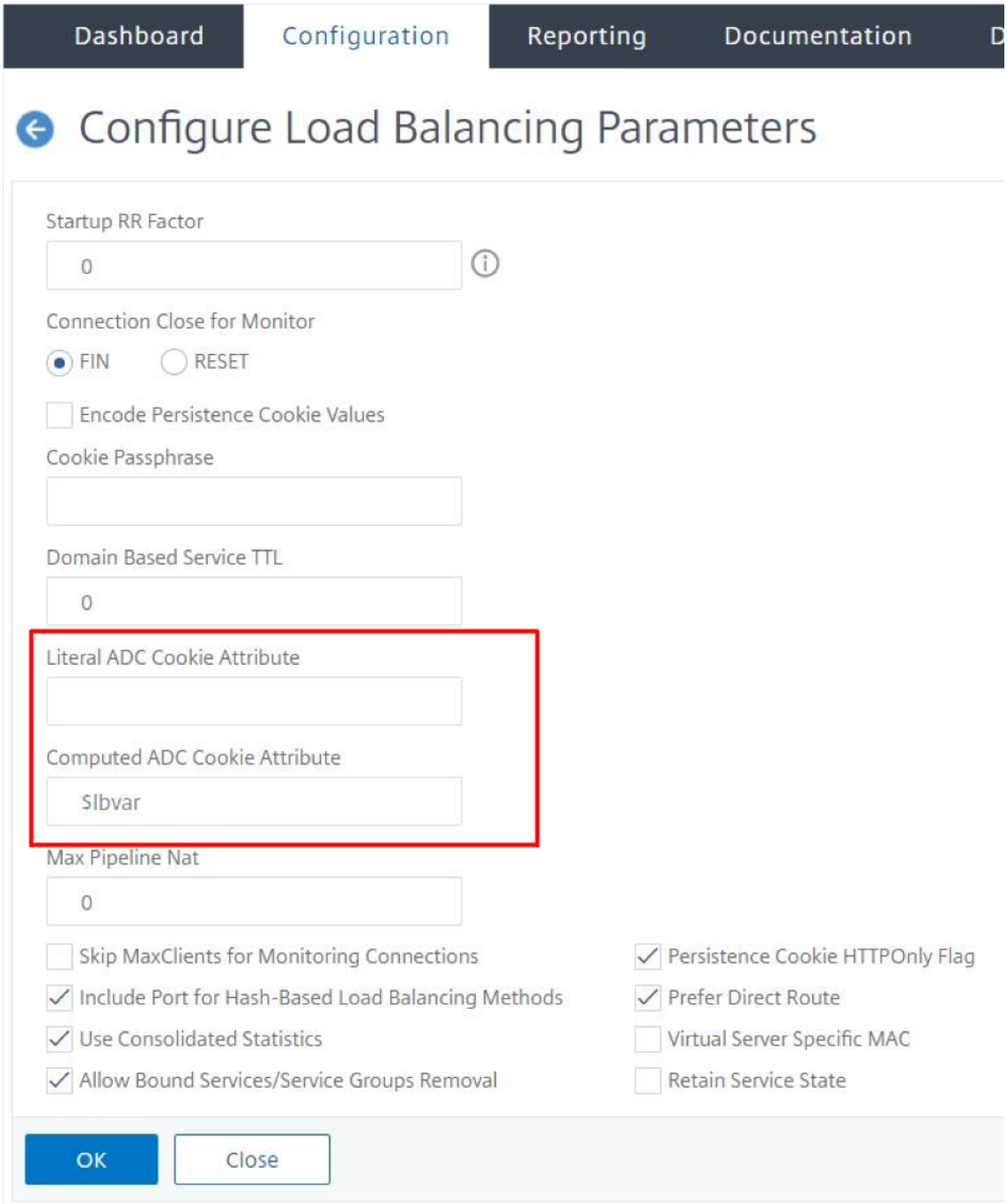
Festlegen der ADC-Cookie-Attribute in Lastenausgleichsparametern über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter ändern**.



2. Geben **Sie im Bereich „Load Balancing-Parameter konfigurieren** “ die entsprechenden Werte für eines der Felder ein, die Ihren Anforderungen entsprechen:

   - **Literales ADC-Cookie-Attribut**
   - **Berechnetes ADC-Cookie-Attribut**



3. Klicken Sie auf **OK**.

Festlegen der ADC-Cookie-Attribute im Load Balancing-Profil über die Befehlszeilenschnittstelle

Um eine Richtlinie für eine bestimmte Anwendung anzuwenden, die auf der NetScaler Appliance konfiguriert ist, können Sie die Cookie-Attributparameter im LB-Profil festlegen, das an den anwendungsspezifischen virtuellen LB-Server gebunden ist.

Die Einstellung **Literal ADC Cookie Attribute** im LB-Profil ermöglicht es Ihnen, die Cookie-Attribute bedingungslos in das von ADC generierte Cookie einzufügen, das für einen virtuellen Server spezifisch ist.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb profile <profile name> -LiteralADCCookieAttribute <string>
<!--NeedCopy-->
```

Beispiel:

```
add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
    =None
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
<!--NeedCopy-->
```

Die Einstellung für das **berechnete ADC-Cookie-Attribut** im LB-Profil ermöglicht es Ihnen, die auf den Client- oder Serverattributen basierenden Cookie-Attribute unter bestimmten Bedingungen in das von ADC generierte Cookie einzufügen. Stellen Sie dann dieses LB-Profil auf einen virtuellen LB-Server ein.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb profile <profile name> -ComputedADCCookieAttribute <ns variable>
<!--NeedCopy-->
```

Beispiel:

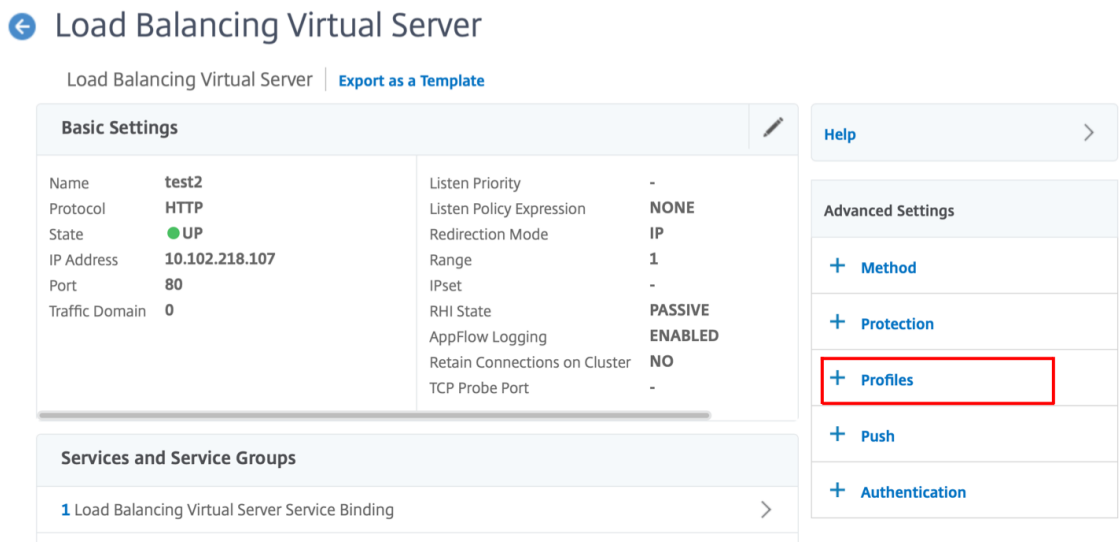
```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""
add lb profile LB-Vserver-Profile-1 -ComputedADCCookieAttributE "
    $cookieattribute_var"

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
```



```
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
add rewrite policy append_samesite_attribute true samesiteassign

add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
bind lb vserver LB-VServer-1 -policyName exception_samesite_attribute -
    priority 90 -gotoPriorityExpression 110 -type RESPONSE
bind lb vserver LB-VServer-1 -policyName append_samesite_attribute -
    priority 100 -gotoPriorityExpression 110 -type RESPONSE
<!--NeedCopy-->
```

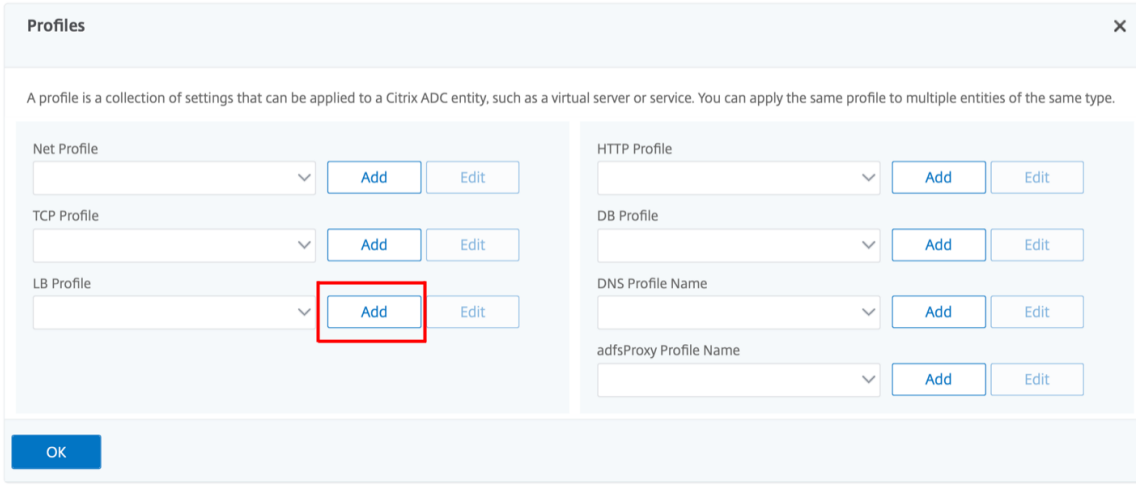
Festlegen der ADC Cookie-Attribute im Load Balancing-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Profile hinzufügen**.



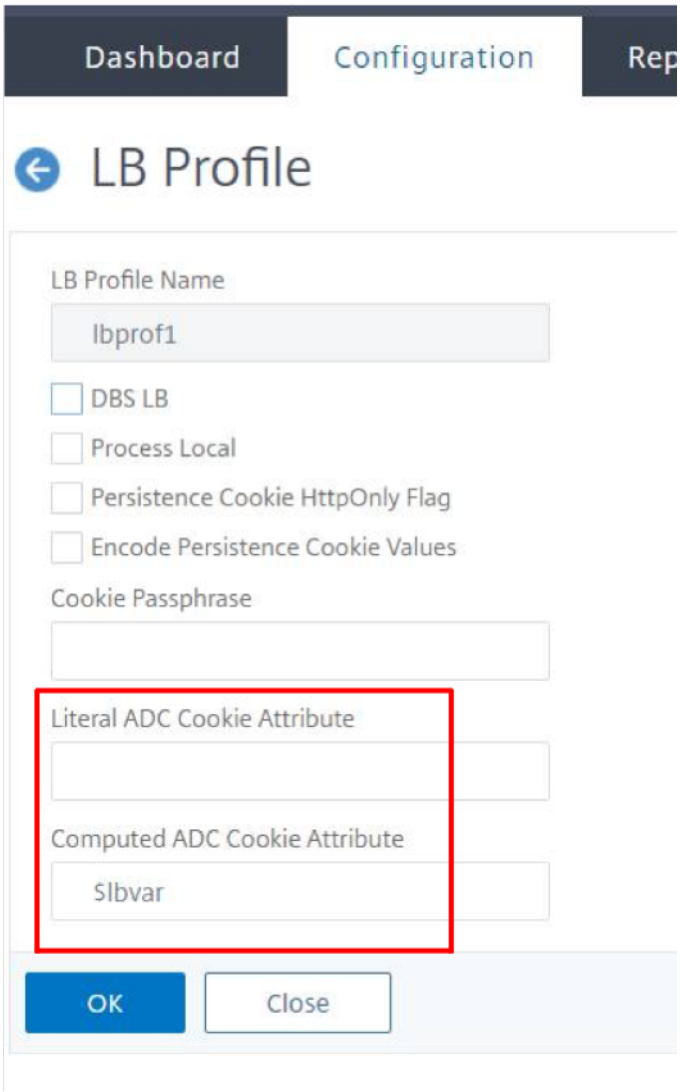
4. Klicken Sie im Abschnitt **Profile** auf **Hinzufügen**, um ein LB-Profil zu erstellen.

   Wenn Sie bereits ein Profil erstellt haben, wählen Sie es aus dem Dropdownmenü **LB-Profil** aus.



5. Geben Sie im Bereich **LB-Profil** die entsprechenden Werte für eines der Felder ein, die auf Ihrer Anforderung basieren:

- **Literales ADC-Cookie-Attribut**
- **Berechnetes ADC-Cookie-Attribut**



1. Klicken Sie auf **OK**.
2. Stellen Sie das erstellte LB-Profil auf den in **Schritt 1**erstellten virtuellen LB-Server ein.

Überprüfen Sie die ns-Variablenkonfiguration

Um zu überprüfen, ob die ADC-ns-Variable in LB-Parametern oder LB-Profil ordnungsgemäß konfiguriert ist, verwenden Sie die Befehle show lb parameter oder show lb profile.

In der folgenden Tabelle sind die verschiedenen Warnmeldungen und ihre Ursache aufgeführt, wenn die Variable ns nicht richtig konfiguriert ist.

Warnmeldung	Gründe
Die NS-Variable ist nicht konfiguriert. Konfigurieren Sie es mit dem Typ text () und dem Gültigkeitsbereich der Transaktion für die Variable	Die NS-Variable ist noch nicht konfiguriert.
Der Gültigkeitsbereich der konfigurierten NS-Variablen ist keine Transaktion.	Die Variable ist konfiguriert, aber der Gültigkeitsbereich ist nicht auf „Transaktion“ gesetzt.
Der Variablentyp ist nicht Text ().	Variable ist konfiguriert, aber der Typ ist nicht auf “Text” gesetzt.
Die konfigurierte Wert-Max-Größe für die NS-Variable ist größer als 255.	Der für die NS-Variable konfigurierte Wert beträgt mehr als 255 Zeichen. **Hinweis:** Eine maximale Länge von 255 Zeichen kann an ein ADC-generiertes Cookie angehängt werden. Die Zeichen, die die maximale Länge überschreiten, werden gekürzt.

Beispielausgabe

Im folgenden Beispiel wird die Warnmeldung angezeigt, wenn die ns-Variable nicht konfiguriert ist.

```
set lb parameter -ComputedADCCookieAttribute "$lbvar"

Warning: NS Variable is not configured. Please configure it with type
    text() and scope transaction
Done
<!--NeedCopy-->
```

Die Warnmeldung wird in der folgenden Ausgabe des `show lb parameter` Befehls angezeigt.

```
show lb parameter

Global LB parameters:
Persistence Cookie HttpOnly Flag: ENABLED
Use Encrypted Persistence Cookie: DISABLED
Use Port For Hash LB: YES
Prefer direct route: YES
Retain Service State: OFF
Start RR Factor: 0
Skip Maxclient for Monitoring: DISABLED
```



```
Monitor Connection Close: FIN
Use consolidated stats for LeastConnection: YES
Allow mac mode based vserver to pick thereturn traffic from services:
    DISABLED
Allow bound service removal: ENABLED
TTL for Domain Based Server: 0 secs

NetScaler Cookie Variable Name: $lbvar(NS Variable is not configured.
    Please configure it with type text() and scope transaction)

Done
<!--NeedCopy-->
```

Beispielkonfiguration für das Einfügen von Cookie-Attributen in die GSLB-Bereitstellung

Die folgende Beispielkonfiguration gilt für die Site-Persistenz, die auf GSLB-Diensten konfiguriert ist, die einem virtuellen LB-Server entsprechen. Um einige zusätzliche Cookie-Attribute an die GSLB-Cookies anzuhängen, führen Sie die folgende Konfiguration durch.

- Stellen Sie die ADC-Cookie-Attribute im LB-Profil ein (LB-vServer-Profile-1).
- Stellen Sie den Literal ADC Cookie-Attributwert, zum Beispiel „sameSite=None“, im LB-Profil ein.
- Stellen Sie das LB-Profil auf den virtuellen Lastausgleichsserver (LB-vServer-1) ein, der den GSLB-Dienst darstellt.

```
add gslb vserver GSLB-VServer-1 SSL -backupLBMethod ROUNDROBIN -
    tolerance 0 -appflowLog DISABLED
add gslb site site1 10.102.148.4 -publicIP 10.102.148.4
add gslb service site1_gsvc1 10.102.148.35 SSL 443 -publicIP
    10.102.148.35 -publicPort 443 -maxClient 0 -siteName site1 -
    sitePersistence HTTPRedirect -sitePrefix ss1 -cltTimeout 180 -
    svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver GSLB-VServer-1 -serviceName site1_gsvc1
bind gslb vserver GSLB-VServer-1 -domainName www.gslb.com -TTL 5

add service service-1 10.102.84.140 SSL 443

add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
    =None
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1

```



```
bind lb vserver LB-VServer-1 service-1
<!--NeedCopy-->
```

> **Hinweis**
>
> Sie können die Cookie-Attribute auch bedingt mithilfe des Berechneten ADC-Cookie-Attributs einfügen.

Beispielkonfiguration für das Einfügen eines Cookie-Attributs bei der Bereitstellung von Content Switching

Die folgende Beispielkonfiguration gilt, wenn mehrere Anwendungen hinter einem virtuellen Content Switching-Server gehostet werden. Um dieselbe Richtlinie auf alle Anwendungen anzuwenden, binden Sie die Rewrite-Richtlinien wie folgt an den virtuellen Content Switching-Server statt an den virtuellen LB-Server:

- Stellen Sie die ADC-Cookie-Attribute in den LB-Parametern ein.

  > **Hinweis:**
  >
  > Sie können die ADC-Cookie-Attribute auch im LB-Profil festlegen.

- Konfigurieren Sie die ns-Variable (cookieattribute_var), deren Type auf Text und Scope auf Transaction gesetzt ist.
- Stellen Sie das berechnete ADC-Cookie-Attribut in den globalen LB-Parametern mithilfe der Variablen ns ein.
- Legen Sie die Rewrite-Richtlinien (exception_samesite_attribute und append_samesite_attribute) für die virtuellen Content-Switching-Server fest, um die Cookie-Attribute einzufügen.

```
add ns variable cookieattribute_var -type "text(100)" -scope
    transaction
set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
add ns assignment samesiteassign -variable "$cookieattribute_var" -set
    ""SameSite=None""

add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
    \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
    typecast_text_t ALT "false").eq("true"))"
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
```



```
add rewrite policy append_samesite_attribute true samesiteassign

add lb vserver LB-VServer-1 SSL 10.102.148.35 443
add lb vserver LB-VServer-2 SSL 10.102.148.36 443

add cs vserver CS-VServer-1 SSL 10.102.148.42 443 -persistenceType
    COOKIEINSERT

add cs action act1 -targetLBVserver v1
add cs action act2 -targetLBVserver v2
add cs policy CS-policy-1 -rule "HTTP.REQ.URL.CONTAINS("file1.html")" -
    action act1
add cs policy CS-policy-2 -rule "HTTP.REQ.URL.CONTAINS("file2.html")" -
    action act2

bind cs vserver CS-VServer-1 -policyName CS-policy-1 -priority 1
bind cs vserver CS-VServer-1 -policyName CS-policy-2 -priority 2

bind cs vserver -policyname exception_samesite_attribute 90 110 -type
    RES_OVERRIDE
bind cs vserver -policyname append_samesite_attribute 100 110 -type
    RES_OVERRIDE
<!--NeedCopy-->
```

Lastausgleichskonfiguration anpassen

May 11, 2023

Nachdem Sie ein grundlegendes Load Balancing-Setup konfiguriert haben, können Sie mehrere Änderungen daran vornehmen, damit die Last genau nach Bedarf verteilt wird. Das Lastenausgleichs-Feature ist komplex. Sie können die Grundelemente ändern, indem Sie eine oder mehrere der folgenden Aktionen ausführen:

- Ändern des Load Balancing-Algorithmus
- Konfigurieren von Load Balancing-Gruppen und deren Verwendung zum Erstellen Ihrer Load Balancing-Konfiguration
- Persistente Client-Server-Verbindungen konfigurieren
- Konfigurieren des Umleitungsmodus
- Zuweisung verschiedener Gewichte zu verschiedenen Diensten mit unterschiedlichen Kapazitäten.

Der Standard-Lastenausgleichsalgorithmus auf der NetScaler Appliance ist die kleinste Verbindungsmeth-

ode. In der kleinsten Verbindungsmethode sendet die Appliance jede eingehende Verbindung an den Dienst, der derzeit die wenigsten Verbindungen verarbeitet. Sie können verschiedene Load Balancing-Algorithmen angeben, von denen jeder für unterschiedliche Bedingungen geeignet ist.

Um Anwendungen wie Einkaufswagen, die erfordern, dass alle Anforderungen desselben Benutzers an denselben Server weitergeleitet werden, können Sie die Appliance so konfigurieren, dass persistente Verbindungen zwischen Clients und Servern aufrechterhalten werden. Sie können auch Persistenz für eine Gruppe virtueller Server angeben. Persistence ermöglicht es der Appliance, einzelne Clientanfragen an denselben Dienst zu richten, unabhängig davon, welcher virtuelle Server in der Gruppe die Clientanforderung erhält.

Sie können den Umleitungsmodus aktivieren und konfigurieren, den die Appliance beim Umleiten von Benutzeranforderungen verwendet, indem Sie zwischen IP-basierter und MAC-basierter Weiterleitung wählen. Sie können verschiedenen Diensten auch Gewichtungen zuweisen und angeben, wie viel Prozent der eingehenden Last an jeden Dienst gerichtet werden muss. Durch die Zuweisung von Gewichten können Sie Server mit unterschiedlichen Kapazitäten in dasselbe Lastenausgleichs-Setup einbeziehen, ohne;

- Überlastung der Server mit geringerer Kapazität oder
- damit die Server mit höherer Kapazität im Leerlauf sitzen können.

Hash-Algorithmus für Persistenz über virtuelle Server hinweg anpassen

May 11, 2023

Die NetScaler-Appliance verwendet Hash-basierte Algorithmen, um die Persistenz auf virtuellen Servern aufrechtzuerhalten. Standardmäßig verwendet die Hash-basierte Load-Balancing-Methode einen Hashwert der IP-Adresse und der Portnummer des Dienstes. Wenn ein Dienst an verschiedenen Ports auf demselben Server verfügbar ist, generiert der Algorithmus unterschiedliche Hashwerte. Daher können verschiedene virtuelle Lastausgleichsserver Anfragen für dieselbe Anwendung an verschiedene Dienste senden, wodurch die Pseudopersistenz unterbrochen wird.

Als Alternative zur Verwendung der Portnummer zur Generierung des Hashwerts können Sie für jeden Dienst eine eindeutige Hash-ID angeben. Für einen Dienst muss derselbe Hash-Identifikationswert auf allen virtuellen Servern angegeben werden. Wenn ein physischer Server mehr als einen Anwendungstyp unterstützt, sollte jeder Anwendungstyp über eine eindeutige Hash-ID verfügen.

Der Algorithmus zur Berechnung des Hashwerts für einen Dienst funktioniert wie folgt:

- Standardmäßig legt eine globale Einstellung die Verwendung der Portnummer in einer Hash-Berechnung fest.
- Wenn Sie eine Hash-ID für einen Dienst konfigurieren, wird diese verwendet, und die Portnummer nicht, unabhängig von der globalen Einstellung.

- Wenn Sie keine Hash-ID konfigurieren, sondern den Standardwert der globalen Einstellung so ändern, dass die Verwendung der Portnummer nicht spezifiziert wird, basiert der Hashwert nur auf der IP-Adresse des Dienstes.
- Wenn Sie keine Hash-ID konfigurieren oder den Standardwert der globalen Einstellung ändern, um die Portnummer zu verwenden, basiert der Hashwert auf der IP-Adresse und der Portnummer des Dienstes.

Sie können auch Hash-Identifikatoren angeben, wenn Sie die CLI verwenden, um Dienste an eine Dienstgruppe zu binden. Im Konfigurationsprogramm können Sie eine Dienstgruppe öffnen und auf der Registerkarte Mitglieder Hash-IDs hinzufügen.

So ändern Sie die globale Einstellung use-portnumber mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
setze den LB-Parameter -UsePortForHashLB        NO)
(JA)
```

Beispiel:

```
> set lb parameter -usePortForHashLb NO
 Done
>show lb parameter
Global LB parameters:
        Persistence Cookie HttpOnly Flag: DISABLED
        Use port for hash LB: NO
 Done
<!--NeedCopy-->
```

So ändern Sie die globale Einstellung use-portnumber mithilfe der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren.
2. Wählen oder deaktivieren Sie die Option Port für hashbasierte LB-Methoden verwenden.

Um einen neuen Dienst zu erstellen und eine Hash-ID für einen Dienst mithilfe der CLI anzugeben

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Hash-ID festzulegen und die Einstellung zu überprüfen:

Dienst hinzufügen < name > (< ip >	< serverName >) < serviceType > < port > -Haschid < positive_integer >

```
show service <name>
<!--NeedCopy-->
```

Beispiel:

```
> add service flbkng 10.101.10.1 http 80 -hashId 12345
 Done
>show service flbkng
        flbkng (10.101.10.1:80) - HTTP
        State: DOWN
        Last state change was at Thu Nov  4 10:14:52 2010
        Time since last state change: 0 days, 00:00:15.990
        Server Name: 10.101.10.1
        Server ID : 0   Monitor Threshold : 0

        Down state flush: ENABLED
        Hash Id: 12345

1)      Monitor Name: tcp-default
                State: DOWN     Weight: 1

 Done
<!--NeedCopy-->
```

Um eine Hash-ID für einen vorhandenen Dienst mithilfe der CLI anzugeben

Geben Sie den Befehl set service, den Namen des Dienstes und **-hashID** gefolgt vom ID-Wert ein.

Um beim Hinzufügen eines Servicegruppenmitglieds eine Hash-ID anzugeben

Um für jedes Mitglied, das der Gruppe hinzugefügt werden soll, eine Hash-ID anzugeben und die Einstellung zu überprüfen, geben Sie an der Befehlszeile die folgenden Befehle ein (Achten Sie darauf, für jedes Mitglied eine eindeutige HashID anzugeben.):

```
bind servicegroup <serviceGroupName> <memberName> <port> -hashId <
   positive_integer>

show servicegroup <serviceGroupName>
```



```
<!--NeedCopy-->
```

Beispiel:

```
 bind servicegroup http_svc_group 10.102.27.153 80 -hashId 2222222

>show servicegroup SRV
        SRV - HTTP
        State: ENABLED  Monitor Threshold : 0
        …

        1)         1.1.1.1:80   State: DOWN     Server Name: 1.1.1.1
              Server ID: 123  Weight: 1
        Hash Id: 32211

                Monitor Name: tcp-default       State: DOWN
        …

        2)         2.2.2.2:80   State: DOWN     Server Name: 2.2.2.2
              Server ID: 123  Weight: 1
        Hash Id: 12345

                Monitor Name: tcp-default       State: DOWN
        …
Done

<!--NeedCopy-->
```

Um eine Hash-ID für einen Dienst mithilfe der GUI anzugeben

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Erstellen Sie einen neuen Dienst oder öffnen Sie einen vorhandenen Dienst und geben Sie die Hash-ID an.

Um mithilfe der GUI eine Hash-ID für ein bereits konfiguriertes Servicegruppenmitglied anzugeben

1. Navigieren Sie zu Traffic Management > Load Balancing > Service Groups.
2. Öffnen Sie ein Mitglied und geben Sie eine eindeutige Hash-ID ein.

Umleitungsmodus konfigurieren

May 11, 2023

Der Umleitungsmodus konfiguriert die von einem virtuellen Server verwendete Methode, um zu bestimmen, wohin eingehender Datenverkehr weitergeleitet werden soll. Die NetScaler-Appliance unterstützt die folgenden Umleitungsmodi. Bevor die Anforderung an einen Server weitergeleitet wird, funktionieren die Umleitungsmodi wie folgt:

- IP-basierte Weiterleitung (Standardeinstellung): Die Ziel-IP-Adresse wird in die IP-Adresse des Servers geändert.
- MAC-basierte Weiterleitung: Die Ziel-MAC-Adresse wird in die MAC-Adresse des Servers geändert. Die Ziel-IP-Adresse wird jedoch nicht geändert. Der MAC-basierte Umleitungsmodus wird hauptsächlich in Firewall-Lastausgleichsbereitstellungen verwendet.
- IP-TUNNEL-basiert: Für die IP-Pakete des Clients wird eine IP-in-IP-Kapselung durchgeführt. In den äußeren IP-Headern wird die Ziel-IP-Adresse auf die IP-Adresse des Servers und die Quell-IP-Adresse auf die Subnetz-IP (SNIP) festgelegt. Die Client-IP-Pakete werden nicht geändert. Dies gilt sowohl für IPv4- als auch für IPv6-Pakete.
- TOS-ID Basiert: Die TOS-ID des virtuellen Servers ist im TOS-Feld des IP-Headers codiert.

Sie können entweder den IP-TUNNEL oder die TOS-Option verwenden, um Direct Server Return (DSR) zu implementieren. Weitere Informationen finden Sie unter:

- Konfigurieren des DSR-Modus bei Verwendung von TOS
- Konfigurieren des Lastenausgleichs im DSR-Modus für IPv6-Netzwerke mithilfe des TOS-Feldes
- Konfigurieren des Lastenausgleichs im DSR-Modus mithilfe von IP Over IP

Sie können MAC-basierte Weiterleitung in Netzwerken konfigurieren, die DSR-Topologie, Link-Lastausgleich oder Firewall-Lastausgleich verwenden. Weitere Informationen zur MAC-basierten Weiterleitung für den Lastausgleich finden Sie unter Konfigurieren von MBF für die Lastausgleichskonfiguration.

So konfigurieren Sie den Umleitungsmodus mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```


> **Hinweis**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die `-m MAC` Option aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie den Umleitungsmodus über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und wählen Sie den Umleitungsmodus aus.

Konfigurieren von virtuellen Servern mit Wildcard-Funktion pro VLAN

August 19, 2021

Wenn Sie den Lastenausgleich für den Datenverkehr in einem bestimmten VLAN (Virtual Local Area Network) konfigurieren möchten, können Sie einen virtuellen Server mit Wildcards mit einer Listenrichtlinie erstellen, die darauf beschränkt, Datenverkehr nur im angegebenen VLAN zu verarbeiten.

So konfigurieren Sie einen virtuellen Server mit Platzhalterzeichen, der ein bestimmtes VLAN mit der CLI überwacht

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Wildcard Server zu konfigurieren, der ein bestimmtes VLAN überwacht, und überprüfen Sie die Konfiguration:

```
add lb vserver <name> <serviceType> IPAddress * Port * -listenpolicy <
    expression> [-listenpriority <positive_integer>]

show vserver
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-vlan1 ANY -listenpolicy "CLIENT.VLAN.ID.EQ(2)
    " -listenpriority 10

show vserver Vserver-LB-vlan1
<!--NeedCopy-->
```


So konfigurieren Sie einen virtuellen Server mit Platzhalterzeichen, der ein bestimmtes VLAN mit der GUI überwacht

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Erstellen Sie einen neuen virtuellen Server oder öffnen Sie einen vorhandenen virtuellen Server.
3. Geben Sie eine Priorität und einen Ausdruck der Listenrichtlinie an.

Nachdem Sie diesen virtuellen Server erstellt haben, binden Sie ihn an einen oder mehrere Dienste, wie unter Einrichten von Basic Load Balancingbeschrieben.

Gewichtungen für Dienste zuweisen

May 11, 2023

In einer Load-Balancing-Konfiguration weisen Sie Diensten Gewichtungen zu, um den Prozentsatz des Datenverkehrs anzugeben, der an jeden Dienst gesendet werden soll. Dienste mit höheren Gewichten können mehr Anfragen bearbeiten; Dienste mit niedrigerem Gewicht können weniger Anfragen bearbeiten. Durch die Zuweisung von Gewichtungen an Dienste kann die NetScaler-Appliance ermitteln, wie viel Datenverkehr jeder Load-Balancing-Server verarbeiten kann, und so die Last effektiver verteilen.

Hinweis: Wenn Sie eine Load-Balancing-Methode verwenden, die die Gewichtung von Diensten unterstützt (z. B. die Round-Robin-Methode), können Sie dem Dienst eine Gewichtung zuweisen.

In der folgenden Tabelle werden die Load-Balancing-Methoden beschrieben, die die Gewichtung unterstützen, und kurz beschrieben, wie sich die Gewichtung darauf auswirkt, wie ein Dienst für jeden Dienst ausgewählt wird.

Methoden des Lastenausgleichs	Serviceauswahl mit Gewichten
Runde Robin	Der virtuelle Server priorisiert die Warteschlange der verfügbaren Dienste so, dass Dienste mit den höchsten Gewichten häufiger an die Spitze der Warteschlange kommen als diejenigen mit den niedrigsten Gewichten und proportional mehr Datenverkehr erhalten. Eine vollständige Beschreibung finden Sie unter Die Round-Robin-Methode.

Methoden des Lastenausgleichs	Serviceauswahl mit Gewichten
Geringste Verbindung	Der virtuelle Server wählt den Dienst mit der besten Kombination aus den wenigsten aktiven Transaktionen und dem höchsten Gewicht aus. Eine vollständige Beschreibung finden Sie unter Die kleinste Verbindungsmethode.
Methode der geringsten Antwortzeit und der geringsten Antwortzeit mit Monitoren	Der virtuelle Server wählt den Dienst mit der besten Kombination aus den wenigsten aktiven Transaktionen und der schnellsten durchschnittlichen Antwortzeit aus. Eine vollständige Beschreibung finden Sie unter Die Methode der kleinsten Reaktionszeit.
Geringste Bandbreite	Der virtuelle Server wählt den Dienst mit der besten Kombination aus geringstem Datenverkehr und höchster Bandbreite aus. Eine vollständige Beschreibung finden Sie unter Die Methode der geringsten Bandbreite.
Am wenigsten Pakete	Der virtuelle Server wählt den Dienst mit der besten Kombination aus den wenigsten Paketen und dem höchsten Gewicht aus. Eine vollständige Beschreibung finden Sie unter Die Methode der kleinsten Pakete.
Benutzerdefinierte Last	Der virtuelle Server wählt den Dienst mit der besten Kombination aus niedrigster Last und höchstem Gewicht aus. Eine vollständige Beschreibung finden Sie unter Die benutzerdefinierte Load-Methode.
Hashing-Methoden und Token-Methode	Die Gewichtung wird von diesen Load-Balancing-Methoden nicht unterstützt.

So konfigurieren Sie einen virtuellen Server, um Diensten Gewichte zuzuweisen, indem Sie die CLI verwenden

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -weight <Value> <ServiceName>
```



```
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -weight 10 Service-HTTP-1
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Server, um Diensten Gewichte zuzuweisen, indem Sie die GUI verwenden

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Öffnen Sie den virtuellen Server und klicken Sie dann auf den Abschnitt **Dienste** .
3. Weisen Sie dem Service in der Gewichtungsspalte ein Gewicht zu.

Konfigurieren der Versionseinstellung für MySQL und Microsoft SQL Server

January 19, 2021

Sie können die Version von Microsoft® SQL Server® und den MySQL -Server für einen Lastausgleichsserver angeben, der vom Typ MSSQL bzw. MySQL ist. Die Versionseinstellung wird empfohlen, wenn Sie erwarten, dass einige Clients nicht dieselbe Version wie Ihr MySQL - oder Microsoft SQL Server-Produkt ausführen. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht.

So legen Sie den Microsoft SQL Server-Versionsparameter mit der CLI fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Microsoft SQL Server-Versionsparameter für einen virtuellen Lastausgleichsserver festzulegen und die Konfiguration zu überprüfen:

```
set lb vserver <name> -mssqlServerVersion <mssqlServerVersion>

show lb vserver <name>
<!--NeedCopy-->
```


Beispiel

```
> set lb vserver myMSSQLvip -mssqlServerVersion 2008R2
 Done
> show lb vserver myMSSQLvip
    myMSSQLvip (190.0.2.12:1433) - MSSQL    Type: ADDRESS
 . . .
 . . .
    MSsql Server Version: 2008R2
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```

So legen Sie den MySQL -Serververversionsparameter mit der CLI fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den MySQL Server-Versionsparameter für einen Lastausgleichsserver festzulegen und die Konfiguration zu überprüfen:

```
set lb vserver <name> -mysqlServerVersion <string>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel

```
> set lb vserver mysqlsvr -mysqlserverversion 5.5.30
 Done
> sh lb vserver mysqlsvr
     mysqlsvr (2.22.2.222:3306) - MYSQL      Type: ADDRESS
 . . .
 . . .
     Mysql Server Version: 5.5.30
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```


So legen Sie den MySQL - oder Microsoft SQL-Serververversionsparameter mit der GUI fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server vom Typ MySQL oder MSSQL, und legen Sie die Serverversion fest.

Virtuelle Multi-IP-Server

May 11, 2023

Der NetScaler unterstützt die Erstellung eines einzelnen virtuellen Lastausgleichsservers mit mehreren nicht konsekutiven/aufeinanderfolgenden IPv4- und IPv6-Adressen vom Typ VIP. Jede an einen virtuellen Server gebundene VIP-Adresse wird als einzelner virtueller Server behandelt. Diese virtuellen Server haben dasselbe Protokoll und andere Einstellungen auf virtueller Serverebene. Ein virtueller Server mit mehreren VIP-Adressen wird auch als virtueller Multi-IP-Server bezeichnet.

Im Folgenden sind einige Vorteile der Verwendung von virtuellen Multi-IP-Servern aufgeführt:

- Ein virtueller Multi-IP-Server entlastet die Erstellung vieler virtueller Server mit denselben Einstellungen und Dienstbindungen.
- Virtuelle Multi-IP-Server reduzieren effektiv die Möglichkeit, die Höchstgrenze für virtuelle Serverentitäten zu erreichen.
- Ein virtueller Multi-IP-Server kann für Clients in verschiedenen Subnetzen verwendet werden, um eine Verbindung zu derselben Gruppe von Servern herzustellen.
- Nur ein virtueller Multi-IP-Server kann für IPv6- und IPv4-Clients verwendet werden, um eine Verbindung zu derselben Gruppe von Servern herzustellen.

Konfiguration eines virtuellen Multi-IP-Servers

Die Konfiguration eines virtuellen Multi-IP-Servers umfasst die folgenden Aufgaben:

- Erstellen Sie ein IPset und binden Sie mehrere IP-Adressen daran.
- Binden Sie das IPset an virtuelle Server mit Lastausgleich.

Beachten Sie die folgenden Punkte in Bezug auf die IPset-Konfiguration:

- Ein IPset kann Folgendes haben:
  - nicht konsekutive/aufeinanderfolgende IPv4-Adressen und IPv6-Adressen
  - Kombinationen von IPv4- und IPv6-Adressen.
- Alle IPv4/IPv6-Adressen, die virtuellen Servern zugeordnet werden sollen, die IPset verwenden, müssen vom Typ VIP sein.

- Ein einzelnes IPset kann an mehrere virtuelle Server gebunden werden.
- IPv4/IPv6-Adressen können unabhängig von vorhandenen IPset-Bindungen an virtuelle Server an IPset gebunden/ungebunden sein.
- Sie müssen die IPset-Bindung an einen virtuellen Server aufheben, bevor Sie ein neues IPset daran binden.

So fügen Sie mithilfe der CLI ein IPset hinzu und binden mehrere VIP-Adressen daran

Geben Sie in der Befehlszeile Folgendes ein:

```
add ipset <name>

bind ipset <name> <IPaddress1 … >

bind ipset <name> <IPaddress2… >

show ipset <name>
<!--NeedCopy-->
```

So binden Sie das IPset mithilfe der CLI an einen virtuellen Server

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -ipset <ipset name>

show lb vserver <name>
<!--NeedCopy-->
```

So fügen Sie ein IPset hinzu und binden mehrere VIP-Adressen mithilfe der GUI daran

Navigieren Sie zu **System** > **Netzwerk** > **IPsets**, und erstellen Sie ein IPset mit mehreren VIP-Adressen.

So binden Sie das IPset mithilfe der GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server, an den Sie das erstellte IPset binden möchten.
2. Legen Sie in den **Grundeinstellungen**den **IPset**-Parameter auf den Namen des erstellten IPset fest.

```
> add ipset IPSET-1


```



```
Done

> bind ipset IPSET-1 9.9.9.10


Done

> bind ipset IPSET-1 1000::20


Done

> add lb vserver LBVS-1 HTTP 8.8.8.10 80  - ipset IPSET-1


Done

> add service SVC-1 3.3.3.10 HTTP 80


Done

> add service SVC-2 3.3.3.100 HTTP 80


Done

> bind lb vserver LBVS-1 SVC-1


Done

> bind lb vserver LBVS-1 SVC-2


Done
```

GSLB-Unterstützung für virtuelle Multi-IP-Server

Floating-IP-Adressen sind für die Hochverfügbarkeitsbereitstellungen erforderlich. Cloud-Bereitstellungen unterstützen keine Floating-IP. Die IP-Set-Funktion unterstützt Sie also bei der Unterstützung von Hochverfügbarkeit in Cloud-Bereitstellungen. Mit der IP-Set-Funktion können Sie jeder der primären und sekundären Instanzen eine private IP-Adresse zuordnen. Eine der privaten

IP-Adressen wird beim Erstellen des virtuellen Servers hinzugefügt. Die andere IP-Adresse ist an einen IP-Set gebunden. Das IP-Set wird dann mit dem virtuellen Server verknüpft. In der Regel wird eine öffentliche IP-Adresse einer der privaten IP-Adressen zugeordnet, basierend darauf, welche Appliance den Datenverkehr empfängt. Während des Failovers ändert sich diese Zuordnung dynamisch, um den Datenverkehr an den neuen Primärdatenverkehr weiterzuleiten.

In GSLB-Bereitstellungen stellt der GSLB-Dienst den virtuellen Server dar und erfordert sowohl die private als auch die öffentliche IP-Adresse des virtuellen Servers. In Cloud-Bereitstellungen werden mehrere private IP-Adressen als IP-Set dargestellt, aber der GSLB-Dienst kann nur eine private IP-Adresse akzeptieren. Daher wird empfohlen, bei der Konfiguration des GSLB-Dienstes die IP-Adresse anzugeben, die beim Hinzufügen des virtuellen Servers oder einer der IP-Adressen im IP-Set konfiguriert wurde. Sie müssen die IP-Set-Funktion im GSLB-Dienst nicht konfigurieren. Der auf dem virtuellen Lastausgleichsserver konfigurierte IP-Set, der mit dem GSLB-Dienst verknüpft ist, ist ausreichend.

In der übergeordneten GSLB-Topologie kann den virtuellen Lastausgleichsservern auf den untergeordneten Sites der IP-Satz zugeordnet sein. Der GSLB-Dienst, der dieser Topologie entspricht, trägt die öffentliche IP-Adresse und eine der privaten IP-Adressen. Die private IP-Adresse kann eine IP-Adresse im IP-Set sein oder diejenige, die beim Hinzufügen des virtuellen Servers auf der untergeordneten Site konfiguriert wurde. Die Kommunikation zwischen den übergeordneten und den untergeordneten Sites verwendet immer die öffentliche IP-Adresse und den öffentlichen Port des GSLB-Dienstes.

Mit IP-Set-Unterstützung können Sie auch einen einzigen virtuellen Serverendpunkt für IPv4- und IPv6-Datenverkehr haben. Zuvor mussten Sie verschiedene virtuelle Server für IPv4- und IPv6-Verkehr konfigurieren. Mit der Unterstützung von IP-Sätzen können Sie IPv4- und IPv6-IP-Adressen demselben IP-Set zuordnen. Sie können verschiedene GSLB-Dienste hinzufügen, die die IPv4- und IPv6-Endpunkte darstellen.

Begrenzen der Anzahl gleichzeitiger Anforderungen für eine Clientverbindung

May 11, 2023

Sie können die Anzahl gleichzeitiger Anfragen auf einer einzelnen Clientverbindung begrenzen. Sie können die Server vor Sicherheitslücken schützen, indem Sie die Anzahl der gleichzeitigen Anfragen begrenzen. Wenn die Client-Verbindung das angegebene maximale Limit erreicht, verwirft die NetScaler-Appliance nachfolgende Anfragen für die Verbindung, bis die Anzahl der ausstehenden Anfragen das Limit unterschreitet.

Sie können den MaxPipelineNAT-Parameter so konfigurieren, dass die Anzahl gleichzeitiger Anfragen auf einer einzelnen Clientverbindung begrenzt wird. Dieser Parameter gilt nur für die folgenden Dien-

sttypen und wenn „SvrTimeout“ auf Null gesetzt ist:

- ANY
- Alle UDP-Diensttypen außer DNS

Der Standardwert des Parameters MaxPipelineAt ist 255. Ein Wert von Null (0) begrenzt die Anzahl gleichzeitiger Anfragen nicht. Wenn kein Limit festgelegt ist, führt die NetScaler-Appliance alle Anfragen aus.

> **Hinweis**
>
> Wenn Sie MaxPipelineAt auf einen höheren Wert setzen, kann die Wahrscheinlichkeit eines Spoofing-Angriffs höher sein. Daher wird empfohlen, MaxPipelineAt auf einen niedrigeren Wert zu setzen.

So begrenzen Sie die Anzahl gleichzeitiger Verbindungen für einen Client mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb parameter -maxPipelineNat <positive_integer>
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -maxPipelineNat 199
<!--NeedCopy-->
```

Um die Anzahl gleichzeitiger Verbindungen für einen Client mithilfe der GUI zu begrenzen

Navigieren Sie zu **Traffic Management > Load Balancing > Configure Load Balancing Parameters**, und geben Sie einen Wert für Max Pipeline NAT-Anforderungen an.

Diameter-Lastausgleich konfigurieren

May 11, 2023

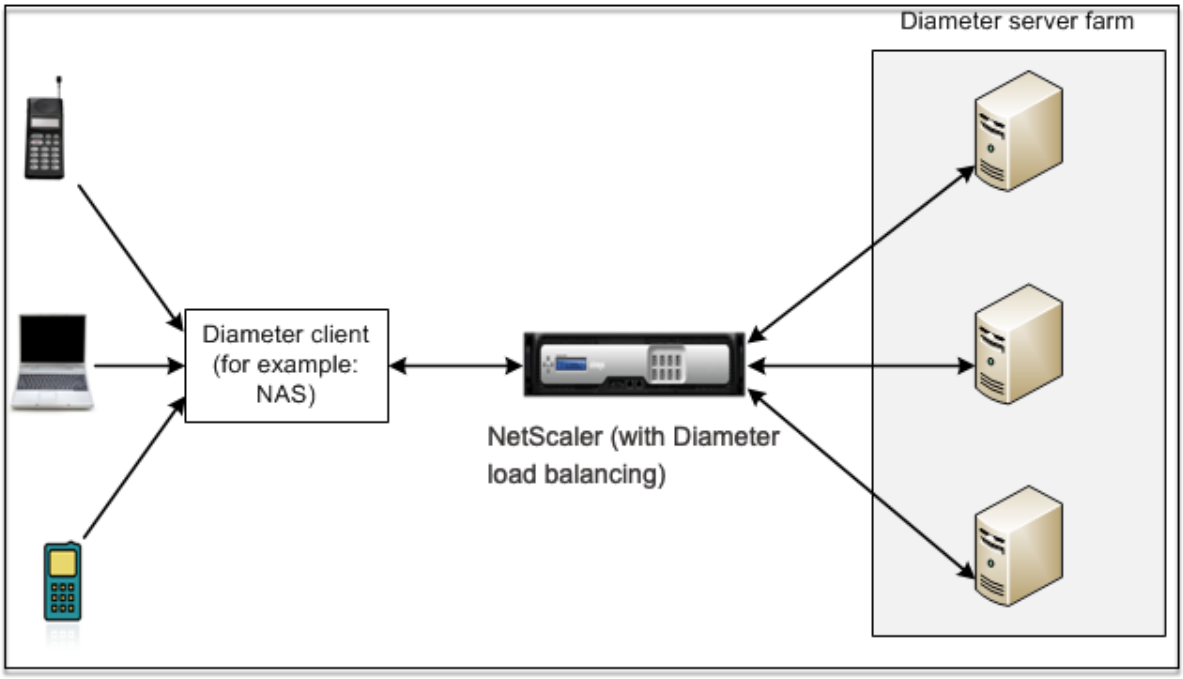
Das Diameter-Protokoll ist ein AAA-Signalisierungsprotokoll (Authentication, Authorization, Accounting) der nächsten Generation, das hauptsächlich auf Mobilgeräten wie Laptops und Mobiltelefonen verwendet wird. Es ist ein Peer-to-Peer-Protokoll, im Gegensatz zu dem traditionellen Client-Server-Modell, das von den meisten anderen Protokollen verwendet wird. In den meisten

Diameter-Bereitstellungen stellen jedoch die Clients die Anfrage her und der Server reagiert auf die Anfrage.

Wenn Diameter-Nachrichten ausgetauscht werden, verarbeitet der Diameter-Server normalerweise viel mehr als der Diameter-Client. Mit der Zunahme der Signalmenge auf der Steuerungsebene wird der Diameter-Server zu einem Engpass. Daher muss für Diameter-Nachrichten ein Lastenausgleich auf mehrere Server verteilt werden. Ein virtueller Server, der den Lastenausgleich von Diameter-Nachrichten durchführt, bietet die folgenden Vorteile:

- Geringere Auslastung der Diameter-Server, was sich in einer schnelleren Reaktionszeit für Endbenutzer niederschlägt.
- Überwachung des Serverzustands und bessere Failover-Funktionen.
- Bessere Skalierbarkeit in Bezug auf die Servererweiterung ohne Änderung der Client-Konfiguration.
- Hohe Verfügbarkeit.
- Entladung mit SSL-Durchmesser.

Die folgende Abbildung zeigt ein Diameter-System in einer NetScaler-Bereitstellung:



Ein Durchmessersystem besteht aus den folgenden Komponenten:

- **Kunde von Diameter.** Unterstützt Diameter Client-Anwendungen zusätzlich zum Basisprotokoll. Durchmesser-Clients werden häufig in Geräten am Rande eines Netzwerks implementiert und bieten Zugangskontrolldienste für dieses Netzwerk. Typische Beispiele für Diameter Clients sind ein Network Access Server (NAS) und der Mobile IP Foreign Agent (FA).
- **Mittel mit einem Diameter.** Stellt Relay-, Proxy-, Weiterleitungs- oder Übersetzungsdienste

bereit. Die NetScaler-Appliance (konfiguriert mit einem virtuellen Diameter-Load-Balancing-Server) spielt die Rolle eines Diameter-Agenten.

- **Diameter des Servers.** Bearbeitet die Authentifizierungs-, Autorisierungs- und Abrechnungsanfragen für einen bestimmten Bereich. Ein Diameter-Server muss zusätzlich zum Basisprotokoll Diameter-Serveranwendungen unterstützen.

In einer typischen Diameter-Topologie sendet ein Endbenutzergerät (z. B. ein Mobiltelefon), wenn es einen Dienst benötigt, eine Anfrage an einen Diameter-Client. Jeder Diameter-Client stellt eine einzelne Verbindung (TCP-Verbindung — SCTP wird noch nicht unterstützt) mit einem Diameter-Server her, wie im Diameter-Basisprotokoll RFC 6733 spezifiziert. Die Verbindung ist langlebig und alle Nachrichten zwischen den beiden Diameter-Knoten (Client und Server) werden über diese Verbindung ausgetauscht. Der NetScaler verwendet nachrichtenbasiertes Load Balancing.

Beispiel:

Ein Mobilfunkanbieter verwendet Diameter für sein Abrechnungssystem. Wenn ein Abonnent eine Prepaid-Nummer verwendet, sendet der Diameter-Client wiederholt Anfragen an den Server, um das verfügbare Guthaben zu überprüfen. Das Diameter-Protokoll stellt eine Verbindung zwischen dem Client und dem Server her, und alle Anfragen werden über diese Verbindung ausgetauscht. Verbindungsbasiertes Load Balancing wäre sinnlos, da es nur eine Verbindung gibt. Aufgrund der großen Anzahl von Nachrichten auf der Verbindung beschleunigt der nachrichtenbasierte Lastausgleich jedoch den Prozess der Abrechnung an den Prepaid-Mobilfunkabonnenten.

So funktioniert der Durchmesserlastenausgleich

Eine Disconnect Peer Request (DPR) zeigt die Absicht des Peers an, die Verbindung zu schließen, mit dem Grund für das Schließen der Verbindung. Der Peer antwortet mit einem DPA (TCP sorgt immer für eine erfolgreiche DPA).

- Wenn die Appliance eine DPR vom Client empfängt, sendet sie die DPR an alle Server und antwortet sofort mit einem DPA an den Client. Die Server antworten mit DPAs, aber die Appliance ignoriert sie. Der Client sendet eine FIN, die die Appliance an alle Server sendet.
- Wenn die Appliance eine DPR vom Server empfängt, antwortet sie nur an diesen Server mit einem DPA und entfernt den Server nicht aus dem Wiederverwendungspool. Wenn der Server eine FIN sendet, antwortet die Appliance mit FIN/ACK und entfernt Verbindungen aus dem Wiederverwendungspool.
- Wenn die Appliance eine FIN vom Client empfängt, sendet sie dem Client eine FIN/ACK, sendet die FIN und entfernt sofort die Serververbindung aus dem Wiederverwendungspool.
- Wenn die Appliance eine FIN vom Server empfängt, sendet sie eine FIN/ACK und entfernt sie aus dem Wiederverwendungspool. Jede neue Nachricht für diesen Server wird über eine neue Verbindung gesendet.

Load Balancing von Diameter-Verkehr

Wenn ein Client eine Anforderung an die NetScaler Appliance sendet, analysiert die Appliance die Anforderung und gleicht sie kontextuell auf einen Diameter-Server basierend auf einem Persist-AVP aus. Die Appliance hat dem Server die Clientidentität angekündigt, sodass keine Routeneinträge hinzugefügt werden, da der Server Nachrichten direkt vom Client erwartet.

Serverinitiierte Anfragen sind nicht so häufig wie Clientanfragen. Serverinitiierte Anfragen ähneln vom Client initiierten Anfragen, außer:

- Da Nachrichten von mehreren Servern empfangen werden, behält die Appliance den Transaktionsstatus bei, indem sie jeder weitergeleiteten Anforderungsnachricht eine eindeutige Hop by Hop (HByH) -Nummer hinzufügt. Wenn die Nachrichtenantwort eintrifft (mit derselben HbYH-Nummer), übersetzt die Appliance diese HbYH-Nummer in die HbYH-Nummer, die auf dem Server empfangen wurde, als die Anfrage eintraf.
- Die NetScaler-Appliance fügt einen Routeneintrag hinzu, indem sie ihre Identität eingibt, da der Client die Appliance als Relay-Agent sieht.

Hinweis: Wenn sich eine Diameter-Nachricht über mehr als ein Paket erstreckt, sammelt die Appliance die Pakete in einer unvollständigen Header-Warteschlange und leitet sie an den Server weiter, wenn die vollständige Nachricht gesammelt ist. In ähnlicher Weise teilt die Appliance, wenn ein einzelnes Paket mehr als eine Diameter-Nachricht enthält, das Paket auf und leitet die Nachrichten an Server weiter, wie vom virtuellen Lastausgleichsserver festgelegt.

Trennen Sie eine Sitzung

Eine Disconnect Peer Request (DPR) zeigt die Absicht des Peers an, die Verbindung zu schließen, mit dem Grund für das Schließen der Verbindung. Der Peer antwortet mit einem DPA (TCP sorgt immer für eine erfolgreiche DPA).

- Wenn die NetScaler-Appliance eine DPR vom Client empfängt, sendet sie die DPR an alle Server und antwortet sofort mit einem DPA an den Client. Die Server antworten mit DPAs, aber die Appliance ignoriert sie. Der Client sendet eine FIN, die die Appliance an alle Server sendet.
- Wenn die Appliance eine DPR vom Server empfängt, antwortet sie nur an diesen Server mit einem DPA und entfernt den Server nicht aus dem Wiederverwendungspool. Wenn der Server eine FIN sendet, antwortet die Appliance mit FIN/ACK und entfernt Verbindungen aus dem Wiederverwendungspool.
- Wenn die Appliance eine FIN vom Client empfängt, sendet sie dem Client eine FIN/ACK, sendet die FIN und entfernt sofort die Serververbindung aus dem Wiederverwendungspool.
- Wenn die Appliance eine FIN vom Server empfängt, sendet sie eine FIN/ACK und entfernt sie aus dem Wiederverwendungspool. Jede neue Nachricht für diesen Server wird über eine neue Verbindung gesendet.

Load Balancing für Durchmesserverkehr konfigurieren

Um die NetScaler-Appliance so zu konfigurieren, dass sie den Durchmesser-Traffic ausgleicht, müssen Sie zuerst die Durchmesserparameter auf der Appliance festlegen, dann den Durchmessermonitor hinzufügen, die Dienste an den Monitor binden, den virtuellen Diameter-Load-Balancing-Server hinzufügen und die Dienste an den virtuellen Server binden.

So konfigurieren Sie den Lastenausgleich für den Diameter-Verkehr mithilfe der Befehlszeilenschnittstelle

Konfigurieren Sie die Durchmesserparameter.

```
set ns diameter -identity <string> -realm <string> -
   serverClosePropagation <YES|NO>
<!--NeedCopy-->
```

Beispiel:

```
set ns diameter -identity mydomain.org -realm org -
   serverClosePropagation YES
<!--NeedCopy-->
```

Fügen Sie einen Durchmessermonitor hinzu.

```
add lb monitor <monitorName> DIAMETER -originHost <string> -originRealm
    <string>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor diameter_mon DIAMETER -originHost mydomain.org -
   originRealm org
<!--NeedCopy-->
```

Erstellen Sie die Diameter-Dienste.

```
add service <name> <IP> DIAMETER <port>
<!--NeedCopy-->
```

Beispiel:

```
add service diameter_svc0 10.102.82.86 DIAMETER 3868

add service diameter_svc1 10.102.82.87 DIAMETER 3868

```



```
add service diameter_svc2 10.102.82.88 DIAMETER 3868

add service diameter_svc3 10.102.82.89 DIAMETER 3868
<!--NeedCopy-->
```

Binden Sie die Diameter-Dienste an den Diameter-Monitor.

```
bind service <name>@ monitorName <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
bind service diameter_svc0 -monitorName diameter_mon

bind service diameter_svc1 -monitorName diameter_mon

bind service diameter_svc2 -monitorName diameter_mon

bind service diameter_svc3 -monitorName diameter_mon
<!--NeedCopy-->
```

Fügen Sie einen virtuellen Diameter-Load-Balancing-Server mit Diameter-Persistenz hinzu.

```
add lb vserver <name> DIAMETER <IPAddress> <port> -persistenceType
   DIAMETER -persistAVPno <positive_integer>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver diameter_vs DIAMETER 10.102.112.152 3868 -
   persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Binden Sie die Diameter-Dienste an den virtuellen Diameter-Load-Balancing-Server.

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver diameter_vs diameter_svc0

bind lb vserver diameter_vs diameter_svc1

bind lb vserver diameter_vs diameter_svc2
```



```
6
7 bind lb vserver diameter_vs diameter_svc3
8 <!--NeedCopy-->
```

Speichern Sie die Konfiguration.

```
1 save ns config
2 <!--NeedCopy-->
```

Hinweis: Sie können den Lastausgleich des Diameter-Datenverkehrs über SSL auch mithilfe des Diensttyps **SSL_DIAMETER** konfigurieren.

So konfigurieren Sie den Lastenausgleich für den Diameter-Verkehr mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **System** > **Einstellungen** > **Durchmesserparameter ändern** und stellen Sie die Durchmesserparameter ein.
2. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und erstellen Sie einen virtuellen Lastausgleichsserver vom Typ Diameter.
3. Erstellen Sie einen Dienst vom Typ Diameter.
4. Erstellen Sie einen Monitor vom Typ Diameter. Stellen Sie unter Spezielle Parameter den Ursprungshost und den Ursprungsbereich ein.
5. Binden Sie den Monitor an den Dienst, und binden Sie den Dienst an den virtuellen Diameter Server.
6. Klicken Sie unter Erweiterte Einstellungen auf **Persistenz**, geben Sie den Durchmesser an, und geben Sie eine Persistenz-AVP-Nummer ein.
7. Klicken Sie auf **Speichern**, und klicken Sie auf **Fertig**.

FIX-Lastausgleich konfigurieren

May 11, 2023

Financial Information Exchange (FIX) -Protokoll ist ein Open-Message-Standard, der in der Finanzindustrie für den elektronischen Austausch von Informationen im Zusammenhang mit Wertpapiertransaktionen zwischen Handelspartnern verwendet wird. Das FIX/SSL_FIX-Protokoll wird ausführlich von Buy-Side- und Sell-Side-Firmen, Handelsplattformen und Regulierungsbehörden für die Kommunikation von Handelsinformationen verwendet.

Mit dieser Funktion können Sie einen virtuellen FIX- oder SSL_FIX-Server für den Lastenausgleich konfigurieren, um eingehende FIX-Nachrichten zu verteilen und die Sicherheit in FIX-Messaging bere-

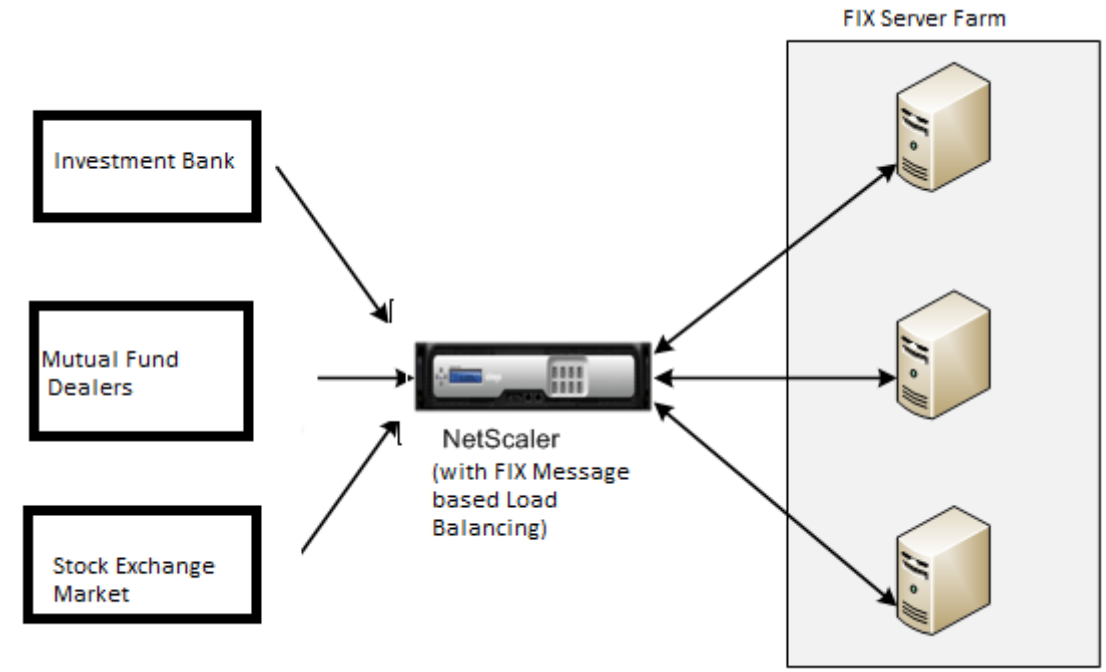
itzustellen. NetScaler unterstützt den nachrichtenbasierten FIX-Lastenausgleich (MBLB) für die Versionen FIX 4.1, FIX 4.2, FIX 4.3 und FIX 4.4.

FIX MBLB auf einer NetScaler Appliance bietet die folgenden Vorteile:

1. Effizientes Management von FIX- oder SSL_FIX-Servern mit hervorragender HA- und Zustandsüberwachung.
2. SYN-Schutz für alle FIX- oder SSL_FIX-Server.
3. FIX Sitzungspersistenz.

So funktioniert FIX Load Balancing

Ein FIX MBLB-Setup enthält einen virtuellen FIX-Lastausgleichsserver und mehrere FIX-Server mit Lastenausgleich. Der virtuelle FIX-Server empfängt eingehenden Clientdatenverkehr, analysiert den eingehenden Datenverkehr in FIX-Nachrichten, wählt für jede FIX-Nachricht einen FIX-Server aus und leitet die Nachricht an den ausgewählten FIX-Server weiter. Die folgende konzeptionelle Zeichnung veranschaulicht ein typisches FIX-Lastenausgleichs-Setup.



In einem einfachen FIX MBLB-Setup verteilt der virtuelle FIX-Server FIX-Nachrichten von Clients an die FIX-Server mit Lastenausgleich mit der Roundrobin-Load-Balancing-Methode. Wenn die Persistenz vom Typ FIXSESSION aktiviert ist, wählt der virtuelle FIX-Server denselben Server für verschiedene FIX-Meldungen aus, die zu derselben FIX-Sitzung gehören. Die FIX-Sitzung wird basierend auf den Werten der **FIX-Felder** SenderCompId (Tag 49) und targetCompid (Tag 56) bestimmt.

Konfigurieren und Überwachen des Lastausgleichs für FIX-Datenverkehr

Im Folgenden sind die Konfigurationen aufgeführt, die Sie vornehmen müssen, um den FIX-Nachrichtenverkehr auszubalancieren:

1. Konfiguration des virtuellen FIX-Load-Balancing-Servers
2. Konfiguration des virtuellen SSL_FIX-Load-Balancing-Servers
3. Konfiguration des FIX-Load-Balancing-Dienstes
4. Konfiguration des SSL_FIX-Load-Balancing-Dienstes
5. Konfiguration der FIXSESSION-Persistenz
6. Persistenz-Timeout festlegen
7. FIX/SSL_FIX-Statistiken anzeigen
8. Überwachung persistenter FIX/SSL_FIX-Sitzungen

So konfigurieren Sie einen FIX-Load-Balancing-Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> FIX <IP> <PORT>
<!--NeedCopy-->
```

Beispiel

```
add lb vserver vs1 FIX 10.102.82.86 3868
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen SSL_FIX-Loadbalancing-Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> SSL_FIX <IP> <PORT>
<!--NeedCopy-->
```

Beispiel

```
add lb vserver vs1 SSL_FIX 10.102.82.86 3868
<!--NeedCopy-->
```

So konfigurieren Sie einen FIX-Dienst mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
add service <name> <ip-addr> FIX <port>
<!--NeedCopy-->
```

Beispiel

```
add service_svc1 10.102.82.86 FIX 3868
<!--NeedCopy-->
```

So konfigurieren Sie einen SSL_FIX-Dienst mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <ip-addr> SSL_FIX <port>
<!--NeedCopy-->
```

Beispiel

```
add service svc1 10.102.82.86 SSL_FIX 3868
<!--NeedCopy-->
```

So konfigurieren Sie die FIXSESSION-Persistenz mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -persistenceType FIXSESSION
<!--NeedCopy-->
```

Beispiel

```
set lb vserver vs1 -persistenceType FIXSESSION
<!--NeedCopy-->
```

So legen Sie das Persistenz-Timeout mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -timeout <value>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver vs1 - timeout 2
<!--NeedCopy-->
```


Um FIX-Statistiken mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat lb vserver <name>
<!--NeedCopy-->
```

Beispiel

```
stat lb vserver_svc1
<!--NeedCopy-->
```

Um den FIX-Dienst mithilfe der Befehlszeilenschnittstelle an den virtuellen FIX-Server zu binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <service name>
<!--NeedCopy-->
```

Beispiel

```
bind lb vserver vs1 svc1
<!--NeedCopy-->
```

Um persistente FIX-Sitzungen mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
show lb persistentSessions <name>
<!--NeedCopy-->
```

Beispiel

```
show lb persistentSessions vs1
<!--NeedCopy-->
```

> **Hinweis**
>
> Hinweis: Sie können jetzt den Lastenausgleich des FIX-Datenverkehrs über SSL mithilfe des Diensttyps SSL_FIX konfigurieren. Dieser Dienst bietet eine sichere Kommunikation für FIX-Nachrichten.

So konfigurieren Sie den virtuellen FIX-Load-Balancing-Server mithilfe der GUI

1. Navigieren Sie zur Seite **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server** und klicken Sie auf **Hinzufügen**, um einen virtuellen FIX Load Balancing-Server zu erstellen.
2. Stellen Sie auf der Seite **Load Balancing Virtual Server** die Serverparameter ein:
   a) Name des virtuellen Servers
   b) Protokolltyp als „FIX“
   c) IP-Adresstyp des Servers
   d) Server-IP-Adresse
   e) Serverportnummer
3. Klicken Sie auf **OK** und **Weiter**, um andere Parameter festzulegen.
4. Wählen Sie im Abschnitt **Dienste** einen neuen virtuellen FIX-Lastausgleichsdienst aus oder fügen Sie ihn hinzu, und binden Sie ihn an den FIX-Server.
5. Stellen Sie im Abschnitt **Persistenz** die folgenden Parameter ein:
   a) Persistenztyp als ‘FIXSESSION’
   b) Timeout-Intervall
6. Klicke auf **OK** und dann auf **Fertig**.

So bearbeiten Sie einen virtuellen FIX-Load-Balancing-Server mithilfe der GUI

Navigieren Sie zur Seite **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen FIX-Server aus und klicken Sie auf **Bearbeiten**.

So löschen Sie einen virtuellen FIX-Lastausgleichsserver mit der GUI

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen FIX-Server aus und klicken Sie auf **Löschen**.

So konfigurieren Sie den virtuellen FIX-Lastausgleichsdienst mit der GUI

1. Navigieren Sie zur Seite **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**, um einen virtuellen FIX Load Balancing-Dienst zu erstellen.
2. Legen Sie auf der Seite **Dienste** die folgenden Parameter fest. Sie können auf den Pfeil “Mehr” klicken, um andere Parameter wie Verkehrsdomäne, Hash-ID, Server-ID, Cache-Typ und Anzahl der aktiven Verbindungen festzulegen.
   a) Dienstname — FIX Virtual Service Name
   b) Wählen Sie den virtuellen Servertyp als (Neu oder Bestehend)
   c) Protokoll — Protokolltyp als ‘FIX’
   d) Server — IP-Adresse des virtuellen Servers

e) Port — Serverportnummer

3. Klicken Sie auf **OK** und **Weiter**, um weitere Parameter wie Monitore, Schwellenwert und Timeout, Profile und Richtlinien festzulegen.
4. Klicke auf **OK** und dann auf **Fertig**.

So bearbeiten Sie einen virtuellen FIX-Load-Balancing-Dienst mithilfe der GUI

Navigieren Sie zur Seite **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services**, wählen Sie einen **FIX-Dienst** aus und klicken Sie auf **Bearbeiten**.

So löschen Sie einen virtuellen FIX-Lastausgleichsdienst mit der GUI

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services** Seite, wählen Sie einen FIX-Dienst aus und klicken Sie auf **Löschen**.

So zeigen Sie FIX-Lastausgleichserver-Statistiken an

Navigieren Sie zur Seite **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server** und klicken Sie dann auf **Statistiken**, um die FIX-Serverstatistiken anzuzeigen.

Um persistente Sessions für einen FIX-Server mithilfe der GUI anzuzeigen

Navigieren Sie zur Seite **Konfiguration** > **Traffic Management** und klicken Sie unter „ **Sitzungen überwachen** “ auf **Virtual Server Persistent Sessions**.

So löschen Sie persistente Sitzungen für einen FIX-Server mithilfe der GUI

1. Navigieren Sie zur Seite „ **Konfiguration** “ > „ **Traffic Management** “ und klicken Sie unter „ **Sitzungen überwachen** “ auf „ **Persistente Sitzungen löschen**“.
2. Stellen Sie auf der Seite **Clear Persistent Sessions** die folgenden Parameter ein:
   a) Virtueller Server — Wählen Sie einen virtuellen FIX-Server
   b) Persistenzparameter — Wählen Sie einen FIX-Persistenzparameter
3. Klicken Sie auf **OK**.

MQTT-Lastausgleich

May 11, 2023

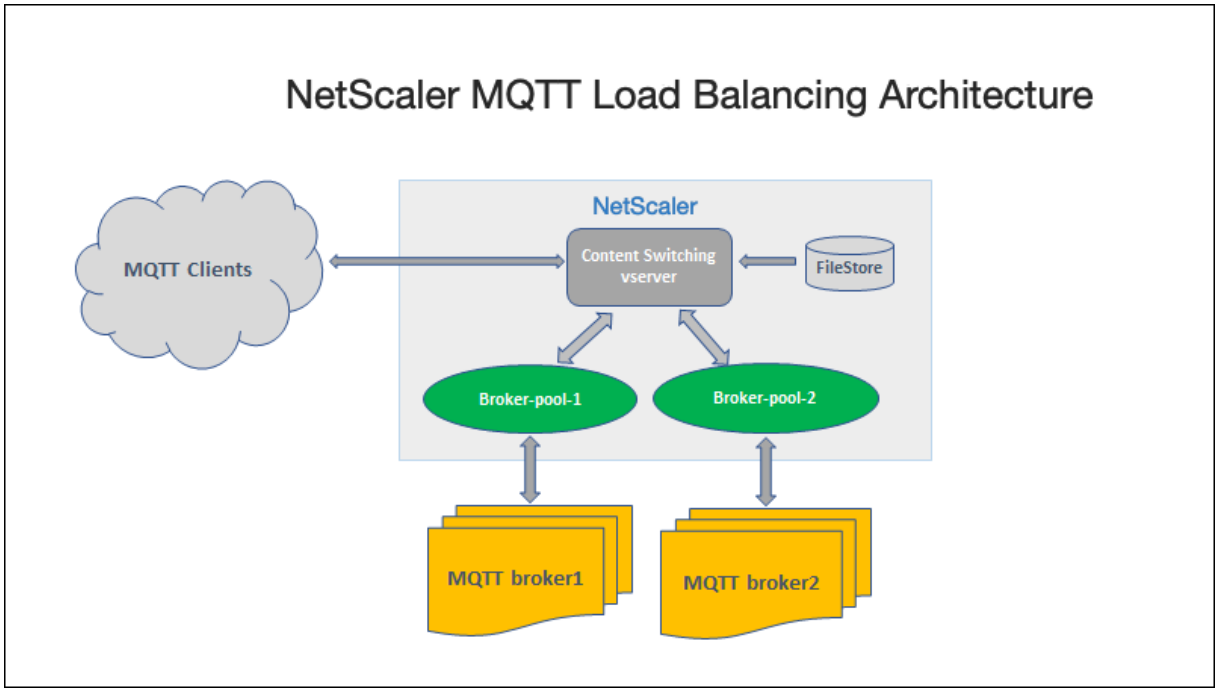
Der Message Queuing Telemetry Transport (MQTT) ist ein OASIS-Standard-Messaging-Protokoll für das Internet der Dinge (IoT). MQTT ist eine flexible und einfach zu bedienende Technologie, die eine effektive Kommunikation innerhalb eines IoT-Systems ermöglicht. MQTT ist ein auf Brokern basierendes Protokoll und wird häufig verwendet, um den Nachrichtenaustausch zwischen Kunden und Broker zu erleichtern.

Die folgenden Hauptvorteile von MQTT machen es zu einer gut geeigneten Option für Ihr IoT-Gerät:

- Zuverlässigkeit
- Schnelle Reaktionszeit
- Fähigkeit, eine unbegrenzte Anzahl von Geräten zu unterstützen
- Veröffentlichen und abonnieren Sie Nachrichten, die sich perfekt für die Kommunikation von vielen zu vielen eignen

IoT ist das Netzwerk miteinander verbundener Geräte, die mit Sensoren, Software, Netzwerkkonnektivität und der erforderlichen Elektronik ausgestattet sind. Die eingebetteten Komponenten ermöglichen es IoT-Geräten, Daten zu sammeln und auszutauschen. Die zunehmende Nutzung von IoT-Geräten bringt mehrere Herausforderungen für die Netzwerkinfrastruktur mit sich, wobei Skalierung die wichtigste ist. Bei einem groß angelegten Einsatz von IoT-Geräten müssen die von jedem IoT-Gerät generierten Daten schnell analysiert werden. Um die Skalierungsanforderungen und die effiziente Nutzung der Ressourcen zu erfüllen, muss die Belastung des Brokerpools gleichmäßig verteilt werden. Mit Unterstützung des MQTT-Protokolls können Sie die NetScaler Appliance in IoT-Bereitstellungen verwenden, um den MQTT-Datenverkehr auszugleichen.

Die folgende Abbildung zeigt die MQTT-Architektur, die eine NetScaler Appliance verwendet, um den Lastausgleich des MQTT-Datenverkehrs zu verwenden.



Eine IoT-Bereitstellung mit dem MQTT-Protokoll besteht aus den folgenden Komponenten:

- **MQTT-Broker.** Ein Server, der alle Nachrichten von den Clients empfängt und die Nachrichten dann an die entsprechenden Zielclients weiterleitet. Der Broker ist dafür verantwortlich, alle Nachrichten zu empfangen, die Nachrichten zu filtern, festzustellen, wer jede Nachricht abonniert hat, und die Nachricht an diese abonnierten Clients zu senden. Der Broker ist der zentrale Knotenpunkt, über den jede Nachricht weitergeleitet werden muss.
- **MQTT-Client.** Jedes Gerät, von einem Mikrocontroller bis hin zu einem vollwertigen Server, auf dem eine MQTT-Bibliothek ausgeführt wird und über ein Netzwerk mit einem MQTT-Broker verbunden ist. Sowohl Herausgeber als auch Abonnenten sind MQTT-Kunden. Die Labels Herausgeber und Abonnenten geben an, ob der Kunde Nachrichten veröffentlicht oder den Empfang von Nachrichten abonniert hat.
- **MQTT-Loadbalancer.** Die NetScaler Appliance ist mit einem virtuellen MQTT-Lastausgleichsserver konfiguriert, um den Lastausgleich des MQTT-Datenverkehrs zu erstellen.

In einer typischen IoT-Bereitstellung verwaltet der Broker (Servercluster) die Gruppe der IoT-Geräte (IoT-Clients). Die Last der NetScaler Appliance gleicht den MQTT-Verkehr an die Broker basierend auf verschiedenen Parametern wie Client-ID, Thema und Benutzername aus.

Load Balancing für MQTT-Traffic konfigurieren

Führen Sie die folgenden Konfigurationsaufgaben durch, damit die NetScaler-Appliance den MQTT-Verkehr ausgleichen kann:

1. Konfigurieren Sie MQTT/MQTT_TLS Dienste oder Dienstgruppen.
2. Konfigurieren Sie den virtuellen Lastausgleichsserver MQTT/MQTT_TLS.
3. Binden Sie die MQTT/MQTT_TLS-Dienste an den virtuellen MQTT/MQTT_TLS Load Balancing-Server.
4. Konfigurieren Sie den virtuellen MQTT/MQTT_TLS Content Switching-Server.
5. Konfigurieren Sie eine Aktion Content Switching, die den virtuellen Zielserver für den Lastausgleich angibt
6. Konfigurieren Sie eine Richtlinie für den Content Switching.
7. Binden Sie die Content Switching-Richtlinie an einen virtuellen Content Switching-Server, der bereits für die Weiterleitung an den bestimmten virtuellen Load-Balancing-Server konfiguriert ist.
8. Speichern Sie die Konfiguration.

So konfigurieren Sie den Lastenausgleich für MQTT-Verkehr mithilfe der CLI

Konfigurieren Sie MQTT/MQTT_TLS Dienste oder Dienstgruppen.

```
add service <name> <IP> <protocol> <port>
```



```
add servicegroup <ServiceGroupName> <Protocol>
bind servicegroup <serviceGroupName> <IP> <port>
<!--NeedCopy-->
```

Beispiel:

```
add service srvc1 10.106.163.3 MQTT 1883
add servicegroup srvcg1 MQTT
bind servicegroup srvcg1 10.106.163.3 1883
<!--NeedCopy-->
```

Konfigurieren Sie den virtuellen Lastausgleichsserver MQTT/MQTT_TLS.

```
add lb vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver lb1 MQTT 10.106.163.9 1883
<!--NeedCopy-->
```

Binden Sie die MQTT/MQTT_TLS-Dienste oder -Dienstgruppen an den virtuellen MQTT-Load-Balancing-Server.

```
bind lb vserver <name> <serviceName>
bind lb vserver <name> <servicegroupName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb1 srvc1
bind lb vserver lb1 srvcg1
<!--NeedCopy-->
```

Konfigurieren Sie den virtuellen MQTT/MQTT_TLS Content Switching-Server.

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver cs1 MQTT 10.106.163.13 1883
<!--NeedCopy-->
```

Konfigurieren Sie eine Aktion Content Switching, die den virtuellen Zielserver für den Lastausgleich angibt.


```
add cs action <name> -targetLBVserver <string> [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add cs action act1 -targetlbvserver lbv1
<!--NeedCopy-->
```

Konfigurieren Sie eine Richtlinie für den Content Switching.

```
add cs policy <policyName> [-url <string> | -rule <expression>] -
    action <actName>
<!--NeedCopy-->
```

Beispiel:

```
add cs policy cspol1  -rule   "MQTT.COMMAND.EQ(CONNECT) && MQTT.CONNECT
    .FLAGS.QOS.eq(2)"  -action act1
<!--NeedCopy-->
```

Binden Sie die Content Switching-Richtlinie an einen virtuellen Content Switching-Server, der bereits für die Weiterleitung an den bestimmten virtuellen Load-Balancing-Server konfiguriert ist.

```
bind cs vserver <virtualServerName> -policyName <policyName> -priority
    <positiveInteger>
<!--NeedCopy-->
```

Beispiel:

```
bind cs vserver cs1  - policyName cspol1 -priority 20
<!--NeedCopy-->
```

Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

So konfigurieren Sie den Lastenausgleich für MQTT-Traffic mithilfe der GUI

1. **Navigieren Sie zu**Traffic Management**>**Load Balancing**>**Virtuelle Server**und erstellen Sie einen virtuellen Lastausgleichsserver vom Typ**MQTT oder MQTT_TLS**.**
2. Erstellen Sie einen Dienst oder eine Dienstgruppe vom Typ MQTT.
3. Binden Sie den Dienst an den virtuellen MQTT-Server.
4. Klicken Sie auf **Speichern**.

Längenbeschränkung für MQTT-Nachrichten

Die NetScaler-Appliance behandelt die Nachrichten mit einer Nachrichtenlänge von mehr als 65536 Byte als Jumbo-Pakete und verwirft sie standardmäßig. Der Parameter `dropmqttjumbomessage` lb entscheidet, ob die Jumbo-Pakete verarbeitet werden sollen oder nicht. Dieser Parameter ist standardmäßig auf **YES**gesetzt, was bedeutet, dass die Jumbo-MQTT-Pakete standardmäßig verworfen werden. Wenn dieser Parameter auf **NEIN**gesetzt ist, verarbeitet die ADC-Appliance sogar Pakete mit einer Nachrichtenlänge von mehr als 65536 Byte.

So konfigurieren Sie die ADC-Appliance für die Verarbeitung von Jumbo-Paketen mithilfe der CLI:

```
Set lb parameter  -dropMqttJumboMessage [YES | NO]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter  -dropMqttJumboMessage no
<!--NeedCopy-->
```

Load Balancing-Konfiguration vor einem Ausfall schützen

May 11, 2023

Wenn ein virtueller Lastausgleichsserver ausfällt oder wenn der virtuelle Server nicht übermäßigen Datenverkehr verarbeiten kann, kann das Lastausgleichs-Setup fehlschlagen. Sie können Ihr Load Balancing-Setup vor einem Ausfall schützen, indem Sie

- die NetScaler Appliance, um überschüssigen Datenverkehr auf eine alternative URL umzuleiten,
- einem virtuellen Backup-Lastausgleichsserver und
- ein stateful Verbindungs-Failover.

Clientanforderungen an eine alternative URL umleiten

August 19, 2021

Sie können Anfragen an eine alternative URL umleiten, indem Sie eine HTTP 302-Weiterleitung verwenden, wenn ein virtueller Lastausgleichsserver vom Typ HTTP oder HTTPS HERUNTERGEHT oder deaktiviert ist. Die alternative URL kann Informationen über den Status des Servers liefern. Die konfigurierte Umleitungs-URL wird im Standort-Header der HTTP-Antwort angegeben. Die genaue URL, die in der Antwort angegeben wird, hängt von den folgenden Konfigurationsoptionen ab:

- Wenn die konfigurierte Umleitungs-URL nur den Domänennamen enthält, wie z. B. http://www.sample1.example.com, hängt die in der HTTP-Antwort angegebene Umleitungs-URL den Uniform Resource Identifier (URI) an. Sie wird in der HTTP-Anforderung an den konfigurierten Domänennamen angegeben. Wenn die Anforderung beispielsweise den http://www.sample2.example.com/images/site_nav.png GET-Header enthält, gibt der Standort-Header in der Umleitungsantwort den Speicherort an: http://www.sample1.example.com/images/site_nav.png Header.

  > **Hinweis**
  >
  > Die Domainnamen in der Anfrage und Antwort können abweichen. In diesem Artikel werden die beiden Domänen als sample1.example.com und sample2.example.com bezeichnet, um das Konzept zu erläutern.

- Wenn die konfigurierte Umleitungs-URL einen vollständigen Pfad enthält, gibt die Umleitungsantwort die vollständig konfigurierte URL an, unabhängig von der URI in der Anfrage. Zum Beispiel sind die folgenden URLs:
  - Angeforderte URL - http://www.redirect.com/en/index.html
  - Umleitungs-URL - http://www.redirect.com/en/site_down.html

In der folgenden Tabelle sind die vorherigen Konfigurationsoptionen aufgeführt:

Konfigurierte Umleitungs-URL	URL in HTTP-Anfrage	Header in HTTP-Antwort
http://www.sample1.example.com	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/index.html
http://www.sample1.example.com/en/error.html	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/error.html

> **Hinweis:**
>
> - Bei der Konfiguration einer http://example.com Umleitungs-URL entspricht die URL nicht mit der http://example.com/ URL, da diese den vollständigen Pfad zum Webroot-Pfad /enthält.
> - Wenn ein virtueller Lastausgleichsserver sowohl mit einem virtuellen Backupserver als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backupserver Vorrang vor der Weiterleitungs-URL. Eine Umleitung wird nur verwendet, wenn sowohl der primäre als auch der virtuelle Backup-Server DOWN sind.

So konfigurieren Sie einen virtuellen Server für die Umleitung der Clientanforderung an eine URL mit der CLI

1. Erstellen Sie einen virtuellen Lastausgleichsserver.

   ```
   set lb vserver -redirect url
   ```

2. Stellen Sie sicher, dass die Option “URL umleiten” wie erwartet funktioniert. Deaktivieren Sie den virtuellen Server.

   ```
   disable vserver <vserver_name>
   ```

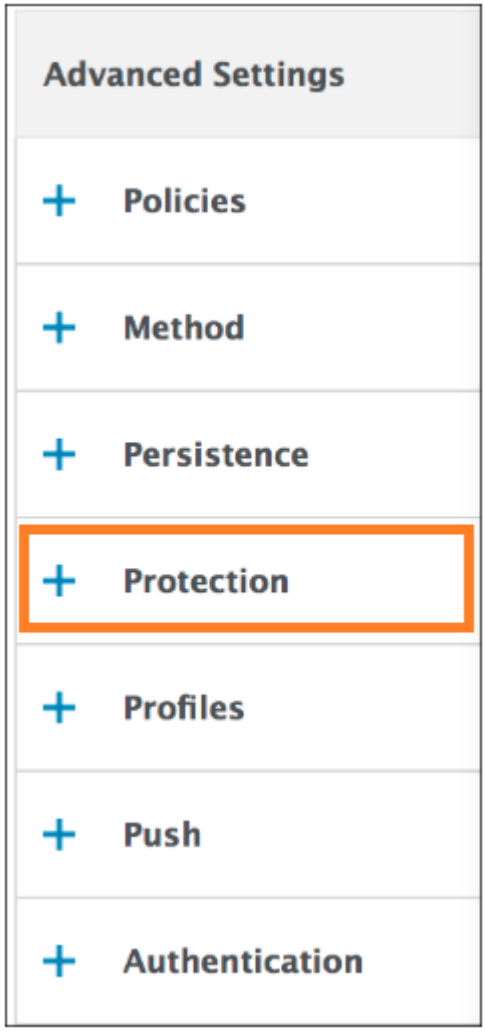
3. Greifen Sie von einem Webbrowser aus auf die Website-URL zu, um zu überprüfen, ob die Anfrage wie erwartet umgeleitet wird. Möglicherweise müssen Sie den Webbrowser-Cache löschen und eine neue Verbindung herstellen, bevor Sie auf die Website zugreifen.

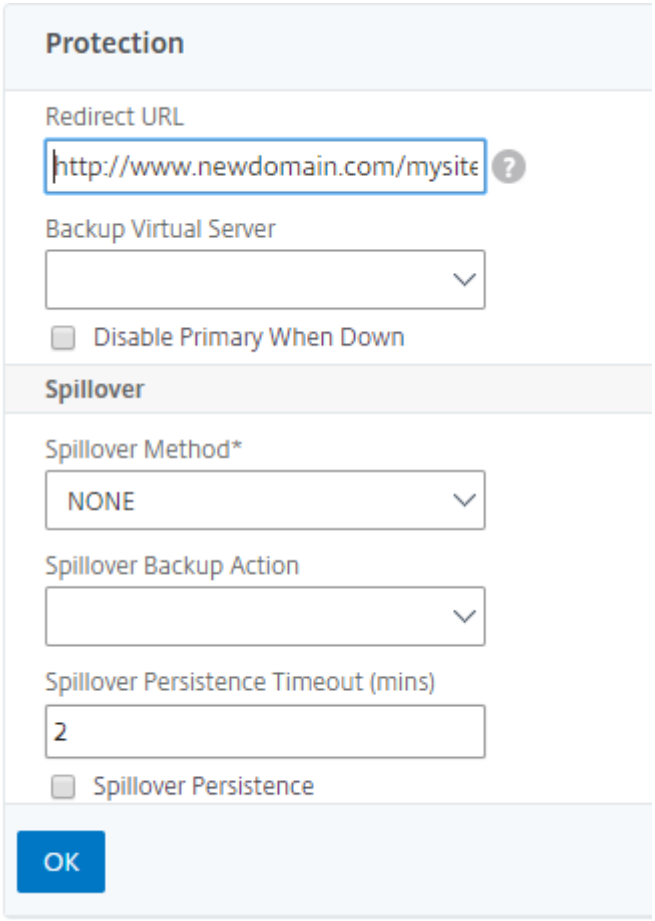
4. Aktivieren Sie den virtuellen Server.

   ```
   enable vserver <vserver_name>
   ```

So konfigurieren Sie einen virtuellen Server für die Umleitung der Clientanforderung an eine URL mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf Hinzufügen, um einen neuen virtuellen Server **hinzuzufügen**.
3. Um einen vorhandenen virtuellen Server zu bearbeiten, wählen Sie den virtuellen Server aus der Liste aus und klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf der Registerkarte **Erweiterte Einstellungen** auf **Schutz**. Geben Sie im Feld **Umleitungs-URL** die Umleitungs-URL ein (z. B. http://www.newdomain.com/mysite/maintenance).





5. Klicken Sie auf **OK**.

Virtuellen Backup-Load-Balancing-Server konfigurieren

June 19, 2023

Sie können die NetScaler Appliance so konfigurieren, dass Anfragen an einen virtuellen Backupserver geleitet werden, wenn der virtuelle Server für den primären Lastausgleich heruntergefahren oder nicht verfügbar ist. Der virtuelle Backup-Server ist ein Proxy und ist für den Client transparent. Die Appliance kann auch eine Benachrichtigung über den Standortausfall an den Client senden.

Der virtuelle Backup-Load-Balancing-Server sorgt für minimale Unterbrechungen, wenn die primäre Methode nicht verfügbar ist, und erhöht so die Verfügbarkeit und Zuverlässigkeit der Load-Balancing-Umgebung.

> Hinweis:
>
> Der virtuelle Backup-Server verarbeitet weiterhin die vorhandenen Verbindungen, auch nach-

> dem der primäre virtuelle Server gelöscht oder deaktiviert wurde.

Sie können einen virtuellen Backup-Load Balancing Server konfigurieren, wenn Sie ihn erstellen, oder Sie können die optionalen Parameter eines vorhandenen virtuellen Servers ändern. Sie können auch einen virtuellen Backup-Server für einen vorhandenen virtuellen Backup-Server konfigurieren und so kaskadierende virtuelle Backup-Server erstellen. Die maximale Tiefe von kaskadierenden virtuellen Backup-Servern beträgt 10.

Wenn Sie mehrere virtuelle Server haben, die sich mit zwei Servern verbinden, haben Sie die Wahl, was passiert, wenn der primäre virtuelle Server AUSFÄLLT und dann wieder hochfährt. Das Standardverhalten besteht darin, dass der primäre virtuelle Server seine Rolle als primär fortsetzt. Sie können den virtuellen Backup-Server jedoch so konfigurieren, dass er bei Übernahme die Kontrolle behält. Sie können beispielsweise die Updates auf dem virtuellen Backup-Server mit dem primären virtuellen Server synchronisieren und dann den ursprünglichen Primärserver manuell zwingen, seine Rolle fortzusetzen. In diesem Fall können Sie festlegen, dass der virtuelle Backupserver die Kontrolle behält, wenn der primäre virtuelle Server herunterfährt und dann wieder hochfährt.

Sie können eine Umleitungs-URL auf dem primären virtuellen Load-Balancing-Server als Fallback konfigurieren, wenn sowohl der primäre als auch der virtuelle Backup-Server AUSGEFALLEN sind oder ihren Schwellenwert für die Bearbeitung von Anfragen erreicht haben. Wenn Dienste, die an virtuelle Server gebunden sind, AUSSER BETRIEB sind, verwendet die Appliance die Umleitungs-URL.

Die **Backup-LB-Methode** wird angezeigt, wenn die folgenden Load-Balancing-Methoden ausgewählt sind:

- Geringste Verbindung
- Geringste Reaktionszeit
- Round Robin
- Geringste Bandbreite
- Wenigste Pakete
- Benutzerdefiniertes Laden
- Geringste Anfrage
- Statische Nähe

> Hinweis
>
> Wenn ein virtueller Load-Balancing-Server sowohl mit einem virtuellen Backup-Server als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backup-Server Vorrang vor der Umleitungs-URL. Eine Weiterleitung wird nur verwendet, wenn die virtuellen Primär- und Backup-Server ausgefallen sind.

So richten Sie einen virtuellen Backup-Server mithilfe der CLI ein

Geben Sie in der Befehlszeile Folgendes ein:


```
set lb vserver <vServerName> -backupVserver <BackupVServerName> [-
    disablePrimaryOnDown]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -backupVserver Vserver-LB-2 -
    disablePrimaryOnDown
<!--NeedCopy-->
```

So richten Sie mithilfe der GUI einen virtuellen Backup-Server ein

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie in den Erweiterten Einstellungen auf **Schutz**und wählen Sie einen virtuellen Backup-Server aus.
3. Wenn Sie möchten, dass der virtuelle Backup-Server die Kontrolle behält, bis Sie den primären virtuellen Server manuell aktivieren, auch wenn der primäre virtuelle Server wieder hochgefahren wird, wählen Sie **Primär deaktivieren, wenn er ausgefallen**ist.

> **Hinweis:** Ab NetScaler Version 12.1 Build 51.xx zeigt die GUI den effektiven Status dieses Servers an und gibt an, ob das Backup aktiv ist oder nicht.
>
> Der effektive Status des aktuellen Servers kann einer der folgenden sein:
>
> - **UP** — Zeigt an, dass der Server aktiv ist
> - **DOWN** — Zeigt an, dass der Server DOWN ist
> - **UP (Backup Active)** — Zeigt an, dass entweder der primäre oder der sekundäre virtuelle Server aktiv ist und der Datenverkehr an den virtuellen Backup-Server weitergeleitet wird.
> - **DOWN (Backup Active)** — Zeigt an, dass sowohl der primäre als auch der virtuelle Backup-Server ausgefallen sind und der Datenverkehr an den virtuellen Backup-Server weitergeleitet wird.
>
> Wenn die Option **Primär deaktivieren bei Ausfall** auf dem primären virtuellen Server aktiviert ist und der Primärserver AUSFÄLLT und wieder AKTIV ist, wird der Datenverkehr weiterhin vom virtuellen Backup-Server bereitgestellt, bis der primäre virtuelle Server explizit erneut aktiviert wird. Sie können den `enable lb vserver <vserver_name>` Befehlsbefehl verwenden, um den primären virtuellen Server erneut zu aktivieren.

Spillover konfigurieren

May 11, 2023

Eine Spillover-Konfiguration auf der Appliance besteht aus einem primären virtuellen Server, der mit einer Spillover-Methode konfiguriert ist, einem Spillover-Schwellenwert und einem virtuellen Backup-Server. Virtuelle Backup-Server können auch für Spillover konfiguriert werden, wodurch eine Kette von virtuellen Backup-Servern entsteht.

Die Spillover-Methode gibt den Betriebszustand an, auf dem Sie Ihre Spillover-Konfiguration basieren möchten (z. B. die Anzahl der hergestellten Verbindungen, die Bandbreite oder der kombinierte Zustand der Serverfarm). Wenn eine neue Verbindung hergestellt wird, überprüft die Appliance, ob der primäre virtuelle Server aktiv ist, und vergleicht den Betriebszustand mit dem konfigurierten Spillover-Schwellenwert. Wenn der Schwellenwert erreicht ist, leitet die Spillover-Funktion neue Verbindungen an den ersten verfügbaren virtuellen Server in der Backup-Kette um. Der virtuelle Backup-Server verwaltet die empfangenen Verbindungen, bis die Last auf dem Primärserver den Schwellenwert unterschreitet.

Wenn Sie die Spillover-Persistenz konfigurieren, verarbeitet der virtuelle Backup-Server die empfangenen Verbindungen weiter, auch wenn die Last auf dem Primärserver unter den Schwellenwert fällt. Wenn Sie die Spillover-Persistenz und ein Zeitlimit für die Spillover-Persistenz konfigurieren, verarbeitet der virtuelle Backup-Server Verbindungen nur für den angegebenen Zeitraum, nachdem die Last auf dem Primärserver unter den Schwellenwert gefallen ist.

Hinweis: Normalerweise wird Spillover ausgelöst, wenn der der Spillover-Methode zugeordnete Wert den Schwellenwert überschreitet (z. B. die Anzahl der Verbindungen). Bei der Spillover-Methode zur Serverintegrität wird der Spillover jedoch ausgelöst, wenn der Zustand der Serverfarm unter den Schwellenwert fällt.

Sie können Spillover auf eine der folgenden Arten konfigurieren:

- Geben Sie eine vordefinierte Spillover-Methode an. Es stehen vier vordefinierte Methoden zur Verfügung, die allgemeine Spillover-Anforderungen erfüllen.
- Konfigurieren Sie den richtlinienbasierten Spillover. Bei richtlinienbasiertem Spillover verwenden Sie eine NetScaler-Regel, um die Bedingungen festzulegen, unter denen ein Spillover stattfindet. NetScaler-Regeln geben Ihnen die Flexibilität, Spillover für verschiedene Betriebsbedingungen zu konfigurieren.

Verwenden Sie richtlinienbasiertes Spillover, wenn eine vordefinierte Methode Ihre Anforderungen nicht erfüllt. Wenn Sie beide für einen primären virtuellen Server konfigurieren, hat die richtlinienbasierte Spillover-Konfiguration Vorrang vor der vordefinierten Methode.

Zunächst erstellen Sie den primären virtuellen Server und die virtuellen Server, die Sie für die Backup-Kette benötigen. Sie richten die Backup-Kette ein, indem Sie einen virtuellen Server als Backup für

den primären Server angeben (d. h. Sie erstellen einen sekundären virtuellen Server), einen virtuellen Server als Backup für den sekundären (d. h. Sie erstellen einen tertiären virtuellen Server) usw. Anschließend konfigurieren Sie Spillover, indem Sie entweder eine vordefinierte Spillover-Methode angeben oder Spillover-Richtlinien erstellen und binden.

Anweisungen zum Zuweisen eines virtuellen Servers als Backup für einen anderen virtuellen Server finden Sie unter Konfigurieren eines virtuellen Backup-Lastausgleichsservers.

Konfigurieren einer vordefinierten Spillover-Methode

Vordefinierte Spillover-Methoden erfüllen einige der gängigsten Spillover-Anforderungen. Um eine der vordefinierten Spillover-Methoden zu verwenden, konfigurieren Sie die Spillover-Parameter auf dem primären virtuellen Server. Um eine Kette von virtuellen Backup-Servern zu erstellen, konfigurieren Sie auch Spillover-Parameter auf virtuellen Backup-Servern.

Wenn die virtuellen Backup-Server ihre eigenen Schwellenwerte erreichen und der Diensttyp TCP ist, sendet die NetScaler-Appliance den Clients einen TCP-Reset. Bei den Diensttypen HTTP, SSL und RTSP werden neue Anfragen an die Umleitungs-URL umgeleitet, die für den primären virtuellen Server konfiguriert ist. Eine Umleitungs-URL kann nur für virtuelle HTTP-, SSL- und RTSP-Server angegeben werden. Wenn keine Umleitungs-URL konfiguriert ist, sendet die NetScaler-Appliance den Clients einen TCP-Reset (wenn der virtuelle Server vom Typ TCP ist) oder eine HTTP 503-Antwort (wenn der virtuelle Server vom Typ HTTP oder SSL ist).

Hinweis: Bei virtuellen RTSP-Servern verwendet die NetScaler-Appliance nur Datenverbindungen für Spillover. Wenn der virtuelle Backup-RTSP-Server nicht verfügbar ist, werden die Anfragen an eine RTSP-URL umgeleitet und eine RTSP-Umleitungsnachricht wird an den Client gesendet.

So konfigurieren Sie eine vordefinierte Spillover-Methode für einen virtuellen Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <vServerName> -soMethod <spillOverType> -soThreshold <
    positiveInteger> -soPersistence ENABLED -soPersistenceTimeout <
    positiveInteger>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver Vserver-LB-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```


So konfigurieren Sie eine vordefinierte Spillover-Methode für einen virtuellen Server mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie in den Erweiterten Einstellungen auf **Schutz**und legen Sie die Spillover-Parameter fest.

Richtlinienbasiertes Spillover konfigurieren

Spillover-Richtlinien, die auf Regeln (Ausdrücke) basieren, ermöglichen es Ihnen, die Appliance für eine breitere Palette von Spillover-Szenarien zu konfigurieren. Beispielsweise können Sie den Spillover basierend auf der Reaktionszeit des virtuellen Servers oder basierend auf der Anzahl der Verbindungen in der Überspannungswarteschlange des virtuellen Servers konfigurieren.

Um richtlinienbasierte Spillover zu konfigurieren, erstellen Sie zunächst eine Spillover-Aktion. Anschließend wählen Sie den Ausdruck aus, den Sie in der Spillover-Richtlinie verwenden möchten, konfigurieren die Richtlinie und verknüpfen die Aktion damit. Schließlich binden Sie die Spillover-Richtlinie an einen virtuellen Server mit Load Balancing, Content Switching oder globalem Serverlastenausgleich. Sie können mehrere Spillover-Richtlinien mit Prioritätsnummern an einen virtuellen Server binden. Die Appliance bewertet die Spillover-Richtlinien in aufsteigender Reihenfolge der Prioritätsnummern und führt die Aktion aus, die mit der letzten Richtlinie verknüpft ist, deren Bewertung TRUE ergibt.

Ein virtueller Server kann auch eine Backup-Aktion haben. Die Sicherungsaktion wird ausgeführt, wenn der virtuelle Server nicht über einen oder mehrere virtuelle Backup-Server verfügt oder wenn alle virtuellen Backup-Server AUSFALLEN, deaktiviert sind oder ihre eigenen Spillover-Grenzwerte erreicht haben.

Wenn eine Spillover-Richtlinie zu einer UNDEF-Bedingung führt (eine Ausnahme, die ausgelöst wird, wenn das Ergebnis der Richtlinienbewertung undefiniert ist), wird eine UNDEF-Aktion ausgeführt. Die UNDEF-Aktion ist immer ACCEPT. Sie können keine UNDEF-Aktion Ihrer Wahl angeben.

Konfiguration einer Spillover-Aktion

Eine Spillover-Aktion wird ausgeführt, wenn die Spillover-Richtlinie, mit der sie verknüpft ist, als TRUE bewertet wird. Derzeit ist SPILLOVER die einzige unterstützte Spillover-Aktion.

So konfigurieren Sie den richtlinienbasierten Spillover mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Spillover-Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:


```
add spillover action <name> -action SPILLOVER

show spillover action <name>
<!--NeedCopy-->
```

Beispiel

```
add spillover action mySoAction -action SPILLOVER
Done
<!--NeedCopy-->
```

```
show spillover action mySoAction
1) Name: mySoAction Action: SPILLOVER
Done
<!--NeedCopy-->
```

Auswahl eines Ausdrucks für die Spillover-Richtlinie

Im Richtlinienausdruck können Sie jeden auf einem virtuellen Server basierenden Ausdruck verwenden, der einen booleschen Wert zurückgibt. Sie können beispielsweise einen der folgenden Ausdrücke verwenden:

```
SYS.VSERVER("vserver").RESPTIME.GT(<int>)
SYS.VSERVER("vserver").STATE.EQ( “ <string>” ), and
SYS.VSERVER("vserver").THROUGHPUT.LT    (<int>)
<!--NeedCopy-->
```

Zusätzlich zu den vorhandenen Funktionen wie RESPTIME, STATE und THROUGHPUT können Sie die folgenden virtuellen serverbasierten Funktionen verwenden, die mit dieser Funktion eingeführt wurden:

`Averagesurgecount`

Gibt die durchschnittliche Anzahl von Anforderungen in den Überspannungswarteschlangen aktiver Dienste zurück. Gibt 0 (Null) zurück, wenn keine aktiven Dienste vorhanden sind. Löst eine UNDEF-Bedingung aus, wenn sie mit einem virtuellen Content Switching- oder globalen Server Load Balancing-Server verwendet wird.

`Activeservices`

Gibt die Anzahl der aktiven Dienste zurück. Löst eine UNDEF-Bedingung aus, wenn sie mit einem virtuellen Content Switching- oder globalen Server Load Balancing-Server verwendet wird.

`Activetransactions`

Gibt den Wert des Leistungsindikators auf Virtual-Serverebene für aktuelle aktive Transaktionen zurück.

ist das dynamische Limit erreicht

Gibt den booleschen Wert TRUE zurück, wenn die Anzahl der Verbindungen, die der virtuelle Server verwaltet, dem dynamisch berechneten Schwellenwert entspricht. Der dynamische Schwellenwert ist die Summe der maximalen Client-Einstellungen (Max Clients) der gebundenen Dienste, die aktiv sind.

Sie können einen Richtlinienausdruck verwenden, um jede der vordefinierten Spillover-Methoden zu implementieren. In der folgenden Tabelle werden die vordefinierten Spillover-Methoden den Ausdrücken zugeordnet, mit denen Sie sie implementieren können:

Tabelle 1. Umwandlung vordefinierter Spillover-Methoden in Richtlinienausdrücke

Vordefinierte Spillover-Methode	Entsprechender Ausdruck
VERBINDUNG	SYS.VSERVER („<vserver-name>„) .CONNECTIONS, wird zusammen mit der Arithmetikfunktion GT (int) verwendet.
BANDBREITE	SYS.VSERVER („<vserver-name>„) .DURCHSATZ, wird zusammen mit der Arithmetikfunktion GT (int) verwendet.
HEALTH	SYS.VSERVER („<vserver-name>„) .HEALTH, wird zusammen mit der Arithmetikfunktion LT (int) verwendet.
DYNAMICCONNECTION	SYS.VSERVER („<vserver-name>”) .IS_DYNAMIC_LIMIT_REACHED **Hinweis**: Wenn Sie einen richtlinienbasierten Spillover mit der Funktion IS_DYNAMIC_LIMIT_REACHED implementieren, müssen Sie auch die vordefinierte DYNAMICCONNECTION-Methode für den virtuellen Server konfigurieren, damit die für Spillover erforderlichen Statistiken funktionieren werden gesammelt.

Konfigurieren einer Spillover-Richtlinie

Eine Spillover-Richtlinie verwendet in der Regel einen booleschen Ausdruck, um die Bedingungen anzugeben, die erfüllt sein müssen, damit ein Spillover stattfindet.

So konfigurieren Sie eine Spillover-Richtlinie mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Spillover-Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
add spillover policy <name> -rule <expression> -action <string> [-
    comment <string>]

show spillover policy <name>
<!--NeedCopy-->
```

Beispiel

```
> add spillover policy mySoPolicy -rule SYS.VSERVER("v1").RESPTIME.GT
    (50) -action mySoAction -comment "Triggers spillover when the
    vserver's response time is greater than 50 ms."
Done

> show spillover policy mySoPolicy

1)  Name: mySoPolicy Rule: "SYS.VSERVER("v1").RESPTIME.GT(50)" Action:
    mySoAction Hits: 0 ActivePolicy: 0
Comment: "Triggers spillover when the vserver's response time is
    greater than 50 ms."
Done
>
<!--NeedCopy-->
```

Binden einer Spillover-Richtlinie an einen virtuellen Server

Sie können eine Spillover-Richtlinie an Load Balancing, Content Switching oder globalen Serverlastenausgleich (virtuelle Server) binden. Sie können mehrere Richtlinien an einen virtuellen Server binden, wobei Goto-Ausdrücke den Ablauf der Auswertung steuern.

So binden Sie eine Spillover-Richtlinie mithilfe der Befehlszeilenschnittstelle an einen virtuellen Server

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Spillover-Richtlinie an einen virtuellen Load Balancing-, Content Switching- oder globalen Serverlastenausgleichsserver zu binden, und überprüfen Sie die Konfiguration:

```
bind (lb | cs | gslb) vserver <name> -policyName <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]

show (lb | cs | gslb) vserver <name>
<!--NeedCopy-->
```

Beispiel

```
> bind lb vserver vserver1 -policyName mySoPolicy -priority 5
Done
> show lb vserver vserver1
vserver1 (2.2.2.12:80) - HTTP Type: ADDRESS
. . .

1)  Spillover Policy Name: mySoPolicy Priority: 5
GotoPriority Expression: END
Flowtype: REQUEST
Done
>
<!--NeedCopy-->
```

Konfiguration einer Backup-Aktion für ein Spillover-Ereignis

Eine Backup-Aktion gibt an, was zu tun ist, wenn der Spillover-Schwellenwert erreicht ist, aber ein oder mehrere virtuelle Backup-Server entweder nicht konfiguriert sind oder ausgefallen, deaktiviert sind oder ihre eigenen Schwellenwerte erreicht haben.

Hinweis: Für die vordefinierten Spillover-Methoden, die direkt auf dem virtuellen Server konfiguriert werden (als Werte des Parameters Spillover Method), ist die Backup-Aktion nicht konfigurierbar. Standardmäßig sendet die Appliance den Clients einen TCP-Reset (wenn der virtuelle Server vom Typ TCP ist) oder eine HTTP 503-Antwort (wenn der virtuelle Server vom Typ HTTP oder SSL ist).

Die Backup-Aktion ist auf dem virtuellen Server konfiguriert. Sie können den virtuellen Server so konfigurieren, dass er Anfragen akzeptiert (nachdem der in der Richtlinie angegebene Schwellenwert erreicht ist), Clients auf eine URL umleitet oder Anfragen einfach verwirft, noch bevor TCP- oder SSL-Verbindungen hergestellt werden, bis die Anzahl der Anfragen unter den Schwellenwert fällt. Daher werden weniger Speicherressourcen genutzt, da die Verbindungen zurückgesetzt werden, noch bevor Datenstrukturen zugewiesen werden.

So konfigurieren Sie eine Backup-Aktion für Spillover mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Backupaktion zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -soBackupAction <soBackupAction>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vs1 -soBackupAction REDIRECT -redirectURL `http://www.
   mysite.com/maintenance`
Done
> show lb vserver vs1
vs1 (10.102.29.76:80) - HTTP Type: ADDRESS
State: UP
. . .
Redirect URL: `http://www.mysite.com/maintenance`
. . .
Done
<!--NeedCopy-->
```

So konfigurieren Sie eine Backupaktion für Spillover mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie in den Erweiterten Einstellungen auf **Schutz**und geben Sie dann eine Spillover-Backup-Aktion an.

Verbindungsfailover

May 11, 2023

Das Verbindungsfailover verhindert eine Unterbrechung des Zugriffs auf Anwendungen, die in einer verteilten Umgebung bereitgestellt werden. In einer NetScaler High Availability (HA) -Setup bezieht sich *Verbindungsfailover* (oder *Verbindungsspiegelung-CM*) darauf, eine etablierte TCP- oder UDP-Verbindung aktiv zu halten, wenn ein Failover auftritt. Die neue primäre NetScaler-Appliance verfügt über Informationen zu den Verbindungen, die vor dem Failover hergestellt wurden, und bedient diese Verbindungen weiterhin. Nach dem Failover bleibt der Client mit demselben physischen Server verbunden. Die neue primäre Appliance synchronisiert die Informationen mit der neuen sekundären

Appliance. Wenn der Parameter L2Conn gesetzt ist, werden Layer 2-Verbindungsparameter ebenfalls mit dem sekundären synchronisiert.

> Hinweis:
>
> Betrachten Sie ein HA-Setup, bei dem ein Client eine Sitzung mit dem primären Knoten einrichtet, der wiederum eine Sitzung mit dem Back-End-Server einrichtet. Wenn in diesem Zustand ein Failover ausgelöst wird, werden die Pakete, die von den vorhandenen Client- und Serverknoten auf einem neuen Primärgerät empfangen werden, als veraltete Pakete behandelt, und die Client- und Serververbindungen werden zurückgesetzt. Wenn ein zustandsloses Verbindungsfailover aktiviert ist (USIP ist ON), werden die Verbindungen nach dem Failover nicht zurückgesetzt, wenn Sie Pakete von Client- oder Serverknoten erhalten. Stattdessen werden die Client- und Serververbindungen dynamisch erstellt.

Sie können das Verbindungs-Failover entweder im zustandslosen oder im statusbehafteten Modus einrichten. Im Failover-Modus für statuslose Verbindungen tauschen die HA-Knoten keine Informationen über die Verbindungen aus, bei denen ein Failover durchgeführt wurde. Diese Methode hat keinen Laufzeit-Overhead.

Im statusbehafteten Verbindungsfailover-Modus synchronisiert das primäre Gerät die Daten der Failover-Verbindungen mit dem neuen sekundären Gerät.

Verbindungs-Failover ist hilfreich, wenn Ihre Bereitstellung über langlebige Verbindungen verfügt. Wenn Sie beispielsweise eine große Datei über FTP herunterladen und während des Downloads ein Failover auftritt, wird die Verbindung unterbrochen, und der Download wird abgebrochen. Wenn Sie das Verbindungs-Failover jedoch im Stateful-Modus konfigurieren, wird der Download auch nach dem Failover fortgesetzt.

Funktionsweise des Verbindungs-Failovers auf NetScaler-Appliances

In einem zustandslosen Verbindungsfailover versucht die neue primäre Appliance, den Paketfluss gemäß den Informationen, die in den empfangenen Paketen enthalten sind, neu zu erstellen.

Im statusbehafteten Failover sendet die primäre Appliance Nachrichten an die sekundäre Appliance, um aktuelle Informationen über die gespiegelten Verbindungen beizubehalten. Die sekundäre Appliance verwaltet die Daten, die sich auf die Pakete beziehen, verwendet sie jedoch nur im Falle eines Failovers. Wenn ein Failover auftritt, verwendet die neue primäre (alte sekundäre) Appliance die gespeicherten Daten über die gespiegelten Verbindungen und akzeptiert Datenverkehr. Während der Übergangsphase können der Client und der Server eine kurze Unterbrechung und erneute Übertragung erfahren.

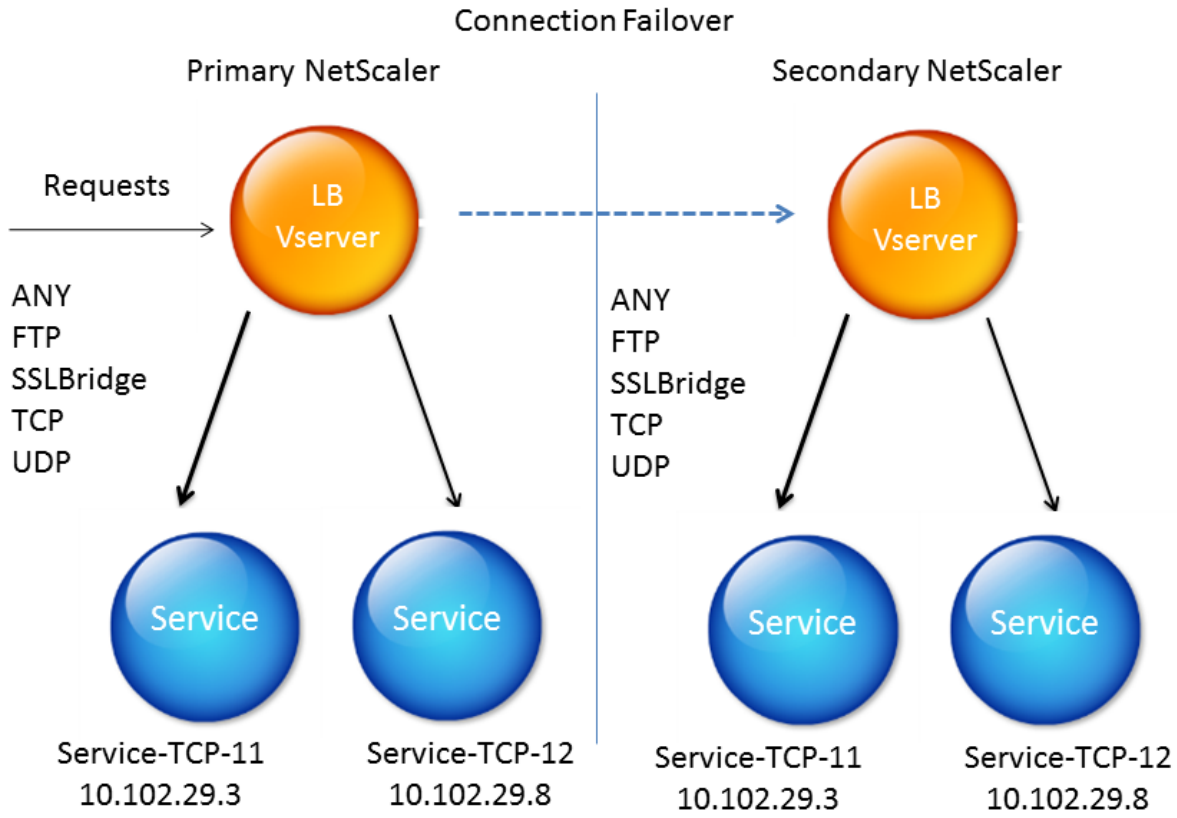
Hinweis:

Stellen Sie sicher, dass sich die primäre Appliance auf der sekundären Appliance selbst autorisieren kann. Um die korrekte Konfiguration der Kennwörter zu überprüfen, verwenden Sie den Befehl show

`rpcnode` von der Befehlszeile aus oder verwenden Sie die RPC-Option des Menüs **Netzwerk** in der GUI.

Eine grundlegende HA-Konfiguration mit Verbindungs-Failover enthält die in der folgenden Abbildung gezeigten Entitäten.

Abbildung 1. Verbindungs-Failover-Entitätsdiagramm



Hinweis

Verbindungs-Failover wird nach einem der folgenden Ereignisse nicht unterstützt:

```
- An upgrade to a later release.
- An upgrade to a later build within the same release, if the new
    build uses a different HA version.
```

Unterstützte Einrichtung

Das Verbindungsfailover kann nur auf virtuellen Servern mit Lastausgleich konfiguriert werden. Es kann nicht auf virtuellen Content Switching-Servern konfiguriert werden. Wenn Sie das Verbindungs-Failover auf virtuellen Lastenausgleichs-Servern aktivieren, die an einen virtuellen Content Switching-

Server angeschlossen sind, funktioniert das Verbindungs-Failover nicht, da die virtuellen Server mit Lastenausgleich den Datenverkehr zunächst nicht akzeptieren.

In der folgenden Tabelle wird das Setup beschrieben, das für Verbindungs-Failover unterstützt wird.

Tabelle 1. Verbindungsfailover — Unterstütztes Setup

Einstellung	Zustandslos	Zustandsvoll
Typ des Dienstes	ANY.	ANY, UDP, TCP, FTP, SSL_BRIDGE.
Load Balancing-Methoden	Alle für den Diensttyp ANY unterstützten Methoden. Wenn die Source IP-Persistenz jedoch nicht festgelegt ist, muss die Methode SRCIPSRCPORTHASH verwendet werden.	Alle Methoden, die für die unterstützten Diensttypen gelten.
Persistence-Typen	SOURCEIP-Beständigkeit.	Alle Typen, die für die unterstützten Servicetypen gelten, werden unterstützt.
USIP	Muss AN sein.	Keine Einschränkung. Es kann EIN oder AUS sein.
Service-Bindungen	Der Dienst kann nur an einen virtuellen Server gebunden werden.	Der Dienst kann an einen oder mehrere virtuelle Server gebunden sein.
Internet Protocol (IP) -Versionen	IPv4 und IPv6	IPV4 und IPv6
Unterstützung für Redundanz	Clustering und Hochverfügbarkeit	Hohe Verfügbarkeit
INC-Modus	Nicht unterstützt	Wird unterstützt, wenn der Diensttyp des virtuellen Servers ANY ist, der Modus DSR (MAC, IPTUNNEL, TOS) ist und USIP für die an den virtuellen Server gebundenen Dienste aktiviert ist.

> **Hinweis:**
>
> Stateful-Verbindungsfailover wird nur für verbindungsbasierte Switching-Dienste unterstützt, z. B. TCP. Da HTTP anforderungsbasiertes Switching verwendet, unterstützt es kein Verbindungs-Failover. In SSL werden die vorhandenen Verbindungen nach dem Failover zurückgesetzt.

Features, die von Verbindungs-Failover betroffen sind

In der folgenden Tabelle sind die Funktionen aufgeführt, die von der Konfiguration des Verbindungsfailovers betroffen sind.

Tabelle 2. Wie sich das Verbindungsfailover auf die NetScaler-Funktionen auswirkt

Feature	Auswirkungen des Verbindungs-Failovers
SYN-Schutz	Wenn bei jeder Verbindung ein Failover auftritt, nachdem die Appliance SYN-ACK ausgegeben hat, aber bevor sie das endgültige ACK erhält, wird die Verbindung vom Verbindungs-Failover nicht unterstützt. Der Client muss die Anforderung erneut ausstellen, um die Verbindung herzustellen.
Überlastungsschutz	Wenn das Failover auftritt, bevor eine Verbindung mit dem Server hergestellt wird, versucht die neue primäre Appliance, die Verbindung mit dem Server herzustellen. Es überträgt auch alle Pakete, die während des Überlastungsschutzes aufbewahrt werden.
Zugriff nicht verfügbar	Wenn diese Option aktiviert ist, hat die Access-Down-Funktionalität Vorrang vor dem Verbindungs-Failover.
Anwendungs-Firewall	Die Funktion der Anwendungs-Firewall wird nicht unterstützt.

Feature	Auswirkungen des Verbindungs-Failovers
INC	Die unabhängige Netzwerkkonfiguration (INC) wird im Hochverfügbarkeitsmodus nur unterstützt, wenn der Diensttyp des virtuellen Servers ANY ist, der Modus DSR (MAC, IPTUNNEL, TOS) ist und USIP für die an den virtuellen Server gebundenen Dienste aktiviert ist. In allen anderen Szenarien wird INC nicht unterstützt.
TCP-Pufferung	Die TCP-Pufferung ist mit der Verbindungsspiegelung nicht kompatibel.
Nach Antwort schließen	Nach dem Failover werden die NATPCBs bei der Antwort möglicherweise nicht geschlossen.

So konfigurieren Sie das Verbindungs-Failover mit der GUI

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**. Öffnen Sie den virtuellen Server, klicken Sie in den **Erweiterten Einstellungen**auf **Schutz**und wählen Sie **Verbindungsfailover** als **zustandsbehaftet**aus.

So konfigurieren Sie das Verbindungsfailover mithilfe von CLI

An der Eingabeaufforderung:

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -connFailover stateful
Done
<!--NeedCopy-->
```

Wenn das Verbindungs-Failover auf einem virtuellen Server deaktiviert ist, werden die dem virtuellen Server zugewiesenen Ressourcen freigegeben.

So deaktivieren Sie das Verbindungsfailover mithilfe von CLI

An der Eingabeaufforderung:


```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -connFailover disable
Done
<!--NeedCopy-->
```

So deaktivieren Sie das Verbindungs-Failover mit der GUI

Navigieren Sie zu **Traffic Management**> **Load Balancing**> **Virtuelle Server**. Öffnen Sie den virtuellen Server, wählen Sie **unter SchutzVerbindungsfailover** als Deaktiviert aus.

Surgewarteschlange leeren

May 11, 2023

Wenn ein physischer Server eine Flut von Anfragen erhält, reagiert er nur langsam auf die Clients, die gerade mit ihm verbunden sind, was die Benutzer unzufrieden und verärgert macht. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Die NetScaler Appliance bietet Funktionen wie Überspannungsschutz, der die Rate steuert, mit der neue Verbindungen zu einem Dienst hergestellt werden können, und so Überlastungen vermeiden.

Die Appliance verbindet Multiplexing zwischen Clients und physischen Servern. Wenn die Appliance eine Client-Anfrage für den Zugriff auf einen Dienst auf einem Server empfängt, sucht sie nach einer bereits bestehenden Verbindung zum Server, die frei ist. Wenn eine freie Verbindung gefunden wird, wird diese Verbindung verwendet, um eine virtuelle Verbindung zwischen dem Client und dem Server herzustellen. Wenn keine bestehende freie Verbindung gefunden wird, stellt die Appliance eine neue Verbindung mit dem Server her und stellt eine virtuelle Verbindung zwischen dem Client und dem Server her. Wenn die Appliance jedoch keine neue Verbindung mit dem Server herstellen kann, sendet sie die Clientanforderung an eine Überspannungswarteschlange. Wenn alle physischen Server, die an den virtuellen Load Balancing- oder Content-Switching-Server gebunden sind, die Obergrenze für Client-Verbindungen erreichen (maximaler Client-Wert, Überspannungsschutzschwelle oder maximale Kapazität des Dienstes), kann die Appliance keine Verbindung zu einem Server herstellen. Die Überspannungsschutzfunktion verwendet die Überspannungswarteschlange, um die Geschwindigkeit zu regulieren, mit der Verbindungen zu den physischen Servern geöffnet werden. Die Appliance verwaltet eine andere Überspannungswarteschlange für jeden Dienst, der an den virtuellen Server gebunden ist.

Die Länge einer Überspannungswarteschlange erhöht sich, wenn eine Anforderung gestellt wird, für die die Appliance keine Verbindung herstellen kann. Die Länge einer Überspannungswarteschlange nimmt unter einer der folgenden Bedingungen ab:

- Eine Anfrage in der Warteschlange wird an den Server gesendet.
- Eine Anfrage wird zeitüberschreitend und wird aus der Warteschlange entfernt.

Wenn die Überspannungswarteschlange für einen Dienst oder eine Dienstgruppe zu lang wird, sollten Sie sie möglicherweise leeren. Sie können die Überspannungswarteschlange eines bestimmten Dienstes oder einer bestimmten Dienstgruppe oder aller Dienste und Dienstgruppen, die an einen virtuellen Lastausgleichsserver gebunden sind, leeren. Das Leeren einer Überspannungswarteschlange wirkt sich nicht auf die bestehenden Verbindungen aus. Nur die Anfragen in der Überspannungswarteschlange werden gelöscht. Für diese Anfragen muss der Kunde eine neue Anfrage stellen.

Sie können auch die Surge-Queue eines virtuellen Content Switching-Servers leeren. Wenn ein virtueller Content Switching-Server einige Anfragen an einen bestimmten virtuellen Lastausgleichsserver weiterleitet und der virtuelle Lastausgleichsserver auch einige andere Anfragen empfängt, werden beim Leeren der Überspannungswarteschlange des virtuellen Content Switching-Servers nur die von diesem virtuellen Content Switching-Server empfangenen Anforderungen geleert. Die anderen Anforderungen in der Überspannungswarteschlange des virtuellen Lastausgleichsservers werden nicht geleert.

Hinweis: Sie können die Überspannungswarteschlangen der Cache-Umleitung, Authentifizierung, VPN oder virtuellen GSLB-Servern oder GSLB-Diensten nicht leeren.

Hinweis: Verwenden Sie die Funktion Überspannungsschutz nicht, wenn die Quell-IP (USIP) aktiviert ist.

So leeren Sie eine Surge-Queue mit der CLI

Der Befehl flush ns SurgeQ funktioniert auf folgende Weise:

- Sie können den Namen eines Dienstes, einer Dienstgruppe oder eines virtuellen Servers angeben, dessen Überspannungswarteschlange geleert werden muss.
- Wenn Sie während der Ausführung des Befehls einen Namen angeben, wird die Überspannungswarteschlange der angegebenen Entität geleert. Wenn mehrere Entitäten denselben Namen haben, leert die Appliance die Überspannungswarteschlangen aller dieser Entitäten.
- Wenn Sie den Namen einer Dienstgruppe und einen Servernamen und einen Port angeben, während der Befehl ausgeführt wird, löscht die Appliance die Überspannungswarteschlange nur des angegebenen Dienstgruppenmitglieds.
- Sie können ein Dienstgruppenmitglied (<serverName> und <port>) nicht direkt angeben, ohne den Namen der Dienstgruppe (<name>) anzugeben, und Sie können nicht <port>

ohne <serverName> angeben. Geben Sie <serverName> und <port> an, wenn Sie die Überspannungswarteschlange für ein bestimmtes Dienstgruppenmitglied leeren möchten.
- Wenn Sie den Befehl ausführen, ohne Namen anzugeben, legt die Appliance die Überspannungswarteschlangen aller auf der Appliance vorhandenen Entitäten.
- Wenn ein Dienstgruppenmitglied mit einem Servernamen identifiziert wird, müssen Sie den Servernamen in diesem Befehl angeben. Sie können seine IP-Adresse nicht angeben.

Geben Sie in der Befehlszeile Folgendes ein:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
<!--NeedCopy-->
```

Beispiele

```
flush ns surgeQ  -name SVC1ANZGB  -serverName 10.10.10.1 80
<!--NeedCopy-->
```

Der vorherige Befehl spült die Überspannungswarteschlange des Dienstes oder virtuellen Servers mit dem Namen SVC1ANZGB und hat die IP-Adresse als 10.10.10

```
flush ns surgeQ
<!--NeedCopy-->
```

Der vorherige Befehl spült alle Überspannungswarteschlangen auf der Appliance.

So leeren Sie eine Überspannungswarteschlange mit der GUI

Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie in der Aktionsliste die Option **Flush Surge Queue**aus.

Lastausgleichsetup verwalten

May 11, 2023

Die Wartung eines bestehenden Load Balancing-Setups erfordert keinen großen Aufwand, solange es unverändert ist, aber die meisten bleiben nicht lange unverändert. Die Erhöhung der Last erfordert neue Server mit Lastenausgleich und schließlich neue NetScaler Appliances, die konfiguriert und dem vorhandenen Setup hinzugefügt werden müssen. Alte Server verschleißen und müssen ausgetauscht werden, sodass einige Server entfernt und andere hinzugefügt werden müssen. Upgrades Ihrer Netzwerkausrüstung oder Änderungen an der Topologie erfordern möglicherweise auch Änderungen

an Ihrem Lastenausgleichs-Setup. Daher müssen Sie Vorgänge auf Serverobjekten, Diensten und virtuellen Servern ausführen. Der Visualizer kann Ihre Konfiguration grafisch anzeigen, und Sie können Operationen an den Entitäten in der Anzeige ausführen. Sie können auch andere Funktionen nutzen, die die Verwaltung des Datenverkehrs durch Ihr Load Balancing-Setup erleichtern.

Serverobjekte verwalten

May 11, 2023

Während des grundlegenden Load Balancing-Setups wird beim Erstellen eines Dienstes ein Serverobjekt mit der IP-Adresse des Dienstes erstellt, falls eines nicht vorhanden ist. Wenn Sie für Ihre Dienstobjekte bevorzugen, die mit Domänennamen anstelle von IP-Adressen benannt sind, haben Sie möglicherweise auch ein oder mehrere Serverobjekte manuell erstellt. Sie können jedes Serverobjekt aktivieren, deaktivieren oder entfernen.

Wenn Sie ein Serverobjekt aktivieren oder deaktivieren, aktivieren oder deaktivieren Sie alle mit dem Serverobjekt verknüpften Dienste. Wenn Sie die NetScaler-Appliance aktualisieren, nachdem Sie ein Serverobjekt deaktiviert haben, wird der Status des Dienstes als AUSSER BETRIEB angezeigt. Wenn Sie beim Deaktivieren eines Serverobjekts eine Wartezeit angeben, verarbeitet das Serverobjekt weiterhin bestehende Verbindungen für die angegebene Zeit, lehnt jedoch neue Verbindungen ab. Wenn Sie ein Serverobjekt entfernen, wird der Dienst, an den es gebunden ist, ebenfalls gelöscht.

So aktivieren Sie einen Server mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
enable server <name>
<!--NeedCopy-->
```

Beispiel:

```
enable server 10.102.29.5
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie ein Serverobjekt mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Servers**.
2. Wählen Sie den Server aus und wählen Sie in der Liste Aktion **Aktivieren oder**Deaktivieren**aus.

So deaktivieren Sie ein Serverobjekt mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
disable server <name> <delay>
<!--NeedCopy-->
```

Beispiel:

```
disable server 10.102.29.5 30
<!--NeedCopy-->
```

So entfernen Sie ein Serverobjekt mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
rm server <name>
<!--NeedCopy-->
```

Beispiel:

```
rm server 10.102.29.5
<!--NeedCopy-->
```

So entfernen Sie ein Serverobjekt mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Servers**.
2. Wählen Sie einen Server aus und klicken Sie auf **Entfernen**.

Dienste verwalten

May 11, 2023

Dienste sind standardmäßig aktiviert, wenn Sie sie erstellen. Sie können jeden Dienst einzeln deaktivieren oder aktivieren. Wenn Sie einen Dienst deaktivieren, geben Sie normalerweise eine Wartezeit an, während der der Dienst weiterhin bestehende Verbindungen verarbeitet, neue jedoch ablehnt, bevor er heruntergefahren wird. Wenn Sie keine Wartezeit angeben, wird der Dienst sofort heruntergefahren. Während der Wartezeit ist der Status DES Dienstes AUSSER BETRIEB.

Sie können einen Dienst entfernen, wenn er nicht mehr verwendet wird. Wenn Sie einen Dienst entfernen, wird er von seinem virtuellen Server getrennt und aus der NetScaler-Konfiguration gelöscht.

So aktivieren oder deaktivieren Sie einen Dienst mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
enable service <name>

disable service <name> <DelayInSeconds>
<!--NeedCopy-->
```

Beispiele:

```
enable service Service-HTTP-1
disable service Service-HTTP-1 30
<!--NeedCopy-->
```

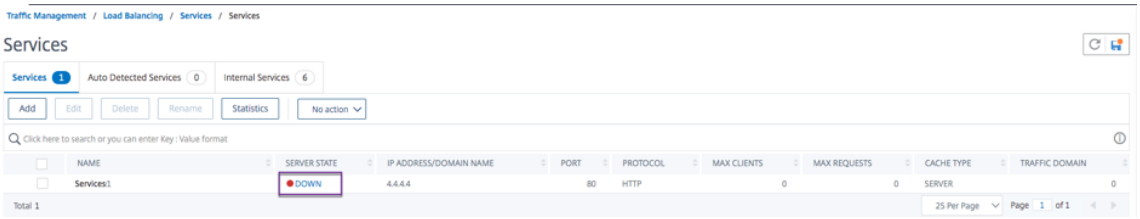
Um einen Dienst mithilfe der GUI zu aktivieren oder zu deaktivieren

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie einen Dienst und wählen Sie in der **Aktionsliste** **Aktivieren** oder **Deaktivieren** aus.

Identifizieren Sie die Ursache für den als DOWN markierten Dienststatus mithilfe der GUI

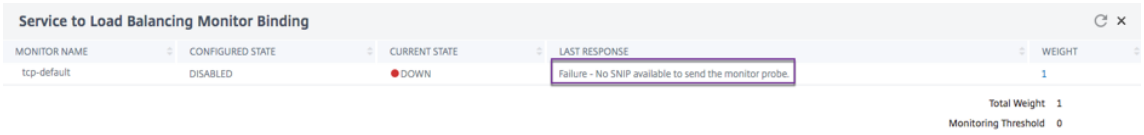
Ab NetScaler Version 13.0 Build 41.20 können Sie die Monitorprüfinformationen für die Dienste, die nicht verfügbar sind, auf der GUI anzeigen, ohne zur Monitor-Bindungsschnittstelle wechseln zu müssen. Der Wert in der Spalte **Serverstatus** der Seite Dienste ist anklickbar. Sie können auf **DOWN** klicken, um die Ursache zu ermitteln, aufgrund derer der Dienst als NICHT ERREICHBAR markiert ist.

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. **Klicken Sie in der Spalte** Serverstatus**, die dem Dienst entspricht, der AUSGEFALLEN ist, auf DOWN.**



Die Seite Service to Load Balancing Monitor Binding wird angezeigt.

In der Spalte Letzte Antwort wird der Grund angezeigt, aus dem der Dienst als NICHT VERFÜGBAR markiert wurde.



Virtuellen Lastausgleichsserver verwalten

May 11, 2023

Virtuelle Server sind standardmäßig aktiviert, wenn Sie sie erstellen. Sie können virtuelle Server manuell deaktivieren und aktivieren. Wenn Sie einen virtuellen Server deaktivieren, wird der Status des virtuellen Dienstes als OUT OF SERVICE angezeigt. In diesem Fall beendet der virtuelle Server alle Verbindungen, entweder sofort oder nachdem bestehende Verbindungen abgeschlossen wurden, je nach Einstellung des DownStateFlush-Parameters. Wenn downStateFlush aktiviert ist (Standard), werden alle Verbindungen geleert. Wenn DEAKTIVIERT, verarbeitet der virtuelle Server weiterhin Anfragen für bestehende Verbindungen.

Sie entfernen einen virtuellen Server nur, wenn Sie den virtuellen Server nicht mehr benötigen. Bevor Sie es entfernen, müssen Sie alle Dienste davon trennen.

So aktivieren oder deaktivieren Sie einen virtuellen Server mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
enable lb vserver <name>
<!--NeedCopy-->
```

```
disable lb vserver <name>
<!--NeedCopy-->
```

Beispiele:

```
enable lb vserver Vserver-LB-1
disable lb vserver Vserver-LB-1
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie einen virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus und wählen Sie in der **Aktionsliste** die Option **Aktivieren** oder **Deaktivieren**aus.

So trennen Sie mithilfe der CLI die Bindung eines Dienstes von einem virtuellen Server

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
unbind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

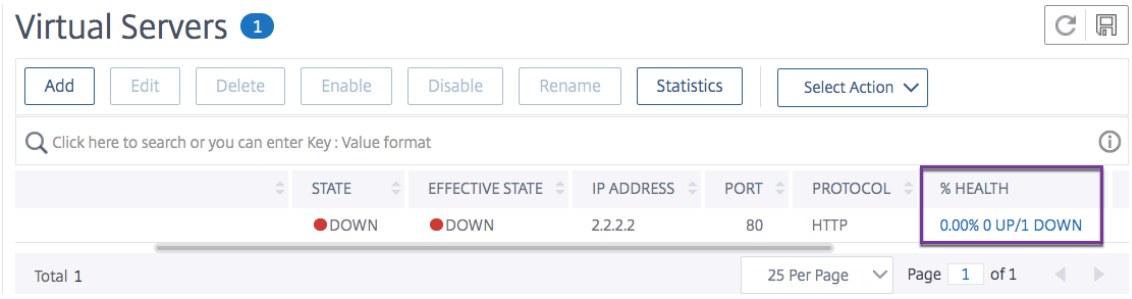
So trennen Sie mithilfe der GUI die Bindung eines Dienstes von einem virtuellen Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und klicken Sie auf den Abschnitt **Dienste** .
3. Wählen Sie einen Dienst aus und klicken Sie auf **Unbind**.

Identifizieren Sie die Ursache für den Status des virtuellen Servers, der mit DOWN gekennzeichnet ist, mit der GUI

Ab NetScaler Version 13.0 Build 41.20 können Sie die Monitor-Sond-Informationen auf der GUI für die virtuellen Server anzeigen, die DOWN sind, ohne zur Monitor Bindungsschnittstelle zu navigieren. Der Wert in der **Spalten% HEALTH** der Seite Virtual Server kann angeklickt werden. Sie können auf den Wert in der Spalte **% HEALTH** klicken, um die Hauptursache zu ermitteln, aufgrund derer der virtuelle Server als NICHT ERREICHBAR markiert ist.

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie in der Spalte **% HEALTH** auf den Wert, der dem virtuellen Server entspricht, der ausgefallen ist.

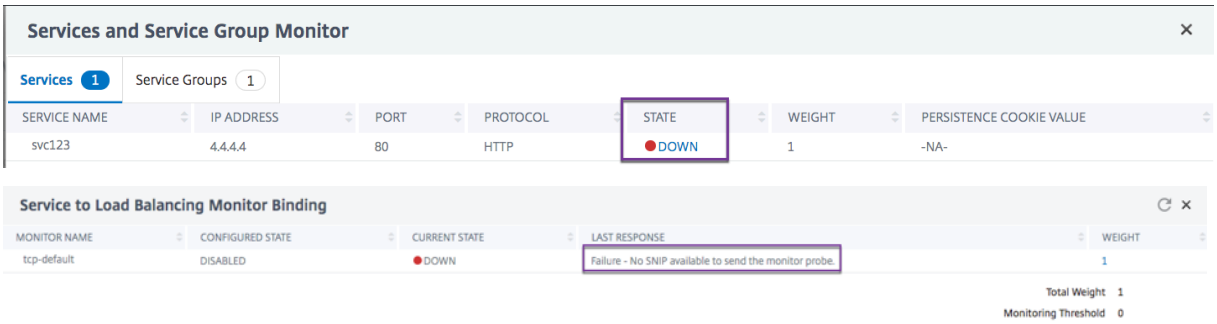


Die Seite Service and Service Group Monitor wird angezeigt. Die an diesen virtuellen Server gebundenen Dienste und Dienstgruppen werden in den entsprechenden Tabs angezeigt.

Wenn Sie Dienste verwenden, die an den virtuellen Load Balancing gebunden sind, gehen Sie wie folgt vor:

Klicken Sie auf der Registerkarte **Dienste** entsprechend dem Dienst, der **nicht** verfügbar ist, auf DOWN.

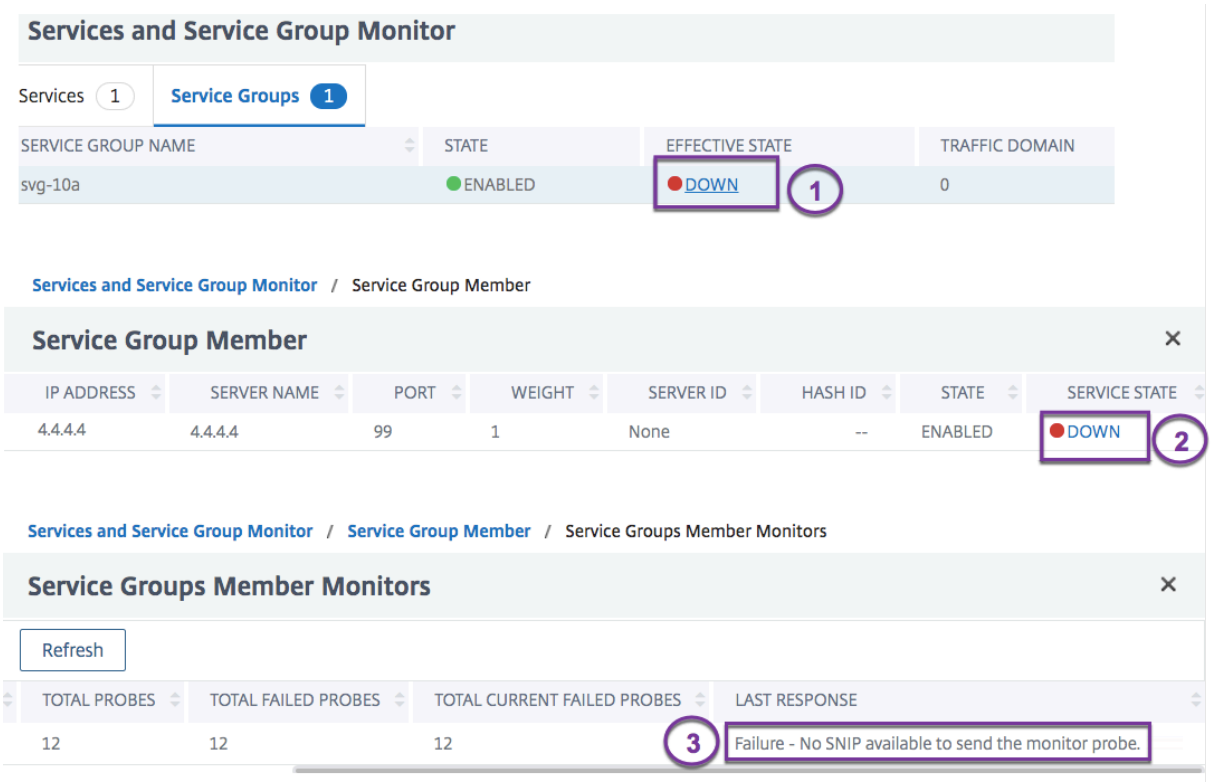
In der Spalte **Letzte Antwort auf** der Seite „Service to Load Balancing Monitor Binding“ wird der Grund angezeigt, aus dem der virtuelle Server als heruntergestuft wurde.



Wenn Sie Dienstgruppen verwenden, die an den virtuellen Load Balancing gebunden sind, gehen Sie wie folgt vor:

Klicken Sie auf der Registerkarte Service Groups**auf DER Seite Services and Service Group Monitor auf**DOWN**und dann auf der Seite Service Group Member auf DOWN.**

In der Spalte **Letzte Antwort auf** der Seite „Mitgliedermonitore für Servicegruppen“ wird der Grund angezeigt, aus dem der virtuelle Server als heruntergestuft wurde.



Visualisierer für Lastenausgleich

April 19, 2023

Der Load Balancing Visualizer ist ein Werkzeug, mit dem Sie die Load Balancing Konfiguration in einem grafischen Format anzeigen und ändern können. Es folgt ein Beispiel für die Visualizer-Anzeige.

Abbildung 1. Anzeige des Load Balancing Visualizers

Sie können den Visualizer verwenden, um Folgendes anzuzeigen:

- Die Dienste und Dienstgruppen, die an einen virtuellen Server gebunden sind.
- Die Monitore, die an jeden Dienst gebunden sind.
- Die Richtlinien, die an den virtuellen Server gebunden sind.
- Die Richtlinienbeschriftungen, falls konfiguriert.
- Konfigurationsdetails eines angezeigten Elements.

Sie können den Visualizer auch verwenden, um neue Objekte hinzuzufügen und zu binden, vorhandene Objekte zu ändern und Objekte zu aktivieren oder zu deaktivieren. Die meisten im Visualizer angezeigten Konfigurationselemente werden unter den gleichen Namen wie in anderen Teilen des Konfigurationsdienstprogramms angezeigt. Im Gegensatz zum Rest des Konfigurationsdienstprogramms gruppiert Visualizer Dienste, die dieselben Konfigurationsdetails aufweisen, und überwacht Bindungen in eine Entität, die als Dienstcontainer bezeichnet wird.

Ein Dienstcontainer besteht aus ähnlichen Diensten und Dienstgruppen, die an einen einzelnen virtuellen Lastausgleichsserver gebunden sind. Die Dienste im Container haben die gleichen Eigenschaften, mit Ausnahme des Namens, der IP-Adresse und des Port, und ihre Monitorbindungen müssen das gleiche Gewicht und den gleichen Bindungsstatus haben. Wenn Sie einen neuen Dienst an einen virtuellen Server binden, wird er in einen vorhandenen Container abgelegt, wenn seine Konfigurations- und Überwachungsbindungen mit denen anderer Dienste übereinstimmen. Ansonsten wird es in einen eigenen Behälter gelegt.

Die folgenden Verfahren enthalten nur die grundlegenden Schritte zur Verwendung des Visualizers. Da der Visualizer Funktionen in anderen Bereichen der Load Balancing-Funktion dupliziert, werden in der gesamten Load Balancing-Dokumentation andere Methoden zum Anzeigen oder Konfigurieren aller Einstellungen bereitgestellt, die im Visualizer konfiguriert werden können.

Hinweis: Der Visualizer benötigt eine grafische Oberfläche, so dass er nur über das Konfigurationsprogramm verfügbar ist.

So zeigen Sie die Eigenschaften des Lastenausgleichs virtueller Server mithilfe des Visualizers an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.

2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf **Visualizer**.

So zeigen Sie Konfigurationsdetails für Dienste, Dienstgruppen und Monitore mithilfe des Visualizers an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf **Visualizer**.
3. Doppelklicken Sie im Dialogfeld Load Balancing Visualizer auf die Entität, um die Konfigurationsdetails der Entität anzuzeigen, die an diesen virtuellen Server gebunden ist. Sie können folgende Aktionen ausführen:

So zeigen Sie Konfigurationsdetails für Richtlinien und Richtlinienbeschriftungen mithilfe des Visualizers im Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf Visualizer.
3. Doppelklicken Sie im Dialogfeld Load Balancing Visualizer auf die Richtlinienentität, um die Richtlinien anzuzeigen, die an diesen virtuellen Server gebunden sind.

So ändern Sie eine Ressource in einer Lastausgleichskonfiguration mithilfe des Visualizers

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie konfigurieren möchten, und klicken Sie dann auf Visualizer.
3. Doppelklicken Sie im Dialogfeld Load Balancing Visualizer im Visualizer-Image auf die Ressource, die Sie ändern möchten.

So fügen Sie eine Lastausgleichskonfiguration mithilfe des Visualizers hinzu

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie konfigurieren möchten, und klicken Sie dann auf Visualizer.
3. Klicken Sie im Dialogfeld Load Balancing Visualizer auf **+**, um die Ressource hinzuzufügen.

Client-Traffic verwalten

May 11, 2023

Die ordnungsgemäße Verwaltung von Clientverbindungen stellt sicher, dass Ihre Anwendungen auch dann für Benutzer verfügbar bleiben, wenn Ihre NetScaler-Appliance hohe Auslastung aufweist. Verschiedene Lastausgleichsfunktionen und andere auf der Appliance verfügbare Funktionen können in ein Lastausgleichs-Setup integriert werden, um die Last effizienter zu verarbeiten, bei Bedarf umzuleiten und die Aufgaben zu priorisieren, die die Appliance ausführen muss:

- **Sitzungsloser Lastausgleich.** Sie können virtuelle Server für den sitzungslosen Lastausgleich konfigurieren und einen Lastausgleich durchführen, ohne Sitzungen in Konfigurationen zu erstellen, die DSR- oder Intrusion-Detection-Systeme (IDS) verwenden.
- **Integriertes Caching.** Sie können HTTP-Anfragen an einen Cache umleiten.
- **Verzögerte Bereinigung.** Sie können die verzögerte Bereinigung virtueller Serververbindungen konfigurieren, um zu verhindern, dass der Bereinigungsprozess CPU-Zyklen in Zeiten verwendet, in denen die NetScaler-Appliance hohen Belastungen ausgesetzt ist.
- **Rewrite.** Sie können die Funktion Rewrite verwenden, um Port und Protokoll bei der Durchführung der HTTP-Umleitung zu ändern, oder die IP-Adresse und den Port des virtuellen Servers in einen benutzerdefinierten Request-Header einfügen.
- **RTSP NAT.**
- **Ratenbasierte Überwachung.** Sie können eine ratenbasierte Überwachung aktivieren, um überschüssigen Traffic umzuleiten.
- **Layer-2-Parameter.** Sie können einen virtuellen Server so konfigurieren, dass die L2-Parameter zur Identifizierung einer Verbindung verwendet werden.
- **ICMP-Antwort**. Sie können die Appliance so konfigurieren, dass ICMP-Antworten an PING-Anforderungen gemäß Ihren Einstellungen gesendet werden. Stellen Sie auf der dem virtuellen Server entsprechenden IP-Adresse die ICMP RESPONSE auf VSVR_CNTRLD ein, und legen Sie auf dem virtuellen Server die fest `ICMP VSERVER RESPONSE`.
  Die folgenden Einstellungen können auf einem virtuellen Server vorgenommen werden:
  - Wenn Sie auf allen virtuellen Servern auf PASSIV eingestellt `ICMP VSERVER RESPONSE` sind, antwortet die Appliance immer.
  - Wenn Sie auf allen virtuellen Servern auf ACTIVE eingestellt `ICMP VSERVER RESPONSE` sind, reagiert die Appliance auch dann, wenn ein virtueller Server UP ist.
  - Wenn Sie bei einigen `ICMP VSERVER RESPONSE` auf ACTIVE und auf anderen PASSIV eingestellt sind, reagiert die Appliance auch dann, wenn ein auf ACTIVE gesetzter virtueller Server UP ist.

Sitzungslose Lastausgleichsserver konfigurieren

May 11, 2023

Wenn die NetScaler-Appliance einen Lastenausgleich durchführt, erstellt und verwaltet sie Sitzungen zwischen Clients und Servern. Die Verwaltung von Sitzungsinformationen belastet die Appliance-Ressourcen erheblich, und in Szenarien wie einer Einrichtung mit Direct Server Return Serverrücklauf (DSR) und dem Lastenausgleich von Intrusion Detection Systems (IDS) sind Sitzungen möglicherweise nicht erforderlich. Um zu vermeiden, dass Sitzungen erstellt werden, wenn sie nicht erforderlich sind, können Sie einen virtuellen Server auf der Appliance für den sitzungslosen Lastenausgleich konfigurieren. Beim sitzungslosen Load Balancing führt die Appliance den Lastenausgleich pro Paket durch.

Der sitzungslose Load Balancing kann im MAC-basierten Weiterleitungsmodus oder im IP-basierten Weiterleitungsmodus betrieben werden.

Für die MAC-basierte Weiterleitung muss die IP-Adresse des sitzungslosen virtuellen Servers auf allen physischen Servern angegeben werden, an die der Datenverkehr weitergeleitet wird.

Für die IP-basierte Weiterleitung im sitzungslosen Load Balancing müssen die IP-Adresse und der Port des virtuellen Servers auf den physischen Servern nicht angegeben werden, da diese Informationen in den weitergeleiteten Paketen enthalten sind. Bei der Weiterleitung eines Pakets vom Client an den physischen Server lässt die Appliance die Clientdetails wie IP-Adresse und Port unverändert und fügt die IP-Adresse und den Port des Ziels hinzu.

Unterstützte Einrichtung

Der sitzungslose NetScaler Load Balancing unterstützt die folgenden Diensttypen und Lastausgleichsmethoden:

Arten von Diensten

- ANY für Mac-basierte Umleitung
- ANY, DNS und UDP für IP-basierte Umleitung

Methoden des Lastenausgleichs

- Runde Robin
- Geringste Bandbreite
- LRTM (Methode mit der geringsten Reaktionszeit)
- Quell-IP-Hash
- Ziel-IP-Hash
- Quell-IP-Ziel-IP-Hash

- Quell-IP-Quellport-Hash
- Benutzerdefinierte Last

Einschränkungen

Beim Sitzungslosen Load Balancing gelten die folgenden Einschränkungen:

- Die Appliance muss im zweiarmigen Modus eingesetzt werden.
- Ein Dienst darf nur an einen virtuellen Server gebunden sein.
- Sitzungsloser Load Balancing wird für Servicegruppen nicht unterstützt.
- Sitzungsloser Lastenausgleich wird für domänenbasierte Dienste (DBS-Dienste) nicht unterstützt.
- Sitzungsloser Lastenausgleich im IP-Modus wird für einen virtuellen Server, der als Backup für einen primären virtuellen Server konfiguriert ist, nicht unterstützt.
- Sie können den Spillover-Modus nicht aktivieren.
- Für alle Dienste, die an einen virtuellen Server mit sitzungslosem Lastenausgleich gebunden sind, muss die Option Quell-IP (USIP) verwenden aktiviert sein.
- Für einen virtuellen Platzhalterserver oder -dienst wird die Ziel-IP-Adresse nicht geändert.

Hinweis:

- Geben Sie bei der Konfiguration eines virtuellen Servers für den sitzungslosen Lastenausgleich ausdrücklich eine unterstützte Lastausgleichsmethode an. Die Standardmethode, Least Connection, kann nicht für den Lastausgleich ohne Sitzung verwendet werden.
- Um den sitzungslosen Lastenausgleich im MAC-basierten Umleitungsmodus auf einem virtuellen Server zu konfigurieren, muss die MAC-basierte Weiterleitungsoption auf der NetScaler-Appliance aktiviert sein.

So fügen Sie mithilfe der CLI einen virtuellen Server ohne Sitzung hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen virtuellen Server ohne Sitzung hinzuzufügen und die Konfiguration zu überprüfen:

```
add lb vserver <name>@ <serviceType> <IPAddress>@ <port> -m <
    redirectionMode> -sessionless <(ENABLED|DISABLED)> -lbMethod <
    load_balancing_method>

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:


```
add lb vserver sesslessv1 any 11.11.12.123 54 -sessionless ENABLED -
    lbMethod roundrobin -m ip
      Done
show lb vserver sesslessv1
     sesslessv1 (11.11.12.123:54) - ANY Type: ADDRESS
     State: DOWN
     ...
     Effective State: DOWN
     Client Idle Timeout: 120 sec
     Down state flush: ENABLED
     ...
     Persistence: NONE
     Sessionless LB: ENABLED
     Connection Failover: DISABLED
     L2Conn: OFF
     1) Policy : cmp_text Priority:8680 Inherited
     2) Policy : cmp_nocmp_ie60 Priority:8690 Inherited
<!--NeedCopy-->
```

So konfigurieren Sie den sitzungslosen Load Balancing auf einem vorhandenen virtuellen Server

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name>@ -m <redirectionMode> -sessionless <(ENABLED|
   DISABLED)> -lbMethod <load_balancing_method>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver sesslessv1 -m mac -sessionless ENABLED -lbmethod lrtm
  Done
<!--NeedCopy-->
```

> **Hinweis**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die `-m MAC` Option aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie einen virtuellen Server ohne Session mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.

2. Öffnen Sie den virtuellen Server und klicken Sie in den Erweiterten Einstellungen auf Traffic Settings und wählen Sie dann Sessionless Load Balancing aus.

HTTP-Anfragen an einen Cache umleiten

May 11, 2023

Die NetScaler Cache-Umleitungsfunktion leitet HTTP-Anforderungen an einen Cache um. Sie können die Auswirkungen der Reaktion auf HTTP-Anfragen erheblich reduzieren und die Leistung Ihrer Website durch die ordnungsgemäße Implementierung der Cache-Umleitungsfunktion verbessern.

Ein Cache speichert häufig angeforderten HTTP-Inhalt. Wenn Sie die Cache-Umleitung auf einem virtuellen Server konfigurieren, sendet die NetScaler-Appliance zwischenspeicherbare HTTP-Anfragen an den Cache und nicht zwischenspeicherbare HTTP-Anfragen an den ursprünglichen Webserver.

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -cacheable <Value>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -cacheable yes
<!--NeedCopy-->
```

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf Verkehrseinstellungen, und wählen Sie Cacheable aus.

Bereinigung virtueller Serververbindungen aktivieren

May 11, 2023

Unter bestimmten Bedingungen können Sie die Einstellung DownStateFlush so konfigurieren, dass vorhandene Verbindungen sofort beendet werden, wenn ein Dienst oder ein virtueller Server als DOWN markiert ist. Durch das Beenden vorhandener Verbindungen werden Ressourcen freigegeben und in bestimmten Fällen wird die Wiederherstellung überlasteter Lastausgleichseinstellungen beschleunigt.

Der Status eines virtuellen Servers hängt vom Status der an ihn gebundenen Dienste ab. Der Status der einzelnen Dienste hängt von den Reaktionen der Server mit Lastausgleich auf Tests und Integritätsprüfungen ab, die von den Monitoren gesendet werden, die an diesen Dienst gebunden sind. Manchmal reagieren die Server mit Lastausgleich nicht. Wenn ein Server langsam oder ausgelastet ist, kann es bei den Überwachungstests zu einem Timeout kommen. Wenn wiederholte Überwachungssonden nicht innerhalb der konfigurierten Zeitüberschreitungszeit beantwortet werden, wird der Dienst mit DOWN gekennzeichnet.

Ein virtueller Server wird nur dann als DOWN markiert, wenn alle an ihn gebundenen Dienste als DOWN markiert sind. Wenn ein virtueller Server heruntergeht, werden alle Verbindungen beendet, entweder sofort oder nachdem bereits vorhandene Verbindungen abgeschlossen werden können.

Aktivieren Sie die DownStateFlush-Einstellung nicht auf den Anwendungsservern, die ihre Transaktionen abschließen müssen. Sie können diese Einstellung auf Webservern aktivieren, deren Verbindungen sicher beendet werden können, wenn sie DOWN markiert haben.

In der folgenden Tabelle werden die Auswirkungen dieser Einstellung auf eine Beispielkonfiguration zusammengefasst, die aus einem virtuellen Server, vServer-LB-1, mit einem daran gebundenen Dienst, Service-TCP-1, besteht. In der Tabelle bezeichnen E und D den Status der DownStateFlush-Einstellung: E bedeutet Aktiviert und D bedeutet Deaktiviert.

Vserver-LB-1	Service-TCP-1	Status der Verbindungen
E	E	Sowohl Client- als auch Serververbindungen werden beendet.

Vserver-LB-1	Service-TCP-1	Status der Verbindungen
E	D	Bei einigen Diensttypen wie TCP, für die die NetScaler-Appliance die Wiederverwendung von Verbindungen nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung von Verbindungen unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn auf diesen Verbindungen eine Transaktion aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Client-Verbindungen beendet.

Vserver-LB-1	Service-TCP-1	Status der Verbindungen
D	E	Bei einigen Diensttypen wie TCP, für die die NetScaler-Appliance die Wiederverwendung von Verbindungen nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung von Verbindungen unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn auf diesen Verbindungen eine Transaktion aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Serververbindungen beendet.
D	D	Weder Client- noch Serververbindungen werden beendet.

Wenn Sie einen Dienst nur deaktivieren möchten, wenn alle etablierten Verbindungen vom Server oder vom Client geschlossen werden, können Sie die Option ordnungsgemäßes Herunterfahren verwenden. Informationen zum ordnungsmäßigen Herunterfahren eines Dienstes finden Sie unter Graceful Shutdown of Services.

So konfigurieren Sie die Einstellung zum Ausfallzustand auf einem virtuellen Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -downStateFlush <Value>
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver Vserver-LB-1 -downStateFlush enabled
<!--NeedCopy-->
```

So konfigurieren Sie die Flush-Einstellung für den Down-State-Flush auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie in den Erweiterten Einstellungen auf Traffic Settings und wählen Sie Down State Flush aus.

Rewrite von Ports und Protokollen für die HTTP-Umleitung

May 11, 2023

Virtuelle Server und die an sie gebundenen Dienste verwenden möglicherweise verschiedene Ports. Wenn ein Dienst mit einer Umleitung auf eine HTTP-Verbindung reagiert, müssen Sie möglicherweise die NetScaler Appliance so konfigurieren, dass der Port und das Protokoll geändert werden, um sicherzustellen, dass die Umleitung erfolgreich durchgeführt wird. Dazu aktivieren und konfigurieren Sie die Einstellung RedirectPortRewrite.

Diese Einstellung wirkt sich nur auf HTTP- und HTTPS-Verkehr aus. Wenn diese Einstellung auf einem virtuellen Server aktiviert ist, schreibt der virtuelle Server den Port bei Weiterleitungen neu und ersetzt den vom Dienst verwendeten Port durch den vom virtuellen Server verwendeten Port.

Wenn der virtuelle Server oder Dienst vom Typ SSL ist, müssen Sie die SSL-Umleitung auf dem virtuellen Server oder Dienst aktivieren. Wenn sowohl der virtuelle Server als auch der Dienst vom Typ SSL sind, aktivieren Sie die SSL-Umleitung auf dem virtuellen Server.

Die Einstellung RedirectPortRewrite kann in den folgenden Szenarien verwendet werden:

- Der virtuelle Server ist vom Typ HTTP und die Dienste sind vom Typ SSL.
- Der virtuelle Server ist vom Typ SSL und die Dienste sind vom Typ HTTP.
- Der virtuelle Server ist vom Typ HTTP und die Dienste sind vom Typ HTTP.
- Der virtuelle Server ist vom Typ SSL und die Dienste sind vom Typ SSL.

Szenario 1: Der virtuelle Server ist vom Typ HTTP und die Dienste sind vom Typ SSL. Die SSL-Weiterleitung und optional das Umschreiben von Port sind für den Dienst aktiviert. Wenn Port Rewrite aktiviert ist, wird der Port von HTTPS-URLs neu geschrieben. HTTP-URLs vom Server werden so wie sie sind an den Client gesendet.

Nur die SSL-Weiterleitung ist aktiviert. Der virtuelle Server kann an jedem Port konfiguriert werden. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

SSL-Weiterleitung und Port-Rewrite sind aktiviert. Der virtuelle Server ist auf Port 80 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/

SSL-Weiterleitung und Port-Rewrite sind aktiviert. Der virtuelle Server ist auf Port 8080 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	http://domain.com:8080/
https://domain.com:444/	http://domain.com:8080/

Szenario 2: Der virtuelle Server ist vom Typ SSL und die Dienste sind vom Typ HTTP. Wenn Port Rewrite aktiviert ist, wird nur der Port von HTTP-URLs neu geschrieben. HTTPS-URLs vom Server werden so wie sie sind an den Client gesendet.

Die SSL-Weiterleitung ist auf dem virtuellen Server aktiviert. Der virtuelle Server kann an jedem Port konfiguriert werden. Siehe folgende Tabelle.

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

SSL-Umleitung und Port-Rewrite sind auf dem virtuellen Server aktiviert. Der virtuelle Server ist auf Port 443 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	https://domain.com/
http://domain.com:8080/	https://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

SSL-Weiterleitung und Port-Rewrite sind aktiviert. Der virtuelle Server ist auf Port 444 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	https://domain.com:444/
http://domain.com:8080/	https://domain.com:444/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Szenario 3: Der virtuelle Server und der Dienst sind vom Typ HTTP. Port-Rewrite muss auf dem virtuellen Server aktiviert sein. Nur der Port von HTTP-URLs wird neu geschrieben. HTTPS-URLs vom Server werden so wie sie sind an den Client gesendet.

Der virtuelle Server ist auf Port 80 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com/

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com:8080/	http://domain.com/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

Der virtuelle Server ist auf Port 8080 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com:8080/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:445/	https://domain.com:445/

Szenario 4: Der virtuelle Server und der Dienst sind vom Typ SSL. Wenn Port Rewrite aktiviert ist, wird nur der Port von HTTPS-URLs neu geschrieben. HTTP-URLs vom Server werden so wie sie sind an den Client gesendet.

Die SSL-Weiterleitung ist auf dem virtuellen Server aktiviert. Der virtuelle Server kann an jedem Port konfiguriert werden. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com:444/

SSL-Umleitung und Port-Rewrite sind auf dem virtuellen Server aktiviert. Der virtuelle Server ist auf Port 443 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
https://domain.com/	https://domain.com/
https://domain.com:444/	https://domain.com/

SSL-Umleitung und Port-Rewrite sind auf dem virtuellen Server aktiviert. Der virtuelle Server ist auf Port 444 konfiguriert. Sehen Sie sich die folgende Tabelle an:

URL vom Server umleiten	An den Client gesendete Umleitungs-URL
http://domain.com/	http://domain.com/
http://domain.com:8080/	http://domain.com:8080/
https://domain.com/	https://domain.com:444/
https://domain.com:445/	https://domain.com:444/

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -redirectPortRewrite (ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie den virtuellen Server, klicken Sie im Bereich Erweiterte Einstellungen auf Verkehrseinstellungen und wählen Sie dann Rewrite aus.

So konfigurieren Sie die SSL-Weiterleitung auf einem virtuellen SSL-Server oder -Dienst mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:


```
set ssl vserver <vServerName> - sslRedirect (ENABLED | DISABLED)

set ssl service <serviceName> - sslRedirect (ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver Vserver-SSL-1 -sslRedirect enabled

set ssl service service-SSL-1 -sslRedirect enabled
<!--NeedCopy-->
```

Um die SSL-Umleitung und die SSL-Portumschreibung auf einem virtuellen SSL-Server oder -Dienst mithilfe der GUI zu konfigurieren

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf SSL-Parameter, und wählen Sie SSL-Umleitung aus.

IP-Adresse und Port eines virtuellen Servers in den Request-Header einfügen

May 11, 2023

Wenn Sie mehrere virtuelle Server haben, die mit verschiedenen Anwendungen im selben Dienst kommunizieren, müssen Sie Folgendes tun:

Konfigurieren Sie die NetScaler Appliance so, dass die IP-Adresse und die Portnummer des entsprechenden virtuellen Servers zu den HTTP-Anforderungen hinzugefügt werden, die an diesen Dienst gesendet werden. Mit dieser Einstellung können Anwendungen, die auf dem Dienst ausgeführt werden, den virtuellen Server identifizieren, der die Anforderung gesendet hat.

Wenn der primäre virtuelle Server ausgefallen ist und der virtuelle Backup-Server aktiv ist, werden die Konfigurationseinstellungen des virtuellen Backup-Servers zu den Clientanforderungen hinzugefügt. Wenn Sie möchten, dass dasselbe Header-Tag hinzugefügt wird, unabhängig davon, ob die Anfragen vom primären virtuellen Server oder vom virtuellen Backup-Server stammen, müssen Sie das erforderliche Header-Tag auf beiden virtuellen Servern konfigurieren.

Hinweis: Diese Option wird für virtuelle Wildcard-Server oder virtuelle Dummy-Server nicht unterstützt.

Um die IP-Adresse und den Port des virtuellen Servers mithilfe der CLI in die Clientanfragen einzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -insertVserverIPPort <insertVserverIPPort> [<
   vipHeader>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -insertVserverIPPort VipAddr
<!--NeedCopy-->
```

Um die IP-Adresse und den Port des virtuellen Servers mithilfe der GUI in die Clientanfragen einzufügen

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie den virtuellen Server, klicken Sie im Bereich Erweiterte Einstellungen auf **Verkehrseinstellungen**, wählen Sie dann Einfügen des virtuellen Servers IP-Port aus, und geben Sie einen IP-Port-Header des virtuellen Servers an.

Verwenden Sie eine angegebene Quell-IP für Back-End-Kommunikation

May 11, 2023

Für die Kommunikation mit den physischen Servern oder anderen Peer-Geräten verwendet die NetScaler Appliance eine IP-Adresse, die ihr gehört, als Quell-IP-Adresse. Die NetScaler-Appliance verwaltet einen Pool ihrer IP-Adressen und wählt dynamisch eine IP-Adresse aus, während sie sich mit einem Server verbindet. Abhängig vom Subnetz, in dem der physische Server abgelegt ist, entscheidet die Appliance, welche IP-Adresse verwendet werden soll. Dieser Adresspool wird zum Senden von Traffic- und Monitor-Sonden verwendet.

In vielen Situationen möchten Sie möglicherweise, dass die Appliance eine bestimmte IP-Adresse oder eine IP-Adresse von einem bestimmten Satz von IP-Adressen für die Back-End-Kommunikation verwendet. Im Folgenden finden Sie einige Beispiele:

- Ein Server kann Monitorprobes vom Datenverkehr unterscheiden, wenn die Quell-IP-Adresse, die für Monitorprobes verwendet wird, zu einem bestimmten Satz gehört.
- Um die Serversicherheit zu verbessern, kann ein Server so konfiguriert werden, dass er auf Anfragen von einem bestimmten Satz von IP-Adressen oder manchmal von einer einzigen bes-

timmten IP-Adresse reagiert. In diesem Fall kann die Appliance nur die vom Server akzeptierten IP-Adressen als Quell-IP-Adresse verwenden.

- Die Appliance kann ihre internen Verbindungen effizient verwalten, wenn sie ihre IP-Adressen in IP-Sets verteilen und eine Adresse aus einem Satz nur für die Verbindung zu einem bestimmten Dienst verwenden kann.

Um die Appliance für die Verwendung einer angegebenen Quell-IP-Adresse zu konfigurieren, erstellen Sie Netzprofile (Netzwerkprofile) und konfigurieren Sie die Appliance-Entitäten für die Verwendung des Profils. Ein Netzprofil kann an den Lastenausgleich oder an virtuelle Server mit Content Switching, virtuelle Server, Dienste, Dienstgruppen oder Monitore von NetScaler Gateway VPN gebunden werden. Ein Netzprofil verfügt über IP-Adressen im Besitz von NetScaler (SNIPs und VIPs), die als Quell-IP-Adresse verwendet werden können. Es kann sich um eine einzelne IP-Adresse oder eine Reihe von IP-Adressen handeln, die als IP-Set bezeichnet werden. Wenn ein Netzprofil über eine IP verfügt, wählt die Appliance dynamisch eine IP-Adresse aus der zum Zeitpunkt der Verbindung eingestellten IP aus. Wenn ein Profil eine einzelne IP-Adresse hat, wird dieselbe IP-Adresse als Quell-IP verwendet.

Wenn ein Netzprofil an einen virtuellen Load Balancing- oder Content Switching-Server gebunden ist, wird das Profil zum Senden von Datenverkehr an alle an ihn gebundenen Dienste verwendet. Wenn ein Netzprofil an eine Dienstgruppe gebunden ist, verwendet die Appliance das Profil für alle Mitglieder der Dienstgruppe. Wenn ein Netzprofil an einen Monitor gebunden ist, verwendet die Appliance das Profil für alle vom Monitor gesendeten Prüfpunkte.

> **Hinweis:**
>
> - Wenn eine NetScaler Appliance eine VIP-Adresse verwendet, um mit einem Server zu kommunizieren, identifiziert sie anhand von Sitzungseinträgen, ob der für die VIP-Adresse bestimmte Datenverkehr eine Antwort von einem Server oder eine Anforderung eines Clients ist.
> - Sie können ein Netzprofil an virtuelle VPN-Server von NetScaler Gateway binden. Beim Binden eines Netzprofils müssen Sie jedoch einige Punkte notieren. Weitere Informationen finden Sie unter Punkte, die beim Binden eines Netzprofils an einen virtuellen VPN-Server zu beachtensind.
> - Die an einen Dienst oder eine Dienstgruppe gebundenen Netzprofil-IPs werden nicht nur zum Senden von Datenverkehr an die entsprechenden Back-End-Server verwendet, sondern auch für die DNS-Anforderungen, die durch ungelöste Back-End-FQDN ausgelöst werden.

Verwendung eines Netzprofils zum Senden von Traffic

Wenn die Option Quell-IP-Adresse (USIP) verwenden aktiviert ist, verwendet die Appliance die IP-Adresse des Clients und ignoriert alle Netzprofile. Wenn die USIP-Option nicht aktiviert ist, wählt die Appliance die Quell-IP auf folgende Weise aus:

- Wenn auf dem virtuellen Server oder der Service-Gruppe kein Netzprofil vorhanden ist, verwendet die Appliance die Standardmethode.
- Wenn nur ein Netzprofil in der Service-Gruppe vorhanden ist, verwendet die Appliance dieses Netzprofil.
- Wenn nur auf dem virtuellen Server ein Netzprofil vorhanden ist, verwendet die Appliance das Netzprofil.
- Wenn sowohl auf dem virtuellen Server als auch auf der Service-/Servicegruppe ein Netzprofil vorhanden ist, verwendet die Appliance das an die Service/Servicegruppe gebundene Netzprofil.

Verwendung eines Netzprofils zum Senden von Monitor-Prüfungen:

Bei Monitor-Prüfungen wählt die Appliance die Quell-IP auf folgende Weise aus:

- Wenn an den Monitor ein Netzprofil gebunden ist, verwendet die Appliance das Netzprofil des Monitors. Es ignoriert die Netzprofile, die an den virtuellen Server oder die Dienstleistungsgruppe gebunden sind.
- Wenn kein Netzprofil an den Monitor gebunden ist,
  - Wenn in der Service-Gruppe ein Netzprofil vorhanden ist, verwendet die Appliance das Netzprofil der Service-/Servicegruppe.
  - Wenn selbst in der Service-/Servicegruppe kein Netzprofil vorhanden ist, verwendet die Appliance die Standardmethode zur Auswahl einer Quell-IP.

Hinweis: Wenn kein Netzwerkprofil an einen Dienst gebunden ist, sucht die Appliance nach einem Netzprofil in der Dienstgruppe, wenn der Dienst an eine Dienstgruppe gebunden ist.

Gehen Sie wie folgt vor, um eine angegebene Quell-IP-Adresse für die Kommunikation zu verwenden:

1. Erstellen Sie IP-Sets aus dem Pool von SNIPs und VIPs, die der NetScaler Appliance gehören. Ein IP-Set kann sowohl aus SNIP- als auch VIP-Adressen bestehen. Anweisungen finden Sie unter Erstellen von IP-Sets.
2. Erstellen von Netzprofilen. Anweisungen finden Sie unter Erstellen eines Netzprofils.
3. Binden Sie die Netzprofile an die Appliance-Entitäten. Anweisungen finden Sie unter Binden eines Netzprofils an eine NetScaler Entität.

> **Hinweis:**
>
> - Ein Netzprofil kann nur die IP-Adressen haben, die auf der NetScaler Appliance als SNIP und VIP angegeben sind.
> - Die Quell-IP-Persistenz wird für von NetScaler initiierte Pakete nicht berücksichtigt.

Netzprofile verwalten

Ein Netzprofil (oder Netzwerkprofil) enthält eine IP-Adresse oder einen IP-Satz. Während der Kommunikation mit physischen Servern oder Peers verwendet die NetScaler Appliance die im Profil angegebe-

nen Adressen als Quell-IP-Adresse.

- Anweisungen zum Erstellen eines Netzwerkprofils finden Sie unter Erstellen eines Netzwerkprofils.
- Anweisungen zum Binden eines Netzwerkprofils an eine NetScaler-Entität finden Sie unter Binden eines Netzprofils an eine NetScaler-Entität.

Erstellen eines IP-Sets

Ein IP-Set ist ein Satz von IP-Adressen, die auf der NetScaler Appliance als Subnetz-IP-Adressen (SNIPs) oder virtuelle IP-Adressen (VIPs) konfiguriert sind. Ein IP-Satz wird mit einem aussagekräftigen Namen identifiziert, der bei der Identifizierung der Verwendung der darin enthaltenen IP-Adressen hilft. Um einen IP-Satz zu erstellen, fügen Sie einen IP-Satz hinzu und binden Sie IP-Adressen im Besitz von NetScaler daran. SNIP-Adressen und VIP-Adressen können im gleichen IP-Set vorhanden sein.

So erstellen Sie einen IP-Satz mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add ipset <name>

bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Oder

```
bind ipset <name> <IPAddress>

show ipset [<name>]
<!--NeedCopy-->
```

Der vorhergehende Befehl zeigt die Namen aller IP-Sets auf der Appliance an, wenn Sie keinen Namen übergeben. Es zeigt die IP-Adressen, die an den angegebenen IP-Satz gebunden sind, wenn Sie einen Namen übergeben.

Beispiele

```
1.
> add ipset skpnwipset
 Done
> bind ipset skpnwipset 21.21.20.1
 Done

```



```
2.
 > add ipset testnwipset
 Done
> bind ipset testnwipset 21.21.21.[21-25]
 IPAddress "21.21.21.21" bound
 IPAddress "21.21.21.22" bound
 IPAddress "21.21.21.23" bound
 IPAddress "21.21.21.24" bound
 IPAddress "21.21.21.25" bound
 Done

3.
 > bind ipset skpipset 11.11.11.101
 ERROR: Invalid IP address
[This IP address could not be added because this is not an IP address
   owned by the NetScaler appliance]
 > add ns ip 11.11.11.101 255.255.255.0 -type SNIP
 ip "11.11.11.101" added
 Done
 > bind ipset skpipset 11.11.11.101
 IPAddress "11.11.11.101" bound
 Done
4.
> sh ipset
1) Name: ipset-1
2) Name: ipset-2
3) Name: ipset-3
4) Name: skpnewipset
 Done

5.
> sh ipset skpnewipset
IP:21.21.21.21
IP:21.21.21.22
IP:21.21.21.23
IP:21.21.21.24
IP:21.21.21.25
 Done
<!--NeedCopy-->
```

So erstellen Sie einen IP-Satz mit der GUI

Navigieren Sie zu **System > Netzwerk > IP-Sets**, und erstellen Sie ein IP-Set.

Erstellen Sie ein Netzprofil

Ein Netzprofil (Netzwerkprofil) besteht aus einer oder mehreren SNIP - oder VIP-Adressen der NetScaler Appliance.

So erstellen Sie ein Netzprofil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add netprofile <name> [-srcIp <srcIpVal>]
<!--NeedCopy-->
```

Wenn SrCipval in diesem Befehl nicht angegeben ist, kann er später mit dem `set netprofile` Befehl bereitgestellt werden.

Beispiele

```
add netprofile skpnetprofile1 -srcIp 21.21.20.1
Done

add netprofile baksnp -srcIp bakipset
Done

set netprofile yahnp -srcIp 12.12.23.1
Done

set netprofile citkbnp -srcIp citkbipset
Done
<!--NeedCopy-->
```

Binden eines Netzprofils an eine NetScaler-Entität

Ein Netzprofil kann an einen virtuellen Lastausgleichsserver, einen Dienst, eine Dienstgruppe oder einen Monitor gebunden werden.

Hinweis: Sie können ein Netzprofil zum Zeitpunkt der Erstellung einer NetScaler-Entität binden oder an eine vorhandene Entität binden.

So binden Sie ein Netzprofil mithilfe der Befehlszeilenschnittstelle an einen Server

Sie können ein Netzprofil an virtuelle Server mit Lastenausgleich und virtuelle Content Switching-Server binden. Geben Sie den entsprechenden virtuellen Server an.

Geben Sie in der Befehlszeile Folgendes ein:


```
set lb vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Oder

```
set cs vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Beispiele

```
set lb vserver skpnwvs1 -netProfile gntnp
 Done
set cs vserver mmdcsv -netProfile mmdnp
 Done
<!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie in den erweiterten Einstellungen auf **Profile**, und legen Sie ein Netzprofil fest.

So binden Sie ein Netzprofil mithilfe der CLI an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Beispiel

```
set service brnssvc1 -netProfile brnsnp
 Done
<!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an einen Dienst

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Klicken Sie in den erweiterten Einstellungen auf **Profile**, und legen Sie ein Netzprofil fest.

So binden Sie ein Netzprofil mithilfe der CLI an eine Dienstgruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
set servicegroup <serviceGroupName> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Beispiel

```
set servicegroup ndhsvcgrp -netProfile ndhnp
 Done
<!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an eine Dienstgruppe

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienstgruppen**, und öffnen Sie eine Dienstgruppe.
2. Klicken Sie in den erweiterten Einstellungen auf **Profile**, und legen Sie ein Netzprofil fest.

So binden Sie ein Netzprofil mithilfe der CLI an einen Monitor

Geben Sie in der Befehlszeile Folgendes ein:

```
set monitor <monitor_name> -netProfile <net_profile_name>
```

Beispiel

```
set monitor brnsecvmon1 -netProfile brnsmonnp
 Done
<!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an einen Monitor

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Öffnen Sie einen Monitor und legen Sie das Netzprofil fest.

Timeoutwert für ungenutzte Clientverbindungen

May 11, 2023

Sie können einen virtuellen Server so konfigurieren, dass alle inaktiven Client-Verbindungen nach Ablauf eines konfigurierten Timeout-Zeitraums (in Sekunden) beendet werden. Wenn Sie diese Einstellung konfigurieren, wartet die NetScaler Appliance auf die angegebene Zeit und schließt die Clientverbindung, wenn sich der Client nach diesem Zeitpunkt im Leerlauf befindet. Standardmäßig ist der Zeitüberschreitungswert des Clients auf 180 Sekunden festgelegt.

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -cltTimeout 100
<!--NeedCopy-->
```

So legen Sie mithilfe der GUI einen Timeout-Wert für inaktive Client-Verbindungen fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Klicken Sie in **den Erweiterten Einstellungen** auf **Verkehrseinstellungen**und legen Sie den Wert für das Client-Leerlauf-Timeout in Sekunden fest.

RTSP-Verbindungen verwalten

May 11, 2023

Die NetScaler-Appliance kann eine von zwei Topologien verwenden — den NAT-On-Modus oder den NAT-Off-Modus —, um den Lastausgleich auf RTSP-Servern vorzunehmen. Im NAT-on-Modus ist Network Address Translation (NAT) auf der Appliance aktiviert und konfiguriert. Sowohl RTSP-Anfragen als auch Antworten werden durch die Appliance geleitet. Daher müssen Sie die Appliance so konfigurieren, dass die Netzwerkadressübersetzung (Network Address Translation, NAT) durchgeführt wird, um die Datenverbindung zu identifizieren.

Weitere Informationen zum Aktivieren und Konfigurieren von NAT finden Sie unter IP-Adressierung.

Im NAT-Aus-Modus ist NAT nicht aktiviert und konfiguriert. Die Appliance empfängt RTSP-Anfragen vom Client und leitet sie mithilfe der konfigurierten Load-Balancing-Methode an den Dienst weiter,

den sie auswählt. Die RTSP-Server mit Lastausgleich senden ihre Antworten direkt an den Client und umgehen dabei die Appliance. Daher müssen Sie die Appliance so konfigurieren, dass der DSR-Modus (Direct Server Return) verwendet wird, und den RTSP-Servern öffentlich zugängliche FQDNs in DNS zuweisen.

Weitere Informationen zum Aktivieren und Konfigurieren des DSR-Modus finden Sie unter Konfigurieren des Lastenausgleichs im Rückgabemodus für Direktserver. Weitere Informationen zum Konfigurieren von DNS finden Sie unter Domänennamensystem. In beiden Fällen müssen Sie bei der Konfiguration des RTSP-Lastenausgleichs auch Rtspnat so konfigurieren, dass er der Topologie des Lastausgleichs entspricht.

So konfigurieren Sie RTSP NAT mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name>  -RTSPNAT <ValueOfRTSPNAT>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vserver-LB-1  -RTSPNAT ON
<!--NeedCopy-->
```

So konfigurieren Sie RTSP-NAT mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen Server vom Typ RTSP.
2. Klicken Sie unter Erweiterte Einstellungen auf **Verkehrseinstellungen**, und wählen Sie **RTSP Natting**aus.

Verwalten Sie den Clientdatenverkehr basierend auf der Verkehrsrate

May 11, 2023

Sie können die Datenverkehrsrate überwachen, die durch virtuelle Server mit Lastenausgleich fließt, und das Verhalten der NetScaler Appliance basierend auf der Datenverkehrsrate steuern. Zum Beispiel:

- Drosseln Sie den Verkehrsfluss, wenn er zu hoch ist.
- Cache Informationen basierend auf der Datenverkehrsrate.

- Wenn die Datenverkehrsrate zu hoch ist, leiten Sie überschüssigen Datenverkehr auf einen anderen virtuellen Lastausgleichsserver um.
- Wenden Sie die ratenbasierte Überwachung auf HTTP- und Domainnamen-System-Anfragen (DNS) an.

Weitere Informationen zu zinsbasierten Richtlinien finden Sie unter Zinsbegrenzung.

Verbindung mit Layer-2-Parametern identifizieren

May 11, 2023

Zur Identifizierung einer Verbindung verwendet die NetScaler Appliance im Allgemeinen das 4-Tupel der Client-IP-Adresse, des Clientports, der Ziel-IP-Adresse und des Zielports. Wenn Sie die Option L2-Verbindung aktivieren, werden zusätzlich zum normalen 4-Tupel die Layer-2-Parameter der Verbindung (Kanalnummer, MAC-Adresse und VLAN-ID) verwendet.

Durch die Aktivierung des L2Conn-Parameters für einen virtuellen Lastausgleichsserver können mehrere TCP- und Nicht-TCP-Verbindungen mit demselben 4-Tupel (<source IP>:::<source port><destination IP>:<destination port>) auf der NetScaler-Appliance koexistieren. Die Appliance verwendet sowohl die 4-Tupel- als auch die Layer-2-Parameter, um TCP- und Nicht-TCP-Verbindungen zu identifizieren.

Sie können die L2Conn-Option in den folgenden Szenarien aktivieren:

- Auf der NetScaler-Appliance sind mehrere VLANs konfiguriert, und für jedes VLAN wird eine Firewall eingerichtet.
- Sie möchten, dass der Datenverkehr, der von den Servern in einem VLAN stammt und an einen virtuellen Server in einem anderen VLAN gebunden ist, die für beide VLANs konfigurierten Firewalls passiert.

Wenn daher eine nCore NetScaler-Appliance, auf der der L2Conn-Parameter für einen oder mehrere virtuelle Lastausgleichsserver festgelegt ist, auf einen Classic-Build oder auf einen nCore-Build herabgestuft wird, der den L2Conn-Parameter nicht unterstützt, werden die Lastausgleichskonfigurationen, die den L2Conn-Parameter verwenden, unwirksam.

So konfigurieren Sie die L2-Verbindungsoption mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <serviceType> <IPAddress>@ <port> -l2Conn ON
<!--NeedCopy-->
```


Beispiel

```
 add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -l2Conn ON
<!--NeedCopy-->
```

So konfigurieren Sie die L2-Verbindungsoption mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option Verkehrseinstellungen und dann Layer-2-Parameter aus.

Konfigurieren Sie die Option Direkte Route bevorzugen

May 11, 2023

Wenn Sie auf einem virtuellen Wildcard-Load Balancing Server explizit eine Route zu einem Ziel konfigurieren, leitet die NetScaler Appliance den Datenverkehr entsprechend der konfigurierten Route weiter. Wenn Sie möchten, dass die Appliance nicht nach der konfigurierten Route sucht, können Sie die Option Direktroute bevorzugen auf NEIN setzen.

Wenn ein Gerät direkt mit einer NetScaler-Appliance verbunden ist, leitet die Appliance den Datenverkehr direkt an das Gerät weiter. Wenn das Ziel eines Pakets beispielsweise eine Firewall ist, muss das Paket nicht über eine andere Firewall weitergeleitet werden. Manchmal möchten Sie jedoch möglicherweise, dass der Datenverkehr durch die Firewall fließt, selbst wenn das Gerät direkt mit ihm verbunden ist. In solchen Fällen können Sie die Option Direkte Route bevorzugen auf NO setzen.

Hinweis: Die Einstellung PreferDirectRoute gilt für alle virtuellen Platzhalterserver auf der NetScaler Appliance.

So legen Sie die Option Direkte Route bevorzugen mit der CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb parameter -preferDirectRoute (YES | NO)
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -preferDirectRoute YES
<!--NeedCopy-->
```


So legen Sie die Option Direkte Route bevorzugen mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren**.
2. Wählen Sie Direkte Route bevorzugen.

Verwenden Sie einen Quellport aus einem bestimmten Portbereich für Back-End-Kommunikation

May 11, 2023

Standardmäßig kommuniziert die NetScaler Appliance bei Konfigurationen mit deaktivierter USIP-Option oder mit aktivierten Proxy-Port-Optionen mit den Servern über einen zufälligen Quellport (größer als 1024).

Die Appliance unterstützt die Verwendung eines Quellports aus einem angegebenen Portbereich für die Kommunikation mit den Servern. Einer der Anwendungsfälle dieser Funktion ist Server, die so konfiguriert sind, dass sie den empfangenen Datenverkehr, der zu einem bestimmten Satz gehört, basierend auf dem Quellport für Protokollierungs- und Überwachungszwecke identifizieren. Beispiel: Identifizieren des internen und externen Datenverkehrs für Protokollierungszwecke.

Die NetScaler-Appliance so zu konfigurieren, dass sie einen Quellport aus einem Portbereich für die Kommunikation mit den Servern verwendet, umfasst die folgenden Aufgaben:

- **Erstellen Sie ein Netzprofil und legen Sie den Quellportbereichsparameter**fest. Ein Quellportbereichsparameter gibt einen oder mehrere Portbereiche an. Die Appliance wählt nach dem Zufallsprinzip einen der freien Ports aus den angegebenen Portbereichen aus und verwendet ihn als Quellport für jede Verbindung zu Servern.
- **Binden Sie das Netzprofil an den Lastenausgleich von virtuellen Servern, Diensten oder Dienstgruppen**: Ein Netzprofil mit Quellportbereichseinstellung kann an einen virtuellen Server, einen Dienst oder eine Dienstgruppe einer Lastausgleichskonfiguration gebunden werden. Für eine Verbindung mit einem virtuellen Server wählt die Appliance nach dem Zufallsprinzip einen der freien Ports aus den angegebenen Portbereichen eines Netzprofils aus und verwendet diesen Port als Quellport für die Verbindung mit einem der gebundenen Server.

So geben Sie einen Quellportbereich oder -bereiche mit der CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
bind netProfile <name> (-srcPortRange <int[-int]> ...)

show netprofile <name>
```



```
<!--NeedCopy-->
```

Um einen oder mehrere Quellportbereiche mithilfe der GUI anzugeben

1. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile**.
2. Stellen Sie den Parameter **Source Port Range** ein, während Sie NetProfiles hinzufügen oder ändern.

Beispielkonfiguration

In der folgenden Beispielkonfiguration verfügt das Netzprofil PARTIAL-NAT-1 über teilweise NAT-Einstellungen und ist an den virtuellen Lastausgleichsserver LBVS-1 gebunden, der vom Typ ANY ist. Für Pakete, die von 192.0.0.0/8 auf LBVS-1 empfangen wurden, übersetzt die NetScaler-Appliance das letzte Oktett der Quell-IP-Adresse des Pakets in 100. Ein Paket mit Quell-IP-Adresse 192.0.2.30, das auf LBVS-1 empfangen wurde, übersetzt die NetScaler Appliance die Quell-IP-Adresse in 100.0.2.30, bevor sie einen der gebundenen Server sendet.

```
```
> add netprofile CUSTOM-SRCPORT-NP-1
Done
> bind netprofile CUSTOM-SRCPRT-NP-1 - srcportrange 2000-3000

Done
> bind netprofile CUSTOM-SRCPRT-NP-1 - srcportrange 5000-6000

Done
> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1

Done
<!--NeedCopy--> ```
```

## Konfigurieren der Quell-IP-Persistenz für Back-End-Kommunikation

May 11, 2023

Standardmäßig verwendet die NetScaler Appliance für eine Lastausgleichskonfiguration mit deaktivierter USIP-Option und einem Netzprofil, das an einen virtuellen Server oder Dienste oder Dienstgruppen gebunden ist, den Roundrobin-Algorithmus, um eine IP-Adresse aus dem Netzprofil für die Kommunikation mit den Servern auszuwählen. Aufgrund dieser Auswahlmethode kann die ausgewählte IP-Adresse für verschiedene Sitzungen eines bestimmten Clients unterschiedlich sein.

 
```

Einige Situationen erfordern, dass die NetScaler Appliance den gesamten Datenverkehr eines bestimmten Clients von derselben IP-Adresse leitet, wenn der Datenverkehr an Server gesendet wird. Die Server können dann beispielsweise Datenverkehr, der zu einem bestimmten Satz gehört, für Protokollierungs- und Überwachungszwecke identifizieren.

Die Quell-IP-Persistenzoption eines Netzprofils ermöglicht es der NetScaler-Appliance, dieselbe im Netzprofil angegebene Adresse zu verwenden, um mit Servern über alle Sitzungen zu kommunizieren, die von einem bestimmten Client zu einem virtuellen Server initiiert wurden.

So aktivieren Sie die Quell-IP-Persistenz in einem Netzprofil mithilfe der CLI

Um die Quell-IP-Persistenz beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie an der Befehlszeile Folgendes ein:

```
add netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Um die Quell-IP-Persistenz in einem vorhandenen Netzprofil zu aktivieren, geben Sie an der Befehlszeile Folgendes ein:

```
set netProfile <name> -srcippersistency ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

So aktivieren Sie die Quell-IP-Persistenz in einem Netzprofil mithilfe der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile**.
2. Wählen Sie **Quell-IP-Persistenz** aus, während Sie ein Netzprofil hinzufügen oder ändern.

Beispiel

In der folgenden Beispielkonfiguration hat Netprofil NETPROFILE-IPPRSTNCY-1 die Quell-IP-Persistenzoption aktiviert und ist an den Lastenausgleich des virtuellen Servers LBVS-1 gebunden.

Die NetScaler Appliance verwendet immer dieselbe IP-Adresse (in diesem Beispiel 192.0.2.11), um mit Servern zu kommunizieren, die an LBVS-1 gebunden sind, für alle Sitzungen, die von einem bestimmten Client zum virtuellen Server initiiert wurden.

```
```



```
> add ipset IPSET-1

Done
> bind ipset IPSET-1 192.0.2.[11-15]
 IPAddress "192.0.2.11" bound
 IPAddress "192.0.2.12" bound
 IPAddress "192.0.2.13" bound
 IPAddress "192.0.2.14" bound
 IPAddress "192.0.2.15" bound
 Done
> add netprofile NETPROFILE-IPPRSTNCY-1 -srcIp IPSET-1 -
   srcippersistency ENABLED

Done
> set lb vserver LBVS-1 -netprofile NETPROFILE-IPPRSTNCY-1

 Done
<!--NeedCopy--> ```
```

Verwenden Sie lokale IPv6-Linkadressen auf der Serverseite eines Load Balancing-Setups

May 11, 2023

Die lokale IPv6-Link-Adresse wird für Dienste, Dienstgruppen und Server einer Lastausgleichskonfiguration unterstützt. Sie können eine lokale IPv6-Adresse des Links zusammen mit der zugehörigen VLAN-ID in Diensten, Dienstgruppen und Serverkonfigurationen angeben. Die NetScaler Appliance verwendet die lokale SNIP6-Adresse des Links aus demselben VLAN, wie in den Diensten, Dienstgruppen und Serverkonfigurationen angegeben, um mit ihnen zu kommunizieren.

Eine lokale IPv6-Adresse und die zugehörige VLAN-ID werden in Diensten, Dienstgruppen und Serverkonfigurationen im folgenden Format angegeben: `<IPv6_Addrs>%<vlan_id>`

Beispielsweise ist `fe80:123:4567::a%2048:`, `fe80:123:4567::a` die link-lokale Adresse UND 2048 ist die VLAN-ID.

```
> add service SERVICE-1 fe80:123:4567::a%2048 HTTP 80

Done
> bind servicegroup SERVICE-GROUP-1 fe80::1%24 80

Done
```



```
> add server SERVER-1 fe80:b:c:d::e:f:a/64%1028

Done
```

Erweiterte Lastenausgleichseinstellungen

August 19, 2021

Neben der Konfiguration virtueller Server können Sie erweiterte Einstellungen für Dienste konfigurieren.

Informationen zum Konfigurieren der erweiterten Lastenausgleichseinstellungen finden Sie in den folgenden Abschnitten:

- Schrittweise die Last eines neuen Dienstes mit langsamem Start auf virtueller Serverebene erhöhen
- Die Option ohne Monitor für Dienste
- Schützen von Anwendungen auf geschützten Servern vor Überlastung des Datenverkehrs
- Bereinigung von virtuellen Server- und Dienstverbindungen aktivieren
- Ordnungsgemäßes Herunterfahren von Diensten
- Aktivieren oder Deaktivieren der Persistenzsitzung auf TROFS-Diensten
- Direkte Anfragen an eine benutzerdefinierte Webseite
- Zugriff auf Dienste aktivieren, wenn sie deaktiviert sind
- TCP-Pufferung von Antworten aktivieren
- Komprimierung aktivieren
- Verwalten der Clientverbindung für mehrere Clientanforderungen
- IP-Adresse des Clients in den Request-Header einfügen
- Standortdetails von der Benutzer-IP-Adresse mit der Geolocation-Datenbank abrufen
- Verwenden Sie die Quell-IP-Adresse des Clients, wenn Sie eine Verbindung zum Server herstellen
- Konfigurieren des Quellports für serverseitige Verbindungen
- Festlegen eines Grenzwerts für die Anzahl der Clientverbindungen
- Festlegen eines Grenzwerts für die Anzahl der Anforderungen pro Verbindung zum Server
- Festlegen eines Schwellenwerts für die an einen Dienst gebundenen Monitore
- Festlegen eines Timeoutwerts für Leerlauf-Clientverbindungen
- Festlegen eines Zeitüberschreitungswertes für Serververbindungen im Leerlauf
- Festlegen eines Grenzwerts für die Bandbreitenauslastung durch Clients
- Umleiten von Clientanforderungen an einen Cache
- VLAN-Bezeichner für VLAN-Transparenz beibehalten

- Konfigurieren des automatischen Statusübergangs basierend auf dem prozentualen Zustand der gebundenen Dienste

Schrittweise die Last eines neuen Dienstes mit langsamem Start auf virtueller Serverebene erhöhen

May 11, 2023

Sie können die NetScaler Appliance so konfigurieren, dass die Auslastung eines Dienstes (die Anzahl der Anforderungen, die der Dienst pro Sekunde erhält) schrittweise erhöht, nachdem der Dienst entweder zu einer Lastenausgleichskonfiguration hinzugefügt wurde oder eine Statusänderung von DOWN zu UP vorgenommen hat (in diesem Dokument lautet der Begriff “neuer Dienst” wird für beide Situationen verwendet). Sie können die Last entweder manuell mit Lastwerten und Intervallen Ihrer Wahl erhöhen (manueller langsamer Start) oder die Appliance so konfigurieren, dass sie die Last in einem bestimmten Intervall erhöht (automatischer langsamer Start), bis der Dienst so viele Anforderungen erhält wie die anderen Dienste in der Konfiguration. Während der Anlaufphase für den neuen Dienst verwendet die Appliance die konfigurierte Load-Balancing-Methode.

Diese Funktion ist nicht weltweit verfügbar. Es muss für jeden virtuellen Server konfiguriert werden. Die Funktion ist nur für virtuelle Server verfügbar, die eine der folgenden Lastausgleichsmethoden verwenden:

- Round Robin
- Geringste Verbindung
- Geringste Reaktionszeit
- Geringste Bandbreite
- Wenigste Pakete
- LRTM (Methode mit der geringsten Reaktionszeit)
- Benutzerdefiniertes Laden

Für diese Funktion müssen Sie die folgenden Parameter festlegen:

- Die Rate neuer Serviceanfragen. Dies ist der Betrag, um den die Anzahl oder der Prozentsatz der Anfragen, die an einen neuen Dienst gesendet werden, bei jeder Erhöhung der Rate erhöht werden soll. Das heißt, Sie geben die Größe des Inkrements entweder als Anzahl der Anfragen pro Sekunde oder als Prozentsatz der Last an, die zu diesem Zeitpunkt von den vorhandenen Diensten getragen wird. Wenn dieser Wert auf 0 (Null) festgelegt ist, wird der langsame Start für neue Dienste nicht ausgeführt.

  Hinweis: In einem automatisierten Langsamstartmodus ist das letzte Inkrement kleiner als der angegebene Wert, wenn der angegebene Wert den neuen Dienst stärker belasten würde als bei den anderen Diensten.

- Das Inkrementintervall in Sekunden. Wenn dieser Wert auf 0 (Null) gesetzt ist, wird die Last nicht automatisch erhöht. Sie müssen es manuell erhöhen.

Bei einem automatisierten langsamen Start wird ein Dienst aus der langsamen Startphase herausgenommen, wenn eine der folgenden Bedingungen zutrifft:

- Die tatsächliche Anforderungsrate ist niedriger als die neue Serviceanforderungsrate.
- Der Dienst empfängt in drei aufeinanderfolgenden Inkrementintervallen keinen Datenverkehr.
- Die Anforderungsrate wurde um das 200-fache erhöht.
- Der Prozentsatz des Datenverkehrs, den der neue Dienst empfangen muss, ist größer oder gleich 100.

Beim manuellen langsamen Start verbleibt der Dienst in der langsamen Startphase, bis Sie ihn aus dieser Phase herausnehmen.

Manueller langsamer Start

Wenn Sie die Last eines neuen Dienstes manuell erhöhen möchten, geben Sie kein Inkrementintervall für den virtuellen Lastausgleichsserver an. Geben Sie nur die neue Serviceanforderungsrate und die Einheiten an. Ohne Angabe eines Intervalls erhöht die Appliance die Last nicht regelmäßig. Es hält die Last des neuen Dienstes auf dem Wert, der durch die Kombination aus der neuen Serviceanforderungsrate und den Einheiten angegeben wird, bis Sie einen der Parameter manuell ändern. Wenn Sie beispielsweise die neue Dienstanforderungsrate und die Einheitenparameter auf 25 bzw. „pro Sekunde“ festlegen, hält die Appliance die Last für den neuen Dienst bei 25 Anfragen pro Sekunde, bis Sie einen der Parameter ändern. Wenn Sie möchten, dass der neue Dienst den langsamen Startmodus verlässt und so viele Anfragen empfängt wie die vorhandenen Dienste, setzen Sie den neuen Parameter für die Dienstanforderungsrate auf 0.

Nehmen wir als Beispiel an, dass Sie einen virtuellen Server verwenden, um im Round-Robin-Modus zwei Dienste, Service1 und Service2, auszugleichen. Gehen Sie außerdem davon aus, dass der virtuelle Server 240 Anfragen pro Sekunde empfängt und dass er die Last gleichmäßig auf die Dienste verteilt. Wenn der Konfiguration ein neuer Dienst, Service3, hinzugefügt wird, sollten Sie dessen Last möglicherweise manuell durch Werte von 10, 20 und 40 Anfragen pro Sekunde erhöhen, bevor Sie ihm seinen vollen Anteil an der Last senden. Die folgende Tabelle zeigt die Werte, auf die Sie die drei Parameter einstellen.

Tabelle 1. Parameterwerte

Parameter	Wert
Intervall in Sekunden	0
Neue Serviceanforderungsrate	10, 20, 40 und 0, in von Ihnen gewählten Intervallen

Parameter	Wert
Einheiten für die neue Serviceanforderungsrate	Anfragen pro Sekunde

Wenn Sie den neuen Parameter für die Serviceanforderungsrate auf 0 setzen, wird Service3 nicht mehr als neuer Dienst betrachtet und erhält seinen vollen Anteil an der Last.

Gehen Sie davon aus, dass Sie während der Anlaufphase für Service3 einen weiteren Dienst, Service4, hinzufügen. In diesem Beispiel wird Service4 hinzugefügt, wenn der neue Parameter für die Serviceanforderungsrate auf 40 gesetzt ist. Daher beginnt Service4, 40 Anfragen pro Sekunde zu empfangen.

Die folgende Tabelle zeigt die Lastverteilung der Dienste während des in diesem Beispiel beschriebenen Zeitraums.

Tabelle 2. Lastverteilung auf Diensten bei manueller Erhöhung der Last

	neue Serviceanforderungsrate = 10 Anfragen/Sekunde (Service3Added)	neue Serviceanforderungsrate = 20 Anfragen/Sekunde	neue Serviceanforderungsrate = 40 Anfragen/Sekunde (Service4Added)	neue Dienstanforderungsrate = 0 Anfragen/Sekunde (neue Dienste verlassen den langsamen Startmodus)
Service1	115	110	80	60
Service2	115	110	80	60
Service3	10	20	40	60
Service4	-	-	40	60
Gesamtzahl der Anforderungen/Sekunde (Last auf dem virtuellen Server)	240	240	240	240

Automatisierter langsamer Start

Wenn Sie möchten, dass die Appliance die Last eines neuen Dienstes automatisch in bestimmten Intervallen erhöht, bis der Dienst als fähig angesehen werden kann, seinen vollen Anteil der Last zu verarbeiten, legen Sie den neuen Parameter für die Serviceanfrage, den Einheitenparameter und das Inkrementintervall fest. Wenn alle Parameter auf andere Werte als 0 eingestellt sind, erhöht die Appliance die Belastung eines neuen Dienstes im angegebenen Intervall um den Wert der neuen Serviceanforderungsrate, bis der Dienst seinen vollen Anteil an der Last erhält.

Angenommen, vier Dienste, Service1, Service2, Service3 und Service4, sind an einen virtuellen Lastausgleichsserver vserver1 gebunden. Gehen Sie außerdem davon aus, dass vserver1 100 Anfragen pro Sekunde empfängt und die Last gleichmäßig auf die Dienste verteilt (25 Anfragen pro Sekunde pro Dienst). Wenn Sie der Konfiguration einen fünften Dienst, Service5, hinzufügen, möchten Sie möglicherweise, dass die Appliance dem neuen Dienst in den ersten 10 Sekunden 4 Anfragen pro Sekunde, in den nächsten 10 Sekunden 8 Anfragen pro Sekunde usw. sendet, bis sie 20 Anfragen pro Sekunde empfängt. Für diese Anforderung zeigt die folgende Tabelle die Werte, auf die Sie die drei Parameter festlegen:

Tabelle 3. Parameterwerte

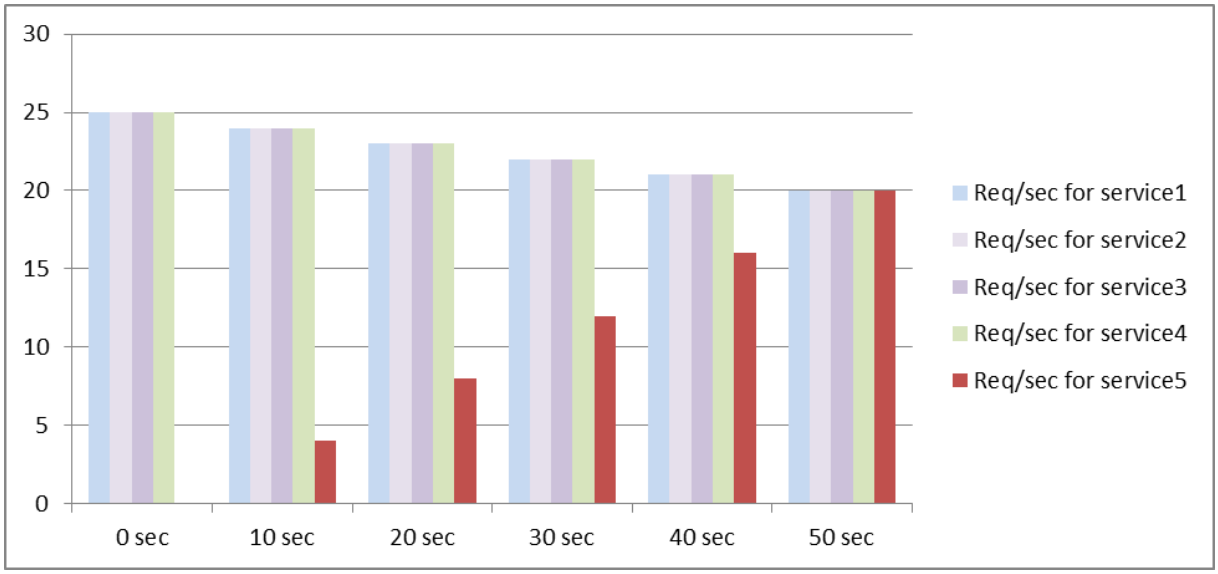
Parameter	**Wert**
Intervall in Sekunden	10
Wert erhöhen	4
Einheiten für die neue Serviceanforderungsrate	Anfragen pro Sekunde

Mit dieser Konfiguration empfängt der neue Dienst 50 Sekunden, nachdem er hinzugefügt wurde oder sein Status von DOWN auf UP geändert wurde, so viele Anfragen wie die vorhandenen Dienste. In jedem Intervall in diesem Zeitraum verteilt die Appliance die überschüssigen Anfragen, die ohne schrittweise Inkremente an den neuen Dienst gesendet worden wären, an die vorhandenen Server. Ohne schrittweise Inkremente hätte beispielsweise jeder Dienst, einschließlich Service5, jeweils 20 Anfragen pro Sekunde erhalten. In schrittweisen Schritten verteilt die Appliance in den ersten 10 Sekunden, wenn Service5 nur 4 Anfragen pro Sekunde empfängt, die überschüssigen 16 Anfragen pro Sekunde an die vorhandenen Dienste, was zu dem in der folgenden Tabelle und Abbildung dargestellten Verteilungsmuster über den Zeitraum von 50 Sekunden führt. Nach Ablauf der 50-Sekunden-Periode wird Service5 nicht mehr als neuer Dienst betrachtet und erhält seinen normalen Anteil am Traffic.

Tabelle 4. Lastverteilungsmuster auf allen Diensten für den Zeitraum von 50 Sekunden unmittelbar nach dem Hinzufügen von Service5

	0 Sekunden	10 Sekunden	20 Sekunden	30 Sekunden	40 Sekunden	50 Sekunden
Anforderung für Service 1	25	24	23	22	21	20
Anforderung/Sekunde für Service 2	25	24	23	22	21	20
Anforderung für Service 3	25	24	23	22	21	20
Anforderung/Sekunde für Service 4	25	24	23	22	21	20
Anforderung für Service 5	0	4	8	12	16	20
Gesamtzahl der Anforderungen/Sekunde (Last auf dem virtuellen Server)	100	100	100	100	100	100

Abbildung 1. Diagramm des Lastverteilungsmusters für alle Dienste für den 50-Sekunden-Zeitraum unmittelbar nach dem Hinzufügen von Service5



Eine alternative Anforderung besteht möglicherweise darin, dass die Appliance Service5 25% der Auslastung der vorhandenen Dienste in den ersten 5 Sekunden, 50% in den nächsten 5 Sekunden usw. sendet, bis 20 Anforderungen pro Sekunde empfangen wird. Für diese Anforderung zeigt die folgende Tabelle die Werte, auf die Sie die drei Parameter festlegen.

Tabelle 5. Parameterwerte

Parameter	Wert
Intervall in Sekunden	5
Wert erhöhen	25
Einheiten für die neue Serviceanforderungsrate	Prozent

Mit dieser Konfiguration empfängt der Dienst 20 Sekunden, nachdem er hinzugefügt wurde oder sein Status von DOWN auf UP geändert wurde, so viele Anfragen wie die vorhandenen Dienste. Die Verkehrsverteilung während der Anlaufphase für den neuen Dienst ist identisch mit der zuvor beschriebenen, wobei die Einheit für die Schrittweite „Anfragen pro Sekunde“ war.

Setze die Parameter für den langsamen Start

Sie legen die Parameter für den langsamen Start fest, indem Sie entweder den Befehl `set lb vserver` oder den `add lb vserver` Befehl verwenden. Der folgende Befehl dient zum Festlegen von langsamen Startparametern beim Hinzufügen eines virtuellen Servers.

So konfigurieren Sie schrittweise Lastinkremente für einen neuen Dienst mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um schrittweise Lasterhöhungen für einen Dienst zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name> <serviceType> <IPAddress> <port> [-
    newServiceRequest <positive_integer>] [<newServiceRequestUnit>] [-
    newServiceRequestIncrementInterval <positive_integer>]

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver BR_LB -newServiceRequest 5 PER_SECOND -
    newServiceRequestIncrementInterval 10
Done

show lb vserver BR_LB
BR_LB (192.0.2.33:80) - HTTP Type: ADDRESS
State: UP
...
...
New Service Startup Request Rate: 5 PER_SECOND, Increment Interval: 10
...
...
Done
<!--NeedCopy-->
```

So konfigurieren Sie schrittweise Lastinkremente für einen neuen Dienst mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option Methode aus und stellen Sie die folgenden Parameter für einen langsamen Start ein:
   - Neue Anforderungsrate für Dienststarts.
   - Neue Service Request Unit.
   - Inkrementierungsintervall.

Kein-Monitor-Option für Dienste

May 11, 2023

Wenn Sie ein externes System verwenden, um Zustandsprüfungen für die Dienste durchzuführen und nicht möchten, dass die NetScaler-Appliance den Zustand eines Dienstes überwacht, können Sie die Option „Keine Überwachung“ für den Dienst festlegen. Wenn Sie dies tun, sendet die Appliance keine Sonden, um den Zustand des Dienstes zu überprüfen, sondern zeigt den Dienst als aktiv an. Selbst wenn der Dienst AUSFÄLLT, sendet die Appliance weiterhin Datenverkehr vom Client an den Dienst, wie in der Load-Balancing-Methode angegeben.

Der Monitor kann sich im Status ENABLED oder DISABLED befinden, wenn Sie die Option „Kein Monitor“ aktivieren. Wenn Sie die Option „Kein Monitor“ entfernen, wird der frühere Status des Monitors wieder aufgenommen.

Sie können die Option „Kein Monitor“ für einen Dienst festlegen, wenn Sie den Dienst erstellen. Sie können die Option „Kein Monitor“ auch für einen vorhandenen Dienst festlegen.

Die Einstellung der Option „Kein Monitor“ hat die folgenden Konsequenzen:

- Wenn ein Dienst, für den Sie die Option „Kein Monitor“ aktiviert haben, ausfällt, zeigt die Appliance den Dienst weiterhin als AKTIV an und leitet den Datenverkehr weiter an den Dienst weiter. Eine dauerhafte Verbindung zum Dienst kann die Situation verschlechtern. In diesem Fall oder wenn viele Dienste, die als UP angezeigt werden, tatsächlich DOWN sind, kann das System fehlschlagen. Um eine solche Situation zu vermeiden, entfernen Sie den Dienst aus der NetScaler-Konfiguration, wenn der externe Mechanismus, der die Dienste überwacht, einen Dienst als DOWN meldet.
- Wenn Sie die Option Kein Monitor für einen Dienst konfigurieren, können Sie den Lastausgleich im Direct Server Return (DSR) -Modus nicht konfigurieren. Wenn Sie für einen vorhandenen Dienst die Option „Kein Monitor“ aktivieren, können Sie den DSR-Modus für den Dienst nicht konfigurieren.

So legen Sie die Option Kein Monitor für einen neuen Dienst mithilfe der Befehlszeilenschnittstelle fest

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen Dienst mit der Option Health Monitor zu erstellen, und überprüfen Sie die Konfiguration:

```
1 add service <serviceName> <IP | serverName> <serviceType> <port> -
     healthMonitor (YES|NO)
2 <!--NeedCopy-->
```

Beispiel:


```
add service nomonsrvc 10.102.21.21 http 80 -healthMonitor no
Done

show service nomonsrvc
nomonsrvc (10.102.21.21:80) - HTTP
State: UP
Last state change was at Mon Nov 15 22:41:29 2010
Time since last state change: 0 days, 00:00:00.970
Server Name: 10.102.21.21
 Server ID : 0 Monitor Threshold : 0
...
Access Down Service: NO
...
Down state flush: ENABLED
Health monitoring: OFF

1 bound monitor:
1) Monitor Name: tcp-default
State: UNKNOWN Weight: 1
Probes: 3 Failed [Total: 3 Current: 3]
Last response: Probe skipped - Health monitoring is turned off.
Response Time: N/A
Done
<!--NeedCopy-->
```

So legen Sie die Option Kein Monitor für einen vorhandenen Dienst mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Option Health Monitor festzulegen:

```
set service <name> -healthMonitor (YES|NO)
<!--NeedCopy-->
```

Beispiel:

```
By default, the state of a service and the state of the corresponding
   monitor are UP.
 >show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP


1) Monitor Name: http-ecv
```



```
 State: UP Weight: 1
Probes: 99992 Failed [Total: 0 Current: 0]
Last response: Success - Pattern found in response.
Response Time: 3.76 millisec
Done

When the no-monitor option is set on a service, the state of the
   monitor changes to UNKNOWN.
set service LB-SVC1 -healthMonitor NO
Done

show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010.
Time since last state change: 5 days, 18:55:48.710
Health monitoring: OFF

1) Monitor Name: http-ecv
   State: UNKNOWN Weight: 1
         Probes: 100028 Failed [Total: 0 Current: 0]
   Last response: Probe skipped - Health monitoring is turned off.
     Response Time: 0.0 millisec
  Done
When the no-monitor option is removed, the earlier state of the monitor
    is resumed.
> set service LB-SVC1 -healthMonitor YES
Done
>show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010
Time since last state change: 5 days, 18:57:47.880
1) Monitor Name: http-ecv
   State: UP Weight: 1
   Probes: 100029 Failed [Total: 0 Current: 0]
   Last response: Success - Pattern found in response.
   Response Time: 5.690 millisec
   Done
<!--NeedCopy-->
```

So stellen Sie die Option „Kein Monitor“ für einen Dienst mithilfe der GUI ein

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.

2. Öffnen Sie den Dienst, und deaktivieren Sie die Integritätsüberwachung.

Anwendungen vor Verkehrsspitzen auf geschützten Servern schützen

May 11, 2023

Die NetScaler-Appliance bietet die Option zum Überspannungsschutz, um die Kapazität eines Servers oder Caches aufrechtzuerhalten. Die Appliance regelt den Fluss von Clientanforderungen an Server und steuert die Anzahl der Clients, die gleichzeitig auf die Server zugreifen können. Die Appliance blockiert alle an den Server übergebenen Überspannungen und verhindert so eine Überlastung des Servers.

Damit der Überspannungsschutz ordnungsgemäß funktioniert, müssen Sie ihn global aktivieren. Weitere Informationen zum Überspannungsschutz finden Sie unter Überspannungsschutz.

So legen Sie Überspannungsschutz für den Dienst mit der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -sp <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -sp ON
<!--NeedCopy-->
```

So richten Sie den Überspannungsschutz für den Dienst mithilfe der GUI ein

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienste**, und öffnen Sie eine Quelle.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Überspannungsschutz**aus.

Bereinigung von virtuellen Server- und Dienstverbindungen ermöglichen

May 11, 2023

Der Status eines virtuellen Servers hängt vom Status der an ihn gebundenen Dienste ab. Der Status der einzelnen Dienste hängt von den Reaktionen der Server mit Lastausgleich auf Tests oder Integritätsprüfungen ab, die von den Monitoren gesendet werden, die an diesen Dienst gebunden sind. Manchmal reagieren die Server mit Lastausgleich nicht. Wenn ein Server langsam oder ausgelastet ist, kann es bei den Überwachungstests zu einem Timeout kommen. Wenn wiederholte Überwachungssonden nicht innerhalb der konfigurierten Zeitüberschreitungszeit beantwortet werden, wird der Dienst mit DOWN gekennzeichnet. Wenn ein Dienst oder virtueller Server als DOWN gekennzeichnet ist, müssen die server- und clientseitigen Verbindungen geleert werden. Durch das Beenden vorhandener Verbindungen werden Ressourcen freigegeben und in bestimmten Fällen wird die Wiederherstellung überlasteter Lastausgleichseinstellungen beschleunigt.

Unter bestimmten Bedingungen können Sie die Einstellung **DownStateFlush** so konfigurieren, dass vorhandene Verbindungen sofort beendet werden, wenn ein Dienst oder ein virtueller Server als DOWN markiert ist. Aktivieren Sie die DownStateFlush-Einstellung nicht auf den Anwendungsservern, die ihre Transaktionen abschließen müssen. Sie können diese Einstellung auf Webservern aktivieren, deren Verbindungen sicher beendet werden können, wenn sie DOWN markiert haben.

In der folgenden Tabelle werden die Auswirkungen dieser Einstellung auf eine Beispielkonfiguration zusammengefasst, die aus einem virtuellen Server, vServer-LB-1, mit einem daran gebundenen Dienst, Service-1, besteht. In der Tabelle bezeichnen E und D den Status der DownStateFlush-Einstellung: E bedeutet Aktiviert und D bedeutet Deaktiviert.

Vserver-LB-1	Service-1	Status der Verbindungen
E	E	Sowohl Client- als auch Serververbindungen werden beendet.

Vserver-LB-1	Service-1	Status der Verbindungen
E	D	Bei einigen Diensttypen wie TCP, für die die NetScaler-Appliance die Wiederverwendung von Verbindungen nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung von Verbindungen unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn auf diesen Verbindungen eine Transaktion aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Client-Verbindungen beendet.

Vserver-LB-1	Service-1	Status der Verbindungen
D	E	Bei einigen Diensttypen wie TCP, für die die NetScaler-Appliance die Wiederverwendung von Verbindungen nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung von Verbindungen unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn auf diesen Verbindungen eine Transaktion aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Serververbindungen beendet.
D	D	Weder Client- noch Serververbindungen werden beendet.

Wenn Sie einen Dienst nur deaktivieren möchten, wenn alle etablierten Verbindungen vom Server oder vom Client geschlossen werden, können Sie die Option ordnungsgemäßes Herunterfahren verwenden. Informationen zum ordnungsmäßigen Herunterfahren eines Dienstes finden Sie unter Graceful Shutdown of Services.

So legen Sie Down State Flush auf dem Dienst mit der CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Beispiel:


```
set service Service-HTTP-1 -downStateFlush enabled
<!--NeedCopy-->
```

Um den Status Flush für den Dienst mithilfe der GUI festzulegen

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Nach unten Status Flush**aus.

So richten Sie State Flush auf dem virtuellen Server mithilfe der CLI ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vsvr1 -downStateFlush enabled
<!--NeedCopy-->
```

So richten Sie State Flush auf dem virtuellen Server mithilfe der GUI ein

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Nach unten Status Flush**aus.

Ordnungsgemäßes Herunterfahren von Diensten

May 11, 2023

Bei geplanten Netzwerkausfällen wie Systemupgrades oder Hardwarewartungen müssen Sie möglicherweise einige Dienste schließen oder deaktivieren. Sie können den Dienst später aktivieren, indem Sie den Befehl “enable service <name> verwenden.

Um zu vermeiden, dass bestehende Sitzungen unterbrochen werden, können Sie einen Dienst in den Status Transition Out of Service (TROFS) versetzen, indem Sie einen der folgenden Schritte ausführen:

- Hinzufügen eines TROFS-Codes oder einer Zeichenfolge zum Monitor — Konfigurieren Sie den Server so, dass er als Antwort an eine Monitorsonde einen bestimmten Code oder eine bestimmte Zeichenfolge sendet.
- Deaktiviere den Dienst explizit und:
  - Stellen Sie eine Verzögerung (in Sekunden) ein.
  - Aktivieren Sie das ordnungsgemäße Herunterfahren.

Hinzufügen eines TROFS-Codes oder einer Zeichenfolge

Wenn Sie nur einen Monitor an einen Dienst binden und der Monitor TROFS-fähig ist, kann er den Dienst auf der Grundlage der Antwort des Servers auf eine Monitorprobe in den TROFS-Status versetzen. Diese Antwort wird mit dem Wert im trofsCode-Parameter für einen HTTP-Monitor oder dem trofsString-Parameter für einen HTTP-ECV- oder TCP-ECV-Monitor verglichen. Wenn der Code übereinstimmt, wird der Dienst in den TROFS-Status versetzt. In diesem Zustand werden die persistenten Verbindungen weiterhin berücksichtigt.

Wenn mehrere Monitore an einen Dienst gebunden sind, wird der effektive Status des Dienstes auf der Grundlage des Status aller Monitore berechnet, die an den Dienst gebunden sind. Nach Erhalt einer TROFS-Antwort wird der Status des TROFS-fähigen Monitors für die Zwecke dieser Berechnung als UP angesehen. Weitere Informationen darüber, wie eine NetScaler Appliance einen Dienst als UP bezeichnet, finden Sie unter Festlegen eines Schwellenwerts für die an einen Dienst gebundenen Monitore.

Wichtig:

- Sie können mehrere Monitore an einen Dienst binden, dürfen jedoch nicht mehr als einen von ihnen TROFS-fähig machen.
- Sie können einen TROFS-fähigen Monitor in einen Monitor konvertieren, der nicht TROFS-fähig ist, aber nicht umgekehrt.

So konfigurieren Sie einen TROFS-Code oder eine Zeichenfolge in einem Monitor mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add lb monitor <monitor-name> HTTP -trofsCode <respcode>

add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>

add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
<!--NeedCopy-->
```


So ändern Sie den TROFS-Code oder die TROFS-Zeichenfolge mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
set lb monitor <trofs monitorname> HTTP -trofscode <newcode>

set lb monitor <trofs monitorname> HTTP-ECV -trofsstring <new string>

set lb monitor <trofs monitorname> TCP-ECV -trofsstring <new string>
<!--NeedCopy-->
```

Hinweis: Sie können den Befehl set nur verwenden, wenn zuvor ein TROFS-fähiger Monitor hinzugefügt wurde. Sie können diesen Befehl nicht verwenden, um den TROFS-Code oder die TROFS-Zeichenfolge für einen Monitor festzulegen, der nicht TROFS-fähig ist.

So konfigurieren Sie einen TROFS-Code oder eine TROFS-Zeichenfolge in einem Monitor mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.
2. Klicken Sie im Bereich Monitore auf Hinzufügen und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie Typ als HTTP aus und geben Sie einen TROFS-Code an.
   - Wählen Sie Typ als HTTP-ECV oder TCP-ECV aus, und geben Sie einen TROFS-String an.

Deaktivierung eines Dienstes

Oft können Sie jedoch nicht abschätzen, wie viel Zeit alle Verbindungen zu einem Dienst benötigen, um die bestehenden Transaktionen abzuschließen. Wenn eine Transaktion nach Ablauf der Wartezeit noch nicht abgeschlossen ist, kann das Herunterfahren des Dienstes zu Datenverlust führen. In diesem Fall können Sie das ordnungsgemäße Herunterfahren des Dienstes festlegen, sodass der Dienst nur deaktiviert wird, wenn alle aktuellen aktiven Client-Verbindungen entweder vom Server oder vom Client geschlossen werden. In der folgenden Tabelle finden Sie Informationen zum Verhalten, wenn Sie zusätzlich zum ordnungsgemäßen Herunterfahren eine Wartezeit angeben.

Die Persistenz wird gemäß der angegebenen Methode aufrechterhalten, auch wenn Sie das ordnungsgemäße Herunterfahren aktivieren. Das System bedient weiterhin alle persistenten Clients, einschließlich neuer Verbindungen von den Clients, es sei denn, der Dienst wird während des ordnungsgemäßen Herunterfahrens als Ergebnis der von einem Monitor durchgeführten Prüfungen auf DOWN markiert.

In der folgenden Tabelle werden die Optionen zum ordnungsmäßigen Herunterfahren beschrieben.

State	Ergebnisse
Das ordnungsgemäße Herunterfahren ist aktiviert und eine Wartezeit ist angegeben.	Der Dienst wird beendet, nachdem die letzte der aktuell aktiven Client-Verbindungen bedient wurde, auch wenn die Wartezeit noch nicht abgelaufen ist. Die Appliance überprüft den Status der Verbindungen einmal pro Sekunde. Wenn die Wartezeit abläuft, werden alle offenen Sitzungen geschlossen.
Das ordnungsgemäße Herunterfahren ist deaktiviert und eine Wartezeit ist angegeben.	Der Dienst wird erst nach Ablauf der Wartezeit heruntergefahren, auch wenn alle hergestellten Verbindungen vor Ablauf bedient werden.
Das ordnungsgemäße Herunterfahren ist aktiviert und es wurde keine Wartezeit angegeben.	Der Dienst wird erst beendet, nachdem die letzte der zuvor hergestellten Verbindungen bedient wurde, unabhängig von der Zeit, die für die Bereitstellung der letzten Verbindung benötigt wurde.
Das ordnungsgemäße Herunterfahren ist deaktiviert und es wurde keine Wartezeit angegeben.	Kein anmutiges Herunterfahren. Der Dienst wird sofort beendet, nachdem die Deaktivierungsoption ausgewählt oder der Befehl zum Deaktivieren ausgegeben wurde. (Die Standardwartezeit beträgt Null Sekunden.)

Um vorhandene Verbindungen zu beenden, wenn ein Dienst oder ein virtueller Server als DOWN markiert ist, können Sie die Option Down-State-Flush verwenden. Weitere Informationen finden Sie unter Bereinigung virtueller Serververbindungen aktivieren.

So konfigurieren Sie ein ordnungsgemäßes Herunterfahren für einen Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen Dienst ordnungsgemäß herunterzufahren und die Konfiguration zu überprüfen:

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```


Beispiel:

```
> disable service svc1 6000 -graceFul YES
Done
>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: GOING OUT OF SERVICE (Graceful, Out Of Service in 5998 seconds)
Last state change was at Mon Nov 15 22:44:15 2010
Time since last state change: 0 days, 00:00:01.160
...
Down state flush: ENABLED

1 bound monitor:
1) Monitor Name: tcp-default
State: UP              Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - live traffic to service.
Response Time: N/A
Done

>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: OUT OF SERVICE
Last state change was at Mon Nov 15 22:44:19 2010
Time since last state change: 0 days, 00:00:03.250
Down state flush: ENABLED

1 bound monitor:
1)  Monitor Name: tcp-default
State: UNKNOWN           Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - service state OFS.
Response Time: N/A
Done
<!--NeedCopy-->
```

So konfigurieren Sie das ordnungsgemäße Herunterfahren eines Dienstes mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Öffnen Sie den Dienst und klicken Sie in der Aktionsliste auf Deaktivieren. Geben Sie eine Wartezeit ein und wählen Sie Graceful aus.

Aktivieren oder Deaktivieren der Persistenzsitzung auf TROFS-Diensten

August 19, 2021

Sie können das TrofsPersistence-Flag festlegen, um anzugeben, ob ein Dienst im Status Transition Out of Service (TROFS) persistente Sitzungen beibehalten muss. Wenn ein Monitor TROFS aktiviert ist, kann er einen Dienst auf der Grundlage der Antwort des Servers auf einen Monitor Probe in den TROFS-Status versetzen. Diese Antwort wird mit dem Wert im Parameter TrofsCode für einen HTTP-Monitor oder dem Parameter TrofsString für einen HTTP-ECV oder TCP-ECV Monitor verglichen. Wenn der Code übereinstimmt, wird der Dienst in den TROFS-Status abgelegt. In diesem Zustand werden die aktiven Clientverbindungen weiterhin berücksichtigt. In einigen Fällen müssen die geehrten aktiven Sitzungen möglicherweise dauerhafte Sitzungen enthalten. In anderen Fällen, insbesondere solchen, die langlebige Persistenzsitzungen oder Persistenzmethoden wie benutzerdefinierte Server-ID beinhalten, kann die Einhaltung der persistenten Sitzungen jedoch verhindern, dass der Dienst in den Out-of-Service-Status übergeht.

Wenn Sie das TROFSPersistence-Flag auf ENABLED setzen, werden persistente Sitzungen berücksichtigt. Wenn Sie es auf DEAKTIVIERT setzen, sind sie dies nicht.

So legen Sie das TROFSPersistence-Flag mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um das`trofsPersistence` Flag für einen neuen virtuellen Server oder einen vorhandenen virtuellen Server festzulegen oder um die Einstellung auf den Standardwert zurückzusetzen:

```
add lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

set lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

unset lb vserver <name> [-trofsPersistence]
<!--NeedCopy-->
```

Argument

trofsPersistence. Beachten Sie aktuelle aktive Clientverbindungen und neue Anforderungen für Persistenzsitzungen, wenn sich der Dienst im TROFS-Status befindet.

Mögliche Werte: ENABLED, DISABLED. Standard: ENABLED.

Beispiele:

```
add lb vserver v1 http 10.102.217.42 80 -persistencetype SOURCEIP -
    trofsPersistence ENABLED
```



```
2
3 set lb vserver v1 -trofsPersistence DISABLED
4
5 unset lb vserver v1 -trofsPersistence
6 <!--NeedCopy-->
```

Direkte Anfragen an eine benutzerdefinierte Webseite

May 11, 2023

> **Warnung**
>
> SureConnect (SC) ist ab NetScaler 12.0 Build 56.20 veraltet. Alternativ empfiehlt Citrix die Verwendung der AppQOE-Funktion. Weitere Informationen finden Sie unterAppQOE.

Damit SureConnect richtig funktioniert, müssen Sie es global festlegen. NetScaler stellt die SureConnect Option bereit, um die Antwort einer Anwendung sicherzustellen.

So legen Sie SureConnect für den Dienst mit der CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set service <name> -sc <Value>
2 <!--NeedCopy-->
```

Beispiel:

```
1 set service Service-HTTP-1 -sc ON
2 <!--NeedCopy-->
```

So richten Sie SureConnect mithilfe der GUI für den Dienst ein

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option Verkehrseinstellungen aus und wählen Sie **Sicher Verbinden**aus.

Zugriff auf Dienste bei Ausfall ermöglichen

May 11, 2023

Sie können den Zugriff auf einen Dienst aktivieren, wenn er deaktiviert ist oder sich im Status DOWN befindet, indem Sie die NetScaler-Appliance so konfigurieren, dass sie den Layer-2-Modus verwendet, um die an den Dienst gesendeten Pakete zu überbrücken. Normalerweise werden die Anforderungspakete verworfen, wenn Anfragen an Dienste weitergeleitet werden, die NICHT verfügbar sind. Wenn Sie die Einstellung **Access Down** aktivieren, werden diese Anforderungspakete jedoch direkt an die Server mit Lastausgleich gesendet.

Weitere Informationen zu den Modi Layer 2 und Layer 3 finden Sie unter IP-Adressierung.

Damit die Appliance Pakete überbrückt, die an die DOWN-Services gesendet werden, aktivieren Sie den Layer-2-Modus mit dem AccessDown-Parameter.

So aktivieren Sie den Zugriff auf einen Dienst mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -accessDown <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -accessDown YES
<!--NeedCopy-->
```

So aktivieren Sie den Zugriff auf einen Dienst mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Zugriff nach unten**aus.

TCP-Pufferung von Antworten aktivieren

May 11, 2023

Die NetScaler-Appliance bietet eine TCP-Pufferoption, die nur Antworten vom Server mit Lastausgleich zwischenspeichert. Auf diese Weise kann die Appliance Serverantworten an den Client mit der maximalen Geschwindigkeit übermitteln, die der Client sie akzeptieren kann. Die Appliance weist 0 bis 4095 MB (MB) Speicher für TCP-Pufferung und von 4 bis 20480 Kilobyte (KB) Speicher pro Verbindung zu.

Hinweis: TCP-Pufferung auf Service-Ebene hat Vorrang vor der globalen Einstellung.
Weitere Informationen zum globalen Konfigurieren von TCP-Pufferung finden Sie unter TCP-Pufferung.

So aktivieren Sie die TCP-Pufferung für einen Dienst mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -TCPB <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -TCPB YES
<!--NeedCopy-->
```

So aktivieren Sie TCP-Pufferung für einen Dienst mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **TCP-Pufferung**aus.

Komprimierung aktivieren

May 11, 2023

Die NetScaler Appliance bietet eine Komprimierungsoption zum transparenten Komprimieren von HTML- und Textdateien mithilfe einer Reihe integrierter Komprimierungsrichtlinien. Die Komprimierung reduziert die Bandbreitenanforderungen und kann die Reaktionsfähigkeit des Servers in Umgebungen mit begrenzter Bandbreite erheblich verbessern. Die Komprimierungsrichtlinien sind mit Diensten verknüpft, die an den virtuellen Server gebunden sind. Die Richtlinien legen fest, ob eine Antwort komprimiert werden kann und komprimierbarer Inhalt an die Appliance gesendet werden kann, die ihn komprimiert und an den Client sendet.

Hinweis: Damit die Komprimierung ordnungsgemäß funktioniert, müssen Sie sie global aktivieren. Weitere Informationen zum globalen Konfigurieren der Komprimierung finden Sie unter Komprimierung.

So aktivieren Sie die Komprimierung für einen Dienst mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -CMP <YES | NO>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -CMP YES
<!--NeedCopy-->
```

So aktivieren Sie die Komprimierung eines Dienstes über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Komprimierung**aus.

Aktivieren Sie die externe Zustandsprüfung für virtuelle UDP- und Nicht-HTTP-Server

September 18, 2023

In öffentlichen Clouds können Sie die NetScaler Appliance als Load Balancer der zweiten Stufe verwenden, wenn der native Load Balancer als erste Stufe verwendet wird. Der native Load Balancer kann ein Application Load Balancer (ALB) oder ein Netzwerklastenausgleichsmodul (NLB) sein. Die meisten Public Clouds unterstützen keine UDP Health Probes in ihren nativen Load Balancern. Wenn diese Server ausgefallen sind, wird ihr aktueller Status daher möglicherweise nicht aktualisiert. Infolgedessen wird der Datenverkehr bedingungslos an NetScaler gesendet, auch wenn die Anforderung nicht bearbeitet werden kann.
Um den Zustand solcher Anwendungen zu überwachen, unterstützt NetScaler HTTP- und TCP-Integritätsprüfungen.

Ein HTTP- oder TCP-Listener wird für einen virtuellen Content Switching-Server erstellt, wenn `probeProtocol` sowohl die als auch die `probePort` Parameter konfiguriert sind. Der Listener spiegelt den Status des virtuellen Servers wider. Der `ProbeSuccessResponseCode` Parameter gilt nur für HTTP und gibt die konfigurierte Zeichenfolge zurück, wenn der Test erfolgreich ist.

So aktivieren Sie die externe Integritätsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server mithilfe der CLI

Geben Sie an der Befehlszeile Folgendes ein:

```
add lb vserver <name> <serviceType> <IPAddress> <port> -ProbeProtocol <
   HTTP/TCP> -ProbePort <port-num> -ProbeSuccessResponseCode<http-code>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-UDP-1 HTTP 10.102.29.60 80 -ProbeProtocol TCP -
   probeport 5000 -probesuccessResponseCode 200ok
<!--NeedCopy-->
```

So aktivieren Sie die externe Integritätsprüfung für virtuelle UDP- und Nicht-HTTP-TCP-Server mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und erstellen Sie dann einen virtuellen Server.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Server zu erstellen.
3. Aktualisieren Sie im Bereich **Grundeinstellungen** die folgenden Details:
   a) Prüfprotokoll — Wählen Sie das Protokoll (HTTP oder TCP) der Sonde für die externe Zustandsprüfung des virtuellen Servers aus.
   b) Test Success Response Code — Geben Sie die Antwortzeichenfolge für eine erfolgreiche Prüfung ein. Dieser Parameter gilt nur für das HTTP-Protokoll.
      - Standardwert: 200ok
      - Maximale Länge: 63
   c) Probe Port — Geben Sie die Portnummer für die HTTP- oder TCP-Überwachung ein.
4. Klicken Sie auf **OK**.

Clientverbindung für mehrere Clientanforderungen verwalten

May 11, 2023

Sie können den Keepalive-Parameter des Clients festlegen, um einen HTTP- oder SSL-Dienst so zu konfigurieren, dass eine Clientverbindung zu einer Website über mehrere Clientanforderungen hinweg geöffnet bleibt. Wenn Client Keep-Alive aktiviert ist, selbst wenn der Webserver mit Lastausgleich eine Verbindung schließt, hält die NetScaler Appliance die Verbindung zwischen dem Client und

sich selbst offen. Diese Einstellung ermöglicht es Diensten, mehrere Clientanforderungen auf einer einzelnen Clientverbindung zu bedienen.

Wenn Sie diese Einstellung nicht aktivieren, öffnet der Client für jede Anfrage, die er an die Website sendet, eine neue Verbindung. Die Client-Keepalive-Einstellung speichert die Paket-Round-Trip-Zeit, die zum Herstellen und Schließen von Verbindungen erforderlich ist. Diese Einstellung reduziert auch die Zeit bis zum Abschluss jeder Transaktion. Client Keep-Alive kann nur für HTTP- oder SSL-Diensttypen aktiviert werden.

Client-Keepalive-Einstellung auf Service-Ebene hat Vorrang vor der globalen Client-Keepalive-Einstellung. Weitere Informationen über das Keep-Alive des Clients finden Sie unter Client Keep-Alive.

So aktivieren Sie den Client Keep-Alive für einen Dienst über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -CKA <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -CKA YES
<!--NeedCopy-->
```

So aktivieren Sie den Client Keep-Alive für einen Dienst über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Client Keep-Alive**aus.

IP-Adresse des Clients in den Anforderungsheader einfügen

May 11, 2023

Ein NetScaler verwendet die Subnetz-IP-Adresse (SNIP), um eine Verbindung zum Server herzustellen. Der Server muss den Client nicht kennen.

In einigen Situationen muss der Server jedoch wissen, welchen Client er bedienen muss. Wenn Sie die Client-IP-Einstellung aktivieren, fügt die Appliance die IPv4- oder IPv6-Adresse des Clients ein und leitet die Anfragen an den Server weiter. Der Server fügt diese Client-IP in den Header der Antworten ein. Der Server ist sich des Clients also bewusst.

> **Hinweis**: Um mehrere Header einzufügen, müssen Sie einen der folgenden Schritte ausführen:
>
> - Fügen Sie Rewrite-Richtlinien hinzu, um CLIENT.IS_SSL zu überprüfen, und fügen Sie den entsprechenden Header ein.
> - Binden Sie die entsprechende Rewrite-Richtlinie für jeden virtuellen Server basierend auf dem Typ.

So fügen Sie die Client-IP-Adresse über die Befehlszeilenschnittstelle in die Clientanfrage ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -CIP <Value> <cipHeader>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -CIP enabled X-Forwarded-For
<!--NeedCopy-->
```

So fügen Sie die Client-IP-Adresse über die grafische Benutzeroberfläche in die Clientanfrage ein

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, und bearbeiten Sie einen Service.
2. Klicken Sie im Bereich **Diensteinstellungen** auf das **Symbol Bearbeiten**.
3. Aktivieren Sie im Bereich **Load Balancing Service** das Kontrollkästchen **Client-IP-Adresse einfügen** .

Standortdetails von der Benutzer-IP-Adresse mit der Geolokalisierungsdatenbank abrufen

May 11, 2023

> **Hinweis** Diese Funktion ist ab NetScaler Version 12.1 Build 50.x und höher verfügbar.

Die NetScaler-Appliance kann Benutzerstandortdetails wie Kontinent, Landkreis und Stadt abrufen. Für jede öffentliche IP-Adresse aus einer Geo-Standortdatenbank. Sie wird mithilfe der erweiterten Richtlinieninfrastruktur durchgeführt. Die abgerufenen Standortdetails werden dann in einer Rewrite-Aktion oder einer Responder Action zur Durchführung der folgenden Anwendungsfälle verwendet.

- Fügen Sie einen HTTP-Header mit Benutzerstandortdetails (wie Land, Stadt) ein, wenn Sie die Clientanfrage an den Back-End-Server senden.
- Fügen Sie der Antwort auf der HTML-Seite einen Ländernamen für einen ungültigen Benutzer hinzu.

Die Appliance kann die Standortdetails auch mithilfe des Überwachungsprotokollierungsmechanismus protokollieren.

Abrufen von Benutzerstandortdetails mithilfe von Geolokationsfunktionen

Die Komponenten interagieren wie folgt:

1. Der Benutzer sendet eine Kundenanfrage von einem bestimmten geografischen Standort aus.
2. Die NetScaler-Appliance sucht aus der Clientanforderung nach der Benutzer-IP-Adresse und ruft die Details des Geo-Standorts ab. Zu den Details gehören Kontinent, Land, Region, Stadt, ISP, Organisation oder benutzerdefinierte Details aus einer Geolokalisierungsdatenbank.
3. Sobald die Standortdetails abgerufen wurden, verwendet die Appliance entweder eine Responder Policy oder eine Rewriterichtlinie, um die Anforderung zu bewerten.
4. In einer Rewriterichtlinie fügt die Appliance einen Header mit den Details des Geo-Standorts hinzu und sendet ihn an den Back-End-Server. Fügen Sie beispielsweise einen benutzerdefinierten HTTP-Header mit Länderinformationen ein.
5. In einer Responder Policy wertet die Appliance die HTTP-Anforderung aus und ermöglicht basierend auf der Richtlinienbewertung den Zugriff auf die Benutzer oder leitet den Benutzer auf eine Fehlerseite um. Darin heißt es, dass die Region, von der aus sie auf die Anwendung zugreifen, keinen Zugriff hat.

Einrichten einer Geolocation-Datenbank

Als Voraussetzung benötigen Sie eine Geolokationsdatenbank, um auf der NetScaler-Appliance ausgeführt werden zu können. Die Geolocation-Datenbankdateien sind mit NetScaler-Firmware verfügbar. Um die Datenbankdateien von einem Anbieter herunterzuladen, konvertieren Sie sie in das NetScaler Format und importieren Sie sie in Ihre Appliance.
Weitere Informationen zur Geolokalisierungsdatenbank finden Sie unter Hinzufügen einer Standortdatei zum Erstellen einer statischen Näherungsdatenbank .

Geolocation-Funktionen

Die folgende Tabelle enthält eine Liste von Geolokationsfunktionen, die Standortdetails einer öffentlichen IP-Adresse abrufen. Diese Funktionen können in Rewrite- oder Responder-Richtlinien verwendet werden.

Geolocation-Funktion	Beispiel
CLIENT.IP.SRC.LOCATION	Asien.In.Karnataka.Bangalore
CLIENT.IP.SRC.LOCATION.GET (1).LOCATION_LONG	Indien
CLIENT.IP.SRC.LOCATION(3)	Asia.In.Karnataka
CLIENT.IP.SRC.LAT_LONG	12,77
CLIENT.IPV6.SRC.LOCATION	Nordamerika.us.California.Santa Clara.Verizon.Citrix
CLIENT.IPV6.SRC.LOCATION(3)	North America.us.Kalifornien
CLIENT.IPV6.SRC.LOCATION.GET(1).LOCATION_L	Vereinigte Staaten
CLIENT.IPV6.SRC.LOCATION.GET(3)	Kalifornien
CLIENT.IPV6.SRC.LAT_LONG	36, -119

Konfigurieren von Geolocation-Funktionen

Um Geolokationsfunktionen mithilfe einer erweiterten Richtlinieninfrastruktur zu konfigurieren, müssen Sie die Funktionen für Lastenausgleich, Rewrite und Responder aktivieren und dann die folgenden Anwendungsfälle abschließen.

Aktivieren Sie Load Balancing, Responder, Rewrite Funktionen

Wenn Sie möchten, dass die NetScaler-Appliance den Benutzerzugriff von einem bestimmten Geo-Standort aus autorisiert, müssen Sie die Funktionen für Lastenausgleich, Rewrite und Responder aktivieren.

```
1 enable ns feature loadbalancing rewrite responder
2 <!--NeedCopy-->
```


Anwendungsfall 1: Konfigurieren der Geolokationsfunktion zum Umleiten ungültiger Benutzer außerhalb des Geo-Standorts

Wenn ein Benutzer aus Indien Zugriff auf eine Webseite anfordert, blockieren Sie die Anfrage und antworten Sie mit einer HTML-Seite mit Ländernamen.

Die folgenden Schritte helfen Ihnen, die Konfiguration dieses Anwendungsfalls abzuschließen.

- Responderaktion hinzufügen
- Responder-Richtlinie hinzufügen
- Bind-Responderrichtlinie an den Lastausgleichsserver

Weitere Informationen zu den GUI-Prozeduren zum Rewrite von Aktionen und zum Rewrite der Richtlinienkonfiguration finden Sie unter Responder.

Responderaktion hinzufügen

Fügen Sie eine Responder Action hinzu, um mit einer HTML-Seite mit dem Ländernamen zu antworten.
Geben Sie in der Befehlszeile Folgendes ein:

```
add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>][-reasonPhrase <
    string>]
<!--NeedCopy-->
```

Beispiel:

```
add responder action responder_act respondwith "HTTP.REQ.VERSION + "
    304 Requested Page not allowed in your country - " + CLIENT.IP.SRC.
    LOCATION.GET (1).LOCATION_LONG + "\r\n""
<!--NeedCopy-->
```

Aktion für Audit-Protokollmeldungen hinzufügen

Sie können Überwachungsnachrichtenaktionen so konfigurieren, dass Nachrichten auf verschiedenen Protokollebenen protokolliert werden, entweder nur im Syslog-Format oder sowohl in Syslog als auch in `newnslog` Formaten. Auditmeldungsaktionen verwenden Ausdrücke, um das Format der Auditmeldungen anzugeben.
So erstellen Sie eine Aktion für Überwachungsnachrichten über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewnslog
 (YES|NO)]
```


Beispiel:

```
add audit messageaction msg1 DEBUG ""Request Location: "+CLIENT.IP.SRC.
    LOCATION"
<!--NeedCopy-->
```

Responder-Richtlinie hinzufügen

Fügen Sie eine Responder Policy hinzu, um Anfragen aus Indien zu identifizieren, und verknüpfen Sie die Aktion des Responders mit dieser Richtlinie.
Geben Sie in der Befehlszeile Folgendes ein:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
<!--NeedCopy-->
```

Beispiel:

```
add responder policy responder_pol CLIENT.IP.SRC.MATCHES_LOCATION("Asia
    .India.\*.\*.\*.\*") responder_act -logaction msg1
<!--NeedCopy-->
```

Bind-Responderrichtlinie an den Lastausgleichsserver

Binden Sie die Responder Policy an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL.
Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver http_vserver -policyName responder_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Anwendungsfall 2: Konfigurieren der Geolocation-Funktion zum Einfügen eines neuen HTTP-Headers mit Standortdetails, damit das Back-End antworten kann

Betrachten Sie ein Szenario, in dem eine NetScaler-Appliance den Benutzerspeicherort in den HTTP-Header einer an den Anwendungsserver gesendeten Anforderung einfügen muss, damit der Server

die Informationen für eine Geschäftslogik verwenden kann.
Die folgenden Schritte helfen Ihnen, die Konfiguration dieses Anwendungsfalls abzuschließen.

- Rewrite-Aktion hinzufügen
- Hinzufügen einer Rewrite-Richtlinie
- Rewriterichtlinie an Lastenausgleich binden

Weitere Informationen zu den GUI-Prozeduren zum Rewrite von Aktionen und zum Rewrite der Richtlinienkonfiguration finden Sie unter Thema Responder .

Rewrite-Aktion hinzufügen

Fügen Sie eine Rewriteaktion hinzu, um einen benutzerdefinierten HTTP-Header mit Details zur Benutzergeolokalisierung in die Anforderung einzufügen und Back-End-Server zu senden.
Geben Sie in der Befehlszeile Folgendes ein:

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
   search <expression>] [-refineSearch <string>][-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add rewrite action rewrite_act insert_http_header "User_location"
   CLIENT.IP.SRC.LOCATION
<!--NeedCopy-->
```

Hinzufügen einer Rewrite-Richtlinie

Fügen Sie eine Rewriterichtlinie hinzu, um zu prüfen, ob die Rewrite-Aktion ausgeführt werden muss. In diesem Fall müssen alle Anfragen, die an den Anwendungsserver gehen, einen benutzerdefinierten HTTP-Header haben, damit die Regel “wahr” sein kann.
Geben Sie in der Befehlszeile Folgendes ein:

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <
   string>] [-logAction <string>]
<!--NeedCopy-->
```

Beispiel:

```
add rewrite policy rewrite_pol true rewrite_act -logaction log_act
<!--NeedCopy-->
```


Rewriterichtlinie an Lastenausgleich binden

Binden Sie die Rewriterichtlinie an den erforderlichen virtuellen Lastausgleichsserver vom Typ HTTP/SSL.
Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver http_vserver -policyName rewrite_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Syslog-Unterstützung für die Protokollierung von Geolokationsdetails (optional)

Wenn Sie es vorziehen, die Geolokationsdetails des Benutzers zu protokollieren, müssen Sie die SYSLOG-Aktion angeben, die ausgeführt werden soll, wenn eine Anforderung mit der Richtlinie übereinstimmt. Die Appliance speichert die Details als Protokollmeldung in der Datei ns.log.
Weitere Informationen zur SYSLOG- und NSLOG-Überwachung finden Sie unter Thema Audit-Protokollierung .

Ausgabe für Benutzergeolocation-Details

Die folgende Ausgabe wird in der Appliance mit dem SYSLOG oder der `newnslog` Aktion protokolliert, wenn Sie versuchen, vom Standort in Bangalore aus auf eine Anwendung zuzugreifen und wenn die Appliance die Geolokalisierungsfunktion “CLIENT.IP.SRC.LOCATION” verwendet.

```
Asia.India.Karnataka.Banglore
<!--NeedCopy-->
```

Beispielausgabeprotokoll:

```
07/23/2018:19:03:54 GMT  Debug 0-PPE-0 : default REWRITE Message 22 0 :
     "Request Location: asia.in.karnataka.bangalore.\*.\*"
07/23/2018:19:23:55 GMT  Debug 0-PPE-0 : default RESPONDER Message 32 0
Done
<!--NeedCopy-->
```


Verwenden Sie die Quell-IP-Adresse des Clients, wenn Sie eine Verbindung zum Server herstellen

May 11, 2023

Sie können die NetScaler Appliance so konfigurieren, dass Pakete vom Client an den Server weitergeleitet werden, ohne die Quell-IP-Adresse zu ändern. Dies ist nützlich, wenn Sie die Client-IP-Adresse nicht in einen Header einfügen können, z. B. wenn Sie mit Nicht-HTTP-Diensten arbeiten.

Weitere Informationen zum globalen Konfigurieren von USIP finden Sie unter Aktivieren der Verwendung des Quell-IP-Modus.

So aktivieren Sie den USIP-Modus für einen Dienst mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -usip (YES | NO)
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -usip YES
<!--NeedCopy-->
```

So aktivieren Sie den USIP-Modus für einen Dienst mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen im Abschnitt Diensteinstellungen die Option **Quell-IP-Adresse verwenden**aus.

Verwenden Sie die Clientquell-IP-Adresse für Back-End-Kommunikation in einer v4-v6-Lastenausgleichskonfiguration

May 11, 2023

Bei Diensten mit deaktiviertem USIP kommuniziert die NetScaler Appliance in einer v4-zu-v6-Load Balancing-Konfiguration mit den zugehörigen Servern von einer der konfigurierten IPv6-SNIP-Adressen (SNIP6).

Für Dienste mit aktiviertem USIP müssen Sie den globalen USIP-NAT-Präfixparameter festlegen, um die zugehörigen Server über die Client-IP-Adresse der Anforderungspakete zu informieren. Das USIP-NAT-Präfix ist ein globales IPv6-Präfix mit der Länge 32/40/48/56/64/96 Bit, das auf der NetScaler-Appliance konfiguriert ist.

Für einen Lastenausgleichsdienst, für den USIP aktiviert ist, übersetzt die Appliance das IPv4-Anforderungspaket in ein IPv6-Paket und legt die Quell-IP-Adresse des übersetzten IPv6-Pakets auf eine Verkettung von Folgendem fest:

- das USIP-NAT-Präfix mit einer Länge von 32/40/48/56/64/96 Bit.
- aufgefüllte Nullen, wenn die USIP-NAT-Präfixlänge weniger als 96 Bit beträgt. Anzahl der mit Nullen aufgefüllten Bits = 96-USIP-NAT-Präfixlänge. Wenn beispielsweise die USIP NAT-Präfixlänge 64 ist, dann ist die Anzahl der mit Nullen aufgefüllten Bits = 96-64 = 32.
- die IPv4-Quelladresse [32 Bit], die im Anforderungspaket empfangen wurde. Mit anderen Worten, die letzten 32 Bits der Quell-IPv6-Adresse werden auf die IPv4-Adresse des Clients gesetzt.

Beim Empfang eines IPv6-Antwortpakets vom Server übersetzt die NetScaler-Appliance das IPv6-Paket in ein IPv4-Paket und setzt die Ziel-IP-Adresse des übersetzten IPv4-Pakets auf die letzten 32 Bit der Ziel-IP-Adresse des IPv6-Pakets.

> **Hinweis**: Diese Funktion wird für die NetScaler Gateway-Konfiguration und die Load-Balancing-Konfigurationen für Content Switching und Cache-Umleitung nicht unterstützt.

Konfigurationsschritte

Die Konfiguration von USIP für eine v4-to-v6-Load-Balancing-Konfiguration umfasst die folgenden Aufgaben:

- **Fügen Sie das globale USIP-NAT-Präfix**hinzu. Es ist ein globales IPv6-Präfix mit der Länge 32/40/48/56/64/96 Bit, das auf der Appliance konfiguriert werden muss.
- **Aktivieren Sie den globalen USIP-Modus**. Weitere Informationen finden Sie unter Aktivieren des Quell-IP-Modus verwenden.
- **Aktivieren Sie den USIP-Modus für Lastausgleichsdienste**. Weitere Informationen finden Sie unter Verwenden der Quell-IP-Adresse des Clients beim Herstellen einer Verbindung mit dem Server.

So fügen Sie mit der CLI ein globales USIP-NAT-Präfixhinzu:

- `set ipv6 -usipnatprefix <prefix/prefix_length>`
- `show ipv6`

Um mithilfe der GUI ein globales USIP-NAT-Präfix hinzuzufügen:

1. Navigieren Sie zu **System** > **Netzwerk**und klicken Sie auf **IPv6-Einstellungen ändern**.

2. Stellen Sie auf dem Bildschirm „ **Konfiguration für IPV6 konfigurieren** “ den **USIP-NAT-Präfixparameter** ein.

Beispiel-Konfiguration

```
> set ipv6 -usipnatprefix 2001:DB8:90::/64
Done

> enable ns mode USIP
Done

> add lb vserver LBVS-1 HTTP 203.0.113.90 80
Done

> add service SVC-1 2001:DB8:5001::30 HTTP 80 -usip yes
Done

> add service SVC-2 2001:DB8:5001::60 HTTP 80 -usip yes
Done

> bind lb vserver LBVS-1 SVC-1
Done

> bind lb vserver LBVS-1 SVC-2
Done

<!--NeedCopy-->
```

Quellports für serverseitige Verbindungen konfigurieren

May 11, 2023

Wenn die NetScaler Appliance eine Verbindung zu einem physischen Server herstellt, kann sie den Quellport aus der Anforderung des Clients verwenden oder einen Proxy-Port als Quellport für die Verbindung verwenden. Sie können den Parameter Proxy-Port verwenden auf YES festlegen, um Situationen wie das folgende Szenario zu behandeln:

- Die NetScaler-Appliance ist mit zwei virtuellen Lastausgleichsservern, LBVS1 und LBVS2, konfiguriert.
- Beide virtuellen Server sind an denselben Dienst gebunden, S-ANY.
- Die Quell-IP-Adresse (des Clients) verwenden (USIP) ist für den Dienst aktiviert.

- Client C1 sendet zwei Anforderungen, Req1 und Req2, für denselben Dienst.
- LBVS1 erhält Req1 und LBVS2 erhält Req2.
- LBVS1 und LBVS2 leiten die Anfrage an S-ANY weiter, und wenn S-ANY die Antwort sendet, leiten LBVS1 und LBVS2 die Antwort an den Client weiter.
- Betrachten Sie zwei Fälle:
  - Verwenden Sie den Client-Port. Wenn die Appliance den Clientport verwendet, verwenden sowohl die virtuellen Server die IP-Adresse des Clients (weil USIP ON ist) als auch den Port des Clients, wenn eine Verbindung zum Server hergestellt wird. Wenn der Dienst die Antwort sendet, kann die Appliance daher nicht feststellen, welcher virtuelle Server die Antwort erhalten muss.
  - Verwenden Sie den Proxy-Port. Wenn die Appliance einen Proxyport verwendet, verwenden die virtuellen Server die IP-Adresse des Clients (weil USIP eingeschaltet ist), aber bei der Verbindung mit dem Server unterschiedliche Ports. Wenn der Dienst die Antwort sendet, identifiziert die Portnummer daher den virtuellen Server, der die Antwort erhalten muss.

Wenn Sie jedoch eine vollständig transparente Konfiguration benötigen, z. B. eine vollständig transparente Cache-Umleitungskonfiguration, müssen Sie die Einstellung Proxy-Port verwenden deaktivieren, damit die NetScaler Appliance den Quellport aus der Clientanforderung verwenden kann.

Die Option Proxyport verwenden wird relevant, wenn die Option Quell-IP verwenden (USIP) aktiviert ist. Für TCP-basierte Diensttypen wie TCP, HTTP und SSL ist die Option standardmäßig aktiviert. Bei UDP-basierten Diensttypen, wie UDP und DNS, einschließlich ANY, ist die Option standardmäßig deaktiviert. Weitere Informationen zur USIP-Option finden Sie unter “Aktivieren des Quell-IP-Modus. “

Sie können die Einstellung **Proxy-Port verwenden** entweder global oder für einen bestimmten Dienst konfigurieren.

Konfigurieren der Einstellung Proxyport verwenden für einen Dienst

Sie konfigurieren die Einstellung **ProxyPort verwenden** für den Dienst, wenn Sie die globale Einstellung außer Kraft setzen möchten.

So konfigurieren Sie die Einstellung Proxyport verwenden für einen Dienst mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -useProxyPort (YES | NO)
<!--NeedCopy-->
```

Beispiel:


```
set service svc1 -useproxyport YES
Done

show service svc1
svc1 (10.102.29.30:80) - HTTP
State: UP
. . .
Use Source IP: YES Use Proxy Port: YES
. . .
Done
<!--NeedCopy-->
```

So konfigurieren Sie die Einstellung „Proxyport verwenden“ für einen Dienst mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option Verkehrseinstellungen aus und wählen Sie **Proxyport verwenden**aus.

Konfigurieren Sie die Einstellung „Proxyport verwenden“ global

Sie konfigurieren die Einstellung **Proxyport verwenden** global, wenn Sie die Einstellung auf alle Dienste auf der NetScaler Appliance anwenden möchten. Die **servicespezifischen Einstellungen “Proxy-Port verwenden** “ überschreibt die globale Einstellung.

So konfigurieren Sie die Einstellung Proxyport global verwenden mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Einstellung **Proxy-Port verwenden** global zu konfigurieren und die Konfiguration zu überprüfen:

```
set ns param -useproxyport ( ENABLED | DISABLED )`
show ns param`
<!--NeedCopy-->
```

Beispiel:

```
set ns param -useproxyport ENABLED

Done

show ns param
Global configuration settings:
```



```
. . .
Use Proxy Port: ENABLED
Done
<!--NeedCopy-->
```

So konfigurieren Sie die Einstellung Proxyport verwenden global mithilfe der GUI

Navigieren Sie zu **System > Einstellungen > Globale Systemeinstellungen ändern**, und wählen oder deaktivieren Sie Proxyport verwenden.

Grenzwert für die Anzahl der Clientverbindungen festlegen

May 11, 2023

Sie können eine maximale Anzahl von Client-Verbindungen angeben, die jeder Load-Balancing-Server verarbeiten kann. Die NetScaler-Appliance öffnet dann nur so lange Client-Verbindungen zu einem Server, bis dieses Limit erreicht ist. Wenn der Lastausgleichsserver seine Grenze erreicht, werden Monitorsonden übersprungen, und der Server wird erst für den Lastausgleich verwendet, wenn er die Verarbeitung bestehender Verbindungen abgeschlossen hat und die Kapazität freigibt.

Weitere Informationen zur Einstellung " **Maximum Client** " finden Sie unter Load Balancing Domain-name Based Services.

Hinweis: Verbindungen, die im Prozess des Schließens sind, werden für dieses Limit nicht berücksichtigt.

So legen Sie mithilfe der CLI ein Limit für die Anzahl der Client-Verbindungen fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -maxclient <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -maxClient 1000
<!--NeedCopy-->
```


So legen Sie mithilfe der GUI ein Limit für die Anzahl der Client-Verbindungen fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Maximale Clients**aus.

Festlegen eines Grenzwerts für die Anzahl der Anforderungen pro Verbindung zum Server

May 11, 2023

Die NetScaler Appliance kann so konfiguriert werden, dass Verbindungen wiederverwendet werden, um die Leistung zu verbessern. In einigen Szenarien können Webserver mit Lastausgleich jedoch Probleme haben, wenn Verbindungen für zu viele Anfragen wiederverwendet werden. Verwenden Sie für HTTP- oder SSL-Dienste die Option max request, um die Anzahl der Anforderungen zu begrenzen, die über eine einzelne Verbindung an einen Lastausgleichswebserver gesendet werden.

Hinweis: Sie können die maximale Anforderungsoption nur für HTTP- oder SSL-Dienste konfigurieren.

Um die Anzahl der Client-Anfragen pro Verbindung mithilfe der CLI zu begrenzen

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <ServiceName> -maxReq <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -maxReq 100
<!--NeedCopy-->
```

Um die Anzahl der Client-Anfragen pro Verbindung mithilfe der GUI zu begrenzen

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Maximale Anforderungen**aus.

Schwellenwert für die an einen Dienst gebundenen Monitore festlegen

May 11, 2023

Die NetScaler-Appliance weist einen Dienst nur dann als AKTIV aus, wenn die Summe der Gewichtungen aller an sie gebundenen Monitore, die aktiv sind, dem für den Dienst konfigurierten Schwellenwert entspricht oder diesen übersteigt. Das Gewicht eines Monitors gibt an, wie viel dieser Monitor dazu beiträgt, den Dienst, an den er gebunden ist, als UP zu bezeichnen.

Standardmäßig ist der Monitorschwellenwert auf 0 und die Monitorgewichte auf 1 festgelegt. Alle Monitore haben dann das gleiche Gewicht und ein Dienst kann AUSFALLEN, wenn einer der Monitore AUSFÄLLT.

Nehmen wir beispielsweise an, dass drei Monitore mit den Namen Monitor-HTTP-1, Monitor-HTTP-2 bzw. Monitor-HTTP-3 an Service-HTTP-1 gebunden sind und dass der für den Dienst konfigurierte Schwellenwert drei beträgt. Angenommen, jedem Monitor werden die folgenden Gewichte zugewiesen:

- Das Gewicht von Monitor-HTTP-1 ist 1.
- Das Gewicht von Monitor-HTTP-2 beträgt 3.
- Das Gewicht von Monitor-HTTP-3 ist 1.

Der Dienst wird nur dann als UP markiert, wenn eine der folgenden Bedingungen zutrifft:

- Monitor-HTTP-2 ist aktiv.
- Monitor-HTTP-2 und Monitor-HTTP-1 oder Monitor-HTTP-3 sind verfügbar
- Alle drei Monitore sind aktiv.

So legen Sie den Monitor-Schwellenwert für einen Dienst mithilfe der CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -monThreshold <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -monThreshold 100
<!--NeedCopy-->
```

So legen Sie den Monitor-Schwellenwert für einen Dienst mithilfe der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.

2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Schwellenwert überwachen**aus.

Timeoutwert für Clientverbindungen im Leerlauf festlegen

May 11, 2023

Sie können den Dienst mit einem Timeout-Wert konfigurieren, um alle inaktiven Client-Verbindungen zu beenden, wenn die konfigurierte Zeit abgelaufen ist. Wenn der Client während der konfigurierten Zeit inaktiv ist, schließt die NetScaler-Appliance die Client-Verbindung.

So legen Sie mithilfe der CLI einen Timeout-Wert für inaktive Clientverbindungen fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -cltTimeout 100
<!--NeedCopy-->
```

So legen Sie mithilfe der GUI einen Timeout-Wert für inaktive Client-Verbindungen fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus, und wählen Sie **Timeout für Client-Idle**aus.

Timeoutwert für Serververbindungen im Leerlauf festlegen

May 11, 2023

Sie können einen Dienst mit einem Timeout-Wert konfigurieren, um alle inaktiven Serververbindungen zu beenden, wenn die konfigurierte Zeit (in Sekunden) abgelaufen ist. Wenn der Server für die konfigurierte Zeit inaktiv ist, schließt die NetScaler-Appliance die Serververbindung.

So legen Sie mithilfe der CLI einen Timeout-Wert für inaktive Serververbindungen fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -svrTimeout <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -svrTimeout 100
<!--NeedCopy-->
```

So legen Sie mithilfe der GUI einen Timeout-Wert für inaktive Serververbindungen fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus, und wählen Sie **Timeout für Serverinaktivität**aus.

Grenzwert für die Bandbreitenauslastung durch Clients festlegen

May 11, 2023

Manchmal haben Server möglicherweise eine begrenzte Bandbreite für die Bearbeitung von Clientanforderungen und können überlastet werden. Um ein Überladen eines Servers zu verhindern, können Sie eine maximale Grenze für die vom Server verarbeitete Bandbreite in Kbps angeben. Die NetScaler-Appliance leitet Anfragen nur so lange an einen Server mit Lastausgleich weiter, bis dieses Limit erreicht ist.

So legen Sie mithilfe der CLI ein maximales Bandbreitenlimit für einen Dienst fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -maxBandwidth <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -maxBandwidth 100
<!--NeedCopy-->
```


So legen Sie mithilfe der GUI ein maximales Bandbreitenlimit für einen Dienst fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Maximale Bandbreite**aus.

Umleiten von Clientanforderungen an einen Cache

August 19, 2021

Sie können einen Dienst so konfigurieren, dass Clientanforderungen an einen Cache umgeleitet werden und die nicht zwischenspeicherbaren Anforderungen an einen Dienst weitergeleitet werden, der von der konfigurierten Lastausgleichsmethode ausgewählt wurde.

So legen Sie die Cache-Umleitung für einen Dienst mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -cacheable <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -cacheable YES
<!--NeedCopy-->
```

So legen Sie die Cache-Umleitung für einen Dienst mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie einen Dienst, und legen Sie den Cache-Typ fest.

VLAN-Bezeichner für VLAN-Transparenz beibehalten

August 19, 2021

Sie können einen virtuellen Lastausgleichsserver so konfigurieren, dass die VLAN-ID des Clients in Paketen beibehalten wird, die an Server weitergeleitet werden sollen. Der virtuelle Server muss ein virtueller Platzhalterserver vom Typ ANY sein und im MAC-Modus funktionieren.

So konfigurieren Sie einen virtuellen Lastausgleichsserver, um die Client-VLAN-ID mit der CLI beizubehalten

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen virtuellen Lastausgleichsserver so zu konfigurieren, dass die Client-VLAN-ID beibehalten und die Konfiguration überprüft wird:

```
set lb vserver <name> -m MAC -macmodeRetainvlan ENABLED

show lb vserver <name>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die `-m MAC` Option aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie einen virtuellen Lastausgleichsserver, um die Client-VLAN-ID mit der GUI beizubehalten

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **VLAN-ID beibehalten**aus.

Automatischen Statusübergang basierend auf der prozentualen Integrität von gebundenen Diensten konfigurieren

May 11, 2023

Sie können einen virtuellen Lastausgleichsserver so konfigurieren, dass er automatisch vom Status UP in den Status DOWN übergeht, wenn der Prozentsatz der aktiven Dienste unter einen konfigurierten Schwellenwert fällt. Wenn Sie beispielsweise 10 Dienste an einen virtuellen Lastausgleichsserver binden und für diesen virtuellen Server einen Schwellenwert von 50% konfigurieren, wechselt er von UP nach DOWN, wenn sechs oder mehr Dienste AUSGEFALLEN sind. Wenn der prozentuale Zustand den Schwellenwert überschreitet, kehrt der virtuelle Server in den Status UP zurück.

Sie können auch einen SNMP-Alarm namens ENTITY-STATE aktivieren, wenn Sie möchten, dass die NetScaler-Appliance Sie benachrichtigt, wenn der prozentuale Zustand der gebundenen Dienste dazu führt, dass sich der Status eines virtuellen Servers ändert.

So konfigurieren Sie prozentuale automatische Statusübergänge mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen automatischen Zustandsübergang für einen virtuellen Server zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -healthThreshold <positive_integer>

show lb vserver <name>
<!--NeedCopy-->
```

So konfigurieren Sie den prozentualen automatischen Statusübergang mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und legen Sie einen **Integritätsschwellenwert**fest.

Um den ENTITY-STATE-Alarm mit der CLI zu aktivieren

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den ENTITY-STATE-SNMP-Alarm zu aktivieren und die Konfiguration zu überprüfen:

```
enable snmp alarm ENTITY-STATE

show snmp alarm
<!--NeedCopy-->
```

Um den ENTITY-STATE-Alarm mithilfe der GUI zu aktivieren

1. Navigieren Sie zu **System > SNMP > Alarme**.
2. Wählen Sie **ENTITY-STATE** aus und wählen Sie in der Liste Aktion **Aktivieren**aus.

Statische Nähe basierend auf dem NetScaler-Standort

June 19, 2023

> **Hinweis**
>
> Der Parameter proximity from self ist ab Version 13.1 Build 48.x verfügbar.

Wenn Sie die statische Proximity-Load-Balancing-Methode konfigurieren, wird ein Server auf der Grundlage der Client-IP-Adresse und nicht anhand der NetScaler-Loopback-IP-Adresse ausgewählt. Infolgedessen könnte die Reaktionszeit höher sein. Wenn der Parameter proximity from self aktiviert ist, stellt er sicher, dass die Anfrage mithilfe der NetScaler-Loopback-IP-Adresse an einen Server gesendet wird, der dem NetScaler am nächsten ist. Wenn Sie diesen Parameter auf YES setzen, wird die Reaktionszeit beschleunigt, wenn sich die Server im Vergleich zum Client näher am NetScaler befinden.

Voraussetzung

Wählen Sie statische Nähe als Lastausgleichsmethode

So konfigurieren Sie den Parameter proximityFromSelf mithilfe der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um den Parameter proximityFromSelf zu konfigurieren und die Konfiguration zu überprüfen

```
set lbparameter -proximityFromSelf <NO/YES>
show lbparameter

<!--NeedCopy-->
```

Beispiel:

```
set lbparameter -proximityFromSelf Yes
<!--NeedCopy-->
```

So konfigurieren Sie den Parameter Proximity from Self mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing**.
2. Klicken Sie auf der Seite Load Balancing im Abschnitt **Einstellungen** auf **Load Balancing-Parameter ändern**.
3. Wählen Sie **Proximity von Self aus**.
4. Klicken Sie auf **OK**.

Integrierte Monitore

May 11, 2023

Die NetScaler Appliance enthält verschiedene integrierte Monitore, mit denen Sie Ihre Dienste überwachen können. Diese integrierten Monitore verarbeiten die meisten gängigen Protokolle. Sie bieten Optionen zum Ändern einiger Parameter, z. B. Intervall, Reaktions-Timeout, um Ihre Anforderungen zu erfüllen. Sie können jedoch den Monitornamen und das Protokoll nicht ändern. Weitere Informationen finden Sie unter Monitore ändern. Sie können einen integrierten Monitor auch an einen Dienst binden und ihn vom Service trennen.

> **Hinweis**
>
> Sie können einen benutzerdefinierten Monitor basierend auf einem integrierten Monitor erstellen. Weitere Informationen zum Erstellen benutzerdefinierter Monitore finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

TCP-basierte Anwendungsüberwachung

May 11, 2023

Die NetScaler-Appliance verfügt über zwei integrierte Monitore, die TCP-basierte Anwendungen überwachen: `tcp-default` und `ping-default`. Wenn Sie einen Dienst erstellen, wird der entsprechende Standardmonitor automatisch an ihn gebunden, sodass der Dienst sofort verwendet werden kann, wenn er UP ist. Der tcp-Standardmonitor ist an alle TCP-Dienste gebunden. Der Ping-Standardmonitor ist an alle Nicht-TCP-Dienste gebunden.

Sie können Standardmonitore nicht löschen oder ändern. Wenn Sie einen anderen Monitor an einen TCP-Dienst binden, ist der Standardmonitor vom Dienst nicht gebunden. In der folgenden Tabelle sind die Monitortypen sowie die Parameter und Überwachungsprozesse aufgeführt, die jedem Typ zugeordnet sind.

Monitor-Typ	Spezifische Parameter	Prozess
tcp	Nicht zutreffend	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein und schließt dann die Verbindung. Wenn die Appliance TCP-Datenverkehr zum Ziel beobachtet, sendet sie keine TCP-Überwachungsanfragen. Dies tritt auf, wenn LRTM deaktiviert ist. Standardmäßig ist LRTM auf diesem Monitor deaktiviert.
http	httprequest [“HEAD/”] — HTTP-Anfrage, die an den Dienst gesendet wird. respcode [200] — Vom Dienst wird eine Reihe von HTTP-Antwortcodes erwartet.	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Nachdem die Verbindung hergestellt wurde, sendet die Appliance HTTP-Anforderungen und vergleicht dann den Antwortcode mit dem konfigurierten Satz von Antwortcodes.

Monitor-Typ	Spezifische Parameter	Prozess
tcp-ecv	send [””] — sind die Daten, die an den Dienst gesendet werden. Die maximal zulässige Länge der Zeichenfolge beträgt 512 Byte. recv [””] — erwartete Antwort des Dienstes. Die maximal zulässige Länge der Zeichenfolge beträgt 128 Byte. Das letzte Zeichen ist die NULL Kündigung.	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, sendet die Appliance mit dem Sendeparameter bestimmte Daten an den Dienst und erwartet eine bestimmte Antwort über den Empfangsparameter. Verschiedene Server senden verschiedene Segmentgrößen. Das Muster muss jedoch innerhalb von 16 TCP-Segmenten liegen.
http-ecv	send [””] — HTTP-Daten, die an den Dienst gesendet werden; recv [””] — die erwarteten HTTP-Antwortdaten vom Dienst	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, sendet die Appliance den Sendeparameter, um die HTTP-Daten an den Dienst zu senden, und erwartet die HTTP-Antwort, die der Empfangsparameter angibt. (HTTP-Body-Teil ohne HTTP-Header enthalten). Leere Antwortdaten entsprechen jeder Antwort. Die erwarteten Daten können sich irgendwo in den ersten 24 K Bytes des HTTP-Textes der Antwort befinden.

Monitor-Typ	Spezifische Parameter	Prozess
ping	Nicht zutreffend	Die NetScaler-Appliance sendet eine ICMP-Echoanforderung an das Ziel des Monitors und erwartet eine ICMP-Echoantwort.

Informationen zum Konfigurieren integrierter Monitore für TCP-basierte Anwendungen finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie TCP-basierte Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
    <string> -resptimeout <integer> [<units>] -retries <integer> -
    downTime <integer> [<units>] -action <action>
<!--NeedCopy-->
```

Beispiel für TCP-Monitortyp:

```
add lb monitor Exch2010-RPC-AddressBook TCP -LRTM ENABLED -interval 10
    -resptimeout 5 -destPort 59601
<!--NeedCopy-->
```

Beispiel für den HTTP-Monitortyp:

```
add lb monitor Mon_S4B_FE_2 HTTP -respCode 200 -httpRequest "GET /
    Autodiscover/XFrame/XFrame.html" -LRTM ENABLED -retries 10 -secure
    YES
<!--NeedCopy-->
```

Beispiel für den HTTP-ECV-Monitortyp:

```
add lb monitor STM_EXC2016_SSLBridge_MON HTTP-ECV -send "GET /owa/
    healthcheck.htm" -recv "200 OK" -LRTM ENABLED -destPort 443 -secure
    YES
<!--NeedCopy-->
```

Beispiel für PING-Monitortyp:


```
add lb monitor lbmon-localhost-ping PING -LRTM DISABLED -destIP
   127.0.0.1
<!--NeedCopy-->
```

SSL-Dienstüberwachung

June 19, 2023

Die NetScaler-Appliance verfügt über integrierte sichere Monitore, TCPS und HTTPS. Sie können die sicheren Monitore verwenden, um HTTP- und Nicht-HTTP-Verkehr zu überwachen. Um einen sicheren HTTP-Monitor zu konfigurieren, wählen Sie als Monitortyp HTTP aus und setzen Sie das sichere Flag. Um einen sicheren TCP-Monitor zu konfigurieren, wählen Sie als Monitortyp TCP aus und setzen Sie das sichere Flag. Die sicheren Monitore funktionieren wie folgt:

- **Sichere TCP-Überwachung.** Die NetScaler-Appliance stellt eine TCP-Verbindung her. Nachdem die Verbindung hergestellt wurde, führt die Appliance einen SSL-Handshake mit dem Server durch. Nachdem der Handshake beendet ist, schließt die Appliance die Verbindung.
- **Sicheres HTTP-Monitoring.** Die NetScaler-Appliance stellt eine TCP-Verbindung her. Nachdem die Verbindung hergestellt wurde, führt die Appliance einen SSL-Handshake mit dem Server durch. Wenn die SSL-Verbindung hergestellt ist, sendet die Appliance HTTP-Anfragen über den verschlüsselten Kanal und überprüft die Antwortcodes.

In der folgenden Tabelle werden die verfügbaren integrierten Monitore für die Überwachung von SSL-Diensten beschrieben.

Monitor-Typ	Sonde	Erfolgskriterien (Direkte Bedingung)
TCP	TCP-Verbindung; SSL-Handshake	Erfolgreiche TCP-Verbindung hergestellt und erfolgreicher SSL-Handshake.
HTTP	TCP-Verbindung; SSL-Handshake; Verschlüsselte HTTP-Anfrage	Eine erfolgreiche TCP-Verbindung wird hergestellt, ein erfolgreicher SSL-Handshake wird ausgeführt und der erwartete HTTP-Antwortcode in der HTTP-Antwort des Servers wird verschlüsselt.

Monitor-Typ	Sonde	Erfolgskriterien (Direkte Bedingung)
TCP-ECV	TCP-Verbindung. SSL-Handshake (Daten, die an einen Server gesendet werden, sind verschlüsselt.)	Eine erfolgreiche TCP-Verbindung wird hergestellt, ein erfolgreicher SSL-Handshake wird ausgeführt und erwartete TCP-Daten werden vom Server empfangen.
HTTP-ECV	TCP-Verbindung; SSL-Handshake (verschlüsselte HTTP-Anfrage)	Eine erfolgreiche TCP-Verbindung wird hergestellt, ein erfolgreicher SSL-Handshake wird ausgeführt und die erwarteten HTTP-Daten werden vom Server empfangen.

Beispielkonfiguration für den HTTP-ECV Health Check Monitor

HTTP-Dienste verfügen über vordefinierte Monitore, die eine erweiterte Inhaltsüberprüfung (ECV) ermöglichen.
Diese Monitore werden verwendet, wenn nach einer erfolgreichen TCP-Verbindung eine Validierung erforderlich ist. Diese Monitore validieren den Dienst als UP, wenn alle folgenden Kriterien erfüllt sind:

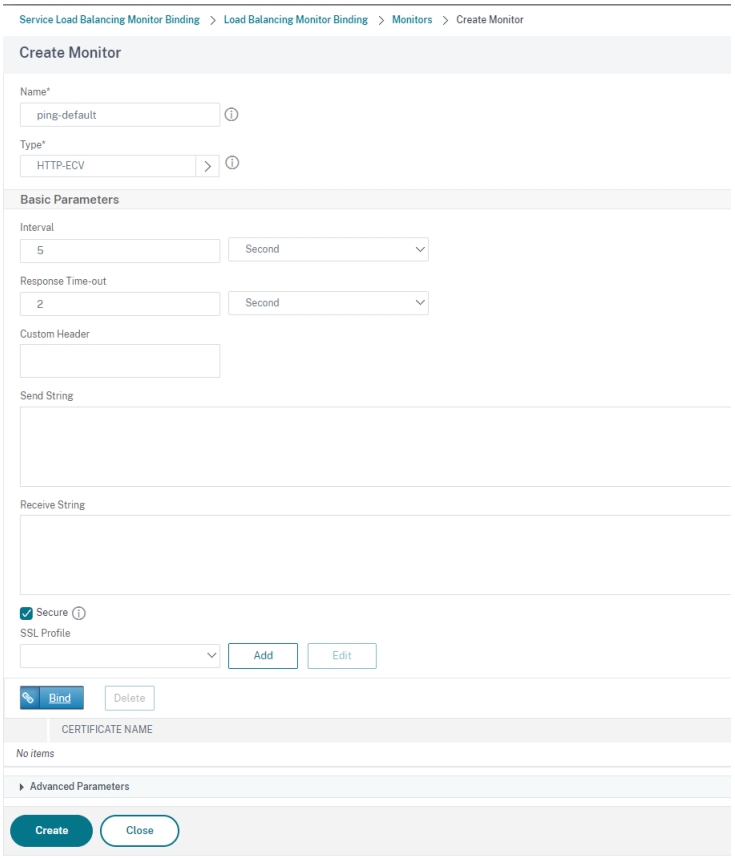
- Eine erfolgreiche TCP-Verbindung.
- Eine bestimmte Art von Anfrage muss generiert werden.
- Als Antwort von der **Empfangszeichenfolge**wird eine bestimmte Nachricht erwartet.

Für diese Monitore wird eine Anforderungszeichenfolge zusammen mit einer Antwortzeichenfolge konfiguriert. Wenn die vom NetScaler-Monitor empfangene Antwortzeichenfolge mit der konfigurierten Zeichenfolge übereinstimmt, wird der Dienst als UP markiert.

Binden Sie einen Monitor über die GUI an einen Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, erstellen Sie einen Dienst und geben Sie das Protokoll als **SSL**an. Klicken Sie auf **OK**.
2. Klicken Sie in den Bereich **Service to Load Balancing Monitor-Bindung** und klicken Sie auf **Bindung hinzufügen**.

3. Wählen Sie als Monitortyp **HTTP-ECV** und klicken Sie auf **Bearbeiten**.
4. Geben **Sie im Bereich Monitor konfigurieren** auf der Registerkarte **Basisparameter** Werte für die folgenden Parameter ein:
   - **Send String** — Die Zeichenfolge, die der Monitor an den Dienst senden muss.
   - **Receive String** — Die Zeichenfolge, die der Monitor empfangen muss, um den Dienst als UP zu markieren.



5. Klicken Sie auf **OK**, um die Monitorkonfiguration abzuschließen.
6. Klicken Sie auf **Select**.
7. Klicken Sie auf **Binden**, um den **HTTP-ECV-Monitor** an den Dienst zu binden.
8. Klicken Sie auf **Schließen**.

Erstellen Sie einen Monitor und binden Sie ihn über die CLI an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitor-name> http-ecv
bind service <servicename> -monitorName <monitor-name>
<!--NeedCopy-->
```


Beispiel:

```
add lb monitor monitor-1 http-ecv
bind service services1 -monitorName monitor-1
<!--NeedCopy-->
```

HTTP/2-Dienstüberwachung

May 11, 2023

Die NetScaler Appliance unterstützt HTTP/2-Monitore zur Überwachung des Integritätsstatus von HTTP/2-Diensten.

Der HTTP/2-Monitor kann auf zwei verschiedene Arten konfiguriert werden. Je nach Datenverkehrstyp können Sie einen HTTP/2-Monitor konfigurieren.

- **HTTP/2 Direkt.** Sie können HTTP/2 Direct für die Überwachung nicht sicherer HTTP/2-Dienste konfigurieren.
- **HTTP/2 SSL.** Sie können HTTP/2 SSL für die Überwachung des sicheren Datenverkehrs über SSL konfigurieren. Aktivieren Sie den Secure Flag-Parameter im HTTP/2, um den SSL-Datenverkehr zu überwachen.

Der http2direct und http2ssl sind die beiden verschiedenen integrierten Monitore, die für das HTTP/2-Protokoll unterstützt werden.

In der folgenden Tabelle sind die Konfigurationstypen und Überwachungsprozesse aufgeführt, die jedem Typ zugeordnet sind.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP/2 Direkt	TCP-Verbindung; HTTP2-Verbindungsvorwort & Einstellungsaushandlung; HTTP2-Anfrage	Der HTTP/2-Antwortstatuscode muss mit dem konfigurierten Antwortcode übereinstimmen.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP/2 SSL	TCP-Verbindung; SSL-Handshake; HTTP2-Verbindungsvorwort & Einstellungen Negotiation; HTTP2-Anfrage	Der Server muss immer ALPN mit dem HTTP/2-Protokoll auswählen und der HTTP/2-Antwortstatuscode muss mit dem konfigurierten Antwortcode übereinstimmen.

Binden Sie den HTTP/2-Monitor über die Befehlszeilenschnittstelle an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:

- `bind service <servicename> -monitorName <name>`
- `bind service <servicename> -monitorName <name>`

Beispiel:

- `bind service s1 -monitorName http2direct`
- `bind service s2 -monitorName http2ssl`

Überwachung des Proxy-Protokolldienstes

May 11, 2023

Die NetScaler Appliance mit einem Proxy-Protokoll unterstützt die Monitorprüfung. Die Monitorprüfung stellt sicher, dass der Back-End-Server auch das Proxy-Protokoll unterstützt. Die NetScaler Appliance verfügt über vier integrierte Monitortypen für HTTP- oder TCP-bezogene Dienste: HTTP, HTTPS, HTTP-ECV und TCP-ECV.

In der folgenden Tabelle sind die Monitortypen sowie die Parameter und Überwachungsprozesse aufgeführt, die jedem Typ zugeordnet sind.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP	`httprequest` [“HEAD /”] — HTTP-Anfrage, die an den Dienst gesendet wird. `respcode` [200] - Vom Dienst wird eine Reihe von HTTP-Antwortcodes erwartet.	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Nachdem die Verbindung hergestellt wurde, sendet die Appliance HTTP-Anforderungen und vergleicht dann den Antwortcode mit dem konfigurierten Satz von Antwortcodes.
HTTPS	`httprequest` [“HEAD /”] — HTTPS-Anfrage, die an den Dienst gesendet wird. `respcode` [200] - Vom Dienst wird eine Reihe von HTTPS-Antwortcodes erwartet.	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Nachdem die Verbindung hergestellt wurde, sendet die Appliance HTTPS-Anfragen und vergleicht dann den Antwortcode mit dem konfigurierten Satz von Antwortcodes.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP-ECV	send [“”] — HTTP-Daten, die an den Dienst gesendet werden. Empfangen [“”] — die erwarteten HTTP-Antwortdaten vom Dienst	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, sendet die Appliance den Sendeparameter, um die HTTP-Daten an den Dienst zu senden, und erwartet die HTTP-Antwort, die der Empfangsparameter angibt. (HTTP-Body-Teil ohne HTTP-Header enthalten). Leere Antwortdaten entsprechen jeder Antwort. Die erwarteten Daten können sich irgendwo in den ersten 24 K Bytes des HTTP-Textes der Antwort befinden.
TCP-ECV	send [“”] - sind die Daten, die an den Dienst gesendet werden. Die maximal zulässige Länge der Zeichenfolge beträgt 512 K Byte. received [“”] - die erwartete Antwort des Dienstes. Die maximal zulässige Länge der Zeichenfolge beträgt 128 KB Byte.	Die NetScaler-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, sendet die Appliance mit dem Sendeparameter bestimmte Daten an den Dienst und erwartet eine bestimmte Antwort über den Empfangsparameter. Verschiedene Server senden verschiedene Segmentgrößen. Das Muster muss jedoch innerhalb von 16 TCP-Segmenten liegen.

Sie können den Proxy-Protokollmonitor mit konfigurieren `netprofile`.

Konfigurieren Sie den Proxy-Protokollmonitor mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

1. Netzprofil mit aktiviertem Proxy-Protokoll hinzufügen

   ```
   add netprofile <name> -proxyProtocol ( ENABLED | DISABLED )
   ```

Beispiel:

```
1 add netprofile profile1 - proxyProtocol ENABLED
```

1. Binden Sie das Netzprofil an einen Dienst.

   ```
   set service <name> -netprofile <netprofile-name>
   ```

Beispiel:

```
1 set service S1 - netprofile profile1
```

> **Hinweis**
>
> Sie können den vorherigen Befehl ausführen, wenn Sie möchten, dass netprofile an einen Dienst gebunden werden soll.

1. Binden Sie das Netzprofil an einen Monitor.

   ```
   set lb monitor <monitor-name> <type> -netprofile <netprofile-name>
   ```

Beispiel:

```
1 set lb monitor http1 HTTPS - netprofile profile1
```

> **Hinweis**
>
> - Sie können den vorherigen Befehl ausführen, wenn das Netzprofil an einen Monitor gebunden sein soll.
> - Sie können einen Monitortyp Ihrer Wahl auswählen. Es kann HTTP, HTTPS, TCP-ECV oder HTTP-ECV sein.
>
> **Wichtig**
>
> - In einem allgemeinen Fall wird das an einen Dienst gebundene Netzprofil (Proxy-Protokoll aktiviert) berücksichtigt.
> - Wenn das Nettoprofil sowohl an den Monitor als auch an den Dienst gebunden ist, wird das an die Überwachung gebundene Netzprofil berücksichtigt. Das an den Dienst gebundene Netzprofil wird ignoriert.

FTP-Dienstüberwachung

May 11, 2023

Um FTP-Dienste zu überwachen, öffnet die NetScaler-Appliance zwei Verbindungen zum FTP-Server. Es stellt zunächst eine Verbindung zum Steuerport her, der zur Übertragung von Befehlen zwischen einem Client und einem FTP-Server verwendet wird. Nachdem es die erwartete Antwort erhalten hat, stellt es eine Verbindung zum Datenport her, der für die Übertragung von Dateien zwischen einem Client und einem FTP-Server verwendet wird. Erst wenn der FTP-Server wie erwartet reagiert, wird er auf beiden Verbindungen als UP markiert.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Die NetScaler-Appliance verfügt über zwei integrierte Monitore für FTP-Dienste: den FTP-Monitor und den FTP-EXTENDED-Monitor. Der FTP-EXTENDED-Monitor ist ein skriptfähiger Monitor. Es verwendet das nsftp.pl-Skript. Das FTP-EXTENDED-Monitorskript wurde erweitert, um sichere Tests an FTP-Dienste zu senden. Sie können einen Monitor vom Typ FTP-EXTENDED erstellen. Das nsftp.pl-Skript wird automatisch aus dem Standardverzeichnis übernommen.

Um sichere FTP-Tests an FTP-Dienste mithilfe der CLI zu senden

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lb monitor <monitorName> <type> -username <string> -password <
     string> -filename <filename>
2 <!--NeedCopy-->
```

Beispiel

```
1 add monitor mon1 FTP-EXTENDED -username root -password freebsd -
     filename fsdf
2 <!--NeedCopy-->
```

Um sichere FTP-Tests an FTP-Dienste mithilfe der GUI zu senden

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**.
2. Geben Sie den Monitortyp als **FTP-EXTENDED**an und stellen Sie die Parameter ein.
3. Geben Sie unter **Spezielle Parameter**einen **Dateinamen**, einen **Benutzernamen**und **ein Kennwort**an.

Informationen zum Konfigurieren integrierter Monitore zur Überprüfung des Status von FTP-Diensten finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Sichere Überwachung von Servern mit SFTP

May 11, 2023

Ein Benutzerskript 'nssftp.pl' wurde hinzugefügt, um die Überwachung durch das SSH File Transfer Protocol (SFTP) zu unterstützen. Sie ist in der aktuellen Liste der integrierten NetScaler Benutzermonitore verfügbar und befindet sich im Verzeichnis /netscaler/monitors. Der SFTP-Monitor verwendet den angegebenen Benutzernamen und das angegebene Kennwort, um zu prüfen, ob die Datei auf dem Server vorhanden ist.

So konfigurieren Sie die sichere Überwachung mithilfe von SFTP mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
    string> -secure ( YES | NO )
<!--NeedCopy-->
```

Beispiel:

```
add monitor SFTP_MON USER -scriptname nssftp.pl -scriptargs "file=
    example.txt;user=sam;password=sam_passwd"
<!--NeedCopy-->
```

So konfigurieren Sie die sichere Überwachung mit SFTP mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore** und geben Sie unter **Typ** den Wert **BENUTZER**an.
2. Wählen Sie unter **Spezielle Parameter**unter **Skriptname**die Option nssftp.pl aus.
3. Geben Sie die **Skriptargumente**an.

Festlegen von SSL-Parametern auf einem sicheren Monitor

August 19, 2021

> **Wichtig**
>
> Diese Funktion wird nur bei den neuen Standardprofilen unterstützt. Weitere Informationen zu diesen Profilen finden Sie unter Überblick über die Infrastruktur der erweiterten SSL-Profile.

Ein Monitor erbt entweder die globalen Einstellungen oder die Einstellungen des Dienstes, an den er gebunden ist. Wenn ein Monitor an einen Nicht-SSL- oder Nicht-SSL_TCP-Dienst gebunden ist, z. B. SSL_BRIDGE, können Sie ihn nicht mit SSL-Einstellungen wie der Protokollversion oder den zu verwendenden Verschlüsselungen konfigurieren. Wenn Ihre Bereitstellung eine SSL-basierte Überwachung der Back-End-Server erfordert, ist die Überwachung daher unwirksam.

Sie können mehr Kontrolle über die SSL-basierte Überwachung von Back-End-Servern haben, indem Sie ein SSL-Profil an einen Monitor binden. Ein SSL-Profil enthält SSL-Parameter, Verschlüsselungsbindungen und ECC-Bindungen. Beispielsweise können Sie Serverauthentifizierung, Verschlüsselung und Protokollversion in einem SSL-Profil festlegen und das Profil an einen Monitor binden. Um die Serverauthentifizierung durchzuführen, müssen Sie auch ein CA-Zertifikat an einen Monitor binden. Um die Clientauthentifizierung durchzuführen, müssen Sie ein Clientzertifikat an den Monitor binden. Neue Parameter für den Befehl bind lb monitor ermöglichen dies.

> **Hinweis:**
>
> Die SSL-Einstellungen werden nur wirksam, wenn Sie einen sicheren Monitor hinzufügen. Außerdem muss der SSL-Profiltyp **BackEnd**sein.

Monitortypen, die SSL-Profile unterstützen

SSL-Profile können an folgende Monitortypen gebunden werden:

- HTTP
- HTTP-ECV
- TCP
- TCP-ECV
- HTTP-INLINE

So geben Sie beim Hinzufügen eines Monitors mithilfe der Befehlszeile ein SSL-Profil an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <type> -secure  YES   -sslprofile <string>

set lb monitor <monitorName> <type> -secure YES -sslprofile <string>
<!--NeedCopy-->
```

Beispiel:

```
add ssl profile prof1 -sslProfileType  BackEnd

add lb monitor mon1 HTTP -secure  YES -sslprofile prof1
<!--NeedCopy-->
```


So binden Sie ein Zertifikatschlüsselpaar mit der Befehlszeile an einen Monitor

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind monitor  <monitor name> -certkeyName <string>  [(-CA  [-crlCheck (
    Mandatory | Optional ) | -ocspCheck ( Mandatory | Optional )]
<!--NeedCopy-->
```

SIP-Dienstüberwachung

May 11, 2023

Ein NetScaler verfügt über zwei integrierte Monitore, mit denen Sie SIP-Dienste überwachen können: dieSIP-UDP- und SIP-TCP-Monitore**.** Ein SIP-Monitor überprüft regelmäßig den SIP-Dienst, an den der SIP-Monitor gebunden ist, indem er SIP-Anforderungsmethoden an den SIP-Dienst sendet. Wenn der SIP-Dienst mit einem Antwortcode antwortet, markiert der Monitor den Dienst als UP. Wenn der SIP-Dienst nicht oder falsch reagiert, wird er als DOWN markiert.

Parameter	Spezifiziert
Sipuri	SIP-Adressierungsschema des SIP-Servers.
`sipmethod`	Typ der SIP-Anforderung, die zum Testen des SIP-Dienstes verwendet wird. Geben Sie eine der folgenden Methoden an: INVITE, OPTION (Standardeinstellung), REGISTER
`respcode`	SIP-Antwortcode, mit dem der SIP-Dienst die Prüfungsanforderung antwortet. Standard: 200.

RADIUS-Dienstüberwachung

May 11, 2023

Der RADIUS-Monitor der NetScaler-Appliance überprüft regelmäßig den Status des RADIUS-Dienstes, an den er gebunden ist, indem er eine Authentifizierungsanfrage an den Dienst sendet. Der RADIUS-Server authentifiziert den RADIUS-Monitor und sendet eine Antwort. Standardmäßig erwartet der Monitor vom RADIUS-Server den Antwortcode 2, die standardmäßige Access-Accept-Antwort. Solange der Monitor die entsprechende Antwort erhält, markiert er den Dienst als aktiv.

Hinweis: Der RADIUS-Monitor unterstützt nur die Authentifizierung vom Typ PAP.

- Wenn der Client erfolgreich authentifiziert wurde, sendet der RADIUS-Server eine Access-Accept-Antwort. Der standardmäßige Access-Accept-Antwortcode ist 2, und dies ist der Code, den die Appliance verwendet.
- Wenn sich der Client nicht erfolgreich authentifizieren kann (z. B. wenn der Benutzername, das Passwort oder der geheime Schlüssel nicht übereinstimmen), sendet der RADIUS-Server eine Access-Reject-Antwort. Der Standard-Antwortcode für Zugriffsverweigerung ist 3, und dies ist der Code, den die Appliance verwendet.

Parameter	Spezifiziert
`userName`	Benutzername auf dem RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3-Server. Dieser Benutzername wird in der Sonde verwendet.
Kennwort	Passwort, das bei der Überwachung von RADIUS/NNTP/FTP-EXTENDED/MYSQL/POP3/LDAP-Servern verwendet wird.
Rad-Key	Gemeinsamer geheimer Schlüsselwert, den der RADIUS-Server bei der Client-Authentifizierung verwendet.
Radnasid	NAS-ID, die in der Payload gekapselt wird, wenn eine Zugriffsanfrage gestellt wird.
Radna Sip	Die IP-Adresse, die in der Payload gekapselt ist, wenn eine Zugriffsanfrage gestellt wird. Wenn RadnaSIP nicht konfiguriert ist, sendet die NetScaler-Appliance die zugeordnete IP-Adresse (MIP) als NAS-IP-Adresse an den RADIUS-Server.

Um einen RADIUS-Dienst zu überwachen, müssen Sie den RADIUS-Server, an den er gebunden ist, wie folgt konfigurieren:

1. Fügen Sie den Benutzernamen und das Kennwort des Clients hinzu, den der Monitor zur Authentifizierung verwendet, in die RADIUS-Authentifizierungsdatenbank.
2. Fügen Sie die IP-Adresse und den geheimen Schlüssel des Clients zur entsprechenden RADIUS-Datenbank hinzu.

3. Fügen Sie die IP-Adressen hinzu, die die Appliance zum Senden von RADIUS-Paketen an die RADIUS-Datenbank verwendet. Wenn die NetScaler Appliance mehr als eine zugeordnete IP-Adresse hat oder wenn eine Subnetz-IP-Adresse (SNIP) verwendet wird, müssen Sie für alle IP-Adressen denselben geheimen Schlüssel hinzufügen.

   Achtung: Wenn die von der Appliance verwendete IP-Adresse nicht zur RADIUS-Datenbank hinzugefügt wird, verwirft der RADIUS-Server alle Pakete.

Informationen zum Konfigurieren integrierter Monitore zur Überprüfung des Status des RADIUS-Servers finden Sie unter Konfigurieren von Monitoren in einem Lastenausgleichs-Setup.

Abrechnungsinformationen von einem RADIUS-Server überwachen

May 11, 2023

Sie können einen Monitor, der als *RADIUS-Buchhaltungsmonitor* bezeichnet wird, konfigurieren, um festzustellen, ob der für Authentifizierung, Autorisierung und Accounting (NetScaler AAA) verwendete RADIUS-Server erwartungsgemäß Buchhaltungsinformationen liefert. Der Monitor ist vom Typ RADIUS_ACCOUNTING. Die Sonde wird durch ein Perl-Skript namens nsbmradius.pl generiert, das sich im Verzeichnis /nsconfig/monitors/ befindet. Das Skript sendet aufeinanderfolgende Abrechnungsanforderungstests an den RADIUS-Server. Die Prüfung gilt nur dann als erfolgreich, wenn der RADIUS-Abrechnungsserver mit einem Paket antwortet, dessen Codefeld auf 5 gesetzt ist, was gemäß RFC 2866 auf ein Accounting-Response-Paket hinweist.

Bei der Konfiguration eines RADIUS-Abrechnungsmonitors müssen Sie einen geheimen Schlüssel angeben. Sie können optionale Parameter angeben, von denen jeder ein RADIUS-Attribut darstellt, wie Acct-Status-Type und Framed-IP-Adresse. Informationen zu diesen Attributen finden Sie in RFC 2865, „Remote Authentication Dial In User Service (RADIUS)“ und RFC 2866, „RADIUS Accounting“. „

So konfigurieren Sie einen RADIUS-Abrechnungsmonitor mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen RADIUS-Abrechnungsmonitor zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> RADIUS_ACCOUNTING [-userName <string>] {
 -password  }
  {
 -radKey  }
  [-radNASip <ip_addr>] [-radAccountType <positive_integer>] [-
     radFramedIP <ip_addr>] [-radAPN <string>] [-radMSISDN <string>] [-
     radAccountSession <string>]
```



```
6
7 show lb monitor <monitorName>
8 <!--NeedCopy-->
```

Beispiel

```
1 add lb monitor radAccntMon RADIUS_ACCOUNTING -radKey "8d#>9jr4rV)L7%a2-
     zW13sM"
2 <!--NeedCopy-->
```

DNS- und DNS-TCP-Dienstüberwachung

May 11, 2023

Die NetScaler-Appliance verfügt über zwei integrierte Monitore, mit denen DNS-Dienste überwacht werden können: DNS und DNS-TCP. Wenn ein Monitor an einen Dienst gebunden ist, überprüft er regelmäßig den Status dieses DNS-Dienstes, indem er eine DNS-Anfrage an ihn sendet. Die Abfrage wird in eine IPv4- oder IPv6-Adresse aufgelöst. Diese IP-Adresse wird dann mit der Liste der von Ihnen konfigurierten Test-IP-Adressen verglichen. Die Liste kann bis zu fünf IP-Adressen enthalten. Wenn die aufgelöste IP-Adresse mit mindestens einer IP-Adresse in der Liste übereinstimmt, wird der DNS-Dienst als aktiv markiert. Wenn die aufgelöste IP mit keiner der IP-Adressen in der Liste übereinstimmt, wird der DNS-Dienst als inaktiv markiert.

Parameter	Beschreibung
abfragen	Die DNS-Abfrage (Domänenname), die an den überwachten DNS-Dienst gesendet wird. Standardwert: “\ 007” Wenn die DNS-Abfrage erfolgreich ist, wird der Dienst als UP gekennzeichnet. Ansonsten ist es als DOWN gekennzeichnet. Wenn die DNS-Abfrage erfolgreich ist, wird der Dienst bei einem Rückwärtsmonitor als DOWN gekennzeichnet. Ansonsten ist es als UP gekennzeichnet. Wenn keine Antwort empfangen wird, wird der Dienst als DOWN markiert.
Abfragetyp	Der Typ der DNS-Abfrage, die gesendet wird. Mögliche Werte: Adresse, Zone.

Parameter	Beschreibung
`IPAddress`	Liste der IP-Adressen, die gegen die Antwort auf die DNS-Überwachungsprobe überprüft werden.
IPv6	Aktivieren Sie dieses Kontrollkästchen, wenn die IP-Adresse das IPv6-Format verwendet.

Informationen zum Konfigurieren der integrierten DNS- oder DNS-TCP-Monitore finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

LDAP-Dienstüberwachung

May 11, 2023

Die NetScaler-Appliance verfügt über einen integrierten Monitor, der zur Überwachung von LDAP-Diensten verwendet werden kann: den LDAP-Monitor. Es überprüft regelmäßig den LDAP-Dienst, an den es gebunden ist, indem es sich authentifiziert und eine Suchabfrage an ihn sendet. Wenn die Suche erfolgreich ist, wird der Dienst als UP markiert. Wenn der LDAP-Server den Eintrag nicht findet, wird eine Fehlermeldung an den LDAP-Monitor gesendet, und der Dienst wird mit DOWN gekennzeichnet.

Konfigurieren Sie den LDAP-Monitor so, dass er die Suche definiert, die er beim Senden einer Abfrage durchführen muss. Sie können den Basis-DN-Parameter verwenden, um einen Speicherort in der Verzeichnishierarchie anzugeben, an dem der LDAP-Server die Testabfrage starten muss. Sie können den Parameter Attribut verwenden, um ein Attribut der Zielentität anzugeben.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Spezifiziert
Basis DN	Basisname für den LDAP-Monitor, von dem aus die LDAP-Suche gestartet werden muss. Wenn der LDAP-Server lokal läuft, ist der Standardwert von base dc=`netscaler`, dc=com.
BindDN	BDN-Name für den LDAP-Monitor.

Parameter	Spezifiziert
Filter	Filter für den LDAP-Monitor. Verwenden Sie den Filterparameter in einer Abfrage, um die Anzahl der Ergebnisse zu begrenzen. Wenn Sie diesen Parameter nicht in der Abfrage angeben, gilt der Filter für die gesamte Objektklasse, was eine kostspielige Operation sein kann, z. B. eine hohe CPU-Auslastung.
Kennwort	Passwort, das bei der Überwachung von LDAP-Servern verwendet wird.
Attribut	Attribut für den LDAP-Monitor.

Informationen zum Konfigurieren des integrierten LDAP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

MySQL-Dienstüberwachung

May 11, 2023

Die NetScaler-Appliance verfügt über einen integrierten Monitor, der zur Überwachung von MySQL-Diensten verwendet werden kann: den MySQL-Monitor. Es überprüft regelmäßig den MySQL-Dienst, an den es gebunden ist, indem es eine Suchanfrage an ihn sendet. Wenn die Suche erfolgreich ist, wird der Dienst als UP markiert. Wenn der MySQL-Server nicht reagiert oder die Suche fehlschlägt, wird eine Fehlermeldung an den MySQL-Monitor gesendet und der Dienst wird als DOWN markiert.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Spezifiziert
Datenbank	Datenbank, die für den MySQL-Monitor verwendet wird.
SQL-Abfrage	SQL-Abfrage, die für den MySQL Monitor verwendet wird.

Informationen zum Konfigurieren eines integrierten MySQL-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie MySQL-Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <string>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor mysql1 USER -scriptName nsmysql.pl -scriptArgs "database=cloud;user=cloud;password=password;query=show tables from cloud"
<!--NeedCopy-->
```

SNMP-Dienstüberwachung

May 11, 2023

Die NetScaler-Appliance verfügt über einen integrierten Monitor, der zur Überwachung von SMNP-Diensten verwendet werden kann: den SNMP-Monitor. Es überprüft regelmäßig den SNMP-Agenten auf dem Dienst, an den es gebunden ist, indem es eine Anfrage nach der Unternehmensidentifikations-ID (OID) sendet, die Sie für die Überwachung konfigurieren. Wenn die Abfrage erfolgreich ist, wird der Dienst als UP markiert. Wenn der SNMP-Dienst die von Ihnen angegebene OID findet, ist die Abfrage erfolgreich und der SNMP-Monitor markiert den Dienst als aktiv. Wenn die OID nicht gefunden wird, schlägt die Abfrage fehl und der SNMP-Monitor markiert den Dienst als DOWN.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Spezifiziert
MPOID	OID, die für den SNMP-Monitor verwendet wird.
SNMP-Gemeinschaft	Community, die für den SNMP-Monitor verwendet wird.
SNMP-Schwellenwert	Schwellenwert, der für den SNMP-Monitor verwendet wird.
SNMP-Version	SNMP-Version, die für die Lastüberwachung verwendet wird. Mögliche Werte: V1, V2.

Informationen zum Konfigurieren des integrierten SNMP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

NNTP-Dienstüberwachung

May 11, 2023

Die NetScaler-Appliance verfügt über einen integrierten Monitor, der zur Überwachung von NNTP-Diensten verwendet werden kann: den NNTP-Monitor. Es überprüft regelmäßig den NNTP-Dienst, an den es gebunden ist, indem es eine Verbindung zu dem Dienst herstellt und prüft, ob die von Ihnen angegebene Newsgroup existiert. Wenn die Newsgroup existiert, ist die Suche erfolgreich und der Dienst ist als UP markiert. Wenn der NNTP-Dienst nicht reagiert oder die Suche fehlschlägt, wird der Dienst als DOWN markiert.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Der NNTP-Monitor kann optional so konfiguriert werden, dass er auch eine Testnachricht an die Newsgroup sendet.

Parameter	Spezifiziert
`userName`	Benutzername auf dem RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3-Server. Dieser Benutzername wird in der Sonde verwendet.
Kennwort	Passwort, das bei der Überwachung von RADIUS/NNTP/FTP-EXTENDED/MYSQL/POP3/LDAP-Servern verwendet wird.
Gruppe	Gruppenname, der für den NNTP-Monitor abgefragt werden soll.

Informationen zum Konfigurieren des integrierten NNTP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

POP3-Dienstüberwachung

May 11, 2023

Die NetScaler-Appliance verfügt über einen integrierten Monitor, der zur Überwachung von POP3-Diensten verwendet werden kann: den POP3-Monitor. Es überprüft regelmäßig den POP3-Dienst, an den es gebunden ist, indem es eine Verbindung mit einem POP3-Server herstellt. Wenn der POP3-

Server innerhalb des konfigurierten Zeitraums mit den richtigen Antwortcodes antwortet, markiert er den Dienst als aktiv. Wenn der POP3-Dienst nicht oder falsch reagiert, markiert er den Dienst als DOWN.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Spezifiziert
Nutzername	Benutzername POP3-Server. Dieser Benutzername wird in der Sonde verwendet.
Kennwort	Passwort, das bei der Überwachung von POP3-Servern verwendet wird.
scriptName	Der Pfad und der Name des auszuführenden Skripts.
dispatcherIP	Die IP-Adresse des Dispatchers, an den die Probe gesendet wird.
Dispatcher-Port	Der Port des Dispatchers, an den der Prüfpunkt gesendet wird.

Informationen zum Konfigurieren des integrierten POP3-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie POP3-Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb monitor pop31 USER -scriptName nspop3.pl -scriptArgs "user=
     test@lbmon1.net;password=Freebsd123"
2
3 <!--NeedCopy-->
```


SMTP-Dienstüberwachung

May 11, 2023

Die NetScaler Appliance verfügt über einen integrierten Monitor, der zur Überwachung von SMTP-Diensten verwendet werden kann: den SMTP-Monitor. Der Monitor überprüft den SMTP-Dienst, an den er gebunden ist, indem er eine Verbindung mit ihm öffnet und eine Reihe von Handshakes durchführt, um sicherzustellen, dass der Server ordnungsgemäß funktioniert. Wenn der SMTP-Dienst die Handshakes ordnungsgemäß abgeschlossen hat, markiert der Monitor den Dienst UP. Andernfalls, wenn der SMTP-Dienst nicht reagiert oder falsch reagiert, markiert er den Dienst DOWN.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Spezifiziert
scriptName	Der Pfad und der Name des auszuführenden Skripts.
dispatcherIP	Die IP-Adresse des Dispatchers, an den die Probe gesendet wird.
Dispatcher-Port	Der Port des Dispatchers, an den der Prüfpunkt gesendet wird.

Informationen zum Konfigurieren des integrierten SMTP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

RTSP-Dienstüberwachung

May 11, 2023

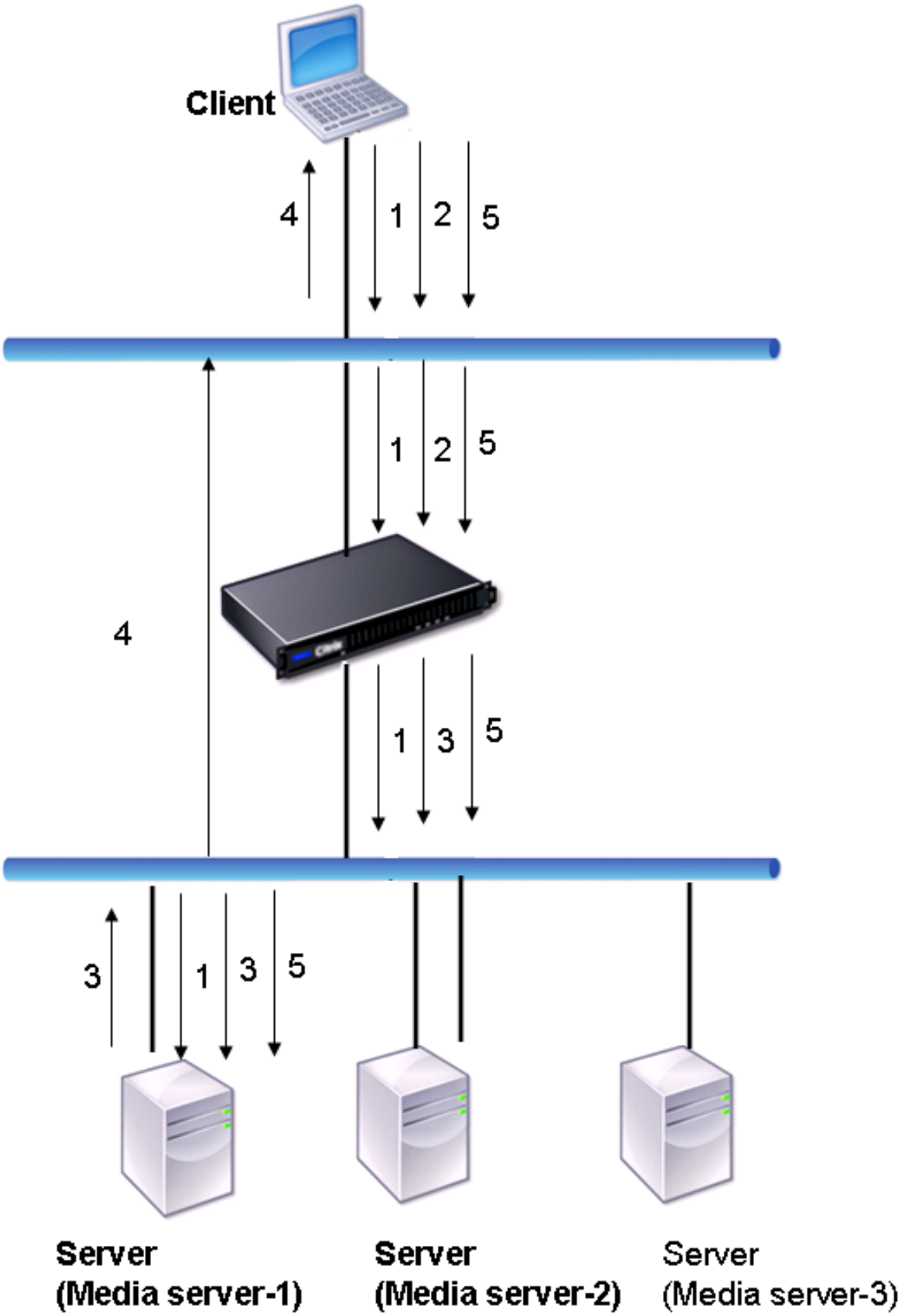
Die NetScaler-Appliance verfügt über einen integrierten Monitor, der zur Überwachung von RTSP-Diensten verwendet werden kann: den RTSP-Monitor. Es überprüft regelmäßig den RTSP-Dienst, an den es gebunden ist, indem es eine Verbindung mit dem RTSP-Server mit Lastausgleich herstellt. Die Art der Verbindung, die geöffnet wird, und die erwartete Reaktion hängen von der Netzwerkkonfiguration ab. Wenn der RTSP-Dienst innerhalb des konfigurierten Zeitraums wie erwartet reagiert, markiert er den Dienst als aktiv. Wenn der Dienst nicht oder falsch reagiert, markiert er den Dienst als INAKTIV.

Die NetScaler-Appliance kann so konfiguriert werden, dass sie RTSP-Server mithilfe von zwei Topologien ausgleicht: NAT-off und NAT-on. RTSP-Server senden ihre Antworten unter Umgehung der Appliance direkt an den Client. Die Appliance muss so konfiguriert sein, dass sie RTSP-Dienste je nach

der von Ihrem Netzwerk verwendeten Topologie unterschiedlich überwacht. Die Appliance kann entweder im Inline- oder Nicht-Inline-Modus sowohl im NAT-Off- als auch im NAT-On-Modus eingesetzt werden.

Im NAT-Off-Modus arbeitet die Appliance als Router: Sie empfängt RTSP-Anfragen vom Client und leitet sie mithilfe der konfigurierten Load-Balancing-Methode an den Dienst weiter, den sie auswählt. Wenn Ihren RTSP-Servern mit Lastausgleich öffentlich zugängliche FQDNs im DNS zugewiesen werden, senden die Load Balancing-Server ihre Antworten direkt an den Client und umgehen dabei die Appliance. Die folgende Abbildung zeigt diese Konfiguration.

Abbildung 1. RTSP im NAT-Off-Modus



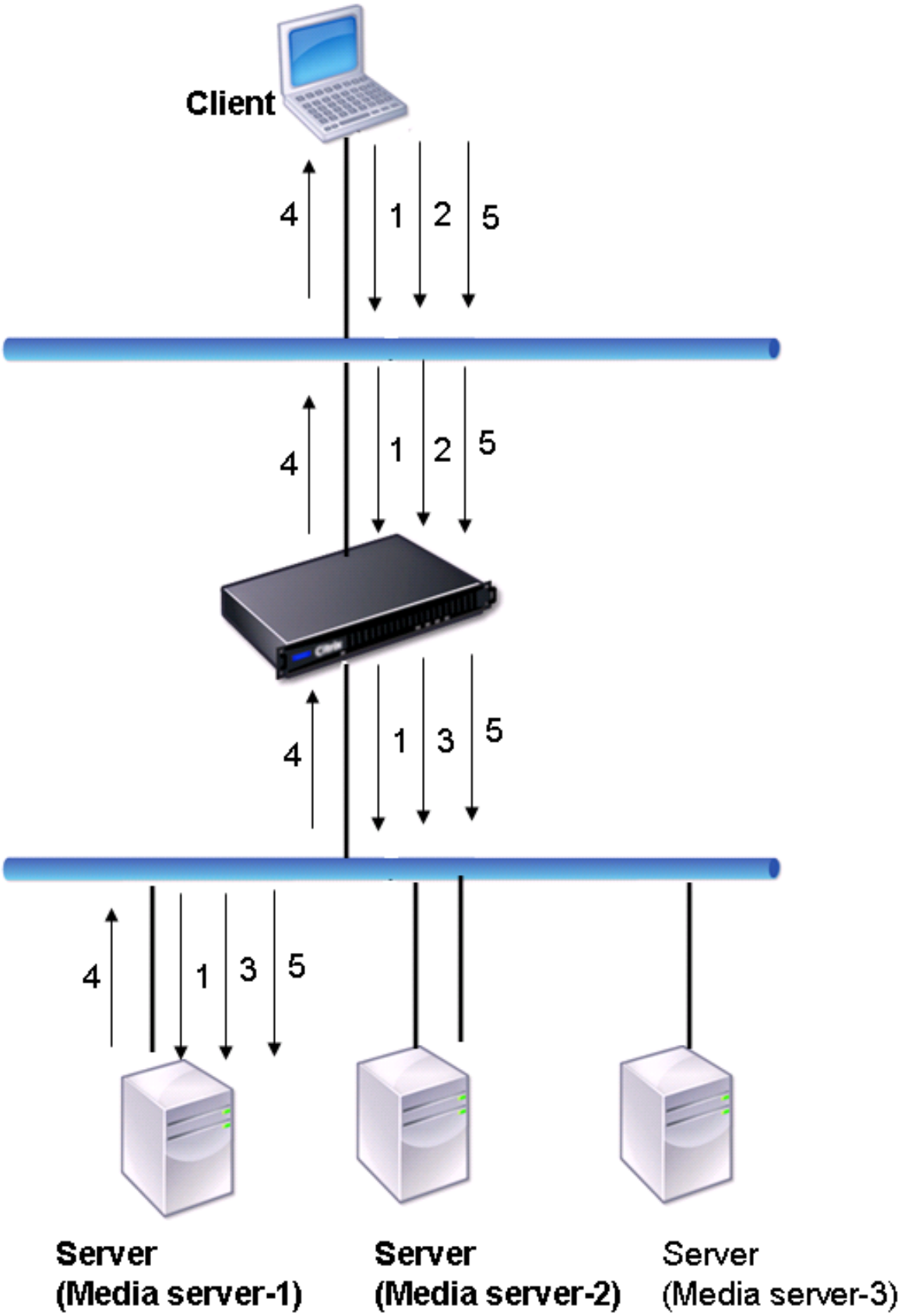
Der Ablauf der Anfragen und Antworten in diesem Szenario sieht wie folgt aus:

1. Der Client sendet eine DESCRIBE-Anfrage an die Appliance. Die Appliance verwendet die konfigurierte Load-Balancing-Methode, um einen Dienst auszuwählen, und leitet die Anfrage an Media Server-1 weiter.
2. Der Client sendet eine SETUP-Anfrage an die Appliance. Wenn die RTSP-Sitzungs-ID in der DESCRIBE-Anfrage ausgetauscht wird, leitet die Appliance die Anforderung mithilfe der RTSPSID-Persistenz an Media Server-1 weiter. Wenn die RTSP-Sitzungs-ID in der SETUP-Anfrage ausgetauscht wird, führt die Appliance einen der folgenden Schritte aus:
   - Wenn die RTSP-Anforderung über dieselbe TCP-Verbindung erfolgt, leitet sie die Anforderung an Media Server-1 weiter, wobei die Persistenz erhalten bleibt.
   - Wenn die Anforderung mit einer anderen TCP-Verbindung eintrifft, verwendet sie die konfigurierte Lastausgleichsmethode, um einen Dienst auszuwählen, und sendet die Anforderung an diesen Dienst, ohne die Persistenz beizubehalten. Dies bedeutet, dass die Anfrage möglicherweise an einen anderen Dienst gesendet wird.
3. Media Server-1 empfängt die SETUP-Anforderung von der Appliance, weist Ressourcen für die Verarbeitung der RTSP-Anforderung zu und sendet die entsprechende Sitzungs-ID an den Client.

   Hinweis: Die Appliance führt kein NAT durch, um die RTSP-Verbindung zu identifizieren, da die RTSP-Verbindungen sie umgehen.
4. Bei nachfolgenden Anfragen verwendet der Client dann die Sitzungs-ID, um die Sitzung zu identifizieren und Kontrollnachrichten an den Medienserver zu senden. Media Server-1 führt die angeforderten Aktionen wie Abspielen, Vorwärts- oder Rückspulen aus.

Im NAT-on-Modus empfängt die Appliance RTSP-Anfragen vom Client und leitet diese Anfragen mithilfe der konfigurierten Load-Balancing-Methode an den entsprechenden Medienserver weiter. Der Medienserver sendet dann seine Antworten über die Appliance an den Client, wie in der folgenden Abbildung dargestellt.

Abbildung 2. RTSP im NAT-on-Modus



Der Ablauf der Anfragen und Antworten in diesem Szenario sieht wie folgt aus:

1. Der Client sendet eine DESCRIBE-Anfrage an die Appliance. Die Appliance verwendet die konfigurierte Load-Balancing-Methode, um einen Dienst auszuwählen, und leitet die Anfrage an Media Server-1 weiter.
2. Der Client sendet eine SETUP-Anfrage an die Appliance. Wenn die RTSP-Sitzungs-ID in der DESCRIBE-Anfrage ausgetauscht wird, leitet die Appliance die Anforderung mithilfe der RTSPSID-Persistenz an Media Server-1 weiter. Wenn die RTSP-Sitzungs-ID in der SETUP-Anfrage ausgetauscht wird, führt die Appliance einen der folgenden Schritte aus:
   - Wenn die RTSP-Anforderung über dieselbe TCP-Verbindung erfolgt, leitet sie die Anforderung an Media Server-1 weiter, wobei die Persistenz erhalten bleibt.
   - Wenn die Anforderung mit einer anderen TCP-Verbindung eintrifft, verwendet sie die konfigurierte Lastausgleichsmethode, um einen Dienst auszuwählen, und sendet die Anforderung an diesen Dienst, ohne die Persistenz beizubehalten. Dies bedeutet, dass die Anfrage möglicherweise an einen anderen Dienst gesendet wird.
3. Media Server-1 empfängt die SETUP-Anforderung von der Appliance, weist Ressourcen für die Verarbeitung der RTSP-Anforderung zu und sendet die entsprechende Sitzungs-ID an den Client.
4. Die Appliance führt NAT durch, um den Client für RTSP-Datenverbindungen zu identifizieren, und die RTSP-Verbindungen werden durch die Appliance geleitet und an den richtigen Client weitergeleitet.
5. Bei nachfolgenden Anfragen verwendet der Client dann die Sitzungs-ID, um die Sitzung zu identifizieren und Kontrollmeldungen an die Appliance zu senden. Die Appliance verwendet die RTSPSID-Persistenz, um den entsprechenden Dienst zu identifizieren, und leitet die Anfrage an Media Server-1 weiter. Media Server-1 führt die angeforderte Aktion aus, z. B. Wiedergabe, Vorlauf oder Rücklauf.

Der RTSP-Monitor verwendet das RTSP-Protokoll, um den Status der RTSP-Dienste auszuwerten. Der RTSP-Monitor stellt eine Verbindung zum RTSP-Server her und führt eine Reihe von Handshakes durch, um sicherzustellen, dass der Server ordnungsgemäß funktioniert.

Parameter	Spezifiziert
RTS-Voranfrage	Die RTSP-Anforderungszeichenfolge, die an den RTSP-Server gesendet wird (z. B. OPTIONS *). Der Standardwert ist 07. Die Länge der Anfrage darf 163 Zeichen nicht überschreiten.
RSP-Code	Satz von Antwortcodes, die vom Dienst erwartet werden.

Anweisungen zum Konfigurieren eines RTSP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

ARP-Anfragen überwachen

May 11, 2023

Die NetScaler-Appliance verfügt über einen integrierten Monitor, der zur Überwachung von ARP-Anfragen verwendet werden kann: den ARP-Monitor. Dieser Monitor sendet regelmäßig eine ARP-Anfrage an den Dienst, an den er gebunden ist, und wartet auf die erwartete Antwort. Wenn es die erwartete Antwort erhält, markiert es den Dienst als aktiv. Wenn es keine oder die falsche Antwort erhält, markiert es den Dienst als DOWN.

ARP sucht eine Hardwareadresse für einen Lastausgleichsserver, wenn nur die Netzwerk-Layer-Adresse bekannt ist. ARP ist mit IPv4 kompatibel, um IP-Adressen in Ethernet-MAC-Adressen zu übersetzen. Die ARP-Überwachung ist für IPv6-Netzwerke nicht relevant und wird daher in diesen Netzwerken nicht unterstützt.

Es gibt keine speziellen Parameter für den ARP-Monitor.

Anweisungen zum Konfigurieren eines ARP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Citrix Virtual Desktops Delivery Controller Service überwachen

May 11, 2023

Bei der Desktop-Virtualisierung kann die NetScaler-Appliance zum Lastausgleich der Citrix Virtual Desktops Delivery Controller-Server verwendet werden, die von der Citrix Virtual Desktops-Umgebung bereitgestellt werden. Die NetScaler-Appliance bietet einen integrierten Monitor, `CITRIX-XD-DDC`, der die Citrix Virtual Desktops Delivery Controller-Server überwacht. Zusätzlich zur Integritätsprüfung können Sie auch überprüfen, ob die Prüfung von einem gültigen Benutzer des Citrix Virtual Desktops Delivery Controller-Servers gesendet wurde.

Der Monitor sendet eine Probe in Form einer XML-Nachricht an den Citrix Virtual Desktops Delivery Controller-Server. Wenn der Server auf die Prüfung mit der Identität der Serverfarm antwortet, wird die Prüfung als erfolgreich betrachtet und der Status des Servers wird als UP markiert. Wenn die HTTP-Antwort keinen Erfolgscode hat oder die Identität der Serverfarm in der Antwort nicht enthalten ist, wird die Prüfung als fehlgeschlagen betrachtet und der Status des Servers wird als DOWN markiert.

Die Option Anmeldeinformationen validieren legt fest, welche Probe vom Monitor an den Citrix Virtual Desktops Delivery Controller-Server gesendet wird, d. h., ob nur der Servername angefordert oder auch die Anmeldeinformationen überprüft werden sollen.

Hinweis: Unabhängig davon, ob die Benutzeranmeldeinformationen (Benutzername, Kennwort und Domäne) auf dem
CITRIX-XD-DDC Monitor angegeben sind, validiert der Citrix Virtual Desktops Delivery Controller-Server die Benutzeranmeldeinformationen nur, wenn die Option zum Überprüfen der Anmeldeinformationen auf dem Monitor aktiviert ist.

Wenn Sie den Assistenten für die Konfiguration des Loadbalancing der Citrix Virtual Desktops-Server verwenden, wird der Monitor CITRIX-XD-DDC automatisch erstellt und an die Citrix Virtual Desktops Delivery Controller-Dienste gebunden.

So fügen Sie mit der Befehlszeilenschnittstelle einen XD-DDC-Monitor mit der Option Anmeldeinformationen validieren hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen XD-DDC-Monitor hinzuzufügen und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> <monitorType> -userName <userName> -
   password <password> -domain <domain_name> -validateCred YES

show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
 > add lb monitor xdddcmon Citrix-xd-ddc -userName Administrator -
    password E12Dc35450a1 -domain dhop -validateCred YES
 Done
> show lb monitor xdddcmon
1) Name......:xdddcmon Type......:CITRIX-XD-DDC State......: ENABLED

Standard parameters:
Interval......:..5 sec...Retries......:..3
Response timeout......:..2 sec...Down time......:..30 sec
Reverse......:..NO...Transparent......:..NO
Secure......:..NO...LRTM......:..ENABLED
Action......:..Not applicable...Deviation......:..0 sec
Destination IP......:..Bound service
Destination port......:..Bound service
Iptunnel......:..NO
TOS......:..NO...TOS ID......:..0
```



```
SNMP Alert Retries......:..0...Success Retries......:..1
Failure Retries......:..0

Special parameters:
User Name..........:"Administrator"
Password...........:*****
DDC Domain.........: "dhop"
Done
<!--NeedCopy-->
```

Um die Option “Anmeldeinformationen validieren” auf einem XD-DDC-Monitor mithilfe der Befehlszeilenschnittstelle anzugeben

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb monitor <monitorName> <monitorType> -userName -password -domain
   <domain_name> -validateCred YES
<!--NeedCopy-->
```

Beispiel:

```
 set lb monitor XD_DDC_21.21.21.22_443_mn CITRIX-xd-ddc -userName
    Administrator -password D123S1R2A123 -domain dhop -validateCred YES
Done
<!--NeedCopy-->
```

So konfigurieren Sie einen XD-DDC-Monitor mit der Option Anmeldeinformationen validieren mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und erstellen Sie einen Monitor des Typs `Citrix-XD-DDC`.

Citrix StoreFront-Stores überwachen

August 15, 2023

Sie können einen Benutzermonitor für einen Citrix StoreFront-Store konfigurieren. Der Monitor bestimmt den Status des StoreFront-Speichers, indem er nacheinander den Kontodienst, den Erkennungsdienst und den Authentifizierungsendpunkt untersucht (wenn der Citrix StoreFront Store ein authentifizierter Speicher ist). Wenn einer dieser Dienste nicht auf den Prüfpunkt reagiert, schlägt

der Monitor Probe fehl, und der StoreFront -Speicher wird als DOWN markiert. Der Monitor sendet Prüfpunkte an die IP-Adresse und den Port des gebundenen Dienstes. Weitere Informationen finden Sie unter Citrix StoreFront Store Services-API.

Hinweis: Monitorsonden stammen von der NSIP-Adresse. Wenn sich das Subnetz eines StoreFront-Servers jedoch von dem der Appliance unterscheidet, wird die Subnetz-IP-Adresse (SNIP) verwendet.

Sie können einen StoreFront-Monitor auch an eine Dienstgruppe binden. Ein Monitor ist an jedes Mitglied der Dienstgruppe gebunden, und die Sonden werden an die IP-Adresse und den Port des gebundenen Mitglieds (Dienst) gesendet. Da jedes Mitglied einer Dienstgruppe nun anhand der IP-Adresse des Mitglieds überwacht wird, können Sie jetzt den StoreFront-Monitor verwenden, um StoreFront-Clusterknoten zu überwachen, die als Mitglieder der Dienstgruppe hinzugefügt wurden.

In früheren Versionen hat der StoreFront Monitor versucht, anonyme Stores zu authentifizieren. Daher kann ein Dienst als DOWN markiert werden und Sie können Citrix Virtual Apps und Citrix Virtual Desktops nicht mithilfe der URL des virtuellen Load-Balancing-Servers starten.

Die Reihenfolge der Tests hat sich geändert. Der Monitor bestimmt nun den Status des StoreFront -Speichers, indem er nacheinander den Kontodienst, das Ermittlungsdokument und dann den Authentifizierungsdienst untersucht und die Authentifizierung für anonyme Speicher überspringt.

Der Hostnamenparameter für StoreFront-Monitore ist veraltet. Der sichere Parameter wird nun verwendet, um zu bestimmen, ob HTTP (Standard) oder HTTPS zum Senden von Monitorprüfungen verwendet werden soll.

Um HTTPS zu verwenden, setzen Sie die sichere Option auf Ja.

Erstellen Sie einen StoreFront-Monitor mit der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen StoreFront-Monitor zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> STOREFRONT <string> -storeName <string> [-
    storefrontacctservice ( YES | NO )] -secure ( YES | NO )

show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel

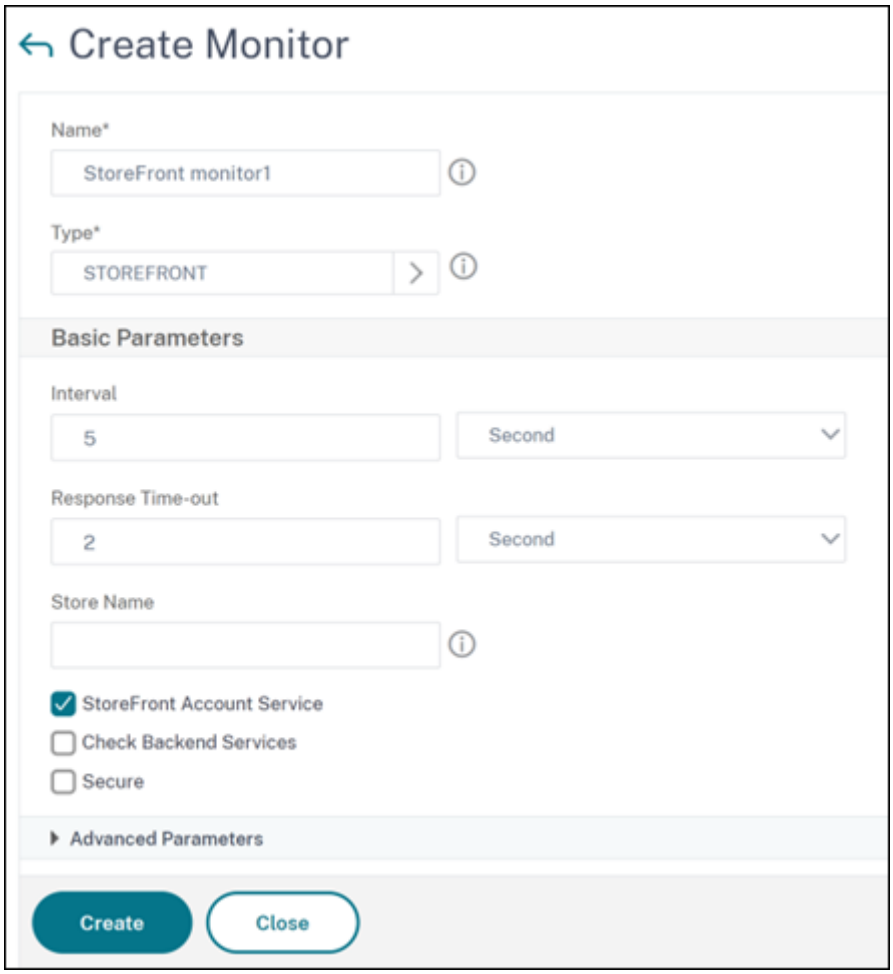
```
add lb monitor storefront_ssl STOREFRONT -storename myStore -
    storefrontacctservice YES -secure YES
<!--NeedCopy-->
```


Erstellen Sie einen StoreFront-Monitor mit der GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und erstellen Sie einen Monitor vom Typ **STOREFRONT**.

Grundlegende Parametereinstellungen:

- Intervall: Das Zeitintervall zwischen zwei aufeinanderfolgenden Sonden. Das Standardzeitintervall ist 5 Sekunden.
- Antwort-Timeout: Die Dauer, für die NetScaler wartet, bevor ein Test als FAILED markiert wird. Die Standarddauer ist 2 Sekunden.
- Store-Name: Der StoreFront-Store, der überwacht werden muss. Standardmäßig verwendet der Benutzermonitor den /Citrix/StoreWeb-Store für die Überwachung.
- StoreFront-Kontodienst: Aktiviert oder deaktiviert Tests für den StoreFront-Kontodienst.
- Backend-Dienste überprüfen: Diese Option ermöglicht die Überwachung von Diensten, die auf dem StoreFront-Server ausgeführt werden.
- Sicher: Aktivieren Sie diese Option, wenn Sie HTTPS verwenden.



> **Hinweis**
>
> Weitere Informationen zu den StoreFront-Monitoren finden Sie in der StoreFront-Dokumentation.

Erweiterter StoreFront-Monitor

NetScaler führt einen erweiterten StoreFront-Monitor ein, der die Authentifizierung und App-Enumeration im Citrix StoreFront-Store im Namen eines Testbenutzerkontos simulieren kann. Sie müssen das Testbenutzerkonto in StoreFront für die Überwachung vorkonfigurieren und aktivieren. Geben Sie die Anmeldeinformationen des Testbenutzers, den Speichernamen und das **nssf_extend.pl-Skript** ein, um die Funktionen dieses Monitors nutzen zu können.

Wenn der StoreFront-Monitor an eine Dienstgruppe gebunden ist, verwendet er die Benutzeranmeldeinformationen, um alle Mitglieder der Dienstgruppe zu überwachen. Daher empfehlen wir, dass Sie die Testbenutzeranmeldeinformationen im Active Directory aller Dienstgruppenmitglieder angeben. Stellen Sie sicher, dass die Anmeldeinformationen des Testbenutzers nicht ablaufen, wenn der Monitor aktiv ist und dass mindestens eine App für den Testbenutzer autorisiert ist.

Konfigurieren Sie den erweiterten StoreFront-Monitor mit der GUI

- Navigieren Sie zu **Traffic Management > Load Balancing > Monitore** und klicken Sie auf **Hinzufügen**.
- Wählen Sie den Typ als **USER**aus.
- Geben Sie im Abschnitt **Grundparameter** die folgenden Details an:
  - **Sichere Argumente**: Geben Sie den Benutzernamen, das Kennwort und den Storenamen in dieses Feld ein. Die Details müssen das Format haben `user=<DomainName\username>;password=<password>;store=/Citrix/StoreWeb`. Wenn der Speichername nicht angegeben wird, `/Citrix/StoreWeb` wird der Standardspeicher für die Überwachung verwendet.
  - **Skriptname**: Wählen Sie das **nssf_extend.pl-Skript** aus.
  - **Intervall** und **Antwortzeitlimit**: Stellen Sie das Zeitintervall und die Reaktion auf höhere Werte ein, vorzugsweise in Minuten. Dadurch wird sichergestellt, dass der Monitortest abgeschlossen ist, da der StoreFront-Monitor mehrere HTTP/HTTPS-Aufrufe durchführt.

Konfigurieren Sie den erweiterten StoreFront-Monitor mit der CLI

Verwenden Sie den folgenden Befehl, um den erweiterten StoreFront-Monitor auf der CLI zu konfigurieren:


```
add lb monitor <monitorName> USER -scriptName nssf_extend.pl -secureArgs "
user=<DomainName\username>;password=<password>;store=/Citrix/StoreWeb;" -
interval 2 Min -resptimeout 1 Min
```

> **Hinweis:**
>
> Verwenden Sie für die Authentifizierung den Parameter Secure Arguments anstelle des Parameters Script Arguments. Der Parameter Secure Arguments speichert die Benutzeranmeldeinformationen in einem verschlüsselten Format.

Fehlermeldungen

In der folgenden Tabelle werden die Fehlermeldungen beschrieben, die angezeigt werden, wenn die Monitorprüfung fehlschlägt. Einzelheiten zum Fehler finden Sie in der Spalte **Beschreibung**.

Fehler	Beschreibung
Unzureichende Anzahl von Argumenten	Der Administrator muss den Benutzernamen und das Kennwort im Parameter Secure Arguments angeben.
Ungültiges Argumentformat	Der Administrator muss die sicheren Argumente im richtigen Format angeben - "user=<DomainName><username>; password=<password>;store=/Citrix/Storeweb oder user=<DomainName><username>; password=<password>
ASP.NET_SessionId oder CSRFToken werden nicht generiert	Der Token CSRF oder die Cookies ASP.NET_SessionId wurden in der Antwort von StoreFront nicht gefunden.
Die Client-Konfiguration konnte nicht abgerufen werden	Der Monitor kann die Client-Konfigurationseinstellungen nicht von StoreFront abrufen.
Das Cookie CtxsDeviceId fehlt	Das Cookie CtxsDeviceId wurde in der Antwort von StoreFront nicht gefunden.
API-Endpunkt für Authentifizierungsmethoden kann nicht abgerufen werden	Der StoreFront-Monitor kann den API-Endpunkt nicht abrufen, um die Liste der konfigurierten Authentifizierungsmethoden abzurufen.

Fehler	Beschreibung
Anmeldung mit Benutzername/Kennwort wird nicht unterstützt	Die Methode für Benutzername und Kennwort ist in StoreFront deaktiviert. Es muss in StoreFront aktiviert sein.
Der Authentifizierungsendpunkt konnte nicht abgerufen werden	Der Endpunkt für die Authentifizierung ist vom Monitor aus nicht erreichbar.
Falscher Benutzername oder falsches Kennwort	Die für den StoreFront-Monitor konfigurierten Testbenutzeranmeldeinformationen sind ungültig.
Falscher Domainname konfiguriert	Der für den StoreFront-Monitor konfigurierte Domainname ist falsch.
Authentifizierung nicht erfolgreich	Die Authentifizierung in StoreFront ist fehlgeschlagen.
Autorisierungs-Cookie wird nicht generiert	Das Autorisierungscookie wurde als Antwort von StoreFront nicht gefunden.
Die Aufzählung enthält nicht alle erforderlichen Felder	Es wurden keine Apps aufgezählt oder die App-Aufzählung war unvollständig.
Fehler bei der App-Aufzählung	Die Aufzählung von Apps aus StoreFront ist fehlgeschlagen.
Abmeldung nicht erfolgreich	Die Abmeldung der Sitzung ist nicht erfolgreich. Dies kann dazu führen, dass sich in StoreFront noch nicht abgelaufene Sitzungen ansammeln.

In den Ausgaben der Befehle `show service <name>` und `show servicegroup <name>` können Sie den Status der Überwachungstest im Feld `Last response` anzeigen.

Beispiel 1:

```
show service svc
State: UP
Last state change was at Wed Aug  2 08:53:37 2023
Time since last state change: 0 days, 00:00:21.900

...

Monitor Name: extended_monitor
State: DOWN    Weight: 1    Passive: 0
Probes: 3    Failed [Total: 3 Current: 3]
```



```
Last response: Failure - Authorization cookie is not generated
Response Time: 5000.000 millisec
<!--NeedCopy-->
```

Beispiel 2:

```
show servicegroup sg_ext_monitor
sg_ext_monitor - HTTP
State: ENABLED Effective State: PARTIAL-UP Monitor Threshold : 0
Max Conn: 0 Max Req: 0 Max Bandwidth: 0 kbits

...

1) Monitor Name: extended_monitor State: ENABLED Weight: 1 Passive: 0
1)   10.106.44.33:80 State: UP Server Name: 10.106.44.33 Server ID:
   None Weight: 1 Order: Default

...

Monitor Name: extended_monitor State: UP Passive: 0
Probes: 4 Failed [Total: 0 Current: 0]
Last response: Success - Probe succeeded.
Response Time: 1.039 millisec
2)    10.106.44.34:80 State: DOWN Server Name: 10.106.44.34 Server ID:
   None Weight: 1 Order: Default

...

Monitor Name: extended_monitor State: DOWN Passive: 0
Probes: 4 Failed [Total: 4 Current: 4]
Last response: Failure - Authorization cookie is not generated
<!--NeedCopy-->
```

Überwachung des Oracle ECV-Dienstes

June 19, 2023

Der Extended Content Verification (ECV) -Monitor auf einem NetScaler kann zur Überwachung von Oracle-Datenbanken verwendet werden. Um den Status jedes Datenbankservers mit Lastausgleich in Echtzeit zu verfolgen, müssen Sie an jeden Dienst einen Oracle ECV-Monitor binden. Der Monitor testet den Dienst, indem er regelmäßige Tests in Form einer SQL-Abfrage an den Dienst sendet. Dies wird manchmal auch als Durchführung einer Integritätsprüfung bezeichnet. Wenn der Oracle

ECV-Monitor zeitnah auf seine Testläufe reagiert und der konfigurierte Ausdruck als wahr ausgewertet wird, markiert er den Service als UP. Wenn er keine zeitnahe Antwort auf die angegebene Anzahl von Testpunkten erhält oder der konfigurierte Ausdruck als falsch ausgewertet wird, markiert er den Dienst als DOWN.
Das Netscaler Oracle ECV-Monitoring unterstützt alle Oracle-Versionen bis 21c und alle kennwortbasierten Authentifizierungsprotokolle.

Nicht unterstützte Sicherheitsfunktionen

Der NetScaler Oracle ECV-Monitor unterstützt nur die kennwortbasierte Authentifizierung. Es unterstützt nicht alle sicherheitsbezogenen Funktionen und Fähigkeiten.

Die folgenden Sicherheitsfunktionen werden nicht unterstützt:

- Datenverschlüsselung (SQLNET.ENCRYPTION_SERVER=erforderlich)
- Datenintegrität (SQLNET.CRYPTO_CHECKSUM_SERVER=erforderlich)
- Lange Kennungen (O8L_LI)
- TLS-Authentifizierung/Verschlüsselung
- Externe Authentifizierungsdienste wie Kerberos und Radius
- Komprimierung
- Oracle-Geldbörse

Benutzerdefinierte Monitore

May 11, 2023

Zusätzlich zu den integrierten Monitoren können Sie benutzerdefinierte Monitore verwenden, um den Status Ihrer Dienste zu überprüfen. Die NetScaler Appliance bietet verschiedene Arten von benutzerdefinierten Monitoren, die auf Skripten basieren, die im NetScaler-Betriebssystem enthalten sind. Die Skripts können verwendet werden, um den Status der Dienste basierend auf der Belastung des Dienstes oder des an den Dienst gesendeten Netzwerkverkehrs zu bestimmen. Benutzerdefinierte Monitore sind die Inline-Monitore, Benutzermonitore und Lastmonitore.

Mit diesen Monitortypen können Sie die mitgelieferte Funktionalität verwenden oder Ihre eigenen Skripts erstellen und diese Skripts verwenden, um den Status des Dienstes zu bestimmen, an den der Monitor gebunden ist.

HTTP-Inline-Monitore konfigurieren

May 11, 2023

Inline-Monitore analysieren und untersuchen die Antworten der Dienste, an die sie gebunden sind, nur wenn diese Dienste Clientanforderungen empfangen. Der Inline-Monitor ist vom Typ HTTP-INLINE und kann nur mit HTTP- und HTTPS-Diensten konfiguriert werden. Ein Inline-Monitor bestimmt, dass der Dienst, an den er gebunden ist, UP ist, indem er seine Antworten auf die Anforderungen überprüft, die an ihn gesendet werden. Wenn keine Clientanforderungen an den Dienst gesendet werden, überprüft der Inline-Monitor den Dienst mithilfe der konfigurierten URL.

Hinweis: Inline-Monitore können nicht an externe oder lokale HTTP- oder HTTPS-Dienste des Global Server Load Balancing (GSLB) gebunden werden, da es sich bei diesen Diensten um virtuelle Server und nicht um tatsächliche Webserver mit Lastausgleich handelt.

Inline-Monitore haben einen Timeout-Wert und eine Anzahl Wiederholungsversuche, wenn die Sonden ausfallen. Sie können einen der folgenden Aktionstypen auswählen, die die NetScaler-Appliance ausführen soll, wenn ein Fehler auftritt:

- **KEINE.** Es werden keine ausdrücklichen Maßnahmen ergriffen. Sie können den Service einsehen und überwachen, und der Monitor zeigt die Anzahl der aktuellen zusammenhängenden Fehlerantworten und der Gesamtzahl der überprüften Antworten an.
- **PROTOKOLLIEREN.** Protokolliert das Ereignis in ns/syslog und zeigt die Zähler an.
- **NACH UNTEN.** Markiert den Dienst als inaktiv und leitet keinen Datenverkehr an den Dienst weiter. Diese Einstellung unterbricht alle dauerhaften Verbindungen zum Dienst. Diese Aktion protokolliert auch das Ereignis und zeigt Leistungsindikatoren an.

Nachdem der Dienst ausgefallen ist, bleibt der Dienst für die konfigurierte Ausfallzeit DOWN. Nach Ablauf der Ausfallzeit verwendet der Inline-Monitor die konfigurierte URL, um den Dienst zu untersuchen, um festzustellen, ob er wieder verfügbar ist. Wenn der Prüfpunkt erfolgreich ist, wird der Status des Dienstes in UP geändert. Der Datenverkehr wird an den Dienst geleitet, und die Überwachung wird wie zuvor fortgesetzt.

Informationen zum Konfigurieren von Inline-Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie HTTP-Inline-Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
1 add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
     <string> -resptimeout <integer> [<units>] -retries <integer> -
     downTime <integer> [<units>] -action <action>
2 <!--NeedCopy-->
```


Beispiel:

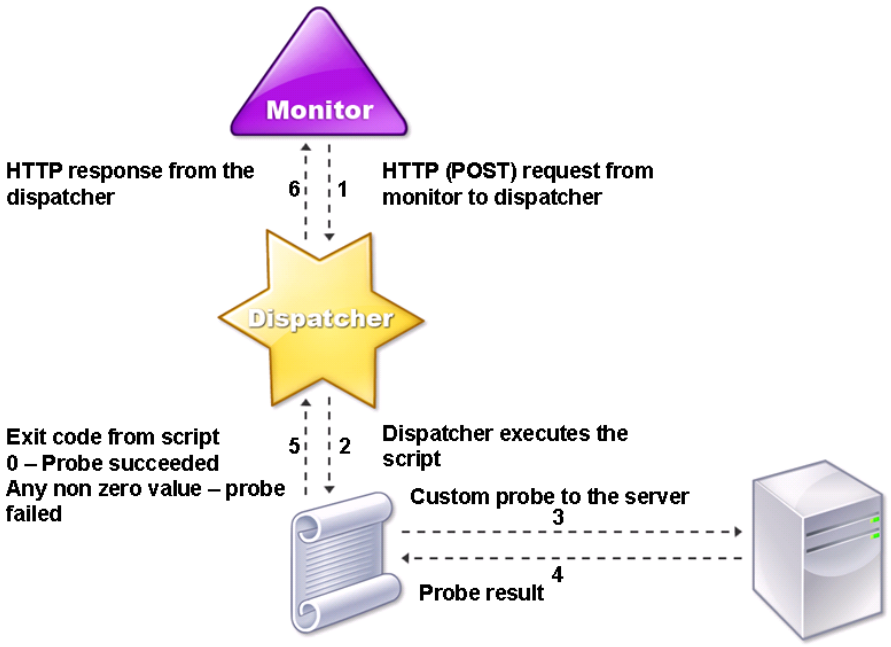
```
add lb monitor http_inline HTTP-INLINE -respCode 200 304 -httpRequest "
    HEAD /var/static/empty.htm" -resptimeout 4 -retries 1 -downTime 2 -
    action NONE
<!--NeedCopy-->
```

Benutzermonitore verstehen

September 1, 2023

Benutzermonitore erweitern den Umfang von benutzerdefinierten Monitoren. Sie können Benutzermonitore erstellen, um den Zustand benutzerdefinierter Anwendungen und Protokolle zu verfolgen, die die NetScaler-Appliance nicht unterstützt. Das folgende Diagramm zeigt, wie ein Benutzermonitor funktioniert.

Abbildung 1. Benutzer-Monitore



Für einen Benutzermonitor sind die folgenden Komponenten erforderlich.

Dispatcher. Ein Prozess auf der Appliance, der Überwachungsanfragen abhört. Ein Dispatcher kann sich auf der Loopback-IP-Adresse (127.0.0.1) und Port 3013 befinden. Dispatcher werden auch als interne Dispatcher bezeichnet. Ein Dispatcher kann auch ein Webserver sein, der das Common Gateway Interface (CGI) unterstützt. Solche Dispatcher werden auch als externe Dispatcher bezeichnet. Sie werden für benutzerdefinierte Skripts verwendet, die nicht in der FreeBSD-Umgebung ausgeführt werden, z. B.

> **Hinweis:**
>
> Sie können den Monitor und den Dispatcher für die Verwendung von HTTPS anstelle von HTTP konfigurieren, indem Sie die Option "sicher" auf dem Monitor aktivieren und als externen Dispatcher konfigurieren. Ein interner Dispatcher versteht jedoch nur HTTP und kann HTTPS nicht verwenden.

In einem HA-Setup wird der Dispatcher sowohl auf den primären als auch auf den sekundären NetScaler-Appliances ausgeführt. Der Dispatcher bleibt auf dem sekundären Gerät inaktiv.

Script. Das Skript ist ein Programm, das benutzerdefinierte Prüfpunkte an den Server mit Lastausgleich sendet und den Antwortcode an den Dispatcher zurückgibt. Das Skript kann einen beliebigen Wert an den Dispatcher zurückgeben, aber wenn eine Prüfung erfolgreich ist, muss das Skript einen Wert von Null (0) zurückgeben. Der Dispatcher betrachtet jeden anderen Wert als Sondenausfall.

Die NetScaler-Appliance ist mit Beispielskripten für häufig verwendete Protokolle gebündelt. Die Skripts sind im Verzeichnis /nsconfig/monitors vorhanden. Wenn Sie ein Script hinzufügen möchten, fügen Sie es dort hinzu. Um ein vorhandenes Skript anzupassen, erstellen Sie eine Kopie mit einem neuen Namen und ändern Sie es.

Wichtig:

- Ab NetScaler Release 13.0 Build 41.20 können Sie das Skript `nsntlm-lwp.pl` verwenden, um einen Monitor zur Überwachung eines sicheren NTLM-Servers zu erstellen.
- Ab Version 10.1 Build 122.17 befinden sich die Skriptdateien für Benutzermonitore an einem neuen Speicherort.

  Wenn Sie eine virtuelle MPX- oder VPX-Appliance auf Version 10.1 Build 122.17 oder höher aktualisieren, lauten die Änderungen wie folgt:

  - Ein neues Verzeichnis namens conflicts wird in /nsconfig/monitors/ erstellt und alle integrierten Skripts der vorherigen Builds werden in dieses Verzeichnis verschoben.
  - Alle neuen integrierten Skripts sind im Verzeichnis /netscaler/monitors/ verfügbar. Alle benutzerdefinierten Skripts sind im Verzeichnis /nsconfig/monitors/ verfügbar.
  - Speichern Sie ein neues benutzerdefiniertes Skript im Verzeichnis /nsconfig/monitors/.
  - Wenn nach Abschluss des Upgrades ein benutzerdefiniertes Skript erstellt und im Verzeichnis /nsconfig/monitors/ gespeichert wird, mit demselben Namen wie das integrierte

Skript, hat das Skript im Verzeichnis /netscaler/monitors/ Vorrang. Das benutzerdefinierte Skript wird nicht ausgeführt.

Wenn Sie eine virtuelle Appliance mit Version 10.1 Build 122.17 oder höher bereitstellen, lauten die Änderungen wie folgt:

- Alle integrierten Skripts sind im Verzeichnis /netscaler/monitors/ verfügbar.
- Das Verzeichnis /nsconfig/monitors/ ist leer.
- Wenn Sie ein benutzerdefiniertes Skript erstellen, müssen Sie es im Verzeichnis /nsconfig/monitors/ speichern.

Damit die Skripts korrekt funktionieren:

- Die maximale Anzahl von Zeichen im Namen des Skripts darf 63 nicht überschreiten.
- Die maximale Anzahl von Script-Argumenten, die einem Script zur Verfügung gestellt werden können, darf 512 nicht überschreiten.
- Die maximale Anzahl von Zeichen, die in den Argumenten des Parameterskripts angegeben werden können, darf 639 nicht überschreiten.

Um das Skript zu debuggen, müssen Sie es mithilfe des nsumon-debug.pl-Skripts von der CLI ausführen. Sie verwenden den Skriptnamen (mit seinen Argumenten), die IP-Adresse und den Port als Argumente des nsumon-debug.pl-Skripts. Benutzer müssen den Skriptnamen, die IP-Adresse, den Port, das Timeout und die Skript-Argumente für das nsumon-debug.pl-Skript verwenden.

Geben Sie bei der CLI Folgendes ein:

```
1 nsumon-debug.pl <scriptname> <IP> <port> <timeout> <partitionID> [
     scriptarguments][is_secure]
2 <!--NeedCopy-->
```

Wichtig: Ab Version 10.5 Build 57.x unterstützen die 11.0-Skriptdateien für Benutzermonitore IPv6-Adressen und beinhalten die folgenden Änderungen:

- Für die folgenden Protokolle wurden neue `pm files` für die IPv6-Unterstützung aufgenommen.
  - RADIUS
  - NNTP
  - POP3
  - SMTP
- Die folgenden Beispielskripte in /netscaler/monitors/ wurden für die IPv6-Unterstützung aktualisiert:
  - nsbmradius.pl
  - nsldap.pl

- nsnntp.pl
- nspop3 nssf.pl
- nssnmp.pl
- nswi.pl
- nstftp.pl
- nssmtp.pl
- nsrdp.pl
- nsntlm-lwp.pl
- nsftp.pl
- nsappc.pl

Stellen Sie nach dem Upgrade auf Version 10.5 Build 57.x oder 11.0 sicher, dass Sie die vorhandenen benutzerdefinierten Skripts mit IPv6-Diensten verwenden möchten, die vorhandenen benutzerdefinierten Skripts mit den Änderungen in den aktualisierten Beispielskripten in /netscaler/monitors/aktualisieren.

> **Hinweis:**
>
> Das Beispielskript nsmysql.pl unterstützt die IPv6-Adresse nicht. Wenn ein IPv6-Dienst an einen Benutzermonitor gebunden ist, der nsmysql.pl verwendet, schlägt der Test fehl.

- Die folgenden LB-Monitortypen wurden aktualisiert, um IPv6-Adressen zu unterstützen:
  - USER
  - SMTP
  - NNTP
  - LDAP
  - SNMP
  - POP3
  - FTP_EXTENDED
  - StoreFront
  - APPC
  - CITRIX_WI_EXTENDED

  Wenn Sie ein benutzerdefiniertes Skript erstellen, das einen dieser LB-Monitortypen verwendet, stellen Sie sicher, dass Sie IPv6-Unterstützung in das benutzerdefinierte Skript aufnehmen. Beziehen Sie sich auf das zugehörige Beispielskript in /netscaler/monitors/ für die Änderungen, die Sie im benutzerdefinierten Skript für die IPv6-Unterstützung vornehmen müssen.

Um den Status des Servers zu verfolgen, sendet der Monitor eine HTTP-POST-Anforderung an den konfigurierten Dispatcher. Diese POST-Anfrage enthält die IP-Adresse und den Port des Servers sowie das Skript, das ausgeführt werden muss. Der Dispatcher führt das Skript als untergeordneten Prozess mit benutzerdefinierten Parametern (falls vorhanden) aus. Anschließend sendet das Skript einen Prüfpunkt an den Server. Das Skript sendet den Status der Sonde (Antwortcode) an den Dispatcher. Der Dispatcher wandelt den Antwortcode in eine HTTP-Antwort um und sendet ihn an den Monitor. Basierend auf der HTTP-Antwort markiert der Monitor den Dienst als hoch oder unten.

Die NetScaler-Appliance protokolliert die Fehlermeldungen in der Datei /var/nslog/nsumond.log, wenn die Prüfungen der Benutzerüberwachung fehlschlagen. Diese detaillierten Fehlermeldungen werden in der GUI und in der CLI für die Befehle `show service`/`service group` angezeigt.

In der folgenden Tabelle sind die Benutzermonitore und die möglichen Gründe für einen Fehler aufgeführt.

Typ des Benutzermonitors	Gründe für Sondenausfall
SMTP	Monitor stellt keine Verbindung zum Server her.
NNTP	Monitor stellt keine Verbindung zum Server her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Monitor findet die NNTP-Gruppe nicht.
LDAP	Monitor stellt keine Verbindung zum Server her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Monitor bindet nicht an den LDAP-Server.
	Monitor findet keinen Eintrag für die Zielentität im LDAP-Server.
FTP	Die Verbindung zum Server ist ab.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Anmeldung fehlgeschlagen.
	Monitor findet die Datei nicht auf dem Server.

Typ des Benutzermonitors	Gründe für Sondenausfall
POP3	Monitor stellt keine Verbindung zur Datenbank her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Anmeldung fehlgeschlagen.
	Die Vorbereitung der SQL-Abfrage schlägt fehl.
	Die Ausführung der SQL-Abfrage schlägt fehl.
SNMP	Monitor stellt keine Verbindung zur Datenbank her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Anmeldung fehlgeschlagen.
	Monitor kann die SNMP-Sitzung nicht erstellen.
	Monitor findet den Objektbezeichner nicht.
	Die Einstellung des Monitorschwellenwerts ist größer oder gleich dem tatsächlichen Schwellenwert des Monitors.
RDP (Windows Terminalserver)	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Monitor kann keinen Socket erstellen.
	In Versionen stimmt nicht überein.
	Der Monitor kann die Verbindung nicht bestätigen.

Sie können die Protokolldatei über die CLI anzeigen, indem Sie die folgenden Befehle verwenden:

```
1 > shell
2 root@ns# cat /var/nslog/nsumond.log
3 root@ns# exit
4 >
5 <!--NeedCopy-->
```


Der Befehl öffnet eine BSD-Shell, zeigt die Protokolldatei auf dem Bildschirm an, schließt die BSD-Shell und bringt Sie zur CLI zurück.

Vor NetScaler Version 13.0 Build 52.X zeigte der Befehl `show service/service group` eine generische Fehlermeldung an, die besagte, dass “Probe fehlgeschlagen” als Ursache für den Fehler des Benutzermonitorprüfens war.

Beispiel:

```
show service ftp

Monitor Name: mon2
State: UNKNOWN  Weight: 1   Passive: 0
Probes: 3    Failed [Total: 0 Current: 0]
Last response: Failure - Probe failed.
Response Time: 1071.838 millisec
<!--NeedCopy-->
```

Ab NetScaler Version 13.0 Build 52.X zeigt der Befehl `show service/service group` die tatsächliche Ursache für den Fehler des Benutzermonitorprüfens an.

Beispiel:

```
show service ftp

Monitor Name: mon2
State: DOWN   Weight: 1   Passive: 0
Probes: 729   Failed [Total: 726 Current: 726]
Last response: Failure - Login failed.
Response Time: 8000.0 millisec
<!--NeedCopy-->
```

Benutzermonitore haben auch einen Timeout-Wert und eine Anzahl von Wiederholungsversuchen für Sondenausfälle. Sie können Benutzermonitore mit Nicht-Benutzermonitoren verwenden. Bei hoher CPU-Auslastung ermöglicht ein Nicht-Benutzermonitor eine schnellere Erkennung eines Serverausfalls.

Wenn der Prüfpunkt des Benutzermonitors bei hoher CPU-Auslastung eine Zeitdauer aufweist, bleibt der Status des Dienstes unverändert.

Example1:

```
add lb monitor <name> USER  -scriptname <script-name> -resptimeout 5
   seconds
<!--NeedCopy-->
```


> Hinweis
>
> Für skriptfähige Monitore muss das Antwort-Timeout auf einen Wert konfiguriert werden, der dem erwarteten Timeout entspricht + 1 Sekunde. Wenn Sie beispielsweise erwarten, dass das Timeout 4 Sekunden beträgt, konfigurieren Sie das Antwort-Timeout auf 5 Sekunden.

Example2:

```
add lb monitor <name> USER -scriptname <script-name> -scriptargs <
    Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wir empfehlen, den `secureargs` Parameter anstelle des `scriptargs` Parameters für alle sensiblen Daten zu verwenden, die sich auf die Skripts beziehen.

Wie benutzt man einen Benutzermonitor, um Websites zu überprüfen

September 11, 2023

Sie können einen Benutzermonitor so konfigurieren, dass er nach bestimmten Websiteproblemen prüft, die von HTTP-Servern mit bestimmten HTTP-Codes gemeldet werden. In der folgenden Tabelle sind die HTTP-Antwortcodes aufgeführt, die dieser Benutzermonitor erwartet.

HTTP-Antwortcode	Bedeutung
200 - Erfolg	Erfolg der Untersuchung.
503 - Dienst nicht verfügbar	Ausfall der Sonde.
404 - nicht gefunden	Das Skript wurde nicht gefunden oder kann nicht ausgeführt werden.
500 - Interner Serverfehler	Interner Fehler/Ressourceneinschränkungen im Dispatcher (zu wenig Speicher, zu viele Verbindungen, unerwarteter Systemfehler oder zu viele Prozesse). Der Service ist nicht mit DOWN markiert.
400 - schlechte Anfrage	Fehler beim Parsen der HTTP-Anfrage.
502 - falsches Gateway	Fehler beim Dekodieren der Antwort des Skripts.

Konfigurieren Sie den Benutzermonitor für HTTP mithilfe der folgenden Parameter.

Parameter	Spezifiziert
scriptName	Der Pfad und der Name des auszuführenden Skripts.
scriptArgs	Die Zeichenketten, die zu den POST-Daten hinzugefügt werden. Ein Backslash (\) -Zeichen im ScriptArgs-Parameter muss mit einem zusätzlichen umgekehrten Schrägstrich maskiert werden, damit der Parameter wie vorgesehen funktioniert. Verwenden Sie zum Beispiel \\n anstelle von \n.
dispatcherIP	Die IP-Adresse des Dispatchers, an den die Probe gesendet wird.
Dispatcher-Port	Der Port des Dispatchers, an den der Prüfpunkt gesendet wird.
Lokaler Dateiname	Der Name einer Monitor-Skriptdatei auf dem lokalen System.
Zielpfad	Ein bestimmter Speicherort auf der NetScaler Appliance, in dem die hochgeladene lokale Datei gespeichert ist.

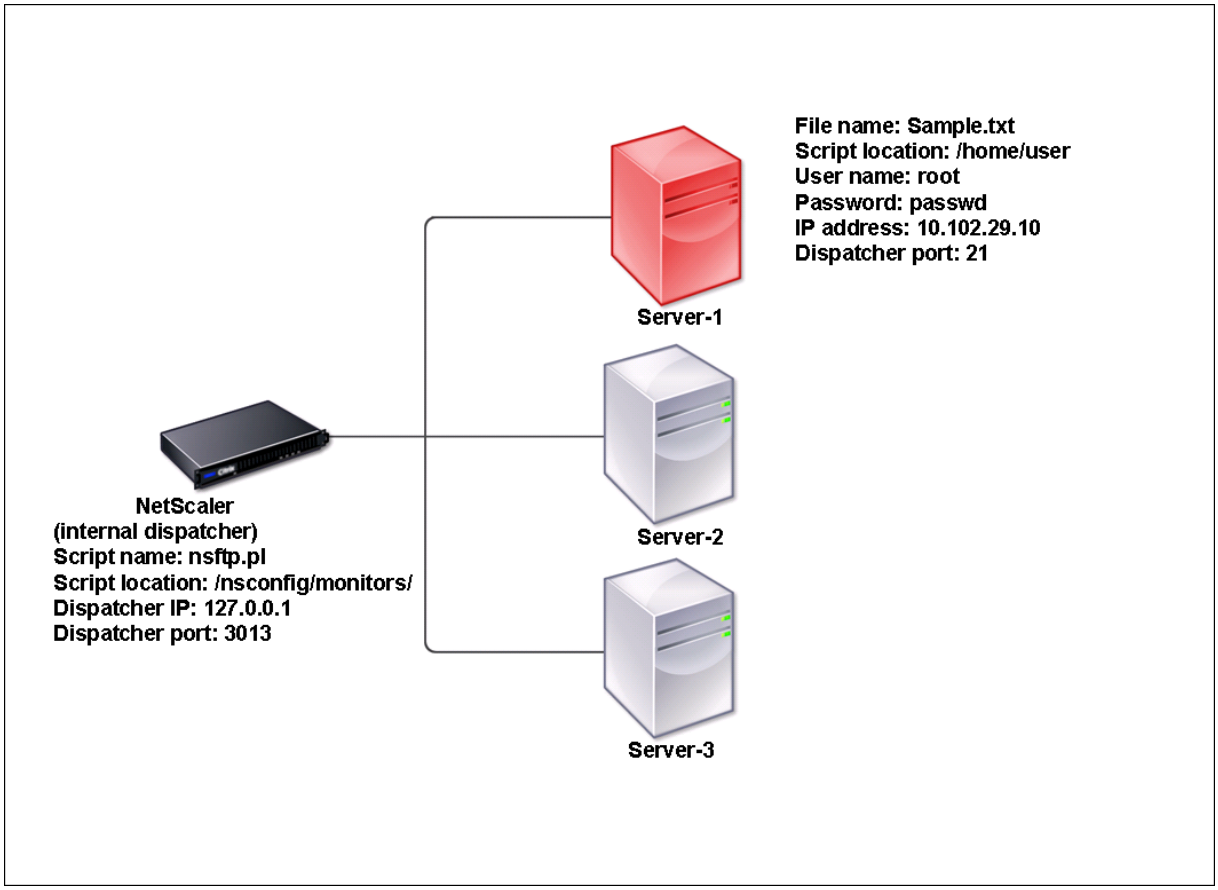
Informationen zum Erstellen eines Benutzermonitors zur Überwachung von HTTP finden Sie unter Monitore in einem Load Balancing-Setup konfigurieren.

Den internen Dispatcher verstehen

May 11, 2023

Sie können einen benutzerdefinierten Benutzermonitor mit dem internen Dispatcher verwenden. Stellen Sie sich einen Fall vor, in dem Sie den Zustand eines Servers anhand des Vorhandenseins einer Datei auf dem Server verfolgen müssen. Das folgende Diagramm veranschaulicht dieses Szenario.

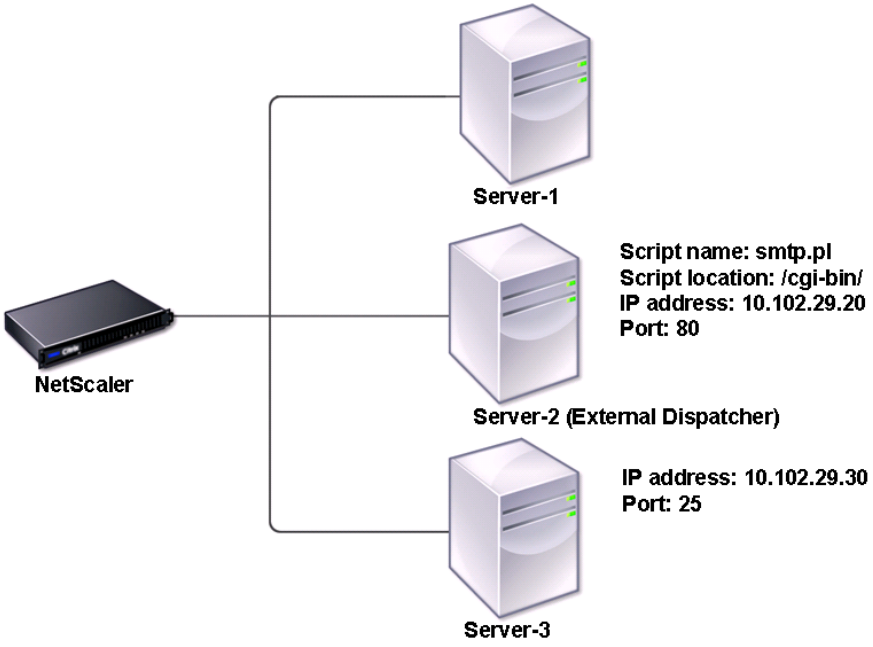
Abbildung 1. Verwenden eines Benutzermonitors mit dem internen Dispatcher



Eine mögliche Lösung besteht darin, ein Perl-Skript zu verwenden, das eine FTP-Sitzung mit dem Server initiiert und auf das Vorhandensein der Datei überprüft. Anschließend können Sie einen Benutzermonitor erstellen, der das Perl-Skript verwendet. Die NetScaler-Appliance enthält ein solches Perl-Skript (nsftp.pl) im Verzeichnis /nsconfig/monitors/.

Sie können einen Benutzermonitor mit einem externen Dispatcher verwenden. Stellen Sie sich einen Fall vor, in dem Sie den Zustand eines Servers anhand des Status eines SMTP-Dienstes auf einem anderen Server verfolgen müssen. Dieses Szenario wird in der folgenden Abbildung veranschaulicht.

Abbildung 2. Verwenden eines Benutzermonitors mit einem externen Dispatcher



Eine mögliche Lösung wäre das Erstellen eines Perl-Skripts, das den Status des SMTP-Dienstes auf dem Server überprüft. Anschließend können Sie einen Benutzermonitor erstellen, der das Perl-Skript verwendet.

Benutzermonitor konfigurieren

May 11, 2023

Benutzermonitore verfolgen den Zustand benutzerdefinierter Anwendungen und Protokolle, die eine NetScaler-Appliance nicht unterstützt. Dies ist ein erweiterter Umfang an benutzerdefinierten Monitoren. Um einen Benutzermonitor zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Schreiben Sie ein Skript, das die daran gebundenen Dienste überwachen kann.
- Laden Sie das Skript in das Verzeichnis `/nsconfig/monitors` auf der NetScaler-Appliance hoch.
- Geben Sie eine ausführbare Berechtigung für das Skript.

Wenn der Monitortyp ein Protokoll ist, das die Appliance nicht unterstützt, müssen Sie nur einen Monitor vom Typ **USER**verwenden. Benutzermonitore unterstützen nur Perl- und Bash-Skripte. Sie unter-

stützen keine Python-Skripte.

> **Hinweis**
>
> Monitorsonden stammen von der NSIP-Adresse. Für den Monitortyp **USER** konfigurierte `scriptargs` wird in den laufenden Konfigurations- und ns.conf-Dateien angezeigt.

Weitere Informationen zu Monitoren finden Sie unter Konfigurieren von Monitoren.

So konfigurieren Sie einen Benutzermonitor über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> USER -scriptname <NameOfScript> -
   scriptargs <Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

Example1:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
   =/home/user/
sample.txt;user=root;password=passwd"
<!--NeedCopy-->
```

Example2:

```
add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
   =/home/user/
sample.txt -secureargs "user=root;password=passwd"
<!--NeedCopy-->
```

> Hinweis
>
> Der Parameter `secureargs` speichert die Skriptsrgumente in einem verschlüsselten Format anstelle des Nur-Text-Formats. Citrix empfiehlt, den Parameter `secureargs` anstelle des scriptargs-Parameters für alle vertraulichen Daten in den Skripts zu verwenden, z. B. Benutzername und Kennwort. Wenn Sie beide Parameter zusammen verwenden möchten, muss das in `-scriptname` angegebene Skript die Argumente in dieser Reihenfolge akzeptieren: `<scriptargs> <secureargs>`. Geben Sie die ersten Argumente im Parameter `<scriptargs>` an; und den Rest der Argumente im Parameter `<secureargs>`. Das heißt, behalten Sie die für die Argumente definierte Reihenfolge bei. Sichere Argumente gelten nur für den internen Dispatcher. Wenn Sie einen externen Dispatcher verwenden möchten, empfiehlt Citrix, die anfälligen Daten in Ihren Skripten zu sichern.

Beispiel 3:

Angenommen, Sie haben den Parameter `scriptargs` bereits mit den Argumenten konfiguriert: “a=b; c=d; e=f”.

```
add monitor mon1 USER -scriptargs "a=b;c=d;e=f"
<!--NeedCopy-->
```

Wenn Sie den Parameter `secureargs` anstelle des Parameters `scriptargs` verwenden möchten, gehen Sie wie folgt vor:

- Nullifizieren Sie den Parameter `scriptargs`.
- Geben Sie alle Argumente unter Parameter `secureargs` an.

```
set monitor mon1 USER -scriptargs "" -secureargs "a=b;c=d;e=f"
<!--NeedCopy-->
```

So konfigurieren Sie einen Benutzermonitor über die GUI

1. Navigieren Sie zu **Traffic Management> Load Balancing> Monitore**und klicken Sie auf **Hinzufügen**.
2. Gehen Sie auf der Seite **Monitor erstellen** wie folgt vor:
   - Wählen Sie den Monitortyp als **USER**aus.
   - Wähle das Script aus dem Dropdown-Menü aus oder lade dein eigenes Script hoch.
   - Geben Sie die entsprechenden Werte für die Felder **Script-Argumente** und **sichere Argumente** ein.
   - Klicken Sie auf **Erstellen**.

   Ein Benutzermonitor wird erstellt.

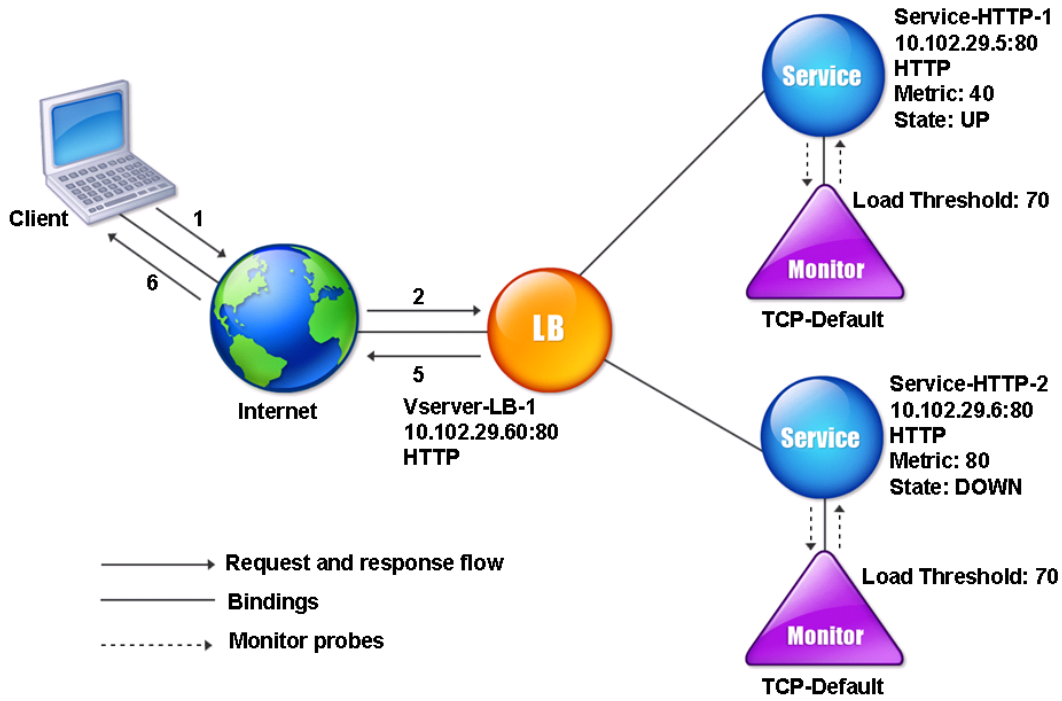
Lastmonitore

May 11, 2023

Lastmonitore verwenden SNMP-abgefragte OIDs, um die Last zu berechnen. Der Load Monitor verwendet für die Abfrage die IP-Adresse des Dienstes, an den er gebunden ist (die Ziel-IP-Adresse). Es sendet eine SNMP-Anfrage an den Dienst, in der die OID für eine Metrik angegeben wird. Bei den Metriken kann es sich um CPU, Arbeitsspeicher oder Anzahl der Serververbindungen handeln. Der Server antwortet auf die Anfrage mit einem Metrikwert. Der metrische Wert in der Antwort wird mit dem Schwellenwert verglichen. Die NetScaler-Appliance berücksichtigt den Dienst nur dann für den Lastenausgleich, wenn die Metrik unter dem Schwellenwert liegt. Der Dienst mit dem niedrigsten Lastwert wird zuerst betrachtet.

Das folgende Diagramm veranschaulicht einen Lastmonitor, der für die Dienste konfiguriert ist, die im grundlegenden Lastenausgleichs-Setup beschrieben sind, das unter Einrichten von Basic Load Balancingbeschrieben wurde.

Abbildung 1. Betrieb von Lastmonitoren



Hinweis: Der Lastmonitor bestimmt nicht den Status des Dienstes. Es ermöglicht der Appliance nur, den Dienst für den Lastenausgleich zu berücksichtigen.

Nachdem Sie den Load Monitor konfiguriert haben, müssen Sie dann die Metriken konfigurieren, die der Monitor verwenden soll. Bei der Lastbeurteilung berücksichtigt der Lastmonitor Serverparameter, sogenannte Metriken, die in den Metriktabellen der Appliance-Konfiguration definiert sind. Es gibt zwei Arten von metrischen Tabellen:

- **Lokal:** Diese Tabelle ist standardmäßig in der Appliance vorhanden. Es besteht aus vier Metriken: Verbindungen, Pakete, Antwortzeit und Bandbreite. Die Appliance spezifiziert diese Metriken für einen Dienst, und SNMP-Abfragen stammen nicht für diese Dienste. Diese Metriken können nicht geändert werden.
- **Benutzerdefiniert.** Eine benutzerdefinierte Tabelle. Jede Metrik ist mit einer OID verknüpft.

Standardmäßig generiert die Appliance die folgenden Tabellen:

- NetScaler

- RADWARE
- CISCO-CSS
- LOKAL
- GIESSEREI
- ALTEON

Sie können entweder die von der Appliance generierten Metriktabellen hinzufügen, oder Sie können Tabellen Ihrer Wahl hinzufügen, wie in der folgenden Tabelle dargestellt. Die Werte in der metrischen Tabelle dienen nur als Beispiele. Berücksichtigen Sie in einem tatsächlichen Szenario die tatsächlichen Werte für die Metriken.

Metrischer Name	OIDs	Gewicht	Schwellenwert
CPU	1.2.3.4	2	70
Speicher	4.5.6.7	3	80
Verbindungen	5.6.7.8	4	90

Um die Last für eine oder mehrere Metriken zu berechnen, weisen Sie jeder Metrik eine Gewichtung zu. Das Standardgewicht ist 1. Das Gewicht stellt die Priorität dar, die jeder Metrik eingeräumt wird. Wenn das Gewicht hoch ist, ist die Priorität hoch. Die Appliance wählt einen Dienst aus, der auf dem SOURCEIPDESTIP-Hash-Algorithmus basiert.

Sie können auch den Schwellenwert für jede Metrik festlegen. Der Schwellenwert ermöglicht es der Appliance, einen Dienst für den Lastenausgleich auszuwählen, wenn der Metrikwert für den Dienst unter dem Schwellenwert liegt. Der Schwellenwert bestimmt auch die Auslastung der einzelnen Dienste.

Lastmonitore konfigurieren

March 10, 2023

Um einen Lastmonitor zu konfigurieren, erstellen Sie zuerst den Lastmonitor. Anweisungen zum Erstellen eines Monitors finden Sie unter Erstellen von Monitoren. Wählen oder erstellen Sie als Nächstes die Metriktabelle, um eine Reihe von Metriken zu definieren, die den Status des Servers bestimmen, und (wenn Sie eine Metriktabelle erstellen) jede Metrik an die Metriktabelle binden.

So erstellen Sie eine Metriktabelle mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:


```
add lb metricTable <metricTableName>

bind lb metricTable <metricTableName> <metric> <SNMPOID>
<!--NeedCopy-->
```

Beispiel:

```
add lb metricTable Table-Custom-1

bind lb metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5 11
<!--NeedCopy-->
```

Um mithilfe des Konfigurationsprogramms eine Metriktabelle zu erstellen und Metriken daran zu binden

1. Navigieren Sie zu **Traffic Management > Load Balancing > Metriktabellen**, und erstellen Sie eine Metriktabelle.
2. Um Metriken zu binden, klicken Sie auf **Binden** und geben Sie eine Metrik und eine SNMP-OID an.

Aufheben der Bindung von Metriken aus einer Metriktabelle

January 19, 2021

Sie können die Bindung von Metriken aus einer Metriktabelle aufheben, wenn die Metriken geändert werden müssen oder wenn Sie die Metriktabelle vollständig entfernen möchten.

So heben Sie die Bindung von Metriken aus einer Metrik-Tabelle mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind lb metricTable <metricTable> <metric>
<!--NeedCopy-->
```

Beispiel:

```
unbind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5
<!--NeedCopy-->
```


So heben Sie die Bindung von Metriken aus einer Metrik-Tabelle mit dem Konfigurationsdienstprogramm auf

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Metrik-Tabellen** .
2. Öffnen Sie eine Metriktabelle, wählen Sie eine Metrik aus, und klicken Sie auf **Löschen**.

Sie können die Details aller konfigurierten Metriktabellen anzeigen, wie Name und Typ, um festzustellen, ob die Metriktabelle intern oder erstellt und konfiguriert ist.

Reverse Monitoring für einen Dienst konfigurieren

May 11, 2023

Ein Reverse-Monitor markiert einen Dienst als DOWN, wenn die Prüfkriterien erfüllt sind, und als UP, wenn sie nicht erfüllt sind. Wenn Sie beispielsweise möchten, dass ein Backup-Dienst nur dann Datenverkehr empfängt, wenn der primäre Dienst AUSGESCHALTET ist, können Sie einen Reverse-Monitor an den sekundären Dienst binden, ihn aber so konfigurieren, dass er den primären Dienst überprüft.

Die NetScaler-Appliance unterstützt die folgenden Reverse-Monitore:

- HTTP
- ICMP
- TCP (ab Version 11.1 Build 49.x)

Konfiguration des HTTP-Reverse-Monitorings für einen Dienst

In der folgenden Tabelle werden die Bedingungen für die direkte und umgekehrte HTTP-Überwachung für einen Dienst beschrieben:

Bedingung	Direkt	Umgekehrt
Verbindung wurde nicht hergestellt.	Scheitern	Scheitern
Der HTTP-Antwortcode entspricht den Spezifikationen der Sonde.	Erfolg	Scheitern
Der HTTP-Antwortcode entspricht nicht den Spezifikationen der Sonde.	Scheitern	Erfolg
Das Zeitlimit für die Sonde ist abgelaufen.	Scheitern	Scheitern

So konfigurieren Sie das HTTP-Reverse-Monitoring für einen Dienst mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <Monitor_Name> HTTP -respCode 200 -httpRequest "HEAD /"
   -destIP <Primary_Service_IP_Address> -destPort 80 -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Konfiguration von ICMP Reverse Monitoring für einen Dienst

In der folgenden Tabelle werden die Bedingungen für die direkte und umgekehrte ICMP-Überwachung für einen Dienst beschrieben:

Bedingung	Direkt	Umgekehrt
Die ICMP-Echoantwort wurde empfangen.	Erfolg	Scheitern
Das Zeitlimit für die Sonde ist abgelaufen.	Scheitern	Erfolg

So konfigurieren Sie das ICMP-Reverse-Monitoring für einen Dienst mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <Monitor_Name> PING -destIP <Primary_Service_IP_Address>
    -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

TCP-Reverse-Monitoring für einen Dienst konfigurieren

Wenn ein direkter TCP-Monitor als Antwort auf eine Monitorprüfung einen RESET empfängt, wird der Dienst als DOWN markiert. Wenn ein Reverse-TCP-Monitor jedoch eine RESET-Antwort empfängt, gilt die Prüfung als erfolgreich und der Dienst wird als UP markiert.

In der folgenden Tabelle werden die Bedingungen der TCP-Reverse-Überwachung für einen Dienst beschrieben:

Bedingung	Direkt	Umgekehrt
Die TCP-Verbindung ist hergestellt.	Erfolg	Scheitern
Das Zeitlimit für die Sonde ist abgelaufen.	Scheitern	Scheitern
Die Antwort auf die Sonde ist RESET.	Scheitern	Erfolg

So konfigurieren Sie die TCP-Reverse-Überwachung für einen Dienst mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <Monitor_Name> TCP -destip <Primary_Service_IP_Address>
    -destport <primary_service_port> -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

So konfigurieren Sie die umgekehrte Überwachung mithilfe der GUI

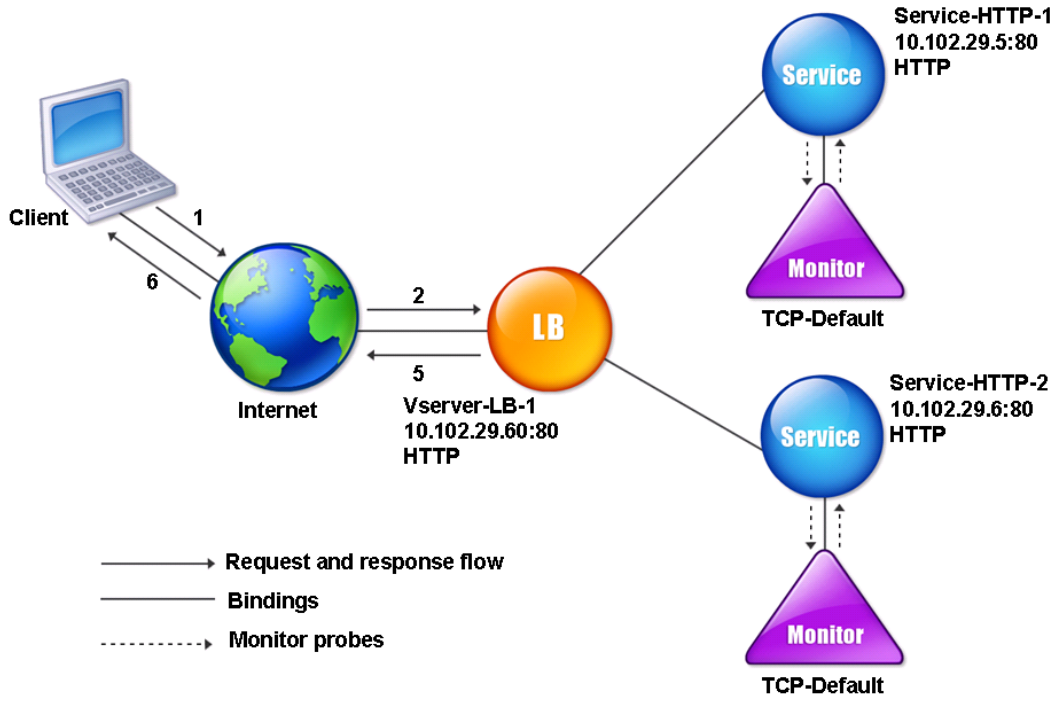
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**.
2. Erstellen Sie einen HTTP-, ICMP- oder TCP-Monitor und wählen Sie **Reverse**aus.

Konfigurieren von Monitoren in einem Lastausgleichs-Setup

August 19, 2021

Um Monitore auf einer Website zu konfigurieren, entscheiden Sie zunächst, ob Sie einen integrierten Monitor verwenden oder einen eigenen Monitor erstellen möchten. Wenn Sie einen Monitor erstellen, können Sie wählen, ob Sie einen Monitor basierend auf einem integrierten Monitor erstellen oder einen benutzerdefinierten Monitor erstellen, der ein Skript verwendet, das Sie zur Überwachung des Dienstes schreiben. Weitere Informationen zum Erstellen benutzerdefinierter Monitore finden Sie unter Benutzerdefinierte Monitore. Sobald Sie einen Monitor ausgewählt oder erstellt haben, binden Sie ihn dann an den entsprechenden Dienst. Die Monitornamen können bis zu 255 Zeichen lang sein. Das folgende Konzeptdiagramm veranschaulicht eine grundlegende Lastausgleichseinrichtung mit Monitoren.

Abbildung 1. Funktionsweise von Monitoren



Wie gezeigt, hat jeder Dienst einen Monitor an ihn gebunden. Der Monitor untersucht den Lastausgleichsserver über seinen Service. Solange der Lastausgleichsserver auf die Sonden reagiert, markiert der Monitor ihn auf UP. Wenn der Lastausgleichsserver innerhalb des festgelegten Zeitraums nicht auf die angegebene Anzahl von Sonden reagiert, markiert der Monitor ihn nach UNTEN.

Dieser Abschnitt enthält die folgenden Details:

- Monitore erstellen
- Konfigurieren von Überwachungsparametern zum Ermitteln des Dienstintegritätszustands
- Binden von Monitoren an Dienste
- Monitore ändern
- Aktivieren und Deaktivieren von Monitoren
- Aufheben der Bindung von Monitoren
- Entfernen von Monitoren
- Anzeigen von Monitoren
- Schließen von Monitorverbindungen
- Ignorieren der Obergrenze für Clientverbindungen für Monitorprobes

Monitore erstellen

May 11, 2023

Die NetScaler-Appliance bietet eine Reihe integrierter Monitore. Es ermöglicht Ihnen auch, benutzerdefinierte Monitore zu erstellen, entweder basierend auf den integrierten Monitoren oder von Grund auf neu.

So erstellen Sie einen Monitor mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> <monitorType> [<interval>]

add lb mon monitor-HTTP-1 HTTP

add lb mon monitor-HTTP-2 TCP 2
<!--NeedCopy-->
```

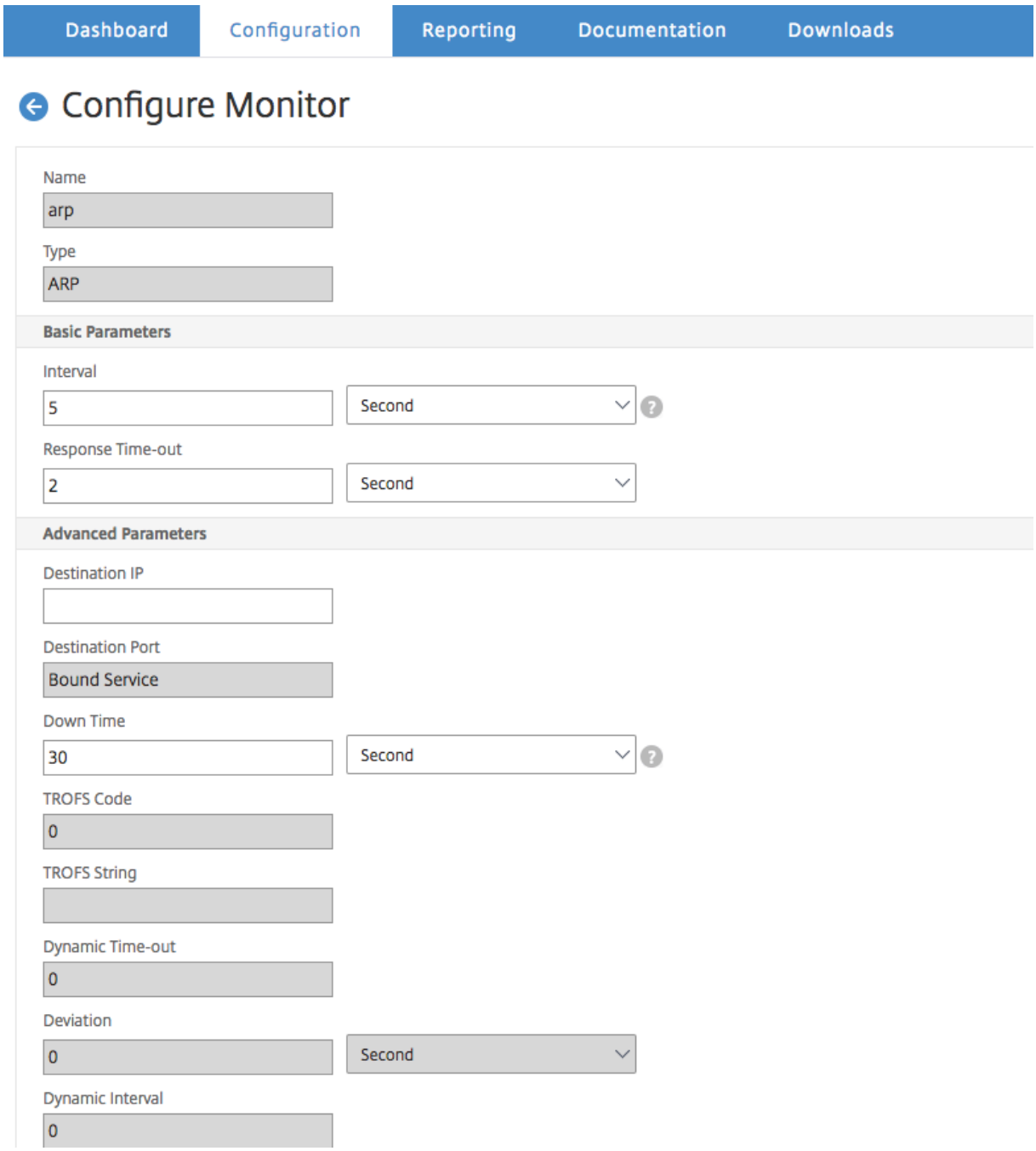
So erstellen Sie einen Monitor mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**.
2. Klicken Sie auf **Hinzufügen** und erstellen Sie einen Monitortyp, der Ihren Anforderungen entspricht.

Der Bildschirm „Monitor erstellen“ enthält zwei Abschnitte: **Grundparameter** und **Erweiterte Parameter**.

Je nach Monitortyp enthält der Abschnitt **Grundparameter** die Parameter, die für jeden Monitor eingestellt werden müssen. Der Abschnitt **Erweiterte Parameter** enthält die Parameter, die in fortgeschrittenen Anwendungsfällen verwendet werden können.

Die folgende Abbildung ist ein Beispiel für eine Seite Monitor erstellen des ARP-Monitortyps.



Hinweis

Vor NetScaler Release 12.0 Build 56.20 werden Basisparameter und Advanced Parameters als Standard Parameters bzw. Special Parameters bezeichnet.

Monitorparameter zum Bestimmen des Dienststatus konfigurieren

May 11, 2023

Sie können die folgenden Überwachungsparameter konfigurieren, um einen Dienst basierend auf den Überwachungssonden als DOWN zu markieren.

Wiederholte Versuche

Maximale Anzahl von Sonden, die gesendet werden sollen, um den Status eines Dienstes zu ermitteln, für den eine Überwachungsprüfung ausfällt.

Fehlgeschlagene Einträge

Anzahl der Wiederholungen, die fehlschlagen müssen, außerhalb der für den Parameter Wiederholungen angegebenen Nummer, damit ein Dienst als DOWN markiert wird. Wenn der Parameter Wiederholungen beispielsweise auf 10 festgelegt ist und der Parameter Failure Retries auf 6 gesetzt ist, müssen von den 10 gesendeten Sonden mindestens sechs Sonden fehlschlagen, wenn der Dienst als DOWN gekennzeichnet werden soll.

alertRetries

Anzahl aufeinanderfolgender Prüfpunktfehler, nach denen die Appliance einen SNMP-Trap namens MonProbeFailed generiert.

AlertRetries auf einen Wert setzen, der höher ist als der Wert “Wiederholungen”

Der Parameter AlertRetries, der die maximale Anzahl aufeinanderfolgender Monitoringprobenfehler angibt, nach denen die NetScaler Appliance ein SNMP-Trap namens MonProbeFailed generiert, kann nun auf einen Wert festgelegt werden, der höher ist als der Wert Retries (der die maximale Anzahl von Prüfpunkten angibt, die gesendet werden sollen, um die Status eines Dienstes, für den ein Monitoring-Test fehlgeschlagen ist). Wenn der Wert von AlertRetries höher als der Wert für Wiederholungen ist, wird der SNMP-Trap erst gesendet, nachdem der Dienst DOWN ist.

Wenn Sie beispielsweise Wiederholungen auf 3, AlertRetries auf 12 und das Zeitintervall auf 5 Sekunden setzen, wird der Dienst nach 15 Sekunden (3*5) als DOWN markiert, aber es wird keine Warnung generiert. Wenn die Monitorproben nach 60 Sekunden (12*5) immer noch ausfallen, generiert die NetScaler-Appliance einen MonProbeFailed-Trap. Wenn eine Prüfung zu einem Zeitpunkt zwischen 15 und 60 Sekunden erfolgreich ist, wird der Dienst als UP markiert und es wird keine Warnung generiert.

Wenn Sie den Wert AlertRetries auf einen höheren Wert als den Wert für Wiederholungen festlegen, können nur echte Warnmeldungen generiert und Fehlalarme bei geplanten Neustarts vermieden werden.

So setzen Sie den AlertRetries-Parameterwert mithilfe der Befehlszeilenschnittstelle auf einen höheren Wert als den Wert für Wiederholungen

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lb monitor <monitorName> [-retries <integer>] [-alertRetries <
     integer>]
2 <!--NeedCopy-->
```

Beispiel:

add lb monitor monitor-HTTP-1 HTTP -retries 3 -alertRetries 12

AlertRetries-Parameterwert mithilfe der GUI auf einen höheren Wert als den Wert für Wiederholungen festlegen

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Monitore**.
2. Klicken Sie auf **Hinzufügen**, um einen neuen Monitor hinzuzufügen, oder wählen Sie einen vorhandenen Monitor aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie in das Feld **Wiederholungen** den Wert für den Parameter Wiederholungen ein.
4. Geben Sie in das Feld **SNMP-Warnmeldungswiederholungen** den Wert für den `alertRetries` Parameter ein.

Monitore an Dienste binden

May 11, 2023

Nachdem Sie einen Monitor erstellt haben, binden Sie ihn an einen Dienst. Sie können einen oder mehrere Monitore an einen Dienst binden. Wenn Sie einen Monitor an einen Dienst binden, bestimmt dieser Monitor, ob der Dienst als UP oder DOWN markiert ist.

Wenn Sie mehrere Monitore an einen Dienst binden, überprüft die NetScaler-Appliance den Status aller Monitore und entscheidet dann über den Status des Dienstes. Sie können verschiedene Gewichte für einen Monitor konfigurieren. Das Gewicht eines Monitors gibt an, wie viel dieser Monitor dazu beiträgt, den Dienst als UP oder DOWN zu kennzeichnen. Ein Monitor mit einem höheren Gewicht kennzeichnet den Dienst häufiger als OBEN oder UNTEN. Das Standardgewicht ist 1. Selbst wenn einer

der Monitore ausfällt, wird der Dienst daher als DOWN markiert. Weitere Informationen finden Sie unter Festlegen eines Schwellenwerts für die an einen Dienst gebundenen Monitore.

Hinweis: Die Ziel-IP-Adresse eines Monitor-Prüfpunkts kann von der IP-Adresse und dem Port des Servers abweichen.

So binden Sie einen Monitor über die Befehlszeilenschnittstelle an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:

```
bind service <name> (-monitorName <string>)
<!--NeedCopy-->
```

Beispiel:

```
bind service s1 -monitorName tcp
<!--NeedCopy-->
```

So binden Sie einen Monitor über die GUI an einen Dienst

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie den Dienst, und fügen Sie einen Monitor hinzu.

Monitore ändern

August 19, 2021

Sie können die Einstellungen für jeden von Ihnen erstellten Monitor ändern.

Hinweis: Für Monitore gelten zwei Parametersätze: diejenigen, die unabhängig vom Typ für alle Monitore gelten, und diejenigen, die spezifisch für einen Monitortyp sind. Informationen zu Parametern für einen bestimmten Monitortyp finden Sie in der Beschreibung für diesen Monitortyp.

So ändern Sie einen vorhandenen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb monitor <monitorName> <type> -interval <interval> -resptimeout <
    resptimeout>
<!--NeedCopy-->
```

Beispiel:


```
set mon monitor-HTTP-1 HTTP -interval 50 milli
-resptimeout 20 milli
<!--NeedCopy-->
```

So ändern Sie einen vorhandenen Monitor über die grafische Benutzeroberfläche

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und öffnen Sie einen zu ändernden Monitor.

Aktivieren und Deaktivieren von Monitoren

August 19, 2021

Standardmäßig sind Monitore, die an Dienste und Dienstgruppen gebunden sind, aktiviert. Wenn Sie einen Monitor aktivieren, beginnt der Monitor mit der Untersuchung der Dienste, an die er gebunden ist. Wenn Sie einen an einen Dienst gebundenen Monitor deaktivieren, wird der Status, den der Dienst mithilfe der anderen an den Dienst gebundenen Monitore bestimmt. Wenn der Dienst nur an einen Monitor gebunden ist und Sie den Monitor deaktivieren, wird der Status des Dienstes mithilfe des Standardmonitors ermittelt.

So aktivieren Sie einen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
enable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

So aktivieren Sie einen Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Wählen Sie einen Monitor aus, und wählen Sie in der Liste Aktion die Option Aktivieren oder Deaktivieren aus.

So deaktivieren Sie einen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
disable lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
disable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Monitore aufheben

August 19, 2021

Sie können die Bindung von Monitoren aus einer Service- und Servicegruppe aufheben. Wenn Sie die Bindung eines Monitors von der Servicegruppe aufheben, werden die Monitore von den einzelnen Diensten, die die Servicegruppe bilden, nicht gebunden. Wenn Sie die Bindung eines Monitors an einen Dienst oder eine Servicegruppe aufheben, untersucht der Monitor weder den Dienst noch die Servicegruppe.

Hinweis: Wenn Sie die Bindung aller vom Benutzer konfigurierten Monitore an einen Dienst oder eine Servicegruppe aufheben, ist der Standardmonitor an den Dienst und die Servicegruppe gebunden. Die Standardüberwachung prüft dann den Dienst oder die Servicegruppen.

So trennen Sie die Bindung eines Monitors von einem Dienst über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
unbind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```


So trennen Sie die Bindung eines Monitors von einem Dienst über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienste**, und öffnen Sie einen zu ändernden Dienst.
2. Klicken Sie in den Abschnitt Monitore, wählen Sie einen Monitor aus und klicken Sie auf **Binden aufheben**.

Monitore entfernen

May 11, 2023

Nachdem Sie einen Monitor, den Sie erstellt haben, von seinem Dienst getrennt haben, können Sie diesen Monitor aus der NetScaler-Konfiguration entfernen. (Wenn ein Monitor an einen Dienst gebunden ist, kann er nicht entfernt werden.)

Hinweis: Wenn Sie Monitore entfernen, die an einen Dienst gebunden sind, ist der Standardmonitor an den Dienst gebunden. Standardmonitore können nicht entfernt werden.

So entfernen Sie einen Monitor mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
rm lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Beispiel:

```
rm lb monitor monitor-HTTP-1 HTTP
<!--NeedCopy-->
```

So entfernen Sie einen Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Wählen Sie einen Monitor aus und klicken Sie auf **Löschen**.

Monitore ansehen

May 11, 2023

Sie können die Dienste und Dienstgruppen anzeigen, die an einen Monitor gebunden sind. Sie können die Einstellungen eines Monitors überprüfen, um Probleme mit Ihrer NetScaler-Konfiguration zu beheben. Im folgenden Verfahren werden die Schritte zum Anzeigen der Bindungen eines Monitors an die Dienste und Dienstgruppen beschrieben.

So zeigen Sie Monitorbindungen mit der CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
show lb monbindings <MonitorName>
<!--NeedCopy-->
```

Beispiel:

```
show lb monbindings monitor-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie Monitorbindungen mit der GUI an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Wählen Sie einen Monitor aus, und klicken Sie in der Liste Aktion auf **Bindungen anzeigen**.

So zeigen Sie Monitore mit der CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
show lb mon monitor-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie Monitore mit der GUI an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**. Die Details der verfügbaren Monitore werden im Bereich Monitore angezeigt.

Monitorverbindungen schließen

May 11, 2023

Die NetScaler-Appliance sendet über die an die Dienste gebundenen Monitore Sonden an die Dienste. Standardmäßig folgen der Monitor auf der Appliance und dem physischen Server auch bei Monitorsonden dem vollständigen Handshake-Vorgang. Dieses Verfahren erhöht jedoch den Aufwand für den Überwachungsprozess und ist möglicherweise nicht immer erforderlich.

Für den TCP-Typ-Monitor können Sie die Appliance so konfigurieren, dass eine Monitor-Probe-Verbindung geschlossen wird, nachdem SYN-ACK vom Dienst empfangen wurde. Setzen Sie dazu den Wert des Parameters MonitorConnectionClose auf RESET. Wenn Sie möchten, dass die Verbindung zwischen Monitor und Sonde den gesamten Vorgang durchläuft, setzen Sie den Wert auf FIN.

Hinweis: Die Einstellung MonitorConnectionClose gilt nur für TCP-Monitore und TCP-Standardmonitore.

Gehen Sie wie folgt vor, um das Schließen der Monitorverbindung mithilfe der Befehlszeilenschnittstelle zu konfigurieren:

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb parameter -monitorConnectionClose <monitor_conn_close_option>
<!--NeedCopy-->
```

Beispiel

```
set lb parameter -monitorConnectionClose RESET
<!--NeedCopy-->
```

So konfigurieren Sie das Schließen der Monitorverbindung mithilfe des Konfigurationsprogramms:

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren**.
2. Wählen Sie **FIN** oder **Reset**.

Schließen von Monitorverbindungen auf Dienst- oder Dienstgruppenebene

Sie können die Appliance auch so konfigurieren, dass eine Monitor-Probe-Verbindung auf Dienst- und Dienstgruppenebene geschlossen wird, indem Sie den Parameter monConnectionClose festlegen. Wenn dieser Parameter nicht gesetzt ist, wird die Monitorverbindung geschlossen, indem der in den globalen Load-Balancing-Parametern festgelegte Wert verwendet wird. Wenn dieser Parameter auf Dienst- oder Dienstgruppenebene festgelegt ist, wird die Monitorverbindung geschlossen, indem eine Verbindungsabbruchmeldung mit dem gesetzten FIN- oder RESET-Bit an den Dienst oder die Dienstgruppe gesendet wird.

So konfigurieren Sie das Schließen der Monitorverbindung auf Serviceebene mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```

So konfigurieren Sie das Schließen der Monitorverbindung auf Dienstgruppenebene mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
 set serviceGroup <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```

So konfigurieren Sie das Schließen der Monitorverbindung auf Serviceebene mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
2. Fügen Sie einen Dienst hinzu oder bearbeiten Sie ihn und stellen Sie in den **Grundeinstellungen**das **Monitoring Connection Close Bit ein**.

So konfigurieren Sie das Schließen von Monitorverbindungen auf Dienstgruppenebene mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Fügen Sie eine Dienstgruppe hinzu oder bearbeiten Sie sie und stellen Sie in den **Grundeinstellungen**das **Monitoring Connection Close Bit ein**.

> **Hinweis:** Um eine Monitor-Probe-Verbindung mithilfe globaler Load-Balancing-Parameter zu schließen, können Sie MonitorConnectionClose auf FIN oder RESET konfigurieren. Wenn Sie den Parameter MonitorConnectionClose auf konfigurieren;
>
> - FIN: Die Appliance führt einen vollständigen TCP-Handshake durch.
> - RESET: Die Appliance schließt die Verbindung, nachdem sie den SYN-ACK vom Dienst erhalten hat.
>
> In der leichteren Version von NetScaler CPX ist der Parameterwert MonitorConnectionClose standardmäßig auf RESET festgelegt und kann auf globaler Ebene nicht in FIN geändert werden. Sie können den Parameter MonitorConnectionClose jedoch auf Serviceebene in FIN ändern.

Obergrenze für Clientverbindungen für Monitorsonden ignorieren

May 11, 2023

Abhängig von Faktoren wie der Kapazität eines physischen Servers können Sie ein Limit für die maximale Anzahl von Client-Verbindungen angeben, die zu einem Dienst hergestellt werden. Wenn Sie ein solches Limit für einen Dienst festgelegt haben, beendet die NetScaler-Appliance das Senden von Anfragen an den Dienst, wenn der Schwellenwert erreicht ist, und setzt das Senden von Verbindungen an den Dienst fort, nachdem die Anzahl der vorhandenen Verbindungen die Grenzwerte erreicht hat. Sie können die Appliance so konfigurieren, dass diese Prüfung übersprungen wird, wenn sie Monitor-Probe-Verbindungen an einen Dienst sendet.

Hinweis: Sie können die Überprüfung der maximalen Anzahl von Client-Verbindungen für einen einzelnen Dienst nicht überspringen. Wenn Sie diese Option angeben, gilt sie für alle Monitore, die an alle auf der NetScaler Appliance konfigurierten Dienste gebunden sind.

So legen Sie die Option “MaxClients für Monitorverbindungen überspringen” über die Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb parameter -monitorSkipMaxClient (ENABLED|DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -monitorSkipMaxClient enabled
<!--NeedCopy-->
```

So legen Sie die Option “MaxClients für Monitorverbindungen überspringen” mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren**.
2. Wählen Sie **MaxClients für die Überwachung von Verbindungen überspringen**aus.

Große Bereitstellungen verwalten

May 11, 2023

Die NetScaler-Appliance enthält mehrere Funktionen, die bei der Konfiguration einer großen Load-Balancing-Bereitstellung hilfreich sind. Anstatt virtuelle Server und Dienste einzeln zu konfigurieren, können Sie Gruppen von virtuellen Servern und Diensten erstellen. Sie können auch eine Reihe von virtuellen Servern und Diensten erstellen und virtuelle Server- und Dienst-IP-Adressen übersetzen oder maskieren.

Sie können die Persistenz für eine Gruppe von virtuellen Servern festlegen. Sie können Monitore an eine Gruppe von Diensten binden. Durch das Erstellen einer Reihe virtueller Server und Dienste identischen Typs können Sie diese Server in einem einzigen Verfahren einrichten und konfigurieren. Dies verkürzt die für die Konfiguration dieser virtuellen Server und Dienste erforderliche Zeit erheblich.

Durch das Übersetzen oder Maskieren von IP-Adressen können Sie virtuelle Server und Dienste ausschalten. Sie können dann Änderungen an Ihrer Infrastruktur vornehmen, ohne Ihre Service- und virtuellen Serverdefinitionen umfassend neu zu konfigurieren.

Bereiche virtueller Server und Services

August 19, 2021

Wenn Sie den Lastenausgleich konfigurieren, können Sie Bereiche von virtuellen Servern und Diensten erstellen, sodass virtuelle Server und Dienste nicht einzeln konfiguriert werden müssen. Sie können beispielsweise eine einzige Prozedur verwenden, um drei virtuelle Server mit drei entsprechenden IP-Adressen zu erstellen. Wenn mehr als ein Argument einen Bereich verwendet, müssen die Bereiche dieselbe Größe haben.

Im Folgenden sind die Typen von Bereichen aufgeführt, die Sie beim Hinzufügen von Diensten und virtuellen Servern zur Konfiguration angeben können:

- **Numerische Bereiche.** Anstatt eine einzelne Zahl einzugeben, können Sie einen Bereich von fortlaufenden Zahlen angeben.

  Beispielsweise können Sie einen Bereich virtueller Server erstellen, indem Sie eine Start-IP-Adresse angeben, z. B. 10.102.29.30, und dann einen Wert für das letzte Byte eingeben, das den Bereich angibt, z. B. 34. In diesem Beispiel werden fünf virtuelle Server mit IP-Adressen erstellt, die zwischen 10.102.29.30 und 10.102.29.34 liegen.

  Hinweis: Die IP-Adressen der virtuellen Server und Dienste müssen fortlaufend sein.

- **Alphabetische Bereiche.** Anstatt einen wörtlichen Buchstaben einzugeben, können Sie einen Bereich für einen einzelnen Buchstaben ersetzen [,]z. B. Dies führt dazu, dass alle Buchstaben des Bereichs einbezogen werden, in diesem Fall C, D, E, F und G.

  Wenn Sie beispielsweise drei virtuelle Server mit dem Namen haben `Vserver-xVserver-y Vserver-z`, und anstatt sie separat `vserver [x-z]` zu konfigurieren, können Sie sie alle kon-

figurieren.

Erstellen einer Reihe von virtuellen Servern

So erstellen Sie einen Bereich virtueller Server mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<port>]

add lb vserver <name>@[<rangeValue>]> <protocol> <IPAddress[<rangeValue>]> [<port>]
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

ODER

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80

vserver "vserverP" added

vserver "vserverQ" added

vserver "vserverR" added

Done
<!--NeedCopy-->
```

So erstellen Sie einen Bereich virtueller Server mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<port>]

add lb vserver <name>@\*\*[\*\*<rangeValue>\*\*]\*\*> <protocol> <IPAddress[<rangeValue>]> [<port>]
<!--NeedCopy-->
```


Beispiel:

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

ODER

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80
vserver "vserverP" added
vserver "vserverQ" added
vserver "vserverR" added
Done
<!--NeedCopy-->
```

So erstellen Sie eine Reihe virtueller Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Fügen Sie einen virtuellen Server hinzu, und geben Sie einen Bereich an.

Erstellen einer Reihe von Dienstleistungen

Wenn Sie einen Bereich für den Dienstnamen angeben, geben Sie auch einen Bereich für die IP-Adresse an.

So erstellen Sie ein Leistungsspektrum mit der CLI

Geben Sie an der Eingabeaufforderung den Befehl ein:

```
add service <name>@ <IP>@ <protocol> <port>
<!--NeedCopy-->
```

Beispiel:

```
> add service serv[1-3] 10.102.29.[102-104] http 80
service "serv1" added
service "serv2" added
service "serv3" added
 Done
<!--NeedCopy-->
```


Dienstgruppen konfigurieren

May 11, 2023

Durch die Konfiguration einer Servicegruppe können Sie eine Gruppe von Diensten so einfach wie ein einzelner Dienst verwalten. Wenn Sie beispielsweise eine Option wie Komprimierung, Integritätsüberwachung oder ordnungsmiges Herunterfahren für eine Servicegruppe aktivieren oder deaktivieren, wird die Option für alle Mitglieder der Dienstgruppe aktiviert.

Nachdem Sie eine Dienstgruppe erstellt haben, können Sie sie an einen virtuellen Server binden und der Gruppe Dienste hinzufügen. Sie können Monitore auch an Servicegruppen binden.

> **Hinweis:**
>
> Sie können einen Dienst und eine Dienstgruppe mit derselben IP-Adresse und demselben Port nicht an denselben virtuellen Server binden.

Die Mitglieder einer Dienstgruppe werden durch IP-Adresse oder Servernamen identifiziert.

Die Verwendung von DBS-Gruppenmitgliedern (Domain Name Based Service) ist von Vorteil, da Sie das Mitglied auf der NetScaler Appliance nicht neu konfigurieren müssen, wenn sich die IP-Adresse des Mitglieds ändert. Die Appliance erkennt solche Änderungen automatisch über den konfigurierten Nameserver. Diese Funktion ist in Cloud-Szenarien nützlich, in denen der Dienstanbieter einen physischen Server ändern oder die IP-Adresse für einen Dienst ändern kann. Wenn Sie ein DBS-Gruppenmitglied angeben, lernt die Appliance die IP-Adresse dynamisch.

Sie können sowohl IP-basierte als auch DBS-Mitglieder an dieselbe Dienstgruppe binden.

Hinweis: Wenn Sie DBS-Dienstgruppenmitglieder verwenden, stellen Sie sicher, dass entweder ein Nameserver angegeben ist oder ein DNS-Server auf der NetScaler Appliance konfiguriert ist. Ein Domänenname wird nur in eine IP-Adresse aufgelöst, wenn der entsprechende Adressdatensatz auf der Appliance oder dem Nameserver vorhanden ist.

Erstellen von Servicegruppen

Sie können bis zu 8192 Dienstgruppen auf der NetScaler Appliance konfigurieren.

So erstellen Sie eine Dienstgruppe über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add servicegroup <ServiceGroupName> <Protocol>
<!--NeedCopy-->
```

Beispiel:


```
add servicegroup Service-Group-1 HTTP
<!--NeedCopy-->
```

So erstellen Sie eine Dienstgruppe mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**, und fügen Sie eine Dienstgruppe hinzu.

Binden einer Dienstgruppe an einen virtuellen Server

Wenn Sie eine Dienstgruppe an einen virtuellen Server binden, werden die Mitgliedsdienste an den virtuellen Server gebunden.

So binden Sie eine Dienstgruppe über die Befehlszeilenschnittstelle an einen virtuellen Server

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name>@ <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

So binden Sie eine Dienstgruppe über die GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Dienstgruppen**aus.

Binden Sie ein Mitglied an eine Dienstgruppe

Durch das Hinzufügen von Diensten zu einer Dienstgruppe kann die Dienstgruppe die Server verwalten. Sie können die Server zu einer Dienstgruppe hinzufügen, indem Sie die IP-Adressen oder die Namen der Server angeben.

Wenn Sie in der GUI ein domänennamenbasiertes Dienstgruppenmitglied hinzufügen möchten, wählen Sie **Serverbasiert**aus.

Mit dieser Option können Sie jeden Server hinzufügen, dem ein Name zugewiesen wurde, unabhängig davon, ob es sich bei dem Namen um eine IP-Adresse oder einen vom Benutzer zugewiesenen Namen handelt.

So fügen Sie Mitglieder über die Befehlszeilenschnittstelle zu einer Dienstgruppe hinzu

Um eine Dienstgruppe zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind servicegroup <serviceGroupName> (<IP>@ | <serverName>) <port>
<!--NeedCopy-->
```

Beispiele:

```
bind servicegroup Service-Group-1 10.102.29.30 80

bind servicegroup Service-Group-2 1000:0000:0000:0000:0005:0600:700a
    :888b 80

bind servicegroup CitrixEdu s1.citrite.net
<!--NeedCopy-->
```

So fügen Sie einer Dienstgruppe mit dem Konfigurationsdienstprogramm Mitglieder hinzu

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienstgruppen**, und öffnen Sie eine Dienstgruppe.
2. Klicken Sie in den Abschnitt Dienstgruppe, und führen Sie eine der folgenden Aktionen aus:
   - Um ein IP-basiertes Dienstgruppenmitglied hinzuzufügen, wählen Sie IP-basiert aus.
   - Um ein servernamenbasiertes Dienstgruppenmitglied hinzuzufügen, wählen Sie Server-basiert aus.

   Wenn Sie ein domänennamenbasiertes Dienstgruppenmitglied hinzufügen möchten, wählen Sie **Serverbasiert**aus. Mit dieser Option können Sie jeden Server hinzufügen, dem ein Name zugewiesen wurde, unabhängig davon, ob es sich bei dem Namen um eine IP-Adresse oder einen vom Benutzer zugewiesenen Namen handelt.
3. Wenn Sie ein neues IP-basiertes Mitglied hinzufügen, geben Sie im Textfeld IP-Adresse die IP-Adresse ein. Wenn die IP-Adresse das IPv6-Format verwendet, aktivieren Sie das Kontroll-kästchen IPv6, und geben Sie die Adresse in das Textfeld IP-Adresse ein.

   Hinweis: Sie können einen Bereich von IP-Adressen hinzufügen. Die IP-Adressen im Bereich müssen aufeinander folgen. Geben Sie den Bereich an, indem Sie die Start-IP-Adresse in das Textfeld IP-Adresse eingeben (z. B. 10.102.29.30). Geben Sie das Endbyte des IP-Adressbereichs

im Textfeld unter Bereich an (z. B. 35). Geben Sie im Textfeld Port den Port ein (z. B. 80), und klicken Sie dann auf Hinzufügen.

4. Klicken Sie auf Erstellen.

Binden eines Monitors an eine Dienstgruppe

Wenn Sie eine Dienstgruppe erstellen, wird der Standardmonitor des für die Gruppe geeigneten Typs automatisch an diese gebunden. Monitore überprüfen regelmäßig die Server in der Dienstgruppe, an die sie gebunden sind, und aktualisieren den Status der Dienstgruppen.

Sie können einen anderen Monitor Ihrer Wahl an die Servicegruppe binden.

So binden Sie einen Monitor mit der Befehlszeilenschnittstelle an eine Dienstgruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
bind serviceGroup <serviceGroupName> -monitorName <string> -monState (
    ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
bind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

So binden Sie den Monitor mit dem Konfigurationsdienstprogramm an eine Dienstgruppe

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Öffnen Sie eine Dienstgruppe, und klicken Sie in Erweiterte Einstellungen auf **Monitore**.

Behalten Sie den ursprünglichen Status eines Dienstgruppenmitglieds nach dem Deaktivieren und Aktivieren eines virtuellen Servers bei

Ab Build 64.x können Sie mit einer neuen globalen Option —retainDisableServer den Status eines Dienstgruppenmitglieds beibehalten, wenn ein Server deaktiviert und wieder aktiviert wird.

Zuvor wurde der Status eines Mitglieds unter den folgenden Bedingungen von DISABLED zu ENABLED geändert:

- Zwei Anwendungen werden auf demselben Port auf einem virtuellen Server bereitgestellt.
- Zwei Dienstgruppen mit einem gemeinsamen Mitglied sind an diesen virtuellen Server gebunden, und das gemeinsame Mitglied ist in einer Gruppe aktiviert und in der anderen deaktiviert.

- Der Server ist deaktiviert und dann wieder aktiviert.

Unter diesen Bedingungen werden durch das Deaktivieren des Servers alle Mitglieder der Dienstgruppe deaktiviert, und das erneute Aktivieren des Servers werden standardmäßig alle Mitglieder unabhängig von ihrem früheren Status aktiviert. Um die Mitglieder wieder in den ursprünglichen Status zurück zu setzen, müssen Sie diese Mitglieder in der Servicegruppe manuell deaktivieren. Dies ist eine umständliche Aufgabe und anfällig für Fehler.

Dienstgruppen verwalten

May 11, 2023

Sie können die Einstellungen der Dienste in einer Dienstgruppe ändern und Aufgaben wie das Aktivieren, Deaktivieren und Entfernen von Dienstgruppen ausführen. Sie können auch die Bindung von Mitgliedern aus einer Dienstgruppe aufheben. Weitere Informationen zu Dienstgruppen finden Sie unter Konfigurieren von Dienstgruppen.

Ändern einer Servicegruppe

Sie können die Attribute von Dienstgruppenmitgliedern ändern. Sie können mehrere Attribute der Dienstgruppe festlegen, z. B. den maximalen Client und die Komprimierung. Die Attribute werden auf den einzelnen Servern in der Servicegruppe festgelegt. Sie können keine Parameter für die Dienstgruppe wie Transportinformationen (IP-Adresse und Port), Gewicht und Server-ID festlegen.

Hinweis: Ein Parameter, den Sie für eine Dienstgruppe festlegen, wird auf die Mitgliedsserver in der Gruppe angewendet, nicht auf einzelne Dienste.

So ändern Sie eine Dienstgruppe über die Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl mit einem oder mehreren der optionalen Parameter ein:

```
set servicegroup <serviceGroupName> [-type <type>] [-maxClient <
    maxClient>] [-maxReq <maxReq>] [-cacheable (YES|NO)] [-cip (ENABLED|
    DISABLED)] [-cipHeader <cipHeader>] [-usip (YES|NO)] [-sc (ON|OFF)]
    [-sp (ON|OFF)] [-cltTimeout <cltTimeout>] [-svrTimeout <svrTimeout>]
     [-cka (YES|NO)] [-TCPB (YES|NO)] [-CMP (\*\*YES\*\*|\*\*NO\*\*)] [-
    maxBandwidth <maxBandwidth>] [-maxThreshold <maxThreshold>] [-state
    (ENABLED|DISABLED)] [-downStateFlush (ENABLED|DISABLED)
<!--NeedCopy-->
```

Beispiel:


```
set servicegroup Service-Group-1 -type TRANSPARENT

set servicegroup Service-Group-1 -maxClient 4096

set servicegroup Service-Group-1 -maxReq 16384

set servicegroup Service-Group-1 -cacheable YES
<!--NeedCopy-->
```

So ändern Sie eine Dienstgruppe mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**, und öffnen Sie die zu ändernde Dienstgruppe.

Entfernen einer Dienstgruppe

Wenn Sie eine Dienstgruppe entfernen, behalten die an die Gruppe gebundenen Server ihre individuellen Einstellungen bei und sind weiterhin auf der NetScaler-Appliance vorhanden.

So entfernen Sie eine Dienstgruppe über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
rm servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
rm servicegroup Service-Group-1
<!--NeedCopy-->
```

So entfernen Sie eine Dienstgruppe mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie eine Dienstgruppe aus und klicken Sie auf **Löschen**.

Entbindung eines Mitglieds von einer Servicegruppe

Wenn Sie ein Mitglied von der Dienstgruppe trennen, gelten die für die Dienstgruppe festgelegten Attribute nicht mehr für das Mitglied, das Sie nicht gebunden haben. Die Mitgliederdienste behalten

jedoch ihre individuellen Einstellungen bei und sind weiterhin auf der NetScaler-Appliance vorhanden.

So lösen Sie Mitglieder über die Befehlszeile von einer Dienstgruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind servicegroup <serviceGroupName> <IP>@ [<port>]
<!--NeedCopy-->
```

Beispiel:

```
unbind servicegroup Service-Group-1 10.102.29.30 80
<!--NeedCopy-->
```

So lösen Sie Mitglieder mithilfe des Konfigurationsdienstprogramms von einer Dienstgruppe

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Öffnen Sie eine Dienstgruppe und klicken Sie in den Abschnitt Mitglieder der Dienstgruppe.
3. Wählen Sie ein Dienstgruppenmitglied aus und klicken Sie auf “ **Binden aufheben**”.

Entbindung einer Dienstgruppe von einem virtuellen Server

Wenn Sie eine Dienstgruppe von einem virtuellen Server trennen, werden die Mitgliederdienste vom virtuellen Server nicht gebunden und bestehen weiterhin auf der NetScaler-Appliance.

So lösen Sie die Bindung einer Dienstgruppe über die Befehlszeile von einem virtuellen Server

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind lb vserver <name>@ <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
unbind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

So lösen Sie die Bindung einer Dienstgruppe mithilfe des Konfigurationsdienstprogramms von einem virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.

2. Öffnen Sie den virtuellen Server und klicken Sie in den Abschnitt Dienstgruppe.
3. Wählen Sie die Dienstgruppe aus und klicken Sie auf “ **Binden aufheben**”.

Binden Sie Monitore von Servicegruppen

Wenn Sie einen Monitor von einer Dienstgruppe trennen, überwacht der Monitor, den Sie ungebunden haben, die einzelnen Dienste, aus denen die Gruppe besteht, nicht mehr.

So lösen Sie einen Monitor über die Befehlszeile von einer Dienstgruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind serviceGroup <serviceGroupName> -monitorName <string>
<!--NeedCopy-->
```

Beispiel:

```
unbind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

So lösen Sie einen Monitor mithilfe des Konfigurationsdienstprogramms von einer Dienstgruppe

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Öffnen Sie eine Servicegruppe und klicken Sie in den Abschnitt Monitore.
3. Wählen Sie einen Monitor aus und klicken Sie auf “ **Binden aufheben**”.

Aktivieren oder Deaktivieren einer Dienstgruppe

Wenn Sie eine Dienstgruppe und die Server aktivieren, werden die zur Dienstgruppe gehörenden Dienste aktiviert. In ähnlicher Weise werden die Dienstgruppe und der Dienst aktiviert, wenn ein zu einer Dienstgruppe gehörender Dienst aktiviert ist. Standardmäßig sind Dienstgruppen aktiviert.

Nachdem Sie einen aktivierten Dienst deaktiviert haben, können Sie den Dienst mithilfe des Konfigurationsdienstprogramms oder der Befehlszeile anzeigen, um die verbleibende Zeit zu sehen, bis der Dienst heruntergefahren wird.

So deaktivieren Sie eine Dienstgruppe über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:


```
disable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
disable servicegroup Service-Group-1
<!--NeedCopy-->
```

So deaktivieren Sie eine Dienstgruppe mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie eine Dienstgruppe aus und klicken Sie in der Liste Aktion auf **Deaktivieren**.

So aktivieren Sie eine Dienstgruppe über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
enable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
enable servicegroup Service-Group-1
<!--NeedCopy-->
```

So aktivieren Sie eine Dienstgruppe mithilfe des Konfigurationsdienstprogramms

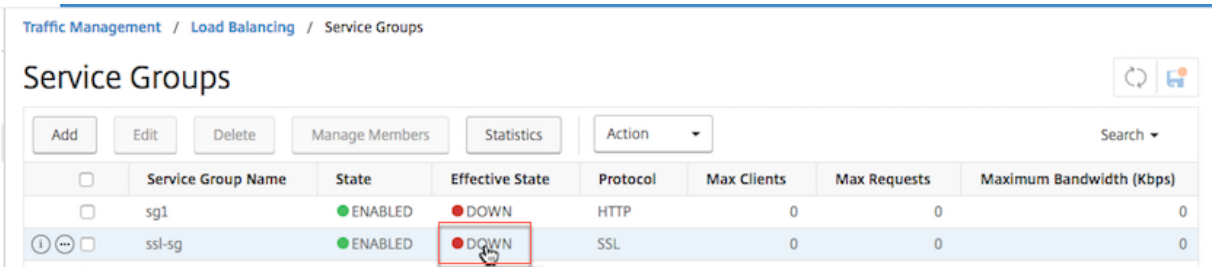
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie eine Dienstgruppe aus und klicken Sie in der Liste Aktion auf **Aktivieren**.

Status der Mitglieder von Servicegruppen anzeigen

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.

Auf der Seite “Dienstgruppen” zeigt die Spalte **Effective State** den Status der Dienstgruppen an. Status UP/DOWN in der Spalte **Effective State** ist anklickbar. Sie können auf den Status klicken und die Liste der Mitglieder zusammen mit ihrem Status in derselben Ansicht abrufen. Wählen Sie ein Mitglied aus und klicken Sie auf die Schaltfläche **Details überwachen**, um den Grund für den Status “DOWN” anzuzeigen.

Hinweis: Vor NetScaler Version 12.0 Build 56.20 war der Status in der Spalte **Effective State** nicht anklickbar.



Anzeigen der Eigenschaften einer Servicegruppe

Sie können die folgenden Einstellungen der konfigurierten Dienstgruppen anzeigen:

- Name
- IP-Adresse
- State
- Protokoll
- Maximale Clientverbindungen
- Maximale Anfragen pro Verbindung
- Maximale Bandbreite
- Schwellenwert überwachen

Das Anzeigen der Details der Konfiguration kann für die Fehlerbehebung bei Ihrer Konfiguration hilfreich sein.

So zeigen Sie die Eigenschaften einer Dienstgruppe über die Befehlszeile an

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die Gruppeneigenschaften oder die Eigenschaften und die Gruppenmitglieder anzuzeigen:

```
show servicegroup <ServiceGroupName>

show servicegroup <ServiceGroupName> -includemembers
<!--NeedCopy-->
```

Beispiel:

```
show servicegroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften einer Dienstgruppe mithilfe des Konfigurationsdienstprogramms an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.

2. Klicken Sie auf den Pfeil neben der Dienstgruppe.

Anzeigen von Servicegruppen-Statistiken

Sie können Service-Gruppen-Statistikdaten anzeigen, z. B. die Rate der Anforderungen, Antworten, Anforderungsbytes und Antwortbytes. Die NetScaler-Appliance verwendet die Statistiken einer Dienstgruppe, um die Belastung der Dienste auszugleichen.

So zeigen Sie die Statistiken einer Dienstgruppe mit der Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:

```
stat servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
stat servicegroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken einer Dienstgruppe mithilfe des Konfigurationsdienstprogramms an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie eine Dienstgruppe aus und klicken Sie auf **Statistiken**.

Load Balancing virtueller Server, die an eine Dienstgruppe gebunden sind

Bei groß angelegten Bereitstellungen kann dieselbe Dienstgruppe an mehrere virtuelle Lastausgleichsserver gebunden werden. In einem solchen Fall können Sie, anstatt jeden virtuellen Server anzuzeigen, um die Dienstgruppe anzuzeigen, an die er gebunden ist, eine Liste aller virtuellen Lastausgleichsserver anzeigen, die an eine Dienstgruppe gebunden sind. Sie können die folgenden Details jedes virtuellen Servers anzeigen:

- Name
- State
- IP-Adresse
- Port

So zeigen Sie die virtuellen Server an eine Dienstgruppe über die Befehlszeile an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die an eine Dienstgruppe gebundenen virtuellen Server anzuzeigen:

```
show servicegroupbindings <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
> show servicegroupbindings SVCGRPDTLS
SVCGRPDTLS - State :ENABLED
1) Test-pers (10.10.10.3:80) - State : DOWN
2) BRVSERV (10.10.1.1:80) - State : DOWN
3) OneMore (10.102.29.136:80) - State : DOWN
4) LBVIP1 (10.102.29.66:80) - State : UP
Done
>
<!--NeedCopy-->
```

So zeigen Sie die virtuellen Server an eine Dienstgruppe mithilfe des Konfigurationsdienstprogramms an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie eine Dienstgruppe aus, und klicken Sie in der Liste Aktion auf **Bindungen anzeigen**.

Gewünschten Satz von Servicegruppenmitgliedern für eine Servicegruppe in einem NITRO-API-Aufruf konfigurieren

May 11, 2023

Es wurde Unterstützung hinzugefügt, um einen gewünschten Satz von Dienstgruppenmitgliedern für eine Dienstgruppe in einem NITRO-API-Aufruf zu konfigurieren. Eine neue API, Desired State API, wurde hinzugefügt, um diese Konfiguration zu unterstützen. Mit der API “Desired State” können Sie:

- Stellen Sie eine Liste der Dienstgruppenmitglieder in einer einzigen PUT-Anforderung auf der Ressource “servicegroup_servicegroupmemberlist_binding” bereit.
- Geben Sie ihr Gewicht und ihren Zustand (optional) in dieser PUT-Anfrage an.
- Synchronisieren Sie die Appliance-Konfiguration effektiv mit Bereitstellungsänderungen um Anwendungsserver.

Die NetScaler-Appliance vergleicht die angeforderte gewünschte Elementgruppe mit der konfigurierten Elementgruppe. Dann bindet es automatisch die neuen Mitglieder und entbindet die Mitglieder, die nicht in der Anfrage anwesend sind.

Hinweis:

- Diese Funktion wird nur für Dienstgruppen des Typs unterstützt `API`.
- Sie können nur IP-Adressbasierte Dienste mithilfe der API für den gewünschten Status binden, domänennamenbasierte Dienste sind nicht zulässig.
- Zuvor kann nur ein Servicegruppenmitglied in einem NITRO -Aufruf gebunden werden.

> **Wichtig**
>
> Die gewünschte State-API für die ServiceGroup-Mitgliedschaft wird in der NetScaler Clusterbereitstellung unterstützt.

Anwendungsfall: Synchronisieren Sie Bereitstellungsänderungen mit der NetScaler Appliance in großen Bereitstellungen wie Kubernetes

Bei großen und hochdynamischen Bereitstellungen (z. B. Kubernetes) besteht die Herausforderung darin, die Appliance-Konfiguration mit der Änderungsrate der Bereitstellungen auf dem neuesten Stand zu halten, um den Anwendungsverkehr genau zu bedienen. In solchen Bereitstellungen sind Controller (Ingress oder E-W Controller) für die Aktualisierung der ADC-Konfiguration verantwortlich. Wann immer Änderungen an der Bereitstellung vorgenommen werden, `kube-api server` sendet den effektiven Satz von Endpunkten über “Endpunkte-Ereignis” an den Controller. Der Controller verwendet den Read-Delta-Modify-Ansatz, bei dem er Folgendes durchführt:

- Ruft die aktuell konfigurierte Endpunktsatz (Dienstgruppenmitgliedergruppe einer Dienstgruppe) für den Dienst von der ADC-Appliance ab.
- Vergleicht die konfigurierte Endpunktsatz mit der Menge im empfangenen Ereignis.
- Bindet die neuen Endpunkte (Mitglieder der Dienstgruppe) oder löst die gelöschten Endpunkte.

Da die Änderungsrate und die Größe der Dienste in dieser Umgebung hoch ist, ist diese Konfigurationsmethode nicht effizient und kann Konfigurationsupdates verzögern.

Die gewünschte Status-API löst das Problem, indem sie die beabsichtigte Mitgliedergruppe für eine Servicegruppe in einer einzigen API akzeptiert und die Konfiguration effektiv aktualisiert.

Erstellen einer Service-Gruppe vom Typ-API mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>]
```


Beispiel:

```
add serviceGroup svg1 HTTP -autoScale API
```

Sie können die Parameterautodisablegraceful, autoDisabledelay und autoScale und konfigurieren, indem Sie den Befehl serviceGroup hinzufügen oder den Befehl serviceGroup festlegen.

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>] [-autoDisablegraceful ( YES | NO)] [-autoDisabledelay <
    secs>]

add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (API |
    CLOUD | DISABLED| DNS |POLICY)]

set serviceGroup <serviceGroupName [-autoDisablegraceful ( YES | NO)]
    [-autoDisabledelay <secs>]

set serviceGroup <serviceGroupName [-autoScale (API |CLOUD | DISABLED|
    DNS |POLICY)]
```

Beispiel:

```
add serviceGroup svg1 HTTP autoDisablegraceful YES -autoDisabledelay
    100

add serviceGroup svg1 HTTP -autoScale API

set serviceGroup svg1 -autoDisablegraceful  YES -autoDisabledelay 100

set serviceGroup svg1 -autoScale API
```

Argumente

autoDisablegraceful

Zeigt ein ordnungsgemäßes Herunterfahren des Dienstes an. Wenn diese Option aktiviert ist, wartet die Appliance darauf, dass alle ausstehenden Verbindungen zu diesem Dienst geschlossen werden, bevor sie den Dienst löscht. Für Clients, die bereits eine dauerhafte Sitzung im System haben, werden weiterhin neue Verbindungen oder Anfragen an diesen Dienst gesendet. Das Servicemitglied wird nur gelöscht, wenn keine ausstehenden Verbindungen bestehen. Standardwert: NO

autoDisabledelay

Zeigt die zulässige Zeit (in Sekunden) für ein ordnungsgemäßes Herunterfahren an. Während dieser Zeit werden weiterhin neue Verbindungen oder Anfragen an diesen Dienst für Clients gesendet, die bereits eine dauerhafte Sitzung im System haben. Verbindungen oder Anfragen von neuen Clients, die keine Persistenzsitzungen auf dem System haben, werden nicht an den Dienst gesendet. Stattdessen werden sie unter anderen verfügbaren Diensten Lastenausgleich durchgeführt. Nach Ablauf der Verzögerungszeit wird das Servicemitglied gelöscht.

Autoscale-API

Das API-Argument Autoscale ermöglicht die Verwendung der API für den gewünschten Status zum Binden der Elementgruppe an eine vorgesehene Dienstgruppe. Sie können die Dienstgruppe von Nicht-Autoscale auf Autoscale-Typ der Desired State-API festlegen, wenn alle bereitgestellten Bedingungen übereinstimmen.

Die gewünschte State-API prüft, ob die IP-Adresse des Dienstgruppenmitglieds mit einem vorhandenen Server verknüpft ist. Wenn die IP-Adresse mit einem vorhandenen Server übereinstimmt, verwendet die API die IP-Adresse und den Namen des vorhandenen Servers erneut. Wenn die IP-Adresse nicht mit einem vorhandenen Server übereinstimmt, erstellt die API einen Server und weist die IP-Adresse selbst als Servernamen zu.

Beispiel:

Stellen Sie sich einen Server mit der IP-Adresse 2.2.2.2 und dem Namen myserver vor, der in einer NetScaler Appliance vorhanden ist. Mit der gewünschten State-API binden Sie eine Reihe von Dienstgruppenmitgliedern, deren IP-Adresse von 2.2.2.1 bis 2.2.2.3 reicht.

Da die IP-Adresse 2.2.2.2 mit einem vorhandenen Server verknüpft ist, verwendet die API die IP-Adresse und den Namen (2.2.2.2 und myserver) erneut. Da es keine Server mit IP-Adressen gibt, 2.2.2.1, 2.2.2.3, erstellt die API Server mit diesen IP-Adressen. Die API weist die IP-Adresse selbst als Namen des Servers zu.

Wenn die im gewünschten Statusbefehl angegebene IP-Adresse mit anderen NetScaler-Entitäten wie dem virtuellen CS-Server in Konflikt steht, tritt ein Konflikt auf. Es wird eine Fehlermeldung angezeigt, die den Grund für den Fehler enthält. Die IP-Adresse des ersten Dienstgruppenmitglieds in der Liste der fehlgeschlagenen Mitglieder wird in der Fehlermeldung angezeigt.

Beispiel:

Stellen Sie sich einen Server mit der IP-Adresse 2.2.2.8 vor, der als LB-Server verwendet wird. Mit der gewünschten State-API versuchen Sie, eine Gruppe von Dienstgruppenmitgliedern zu binden, deren IP-Adresse von 2.2.2.2 bis 2.2.2.11 reicht.

Da 2.2.2.8 bereits für den LB-Dienst verwendet wird, tritt ein Konflikt auf. Die folgende Fehlermeldung wird angezeigt, die den Grund für den Fehler und die fehlgeschlagenen Mitgliedsbindungen enthält:


```
{
  "errorcode": 304, "message": "Address already in use", "severity": "
     ERROR", "servicegroup_servicegroupmemberlist_binding": {
  "servicegroupname": "sg1", "failedmembers": [ {
  "ip": "2.2.2.8", "port": 80  }
 , {
  "ip": "2.2.2.9", "port": 80  }
  ]  }
   }

<!--NeedCopy-->
```

Der Fehlercode 304 zeigt das erste Dienstgruppenmitglied in der Liste der fehlgeschlagenen Mitglieder an, die 2.2.2.8 lautet.

Der Befehl `set serviceGroup Autoscale` schlägt möglicherweise fehl, wenn die vorhandenen Memberbindungen eine der folgenden Bedingungen erfüllen:

- Wenn der an die Dienstgruppe gebundene Server entweder ein Nameserver oder ein domänenbasierter Server ist.
- Wenn der Loopback-Servername etwas anderes ist als 127.0.0.1 oder 0000:0000:0000:0000:0000:0000:0000:0
- Wenn Sie verschiedene Arten von Autoscale (Cloud, API, DNS und Richtlinie) in einem festgelegten ServiceGroup-Befehl auswählen und den Befehl ServiceGroup hinzufügen.

Wichtig:

- Die Parameter AutoDisableGraceful und AutoDisableDelay gelten nur für die Dienstgruppen vom Autoscale-Typ “API” und “CLOUD”.
- Wenn die Parameter AutoDisableGraceful oder AutoDisableDelay nicht konfiguriert sind, werden die Dienstmitglieder sofort gelöscht.

Lösen Sie ein Mitglied der Servicegruppe ordnungsgemäß

Wenn eines der Dienstgruppenmitglieder nicht in der Liste des gewünschten Status enthalten ist, sind diese Mitglieder basierend auf der Parameterkonfiguration `autoDisablegraceful` oder `autoDisabledelay` ordnungsgemäß ungebunden.

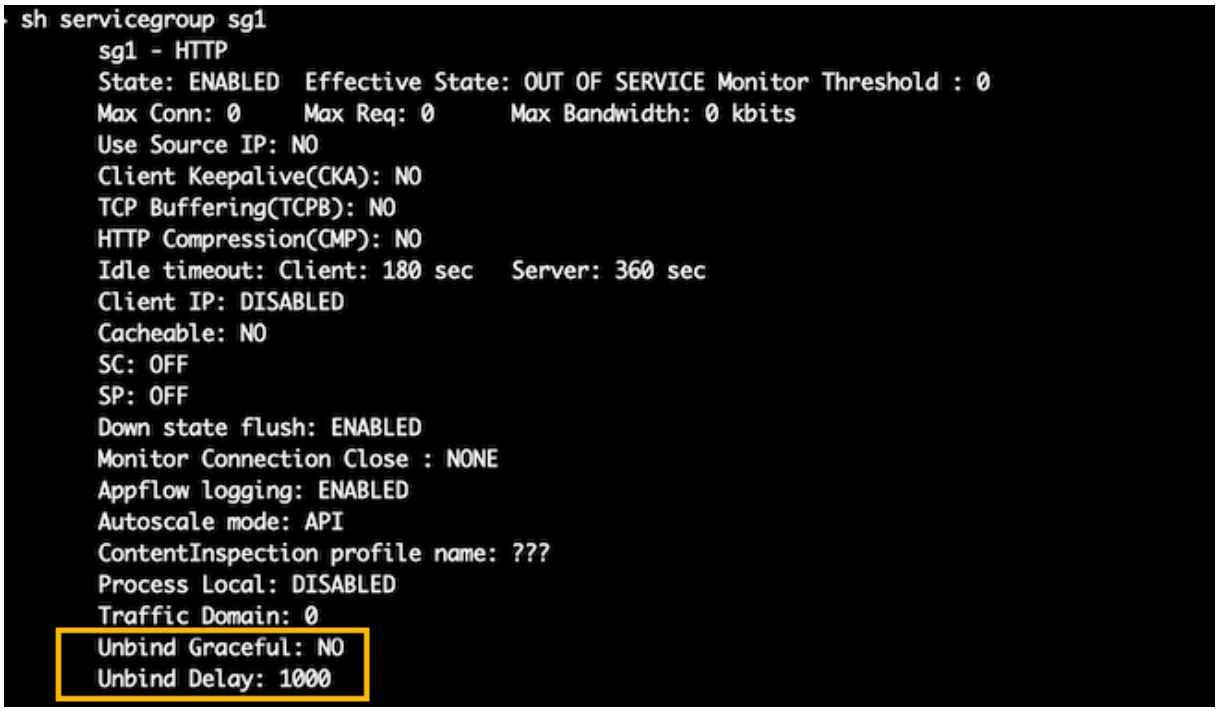
- Wenn einer dieser Parameter festgelegt ist, ist das Dienstgruppenmitglied ordnungsgemäß ungebunden.
- Wenn keiner dieser Parameter festgelegt ist, ist das Dienstgruppenmitglied sofort ungebunden.

Hinweis:

- Dienstgruppenmitglieder, die für ordnungsgemäß “unbind” identifiziert wurden, werden nur angezeigt, wenn der Befehl show service group ausgeführt wird.

- Sie können keinen Vorgang (z. B. Set, Unset) für das Dienstgruppenmitglied ausführen, das für die ordnungsgemäße Aufheben der Bindung identifiziert wurde.

Die folgende Abbildung zeigt ein Beispiel für den Befehl show service group.

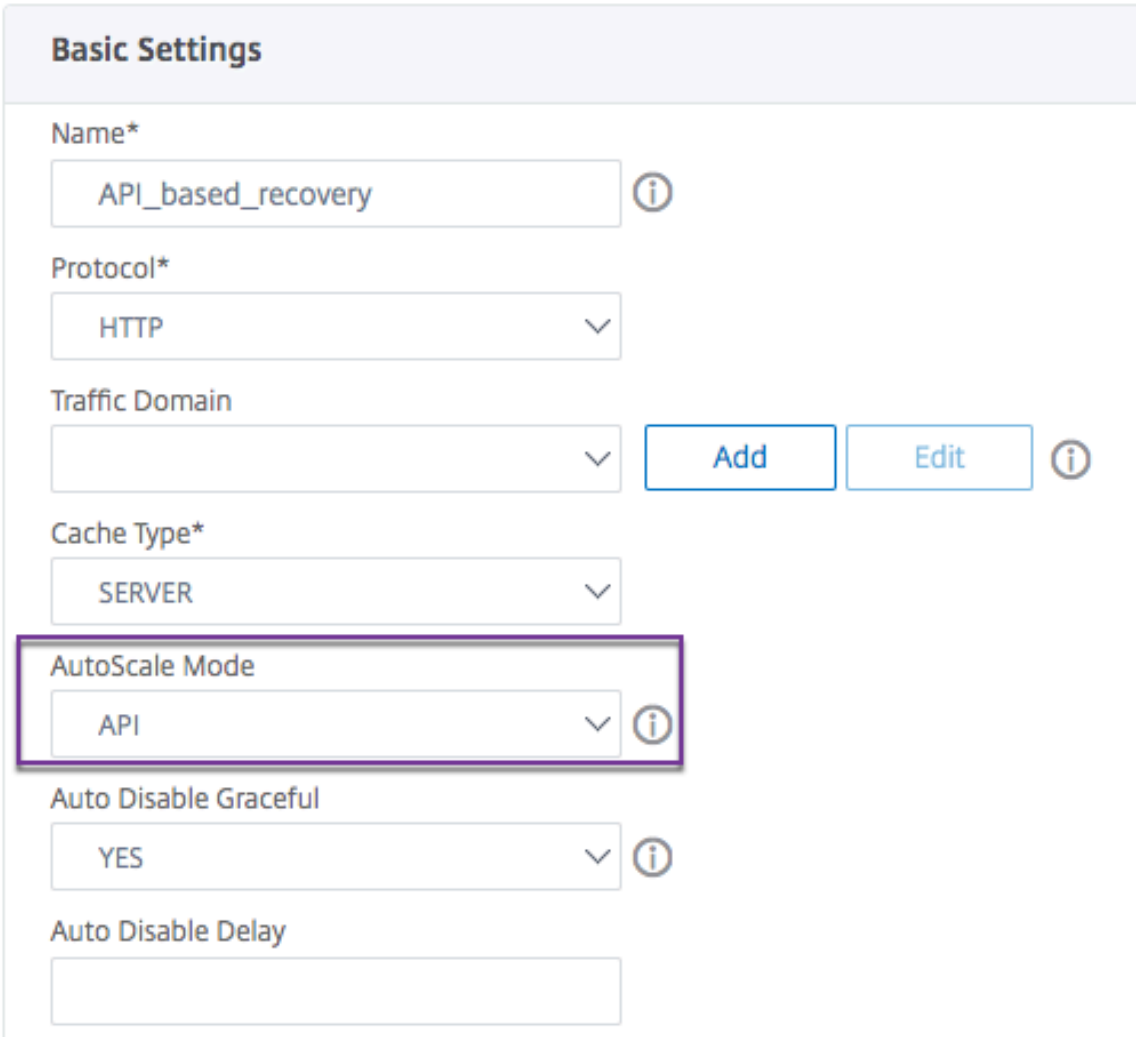


Erstellen einer Dienstgruppe vom Typ API über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienstgruppen**, und klicken Sie auf **Hinzufügen**.
2. Wählen Sie im **AutoScale-Modus** die Option **API** aus.

Konfigurieren des ordnungsgemäßen Herunterfahrens oder einer Zeitverzögerung für eine Dienstgruppe vom Typ API über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Service Groups**.



2. Wählen Sie im **AutoScale-Modus** die Option **API** aus.
3. Wählen Sie in **Auto Disable Graceful** die Option **JA**.
4. Geben Sie im **Auto Disable Delay**die Wartezeit für ein ordnungsgemäßes Herunterfahren ein.

Hinweis: Die Felder **"Graceful automatisch deaktivieren** " oder " **Verzögerung der automatischen Anzeige** " sind nur aktiviert, wenn Sie im **AutoScale-ModusAPI**oder**CLOUD**auswählen.

Automatische domänenbasierten Dienstgruppenskalierung konfigurieren

May 11, 2023

Eine domänenbasierte Dienstgruppe besteht aus Mitgliedern, deren IP-Adressen durch Auflösen der Domänennamen von Servern abgerufen werden, die an die Dienstgruppe gebunden sind. Die Domä-

nennamen werden von einem Nameserver aufgelöst, dessen Details Sie auf der Appliance konfigurieren. Eine domänenbasierte Dienstgruppe kann auch Mitglieder auf der Grundlage von IP-Adressen enthalten.

Der Prozess der Namensauflösung für einen domänenbasierten Server gibt möglicherweise mehr als eine IP-Adresse zurück. Die Anzahl der IP-Adressen in der DNS-Antwort wird durch die Anzahl der Adresseinträge (A) bestimmt, die für den Domänennamen auf dem Nameserver konfiguriert sind. Selbst wenn der Namensauflösungsprozess mehrere IP-Adressen zurückgibt, ist nur eine IP-Adresse an die Dienstgruppe gebunden. Um eine Servicegruppe nach oben oder nach unten zu skalieren, müssen Sie andere domänenbasierte Server manuell an bzw. von der Servicegruppe binden und aufheben.

Sie können jedoch eine domänenbasierte Dienstgruppe so konfigurieren, dass sie automatisch basierend auf dem vollständigen Satz von IP-Adressen skaliert wird, der von einem DNS-Nameserver für einen domänenbasierten Server zurückgegeben wird. Um die automatische Skalierung zu konfigurieren, aktivieren Sie beim Binden eines domänenbasierten Servers an eine Dienstgruppe die automatische Skalierungsoption. Im Folgenden finden Sie die Schritte zum Konfigurieren einer domänenbasierten Dienstgruppe, die automatisch skaliert:

- Fügen Sie einen Nameserver zum Auflösen von Domänennamen hinzu. Weitere Informationen zum Konfigurieren eines Nameservers auf der Appliance finden Sie unter Hinzufügen eines Nameservers.
- Fügen Sie einen domänenbasierten Server hinzu. Informationen zum Hinzufügen eines domänenbasierten Servers finden Sie unter Konfigurieren eines Serverobjekts.
- Fügen Sie eine Dienstgruppe hinzu, und ordnen Sie den domänenbasierten Server der Dienstgruppe zu, wobei die Autoscale-Option auf DNS festgelegt ist. Informationen zum Hinzufügen einer Dienstgruppe finden Sie unter Konfigurieren von Dienstgruppen.

Wenn ein domänenbasierter Server an eine Dienstgruppe gebunden ist und die Option für die automatische Skalierung auf der Bindung festgelegt ist, werden automatisch ein UDP-Monitor und ein TCP-Monitor erstellt und an den domänenbasierten Server gebunden. Die beiden Monitore fungieren als Resolver. Der TCP-Monitor ist standardmäßig deaktiviert, und die Appliance verwendet den UDP-Monitor, um DNS-Abfragen an den Namenserver zu senden, um den Domänennamen aufzulösen. Wenn die DNS-Antwort gekürzt wird (das TC-Flag auf 1 gesetzt ist), greift die Appliance auf TCP zurück und verwendet den TCP-Monitor, um die DNS-Abfragen über TCP zu senden. Danach verwendet die Appliance weiterhin nur den TCP-Monitor.

Die DNS-Antwort des Nameservers kann mehrere IP-Adressen für den Domainnamen enthalten. Wenn die automatische Skalierungsoption festgelegt ist, fragt die Appliance jede der IP-Adressen mithilfe des Standardmonitors ab und nimmt dann nur die IP-Adressen in die Dienstgruppe auf, die aktiv und verfügbar sind. Nachdem die IP-Adresseinträge, wie durch ihre Time-to-Live (TTL) -Werte definiert, ablaufen, fragt der UDP-Monitor (oder der TCP-Monitor, falls die Appliance wieder den TCP-Monitor verwendet hat) den Nameserver nach der Domänenauflösung ab und schließt alle

neuen IP-Adressen in der Dienstgruppe ein. Wenn eine IP-Adresse, die Teil der Dienstgruppe ist, in der DNS-Antwort nicht vorhanden ist, entfernt die Appliance diese Adresse aus der Dienstgruppe, nachdem vorhandene Verbindungen zum Gruppenmitglied ordnungsgemäß geschlossen wurden. In diesem Prozess können keine neuen Verbindungen mit dem Mitglied hergestellt werden. Wenn ein Domainname, der in der Vergangenheit erfolgreich aufgelöst wurde, zu einer NXDOMAIN-Antwort führt, werden alle mit dieser Domäne verknüpften Dienstgruppenmitglieder entfernt.

Statische (auf IP-Adressen basierende) Mitglieder und dynamisch skalierende domänenbasierte Mitglieder können in einer Dienstgruppe koexistieren. Sie können auch Mitglieder mit unterschiedlichen Domänennamen mit der Option für die automatische Skalierung an eine Dienstgruppe binden. Jeder Domänenname, der einer Dienstgruppe zugeordnet ist, muss jedoch innerhalb der Dienstgruppe eindeutig sein. Sie müssen die automatische Skalierungsoption für jeden domänenbasierten Server aktivieren, den Sie für die automatische Dienstgruppenskalierung verwenden möchten. Wenn eine IP-Adresse einer oder mehreren Domänen gemeinsam ist, wird die IP-Adresse nur einmal zur Dienstgruppe hinzugefügt.

> **Wichtig**
>
> - DNS Autoscale wird in einer Cluster-Bereitstellung unterstützt.
> - Die Pfadüberwachung für Autoscale-Dienstgruppen wird in der Cluster-Bereitstellung nicht unterstützt.

So konfigurieren Sie eine Dienstgruppe für die automatische Skalierung über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Dienstgruppe zu konfigurieren und die Konfiguration zu überprüfen:

```
add servicegroup <serviceGroupName> <serviceType> -autoscale DNS
<!--NeedCopy-->
```

Beispiel

Im folgenden Beispiel ist Server1 ein domänenbasierter Server. Die DNS-Antwort enthält mehrere IP-Adressen. Fünf Adressen sind verfügbar und werden der Servicegruppe hinzugefügt.

```
> add serviceGroup servGroup -autoScale YES
 Done
> sh servicegroup servGroup
        servGroup - HTTP
         State: ENABLED  Monitor Threshold : 0
               . . .
               . . .
```



```
        1)   192.0.2.31:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        2)   192.0.2.32:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        3)   192.0.2.36:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        4)   192.0.2.55:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.

        5)   192.0.2.80:80   State: UP       Server Name: server1 (Auto
             scale)    Server ID: None Weight: 1

                Monitor Name: tcp-default       State: UP
                Probes: 2       Failed [Total: 0 Current: 0]
                Last response: Success - TCP syn+ack received.
 Done
<!--NeedCopy-->
```

So konfigurieren Sie eine Dienstgruppe für die automatische Skalierung mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Erstellen Sie eine Dienstgruppe und setzen Sie den Autoscale-Modus auf DNS.

TTL-Werte überschreiben

> **Hinweis:**
>
> Diese Option wird von NetScaler 12.1 Build 51.xx und höher unterstützt.

Die NetScaler-Appliance ist so konfiguriert, dass sie den DNS-Server während des Anwendungsstarts regelmäßig nach einem Update im SRV-Eintrag abfragt, der mit der Anwendung verknüpft ist. Standardmäßig hängt die Periodizität für diese Abfrage von der im SRV-Datensatz veröffentlichten TTL ab. In Microservice- oder Cloud-World-Anwendungen ändern sich Bereitstellungen dynamischer. Daher müssen Proxys Änderungen an der Anwendungsbereitstellung schneller aufnehmen. Daher wird Benutzern empfohlen, den TTL-Parameter des domänenbasierten Dienstes explizit auf einen Wert festzulegen, der niedriger als der SRV-Datensatz-TTL ist und für Ihre Bereitstellung optimal ist. Sie können den TTL-Wert mit zwei Methoden überschreiben:

- Beim Binden eines Mitglieds an die Dienstgruppe
- Festlegen des TTL-Werts global mithilfe des Befehls set lb parameter.

Falls der TTL-Wert sowohl beim Binden des Dienstgruppenmitglieds als auch global konfiguriert wird, hat der beim Binden des Dienstgruppenmitglieds angegebene TTL-Wert Vorrang.
Wenn der TTL-Wert weder beim Binden eines Dienstgruppenmitglieds noch auf globaler Ebene angegeben wird, wird das DBS-Überwachungsintervall vom TTL-Wert in der DNS-Antwort abgeleitet.

Überschreiben der TTL-Werte mit der CLI

- Um den TTL-Wert beim Binden zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
    >])
<!--NeedCopy-->
```

Beispiel:

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Um den TTL-Wert global zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -dbsTTL 15
```



```
<!--NeedCopy-->
```

Überschreiben der TTL-Werte mit der GUI

Um den TTL-Wert beim Binden zu überschreiben:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie auf der Seite **Dienstgruppen** die Dienstgruppe aus, die Sie erstellt haben, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Load Balancing-Dienstgruppen** auf **Dienstgruppenmitglieder**.
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie im Feld **Domänenbasierter Dienst TTL**den TTL-Wert ein.

Um den TTL-Wert auf globaler Ebene zu überschreiben:

1. Navigieren Sie zu **Verkehrsmanagement** > **Load Balancing** > **Load Balancing-Parameter ändern**
2. Geben Sie im Feld **Domänenbasierter Dienst TTL**den TTL-Wert ein.

> **Hinweis:**
>
> Wenn der TTL-Wert des domänenbasierten Servers auf 0 gesetzt ist, wird der TTL-Wert aus dem Datenpaket verwendet.

Festlegen verschiedener Nameserver für Dienstgruppen- und Domänennamenbindungen

> **Hinweis:**
>
> Diese Option wird von NetScaler 12.1 Build 51.xx und höher unterstützt.

Sie können verschiedene Nameserver für verschiedene Domainnamen in einer bestimmten Gruppe konfigurieren. Das Festlegen des NameServer-Parameters ist optional, während ein DBS-Server an die Dienstgruppe gebunden wird. Wenn kein Nameserver angegeben wird, während ein Mitglied an die Dienstgruppe gebunden wird, wird der global konfigurierte Nameserver berücksichtigt.

Angeben von Nameservern beim Binden eines Servers an Dienstgruppen über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```


Beispiel:

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Angabe von Nameservern beim Binden eines Servers an Dienstgruppen über die GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie auf der Seite **Dienstgruppen** die Dienstgruppe aus, die Sie erstellt haben, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Load Balancing-Dienstgruppen** auf **Dienstgruppenmitglieder**.
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie **unter**Nameserver den Namen des Nameservers an, an den die Abfrage für die gebundene Domäne gesendet werden muss.

Automatisch verzögertes TROFS

Sie können die korrekte Übertragung von Mitgliedern in einer Dienstgruppe in den TROFS-Status konfigurieren, wenn IP-Adressen aus der DNS-Antwort entfernt werden. Wenn die Option TROFS mit automatischer Verzögerung aktiviert ist, wartet NetScaler auf den höchsten Antwort-Timeout auf allen Monitoren, die an die Servicegruppe angeschlossen sind, bevor die Mitglieder in den TROFS-Status versetzt werden.

Diese Option ist nützlich, wenn ein neuer Satz von IP-Adressen die vorhandenen vollständig ersetzt und die Konnektivität überprüft werden muss, bevor die neuen IP-Adressen hinzugefügt werden.

> **Hinweis:**
>
> Die Option `-autoDelayedTrofs` wird ab NetScaler 13.1 Build 37.xx und höher unterstützt.

Konfigurieren Sie automatisch verzögertes TROFS mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>] [-autoDelayedTrofs ( YES | NO)]
<!--NeedCopy-->
```

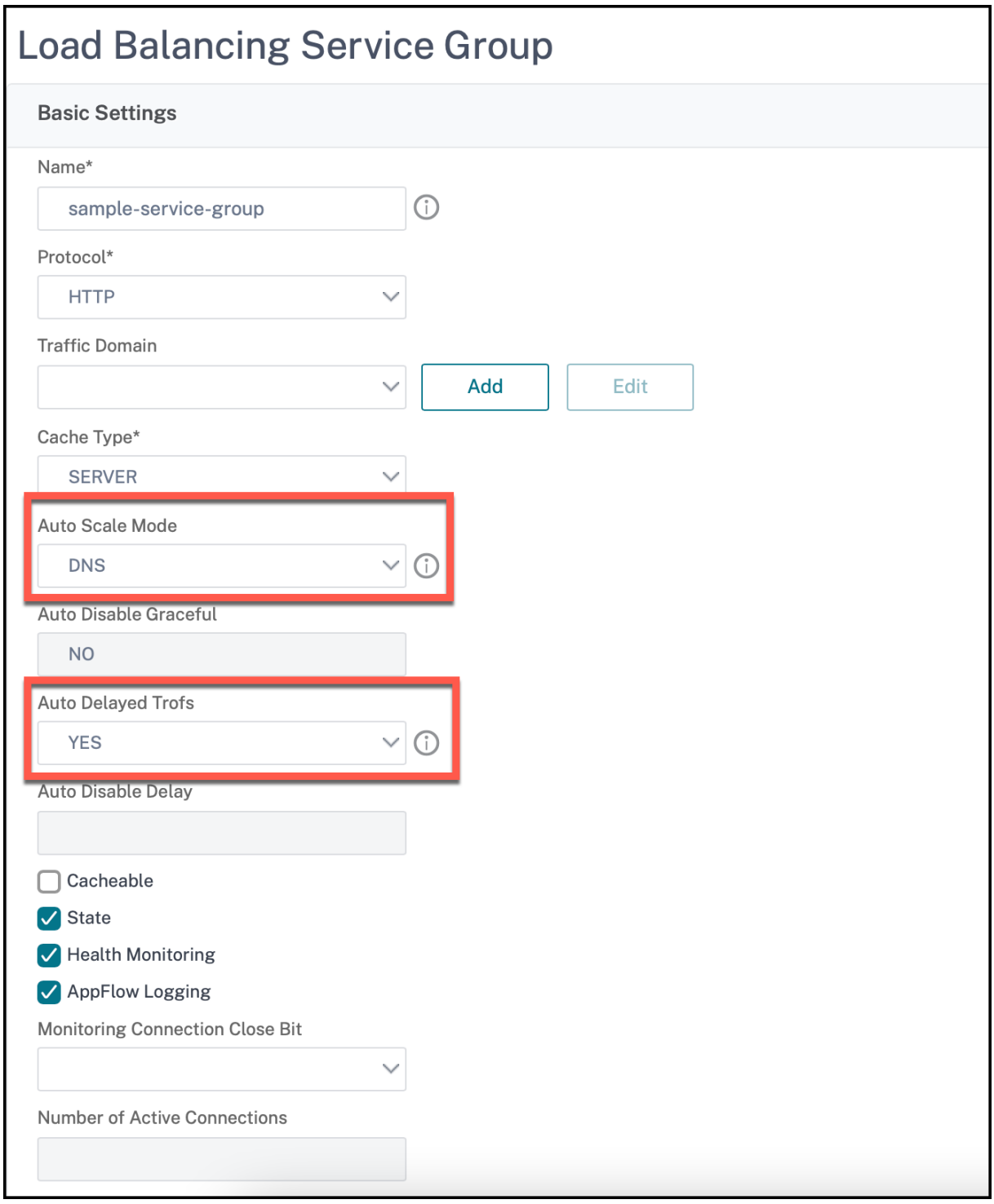
Beispiel


```
> add serviceGroup sg1 HTTP -autoScale DNS -autoDelayedTrofs YES
<!--NeedCopy-->
```

Konfigurieren Sie automatisch verzögertes TROFS über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Service Groups**.
2. Wählen Sie für **AutoScale Mode** die Option **DNS** aus.
3. Wählen Sie unter **Automatisch verzögerte Trofs**die Option **JA**aus.

> **Hinweis:**
>
> Die Option Auto Delayed Trofs ist nur aktiviert, wenn Sie DNS im AutoScale-Modus auswählen.



Dienstermittlung mit DNS-SRV-Datensätzen

May 11, 2023

Ein SRV-Record (Service Record) ist eine Spezifikation von Daten im Domain Name System, die den Standort definiert, d. h. den Hostnamen und die Portnummer der Server für bestimmte Dienste. Der Datensatz definiert auch das Gewicht und die Priorität jedes Servers.

Beispiel für einen SRV-Datensatz:

_http._tcp.example.com. 100 IN SRV 10 60 5060 a.example.com.

In der folgenden Tabelle werden die einzelnen Elemente in einem SRV-Datensatz beschrieben:

Service	Protocol	Name	TTL	Class	SRV	Priority	Weight	Port	Target
HTTP	TCP	example.com	100	IN	SRV	10	60	5060	a.example.com

Sie können die DNS-SRV-Einträge verwenden, um die Dienstendpunkte zu ermitteln. Die NetScaler-Appliance ist so konfiguriert, dass sie die DNS-Server regelmäßig mit dem SRV-Eintrag abfragt, der einem Dienst zugeordnet ist. Beim Empfang des SRV-Datensatzes ist jeder im SRV-Datensatz veröffentlichte Zielhost an eine dem Dienst zugeordnete Dienstgruppe gebunden. Jede der Bindungen erbt den Port, die Priorität und das Gewicht vom SRV-Datensatz. Für jede Dienstbereitstellung muss der Benutzer die NetScaler-Appliance einmal konfigurieren, während er sie aufruft, sodass sie als Single-Touch-Bereitstellung für Anwendungen zur Verfügung steht.

Wichtig: Das Gewicht dynamisch gelernter Servicegruppenmitglieder kann nicht mit der CLI oder der GUI geändert werden.

Anwendungsfall: Load-Balancing-Microservices

Anwendungen bewegen sich von monolithischen Architekturen in Richtung Microservice-Architektur. Durch die Umstellung auf die Microservice-Architektur zusammen mit der automatischen Back-End-Server-Lösung wird die Anwendungsbereitstellung dynamischer. Um eine solche dynamische Bereitstellung zu unterstützen, müssen die Proxys oder ADC in der Lage sein, die Back-End-Anwendungs- oder Service-Instanzen dynamisch zu erkennen und in die Proxy-Konfiguration aufzunehmen.
Die Funktion zur Diensterkennung mithilfe von DNS-SRV-Einträgen unterstützt die Konfiguration der NetScaler-Appliance in einem solchen dynamischen Bereitstellungsszenario. Anwendungsentwickler können einige Orchestrierungsplattformen verwenden, um die Anwendung bereitzustellen. Orchestrierungsplattformen beim Instanziieren von Containern während der Anwendungsbereitstellung weisen möglicherweise nicht den protokollspezifischen Standardport für jeden dieser Container zu. In solchen Szenarien wird das Erkennen der Portinformationen der Schlüssel zur Konfiguration der NetScaler Appliance. SRV-Aufzeichnungen sind in einem solchen Szenario hilfreich. SRV-Datensatzparameter wie Priorität und Gewicht können für einen besseren Lastenausgleich von Anwendungen verwendet werden.

- Der Prioritätsparameter kann verwendet werden, um die Priorität des Serverpools zu bestimmen.

- Der Gewichtsparameter kann verwendet werden, um die Kapazität der Backend-Serviceinstanzen zu bestimmen, und kann daher für den gewichteten Lastenausgleich verwendet werden.
- Immer wenn sich der Backend-Serverpool ändert, z. B. wenn eine Back-End-Instanz aus dem Pool entfernt wird, wird die Instanz freundlicherweise erst entfernt, nachdem alle bestehenden Client-Verbindungen berücksichtigt wurden.

> **Hinweis:**
>
> - Bei einer auf A/AAAA-Datensätzen basierenden Diensterkennung haben alle aufgelösten IP-Adressen das gleiche Gewicht, da Sie die Gewichtung der aufgelösten Domäne zuweisen.
> - Wenn das Gewicht in der SRV-Antwort größer als 100 ist, werden keine Dienste erstellt.

Prioritätsbasierter Lastenausgleich mithilfe von SRV-Datensätzen

Sie können SRV-Datensätze verwenden, um einen prioritätsbasierten Lastenausgleich durchzuführen. Der prioritätsbasierte Serverpool kann eine Alternative für die virtuellen Backup-Server sein. Die Datei ns.conf erfordert im Vergleich zu den virtuellen Backup-Servern nur eine minimale Konfiguration.

Beim prioritätsbasierten Lastenausgleich mit SRV-Datensätzen wird jedem Serverpool eine Prioritätsnummer zugewiesen. Die kleinste Zahl hat die höchste Priorität. Einer der Server im Pool der höchsten Priorität wird für den Lastenausgleich ausgewählt, basierend auf dem Zustand und der Verfügbarkeit des Servers. Wenn alle Server im Serverpool mit der höchsten Priorität ausgefallen sind, werden die Server mit der nächsthöheren Priorität für den Lastenausgleich ausgewählt. Wenn die Server im Serverpool mit der höchsten Priorität jedoch wieder aktiv sind, werden die Server erneut aus dem Pool mit der höchsten Priorität ausgewählt.

Der Wechsel von einem Serverpool mit Priorität zu einem anderen Serverpool erfolgt problemlos, indem die vorhandenen Clienttransaktionen gelöscht werden. Daher stellen die aktuellen Clients keine Unterbrechung des Anwendungszugriffs fest.

So aktivieren Sie die Abfrage von SRV-Datensätzen mit der CLI

Führen Sie die folgenden Aufgaben aus, um die Abfrage von SRV-Datensätzen zu aktivieren:

1. Erstellen Sie einen Server, indem Sie den Abfragetypparameter als SRV angeben.

   Geben Sie in der Befehlszeile Folgendes ein:

   ```
   add server <name> <domain> [-queryType <queryType>])
   <!--NeedCopy-->
   ```

   Beispiel:


```
add server web_serv example.com -queryType SRV
<!--NeedCopy-->
```

Hinweis:

- Standardmäßig werden IPv4-Abfragen gesendet. Um IPv6-Abfragen zu senden, müssen Sie die IPv6-Domäne aktivieren.
- Der SRV-Zieldomänenname darf 127 Zeichen nicht überschreiten.

2. Erstellen Sie eine Dienstgruppe mit dem Autoscale-Modus als DNS.

   Geben Sie in der Befehlszeile Folgendes ein:

```
add serviceGroup <serviceGroupName> <serviceType> [-autoScale <
    autoScale>]
<!--NeedCopy-->
```

   Beispiel:

```
add servicegroup svc_grp_1 http -autoscale dns
<!--NeedCopy-->
```

3. Binden Sie den in Schritt 1 erstellten Server als Mitglied an die Dienstgruppe.

   Geben Sie in der Befehlszeile Folgendes ein:

```
bind serviceGroup <serviceGroupName> <serverName>
<!--NeedCopy-->
```

   Beispiel:

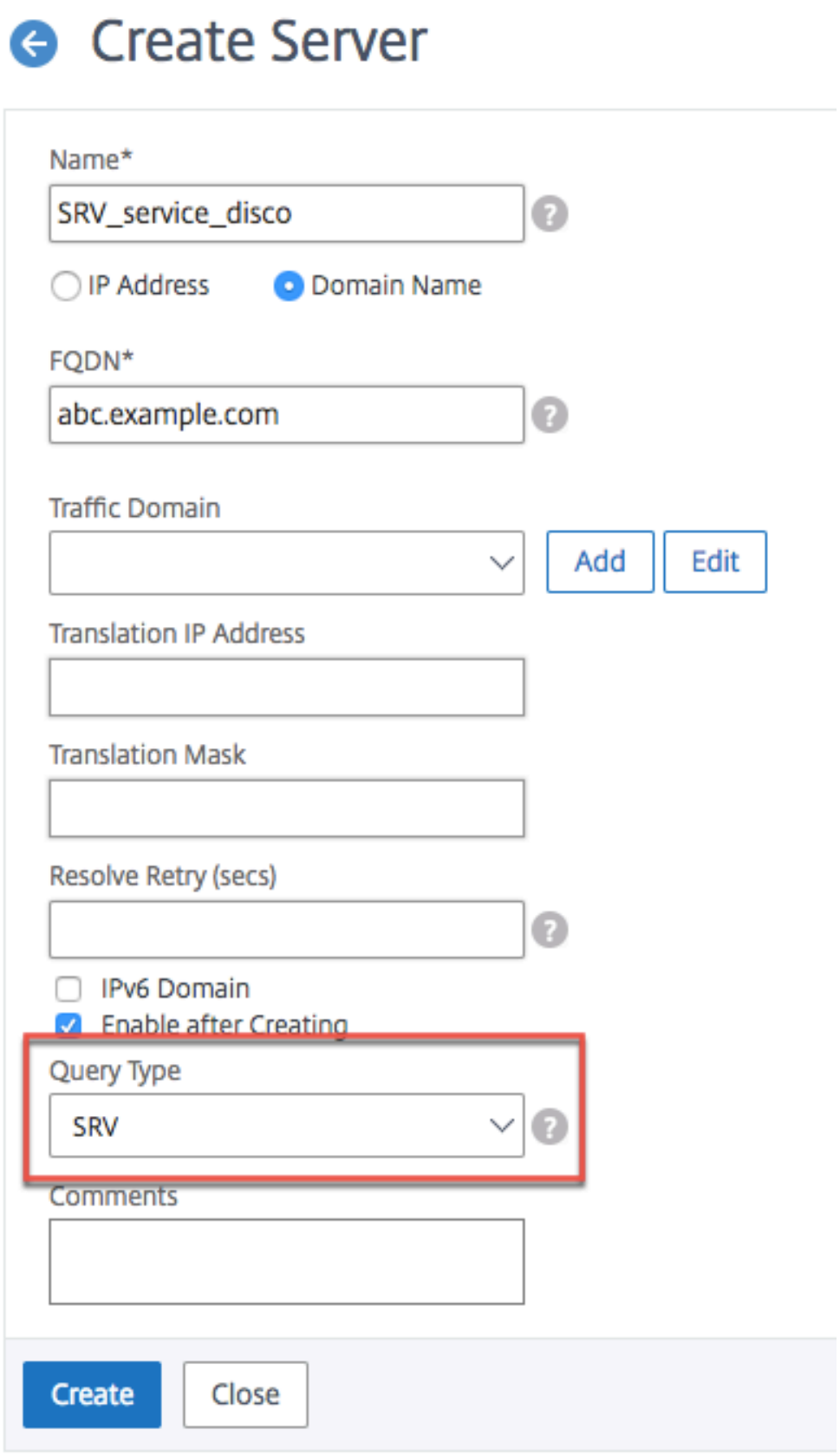
```
bind servicegroup svc_grp_1 web_serv
<!--NeedCopy-->
```

> **Hinweis:**
>
> - Wenn Sie Server an Servicegruppenmitglieder binden, müssen Sie die Portnummer für SRV-Servertypen nicht eingeben. Falls Sie eine Portnummer für den SRV-Servertyp angeben, wird eine Fehlermeldung angezeigt.
> - Sie können optional einen Nameserver und einen TTL-Wert angeben, während Sie einen Server an die Dienstgruppe binden.

So aktivieren Sie die Abfrage von SRV-Datensätzen mithilfe der GUI

Einen Server erstellen

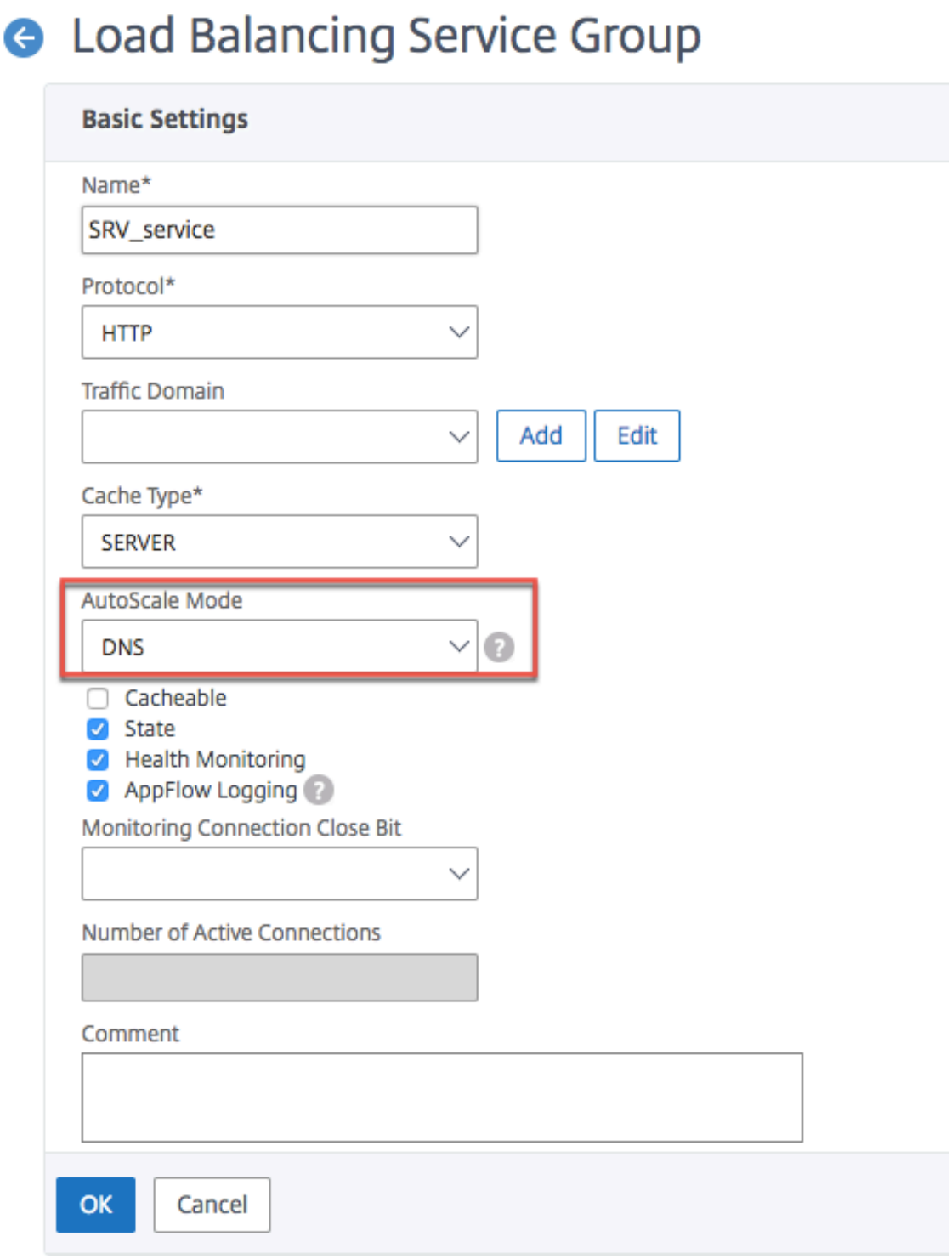
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Server**, und klicken Sie auf **Hinzufügen** .



2. Wählen Sie auf der Seite **Server erstellen** den Domänennamen aus.
3. Geben Sie die Details aller erforderlichen Parameter ein.
4. Wählen Sie unter **Abfragetyp**die Option **SRV**aus.
5. Klicken Sie auf **Erstellen**.

Erstellen Sie eine Dienstgruppe mit dem Autoscale-Modus als DNS

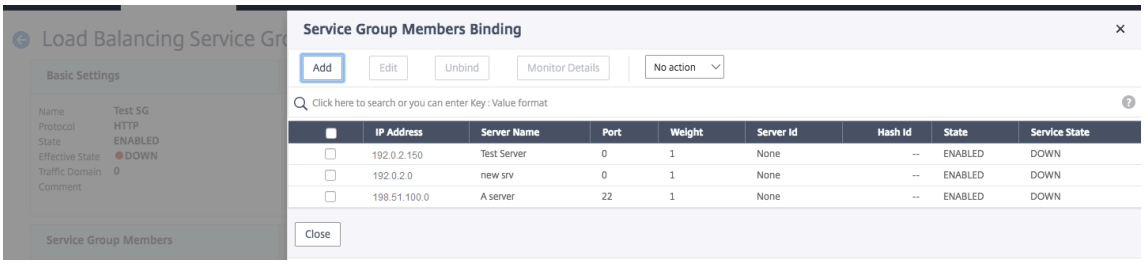
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Geben Sie auf der Seite **Load Balancing Service Group** Details zu allen erforderlichen Parametern ein.
3. Wählen Sie für **AutoScale Mode** die Option **DNS** aus.



4. Klicken Sie auf **OK**.

Server an das Mitglied der Servicegruppe binden

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie auf der Seite **Dienstgruppen** die Dienstgruppe aus, die Sie erstellt haben, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Load Balancing-Dienstgruppen** auf **Dienstgruppenmitglieder**.
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Schließen** .



Hinweis:

- Während der Bindung müssen Sie die Portnummer für SRV-Servertypen nicht eingeben. Falls Sie eine Portnummer für den SRV-Servertyp eingeben, wird eine Fehlermeldung angezeigt.
- Sie können optional einen Nameserver und einen TTL-Wert angeben, während Sie einen Server an die Dienstgruppe binden.

TTL-Werte überschreiben

Die NetScaler-Appliance ist so konfiguriert, dass sie den DNS-Server während des Anwendungsstarts regelmäßig nach einem Update im SRV-Eintrag abfragt, der mit der Anwendung verknüpft ist. Standardmäßig hängt die Periodizität für diese Abfrage von der im SRV-Datensatz veröffentlichten TTL ab. In Microservice- oder Cloud-World-Anwendungen ändern sich Bereitstellungen dynamischer. Daher müssen Proxys Änderungen an der Anwendungsbereitstellung schneller aufnehmen. Daher wird Benutzern empfohlen, den TTL-Parameter des domänenbasierten Dienstes explizit auf einen Wert festzulegen, der niedriger als der SRV-Datensatz-TTL ist und für Ihre Bereitstellung optimal ist. Sie können den TTL-Wert mit zwei Methoden überschreiben:

- Beim Binden eines Mitglieds an die Dienstgruppe
- Festlegen des TTL-Werts global mithilfe des Befehls set lb parameter.

Falls der TTL-Wert sowohl beim Binden des Dienstgruppenmitglieds als auch global konfiguriert wird, hat der beim Binden des Dienstgruppenmitglieds angegebene TTL-Wert Vorrang.
Wenn der TTL-Wert weder beim Binden eines Dienstgruppenmitglieds noch auf globaler Ebene angegeben wird, wird das DBS-Überwachungsintervall vom TTL-Wert in der DNS-Antwort abgeleitet.

Überschreiben der TTL-Werte mit der CLI

- Um den TTL-Wert beim Binden zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
    >])
<!--NeedCopy-->
```

Beispiel:

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Um den TTL-Wert global zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```

Überschreiben der TTL-Werte mit der GUI

Um den TTL-Wert beim Binden zu überschreiben:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie auf der Seite **Dienstgruppen** die Dienstgruppe aus, die Sie erstellt haben, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Load Balancing-Dienstgruppen** auf **Dienstgruppenmitglieder**.
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie im Feld **Domänenbasierter Dienst TTL**den TTL-Wert ein.

Um den TTL-Wert auf globaler Ebene zu überschreiben:

1. Navigieren Sie zu **Verkehrsmanagement** > **Load Balancing** > **Load Balancing-Parameter ändern**
2. Geben Sie im Feld **Domänenbasierter Dienst TTL**den TTL-Wert ein.

> **Hinweis**: Wenn der TTL-Wert des domänenbasierten Servers auf 0 festgelegt ist, wird der TTL-Wert aus dem Datenpaket verwendet.

Festlegen verschiedener Nameserver für Dienstgruppen- und Domänennamenbindungen

Sie können verschiedene Nameserver für verschiedene Domainnamen in einer bestimmten Gruppe konfigurieren. Das Festlegen des NameServer-Parameters ist optional, während ein DBS-Server an die Dienstgruppe gebunden wird. Wenn kein Nameserver angegeben wird, während ein Mitglied an die Dienstgruppe gebunden wird, wird der global konfigurierte Nameserver berücksichtigt.

Angeben von Nameservern beim Binden eines Servers an Dienstgruppen über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```

Beispiel:

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Angabe von Nameservern beim Binden eines Servers an Dienstgruppen über die GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**.
2. Wählen Sie auf der Seite **Dienstgruppen** die Dienstgruppe aus, die Sie erstellt haben, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Load Balancing-Dienstgruppen** auf **Dienstgruppenmitglieder**.
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie **unter**Nameserver den Namen des Nameservers an, an den die Abfrage für die gebundene Domäne gesendet werden muss.

IP-Adresse eines domänenbasierten Servers übersetzen

May 11, 2023

Um die Wartung der NetScaler-Appliance und der damit verbundenen domänenbasierten Server zu vereinfachen, können Sie IP-Adressmasken und Übersetzungs-IP-Adressen konfigurieren. Diese Funktionen arbeiten zusammen, um eingehende DNS-Pakete zu analysieren und eine neue IP-Adresse durch eine DNS-aufgelöste IP-Adresse zu ersetzen.

Wenn sie für einen domänenbasierten Server konfiguriert ist, ermöglicht die IP-Adressübersetzung die Appliance, eine alternative Server-IP-Adresse zu finden, wenn Sie den Server zur Wartung abschalten oder wenn Sie andere Infrastrukturänderungen vornehmen, die sich auf den Server auswirken.

Bei der Konfiguration der Maske müssen Sie Standard-IP-Maskenwerte (eine Potenz von zwei, minus eins) und Nullen verwenden, z. B. 255.255.0.0. Werte, die nicht Null sind, sind nur in den Startoktetten zulässig.

Wenn Sie eine Übersetzungs-IP für einen Server konfigurieren, stellen Sie eine 1:1 -Entsprechung zwischen einer Server-IP-Adresse und einem alternativen Server her, der in seiner IP-Adresse führende oder nachstehende Oktette teilt. Die Maske blockiert bestimmte Oktette in der IP-Adresse des ursprünglichen Servers. Die DNS-aufgelöste IP-Adresse wird in eine neue IP-Adresse umgewandelt, indem die Übersetzungs-IP-Adresse und die Übersetzungsmaske angewendet werden.

Sie können beispielsweise eine Übersetzungs-IP-Adresse von 10.20.0.0 und eine Übersetzungsmaske von 255.255.0.0 konfigurieren. Wenn eine DNS-aufgelöste IP-Adresse für einen Server 40.50.27.3 lautet, wird diese Adresse in 10.20.27.3 umgewandelt. In diesem Fall liefert die Übersetzungs-IP-Adresse die ersten beiden Oktette der neuen Adresse, und die Maske durchläuft die letzten beiden Oktette der ursprünglichen IP-Adresse. Der Verweis auf die ursprüngliche IP-Adresse, wie sie von DNS aufgelöst wurde, geht verloren. Monitore für alle Dienste, an die der Server gebunden ist, melden auch die transformierte IP-Adresse.

Bei der Konfiguration einer Übersetzungs-IP-Adresse für einen domänenbasierten Server geben Sie eine Maske und eine IP-Adresse an, in die die DNS-aufgelöste IP-Adresse übersetzt werden soll.

Hinweis: Die Übersetzung der IP-Adresse ist nur für domänenbasierte Server möglich. Sie können diese Funktion nicht für IP-basierte Server verwenden. Das Adressmuster kann nur auf IPv4-Adressen basieren.

So konfigurieren Sie eine Übersetzungs-IP-Adresse für einen Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
add server <name>@ <serverDomainName> -translationIp <
    translationIPAddress> -translationMask <netMask> -state <ENABLED|
    DISABLED>
<!--NeedCopy-->
```

Beispiel:

```
add server myMaskedServer www.example.com -translationIp 10.10.10.10 -
    translationMask
255.255.0.0 -state ENABLED
<!--NeedCopy-->
```

So konfigurieren Sie eine Übersetzungs-IP-Adresse für einen Server mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Server**, erstellen Sie einen domänenbasierten Server und geben Sie eine Übersetzungs-IP-Adresse an.

IP-Adresse eines virtuellen Servers maskieren

May 11, 2023

Sie können eine Maske und ein Muster anstelle einer festen IP-Adresse für einen virtuellen Server konfigurieren. Auf diese Weise kann Datenverkehr, der an eine der IP-Adressen gerichtet ist, die der Maske und dem Muster entsprechen, an einen bestimmten virtuellen Server umgeleitet werden. Sie können beispielsweise eine Maske konfigurieren, mit der die ersten drei Oktette einer IP-Adresse variabel sein können, sodass der Datenverkehr zu 111.11.11.198, 22.22.22.198 und 33.33.33.198 an denselben virtuellen Server gesendet wird.

Durch die Konfiguration einer Maske für eine IP-Adresse eines virtuellen Servers können Sie eine Neukonfiguration Ihrer virtuellen Server aufgrund einer Änderung des Routing oder einer anderen Infrastrukturänderung vermeiden. Die Maske ermöglicht es dem Datenverkehr, ohne umfangreiche Neukonfiguration Ihrer virtuellen Server weiterzufließen.

Die Maske für eine IP-Adresse eines virtuellen Servers funktioniert anders als eine IP-Musterdefinition für einen Server, die unter Übersetzen der IP-Adresse eines domänenbasierten Serversbeschrieben ist. Bei einer IP-Adressmaske des virtuellen Servers wird eine Maske ungleich Null als Oktett interpretiert, das berücksichtigt wird. Bei einem Dienst wird der Wert ungleich Null blockiert.

Für eine virtuelle Server-IP-Adresse können außerdem führende oder nachfolgende Werte berücksichtigt werden. Wenn die IP-Adressmaske des virtuellen Servers Werte von der linken Seite der IP-

Adresse berücksichtigt, wird dies als Vorwärtsmaske bezeichnet. Wenn die Maske die Werte auf der rechten Seite der Adresse berücksichtigt, wird dies als Umkehrmaske bezeichnet.

Hinweis: Die NetScaler-Appliance wertet alle virtuellen Server mit Vorwärtsmaske aus, bevor virtuelle Server mit umgekehrter Maske ausgewertet werden.

Wenn Sie eine IP-Adresse eines virtuellen Servers maskieren, müssen Sie auch ein IP-Adressmuster erstellen, um eingehenden Datenverkehr mit dem richtigen virtuellen Server abzugleichen. Wenn die Appliance ein eingehendes IP-Paket empfängt, stimmt sie die Ziel-IP-Adresse im Paket mit den Bits ab, die im IP-Adressmuster berücksichtigt werden, und nachdem sie eine Übereinstimmung gefunden hat, wendet sie die IP-Adressmaske an, um die endgültige Ziel-IP-Adresse zu erstellen.

Betrachten Sie das folgende Beispiel:

- Ziel-IP-Adresse im eingehenden Paket: 10.102.27.189
- IP-Adress-Muster: 10.102.0.0
- IP-Maske: 255.255.0.0
- Konstruierte (endgültige) Ziel-IP-Adresse: 10.102.27.189.

In diesem Fall stimmen die ersten 16 Bit in der ursprünglichen Ziel-IP-Adresse mit dem IP-Adressmuster für diesen virtuellen Server überein, sodass dieses eingehende Paket an diesen virtuellen Server weitergeleitet wird.

Wenn eine Ziel-IP-Adresse mit den IP-Mustern für mehr als einen virtuellen Server übereinstimmt, hat die längste Übereinstimmung Vorrang. Betrachten Sie das folgende Beispiel:

- Virtueller Server 1: IP-Pattern 10.10.0.0, IP-Maske 255.255.0.0
- Virtueller Server 2: IP-Pattern 10.10.10.0, IP-Maske 255.255.255.0
- Ziel-IP-Adresse im Paket: 10.10.10.45.
- Ausgewählter virtueller Server: Virtueller Server 2.

Das mit Virtual Server 2 verknüpfte Muster stimmt mit mehr Bits überein als das mit Virtual Server 1 verknüpfte, sodass IPs, die damit übereinstimmen, an Virtual Server 2 gesendet werden.

Hinweis: Ports werden auch berücksichtigt, wenn ein Tie-Breaker erforderlich ist.

So konfigurieren Sie eine IP-Adressmaske eines virtuellen Servers über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name>@ http -ipPattern <ipAddressPattern> -ipMask <
    ipMask> <listenPort>
<!--NeedCopy-->
```

Beispiel:

Mustervergleich basierend auf Präfix-Oktetten:

```
add lb vserver myLBVserver http -ippattern 10.102.0.0 -ipmask
   255.255.0.0 80
<!--NeedCopy-->
```

Mustervergleich basierend auf nachgestellten Oktetten:

```
add lb vserver myLBVserver1 http -ippattern 0.0.22.74 -ipmask
   0.0.255.255 80
<!--NeedCopy-->
```

Ändern Sie einen musterbasierten virtuellen Server:

```
set lb vserver myLBVserver1 -ippattern 0.0.22.74 -ipmask 0.0.255.255
<!--NeedCopy-->
```

Wenn Sie den Virtual Server 1 wie folgt konfigurieren:

```
add lb vserver vs1 HTTP -ippattern 100.1.1.0 -ipmask 255.255.255.0 80
<!--NeedCopy-->
```

Die NetScaler-Appliance antwortet nicht auf eine ARP-Anfrage für alle IP-Adressen. Es reagiert jedoch auf den Datenverkehr des virtuellen Servers, der an alle IP-Adressen in diesem Muster weitergeleitet wird.

So konfigurieren Sie eine IP-Adressmaske eines virtuellen Servers mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie in der Liste Adresstyp IP-Pattern aus und geben Sie ein IP-Muster und eine IP-Maske an.

Lastausgleichs für häufig verwendete Protokolle konfigurieren

May 11, 2023

Neben Websites und webbasierten Anwendungen erhalten andere Arten von netzwerkbereitgestellten Anwendungen, die andere gängige Protokolle verwenden, häufig große Datenverkehrsmengen und profitieren daher vom Lastenausgleich. Mehrere dieser Protokolle erfordern spezifische Konfigurationen, damit der Lastausgleich ordnungsgemäß funktioniert. Unter ihnen sind FTP, DNS, SIP und RTSP.

Wenn Sie Ihre NetScaler Appliance so konfigurieren, dass sie Domänennamen für Ihre Server anstelle von IPs verwendet, müssen Sie möglicherweise auch IP-Übersetzung und -Maskierung für diese Server einrichten.

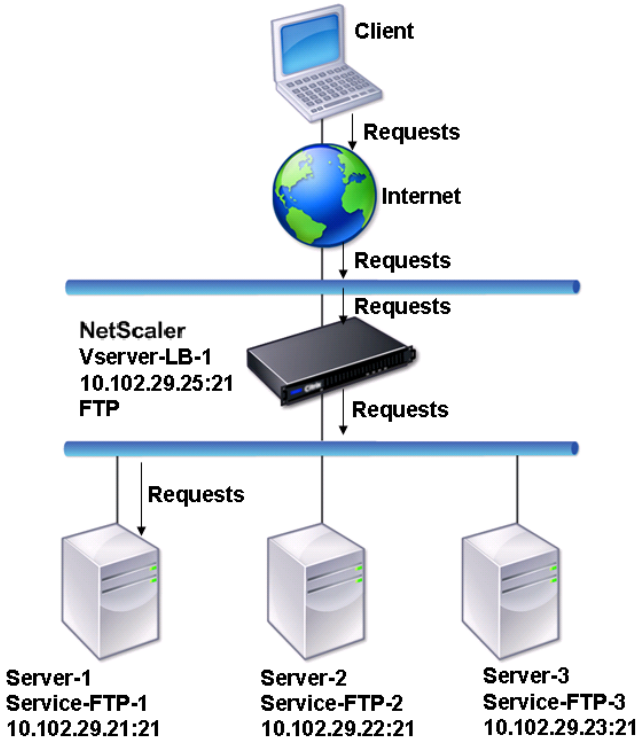
Lastausgleich für eine Gruppe von FTP-Servern

May 11, 2023

Die NetScaler-Appliance kann für den Lastenausgleich von FTP-Servern verwendet werden. FTP erfordert, dass der Benutzer zwei Verbindungen an zwei verschiedenen Ports zu demselben Server initiiert: die Kontrollverbindung, über die der Client Befehle an den Server sendet, und die Datenverbindung, über die der Server Daten an den Client sendet. Wenn der Client eine FTP-Sitzung initiiert, indem er eine Kontrollverbindung zum FTP-Server öffnet, verwendet die Appliance die konfigurierte Load-Balancing-Methode, um einen FTP-Dienst auszuwählen, und leitet die Kontrollverbindung an diesen weiter. Der FTP-Server mit Load Balancing öffnet dann eine Datenverbindung zum Client für den Informationsaustausch.

Das folgende Diagramm beschreibt die Topologie einer Load-Balancing-Konfiguration für eine Gruppe von FTP-Servern.

Abbildung 1. Grundlegende Load Balancing-Topologie für FTP-Server



Im Diagramm sind die Dienste Service-FTP-1, Service-FTP-2 und Service-FTP-3 an den virtuellen Server vServer-LB-1 gebunden. vServer-LB-1 leitet die Verbindungsanforderung des Clients an einen der Dienste weiter, wobei die Methode zum Lastausgleich mit der geringsten Verbindung verwendet wird. Nachfolgende Anfragen werden an den Dienst weitergeleitet, den die Appliance ursprünglich für den Lastenausgleich ausgewählt hat.

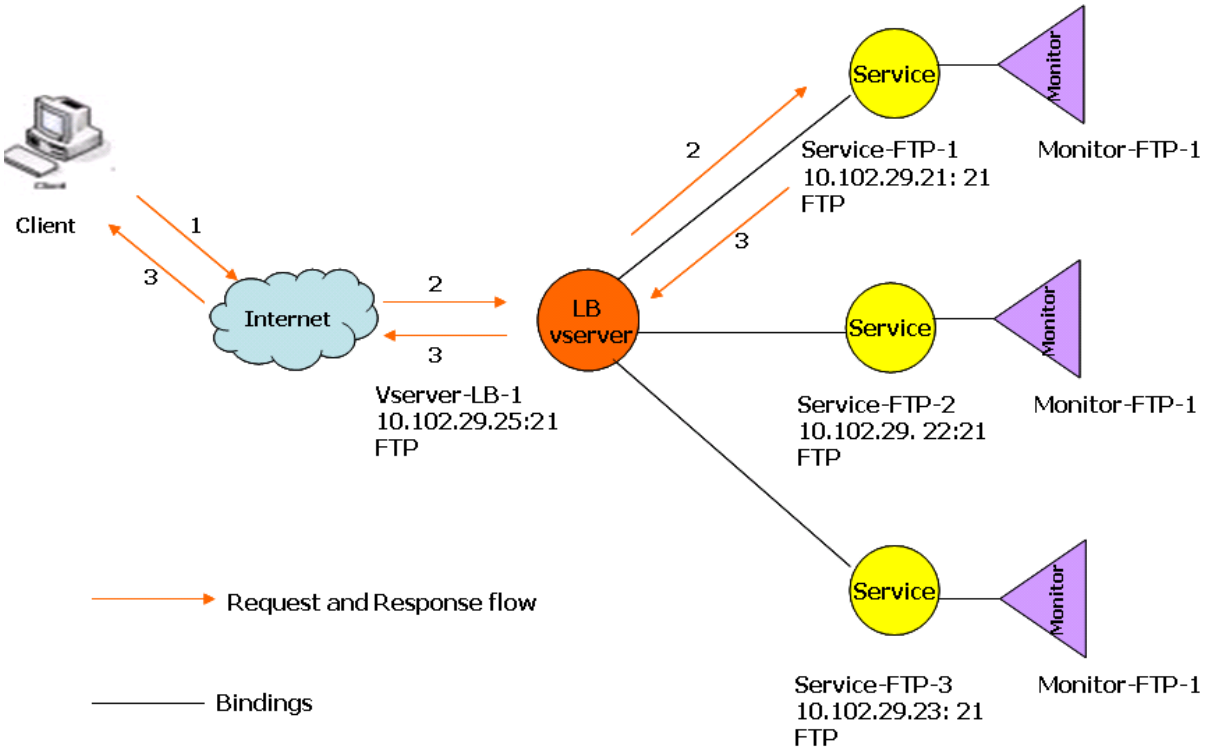
In der folgenden Tabelle sind die Namen und Werte der grundlegenden Entitäten aufgeführt, die auf der Appliance konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Vserver	Vserver-LB-1	10.102.29.25	21	FTP
Services	Service-FTP-1	10.102.29.21	21	FTP
	Service-FTP-2	10.102.29.22	21	FTP
	Service-FTP-3	10.102.29.23	21	FTP
Monitore	FTP	Ohne	Ohne	Ohne

Das folgende Diagramm zeigt die Load Balancing-Entitäten und die Werte der Parameter, die auf der

Appliance konfiguriert werden müssen.

Abbildung 2. Lastenausgleich FTP-Server-Entitätsmodell



Die Appliance kann auch eine passive FTP-Option bereitstellen, um von außerhalb einer Firewall auf FTP-Server zuzugreifen. Wenn ein Client die passive FTP-Option verwendet und eine Kontrollverbindung zum FTP-Server initiiert, initiiert der FTP-Server auch eine Kontrollverbindung zum Client. Es initiiert dann eine Datenverbindung, um eine Datei über die Firewall zu übertragen.

Informationen zum Erstellen von Diensten und virtuellen Servern vom Typ FTP finden Sie unter Einrichten des Basic Load Balancing. Benennen Sie die Entitäten und legen Sie die Parameter auf die in den Spalten der vorherigen Tabelle beschriebenen Werte fest. Wenn Sie ein grundlegendes Lastausgleichs-Setup konfigurieren, ist ein Standardmonitor an die Dienste gebunden.

Binden Sie als Nächstes den FTP-Monitor an die Dienste, indem Sie das im Abschnitt Binden von Monitoren an Dienstebeschriebenen Verfahren befolgen.

So erstellen Sie FTP-Monitore mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lb monitor <MonitorName> FTP -interval <Interval> -userName <
     UserName> -password <Password>
2 <!--NeedCopy-->
```


Beispiel:

```
add lb monitor monitor-FTP-1 FTP -interval 360 -userName User -password
    User
<!--NeedCopy-->
```

So erstellen Sie FTP-Monitore mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor vom Typ FTP, und geben Sie unter Spezielle Parameter einen Benutzernamen und ein Kennwort an.

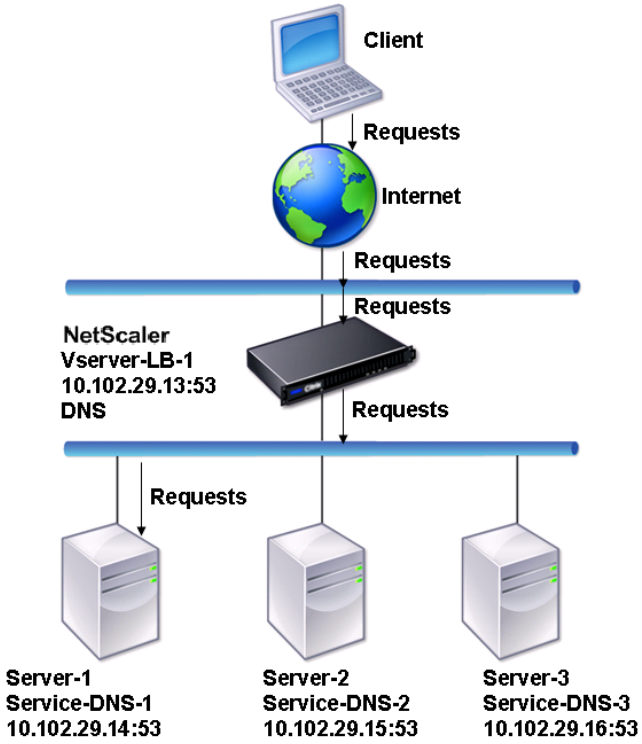
Lastausgleich für DNS-Server

May 11, 2023

Wenn Sie die DNS-Auflösung eines Domainnamens anfordern, verwendet die NetScaler-Appliance die konfigurierte Load-Balancing-Methode, um einen DNS-Dienst auszuwählen. Der DNS-Server, an den der Dienst gebunden ist, löst dann den Domainnamen auf und gibt die IP-Adresse als Antwort zurück. Die Appliance kann auch DNS-Antworten zwischenspeichern und die zwischengespeicherten Informationen verwenden, um auf zukünftige Anforderungen zur Auflösung desselben Domänennamens zu antworten. Der Lastenausgleich von DNS-Servern verbessert die DNS-Reaktionszeiten.

Das folgende Diagramm beschreibt die Topologie einer Lastausgleichskonfiguration, die eine Gruppe von DNS-Diensten mit Lastenausgleich ausgleicht.

Abbildung 1. Grundlegende Load Balancing-Topologie für DNS-Server

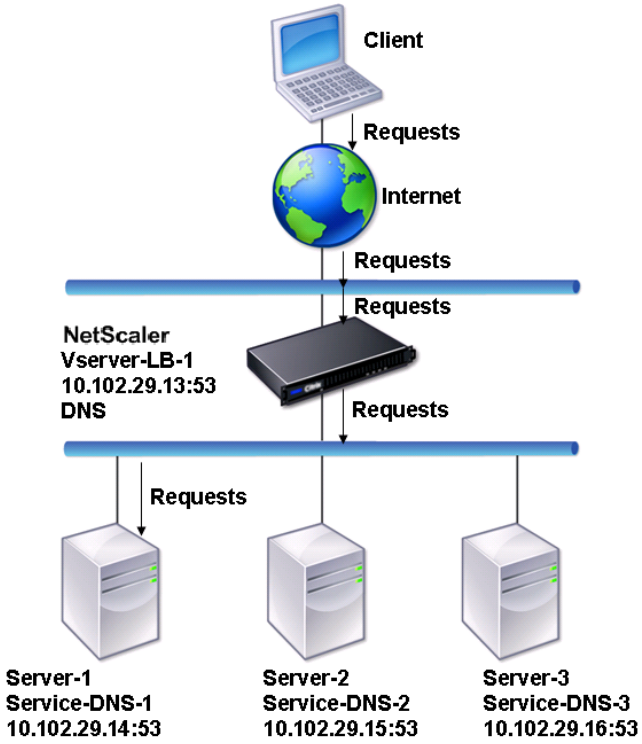


Im Diagramm sind die Dienste Service-DNS-1, Service-DNS-2 und Service-DNS-3 an den virtuellen Server vServer-LB-1 gebunden. Der virtuelle Server vServer-LB-1 leitet Clientanfragen an einen Dienst weiter, wobei die Methode zum Lastausgleich mit der geringsten Verbindung verwendet wird. In der folgenden Tabelle sind die Namen und Werte der grundlegenden Entitäten aufgeführt, die auf der Appliance konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.13	53	DNS
Services	Service-DNS-1	10.102.29.14	53	DNS
	Service-DNS-2	10.102.29.15	53	DNS
	Service-DNS-3	10.102.29.16	53	DNS
Monitore	monitor-DNS-1	Ohne	Ohne	Ohne

Das folgende Diagramm zeigt die Load Balancing-Entitäten und die Werte der Parameter, die auf der Appliance konfiguriert werden müssen.

Abbildung 2. Load Balancing DNS-Server-Entitätsmodell



Informationen zum Konfigurieren eines grundlegenden DNS-Lastenausgleichs-Setups finden Sie unter Einrichten des Basic Load Balancing. Befolgen Sie die Verfahren zum Erstellen von Diensten und virtuellen Servern vom Typ DNS, benennen Sie die Entitäten und legen Sie die Parameter anhand der in der vorherigen Tabelle beschriebenen Werte fest. Wenn Sie ein grundlegendes Lastausgleichs-Setup konfigurieren, ist der standardmäßige Ping-Monitor an die Dienste gebunden. Anweisungen zum Binden eines DNS-Monitors an DNS-Dienste finden Sie auch unter Binden von Monitoren an Dienste.

Im folgenden Verfahren werden die Schritte zum Erstellen eines Monitors beschrieben, der basierend auf einer Abfrage einen Domänennamen der IP-Adresse zuordnet.

So konfigurieren Sie DNS-Monitore mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> DNS -query <domainName> -queryType <
    Address|ZONE> -IPAddress <ipAddress>
<!--NeedCopy-->
```

Beispiel:


```
add lb monitor monitor-DNS-1 DNS -query www.citrix.com -queryType
    Address -IPAddress 10.102.29.66

add lb monitor monitor-DNS-2 DNS -query www.citrix2.com -queryType
    Address -IPAddress
1000:0000:0000:0000:0005:0600:700a::888b-888d
<!--NeedCopy-->
```

So konfigurieren Sie DNS-Monitore mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor vom Typ DNS, und geben Sie unter Spezielle Parameter einen Abfrage- und Abfragetyp an.

Lastausgleich für domänennamenbasierte Dienste

May 11, 2023

Wenn Sie einen Dienst für den Lastenausgleich erstellen, können Sie eine IP-Adresse angeben. Alternativ können Sie einen Server mit einem Domainnamen erstellen. Der Servername (Domainname) kann mithilfe eines IPv4- oder IPv6-Nameservers oder durch Hinzufügen eines autorisierenden DNS-Eintrags (Ein Datensatz für IPv4 oder AAAA-Eintrag für IPv6) zur NetScaler-Konfiguration aufgelöst werden.

Wenn Sie Dienste mit Domänennamen anstelle von IP-Adressen konfigurieren und der Nameserver den Domänennamen in eine neue IP-Adresse auflöst, führt der an den Dienst gebundene Monitor eine Zustandsprüfung für die neue IP-Adresse durch und aktualisiert die Dienst-IP-Adresse nur dann, wenn die IP-Adresse fehlerfrei ist. Der Monitor kann der Standardmonitor sein, der an den Dienst gebunden ist, oder Sie können jeden anderen unterstützten Monitor binden. Er untersucht den Dienst in regelmäßigen Abständen, die in den Monitorparametern definiert sind. Wenn der Domainname in eine neue IP-Adresse aufgelöst wird, sendet der Monitor eine neue Probe, um den Zustand des Dienstes zu überprüfen. Alle nachfolgenden Sonden befinden sich im vordefinierten Intervall.

Hinweis: Wenn Sie die IP-Adresse eines Servers ändern, wird der entsprechende Dienst für die erste Clientanfrage markiert. Der Nameserver löst die Dienst-IP-Adresse für die nächste Anfrage in die geänderte IP-Adresse auf, und der Dienst wird als UP markiert.

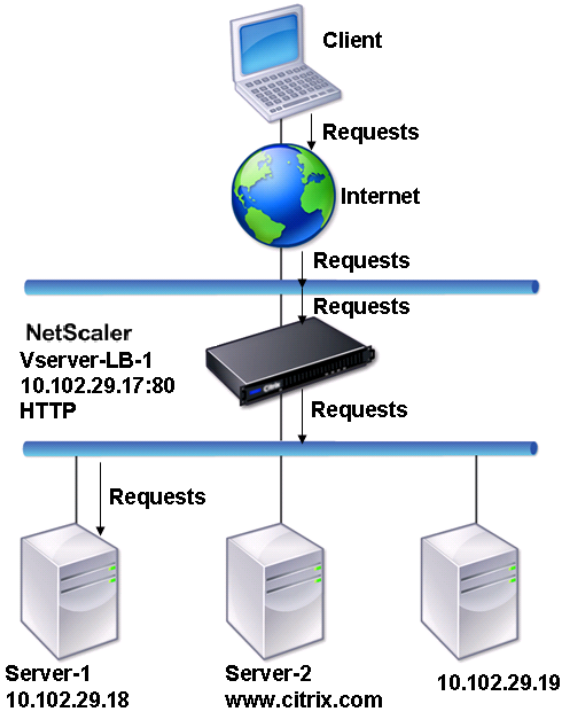
Für Dienste, die auf Domainnamen basieren, gelten die folgenden Einschränkungen:

- Die maximale Länge des Domainnamens beträgt 255 Zeichen.

- Der Parameter Maximum Client wird verwendet, um einen Dienst zu konfigurieren, der den auf Domänennamen basierenden Server darstellt. Beispielsweise wird für die Dienste, die an einen virtuellen Server gebunden sind, ein MaxClient von 1000 festgelegt. Wenn die Anzahl der Verbindungen auf dem virtuellen Server 2000 erreicht, ändert der DNS-Resolver die IP-Adresse der Dienste. Da der Verbindungszähler des Dienstes jedoch nicht zurückgesetzt wird, kann der virtuelle Server keine neuen Verbindungen aufnehmen, bis alle alten Verbindungen geschlossen sind.
- Wenn sich die IP-Adresse des Dienstes ändert, ist es schwierig, die Persistenz aufrechtzuerhalten.
- Wenn die Auflösung des Domainnamens aufgrund eines Timeouts fehlschlägt, verwendet die Appliance die alten Informationen (IP-Adresse).
- Wenn die Überwachung feststellt, dass ein Dienst ausgefallen ist, führt die Appliance eine DNS-Auflösung für den Dienst (der den auf dem Domainnamen basierenden Server darstellt) durch, um eine neue IP-Adresse zu erhalten.
- Statistiken werden in einem Dienst gesammelt und nicht zurückgesetzt, wenn sich die IP-Adresse ändert.
- Wenn eine DNS-Auflösung den Code „Namensfehler“ (3) zurückgibt, markiert die Appliance den Dienst als inaktiv und ändert die IP-Adresse auf Null.

Wenn die Appliance eine Anforderung für einen Dienst erhält, wählt sie den Zieldienst aus. Auf diese Weise gleicht die Appliance die Belastung Ihrer Dienste aus. Das folgende Diagramm beschreibt die Topologie einer Lastausgleichskonfiguration, die eine Gruppe von domainnamenbasierten Servern (DBS) ausgleicht.

Abbildung 1. Grundlegende Load Balancing-Topologie für DBS-Server



Die Dienste Service-HTTP-1, Service-Http-2 und Service-Http-3 sind an den virtuellen Server vServer-LB-1 gebunden. Der virtuelle Server vServer-LB-1 verwendet die Methode für den Lastausgleich am wenigsten für die Verbindung, um den Dienst auszuwählen. Die IP-Adresse des Dienstes wird mit dem Nameserver vServer-LB-2 aufgelöst.

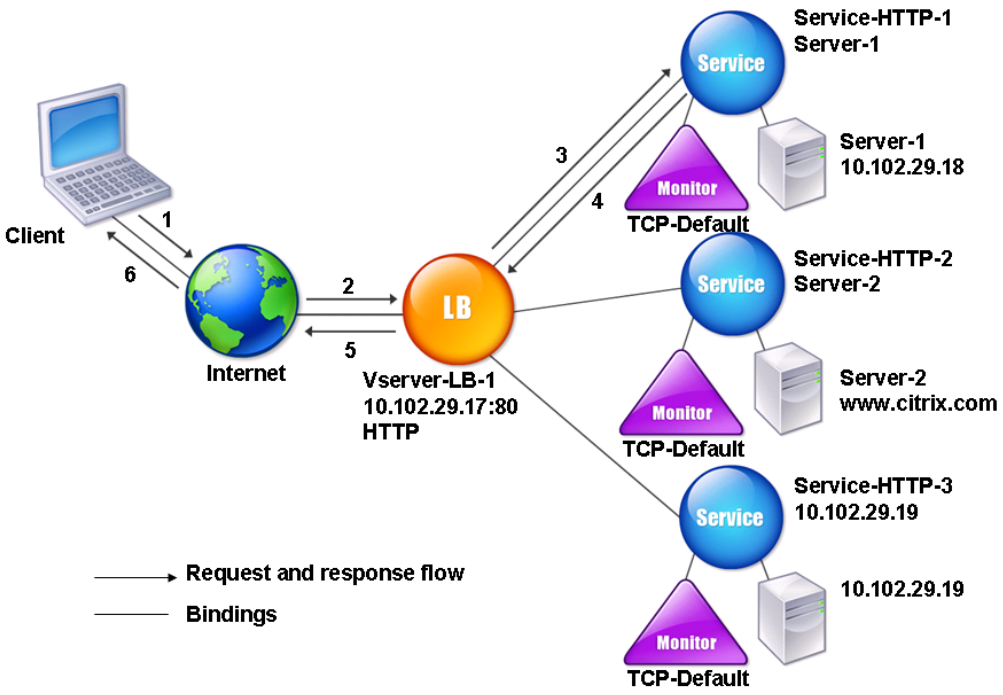
In der folgenden Tabelle sind die Namen und Werte der grundlegenden Entitäten aufgeführt, die auf der Appliance konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.17	80	HTTP
	Vserver-LB-2	10.102.29.20	53	DNS
Server	server-1	10.102.29.18	80	HTTP
	server-2	www.citrix.com	80	HTTP
Services	Service-HTTP-1	server-1	80	HTTP
	Service-HTTP-2	server-2	80	HTTP
	Service-HTTP-2	10.102.29.19	80	HTTP
Monitore	Standard	Ohne	Ohne	Ohne

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Nameserver	Ohne	10.102.29.19	Ohne	Ohne

Das folgende Diagramm zeigt die Load Balancing-Entitäten und die Werte der Parameter, die auf der Appliance konfiguriert werden müssen.

Abbildung 2. Lastenausgleich DBS-Server-Entitätsmodell



Informationen zum Konfigurieren eines grundlegenden Load Balancing-Setups finden Sie unter Einrichten des Basic Load Balancing. Erstellen Sie die Dienste und virtuellen Server vom Typ HTTP, benennen Sie die Entitäten und legen Sie die Parameter anhand der in der vorherigen Tabelle beschriebenen Werte fest.

Sie können externe Nameserver hinzufügen, entfernen, aktivieren und deaktivieren. Sie können einen Namenserver erstellen, indem Sie seine IP-Adresse angeben, oder Sie können einen vorhandenen virtuellen Server als Namenserver konfigurieren.

So fügen Sie mithilfe der Befehlszeilenschnittstelle einen Nameserver hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add dns nameServer <dnsVserverName>
<!--NeedCopy-->
```

Beispiel:

```
add dns nameServer Vserver-LB-2
<!--NeedCopy-->
```

So fügen Sie mithilfe des Konfigurationsprogramms einen Nameserver hinzu

1. Navigieren Sie zu **Traffic Management** > **DNS** > ****Nameserver****.
2. Erstellen Sie einen DNS-Nameserver vom Typ Virtueller DNS-Server und wählen Sie einen Server aus der Liste der virtuellen DNS-Server aus.

Sie können auch einen autoritativen Nameserver hinzufügen, der den Domainnamen in eine IP-Adresse auflöst.

> **Hinweis**
>
> Sie können einen Nameserver vom Typ TCP, UDP oder UDP_TCP zu Resolver-DBS-Sonden hinzufügen. Wenn jedoch TCP- und UDP-Nameserver koexistieren und ein UDP-Nameserver eine Antwort mit dem abgeschnittenen Bit erhält, wird diese Antwort über den TCP-Nameserver nicht wiederholt.

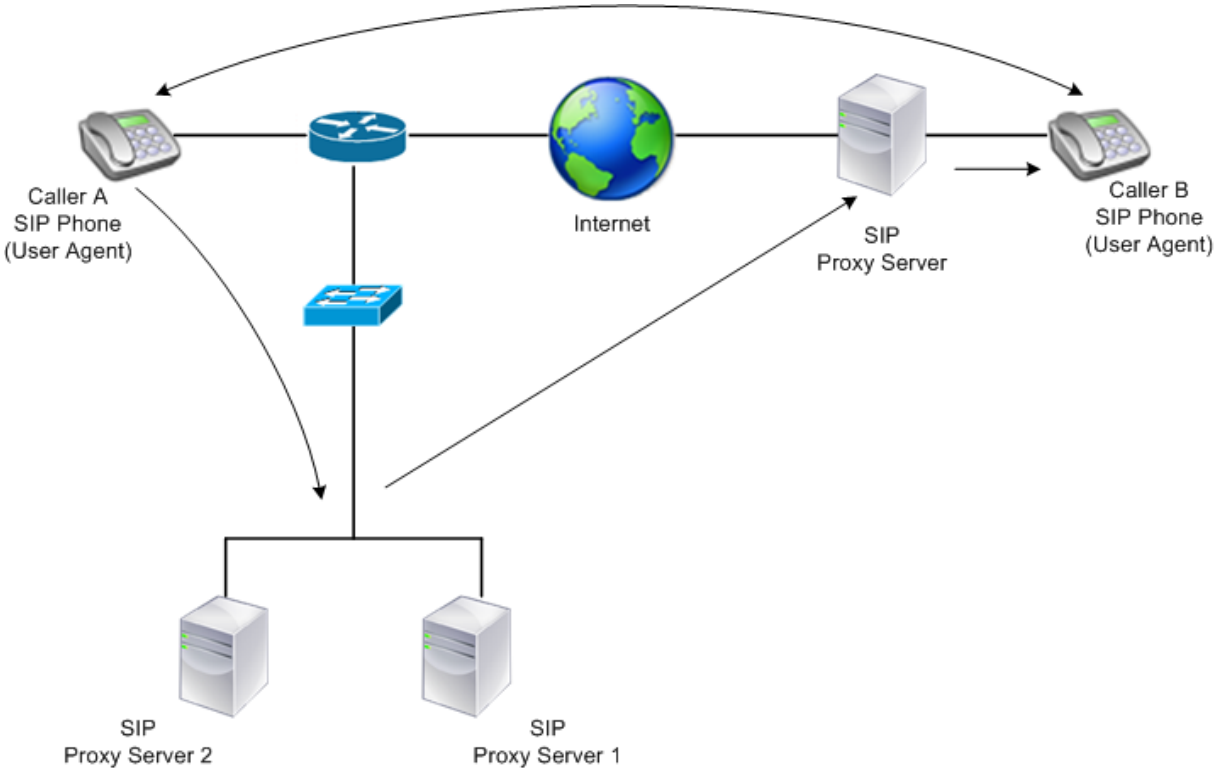
Lastausgleich für einer Gruppe von SIP-Servern

May 11, 2023

Das Session Initiation Protocol (SIP) wurde entwickelt, um multimediale Kommunikationssitzungen zu initiieren, zu verwalten und zu beenden. Es hat sich als Standard für Internettelefonie (VoIP) herausgestellt. SIP-Nachrichten können über TCP oder UDP übertragen werden. Es gibt zwei Arten von SIP-Nachrichten: Anforderungsnachrichten und Antwortnachrichten.

Der Datenverkehr in einem SIP-basierten Kommunikationssystem wird über dedizierte Geräte und Anwendungen (Entitäten) geleitet. In einer multimedialen Kommunikationssitzung tauschen diese Entitäten Nachrichten aus. Die folgende Abbildung zeigt ein grundlegendes SIP-basiertes Kommunikationssystem:

Abbildung 1. SIP-basiertes Kommunikationssystem



Mit einem NetScaler können Sie SIP-Nachrichten über UDP oder über TCP (einschließlich TLS) laden. Sie können den NetScaler so konfigurieren, dass er SIP-Anfragen an eine Gruppe von SIP-Proxyservern ausgleicht. Dazu erstellen Sie einen virtuellen Lastausgleichsserver, bei dem die Load-Balancing-Methode und der Persistenztyp auf eine der folgenden Kombinationen festgelegt sind:

- Call-ID-Hash-Load-Balancing-Methode ohne Persistenzeinstellung
- Call-ID-basierte Persistenz mit geringster Verbindung oder Round-Robin-Load-Balancing-Methode
- Regelbasierte Persistenz mit der geringsten Verbindungs- oder Roundrobin-Lastausgleichsmethode

Standardmäßig hängt der NetScaler RPORT über den Header der SIP-Anforderung an, so dass der Server die Antwort an die Quell-IP-Adresse und den Port zurücksendet, von dem die Anforderung stammt.

Hinweis: Damit der Lastenausgleich funktioniert, müssen Sie die SIP-Proxys so konfigurieren, dass sie keine privaten IP-Adressen oder privaten Domänen zum SIP-Header/Payload hinzufügen. SIP-Proxys müssen dem SIP-Header einen Domainnamen hinzufügen, der mit der IP-Adresse des virtuellen SIP-Servers übereinstimmt. Außerdem müssen die SIP-Proxys mit einer gemeinsamen Datenbank kommunizieren, um Registrierungsinformationen auszutauschen.

Vom Server initiierter Datenverkehr

Für vom SIP-Server initiierten ausgehenden Datenverkehr konfigurieren Sie RNAT auf dem NetScaler so, dass die von den Clients verwendeten privaten IP-Adressen in öffentliche IP-Adressen übersetzt werden.

Wenn Sie SIP-Parameter konfiguriert haben, die den RNAT-Quell- oder Zielport enthalten, vergleicht die Appliance die Werte der Quell- und Zielports der Anforderungspakete mit dem RNAT-Quellport und dem RNAT-Zielport. Wenn einer der Werte übereinstimmt, aktualisiert die Appliance den VIA-Header mit RPORT. Die SIP-Antwort des Clients durchläuft dann denselben Pfad wie die Anfrage.

Für serverinitiierten SSL-Verkehr verwendet der NetScaler ein integriertes Zertifikatsschlüsselpaar. **Wenn Sie ein benutzerdefiniertes Zertifikatsschlüsselpaar verwenden möchten, binden Sie das benutzerdefinierte Zertifikatsschlüsselpaar an den internen NetScaler-Dienst mit dem Namen nsrnatsip-127.0.0.1-5061.**

Unterstützung für Richtlinien und Ausdrücke

Die Sprache der NetScaler Standardausdrücke enthält mehrere Ausdrücke, die mit SIP-Verbindungen (Session Initiation Protocol) arbeiten. Diese Ausdrücke können nur an SIP-basierte (sip_udp, sip_tcp oder sip_ssl) virtuelle Server und an globale Bindungspunkte gebunden werden. Sie können diese Ausdrücke in Richtlinien für Content Switching, Ratenbegrenzung, Responder und Rewrite verwenden.

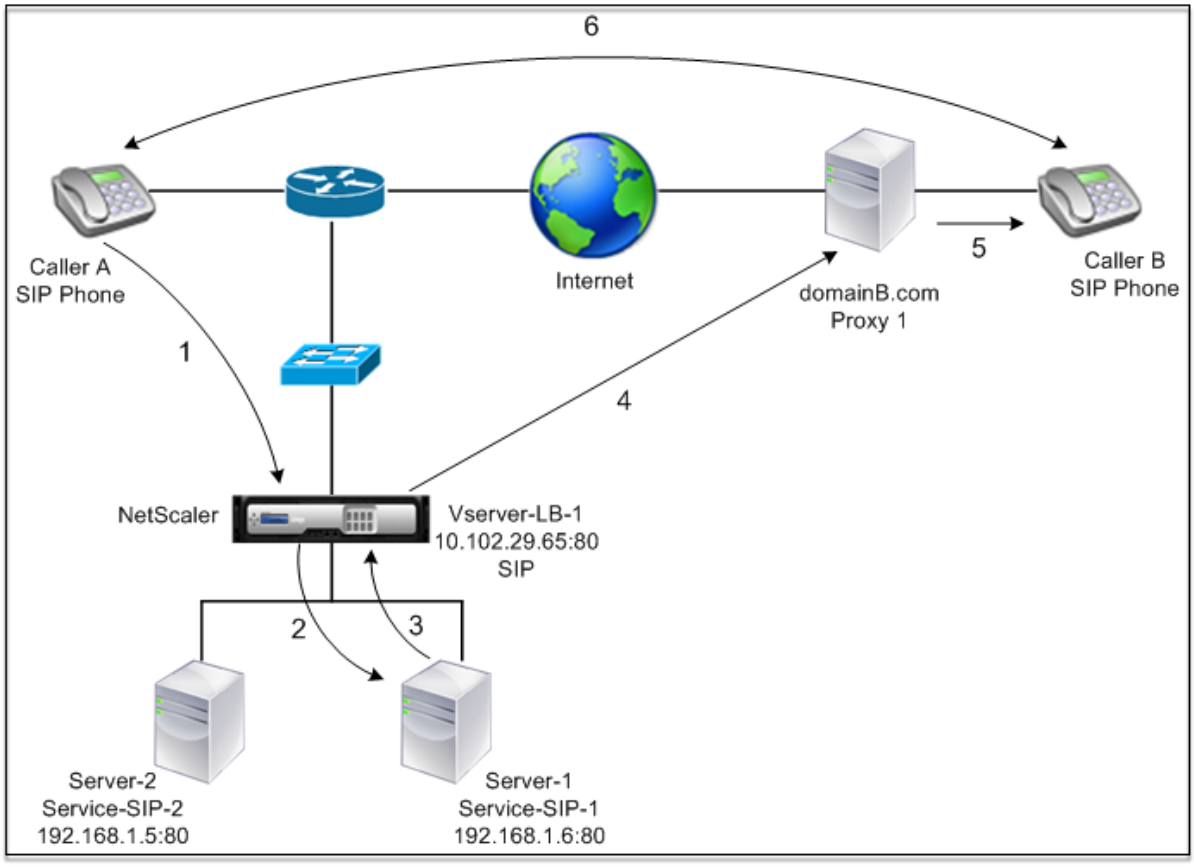
Konfiguration des Load Balancings für SIP-Signalverkehr über TCP oder UDP

Der NetScaler kann SIP-Server, die Anfragen über UDP oder TCP senden, einschließlich TCP-Verkehr, der durch TLS gesichert ist, Load Balancing durchführen. Der ADC bietet die folgenden Diensttypen für den Lastenausgleich der SIP-Server:

- SIP_UDP — Wird verwendet, wenn SIP-Server SIP-Nachrichten über UDP senden.
- SIP_TCP — Wird verwendet, wenn SIP-Server SIP-Nachrichten über TCP senden.
- SIP_SSL — Wird verwendet, um den SIP-Signalverkehr über TCP mithilfe von SSL oder TLS zu sichern. Der NetScaler unterstützt die folgenden Modi:
  - Durchgängige TLS-Verbindung zwischen dem Client, dem ADC und dem SIP-Server.
  - TLS-Verbindung zwischen dem Client und dem ADC und TCP-Verbindung zwischen dem ADC und dem SIP-Server.
  - TCP-Verbindung zwischen dem Client und dem ADC und TLS-Verbindung zwischen dem ADC und dem SIP-Server.

Die folgende Abbildung zeigt die Topologie eines Setups, das für den Lastenausgleich einer Gruppe von SIP-Servern konfiguriert ist, die SIP-Nachrichten über TCP oder UDP senden.

Abbildung 2. SIP Load Balancing Topologie



Entitätstyp	Name	IP-Adresse	Port	Diensttyp//Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.65	80	SIP_UDP/SIP_TCP/SIP_SSL
Services	Service-SIP-1	192.168.1.6	80	SIP_UDP/SIP_TCP/SIP_SSL
	Service-SIP-2	192.168.1.5	80	SIP_UDP/SIP_TCP/SIP_SSL
Monitore	Standard	Ohne	80	SIP_UDP/SIP_TCP/SIP_SSL

Im Folgenden finden Sie eine Übersicht über die Konfiguration des grundlegenden Load-Balancings für SIP-Verkehr:

1. Konfigurieren Sie Dienste und konfigurieren Sie einen virtuellen Server für jede Art von SIP-Verkehr, den Sie ausgleichen möchten:

   - **SIP_UDP** — Wenn Sie den SIP-Verkehr über UDP ausgleichen.
   - **SIP_TCP** — Wenn Sie den SIP-Verkehr über TCP ausgleichen.
   - **SIP_SSL** — Wenn Sie den SIP-Verkehr über TCP ausgleichen und sichern.

   Hinweis: Wenn Sie SIP_SSL verwenden, stellen Sie sicher, dass Sie ein SSL-Zertifikatsschlüsselpaar erstellen. Weitere Informationen finden Sie unter Hinzufügen eines Zertifikatsschlüsselpaars.

2. Binden Sie die Dienste an die virtuellen Server.
3. Wenn Sie die Zustände der Dienste mit einem anderen Monitor als dem Standardmonitor (**tcp-default**) überwachen möchten, erstellen Sie einen benutzerdefinierten Monitor und binden Sie ihn an die Dienste. Der NetScaler bietet zwei benutzerdefinierte Monitortypen, **SIP-UDP und SIP-TCP, für die Überwachung von SIP-Diensten**.
4. Wenn Sie einen virtuellen SIP_SSL-Server verwenden, binden Sie ein SSL-Zertifikatsschlüsselpaar an den virtuellen Server.
5. Wenn Sie den NetScaler als Gateway für die SIP-Server in Ihrer Bereitstellung verwenden, konfigurieren Sie RNAT.
6. Wenn Sie RPORT an die SIP-Nachrichten anhängen möchten, die vom SIP-Server initiiert werden, konfigurieren Sie die SIP-Parameter.

So konfigurieren Sie mithilfe der Befehlszeilenschnittstelle ein grundlegendes Load-Balancing-Setup für SIP-Verkehr

Erstellen Sie einen oder mehrere Dienste. Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-SIP-UDP-1 192.0.2.5 SIP_UDP 80
<!--NeedCopy-->
```

Erstellen Sie so viele virtuelle Server wie nötig, um die von Ihnen erstellten Dienste zu verarbeiten. Der virtuelle Servertyp muss mit dem Typ der Dienste übereinstimmen, die Sie an ihn binden. Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 SIP_UDP 10.102.29.60 80
<!--NeedCopy-->
```

Binden Sie jeden Dienst an einen virtuellen Server. Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serverName>
<!--NeedCopy-->
```


Beispiel:

```
bind lb vserver Vserver-LB-1 Service-SIP-UDP-1
<!--NeedCopy-->
```

(Optional) Erstellen Sie einen benutzerdefinierten Monitor vom Typ SIP-UDP oder SIP-TCP und binden Sie den Monitor an den Dienst. Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> <monitorType> [<interval>]

bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor mon1 sip-UDP -sipMethod REGISTER -sipuRI sip:mon@test.
    com -sipregURI sip:mon@test.com -respcode 200

bind monitor mon1 Service-SIP-UDP-1
<!--NeedCopy-->
```

Wenn Sie einen virtuellen SIP_SSL-Server erstellt haben, binden Sie ein SSL-Zertifikatsschlüsselpaar an den virtuellen Server. Geben Sie in der Befehlszeile Folgendes ein: Geben Sie an der Befehlszeile Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -
    CA - skipCAName
<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1
<!--NeedCopy-->
```

Konfigurieren Sie RNAT so, wie es Ihre Netzwerktopologie erfordert. Geben Sie an der Befehlszeile einen der folgenden Befehle ein, um jeweils einen RNAT-Eintrag zu erstellen, der eine Netzwerkadresse als Bedingung und SNIP als NAT-IP-Adresse verwendet, einen RNAT-Eintrag, der eine Netzwerkadresse als Bedingung und eine eindeutige IP-Adresse als NAT-IP-Adresse verwendet, einen RNAT-Eintrag, der eine ACL als Bedingung und einen SNIP als NAT-IP-Adresse verwendet, oder einen RNAT-Eintrag, der eine ACL als Bedingung verwendet und eindeutige IP-Adresse als NAT-IP-Adresse:

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ ...

```



```
show rnat
<!--NeedCopy-->
```

Beispiel:

```
add rnat RNAT-1 192.168.1.0 255.255.255.0

bind rnat RNAT-1 -natip 10.102.29.50
<!--NeedCopy-->
```

Wenn Sie ein benutzerdefiniertes Zertifikatsschlüsselpaar verwenden möchten, binden Sie das benutzerdefinierte Zertifikatsschlüsselpaar an den internen NetScaler-Dienst mit dem Namen nsrnatsip-127.0.0.1-5061.

```
add ssl certKey <certkeyName> -cert <string> [-key <string>]

bind ssl service <serviceName> -certkeyName <string>
<!--NeedCopy-->
```

Beispiel:

```
add ssl certKey c1 -cert cert.epm -key key.ky

bind ssl service nsrnatsip-127.0.0.1-5061 -certkeyName c1
<!--NeedCopy-->
```

Wenn Sie RPORT an die SIP-Nachrichten anhängen möchten, die der SIP-Server initiiert, geben Sie in der Befehlszeile den folgenden Befehl ein:

```
set lb sipParameters -rnatSrcPort <rnatSrcPort> -rnatDstPort<
    rnatDstPort> -retryDur <integer> -addRportVip <addRportVip> -
    sip503RateThreshold <sip503_rate_threshold_value>
<!--NeedCopy-->
```

Beispielkonfiguration für den Lastenausgleich des SIP-Datenverkehrs über UDP

```
add service service-UDP-1 10.102.29.5 SIP_UDP 80

Done

add lb vserver vserver-LB-1 SIP_UDP 10.102.29.60 80

Done

```



```
bind lb vserver vserver-LB-1 service-UDP-1

Done

add lb mon mon1 sip-udp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-UDP-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Beispielkonfiguration für den Lastenausgleich des SIP-Datenverkehrs über TCP

```
add service service-TCP-1 10.102.29.5 SIP_TCP 80

Done

add lb vserver vserver-LB-1 SIP_TCP 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-TCP-1

Done

add lb mon mon1 sip-tcp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-TCP-1

```



```
Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
    -addRportVip ENABLED -sip503RateThreshold 1000

Done
<!--NeedCopy-->
```

Beispielkonfiguration für Lastenausgleich und Sicherung des SIP-Datenverkehrs über TCP

```
add service service-SIP-SSL-1 10.102.29.5 SIP_SSL 80

Done

add lb vserver vserver-LB-1 SIP_SSL 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-SIP-SSL

Done

add lb mon mon1 sip-tCP -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-SIP-SSL

Done

bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done
```



```
28
29 set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
       -addRportVip ENABLED -sip503RateThreshold 1000
30
31 Done
32 <!--NeedCopy-->
```

So konfigurieren Sie ein grundlegendes Load Balancing-Setup für SIP-Datenverkehr über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle**Server und fügen Sie einen virtuellen Server vom Typ SIP_UDP, SIP_TCP oder SIP_SSL hinzu.
2. Klicken Sie auf den Abschnitt **Service** und fügen Sie einen Dienst vom Typ SIP_UDP, SIP_TCP oder SIP_SSL hinzu.
3. (Optional) Klicken Sie auf den Abschnitt **Monitor** und fügen Sie einen Monitor des Typs hinzu: SIP-UDP oder SIP-TCP.
4. Binden Sie den Monitor an den Dienst, und binden Sie den Dienst an den virtuellen Server.
5. Wenn Sie einen virtuellen SIP_SSL-Server erstellt haben, binden Sie ein SSL-Zertifikatsschlüsselpaar an den virtuellen Server. Klicken Sie auf den Abschnitt Zertifikate und binden Sie ein Zertifikatsschlüsselpaar an den virtuellen Server.
6. Konfigurieren Sie RNAT so, wie es Ihre Netzwerktopologie erfordert. Um RNAT zu konfigurieren:
   a) Navigieren Sie zu **System > Netzwerk > Routen**.
   b) Klicken Sie auf der Seite Routen auf die Registerkarte **RNAT** .
   c) Klicken Sie im Detailbereich auf **RNAT konfigurieren**.
   d) Führen Sie im Dialogfeld „RNAT konfigurieren“ einen der folgenden Schritte aus:
      - Wenn Sie die Netzwerkadresse als Bedingung für das Erstellen eines RNAT-Eintrags verwenden möchten, klicken Sie auf **Netzwerk** und legen Sie die folgenden Parameter fest:
        - Netzwerk
        - Netzmaske
      - Wenn Sie eine erweiterte ACL als Bedingung für das Erstellen eines RNAT-Eintrags verwenden möchten, klicken Sie auf **ACL** und legen Sie die folgenden Parameter fest:
        - ACL-Name
        - Port umleiten
   e) Um eine SNIP-Adresse als NAT-IP-Adresse festzulegen, fahren Sie mit Schritt 7 fort.
   f) Um eine eindeutige IP-Adresse als NAT-IP festzulegen, wählen Sie in der Liste Verfügbare NAT-IP (n) die IP-Adresse aus, die Sie als NAT-IP festlegen möchten, und klicken Sie dann

auf Hinzufügen. Die ausgewählte NAT-IP wird in der Liste der konfigurierten NAT-IPs angezeigt.

g) Klicken Sie auf Erstellenund dann auf Schließen.

Wenn Sie ein benutzerdefiniertes Zertifikatsschlüsselpaar verwenden möchten, binden Sie das benutzerdefinierte Zertifikatsschlüsselpaar an den internen NetScaler-Dienst mit dem Namen nsrnatsip-127.0.0.1-5061. Um das Paar zu binden:

a) Navigieren Sie zu **Traffic Management > Load Balancing > Services** und klicken Sie auf die Registerkarte Interne Dienste.

b) **Wählen Sie nsrnatsip-127.0.0.1-5061 und klicken Sie auf Bearbeiten.**

c) Klicken Sie auf den Abschnitt **Zertifikate** und binden Sie ein Zertifikatsschlüsselpaar an den internen Dienst.

7. Wenn Sie RPORT an die SIP-Nachrichten anhängen möchten, die der SIP-Server initiiert, konfigurieren Sie die SIP-Parameter. Navigieren Sie zu **Traffic Management > Load Balancing** und klicken Sie auf SIP-Einstellungen ändern, legen Sie die verschiedenen SIP-Parameter fest.

Beispiel für einen SIP-Ausdruck und eine Richtlinie: Komprimierung in Client-Anfragen aktiviert

Ein NetScaler kann komprimierte Client-SIP-Anfragen nicht verarbeiten, daher schlägt die Client-SIP-Anfrage fehl.

Sie können eine Responder-Richtlinie konfigurieren, die die SIP NEGOTITE-Nachricht vom Client abfängt und nach dem Komprimierungsheader sucht. Wenn die Nachricht einen Kompressionsheader enthält, antwortet die Richtlinie mit „400 Bad Request“, sodass der Client die Anfrage erneut sendet, ohne sie zu komprimieren.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Responder-Richtlinie zu erstellen:

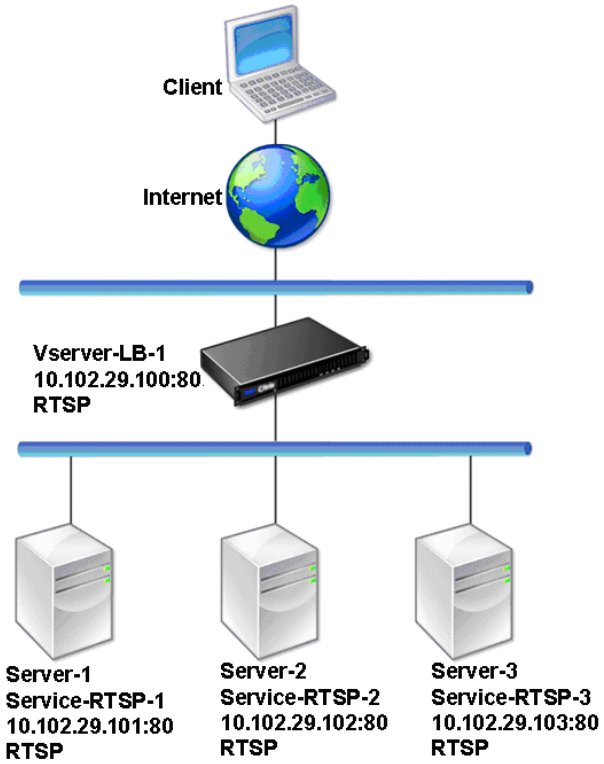
```
add responder action sipaction1 respondwith q{
 "SIP/2.0 400 Bad Requestrnrn" }


Done

add responder policy sippol1

add responder policy sippol1 "SIP.REQ.METHOD.EQ("NEGOTIATE")&&SIP.REQ.
   HEADER("Compression").EXISTS" sipaction1
<!--NeedCopy-->
```


Lastausgleich für RTSP-Server

May 11, 2023

Die NetScaler Appliance kann die Belastung von RTSP-Servern ausgleichen, um die Leistung von Audio- und Videostreams über Netzwerke zu verbessern. Das folgende Diagramm beschreibt die Topologie eines Lastausgleichs-Setups, das für den Lastausgleich einer Gruppe von RTSP-Servern konfiguriert ist.

Abbildung 1. Load-Balancing-Topologie für RTSP



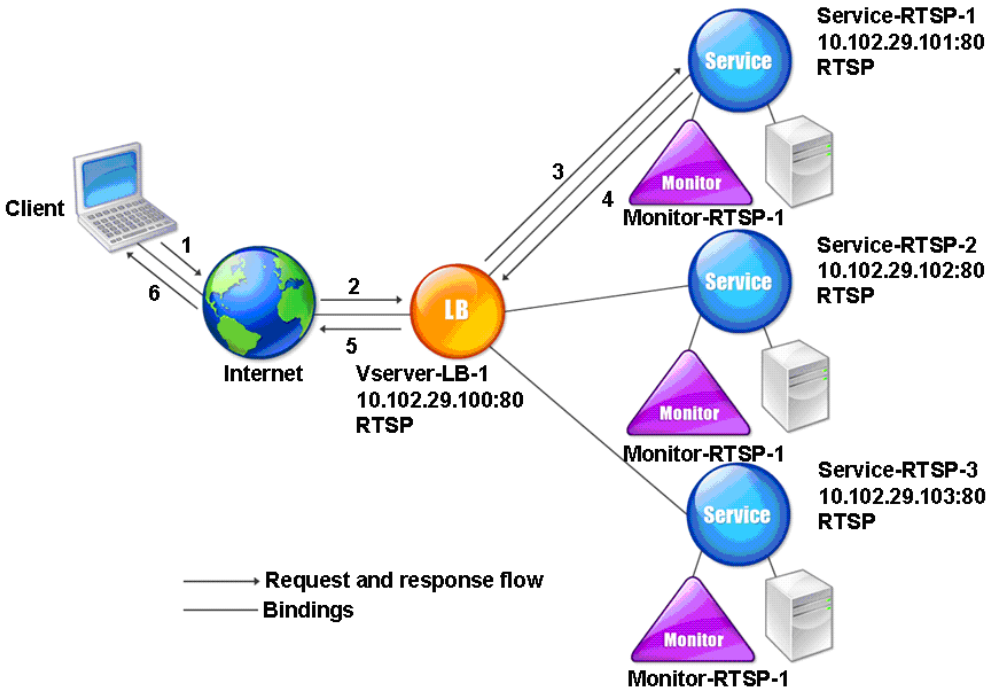
In dem Beispiel sind die Dienste Service-RTSP-1, Service-RTSP-2 und Service-RTSP-3 an den virtuellen Server vServer-LB-1 gebunden. In der folgenden Tabelle sind die Namen und Werte der Beispielentitäten aufgeführt.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.100	554	RTSP
Services	Service-RTSP-1	10.102.29.101	554	RTSP
	Service-RTSP-2	10.102.29.102	554	RTSP

Entitätstyp	Name	IP-Adresse	Port	Protokoll
	Service-RTSP-3	10.102.29.103	554	RTSP
Monitore	Monitor-RTSP-1	Ohne	554	RTSP

Das folgende Diagramm zeigt die Load Balancing-Entitäten, die in der RTSP-Konfiguration verwendet werden.

Abbildung 2. Load Balancing RTSP Server Entitätsmodell



Informationen zum Konfigurieren eines grundlegenden Lastenausgleichs-Setups für RTSP-Server finden Sie unter Einrichten des Basic Load Balancing. Erstellen Sie Dienste und virtuelle Server vom Typ RTSP. Wenn Sie ein grundlegendes Lastausgleichs-Setup konfigurieren, ist der standardmäßige TCP-Standardmonitor an die Dienste gebunden. Informationen zum Binden eines RTSP-Monitors an diese Dienste finden Sie unter Binden von Monitoren an Dienste. Im folgenden Verfahren wird beschrieben, wie ein Monitor erstellt wird, der RTSP-Server überprüft.

So konfigurieren Sie RTSP-Monitore mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor Monitor-RTSP-1 RTSP
<!--NeedCopy-->
```

So konfigurieren Sie RTSP-Monitore mit der GUI

Navigieren Sie zu Traffic Management > Load Balancing > Monitore, und erstellen Sie einen Monitor vom Typ RTSP.

Load Balance-Remotedesktopprotokollserver

May 11, 2023

Remote Desktop Protocol (RDP) ist ein mehrkanalfähiges Protokoll, das separate virtuelle Kanäle für Präsentationsdaten, serielle Gerätekommunikation, Lizenzierungsinformationen, hochverschlüsselte Daten (Tastatur- und Mausaktivität) usw. ermöglicht.

RDP wird verwendet, um einem anderen Computer im Netzwerk eine GUI zur Verfügung zu stellen. RDP wird mit Windows-Terminalservern verwendet, um einen schnellen Zugriff mit nahezu Echtzeitübertragung von Mausbewegungen und Tastendrücken auch über Verbindungen mit geringer Bandbreite zu ermöglichen.

Wenn mehrere Terminalserver bereitgestellt werden, um Remote-Desktop-Dienste bereitzustellen, sorgt die NetScaler-Appliance für den Lastenausgleich der Terminalserver (Windows 2003 und 2008 Server Enterprise Editions). Manchmal möchte ein Benutzer, der remote auf eine Anwendung zugreift, die Anwendung auf dem Remote-Computer laufen lassen, aber den lokalen Computer herunterfahren. Der Benutzer schließt daher die lokale Anwendung, ohne sich von der Remote-Anwendung abzumelden. Nach dem erneuten Verbinden mit dem Remote-Computer muss der Benutzer in der Lage sein, mit der Remote-Anwendung fortzufahren. Um diese Funktionalität bereitzustellen, berücksichtigt die NetScaler RDP-Implementierung das Routingtoken (Cookie), das vom Terminaldienstes-Sitzungsverzeichnis oder Broker festgelegt wurde, so dass der Client wieder eine Verbindung zu demselben Terminalserver herstellen kann, mit dem er zuvor verbunden war. Das Sitzungsverzeichnis, das auf dem Windows 2003 Terminal Server implementiert ist, wird auf dem Windows 2008 Terminal Server als Broker bezeichnet.

Wenn eine TCP-Verbindung zwischen dem Client und dem virtuellen Load-Balancing-Server hergestellt wird, wendet der NetScaler die angegebene Lastausgleichsmethode an und leitet die Anfrage an einen der Terminalserver weiter. Der Terminalserver überprüft das Sitzungsverzeichnis, um festzustellen, ob der Client eine Sitzung auf einem anderen Terminalserver in der Domäne ausführt.

Wenn auf einem anderen Terminalserver keine aktive Sitzung vorhanden ist, antwortet der Terminalserver mit der Clientanforderung, und die NetScaler Appliance leitet die Antwort an den Client weiter.

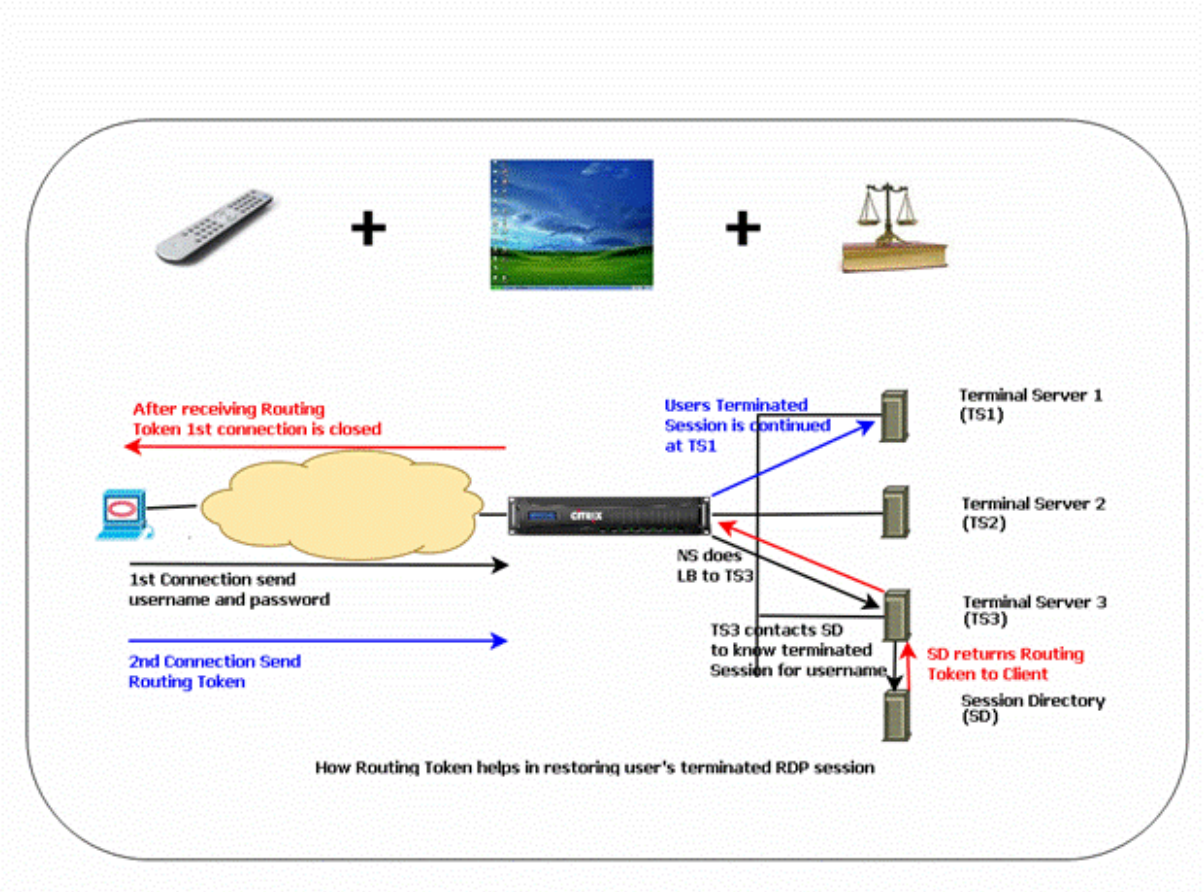
Wenn auf einem anderen Terminalserver eine aktive Sitzung stattfindet, fügt der Terminalserver, der die Anforderung erhält, ein Cookie (als Routing-Token bezeichnet) mit den Details der aktiven Sitzung ein und gibt die Pakete an die NetScaler Appliance zurück, die das Paket an den Client zurückgibt. Der Server schließt die Verbindung mit dem Client. Wenn der Client erneut versucht, eine Verbindung herzustellen, liest der NetScaler die Cookie-Informationen und leitet das Paket an den Terminalserver weiter, auf dem der Client eine aktive Sitzung hat.

Der Benutzer auf dem Client-Computer erlebt eine Fortsetzung des Dienstes und muss keine spezifischen Maßnahmen ergreifen.

Hinweis: Für die Windows-Sitzungsverzeichnisfunktion ist der Remote Desktop-Client erforderlich, der zuerst mit Windows XP veröffentlicht wurde. Wenn eine Sitzung mit einem Windows 2000- oder Windows NT 4.0-Terminalserver-Client unterbrochen wird und der Client erneut eine Verbindung herstellt, wird der Server, mit dem die Verbindung hergestellt wird, durch den Load-Balancing-Algorithmus ausgewählt.

Das folgende Diagramm beschreibt den RDP-Lastenausgleich.

Abbildung 1. Load-Balancing-Topologie für RDP



Hinweis

- Wenn ein RDP-Dienst konfiguriert ist, wird die Persistenz automatisch mithilfe eines Routing-Tokens aufrechterhalten. Sie müssen die Persistenz nicht explizit aktivieren.
- Die NetScaler-Appliance unterstützt nur IP-basierte Cookies.
- Das nsrdp.pl-Skript wird auf keiner aktuellen Version von Windows-Servern unterstützt.

Stellen Sie sicher, dass die getrennten RDP-Sitzungen auf den Terminalservern im Backend gelöscht werden, um zu verhindern, dass zwischen zwei Terminalservern hin- und herflattern, wenn eine RDP-Sitzung getrennt wird, ohne sich abzumelden. Weitere Informationen finden Sie unter `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758177(v=ws.10)##BKMK_2`.

Wenn Sie einen RDP-Dienst hinzufügen, fügt NetScaler standardmäßig einen Monitor vom Typ TCP hinzu und bindet ihn an den Dienst. Der Standardmonitor ist ein einfacher TCP-Monitor, der überprüft, ob am 3389-Port auf dem für den RDP-Dienst angegebenen Server ein Abhörvorgang stattfindet. Wenn bei 3389 ein Abhörvorgang stattfindet, markiert NetScaler diesen Dienst als AKTIV und wenn kein Abhörvorgang stattfindet, markiert es den Dienst als INAKTIV.

Für eine effizientere Überwachung eines RDP-Dienstes können Sie zusätzlich zum Standardmonitor einen Skriptmonitor konfigurieren, der für das RDP-Protokoll vorgesehen ist. Wenn Sie den

Scripting-Monitor konfigurieren, öffnet der NetScaler eine TCP-Verbindung zum angegebenen Server und sendet ein RDP-Paket. Der Monitor markiert den Dienst nur dann als aktiv, wenn er eine Bestätigung der Verbindung vom physischen Server erhält. Daher kann der NetScaler anhand des Scripting-Monitors erkennen, ob der RDP-Dienst bereit ist, eine Anfrage zu bearbeiten.

Der Monitor ist ein benutzerdefinierter Monitor und das Skript befindet sich auf dem NetScaler unter /nsconfig/monitors/nsrdp.pl. Wenn Sie den Benutzermonitor konfigurieren, führt der NetScaler das Skript automatisch aus. Um den Scripting-Monitor zu konfigurieren, fügen Sie den Monitor hinzu und binden Sie ihn an den RDP-Dienst.

Um den RDP-Lastenausgleich zu konfigurieren, erstellen Sie Dienste vom Typ RDP und binden Sie sie an einen virtuellen RDP-Server.

So konfigurieren Sie RDP-Load-Balancing-Dienste mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein RDP-Load-Balancing-Setup zu konfigurieren und die Konfiguration zu überprüfen:

```
add service <name>@ <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Hinweis: Wiederholen Sie den vorherigen Befehl, um weitere Dienste hinzuzufügen.

Beispiel

```
> add service ser1 10.102.27.182 RDP 3389
Done
> add service ser2 10.102.27.183 RDP 3389
Done
>show service ser1
ser1 (10.102. 27.182:3389) - RDP
        State: UP
…
            Server Name: 10.102.27.182
            Server ID : 0           Monitor Threshold : 0
        Down state flush: ENABLED
…
1)      Monitor Name: tcp-default
                State: UP       Weight: 1
…
                Response Time: 4.152 millisec
 Done
<!--NeedCopy-->
```


So konfigurieren Sie RDP-Load-Balancing-Dienste mithilfe des Konfigurationsprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Services**und erstellen Sie Dienste vom Typ RDP.

So konfigurieren Sie einen virtuellen RDP-Load-Balancing-Server mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um einen virtuellen RDP-Load-Balancing-Server zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name>@ <serviceType> <ipAddress> <port>

bind lb vserver <name>@ <serviceName>

Bind all the RDP services to be load balanced to the virtual server.
<!--NeedCopy-->
```

Beispiel:

In diesem Beispiel sind zwei RDP-Dienste an den virtuellen RDP-Server gebunden.

```
add lb vs v1 rdP 10.102.27.186 3389
Done

bind lb vs v1 ser1
service "ser1" bound

bind lb vs v1 ser2
service "ser2" bound
Done

sh lb vs v1
v1 (10.102.27.186:3389) - RDP   Type: ADDRESS
State: UP
…
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION
  Current Method: Round Robin, Reason: A new service is bound
Mode: IP
Persistence: NONE
  L2Conn: OFF

1) ser1 (10.102.27.182: 3389) - RDPState: UP   Weight: 1
```



```
2) ser2 (10.102.27.183: 3389) - RDPState: UP   Weight: 1
Done
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen RDP-Load-Balancing-Server mithilfe des Konfigurationsprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, erstellen Sie einen virtuellen Server vom Typ RDP und binden Sie RDP-Dienste an diesen virtuellen Server.

So konfigurieren Sie einen Skriptmonitor für RDP-Dienste mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add lb monitor <monitorName> USER -scriptName nsrdp.pl

bind lb monitor <monitorName> <rdpServiceName>
<!--NeedCopy-->
```

Beispiel:

```
add service ser1 10.102.27.182 RDP 3389

add lb monitor RDP_MON USER -scriptName nsrdp.pl

bind lb monitor RDP_MON ser1

<!--NeedCopy-->
```

So konfigurieren Sie einen Skriptmonitor für RDP-Dienste mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**und erstellen Sie einen Monitor vom Typ USER.
2. Wählen Sie unter Spezielle Parameter in der Liste Skriptname die Option nsrdp.pl aus, und binden Sie diesen Monitor dann an einen RDP-Dienst.

Prioritätsreihenfolge für Lastausgleich

May 11, 2023

Mit der Funktion “Prioritätsreihenfolge für Dienste” können Sie die Reihenfolge von Diensten oder Dienstgruppen basierend auf den Auswahleinstellungen für den Lastausgleich priorisieren. Sie können die Prioritätsreihenfolge konfigurieren, wenn Sie Folgendes tun:

- Binden Sie einen Dienst an einen virtuellen Lastausgleichsserver.
- Binden Sie eine Dienstgruppe an einen virtuellen Lastausgleichsserver.
- Binden Sie ein Dienstgruppenmitglied an die Lastausgleichsdienstgruppe.

Derzeit können Sie die Prioritätsreihenfolge für Dienste mithilfe der folgenden Methoden konfigurieren. Diese Ansätze haben jedoch die folgenden Einschränkungen:

- Konfigurieren einer virtuellen Backupserverkette: Die Anzahl der Konfigurationszeilen ist hoch, und Sie müssen den Befehl `show` mehrmals ausführen, um den Status aller LB-Dienste für jeden virtuellen Server zu ermitteln.
- Konfigurieren des bevorzugten Speicherorts: Sie müssen Standorteinträge für alle Ihre Anwendungsendpunkte erstellen.

Die Prioritätsreihenfolge für Dienste behebt die vorherigen Einschränkungen mit weniger Konfigurationsbefehlen und hilft Ihnen, die bevorzugte Standortkonfiguration zu erreichen, ohne dass die IP-Adressen aller Lastausgleichsdienste standortbezogen dargestellt werden müssen.

Konfigurieren der Prioritätsreihenfolge für Lastausgleich

Um die Prioritätsreihenfolge für Lastausgleichsdienste zu konfigurieren, wird der Parameter `-order <number>` zu den Bindungsbefehlen hinzugefügt.

> **Hinweis:**
>
> Die niedrigste Auftragsnummer hat die höchste Priorität.

Befehl:

```
bind lb vserver <vservername> <servicename/servicegroupname> -order <number>
```

Stellen Sie sich beispielsweise eine Reihe von Diensten vor, die an einen virtuellen Lastausgleichsserver (vs1) gebunden sind. Mit dem Parameter
`- order <number>` können Sie die Reihenfolge der Auswahl der Dienste wie folgt priorisieren:

- Set 1 (s1, s2) bound to vs1 – order 1

- Set 2 (s3, s4) bound to vs1 – order 2
- Set 3 (s5, s6) bound to vs1 – order 3

Nachdem Sie die Dienste an vs1 gebunden haben und wenn vs1 den Clientverkehr empfängt, ist die Reihenfolge der Auswahl der Dienste wie folgt:

- Der virtuelle Server (vs1) wählt zuerst die Dienste in Satz 1 (s1 und s2) mit der laufenden Nummer 1 aus, da dieser Menge die niedrigste Ordnungsnummer zugewiesen ist. Standardmäßig hat die niedrigste Auftragsnummer die höchste Priorität.
- Wenn alle Dienste in Satz 1 DOWN sind, wählt vs1 Satz 2 (s3 und s4) mit der laufenden Nummer 2.
- Wenn alle Dienste in Satz 1 und Satz 2 ausgefallen sind, wählt vs1 Satz 3 (s5 und s6) mit der laufenden Nummer 3.

Konfigurieren der Prioritätsreihenfolge für Load-Balancing-Dienste über die CLI

Um die Prioritätsreihenfolge für die Lastausgleichsdienste zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

1. Fügen Sie einen virtuellen LB-Server hinzu.

   ```
   add lb vserver vs1 HTTP 1.1.1.1 80
   ```

2. LB-Dienste hinzufügen.

   ```
   add service s[1-6] 2.2.2.[1-6] HTTP 80
   ```

3. Legen Sie die Auftragsnummer fest und binden Sie die Dienste an den virtuellen LB-Server.

   ```
   bind lb vserver vs1 s1 -order 1
   bind lb vserver vs1 s2 -order 1
   bind lb vserver vs1 s3 -order 2
   bind lb vserver vs1 s4 -order 2
   bind lb vserver vs1 s5 -order 3
   bind lb vserver vs1 s6 -order 3
   ```

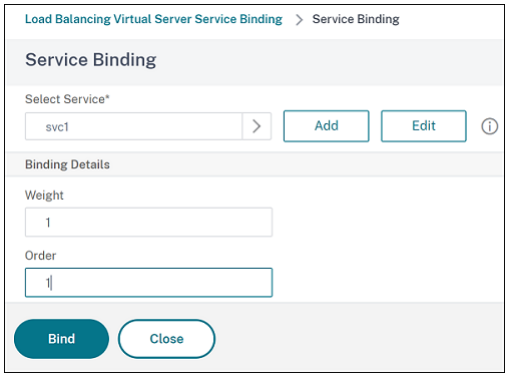
Konfigurieren der Prioritätsreihenfolge für Load Balancing-Dienste über die GUI

Voraussetzungen:

- Sie haben einen virtuellen Lastausgleichsserver erstellt.
- Sie haben Dienste erstellt.

Gehen Sie wie folgt vor, um die Prioritätsreihenfolge für Lastausgleichsdienste zu konfigurieren und sie an den virtuellen Server zu binden:

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und doppelklicken Sie auf den virtuellen Lastausgleichs
2. Klicken Sie in **Load Balancing Virtual Server**im Abschnitt **Dienste und Dienstgruppen** auf **Load Balancing Virtual Server Service Binding**.
3. Klicken Sie im Dialogfeld **Lastenausgleichsdienstbindung für virtuelle Server** auf **Bindung hinzufügen**.
4. Wählen Sie im Dialogfeld **Dienstbindung** einen Dienst aus.
5. Geben Sie eine Zahl in das Feld **Reihenfolge** ein, um die Prioritätsreihenfolge für den Dienst festzulegen.



6. Klicken Sie auf**Binden**.
7. Wiederholen Sie die Schritte 1—6, um unterschiedliche Prioritätsreihenfolgennummern für verschiedene Dienste zu konfigurieren

Konfigurieren der Prioritätsreihenfolge für Load-Balancing-Dienste mithilfe

Standardmäßig hat die niedrigste Auftragsnummer die höchste Priorität. Sie können dieses Standardverhalten jedoch mithilfe der neuen LB-Aktion und der Richtlinienbefehle aufschieben. Sie können die Reihenfolge der Serviceauswahl basierend auf dem eingehenden Clientverkehr oder den Kundendaten konfigurieren.

Stellen Sie sich beispielsweise eine Reihe von Diensten vor, die an einen virtuellen Server (vs1) gebunden sind. Mit dem Parameter – `order` <`number`> haben Sie die Prioritätsreihenfolge für Dienste wie folgt konfiguriert:

- Set 1 (s1, s2) bound to vs1 – order 1
- Set 2 (s3, s4) bound to vs1 – order 2
- Set 3 (s5, s6) bound to vs1 – order 3

Standardmäßig hat die niedrigste Auftragsnummer die höchste Priorität. Daher ist die standardmäßige Prioritätsreihenfolge der Präferenz 1, 2 und 3 für Dienste in Set 1, Set2 bzw. Set3. Für einen

bestimmten Client-Traffic möchten Sie jedoch die Prioritätsreihenfolge auf 3, 1 und 2 ändern. Um dies zu erreichen, können Sie eine LB-Richtlinie hinzufügen und an vs1 binden.

Ein LB-Richtlinienbefehl besteht aus zwei Elementen: einer Regel und einer Aktion. Die Regel ist mit einer Aktion verknüpft, die ausgeführt wird, wenn eine Anforderung mit der Regel übereinstimmt.

> **Hinweis:**
>
> Die LB-Richtlinienbefehle gelten sowohl für die LB- als auch für die GSLB-Konfiguration und gelten für die Anforderungen, die von der NetScaler-Appliance verarbeitet werden.

LB-Aktion

Ausdruck:

```
add lb action <name> <type> <string>
```

Beispiel:

```
add lb action act1 -type SELECTIONORDER -value 3 2 1
```

Parameter:

- `name`: Name der Aktion.
- `type`: Art der Aktion.
- `string`: Wert für die angegebene Aktion.

LB-Richtlinie

Ausdruck:

```
add lb policy <name> <rule> <action> <undefaction>
```

Beispiel:

```
add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
```

Parameter:

- `name`: Name der Richtlinie.
- `rule`: Eine Regel besteht aus einem oder mehreren Ausdrücken. Die Regel ist mit einer Aktion verknüpft, die ausgeführt wird, wenn die Anforderung mit der Regel übereinstimmt.
- `action`: DROP, NOLBACTION und RESET werden unterstützt.
- `undefaction`: Die NetScaler-Appliance generiert ein undefiniertes Ereignis (UNDEF-Ereignis), wenn eine Anforderung nicht mit einer Richtlinie übereinstimmt. Sie können den Befehl

`set lb param -undefAction <action>` verwenden, um die undefinierte Aktion festzulegen. Sie können diese Aktionen einem undefinierten Ereignis zuweisen: DROP, NOLBACTION und RESET.

Betrachten wir ein Beispiel, in dem Sie eine LB-Aktion, eine LB-Richtlinie, hinzufügen und die Richtlinie wie folgt an einen virtuellen Lastausgleichsserver (vs1) binden:

```
add lb action act1 -type SELECTIONORDER -value 3 1 2

add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1

bind lb vserver vs1 -policyName pol1 -priority 10
```

Die Regel wählt den Clientdatenverkehr aus, der der IP-Adresse `8.8.8.8` entspricht und sendet diesen Datenverkehr an vs1. Der Aktionstyp LB (`SELECTIONORDER`) definiert die Auswahlreihenfolge für Dienste. Nachdem Sie die LB-Richtlinie an vs1 gebunden haben und wenn vs1 den Clientdatenverkehr von der IP-Adresse `8.8.8.8` empfängt, werden die Dienste in der folgenden Reihenfolge ausgewählt:

1. Der virtuelle Server (vs1) wählt Dienste in Satz 3 (s5 und s6) mit der Prioritätsreihenfolge 3 aus.
2. Wenn alle Dienste in Satz 3 DOWN sind, wählt vs1 Satz 1 (s1 und s2) mit der Prioritätsreihenfolge 2 aus.
3. Wenn alle Dienste in Satz 3 und Satz 2 ausgefallen sind, wählt der vs1 Satz 1 (s1 und s2) mit der Reihenfolge 1.

Konfigurieren der Prioritätsreihenfolge für Load Balancing-Dienste mit LB-Richtlinienbefehlen über die CLI

Um die Prioritätsreihenfolge für Lastausgleichsdienste über LB-Richtlinienbefehle zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:

1. Fügt eine LB-Aktion hinzu.

   ```
   add lb action act1 -type SELECTIONORDER -value 3 1 2
   ```

2. Eine LB-Richtlinie hinzufügen.

   ```
   add lb policy pol1 -rule CLIENT.IP.SRC.EQ(8.8.8.8)-action act1
   ```

3. Fügen Sie einen virtuellen LB-Server hinzu.

   ```
   add lb vserver vs1 HTTP 1.1.1.1 80
   ```

4. Binden Sie die LB-Richtlinie an den virtuellen LB-Server.

   ```
   bind lb vs vs1 -policyName pol1 -priority 10
   ```

5. LB-Dienste hinzufügen.

   ```
   add service s[1-6] 2.2.2.[1-6] HTTP 80
   ```


6. Legen Sie die Reihenfolge fest und binden Sie die Dienste an den virtuellen LB-Server.

```
bind lb vserver vs1 s1 -order 1

bind lb vserver vs1 s2 -order 1

bind lb vserver vs1 s3 -order 2

bind lb vserver vs1 s4 -order 2

bind lb vserver vs1 s5 -order 3

bind lb vserver vs1 s6 -order 3
```

Konfigurieren der Prioritätsreihenfolge für Lastausgleichsdienste mit den Befehlen der LB-Richtlinie über die GUI

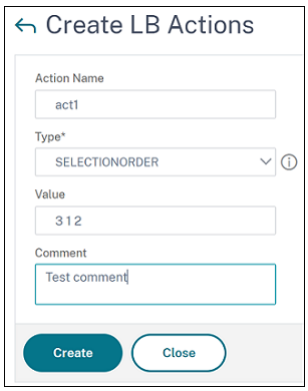
Voraussetzungen:

- Sie haben einen virtuellen Lastausgleichsserver erstellt.
- Sie haben Dienste erstellt.

Schritt 1 — Erstellen einer LB-Aktion:

1. Navigieren Sie zu **AppExpert > LB > Aktionen**.
2. Klicken Sie in**LB-Aktionen**auf**Hinzufügen**.
3. Geben**Sie im Dialogfeld LB-Aktionen erstellen** Werte für die folgenden Parameter an:
   - **Name der Aktion**: act1
   - **Typ**: SELECTIONORDER
   - **Wert**: 3 1 2

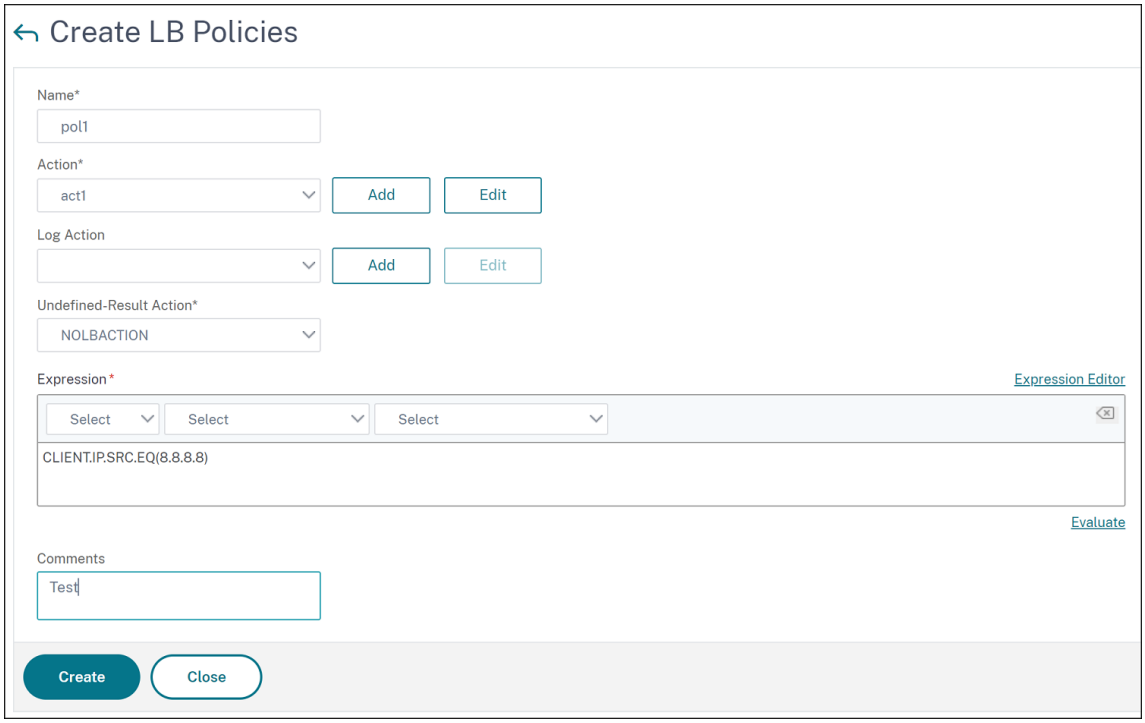
     > **Hinweis:**
     >
     > Die Zahlen im Feld **Wert**sind durch ein Leerzeichen getrennt.



4. Klicken Sie auf **Erstellen**.

Schritt 2 — Erstellen einer LB-Richtlinie:

1. Navigieren Sie zu **AppExpert > LB > Richtlinien**.
2. Klicken Sie in den**LB-Richtlinien**auf**Hinzufügen**.
3. Geben**Sie im Dialogfeld LB-Richtlinien erstellen** Werte für die folgenden Parameter an:
   - **Vorname**: pol 1
   - **Aktion**: act 1
   - **Aktion mit undefiniertem Ergebnis**: NOLBACTION
   - **Ausdruck**: CLIENT.IP.SRC.EQ (8.8.8.8)



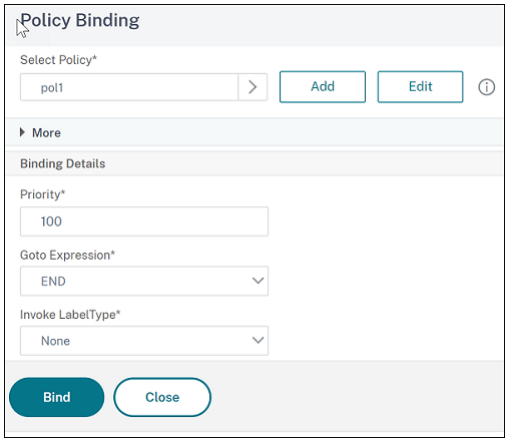
4. Klicken Sie auf**Erstellen**.

Schritt 3 — Binden Sie die LB-Richtlinie an den virtuellen LB-Server:

1. Navigieren Sie zu**Traffic Management > LB > Virtuelle Server**, und doppelklicken Sie auf den virtuellen Server.
2. Klicken Sie in**“Erweiterte Einstellungen**” auf**Richtlinien**.
3. Klicken Sie im Abschnitt**Richtlinien**auf das Pluszeichen (+).
4. Geben Sie im Dialogfeld **Typ wählen** Werte für die folgenden Parameter an:
   - **Richtlinie wählen**: LB
   - **Typ wählen**: Anfrage
5. Klicken Sie auf **Bindung hinzufügen**.

6. Geben Sie im Dialogfeld **Richtlinienbindung** Werte für die folgenden Parameter an:

   - **Wählen Sie Policy**: pol 1
   - **Priorität**: 10
   - **Gehe zu Expression**: END
   - **LabelType aufrufen**: Keine



7. Klicken Sie auf **Bind**.

Schritt 4 — Prioritätsreihenfolge für Lastausgleichsdienste konfigurieren:

Informationen zum Konfigurieren der Prioritätsreihenfolge für Lastausgleichsdienste finden Sie im Abschnitt **Konfigurieren der Prioritätsreihenfolge für Lastausgleichsdienste über die GUI**.

Persistenzeinstellungen für Dienste

Wenn Persistenz für einen Dienst konfiguriert ist, wird standardmäßig immer Persistenz bevorzugt.

Stellen Sie sich zum Beispiel einen Dienst mit konfigurierter Persistenz und Prioritätsreihenfolge 1 vor. Wenn ein Dienst mit der Prioritätsreihenfolge 0 AKTIV ist, wird immer der Dienst mit der Prioritätsreihenfolge 1 bevorzugt.

Sie können dieses Standardverhalten jedoch mit dem folgenden CLI-Befehl überschreiben:

```
set lb param -overridePersistencyforOrder <YES/NO>
```

Betrachten wir das folgende Beispiel:

Eine Reihe von Diensten ist an einen virtuellen Server (vs1) mit der folgenden Prioritätsreihenfolge gebunden:

- Set 1 (s1, s2) bound to vs1 – order 1
- Set 2 (s3, s4) bound to vs1 – order 2

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Persistenz zu überschreiben:

```
set lb parameter -overridePersistencyforOrder YES
```


Wenn Satz 1 (Dienste mit Persistenz sind konfiguriert) DOWN ist, dann behandeln Set 2 Dienste alle Anforderungen, bis die Dienste von Satz 1 UP sind. Ein Persistenzeintrag für Priorität 2 wird erstellt.

Nehmen wir an, dass die Set-1-Dienste nach einiger Zeit aktiv sind. Jetzt sind sowohl Set 1- als auch Set 2-Dienste UP, um die Anforderungen zu bearbeiten. In diesem Szenario werden neue Lastausgleichsentscheidungen getroffen, da Dienstleistungen mit höherem Auftrag in Betrieb sind. Der Persistenzeintrag wird mit einem neuen Load-Balancing-Eintrag überschrieben.

Priorität umschalten

Mit der Funktion zum Umschalten der Priorität können Sie während des Versionsupgrades für einen Dienst mit einer höheren Priorität den gesamten Datenverkehr auf einen Dienst mit niedriger Priorität umschalten. Sie können die folgenden Befehle verwenden, um die Priorität umzuschalten:

- `set lb vserver -toggleorder<Ascending/Descending>`
- `set lb vserver v1 -orderthreshold 80`

Betrachten wir zum Beispiel, dass es zwei Dienste mit den folgenden Prioritäten gibt:

- Service 1- order 0
- Service 2 – order 1

Standardmäßig verarbeitet Dienst 1 den gesamten Datenverkehr. Wenn Dienst 1 aktualisiert werden muss, muss der Datenverkehr zu Dienst 2 umgeleitet werden.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Priorität umzuschalten:

```
set lb vserver -toggleorder Descending
```

Standardmäßig hat 0 eine höhere Priorität. Nach dem Umschalten der Priorität wird 1 jedoch als höhere Priorität betrachtet. Wenn für den Dienst ein Persistenzeintrag vorhanden ist, wird das Verhalten der Persistenzeinstellung wie im Abschnitt **Persistenzeinstellungen für Dienste** erläutert.

Anwendungsfall 1: SMPP-Lastausgleich

May 11, 2023

Millionen von Kurznachrichten werden täglich zwischen Einzelpersonen und Mehrwertdienstanbietern wie Banken, Werbetreibenden und Verzeichnisdiensten ausgetauscht, indem das Short Message Peer-to-Peer (SMPP) -Protokoll verwendet wird. Oft verzögert sich die Nachrichtenzustellung, weil die Server überlastet sind und der Datenverkehr nicht optimal auf die Server verteilt wird. Der NetScaler unterstützt den SMPP-Lastenausgleich und sorgt für eine optimale Verteilung von Nachrichten auf Ihren Servern, wodurch Leistungseinbußen und Ausfällen vorgebeugt wird.

Der NetScaler führt einen Lastenausgleich auf der Serverseite durch, wenn Nachrichten von Clients empfangen werden, und auf der Clientseite, wenn Nachrichten von Servern empfangen werden.

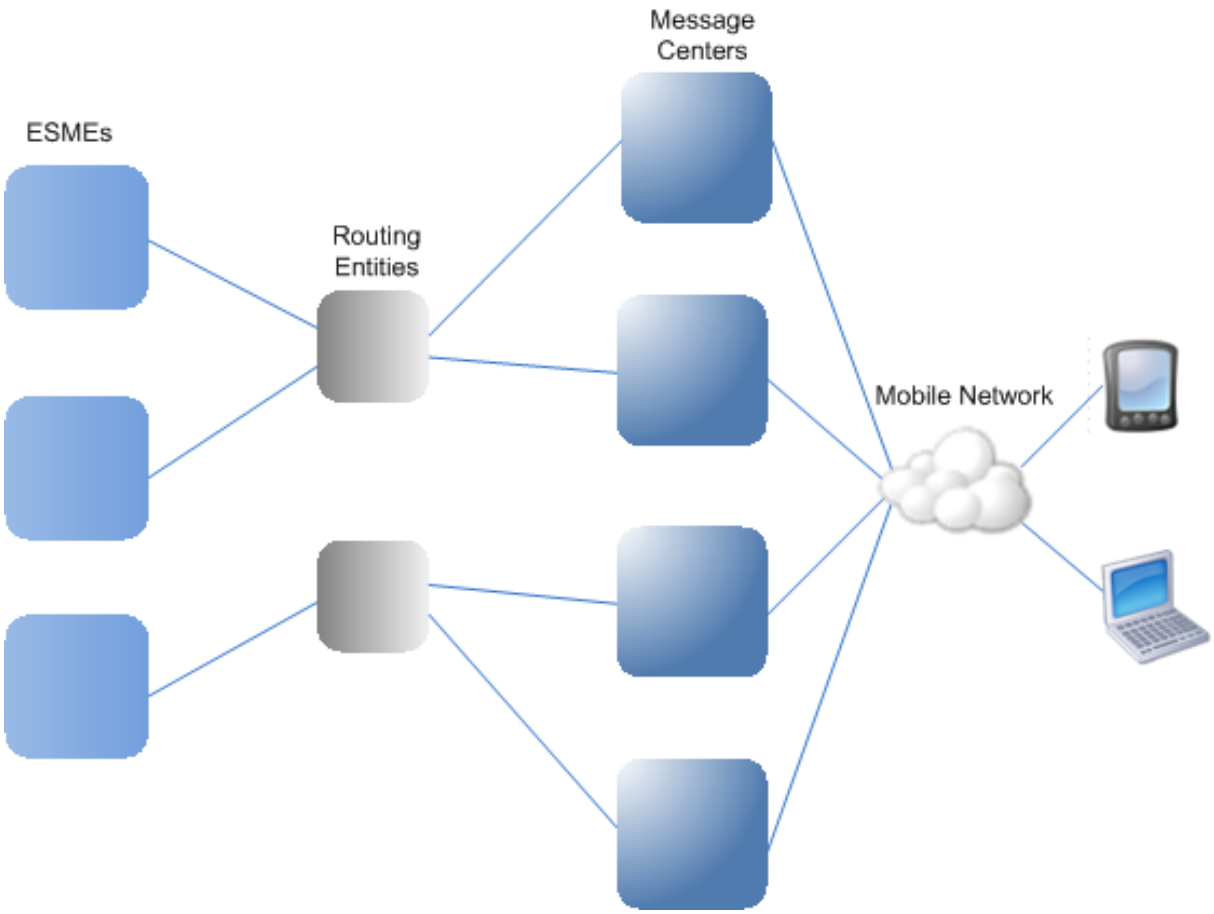
Der Lastausgleich von SMPP-Nachrichten durch den NetScaler bietet die folgenden Vorteile:

- Bessere Lastverteilung auf Servern, was zu schnelleren Reaktionszeiten für Endbenutzer führt
- Überwachung des Serverzustands und bessere Failover-Funktionen
- Schnelles und einfaches Hinzufügen neuer Server (Message Center) ohne Änderung der Client-Konfiguration
- Hohe Verfügbarkeit

Einführung in SMPP

SMPP ist ein Anwendungsschicht-Protokoll für die Übertragung von Kurznachrichten zwischen externen Kurznachrichtentitäten (ESME), Routing-Entitäten (RE) und Message Centers (MC) über langlebige TCP-Verbindungen. Es wird zum Senden von Kurznachrichtendiensten (SMS) zwischen Freunden, Kontakten und Dritten wie Banken (Mobile Banking), Werbetreibenden (Mobile Commerce) und Verzeichnisdiensten verwendet. Nachrichten von einer ESME (Non-Mobile Entity) kommen beim MC an, der sie an Short Message Entities (KMU) wie Mobiltelefone weiterleitet. SMPP wird auch von KMU verwendet, um Kurznachrichten an Dritte zu senden (z. B. für den Kauf von Produkten, Rechnungszahlung und Geldüberweisung). Diese Nachrichten kommen am MC an und werden an den Ziel-MC oder ESME weitergeleitet.

Das folgende Diagramm zeigt die verschiedenen SMPP-Entitäten: ESMEs, REs und MCs in einem Mobilfunknetz.



Architekturübersicht der verschiedenen SMPP-Entitäten in einem Mobilfunknetz

Hinweis: Die Begriffe Client und ESME werden im gesamten Dokument synonym verwendet.

Ein ESME (Client) stellt in einem der drei Modi eine Verbindung zum MC her: als Sender, Empfänger oder Transceiver. Als Sender kann er nur Nachrichten zur Zustellung senden. Als Empfänger kann es nur Nachrichten empfangen. Als Transceiver kann die ESME Nachrichten sowohl senden als auch empfangen. Die ESME sendet dem MC eine der drei Nachrichten (auch bekannt als PDUs): bind_transmitter, bind_receiver oder bind_transceiver. Der MC antwortet mit bind_transmitter_resp, bind_receiver_resp oder bind_transceiver_resp, je nachdem, was für die Anfrage erforderlich ist.

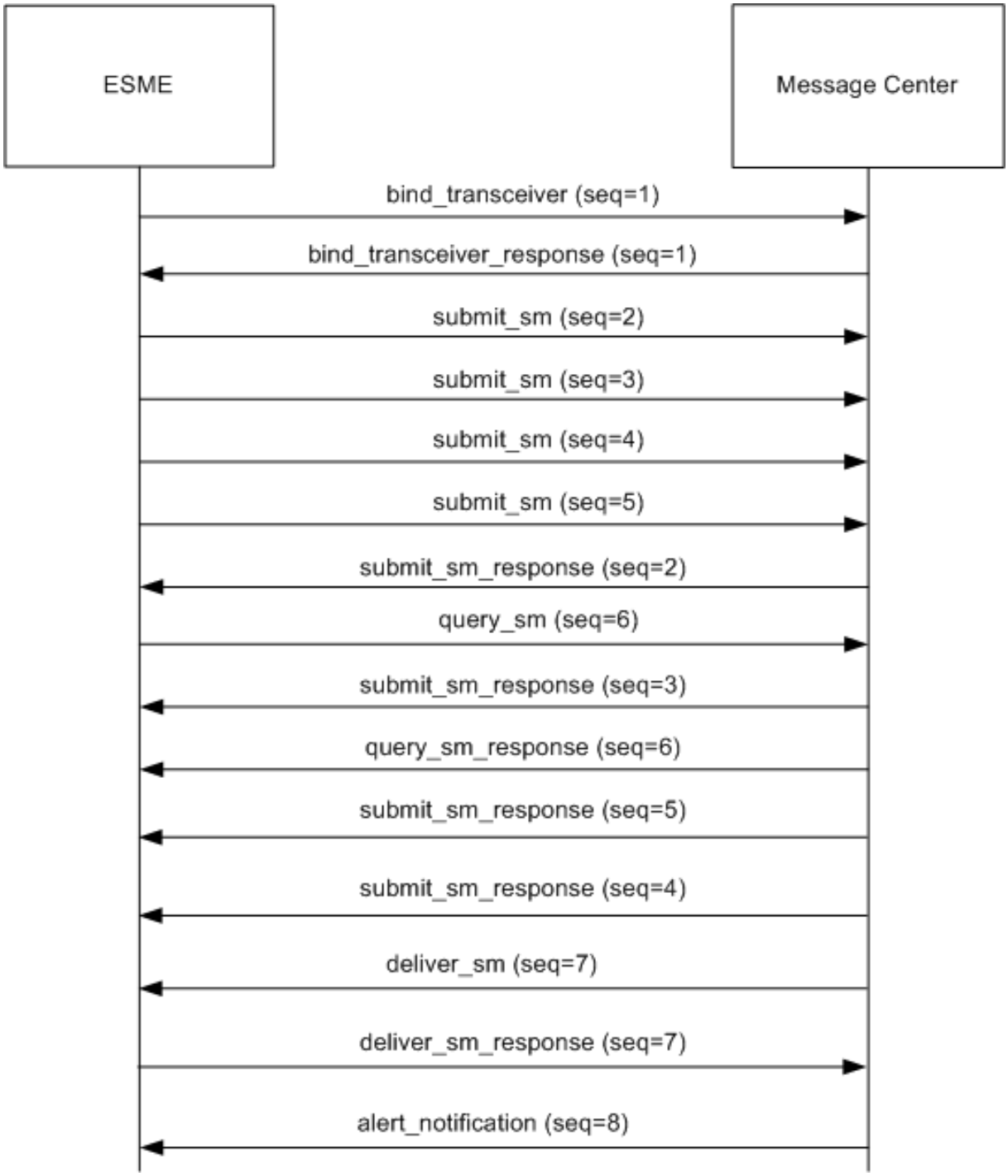
Nachdem die Verbindung hergestellt wurde, kann die ESME, je nachdem, in welchem Modus sie an den MC gebunden ist, eine submit_sm- oder data_sm-Nachricht senden, eine deliver_sm- oder data_sm-Nachricht empfangen oder jede dieser Arten von Nachrichten senden und empfangen. Die ESME kann auch Zusatznachrichten wie query_sm, replace_sm und cancel_sm senden, um den Status einer früheren Nachrichtenzustellung abzufragen, eine frühere Nachricht durch eine neue Nachricht zu ersetzen oder eine nicht zugestellte Nachricht zu stornieren.

Wenn eine Nachricht nicht zugestellt wird, weil kein ESME verfügbar ist oder ein Mobilfunkabonnent

nicht online ist, wird die Nachricht in die Warteschlange gestellt. Später, wenn der MC feststellt, dass der mobile Teilnehmer jetzt erreichbar ist, sendet er über eine Empfänger- oder Transceiver-Sitzung eine alert_notification-PDU an die ESME und fordert die Zustellung aller Nachrichten in der Warteschlange an.

Jede Anforderungs-PDU hat eine eindeutige Sequenznummer. Die Antwort-PDU hat dieselbe Sequenznummer wie die ursprüngliche Anfrage. Da der Nachrichtenaustausch über SMPP im asynchronen Modus erfolgen kann, kann eine ESME oder ein MC mehrere Anfragen gleichzeitig senden. Die Sequenznummer spielt eine entscheidende Rolle bei der Rückgabe der Antwort in derselben SMPP-Sitzung. Mit anderen Worten, die Sequenznummer ermöglicht den Abgleich von Anfrage und Antwort.

Das folgende Diagramm zeigt, wie der Verkehrsfluss die verschiedenen PDUs verwendet, wenn der ESME als Transceiver bindet.



Einschränkung:

Die NetScaler Appliance unterstützt keine ausgehenden Vorgänge. Das heißt, ein Nachrichtencenter kann keine SMPP-Sitzung mit einer ESME über die NetScaler Appliance initiieren.

So funktioniert SMPP Load Balancing auf dem NetScaler

Ein ESME (Client) sendet eine Bindungsnachricht, um eine Verbindung zum NetScaler herzustellen. Der ADC authentifiziert jede ESME und antwortet bei Erfolg mit einer entsprechenden Meldung. Der NetScaler stellt eine Verbindung mit jedem Message Center her und verteilt die Last aller Nachrichten auf diese Message Centers. Wenn der ADC eine Nachricht von einem Client empfängt, verwendet er eine offene Verbindung zum Message Center erneut oder sendet eine Bindungsanforderung an ein Message Center, wenn keine offene Verbindung verfügbar ist.

Der ADC kann Load-Balance-Nachrichten, die von den Clients und von den Servern stammen, ausgleichen. Es kann den Zustand der Nachrichtenzentren überwachen und verkettete Nachrichten verarbeiten. Es bietet auch Unterstützung für das Content Switching für die Nachrichtenzentren.

Nachrichten, die von den eSMEs stammen

Jeder ESME muss zur Authentifizierung als Benutzer auf dem NetScaler hinzugefügt werden. Der Client stellt eine TCP-Verbindung mit einem virtuellen SMPP-Server her, der auf dem ADC konfiguriert ist, indem er eine Bindungsanforderung sendet. Der ADC authentifiziert den Client und analysiert, falls dies erfolgreich ist, die Bindungsnachricht. Der ADC sendet dann die Anfrage an das Message Center, das mit der konfigurierten Load-Balancing-Methode ausgewählt wurde. Wenn eine Verbindung zum Message Center nicht zur Wiederverwendung verfügbar ist, öffnet der ADC eine TCP-Verbindung mit dem Message Center, indem er eine neue Bindungsanforderung an das Message Center sendet.

Bevor die Antwort (submit_sm_resp oder data_sm_resp) vom Message Center an den Client weitergeleitet wird, fügt der ADC der Nachrichten-ID eine benutzerdefinierte Server-ID hinzu, um das Message Center für Nebenvorgänge wie Abfragen, Ersetzen oder Stornieren von Anfragen für eine Nachricht durch den Client zu identifizieren. Anfragen von anderen Clients werden auf die gleiche Weise ausbalanciert.

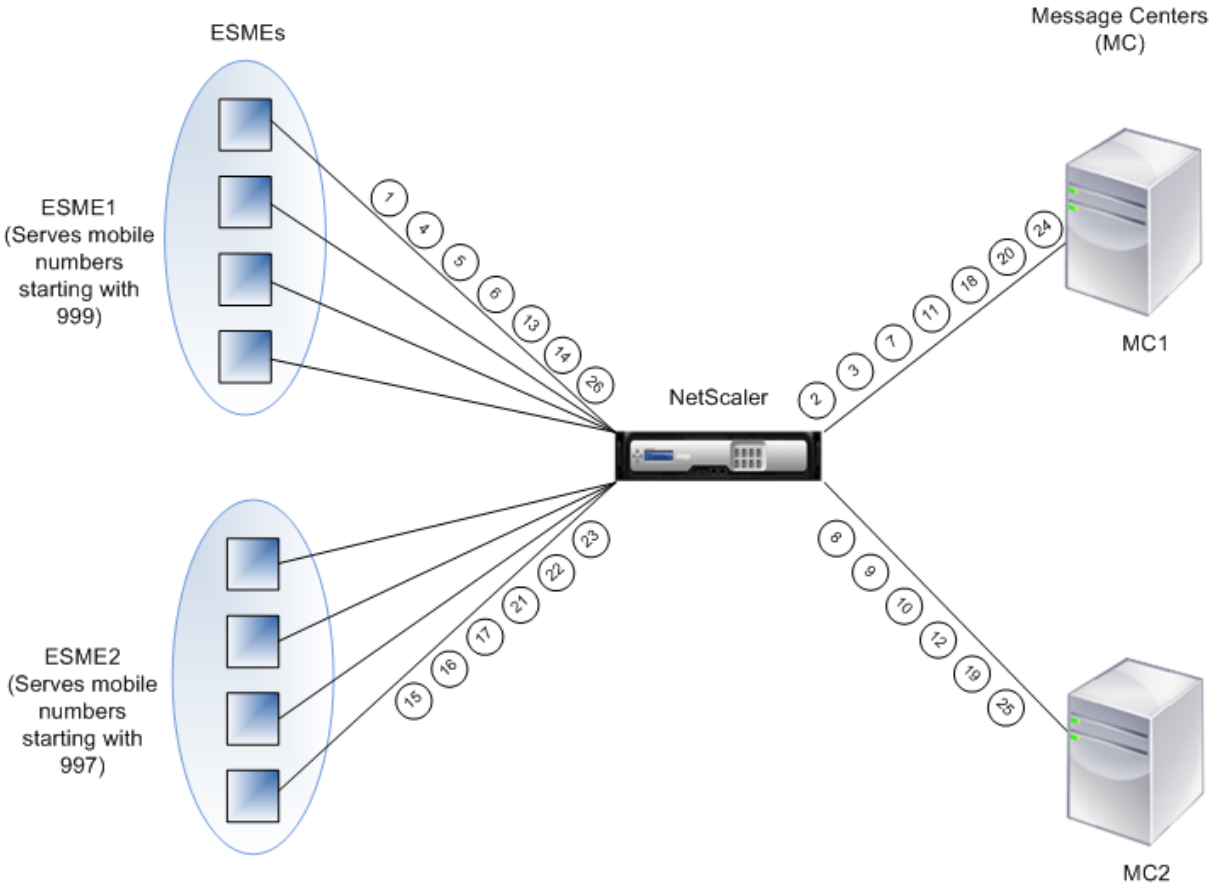
In der ursprünglichen Bindungsanforderung gibt ein Client den Adressbereich an, den er bedienen kann. Dieser Bereich wird für die Weiterleitung von deliver_sm- oder data_sm-Nachrichten von den Message Centern an die Clients verwendet.

Nachrichten, die aus einem Message Center stammen

ESMEs, die einen bestimmten Adressbereich verwalten können, werden zu einem Cluster zusammengefasst. Alle Knoten in einem Cluster bieten dieselben Anmeldeinformationen. Innerhalb eines Clusters wird nur die Round-Robin-Methode für den Lastenausgleich verwendet. Um von Mobilgeräten ausgehende Nachrichten (MO) zuzustellen, sendet das Message Center eine deliver_sm-Nachricht an den NetScaler. Wenn ein Cluster, der den Zieladressbereich bedienen kann (z. B. Zahlen, die mit 998 beginnen), an den ADC gebunden ist, wählt er diesen Cluster aus und verteilt dann die Nachricht auf die ESME-Knoten in diesem Cluster.

Wenn eine ESME, die deliver_sm-Nachrichten für den Adressbereich bereitstellen kann, nicht an den ADC gebunden ist und Message Queuing aktiviert ist, wird die Nachricht in die Warteschlange gestellt, bis ein solcher Client in einem Empfänger- oder Transceivermodus eine Verbindung zum ADC herstellt. Sie können die Größe der Warteschlange angeben.

Das folgende Diagramm veranschaulicht den internen Fluss von PDUs zwischen eSMEs, NetScaler und den Message Centern. Der Einfachheit halber werden nur zwei ESMEs und zwei Message Center angezeigt.



Nachrichtenfluss (PDUs):

1. ESME1 sendet eine Bindungsanforderung an NetScaler
2. NetScaler sendet eine Bindungsanforderung an MC1
3. MC1 sendet eine Bindungsantwort an NetScaler
4. NetScaler sendet eine Bindungsantwort an ESME1
5. ESME1 sendet submit_sm (1) an NetScaler
6. ESME1 sendet submit_sm (2) an NetScaler
7. NetScaler leitet submit_sm (1) an MC1 weiter
8. NetScaler sendet eine Bindungsanforderung an MC2
9. MC2 sendet eine Bindungsantwort an NetScaler
10. NetScaler leitet submit_sm (2) an MC2 weiter

11. MC1 sendet submit_sm_resp (1) an NetScaler
12. MC2 sendet submit_sm_resp (2) an NetScaler
13. NetScaler leitet submit_sm_resp (1) an ESME1 weiter
14. NetScaler leitet submit_sm_resp (2) an ESME1 weiter
15. ESME2 sendet eine Bindungsanforderung an NetScaler
16. NetScaler sendet eine Bindungsantwort an ESME2
17. ESME2 sendet submit_sm (3) an NetScaler
18. NetScaler leitet submit_sm (3) an MC1 weiter
19. MC2 sendet deliver_sm an NetScaler (ESME2 bedient den in der Nachricht angegebenen Adressbereich)
20. MC1 sendet submit_sm_resp (3) an NetScaler
21. NetScaler leitet submit_sm_resp (3) an ESME2 weiter
22. NetScaler leitet deliver_sm an ESME2 weiter
23. ESME2 sendet deliver_sm_resp an NetScaler
24. MC1 sendet alert_notification an NetScaler (ESME1 bedient den in der Nachricht angegebenen Adressbereich)
25. NetScaler leitet deliver_sm_resp an MC2 weiter
26. NetScaler leitet die alert_notification an ESME1 weiter

Gesundheitsüberwachung von Nachrichtenzentren

Standardmäßig ist ein TCP_Default-Monitor an einen SMPP-Dienst gebunden, Sie können jedoch einen benutzerdefinierten Monitor vom Typ SMPP binden. Der benutzerdefinierte Monitor öffnet eine TCP-Verbindung zum Message Center und sendet ein enquire_link-Paket. Je nach Erfolg oder Misserfolg der Sonde wird der Dienst mit UP oder DOWN markiert.

Umschalten von Inhalten in Message Centern

Message Center können mehrere Verbindungen von ESMEs akzeptieren (oder Anfragen binden). Sie können den NetScaler so konfigurieren, dass diese Anforderungen basierend auf den SMPP-Bind-Parametern mit Inhalt wechselt. Im Folgenden finden Sie einige allgemeine Ausdrücke zum Konfigurieren von Methoden zum Auswählen eines Nachrichtenzentrums:

- Basierend auf dem Adressbereich: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtenzentrum aus, wenn der Adressbereich bei 988 beginnt.

Beispiel:

SMPP.BINDINFO.ADDRESS_RANGE.CONTAINS(“^988”)

- Basierend auf der ESME-ID: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Message Center aus, wenn die ESME-ID ESME1 entspricht.

Beispiel:

SMPP.BINDINFO.SYSTEM_ID.EQ („ESME1”)

- Basierend auf dem ESME-Typ: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Message Center aus, wenn der ESME-Typ VMS ist. VMS steht für Voicemail-System.

Beispiel:

SMPP.BINDINFO.SYSTEM_TYPE.EQ („VIRTUELLE RECHNER“)

- Basierend auf dem Nummerntyp (TON) der ESME: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtenzentrum aus, wenn TON gleich 1 ist (1 steht für eine internationale Zahl).

Beispiel:

SMPP.BINDINFO.ADDR_TON.EQ (1)

- Basierend auf dem Number Plan Indicator (NPI) der ESME: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtenzentrum aus, wenn NPI gleich 0 ist (0 steht für eine unbekannte Verbindung).

Beispiel:

SMPP.BINDINFO.ADDR_NPI.EQ (0)

- Basierend auf dem Bindungstyp: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtenzentrum aus, wenn der Bindungstyp TRANSCEIVER ist. (Ein Transceiver kann Nachrichten senden und empfangen.)

Beispiel:

SMPP.BINDINFO.TYPE.EQ (TRANSCEIVER)

Behandlung verketteter Nachrichten

Eine SMS kann maximal 140 Byte enthalten. Längere Nachrichten müssen in kleinere Teile aufgeteilt werden. Wenn das Zielhandy dazu in der Lage ist, werden die Nachrichten kombiniert und als eine lange SMS zugestellt. Der NetScaler leitet die Fragmente einer Nachricht an dasselbe Message Center weiter. Jede Nachricht enthält eine Referenznummer, eine Sequenznummer und die Gesamtzahl der Fragmente. Die Referenznummer ist für jedes Fragment einer langen Nachricht dieselbe. Die Sequenznummer gibt die Position des bestimmten Fragments in der vollständigen Nachricht an. Nachdem alle Fragmente empfangen wurden, fasst die ESME die Fragmente zu einer langen Nachricht zusammen und übermittelt die Nachricht an den mobilen Abonnenten.

Wenn ein Client die Verbindung zu einer aktiven Verbindung trennt, wird die Verbindung zum Message Center nicht geschlossen. Es wird für Anfragen von anderen Kunden wiederverwendet.

Einschränkung

Nachrichten-IDs aus dem Message Center, die länger als 59 Byte sind, werden nicht unterstützt. Wenn die vom Message Center zurückgegebene Nachrichten-ID-Länge mehr als 59 Byte beträgt, schlagen zusätzliche Operationen fehl und der NetScaler reagiert mit einer Fehlermeldung.

Konfiguration des SMPP-Load-Balancings auf dem NetScaler

Führen Sie die folgenden Aufgaben aus, um den SMPP-Lastenausgleich auf dem ADC zu konfigurieren:

1. Fügen Sie einen SMPP-Benutzer hinzu. Der ADC authentifiziert den Benutzer, bevor er eine Bindungsanforderung des Benutzers akzeptiert. Der Benutzer ist in der Regel ein ESME.
2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu und geben Sie das Protokoll als SMPP an.
3. Fügen Sie einen Dienst hinzu, indem Sie das Protokoll als SMPP und eine benutzerdefinierte Server-ID angeben, die für jeden Server eindeutig ist. Binden Sie den Dienst an den zuvor erstellten virtuellen Load-Balancing-Server.
4. Erstellen Sie optional eine Dienstgruppe und fügen Sie der Dienstgruppe Dienste hinzu.
5. Fügen Sie optional einen Monitor vom Typ SMPP-ECV hinzu und binden Sie ihn an den Dienst. Ein TCP-Standardmonitor ist standardmäßig gebunden.
6. Stellen Sie die SMPP-Parameter wie den Client-Modus und die Nachrichtenwarteschlange ein.

So konfigurieren Sie den SMPP-Lastenausgleich mithilfe der Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
add smpp user <username> -password <password>
add service <name> <IP> SMPP <port>  - customserverID <customserverID>
add lb vserver <name> <IP> SMPP <port>
bind lb vserver <name> <service name>
set smpp param
<!--NeedCopy-->
```

Beispiel

```
add smpp user smppclient1 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add smpp user smppclient2 -password c03ebb540695b6110eb31172f32245a1 -
    encrypted -encryptmethod ENCMTHD_2
add service smmpsvc 10.102.84.140 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID ab -CKA NO -TCPB NO -CMP NO
```



```
add service smmpsvc2 10.102.81.175 SMPP 2775 -gslb NONE -maxClient 0 -
    maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
     180 -svrTimeout 360 -CustomServerID xy -CKA NO -TCPB NO -CMP NO
add lb vserver smppvs SMPP 10.102.239.179 2775 -persistenceType NONE -
    cltTimeout 180
bind lb vserver smppvs smmpsvc2
bind lb vserver smppvs smmpsvc
set smpp param -addrrange "d*"
<!--NeedCopy-->
```

So konfigurieren Sie den SMPP-Lastenausgleich mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **System > Benutzerverwaltung > SMPP-Benutzer**, und fügen Sie einen SMPP-Benutzer hinzu.
2. Navigieren Sie zu **Traffic Management > Load Balancing > SMPP-Parameter konfigurieren**, und legen Sie die für Ihre Bereitstellung erforderlichen Parameter fest.
3. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und fügen Sie einen virtuellen Server vom Typ SMPP hinzu.
4. Klicken Sie im Abschnitt Dienst, fügen Sie einen Dienst vom Typ SMPP hinzu, und geben Sie eine Server-ID an.

Anwendungsfall 2: Regelbasierten Persistenz basierend auf einem Name-Wert-Paar in einem TCP-Byte-Stream konfigurieren

May 11, 2023

Einige Protokolle übertragen Name-Wert-Paare in einem TCP-Bytestream. Das Protokoll im TCP-Bytestream in diesem Beispiel ist das FIX-Protokoll (Financial Information eXchange). In der Nicht-XML-Implementierung ermöglicht das FIX-Protokoll zwei Hosts, die über ein Netzwerk kommunizieren, geschäftliche oder handelsbezogene Informationen als Liste von Name-Wert-Paaren (genannt “FIX-Felder”) auszutauschen. Das Feldformat ist<tag>=<value><delimiter>. Dieses traditionelle Tag-Value-Format macht das FIX-Protokoll ideal für diesen Anwendungsfall.

Das Tag in einem FIX-Feld ist ein numerischer Bezeichner, der die Bedeutung des Feldes angibt. Im Beispiel;

- Das Tag 35 gibt den Nachrichtentyp an.
- Der Wert nach dem Gleichheitszeichen hat eine bestimmte Bedeutung für das angegebene Tag und ist einem Datentyp zugeordnet. Der Wert A für das Tag 35 gibt an, dass es sich bei der Nachricht um eine Anmeldenachricht handelt.

- Das Trennzeichen ist das nicht druckende Start of Header (SOH) ASCII-Zeichen (0x01), welches das Caret-Symbol (^) ist.
- Jedem Feld wird außerdem ein Name zugewiesen. Das Feld mit Tag 35 ist das MsgType-Feld.

Es folgt ein Beispiel für eine Anmeldemeldung.

8=FIX.4.1 9=61 35=A 49=INVMGR 56=BRKR 34=1 52= 20000426-12:05:06 98=0 108=30 10=157

Ihre Wahl des Persistenztyps für eine Tag-Werteliste wie die oben gezeigte hängt von den Optionen ab, die Ihnen zum Extrahieren einer bestimmten Zeichenfolge aus der Liste zur Verfügung stehen. Token-basierte Persistenzmethoden erfordern, dass Sie den Offset und die Länge des Tokens angeben, das Sie aus der Nutzlast extrahieren möchten. Das FIX-Protokoll erlaubt dies nicht, da der Offset eines bestimmten Feldes und die Länge seines Wertes von Nachricht zu Nachricht variieren können. Diese Variation hängt vom Nachrichtentyp, den vorhergehenden Feldern und den Längen der vorhergehenden Werte ab. Es variiert auch je nach Implementierung von einer zur anderen, je nachdem, ob benutzerdefinierte Felder definiert wurden. Solche Variationen machen es unmöglich, den exakten Versatz eines bestimmten Feldes vorherzusagen oder die Länge des Wertes anzugeben, der als Token extrahiert werden soll. In diesem Fall ist die regelbasierte Persistenz der bevorzugte Persistenztyp.

Angenommen, ein virtueller Server fixlb1 ermöglicht den Lastenausgleich TCP-Verbindungen zu einer Farm von Servern, die Instanzen einer Fix-fähigen Anwendung hosten. Sie möchten die Persistenz für Verbindungen auf der Grundlage des Wertes des SenderCompid-Feldes konfigurieren, in dem das Unternehmen identifiziert wird, das die Nachricht sendet. Das Tag für dieses FIX-Feld ist 49 (im Beispiel der früheren Anmeldemeldung angezeigt).

Um die regelbasierte Persistenz für den virtuellen Lastausgleichsserver zu konfigurieren, legen Sie den Persistenztyp für den virtuellen Lastausgleichsserver auf RULE fest und konfigurieren Sie den Regelparameter mit einem Ausdruck. Bei dem Ausdruck muss es sich um einen Ausdruck handeln, der den Teil der TCP-Payload extrahiert, in dem Sie das senderCompID-Feld erwarten, die resultierende Zeichenfolge anhand der Trennzeichen typisiert und dann den Wert des SenderCompID-Felds (Tag 49) wie folgt extrahiert:

```
set lb vserver fixlb1 -persistenceType RULE -rule "CLIENT.TCP.PAYLOAD(300).
TYPECAST_NVLIST_T('=','^').VALUE("\49\")"
```

Hinweis: In dem Ausdruck wurden Backslash-Zeichen verwendet, da es sich um einen CLI-Befehl handelt. Wenn Sie das Konfigurationsprogramm verwenden, geben Sie die umgekehrten Schrägstriche nicht ein.

Wenn der Client eine FIX-Nachricht sendet, die die Namenwerteliste im Beispiel einer früheren Anmeldemeldung enthält, extrahiert der Ausdruck den Wert INVMGR, und die NetScaler-Appliance erstellt eine Persistenzsitzung, die auf diesem Wert basiert.

Das Argument für die Funktion PAYLOAD () kann so groß sein, wie Sie es für notwendig halten, um das Feld SenderCompid in die von der Funktion extrahierte Zeichenfolge aufzunehmen. Optional

können Sie die Funktion SET_TEXT_MODE (IGNORECASE) verwenden, wenn die Appliance den Fall ignoriert, wenn Sie den Wert des Felds extrahieren, und die HASH-Funktion zum Erstellen einer Persistenzsitzung basierend auf einem Hash des extrahierten Wertes. Der folgende Ausdruck verwendet die Funktionen SET_TEXT_MODE (IGNORECASE) und HASH:

```
CLIENT.TCP.PAYLOAD(500).TYPECAST_NVLIST_T('=','^').SET_TEXT_MODE(IGNORECASE
).VALUE("49").HASH
```

Im Folgenden finden Sie weitere Beispiele für Regeln, die Sie verwenden können, um die Persistenz für FIX-Verbindungen zu konfigurieren (<tag> ersetzen Sie sie durch das Tag des Felds, dessen Wert Sie extrahieren möchten):

- Um den Wert eines beliebigen FIX-Feldes in den ersten 300 Byte der TCP-Payload zu extrahieren, können Sie den Ausdruck CLIENT.TCP.PAYLOAD (300) .BEFORE_STR („^“) .AFTER_STR (“ =“) verwenden.<tag>
- Verwenden Sie den Ausdruck CLIENT.TCP.PAYLOAD (100) .SUBSTR (80,20) .TYPECAST_NVLIST_T (‘=’, ‘^’) .VALUE (“ „), um eine Zeichenfolge zu extrahieren, die bei Offset 80 20 Byte lang ist, die Zeichenfolge in eine Name-Wert-Liste umzuwandeln und dann den Wert des gewünschten Felds zu extrahieren.<tag>
- Verwenden Sie den Ausdruck CLIENT.TCP.PAYLOAD (100) .TYPECAST_NVLIST_T (‘=’, ‘^’) .VALUE (“ „,2), um die ersten 100 Byte der TCP-Payload zu extrahieren, die Zeichenfolge in eine Name-Wert-Liste umzuwandeln und den Wert des dritten Vorkommens des gewünschten Felds zu extrahieren.<tag>
  Hinweis: Wenn das zweite Argument, das an die
  VALUE () -Funktion übergeben wird,
  n ist, extrahiert die Appliance den Wert der
  (n+1)
  th -Instanz des Felds, da die Zählung bei Null (
  0) beginnt.

Im Folgenden finden Sie weitere Beispiele für Regeln, mit denen Sie die Persistenz konfigurieren können. Nur die nutzungsbasierten Ausdrücke können Daten auswerten, die über das FIX-Protokoll übertragen werden. Die anderen Ausdrücke sind allgemeinere Ausdrücke für die Konfiguration der Persistenz auf der Grundlage niedrigerer Netzwerkprotokolle.

- CLIENT.TCP.PAYLOAD (100)
- CLIENT.TCP.PAYLOAD (100) .HASH
- CLIENT.TCP.PAYLOAD (100) .SUBSTR (5,10)
- CLIENT.TCP.SRCPORT
- CLIENT.TCP.DSTPORT
- CLIENT.IP.SRC
- CLIENT.IP.DST
- CLIENT.IP.SRC.GET4

- CLIENT.IP.DST.GET4
- CLIENT.ETHER.SRCMAC.GET6
- CLIENT.ETHER.DSTMAC.GET5
- CLIENT.VLAN.ID

Anwendungsfall 3: Lastausgleich im DSR-Modus konfigurieren

May 11, 2023

Der Lastausgleich im DSR-Modus (Direct Server Return) ermöglicht es dem Server, direkt auf Clients zu antworten, indem er einen Rückpfad verwendet, der nicht durch die NetScaler-Appliance fließt. Im DSR-Modus kann die Appliance jedoch weiterhin Zustandsprüfungen für Dienste durchführen. In einer Umgebung mit hohem Datenvolumen erhöht das direkte Senden von Serverdatenverkehr an den Client im DSR-Modus die gesamte Paketverarbeitungskapazität der Appliance, da die Pakete nicht durch die Appliance fließen.

Der DSR-Modus weist die folgenden Funktionen und Einschränkungen auf:

- Es unterstützt den Einarmmodus und den Inline-Modus.
- Die Appliance altert Sitzungen basierend auf dem Leerlaufzeitlimit aus.
- Da die Appliance keine TCP-Verbindungen proxyiert (dh sie sendet SYN-ACK nicht an den Client), schließt sie SYN-Angriffe nicht aus. Mit dem SYN-Paketratenfilter können Sie die Rate von SYNs für den Server steuern. Um die Rate von SYNs zu steuern, legen Sie einen Schwellenwert für die SYN-Rate fest. Um Schutz vor SYN-Angriffen zu erhalten, müssen Sie die Appliance so konfigurieren, dass sie TCP-Verbindungen als Proxy verwendet. Dies erfordert jedoch, dass der umgekehrte Verkehr durch die Appliance fließt.
- In einer DSR-Konfiguration ersetzt die NetScaler-Appliance die IP-Adresse des virtuellen Lastausgleichsservers nicht durch die IP-Adresse des Zielservers. Stattdessen leitet er Pakete an einen Dienst weiter, indem er die MAC-Adresse des Servers verwendet. Der VIP muss auf dem Server konfiguriert sein und ARP muss für den VIP deaktiviert sein, der auf dem Server konfiguriert ist. Dadurch wird verhindert, dass die Clientanforderung die Appliance umgeht, wenn sie im Einarmmodus konfiguriert ist. Beispielsweise muss ein Benutzer VIP in der Loopback-Schnittstelle konfigurieren und den ARP für denselben VIP deaktivieren.
- Die Appliance ruft die MAC-Adresse des Servers vom Monitor ab, der an den Dienst gebunden ist. Benutzerdefinierte Benutzermonitore (Monitore vom Typ USER), die auf der NetScaler-Appliance gespeicherte Skripts verwenden, lernen jedoch nicht die MAC-Adresse eines Servers. Wenn Sie in einer DSR-Konfiguration nur benutzerdefinierte Monitore verwenden, versucht die Appliance für jede Anforderung, die der virtuelle Server empfängt, die Ziel-IP-Adresse in eine MAC-Adresse aufzulösen (indem sie ARP-Anfragen sendet). Da es sich bei der Ziel-IP-Adresse um eine virtuelle IP-Adresse handelt, die der NetScaler Appliance gehört, werden die ARP-

Anforderungen immer in die MAC-Adresse der NetScaler-Schnittstelle aufgelöst. Daher wird der gesamte vom virtuellen Server empfangene Datenverkehr auf die Appliance zurückgeführt. Wenn Sie Benutzermonitore in einer DSR-Konfiguration verwenden, müssen Sie auch einen anderen Monitor (z. B. einen PING-Monitor) für die Dienste konfigurieren, idealerweise mit einem längeren Intervall zwischen den Prüfpunkten, damit die MAC-Adresse der Server erlernt werden kann.

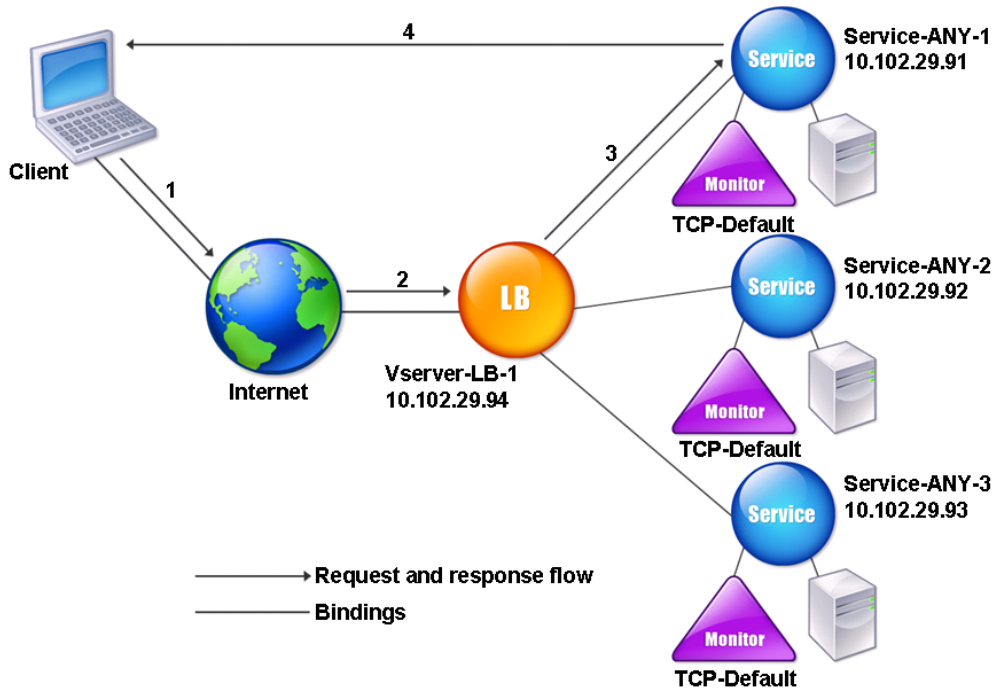
- Die NetScaler-Appliance lernt die Server-L2-Parameter vom Monitor, der an den Dienst gebunden ist. Konfigurieren Sie für UDP-ECV-Monitore eine Empfangszeichenfolge, damit die Appliance die L2-Parameter des Servers lernen kann. Wenn die Empfangszeichenfolge nicht konfiguriert ist und der Server nicht reagiert, lernt die Appliance die L2-Parameter nicht, aber der Dienst ist auf UP eingestellt. Der Traffic für diesen Dienst ist schwarz.

Im Beispielszenario werden die Dienste Service-ANY-1, Service-ANY-2 und Service-ANY-3 erstellt und an den virtuellen Server Vserver-LB-1 gebunden. Der virtuelle Server verteilt die Client-Anfrage an einen Dienst, und der Dienst reagiert direkt auf die Clients, wobei die NetScaler-Appliance umgangen wird. In der folgenden Tabelle sind die Namen und Werte der Entitäten aufgeführt, die auf der NetScaler-Appliance im DSR-Modus konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Monitore	TCP	Ohne	Ohne

Das folgende Diagramm zeigt die Load-Balancing-Entitäten und Werte der Parameter, die auf der Appliance konfiguriert werden sollen.

Abbildung 1. Entitätsmodell für Load Balancing im DSR-Modell



Damit die Appliance im DSR-Modus ordnungsgemäß funktioniert, muss die Ziel-IP in der Client-Anfrage unverändert sein. Stattdessen ändert die Appliance den Ziel-MAC auf den des ausgewählten Servers. Diese Einstellung ermöglicht es dem Server, die Client-MAC-Adresse für die Weiterleitung von Anforderungen an den Client unter Umgehung des Servers zu bestimmen.

Als Nächstes konfigurieren Sie ein grundlegendes Lastenausgleichs-Setup wie unter Einrichten des Basic Load Balancingbeschrieben, benennen die Entitäten und Festlegen der Parameter mit den in der vorherigen Tabelle beschriebenen Werten.

Nachdem Sie das grundlegende Lastausgleichs-Setup konfiguriert haben, müssen Sie es für den DSR-Modus anpassen. Dazu konfigurieren Sie eine unterstützte Lastausgleichsmethode, z. B. die Quell-IP-Hash-Methode mit einem virtuellen Server ohne Sitzung. Sie müssen auch den Umleitungsmodus so einstellen, dass der Server die Client-MAC-Adresse für die Weiterleitung von Antworten ermitteln und die Appliance Bypass kann.

Nachdem Sie die Load Balancing-Methode und den Umleitungsmodus konfiguriert haben, müssen Sie den USIP-Modus für jeden Dienst aktivieren. Der Dienst verwendet dann die Quell-IP-Adresse, um Antworten weiterzuleiten.

So konfigurieren Sie die Load-Balancing-Methode und den Umleitungsmodus für einen virtuellen Server ohne Sitzung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
   RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPHash -m MAC -sessionless
   enabled
<!--NeedCopy-->
```

> **Hinweis**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die MAC-Option -m aktiviert ist, müssen Sie einen Monitor binden, der kein Benutzer ist.

So konfigurieren Sie die Load-Balancing-Methode und den Umleitungsmodus für einen virtuellen Server ohne Sitzung mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server, wählen Sie Umleitungsmodus als MAC-basiert und Methode als SOURCEIPHASH.
3. Wählen Sie unter Traffic Settings Sessionless Load Balancing aus.

So konfigurieren Sie einen Dienst für die Verwendung der Quell-IP-Adresse mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```


So konfigurieren Sie einen Dienst für die Verwendung der Quell-IP-Adresse mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie einen Dienst und wählen Sie unter Verkehrseinstellungen die Option **Quell-IP-Adresse verwenden**aus.

Einige zusätzliche Schritte sind in bestimmten Situationen erforderlich, die in den nachfolgenden Abschnitten beschrieben werden.

Anwendungsfall 4: LINUX-Servern im DSR-Modus konfigurieren

May 11, 2023

Das LINUX-Betriebssystem erfordert, dass Sie auf jedem Lastausgleichsserver im DSR-Cluster eine Loopback-Schnittstelle mit der virtuellen IP-Adresse (VIP) der NetScaler Appliance einrichten.

Um den LINUX-Server im DSR-Modus zu konfigurieren

Um eine Rücklaufschnittstelle mit dem VIP der NetScaler Appliance auf jedem Server mit Lastausgleich zu erstellen, geben Sie an der Eingabeaufforderung des Linux-Betriebssystems die folgenden Befehle ein:

```
ifconfig dummy0 up

ifconfig dummy0:0 inet <netscaler vip> netmask 255.255.255.255 up

echo 1 > /proc/sys/net/ipv4/conf/dummy0/arp_ignore

echo 2 > /proc/sys/net/ipv4/conf/dummy0/arp_announce
<!--NeedCopy-->
```

Führen Sie dann die Software aus, die die TOS-ID neu zu VIP zuordnet.

Hinweis: Fügen Sie der Software die richtigen Zuordnungen hinzu, bevor Sie sie ausführen. In den vorherigen Befehlen verwendet der LINUX-Server dummy0, um eine Verbindung zum Netzwerk herzustellen. Wenn Sie diesen Befehl verwenden, geben Sie den Namen der Schnittstelle ein, die Ihr LINUX-Server für die Verbindung mit dem Netzwerk verwendet.

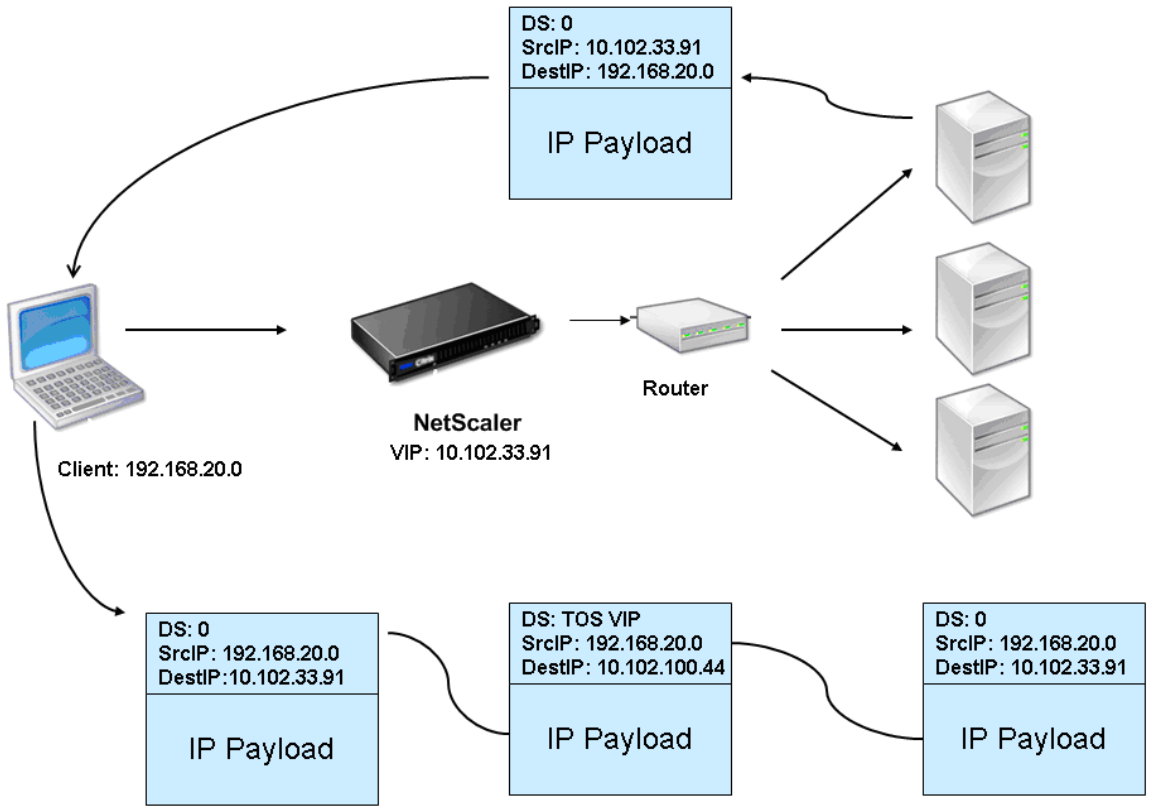
Anwendungsfall 5: DSR-Modus beim Verwenden von TOS konfigurieren

May 11, 2023

Differentiated Services (DS), auch bekannt als TOS (Type of Service), ist ein Feld, das Teil des IPv4-Paket-Headers ist. Das entsprechende Feld im IPv6-Header ist Traffic Class. TOS wird von Protokollen der oberen Layer verwendet, um den Pfad für ein Paket zu optimieren. Die TOS-Informationen kodieren die virtuelle IP-Adresse (VIP) der NetScaler-Appliance, und die Load Balancing-Server extrahieren die VIP daraus.

Im folgenden Szenario fügt die Appliance den VIP zum **TOS-Feld** im Paket hinzu und leitet das Paket dann an den Load Balancing-Server weiter. Der Load Balancing-Server reagiert dann direkt auf den Client und umgeht dabei die Appliance, wie in der folgenden Abbildung dargestellt.

Abbildung 1. Die NetScaler Appliance im DSR-Modus mit TOS



Die TOS-Funktion ist wie folgt für eine kontrollierte Umgebung angepasst:

- In der Umgebung dürfen sich im Pfad zwischen der Appliance und den Servern mit Lastausgleich keine Geräte befinden, die den Status des Zustands beeinflussen, wie z. B. Stateful-Firewalls und TCP-Gateways.

- Router an allen Eintrittspunkten zum Netzwerk müssen das TOS-Feld aus allen eingehenden Paketen entfernen, um sicherzustellen, dass der Load Balancing-Server kein anderes TOS-Feld mit dem von der Appliance hinzugefügten verwechselt.
- Jeder Server kann nur 63 VIPs haben.
- Der Zwischenrouter darf keine ICMP-Fehlermeldungen bezüglich Fragmentierung versenden. Der Client versteht die Nachricht nicht, da die Quell-IP-Adresse die IP-Adresse des Load Balancing-Servers und nicht des NetScaler VIP ist.
- Die Nutzungsbedingungen gelten nur für IP-basierte Dienste. Sie können mit TOS keine auf Domainnamen basierenden Dienste verwenden.

Im Beispiel wird Service-ANY-1 erstellt und an den virtuellen Server vServer-LB-1 gebunden. Der virtuelle Server verteilt die Client-Anfrage an den Dienst, und der Dienst reagiert direkt auf die Clients und umgeht dabei die Appliance. In der folgenden Tabelle sind die Namen und Werte der Entitäten aufgeführt, die auf der Appliance im DSR-Modus konfiguriert sind.

Typ der Entität	Name	IP-Adresse	Protokoll
Virtueller Server	Vserver-LB-1	10.102.33.91	ANY
Services	Service-ANY-1	10.102.100.44	ANY
Monitore	PING	Ohne	Ohne

DSR mit TOS erfordert, dass der Lastenausgleich auf Schicht 3 eingerichtet ist. Informationen zum Konfigurieren eines grundlegenden Load Balancing-Setups für Layer 3 finden Sie unter Einrichten des Basic Load Balancing. Benennen Sie die Entitäten und legen Sie die Parameter anhand der in der vorherigen Tabelle beschriebenen Werte fest.

Nachdem Sie das Load-Balancing-Setup konfiguriert haben, müssen Sie das Load-Balancing-Setup für den DSR-Modus anpassen, indem Sie den Umleitungsmodus so konfigurieren, dass der Server das Datenpaket dekapseln und dann direkt auf den Client antworten und die Appliance Bypass kann.

Nachdem Sie den Umleitungsmodus angegeben haben, können Sie die Appliance optional aktivieren, um den Server transparent zu überwachen. Dadurch kann die Appliance die Server mit Lastausgleich transparent überwachen.

So konfigurieren Sie den Umleitungsmodus für den virtuellen Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <vServerName> -m <Value> -tosId <Value>
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver Vserver-LB-1 -m TOS -tosId 3
<!--NeedCopy-->
```

So konfigurieren Sie den Umleitungsmodus für den virtuellen Server mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und wählen Sie im Umleitungsmodus die TOS-ID aus.

So konfigurieren Sie den transparenten Monitor für TOS mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add monitor <MonitorName> <Type> -destip <DestinationIP> -tos <Value> -
    tosId <Value>
<!--NeedCopy-->
```

Beispiel:

```
add monitor mon1 PING -destip 10.102.33.91 -tos Yes  -tosId 3
<!--NeedCopy-->
```

So erstellen Sie den transparenten Monitor für TOS mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor, wählen Sie TOS aus und geben Sie die TOS-ID ein, die Sie für den virtuellen Server angegeben haben.

Wildcard-TOS-Monitore

Bei einer Lastausgleichskonfiguration im DSR-Modus mit dem TOS-Feld muss für die Überwachung der Dienste ein TOS-Monitor erstellt und an diese Dienste gebunden werden. Für jede Lastenausgleichskonfiguration im DSR-Modus unter Verwendung des TOS-Feldes ist ein separater TOS-Monitor erforderlich, da ein TOS-Monitor die VIP-Adresse und die TOS-ID benötigt, um einen kodierten Wert der VIP-Adresse zu erstellen. Der Monitor erstellt Probe-Pakete, in denen das **TOS-Feld** auf den codierten Wert der VIP-Adresse festgelegt ist. Anschließend werden die Testpakete an die Server gesendet, die durch die Dienste einer Load-Balancing-Konfiguration repräsentiert werden.

Bei vielen Load-Balancing-Konfigurationen ist die Erstellung eines separaten benutzerdefinierten TOS-Monitors für jede Konfiguration eine erhebliche, umständliche Aufgabe. Die Verwaltung dieser TOS-Monitore ist ebenfalls eine wichtige Aufgabe. Jetzt können Sie TOS-Monitore mit Platzhaltern erstellen. Erstellen Sie nur einen Wildcard-TOS-Monitor für alle Load-Balancing-Konfigurationen, die dasselbe Protokoll verwenden (z. B. TCP oder UDP).

Ein Wildcard-TOS-Monitor hat die folgenden obligatorischen Einstellungen:

- Typ = <protocol>
- TOS = Ja

Die folgenden Parameter können auf einen Wert gesetzt oder leer gelassen werden:

- Ziel-IP
- Ziel-Port
- TOS-ID

Ein Platzhalter-TOS-Monitor (mit nicht festgelegten Ziel-IP, Ziel-Port und TOS-ID), der an einen DSR-Dienst gebunden ist, erlernt automatisch die TOS-ID und die VIP-Adresse des virtuellen Lastausgleichsservers. Der Monitor erstellt Prüfpakete mit dem TOS-Feld auf die codierte VIP-Adresse und sendet dann die Prüfpakete an den Server, der vom DSR-Dienst dargestellt wird.

So erstellen Sie einen Platzhalter-TOS-Monitor mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> <Type> -tos YES

show lb monitor <monitorName>
<!--NeedCopy-->
```

So binden Sie einen Wildcard-TOS-Monitor mithilfe der CLI an einen Dienst

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb monitor <monitorName> <serviceName>

show lb monitor <monitorName>
<!--NeedCopy-->
```

So erstellen Sie mithilfe der GUI einen TOS-Monitor mit Platzhaltern

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**.
2. Fügen Sie einen Monitor mit den folgenden Parametereinstellungen hinzu:

- Typ = <protocol>
- TOS = JA

Um einen Wildcard-TOS-Monitor mithilfe der GUI an einen Dienst zu binden

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
2. Öffnen Sie einen Dienst und binden Sie einen Wildcard-TOS-Monitor daran.

In der folgenden Beispielkonfiguration handelt es sich bei V1, V2 und V3 um virtuelle Lastausgleichsserver des Typs ANY, deren TOS-ID jeweils auf 1, 2 und 3 festgelegt ist. S1, S2, S3, S4 und S5 sind Dienste des Typs ANY. S1 und S2 sind sowohl an V1 als auch an V2 gebunden. S3, S4 und S5 und sind sowohl an V1 als auch an V3 gebunden. WLCD-TOS-MON ist ein Wildcard-TOS-Monitor vom Typ TCP und ist an S1, S2, S3, S4 und S5 gebunden.

WLCD-TOS-MON lernt automatisch die TOD-ID und die VIP-Adresse von virtuellen Servern, die an S1, S2, S3, S4 und S5 gebunden sind.

Da S1 an V1 und V2 gebunden ist, erstellt WLCD-TOS-MON zwei Arten von Prüfpaketen für S1, eines mit dem **TOS-Feld** auf die codierte VIP-Adresse (203.0.113.1) von V1 und das andere mit der VIP-Adresse (203.0.113.2) von V2. Der NetScaler sendet diese Prüfpakete dann an den durch S1 dargestellten Server. In ähnlicher Weise erstellt WLCD-TOS-MON Testpakete für S2, S3, S4 und S5.

```
add lb monitor WLCD-TOS-MON  TCP -tos YES

Done

add lb vserver V1 ANY 203.0.113.1 * -m TOS  - tosID 1

Done

add lb vserver V2 ANY 203.0.113.2 * -m TOS  - tosID 2

Done

add lb vserver V3 ANY 203.0.113.3 * -m TOS  - tosID 3

Done

add service S1 198.51.100.1 ANY *

Done

add service S2 198.51.100.2 ANY *

Done
```



```
24
25 add service S3 198.51.100.3 ANY *
26
27 Done
28
29 add service S4 198.51.100.4 ANY *
30
31 Done
32
33 add service S5 198.51.100.5 ANY *
34
35 Done
36
37 bind lb monitor WLCD-TOS-MON S1
38
39 Done
40
41 bind lb monitor WLCD-TOS-MON S2
42
43 Done
44
45 bind lb monitor WLCD-TOS-MON S3
46
47 Done
48
49 bind lb monitor WLCD-TOS-MON S4
50
51 Done
52
53 bind lb monitor WLCD-TOS-MON S5
54
55 Done
56
57 bind lb vserver V1 S1, S2, S3, S4, S5
58
59 Done
60
61 bind lb vserver V2, S1, S2
62
63 Done
64
65 bind lb vserver V3 S3, S4, S5
66
67 Done
68 <!--NeedCopy-->
```


Anwendungsfall 6: Lastausgleich im DSR-Modus für IPv6-Netzwerke mit dem TOS-Feld konfigurieren

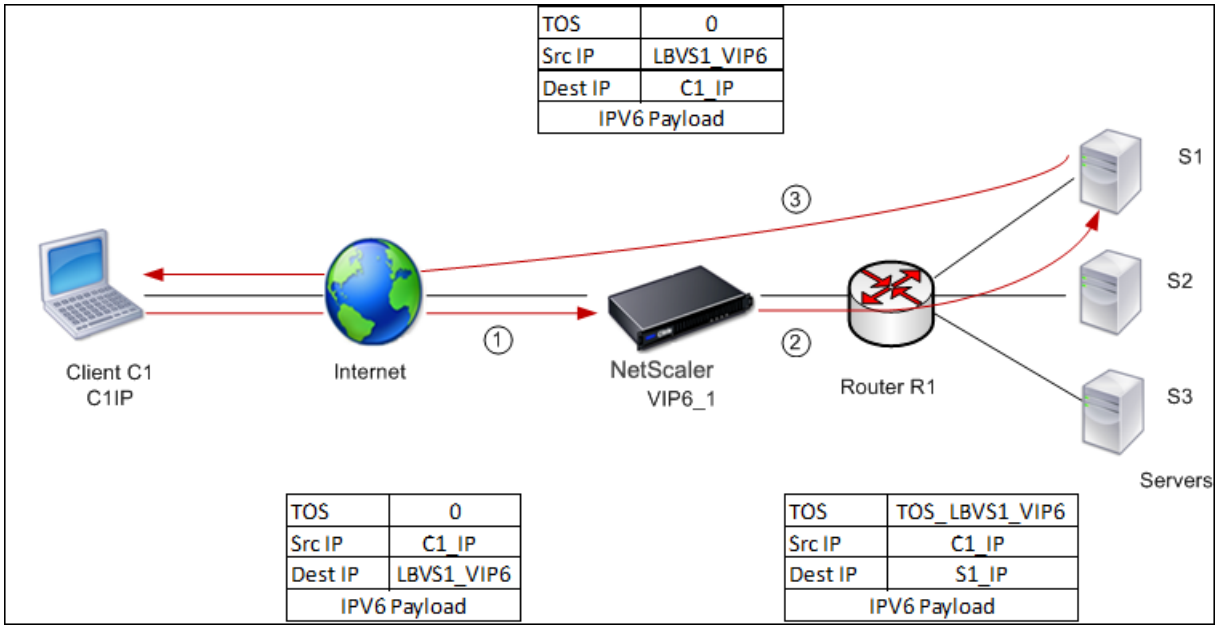
May 11, 2023

Sie können den Lastausgleich im Direct Server Return (DSR) -Modus für IPv6-Netzwerke konfigurieren, indem Sie das Feld Type of Service (TOS) verwenden, wenn sich die NetScaler-Appliance und die Server in unterschiedlichen Netzwerken befinden.

Hinweis: Das TOS-Feld wird auch als Feld Traffic Class bezeichnet.

Wenn ein Client im DSR-Modus eine Anfrage an eine VIP6-Adresse auf einer NetScaler-Appliance sendet, leitet die Appliance diese Anfrage an den Server weiter, indem sie die IPv6-Zieladresse des Pakets in die IPv6-Adresse des Servers ändert und einen codierten Wert der VIP6-Adresse in das TOS-Feld (auch Verkehrsklasse genannt) des IPv6-Headers festlegt. Sie können den Server so konfigurieren, dass er die Informationen im TOS-Feld verwendet, um die VIP6-Adresse aus dem codierten Wert abzuleiten, der dann als Quell-IP-Adresse in Antwortpaketen verwendet wird. Der Antwortverkehr geht direkt an den Client und umgeht die Appliance.

Stellen Sie sich ein Beispiel vor, bei dem ein virtueller Lastausgleichsserver LBVS1, der auf einer NetScaler-Appliance NS1 konfiguriert ist, zum Lastausgleich des Datenverkehrs zwischen den Servern S1, S2 und S3 verwendet wird. Die NetScaler-Appliance NS1 und die Server S1, S2 und S3 befinden sich in unterschiedlichen Netzwerken, sodass der Router R1 zwischen NS1 und den Servern bereitgestellt wird.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entitäten	Name
IPv6-Adresse des Clients C1	C1_IP (nur zu Referenzzwecken)
Virtueller Lastausgleichsserver auf NS1	LBVS1
IPv6-Adresse von LBVS1	LBVS1_VIP6 (nur zu Referenzzwecken)
TOS-Wert	TOS_LBVS1_VIP6 (nur zu Referenzzwecken)
Service für Server S1 auf NS1	SVC_S1
IPv6-Adresse für Server S1	S1_IP (nur zu Referenzzwecken)
Service für Server S2 auf NS1	SVC_S2
IPv6-Adresse für Server S1	S2_IP (nur zu Referenzzwecken)
Service für Server S3 auf NS1	SVC_S3
IPv6-Adresse für Server S1	S3_IP (nur zu Referenzzwecken)

Im Folgenden sehen Sie den Verkehrsfluss im Beispielszenario:

1. Client C1 sendet eine Anfrage an den virtuellen Server LBVS1.
2. Der Load-Balancing-Algorithmus von LBVS1 wählt den Server S1 aus und die Appliance öffnet eine Verbindung zu S1. NS1 sendet die Anfrage an S1 mit:
   - TOS-Feld auf TOS_LBVS1_VIP6 gesetzt.
   - Quell-IP-Adresse als C1_IP.

3. Der Server S1 verwendet nach Erhalt der Anfrage die Informationen im TOS-Feld, um die LBVS1_VIP6-Adresse abzuleiten, die die IP-Adresse des virtuellen Servers LBVS1 auf NS1 ist. Der Server sendet die Antwort direkt an C1 und umgeht dabei die Appliance mit:
    - Die Quell-IP-Adresse wurde auf die abgeleitete LBVS1_VIP6-Adresse festgelegt, sodass der Client mit dem virtuellen Server LBVS1 auf NS1 und nicht mit Server S1 kommuniziert.

Um den Lastenausgleich im DSR-Modus mithilfe von TOS zu konfigurieren, führen Sie die folgenden Schritte auf der Appliance aus

1. Aktivieren Sie den USIP-Modus global.
2. Fügen Sie die Server als Dienste hinzu.
3. Konfigurieren Sie einen virtuellen Load-Balancing-Server mit einem TOS-Wert.
4. Binden Sie die Dienste an den virtuellen Server.

So konfigurieren Sie den Lastenausgleich im DSR-Modus mithilfe von TOS mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns mode USIP

add service <serviceName> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Wiederholen Sie den vorherigen Befehl so oft wie nötig, um jeden Server als Dienst auf der NetScaler Appliance hinzuzufügen.

```
add lb vserver <name> <serviceType> <ip> <port> -m <redirectionMode> -
    tosId <positive_integer>

bind lb vserver <vserverName> <serviceName>
<!--NeedCopy-->
```

So aktivieren Sie den USIP-Modus mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen > Modi konfigurieren**und wählen Sie **Quell-IP-Adresse verwenden**aus.

So erstellen Sie Dienste mithilfe des Konfigurationsprogramms

Navigieren Sie zu **Traffic Management > Load Balancing > Services**und erstellen Sie einen Dienst.

So erstellen Sie einen virtuellen Lastausgleichsserver und binden Dienste mithilfe des Konfigurationsprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und erstellen Sie einen virtuellen Server.
2. Klicken Sie im Abschnitt Dienst, um einen Dienst an diesen virtuellen Server zu binden.

Anwendungsfall 7: Lastausgleich im DSR-Modus mit IP-over-IP konfigurieren

May 11, 2023

Sie können eine NetScaler-Appliance so konfigurieren, dass sie den Direktserverrückkehrmodus (DSR) über Layer-3-Netzwerke hinweg verwendet, indem Sie IP-Tunneling verwenden, auch als *IP over IP-Konfiguration* bezeichnet. Wie bei Standard-Load Balancing-Konfigurationen für den DSR-Modus können Server direkt auf Clients reagieren, anstatt einen Rückkehrpfad über die NetScaler-Appliance zu verwenden. Dies verbessert die Reaktionszeit und den Durchsatz. Wie im Standard-DSR-Modus überwacht die NetScaler-Appliance die Server und führt Zustandsprüfungen an den Anwendungsports durch.

Bei der IP-over-IP-Konfiguration müssen sich die NetScaler-Appliance und die Server nicht im selben Layer-2-Subnetz befinden. Stattdessen kapselt die NetScaler-Appliance die Pakete, bevor sie an den Zielserver gesendet werden. Nachdem der Zielserver die Pakete empfängt, entkapselt er die Pakete und sendet dann seine Antworten direkt an den Client. Dies wird oft als L3DSR bezeichnet.

So konfigurieren Sie den L3-DSR-Modus auf Ihrer NetScaler-Appliance:

- Erstellen Sie einen virtuellen Lastausgleichsserver. Stellen Sie den Modus auf IPTUNNEL ein und aktivieren Sie das sitzungslose Tracking.
- Erstellen Sie Dienste. Erstellen Sie für jede Back-End-Anwendung einen Dienst und binden Sie die Dienste an den virtuellen Server.
- Konfigurieren Sie für die Entkapselung. Konfigurieren Sie entweder eine NetScaler-Appliance oder einen Back-End-Server als Entkapselungsgerät.

  > Hinweis:
  >
  > Wenn Sie eine NetScaler-Appliance verwenden, ist das Entkapselungs-Setup ein IP-Tunnel zwischen den ADC-Appliances, wobei das Back-End L2DSR zu den realen Servern durchführt.

Konfigurieren eines virtuellen Lastausgleichsservers

Konfigurieren Sie einen virtuellen Server für die Verarbeitung von Anforderungen an Ihre Anwendungen. Weisen Sie den Diensttyp zu, der dem Dienst entspricht, oder verwenden Sie einen Typ ANY für mehrere Dienste.
Stellen Sie die Weiterleitungsmethode auf IPTUNNEL ein und ermöglichen Sie dem virtuellen Server, im sitzungslosen Modus zu arbeiten. Konfigurieren Sie jede Load Balancing-Methode, die Sie verwenden möchten.

So erstellen und konfigurieren Sie einen virtuellen Lastausgleichsserver für IP-über-IP-DSR mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen virtuellen Lastausgleichsserver für IP über IP-DSR zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name> serviceType <serviceType> IPAddress <ip> Port <
    port> -lbMethod <method> -m <ipTunnelTag> -sessionless [ENABLED |
    DISABLED]

show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

Im folgenden Beispiel haben wir die Load Balancing-Methode als SourcePhash gewählt und den sitzungslosen Lastenausgleich konfiguriert.

```
add lb vserver Vserver-LB-1 ANY 1.1.1.80 * -lbMethod SourceIPHash -m
    IPTUNNEL -sessionless ENABLED
<!--NeedCopy-->
```

So erstellen und konfigurieren Sie einen virtuellen Lastausgleichsserver für IP über IP-DSR mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Erstellen Sie einen virtuellen Server und geben Sie den Umleitungsmodus als **IP-Tunnel-basiert**an.

Konfigurieren von Diensten für IP-über-IP-DSR

Konfigurieren Sie nach dem Erstellen Ihres Servers mit Lastausgleich einen Dienst für jede Ihrer Anwendungen. Der Dienst verarbeitet den Datenverkehr von der NetScaler-Appliance zu diesen

Anwendungen und ermöglicht es der NetScaler-Appliance, den Zustand der einzelnen Anwendungen zu überwachen.

Weisen Sie die Dienste zu, um den USIP-Modus zu verwenden, und binden Sie einen Monitor vom Typ IPTUNNEL an den Dienst zur tunnelbasierten Überwachung.

So erstellen und konfigurieren Sie einen Dienst für IP-über-IP-DSR mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Dienst zu erstellen, und erstellen Sie optional einen Monitor und binden Sie ihn an den Dienst:

```
add service <serviceName> <serverName> <serviceType> <port> -usip <usip
    >

add monitor <monitorName> <monitorType> -destip <ip> -iptunnel <
    iptunnel>

bind service <serviceName> -monitorName <monitorName>
<!--NeedCopy-->
```

Beispiel:

Im folgenden Beispiel wird ein Monitor vom Typ IPTUNNEL erstellt.

```
add monitor mon_DSR PING -destip 1.1.1.80 -iptunnel yes
add service svc_DSR01 2.2.2.100 ANY * -usip yes
bind service svc_DSR01 -monitorName mon_DSR
<!--NeedCopy-->
```

Ein alternativer Ansatz zur Vereinfachung des Routing sowohl auf dem Server als auch auf der ADC-Appliance besteht darin, sowohl den ADC als auch den Server so einzurichten, dass sie eine IP aus demselben Subnetz verwenden. Dadurch wird sichergestellt, dass jeder Datenverkehr mit einem Ziel eines Tunnelendpunkts über den Tunnel gesendet wird. Im Beispiel wird 10.0.1.0/30 verwendet.

> **Hinweis:**
>
> Der Zweck des Monitors besteht darin, sicherzustellen, dass der Tunnel aktiv ist, indem der Loopback jedes Servers durch den IP-Tunnel erreicht wird. Wenn der Dienst nicht verfügbar ist, überprüfen Sie, ob das äußere IP-Routing zwischen ADC und Server gut ist. Überprüfen Sie auch, ob die inneren IP-Adressen über den IP-Tunnel erreichbar sind. Auf dem Server sind möglicherweise Routen erforderlich, oder je nach gewählter Implementierung wird PBR zu ADC hinzugefügt.

Beispiel:


```
add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
add netProfile netProfile_DSR -srcIP 10.0.1.2
add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
   YES -netProfile netProfile_DSR
<!--NeedCopy-->
```

So konfigurieren Sie einen Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor und wählen Sie **IP-Tunnel**aus.

So erstellen und konfigurieren Sie einen Dienst für IP-über-IP-DSR mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Erstellen Sie einen Dienst und wählen Sie auf der Registerkarte **Einstellungen** die Option **Quell-IP-Adresse verwenden**aus.

So binden Sie einen Dienst mithilfe der Befehlszeilenschnittstelle an einen virtuellen Lastausgleichsserver

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-DSR-1
<!--NeedCopy-->
```

So binden Sie einen Dienst mithilfe der GUI an einen virtuellen Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und klicken Sie in den Abschnitt “ **Dienste** “, um einen Dienst an den virtuellen Server zu binden.

Verwenden der Client-IP-Adresse im Outer Header von Tunnelpaketen

Der NetScaler unterstützt die Verwendung der Clientquell-IP-Adresse als Quell-IP-Adresse im äußeren Header von Tunnelpaketen, die sich auf den Rückgabemodus des Direktservers mit IP-Tunneling beziehen. Diese Funktion wird für DSR mit IPv4 und DSR mit IPv6-Tunneling-Modi unterstützt. Um

diese Funktion zu aktivieren, aktivieren **Sie den Parameter Clientquell-IP-Adresse verwenden** für IPv4 oder IPv6. Diese Einstellung wird global auf alle DSR-Konfigurationen angewendet, die IP-Tunneling verwenden.

So verwenden Sie eine Clientquell-IP-Adresse als Quell-IP-Adresse über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set iptunnelparam -useclientsourceip [YES | NO]`
- `show iptunnelparam`

So verwenden Sie die Clientquell-IP-Adresse als Quell-IP-Adresse über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Netzwerk**.
2. Klicken Sie auf der Registerkarte **Einstellungen** auf **Globale IPv4-Tunneleinstellungen**.
3. Wählen Sie auf der Seite **Globale IPv4-Tunnelparameter konfigurieren** die Option **Clientquell-IP verwenden** aus.
4. Klicken Sie auf **OK**.

So verwenden Sie die Clientquell-IP-Adresse als Quell-IP-Adresse über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set ip6tunnelparam -useclientsourceip [YES | NO]`
- `show ip6tunnelparam`

So verwenden Sie die Clientquell-IP-Adresse als Quell-IP-Adresse über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Netzwerk**.
2. Klicken Sie auf der Registerkarte **Einstellungen** auf **Globale IPv6-Tunneleinstellungen**.
3. Wählen Sie auf der Seite **Globale IPv6-Tunnelparameter konfigurieren** die Option **Clientquell-IP verwenden** aus.
4. Klicken Sie auf **OK**.

Konfiguration der Entkapselung

Sie können entweder eine NetScaler-Appliance oder einen Back-End-Server als Entkapselung konfigurieren.

NetScaler Entkapselung

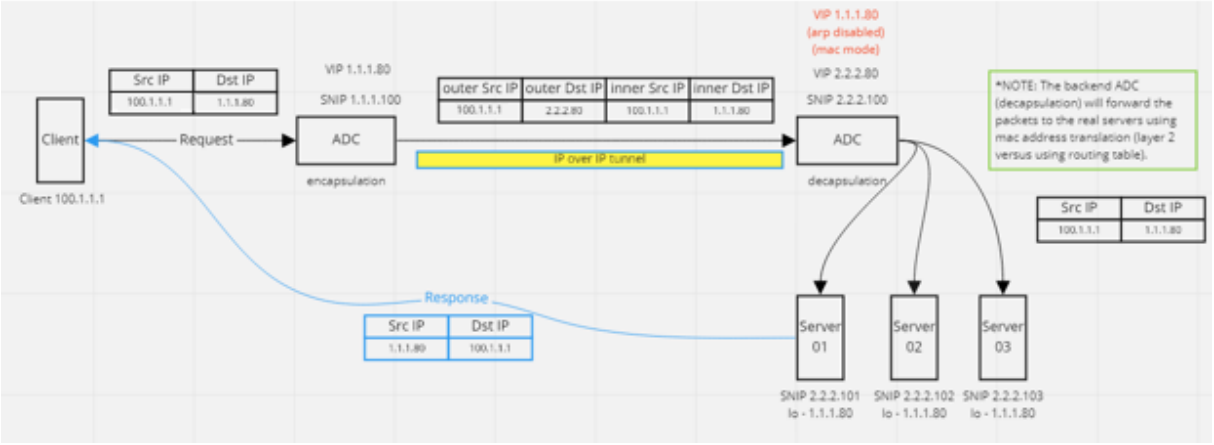
Wenn eine NetScaler-Appliance als Entkapselung verwendet wird, muss in der NetScaler-Appliance ein IP-Tunnel erstellt werden. Weitere Informationen finden Sie unter Konfigurieren von IP-Tunneln.

Das NetScaler Dekapselungs-Setup besteht aus den folgenden zwei virtuellen Servern:

- Der erste virtuelle Server empfängt das gekapselte Paket und entfernt die äußere IP-Kapselung.
- Der zweite virtuelle Server verfügt über die IP des ursprünglichen Dienstes im Front-End ADC und leitet das Paket mithilfe der MAC-Adresse der gebundenen Dienste mithilfe der MAC-Adresse der gebundenen Dienste an das Back-End weiter. Dieses Setup wird normalerweise als L2DSR bezeichnet. Stellen Sie sicher, dass Sie ARP auf diesem virtuellen Server deaktivieren.

Beispiel-Setup:

Die folgende Abbildung zeigt ein Entkapselungs-Setup mit den ADC-Appliances.



Die vollständige Konfiguration, die für das Setup erforderlich ist, lautet wie folgt.

Front-End-ADC-Konfiguration:

```
add service svc_DSR01 2.2.2.80 ANY * -usip YES -useproxyport NO
add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED
bind lb vserver vip_DSR_ENCAP svc_DSR01
<!--NeedCopy-->
```

Back-End-ADC-Konfiguration:

```
add ipTunnel DSR-IPIP 1.1.1.100 255.255.255.255 *

add service svc_DSR01_01 2.2.2.101 ANY * -usip YES -useproxyport NO
add service svc_DSR01_02 2.2.2.102 ANY * -usip YES -useproxyport NO
add service svc_DSR01_03 2.2.2.103 ANY * -usip YES -useproxyport NO

```



```
add lb vserver vs_DSR_DECAP ANY 2.2.2.80 * -lbMethod SOURCEIPHASH -m IPTUNNEL -sessionless ENABLED -netProfile netProf_DSR_MBF_noIP

add ns ip 1.1.1.80 255.255.255.255 -type VIP -arp DISABLED -snmp DISABLED
add lb vserver vs_DSR_Relay ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m MAC -sessionless ENABLED

bind lb vserver vs_DSR_DECAP svc_DSR01_01
bind lb vserver vs_DSR_DECAP svc_DSR01_02
bind lb vserver vs_DSR_DECAP svc_DSR01_03

bind lb vserver vip_DSR_Relay svc_DSR01_01
bind lb vserver vip_DSR_Relay svc_DSR01_02
bind lb vserver vip_DSR_Relay svc_DSR01_03

add netProfile netProf_DSR_MBF_noIP -MBF ENABLED
add lb monitor mon_DSR_MAC PING -netProfile netProf_DSR_MBF_noIP
bind service svc_DSR01_01 -monitorName mon_DSR_MAC
bind service svc_DSR01_02 -monitorName mon_DSR_MAC
bind service svc_DSR01_03 -monitorName mon_DSR_MAC
<!--NeedCopy-->
```

Das folgende Beispiel zeigt ein Test-Setup mit Ubuntu- und Red Hat Servern, auf denen apache2 ausgeführt wird. Diese Befehle werden auf jedem Back-End-Server eingerichtet.

```
sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
sudo sysctl net.ipv4.conf.all.arp_ignore=1
sudo sysctl net.ipv4.conf.all.arp_announce=2
sudo sysctl net.ipv4.conf.eth4.rp_filter=2 (The interface has the external IP with route towards the ADC)
sudo sysctl net.ipv4.conf.all.forwarding=1
sudo ip link set dev lo arp on
<!--NeedCopy-->
```

Entkapselung des Backend-Servers

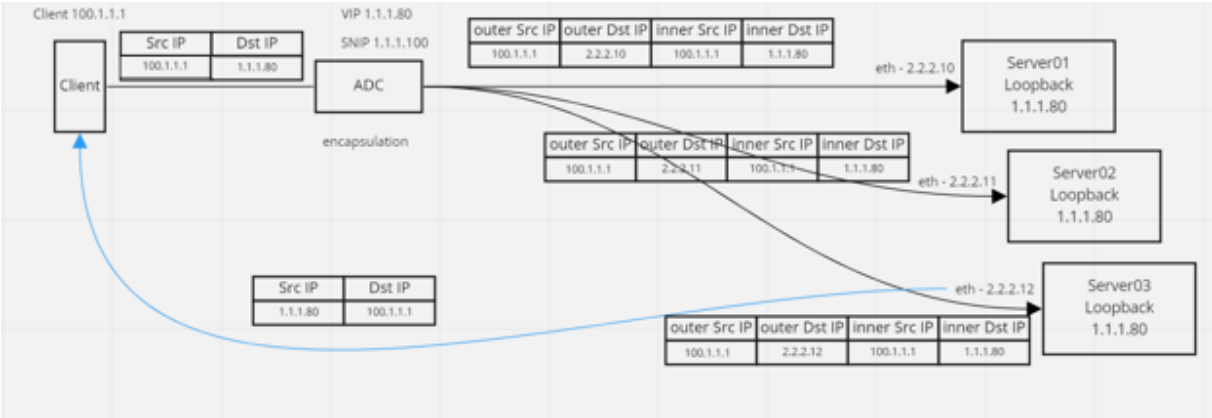
Wenn Sie die Back-End-Server als Entkapselung verwenden, variiert die Back-End-Konfiguration je nach Serverbetriebssystemtyp. Sie können einen Back-End-Server als Entkapselung konfigurieren, indem Sie die folgenden Schritte ausführen:

1. Konfigurieren Sie eine Loop-Back-Schnittstelle mit IP für Dienst-IP.
2. Erstellen Sie eine Tunnelschnittstelle.
3. Fügen Sie eine Route über Tunnelschnittstelle hinzu.

4. Konfigurieren Sie die Einstellungen der Benutzeroberfläche nach Bedarf für den Datenverkehr

> Hinweis:
>
> Windows-Betriebssystem-Server können IP-Tunneln nicht nativ durchführen, daher werden die Befehle als Beispiele für Linux-basierte Systeme bereitgestellt. Plug-Ins von Drittanbietern sind für Windows-Betriebssystem-Server verfügbar, das liegt jedoch außerhalb des Geltungsbereichs dieses Beispiels.

Die folgende Abbildung zeigt ein Entkapselungs-Setup unter Verwendung der Back-End-Server.



Beispielkonfiguration:

In diesem Beispiel ist 1.1.1.80 die virtuelle IP-Adresse (VIP) von NetScaler und 2.2.2.10-2.2.2.12 sind die IP-Adressen des Back-End-Servers. Die VIP-Adresse ist in der Loopback-Schnittstelle konfiguriert und eine Route wird über die Tunnelschnittstelle hinzugefügt. Die Monitore verwenden die Server-IP und tunneln die Monitorpakete mithilfe der Tunnelendpunkte über den IP-Tunnel.

Die vollständige Konfiguration, die für das Setup erforderlich ist, lautet wie folgt.

Front-End-ADC-Konfiguration:

Die folgende Konfiguration erstellt einen Monitor, der den Tunnelendpunkt als Quelle verwendet. Senden Sie dann Pings über den Tunnel an die Dienst-IP-Adresse.

```
add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
add netProfile netProfile_DSR -srcIP 10.0.1.2
add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
    YES -netProfile netProfile_DSR
<!--NeedCopy-->
```

Die folgende Konfiguration erstellt einen VIP für den Dienst, der die ursprüngliche Quell-IP-Adresse verwendet. Leitet dann den Datenverkehr über den IP-Tunnel an Back-End-Server weiter.

```
add service svc_DSR01 2.2.2.10 ANY * -usip YES -useproxyport NO
bind service svc_DSR01 -monitorName mon_DSR
```



```
3
4  add service svc_DSR02 2.2.2.11 ANY * -usip YES -useproxyport NO
5  bind service svc_DSR02 -monitorName mon_DSR
6
7  add service svc_DSR03 2.2.2.12 ANY * -usip YES -useproxyport NO
8  bind service svc_DSR03 -monitorName mon_DSR
9
10 add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
       IPTUNNEL -sessionless ENABLED
11 bind lb vserver vip_DSR_ENCAP svc_DSR01
12 bind lb vserver vip_DSR_ENCAP svc_DSR02
13 bind lb vserver vip_DSR_ENCAP svc_DSR03
14 <!--NeedCopy-->
```

Back-End-Serverkonfiguration jedes Servers:

Die folgenden Befehle sind erforderlich, damit der Back-End-Server das IPIP-Paket empfangen, die äußere Kapselung entfernt und dann vom Loopback auf die ursprüngliche Client-IP reagiert. Dadurch wird sichergestellt, dass die IP-Adressen in dem vom Client empfangenen Paket mit den IP-Adressen in der ursprünglichen Anforderung übereinstimmen.

```
1  modprobe ipip
2  sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
3  nmcli connection add type ip-tunnel ip-tunnel.mode ipip con-name tun0
4  ifname tun0 remote 198.51.100.5 local 203.0.113.10
5  nmcli connection modify tun0 ipv4.addresses '10.0.1.1/30'
6  nmcli connection up tun0
7  sudo sysctl net.ipv4.conf.all.arp_ignore=1
8  sudo sysctl net.ipv4.conf.all.arp_announce=2
9  sudo sysctl net.ipv4.conf.tun0.rp_filter=2
10 sudo sysctl net.ipv4.conf.all.forwarding=1
11 sudo ip link set dev lo arp off
12 <!--NeedCopy-->
```

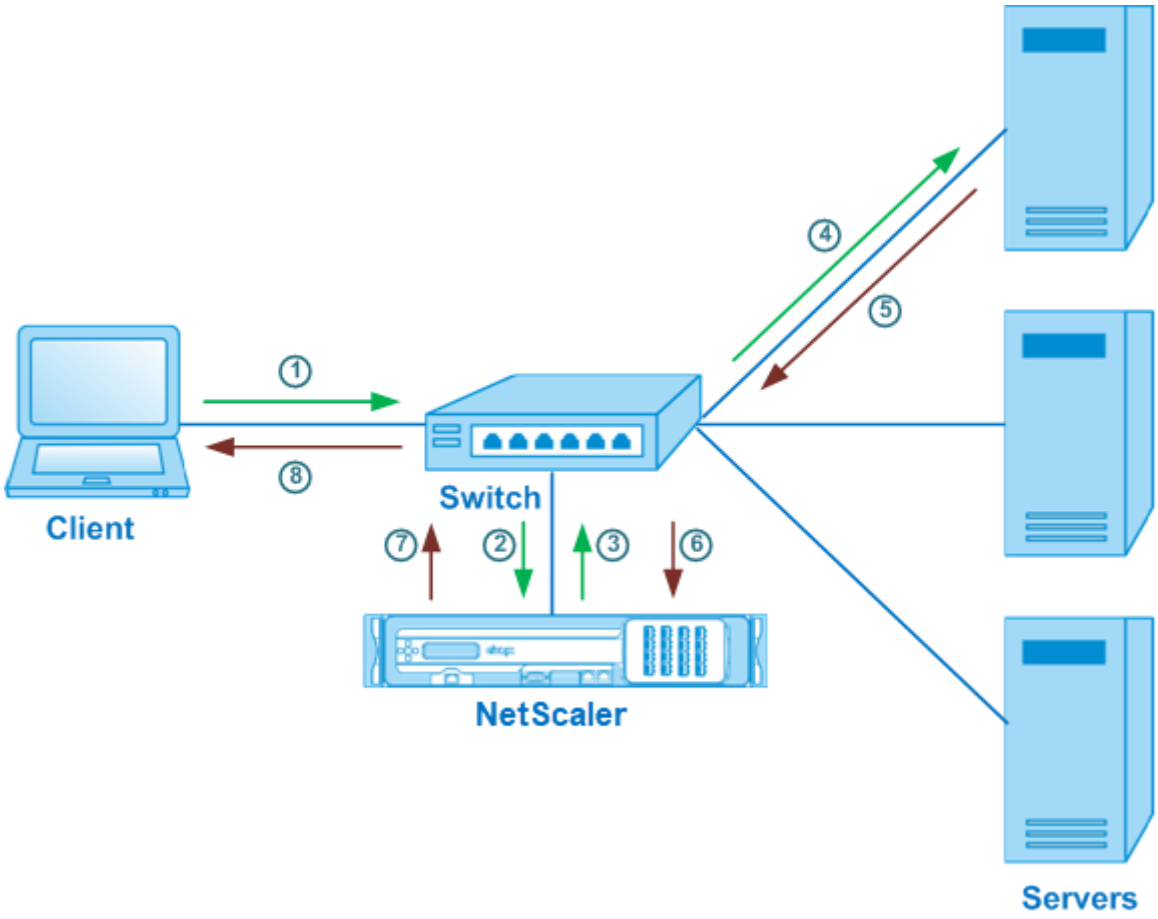
Anwendungsfall 8: Lastausgleich im Einarmmodus konfigurieren

May 11, 2023

In einem einarmigen Setup verbinden Sie die NetScaler-Appliance über ein einzelnes VLAN mit dem Netzwerk. Die Appliance empfängt die Anfrage vom Client in einem einzelnen VLAN und sendet die Anfrage an den Server im selben VLAN. Dies ist eines der einfachsten Bereitstellungsszenarien, bei denen der Router, die Server und die Appliance alle mit demselben Switch verbunden sind. Clien-

tanforderungen am Switch werden an die Appliance weitergeleitet, und die Appliance verwendet die konfigurierte Lastausgleichsmethode, um den Dienst auszuwählen.

Abbildung 1. Lastausgleich im Einarmmodus



Im Beispielszenario werden die Dienste Service-ANY-1, Service-ANY-2 und Service-ANY-3 erstellt und an den virtuellen Server Vserver-LB-1 gebunden. Die Last des virtuellen Servers verteilt die Clientanforderung auf einen Dienst. In der folgenden Tabelle sind die Namen und Werte der Entitäten aufgeführt, die auf der Appliance im einarmigen Modus konfiguriert sind.

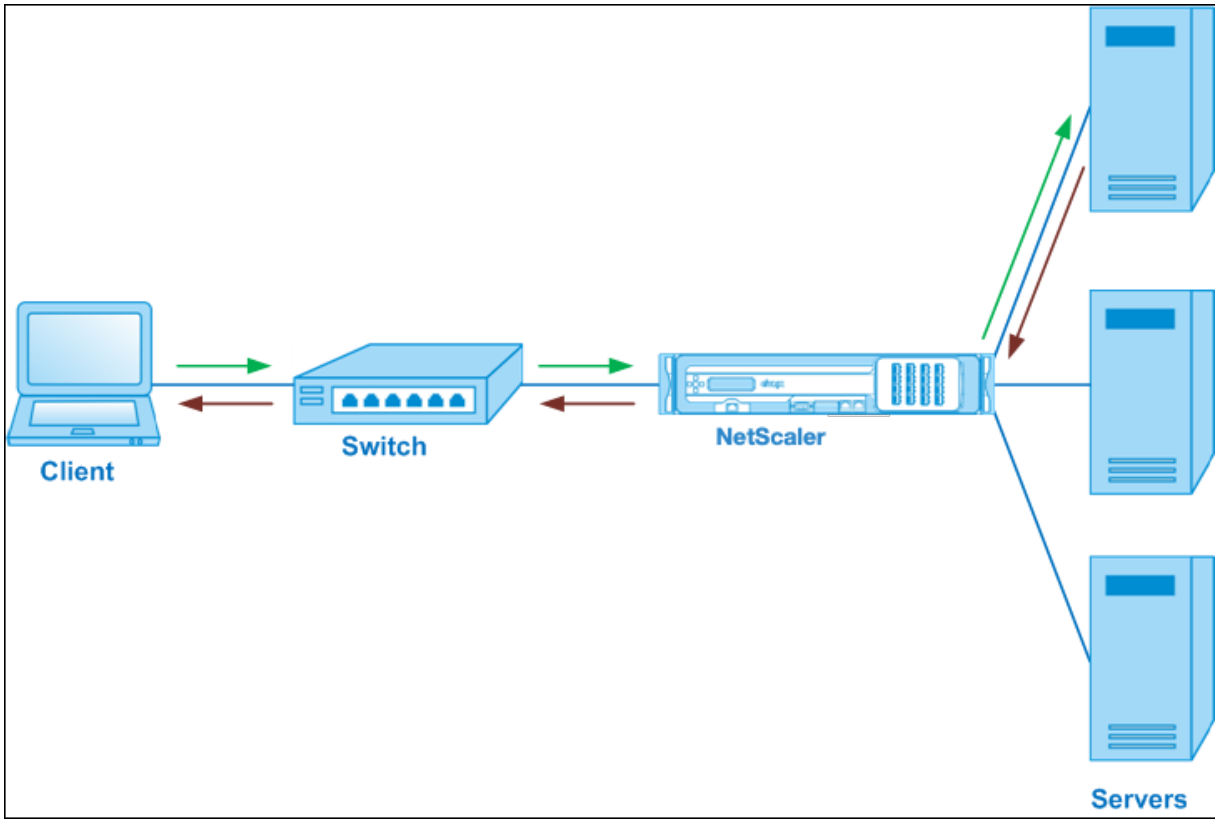
Entitätstyp	Name	IP-Adresse	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Monitore	TCP	Ohne	Ohne

Informationen zum Konfigurieren eines Load Balancing-Setups im Einarmmodus finden Sie unter Einrichten des Basic Load Balancing.

Anwendungsfall 9: Lastausgleich im Inlinemodus konfigurieren

May 11, 2023

In einem Setup im Inline-Modus (auch als Zweiarm-Modus bezeichnet) verbinden Sie die NetScaler-Appliance über mehrere VLANs mit dem Netzwerk. Die Appliance empfängt die Anfrage vom Client in einem VLAN und sendet die Anfrage an den Server in einem anderen VLAN. In der zweiarmigen Konfiguration ist die Appliance zwischen den Servern und dem Client verbunden. Clientanforderungen am Switch werden an die Appliance weitergeleitet, und die Appliance verwendet die konfigurierte Lastausgleichsmethode, um den Dienst auszuwählen.



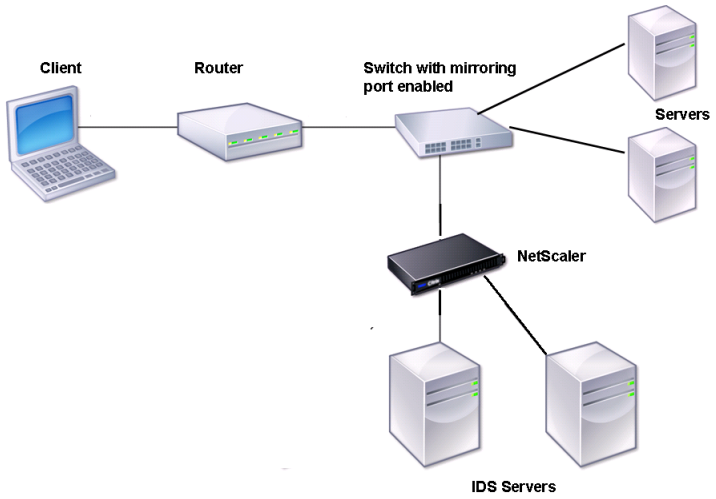
Die Konfiguration und das Entitätsdiagramm für den Inlinemodus sind die gleichen wie unter Load Balancing im Einarmmodus konfigurierenbeschrieben.

Anwendungsfall 10: Lastausgleich von Intrusion-Detection-System-Servern

May 11, 2023

Damit die NetScaler-Appliance den Lastenausgleich von IDS-Servern (Intrusion Detection System) unterstützt, müssen die IDS-Server und -Clients über einen Switch verbunden sein, auf dem die Portspiegelung aktiviert ist. Der Client sendet eine Anfrage an den Server. Da die Portspiegelung auf dem Switch aktiviert ist, werden die Anforderungspakete kopiert oder an den Port des virtuellen NetScaler-Appliance-Servers gesendet. Die Appliance verwendet dann die konfigurierte Load-Balancing-Methode, um einen IDS-Server auszuwählen, wie in der folgenden Abbildung dargestellt.

Abbildung 1. Topologie von IDS-Servern mit Lastausgleich



Hinweis: Derzeit unterstützt die Appliance nur den Lastausgleich passiver IDS-Geräte.

Wie im vorherigen Diagramm dargestellt, funktioniert das IDS-Load-Balancing-Setup wie folgt:

1. Die Client-Anfrage wird an den IDS-Server gesendet, und ein Switch mit aktiviertem Mirroring-Port leitet diese Pakete an den IDS-Server weiter. Die Quell-IP-Adresse ist die IP-Adresse des Clients, und die Ziel-IP-Adresse ist die IP-Adresse des Servers. Die Quell-MAC-Adresse ist die MAC-Adresse des Routers, und die Ziel-MAC-Adresse ist die MAC-Adresse des Servers.
2. Der Datenverkehr, der durch den Switch fließt, wird auf die Appliance gespiegelt. Die Appliance verwendet die Layer-3-Informationen (Quell-IP-Adresse und Ziel-IP-Adresse), um das Paket an den ausgewählten IDS-Server weiterzuleiten, ohne die Quell-IP-Adresse oder die Ziel-IP-Adresse zu ändern. Es ändert die Quell-MAC-Adresse und die Ziel-MAC-Adresse in die MAC-Adresse des ausgewählten IDS-Servers.

Hinweis: Beim Lastenausgleich von IDS-Servern können Sie die Lastausgleichsmethoden SRCIPHASH, DESTIPHASH oder SRCIPDESTIPHASH konfigurieren. Die Methode SRCIPDESTIPHASH wird empfohlen, da Pakete, die vom Client zu einem Dienst auf der Appliance fließen, an einen einzelnen IDS-Server gesendet werden müssen.

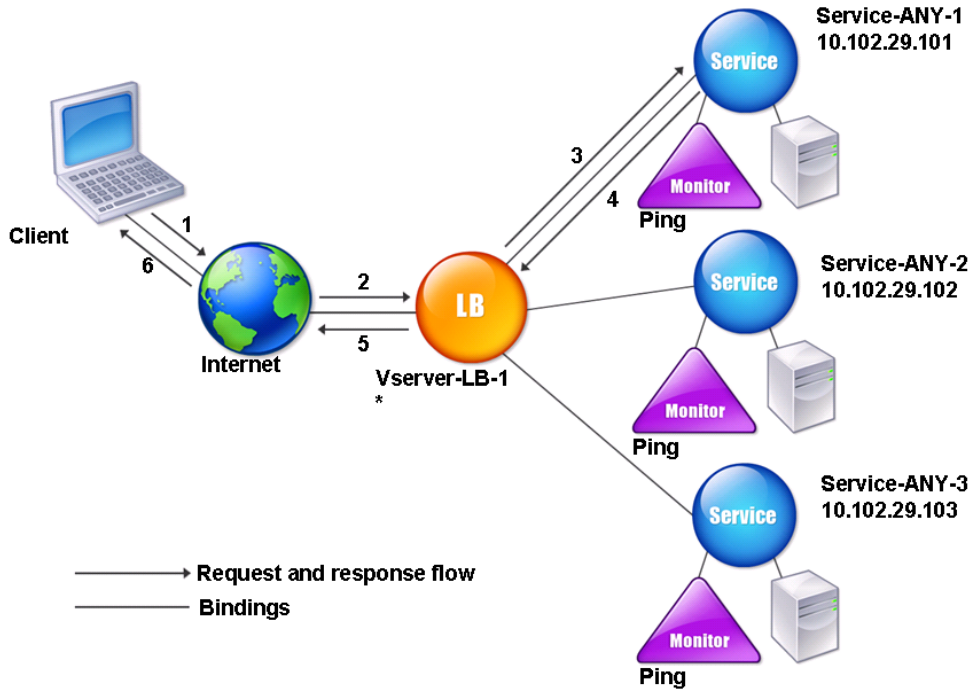
Angenommen, Service-ANY-1, Service-ANY-2 und Service-ANY-3 werden erstellt und an vServer-LB-1 gebunden. Der virtuelle Server verteilt die Belastung der Dienste. In der folgenden Tabelle sind die Namen und Werte der auf der Appliance konfigurierten Entitäten aufgeführt.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	*	*	ANY
Services	Service-ANY-1	10.102.29.101	*	ANY
	Service-ANY-2	10.102.29.102	*	ANY
	Service-ANY-3	10.102.29.103	*	ANY
Monitore	Ping	Ohne	Ohne	Ohne

Hinweis: Sie können den Inline-Modus oder den Einarmmodus für ein IDS-Load-Balancing-Setup verwenden.

Das folgende Diagramm zeigt die Load-Balancing-Entitäten und Werte der Parameter, die auf der Appliance konfiguriert werden sollen.

Abbildung 2. Entitätsmodell für Load Balancing IDS Server



Um ein IDS-Load Balancing-Setup zu konfigurieren, müssen Sie zunächst die MAC-basierte Weiterleitung aktivieren. Deaktivieren Sie auch die Layer-2- und Layer-3-Modi auf der Appliance.

So aktivieren Sie die MAC-basierte Weiterleitung mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns mode <ConfigureMode>
<!--NeedCopy-->
```

Beispiel:

```
enable ns mode MAC
<!--NeedCopy-->
```

So aktivieren Sie die MAC-basierte Weiterleitung mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **System > Einstellungen > Modi konfigurieren**und wählen Sie **MAC-basierte Weiterleitung**aus.

Als Nächstes finden Sie unter “Einrichten des Basic Load Balancing”, um ein grundlegendes Load Balancing-Setup zu konfigurieren.

Nachdem Sie das grundlegende Lastausgleichs-Setup konfiguriert haben, müssen Sie es für IDS anpassen, indem Sie eine unterstützte Lastausgleichsmethode konfigurieren (z. B. die SRCIPDESTIP-Hash-Methode auf einem virtuellen Server ohne Sitzungsfunktion) und den MAC-Modus aktivieren. Die Appliance behält den Verbindungsstatus nicht bei und leitet die Pakete nur an die IDS-Server weiter, ohne sie zu verarbeiten. Die Ziel-IP-Adresse und der Port bleiben unverändert, da sich der virtuelle Server im MAC-Modus befindet.

So konfigurieren Sie eine Load Balancing-Methode und einen Umleitungsmodus für einen sitzungslosen virtuellen Server mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
     RedirectionMode> -sessionless <Value>
2 <!--NeedCopy-->
```

Beispiel:

```
1 set lb vserver Vserver-LB-1 -lbMethod SourceIPDestIPHash -m MAC -
     sessionless enabled
2 <!--NeedCopy-->
```

> **Hinweis**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die Option -m MAC aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie eine Load Balancing-Methode und einen Umleitungsmodus für einen sitzungslosen virtuellen Server mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und wählen Sie im Umleitungsmodus MAC Based aus.
3. Klicken Sie in den Erweiterten Einstellungen auf Methoden und wählen Sie SCRIPDESTIPHASH aus. Klicken Sie auf Verkehrseinstellungen, und wählen Sie Sitzungsloser Lastenausgleich aus.

So legen Sie einen Dienst zur Verwendung der Quell-IP-Adresse mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:


```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```

So legen Sie einen Dienst zur Verwendung der Quell-IP-Adresse mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
2. Öffnen Sie einen Dienst und wählen Sie in den Einstellungen die Option **Quell-IP-Adresse verwenden**aus.

Damit USIP korrekt funktioniert, müssen Sie es global festlegen. Weitere Informationen zum globalen Konfigurieren von USIP finden Sie unter IP-Adressierung.

Anwendungsfall 11: Netzwerkverkehr mit Listenrichtlinien isolieren

May 11, 2023

> **Hinweis:**
>
> Die Lösung zur Datenverkehrsisolierung, die virtuelle Shadow-Server verwendet, um die Isolierung mehrerer Mandanten zu simulieren, wird nicht mehr empfohlen. Alternativ empfiehlt Citrix, die NetScaler Admin Partitioning-Funktion für solche Bereitstellungen zu verwenden. Weitere Informationen finden Sie unter Admin-Partitionierung.

Eine häufige Sicherheitsanforderung in einem Rechenzentrum besteht darin, die Isolierung des Netzwerkpfads zwischen dem Datenverkehr verschiedener Anwendungen oder Mandanten aufrechtzuerhalten. Der Datenverkehr einer Anwendung oder eines Mandanten muss vom Verkehr anderer Anwendungen oder Mandanten isoliert werden. Ein Finanzdienstleistungsunternehmen möchte beispielsweise den Datenverkehr seiner Versicherungsabteilung von dem seiner Finanzdienstleistungsanwendungen trennen. In der Vergangenheit konnte dies leicht durch die physische Trennung von Netzwerkdienstgeräten wie Firewalls, Load Balancern und IdP sowie durch Netzwerküberwachung und logische Trennung in der Switching-Struktur erreicht werden.

Im Zuge der Weiterentwicklung der Rechenzentrumsarchitekturen hin zu virtualisierten Rechenzentren mit mehreren Mandanten werden Netzwerkdienste auf der Aggregationsebene eines Rechenzentrums konsolidiert. Diese Entwicklung hat die Netzwerkpfadisolierung zu einer wichtigen Kompo-

nente für Netzwerkdienstgeräte gemacht und erhöht die Anforderung an ADCs, den Verkehr auf den Ebenen L4 bis L7 zu isolieren. Darüber hinaus muss der gesamte Datenverkehr eines bestimmten Mandanten über eine Firewall laufen, bevor die Service-Schicht erreicht wird.

Um die Anforderung der Isolierung der Netzwerkpfade zu erfüllen, identifiziert eine NetScaler Appliance die Netzwerkdomänen und steuert den Datenverkehr in den Domänen. Die NetScaler Lösung besteht aus zwei Hauptkomponenten: Listen Policies und Shadow Virtual Server.

Jedem zu isolierenden Netzwerkpfad wird ein virtueller Server zugewiesen, auf dem eine Listen-Policy definiert ist, sodass der virtuelle Server nur Datenverkehr von einer bestimmten Netzwerkdomäne abhört.

Um den Datenverkehr zu isolieren, können Listen-Richtlinien auf mehreren Client-Parametern oder deren Kombinationen basieren, und den Richtlinien können Prioritäten zugewiesen werden. In der folgenden Tabelle sind die Parameter aufgeführt, die in Listen-Richtlinien zur Identifizierung des Datenverkehrs verwendet werden können.

Kategorie	Parameter
Ethernet-Protokoll	Quell-MAC-Adresse, Ziel-MAC-Adresse
Netzwerkschnittstelle	Netzwerk-ID, Empfangsdurchsatz, Sendedurchsatz, Übertragungsdurchsatz
IP-Protokoll	Quell-IP-Adresse, Ziel-IP-Adresse
IPv6-Protokoll	Quell-IPv6-Adresse, Ziel-IPv6-Adresse
TCP-Protokoll	Quellport, Zielport, maximale Segmentgröße, Nutzlast und andere Optionen
UDP-Protokoll	Quellport, Zielport
VLAN	ID

Tabelle 1. Client-Parameter, die zur Definition von Listen-Richtlinien verwendet werden

Auf der NetScaler-Appliance wird für jede Domäne ein virtueller Server konfiguriert, wobei eine Listen-Richtlinie festlegt, dass der virtuelle Server nur den Datenverkehr für diese Domäne abhören soll. Für jede Domain ist außerdem ein virtueller Shadow-Load-Balancing-Server konfiguriert, der den für jede Domain bestimmten Datenverkehr abhört. Jeder der virtuellen Shadow-Load-Balancing-Server hat eine Wildcard-IP-Adresse (*) und einen Port, und sein Diensttyp ist auf ANY festgelegt.

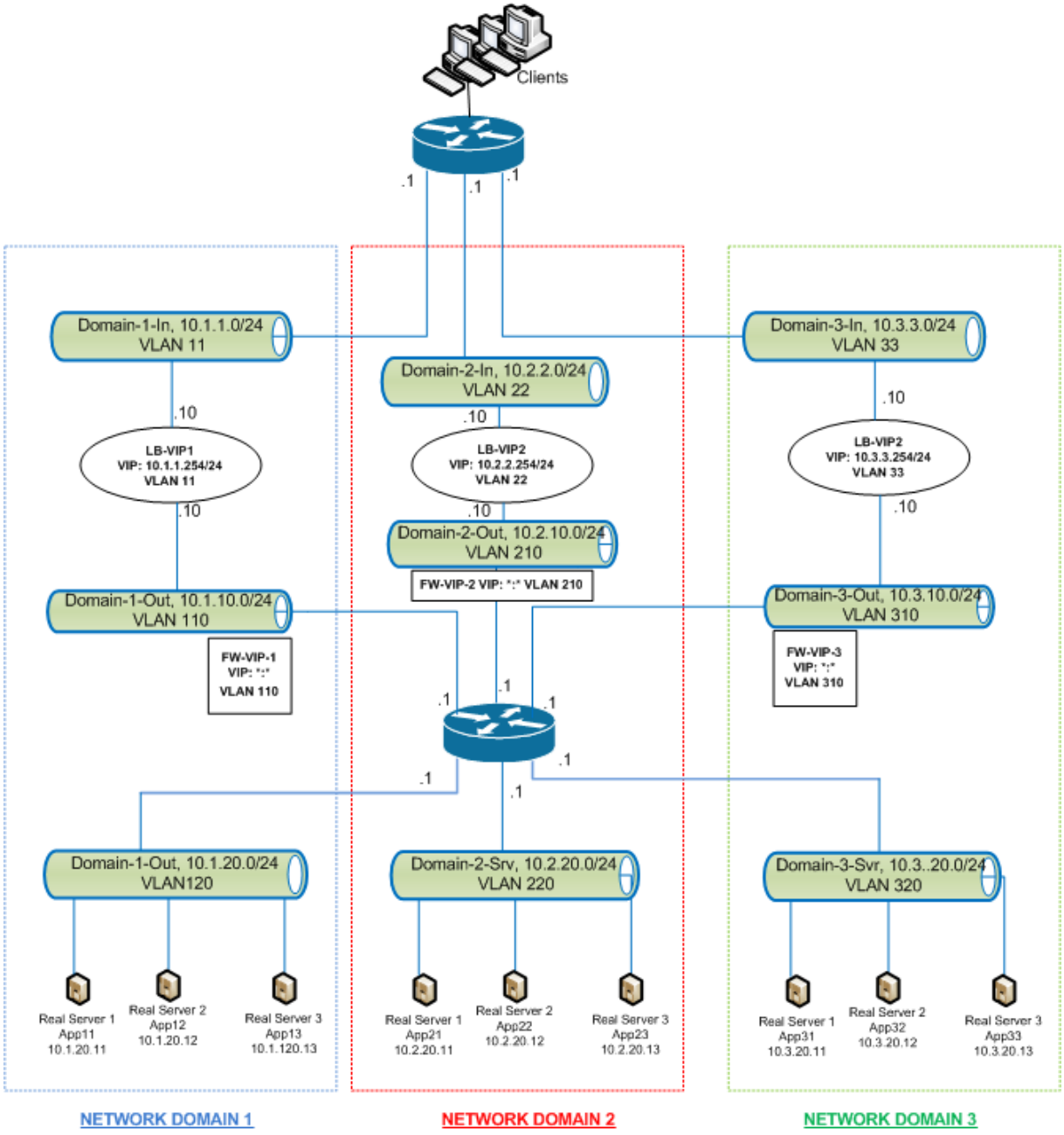
In jeder Domain ist eine Firewall für die Domain als Dienst an den virtuellen Shadow-Load-Balancing-Server gebunden, der den gesamten Datenverkehr durch die Firewall weiterleitet. Lokaler Verkehr wird an sein Ziel weitergeleitet, und Datenverkehr, der für eine andere Domain bestimmt ist, wird an die Firewall für diese Domain weitergeleitet. Die virtuellen Shadow-Load-Balancing-Server sind für

die Umleitung im MAC-Modus konfiguriert.

Wie Netzwerkpfade isoliert sind

Die folgende Abbildung zeigt einen typischen Datenverkehrsfluss zwischen Domänen. Betrachten Sie den Verkehrsfluss innerhalb von Netzwerkdomäne 1 und zwischen Netzwerkdomäne 1 und Netzwerkdomäne 2.

Abbildung 1. Isolierter Netzwerkpfad



Verkehr innerhalb der Netzwerkdomäne 1

Netzwerkdomäne 1 hat drei VLANs: VLAN 11, VLAN110 und VLAN120. Die folgenden Schritte beschreiben den Verkehrsfluss.

- Ein Client von VLAN 11 sendet eine Anfrage für einen Dienst, der aus dem Servicepool in VLAN 120 verfügbar ist.
- Der virtuelle Lastausgleichsserver LB-VIP1, der so konfiguriert ist, dass er den Datenverkehr von VLAN 11 abhört, empfängt die Anfrage und leitet die Anfrage an VLAN 110 weiter. Der virtuelle Server in VLAN 110 leitet die Anfrage an den virtuellen Shadow-Load-Balancing-Server FW-VIP-1 weiter.
- FW-VIP-1, das so konfiguriert ist, dass es den Datenverkehr von VLAN 110 abhört, empfängt die Anfrage und leitet sie an VLAN 120 weiter.
- Der virtuelle Lastausgleichsserver in VLAN 120 verteilt die Anforderung auf einen der physischen Server App11, App12 oder App13.
- Die vom physischen Server gesendete Antwort kehrt über denselben Pfad zum Client in VLAN 11 zurück.

Diese Konfiguration stellt sicher, dass der Datenverkehr innerhalb des NetScaler immer für den gesamten Datenverkehr, der von einem Client stammt, getrennt wird.

Verkehr zwischen Netzwerkdomäne 1 und Netzwerkdomäne 2

Netzwerkdomäne 1 hat drei VLANs: VLAN 11, VLAN 110 und VLAN 120. Netzwerkdomäne 2 hat auch drei VLANs: VLAN 22, VLAN 210 und VLAN 220. Die folgenden Schritte beschreiben den Verkehrsfluss von VALN 11 zu VLAN 22.

- Ein Client von VLAN 11, das zur Netzwerkdomäne 1 gehört, sendet eine Anfrage für einen Dienst, der aus dem Servicepool in VLAN 220 verfügbar ist, das zur Netzwerkdomäne 2 gehört.
- In Netzwerkdomäne 1 empfängt der virtuelle Lastausgleichsserver LB-VIP1, der so konfiguriert ist, dass er den Datenverkehr von VLAN 11 abhört, die Anfrage und leitet die Anfrage an VLAN 110 weiter.
- Der virtuelle Shadow-Load-Balancing-Server FW-VIP-1, der so konfiguriert ist, dass er den VLAN 110-Verkehr abhört, der für eine andere Domäne bestimmt ist, empfängt die Anfrage und leitet sie an den virtuellen Firewallserver FW-VIP-2 weiter, da die Anfrage an einen physischen Server in Netzwerkdomäne 2 gerichtet ist.
- In Netzwerkdomäne 2 leitet FW-VIP-2 die Anfrage an VLAN 220 weiter.
- Der virtuelle Lastausgleichsserver in VLAN 220 verteilt die Anforderung auf einen der physischen Server App21, App22 oder App23.
- Die vom physischen Server gesendete Antwort kehrt über denselben Pfad durch die Firewall in Netzwerkdomäne 2 und dann zu Netzwerkdomäne 1 zurück, um den Client in VLAN 11 zu erreichen.

Konfigurationsschritte

Gehen Sie wie folgt vor, um die Netzwerkpfadisolierung mithilfe von Listen-Richtlinien zu konfigurieren:

- Fügen Sie Listen-Richtlinienausdrücke hinzu. Jeder Ausdruck gibt eine Domain an, für die der Verkehr bestimmt ist. Sie können die VLAN-ID oder andere Parameter verwenden, um den Verkehr zu identifizieren.
- Konfigurieren Sie für jede Netzwerkdomäne zwei virtuelle Server wie folgt:
  - Erstellen Sie einen virtuellen Lastausgleichsserver, für den Sie eine Listenrichtlinie angeben, die den für diese Domäne bestimmten Datenverkehr identifiziert. Sie können den Namen eines zuvor erstellten Ausdrucks angeben oder beim Erstellen des virtuellen Servers einen Ausdruck erstellen.
  - Erstellen Sie einen anderen virtuellen Lastausgleichsserver, der als Schattenserver bezeichnet wird, für den Sie einen Listenrichtlinienausdruck angeben, der auf Datenverkehr für eine Domäne angewendet wird. Stellen Sie auf diesem virtuellen Server den Diensttyp auf ANY und die IP-Adresse und den Port auf ein Sternchen (*) ein. Aktivieren Sie die MAC-basierte Weiterleitung auf diesem virtuellen Server.
  - Aktivieren Sie die L2-Verbindungsoption auf beiden virtuellen Servern.
    Zur Identifizierung einer Verbindung verwendet die NetScaler Appliance im Allgemeinen das 4-Tupel der Client-IP-Adresse, des Clientports, der Ziel-IP-Adresse und des Zielports. Wenn Sie die Option L2-Verbindung aktivieren, werden zusätzlich zum normalen 4-Tupel die Layer-2-Parameter der Verbindung (Kanalnummer, MAC-Adresse und VLAN-ID) verwendet.
- Fügen Sie Dienste hinzu, die die Serverpools in der Domäne darstellen, und binden Sie sie an den virtuellen Server.
- Konfigurieren Sie die Firewall für jede Domäne als Dienst und binden Sie alle Firewall-Dienste an den virtuellen Shadow-Server.

So isolieren Sie den Netzwerkverkehr mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add policy expression <expressionName> <listenPolicyExpression>

add lb vserver <name> <serviceType> <ip> <port> -l2conn ON -
   listenPolicy <expressionName>
<!--NeedCopy-->
```

Fügen Sie für jede Domain einen virtuellen Lastausgleichsserver hinzu. Dieser virtuelle Server ist für den Verkehr derselben Domain vorgesehen.


```
add lb vserver <name> ANY * * -l2conn ON -m MAC -listenPolicy <
    expressionName>
<!--NeedCopy-->
```

Fügen Sie für jede Domain einen virtuellen Shadow-Load-Balancing-Server hinzu. Dieser virtuelle Server ist für den Verkehr anderer Domänen vorgesehen.

Beispiel:

```
add policy expression e110 client.vlan.id==110
add policy expression e210 client.vlan.id==210
add policy expression e310 client.vlan.id==310
add policy expression e11 client.vlan.id==11
add policy expression e22 client.vlan.id==22
add policy expression e33 client.vlan.id==33

add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -persistenceType NONE -
    listenPolicy e11
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP2 HTTP 10.2.2.254 80 -persistenceType NONE -
    listenPolicy e22
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP3 HTTP 10.3.3.254 80 -persistenceType NONE -
    listenPolicy e33
-cltTimeout 180 -l2Conn ON


add lb vserver FW-VIP-1 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e110 -Listenpriority 1 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-2 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e210 -Listenpriority 2 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-3 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e310 -Listenpriority 3 -m MAC -cltTimeout
    120


add service RD-1 10.1.1.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
```



```
    NO -TCPB NO -CMP NO
27
28 add service RD-2 10.2.2.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
29 -usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO
30
31 add service RD-3 10.3.3.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
32 -usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO
33
34
35 bind lb vserver FW-VIP-1 RD-1
36
37 bind lb vserver FW-VIP-2 RD-2
38
39 bind lb vserver FW-VIP-3 RD-3
40 <!--NeedCopy-->
```

So isolieren Sie den Netzwerkverkehr mit dem Konfigurationsdienstprogramm

1. Fügen Sie Dienste hinzu, die die Server repräsentieren, wie unter Service erstellenbeschrieben.
2. Fügen Sie jede Firewall als Dienst hinzu:
   a) Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
   b) Erstellen Sie einen Dienst, indem Sie das Protokoll als ANY, den Server als IP-Adresse der Firewall und den Port als 80 angeben.
3. Konfigurieren Sie einen virtuellen Lastausgleichsserver.
4. Konfigurieren Sie den virtuellen Shadow-Load-Balancing-Server.
5. Wiederholen Sie für jede Netzwerkdomäne die Schritte 3 und 4.
6. Öffnen Sie im Bereich Load Balancing Virtual Servers die virtuellen Server, die Sie erstellt haben, und überprüfen Sie die Einstellungen.

Anwendungsfall 12: Citrix Virtual Desktops für den Lastausgleich konfigurieren

May 11, 2023

Für eine verbesserte Leistung bei der Bereitstellung virtueller Desktop-Anwendungen können Sie die NetScaler-Appliance in Citrix Virtual Desktops integrieren und die NetScaler-Load Balancing-Funktion

verwenden, um die Last auf die Desktop Delivery Controller (DDC) -Server zu verteilen.

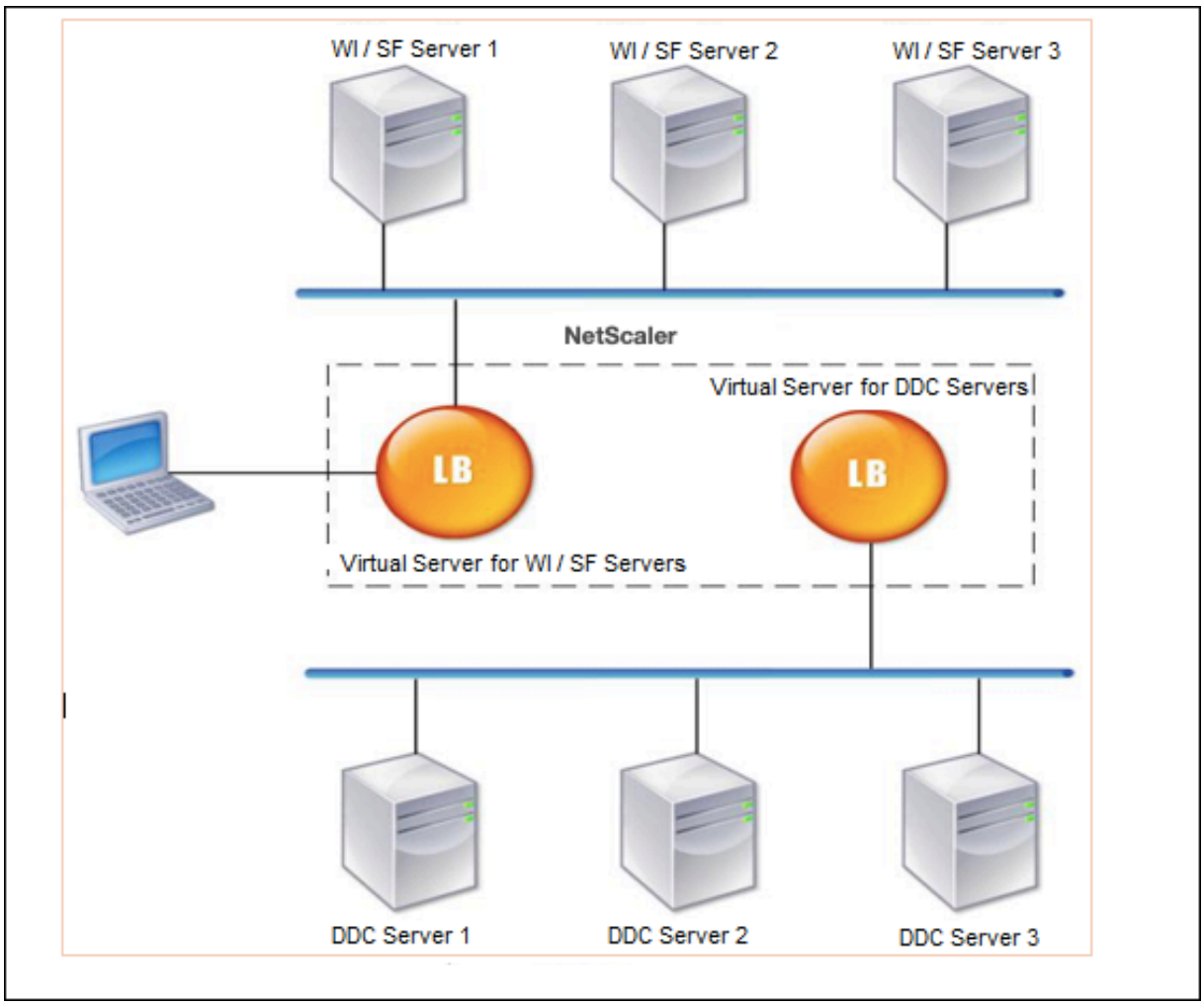
Im Allgemeinen verwenden Sie Citrix Virtual Desktops in Situationen, in denen Anwendungen nicht mit der Ausführung auf einem Terminalserver oder virtuellen Apps kompatibel sind oder wenn jeder virtuelle Desktop individuelle Anforderungen hat. In solchen Fällen benötigen Sie einen Desktop-Host für jeden Benutzer, der eine Verbindung herstellt. Die Hosts können jedoch gepoolt werden, sodass Sie für jeden aktuell verbundenen Benutzer nur einen Host benötigen.

Der für Citrix Virtual Desktops bereitgestellte Kernanwendungsdienst ist der Desktop Delivery Controller (DDC). Das DDC ist auf einem Server installiert und seine Hauptfunktion besteht darin, Desktop-Hosts zu registrieren und Client-Verbindungen zu ihnen zu vermitteln.

Das DDC authentifiziert auch Benutzer und verwaltet die Zusammenstellung der virtuellen Desktop-Umgebungen der Benutzer, indem es den Status der Desktops steuert und die Desktops startet und stoppt.

Im Allgemeinen werden mehrere DDCs installiert, um die Verfügbarkeit zu verbessern.

Die folgende Abbildung zeigt die Topologie einer NetScaler-Appliance, die mit Citrix Virtual Desktops arbeitet.



Hinweis:

Sie können zwar das HTTP-Protokoll verwenden, wir empfehlen jedoch, SSL für die Kommunikation zwischen dem Client und der NetScaler-Appliance zu verwenden. Sie können das HTTP-Protokoll für die Kommunikation zwischen dem NetScaler und den DDC-Servern verwenden, obwohl Sie das SSL-Protokoll für die Kommunikation mit dem Client verwenden.

So konfigurieren Sie den Lastenausgleich für Citrix Virtual Desktops über die GUI

1. Erstellen Sie einen Dienst.
   a) Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**.
   b) Erstellen Sie einen Dienst, indem Sie einen Namen, eine IP-Adresse, einen Port und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.
2. Erstellen Sie einen virtuellen Lastausgleichsserver.
   a) Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server** und klicken Sie auf **Hinzufügen**.

b) Erstellen Sie einen virtuellen Server, indem Sie einen Namen, eine IP-Adresse, einen Port und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.
4. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server** und wählen Sie einen Server aus.
   a) Klicken Sie auf **Edit**.
   b) Klicken Sie in den **Diensten und Dienstgruppen**auf **>** und klicken Sie auf **Bindung hinzufügen**.
   c) Wählen Sie den Service aus, den Sie binden möchten, und geben Sie den Gewichtswert ein.
   d) Klicken Sie auf **Bind**.

So konfigurieren Sie den Lastenausgleich für Citrix Virtual Desktops über die Befehlszeilenschnittstelle

- Um einen Dienst zu erstellen, geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Um einen virtuellen Server zu erstellen, geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Beispiel:

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80

- Um einen Dienst an einen virtuellen Lastausgleichsserver zu binden, geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

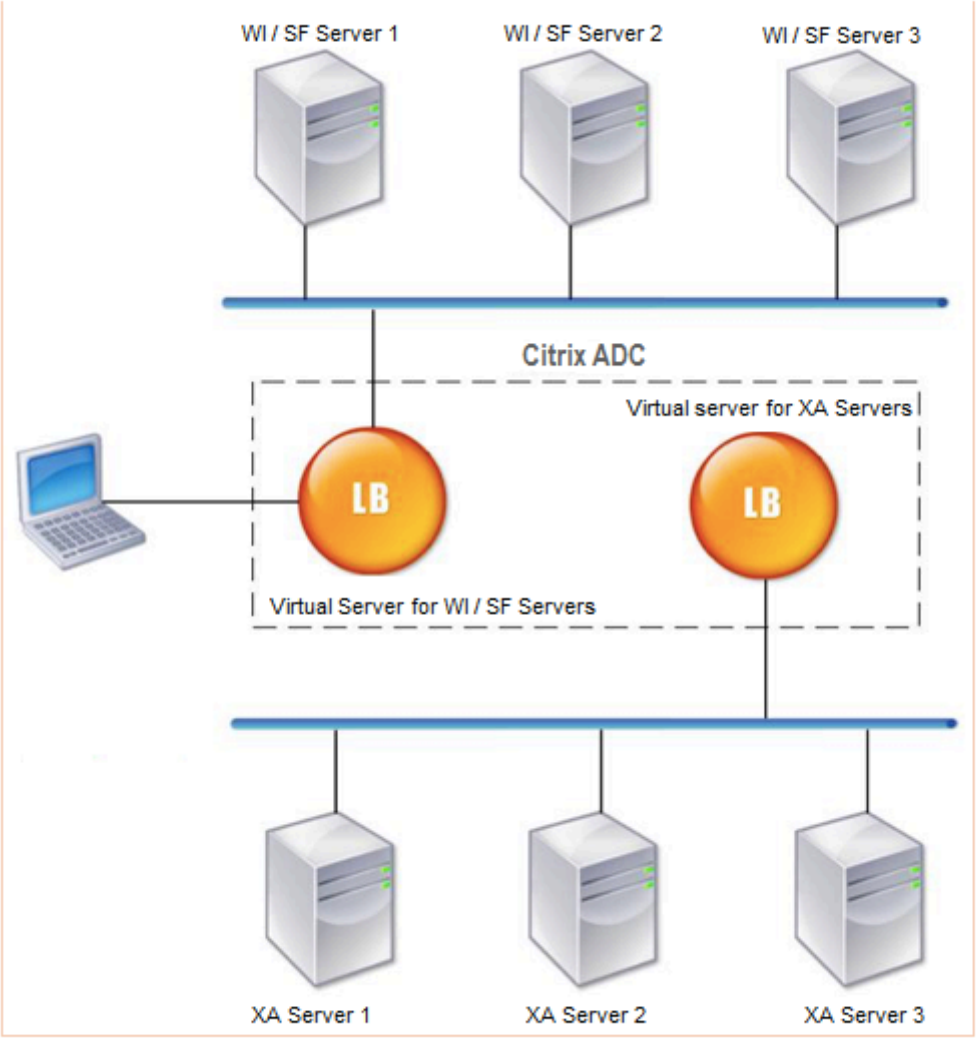
Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```


Anwendungsfall 13: Citrix Virtual Apps für den Lastausgleich konfigurieren

May 11, 2023

Für eine effiziente Bereitstellung von Anwendungen können Sie die NetScaler-Appliance in Citrix Virtual Apps integrieren und die NetScaler Load Balancing-Funktion verwenden, um die Last auf die Citrix Virtual Apps-Serverfarmen zu verteilen. Die folgende Abbildung zeigt ein Topologiediagramm eines solchen Aufbaus.



Die Webinterface-Server bieten sicheren Zugriff auf Citrix Virtual Apps-Anwendungsressourcen über den Webbrowser des Benutzers. Der Webinterface-Client präsentiert den Benutzern alle Ressourcen wie Anwendungen, Inhalte und Desktops, die in den Citrix Virtual Apps-Serverfarmen zur Verfügung

gestellt werden. Benutzer können über einen Standard-Webbrowser oder über das Citrix Online Plug-in auf die veröffentlichten Ressourcen zugreifen.

Der Webbrowser auf dem Gerät des Benutzers sendet Informationen an den Webserver, der mit den Servern in der Serverfarm kommuniziert, um dem Benutzer Zugriff auf die Ressourcen zu gewähren.

Das Webinterface und der XML Broker sind ergänzende Dienste. Das Webinterface bietet Benutzern Zugriff auf Anwendungen, und der XML-Broker bewertet die Benutzerberechtigungen, um festzustellen, welche Anwendungen im Webinterface angezeigt werden.

Der XML-Dienst ist auf allen Servern in der Serverfarm installiert. Der im Webinterface angegebene XML-Dienst fungiert als XML-Broker. Basierend auf den vom Webinterface-Server übergebenen Benutzeranmeldeinformationen sendet der XML-Broker-Server eine Liste der Anwendungen, auf die der Benutzer zugreifen kann.

In großen Unternehmen, in denen mehrere Webinterface-Server und XML-Broker-Server bereitgestellt werden, empfiehlt Citrix den Lastausgleich dieser Server mithilfe der NetScaler-Appliance. Konfigurieren Sie einen virtuellen Server für den Lastausgleich der Webinterface-Server und einen anderen für die XML Broker-Server. Die Load Balancing-Methode und andere Features können bei Bedarf auf dem virtuellen Server konfiguriert werden.

> **Hinweis**
>
> Sie können zwar das HTTP-Protokoll verwenden, Citrix empfiehlt jedoch, SSL für die Kommunikation zwischen dem Client und dem NetScaler zu verwenden. Sie können das HTTP-Protokoll für die Kommunikation zwischen dem NetScaler und den WI-Servern verwenden, obwohl Sie das SSL-Protokoll für die Kommunikation mit dem Client verwenden.

So konfigurieren Sie den Lastausgleich für Citrix Virtual Apps über die GUI

1. Erstellen Sie einen Dienst.
   a) Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**.
   b) Erstellen Sie einen Dienst, indem Sie einen Namen, eine IP-Adresse, einen Port und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.
2. Erstellen Sie einen virtuellen Lastausgleichsserver.
   a) Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server** und klicken Sie auf **Hinzufügen**.
   b) Erstellen Sie einen virtuellen Server, indem Sie einen Namen, eine IP-Adresse, einen Port und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.
3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.
4. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server** und wählen Sie einen Server aus.
   a) Klicken Sie auf **Edit**.

b) Klicken Sie in den **Diensten und Dienstgruppen**auf **>** und klicken Sie auf **Bindung hinzufügen**.
c) Wählen Sie den Dienst aus, den Sie binden möchten, und geben Sie den Gewichtswert ein.
d) Klicken Sie auf **Bind**.

So konfigurieren Sie den Lastausgleich für Citrix Virtual Apps mithilfe der Befehlszeilenschnittstelle

- Um einen Dienst zu erstellen, geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Um einen virtuellen Server zu erstellen, geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

- Um einen Dienst an einen virtuellen Lastausgleichsserver zu binden, geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

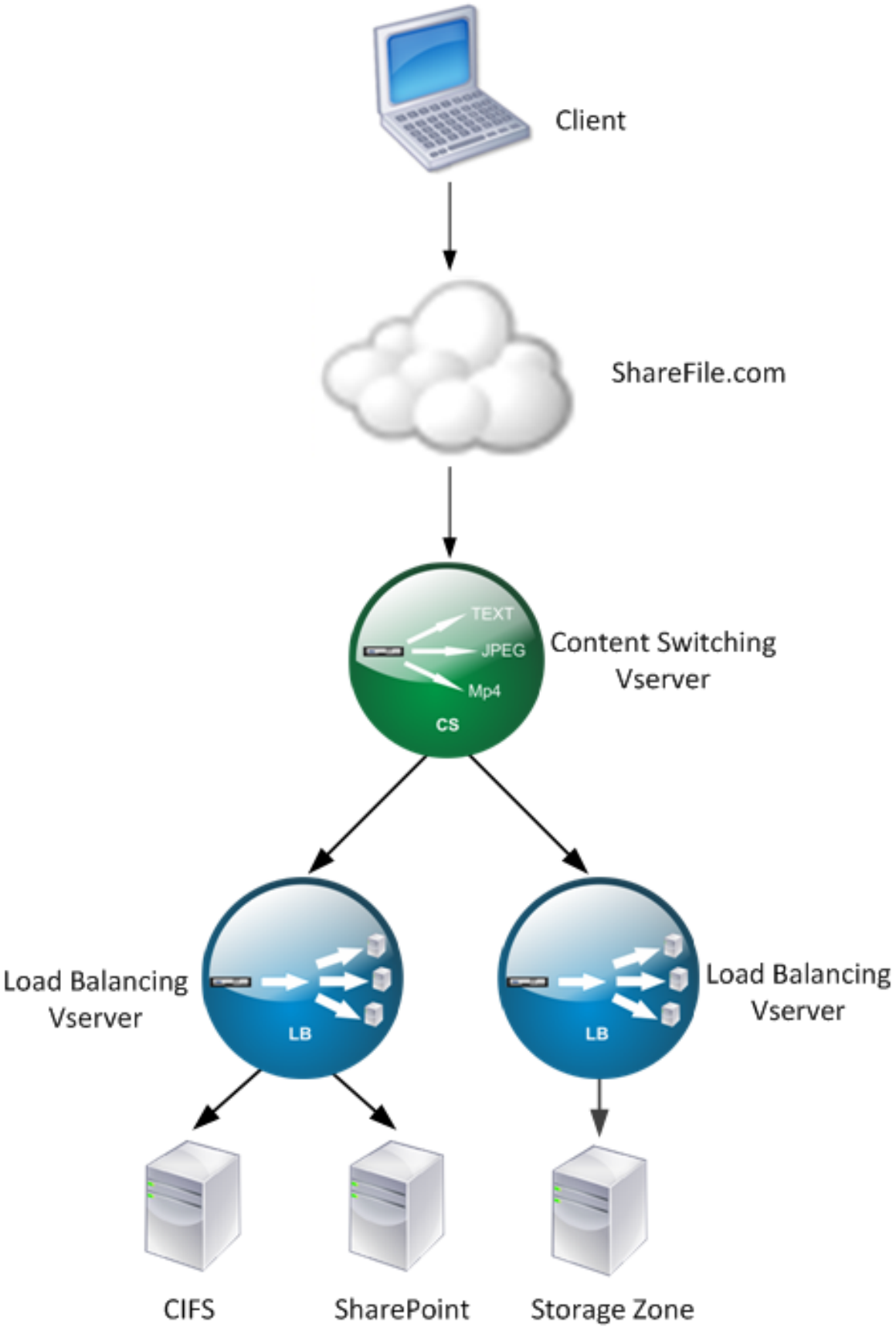

Anwendungsfall 14: ShareFile-Assistent zum Lastausgleich Citrix ShareFile

May 11, 2023

Sie können den Load Balancing für Citrix ShareFile mithilfe des Assistenten konfigurieren. Der Citrix ShareFile-Assistent hilft beim Einrichten der Load-Balancing-Konfiguration für die ShareFile-Site, die auf dem angeforderten Inhaltstyp basiert. Der Content Switching Server leitet die Anfrage weiter, je nachdem, ob es sich um eine StorageZone-, CIFS- oder eine SharePoint-Anfrage handelt. Der Content Switching basiert auf Richtlinien. Der Assistent generiert automatisch die Richtlinien, um festzustellen, ob es sich bei der Anfrage um StorageZone, CIFS oder SharePoint handelt. Der virtuelle Content Switching-Server verwendet diese Richtlinien, um die Anfrage an den richtigen Load Balancing-Server weiterzuleiten.

Ein typischer Datenfluss kann wie in der folgenden Abbildung dargestellt werden.

Abbildung 1. ShareFile-Datenlastenausgleich

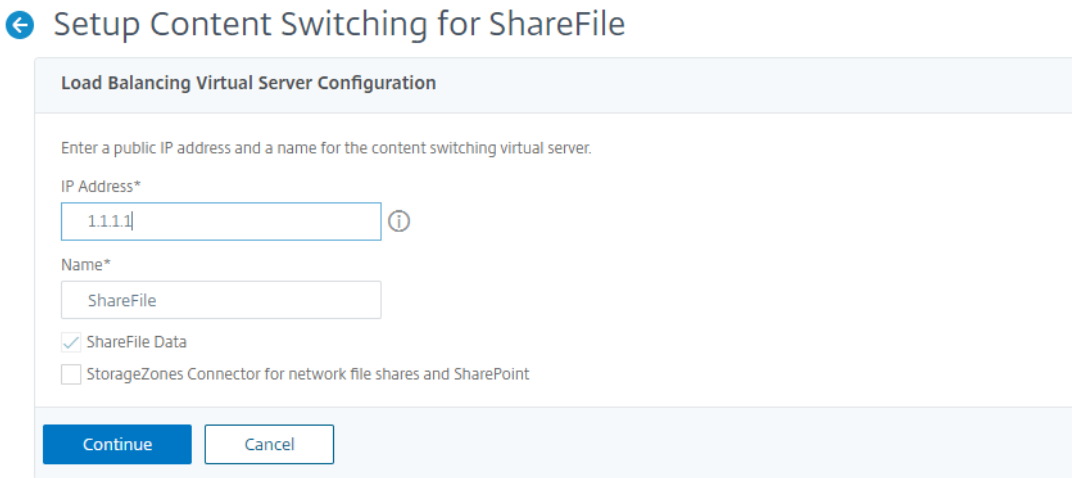


Sie können sich die virtuellen Lastausgleichsserver ansehen, die der ShareFile-Assistent erstellt, indem Sie zu **Traffic Management > Virtuelle Server und**Dienste > Virtuelle**Server**navigieren. Sie können die mit dem ShareFile-Assistenten erstellten virtuellen Server nicht manuell entfernen. Verwenden Sie den Assistenten, um die virtuellen Server zu entfernen.

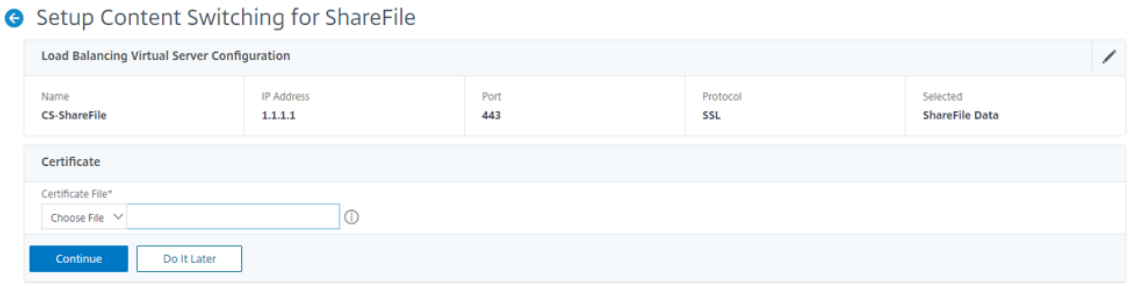
NetScaler verwendet die LDAP-Authentifizierung für SharePoint- oder CIFS-Anfragen. Die Hash-Authentifizierung wird für die Authentifizierung von Anfragen für StorageZones verwendet.

So konfigurieren Sie eine NetScaler-Appliance für den Lastenausgleich: Citrix ShareFile

1. Klicken Sie im Navigationsbereich auf **Traffic Management**.
2. Klicken Sie im Abschnitt **Citrix ShareFile** auf **NetScaler for ShareFile einrichten**.
3. Geben Sie auf der Seite **„Content Switching für ShareFile einrichten** “ die folgenden Informationen ein:
   - IP-Adresse: IP-Adresse des virtuellen Content Switching-Servers.
   - Name: Name des virtuellen Content Switching-Servers.
   - Wenn Sie Load Balancing für CIFS oder SharePoint einrichten möchten, klicken Sie auf das Kontrollkästchen **StorageZone Connector for Network File Shares/SharePoint**, und klicken Sie dann auf **Weiter**. Standardmäßig ist das Kontrollkästchen **ShareFile-Daten** aktiviert.

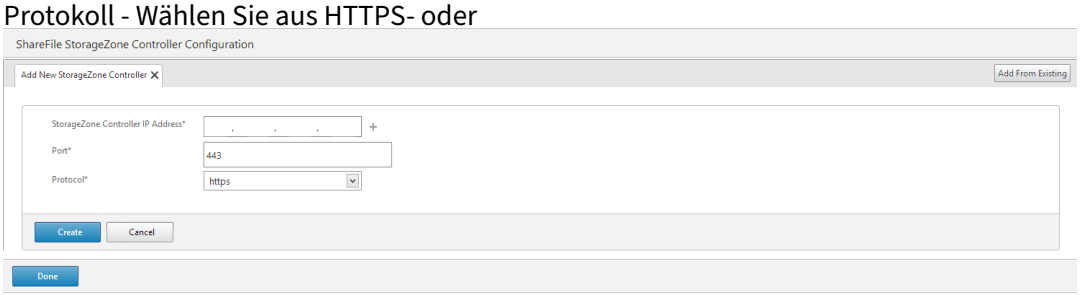


4. Geben Sie ein gültiges Zertifikat ein. Wenn Sie ein Zertifikat haben, klicken Sie auf **Choose Certificate und wählen** Sie in der Dropdownliste das Zertifikat aus. Wenn Sie ein Zertifikat installieren müssen, klicken Sie auf **Zertifikat installieren** und geben Sie das Zertifikatsschlüssel-

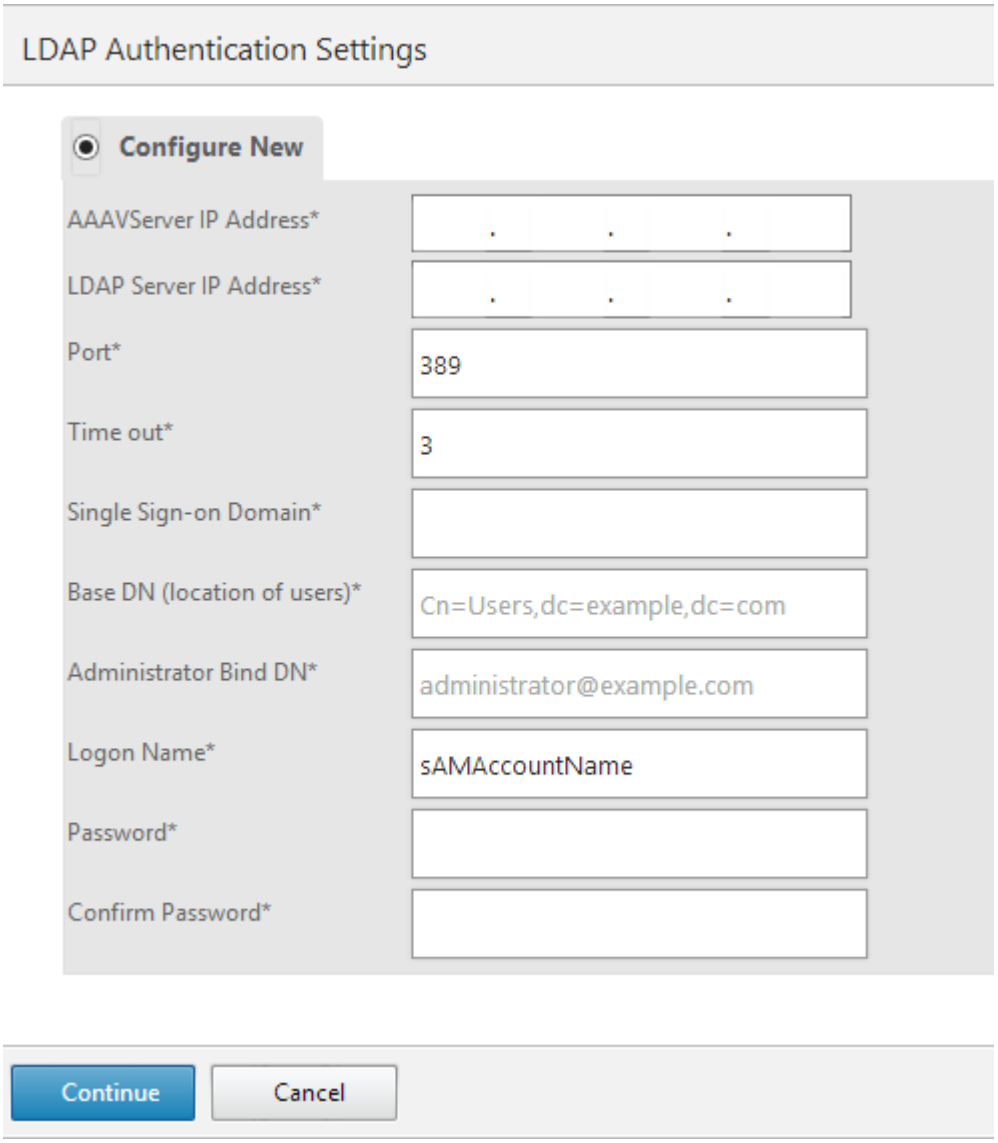


paar ein.

5. Klicken Sie auf **Weiter**.
6. **Geben Sie im Dialogfeld Neuen StorageZone-Controller hinzufügen** die Werte der folgenden Parameter an:
   - IP-Adresse des StorageZone Controllers — IP-Adresse
   - Port — Portnummer. Der Standardwert ist 443.
   - Protokoll - Wählen Sie aus HTTPS- oder



7. Klicken Sie auf **Erstellen** und dann auf **Fertig**. Der Assistent erstellt automatisch einen Dienst und generiert automatisch den Namen des Dienstes.
8. Wenn Sie den Lastenausgleich für CIFS oder SharePoint in Schritt 4.c ausgewählt haben, geben Sie die Werte für LDAP-Authentifizierungseinstellungen an:
   - IP-Adresse des virtuellen NetScaler AAA-Servers - IP-Adresse des virtuellen NetScaler AAA-Servers
   - LDAP-Server-IP-Adresse — IP-Adresse des LDAP-Servers
   - Port — Portnummer. Der Standardwert ist 389
   - Timeout - Der Timeout-Wert in Minuten
   - Single Sign-On-Domäne — Single-Sign-On-Domänenname
   - Basis-DN — Basisdomänenname
   - Administrator Bind DN — LDAP-Kontoname mit dem Domainnamen, z. B. administrator@domainname.com
   - Anmeldename - Anmeldename ist der samAccountName
   - Kennwort und Kennwort bestätigen - Geben Sie das Kennwort ein und bestätigen Sie das Kennwort



9. Klicken Sie auf **Weiter** und dann auf **Fertig**.

So entfernen Sie die Load-Balancing-Konfiguration für ShareFile

1. Klicken Sie im Navigationsbereich auf **Traffic Management**.
2. Klicken Sie im Abschnitt **Citrix ShareFile** auf **ShareFile-Konfiguration entfernen**.

Anwendungsfall 15: Layer-4-Lastausgleich auf der NetScaler-Appliance konfigurieren

May 11, 2023

Der Layer-4-Load Balancer (TCP- und UDP-Ports) verwendet Informationen, die in der Netzwerktransportschicht bereitgestellt werden, um Clientanforderungen über die Servergruppen hinweg zu leiten.

Wenn eine Layer-4-Verbindung zwischen einem Client und einem Server hergestellt wird, hat sie eine Paketansicht des zwischen ihnen ausgetauschten Datenverkehrs. Der Layer-4-Load Balancer trifft seine Routing-Entscheidungen basierend auf den Adressinformationen, die aus den ersten Paketen im TCP-Stream extrahiert wurden, und prüft den Paketinhalt nicht. Daher wird der Lastenausgleich der Layer 4 auch als verbindungsbasierter Lastausgleich bezeichnet.

Der Layer-4-Load-Balancer überwacht den Zustand eines Servers. Der Verkehr wird nicht an den Server weitergeleitet, wenn er DOWN ist.

Der Layer-4-Lastenausgleich ist für verschiedene Anwendungen nützlich, die TCP- oder UDP-Nutzlasten verwenden. Solche Protokolle tauschen Daten als TCP-Nutzlast aus und haben keine bestimmte Struktur, der sie folgen müssen.

So konfigurieren Sie den Lastenausgleich auf Layer 4 über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

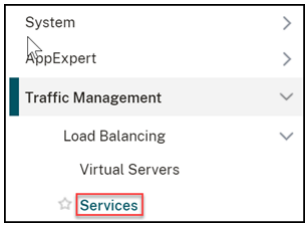
```
add service <name> <serverName> <serviceType> <port>
add lb vserver <name> <serviceType> <ip> <port>
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
add service TCPservice 192.0.2.3 TCP 1
add lb vserver TCPserver TCP 192.0.2.4 1
bind lb vserver TCPserver TCPservice
<!--NeedCopy-->
```

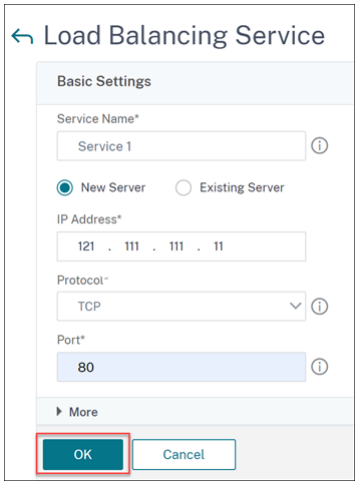
So konfigurieren Sie Layer-4-Lastenausgleich über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.



2. Klicken Sie auf **Hinzufügen** zu einem Dienst erstellen.
3. Geben Sie die erforderlichen Details unter **Dienstname** und **IP-Adresse**an.

4. Wählen Sie im **Protokoll** entweder **TCPoder UDP**aus.
5. Klicken Sie auf **OK**.



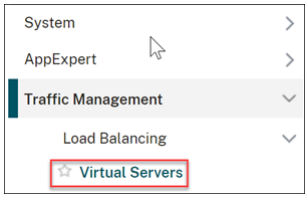
6. Klicken Sie auf **Fertig**.

   Ein Dienst wird erstellt.

   Wenn Sie einen Dienst mit UDP als Transportschichtprotokoll erstellen, wird automatisch ein Ping-Monitor (integrierter Monitor) an den Dienst gebunden. Wenn Sie einen Dienst mit TCP als Transportschichtprotokoll erstellen, wird ein **tcp_default-Monitor** automatisch an den Dienst gebunden.

   Für das Lastausgleichs-Setup können Sie Ihren Dienst an einen anderen Monitortyp oder mehrere Monitore binden. Für Vorabüberwachungsanforderungen können Sie den **tcp-ecv-Monitor** verwenden und die Anforderungs- und Antwortnachrichten konfigurieren.

7. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.

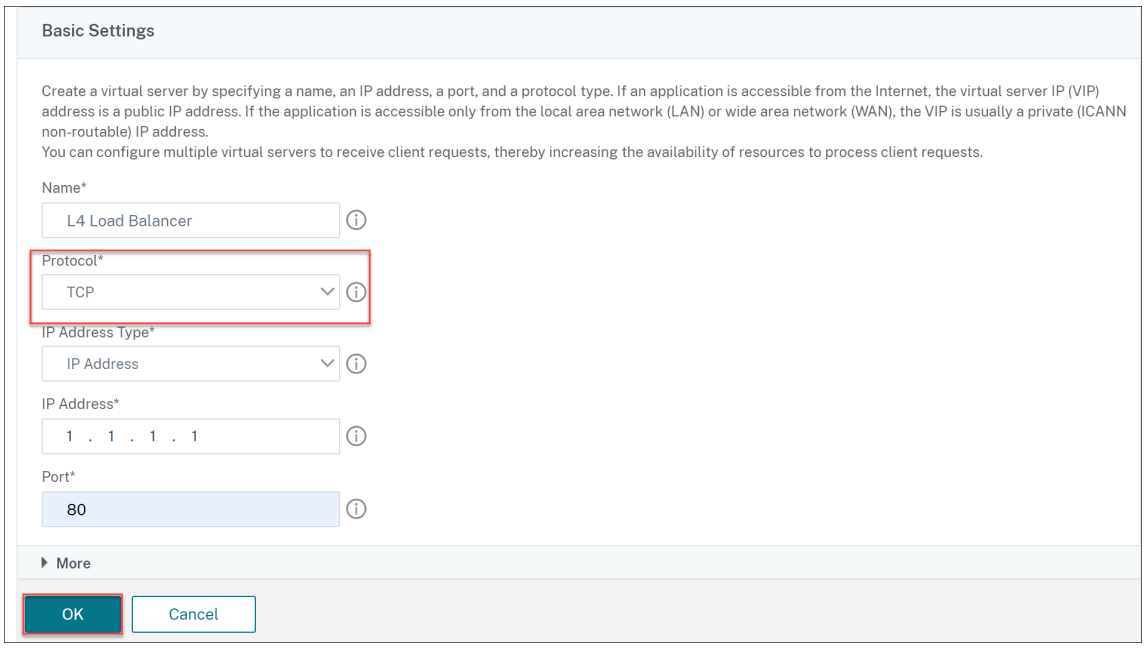


8. Klicken Sie auf **Hinzufügen**, um einen neuen virtuellen Server zu erstellen.

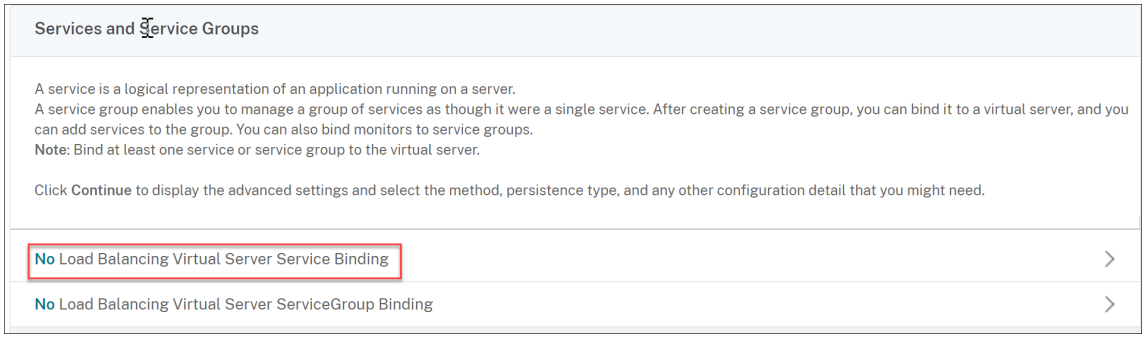
   Wenn der Lastausgleich konfiguriert ist, können Sie über die IP-Adresse oder den FQDN des virtuellen Servers eine Verbindung zur Website, Anwendung oder zum Server mit Lastausgleich herstellen.

9. Geben Sie die erforderlichen Details unter **Name**, **IP-Adresstyp**und **IP-Adresse**an.
10. Wählen Sie im **Protokoll** entweder **TCPoder UDP**aus.
11. Geben Sie eine Portnummer (0—1023 basierend auf der Art des Dienstes) in **Port**ein.

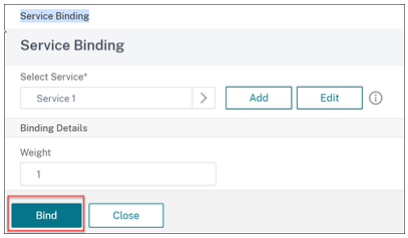
12. Klicken Sie auf **OK**.



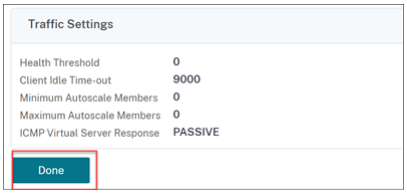
13. Klicken Sie auf **Kein Load Balancing Virtual Server Service Binding** in **Dienste und Dienstgruppen**.



14. Wählen Sie auf der Seite **Dienstbindung** unter **Dienst auswählen die Option Zum Auswählenklickenaus**.
15. Wählen Sie den zu gebundenen Dienst aus und klicken Sie auf **Auswählen**.
16. Klicken Sie auf **Bind**, um den Dienst an den virtuellen Server zu binden.



17. Klicken Sie auf **Weiter**.
18. Klicken Sie auf **Fertig**.



Die Konfiguration des virtuellen Layer-4-Servers für den Lastausgleich ist abgeschlossen.

Problembehandlung

May 11, 2023

Wenn der Lastenausgleich nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf NetScaler-Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Problembehandlung beim Load Balancing

Optimale Ergebnisse erzielen Sie, wenn Sie die folgenden Ressourcen verwenden, um ein Problem mit dem Content Switching auf einer NetScaler-Appliance zu beheben:

- Neueste ns.conf-Datei
- Relevante `newnslog` Dateien
- Ätherische Paketspuren, die auf der Appliance und dem relevanten Client aufgezeichnet werden, wenn möglich
- Die Datei ns.log

Zusätzlich zu den oben genannten Ressourcen beschleunigen die folgenden Tools die Fehlerbehebung:

- Ein Browser-Add-On-Tool, das HTTP-Header anzeigen kann. Dies kann zur Behebung von Persistenzproblemen verwendet werden.
- Die Wireshark-Anwendung, die für die NetScaler-Trace-Dateien angepasst wurde.

Behebung von Load-Balancing-Problemen

- **Problem**

Die CPU-Auslastung erreicht 100%, wenn ein Benutzermonitor an einen Dienst gebunden ist, der an einen virtuellen Server gebunden ist, auf dem die MAC-Option -m aktiviert ist.

- **Auflösung**

Binden Sie einen Monitor, der kein Benutzer ist, an den Dienst.

- **Problem**

  Ich habe ein Benutzerskript für die Überwachung erstellt, aber es funktioniert nicht.

  Auflösung

  Überprüfen Sie die Anzahl der Argumente im Skript. Das Limit liegt bei 512. Ein Skript mit mehr als 512 Argumenten funktioniert möglicherweise nicht richtig. Verwenden Sie das nsumon-debug.pl-Skript von der CLI aus, um das Skript zu debuggen.

- **Problem**

  Ich sehe viele Monitorsonden, und sie scheinen den Netzwerkverkehr unnötig zu erhöhen. Gibt es eine Möglichkeit, die Monitorsonden auszuschalten?

  Auflösung

  Sie können die Monitor-Sondeverbindungen deaktivieren, indem Sie den Monitor deaktivieren oder den Wert des HealthMonitor-Parameters im Befehl set service auf NO einstellen. Mit der Option NO zeigt die Appliance den Dienst jederzeit als UP an.

- **Problem**

  Ich habe Monitore für Dienste eingerichtet, aber Verbindungen werden immer noch zu Servern geleitet, die AUSGEFALLEN sind.

  Auflösung

  Wahrscheinlich müssen Sie die Intervalle der Monitorsonden verringern. Die NetScaler-Appliance erkennt den Status DOWN erst, wenn der Monitor eine Sonde sendet.

- **Problem**

  Eine an den Monitor gebundene Metrik ist in den lokalen und benutzerdefinierten Metriktabellen vorhanden.

  Auflösung

  Fügen Sie dem Metriknamen das lokale Präfix hinzu, wenn die Metrik aus der lokalen Metriktabelle ausgewählt wurde. Wenn die Metrik jedoch aus der benutzerdefinierten Tabelle ausgewählt wird, müssen Sie kein Präfix hinzufügen.

- **Problem**

  Die Monitorproben zu einem Dienst erreichen den Dienst nicht.

  Auflösung

  Prüfen Sie, ob Sie ein Limit für die Anzahl der Verbindungen für einen Dienst festgelegt haben. Falls ja, nehmen Sie Monitor-Probe-Verbindungen von dieser Beschränkung aus, indem Sie den Parameter MonitorSkipMaxClient auf ENABLED setzen.

- **Problem**

  Ich kann die Server anpingen, aber der Status der Dienste wird immer als DOWN angezeigt.

  Auflösung

  Überprüfen Sie den konfigurierten Monitortyp. Wenn beispielsweise ein Server nicht für SSL konfiguriert ist und Sie einen HTTPS-Monitor verwenden, wird der Status des Dienstes als DOWN markiert. In diesem Fall muss die Verwendung eines TCP-Monitors den Status des Dienstes in UP ändern.

- **Problem**

  Das Festlegen eines Gewichts für Lastmessgeräte hilft nicht bei der Entscheidung über den Status des Dienstes.

  Auflösung

  Lastmonitore können nicht über den Status des Dienstes entscheiden. Daher ist es unangemessen, ein Gewicht auf den Lastmonitoren festzulegen.

- **Problem**

  Ein Dienst ist nicht stabil.

  Auflösung

  Erwägen Sie, die folgenden Komponenten zu beheben:

  - Stellen Sie sicher, dass ein korrekter Server an den Dienst gebunden ist.
  - Überprüfen Sie den Monitortyp, der an den Dienst gebunden ist.
  - Überprüfen Sie die Gründe für die Monitorfehler. Sie können einen Dienst auf der Seite Dienste öffnen und die Details zur Anzahl der Prüfungen, Ausfälle und den letzten Antwortstatus für den Monitor auf der Registerkarte Monitore des Dialogfelds Service konfigurieren überprüfen. Um die Details anzuzeigen, klicken Sie auf den konfigurierten Monitor.
  - Wenn es sich um einen benutzerdefinierten Monitor handelt, binden Sie einen TCP- oder Ping-Monitor an den Dienst und überprüfen Sie den Status des Monitors. Wenn das Problem dadurch behoben wird, liegt ein Problem mit dem benutzerdefinierten Monitor vor, und der Monitor muss weiter untersucht werden.
  - Sie können Paketspuren auf der NetScaler-Appliance aufzeichnen und die Monitorproben und die Serverantwort für weitere Untersuchungen überprüfen.

- **Problem**

  Die virtuelle IP-Adresse (VIP) ist nicht stabil oder ihr Status wird als DOWN angezeigt.

  Auflösung

  Erwägen Sie, die folgenden Komponenten zu beheben:

  - Stellen Sie sicher, dass die Load-Balancing-Funktion lizenziert ist.

- Stellen Sie sicher, dass die Funktion aktiviert ist.
- Stellen Sie sicher, dass ein geeigneter Dienst an den virtuellen Server gebunden ist.
- Wenn der Status der VIP-Adresse als DOWN angezeigt wird, stellen Sie sicher, dass der Dienst von einem Administrator aktiviert wurde. Ist dies nicht der Fall, muss der Status des Dienstes Out-Of-Service sein. In einem solchen Fall müssen Sie den Dienst aktivieren und überprüfen, ob das Problem behoben ist.
- Überprüfen Sie die Dienste, die an den virtuellen Server gebunden sind, und führen Sie die Schritte zur Fehlerbehebung durch, die für das Problem nicht stabil sind.
- Wenn die VIP-Adresse nicht stabil ist, müssen alle an den virtuellen Server gebundenen Dienste fehlschlagen. Überprüfen Sie daher, ob alle Dienste gleichzeitig fehlschlagen. Wenn dies der Fall ist, liegt ein Netzwerkproblem zwischen der NetScaler-Appliance und den Servern vor.

- **Problem**

  Die Website weist einen ungleichmäßigen Lastenausgleich auf.

  Auflösung

  Erwägen Sie, die folgenden Komponenten zu beheben:

  - Überprüfen Sie die auf der Appliance konfigurierte Load-Balancing-Methode.
  - Überprüfen Sie, ob die mit den Diensten verknüpften Gewichte wie erwartet sind.
  - Wenn die Load Balancing-Methode eine andere als Round Robin ist, überprüfen Sie die Anzahl der Verbindungen mit dem in der `newnslog` Datei protokollierten Server. Sie können den folgenden Befehl ausführen, um die Nummer in der `newnslog` Datei zu überprüfen:

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

    Überprüfen Sie die Dienste für den spezifischen virtuellen Server und prüfen Sie die Antwortzeit, Open Etablierte Verbindungen (OE), Anzahl der Anfragen, Persistente Anfragen und die dauerhafte Rate (P), um das Problem weiter zu beheben.
  - Wenn die Load Balancing-Methode Round-Robin ist, überprüfen Sie die dauerhaften Anforderungen wie im vorherigen Schritt erwähnt. Überprüfen Sie außerdem, ob der Dienst nicht stabil ist. Ist dies nicht der Fall, führen Sie die für das Problem „Service nicht stabil“ genannten Schritte zur Fehlerbehebung durch
  - Überprüfen Sie, ob die Persistenz auf der Appliance konfiguriert ist.
  - Überprüfen Sie, ob ein Dienst nicht stabil ist. Wenn ja, führen Sie die Schritte zur Fehlerbehebung durch, die für das Problem nicht stabil aufgeführt sind.

- **Problem**

  Der Dienststatus wird als DOWN angezeigt.

Auflösung

Erwägen Sie, die folgenden Komponenten zu beheben:

- Überprüfen Sie, ob eine SNIP-Adresse konfiguriert ist.
- Stellen Sie sicher, dass die entsprechenden Monitore an den Dienst gebunden sind.
- Wenn benutzerdefinierte Monitore an den Dienst gebunden sind, binden Sie einen TCP- oder Ping-Monitor an den Dienst und überprüfen Sie den Status des Monitors. Wenn das Problem dadurch behoben wird, liegt ein Problem mit dem benutzerdefinierten Monitor vor, und der Monitor muss weiter untersucht werden.
- Überprüfen Sie, ob der Status des Dienstes als DOWN für den Server angezeigt wird, der sich in einem anderen Subnetz befindet. Wenn ja, überprüfen Sie, ob Use Subnet IP (USNIP) das Problem behebt, da dies darauf zurückzuführen sein kann, dass die MIP-Adresse nicht mit dem Server kommunizieren kann.

- **Problem**

  Es gibt ein Problem mit der Reaktionszeit.

  Auflösung

  Erwägen Sie, die folgenden Komponenten zu beheben:

  - Überprüfen Sie die Antwortzeit des Servers anhand der Servicestatistiken, indem Sie entweder den folgenden Befehl ausführen:

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

  - Prüfen Sie, ob der Dienst nicht stabil ist und ob der Dienststatus als DOWN-Probleme angezeigt wird.

- **Problem**

  Einer der Server verarbeitet mehr Anfragen als die anderen Server mit Lastausgleich.

  Auflösung

  Erwägen Sie, die folgenden Komponenten zu beheben:

  - Überprüfen Sie die Load-Balancing-Methode. Verwenden Sie die Round-Robin-Methode, um die Client-Anfrage unabhängig von der Auslastung der Server gleichmäßig zu verteilen.
  - Bestimmen Sie, ob die Persistenz für die Lastausgleichskonfiguration aktiviert ist. Wenn Persistenz aktiviert ist, trägt ein bestimmter Server möglicherweise eine schwerere Last, um seine Sitzung aufrechtzuerhalten, insbesondere Wenn die Persistenzsitzungen lang sind.
  - Überprüfen Sie, ob jedem Dienst Gewichtungen zugewiesen sind. Die Zuweisung der richtigen Gewichte trägt zur richtigen Lastverteilung bei.

- **Problem**

Verbindungen zu einem bestimmten Load-Balancing-Server sind blockiert. Beispielsweise könnten alle Verbindungen zu einem Outlook-Server ins Stocken geraten.

Auflösung

Erwägen Sie, die folgenden Komponenten zu beheben:

- Überprüfen Sie die Load-Balance-Methode. Wenn es sich um Round-Robin-Verfahren handelt, sollten Sie erwägen, die Methode auf die geringste Anzahl von Verbindungen umzustellen.
- Ziehen Sie in Betracht, die Zeitüberschreitung für den Monitor zu reduzieren. Ein kürzerer Timeout-Zeitraum hilft dabei, einen Dienst früher als DOWN zu markieren, was dazu beitragen würde, den Datenverkehr auf den funktionsfähigen Server zu lenken.
- Wenn die Verbindungen über einen längeren Zeitraum ins Stocken geraten sind, kann sich eine Überspannungswarteschlange aufbauen. Erwägen Sie, die Überspannungswarteschlange zu leeren, um einen plötzlichen Anstieg der Belastung des Servers zu vermeiden.
- Wenn die Server auf ihrer maximalen Ebene arbeiten, sollten Sie erwägen, einen neuen Server für eine bessere Leistung hinzuzufügen.

- **Problem**

  Ein Großteil der Verbindungen wird an einen bestimmten Server weitergeleitet, auch wenn die Methode mit den wenigsten Verbindungen für den Lastenausgleich konfiguriert ist.

  Auflösung

  Stellen Sie fest, ob die Persistenz konfiguriert ist und vom Typ Quell-IP ist. Wenn die Quell-IP-Persistenz auch bei der Methode mit den wenigsten Verbindungen konfiguriert ist, gehen die Anfragen an einen bestimmten Server. Die IP-Adresse des Servers ist für die Verwaltung der Sitzungsinformationen erforderlich. Erwägen Sie, HTTP-Cookies basierte Persistenz zu verwenden.

- **Tipps zur Fehlerbehebung**
  Bei anderen Problemen sollten Sie die folgenden Tipps beachten, um ein oben nicht aufgeführtes Problem zu beheben:

  - Wenn mehrere Lastmonitore an einen Dienst gebunden sind, ist die Last auf dem Dienst die Summe aller Werte auf den Lastmonitoren, die an ihn gebunden sind. Damit der Lastenausgleich ordnungsgemäß funktioniert, müssen Sie dieselben Monitore an alle Dienste binden.
  - Wenn Sie einen an den Dienst gebundenen Load Monitor deaktivieren und der Dienst an einen virtuellen Server gebunden ist, verwendet der virtuelle Server die Round-Robin-Methode für den Lastenausgleich.
  - Wenn Sie einen Dienst an einen virtuellen Server binden, auf dem die Lastausgleichsmethode CUSTOMLOAD lautet und der Dienststatus UP lautet, verwendet der virtuelle Server

die erste Roundrobin-Methode für den Lastenausgleich. Es befindet sich weiterhin im Round-Robin, wenn der Dienst keine benutzerdefinierten Lastmonitore hat oder wenn der Status mindestens eines der benutzerdefinierten Lastmonitore nicht UP ist.

- Alle Dienste, die an einen virtuellen Server gebunden sind, auf dem die Lastausgleichsmethode CUSTOMLOAD lautet, müssen die Dienste über Lastüberwachungen verfügen, die an sie gebunden sind.
- Die CUSTOMLOAD Load Balancing-Methode folgt auch dem Start-Rund-Robin.
- Wenn Sie eine metrikbasierte Bindung deaktivieren und dies die letzte aktive Metrik ist, verwendet der spezifische virtuelle Server die Roundrobin-Methode für den Lastenausgleich. Eine Metrik wird deaktiviert, indem der metrische Schwellenwert auf Null gesetzt wird.
- Wenn eine an einen Monitor gebundene Metrik den Schwellenwert überschreitet, wird dieser bestimmte Dienst bei der Lastverteilung nicht berücksichtigt. Wenn alle Dienste den Schwellenwert erreicht haben, verwendet der virtuelle Server die Round-Robin-Methode für den Lastenausgleich und es wird eine Fehlermeldung „5xx — Server ausgelastet Fehler“ angezeigt.
- Maximal 10 Metriken aus einer benutzerdefinierten Tabelle können an den Monitor gebunden werden.
- Die OIDs müssen skalare Variablen sein.
- Für ein erfolgreiches Load-Balancing muss das Intervall so gering wie möglich sein. Wenn das Intervall hoch ist, verlängert sich der Zeitraum für das Abrufen des Lastwerts. Infolgedessen erfolgt der Lastenausgleich unter Verwendung falscher Werte.
- Ein Benutzer kann die lokale Tabelle nicht ändern.

Häufig gestellte Fragen zum Lastausgleich

May 11, 2023

Welche verschiedenen Load-Balancing-Richtlinien kann ich auf der NetScaler-Appliance erstellen?

Sie können die folgenden Arten von Load-Balancing-Richtlinien auf der NetScaler-Appliance erstellen:

- Geringste Verbindungen
- Runde Robin
- Geringste Reaktionszeit
- Geringste Bandbreite
- Wenigste Pakete
- URL-Hashing

- Hashing von Domainnamen
- Hashing der Quell-IP-Adresse
- Hashing der Ziel-IP-Adresse
- Quell-IP — Ziel-IP-Hashing
- Token
- LRTM

Kann ich die Sicherheit der Webfarm erreichen, indem ich Load Balancing mithilfe der NetScaler-Appliance implementiere?

Ja. Sie können die Sicherheit der Webfarm erreichen, indem Sie den Lastenausgleich mithilfe der NetScaler-Appliance implementieren. Mit der NetScaler Appliance können Sie die folgenden Optionen der Load-Balancing-Funktion implementieren:

- Verstecken von IP-Adressen: Ermöglicht es Ihnen, die eigentlichen Server aus Sicherheitsgründen und zur Erhaltung der IP-Adresse so zu installieren, dass sie sich in einem privaten IP-Adressraum befinden. Dieser Prozess ist für den Endbenutzer transparent, da die NetScaler-Appliance Anfragen im Namen des Servers akzeptiert. Im Modus zum Verstecken von Adressen isoliert die Appliance die beiden Netzwerke vollständig. Daher kann ein Client über eine andere VIP auf der Appliance für diesen Dienst auf einen Dienst zugreifen, der im privaten Subnetz ausgeführt wird, z. B. FTP- oder Telnet-Server.
- Portzuordnung: Ermöglicht aus Sicherheitsgründen, dass die tatsächlichen TCP-Dienste auf nicht standardmäßigen Ports gehostet werden. Dieser Vorgang ist für den Endbenutzer transparent, da die NetScaler Appliance Anforderungen im Namen des Servers an die standardmäßige angekündigte IP-Adresse und Portnummer annimmt.

Welche Geräte kann ich zum Lastenausgleich mit einer NetScaler Appliance verwenden?

Sie können die folgenden Geräte mit einer NetScaler Appliance ausgleichen:

- Serverfarmen
- Caches oder Reverse-Proxys
- Firewall-Geräte
- Systeme zur Erkennung von Eindringlingen
- SSL-Offload-Geräte
- Kompressionsgeräte
- Content Inspection Server

Warum implementiere ich die Load Balancing-Funktion für die Website?

Sie können die Funktion Lastenausgleich für die Website implementieren, um folgende Vorteile zu nutzen:

- Verkürzen Sie die Reaktionszeit: Wenn Sie die Load-Balancing-Funktion für die Website implementieren, ist einer der Hauptvorteile die Steigerung der Ladezeit, auf die Sie sich freuen können. Da sich zwei oder mehr Server die Last des Web-Traffics teilen, hat jeder der Server eine geringere Traffic-Last als ein einzelner Server allein. Dies bedeutet, dass mehr Ressourcen zur Verfügung stehen, um die Kundenanfragen zu erfüllen. Dies führt zu einer schnelleren Website.
- Redundanz: Die Implementierung der Load-Balancing-Funktion führt zu einer gewissen Redundanz. Wenn die Website beispielsweise über drei Server ausgeglichen ist und einer von ihnen überhaupt nicht reagiert, können die anderen beiden weiterhin laufen und die Websitebesucher bemerken keine Ausfallzeiten. Jede Load Balancing-Lösung sendet sofort den Datenverkehr an den Back-End-Server, der nicht verfügbar ist.

Warum muss ich die Mac Based Forwarding (MBF) Option für Link Load Balancing (LLB) deaktivieren?

- Wenn Sie die MBF-Option aktivieren, berücksichtigt die NetScaler Appliance, dass der eingehende Datenverkehr vom Client und der ausgehende Datenverkehr zum selben Client über denselben Upstream-Router fließt. Die LLB-Funktion erfordert jedoch den besten Pfad, der für den Rückverkehr gewählt werden muss.
- Das Aktivieren der MBF-Option unterbricht diesen Topologieentwurf, indem der ausgehende Datenverkehr über den Router gesendet wird, der den eingehenden Clientdatenverkehr weitergeleitet hat.

Netzwerke

May 11, 2023

Die folgenden Themen bieten eine konzeptionelle Referenz und Anweisungen zur Konfiguration der verschiedenen Netzwerkkomponenten auf der NetScaler-Appliance.

IP-Adressierung	Lernen Sie die verschiedenen Typen von NetScaler-eigenen IP-Adressen kennen und erfahren Sie, wie Sie diese erstellen, anpassen und entfernen können.

Schnittstellen	Konfigurieren Sie einige der grundlegenden Netzwerkkonfigurationen, die für den Einstieg erforderlich sind.
Zugriffskontrolllisten (ACLs)	Konfigurieren Sie die verschiedenen Arten von Zugriffskontrolllisten und erfahren Sie, wie Sie sie erstellen, anpassen und entfernen.
IP-Routing	Lernen Sie die Routing-Funktionen der NetScaler-Appliance kennen und konfigurieren Sie sie, sowohl statisch als auch dynamisch.
Internetprotokoll Version 6 (IPv6)	Erfahren Sie, wie die NetScaler-Appliance IPv6 unterstützt.
Traffic-Domänen	Lernen Sie Verkehrsdomänen kennen und konfigurieren Sie sie, um den Netzwerkverkehr für verschiedene Anwendungen zu segmentieren.
VXLAN	Lernen und konfigurieren Sie VxLANs, um die Skalierbarkeitsanforderungen in Ihrem Rechenzentrum zu erfüllen.

IP-Adressierung

May 11, 2023

Bevor Sie die NetScaler-Appliance konfigurieren können, müssen Sie die NSIP-Adresse, auch Management-IP-Adresse genannt, zuweisen. Sie können auch andere Netscaler-eigene IP-Adressen erstellen, um Server zu abstrahieren und Verbindungen zu den Servern herzustellen. Bei dieser Art von Konfiguration dient die Appliance als Proxy für die abstrahierten Server. Sie können Verbindungen auch als Proxy verwenden, indem Sie Netzwerkadressübersetzungen (INAT und RNAT) verwenden. Bei der Bereitstellung von Proxy-Verbindungen kann sich die Appliance entweder als Bridging-Gerät (Layer 2) oder als Paketweiterleitungsgerät (Layer 3) verhalten. Um die Paketweiterleitung effizienter zu gestalten, können Sie statische ARP-Einträge konfigurieren. Für IPv6 können Sie die Neighbor Discovery (ND) konfigurieren.

Konfigurieren von IP-Adressen im Besitz von NetScaler

May 11, 2023

Die NetScaler-eigenen IP-Adressen — NSIP-Adresse, virtuelle IP-Adressen (VIPs), Subnetz-IP-Adressen (SNIPs) und Global Server Load Balancing Site IP-Adressen (GSLBIPs) — existieren nur auf der NetScaler-Appliance. Das NSIP identifiziert den NetScaler in Ihrem Netzwerk eindeutig und ermöglicht den Zugriff auf die Appliance. Ein VIP ist eine öffentliche IP-Adresse, an die ein Client Anfragen sendet. Der NetScaler beendet die Client-Verbindung am VIP und initiiert eine Verbindung mit einem Server. Diese neue Verbindung verwendet ein SNIP oder ein MIP als Quell-IP-Adresse für Pakete, die an den Server weitergeleitet werden. Wenn Sie mehrere geografisch verteilte Rechenzentren haben, kann jedes Rechenzentrum durch ein eindeutiges GSLBIP identifiziert werden. Sie können einige Netscaler-eigene IP-Adressen konfigurieren, um Verwaltungsanwendungen Zugriff zu gewähren.

Konfigurieren der NSIP-Adresse

May 11, 2023

Die NSIP-Adresse ist die IP-Adresse, unter der Sie zu Verwaltungszwecken auf die NetScaler-Appliance zugreifen. Die Appliance kann nur ein NSIP haben, das auch als Management-IP-Adresse bezeichnet wird. Sie müssen diese IP-Adresse hinzufügen, wenn Sie den NetScaler zum ersten Mal konfigurieren. Sie können eine NSIP-Adresse nicht entfernen. Aus Sicherheitsgründen sollte es sich bei dem NSIP um eine nicht routbare IP-Adresse im LAN Ihres Unternehmens handeln.

Wenn Sie diese Adresse ändern, müssen Sie die NetScaler-Appliance neu starten. Wenn sich die Subnetzadresse der neuen NSIP-Adresse von der vorherigen unterscheidet, müssen Sie eine Standardroute für dieses Subnetz hinzufügen, damit die neue NSIP-Adresse von anderen Netzwerken im LAN aus erreichbar ist.

> **Wichtig**
>
> Die Konfiguration der NSIP-Adresse ist obligatorisch.

Das Ändern der NSIP-Adresse einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- Ändern Sie die NSIP-Adresse.
- Fügen Sie eine Standardroute für die Subnetzadresse der NSIP-Adresse hinzu, falls keine vorhanden ist.
- Speichern Sie die Konfiguration.
- Starten Sie die Appliance neu.

Befehlszeilenprozeduren

So ändern Sie die NSIP-Adresse mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set ns config -IPAddress** <ip_addr> **-netmask** <netmask>
- **show ns config**

So fügen Sie mit der CLI eine Standardroute hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- **add route 0 0** <gateway IP address>
- **Route zeigen**

Um die Konfiguration mit der CLI zu speichern:

Geben Sie in der Befehlszeile Folgendes ein:

- **Konfiguration speichern**

NetScaler-Appliance mithilfe der CLI neu starten:

Geben Sie in der Befehlszeile Folgendes ein:

- **reboot**

GUI-Prozeduren

NSIP-Adresse mithilfe der GUI konfigurieren:

1. Klicken Sie auf der **Konfigurationsseite** oben rechts auf das Zahnradsymbol.
2. Klicken Sie auf das **NSIP-Adressfenster**.
3. Stellen Sie auf der **NSIP-Adressseite** die folgenden Parameter ein und klicken Sie dann auf **Fertig**:
    - NSIP-Adresse
    - Netzmaske

Um mithilfe der GUI eine Standardroute hinzuzufügen:

Navigieren Sie zu **System** > **Netzwerk** > **Routen** und fügen Sie auf der Registerkarte **Basic** eine Standardroute mit den folgenden Parametereinstellungen hinzu, und klicken Sie dann auf **Erstellen**.

- Netzwerk (auf Null gesetzt)
- Netzmaske (auf Null gesetzt)
- Gateway (IP-Adresse des Gateways)

Um den NetScaler mithilfe der GUI neu zu starten:

1. Klicken Sie auf der Registerkarte **Systeminformationen** des **Systemknotens** auf **Reboot**.
2. Wenn Sie zum Neustart aufgefordert werden, wählen Sie **Konfiguration speichern** aus, um sicherzustellen, dass Sie keine Konfigurationen verlieren.

Beispiel-Konfiguration

Im folgenden Beispiel wird die NSIP-Adresse einer NetScaler-Appliance in 192.0.2.90 geändert, die eine andere Subnetzadresse (192.0.2.0/24) als die vorherige NSIP-Adresse hat. Daher wird eine Standardroute für dieses Subnetz hinzugefügt, so dass die neue NSIP-Adresse von anderen Netzwerken erreichbar ist.

```
> set nsconfig -ipAddress 192.0.2.90 -netmask 255.255.255.0

 Warning: The configuration must be saved and the system rebooted for
    these settings to take effect
> add route 0 0 192.0.2.1

 Warning: The configuration must be saved and the system rebooted for
    these settings to take effect
> save config

 Done
> reboot
```

Virtuelle IP-Adressen (VIP) konfigurieren und verwalten

May 11, 2023

Die Konfiguration einer virtuellen Server-IP-Adresse (VIP) ist bei der Erstkonfiguration des NetScaler nicht erforderlich. Wenn Sie den Lastenausgleich konfigurieren, weisen Sie virtuellen Servern VIP-Adressen zu.

Weitere Informationen zum Konfigurieren eines Load Balancing-Setups finden Sie unter Load Balancing.

In einigen Situationen müssen Sie VIP-Attribute anpassen oder eine VIP-Adresse aktivieren oder deaktivieren. Eine VIP-Adresse ist normalerweise einem virtuellen Server zugeordnet, und einige der VIP-Attribute werden an die Anforderungen des virtuellen Servers angepasst. Sie können denselben virtuellen Server auf mehreren NetScaler-Appliances hosten, die sich in derselben Broadcast-Domäne befinden, indem Sie ARP- und ICMP-Attribute verwenden. Nachdem Sie einen VIP (oder eine beliebige IP-Adresse) hinzugefügt haben, sendet die Appliance ARP-Anfragen und beantwortet sie

dann. VIPs sind die einzigen Netscaler-eigenen IP-Adressen, die deaktiviert werden können. Wenn eine VIP-Adresse deaktiviert ist, fällt der virtuelle Server, der sie verwendet, aus und reagiert nicht auf ARP-, ICMP- oder L4-Dienstanfragen. Als Alternative zur Erstellung einer VIP-Adresse nach der anderen können Sie einen aufeinanderfolgenden Bereich von VIP-Adressen angeben.

Um eine VIP-Adresse mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- füge ns ip <IPAddress><netmask>-type hinzu <type>
- show ns ip <IPAddress>

Beispiel:

```
> add ns ip 10.102.29.59 255.255.255.0 -type VIP
 Done
<!--NeedCopy-->
```

So erstellen Sie mit der CLI eine Reihe von VIP-Adressen:

Geben Sie in der Befehlszeile Folgendes ein:

- füge ns ip <IPAddress><netmask>-type hinzu <type>
- show ns ip <IPAddress>

Beispiel:

```
> add ns ip 10.102.29.[60-64] 255.255.255.0 -type VIP
ip "10.102.29.60" added
ip "10.102.29.61" added
ip "10.102.29.62" added
ip "10.102.29.63" added
ip "10.102.29.64" added
 Done
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie eine IPv4-VIP-Adresse mithilfe der CLI:

Geben Sie an der Befehlszeile einen der folgenden Befehlssätze ein, um einen VIP zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

- aktiviere NS-IP <IPAddress>
- show ns ip <IPAddress>
- deaktiviere NS-IP <IPAddress>
- show ns ip <IPAddress>

Beispiel:


```
> enable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Enabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled
 Done
> disable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Disabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled

 Done
<!--NeedCopy-->
```


So konfigurieren Sie eine VIP-Adresse mithilfe der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**und fügen Sie eine neue IP-Adresse hinzu oder bearbeiten Sie eine bestehende Adresse.

Um eine Reihe von VIP-Adressen mithilfe der GUI zu erstellen:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Wählen Sie in der **Aktionsliste** die Option **Bereich hinzufügen**aus.

Um eine VIP-Adresse mithilfe der GUI zu aktivieren oder zu deaktivieren:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie eine VIP-Adresse aus.
   - Halten Sie die **Strg-Taste gedrückt** und wählen Sie mehrere Serveradresseinträge aus.
   - Halten Sie die **Umschalttaste gedrückt** und wählen Sie einen Bereich von Serveradresseinträgen aus.
   - Wählen Sie alle Adressen aus, indem Sie das Kontrollkästchen auf der linken Seite der Kopfzeile aktivieren.
3. Wählen Sie in der **Aktionsliste** die Option **Deaktivieren** oder **Aktivieren**aus.

Erkennung einer NetScaler-Appliance in einem UDP-Load-Balancing-Setup durch TTL-Updates

Die folgende Tabelle zeigt, wie eine NetScaler-Appliance den TTL-Wert empfangener Pakete in verschiedenen Funktionen verarbeitet.

Funktionalität	TTL-Wert
Virtueller Server	TTL ist auf 255 gesetzt, wenn die Anfrage an die Backend-Server weitergeleitet wird. TTL wird um 1 verringert, wenn die Antwort an den Client weitergeleitet wird.
L2-Modus	TTL wird nicht geändert.
L3-Modus	TTL ist auf 255 gesetzt.
INAT	TTL ist auf 255 gesetzt, wenn die Anfrage an den Backend-Server weitergeleitet wird. TTL wird um 1 verringert, wenn die Antwort an den Client weitergeleitet wird.

In einigen Unternehmen/Szenarien, in denen eine Überwachungsanwendung ausgeführt wird, muss

die NetScaler-Appliance eines Load-Balancing-Setups als eines der Hop in einer Traceroute erkannt werden. Eine NetScaler-Appliance eines Load-Balancing-Setups wird in einer Traceroute nicht erkannt, da die Appliance den TTL-Wert standardmäßig auf 255 setzt, anstatt ihn zu verringern, wenn die Anfrage an einen Backend-Server weitergeleitet wird.

Um diese Anforderung zu erfüllen, kann der **TTL-Parameter Decrement** einer VIP-Adresse verwendet werden. Dieser Parameter gilt für alle virtuellen UDP-Server, die diesen VIP verwenden.

Wenn Sie den Parameter **Decrement TTL** eines VIP aktivieren, verringert die NetScaler-Appliance den TTL-Wert um 1, anstatt ihn auf 255 zu setzen, wenn Anfragen weitergeleitet werden, die auf den virtuellen UDP-Servern empfangen werden, die diesen VIP verwenden.

Überwachungsanwendungen, die Traceroute-Daten verwenden, können nun erkennen, ob eine NetScaler-Appliance oder ein UDP-Load-Balancing-Setup vorhanden ist.

Bevor du anfängst

Bevor Sie beginnen, eine NetScaler-Appliance so zu konfigurieren, dass sie in einer Traceroute eines Load Balancing-Setups erkannt wird, beachten Sie die folgenden Punkte:

- Der TTL-Parameter Decrement wird nur für virtuelle UDP-Lastausgleichsserver unterstützt.
- Der TTL-Parameter Decrement wird sowohl für IPv4-VIP- als auch für IPv6-VIP- (VIP6) -Adressen unterstützt.
- Der TTL-Parameter Decrement wird für eigenständige NetScaler-Appliances sowie für Hochverfügbarkeits- (HA) und Cluster-Setups unterstützt.

Konfigurationsschritte

Die Konfiguration einer NetScaler-Appliance, die in einer Traceroute eines UDP-Load-Balancing-Setups erkannt wird, umfasst die folgenden Aufgaben:

- Erstellen Sie eine UDP-Load-Balancing-Konfiguration
- Aktivieren Sie den TTL-Parameter Decrement für die VIP-Adresse

CLI-Verfahren

Um die TTL-Option zur Erhöhung des TTL-Werts für eine VIP-Adresse mit der CLI zu aktivieren:

- Um die TTL-Option für eine VIP-Adresse zu aktivieren und gleichzeitig die VIP-Adresse hinzuzufügen, geben Sie in der Befehlszeile Folgendes ein:
  - **ns-IP hinzufügen** <ip><mask>-**Typ VIP** -**DecrementTTL**ENABLED
  - **show ns ip** <VIP address>
- Um die TTL-Option für eine bestehende VIP-Adresse zu aktivieren, geben Sie in der Befehlszeile Folgendes ein:

- **set ns ip** <ip> <mask> -**decrementTTL ENABLED**
- **show ns ip** <VIP address>

Gehen Sie wie folgt vor, um die TTL-Option für eine VIP6-Adresse zu aktivieren, indem Sie die CLI verwenden:

- Um die TTL-Option für eine VIP6-Adresse zu aktivieren und gleichzeitig die VIP6-Adresse hinzuzufügen, geben Sie in der Befehlszeile Folgendes ein:
  - **add ns ip6** <IP6/prefix> <mask> -**type VIP** -**decrementTTL ENABLED**
  - **show ns ip6** <VIP6/prefix>
- Um die TTL-Option für eine bestehende VIP6-Adresse zu aktivieren, geben Sie in der Befehlszeile Folgendes ein:
  - **set ns ip6** <ip6/prefix> <mask> -**decrementTTL ENABLED**
  - **show ns ip6** <VIP6 address>

```
1     > add ns ip 203.0.113.30 -type VIP -decrementTTL ENABLED
2      Done
3
4     > add ns ip6  2001:DB8:5001::30 -type VIP -decrementTTL ENABLED
5      Done
6 <!--NeedCopy-->
```

GUI-Prozeduren

Um die TTL-Option zur Erhöhung des TTL-Werts für eine VIP-Adresse mithilfe der GUI zu aktivieren:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**und aktivieren Sie den Parameter **Decrement TTL**, während Sie eine neue VIP-Adresse hinzufügen oder eine bestehende Adresse bearbeiten.

Um die TTL-Option zur Erhöhung des TTL-Werts für eine VIP6-Adresse mithilfe der GUI zu aktivieren:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv6s**und aktivieren Sie den Parameter **Decrement TTL**, während Sie eine neue VIP6-Adresse hinzufügen oder eine bestehende Adresse bearbeiten.

ARP-Antwortunterdrückung für virtuelle IP-Adressen (VIPs) konfigurieren

May 11, 2023

Sie können die NetScaler-Appliance so konfigurieren, dass sie auf ARP-Anfragen für eine virtuelle IP-Adresse (VIP) reagiert oder nicht, und zwar auf der Grundlage des Status der virtuellen Server, die diesem VIP zugeordnet sind.

Wenn virtuelle Server V1 vom Typ HTTP und V2 vom Typ HTTPS die VIP-Adresse 10.102.29.45 auf einer NetScaler-Appliance gemeinsam nutzen, können Sie die Appliance so konfigurieren, dass sie auf keine ARP-Anfrage für VIP 10.102.29.45 reagiert, wenn sich sowohl V1 als auch V2 im Status DOWN befinden.

Die folgenden drei Optionen sind für die Konfiguration der ARP-Antwortunterdrückung für eine virtuelle IP-Adresse verfügbar.

- **KEINE**. Die NetScaler-Appliance reagiert auf jede ARP-Anfrage für die VIP-Adresse, unabhängig vom Status der virtuellen Server, die der Adresse zugeordnet sind.
- **EIN VSERVER.** Die NetScaler-Appliance reagiert auf jede ARP-Anfrage für die VIP-Adresse, wenn sich mindestens einer der zugehörigen virtuellen Server im Status UP befindet.
- **ALLES VSERVER.** Die NetScaler-Appliance reagiert auf jede ARP-Anfrage für die VIP-Adresse, wenn sich alle zugehörigen virtuellen Server im Status UP befinden.

Die folgende Tabelle zeigt das Beispielverhalten der NetScaler-Appliance für ein VIP, das mit zwei virtuellen Servern konfiguriert ist:

Assoziierte virtuelle Server für einen VIP	BUNDESSTAAT 1	BUNDESSTAAT 2	BUNDESSTAAT 3	BUNDESSTAAT 4
NONE				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Auf eine ARP-Anfrage für diesen VIP antworten?	Ja	Ja	Ja	Ja
EIN VSERVER				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Auf eine ARP-Anfrage für diesen VIP antworten?	Ja	Ja	Ja	Nein
ALLE VSERVER				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN

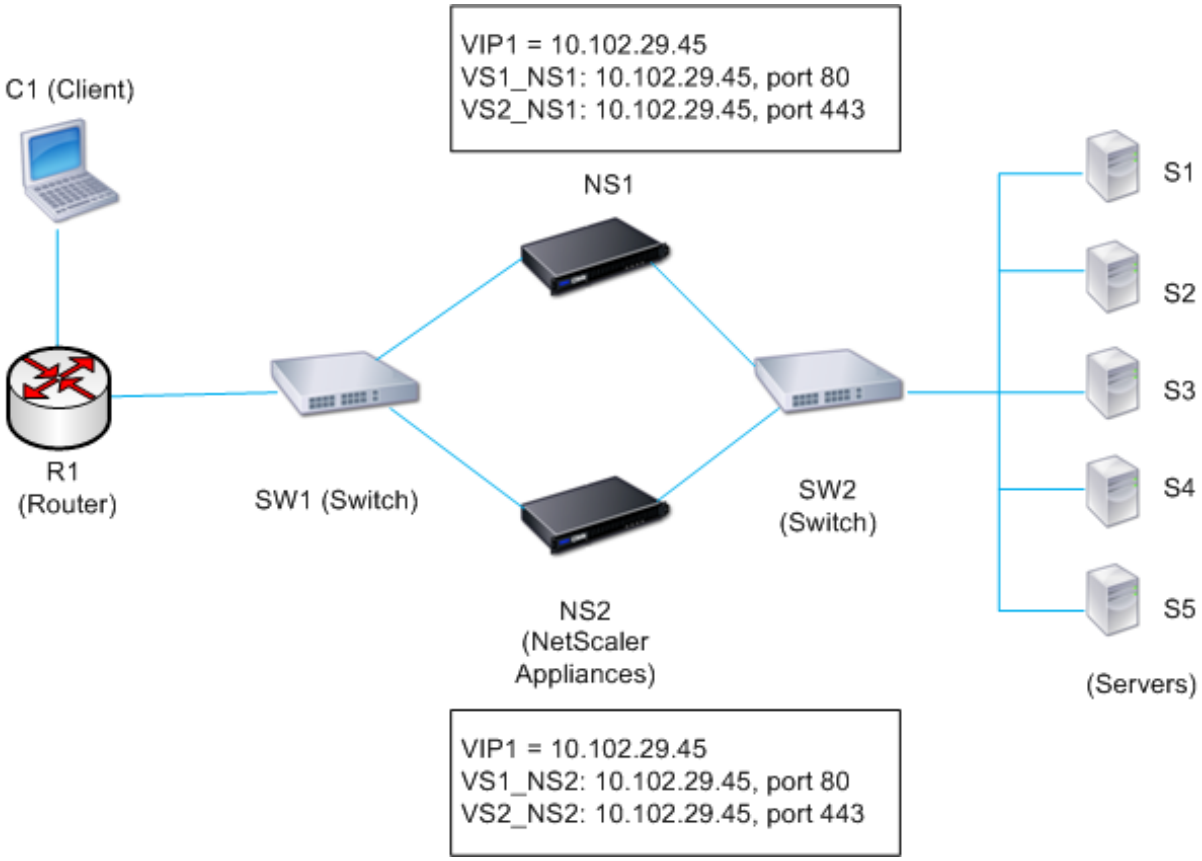
Assoziierte virtuelle Server für einen VIP	BUNDESSTAAT 1	BUNDESSTAAT 2	BUNDESSTAAT 3	BUNDESSTAAT 4
Auf eine ARP-Anfrage für diesen VIP antworten?	Ja	Nein	Nein	Nein

Stellen Sie sich ein Beispiel vor, in dem Sie die Leistung von zwei virtuellen Servern, V1 und V2, testen möchten, die dieselbe VIP-Adresse haben, aber von unterschiedlichen Typen sind und jeweils auf den NetScaler-Appliances NS1 und NS2 konfiguriert sind. Nennen wir die gemeinsame VIP-Adresse *VIP1*.

V1 verteilt die Server S1, S2 und S3. V2 verteilt die Server S4 und S5.

Sowohl auf NS1 als auch auf NS2 ist für VIP1 der ARP-Unterdrückungsparameter auf ALL_VSERVER gesetzt. Wenn Sie die Leistung von V1 und V2 auf NS1 testen möchten, müssen Sie V1 und V2 auf NS2 manuell deaktivieren, damit NS2 auf keine ARP-Anfrage für VIP1 reagiert.

Abbildung 1.



Der Ausführungsablauf sieht wie folgt aus:

1. Client C1 sendet eine Anfrage an V1. Die Anfrage erreicht R1.
2. R1 hat keinen APR-Eintrag für die IP-Adresse (VIP1) von V1, daher sendet R1 eine ARP-Anfrage für VIP1.
3. NS1 antwortet mit der Quell-MAC-Adresse MAC1 und der Quell-IP-Adresse VIP1. NS2 antwortet nicht auf die ARP-Anfrage.
4. SW1 lernt den Port für VIP1 aus der ARP-Antwort und aktualisiert seine Bridgetabelle, und R1 aktualisiert den ARP-Eintrag mit MAC1 und VIP1.
5. R1 leitet das Paket an die Adresse VIP1 auf NS1 weiter.
6. Der Load-Balancing-Algorithmus von NS1 wählt Server S2 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S2. Wenn S2 eine Antwort an den Client sendet, kehrt die Antwort über denselben Pfad zurück.
7. Jetzt möchten Sie die Leistung von V1 und V2 auf NS2 testen, also aktivieren Sie V1 und V2 auf NS2 und deaktivieren sie auf NS1. NS2 sendet jetzt eine ARP-Nachricht für VIP1. In der Nachricht ist MAC2 die Quell-MAC-Adresse und VIP1 ist die Quell-IP-Adresse.
8. SW1 ermittelt die Portnummer für das Erreichen von MAC2 aus dem ARP-Broadcast und aktualisiert seine Bridge-Tabelle, um nachfolgende Client-Anforderungen für VIP1 an NS2 zu senden. R1 aktualisiert seine ARP-Tabelle.
9. Nehmen wir nun an, dass der ARP-Eintrag für VIP1 in der ARP-Tabelle von R1 zu einem Timeout kommt und Client C1 eine Anfrage für V1 sendet. Da R1 keinen APR-Eintrag für VIP1 hat, sendet es eine ARP-Anfrage für VIP1.
10. NS2 antwortet mit einer Quell-MAC-Adresse und VIP1 als Quell-IP-Adresse. NS1 antwortet nicht auf die ARP-Anfrage.

So konfigurieren Sie die ARP-Antwortunterdrückung mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set ns ip** -**arpResponse** <arpResponse>]
- **sh ns ip** <IPAddress>

Beispiel:

```
1 > set ns ip 10.102.29.96 -arpResponse ALL_VSERVERS
2  Done
3 <!--NeedCopy-->
```

So konfigurieren Sie die ARP-Antwortunterdrückung mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Öffnen Sie einen IP-Adresseintrag und wählen Sie den Typ der ARP-Antwort aus.

Subnetz-IP-Adressen (SNIPs) konfigurieren

May 11, 2023

Eine Subnetz-IP-Adresse (SNIP) ist eine NetScaler-eigene IP-Adresse, die vom NetScaler für die Kommunikation mit den Servern verwendet wird.

Der NetScaler verwendet die Subnetz-IP-Adresse als Quell-IP-Adresse, um Client-Verbindungen zu Servern als Proxy zu verwenden. Es verwendet auch die Subnetz-IP-Adresse, wenn es seine eigenen Pakete generiert, z. B. Pakete, die sich auf dynamische Routing-Protokolle beziehen, oder um Monitorproben zu senden, um den Zustand der Server zu überprüfen. Abhängig von Ihrer Netzwerktopologie müssen Sie möglicherweise einen oder mehrere SNIPs für verschiedene Szenarien konfigurieren.

Um eine SNIP-Adresse auf einem NetScaler zu konfigurieren, fügen Sie die SNIP-Adresse hinzu und aktivieren dann den globalen Modus Use Subnet IP (USNIP). Als Alternative zur Erstellung von SNIPs einzeln können Sie einen aufeinanderfolgenden Bereich von SNIPs angeben.

So konfigurieren Sie eine SNIP-Adresse mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- add ns ip <IPAddress> <netmask> -type SNIP
- show ns ip <IPAddress>

Beispiel:

```
> add ns ip 10.102.29.203 255.255.255.0 -type SNIP
 Done
<!--NeedCopy-->
```

Um einen Bereich von SNIP-Adressen mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- add ns ip <IPAddress> <netmask> -type SNIP
- show ns ip <IPAddress>

Beispiel:

```
> add ns ip 10.102.29.[205-209] 255.255.255.0 -type SNIP
ip "10.102.29.205" added
ip "10.102.29.206" added
ip "10.102.29.207" added
ip "10.102.29.208" added
ip "10.102.29.209" added
 Done
<!--NeedCopy-->
```


So aktivieren oder deaktivieren Sie den USNIP-Modus mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns modeUSNIP
- disable ns modeUSNIP

So konfigurieren Sie eine SNIP-Adresse mithilfe der GUI:

Navigieren Sie zu System > Netzwerk > IPs > IPv4s und fügen Sie eine neue SNIP-Adresse hinzu oder bearbeiten Sie eine bestehende Adresse.

Um einen Bereich von SNIP-Adressen mithilfe der GUI zu erstellen:

1. Navigieren Sie zu System > Netzwerk > IPs > IPv4s.
2. Wählen Sie in der Aktionsliste die Option Bereich hinzufügen aus.

So aktivieren oder deaktivieren Sie den USNIP-Modus mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns mode USNIP
- disable ns mode USNIP

Um den USNIP-Modus mithilfe der GUI zu aktivieren oder zu deaktivieren:

1. Navigieren Sie zu System > Einstellungen und klicken Sie in der Gruppe Modi und Funktionen auf Modi ändern.
2. Aktivieren oder deaktivieren Sie die Option Subnetz-IP verwenden.

Verwenden von SNIPs für ein direkt verbundenes Serversubnetz

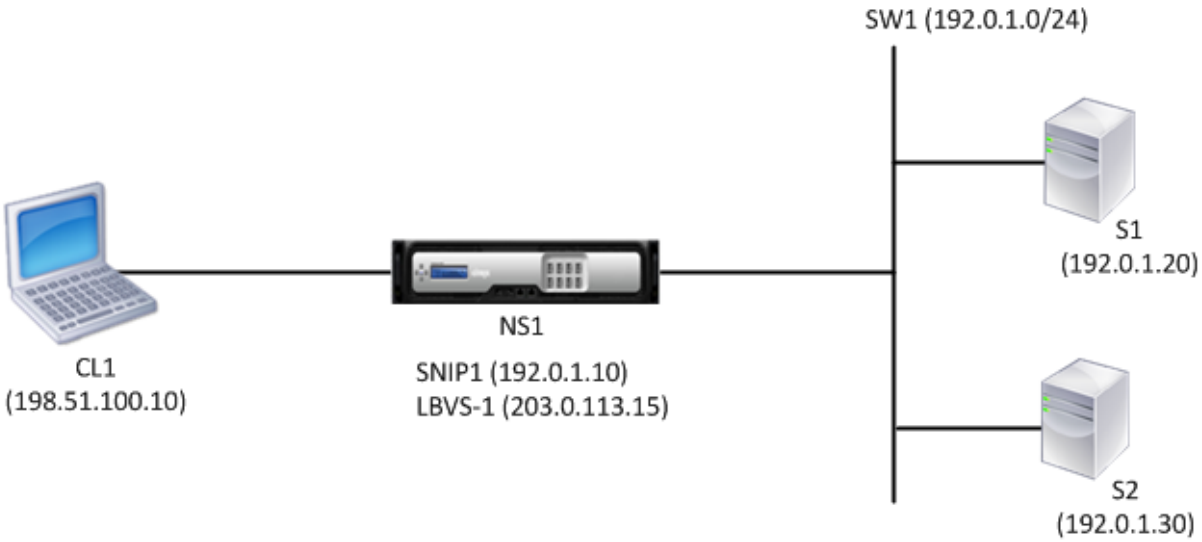
Um die Kommunikation zwischen dem NetScaler und einem Server zu ermöglichen, der entweder direkt mit dem NetScaler verbunden ist oder nur über einen L2-Switch verbunden ist, müssen Sie eine Subnetz-IP-Adresse konfigurieren, die zum Subnetz des Servers gehört. Sie müssen mindestens eine Subnetz-IP-Adresse für jedes direkt verbundene Subnetz konfigurieren, mit Ausnahme des direkt verbundenen Verwaltungssubnetzes, das über NSIP verbunden ist.

Stellen Sie sich ein Beispiel für ein Lastenausgleichs-Setup vor, bei dem der virtuelle Lastausgleichsserver LBVS1 auf NetScaler NS1 zum Lastenausgleich der Server S1 und S2 verwendet wird, die über den L2-Switch SW1 mit NS1 verbunden sind. S1 und S2 gehören demselben Subnetz an.

Die SNIP-Adresse SNIP1, die zum selben Subnetz wie S1 und S2 gehört, ist auf NS1 konfiguriert. Sobald SNIP1 konfiguriert ist, sendet NS1 ARP-Pakete für SNIP1.

Die Dienste SVC-S1 und SVC-S2 auf NS1 stehen für S1 und S2. Sobald diese Dienste konfiguriert sind, sendet NS1 ARP-Anfragen für S1 und S2, um die IP-zu-Mac-Zuordnung zu lösen. Nachdem S1 und S2 antworten, sendet NS1 ihnen Überwachungssonden in regelmäßigen Abständen von der Adresse SNIP1, um ihre Gesundheit zu überprüfen.

Weitere Informationen zum Konfigurieren des Lastenausgleichs auf einem NetScaler finden Sie unter Load Balancing.



Es folgt der Verkehrsfluss in diesem Beispiel:

1. Client C1 sendet ein Anforderungspaket an LBVS-1. Das Anforderungspaket enthält:
   - Quell-IP = IP-Adresse des Clients (198.51.100.10)
   - Ziel-IP = IP-Adresse von LBVS-1 (203.0.113.15)
2. LBVS1 von NS1 empfängt das Anforderungspaket.
3. Der Load-Balancing-Algorithmus von LBVS1 wählt Server S2 aus.
4. Da S2 direkt mit NS1 verbunden ist und SNIP1 (192.0.1.10) die einzige IP-Adresse auf NS1 ist, die zu demselben Subnetz wie S2 gehört, öffnet NS1 eine Verbindung zwischen SNIP1 und S2.
5. NS1 sendet das Anforderungspaket von SNIP1 an S2. Das Anforderungspaket enthält:
   - Quell-IP = SNIP1 (192.0.1.10)
   - Ziel-IP = IP-Adresse von S2 (192.0.1.30)
6. Die Antwort von S2 gibt den gleichen Pfad zurück.

Verwenden von SNIPs für Serversubnetze, die über einen Router verbunden sind

Um die Kommunikation zwischen dem NetScaler und Servern in Subnetzen zu ermöglichen, die über einen Router verbunden sind, müssen Sie mindestens eine Subnetz-IP-Adresse konfigurieren, die zum Subnetz der direkt mit dem Router verbundenen Schnittstelle gehört. Der ADC verwendet diese Subnetz-IP-Adresse, um mit Servern in Subnetzen zu kommunizieren, die über den Router erreicht werden können.

Stellen Sie sich ein Beispiel für ein Lastausgleichs-Setup vor, bei dem der virtuelle Lastausgleichsserver LBVS1 auf NetScaler NS1 verwendet wird, um die Server S1, S2, S3 und S4, die über den Router R1 mit NS1 verbunden sind, zu lastenausgleichen.

S1 und S2 gehören zu demselben Subnetz, 192.0.2.0/24, und sind über den L2-Switch SW1 mit R1 verbunden. S3 und S4 gehören zu einem anderen Subnetz, 192.0.3.0/24, und sind über den L2-Switch SW2 mit R1 verbunden.

NetScaler NS1 ist über das Subnetz 192.0.1.0/24 mit dem Router R1 verbunden. Die SNIP-Adresse SNIP1, die zu demselben Subnetz gehört wie die direkt mit dem Router verbundene Schnittstelle (192.0.1.0/24), ist auf NS1 konfiguriert. NS1 verwendet diese Adresse für die Kommunikation mit Servern S1 und S2 sowie mit Servern S3 und S4.

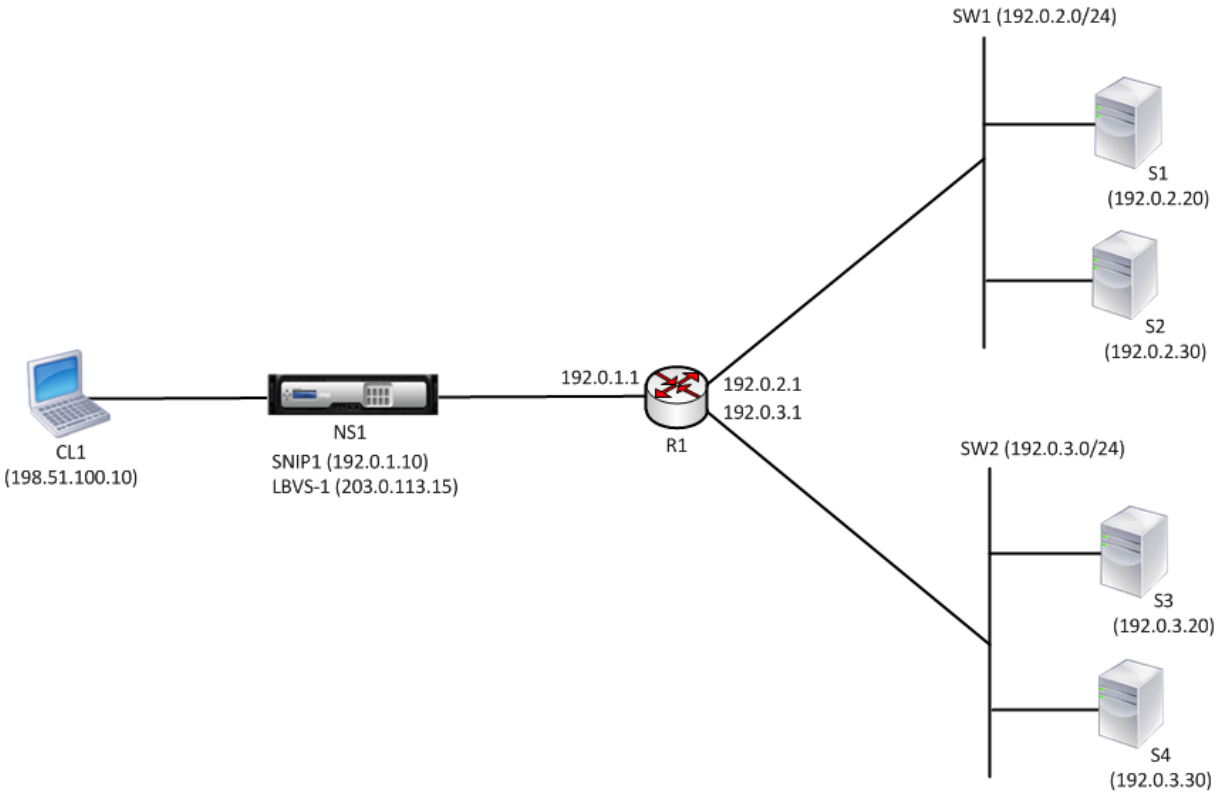
Weitere Informationen zum Konfigurieren des Lastenausgleichs auf einem NetScaler finden Sie unter Load Balancing.

Sobald die Adresse SNIP1 konfiguriert ist, sendet NS1 ARP-Ankündigungspakete für SNIP1.

Die Routingtabelle von NS1 besteht aus Routeneinträgen für S1, S2, S3 und S4 bis R1. Diese Routeneinträge sind entweder statische Routeneinträge oder werden von R1 an NS1 unter Verwendung dynamischer Routing-Protokolle angekündigt.

Die Dienste SVC-S1, SVC-S2, SVC-S3 und SVC-S4 auf NS1 stellen die Server S1, S2, S3 und S4 dar. NS1 stellt in seinen Routingtabellen fest, dass diese Server über R1 erreichbar sind. NS1 sendet ihnen Überwachungssonden in regelmäßigen Abständen, von der Adresse SNIP1, um ihre Gesundheit zu überprüfen.

Weitere Informationen zum IP-Routing auf einem NetScaler finden Sie unter IP-Routing.



Es folgt der Verkehrsfluss in diesem Beispiel:

1. Client C1 sendet ein Anforderungspaket an LBVS-1. Das Anforderungspaket enthält:
   - Quell-IP = IP-Adresse des Clients (198.51.100.10)
   - Ziel-IP = IP-Adresse von LBVS-1 (203.0.113.15)
2. LBVS1 von NS1 empfängt das Anforderungspaket.
3. Der Load-Balancing-Algorithmus von LBVS1 wählt Server S3 aus.
4. NS1 überprüft seine Routing-Tabelle und stellt fest, dass S3 über R1 erreichbar ist. SNIP1 (192.0.1.10) ist die einzige IP-Adresse auf NS1, die zu demselben Subnetz gehört wie Router R1. NS1 öffnet über R1 eine Verbindung zwischen SNIP1 und S3.
5. NS1 sendet das Anforderungspaket von SNIP1 an R1. Das Anforderungspaket enthält:
   - Quell-IP-Adresse = SNIP1 (192.0.1.10)
   - Ziel-IP-Adresse = IP-Adresse von S3 (192.0.3.20)
6. Die Anfrage erreicht R1, das seine Routing-Tabelle überprüft und das Anforderungspaket an S3 weiterleitet.
7. Die Antwort von S3 gibt den gleichen Pfad zurück.

Verwendung von SNIPs für mehrere Serversubnetze (VLANs) auf einem L2-Switch

Wenn Sie mehrere Serversubnetze (VLANs) auf einem L2-Switch haben, der mit einem NetScaler verbunden ist, müssen Sie mindestens eine SNIP-Adresse für jedes der Serversubnetze konfigurieren, damit der NetScaler mit diesen Serversubnetzen kommunizieren kann.

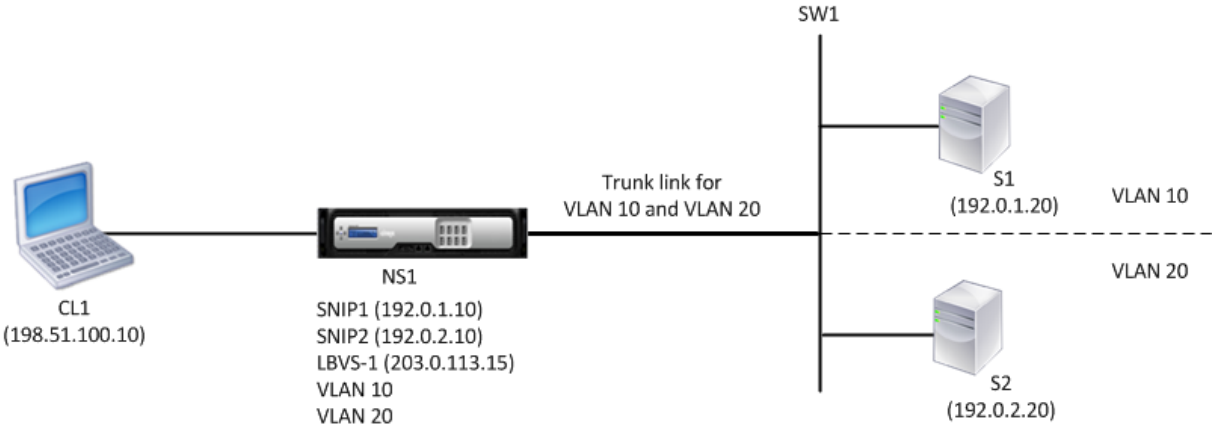
Stellen Sie sich ein Beispiel für ein Lastenausgleichs-Setup vor, bei dem der virtuelle Lastausgleichsserver LBVS1 auf NetScaler NS1 zum Lastenausgleich der Server S1 und S2 verwendet wird, die über den L2-Switch SW1 mit NS1 verbunden sind. S1 und S2 gehören zu verschiedenen Subnetzen und sind Teil von VLAN 10 bzw. VLAN20. Die Verbindung zwischen NS1 und SW1 ist eine Trunk-Verbindung und wird von VLAN10 und VLAN20 gemeinsam genutzt.

Weitere Informationen zum Konfigurieren des Lastenausgleichs auf einem NetScaler finden Sie unter Load Balancing.

Subnetz-IP-Adressen SNIP1 (nur zu Referenzzwecken) und SNIP2 (nur zu Referenzzwecken) werden auf NS1 konfiguriert. NS1 verwendet SNIP1 (auf VLAN 10), um mit Server S1 zu kommunizieren, und SNIP2 (auf VLAN 20), um mit S2 zu kommunizieren. Sobald SNIP1 und SNIP2 konfiguriert sind, sendet NS1 ARP-Ankündigungspakete für SNIP1 und SNIP2.

Weitere Informationen zum Konfigurieren von VLANs auf einem NetScaler finden Sie unter Konfigurieren eines VLAN.

Die Dienste SVC-S1 und SVC-S2 auf NS1 stellen Server S1 und S2 dar. Sobald diese Dienste konfiguriert sind, sendet NS1 ARP-Anfragen für sie. Nachdem S1 und S2 reagiert haben, sendet NS1 ihnen in regelmäßigen Abständen Überwachungssonden, um ihren Zustand zu überprüfen. NS1 sendet Überwachungstests von der Adresse SNIP1 an S1 und von der Adresse SNIP2 an S2.



Es folgt der Verkehrsfluss in diesem Beispiel:

1. Client C1 sendet ein Anforderungspaket an LBVS-1. Das Anforderungspaket enthält:
   - Quell-IP = IP-Adresse des Clients (198.51.100.10)
   - Ziel-IP = IP-Adresse von LBVS-1 (203.0.113.15)
2. LBVS1 von NS1 empfängt das Anforderungspaket.
3. Der Load-Balancing-Algorithmus von LBVS1 wählt Server S2 aus.
4. Da S2 direkt mit NS1 verbunden ist und SNIP2 (192.0.2.10) die einzige IP-Adresse auf NS1 ist, die zu demselben Subnetz wie S2 gehört, öffnet NS1 eine Verbindung zwischen SNIP2 und S2. Hinweis: Wenn S1 ausgewählt ist, öffnet NS1 eine Verbindung zwischen SNIP1 und S1.
5. NS1 sendet das Anforderungspaket von SNIP2 an S2. Das Anforderungspaket enthält:
   - Quell-IP = SNIP1 (192.0.2.10)
   - Ziel-IP = IP-Adresse von S2 (192.0.2.20)
6. Die Antwort von S2 gibt den gleichen Pfad zurück.

GSLB-Site-IP-Adressen (GSLBIP) konfigurieren

May 11, 2023

Eine GSLB-Standort-IP-Adresse (GSLBIP) ist eine IP-Adresse, die einer GSLB-Site zugeordnet ist. Es ist nicht zwingend erforderlich, bei der ersten Konfiguration der NetScaler-Appliance eine GSLBIP-Adresse anzugeben. Eine GSLBIP-Adresse wird nur verwendet, wenn Sie eine GSLB-Site erstellen.

Weitere Informationen zum Erstellen einer GSLB-Site-IP-Adresse finden Sie unter Globaler Server-Lastenausgleich.

Entfernen einer NetScaler-eigenen IP-Adresse

May 11, 2023

Sie können jede IP-Adresse außer der NSIP entfernen. Die folgende Tabelle enthält Informationen zu den Prozessen, die Sie befolgen müssen, um die verschiedenen Arten von IP-Adressen zu entfernen. Bevor Sie einen VIP entfernen, entfernen Sie den zugehörigen virtuellen Server.

Typ der IP-Adresse	Implikationen
Subnetz-IP-Adresse (SNIP)	Wenn die zu entfernende IP-Adresse die letzte IP-Adresse im Subnetz ist, wird die zugehörige Route aus der Routing-Tabelle gelöscht. Wenn die zu entfernende IP-Adresse das Gateway im entsprechenden Routeneintrag ist, wird das Gateway für diese Subnetzroute auf eine andere Netscaler-eigene IP-Adresse geändert.
IP-Adresse des virtuellen Servers (VIP)	Bevor Sie einen VIP entfernen, müssen Sie zuerst den damit verbundenen virtuellen Server entfernen. Informationen zum Entfernen des virtuellen Servers finden Sie unter Load Balancing.
GSLB-Site-IP-Adresse	Bevor Sie eine GSLB-Site-IP-Adresse entfernen, müssen Sie die zugehörige Site entfernen. Informationen zum Entfernen der Site finden Sie unter Globaler Server-Lastenausgleich.

So entfernen Sie eine IP-Adresse mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

rm ns ip <IPaddress>

Beispiel:

```
1 > rm ns ip 10.102.29.54
2 Done
3 <!--NeedCopy-->
```

IP-Adresse mithilfe der GUI entfernen:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**und löschen Sie die IP-Adresse.

Anwendungszugriffssteuerungen konfigurieren

May 11, 2023

Anwendungszugriffskontrollen, auch bekannt als Verwaltungszugriffskontrollen, bilden einen einheitlichen Mechanismus zur Verwaltung der Benutzerauthentifizierung und zur Implementierung von Regeln, die den Benutzerzugriff auf Anwendungen und Daten festlegen. Sie können SNIPs so konfigurieren, dass Verwaltungsanwendungen Zugriff erhalten. Der Verwaltungszugriff für das NSIP ist standardmäßig aktiviert und kann nicht deaktiviert werden. Sie können es jedoch mithilfe von ACLs steuern.

Informationen zur Verwendung von ACLs finden Sie unter Zugriffssteuerungslisten (ACLs).

Die NetScaler Appliance unterstützt keinen Verwaltungszugriff auf VIPs.

Die folgende Tabelle enthält eine Zusammenfassung der Interaktion zwischen dem Verwaltungszugriff und bestimmten Diensteinstellungen für Telnet.

Zugriff für das Management	Telnet (Status konfiguriert auf dem NetScaler)	Telnet (Effektiver Status auf IP-Ebene)
Smartcard	Smartcard	Smartcard
Smartcard	Deaktivieren	Deaktivieren
Deaktivieren	Smartcard	Deaktivieren
Deaktivieren	Deaktivieren	Deaktivieren

Die folgende Tabelle bietet einen Überblick über die IP-Adressen, die als Quell-IP-Adressen im ausgehenden Datenverkehr verwendet werden.

Anwendung/ IP	NSIP	SNIP	VIP
ARP	Ja	Ja	Nein
Serverseitiger Verkehr	Nein	Ja	Nein
RNAT	Nein	Ja	Ja
ICMP-PING	Ja	Ja	Nein
Dynamisches Routing	Ja	Ja	Ja

Die folgende Tabelle bietet einen Überblick über die Anwendungen, die auf diesen IP-Adressen ver-

fügbar sind.

Anwendung/ IP	NSIP	SNIP	VIP
SNMP	Ja	Ja	Ja
Zugriff auf das System	Ja	Ja	Nein

Sie können auf den NetScaler zugreifen und ihn verwalten, indem Sie Anwendungen wie Telnet, SSH, GUI und FTP verwenden.

Hinweis: Telnet und FTP sind auf dem NetScaler aus Sicherheitsgründen deaktiviert. Um sie zu aktivieren, wenden Sie sich an den Kundensupport. Nachdem die Anwendungen aktiviert wurden, können Sie die Steuerelemente auf IP-Ebene anwenden.

Um den NetScaler so zu konfigurieren, dass er auf diese Anwendungen reagiert, müssen Sie die spezifischen Verwaltungsanwendungen aktivieren. Wenn Sie den Verwaltungszugriff für eine IP-Adresse deaktivieren, werden bestehende Verbindungen, die die IP-Adresse verwenden, nicht beendet, es können jedoch keine neuen Verbindungen initiiert werden.

Außerdem sind die nicht verwalteten Anwendungen, die auf dem zugrundeliegenden FreeBSD-Betriebssystem laufen, anfällig für Protokollangriffe, und diese Anwendungen nutzen die Angriffsschutzfunktionen der NetScaler-Appliance nicht aus.

Sie können den Zugriff auf diese nicht verwalteten Anwendungen auf einem SNIP oder NSIP blockieren. Wenn der Zugriff blockiert ist, kann ein Benutzer, der mithilfe von SNIP oder NSIP eine Verbindung zu einem NetScaler herstellt, nicht auf die Verwaltungsanwendungen zugreifen, die auf dem zugrunde liegenden Betriebssystem ausgeführt werden.

So konfigurieren Sie den Verwaltungszugriff für eine IP-Adresse mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

set ns ip <IPAddress> -mgmtAccess <value> -**telnet** <value> -**ftp** <value> -**gui** <value> -**ssh** <value> -**snmp** <value> -**restrictAccess** (**ENABLED** | **DISABLED**)

Beispiel:

```
1  > set ns ip 10.102.29.54 -mgmtAccess enabled -restrictAccess ENABLED
2   Done
3 <!--NeedCopy-->
```

Gehen Sie wie folgt vor, um den Verwaltungszugriff für eine IP-Adresse mithilfe der GUI zu aktivieren:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Öffnen Sie einen IP-Adresseintrag, und wählen Sie die Option **Verwaltungszugriff aktivieren**, um die aufgelisteten Anwendungen zu unterstützen.

Aktivieren des sicheren Zugriffs auf NetScaler GUI mit einer Subnetz-IP-Adresse (SNIP)

Der sichere Zugriff auf die NetScaler GUI ist standardmäßig für die NetScaler IP (NSIP) aktiviert. Sie können den sicheren Zugriff auf die NetScaler Appliance auch mithilfe einer Subnetz-IP-Adresse der Appliance aktivieren.

Nach dem Konfigurieren einer SNIP-Adresse für den sicheren Zugriff auf ein Hochverfügbarkeitspaar steht der sichere Zugriff auf die primäre Appliance zur Verfügung, wenn Sie auf die SNIP-Adresse zugreifen.

NetScaler CLI-Verfahren

So aktivieren Sie den sicheren Zugriff auf NetScaler GUI mit einer Subnetz-IP-Adresse (SNIP) über die Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

set ns ip <SNIP_Address>**-type SNIP -gui SECUREONLY -mgmtAccess ENABLED**

Beispiel:

```
> set ns ip 203.0.113.99 -mgmtAccess enabled -restrictAccess ENABLED

 Done
<!--NeedCopy-->
```

NetScaler-Proxyverbindungen

May 11, 2023

Wenn ein Client eine Verbindung initiiert, beendet die NetScaler Appliance die Client-Verbindung, initiiert eine Verbindung zu einem entsprechenden Server und sendet das Paket an den Server. Die Appliance führt diese Aktion nicht für den Diensttyp UDP oder ANY aus.

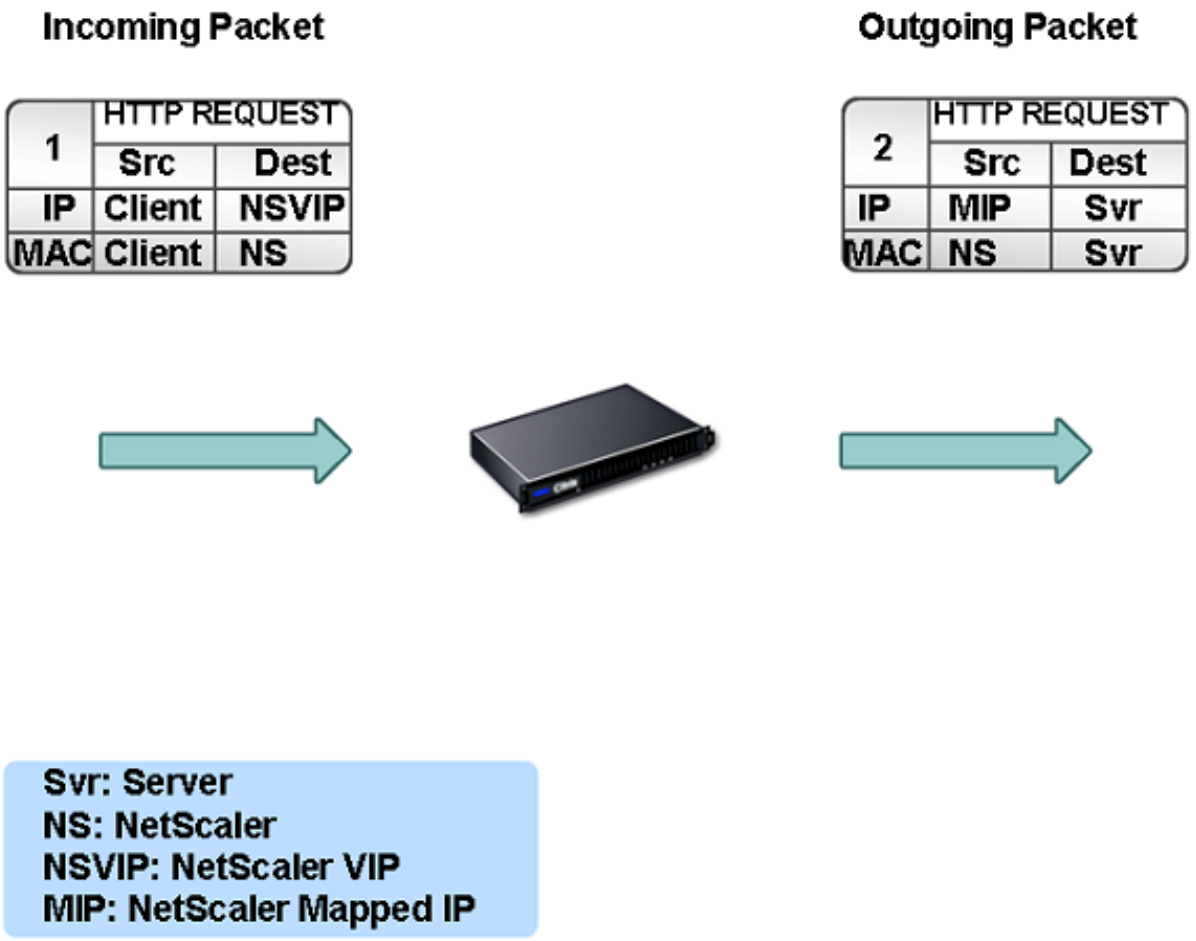
Weitere Informationen zu Diensttypen finden Sie unter Load Balancing.

Sie können den NetScaler so konfigurieren, dass das Paket verarbeitet wird, bevor Sie die Verbindung mit einem Server initiieren. Das Standardverhalten besteht darin, die Quell- und Ziel-IP-Adressen eines Pakets zu ändern, bevor das Paket an den Server gesendet wird. Sie können den NetScaler so konfigurieren, dass er die Quell-IP-Adresse der Pakete beibehält, indem Sie den Modus Quell-IP verwenden aktivieren.

So wird die Ziel-IP-Adresse ausgewählt

Der an die NetScaler-Appliance gesendete Datenverkehr kann an einen virtuellen Server oder an einen Dienst gesendet werden. Die Appliance verarbeitet den Datenverkehr zu virtuellen Servern und Diensten unterschiedlich. Der NetScaler beendet den an einer virtuellen Server-IP-Adresse (VIP) empfangenen Datenverkehr und ändert die Ziel-IP-Adresse in die IP-Adresse des Servers, bevor er den Datenverkehr an den Server weiterleitet, wie in der folgenden Abbildung dargestellt.

Abbildung 1. Proxyverbindungen zu VIPs



Pakete, die für einen Dienst bestimmt sind, werden direkt an den entsprechenden Server gesendet, und der NetScaler ändert die Ziel-IP-Adressen nicht. In diesem Fall fungiert der NetScaler als Proxy.

So wird die Quell-IP-Adresse ausgewählt

Wenn die NetScaler-Appliance mit den physischen Servern oder Peer-Geräten kommuniziert, verwendet sie standardmäßig nicht die IP-Adresse des Clients. NetScaler verwaltet einen Pool von Subnetz-

IP-Adressen (SNIPs) und wählt aus diesem Pool eine IP-Adresse aus, die als Quell-IP-Adresse für eine Verbindung zum physischen Server verwendet wird. Abhängig vom Subnetz, in dem sich der physische Server befindet, wählt NetScaler eine bestimmte SNIP-Adresse aus.

Hinweis: Wenn die Option Quell-IP (USIP) verwenden aktiviert ist, verwendet die Appliance die IP-Adresse des Clients.

Quell-IP-Modus verwenden aktivieren

May 11, 2023

Wenn die NetScaler-Appliance mit den physischen Servern oder Peer-Geräten kommuniziert, verwendet sie standardmäßig eine ihrer eigenen IP-Adressen als Quell-IP. Die Appliance verwaltet einen Pool von Subnetz-IP-Adressen (SNIPs) und wählt eine IP-Adresse aus diesem Pool aus, die als Quell-IP-Adresse für eine Verbindung zum physischen Server verwendet wird. Die Entscheidung, eine SNIP-Adresse auszuwählen, hängt vom Subnetz ab, in dem sich der physische Server befindet.

Bei Bedarf können Sie die NetScaler-Appliance so konfigurieren, dass sie die IP-Adresse des Clients als Quell-IP verwendet. Einige Anwendungen benötigen die tatsächliche IP-Adresse des Clients. Die folgenden Anwendungsfälle sind einige Beispiele:

- Die IP-Adresse des Kunden im Webzugriffsprotokoll wird zu Abrechnungszwecken oder zur Nutzungsanalyse verwendet.
- Die IP-Adresse des Kunden wird verwendet, um das Herkunftsland des Kunden oder den ursprünglichen ISP des Kunden zu bestimmen. Beispielsweise bieten viele Suchmaschinen wie Google Inhalte, die für den Standort relevant sind, zu dem der Nutzer gehört.
- Die Anwendung muss die IP-Adresse des Clients kennen, um zu überprüfen, ob die Anfrage von einer vertrauenswürdigen Quelle stammt.
- Manchmal benötigt eine Firewall zwischen dem Anwendungsserver und dem NetScaler die IP-Adresse des Clients, obwohl ein Anwendungsserver die IP-Adresse des Clients nicht benötigt, um den Datenverkehr zu filtern.

Aktivieren Sie den Modus “Use Source IP” (USIP), wenn der NetScaler die IP-Adresse des Clients für die Kommunikation mit den Servern verwenden soll.

Die folgende Abbildung zeigt, wie die Appliance IP-Adressen im USIP-Modus verwendet.

Voraussetzungen

Bevor Sie den USIP-Modus aktivieren, beachten Sie die folgenden Punkte:

- Aktivieren Sie USIP in den folgenden Situationen:
  - Lastausgleich der IDS-Server (Intrusion Detection System)
  - SMTP-Lastausgleich
  - Failover für statuslose Verbindungen
  - Sitzungsloser Lastausgleich
  - Wenn Sie den Direct Server Return (DSR) -Modus verwenden
- Die globale USIP-Einstellung gilt nur für Dienste, die erstellt werden, nachdem die globale USIP-Einstellung vorgenommen wurde. Mit anderen Worten, die globale USIP-Einstellung gilt nicht für die vorhandenen Dienste, wenn die globale USIP-Einstellung vorgenommen wird. Beispielsweise wird USIP nicht für die vorhandenen Dienste deaktiviert, wenn Sie USIP global deaktivieren. Es verhindert jedoch, dass die anschließend erstellten Dienste USIP automatisch aktivieren.

  Um USIP für eine Reihe vorhandener Dienste zu aktivieren oder zu deaktivieren, müssen Sie USIP für jeden dieser Dienste aktivieren oder deaktivieren.
- Wenn USIP aktiviert ist, müssen Sie das Gateway des Servers auf eine der NetScaler-eigenen IP-Adressen (vom Typ Subnet IP (SNIP)) festlegen, damit die Antwort des Servers immer über die NetScaler-Appliance erfolgt.
- Wenn Sie USIP aktivieren, setzen Sie das Leerlauf-Timeout für Serververbindungen auf einen Wert, der unter dem Standardwert liegt, damit inaktive Verbindungen serverseitig schnell gelöscht werden.
- Wenn Sie USIP aktivieren, aktivieren Sie für eine transparente Cache-Umleitung auch L2CONN.

- Da HTTP-Verbindungen nicht wiederverwendet werden, wenn USIP aktiviert ist, kann sich eine große Anzahl serverseitiger Verbindungen ansammeln. Inaktive Serververbindungen können Verbindungen für andere Clients blockieren. Legen Sie daher Grenzwerte für die maximale Anzahl von Verbindungen zu einem Dienst fest. Citrix empfiehlt außerdem, den HTTP-Server-Timeout-Wert für einen Dienst, für den USIP aktiviert ist, auf einen niedrigeren Wert als den Standardwert festzulegen, damit inaktive Verbindungen serverseitig schnell gelöscht werden.
- Als Alternative zum USIP-Modus haben Sie die Möglichkeit, die IP-Adresse (CIP) des Clients in den Anforderungsheader der serverseitigen Verbindung für einen Anwendungsserver einzufügen, der die IP-Adresse des Clients benötigt.
- In früheren NetScaler-Versionen hatte der USIP-Modus die folgenden Quellportoptionen für serverseitige Verbindungen:
  - **Verwenden Sie den Port des Clients**. Mit dieser Option können Verbindungen nicht wiederverwendet werden. Für jede Anfrage des Clients wird eine neue Verbindung mit dem physischen Server hergestellt.
  - **Verwenden Sie den Proxy-Port**. Mit dieser Option ist die Wiederverwendung von Verbindungen für alle Anfragen desselben Clients möglich.

  In den späteren NetScaler-Versionen wird, wenn USIP aktiviert ist, standardmäßig einen Proxyport für serverseitige Verbindungen verwendet und Verbindungen nicht wiederverwendet. Wenn Verbindungen nicht wiederverwendet werden, wirkt sich dies möglicherweise nicht auf die Geschwindigkeit des Verbindungsaufbaus aus.

  Standardmäßig ist die Option Proxy-Port verwenden aktiviert, wenn der USIP-Modus aktiviert ist.

  Hinweis: Wenn Sie den USIP-Modus aktivieren, wird empfohlen, die Option Proxy-Port verwenden zu aktivieren.

  Weitere Informationen zur Option Proxy-Port verwenden finden Sie unter Konfigurieren des Quellports für serverseitige Verbindungen.

Konfigurationsschritte

Aktivieren Sie den USIP-Modus (Use Source IP), wenn NetScaler die IP-Adresse des Clients für die Kommunikation mit den Servern verwenden soll. Standardmäßig ist der USIP-Modus deaktiviert. Der USIP-Modus kann global auf dem NetScaler oder in einem bestimmten Dienst aktiviert werden. Wenn Sie es global aktivieren, ist USIP standardmäßig für alle später erstellten Dienste aktiviert. Wenn Sie USIP für einen bestimmten Dienst aktivieren, wird die IP-Adresse des Clients nur für den Datenverkehr verwendet, der an diesen Dienst weitergeleitet wird.

CLI-Verfahren

Um den USIP-Modus global über die CLI zu aktivieren oder zu deaktivieren:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **enable ns mode USIP**
- **disable ns mode USIP**

So aktivieren Sie den USIP-Modus für einen Dienst über die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

set service <name>@ -**usip** (**YES** | **NO**)

Beispiel:

```
> set service Service-HTTP-1 -usip YES
Done
<!--NeedCopy-->
```

GUI-Verfahren

Um den USIP-Modus global über die GUI zu aktivieren:

1. Navigieren Sie zu **System** > **Einstellungen**und klicken Sie in der Gruppe **Modi und Funktionen** auf **Modi ändern**.
2. Wählen Sie die Option **Quell-IP verwenden**.

Um den USIP-Modus für einen Dienst über die GUI zu aktivieren:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, und bearbeiten Sie einen Service.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **Diensteinstellungen** und dann **Quell-IP-Adresse verwenden** aus.

Netzwerkadressübersetzung konfigurieren

May 11, 2023

Network Address Translation (NAT) beinhaltet die Änderung der Quell- und/oder Ziel-IP-Adressen und/oder der TCP/UDP-Portnummern von IP-Paketen, die die NetScaler-Appliance passieren. Die Aktivierung von NAT auf der Appliance erhöht die Sicherheit Ihres privaten Netzwerks und schützt es vor einem öffentlichen Netzwerk wie dem Internet, indem die Quell-IP-Adressen Ihres Netzwerks geändert werden, wenn Daten den NetScaler passieren. Mithilfe von NAT-Einträgen kann

Ihr gesamtes privates Netzwerk auch durch einige gemeinsam genutzte öffentliche IP-Adressen dargestellt werden. Der NetScaler unterstützt die folgenden Arten der Netzwerkadressübersetzung:

- **Eingehendes NAT (INAT).** Der NetScaler ersetzt die Ziel-IP-Adresse in den vom Client generierten Paketen durch die private IP-Adresse des Servers.
- **Umgekehrtes NAT (RNAT).** NetScaler ersetzt die Quell-IP-Adresse in den von den Servern generierten Paketen durch die öffentlichen NAT-IP-Adressen.

Übersetzung eingehender Netzwerkadressen

May 11, 2023

Wenn ein Client ein Paket an eine NetScaler-Appliance sendet, die für Inbound Network Address Translation (INAT) konfiguriert ist, übersetzt die Appliance die öffentliche Ziel-IP-Adresse des Pakets in eine private Ziel-IP-Adresse und leitet das Paket an den Server unter dieser Adresse weiter.

Die folgenden Konfigurationen werden unterstützt:

- **IPv4-IPv4-Mapping**: Eine öffentliche IPv4-Adresse auf der NetScaler-Appliance hört Verbindungsanfragen im Namen eines privaten IPv4-Servers ab. Die NetScaler-Appliance übersetzt die öffentliche Ziel-IP-Adresse des Pakets in die Ziel-IP-Adresse des Servers. Dann leitet die Appliance das Paket an den Server unter dieser Adresse weiter.
- **IPv4-IPv6-Mapping**: Eine öffentliche IPv4-Adresse auf der NetScaler-Appliance hört Verbindungsanfragen im Namen eines privaten IPv6-Servers ab. Die NetScaler-Appliance erstellt ein IPv6-Anforderungspaket mit der IP-Adresse des IPv6-Servers als Ziel-IP-Adresse.
- **IPv6-IPv4-Mapping**: Eine öffentliche IPv6-Adresse auf der NetScaler-Appliance hört Verbindungsanfragen im Namen eines privaten IPv4-Servers ab. Die NetScaler-Appliance erstellt ein IPv4-Anforderungspaket mit der IP-Adresse des IPv4-Servers als Ziel-IP-Adresse.
- **IPv6-IPv6-Mapping**: Eine öffentliche IPv6-Adresse auf der NetScaler-Appliance hört Verbindungsanfragen im Namen eines privaten IPv6-Servers ab. Die NetScaler-Appliance übersetzt die öffentliche Ziel-IP-Adresse des Pakets in die Ziel-IP-Adresse des Servers. Dann leitet die Appliance das Paket an den Server unter dieser Adresse weiter.

Wenn die Appliance ein Paket an einen Server weiterleitet, wird die dem Paket zugewiesene Quell-IP-Adresse wie folgt bestimmt:

- Wenn der Modus „Subnetz-IP verwenden“ (USNIP) aktiviert und der Modus „Quell-IP verwenden“ (USIP) deaktiviert ist, verwendet die Appliance eine Subnetz-IP-Adresse (SNIP) als Quell-IP-Adresse.
- Wenn der USIP-Modus aktiviert und der USNIP-Modus deaktiviert ist, verwendet die Appliance die Client-IP-Adresse (CIP) als Quell-IP-Adresse.
- Wenn sowohl der USIP- als auch der USNIP-Modus aktiviert sind, hat der USIP-Modus Vorrang.

- Sie können den NetScaler auch so konfigurieren, dass er eine eindeutige IP-Adresse als Quell-IP-Adresse verwendet, indem Sie den ProxyIP-Parameter festlegen.
- Wenn keiner der oben genannten Modi aktiviert ist und keine eindeutige IP-Adresse angegeben wurde, versucht der NetScaler, eine MIP als Quell-IP-Adresse zu verwenden.
- Wenn sowohl der USIP- als auch der USNIP-Modus aktiviert sind und eine eindeutige IP-Adresse angegeben wurde, lautet die Rangfolge wie folgt: USIP-Unique IP-USNIP-MIP-Error.

Um den NetScaler vor DoS-Angriffen zu schützen, können Sie den TCP-Proxy aktivieren. Wenn in Ihrem Netzwerk jedoch andere Schutzmechanismen verwendet werden, können Sie diese deaktivieren.

INAT-Regeln konfigurieren

Sie können einen INAT-Eintrag erstellen, ändern oder entfernen.

CLI-Verfahren

Um einen INAT-Eintrag mit der CLI zu erstellen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen INAT-Eintrag zu erstellen und dessen Konfiguration zu überprüfen:

- **add inat** <name> <publicIP> <privateIP> [-**tcpproxy** (**ENABLED** | **DISABLED**)] [-**ftp** (**ENABLED** | **DISABLED**)] [-**usip** (**ON** | **OFF**)] [-**usnip** (**ON** | **OFF**)] [-**proxyIP** \<**ip_addr > ipv6_addr>**]
- **show inat** [\<name>]

Beispiel:

```
> add inat ip4-ip4 172.16.1.2 192.168.1.1 -proxyip 10.102.29.171
 Done
<!--NeedCopy-->
```

Um einen INAT-Eintrag mit der CLI zu ändern:

Um einen INAT-Eintrag zu ändern, geben Sie den `set inat` Befehl, den Namen des Eintrags und die zu ändernden Parameter mit ihren neuen Werten ein.

Um eine INAT-Konfiguration mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- **rm inat** <name>

Beispiel:


```
> rm inat ip4-ip4
 Done
<!--NeedCopy-->
```

GUI-Verfahren

INAT-Eintrag mithilfe der GUI konfigurieren:

Navigieren Sie zu **System** > **Netzwerk** > **Routen** > **INAT**und fügen Sie einen INAT-Eintrag hinzu oder bearbeiten Sie einen vorhandenen INAT-Eintrag.

INAT-Konfiguration mithilfe der GUI entfernen:

Navigieren Sie zu **System** > **Netzwerk** > **Routen** > **INAT**und löschen Sie die INAT-Konfiguration.

Verbindungs-Failover für INAT-Regeln

Verbindungs-Failover oder Verbindungsspiegelung ermöglichen es dem primären Knoten, Verbindungs- und Persistenzinformationen auf den sekundären Knoten zu duplizieren, um eine hohe Verfügbarkeit zu gewährleisten. Die Statusinformationen der Verbindung werden regelmäßig mit dem sekundären Knoten geteilt, wenn die Verbindungsspiegelung aktiviert ist.

Die Aktivierung des Verbindungs-Failovers bietet mehr Zuverlässigkeit, geht jedoch mit dem Preis einher, dass ein Teil der Systemzeit für die gemeinsame Nutzung der Statusinformationen aufgewendet wird. Die Verbindungsdaten werden bei jeder Paket- oder Flow-Status-Aktualisierung mit der Standby-Einheit synchronisiert. Daher darf es nur an Orten verwendet werden, an denen die Zuverlässigkeit der Verbindungsebene von größter Bedeutung ist.

Hochverfügbarkeits-Setups der NetScaler-Appliance unterstützen Verbindungsfailover für INAT-Verbindungen. Der primäre Knoten sendet in regelmäßigen Abständen INAT-Mappings und andere INAT-bezogene Verbindungsinformationen an den sekundären Knoten. Die sekundäre Appliance verwendet die Zuordnungs- und Verbindungsinformationen nur im Falle eines Failovers.

Wenn ein Failover auftritt, enthält der neue primäre Knoten Informationen über die INAT-Verbindungen, die vor dem Failover hergestellt wurden. Daher werden diese Verbindungen auch nach dem Failover weiterhin bereitgestellt.

Aus Sicht des Kunden ist das Failover transparent. Während der Übergangsphase können der Client und der Server eine kurze Unterbrechung und erneute Übertragung erfahren. Der Verbindungsfailover kann gemäß der INAT-Regel aktiviert werden.

Um das Verbindungs-Failover für eine INAT-Regel zu aktivieren, aktivieren Sie den Parameter `connFailover` dieser spezifischen RNAT-Regel mithilfe der CLI.

CLI-Verfahren

Verbindungs-Failover für eine INAT-Regel mithilfe der CLI aktivieren:

Um das Verbindungs-Failover beim Hinzufügen einer INAT-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

- **add inat** <name> <publicIP> <privateIP> [-**tcpproxy** (**ENABLED** | **DISABLED**)] [-**ftp** (**ENABLED** | **DISABLED**)] [-**usip** (**ON** | **OFF**)] [-**usnip** (**ON** | **OFF**)] [-**proxyIP** \<ip_addr|ipv6_addr>] -**connfailover** (**ENABLED** | **DISABLED**)
- **show inat** <name>

Um den Verbindungs-Failover zu aktivieren, während eine bestehende INAT-Regel geändert wird, geben Sie in der Befehlszeile Folgendes ein:

- **set inat -connfailover** (**ENABLED** | **DISABLED**)
- **show inat** <name>

Koexistenz von INAT und virtuellen Servern

May 11, 2023

Wenn sowohl INAT als auch RNAT konfiguriert sind, hat die INAT-Regel Vorrang vor der RNAT-Regel. Wenn RNAT mit einer NAT-IP-Adresse (Network Address Translation IP) konfiguriert ist, wird die NAT-IP-Adresse als Quell-IP-Adresse für diesen RNAT-Client ausgewählt.

Die standardmäßige öffentliche Ziel-IP in einer INAT-Konfiguration ist die virtuelle IP-Adresse (VIP) des NetScaler-Geräts. Virtuelle Server verwenden auch VIPs. Wenn sowohl INAT als auch ein virtueller Server dieselbe IP-Adresse verwenden, überschreibt die vserver-Konfiguration die INAT-Konfiguration.

Im Folgenden finden Sie einige Beispielszenarien für die Konfiguration und deren Auswirkungen.

Fall	Ergebnis
Sie haben einen virtuellen Server und einen Dienst so konfiguriert, dass alle auf einem bestimmten NetScaler-Port empfangenen Datenpakete direkt an den Server gesendet werden. Sie haben auch INAT konfiguriert und TCP aktiviert. Wenn INAT auf diese Weise konfiguriert wird, werden alle über eine TCP-Engine empfangenen Datenpakete gesendet, bevor sie an den Server gesendet werden.	Alle auf dem NetScaler empfangenen Pakete, mit Ausnahme der am angegebenen Port empfangenen Pakete, passieren die TCP-Engine.
Sie haben einen virtuellen Server und einen Dienst so konfiguriert, dass alle Datenpakete des Diensttyps TCP, die an einem bestimmten Port auf dem NetScaler empfangen werden, an den Server gesendet werden, nachdem sie die TCP-Engine passiert haben. Sie haben auch INAT konfiguriert und TCP deaktiviert. Wenn INAT auf diese Weise konfiguriert wird, werden die empfangenen Datenpakete direkt an den Server gesendet.	Nur Pakete, die auf dem angegebenen Port empfangen werden, passieren die TCP-Engine.
Sie haben einen virtuellen Server und einen Dienst konfiguriert, um alle empfangenen Datenpakete an einen von zwei Servern zu senden. Sie versuchen, INAT so zu konfigurieren, dass alle empfangenen Datenpakete an einen anderen Server gesendet werden.	Die INAT-Konfiguration ist nicht zulässig.
Sie haben INAT so konfiguriert, dass alle empfangenen Datenpakete direkt an einen Server gesendet werden. Sie versuchen, einen virtuellen Server und einen Dienst so zu konfigurieren, dass alle empfangenen Datenpakete an zwei verschiedene Server gesendet werden.	Die vserver-Konfiguration ist nicht zulässig.

Staatenlos NAT46

May 11, 2023

Die statuslose NAT46-Funktion ermöglicht die Kommunikation zwischen IPv4- und IPv6-Netzwerken über die IPv4-zu-IPv6-Paketübersetzung und umgekehrt, ohne dass Sitzungsinformationen auf der NetScaler-Appliance gespeichert werden müssen.

Bei einer statuslosen NAT46-Konfiguration übersetzt die Appliance ein IPv4-Paket in IPv6 oder ein IPv6-Paket in IPv4, wie in den RFCs 6145 und 2765 definiert.

Eine statuslose NAT46-Konfiguration auf der NetScaler-Appliance besteht aus den folgenden Komponenten:

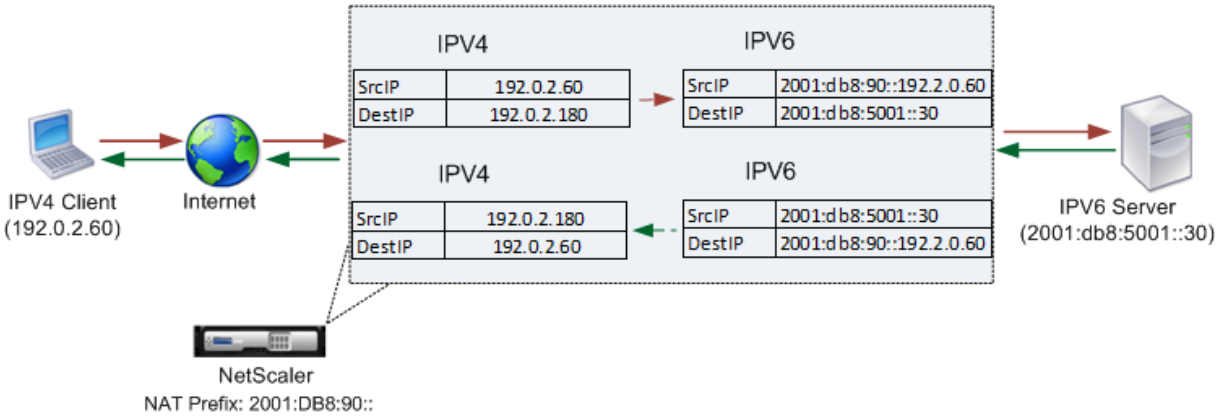
- **IPv4-IPv6-INAT-Eintrag.** Ein INAT-Eintrag, der eine 1:1 -Beziehung zwischen einer IPv4-Adresse und einer IPv6-Adresse definiert. Mit anderen Worten, eine IPv4-Adresse auf der Appliance hört Verbindungsanfragen im Namen eines IPv6-Servers ab. Ein IPv4-Anforderungspaket für diese IPv4-Adresse wird in ein IPv6-Paket übersetzt, und dann wird das IPv6-Paket an den IPv6-Server gesendet.

  Die Appliance übersetzt ein IPv6-Antwortpaket in ein IPv4-Antwortpaket, wobei das Quell-IP-Adressfeld als die im INAT-Eintrag angegebene IPv4-Adresse festgelegt ist. Das übersetzte Paket wird dann an den Client gesendet.

- **NAT46 IPv6-Präfix.** Ein globales IPv6-Präfix der Länge 96 Bit (128-32=96), das auf der Appliance konfiguriert ist. Bei der Übersetzung von IPv4-Paketen in IPv6-Pakete legt die Appliance die Quell-IP-Adresse des übersetzten IPv6-Pakets auf eine Verkettung des NAT46-IPv6-Präfixes [96 Bit] und der IPv4-Quelladresse [32 Bit] fest, die im Anforderungspaket empfangen wurde.

  Während der Übersetzung von IPv6-Paketen zu IPv4-Paketen setzt die Appliance die Ziel-IP-Adresse des übersetzten IPv4-Pakets auf die letzten 32 Bits der Ziel-IP-Adresse des IPv6-Pakets.

Stellen Sie sich ein Beispiel vor, in dem ein Unternehmen die Website www.example.com auf dem Server S1 hostet, der über eine IPv6-Adresse verfügt. Um die Kommunikation zwischen IPv4-Clients und IPv6-Server S1 zu ermöglichen, wird die NetScaler Appliance NS1 mit einer statuslosen NAT46-Konfiguration bereitgestellt, die einen IPv4-IPv6-INAT-Eintrag für Server S1 und ein NAT46-Präfix umfasst. Der INAT-Eintrag enthält eine IPv4-Adresse, an der die Appliance Verbindungsanfragen von IPv4-Clients im Namen des IPv6-Servers S1 abhört.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt:

Entitäten	Name	Wert
IP-Adresse des Clients	client_IPv4 (nur zu Referenzzwecken)	192.0.2.60
IPv6-Adresse des Servers	sevr_IPv6 (nur zu Referenzzwecken)	2001:DB8:5001::30
IPv4-Adresse, die im INAT-Eintrag für den IPv6-Server S1 definiert ist	Map-Sevr-IPv4 (nur zu Referenzzwecken)	192.0.2.180
IPv6-Präfix für die NAT 46-Übersetzung	NAT46_Prefix (nur zu Referenzzwecken)	2001:DB8:90::

Es folgt der Verkehrsfluss in diesem Beispiel:

1. Der IPv4-Client CL1 sendet ein Anforderungspaket an die Map-Sevr-IPv4-Adresse (192.0.2.180) auf der NetScaler-Appliance.
2. Die Appliance empfängt das Anforderungspaket und durchsucht die NAT46-INAT-Einträge nach der IPv6-Adresse, die der Map-Sevr-IPv4-Adresse (192.0.2.180) zugeordnet ist. Es findet die SEVR-IPv6-Adresse (2001:DB 8:5001::30).
3. Die Appliance erstellt ein übersetztes IPv6-Anforderungspaket mit:
   - Ziel-IP-Adressfeld = SEVR-IPv6 = 2001:DB 8:5001::30
   - Quell-IP-Adressfeld = Verkettung von NAT-Präfix (erste 96 Bit) und Client_IPv4 (letzte 32 Bit) = 2001:DB 8:90: :192.0.2.60
4. Die Appliance sendet die übersetzte IPv6-Anfrage an SEVR-IPv6.
5. Der IPv6-Server S1 sendet daraufhin ein IPv6-Paket an die NetScaler-Appliance mit:
   - Ziel-IP-Adressfeld = Verkettung von NAT-Präfix (erste 96 Bit) und Client_IPv4 (letzte 32 Bit) = 2001:DB 8:90: :192.0.2.60

- Quell-IP-Adressfeld = SEVR-IPv6 = 2001:DB 8:5001::30

6. Die Appliance empfängt das IPv6-Antwortpaket und überprüft, ob ihre Ziel-IP-Adresse mit dem auf der Appliance konfigurierten NAT46-Präfix übereinstimmt. Da die Zieladresse mit dem NAT46-Präfix übereinstimmt, durchsucht die Appliance die NAT46-INAT-Einträge nach der IPv4-Adresse, die der SEVR-IPv6-Adresse zugeordnet ist (2001:DB 8:5001: :30). Es findet die Map-Sevr-IPv4-Adresse (192.0.2.180).
7. Die Appliance erstellt ein IPv4-Antwortpaket mit:
   - Ziel-IP-Adressfeld = Das NAT46-Präfix wurde aus der Zieladresse der IPv6-Antwort entfernt = Client_IPv4 (192.0.2.60)
   - Quell-IP-Adressfeld = Map-Sevr-IPv4-Adresse (192.0.2.180)
8. Die Appliance sendet die übersetzte IPv4-Antwort an den Client CL1.

Einschränkungen von Stateless NAT46

Die folgenden Einschränkungen gelten für statusloses NAT46:

- Die Übersetzung von IPv4-Optionen wird nicht unterstützt.
- Die Übersetzung von IPv6-Routing-Headern wird nicht unterstützt.
- Die Übersetzung von Hop-by-Hop-Erweiterungsheadern von IPv6-Paketen wird nicht unterstützt.
- Die Übersetzung von ESP- und EH-Headern von IPv4-Paketen wird nicht unterstützt.
- Die Übersetzung von Multicast-Paketen wird nicht unterstützt.
- Die Übersetzung von Zieloptionsheadern und Quell-Routing-Headern wird nicht unterstützt.
- Die Übersetzung fragmentierter IPv4-UDP-Pakete, die keine UDP-Prüfsumme enthalten, wird nicht unterstützt.

Stateless NAT46 konfigurieren

Das Erstellen der erforderlichen Entitäten für die statuslose NAT46-Konfiguration auf der NetScaler-Appliance umfasst die folgenden Verfahren:

1. Erstellen Sie einen IPv4-IPv6-Mapping-INAT-Eintrag mit aktiviertem Stateless Mode.
2. Erstellen Sie ein NAT46-IPv6-Präfix.

CLI-Verfahren

So konfigurieren Sie einen INAT-Mapping-Eintrag mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- füge den <name><publicIPv4><privateIPv6>-mode STATELESS hinzu
- show inat <name>

Um ein NAT46-Präfix mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- setze inatparam -nat46v6Prefix <ipv6_addr|*>
- show inatparam

Beispiel:

```
 > add inat exmpl-com-stls-nat46 192.0.2.180
2001:DB8:5001::30 -mode stateless
Done

> set inatparam -nat46v6Prefix 2001:DB8:90::/96
Done
<!--NeedCopy-->
```

GUI-Verfahren

Um einen INAT-Mapping-Eintrag mithilfe der GUI zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie zu System > Netzwerk > Routen > INAT.
2. Fügen Sie einen neuen INAT-Eintrag hinzu oder bearbeiten Sie einen vorhandenen INAT-Eintrag.
3. Legen Sie die folgenden Parameter fest:
    - Vorname*
    - Öffentliche IP-Adresse*
    - Private IP-Adresse* (Markieren Sie das IPv6-Kontrollkästchen und geben Sie die Adresse im IPv6-Format ein.)
    - Modus (Wählen Sie Stateless aus der Dropdownliste aus.)

    * Ein erforderlicher Parameter

Um ein NAT46-Präfix mithilfe der GUI zu erstellen:

Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungenauf INAT-Parameter konfigurieren**, und legen Sie den**Präfix-Parameter** fest.

Einstellung globaler Parameter für Stateless NAT46

Die Appliance stellt einige optionale globale Parameter für statuslose NAT46-Konfigurationen bereit.

Gehen Sie wie folgt vor, um globale Parameter für statusloses NAT46 mithilfe der CLI festzulegen:

Geben Sie in der Befehlszeile Folgendes ein:

- **set inatparam** [-**nat46IgnoreTOS** (**YES** | **NO**)] [-**nat46ZeroCheckSum** (**ENABLED** | **DISABLED**)] [-**nat46v6Mtu** \<positive_integer>] [-**nat46FragHeader** (**ENABLED** | **DISABLED**)]
- **show inatparam**

Beispiel:

```
> set inatparam -nat46IgnoreTOS YES -nat46ZeroCheckSum DISABLED -
    nat46v6Mtu 1400 -nat46FragHeader DISABLED
 Done
<!--NeedCopy-->
```

Um globale Parameter für statusloses NAT46 mithilfe der GUI festzulegen:

Navigieren Sie zu **System** > **Netzwerk**und klicken Sie in der Gruppe **Einstellungenauf INAT-Parameter konfigurieren**.

DNS64

May 11, 2023

Die NetScaler DNS64-Funktion reagiert mit einem synthetisierten DNS-AAAA-Datensatz auf einen IPv6-Client, der eine AAAA-Anfrage für eine reine IPv4-Domäne sendet. Die DNS64-Funktion wird zusammen mit der NAT64-Funktion verwendet, um eine nahtlose Kommunikation zwischen reinen IPv6-Clients und reinen IPv4-Servern zu ermöglichen. DNS64 ermöglicht die Erkennung der IPv4-Domäne durch reine IPv6-Clients, und NAT64 ermöglicht die Kommunikation zwischen den Clients und Servern.

Für die Synthese eines AAAA-Eintrags ruft die NetScaler-Appliance einen DNS-A-Datensatz von einem DNS-Server ab. Das DNS64-Präfix ist ein 96-Bit-IPv6-Präfix, das auf der NetScaler-Appliance konfiguriert ist. Die NetScaler-Appliance synthetisiert den AAAA-Datensatz durch Verkettung des DNS64-Präfixes (96 Bit) und der IPv4-Adresse (32 Bit).

Um die Kommunikation zwischen IPv6-Clients und IPv4-Servern zu ermöglichen, kann eine NetScaler-Appliance mit DNS64- und NAT64-Konfiguration entweder auf der IPv6-Clientseite oder auf der IPv4-Serverseite bereitgestellt werden. In beiden Fällen ist die DNS64-Konfiguration auf der NetScaler-Appliance ähnlich und beinhaltet einen virtuellen Lastausgleichsserver, der als Proxyserver für DNS-Server fungiert. Wenn die NetScaler-Appliance auf der Clientseite bereitgestellt wird, muss der virtuelle Load-Balancing-Server auf dem IPv6-Client als Nameserver für eine Domäne angegeben werden.

Stellen Sie sich ein Beispiel vor, in dem eine NetScaler-Appliance mit DNS64- und NAT64-Konfiguration auf der IPv4-Seite konfiguriert ist. In diesem Beispiel hostet ein Unternehmen

die Website www.example.com auf dem Server S1, der eine IPv4-Adresse hat. Um die Kommunikation zwischen IPv6-Clients und dem IPv4-Server S1 zu ermöglichen, wird die NetScaler Appliance NS1 mit einer DNS64- und statusfähigen NAT64-Konfiguration bereitgestellt.

Die DNS64-Konfiguration umfasst den virtuellen DNS-Lastausgleichsserver LBVS-DNS64-1, auf dem die DNS64-Option aktiviert ist. Eine DNS64-Richtlinie mit dem Namen DNS64-Policy-1 und eine zugehörige DNS64-Aktion mit dem Namen DNS64-Action-1 sind ebenfalls auf NS1 konfiguriert, und DNS64-Policy-1 ist an LBVS-DNS64-1 gebunden. LBVS-DNS64-1 fungiert als DNS-Proxyserver für die DNS-Server DNS-1 und DNS-2.

Wenn der bei LBVS-DNS64-1 eingehende Verkehr den in DNS64-Policy-1 angegebenen Bedingungen entspricht, wird der Datenverkehr gemäß den Einstellungen in DNS64-Action-1 verarbeitet. DNS64-Action-1 gibt das DNS64-Präfix an, das zusammen mit dem von einem DNS-Server empfangenen A-Eintrag verwendet wird, um einen AAAA-Eintrag zu synthetisieren.

Der globale DNS-Parameter cacherecords ist auf der NetScaler-Appliance aktiviert, sodass die Appliance DNS-Einträge zwischenspeichert. Diese Einstellung ist erforderlich, damit der DNS64 ordnungsgemäß funktioniert.

In der folgenden Tabelle sind die im obigen Beispiel verwendeten Einstellungen aufgeführt: DNS64-Beispieleinstellungen.

Es folgt der Verkehrsfluss in diesem Beispiel:

1. Der IPv6-Client CL1 sendet eine DNS-AAAA-Anfrage für die IPv6-Adresse der Site www.example.com.
2. Die Anfrage wird vom virtuellen DNS-Lastausgleichsserver LBVS-DNS64-1 auf der NetScaler Appliance NS1 empfangen.
3. NS1 überprüft seine DNS-Cache-Einträge auf den angeforderten AAAA-Eintrag und stellt fest, dass der AAAA-Eintrag für die Site www.example.com nicht im DNS-Cache vorhanden ist.
4. Der Load-Balancing-Algorithmus von LBVS-DNS64-1 wählt den DNS-Server DNS-1 aus und leitet die AAAA-Anfrage an ihn weiter.
5. Da die Site www.example.com auf einem IPv4-Server gehostet wird, hat der DNS-Server DNS-1 keinen AAAA-Eintrag für die Site www.example.com.
6. DNS-1 sendet entweder eine leere DNS-AAAAA-Antwort oder eine Fehlermeldung an LBVS-DNS64-1.
7. Da die DNS64-Option auf LBVS-DNS64-1 aktiviert ist und die AAAA-Anfrage von CL1 der in DNS64-Policy-1 angegebenen Bedingung entspricht, sendet NS1 eine DNS-A-Anfrage an DNS-1 für die IPv4-Adresse von www.example.com.
8. DNS-1 reagiert, indem es den DNS-A-Eintrag für www.example.com an LBVS-DNS64-1 sendet. Der A-Datensatz enthält die IPv4-Adresse für www.example.com.
9. NS1 synthetisiert einen AAAA-Datensatz für die Site www.example.com mit:
    - IPv6 address for site www.example.com = Concatenation of DNS64 Prefix (96 bits) specified in the associated DNS64action, and IPv4 address of DNS A record (32 bits) = 2001:DB8:300::192.0.2.60

10. NS1 sendet den synthetisierten AAAA-Datensatz an den IPv6-Client CL1. NS1 speichert auch den A-Datensatz in seinem Speicher. NS1 verwendet den zwischengespeicherten A-Datensatz, um AAAA-Datensätze für nachfolgende AAAA-Anfragen zu synthetisieren.

Punkte, die bei einer DNS64-Konfiguration zu beachten sind

Bevor Sie DNS64 auf einer NetScaler-Appliance konfigurieren, sollten Sie die folgenden Punkte berücksichtigen:

- Die DNS64-Funktion der NetScaler-Appliance entspricht RFC 6174.
- Die DNS64-Funktion der NetScaler-Appliance unterstützt DNSSEC nicht. Die NetScaler-Appliance synthetisiert keinen AAAA-Datensatz aus einer DNSSEC-Antwort, die von einem DNS-Server empfangen wurde. Eine Antwort wird nur dann als DNSSEC-Antwort klassifiziert, wenn sie RRSIG-Datensätze enthält.
- Die NetScaler-Appliance unterstützt das DNS64-Präfix mit einer Länge von nur 96 Bit.
- Obwohl die DNS64-Funktion zusammen mit der NAT64-Funktion verwendet wird, sind die DNS64- und NAT64-Konfigurationen von der NetScaler-Appliance unabhängig. Für einen bestimmten Flow müssen Sie denselben IPv6-Präfixwert für das DNS64-Präfix und die NAT64-Präfixparameter angeben, damit die vom Client empfangenen synthetisierten IPv6-Adressen an die bestimmte NAT64-Konfiguration weitergeleitet werden. Weitere Informationen zum Konfigurieren von NAT64 auf einer NetScaler Appliance finden Sie unter Stateful NAT64.
- Im Folgenden sind die verschiedenen Fälle der DN64-Verarbeitung durch die NetScaler Appliance aufgeführt:
  - Wenn die AAAA-Antwort des DNS-Servers AAAA-Einträge enthält, wird jeder Datensatz in der Antwort auf den Satz von Ausschlussregeln überprüft, der auf der NetScaler-Appliance für die jeweilige DNS64-Konfiguration konfiguriert ist. Der NetScaler entfernt die IPv6-Adressen, deren Präfix der Ausnahmeregel entspricht, aus der Antwort. Wenn die resultierende Antwort mindestens einen IPv6-Datensatz enthält, leitet die NetScaler-Appliance diese Antwort an den Client weiter. Andernfalls synthetisiert die Appliance eine AAAA-Antwort aus dem A-Datensatz der Domäne und sendet sie an den IPv6-Client.
  - Wenn die AAAA-Antwort des DNS-Servers eine leere Antwortantwort ist, fordert die Appliance A-Ressourceneinträge mit demselben Domainnamen an oder sucht in ihren eigenen Datensätzen, ob die Appliance ein authentischer Domainnamenserver für die Domain ist. Wenn die Anfrage zu einer leeren Antwort oder einem leeren Fehler führt, wird diese an den Client weitergeleitet.
  - Wenn die Antwort des DNS-Servers RCODE=1 (Formatfehler) enthält, leitet die NetScaler-Appliance dies an den Client weiter. Wenn vor dem Timeout keine Antwort erfolgt, sendet die NetScaler-Appliance eine Antwort mit RCODE=2 (Serverausfall) an den Client.

  - Wenn die Antwort des DNS-Servers einen CNAME enthält, wird die Kette so lange verfolgt, bis der abschließende A- oder AAAA-Datensatz erreicht ist. Wenn der CNAME keine AAAA-Ressourceneinträge hat, ruft die NetScaler-Appliance den DNS-A-Datensatz ab, der für die Synthese des AAAA-Datensatzes verwendet werden soll. Die CNAME-Kette wird zusammen mit dem synthetisierten AAAA-Datensatz zum Antwortabschnitt hinzugefügt und dann an den Client gesendet.

- Die DNS64-Funktion der NetScaler-Appliance unterstützt auch die Beantwortung von PTR-Anfragen. Wenn eine PTR-Anfrage für eine Domäne mit einer IPv6-Adresse auf der Appliance empfangen wird und die IPv6-Adresse mit einem der konfigurierten DNS64-Präfixe übereinstimmt, erstellt die Appliance einen CNAME-Datensatz, der die IP6-ARPA-Domäne dem entsprechenden IN-ADDR zuordnet. Die ARPA-Domain und die neu gegründete IN-ADDR.ARPA-Domain werden zur Auflösung verwendet. Die Appliance durchsucht die lokalen PTR-Einträge und wenn die Datensätze nicht vorhanden sind, sendet die Appliance eine PTR-Anfrage für die IN-ADDR.ARPA-Domäne an den DNS-Server. Die NetScaler-Appliance verwendet die Antwort des DNS-Servers, um die Antwort für die erste PTR-Anfrage zu synthetisieren.

Konfigurationsschritte

Das Erstellen der erforderlichen Entitäten für die statusmäßige NAT64-Konfiguration auf der NetScaler-Appliance umfasst die folgenden Verfahren:

- **Fügen Sie DNS-Dienste hinzu.** DNS-Dienste sind logische Darstellung von DNS-Servern, für die die NetScaler Appliance als DNS-Proxyserver fungiert. Weitere Informationen zum Festlegen optionaler Parameter eines Dienstes finden Sie unter Load Balancing.
- **Fügen Sie DNS64-Aktion und DNS64-Richtlinie hinzu, und binden Sie dann die DNS64-Aktion an die DNS64-Richtlinie.** Eine DNS64-Richtlinie legt die Bedingungen fest, die gemäß den Einstellungen in der zugehörigen DNS64-Aktion mit dem Datenverkehr für die DNS64-Verarbeitung abgeglichen werden. Die DNS64-Aktion gibt das obligatorische DNS64-Präfix und die optionalen Einstellungen für die Ausschlussregel und die zugeordneten Regeln an.
- **Erstellen Sie einen virtuellen DNS-Lastausgleichsserver und binden Sie die DNS-Dienste und die DNS64-Richtlinie daran.** Der virtuelle DNS-Lastenausgleichsserver fungiert als DNS-Proxyserver für DNS-Server, die durch die gebundenen DNS-Dienste repräsentiert werden. Datenverkehr, der auf dem virtuellen Server eintrifft, wird mit der gebundenen DNS64-Richtlinie für die DNS64-Verarbeitung abgeglichen. Weitere Informationen zum Festlegen optionaler Parameter eines virtuellen Lastausgleichsservers finden Sie unter Load Balancing.

  Hinweis: Die CLI verfügt über separate Befehle für diese beiden Aufgaben, aber die GUI kombiniert sie in einem einzigen Dialogfeld.

  Aktivieren Sie das Zwischenspeichern von DNS-Einträgen. Aktivieren Sie den globalen Parameter für die NetScaler Appliance, um DNS-Einträge zwischenzuspeichern, die über

DNS-Proxyvorgänge abgerufen werden. Weitere Informationen zum Aktivieren des Zwischenspeichers von DNS-Datensätzen finden Sie unter Domänennamensystem.

CLI-Verfahren

Um einen Dienst vom Typ DNS mithilfe der CLI zu erstellen, gehen Sie wie folgt vor:

Geben Sie in der Befehlszeile Folgendes ein:

- add service <name> <IP> <serviceType> <port> …

Um eine DNS64-Aktion mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- add dns action64 <actionName> -Prefix <ipv6_addr|*> [-mappedRule \<expression>] [-excludeRule \<expression>]

So erstellen Sie eine DNS64-Richtlinie mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- add dns policy64 <name> -rule <expression> -action <string>

Um einen virtuellen DNS-Lastausgleichsserver mithilfe der CLI zu erstellen, gehen Sie wie folgt vor:

Geben Sie in der Befehlszeile Folgendes ein:

- add lb vserver <name> DNS <IPAddress> <port> -dns64 (ENABLED | DISABLED) [-bypassAAAA (YES | NO)] …

So binden Sie die DNS-Dienste und die DNS64-Richtlinie an den virtuellen DNS-Lastausgleichsserver mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- bind lb vserver <name> <serviceName> …
- bind lb vserver <name> -policyName <string> -priority <positive_integer> …

GUI-Verfahren

Um einen Dienst vom Typ DNS mithilfe der GUI zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services und fügen Sie einen neuen Dienst hinzu.
2. Legen Sie die folgenden Parameter fest:
   - Name des Diensts*
   - Server*
   - Protokoll* (Wählen Sie DNS aus der Dropdown-Liste aus.)

- Port*

Um eine DNS64-Aktion mithilfe der GUI zu erstellen:

Navigieren Sie zu Traffic Management > DNS > Actions und fügen Sie auf der Registerkarte DNS Actions64 eine neue DNS64-Aktion hinzu.

So erstellen Sie eine DNS64-Richtlinie mithilfe der GUI:

Navigieren Sie zu Traffic Management > DNS > Policies und fügen Sie auf der Registerkarte DNS-Policies64 eine neue DNS64-Richtlinie hinzu.

Gehen Sie wie folgt vor, um einen virtuellen DNS-Lastausgleichsserver zu erstellen und die DNS-Dienste und die DNS64-Richtlinie mithilfe der GUI daran zu binden:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server und fügen Sie einen neuen virtuellen Server hinzu.
2. Legen Sie die folgenden Parameter fest:
   - Vorname*
   - IP-Adresse*
   - Protokoll* (Wählen Sie DNS aus der Dropdown-Liste aus.)
   - Port*
3. Wählen Sie die Option DNS64 aktivieren.
4. Binden Sie den Dienst im Bereich Dienste an den virtuellen Server.
5. Binden Sie die Richtlinie im Bereich Richtlinien an den virtuellen Server.

Beispielkonfiguration

```
 > add service SVC-DNS-1 203.0.113.50 DNS 53
 Done

> add service SVC-DNS-2 203.0.113.60 DNS 53
 Done

> add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
 Done

> add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET
   (2001:DB8:5001::/64)"
-action DNS64-Action-1
 Done

> add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
 Done

```



```
> bind lb vserver LBVS-DNS64-1 SVC-DNS-1
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-2
 Done

> bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
 Done

<!--NeedCopy-->
```

Zustandsbehaftete NAT64-Übersetzung

May 12, 2023

Die statusmäßige NAT64-Funktion ermöglicht die Kommunikation zwischen IPv6-Clients und IPv4-Servern über die IPv6-zu-IPv4-Paketübersetzung und umgekehrt, wobei die Sitzungsinformationen auf der NetScaler-Appliance erhalten bleiben.

Eine statusmäßige NAT64-Konfiguration auf der NetScaler-Appliance besteht aus den folgenden Komponenten:

- **NAT64-Regel**— Ein Eintrag, der aus einer ACL6-Regel und einem Netzprofil besteht, das aus einem Pool von NetScaler-eigenen SNIP-Adressen besteht.
- **NAT64-IPv6-Präfix**— Ein globales IPv6-Präfix mit einer Länge von 96 Bit (128-32=96), das auf der Appliance konfiguriert ist.
  Hinweis: Derzeit unterstützt die NetScaler-Appliance nur ein Präfix, das gemeinsam mit allen NAT 64-Regeln verwendet wird.

Die NetScaler-Appliance betrachtet ein eingehendes IPv6-Paket für die NAT64-Übersetzung, wenn alle der folgenden Bedingungen erfüllt sind:

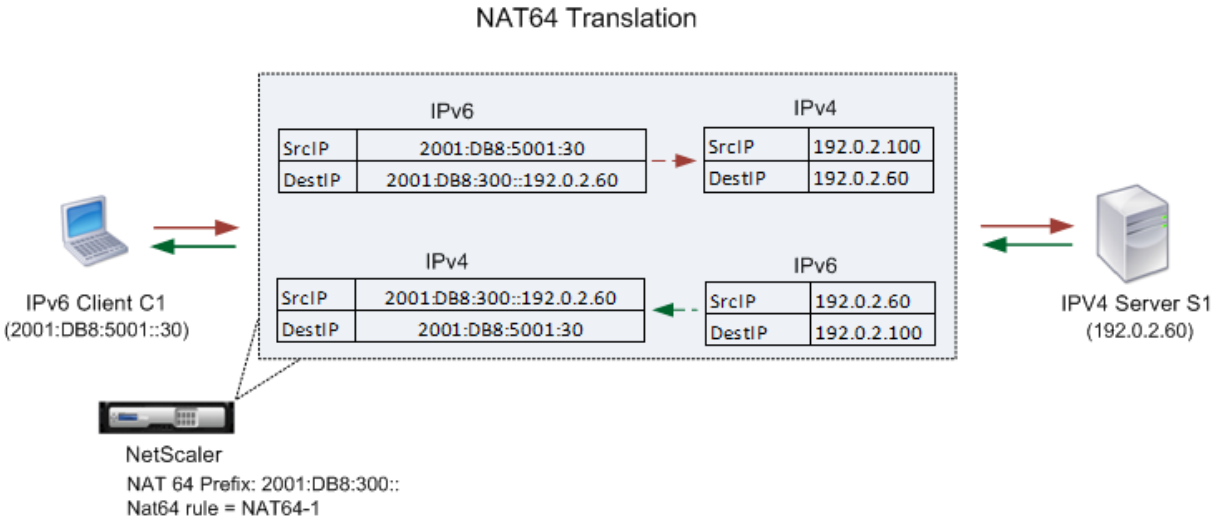
- Das eingehende IPv6-Paket entspricht der ACL6-Regel, die an eine NAT64-Regel gebunden ist.
- Die Ziel-IP-Adresse des IPv6-Pakets entspricht dem NAT64-IPv6-Präfix.

Wenn ein von der NetScaler-Appliance empfangenes IPv6-Anforderungspaket mit einer in einer NAT64-Regel definierten ACL6 übereinstimmt und die Ziel-IP des Pakets mit dem NAT64-IPv6-Präfix übereinstimmt, betrachtet die NetScaler-Appliance das IPv6-Paket zur Übersetzung.

Die Appliance übersetzt dieses IPv6-Paket in ein IPv4-Paket mit einer Quell-IP-Adresse, die einer der IP-Adressen entspricht, die an das in der NAT64-Regel definierte Netzprofil gebunden sind, und einer Ziel-IP-Adresse, die aus den letzten 32 Bit der Ziel-IPv6-Adresse des IPv6-Anforderungspakets besteht. Die NetScaler-Appliance erstellt eine NAT64-Sitzung für diesen bestimmten Flow und

leitet das Paket an den IPv4-Server weiter. Nachfolgende Antworten vom IPv4-Server und Anfragen vom IPv6-Client werden von der Appliance auf der Grundlage der Informationen in der jeweiligen NAT64-Sitzung entsprechend übersetzt.

Stellen Sie sich ein Beispiel vor, in dem ein Unternehmen die Website www.example.com auf dem Server S1 hostet, der über eine IPv4-Adresse verfügt. Um die Kommunikation zwischen IPv6-Clients und IPv4-Server S1 zu ermöglichen, wird die NetScaler Appliance NS1 mit einer statusbehafteten NAT64-Konfiguration bereitgestellt, die eine NAT64-Regel und ein NAT64-Präfix enthält. Eine zugeordnete IPv6-Adresse des Servers S1 wird gebildet, indem das NAT64-IPv6-Präfix [96 Bit] und die IPv4-Quelladresse [32 Bit] verkettet werden. Diese zugeordnete IPv6-Adresse wird dann manuell auf den DNS-Servern konfiguriert. Die IPv6-Clients erhalten die zugeordnete IPv6-Adresse von den DNS-Servern, um mit dem IPv4-Server S1 zu kommunizieren.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: Beispieleinstellungen für Stateful NAT64.

Es folgt der Verkehrsfluss in diesem Beispiel:

1. Der IPv6-Client CL1 sendet ein Anforderungspaket an die Map-Sevr-IPv6-Adresse (2001:DB 8:300: :192.0.2.60).
2. Die NetScaler-Appliance empfängt das Anforderungspaket. Wenn das Anforderungspaket mit der in der NAT64-Regel definierten ACL6 übereinstimmt und die Ziel-IP-Adresse des Pakets mit dem NAT64-IPv6-Präfix übereinstimmt, betrachtet NetScaler das IPv6-Paket zur Übersetzung.
3. Die Appliance erstellt ein übersetztes IPv4-Anforderungspaket mit:
   - Ziel-IP-Adressfeld, das das NAT64-Präfix enthält, das aus der Zieladresse der IPv6-Anfrage entfernt wurde (sevr_IPv4 = 192.0.2.60)
   - Feld für die Quell-IP-Adresse, das eine der an Netprofile-1 gebundenen IPv4-Adressen enthält (in diesem Fall 192.0.2.100)

4. Die NetScaler-Appliance erstellt eine NAT64-Sitzung für diesen Flow und sendet die übersetzte IPv4-Anfrage an Server S1.
5. Der IPv64-Server S1 sendet daraufhin ein IPv4-Paket an die NetScaler-Appliance mit:
    - Ziel-IP-Adressfeld, das 192.0.2.100 enthält
    - Quell-IP-Adressfeld, das die Adresse von SEVR_IPv4 enthält (192.0.2.60)
6. Die Appliance empfängt das IPv4-Antwortpaket, durchsucht alle Sitzungseinträge und stellt fest, dass das IPv6-Antwortpaket mit dem in Schritt 4 erstellten NAT64-Sitzungseintrag übereinstimmt. Die Appliance betrachtet das IPv4-Paket für die Übersetzung.
7. Die Appliance erstellt ein übersetztes IPv6-Antwortpaket mit:
    - Ziel-IP-Adresse Feld=client_IPv6=2001:DB 8:5001::30
    - Quell-IP-Adressfeld = Verkettung von NAT64-Präfix (erste 96 Bit) und SEVR_IPv4 (letzte 32 Bit) =2001:DB 8:300: :192.0.2.60
8. Die Appliance sendet die übersetzte IPv6-Antwort an den Client CL1.

Einschränkungen von Statelful NAT64

Die folgenden Einschränkungen gelten für stateful-NAT64:

- Die Übersetzung von IPv4-Optionen wird nicht unterstützt.
- Die Übersetzung von IPv6-Routing-Headern wird nicht unterstützt.
- Die Übersetzung von Hop-by-Hop-Erweiterungsheadern von IPv6-Paketen wird nicht unterstützt.
- Die Übersetzung von ESP- und EH-Headern von IPv6-Paketen wird nicht unterstützt.
- Die Übersetzung von Multicast-Paketen wird nicht unterstützt.
- Pakete von Stream Control Transmission Protocol (SCTP), Datagram Congestion Control Protocol (DCCP) und IPSec werden nicht übersetzt.

Konfiguration von Stateful NAT64

Das Erstellen der erforderlichen Entitäten für die statusmäßige NAT64-Konfiguration auf der NetScaler-Appliance umfasst die folgenden Verfahren:

1. Fügen Sie eine ACL6-Regel mit der Aktion ALLOW hinzu.
2. Fügen Sie ein IPset hinzu, das mehrere IP-Adressen bindet.
3. Fügen Sie ein Netzprofil hinzu und binden Sie das IPset daran. Wenn Sie nur eine IP-Adresse binden möchten, müssen Sie keine IPset-Entität erstellen. Binden Sie in diesem Fall die IP-Adresse direkt an das Netzprofil.
4. Fügen Sie eine NAT64-Regel hinzu, die die Bindung der ACl6-Regel und des Netzprofils an die NAT64-Regel beinhaltet.

5. Fügen Sie ein NAT64-IPv6-Präfix hinzu.

CLI-Verfahren

So fügen Sie eine ACL6-Regel mithilfe der CLI hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- <acl6name><acl6action>füge ns acl6 hinzu…

Um ein IPSet hinzuzufügen und mehrere IPs daran zu binden, verwenden Sie die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- add ipset <name>
- bind ipset <name> <IPaddress …>

Um ein Netzprofil mit der CLI hinzuzufügen:

Geben Sie in der Befehlszeile Folgendes ein:

- add netprofile <name> -srcIP <IPaddress or IPset>

So fügen Sie mit der CLI eine NAT64-Regel hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- add nat64 <name> <acl6name> -netProfile <string>

So fügen Sie mit der CLI ein NAT64-Präfix hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- set ipv6 -natprefix <ipv6_addr|*>

Beispiel:

```
 > add acl6 ACL6-1 ALLOW -srcIPv6 2001:DB8:5001::30
 Done

> apply acls6
 Done

> add ip 192.0.2.100 255.255.255.0  - type SNIP
 Done

> add ip 192.0.2.102 255.255.255.0   - type SNIP
 Done

> add ipset IPset-1
 Done
```



```
15
16 > bind ipset IPset-1 192.0.2.100 192.0.2.102
17 IPAddress "192.0.2.100" bound
18 IPAddress "192.0.2.102" bound
19  Done
20
21 > add netprofile Netprofile-1 -srcIP IPset-1
22  Done
23
24 > add nat64 NAT64-1 ACL6-1 -netprofile Netprofile-1
25  Done
26
27 > set ipv6 -natprefix 2001:DB8:300::/96
28  Done
29 <!--NeedCopy-->
```

GUI-Verfahren

So fügen Sie mit der GUI eine NAT64-Regel hinzu:

Navigieren Sie zu System > Netzwerk > Routen > NAT64 und geben Sie eine neue NAT64-Regel ein, oder bearbeiten Sie eine bestehende Regel.

So fügen Sie mit der GUI ein NAT64-Präfix hinzu:

Navigieren Sie zu System > Netzwerk, klicken Sie in der Gruppe Einstellungenauf INAT-Parameter konfigurieren, und legen Sie den Präfix-Parameter fest.

RNAT

May 11, 2023

Bei Reverse Network Address Translation (RNAT) ersetzt die NetScaler-Appliance die Quell-IP-Adressen in den von den Servern generierten Paketen durch öffentliche NAT-IP-Adressen. Standardmäßig verwendet die Appliance eine SNIP-Adresse als NAT-IP-Adresse. Sie können die Appliance auch so konfigurieren, dass sie für jedes Subnetz eine eindeutige NAT-IP-Adresse verwendet. Sie können RNAT auch mithilfe von Zugriffssteuerungslisten (Access Control Lists, ACLs) konfigurieren. Die Modi Quell-IP (USIP) verwenden, Subnetz-IP verwenden (USNIP) und Link Load Balancing (LLB) wirken sich auf den Betrieb von RNAT aus. Sie können Statistiken anzeigen, um RNAT zu überwachen.

Hinweis: Der kurzlebige Portbereich für RNAT auf der NetScaler-Appliance ist 1024-65535.

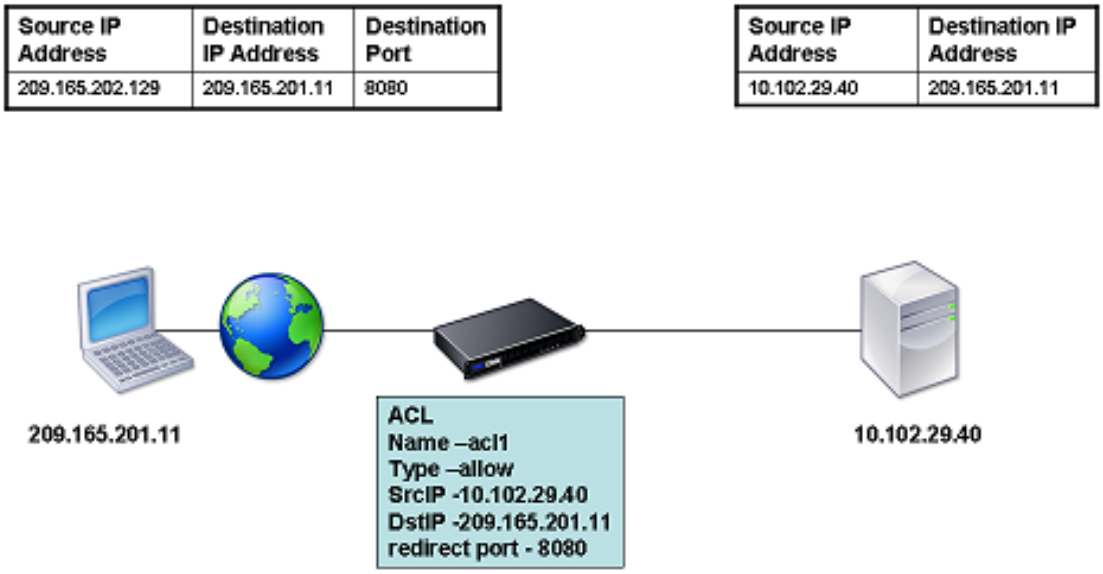
Sie können entweder eine Netzwerkadresse oder eine erweiterte ACL als Bedingung für einen RNAT-Eintrag verwenden:

- **Verwenden einer Netzwerkadresse.** Wenn Sie eine Netzwerkadresse verwenden, wird die RNAT-Verarbeitung für alle Pakete ausgeführt, die aus dem angegebenen Netzwerk kommen.
- **Verwenden erweiterter ACLs.** Wenn Sie ACLs verwenden, wird die RNAT-Verarbeitung für alle Pakete durchgeführt, die den ACLs entsprechen. Um die NetScaler-Appliance so zu konfigurieren, dass sie eine eindeutige IP-Adresse für Datenverkehr verwendet, der einer ACL entspricht, müssen Sie die folgenden drei Aufgaben ausführen:

  1. Konfigurieren Sie die ACL.
  2. Konfigurieren Sie RNAT, um die Quell-IP-Adresse und den Zielport zu ändern.
  3. Wenden Sie die ACL an.

  Das folgende Diagramm zeigt, dass RNAT mit einer ACL konfiguriert ist.

  Abbildung 1. RNAT mit einer ACL



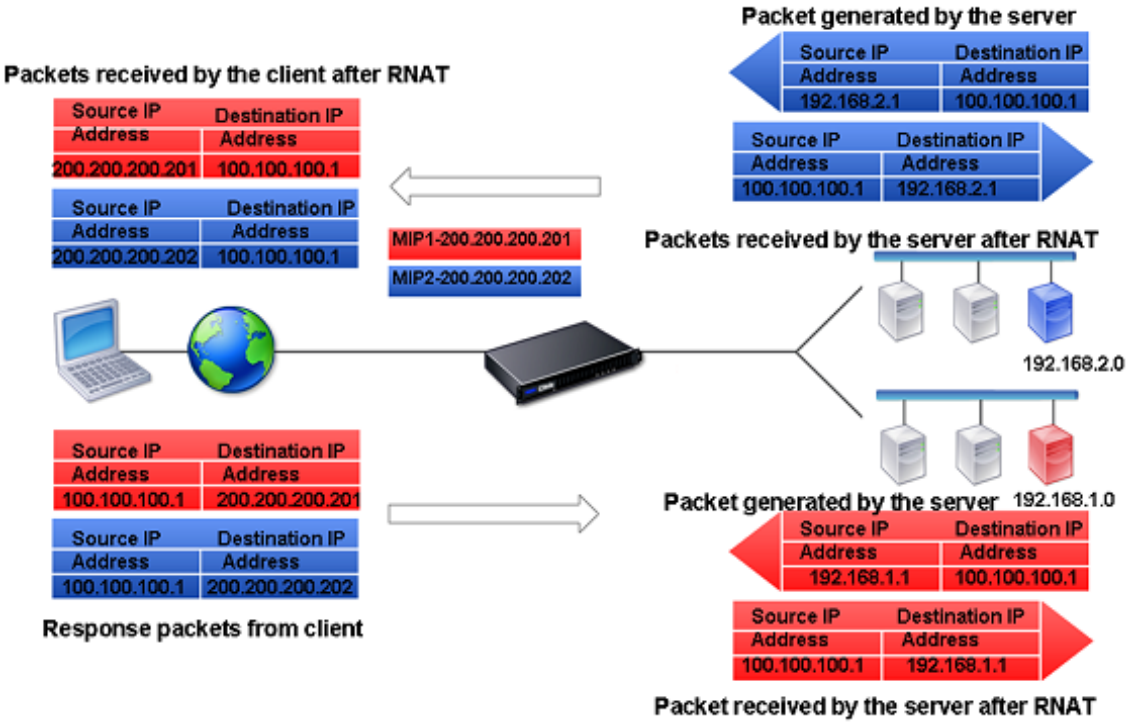
Sie haben die folgenden grundlegenden Optionen für den Typ der NAT-IP-Adresse:

- **Verwenden eines SNIP als NAT-IP-Adresse.** Wenn Sie ein SNIP als NAT-IP-Adresse verwenden, ersetzt die NetScaler-Appliance die Quell-IP-Adressen der servergenerierten Pakete durch eine SNIP. Daher muss die SNIP-Adresse eine öffentliche IP-Adresse sein. Wenn der Modus „Subnetz-IP verwenden“ (USNIP) aktiviert ist, kann der NetScaler eine Subnetz-IP-Adresse (SNIP) als NAT-IP-Adresse verwenden.
- **Verwendung einer eindeutigen IP-Adresse als NAT-IP-Adresse.** Wenn Sie eine eindeutige IP-

Adresse als NAT-IP-Adresse verwenden, ersetzt die NetScaler-Appliance die Quell-IP-Adressen der servergenerierten Pakete durch die angegebene eindeutige IP-Adresse. Bei der eindeutigen IP-Adresse muss es sich um eine öffentliche Netscaler-eigene IP-Adresse handeln. Wenn mehrere NAT-IP-Adressen für ein Subnetz konfiguriert sind, verwendet die NAT-IP-Auswahl den Round-Robin-Algorithmus.

Diese Konfiguration ist in der folgenden Abbildung dargestellt.

Abbildung 2. Verwenden einer eindeutigen IP-Adresse als NAT-IP-Adresse



Voraussetzungen

Beachten Sie vor der Konfiguration einer RNAT-Regel die folgenden Punkte:

- Wenn RNAT und Use Source IP (USIP) beide auf der NetScaler-Appliance konfiguriert sind, hat RNAT Vorrang. Mit anderen Worten, die Quell-IP-Adresse der Pakete, die einer RNAT-Regel entspricht, wird entsprechend der Einstellung in der RNAT-Regel ersetzt.
- In einer Topologie, in der die NetScaler-Appliance sowohl Link Load Balancing (LLB) als auch RNAT für den vom Server stammenden Datenverkehr durchführt, wählt die Appliance die Quell-IP-Adresse auf der Grundlage des Routers aus. Die LLB-Konfiguration bestimmt die Auswahl des Routers. Weitere Informationen zu LLB finden Sie unter Link-Lastenausgleich.

RNAT konfigurieren

Die folgenden Anweisungen enthalten separate Befehlszeilenverfahren zum Erstellen von RNAT-Einträgen, die unterschiedliche Bedingungen und verschiedene Arten von NAT-IP-Adressen verwenden. In der GUI können alle Varianten im selben Dialogfeld konfiguriert werden, sodass es nur ein Verfahren für GUI-Benutzer gibt.

CLI-Verfahren

Um eine RNAT-Regel mit der CLI zu erstellen:

Geben Sie an der Eingabeaufforderung Folgendes ein, um die Regel zu erstellen und die Konfiguration zu überprüfen:

- `add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))`
- `bind rnat <name> <natIP>@ …`
- `show rnat`

So ändern oder entfernen Sie eine RNAT-Regel mithilfe der CLI:

- Um eine RNAT-Regel zu ändern:

  `set rnat <name> (<aclname> [-redirectPort <port>])`

- Um eine RNAT-Regel zu entfernen, geben Sie den Befehl ein.

  `rm rnat <name>`

Verwenden Sie den folgenden Befehl, um die Konfiguration zu überprüfen:

- `show rnat`

Beispiele:

```
A network address as the condition and a SNIP address as the NAT IP
    address:

> add rnat RNAT-1 192.168.1.0 255.255.255.0
Done

A network address as the condition and a unique IP address as the NAT
    IP address:

> add rnat RNAT-2 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-2 -natip 10.102.29.50
Done

```



```
If instead of a single NAT IP address you specify a range, RNAT entries are created with all the NetScaler-owned IP addresses, except the NSIP, that fall within the range specified:

> add rnat RNAT-3 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-3 -natip 10.102.29.[50-110]
Done


An ACL as the condition and a SNIP address as the NAT IP address:

> add rnat RNAT-4 acl1
Done

An ACL as a condition and a unique IP address as the NAT IP address:

> add rnat RNAT-4 acl1
Done

> bind rnat RNAT-4 -natip 10.102.29.50
Done

If instead of a single NAT IP address you specify a range, RNAT entries are created with all the NetScaler-owned IP addresses, except the NSIP, that fall within the range specified:

> add rnat RNAT-5 acl1
Done

> bind rnat RNAT-5 -natip 10.102.29.[50-70]
Done

<!--NeedCopy-->
```

GUI-Verfahren

Um einen RNAT-Eintrag mit der GUI zu erstellen:

Navigieren Sie zu **System** > **Netzwerk** > **NATs**, klicken Sie auf die Registerkarte **RNAT** und fügen Sie eine neue RNAT-Regel hinzu oder bearbeiten Sie eine bestehende Regel.

RNAT überwachen

Sie können RNAT-Statistiken anzeigen, um Probleme im Zusammenhang mit der IP-Adressübersetzung zu beheben.

In der folgenden Tabelle werden die Statistiken beschrieben, die mit RNAT und RNAT IP verknüpft sind.

Statistik	Beschreibung
Empfangene Byte	Während RNAT-Sitzungen empfangene Byte
Gesendete Bytes	Während RNAT-Sitzungen gesendete Byte
Empfangene Pakete	Während RNAT-Sitzungen empfangene Pakete
Gesendete Pakete	Während RNAT-Sitzungen gesendete Pakete
Syn wurde gesendet	Verbindungsanfragen, die während RNAT-Sitzungen gesendet wurden
Aktuelle Sitzungen	Derzeit aktive RNAT-Sitzungen

Um RNAT-Statistiken mit der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **stat rnat**

Beispiel:

```
> stat rnat

RNAT summary
                                Rate (/s)            Total
Bytes Received                    0                    0
Bytes Sent                        0                    0
Packets Received                  0                    0
Packets Sent                      0                    0
Syn Sent                          0                    0
Current RNAT sessions            --                    0
 Done
>
<!--NeedCopy-->
```

Um RNAT mithilfe der GUI zu überwachen:

Navigieren Sie zu System**>**Netzwerk**>**NATs**, klicken Sie auf die Registerkarte**RNAT**und dann auf Statistiken.**

RNAT6 konfigurieren

RNAT-Regeln (Reverse Network Address Translation) für IPv6-Pakete werden als RNAT6 bezeichnet. Wenn ein von einem Server generiertes IPv6-Paket die in der RNAT6-Regel angegebenen Bedingungen erfüllt, ersetzt die Appliance die Quell-IPv6-Adresse des IPv6-Pakets durch eine konfigurierte NAT-IPv6-Adresse, bevor sie es an das Ziel weiterleitet. Die NAT-IPv6-Adresse ist eine der NetScaler-eigenen SNIP6- oder VIP6-Adressen.

Bei der Konfiguration einer RNAT6-Regel können Sie entweder ein IPv6-Präfix oder eine ACL6 als Bedingung angeben:

- **Verwenden einer IPv6-Netzwerkadresse**. Wenn Sie ein IPv6-Präfix verwenden, führt die Appliance die RNAT-Verarbeitung für die IPv6-Pakete durch, deren IPv6-Adresse mit dem Präfix übereinstimmt.
- **Verwendung von ACL6s**. Wenn Sie eine ACL6 verwenden, führt die Appliance eine RNAT-Verarbeitung für die IPv6-Pakete durch, die den in der ACL6 angegebenen Bedingungen entsprechen.

Sie haben eine der folgenden Optionen, um die NAT-IP-Adresse festzulegen:

- Geben Sie einen Satz von NetScaler-eigenen SNIP6- und VIP6-Adressen für eine RNAT6-Regel an. Die NetScaler-Appliance verwendet eine der IPv6-Adressen aus diesem Satz als NAT-IP-Adresse für jede Sitzung. Die Auswahl basiert auf dem Round-Robin-Algorithmus und erfolgt für jede Sitzung.
- Geben Sie keine NetScaler-eigene SNIP6- oder VIP6-Adresse für eine RNAT6-Regel an. Die NetScaler-Appliance verwendet eine beliebige der NetScaler-eigenen SNIP6- oder VIP6-Adressen als NAT-IP-Adresse. Die Auswahl basiert auf dem Next-Hop-Netzwerk, für das ein IPv6-Paket bestimmt ist, das der RNAT-Regel entspricht.

CLI-Verfahren

Um eine RNAT6-Regel mit der CLI zu erstellen:

Geben Sie an der Eingabeaufforderung Folgendes ein, um die Regel zu erstellen und die Konfiguration zu überprüfen:

- **add rnat6** <name> (<network> | (<acl6name> [-**redirectPort** \<port>]))
- **bind rnat6** <name> <natIP6>@ …
- **show rnat6**

So ändern oder entfernen Sie eine RNAT6-Regel mithilfe der CLI:

- Um eine RNAT6-Regel zu ändern, deren Bedingung ACL6 ist, geben Sie den Befehl **set rnat6** <name> ein, gefolgt von einem neuen Wert für den Parameter **redirectPort**.
- Um eine RNAT6-Regel zu entfernen, geben Sie den Befehl **clear rnat6** <name> ein.

GUI-Verfahren

So konfigurieren Sie eine RNAT6-Regel mithilfe der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **NATs**, klicken Sie auf die Registerkarte **RNAT6** und fügen Sie eine neue RNAT6-Regel hinzu oder bearbeiten Sie eine bestehende Regel.

RNAT6 überwachen

Sie können Statistiken zur RNAT6-Funktion anzeigen, um die Leistung zu überwachen oder Probleme im Zusammenhang mit der RNAT6-Funktion zu beheben. Sie können eine Zusammenfassung der Statistiken der RNAT6-Regeln oder einer bestimmten RNAT6-Regel anzeigen. Die statistischen Zähler geben Ereignisse seit dem letzten Neustart der NetScaler-Appliance wieder. Alle diese Zähler werden auf 0 zurückgesetzt, wenn die NetScaler-Appliance neu gestartet wird.

Im Folgenden sind einige der Statistikzähler aufgeführt, die mit der RNAT6-Funktion verknüpft sind:

- **Empfangene Byte** — Gesamtzahl der während RNAT6-Sitzungen empfangenen Byte.
- **Gesendete Byte** — Gesamtzahl der während RNAT6-Sitzungen gesendeten Byte.
- **Empfangene Pakete** — Gesamtzahl der während RNAT6-Sitzungen empfangenen Pakete.
- **Gesendete Pakete** — Gesamtzahl der Pakete, die während RNAT6-Sitzungen gesendet wurden.
- **Syn sent** — Gesamtzahl der Verbindungsanfragen, die während RNAT6-Sitzungen gesendet wurden
- **Aktuelle Sitzungen** - Derzeit aktive RNAT6-Sitzungen

Um mit der CLI eine zusammengefasste Statistik aller RNAT6-Regeln anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **stat rnat6**

Um Statistiken für eine angegebene RNAT6-Regel mithilfe der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **stat rnat6** [\<rnat6 rule name>]

So zeigen Sie RNAT6-Statistiken mit der GUI an:

Navigieren Sie zu **System** > **Netzwerk** > **NATs**, klicken Sie auf die Registerkarte **RNAT6** und dann auf **Statistiken.**

```
1 > stat rnat6
2
3 RNAT6 summary
4
5                            Rate (/s)               Total
6
```



```
Bytes Received              178                20644

Bytes Sent                  178                20644

Packets Received             5                  401

Packets Sent                 5                  401

Syn Sent                     0                    2

Current RNAT6 sessions      --                    1

Done

<!--NeedCopy-->
```

Startzeit und Gründe für Verbindungsabbruch in RNAT-Logeinträgen protokollieren

Zur Diagnose oder Behebung von Problemen im Zusammenhang mit RNAT protokolliert die NetScaler-Appliance RNAT-Sitzungen, wenn sie geschlossen werden.

Eine Protokollnachricht für eine RNAT-Sitzung besteht aus den folgenden Informationen:

- NetScaler-eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel der Protokollerstellung
- Protokoll der RNAT-Sitzung
- Quell-IP-Adresse
- RNAT-IP-Adresse
- Ziel-IP-Adresse
- Startzeit der RNAT-Sitzung
- Schließzeit der RNAT-Sitzung
- Gesamtzahl der von der NetScaler-Appliance für diese RNAT-Sitzung gesendeten Byte
- Gesamtzahl der von der NetScaler-Appliance für diese RNAT-Sitzung empfangenen Byte
- Grund für den Abschluss der RNAT-Sitzung. Die NetScaler-Appliance protokolliert den Schließgrund für TCP-RNAT-Sitzungen, die den TCP-Proxy (TCP-Proxy deaktiviert) der Appliance nicht verwenden. Im Folgenden sind die Arten von Schließungsgründen aufgeführt, die für TCP-RNAT-Sitzungen protokolliert werden:
  - **TCP-FIN**. Die RNAT-Sitzung wurde geschlossen, weil eine TCP-FIN entweder vom Quell- oder Zielgerät gesendet wurde.
  - **TCP RST**. Die RNAT-Sitzung wurde aufgrund eines TCP-Resets geschlossen, der entweder vom Quell- oder Zielgerät gesendet wurde.

- **TIMEOUT**. Die RNAT-Sitzung hat ein Timeout überschritten.

Die folgende Tabelle zeigt einige Beispiele für Protokolleinträge für RNAT-Sitzungen.

Art des Eintrags	Beispiel für einen Logeintrag
Beispiel für einen Protokolleintrag für eine UDP-RNAT-Sitzung	Dec 1 15:28:12 10.102.53.114 12/01/2015:15:28:12 GMT 0-PPE-0 : default UDP NAT_OTHERCONN_DELINK 154 0 : Source 1.2.2.5:23431 - Destination 192.168.123.122:22 - NatIP 192.168.123.1:4045 - Destination 192.168.123.122:22 - Start Time 12/01/2015:15:26:58 GMT - Delink Time 12/01/2015:15:28:12 GMT - Total_bytes_send 2511 - Total_bytes_recv 3725
Beispiel für einen Protokolleintrag für eine TCP-RNAT-Sitzung. Der Protokolleintrag zeigt, dass die Sitzung aufgrund eines TCP-Resets geschlossen wurde	Dec 1 15:29:59 10.102.53.114 12/01/2015:15:27:59 GMT 0-PPE-0 : default TCP NAT_OTHERCONN_DELINK 152 0 : Source 1.2.2.5:33826 - Destination 192.168.123.122:22 - NatIP 192.168.123.1:2384 - Destination 192.168.123.122:22 - Start Time 12/01/2015:15:27:40 GMT - Delink Time 12/01/2015:15:27:59 GMT - Total_bytes_send 2147 - Total_bytes_recv 3257 - Closure Reason TCP RST
Beispiel für einen Protokolleintrag für eine TCP-RNAT-Sitzung. Der Protokolleintrag zeigt, dass die Sitzung abgelaufen ist	Dec 1 15:30:12 10.102.53.114 12/01/2015:15:30:12 GMT 0-PPE-0 : default TCP NAT_OTHERCONN_DELINK 155 0 : Source 1.2.2.5:64976 - Destination 192.168.123.115:22 - NatIP 192.168.123.1:19636 - Destination 192.168.123.115:22 - Start Time 12/01/2015:15:27:25 GMT - Delink Time 12/01/2015:15:30:12 GMT - Total_bytes_send 0 - Total_bytes_recv 0 - Closure Reason TIMEOUT

Stateful Connection Failover für RNAT

Das Verbindungsfailover verhindert eine Unterbrechung des Zugriffs auf Anwendungen, die in einer verteilten Umgebung bereitgestellt werden. Die NetScaler Appliance unterstützt jetzt Stateful Connection Failover für Verbindungen, die sich auf RNAT-Regeln in einem NetScaler High Availability (HA)

-Setup beziehen. In einem HA-Setup bezieht sich Verbindungs-Failover (oder Verbindungsspiegelung) auf den Prozess, bei dem eine bestehende TCP- oder UDP-Verbindung aktiv gehalten wird, wenn ein Failover auftritt.

Die primäre Appliance sendet Nachrichten an die sekundäre Appliance, um aktuelle Informationen über die RNAT-Verbindungen zu synchronisieren. Die sekundäre Appliance verwendet diese Verbindungsinformationen nur im Falle eines Failovers. Wenn ein Failover auftritt, verfügt die neue primäre NetScaler-Appliance über Informationen über die Verbindungen, die vor dem Failover hergestellt wurden, und stellt diese Verbindungen daher auch nach dem Failover weiter bereit. Aus Sicht des Kunden ist dieser Failover transparent. Während der Übergangszeit kann es auf dem Client und dem Server zu kurzen Unterbrechungen und erneuten Übertragungen kommen.

Verbindungs-Failover kann per RNAT-Regel aktiviert werden. Um das Verbindungs-Failover für eine RNAT-Regel zu aktivieren, aktivieren Sie den ConnFailover-Parameter (Connection Failover) dieser bestimmten RNAT-Regel, indem Sie entweder die CLI oder die GUI verwenden.

So aktivieren Sie den Verbindungs-Failover für eine RNAT-Regel mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- `set rnat <name> -connfailover (ENABLED | DISABLED)`
- `show rnat`

Um den Verbindungs-Failover für eine RNAT-Regel mithilfe der GUI zu aktivieren:

1. Navigieren Sie zu **System** > **Netzwerk** > **NATs**, und klicken Sie dann auf die Registerkarte **RNAT** .
2. Wählen Sie **Verbindungs-Failover** aus, während Sie eine neue RNAT-Regel hinzufügen oder eine vorhandene Regel bearbeiten.

Reservieren des Quellports für RNAT-Verbindungen zu Servern

Für eine Anforderung, die auf eine RNAT-Konfiguration trifft, bei der eine oder mehrere RNAT-IP-Adressen und “Proxy-Portparameter verwenden” deaktiviert sind, verwendet die NetScaler-Appliance eine der RNAT-IP-Adresse und den Quellport der RNAT-Anforderung für die Verbindung mit Servern. Vor dem 13.0 47.x-Build schlägt die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-Clients) zum Server fehl, wenn derselbe Quellport bereits in einigen anderen Verbindungen verwendet wurde.

- **Quellport kleiner als 1024**. Standardmäßig behält sich die NetScaler-Appliance die ersten 1024 Ports einer IP-Adresse im Besitz von NetScaler (einschließlich RNAT-IP-Adressen) vor. Vor dem 13.0 47.x-Build schlägt die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-Clients) zum Server fehl, wenn der Quellport der RNAT-Anforderung kleiner oder gleich 1024 ist. Mit dem 13.0 47.x-Build ist die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-

Clients) zum Server erfolgreich, selbst wenn der Quellport der RNAT-Anforderung kleiner oder gleich 1024 ist.

- **Quellport größer als 1024**. Vor dem 13.0 47.x-Build schlägt die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-Clients) zum Server fehl, wenn derselbe Quellport bereits in einigen anderen Verbindungen verwendet wurde. Mit 13.0 47.x Build können Sie im `Retain Source Port range` (`retainsourceportrange`) -Parameter im Rahmen einer RNAT-Konfiguration einen Bereich von RNAT-Client-Quellports angeben. Die NetScaler-Appliance behält diese RNAT-Client-Quellports an der RNAT-IP-Adresse vor, die nur für die RNAT-Verbindung zu Servern verwendet werden.

Entfernen von RNAT-Sitzungen

Sie können alle unerwünschten oder ineffizienten RNAT-Sitzungen aus der NetScaler-Appliance entfernen. Die Appliance gibt sofort die für diese Sitzungen zugewiesenen Ressourcen (wie den Port der NAT-IP-Adresse und den Speicher) frei, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance verwirft auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte RNAT-Sitzungen von der NetScaler-Appliance entfernen.

Um alle RNAT-Sitzungen mit der CLI zu löschen:

Geben Sie in der Befehlszeile Folgendes ein:

- **flush rnatsession**

Um selektive RNAT-Sitzungen mit der CLI zu löschen:

Geben Sie in der Befehlszeile Folgendes ein:

- **flush rnatsession** ((-**network** <ip_addr> -**netmask** <netmask>) | -**natIP** <ip_addr> | -**aclname** <string>)

Um alle oder ausgewählte RNAT-Sitzungen mit der GUI zu löschen:

1. Navigieren Sie zu **System** > **Netzwerk** > **NATs** und klicken Sie dann auf die Registerkarte **RNAT**.
2. Klicken Sie im Menü **Aktionen** auf **RNAT-Sitzungen leeren**, um alle oder nur ausgewählte RNAT-Sitzungen zu entfernen (z. B. um RNAT-Sitzungen mit einer bestimmten RNAT-IP zu entfernen oder die zu einer bestimmten Netzwerk- oder ACL-basierten RNAT-Regel gehören).

Beispielkonfigurationen:

```
1     Clear all RNAT sessions existing on a NetScaler appliance
2
3     > flush rnatsession
4
5     Done
```



```
6
7     Clear all RNAT sessions belonging to network based RNAT rules that
          has 203.0.113.0/24 network as the matching condition.
8
9     > flush rnatsession -network 203.0.113.0 -netmask 255.255.255.0
10
11    Done
12
13    Clear all RNAT sessions with RNAT IP 192.0.2.90.
14
15    > flush rnatsession -natIP 192.0.2.90
16
17    Done
18
19    Clear all RNAT sessions belonging to ACL based RNAT rules that has
          ACL-RNAT-1 as the matching condition.
20
21    > flush rnatsession -aclname ACL-RNAT-1
22
23    Done
24 <!--NeedCopy-->
```

Präfixbasierte IPv6-IPv4-Übersetzung konfigurieren

May 11, 2023

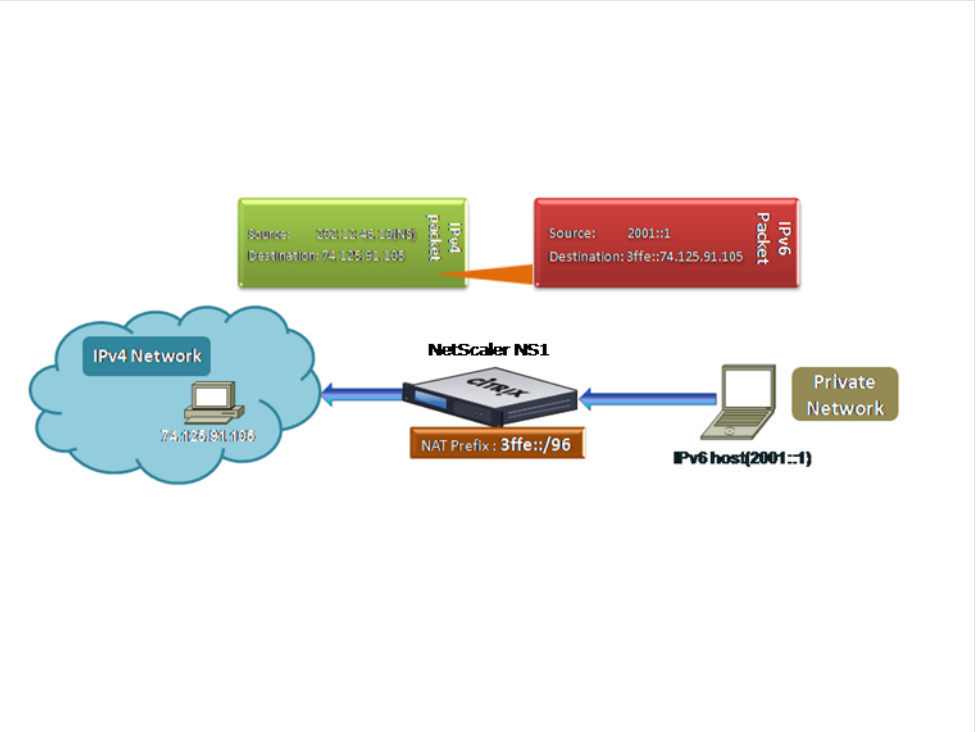
Bei der präfixbasierten Übersetzung werden Pakete, die von privaten IPv6-Servern gesendet werden, in IPv4-Pakete übersetzt, wobei ein in der NetScaler-Appliance konfiguriertes IPv6-Präfix verwendet wird. Dieses Präfix hat eine Länge von 96 Bit (128-32=96). Die IPv6-Server betten die Ziel-IP-Adresse der IPv4-Server oder -Hosts in die letzten 32 Bit des Ziel-IP-Adressfeldes der IPv6-Pakete ein. Die ersten 96 Bit des Ziel-IP-Adressfeldes werden als IPv6-NAT-Präfix festgelegt.

Die NetScaler-Appliance vergleicht die ersten 96 Bit der Ziel-IP-Adresse aller eingehenden IPv6-Pakete mit dem konfigurierten Präfix. Wenn eine Übereinstimmung vorliegt, generiert die NetScaler-Appliance ein IPv4-Paket und legt die Ziel-IP-Adresse als die letzten 32 Bit der Ziel-IP-Adresse des übereinstimmenden IPv6-Pakets fest. IPv6-Pakete, die an dieses Präfix adressiert sind, müssen an den NetScaler weitergeleitet werden, damit die IPv6-IPv4-Übersetzung vom NetScaler durchgeführt wird.

In der folgenden Abbildung ist 3ffe: :/96 als IPv6-NAT-Präfix auf NetScaler NS1 konfiguriert. Der IPv6-Host sendet ein IPv6-Paket mit der Ziel-IP-Adresse 3ffe::74.125.91.105. NS1 vergleicht die ersten 96

Bit der Ziel-IP-Adresse aller eingehenden IPv6-Pakete mit dem konfigurierten Präfix, und sie stimmen überein. NS1 generiert dann ein IPv4-Paket und legt die Ziel-IP-Adresse auf 74.125.91.105 fest.

Abbildung 1. IPv6-IPv4-Präfixbasierte Übersetzung



So konfigurieren Sie die präfixbasierte IPv6-IPv4-Übersetzung mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- set ipv6 [-natprefix \<ipv6_addr|*>]
- show ipv6

Beispiel:

```
> set ipv6 -natprefix 3ffe::/96
 Done
<!--NeedCopy-->
```

So konfigurieren Sie die präfixbasierte IPv6-IPv4-Übersetzung mithilfe der GUI:

Navigieren Sie zu System > Netzwerk, klicken Sie in der Gruppe Einstellungenauf INAT-Parameter konfigurieren, und legen Sie den Präfix-Parameter fest.

IP-Präfix NAT

May 11, 2023

Die NetScaler-Appliance unterstützt die Übersetzung eines Teils der Quell-IP-Adresse anstelle der vollständigen Adresse der auf der Appliance empfangenen Pakete. Das IP-Präfix NAT beinhaltet die Änderung eines oder mehrerer Oktette oder Bits der Quell-IP-Adresse.

Die NetScaler-Appliance unterstützt das IP-Präfix NAT für Lastausgleichskonfigurationen der folgenden Typen: ANY, UDP, DNS, TCP und HTTP.

Anwendungsfall: Zonifizierung von Clients für die Bereitstellung einer NetScaler-Appliance und eines Optimierungsgeräts

Das IP-Präfix NAT ist sehr nützlich in einer Bereitstellung, die eine NetScaler-Appliance und ein Optimierungsgerät (z. B. Citrix ByteMobile) umfasst. Bei dieser Art der Bereitstellung gibt es verschiedene geografisch verteilte Client-Netzwerke, die dieselbe Netzwerkadresse verwenden. Die NetScaler-Appliance muss den von jedem der Client-Netzwerke empfangenen Datenverkehr an das Optimierungsgerät senden, bevor sie an das Ziel weitergeleitet wird.

Das Gerät sendet den optimierten Datenverkehr zurück an die NetScaler-Appliance. Da die Optimierungsanforderungen für den Datenverkehr von jedem Client-Netzwerk unterschiedlich sind, muss das Optimierungsgerät das Client-Netzwerk jedes empfangenen Pakets erkennen. Die Lösung besteht darin, den Datenverkehr von jedem Client-Netzwerk mithilfe von VLANs in eine andere Zone zu trennen. Das IP-Präfix NAT mit einer anderen Einstellung wird für jede Zone konfiguriert. Die NetScaler-Appliance übersetzt das letzte Oktett der Quell-IP-Adresse jedes Pakets, und der übersetzte Oktettwert ist für jede Zone unterschiedlich.

Stellen Sie sich ein Beispiel für zwei Zonen, Z1 und Z2, vor, die sich die Netzwerkadresse 192.0.2.0/24 teilen. Auf der NetScaler-Appliance sind die IP-Präfix-NAT-Entitäten mit den Namen natrule-1 und natrule-2 für diese beiden Zonen konfiguriert. Bevor die Appliance ein Paket von Z1 weiterleitet, übersetzt natrule-1 das letzte Oktett der Quell-IP-Adresse des Pakets in 100. In ähnlicher Weise übersetzt natrule-2 für Pakete von Z2 das letzte Oktett der Quell-IP-Adresse in 200. Für zwei Clients, CL1-Z1 in Zone Z1 und CL1-Z2 in Zone Z2, jeweils mit der IP-Adresse 192.0.2.30, übersetzt die NetScaler-Appliance die Quell-IP-Adresse der Pakete von CL1-Z1 in 100.0.2.30 und der Pakete von CL1-Z2 in 200.0.2.30. Das Optimierungsgerät, an das die NetScaler-Appliance die übersetzten Pakete sendet, ist so konfiguriert, dass es die Quell-IP-Adresse eines Pakets verwendet, um die Zone zu erkennen, sodass es die entsprechende Optimierung anwendet, die für die Zone konfiguriert ist, aus der das Paket stammt.

Konfigurationsschritte

Die Konfiguration des IP-Präfix NAT besteht aus den folgenden Schritten:

- **Erstellen Sie ein Netzprofil und legen Sie den NAT-Regelparameter eines Netzprofils**fest. Eine NAT-Regel spezifiziert zwei IP-Adressen und eine Netzmaske. Die erste IP-Adresse

(angegeben durch den Parameter IP-Adresse) ist die Quell-IP-Adresse, die mit der zweiten (angegeben durch den Parameter IP Rewrite) übersetzt werden soll. Die Netzmaske gibt den Teil der Quell-IP-Adresse an, der mit demselben Teil der zweiten IP-Adresse übersetzt werden soll.

- **Binden Sie das Netzprofil an virtuelle Load-Balancing-Server oder -Dienste**. Ein Netzprofil mit NAT-Regeleinstellung kann an einen virtuellen Server oder Dienst vom Typ ANY, UDP, DNS, TCP und HTTP gebunden werden. Nachdem ein Netzprofil an einen virtuellen Server oder Dienst gebunden wurde, gleicht die NetScaler-Appliance die Quell-IP-Adresse der eingehenden Pakete, die sich auf den virtuellen Server oder Dienst beziehen, mit der NAT-Regeleinstellung ab. Der NetScaler führt dann IP-Präfix-NAT für Pakete durch, die der NAT-Regel entsprechen.

So konfigurieren Sie die IP-Präfix-NAT-Übersetzung mithilfe der Befehlszeile:

Geben Sie in der Befehlszeile Folgendes ein:

- **netProfile binden** <ip_addr><netmask><rewriteIp><name>(-** natRule**)
- **show netprofile** <name>

So konfigurieren Sie das IP-Präfix NAT mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile**.
2. Stellen Sie beim Hinzufügen oder Ändern von NetProfiles die folgenden Parameter unter NAT-Regeln ein.
    - IP-Adresse
    - Netzmaske
    - IP umschreiben

Beispiel-Konfiguration

In der folgenden Beispielkonfiguration hat das Netzprofil PARTIAL-NAT-1 NAT-Einstellungen mit dem IP-Präfix und ist an den virtuellen Lastausgleichsserver LBVS-1 gebunden, der vom Typ ANY ist. Für Pakete, die von 192.0.0.0/8 auf LBVS-1 empfangen wurden, übersetzt die NetScaler-Appliance das letzte Oktett der Quell-IP-Adresse des Pakets in 100. Ein Paket mit Quell-IP-Adresse 192.0.2.30, das auf LBVS-1 empfangen wurde, übersetzt die NetScaler Appliance die Quell-IP-Adresse in 100.0.2.30, bevor sie einen der gebundenen Server sendet.

```
> add netprofile PARTIAL-NAT-1
Done

> bind netprofile PARTIAL-NAT-1  - natrule 192.0.0.0 255.0.0.0 100.0.0.0
Done

> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1
```



```
Done
<!--NeedCopy-->
```

Statisches ARP

May 11, 2023

Sie können statische ARP-Einträge zur ARP-Tabelle hinzufügen und statische ARP-Einträge daraus entfernen. Nachdem Sie einen Eintrag hinzugefügt haben, sollten Sie die Konfiguration überprüfen. Wenn sich die IP-Adresse, der Port oder die MAC-Adresse ändern, nachdem Sie einen statischen ARP-Eintrag erstellt haben, müssen Sie den statischen Eintrag entfernen oder manuell anpassen. Daher wird das Erstellen statischer ARP-Einträge nicht empfohlen, sofern dies nicht erforderlich ist.

Um einen statischen ARP-Eintrag mit der CLI hinzuzufügen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add arp -IPAddress** <ip_addr> -**mac**<mac_addr> -**ifnum** <interface_name>
- **show arp** <IPAddress>

Beispiel:

```
> add arp -ip 10.102.29.6 -mac 00:24:e8:73:ca:ec -ifnum 1/1
 Done
<!--NeedCopy-->
```

Um einen statischen ARP-Eintrag mit der CLI zu entfernen:

Geben Sie in der Befehlszeile den Befehl **rm arp** und die IP-Adresse ein.

Um einen statischen ARP-Eintrag mithilfe der GUI hinzuzufügen:

Navigieren Sie zu **System** > **Netzwerk** > **ARP-Tabelle**und fügen Sie einen statischen ARP-Eintrag hinzu.

Geben Sie ein VLAN in einem statischen ARP-Eintrag an

In einem statischen ARP-Eintrag können Sie das VLAN angeben, über das das Zielgerät zugänglich ist. Diese Funktion ist nützlich, wenn die im statischen ARP-Eintrag angegebene Schnittstelle Teil mehrerer markierter VLANs ist und das Ziel über eines der VLANs zugänglich ist. Die NetScaler-Appliance enthält die angegebene VLAN-ID in den ausgehenden Paketen, die dem statischen ARP-Eintrag entspricht. Wenn Sie in einem ARP-Eintrag keine VLAN-ID angeben und die angegebene

Schnittstelle Teil mehrerer markierter VLANs ist, weist die Appliance dem ARP-Eintrag das native VLAN der Schnittstelle zu.

Angenommen, die NetScaler-Schnittstelle 1/2 ist Teil des nativen VLAN 2 und der markierten VLANs 3 und 4, und Sie fügen einen statischen ARP-Eintrag für Netzwerkgerät A hinzu, das Teil von VLAN 3 ist und über die Schnittstelle 1/2 zugänglich ist. Sie müssen VLAN 3 im ARP-Eintrag für Netzwerkgerät A angeben. Die NetScaler-Appliance nimmt dann das markierte VLAN 3 in alle Pakete auf, die für Netzwerkgerät A bestimmt sind, und sendet sie von der Schnittstelle 1/2.

Wenn Sie keine VLAN-ID angeben, weist die NetScaler-Appliance dem ARP-Eintrag systemeigenes VLAN 2 zu. Pakete, die für Gerät A bestimmt sind, werden im Netzwerkpfad verworfen, da sie kein markiertes VLAN 3 angeben, bei dem es sich um das VLAN für Gerät A handelt.

Um ein VLAN in einem statischen ARP-Eintrag mithilfe der CLI anzugeben:

Geben Sie in der Befehlszeile Folgendes ein:

- **add arp -IPAddress** <ip_addr> **-mac**<mac_addr> **-ifnum** <interface_name> [-**vlan** \<positive_integer>]
- **show arp** <IPAddress>

Beispiel:

```
> add arp -ip 198.51.100.91 -mac 36:db:4b:f6:12:15 -ifnum 1/2 -vlan 3
Done
<!--NeedCopy-->
```

Festlegen des Timeouts für dynamische ARP-Einträge

January 19, 2021

Sie können global eine Alterungszeit (Timeout-Wert) für dynamisch erlernte ARP-Einträge festlegen. Der neue Wert gilt nur für ARP-Einträge, die dynamisch gelernt werden, nachdem der neue Wert festgelegt wurde. Frühere ARP-Einträge laufen nach der zuvor konfigurierten Alterungszeit ab. Sie können einen ARP-Timeoutwert von 1 bis 1200 Sekunden angeben.

So legen Sie das Timeout für dynamische ARP-Einträge mit der Befehlszeilenschnittstelle fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set arpparam** -**timeout** <positive_integer>]
- **show arpparam**

Beispiel:


```
> set arpparam -timeout 500
 Done
<!--NeedCopy-->
```

So legen Sie das Timeout für dynamische ARP-Einträge mit der Befehlszeilenschnittstelle auf den Standardwert fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **unset arpparam**
- **show arpparam**

Beispiel:

```
> unset arpparam
 Done
<!--NeedCopy-->
```

So legen Sie das Timeout für dynamische ARP-Einträge mit der GUI fest:

Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen** auf **ARP Globale Parameter konfigurieren**, und legen Sie den Parameter **ARP Table Entry Timeout** fest.

Entdeckung des Nachbarn

May 11, 2023

Neighbor Discovery (ND) ist eines der wichtigsten Protokolle von IPv6. Es ist ein nachrichtenbasiertes Protokoll, das die Funktionen von Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) und Router Discovery kombiniert. ND ermöglicht es Knoten, ihre Link-Layer-Adressen bekannt zu geben und die MAC-Adressen oder Link-Layer-Adressen der benachbarten Knoten zu erhalten. Dieser Vorgang wird vom Neighbor Discovery Protocol (ND6) ausgeführt.

Neighbor Discovery kann die folgenden Funktionen ausführen:

- **Routererkennung**: Ermöglicht es einem Host, die lokalen Router auf einer angeschlossenen Verbindung zu erkennen und automatisch einen Standardrouter zu konfigurieren.
- **Präfixerkennung**: Ermöglicht es dem Host, die Netzwerkpräfixe für lokale Ziele zu ermitteln.

  Hinweis: Die NetScaler-Appliance unterstützt Prefix Discovery nicht.
- **Parametererkennung**: Ermöglicht es einem Host, zusätzliche Betriebsparameter wie MTU und das Standard-Hop-Limit für ausgehenden Datenverkehr zu ermitteln.

- **Automatische Adresskonfiguration**: Ermöglicht Hosts die automatische Konfiguration von IP-Adressen für Schnittstellen mit und ohne Stateful-Adreßkonfigurationsdienste wie DHCPv6. Der NetScaler unterstützt keine automatische Adresskonfiguration für globale IPv6-Adressen.
- **Adressauflösung: Entspricht**ARP in IPv4 und ermöglicht es einem Knoten, die IPv6-Adresse eines benachbarten Knotens in seine Link-Layer-Adresse aufzulösen.
- **Erkennung unerreichbarer Nachbarn**: Ermöglicht es einem Knoten, den Erreichbarkeitsstatus eines Nachbarn zu ermitteln.
- **Erkennung doppelter Adressen**: Ermöglicht es einem Knoten, festzustellen, ob eine NSIP-Adresse bereits von einem benachbarten Knoten verwendet wird.
- **Umleitung**: Entspricht der IPv4-ICMP-Umleitungsnachricht und ermöglicht es einem Router, den Host an eine bessere First-Hop-IPv6-Adresse umzuleiten, um ein Ziel zu erreichen.

Hinweis: Die NetScaler-Appliance unterstützt IPv6-Redirect nicht.

Konfigurationsschritte

Die Konfiguration von Neighbor Discovery umfasst die folgenden Aufgaben:

- IPv6-Nachbarn hinzufügen
- (Optional) IPv6-Nachbarn entfernen

CLI-Verfahren

IPv6-Nachbarn mithilfe der CLI hinzufügen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add nd6** <neighbor> <mac> <ifnum> [-**vlan** \<integer>]
- **sh nd6**

Beispiel:

```
> add nd6 2001::1 00:04:23:be:3c:06 1/1  -vlan 1
 Done

> show nd6
   Neighbor                MAC-Address(Vlan, Interface)       State
             TIME
   --------                ----------------------------       -----
            --------
1) ::1                     00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
        PERMANENT
2) fe80::2d0:68ff:fe0b:58da 00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
        PERMANENT
```



```
3) 2001::1                    00:04:23:be:3c:06(   1,   1/1)   REACHABLE
          STATIC
 Done
<!--NeedCopy-->
```

So entfernen Sie einen Nachbarermittlungseintrag mithilfe der Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

- **rm nd6** <Neighbor> -**vlan** <VLANID>

Beispiel:

```
 rm nd6 3ffe:100:100::1 -vlan 1
<!--NeedCopy-->
```

So entfernen Sie alle Nachbarermittlungseinträge mithilfe der Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

- **klar nd6**

GUI-Verfahren

IPv6-Nachbarn mithilfe der GUI hinzufügen:

Navigieren Sie zu **System** > **Netzwerk** > **IPv6-Nachbarn**und fügen Sie einen neuen IPv6-Nachbarn hinzu.

Neighbor Discovery-Eintrag mithilfe der GUI entfernen:

Navigieren Sie zu **System** > **Netzwerk** > **IPv6-Nachbarn**und löschen Sie den IPv6-Nachbarn.

Um alle Neighbor-Discovery-Einträge mit der GUI zu entfernen:

Navigieren Sie zu **System** > **Netzwerk** > **IPv6-Nachbarn**und klicken Sie auf **Löschen**.

IP-Tunnel

May 11, 2023

Ein IP-Tunnel ist ein Kommunikationskanal, der mithilfe von Kapselungstechnologien zwischen zwei Netzwerken, die keinen Routingpfad haben, erstellt werden kann. Jedes IP-Paket, das von den beiden Netzwerken gemeinsam genutzt wird, wird in ein anderes Paket gekapselt und dann über den Tunnel gesendet.

Die NetScaler Appliance implementiert IP-Tunneling auf folgende Weise:

- **NetScaler als Encapsulator (Load Balancing mit DSR-Modus)**: Stellen Sie sich eine Organisation vor, die über mehrere Rechenzentren in verschiedenen Ländern verfügt, wobei sich der NetScaler möglicherweise an einem Standort befindet und sich die Backend-Server in einem anderen Land befinden. Im Wesentlichen befinden sich der NetScaler und die Backend-Server in unterschiedlichen Netzwerken und sind über einen Router verbunden.

  Wenn Sie Direct Server Return (DSR) auf diesem NetScaler konfigurieren, wird das vom Quellsubnetz gesendete Paket vom NetScaler gekapselt und über einen Router und einen Tunnel an den entsprechenden Backend-Server gesendet. Der Backend-Server entkapselt das Paket und antwortet direkt an den Client, ohne dass das Paket über den NetScaler übertragen wird.

- **NetScaler als Entkapseler: Stellen Sie sich ein Unternehmen vor, das** über mehrere Rechenzentren verfügt, von denen jedes über NetScaler und Backend-Server verfügt. Wenn ein Paket von Rechenzentrum A an Rechenzentrum B gesendet wird, wird es normalerweise über einen Vermittler gesendet, beispielsweise einen Router oder einen anderen NetScaler. Der NetScaler verarbeitet das Paket und leitet es dann an den Backend-Server weiter. Wenn jedoch ein gekapseltes Paket gesendet wird, muss der NetScaler in der Lage sein, das Paket zu entkapseln, bevor es an die Backend-Server gesendet wird. Damit der NetScaler als Entkapseler fungieren kann, wird ein Tunnel zwischen dem Router und dem NetScaler hinzugefügt. Wenn das gekapselte Paket mit zusätzlichen Header-Informationen den NetScaler erreicht, wird das Datenpaket entkapselt, d. h. die zusätzlichen Header-Informationen werden entfernt, und das Paket wird dann an die entsprechenden Back-End-Server weitergeleitet.

  Der NetScaler kann auch als Entkapselung für die Load Balancing-Funktion verwendet werden, insbesondere in Szenarien, in denen die Anzahl der Verbindungen auf einem vServer einen Schwellenwert überschreitet und alle neuen Verbindungen dann an einen Backup-vserver umgeleitet werden.

Die IP-Tunnel-Funktion ist mit einer NetScaler Premium Edition-Lizenz verfügbar. Weitere Informationen zu NetScaler Editionslizenzen und der NetScaler-Funktionsmatrix finden Sie im Datenblatt zu NetScaler Editions.

IP-Tunnel konfigurieren

Die Konfiguration von IP-Tunneln auf einer NetScaler Appliance besteht aus der Erstellung von IP-Tunnelentitäten. Eine IP-Tunnelentität gibt die lokalen und externen Tunnelendpunkt-IP-Adressen sowie das für den IP-Tunnel zu verwendende Protokoll an.

Hinweis: Bei der Konfiguration eines IP-Tunnels in einem Cluster-Setup muss es sich bei der lokalen IP-Adresse um eine Striped SNIP-Adresse handeln.

CLI-Verfahren

So erstellen Sie einen IP-Tunnel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **iptunnel hinzufügen** <name><remote><remoteSubnetMask><local>-**Typ** -**Protokoll** (**ipoverip** | **GRE**)
- **show iptunnel**

So entfernen Sie einen IP-Tunnel mithilfe der CLI:

Um einen IP-Tunnel zu entfernen, geben Sie den Befehl **rm iptunnel** und den Namen des Tunnels ein.

So erstellen Sie einen IPv6-Tunnel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **ip6-Tunnel hinzufügen** <name><remoteIp><local>
- **ip6-Tunnel anzeigen**

So entfernen Sie einen IPv6-Tunnel mithilfe der CLI:

Um einen IPv6-Tunnel zu entfernen, geben Sie den Befehl **rm ip6tunnel** und den Namen des Tunnels ein.

GUI-Verfahren

So erstellen Sie einen IP-Tunnel mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IP-Tunnel**und fügen Sie einen neuen IP-Tunnel hinzu.

So erstellen Sie einen IPv6-Tunnel mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IP-Tunnel** > **IPv6-Tunnel**und fügen Sie einen neuen IPv6-Tunnel hinzu.

Weltweites Anpassen von IP-Tunneln

Durch die globale Angabe der Quell-IP-Adresse können Sie allen Tunneln eine gemeinsame Quell-IP-Adresse zuweisen. Da die Fragmentierung CPU-intensiv ist, können Sie außerdem global angeben, dass die NetScaler Appliance jedes Paket löscht, das fragmentiert werden muss. Wenn Sie alternativ alle Pakete fragmentieren möchten, solange ein CPU-Schwellenwert nicht erreicht wird, können Sie den CPU-Schwellenwert global angeben.

CLI-Verfahren

So passen Sie IP-Tunnel mithilfe der CLI global an:

Geben Sie in der Befehlszeile Folgendes ein:

- **set ipTunnelParam** -**srcIP** <sourceIPAddress> -**srcIPRoundRobin** (**YES** | **NO**)-**dropFrag** [**YES** | **NO**] -**dropFragCpuThreshold** <Positive integer>
- **show ipTunnelParam**

Beispiel:

```
> set iptunnelparam  - srcIP 12.12.12.22 -dropFrag Yes  -
   dropFragCpuThreshold 50
 Done

> set iptunnelparam -srcIPRoundRobin YES -dropFrag Yes  -
   dropFragCpuThreshold 50
 Done
<!--NeedCopy-->
```

So passen Sie IPv6-Tunnel mithilfe der CLI global an:

Geben Sie in der Befehlszeile Folgendes ein:

- **set ip6tunnelparam** -**srcIP** <IPv6Address> -**srcIPRoundRobin** (**YES** | NO)-**dropFrag** [**YES** | **NO**] -**dropFragCpuThreshold** <Positive integer>
- **show ip6tunnelparam**

GUI-Verfahren

So passen Sie IP-Tunnel mithilfe der GUI global an:

Navigieren Sie zu **System** > **Netzwerk** und klicken Sie in der Gruppe Einstellungen auf **Globale IPv4-Tunneleinstellungen**.

1. Navigieren Sie zu **System** > **Netzwerk** und klicken Sie in der Gruppe **Einstellungen** auf **Globale IPv6-Tunneleinstellungen**.
2. Stellen Sie im Dialogfeld **Globale IP-Tunnelparameter konfigurieren** die Parameter ein.

So passen Sie IPv6-Tunnel mithilfe der GUI global an:

1. Navigieren Sie zu **System** > **Netzwerk** und klicken Sie in der Gruppe **Einstellungen** auf **Globale IPv6-Tunneleinstellungen**.
2. Stellen Sie im Dialogfeld **Globale IP-Tunnelparameter konfigurieren** die Parameter ein.

GRE-Payload-Optionen in einem GRE-IP-Tunnel

Für einen konfigurierten GRE-IP-Tunnel kapselt die NetScaler Appliance das gesamte Layer-2-Paket, einschließlich des Ethernet-Headers und des VLAN-Headers (dot1q VLAN-Tag). IP-GRE-Tunnel

zwischen NetScaler-Appliances und einigen Geräten von Drittanbietern sind möglicherweise nicht stabil, da diese Geräte von Drittanbietern nicht für die Verarbeitung einiger Layer-2-Paketheader programmiert sind. Um einen stabilen IP-GRE-Tunnel zwischen einer NetScaler-Appliance und einem Drittanbietergerät zu konfigurieren, können Sie den GRE-Payload-Parameter des GRE-IP-Tunnel-Befehlssatzes verwenden. Die GRE-Payload-Einstellung kann auch auf einen GRE mit IPSec-Tunnel angewendet werden.

Sie können den GRE-Payload-Parameter so einstellen, dass er eine der folgenden Aktionen ausführt, bevor das Paket durch den GRE-Tunnel gesendet wird:

- **Ethernet mit DOT1Q**. Tragen Sie den Ethernet-Header sowie den VLAN-Header. Dies ist die Standardeinstellung. Für einen Tunnel, der an eine Netbridge gebunden ist, enthalten der innere Ethernet-Header und der VLAN-Header Informationen aus der ARP- und Bridge-Tabelle der NetScaler Appliance. Für einen Tunnel, der als nächster Hop zu einer PBR-Regel festgelegt ist, wird die innere Ethernet-Ziel-MAC-Adresse auf Null gesetzt und der VLAN-Header gibt das Standard-VLAN an. Das gekapselte (GRE) -Paket, das vom NetScaler-Tunnelendpunkt gesendet wird, hat das folgende Format:

Outer Ethernet Header	Outer IP Header	GRE Header	Inner Ethernet	Inner VLAN header	Inner IP/IPv6/ARP header	Inner TCP/UDP Header	Payload

- **Ethernet**. Tragen Sie den Ethernet-Header, aber lassen Sie den VLAN-Header fallen. Da die Pakete keine VLAN-Informationen im Tunnel enthalten, müssen Sie für einen Tunnel mit dieser Einstellung, der an eine Netbridge gebunden ist, ein entsprechendes VLAN an die Netbridge binden, damit der NetScaler beim Empfang von Paketen im Tunnel diese Pakete an das angegebene VLAN weiterleiten kann. Wenn der Tunnel als nächster Hop in einer PBR-Regel festgelegt ist, leitet der NetScaler die Pakete weiter, die im Tunnel empfangen werden. Das gekapselte (GRE) -Paket, das vom NetScaler-Tunnelendpunkt gesendet wird, hat das folgende Format:

Outer Ethernet header	Outer IP header	GRE Header	Inner Ethernet header	Inner IP/IPv6/ARP header	Inner TCP/UDP header	Payload

- **IP**. Löschen Sie den Ethernet-Header sowie den VLAN-Header. Da Tunnel mit dieser Einstellung keine Layer-2-Header enthalten, können diese Tunnel nicht an eine Netbridge gebunden werden, sondern können als nächster Hop in einer PBR-Regel festgelegt werden. Das Peer-Tunnel-Endgerät verbraucht das Paket beim Empfang entweder oder leitet es weiter. Das gekapselte (GRE) -Paket, das vom NetScaler-Tunnelendpunkt gesendet wird, hat das folgende Format:

Outer Ethernet header	Outer IP header	GRE header	Inner IP/IPv6 header	Inner TCP/UDP header	Payload

So löschen Sie Layer-2-Header von Paketen in einem GRE-IP-Tunnel mit der CLI:

- **add ipTunnel** <name> <remote> <remoteSubnetMask> <local> [-**protocol** \<GRE> [-**vlan** \<positive_integer>]] [-**grepayload** \<grepayload>] [-**ipsecProfileName** \<string>]
- **iptunnel anzeigen** <tunnelname>

Beispiel:

```
> add iptunnel IPTUNNEL-1 203.0.113.133 255.255.255.0 198.51.100.15 -
    protocol GRE  - grepayload Ethernet -ipsecProfileName IPTUNNEL-IPSEC
    -1
Done
<!--NeedCopy-->
```

IPv6-Verkehr durch GRE-IPV4-Tunnel

Die NetScaler Appliance unterstützt die Übertragung von IPv6-Verkehr über einen IPv4-GRE-Tunnel. Diese Funktion kann verwendet werden, um die Kommunikation zwischen isolierten IPv6-Netzwerken zu ermöglichen, ohne die IPv4-Infrastruktur zwischen ihnen zu aktualisieren.

Um diese Funktion zu konfigurieren, verknüpfen Sie eine PBR6-Regel mit dem konfigurierten IPv4-GRE-Tunnel, über den der NetScaler IPv6-Verkehr senden und empfangen soll. Die Quell-IPv6-Adresse und die IPv6-Zieladressenparameter der PBR6-Regel geben die IPv6-Netzwerke an, deren Verkehr den IPv4-GRE-Tunnel durchqueren soll.

Hinweis: Das IPSec-Protokoll wird in GRE-IPv4-Tunneln, die für die Übertragung von IPv6-Paketen konfiguriert sind, nicht unterstützt.

So erstellen Sie einen GRE-IPv4-Tunnel mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ipTunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol GRE**
- **show ipTunnel** <name>

So verknüpfen Sie eine PBR6-Regel mithilfe der CLI einem GRE-IPv4-Tunnel:

- **add ns pbr6** <pbrName> **ALLOW** -**srcIPv6** <network-range> -**dstIPv6** <network-range> -**ipTunnel** <tunnelName>
- **show pbr**

Beispiel-Konfiguration

In der folgenden Beispielkonfiguration wird der GRE-IP-Tunnel TUNNEL-V6onV4 mit der IP-Adresse 10.10.6.30 des Remote-Tunnelendpunkts und der IP-Adresse 10.10.5.30 des lokalen Tunnelendpunkts erstellt. Der Tunnel ist dann an pbr6 PBR6-V6onV4 gebunden. Der srciPv6 spezifiziert das

IPv6-Netzwerk, das mit dem lokalen Endpunkt verbunden ist, und DestipV6 spezifiziert das IPv6-Netzwerk, das mit dem Remote-Endpunkt verbunden ist. Der Datenverkehr dieser IPv6-Netzwerke darf den GRE-IPv4-Tunnel passieren.

```
> add ipTunnel TUNNEL-V6onV4 10.10.6.30 255.255.255.255 10.10.5.30 -
   protocol GRE
-ipsecProfileName None
Done
> add ns pbr6 PBR6-V6onV4 ALLOW -srcIPv6 = 2001:0db8:1::1-2001:0db8
   :1::255 -destIPv6 =
1-2001:0db8:4::255 -ipTunnel TUNNEL-V6onV4
<!--NeedCopy-->
```

Senden Sie den Antwortverkehr über einen IP-IP-Tunnel

Sie können eine NetScaler Appliance so konfigurieren, dass Antwortverkehr über einen IP-IP-Tunnel gesendet wird, anstatt ihn zurück an die Quelle weiterzuleiten. Wenn die Appliance eine Anfrage von einem anderen NetScaler oder einem Drittanbietergerät über einen IP-IP-Tunnel empfängt, leitet sie standardmäßig den Antwortverkehr weiter, anstatt ihn durch den Tunnel zu senden. Sie können richtlinienbasierte Routen (PBRs) verwenden oder die MAC-basierte Weiterleitung (MBF) aktivieren, um die Antwort durch den Tunnel zu senden.

Geben Sie in einer PBR-Regel die Subnetze an beiden Endpunkten an, deren Verkehr den Tunnel durchqueren soll. Geben Sie auch den nächsten Hop als Tunnelnamen ein. Wenn der Antwortverkehr der PBR-Regel entspricht, sendet die NetScaler Appliance den Datenverkehr durch den Tunnel.

Alternativ können Sie MBF aktivieren, um diese Anforderung zu erfüllen, aber die Funktionalität ist auf den Datenverkehr beschränkt, für den die NetScaler Appliance Sitzungsinformationen speichert (z. B. Verkehr im Zusammenhang mit Loadbalancing oder RNAT-Konfigurationen). Die Appliance verwendet die Sitzungsinformationen, um den Antwortverkehr durch den Tunnel zu senden.

CLI-Verfahren

Um eine PBR-Regel zu erstellen und ihr den IP-IP-Tunnel mithilfe der CLI zuzuordnen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ns pbr** <pbr_name> **ALLOW** -**srcIP** = <local_subnet_range> -**destIP** = <remote_subnet_range> -**ipTunnel** <tunnel_name>
- **apply ns pbrs**
- **show ns pbr** <pbr_name>

So aktivieren Sie die MAC-basierte Weiterleitung mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **enable ns mode MBF**
- **show ns mode**

GUI-Verfahren

PBR-Regel erstellen und ihr den IP-IP-Tunnel mithilfe der GUI zuordnen:

1. Navigieren Sie zu **System** > **Netzwerk** > **PBRs**. Erstellen Sie auf der Registerkarte **PBRs** eine **PBR-Regel**.
2. Stellen Sie beim Erstellen des PBR den **Next Hop Type** auf **IP-Tunnel** und den **IP-Tunnelnamen** auf den konfigurierten IP-IP-Tunnelnamen ein.

So aktivieren Sie die MAC-basierte Weiterleitung mithilfe der GUI:

1. Navigieren Sie zu **System** > **Einstellungen**und klicken Sie unter **Modi und Funktionen**auf **Modi konfigurieren**.
2. Wählen Sie auf der Seite **Modi konfigurieren** die Option **MAC-basierte Weiterleitung** aus.

Beispielkonfiguration

Betrachten Sie ein Beispiel für einen IPIP-Tunnel, NS1-NS2-IPIP, der zwischen zwei NetScaler-Appliances NS1 und NS2 eingerichtet ist.

Standardmäßig leitet NS2 für jede Anfrage, die NS2 über den Tunnel empfängt, den Antwortverkehr an die Quelle weiter, anstatt ihn (an NS1) durch den Tunnel zu senden.

Sie können richtlinienbasierte Routen (PBRs) konfigurieren oder die MAC-basierte Weiterleitung (MBF) auf NS2 aktivieren, damit die Antwort durch den Tunnel gesendet werden kann.

In der folgenden Beispielkonfiguration auf NS2 ist NS1-NS2-IPIP ein IPIP-Tunnel und NS1-NS2-IPIP-PBR ist eine PBR-Regel. Für Anfragen (mit innerer Quell-IP-Adresse im Bereich 10.102.147.0-10.102.147.255 und innerer Ziel-IP-Adresse im Bereich 10.102.147.0-10.102.147.255), die von NS2 über den Tunnel empfangen werden, sendet NS2 die entsprechende Antwort durch den Tunnel (an NS1), anstatt sie an die Quelle weiterzuleiten. Die Funktionalität ist auf den Datenverkehr beschränkt, der der PBR-Regel entspricht.

```
1 > add iptunnel NS1-NS2-IPIP 192.0.2.99 255.255.255.255 203.0.113.99 -
     protocol IPIP
2
3 Done
4 > add pbr NS1-NS2-IPIP-PBR -srcIP 10.102.147.0-10.102.147.255 - destIP
     10.20.1.0-10.20.1.255 - ipTunnel NS1-NS2-IPIP
5
6 Done
7 > apply pbrs
```



```
8
9  Done
10 <!--NeedCopy-->
```

Alternativ kann MBF auf NS2 aktiviert werden. Die Funktionalität ist auf den Datenverkehr beschränkt, für den NS2 Sitzungsinformationen speichert (z. B. Datenverkehr im Zusammenhang mit Lastenausgleich oder RNAT Konfigurationen).

```
1 > enable ns mode MBF
2
3 Done
4 <!--NeedCopy-->
```

IPv4-Pakete der Klasse E

May 11, 2023

Standardmäßig verwirft die NetScaler-Appliance alle Pakete, wenn sie eine IPv4-Adresse der Klasse E in den Feldern Quell-IP oder Ziel-IP enthalten. Wenn Ihr Setup IPv4-Adressen der Klasse E verwendet, können Sie die NetScaler-Appliance so konfigurieren, dass sie IPv4-Pakete der Klasse E verarbeitet.

Voraussetzungen

Bevor Sie mit der Konfiguration einer NetScaler-Appliance für die Verarbeitung von IPv4-Paketen der Klasse E beginnen, beachten Sie die folgenden Punkte:

- NetScaler-Appliances unterstützen keine Konfiguration von NetScaler-eigenen IPv4-Adressen (z. B. SNIP und VIP) im Klasse-E-Bereich. NetScaler-Appliances unterstützen nur die Verarbeitung von IPv4-Paketen der Klasse E.
- Eine NetScaler-Appliance verwendet intern IPv4-Adressen der Klasse E für die IPv6-Funktion. Die NetScaler-Appliance unterstützt nicht, dass beide Funktionen (Verarbeitung von IPv4-Paketen der Klasse E und IPv6-Unterstützung) gleichzeitig funktionieren. Die NetScaler-Appliance schränkt ein, dass die IPv6-Funktion nicht aktiviert ist, wenn die Verarbeitung von IPv4-Paketen der Klasse E aktiviert ist, und umgekehrt.

Konfigurationsschritte

Die Konfiguration einer NetScaler-Appliance für die Verarbeitung von IPv4-Paketen der Klasse E besteht aus der Aufgabe, den Layer-3-Parameter der **IPv4-Adresse der Klasse E (**AllowClassIPv4**)**zu aktivieren.

CLI-Verfahren

So konfigurieren Sie die NetScaler-Appliance für die Verarbeitung von IPv4-Paketen der Klasse E mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set l3param**-allowClassEipv4**(AKTIVIERT | DEAKTIVIERT)****
- **l3param anzeigen**

Beispielkonfiguration:

```
> set l3param -allowClassEIPv4 ENABLED

Done

> sh l3param

    Network L3 related Configuration Parameters

    icmpgen_rate_threshold      : 100

    srcnat                      : ENABLED

    override_rnat               : DISABLED

    drop_df_flag                : DISABLED

    .

    .

    .

    IPv6DynamicRouting          : DISABLED

    allowClassEIPv4             : ENABLED

Done
<!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie die NetScaler-Appliance für die Verarbeitung von IPv4-Paketen der Klasse E mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk**und klicken Sie dann im Abschnitt **Einstellungen** auf **Layer-3-Parameter konfigurieren**.
2. Wählen Sie **IPv4-Class-E-Adressenclients** aus und klicken Sie auf **OK.**

Auf NetScaler-Appliance verfügbare freie Ports für eine neue Back-End-Verbindung überwachen

May 11, 2023

Für die Kommunikation mit den physischen Servern oder anderen Peer-Geräten verwendet die NetScaler-Appliance eine Citrix-eigene IP-Adresse als Quell-IP-Adresse. Die NetScaler-Appliance verwaltet einen Pool ihrer IP-Adressen und wählt dynamisch eine IP-Adresse aus, während sie sich mit einem Server verbindet. Abhängig vom Subnetz, in dem der physische Server abgelegt ist, entscheidet die Appliance, welche IP-Adresse verwendet werden soll. Dieser Adresspool wird zum Senden von Traffic- und Monitor-Sonden verwendet.

Sie können die Gesamtzahl der freien Ports anzeigen, die auf den NetScaler-eigenen IP-Adressen für eine neue Back-End-Verbindung verfügbar sind. Diese Informationen helfen Ihnen bei der Entscheidung, ob Sie mehr NetScaler-eigene IP-Adressen benötigen, wenn die verfügbaren freien Ports fast erschöpft sind.

Sie können die folgenden Informationen für die NetScaler-Appliance bereitstellen, um die Gesamtzahl der freien Ports zu berechnen, die für eine neue Back-End-Verbindung verfügbar sind:

- IP-Adresse im Besitz von Citrix (optional)
- Ziel-IP-Adresse
- Destination port
- TCP- oder Nicht-TCP-Protokoll

Wenn Sie alle Informationen mit Ausnahme der Angabe einer Citrix eigenen IP-Adresse angeben:

- Die NetScaler-Appliance führt eine Routensuche durch, um alle NetScaler-eigenen IP-Adressen zu finden, die eine Verbindung zur Ziel-IP-Adresse herstellen können. Die Appliance sucht dann die Gesamtzahl der freien Ports, die auf diesen NetScaler-eigenen IP-Adressen für die angegebene neue Back-End-Verbindung verfügbar sind, und zeigt sie an.

  > **Hinweis:**
  >
  > Die NetScaler-Appliance führt keinen ECMP-Suchpfad oder LLB-Suchpfad oder PBR-Suchpfad durch, um die NetScaler-eigenen IP-Adressen zu finden, die eine Verbindung zur Ziel-IP-Adresse herstellen können.

Wenn Sie alle Informationen angeben, einschließlich der Angabe einer Citrix eigenen IP-Adresse:

- Die NetScaler-Appliance zeigt die Anzahl der freien Ports an, die an der angegebenen IP-Adresse für die angegebene neue Back-End-Verbindung verfügbar sind.

Voraussetzungen

Bevor Sie die Gesamtzahl der freien Ports anzeigen, die für eine neue Back-End-Verbindung verfügbar sind, sollten Sie die folgenden Punkte beachten:

- Die NetScaler-Appliance führt keinen ECMP-Suchpfad oder LLB-Suchpfad oder PBR-Suchpfad durch, um die NetScaler-eigenen IP-Adressen zu finden, die eine Verbindung zur Ziel-IP-Adresse herstellen können.
- Die NetScaler-Appliance unterstützt nicht die Anzeige freier Ports, die für eine lokale Link-IP-Adresse verfügbar sind.

Schritte zum Anzeigen der Anzahl der freien Ports, die auf einer NetScaler-Appliance für eine neue Back-End-Verbindung verfügbar sind

So zeigen Sie die Gesamtzahl der freien Ports an, die auf einer NetScaler-Appliance für eine neue Back-End-Verbindung verfügbar sind:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **show portallocation** [-**srcIP** \<ip_addr|ipv6_addr>] -**destIP** <ip_addr|ipv6_addr> -**destPort** <port> -**protocol** <1 for TCP, 0 for non-TCP protocol>

Beispiel: Gesamtzahl der freien Ports, die auf einer eigenständigen NetScaler-Appliance verfügbarsind:

```
> show portallocation -destip 198.51.100.30 -destport 80 -protocol 1

        Freeports available : 64505
 Done


> show portallocation -srcip 192.0.2.30 -destip 198.51.100.30 -destport
    80 -protocol 1

        Freeports available for IPAddress 192.0.2.30 : 20505
 Done
<!--NeedCopy-->
```

Beispiel — Gesamtzahl der freien Ports, die in einem Cluster-Setup verfügbar sind:

In der folgenden Beispielausgabe wird die Gesamtzahl der freien Ports angezeigt, die auf jedem Knoten eines Cluster-Setups mit zwei Knoten verfügbar sind.


```
> show portallocation -destip 198.51.100.30 -destport 80 -protocol 1

    Node Id: 1
    Freeports available : 32321

    Node Id: 0
    Freeports available : 32184

Done
<!--NeedCopy-->
```

Überwachen Sie die Port-Nutzung auf einer NetScaler-Appliance für Back-End-Verbindungen mithilfe von SNMP

Sie können den SNMP-Alarm `PORT-ALLOC-EXCEED` verwenden, um die Portnutzung auf einer NetScaler-Appliance für Back-End-Verbindungen zu überwachen.

Der SNMP-Alarm `PORT-ALLOC-EXCEED` umfasst die Parameter `high-threshold` und `normal-threshold`, die die Gesamtzahl der zugewiesenen Ports der NetScaler-eigenen IP-Adressen als Prozentsätze angeben. Wenn der Parameter `high-threshold` beispielsweise auf 90 festgelegt ist, generiert und sendet die NetScaler-Appliance Trap-Nachrichten, wenn das folgende Ereignis eintritt:

- wenn der Prozentsatz der Portzuweisung 90 Prozent für eine der NetScaler-eigenen IP-Adressen für die Back-End-Verbindungen übersteigt

Die SNMP-Benachrichtigungen helfen Ihnen bei der Entscheidung, ob Sie mehr NetScaler-eigene IP-Adressen benötigen, wenn die verfügbaren freien Ports fast erschöpft sind.

So überwachen Sie die Portnutzung auf einer NetScaler-Appliance auf Back-End-Verbindungen mithilfe von SNMP

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set snmp alarm PORT-ALLOC-EXCEED** -**logging** (ENABLED | DISABLED) -**severity** <severity> -**state** (ENABLED | DISABLED) -**thresholdValue** <positive_integer> [-**normalValue** \<positive_integer>] -**time** <secs>
- **sh snmp alarm PORT-ALLOC-EXCEED**

Beispiel:

```
> set snmp alarm PORT-ALLOC-EXCEED -logging ENABLED  -severity Major -
    state ENABLED -thresholdValue 90 -time 1200
Done

> sh snmp alarm port-alloc-EXCEED
```



```
5
6  Alarm                    Alarm Threshold     Normal Threshold    Time
       State       Severity        Logging
7  -----                    ---------------     ----------------    ----
       --------    -------------   --------
8  1) PORT-ALLOC-EXCEED    80                  80                  7200
       ENABLED     Major           ENABLED
9  Done
10
11 <!--NeedCopy-->
```

Weitere Informationen zum Konfigurieren von SNMP-Alarmen und SNMP-Trap-Listenern finden Sie unter Konfigurieren des NetScaler zum Generieren von SNMP-Traps.

Schnittstellen

May 11, 2023

Bevor Sie mit der Konfiguration von Schnittstellen beginnen, entscheiden Sie, ob Ihre Konfiguration den MAC-basierten Weiterleitungsmodus verwenden kann, und aktivieren oder deaktivieren Sie diese Systemeinstellung entsprechend. Die Anzahl der Schnittstellen in Ihrer Konfiguration ist für die verschiedenen Modelle der NetScaler-Appliance unterschiedlich. Zusätzlich zur Konfiguration einzelner Schnittstellen können Sie Schnittstellen logisch gruppieren, indem Sie VLANs verwenden, um den Datenfluss innerhalb einer Reihe von Schnittstellen einzuschränken, und Sie können Links zu Kanälen zusammenfassen. In einem Hochverfügbarkeits-Setup können Sie bei Bedarf eine virtuelle MAC-Adresse konfigurieren. Wenn Sie den L2-Modus verwenden, möchten Sie möglicherweise die Alterung der Bridge-Tabelle ändern.

Wenn Ihre Konfiguration abgeschlossen ist, entscheiden Sie, ob Sie die Systemeinstellung für die MTU-Pfaderkennung aktivieren möchten. NetScaler-Appliances können mithilfe von VRRP im Active-Active-Modus bereitgestellt werden. Eine aktiv-aktive Bereitstellung verhindert nicht nur Ausfallzeiten, sondern nutzt auch effizient alle NetScaler-Appliances in der Bereitstellung. Mit dem Tool Network Visualizer können Sie die Netzwerkkonfiguration einer NetScaler Bereitstellung anzeigen und Schnittstellen, Kanäle, VLANs und Bridge-Gruppen konfigurieren.

Mac-basierte Weiterleitung konfigurieren

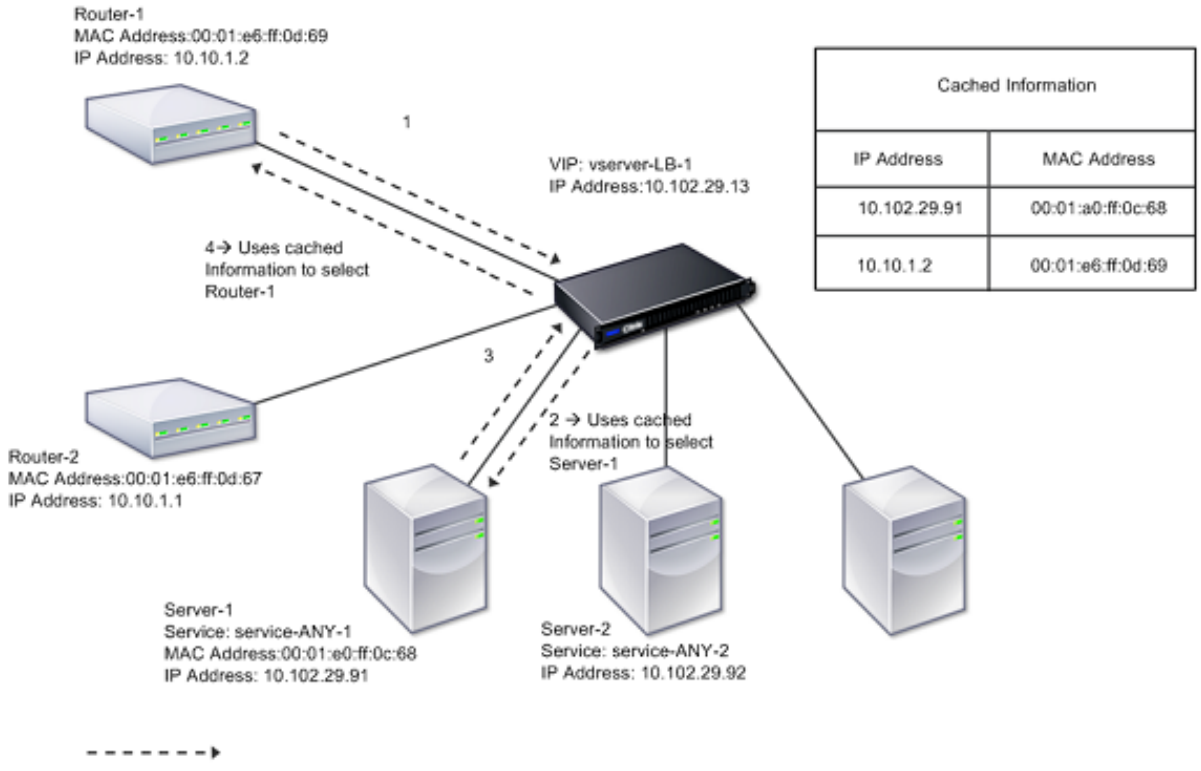
May 11, 2023

Wenn MAC-based Forwarding (MBF) aktiviert ist und eine Anforderung die NetScaler-Appliance erreicht, merkt sich die Appliance die Quell-MAC-Adresse des Frames und verwendet sie als Ziel-MAC-Adresse für die resultierenden Antworten. MAC-basierte Weiterleitung kann verwendet werden, um Suchvorgänge mit mehreren Routen/ARP und asymmetrische Paketflüsse zu vermeiden. Eine MAC-basierte Weiterleitung kann erforderlich sein, wenn der NetScaler mit mehreren statusbehafteten Geräten wie VPNs oder Firewalls verbunden ist, da dadurch sichergestellt wird, dass der Rückdatenverkehr an dasselbe Gerät gesendet wird, von dem der ursprüngliche Datenverkehr kam.

Die MAC-basierte Weiterleitung ist nützlich, wenn Sie VPN-Geräte verwenden, da sie garantiert, dass der gesamte Datenverkehr, der über ein VPN fließt, über dasselbe VPN-Gerät zurückgeleitet wird.

Das folgende Topologiediagramm veranschaulicht den Prozess der MAC-basierten Weiterleitung.

Abbildung 1. MAC-basierten Weiterleitungsmodus



Wenn MAC-basierte Weiterleitung (MBF) aktiviert ist, speichert der NetScaler die MAC-Adresse von:

- Die Quelle (ein übertragendes Gerät wie Router, Firewall oder VPN-Gerät) der eingehenden Verbindung.
- Der Server, der auf die Anfragen reagiert.

Wenn ein Server über die NetScaler-Appliance antwortet, setzt die Appliance die Ziel-MAC-Adresse des Antwortpakets auf die zwischengespeicherte Adresse, um sicherzustellen, dass der Datenverkehr symmetrisch fließt, und leitet die Antwort dann an den Client weiter. Der Prozess umgeht die Routentabellensuche und die ARP-Suchfunktionen. Wenn der NetScaler jedoch eine Verbindung initiiert, verwen-

det er die Route- und ARP-Tabellen für die Suchfunktion. In einer direkten Serverrückgabekonfiguration müssen Sie die MAC-basierte Weiterleitung aktivieren.

Weitere Informationen zu Konfigurationen für Direct Server Return finden Sie unter Lastenausgleich.

Einige Bereitstellungstopologien erfordern möglicherweise eingehende und ausgehende Pfade, um durch verschiedene Router zu fließen. MAC-basiertes Forwarding würde dieses Topologiedesign zerstören.

MBF sollte in folgenden Situationen deaktiviert werden:

- **Wenn ein Server eine Netzwerkschnittstellenkarte (NIC) -Teaming-Verbindung verwendet, ohne LACP (802.1ad Link Aggregation) zu verwenden.** Um in dieser Situation die MAC-basierte Weiterleitung zu aktivieren, müssen Sie ein Layer-3-Gerät zwischen dem NetScaler und dem Server verwenden.
  Hinweis: MBF kann aktiviert werden, wenn der Server NIC-Teaming mit LACP verwendet, da die virtuelle Schnittstelle eine MAC-Adresse verwendet.
- **Wenn Firewall-Clustering verwendet wird**. Firewall-Clustering geht davon aus, dass ARP verwendet wird, um die MAC-Adresse für eingehenden Datenverkehr aufzulösen. Manchmal kann es sich bei der eingehenden MAC-Adresse um eine nicht geclusterte MAC-Adresse handeln und sollte nicht für die Verarbeitung eingehender Pakete verwendet werden.

Wenn MBF deaktiviert ist, verwendet die Appliance L2- oder L3-Konnektivität, um die Antworten von Servern an die Clients weiterzuleiten. Abhängig von der Routentabelle können die für ausgehende und eingehende Verbindungen verwendeten Router unterschiedlich sein. Bei umgekehrtem Verkehr (Antwort vom Server):

- Wenn sich Quelle und Ziel in unterschiedlichen IP-Subnetzen befinden, verwendet die Appliance die Routensuche, um das Ziel zu finden.
- Wenn sich die Quelle im selben Subnetz wie das Ziel befindet, sucht der NetScaler in der ARP-Tabelle nach der Netzwerkschnittstelle und leitet den Datenverkehr an diese weiter. Wenn die ARP-Tabelle nicht existiert, fordert der NetScaler die ARP-Einträge an.

So aktivieren oder deaktivieren Sie die MAC-basierte Weiterleitung mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **enable ns mode MBF**
- **disable ns mode MBF**

Gehen Sie wie folgt vor, um die MAC-basierte Weiterleitung mithilfe der GUI zu aktivieren oder zu deaktivieren:

1. Navigieren Sie zu **System** > **Einstellungen**und klicken Sie in der Gruppe **Modi und Funktionen** auf **Modi konfigurieren**.
2. Wählen oder deaktivieren Sie die Option **MAC-basierte Weiterleitung** .

MAC-basierte Weiterleitung für ein Load-Balancing-Setup

Bei einigen Load-Balancing-Setups ist es erforderlich, dass die NetScaler-Appliance den globalen MBF (falls aktiviert) für diese Setups umgeht und stattdessen die Route/ARP-Lookups verwendet, um Pakete an das Ziel zu senden.

Der MBF-Parameter eines Netzprofils wird verwendet, um MBF für eine bestimmte Load-Balancing-Konfiguration zu aktivieren oder zu deaktivieren. MBF kann sowohl für die Clientseite als auch für die Serverseite einer Load-Balancing-Konfiguration festgelegt werden, indem Netzprofile (MBF aktiviert oder deaktiviert) an den virtuellen Server und die Dienste gebunden werden.

Wenn beispielsweise ein Netzprofil mit deaktiviertem MBF an den virtuellen Server einer Load-Balancing-Konfiguration gebunden ist, umgeht die NetScaler-Appliance den globalen MBF (falls aktiviert) und verwendet stattdessen die Route/ARP-Lookups zum Senden von Antwortpaketen an Clients.

Voraussetzungen

Bevor Sie mit der Konfiguration von MBF für eine Load-Balancing-Konfiguration beginnen, beachten Sie die folgenden Punkte:

- In einer Load-Balancing-Konfiguration können die Clientseite (virtueller Server) und die Serverseite (Service/Servicegruppen) unterschiedliche MBF-Einstellungen haben.
- Eine Load-Balancing-Konfiguration erbt die globale MBF-Einstellung, wenn MBF nicht explizit in den an den virtuellen Server und die Dienste gebundenen Netzprofilen festgelegt ist.
- In einer Lastausgleichskonfiguration erbt die Serverseite (Dienst) die clientseitige MBF-Einstellung des an den virtuellen Server gebundenen Netzprofils, wenn kein Netzprofil an den Dienst gebunden ist.
- In einer Load-Balancing-Konfiguration mit Direct Server Return Serverrückgabemodus erbt die Clientseite die MBF-Einstellung im an den Dienst gebundenen Netzprofil.
- In einer Content Switching-Konfiguration übernimmt die Clientseite die MBF-Einstellung im Netzprofil, das an den virtuellen Content Switching-Server gebunden ist, anstatt vom virtuellen Ziel-Ladausgleichsserver.

Einschränkungen

Bevor Sie mit der Konfiguration von MBF für eine Load-Balancing-Konfiguration beginnen, beachten Sie die folgenden Einschränkungen:

- Die MBF-Einstellung für Load-Balancing-Konfigurationen wird in einem Cluster-Setup nicht unterstützt.

- Bei einem virtuellen Lastausgleichsserver mit MAC-Modus oder L2Conn-Einstellungen ist MBF unabhängig von der MBF-Einstellung im an den virtuellen Server gebundenen Netzprofil aktiviert.
- Die NetScaler-Appliance unterstützt die Einstellung von MBF für Load Balancing-Monitore mithilfe des Netzprofils nicht. Mit anderen Worten, die MBF-Einstellung eines Netzprofils wird nicht auf die Monitore angewendet, an die das Netzprofil gebunden ist. Die globale MBF-Einstellung wird unabhängig von der MBF-Einstellung des gebundenen Netzprofils auf Monitore angewendet.

MBF für die Load-Balancing-Konfiguration konfigurieren

Die Konfiguration von MBF für eine Load-Balancing-Konfiguration umfasst die folgenden Aufgaben:

- Aktivieren Sie den MBF-Parameter in einem Netzprofil.
- Binden Sie das Netzprofil an einen virtuellen Lastausgleichsserver oder an virtuelle Dienste.

So aktivieren Sie MBF in einem Netzprofil mithilfe der CLI:

- Um MBF beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie in der Befehlszeile Folgendes ein:
  - **add netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)
  - **show netprofile** <name>
- Um MBF in einem vorhandenen Netzprofil zu aktivieren, geben Sie an der Befehlszeile Folgendes ein:
  - **set netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)
  - **show netprofile** <name>

So aktivieren Sie MBF in einem Netzprofil mithilfe der GUI**

1. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile**.
2. Aktivieren Sie den **MBF-Parameter**, während Sie ein Netzprofil hinzufügen oder ändern.

In der folgenden Beispielkonfiguration ist MBF für das Netzprofil NETPROFILE-MBF-LBVS aktiviert und an den virtuellen Lastausgleichsserver LBVS-1 gebunden. Außerdem hat Netprofil NETPROFILE-MBF-SVC MBF aktiviert und ist an einen Lastausgleichsdienst SVC-1 gebunden.

```
> add netprofile NETPROFILE-MBF-LBVS -MBF ENABLED

Done

> add netprofile NETPROFILE-MBF-SVC -MBF ENABLED

Done

> set lb vserver LBVS-1 -netprofile NETPROFILE-MBF-LBVS
```



```
10
11 Done
12
13 > set service SVC-1 -netprofile NETPROFILE-MBF-SVC
14
15 Done
16
17 <!--NeedCopy-->
```

Netzwerkschnittstellen konfigurieren

May 11, 2023

Netzwerkschnittstellen in der NetScaler-Appliance sind in <slot><port> der Schreibweise nummeriert. Nachdem Sie Ihre Schnittstellen konfiguriert haben, zeigen Sie die Schnittstellen und ihre Einstellungen an, um die Konfiguration zu überprüfen. Sie können diese Informationen auch anzeigen, um ein Problem in der Konfiguration zu beheben.

Um die Netzwerkschnittstellen zu verwalten, können Sie Folgendes tun:

- Aktivieren Sie einige Schnittstellen und deaktivieren Sie andere.
- Setze eine Schnittstelle zurück, um ihre Einstellungen neu auszuhandeln.
- Löscht die gesammelten Statistiken für eine Schnittstelle.

Um die Konfiguration zu überprüfen, können Sie die Schnittstelleneinstellungen anzeigen. Sie können die Statistiken für eine Schnittstelle anzeigen, um deren Zustand zu bewerten.

Stellen Sie die Netzwerkschnittstellenparameter ein

Die Netzwerkschnittstellenkonfiguration wird weder synchronisiert noch weitergegeben. Bei einem HA-Paar müssen Sie die Konfiguration auf jeder Einheit unabhängig durchführen.

So legen Sie die Netzwerkschnittstellenparameter mit der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

```
1 -  set interface <id> [-speed <speed>] [-duplex <duplex>] [-flowControl
      <flowControl>] [-autoneg ( DISABLED | ENABLED )] [-haMonitor ( ON |
      OFF )] [ ( ON | OFF )] [-tagall ( ON | OFF )] [-lacpMode <lacpMode
     >] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>]
     [-lacpTimeout (LONG | SHORT )] [-ifAlias <string>] [-throughput <
     positive_integer>][-bandwidthHigh <positive_integer> [-
     bandwidthNormal <positive_integer>]]
```



```
-  show interface [<id>]
<!--NeedCopy-->
```

Beispiel:

```
> set interface 1/8 -duplex full
 Done
<!--NeedCopy-->
```

So stellen Sie die Netzwerkschnittstellenparameter mithilfe der GUI ein:

Navigieren Sie zu **System > Netzwerk > Schnittstellen**, wählen Sie die Netzwerkschnittstelle aus, die Sie ändern möchten (z. B. 1/8), klicken Sie auf **Bearbeiten**und legen Sie dann die Parameter fest.

Einstellung der Empfangsringgröße und des Ringtyps für eine Schnittstelle

Sie können die Empfangsringgröße und den Ringtyp für IX-, F1X-, F2X- oder F4X-Schnittstellen auf NetScaler MPX- und SDX-Plattformen erhöhen.

Eine größere Ringgröße bietet mehr Dämpfung, um mit hohem Traffic fertig zu werden, kann jedoch die Leistung beeinträchtigen. Eine Ringgröße von bis zu 8192 wird für IX-Schnittstellen unterstützt. Eine Ringgröße von bis zu 4096 wird für F1X-, F2X- und F4X-Schnittstellen unterstützt. Die Standard-Ringgröße bleibt 2048.

Die Ringtypen von Schnittstellen sind standardmäßig elastisch. Ihre Größe nimmt je nach Paketeintrittsrate zu oder ab. Sie können den Ringtyp als „fest“ konfigurieren. In diesem Fall ändert sich die Ringgröße nicht je nach Verkehrsrate.

Hinweis: Diese Funktion wird ab Version 13.0 Build 41.x unterstützt und auf Plattformen unterstützt, die über IX-, F1X-, F2X- oder F4X-Schnittstellen verfügen.

Verwenden Sie den `show hardware` Befehl, um festzustellen, ob Ihre Appliance über IX-, F1X-, F2X- oder F4X-Schnittstellen verfügt.

Beispiele:

Das folgende Modell verfügt über 16 F1X (10G) -Schnittstellen und 4 F4X-Schnittstellen (40G).

```
> sh hardware
        Platform: NSMPX-25000-40G 20\*CPU+16\*F1X+4\*F4X+2\*E1K+2*CVM
           N3 250040
        Manufactured on: 12/16/2016
        CPU: 2800MHZ
        Host Id: 234913926
        Serial no: N43RJCRV3X
        Encoded serial no: N43RJCRV3X
        Netscaler UUID: 336a32d6-2cfa-11e8-bf01-00e0ed5dd23c
```



```
9          BMC Revision: 4.08
10  Done
11 <!--NeedCopy-->
```

Das folgende Modell hat 2 1X (10G) Schnittstellen.

```
1  > sh hardware
2          Platform: NSMPX-10500 8\*CPU+2\*E1K+8\*E1K+2\*IX+8*CVM 1620
               760100
3          Manufactured on: 12/27/2010
4          CPU: 2832MHZ
5          Host Id: 1707114630
6          Serial no: 7VZZV1ZXJ4
7          Encoded serial no: 7VZZV1ZXJ4
8          Netscaler UUID: eb1bfd72-5176-11e7-ba18-00e0ed1b0d12
9   Done
10 <!--NeedCopy-->
```

Um Ringgröße und Ringtyp mithilfe der CLI zu konfigurieren, geben Sie
in der Befehlszeile Folgendes ein:

```
1  set interface <id> -ringsize <positive_integer> -ringtype ( Elastic |
       Fixed )
2  <!--NeedCopy-->
```

Parameter:

`ringsize`:

Die Empfangsringgröße der Schnittstelle. Eine höhere Zahl bietet mehr Puffer für den eingehenden Verkehr.

Standardwert: 2048
Mindestwert: 512
Maximalwert: 16384

`ringtype`:

Der Empfangsklingeltyp der Schnittstelle. Ein fester Ringtyp weist die konfigurierte Anzahl von Puffern unabhängig von der Verkehrsrate vorab zu. Im Gegensatz dazu dehnt sich ein elastischer Ring je nach eingehendem Verkehr aus und schrumpft.

Mögliche Werte: Elastic, Fixed

Standardwert: Elastic

Beispiel:


```
> set interface 40/2 -ringsize 4096 -ringtype Fixed
 Done
> show interface 40/2

1)      Interface 40/2 (40G Ethernet, CR4, 40 Gbit) #21  flags=0xc020 <
    ENABLED, UP, UP, autoneg, HAMON, HEARTBEAT, 802.1q> MTU=1500, native
     vlan=10, MAC=00:e0:ed:75:14:2a, uptime 119h26m32s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
           throughput 0
        Actual: media UTP, speed 40000, duplex FULL, fctl OFF,
           throughput 40000
        LLDP Mode: NONE, LR Priority: 1024
        RX: Pkts(1443972660032) Bytes(1457207315336105) Errs(0) Drops
           (53319) Stalls(0)
        TX: Pkts(1452311431262) Bytes(1458534011197761) Errs(0) Drops
           (788) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
        Rx Ring: Configured size=4096, Actual size=4096, Type: Fixed
 Done
<!--NeedCopy-->
```

Die letzte Zeile zeigt die konfigurierte und tatsächliche Ringgröße sowie den Ringtyp.

So konfigurieren Sie Ringgröße und Ringtyp mithilfe der GUI:

1. Navigieren Sie zu **System > Netzwerk > Schnittstellen**.
2. Wählen Sie Ihre Oberfläche aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie im **Feld Ringgröße**eine der folgenden Optionen an:
   - **IX-Schnittstellen:** 512, 1024, 2048, 4096 oder 8192.
   - **F1X-, F2X- oder F4X-Schnittstellen:** 512, 1024, 2048 oder 4096.
4. Wählen Sie unter **Ringtyp**die Option Elastisch oder Fest aus.
5. Klicken Sie auf **OK**.

Netzwerkschnittstellen aktivieren und deaktivieren

Standardmäßig sind die Netzwerkschnittstellen aktiviert. Deaktivieren Sie alle Netzwerkschnittstellen, die nicht mit dem Netzwerk verbunden sind, sodass sie keine Pakete senden oder empfangen kann. Das Deaktivieren einer Netzwerkschnittstelle, die in einem Hochverfügbarkeitssetup mit dem Netzwerk verbunden ist, kann zu einem Failover führen.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

So aktivieren oder deaktivieren Sie eine Netzwerkschnittstelle mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

```
- enable interface <interface_num>
- show interface <interface_num>
- disable interface <interface_num>
- show interface <interface_num>
<!--NeedCopy-->
```

Beispiel:

```
> enable interface 1/8
 Done
> show interface 1/8
        Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
        flags=0x4004000 <ENABLED, DOWN, BOUND to LA/1, down, autoneg,
           802.1q>
        MTU=1514, MAC=00:d0:68:15:fd:3d, downtime 906h58m40s
        Requested: media UTP, speed AUTO, duplex FULL, fctl OFF,
           throughput 0
        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
Done
<!--NeedCopy-->
```

Um eine Netzwerkschnittstelle mithilfe der GUI zu aktivieren oder zu deaktivieren:

1. Navigieren Sie zu **System > Netzwerk > Schnittstellen**.
2. Wählen Sie die Netzwerkschnittstelle aus und wählen Sie in der **Aktionsliste** die Option Aktivieren oder Deaktivieren aus.

Netzwerkschnittstellen zurücksetzen

Die Netzwerkschnittstelleneinstellungen steuern Eigenschaften wie Duplex und Geschwindigkeit. Um die Einstellungen einer Netzwerkschnittstelle neu auszuhandeln, müssen Sie sie zurücksetzen.

Um eine Netzwerkschnittstelle mit der CLI zurückzusetzen:

Geben Sie in der Befehlszeile Folgendes ein:

```
- reset interface <interface_num>
- show interface <interface_num>
```



```
<!--NeedCopy-->
```

Beispiel:

```
> reset interface 1/8
 Done
<!--NeedCopy-->
```

Um eine Netzwerkschnittstelle mithilfe der GUI zurückzusetzen:

1. Navigieren Sie zu **System > Netzwerk > Schnittstellen**.
2. Wählen Sie die Netzwerkschnittstelle aus und wählen Sie in der **Aktionsliste** die Option **Schnittstelle zurücksetzen**aus.

Überwachen Sie eine Netzwerkschnittstelle

Sie können Netzwerkschnittstellenstatistiken anzeigen, um Parameter zu überwachen, und anhand der Informationen den Zustand der Netzwerkschnittstelle überprüfen. Sie können Parameter wie gesendete und empfangene Pakete, Durchsatz, LACP-Dateneinheiten (Link Aggregate Control Protocol) und Fehler überwachen. Sie können die Statistiken einer Netzwerkschnittstelle löschen, um deren Statistiken ab dem Zeitpunkt des Löschens der Statistiken zu überwachen.

Gehen Sie wie folgt vor, um die Statistiken der Netzwerkschnittstellen mit der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

```
-  stat interface <interface_num>
<!--NeedCopy-->
```

Beispiel:

```
> stat interface 1/8
 Done
<!--NeedCopy-->
```

So löschen Sie die Statistiken einer Netzwerkschnittstelle mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

```
-  clear interface <interface_num>
<!--NeedCopy-->
```

Beispiel:

```
> clear interface 1/8
 Done
```



```
<!--NeedCopy-->
```

Um die Statistiken einer Schnittstelle mithilfe der GUI anzuzeigen:

Navigieren Sie zu **System > Netzwerk > Schnittstellen**, wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf **Schnittstellenstatistiken**.

Um die Statistiken einer Netzwerkschnittstelle mithilfe der GUI zu löschen:

1. Navigieren Sie zu **System > Netzwerk > Schnittstellen**.
2. Wählen Sie die Netzwerkschnittstelle aus und wählen Sie in der **Aktionsliste** die Option **Statistik löschen**aus.

Weiterleitungssitzungsregeln konfigurieren

May 11, 2023

Standardmäßig erstellt die NetScaler-Appliance keine Sitzungseinträge für den Datenverkehr, den sie nur weiterleitet (L3-Modus). Für den Fall, dass eine Client-Anfrage, die die Appliance an einen Server weiterleitet, zu einer Antwort führt, die über denselben Pfad zurückgegeben werden muss, können Sie eine Weiterleitungssitzungsregel erstellen. Eine Regel für Weiterleitungssitzungen erstellt Weiterleitungssitzungseinträge für Datenverkehr, der von einem bestimmten Netzwerk stammt oder für dieses bestimmt ist und vom NetScaler weitergeleitet wird. Sie können Weiterleitungssitzungsregeln für IPv4-Datenverkehr sowie IPv6-Datenverkehr erstellen.

Bei der Konfiguration einer Regel für IPv4-Weiterleitungssitzungen können Sie entweder eine IPv4-Netzwerkadresse oder eine erweiterte ACL als Bedingung für die Identifizierung des IPv4-Datenverkehrs angeben, für den ein Weiterleitungssitzungseintrag erstellt werden soll:

- **Netzwerkadresse**. Wenn Sie eine IPv4-Netzwerkadresse angeben, erstellt die Appliance Weiterleitungssitzungen für IPv4-Verkehr, dessen Quelle oder Ziel mit der Netzwerkadresse übereinstimmt.
- **Erweiterte ACL-Regel**. Wenn Sie eine erweiterte ACL-Regel angeben, erstellt die Appliance Weiterleitungssitzungen für IPv4-Verkehr, die den in der erweiterten ACL-Regel angegebenen Bedingungen entsprechen.

Bei der Konfiguration einer Regel für IPv6-Weiterleitungssitzungen können Sie entweder ein IPv6-Präfix oder eine ACL6 als Bedingung für die Identifizierung des IPv6-Datenverkehrs angeben, für den ein Weiterleitungssitzungseintrag erstellt werden soll:

- **IPv6-Präfix**. Wenn Sie ein IPv6-Präfix angeben, erstellt die Appliance Weiterleitungssitzungen für IPv6-Verkehr, dessen Quelle oder Ziel mit dem IPv6-Präfix übereinstimmt.
- **ACL6-Regel**. Wenn Sie eine ACL6-Regel angeben, erstellt die Appliance Weiterleitungssitzungen für IPv6-Verkehr, die den in der ACL6-Regel angegebenen Bedingungen entsprechen.

So erstellen Sie mit der CLI eine Regel für IPv4-Weiterleitungssitzungen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Weiterleitungssitzungsregel zu erstellen und die Konfiguration zu überprüfen:

- ForwardingSession hinzufügen <name>[\<network>\<netmask>] | [-aclname\<string>] -connfailover (AKTIVIERT | DEAKTIVIERT)
- show forwardingSession

Beispiel:

```
A network address as the condition:

> add forwardingSession fs-nw-1 10.102.105.51 255.255.255.255
 Done

An ACL as the condition:

> add forwardingSession fs-acl-1 acl1
 Done
<!--NeedCopy-->
```

So konfigurieren Sie eine Regel für eine IPv4-Weiterleitungssitzung mithilfe der GUI:

Navigieren Sie zu System > Netzwerk > Weiterleitungssitzungen, fügen Sie eine neue IPv4-Weiterleitungssitzung hinzu oder bearbeiten Sie eine bestehende Weiterleitungssitzung.

So erstellen Sie mit der CLI eine Regel für IPv6-Weiterleitungssitzungen:

- Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Weiterleitungssitzungsregel zu erstellen und die Konfiguration zu überprüfen:
  - <string>ForwardingSession hinzufügen <name>[\<IPv6 prefix>] | [-acl6name\]
  - show forwardingSession

  Beispiel:

```
    An IPv6 prefix as the condition:

    > add forwardingSession fsv6-pfx-1 3ffe::/64
     Done

    An ACL6 rule as the condition:

    > add forwardingSession fsv6-acl6-1  - acl6name ACL6-FS
     Done
<!--NeedCopy-->
```


Um eine Regel für eine IPv6-Weiterleitungssitzung mithilfe der GUI zu konfigurieren, gehen Sie wie folgt vor:

Navigieren Sie zu System > Netzwerk > Weiterleitungssitzungen, fügen Sie eine neue IPv6-Weiterleitungssitzung hinzu oder bearbeiten Sie eine bestehende Weiterleitungssitzung.

Einer bestehenden Regel für Weiterleitungssitzungen eine ACL-Regel zuweisen

Sie können einer auf Netzwerkadresse/IPv6-Präfix basierenden Weiterleitungssitzungsregel eine ACL-Regel zuweisen. In diesem Fall wird sie zu einer ACL-basierten Weiterleitungssitzungsregel. Sie können in einer ACL-basierten Weiterleitungssitzungsregel auch eine bestehende ACL-Regel in eine andere ACL-Regel ändern. Nachdem das Timeout für die vorhandenen zugehörigen Weiterleitungssitzungseinträge (falls vorhanden) überschritten wurde, verwenden die Regeln die neu zugewiesene ACL, um den IPv4-/IPv6-Verkehr zu identifizieren, für den ein Weiterleitungssitzungseintrag erstellt werden soll.

So weisen Sie einer vorhandenen IPv4-Weiterleitungssitzungsregel mithilfe der CLI eine erweiterte ACL-Regel zu:

Geben Sie an der Eingabeaufforderung

- `set forwardingSession <name> [-aclname <string>]`
- `show forwardingSession <name>`

So weisen Sie einer vorhandenen IPv6-Weiterleitungssitzungsregel mithilfe der CLI eine ACL6-Regel zu:

Geben Sie an der Eingabeaufforderung

- `set forwardingSession <name> [-acl6name <string>]`
- `show forwardingSession <name>`

Beispiel:

```
> add forwardingSession FS-1 -aclname ACL-9
Done

> add forwardingSession FS6-1  - acl6name ACL6-9
Done
```

Deaktivieren der Lenkung für Weiterleitungssitzungen in einem Cluster-Setup

Das Standardverhalten eines NetScaler-Clusters besteht darin, dass der Knoten, der Datenverkehr empfängt (Flow-Empfänger), den Datenverkehr an einen anderen Knoten (Flow-Prozessor) weiterleitet, der den Datenverkehr verarbeitet. Die Weiterleitung des Datenverkehrs vom Flow-Empfänger zum Flow-Prozessor erfolgt über die Cluster-Backplane und wird als Lenkung bezeichnet.

Die Steuerung kann bei der Verarbeitung in Echtzeit oder wenn das Setup Verbindungen mit hoher Latenz beinhaltet, ein Mehraufwand sein.

Die Steuerung für Weiterleitungssitzungen kann jetzt deaktiviert werden, sodass die Verarbeitung lokal auf dem Flow-Empfänger erfolgt. Das heißt, der Durchflussempfänger wird zum Durchflussprozessor.

Voraussetzungen

Beachten Sie die folgenden Punkte, bevor Sie die Regeln für Weiterleitungssitzungen in einem Cluster-Setup konfigurieren:

- Sie müssen Linksets so konfigurieren, dass sie für die Weiterleitung von Sitzungen verwendet werden.
- Sie müssen MAC Based Forwarding (MBF) im Cluster-Setup aktivieren.

Konfiguration der Regeln für Weiterleitungssitzungen in einem Cluster-Setup

Das Deaktivieren der Steuerung für Weiterleitungssitzungsregeln in einem Cluster-Setup kann auf den folgenden zwei Ebenen erfolgen:

- **Spezifische Regelebene für Weiterleitungssitzungen**. Aktivieren Sie den Parameter Process Local, während Sie eine neue Regel für die Weiterleitungssitzung hinzufügen oder eine bestehende Regel für eine Weiterleitungssitzung bearbeiten.
- **Weltweite Ebene**. Aktivieren Sie den Parameter Process Local, während Sie eine neue Cluster-Instance hinzufügen oder eine vorhandene Cluster-Instance bearbeiten. Die globale Einstellung hat Vorrang vor der Regeleinstellung für Weiterleitungssitzungen.

CLI-Verfahren

So deaktivieren Sie die Steuerung für eine Weiterleitungssitzungsregel in einem Cluster-Setup mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlsätze ein:

- Wenn Sie eine neue Weiterleitungssitzungsregel hinzufügen:
  - **ForwardingSession hinzufügen******(([\]) | -**acl6name | - aclname**) - ProcessLocal AKTIVIERT****<name><network><netmask><string><string>
  - **show forwardingSession** <name>
- Wenn Sie eine bestehende Regel für Weiterleitungssitzungen neu konfigurieren, gehen Sie wie folgt vor:
  - **set ForwardingSession- ProcessLocal AKTIVIERT**<name>

- **show forwardingSession** <name>

So deaktivieren Sie die Steuerung für alle (globalen) Weiterleitungssitzungsregeln in einem Cluster-Setup mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlsätze ein:

- Wenn Sie eine neue Cluster-Instanz hinzufügen:
  - **Clusterinstanz hinzufügen** <clid>-**ProcessLocal Enabled**
  - **Cluster-Instanz anzeigen** <clid>
- Wenn Sie eine bestehende Cluster-Instance neu konfigurieren:
  - **Clusterinstanz einrichten** <clid>—**ProcessLocal aktiviert**
  - **Cluster-Instanz anzeigen** <clid>

Beispielkonfiguration:

Im Folgenden finden Sie zwei Beispiele für die Deaktivierung von Steering auf Regelebene für Weiterleitungssitzungen und ein Beispiel für die Deaktivierung von Steering auf globaler Ebene.

```
An IPv4 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV4-1 10.102.105.51
    255.255.255.255 -processLocal Enabled
Done

An IPv6 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV6-1  - acl6name ACL6-
    FWD-SESSN-1 -processLocal Enabled
Done

A cluster setup, with an instance ID 10, has steering disabled at
    global level:

> set cluster instance 10 -processLocal Enabled
Done
<!--NeedCopy-->
```

GUI-Verfahren

So deaktivieren Sie die Steuerung für eine Weiterleitungssitzungsregel in einem Cluster-Setup mithilfe der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Weiterleitungssitzungen**und wählen Sie **Lokal verarbeiten** aus, während Sie eine neue Regel für Weiterleitungssitzungen hinzufügen oder eine bestehende Regel

für Weiterleitungssitzungen bearbeiten.

So deaktivieren Sie die Steuerung für alle (globalen) Weiterleitungssitzungsregeln in einem Cluster-Setup mithilfe der GUI:

Navigieren Sie zu **System** > **Cluster**und wählen Sie **Process Local** aus, während Sie eine Clusterkonfiguration hinzufügen oder eine bestehende Clusterkonfiguration ändern.

VLANs verstehen

May 11, 2023

Eine NetScaler-Appliance unterstützt Layer-2-Port und IEEE 802.1q-markierte VLANs. VLAN-Konfigurationen sind nützlich, wenn Sie den Verkehr auf bestimmte Stationsgruppen beschränken müssen. Sie können eine Netzwerkschnittstelle als Teil mehrerer VLANs konfigurieren, indem Sie IEEE 802.1q-Tagging verwenden.

Sie können VLANs konfigurieren und sie an IP-Subnetze binden. Der NetScaler führt dann die IP-Weiterleitung zwischen diesen VLANs durch (wenn er als Standardrouter für die Hosts in diesen Subnetzen konfiguriert ist).

Der NetScaler unterstützt die folgenden Arten von VLANs:

- **Portbasierte VLANs.** Die Mitgliedschaft in einem portbasierten VLAN wird durch eine Reihe von Netzwerkschnittstellen definiert, die sich eine gemeinsame, exklusive Layer-2-Broadcast-Domäne teilen. Sie können mehrere portbasierte VLANs konfigurieren. Standardmäßig sind alle Netzwerkschnittstellen auf dem NetScaler Mitglieder von VLAN 1.

  Wenn Sie 802.1q-Tagging auf den Port anwenden, gehört die Netzwerkschnittstelle zu einem portbasierten VLAN. Der Layer-2-Verkehr wird innerhalb eines portbasierten VLAN überbrückt, und Layer-2-Broadcasts werden an alle Mitglieder des VLAN gesendet, wenn der Layer-2-Modus aktiviert ist. Wenn Sie eine Netzwerkschnittstelle ohne Tags als Mitglied eines neuen VLAN hinzufügen, wird sie aus dem aktuellen VLAN entfernt.

- **Standard-VLAN.** Standardmäßig sind die Netzwerkschnittstellen auf dem NetScaler als ungetaggte Netzwerkschnittstellen in einem einzigen, portbasierten VLAN enthalten. Dieses VLAN ist das Standard-VLAN. Es hat eine VLAN-ID (VID) von 1. Dieses VLAN ist permanent vorhanden. Sie kann nicht gelöscht werden und ihre VID kann nicht geändert werden.

  Wenn Sie einem anderen VLAN als Mitglied ohne Tagged eine Netzwerkschnittstelle hinzufügen, wird die Netzwerkschnittstelle automatisch aus dem Standard-VLAN entfernt. Wenn Sie eine Netzwerkschnittstelle von ihrem aktuellen portbasierten VLAN trennen, wird sie wieder zum Standard-VLAN hinzugefügt.

- **Verschlagwortet mit VLANs.** 802.1q-Tagging (definiert im IEEE 802.1q-Standard) ermöglicht es einem Netzwerkgerät (wie dem NetScaler), Informationen zu einem Frame auf Layer 2 hinzuzufügen, um die VLAN-Mitgliedschaft des Frames zu identifizieren. Durch Tagging können Netzwerkumgebungen über VLANs verfügen, die sich über mehrere Geräte erstrecken. Ein Gerät, das das Paket empfängt, liest das Tag und erkennt das VLAN, zu dem der Frame gehört. Einige Netzwerkgeräte unterstützen nicht den Empfang von Paketen mit und ohne Tags auf derselben Netzwerkschnittstelle, insbesondere Force10-Switches. In solchen Fällen müssen Sie sich an den Kundensupport wenden, um Unterstützung zu erhalten.

  Die Netzwerkschnittstelle kann ein markiertes oder ein ungetaggtes Mitglied eines VLAN sein. Jede Netzwerkschnittstelle ist ein unmarkiertes Mitglied nur eines VLANs (seines nativen VLAN). Diese Netzwerkschnittstelle überträgt die Frames für das native VLAN als ungetaggte Frames. Eine Netzwerkschnittstelle kann Teil von mehr als einem VLAN sein, wenn die anderen VLANs gekennzeichnet sind.

  Wenn Sie das Tagging konfigurieren, achten Sie darauf, dass die Konfiguration des VLAN an beiden Enden der Verbindung übereinstimmt. Der Port, mit dem der NetScaler eine Verbindung herstellt, muss sich im selben VLAN wie die NetScaler-Netzwerkschnittstelle befinden.

  Hinweis: Diese VLAN-Konfiguration ist weder synchronisiert noch propagiert, daher müssen Sie die Konfiguration auf jeder Einheit in einem HA-Paar unabhängig voneinander durchführen.

Regeln zur Klassifizierung von Frames anwenden

VLANs haben zwei Arten von Regeln für die Klassifizierung von Frames:

- **Eingangsregeln.** Ingress-Regeln klassifizieren jeden Frame so, dass er nur zu einem einzigen VLAN gehört. Wenn ein Frame auf einer Netzwerkschnittstelle empfangen wird, werden die folgenden Regeln angewendet, um den Frame zu klassifizieren:
  - Wenn der Frame ungetaggt ist oder einen Tag-Wert gleich 0 hat, wird die VID des Frames auf die Port-VID (PVID) der Empfangsschnittstelle gesetzt, die als zum nativen VLAN gehörend eingestuft wird. (PVIDs sind im IEEE 802.1q-Standard definiert.)
  - Wenn der Frame einen Tag-Wert hat, der FFF entspricht, wird der Frame gelöscht.
  - Wenn die VID des Frames ein VLAN angibt, zu dem die empfangende Netzwerkschnittstelle kein Mitglied ist, wird der Frame gelöscht. Wenn beispielsweise ein Paket von einem Subnetz, das der VLAN-ID 12 zugeordnet ist, an ein Subnetz gesendet wird, das der VLAN-ID 10 zugeordnet ist, wird das Paket verworfen. Wenn ein Paket ohne Tags mit VID 9 von dem der VLAN-ID 10 zugeordneten Subnetz an eine Netzwerkschnittstelle PVID 9 gesendet wird, wird das Paket verworfen.
- **Regeln für ausgehenden Traffic.** Die folgenden Ausgangsregeln werden angewendet:

- Wenn die VID des Frames ein VLAN angibt, zu dem die Übertragungsnetzwerkschnittstelle kein Mitglied ist, wird der Frame verworfen.
- Während des Lernprozesses (definiert durch den IEEE 802.1q-Standard) werden Src MAC und VID verwendet, um die Bridge-Lookup-Tabelle des NetScaler zu aktualisieren.
- Ein Frame wird verworfen, wenn seine VID ein VLAN angibt, das keine Mitglieder hat. (Sie definieren Mitglieder, indem Sie Netzwerkschnittstellen an ein VLAN binden.)

VLANs und Paketweiterleitung auf dem NetScaler

Der Weiterleitungsprozess auf der NetScaler-Appliance ähnelt dem auf jedem Standard-Switch. Der NetScaler führt die Weiterleitung jedoch nur durch, wenn der Layer-2-Modus aktiviert ist. Die wichtigsten Merkmale des Weiterleitungsprozesses sind:

- Topologieeinschränkungen werden durchgesetzt. Zur Durchsetzung gehören die Auswahl jeder Netzwerkschnittstelle im VLAN als Übertragungsport (abhängig vom Status der Netzwerkschnittstelle), Überbrückungsbeschränkungen (Weiterleitung nicht an der empfangenden Netzwerkschnittstelle) und MTU-Einschränkungen.
- Frames werden auf der Grundlage von Informationen gefiltert, die in der Bridgetabellensuche in der Forwarding Database (FDB) -Tabelle des NetScaler enthalten sind. Die Suche nach der Bridgetabelle basiert auf dem Ziel-MAC und der VID. Pakete, die an die MAC-Adresse des NetScaler adressiert sind, werden in den oberen Layer verarbeitet.
- Alle Broadcast- und Multicast-Frames werden an jede Netzwerkschnittstelle weitergeleitet, die Mitglied des VLAN ist. Die Weiterleitung erfolgt jedoch nur, wenn der L2-Modus aktiviert ist. Wenn der L2-Modus deaktiviert ist, werden die Broadcast- und Multicast-Pakete verworfen. Dies gilt auch für MAC-Adressen, die derzeit nicht in der Bridging-Tabelle enthalten sind.
- Ein VLAN-Eintrag enthält eine Liste von Mitgliedsnetzwerkschnittstellen, die Teil seiner Elementgruppe ohne Tags sind. Bei der Weiterleitung von Frames an diese Netzwerkschnittstellen wird kein Tag in den Frame eingefügt.
- Wenn die Netzwerkschnittstelle ein markiertes Mitglied dieses VLANs ist, wird das Tag in den Frame eingefügt, wenn der Frame weitergeleitet wird.

Wenn ein Benutzer Broadcast- oder Multicast-Pakete sendet, ohne dass das VLAN identifiziert wird, also während der Duplicate Address Detection (DAD) für NSIP oder ND6 für den nächsten Hop der Route, wird das Paket an alle Netzwerkschnittstellen gesendet, wobei das entsprechende Tagging entweder auf den Ein- und Ausgangsregeln basiert. ND6 identifiziert normalerweise ein VLAN, und ein Datenpaket wird nur über dieses VLAN gesendet. Portbasierte VLANs sind für IPv4 und IPv6 üblich. Für IPv6 unterstützt NetScaler Präfix-basierte VLANs.

VLAN konfigurieren

May 11, 2023

Sie können VLANs in den folgenden Umgebungen implementieren:

- Einzelnes Subnetz
- Mehrere Subnetze
- Einzelnes LAN
- VLANs (kein Tagging)
- VLANs (802.1q-Tagging)

Wenn Sie VLANs konfigurieren, deren Mitglieder nur ungetaggte Netzwerkschnittstellen sind, ist die Gesamtzahl der möglichen VLANs auf die Anzahl der im NetScaler verfügbaren Netzwerkschnittstellen begrenzt. Wenn mehr IP-Subnetze mit einer VLAN-Konfiguration erforderlich sind, muss 802.1q-Tagging verwendet werden.

Wenn Sie eine Netzwerkschnittstelle an ein VLAN binden, wird die Netzwerkschnittstelle aus dem Standard-VLAN entfernt. Wenn die Netzwerkschnittstellen Teil von mehr als einem VLAN sein müssen, können Sie die Netzwerkschnittstellen als markierte Mitglieder an die VLANs binden.

Sie können den NetScaler so konfigurieren, dass er den Verkehr zwischen VLANs auf Ebene 3 weiterleitet. In diesem Fall ist ein VLAN einem einzelnen IP-Subnetz zugeordnet. Die Hosts in einem VLAN, die zu einem einzelnen Subnetz gehören, verwenden dieselbe Subnetzmaske und ein oder mehrere Standard-Gateways, die mit diesem Subnetz verbunden sind. Die Konfiguration von Layer 3 für ein VLAN ist optional. Layer 3 wird für die IP-Weiterleitung (Inter-VLAN-Routing) verwendet. Jedes VLAN hat eine eindeutige IP-Adresse und eine Subnetzmaske, die ein IP-Subnetz für das VLAN definieren. In einer HA-Konfiguration wird diese IP-Adresse mit den anderen NetScaler-Appliances geteilt. Der NetScaler leitet Pakete zwischen konfigurierten IP-Subnetzen (VLANs) weiter.

Wenn Sie den NetScaler konfigurieren, dürfen Sie keine überlappenden IP-Subnetze erstellen. Dadurch wird die Layer-3-Funktionalität beeinträchtigt.

Jedes VLAN ist eine einzigartige Layer-2-Broadcast-Domäne. Zwei VLANs, die jeweils an separate IP-Subnetze gebunden sind, können nicht zu einer einzigen Broadcast-Domäne zusammengefasst werden. Für die Weiterleitung von Datenverkehr zwischen zwei VLANs ist ein Layer-3-Weiterleitungsgerät (Routing) erforderlich, z. B. die NetScaler-Appliance.

Konfiguration von VLANs in einem HA-Setup

Die VLAN-Konfiguration für ein Hochverfügbarkeits-Setup erfordert, dass die NetScaler-Appliances dieselbe Hardwarekonfiguration haben und die darauf konfigurierten VLANs Spiegelbilder sein müssen.

Die richtige VLAN-Konfiguration wird automatisch implementiert, wenn die Konfiguration zwischen den NetScaler-Appliances synchronisiert wird. Das Ergebnis sind identische Aktionen auf allen Geräten. Wenn Sie beispielsweise die Netzwerkschnittstelle 0/1 zu VLAN2 hinzufügen, wird diese Netzwerkschnittstelle zu VLAN 2 auf allen Appliances hinzugefügt, die am Hochverfügbarkeits-Setup teilnehmen.

Hinweis: Wenn Sie in einem HA-Setup netzwerkschnittstellenspezifische Befehle verwenden, werden die von Ihnen erstellten Konfigurationen nicht an die andere NetScaler-Appliance weitergegeben. Sie müssen diese Befehle auf jeder Appliance in einem HA-Paar ausführen, um sicherzustellen, dass die Konfiguration der beiden Appliances im HA-Paar synchronisiert bleibt.

Ein VLAN erstellen oder ändern

Um ein VLAN zu konfigurieren, erstellen Sie eine VLAN-Entität und binden dann Netzwerkschnittstellen und IP-Adressen an das VLAN. Wenn Sie ein VLAN entfernen, werden seine Mitgliedsschnittstellen dem Standard-VLAN hinzugefügt.

CLI-Verfahren

Um ein VLAN mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- `add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED|DISABLED)]`
- `sh vlan <id>`

Beispiel:

```
1    > add vlan 2  -aliasName "Network A"   Done
2 <!--NeedCopy-->
```

Um eine Schnittstelle mit der CLI an ein VLAN zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- `bind vlan <id> -ifnum <slot/port>`
- `sh vlan <id>`

Beispiel:

```
1    > bind vlan 2 -ifnum 1/8   Done
2 <!--NeedCopy-->
```

Um eine IP-Adresse mit der CLI an ein VLAN zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- `bind vlan <id> -IPAddress <IPAddress> <netMask>`
- `sh vlan <id>`

Beispiel:

```
1    > bind vlan 2 -IPAddress 10.102.29.54 255.255.255.0   Done
2 <!--NeedCopy-->
```

Um ein VLAN mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- `rm vlan <id>`

GUI-Verfahren

So konfigurieren Sie ein VLAN mithilfe der GUI:

1. Navigieren Sie zu System > Netzwerk > VLANs, fügen Sie ein neues VLAN hinzu oder bearbeiten Sie ein vorhandenes VLAN.
2. Um eine IP-Adresse an ein VLAN zu binden, wählen Sie unter IP-Bindungen die Option Aktiv aus, die der IP-Adresse entspricht, die Sie an das VLAN binden möchten (z. B. 10.102.29.54). In der Spalte Typ wird der IP-Adresstyp (z. B. zugeordnete IP, virtuelle IP oder Subnetz-IP) für jede IP-Adresse in der Spalte IP-Adresse angezeigt.
3. Um eine Netzwerkschnittstelle an ein VLAN zu binden, wählen Sie unter Schnittstellenbindungen die Option Aktiv aus, die der Schnittstelle entspricht, die Sie an das VLAN binden möchten.

Überwachung von VLANs

Sie können VLAN-Statistiken wie empfangene Pakete, empfangene Byte, gesendete Pakete und gesendete Byte anzeigen und die Informationen verwenden, um Anomalien zu identifizieren und/oder ein VLAN zu debuggen.

Gehen Sie wie folgt vor, um die Statistiken eines VLANs mithilfe der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- `stat vlan <vlanID>`

Beispiel:

```
1    stat vlan 2
2 <!--NeedCopy-->
```

Um die Statistiken eines VLANs mithilfe der GUI anzuzeigen:

1. Navigieren Sie zu System > Netzwerk > VLANs.
2. Wählen Sie das VLAN aus, und klicken Sie auf Statistiken.

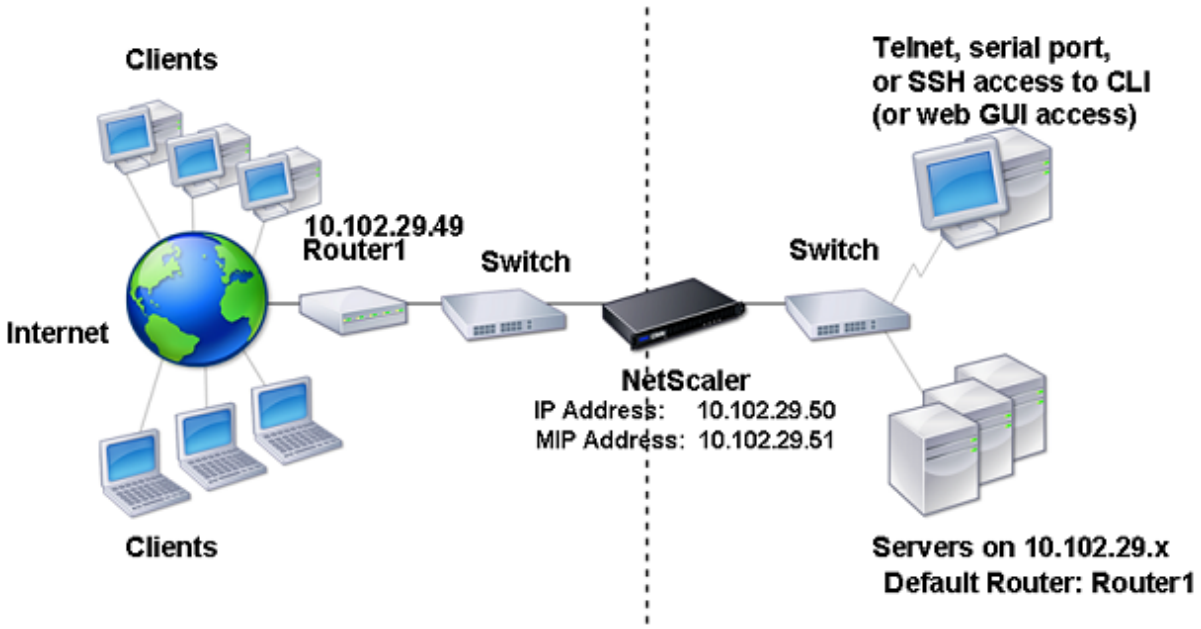
VLANs in einem einzigen Subnetz konfigurieren

May 11, 2023

Bevor Sie ein VLAN in einem einzelnen Subnetz konfigurieren, stellen Sie sicher, dass der Layer-2-Modus aktiviert ist.

Die folgende Abbildung zeigt eine einzelne Subnetzumgebung.

Abbildung 1. VLAN in einem einzelnen Subnetz



In der obigen Abbildung:

1. Der Standardrouter für den NetScaler und die Server ist Router 1.
2. Der Layer-2-Modus muss auf dem NetScaler aktiviert sein, damit der NetScaler direkten Zugriff auf die Server hat.
3. Für dieses Subnetz kann ein virtueller Server für den Lastenausgleich auf der NetScaler Appliance konfiguriert werden.

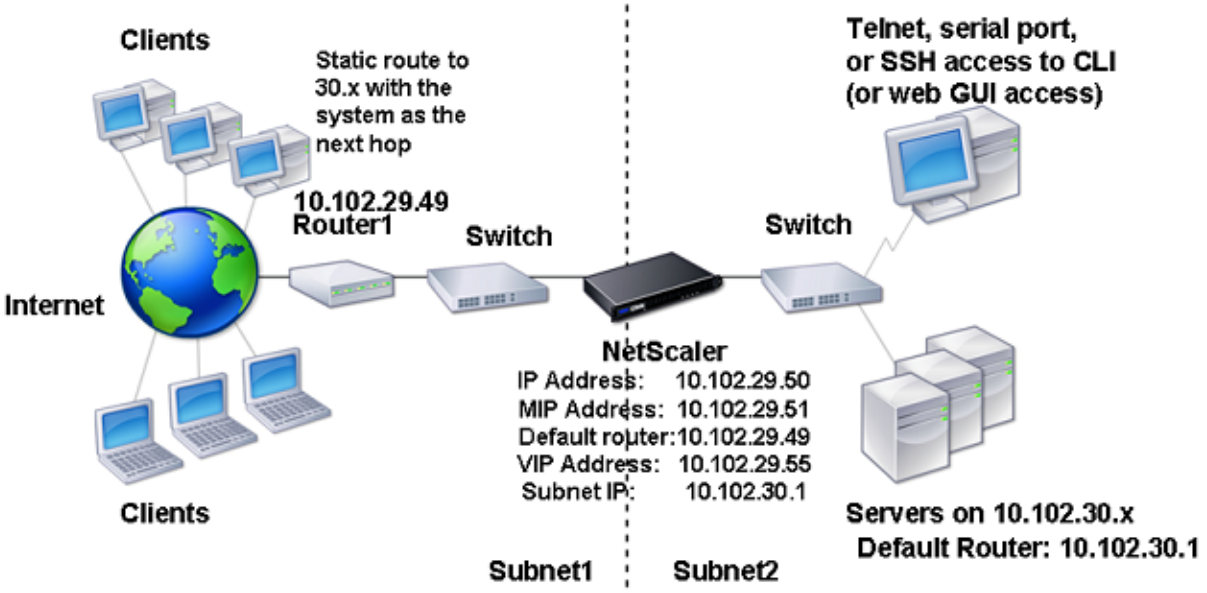
Um ein VLAN in einem einzelnen Subnetz zu konfigurieren, befolgen Sie die unter Konfigurieren eines VLANbeschriebenen Anweisungen.

Konfigurieren von VLANs auf mehreren Subnetzen

August 19, 2021

Um ein einzelnes VLAN über mehrere Subnetze hinweg zu konfigurieren, müssen Sie eine VIP für das VLAN hinzufügen und das Routing entsprechend konfigurieren. Die folgende Abbildung zeigt ein einzelnes VLAN, das über mehrere Subnetze konfiguriert ist.

Abbildung 1. Mehrere Subnetze in einem einzigen VLAN



So konfigurieren Sie ein einzelnes VLAN über mehrere Subnetze hinweg:

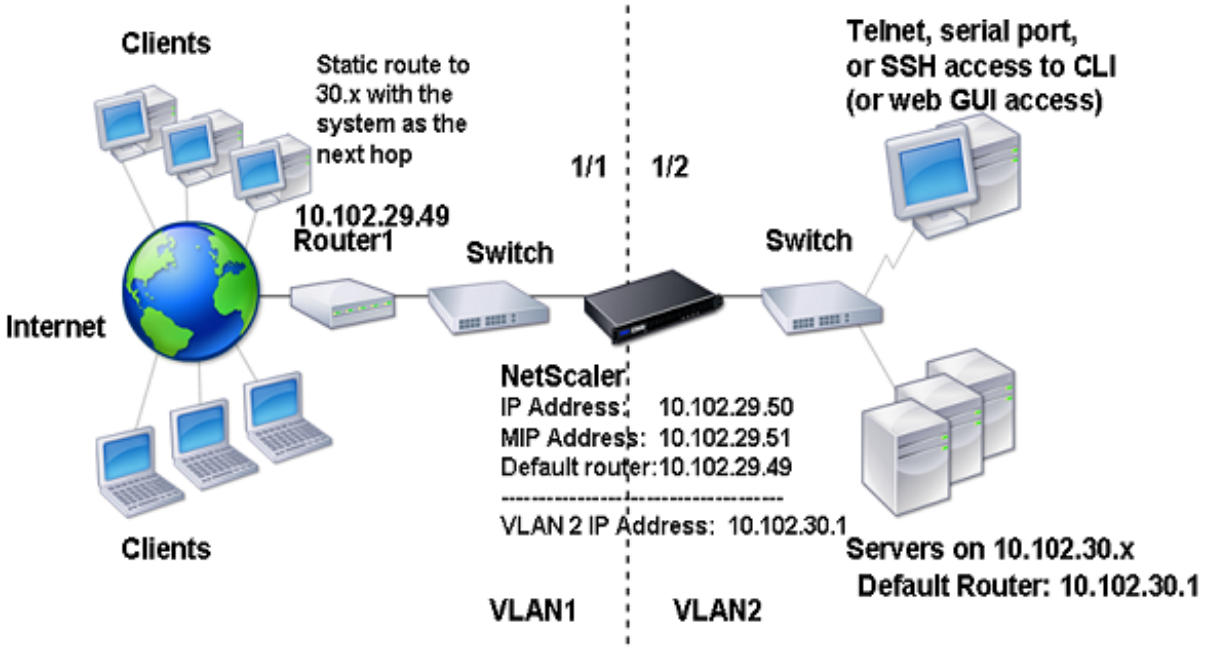
1. Deaktivieren Sie den Layer-2-Modus. Informationen zum Deaktivieren des Layer-2-Modus finden Sie unter Paketweiterleitungsmodi.
2. Fügen Sie eine VIP-Adresse hinzu. Informationen zum Hinzufügen einer VIP-Adresse finden Sie unter Konfigurieren und Verwalten virtueller IP-Adressen (VIPs).
3. RNAT Regel konfigurieren. Informationen zum Konfigurieren der RNAT-ID finden Sie unter Konfigurieren von RNAT.

Mehrere nicht getaggte VLANs in mehreren Subnetzen konfigurieren

May 11, 2023

In Umgebungen mit mehreren VLANs ohne Tags in mehreren Subnetzen wird für jedes IP-Subnetz ein VLAN konfiguriert. Eine Netzwerkschnittstelle ist nur an ein VLAN gebunden. Die folgende Abbildung zeigt diese Konfiguration.

Abbildung 1. Mehrere Subnetze mit VLANs — kein Tagging



Führen Sie die folgenden Aufgaben aus, um die in der obigen Abbildung gezeigte Konfiguration zu implementieren:

1. Fügen Sie VLAN 2 hinzu.
2. Binden Sie die 1/2-Netzwerkschnittstelle des NetScaler als Netzwerkschnittstelle ohne Tags an VLAN 2 an.
3. Binden Sie die IP-Adresse und die Subnetzmaske an VLAN 2.

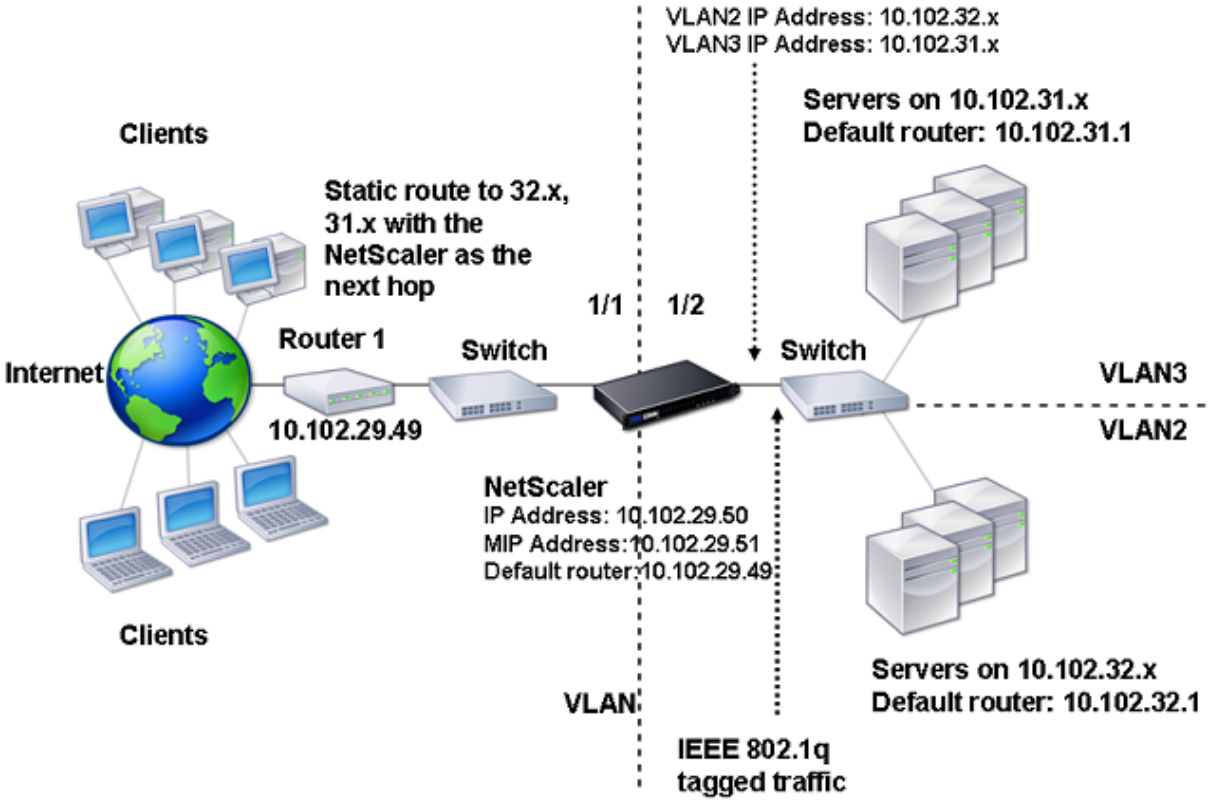
Anweisungen zu diesen Aufgaben finden Sie unter Konfigurieren eines VLAN.

Mehrerer VLANs mit 802.1q-Tagging konfigurieren

May 11, 2023

Für mehrere VLANs mit 802.1q-Tagging ist jedes VLAN mit einem anderen IP-Subnetz konfiguriert. Jede Netzwerkschnittstelle befindet sich in einem VLAN. Eines der VLANs ist wie gekennzeichnet eingerichtet. Die folgende Abbildung zeigt diese Konfiguration.

Abbildung 1. Mehrere VLANs mit IEEE 802.1q-Tagging



Führen Sie die folgenden Aufgaben aus, um die in der obigen Abbildung gezeigte Konfiguration zu implementieren:

1. Fügen Sie VLAN 2 hinzu.
2. Binden Sie die 1/2-Netzwerkschnittstelle des NetScaler als Netzwerkschnittstelle ohne Tags an VLAN 2 an.
3. Binden Sie die IP-Adresse und die Netzmaske an VLAN 2.
4. Fügen Sie VLAN 3 hinzu.
5. Binden Sie die 1/2-Netzwerkschnittstelle des NetScaler als markierte Netzwerkschnittstelle an VLAN 3 an.
6. Binden Sie die IP-Adresse und die Netzmaske an VLAN 3.

Anweisungen zu diesen Aufgaben finden Sie unter Konfigurieren eines VLAN.

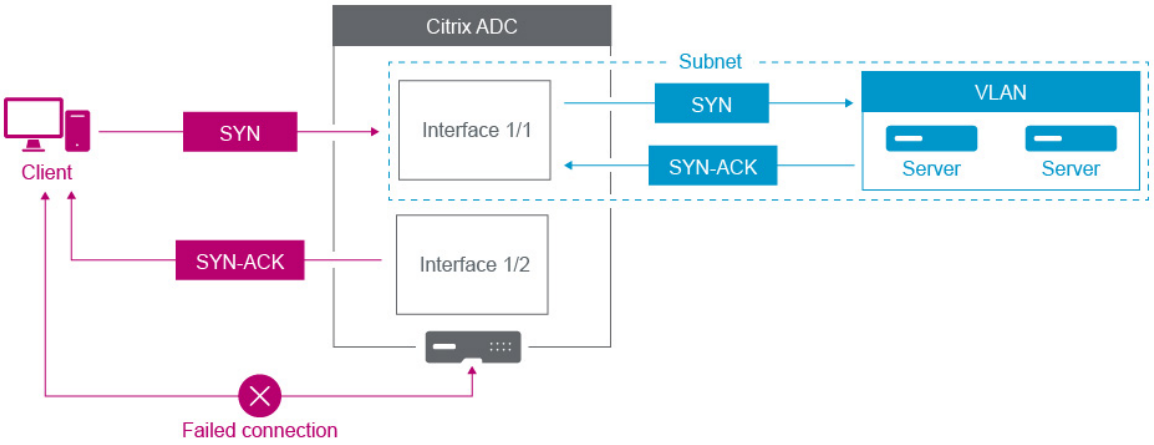
Ordnen Sie mithilfe von VLANs ein IP-Subnetz einer NetScaler-Schnittstelle zu

May 11, 2023

Standardmäßig bietet eine NetScaler Appliance keine Unterscheidung zwischen Netzwerkschnittstellen.

Die Appliance funktioniert eher wie ein Netzwerk-Hub als ein Switch. Dies kann zu Layer-3-Netzwerkschleifen führen, in denen doppelter Datenverkehr über mehrere Schnittstellen übertragen wird.

In solchen Szenarien ist es je nach Netzwerkdesign möglich, dass eine Anfrage auf einer Schnittstelle übertragen wird und die entsprechende Antwort auf einer anderen Schnittstelle empfangen wird.



Beispielsweise können ein auf einer Schnittstelle gesendetes SYN-Paket und die auf einer anderen Schnittstelle empfangene SYN-ACK-Antwort zu einem Verbindungsausfall führen, da die Appliance erwartet, das SYN-ACK auf derselben Schnittstelle zu empfangen, die das ursprüngliche SYN-Paket gesendet hat.

Um solche Probleme zu lösen, kann die Appliance interne oder externe VLANs verwenden, um bestimmte Subnetze Schnittstellen zuzuordnen.

Voraussetzungen

Bevor Sie beginnen, mithilfe von VLANs ein IP-Subnetz einer NetScaler-Schnittstelle zuzuordnen, beachten Sie die folgenden Punkte:

- Die Netzwerkkonnektivität kann versehentlich verloren gehen, wenn ein VLAN dem Subnetz oder der Schnittstelle zugeordnet wird, das derzeit für den Zugriff auf die NetScaler-GUI oder die Befehlszeilenschnittstelle verwendet wird. Daher wird in solchen Szenarien dringend empfohlen, die Änderung vorzunehmen, indem über die serielle Konsole einer physischen NetScaler-Appliance oder über die virtuelle serielle Konsole eines NetScaler VPX auf die Befehlszeilenschnittstelle zugegriffen wird.
- Die NetScaler-Verwaltungsschnittstellen verfügen nicht über bestimmte Funktionen zur Hardwareoptimierung, weshalb sie für den Einsatz im Produktionsdatenverkehr weniger wünschenswert sind. Daher wird empfohlen, den NetScaler so zu konfigurieren, dass er nur die Verwaltungsschnittstellen für den Verwaltungsverkehr (NSIP) verwendet. In der Standardkonfiguration gibt es keine logische Unterscheidung zwischen den Verwaltungsschnittstellen

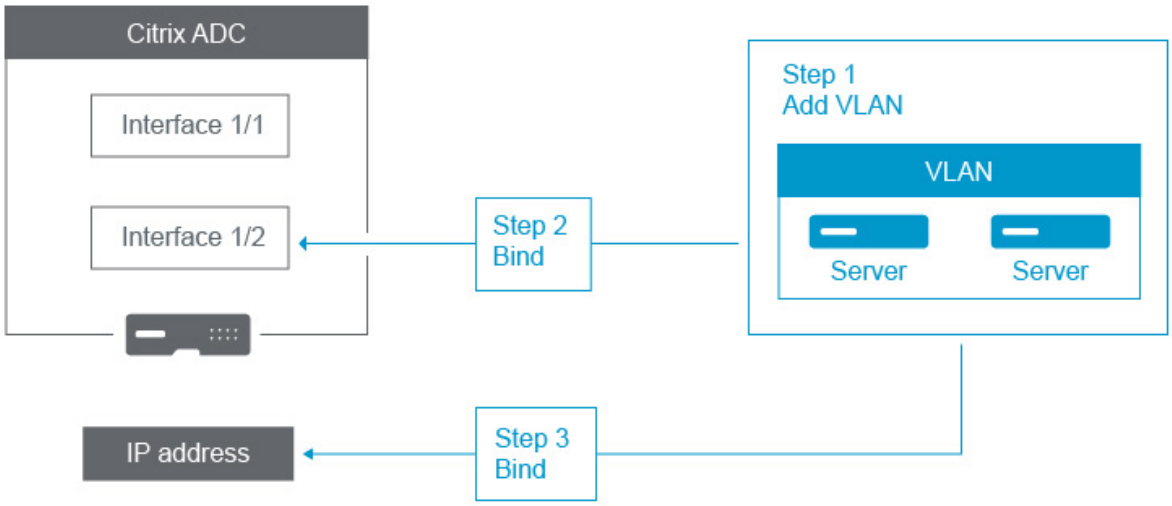
und Datenschnittstellen auf einem Hardware-NetScaler. Um dieses Ziel zu erreichen, wird empfohlen, dass sich das NSIP in einem vom Datenverkehr getrennten VLAN befindet, sodass der Verwaltungsdatenverkehr auf einer separaten Schnittstelle erfolgen kann.

Obwohl das Konzept dasselbe ist, müssen Sie NSVLAN anstelle der folgenden Anweisungen konfigurieren, um die VLAN-Zuordnungen des Subnetzes zu ändern, das die NSIP-Adresse enthält. Solche Änderungen erfordern auch einen Neustart des NetScaler, um wirksam zu werden. Weitere Informationen finden Sie unter Konfigurieren von NSVLAN.

- Bei NetScaler SDX wird dringend empfohlen, dass sich das NSIP jeder Instanz im selben Subnetz und VLAN befindet wie die SVM (Management Service GUI) und XenServer des SDX. Die SVM kommuniziert mit Instanzen über das Netzwerk. Wenn sich SVM, XenServer und Instanzen nicht im selben VLAN und Subnetz befinden, muss der Verwaltungsverkehr außerhalb des SDX fließen. In dieser Situation können Netzwerkprobleme dazu führen, dass der Instanzstatus gelb oder rot angezeigt wird. Dadurch können Verwaltungs- und Konfigurationsänderungen der NetScaler-Instances verhindert werden.

Konfigurationsschritte

Das Zuordnen eines IP-Subnetzes zu einer NetScaler-Schnittstelle umfasst die folgenden Aufgaben:



Fügen Sie ein VLANhinzu. Wenn Sie beim Hinzufügen eines VLAN das VLAN taggen, müssen Sie eine VLAN-Nummer auswählen, die im Netzwerk-Switch für den zugehörigen Switch-Port definiert ist. Wenn das VLAN nicht gekennzeichnet ist und intern in der Appliance ist, wird empfohlen, dass Sie die VLAN-Nummer auswählen, die in der Switch-Konfiguration verfügbar ist, damit Sie leicht darauf zugreifen können.

Binden Sie eine Schnittstelle an das VLAN. Wenn Sie Link Aggregation verwenden, verknüpfen Sie das VLAN während der Bindung mit dem LA-Kanal (z. B. LA/1) und nicht mit der physischen Schnittstelle. Das VLAN darf nur mit einer Netzwerkschnittstelle verknüpft sein.

Wenn Sie den Traffic auf der Schnittstelle taggen möchten, verwenden Sie die Option tagged (Tag). Andernfalls verlässt der Datenverkehr die Appliance ohne Tagging und wird dem nativen VLAN des Switch-Ports zugeordnet.

Binden Sie eine IP-Adresse an das VLAN. Wenn Sie während der Bindung mehr als eine IP-Adresse aus demselben Subnetz binden, tritt ein Fehler auf. Wenn eine IP-Adresse mit einem VLAN verknüpft ist, werden alle IP-Adressen in diesem Subnetz automatisch dem VLAN zugeordnet.

> **Hinweis:**
>
> In einem Hochverfügbarkeitssetup (HA) werden diese VLAN-Konfigurationen während der HA-Synchronisierung automatisch vom primären Knoten zum sekundären Knoten hinzugefügt. Weitere Informationen zu Hochverfügbarkeits-Setups finden Sie unter Hochverfügbarkeit.

CLI-Verfahren

Um ein VLAN mit der CLI hinzuzufügen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add vlan** <id>
- **Ash Vlan** <id>

Um eine Schnittstelle mit der CLI an ein VLAN zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- **bind vlan** <id>-**ifnum** <slot/port>
- **Ash Vlan** <id>

Um eine IP-Adresse mit der CLI an ein VLAN zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- **Vlan binden- IP-Adresse** <id><IPAddress><netMask>
- **Ash Vlan** <id>

Beispiel:

```
> add vlan 100

> bind vlan 100 -ifnum 1/1

> bind vlan 100 -ipAddress 10.0.1.0 255.255.255.0
<!--NeedCopy-->
```


GUI-Verfahren

So konfigurieren Sie ein VLAN mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VLANs**und fügen Sie ein neues VLAN hinzu.
2. Um eine Netzwerkschnittstelle an ein VLAN zu binden, wählen Sie unter **Schnittstellenbindungen**die Option **Aktiv** aus, die der Schnittstelle entspricht, die Sie an das VLAN binden möchten.
3. Um eine IP-Adresse an ein VLAN zu binden, wählen Sie unter **IP-Bindungen**die Option **Aktiv** aus, die der IP-Adresse entspricht, die Sie an das VLAN binden möchten (z. B. 10.102.29.54). In der Spalte **Typ** wird der IP-Adresstyp für jede IP-Adresse in der Spalte **IP-Adresse** angezeigt.

Bewährte Methoden für NetScaler-Appliance-Netzwerke und VLAN

May 11, 2023

Eine NetScaler-Appliance verwendet VLANs, um zu bestimmen, welche Schnittstelle für welchen Datenverkehr verwendet werden muss. Darüber hinaus nimmt die NetScaler-Appliance nicht an Spanning Tree teil. Ohne die richtige VLAN-Konfiguration kann die NetScaler-Appliance nicht bestimmen, welche Schnittstelle verwendet werden soll, und sie kann eher wie ein HUB als wie ein Switch oder ein Router funktionieren. Mit anderen Worten, die NetScaler-Appliance kann alle Schnittstellen für jede Konversation verwenden.

Symptome einer VLAN-Fehlkonfiguration

VLAN-Fehlkonfigurationsprobleme können sich in vielen Formen äußern, darunter Leistungsprobleme, Unfähigkeit, Verbindungen herzustellen, nach dem Zufallsprinzip unterbrochene Sitzungen und in schwerwiegenden Situationen Netzwerkstörungen, die scheinbar nichts mit der NetScaler-Appliance selbst zu tun haben. Die NetScaler-Appliance kann je nach Art der Interaktion mit Ihrem Netzwerk auch MAC-Verschiebungen, stummgeschaltete Schnittstellen und/oder Übertragungs- oder Empfangspufferüberläufe der Verwaltungsschnittstelle melden.

MAC-Moves (counter nic_tot_bdg_mac_moved): Dieses Problem weist darauf hin, dass die NetScaler-Appliance mehr als eine Schnittstelle verwendet, um mit demselben Gerät zu kommunizieren (MAC-Adresse), da sie nicht richtig bestimmen konnte, welche Schnittstelle verwendet werden sollte.

Stummschaltete Schnittstellen (counter nic_err_bdg_muted): Dieses Problem weist darauf hin, dass die NetScaler-Appliance aufgrund von VLAN-Konfigurationsproblemen erkannt hat, dass sie aufgrund von VLAN-Konfigurationsproblemen eine Routing-Schleife erstellt, und daher eine oder mehrere der störenden Schnittstellen heruntergefahren hat, um einen Netzwerkausfall zu verhindern.

Schnittstellenpufferüberläufe, die sich in der Regel auf Verwaltungsschnittstellen beziehen (counter nic_err_tx_overflow): Dieses Problem kann verursacht werden, wenn zu viel Datenverkehr über eine Verwaltungsschnittstelle übertragen wird. Die Verwaltungsschnittstellen der NetScaler-Appliance sind nicht für die Verarbeitung großer Datenverkehrsmengen konzipiert. Dies kann auf Netzwerk- und VLAN-Fehlkonfigurationen zurückzuführen sein, die die NetScaler-Appliance veranlassen, eine Verwaltungsschnittstelle für den Produktionsdatenverkehr zu verwenden. Dies tritt häufig auf, weil die NetScaler-Appliance den Verkehr im VLAN/Subnetz des NSIP (NSVLAN) nicht vom regulären Produktionsverkehr unterscheiden kann. Es wird dringend empfohlen, dass sich das NSIP in einem separaten VLAN und Subnetz von allen Produktionsgeräten wie Workstations und Servern befindet.

Orphan ACKs (counter tcp_err_orphan_ack): Dieses Problem weist darauf hin, dass die NetScaler-Appliance ein ACK-Paket empfangen hat, das sie nicht erwartet hatte, normalerweise auf einer anderen Schnittstelle als der ACK-Verkehr, von dem der ACK-Verkehr stammt. Diese Situation kann durch VLAN-Fehlkonfigurationen verursacht werden, bei denen die NetScaler-Appliance über eine andere Schnittstelle sendet, als das Zielgerät normalerweise für die Kommunikation mit der NetScaler-Appliance verwenden würde (häufig in Verbindung mit MAC-Verschiebungen).

Hohe Wiederholungs- oder Weiterübertragungsraten lassen nach (Zähler: tcp_err_retransmit_giveups, tcp_err_7th_retransfer, verschiedene andere Wiederübertragungszähler): Die NetScaler-Appliance versucht insgesamt 7 Mal, ein TCP-Paket erneut zu übertragen, bevor sie aufgibt und die Verbindungbeendet. Diese Situation kann zwar durch Netzwerkbedingungen verursacht werden, tritt jedoch häufig als Folge einer Fehlkonfiguration von VLAN und Schnittstelle auf.

Hochverfügbarkeit Split Brain: Split Brainist ein Zustand, bei dem beide Hochverfügbarkeitsknoten glauben, dass sie primär sind, was zu doppelten IP-Adressen und zum Verlust der NetScaler-Appliance-Funktionalität führt. Dies wird verursacht, wenn die beiden Hochverfügbarkeitsknoten nicht über Hochverfügbarkeits-Heartbeats auf dem UDP-Port 3003 unter Verwendung von NSIP über eine beliebige Schnittstelle miteinander kommunizieren können. Dies wird in der Regel durch VLAN-Fehlkonfigurationen verursacht, bei denen das native VLAN auf den NetScaler-Appliance-Schnittstellen keine Konnektivität zwischen NetScaler-Appliances hat.

Bewährte Methoden für VLAN- und Netzwerkkonfigurationen

1. Jedes Subnetz muss mit einem VLAN verknüpft sein.
2. Mit demselben VLAN kann mehr als ein Subnetz verknüpft werden (abhängig von Ihrem Netzwerkdesign).
3. Jedes VLAN sollte nur einer Schnittstelle zugeordnet sein (für die Zwecke dieser Diskussion gilt ein LA-Kanal als eine einzelne Schnittstelle).
4. Wenn Sie möchten, dass einer Schnittstelle mehr als ein Subnetz zugeordnet wird, müssen die Subnetze gekennzeichnet werden.

5. Entgegen der landläufigen Meinung ist die Mac-Based-Forwarding (MBF) -Funktion der NetScaler-Appliance nicht darauf ausgelegt, diese Art von Problem zu lösen. MBF wurde in erster Linie für den DSR-Modus (Direct Server Return) der NetScaler-Appliance entwickelt, der in den meisten Umgebungen selten verwendet wird (er ist so konzipiert, dass der Datenverkehr die NetScaler-Appliance auf dem Rückpfad von den Back-End-Servern absichtlich Bypass kann). MBF kann in einigen Fällen VLAN-Probleme verbergen, aber bei der Lösung dieser Art von Problemen sollte man sich nicht darauf verlassen.
6. Jede Schnittstelle auf der NetScaler-Appliance erfordert ein systemeigenes VLAN (im Gegensatz zu Cisco, wo native VLANs optional sind), obwohl die TagAll-Einstellung auf einer Schnittstelle verwendet werden kann, damit kein unmarkierter Datenverkehr die fragliche Schnittstelle verlässt.
7. Das native VLAN kann bei Bedarf für Ihr Netzwerkdesign mit Tags versehen werden (dies ist die TagAll-Option für die Schnittstelle).
8. Das VLAN für das Subnetz des NSIP Ihrer NetScaler-Appliance ist ein Sonderfall. Dies wird als NSVLAN bezeichnet. Die Konzepte sind dieselben, aber die Befehle zur Konfiguration sind unterschiedlich, und Änderungen am NSVLAN erfordern einen Neustart der NetScaler-Appliance, um wirksam zu werden. Wenn Sie versuchen, ein VLAN an ein SNIP zu binden, das dasselbe Subnetz wie das NSIP nutzt, erhalten Sie die Meldung „Operation not permitted“. Dies liegt daran, dass Sie stattdessen die NSVLAN-Befehle verwenden müssen. Bei einigen Firmware-Versionen können Sie außerdem kein NSVLAN einrichten, wenn diese VLAN-Nummer über den Befehl vorhanden ist. `add VLAN` Entfernen Sie einfach das VLAN und stellen Sie das NSVLAN erneut ein.
9. Hochverfügbare Heartbeats verwenden immer das native VLAN der jeweiligen Schnittstelle (optional markiert, wenn die TagAll-Option auf der Schnittstelle gesetzt ist).
10. Es muss eine Kommunikation zwischen mindestens einem Satz systemeigener VLANs auf den beiden Knoten eines Hochverfügbarkeitspaares bestehen (dies kann direkt oder über einen Router erfolgen). Die nativen VLANs werden für Hochverfügbarkeits-Taktsignale verwendet. Wenn die NetScaler-Appliances auf keiner Schnittstelle zwischen nativen VLANs kommunizieren können, führt dies zu Hochverfügbarkeits-Failovers und möglicherweise zu einer Split-Brain-Situation, in der beide NetScaler-Appliances denken, dass sie primär sind (was unter anderem zu doppelten IP-Adressen führt).
11. Die NetScaler-Appliance nimmt nicht an Spanning Tree teil. Daher ist es nicht möglich, Spanning Tree zu verwenden, um Schnittstellenredundanz zu gewährleisten, wenn eine NetScaler-Appliance verwendet wird. Verwenden Sie zu diesem Zweck stattdessen eine Form der Link-Aggregation (LACP oder manuelles LAG).

    Hinweis: Wenn Sie eine Link-Aggregation zwischen mehreren physischen Switches einrichten möchten, müssen Sie die Switches als virtuellen Switch konfigurieren, indem Sie eine Funktion wie den Switch Stack von Cisco verwenden.

12. Die Hochverfügbarkeitssynchronisierung und die Befehlsverbreitung verwenden standardmäßig das NSIP/NSVLAN. Um diese auf ein anderes VLAN zu verteilen, können Sie die SyncVLAN-Option des Befehls verwenden. `set HA node`

13. In der Standardkonfiguration der NetScaler Appliance ist nichts integriert, was darauf hindeutet, dass eine Verwaltungsschnittstelle (0/1 oder 0/2) nur auf den Verwaltungsdatenverkehr beschränkt ist. Diese Einschränkung muss vom Endbenutzer durch die VLAN-Konfiguration durchgesetzt werden. Die Verwaltungsschnittstellen sind nicht für den Datenverkehr konzipiert, daher muss Ihr Netzwerkdesign diesen Punkt berücksichtigen. Den Verwaltungsschnittstellen, die auf der Hauptplatine der NetScaler Appliance enthalten sind, fehlen verschiedene Offloading-Funktionen wie CRC-Offload, größere Paketpuffer und andere Optimierungen, sodass sie bei der Verarbeitung großer Datenverkehrsmengen viel weniger effizient sind. Um Produktionsdaten und Verwaltungsdatenverkehr zu trennen, darf sich das NSIP nicht im selben Subnetz/VLAN wie Ihr Datenverkehr befinden.

14. Wenn für die Übertragung des Verwaltungsdatenverkehrs eine Verwaltungsschnittstelle verwendet werden soll, empfiehlt es sich, dass sich die Standardroute in einem anderen Subnetz als dem Subnetz des NSIP (NSVLAN) befindet.

    In vielen Konfigurationen wird die Standardroute für die Workstation-Kommunikation verwendet (in einem Internetszenario). Wenn sich die Standardroute im selben Subnetz wie das NSIP befindet, kann die ADC-Appliance die Verwaltungsschnittstelle verwenden, um Datenverkehr zu senden und zu empfangen. Diese Nutzung des Datenverkehrs kann die Verwaltungsschnittstelle überlasten.

15. Außerdem müssen sich ein SDX, die SVM, XenServer und alle NetScaler-Instanz-NSIPs im selben VLAN und Subnetz befinden. Es gibt keine **Rückwandplatine** in der SDX-Appliance, die die Kommunikation zwischen SVM/Xen/Instanzen ermöglicht. Wenn sie sich nicht auf demselben VLAN/Subnetz/Interface befinden, muss der Datenverkehr zwischen ihnen die physische Hardware verlassen, über Ihr Netzwerk weitergeleitet werden und zurückkehren.

    Diese Konfiguration kann zu offensichtlichen Verbindungsproblemen zwischen den Instanzen und der SVM führen und wird daher nicht empfohlen. Ein häufiges Symptom hierfür ist eine gelbe Instanzstatusanzeige in der SVM für die fragliche VPX-Instanz und die Unfähigkeit, die SVM zur Neukonfiguration einer VPX-Instanz zu verwenden.

16. Wenn einige VLANs an Subnetze gebunden sind und andere nicht, werden während eines Hochverfügbarkeits-Failovers keine GARP-Pakete für IP-Adressen in den Subnetzen gesendet, die nicht an ein VLAN gebunden sind. Diese Konfiguration kann bei Failovers mit hoher Verfügbarkeit zu Verbindungsabbrüchen und Verbindungsproblemen führen. Dieses Problem wird dadurch verursacht, dass die NetScaler-Appliance die Änderung der Netzwerk-MAC-Besitz-IP-Adressen auf nicht VMAC-konfigurierten NetScaler-Appliances nicht benachrichtigen kann.

Die Symptome hierfür sind, dass der Leistungsindikator ip_tot_floating_ip_err nach einem Hochverfügbarkeits-Failover länger als einige Sekunden auf der früheren primären NetScaler Appliance inkrementiert wird, was darauf hinweist, dass das Netzwerk keine GARP-Pakete empfangen oder verarbeitet hat und das Netzwerk weiterhin Daten an die neue sekundäre NetScaler Appliance.

NSVLAN konfigurieren

May 11, 2023

NSVLAN ist ein VLAN, an das das Subnetz der NetScaler Management IP (NSIP)-Adresse gebunden ist. Das NSIP-Subnetz ist nur auf Schnittstellen verfügbar, die mit NSVLAN verknüpft sind. Standardmäßig ist NSVLAN VLAN 1, aber Sie können ein anderes VLAN als NSVLAN festlegen. In diesem Fall müssen Sie die NetScaler Appliance neu starten, damit die Änderung wirksam wird. Nach dem Neustart ist der NSIP-Subnetzverkehr auf das neue NSVLAN beschränkt.

Der Datenverkehr aus dem NetScaler IP-Subnetz kann mit der für NSVLAN angegebenen VLAN-ID (802.1q) gekennzeichnet werden. Sie müssen die angeschlossene Switch-Schnittstelle so konfigurieren, dass dieselbe VLAN-ID auf der verbundenen Schnittstelle markiert und zugelassen wird. Wenn Sie Ihre NSVLAN-Konfiguration entfernen, wird das NSIP-Subnetz automatisch an VLAN 1 gebunden, wodurch das Standard-NSVLAN wiederhergestellt wird.

So konfigurieren Sie NSVLAN mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set ns config -nsvlan** <positive_integer> -**ifnum** <interface_name> … [-**tagged** (YES|NO)]
- **show ns config**

> **Hinweis:**
>
> Die Konfiguration wird nach dem Neustart der NetScaler Appliance wirksam.

Beispiel:

```
> set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged YES
 Done

> save config
 Done
<!--NeedCopy-->
```

So stellen Sie die standardmäßige NSVLAN-Konfiguration über die CLIwieder her:

Geben Sie in der Befehlszeile Folgendes ein:

- **unset ns config -nsvlan**
- **show ns config**

Beispiel:

```
> unset ns config -nsvlan
 Done
<!--NeedCopy-->
```

So konfigurieren Sie NSVLAN mit der GUI:

Navigieren Sie zu **System** > **Einstellungen**, und klicken Sie in der Gruppe **Einstellungen** auf **NSVLAN-Einstellungen ändern**.

MTU auf dem NSVLAN einrichten

Standardmäßig ist die MTU des NSVLAN auf 1500 Byte eingestellt. Sie können diese Einstellung ändern, um den Durchsatz und die Netzwerkleistung zu optimieren. Beispielsweise können Sie das NSVLAN für die Verarbeitung von Jumbo-Frames konfigurieren.

So legen Sie die MTU des NSVLAN mit der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- **set vlan** <id> **-mtu** <positive_integer>
- **show vlan** <id>

So legen Sie die MTU des NSVLAN über die GUI fest:

Navigieren Sie zu **System** > **Netzwerk** > **VLANs**, öffnen Sie das NSVLAN und legen Sie den Parameter **Maximale Übertragungseinheit** fest.

Beispielkonfiguration:

In der folgenden Beispielkonfiguration ist VLAN 100 das NSVLAN.

```
> set ns config -nsvlan 100 -ifnum 1/1 -tagged no

  Warning: The configuration must be saved and the system rebooted for
     these settings to take effect

> set vlan 100 -mtu 1600

  Done

> sh vlan

  1)  VLAN ID: 1
```



```
12
13        Link-local IPv6 addr:
14      fe80::947b:52ff:fead:12d5/64
15
16        Interfaces : 1/2 LO/1
17
18    2)  VLAN ID: 100    VLAN Alias Name:
19
20        MTU: 1600
21
22        Interfaces : 1/1
23
24        IPs :
25
26            10.102.53.114     Mask: 255.255.255.0
27
28    Done
29
30  > save config
31
32    Done
33  <!--NeedCopy-->
```

Liste zulässiger VLANs konfigurieren

May 11, 2023

NetScaler akzeptiert und sendet markierte Pakete eines VLAN auf einer Schnittstelle, wenn das VLAN explizit auf der NetScaler-Appliance konfiguriert ist und die Schnittstelle an das VLAN gebunden ist. Bei einigen Bereitstellungen (z. B. Bump in the Wire) muss die NetScaler-Appliance als transparentes Gerät fungieren, das markierte Pakete akzeptiert und weiterleitet, die sich auf eine große Anzahl von VLANs beziehen. Für diese Anforderung ist die Konfiguration und Verwaltung einer großen Anzahl von VLANs keine praktikable Lösung.

Die Liste der zulässigen VLANs auf einer Schnittstelle gibt eine Liste von VLANs an. Die Schnittstelle akzeptiert und sendet auf transparente Weise markierte Pakete, die sich auf die angegebenen VLANs beziehen, ohne dass diese VLANs explizit auf der Appliance konfiguriert werden müssen.

Punkte, die vor der Konfiguration der Liste der zulässigen VLANs zu beachten sind

Beachten Sie die folgenden Punkte, bevor Sie die Liste der zulässigen VLANs konfigurieren

- In einem Hochverfügbarkeits-Setup wird die Liste der zulässigen VLANs nicht weitergegeben oder synchronisiert. Daher müssen Sie die Liste der zulässigen VLANs auf beiden Knoten konfigurieren.
- Der Datenverkehr eines nativen VLANs kann an die Schnittstellen weitergegeben werden, die keine Mitglieder sind, die das native VLAN in der Liste der zulässigen VLANs angeben.
- Maximal 60 VLAN-Bereiche können als Teil der zulässigen VLAN-Liste für eine Schnittstelle angegeben werden.
- Die NetScaler Appliance unterstützt keine zulässigen VLAN-Liste auf Schnittstellen, die Teil von Linkaggregationskanälen oder redundanten Schnittstellensätzen sind. Weitere Informationen zum redundanten Schnittstellenset finden Sie unter Redundant Interface Set.
- Zulässige VLAN-Liste wird in einer NetScaler Clusterkonfiguration nicht unterstützt.
- Die NetScaler-Appliance unterstützt keine Liste der zulässigen VLANs für Bridge-Gruppen.
- Die NetScaler-Appliance unterstützt keine Liste der zulässigen VLANs für VXLANs.

Liste zulässiger VLANs konfigurieren

So konfigurieren Sie die Liste der zulässigen VLANs mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set interface** <id> **-trunkmode** (ON|OFF) **-trunkAllowedVlan** <int[-int]> …
- **show interface** <id>

So konfigurieren Sie die Liste der zulässigen VLANs mithilfe der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Schnittstellen**, wählen Sie eine Netzwerkschnittstelle aus, klicken Sie auf **Bearbeiten**und stellen Sie dann die folgenden Parameter ein:

- Trunk-Modus
- Zulässiges Trunk-VLAN

Beispielkonfiguration:

In der folgenden Beispielkonfiguration werden VLANS in den Bereichen 100-120, 190-200 und 300-330 als Teil der zulässigen VLAN-Liste für Schnittstelle 1/2 angegeben.

```
> set int 1/2 -trunkmode on -trunkallowedVlan 100-120 190-200 300-330

Done

> sh int 1/2

1)      Interface 1/2 (Gig Ethernet 10/100/1000 MBits) #6
        flags=0xc020

        <ENABLED, UP, UP, AUTONEG OFF, HEARTBEAT, 802.1q, trunkmode>
```



```
11
12          Trunk Allowed Vlans:  100-120 190-200 300-330
13
14  Done
15
16  <!--NeedCopy-->
```

Bridge-Gruppen konfigurieren

May 11, 2023

Wenn Sie zwei oder mehr VLANs zu einer einzigen Domain zusammenführen möchten, ändern Sie in der Regel die VLAN-Konfiguration auf allen Geräten in den separaten Domänen. Das kann eine mühsame Aufgabe sein. Um mehrere VLANs einfacher zu einer einzigen Broadcast-Domäne zusammenzuführen, können Sie Bridge-Gruppen verwenden.

Die Bridge-Gruppen-Funktion funktioniert genauso wie ein VLAN. Mehrere VLANs können an eine einzelne Bridge-Gruppe gebunden werden, und alle VLANs, die an dieselbe Bridge-Gruppe gebunden sind, bilden eine einzige Broadcast-Domäne. Sie können nur Layer-2-VLANs an eine Bridge-Gruppe binden. Für die Layer-3-Funktionalität müssen Sie einer Bridge-Gruppe eine IP-Adresse zuweisen.

Im Layer-2-Modus wird ein Broadcast-Paket, das auf einer Schnittstelle eines bestimmten VLAN empfangen wird, mit anderen VLANs verbunden, die derselben Bridge-Gruppe angehören. Im Fall eines Unicast-Pakets durchsucht die NetScaler-Appliance ihre Bridge-Tabelle nach den erlernten MAC-Adressen aller VLANs, die zu derselben Bridge-Gruppe gehören.

Im Layer-3-Weiterleitungsmodus ist ein IP-Subnetz an eine Bridge-Gruppe gebunden. Der NetScaler akzeptiert eingehende Pakete, die zum gebundenen Subnetz gehören, und leitet die Pakete nur an VLANs weiter, die an die Bridge-Gruppe gebunden sind.

IPv6-Routing kann auf einer konfigurierten Bridge-Gruppe aktiviert werden.

> **Hinweis**
>
> Die Bridge-Gruppen-Funktion und der Bridge-BPDU-Modus können nicht zusammenarbeiten.

Konfigurationsschritte

Gehen Sie wie folgt vor, um eine Bridge-Gruppe zu konfigurieren:

- Layer-2-Modus aktivieren
- Fügen Sie eine Bridgegroup hinzu und binden Sie VLANs an die Bridgegroup

CLI-Verfahren

Um den Layer-2-Modus mithilfe der CLI zu aktivieren: Geben
Sie in der Befehlszeile Folgendes ein:

- **enable ns mode l2**
- **show ns mode**

So fügen Sie eine Bridge-Gruppe hinzu und binden VLANs mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **add bridgegroup** <id> [-**ipv6DynamicRouting** (**ENABLED** | **DISABLED**)]
- **bind bridgegroup** <id> -**vlan** <positive_integer>
- **Brückengruppe anzeigen** <id>

Beispiel:

```
> add bridgegroup 12
 Done
<!--NeedCopy-->
```

Um eine Bridge-Gruppe mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- **RM Bridgegroup** <id>

Beispiel:

```
 rm bridgegroup 12
<!--NeedCopy-->
```

GUI-Prozeduren

So konfigurieren Sie eine Bridge-Gruppe mithilfe der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge-Gruppen**, fügen Sie eine neue Bridge-Gruppe hinzu und binden Sie VLANs an die Bridgegroup, oder bearbeiten Sie eine bestehende Bridge-Gruppe.

Konfigurieren von virtuellen MACs

August 19, 2021

Die primären und sekundären Knoten in einem Hochverfügbarkeitssetup (High Availability, HA) verwenden die schwebende Entität für virtuelle MAC-Adressen. Der primäre Knoten besitzt die schwebenden IP-Adressen (wie MIP, SNIP und VIP) und antwortet auf ARP-Anfragen für diese IP-Adressen mit

einer eigenen MAC-Adresse. Daher wird die ARP-Tabelle eines externen Geräts, z. B. eines Upstream-Routers, mit der schwebenden IP-Adresse und der MAC-Adresse des primären Knotens aktualisiert.

Wenn ein Failover auftritt, übernimmt der sekundäre Knoten als neuer primärer Knoten. Der frühere sekundäre Knoten verwendet Gratuitous ARP (GARP), um die schwebenden IP-Adressen anzukündigen, die er vom alten Primärknoten gelernt hatte. Die MAC-Adresse, die der neue primäre Knoten angibt, ist die MAC-Adresse seiner eigenen Netzwerkschnittstelle. Einige Geräte (einige Router) akzeptieren diese GARP-Nachrichten nicht. Daher behalten diese externen Geräte die IP-Adressen-zu-MAC-Adressenzuordnung, die der alte primäre Knoten angekündigt hatte. Dies kann dazu führen, dass eine GSLB-Site heruntergeht.

Daher müssen Sie einen virtuellen MAC auf beiden Knoten eines HA-Paares konfigurieren. Dies bedeutet, dass beide Knoten identische MAC-Adressen haben. Wenn ein Failover auftritt, bleibt die MAC-Adresse des sekundären Knotens unverändert, und die ARP-Tabellen auf den externen Geräten müssen nicht aktualisiert werden.

Informationen zu den Verfahren zum Konfigurieren eines virtuellen MAC finden Sie unter Konfigurieren virtueller MAC-Adressen.

Verbindungsaggregation konfigurieren

May 11, 2023

Die Linkaggregation kombiniert Daten, die von mehreren Ports kommen, in einer einzigen Hochgeschwindigkeitsverbindung. Die Konfiguration der Link-Aggregation erhöht die Kapazität und Verfügbarkeit des Kommunikationskanals zwischen der NetScaler-Appliance und anderen angeschlossenen Geräten. Eine aggregierte Verbindung wird auch als “Kanal” bezeichnet. Sie können die Kanäle manuell konfigurieren oder das Link Aggregation Control Protocol (LACP) verwenden. Sie können LACP nicht auf einen manuell konfigurierten Kanal anwenden, und Sie können auch keinen von LACP erstellten Kanal manuell konfigurieren.

Wenn eine Netzwerkschnittstelle an einen Kanal gebunden ist, haben die Kanalparameter Vorrang vor den Netzwerkschnittstellenparametern. (Das heißt, die Netzwerkschnittstellenparameter werden ignoriert.) Eine Netzwerkschnittstelle kann nur an einen Kanal gebunden werden.

Wenn eine Netzwerkschnittstelle an einen Kanal gebunden ist, löscht sie ihre VLAN-Konfiguration. Wenn Netzwerkschnittstellen entweder manuell oder durch LACP an einen Kanal gebunden sind, werden sie aus den VLANs entfernt, zu denen sie ursprünglich gehörten, und dem Standard-VLAN hinzugefügt. Sie können den Kanal jedoch wieder an das alte oder an ein neues VLAN binden. Wenn Sie beispielsweise die Netzwerkschnittstellen 1/2 und 1/3 an ein VLAN mit der ID 2 binden und sie dann an einen Kanal LA/1 binden, werden die Netzwerkschnittstellen in das Standard-VLAN verschoben, Sie können sie jedoch wieder an VLAN 2 binden.

Manuelles Konfigurieren der Link-Aggregation

Wenn Sie einen Link-Aggregationskanal erstellen, ist sein Status DOWN, bis Sie eine aktive Schnittstelle daran binden. Du kannst einen Kanal jederzeit ändern. Sie können Kanäle entfernen oder sie aktivieren/deaktivieren.

CLI-Verfahren

So erstellen Sie mit der CLI einen Link-Aggregationskanal:

Geben Sie in der Befehlszeile Folgendes ein:

- add channel <id> [-ifnum \<interfaceName> ...] [-state (ENABLED | DISABLED)] [-speed \<speed>] [-flowControl \<flowControl>] [-haMonitor (ON | OFF)][-tagall (ON | OFF)] [-ifAlias \<string>] [-throughput \<positive_integer>] [-bandwidthHigh \<positive_integer> [-bandwidthNormal \<positive_integer>]]
- show channel

Beispiel:

```
> add channel LA/1 -ifnum 1/8
Done
<!--NeedCopy-->
```

So binden Sie eine Schnittstelle mit der Befehlszeilenschnittstelle an einen vorhandenen Verbindungsaggregationskanal oder lösen Sie die Bindung von einer Schnittstelle aus:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- bind channel <id> <interfaceName>
- unbind channel <id> <interfaceName>

Beispiel:

```
bind channel LA/1 1/8
<!--NeedCopy-->
```

So ändern Sie einen Link-Aggregationskanal mithilfe der CLI:

Geben Sie in der Befehlszeile den Befehl
set channel, die Kanal-ID und die zu ändernden Parameter mit ihren neuen Werten ein.

Um einen Link-Aggregationskanal mit der CLI zu entfernen:

Wichtig: Wenn ein Kanal entfernt wird, induzieren die daran gebundenen Netzwerkschnittstellen Netzwerkschleifen, die die Netzwerkleistung beeinträchtigen. Sie müssen die Netzwerkschnittstellen deaktivieren, bevor Sie den Kanal entfernen.

Geben Sie in der Befehlszeile Folgendes ein:

- rm channel <id>

Beispiel:

```
> rm channel LA/1
 Done
<!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie einen Link-Aggregationskanal mithilfe der GUI:

Navigieren Sie zu System > Netzwerk > Kanäle, fügen Sie einen neuen Kanal hinzu oder bearbeiten Sie einen vorhandenen Kanal.

Um einen Link-Aggregationskanal mithilfe der GUI zu entfernen:

> **Wichtig:**
>
> Wenn ein Kanal entfernt wird, induzieren die daran gebundenen Netzwerkschnittstellen Netzwerkschleifen, die die Netzwerkleistung verringern. Sie müssen die Netzwerkschnittstellen deaktivieren, bevor Sie den Kanal entfernen.

Navigieren Sie zu System > Netzwerk > Kanäle, wählen Sie den Kanal aus, den Sie entfernen möchten, und klicken Sie auf Löschen.

Konfiguration der Link-Aggregation mithilfe des Link Aggregation Control Protocol

Das Link Aggregation Control Protocol (LACP) ermöglicht Netzwerkgeräten den Austausch von Link-Aggregationsinformationen durch den Austausch von LACP-Dateneinheiten (LACPDUs). Daher können Sie LACP nicht auf Netzwerkschnittstellen aktivieren, die Mitglieder eines Kanals sind, den Sie manuell erstellt haben.

Wenn Sie LACP zur Konfiguration der Link-Aggregation verwenden, verwenden Sie andere Befehle und Parameter zum Ändern von Link-Aggregationskanälen als zum Erstellen von Link-Aggregationskanälen. Um einen Kanal zu entfernen, müssen Sie LACP auf allen Schnittstellen deaktivieren, die Teil des Kanals sind.

Hinweis: In einer Hochverfügbarkeitskonfiguration werden LACP-Konfigurationen weder propagiert noch synchronisiert.

Konfiguration der LACP-Systempriorität

Die LACP-Systempriorität bestimmt, welches Peer-Gerät eines LACP-LA-Kanals die Kontrolle über den LA-Kanal haben kann. Diese Nummer wird global auf alle LACP-Kanäle der Appliance angewendet. Je geringer der Wert, desto höher die Priorität.

So konfigurieren Sie die LACP-Systempriorität mithilfe der CLI:

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Priorität für eine eigenständige Appliance festzulegen und die Konfiguration zu überprüfen:

- set lacp -sysPriority <positive_integer>
- show lacp

Beispiel:

```
set lacp -sysPriority 50
<!--NeedCopy-->
```

Um die Priorität für einen bestimmten Clusterknoten festzulegen, melden Sie sich an der Cluster-IP-Adresse an und geben Sie an der Befehlszeile die folgenden Befehle ein:

- set lacp -sysPriority <positive_integer> -ownerNode <positive_integer>
- show lacp

Beispiel:

```
set lacp -sysPriority 50 -ownerNode 2
<!--NeedCopy-->
```

So konfigurieren Sie die LACP-Systempriorität mithilfe der GUI:

1. Navigieren Sie zu System > Netzwerk > Schnittstellen und wählen Sie in der Aktionsliste die Option Set LACP aus.
2. Geben Sie die Systempriorität und den Eigentümerknoten an (gilt nur für ein Cluster-Setup).

Link-Aggregationskanäle erstellen

Um einen Link-Aggregationskanal mithilfe von LACP zu erstellen, müssen Sie LACP aktivieren und auf jeder Schnittstelle, die Sie Teil des Kanals sein möchten, denselben LACP-Schlüssel angeben. Wenn Sie beispielsweise LACP aktivieren und den LACP-Schlüssel an den Schnittstellen 1/1 und 1/2 auf 3 setzen, wird ein Link-Aggregationskanal LA/3 erstellt, an den die Schnittstellen 1/1 und 1/2 automatisch gebunden werden.

Hinweis:

- Wenn Sie LACP auf einer Netzwerkschnittstelle aktivieren, müssen Sie den LACP-Schlüssel angeben.
- Standardmäßig ist LACP auf allen Netzwerkschnittstellen deaktiviert.

Um einen LACP-Kanal mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- set interface <id> [-lacpMode \<lacpMode>] [-lacpKey\<positive_integer>] [-lacpPriority \<positive_integer>] [-lacpTimeout (LONG | SHORT)]
- show interface [\<id>]

So erstellen Sie einen LACP-Kanal mit der GUI:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Netzwerkschnittstelle und stellen Sie die Parameter ein.

Link-Aggregationskanäle ändern

Nachdem Sie einen LACP-Kanal erstellt haben, indem Sie Schnittstellen angegeben haben, können Sie die Eigenschaften des Kanals ändern.

So ändern Sie einen LACP-Kanal mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- set channel <id> [-ifnum \<interfaceName> ...] [-state (ENABLED | DISABLED)] [-speed \<speed>] [-flowControl \<flowControl>] [-haMonitor (ON | OFF)] [-ifAlias \<string>] [-throughput \<positive_integer>] [-tagall (ON | OFF)] [-bandwidthHigh \<positive_integer> [-bandwidthNormal \<positive_integer>]]
- show channel

Beispiel:

```
> set channel LA/3 -state ENABLED -speed 10000
 Done
<!--NeedCopy-->
```

Um einen LACP-Kanal mithilfe der GUI zu modifizieren:

Navigieren Sie zu System > Netzwerk > Kanäle und ändern Sie einen vorhandenen LACP-Kanal.

Einen Link-Aggregationskanal entfernen

Um einen Link-Aggregationskanal zu entfernen, der mithilfe von LACP erstellt wurde, müssen Sie LACP auf allen Schnittstellen deaktivieren, die Teil des Kanals sind.

Um einen LACP-Kanal mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- set interface <id> -lacpMode Disable
- show interface [\<id>]

Um einen LACP-Kanal mithilfe der GUI zu entfernen:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Netzwerkschnittstelle und deaktivieren Sie die Option LACP aktivieren.

Link-Redundanz mithilfe von LACP-Kanälen

Link-Redundanz unter Verwendung von LACP-Kanälen ermöglicht es dem NetScaler, einen LACP-Kanal in logische Unterkanäle zu unterteilen, wobei ein Unterkanal aktiv ist und die anderen im Standby-Modus sind. Wenn der aktive Unterkanal einen Mindestdurchsatzschwellenwert nicht erreicht, wird einer der Standby-Unterkanäle aktiv und übernimmt die Leitung.

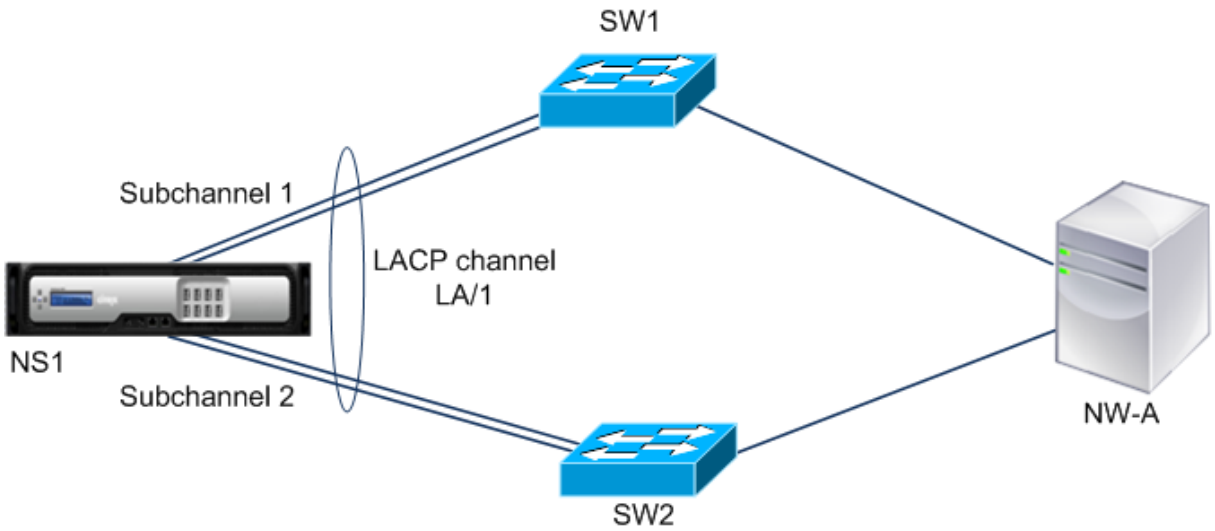
Ein Unterkanal wird aus Links erstellt, die Teil des LACP-Kanals sind und mit einem bestimmten Gerät verbunden sind. Beispielsweise erstellt der ADC für einen LACP-Kanal mit vier Schnittstellen auf einem NetScaler, wobei zwei der Schnittstellen mit Gerät A und die anderen beiden mit Gerät B verbunden sind, zwei logische Unterkanäle, einen Unterkanal mit zwei Verbindungen zu Gerät A und einen weiteren Unterkanal mit zwei Verbindungen zu Gerät B.

Um die Verbindungsredundanz für einen LACP-Kanal zu konfigurieren, legen Sie den Parameter lrMinThroughput fest, der den minimalen Durchsatzschwellenwert (in Mbit/s) angibt, den der aktive Subkanal erreichen muss. Wenn Sie diesen Parameter festlegen, werden die Unterkanäle automatisch erstellt. Wenn der maximal unterstützte Durchsatz des aktiven Kanals unter den Wert lrMinThroughput fällt, erfolgt ein Link-Failover und ein Standby-Unterkanal wird aktiv.

Wenn Sie den Parameter lrMinThroughput eines LACP-Kanals deaktivieren oder den Wert auf Null setzen, wird die Verbindungsredundanz für diesen Kanal deaktiviert. Dies ist die Standardeinstellung.

Beispiel

Stellen Sie sich ein Beispiel für eine Link-Redundanz vor, die zwischen NetScaler NS1 und den Switches SW1 und SW2 konfiguriert ist.



NS1 ist über SW1 und SW2 mit dem Netzwerkgerät NW-A verbunden.
Auf NS1 wird der LACP-Kanal LA/1 aus den Schnittstellen 1/1, 1/2, 1/3 und 1/4 erstellt. Die Schnittstellen 1/1 und 1/2 von NS1 sind mit SW1 verbunden, und die Schnittstellen 1/3 und 1/4 sind mit SW2 verbunden. Jeder der vier Links unterstützt einen maximalen Durchsatz von 1000 Mbit/s.
Wenn der Parameter lrMinThroughput auf einen bestimmten Wert gesetzt ist (z. B. 2000), erstellt NS1 zwei logische Unterkanäle aus LA/1, einen Unterkanal (z. B. Unterkanal 1) über die Schnittstellen 1/1 und 1/2 (verbunden mit SW1) und der andere Unterkanal (Unterkanal 2) über die Schnittstellen 1/3 und 1/4 (verbunden mit SW2).

NS1 wendet einen Algorithmus an, um einen Unterkanal (z. B. Unterkanal 1) aktiv zu machen und den anderen in den Standby-Modus zu versetzen. NS1 und Netzwerkgerät NW-A sind nur über den aktiven Unterkanal miteinander erreichbar.

Angenommen, Subkanal 1 ist aktiv und sein maximaler unterstützter Durchsatz fällt unter den Wert lrMinThroughput (z. B. fällt eine seiner Verbindungen aus und der maximal unterstützte Durchsatz fällt auf 1000 Mbit/s). Subchannel 2 wird aktiv und übernimmt die Leitung.

Link-Redundanz mithilfe von LACP-Kanälen in einem Hochverfügbarkeits-Setup

Wenn Sie in einer Hochverfügbarkeitskonfiguration (HA) die auf Durchsatz (Durchsatzparameter) basierende HA-Failover- und Link-Redundanz (LRMinThroughput-Parameter) auf einem LACP-Kanal konfigurieren möchten, müssen Sie den Durchsatzparameter auf einen Wert setzen, der kleiner oder gleich dem des LRMinThroughput-Parameters ist.

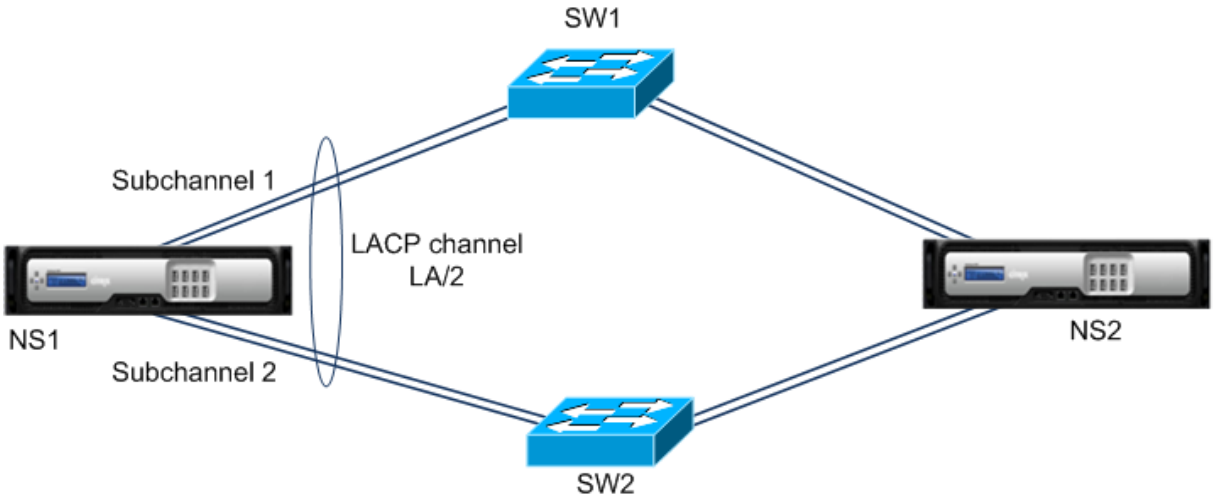
Der maximal unterstützte Durchsatz eines LACP-Kanals wird als der maximal unterstützte Durchsatz des aktiven Subkanals berechnet.

Wenn der Durchsatzparameterwert gleich oder kleiner als der Wert des lrminThroughput-Parameters ist, erfolgt ein HA-Failover, wenn die beiden folgenden Bedingungen gleichzeitig vorliegen:

- Keiner der maximal unterstützten Durchsätze der Subkanäle entspricht dem Wert des LRMinThroughput-Parameters.
- Der maximal unterstützte Durchsatz des LACP-Kanals entspricht nicht dem Wert des Durchsatzparameters

Stellen Sie sich ein Beispiel für ein HA-Setup mit NetScalers NS1 und NS2 mit den Switches SW1 und SW2 vor. NS1 ist über SW1 und SW2 mit NS2 verbunden.

Auf NS1 wird der LACP-Kanal LA/1 aus den Schnittstellen 1/1, 1/2, 1/3 und 1/4 erstellt. Die Schnittstellen 1/1 und 1/2 von NS1 sind mit SW1 verbunden, und die Schnittstellen 1/3 und 1/4 sind mit SW2 verbunden. Jeder der vier Links unterstützt einen maximalen Durchsatz von 1000 Mbit/s.



In diesem Beispiel sind die LACP-Parametereinstellungen aufgeführt:

Parameter	Wert
Durchsatz	2000
lrm im Durchsatz	2000

NS1 bildet zwei Unterkanäle aus LA/1, wobei ein Unterkanal (z. B. Unterkanal 1) die Schnittstellen 1/1 und 1/2 (mit SW1 verbunden) und der andere Unterkanal (Unterkanal 2) die Schnittstellen 1/3 und 1/4 (verbunden mit SW2) verwendet. Jeder der beiden Subkanäle unterstützt einen maximalen Durchsatz von 2000 Mbit/s. Unter Anwendung eines Algorithmus macht NS1 einen Unterkanal (sagen wir Unterkanal 1) aktiv und den anderen in den Standby-Modus.

Angenommen, Subkanal 1 ist aktiv und sein maximaler unterstützter Durchsatz fällt unter den Wert lrMinThroughput (z. B. fällt eine seiner Verbindungen aus und der maximal unterstützte Durchsatz fällt auf 1000 Mbit/s). Subchannel 2 wird aktiv und übernimmt die Leitung. HA-Failover findet nicht statt, da der maximal unterstützte Durchsatz des LACP-Kanals nicht unter dem Wert des Durchsatzparameters liegt:

Maximaler unterstützter Durchsatz des LACP-Kanals = Maximaler unterstützter Durchsatz des aktiven Kanals = Maximaler unterstützter Durchsatz von Subkanal 2 = 2000 Mbit/s

Wenn der maximal unterstützte Durchsatz von Subkanal 2 ebenfalls unter den lrminThroughput-Wert fällt (z. B. wenn eine seiner Verbindungen ausfällt und der maximal unterstützte Durchsatz auf 1000 Mbit/s fällt), erfolgt ein HA-Failover, da der maximal unterstützte Durchsatz des LACP-Kanals dann unter dem Durchsatzparameterwert liegt:

Konfigurieren Sie die Link-Redundanz mithilfe von LACP-Kanälen

So konfigurieren Sie die Link-Redundanz für einen LACP-Kanal mithilfe der CLI:

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den Kanal zu konfigurieren und die Konfiguration zu überprüfen:

- **set channel** <id> -lrMinThroughput <positive_integer>
- **show channel**

Beispiel:

```
> set channel la/1 - lrMinThroughput 2000
Done
> set channel la/2 - throughput 2000 - lrMinThroughput 2000
Done
<!--NeedCopy-->
```

So konfigurieren Sie die Link-Redundanz für einen LACP-Kanal mithilfe der GUI

1. Navigieren Sie zu System > Netzwerk > Kanäle.
2. Wählen Sie im Detailbereich einen LACP-Kanal aus, für den Sie die Link-Redundanz konfigurieren möchten, und klicken Sie dann auf Bearbeiten.
3. Stellen Sie im Dialogfeld „LACP-Kanal konfigurieren“ den Parameter lrminThroughput ein.
4. Klicken Sie auf Schließen.

Redundantes Schnittstellenset

June 2, 2023

> **Hinweis:**
>
> Die Link-Redundanzkonfiguration wird auf einer NetScaler VPX-Instanz, die auf einer NetScaler SDX-Appliance gehostet wird, nicht unterstützt.

Ein redundanter Schnittstellensatz ist ein Satz von Schnittstellen, bei denen eine der Schnittstellen aktiv ist und die übrigen im Standby-Modus sind. Wenn die aktive Schnittstelle ausfällt, übernimmt eine der Standby-Schnittstellen die Funktion und wird aktiv.

Im Folgenden sind die Hauptvorteile der Verwendung redundanter Schnittstellensätze aufgeführt:

- Ein redundanter Schnittstellensatz gewährleistet die Zuverlässigkeit der Verbindung zwischen der NetScaler-Appliance und einem Peer-Gerät, indem Backup-Verbindungen zwischen ihnen bereitgestellt werden.

- Im Gegensatz zur Link-Redundanz mit LACP ist für einen redundanten Schnittstellensatz keine Konfiguration auf dem Peer-Gerät erforderlich. Für das Peer-Gerät erscheint der redundante Schnittstellensatz als einzelne Schnittstellen und nicht als Satz oder Sammlung.
- In einer Hochverfügbarkeitskonfiguration (HA) können redundante Schnittstellensätze die Anzahl der HA-Failover minimieren.

> **Hinweis**
>
> Redundant Interface Set war früher als "NIC-Bundling" bekannt, als es erstmals in Version 10.5 eingeführt wurde.

So funktioniert ein redundanter Schnittstellensatz

Bei einem redundanten Schnittstellensatz leitet die NetScaler-Appliance eine MAC-Adresse auf der Grundlage eines internen Algorithmus ab und weist sie dem redundanten Schnittstellensatz zu. Diese MAC-Adresse wird von allen Mitgliedsschnittstellen gemeinsam genutzt und jeweils nur von der aktiven Schnittstelle verwendet. Die aktive Schnittstelle sendet GARP-Nachrichten, die die dem redundanten Schnittstellensatz zugewiesene MAC-Adresse und nicht die eigene physische MAC-Adresse der Schnittstelle enthalten. Wenn die aktuelle aktive Schnittstelle ausfällt und von einer anderen Schnittstelle übernommen wird, sendet die neue aktive Schnittstelle GARP-Nachrichten. Das Peer-Gerät aktualisiert seine Weiterleitungstabelle mit den neuen aktiven Schnittstelleninformationen. Die Standby-Schnittstellen senden keine GARP-Nachrichten. Die Standby-Schnittstellen senden keine Pakete und sie verwerfen alle Pakete, die sie empfangen.

In einem redundanten Schnittstellensatz basiert die Auswahl der Mitgliedsschnittstelle als aktiv auf einem der folgenden Faktoren:

- **Redundante Schnittstellenpriorität**. Dies ist ein Parameter einer Schnittstelle und definiert die Priorität der Schnittstelle in einem redundanten Schnittstellensatz für die Auswahl des aktiven Mitglieds. Dieser Parameter gibt eine positive Ganzzahl an. Senken Sie den Wert, um die Priorität der aktiven Mitgliederauswahl zu erhöhen. Die Mitgliederschnittstelle mit der höchsten Priorität (niedrigster Wert) wird als aktive Schnittstelle des redundanten Schnittstellensatzes ausgewählt.
- **Verbindliche Reihenfolge der Mitgliederschnittstellen**. Wenn alle Mitgliedsschnittstellen dieselbe redundante Schnittstellenpriorität haben, wird die Mitgliedsschnittstelle, die zuerst an den redundanten Schnittstellensatz gebunden wurde, als aktive Schnittstelle des redundanten Schnittstellensatzes ausgewählt.

In einem redundanten Schnittstellensatz wird die aktive Schnittstellenauswahl in einem der folgenden Ereignisse ausgelöst:

- Wenn die aktuelle aktive Schnittstelle ausfällt oder Sie sie deaktivieren.
- Wenn Sie die Priorität einer Standby-Schnittstelle auf einen Wert setzen, der niedriger ist als der der aktuellen aktiven Schnittstelle. Die Standby-Schnittstelle übernimmt die Funktion der

aktiven Schnittstelle.
- Wenn Sie eine Schnittstelle binden, deren Priorität niedriger ist als die der aktuellen aktiven Schnittstelle. Die neu gebundene Schnittstelle übernimmt die Funktion der aktiven Schnittstelle.

Punkte, die bei der Konfiguration redundanter Schnittstellensätze zu beachten sind

Beachten Sie die folgenden Punkte, bevor Sie einen redundanten Schnittstellensatz konfigurieren:

- In einer eigenständigen Appliance oder einer Appliance in einem Hochverfügbarkeits-Setup wird ein verbindungsredundanter Satz in der LR/X-Notation angegeben, wobei X zwischen 1 und 4 liegen kann. Zum Beispiel LR/1.
- In einer Hochverfügbarkeitskonfiguration werden redundante Schnittstellensatzkonfigurationen nicht an den sekundären Knoten weitergegeben oder synchronisiert.
- Sie können maximal vier redundante Schnittstellensätze auf einer NetScaler-Appliance konfigurieren.
- Sie können maximal 16 Schnittstellen an einen redundanten Schnittstellensatz binden.
- Mitgliedsschnittstellen eines redundanten Schnittstellensatzes können nicht an einen anderen redundanten Schnittstellensatz gebunden werden.
- Mitgliedsschnittstellen eines redundanten Schnittstellensatzes können nicht an einen Link Aggregate (LA) -Kanal gebunden werden.
- LA-Kanäle können nicht an einen redundanten Schnittstellensatz gebunden werden.
- Redundante Schnittstellensätze können nicht an einen LA-Kanal gebunden werden.
- In einem Cluster-Setup:
  - Redundante Schnittstellensätze können nicht an eine Cluster-Link-Aggregation gebunden werden.
  - Ein verbindungsredundanter Satz wird in der N/LR/X-Notation angegeben (z. B. 1/LR/3). Wobei:
    N die ID des Clusterknotens ist, auf dem der redundante Schnittstellensatz erstellt werden soll.
    X ist ein link-redundanter Set-Identifier auf einem Clusterknoten. X kann im Bereich 1—4 liegen.
  - Eine Cluster-Link-Aggregation kann nicht an einen redundanten Schnittstellensatz gebunden werden.
  - Ein redundanter Schnittstellensatz kann nur die Schnittstellen des Knotens enthalten, zu dem der redundante Schnittstellensatz gehört.
  - Eine bestehende Konfiguration eines elink-Redundanzsatzes auf einer eigenständigen Appliance wechselt automatisch zur Cluster-Notation (N/LR/X), nachdem die Appliance zu einem Cluster-Setup hinzugefügt wurde.

Konfigurationsschritte

Die Konfiguration eines redundanten Schnittstellensatzes auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- **Erstellen Sie einen redundanten Schnittstellensatz**. Verwenden Sie die Channel-Befehlsoperation, um einen redundanten Schnittstellensatz zu erstellen.

  In einer eigenständigen Appliance oder einer Appliance in einem Hochverfügbarkeits-Setup wird ein verbindungsredundanter Satz in der LR/X-Notation angegeben, wobei X zwischen 1 und 4 liegen kann. Zum Beispiel LR/1.

  In einem Cluster-Setup wird ein verbindungsredundanter Satz in N/LR/X angegeben (z. B. 1/LR/3), wobei: N die ID des Clusterknotens ist, auf dem der redundante Schnittstellensatz erstellt werden soll; X die ID des verbindungsredundanten Satzes auf einem Clusterknoten ist. X kann im Bereich 1—4 liegen.

- **Binden Sie Schnittstellen an den redundanten Schnittstellensatz**. Ordnen Sie die gewünschten Schnittstellen dem redundanten Schnittstellensatz zu. Eine Schnittstelle kann nicht Teil mehrerer redundanter Schnittstellensätze sein.

- **(Optional) Legen Sie eine redundante Schnittstellenpriorität für die Mitgliederschnittstelle**fest. Verwenden Sie den Schnittstellenbefehl, um die Priorität der redundanten Schnittstelle auf einer gewünschten Mitgliedsschnittstelle eines redundanten Schnittstellensatzes festzulegen.

Um einen redundanten Schnittstellensatz mit der CLI zu erstellen:

An der Eingabeaufforderung:

- Kanal hinzufügen <ID>
- Kanal einblenden <ID>

Um Schnittstellen mit der CLI an einen redundanten Schnittstellensatz zu binden:

An der Eingabeaufforderung:

- Kanal binden <ID><ifnum>
- Kanal einblenden <ID>

So legen Sie mithilfe der CLI eine redundante Schnittstellenpriorität für eine Schnittstelle fest:

An der Eingabeaufforderung:

- Schnittstelle setzen <ID>-lrsetpriority <positive_integer>
- Oberfläche einblenden <ID>

Beispielkonfiguration 1:

Im folgenden Beispiel wird ein redundanter Schnittstellensatz LR/1 erstellt, und die Schnittstellen 1/1, 1/2, 1/3 und 1/4 sind an LR/1 gebunden. Die redundante Schnittstellenpriorität ist für all diese Mitgliedsschnittstellen auf einen Standardwert von 1024 festgelegt. Die Ausgabe des Befehls show channel zeigt an, dass die Schnittstelle 1/1 die aktuelle aktive Schnittstelle für den redundanten Schnittstellensatz lr/1 ist.

```
> add channel lr/1
 Done
> bind channel lr/1 1/1 1/2 1/3 1/4
 Done
> show channel
1)    Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Active Member
                1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
Done
<!--NeedCopy-->
```

Beispielkonfiguration 2:

Im folgenden Beispiel wird eine redundante Schnittstellenpriorität der Mitgliedsschnittstelle 1/4 auf 100 gesetzt, was niedriger ist als die eingestellte redundante Schnittstellenpriorität aller anderen Mitgliedsschnittstellen von LR/1.

Die Ausgabe des Befehls show channel zeigt an, dass die Schnittstelle 1/4 die aktuelle aktive Schnittstelle für den redundanten Schnittstellensatz LR/1 ist.

```
> set interface 1/4 -lrsetPriority 100
Done
> show channel
```



```
1)      Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Active Member
Done
<!--NeedCopy-->
```

Beispielkonfiguration 3:

Stellen Sie sich ein Cluster-Setup mit vier Knoten N1, N2, N3 und N4 vor. In diesem Beispiel wird der redundante Schnittstellensatz 1/LR/3 auf dem Knoten N1 erstellt, und die Schnittstellen 1/1/1, 1/1/2 und 1/1/3 sind daran gebunden. Die redundante Schnittstellenpriorität ist für all diese Mitgliedsschnittstellen auf einen Standardwert von 1024 festgelegt. Die Ausgabe des Befehls show channel zeigt an, dass Schnittstelle 1/1/1 die aktuelle aktive Schnittstelle für redundante Schnittstellensatz 1/LR/3 ist.

```
    > add channel 1/LR/3

    Done
    > bind channel 1/LR/3 1/1/1 1/1/2 1/1/3

    Done
    > show channel
    1)    Interface 1/LR/3 (Link Redundant) #14
            flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON,
               802.1q>
            MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0
               h00m00s
            Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
            throughput 0
```



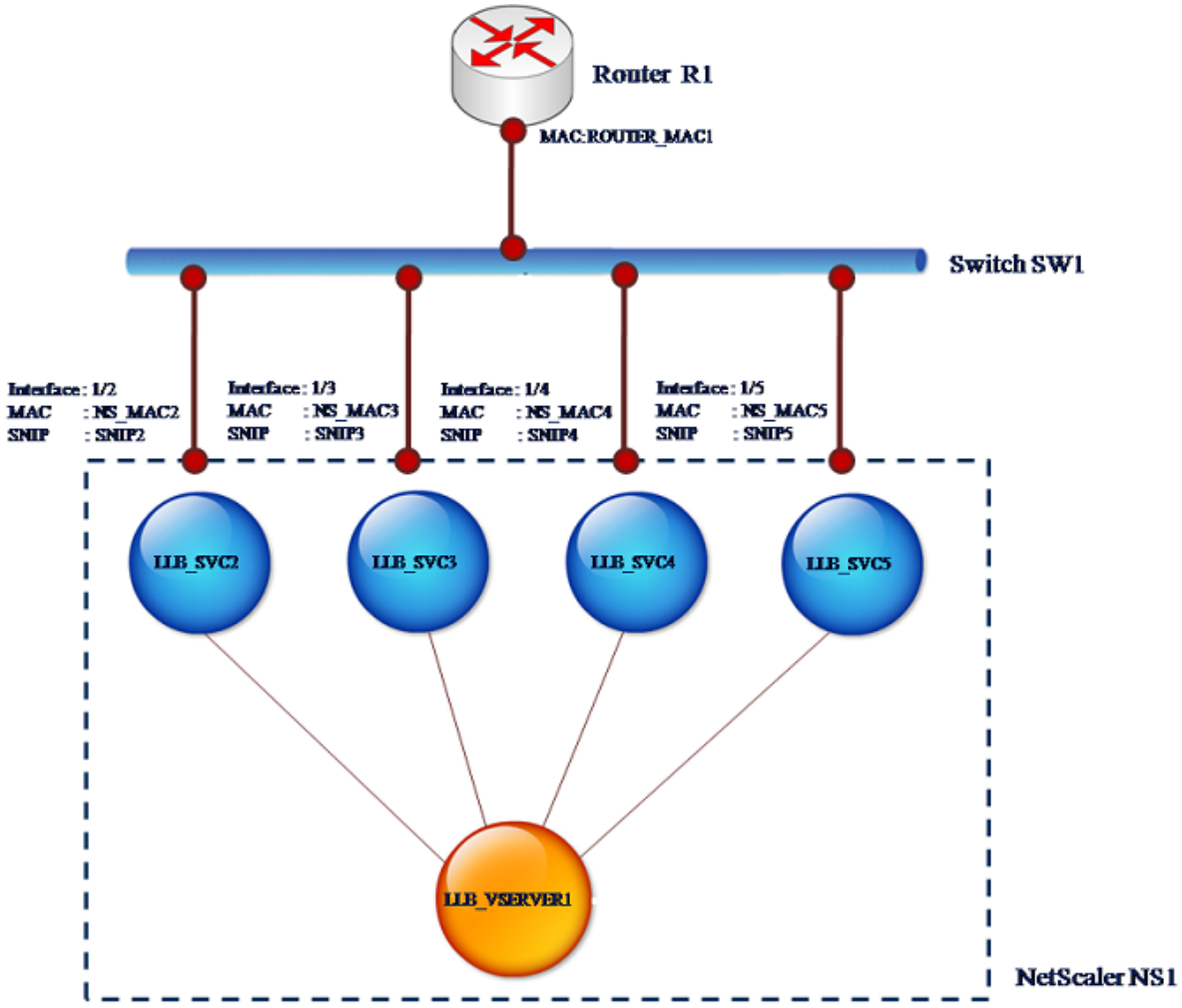
```
            Actual: throughput 1000
            LLDP Mode: NONE,
            RX: Pkts(66) Bytes(4406) Errs(0) Drops(82) Stalls(0)
            TX: Pkts(55) Bytes(2626) Errs(0) Drops(145) Stalls(0)
            NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
                (0)
            Bandwidth thresholds are not set.

            1/1/1: UTP-1000-FULL-OFF UP  0h14m06s LR Active Member
            1/1/2: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
            1/1/3: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member

    Done
<!--NeedCopy-->
```

SNIP-Adresse an eine Schnittstelle binden

May 11, 2023

Sie können jetzt eine NetScaler-eigene SNIP-Adresse an eine Schnittstelle binden, ohne Layer-3-VLANs zu verwenden. Alle Pakete, die sich auf die SNIP-Adresse beziehen, werden nur über die gebundene Schnittstelle übertragen.

Diese Funktion kann in einem Szenario nützlich sein, in dem der Upstream-Switch keine Link-Aggregationskanäle unterstützt und Sie möchten, dass die NetScaler-Appliance den von einem Server stammenden Datenverkehr über die vier Links zum Upstream-Switch lastenverteilt, wie in der folgenden Abbildung dargestellt.



In den folgenden Tabellen werden die Beispieleinstellungen für das Szenario beschrieben:

Entität	Name	Wert
SNIP-Adressen auf NS1	SNIP2 (nur zu Referenzzwecken)	10.10.10.2
	SNIP3 (nur zu Referenzzwecken)	10.10.10.3
	SNIP4 (nur zu Referenzzwecken)	10.10.10.4
	SNIP5 (nur zu Referenzzwecken)	10.10.10.5
Virtueller LLB-Server auf NS1	LLB_VSERVER1	-

Entität	Name	Wert
Transparenter Monitor auf NS1	TRANS_MON	-
LLB-Dienste auf NS1	LLB_SVC2	10.10.10.240
	LLB_SVC3	10.10.10.120
	LLB_SVC4	10.10.10.60
	LLB_SVC5	10.10.10.30
MAC-Adresse der Schnittstelle 1/2 auf NS1	NS_MAC_2 (nur zu Referenzzwecken)	00:e0:ed:0f:bc:e0
MAC-Adresse der Schnittstelle 1/3 auf NS1	NS_MAC_3 (nur zu Referenzzwecken)	00:e0:ed:0f:bc:df
MAC-Adresse der Schnittstelle 1/4 auf NS1	NS_MAC_4 (nur zu Referenzzwecken)	00:e0:ed:0f:bc:de
MAC-Adresse der Schnittstelle 1/5 auf NS1	NS_MAC_5 (nur zu Referenzzwecken)	00:e0:ed:1c:89:53
IP-Adresse des Routers R1	router_IP (nur zu Referenzzwecken)	10.10.10.1
MAC-Adresse der Schnittstelle von R1	ROUTER_MAC1 (nur zu Referenzzwecken)	00:21:a1:2d:db:cc

Um die Beispieleinstellungen zu konfigurieren:

1. Fügen Sie vier verschiedene SNIPs in verschiedenen Subnetzbereichen hinzu. Dies ist für ARP auf vier verschiedenen Links gelöst werden. Weitere Informationen zum Erstellen einer SNIP-Adresse finden Sie unter Konfigurieren von Subnetz-IP-Adressen (SNIPs).

   CLI-Beispiel:

```
> add ns ip 10.10.10.2 255.255.255.0 -type SNIP
 Done
> add ns ip 10.10.10.3 255.255.255.128 - type SNIP
Done
> add ns ip 10.10.10.4 255.255.255.192 - type SNIP
Done
> add ns ip 10.10.10.5 255.255.255.224 - type SNIP
Done
<!--NeedCopy-->
```


2. Fügen Sie vier verschiedene Dummy-Dienste in den hinzugefügten SNIP-Subnetzen hinzu. Damit soll sichergestellt werden, dass der Datenverkehr mit Quell-IP als einer der vier konfigurierten SNIPs gesendet wird. Weitere Informationen zum Erstellen eines Dienstes finden Sie unter Einrichten des grundlegenden Lastenausgleichs.

   CLI-Beispiel:

```
> add service LLB_SVC2 10.10.10.240 any *
 Done
> add service LLB_SVC3 10.10.10.120 any *
 Done
> add service LLB_SVC4 10.10.10.60 any *
 Done
> add service LLB_SVC5 10.10.10.30 any *
 Done
<!--NeedCopy-->
```

3. Fügen Sie einen transparenten Ping-Monitor zur Überwachung des Gateway hinzu. Binden Sie den Monitor an jeden der konfigurierten Dummy-Dienste. Dies ist, um den Zustand der Dienste als UP zu machen. Weitere Informationen zum Erstellen eines transparenten Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing-Setup.

   CLI-Beispiel:

```
> add monitor TRANS_MON ping -destIP 10.10.10.1 -transparent YES
 Done
> bind monitor TRANS_MON LLB_SVC2
 Done
> bind monitor TRANS_MON LLB_SVC3
 Done
> bind monitor TRANS_MON LLB_SVC4
 Done
> bind monitor TRANS_MON LLB_SVC5
 Done
<!--NeedCopy-->
```

4. Fügen Sie einen Link Load Balancing (LLB) virtuellen Server hinzu und binden Sie die Dummy-Dienste an ihn. Weitere Informationen zum Erstellen eines virtuellen LLB-Servers finden Sie unter Konfigurieren eines grundlegenden LLB-Setups.

   CLI-Beispiel:

```
> add lb vserver LLB_VSERVER1 any
 Done
> set lb vserver LLB_VSERVER1 -lbmethod ROUNDROBIN
 Done
```



```
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
<!--NeedCopy-->
```

5. Fügen Sie den virtuellen LLB-Server als Standard-LLB-Route hinzu. Weitere Informationen zum Erstellen einer LLB-Route finden Sie unter Konfigurieren eines grundlegenden LLB-Setups.

   CLI-Beispiel:

```
> add lb route 0.0.0.0 0.0.0.0  LLB_VSERVER1
 Done
<!--NeedCopy-->
```

6. Fügen Sie für jeden Dummy-Dienst einen ARP-Eintrag mit der MAC-Adresse des Gateway hinzu. Auf diese Weise ist das Gateway über diese Dummy-Dienste erreichbar. Weitere Informationen zum Hinzufügen eines ARP-Eintrags finden Sie unter Konfigurieren von statischem ARP.

   CLI-Beispiel:

```
> add arp -ipaddress 10.10.10.240 -mac 00:21:a1:2d:db:cc -ifnum
   1/2
 Done
> add arp -ipaddress 10.10.10.120 -mac 00:21:a1:2d:db:cc -ifnum
   1/3
 Done
> add arp -ipaddress 10.10.10.60 -mac 00:21:a1:2d:db:cc -ifnum 1/4
 Done
> add arp -ipaddress 10.10.10.30 -mac 00:21:a1:2d:db:cc -ifnum 1/5
 Done
<!--NeedCopy-->
```

7. Binden Sie eine bestimmte Schnittstelle an ein SNIP, indem Sie für jedes dieser SNIPs einen ARP-Eintrag hinzufügen. Dadurch soll sichergestellt werden, dass der Antwortdatenverkehr dieselbe Schnittstelle erreicht, über die die Anforderung ausgegangen ist. Weitere Informationen zum Hinzufügen eines ARP-Eintrags finden Sie unter Konfigurieren von statischem ARP.

   CLI-Beispiel:

```
> add arp -ipAddress 10.10.10.2 -mac 00:e0:ed:0f:bc:e0 -ifnum 1/2
 Done
```



```
> add arp -ipAddress 10.10.10.3 -mac 00:e0:ed:0f:bc:df -ifnum 1/3
 Done
> add arp -ipAddress 10.10.10.4 -mac 00:e0:ed:0f:bc:de -ifnum 1/4
 Done
> add arp -ipAddress 10.10.10.5 -mac 00:e0:ed:1c:89:53 -ifnum 1/5
 Done
<!--NeedCopy-->
```

Überwachen Sie die Bridge-Tabelle und ändern Sie die Alterungszeit

May 11, 2023

Die NetScaler-Appliance überbrückt Frames auf der Grundlage einer Bridge-Tabellensuche nach der Ziel-MAC-Adresse und der VLAN-ID. Die Appliance führt die Weiterleitung jedoch nur durch, wenn der Layer-2-Modus aktiviert ist.

Die Brückentabelle wird dynamisch generiert, aber Sie können sie anzeigen, die Alterungszeit für die Bridge-Tabelle ändern und Bridging-Statistiken einsehen. Alle MAC-Einträge in der Bridge-Tabelle werden mit der Alterungszeit aktualisiert.

So legen Sie die Alterungszeit von Bridge-Tabelleneinträgen mithilfe der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- **setze l2param- bridgeagetimeout** <positive_integer>
- **l2param anzeigen**

Beispiel:

```
> set l2param -bridgeagetimeout 90
 Done
<!--NeedCopy-->
```

Gehen Sie wie folgt vor, um die Statistiken einer Bridgetabelle mit der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **Stat-Brücke**

So legen Sie die Alterungszeit von Bridge-Tabelleneinträgen mithilfe der GUI fest:

Navigieren Sie zu **System** > **Netzwerk**. Klicken Sie auf der **Netzwerkseite** im Abschnitt **Einstellungen** auf **Layer2-Parameter konfigurieren und legen Sie den ParameterTimeout-Wert für die Bridge-Tabelleneinträge (Sekunden)** fest.

Gehen Sie wie folgt vor, um die Statistiken einer Bridgetabelle mithilfe der GUI anzuzeigen:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge-Tabelle**, wählen Sie die MAC-Adresse aus und klicken Sie auf **Statistiken**.

NetScaler-Appliances im Aktiv-Aktiv-Modus mit VRRP

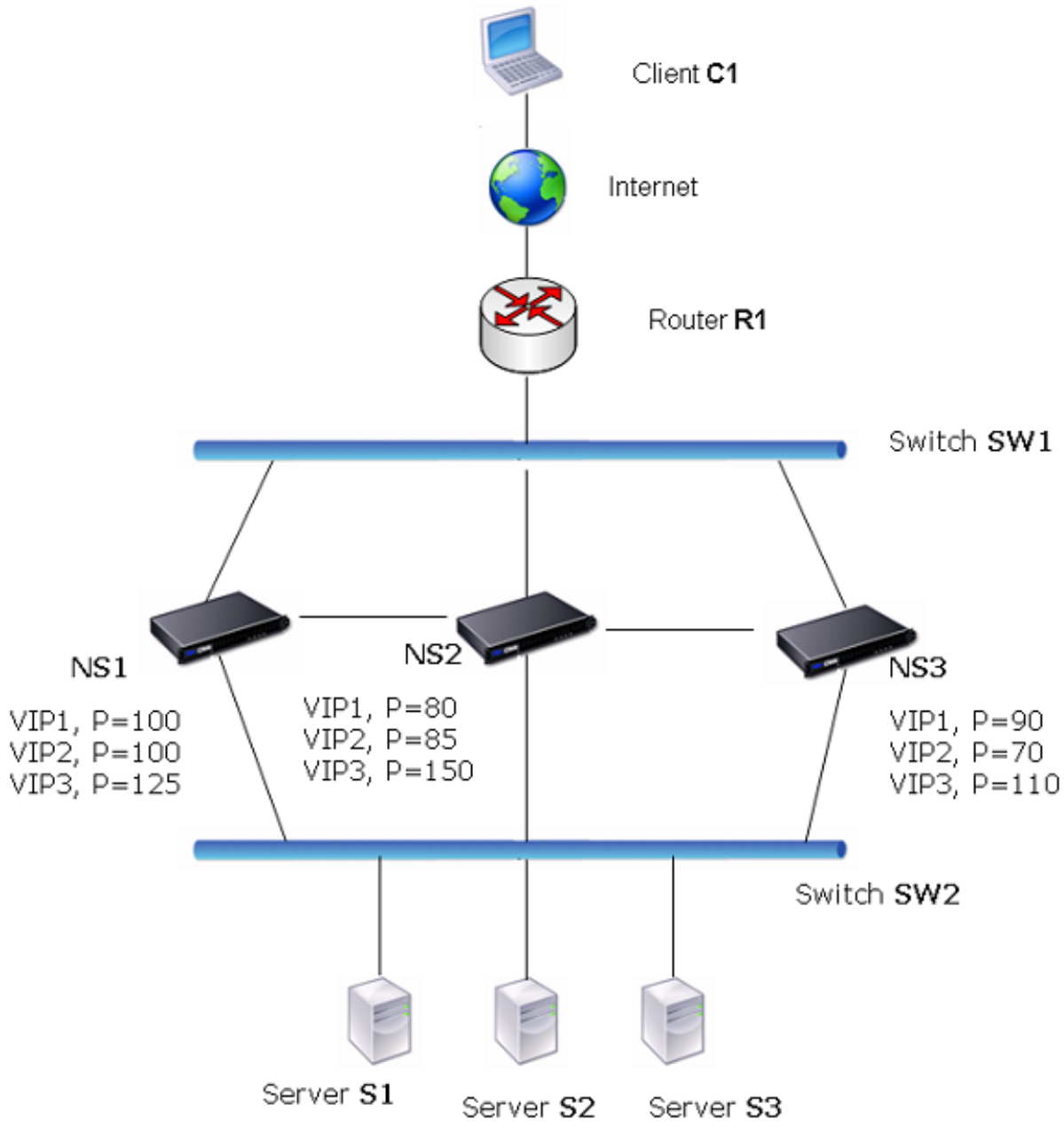
May 11, 2023

Eine aktiv-aktive Bereitstellung verhindert nicht nur Ausfallzeiten, sondern nutzt auch effizient alle NetScaler-Appliances in der Bereitstellung. Im aktiven Bereitstellungsmodus werden dieselben VIPs auf allen NetScaler-Appliances in der Konfiguration konfiguriert, jedoch mit unterschiedlichen Prioritäten, sodass ein bestimmter VIP jeweils nur auf einer Appliance aktiv sein kann.

Der aktive VIP wird Master-VIP genannt, und die entsprechenden VIPs auf den anderen NetScaler-Appliances werden als Backup-VIPs bezeichnet. Wenn ein Master-VIP ausfällt, übernimmt der Backup-VIP mit der höchsten Priorität die Leitung und wird zum Master-VIP. Alle NetScaler-Appliances in einer aktiv-aktiven Bereitstellung verwenden das VRRP-Protokoll (Virtual Router Redundancy Protocol), um ihre VIPs und die entsprechenden Prioritäten in regelmäßigen Abständen bekannt zu geben.

NetScaler-Appliances im Active-Active-Modus können so konfiguriert werden, dass kein NetScaler inaktiv ist. In dieser Konfiguration sind auf jedem NetScaler verschiedene Gruppen von VIPs aktiv. Im folgenden Diagramm sind beispielsweise VIP1, VIP2, VIP3 und VIP4 auf den Appliances NS1, NS2 und NS3 konfiguriert. Aufgrund ihrer Prioritäten sind VIP1 und VIP 2 auf NS1 aktiv, VIP3 ist auf NS2 aktiv und VIP 4 ist auf NS3 aktiv. Wenn beispielsweise NS1 ausfällt, werden VIP1 auf NS3 und VIP2 auf NS2 aktiv.

Abbildung 1. Eine Active-Active-Konfiguration



Die NetScaler-Appliances im obigen Diagramm verarbeiten den Datenverkehr wie folgt:

1. Client C1 sendet eine Anfrage an VIP1. Die Anfrage erreicht R1.
2. R1 hat keinen ARP-Eintrag für VIP1, daher sendet es eine ARP-Anfrage für VIP1.
3. VIP1 ist in NS1 aktiv, daher antwortet NS1 mit einer Quell-MAC-Adresse als virtueller MAC (z. B. virtueller MAC1), der VIP1 zugeordnet ist, und VIP1 als Quell-IP-Adresse.
4. SW1 lernt den Port für VIP1 aus der ARP-Antwort und aktualisiert seine Bridge-Tabelle.
5. R1 aktualisiert den ARP-Eintrag mit virtuellem MAC1 und VIP1.

6. R1 leitet das Paket an das VIP1 auf NS1 weiter.
7. Der Load-Balancing-Algorithmus von NS1 wählt Server S2 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S2.
8. S2 antwortet auf das SNIP auf dem NetScaler.
9. NS1 sendet die Antwort von S2 an den Client. In der Antwort fügt NS1 die MAC-Adresse der physischen Schnittstelle als Quell-MAC-Adresse und VIP1 als Quell-IP-Adresse ein.
10. Sollte NS1 ausfallen, verwenden die NetScaler-Appliances das VRRP-Protokoll, um den VIP1 mit der höchsten Priorität auszuwählen. In diesem Fall wird VIP1 auf NS3 aktiv, und die folgenden beiden Schritte aktualisieren die Active-Active-Konfiguration.
11. NS3 sendet eine GARP-Nachricht für VIP1. In der Nachricht ist virtuelles MAC1 die Quell-MAC-Adresse und VIP1 ist die Quell-IP-Adresse.
12. SW1 lernt den neuen Port für den virtuellen MAC1 aus dem GARP-Broadcast und aktualisiert seine Bridge-Tabelle, um nachfolgende Client-Anforderungen für VIP1 an NS3 zu senden. R1 aktualisiert seine ARP-Tabelle.

Die Priorität eines VIP kann durch Gesundheitstracking geändert werden. Wenn Sie das Health Tracking aktivieren, sollten Sie sicherstellen, dass die Präemption ebenfalls aktiviert ist, sodass ein VIP, dessen Priorität niedriger ist, von einem anderen VIP präemptiv werden kann.

In einigen Situationen kann der Traffic einen Backup-VIP erreichen. Um zu verhindern, dass dieser Datenverkehr verloren geht, können Sie die gemeinsame Nutzung auf Knotenbasis aktivieren, während Sie eine aktiv-aktive Konfiguration erstellen. Oder Sie können die globale Option „An Master senden“ aktivieren. Auf einem Knoten, auf dem das Teilen aktiviert ist, hat es Vorrang vor dem Senden an den Master.

Überwachung des Gesundheitszustands

Die Basispriorität (BP-Bereich 1-255) bestimmt normalerweise, welcher VIP der Master-VIP ist, aber die effektive Priorität (EP) kann sich auch auf die Bestimmung auswirken.

Wenn beispielsweise ein VIP auf NS1 eine Priorität von 101 hat und derselbe VIP auf NS2 eine Priorität von 99 hat, ist der VIP auf NS1 aktiv. Wenn jedoch zwei vServer den VIP auf NS1 verwenden und einer von ihnen ausfällt, kann die Health Tracking die EP von VIP auf NS1 reduzieren. VRRP macht dann den VIP auf NS2 zum aktiven VIP.

Im Folgenden sind die Optionen zur Gesundheitsüberwachung für die Änderung von EP aufgeführt:

- **KEINE.** Kein Tracking. EP = BP
- **ALLE.** Wenn alle virtuellen Server in Betrieb sind, ist EP = BP. Andernfalls ist EP = 0.
- **EINS.** Wenn mindestens ein virtueller Server aktiv ist, dann EP = BP. Andernfalls ist EP = 0.
- **PROGRESSIV.** Wenn ALLE virtuellen Server in Betrieb sind, dann EP = BP. Wenn ALLE virtuellen Server AUSGEFALLEN sind, ist EP = 0. Andernfalls ist EP = BP (1 — K/N), wobei N die Gesamtzahl

der virtuellen Server ist, die dem VIP zugeordnet sind, und k die Anzahl der virtuellen Server ist, die ausgefallen sind.

Hinweis: Wenn Sie einen anderen Wert als NONE angeben, sollte die Präemption aktiviert sein, sodass der Backup-VIP mit der höchsten Priorität aktiv wird, wenn die Priorität des Master-VIP herabgestuft wird.

Vorkaufsrecht

Die Präemption eines aktiven VIP durch einen anderen VIP, der eine höhere Priorität erreicht, ist standardmäßig aktiviert und sollte normalerweise aktiviert sein. In einigen Fällen möchten Sie es jedoch möglicherweise deaktivieren. Preemption ist eine Einstellung pro Knoten für jeden VIP.

Eine Präemption kann in den folgenden Situationen auftreten:

- Ein aktiver VIP geht verloren und ein VIP mit niedrigerer Priorität nimmt seinen Platz ein. Wenn der VIP mit der höheren Priorität wieder online ist, geht er dem aktuell aktiven VIP zuvor.
- Durch das Health Tracking wird die Priorität eines Backup-VIP höher als die des aktiven VIP. Der Backup-VIP kommt dann dem aktiven VIP zuvor.

Freigeben

Falls der Datenverkehr eine Backup-VIP erreicht, wird der Datenverkehr gelöscht, sofern die Sharing-Option auf dem Backup-VIP nicht aktiviert ist. Dieses Verhalten ist eine Einstellung pro Knoten für jeden VIP und ist standardmäßig deaktiviert.

In der Abbildung **Eine aktive Konfiguration** VIP1 auf NS1 ist aktiv und VIP1-VIPs auf NS2 und NS3 sind Backups. Unter bestimmten Umständen kann der Datenverkehr VIP1 auf NS2 erreichen. Wenn die Freigabe auf NS2 aktiviert ist, wird dieser Datenverkehr verarbeitet und nicht gelöscht.

Aktiv-Aktiv-Modus konfigurieren

May 11, 2023

Auf jeder NetScaler-Appliance, die Sie im Active-Active-Modus bereitstellen möchten, müssen Sie einen virtuellen MAC hinzufügen und den virtuellen MAC an einen VIP binden. Der virtuelle MAC für einen bestimmten VIP muss auf jeder Appliance gleich sein. Wenn beispielsweise VIP 10.102.29.5 auf den Appliances erstellt wird, muss auf jedem NetScaler eine virtuelle Router-ID (VRID) erstellt und auf jedem NetScaler an VIP 10.102.29.5 gebunden werden. Wenn Sie einen virtuellen MAC an einen VIP binden, sendet die Appliance VRRP-Werbung an jedes VLAN, das an diesen VIP gebunden ist. Der virtuelle MAC kann von verschiedenen VIPs gemeinsam genutzt werden, die auf demselben NetScaler konfiguriert sind.

Konfiguration des aktiven IPv4-Modus

Führen Sie die folgenden Aufgaben auf jeder der NetScaler-Appliances aus, die in die Active-Active-Konfiguration aufgenommen werden sollen:

- **Fügen Sie eine virtuelle MAC-Adresse**hinzu. Fügen Sie eine virtuelle MAC-Adresse hinzu, indem Sie eine VRID hinzufügen. Sie können für diese VRID-Adresse auch eine Priorität angeben und Präemption und gemeinsame Nutzung aktivieren oder deaktivieren.
- **Fügen Sie eine VIP-Adresse hinzu und verknüpfen Sie die VRID des virtuellen MAC**. Fügen Sie eine VIP-Adresse hinzu und legen Sie den VRID-Parameter auf die neu erstellte VRID fest. Die Attribute der VRID (z. B. Priorität und Präemption) sind an diese VIP-Adresse gebunden.
  Hinweis: Dieselbe VIP-Adresse muss allen anderen NetScaler-Appliances hinzugefügt werden.

So fügen Sie mithilfe der CLI eine virtuelle MAC-Adresse hinzu

Geben Sie in der Befehlszeile Folgendes ein:

- **vRid hinzufügen** <tracking><id>[-**Priorität** \<positive_integer>] [-**Präemption** (**AKTIVIERT**|DEAKTIVIERT**)][-**sharing** (**ENABLED**|**DISABLED**)] [-**Tracking\]**
- **show vrid**

Um eine VIP-Adresse mit der CLI hinzuzufügen:

Geben Sie in der Befehlszeile Folgendes ein:

- **füge ns ip** hinzu <IPv4Address>-type VIP -vrid <value>
- **show ns ip**

So konfigurieren Sie einen virtuellen MAC mithilfe der GUI:

1. Navigieren Sie auf der Registerkarte **VMAC** zu **System** > **Netzwerk**> **VMAC**, fügen Sie einen neuen virtuellen MAC hinzu oder bearbeiten Sie einen vorhandenen virtuellen MAC.
2. Legen Sie die folgenden Parameter fest:
   - Virtuelle Router-ID
   - Priorität
   - Nachverfolgung
   - Vorkaufsrecht
   - Freigeben

Gehen Sie wie folgt vor, um eine VIP-Adresse zu konfigurieren und ihr die VRID zuzuordnen, indem Sie die GUI verwenden:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**und fügen Sie auf der Registerkarte **IPv4s** eine IP-Adresse vom Typ VIP hinzu.
2. Wählen Sie beim Hinzufügen der IP-Adresse die virtuelle Router-ID aus dem **Dropdown-Feld Virtuelle Router-ID** aus.

Beispielkonfiguration:

Die folgende Beispielkonfiguration ist für die Bereitstellung der NetScaler-Appliances NS1 und NS2 im aktiven IPv4-Modus vorgesehen. Die VIP-Adresse 203.0.113.10 ist sowohl auf NS1 als auch auf NS2 konfiguriert und hat auf jeder Appliance einen anderen Prioritätswert. Auf jeder Appliance ist diese VIP-Adresse an eine virtuelle MAC-Adresse gebunden. 203.0.113.10 ist Master auf NS2, da ihre Priorität (200) auf NS2 höher ist als auf NS1 (100).

```
    Settings on NS1

    > add vrid 10 -Priority 100 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done

    Settings on NS2

    > add vrid 10 -Priority 200 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done
<!--NeedCopy-->
```

Konfiguration des aktiven IPv6-Modus

Führen Sie die folgenden Aufgaben auf jeder der NetScaler-Appliances aus, die in die Active-Active-Konfiguration aufgenommen werden sollen:

- **Fügen Sie eine virtuelle MAC6-Adresse**hinzu. Fügen Sie eine virtuelle MAC6-Adresse hinzu, indem Sie eine VRID6 hinzufügen. Sie können für diese VRID6-Adresse auch eine Priorität angeben und Präemption und gemeinsame Nutzung aktivieren oder deaktivieren.
- **Fügen Sie eine VIP6-Adresse**hinzu. Fügen Sie eine VIP6-Adresse hinzu. Setzen Sie den VRID6-Parameter auf den VRID6 des neu erstellten virtuellen MAC6. Die Attribute des virtuellen MAC6 (z. B. Priorität und Präemption) sind an diese VIP6-Adresse gebunden.
  Hinweis: Dieselbe VIP6-Adresse muss allen anderen NetScaler-Appliances hinzugefügt werden.

So fügen Sie mithilfe der CLI eine virtuelle MAC6-Adresse hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- **add vrID6** <id> [-**priority** \<positive_integer>] [-**preemption** (**ENABLED** | **DISABLED**)] [-**sharing** (**ENABLED** | **DISABLED**)]
- **show vrID6**

Um eine VIP6-Adresse mit der CLI hinzuzufügen:

Geben Sie in der Befehlszeile Folgendes ein:

- **füge ns ip6hinzu -**tippe** VIP - vrid** <IPv6Address><value>
- **show ns ip6**

Um einen virtuellen MAC6 mithilfe der GUI zu konfigurieren:

1. **Navigieren Sie zu**System**>**Netzwerk**>**VMAC**und fügen Sie auf der Registerkarte**VMAC6**einen neuen virtuellen MAC6 hinzu oder bearbeiten Sie einen vorhandenen VMAC6.**
2. Legen Sie die folgenden Parameter fest:
   - Virtuelle Router-ID
   - Priorität
   - Vorkaufsrecht
   - Freigeben

Um eine VIP6-Adresse zu konfigurieren und ihr die VRID zuzuordnen, verwenden Sie die GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**und fügen Sie auf der Registerkarte **IPv6s** eine IPv6-Adresse vom Typ VIP hinzu.
2. Wählen Sie beim Hinzufügen der VIP6-Adresse die VRID6 aus dem Dropdown-Feld **Virtuelle Router-ID** aus.

Beispielkonfiguration:

Die folgende Beispielkonfiguration ist für die Bereitstellung der NetScaler-Appliances NS1 und NS2 im aktiven IPv6-Modus vorgesehen. Die VIP6-Adresse 2001:db8: :5001 ist sowohl auf NS1 als auch auf NS2 konfiguriert und hat auf jeder Appliance einen anderen Prioritätswert. Auf jeder Appliance ist diese VIP6-Adresse an eine virtuelle MAC6-Adresse gebunden. 2001:db8: :5001 ist Master auf NS2, weil ihre Priorität (200) auf NS2 höher ist als auf NS1 (100).

```
1     Settings on NS1
2     > add vrid6 10 - Priority 100 - Preemption Enable - sharing Enable
3
4     Done
5     > add ns ip6 2001:db8::5001 - type VIP - vrid6 10
6
7     Done
8     Settings on NS2
9     > add vrid6 10 - Priority 200 - Preemption Enable - sharing Enable
10
11    Done
```



```
    > add ns ip6 2001:db8::5001  -type VIP  -vrid6 10

    Done
<!--NeedCopy-->
```

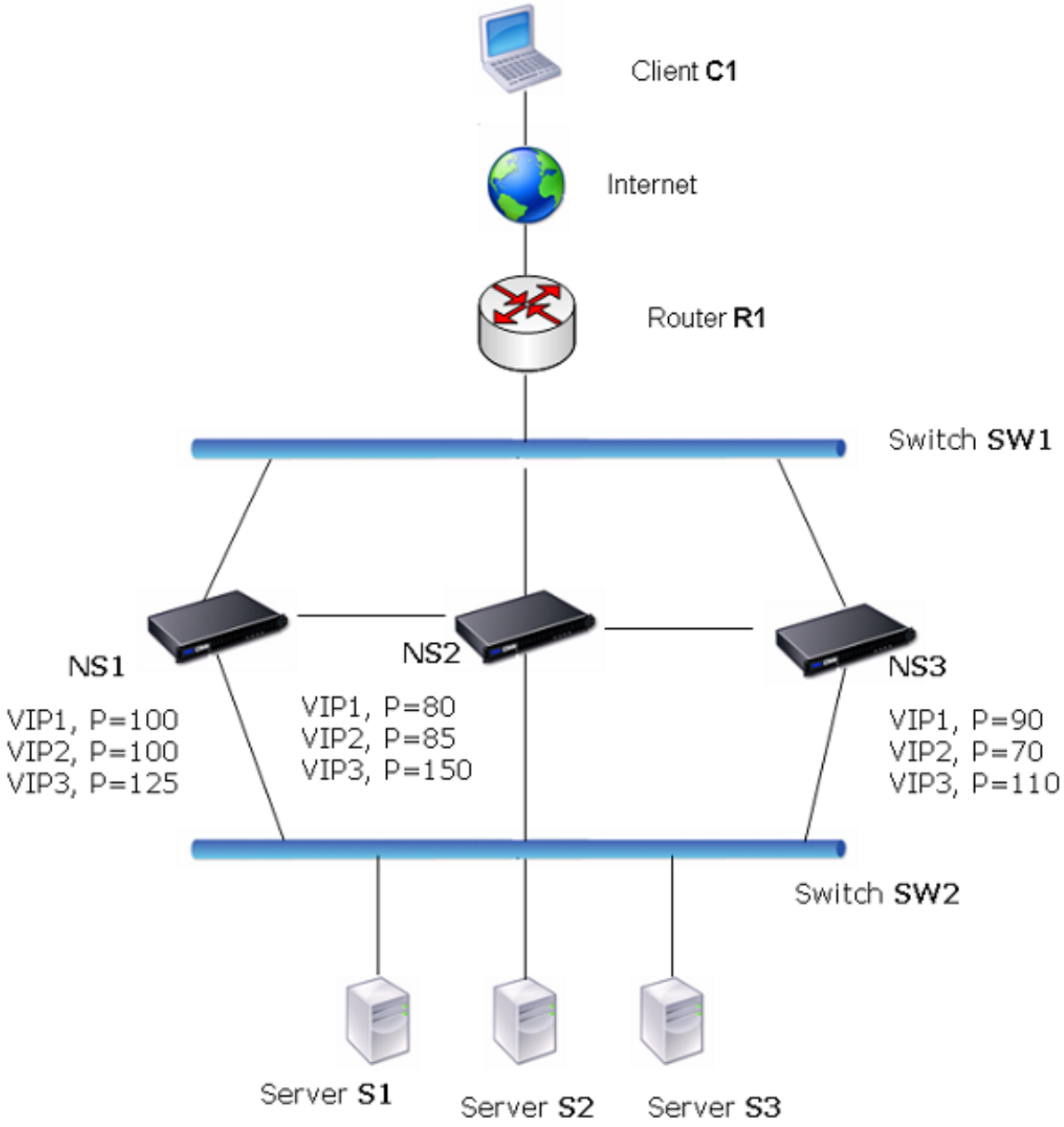
An Master senden konfigurieren

May 11, 2023

Normalerweise erreicht der an einen VIP gerichtete Datenverkehr die NetScaler-Appliance, auf der der VIP aktiv ist, da eine ARP-Anfrage mit dem VIP und einem virtuellen MAC auf dieser Appliance den Upstream-Router erreicht hat. In einigen Fällen, z. B. bei statischen Routen, die auf dem Upstream-Router für das VIP-Subnetz konfiguriert sind, oder bei einer Topologie, die diese Route blockiert, kann der Datenverkehr jedoch eine NetScaler-Appliance erreichen, auf der sich der VIP im Backup-Status befindet. Wenn Sie möchten, dass diese Appliance die Datenpakete an die Appliance weiterleitet, auf der der VIP aktiv ist, müssen Sie die Option An Master senden aktivieren. Dieses Verhalten ist eine Einstellung pro Knoten und standardmäßig deaktiviert.

Im folgenden Diagramm ist VIP1 beispielsweise auf NS1, NS2 und NS3 konfiguriert und auf NS1 aktiv. Unter bestimmten Umständen kann der Traffic für VIP1 (aktiv auf NS1) VIP1 auf NS3 erreichen. Wenn die Option An Master senden auf NS3 aktiviert ist, leitet NS3 den Datenverkehr über NS2 an NS1 weiter, indem Routeneinträge für NS1 verwendet werden.

Abbildung 1. Eine Active-Active-Konfiguration mit aktivierter Option An Master senden



So aktivieren Sie das Senden an den Master mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

```
set vrIDParam -sendToMaster (ENABLED        DISABLED)
```

Beispiel:


```
> set vrIDParam -sendToMaster ENABLED
 Done
<!--NeedCopy-->
```

Um das Senden an den Master mithilfe der GUI zu aktivieren:

1. Navigieren Sie zu **System** > **Netzwerk**und klicken Sie in der Gruppe **Einstellungen** auf **Virtuelle Router-Parameter**.
2. Wählen Sie die Option **An Master senden** .

VRRP-Kommunikationsintervallen konfigurieren

May 11, 2023

Bei einer aktiv-aktiven Bereitstellung verwenden alle NetScaler-Knoten das Virtual Router Redundancy Protocol (VRRP), um ihre Master-VIP-Adressen und die entsprechenden Prioritäten in VRRP-Werbepaketen (Hallo-Nachrichten) in regelmäßigen Abständen bekannt zu geben.

VRRP verwendet die folgenden Kommunikationsintervalle:

- **Hallo Interval**. Intervall zwischen den VRRP-Hello-Nachrichten, die ein Knoten einer Master-VIP-Adresse an seine Peer-Knoten sendet.
- **Totes Intervall**. Zeit, nach der ein Knoten einer Backup-VIP-Adresse den Status der Master-VIP-Adresse als DOWN betrachtet, wenn keine VRRP-Hello-Nachrichten vom Knoten der Master-VIP-Adresse empfangen werden. Nach dem Totintervall übernimmt die Backup-VIP-Adresse die Funktion und wird zur Master-VIP-Adresse.

Sie können diese Intervalle auf einen gewünschten Wert ändern. Beide Kommunikationsintervalle beziehen sich auf die Einstellung pro Knoten für alle VIP-Adressen in diesem Knoten.

So konfigurieren Sie die VRRP-Kommunikationsintervalle mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set vrIDParam** [-**helloInterval** \<msecs>] [-**deadInterval** \<secs>]
- **sh vrIDParam**

Beispiel:

```
> set vrIDParam -helloInterval 500 -deadInterval 2
 Done
<!--NeedCopy-->
```

So konfigurieren Sie die VRRP-Kommunikationsintervalle mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk**und klicken Sie in der Gruppe **Einstellungen** auf **Virtuelle Router-Parameter**.
2. Stellen **Sie unter Virtuelle Router-Parameter konfigurieren**die Parameter **Hello Interval** und **Dead Interval** ein.
3. Klicken Sie auf **OK**.

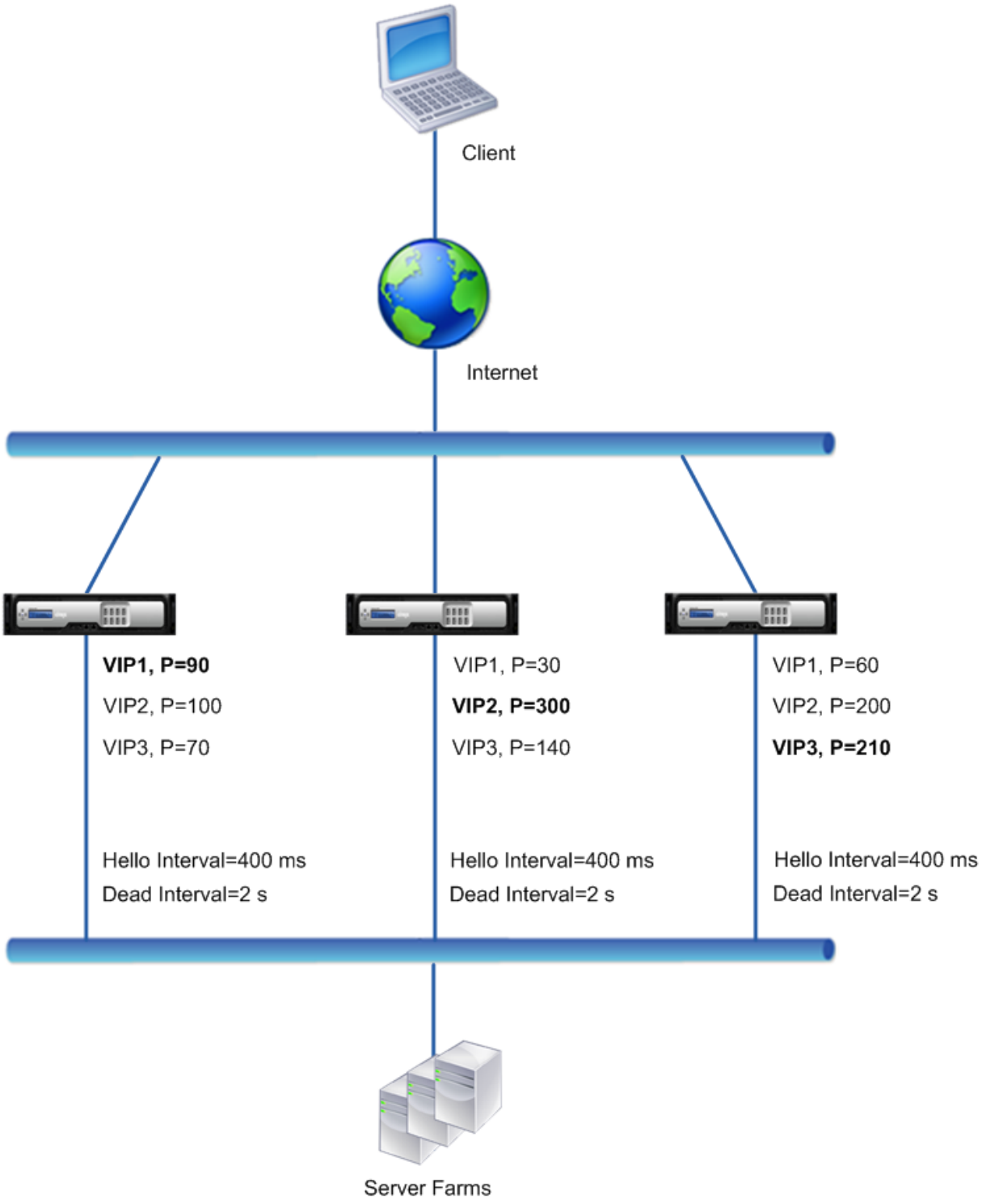
Beispiel 1: Knoten mit den gleichen VRRP-Totintervallen

Ziehen Sie eine aktiv-aktive Bereitstellung in Betracht, die aus NetScalers NS1, NS2 und NS3 besteht. Die virtuellen IP-Adressen VIP1, VIP2, VIP3 sind auf jedem dieser ADCs konfiguriert. Aufgrund ihrer Prioritäten ist VIP1 auf NS1 aktiv, VIP2 ist auf NS2 aktiv und VIP3 ist auf NS3 aktiv.

Wie in der folgenden Tabelle dargestellt, ist das Totintervall auf allen drei Knoten auf denselben Wert (2 Sekunden) gesetzt. Die VRRP-Kommunikationsintervalle (Hallo-Intervall und Totintervall) eines Knotens gelten für alle auf dem Knoten konfigurierten VRIDs und gelten wiederum für alle VIP-Adressen, die den VRIDs auf dem Knoten zugeordnet sind.

Auf jedem Knoten verwenden die VIP-Adressen, die auf diesem Knoten aktiv sind (Master), das Hallo-Intervall, und das tote Intervall wird von den VIP-Adressen verwendet, die auf diesem Knoten inaktiv sind (Backup). Die Präemption ist für die VIP-Adressen in allen drei Knoten deaktiviert.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VRRP-Intervall Beispiel 1 Einstellungen.



Der Ausführungsablauf sieht wie folgt aus:

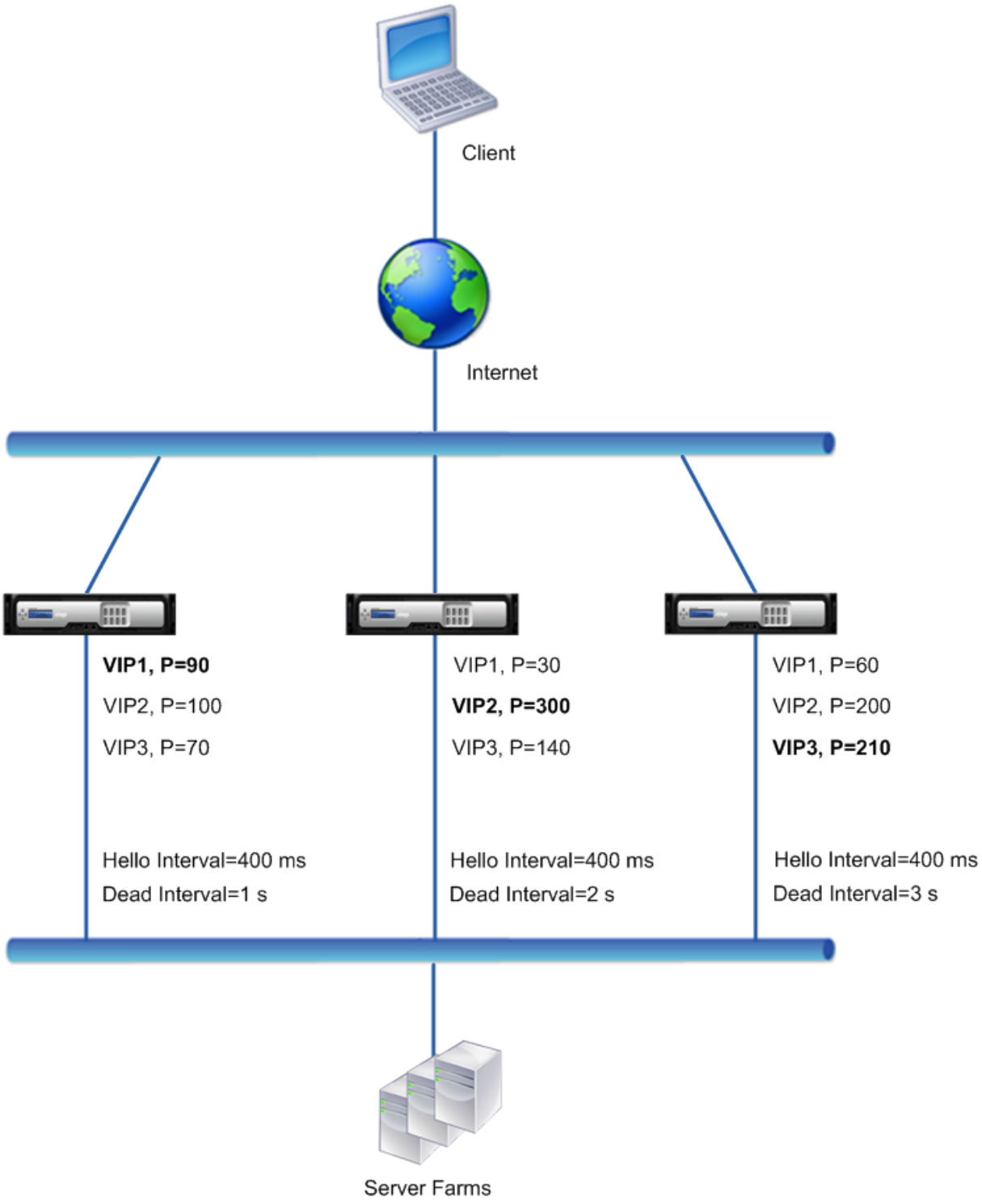
1. NS1 sendet Hello-Nachrichten in einem festgelegten Hallo-Intervall von 400 ms an NS2 und NS3 für die VIP1-Adresse, da VIP1 auf NS1 aktiv ist (der Master). In ähnlicher Weise sendet NS2 Hallo-Nachrichten für VIP2 und NS3 sendet Hallo-Nachrichten für VIP3.

2. Auf NS1 gilt das festgelegte Totzeitintervall für VIP2 und VIP3, da sie auf NS1 inaktiv sind (Backups). In ähnlicher Weise gilt auf NS2 das festgelegte Tot-Intervall für VIP1 und VIP3, und auf NS3 gilt das festgelegte Tot-Intervall für VIP1 und VIP2.
3. Wenn NS1 ausfällt, betrachten NS2 und NS3 NS1 als ausgefallen, wenn sie 2 Sekunden lang keine Hallo-Nachrichten von NS1 erhalten (das tote Intervall). VIP1 auf NS3 übernimmt die Funktion und wird aktiv (Master), da seine VRID-Priorität (60) höher ist als die von VIP1 von NS2 (30).

Beispiel 2: Knoten mit unterschiedlichen VRRP-Totintervallen

Stellen Sie sich eine VRRP-Bereitstellung vor, die der in Beispiel 1 beschriebenen Bereitstellung ähnelt, jedoch mit einem anderen Totintervall auf jedem Knoten (NS1, NS2 und NS3). Die Präemption ist für die VIP-Adressen in allen drei Knoten deaktiviert.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VRRP-Intervall Beispiel 2 Einstellungen.



Der Ausführungsablauf ist wie folgt, wenn NS1 ausfällt:

1. NS2 betrachtet NS1 als ausgefallen, nachdem 2 Sekunden lang keine Hallo-Nachrichten von NS1 empfangen wurden (das tote Intervall von NS2).
2. VIP1 auf NS2 übernimmt die Kontrolle und wird aktiv (Master). NS2 beginnt jetzt, Hallo-

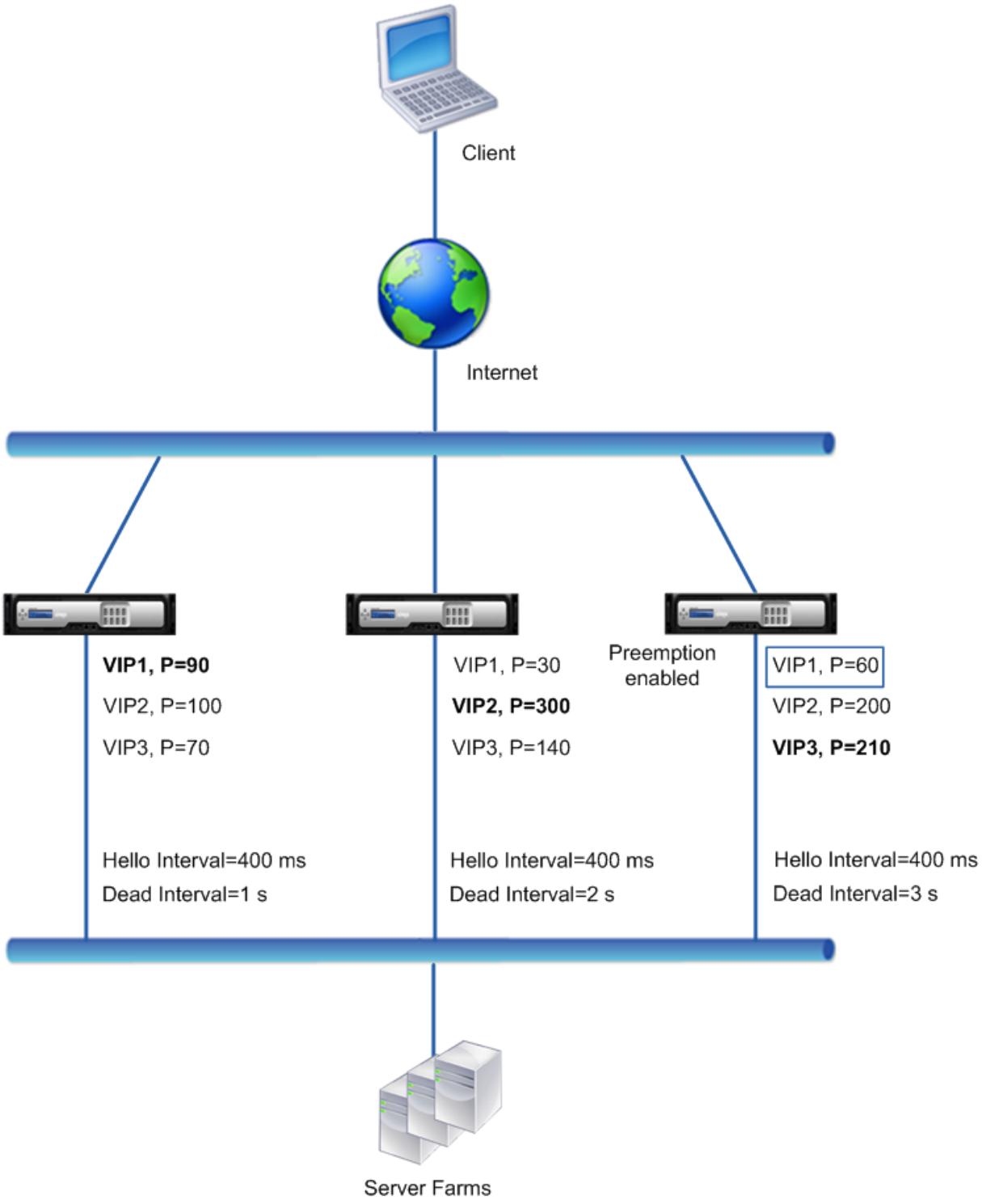
Nachrichten für VIP1 zu senden.

Obwohl VIP1 auf NS3 eine höhere VRIP-Priorität (60) hat als VIP1 auf NS2 (30), verhindert das größere Totintervall von NS3 (3 Sekunden gegenüber 2 Sekunden für NS2), dass VIP1 auf NS3 die Kontrolle übernimmt, bevor VIP 1 auf NS2 dies bereits getan hat.

Beispiel 3: Knoten mit unterschiedlichen Totintervallen und aktivierter Präemption

Betrachten Sie eine VRRP-Bereitstellung ähnlich der in Beispiel1 beschriebenen Bereitstellung, jedoch mit unterschiedlichen Deadintervallen auf den drei Knoten NS1, NS2 und NS3 und mit aktivierter Präemption für die VIP1-Adresse auf NS3.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VRRP-Intervall Beispiel 3 Einstellungen.



Der Ausführungsablauf ist wie folgt, wenn NS1 ausfällt:

1. NS2 betrachtet NS1 als ausgefallen, nachdem 2 Sekunden lang keine Hallo-Nachrichten von NS1 empfangen wurden (das eingestellte Tot-Intervall von NS2). Zu diesem Zeitpunkt betrachtet NS3 mit einem Totintervall von 3 Sekunden NS1 nicht als ausgefallen.

2. VIP1 auf NS2 übernimmt die Kontrolle und wird aktiv (Master). NS2 beginnt jetzt, Hallo-Nachrichten für VIP1 zu senden.
3. Beim Empfang von Hello-Nachrichten von NS2 für VIP1 nimmt NS3 NS2 für VIP1 vor, da die Präemption für VIP1 von NS3 aktiviert ist und die VRID-Priorität (60) von VIP1 von NS3 höher ist als die (30) von VIP1 von NS2.
4. VIP1 auf NS3 übernimmt die Kontrolle und wird aktiv (Master). NS3 beginnt jetzt mit dem Senden von Hallo Nachrichten für VIP1.

Health Tracking basierend auf dem Schnittstellenstatus konfigurieren

May 11, 2023

Um sicherzustellen, dass eine Backup-VIP-Adresse die Funktion des Master-VIP übernimmt, bevor der Knoten der aktuellen Master-VIP-Adresse vollständig ausfällt, können Sie einen Knoten so konfigurieren, dass er die Priorität einer VIP-Adresse ändert, wenn sich der Status einer Schnittstelle auf dem Knoten ändert. Beispielsweise reduziert der Knoten die Priorität einer VIP-Adresse, wenn sich der Status einer Schnittstelle zu DOWN ändert, und erhöht die Priorität, wenn der Status der Schnittstelle zu UP wechselt. Diese Funktion ist eine Konfiguration pro Knoten für jede VIP-Adresse.

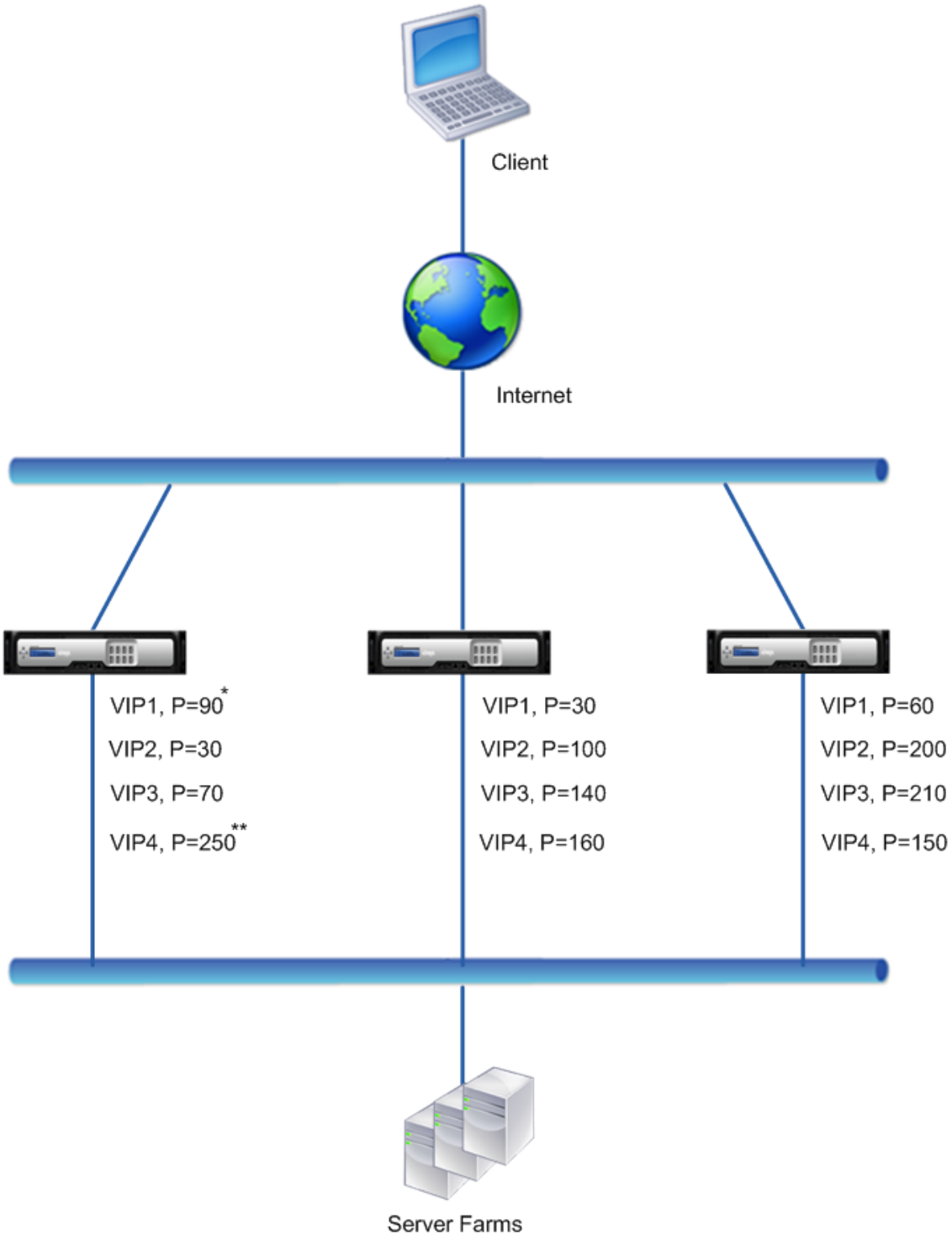
Beispiel

Ziehen Sie eine aktiv-aktive Bereitstellung in Betracht, die aus NetScalers NS1, NS2 und NS3 besteht. Die virtuellen IP-Adressen VIP1, VIP2, VIP3 und VIP4 sind auf jedem dieser ADCs konfiguriert. Aufgrund ihrer Prioritäten sind VIP1 und VIP4 auf NS1 aktiv, VIP2 ist auf NS2 aktiv und VIP3 ist auf NS3 aktiv.

Um sicherzustellen, dass die aktiven VIP-Adressen auf NS1 entweder von NS2 oder NS3 übernommen werden, bevor NS1 vollständig ausfällt, wird für die VIP1- und VIP4-Adressen auf NS1 eine schnittstellenbasierte Health Tracking konfiguriert. Die Konfiguration der schnittstellenbasierten Health Tracking für eine VIP-Adresse umfasst die Zuordnung der gewünschten Schnittstellen und das Festlegen des Parameters mit reduzierter Priorität (trackIfNumPriority) für die zugehörige VRID der VIP-Adresse. Auf NS1 sind beispielsweise die Schnittstellen 1/2, 1/3 und 1/5 der VRID von VIP1 zugeordnet, und die reduzierte Priorität ist auf 20 festgelegt.

Die Präemption ist für diese VIP-Adressen in allen drei Knoten aktiviert.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: Beispieleinstellungen für Health Tracking.



* Packet Interfaces = 1/2, 1/3, 1/5
Reduced Priority = 20

** Packet Interfaces = 1/5, 1/7
Reduced Priority = 55

Der Ausführungsablauf auf NS1 ist wie folgt, wenn mehrere Schnittstellen auf NS1 ausfallen:

1. Wenn Schnittstelle 1/3 ausfällt, wird die Priorität der Adresse VIP1 um 20 reduziert (der reduzierte Prioritätswert von VIP1), da Schnittstelle 1/3 mit VIP1 verknüpft ist:
   - Effektive Priorität von VIP1 = (Aktuelle Priorität — reduzierte Priorität) = (90-20) = 70
2. In ähnlicher Weise wird die Priorität der Adresse VIP1 weiter reduziert, wenn die Schnittstelle 1/5 ausfällt:
   - Effektive Priorität von VIP1 = (Aktuelle Priorität — reduzierte Priorität) = (70-20) = 50
3. Zu diesem Zeitpunkt ist die effektive Priorität von VIP1 auf NS1 geringer als die Priorität von VIP1 auf NS3. NS3 nimmt NS1 für VIP1 vor. VIP1 auf NS3 übernimmt die Kontrolle und wird aktiv (Master).
4. Da die Schnittstelle 1/5 auch mit VIP4 verknüpft ist, wird die Priorität von VIP4 außerdem um den reduzierten Prioritätswert von VIP4 reduziert (55).
   - Effektive Priorität von VIP4 = (250 - 55) = 195
5. Wenn die Schnittstelle 1/7 ausfällt, wird die Priorität von VIP4 weiter reduziert:
   - Effektive Priorität von VIP4 = (Aktuelle Priorität — reduzierte Priorität) = (195-55) = 145
6. Zu diesem Zeitpunkt ist die effektive Priorität von VIP4 auf NS1 geringer als die Priorität von VIP4 auf NS2. NS2 nimmt NS1 für VIP4 vor. VIP4 auf NS3 übernimmt die Kontrolle und wird aktiv (Master). Diese Konfiguration stellt sicher, dass keine der vier VIP-Adressen auf NS1 aktiv ist, bevor sie vollständig ausfällt.

Konfigurationsschritte für den aktiven IPv4-Modus

Um diese Funktion auf einem Knoten für eine VIP-Adresse zu konfigurieren, legen Sie den Parameter Reduced Priority (trackIfNumPriority) fest und verknüpfen dann die Schnittstellen, deren Status verfolgt werden soll, um die Priorität der VIP-Adresse zu ändern. Wenn sich der Status der zugehörigen Schnittstelle in DOWN oder UP ändert, reduziert oder erhöht der Knoten die Priorität der VIP-Adresse um den konfigurierten Wert für reduzierte Priorität (trackIfNumPriority).

Um eine reduzierte Priorität festzulegen und Schnittstellen mithilfe der CLI an die virtuelle Router-ID zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- **setze vrID** <positive_integer><id>[-** trackIfNumPriority\]
- **bind vrID** <id> -**trackifNum** <interface_name>
- **vRID anzeigen** <id>

Beispiel:

```
1     > set vrID 125 -trackifNumPriority 10
2     Done
3
4     > bind vrID 125 -trackifNum 1/4 1/5
```



```
    Done
<!--NeedCopy-->
```

Um eine reduzierte Priorität festzulegen und Schnittstellen mithilfe der GUI an die virtuelle Router-ID zu binden:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC.**
2. **Wählen Sie auf der Registerkarte**VMACs**eine virtuelle Router-ID aus und klicken Sie auf Bearbeiten.**
3. Stellen **Sie unter Virtuellen MAC konfigurieren**den Parameter **Reduced Priority** ein.
4. Wählen Sie die Option **Für die VRID getrackte Schnittstellen** aus und fügen Sie unter **Schnittstellen zuordnen Schnittstellen**zur virtuellen Router-ID hinzu.

Konfigurationsschritte für den aktiven IPv6-Modus

Um diese Funktion auf einem Knoten für eine VIP6-Adresse zu konfigurieren, legen Sie den Parameter Reduced Priority (trackIfNumPriority) fest und verknüpfen dann die Schnittstellen, deren Status verfolgt werden soll, um die Priorität der VIP6-Adresse zu ändern. Wenn sich der Status der zugehörigen Schnittstelle in DOWN oder UP ändert, reduziert oder erhöht der Knoten die Priorität der VIP6-Adresse um den konfigurierten Wert für reduzierte Priorität (trackIfNumPriority).

Um die Priorität einer VIP-Adresse automatisch mithilfe der CLI zu ändern, gehen Sie wie folgt vor:

Geben Sie in der Befehlszeile einen der folgenden Befehlssätze ein.

- Wenn Sie einen neuen virtuellen MAC6 hinzufügen:
  - **add vrID6** <id> [-**trackifNumPriority** \<positive_integer>]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>
- Wenn Sie einen vorhandenen virtuellen MAC6 neu konfigurieren:
  - **set vrID6** <id> [-**trackifNumPriority** \<positive_integer>]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>

Beispiel:

```
    > set vrID6 130 -trackifNumPriority 10
    Done

    > bind vrID6 130 -trackifNum 1/4 1/5
    Done
<!--NeedCopy-->
```


Verzögerung der Präemption

May 11, 2023

Standardmäßig verhindert eine Backup-VIP-Adresse die Master-VIP-Adresse, sobald ihre Priorität höher ist als die der Master-VIP. Bei der Konfiguration einer Backup-VIP-Adresse können Sie einen Zeitraum angeben, um den die Präemption verzögert werden soll. Die Präemptionsverzögerungszeit ist eine Einstellung pro Knoten für jede Backup-VIP-Adresse.

Die Einstellung für die Präemptionsverzögerung für einen Backup-VIP gilt unter den folgenden Bedingungen nicht:

- Der Knoten des Master-VIP fällt aus. In diesem Fall übernimmt der Backup-VIP nach Ablauf des auf dem Backup-VIP-Knoten festgelegten Totintervalls die Backup des Master-VIP.
- Die Priorität des Master-VIP ist auf Null gesetzt. Der Backup-VIP übernimmt nach Ablauf des auf dem Backup-VIP-Knoten festgelegten Ausfallintervalls die Backup des Master-VIP.

Beispiel: Verzögerung der Präemption

Ziehen Sie eine aktiv-aktive Bereitstellung in Betracht, die aus den NetScaler-Appliances NS1 und NS2 besteht. Die virtuelle IP-Adresse VIP1 ist auf jeder dieser Appliances konfiguriert. Aufgrund ihrer Prioritäten ist VIP1 Master auf NS2. Die Präemption ist aktiviert und die Wartezeit für die Präemption ist für VIP1 auf diesen beiden Knoten festgelegt.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entität und Parameter	Einstellungen auf NS1	Einstellungen auf NS2
VIP1 (nur zu Referenzzwecken)	**IP-Adresse:192.0.1.10, **VRID: 10, Priorität:100, Präemption:Aktiviert, Präemptionsverzögerungszeit:** 1000 Sekunden**	**IP-Adresse:192.0.1.10, **VRID: 10, Priorität:200, Präemption:Aktiviert, Präemptionsverzögerungszeit:** 2000 Sekunden**
Totes Intervall	1 Sekunden	2 Sekunden

Im Folgenden finden Sie einige Beispiele für ein mögliches Präemptionsverhalten in diesem Setup:

- Wenn die Priorität von VIP1 auf NS1 auf einen höheren Wert (z. B. 210) als der von VIP1 auf NS2 gesetzt ist, übernimmt VIP1 auf NS1 nach der eingestellten Präemptionsverzögerungszeit (1000 Sekunden) die Rolle des Masters.
- Wenn dieser Bereitstellung ein dritter Knoten NS3 mit den folgenden VRRP-Einstellungen

hinzugefügt wird, wird VIP1 auf NS3 nach der eingestellten Präemptionsverzögerungszeit (3000 Sekunden) zum Master.
  - VIP1
    * GITTER: 30
    * IP-Adresse:
    * Priorität = 300
    * Vorkaufsverzögerungszeit = 3000 Sekunden
- Wenn NS2 ausfällt, übernimmt VIP1 auf NS1 nach 1 Sekunde die Rolle des Masters (eingestelltes Totzeitintervall auf NS1). Die Wartezeit bei der Präemption für VIP1 auf NS1 gilt in diesem Fall nicht.
- Wenn NS2 ausfällt und NS1 neu gestartet wird, wird VIP1 auf NS1 1 Sekunde nach dem Hochfahren von NS1 zum Master (festgelegtes Totzeitintervall auf NS1). Die Wartezeit bei der Präemption für VIP1 auf NS1 gilt in diesem Fall nicht.
- Wenn die Priorität von VIP1 auf NS2 auf Null gesetzt ist, wechselt VIP1 in den Standby-Modus. VIP1 auf NS1 übernimmt nach 1 Sekunde die Funktion des Masters (eingestelltes Tot-Intervall auf NS1). Die Wartezeit bei der Präemption für VIP1 auf NS1 gilt in diesem Fall nicht.

Delay Preemption für den aktiven IPv4-Modus konfigurieren

Um die Präemptionsverzögerungszeit für eine VIP-Adresse zu konfigurieren, legen Sie den Parameter Preemption Delay Timer der zugehörigen virtuellen MAC-Adresse fest. Sie können diesen Parameter dann festlegen, wenn Sie die Adresse hinzufügen, oder Sie können eine bestehende virtuelle MAC-Adresse ändern.

So konfigurieren Sie die Wartezeit für die Präemption mithilfe der CLI:

- Um die Wartezeit beim Hinzufügen eines virtuellen MAC festzulegen, geben Sie in der Befehlszeile Folgendes ein:
  - **add vrID** <id> -**preemptiondelaytimer** <secs>
  - **show vrID**
- Um die Wartezeit bei der Änderung eines virtuellen MAC festzulegen, geben Sie in der Befehlszeile Folgendes ein:
  - **set vrID** <id> -**preemptiondelaytimer** <secs>
  - **show vrID**

So konfigurieren Sie die Wartezeit für die Präemption mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**.
2. Auf der Registerkarte **VMAC** . Stellen Sie beim Hinzufügen eines neuen virtuellen MAC oder beim Bearbeiten eines vorhandenen virtuellen MAC den Parameter **Preemption Delay Timer** ein.

Beispielkonfiguration:

Die folgende Konfiguration verwendet die in der Tabelle im Abschnitt Beispiel: Delaying Preemption aufgeführten Einstellungen.

```
1      Settings on NS1
2
3      > set vrid param  -deadInterval 1
4
5      Done
6
7      > add ns ip 192.0.1.10 255.255.255.255  -type VIP
8
9      Done
10
11     > add vrid 10  -Priority 100  -Preemption Enable  -
           preemptiondelaytimer 1000
12
13     Done
14
15     > bind ns ip 192.0.1.10 255.255.255.255  -vrid 10
16
17     Done
18
19     Settings on NS2
20
21     > set vrid param  -deadInterval 2
22
23     Done
24
25     > add ns ip 192.0.1.10 255.255.255.255  -type VIP
26
27     Done
28
29     > add vrid 20  -Priority 200  -Preemption Enable  -
           preemptiondelaytimer 2000
30
31     Done
32
33     > set ns ip 192.0.1.10 255.255.255.255  -vrid 10
34
35     Done
36 <!--NeedCopy-->
```


Delay Preemption für den aktiven IPv6-Modus konfigurieren

Um die Präemptionsverzögerungszeit für eine VIP6-Adresse zu konfigurieren, legen Sie den Timer-Parameter für die Präemptionsverzögerung der zugehörigen virtuellen MAC6-Adresse fest. Sie können diesen Parameter dann festlegen, wenn Sie die virtuelle MAC6-Adresse hinzufügen, oder Sie können eine vorhandene virtuelle MAC6-Adresse ändern.

So konfigurieren Sie die Wartezeit für die Präemption mithilfe der CLI:

- Um die Wartezeit beim Hinzufügen eines virtuellen MAC6 festzulegen, geben Sie in der Befehlszeile Folgendes ein:
  - **add vrID6** <id> -**preemptiondelaytimer** <secs>
  - **show vrID6**
- Um die Wartezeit bei der Änderung eines virtuellen MAC6 festzulegen, geben Sie in der Befehlszeile Folgendes ein:
  - **set vrID6** <id> -**preemptiondelaytimer** <secs>
  - **show vrID6**

So konfigurieren Sie die Wartezeit für die Präemption mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**.
2. Auf der Registerkarte **VMAC6** . Legen Sie beim Hinzufügen einer virtuellen MAC6-Adresse oder beim Bearbeiten einer vorhandenen virtuellen MAC6-Adresse den Parameter **Zeitüberschreitung** fest.

Beibehalten einer VIP-Adresse im Backupstatus

January 19, 2021

Sie können erzwingen, dass eine VIP-Adresse immer im Backup-Zustand bleibt. Dieser Vorgang ist hilfreich bei der Wartung oder beim Testen einer VRRP-Bereitstellung.

Wenn eine VIP-Adresse gezwungen ist, im Backup-Zustand zu bleiben, nimmt sie nicht an VRRP-Statusübergängen teil. Außerdem kann es nicht Master werden, selbst wenn alle anderen Knoten heruntergehen.

Um zu erzwingen, dass eine VIP-Adresse im Backup-Zustand bleibt, legen Sie die Priorität der zugeordneten virtuellen MAC-Adresse auf Null fest. Um sicherzustellen, dass keine der VIP-Adressen eines Knotens Datenverkehr während eines Wartungsprozesses auf dem Knoten verarbeitet, setzen Sie alle Prioritäten auf Null.

Sie können die Priorität einer virtuellen MAC-Adresse festlegen, während Sie die Adresse hinzufügen oder ändern.

So erzwingen Sie, dass eine VIP-Adresse mit der CLI im Backup-Zustand bleibt:

- Um die Priorität beim Hinzufügen eines virtuellen MAC festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add vrID** <id> -**priority** 0
  - **show vrID**
- Um die Priorität beim Ändern eines virtuellen MAC festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set vrID** <id> -**priority** 0
  - **show vrID**

So erzwingen Sie, dass eine VIP-Adresse mit der GUI im Backup-Zustand bleibt:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**.
2. Legen Sie auf der Registerkarte **VMAC** beim Hinzufügen eines neuen virtuellen MAC oder beim Bearbeiten eines vorhandenen virtuellen MAC den Parameter **Priority** auf Null fest.

Netzwerk-Visualizer

May 11, 2023

Der Netzwerkvisualizer zeigt eine grafische Ansicht aller Schnittstellen, Kanäle, VLANs, IP-Adressen und Bindungen zu VLANs auf einer NetScaler-Appliance. Eine aktivierte Schnittstelle oder ein aktivierter Kanal hat ein schwarzes Etikett. Eine deaktivierte Schnittstelle oder ein deaktivierter Kanal ist rot gekennzeichnet.

Dieses vollständige Bild der Netzwerkverbindungen der Appliance kann nützlich sein, um Fehler im Netzwerkdesign zu erkennen und das Netzwerk zu optimieren. Es kann einem neuen Administrator auch helfen, die Netzwerkkonfiguration der Appliance leicht zu verstehen.

Um den Network Visualizer zu öffnen:

Navigieren Sie zu **System** > **Netzwerk**. Klicken Sie unter **Monitorverbindungen**auf **Network Visualizer**.

Link Layer Discovery Protocol konfigurieren

May 11, 2023

Der NetScaler unterstützt den Industriestandard (IEEE 802.1AB) Link Layer Discovery Protocol (LLDP). LLDP ist ein Layer-2-Protokoll, das es dem NetScaler ermöglicht, seine Identität und Funktionen den

direkt angeschlossenen Geräten mitzuteilen und auch die Identität und Fähigkeiten dieser Nachbargeräte zu ermitteln.

> **Hinweis:**
> Das Link Layer Discovery Protocol (LLDP) wird nur auf NetScaler MPX-Plattformen unterstützt.

Mithilfe von LLDP überträgt und empfängt der NetScaler Informationen in Form von LLDP-Nachrichten, die als LLDP-Paketdateneinheiten (LLDPUs) bekannt sind. Eine LLDPU ist eine Abfolge von Informationselementen vom Typ, Länge, Wert (TLV). Jedes TLV enthält eine bestimmte Art von Informationen über das Gerät, das die LLDPDU überträgt. Der NetScaler sendet die folgenden TLVs in jeder LLDPU:

- Fahrgestell-ID
- Port-ID
- Wert der Nutzungsdauer
- Name des Systems
- Beschreibung des Systems
- Beschreibung des Hafens
- Fähigkeiten des Systems
- Adresse des Managements
- Port-VLAN-ID
- Link-Aggregation

Hinweis: Sie können die TLVs, die in LLDP-Nachrichten gesendet werden sollen, nicht angeben.

NetScaler-Schnittstellen unterstützen die folgenden LLDP-Modi:

- **KEINE**. Die Schnittstelle empfängt weder LLDP-Nachrichten von noch überträgt sie an das direkt angeschlossene Gerät.
- **SENDER**. Die Schnittstelle überträgt LLDP-Nachrichten an das direkt angeschlossene Gerät, empfängt jedoch keine LLDP-Nachrichten von dem direkt angeschlossenen Gerät.
- **EMPFÄNGER**. Die Schnittstelle empfängt LLDP-Nachrichten von dem direkt angeschlossenen Gerät, überträgt jedoch keine LLDP-Nachrichten an das direkt angeschlossene Gerät.
- **TRANSCEIVER**. Die Schnittstelle überträgt LLDP-Nachrichten an das direkt angeschlossene Gerät und empfängt LLDP-Nachrichten von diesem.

Der LLDP-Modus einer Schnittstelle hängt vom LLDP-Modus ab, der auf globaler Ebene und der Schnittstellenebene konfiguriert ist. Die folgende Tabelle zeigt die Modi, die sich aus den verfügbaren Kombinationen von Einstellungen auf globaler und Schnittstellenebene ergeben: Interface- und LLDP-Modi auf globaler Ebene.

Beachten Sie die folgenden Punkte im Zusammenhang mit LLDP-Nachrichten, die vom NetScaler übertragen oder empfangen werden:

- **Übertragung von LLDP-Nachrichten.** Der NetScaler überträgt LLDPUs von Schnittstellen, die entweder im TRANSMITTER- oder TRANSCEIVER-LLDP-Modus arbeiten.

Im Folgenden sind die globalen LLDP-Übertragungsparameter auf dem NetScaler aufgeführt:

- **Zeitschaltuhr**. Intervall in Sekunden zwischen LLDPUs, die der NetScaler an ein direkt angeschlossenes Gerät sendet.
- **Holdtime-Multiplikator.** Ein Multiplikator zur Berechnung der Dauer, für die das empfangende Gerät die LLDP-Informationen in seiner Datenbank speichert, bevor sie verworfen oder entfernt werden. Die Dauer wird berechnet, indem der **Holdtime-Multiplikator-Parameterwert** mit dem Timer-Parameterwert multipliziert wird.

- **Empfangen von LLDP-Nachrichten.** Der NetScaler speichert die LLDPDU-Informationen in seiner Management Information Base (MIB). Die gespeicherten LLDP-Informationen werden unter der ID der Schnittstelle klassifiziert oder gruppiert, die die LLDPDU empfangen hat. Der NetScaler speichert diese LLDP-Informationen für die in der empfangenen LLDPU angegebene Dauer.

  Wenn der ADC eine weitere LLDPDU auf einer Schnittstelle empfängt, bevor die gespeicherten LLDP-Informationen für diese Schnittstelle verworfen werden, ersetzt der ADC die gespeicherten LLDP-Informationen für diese Schnittstelle durch Informationen in der neuen LLDPDU.

Konfigurationsschritte

Die Konfiguration von LLDP auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

1. **Legt die LLDP-Parameter auf globaler Ebene fest.** In dieser Aufgabe legen Sie die globalen LLDP-Parameter wie LLDP-Timer, Hold Time Multiplier und LLDP-Modus fest.
2. **Stellen Sie die LLDP-Parameter auf Schnittstellenebene ein.** In dieser Aufgabe legen Sie den LLDP-Modus für eine Schnittstelle fest.
3. **(Optional) Zeigt Informationen zum Nachbargerät an.** Sie können die LLDP-Informationen des Nachbargeräts anzeigen, die auf allen NetScaler-Schnittstellen gesammelt wurden, oder nur die LLDP-Informationen, die auf bestimmten Schnittstellen gesammelt wurden. Wenn Sie keine Schnittstelle angeben, werden die Informationen für alle Schnittstellen angezeigt.

Im Folgenden sind die Voraussetzungen für die Konfiguration von LLDP auf einem NetScaler aufgeführt:

1. Stellen Sie sicher, dass Sie das Standard-LLDP-Protokoll (IEEE 802.1AB) verstehen.
2. Stellen Sie sicher, dass Sie LLDP auf den gewünschten direkt verbundenen Geräten konfiguriert haben.

CLI-Verfahren

Um LLDP-Parameter auf globaler Ebene mithilfe der CLI festzulegen:

Geben Sie in der Befehlszeile Folgendes ein:

- <positive_integer><Mode>setze den lldp-Parameter [- [-holdtimeXMult [-Mode\][-timer <positive_integer>]]
- show lldp param

Um eine Schnittstelle für LLDP mit der CLI zu konfigurieren:

Geben Sie in der Befehlszeile Folgendes ein:

- Setze die Schnittstelle <id>-lldpmode <lldpmode>
- show interface <id>

So zeigen Sie mithilfe der CLI Informationen zum Nachbargerät an:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- lldp-Nachbarn anzeigen
- lldp-Nachbarn anzeigen <ifnum>

GUI-Verfahren

Um die LLDP-Parameter auf globaler Ebene mithilfe der GUI festzulegen:

1. Navigieren Sie zu System > Netzwerk und klicken Sie auf LLDP-Parameter konfigurieren.
2. Legen Sie die folgenden Parameter fest:
    - Timer-Multiplikator halten
    - Schaltuhr
    - Modus

Um eine Schnittstelle für LLDP mithilfe der GUI zu konfigurieren:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Schnittstelle und stellen Sie den LLDP-Modusparameter ein.

Um Informationen über Nachbargeräte mithilfe der GUI anzuzeigen:

Navigieren Sie zu System > Netzwerk > Schnittstellen und wählen Sie in der Aktionsliste die Option LLDP-Nachbarn anzeigen aus.

LLDP-Unterstützung in einem Cluster-Setup

In einem Cluster-Setup zeigen GUI und CLI die LLDP-Nachbarkonfiguration aller oder bestimmter Clusterknoten an, wenn über die Cluster-IP-Adresse (CLIP) auf die GUI oder CLI zugegriffen wird. Jede Änderung, die am LLDP-Modus auf globaler Ebene vorgenommen wird, wird auf den LLDP-Modus auf globaler Ebene auf jedem Clusterknoten angewendet.

Stellen Sie sich ein Beispiel für ein Cluster-Setup mit drei Knoten, NS1, NS2 und NS3, vor. Jeder dieser Knoten ist mit den beiden Routern Router-1 und Router-2 verbunden. Die folgende Ausgabe wird angezeigt, wenn der Vorgang **show lldp neighbor -summary** auf der Cluster-CLI ausgeführt wird, auf die über die Cluster-IP-Adresse (CLIP) des Cluster-Setups zugegriffen wird. Die Ausgabe zeigt die LLDP-Nachbarinformationen all dieser Knoten.

```
> show lldp neighbor -summary

Node Id: 1
------------------------------------------------------------
    Interface    ChassisId           PortId     System name
------------------------------------------------------------
1     1/1/1      fe:c7:3b:13:bd:11    1/1         Router-1

2     1/1/2      12:68:7b:9e:4c:11    1/1         Router-2

Node Id: 2
------------------------------------------------------------
    Interface    ChassisId           PortId     System name
------------------------------------------------------------
1     2/1/1      fe:c7:3b:13:bd:12    1/2        Router-1

2     2/1/2      12:68:7b:9e:4c:12    1/2        Router-2

Node Id: 3
------------------------------------------------------------
    Interface    ChassisId            PortId     System name
------------------------------------------------------------

1     3/1/1       fe:c7:3b:13:bd:13    1/3        Router-1

2     3/1/2       12:68:7b:9e:4c:13    1/3        Router-2

Done
<!--NeedCopy-->
```

Jumbo Frames

May 11, 2023

NetScaler-Appliances unterstützen das Empfangen und Senden von Jumbo-Frames mit bis zu 9216 Byte an IP-Daten. Jumbo-Frames können große Dateien effizienter übertragen als dies mit der stan-

dardmäßigen IP-MTU-Größe von 1500 Byte möglich ist.

Eine NetScaler-Appliance kann Jumbo-Frames in den folgenden Bereitstellungsszenarien verwenden:

- Jumbo zu Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Jumbo-Frames.
- Von Non-Jumbo zu Jumbo. Die Appliance empfängt Daten als reguläre Frames und sendet sie als Jumbo-Frames.
- Jumbo bis Non-Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als reguläre Frames.

Die NetScaler-Appliance unterstützt Jumbo-Frames in einer Load-Balancing-Konfiguration für die folgenden Protokolle:

- TCP
- Jedes Protokoll über TCP (z. B. HTTP)
- SIP
- RADIUS

Jumbo-Frames-Unterstützung auf einer NetScaler-Appliance konfigurieren

May 11, 2023

Damit die NetScaler-Appliance Jumbo-Frames unterstützt, setzen Sie die MTU auf mehr als 1500 an Schnittstellen oder LA-Kanälen sowie auf VLANs, auf denen die NetScaler-Appliance Jumbo-Frames unterstützen soll.

Punkte, die Sie berücksichtigen sollten, bevor Sie die MTU von Schnittstellen, LA-Kanälen oder VLANs auf einer NetScaler-Appliance festlegen

1. Wenn Sie einen LA-Kanal erstellen, übernimmt der Kanal die MTU der ersten gebundenen Schnittstelle, falls für den Kanal keine MTU angegeben ist.
2. Die MTU für einen Kanal wird an alle gebundenen Schnittstellen weitergegeben.
3. Wenn eine Schnittstelle an den Kanal gebunden ist, dessen MTU sich von der MTU der Schnittstelle unterscheidet, wird die Schnittstelle in die inaktive Liste aufgenommen.
4. Wenn Sie die MTU einer Mitgliederschnittstelle ändern, wird die Schnittstelle in die Liste der inaktiven Benutzer aufgenommen.
5. Wenn eine Schnittstelle vom Kanal getrennt ist, behält die Schnittstelle den MTU-Wert des Kanals bei.

6. Sie können die MTU für eine Schnittstelle, einen Kanal oder ein VLAN auf einen Wert im Bereich von 1500-9216 festlegen.
7. Sie können die MTU nicht im Standard-VLAN festlegen. Die NetScaler-Appliance verwendet die MTU der Schnittstelle, über die sie Daten vom oder zum Standard-VLAN empfängt oder sendet.
8. Für TCP-basierten Datenverkehr in einer Load-Balancing-Konfiguration auf einer NetScaler-Appliance werden MSSs an jedem Endpunkt entsprechend eingerichtet, um Jumbo-Frames zu unterstützen:
    - Für eine Verbindung zwischen einem Client und einem virtuellen Lastausgleichsserver auf der NetScaler-Appliance wird die MSS auf der NetScaler-Appliance in einem TCP-Profil festgelegt, das dann an den virtuellen Lastausgleichsserver gebunden ist.
    - Für eine Verbindung zwischen der NetScaler-Appliance und einem Server wird das MSS auf NS1 in einem TCP-Profil festgelegt, das dann an den Dienst gebunden ist, der den Server auf der NetScaler-Appliance darstellt.
    - Standardmäßig ist ein TCP-Profil nstcp_default_profile an alle TCP-basierten Load Balancing-Server und -Dienste auf der NetScaler-Appliance gebunden.
    - Zur Unterstützung von Jumbo-Frames können Sie entweder den MSS-Wert des TCP-Profils nstcp_default_profile ändern oder ein benutzerdefiniertes TCP-Profil erstellen und dessen MSS entsprechend festlegen und dann das benutzerdefinierte TCP-Profil an die gewünschten virtuellen Lastausgleichsserver und -dienste binden.
    - Der Standard-MSS-Wert eines TCP-Profils ist 1460.

CLI-Verfahren

So legen Sie die MTU einer Schnittstelle mit der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- stelle Schnittstelle <id>-mtu ein <positive_integer>
- show interface <id>

Beispiel:

```
1 > set interface 10/1  - mtu 9000
2 Done
3 <!--NeedCopy-->
```

So legen Sie die MTU eines Kanals mit der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- Kanal <id>-mtu einstellen <positive_integer>
- Kanal einblenden <id>

Beispiel:

```
> set channel LA/1 -mtu 9000
Done
<!--NeedCopy-->
```

So legen Sie die MTU eines VLANs mithilfe der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- <id>vlan -mtu hinzufügen <positive_integer>
- show vlan <id>

Beispiel:

```
> set vlan 20 -mtu 9000
Done
<!--NeedCopy-->
```

GUI-Verfahren

So legen Sie die MTU einer Schnittstelle mithilfe der GUI fest:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Schnittstelle und stellen Sie den Parameter Maximale Übertragungseinheit ein.

So legen Sie die MTU eines Kanals mithilfe der GUI fest:

Navigieren Sie zu System > Netzwerk > Kanäle, öffnen Sie den Kanal und stellen Sie den Parameter Maximale Übertragungseinheit ein.

So legen Sie die MTU eines VLANs mithilfe der GUI fest:

Navigieren Sie zu System > Netzwerk > VLANs, öffnen Sie das VLAN und legen Sie den Parameter Maximale Übertragungseinheit fest.

Anwendungsfall 1 — Jumbo zu Jumbo Setup

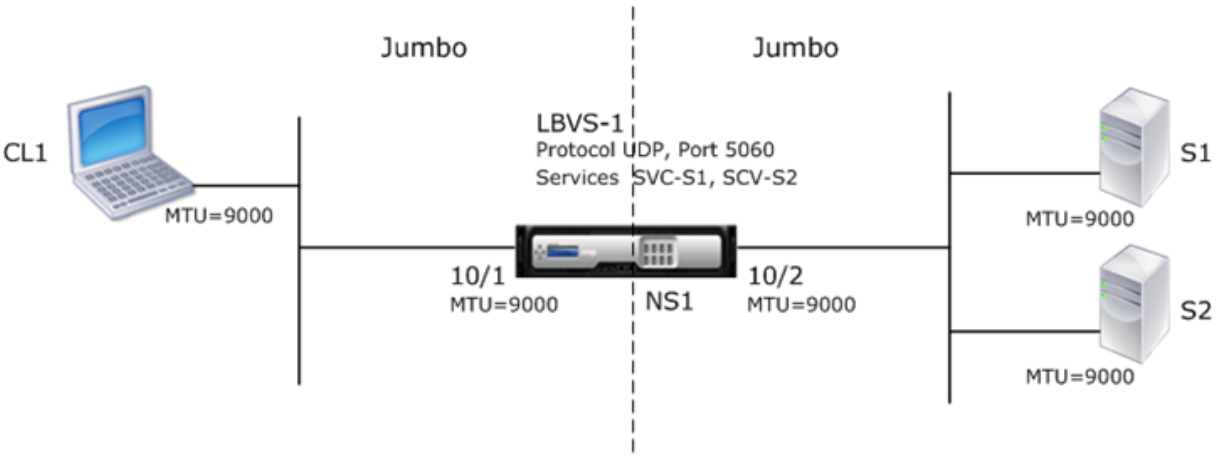
May 11, 2023

Stellen Sie sich ein Beispiel für ein Jumbo-zu-Jumbo-Setup vor, bei dem der virtuelle SIP-Lastenausgleichsserver LBVS-1, der auf der NetScaler Appliance NS1 konfiguriert ist, zum Lastausgleich des SIP-Datenverkehrs zwischen den Servern S1 und S2 verwendet wird. Die Verbindung zwischen Client CL1 und NS1 und die Verbindung zwischen NS1 und den Servern unterstützen Jumbo-Frames.

Die Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr vom oder zum Client CL1. Die Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr vom oder zum Server S1 oder S2. Die Schnittstellen 10/1 und 10/2 von NS1 sind Teil von VLAN 10 bzw. VLAN 20.

Zur Unterstützung von Jumbo-Frames ist die MTU auf NS1 für die Schnittstellen 10/1, 10/2 und die VLANs VLAN 10, VLAN 20 auf 9216 gesetzt.

Alle anderen Netzwerkgeräte, einschließlich CL1, S1, S2, sind in diesem Setup-Beispiel ebenfalls für die Unterstützung von Jumbo-Frames konfiguriert.



In der folgenden Tabelle sind die im Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
Die IP-Adresse des Clients CL1	-	192.0.2.10
Die IP-Adresse der Server	S1	198.51.100.19
	S2	198.51.100.20
SNIP-Adresse auf NS1		198.51.100.18
MTU für Schnittstellen und VLANs auf NS1 spezifiziert	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
Dienste auf NS1, die Server darstellen	SVC-S1	**IP-Adresse:198.51.100.19, **Protokoll: SIP, Port: 5060****
	SVC-S2	**IP-Adresse:198.51.100.20, **Protokoll: SIP, Port: 5060****

Entität	Name	Details
Virtueller Lastausgleichsserver auf VLAN 10	LBVS-1	**IP-Adresse:** 203.0.113.15, **Protokoll: SIP, Port:5060, **Bound-Dienste** : SVC-S1**, SVC-S2

Im Folgenden ist der Verkehrsfluss der Anfrage von CL1 an NS1 dargestellt:

1. CL1 erstellt eine 20000-Byte-SIP-Anfrage, die an LBVS-1 von NS1 gesendet wird.
2. CL1 sendet die Anforderungsdaten in IP-Fragmenten an LBVS-1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000), die auf der Schnittstelle festgelegt ist, von der CL1 diese Fragmente an NS1 sendet.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 2048] = 2068
3. NS1 empfängt die IP-Fragmente der Anforderung an Schnittstelle 10/1. NS1 akzeptiert diese Fragmente, da die Größe jedes dieser Fragmente gleich oder kleiner als die MTU (9000) der Schnittstelle 10/1 ist.
4. NS1 setzt diese IP-Fragmente wieder zusammen, um die 20000-Byte-SIP-Anfrage zu bilden. NS1 verarbeitet diese Anfrage.
5. Der Load-Balancing-Algorithmus von LBVS-1 wählt Server S1 aus.
6. NS1 sendet die Anforderungsdaten in IP-Fragmenten an S1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000) der Schnittstelle 10/2, von der NS1 diese Fragmente an S1 sendet. Die IP-Pakete werden mit einer SNIP-Adresse von NS1 bezogen.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 2048] = 2068

Es folgt der Verkehrsfluss der Antwort von S1 auf CL1 in diesem Beispiel:

1. Server S1 erstellt eine 30000-Byte-SIP-Antwort zum Senden an die SNIP-Adresse von NS1.
2. S1 sendet die Antwortdaten in IP-Fragmenten an die SNIP-Adresse von NS1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000), die auf der Schnittstelle festgelegt ist, von der S1 diese Fragmente an NS1 sendet.

- Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
- Größe des zweiten und dritten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
- Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 3068] = 3088

3. NS1 empfängt die Antwort-IP-Fragmente an Schnittstelle 10/2. NS1 akzeptiert diese Fragmente, da die Größe jedes Fragments gleich oder kleiner als die MTU (9000) der Schnittstelle 10/2 ist.
4. NS1 setzt diese IP-Fragmente wieder zusammen, um die 30000-Byte-SIP-Antwort zu bilden. NS1 verarbeitet diese Antwort.
5. NS1 sendet die Antwortdaten in IP-Fragmenten an CL1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000) der Schnittstelle 10/1, von der NS1 diese Fragmente an CL1 sendet. Die IP-Fragmente werden mit der IP-Adresse von LBVS-1 beschafft.
   - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
   - Größe des zweiten und dritten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
   - Größe des letzten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 3068] = 3088

Konfigurationsaufgaben

In der folgenden Tabelle sind die Aufgaben, NetScaler-Befehle und Beispiele für die Erstellung der erforderlichen Konfiguration auf der NetScaler-Appliance aufgeführt.

Aufgabe	NetScaler-Befehlssyntax	Beispiel
Stellen Sie die MTU der gewünschten Schnittstellen für die Unterstützung von Jumbo-Frames ein	Schnittstelle <id>-mtu setzen<positive_integer>, Schnittstelle anzeigen <id>	setint 10/1 -mtu 9000 setint 10/2 -mtu 9000
Erstellen Sie VLANs und legen Sie die MTU der gewünschten VLANs für die Unterstützung von Jumbo-Frames fest	<positive_integer>vlan <id>-mtu hinzufügen, vlan anzeigen <id>	vlan 10 -mtu 9000 hinzufügen vlan 20 -mtu 9000
Binden Sie Schnittstellen an VLANs	<interface_name>vlan <id>-ifnum binden, vlan anzeigen <id>	binde vlan 10 -ifnum 10/1 binde vlan 20 -ifnum 10/2

Aufgabe	NetScaler-Befehlssyntax	Beispiel
Fügen Sie eine SNIP-Adresse hinzu	füge ns ip hinzu <IPAddress><netmask>-type SNIP, zeige ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Dienste erstellen, die SIP-Server repräsentieren	<port>Dienst <serviceName><ip>SIP_UDP hinzufügen, Dienst anzeigen <name>	Dienst hinzufügen SVC-S1 198.51.100.19 SIP_UDP 5060 Dienst hinzufügen SVC-S2 198.51.100.20 SIP_UDP 5060
Erstellen Sie virtuelle SIP-Lastausgleichsserver und binden Sie die Dienste daran	<vserverName><serviceName>füge lb vserver <name>SIP_UDP hinzu, <ip><port>bind lb vserver, zeige lb vserver <name>	füge lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 Bindung lb vserver LBVS-1 SVC-S1 bindung lb vserver LBVS-1 SVC-S2 hinzu
Speichern Sie die Konfiguration	NS-Konfiguration speichern, NS-Konfiguration anzeigen	

Anwendungsfall 2 — Nicht-Jumbo-zu-Jumbo-Setup

May 11, 2023

Stellen Sie sich ein Beispiel für ein reguläres bis großes Setup vor, bei dem der virtuelle Lastausgleichsserver LBVS-1, der auf einer NetScaler-Appliance NS1 konfiguriert ist, für den Lastenausgleich des Datenverkehrs zwischen den Servern S1 und S2 verwendet wird. Die Verbindung zwischen Client CL1 und NS1 unterstützt reguläre Frames, und die Verbindung zwischen NS1 und den Servern unterstützt Jumbo-Frames.

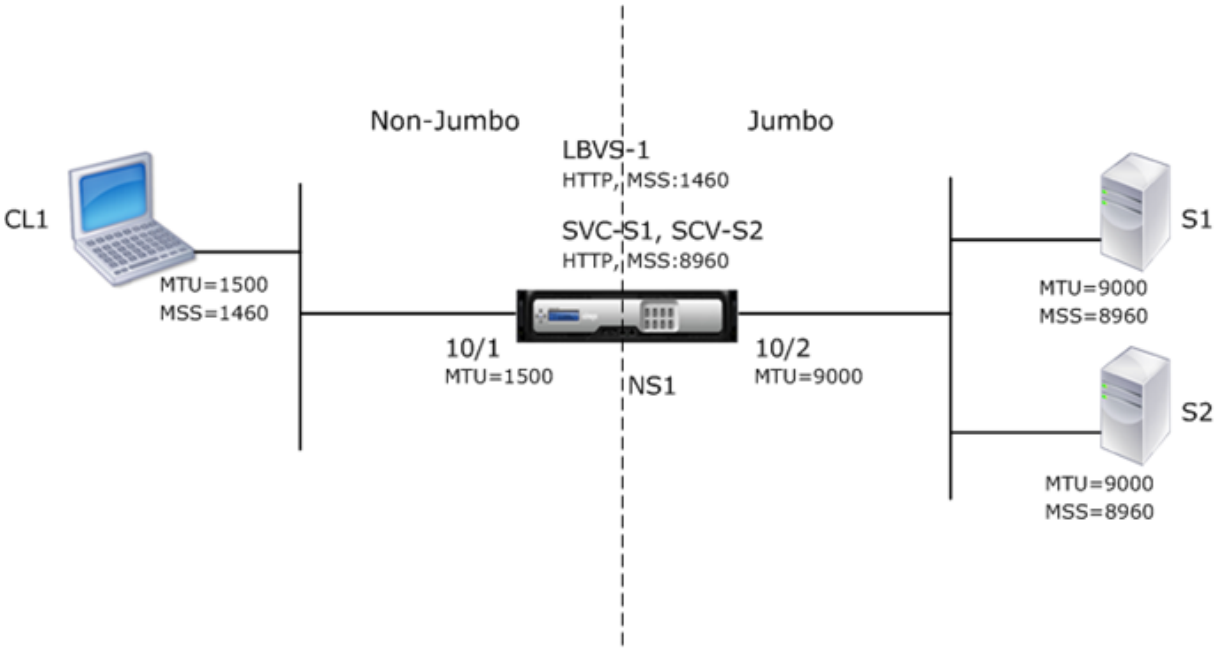
Die Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr vom oder zum Client CL1. Die Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr vom oder zum Server S1 oder S2.

Die Schnittstellen 10/1 und 10/2 von NS1 sind Teil von VLAN 10 bzw. VLAN 20. Um nur reguläre Frames zwischen CL1 und NS1 zu unterstützen, ist die MTU sowohl für die Schnittstelle 10/1 als auch für VLAN 10 auf den Standardwert 1500 gesetzt.

Für die Unterstützung von Jumbo-Frames zwischen NS1 und den Servern ist die MTU für die Schnittstelle 10/2 und VLAN 20 auf 9000 eingestellt. Server und alle anderen Netzwerkgeräte zwischen NS1 und den Servern sind ebenfalls für die Unterstützung von Jumbo-Frames konfiguriert.

Da der HTTP-Verkehr auf TCP basiert, werden MSSs an jedem Endpunkt entsprechend für die Unterstützung von Jumbo-Frames festgelegt.

- Zur Unterstützung von Jumbo-Frames für die Verbindung zwischen einer SNIP-Adresse von NS1 und S1 oder S2 wird die MSS auf NS1 entsprechend in einem benutzerdefinierten TCP-Profil festgelegt, das an die Dienste (SVC-S1 und SVC-S1) gebunden ist, die S1 und S2 auf NS1 repräsentieren.
- Um nur reguläre Frames für die Verbindung zwischen CL1 und dem virtuellen Server LBVS-1 von NS1 zu unterstützen, wird das Standard-TCP-Profil nstcp_default_profile verwendet, das standardmäßig an LBVS-1 gebunden ist und dessen MSS auf den Standardwert 1460 gesetzt ist.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
Die IP-Adresse des Clients CL1		192.0.2.10
Die IP-Adresse der Server	S1	198.51.100.19
	S2	198.51.100.20
SNIP-Adresse auf NS1		198.51.100.18
MTU für Schnittstellen und VLANs auf NS1 spezifiziert	10/1	1500
	10/2	9000
	VLAN 10	1500
	VLAN 20	9000
Standard-TCP-Profil	nstcp_default_profile	MSS:1460

Entität	Name	Details
Benutzerdefiniertes TCP-Profil	NS1-SERVERS-JUMBO	GEWICHT: 8960
Dienste auf NS1, die Server darstellen	SVC-S1	IP-Adresse: 198.51.100.19, Protokoll: HTTP, Port: 80, TCP-Profil: NS1-SERVERS-JUMBO (MSS: 8960)
	SVC-S2	IP-Adresse: 198.51.100.20, Protokoll: HTTP, Port: 80, TCP-Profil: NS1-SERVERS-JUMBO (MSS: 8960)
Virtueller Lastausgleichsserver auf VLAN 10	LBVS-1	IP-Adresse = 203.0.113.15, Protokoll: HTTP, Port: 80, Gebundene Dienste: SVC-S1, SVC-S2, TCP-Profil: nstcp_default_profile (MSS:1460)

Es folgt der Verkehrsfluss von CL1s Anfrage an S1 in diesem Beispiel:

1. Der Client CL1 erstellt eine 200-Byte-HTTP-Anforderung zum Senden an den virtuellen Server LBVS-1 von NS1.
2. CL1 öffnet eine Verbindung zu LBVS-1 von NS1. CL1 und NS1 tauschen beim Verbindungsaufbau ihre jeweiligen TCP-MSS-Werte aus.
3. Da NS1 MSS größer ist als die HTTP-Anforderung, CL1 sendet die Anforderungsdaten in einem einzigen IP-Paket an NS1.

   Größe des Anforderungspakets = [IP-Header + TCP-Header + TCP-Anfrage] = [20 + 20 + 200] = 240
4. NS1 empfängt das Anforderungspaket an der Schnittstelle 10/1 und verarbeitet dann die HTTP-Anforderungsdaten im Paket.
5. Der Load Balancing-Algorithmus von LBVS-1 wählt Server S1 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S1. NS1 und CL1 tauschen beim Verbindungsaufbau ihre jeweiligen TCP-MSS-Werte aus.
6. Da der MSS von S1 größer ist als die HTTP-Anforderung, sendet NS1 die Anforderungsdaten in einem einzigen IP-Paket an S1.

Größe des Anforderungspakets = [IP-Header + TCP-Header + [TCP-Anforderung] = [20 + 20 + 200] = 240

Es folgt der Verkehrsfluss von S1 Antwort auf CL1 in diesem Beispiel:

1. Server S1 erstellt eine 18000-Byte-HTTP-Antwort, die an die SNIP-Adresse von NS1 gesendet wird.
2. S1 segmentiert die Antwortdaten in Vielfache des MSS von NS1 und sendet diese Segmente in IP-Paketen an NS1. Diese IP-Pakete werden von der IP-Adresse von S1 bezogen und an die SNIP-Adresse von NS1 bestimmt.
   - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Segment = MSS-Größe von NS1)] = [20 + 20 + 8960] = 9000
   - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120
3. NS1 empfängt die Antwortpakete an Schnittstelle 10/2.
4. Aus diesen IP-Paketen setzt NS1 alle TCP-Segmente zu den HTTP-Antwortdaten von 18000 Byte zusammen. NS1 verarbeitet diese Antwort.
5. NS1 segmentiert die Antwortdaten in Vielfache des MSS von CL1 und sendet diese Segmente in IP-Paketen von der Schnittstelle 10/1 an CL1. Diese IP-Pakete werden von der IP-Adresse von LBVS-1 bezogen und an die IP-Adresse von CL1 bestimmt.
   - Größe aller Pakete außer dem letzten = [IP-Header + TCP-Header + (TCP-Nutzlast = MSS-Größe von CL1)] = [20 + 20 + 1460] = 1500
   - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 480] = 520

Konfigurationsaufgaben

In der folgenden Tabelle sind die Aufgaben, NetScaler-Befehle und Beispiele für die Erstellung der erforderlichen Konfiguration auf der NetScaler-Appliance aufgeführt.

Aufgaben	CLI-Syntax	Beispiele
Stellen Sie die MTU der gewünschten Schnittstellen für die Unterstützung von Jumbo-Frames ein	Schnittstelle <id>-mtu setzen<positive_integer>, Schnittstelle anzeigen <id>	setint 10/1 -mtu 1500 setint 10/2 -mtu 9000
Erstellen Sie VLANs und legen Sie die MTU der gewünschten VLANs für die Unterstützung von Jumbo-Frames fest	<positive_integer>vlan <id>-mtu hinzufügen, vlan anzeigen <id>	vlan 10 -mtu 1500 hinzufügen vlan 20 -mtu 9000 hinzufügen

Aufgaben	CLI-Syntax	Beispiele
Binden Sie Schnittstellen an VLANs	<interface_name>vlan <id>-ifnum binden, vlan anzeigen <id>	binde vlan 10 -ifnum 10/1 binde vlan 20 -ifnum 10/2
Fügen Sie eine SNIP-Adresse hinzu	füge ns ip hinzu <IPAddress><netmask>-type SNIP, zeige ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Dienste erstellen, die HTTP-Server darstellen	Dienst <serviceName><ip>HTTP hinzufügen<port>, Dienst anzeigen <name>	Dienst SVC-S1 198.51.100.19 http 80 hinzufügen, Dienst SVC-S2 hinzufügen 198.51.100.20 http 80
Erstellen Sie virtuelle HTTP-Lastausgleichsserver und binden Sie die Dienste daran	lb vserver <name>HTTP hinzufügen <ip><port>, lb vserver binden <vserverName><serviceName>, lb vserver anzeigen <name>	füge lb vserver LBVS-1 http 203.0.113.15 80 hinzu, binde lb vserver LBVS-1 SVC-S1, bindung lb vserver LBVS-1 SVC-S2
Erstellen Sie ein benutzerdefiniertes TCP-Profil und stellen Sie dessen MSS für die Unterstützung von Jumbo-Frames ein	<positive_integer>füge tcpProfile <name>-mss hinzu, zeige TCPProfile <name>	add tcpprofile NS1-SERVERS-JUMBO -mss 8960
Binden Sie das benutzerdefinierte TCP-Profil an die gewünschten Dienste	<string>Dienst <Name>-TcpProfileName setzen, Dienst anzeigen <name>	setze Dienst SVC-S1 -TCPProfilname NS1-SERVERS-JUMBO, setze Dienst SVC-S2 -TCPProfilname NS1-SERVERS-JUMBO
Speichern Sie die Konfiguration	NS-Konfiguration speichern, NS-Konfiguration anzeigen	

Anwendungsfall 3 — Koexistenz von Jumbo- und Nicht-Jumbo-Flüssen auf demselben Schnittstellensatz

May 11, 2023

Stellen Sie sich ein Beispiel vor, in dem die virtuellen Lastausgleichsserver LBVS-1 und LBVS-2 auf der NetScaler Appliance NS1 konfiguriert sind. LBVS-1 wird verwendet, um den HTTP-Verkehr zwischen den Servern S1 und S2 zu verteilen, und LBVS-2 wird verwendet, um den Datenverkehr zwischen den Servern S3 und S4 auszugleichen.

CL1 ist auf VLAN 10, S1 und S2 sind auf VLAN20, CL2 ist auf VLAN 30 und S3 und S4 sind auf VLAN 40. VLAN 10 und VLAN 20 unterstützen Jumbo-Frames, und VLAN 30 und VLAN 40 unterstützen nur reguläre Frames.

Mit anderen Worten, die Verbindung zwischen CL1 und NS1 und die Verbindung zwischen NS1 und Server S1 oder S2 unterstützen Jumbo-Frames. Die Verbindung zwischen CL2 und NS1 und die Verbindung zwischen NS1 und Server S3 oder S4 unterstützen nur reguläre Frames.

Die Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr von oder zu Clients. Die Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr von oder zu den Servern.

Die Schnittstelle 10/1 ist sowohl an VLAN 10 als auch an VLAN 30 als markierte Schnittstelle gebunden, und die Schnittstelle 10/2 ist als markierte Schnittstelle sowohl an VLAN 20 als auch an VLAN 40 gebunden.

Für die Unterstützung von Jumbo-Frames ist die MTU für die Schnittstellen 10/1 und 10/2 auf 9216 eingestellt.

Auf NS1 ist die MTU auf 9000 für VLAN 10 und VLAN 20 für die Unterstützung von Jumbo-Frames festgelegt, und die MTU ist auf den Standardwert 1500 für VLAN 30 und VLAN 40 gesetzt, um nur reguläre Frames zu unterstützen.

Die effektive MTU auf einer NetScaler-Schnittstelle für mit VLAN markierte Pakete entspricht der MTU der Schnittstelle oder der MTU des VLAN, je nachdem, welcher Wert niedriger ist. Zum Beispiel:

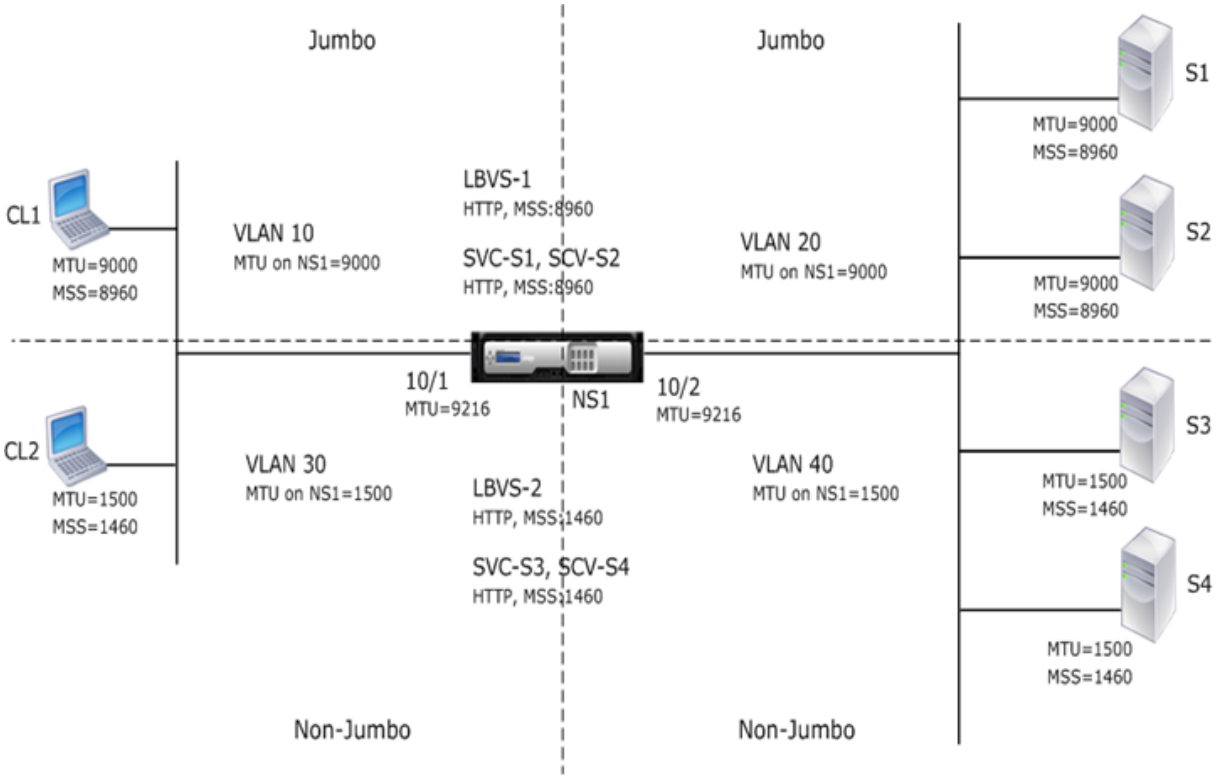
- Die MTU der Schnittstelle 10/1 ist 9216. Die MTU von VLAN 10 ist 9000. Auf der Schnittstelle 10/1 beträgt die MTU der mit VLAN 10 markierten Paketen 9000.
- Die MTU der Schnittstelle 10/2 ist 9216. Die MTU von VLAN 20 ist 9000. Auf der Schnittstelle 10/2 beträgt die MTU der mit VLAN 20 markierten Paketen 9000.
- Die MTU der Schnittstelle 10/1 ist 9216. Die MTU von VLAN 30 beträgt 1500. Auf der Schnittstelle 10/1 beträgt die MTU der mit VLAN 30 markierten Paketen 1500.
- Die MTU der Schnittstelle 10/2 ist 9216. Die MTU von VLAN 40 beträgt 1500. Auf der Schnittstelle 10/2 beträgt die MTU der mit VLAN 40 markierten Paketen 9000.

CL1, S1, S2 und alle Netzwerkgeräte zwischen CL1 und S1 oder S2 sind für Jumbo-Frames konfiguriert.

Da der HTTP-Verkehr auf TCP basiert, werden MSSs an jedem Endpunkt entsprechend für die Unterstützung von Jumbo-Frames festgelegt.

- Für die Verbindung zwischen CL1 und dem virtuellen Server LBVS-1 von NS1 wird das MSS auf NS1 in einem TCP-Profil festgelegt, das dann an LBVS-1 gebunden ist.

- Für die Verbindung zwischen einer SNIP-Adresse von NS1 und S1 wird die MSS auf NS1 in einem TCP-Profil festgelegt, das dann an den Dienst (SVC-S1) gebunden ist, der S1 auf NS1 darstellt.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: Jumbo-Frames Anwendungsfall 3 Beispieleinstellungen.

Im Folgenden ist der Verkehrsfluss von CL1 Anforderung an S1:

1. Der Client CL1 erstellt eine 20000-Byte-HTTP-Anforderung zum Senden an den virtuellen Server LBVS-1 von NS1.
2. CL1 öffnet eine Verbindung zu LBVS-1 von NS1. CL1 und NS1 tauschen beim Verbindungsaufbau ihre TCP-MSS-Werte aus.
3. Da der MSS-Wert von NS1 kleiner ist als die HTTP-Anforderung, segmentiert CL1 die Anforderungsdaten in Vielfaches von NS1 MSS und sendet diese Segmente in IP-Paketen, die als VLAN 10 gekennzeichnet sind, an NS1.
    - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Segment=NS1 MSS)] = [20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120
4. NS1 empfängt diese Pakete an Schnittstelle 10/1. NS1 akzeptiert diese Pakete, da die Größe dieser Pakete gleich oder kleiner ist als die effektive MTU (9000) der Schnittstelle 10/1 für mit VLAN 10 getaggte Pakete.
5. Aus den IP-Paketen stellt NS1 alle TCP-Segmente zur 20000-Byte-HTTP-Anforderung zusam-

men. NS1 verarbeitet diese Anfrage.

6. Der Load Balancing-Algorithmus von LBVS-1 wählt Server S1 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S1. NS1 und CL1 tauschen beim Verbindungsaufbau ihre jeweiligen TCP-MSS-Werte aus.
7. NS1 segmentiert die Anforderungsdaten in Vielfaches des MSS von S1 und sendet diese Segmente in IP-Paketen, die als VLAN 20 an S1 gekennzeichnet sind.
    - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Nutzlast = S1 MSS)] = [20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120

Im Folgenden ist der Verkehrsfluss der Reaktion von S1 auf CL1 dargestellt:

1. Server S1 erstellt eine 30000-Byte-HTTP-Antwort, die an die SNIP-Adresse von NS1 gesendet wird.
2. S1 segmentiert die Antwortdaten in ein Vielfaches des MSS von NS1 und sendet diese Segmente in IP-Paketen, die als VLAN 20 an NS1 gekennzeichnet sind. Diese IP-Pakete werden von der IP-Adresse von S1 bezogen und an die SNIP-Adresse von NS1 bestimmt.
    - Größe der ersten drei Pakete = [IP-Header + TCP-Header + (TCP-Segment = MSS-Größe von NS1)] = [20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 3120] = 3160
3. NS1 empfängt die Antwortpakete an Schnittstelle 10/2. NS1 akzeptiert diese Pakete, da ihre Größe dem effektiven MTU-Wert (9000) der Schnittstelle 10/2 für mit VLAN 20 getaggte Pakete entspricht oder kleiner ist.
4. Aus diesen IP-Paketen stellt NS1 alle TCP-Segmente zur 30000-Byte-HTTP-Antwort zusammen. NS1 verarbeitet diese Antwort.
5. NS1 segmentiert die Antwortdaten in Vielfache des MSS von CL1 und sendet diese Segmente in IP-Paketen, die als VLAN 10 gekennzeichnet sind, von der Schnittstelle 10/1 an CL1. Diese IP-Pakete werden von der IP-Adresse von LBVS bezogen und zur IP-Adresse von CL1 bestimmt.
    - Größe der ersten drei Pakete = [IP-Header + TCP-Header + [(TCP-Nutzlast = MSS-Größe von CL1)] = [20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 3120] = 3160

Konfigurationsaufgaben

In der folgenden Tabelle werden Aufgaben, Befehle und Beispiele zum Erstellen der erforderlichen Konfiguration auf der NetScaler Appliance aufgeführt: Jumbo-Frames Anwendungsfall 3 Konfigurationsaufgaben.

NetScaler Unterstützung für Microsoft Direct Access-Bereitstellung

May 11, 2023

Microsoft Direct Access ist eine Technologie, die es Remotebenutzern ermöglicht, sich nahtlos und sicher mit den internen Netzwerken des Unternehmens zu verbinden, ohne dass eine separate VPN-Verbindung hergestellt werden muss. Im Gegensatz zu VPN-Verbindungen, bei denen der Benutzer zum Öffnen und Schließen von Verbindungen eingreifen muss, stellt ein Direct Access-fähiger Client automatisch eine Verbindung zu den internen Netzwerken des Unternehmens her, sobald der Client eine Verbindung zum Internet herstellt.

Manage-Out ist eine Microsoft Direct Access-Funktion, mit der Administratoren innerhalb des Unternehmensnetzwerks eine Verbindung zu Direct Access-Clients außerhalb des Netzwerks herstellen und diese verwalten können (z. B. das Ausführen von Verwaltungsaufgaben wie das Planen von Dienstupdates und die Bereitstellung von Remote-Support).

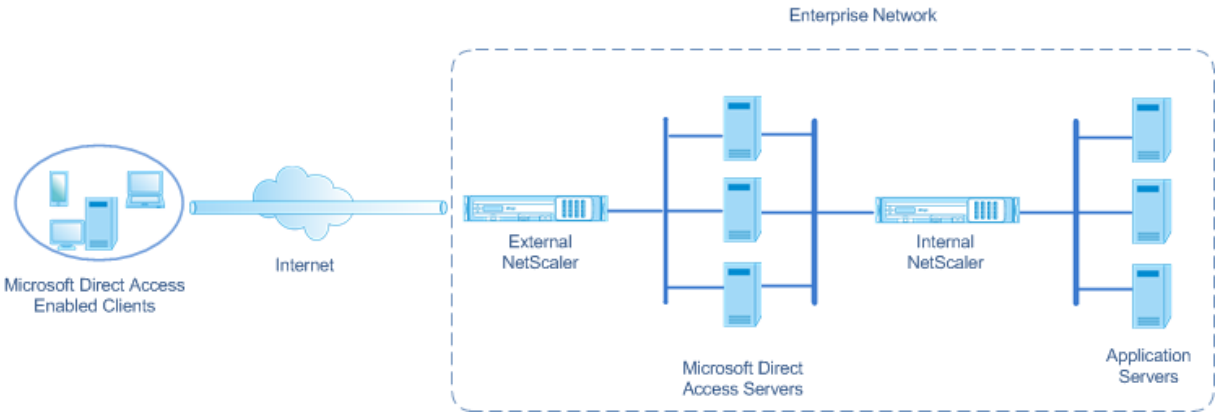
In einer Direct Access-Bereitstellung bieten NetScaler-Appliances hohe Verfügbarkeit, Skalierbarkeit, hohe Leistung und Sicherheit. Die NetScaler-Load-Balancing-Funktion sendet den Client-Datenverkehr über den am besten geeigneten Server. Die Appliances können den Manage-Out-Traffic auch über den richtigen Pfad weiterleiten, um den Client zu erreichen.

Architektur

Die Architektur einer Microsoft Direct Access-Bereitstellung besteht aus Direct Access-fähigen Clients, Direct Access-Servern, Anwendungsservern sowie internen und externen NetScaler-Appliances. Clients stellen über einen Direct Access-Server eine Verbindung zu einem Anwendungsserver her. Eine externe NetScaler-Appliance verteilt den Client-Datenverkehr zu einem Direct Access-Server, und eine interne NetScaler-Appliance leitet den Client-Datenverkehr vom Direct Access-Server an den Zielanwendungsserver weiter. Direct Access wird verwendet, um den IPv6-Verkehr des Clients über das IPv4-Netzwerk zu tunneln. Ein virtueller IPv4-Lastausgleichsserver auf der externen NetScaler-Appliance verteilt den getunnelten Datenverkehr des Clients auf einen der Direct Access-Server. Der Direct Access-Server extrahiert die IPv6-Pakete aus den IPv4-Paketen des empfangenen Clients und sendet sie über die interne NetScaler-Appliance an den Zielanwendungsserver. Die interne NetScaler-Appliance verfügt über Regeln für Weiterleitungssitzungen, wobei die Option Quell-Route-Cache aktiviert ist, um Layer-2- und Layer-3-Verbindungsinformationen über den Client-Verkehr vom Direct Access Server zu speichern. Die NetScaler-Appliance speichert die folgenden Layer-2- und Layer-3-Informationen in einer Tabelle, die als Quell-Route-Cache-Tabelle bezeichnet wird:

- Quell-IP-Adresse des empfangenen Pakets
- MAC-Adresse des Direct Access-Servers, der das Paket gesendet hat
- VLAN-ID der NetScaler-Appliance, die das Paket empfangen hat
- Schnittstellen-ID der NetScaler-Appliance, die das Paket empfangen hat

Die NetScaler-Appliance verwendet die Informationen in der Quell-Route-Cache-Tabelle, um eine Antwort an denselben Direct Access-Server weiterzuleiten, da sie über die Tunnelinformationen verfügt, um den Client zu erreichen. Außerdem verwendet die interne Appliance die Quell-Route-Cache-Tabelle, um den Verwaltungsdatenverkehr des Anwendungsservers an den entsprechenden Direct Access-Server weiterzuleiten, um einen bestimmten Client zu erreichen.



Konfiguration der internen NetScaler-Appliance in einer Microsoft Direct Access-Bereitstellung

Um die interne NetScaler-Appliance für die Weiterleitung der Antwort und Verwaltung des Datenverkehrs eines Anwendungsservers an das entsprechende Direct Access Gateway zu konfigurieren, konfigurieren Sie die Regeln für die Weiterleitung von Sitzungen. Setzen Sie in jeder Regel den Parameter sourceroutecache auf ENABLED.

So erstellen Sie eine Weiterleitungssitzungsregel mithilfe der Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

- **add forwardingSession** <name> ((<network> [\<netmask>]) | **-acl6name** <string> | **-aclname** <string>) **-sourceroutecache** (**ENABLED** | **DISABLED**]
- **show forwardingsession** <name>

Beispielkonfiguration:

Im folgenden Beispiel wird die Weiterleitungsregel MS-DA-FW-1 auf der internen NetScaler-Appliance erstellt. Die Weiterleitungssitzung speichert Layer-2- und Layer-3-Informationen für alle eingehenden IPv6-Pakete von einem Direct Access-Server, der dem Quell-IPv6-Präfix 2001:DB8::/96 entspricht.

```
1 > add forwardingSession MS-DA-FW-1 2001:DB8::/96 -sourceroutecache -
    ENABLED
2  Done
```


Quell-Route-Cache-Tabelle anzeigen

Sie können die Quell-Route-Cache-Tabelle anzeigen, um unerwünschte Verbindungen zwischen Direktzugriffsservern und Anwendungsservern zu überwachen oder zu erkennen.

Um die Quell-Route-Cache-Tabelle mit der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **Quellroute und Cachetable anzeigen**

Beispiel:

```
> show sourceroutecachetable
SOURCEIP            MAC                 VLAN    INTERFACE
2001:DB8:5001:10    56:53:24:3d:02:eb    30        1/2
2001:DB8:5003:30    60:54:35:3e:04:bd    60        1/3
Done
```

Löschen der Quell-Route-Cache-Tabelle

Sie können alle Einträge aus der Quell-Route-Cache-Tabelle auf einer NetScaler-Appliance löschen.

Um die Quell-Route-Cache-Tabelle mit der CLI zu löschen:

Geben Sie in der Befehlszeile Folgendes ein:

- **flush ns sourceroutecachetable**

Zugriffssteuerungslisten

May 11, 2023

Access Control Lists (ACLs) filtern den IP-Verkehr und schützen Ihr Netzwerk vor unbefugtem Zugriff. Eine ACL ist eine Reihe von Bedingungen, die der NetScaler auswertet, um zu bestimmen, ob der Zugriff zugelassen wird. Zum Beispiel möchte die Finanzabteilung wahrscheinlich nicht zulassen, dass andere Abteilungen wie Personalabteilung und Dokumentation auf ihre Ressourcen zugreifen, und diese Abteilungen möchten den Zugriff auf ihre Daten einschränken.

Wenn der NetScaler ein Datenpaket empfängt, vergleicht er die Informationen im Datenpaket mit den in der ACL angegebenen Bedingungen und erlaubt oder verweigert den Zugriff. Der Administrator der Organisation kann ACLs so konfigurieren, dass sie in den folgenden Verarbeitungsmodi funktionieren:

- Zulassen — Verarbeitet das Paket.
- BRIDGE — Überbrückt das Paket mit dem Ziel, ohne es zu verarbeiten. Das Paket wird direkt per Layer-2- und Layer-3-Weiterleitung gesendet.

- Ablehnen — das Paket fallen lassen.

ACL-Regeln sind die erste Verteidigungsstufe auf dem NetScaler.

NetScaler unterstützt die folgenden Typen von ACLs:

- **Einfache ACLs** filtern Pakete basierend auf ihrer Quell-IP-Adresse und optional ihrem Protokoll, ihrem Zielport oder ihrer Verkehrsdomäne. Jedes Paket, das die in der ACL angegebenen Merkmale aufweist, wird gelöscht.
- **Erweiterte ACLs** filtern Datenpakete basierend auf verschiedenen Parametern wie Quell-IP-Adresse, Quellport, Aktion und Protokoll. Eine erweiterte ACL definiert die Bedingungen, die ein Paket erfüllen muss, damit NetScaler das Paket verarbeiten, das Paket überbrücken oder das Paket löschen kann.

Nomenklatur

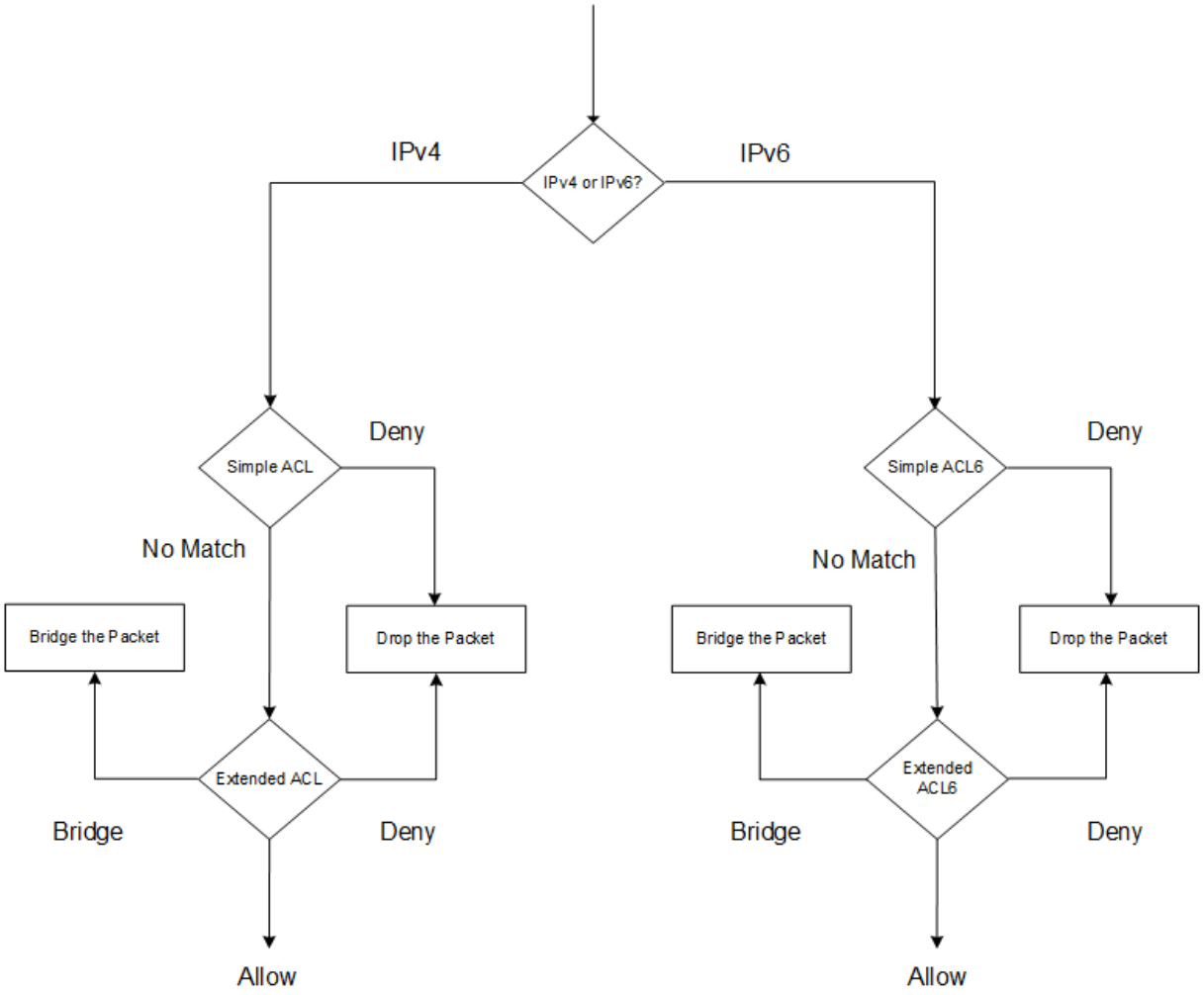
In den NetScaler-Benutzeroberflächen beziehen sich die Begriffe einfache ACL und erweiterte ACL auf ACLs, die IPv4-Pakete verarbeiten. Eine ACL, die IPv6-Pakete verarbeitet, wird als einfache ACL6 und/oder erweiterte ACL6 bezeichnet. Bei der Erörterung beider Typen werden in dieser Dokumentation manchmal beide als einfache ACLs oder erweiterte ACLs bezeichnet.

ACL-Priorität

Wenn sowohl einfache als auch erweiterte ACLs konfiguriert sind, werden eingehende Pakete zuerst mit den einfachen ACLs verglichen.

Der NetScaler ermittelt zunächst, ob es sich bei dem eingehenden Paket um ein IPv4- oder ein IPv6-Paket handelt, und vergleicht dann die Eigenschaften des Pakets mit einfachen ACLs oder einfachen ACL6s. Wenn eine Übereinstimmung gefunden wird, wird das Paket verworfen. Wenn keine Übereinstimmung gefunden wird, wird das Paket mit erweiterten ACLs oder erweiterten ACL6s verglichen. Wenn dieser Vergleich zu einer Übereinstimmung führt, wird das Paket wie in der ACL angegeben behandelt. Das Paket kann überbrückt, gelöscht oder zugelassen werden. Wenn keine Übereinstimmung gefunden wird, ist das Paket zulässig.

Abbildung 1. Einfache und erweiterte ACLs Flow Sequenz



Einfache ACLs und einfache ACL6s

May 11, 2023

Eine einfache ACL oder einfache ACL6 verwendet wenige Parameter und kann nur zum Löschen von IP-Paketen konfiguriert werden. Pakete können basierend auf ihrer Quell-IP-Adresse und optional ihres Protokolls, ihres Zielports oder ihrer Verkehrsdomäne gelöscht werden.

Wenn Sie eine einfache ACL oder eine einfache ACL6 erstellen, können Sie eine Time to Live (TTL) in Sekunden angeben, nach der die ACL abläuft. ACLs mit TTLs werden nicht gespeichert, wenn Sie die Konfiguration speichern. Sie können einfache ACLs und einfache ACL6s anzeigen, um deren Konfiguration zu überprüfen, und Sie können ihre Statistiken anzeigen.

Konfiguration einfacher ACLs und einfacher ACL6s

Die Konfiguration einer einfachen ACL oder einer einfachen ACL6 auf einem NetScaler kann die folgenden Aufgaben beinhalten.

- **Erstellen Sie einfache ACLs oder einfache ACL6s**. Erstellen einfacher ACLs oder einfacher ACL6s zum Löschen (Verweigern) von Paketen basierend auf ihrer Quell-IP-Adresse und optional ihrem Protokoll, ihrem Zielport oder ihrer Verkehrsdomäne.
- **Entfernen Sie einfache ACLs oder einfache ACL6s**. Diese ACLs können nach der Erstellung nicht geändert werden. Wenn Sie eine einfache ACL oder eine einfache ACL6 ändern müssen, müssen Sie sie entfernen und eine erstellen.

CLI-Verfahren

Um eine einfache ACL mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

```
1 - ns simpleacl <aclname> DENY -srcIP <ip_addr> [-destPort <port> -
    protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 - show ns simpleacl [<aclname>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add simpleacl rule1 DENY -srcIP 10.102.29.5 -TTL 600
2 Done
3 <!--NeedCopy-->
```

Um ein einfaches ACL6 mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

```
1 - add ns simpleacl6 <aclname> DENY - srcIPv6 <ipv6_addr|null> [-
    destPort <port> -protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 - show ns simpleacl6 [<aclname>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add ns simpleacl6 rule1 DENY - srcIPv6 3ffe:192:168:215::82 -
    destPort 80 -Protocol TCP -TTL 9000
2  Done
3 <!--NeedCopy-->
```

Um eine einzelne einfache ACL mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- **Herr ns simpleacl** <aclname>
- **zeig uns simpleacl**

Um ein einzelnes einfaches ACL6 mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- **rm ns simpleacl6**<aclname>
- **zeige uns simpleacl6**

Um alle einfachen ACLs mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- **klar ns simpleacl**
- **zeig uns simpleacl**

Um alle einfachen ACL6s mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

- **clear ns simpleacl6**
- **zeige uns simpleacl6**

GUI-Verfahren

Um eine einfache ACL mithilfe der GUI zu erstellen:

Navigieren Sie zu **System > Netzwerk > ACLs** und fügen Sie auf der Registerkarte **Einfache ACLs** eine neue einfache ACL hinzu.

Um ein einfaches ACL6 mit der GUI zu erstellen:

Navigieren Sie zu **System > Netzwerk > ACLs** und fügen Sie auf der Registerkarte **Einfache ACL6s** eine neue einfache ACL6 hinzu.

Um eine einzelne einfache ACL mithilfe der GUI zu entfernen:

Navigieren Sie zu **System > Netzwerk > ACLs** und löschen Sie auf der Registerkarte **Einfache ACLs** die einfache ACL.

Um ein einzelnes einfaches ACL6 mit der GUI zu entfernen:

Navigieren Sie zu **System > Netzwerk > ACLs** und löschen Sie auf der Registerkarte **Einfache ACL6s** die einfache ACL6.

Um alle einfachen ACLs mit der GUI zu entfernen:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.

2. Klicken Sie auf der Registerkarte **Einfache ACLs** in der Liste **Aktionen** auf **Löschen**.

Um alle einfachen ACL6s mit der GUI zu entfernen:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.
2. **Klicken Sie auf der Registerkarte**Simple ACL6s**in der Liste**Aktion**auf Löschen.**

Anzeigen einfacher ACL- und einfacher ACL6-Statistiken

Sie können die einfachen ACL-Statistiken (oder einfache ACL6) anzeigen, die die Anzahl der Übereinstimmungen, die Anzahl der Fehler und die Anzahl der konfigurierten einfachen ACLs enthalten.

In der folgenden Tabelle werden die Statistiken beschrieben, die Sie für einfache ACLs und einfache ACL6s anzeigen können.

Statistik	Zeigt an
ACL übereinstimmen	Pakete, die mit einer ACL übereinstimmen
ACL verpasst	Pakete, die keiner ACL entsprechen
Anzahl ACL	Anzahl der konfigurierten ACLs

CLI-Verfahren

Um einfache ACL-Statistiken mit der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **starte uns simpleacl**

Beispiel:

```
> stat ns simpleacl

SimpleACL Statistics

                                          Rate (/s)
                                             Total
SimpleACL hits                                  0
                        0
SimpleACL misses                                0
    51872
SimpleACLs count                               --
                        2
Done
<!--NeedCopy-->
```


Um einfache ACL6-Statistiken mit der CLI anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **starte uns simpleacl6**

GUI-Verfahren

Um einfache ACL-Statistiken mithilfe der GUI anzuzeigen:

Navigieren Sie zu System**>**Netzwerk**>**ACLs**und wählen Sie auf der Registerkarte**Einfache ACLs**die ACL aus und klicken Sie auf Statistiken.**

Um einfache ACL6-Statistiken mithilfe der GUI anzuzeigen:

Navigieren Sie zu **System > Netzwerk > ACLs**, wählen Sie auf der Registerkarte **Einfache ACL6s** die einfache ACL6 aus und klicken Sie auf **Statistik**.

Bestehende Verbindungen beenden

Bei einer einfachen ACL oder einfachen ACL6 blockiert der NetScaler alle neuen Verbindungen, die den in der ACL angegebenen Bedingungen entsprechen. Pakete, die sich auf bestehende Verbindungen beziehen, die vor der Erstellung der ACL hergestellt wurden, werden nicht blockiert. Um zuvor hergestellte Verbindungen zu beenden, die einer vorhandenen ACL entsprechen, können Sie einen Flush-Vorgang von der CLI oder der GUI aus ausführen.

Flush kann in den folgenden Fällen nützlich sein:

- Sie erhalten eine Liste mit IP-Adressen auf der schwarzen Liste und möchten den Zugriff dieser IP-Adressen auf den NetScaler vollständig blockieren. In diesem Fall erstellen Sie einfache ACLs oder einfache ACL6s, um neue Verbindungen von diesen IP-Adressen zu blockieren und dann alle vorhandenen Verbindungen zu leeren, die diesen Adressen zugeordnet sind.
- Sie möchten viele Verbindungen von einem bestimmten Netzwerk aus beenden, ohne sich die Zeit zu nehmen, sie einzeln zu beenden.

Voraussetzungen

- Wenn Sie Flush ausführen, durchsucht der NetScaler alle seine etablierten Verbindungen und beendet die Verbindungen, die den Bedingungen entsprechen, die in einer der einfachen ACLs angegeben sind, die auf dem ADC konfiguriert sind.
- Wenn Sie planen, mehr als eine einfache ACL zu erstellen und vorhandene Verbindungen zu leeren, die zu einer von ihnen passen, können Sie die Auswirkungen auf die Leistung

minimieren, indem Sie zuerst alle einfachen ACLs erstellen und dann nur einmal Flush ausführen.

CLI-Verfahren

Um alle bestehenden IPv4-Verbindungen, die mit einer Ihrer konfigurierten einfachen ACLs übereinstimmen, zu beenden, verwenden Sie die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **simplecal -SetSessions leeren**

Um alle bestehenden IPv6-Verbindungen, die mit Ihren konfigurierten einfachen ACL6s übereinstimmen, zu beenden, verwenden Sie die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **flush simpleacl6 - EST-Sitzungen**

GUI-Verfahren

Um alle bestehenden IPv4-Verbindungen, die mit einer Ihrer konfigurierten einfachen ACLs übereinstimmen, zu beenden, verwenden Sie die GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.
2. Klicken Sie auf der Registerkarte **Einfache ACLs** in der Liste **Aktionen** auf **Flush**.

Um alle bestehenden IPv6-Verbindungen, die mit Ihren konfigurierten einfachen ACL6s übereinstimmen, zu beenden, verwenden Sie die GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.
2. **Klicken Sie auf der Registerkarte**Simple ACL6s**in der Liste**Aktion**auf Flush.**

Erweiterte ACLs und erweiterte ACL6s

May 11, 2023

Erweiterte ACLs und erweiterte ACL6s bieten Parameter und Aktionen, die mit einfachen ACLs nicht verfügbar sind. Sie können Daten basierend auf Parametern wie Quell-IP-Adresse, Quellport, Aktion und Protokoll filtern. Sie können Aufgaben angeben, um ein Paket zuzulassen, ein Paket zu verweigern oder ein Paket zu überbrücken.

Erweiterte ACLs und ACL6s können nach ihrer Erstellung geändert werden, und Sie können ihre Prioritäten neu nummerieren, um die Reihenfolge anzugeben, in der sie ausgewertet werden.

Hinweis: Wenn Sie sowohl einfache als auch erweiterte ACLs konfigurieren, haben einfache ACLs Vorrang vor erweiterten ACLs.

Die folgenden Aktionen können für erweiterte ACLs und ACL6s ausgeführt werden: Ändern, Anwenden, Deaktivieren, Aktivieren, Entfernen und Umnummerieren (Priorität). Sie können erweiterte ACLs und ACL6s anzeigen, um ihre Konfiguration zu überprüfen, und Sie können ihre Statistiken anzeigen.

Sie können den NetScaler so konfigurieren, dass Details für Pakete protokolliert werden, die einer erweiterten ACL entsprechen.

Anwenden erweiterter ACLs und erweiterter ACL6s: Im Gegensatz zu einfachen ACLs und ACL6s funktionieren erweiterte ACLs und ACL6s, die auf dem NetScaler erstellt wurden, erst dann, wenn sie angewendet werden. Wenn Sie Änderungen an einer erweiterten ACL oder ACL6 vornehmen, z. B. das Deaktivieren der ACLs, das Ändern einer Priorität oder das Löschen der ACLs, müssen Sie die erweiterten ACLs oder ACL6 erneut anwenden. Sie müssen sie erneut anwenden, nachdem Sie die Protokollierung aktiviert haben. Das Verfahren zum Anwenden erweiterter ACLs oder ACL6s wendet alle ACLs erneut an. Wenn Sie beispielsweise erweiterte ACL-Regeln 1 bis 10 angewendet haben und dann Regel 11 erstellen und anwenden, werden die ersten 10 Regeln neu angewendet.

Wenn eine Sitzung über eine DENY-ACL verfügt, wird diese Sitzung beendet, wenn Sie die ACLs anwenden.

Erweiterte ACLs und ACL6s sind standardmäßig aktiviert. Wenn sie angewendet werden, beginnt der NetScaler, eingehende Pakete mit ihnen zu vergleichen. Wenn Sie sie jedoch deaktivieren, werden sie erst verwendet, wenn Sie sie wieder aktivieren, selbst wenn sie erneut angewendet werden.

Neunummerierung der Prioritäten von Extended ACLs und Extended ACL6: Prioritätsnummern bestimmen die Reihenfolge, in der erweiterte ACLs oder ACL6 mit einem Paket abgeglichen werden. Eine ACL mit einer niedrigeren Prioritätsnummer hat eine höhere Priorität. Es wird vor ACLs mit höheren Prioritätsnummern (niedrigere Prioritäten) ausgewertet, und die erste ACL, die mit dem Paket übereinstimmt, bestimmt die auf das Paket angewendete Aktion.

Wenn Sie eine erweiterte ACL oder ACL6 erstellen, weist der NetScaler ihm automatisch eine Prioritätsnummer zu, die ein Vielfaches von 10 ist, sofern Sie nichts anderes angeben. Wenn beispielsweise zwei erweiterte ACLs Prioritäten von 20 bzw. 30 haben und Sie möchten, dass eine dritte ACL einen Wert zwischen diesen Zahlen hat, können Sie ihr einen Wert von 25 zuweisen. Wenn Sie später die Reihenfolge beibehalten möchten, in der die ACLs ausgewertet werden, aber ihre Nummerierung auf ein Vielfaches von 10 zurücksetzen möchten, können Sie die Neunummerierungsprozedur verwenden.

Konfigurieren von erweiterten ACLs und Extended ACL6s

Die Konfiguration einer erweiterten ACL oder ACL6 auf einem NetScaler besteht aus den folgenden Aufgaben.

- **Erstellen Sie eine erweiterte ACL oder ACL6.** Erstellen Sie eine erweiterte ACL oder ACL6, um ein Paket entweder zuzulassen, zu verweigern oder zu überbrücken. Sie können eine IP-Adresse oder einen Bereich von IP-Adressen angeben, die mit den Quell- oder Ziel-IP-Adressen der Pakete übereinstimmen. Sie können ein Protokoll angeben, das mit dem Protokoll eingehender Pakete übereinstimmt.
- (Optional) **Ändern Sie eine erweiterte ACL oder ACL6**. Sie können erweiterte ACLs oder ACL6s ändern, die Sie zuvor erstellt haben. Oder wenn Sie einen vorübergehend außer Betrieb nehmen möchten, können Sie ihn deaktivieren und später wieder aktivieren.
- **Wenden Sie erweiterte ACLs oder ACL6s an**. Nachdem Sie eine erweiterte ACL oder ACL6 erstellt, geändert, deaktiviert oder erneut aktiviert oder gelöscht haben, müssen Sie die erweiterten ACLs oder ACL6 anwenden, um sie zu aktivieren.
- (Optional) **Nummerieren Sie die Prioritäten von erweiterten ACLs oder ACL6**neu. Wenn Sie ACLs mit Prioritäten konfiguriert haben, die kein Vielfaches von 10 sind und die Nummerierung auf ein Vielfaches von 10 wiederherstellen möchten, verwenden Sie die Neunummerierungsprozedur.

CLI-Verfahren

Um eine erweiterte ACL mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ns acl** <aclname> <aclaction> [-**srcIP** [\<operator>] <srcIPVal>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIP** [\<operator>] <destIPVal>] [-**destPort** [\<operator>] <destPortVal>] [-**TTL** \<positive_integer>] [-**srcMac** \<mac_addr>] [(-**protocol** \<protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** \<positive_integer>] [-**interface** \<interface_name>] [-**icmpType** \<positive_integer> [-**icmpCode** \<positive_integer>]] [-**priority** \<positive_integer>] [-**state** (ENABLED | DISABLED)] [-**logstate** (ENABLED | DISABLED) [-**ratelimit** \<positive_integer>]]
- **show ns acl** [\<aclName>]

So erstellen Sie eine erweiterte ACL6 mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ns acl6** <acl6name> <acl6action> [-**srcIPv6** [\<operator>] <srcIPv6Val>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIPv6** [\<operator>] <destIPv6Val>] [-**destPort** [\<operator>] <destPortVal>] [-**TTL** \<positive_integer>] [-**srcMac** \<mac_addr>] [(-**protocol** \<protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** \<positive_integer>] [-**interface** \<interface_name>] [-**icmpType** \<positive_integer> [-**icmpCode** \<positive_integer>]] [-**priority** \<positive_integer>] [-**state** (ENABLED | DISABLED)]

- **show ns acl6** [\<aclName>]

So ändern Sie eine erweiterte ACL mit der CLI:

Um eine erweiterte ACL zu ändern, geben Sie den Befehl **set ns acl**, den Namen der erweiterten ACL und die zu ändernden Parameter mit ihren neuen Werten ein.

So ändern Sie eine erweiterte ACL6 mit der CLI:

Um eine erweiterte ACL6 zu ändern, geben Sie den Befehl **set ns acl6**, den Namen des erweiterten ACL6 und die zu ändernden Parameter mit ihren neuen Werten ein.

So deaktivieren oder aktivieren Sie eine erweiterte ACL mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **disable ns acl** <aclname>
- **enable ns acl** <aclname>

So deaktivieren oder aktivieren Sie eine erweiterte ACL6 über die CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **disable ns acl6** <aclname>
- **enable ns acl6** <aclname>

So wenden Sie erweiterte ACLs über die CLIan:

Geben Sie in der Befehlszeile Folgendes ein:

- **apply ns acls**

So wenden Sie erweiterte ACL6s über die CLI an:

Geben Sie in der Befehlszeile Folgendes ein:

- **apply ns acls6**

So nummerieren Sie die Prioritäten erweiterter ACLs über die CLIneu:

Geben Sie in der Befehlszeile Folgendes ein:

- **ns acls neu nummerieren**

So nummerieren Sie die Prioritäten erweiterter ACL6s über die CLI neu:

Geben Sie in der Befehlszeile Folgendes ein:

- **renumber ns acls6**

GUI-Verfahren

So konfigurieren Sie eine erweiterte ACL mit der GUI:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und fügen Sie auf der Registerkarte **Erweiterte ACLs** eine neue erweiterte ACL hinzu oder bearbeiten Sie eine vorhandene erweiterte ACL. Um eine vorhandene erweiterte ACL zu aktivieren oder zu deaktivieren, wählen Sie sie aus und wählen Sie dann **Aktivieren** oder **Deaktivieren** aus der **Aktionsliste** aus.

So konfigurieren Sie eine erweiterte ACL6s mit der GUI:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und fügen Sie auf der Registerkarte **Erweiterte ACL6s** eine neue erweiterte ACL6 hinzu oder bearbeiten Sie eine vorhandene erweiterte ACL6. Um eine vorhandene erweiterte ACL6 zu aktivieren oder zu deaktivieren, wählen Sie es aus und wählen Sie dann **Aktivieren** oder **Deaktivieren** aus der **Aktionsliste** aus.

So wenden Sie erweiterte ACLs mit der GUI an:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACLs** in der Liste **Aktion** auf **Anwenden**.

So wenden Sie erweiterte ACL6s mit der GUI an:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACL6s** in der Liste **Aktion** auf **Anwenden**.

So nummerieren Sie die Prioritäten erweiterter ACLs über die GUI neu:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACLs** in der Liste **Aktion** auf **Priorität(n) neu nummerieren**.

So nummerieren Sie die Prioritäten von erweiterten ACL6s über die GUI neu:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACL6s** in der Liste **Aktion** auf **Priorität(n) neu nummerieren**.

Beispielkonfigurationen

Die folgende Tabelle zeigt Beispiele für die Konfiguration erweiterter ACL-Regeln über die Befehlszeilenschnittstelle: ACLS-Beispielkonfigurationen.

Protokollieren von erweiterten ACLs

Sie können den NetScaler so konfigurieren, dass Details für Pakete protokolliert werden, die erweiterten ACLs entsprechen.

Zusätzlich zum ACL-Namen enthalten die protokollierten Details paketspezifische Informationen wie Quell- und Ziel-IP-Adressen. Die Informationen werden je nach Art der aktivierten globalen Protokollierung (`syslog or nslog`) entweder in der Syslog-Datei oder in der Datei `nslog` gespeichert.

Die Protokollierung muss sowohl auf globaler Ebene als auch auf ACL-Ebene aktiviert sein. Die globale Einstellung hat Vorrang.

Um die Protokollierung zu optimieren, werden, wenn mehrere Pakete aus demselben Flow mit einer ACL übereinstimmen, nur die Details des ersten Pakets protokolliert, und der Zähler wird für jedes Paket, das zum selben Flow gehört, inkrementiert. Ein Flow ist definiert als eine Reihe von Paketen, die dieselben Werte für die Quell-IP-Adresse, die Ziel-IP-Adresse, den Quellport, den Zielport und die Protokollparameter aufweisen. Um eine Überschwemmung von Protokollmeldungen zu vermeiden, führt der NetScaler eine interne Ratenbegrenzung durch, sodass Pakete, die zum selben Flow gehören, nicht wiederholt protokolliert werden. Die Gesamtzahl der verschiedenen Flows, die zu einem bestimmten Zeitpunkt protokolliert werden können, ist auf 10.000 begrenzt.

Hinweis: Sie müssen ACLs anwenden, nachdem Sie die Protokollierung aktiviert haben.

CLI-Verfahren

So konfigurieren Sie die erweiterte ACL-Protokollierung mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Protokollierung zu konfigurieren und die Konfiguration zu überprüfen:

- **set ns acl** <aclName> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** \<positive_integer>]
- **apply acls**
- **show ns acl** [\<aclName>]

GUI-Verfahren

So konfigurieren Sie die erweiterte ACL-Protokollierung mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs** und öffnen Sie auf der Registerkarte **Erweiterte ACLs** die erweiterte ACL.
2. Legen Sie die folgenden Parameter fest:
   - **Protokollstatus**— Aktiviert oder deaktiviert die Protokollierung von Ereignissen, die sich auf die erweiterte ACL-Regel beziehen. Die Protokollmeldungen werden auf dem konfigurierten `syslog or auditlog`-Server gespeichert.
   - **Log Rate Limit**— Maximale Anzahl von Protokollmeldungen, die pro Sekunde generiert werden sollen. Wenn Sie diesen Parameter festlegen, müssen Sie den Parameter Log State aktivieren.

Beispiel-Konfiguration

```
> set ns acl restrict -logstate ENABLED -ratelimit 120
Warning: ACL modified, apply ACLs to activate change

> apply ns acls
Done
```



```
<!--NeedCopy-->
```

Protokollieren von erweiterten ACL6s

Sie können die NetScaler-Appliance so konfigurieren, dass Details für Pakete protokolliert werden, die einer erweiterten ACL6-Regel entsprechen. Zusätzlich zum ACL6-Namen enthalten die protokollierten Details paketspezifische Informationen wie Quell- und Ziel-IP-Adressen. Die Informationen werden entweder in einem Syslog oder einer Datei `nslog`gespeichert, abhängig von der Art der Protokollierung (`syslog or nslog`), die Sie in der NetScaler-Appliance konfiguriert haben.

Um die Protokollierung zu optimieren, werden nur die Details des ersten Pakets protokolliert, wenn mehrere Pakete aus demselben Fluss mit einem ACL6 übereinstimmen. Der Zähler wird für jedes andere Paket erhöht, das zum selben Flow gehört. Ein Flow ist definiert als eine Reihe von Paketen, die dieselben Werte für die folgenden Parameter haben:

- Quell-IP
- Ziel-IP
- Quell-Port
- Destination port
- Protokoll (TCP oder UDP)

Wenn ein eingehendes Paket nicht aus demselben Flow stammt, wird ein neuer Flow erstellt. Die Gesamtzahl der verschiedenen Flows, die zu einem bestimmten Zeitpunkt protokolliert werden können, ist auf 10.000 begrenzt.

CLI-Verfahren

So konfigurieren Sie die Protokollierung für eine erweiterte aCl6-Regel mit der CLI:

- Um die Protokollierung beim Hinzufügen der erweiterten ACL6-Regel zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add acl6** <acl6Name> <acl6action> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** \<positive_integer>]
  - **apply acls6**
  - **show acl6** [\<acl6Name>]
- Um die Protokollierung für eine vorhandene erweiterte ACL6-Regel zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set acl6** <acl6Name> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** \<positive_integer>]
  - **show acl6** [\<acl6Name>]
  - **apply acls6**

GUI-Verfahren

So konfigurieren Sie die erweiterte ACL6-Protokollierung mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und klicken Sie dann auf die Registerkarte **Extended ACL6s** .
2. Legen Sie die folgenden Parameter fest, während Sie eine vorhandene erweiterte ACL6-Regel hinzufügen oder ändern.
   - **Protokollstatus** — Aktivieren oder deaktivieren Sie die Protokollierung von Ereignissen im Zusammenhang mit der erweiterten ACL6s-Regel. Die Protokollmeldungen werden im konfigurierten Syslog- oder `auditlog`-Server gespeichert.
   - **Log Rate Limit**— Maximale Anzahl von Protokollmeldungen, die pro Sekunde generiert werden sollen. Wenn Sie diesen Parameter festlegen, müssen Sie den Parameter **Log State** aktivieren.

Beispiel-Konfiguration

```
> set acl6 ACL6-1 -logstate ENABLED -ratelimit 120
Done

> apply acls6
Done
<!--NeedCopy-->
```

Anzeigen erweiterter ACLs und erweiterter ACL6s-Statistiken

Sie können Statistiken zu erweiterten ACLs und ACL6s anzeigen.

In der folgenden Tabelle sind die Statistiken aufgeführt, die mit erweiterten ACLs und ACL6s verknüpft sind, sowie deren Beschreibungen.

Statistik	Spezifiziert
ACL-Übereinstimmungen zulassen	Pakete, die ACLs entsprechen, wobei der Verarbeitungsmodus auf Allow festgelegt ist. NetScaler verarbeitet diese Pakete.
NAT ACL Begegnungen	Pakete, die mit einer NAT-ACL übereinstimmen, was zu einer NAT-Sitzung führt.
ACL-Spiele verweigern	Pakete wurden gelöscht, weil sie ACLs mit dem Verarbeitungsmodus auf DENY festgelegt sind.

Statistik	Spezifiziert
Bridge ACL Übereinstimmungen	Pakete, die einer Bridge-ACL entsprechen, die im transparenten Modus die Dienstverarbeitung umgeht.
ACL-Übereinstimmungen	Pakete, die mit einer ACL übereinstimmen.
ACL verpasst	Pakete, die keiner ACL entsprechen.
ACL-Anzahl	Gesamtzahl der von Benutzern konfigurierten ACL-Regeln.
Effektive ACL-Anzahl	Gesamtzahl der intern konfigurierten effektiven ACL. Für eine erweiterte ACL mit einer Reihe von IP-Adressen erstellt die NetScaler-Appliance intern eine erweiterte ACL für jede IP-Adresse. Beispielsweise erstellt der NetScaler für eine erweiterte ACL mit 1000 IPv4-Adressen (Bereich oder Datensatz) intern 1000 erweiterte ACLs.

CLI-Verfahren

So zeigen Sie die Statistiken aller erweiterten ACLs mit der CLI an:

Geben Sie in der Befehlszeile Folgendes ein:

- **stat ns acl**

So zeigen Sie die Statistiken aller erweiterten ACL6s mit der CLI an:

Geben Sie in der Befehlszeile Folgendes ein:

- **stat ns acl6**

GUI-Verfahren

So zeigen Sie die Statistiken einer erweiterten ACL über die GUI an:

- Navigieren Sie zu **System > Netzwerk > ACLs**, wählen Sie auf der Registerkarte **Erweiterte ACLs** die erweiterte ACL aus und klicken Sie auf **Statistik**.

So zeigen Sie die Statistiken einer erweiterten ACL6 über die GUI an:

- Navigieren Sie zu **System > Netzwerk > ACLs**, wählen Sie auf der Registerkarte **Erweiterte ACL6s** die erweiterte ACL aus und klicken Sie auf **Statistik**.

Stateful-ACLs

Eine statusbehaftete ACL-Regel erstellt eine Sitzung, wenn eine Anforderung mit der Regel übereinstimmt, und erlaubt die resultierenden Antworten, auch wenn diese Antworten mit einer Ablehnungs-ACL-Regel in der NetScaler-Appliance übereinstimmen. Eine stateful ACL entlastet die Arbeit, mehr ACL-Regeln/Weiterleitungssitzungsregeln zu erstellen, um diese spezifischen Antworten zuzulassen.

Stateful ACLs können am besten in einer Edge-Firewall-Bereitstellung einer NetScaler-Appliance verwendet werden, die folgende Anforderungen erfüllt:

- Die NetScaler-Appliance muss Anfragen zulassen, die von internen Clients initiiert wurden, und die zugehörigen Antworten aus dem Internet.
- Die Appliance muss die Pakete aus dem Internet löschen, die nicht mit Clientverbindungen zusammenhängen.

Voraussetzungen

Bevor Sie statusbehaftete ACL-Regeln konfigurieren, beachten Sie die folgenden Punkte:

- Die NetScaler-Appliance unterstützt statusbehaftete ACL-Regeln und stateful ACL6-Regeln.
- In einem Hochverfügbarkeitssetup werden die Sitzungen für eine statusbehaftete ACL-Regel nicht mit dem sekundären Knoten synchronisiert.
- Sie können eine ACL-Regel nicht als stateful konfigurieren, wenn die Regel an eine NetScaler NAT-Konfiguration gebunden ist. Einige Beispiele für NetScaler NAT-Konfigurationen sind:
  - RNAT
  - Large Scale NAT (Großmaßstab NAT44, DS-Lite, Großmaßstab NAT64)
  - NAT64
  - Weiterleitungssitzung
- Sie können eine ACL-Regel nicht als statusbehaftet konfigurieren, wenn TTL und Established Parameter für diese ACL-Regel festgelegt sind.
- Die für eine stateful ACL-Regel erstellten Sitzungen existieren unabhängig von den folgenden ACL-Operationen bis zum Timeout weiterhin:
  - ACL entfernen
  - Deaktivieren Sie ACL
  - Löschen Sie ACL
- Stateful-ACLs werden für die folgenden Protokolle nicht unterstützt:
  - Aktiv FTP
  - TFTP

Konfigurieren von stateful IPv4-ACL-Regeln

Die Konfiguration einer stateful ACL-Regel besteht darin, den stateful Parameter einer ACL-Regel zu aktivieren.

So aktivieren Sie den stateful Parameter einer ACL-Regel über die CLI:

- Um den statusbehafteten Parameter beim Hinzufügen einer ACL-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add acl** <lname> ALLOW -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>
- Um den statusbehafteten Parameter einer vorhandenen ACL-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set acl** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>

So aktivieren Sie den stateful Parameter einer ACL-Regel über die GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und auf der Registerkarte **Erweiterte ACLs**.
2. Aktivieren Sie den **Stateful-Parameter**, während Sie eine vorhandene ACL-Regel hinzufügen oder ändern.

Beispiel-Konfiguration

```
> add acl ACL-1 allow -srciP 1.1.1.1 -stateful Yes

Done

> apply acls

Done

> show acl

1)         Name: ACL-1

    Action: ALLOW                          Hits: 0

    srcIP = 1.1.1.1

    destIP
```



```
18
19      srcMac:
20
21      Protocol:
22
23      Vlan:                                   Interface:
24
25      Active Status: ENABLED                   Applied Status: NOTAPPLIED
26
27      Priority: 10                             NAT: NO
28
29      TTL:
30
31      Log Status: DISABLED
32
33      Forward Session: NO
34
35      Stateful: YES
36  <!--NeedCopy-->
```

Konfigurieren Sie stateful ACL6-Regeln

Die Konfiguration einer stateful ACL6-Regel besteht darin, den stateful Parameter einer ACL6-Regel zu aktivieren.

So aktivieren Sie den stateful Parameter einer ACL6-Regel über die CLI:

- Um den statusbehafteten Parameter beim Hinzufügen einer ACL6-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add acl6** <name> ALLOW -stateful (ENABLED | DISABLD)
  - **apply acls6**
  - **show acl6** <name>
- Um den statusbehafteten Parameter einer vorhandenen ACL6-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set acl6** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls6**
  - **show acl6** <name>

So aktivieren Sie den stateful Parameter einer ACL6-Regel über die GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und auf der Registerkarte **Erweiterte ACL6s** .
2. Aktivieren Sie den **Stateful-Parameter**, während Sie eine vorhandene ACL6-Regel hinzufügen oder ändern.

Beispiel-Konfiguration

```
>  add acl6 ACL6-1 allow -srcipv6 1000::1  - stateful Yes

Done

>  apply acls6

Done

> show acl6

1)    Name: ACL6-1

    Action: ALLOW                          Hits: 0

    srcIPv6 = 1000::1

    destIPv6

    srcMac:

    Protocol:

    Vlan:                                 Interface:

    Active Status: ENABLED                 Applied Status: NOTAPPLIED

    Priority: 10                           NAT: NO

    TTL:

    Forward Session: NO

    Stateful: YES
<!--NeedCopy-->
```

Datensatzbasierte erweiterte ACLs

Viele ACLs sind in einem Unternehmen erforderlich. Das Konfigurieren und Verwalten vieler ACLs ist schwierig und umständlich, wenn sie häufige Änderungen erfordern.

Eine NetScaler-Appliance unterstützt Datensätze in erweiterten ACLs. Dataset ist eine vorhandene Funktion einer NetScaler-Appliance. Ein Datensatz ist ein Array von indizierten Mustern von Typen:

Zahl (Ganzzahl), IPv4-Adresse oder IPv6-Adresse.

Die Unterstützung von Datensätzen in erweiterten ACLs ist nützlich, um mehrere ACL-Regeln zu erstellen, die gemeinsame ACL-Parameter erfordern.

Während Sie eine ACL-Regel erstellen, können Sie anstelle der allgemeinen Parameter ein Dataset angeben, das diese allgemeinen Parameter enthält.

Alle am Datensatz vorgenommenen Änderungen werden automatisch in den ACL-Regeln wiedergegeben, die diesen Datensatz verwenden. ACLs mit Datensätzen sind einfacher zu konfigurieren und zu verwalten. Sie sind auch kleiner und einfacher zu lesen als die herkömmlichen ACLs.

Derzeit unterstützt die NetScaler-Appliance nur die folgenden Arten von Datensätzen für die erweiterten ACLs:

- IPv4-Adresse (zur Angabe der Quell-IP-Adresse oder der Ziel-IP-Adresse oder beides für eine ACL-Regel)
- number (zur Angabe des Quellports oder des Zielports oder beides für eine ACL-Regel)

Voraussetzungen

Beachten Sie vor dem Konfigurieren von datensatzbasierten erweiterten ACL-Regeln die folgenden Punkte:

- Stellen Sie sicher, dass Sie mit der Dataset-Funktion einer NetScaler-Appliance vertraut sind. Weitere Informationen zu Datensätzen finden Sie unter Mustersätze und Datensätze.
- Die NetScaler-Appliance unterstützt Datasets nur für erweiterte IPv4-ACLs.
- Die NetScaler-Appliance unterstützt nur die folgenden Arten von Datensätzen für die erweiterten ACLs:
  - IPv4-Adresse
  - number
- Die NetScaler-Appliance unterstützt datensatzbasierte erweiterte ACLs für alle NetScaler-Setups: Standalone, Hochverfügbarkeit und Cluster.
- Für eine erweiterte ACL mit Datensätzen, die Bereiche enthalten, erstellt die NetScaler-Appliance intern eine erweiterte ACL für jede Kombination der Datensatzwerte.
  - **Beispiel 1**: Für eine IPv4-Datensatzbasierte erweiterte ACL mit 1000 IPv4-Adressen, die an den Datensatz gebunden sind und der Datensatz auf den Quell-IP-Parameter festgelegt ist, erstellt die NetScaler-Appliance intern 1000 erweiterte ACLs.
  - **Beispiel 2**: Eine datensatzbasierte erweiterte ACL mit folgenden Parametern:
    - Die Quell-IP ist auf einen Datensatz mit 5 IP-Adressen festgelegt.
    - Die Ziel-IP ist auf einen Datensatz mit 5 IP-Adressen festgelegt.

    * Der Quellport ist auf einen Datensatz mit 5 Ports eingestellt.
    * Der Zielport ist auf einen Datensatz mit 5 Ports festgelegt.

  Die NetScaler-Appliance erstellt intern 625 erweiterte ACLs. Jede dieser internen ACLs enthält eine eindeutige Kombination der oben genannten vier Parameterwerte.

- Die NetScaler-Appliance unterstützt maximal 10K erweiterte ACLs. Für eine IPv4-Dataset-basierte erweiterte ACL mit einer Reihe von IP-Adressen, die an den Datensatz gebunden sind, erstellt die NetScaler-Appliance keine internen ACLs, sobald die Gesamtzahl der erweiterten ACLs die maximale Grenze erreicht hat.
- Die folgenden Zähler sind im Rahmen der erweiterten ACL-Statistik vorhanden:

    * **ACL-Zählung**. Gesamtzahl der von Benutzern konfigurierten ACL-Regeln.
    * **Effektive ACL-Anzahl**. Gesamtzahl der effektiven ACL-Regeln, die die NetScaler-Appliance intern konfiguriert.

  Weitere Informationen finden Sie unter Anzeigen von erweiterten ACL und erweiterten ACL6s-Statistiken.

- Die NetScaler-Appliance unterstützt keine Vorgänge `set` und `unset` zum Verbinden/Dissoziieren von Datensätzen mit den Parametern einer erweiterten ACL. Sie können die ACL-Parameter nur während des Vorgangs `add` auf ein Dataset einstellen.

Konfigurieren von datensatzbasierten erweiterten ACLs

Das Konfigurieren einer auf Dataset basierenden erweiterten ACL-Regel besteht aus den folgenden Aufgaben:

- **Fügen Sie einen Datensatz hinzu**. Ein Datensatz ist ein Array von indizierten Mustern von Typen: Zahl (Ganzzahl), IPv4-Adresse oder IPv6-Adresse. In dieser Aufgabe erstellen Sie einen Datasetyp, z. B. einen Datensatz vom Typ IPv4.
- **Binden Sie Werte an das Dataset**. Geben Sie einen Wert oder einen Wertebereich für das Dataset an. Die angegebenen Werte müssen vom gleichen Typ wie der Dataset-Typ sein. Sie können beispielsweise eine IPv4-Adresse oder einen IPv4-Adressbereich oder einen IPv4-Adressbereich in CIDR-Notation für eine IPv4-Datenmenge angeben.
- **Fügen Sie eine erweiterte ACL hinzu und legen Sie ACL-Parameter für das Dataset fest**. Fügen Sie eine erweiterte ACL hinzu und legen Sie die erforderlichen ACL-Parameter für den Datensatz fest. Diese Einstellung führt dazu, dass die Parameter auf die im Datensatz angegebenen Werte festgelegt sind.
- **Wenden Sie erweiterte ACLs an**. Wenden Sie die ACLs an, um neue oder geänderte erweiterte ACLs zu aktivieren.

So fügen Sie ein Richtlinien-Dataset mit der CLI hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- **add policy dataset** <name> <type>
- **show policy dataset**

So binden Sie ein Muster mit der CLI an den Datensatz:

Geben Sie in der Befehlszeile Folgendes ein:

- **bind policy dataset** <name> <value> [-endRange \<string>]
- **show policy dataset**

So fügen Sie eine erweiterte ACL hinzu und legen die ACL-Parameter über die Befehlszeilenschnittstelle auf das Dataset fest:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ns acl** <aclname> <aclaction> [-**srcIP** [\<operator>] <srcIPVal>] [-**srcPort** [\<operator>] <srcPortVal>] [-**destIP** [\<operator>] <destIPVal>] [-**destPort** [\<operator>] <destPortVal>] …
- **show acls**

So wenden Sie erweiterte ACLs mithilfe der CLI an:

Geben Sie in der Befehlszeile Folgendes ein:

- **apply acls**

Beispiel-Konfiguration

In der folgenden Beispielkonfiguration einer datensatzbasierten erweiterten ACL werden zwei IPv4-Datensätze `DATASET_IP_ACL_1` und `DATASET_IP_ACL_2` erstellt. Zwei Port-Datensätze `DATASET_PORT_ACL_1` und `DATASET_PORT_ACL_1` werden erstellt.

Zwei IPv4-Adressen: 192.0.2.30 und 192.0.2.60 sind an gebunden `DATASET_IP_ACL_1`. Zwei IPv4-Adressbereiche: (198.51.100.15 - 45) und (203.0.113.60-90) sind an `DATASET_IP_ACL_2` gebunden. `DATASET_IP_ACL_1` wird dann für den Parameter `srcIP` und `DATASET_IP_ACL_1` für den Parameter `destIP`vder erweiterten ACL `ACL-1`vangegeben.

Zwei Portnummern: 2001 und 2004, sind an gebunden `DATASET_PORT_ACL_1`. Zwei Portbereiche: (5001-5040) und (8001-8040) sind an `DATASET-PORT-ACL-2` gebunden. `DATASET_IP_ACL_1` wird dann für den Parameter `srcIP` und `DATASET_IP_ACL_1` für den Parameter `destIP` der erweiterten ACL`ACL-1` angegeben.

```
add policy dataset DATASET_IP_ACL_1 IPV4
add policy dataset DATASET_IP_ACL_2 IPV4

```



```
add policy dataset DATASET_PORT_ACL_1 NUM
add policy dataset DATASET_PORT_ACL_2 NUM

bind dataset DATASET_IP_ACL_1 192.0.2.30
bind dataset DATASET_IP_ACL_1 192.0.2.60
bind dataset DATASET_IP_ACL_2 198.51.100.15 -endrange 198.51.100.45
bind dataset DATASET_IP_ACL_2 203.0.113.1/24

bind dataset DATASET_PORT_ACL_1 2001
bind dataset DATASET_PORT_ACL_1 2004
bind dataset DATASET_PORT_ACL_2 5001 -endrange 5040
bind dataset DATASET_PORT_ACL_2 8001 -endrange 8040

add ns acl ACL-1 ALLOW -srcIP DATASET_IP_ACL_1 -destIP DATASET_IP_ACL_2
-srcPort DATASET_PORT_ACL_1 -destPort DATASET_PORT_ACL_2  - protocol TCP
<!--NeedCopy-->
```

MAC-Adress-Platzhaltermaske für ACLs

August 19, 2021

Ein Platzhaltermasken-Parameter wurde für erweiterte ACLs und ACL6s eingeführt und wird zusammen mit dem Quell-MAC-Adressparameter verwendet, um einen Bereich von MAC-Adressen zu definieren, die mit der Quell-MAC-Adresse eingehender Pakete übereinstimmen.

Platzhaltermasken geben an, welche Hexadezimalziffern der MAC-Adresse verwendet werden und welche Hexadezimalziffern ignoriert werden. Der Parameter Platzhaltermaske gibt eine Reihe von Einsen und Nullen an und hat eine Länge von 12 Ziffern. Jede Ziffer ist eine Maske für die entsprechende hexadezimale Ziffer der MAC-Adresse. Eine Nullziffer in der Platzhaltermaske gibt an, dass die entsprechende Hexadezimalziffer der MAC-Adresse berücksichtigt werden muss, und eine Ziffer gibt an, dass die entsprechende Hexadezimalziffer ignoriert werden soll.

Die Platzhaltermaske muss die folgenden Bedingungen erfüllen:

- Hat nur eine Reihe von Nullen
- Hat nur eine Reihe von
- Beginnen Sie mit einer Reihe von Nullen

Im Folgenden finden Sie einige Beispiele für gültige Platzhaltermasken:

- 000000111111
- 000000011111
- 000011111111

Im Folgenden finden Sie einige Beispiele für ungültige Platzhaltermasken:

- 000000111100
- 111110000000
- 010101010101

Für eine ACL definiert eine Platzhaltermaske 000000111111 für MAC-Adresse 96:fa:95:1d:67:4a den MAC-Adressbereich 96:FA:95:00:00:00 - 96:FA:95:FF:FF:FF. Dieser MAC-Adressbereich wird mit der Quell-MAC-Adresse der eingehenden Pakete abgeglichen.

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer ACL-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add ns acl <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl <aclname>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add ns acl ACL-1 ALLOW  -protocol TCP  -srcport 2000-3000 -srcMac 96:fa
     :95:1d:67:4a
2   -srcMacMask 000000111111
3 Done
4 <!--NeedCopy-->
```

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer ACL6-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add ns acl6 <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl6 <acl6name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add ns acl6 ACL6-1 ALLOW -destIPv6 2001::45 -srcMac 96:fa:90:1d:67:4a
2  -srcMacMask 000000001111
3 Done
4 <!--NeedCopy-->
```

Datenverkehr auf internen Ports blockieren

May 11, 2023

Standardmäßig blockiert eine NetScaler-Appliance keine Art von internem Datenverkehr, selbst wenn ACL-Regeln verwendet werden.

In der folgenden Tabelle sind die internen Datenverkehrstypen aufgeführt, die eine NetScaler-Appliance auch mit ACL-Regeln nicht blockiert:

NetScaler-Setup	Protokoll	Ziel-Port	Ziel-IP-Adresse
Alle	TCP	3008–3011	NSIP oder SNIP
Alle	TCP	179	NSIP oder SNIP
Alle	UDP	520	NSIP oder SNIP
Hohe Verfügbarkeit	UDP	3003	NSIP
Hohe Verfügbarkeit	TCP	22	NSIP
Cluster	UDP	7000	NSIP

Diese Funktion, die zuvor genannten Datenverkehrstypen nicht zu blockieren, wird durch die Standardeinstellung des globalen Layer-3 `Implicit ACL Allow` (`implicitACLAllow`)-Parameters festgelegt.

Sie können diesen Parameter deaktivieren, wenn Sie die zuvor genannten Datenverkehrstypen mit den ACL-Regeln blockieren möchten. Eine Appliance in einem Hochverfügbarkeitssetup macht eine Ausnahme für ihren Partnerknoten (primär oder sekundär). Es blockiert nicht den Datenverkehr von diesem Knoten.

So deaktivieren oder aktivieren Sie diesen Parameter mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set l3param** -**implicitACLAllow** [ENABLED|DISABLED]
- **sh l3param**

Hinweis: Der Parameter implicitACLAllow ist standardmäßig aktiviert.

Beispiel:

```
> set l3param -implicitACLAllow DISABLED
Done
<!--NeedCopy-->
```


IP-Routing

May 11, 2023

NetScaler-Appliances unterstützen sowohl dynamisches als auch statisches Routing. Da einfaches Routing nicht die Hauptaufgabe eines NetScaler ist, besteht das Hauptziel der Ausführung dynamischer Routing-Protokolle darin, Route Health Injection (RHI) zu aktivieren, sodass ein Upstream-Router aus mehreren Routen zu einem topografisch verteilten virtuellen Server die beste auswählen kann.

Die meisten NetScaler-Implementierungen verwenden einige statische Routen, um den Routing-Overhead zu reduzieren. Sie können statische Backup-Routen erstellen und Routen überwachen, um den automatischen Switchover für den Fall zu aktivieren, dass eine statische Route ausfällt. Sie können auch Gewichtungen zuweisen, um den Lastenausgleich zwischen statischen Routen zu erleichtern, Nullrouten erstellen, um Routingschleifen zu vermeiden, und statische IPv6-Routen konfigurieren. Sie können richtlinienbasierte Routen (PBRs) konfigurieren, für die Routing-Entscheidungen auf von Ihnen angegebenen Kriterien basieren.

Dynamische Routen konfigurieren

May 11, 2023

Wenn ein dynamisches Routing-Protokoll aktiviert ist, überwacht der entsprechende Routing-Prozess Routenaktualisierungen und kündigt Routen an. Routing-Protokolle ermöglichen es einem Upstream-Router, die Equal Cost Multipath (ECMP) -Technik zu verwenden, um den Datenverkehr auf identische virtuelle Server zu verteilen, die auf zwei eigenständigen NetScaler-Appliances gehostet werden. Dynamisches Routing auf einer NetScaler-Appliance verwendet drei Routingtabellen. In einem Setup mit hoher Verfügbarkeit spiegeln die Routingtabellen auf der sekundären Appliance die auf der primären Appliance.

Informationen zu Befehlsreferenzhandbüchern und nicht unterstützten Befehlen für das dynamische Routingprotokoll finden Sie unter Befehlsreferenzhandbücher für das dynamische Routing-Protokoll und nicht unterstützte Befehle.

NetScaler unterstützt die folgenden Protokolle:

- Routing Information Protocol (RIP) Version 2
- Öffnen Sie Shortest Path First (OSPF) Version 2
- Border Gateway Protocol (BGP)
- Routing Information Protocol der nächsten Generation (RiPNG) für IPv6
- Öffnen Sie Shortest Path First (OSPF) Version 3 für IPv6
- ISIS-Protokoll

Sie können mehrere Protokolle gleichzeitig aktivieren.

Routing-Tabellen in NetScaler

In einer NetScaler-Appliance enthalten die NetScaler-Kernel-Routingtabelle, die FreeBSD-Kernel-Routing-Tabelle und die NSM-FIB-Routingtabelle jeweils unterschiedliche Routen und dienen einem anderen Zweck. Sie kommunizieren miteinander, indem sie UNIX-Routing-Sockets verwenden. Routenaktualisierungen werden nicht automatisch von einer Routingtabelle an eine andere weitergegeben. Sie müssen die Weitergabe von Routenaktualisierungen für jede Routingtabelle konfigurieren.

NS-Kernel-Routingtabelle

Die NS-Kernel-Routing-Tabelle enthält Subnetzrouten, die dem NSIP und jedem SNIP und MIP entsprechen. Normalerweise sind in der NS-Kernel-Routing-Tabelle keine Routen vorhanden, die VIPs entsprechen. Die Ausnahme ist ein VIP, das mithilfe des Befehls add ns ip hinzugefügt und mit einer anderen Subnetzmaske als 255.255.255.255 konfiguriert wurde. Wenn mehrere IP-Adressen zu demselben Subnetz gehören, werden sie als eine einzige Subnetzroute abstrahiert. Darüber hinaus enthält diese Tabelle eine Route zum Loopback-Netzwerk (127.0.0.0) und alle statischen Routen, die über die CLI (CLI) hinzugefügt wurden. Die Einträge in dieser Tabelle werden vom NetScaler bei der Paketweiterleitung verwendet. Über die CLI können sie mit dem Befehl show route überprüft werden.

FreeBSD-Routingtabelle

Der einzige Zweck der FreeBSD-Routingtabelle besteht darin, die Initiierung und Beendigung des Verwaltungsverkehrs (Telnet, SSH usw.) zu erleichtern. In einer NetScaler-Appliance sind diese Anwendungen eng mit FreeBSD verbunden, und es ist unerlässlich, dass FreeBSD über die notwendigen Informationen verfügt, um den Datenverkehr zu und von diesen Anwendungen abzuwickeln. Diese Routingtabelle enthält eine Route zum NSIP-Subnetz und eine Standardroute. Darüber hinaus fügt FreeBSD Routen vom Typ WasCloned (W) hinzu, wenn der NetScaler Verbindungen zu Hosts in lokalen Netzwerken aufbaut. Aufgrund des hochspezialisierten Nutzens der Einträge in dieser Routingtabelle Bypass alle anderen Route-Updates aus dem NS-Kernel und den NSM-FIB-Routingtabellen die FreeBSD-Routingtabelle. Ändern Sie es nicht mit dem Befehl route. Die FreeBSD-Routingtabelle kann mit dem Befehl netstat von jeder UNIX-Shell aus überprüft werden.

Netzwerkdienstmodul (NSM) FIB

Die NSM-FIB-Routingtabelle enthält die anzeigbaren Routen, die von den dynamischen Routing-Protokollen an ihre Peers im Netzwerk verteilt werden. Es kann enthalten:

- **Verbundene Strecken**. IP-Subnetze, die direkt vom NetScaler aus erreichbar sind. In der Regel sind Routen, die dem NSIP-Subnetz entsprechen, und Subnetze, über die Routing-Protokolle aktiviert sind, in NSM FIB als verbundene Routen vorhanden.
- **Kernel-Routen**. Alle VIP-Adressen, auf denen die Option -hostRoute aktiviert ist, sind in NSM FIB als Kernel-Routen vorhanden, sofern sie die erforderlichen RHI-Levels erfüllen. Darüber hinaus enthält NSM FIB alle auf der CLI konfigurierten statischen Routen, für die die Option - advertise aktiviert ist. Wenn der NetScaler im SRADV-Modus (Static Route Advertisement) arbeitet, sind alternativ alle auf der CLI konfigurierten statischen Routen in NSM FIB vorhanden. Diese statischen Routen sind in NSM FIB als Kernel-Routen gekennzeichnet, da sie eigentlich zur NS-Kernel-Routing-Tabelle gehören.
- **Statische Routen**. Normalerweise ist jede in VTYSH konfigurierte statische Route in NSM FIB vorhanden. Wenn die administrativen Entfernungen von Protokollen geändert werden, ist dies möglicherweise nicht immer der Fall. Ein wichtiger Punkt, den es zu beachten gilt, ist, dass diese Routen niemals in die NS-Kernel-Routing-Tabelle gelangen können.
- **Gelernte Routen**. Wenn der NetScaler so konfiguriert ist, dass er Routen dynamisch lernt, enthält die NSM-FIB Routen, die von den verschiedenen dynamischen Routing-Protokollen gelernt wurden. Von OSPF erlernte Routen bedürfen jedoch einer speziellen Verarbeitung. Sie werden nur dann auf FIB heruntergeladen, wenn die Option fib-install für den OSPF-Prozess aktiviert ist. Dies kann über die Router-Config-Ansicht in VTYSH erfolgen.

Dynamisches Routing in einem Hochverfügbarkeits-Setup

In einem Hochverfügbarkeits-Setup führt der primäre Knoten den Routing-Prozess aus und leitet Routing-Tabellenaktualisierungen an den sekundären Knoten weiter. Die Routingtabelle des sekundären Knotens spiegelt die Routingtabelle des primären Knotens wider.

Ununterbrochene Weiterleitung

Nach dem Failover benötigt der sekundäre Knoten einige Zeit, um das Protokoll zu starten, die Routen zu erlernen und seine Routingtabelle zu aktualisieren. Dies wirkt sich jedoch nicht auf das Routing aus, da die Routingtabelle auf dem sekundären Knoten mit der Routingtabelle auf dem primären Knoten identisch ist. Diese Betriebsart wird als Non-Stop-Forwarding bezeichnet.

Mechanismus zur Vermeidung von Schwarzen Löchern

Nach dem Failover injiziert der neue Primärknoten alle seine VIP-Routen in den Upstream-Router. Dieser Router behält jedoch die Routen des alten Primärknotens 180 Sekunden lang bei. Da der Router sich des Failovers nicht bewusst ist, versucht er, den Datenverkehr zwischen den beiden Knoten auszugleichen. In den 180 Sekunden, bevor die alten Routen ablaufen, sendet der Router die Hälfte des Datenverkehrs an den alten, inaktiven Primärknoten, der praktisch ein schwarzes Loch darstellt.

Um dies zu verhindern, weist der neue primäre Knoten beim Einfügen einer Route eine Metrik zu, die geringfügig niedriger ist als die, die vom alten primären Knoten angegeben wurde.

Schnittstellen für die Konfiguration von dynamischem Routing

Um dynamisches Routing zu konfigurieren, können Sie entweder die GUI oder eine Befehlszeilenschnittstelle verwenden. Der NetScaler unterstützt zwei unabhängige Befehlszeilenschnittstellen: die CLI und die Virtual Teletype Shell (VTYSH). Die CLI ist die native Shell der Appliance. VTYSH wird von ZeBos verfügbar gemacht. Die NetScaler Routing Suite basiert auf ZebOS, der kommerziellen Version von GNU Zebra.

> **Hinweis:**
>
> Citrix empfiehlt, VTYSH für alle Befehle zu verwenden, mit Ausnahme derjenigen, die nur in der CLI konfiguriert werden können. Die Verwendung der CLI sollte im Allgemeinen auf Befehle zur Aktivierung der Routing-Protokolle, zur Konfiguration der Host-Route-Werbung und zum Hinzufügen statischer Routen für die Paketweiterleitung beschränkt sein.

Referenzhandbücher für Dynamic Routing-Protokoll und nicht unterstützte Befehle

In der folgenden Tabelle sind Links für Befehlsreferenzhandbücher für verschiedene dynamische Routingprotokolle und nicht unterstützte Befehle auf der NetScaler Appliance aufgeführt: Referenzhandbücher für dynamische Routingprotokolle und nicht unterstützte Befehle.

RIP konfigurieren

May 11, 2023

Das Routing Information Protocol (RIP) ist ein Distance Vector-Protokoll. Der NetScaler unterstützt RIP, wie in RFC 1058 und RFC 2453 definiert. RIP kann in jedem Subnetz ausgeführt werden.

Nachdem Sie RIP aktiviert haben, müssen Sie die Ankündigung von RIP-Routen konfigurieren. Zur Problembehandlung können Sie die RIP-Propagierung einschränken. Sie können die RIP-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

RIP aktivieren und deaktivieren

Verwenden Sie eines der folgenden Verfahren, um RIP zu aktivieren oder zu deaktivieren. Nachdem Sie RIP aktiviert haben, startet die NetScaler-Appliance den RIP-Prozess. Nachdem Sie RIP deaktiviert haben, stoppt die Appliance den RIP-Prozess.

So aktivieren oder deaktivieren Sie das RIP-Routing mithilfe der CLI:

Geben Sie in der Befehlszeile einen der folgenden Befehle ein, um RIP zu aktivieren oder zu deaktivieren:

- **enable ns feature RIP**
- **disable ns feature RIP**

RIP-Routing mithilfe der GUI aktivieren oder deaktivieren:

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie in der Gruppe **Modi und Funktionen** auf **Erweiterte Funktionen ändern**.
2. Wählen oder deaktivieren Sie die Option **RIP-Routing**.

Werberouten

RIP ermöglicht es einem Upstream-Router, den Datenverkehr zwischen zwei identischen virtuellen Servern, die auf zwei eigenständigen NetScaler-Appliances gehostet werden, auszugleichen. Route-Werbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem NetScaler befinden.

Um RIP so zu konfigurieren, dass Routen mithilfe der VTYSH-Befehlszeile angekündigt werden:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router rip	Starten Sie den RIP-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
redistribute static	Verteilen Sie statische Routen neu.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
```



```
<!--NeedCopy-->
```

Beschränkung von RIP-Weiterleitungen

Wenn Sie Probleme mit Ihrer Konfiguration beheben müssen, können Sie den Nur-Listenmodus auf jeder beliebigen Schnittstelle konfigurieren.

RIP-Propagierung mithilfe der VTYSH-Befehlszeile einschränken:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router rip	Starten Sie den RIP-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
passive-interface < vlan_name>	Unterdrückt Routing-Aktualisierungen an Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Überprüfung der RIP-Konfiguration

Sie können die Routing-Tabelle und andere RIP-Einstellungen anzeigen.

RIP-Einstellungen mithilfe der VTYSH-Befehlszeile anzeigen:

Geben Sie in der Befehlszeile die folgenden Befehle in der folgenden Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
sh rip	Zeigt die aktualisierte RIP-Routing-Tabelle an.
sh rip interface <vlan_name>	Zeigt RIP-Informationen für das angegebene VLAN an.

Beispiel:

```
NS# VTYSH
NS# sh rip
NS# sh rip interface VLAN0
<!--NeedCopy-->
```

OSPF konfigurieren

May 11, 2023

Der NetScaler unterstützt Open Shortest Path First (OSPF) Version 2 (RFC 2328). Die Funktionen von OSPF auf dem NetScaler sind:

- Wenn ein vserver aktiv ist, können die Host-Leitungen zum vserver in die Routingprotokolle eingespeist werden.
- OSPF kann in jedem Subnetz ausgeführt werden.
- Das von benachbarten OSPF-Routern beworbene Routenlernen kann auf dem NetScaler deaktiviert werden.
- Der NetScaler kann externe Typ-1- oder Typ-2-Metriken für alle Routen ankündigen.
- Der NetScaler kann vom Benutzer festgelegte Metrikeinstellungen für VIP-Routen ankündigen. Sie können beispielsweise eine Metrik pro VIP ohne spezielle Routenkarten konfigurieren.
- Sie können die OSPF-Bereichs-ID für den NetScaler angeben.
- Der NetScaler unterstützt nicht so stummelige Bereiche (NSSAs). Eine NSSA ähnelt einem OSPF-Stub-Bereich, ermöglicht jedoch die begrenzte Einschleusung externer Routen in den Stub-Bereich. Zur Unterstützung von NSSAs wurden ein neues Optionsbit (das N-Bit) und ein neuer Typ (Typ 7) des Link State Advertisement (LSA) -Bereichs definiert. LSAs vom Typ 7 unterstützen externe Routeninformationen innerhalb einer NSSA. Ein NSSA Area Border Router (ABR) übersetzt eine LSA vom Typ 7 in eine LSA vom Typ 5, die in die OSPF-Domäne übertragen wird. Die OSPF-Spezifikation definiert nur die folgenden allgemeinen Klassen der Flächenkonfiguration:

- Typ 5 LSA: Ursprünglich von Routern innerhalb des Gebiets werden von AS-Boarder-Routern (ASBRs) in die Domäne überflutet.
- Stub: Erlaubt keine Typ-5-LSAs in/im gesamten Gebiet zu übertragen und hängt stattdessen vom Standardrouting zu externen Zielen ab.

Nachdem Sie OSPF aktiviert haben, müssen Sie die Ankündigung von OSPF-Routen konfigurieren. Zur Fehlerbehebung können Sie die OSPF-Ausbreitung einschränken. Sie können OSPF-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

OSPF aktivieren und deaktivieren

Um OSPF zu aktivieren oder zu deaktivieren, müssen Sie entweder die CLI oder die GUI verwenden. Wenn OSPF aktiviert ist, startet NetScaler den OSPF-Prozess. Wenn OSPF deaktiviert ist, stoppt der NetScaler den OSPF-Routingprozess.

So aktivieren oder deaktivieren Sie das OSPF-Routing mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

1. **ns-Funktion aktivieren OSPF**
2. **Deaktivieren Sie die NS-Funktion OSPF**

So aktivieren oder deaktivieren Sie das OSPF-Routing mithilfe der GUI:

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie in der Gruppe **Modi und Funktionen** auf **Erweiterte Funktionen ändern**.
2. Wählen oder löschen Sie die **OSPF-Routing-Option** .

Werbung für OSPF Routes

OSPF ermöglicht es einem Upstream-Router, den Datenverkehr zwischen zwei identischen virtuellen Servern auszugleichen, die auf zwei eigenständigen NetScaler Appliances gehostet werden. Routenwerbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem NetScaler befinden.

So konfigurieren Sie OSPF für die Ankündigen von Routen mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Der globale Konfigurationsmodus wechselt.

Befehl	Spezifiziert
router OSPF	Starten Sie den OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
network A.B.C.D/M area <0-4294967295>	Routing in einem IP-Netzwerk aktivieren.
redistribute static	Verteilen Sie statische Routen neu.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# network 10.102.29.0/24 area 0
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Beschränken von OSPF-Propagierungen

Wenn Sie Ihre Konfiguration beheben müssen, können Sie den Nur-Listen-Modus für ein bestimmtes VLAN konfigurieren.

So beschränken Sie die OSPF-Propagierung mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router OSPF	Starten Sie den OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
passive-interface < vlan_name>	Unterdrückt Routing-Aktualisierungen an Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Prüfen der OSPF-Konfiguration

Sie können aktuelle OSPF-Nachbarn und OSPF-Routen anzeigen.

So zeigen Sie die OSPF-Einstellungen mithilfe der VTYSH-Befehlszeile an:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
sh OSPF neighbor	Zeigt aktuelle Nachbarn an.
sh OSPF route	Zeigt OSPF-Routen an.

Beispiel:

```
>VTYSH
NS# sh ip OSPF neighbor
NS# sh ip OSPF route
<!--NeedCopy-->
```

Konfigurieren des ordnungsgemäßen Neustarts für OSPF

In einem Nicht-INC-Hochverfügbarkeits-Setup (HA), in dem ein Routingprotokoll konfiguriert wird, werden nach einem Failover Routing-Protokolle konvergiert und Routen zwischen dem neuen primären Knoten und den benachbarten Nachbarroutern werden erlernt. Es dauert einige Zeit, bis das Routenlernen abgeschlossen ist. Während dieser Zeit verzögert sich die Weiterleitung von Paketen, die Netzwerkleistung kann gestört werden und Pakete können verworfen werden.

Ein ordnungsgemäßer Neustart ermöglicht es einem HA-Setup während eines Failovers, seine benachbarten Router anzuweisen, die gelernten Routen des alten primären Knotens nicht aus ihren Routing-Datenbanken zu entfernen. Unter Verwendung der Routing-Informationen des alten primären Knotens beginnen der neue primäre Knoten und die angrenzenden Router sofort mit der Weiterleitung von Paketen, ohne die Netzwerkleistung zu beeinträchtigen.

> **Hinweis:**
>
> Ein ordnungsgemäßer Neustart wird für Hochverfügbarkeits-Setups im INC-Modus nicht unterstützt.

Um einen ordnungsmäßigen Neustart für OSPF mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.
router-id <id>	NS(config)# router-id 1.1.1.1	Legt eine Routerkennung für die NetScaler Appliance fest. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Dieselbe ID muss im anderen Knoten in einer Hochverfügbarkeits-Einrichtung angegeben werden, die für einen ordnungsgemäßen Neustart eingerichtet ist, damit sie in der HA-Einrichtung ordnungsgemäß funktioniert.
ospf restart grace-period <1-1800>	NS(config)# ospf restart grace-period 170	Gibt die Nachfrist in Sekunden an, für die die Routen in den Hilfsgeräten beibehalten werden sollen. Standardwert: 120 Sekunden.

Befehl	Beispiel	Beschreibung des Befehls
ospf restart helper max-grace-period <1-1800>	NS(config)# ospf restart helper max-grace-period 180	Dies ist ein optionaler Befehl zum Begrenzen der maximalen Nachfrist, für die sich die NetScaler Appliance im Hilfsmodus befindet. Wenn die NetScaler Appliance eine undurchsichtige LSA mit einer Gnade erhält, die größer als die festgelegte Max-Grace-Periode des Helfers ist, wird die LSA verworfen und der NetScaler wird nicht in den Hilfsmodus versetzt.
router ospf	NS(config)# router ospf	Startet den OSPF-Routing-Prozess und wechselt in den Konfigurationsmodus für den Routing-Prozess.
network A.B.C.D/M area <0-4294967295>	NS(config-router)# network 192.0.2.0/24 area 0	Ermöglicht das Routing in einem IP-Netzwerk.
capability restart graceful	NS(config-router)# capability restart graceful	Ermöglicht einen ordnungsgemäßen Neustart des OSPF-Routing-Prozesses.
redistribute kernel	NS(config-router)# redistribute kernel	Verteilt Kernel-Routen neu.

BGP konfigurieren

May 11, 2023

Die NetScaler Appliance unterstützt BGP (RFC 4271). Die Funktionen von BGP auf dem NetScaler sind:

- Der NetScaler kündigt Routen an BGP-Peers an.
- Der NetScaler injiziert Hostrouten an virtuelle IP-Adressen (VIPs), die durch den Zustand der zugrunde liegenden virtuellen Server bestimmt werden.

- Der NetScaler generiert Konfigurationsdateien für die Ausführung von BGP auf dem sekundären Knoten nach einem Failover in einer HA-Konfiguration.
- Dieses Protokoll unterstützt IPv6-Routenaustausch.
- Unterstützung als Override im Border Gateway-Protokoll

Nachdem Sie BGP aktiviert haben, müssen Sie die Ankündigung von BGP-Routen konfigurieren. Zur Fehlerbehebung können Sie die BGP-Ausbreitung einschränken. Sie können die BGP-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

BGP aktivieren und deaktivieren

Um BGP zu aktivieren oder zu deaktivieren, müssen Sie entweder die CLI oder die GUI verwenden. Wenn BGP aktiviert ist, startet die NetScaler Appliance den BGP-Prozess. Wenn BGP deaktiviert ist, stoppt die Appliance den BGP-Prozess.

So aktivieren oder deaktivieren Sie das BGP-Routing über die CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns feature BGP
- disable ns feature BGP

So aktivieren oder deaktivieren Sie das BGP-Routing über die GUI:

1. Navigieren Sie zu System > Einstellungen, klicken Sie in der Gruppe Modi und Funktionen auf Erweiterte Funktionen ändern.
2. Wählen oder löschen Sie die Option BGP-Routing.

Werbung für IPv4-Strecken

Sie können die NetScaler Appliance so konfigurieren, dass Hostrouten an VIPs angekündigt und Routen an nachgeschaltete Netzwerke angekündigt werden.

So konfigurieren Sie BGP mit der VTYSH-Befehlszeile für die Ankündigen von IPv4-Routen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter. Mögliche Werte: 1 bis 4.294.967.295.

Befehl	Spezifiziert
Nachbar < IPv4 address> Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der lokalen IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Adress-Familie IPv4	Rufen Sie den Konfigurationsmodus für die
Neighbor < IPv4 address> activate	Tauschen Sie Präfixe für die IPv4-Routerfamilie zwischen dem Peer und dem lokalen Knoten mithilfe der lokalen Linkadresse aus.
redistribute kernel	Verteilen Sie Kernel-Routen neu.
redistribute static	Verteilen Sie statische Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor 10.102.29.170 remote-as 100
NS(config-router)# Address-family ipv4
NS(config-router-af)# Neighbor 10.102.29.170 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Werbung für IPv6 BGP-Routen

Border Gateway Protocol (BGP) ermöglicht es einem Upstream-Router, den Datenverkehr zwischen zwei identischen virtuellen Servern auszugleichen, die auf zwei eigenständigen NetScaler Appliances gehostet werden. Routenwerbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem NetScaler befinden.

Voraussetzungen für IPv6 BGP

Bevor Sie mit der Konfiguration von IPv6 BGP beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das IPv6-BGP-Protokoll verstehen.
- Aktivieren Sie die IPv6-Funktion.

Konfigurationsschritte

So konfigurieren Sie BGP mit der VTYSH-Befehlszeile für die Ankündigen von IPv6-Routen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter. Mögliche Werte: 1 bis 4.294.967.295.
Nachbar < IPv6 address> Remote-as < as-number>	Aktualisieren Sie die IPv6-BGP-Nachbartabelle mit der lokalen IPv6-Adresse des Nachbarn im angegebenen autonomen System.
Adress-Familie IPv6	Rufen Sie den Konfigurationsmodus für die
Nachbar < IPv6 address> aktiviert	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen dem Peer und dem lokalen Knoten mithilfe der lokalen Linkadresse aus.
redistribute kernel	Verteilen Sie Kernel-Routen neu.
redistribute static	Verteilen Sie statische Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor a1bc::102 remote-as 100
NS(config-router)# Address-family ipv6
NS(config-router-af)# Neighbor a1bc::102 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Überprüfung der BGP-Konfiguration

Sie können VTYSH verwenden, um BGP-Einstellungen anzuzeigen.

So zeigen Sie die BGP-Einstellungen mit der VTYSH-Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

```
VTYSH
You are now in the VTYSH command prompt. An output similar to the
   following appears:
NS170#
At the VTYSH command prompt, type:
NS170# sh ip BGP
NS170# sh BGP
NS170# sh ip BGP neighbors
NS170# sh ip BGP summary
NS170# sh ip BGP route-map <map-tag>
<!--NeedCopy-->
```

Unterstützung als Override im Border Gateway-Protokoll

Als Teil der BGP-Schleifenverhinderungsfunktionalität lässt der Router das Paket fallen, wenn ein Router ein BGP-Paket empfängt, das die Autonome Systemnummer (ASN) des Routers im Pfad für Autonome Systeme (AS) enthält. Es wird davon ausgegangen, dass das Paket vom Router stammt und den Ort erreicht hat, von dem es stammt.

Wenn ein Unternehmen über mehrere Standorte mit derselben ASN verfügt, führt die BGP-Schleifenprävention dazu, dass die Standorte mit einer identischen ASN nicht durch eine andere ASN verknüpft werden. Routing-Aktualisierungen (BGP-Pakete) werden verworfen, wenn sie von einem anderen Standort empfangen werden.

Um dieses Problem zu lösen, wurde dem ZeBOS BGP-Routingmodul des NetScaler die BGP AS-Override-Funktionalität hinzugefügt.

Wenn AS-Override für ein Peer-Gerät aktiviert ist und die NetScaler Appliance ein BGP-Paket zur Weiterleitung an den Peer empfängt und die ASN des Pakets mit der des Peers übereinstimmt, ersetzt die Appliance die ASN des BGP-Pakets vor der Weiterleitung des Pakets durch eine eigene ASN-Nummer.

Sie können AS-Override für einen bestimmten Nachbarn oder eine Gruppe von Nachbarn (Peer-Group) aktivieren, indem Sie die VTYSH-Befehlszeile verwenden.

So konfigurieren Sie BGP AS-Override für einen IPv4-Nachbarn mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.

Befehl	Spezifiziert
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
Nachbar < IPv4 address> Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Nachbar <IPv4 address>als Override	Aktiviert BGP als Override für den angegebenen Nachbarn.

```
    > VTYSH NS# configure terminal
    NS(config)# router BGP 200
    NS(config-router)# Neighbor 192.0.2.100 remote-as 100
    NS(config-router)# Neighbor 10.102.29.100 as-override
<!--NeedCopy-->
```

So konfigurieren Sie BGP AS-Override für eine IPv4-BGP-Peer-Gruppe mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
****Nachbar-Peer-Group**** <peer group name>	Erstellen Sie eine BGP-Peer-Gruppe.
****Nachbar-Peer-Gruppe**** <IPv4 address><peer group name>	Ordnen Sie Nachbarn der angegebenen Peer-Gruppe zu.
Nachbar <peer group name>Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Nachbar <peer group name>als Override	Aktiviert BGP als Override für alle Nachbarn, die mit der angegebenen Peer-Gruppe verknüpft sind.

```
    > VTYSH NS# configure terminal
    NS(config)# router BGP 200
    NS(config-router)# neighbor external-peers-1 peer-group
    NS(config-router)# neighbor 192.0.2.101 peer-group external-peers-1
```



```
5     NS(config-router)# neighbor 192.0.2.102 peer-group external-peers-1
6     NS(config-router)# neighbor 192.0.2.103 peer-group external-peers-1
7     NS(config-router)# Neighbor external-peers-1 remote-as 100
8     NS(config-router)# Neighbor external-peers-1 as-override
9  <!--NeedCopy-->
```

So konfigurieren Sie BGP AS-Override für einen IPv6-Nachbarn mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
Nachbar < IPv6 address> Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Nachbar <IPv6 address>als Override	Aktiviert BGP als Override für den angegebenen Nachbarn.
Adress-Familie IPv6	Rufen Sie den Konfigurationsmodus für die
Nachbar < IPv6 address> aktiviert	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen dem angegebenen Nachbarn und dem NetScaler mithilfe der lokalen Linkadresse aus.
Nachbar <IPv6 address>als Override	Aktiviert BGP als Override für den angegebenen Nachbarn.

```
1     > VTYSH NS# configure terminal
2     NS(config)# router BGP 200
3     NS(config-router)# Neighbor a1bc::102 remote-as 100
4     NS(config-router)# Neighbor a1bc::102 as-override
5     NS(config-router)# Address-family ipv6
6     NS(config-router-af)# Neighbor a1bc::102 activate
7     NS(config-router)# Neighbor a1bc::102 as-override
8  <!--NeedCopy-->
```

So konfigurieren Sie BGP AS-Override für IPv6-Peer-Group mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
****Nachbar-Peer-Group****<peer group name>	Erstellen Sie eine BGP-Peer-Gruppe.
****Nachbar-Peer-Group**** <IPv6 address><peer group name>	Ordnen Sie der angegebenen Peer-Gruppe einen Nachbarn zu.
Nachbar <peer group name>Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Nachbar <peer group name>als Override	Aktiviert BGP als Override für alle Nachbarn, die mit der angegebenen Peer-Gruppe verknüpft sind.
Adress-Familie IPv6	Rufen Sie den Konfigurationsmodus für die
Nachbar <peer group name>aktiviert	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen den Nachbarn der angegebenen Peer-Gruppe und dem NetScaler mithilfe der lokalen Linkadresse aus.
Nachbar <peer group name>als Override	Aktiviert BGP als Override für alle Nachbarn, die mit der angegebenen Peer-Gruppe verknüpft sind.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# neighbor external-peers-2 peer-group
4      NS(config-router)# neighbor 2001::1 peer-group external-peers-2
5      NS(config-router)# neighbor 2001::2 peer-group external-peers-2
6      NS(config-router)# Neighbor external-peers-2 remote-as 100
7      NS(config-router)# Neighbor external-peers-2 as-override
8      NS(config-router)# Address-family ipv6
9      NS(config-router-af)# Neighbor external-peers-2 activate
10     NS(config-router)# Neighbor external-peers-2 as-override
11 <!--NeedCopy-->
```


Ordnungsgemäßer Neustart

In einem Nicht-INC-Hochverfügbarkeits-Setup (HA), in dem ein Routingprotokoll konfiguriert wird, werden nach einem Failover Routing-Protokolle konvergiert und Routen zwischen dem neuen primären Knoten und den benachbarten Nachbarroutern werden erlernt. Es dauert einige Zeit, bis das Routenlernen abgeschlossen ist. Während dieser Zeit verzögert sich die Weiterleitung von Paketen, die Netzwerkleistung kann gestört werden und Pakete können verworfen werden.

Ein ordnungsgemäßer Neustart ermöglicht es einem HA-Setup während eines Failovers, seine benachbarten Router anzuweisen, die gelernten Routen des alten primären Knotens nicht aus ihren Routing-Datenbanken zu entfernen. Unter Verwendung der Routing-Informationen des alten primären Knotens beginnen der neue primäre Knoten und die angrenzenden Router sofort mit der Weiterleitung von Paketen, ohne die Netzwerkleistung zu beeinträchtigen.

> **Hinweis:**
>
> Ein ordnungsgemäßer Neustart wird für Hochverfügbarkeits-Setups im INC-Modus nicht unterstützt.

Konfigurieren des ordnungsgemäßen Neustarts für BGP

Um einen ordnungsmäßigen Neustart für BGP über die VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.

Befehl	Beispiel	Beschreibung des Befehls
router-id <ID>	NS(config)# router-id 1.1.1.1	Eine Routerkennung für die NetScaler Appliance. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Derselbe Bezeichner muss auf dem anderen Knoten in einem Hochverfügbarkeits-Setup angegeben werden, damit ein ordnungsgemäßer Neustart ordnungsgemäß funktioniert.
router bgp <AS-number>	NS(config)# router bgp 5	Ruft den BGP-Konfigurationsmodus auf
bgp graceful-restart	NS(config)# bgp graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart des BGP-Routing-Prozesses.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Gibt die Nachfrist in Sekunden an, in der die Helfer-Router nach einem Failover auf eine TCP-Verbindung vom neuen primären Knoten warten. Für diese Zeitspanne bewahren die Helfer-Router die Routen bei.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Gibt die Zeit in Sekunden an, zu der die NetScaler Appliance im Hilfsmodus die veralteten Routen für den Neustart von Nachbarroutern beibehält. Der Standardwert beträgt 360 Sekunden.

Befehl	Beispiel	Beschreibung des Befehls
neighbor <IPv4 address of the peer router> remote-as <AS-number>	NS(config-router)# neighbor 192.0.2.30 remote-as 2	Richtet BGP-Peering mit dem angegebenen Nachbar-Router-Gerät ein.
neighbor <IPv4 address of the peer router> capability graceful-restart	NS(config-router)# neighbor 192.0.2.30 capability graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart mit dem angegebenen Nachbarn.
redistribute kernel	NS(config-router)# redistribute kernel	Verteilt Kernel-Routen neu.

Konfigurieren des ordnungsgemäßen Neustarts für IPv6 BGP

Um einen ordnungsmäßigen Neustart für IPv6 BGP mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.
router-id <id>	NS(config)# router-id 1.1.1.1	Legt eine Routerkennung für die NetScaler Appliance fest. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Dieselbe ID muss im anderen Knoten in einem Hochverfügbarkeits-Setup angegeben werden, damit ein ordnungsgemäßer Neustart ordnungsgemäß funktioniert.
router bgp <AS-number>	NS(config)# router bgp 5	Ruft den Konfigurationsmodus für das BGP-Protokoll auf

Befehl	Beispiel	Beschreibung des Befehls
bgp graceful-restart	NS(config)# bgp graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart des BGP-Routing-Prozesses.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Gibt die Nachfrist in Sekunden an, in der die Helfer-Router nach einem Failover auf eine TCP-Verbindung vom neuen primären Knoten warten. Für diese Zeitspanne bewahren die Helfer-Router die Routen bei. Der Standardwert beträgt 360 Sekunden.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Gibt die Zeit in Sekunden an, zu der die NetScaler Appliance im Hilfsmodus die veralteten Routen für den Neustart von Nachbarroutern beibehält. Der Standardwert beträgt 360 Sekunden.
neighbor <IPv6 address> remote-as <AS-number>	NS(config-router)# neighbor 2001:db8::10 remote-as 2	Richtet BGP-Peering mit dem angegebenen Nachbar-Router-Gerät ein.
address-family ipv6	NS(config-router)#address-family ipv6	Geht in den Konfigurationsmodus für die Adressfamilie.
neighbor <IPv6 address of the neighbor> activate	NS(config-router-af)#neighbor 2001:db8::10 activate	Ermöglicht den Austausch von Adressfamilien-Routen mit dem angegebenen Nachbar-Router-Gerät.
neighbor <IPv6 address of the neighbor> capability graceful-restart	NS(config-router-af)#neighbor 2001:db8::10 capability graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart mit dem angegebenen Nachbar-Router-Gerät.
redistribute kernel	NS(config-router-af)#redistribute kernel	Verteilt Kernel-Routen neu.

Befehl	Beispiel	Beschreibung des Befehls
exit-address-family	NS(config-router-af)#exit-address-family	Beenden des Konfigurationsmodus der Adressfamilie

Konfigurieren der MD5-Authentifizierung für IPv4 BGP

Die NetScaler Appliance unterstützt die MD5-Authentifizierung für das Border Gateway Protocol (BGP). Wenn die Authentifizierung aktiviert ist, wird jedes TCP-Segment, das zu BGP gehört, das zwischen der NetScaler Appliance und ihrem Peer-Gerät ausgetauscht wird, nur überprüft und akzeptiert, wenn die Authentifizierung erfolgreich ist. Damit die Authentifizierung erfolgreich ist, müssen beide Peers mit demselben MD5-Kennwort konfiguriert sein. Wenn die Authentifizierung fehlschlägt, wird die BGP-Nachbarbeziehung nicht hergestellt. Die Unterstützung der MD5-Authentifizierung für BGP in der NetScaler Appliance ist mit RFC 2385 kompatibel.

Bevor Sie beginnen

Beachten Sie die folgenden Punkte, bevor Sie mit der Konfiguration der BGP-MD5-Authentifizierung beginnen:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten der BGP-MD5-Authentifizierung verstehen, die in RFC 2385 beschrieben sind.
- Die BGP-MD5-Authentifizierung wird für NetScaler Administratorpartitionen nicht unterstützt.
- Die BGP-MD5-Authentifizierung wird für IPv6-BGP-Konfigurationen nicht unterstützt.
- Die BGP-MD5-Authentifizierung wird sowohl für NetScaler-Clusterkonfigurationen als auch für Konfigurationen mit hoher Verfügbarkeit unterstützt.
- Aufgrund des folgenden Problems in FreeBSD empfiehlt Citrix, niedrige Keep-Live- und Hold-Time-Werte (z. B. 5 und 15) festzulegen und einen ordnungsgemäßen Neustart für eine BGP-Sitzung in einer Layer-2-Hochverfügbarkeitskonfiguration zu konfigurieren. Andernfalls kann es bei aktivierter MD5-Authentifizierung länger dauern, bis BGP nach einem Failover eine Verbindung mit dem Nachbarn wiederhergestellt hat.
  - Das letzte ACK von FreeBSD enthält keinen md5-Digest:
    * https://forums.freebsd.org/threads/11170/
    * http://support.pfsense.narkive.com/povrH5HI/bgp-md5-weird-behavior-when-connection-closes

Konfigurationsschritte

Um die MD5-Authentifizierung für IPv4 BGP mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
vtysh	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Der globale Konfigurationsmodus wechselt.
router bgp <AS-number>	Ruft den Konfigurationsmodus für das BGP-Protokoll auf <AS-number>ist eine autonome BGP-Systemnummer und ist ein erforderlicher Parameter.
neighbor <neighbour IPv4 address> remote-as < AS-number >	Aktualisiert die IPv4-BGP-Tabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
neighbor < neighbour IPv4 address > password < password in double quotes>	Konfiguriert die MD5-Authentifizierung für den angegebenen Nachbarn mit dem angegebenen MD5-Kennwort. Damit die MD5-Authentifizierung erfolgreich ist, müssen Sie dasselbe MD5-Kennwort auf der NetScaler Appliance und der Nachbar-Appliance konfigurieren.

```
> vtysh

ns# configure terminal

ns(config)#router bgp 5

ns(config-router)#neighbor 20.20.20.138 remote-as 1

ns(config-router)#neighbor 20.20.20.138 password  “secret”

ns(config-router)#redistribute kernel

ns(config-router)#exit

<!--NeedCopy-->
```


Konfiguration von 4-Byte-BGP-ASNs im Plain- und Asdot-Format

Die NetScaler Appliance unterstützt das Konfigurieren und Anzeigen von 4-Byte-BGP-Systemnummern (ASN) in einem Plain- oder Asdot-Format, wie in RFC 5396 definiert.

- **asplain**. Dezimalwertnotation, bei der sowohl 2-Byte- als auch 4-Byte-ASNs als Dezimalwert dargestellt werden Beispielsweise ist 65527 eine 2-Byte-ASN und 234567 eine 4-Byte-ASN.
- **asdot** Autonomes System Punktnotation, bei der 2-Byte-ASNs als Dezimalwert (wie in asplain) und 4-Byte-ASNs in einer Punktnotation dargestellt werden. Beispielsweise ist 65527 eine 2-Byte-ASN und 3,37959 eine 4-Byte-ASN. (3,37959 ist das Asdot-Format für die Dezimalzahl 234567).

Beispiele für die Konfiguration von BGP ASN in den Formaten asplain und asdot

Standardmäßig zeigt die NetScaler Appliance die BGP-ASNs in einem einfachen Format an, Sie können jedoch so konfigurieren, dass sie im Asdot-Format angezeigt werden. Sie können lokale und Remote-BGP-ASNs im Plain- oder Asdot-Format konfigurieren.

Im Folgenden sind einige Beispiele für die Konfiguration von BGP ASN in den Formaten asplain und asdot aufgeführt:

- Zeigen Sie die BGP AS-Nummer in einem einfachen Format an. Standardmäßig zeigt die NetScaler Appliance die BGP AS-Nummer in einem einfachen Format an.

```
ns#conf t
ns(config)# router bgp 196908
ns(config-router)# end
ns#
ns# sh run router bgp
!
router bgp 196908
!
<!--NeedCopy-->
```

- Zeigen Sie die BGP AS-Nummer im Asdot-Format an. Führen Sie den Befehl bgp `asnotation-dot` aus, um die BGP AS-Nummer im asdot-Format anzuzeigen.

```
ns#conf t
ns(config)#router bgp 196908
ns(config-router)#bgp asnotation-dot
ns(config-router)#end
ns#
ns#sh run router bgp
!
router bgp 3.300
```



```
bgp asnotation-dot
!
<!--NeedCopy-->
```

- Konfigurieren und zeigen Sie die BGP AS-Nummer im asdot-Format an. Führen Sie den Befehl `bgp asnotation-dot` aus, um die BGP AS-Nummer im asdot-Format anzuzeigen.

```
ns# conf t
ns(config)# router bgp 3.300
ns(config-router)# bgp asnotation-dot
ns#
ns# sh run router bgp
!
router bgp 3.300
bgp asnotation-dot
!
<!--NeedCopy-->
```

- Zeigen Sie die BGP AS-Nummer wieder in einem einfachen Format aus dem asdot-Format an. Führen Sie den Befehl bgp `no asnotation-dot` aus, um die BGP AS-Nummer wieder im Plain-Format anzuzeigen.

```
ns#conf t
ns(config)#router bgp 3.300
ns(config-router)#no bgp asnotation-dot
ns(config-router)#end
ns#

ns#sh run router bgp
!
router bgp 196908
!
<!--NeedCopy-->
```

- Konfigurieren und zeigen Sie die Remote-AS-Nummer im asdot-Format an. Führen Sie den Befehl `bgp asnotation-dot` aus. In der Beispielkonfiguration ist die Remote-AS-Nummer 80000 im asdot-Format 1.14464 konfiguriert.

```
ns# conf t
ns(config)# router bgp 3.300
ns(config-router)# bgp asnotation-dot
ns(config-router)# neighbor 192.168.1.2 remote-as 1.14464
ns(config-router)#end
ns#
ns#
```



```
ns#sh run router bgp
!
router bgp 3.300
bgp asnotation-dot
neighbor 192.168.1.2 remote-as 1.14464
!
ns#
<!--NeedCopy-->
```

- Zeigen Sie die lokalen BGP-Nummern und Remote-AS-Nummern im asplain-Format aus dem asdot-Format an. Führen Sie den Befehl bgp `no asnotation-dot` aus.

```
ns#conf t
ns(config)#router bgp 3.300
ns(config-router)#no bgp asnotation-dot
ns(config-router)#end
ns#

ns#sh run router bgp
!
router bgp 196908
neighbor 192.168.1.2 remote-as 80000
!
ns#
<!--NeedCopy-->
```

> **Hinweis:**
>
> Anstatt für einzelne BGP-Nachbarn zu konfigurieren, kann dieselbe asplain- oder asdot-Konfiguration auch für BGP-Peer-Groups verwendet werden.

IPv6 RIP konfigurieren

May 11, 2023

IPv6 Routing Information Protocol (RIP) oder RIPNG ist ein Distance Vector-Protokoll. Dieses Protokoll ist eine Erweiterung von RIP zur Unterstützung von IPv6. Nachdem Sie IPv6-RIP aktiviert haben, müssen Sie die Ankündigung von IPv6-RIP-Routen konfigurieren. Zur Problembehandlung können Sie die IPv6-RIP-Propagierung einschränken. Sie können die IPv6-RIP-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

Voraussetzungen für IPv6-RIP

Bevor Sie mit der Konfiguration von IPv6-RIP beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das IPv6-RIP-Protokoll verstehen.
- Installieren Sie die IPv6PT-Lizenz auf der NetScaler Appliance.
- Aktivieren Sie die IPv6-Funktion.

Werbung für IPv6-RIP-Routen

IPv6-RIP ermöglicht es einem Upstream-Router, den Datenverkehr zwischen zwei identischen vServern, die auf zwei eigenständigen NetScaler-Geräten gehostet werden, auszugleichen. Route-Werbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem NetScaler befinden.

Um IPv6-RIP so zu konfigurieren, dass IPv6-Routen mithilfe der VTYSH-Befehlszeile angekündigt werden:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
IPv6-Rip-Router	Starten Sie den IPv6-RIP-Routingprozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
redistribute static	Verteilen Sie statische Routen neu.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```


Einschränkung von IPv6-RIP-Propagationen

Wenn Sie Probleme mit Ihrer Konfiguration beheben müssen, können Sie den Nur-Listen-Modus auf jeder beliebigen Schnittstelle konfigurieren.

Um die IPv6-RIP-Propagierung mithilfe der VTYSH-Befehlszeile einzuschränken:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
IPv6-Rip-Router	Starten Sie den IPv6-RIP-Routingprozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
passive-interface < vlan_name>	Unterdrückt Routing-Aktualisierungen an Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Überprüfen der IPv6-RIP-Konfiguration

Sie können VTYSH verwenden, um die IPv6-RIP-Routingtabelle und IPv6-RIP-Informationen für ein bestimmtes VLAN anzuzeigen.

Um die IPv6-RIP-Einstellungen mithilfe der VTYSH-Befehlszeile anzuzeigen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
sh ipv6 rip	Zeigt die aktualisierte IPv6-RIP-Routingtabelle an.

Befehle	Spezifiziert
sh ipv6 rip interface <vlan_name>	Zeigt IPv6-RIP-Informationen für das angegebene VLAN an.

Beispiel:

```
NS# VTYSH
NS# sh ipv6 rip
NS# sh ipv6 rip interface VLAN0
<!--NeedCopy-->
```

IPv6 OSPF konfigurieren

May 11, 2023

IPv6 OSPF oder OSPF Version 3 (OSPF v3) ist ein Link-State-Protokoll, das zum Austausch von IPv6-Routing-Informationen verwendet wird. Nachdem Sie IPv6-OSPF aktiviert haben, müssen Sie die Ankündigung von IPv6-OSPF-Routen konfigurieren. Zur Fehlerbehebung können Sie die IPv6-OSPF-Ausbreitung einschränken. Sie können IPv6-OSPF-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

Voraussetzungen für IPv6 OSPF

Bevor Sie mit der Konfiguration von IPv6 OSPF beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das IPv6-OSPF-Protokoll verstehen.
- Installieren Sie die IPv6PT-Lizenz auf der NetScaler Appliance.
- Aktivieren Sie die IPv6-Funktion.

Werbung für IPv6-Strecken

IPv6-OSPF ermöglicht einem Upstream-Router den Lastenausgleich zwischen zwei identischen vServern, die auf zwei eigenständigen NetScaler-Geräten gehostet werden. Routenwerbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem NetScaler befinden.

So konfigurieren Sie IPv6-OSPF für die Beankündigen von IPv6-Routen mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router ipv6 OSPF	Starten Sie den IPv6-OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
redistribute static	Verteilen Sie statische Routen neu.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Beschränken von IPv6-OSPF-Propagierungen

Wenn Sie Ihre Konfiguration beheben müssen, verwenden Sie VTYSH, um den Nur-Listen-Modus für ein bestimmtes VLAN zu konfigurieren.

So beschränken Sie die IPv6-OSPF-Weitergabe mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router ipv6 OSPF	Starten Sie den IPv6-OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.

Befehle	Spezifiziert
passiv-schnittstelle < vlan_name >	Unterdrückt Routing-Aktualisierungen an Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Überprüfung der IPv6-OSPF-Konfiguration

Sie verwenden VTYSH, um aktuelle IPv6-OSPF-Nachbarn und IPv6-OSPF-Routen anzuzeigen.

So zeigen Sie die IPv6-OSPF-Einstellungen mithilfe der VTYSH-Befehlszeile an:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
sh ipv6 OSPF Nachbar	Zeigt aktuelle Nachbarn an.
sh ipv6 OSPF-Route	IPv6-OSPF-Routen anzeigen.

Beispiel:

```
>VTYSH
NS# sh ipv6 OSPF neighbor
NS# sh ipv6 OSPF route
<!--NeedCopy-->
```

OSPFv3-Authentifizierung

Um die Integrität, Datenherkunftsauthentifizierung und Datenvertraulichkeit von OSPFv3-Paketen sicherzustellen, muss die OSPFv3-Authentifizierung auf OSPFv3-Peers konfiguriert werden.

Die NetScaler Appliance unterstützt die OSPFv3-Authentifizierung und ist teilweise mit RFC 4552 kompatibel. Die OSPFv3-Authentifizierung basiert auf den beiden IPSec-Protokollen: Authentication Header (AH) und Encapsulating Security Payload (ESP). Die NetScaler Appliance unterstützt nur das AH-Protokoll für die OSPFv3-Authentifizierung.

Die OSPFv3-Authentifizierung verwendet manuell definierte IPSec-Sicherheitszuordnungen (SAs) zwischen den OSPFv3-Peers und stützt sich nicht auf das IKE-Protokoll für die Bildung dynamischer SAs. Manuelle SAs definieren die Sicherheitsparameter Index (SPI) -Werte, Algorithmen und Schlüssel, die zwischen den Peers verwendet werden sollen. Manuelle SAs erfordern keine Verhandlungen zwischen den Peers. Daher muss dieselbe SA für beide Peers definiert werden.

Sie können die OSPFv3-Authentifizierung in einem VLAN oder für einen OSPFv3-Bereich konfigurieren. Bei der Konfiguration für ein VLAN werden die Einstellungen auf alle Schnittstellen angewendet, die Mitglieder des VLAN sind. Wenn Sie die OSPFv3-Authentifizierung für einen OSPF-Bereich konfigurieren, werden die Einstellungen auf alle VLANs in diesem Bereich angewendet. Die Einstellungen werden wiederum auf alle Schnittstellen angewendet, die Mitglieder dieser VLANs sind. Diese Einstellungen gelten nicht für Mitglieds-VLANs, für die Sie die OSPFv3-Authentifizierung direkt konfiguriert haben.

Beachten Sie die folgenden Punkte und Einschränkungen, bevor Sie die OSPFv3-Authentifizierung auf einer NetScaler Appliance konfigurieren:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten der OSPFv3-Authentifizierung verstehen, die in RFC 4552 beschrieben sind.
- Für die OSPFv3-Authentifizierung wird nur das Authentifizierungs-Header-Protokoll unterstützt. Capsulating Security Payload (ESP) wird nicht unterstützt.
- Sie müssen eine SA mit derselben Einstellung auf der Peer-Schnittstelle definieren.
- Das erneute Keying von manuellen Tasten wird nicht unterstützt.

So konfigurieren Sie die OSPFv3-Authentifizierung auf einem VLAN über die VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angezeigten Reihenfolge ein: VLAN-Befehle zur OspFv3-Authentifizierung.

Beispiel:

```
1 > VTYSH NS# configure terminal
2 NS(config)# interface vlan2
3 NS(config-if)# ipv6 ospf authentication ipsec spi 256 md5 123456789
     ABCDEF0123456789ABCDEF0
4 <!--NeedCopy-->
```

So konfigurieren Sie die OSPFv3-Authentifizierung in einem OSPF-Bereich über die VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angezeigten Reihenfolge ein: OSPFv3-Authentifizierung OSPF-Bereichsbefehle.

Beispiel:

```
1 > VTYSH NS# configure terminal
2 ns(config)#router ipv6 ospf 30
3 ns(config-router)# area 1 authentication ipsec spi 256
     md5123456789ABCDEF0123456789ABCDEF0
4 <!--NeedCopy-->
```

Konfigurieren des ordnungsgemäßen Neustarts für IPv6 OSPF

In einem Nicht-INC-Hochverfügbarkeits-Setup (HA), in dem ein Routingprotokoll konfiguriert wird, werden nach einem Failover Routing-Protokolle konvergiert und Routen zwischen dem neuen primären Knoten und den benachbarten Nachbarroutern werden erlernt. Es dauert einige Zeit, bis das Routenlernen abgeschlossen ist. Während dieser Zeit verzögert sich die Weiterleitung von Paketen, die Netzwerkleistung kann gestört werden und Pakete können verworfen werden.

Ein ordnungsgemäßer Neustart ermöglicht es einem HA-Setup während eines Failovers, seine benachbarten Router anzuweisen, die gelernten Routen des alten primären Knotens nicht aus ihren Routing-Datenbanken zu entfernen. Unter Verwendung der Routing-Informationen des alten primären Knotens beginnen der neue primäre Knoten und die angrenzenden Router sofort mit der Weiterleitung von Paketen, ohne die Netzwerkleistung zu beeinträchtigen.

> **Hinweis:**
>
> Ein ordnungsgemäßer Neustart wird für Hochverfügbarkeits-Setups im INC-Modus nicht unterstützt.

Um einen ordnungsmäßigen Neustart für IPv6-OSPF mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	> VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.

Befehl	Beispiel	Beschreibung des Befehls
router-id id>	NS(config)#router-id 1.1.1.1	Legt eine Routerkennung für die NetScaler Appliance fest. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Dieselbe ID muss im anderen Knoten in einer Hochverfügbarkeits-Einrichtung angegeben werden, die für einen ordnungsgemäßen Neustart eingerichtet ist, damit sie in der HA-Einrichtung ordnungsgemäß funktioniert.
IPv6ospf restart grace-period <1-1800>	NS(config)# IPv6ospf restart grace-period 170	Gibt die Nachfrist in Sekunden an, für die die Routen in den Hilfsgeräten beibehalten werden sollen. Standardwert: 120 Sekunden.
IPv6 ospf restart helper max-grace-period <1-1800>	NS(config)# IPv6 ospf restart helper max-grace-period 180	Dies ist ein optionaler Befehl zum Begrenzen der maximalen Nachfrist, für die sich die NetScaler Appliance im Hilfsmodus befindet. Wenn die NetScaler Appliance eine undurchsichtige LSA mit einer Gnade erhält, die größer als die festgelegte Max-Grace-Periode des Helfers ist, wird die LSA verworfen und der NetScaler wird nicht in den Hilfsmodus versetzt.
interface <VLANID>	NS(config)#interface vlan3	Ruft den VLAN-Konfigurationsmodus auf

Befehl	Beispiel	Beschreibung des Befehls
ipv6 router ospf area <area_id> tag <tag_id>	NS(config-if)#ipv6 router ospf area 0 tag 1	Startet den IPv6-OSPF-Routing-Prozess in einem VLAN.
exit	NS(config-if)#exit	Beenden Sie den VLAN-Konfigurationsmodus.
router ipv6 ospf	NS(config)# router ipv6 ospf 1	Startet den IPv6-OSPF-Routing-Prozess und wechselt in den Konfigurationsmodus für den Routing-Prozess.
capability restart graceful	NS(config-router)#capability restart graceful	Ermöglicht einen ordnungsgemäßen Neustart des IPv6-OSPF-Routing-Prozesses.
redistribute kernel	NS(config-router)# redistribute kernel	Verteilt Kernel-Routen neu.

ISIS konfigurieren

May 11, 2023

Die NetScaler-Appliance unterstützt das dynamische Routing-Protokoll Intermediate System-to-Intermediate System (IS-IS oder ISIS). Dieses Protokoll unterstützt sowohl den IPv4- als auch den IPv6-Routenaustausch. IS-IS ist ein Link-State-Protokoll und daher weniger anfällig für Routing-Schleifen. Mit den Vorteilen einer schnelleren Konvergenz und der Fähigkeit, größere Netzwerke zu unterstützen, kann ISIS in Netzwerken von Internetdienstanbietern (ISP) sehr nützlich sein.

Voraussetzungen für die Konfiguration von ISIS

Bevor Sie mit der Konfiguration von ISIS beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das ISIS-Protokoll verstehen.
- Aktivieren Sie für IPV6-Routen:
  - Funktion zur Übersetzung des IPv6-Protokolls.
  - IPv6-Option für dynamisches Routing auf den VLANs, auf denen Sie das ISIS-Protokoll ausführen möchten.

ISIS aktivieren

Verwenden Sie eines der folgenden Verfahren, um die ISIS-Routing-Funktion auf der NetScaler-Appliance zu aktivieren.

Um ISIS-Routing mit der CLI zu aktivieren:

Geben Sie in der Befehlszeile Folgendes ein:

enable ns feature ISIS

Um ISIS-Routing mithilfe der GUI zu aktivieren:

1. Navigieren Sie zu System > Einstellungen, klicken Sie in der Gruppe Modi und Funktionen auf Erweiterte Funktionen ändern.
2. Wählen oder deaktivieren Sie die Option ISIS-Routing.

Einen ISIS-Routing-Prozess erstellen und auf einem VLAN starten

Um einen ISIS-Routing-Prozess zu erstellen, müssen Sie die VTYSH-Befehlszeile verwenden.

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beschreibung
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Wechselt in den globalen Konfigurationsmodus.
router ISIS [tag]	Erstellt einen ISIS-Routing- und Konfigurationsmodus für den Routingprozess.
net XX….XXXX.YYYY.YYYY.YYYY.00	Gibt einen NET-Wert für den Routing-Prozess an, wobei: ·**XX… .XXXX** die Bereichsadresse ist (kann 1—13 Byte sein), ·**YYYY.YYYY.YYYY** ist die System-ID (6 Byte), ·**00** ist der N-Selektor (1 Byte).
is-type (level-1|level-1-2|level-2-only)	Setzt den ISIS-Routing-Prozess auf die angegebene Routing-Ebene. Standard: level-1-2.
ns IPv6-routing	Startet den dynamischen IPv6-Routing-Daemon.
interface <vlan_name>	Wechselt in den VLAN-Konfigurationsmodus.
ip router ISIS	Aktiviert den ISIS-Routing-Prozess im VLAN für den IPv4-Routenaustausch.

Befehl	Beschreibung
ipv6 router ISIS	Aktiviert den ISIS-Routing-Prozess im VLAN für den IPv6-Routenaustausch.

Beispiel:

```
> VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# net 15.aabb.ccdd.0097.00
NS(config-router)# is-type level-1
NS(config-router)# exit
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)#  ip router isis 11
NS(config-if)# ipv6 router isis 11
<!--NeedCopy-->
```

Werberouten

Route-Werbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter der NetScaler-Appliance befinden.

Um ISIS so zu konfigurieren, dass Routen mithilfe der VTYSH-Befehlszeile angekündigt werden:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beschreibung
VTYSH	Zeigt die VTYSH-Befehlszeile an.
configure terminal	Wechselt in den globalen Konfigurationsmodus.
router ISIS [tag]	Startet die ISIS-Routing-Instance und wechselt in den Konfigurationsmodus für den Routing-Prozess.
redistribute connected (level-1 or level-1-2 or level-2)	Verteilt verbundene Routen neu, wobei: **level-1: Umverteilung verbundener Routen in Level-1**, **level-1-2**: Umverteilung verbundener Routen in Level-1 und Level-2, **level-2**: Umverteilung verbundener Routen in Level-2.

Befehl	Beschreibung
Kernel weiterverteilen (Level-1 oder Level-1-2 oder Level-2)	Verteilt Kernel-Routen neu, wobei: **level-1**: Umverteilung der Kernel-Routen in Level-1, **level-1-2**: Umverteilen von Kernel-Routen in Level-1 und Level-2, **level-2**: Umverteilen von Kernel-Routen in Level-2.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# redistribute connected level-1
NS(config-router)# redistribute kernel level-1
<!--NeedCopy-->
```

Begrenzung der ISIS-Ausbreitung

Wenn Sie Probleme mit Ihrer Konfiguration beheben müssen, können Sie den Nur-Listen-Modus auf einem beliebigen VLAN konfigurieren.

ISIS-Ausbreitung mithilfe der VTYSH-Befehlszeile einschränken:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beschreibung
VTYSH	Zeigt die VTYSH-Befehlszeile an.
configure terminal	Wechselt in den globalen Konfigurationsmodus.
router isis [tag]	Wechselt in den Konfigurationsmodus für den Routing-Prozess.
passive-interface <vlan_name>	Unterdrückt Routing-Updates auf Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
```



```
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Überprüfung der ISIS-Konfiguration

Sie können VTYSH verwenden, um die ISIS-Routing-Tabelle und ISIS-Informationen für ein bestimmtes VLAN anzuzeigen.

ISIS-Einstellungen mithilfe der VTYSH-Befehlszeile anzeigen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Beschreibung
VTYSH	Zeigt die VTYSH-Befehlszeile an.
show ip isis route	Zeigt die aktualisierte IPv4-ISIS-Routing-Tabelle an.
show ipv6 isis route	Zeigt die aktualisierte IPv6-IS-Routing-Tabelle an.
sh isis interface <vlan_name>	Zeigt IPv6-ISIS-Informationen für das angegebene VLAN an.

Beispiel:

```
NS# VTYSH
NS#  show ip isis route
NS#  show ipv6 isis route
NS# sh isis interface VLAN0
<!--NeedCopy-->
```

Routen in NetScaler-Routingtabelle installieren

May 11, 2023

Die NetScaler-Appliance kann Routen verwenden, die von verschiedenen Routing-Protokollen gelernt wurden, nachdem Sie die Routen in der Routingtabelle der Appliance installiert haben.

So installieren Sie verschiedene Routen in die interne Routingtabelle über die VTYSH-Befehlszeile:

Geben Sie in der CLI die folgenden Befehle ein, die für die Routen geeignet sind, die Sie installieren möchten:

Befehle	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
ns route-install Standard	Installieren Sie IPv4-Standardrouten zur internen Routingtabelle.
ns route-install RIP	Installieren Sie IPv4-RIP-spezifische Routen zur internen Routingtabelle.
ns route-install BGP	Installieren Sie IPv4-BGP-spezifische Routen zur internen Routingtabelle.
ns route-install OSPF	Installieren Sie IPv4-OSPF-spezifische Routen zur internen Routingtabelle.
ns route-install IPv6 Default	Installieren Sie IPv6-Standardrouten zur internen Routingtabelle.
ns route-install IPv6 RIP	Installieren Sie IPv6-RIP-spezifische Routen zur internen Routingtabelle.
ns route-install IPv6 BGP	Installieren Sie IPv6-BGP-spezifische Routen zur internen Routingtabelle.
ns route-install IPv6 OSPF	Installieren Sie IPv6-OSPF-spezifische Routen für die interne Routingtabelle.

Beispiel:

```
>VTYSH
NS# configure terminal
NS# ns route-install Default
NS(config)# ns route-install RIP
NS(config)# ns route-install BGP
NS(config)# ns route-install OSPF
NS# ns route-install IPv6 Default
NS(config)# ns route-install IPv6 RIP
NS(config)# ns route-install IPv6 BGP
NS(config)# ns route-install IPv6 OSPF
<!--NeedCopy-->
```


Maximale Anzahl von ECMP-Routen, die in einer NetScaler-Appliance unterstützt werden

In einer NetScaler-Appliance werden bis zu 32 ECMP-Routen (Equal Cost Multiple Path) unterstützt. Die Routenauswahl basiert auf fünf Tupeln. Weitere Informationen finden Sie unter Routenauswahl anhand von fünf Tupeln.

Werbung von SNIP und VIP Routen zu selektiven Gebieten

January 19, 2021

Um einige SNIP-Adressen in selektiven Bereichen anzukündigen, können die Aktivierung des DRADV-Modus oder die Weiterverteilung von Verbindungen ZEBOS-Operationen nicht verwendet werden. Dies liegt daran, dass diese Operationen alle verbundenen Routen an ZEBOs senden. Außerdem ist das Hinzufügen von statischen Dummy-Routen in ZEBOs für die erforderlichen Subnetze oder das Hinzufügen von ACLs in ZEBOs, um unerwünschte verbundene Routen zu filtern, eine umständliche und mühsame Aufgabe.

Die Netzwerkroute und die Tag-Optionen beheben dieses Problem. Sie können die Option Netzwerkroute für nur eine SNIP-Adresse pro Subnetz aktivieren. Die verbundene Route für diese SNIP-Adresse wird als Kernelroute an ZebOS gesendet.

Für VIP- und SNIP-Adressen kann Tag eine ganze Zahl von 1 bis 4294967295 zugewiesen werden. Dieser Parameter kann nur festgelegt werden, wenn Hostroute oder Netzwerkroute für VIP- oder SNIP-Adressen aktiviert ist. Der Tag-Wert, der mit VIP- und SNIP-Adressen verknüpft ist, wird zusammen mit ihren Routen an ZEBOs gesendet. Tags mit unterschiedlichen Werten können für VIP- und SNIP-Routen eingestellt werden. Diese Tag-Werte können dann in Routenkarten in ZEBOs abgeglichen und in selektive Bereiche beworben werden.

SNIP-Routen in selektive Bereiche bewerben

So konfigurieren Sie die Netzwerk-Routen- und Tag-Parameter einer SNIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- Wenn Sie eine neue SNIP-Adresse hinzufügen:
  - **add ns ip** <IPAddress>@ <netmask> -**type SNIP** -**networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **ns ip anzeigen** <IPAddress>
- Wenn Sie eine vorhandene SNIP-Adresse neu konfigurieren:

- **set ns ip** <IPAddress>@ <netmask> -**type SNIP** - **networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
- **ns ip anzeigen** <IPAddress>

So konfigurieren Sie die Netzwerk-Routen- und Tag-Parameter einer SNIP-Adresse mit der GUI:

1. Navigieren Sie zu **System**> **Netzwerk**> **IPs**> **IPv4s**.
2. Legen Sie die Parameter **Netzwerkroute** und **Tag** fest, während Sie eine Subnetz-IP (SNIP) -Adresse hinzufügen oder eine vorhandene Subnetz-IP-Adresse ändern.

Bewerben Sie VIP-Routen in selektive Bereiche

So konfigurieren Sie die Host-Routen- und Tag-Parameter einer VIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein.

- Wenn Sie eine neue VIP-Adresse hinzufügen:
  - **add ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **ns ip anzeigen** <IPAddress>
- Wenn Sie eine vorhandene VIP-Adresse neu konfigurieren:
  - **set ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **ns ip anzeigen** <IPAddress>

So konfigurieren Sie die Netzwerk-Routen- und Tag-Parameter einer VIP-Adresse mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Legen Sie die **Hostroute** und **Tag-Parameter** fest, während Sie eine VIP-Adresse hinzufügen oder eine vorhandene VIP-Adresse ändern.

Bidirektionale Weiterleitungserkennung konfigurieren

May 11, 2023

Das BFD-Protokoll (Bidirectional Forwarding Detection) ist ein Mechanismus zur schnellen Erkennung von Ausfällen von Weiterleitungspfaden. BFD erkennt Pfadfehler in der Größenordnung von Millisekunden. BFD wird mit dynamischen Routing-Protokollen verwendet.

Im BFD-Betrieb tauschen Routing-Peers BFD-Pakete in einem ausgehandelten Intervall aus. Wenn innerhalb des ausgehandelten Intervalls plus Gnadenintervall kein Paket von einem Peer empfangen wird, gilt der Peer als tot und eine Benachrichtigung wird an die Gruppe der registrierten

Routing-Protokolle gesendet. Im Gegenzug berechnen die Routing-Protokolle den besten Pfad neu und programmieren die Routing-Tabelle neu. BFD unterstützt im Vergleich zu den von den Routing-Protokollen bereitgestellten Timern ein kleineres Zeitintervall, was zu einer schnelleren Erkennung von Ausfällen führt.

Die NetScaler-Appliance unterstützt BFD für die folgenden Routing-Protokolle: BGP (IPv4 und IPv6), OSPFv2 (IPv4) und OSPFv3 (IPv6). Die BFD-Unterstützung in der NetScaler-Appliance entspricht den RFCs 5880, 5881 und 5883.

Punkte, die bei der Konfiguration der Erkennung bidirektionaler Weiterleitungen zu beachten sind

Bevor Sie mit der Konfiguration von BFD beginnen, sollten Sie die folgenden Punkte beachten:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten von BFD verstehen, die in den RFCs 5880, 5881 und 5883 beschrieben werden.
- BFD auf einer NetScaler-Appliance wird für die folgenden Routing-Protokolle unterstützt:
  - BGP (IPv4 und IPv6)
  - OSPFv2 (IPv4)
  - OSPFv3 (IPv6)
- BFD auf einer NetScaler-Appliance wird für die folgenden Routing-Protokolle nicht unterstützt:
  - ISIS
  - RIP (IPv4)
  - RipNG (IPv6)
- Die folgenden BFD-Funktionen werden auf einer NetScaler-Appliance nicht unterstützt:
  - BFD Echo-Modus
  - BFD-Authentifizierung
  - BFD Demand asynchroner Modus
- Die Mindestwerte für BFD-Intervall- und BFD Rx-Timer betragen 100 Millisekunden.
- Wenn BFD in einer Topologie mit gemeinsam genutzten IP-Adressen verwendet wird (z. B. in einem Layer-2-Hochverfügbarkeits-Setup mit SNIP-Adressen oder einem Cluster-Setup mit Striped IP-Adressen), bringt BFD die aktiven Sitzungen während eines Failovers zum Erliegen, da die BFD-Fehlererkennungszeit (Reihenfolge der Millisekunden) geringer ist als das HA-Failover-Erkennungsintervall (3—4 Sekunden). Daher empfiehlt Citrix, Graceful Restart in Layer-2-HA-Topologien zu verwenden, da die Routen während des Failover-Prozesses beibehalten werden.

Konfigurationsschritte

Die Konfiguration von BFD auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- BFD-Parameter konfigurieren

- BFD-Unterstützung für dynamische Routing-Protokolle konfigurieren

BFD-Parameter konfigurieren

Die NetScaler-Appliance stellt separate BFD-Sitzungsparameter für Single-Hop-Sitzungen, IPv4-Multi-Hop-Sitzungen und IPv6-Multi-Hop-Sitzungen bereit. Wenn Sie BFD-Parameter nicht für einen Sitzungstyp konfigurieren, werden die Standardwerte für diese Sitzung angewendet.

Der Standardwert jedes BFD-Parameters ist derselbe für Single-Hop-Sitzungen, IPv4-Multi-Hop-Sitzungen und IPv6-Multi-Hop-Sitzungen. In der folgenden Tabelle wird der Standardwert jedes BFD-Parameters angezeigt.

BFD-Parametername	Standardwert
Intervall	750 Millisekunden
Minimaler Rx	500 Millisekunden
Multiplikator	3

> **WICHTIG:**
>
> Die Initialisierung von Mellanox-NICs in einer NetScaler ADC-Appliance dauert etwa 1500 ms. Sie müssen die BFD-Timer für eine NetScaler-Appliance mit Mellanox-NICs auf mehr als 1500 ms einstellen. Citrix empfiehlt, die BFD-Timer auf 3000 ms einzustellen:
>
> - Intervall Tx = 600 ms
> - Minimaler Rx = 600 ms
> - Multiplikator = 5

Konfiguration von BFD-Parametern für eine einzelne Hop-Sitzung

Um BFD-Parameter für eine einzelne Hop-Sitzung mithilfe der `VTYSH` Befehlszeile zu konfigurieren, geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die `VTYSH` Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`interface` `vlan ID>`	Rufen Sie den Schnittstellenkonfigurationsmodus auf.

Befehl	Spezifiziert
`bfd singlehop-peer interval <num> minrx <num> multiplier <num>`	Konfigurieren Sie die BFD-Parameter auf der angegebenen Schnittstelle.

Beispielkonfiguration:

```
> vtysh

ns# configure terminal

ns(config)# interface vlan3

ns(config-if)# bfd singlehop-peer interval 200 minrx 200 multiplier 5

ns(config-if)# exit
<!--NeedCopy-->
```

Konfiguration von BFD-Parametern für IPv4-Multi-Hop-Sitzungen

Um BFD-Parameter für IPv4-Multi-Hop-Sitzungen mithilfe der VTYSH Befehlszeile zu konfigurieren, geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`bfd multihop-peer <ipv4addr> interval <num> minrx <num> multiplier <num>`	Konfigurieren Sie die BFD-Parameter für IPv4-Multi-Hop-Sitzungen.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)# bfd multihop-peer 20.20.20.138 interval 300 minrx 300
       multiplier 5
```



```
6
7       ns(config)# exit
8   <!--NeedCopy-->
```

Konfiguration von BFD-Parametern für IPv6-Multi-Hop-Sitzungen

Um BFD-Parameter für IPv6-Multi-Hop-Sitzungen mithilfe der VTYSH Befehlszeile zu konfigurieren, geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`bfd multihop-peer ipv6 <ipv6addr> interval <num> minrx <num> multiplier <num>`	Konfigurieren Sie die BFD-Parameter für IPv6-Multi-Hop-Sitzungen.

Beispielkonfiguration:

```
1       > vtysh
2
3       ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx
            500 multiplier 5
4
5       ns(config)# exit
6   <!--NeedCopy-->
```

BFD-Unterstützung für dynamische Routing-Protokolle konfigurieren

Sie können BFD für ein dynamisches Routing-Protokoll für eine Art von Sitzung mit einem Peer aktivieren. Zum Beispiel Einzelhüpfen und mehrere Hopfen. Die NetScaler-Appliance wendet die entsprechenden BFD-Parametereinstellungen auf die Sitzung an.

Konfiguration von BFD für eine IPv4-BGP-Single-Hop-Sitzung

Um BFD für eine IPv4-BGP-Single-Hop-Sitzung mithilfe der VTYSH Befehlszeile zu konfigurieren, geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router bgp <asnumber>`	Autonomes BGP-System. `asnumber` ist ein erforderlicher Parameter.
`neighbor <ipv4addr> remote-as <num>`	Aktualisieren Sie die IPv4-BGP-Tabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
`neighbor <ipv4addr> fall-over bfd`	Aktiviere BFD für den angegebenen Nachbarn.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)#router bgp 1

    ns(config-router)#neighbor 20.20.20.138 remote-as 1

    ns(config-router)#neighbor 20.20.20.138 fall-over bfd

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Konfiguration von BFD für eine IPv4-BGP-Multi-Hop-Sitzung

Um BFD für eine IPv4-BGP-Multi-Hop-Sitzung mithilfe der VTYSH Befehlszeile zu konfigurieren, geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.

Befehl	Spezifiziert
`router bgp <asnumber>`	Autonomes BGP-System. `asnumber` ist ein erforderlicher Parameter.
`neighbor <ipv4addr> remote-as <num>`	Aktualisieren Sie die IPv4-BGP-Tabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
`neighbor <ipv4addr> fall-over bfd multihop`	Aktiviere BFD für den angegebenen Nachbarn.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)#router bgp 1

    ns(config-router)#neighbor 20.20.20.138 remote-as 1

    ns(config-router)#neighbor 20.20.20.138 fall-over bfd multihop

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Konfiguration von BFD für eine IPv6-BGP-Single-Hop-Sitzung

Um BFD für eine IPv6-BGP-Single-Hop-Sitzung mithilfe der `VTYSH` Befehlszeile zu konfigurieren, geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die `VTYSH` Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router bgp <asnumber>`	Autonomes BGP-System. `asnumber` ist ein erforderlicher Parameter.

Befehl	Spezifiziert
`neighbor <ipv6addr> remote-as <num>`	Aktualisieren Sie die IPv6-BGP-Tabelle mit der lokalen IPv6-Adresse des Links im angegebenen autonomen System.
`neighbor <ipv6addr> fall-over bfd`	Aktiviere BFD für den angegebenen Nachbarn.
`address-family ipv6`	Rufen Sie den Konfigurationsmodus für die
`neighbor <ipv6addr> activate`	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen dem Peer und dem lokalen Knoten mithilfe der lokalen Linkadresse aus.

Beispielkonfiguration:

```
> vtysh

ns# configure terminal ns(config)#router bgp 1

ns(config-router)#neighbor 30fe:123::124 remote-as 1

ns(config-router)#neighbor 30fe:123::124 fall-over bfd

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 30fe:123::124 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#exit

<!--NeedCopy-->
```

Konfiguration von BFD für eine IPv6-BGP-Multi-Hop-Sitzung

Um BFD für eine IPv6-BGP-Multi-Hop-Sitzung mithilfe der VTYSH Befehlszeile zu konfigurieren, geben Sie an der Befehlszeile die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.

Befehl	Spezifiziert
`router bgp <asnumber>`	Autonomes BGP-System. `asnumber` ist ein erforderlicher Parameter.
`neighbor <ipv6addr> remote-as <num>`	Aktualisieren Sie die IPv6-BGP-Tabelle mit der lokalen IPv6-Adresse des Links im angegebenen autonomen System.
`neighbor <ipv6addr> fall-over bfd multihop`	Aktiviere BFD für den angegebenen Nachbarn.
`address-family ipv6`	Rufen Sie den Konfigurationsmodus für die
`neighbor <ipv6addr> activate`	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen dem Peer und dem lokalen Knoten aus, indem Sie die link-lokale Adresse verwenden.

Beispielkonfiguration:

```
> vtysh

ns# configure terminal

ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx 500
    multiplier 5

ns(config)#router bgp 1

ns(config-router)#neighbor 20fe:125::138 remote-as 1

ns(config-router)#neighbor 20fe:125::138 fall-over bfd multihop

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 20fe:125::138 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#end

<!--NeedCopy-->
```


BFD für OSPFv2 (IPv4) auf Schnittstellen konfigurieren

Sie können BFD auf allen oder auf einer bestimmten Schnittstelle aktivieren, die das OSPFv2-Protokoll verwendet.

So konfigurieren Sie BFD für OSPFv2 auf allen Schnittstellen mithilfe der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router ospf <process tag>`	Rufen Sie den OSPFv2-Konfigurationsmodus auf.
`bfd all-interfaces`	Aktivieren Sie BFD auf allen Schnittstellen, die OSPFv2 verwenden.

Beispielkonfiguration:

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router ospf 1
6
7      ns(config-router)#bfd all-interfaces
8
9      ns(config-router)#redistribute kernel
10
11     ns(config-router)#exit
12 <!--NeedCopy-->
```

So konfigurieren Sie BFD für OSPFv2 auf einer bestimmten Schnittstelle mithilfe der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.

Befehl	Spezifiziert
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`interface` `<vlan ID>`	Rufen Sie den Schnittstellenkonfigurationsmodus auf.
`ip ospf bfd`	Aktivieren Sie BFD auf der angegebenen Schnittstelle, die OSPFv2 verwendet.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan5

    ns(config-if)# ip ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```

BFD für OSPFv3 (IPv6) auf Schnittstellen konfigurieren

Sie können BFD auf allen oder auf einer bestimmten Schnittstelle aktivieren, die das OSPFv3-Protokoll verwendet.

So konfigurieren Sie BFD für OSPFv3 auf allen Schnittstellen mithilfe der Befehlszeile: VTYSH

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router ipv6 ospf <process tag>`	Rufen Sie den OSPFv3-Konfigurationsmodus auf.
`bfd all-interfaces`	Aktivieren Sie BFD auf allen Schnittstellen, die OSPFv3 verwenden.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)#router ipv6 ospf 10

    ns(config-router)#bfd all-interfaces

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

So konfigurieren Sie BFD für OSPFv3 auf einer bestimmten Schnittstelle mithilfe der Befehlszeile: VTYSH

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
`vtysh`	Zeigt die VTYSH Befehlszeile an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`interface` <vlan ID>	Rufen Sie den Schnittstellenkonfigurationsmodus auf.
`ipv6 ospf bfd`	Aktivieren Sie BFD auf der angegebenen Schnittstelle, die OSPFv3 verwendet.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan15

    ns(config-if)# ipv6 ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```


Statische Routen konfigurieren

May 11, 2023

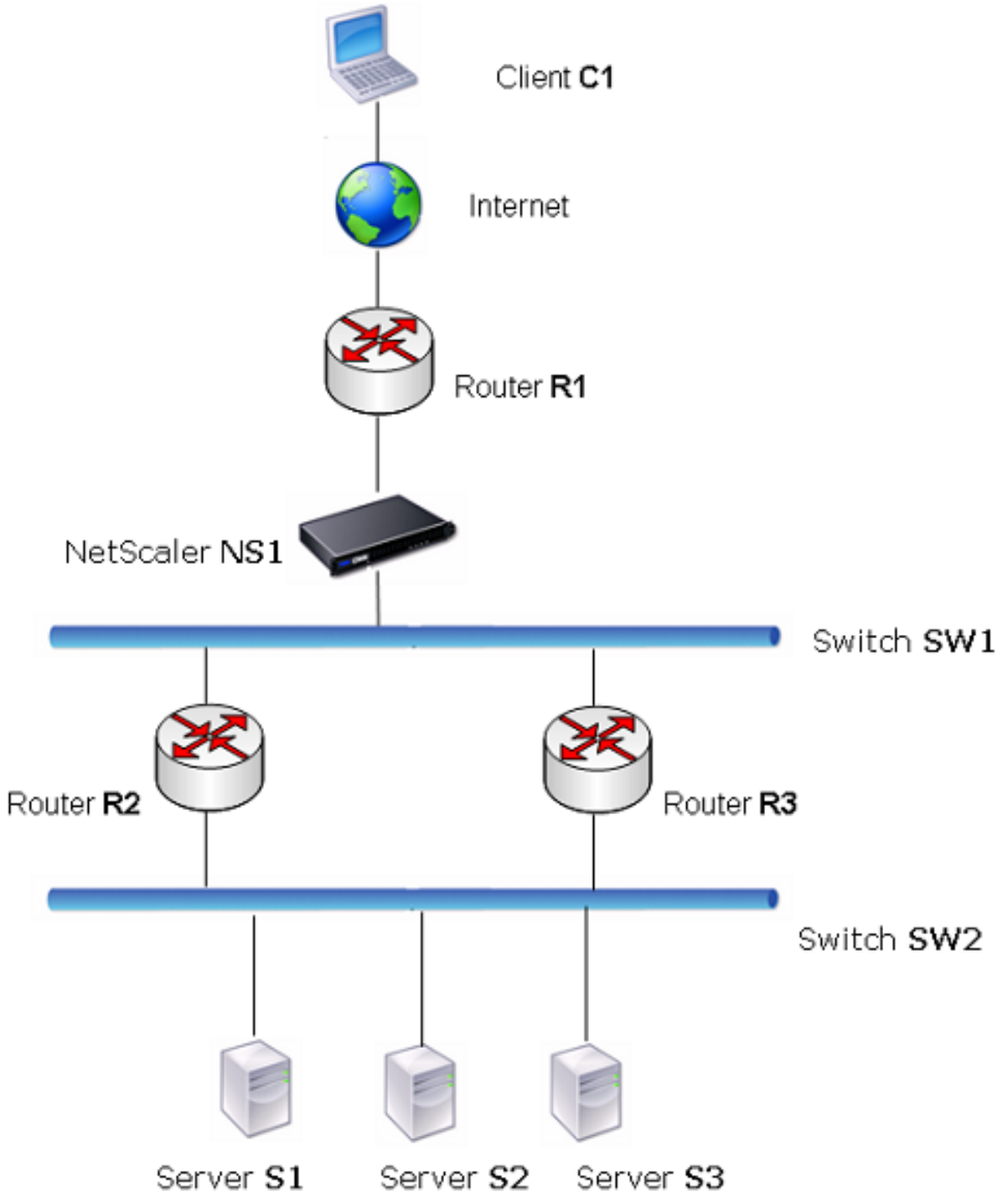
Statische Routen werden manuell erstellt, um die Leistung Ihres Netzwerks zu verbessern. Sie können statische Routen überwachen, um Betriebsunterbrechungen zu vermeiden. Außerdem können Sie ECMP-Routen Gewichte zuweisen und Nullrouten erstellen, um Routingschleifen zu vermeiden.

Überwachte statische Routen. Wenn eine manuell erstellte (statische) Route ausfällt, wird eine Backup-Route nicht automatisch aktiviert. Sie müssen die inaktive primäre statische Route manuell löschen. Wenn Sie die statische Route jedoch als überwachte Route konfigurieren, kann die NetScaler-Appliance automatisch eine Backup-Route aktivieren.

Die statische Routenüberwachung kann auch auf der Erreichbarkeit des Subnetzes basieren. Ein Subnetz ist normalerweise mit einer einzigen Schnittstelle verbunden, aber es kann logisch über andere Schnittstellen darauf zugegriffen werden. Subnetze, die an ein VLAN gebunden sind, sind nur zugänglich, wenn das VLAN aktiv ist. VLANs sind logische Schnittstellen, über die Pakete vom NetScaler übertragen und empfangen werden. Eine statische Route wird als DOWN markiert, wenn sich der nächste Hop in einem Subnetz befindet, das nicht erreichbar ist.

Hinweis: In einem Hochverfügbarkeits-Setup (HA) ist der Standardwert für Monitored State Routes (MSRs) auf dem sekundären Knoten UP. Der Wert ist so festgelegt, dass bei einem Failover keine Statusübergangslücke entsteht, die dazu führen könnte, dass Pakete auf diesen Routen verloren gehen.

Stellen Sie sich die folgende einfache Topologie vor, in der ein NetScaler den Datenverkehr zu einem Standort über mehrere Server verteilt.



Router R1 überträgt den Datenverkehr zwischen dem Client und der NetScaler-Appliance. Die Appliance kann die Server S1 und S2 über die Router R2 oder R3 erreichen. Es hat zwei statische Routen,

über die das Subnetz der Server erreicht werden kann, eine mit R2 als Gateway und eine mit R3 als Gateway. Bei beiden Routen ist die Überwachung aktiviert. Die administrative Entfernung der statischen Route mit Gateway R2 ist geringer als die der statischen Route mit Gateway R3. Daher wird R2 R3 vorgezogen, um den Datenverkehr an die Server weiterzuleiten. Außerdem zeigt die Standardroute auf dem NetScaler auf R1, sodass der gesamte Internetverkehr ordnungsgemäß beendet wird.

Wenn R2 ausfällt, während die Überwachung auf der statischen Route aktiviert ist, die R2 als Gateway verwendet, markiert der NetScaler sie als DOWN. Der NetScaler verwendet jetzt die statische Route mit R3 als Gateway und leitet den Datenverkehr über R3 an die Server weiter.

Der NetScaler unterstützt die Überwachung statischer IPv4- und IPv6-Routen. Sie können den NetScaler so konfigurieren, dass er eine statische IPv4-Route überwacht, indem Sie entweder einen neuen ARP- oder PING-Monitor erstellen oder vorhandene ARP- oder PING-Monitore verwenden. Sie können den NetScaler so konfigurieren, dass er eine statische IPv6-Route überwacht, indem Sie entweder einen neuen Neighbor Discovery für IPv6 (ND6) oder einen PING-Monitor erstellen oder die vorhandenen ND6- oder PING-Monitore verwenden.

Gewichtete statische Routen. Wenn die NetScaler-Appliance Routing-Entscheidungen trifft, die Routen mit gleicher Entfernung und gleichen Kosten beinhalten, d. h. Equal Cost Multi-Path (ECMP) -Routen, verteilt sie die Last zwischen ihnen, indem sie einen Hashing-Mechanismus verwendet, der auf den Quell- und Ziel-IP-Adressen basiert. Für eine ECMP-Route können Sie jedoch einen Gewichtungswert konfigurieren. Der NetScaler verwendet dann sowohl das Gewicht als auch den Hashwert, um die Last auszugleichen.

Null-Routen. Wenn die bei einer Routing-Entscheidung gewählte Route inaktiv ist, wählt die NetScaler-Appliance eine Backup-Route. Wenn nicht mehr auf alle Backup-Routen zugegriffen werden kann, leitet die Appliance das Paket möglicherweise an den Absender um, was zu einer Routing-Schleife führen kann, die zu einer Netzwerküberlastung führen kann. Um diese Situation zu verhindern, können Sie eine Nullroute erstellen, die eine Nullschnittstelle als Gateway hinzufügt. Die Nullroute ist niemals die bevorzugte Route, da sie eine höhere administrative Entfernung als die anderen statischen Routen hat. Es wird jedoch ausgewählt, wenn auf die anderen statischen Routen nicht mehr zugegriffen werden kann. In diesem Fall verwirft die Appliance das Paket und verhindert eine Routing-Schleife.

Statische IPv4-Routen konfigurieren

Sie können eine einfache statische Route oder eine Nullroute hinzufügen, indem Sie einige Parameter festlegen, oder Sie können zusätzliche Parameter festlegen, um eine überwachte oder überwachte und gewichtete statische Route zu konfigurieren. Sie können die Parameter einer statischen Route ändern. Sie könnten beispielsweise einer ungewichteten Route ein Gewicht zuweisen oder die Überwachung einer überwachten Route deaktivieren.

CLI-Verfahren

Um eine statische Route mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- Route hinzufügen <network><netmask><gateway>[-cost\<positive_integer>] [-advertise (DEAKTIVIERT | AKTIVIERT)]
- Route anzeigen [\<network>\ <netmask>[\<gateway>] [\<routeType>] [-detail]

Beispiel:

```
> add route 10.102.29.0 255.255.255.0 10.102.29.2 -cost 2 -advertise
   ENABLED
 Done
<!--NeedCopy-->
```

Um eine überwachte statische Route mit der CLI zu erstellen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine überwachte statische Route zu erstellen und die Konfiguration zu überprüfen:

- <positive_integer>Route hinzufügen <network><netmask><gateway>[-distance\<positive_integer>] [-weight][-msr (ENABLED | DISABLED) [-monitor <string>]]
- Route anzeigen [\<network>\ <netmask>[\<gateway>] [\<routeType>] [-detail]

Beispiel:

```
> add route 10.102.29.0 255.255.255.0 10.102.29.3 -distance 5 -weight 6
    -msr ENBLED -monitor PING
 Done
<!--NeedCopy-->
```

Um eine Nullroute mit der CLI zu erstellen:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- Route <network><netmask>null hinzufügen
- Route zeigen <network><netmask>

Beispiel:

```
> add route 10.102.29.0 255.255.255.0 null
 Done
<!--NeedCopy-->
```

Um eine statische Route mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

RM-Route <network><netmask><gateway>

Beispiel:

```
> rm route 10.102.29.0 255.255.255.0 10.102.29.3
 Done
<!--NeedCopy-->
```

GUI-Verfahren

Um eine statische Route mit der GUI zu konfigurieren:

Navigieren Sie zu System > Netzwerk > Routen und fügen Sie auf der Registerkarte Basic eine neue statische Route hinzu oder bearbeiten Sie eine bestehende statische Route.

Um eine Route mithilfe der GUI zu entfernen:

Navigieren Sie zu System > Netzwerk > Routen und löschen Sie auf der Registerkarte Basic die statische Route.

Statische IPv6-Routen konfigurieren

Sie können maximal sechs statische IPv6-Standardrouten konfigurieren. IPv6-Routen werden auf der Grundlage ausgewählt, ob die MAC-Adresse des Zielgeräts erreichbar ist. Dies kann mithilfe der IPv6-Funktion Neighbor Discovery ermittelt werden. Die Routen haben einen Lastenausgleich und es werden nur quell-/zielbasierte Hash-Mechanismen verwendet. Daher werden Routenauswahlmechanismen wie Round Robin nicht unterstützt. Die nächste Hop-Adresse in der Standardroute muss nicht zum NSIP-Subnetz gehören.

CLI-Verfahren

Um eine IPv6-Route mit der CLI zu erstellen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine IPv6-Route zu erstellen und die Konfiguration zu überprüfen:

- <positive_integer>Route6 hinzufügen <network><gateway>[-vlan\]
- <gateway>zeige Route 6 [\ <network>[\]

Beispiel:

```
> add route6 ::/0 FE80::67 -vlan 5
 Done
<!--NeedCopy-->
```


So erstellen Sie mit der CLI eine überwachte statische IPv6-Route:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine überwachte statische IPv6-Route zu erstellen und die Konfiguration zu überprüfen:

- <string>Route6 hinzufügen <network><gateway>[-msr (AKTIVIERT | DEAKTIVIERT) [-monitor\]
- <gateway>zeige Route 6 [\ <network>[\]

Beispiel:

```
> add route6 ::/0 2004::1 -msr ENABLED -monitor PING
 Done
<!--NeedCopy-->
```

Um eine IPv6-Route mit der CLI zu entfernen:

Geben Sie in der Befehlszeile Folgendes ein:

RM Route6 <network><gateway>

Beispiel:

```
> rm route6 ::/0 FE80::67
 Done
<!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie eine IPv6-Route mithilfe der GUI:

Navigieren Sie zu System > Netzwerk > Routen und fügen Sie auf der Registerkarte IPv6 eine neue IPv6-Route hinzu oder bearbeiten Sie eine bestehende IPv6-Route.

Um eine IPv6-Route mithilfe der GUI zu entfernen:

Navigieren Sie zu System > Netzwerk > Routen, und löschen Sie auf der Registerkarte IPv6 die IPv6-Route.

Routenintegritätseinschleusung basierend auf Einstellungen für virtuelle Server

May 11, 2023

Die folgende Option und der folgende Parameter wurden eingeführt, um die Route Health Injection (RHI) -Funktionalität der NetScaler-Appliance zur Werbung für die Route einer VIP-Adresse zu steuern.

- **VSVR_CNTRLD**. Es ist eine Option für den Parameter (Vserver RHI Level) einer VIP-Adresse. Wenn diese Option auf den Vserver RHI Level-Parameter gesetzt ist, hängt das Verhalten von RHI bei der Werbung für die Route der VIP-Adresse von der Einstellung des RHI STATE-Parameters auf allen zugehörigen virtuellen Servern der VIP-Adresse zusammen mit deren Status ab.
- **BUNDESSTAAT RHI**. Es ist ein Parameter des virtuellen Servers. Sie können den RHI STATE-Parameter entweder auf PASSIVE oder ACTIVE setzen. Standardmäßig ist der RHI STATE-Parameter auf PASSIVE gesetzt.

Wenn für eine VIP-Adresse der RHI-Parameter (Vserver RHI Level) auf VSVR_CNTRLD gesetzt ist, gelten für die VIP-Adresse auf der Grundlage der RHI STATE-Einstellungen auf den virtuellen Servern, die mit der VIP-Adresse verknüpft sind, unterschiedliche RHI-Verhaltensweisen für die VIP-Adresse:

- Wenn Sie RHI STATE auf allen virtuellen Servern auf PASSIVE setzen, kündigt der NetScaler immer die Route für die VIP-Adresse an.
- Wenn Sie RHI STATE auf allen virtuellen Servern auf ACTIVE setzen, kündigt der NetScaler die Route für die VIP-Adresse an, wenn sich mindestens einer der zugehörigen virtuellen Server im Status UP befindet.
- Wenn Sie RHI STATE auf einigen auf ACTIVE und auf anderen auf PASSIVE setzen, kündigt der NetScaler die Route für die VIP-Adresse an, wenn sich mindestens einer der zugehörigen virtuellen Server, dessen RHI STATE auf ACTIVE gesetzt ist, im Status UP befindet.

Die folgende Tabelle zeigt das Beispiel für ein RHI-Verhalten für eine VIP-Adresse auf der Grundlage der RHI STATE-Einstellungen auf den virtuellen Servern, die der VIP-Adresse zugeordnet sind. Die NetScaler-Appliance verfügt über zwei virtuelle Server V1 und V2, die der VIP-Adresse zugeordnet sind:

Assoziierte virtuelle Server für einen VIP	Bundesstaat 1	Bundesstaat 2	Bundesstaat 3	Bundesstaat 4
RHI State ist auf allen virtuellen Servern auf PASSIVE gesetzt				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Die Route für diese VIP-Adresse bewerben?	Ja	Ja	Ja	Ja

Assoziierte virtuelle Server für einen VIP	Bundesstaat 1	Bundesstaat 2	Bundesstaat 3	Bundesstaat 4
RHI State ist auf allen virtuellen Servern auf ACTIVE gesetzt				
V1	UP	UP	DOWN	DOWN
V2	UP	DOWN	UP	DOWN
Die Route für diese VIP-Adresse bewerben?	Ja	Ja	Ja	Nein
RHI State ist auf einem virtuellen Server auf ACTIVE und auf dem anderen auf PASSIVE gesetzt				
V1 (RHI-Status = AKTIV)	UP	UP	DOWN	DOWN
V2 (RHI-Zustand = PASSIV)	UP	DOWN	UP	DOWN
Die Route für diese VIP-Adresse bewerben?	Ja	Ja	Nein	Nein

Gehen Sie wie folgt vor, um RHI für eine VIP-Adresse zu konfigurieren, die auf der RHI-Parametereinstellung (RHI State) der zugehörigen virtuellen Server basiert:

- Stellen Sie den Parameter RHI (Vserver RHI Level) für die VIP-Adresse auf VSVR_CNTRLD ein.
- Stellen Sie den RHI State-Parameter für jeden virtuellen Server ein, der der VIP-Adresse zugeordnet ist.

So legen Sie das vServer RHI Level für eine VIP-Adresse mithilfe der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- **richte uns ein [** <IPAddress><vserverRHILevel>-** vServerRhilevel\]

So legen Sie den RHI-State-Parameter eines virtuellen Servers mit der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- **set lb vserver** <name>[-**RHIState** (**PASSIV** | **AKTIV)]**

So legen Sie den vServer RHI-Level für eine VIP-Adresse mit der GUI fest

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**.
2. Wählen Sie eine VIP-Adresse aus und klicken Sie dann auf **Bearbeiten**.
3. **Stellen Sie den**Vserver RHI Level-Parameter auf **VSVR_CNTRLDein, und klicken Sie dann auf OK.**

So legen Sie den RHI-State-Parameter eines virtuellen Servers mithilfe der GUI fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie einen virtuellen Load-Balancing-Server aus, und klicken Sie dann auf **Bearbeiten**.
3. Legen Sie den Parameter **RHI State** fest, und klicken Sie dann auf **OK** .

Richtlinienbasierte Routen konfigurieren

May 11, 2023

Richtlinienbasiertes Routing stützt Routing-Entscheidungen auf Kriterien, die Sie angeben. Eine Policy-Based Route (PBR) legt Kriterien für die Auswahl von Paketen und in der Regel einen nächsten Hop fest, an den die ausgewählten Pakete gesendet werden sollen. Sie können die NetScaler-Appliance beispielsweise so konfigurieren, dass ausgehende Pakete von einer bestimmten IP-Adresse oder einem bestimmten Bereich an einen bestimmten Next-Hop-Router weitergeleitet werden. Jedes Paket wird in der durch die angegebenen Prioritäten bestimmten Reihenfolge mit jeder konfigurierten PBR abgeglichen, bis eine Übereinstimmung gefunden wird. Wenn keine Übereinstimmung gefunden wird oder wenn die übereinstimmende PBR eine DENY-Aktion angibt, wendet NetScaler die Routingtabelle für normales zielbasiertes Routing an.

Ein PBR stützt Routing-Entscheidungen für die Datenpakete auf Parameter wie Quell-IP-Adresse, Quellport, Ziel-IP-Adresse, Zielport, Protokoll und Quell-MAC-Adresse. Ein PBR definiert die Bedingungen, die ein Paket erfüllen muss, damit der NetScaler das Paket weiterleiten kann. Diese Aktionen werden als „Verarbeitungsmodi“ bezeichnet. „ Die Verarbeitungsmodi sind:

- **ERLAUBEN.** Die Appliance sendet das Paket an den angegebenen Next-Hop-Router.
- **LEUGNEN.** Der NetScaler wendet die Routingtabelle für normales zielbasiertes Routing an.

Sie können PBRs für ausgehenden IPv4- und IPv6-Verkehr erstellen.

Viele Benutzer erstellen zunächst PBRs und ändern sie dann. Um ein neues PBR zu aktivieren, müssen Sie es anwenden. Um eine PBR zu deaktivieren, können Sie sie entweder entfernen oder deaktivieren. Sie können die Prioritätsnummer eines PBR ändern, um ihm eine höhere oder niedrigere Priorität zu geben.

Policy-Based Routes (PBR) für IPv4-Verkehr

May 11, 2023

Die Konfiguration von PBRs umfasst die folgenden Aufgaben:

- Erstellen Sie eine PBR.
- Wenden Sie PBRs an.
- (Optional) Deaktivieren oder aktivieren Sie eine PBR.
- (Optional) Nummerieren Sie die Priorität des PBR neu.

PBR erstellen oder ändern

Sie können nicht zwei PBRs mit denselben Parametern erstellen. Wenn Sie versuchen, ein Duplikat zu erstellen, wird eine Fehlermeldung angezeigt.

Sie können die Priorität einer PBR konfigurieren. Die Priorität (ein ganzzahliger Wert) definiert die Reihenfolge, in der die NetScaler-Appliance PBRs auswertet. Wenn Sie eine PBR erstellen, ohne eine Priorität anzugeben, weist der NetScaler automatisch eine Priorität zu, die ein Vielfaches von 10 ist.

Wenn ein Paket die von der PBR definierte Bedingung erfüllt, führt der NetScaler eine Aktion aus. Wenn das Paket nicht der durch die PBR definierten Bedingung entspricht, vergleicht der NetScaler das Paket mit der PBR mit der nächsthöheren Priorität.

Anstatt die ausgewählten Pakete an einen Next-Hop-Router zu senden, können Sie den PBR so konfigurieren, dass er sie an einen virtuellen Link-Load-Balancing-Server sendet, an den Sie mehrere Next-Hops gebunden haben. Diese Konfiguration kann ein Backup bereitstellen, falls ein Next-Hop-Link ausfällt.

Sehen Sie sich das folgende Beispiel an. Zwei PBRs, p1 und p2, sind auf dem NetScaler konfiguriert und ihnen werden automatisch die Prioritäten 20 und 30 zugewiesen. Sie müssen einen dritten PBR, p3, hinzufügen, der unmittelbar nach dem ersten PBR, p1, ausgewertet werden soll. Das neue PBR, p3, muss eine Priorität zwischen 20 und 30 haben. In diesem Fall können Sie die Priorität auf 25 festlegen.

CLI-Verfahren

Um eine PBR mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- add ns pbr <name> <action> [-srcIP [\<operator>] <srcIPVal>] [-srcPort [\<operator>] <srcPortVal>] [-destIP [\<operator>] <destIPVal>] [-destPort [\<operator>] <destPortVal>] [-nextHop \<nextHopVal>] [-srcMac \<mac_addr>] [-protocol \<protocol> |-protocolNumber \<positive_integer>] [-vlan \<positive_integer>] [-interface \<interface_name>] [-priority \<positive_integer>] [-msr (ENABLED | DISABLED) [-monitor \<string>]] [-state (ENABLED | DISABLED)]
- show ns pbr

Beispiel:

```
> add ns pbr pbr1  allow -srcip 10.102.37.252 -destip 10.10.10.2 -
    nexthop 10.102.29.77
 Done
<!--NeedCopy-->
```

So ändern Sie die Priorität einer PBR mithilfe der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Priorität zu ändern und die Konfiguration zu überprüfen:

- set ns pbr <name> [-action (ALLOW | DENY)] [-srcIP [\<operator>] <srcIPVal>] [-srcPort [\<operator>] <srcPortVal>] [-destIP [\<operator>] <destIPVal>] [-destPort [\<operator>] <destPortVal>] [-nextHop \<nextHopVal>] [-srcMac \<mac_addr>] [-protocol \<protocol> | -protocolNumber \<positive_integer>] [-vlan \<positive_integer>] [-interface \<interface_name>] [-priority \<positive_integer>] [-msr (ENABLED | DISABLED) [-monitor \<string>]] [-state (ENABLED | DISABLED)]
- show ns pbr [\<name>]

Beispiel:

```
> set ns pbr pbr1 -priority 23
 Done
<!--NeedCopy-->
```

Um eine oder alle PBRs mit der CLI zu entfernen:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- rm ns pbr <name>
- clear ns pbrs

Beispiel:


```
> rm ns pbr pbr1
 Done

> clear ns PBRs
 Done
<!--NeedCopy-->
```

GUI-Verfahren

Um eine PBR mit der GUI zu erstellen:

Navigieren Sie zu System > Netzwerk > PBRs und fügen Sie auf der Registerkarte PBRs eine neue PBR hinzu oder bearbeiten Sie eine vorhandene PBR.

Um eine oder alle PBRs mithilfe der GUI zu entfernen:

Navigieren Sie zu System > Netzwerk > PBRs und löschen Sie auf der Registerkarte PBRs die PBR.

PBR anwenden

Sie müssen eine PBR anwenden, um sie zu aktivieren. Das folgende Verfahren wendet erneut alle PBRs an, die Sie nicht deaktiviert haben. Die PBRs bilden einen Speicherbaum (Lookup-Tabelle). Wenn Sie beispielsweise 10 PBRs (p1 - p10) erstellen und dann eine weitere PBR (p11) erstellen und anwenden, werden alle PBRs (p1 - p11) neu angewendet und eine neue Nachschlagetabelle wird erstellt. Wenn zu einer Sitzung ein DENY-PBR-Wert gehört, wird die Sitzung zerstört.

Sie müssen dieses Verfahren nach jeder Änderung anwenden, die Sie an einer PBR vornehmen. Beispielsweise müssen Sie dieses Verfahren befolgen, nachdem Sie eine PBR deaktiviert haben.

Hinweis: Auf der NetScaler-Appliance erstellte PBRs funktionieren erst, wenn sie angewendet werden.

So wenden Sie eine PBR mit der CLI an:

Geben Sie in der Befehlszeile Folgendes ein:

als PBRs anwenden

So wenden Sie eine PBR mit der GUIan:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBRs die PBR aus und wählen Sie in der Aktionsliste die Option Anwenden aus.

PBRs aktivieren oder deaktivieren

Standardmäßig sind die PBRs aktiviert. Das bedeutet, dass die NetScaler-Appliance eingehende Pakete automatisch mit den konfigurierten PBRs vergleicht, wenn PBRs angewendet werden. Wenn eine PBR in der Nachschlagetabelle nicht erforderlich ist, aber in der Konfiguration beibehalten werden muss, muss sie deaktiviert werden, bevor die PBRs angewendet werden. Nachdem die PBRs angewendet wurden, vergleicht der NetScaler eingehende Pakete nicht mit deaktivierten PBRs.

So aktivieren oder deaktivieren Sie eine PBR mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns pbr <name>
- deaktiviere ns pbr <name>

Beispiel:

```
> enable ns PBR pbr1
 Done
> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
        Active Status: ENABLED                  Applied Status: APPLIED
        Priority: 10
        NextHop: 10.102.29.77

 Done

> disable ns PBR pbr1
Warning: PBR modified, use 'apply pbrs' to commit this operation

> apply pbrs
 Done

> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
        Active Status: DISABLED                 Applied Status:
            NOTAPPLIED
```



```
        Priority: 10
        NextHop: 10.102.29.77
Done
<!--NeedCopy-->
```

Um eine PBR mithilfe der GUI zu aktivieren oder zu deaktivieren:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBRs die PBR aus und wählen Sie in der Aktionsliste die Option Aktivieren oder Deaktivieren aus.

PBRs neu nummerieren

Sie können die PBRs automatisch neu nummerieren, um ihre Prioritäten auf ein Vielfaches von 10 festzulegen.

Um PBRs mit der CLI neu zu nummerieren:

Geben Sie in der Befehlszeile Folgendes ein:

- ns pbrs neu nummerieren

Um PBRs mithilfe der GUI neu zu nummerieren:

Navigieren Sie zu System > Netzwerk > PBRs und wählen Sie auf der Registerkarte PBRs in der Aktionsliste die Option Priorität (n) neu nummerieren aus.

Anwendungsfall — PBR mit mehreren Hops

Stellen Sie sich ein Szenario vor, in dem zwei PBRs, PBR1 und PBR2, auf der NetScaler Appliance NS1 konfiguriert sind. PBR1 leitet alle ausgehenden Pakete mit der Quell-IP-Adresse 10.102.29.30 an den Next-Hop-Router R1 weiter. PBR2 leitet alle ausgehenden Pakete mit der Quell-IP-Adresse 10.102.29.90 an den Next-Hop-Router R2 weiter. R3 ist ein weiterer Next-Hop-Router, der mit NS1 verbunden ist.

Wenn Router R1 ausfällt, werden alle ausgehenden Pakete, die mit PBR1 übereinstimmten, verworfen. Um diese Situation zu vermeiden, können Sie beim Erstellen oder Ändern einer PBR im nächsten Hop-Feld einen virtuellen Link Load Balancing-Server (LLB) angeben. Mehrere Next-Hops sind als Dienste an den virtuellen LLB-Server gebunden (zum Beispiel R1, R2 und R3). Wenn R1 nun ausfällt, werden alle Pakete, die mit PBR1 übereinstimmten, an R2 oder R3 weitergeleitet, wie es durch die auf dem virtuellen LLB-Server konfigurierte LB-Methode bestimmt wird.

Die NetScaler-Appliance gibt in den folgenden Fällen einen Fehler aus, wenn Sie versuchen, eine PBR mit einem virtuellen LLB-Server als nächsten Hop zu erstellen:

- Hinzufügen einer weiteren PBR mit demselben virtuellen LLB-Server.

- Angabe eines nicht existierenden virtuellen LLB-Servers.
- Angabe eines virtuellen LLB-Servers, für den die gebundenen Dienste keine nächsten Hops sind.
- Angeben eines virtuellen LLB-Servers, für den die LB-Methode nicht auf eine der folgenden Werte festgelegt ist:
  - ROUNDROBIN
  - DESTINATIONIPHASH
  - SOURCEIPHASH
  - SRCIPDESTIPHASH
  - LEASTPACKETS
  - LEASTBANDWIDTH
  - LTRM
  - CALLIDHASH
  - CUSTOM LOAD
- Angabe eines virtuellen LLB-Servers, für den der LB-Persistenztyp nicht auf einen der folgenden Werte gesetzt ist:
  - DESTIP
  - SOURCEIP
  - SRCDSTIP

In der folgenden Tabelle sind die Namen und Werte der auf der NetScaler-Appliance konfigurierten Entitäten aufgeführt:

Typ der Entität	Name	IP-Adresse
Virtueller Server für Link-Load-Balancing	LLB1	Nicht verfügbar
Dienstleistungen (nächste Geschäfte)	Router1	1.1.1.254
	Router2	2.2.2.254
	Router3	3.3.3.254
PBRs	PBR1	Nicht verfügbar
	PBR2	Nicht verfügbar

Tabelle 1. Beispielwerte für die Erstellung von Entitäten

Um die oben beschriebene Konfiguration zu implementieren, müssen Sie:

1. Erstellen Sie die Dienste Router1, Router2 und Router3, die die Next-Hop-Router R1, R2 und R3 repräsentieren.
2. Erstellen Sie den virtuellen Link-Load-Balancing-Server LLB1 und binden Sie die Dienste

Router1, Router2 und Router3 daran.

3. Erstellen Sie die PBRs PBR1 und PBR2, wobei die Next-Hop-Felder jeweils auf LLB1 und 2.2.2.254 (IP-Adresse des Routers R2) gesetzt sind.

So erstellen Sie einen Dienst über die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- Dienst hinzufügen <name><IP><serviceType><port>
- show service <name>

Beispiel:

```
> add service Router1 1.1.1.254 ANY *
 Done
> add service Router2 2.2.2.254 ANY *
 Done
> add service Router3 3.3.3.254 ANY *
 Done
<!--NeedCopy-->
```

So erstellen Sie einen Dienst über die GUI:

Navigieren Sie zu Traffic Management > Load Balancing > Servicesund erstellen Sie einen Dienst.

Um einen virtuellen Link-Load-Balancing-Server zu erstellen und einen Dienst mithilfe der CLI zu binden, gehen Sie wie folgt vor:

Geben Sie in der Befehlszeile Folgendes ein:

- lb vserver hinzufügen <name><serviceType>
- binde lb vserver < name> <serviceName>
- lb vserver anzeigen < name>

Beispiel:

```
> add lb vserver LLB1 ANY
 Done
> bind lb vserver LLB1 Router1 Router2 Router3
 Done
<!--NeedCopy-->
```

Um einen virtuellen Link-Load-Balancing-Server zu erstellen und einen Dienst mithilfe der GUI zu binden, gehen Sie wie folgt vor:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server, und erstellen Sie einen virtuellen Server für den Link-Lastenausgleich. Geben Sie **ANY** im Feld **Protokoll** an.
   Hinweis: Vergewissern Sie sich, dass
   Direkt adressierbar deaktiviert ist.

2. Aktivieren Sie auf der Registerkarte **Dienste** in der Spalte **Aktiv** das Kontrollkästchen für den Dienst, den Sie an den virtuellen Server binden möchten.

Um eine PBR mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- <nextHopVal>füge ns pbr <name><action>[-script [\]] [-nextHop\ <operator><srcIPVal>] hinzu
- show ns pbr

Beispiel:

```
> add pbr PBR1 ALLOW -srcIP 10.102.29.30 -nextHop LLB1
 Done
> add pbr PBR2 ALLOW -srcIP 10.102.29.90 -nextHop 2.2.2.254
 Done
<!--NeedCopy-->
```

Um eine PBR mit der GUI zu erstellen:

Navigieren Sie zu System > Netzwerk > PBRs, fügen Sie auf der Registerkarte PBRs eine neue PBR hinzu.

Policy-Based Routes (PBR6) für IPv6-Verkehr

May 11, 2023

Die Konfiguration von PBR6s umfasst die folgenden Aufgaben:

- Erstellen Sie eine PBR6.
- PBR6s auftragen.
- (Optional) Deaktivieren oder aktivieren Sie einen PBR6.
- (Optional) Nummerieren Sie die Priorität des PBR6 neu.

PBR6 erstellen oder ändern

Sie können nicht zwei PBR6 mit denselben Parametern erstellen. Wenn Sie versuchen, ein Duplikat zu erstellen, wird eine Fehlermeldung angezeigt.

Sie können die Priorität einer PBR6 konfigurieren. Die Priorität (ein ganzzahliger Wert) definiert die Reihenfolge, in der die NetScaler-Appliance PBR6s auswertet. Wenn Sie eine PBR6 erstellen, ohne eine Priorität anzugeben, weist der NetScaler automatisch eine Priorität zu, die ein Vielfaches von 10 ist.

Wenn ein Paket die von der PBR6 definierte Bedingung erfüllt, führt der NetScaler eine Aktion aus. Wenn das Paket nicht der von der PBR6 definierten Bedingung entspricht, vergleicht der NetScaler das Paket mit der PBR6 mit der nächsthöheren Priorität.

CLI-Verfahren

Um eine PBR6 mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ns pbr6** <name> <action> [-srcIPv6 [\<operator>] <srcIPv6Val>] [-srcPort [\<operator>] <srcPortVal>] [-destIPv6 [\<operator>] <destIPv6Val>] [-destPort [\<operator>] <destPortVal>] [-srcMac \<mac_addr>] [-protocol \<protocol> |-protocolNumber \<positive_integer>] [-vlan \<positive_integer>] [-interface \<interface_name>] [-priority \<positive_integer>] [-state (ENABLED | DISABLED)] [-msr (ENABLED | DISABLED) [-monitor \<string>]] [-nextHop \<nextHopVal>] [-nextHopVlan \<positive_integer>]
- show ns pbr

So ändern oder entfernen Sie eine PBR6 mithilfe der CLI:

Um einen PBR6 zu ändern, geben **Sie den Befehl set pbr6** <name>und die zu ändernden Parameter mit ihren neuen Werten ein.

Um eine oder alle PBR6s mit der CLI zu entfernen:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **rm ns pbr6** <name>
- **Clear ns pbr6**

GUI-Verfahren

Um eine PBR6 mithilfe der GUI zu erstellen oder zu ändern:

Navigieren Sie zu System > Netzwerk > PBRs und fügen Sie auf der Registerkarte PBR6s eine neue PBR6 hinzu oder bearbeiten Sie eine vorhandene PBR6.

Um einen oder alle PBR6 mit der GUI zu entfernen:

Navigieren Sie zu System > Netzwerk > PBRs und löschen Sie auf der Registerkarte PBR6s die PBR6.

PBR6s anwenden

Sie müssen einen PBR6 anwenden, um ihn zu aktivieren. Das folgende Verfahren wendet erneut alle PBR6 an, die Sie nicht deaktiviert haben. Die PBR6 bilden einen Speicherbaum (Lookup-Tabelle). Wenn Sie beispielsweise 10 PBR6 (p6_1 - p6_10) erstellen und dann ein weiteres PBR6

(p6_11) erstellen und anwenden, werden alle PBR6 (p6_1 - p6_11) neu angewendet und eine neue Nachschlagetabelle wird erstellt. Wenn zu einer Sitzung ein DENY PBR6 gehört, wird die Sitzung zerstört.

Sie müssen dieses Verfahren nach jeder Änderung anwenden, die Sie an einer PBR6 vornehmen. Beispielsweise müssen Sie dieses Verfahren befolgen, nachdem Sie eine PBR6 deaktiviert haben.

Hinweis: PBR6s, die auf der NetScaler-Appliance erstellt wurden, funktionieren erst, wenn sie angewendet werden.

So wenden Sie PBR6s mit der CLI an:

Geben Sie in der Befehlszeile Folgendes ein:

- **apply ns PBR6**

PBR6s mithilfe der GUI anwenden:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBR6s die PBR6 aus und wählen Sie in der Aktionsliste die Option Anwenden aus.

PBR6 aktivieren oder deaktivieren

Standardmäßig sind die PBR6s aktiviert. Das bedeutet, dass die NetScaler-Appliance ausgehende IPv6-Pakete automatisch mit den konfigurierten PBR6-Paketen vergleicht, wenn PBR6 angewendet werden. Wenn eine PBR6 in der Nachschlagetabelle nicht erforderlich ist, sie aber in der Konfiguration beibehalten werden muss, muss sie deaktiviert werden, bevor die PBR6 angewendet werden. Nachdem die PBR6 installiert wurden, vergleicht der NetScaler eingehende Pakete nicht mit deaktivierten PBR6s.

Um eine PBR6 mit der CLI zu aktivieren oder zu deaktivieren:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **enable ns pbr** <name>
- **disable ns pbr** <name>

PBR6 mithilfe der GUI aktivieren oder deaktivieren:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBR6s die PBR6 aus und wählen Sie in der Aktionsliste die Option Aktivieren oder Deaktivieren aus.

PBR6s neu nummerieren

Sie können die PBR6 automatisch neu nummerieren, um ihre Prioritäten auf ein Vielfaches von 10 festzulegen.

PBR6s mit der CLI neu nummerieren:

Geben Sie in der Befehlszeile Folgendes ein:

- **renumber ns pbr6**

Um PBR6s mithilfe der GUI neu zu nummerieren:

Navigieren Sie zu System > Netzwerk > PBRs, wählen Sie auf der Registerkarte PBR6s in der Liste Aktion die Option Priorität (n) neu nummerieren aus.

MAC-Adress-Platzhaltermaske für PBRs

January 19, 2021

Ein Platzhaltermasken-Parameter wurde für erweiterte PBRs und PBR6s eingeführt und wird zusammen mit dem Quell-MAC-Adressparameter verwendet, um einen Bereich von MAC-Adressen zu definieren, die mit der MAC-Quelladresse ausgehender Pakete übereinstimmen.

Platzhaltermasken geben an, welche Hexadezimalziffern der MAC-Adresse verwendet werden und welche Hexadezimalziffern ignoriert werden. Der Parameter Platzhaltermaske gibt eine Reihe von Einsen und Nullen an und hat eine Länge von 12 Ziffern. Jede Ziffer ist eine Maske für die entsprechende hexadezimale Ziffer der MAC-Adresse. Eine Nullziffer in der Platzhaltermaske gibt an, dass die entsprechende Hexadezimalziffer der MAC-Adresse berücksichtigt werden muss, und eine Ziffer gibt an, dass die entsprechende Hexadezimalziffer ignoriert werden soll.

Die Platzhaltermaske sollte die folgenden Bedingungen erfüllen:

- Hat nur eine Reihe von Nullen
- Hat nur eine Reihe von
- Beginnen Sie mit einer Reihe von Nullen

Im Folgenden finden Sie einige Beispiele für gültige Platzhaltermasken:

- 000000111111
- 000000011111
- 000011111111

Im Folgenden finden Sie einige Beispiele für ungültige Platzhaltermasken:

- 000000111100
- 111110000000
- 010101010101

Für eine PBR-Regel definiert eine Platzhaltermaske 000000111111 für MAC-Adresse 96:fa: 95:1 d: 67:4 a den MAC-Adressbereich 96:FA: 95:00:00:00 - 96:FA:95:FF:FF:FF. Dieser MAC-Adressbereich wird mit der Quell-MAC-Adresse der ausgehenden Pakete abgeglichen.

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer PBR-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show ns pbr** <pbrname>

Beispiel:

```
> add ns pbr PBR-1 ALLOW -srcip 192.0.2.34 -srcMac 96:fa:95:1d:67:4a
    - srcMacMask 000000111111 -nexthop 198.51.100.1

 Done
```

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer PBR6-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr6** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show pbr6** <pbr6name>

Beispiel:

```
> add ns pbr6 PBR6-1 ALLOW  - srcipv6 2001:db8:0::7 -srcMac 96:fa:95:1d
   :67:4a   - srcMacMask 000000001111 -nexthop 2001:db8:0::1
 Done
```

NULL-Richtlinienbasierten Routen zum Löschen ausgehender Pakete

May 12, 2023

In einigen Situationen kann es erforderlich sein, dass die NetScaler-Appliance bestimmte ausgehende Pakete verwirft, anstatt sie weiterzuleiten, z. B. in Testfällen und während der Bereitstellungsmigration.

Auf NULL-Richtlinien basierende Routen können verwendet werden, um bestimmte ausgehende Pakete zu löschen. Ein NULL-PBR-Typ ist ein PBR-Typ, bei dem der Parameter nexthop auf NULL gesetzt ist. Die NetScaler-Appliance verwirft ausgehende Pakete, die einer NULL-PBR entsprechen.

Konfiguration von NULL-PBRs für IPv4-Pakete

Um eine NULL-PBR mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ns pbr** <name> ALLOW [**-td** <positive_integer>] [-**srcIP** [<operator>] <srcIPVal>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIP** [<operator>] <destIPVal>] [-**destPort** [<operator>] <destPortVal>] (-**nextHop NULL**) [**srcMac** <mac_addr> [-**srcMacMask** <string>]] [-**protocol** <protocol> | -**protocolNumber** <positive_integer>] [-**vlan** <positive_integer> | -**vxlan** <positive_integer>] [-**interface** <interface_name>] [-**priority** <positive_integer>] [-**msr** (**ENABLED** | **DISABLED**) [-**monitor** <string>]] [-**state** (**ENABLED** | **DISABLED**)[-**ownerGroup** <string>]
- **apply ns pbrs**
- **show ns pbr**<id>

So konfigurieren Sie eine NULL-PBR mithilfe der GUI:

Navigieren Sie zu **System** > **Netzwerk**> **PBRs** und fügen Sie auf der Registerkarte **PBRs** eine **neue NULL-PBR hinzu oder bearbeiten Sie eine vorhandene NULL-PBR**.

Beispiel-Konfiguration

In der folgenden Beispielkonfiguration ist NULL PBR6 PBR6-NULL-EXAMPLE-1 für das Löschen aller ausgehenden IPv6-Pakete von der Schnittstelle 1/5 konfiguriert.

```
> add ns pbr PBR6-NULL-EXAMPLE-1 ALLOW  - nextHop NULL -interface 1/5
 Done

> apply ns pbr6
 Done
```

Verkehrsverteilung auf mehreren Routen basierend auf fünf Tupelinformationen

May 11, 2023

In einem Load Balancing-Setup kann eine NetScaler-Appliance über mehrere Routen verfügen, um ein Paket an ihr Ziel zu senden. Zum Beispiel: zu einem Server und zu einem Client.

Eine NetScaler-Appliance verwendet einen Hashing-Algorithmus, um eine Route zum Senden des Pakets an sein Ziel auszuwählen.

Der Hash-Algorithmus verwendet die folgenden zwei Tupel eines Pakets, um einen Hash zu berechnen, auf dessen Grundlage die NetScaler-Appliance eine Route für das Paket auswählt.

- Quell-IP-Adresse

- Ziel-IP-Adresse

Die Auswahl von Routen basierend auf zwei Tupelinformationen kann zu einer ungleichmäßigen Verteilung des Verkehrs auf den verfügbaren Routen führen. Diese ungleichmäßige Verkehrsverteilung führt auf einigen Strecken zu einer Überlastung des Verkehrs.

Um dieses Problem zu beheben, verwendet die NetScaler-Appliance ab Build 13.0 71.x die folgenden fünf Tupelinformationen eines Pakets im Hashing-Algorithmus, um eine Route für das Paket auszuwählen:

- Quell-IP-Adresse (Client-IP)
- Quellport (Client-Port)
- Ziel-IP-Adresse (Service-IP)
- Zielport (Serviceport)
- Nummer des Protokolls

Die Auswahl der Routen anhand von Informationen aus fünf Tupeln gewährleistet eine gleichmäßige Verteilung des Verkehrs auf den verfügbaren Routen. Diese gleichmäßige Verteilung des Verkehrs verhindert eine Überlastung des Verkehrs auf einer Route.

Betrachten Sie ein Beispiel für ein Load Balancing Setup, bei dem ein Client eine Anfrage an die VIP-Adresse sendet. Die NetScaler-Appliance verwendet die folgenden fünf Tupelinformationen, um eine Route zum Senden des Anforderungspakets an den Server mit Lastausgleich auszuwählen:

- Quell-IP-Adresse (Client-IP-Adresse)
- Quellport (Client-Port)
- Ziel-IP-Adresse (Service-IP-Adresse)
- Zielport (Dienstportnummer)
- Nummer des Protokolls

Wenn der Modus “Quell-IP verwenden” (USIP) aktiviert ist, werden alle fünf Tupel als Hash-Eingabe für die Auswahl einer Route betrachtet. Wenn der Modus “Subnetz-IP verwenden” (USNIP) aktiviert ist, werden sowohl SNIP als auch Quellport nicht als Eingabe betrachtet, da sie nach der Routenauswahl ausgewählt werden. Informationen zur Konfiguration des USIP- und USNIP-Modus finden Sie unter Aktivieren des Quell-IP-Modus und Konfigurieren von Subnetz-IP-Adressen (SNIPs).

> **Hinweis:**
>
> Ab Build 13.1 30.x verwendet die NetScaler-Appliance den Fünf-Tupel-Hash-Algorithmus anstelle des Zwei-Tupel-Hash-Algorithmus, um eine Route für Load Balancing Monitorprüfungen auszuwählen.

Vorrang bei anderen auf der Routenauswahl basierenden NetScaler-Funktionen

In diesem Abschnitt wird die Priorität der Routenauswahl basierend auf dem Feature mit fünf Tupeln und anderen Funktionen im Zusammenhang mit der Routenauswahl in einer NetScaler-Appliance er-

läutert.

- **Policy-basierte Routen (PBR)**. PBR-Regeln haben immer Vorrang vor der Routenauswahl basierend auf fünf Tupel.
- **Mac-basierte Weiterleitung (MBF)**. In einer Load-Balancing-Konfiguration hat die auf fünf Tupel basierende MBF- oder Routenauswahl in den folgenden Fällen Vorrang:
  - Für einen Client initiierten Datenverkehr zur VIP-Adresse der Load Balancing-Konfiguration in der NetScaler-Appliance:
    * Fordert Datenverkehr an, der für einen Server mit Lastausgleich bestimmt Die Routenauswahl auf der Grundlage von fünf Tupeln hat Vorrang vor MBF.
    * Response Traffic, der für den Client bestimmt ist. MBF hat Vorrang vor der Routenauswahl basierend auf fünf Tupeln.
  - Für einen Server, der den Datenverkehr zur SNIP-Adresse in der NetScaler-Appliance initiiert hat:
    * Response Traffic, der für den Client bestimmt ist. Die Routenauswahl auf der Grundlage von fünf Tupeln hat Vorrang vor MBF.
    * Fordert Datenverkehr an, der für einen Server mit Lastausgleich bestimmt MBF hat Vorrang vor der Routenauswahl basierend auf fünf Tupeln.

Problembehandlung von Routingproblemen

May 11, 2023

Um Ihren Fehlerbehebungsprozess so effizient wie möglich zu gestalten, sammeln Sie zunächst Informationen über Ihr Netzwerk. Sie benötigen die folgenden Informationen über die NetScaler-Appliance und andere Systeme im Netzwerk:

- Vollständiges Topologiediagramm, einschließlich Schnittstellenkonnektivität und Details zum Zwischenschalter.
- Konfiguration wird ausgeführt. Sie können den Befehl show running verwenden, um die laufende Konfiguration für ns.conf und Zebos.conf abzurufen.
- Ausgabe des Befehls History, um festzustellen, ob Konfigurationsänderungen vorgenommen wurden, als das Problem auftrat.
- Ausgabe der Befehle Top und ps -ax, um festzustellen, ob ein Routing-Daemon die CPU überbeansprucht oder sich schlecht benimmt.
- Alle Routing-bezogenen Kerndateien in /var/core - nsm, bgpd, ospfd oder ripd. Überprüfe den Zeitstempel, um zu sehen, ob sie relevant sind.
- dr_error.log- und dr_info.log Dateien aus /var/log.
- Ausgabe des Datumsbefehls und der Uhrzeitdetails für alle relevanten Systeme. Druckt die

Daten nacheinander auf allen Geräten aus, sodass die Uhrzeiten in den Protokollmeldungen mit verschiedenen Ereignissen korreliert werden können.
- Relevante ns.log, newnslog-Dateien.
- Konfigurationsdateien, Protokolldateien und Details zum Befehlsverlauf von Upstream- und Downstream-Routern.

Häufig gestellte Fragen zum Generischen Routing

January 19, 2021

Benutzer haben in der Regel die folgenden Fragen zur Behandlung von generischen Routingproblemen:

- Wie speichere ich die Konfigurationsdateien?

  Der Schreibbefehl von VTYSH speichert nur Zebos.conf. Führen Sie den Befehl save ns config von CLI aus, um sowohl ns.conf als auch zebos.conf Dateien zu speichern.

- Wenn ich sowohl eine statische Standardroute als auch eine dynamisch erlernte Standardroute konfiguriert habe, welche ist die bevorzugte Standardroute?

  Die dynamisch erlernte Route ist die bevorzugte Standardroute. Dieses Verhalten ist für Standardrouten eindeutig. Im Falle des Netzwerkdienstleistungsmoduls (Network Services Module, NSM) wird jedoch eine statisch konfigurierte Route im RIB gegenüber einer dynamischen Route bevorzugt. Die Route, die in die NSM FIB heruntergeladen wird, ist die statische Route.

- Wie kann ich die Werbung für Standardrouten blockieren?

  Die Standardroute wird nicht in ZEBOs injiziert.

- Wie kann ich die Debug-Ausgabe von Netzwerk-Daemons anzeigen?

  Sie können die Debugging-Ausgabe von Netzwerk-Daemons in eine Datei schreiben, indem Sie den folgenden Protokolldatei-Befehl aus der globalen Konfigurationsansicht in VTYSH eingeben:

  ```
  ns(config)# log file /var/ZebOS.log
  <!--NeedCopy-->
  ```

  Sie können die Debug-Ausgabe an die Konsole leiten, indem Sie den Terminalmonitor-Befehl aus der VTYSH Benutzeransicht eingeben:

  ```
  ns# terminal monitor
  <!--NeedCopy-->
  ```


- Wie sammle ich Kerne laufender Daemons?

  Sie können das gcore-Dienstprogramm verwenden, um Kerne von laufenden Daemons für die Verarbeitung durch gdb zu sammeln. Dies kann beim Debuggen von Daemons hilfreich sein, ohne den gesamten Routingvorgang zum Stillstand zu bringen.

```
gcore [-s] [-c core] [executable] pid
<!--NeedCopy-->
```

  Die Option -s stoppt den Daemon vorübergehend, während das Core-Image gesammelt wird. Dies ist eine empfohlene Option, da sie garantiert, dass das resultierende Image den Kern in einem konsistenten Zustand zeigt.

```
root@ns#gcore -s -c nsm.core /netscaler/nsm 342
<!--NeedCopy-->
```

- Wie führe ich einen Stapel von ZeBOS-Befehlen aus?

  Sie können einen Stapel von ZeBOS-Befehlen aus einer Datei ausführen, indem Sie den Befehl VTYSH -f <file-name> eingeben. Dadurch wird die laufende Konfiguration nicht ersetzt, sondern an sie angehängt. Wenn Sie jedoch Befehle zum Löschen der vorhandenen Konfiguration in der Batchdatei einfügen und diese dann für die neue gewünschte Konfiguration hinzufügen, können Sie diesen Mechanismus verwenden, um eine bestimmte Konfiguration zu ersetzen:

```
!
router bgp 234
network 1.1.1.1 255.255.255.0
!
route-map bgp-out2 permit 10
 set metric 9900
 set community 8602:300
!
<!--NeedCopy-->
```

Problembehandlung von OSPF-spezifischen Problemen

May 11, 2023

Bevor Sie mit dem Debuggen eines OSPF-spezifischen Problems beginnen, müssen Sie Informationen von der NetScaler-Appliance und allen Systemen im betroffenen LAN, einschließlich Upstream- und Downstream-Routern, sammeln. Geben Sie zunächst die folgenden Befehle ein:

1. zeige die Schnittstelle von nscli und VTYSH

2. zeige die IP-OSPF-Schnittstelle
3. zeige IP OSPF Nachbardetails
4. IP-Route anzeigen
5. IP-OSPF-Route anzeigen
6. Zusammenfassung der IP-OSPF-Datenbank anzeigen
    - Wenn die Datenbank nur wenige LSAs enthält, geben Sie show ip ospf database router, show ip ospf database A. network, show ip ospf database external und andere Befehle ein, um die vollständigen Details der LSAs abzurufen.
    - Wenn die Datenbank eine große Anzahl von LSAs enthält, geben Sie den Befehl show ip ospf database self-originated ein.
7. zeig ip ospf
8. zeig uns. Dadurch wird sichergestellt, dass die Details aller VIPs, die von Interesse sind, enthalten sind.
9. Rufen Sie die Protokolle von Peering-Geräten ab und führen Sie den folgenden Befehl aus:

    ```
    gcore -s -c xyz.core /netscaler/ospfd <pid>
    ```

    Hinweis: Der Befehl gcore ist unterbrechungsfrei.

Sammeln Sie zusätzliche Informationen vom NetScaler wie folgt:

1. Aktivieren Sie die Protokollierung von Fehlermeldungen, indem Sie den folgenden Befehl aus der globalen Konfigurationsansicht in VTYSH eingeben:

    ```
    ns(config)# log file /var/ospf.log
    <!--NeedCopy-->
    ```

2. Aktivieren Sie das Debuggen von ospf-Ereignissen und protokollieren Sie sie mit dem folgenden Befehl:

    ```
    ns(config) #log file /var/ospf.log
    <!--NeedCopy-->
    ```

    Debug ospf lsa packet nur dann aktivieren, wenn die Anzahl der LSAs in der Datenbank relativ klein ist (< 500).

Internetprotokoll Version 6 (IPv6)

May 11, 2023

Eine NetScaler-Appliance unterstützt sowohl serverseitiges als auch clientseitiges IPv6 und kann daher als IPv6-Knoten fungieren. Es kann Verbindungen von IPv6-Knoten (sowohl Hosts als auch Router) und von IPv4-Knoten akzeptieren und eine Protokollübersetzung (RFC 2765) durchführen, bevor Datenverkehr an die Dienste gesendet wird.

In der folgenden Tabelle sind einige der IPv6-Funktionen aufgeführt, die die NetScaler-Appliance unterstützt.

Tabelle 1. Einige unterstützte IPv6-Funktionen

IPv6-Funktionen
IPv6-Adressen für SNIPs (NSIP6, VIP6 und SNIP6)
Nachbarerkennung (Adressauflösung, Erkennung doppelter Adressen, Erkennung unerreichbarer Nachbarn, Routererkennung)
Verwaltungsanwendungen (ping6, telnet6, ssh6)
Statisches Routing und dynamisches Routing (OSPF, BGP, RIPNG und ISIS)
Portbasierte VLANs
Zugriffskontrolllisten für IPv6-Adressen (ACL6)
IPv6-Protokolle (TCP6, UDP6, ICMP6)
Serverseitiger Support (IPv6-Adressen für vServer, Dienste)
USIP (Quell-IP verwenden) und DSR (Direct Server Return) für IPv6
SNMP und VPN für IPv6
HA mit nativer IPv6-Knotenadresse
IPv6-Adressen für MIPs
Path-MTU-Erkennung für IPv6

Implementierung der IPv6-Unterstützung

Sie müssen die IPv6-Funktion auf einer NetScaler-Appliance aktivieren, bevor Sie sie verwenden oder konfigurieren können. Wenn IPv6 deaktiviert ist, verarbeitet der NetScaler keine IPv6-Pakete. Es zeigt die folgende Warnung an, wenn Sie einen nicht unterstützten Befehl ausführen:

```
"Warning: Feature(s) not enabled [IPv6PT]"
<!--NeedCopy-->
```

Verwenden Sie eines der folgenden Verfahren, um IPv6 zu aktivieren oder zu deaktivieren.

CLI-Verfahren

Gehen Sie wie folgt vor, um IPv6 mithilfe der CLI zu aktivieren oder zu deaktivieren:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns feature ipv6pt
- disable ns feature ipv6pt

GUI-Verfahren

Um IPv6 mithilfe der GUI zu aktivieren oder zu deaktivieren:

1. Navigieren Sie zu **System** > **Einstellungen**und klicken Sie in der Gruppe **Modi und Funktionen** auf **Erweiterte Funktionen konfigurieren**.
2. Wählen oder deaktivieren Sie die Option **IPv6-Protokollübersetzung** .

VLAN-Unterstützung

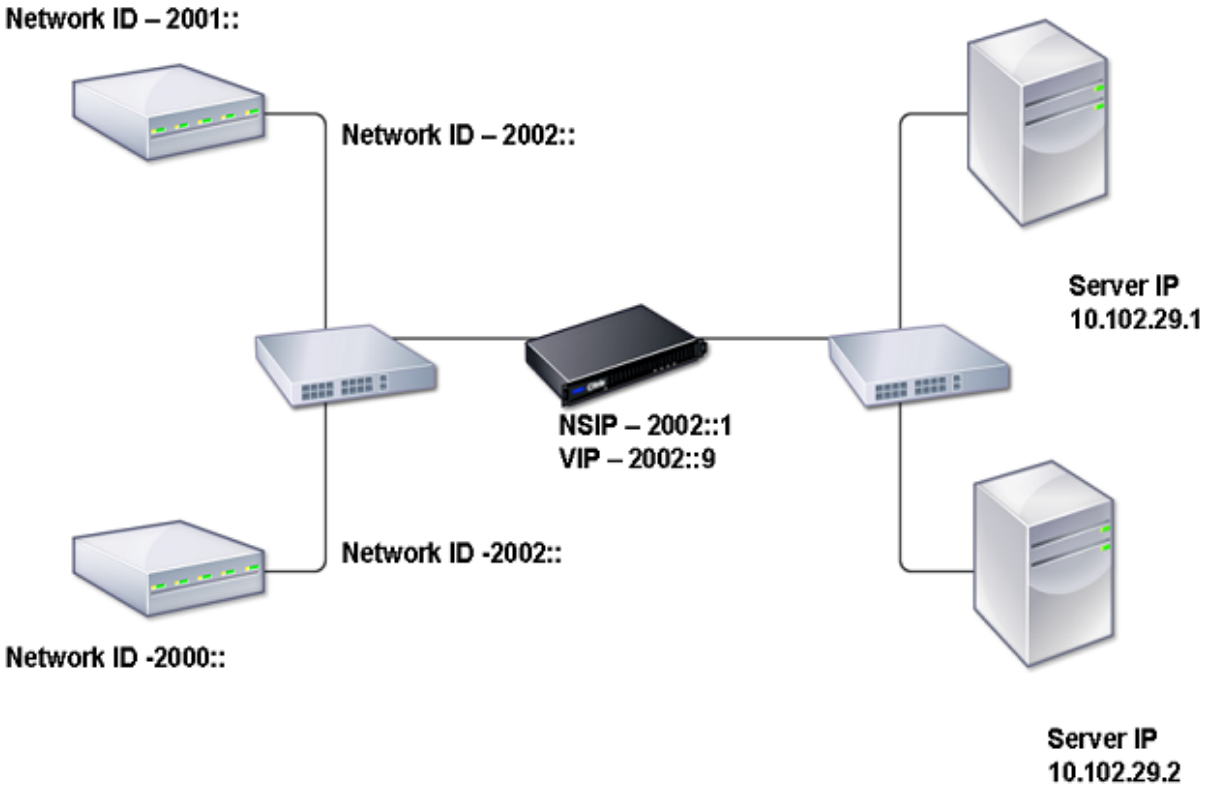
Wenn Sie Broadcast- oder Multicast-Pakete senden müssen, ohne das VLAN zu identifizieren (z. B. während DAD für NSIP oder ND6 für den nächsten Hop der Route), können Sie die NetScaler-Appliance so konfigurieren, dass das Paket an allen Schnittstellen mit entsprechendem Tagging gesendet wird. Das VLAN wird durch ND6 identifiziert, und ein Datenpaket wird nur auf das VLAN gesendet. Weitere Informationen zu ND6 und VLANs finden Sie unter Konfigurieren von Neighbor Discovery.

Port-basierte VLANs sind für IPv4 und IPv6 üblich. Präfixbasierte VLANs werden für IPv6 unterstützt.

Einfaches Einsatzszenario

Im Folgenden finden Sie ein Beispiel für ein einfaches Load-Balancing-Setup, das aus einem virtuellen IPv6-Server und IPv4-Diensten besteht, wie im folgenden Topologiediagramm dargestellt.

Abbildung 1. IPv6-Beispieltopologie



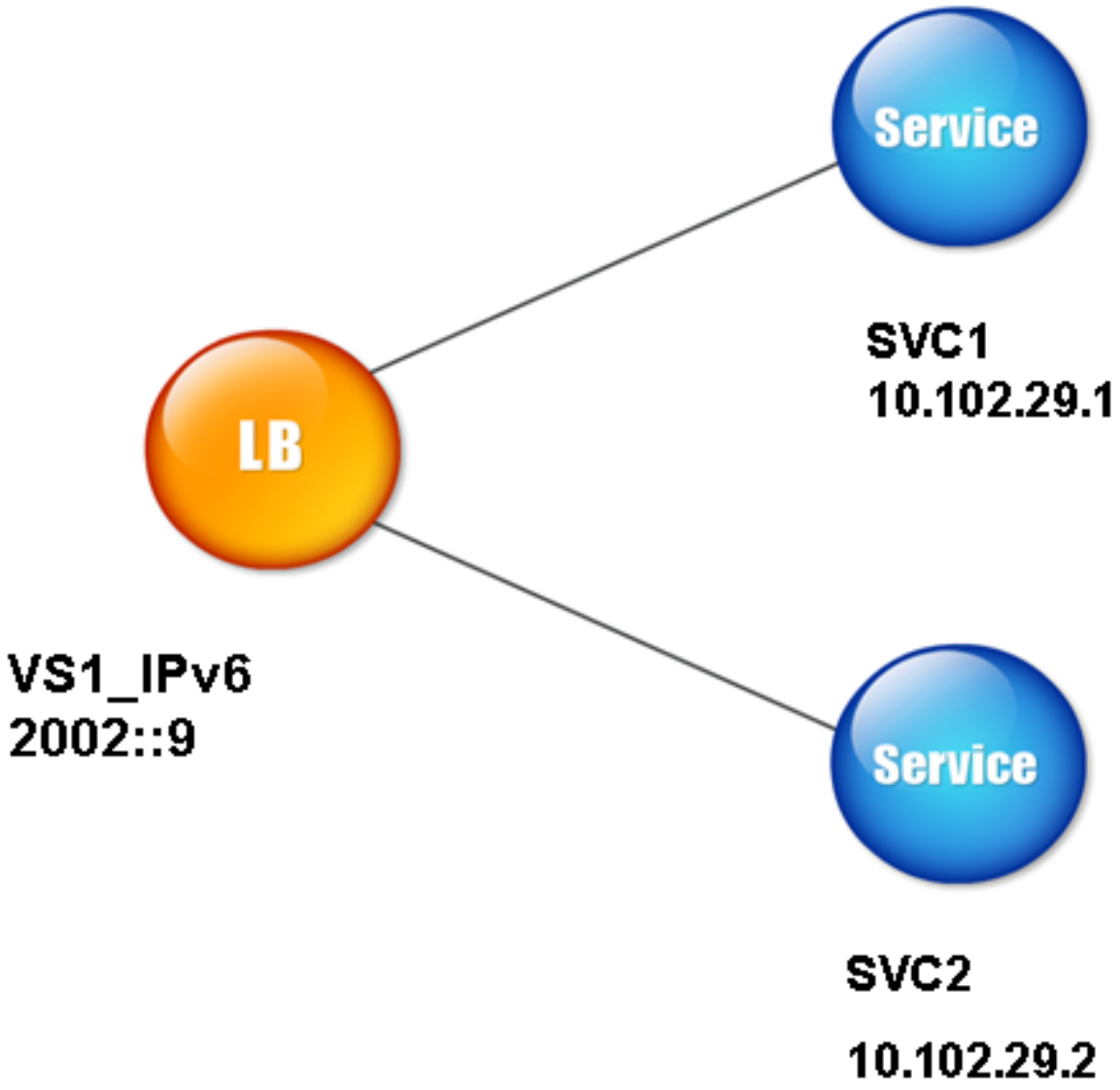
In der folgenden Tabelle sind die Namen und Werte der Entitäten zusammengefasst, die auf dem NetScaler konfiguriert werden müssen.

Tabelle 2. Beispielwerte für die Erstellung von Entitäten

Entitätstyp	Name	Wert
LB V-Server	VS1_IPv6	2002::9
Services	SVC1	10.102.29.1
	SVC2	10.102.29.2

Die folgende Abbildung zeigt die Entitäten und Werte der Parameter, die auf dem NetScaler konfiguriert werden sollen.

Abbildung 2. IPv6-Entitätsdiagramm



Um dieses Bereitstellungsszenario zu konfigurieren, müssen Sie wie folgt vorgehen:

1. Erstellen Sie einen IPv6-Dienst.
2. Erstellen Sie einen IPv6-LB-vserver.
3. Binden Sie die Dienste an den vserver.

CLI-Verfahren

So erstellen Sie IPv4-Dienste mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **Dienst hinzufügen** <Name><IPAddress><Protocol><Port>
- **sh-Dienst** <Name>

Beispiel:

```
> add service SVC1 10.102.29.1 HTTP 80
Done

>add service SVC2 10.102.29.2 HTTP 80
Done
<!--NeedCopy-->
```

Um einen IPv6-vserver mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- **lb vserver hinzufügen** <Name><IPAddress><Protocol><Port>
- **sh lab vserver** <Name>

Beispiel:

```
> add lb vserver VS1_IPv6 2002::9 HTTP 80
Done
<!--NeedCopy-->
```

Um einen Dienst mit der CLI an einen LB-vserver zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- **binde lb vserver** <name><service>
- **sh lb vserver** <name>

Beispiel:

```
> bind lb vserver VS1_IPv6 SVC1
Done
<!--NeedCopy-->
```

GUI-Verfahren

So erstellen Sie IPv4-Dienste mithilfe der GUI:

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, klicken Sie auf **Hinzufügen**und legen Sie dann die folgenden Parameter fest:

- Dienstname
- IP-Adresse
- Protokoll

- Port

Um einen IPv6-vServer mithilfe der GUI zu erstellen:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, klicken Sie auf **Hinzufügen**und aktivieren Sie das Kontrollkästchen **IPv6** .
2. Legen Sie die folgenden Parameter fest:
   - Name
   - Protokoll
   - IP-Adresstyp
   - IP-Adresse
   - Port

Um einen Dienst mithilfe der GUI an einen LB-vserver zu binden:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie auf der Seite **Load Balancing Virtual** Servers den vServer aus, für den Sie den Dienst binden möchten (z. B. VS1_IPv6).
3. Klicken Sie auf **Öffnen**.
4. Aktivieren **Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing)** auf der Registerkarte **Dienste** das Kontrollkästchen **Aktiv**, das dem Dienst entspricht, den Sie an den vServer binden möchten (z. B. SVC1).
5. Klicken Sie auf **OK**.
6. Wiederholen Sie die Schritte 1 bis 4, um den Dienst zu binden (z. B. SVC2 an den vServer).

Änderung des Host-Headers

Wenn eine HTTP-Anfrage eine IPv6-Adresse im Host-Header hat und der Server die IPv6-Adresse nicht versteht, müssen Sie die IPv6-Adresse einer IPv4-Adresse zuordnen. Die IPv4-Adresse wird dann im Host-Header der HTTP-Anfrage verwendet, die an den vServer gesendet wird.

CLI-Verfahren

Um die IPv6-Adresse im Host-Header mithilfe der CLI in eine IPv4-Adresse zu ändern:

Geben Sie in der Befehlszeile Folgendes ein:

- **set ns ip6** <IPv6Address> -**map** <IPAddress>
- **sh und ip6** <IPv6Address>

Beispiel:

```
> set ns ip6 2002::9 -map 200.200.200.200
Done
<!--NeedCopy-->
```


GUI-Verfahren

Um die IPv6-Adresse im Host-Header mithilfe der GUI in eine IPv4-Adresse zu ändern:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** und wählen Sie auf der Registerkarte **IPv6s** die IP-Adresse aus, für die Sie eine zugeordnete IP-Adresse konfigurieren möchten, z. B. 2002:0:0:0:0:0:0:9, und klicken Sie auf Bearbeiten.
2. Geben Sie in das Textfeld **Zugeordnete IP** die zugeordnete IP-Adresse ein, die Sie konfigurieren möchten, z. B. 200.200.200.200.

VIP-Einfügung

Wenn eine IPv6-Adresse an einen IPv4-basierten Server gesendet wird, versteht der Server die IP-Adresse im HTTP-Header möglicherweise nicht und generiert möglicherweise einen Fehler. Um dies zu vermeiden, können Sie dem IPv6-VIP eine IPv4-Adresse zuordnen. Anschließend können Sie die VIP-Einfügung aktivieren, um das Einfügen der IPv4-VIP-Adresse und Portnummer in die an die Server gesendeten HTTP-Anfragen zu ermöglichen.

CLI-Verfahren

So konfigurieren Sie eine Map-IPv6-Adresse mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

set ns ip6 <IPv6Address> -**map** <IPAddress>

Beispiel:

```
> set ns ip6 2002::9 -map 200.200.200.200
 Done
<!--NeedCopy-->
```

Um die VIP-Einfügung mit der CLI zu aktivieren:

Geben Sie in der Befehlszeile Folgendes ein:

- **set lb vserver** <name> -**insertVserverIPPort** <Value>
- **sh lb vserver** <name>

Beispiel:

```
> set lb vserver VS1_IPv6 -insertVserverIPPort ON
 Done

<!--NeedCopy-->
```


GUI-Verfahren

So konfigurieren Sie eine Map-IPv6-Adresse mithilfe der GUI:

1. **Navigieren Sie zu**System**>**Netzwerk**>**IPs**, wählen Sie auf der Registerkarte**IPv6s**die IP-Adresse aus, für die Sie eine Map-IP-Adresse konfigurieren möchten, z. B. 2002:0:0:0:0:0:0:9, und klicken Sie auf Bearbeiten.**
2. Geben Sie in das Textfeld **Zugeordnete IP** die Zuordnungs-IP-Adresse ein, die Sie konfigurieren möchten, z. B. 200.200.200.200.

Um die VIP-Einfügung mithilfe der GUI zu aktivieren:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie den virtuellen Server aus, für den Sie das Einfügen von Port aktivieren möchten, und klicken Sie auf **Bearbeiten**.
2. Wählen Sie auf der Registerkarte **Erweitert** unter **Verkehrseinstellungen**im Dropdownlistenfeld **Vserver IP Port Insertion** die Option **VIPADDR**aus.
3. Geben Sie im Textfeld **Vserver IP Port Insertion** den VIP-Header ein.

Traffic-Domänen

May 11, 2023

> **Warnung**
>
> Citrix empfiehlt, Adminpartitionen anstelle von Traffic Domains zu verwenden. Weitere Informationen finden Sie auf der Seite Admin-Partitionierung .

Verkehrsdomänen sind eine Möglichkeit, den Netzwerkverkehr für verschiedene Anwendungen zu segmentieren. Sie können Verkehrsdomänen verwenden, um mehrere isolierte Umgebungen in einer NetScaler-Appliance zu erstellen. Eine Anwendung, die zu einer bestimmten Verkehrsdomäne gehört, kommuniziert mit Entitäten und verarbeitet den Datenverkehr innerhalb dieser Domäne. Der Verkehr, der zu einer Verkehrsdomäne gehört, kann die Grenze einer anderen Verkehrsdomäne nicht überschreiten.

Vorteile der Verwendung von Traffic Domains

Die Hauptvorteile der Verwendung von Verkehrsdomänen auf einer NetScaler-Appliance sind folgende:

- **Verwendung doppelter IP-Adressen in einem Netzwerk**. Verkehrsdomänen ermöglichen es Ihnen, doppelte IP-Adressen im Netzwerk zu verwenden. Sie können dieselbe IP-Adresse oder Netzwerkadresse mehreren Geräten in einem Netzwerk oder mehreren Entitäten auf

einer NetScaler-Appliance zuweisen, solange jede der doppelten Adressen zu einer anderen Verkehrsdomäne gehört.

- **Verwendung doppelter Entitäten auf der NetScaler-Appliance**. Mit Verkehrsdomänen können Sie auch doppelte NetScaler-Feature-Entitäten auf der Appliance verwenden. Sie können Entitäten mit denselben Einstellungen erstellen, solange jede Entität einer separaten Verkehrsdomäne zugewiesen ist.
  Hinweis: Doppelte Entitäten mit demselben Namen werden nicht unterstützt.
- **Mehrverhältnis**. Mithilfe von Verkehrsdomänen können Sie Hosting-Dienste für mehrere Kunden bereitstellen, indem Sie die Art des Anwendungsverkehrs jedes Kunden innerhalb eines definierten Adressraums im Netzwerk isolieren.

Eine Verkehrsdomäne wird eindeutig durch eine Kennung identifiziert, bei der es sich um einen ganzzahligen Wert handelt. Jede Verkehrsdomäne benötigt ein VLAN oder eine Reihe von VLANs. Die Isolationsfunktionalität der Verkehrsdomäne hängt von den an die Verkehrsdomäne gebundenen VLANs ab. Mehr als ein VLAN kann an eine Verkehrsdomäne gebunden sein, aber dasselbe VLAN kann nicht Teil mehrerer Verkehrsdomänen sein. Daher hängt die maximale Anzahl von Verkehrsdomänen, die erstellt werden können, von der Anzahl der auf der Appliance konfigurierten VLANS ab.

Standard-Verkehrsdomäne

Eine NetScaler-Appliance verfügt über eine vorkonfigurierte Verkehrsdomäne, die als *Standardverkehrsdomäne*bezeichnet wird und eine ID von 0 hat. Alle Werkseinstellungen und Konfigurationen sind Teil der Standard-Verkehrsdomäne. Sie können andere Traffic-Domains erstellen und dann den Traffic zwischen der Standard-Verkehrsdomäne und den anderen Verkehrsdomänen segmentieren. Sie können die Standardverkehrsdomäne nicht von der NetScaler-Appliance entfernen. Jede Feature-Entität, die Sie erstellen, ohne die ID der Verkehrsdomäne festzulegen, wird automatisch mit der Standard-Verkehrsdomäne verknüpft.

Hinweis: Einige Funktionen und Konfigurationen werden nur in der Standard-Verkehrsdomäne unterstützt. Sie funktionieren nicht in nicht standardmäßigen Datenverkehrsdomänen. Eine Liste der Funktionen, die in allen Verkehrsdomänen unterstützt werden, finden Sie unter Unterstützte NetScaler Features in Traffic-Domains.

Funktionsweise von Traffic-Domänen

Betrachten Sie als Beispiel für Verkehrsdomänen ein Beispiel, in dem zwei Verkehrsdomänen mit den IDs 1 und 2 auf der NetScaler-Appliance NS1 konfiguriert sind.

In der Verkehrsdomäne 1 ist der virtuelle Lastausgleichsserver LBVS-TD1 für den Lastausgleich des Datenverkehrs zwischen den Servern S1 und S2 konfiguriert. Auf der NetScaler-Appliance werden die Server S1 und S2 durch die Dienste SVC1-TD1 bzw. SVC2-TD1 dargestellt. Die Server S1 und S2 sind über den L2-Switch SW2-TD1 mit NS1 verbunden. Der Client CL-TD1 befindet sich in einem privaten

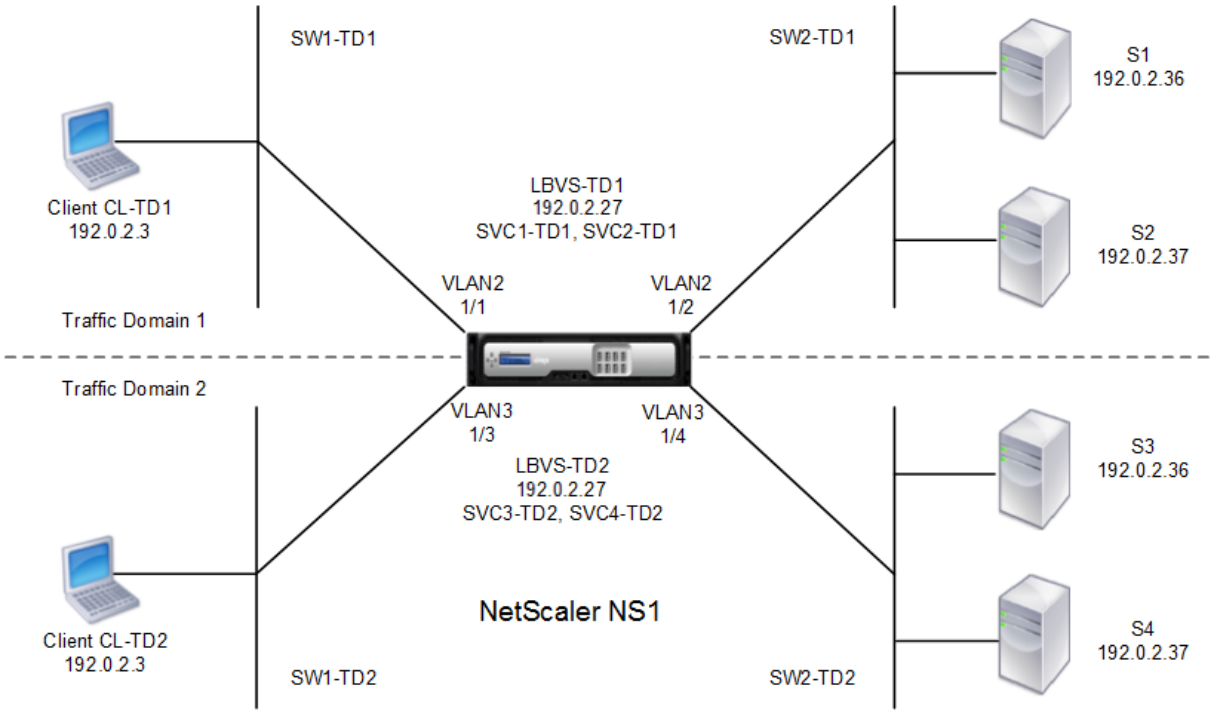
Netzwerk, das über den L2-Switch SW1-TD1 mit NS1 verbunden ist. SW1-TD1 und SW2-TD1 sind mit VLAN 2 von NS1 verbunden. VLAN 2 ist an die Verkehrsdomäne 1 gebunden, was bedeutet, dass der Client CL-TD1 und die Server S1 und S2 Teil der Verkehrsdomäne 1 sind.

Ähnlich ist in der Verkehrsdomäne 2 der virtuelle Lastausgleichsserver LBVS-TD2 so konfiguriert, dass der Datenverkehr über S3 und S4 ausbalanciert wird. Auf der NetScaler-Appliance werden die Server S3 und S4 durch die Dienste SVC3-TD2 bzw. SVC4-TD2 dargestellt. Die Server S3 und S4 sind über den L2-Switch SW2-TD2 mit NS1 verbunden. Der Client CL-TD2 befindet sich in einem privaten Netzwerk, das über den L2-Switch SW1-TD2 mit NS1 verbunden ist. SW1-TD2 und SW2-TD2 sind mit VLAN 3 von NS1 verbunden. VLAN 3 ist an die Verkehrsdomäne 2 gebunden, was bedeutet, dass der Client CL-TD2 und die Server S3 und S4 Teil der Verkehrsdomäne 2 sind.

Auf der NetScaler-Appliance teilen die Entitäten LBVS-TD1 und LBVS-TD2 dieselben Einstellungen, einschließlich der IP-Adresse. Gleiches gilt für SVC1-TD1 und SVC3-TD2 sowie für SVC2-TD1 und SVC4-TD2. Dies ist möglich, da sich diese Entitäten in verschiedenen Verkehrsdomänen befinden.

In ähnlicher Weise teilen sich die Server S1 und S3, S2 und S4 dieselbe IP-Adresse, und die Clients CL-TD1 und CL-TD2 haben jeweils dieselbe IP-Adresse.

Abbildung 1. Funktionsweise von Verkehrsdomänen



In der folgenden Tabelle sind die im Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
Einstellungen in der Verkehrsdomäne 1		
VLANs, die an Verkehrsdomäne 1 gebunden sind	VLAN 2	VLAN-ID: 2 Schnittstellen gebunden: 1/1, 1/2
Client ist mit TD1 verbunden	CL-TD1 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.3
Virtueller Lastausgleichsserver in TD1	LBVS-TD1	IP-Adresse: 192.0.2.27
Dienst gebunden an virtuellen Server LBVS-TD1	SVC1-TD1	IP-Adresse: 192.0.2.36
Dienst gebunden an virtuellen Server LBVS-TD1	SVC2-TD1	IP-Adresse: 192.0.2.37
SNIP	SNIP-TD1 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.27
Einstellungen in der Verkehrsdomäne 2		
VLAN an Verkehrsdomäne 2 gebunden	VLAN 3	VLAN-ID: 3 Schnittstellen gebunden: 1/3, 1/4
Client ist mit TD2 verbunden	CL-TD2 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.3
Virtueller Lastausgleichsserver in TD2	LBVS-TD2	IP-Adresse: 192.0.2.27
Dienst gebunden an virtuellen Server LBVS-TD2	SVC3-TD2	IP-Adresse: 192.0.2.36
Dienst gebunden an virtuellen Server LBVS-TD2	SVC4-TD2	IP-Adresse: 192.0.2.37
SNIP zu TD2	SNIP-TD2 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.29

Es folgt der Verkehrsfluss in der Verkehrsdomäne 1:

1. Client CL-TD1 sendet eine ARP-Anforderung für die IP-Adresse von 192.0.2.27 über den L2-Switch SW1-TD1.
2. Die ARP-Anforderung erreicht NS1 auf der Schnittstelle 1/1, die an VLAN 2 gebunden ist. Da VLAN

2 an die Verkehrsdomäne 1 gebunden ist, aktualisiert NS1 die ARP-Tabelle der Verkehrsdomäne 1 für die IP-Adresse des Clients CL-TD1.

3. Da die ARP-Anforderung in der Verkehrsdomäne 1 empfangen wird, sucht NS1 nach einer in der Verkehrsdomäne 1 konfigurierten Entität mit einer IP-Adresse von 192.0.2.27. NS1 stellt fest, dass ein virtueller Lastausgleichsserver LBVS-TD1 in der Verkehrsdomäne 1 konfiguriert ist und die IP-Adresse 192.0.2.27 hat.
4. NS1 sendet eine ARP-Antwort mit der MAC-Adresse der Schnittstelle 1/1.
5. Die ARP-Antwort erreicht CL-TD1. CL-TD1 aktualisiert seine ARP-Tabelle für die IP-Adresse von LBVS-TD1 mit der MAC-Adresse der Schnittstelle 1/1 von NS1.
6. Client CL-TD1 sendet eine Anfrage an 192.0.2.27. Die Anfrage wird von LBVS-TD1 auf Port 1/1 von NS1 empfangen.
7. Der Lastausgleichsalgorithmus von LBVS-TD1 wählt Server S2 aus, und NS1 öffnet eine Verbindung zwischen einem SNIP in der Verkehrsdomäne 1 (192.0.2.27) und S2.
8. S2 antwortet auf SNIP 192.0.2.27 auf NS1.
9. NS1 sendet die Antwort von S2 an den Client CL-TD1.

Es folgt der Verkehrsfluss in der Verkehrsdomäne 2:

1. Client CL-TD2 sendet eine ARP-Anforderung für die IP-Adresse von 192.0.2.27 über den L2-Switch SW1-TD2.
2. Die ARP-Anforderung erreicht NS1 auf der Schnittstelle 1/3, die an VLAN 3 gebunden ist. Da VLAN 3 an die Verkehrsdomäne 2 gebunden ist, aktualisiert NS1 den ARP-Table-Eintrag der Verkehrsdomäne 2 für die IP-Adresse des Clients CL-TD2, obwohl ein ARP-Eintrag für dieselbe IP-Adresse (CL-TD1) bereits in der ARP-Tabelle der Verkehrsdomäne 1 vorhanden ist.
3. Da die ARP-Anforderung in der Verkehrsdomäne 2 empfangen wird, durchsucht NS1 die Verkehrsdomäne 2 nach einer Entität mit einer IP-Adresse von 192.0.2.27. NS1 stellt fest, dass der virtuelle Lastausgleichsserver LBVS-TD2 in der Verkehrsdomäne 2 konfiguriert ist und die IP-Adresse 192.0.2.27 hat. NS1 ignoriert LBVS-TD1 in der Verkehrsdomäne 1, obwohl es dieselbe IP-Adresse wie LBVS-TD2 hat.
4. NS1 sendet eine ARP-Antwort mit der MAC-Adresse der Schnittstelle 1/3.
5. Die ARP-Antwort erreicht CL-TD2. CL-TD2 aktualisiert seinen ARP-Tabelleneintrag für die IP-Adresse von LBVS-TD2 mit der MAC-Adresse der Schnittstelle 1/3 von NS1.
6. Client CL-TD2 sendet eine Anfrage an 192.0.2.27. Die Anforderung wird von LBVS-TD2 auf der Schnittstelle 1/3 von NS1 empfangen.
7. Der Lastausgleichsalgorithmus von LBVS-TD2 wählt Server S3 aus, und NS1 öffnet eine Verbindung zwischen einem SNIP in der Verkehrsdomäne 2 (192.0.2.29) und S3.
8. S2 antwortet auf SNIP 192.0.2.29 auf NS1.
9. NS1 sendet die Antwort von S2 an den Client CL-TD2.

Unterstützte NetScaler-Funktionen in Verkehrsdomänen

Die NetScaler-Funktionen in der folgenden Liste werden in allen Verkehrsdomänen unterstützt.

> **Wichtig**
>
> Jede unten nicht aufgeführte NetScaler-Funktion wird nur in der Standardverkehrsdomäne unterstützt.

- ARP-Tabelle
- ND6-Tabelle
- Bridge-Tisch
- Alle Arten von IPv4- und IPv6-Adressen
- IPv4- und IPv6-Routen
- ACL und ACL6
- PBR & PBR6
- INAT
- RNAT
- RNAT6
- MSR
- MSR6
- Netzprofile
- SNMP-MIBs
- Fragmentierung
- Monitore (skriptfähige Monitore werden nicht unterstützt)
- Content Switching
- Cacheumleitung
- Persistency (Persistenzgruppen werden nicht unterstützt)
- Dienst (Domänenbasierte Dienste werden nicht unterstützt)
- Servicegruppe (Domänenbasierte Dienstgruppen werden nicht unterstützt)
- Richtlinien (*)
- PING
- TRACEROUTE
- PMTU
- Hochverfügbarkeit (Verbindungsspiegelung wird nicht unterstützt)
- Cluster (Unterstützt auf L2-Clustern. Auf L3-Clustern nicht unterstützt)
- Cookie-Persistenz
- MSS
- Protokollierung (Syslog wird nicht unterstützt)
- Überlastungsschutz
- Load Balancing (Die folgenden Typen werden nicht unterstützt:)
  - TFTP

  - RTSP
  - Diameter
  - SIP
  - SMPP
- NAT46
- NAT64
- DNS64
- Sitzungsregeln weiterleiten
- SNMP

> **Hinweis**
>
> - * Richtlinien haben keine globalen Verbindungspunkte für Traffic-Domains. Richtlinien können jedoch an einen bestimmten virtuellen Lastausgleichsserver einer Verkehrsdomäne gebunden werden.
> - Global Server Loading Balancing (GSLB) und ADNS-Funktionen in NetScaler sind sich der Verkehrsdomänen nicht bewusst. Wenn die GSLB-Konfiguration für alle Verkehrsdomänen gemeinsam genutzt werden muss, funktionieren die GSLB-Methoden Statische Nähe und Round Trip Time (RTT) nicht. Als Problemumgehung in diesem Szenario können Sie andere GSLB-Methoden als RTT und Static Proximity verwenden. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX202277.

Konfigurieren von Verkehrsdomänen

Das Konfigurieren einer Verkehrsdomäne auf der NetScaler-Appliance umfasst die folgenden Aufgaben:

- **Fügen Sie VLANs hinzu.** Erstellen Sie VLANs und binden Sie bestimmte Schnittstellen an sie.
- **Erstellen Sie eine Traffic-Domain-Entität und binden Sie VLANs daran.** Dies beinhaltet die folgenden zwei Aufgaben:
  - Erstellen Sie eine Traffic-Domain-Entität, die eindeutig durch eine ID identifiziert wird, die ein ganzzahliger Wert ist.
  - Binden Sie die angegebenen VLANs an die Verkehrsdomänen-Entität. Alle Schnittstellen, die an die angegebenen VLANs gebunden sind, sind mit der Verkehrsdomäne verknüpft. Mehr als ein VLAN kann an eine Verkehrsdomäne gebunden sein, aber ein VLAN kann nicht Teil mehrerer Verkehrsdomänen sein.
- **Erstellen Sie Feature-Entitäten in der Verkehrsdomäne**. Erstellen Sie die erforderlichen Feature-Entitäten in der Verkehrsdomäne. Die CLI-Befehle und Konfigurationsdialogfelder aller unterstützten Funktionen in einer nicht standardmäßigen Verkehrsdomäne enthalten einen Parameter, der als *Traffic Domain Identifier* (td) bezeichnet wird. Wenn Sie eine Feature-Entity konfigurieren und möchten, dass die Entität einer bestimmten Verkehrsdomäne zugeordnet

wird, müssen Sie den td angeben. Jede Feature-Entity, die Sie ohne Festlegen des td erstellen, wird automatisch der Standardverkehrsdomäne zugeordnet.

Um Ihnen eine Vorstellung davon zu geben, wie Feature-Entitäten einer Verkehrsdomäne zugeordnet sind, behandelt dieses Thema die Verfahren zum Konfigurieren aller Entitäten, die in der Abbildung mit dem Titel Wie Traffic-Domains funktionieren.

Die CLI verfügt über zwei Befehle für diese beiden Aufgaben, aber die GUI kombiniert sie in einem einzigen Dialogfeld.

CLI-Verfahren

So erstellen Sie ein VLAN und binden Sie über die CLI Schnittstellen an dieses:

Geben Sie in der Befehlszeile Folgendes ein:

- **add vlan** <id>
- **bind vlan** <id>-**ifnum** <slot/port>
- **show vlan** <id>

So erstellen Sie eine Traffic-Domain-Entität und binden VLANs über die CLI an sie:

Geben Sie in der Befehlszeile Folgendes ein:

- **add ns trafficdomain** <td>
- **bind ns trafficdomain** <td> -**vlan** <id>
- **zeige uns Trafficdomain** <td>

So erstellen Sie einen Dienst über die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **Dienst hinzufügen** <name><IP><serviceType><port>-**td** <id>
- **show service** <name>

So erstellen Sie einen virtuellen Lastausgleichsserver und binden Dienste über die Befehlszeile an diesen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add lb vserver** <name> <serviceType> <IPAddress> <port> -**td** <id>
- **binde lb vserver** <name><serviceName>
- **show lb vserver** <name>

GUI-Verfahren

So erstellen Sie ein VLAN über die GUI:

Navigieren Sie zu **System** > **Netzwerk** > **VLANs**, klicken Sie auf **Hinzufügen**und legen Sie die Parameter fest.

So erstellen Sie über die GUI eine Traffic-Domain-Entität:

Navigieren Sie zu **System** > **Netzwerk** > **Traffic Domains**, klicken Sie auf **Hinzufügen**, und **legen Sie im Dialogfeld Traffic Domain erstellen** die Parameter fest.

So erstellen Sie einen Dienst über die GUI:

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, klicken Sie auf **Hinzufügen**, und legen Sie die Parameter fest.

So erstellen Sie über die GUI einen virtuellen Lastausgleichsserver:

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, klicken Sie auf **Hinzufügen**, und legen Sie die Parameter fest.

Bindungen von Inter Traffic-Dom

May 11, 2023

Sie können Dienste in einer Verkehrsdomäne an einen virtuellen Server in einer anderen Verkehrsdomäne binden. Alle Dienste, die an einen virtuellen Server in einer anderen Verkehrsdomäne gebunden werden sollen, müssen sich in derselben Verkehrsdomäne befinden.

Sie konfigurieren diese Unterstützung, indem Sie den vorhandenen Befehl bind lb vserver oder das zugehörige GUI-Verfahren verwenden.

Diese Funktion kann die Interaktion zwischen verschiedenen Verkehrsdomänen erleichtern. In einem Unternehmen können Server in verschiedenen Verkehrsdomänen gruppiert werden. Virtuelle Server werden in einer Verkehrsdomäne erstellt, die dem Internet zugewandt ist. Ein virtueller Server aus dieser Verkehrsdomäne kann so konfiguriert werden, dass er Server in einer anderen Verkehrsdomäne ausgleicht. Dieser virtuelle Server empfängt Verbindungsanfragen aus dem Internet, um an die gebundenen Server weitergeleitet zu werden.

Wenn ein NetScaler in einer Cloud-Infrastruktur verwendet wird, kann jedem Mandanten eine separate Verkehrsdomäne zugewiesen werden, und alle Ressourcen (einschließlich Server) für einen Mandanten können in der Verkehrsdomäne des Mandanten zusammengefasst werden. Für jeden Mandanten wird ein virtueller Server für Load-Balancing-Server in seiner Verkehrsdomäne erstellt. Alle diese virtuellen Server sind in einer einzigen Verkehrsdomäne zusammengefasst, die dem Internet zugewandt ist.

Stellen Sie sich ein Beispiel vor, bei dem der Cloud-Dienstanbieter Example-Cloud-A drei Verkehrsdomänen mit den IDs 10, 20 und 30 hat, die auf der NetScaler-Appliance NS1 konfiguriert sind.

Example-Org-A und Example-Org-B sind Mandanten von Example-Cloud-A. Mandant A wird die Verkehrsdomäne 20 zugewiesen, und Mandant B wird die Domäne 30 zugewiesen. Die Server S1 und S2 befinden sich in der Verkehrsdomäne 20 und die Server S3 und S4 befinden sich in der Verkehrsdomäne 30.

Die Verkehrsdomäne 10 ist dem Internet zugewandt. Die virtuellen Server LBVS-1 und LBVS-2 werden in der Verkehrsdomäne 10 erstellt. LBVS-1 in der Verkehrsdomäne 10 ist so konfiguriert, dass er die Server S1 und S2, die sich in der Verkehrsdomäne 20 befinden, ausgleicht. LBVS-2 in der Verkehrsdomäne 10 ist für den Lastenausgleich der Server S3 und S4 konfiguriert, die sich in der Verkehrsdomäne 30 befinden.

Daher akzeptieren diese virtuellen Server Internetverbindungsanforderungen für Server, die sich in einer anderen Datenverkehrsdomäne als die der virtuellen Server befinden.

virtuelle MAC-basierte Verkehrsdomänen

May 11, 2023

Sie können eine Verkehrsdomäne mit einer virtuellen MAC-Adresse statt mit VLANs verknüpfen. Der NetScaler sendet dann die virtuelle MAC-Adresse der Verkehrsdomäne in allen Antworten auf ARP-Abfragen für Netzwerkentitäten in dieser Domäne. Dadurch kann der ADC nachfolgenden eingehenden Verkehr auf der Grundlage der Ziel-MAC-Adresse für verschiedene Verkehrsdomänen trennen, da die Ziel-MAC-Adresse die virtuelle MAC-Adresse einer Verkehrsdomäne ist. Nachdem Sie Entitäten in einer Verkehrsdomäne erstellt haben, können Sie diese einfach verwalten und überwachen, indem Sie Operationen auf der Ebene der Verkehrsdomäne ausführen.

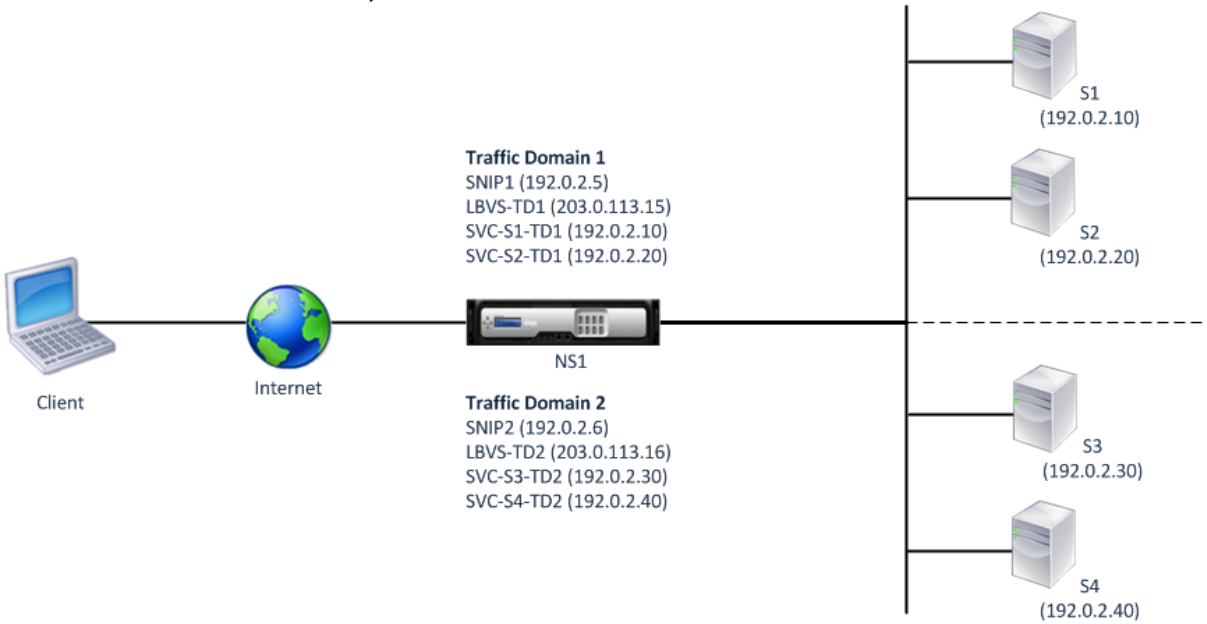
Stellen Sie sich ein Beispiel vor, in dem zwei Verkehrsdomänen mit den IDs 1 und 2 auf der NetScaler Appliance NS1 konfiguriert sind. Der NetScaler erstellt eine virtuelle MAC-Adresse, virtuelles MAC1, und ordnet sie der Verkehrsdomäne 1 zu. In ähnlicher Weise erstellte der NetScaler eine weitere virtuelle MAC-Adresse, virtuelle MAC2, und verknüpft sie mit der Verkehrsdomäne 2.

In der Verkehrsdomäne 1 ist der virtuelle Lastausgleichsserver LBVS-TD1 für den Lastausgleich des Datenverkehrs zwischen den Servern S1 und S2 konfiguriert. Auf der NetScaler-Appliance werden die Server S1 und S2 durch die Dienste SVC1-TD1 bzw. SVC2-TD1 dargestellt. Eine Subnetz-IP-Adresse (SNIP) SNIP1 ist konfiguriert, damit der NetScaler mit S1 und S2 kommunizieren kann. Da der virtuelle MAC1 mit der Verkehrsdomäne 1 verknüpft ist, sendet die Appliance in allen ARP-Ankündigungen und ARP-Antworten für LBVS-TD1 und SNIP1 den virtuellen MAC1 als MAC-Adresse.

Ähnlich ist in der Verkehrsdomäne 2 der virtuelle Lastausgleichsserver LBVS-TD2 so konfiguriert, dass der Datenverkehr über S3 und S4 ausbalanciert wird. Auf der NetScaler-Appliance werden die Server S3 und S4 durch die Dienste SVC3-TD2 bzw. SVC4-TD2 dargestellt. Eine SNIP-Adresse, SNIP2, ist konfiguriert, damit der NetScaler mit S3 und S4 kommunizieren kann. Da virtueller MAC2

mit Verkehrsdomäne 2 verknüpft ist, sendet die Appliance virtuellen MAC2 als MAC-Adresse in allen ARP-Ankündigungen und ARP-Antworten für LBVS-TD2 und SNIP2.

Der NetScaler trennt den nachfolgenden eingehenden Datenverkehr für Verkehrsdomänen 1 oder 2 auf Basis der Ziel-MAC-Adresse, wenn die Ziel-MAC-Adresse virtueller MAC1 oder virtueller MAC2 ist.



In der folgenden Tabelle sind die Einstellungen aufgeführt, die im Beispiel verwendet werden: Beispieleinstellungen für virtuelle MAC-basierte Datenverkehrsdomäne.

Bevor Sie beginnen

Die folgenden Punkte sollten Sie berücksichtigen, bevor Sie eine virtuelle MAC-basierte Verkehrsdomäne konfigurieren:

1. virtuelle MAC-basierte Verkehrsdomänen sind der einfachste Weg, eine Trennung des Netzwerkverkehrs zu erreichen.
2. Da virtuelle MAC-basierte Verkehrsdomänen den Netzwerkverkehr auf der Grundlage virtueller MAC-Adressen und nicht anhand von VLANs trennen, können Sie auf einem NetScaler keine doppelten IP-Adressen auf verschiedenen virtuellen MAC-basierten Verkehrsdomänen erstellen.
3. virtuelle MAC-basierte Verkehrsdomänen funktionieren nicht, wenn der NetScaler nur im L2-Modus bereitgestellt wird.
4. Sowohl VLAN- als auch virtuelle MAC-basierte Verkehrsdomänen können auf einem NetScaler koexistieren. Virtuelle MAC-basierte Verkehrsdomänen laufen tatsächlich auf allen VLANs, die nicht an eine VLAN-basierte Verkehrsdomäne gebunden sind.

Konfigurationsschritte

Die Konfiguration einer virtuellen MAC-basierten Verkehrsdomäne auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- Erstellen Sie eine Traffic-Domain-Entität und aktivieren Sie die virtuelle MAC-Option. Erstellen Sie eine Traffic-Domain-Entität, die eindeutig durch eine ID identifiziert wird, bei der es sich um einen Integer-Wert handelt, und aktivieren Sie dann die virtuelle MAC-Option. Nach dem Erstellen der Datenverkehrsdomänen-Entität erstellt der NetScaler eine virtuelle MAC-Adresse und ordnet sie dann der Verkehrsdomänen-Entität zu.
- Erstellen Sie Feature-Entitäten in der Verkehrsdomäne Erstellen Sie die erforderlichen Feature-Entitäten in der Verkehrsdomäne, indem Sie bei der Konfiguration dieser Feature-Entitäten den Traffic Domain Identifier (td) angeben. NetScaler-eigene Netzwerkentitäten, die in einer virtuellen MAC-basierten Verkehrsdomäne erstellt wurden, sind der virtuellen MAC-Adresse zugeordnet, die der Verkehrsdomäne zugeordnet ist. Der NetScaler sendet dann die virtuelle MAC-Adresse der Verkehrsdomäne in Form von ARP-Ankündigungen und ARP-Antworten für diese Netzwerkentitäten.

CLI-Verfahren

So erstellen Sie mit der CLI eine virtuelle MAC-basierte Verkehrsdomäne:

Geben Sie in der Befehlszeile Folgendes ein:

- ns hinzufügen TrafficDomain <td> [-vmac (ENABLED | DISABLED)]
- show ns trafficdomain <td>

So konfigurieren Sie eine SNIP-Adresse mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- add ns ip <IPAddress> <netmask> -type SNIP –td <id>
- show ns ip <IPAddress> -td <id>

So erstellen Sie einen Dienst über die CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- add service <name> <IP> <serviceType> <port> -td <id>
- show service <name> -td <id>

So erstellen Sie einen virtuellen Lastausgleichsserver und binden Dienste über die Befehlszeile an diesen:

Geben Sie in der Befehlszeile Folgendes ein:

- add lb vserver <name> <serviceType> <IPAddress> <port> -td <id>
- bind lb vserver <name> <serviceName>

- show lb vserver <name> -td <id>

Beispiel:

```
> add ns trafficDomain 1 -vmac ENABLED
 Done
> add ns trafficDomain 2 -vmac ENABLED
 Done

> add ns ip 192.0.2.5 255.255.255.0 -type -SNIP -td 1
 Done
> add service  SVC-S1-TD1  192.0.2.10 HTTP 80 -td 1
 Done
> add service  SVC-S2-TD1  192.0.2.20 HTTP 80 -td 1
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.15 80 -td 1
 Done
> bind lb vserver  LBVS-TD1 SVC-S1-TD1
 Done
> bind lb vserver  LBVS-TD1 SVC-S2-TD1
 Done

> add ns ip 192.0.2.6 255.255.255.0 -type -SNIP -td 2
 Done
> add service  SVC-S3-TD2  192.0.2.30 HTTP 80 -td 2
 Done
> add service  SVC-S4-TD2  192.0.2.40 HTTP 80 -td 2
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.16 80 -td 1
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
<!--NeedCopy-->
```

GUI-Verfahren

Gehen Sie wie folgt vor, um eine virtuelle MAC-basierte Verkehrsdomäne mithilfe der GUI zu erstellen:

1. Navigieren Sie zu System > Netzwerk > Schnittstellen.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Stellen Sie auf der Seite Traffic-Domain erstellen die folgenden Parameter ein:
    - Traffic-Domain-ID*

- Mac aktivieren

4. Klicken Sie auf Erstellen.

So konfigurieren Sie eine SNIP-Adresse mithilfe der GUI:

1. Navigieren Sie zu System > Netzwerk > IPs > IPv4
2. Navigieren Sie zu Netzwerk > IPs > IPv4
3. Klicken Sie im Detailbereich auf Hinzufügen
4. Stellen Sie auf der Seite Create IP die folgenden Parameter ein. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
   - IP-Adresse
   - Netzmaske
   - IP-Typ
   - Domain-ID für Traffic
5. Klicken Sie auf Erstellen.

So erstellen Sie einen Dienst über die GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Stellen Sie auf der Seite mit den Grundeinstellungen die folgenden Parameter ein. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
   - Dienstname
   - Server
   - Protokoll
   - Port
   - Domain-ID für Traffic
4. Klicken Sie auf Weiter und dann auf Fertig.
5. Wiederholen Sie die Schritte 2-4, um einen weiteren Dienst zu erstellen.
6. Klicken Sie auf Schließen.

Um einen virtuellen Lastausgleichsserver zu erstellen und Dienste mithilfe der GUI an ihn zu binden, gehen Sie wie folgt vor:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Bereich Load Balancing Virtual Servers auf Hinzufügen.
3. Stellen Sie im Dialogfeld Virtuelle Server erstellen (Load Balancing) die folgenden Parameter ein. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Feld.
   - Name
   - IP-Adresse
   - Protokoll
   - Port

- Domain-ID für Traffic

4. Klicken Sie auf Weiter und klicken Sie im Servicebereich auf >.
5. Klicken Sie auf der Seite Service auf Einfügen und aktivieren Sie dann das Kontrollkästchen für die Dienste, die Sie an den virtuellen Server binden möchten.
6. Klicken Sie auf Weiter und dann auf Fertig.
7. Wiederholen Sie die Schritte 2-5, um einen weiteren virtuellen Server zu erstellen

VXLAN

May 11, 2023

NetScaler-Appliances unterstützen Virtual eXtensible Local Area Networks (VXLANs). Ein VXLAN überlagert Layer-2-Netzwerke mit einer Layer-3-Infrastruktur, indem es Layer-2-Frames in UDP-Paketen kapselt. Jedes Overlay-Netzwerk wird als VXLAN-Segment bezeichnet und durch eine eindeutige 24-Bit-ID, den VXLAN Network Identifier (VNI), identifiziert. Nur Netzwerkgeräte innerhalb desselben VXLAN können miteinander kommunizieren.

VxLANs bieten dieselben Ethernet-Layer-2-Netzwerkdienste wie VLANs, sind jedoch erweiterbar und flexibler. Die beiden Hauptvorteile der Verwendung von VxLANs sind die folgenden:

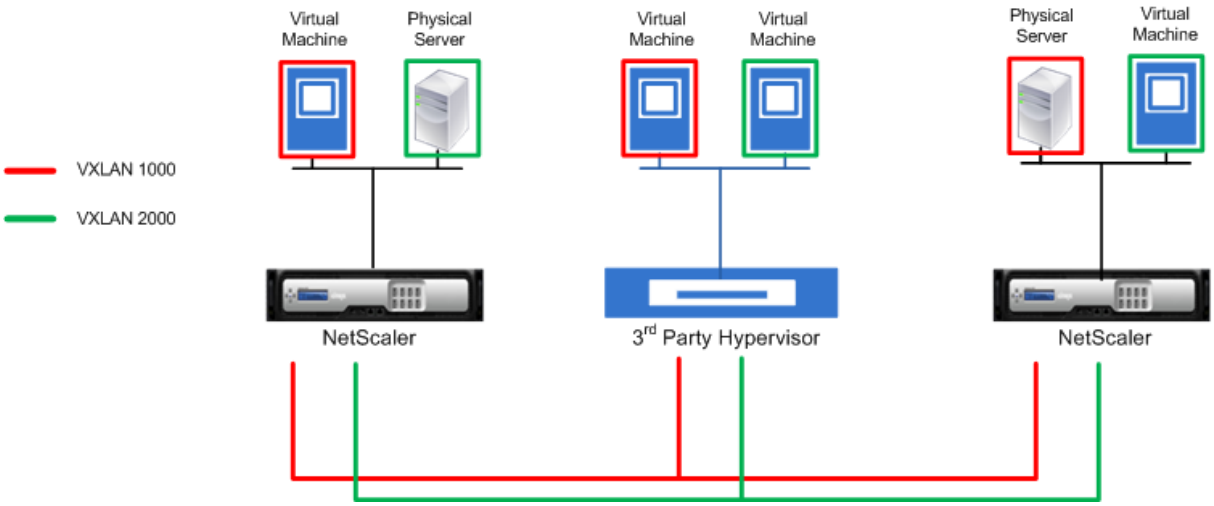
- **Höhere Skalierbarkeit.** Servervirtualisierung und Cloud-Computing-Architekturen haben die Nachfrage nach isolierten Layer-2-Netzwerken in einem Rechenzentrum dramatisch erhöht. Die VLAN-Spezifikation verwendet eine 12-Bit-VLAN-ID, um ein Layer-2-Netzwerk zu identifizieren, sodass Sie nicht über 4094 VLANs hinaus skalieren können. Diese Zahl kann unzureichend sein, wenn Tausende isolierter Layer-2-Netzwerke erforderlich sind. Das 24-Bit-VNI bietet Platz für bis zu 16 Millionen VXLAN-Segmente in derselben administrativen Domäne.
- **Höhere Flexibilität.** Da VXLAN Layer-2-Datenrahmen über Layer-3-Pakete überträgt, erweitern VXLANs L2-Netzwerke über verschiedene Teile eines Rechenzentrums und über geografisch getrennte Rechenzentren. Anwendungen, die in verschiedenen Teilen eines Rechenzentrums und in verschiedenen Rechenzentren gehostet werden, aber Teil desselben VXLAN sind, werden als ein zusammenhängendes Netzwerk angezeigt.

So funktionieren VxLANs

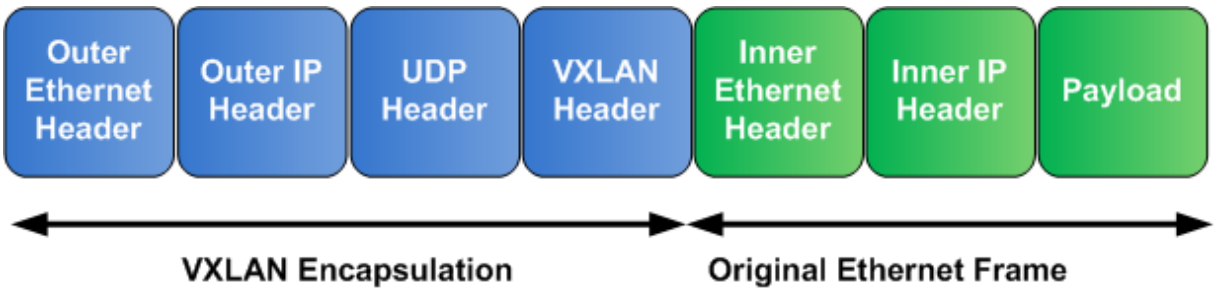
VXLAN-Segmente werden zwischen VXLAN-Tunnel-Endpunkten (VTEPs) erstellt. VTEPs unterstützen das VXLAN-Protokoll und führen die VXLAN-Kapselung und -Entkapselung durch. Sie können sich ein VXLAN-Segment als Tunnel zwischen zwei VTEPs vorstellen, wobei ein VTEP einen Layer2-Frame mit einem UDP-Header und einem IP-Header kapselt und ihn durch den Tunnel sendet. Der andere VTEP empfängt und entkapselt das Paket, um den Layer-2-Frame zu erhalten. Ein NetScaler ist ein Beispiel

für ein VTEP. Andere Beispiele sind Hypervisoren von Drittanbietern, VXLAN-fähige virtuelle Maschinen und VXLAN-fähige Switches.

Die folgende Abbildung zeigt virtuelle Maschinen und physische Server, die über VXLAN-Tunnel miteinander verbunden sind.



Die folgende Abbildung zeigt das Format eines VXLAN-Pakets.



VxLANs auf einem NetScaler verwenden einen Layer-2-Mechanismus zum Senden von Broadcast-, Multicast- und unbekannten Unicast-Frames. Ein VXLAN unterstützt die folgenden Modi für das Senden dieser L2-Frames.

- **Unicast-Modus**: In diesem Modus geben Sie die IP-Adressen von VTEPs an, während Sie ein VXLAN auf einem NetScaler konfigurieren. Der NetScaler sendet Broadcast-, Multicast- und unbekannte Unicast-Frames über Layer 3 an alle VTEPs dieses VXLAN.
- **Multicast-Modus**: In diesem Modus geben Sie eine Multicast-Gruppen-IP-Adresse an, während Sie ein VXLAN auf einem NetScaler konfigurieren. NetScaler unterstützen das IGMP-Protokoll (Internet Group Management Protocol) nicht. NetScaler verlassen sich auf den Upstream-Router, um einer Multicast-Gruppe beizutreten, die sich eine gemeinsame Multicast-Gruppen-IP-Adresse teilt. Der NetScaler sendet Broadcast-, Multicast- und unbekannte Unicast-Frames über Layer 3 an die Multicast-Gruppen-IP-Adresse dieses VXLAN.

Ähnlich wie bei einer Layer-2-Bridgetabelle verwalten NetScaler VXLAN-Zuordnungstabellen, die auf dem inneren und äußeren Header der empfangenen VXLAN-Pakete basieren. In dieser Tabelle wer-

den die MAC-Adressen des Remote-Hosts den VTEP-IP-Adressen für ein bestimmtes VXLAN zugeordnet. Der NetScaler verwendet die VXLAN-Zuordnungstabelle, um die Ziel-MAC-Adresse eines Layer-2-Frames zu ermitteln. Wenn ein Eintrag für diese MAC-Adresse in der VXLAN-Tabelle vorhanden ist, sendet der NetScaler den Layer-2-Frame über Layer 3 mithilfe des VXLAN-Protokolls an die zugeordnete VTEP-IP-Adresse, die im Zuordnungseintrag für ein VXLAN angegeben ist.

Da VXLANs ähnlich wie VLANs funktionieren, unterstützen die meisten NetScaler-Funktionen, die VLAN als Klassifizierungsparameter unterstützen, VXLAN. Zu diesen Funktionen gehört eine optionale VXLAN-Parametereinstellung, die den VXLAN-VNI spezifiziert.

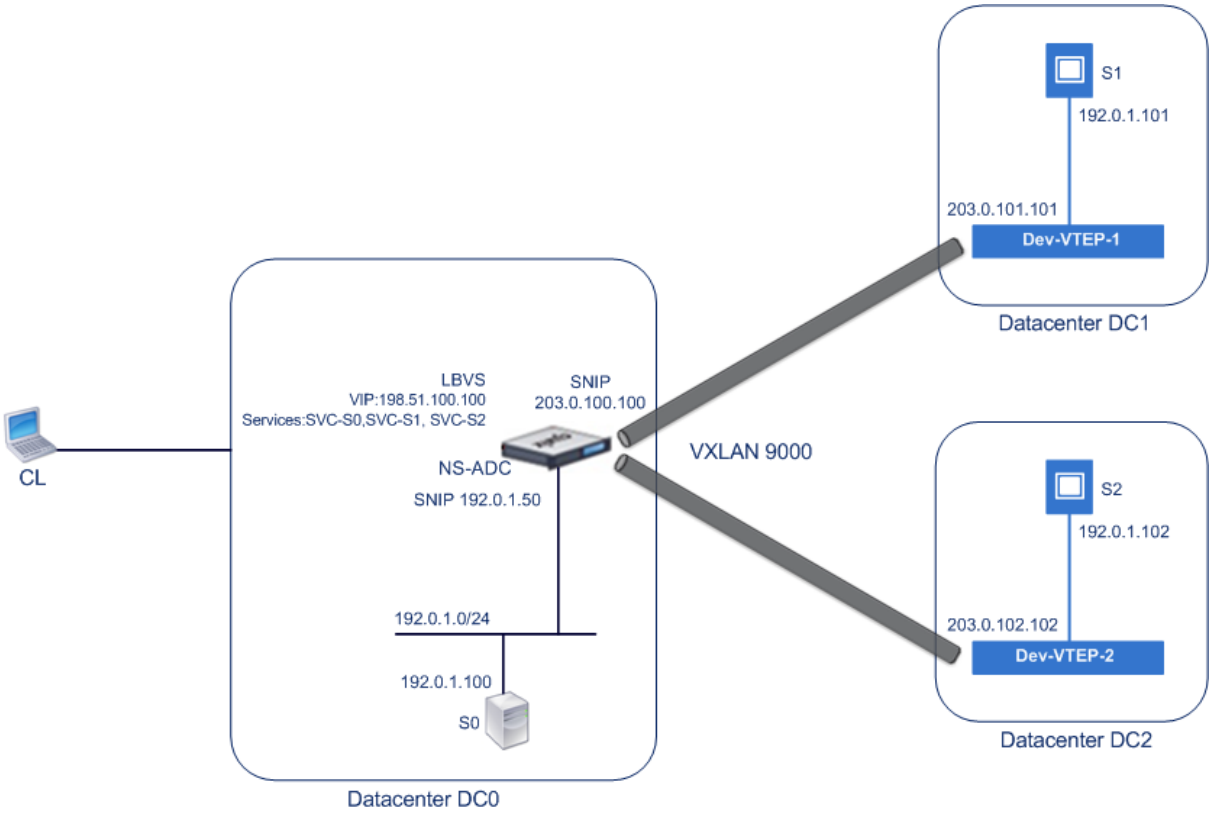
In einer Hochverfügbarkeitskonfiguration (HA) wird die VXLAN-Konfiguration an den sekundären Knoten weitergegeben oder synchronisiert.

VXLAN-Anwendungsfall: Lastenausgleich zwischen Rechenzentren

Um die VXLAN-Funktionalität eines NetScalers zu verstehen, schauen Sie sich ein Beispiel an, in dem Example Corp eine Site unter www.example.com hostet. Um die Verfügbarkeit der Anwendung sicherzustellen, wird die Site auf den drei Servern S0, S1 und S2 gehostet. Ein virtueller Lastausgleichsserver, LBVS, auf NetScaler NS-ADC wird für den Lastenausgleich dieser Server verwendet. S0, S1 und S2 befinden sich jeweils in den Rechenzentren DC0, DC1 und DC2. In DC0 ist der Server S0 mit NS-ADC verbunden.

S0 ist ein physischer Server und S1 und S2 sind virtuelle Maschinen (VMs). S1 läuft auf dem Virtualisierungs-Hostgerät Dev-VTEP-1 im Rechenzentrum DC1 und S2 läuft auf dem Hostgerät Dev-VTEP-2 in DC2. NS-ADC, Dev-VTEP-1 und Dev-VTEP-2 unterstützen das VXLAN-Protokoll.

S0, S1 und S2 sind Teil desselben privaten Subnetzes, 192.0.1.0/24. S0, S1 und S2 sind Teil einer gemeinsamen Broadcast-Domäne. VXLAN 9000 ist auf NS-ADC, Dev-VTEP-1 und Dev-VTEP-2 konfiguriert. Die Server S1 und S2 sind Teil von VXLAN9000 auf Dev-VTEP-1 bzw. Dev-VTEP-2.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VXLAN-Einstellungen.

Die Dienste SVC-S0, SVC-S1 und SVC-S2 auf NS-ADC stellen S0, S1 und S2 dar. Sobald diese Dienste konfiguriert sind, sendet NS-ADC ARP-Anfragen für S0, S1 und S2, um die IP-zu-Mac-Zuordnung zu lösen. Diese ARP-Anfragen werden auch über VXLAN 9000 an Dev-VTEP-1 und Dev-VTEP-2 gesendet.

Im Folgenden sehen Sie den Verkehrsfluss für die Auflösung der ARP-Anfrage für S2:

1. NS-ADC sendet eine ARP-Anfrage für S2, um die IP-zu-Mac-Zuordnung zu lösen. Dieses Paket hat:
   - Quell-IP-Adresse = Subnetz-IP-Adresse Snip-for-Servers (192.0.1.50)
   - Quell-MAC-Adresse = MAC-Adresse der NS-ADC-Schnittstelle, von der das Paket gesendet wird = NS-MAC-1
2. NS-ADC bereitet das ARP-Paket für den Versand über das VXLAN 9000 vor, indem es das Paket mit den folgenden Headern kapselt:
   - VXLAN-Header mit einer ID (VNI) von 9000
   - Standard-UDP-Header, UDP-Prüfsumme auf 0×0000 und Zielport auf 4789 gesetzt.
3. NS-ADC sendet das resultierende gekapselte Paket an Dev-VTEP-1 und Dev-VTEP-2 auf VXLAN-9000. Das gekapselte Paket hat:
   - Quell-IP-Adresse = SNIP-VTEP-0 (203.0.100.100).
4. Dev-VTEP-2 empfängt das UDP-Paket und entkapselt den UDP-Header, woraus Dev-VTEP-2

erfährt, dass es sich bei dem Paket um ein VXLAN-bezogenes Paket handelt. Dev-VTEP-2 entkapselt dann den VXLAN-Header und lernt die VXLAN-ID des Pakets. Das resultierende Paket ist das ARP-Anforderungspaket für S2, das mit Schritt 1 identisch ist.

5. Vom inneren und äußeren Header des VXLAN-Pakets aus erstellt Dev-VTEP-2 in seiner VXLAN-Zuordnungstabelle einen Eintrag, der die Zuordnung der MAC-Adresse (NS-MAC-1) und SNIP-VTEP-0 (203.0.100.100) für VXLAN9000 zeigt.
6. Dev-VTEP-2 sendet das ARP-Paket an S2. Das Antwortpaket von S2 erreicht Dev-VTEP-2. Dev-VTEP-2 führt eine Suche in seiner VXLAN-Zuordnungstabelle durch und ermittelt eine Übereinstimmung mit der Ziel-MAC-Adresse NS-MAC-1. Der Dev-VTEP-2 weiß jetzt, dass NS-MAC-1 über SNIP-VTEP-0 (203.0.100.100) über VXLAN 9000 erreichbar ist.
7. S2 antwortet mit seiner MAC-Adresse (MAC-S2). Das ARP-Antwortpaket enthält:
   - Ziel-IP-Adresse = Subnetz-IP-Adresse Snip-for-Servers (192.0.1.50)
   - Ziel-MAC-Adresse = NS-MAC-1
8. Das Antwortpaket von S2 erreicht Dev-VTEP-2. Dev-VTEP-2 führt eine Suche in seiner VXLAN-Zuordnungstabelle durch und ermittelt eine Übereinstimmung mit der Ziel-MAC-Adresse NS-MAC-1. Der Dev-VTEP-2 weiß jetzt, dass NS-MAC-1 über SNIP-VTEP-0 (203.0.100.100) über VXLAN 9000 erreichbar ist. Dev-VTEP-2 kapselt die ARP-Antwort mit VXLAN- und UDP-Headern und sendet das resultierende Paket an SNIP-VTEP-0 (203.0.100.100) von NS-ADC.
9. NS-ADC entkapselt beim Empfang des Pakets das Paket, indem es die VXLAN- und UDP-Header entfernt. Das resultierende Paket ist die ARP-Antwort von S2. NS-ADC aktualisiert seine VXLAN-Zuordnungstabelle für die MAC-Adresse von S2 (MAC-S2) mit der IP-Adresse von Dev-VTEP-2 (203.0.102.102) für VXLAN 9000. NS-ADC aktualisiert auch seine ARP-Tabelle für die IP-Adresse von S2 (192.0.1.102) mit der MAC-Adresse von S2 (MAC-S2).

In diesem Beispiel ist der Verkehrsfluss für den virtuellen Load-Balancing-Server LBVS dargestellt:

1. Client CL sendet ein Anforderungspaket an LBVS von NS-ADC. Das Anforderungspaket enthält:
   - Quell-IP-Adresse = IP-Adresse des Client CL (198.51.100.90)
   - Ziel-IP-Adresse = IP-Adresse (VIP) von LBVS = 198.51.110.100
2. LBVS von NS-ADC empfängt das Anforderungspaket, und sein Load-Balancing-Algorithmus wählt Server S2 des Rechenzentrums DC2 aus.
3. NS-ADC verarbeitet das Anforderungspaket und ändert seine Ziel-IP-Adresse in die IP-Adresse von S2 und seine Quell-IP-Adresse in eine der auf NS-ADC konfigurierten Subnetz-IP-Adressen (SNIP). Das Anforderungspaket enthält:
   - Quell-IP-Adresse = Subnetz-IP-Adresse auf NS-ADC= Snip-for-Servers (192.0.1.50)
   - Ziel-IP-Adresse = IP-Adresse von S2 (192.0.1.102)
4. NS-ADC findet in seiner Bridge-Tabelle einen VXLAN-Mapping-Eintrag für S2. Dieser Eintrag gibt an, dass S2 über Dev-VTEP-2 über VXLAN 9000 erreichbar ist.
5. NS-ADC bereitet das Paket für den Versand über das VXLAN 9000 vor, indem es das Paket mit den folgenden Headern kapselt:
   - VXLAN-Header mit einer ID (VNI) von 9000

- Standard-UDP-Header, UDP-Prüfsumme auf 0×0000 und Zielport auf 4789 gesetzt.

6. NS-ADC sendet das resultierende gekapselte Paket an Dev-VTEP-2. Das Anforderungspaket enthält:
   - Quell-IP-Adresse = SNIP-Adresse = SNIP-VTEP-0 (203.0.100.100)
   - Ziel-IP-Adresse = IP-Adresse von Dev-vTEP-2 (203.0.102.102)
7. Dev-VTEP-2 empfängt das UDP-Paket und entkapselt den UDP-Header, woraus Dev-VTEP-2 erfährt, dass es sich bei dem Paket um ein VXLAN-bezogenes Paket handelt. Dev-VTEP-2 entkapselt dann den VXLAN-Header und lernt die VXLAN-ID des Pakets. Das resultierende Paket ist dasselbe Paket wie in Schritt 3.
8. Dev-VTEP-2 leitet das Paket dann an S2 weiter.
9. S2 verarbeitet das Anforderungspaket und sendet die Antwort an die SNIP-Adresse von NS-ADC. Das Antwortpaket enthält:
   - Quell-IP-Adresse = IP-Adresse von S2 (192.0.1.102)
   - Ziel-IP-Adresse = Subnetz-IP-Adresse auf NS-ADC= Snip-for-Servers (192.0.1.50)
10. Dev-VTEP-2 kapselt das Antwortpaket auf die gleiche Weise, wie NS-ADC das Anforderungspaket in den Schritten 4 und 5 gekapselt hat. Dev-VTEP-2 sendet dann das gekapselte UDP-Paket an die SNIP-Adresse SNIP-for-Servers (192.0.1.50) von NS-ADC.
11. NS-ADC entkapselt das Paket nach Empfang des gekapselten UDP-Pakets, indem es die UDP- und VXLAN-Header auf die gleiche Weise entfernt, wie Dev-VTEP-2 das Paket in Schritt 7 entkapselt hat. Das resultierende Paket ist dasselbe Antwortpaket wie in Schritt 9.
12. NS-ADC verwendet dann die Sitzungstabelle für den Lastausgleich des virtuellen Servers LBVS und leitet das Antwortpaket an den Client CL weiter. Das Antwortpaket enthält:
    - Quell-IP-Adresse = IP-Adresse des Client CL (198.51.100.90)
    - Ziel-IP-Adresse = IP-Adresse (VIP) von LBVS (198.51.110.100)

Punkte, die bei der Konfiguration von VXLANs zu beachten sind

Beachten Sie die folgenden Punkte, bevor Sie VxLANs auf einem NetScaler konfigurieren:

- Auf einem NetScaler können maximal 2048 VXLANs konfiguriert werden.
- VXLANs werden in einem Cluster nicht unterstützt.
- Link-lokale IPv6-Adressen können nicht für jedes VXLAN konfiguriert werden.
- NetScaler unterstützen das IGMP-Protokoll (Internet Group Management Protocol) zur Bildung einer Multicast-Gruppe nicht. NetScaler verlassen sich auf das IGMP-Protokoll seines Upstream-Routers, um einer Multicast-Gruppe beizutreten, die sich eine gemeinsame Multicast-Gruppen-IP-Adresse teilt. Sie können beim Erstellen von VXLAN-Bridge-Tabelleneinträgen eine Multicast-Gruppen-IP-Adresse angeben, aber die Multicast-Gruppe muss auf dem Upstream-Router konfiguriert werden. Der NetScaler sendet Broadcast-, Multicast- und unbekannte Unicast-Frames über Layer 3 an die Multicast-Gruppen-IP-Adresse dieses VXLAN. Der Upstream-Router leitet das

Paket dann an alle VTEPs weiter, die Teil der Multicast-Gruppe sind.

- Die VXLAN-Kapselung fügt jedem Paket einen Overhead von 50 Byte hinzu:

  Äußerer Ethernet-Header (14) + UDP-Header (8) + IP-Header (20) + VXLAN-Header (8) = 50 Byte

  Um Fragmentierung und Leistungseinbußen zu vermeiden, müssen Sie die MTU-Einstellungen aller Netzwerkgeräte in einem VXLAN-Pfad, einschließlich der VXLAN-VTEP-Geräte, anpassen, um die 50 Byte Overhead in den VXLAN-Paketen zu bewältigen.

  Wichtig: Jumbo-Frames werden auf den virtuellen NetScaler VPX-Appliances, NetScaler SDX-Appliances und NetScaler MPX 15000/17000-Appliances nicht unterstützt. Diese Appliances unterstützen eine MTU-Größe von nur 1500 Byte und können nicht an den 50-Byte-Overhead von VXLAN-Paketen angepasst werden. VXLAN-Verkehr kann fragmentiert sein oder Leistungseinbußen erleiden, wenn sich eine dieser Appliances im VXLAN-Pfad befindet oder als VXLAN-VTEP-Gerät fungiert.
- Auf NetScaler SDX-Appliances funktioniert die VLAN-Filterung nicht für VXLAN-Pakete.
- Sie können keinen MTU-Wert für ein VXLAN festlegen.
- Sie können keine Schnittstellen an ein VXLAN binden.

Konfigurationsschritte

Die Konfiguration eines VXLAN auf einer NetScaler-Appliance umfasst die folgenden Aufgaben.

- **Fügen Sie eine VXLAN-Entität**hinzu. Erstellen Sie eine VXLAN-Entität, die eindeutig durch eine positive Ganzzahl identifiziert wird, die auch als VXLAN Network Identifier (VNI) bezeichnet wird. In diesem Schritt können Sie auch den Ziel-UDP-Port von Remote-VTEP angeben, auf dem das VXLAN-Protokoll ausgeführt wird. Standardmäßig ist der Ziel-UDP-Portparameter für die VXLAN-Entität auf 4789 festgelegt. Diese UDP-Porteinstellung muss mit den Einstellungen auf allen Remote-VTEPs für dieses VXLAN übereinstimmen. Sie können VLANs auch an dieses VXLAN binden. Der Datenverkehr (einschließlich Broadcasts, Multicasts, unbekannte Unicasts) aller gebundenen VLANs ist über dieses VXLAN zulässig. Wenn keine VLANs an das VXLAN gebunden sind, lässt der NetScaler den Verkehr aller VLANs in diesem VXLAN zu, die nicht Teil anderer VXLANs sind.
- **Binden Sie die lokale VTEP-IP-Adresse und an die VXLAN-Entität**. Binden Sie eine der konfigurierten SNIP-Adressen an das VXLAN, um ausgehende VXLAN-Pakete zu beziehen.
- **Fügen Sie einen Bridgetable-Eintrag**hinzu. Fügen Sie einen Bridgetable-Eintrag hinzu, der die VXLAN-ID und die Remote-VTEP-IP-Adresse für das zu erstellende VXLAN angibt.
- **(Optional) Binden Sie verschiedene Feature-Entitäten an das konfigurierte VXLAN**. VXLANs funktionieren ähnlich wie VLANs. Die meisten NetScaler-Funktionen, die VLAN als Klassifizierungsparameter unterstützen, unterstützen auch VXLAN. Zu diesen Funktionen gehört eine optionale VXLAN-Parametereinstellung, die den VXLAN-VNI spezifiziert.

- **(Optional) Zeigen Sie die VXLAN-Zuordnungstabelle an.** Zeigen Sie die VXLAN-Zuordnungstabelle an, die Zuordnungseinträge für die Remote-Host-MAC-Adresse zur VTEP-IP-Adresse für ein bestimmtes VXLAN enthält. Mit anderen Worten, eine VXLAN-Zuordnung besagt, dass ein Host über den VTEP in einem bestimmten VXLAN erreichbar ist. Der NetScaler lernt VXLAN-Zuordnungen und aktualisiert seine Zuordnungstabelle anhand der empfangenen VXLAN-Pakete. Der NetScaler verwendet die VXLAN-Zuordnungstabelle, um nach der Ziel-MAC-Adresse eines Layer-2-Frames zu suchen. Wenn ein Eintrag für diese MAC-Adresse in der VXLAN-Tabelle vorhanden ist, sendet der NetScaler den Layer-2-Frame über Layer 3 mithilfe des VXLAN-Protokolls an die zugeordnete VTEP-IP-Adresse, die im Zuordnungseintrag für ein VXLAN angegeben ist.

CLI-Verfahren

So fügen Sie eine VXLAN-Entität mithilfe der CLI hinzu:

Geben Sie an der Eingabeaufforderung

- **vxlan hinzufügen** <id>
- **vxlan anzeigen**<id>

So binden Sie die lokale VTEP-IP-Adresse mithilfe der CLI an das VXLAN:

Geben Sie an der Eingabeaufforderung

- **bind vxlan** <id> -**SrcIP** <IPaddress>
- **show vxlan** <id>

Um eine Bridgetable mit der CLI hinzuzufügen:

Geben Sie an der Eingabeaufforderung

- **add bridgetable** -**mac** <macaddress> -**vxlan** <ID> -**vtep** <IPaddress>
- **show bridgetable**

Gehen Sie wie folgt vor, um die VXLAN-Weiterleitungstabelle mithilfe der Befehlszeile anzuzeigen:

Geben Sie in der Befehlszeile Folgendes ein:

- **show bridgetable**

GUI-Verfahren

Um eine VXLAN-Entität hinzuzufügen und eine lokale VTEP-IP-Adresse mithilfe der GUI zu binden:

Navigieren Sie zu **System** > **Netzwerk** > **VXLANs und fügen Sie eine neue VXLAN-Entität**hinzu oder ändern Sie eine vorhandene VXLAN-Entität.

Um ein Bridgetable mithilfe der GUI hinzuzufügen:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge-Tabelle**und legen Sie beim Hinzufügen oder Ändern eines VXLAN-Bridge-Tabelleneintrags die folgenden Parameter fest:

- MAC
- VTEP
- VXLAN-ID

Um die VXLAN-Weiterleitungstabelle mithilfe der GUI anzuzeigen:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge-Tabelle**.

```
Example
> add vxlan 9000
Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.101.101

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
   203.0.102.102

Done
```

Unterstützung von IPv6 Dynamic Routing-Protokollen auf VxLANs

Die NetScaler-Appliance unterstützt dynamische IPv6-Routingprotokolle für VXLANs. Sie können verschiedene dynamische IPv6-Routing-Protokolle (z. B. OSPFv3, RIPNG, BGP) auf VXLANs über die VTYSH-Befehlszeile konfigurieren. Dem VXLAN-Befehlssatz wurde eine Option IPv6 Dynamic Routing Protocol hinzugefügt, mit der dynamische IPv6-Routingprotokolle in einem VXLAN aktiviert oder deaktiviert werden können. Nach der Aktivierung dynamischer IPv6-Routingprotokolle in einem VXLAN müssen Prozesse im Zusammenhang mit den dynamischen IPv6-Routingprotokollen im VXLAN mithilfe der VTYSH-Befehlszeile gestartet werden.

So aktivieren Sie dynamische IPv6-Routingprotokolle auf einem VXLAN mit der CLI:

- **add vxlan** <ID> [-**ipv6DynamicRouting** (**ENABLED** | **DISABLED**)]
- **show vxlan**

```
In the following sample configuration, VXLAN-9000 is created and has
   IPv6 dynamic routing protocols enabled on it. Then, using the VTYSH
   command line, process for the IPv6 OSPF protocol is started on the
   VXLAN.
```



```
2
3  > add vxlan 9000 -ipv6DynamicRouting ENABLED
4
5  Done
6  > bind vxlan 9000 -srcIP 203.0.100.100
7
8  Done
9  > add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
       203.0.101.101
10
11 Done
12 > VTYSH
13 NS# configure terminal
14 NS(config)# ns IPv6-routing
15 NS(config)# interface VXLAN-9000
16 NS(config-if)# ipv6 router OSPF area 3
```

Erweitern von VLANs von mehreren Unternehmen auf eine Cloud mithilfe von VXLAN-VLAN-Karten

CloudBridge Connector-Tunnel werden verwendet, um das VLAN eines Unternehmens auf eine Cloud auszudehnen. VLANs, die von mehreren Unternehmen aus erweitert werden, können sich überschneidende VLAN-IDs haben. Sie können die VLANs jedes Unternehmens isolieren, indem Sie sie einem eindeutigen VXLAN in der Cloud zuordnen. Auf einer NetScaler-Appliance, dem CloudBridge-Connector-Endpunkt in der Cloud, können Sie eine VXLAN-VLAN-Map konfigurieren, die die VLANs eines Unternehmens mit einem eindeutigen VXLAN in der Cloud verbindet. VXLANs unterstützen VLAN-Tagging zur Erweiterung mehrerer VLANs eines Unternehmens vom CloudBridge Connector auf dasselbe VXLAN.

Führen Sie die folgenden Aufgaben aus, um VLANs mehrerer Unternehmen auf eine Cloud zu erweitern:

1. Erstellen Sie eine VXLAN-VLAN-Map.
2. Binden Sie die VXLAN-VLAN-Map an eine Netzwerkbridge- oder PBR-basierte CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance in der Cloud.
3. (Optional) Aktivieren Sie das VLAN-Tagging in einer VXLAN-Konfiguration.

CLI-Verfahren

Um eine VXLAN-VLAN-Map mit der CLI hinzuzufügen:

- **add vxlanVlanMap** <name>
- **show vxlanVlanMap** <name>

So binden Sie ein VXLAN und VLANS mit der CLI an eine VXLAN-VLAN-Karte:

- **bind vxlanVlanMap** <name> [-**vxlan** \<positive_integer> -**vlan** \<int[-int]> …]
- **show vxlanVlanMap** <name>

So binden Sie eine VXLAN-VLAN-Map mithilfe der CLI an einen auf einer Netzwerkbrücke basierenden CloudBridge Connector-Tunnel:

Geben Sie in der Befehlszeile einen der folgenden Befehlssätze ein.

Wenn Sie eine neue Netzwerkbrücke hinzufügen:

- **add netbridge** <name> [-**vxlanVlanMap** \<string>]
- **show netbridge** <name>

wenn Sie eine bestehende Netzwerkbrücke neu konfigurieren:

- **set netbridge** <name> [-**vxlanVlanMap** \<string>]
- **show netbridge** <name>

So binden Sie eine VXLAN-VLAN-Map mithilfe der CLI an einen PBR-basierten CloudBridge Connector-Tunnel:

Geben Sie in der Befehlszeile einen der folgenden Befehlssätze ein.

Wenn Sie eine neue PBR hinzufügen:

- **add pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**vxlanVlanMap** \<name>])
- **show pbr** <name>

wenn Sie eine bestehende PBR neu konfigurieren:

- **set pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**vxlanVlanMap** \<name>])
- **show pbr** <name>

Um VLAN-Tags in Pakete aufzunehmen, die sich auf ein VXLAN beziehen, verwenden Sie die CLI:

Geben Sie in der Befehlszeile einen der folgenden Befehlssätze ein.

wenn ein neues VXLAN hinzugefügt wird:

- **add vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

wenn Sie ein vorhandenes VXLAN neu konfigurieren:

- **set vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

GUI-Verfahren

Um eine VXLAN-VLAN-Map mithilfe der GUI hinzuzufügen:

Navigieren Sie zu **System** > **Netzwerk** > **VXLAN VLAN Map und fügen Sie eine VXLAN-VLAN-Map**hinzu.

So binden Sie eine VXLAN-VLAN-Map mithilfe der GUI an einen Netbridge-basierten CloudBridge Connector-Tunnel:

Navigieren Sie zu **System** > **CloudBridge Connector** > **Network Bridge**, wählen Sie eine VXLAN-VLAN-Map aus der **VXLAN-VLAN-Dropdown-Liste** aus, während Sie eine neue Netzwerkbrücke hinzufügen oder eine bestehende Netzwerkbrücke neu konfigurieren.

So binden Sie eine VXLAN-VLAN-Map mithilfe der GUI an einen PBR-basierten CloudBridge Connector-Tunnel:

Navigieren Sie zu **System** > **Netzwerk** > **PBRs**und wählen Sie auf der Registerkarte Policy Based Routing (PBRs) eine **VXLAN-VLAN-Map aus der VXLAN-VLAN-Dropdown-Liste** aus, während Sie eine **neue PBR hinzufügen oder eine vorhandene** PBR neu konfigurieren.

So fügen Sie mithilfe der GUI VLAN-Tags in Pakete ein, die sich auf ein VXLAN beziehen:

Navigieren Sie zu **System** > **Netzwerk** > **VXLANs**, aktivieren Sie die **innere VLAN-Tagging**, während Sie ein neues VXLAN hinzufügen oder ein vorhandenes VXLAN neu konfigurieren.

```
1  > add vxlanVlanMap VXLANVLAN-DC1
2
3  Done
4
5  > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3000 -vlan 3
6
7  Done
8
9  > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3500 -vlan 4
10
11 Done
12
13 >add vxlanVlanMap VXLANVLAN-DC2
14
15 Done
16
17 > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 8000 -vlan 3 4
18
19 Done
20
21 > set pbr PBR-CBC-DC-1-CLOUD ALLOW  -ipTunnel  CBC-DC-1-CLOUD -
      vxlanVlanMap VXLANVLAN-DC1
22
23 Done
24
```



```
25 > set pbr PBR-CBC-DC-2-CLOUD ALLOW  -ipTunnel  CBC-DC-2-CLOUD -
      vxlanVlanMap VXLANVLAN-DC2
26
27 Done
```

Geneve-Tunnel

May 11, 2023

Eine NetScaler-Appliance unterstützt das Generic Network Virtualization Encapsulation (Geneve) -Protokoll, wie in RFC 8926 definiert.
Servervirtualisierung und Cloud-Computing-Architektur haben die Nachfrage nach isolierten Layer-2-Netzwerken in einem Rechenzentrum erhöht.

Das VLAN-Limit von 4094 hat sich als unzureichend erwiesen und Kapselungsprotokolle wie VXLAN und NVGRE wurden eingeführt, um diese Einschränkung zu überwinden. Diese Protokolle unterscheiden sich hauptsächlich in der Implementierung der Steuerungsebene. Das Geneve-Protokoll definiert keine Spezifikationen für die Steuerungsebene. Das Protokoll überlässt der Implementierung, um die Spezifikationen der Steuerebene zu definieren.

Das Geneve-Protokoll ist eine Verkapselungstechnologie, die darauf abzielt, Layer-2-Overlay-Netzwerke über Layer-3-Infrastruktur zu erstellen, indem Layer-2-Frames in UDP-Pakete eingekapselt werden.

Eine eindeutige 24-Bit-ID namens VNID identifiziert jedes VLAN. Nur innerhalb derselben Segment-ID (VNID) können miteinander kommunizieren. Eine NetScaler-Appliance unterstützt die Geneve-Kapselung auf dem UDP-Port 6081.

Es gibt zwei Arten von Geneve-Tunneln, die erstellt werden können:

- Tunnel können ein vorhandenes VLAN im L2- oder L3-Modus erweitern. Im L2-Modus erfolgt das Bridging zwischen VLAN und Tunnel und die Einträge werden in der Bridge-Tabelle aktualisiert.

  Im L3-Modus wird Proxy-ARP wirksam, um die MAC-Adresse und die Tunnelinformationen der Client/Server-Adresse zu ermitteln. Die ARP-Tabelle enthält die entsprechenden MAC- und Tunnelinformationen.

- Geneve Tunnel kann mit verschiedenen VLANs im L3-Modus arbeiten, indem richtlinienbasierte Routen (PBRs) verwendet werden.
  Wenn ein Paket an einen Host gesendet werden muss, der in einem Geneve Tunnelsegment erreichbar ist, kapselt die NetScaler-Appliance das Paket in einem Geneve Tunnel-Header und sendet es an den Tunnelendpunkt.

NetScaler kann auch als Tunnelendpunkt fungieren. Ein Tunnelendpunkt entsteht und endet in Geneve-Tunneln. Wenn der Layer-2-Modus aktiviert ist, fungiert die NetScaler-Appliance als Tunnelendpunkt und überbrückt Pakete zwischen VLANs und Geneve Tunnels. Der NetScaler lernt die VNID und den Tunnelendpunkt, auf dem eine MAC-Adresse erreichbar ist. Dann speichert es diese Informationen in der Bridging-Tabelle.

Geneve-Tunnel wird in NetScaler-Administratorpartitionen, NetScaler-Hochverfügbarkeitssetups und NetScaler-Clustersetups unterstützt.

In einem Hochverfügbarkeitssetup wird eine Geneve-Tunnelkonfiguration an den sekundären Knoten weitergegeben oder synchronisiert. In einem Cluster-Setup ist die Geneve-Tunnelkonfiguration (Striped) identisch und auf allen Clusterknoten vorhanden.

Tunnel in Genf konfigurieren

Das Konfigurieren eines Geneve-Tunnels auf einer NetScaler-Appliance umfasst die folgenden Aufgaben:

- Einen IP-Tunnel mit Protokoll hinzufügen
- Eine Netzbrücke hinzufügen
- binde den Genfer Tunnel an die Netzbrücke

So fügen Sie mit der CLI einen IP-Tunnel mit dem Geneve-Protokollhinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- **add iptunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol** <Geneve> -**destPort** <port> -**tosInherit** (**ENABLED** | **DISABLED**) -**vlanTagging** (**ENABLED** | **DISABLED**) -**vnid**
- **show iptunnel**

So fügen Sie eine Net Bridge mit der CLI hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- **add netbridge** <name>
- **show netbridge**

So binden Sie den Geneve-Tunnel über die CLI an Netbridge:

Geben Sie in der Befehlszeile Folgendes ein:

- **bind netbridge** <name> -**vlan** <Vlan ID> -**tunnel** <tunnel name>
- **show netbridge**

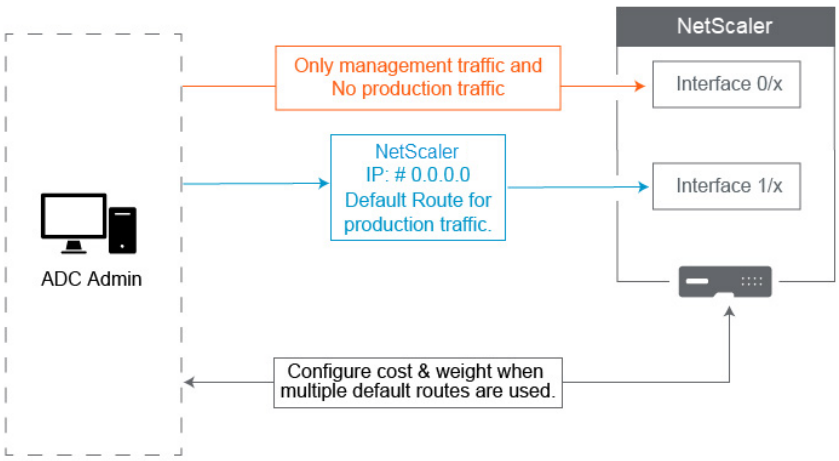
Bewährte Methoden für Netzwerkkonfigurationen

May 11, 2023

In den folgenden Abschnitten werden einige bewährte Methoden für die Konfiguration von Netzwerkfunktionen auf einer NetScaler-Appliance beschrieben.

Routing und Standardrouten

Im Folgenden finden Sie einige bewährte Methoden für die Konfiguration von Layer-3-Funktionen auf einer NetScaler-Appliance.



- **Die Schnittstelle `0/x` auf einer NetScaler Appliance oder NetScaler SDX-Appliance darf nicht für den Produktionsverkehr verwendet werden**. Auf einem MPX oder SDX `0/x` werden die benannten Interfaces auf die Management Interfaces verwiesen. Dies bedeutet nicht, dass Sie diese Schnittstellen für die Verwaltung verwenden müssen. Das bedeutet, dass diese Schnittstellen NICHT für den Produktionsverkehr konzipiert sind. Sie verfügen nicht über die Hardwarepuffer und Optimierungen, die erforderlich sind, um einen dauerhaften Durchsatz von 1 Gbit/s zu erreichen. Wenn sich Ihre Standardroute im selben Subnetz wie Ihr NSIP befindet, müssen Sie daher entweder die Standardroute ändern oder eine `1/x` Schnittstelle für Ihr Verwaltungsnetzwerk verwenden, da die `1/x` Schnittstellen vollständig für den 1-Gbit/s-Produktionsverkehr optimiert sind.

  > **Hinweis**:
  >
  > Dies gilt nicht für eine NetScaler VPX-Appliance.

  - **Variante 1.** Keine Verbindung zu Schnittstellen herstellen `0/x` — Trennen Sie das Kabel von der Schnittstelle `0/1`. NetScaler wartet auf den anderen Schnittstellen auf das NSIP.

(HINWEIS: Dies ist keine Option für SDX, da SVM und XenServer nur mit `0/x` Schnittstellen sprechen können)

- **Option 2**: Ändern Sie die Standardroute auf eine andere Schnittstelle, wie im nächsten Abschnitt beschrieben.

- **Das Standard-Gateway (Route 0.0.0.0) sollte sich in einem Produktionsnetzwerk und nicht auf einer Schnittstelle befinden.** `0/x` Wenn Sie einen NetScaler zum ersten Mal einrichten, werden Sie nach NSIP, Subnetzmaske und Gateway-Adresse gefragt. Das Problem, das für Administratoren entsteht, besteht darin, dass sie ihre Standardroute gerade so konfiguriert haben, dass sie über die Schnittstelle 0/1 in ihrem Verwaltungsnetzwerk verläuft.

  - Um zu überprüfen, was Ihre Routen sind, führen Sie die CLI `show route` aus. Ihr Standard-Gateway ist die IP in der Zeile, in der Netzwerk und Netzmaske 0.0.0.0 sind. Hier ist ein Beispiel, in dem sich das Gateway auf Zeile 1 befindet:

```
1  > sh route
2          Network          Netmask          Gateway/OwnedIP
               State   Traffic Domain  Type
3          -------          -------          ---------------
               -----   --------------  ----
4  1)      0.0.0.0          0.0.0.0          10.25.213.65     UP
            0               STATIC
5  2)      127.0.0.0        255.0.0.0        127.0.0.1        UP
            0               PERMANENT
6  3)      10.25.213.64     255.255.255.192  10.25.213.68     UP
            0               DIRECT
7  4)      172.16.0.0       255.255.255.0    172.16.0.1       UP
            0               DIRECT
8
9  <!--NeedCopy-->
```

  - Um zu überprüfen, welche Schnittstelle und welches VLAN für Ihr Standard-Gateway verwendet werden, überprüfen Sie die ARP-Tabelle mit `sh arp` in der CLI. Sie können auch mithilfe von `show arp | grep 10.25.213.65`. Hier ist ein Beispiel, in dem Sie sehen, dass das Gateway 10.25.213.65 Interface 1/1 und VLAN 1 verwendet:

```
1  > sh arp
2          IP               MAC               Iface VLAN
               Origin     TTL     Traffic Domain
3          --               ---               ----- ----
               ------     ---     --------------
4  1)      127.0.0.1        02:00:18:a4:00:1e  LO/1  1
       PERMANENT  N/A    0
5  2)      10.25.213.70     02:00:0f:46:00:28  1/1   1
```



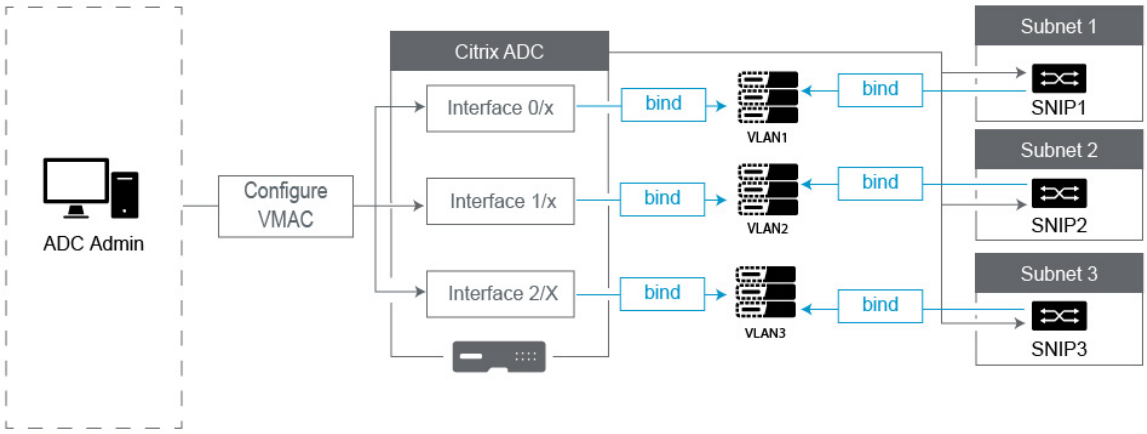
```
        DYNAMIC     967     0
6   3)      10.25.213.68      02:00:18:a4:00:1e   LO/1   1
        PERMANENT   N/A     0
7   4)      10.25.213.67      02:00:0f:46:00:28   1/1    1
        DYNAMIC     641     0
8   5)      10.25.213.65      00:08:e3:ff:fd:90   1/1    1
        DYNAMIC     483     0
9   <!--NeedCopy-->
```

- Ändern Sie die Standardroute, um ein Gateway in Ihrem Produktionssubnetz und Ihrer Schnittstelle zu verwenden. Nehmen wir an, Ihr Verwaltungsnetzwerk ist 10.0.0.0/24 mit Gateway 10.0.0.1 und Ihr Produktionsnetzwerk ist 10.1.1.0/24 mit Gateway 10.1.1.1. Richten Sie Ihre Konfiguration wie folgt ein:
  * SNIP: (Verwaltungszugriff deaktiviert) 10.1.1.2
  * NSIP: (Verwaltungszugriff aktiviert) 10.0.0.2
  * Standardroute: 0.0.0.0 0.0.0.0 10.1.1.1 (System > Netzwerk > Routen). Dies verwendet einen Router im SNIP-Netzwerk anstelle des NSIP-Netzwerks.

    > **Hinweis**:
    >
    > Eine Änderung des Standard-Gateways kann den Verwaltungsdatenverkehr unterbrechen, sofern Sie keine statischen Routen oder eine richtlinienbasierte Route konfigurieren oder die MAC-basierte Weiterleitung aktivieren.

Schnittstellen, Kanäle und VLANs

Im Folgenden finden Sie einige bewährte Methoden für die Konfiguration von Layer-2-Funktionen auf einer NetScaler-Appliance.



- **Verbinden Sie nicht mehrere Schnittstellen/Kanäle mit demselben VLAN, einschließlich VLAN 1:**
  - Wenn Sie Ihre VLANs nicht richtig konfigurieren, kann dies zu unerwartetem Paket-Routing in Ihrem Netzwerk und Layer-2-Schleifen führen, wenn mehr als eine aktive Schnittstelle mit demselben VLAN vorhanden ist (entweder Native oder Tagged).
  - Standardmäßig befinden sich alle Schnittstellen und Kanäle im nativen VLAN 1. Dies führt zu zwei möglichen Problemen:
    * Der NetScaler geht davon aus, dass sich der gesamte empfangene Datenverkehr im selben Netzwerk befindet, und verwendet daher eine beliebige Schnittstelle, um den Datenverkehr zu senden. Wenn Sie auf der Schnittstelle, über die Daten gesendet wurden, ein anderes natives VLAN haben, wird der Datenverkehr nicht wie erwartet weitergeleitet.
    * Wenn der NetScaler Broadcast-Pakete an einem Port empfängt, kann er sie an einem anderen Port erneut übertragen. Wenn sich beide Switchports im selben VLAN befinden, haben Sie gerade eine Layer-2-Schleife erstellt.
  - Um eine Schnittstelle/einen Kanal aus VLAN 1 zu entfernen:
    * Wenn Sie keine nativen VLANs auf Ihrer Switch-Schnittstelle/Ihrem Port-Channel verwenden. Ändern Sie das native VLAN auf der NetScaler Interface/Channel auf eine ungenutzte VLAN-Nummer wie 999. Sie sollten nicht dieselbe ungenutzte VLAN-Nummer für mehrere Kanäle oder Schnittstellen verwenden, da dadurch eine Layer-2-Schleife entsteht.
    * Wenn Sie native VLANs auf Ihrer Switch-Schnittstelle/Ihrem Port-Channel verwenden. Ändern Sie das systemeigene VLAN auf der NetScaler-Schnittstelle/dem NetScaler-Kanal entsprechend. Achten Sie jedoch darauf, nicht mehrere aktive Schnittstellen oder Kanäle im selben VLAN zu haben, da dadurch Layer-2-Loops entstehen.
    * Sie können das native VLAN nicht entfernen. Stattdessen können Sie es ändern oder TagAll für die Schnittstelle oder den Kanal festlegen. Wenn der Switch-Port nicht mit einem nativen VLAN ohne Tags konfiguriert ist, aktivieren Sie Tagall auf der Schnittstelle, damit Heartbeat-Pakete mit hoher Verfügbarkeit gekennzeichnet werden.
  - Um das native VLAN auf einer Schnittstelle anzuzeigen, führen Sie es `sh interface` in CLI aus. Dadurch werden Sie auch darüber informiert, ob die Schnittstelle die TAGALL-Option verwendet.
- **Binden Sie eine Schnittstelle an Ihr VLAN** — Der NetScaler fügt standardmäßig kein neues VLAN an eine Schnittstelle an. Das bedeutet, dass das VLAN erst verwendet wird, wenn Sie es an eine Schnittstelle binden. Wenn das neue VLAN nicht an eine Schnittstelle gebunden ist und

dieses VLAN markiert ist, löscht der NetScaler den gesamten eingehenden Datenverkehr von diesem VLAN. Binden Sie dasselbe VLAN auch nicht an mehr als eine Schnittstelle.

  - Binden Sie Subnetze an Ihre VLANs. Der NetScaler funktioniert nicht wie ein typischer Router. Die meisten Router verbinden IPs mit Schnittstellen. Auf einem NetScaler schweben die IPs auf jeder Schnittstelle, sofern nicht anders konfiguriert. Daher müssen Sie für jedes Subnetz, für das Sie sicherstellen möchten, dass der NetScaler über ein bestimmtes VLAN sendet, insbesondere wenn der NetScaler diesen Verkehr initiiert, ein SNIP innerhalb dieses Subnetzes an das VLAN binden.
  - Ein häufiges Argument, das wir dagegen hören, ist, dass es früher einwandfrei funktioniert hat und jetzt nicht mehr funktioniert, ohne das Subnetz an das VLAN zu binden. Dies tritt häufig auf, weil der NetScaler lernt, welches VLAN er aussenden soll. Dies kann jedoch einige Zeit in Anspruch nehmen, da er seine ARP-Tabellen erstellt. Nach einem Neustart oder einem Firmware-Upgrade, wenn es erneut mit dem Erstellen der ARP-Tabellen beginnt, lernt es möglicherweise zunächst und verwendet daher einen anderen Pfad als Sie möchten, z. B. Ihre Standardroute. Am besten weisen Sie ihm an, welchen Pfad er einschlagen soll, indem Sie das SNIP an das VLAN binden. Sobald ein SNIP an ein VLAN gebunden ist, wird das gesamte Subnetz für dieses SNIP an das VLAN gebunden.
  - Stellen Sie sicher, dass jedes SNIP an ein VLAN gebunden ist (außer in Fällen, in denen Sie mehr als 1 SNIP in einem Subnetz haben, dann müssen Sie nur eines binden) und dass das VLAN wiederum nur an eine Schnittstelle oder einen Kanal gebunden ist. Oft ist es auch am besten, in jedem Subnetz ein SNIP zu haben, aber das ist nicht erforderlich, da die spezifischste Route für jedes Zielsubnetz verwendet wird, das kein SNIP hat.

- Um das von einem Subnetz verwendete VLAN und die Schnittstelle zu identifizieren, gehen Sie wie folgt vor:

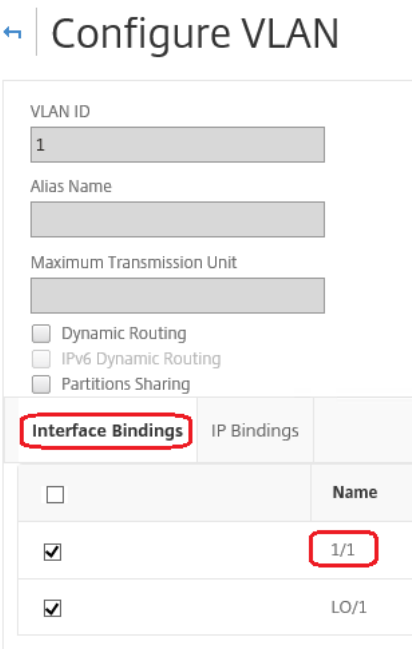
  1. Gehen Sie zu **System> Netzwerk > VLANs**.
  2. Bearbeiten Sie jedes konfigurierte VLAN nacheinander, bis Sie die richtige IP-Adresse gefunden haben, wie im nächsten Schritt erläutert.
  3. Klicken Sie auf die Registerkarte IP-Bindungen, um zu sehen, welche IP und somit welches Subnetz gebunden ist und daher dieses VLAN verwendet.
  4. Sobald Sie das VLAN identifiziert haben, an das eine IP gebunden ist, wobei sich diese IP innerhalb des Subnetzes der Standardroute befindet, klicken Sie auf die Schnittstellenbindungen. Jede Schnittstelle oder jeder Kanal, der an dieses VLAN gebunden ist, wird verwendet.

Beispiel

Nehmen wir an, die Standardroute lautet `0.0.0.0 0.0.0.0 10.1.1.1`.

Angenommen, Sie haben zwei SNIPs von 10.0.0.5 und 10.1.1.69. Da sich 10.1.1.69 im Subnetz der Standardroute befindet, sollten Sie nach dieser suchen. In den folgenden Screenshots überprüfen wir VLAN 1 und wir sehen, dass die IP 10.1.1.69 an dieses VLAN gebunden ist, sodass wir wissen, dass wir es mit dem richtigen VLAN zu tun haben.

Klicken Sie nun auf Interface Bindings. In den VLAN-Schnittstellenbindungen sehen wir, dass Interface für dieses Subnetz verwendet `1/1` wird und daher für die Standardroute verwendet wird.



> **HINWEIS**:
>
> Wenn Sie keine IPs an Ihre VLANs gebunden haben, werden diese standardmäßig an VLAN 1 gesendet. Schauen Sie sich in diesem Fall also an, welche Schnittstellen an VLAN 1 gebunden sind. Dies bedeutet auch, dass der NetScaler Ihre konfigurierten VLANs nicht für den von ihm initiierten Datenverkehr verwendet, es sei denn, Sie binden eine IP an das neue VLAN.

Unentgeltliches ARP

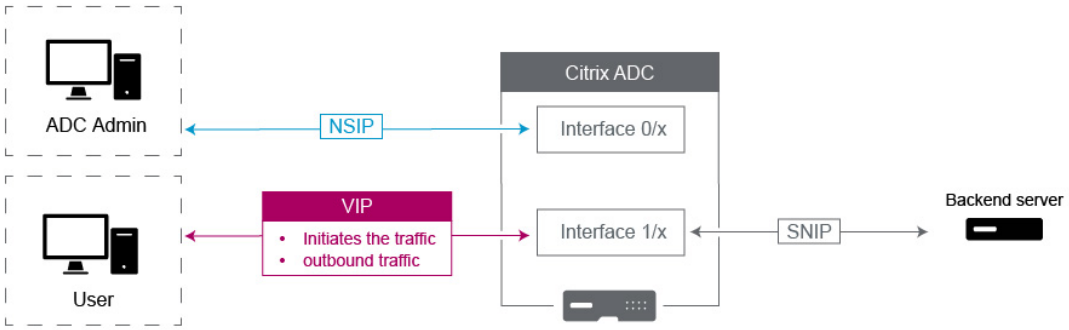
Wenn GARP nicht funktioniert, verwenden Sie VMAC. Standardmäßig verwendet der NetScaler GARP, um seine IP-zu-MAC-Adressbindungen an andere Netzwerkgeräte weiterzuleiten. Dies funktioniert normalerweise problemlos. Wenn Sie jedoch mehr Dienste im NetScaler erstellen, können Probleme auftreten, wenn ein Failover auf einem HA-Paar auftritt. Das häufigste Problem ist, dass die Dienste in dem NetScaler, auf den Sie ein Failover ausgeführt haben, nicht verfügbar sind, weil einige Netzwerkgeräte ihre ARP-Tabellen nicht mit der neuen MAC-Adresse aktualisiert haben. Sie können dies leicht überprüfen, indem Sie in ihren ARP-Tabellen nachsehen, ob die MAC-Adressen mit denen auf dem jetzt primären NetScaler übereinstimmen. In diesem Fall ist es sehr wahrscheinlich, dass einige Ihrer Netzwerkgeräte die Anzahl der GARP-Werbung einschränken, die sie akzeptieren. In diesem Fall

ist es notwendig, VMAC auf all Ihren aktiven Schnittstellen und/oder Kanälen zu konfigurieren. Wenn Sie eine umfangreiche Konfiguration auf Ihrem NetScaler erwarten, ist es möglicherweise am besten, VMAC für alle Schnittstellen und Kanäle während der ersten Bereitstellung zu konfigurieren.

> **HINWEIS**:
>
> Vergessen Sie nicht, VMAC für die Schnittstelle oder den Kanal zu konfigurieren, die von Ihrer Standardroute verwendet werden.

NetScaler-eigene IP-Adressen

In diesem Abschnitt werden die bewährten Methoden für die Konfiguration von NetScaler-eigenen IP-Adressen beschrieben:



- **NetScaler IP (NSIP)**: Im Allgemeinen wird diese IP für die Verwaltung verwendet, da sie die einzige IP ist, die nur für einen einzelnen NetScaler in einer HA- oder Cluster-Umgebung gilt. Beachten Sie auch, dass LDAP-, RADIUS- und vom Benutzer geskripteter Monitor-Verkehr (wie der LDAP-Monitor und der StoreFront-Monitor) vom NSIP stammen und somit über das VLAN und die Schnittstelle weitergeleitet werden, an die das NSIP gebunden ist (standardmäßiges natives VLAN 1). Wenn Sie den LDAP- und RADIUS-Verkehr vom SNIP beziehen möchten, erstellen Sie einen virtuellen LB-Server für Ihre Back-End-Server.
- **Subnetz-IP (SNIP)**: Diese IP-Adresse wird verwendet, um die Kommunikation mit Back-End-Servern zu initiieren und wird immer den Datenverkehr initiieren. In diesen Fällen kann es jedoch das Ziel für den Verkehr sein:
  - Sie kann als Gateway-Adresse auf anderen Geräten verwendet werden, wenn Layer-3-Routing auf dem NetScaler durchgeführt wird.
  - Wenn es aktiviert ist, kann es Verwaltungsdienste wie den Zugriff auf die GUI, SSH und SNMP akzeptieren.

- **Virtuelle IP (VIP)**: Das VIP ist insofern einzigartig, als es niemals zur Initiierung von ausgehendem Datenverkehr verwendet wird. Es ist nur für den Empfang von Traffic vorgesehen. Sobald es Datenverkehr empfängt, antwortet es und sendet ausgehenden Datenverkehr an den Client zurück. Mit anderen Worten, die VIP-Adresse initiiert den ausgehenden Verkehr nicht.

Beachten Sie, dass dies auch nicht als Quelle für die Kommunikation mit Back-End-Servern verwendet wird, die beispielsweise in einem virtuellen LB-Server verwendet werden.

Konfigurieren, um NetScaler FreeBSD-Datenverkehr von einer SNIP-Adresse aus zu beziehen

May 12, 2023

Einige NetScaler-Datenfunktionen laufen auf dem zugrunde liegenden FreeBSD-Betriebssystem statt auf dem NetScaler-Betriebssystem. Aus diesem Grund senden diese Funktionen Datenverkehr, der von der NetScaler-IP-Adresse (NSIP) stammt, anstatt von einer SNIP-Adresse. Es ist nicht wünschenswert, den Datenverkehr von der NSIP-Adresse zu beziehen, wenn Ihr Setup über Konfigurationen verfügt, um den gesamten Management- und Datenverkehr zu trennen.

Die folgenden NetScaler-Datenfunktionen laufen auf dem zugrunde liegenden FreeBSD-Betriebssystem und senden Datenverkehr, der von der NetScaler-IP-Adresse (NSIP) stammt:

- Skriptfähige Monitore für den Lastausgleich
- GSLB Autosync

Um dieses Problem zu beheben, können Sie den globalen Layer-2-Parameter verwenden:. `useNetprofileBSDtraffic` Wenn Sie diesen Parameter aktivieren, senden die NetScaler-Funktionen Datenverkehr, der von einer der SNIP-Adressen in einem der Funktion zugeordneten Netzprofil stammt.

Voraussetzungen

Bevor Sie die NetScaler-Appliance so konfigurieren, dass sie den mit NetScaler-Funktionen verbundenen Datenverkehr von einer SNIP-Adresse bezieht, beachten Sie die folgenden Punkte:

- Derzeit wird der globale Layer-2-Parameter nur für skriptfähige `useNetprofileBSDtraffic` Monitore für den Lastenausgleich unterstützt.

  Um die NetScaler-Appliance so zu konfigurieren, dass sie GSLB-Autosync-Verkehr von einer SNIP-Adresse bezieht, können Sie erweiterte ACL-Regeln und RNAT-Regeln als Workaround verwenden.

- Die `useNetprofileBSDtraffic` Unterstützung von skriptfähigen Monitoren für den Lastenausgleich gilt nur für Netzprofile, die an die zugehörigen Dienste gebunden sind. Die `useNetprofileBSDtraffic` Unterstützung gilt nicht für Netzprofile, die an die entsprechenden Dienstgruppen gebunden sind.

  Mit anderen Worten, die NetScaler Appliance verwendet keine SNIP-Adresse aus den Netzprofilen, die an die Dienstgruppen gebunden sind, um den Lastenausgleich skriptfähig zu beziehen, überwacht den Datenverkehr.

- Der `useNetprofileBSDtraffic` Support gilt nicht für SSL-Dienste.

  Mit anderen Worten, die NetScaler Appliance verwendet keine SNIP-Adresse aus den Netzprofilen, die an die SSL-Dienste gebunden sind, um den Datenverkehr für den Lastenausgleich für skriptfähige Monitore zu beschaffen.

Konfigurieren der NetScaler Appliance, um skriptfähig zu beziehen, überwacht den Datenverkehr von einer SNIP-Adresse

Die Konfiguration der NetScaler-Appliance zur Quelle skriptfähiger Monitore von einer SNIP-Adresse umfasst die folgenden Aufgaben:

- Aktivieren Sie den globalen Layer-2-Parameter. `useNetprofileBSDtraffic`
- Erstellen Sie ein Netzprofil und binden Sie mindestens eine SNIP-Adresse daran.
- Binden Sie das Netzprofil an die Load Balancing-Dienste, die skriptfähige Monitore verwenden.

Um den Layer-2-Parameter UsenetProfileBSDTraffic mit der CLI zu aktivieren:

Geben Sie in der Befehlszeile Folgendes ein:

- **set l2param**-**UsenetProfileBSDTraffic (AKTIVIERT/DEAKTIVIERT**)****
- **l2param anzeigen**

Um ein Netzprofil zu erstellen und SNIP-Adressen mit der CLI daran zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- ****NetProfile hinzufügen - Scrip**** <name><string>
- **NetProfile anzeigen**

Um ein Netzprofil mit der CLI an einen Load Balancing-Dienst zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- **Dienst einrichten** <name>-**NetProfile** <string>
- **show service** <name>

Beispiel-Konfiguration

Die folgende Beispielkonfiguration ermöglicht es einer NetScaler-Appliance, skriptfähige Monitor-Traffic von einer SNIP-Adresse zu beziehen. Ein Netzprofil NETPROFILE-1 ist mit der daran gebundenen SNIP-Adresse 198.51.100.20 konfiguriert. Ein Benutzer-/skriptfähiger Monitor USER-MONITOR-1 wird erstellt und ist an einen Load-Balancing-Dienst SERVICE-1 gebunden. NETPROFILE-1 ist an SERVICE-1 gebunden. Die NetScaler-Appliance bezieht alle skriptfähigen Monitor-Pakete von USER-MONITOR-1 von der SNIP-Adresse 198.51.100.20.

```
set l2param -useNetprofileBSDtraffic ENABLED

set netprofile NETPROFILE-1 -srcip 198.51.100.20

add lb monitor USER-MONITOR-1 USER -scriptName nsftp.pl -scriptArgs "
    file=Index.png;user=nsroot;password=nsroot" -dispatcherIP 127.0.0.1
    -dispatcherPort 3013 -destIP 203.0.113.90 -destPort 21

bind service SERVICE-1 -monitorName USER-MONITOR-1

set service SERVICE-1 -netProfile NETPROFILE-1

<!--NeedCopy-->
```

Konfigurieren Sie die NetScaler-Appliance so, dass sie GSLB-Autosync-Verkehr von einer SNIP-Adresse bezieht

Die Konfiguration der NetScaler-Appliance für die Beschaffung von GSLB-Autosync-Verkehr von einer SNIP-Adresse umfasst die folgenden Aufgaben zur Problemumgehung:

- **Erstellen Sie eine erweiterte ACL-Regel**. Eine erweiterte ACL-Regel identifiziert die GSLB-Autosync-Pakete. Diese Identifizierung basiert auf den Quell-IP- und Ziel-IP-Adressen.
- **Wenden Sie ACLs an.** Durch das Anwenden von ACLs wird die neu erstellte ACL-Regel aktiviert.
- **Erstellen Sie eine ACL-basierte RNAT-Regel**. Eine RNAT-Regel ändert die Quell-IP-Adresse dieser Pakete von der NSIP-Adresse in eine SNIP-Adresse.

> **Hinweis:**
>
> In einem Hochverfügbarkeits- oder Cluster-Setup müssen Sie ACL- und RNAT-Regeln für alle NSIP-Adressen des Setups hinzufügen.

Um eine erweiterte ACL mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add acl** <aclname> **ALLOW** -**srcIP** = <NSIP address> -**destIP** = <destination IP address of the packets>

- **show acl** <aclName>

So wenden Sie erweiterte ACLs mithilfe der CLI an:

Geben Sie in der Befehlszeile Folgendes ein:

- **apply acls**

Um eine ACL-basierte RNAT-Regel mit der CLI zu erstellen:

Geben Sie in der Befehlszeile Folgendes ein:

- **add rnat** <name> <aclname>
- **bind rnat** <name> -**natIP** <SNIP address - source IP address for the packets>
- **show rnat** <name>

Beispiel-Konfiguration

Die folgende Beispielkonfiguration ermöglicht es einer NetScaler-Appliance, GSLB-Autosync-Verkehr von einer SNIP-Adresse zu beziehen. ACL-2 identifiziert GSLB-Autosync-Pakete, die von der NSIP-Adresse 192.0.1.20 stammen und für die GSLB-Standort-IP-Adresse 203.0.113.20 bestimmt sind. RNAT-2 ändert die Quell-IP-Adresse für diese identifizierten Pakete in die SNIP-Adresse 198.51.100.20.

```
add acl ACL-2 ALLOW -srcIP = 192.0.1.20  -destIP = 203.0.113.20

apply acls

add rnat RNAT-2 ACL-2

bind rnat RNAT-2 -natIP 198.51.100.20
<!--NeedCopy-->
```

Beobachtbarkeit

July 4, 2023

Aufgrund der zunehmenden Komplexität moderner Anwendungen wird die Überwachung und Fehlerbehebung von Anwendungen für IT-Teams immer schwieriger. Außerdem ist es für Softwareentwicklungsteams wichtiger, einen Einblick in das Verhalten von Infrastruktur und Anwendungen zu erhalten. Observability schließt diese Lücke, indem sie tiefere Einblicke in die gesamte Infrastruktur bietet. Observability-Tools können kontinuierlich Telemetriedaten zur Anwendungs- oder Systemleistung erfassen, indem sie in verschiedene IT-Infrastrukturkomponenten integriert werden und einen ganzheitlichen Einblick in Ihre IT-Infrastruktur bieten.

Einige der Vorteile von Observability lassen sich wie folgt zusammenfassen:

- Schnellere Fehlerbehebung: Detaillierte Dateneinblicke aus Observability-Tools helfen Ihnen, Systemprobleme schneller zu diagnostizieren und zu beheben.
- Verbesserte Anwendungsleistung: Die Überwachung wichtiger Kennzahlen und die Identifizierung von Problemen helfen Entwicklern, datengestützte Entscheidungen zur Verbesserung der Anwendungsleistung zu treffen.
- Verbesserte Zuverlässigkeit und bessere Benutzererfahrung: Observability-Daten ermöglichen es Entwicklern, Systemausfälle, die die Benutzererfahrung beeinträchtigen könnten, proaktiv zu beheben.

Was ist Beobachtbarkeit

Beobachtbarkeit ist die Fähigkeit, den internen Zustand eines Systems zu verstehen, indem die von ihm produzierten Daten wie Protokolle, Metriken, Traces und Ereignisse analysiert werden. Observability ermöglicht es Ihnen, spezifische Fragen zum Verhalten Ihres Systems bei Ausfällen zu verstehen und zu beantworten. Mit einem tiefen Verständnis Ihrer Systeme können Sie besser auf das Unbekannte vorbereitet sein.
Sie können beispielsweise verfolgen, wie langsam oder schnell, was kaputt ist und was getan werden sollte, um die Systemleistung zu verbessern.

Metriken, Protokolle und Traces sind die wichtigsten Säulen der Beobachtbarkeit.

- Metriken: Metriken sind eine numerische Darstellung von Daten, die über einen bestimmten Zeitraum gemessen wurden. Metrische Daten sind nützlich, um den Zustand eines Systems im Laufe der Zeit zu verfolgen. Diese numerischen Messungen umfassen CPU-Auslastung, Speicherauslastung und Fehlerraten.
- Protokolle: Protokolle sind Nachrichten oder Aufzeichnungen, die Ereignisse beschreiben, die zu einem bestimmten Zeitpunkt eingetreten sind. Normalerweise werden diese Nachrichten oder Datensätze von einer Anwendung oder einem System generiert.
- Traces: Traces stellen die Reise einer Anfrage dar, die sich durch die verschiedenen Teile eines verteilten Systems bewegt. Traces dokumentieren, wie eine Anfrage bearbeitet wird und wie lange es dauert, bis sie abgeschlossen ist. Diese Daten können helfen, Engpässe und andere Latenzprobleme zu identifizieren.

Überwachung versus Beobachtbarkeit

Bei der Überwachung handelt es sich um eine Reihe von Tools oder Lösungen, mit denen Sie informiert werden, wenn etwas nicht stimmt. Mit Observability können Sie erkennen, was passiert, und schnell die Ursache der Probleme lokalisieren, um zu erfahren, warum sie passiert sind. Es integriert die durch die Überwachung generierten Fakten und Daten, um Ihnen einen umfassenden

Überblick über die Leistung und den Zustand Ihres Systems zu bieten. Mithilfe von Observability können Sie Ihre Daten automatisch analysieren und die Benutzererfahrung auf der Grundlage einer schnellen, genauen Eingabe verbessern.

Beobachtbarkeit mit NetScaler

Wenn NetScaler als Proxy für Anwendungsbereitstellungen bereitgestellt wird, überprüft NetScaler jede Benutzeranfrage oder Antwort auf globales Routing und lokales Rechenzentrumsrouting. Mit den Tausenden von Protokollen und Zählern, die NetScaler zur Verfügung stellt, können Sie detaillierte Informationen über HTTP-, TCP-, SSL- und DNS-Pakete abrufen. Sie können diese umfangreichen Daten und Erkenntnisse von NetScaler nutzen, um Probleme zu beheben und zu lokalisieren. Sie können die Daten von NetScaler auf Ihre bevorzugten Observability-Endpunkte exportieren, um Visualisierungen zu erstellen und detaillierte Anwendungseinblicke in Echtzeit zu erhalten.

NetScaler bietet Integrationen mit beliebten Observability-Tools wie Prometheus, Splunk, Elastic-Search und Kafka.
Die direkte Integration von NetScaler ist in Prometheus verfügbar. Bei der direkten Integration müssen Sie keinen zusätzlichen Agenten oder Knoten bereitstellen, um die Daten zu exportieren und benutzerdefinierte Dashboards für Ihre Bedürfnisse zu erstellen. Prometheus konzentriert sich auf die Überwachung von Zeitreihendaten, bei der numerische Metriken von allen Entitäten erfasst werden.

NetScaler ADM verfügt über mehrere integrierte Observability-Funktionen wie SSL-Einblicke, Einblicke in Webtransaktionen und API-Einblicke.

NetScaler kann im Rahmen der Observability drei Arten von Erkenntnissen bereitstellen:

- Einblicke in Anwendungen und APIs: Einblicke in den Anwendungsstatus helfen bei der Fehlerbehebung, welche Anwendungswebsite eine hohe Latenz, eine hohe Anzahl von Fehlern oder eine unterdurchschnittliche Leistung aufweist. Es umfasst auch die Überwachung von Fehlern, Datenverkehr, Latenz und Sättigung. Zusammengefasst werden diese Signale als die goldenen Signale zur Überwachung des Status von Anwendungen bezeichnet.
- Einblicke in die Anwendungs- und API-Sicherheit: Zu den Erkenntnissen zur Anwendungssicherheit gehören erkannte oder verhinderte WAF-Verstöße im Vergleich zum Gesamtverkehr, die am häufigsten von WAF- oder BOT-Verstößen betroffene Anwendung sowie CVEs, BOT-Klassifizierungen wie gute und schlechte Bots, und liefert Informationen über Angreifer.
- Einblicke in die Netzwerkinfrastruktur: Die Einblicke in die NetScaler-Infrastruktur beinhalten Informationen über den NetScaler, z. B. die CPU-Auslastung, Speicher- und Festplattennutzung sowie Netzwerkschnittstellentelemetrie. Sie können auch spezifische Einblicke auf Funktionsebene wie SSL, GSLB, Multipath TCP (MPTCP) und Einblicke in die SSL-TLS-Überwachung wie Details zum Ablauf von Zertifikaten, verwendetes Protokoll und Verschlüsselungsstärke erhalten.

Detaillierte Informationen zum direkten Export von Metriken aus NetScaler nach Prometheus finden Sie unter NetScaler , Anwendungen und Anwendungssicherheit mit Prometheus überwachen.

Überwachung von NetScaler, Anwendungen und Anwendungssicherheit mit Prometheus

September 1, 2023

Metriken sind eine numerische Darstellung von Daten, die über einen bestimmten Zeitraum gemessen werden. Metrische Daten sind nützlich, um den
Zustand eines Systems im Laufe der Zeit zu verfolgen. Prometheus ist ein Open-Source-Überwachungstool, das Kennzahlendaten sammelt und diese Daten mit einem Zeitstempel speichert, zu dem die Daten aufgezeichnet wurden.

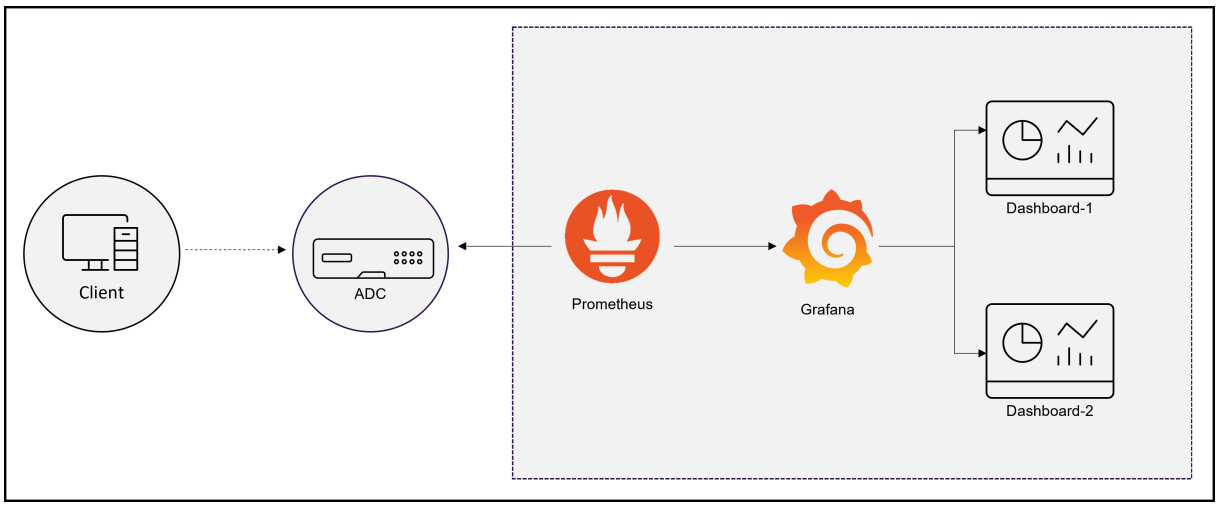
Durch die Überwachung und Analyse von Metriken können Sie den Zustand Ihrer Anwendungen verfolgen, Anomalien erkennen, Warnmeldungen erstellen und die erforderlichen Korrekturmaßnahmen ergreifen, um eine robuste Softwarebereitstellung zu gewährleisten.

NetScaler unterstützt jetzt den direkten Export von Metriken nach Prometheus. Sie können die umfangreichen Metriken von NetScaler ADC verwenden, um den NetScaler-Zustand und den Anwendungsstatus zu überwachen. Sie können beispielsweise Metriken zur CPU- und Speichernutzung sammeln, um den Zustand von NetScaler zu ermitteln. In ähnlicher Weise können Sie Metriken wie die Anzahl der pro Sekunde empfangenen HTTP-Anfragen oder die Anzahl der aktiven Clients verwenden, um den Zustand der Anwendung zu überwachen.

Export von Metriken von NetScaler nach Prometheus

NetScaler unterstützt den Prometheus-Pull-Modus sowie den Push-Modus. Im Pull-Modus müssen Sie ein Zeitreihenprofil konfigurieren, das Prometheus in regelmäßigen Abständen abfragt und die Metrikdaten direkt abruft, ohne dass eine Exporter-Ressource dazwischen liegt. Im Pull-Modus können Sie einem Benutzer ohne Superuser-Rechte den Lesezugriff aktivieren, um Metriken nach Prometheus zu exportieren. Mit Grafana können Sie die nach Prometheus exportierten NetScaler-Metriken visualisieren, um sie einfacher zu interpretieren und zu verstehen.

Das folgende Diagramm zeigt eine Integration von Prometheus und Grafana mit NetScaler.



Konfigurieren Sie den Export von Metriken von NetScaler nach Prometheus und die Visualisierung mit Grafana

Sie müssen die folgenden Schritte ausführen, um den Export von Metriken von NetScaler nach Prometheus zu konfigurieren und ihn mit Grafana zu visualisieren.

1. Konfigurieren Sie NetScaler mit einem Zeitreihenanalyseprofil für den Export von Metriken nach Prometheus.
2. Installieren Sie Prometheus und konfigurieren Sie es mit den NetScaler-spezifischen Parametern.
3. Fügen Sie Prometheus als Datenquelle in Grafana hinzu.
4. Erstellen Sie eine Visualisierung in Grafana

Konfigurieren Sie ein Zeitreihenanalyseprofil auf NetScaler, um den Prometheus-Pull-Modus zu unterstützen

Führen Sie die folgenden Schritte aus, um den Pull-Modus mit der NetScaler CLI zu konfigurieren:

1. Erstellen Sie ein Analyseprofil mit dem Typ als Zeitreihe. Geben Sie die Schemadatei mit den erforderlichen NetScaler-Metriken an.

```
1 add analytics profile <timeseries_profile_name> -type timeseries -
     schemaFile <name_of_schema_file>
2 -outputMode Prometheus -serveMode PULL -metrics ENABLED
```

   In diesem Befehl:

   - `timeseries_profile_name`: Geben Sie den Namen des Zeitreihenprofils an.
   - `schemaFile`: Geben Sie den Namen der Schemadatei mit NetScaler-Zählern an. Standardmäßig ist eine Schemadatei `/var/metrics_conf/schema.json` mit einer Liste

von Zählern konfiguriert. Eine Referenzschemadatei `reference_schema.json` mit allen unterstützten Zählern ist ebenfalls unter dem Pfad `/var/metrics_conf/` verfügbar. Diese Schemadatei kann als Referenz verwendet werden, um eine benutzerdefinierte Liste von Zählern zu erstellen. Wenn Sie die Schemadatei angeben, wird der Pfad der Schemadatei `/var/metrics_conf/` automatisch hinzugefügt und Sie müssen nur den Namen der Schemadatei angeben. Wenn Sie beispielsweise eine Schemadatei `schema1.json` mit einer benutzerdefinierten Liste von Leistungsindikatoren unter `/var/metrics_conf/` erstellt haben, müssen Sie nur den Dateinamen als `schema1.json` angeben.

- `outputMode`: Stellen Sie den Ausgabemodus auf Prometheus ein.
- `serveMode`: Geben Sie den Prometheus-Pull-Modus an.
- `metrics`: Aktivieren Sie das Erfassen von Metriken von NetScaler.

> **Hinweis:**
>
> Mit dem Befehl add können Sie ein Analyseprofil mit allen erforderlichen Parametern konfigurieren. Wenn Sie nach der Erstellung des Profils Änderungen vornehmen müssen, können Sie den Befehl set verwenden, um die entsprechenden Maßnahmen zu ergreifen, z. B. die Metriken zu deaktivieren und den Servermodus zu ändern. Sie können den schreibgeschützten Prometheus-Zugriff für einen Nicht-Superuser konfigurieren. Weitere Informationen finden Sie unter Konfiguration des schreibgeschützten Prometheus-Zugriffs für Nicht-Superuser.

Installieren und konfigurieren Sie Prometheus für den Metrikenexport aus NetScaler

Sie können Prometheus von Repositorys wie DockerHub oder Quay oder dem offiziellen Prometheus-Repository herunterladen.

Um Prometheus als Docker-Container auszuführen, verwenden Sie den folgenden Befehl:

```
1    docker run -dp 39090:9090 -v /tmp/prometheus.yml:/etc/prometheus/
        prometheus.yml --name native_prom prom/prometheus:latest  > **
        Hinweis:** > > Hier wird `/tmp/prometheus.yml` als Pfad zur
        Datei `prometheus.yml` verwendet. Stattdessen können Sie den
        Pfad auf Ihrer virtuellen Maschine angeben.
```

Sie müssen das `prometheus.yml` mit den NetScaler-Parametern bearbeiten.

Um Metriken aus NetScaler zu exportieren, müssen Sie im Abschnitt **Prometheus YAML Scrape-Konfiguration** die folgenden NetScaler-spezifischen Parameter angeben. Der Abschnitt Scrape-Konfiguration spezifiziert eine Reihe von Zielen und Konfigurationsparametern, die beschreiben, wie sie ausgelesen werden.

- `metrics_path`: Geben Sie den HTTP-Ressourcenpfad in NetScaler (/nitro/v1/config/systemfile) an, um Metriken abzurufen.
- `username`: Geben Sie den NetScaler-Benutzernamen an.
- `password`: Geben Sie das NetScaler-Kennwort an.
- `targets`: Geben Sie die IP-Adresse des NetScaler an, von dem Sie Metriken exportieren müssen,
  die Metriken und den Port, den Sie verfügbar machen möchten.
- `filename` : Geben Sie den Namen des konfigurierten Zeitreihenprofils anstelle von `timeseries_profile_name` at in der `metrics_prom_<timeseries_profile_name>.log` Datei an.
- `filelocation`: Geben Sie den Speicherort der Datei an als `/var/nslog`.

Im Folgenden finden Sie den Abschnitt zur Scrap-Konfiguration der Prometheus-YAML, um die NetScaler-IP-Adresse als Ziel auf Prometheus hinzuzufügen, um Metriken zu exportieren. Hier wird HTTP als Schema verwendet. Sie können entweder HTTP oder HTTPS verwenden.

```
scrape_configs:
  - job_name: 'vpx2_metrics_direct'
    metrics_path: /nitro/v1/config/systemfile
    params:
      args: ['filename:metrics_prom_ns_analytics_time_series_profile.
         log,filelocation:/var/nslog']
      format: ['prometheus']
    basic_auth:
     username: 'prom_user'
     password: 'user_password'
    scheme: http
    scrape_interval: 30s
    static_configs:
     - targets: ['10.102.34.231:80']
<!--NeedCopy-->
```

Fügen Sie Prometheus als Datenquelle in Grafana hinzu

Wenn Sie Metriken mithilfe von Grafana-Dashboards visualisieren möchten, müssen Sie Prometheus als Datenquelle in Grafana hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Prometheus als Datenquelle in Grafana.

Erstellen Sie die Visualisierung von Metriken in Grafana

Sie können ein Grafana-Dashboard erstellen und die wichtigsten Kennzahlen und den entsprechenden Visualisierungstyp auswählen.

Das folgende Verfahren zeigt, wie Sie dem Grafana-Bedienfeld eine Metrik hinzufügen und ein Beispiel für ein Visualisierungs-Dashboard erstellen.

1. Geben Sie den Titel des Panels an.
2. Geben Sie auf der Registerkarte Abfrage für die Abfrage A die erforderliche Metrik an.
3. Wählen Sie auf der Registerkarte Einstellungen den Visualisierungstypaus.

Sie können die Daten und ihre Darstellung in Grafana ändern. Weitere Informationen finden Sie in der Grafana-Dokumentation.

Im Folgenden finden Sie ein Beispiel für ein Grafana-Dashboard mit einigen NetScaler-Metriken:

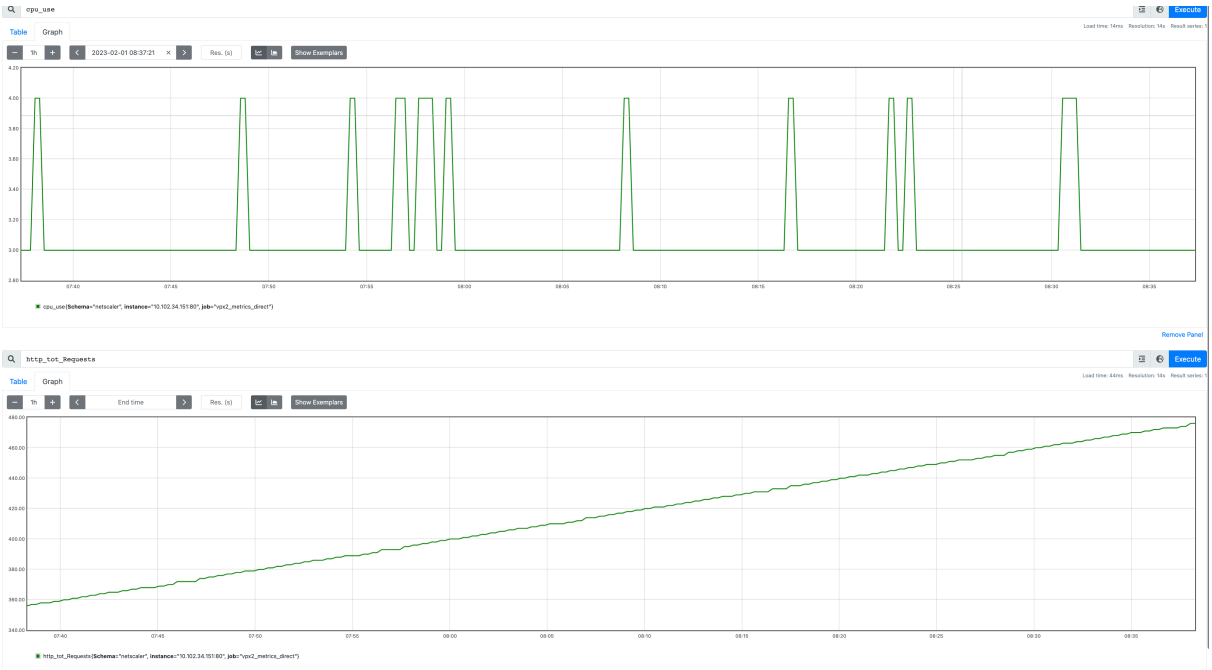
In diesem Dashboard sehen Sie Grafiken für verschiedene NetScaler-Metriken wie:

- `vsvr_tot_Hits`: Zeigt die Anzahl der vom virtuellen Server empfangenen Anfragen an.
- `cc_cpu_use`: Zeigt den Prozentsatz der CPU-Auslastung an.
- `http_tot_Requests`: Zeigt empfangene HTTP-Anfragen an.
- `serv_tot_serviced`: Zeigt an, dass die Anfrage bearbeitet wird.
- `mem_cur_used_size`: Zeigt den aktuell verwendeten Speicher der NetScaler Appliance an.

Beispiele für Prometheus-Grafiken

Mit dem Prometheus-Expressionsbrowser können Sie die vom Prometheus-Server gesammelten Zeitreihenmetriken anzeigen. Sie können auf den Expressionsbrowser zugreifen, indem Sie `prometheu-server-ip-address/graph` in Ihrem Browser auf zeigen. Sie können einen Ausdruck eingeben und das Ergebnis entweder als Tabelle oder als Grafik im Zeitverlauf sehen. Geben Sie an, welche genaue Metrik Sie anzeigen möchten, indem Sie den Namen der Metrik in das Feld Ausdruck eingeben. Sie können mehrere Zähler mithilfe verschiedener Bedienfelder angeben.

Das folgende Diagramm zeigt Prometheus-Diagramme für zwei NetScaler-Metriken `cpu_use` und `http_tot_requests`.



Beispiel für ein Grafana-Armaturenbrett

Sie können die Beispiel-Dashboards von der NetScaler-Downloadseite herunterladen.

Im Folgenden finden Sie ein Beispiel für ein Grafana-Dashboard mit der Option, die verschiedenen Metriken der gesamten Infrastruktur an einem Ort anzuzeigen, z. B. den NetScaler-Status, den Status des virtuellen Servers, den Anwendungsstatus (HTTP- und TCP-Apps) und die Anwendungssicherheit (SSL-Apps).

Sie können den entsprechenden Abschnitt im Dashboard erweitern, um die detaillierte Visualisierung

der einzelnen Abschnitte wie HTTP-Apps, SSL-Apps, TCP-Apps, virtuelle Serverstatistiken (vStats) und NetScaler-Statistiken anzuzeigen.

Das folgende Diagramm zeigt ein Beispiel für ein Grafana-Dashboard mit erweiterten NetScaler-Statistiken:

Weitere Informationen

Schema mit den erforderlichen NetScaler-Zählern für den Export

Metrics Collector exportiert die in der konfigurierten Schemadatei vorhandenen Zähler. Die `/var/metrics_conf/schema.json` Datei ist die Standardschemadatei, die im Analyseprofil konfiguriert ist.

Die Schemadatei ist eine Liste von Entitätstypen und zugehörigen Zählern. Im Schema sind alle Zähler auf globaler Ebene oder auf Systemebene nach dem Entitätstyp gruppiert. `netscaler` Einige der globalen Zähler sind die CPU-Auslastung (`cpu_use`), die Verwaltungs-CPU-Auslastung (`mgmt_cpu_use`) und die Gesamtzahl der empfangenen HTTP-Anfragen (`http_tot_Requests`). Die spezifischen Leistungsindikatoren für Dienstgruppen, `lbvservercsvserver`, usw. sind unter den jeweiligen Entitätstypen aufgeführt.

Im Folgenden finden Sie ein Beispiel für Zähler in der `schema.json` Datei für die virtuelle Authentifizierungsserver (`vserver_authn`) -Entität.

```
1 "vserver_authn":
2   [
3       {
```



```
"name":"si_tot_Requests","rate":"True" }
,
     {
"name":"si_tot_Responses","rate":"True" }
,
     {
"name":"si_tot_RequestBytes","rate":"True" }
,
     {
"name":"si_cur_state","rate":"False" }
,
     {
"name":"si_tot_ResponseBytes","rate":"True" }
,
     {
"name":"si_peer_port","rate":"True" }
,
     {
"name":"vsvr_Protocol","rate":"False" }

 ]
```

In der folgenden Tabelle werden die in diesem Beispiel genannten Leistungsindikatoren erläutert:

Indikatorname	Beschreibung
si_tot_Requests	Gesamtzahl der auf diesem Dienst oder virtuellen Server eingegangenen Anfragen.
si_tot_Responses	Gesamtzahl der auf diesem Dienst oder virtuellen Server eingegangenen Antworten.
si_tot_RequestBytes	Gesamtzahl der auf diesem Dienst oder virtuellen Server empfangenen Anforderungsbytes.
si_cur_state	Aktueller Status des virtuellen Servers.
si_tot_ResponseBytes	Gesamtzahl der auf diesem Dienst oder virtuellen Server empfangenen Antwortbytes.
si_peer_port	Der Port, auf dem der Dienst ausgeführt wird.
vsvr_Protocol	Mit dem virtuellen Server verknüpftes Protokoll.

Das `rate` Feld kann so eingestellt werden, als `True` ob der Zinswert eines Zählers exportiert werden muss. Beispielsweise wird die Rate von `si_tot_Requests` exportiert, wenn `rate` auf `True` für `si_tot_Requests` festgelegt ist.

Im Folgenden finden Sie ein Beispiel für Zähler der `netscaler` Entität.

```
 "netscaler":
   [
        {
"name":"cpu_use","rate":"False" }
,
        {
"name":"mgmt_cpu_use","rate":"False" }
,
        {
"name":"tcp_tot_rxpkts","rate":"True" }
,
        {
"name":"tcp_tot_rxbytes","rate":"True" }
,
        {
"name":"tcp_tot_txpkts","rate":"True" }
,
        {
"name":"tcp_tot_txbytes","rate":"True" }
,
        {
"name":"tcp_cur_ClientConnEst","rate":"False" }
,
        {
"name":"tcp_cur_ServerConnEst","rate":"False" }
,
        {
"name":"tcp_cur_ClientConn","rate":"False" }
,
        {
"name":"tcp_cur_ClientConnClosing","rate":"False" }
,
        {
"name":"tcp_tot_ClientOpen","rate":"True" }
,
        {
"name":"tcp_cur_ServerConn","rate":"False" }
,
        {
```



```
"name":"tcp_cur_ServerConnClosing","rate":"False" }
,
        {
"name":"http_tot_Requests","rate":"True" }
,
        {
"name":"http_tot_Responses","rate":"True" }
,
        {
"name":"http_tot_Gets","rate":"True" }
,
        {
"name":"http_tot_Posts","rate":"True" }
,
        {
"name":"http_tot_Others","rate":"True" }
,
   ]
```

In der folgenden Tabelle werden die in diesem Beispiel genannten Leistungsindikatoren erläutert:

Indikatorname	Beschreibung
cpu_use	Zeichnet die prozentuale CPU-Auslastung auf (CPU-Auslastungsprozentsatz * 10).
tcp_tot_rxpkts	Empfangene TCP-Pakete.
tcp_tot_rxbytes	Empfangene Byte an TCP-Daten.
tcp_tot_txpkts	TCP-Pakete wurden übertragen.
tcp_tot_txbytes	Byte an übertragenen TCP-Daten.
tcp_cur_ClientConnEst	Aktuelle Client-Verbindungen befinden sich im Status Established, was darauf hinweist, dass eine Datenübertragung zwischen der NetScaler-Appliance und dem Client stattfinden kann.
tcp_cur_ServerConnEst	Aktuelle Serververbindungen befinden sich im Status Etabliert, was darauf hinweist, dass eine Datenübertragung zwischen der NetScaler-Appliance und dem Server stattfinden kann.

Indikatorname	Beschreibung
tcp_cur_ClientConn	Client-Verbindungen, einschließlich Verbindungen im Status „Öffnet“, „Aufgebaut“ und „Wird geschlossen“. Serververbindungen, einschließlich Verbindungen im Status Wird geöffnet, hergestellt und geschlossen.
tcp_cur_ClientConnClosing	Client-Verbindungen im Status „Beenden“, was darauf hinweist, dass der Verbindungsabbruch zwar eingeleitet, aber noch nicht abgeschlossen ist.
tcp_cur_ServerConn	Serververbindungen, einschließlich Verbindungen im Status Wird geöffnet, hergestellt und geschlossen.
tcp_cur_ServerConnClosing	Serververbindungen im Status „Beenden“, was darauf hinweist, dass der Verbindungsabbruch zwar eingeleitet, aber noch nicht abgeschlossen ist.
http_tot_Requests	Dieser Zähler verfolgt HTTP-Anfragen, die mit der GET-Methode empfangen wurden.
http_tot_Responses	Dieser Zähler verfolgt HTTP-Anfragen, die mit der POST-Methode empfangen wurden.
http_tot_Gets	Dieser Zähler verfolgt HTTP-Anfragen, die mit der GET-Methode empfangen wurden.
http_tot_Posts	Dieser Zähler verfolgt empfangene HTTP-Anfragen.
http_tot_Others	Dieser Zähler verfolgt HTTP-Anfragen, die mit anderen Methoden als GET und POST empfangen wurden.

Im Folgenden finden Sie ein Beispiel für Zähler der vserver_ssl Entität.

```
"vserver_ssl":
[
    {
 "name":"ssl_ctx_tot_session_hits","rate":"True" }
 ,
    {
 "name":"ssl_ctx_tot_session_new","rate":"True" }
```



```
8   ,
9      {
10  "name":"ssl_ctx_tot_enc_bytes","rate":"True" }
11  ,
12     {
13  "name":"ssl_ctx_tot_dec_bytes","rate":"True" }
14  ,
15 ]
```

In der folgenden Tabelle werden die in diesem Beispiel genannten SSL-Zähler erläutert:

Indikatorname	Beschreibung
ssl_ctx_tot_session_hits	Dieser Zähler verfolgt die Anzahl der Sitzungszugriffe.
ssl_ctx_tot_session_new	Dieser Zähler verfolgt die Anzahl der neu erstellten Sitzungen.
ssl_ctx_tot_enc_bytes	Dieser Zähler verfolgt die Anzahl der verschlüsselten Bytes pro virtuellem SSL-Server.
ssl_ctx_tot_dec_bytes	Dieser Zähler verfolgt die Anzahl der Byte, die pro virtuellem SSL-Server entschlüsselt wurden.

Konfigurieren Sie den schreibgeschützten Prometheus-Zugriff für einen Nicht-Superuser

Gehen Sie wie folgt vor, um den schreibgeschützten Prometheus-Zugriff für einen Nicht-Superuser zu konfigurieren.

1. Fügen Sie der NetScaler Appliance einen neuen Benutzer hinzu.

   ```
   add system user <ns_user_name> <ns_user's_password> -externalAuth
       enabled -promptString user-%u-at-%T logging enaBLED
   ```

   Beispiel:

   ```
   add system user nspaul nspaul -externalAuth enabled -promptString
       user-%u-at-%T logging enaBLED
   ```

2. Erstellen Sie eine Befehlsrichtlinie für einen Benutzer, der nur Lesezugriff hat. Diese Befehlsrichtlinie ermöglicht den schreibgeschützten Zugriff von jeder Datei unter dem `/var/nslog/ directory`.


```
add system cmdPolicy read-only-prometheus ALLOW "(^man.*)|(^show\\s+(?!system)(?!configstatus)(?!ns ns\\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!techsupport).*)|(^stat.*)|(show system file .* -filelocation \"/var/nslog\")"
```

3. Wenn Metriken nur in eine bestimmte Datei geschrieben werden, können Sie den Benutzerzugriff sogar so einschränken, dass sie nur diese bestimmte Datei abrufen können.

```
add system cmdPolicy read-only-prometheus ALLOW "(^man.*)|(^show\\s+(!system)(!configstatus)(!ns ns\\.conf)(!ns savedconfig)
(!ns runningConfig)(!gslb   runningConfig)(!audit messages)(!techsupport).*)|(^stat.*)
|(show system file metrics_prom_<name_of_timeseries_profile>.log -filelocation \"/var/nslog\")"
```

> **Hinweis:**
>
> Geben Sie im `show system file` Befehl den Namen des Zeitreihenprofils an, das Sie anstelle von konfiguriert haben `name_of_ timeseries_profile`.

4. Binden Sie einen Benutzer an die Befehlsrichtlinie.

```
bind system user <userName> ((<policyName> <priority>) | -partitionName <string>)
```

Zum Beispiel:

```
bind system user user1 read-only-prometheus 0
```

Verwenden Sie die folgenden Befehle, um einen Benutzer aus der Befehlsrichtlinie zu entbinden und ihn aus der Befehlsrichtlinie zu entfernen:

1. Entbindet einen konfigurierten Benutzer von der Systembefehlsrichtlinie.

```
unbind system user <userName> (<policyName> | -partitionName <string>
```

Beispiel:

```
unbind system user user1 read-only-prometheus
```

2. Entfernen Sie den Befehl Policy aus NetScaler.

```
rm system cmdPolicy read-only-prometheus
```


Abonnement von Zählern für mehrere Zeitreihenprofile

Jetzt unterstützt NetScaler die Erstellung mehrerer Zeitreihenprofile und spezifiziert für jedes Profil unterschiedliche Zähler. Außerdem können Sie nur die Zähler exportieren, die Ihren Anforderungen entsprechen.

Sie müssen mehrere `schema.json` Dateien erstellen, die die erforderlichen Zähler mit eindeutigen Namen und der `.json` Erweiterung enthalten, um mehrere Zeitreihenprofile zu konfigurieren. Eine Referenzschemadatei `reference_schema.json` ist unter dem Pfad `/var/metrics_conf/` für Ihre Referenz verfügbar.

Die Konfiguration der beiden neuen Zeitreihenprofile sieht wie folgt aus:

```
add analytics profile ns_analytics_timeseries_profile_1   -type
    timeseries -schemaFile schema1.json

set analytics profile  ns_analytics_timeseries_profile_1 -outputMode
    prometheus -serveMode PULL -metrics ENABLED

add analytics profile ns_analytics_timeseries_profile_2   -type
    timeseries -schemaFile schema2.json

set analytics profile  ns_analytics_timeseries_profile_2 -outputMode
    prometheus -serveMode PULL -metrics ENABLED
```

In diesem Beispiel haben `schema1.json` und `schema2.json` unterschiedliche Zählersätze.

Prometheus-Konfiguration

Die Konfiguration einer `prometheus.yml` Beispieldatei sieht wie folgt aus:

```
scrape_configs:
  - job_name: 'vpx2_metrics_direct'
    metrics_path: /nitro/v1/config/systemfile
    params:
      args: ['filename:metrics_prom_ns_analytics_time_series_profile.
          log,filelocation:/var/nslog']
      format: ['prometheus']
    basic_auth:
     username: 'prom_user'
     password: 'user_password'
    scheme: https
    scrape_interval: 30s
    static_configs:
     - targets: ['<ADC1-ip>:<port>', '<ADC2-ip>:<port>']
```



```
<!--NeedCopy-->
```

Exportieren von Auditprotokollen und Ereignissen direkt von NetScaler nach Splunk

September 1, 2023

Mithilfe der Prüfprotokollierung können Sie die NetScaler-Zustände und Statusinformationen protokollieren, die von verschiedenen Modulen in NetScaler gesammelt wurden. Durch die Überprüfung der Protokolle können Sie Probleme oder Fehler beheben und beheben.

Sie können jetzt Audit-Logs und Ereignisse von NetScaler auf branchenübliche Log-Aggregator-Plattformen wie Splunk exportieren und so aussagekräftige Erkenntnisse gewinnen.

Es gibt mehrere Möglichkeiten, Audit-Logs von NetScaler nach Splunk zu exportieren. Sie können Splunk entweder als Syslog-Server oder als HTTP-Server konfigurieren. Dieses Thema enthält Informationen zur Konfiguration von Splunk als HTTP-Server mithilfe des Splunk HTTP Event Collectors. Mit dem HTTP-Event-Collector können Sie Audit-Logs über HTTP (oder HTTPS) direkt von Ihrem NetScaler an die Splunk-Plattform senden.

Konfigurieren Sie den Export von Auditprotokollen von NetScaler nach Splunk

Um den Export von Audit-Logs zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Konfigurieren Sie den HTTP-Event-Collector auf Splunk.
2. Erstellen Sie einen Collector-Service und ein Zeitreihenanalyseprofil auf NetScaler.

HTTP-Event-Collector auf Splunk konfigurieren

Sie können Audit-Logs an Splunk weiterleiten, indem Sie einen HTTP-Event-Collector konfigurieren.

Informationen zur Konfiguration des HTTP-Event-Collectors finden Sie in der Splunk-Dokumentation .

Nachdem Sie den HTTP-Event-Collector konfiguriert haben, kopieren Sie das Authentifizierungstoken und speichern Sie es als Referenz. Sie müssen dieses Token bei der Konfiguration des Analyseprofils auf NetScaler angeben.

Konfigurieren Sie das Zeitreihenanalyseprofil auf NetScaler

Gehen Sie wie folgt vor, um NetScaler-Audit-Logs nach Splunk zu exportieren.

1. Erstellen Sie einen Collector-Service für Splunk.

```
add service <collector> <splunk-server-ip-address> <protocol> <
    port>
```

Beispiel:

```
add service splunk_service 10.102.34.155 HTTP 8088
```

In dieser Konfiguration:

- `ip-address`: Geben Sie die IP-Adresse des Splunk-Servers an.
- `collector-name`: Geben Sie den Kollektor an.
- `protocol`: Geben Sie das Protokoll als HTTP oder HTTPS an
- `port`: Geben Sie die Portnummer an.

2. Erstellen Sie ein Zeitreihenanalyseprofil.

```
1    add analytics profile <profile-name> -type time series -
        auditlog enabled -collectors <collector-name>  -
        analyticsAuthToken <"auth-tocken">
2    -analyticsEndpointContentType <"Application/json"> -
        analyticsEndpointMetadata <"meta-data-for-endpoint:"> -
        analyticsEndpointUrl <"endpoint-url">
```

Beispiel:

```
1    add analytics profile audit_profile -type timeseries -auditlog
         enabled -collectors splunk -analyticsAuthToken "
        1234-5678-12345" -analyticsEndpointContentType "Application
        /json" -analyticsEndpointMetadata "Event:" -
        analyticsEndpointUrl "/services/collector/event"
```

In dieser Konfiguration:

- `auditlog`: Geben Sie den Wert an, `enabled` um die Überwachungsprotokollierung zu aktivieren.
- `analyticsAuthToken`: Geben Sie das Authentifizierungstoken an, das beim Senden von Protokollen an Splunk im Autorisierungsheader enthalten sein soll. Dieses Token ist das Authentifizierungstoken, das auf dem Splunk-Server bei der Konfiguration des HTTP-Event-Collectors erstellt wurde.
- `analyticsEndpointContentType`: Geben Sie das Format der Protokolle an.
- `analyticsEndpointMetadata`: Geben Sie die endpunktspezifischen Metadaten an.

- `analyticsEndpointUrl`: Geben Sie den Speicherort auf dem Endpunkt für den Export von Protokollen an.

> **Hinweis:**
>
> Sie können die Parameter des Zeitreihenanalyseprofils mithilfe des `set analytics profile` Befehls ändern.

3. Überprüfen Sie die Konfiguration des Analytics-Profils mit dem Befehl show analytics profile.

```
# show analytics profile audit_profile

1)    Name: audit_profile
      Collector: splunk
      Profile-type: timeseries
            Output Mode: avro
            Metrics: DISABLED
              Schema File: schema.json
              Metrics Export Frequency: 30
            Events: DISABLED
            Auditlog: ENABLED
            Serve mode: Push
       Authentication Token: <auth-token>
       Endpoint URL: /services/collector/event
       Endpoint Content-type: Application/json
       Endpoint Metadata: Event:
       Reference Count: 0
```

Sobald die Konfiguration erfolgreich ist, werden die Audit-Logs als HTTP-Payloads an Splunk gesendet und Sie können sie auf der Benutzeroberfläche der Splunk-Anwendung einsehen.

Konfigurieren Sie den Export von Ereignissen von NetScaler nach Splunk

Um den Export von Ereignissen von NetScaler nach Splunk zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Konfigurieren Sie den HTTP-Event-Collector auf Splunk, indem Sie den Schritten unter HTTP-Event-Collector auf Splunk konfigurierenfolgen.
2. Erstellen Sie mit dem folgenden Befehl einen Collector-Dienst auf NetScaler.

```
add service <collector> <splunk-server-ip-address> <protocol> <
   port>
```

Beispiel:


```
add service splunk_service 10.102.34.155 HTTP 8088
```

In dieser Konfiguration:

- `ip-address`: Geben Sie die IP-Adresse des Splunk-Servers an.
- `collector-name`: Geben Sie den Kollektor an.
- `protocol`: Geben Sie das Protokoll als HTTP oder HTTPS an.
- `port`: Geben Sie die Portnummer an.

3. Erstellen Sie mit dem Befehl ein Zeitreihenanalyseprofil auf NetScaler. `add analytics profile` Sie müssen die `-events enabled` Option bei der Erstellung des Analyseprofils angeben, um die Exportereignisse zu aktivieren.

   Beispiel:

```
add analytics profile event_profile -type timeseries -events
    enabled -collectors splunk -analyticsAuthToken "1234-5678-12345
    " -analyticsEndpointContentType "Application/json" -
    analyticsEndpointMetadata "Event:" -analyticsEndpointUrl "/
    services/collector/event"
```

4. Überprüfen Sie die Konfiguration des Analyseprofils mit dem `show analytics profile` Befehl.

```
# show analytics profile event_profile

1)    Name: event_profile
      Collector: splunk
      Profile-type: timeseries
            Output Mode: avro
            Metrics: DISABLED
              Schema File: schema.json
              Metrics Export Frequency: 30
            Events: ENABLED
            Auditlog: DISABLED
            Serve mode: Push
       Authentication Token: <auth-token>
       Endpoint URL: /services/collector/event
       Endpoint Content-type: Application/json
       Endpoint Metadata: Event:
       Reference Count: 0
```


Prioritäts-Lastausgleich

May 11, 2023

Mit der Funktion für den Prioritätslastenausgleich können Sie jedem der Dienste oder Dienstgruppen, die an einen virtuellen Server für den Prioritätslastausgleich gebunden sind, eine Prioritätsnummer zuweisen. Ein Dienst oder eine Dienstgruppe mit der niedrigsten Nummer hat die höchste Priorität. Der Anwendungsdatenverkehr wird nur an diesen Dienst oder eine Dienstgruppe verteilt, solange dieser Dienst oder die Dienstgruppe aktiv ist. Der Dienst oder die Dienstgruppe, dem die nächste Prioritätsnummer zugewiesen wurde, wird erst betriebsbereit, wenn alle Dienste oder Mitglieder der Dienstgruppe mit der höchsten Priorität NICHT verfügbar sind. Wenn jedoch einer der Dienste oder ein Mitglied der Dienstgruppe mit der höchsten Priorität wieder verfügbar wird, wird der Datenverkehr an diesen Dienst oder die Dienstgruppe umgeleitet.

Stellen Sie sich zum Beispiel die Dienstgruppen SVG1, SVG2 und SVG3 vor, die an einen virtuellen Server für den Prioritätslastausgleich gebunden sind. Die maximale Anzahl von Prioritätsgruppen ist auf drei festgelegt. Sie weisen jeder Gruppe die Priorität wie folgt zu:

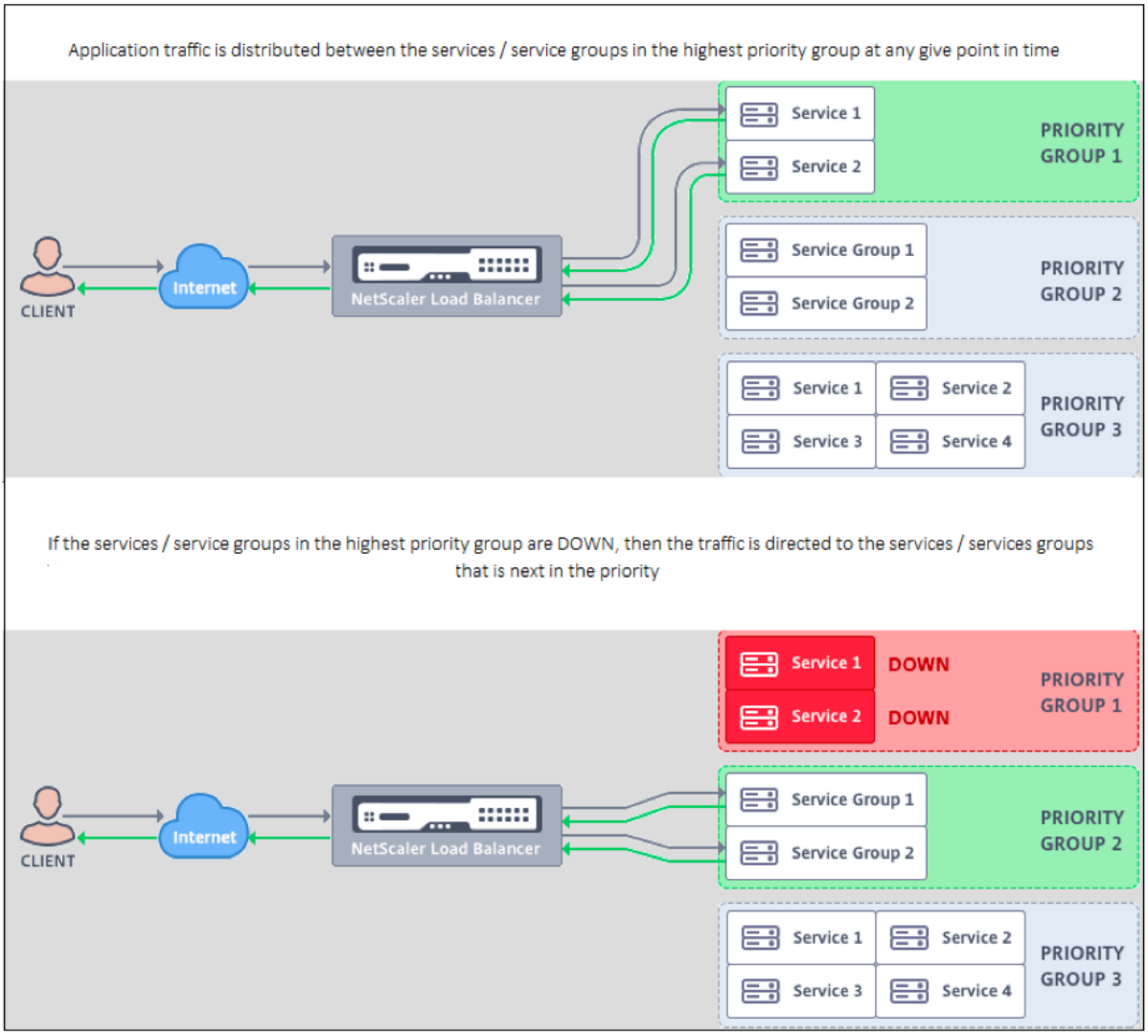
- SVG1 — Priorität 1
- SVG2 — Priorität 2
- SVG3 — Priorität 3

In diesem Szenario wird der Anwendungsdatenverkehr an die Dienstgruppe SVG1 weitergeleitet, da dieser Gruppe die Nummer mit der niedrigsten Priorität zugewiesen wird. Wenn alle Mitglieder in SVG1 DOWN sind, wird der Datenverkehr an die Dienstgruppe SVG2 verteilt, da dieser Gruppe die nächsthöhere Prioritätsnummer zugewiesen wird. Wenn alle Mitglieder in SVG2 ebenfalls DOWN sind, wird der Verkehr an SVG3 verteilt. Wenn jedoch eines der Mitglieder in SVG1 UP ist, wird der Datenverkehr zu SVG1 umgeleitet, da SVG1 die niedrigste Nummer zugewiesen wird und die höchste Priorität hat.

Sie können einem Dienst oder einer Dienstgruppe eine Priorität zuweisen, um den spezifischen Dienst oder die Dienstgruppe mit der höchsten Priorität zu aktualisieren, wann immer dies erforderlich ist, ohne dass sich dies auf den Produktionsverkehr auswirkt.

Wenn das Upgrade nicht erfolgreich ist, können Sie außerdem problemlos zu dem Dienst oder der Dienstgruppe wechseln, der in der Prioritätsstufe als Nächstes an erster Stelle steht, und das mit minimalen oder gar keinen Auswirkungen auf den Produktionsverkehr.

Die folgende Abbildung zeigt die Funktion zum Prioritätslastausgleich.



Priority Load Balancing konfigurieren

> **Hinweis**
>
> Die NetScaler Priority Load Balancing-Konfiguration wird nur über die GUI unterstützt. Sie können den Priority-Load-Balancing nicht mithilfe der CLI konfigurieren.

1. Navigieren Sie zu **Traffic Management** > **Priority Load Balancing**> **Virtual*Servers** und geben Sie das Protokoll für den virtuellen Server, die IP-Adresse und die Portnummer des virtuellen Servers an.
2. Geben Sie im Feld **Maximale Prioritätsgruppen** die Anzahl der Prioritätsdienste oder der Dienstgruppen ein, die an diesen virtuellen Server gebunden werden können. Der Standardwert ist 2, und die maximale Priorität, die festgelegt werden kann, ist 10. Dieser Parameter kann nach der Konfiguration nicht bearbeitet werden.

Hinweis:

Nachdem Sie die maximale Anzahl von Prioritätsgruppen angegeben und auf **OK**geklickt haben, werden ein virtueller Content Switching-Server und eine „n“ Anzahl von virtuellen Backup-Load-Balancing-Servern erstellt. Das Alphabet „n“ steht für die maximale Anzahl von Prioritätsgruppen.

Wenn Sie beispielsweise den Namen des virtuellen Servers als vs1 eingegeben und die maximale Prioritätsgruppe auf 5 festgelegt haben, werden ein virtueller Content-Switching-Server mit dem Namen `_Pri.LB##vs1##MaxPri=5` und den folgenden 5 virtuellen Lastausgleichsservern erstellt.

- `_Pri.LB##vs1##MaxPri=5_LB1`
- `_Pri.LB##vs1##MaxPri=5_LB2`
- `_Pri.LB##vs1##MaxPri=5_LB3`
- `_Pri.LB##vs1##MaxPri=5_LB4`
- `_Pri.LB##vs1##MaxPri=5_LB5`

3. Nachdem Sie die maximale Anzahl von Prioritätsgruppen angegeben und auf **OK**geklickt haben, werden Sie aufgefordert, die Dienste oder Dienstgruppen auszuwählen, die an diesen virtuellen Content Switching-Server gebunden sein müssen.

   - Um Dienste an den virtuellen Server zu binden, klicken Sie im Abschnitt Dienste auf **Einfügen** . Wählen Sie anschließend entweder einen vorhandenen Dienst aus oder erstellen Sie einen Dienst und legen Sie die Priorität für diesen Dienst fest. Legen Sie außerdem die Prioritätsnummer fest, an die dieser Dienst gebunden sein muss.
   - Um Dienstgruppen an den virtuellen Server zu binden, klicken Sie im Abschnitt Dienstgruppen auf **Einfügen** . Wählen Sie als Nächstes entweder eine vorhandene Dienstgruppe aus oder erstellen Sie eine Dienstgruppe und legen Sie die Priorität für diese Dienstgruppe fest. Legen Sie außerdem die Prioritätsnummer fest, an die diese Dienstgruppe gebunden sein muss.

   Wiederholen Sie Schritt 3, abhängig von der maximalen Anzahl von Prioritätsgruppen, die Sie eingegeben haben.

   Hinweis:

   - Der Dienst oder die Dienstgruppe mit der höchsten Priorität ist an den virtuellen Lastausgleichsserver gebunden, der die höchste Priorität hat.

   Wenn Sie beispielsweise Dienstgruppen die Priorität 1 `SG_App1 and SG_App2` bzw. 2 zugewiesen haben, `SG_App1` ist dies an `virtual server _Pri.LB##vs1##MaxPri=5_LB1 and SG_App2` ist dazu verpflichtet `virtual server _Pri.LB##vs1##MaxPri=5_LB2` in Schritt 2 erstellt.

   - Um die Priorität der Dienstgruppe oder des Dienstes zu ändern, klicken Sie auf der Seite

Priority Load Balancing Virtual Server auf das Bearbeitungssymbol und ändern Sie die Priorität nach Bedarf.

- Sie können die Lastausgleichsmethoden und die Persistenz für jeden virtuellen Server nicht explizit festlegen, da die Konfiguration aller virtuellen Lastausgleichsserver identisch ist.

4. Füllen Sie in den Abschnitten Erweiterte Einstellungen die andere Konfiguration aus, die Ihren Anforderungen entspricht.

> **Wichtig:**
>
> Die Entitäten, die während der Priority Load Balancing-Konfiguration erstellt wurden, dürfen nicht von anderen Tabs in der GUI und auch von der CLI aus geändert werden. Es wird empfohlen, die Prioritäts-Load Balancing-Entitäten nur über die Registerkarte Priority Load Balancing zu ändern.

NetScaler Erweiterungen

May 11, 2023

NetScaler-Erweiterungen können verwendet werden, um eine NetScaler-Appliance anzupassen, indem Erweiterungscode geschrieben wird. Derzeit werden Richtlinienerweiterungen und Protokollerweiterungen unterstützt. Richtlinienerweiterungen können verwendet werden, um die Richtliniensprache zu erweitern. Protokollerweiterungen können verwendet werden, um Unterstützung für benutzerdefinierte Protokolle auf einer NetScaler-Appliance hinzuzufügen.

NetScaler-Erweiterungen werden auch auf NetScaler CPX unterstützt.

Dieses Dokument enthält die folgenden Informationen:

- NetScaler Extensions — Sprachübersicht
- NetScaler Extensions — Bibliotheksreferenz
- NetScaler Extensions API-Referenz
- Protokollerweiterungen
- Richtlinienerweiterungen

NetScaler-Erweiterungen - Sprachübersicht

May 11, 2023

Die Erweiterungssprache basiert auf der Programmiersprache Lua 5.2. Lua bietet eine kompakte Ausführungsengine mit guter Leistung, die für die Einbettung in C-Programme wie NetScaler-Software

konzipiert ist.

Die Erweiterungssprache wird dynamisch typisiert, was bedeutet, dass jedes Objekt seine eigenen Typinformationen enthält. Jede Variable kann während der Ausführung jederzeit einen beliebigen Typ enthalten, daher werden Variablentypen nicht deklariert.

Die Sprache ist auch eine freie Form, bei der Leerzeichen zwischen Tokens ignoriert werden. Anweisungen können durch Semikolons getrennt werden, aber das ist nicht erforderlich und wird normalerweise nicht durchgeführt. Blöcke von Anweisungen werden in der Regel am Ende beendet. Blöcke wie das {und} in C oder Java stehen nicht in Klammern.

Identifikatoren sind Buchstabenfolgen (a bis z und A bis Z), Ziffern (0 bis 9) und Unterstrichen (_), die nicht mit einer Ziffer beginnen. Bei Bezeichnern wird zwischen Groß- und Kleinschreibung unterschieden, sodass var, VAR und Var unterschiedliche Identifikatoren sind.

Kommentare werden mit – begonnen. Alles, was danach kommt, wird bis zum Ende der Zeile ignoriert. Beispiel:

```
-- This is a comment.
```

Einfache Typen

May 11, 2023

Die Sprache erlaubt Werte der folgenden einfachen Typen:

- Zahlen
- Saiten
- Boolesch
- Null
- Andere Typen

Zahlen

Alle Zahlen (gerade Ganzzahlen) werden durch IEEE 754-Fließkommawerte dargestellt. Ganzzahlen bis 2^54 haben exakte Repräsentationen. Numerische Werte können wie folgt dargestellt werden:

- Dezimalzahlen mit und ohne Vorzeichen (Beispiele: 10, -5)
- Reelle Zahlen mit Dezimalstellen (10,5, 3,14159)
- Reelle Zahlen mit Exponenten (1,0e+10)
- Hexadezimalzahlen (0xffff0000)

NetScaler-Richtlinienausdrücke haben drei numerische Typen:

- 32-Bit-Ganzzahlen (num_at)

- 64-Bit-Ganzzahlen (unsigned_long_at)
- 64-Bit-Fließkomma (double_at)

All diese Werte werden in den Zahlentyp umgewandelt, wenn sie an eine Erweiterungsfunktion übergeben werden, und Zahlen werden in den erwarteten numerischen Richtlinientyp konvertiert, wenn sie zurückgegeben werden.

Saiten

Zeichenketten sind Bytefolgen beliebiger Länge. Sie entsprechen dem Policy-Typ **text_at.** Zeichenketten können Null (0x00) Byte enthalten. Beliebige Binärdaten können in Zeichenketten gespeichert werden, einschließlich einer beliebigen Zeichencode-Repräsentation (z. B. UTF-8 und vollständiger Unicode). Zeichenkettenfunktionen **wie string.upper () gehen** jedoch von 8-Bit-ASCII aus.

Zeichenketten werden automatisch zugewiesen, wenn sie verwendet werden. Es ist nicht notwendig (oder gar möglich), explizit Puffer für Zeichenketten zuzuweisen. Zeichenketten werden außerdem automatisch durch die Speicherbereinigung freigegeben, wenn sie nicht mehr verwendet werden. Es ist nicht nötig (oder gar möglich), Zeichenketten explizit freizugeben. Durch diese automatische Zuweisung und Deallokation werden einige häufig auftretende Probleme in Sprachen wie C vermieden, wie Speicherlecks und hängende Zeiger.

Zeichenkettenliterale sind Zeichenketten, die in doppelte oder einfache Anführungszeichen gesetzt sind. Es gibt keinen Unterschied zwischen den beiden Arten von Anführungszeichen: „a string literal“ ist dasselbe wie „a string literal“. Die übliche Maskierung mit umgekehrtem Schrägstrich ist verfügbar:\ s (Glocke),\ b (Rücktaste),\ f (Formularfeed),\ n (Zeilenumbruch),\ t (horizontaler Tabulator),\\ (umgekehrter Schrägstrich),\ “(doppeltes Anführungszeichen) und\ ‘(einfaches Anführungszeichen). Dezimale Bytewerte können durch einen umgekehrten Schrägstrich und eine bis drei Ziffern (\ d,\ dd,\ ddd) eingegeben werden. Hexadezimale Bytewerte können durch einen umgekehrten Schrägstrich, ein X und zwei Hexadezimalzahlen (\ xhh) eingegeben werden

Eine spezielle Syntax, die sogenannte Notation mit langen Klammern, kann für lange, mehrzeilige Zeichenkettenliterale verwendet werden. Diese Notation schließt die Zeichenfolge in doppelte eckige Klammern mit null oder mehr Gleichheitszeichen zwischen den Klammern ein. Die Idee ist, eine Kombination aus Klammern und Gleichungen zu finden, die nicht in der Zeichenfolge enthalten ist. In der Zeichenfolge werden keine Escape-Sequenzen berücksichtigt. Beispiele:

[[Dies ist eine mehrzeilige Zeichenfolge mit langer Klammerschreibweise.]]

[= [Dies ist eine mehrzeilige Zeichenfolge in langer Schreibweise mit [[und]] und einem unesmaskierten Zeichen darin.] =]

Langklammer Notation kann verwendet werden, um einen mehrzeiligen Kommentar zu machen. Beispiel:


```
– [[
Dies ist ein mehrzeiliger Kommentar.
–]]
```

Boolesch

Die üblichen booleschen Werte „wahr“ und „falsch“ werden bereitgestellt. Beachten Sie, dass boolesche Werte sich von Zahlenwerten unterscheiden, im Gegensatz zu C, wo Null als falsch angenommen wird und jeder Wert ungleich Null als wahr angenommen wird.

Null

Null ist ein besonderer Wert, der „kein Wert“ bedeutet. Es ist ein eigener Typ und entspricht keinem anderen Wert, im Gegensatz zu C, wo NULL als Null definiert ist.

Andere Typen

Es gibt zwei weitere Typen, Benutzerdaten und Threads. Dies sind fortgeschrittene Themen und werden hier nicht behandelt.

Variablen

January 19, 2021

Variablen enthalten Werte, die sich während der Ausführung der Erweiterung ändern können. Aufgrund der dynamischen Eingabe kann jede Variable Werte jedes Typs enthalten. Es gibt keine Typdeklarationen für Variablen. Stattdessen wird der Typ einer Variablen zur Laufzeit bestimmt. Tatsächlich kann sich der Typ des Werts einer Variablen während der Ausführung ändern, obwohl dies keine empfohlene Vorgehensweise ist. Eine Variable hat anfänglich den Wert nil.

Variablennamen sind Bezeichner, also Zeichenfolgen aus Buchstaben, Ziffern und Unterstrichen, die nicht in einer Ziffer beginnen. Beispiele: Header, combined_headers.

Globale Variablen

In Lua sind Variablen, die nicht anderweitig deklariert werden, global innerhalb des Programms. Globale Variablen sind jedoch in Richtlinienerweiterungsfunktionen nicht zulässig, da es mehrere Paketmodule gibt, in denen eine Funktion ausgeführt werden kann und jede Packet Engine über einen eigenen Speicher verfügt.

Wenn Sie eine globale Variable in Ihrer Erweiterung verwenden, erhalten Sie einen Laufzeitfehler: Versuchen Sie, eine in **/var/log/ns.log**gemeldete globale Variable zu aktualisieren oder zu erstellen.

Tippfehler in Variablennamen sind ein potenzielles Problem, da die Variable mit dem Tippfehler als eine andere globale Variable interpretiert wird und keinen Syntaxfehler verursacht wie in Sprache wie C oder Java. Wie oben erwähnt, erhalten Sie stattdessen einen Laufzeitfehler.

Lokale Variablen

Eine Variable kann als lokal für einen Anweisungsblock deklariert werden, z. B. eine Funktion. Dies geschieht durch den lokalen Variablennamen. Die Variable wird auf den Block beschränkt, dh sie existiert nur innerhalb des Blocks. Die lokale Deklaration kann der Variablen optional einen Wert zuweisen.

Beispiele:

```
local headers = {}
local combined_headers = {}
```

Ausdrücke

August 19, 2021

Ausdrücke berechnen Werte aus Variablen- und Literalwerten.

- Arithmetische Operationen
- Relationale Vorgänge
- Logische Vorgänge
- Verkettung
- Testdauer
- Rangfolge

Arithmetische Operationen

Arithmetische Operationen werden für Zahlenwerte durchgeführt. Wenn ein Zeichenfolgenwert in einer arithmetischen Operation verwendet wird, wird er in eine Zahl konvertiert — wenn dies fehlschlägt, wird ein Fehler zurückgegeben.

a + b	a und b hinzufügen

a - b	subtrahieren b von a
a * b	multiplizieren a und b
a/b	dividieren a durch b
a% b	modulo = a - math.floor (a/b) *b
a ^ b	a auf die b Kraft erhöhen; b kann eine beliebige Zahl sein
-a	negieren Sie ein

Relationale Vorgänge

Relationale Operationen vergleichen zwei Werte und geben true zurück, wenn die Beziehung erfüllt ist, und false, wenn dies nicht der Fall ist. Relationale Operationen können zwischen Werten eines beliebigen Typs durchgeführt werden. Wenn die Werte nicht vom gleichen Typ sind, wird false zurückgegeben. Zahlen werden auf die übliche Weise verglichen. Strings werden mit der Sortiersequenz für das aktuelle Gebietsschema verglichen.

a == b	a ist gleich b
a ~= b	a ist nicht gleich b
a < b	a ist kleiner als b
a > b	a ist größer als b
a <= b	a ist kleiner oder gleich b
a >= b	a ist größer oder gleich b

Logische Operationen

Logische Operationen werden traditionell für boolesche Werte ausgeführt, aber in dieser Sprache können sie für zwei beliebige Werte ausgeführt werden. nil und false gilt als falsch und jeder andere Wert gilt als wahr. Logische Operationen verwenden eine Kurzschnittauswertung. Wenn der erste Wert das Ergebnis der Operation bestimmt, wird der zweite Wert nicht ausgewertet.

a und b	Wenn a falsch oder nil ist, geben Sie eine else zurück b
a oder b	Wenn a nicht falsch und nicht nil ist, geben Sie eine else zurück b
nicht ein	wenn a nicht falsch oder nil ist, gibt false zurück sonst true zurück

Die Operationen “und” und “oder” können für die bedingte Auswertung innerhalb eines Ausdrucks verwendet werden:

a oder b	kann verwendet werden, um einen Standardwert b bereitzustellen, wenn a nicht initialisiert ist (nil). Dies ist nützlich für optionale Parameter in Funktionen.
a und b oder c	kann verwendet werden, um nicht-nil b oder c basierend auf der Bedingung a zu wählen. Wenn a wahr ist, gibt a und b “b” zurück, und b oder c gibt b zurück. Wenn a falsch ist, dann a und b gibt false zurück oder c gibt c. Dies ist äquivalent zu einem? b: c in der Programmiersprache C.

Verkettung

String-Verkettung ist s1.. s2. Dadurch wird eine neue Zeichenfolge erstellt, die groß genug ist, um den Inhalt von s1 und s2 zu halten, und kopiert den Inhalt in die neue Zeichenfolge. Ein Fehler tritt auf, wenn s1 oder s2 keine Zeichenfolgen sind. Beachten Sie, dass wiederholte Verkettung einen erheblichen Kopieraufwand haben kann. Wenn Sie eine Zeichenfolge von n Bytes erstellen, indem Sie jeweils ein Byte verketten, kopiert dies n* (n+1) /2 Bytes. Für eine bessere Leistung können Sie Teile einer Zeichenfolge, die in eine Tabelle verkettet werden soll (später diskutiert) und dann die Funktion table.concat () verwenden. Ein Beispiel dafür wird im Beispiel COMBINE_HEADERS () gezeigt.

Testdauer

Die Länge eines Strings s wird von #s zurückgegeben. Der Operator # wird auch mit Array-Tabellen verwendet, wie später erläutert.

Rangfolge

Die Operatorpriorität bestimmt die Reihenfolge, in der Operationen in einem Ausdruck ausgeführt werden, wobei Operationen mit höherer Priorität vor denen mit niedrigerer Priorität ausgeführt werden. Die Prioritätsreihenfolge kann wie gewohnt durch Klammern überschrieben werden. Beispielsweise hat in`a + b \* c`, * eine höhere Priorität als +, daher wird der Ausdruck als ausgewertet`a + (b \* c)`.

höchste	^
-	nicht # - (unär)
-	* / %
-	..
-	= ~= < > <= >=
-	und
niedrigste	oder

Operationen mit der gleichen Priorität werden von links nach rechts (links assoziativ) ausgeführt, außer ^ und.., die von rechts nach links ausgeführt werden (rechts assoziativ). Daher wird a^b^c als a^ (b^c) ausgewertet.

Zuweisung

January 19, 2021

Die Zuweisungsanweisung wertet einen Ausdruck aus und weist den resultierenden Wert einer Variablen zu.

```
variable = expression
```

Wie bereits erwähnt, können Werte eines beliebigen Typs jeder Variablen zugewiesen werden, so dass Folgendes erlaubt ist:


```
local v1 = "a string literal"
v1 = 10
```

Eine Zuweisungsanweisung kann tatsächlich mehrere Variablen mit dem Formular

variable1, variable2, … = expression1, expression2, …

Wenn mehr Variablen als Ausdrücke vorhanden sind, werden den zusätzlichen Variablen nil zugewiesen. Wenn mehr Ausdrücke als Variablen vorhanden sind, werden die zusätzlichen Ausdruckswerte verworfen. Die Ausdrücke werden alle vor den Zuweisungen ausgewertet, so dass diese verwendet werden können, um die Werte zweier Variablen prägnant auszutauschen:

v1, v2 = v2, v1

entspricht

tmp = v1
v2 = v1
v1 = tmp

Tabellen

August 19, 2021

Tabellen sind Sammlungen von Einträgen mit Schlüsseln und Werten. Sie sind die einzige aggregierte Datenstruktur zur Verfügung gestellt. Alle anderen Datenstrukturen (Arrays, Listen, Sets usw.) werden aus Tabellen erstellt. Tabellenschlüssel und -werte können beliebig sein, einschließlich anderer Tabellen. Schlüssel und Werte innerhalb derselben Tabelle können Typen mischen.

- Tabellenkonstruktoren
- Tabellenverwendung
- Tabellen als Arrays
- Tabellen als Datensätze

Tabellenkonstruktoren

Mit Tabellenkonstruktoren können Sie eine Tabelle mit Schlüsseln und zugehörigen Werten angeben. Die Syntax lautet:

{[key1] = value1, [key2] = value2, …}

wobei die Schlüssel und Werte Ausdrücke sind. Wenn es sich bei den Schlüsseln um Zeichenfolgen handelt, die keine reservierten Wörter sind, können die Klammern und Anführungszeichen um die Schlüssel weggelassen werden. Beispiel:

{key1 = “value1”, key2 = “value2”, key3 = “value3”}

Eine leere Tabelle wird einfach durch {} angegeben.

Ein Tabellenkonstruktor kann in einer Zuweisung verwendet werden, um eine Variable auf eine Tabelle zu verweisen. Beispiele:

local t1 = {} – set t1 to an empty table
local t2 = {key1 = “value1”, key2 = “value2”, key3 = “value3”}

Beachten Sie, dass Tabellen selbst anonym sind. Mehr als eine Variable kann auf dieselbe Tabelle verweisen. Fortsetzung des obigen Beispiels:

local t3 = t2 — sowohl t2 als auch t3 beziehen sich auf dieselbe Tabelle

Tabellenverwendung

Wie erwartet, können Sie Schlüssel verwenden, um Werte in einer Tabelle zu finden. Die Syntax ist[Tabellenschlüssel], wobei Tabelle eine Tabellenreferenz ist (normalerweise eine Variable, der einer Tabelle zugewiesen wurde), und Schlüssel ist ein Ausdruck, der den Schlüssel bereitstellt. Wenn dies in einem Ausdruck verwendet wird und der Schlüssel in der Tabelle vorhanden ist, wird der Wert zurückgegeben, der dem Schlüssel zugeordnet ist. Wenn sich der Schlüssel nicht in der Tabelle befindet, gibt dies null zurück. Wenn dies als Variable in einer Zuweisung verwendet wird und der Schlüssel nicht in der Tabelle vorhanden ist, wird ein neuer Eintrag für den Schlüssel und den Wert erstellt. Wenn der Schlüssel bereits in der Tabelle vorhanden ist, wird der Wert des Schlüssels durch den neuen Wert ersetzt. Beispiele:

local t = {} — setzt t auf eine leere Tabelle
t[“k1”] = “v1” — erstellt einen Eintrag für den Schlüssel “k1” und den Wert “v1”
v1 = t[“k1”] — setzt v1 auf den Wert für Schlüssel “k1” = “v1”
t[“k1”] = “new_v1” — setzt den Wert für Schlüssel “k1” auf “new_v1”

Tabelle als Arrays

Das traditionelle Array kann mit einer Tabelle mit Integer-Schlüsseln als Indizes implementiert werden. Ein Array kann beliebige Indizes haben, einschließlich negativer, aber die Konvention besteht darin, Arrays am Index 1 zu starten (nicht 0, wie es bei Sprachen wie C und Java der Fall ist). Es gibt einen speziellen Tabellenkonstruktor für solche Arrays:

{value1, value2, value3, … }

Array-Referenzen sind dann[Array-Index].

Der Längenoperator # gibt die Anzahl der Elemente in einem Array mit aufeinanderfolgenden Indizes ab 1. Beispiel:

local a = {“value1”, “value2”, “value3”}
local length = #a – sets length to the length of array a = 3

Arrays können dünn sein, wobei nur die definierten Elemente zugewiesen werden. Aber # kann nicht für ein spärliches Array mit nicht aufeinanderfolgenden Indizes verwendet werden. Beispiel:

local sparse_array = {} — richte ein leeres Array ein
sparse_array[1] = “value1” — füge ein Element bei Index 1
sparse_array[99] = “value99” hinzu — füge ein Element bei Index 99 hinzu

Mehrdimensionale Arrays können als Tabellen von Tabellen eingerichtet werden. Zum Beispiel könnte eine 3x3-Matrix eingerichtet werden durch:

local m = {{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}
lokal v22 = m[2][2] — setzt v22 auf 5

Tabellen als Datensätze

Datensätze mit Feldern können als Tabellen mit Feldnamenschlüsseln implementiert werden. Das Referenzformular table.field kann für die Tabelle[“field”]verwendet werden. Beispiele:

local person = {name = “John Smith”, phone = “777-777-7777”}
local name = person.name – sets name to “John Smith”

Ein Array von Tabellen kann für eine Sequenz von Datensätzen verwendet werden. Beispiel:

local people = {
{name = “John Smith”, phone = “777-777-7777”},
{name = “Jane Doe”, phone = “888-888-8888”}
…
}

name = people[2].name - setzt den Namen auf “Jane Doe”

Steuerungsstrukturen

May 11, 2023

Die Sprache der Erweiterungsfunktion stellt die üblichen Anweisungen zur Steuerung der Programmausführung bereit.

- Wenn dann sonst
- Während, mach und wiederhole bis
- Numerisch für
- Pause

- Goto

Wenn dann sonst

Bei Anweisungen werden Anweisungsblöcke ausgewählt, die auf der Grundlage einer oder mehrerer Bedingungen ausgeführt werden sollen. Es gibt drei Formen:

Wenn dann Formular

```
if expression then
     statements to execute if expression is not false or nil
end
<!--NeedCopy-->
```

Wenn dann sonst Formular

```
if expression then
     statements to execute if expression is not false or nil
else
     statements to execute if expression is false or nil
end
<!--NeedCopy-->
```

Wenn dann elseif sonst Formular

```
if expression1 then
     statements to execute if expression1 is not false or nil
     elseif expression2 then
          statements to execute if expression2 is not false or nil
. . .
else
     statements to execute if all expressions are false or nil
end
<!--NeedCopy-->
```

Beispiel:

```
if headers[name] then

     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value
```



```
5
6  else
7
8       headers[name] = {
9   name .. ":" .. value }
10
11
12 end
13 <!--NeedCopy-->
```

Hinweis:

- Der Ausdruck ist nicht in Klammern eingeschlossen, wie dies in C und Java der Fall ist.
- Es gibt kein Äquivalent zur C/Java-Switch-Anweisung. Sie müssen eine Reihe von if elseif-Anweisungen verwenden, um das Äquivalent zu erreichen.

Während, mach und wiederhole bis

Die Anweisungen **while** und **repeat** stellen Schleifen bereit, die durch einen Ausdruck gesteuert werden.

```
1  while expression do
2       statements to execute while expression is not false or nil
3  end
4
5  repeat
6
7       statements to execute until expression is not false or nil
8
9  until expression
10 <!--NeedCopy-->
```

Beispiel für while:

```
1  local a = {
2   1, 2, 3, 4 }
3
4  local sum, i = 0, 1 -- multiple assignment initializing sum and i
5  while i <= #a do -- check if at the end of the array
6       sum = sum + a[i] -- add array element with index i to sum
7       i = i + 1 -- move to the next element
8  end
9  <!--NeedCopy-->
```

Beispiel für die Wiederholung:


```
sum, i = 0, 1 -- multiple assignment initializing sum and i
repeat
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
until i > #a -- check if past the end of the array
<!--NeedCopy-->
```

Natürlich ist es möglich, eine Schleife zu schreiben, die nicht endet, wenn Sie beispielsweise in einem dieser Beispiele die Anweisung i = i + 1 weglassen. Wenn eine solche Funktion ausgeführt wird, erkennt NetScaler, dass die Funktion nicht innerhalb einer angemessenen Zeit abgeschlossen wurde, und beendet sie mit einem Laufzeitfehler:

```
Cpu limit reached. Terminating extension execution in [[string "function
extension function..."]]: line line-number.
```

wird in /var/log/ns.log gemeldet.

Numerisch für

Es gibt zwei Arten von vier Schleifen. Das erste ist das numerische for, das der üblichen Verwendung der for-Anweisung in C und Java ähnelt. Die numerische Anweisung for initialisiert eine Variable, testet, ob die Variable einen Endwert übergeben hat, und führt andernfalls einen Block von Anweisungen aus, erhöht die Variable und wiederholt sich. Die Syntax für die numerische For-Schleife lautet:

```
for variable = initial, final, increment do

     statements in the loop body

end
<!--NeedCopy-->
```

wobei initial, final und increment alle Ausdrücke sind, die Zahlen ergeben (oder in diese umgewandelt werden können). Variable wird als lokal für den For-Loop-Anweisungsblock betrachtet; sie kann nicht außerhalb der Schleife verwendet werden. Inkrement kann weggelassen werden; der Standardwert ist 1. Die Ausdrücke werden zu Beginn der Schleife einmal ausgewertet. Die Endbedingung ist variabel > final, wenn das Inkrement positiv ist, und variabel < final, wenn das Inkrement negativ ist. Die Schleife wird sofort beendet, wenn das Inkrement 0 ist.

Beispiel (entspricht den Schleifen while und repeat im vorherigen Abschnitt):

```
sum = 0
for i = 1, #a do -- increment defaults to 1
     sum = sum + a[i]
end
```



```
<!--NeedCopy-->
```

Die zweite Art von For-Schleifen ist die generische For-Schleife, die für flexiblere Arten von Schleifen verwendet werden kann. Es beinhaltet die Verwendung von Funktionen, auf die später nach der Einführung der Funktionen eingegangen wird.

Pause

Die Break-Anweisung wird innerhalb einer while-, repeat- oder for-schleife verwendet. Es beendet die Schleife und setzt die Ausführung bei der ersten Anweisung nach der Schleife fort. Beispiel (entspricht auch den vorangegangenen while, repeat und for loops):

```
sum, i = 0, 1
while true do
     if i > #a then
          break
     end
     sum = sum + a[i]
     i = i + 1
end
<!--NeedCopy-->
```

Goto

Die goto-Anweisung kann verwendet werden, um zu einem Label vorwärts oder rückwärts zu springen. Das Label ist ein Bezeichner und seine Syntax lautet: :label::. Die goto-Anweisung lautet gotolabel. Beispiel (entspricht wieder den vorherigen Schleifen):

```
sum, i = 0, 1
::start_loop::
     if i > #a then
          goto end_loop -- forward jump
     end
     sum = sum + a[i]
     i = i + 1
     goto start_loop -- backwards jump
::end_loop::
. . .
<!--NeedCopy-->
```

Es gibt seit langem eine Kontroverse über die Verwendung von Gotos in der Programmierung. Im Allgemeinen sollten Sie versuchen, die anderen Kontrollstrukturen zu verwenden, um Ihre Funktionen

lesbarer und zuverlässiger zu machen. Der gelegentliche umsichtige Einsatz von Gotos kann jedoch zu besseren Programmen führen. Insbesondere Gotos können bei der Behandlung von Fehlern nützlich sein.

Funktionen

May 11, 2023

Funktionen sind ein Grundbaustein der Programmierung - sie sind eine bequeme und leistungsstarke Möglichkeit, Anweisungen zu gruppieren, die eine Aufgabe ausführen. Sie sind die Schnittstelle zwischen der NetScaler-Appliance und dem Erweiterungscode. Für Richtlinien definieren Sie Funktionen zur Richtlinienerweiterung. Für Protokolle implementieren Sie Callback-Funktionen für das Protokollverhalten. Funktionen bestehen aus Funktionsdefinitionen, die angeben, welche Werte in die und aus der Funktion übergeben werden und welche Anweisungen für die Funktion ausgeführt werden, und Funktionsaufrufen, die Funktionen mit bestimmten Eingabedaten ausführen und Ergebnisse aus der Funktion erhalten.

Callback-Funktionen für Protokollverhalten

Das TCP-Clientverhalten besteht aus einer Callback-Funktion (on_data), die TCP-Clientdaten-Stream-Ereignisse verarbeitet. Um Message Based Load Balancing (MBLB) für ein TCP-basiertes Protokoll zu implementieren, können Sie Code für diese Callback-Funktion hinzufügen, um den TCP-Datenstrom vom Client zu verarbeiten und den Byte-Stream in Protokollnachrichten zu analysieren.

Die Callback-Funktionen in einem Verhalten werden mit einem Kontext aufgerufen, bei dem es sich um den Status des Verarbeitungsmoduls handelt. Der Kontext ist die Instanz des Verarbeitungsmoduls. Beispielsweise werden die TCP-Clientverhaltens-Callbacks mit unterschiedlichen Kontexten für verschiedene Client-TCP-Verbindungen aufgerufen.

Zusätzlich zum Kontext können die Verhaltensrückrufe andere Argumente haben. Normalerweise wird der Rest der Argumente als Nutzlast übergeben, was die Sammlung aller Argumente ist. Die Instanzen des programmierbaren Verarbeitungsmoduls können also als eine Kombination aus Instanzstatus und Ereignisrückruffunktionen angesehen werden, dh dem Kontext plus Verhalten. Und der Verkehr fließt durch die Pipeline als Ereignisnutzlast.

Prototyp der TCP-Client-Callback-Funktion:

```

                Function                client on_data (ctxt, payload)

                                                //.code

```



```
                end


<!--NeedCopy-->
```

Hierbei gilt:

- ctxt - Verarbeitungskontext für TCP-Clients
- Nutzlast — Event-Payload
  - payload.data — Empfangene TCP-Daten, verfügbar als Byte-Stream

Funktionen zur Erweiterung von Richtlinien

Da die NetScaler-Richtlinienausdruckssprache typisiert ist, muss die Definition einer Erweiterungsfunktion die Typen ihrer Eingaben und ihren Rückgabewert angeben. Die **Lua-Funktionsdefinition** wurde um folgende Typen erweitert:

```
function self-type: function-name(parameter1: parameter1-type, and so
   on): return-type
     statements
end

<!--NeedCopy-->
```

Hierbei gilt:

Die Typen sind NSTEXT, NSNUM, NSBOOL oder NSDOUBLE.

Selbsttyp ist der Typ des impliziten Selbstparameters, der an die Funktion übergeben wird. Wenn die Erweiterungsfunktion in einem NetScaler-Richtlinienausdruck verwendet wird, ist dies der Wert, der durch den Ausdruck links neben der Funktion generiert wird. Eine andere Möglichkeit, dies zu sehen, besteht darin, dass die Funktion diesen Typ in der NetScaler Richtliniensprache erweitert.

Die Parametertypen sind die Typen jedes Parameters, der im Erweiterungsfunktionsaufruf im Richtlinienausdruck angegeben ist. Eine Erweiterungsfunktion kann null oder mehr Parameter haben.

Rückgabetyp ist der Typ des Werts, der vom Erweiterungsfunktionsaufruf zurückgegeben wird. Es ist die Eingabe für den Teil des Richtlinienausdrucks, falls vorhanden, rechts von der Funktion oder der Wert des Ausdrucksergebnisses.

Beispiel:

```
function NSTEXT:COMBINE_HEADERS(): NSTEXT
```

Verwendung der Erweiterungsfunktion in einem Richtlinienausdruck:

```
HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n").COMBINE_HEADERS()
```


Hier ist der Selbstparameter das Ergebnis von `HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1\r\n")`, bei dem es sich um einen Textwert handelt. Das Ergebnis des Aufrufs COMBINE_HEADERS () ist Text, und da sich rechts von diesem Aufruf nichts befindet, ist das Ergebnis des gesamten Ausdrucks Text.

Lokale Funktionsdefinition

Neben Erweiterungsfunktionen können in einer Erweiterungsdatei keine globalen Funktionen definiert werden. Lokale Funktionen können jedoch innerhalb von Erweiterungsfunktionen mithilfe der normalen Lua-Funktionsanweisung definiert werden. Dies deklariert den Namen der Funktion und die Namen ihrer Parameter (auch als Argumente bekannt) und gibt wie alle Deklarationen in Lua keine Typen an. Die Syntax dafür lautet:

```
local function function-name(parameter1-name, parameter2-name, and so
   on)
     statements
end

<!--NeedCopy-->
```

Die Funktions- und Parameternamen sind alle Bezeichner. (Der Funktionsname ist eigentlich eine Variable und die Funktionsanweisung ist eine Abkürzung für lokale Funktionsname = Funktion (Parameter1 usw.), aber Sie müssen diese Feinheit nicht verstehen, um Funktionen zu verwenden.)

Beachten Sie, dass usw. hier für die Fortsetzung des Musters von Parameternamen anstelle des üblichen… verwendet wird. Dies liegt daran, dass… selbst tatsächlich eine variable Parameterliste bedeutet, auf die hier nicht eingegangen wird.

Funktionskörper und Rückkehr

Der Anweisungsblock zwischen den Funktions- und End-Anweisungen ist der Funktionskörper. Im Funktionskörper wirken die Funktionsparameter wie lokale Variablen, wobei Werte, die von den Funktionsaufrufen geliefert werden, wie zuvor beschrieben.

Die Anweisung return liefert Werte, die an den Aufrufer der Funktion zurückgegeben werden. Es muss am Ende eines Blocks erscheinen (in einer Funktion, wenn dann, for-Schleife usw. Es kann in seinem eigenen Block sein, kehre zurück… end). Es gibt keinen, einen oder mehr als einen Rückgabewert an:

```
return -- returns nil
return expression -- one return value
return expression1, expression2, ... -- multiple return values

<!--NeedCopy-->
```


Beispiele:

```
local function fsum(a)
     local sum = 0
     for i = 1, #a do
          sum = sum + a[i]
     end
     return sum
end

Local function fsum_and_average(a)
     local sum = 0
     for i = 1, #a do
          sum = sum + a[i]
     end
     return sum, sum/#a
end

<!--NeedCopy-->
```

Funktion ruft

Ein Funktionsaufruf führt den Rumpf einer Funktion aus, liefert Werte für ihre Parameter und empfängt Ergebnisse. Die Syntax für einen Funktionsaufruf ist Funktionsname (Ausdruck1, Ausdruck2 usw.), wobei die Funktionsparameter auf die entsprechenden Ausdrücke gesetzt werden. Die Anzahl der Ausdrücke und Parameter muss nicht gleich sein. Wenn es weniger Ausdrücke als Parameter gibt, werden die verbleibenden Parameter auf Null gesetzt. So können Sie am Ende des Aufrufs einen oder mehrere Parameter optional machen, und Ihre Funktion kann überprüfen, ob sie angegeben sind, indem sie prüft, ob sie nicht Null sind. Ein üblicher Weg, dies zu tun, ist die Oderoperation:

```
function f(p1, p2) -- p2 is optional
     p2 = p2 or 0 -- if p2 is nil, set to a default of 0
     . . .
end

<!--NeedCopy-->
```

Wenn es mehr Ausdrücke als Parameter gibt, werden die verbleibenden Ausdruckswerte ignoriert.

Wie bereits erwähnt, können Funktionen mehrere Werte zurückgeben. Diese Rückgaben können in einer Anweisung mit mehreren Zuweisungen verwendet werden. Beispiel:

```
local my_array = {
```



```
 1, 2, 3, 4 }

local my_sum, my_ave = sum_and_average(my_array)

<!--NeedCopy-->
```

Iterator-Funktionen und generische for-Schleifen

Jetzt, da wir Funktionen eingeführt haben, können wir über generische for-Schleifen sprechen. Die Syntax für die generische for-Schleife (mit einer Variablen) lautet:

```
for variable in iterator(parameter1, parameter2, and so on) do
     statements in the for loop body
end

<!--NeedCopy-->
```

Wobei iterator () eine Funktion mit null oder mehr Parametern ist, die bei jeder Iteration des Schleifenkörpers einen Wert für eine Variable liefern. Die Iterator-Funktion verfolgt mithilfe einer Technik namens Closure, wo sie sich in der Iteration befindet, über die Sie sich hier keine Sorgen machen müssen. Es signalisiert das Ende der Iteration, indem es Null zurückgibt. Iteratorfunktionen können mehr als einen Wert zur Verwendung in einer Mehrfachzuweisung zurückgeben.

Das Schreiben einer Iterator-Funktion geht über den Rahmen dieses Papiers hinaus, aber es gibt nur wenige nützliche integrierte Iteratoren, die das Konzept veranschaulichen. Einer ist der Iterator pairs (), der die Einträge in einer Tabelle durchläuft und zwei Werte zurückgibt, den Schlüssel und den Wert des nächsten Eintrags.

Beispiel:

```
local t = {
 k1 = "v1", k2 = "v2", k3 = "v3" }

local a = {
  }
  -- array to accumulate key-value pairs
local n = 0 -- number of key-value pairs
for key, value in pairs(t) do
     n = n + 1
     a[n] = key.. " = ".. Value -- add key-value pair to the array
end
local s = table.concat(a, ";") -- concatenate all key-value pairs into
    one string

```



```
<!--NeedCopy-->
```

Ein weiterer nützlicher Iterator ist die `string.gmatch()` Funktion, die im folgenden `COMBINE_HEADERS()` Beispiel verwendet wird.

NetScaler Erweiterungen - Bibliotheksreferenz

May 11, 2023

Die Liste der Bibliotheken, die in Richtlinienerweiterungen unterstützt werden.

- Basisbibliothek
- Zeichenfolgenbibliothek
- Reguläre Ausdrucksmuster - Zeichenklassen
- Muster für reguläre Ausdrücke — Musterelemente
- Tabellenbibliothek
- Mathematische Bibliothek
- Bitwise-Bibliothek
- Betriebssystembibliothek
- NetScaler-Bibliothek

Basisbibliothek

asserieren (v [, Nachricht])	Ergibt einen Fehler mit einer optionalen Meldung, wenn v falsch ist.
Fehler (Nachricht)	Beendet eine Funktion und meldet die Fehlermeldung.
Beeinträchtigung (a)	Iterator für ein Array a. Gibt einen Index und einen Wert für jede Iteration zurück.
Paare (t)	Iterator für eine Tabelle t. Gibt einen Schlüssel und einen Wert für jede Iteration zurück.
zu Zahl (e [, Basis])	Konvertiert e in eine Zahl mit optionaler Basis.
an der Saite (v)	Konvertiert v in eine Zeichenfolge
typ (v)	Gibt den Typ von v zurück: Zahl, Zeichenfolge, boolescher Wert, Tabelle usw.

getmetatable (Objekt)	Gibt Null zurück, wenn das Objekt keine Metatabelle hat. Andernfalls, wenn die Metatabelle des Objekts ein Feld „__metatable“ hat, wird der zugehörige Wert zurückgegeben. Andernfalls wird die Metatabelle des angegebenen Objekts zurückgegeben.
setmetatable (Tabelle, Metatabelle)	Legt die Metatabelle für die angegebene Tabelle fest. (Sie können die Metatabelle anderer Typen nicht von Lua aus ändern, nur von C.) Wenn Metatabelle Null ist, wird die Metatabelle der angegebenen Tabelle entfernt. Wenn die ursprüngliche Metatabelle ein Feld „__metatable“ hat, wird ein Fehler ausgelöst.
auswählen (index, ···)	Gibt alle Argumente nach dem Argumentnummernindex zurück. Wenn Index Zeichenfolge # ist, dann gibt es die Gesamtzahl der zusätzlichen Argumente, die er empfangen hat.
pcall (f [, arg1, ··])	Ruft Funktion f mit den angegebenen Argumenten im geschützten Modus auf. Es gibt als erstes Ergebnis einen Statuscode zurück, der angibt, ob der Anruf erfolgreich war oder nicht. Wenn der Aufruf erfolgreich war, werden zusammen mit dem Statuscode auch alle Ergebnisse des Anrufs zurückgegeben, andernfalls wird eine Fehlermeldung zurückgegeben.
xpcall (f, msgh [, arg1, ···])	Diese Funktion ähnelt pcall, außer dass sie auch ein Argument für die Fehlerbehandlung benötigt.
_VERSION	Gibt die aktuelle Interpreter-Version zurück.

Zeichenfolgenbibliothek

Zeichenfolge (s [, i [, j]])	Gibt die Bytewerte für s [i] bis s [j] zurück. Standard i = 1 und j = i
Zeichenfolge (…)	Gibt einen String zurück, der aus den Integer-Parametern konstruiert wurde.
string.find (s, pattern [, init [, einfach])	Sucht nach der ersten Übereinstimmung eines regulären Ausdrucksmusters in s. Gibt den ersten und letzten Index von match oder nil. init ist der Startindex, Standard 1. plain = true bedeutet, dass das Muster kein Regex ist.
string.format (Formular,…)	Gibt eine formatierte Version der Parameter zurück.
string.gmatch (s, Muster)	Iterator für die Suche nach s mit dem Regex-Muster. Gibt übereinstimmende Werte zurück.
string.gsub (s, Muster, Antwort [, n])	Gibt eine Kopie von s zurück, in der alle (oder n) Vorkommen des Musters durch repl ersetzt wurden.
string.len (s)	Gibt die Länge der Zeichenfolge zurück.
Zeichenfolge. Lower (s)	Gibt eine Kopie der Zeichenfolge zurück, die in Kleinbuchstaben konvertiert wurde.
string.match (s, Muster [, Init])	Sucht nach der ersten Übereinstimmung des Regex-Musters in s und gibt die Captures oder das gesamte Muster zurück. init ist der zu startende Index, Standard 1.
string.rep (s, n [, step])	Gibt einen String zurück, der n Kopien von s ist, mit Separator sep, Standard kein Trennzeichen
Zeichenfolge. Umgekehrt (s)	Gibt eine Zeichenfolge zurück, die umgekehrt ist.
string.sub (s, i [, j])	Gibt die Teilzeichenfolge von s [i] bis s [j] zurück, Standard j ist das Ende der Zeichenfolge.
Zeichenfolge. Upper (s)	Gibt eine Kopie der in Großbuchstaben konvertierten Zeichenfolge zurück.

string.dump (Funktion)	Gibt eine Zeichenfolge zurück, die eine binäre Darstellung der angegebenen Funktion enthält.

Reguläre Ausdrucksmuster — Zeichenklassen

x	das Zeichen x, außer bei magischen Zeichen ^$ ()%. [] *+-?)
.	irgendein Zeichen
%a	irgendein Buchstabe
%c	irgendein Steuerzeichen
%d	jede Ziffer
%g	jedes druckbare Zeichen außer Leerzeichen
%l	beliebiger Kleinbuchstabe
%p	beliebiges Satzzeichen
%s	ein beliebiges Leerzeichen
%u	beliebiger Großbuchstabe
%w	beliebiger Alpha-Zahlen-Buchstabe
%x	ein entkommenes magisches Zeichen x (zum Beispiel%%)
[einstellen]	eine Reihe von Zeichen: Sequenz einzelner Zeichen, Bereiche X-Y und %-Klassen
[^set]	Charaktere, die nicht im Set enthalten sind.

Muster für reguläre Ausdrücke — Musterelemente

X	eine Charakterklasse
X*	0 oder mehr längste Wiederholungen von Zeichen in X

X+	1 oder mehr Wiederholungen von Zeichen in X
X-	0 oder mehr kürzeste Wiederholungen von Zeichen in X
X?	0 oder 1 Zeichen in X
%n	n=1 bis 9; entspricht der n-ten erfassten Zeichenfolge
%bxy	entspricht einer Teilzeichenfolge zwischen zwei ausgeglichenen Zeichen x und y. Beispiel %b () entspricht einer Teilzeichenfolge zwischen zwei ausgeglichenen Klammern.
%f [gesetzt]	entspricht einer leeren Zeichenfolge an einer beliebigen Position, sodass das nächste Zeichen zu set gehört und das vorherige Zeichen nicht zu set.

Ein Muster ist eine Abfolge von Musterelementen. ^pattern entspricht dem Anfang einer Zeichenfolge und pattern$ entspricht dem Ende der Zeichenfolge.

Übereinstimmende Teilzeichenfolgen können mit (Muster) erfasst werden. Klammern ohne Muster () erfassen die aktuelle Zeichenkettenposition (eine Zahl).

Tabellenbibliothek

table.concat (liste [, step [, i [, j]]])	Gibt eine Zeichenkettenliste [i].. sep.. list [i+1].. sep.. list [j] zurück. Standard sep ist die leere Zeichenfolge. Der Standardwert i ist 1, j ist #list.
table.insert (Liste, [pos,] Wert)	Fügt Wert in die Liste an Indexposen ein. Die Standardeinstellung für pos ist #list (Ende der Liste).
Tabelle.pack (…)	Gibt ein Array mit den Parametern ab Index 1 und einen Schlüssel n mit der Gesamtzahl der Parameter.

table.remove (liste [, pos])	Entfernt aus der Liste das Element an Position pos, Verschieben Elemente, um die Position zu füllen. Gibt das entfernte Element zurück. Default for posis #list (end of the list.)
table.sort (liste [, komp])	Sortieren Sie die Elemente der Liste an Ort und Stelle. comp ist die Vergleichsfunktion zu verwenden. Die Standardeinstellung für comp ist <.
table.unpack (Liste [, i [, j]])	Gibt Liste [i] bis Liste [j] zurück. Die Standardeinstellung für i ist 1 und j ist #list <c/ode>.

Mathematische Bibliothek

Verschiedene trigonometrische und logarithmische Funktionen sind nicht dargestellt.

math.abs (x)	Gibt den absoluten Wert von x zurück.
math.ceil (x)	Gibt die kleinste Ganzzahl >= x zurück.
math.floor (x)	Gibt die größte Ganzzahl <= x zurück.
math.fmod (x, y)	Gibt den Rest von x/y zurück und rundet den Quotienten gegen Null.
math.huge	Ein Wert >= jede andere Zahl.
mathematisch.max (x,…)	Gibt das maximale Argument zurück.
math.min (x,…)	Gibt das minimale Argument zurück.
math.modf (x)	Gibt die Ganzzahl- und Bruchteile von x zurück.
mathematisch.zufällig ()	Gibt eine Pseudozufallszahl zwischen 0 und 1 zurück.
mathematisch zufällig (m)	Gibt eine pseudozufällige Ganzzahl zwischen 1 und m zurück.
math.random (m, n)	Gibt eine pseudozufällige Ganzzahl zwischen m und n zurück.
math.randomseed (x)	Setzt den Pseudozufallszahlengenerator auf x.

math.sqrt (x)	Gibt die Quadratwurzel von x zurück (x^0,5)
math.acos (x)	Gibt den Arkuskosinus von x (im Bogenmaß) zurück.
mathematisch.asin (x)	Gibt den Arkussinus von x (im Bogenmaß) zurück.
math.atan (x)	Gibt den Arkustangens von x (im Bogenmaß) zurück.
math.atan2 (y, x)	Gibt den Arkustangens von y/x (im Bogenmaß) zurück.
math.cos (x)	Gibt den Kosinus von x zurück.
math.cosh (x)	Gibt den hyperbolischen Kosinus von x zurück.
math.sin (x)	Gibt den Sinus von x zurück.
math.sinh (x)	Gibt den hyperbolischen Sinus von x zurück.
math.tan (x)	Gibt den Tangens von x zurück.
math.tanh (x)	Gibt den hyperbolischen Tangens von x zurück.
math.deg (x)	Gibt den Winkel x (im Bogenmaß angegeben) in Grad zurück.
mathematisch.exp (x)	Gibt den Wert e^x zurück.
math.frexp (x)	Gibt m und e so zurück, dass x = m2e, e eine Ganzzahl ist und der Absolutwert von m im Bereich [0,5, 1) liegt.
math.ldexp (ich, e)	Gibt m2e zurück (e sollte eine ganze Zahl sein).
math.log (x [, Basis])	Gibt den Logarithmus von x in der angegebenen Basis zurück. Die Standardeinstellung für base ist e.
math.pow (x, y)	Gibt x^y zurück.
math.rad (x)	Gibt den Winkel x (in Grad angegeben) im Bogenmaß zurück.
math.pi	Der Wert von π.

Bitwise-Bibliothek

Sofern nicht anders angegeben:

- Alle Funktionen akzeptieren numerische Argumente im Bereich (-2^51, +2^51).
- Jedes Argument wird auf den Rest seiner Division durch 2^32 normalisiert und zu einer Ganzzahl gekürzt (auf eine nicht spezifizierte Weise), sodass sein Endwert in den Bereich [0,2^32 - 1] fällt.
- Alle Ergebnisse liegen im Bereich [0,2^32 - 1].

bit32.arshift (x, disp)	Gibt x arithmetisch verschobene Disp-Bits nach rechts (+disp) oder links (-disp) zurück.
bit32.band (…)	Gibt die Bitanzahl und der Argumente zurück.
bit32.bnot (x)	Gibt die bitweise Negation von x zurück.
bit32.bor (…)	Gibt den bitweisen Wert oder der Argumente zurück.
bit32.btest(…)	Gibt True zurück, wenn das bitweise und der Argumente nicht Null ist.
bit32.bx oder (…)	Gibt das bitweise Exklusiv oder der Argumente zurück.
bit32.extract (n, Feld [, Breite])	Gibt die Bits in n von Feld zu Feld + Breite - 1 (Bitzahl von den meisten zu den geringsten signifikanten). Die Standardbreite ist 1.
bit32.replace (n, v, Feld [, Breite])	Gibt eine Kopie von n zurück, wobei die Bits von Feld zu Feld + Breite -1 ersetzt durch v. Die Standardbreite ist 1.
bit32.lrotate (x, disp)	Gibt x gedrehte Disp-Bits nach links (+disp) oder rechts (-disp) zurück.
bit32.lshift (x, disp)	Gibt x verschobene Disp-Bits nach links (+disp) oder rechts (-disp) zurück.
bit32.rrotate (x, disp)	Gibt x gedrehte Disp-Bits nach rechts (+disp) oder links (-disp) zurück.
bit32.rshift (x, disp)	Gibt x verschobene Disp-Bits nach rechts (+disp) oder links (-disp) zurück.

Betriebssystembibliothek

os.clock ()	Gibt eine Näherung des Betrags in Sekunden der CPU-Zeit zurück.
os.date ([Format [, Uhrzeit]])	Gibt eine Zeichenfolge oder eine Tabelle mit Datum und Uhrzeit zurück, formatiert gemäß dem angegebenen Zeichenfolgenformat.
os.time ([Tabelle])	Gibt die aktuelle Zeit zurück, wenn sie ohne Argumente aufgerufen wird, oder eine Zeit, die das Datum und die Uhrzeit darstellt, die in der angegebenen Tabelle angegeben ist.
os.difftime (t2, t1)	Gibt die Anzahl der Sekunden vom Zeitpunkt t1 bis zum Zeitpunkt t2 zurück.

NetScaler-Bibliothek

ns.logger:level (Nachricht)	Um Meldungen zu protokollieren, deren Stufe „Notfall“, „Warnung“, „Kritisch“, „Fehler“, „Warnung“, „Hinweis“, „Info“ oder „Debug“ ist. Die Parameter sind die gleichen wie die C printf () -Funktion: eine Formatzeichenfolge und eine variable Anzahl von Argumenten, die Werte für die% -Bezeichner in der Formatzeichenfolge angeben.

API-Referenz für NetScaler-Erweiterungen

May 11, 2023

Verhalten ist eine Formalisierung gängiger programmierbarer Muster, die auf einer NetScaler-Appliance verfügbar sind. Ein virtueller TCP-Server unterstützt beispielsweise ein TCP-Clientverhalten und ein TCP-Serververhalten. Ein Verhalten ist ein vordefinierter Satz von Callback-Funktionen. Sie können Verhaltensweisen implementieren, indem Sie Callback-Funktionen bereitstellen. Ein TCP-Clientverhalten kann beispielsweise aus der Funktion on_data bestehen, die den TCP-Datenstrom verarbeitet.

Verhalten des TCP-Clients

on_data — Funktionsrückruf für TCP-Client-Datenereignisse. Der Callback benötigt zwei Argumente:

- **ctxt** - Verarbeitungskontext für TCP-Clients
- **Nutzlast** — Event-Payload
  - **payload.data** — Empfangene TCP-Daten, verfügbar als Byte-Stream

Verhalten des TCP-Servers

on_data — Funktionsrückruf für TCP-Serverdatenereignisse, der Callback benötigt zwei Argumente:

- **ctxt - Kontext** für die TCP-Serververarbeitung
- **Nutzlast** — Event-Payload
  - **payload.data** — empfangene TCP-Daten, verfügbar als Byte-Stream

TCP-Clientkontext

Der Kontext, der an die TCP-Client-Event-Callbacks übergeben wird:

- **ctxt.output** — Der nächste Verarbeitungskontext in der Pipeline. Callback-Handler für Erweiterungen können Daten vom Typ ns.tcp.stream an ctxt.output senden, indem sie die Ereignisse DATA verwenden, was eine partielle Nachricht bedeutet, oder EOM, was eine Nachricht am Ende des Protokolls bedeutet. Das EOM-Ereignis kann TCP-Daten enthalten oder auch nicht. Ein EOM-Ereignis mit TCP-Daten kann ohne vorheriges DATA-Ereignis gesendet werden, um die gesamten Protokollnachrichtendaten zu senden und das Ende der Nachricht zu markieren. Die Entscheidung für den Lastenausgleich wird stromabwärts vom virtuellen Lastausgleichsserver anhand der ersten empfangenen Daten getroffen. Nach Erhalt der EOM-Nachricht wird eine neue Load-Balancing-Entscheidung getroffen. Um Protokollnachrichtendaten zu streamen, senden Sie also mehrere DATA-Ereignisse, wobei das letzte Ereignis als EOM gilt. Alle aufeinanderfolgenden DATA-Ereignisse und die folgenden EOM-Ereignisse werden an dieselbe Serververbindung gesendet, die bei der Lastausgleichsentscheidung für das erste DATA-Ereignis in der Sequenz ausgewählt wurde.
- **ctxt.input** — Der vorherige Verarbeitungskontext in der Pipeline, aus dem die TCP-Stream-Daten stammen.
- **ctxt:hold (data)** — Funktion zum Speichern der Daten für die zukünftige Verarbeitung. Wenn ein Anruf mit Daten unterbrochen wird, werden die Daten im Kontext gespeichert. Wenn später mehr Daten im gleichen Kontext empfangen werden, werden neu empfangene Daten an die zuvor gespeicherten Daten angehängt und der kombinierte Datenstrom wird dann an die on_data-Callback-Funktion übergeben. Nach dem Aufruf einer Sperre ist die Datenreferenz nicht mehr verwendbar und gibt bei jeder Verwendung einen Fehler aus.

- **ctxt.vserver — Der virtuelle Serverkontext** .
- **ctxt.client** — Kontext für die Verarbeitung von Clientverbindungen. Dieser Verarbeitungskontext kann verwendet werden, um Daten an den Client zu senden und einige verbindungsbezogene Informationen wie IP-Adresse, Quell- und Zielports abzurufen.
- **ctxt:close ()** — Schließt die Client-Verbindung, indem FIN an den Client gesendet wird. Nach dem Aufrufen dieser API ist der Client-Verarbeitungskontext nicht mehr verwendbar und gibt bei jeder Verwendung einen Fehler aus.

TCP-Serverkontext

Der Kontext, der an die TCP-Serverereignisrückrufe übergeben wird:

- **ctxt.output** — Der nächste Verarbeitungskontext in der Pipeline. Callback-Handler für Erweiterungen können Daten vom Typ ns.tcp.stream an ctxt.output senden, indem sie die Ereignisse DATA verwenden, was eine partielle Nachricht bedeutet, oder EOM, was eine Nachricht am Ende des Protokolls bedeutet.
- **ctxt.input** — Der vorherige Verarbeitungskontext in der Pipeline, aus dem die TCP-Stream-Daten stammen.
- **ctxt:hold (data)** — Funktion zum Speichern der Daten für die zukünftige Verarbeitung. Wenn ein Anruf mit Daten unterbrochen wird, werden die Daten im Kontext gespeichert. Wenn später mehr Daten im gleichen Kontext empfangen werden, werden neu empfangene Daten an die zuvor gespeicherten Daten angehängt und der kombinierte Datenstrom wird dann an die on_data-Callback-Funktion übergeben. Nach dem Aufruf einer Sperre ist die Datenreferenz nicht mehr verwendbar und gibt bei jeder Verwendung einen Fehler aus.
- **ctxt.vserver — Der virtuelle Serverkontext** .
- **ctxt.server** — Kontext für die Verarbeitung von Serververbindungen. Dieser Verarbeitungskontext kann verwendet werden, um Daten an den Server zu senden und einige verbindungsbezogene Informationen wie IP-Adresse, Quell- und Zielports abzurufen.
- **ctxt:reuse_server_connection ()** — Diese API wird verwendet, um zu ermöglichen, dass die Serververbindung nur im Serverkontext für andere Client-Verbindungen wiederverwendet werden kann. Diese API kann nur verwendet werden, wenn ein EOM-Ereignis (in der ns.send () API) verwendet wird, um die Daten im Client-Kontext zu senden. Andernfalls gibt die ADC-Appliance einen Fehler aus.

  Damit eine Serververbindung von anderen Clients wiederverwendet werden kann, muss diese API am Ende jeder Antwortnachricht aufgerufen werden. Wenn nach dem Aufruf dieser API weitere Daten über diese Serververbindung empfangen werden, wird dies als Fehler behandelt und die Serververbindung wird geschlossen. Wenn diese API nicht verwendet wird, kann die

Serververbindung nur für den Client verwendet werden, für den sie geöffnet wurde. Wenn derselbe Server für eine weitere Lastausgleichsentscheidung für diesen Client ausgewählt wird, wird dieselbe Serververbindung verwendet, um die Client-Daten zu senden. Nach der Verwendung dieser API ist die Serververbindung nicht mehr an die Client-Verbindung gebunden, für die sie geöffnet wurde, und kann für eine neue Lastausgleichsentscheidung für jede andere Client-Verbindung wiederverwendet werden. Nach dem Aufruf dieser API ist der Serverkontext nicht mehr verwendbar und löst bei jeder Verwendung einen Fehler aus.

Hinweis: Diese API ist in NetScaler 12.1 Build 49.xx und höher verfügbar.

- **ctxt:close ()** — Schließt die Serververbindung, indem FIN an den Server gesendet wird. Nach dem Aufruf dieser API ist der Client-Verarbeitungskontext nicht mehr verwendbar und zeigt bei jeder Verwendung einen Fehler an.

  Hinweis: Diese API ist in NetScaler 12.1 Build 50.xx und höher verfügbar.

Vserver-Kontext

Der virtuelle Benutzerserverkontext, der über die an Callbacks übergebenen Kontexte verfügbar ist:

- **vserver:counter_increment (counter_name)** — Erhöht den Wert eines als Argument übergebenen virtuellen Serverzählers. Derzeit werden die folgenden integrierten Zähler unterstützt.
  - **- invalid_messages** — Anzahl der ungültigen Anfragen/Antworten auf diesem virtuellen Server.
  - **- invalid_messages_dropped** — Anzahl der ungültigen Anfragen/Antworten, die von diesem virtuellen Server gelöscht wurden.
- **vserver.params** — Die konfigurierten Parameter für den virtuellen Benutzerserver. Parameter ermöglichen die Konfigurierbarkeit von Erweiterungen. Der Erweiterungscode kann auf Parameter zugreifen, die in der CLI angegeben sind, um einen virtuellen Benutzerserver hinzuzufügen.

Kontext der Client-Verbindung

Kontext zur Verarbeitung von Client-Verbindungen, um verbindungsbezogene Informationen abzurufen.

- **client.ssl — SSL-Kontext**
- **client.tcp — TCP-Kontext**
- **client.is_ssl — True, wenn die Client-Verbindung SSL-basiert** ist

Kontext der Serververbindung

Kontext zur Verarbeitung von Serververbindungen, um verbindungsbezogene Informationen abzurufen.

- **server.ssl — SSL-Kontext**
- **server.tcp — TCP-Kontext**
- **server.is_ssl — True, wenn die Serververbindung SSL-basiert** ist

TCP-Kontext

Der TCP-Kontext arbeitet mit dem TCP-Protokoll.

- **tcp.srcport — Quellport** als Zahl
- **tcp.dstport - Zielport** als Zahl

IP-Kontext

Der IP-Kontext funktioniert mit IP- oder IPv6-Protokolldaten.

- **ip.src** — Quell-IP-Adresskontext.
- **ip.dst** — Kontext der Ziel-IP-Adresse.

Hinweis: Diese API ist in NetScaler 12.1 Build 51.xx und höher verfügbar.

IP-Adresskontext

Der IP-Adresskontext funktioniert mit IP- oder IPv6-Adressdaten.

- **<address>.to_s** - Die Adresszeichenfolge in der entsprechenden ASCII-Notation.
- **<address>.to_n** - Der numerische Wert der Adresse als Bytefolge in Netzwerkreihenfolge (4 Byte für IPv4 und 16 Byte für IPv6).
- **<address>.version** - Gibt 4 für IPv4 und 6 für IPv6 zurück.
- **<address>:subnet(<prefix value>)** - Gibt die Subnetzadresszeichenfolge zurück, nachdem die Präfixnummer angewendet wurde.
  - Für eine IPv4-Adresse muss der Wert zwischen 0 und 32 liegen
  - Für eine IPv6-Adresse muss der Wert zwischen 0 und 128 liegen.
- **<address>:apply_mask(<mask string>)** - Gibt die Adresszeichenfolge nach dem Anwenden der Maskenzeichenfolge zurück. Die API validiert die Version des Arguments und führt eine entsprechende Fehlerprüfung durch.
- **address>:eq(<address string>)** - Gibt „Wahr“ oder „Falsch“ zurück, je nachdem, ob das Argument dem Adressobjekt entspricht. Die API validiert die Version der Argumente.

Hinweis: Diese API ist in NetScaler 12.1 Build 51.xx und höher verfügbar.

SSL-Kontext

Der SSL-Kontext enthält Informationen zur Frontend-SSL-Verbindung.

- **ssl.cert** — SSL-Zertifikatskontext. Für die Clientverbindung stellt es den Client-Zertifikatskontext und für die Serververbindung den Serverzertifikatskontext bereit.
- **ssl.version** — Eine Zahl, die die SSL-Protokollversion der aktuellen Transaktion darstellt, wie folgt:

  - 0: The transaction is not SSL-based
  - 0x002: The transaction is SSLv2
  - 0x300: The transaction is SSLv3
  - 0x301: The transaction is TLSv1
  - 0x302: The transaction is TLSv1.1
  - 0x303: The transaction is TLSv1.2

- **ssl.cipher_name — SSL-Verschlüsselungsname** als Zeichenfolge, wenn er von einer SSL-Verbindung aus aufgerufen wird, andernfalls gibt er eine NULL-Zeichenfolge zurück.
- **ssl.cipher_bits — Anzahl der Bits** im kryptografischen Schlüssel.

Kontext des SSL-Zertifikats

- **cert.Version — Versionsnummer** des Zertifikats. Wenn die Verbindung nicht SSL-basiert ist, wird 0 zurückgegeben.
- **cert.valid_not_before — Datum im Zeichenkettenformat, vor dem** das Zertifikat nicht gültig ist.
- **cert.valid_not_after — Datum im Zeichenkettenformat, nach dem** das Zertifikat nicht mehr gültig ist.
- **cert.days_to_EXPIRE — Anzahl der Tage, vor denen das Zertifikat gültig** ist. Gibt -1 für ein abgelaufenes Zertifikat zurück.
- **cert.to_PEM** — Zertifikat im Binärformat.
- **cert.issuer** — Distinguished Name (DN) des Emittenten im Zertifikat als Namenswertliste. Ein Gleichheitszeichen („=“) ist das Trennzeichen für den Namen und den Wert, und der Schrägstrich („/“) ist das Trennzeichen, das die Name-Wert-Paare voneinander trennt.

  Es folgt ein Beispiel für den zurückgegebenen DN:
  /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@n
- **cert.auth_keyid** — Kontext der Authority Key Identifier-Erweiterung des X.509 V3-Zertifikats.
  - **auth_keyid.exists** — TRUE, wenn das Zertifikat eine Authority Key Identifier-Erweiterung enthält.

  - **auth_keyid.issuer_name** — Distinguished Name des Ausstellers im Zertifikat als Name-Wert-Liste.
    Ein Gleichheitszeichen (=) ist das Trennzeichen für den Namen und den Wert, und der Schrägstrich (/) ist das Trennzeichen, das die Name-Wert-Paare voneinander trennt.

  Beispiel:
  /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@m

  - **auth_keyid.keyid — KeyIdentifier-Feld** des Authority Key Identifier als Blob
  - **auth_keyid.cert_serialnumber — Feld SerialNumber** des Authority Key Identifier als Blob.

- **cert.pk_algorithm** — Name des vom Zertifikat verwendeten Public-Key-Algorithmus.
- **cert.pk_size — Größe** des im Zertifikat verwendeten öffentlichen Schlüssels.
- **cert.serialnumber — Seriennummer** des Client-Zertifikats. Wenn es sich um eine Nicht-SSL-Transaktion handelt oder ein Fehler im Zertifikat vorliegt, wird eine leere Zeichenfolge zurückgegeben.
- **cert.signature_algorithm** — Name des kryptografischen Algorithmus, der von der CA verwendet wird, um dieses Zertifikat zu signieren.
- **cert.subject_keyid — Subject KeyID** des Client-Zertifikats. Wenn es keine Subject KeyID gibt, ergibt dies ein Textobjekt der Länge Null.
- **cert.subject** — Distinguished Name des Subjekts als Namenswert. Ein Gleichheitszeichen (=) trennt Namen und Werte und ein Schrägstrich (/) trennt Name-Wert-Paare.

Beispiel:
/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycom

NetScaler-Bibliotheken

- **ns.tcp.stream** — Stringähnliche Bibliothek zur Behandlung von TCP-Daten als Byte-Stream. Die maximale Größe der TCP-Stream-Daten, mit denen diese APIs arbeiten können, beträgt 128 KB. Die Funktionen der ns.tcp.stream-Bibliothek können auch im üblichen objektorientierten Aufrufstil von Erweiterungen aufgerufen werden. Beispielsweise ist data:len() dasselbe wie ns.tcp.stream.len(data)

  - **ns.tcp.stream.len (data) - Gibt die Länge der Daten** in Byte zurück, ähnlich wie bei Luas String.len
  - **ns.tcp.stream.find (data, pattern [, init])** — Funktion ähnlich wie Luas string.find. Darüber hinaus führt es auch einen teilweisen Abgleich am Ende der Daten durch. Bei teilweiser Übereinstimmung wird der Startindex zurückgegeben und der Endindex wird Null.

  - **ns.tcp.stream.split (data, length)** - Teilt die Daten in zwei Blöcke auf, der erste Block hat die angegebene Länge. Nach einer erfolgreichen Aufteilung sind die Originaldaten nicht mehr als TCP-Datenstrom nutzbar. Jeder Versuch, es auf diese Weise zu verwenden, führt zu einem Fehler.
  - **ns.tcp.stream.byte(data[, i [, j]])** - Function similar to Lua's string.byte. Gibt die internen numerischen Codes der Zeichen data [i], data [i+1],..., data [j] zurück.
  - n**s.tcp.stream.sub (data, i [, j])** — Funktion ähnlich wie Luas string.sub. Gibt die Teilzeichenfolge von s zurück, die bei i beginnt und bis j andauert.
  - **ns.tcp.stream.match (data, pattern, [, init])** — Funktion ähnlich wie Luas string.match. Sucht nach der ersten *Musterübereinstimmung* in der Zeichenfolge s.

- **ns.send(processing_ctxt, event_name, event_data)** — Generische Funktion zum Senden von Ereignissen an einen Verarbeitungskontext. Event-Daten sind eine Lua-Tabelle, die beliebigen Inhalt haben kann. Die Inhalte hängen von der Veranstaltung ab. Nachdem die ns.send () -API aufgerufen wurde, ist die Datenreferenz nicht mehr verwendbar. Jeder Versuch, es zu verwenden, verursacht einen Fehler.

- **ns.pipe(src_ctxt, dest_ctxt)** — Mithilfe eines Aufrufs der pipe()-API kann Erweiterungscode den Quellkontext mit einem Zielkontext verbinden. Nach einem Pipe-Aufruf gehen alle Ereignisse, die vom Quellkontext an das nächste Modul in der Pipeline gesendet werden, direkt an den Zielkontext. Diese API wird normalerweise von dem Modul verwendet, das den pipe()-Aufruf ausführt, um sich selbst aus der Pipeline zu entfernen.

- **ns.inet** — Bibliothek für Internetadressen.

  - **ns.inet.apply_mask (address_str, mask_str) — gibt die Adresszeichenfolge zurück, nachdem die Maskenzeichenfolge angewendet wurde** .
  - **ns.inet.aton (address_str)** — Gibt den numerischen Wert der Adresse als Bytefolge in Netzwerkreihenfolge zurück (4 Byte für IPv4 und 16 Byte für IPv6).
  - **ns.inet.ntoa (byte_str) — Konvertiert einen numerischen Bytewert** als Bytefolge in eine Adresszeichenfolge.
  - **ns.inet.ntohs (number)** — Konvertiert die angegebene Netzwerk-Bytereihenfolge in die Host-Bytereihenfolge. Wenn die Eingabe größer als 2^16 - 1 ist, wird ein Fehler ausgegeben.
  - **ns.inet.htons (number) - Konvertiert die angegebene Host-Bytereihenfolge** in die Netzwerk-Bytereihenfolge. Wenn die Eingabe größer als 2^16 - 1 ist, wird ein Fehler ausgegeben.
  - **ns.inet.ntohl (number)** — Konvertiert die angegebene Netzwerk-Bytereihenfolge in die Host-Bytereihenfolge. Wenn die Eingabe größer als 2^32 - 1 ist, wird ein Fehler ausgegeben.
  - **ns.inet.htonl (number)** - Konvertiert die angegebene Host-Bytereihenfolge in die Netzwerk-Bytereihenfolge. Wenn die Eingabe größer als 2^32 - 1 ist, wird ein Fehler

ausgegeben.

- **ns.inet.subnet (address_str, subnet_value)** — Gibt die Subnetzadressenzeichenfolge nach Anwendung des angegebenen Subnetzes zurück.

Protokollerweiterungen

May 11, 2023

Die NetScaler-Appliances bieten native Unterstützung für Protokolle wie HTTP. Darüber hinaus können Sie Protokollerweiterungen verwenden, um Unterstützung für benutzerdefinierte Protokolle hinzuzufügen. Derzeit werden nur TCP-basierte benutzerdefinierte Protokolle unterstützt, beispielsweise das Message Queuing Telemetry Transport (MQTT) -Protokoll. Für sichere Transaktionen wird auch TCP über SSL unterstützt.

Die Protokollerweiterungen auf der NetScaler-Appliance sind Teil der High-Level-Skripting-Infrastruktur, die auf der NetScaler-Appliance verfügbar ist. Die Skriptsprache basiert auf der Programmiersprache Lua 5.2. Um einer NetScaler-Appliance ein benutzerdefiniertes Protokoll hinzuzufügen, muss der Benutzer Erweiterungscode schreiben, um die entsprechenden Verhaltensweisen zu implementieren. Die Verhaltensweisen ns.tcp.client und ns.tcp.server sind beispielsweise auf TCP-basierte Protokolle anwendbar. Um ein Verhalten zu implementieren, implementieren Sie nur die Callbacks, die Sie anpassen möchten. Wenn Callback nicht implementiert ist, wird der Standardwert wirksam. Weitere Informationen zur Skriptsprache finden Sie unter NetScaler Extensions - Sprachübersicht. Weitere Informationen zu Verhaltensweisen finden Sie unter API-Referenz für NetScaler Extensions.

Die NetScaler Protokollerweiterungen können für Folgendes verwendet werden:

- Fügen Sie mithilfe von Erweiterungen programmgesteuert neue Protokollunterstützung auf der NetScaler-Appliance hinzu.
- Analysieren Sie den Protokollverkehr und führen Sie ein protokollspezifisches nachrichtenbasiertes Load-Balancing (MBLB) durch.
- Konfigurieren Sie die Persistenz für den Lastausgleich.

Protokollerweiterungen - Architektur

May 11, 2023

Um die Erweiterbarkeit auf Datenverkehrsebene zu erreichen, wird die Verkehrsverarbeitung auf einer NetScaler-Appliance als Pipeline aus separaten Verarbeitungsmodulen bereitgestellt. Der Verkehr fließt durch sie, während er ihn vom Eingang bis zum Ausgang verarbeitet. Diese Module in

der Pipeline folgen einem Shared-Nothing-Modell. Die Nachrichtenübergabe wird verwendet, um die Verkehrsdaten von einem Modul in der Pipeline zum nächsten Modul zu senden.

Bestimmte Punkte in der Datenverkehrsverarbeitungspipeline sind erweiterbar, sodass Sie Code hinzufügen können, um das NetScaler-Verhalten anzupassen.

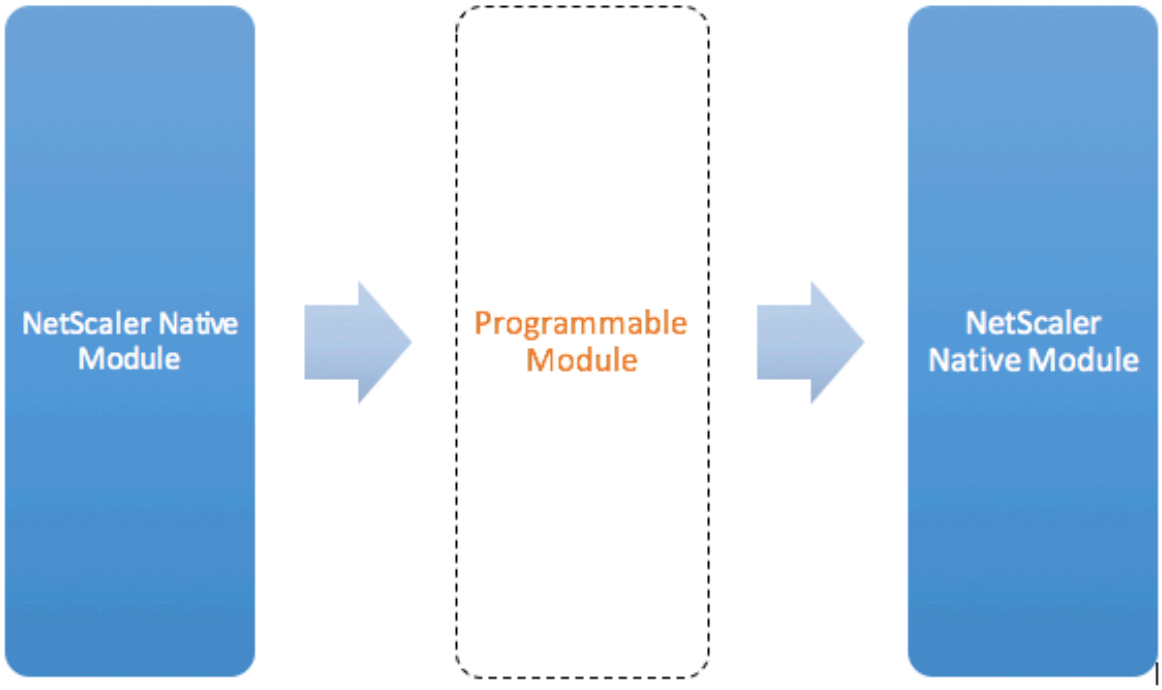


Figure: A Programmable Module In the Traffic Pipeline

Standardmäßig umgeht der Verkehr ein programmierbares Modul, zu dem Sie keinen Code hinzufügen.

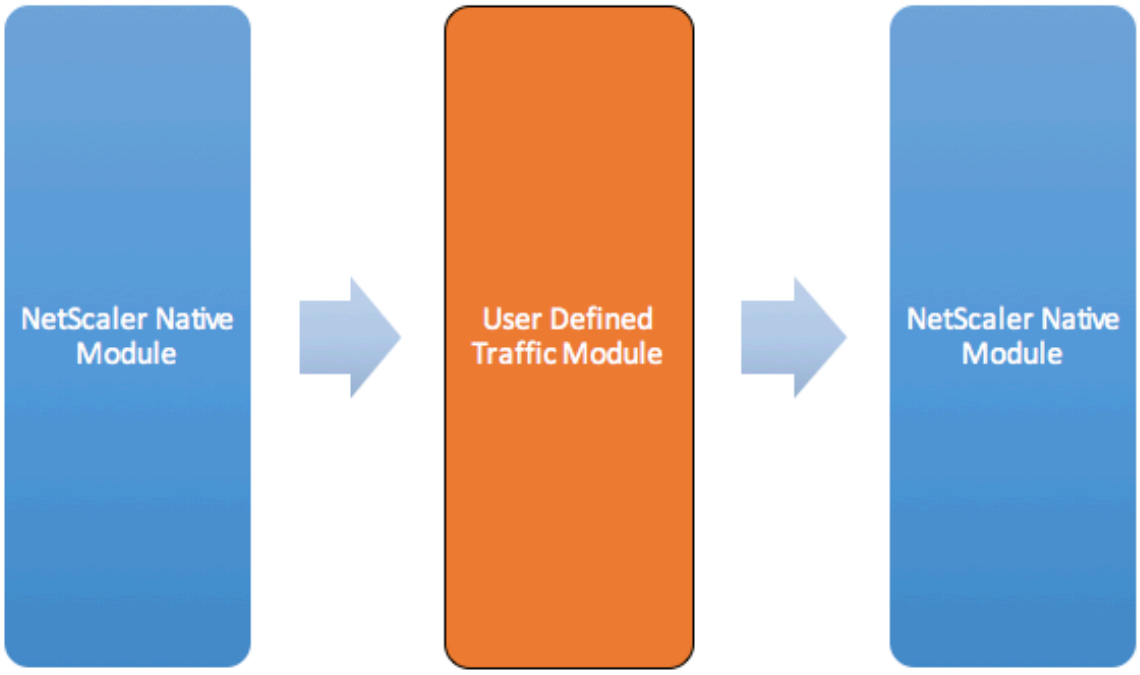


Figure: User Defined Traffic Module

Verhaltensweisen

Die programmierbaren Schnittstellen zur Anpassung der Verkehrssteuerung werden als Verhalten bezeichnet. Verhalten ist im Grunde eine Formalisierung gängiger programmierbarer Muster, die auf einer NetScaler-Appliance verfügbar sind. Die Verhaltensweisen bestehen aus einem vordefinierten Satz von Event-Callback-Funktionen. Sie können ein Verhalten implementieren, indem Sie Callback-Funktionen bereitstellen, die dem Verhalten entsprechen.

Das Verhalten des TCP-Clients besteht beispielsweise aus einer Callback-Funktion (on_data), die TCP-Client-Datenstream-Ereignisse verarbeitet. Um Message Based Load Balancing (MBLB) für ein TCP-basiertes Protokoll zu implementieren, können Sie Code für diese Callback-Funktion hinzufügen, um den TCP-Datenstrom vom Client zu verarbeiten und den Byte-Stream in Protokollnachrichten zu analysieren.

Kontext:

Die Callback-Funktionen in einem Verhalten werden mit einem Kontext aufgerufen, bei dem es sich um den Status des Verarbeitungsmoduls handelt. Der Kontext ist die Instanz des Verarbeitungsmoduls. Beispielsweise werden die TCP-Clientverhaltens-Callbacks mit unterschiedlichen Kontexten für verschiedene Client-TCP-Verbindungen aufgerufen.

Nutzlast:

Zusätzlich zum Kontext können die Verhaltensrückrufe andere Argumente haben. Normalerweise wird der Rest der Argumente als Nutzlast übergeben, was die Sammlung aller Argumente ist.

Die Instanzen des programmierbaren Verarbeitungsmoduls können also als eine Kombination aus Instanzstatus und Ereignisrückruffunktionen angesehen werden, dh dem Kontext plus Verhalten. Und der Verkehr fließt durch die Pipeline als Ereignisnutzlast.

Informationen zu NetScaler API-Erweiterungen finden Sie unter Referenz zur NetScaler-Erweiterung.

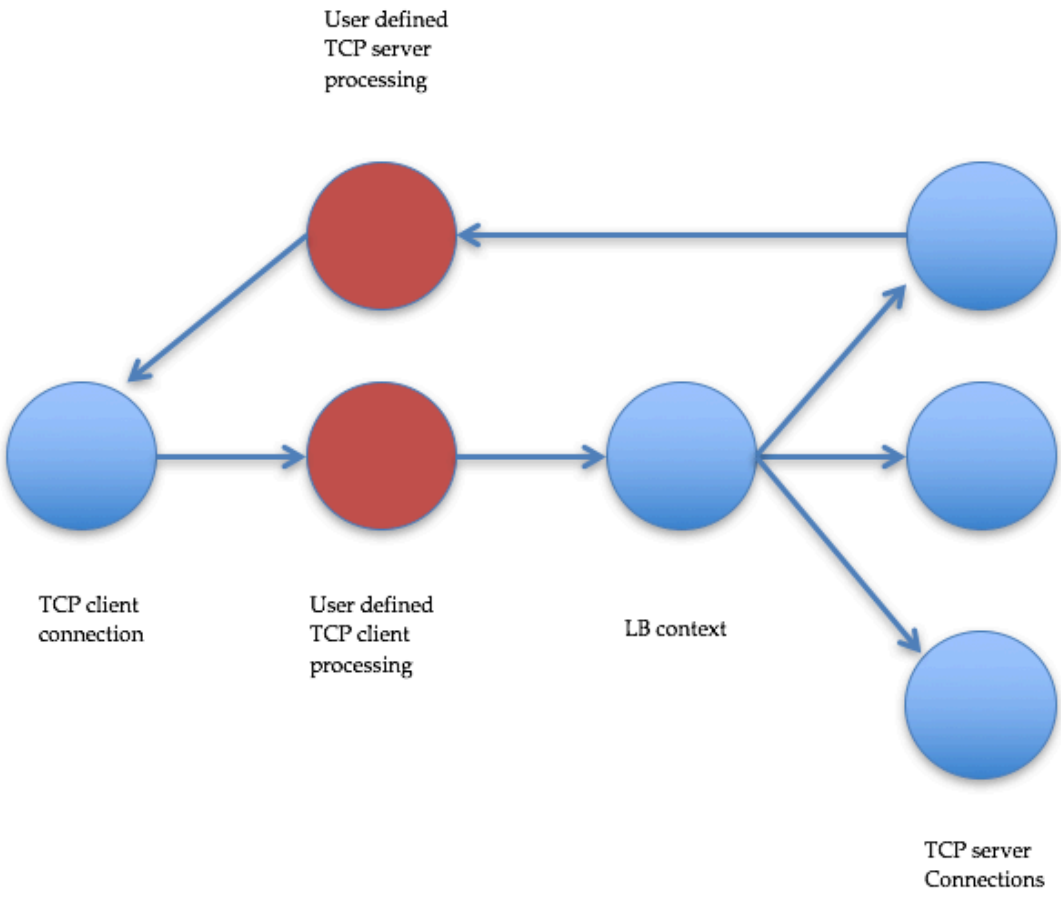
Das folgende Code-Snippet zeigt eine benutzerdefinierte Funktion zum Behandeln von TCP-Clientdatenstromereignissen. Der Kontext und die Payload werden per NetScaler-Code an die Funktion übergeben. Dieser Code leitet einfach die bei jedem Aufruf empfangenen TCP-Daten an den nächsten Verarbeitungsmodulkontext in der Pipeline weiter. In diesem Fall ist das nächste Modul der Load Balancing (LB) -Kontext, bei dem es sich um ein natives NetScaler Modul handelt.

```
function client.on_data(ctxt, payload)
    ns.send(ctxt.output, "DATA", {
 data = payload.data }
 )
end
<!--NeedCopy-->
```

Protokollerweiterungen - Traffic-Pipeline für benutzerdefinierte TCP-Client- und Serververhalten

May 11, 2023

Die folgende Abbildung zeigt die Beispielprotokollerweiterung — Datenverkehrspipeline für benutzerdefiniertes TCP-Client- und Serververhalten.



Traffic Pipeline For User Defined TCP Client And Server Behaviors

Fügen Sie mithilfe von Protokollerweiterungen ein benutzerdefiniertes Protokoll hinzu

Die Befehle der Befehlszeilenschnittstelle (CLI) für benutzerdefinierte Protokolle verwenden das Schlüsselwort „user“, um den benutzerdefinierten Charakter der zugrunde liegenden Konfigurationsentitäten zu kennzeichnen. Mit Hilfe von Erweiterungscode können Sie dem System ein neues Benutzerprotokoll hinzufügen und virtuelle Benutzerserver für benutzerdefinierte Protokolle hinzufügen. Die virtuellen Benutzerserver sind wiederum konfigurierbar, indem Parameter festgelegt werden. Konfigurierte Werte für virtuelle Serverparameter sind im Erweiterungscode verfügbar.

Das folgende Beispiel veranschaulicht den Benutzerablauf beim Hinzufügen von Unterstützung für ein neues Protokoll. Das Beispiel fügt dem System die Unterstützung des MQTT-Protokolls hinzu. MQTT ist ein Maschine-zu-Maschine-Konnektivitätsprotokoll für das Internet der Dinge. Es ist ein einfacher Nachrichten-Transport zum Veröffentlichen und Abonnieren. Dieses Protokoll ist nützlich für Verbindungen mit entfernten Standorten und verwendet Client- und Broker-Tools, um Nachrichten

an Abonnenten zu veröffentlichen.

1. Importieren Sie die Implementierungsdatei der MQTT-Protokollerweiterung in das NetScaler-System. Die Codeliste für mqtt.lua ist unten angegeben. Das folgende Beispiel importiert die MQTT-Erweiterungsdatei, die auf einem Webserver gehostet wird.

   ```
   import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
   ```

2. Fügen Sie dem System mithilfe der Erweiterung ein neues TCP-basiertes Benutzerprotokoll hinzu.

   ```
   add user protocol MQTT -transport TCP -extension mqtt_code
   ```

3. Fügen Sie einen vServer für den Benutzerlastenausgleich hinzu und binden Sie Backend-Dienste daran.

   ```
   add service mqtt_svr1 10.217.24.48 USER_TCP 1501
   add service mqtt_svr2 10.217.24.48 USER_TCP 1502
   add lb vserver mqtt_lb USER_TCP  - lbmethod USER_TOKEN
   bind lb vserver mqtt_lb mqtt_svr1
   bind lb vserver mqtt_lb mqtt_svr2
   <!--NeedCopy-->
   ```

4. Fügen Sie einen Benutzer-vserver für das neu hinzugefügte Protokoll hinzu. Stellen Sie defaultlb auf den oben konfigurierten LB-vserver ein.

   ```
   add user vserver mqtt_vs MQTT 10.217.24.28 8765 -defaultLb mqtt_lb
   ```

5. Aktivieren Sie optional die MQTT-Sitzungspersistenz basierend auf ClientID und legen Sie den Persistenztyp auf USERSESSION fest.

   ```
   set lb vserver mqtt_lb -persistenceType USERSESSION
   ```

Protokollerweiterungen - Anwendungsfälle

May 11, 2023

Protokollerweiterungen können für die folgenden Anwendungsfälle verwendet werden.

- Nachrichtenbasiertes Load Balancing (MBLB)
- Streamen
- Token-basierter Lastenausgleich
- Persistenz beim Lastenausgleich
- Auf TCP-Verbindungen basierender Lastenausgleich
- Inhaltsbasierter Lastenausgleich
- SSL

- Verkehr ändern
- Versenden Sie den Datenverkehr zum Client oder Server
- Prozessdaten zum Verbindungsaufbau

Nachrichtenbasierter Lastenausgleich

Protokollerweiterungen unterstützen Message Based Load Balancing (MBLB), mit dem jedes Protokoll auf einer NetScaler-Appliance analysiert und die über eine Client-Verbindung eingehenden Protokollnachrichten lastenverteilt werden können, d. h. die Nachrichten über mehrere Serververbindungen verteilt werden können. MBLB wird durch Benutzercode erreicht, der den Client-TCP-Datenstrom analysiert.

Der TCP-Datenstrom wird an die on_data-Callbacks für das Client- und Serververhalten übergeben. Der TCP-Datenstrom steht den Erweiterungsfunktionen über eine Schnittstelle wie eine Lua-Zeichenfolge zur Verfügung. Sie können eine API verwenden, die der Lua-String-API ähnelt, um den TCP-Datenstrom zu analysieren.

Zu den nützlichen APIs gehören:

```
data:len()
```

```
data:find()
```

```
data:byte()
```

```
data:sub()
```

```
data:split()
```

Sobald der TCP-Datenstrom in eine Protokollnachricht geparst wurde, erreicht der Benutzercode den Lastenausgleich, indem er die Protokollnachricht einfach an den nächsten verfügbaren Kontext aus dem Kontext sendet, der an den on_data-Callback für den Client übergeben wurde.

Die ns.send () API wird verwendet, um Nachrichten an andere Verarbeitungsmodule zu senden. Zusätzlich zum Zielkontext verwendet die Sende-API den Eventnamen und die optionale Payload als Argumente. Es besteht eine Eins-zu-Eins-Entsprechung zwischen dem Eventnamen und den Namen der Callback-Funktionen für die Verhaltensweisen. <event_name>Die Callbacks für Ereignisse werden on_ aufgerufen. Die Callback-Namen verwenden nur Kleinbuchstaben.

Beispielsweise sind die on_data-Callbacks des TCP-Clients und des Servers benutzerdefinierte Handler für Ereignisse mit dem Namen „DATA“. Um die gesamte Protokollnachricht in einem Sendeaufruf zu senden, wird das EOM-Ereignis verwendet. EOM, das für Ende der Nachricht steht, bedeutet das Ende der Protokollnachricht an den LB-Kontext im Downstream, sodass für Daten, die auf diese Nachricht folgen, eine neue Load-Balancing-Entscheidung getroffen wird.

Der Erweiterungscode empfängt im Ereignis on_data manchmal nicht die gesamte Protokollnachricht. In einem solchen Fall können die Daten mithilfe der ctxt:hold () -API gespeichert werden.

Die Hold-API ist sowohl für TCP-Client- als auch für Server-Callback-Kontexte verfügbar. Wenn „Mit Daten speichern“ aufgerufen wird, werden die Daten im Kontext gespeichert. Wenn mehr Daten im gleichen Kontext empfangen werden, werden die neu empfangenen Daten an die zuvor gespeicherten Daten angehängt und die on_data Callback-Funktion wird erneut mit den kombinierten Daten aufgerufen.

Hinweis: Die verwendete Lastausgleichsmethode hängt von der Konfiguration des virtuellen Lastausgleichsservers ab, die dem Lastausgleichskontext entspricht.

Der folgende Codeausschnitt zeigt die Verwendung der Sende-API zum Senden der geparsten Protokollnachricht.

Beispiel:

```
    function client.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to lb
        ns.send(ctxt.output, "EOM", {
 data = message }
 )
    end -- client.on_data

    function server.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to client
        ns.send(ctxt.output, "EOM", {
 data = message }
 )

    end -- server.on_data
<!--NeedCopy-->
```

Streamen

In einigen Szenarien ist es möglicherweise nicht erforderlich, den TCP-Datenstrom so lange zu halten, bis die gesamte Protokollnachricht erfasst ist. Tatsächlich wird es nicht empfohlen, es sei denn, es ist erforderlich. Das Speichern der Daten erhöht die Speichernutzung auf der NetScaler-Appliance und kann die Appliance anfällig für DDoS-Angriffe machen, da der Speicher der NetScaler-Appliance mit unvollständigen Protokollmeldungen auf vielen Verbindungen erschöpft wird.

Benutzer können TCP-Daten in den Callback-Handlern der Erweiterung streamen, indem sie die Sende-API verwenden. Anstatt die Daten so lange zu speichern, bis die gesamte Nachricht erfasst ist, können Daten in Blöcken gesendet werden. Beim Senden von Daten an ctxt.output mithilfe des DATA-Ereignisses wird eine teilweise Protokollnachricht gesendet. Darauf können weitere DATA-Ereignisse folgen. Ein EOM-Ereignis muss gesendet werden, um das Ende der Protokollnachricht zu markieren. Der nachgeschaltete Load-Balancing-Kontext trifft die Lastausgleichsentscheidung für die ersten empfangenen Daten. Nach Erhalt der EOM-Nachricht wird eine neue Load-Balancing-Entscheidung getroffen.

Um Protokollnachrichtendaten zu streamen, senden Sie mehrere DATA-Ereignisse, gefolgt von einem EOM-Ereignis. Die aufeinanderfolgenden DATA-Ereignisse und das folgende EOM-Ereignis werden an dieselbe Serververbindung gesendet, die per Lastausgleichsentscheidung für das erste DATA-Ereignis in der Sequenz ausgewählt wurde.

Bei einem Send-to-Client-Kontext sind EOM- und DATA-Ereignisse praktisch identisch, da es für EOM-Ereignisse keine spezielle Behandlung durch den nachgeschalteten Client-Kontext gibt.

Token-basierter Lastenausgleich

Für nativ unterstützte Protokolle unterstützt eine NetScaler-Appliance eine tokenbasierte Load-Balancing-Methode, die PI-Ausdrücke verwendet, um das Token zu erstellen. Bei Erweiterungen ist das Protokoll nicht im Voraus bekannt, sodass PI-Ausdrücke nicht verwendet werden können. Für den tokenbasierten Lastenausgleich müssen Sie den standardmäßigen virtuellen Lastausgleichsserver so einrichten, dass er die USER_TOKEN-Load-Balancing-Methode verwendet, und den Token-Wert aus dem Erweiterungscode angeben, indem Sie die Sende-API mit einem Feld user_token aufrufen. Wenn der Token-Wert von der Sende-API gesendet wird und die USER_TOKEN-Ladausgleichsmethode auf dem virtuellen Standardserver für den Lastausgleich konfiguriert ist, wird die Lastausgleichsentscheidung getroffen, indem ein Hash auf der Grundlage des Tokenwerts berechnet wird. Die maximale Länge des Tokenwerts beträgt 64 Byte.

```
add lb vserver v\\_mqttlb USER\\_TCP -lbMethod USER\\_TOKEN
```

Der Codeausschnitt im folgenden Beispiel verwendet eine Sende-API, um einen LB-Tokenwert zu senden.

Beispiel:

```
1          -- send the message to lb
2
3
4
5
6          -- user_token is set to do LB based on clientID
7
```



```
8
9
10
11          ns.send(ctxt.output, "EOM", {
12   data = message,
13
14                                      user_token = token_info }
15   )
16  <!--NeedCopy-->
```

Persistenz beim Lastenausgleich

Die Persistenz des Load-Balancings steht in engem Zusammenhang mit dem tokenbasierten Load Balancing. Benutzer müssen in der Lage sein, den Wert der Persistenzsitzung programmgesteuert zu berechnen und ihn für die Persistenz beim Load Balancing zu verwenden. Die Sende-API wird verwendet, um Persistenzparameter zu senden. Um die Load Balancing-Persistenz zu verwenden, müssen Sie den Persistenztyp USERSESSION auf dem virtuellen Standardserver für den Lastausgleich festlegen und einen Persistenzparameter aus dem Erweiterungscode bereitstellen, indem Sie die Sende-API mit einem Feld user_session aufrufen. Die maximale Länge des Persistenzparameterwerts beträgt 64 Byte.

Wenn Sie mehrere Persistenztypen für ein benutzerdefiniertes Protokoll benötigen, müssen Sie Benutzerpersistentypen definieren und konfigurieren. Die Namen der Parameter, die zur Konfiguration der virtuellen Server verwendet werden, werden vom Protokollimplementer festgelegt. Der konfigurierte Wert eines Parameters ist auch für den Erweiterungscode verfügbar.

Die folgende CLI und Codeausschnitt zeigen die Verwendung einer Sende-API zur Unterstützung der Persistenz des Lastenausgleichs. Die Codeauflistung im Abschnitt Codeauflistung für mqtt.lua veranschaulicht auch die Verwendung des Feldes user_session.

Für die Persistenz müssen Sie den Persistenztyp USERSESSION auf dem virtuellen Lastausgleichsserver angeben und den Wert user_session von der ns.send API übergeben.

```
add lb vserver v\\_mqttlb USER\\_TCP -persistencetype USERSESSION
```

Senden Sie die MQTT-Nachricht an den Load Balancer, wobei das Feld user_session in der Payload auf clientID gesetzt ist.

Beispiel:

```
1  -- send the data so far to lb
2
3  -- user_session is set to clientID as well (it will be used to persist
       session)
4
```



```
ns.send(ctxt.output,  “DATA” , {
 data = data, user_session = clientID }
 )
<!--NeedCopy-->
```

Auf TCP-Verbindungen basierender Lastenausgleich

Für einige Protokolle ist MBLB möglicherweise nicht erforderlich. Stattdessen benötigen Sie möglicherweise einen auf TCP-Verbindungen basierenden Lastenausgleich. Beispielsweise muss das MQTT-Protokoll den ersten Teil des TCP-Streams analysieren, um das Token für den Lastenausgleich zu ermitteln. Und alle MQTT-Nachrichten auf derselben TCP-Verbindung müssen an dieselbe Serververbindung gesendet werden.

Ein auf TCP-Verbindungen basierender Lastenausgleich kann erreicht werden, indem die Sende-API nur mit DATA-Ereignissen verwendet wird und kein EOM gesendet wird. Auf diese Weise stützt der Downstream-Load-Balancing-Kontext die Lastausgleichsentscheidung auf die zuerst empfangenen Daten und sendet alle nachfolgenden Daten an dieselbe Serververbindung, die durch die Lastausgleichsentscheidung ausgewählt wurde.

In einigen Anwendungsfällen ist es möglicherweise auch erforderlich, die Bearbeitung von Erweiterungen zu Bypass, nachdem die Entscheidung für den Lastenausgleich getroffen wurde. Das Umgehen der Nebenstellenaufrufe führt zu einer besseren Leistung, da der Datenverkehr ausschließlich durch systemeigenen Code verarbeitet wird. Die Umgehung kann mithilfe der ns.pipe () -API erfolgen. Ein Aufruf des Pipe () API-Erweiterungscodes kann den Eingabekontext mit einem Ausgabekontext verbinden. Nach dem Aufruf von pipe () gehen alle Ereignisse, die aus dem Eingabekontext kommen, direkt in den Ausgabekontext. Tatsächlich wird das Modul, von dem aus der pipe () -Aufruf erfolgt, aus der Pipeline entfernt.

Das folgende Code-Snippet zeigt Streaming und die Verwendung der pipe () API, um ein Modul zu umgehen. Die Codeauflistung im Abschnitt Codeauflistung für mqtt.lua veranschaulicht auch, wie man Streaming und die Verwendung der pipe () API verwendet, um das Modul für den Rest des Datenverkehrs auf der Verbindung zu Bypass.

Beispiel:

```
        -- send the data so far to lb
        ns.send(ctxt.output, "DATA", {
  data = data,
                                      user_token = clientID }
  )
        -- pipe the subsequent traffic to the lb - to bypass the client
            on_data handler
        ns.pipe(ctxt.input, ctxt.output)
```



```
<!--NeedCopy-->
```

Inhaltsbasierter Lastenausgleich

Bei nativen Protokollen wird die Funktion zum Content Switching wie bei Protokollerweiterungen unterstützt. Mit dieser Funktion können Sie die Daten an den ausgewählten Load Balancer senden, anstatt die Daten an den Standard-Load Balancer zu senden.

Die Funktion zum Umschalten von Inhalten für Protokollerweiterungen wird mithilfe der ctxt:lb_connect () -API erreicht.<lbname> Diese API ist für den TCP-Clientkontext verfügbar. Mithilfe dieser API kann der Erweiterungscode einen Lastausgleichskontext abrufen, der einem bereits konfigurierten virtuellen Load-Balancing-Server entspricht. Sie können dann die Sende-API mit dem so erhaltenen Load-Balancing-Kontext verwenden.

Der LB-Kontext kann manchmal NULL sein:

- Virtueller Server ist nicht vorhanden
- Der virtuelle Server ist nicht vom Typ Benutzerprotokoll
- Der Status des virtuellen Servers ist nicht UP
- Der virtuelle Server ist ein virtueller Benutzerserver, kein virtueller Lastausgleichsserver

Wenn Sie den virtuellen Ziel-Lastausgleichsserver entfernen, während er verwendet wird, werden alle mit diesem virtuellen Lastausgleichsserver verknüpften Verbindungen zurückgesetzt.

Der folgende Codeausschnitt zeigt die Verwendung der lb_connect () -API. Der Code ordnet die Client-ID mithilfe der Lua-Tabelle lb_map den Namen virtueller Load-Balancing-Server (lbname) zu und ruft dann mit lb_connect () den LB-Kontext für lbname ab. Und schließlich sendet es mithilfe der Send-API an den LB-Kontext.

```
    local lb_map = {

       ["client1*"] = "lb_1",
       ["client2*"] = "lb_2",
       ["client3*"] = "lb_3",
       ["client4*"] = "lb_4"
     }


    -- map the clientID to the corresponding LB vserver and connect to
       it
    for client_pattern, lbname in pairs(lb_map) do
       local match_idx = string.find(clientID, client_pattern)
       if (match_idx == 1) then
      lb_ctxt = ctxt:lb_connect(lbname)
      if (lb_ctxt == nil) then
```



```
16          error("Failed to connect to LB vserver: " .. lbname)
17       end
18       break
19        end
20     end
21     if (lb_ctxt == nil) then
22     -- If lb context is NULL, the user can raise an error or send data
          to default LB
23        error("Failed to map LB vserver for client: " .. clientID)
24     end
25 -- send the data so far to lb
26 ns.send(lb_ctxt, "DATA", {
27  data = data }
28
29 <!--NeedCopy-->
```

SSL

SSL für Protokolle, die Erweiterungen verwenden, wird auf ähnliche Weise unterstützt, wie SSL für native Protokolle unterstützt wird. Mit demselben Parsing-Code für die Erstellung benutzerdefinierter Protokolle können Sie eine Protokollinstanz über TCP oder über SSL erstellen, die dann zur Konfiguration der virtuellen Server verwendet werden kann. Ebenso können Sie Benutzerdienste über TCP oder SSL hinzufügen.

Weitere Informationen finden Sie unter Konfigurieren von SSL-Offloading für MQTT und Konfigurieren von SSL-Offloading für MQTT mit End-to-End-Verschlüsselung.

Serververbindungs-Multiplexing

Manchmal sendet der Client jeweils eine Anfrage und sendet die nächste Anfrage erst, nachdem die Antwort für die erste Anfrage vom Server empfangen wurde. In einem solchen Fall kann die Serververbindung für andere Client-Verbindungen und für die nächste Nachricht auf derselben Verbindung wiederverwendet werden, nachdem die Antwort an den Client gesendet wurde. Um die Wiederverwendung der Serververbindung durch andere Client-Verbindungen zu ermöglichen, müssen Sie die API ctxt: reuse_server_connection () im serverseitigen Kontext verwenden.

Hinweis: Diese API ist in NetScaler 12.1 Build 49.xx und höher verfügbar.

Verkehr ändern

Um Daten in der Anfrage oder Antwort zu ändern, müssen Sie die systemeigene Rewrite-Funktion verwenden, die einen erweiterten Policy-PI-Ausdruck verwendet. Da Sie PI-Ausdrücke in Erweiterungen

nicht verwenden können, können Sie die folgenden APIs verwenden, um TCP-Streamdaten zu ändern.

```
data:replace(offset, length, new_string)
data:insert(offset, new_string)
data:delete(offset, length)
data:gsub(pattern, replace [,n]))
```

Das folgende Code-Snippet zeigt die Verwendung von replace () API.

```
-- Get the offset of the pattern, we want to replace
   local old_pattern =  "pattern to repalace"
local old_pattern_length = old_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
    goto send_data
   end
  -- If the data we want to modify is not completely present, then
  -- wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
data:replace(pat_off, old_pattern_length,  "new pattern" )
::send_data::
ns.send(ctxt.output,  "EOM" , {
 data = data }
 )
::done::
```

Das folgende Code-Snippet zeigt die Verwendung von insert () API.

```
data:insert(5,  "pattern to insert" )
```

Das folgende Code-Snippet zeigt die Verwendung von insert () API, wenn wir nach oder vor einem Muster einfügen möchten:

```
-- Get the offset of the pattern, after or before which we want to
    insert
   local pattern =  "pattern after/before which we need to insert"
local pattern_length = pattern:len()
   local pat_off, pat_end = data:find(pattern)
-- pattern is not present
   if (not pat_off) then
```



```
    goto send_data
   end
  -- If the pattern after which we want to insert is not
  -- completely present, then wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
-- Insert after the pattern
data:insert(pat_end + 1,  “pattern to insert” )
   -- Insert before the pattern
data:insert(pat_off,  “pattern to insert” )
::send_data::
    ns.send(ctxt.output,  “EOM” , {
 data = data }
 )
::done::
```

Das folgende Code-Snippet zeigt die Verwendung von delete () API.

```
-- Get the offset of the pattern, we want to delete
   local delete_pattern =  “pattern to delete”
local delete_pattern_length = delete_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
          goto send_data
   end
  -- If the data we want to delete is not completely present,
  -- then wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
    goto done
  end
data:delete(pat_off, delete_pattern_length)
::send_data::
ns.send(ctxt.output,  “EOM” , {
 data = data }
 )
::done::
```

Das folgende Code-Snippet zeigt die Verwendung von gsub () API.


```
    -- Replace all the instances of the pattern with the new string
data:gsub( “old pattern” , “new string” )
-- Replace only 2 instances of “old pattern”
data:gsub( “old pattern” , “new string” , 2)
-- Insert new_string before all instances of “http”
data:gsub( “input data” , “(http)” , “new_string%1” )
-- Insert new_string after all instances of “http”
data:gsub( “input data” , “(http)” , “%1new_string” )
-- Insert new_string before only 2 instances of “http”
data:gsub( “input data” , “(http)” , “new_string%1” , 2)
```

Hinweis: Diese API ist in NetScaler 12.1 Build 50.xx und höher verfügbar.

Versenden Sie den Datenverkehr zum Client oder Server

Sie können die ns.send () -API verwenden, um Daten, die aus dem Erweiterungscode stammen, an einen Client und einen Backend-Server zu senden. Um eine Antwort direkt mit einem Client aus dem Client-Kontext zu senden oder zu empfangen, müssen Sie ctxt.client als Ziel verwenden. Um eine Antwort direkt mit einem Backend-Server aus dem Serverkontext zu senden oder zu empfangen, müssen Sie ctxt.server als Ziel verwenden. Die Daten in der Payload können TCP-Stream-Daten oder eine Lua-Zeichenfolge sein.

Um die Verarbeitung des Datenverkehrs auf einer Verbindung zu beenden, können Sie die ctxt:close () -API entweder vom Client- oder vom Serverkontext aus verwenden. Diese API schließt die clientseitige Verbindung oder alle damit verknüpften Serververbindungen.

Wenn Sie die ctxt:close () -API aufrufen, sendet der Erweiterungscode ein TCP-FIN-Paket an die Client- und Serververbindungen. Wenn über diese Verbindung mehr Daten vom Client oder Server empfangen werden, setzt die Appliance die Verbindung zurück.

Das folgende Codeausschnitt zeigt die Verwendung von ctxt.client und ctxt:close () APIs.

```
    -- If the input packet is not MQTT CONNECT type, then
-- send some error response to the client.
function client.on_data(ctxt, payload)
    local data = payload.data
    local offset = 1
    local msg_type = 0
    local error_response = “Missing MQTT Connect packet.”
    byte = data:byte(offset)
msg_type = bit32.rshift(byte, 4)
if (msg_type ~= 1) then
-- Send the error response
   ns.send(ctxt.client, “DATA” , {
```



```
 data = error_response }
 )
-- Since error response has been sent, so now close the connection
    ctxt:close()
end
```

Der folgende Codeausschnitt zeigt das Beispiel, wenn der Benutzer die Daten in den normalen Verkehrsfluss injizieren kann.

```
-- After sending request, send some log message to the server.
function client.on_data(ctxt, payload)
local data = payload.data
local log_message =  “client id :  “..data:sub(3, 7)..”  user name :  “
    data:sub(9, 15)
-- Send the request we get from the client to backend server
ns.send(ctxt.output,  “DATA” , {
 data = data }
 )
After sending the request, also send the log message
ns.send(ctxt.output,  “DATA” , {
 data = log_message”  }
 )
end
```

Der folgende Codeausschnitt zeigt die Verwendung der ctxt.to_server API.

```
-- If the HTTP response status message is  “Not Found” ,
-- then send another request to the server.
function server.on_data(ctxt, payload)
    local data = payload.data
    local request  “GET /default.html HTTP/1.1\r\n\r\n” ss
    local start, end = data:find( “Not Found” )
    if (start) then
    -- Send the another request to server
        ns.send(ctxt.server,  “DATA” , {
 data = request }
 )
end
```

Hinweis: Diese API ist in NetScaler 12.1 Build 50.xx und höher verfügbar.

Datenverarbeitung beim Verbindungsaufbau

Es kann einen Anwendungsfall geben, in dem Sie einige Daten beim Verbindungsaufbau senden möchten (wenn das endgültige ACK empfangen wird). Im Proxyprotokoll möchten Sie beispielsweise die Quell- und Ziel-IP-Adressen und -Ports des Clients beim Verbindungsaufbau an den Backend-Server senden. In diesem Fall können Sie den Callback-Handler client.init () verwenden, um die Daten beim Verbindungsaufbau zu senden.

Der folgende Codeausschnitt zeigt die Verwendung von client.init() Callback:

```
1 -- Send a request to the next processing context
2 -- on the connection establishment.
3 function client.init(ctxt)
4    local request  “PROXY TCP4”  + ctxt.client.ip.src.to_s +  “  “ +
        ctxt.client.ip.dst.to_s +  “  “ + ctxt.client.tcp.srcport +  “  “
         +     ctxt.client.tcp.dstport
5 -- Send the another request to server
6    ns.send(ctxt.output,  “DATA” , {
7  data = request }
8  )
9   end
```

Hinweis: Diese API ist in NetScaler 13.0 Build xx.xx und höher verfügbar.

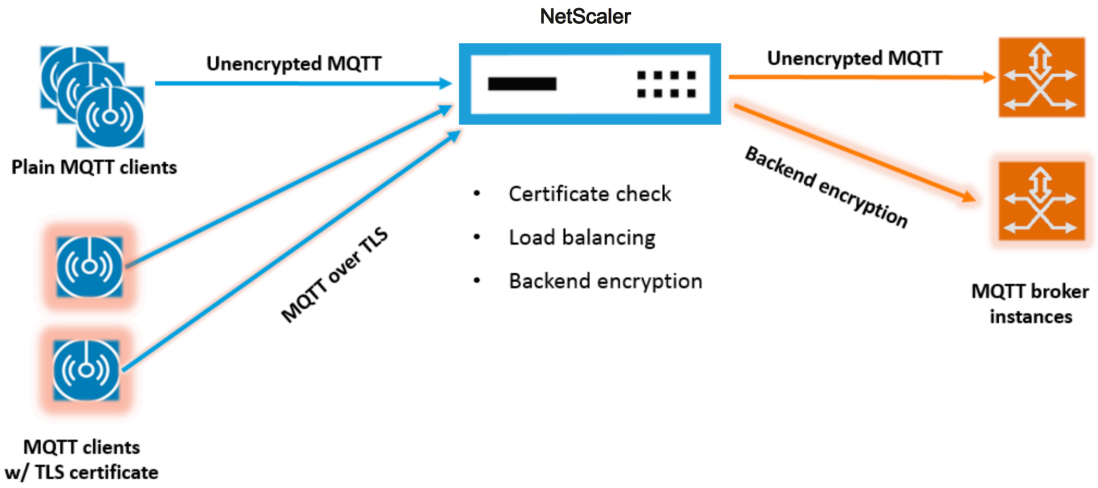
Tutorial — MQTT-Protokoll zur NetScaler-Appliance mit Protokollerweiterungen hinzufügen

May 11, 2023

Die Befehle der Befehlszeilenschnittstelle (CLI) für benutzerdefinierte Protokolle verwenden das Schlüsselwort „user“, um den benutzerdefinierten Charakter der zugrunde liegenden Konfigurationsentitäten zu kennzeichnen. Mit Hilfe von Erweiterungscode können Sie dem System ein neues Benutzerprotokoll hinzufügen und virtuelle Benutzerserver für benutzerdefinierte Protokolle hinzufügen. Die virtuellen Benutzerserver sind wiederum konfigurierbar, indem Parameter festgelegt werden. Konfigurierte Werte für virtuelle Serverparameter sind im Erweiterungscode verfügbar.

Das MQTT-Protokoll wird zur Veranschaulichung verwendet.

Das folgende Diagramm zeigt eine NetScaler-Appliance sowie MQTT-Client- und Broker-Tools.



Codeauflistung für mqtt.lua

May 11, 2023

Die folgende Codeliste, mqtt.lua, enthält den Code zur Implementierung des MQTT-Protokolls auf NetScaler mithilfe von Protokollerweiterungen. Im Code ist nur die TCP-Client-Daten-Callback-Funktion definiert - client.on_data (). Für Serverdaten wird keine Callback-Funktion hinzugefügt und der Server zum Client verwendet den schnellen nativen Pfad. Für Client-Daten analysiert der Code die CONNECT MQTT-Protokollnachricht und extrahiert die ClientID. Anschließend verwendet es den Wert clientId for user_token, der verwendet wird, um den gesamten Client-Verkehr für die Verbindung auf der Grundlage der ClientID auszubalancieren, indem die LB-Methode für den LB-vserver auf USER_TOKEN festgelegt wird. Es verwendet die ClientID auch für den Wert user_session, der für die LB-Persistenz verwendet werden kann, indem der Persistenztyp für den LB-vserver auf USERSESSION festgelegt wird. Der Code verwendet ns.send (), um LB auszuführen und die Anfangsdaten zu senden. Es verwendet die ns.pipe () API, um den Rest des Clientdatenverkehrs direkt an die Serververbindung zu senden, wobei Aufrufe an den Extension-Callback-Handler umgangen werden.

```
--[[

  MQTT event handler for TCP client data

    ctxt - TCP client side App processing context.

    data - TCP Data stream received.

    - parse the client ID from the connect message - the first message
       should be connect
```



```
10
11      - send the data to LB with ClientID as user token and session
12
13      - pipe the subsequent data to LB directly. This way the subsequent
            MQTT traffic will
14
15        bypass the tcp client on_data handler
16
17      - if a parse error is seen, throw an error so the connection is
            reset
18
19  --]]
20
21  function client.on_data(ctxt, payload)
22
23      local data = payload.data
24
25      local data_len = data:len()
26
27      local offset = 1
28
29      local byte = nil
30
31      local utf8_str_len = 0
32
33      local msg_type = 0
34
35      local multiplier = 1
36
37      local max_multiplier = 128 * 128 * 128
38
39      local rem_length = 0
40
41      local clientID = nil
42
43      -- check if MQTT fixed header is present (fixed header length is
            atleast 2 bytes)
44
45      if (data_len < 2) then
46
47          goto need_more_data
48
49      end
50
51      byte = data:byte(offset)
```



```
52
53      offset = offset + 1
54
55         -- check for connect packet - type value 1
56
57      msg_type = bit32.rshift(byte, 4)
58
59      if (msg_type ~= 1) then
60
61          error("Missing MQTT Connect packet.")
62
63      end
64
65      -- parse the remaining length
66
67      repeat
68
69          if (multiplier > max_multiplier) then
70
71             error("MQTT CONNECT packet parse error - invalid Remaining
                  Length.")
72
73         end
74
75         if (data_len < offset) then
76
77            goto need_more_data
78
79         end
80
81         byte = data:byte(offset)
82
83         offset = offset + 1
84
85         rem_length = rem_length + (bit32.band(byte, 0x7F) * multiplier)
86
87         multiplier = multiplier * 128
88
89      until (bit32.band(byte, 0x80) == 0)
90
91      -- protocol name
92
93      -- check if protocol name length is present
94
95      if (data_len < offset + 1) then
```



```
96
97          goto need_more_data
98
99       end
100
101      -- protocol name length MSB
102
103      byte = data:byte(offset)
104
105      offset = offset + 1
106
107      utf8_str_len = byte * 256
108
109      -- length LSB
110
111      byte = data:byte(offset)
112
113      offset = offset + 1
114
115      utf8_str_len = utf8_str_len + byte
116
117         -- skip the variable header for connect message
118
119      -- the four required fields (protocol name, protocol level, connect
             flags, keep alive)
120
121      offset = offset + utf8_str_len + 4
122
123      -- parse the client ID
124
125      --
126
127      -- check if client ID len is present
128
129      if (data_len < offset + 1) then
130
131         goto need_more_data
132
133      end
134
135         -- client ID length MSB
136
137      byte = data:byte(offset)
138
139      offset = offset + 1
```



```
140
141     utf8_str_len = byte * 256
142
143     -- length LSB
144
145     byte = data:byte(offset)
146
147     offset = offset + 1
148
149     utf8_str_len = utf8_str_len + byte
150
151     if (data_len < (offset + utf8_str_len - 1)) then
152
153         goto need_more_data
154
155     end
156
157     clientID = data:sub(offset, offset + utf8_str_len - 1)
158
159     -- send the data so far to lb, user_token is set to do LB based on
           clientID
160
161     -- user_session is set to clientID as well (it will be used to
           persist session)
162
163     ns.send(ctxt.output, "DATA", {
164 data = data,
165
166                                 user_token = clientID,
167
168                                 user_session = clientID }
169 )
170
171        -- pipe the subsequent traffic to the lb - to bypass the
              extension handler
172
173     ns.pipe(ctxt.input, ctxt.output)
174
175     goto parse_done
176
177     ::need_more_data::
178
179     ctxt:hold(data)
180
181     ::parse_done::
```



```
182
183     return
184
185 end
186 <!--NeedCopy-->
```

MQTT über Protokollerweiterungen konfigurieren

May 11, 2023

Die folgenden Schritte fügen der NetScaler-Appliance ein MQTT-Protokoll hinzu.

Importieren Sie die Erweiterungsdatei von einem Webserver (über HTTP) oder Ihrer lokalen Workstation in die NetScaler Appliance. Weitere Informationen zum Importieren der Erweiterungsdatei finden Sie unter Importieren von Erweiterungen.

```
import ns extension local:mqtt_generic_fs.lua mqtt_code
```

Fügen Sie dem System mithilfe der Erweiterung ein neues TCP-basiertes Benutzerprotokoll hinzu.

```
add user protocol MQTT -transport TCP -extension mqtt_code
```

Fügen Sie einen Dienst vom Typ USER_TCP hinzu, um anzugeben, dass es sich um ein benutzerdefiniertes Protokoll handelt.

```
add service s1 10.102.90.112 USER_TCP 80
```

Fügen Sie einen vServer für den Benutzerlastenausgleich hinzu und binden Sie Backend-Dienste daran.

```
add lb vs mysv USER_TCP
```

```
bind lb vs mysv s1
```

Fügen Sie einen virtuellen Benutzerserver für das neu hinzugefügte Protokoll hinzu und machen Sie den im vorherigen Schritt konfigurierten virtuellen Load Balancing-Server zum Standard-Load Balancer.

```
add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv
```

Aktivieren Sie optional die MQTT-Sitzungspersistenz basierend auf ClientID und legen Sie den Persistenztyp auf USERSESSION fest.

```
set lb vserver mqtt_lb -persistenceType USERSESSION
```


SSL-Offloading für MQTT konfigurieren

May 11, 2023

Sie können SSL-Offloading für Benutzerprotokolle implementieren, indem Sie eine SSL-Instanz für das Protokoll hinzufügen. Das folgende Beispiel zeigt, wie SSL-Offloading für ein Benutzerprotokoll durchgeführt wird. Der Datenverkehr zu den Backend-Diensten ist bei dieser Konfiguration unverschlüsselt.

Hinweis: Dieses Beispiel enthält keine Details zum Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars und zum Binden an einen virtuellen Server. Weitere Informationen finden Sie unter SSL-Zertifikate.

Die folgenden Befehle fügen das MQTT_SSL-Protokoll hinzu, indem mqtt.lua mit dem Transportwert SSL eingefügt wird.

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```

Mit den folgenden Befehlen wird ein virtueller Server für den Benutzerlastenausgleich hinzugefügt und Backend-Dienste daran gebunden.

```
add service mqtt_svr1 10.217.24.48 USER_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_TCP 1502
add lb vserver mqtt_lb USER_TCP  - lbMethod ROUNDROBIN
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

Der folgende Befehl fügt einen virtuellen Benutzerserver für das neu hinzugefügte Protokoll MQTT_SSL hinzu. Die Verwendung von MQTT_SSL bedeutet, dass die NetScaler-Appliance SSL-Offloading vornimmt, da MQTT_SSL mit SSL-Transport konfiguriert wurde. Mit dem Befehl wird die Standardeinstellung auch auf den virtuellen Load-Balancing-Server festgelegt, der im vorherigen Schritt konfiguriert wurde.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Für das SSL-Offloading müssen Sie außerdem die SSL-Funktion aktivieren und einen Certkey an den virtuellen Benutzerserver binden. Weitere Informationen finden Sie in den folgenden Artikeln:

Hinzufügen oder Aktualisieren eines Zertifikatsschlüsselpaars

Binden Sie das Zertifikatschlüsselpaar an den virtuellen SSL-Server

Beispiel:


```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Konfiguration von SSL-Offloading mit Ende-zu-Ende-Verschlüsselung für MQTT

May 11, 2023

Das folgende Beispiel zeigt, wie SSL-Offloading für MQTT mit Ende-zu-Ende-Verschlüsselung durchgeführt wird.

Hinweis: Dieses Beispiel enthält keine Details zum Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars und zum Binden an einen virtuellen Server. Weitere Informationen finden Sie unter SSL-Zertifikate.

Die folgenden Befehle importieren die Erweiterungsdatei und fügen Sie das MQTT_SSL-Protokoll mit SSL-Transport hinzu.

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```

Mit den folgenden Befehlen wird ein virtueller Server für den Benutzerlastenausgleich hinzugefügt und Backend-Dienste daran gebunden. Sowohl der virtuelle Load Balancing-Server als auch die Dienste sind für den Diensttyp USER_SSL_TCP konfiguriert.

```
add service mqtt_svr1 10.217.24.48 USER_SSL_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_SSL_TCP 1502
add lb vserver mqtt_lb USER_SSL_TCP  - lbmethod RR
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

Der folgende Befehl fügt einen virtuellen Benutzerserver für das neu hinzugefügte Protokoll MQTT_SSL hinzu. Die Verwendung von MQTT_SSL bedeutet, dass die NetScaler-Appliance SSL-Offloading vornimmt, da MQTT_SSL mit SSL-Transport konfiguriert wurde. Der Befehl macht

auch den virtuellen Load Balancing-Server, der im vorherigen Schritt konfiguriert wurde, zum Standard-Load Balancer.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Für die Ende-zu-Ende-Verschlüsselung müssen Sie außerdem die SSL-Funktion aktivieren und einen Certkey an den Benutzer und die virtuellen Standardserver für den Lastausgleich binden. Weitere Informationen finden Sie in den folgenden Artikeln:

Hinzufügen oder Aktualisieren eines Zertifikatsschlüsselpaars

Binden Sie das Zertifikatschlüsselpaar an den virtuellen SSL-Server

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_lb  -certkeyName mqtt_svr_cert_key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Tutorial — Lastausgleich von Syslog-Meldungen mithilfe von Protokollerweiterungen

May 11, 2023

Das auf der NetScaler-Appliance verfügbare Syslog-Protokoll funktioniert nur für die auf der NetScaler-Appliance generierten Nachrichten. Es führt keinen Lastenausgleich für die von externen Knoten kommenden Nachrichten durch. Um den Lastenausgleich solcher Nachrichten zu erreichen, müssen Sie die Funktion für Protokollerweiterungen verwenden und die Logik zum Analysieren von Syslog-Nachrichten mithilfe der Programmiersprache Lua 5.2 schreiben.

Code zum Analysieren von Syslog-Nachrichten

Im Code ist nur die TCP-Client-Daten-Callback-Funktion definiert - client.on_data (). Für Serverdaten wird keine Callback-Funktion hinzugefügt und der Server zum Client verwendet den schnellen nativen Pfad. Der Code identifiziert die Nachrichtengrenze anhand des nachfolgenden Zeichens. Wenn das TCP-Paket mehr als eine Syslog-Nachrichten enthält, teilen wir das Paket basierend auf dem nachfolgenden Zeichen und Lastverteilung jeder Nachricht.

```
--[[
```



```
2
3   Syslog event handler for TCP client data
4
5     ctxt - TCP client side App processing context.
6
7     data - TCP Data stream received.
8
9  --]]
10
11 function client.on_data(ctxt, payload)
12
13                   local message = nil
14
15                   local data_len
16
17                   local data = payload.data
18
19                   local trailing_character = "\n"
20
21                   ::split_message::
22
23                                       -- Get the offset of trailing
                                            character
24
25                                       local new_line_character_offset =
                                            data:find(trailing_character)
26
27                                       -- If trailing character is not
                                            found, then wait for more data.
28
29                                       if (not new_line_character_offset)
                                            then
30
31                                                           goto
                                                               need_more_data
32
33                                       end
34
35                                       -- Get the length of the current
                                            message
36
37                                       data_len = data:len()
38
39                                       -- Check whether we have more than
                                            one message
```



```
40
41                                      -- by comparing trailing character
                                           offset and
42
43                                      -- current data length
44
45                                      if (data_len >
                                           new_line_character_offset) then
46
47                                                      -- If we have
                                                         more than one
                                                         message, then
                                                         split
48
49                                                      -- the data into
                                                         two parts such
                                                          that first
                                                         part
50
51                                                      -- will contain
                                                         message upto
                                                         trailing
                                                         character
52
53                                                      -- offset and
                                                         second part
                                                         will contain
54
55                                                      -- remaining
                                                         message.
56
57                                                      message, data =
                                                         data:split(
                                                         new_line_character_offse
                                                         )
58
59                                      else
60
61                                                      message = data
62
63                                                      data = nil
64
65                                      end
66
67  -- Send the data to the backend server.
```



```
68
69                                      ns.send(ctxt.output, "EOM", {
70   data = message }
71   )
72
73                                      goto done
74
75                                      ::need_more_data::
76
77                                                      -- Wait for more
                                                           data
78
79                                                      ctxt:hold(data)
80
81                                                      data = nil
82
83                                                      goto done
84
85                                      ::done::
86
87                                                      -- If we have
                                                           more data to
                                                           parse,
88
89                                                      -- then do
                                                           parsing again.
90
91                                                      if (data) then
92
93                                                                      goto
                                                                          split_
94
95                                                      end
96
97 end
98 <!--NeedCopy-->
```


Konfiguration des Syslog-Protokolls mithilfe von Protokollerweiterungen

May 11, 2023

Die folgenden Schritte fügen der NetScaler-Appliance ein Benutzer-SYSLOG-Protokoll hinzu.

Importieren Sie die Erweiterungsdatei von einem Webserver (über HTTP) oder Ihrer lokalen Workstation in die NetScaler Appliance. Weitere Informationen zum Importieren der Erweiterungsdatei finden Sie unter Erweiterungen importieren.

```
import ns extension local:syslog_parser.lua syslog_parser_code
```

Fügen Sie dem System mithilfe der Erweiterung ein neues TCP-basiertes Benutzerprotokoll hinzu.

```
add user protocol USER_SYSLOG -transport TCP -extension syslog_parser_code
```

Fügen Sie einen Dienst vom Typ USER_TCP hinzu, um anzugeben, dass es sich um ein benutzerdefiniertes Protokoll handelt.

```
add service s1 10.102.90.112 USER_TCP 80
```

Fügen Sie einen vServer für den Benutzerlastenausgleich hinzu und binden Sie Backend-Dienste daran.

```
1 add lb vs mysv USER_TCP
2
3 bind lb vs mysv s1
4 <!--NeedCopy-->
```

Fügen Sie einen virtuellen Benutzerserver für das neu hinzugefügte Protokoll hinzu und machen Sie den im vorherigen Schritt konfigurierten virtuellen Load Balancing-Server zum Standard-Load Balancer.

```
add user vs v_syslog USER_SYSLOG 10.217.24.28 80 -defaultlb mysv
```

Befehlsreferenz zur Protokollerweiterungen

May 11, 2023

In der folgenden Tabelle sind alle neuen Befehle aufgeführt, die für benutzerdefinierte Protokolle hinzugefügt wurden, sowie die vorhandenen Befehle, die für benutzerdefinierte Protokolle geändert wurden.

```
show lb persistentSessions [<vserv-name>]
```


- **CLI-Befehl:**

  ```
  add user protocol <name> -transport ( TCP | SSL )-extension <string> -comment <string>]>
  ```

- **Beschreibung:**

  Fügt der NetScaler-Appliance mithilfe von Erweiterungen ein neues Benutzerprotokoll hinzu. Derzeit werden nur Benutzerprotokolle mit dem Transportwert TCP oder SSL unterstützt.

  > **Beispiel:**
  >
  > Benutzerprotokoll hinzufügen MQTT -transport TCP -extension mqtt_code

- **CLI-Befehl:**

  ```
  rm user protocol <name>
  ```

- **Beschreibung:**

  Entfernt ein Benutzerprotokoll, das zuvor der NetScaler-Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > RM-Benutzerprotokoll mqtt

- **CLI-Befehl:**

  ```
  set user protocol <name> -comment <string>
  ```

- **Beschreibung:**

  Ändert die Einstellungen für ein Benutzerprotokoll, das zuvor der NetScaler-Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > setuser protocol mqtt -comment „MQTT-Protokollimplementierung“

- **CLI-Befehl:**

  ```
  unset user protocol <name> -comment
  ```

- **Beschreibung:**

  Entfernt Einstellungen für ein Benutzerprotokoll, das zuvor der NetScaler-Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > Benutzerprotokoll unset mqtt -comment „Implementierung des MQTT-Protokolls“

- **CLI-Befehl:**

  ```
  update ns extension <extension name>
  ```


- **Beschreibung:**

  Aktualisiert die Implementierung für ein zuvor hinzugefügtes Benutzerprotokoll mithilfe von Erweiterungen.

  Sie können die Protokollimplementierung nur aktualisieren, wenn das Protokoll von keinem virtuellen Benutzerserver verwendet wird.

  > **Beispiel:**
  >
  > Aktualisierung der NS-Erweiterung my-extension

- **CLI-Befehl:**

```
add lb vserver <name> [USER_TCP | USER_SSL_TCP] [-lbmethod USER_TOKEN]
[-persistencetype USERSESSION] [-timeout <value>]
```

- **Beschreibung:**

  Fügt der NetScaler-Appliance einen virtuellen Lastausgleichsserver hinzu. Dies ist ein vorhandener CLI-Befehl.

  Für virtuelle Benutzerserver mit Lastausgleich ist der zu verwendende Diensttyp USER_TCP oder USER_SSL_TCP. Die IP-Adresse und der Port sind bei virtuellen Servern für den Benutzerlastenausgleich nicht zulässig.

  Für virtuelle Server mit Benutzerlastenausgleich ist nur die ROUNDROBIN-Load-Balancing-Methode zulässig, und der Token-Wert wird durch den Erweiterungscode bereitgestellt. Ebenso ist nur die Persistenz von USERSESSION zulässig, und die Persistenzeinstellung wird durch den Erweiterungscode bereitgestellt.

  > **Beispiel:**
  >
  > füge lb vserver mysv USER_TCP —lbmethod ROUNDROBIN hinzu

- **CLI-Befehl:**

```
add user vserver <name> <userProtocol> <IPAddress> <port> -defaultLB <
string> [-params <string>] [-comment <string>]
```

- **Beschreibung:**

  Fügt mithilfe von Erweiterungen einen virtuellen Server für ein Benutzerprotokoll hinzu. Der konfigurierte virtuelle Standardserver für den Benutzerlastenausgleich steht dem TCP-Client-Datenerweiterungshandler als ctxt.output zur Verfügung. Für einen virtuellen Server können Erweiterungsparameter mithilfe der Option -params mit einem Namen und einem Wertepaar festgelegt werden. Der entsprechende Parameterwert steht den Erweiterungshandlern als ctxt.vserver.params.<paramName> zur Verfügung.

> **Beispiel:**
>
> Benutzer hinzufügen vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv

- **CLI-Befehl:**

```
rm user vserver <name>
```

- **Beschreibung:**

  Entfernt einen virtuellen Benutzerserver, der der NetScaler-Appliance zuvor hinzugefügt wurde.

> **Beispiel:**
>
> rm user vserver v_mqtt

- **CLI-Befehl:**

```
set user vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-defaultLB
<string>] [-params <string>] [-comment <string>]
```

- **Beschreibung:**

  Ändert die Einstellungen für einen virtuellen Benutzerserver, der zuvor der NetScaler-Appliance hinzugefügt wurde. Wenn einem Erweiterungsparameter durch die Option -params ein neuer Wert zugewiesen wird, wird der alte Wert überschrieben.

> **Beispiel:**
>
> set user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment „Implementierung des MQTT-Protokolls“

- **CLI-Befehl:**

```
unset user vserver <name> [-params] [-comment]
```

- **Beschreibung:**

  Entfernt die Einstellungen für einen virtuellen Benutzerserver, der zuvor der NetScaler-Appliance hinzugefügt wurde. Wenn Sie die Option —params verwenden, um einen Erweiterungsparameter aufzuheben, wird der entsprechende Parameterwert, der für Erweiterungshandler verfügbar ist, auf Null geändert.

> **Beispiel:**
>
> unset user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment „Implementierung des MQTT-Protokolls“

- **CLI-Befehl:**

```
show user protocol [<name>]
```


- **Beschreibung:**

  Zeigt Informationen über ein Benutzerprotokoll an, z. B. Erweiterungen und Rückrufe.

  > **Beispiel:**
  >
  > Benutzerprotokoll anzeigen mqtt

- **CLI-Befehl:**

  ```
  show user vserver [<name>]
  ```

- **Beschreibung:**

  Zeigt Informationen über einen virtuellen Benutzerserver an.

  > **Beispiel:**
  >
  > zeige den Benutzer vserver vs_mqtt

- **CLI-Befehl:**

  ```
  stat user vserver [<name>]
  ```

- **Beschreibung:**

  Zeigt Statistiken über einen virtuellen Benutzerserver an.

  > **Beispiel:**
  >
  > stat user vserver vs_mqtt

- **CLI-Befehl:**

  ```
  show lb persistentSessions [<vserv-name>]
  ```

- **Beschreibung:**

  Zeigt Informationen über persistente Sitzungen an. Dies ist eine bestehende CLI. Für Benutzerprotokolle wird der Persistenztyp als USERSESSION angezeigt.

- **CLI-Befehl:**

  ```
  rm lb vserver <name>
  ```

- **Beschreibung:**

  Entfernt einen Benutzer-LB-vserver, der zuvor der NetScaler-Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > rm lb vserver mysv

- **CLI-Befehl:**

  ```
  add service <name> <IPAddr> (USER_TCP | USER_SSL_TCP)<Port>
  ```


- **Beschreibung:**

  Fügt einen Backend-Dienst hinzu, der für ein Benutzerprotokoll verwendet werden soll. Dies ist ein vorhandener CLI-Befehl mit den neuen Diensttypen USER_TCP und USER_SSL_TCP.

  > **Beispiel:**
  >
  > add service mqtt_svr1 10.217.24.48 USER_TCP 1501
  >
  > **Hinweis**: Die vorhandenen Befehle „set service und unset service“ können verwendet werden, um die Einstellungen eines zuvor hinzugefügten Dienstes für ein Benutzerprotokoll zu entfernen oder zu ändern.

- **CLI-Befehl:**

  ```
  bind lb vserver <name> <serviceName>
  ```

- **Beschreibung:**

  Bindet einen Dienst an einen Benutzer LB vserver. Der Diensttyp sollte USER_TCP/USER_SSL_TCP für die Bindung an einen LB-vServer mit dem Typ USER_TCP/USER_SSL_TCP sein.

  > **Beispiel:**
  >
  > bind lb vserver mysv mqtt_svr1

- **CLI-Befehl:**

  ```
  unbind lb vserver <name> <serviceName>
  ```

- **Beschreibung:**

  Entbindet einen zuvor gebundenen Dienst an einen Benutzer-LB-vserver.

  > **Beispiel:**
  >
  > unbind lb vserver mysv mqtt_svr1

- **CLI-Befehl:**

  ```
  rm service <name>
  ```

- **Beschreibung:**

  Entfernt einen Dienst, der zuvor für ein Benutzerprotokoll hinzugefügt wurde.

  > **Beispiel:**
  >
  > rm-Dienst mqtt_svr1

Problembehandlung bei Protokollerweiterungen

May 11, 2023

Wenn sich Ihre Erweiterungsfunktion nicht wie erwartet verhält, können Sie die Funktion zur Nachverfolgung von Erweiterungen verwenden, um das Verhalten Ihrer Erweiterungsfunktion zu überprüfen. Sie können Ihrer Erweiterungsfunktion auch die Protokollierung hinzufügen, indem Sie die benutzerdefinierte Protokollierungsfunktion verwenden, mit der Sie die Protokollebene definieren können, die auf der NetScaler-Appliance erfasst werden soll.

Benutzerdefiniertes Logging

Sie können Ihrer Erweiterungsfunktion auch Ihre eigene Protokollierung hinzufügen. Verwenden Sie dazu die eingebaute Funktion ns.logger:level (), wobei Level für Notfall, Warnung, Kritisch, Fehler, Warnung, Hinweis, Info oder Debug steht. Die Parameter sind dieselben wie bei der C-Funktion printf (): eine Formatzeichenfolge und eine variable Anzahl von Argumenten, um Werte für das in der Formatzeichenfolge angegebene% bereitzustellen. Sie könnten beispielsweise der COMBINE_HEADERS-Funktion Folgendes hinzufügen, um das Ergebnis eines Aufrufs zu protokollieren:

```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"

ns.logger:info("Result: %s", result_str)

return result_str
<!--NeedCopy-->
```

Die obige Funktion würde die folgende Meldung nach/var/log/ns.log für die Beispieleingabe protokollieren, die in den abgekürzten Protokollnachrichtenbeispielen im Abschnitt Extension Tracing oben gezeigt wird.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: \*/\*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Richtlinienerweiterungen

May 11, 2023

Mit der Funktion zur Richtlinienerweiterung können Sie Erweiterungsfunktionen für integrierte Richtlinientypen schreiben. Die Erweiterungen können in Richtlinienausdrücken verwendet werden,

genau wie integrierte Funktionen. Sie werden ausgeführt, wenn die entsprechenden Richtlinienausdrücke ausgewertet werden. Diese Funktion ist nützlich für:

- Hinzufügen benutzerdefinierter Funktionen zu bestehenden Richtlinien.
- Implementierung logischer Konstrukte für komplexe Kundenanforderungen.

Die Funktion zur Richtlinienerweiterung behebt diese Einschränkungen, indem sie es Benutzern ermöglicht, Erweiterungsfunktionen für integrierte Richtlinientypen zu schreiben. Die Erweiterungen können dann in den Richtlinienausdrücken verwendet werden, genau wie integrierte Funktionen. Sie werden ausgeführt, wenn die entsprechenden Richtlinienausdrücke ausgewertet werden.

In der folgenden Tabelle sind die Richtlinientypen aufgeführt, die beim Schreiben einer Erweiterung verwendet werden können, sowie die zugehörigen Zuordnungen.

Richtlinientyp	Zugeordneter Richtlinientyp	Ausgabe
TEXT_T	NSTEXT	Zeichenfolge
BOOL_AT	NSBOOL	Boolesch
NUM_AT	NSNUM	Zahl (Gleitkommazahl mit doppelter Genauigkeit)
DOUBLE_AT	NSDOUBLE	Zahl (Gleitkommazahl mit doppelter Genauigkeit)

Voraussetzungen für die Verwendung von Richtlinienerweiterungen

Die importierten Funktionen müssen den bestehenden Richtlinienstandards entsprechen. Deshalb:

- Der Funktionsname muss mit einem Buchstaben beginnen und kann Zahlen oder Unterstriche enthalten.
- Der Funktionsname wird in den NetScaler-Richtlinien so behandelt, dass Groß- und Kleinschreibung nicht berücksichtigt wird.
- Die Funktion muss einen einzelnen Wert zurückgeben, auch wenn die Erweiterungssprache mehrere Werte zurückgibt.
- Funktionen mit einer variablen Anzahl von Argumenten werden nicht unterstützt.

Wie funktionieren Policenerweiterungen?

Die vorhandenen Richtlinien auf einer NetScaler-Appliance verwenden einen Interpreter, um die Funktionen auszuwerten, die in eine Richtlinienerweiterungsdatei importiert werden. Wenn ein Benutzer eine neue Funktion in eine Richtlinienerweiterungsdatei importiert:

1. Die Erweiterungsdatei wird auf Syntax und andere Bedingungen überprüft.

2. Schlägt die Validierung fehl, wird der Fehler dem Benutzer gemeldet.
3. Wenn die Überprüfung erfolgreich ist, wird die Erweiterungsdatei in die NetScaler-Appliance importiert und ihr Inhalt kann wie jede integrierte Richtlinienfunktion in Richtlinienausdrücken verwendet werden.
    a) Wenn die Auswertung des Richtlinienausdrucks während der Laufzeit einen Fehler zurückgibt, wird dieser als Undef-Ereignis gemeldet und der zugehörige Fehlerzähler wird erhöht. **Hinweis:** Wenn ein Policy-Undef-Ereignis eintritt und die Richtlinienregel eine oder mehrere Funktionen zur Richtlinienerweiterung enthält, zeigt der `show ns extension <name>` Befehl die untergeordneten Treffer an, wenn er auf diese Richtlinienerweiterungen angewendet wird. Wenn die Erweiterungsfunktion abgebrochen wird, wird der Wert des Abbruchzählers erhöht.
    b) Wenn die Bewertung des Richtlinienausdrucks erfolgreich ist, wird die Ausdrucksauswertung fortgesetzt, bis der gesamte Ausdruck ausgewertet ist oder bis sie aufgrund eines Fehlers abgebrochen wird.

Wenn die Ausführung der Erweiterungsfunktion zu lange dauert, wird sie abgebrochen und der Fehlerzähler für diese Erweiterungsfunktion wird erhöht. Die Erweiterungsfunktion ist in einer Sandbox ausgeführt, wodurch Folgendes verhindert wird:

- Übermäßige CPU-Auslastung auf der NetScaler-Appliance.
- Übermäßiger Speicherverbrauch auf der NetScaler-Appliance.
- Verwendung schädlicher integrierter Bibliotheken oder Bibliotheken oder Binärdateien von Drittanbietern.
- Langfristige Skripts, die möglicherweise einen Neustart der NetScaler Appliance verursachen könnten.

Konfiguration von Richtlinienerweiterungen

May 11, 2023

Wenn Ihre Richtlinienerweiterungsdatei fertig ist, importieren Sie sie in die NetScaler-Appliance. Der Importvorgang kopiert die Erweiterungsdatei in ein Verzeichnis auf der NetScaler-Appliance und sucht nach Syntaxfehlern.

Nach dem Import müssen Sie die Erweiterungsdatei für die Verwendung in den Richtlinienausdrücken zur Verfügung stellen.

Hinweis: Der Importbefehl wird verwendet \<src\>, um den Dateiinhalt von einer externen Quelle oder einer internen Quelle auf das NetScaler-Dateisystem herunterzuladen. Um diesen Dateiinhalt zum ersten Mal in eine oder mehrere Paket-Engines zu laden, verwenden Sie den Befehl add. Wenn der Dateiinhalt aktualisiert wird, kann der aktualisierte Inhalt in das NetScaler-Dateisystem heruntergе-

laden werden, indem der Importbefehl mit dem Argument overwrite ausgegeben wird. Der Befehl aktualisiert den Inhalt im Dateisystem. Um den aktualisierten Inhalt in eine oder mehrere Paket-Engines zu laden, verwenden Sie den Befehl update.

Konfigurieren von Richtlinienerweiterungen mit der CLI

1. Importieren Sie die Richtlinienerweiterungsdatei entweder von einem Webserver (über HTTP) oder von Ihrer lokalen Workstation in die NetScaler Appliance.

   a) HTTP-Import

   Wenn Sie über einen Webserver verfügen, können Sie die Erweiterungsdatei im Webserver-Verzeichnis speichern und in die NetScaler-Appliance importieren.

   ```
   import ns extension <src> <name> [-comment<string>] [-
      overwrite]
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   import ns extension http://myhost/path/to/extension
      myextension -comment  “Custom crc calculation
   <!--NeedCopy-->
   ```

   b) Lokaler Import

   Sie können den SSH-Client verwenden, um die Erweiterungsdatei von Ihrer Workstation in das /var/tmp-Verzeichnis der NetScaler Appliance zu kopieren

   ```
   scp extension-file-name <ns-userid@ns-ip-addr>:/var/tmp
   <!--NeedCopy-->
   ```

   Hierbei gilt:

   - `extension-file-name` ist der Name der Erweiterungsdatei auf Ihrem Client-Computer.
   - `ns-userid` ist der Benutzer der NetScaler Appliance mit der Berechtigung, in /var/tmp zu schreiben.
   - `ns-ip-addr` ist die NetScaler IP-Adresse.

   Führen Sie nach dem Kopieren der Datei auf die NetScaler Appliance den Importbefehl auf der NetScaler Appliance aus.

   ```
   import ns extension local:<extension-file-name extension-name>
   <!--NeedCopy-->
   ```


Hinweis: Die CLI muss verwendet werden, um eine lokale Erweiterungsdatei zu importieren, indem der Befehl
import ausgeführt wird.

2. Fügen Sie der Paket-Engine die Richtlinienerweiterung zur Evaluierung hinzu.

```
add ns extension <name> [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add ns extension myextension
<!--NeedCopy-->
```

Nachdem eine Erweiterungsdatei importiert wurde, können Sie sie aktualisieren, indem Sie den Parameter -overwrite in den Importbefehl aufgenommen haben, oder sie entfernen. Sie können auch die Details einer importierten Erweiterungsdatei anzeigen.

Aktualisieren Sie eine Erweiterungsdatei auf der NetScaler-Appliance von der Quelle

Geben Sie in der Befehlszeile Folgendes ein:

```
update ns extension <name>
<!--NeedCopy-->
```

Hinweis: Sie können die Erweiterungsdatei erst aktualisieren, nachdem Sie die angegebene Erweiterungsdatei mit dem Parameter -overwrite in die NetScaler-Appliance importiert haben.

Beispiel:

```
update ns extension myextension
<!--NeedCopy-->
```

Entfernen einer Erweiterungsdatei aus der NetScaler Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm ns extension <name>
<!--NeedCopy-->
```

Beispiel:

```
rm ns extension myextension
<!--NeedCopy-->
```


Anzeigen der Details der angegebenen Erweiterungsfunktion auf der NetScaler Appliance

Geben Sie in der Befehlszeile Folgendes ein:

```
show ns extension <name>
<!--NeedCopy-->
```

Beispiel:

```
show ns extension myextension
<!--NeedCopy-->
```

Konfigurieren Sie Richtlinienerweiterungen mithilfe der GUI

1. Importieren Sie die Richtlinienerweiterungsdatei entweder von einem Webserver (über HTTP) oder von Ihrer lokalen Workstation in die NetScaler Appliance.
   a) Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, klicken Sie auf **Richtlinienerweiterung** . Wählen Sie in der Dropdownliste **Importieren von die URL für den Speicherort der Erweiterungsdatei aus**, die Sie importieren möchten.
   b) Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, **Richtlinienerweiterung**, und importieren Sie die Erweiterungsdatei, indem Sie in der Dropdownliste **Importieren** von Datei auswählen.
2. Fügen Sie der Paket-Engine die Richtlinienerweiterung zur Evaluierung hinzu.

   Navigieren Sie zu **AppExpert** > **Policy Extensions** und fügen Sie auf der Registerkarte**Policy Extensions** die Erweiterungsdatei hinzu.

Aktualisieren Sie eine Erweiterungsdatei auf der NetScaler-Appliance von der Quelle

Navigieren Sie zu **AppExpert** > **Policy Extensions** und aktualisieren Sie auf der Registerkarte **Policy Extensions** die Erweiterungsdatei.

Entfernen einer Erweiterungsdatei aus der NetScaler Appliance

Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen** und entfernen Sie auf der Registerkarte **Richtlinienerweiterungen** die Erweiterungsdatei.

Anzeigen der Details der angegebenen Erweiterungsfunktion auf der NetScaler Appliance

Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, und klicken Sie auf der Registerkarte **Funktionen für Richtlinienerweiterungen** auf den Pfeil auf die Dropdownliste der Erweiterungsfunktion, für die Sie die Details anzeigen möchten.

Richtlinienerweiterungen - Anwendungsfälle

May 11, 2023

Bestimmte Kundenanwendungen haben Anforderungen, die mit bestehenden Richtlinien und Ausdrücken nicht erfüllt werden können. Mit der Funktion zur Richtlinienerweiterung können Kunden ihren Anwendungen maßgeschneiderte Funktionen hinzufügen, um ihren Anforderungen gerecht zu werden.

Die folgenden Anwendungsfälle veranschaulichen das Hinzufügen neuer Funktionen mithilfe der Richtlinienerweiterungsfunktion auf der NetScaler-Appliance.

- Fall 1: Benutzerdefinierter Hash
- Fall 2: Doppelte Schrägstriche in URLs zusammenfassen
- Fall 3: Header kombinieren

Fall 1: Benutzerdefinierter Hash

Die CUSTOM_HASH-Funktion bietet einen Mechanismus zum Einfügen eines beliebigen Hashwerts in die an den Client gesendeten Antworten. In diesem Anwendungsfall wird die Hash-Funktion verwendet, um den Hash der Abfragezeichenfolge für eine HTTP-Rewrite-Anfrage zu berechnen und einen HTTP-Header namens CUSTOM_HASH mit dem berechneten Wert einzufügen. Die Funktion CUSTOM_HASH implementiert den DJB2-Hash-Algorithmus.

Beispiel für die Verwendung von CUSTOM_HASH:

```
> add rewrite action test_custom_hash insert_http_header "CUSTOM_HASH"
   "HTTP.REQ.URL.QUERY.CUSTOM_HASH"
<!--NeedCopy-->
```

Beispieldefinition von CUSTOM_HASH ():

```
    -- Extension function to compute custom hash on the text

    -- Uses the djb2 string hash algorithm
    function NSTEXT:CUSTOM_HASH() : NSTEXT

        local hash = 5381

        local len = string.len(self)

        for i = 1, len do

            hash = bit32.bxor((hash * 33), string.byte(self, i))
```



```
13
14          end
15
16          return tostring(hash)
17
18      end
19  <!--NeedCopy-->
```

Zeilenweise Beschreibung des obigen Beispiels:

```
1  function NSTEXT:CUSTOM_HASH() : NSTEXT
2
3  Defines the CUSTOM_HASH() function, with text input and a text return
       value.
4
5  local hash = 5381
6  local len = string.len(self)
7
8  Declares two local variables:
9
10  - hash. Accumulates the compute hash value and is seeded with the
       number 5381
11
12  - len. Sets to the length of the self input text string, using the
       built-in string.len() function.
13
14 for i = 1, len do
15       hash = bit32.bxor((hash * 33), string.byte(self, i))
16 end
17
18 Iterates through each byte of the input string and adds the byte to the
       hash. It uses the built-in string.byte() function to get the byte
      and the built-in bit32.bxor() function to compute the XOR of the
      existing hash value (multiplied by 33) and the byte.
19
20 return tostring(hash)
21
22 Calls the built-in tostring() function to convert the numeric hash
      value to a string and returns the string as the value of the
      function.
23 <!--NeedCopy-->
```


Fall 2: Doppelte Schrägstriche in URLs zusammenfassen

Das Zusammenklappen doppelter Schrägstriche in URLs verbessert die Renderzeit der Website, da Browser die URLs mit einem Schrägstrich effizienter analysieren. Die URLs mit einem Schrägstrich dienen auch dazu, die Kompatibilität mit Anwendungen zu gewährleisten, die keine doppelten Schrägstriche akzeptieren. Mit der Funktion zur Richtlinienerweiterung können Kunden eine Funktion hinzufügen, die die doppelten Schrägstriche in den URLs durch einfache Schrägstriche ersetzt. Das folgende Beispiel veranschaulicht das Hinzufügen einer Richtlinienerweiterungsfunktion, die doppelte Schrägstriche in URLs ausblendet.

Beispieldefinition für COLLAPSE_DOUBLE_SLASHES ():

```
    -- Collapse double slashes in URL to a single slash and return the
       result
    function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

        local result = string.gsub(self, "//", "/")

        return result

    end
<!--NeedCopy-->
```

Zeilenweise Beschreibung des obigen Beispiels:

```
function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT

Declares the COLLAPSE_DOUBLE_SLASHES() function with text input and
   return.

local result = string.gsub(self, "//", "/")

Declares a local variable named result and uses the built-in string.
   gsub() function to replace all double slashes with single slashes in
    the self input text.

The second parameter of string.gsub() is actually a regular expression
   pattern, although here a simple string is used for the pattern.

return result

Returns the resulting string.
<!--NeedCopy-->
```


Fall 3: Header kombinieren

Bestimmte Kundenanwendungen können nicht mehrere Header in einer Anfrage verarbeiten. Außerdem verbraucht das Parsen doppelter Header mit denselben Header-Werten oder mehrerer Header mit demselben Namen, aber unterschiedlichen Werten in einer Anfrage Zeit und Netzwerkressourcen. Mit der Funktion zur Richtlinienerweiterung können Kunden eine Funktion hinzufügen, um diese Header zu einzelnen Headern zu kombinieren, wobei ein Wert die ursprünglichen Werte kombiniert. Kombinieren Sie beispielsweise die Werte der Header H1 und H2.

Ursprüngliche Anfrage:

```
GET /combine_headers HTTP/1.1
User-Agent: amigo unit test
Host: myhost
H2: h2val1
H1: abcd
Accept: \*/\*
H2: h2val2
Content-Length: 0
H2: h2val3
H1: 1234
<!--NeedCopy-->
```

Geänderte Anfrage:

```
GET /combine_headers HTTP/1.1
User-Agent: amigo unit test
Host: myhost
H2: h2val1, h2val2, h2val3
H1: abcd, 1234
Accept: \*/\*
Content-Length: 0
<!--NeedCopy-->
```

Im Allgemeinen erfolgt diese Art der Anforderungsänderung mithilfe der Rewrite-Funktion, wobei Richtlinienausdrücke verwendet werden, um den Teil der Anfrage, der geändert werden soll (das Ziel), und die durchzuführende Änderung (der String-Builder-Ausdruck) abzugrenzen. Richtlinienausdrücke sind jedoch nicht in der Lage, über eine beliebige Anzahl von Headern zu iterieren.

Die Lösung dieses Problems erfordert eine Erweiterung der politischen Fazilität. Dazu definieren wir eine Erweiterungsfunktion namens COMBINE_HEADERS. Mit dieser Funktion können wir die folgende Rewrite-Aktion einrichten:

```
> add rewrite action combine_headers_act replace 'HTTP.REQ.FULL_HEADER
.AFTER_STR("HTTP/1.1rn")''HTTP.REQ.FULL_HEADER.AFTER_STR("HTTP/1.1rn").
```


COMBINE_HEADERS'

Hier ist das Rewrite-Ziel HTTP.REQ.FULL_HEADER.AFTER_STR („http/1.1RN“). AFTER_STR („http/1.1Rn“) ist erforderlich, da FULL_HEADER die erste Zeile der HTTP-Anfrage enthält (z. B. GET /combine_headers HTTP/1.1).

Der String-Builder-Ausdruck ist HTTP.REQ.FULL_HEADER.AFTER_STR(“HTTP/1.1rn”).COMBINE_HEADERS, wobei die Header (abzüglich der ersten Zeile) in die Erweiterungsfunktion COMBINE_HEADERS eingegeben werden, die die Werte für Header kombiniert und zurückgibt.

Beispieldefinition von COMBINE_HEADERS ():

```
    -- Extension function to combine multiple headers of the same name
       into one header.



    function NSTEXT:COMBINE_HEADERS(): NSTEXT

        local headers = {
}
-- headers

        local combined_headers = {
}
-- headers with final combined values
        -- Iterate over each header (format "name:valuer\r\n")

        -- and build a list of values for each unique header name.

        for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n"
           ) do

            if headers[name] then

                local next_value_index = #(headers[name]) + 1

                headers[name][next_value_index] = value

            else

                headers[name] = {
name .. ":" .. value }


            end
```



```
33
34          end
35
36
37
38          -- iterate over the headers and concat the values with
                separator ","
39
40          for name, values in pairs(headers) do
41
42              local next_header_index = #combined_headers + 1
43
44              combined_headers[next_header_index] = table.concat(values,
                    ",")
45
46          end
47
48
49
50          -- Construct the result headers using table.concat()
51
52          local result_str = table.concat(combined_headers, "\r\n") .. "\
                r\n\r\n"
53
54          return result_str
55
56      end
57  <!--NeedCopy-->
```

Zeilenweise Beschreibung des obigen Beispiels:

```
1  function NSTEXT:COMBINE_HEADERS(): NSTEXT
2
3  Defines the COMBINE_HEADERS extension function, with the text input
       into the function from the policy expression and a text return type
       to the policy expression.
4
5  local headers = {
6    }
7    -- headers
8  local combined_headers = {
9    }
10   -- headers with final combined values
11
12 Declares local variables headers and combined_headers and initialize
```



```
    these variables to empty tables. headers will be a table of arrays
    of strings, where each array holds one or more values for a header.
    combined_headers will be an array of strings, where each array
    element is a header with its combined values.

for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n") do
. . .
end
<!--NeedCopy-->
```

Dieses generische For-Loop analysiert jeden Header in der Eingabe. Der Iterator ist die integrierte Funktion string.gmatch(). Diese Funktion benötigt zwei Parameter: eine zu durchsuchende Zeichenfolge und ein Muster, das verwendet wird, um Teile der Zeichenfolge abzugleichen. Die zu durchsuchende Zeichenfolge wird vom impliziten Parameter self bereitgestellt, der der Text für die in die Funktion eingegebenen Header ist.

Das Muster wird mit einem regulären Ausdruck (kurz Regex) ausgedrückt. Dieser Regex entspricht dem Header-Namen und -Wert für jeden Header, den der HTTP-Standard als ***name*:*value*\r\n** definiert. Die Klammern im Regex geben die passenden Teile an, die extrahiert werden sollen. Das Regex-Schema lautet also **(*match-name*):(*match-value*)\r\n**. Das ***Match-Name-Muster*** muss mit allen Zeichen außer dem Doppelpunkt übereinstimmen. Das steht geschrieben `[^:]+`. `[^:]` ist ein beliebiges Zeichen außer `:` und `+` ist eine oder mehrere Wiederholungen. In ähnlicher Weise muss das *Match-Value-Muster* mit allen Zeichen außer dem `\r\n` übereinstimmen, daher wird es so geschrieben: `[^\r\n]*`. `[^\r\n]` entspricht allen Zeichen außer `\r` und `\n`, und `*` ist null oder mehr Wiederholungen. Das ergibt den kompletten Regex `([^:]+):([^\r\n]*)\r\n`.

Die for -Anweisung verwendet eine Mehrfachzuweisung, um Namen und Wert für die beiden Treffer festzulegen, die vom Iterator string.gmatch () zurückgegeben werden. Diese werden implizit als lokale Variablen im Hauptteil der for-Schleife deklariert.

```
if headers[name] then
     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value
else
     headers[name] = {
 name .. ":" .. value }

end
<!--NeedCopy-->
```

Diese Anweisungen innerhalb der for-Schleife setzen die Headernamen und -werte in die Header-Tabelle. Wenn ein Header-Name zum ersten Mal analysiert wird (sagen wir H2: h2val1 in der Beispieleingabe), gibt es keinen Headereintrag für den Namen und headers [name] ist Null.

Da nil als falsch behandelt wird, wird die else-Klausel ausgeführt. Dies setzt den Header-Eintrag für name auf ein Array mit einem Zeichenfolgenwert *name*:*value*.

Hinweis: Der Array-Konstruktor in der Else-Schleife entspricht {[1] = name.. ":".. value}, wodurch das erste Element des Arrays festgelegt wird.) Für den ersten H2-Header wird headers["H2"] = {"H2:h2val1"} festgelegt.

Bei nachfolgenden Instanzen eines Headers (sagen wir H2: h2val2 in der Beispieleingabe). headers[name] ist nicht null, daher wird die Then-Klausel ausgeführt. Dies bestimmt den nächsten verfügbaren Index im Array-Wert für Header [Name] und fügt den Header-Wert in diesen Index ein. Für den zweiten H2-Header wird headers["H2"] = {"H2:h2val1", "h2val2"} festgelegt.

```
for name, values in pairs(headers) do
    local next_header_index = #combined_headers + 1
    combined_headers[next_header_index] = table.concat(values, ",")
end
<!--NeedCopy-->
```

Nachdem die ursprünglichen Header analysiert und die Header-Tabelle ausgefüllt wurden, erstellt diese Schleife das Array combined_headers. Es verwendet die Funktion pairs () als For-Loop-Iterator.

Jeder Aufruf von pairs () gibt den Namen und Wert des nächsten Eintrags in der Header-Tabelle zurück.

Die nächste Zeile bestimmt den nächsten verfügbaren Index im Array combined_headers, und die nächste Zeile setzt dieses Array-Element auf den kombinierten Header. Es verwendet die eingebaute Funktion table.concat (), die als Argumente ein Array von Zeichenketten und eine Zeichenfolge verwendet, die als Trennzeichen verwendet wird, und eine Zeichenfolge zurückgibt, die die Verkettung der Array-Zeichenketten darstellt, getrennt durch das Trennzeichen.

Beispielsweise ergibt dies für Werte = {"h2:h2val1", „h2val2"} „h2:h2val1, h2val2"

```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
<!--NeedCopy-->
```

Nachdem das Array combined_headers erstellt wurde, verkettet es die Elemente zu einer Zeichenfolge und fügt ein doppeltes\ r\ n hinzu, das die HTTP-Header beendet.

```
return result_str
<!--NeedCopy-->
```

Gibt eine Zeichenfolge als Ergebnis der Erweiterungsfunktion COMBINE_HEADERS zurück.

Problembehandlung bei Richtlinienerweiterungen

May 11, 2023

Wenn sich Ihre Erweiterungsfunktion nicht wie erwartet verhält, können Sie die Funktion zur Nachverfolgung von Erweiterungen verwenden, um das Verhalten Ihrer Erweiterungsfunktion zu überprüfen. Sie können Ihrer Erweiterungsfunktion auch die Protokollierung hinzufügen, indem Sie die benutzerdefinierte Protokollierungsfunktion verwenden, mit der Sie die Protokollebene definieren können, die auf der NetScaler-Appliance erfasst werden soll.

Dieses Thema enthält Informationen zu:

- Nachverfolgung von Erweiterungen
- Benutzerdefiniertes Logging

Nachverfolgung von Erweiterungen

Um zu zeigen, was Ihre Erweiterungsfunktion tut, protokolliert die Erweiterungsablaufverfolgung die Ausführung der Funktion im NetScaler-Systemprotokoll (/var/log/ns.log). Die Trace-Protokollierung verwendet das DEBUG-Log-Level, das normalerweise nicht aktiviert ist. Daher müssen Sie ALLE Log-Levels aktivieren. Anschließend können Sie das Tracing aktivieren, indem Sie die Option -trace des Erweiterungsbefehls set ns festlegen. Die verfügbaren Einstellungen sind:

- aus- und ausschalten der Ablaufverfolgung (entspricht der unset-ns-Erweiterung -trace).
- ruft Trace-Funktionsaufrufe mit Argumenten und Funktionsrückgaben mit dem ersten Rückgabewert auf.
- Linien folgen den obigen Zahlen plus Zeilennummern für ausgeführte Zeilen.
- alle verfolgen das Obige plus lokale Variablen, die durch ausgeführte Zeilen geändert wurden.

Beispiel:

```
set audit syslogParams -loglevel ALL

set ns extension combine_headers -trace all
<!--NeedCopy-->
```

Jede Trace-Nachricht hat das Format

```
log-header : default NSEXTENSION Message message-number 0 : "TRACE function
-name CALL call-number: event"
```

Hierbei gilt:

- Log-Header liefert Zeitstempel, die NetScaler-IP-Adresse und die Packet Engine-ID.
- Nachrichtennummer ist eine fortlaufende Nummer, die die Protokollnachricht identifiziert.

- Funktionsname ist der Name der Erweiterungsfunktion.
- call-number ist eine fortlaufende Nummer für jeden Aufruf einer Erweiterungsfunktion. Es kann verwendet werden, um alle Trace-Meldungen für einen Erweiterungsfunktionsaufruf zu gruppieren.
- Das Ereignis ist eines der folgenden:
  - CALL function name; parameter-values gibt an, dass die Funktion mit den angegebenen Parametern aufgerufen wurde.
  - RETURN FROM Funktionsname; return = value gibt an, dass eine Funktion den angegebenen (ersten) Wert zurückgegeben hat. (Zusätzliche Rückgabewerte werden nicht gemeldet.)
  - LINE-Zeilennummer; variable-values gibt an, dass eine Zeile ausgeführt wurde, und listet alle Variablen mit geänderten Werten auf.

Hierbei gilt:

- Wert oder Werte ist
  - eine Zahl, mit oder ohne Dezimaltrennzeichen,
  - eine Zeichenfolge, eingeschlossen in doppelte Anführungszeichen und mit Escape-Zeichen, wie zuvor beschrieben,
  - ein boolescher Wert wahr oder falsch,
  - nil,
  - ein Tabellenkonstruktor im Format {[key1] =value1, [key2] =value2,…}.
- parameter-values ist Parameter1 = Wert1; Parameter2 = Wert2,…
- Variablenwerte sind Variable1 = Wert1; Variable2 = Wert2,…

Ein Beispiel für abgekürzte Protokollmeldungen:

```
>shell tail -f /var/log/ns.log | grep TRACE | more

... NSEXTENSION Message 3035 0 : "TRACE combine_headers CALL 30 : CALL
    COMBINE_HEADERS; self = "User-Agent: curl/7.24.0 (amd64-portbld-
    freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nHost:
    10.217.24.7\r\nAccept: \*/\*\r\nH2: h2val1\r\nH1: abcd\r\nH2: h2val2
    \r\nH2: h2val3\r\n\r\n""

... NSEXTENSION Message 3036 0 : "TRACE combine_headers CALL 30 : LINE
    4; headers = {
  }
 "

... NSEXTENSION Message 3037 0 : "TRACE combine_headers CALL 30 : LINE
    5; combined_headers = {
  }
 "
```



```
12
13 ... NSEXTENSION Message 3038 0 : "TRACE combine_headers CALL 30 : CALL
      gmatch"
14
15 ... NSEXTENSION Message 3039 0 : "TRACE combine_headers CALL 30 :
      RETURN FROM gmatch; return = function 0x2bee5a80"
16
17 ... NSEXTENSION Message 3040 0 : "TRACE combine_headers CALL 30 : CALL
      for iterator"
18
19 ... NSEXTENSION Message 3041 0 : "TRACE combine_headers CALL 30 :
      RETURN FROM for iterator; return = " curl/7.24.0 (amd64-portbld-
      freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""
20
21 ... NSEXTENSION Message 3042 0 : "TRACE combine_headers CALL 30 : LINE
      9; name = "User-Agent"; value = " curl/7.24.0 (amd64-portbld-
      freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""
22
23 ... NSEXTENSION Message 3043 0 : "TRACE combine_headers CALL 30 : LINE
      10"
24
25 ... NSEXTENSION Message 3044 0 : "TRACE combine_headers CALL 30 : LINE
      14; headers = {
26  ["User-Agent"]={
27  [1]="User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
        OpenSSL/0.9.8y zlib/1.2.3" }
28   }
29  "
30
31 . . .
32
33 ... NSEXTENSION Message 3117 0 : "TRACE combine_headers CALL 30 : CALL
      for iterator"
34
35 ... NSEXTENSION Message 3118 0 : "TRACE combine_headers CALL 30 :
      RETURN FROM for iterator; return = nil"
36
37 ... NSEXTENSION Message 3119 0 : "TRACE combine_headers CALL 30 : LINE
      19"
38
39 ... NSEXTENSION Message 3120 0 : "TRACE combine_headers CALL 30 : CALL
      concat"
40
41 ... NSEXTENSION Message 3121 0 : "TRACE combine_headers CALL 30 :
      RETURN FROM concat; return = "User-Agent: curl/7.24.0 (amd64-portbld
```



```
      -freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
      nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3""
      ... NSEXTENSION Message 3122 0 : "TRACE combine_headers CALL 30 :
      LINE 25; result_str = "User-Agent: curl/7.24.0 (amd64-portbld-
      freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
      nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3\r\
      n\r\n""
42
43 ... NSEXTENSION Message 3123 0 : "TRACE combine_headers CALL 30 :
      RETURN FROM COMBINE_HEADERS; return = "User-Agent: curl/7.24.0 (
      amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r
      \nH1: abcd\r\nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1,
      h2val2, h2val3\r\n\r\n""
44 <!--NeedCopy-->
```

Benutzerdefiniertes Logging

Sie können Ihrer Erweiterungsfunktion auch Ihre eigene Protokollierung hinzufügen. Verwenden Sie dazu die eingebaute Funktion ns.logger:*level*(), wobei *Level* für Notfall, Warnung, Kritisch, Fehler, Warnung, Hinweis, Info oder Debug steht. Die Parameter sind dieselben wie bei der C-Funktion printf (): eine Formatzeichenfolge und eine variable Anzahl von Argumenten, um Werte für das in der Formatzeichenfolge angegebene% bereitzustellen. Sie könnten beispielsweise der COMBINE_HEADERS-Funktion Folgendes hinzufügen, um das Ergebnis eines Aufrufs zu protokollieren:

```
1 local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
2
3 ns.logger:info("Result: %s", result_str)
4
5 return result_str
6 <!--NeedCopy-->
```

Die obige Funktion würde die folgende Meldung nach/var/log/ns.log für die Beispieleingabe protokollieren, die in den abgekürzten Protokollnachrichtenbeispielen im Abschnitt Extension Tracing oben gezeigt wird.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: */*^M H2: h2val1, h2val2,
h2val3^M ^M"
```


Optimierung

May 11, 2023

Die NetScaler-Optimierungsfunktionen reduzieren die Transaktionszeiten zwischen den Clients und den Servern und reduzieren den Bandbreitenverbrauch. Sie verbessern auch die Serverleistung, indem sie einige Aufgaben auslasten und andere effizienter machen.

Feature	Beschreibung
Client Keep-Alive	Verarbeitet mehrere Anfragen für eine einzelne Clientverbindung. Der Client muss nicht für jede Anforderung an den Server eine neue Verbindung aushandeln.
HTTP-Komprimierung	Komprimiert HTTP-Antworten, die von den Servern an kompressionsfähige Browser gesendet werden. Die kleineren Antworten reduzieren die Downloadzeit und sparen Bandbreite.
Integriertes Caching	Speichert Antworten auf Kundenanfragen. Nachfolgende Anfragen für denselben Inhalt werden aus dem NetScaler-Cache bedient, anstatt an den Ursprungsserver weitergeleitet zu werden.
Front-End-Optimierung	Reduziert die Lade- und Renderzeit von Webseiten, indem der an den Client-Browser übermittelte Inhalt vereinfacht und optimiert wird. **Hinweis**: Unterstützt ab NetScaler 10.5.

Keep-Alive für Kunden

May 11, 2023

Mit der Client-Keep-Alive-Funktion können Anfragen mehrerer Clients über eine einzige Verbindung gesendet werden. Diese Funktion kommt dem Transaktionsmanagement zugute. Wenn der Client-Keep-Alive-Modus auf einer Appliance aktiviert ist und die Serverantwort auf die Clientanforderung die Verbindung enthält: Schließen Sie den HTTP-Header und führt die folgenden Aufgaben aus:

- Benennt den vorhandenen Connection Headernamen um, indem die Zeichen im Kopfzeilennamen gemischt werden.
- Fügt einen neuen Connection: Header mit Keep-Alive als Wert für den Header hinzu.

Der Client Keep-Alive-Modus ermöglicht es der NetScaler Appliance, mehrere Anfragen und Antworten über dieselbe Socket-Verbindung zu verarbeiten. Die Funktion hält die Verbindung zwischen dem Client und der Appliance (clientseitige Verbindung) auch dann geöffnet, nachdem der Server die Verbindung mit der Appliance geschlossen hat. Dies ermöglicht Anfragen mehrerer Clients über eine einzige Verbindung und speichert die beim Öffnen und Schließen einer Verbindung verbundenen Rundreisen. Client Keep-Alive ist in SSL-Sitzungen am vorteilhaftesten.

Client Keep-Alive ist für die folgenden Szenarien nützlich:

- Wenn der Server das Client-Keep-Alive nicht unterstützt.
- Wenn der Server das Client-Keep-Alive unterstützt, eine Anwendung auf dem Server jedoch nicht unterstützt.

> **Hinweis:**
> Client Keep-Alive ist für HTTP- und SSL-Verkehr anwendbar. Client-keep Alive kann global konfiguriert werden, um den gesamten Datenverkehr abzuwickeln. Sie können es auch für bestimmte Dienste aktivieren.

In der Client-Keep-Alive-Umgebung fangen die konfigurierten Dienste den Client-Datenverkehr ab und die Client-Anfrage wird an den Ursprungsserver weitergeleitet. Der Server sendet die Antwort und schließt die Verbindung zwischen dem Server und der Appliance. Wenn in der Serverantwort ein Header „Connection: Close“ vorhanden ist, korrumpiert die Appliance diesen Header in der clientseitigen Antwort und die clientseitige Verbindung bleibt offen. Dadurch muss der Client für die nächste Anfrage keine neue Verbindung öffnen. Stattdessen wird die Verbindung zum Server erneut geöffnet.

> **Hinweis:**
> Wenn ein Server zwei „Connection: Close“ -Header zurücksendet, wird nur einer bearbeitet. Dies führt zu erheblichen Verzögerungen beim Client-Rendern des Objekts, da ein Client nicht davon ausgeht, dass das Objekt vollständig geliefert wurde, bis die Verbindung geschlossen wird.

Client-Keep-Alive konfigurieren

Client Keep-Alive ist auf dem NetScaler standardmäßig deaktiviert, sowohl global als auch auf Serviceebene. Daher müssen Sie die Funktion im erforderlichen Umfang aktivieren.

> **Hinweis:**
> Wenn Sie das Client-Keep-Alive global aktivieren, ist es für alle Dienste aktiviert, unabhängig davon, ob Sie es auf Dienstebene aktivieren. Außerdem müssen Sie einige HTTP-Parameter kon-

figurieren, um Folgendes zu spezifizieren:

- die maximale Anzahl von HTTP-Verbindungen, die im Pool zur Wiederverwendung von Verbindungen beibehalten werden.
- aktivieren Sie das Verbindungsmultiplexing und aktivieren Sie die Persistenz. `Etag`

Hinweis:
Wenn Persistent `ETag` aktiviert ist, enthält der Header `ETag` Informationen über den Server, der den Inhalt bereitgestellt hat. Dadurch wird sichergestellt, dass bedingte Cache-Validierungsanfragen oder Browseranfragen für diesen Inhalt immer denselben Server erreichen.

Konfigurieren der Client-Keepalive-Funktion mithilfe der NetScaler Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Aktivieren Sie den Client-Keep-Alive auf dem NetScaler.
   - Auf globaler Ebene - `enable ns mode cka`
   - Auf Serviceniveau - `set service <name> -CKA YES`

   Hinweis:

   Client Keep-Alive kann nur für HTTP- und SSL-Dienste aktiviert werden.
2. Konfigurieren Sie HTTP-Parameter für das HTTP-Profil, das an einen oder mehrere Dienste gebunden ist.

```
1 set ns httpProfile <name> -maxReusePool <value> -conMultiplex
     ENABLED -persistentETag ENABLED
2 <!--NeedCopy-->
```

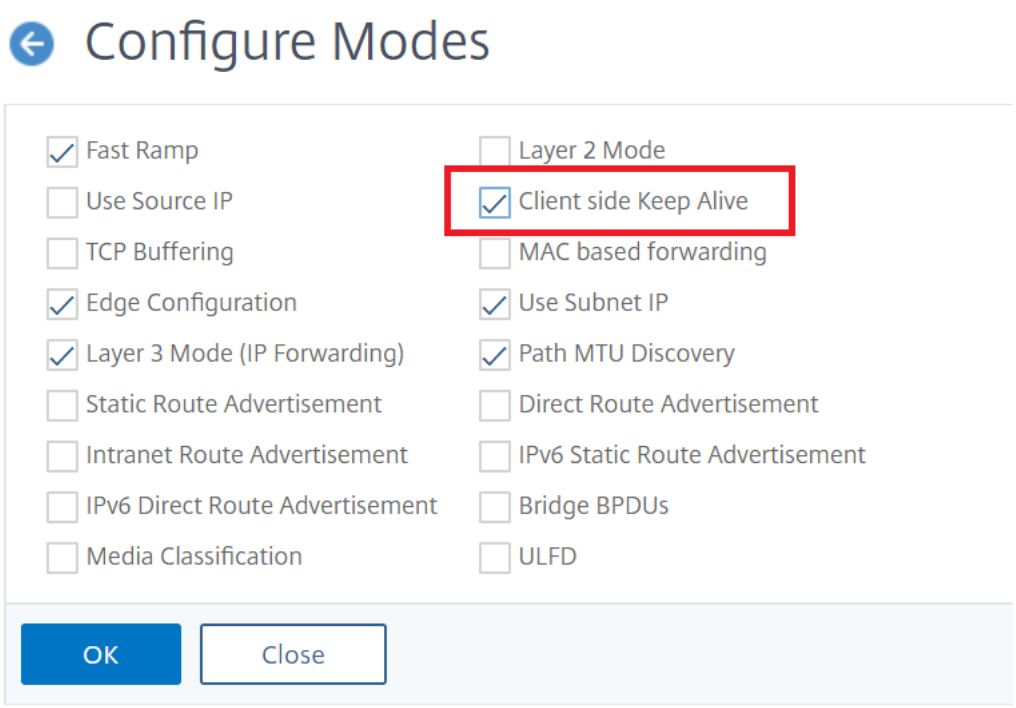
Hinweis:

Konfigurieren Sie diese Parameter im `nshttp_default _profile HTTP` Profil, um sie global verfügbar zu machen.

Konfigurieren Sie den Client-Keep-Alive mithilfe der NetScaler-GUI

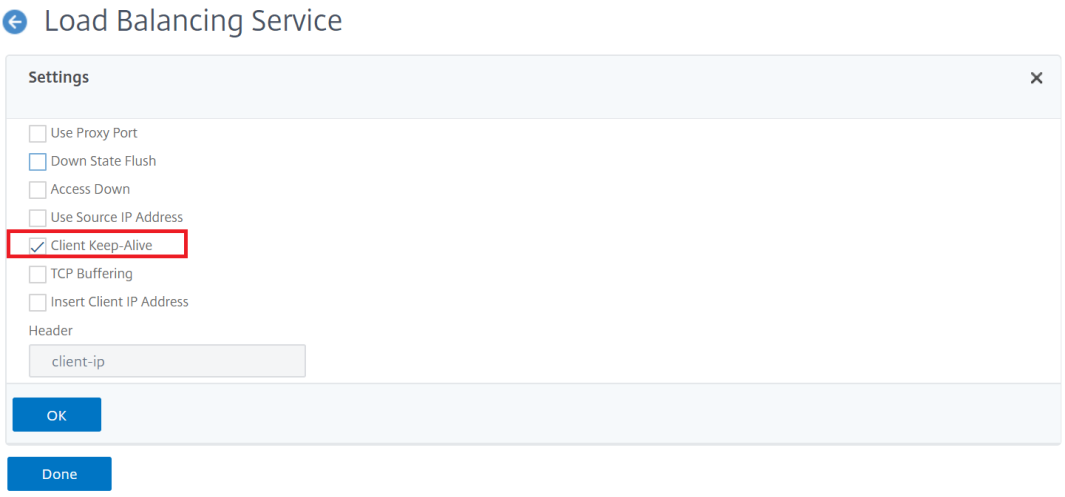
1. Aktivieren Sie den Client-Keep-Alive auf dem NetScaler.
   - Auf globaler Ebene

     Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Modi konfigurieren** und wählen Sie **Client-seitig Keep Alive**aus.



- Auf Serviceniveau

  Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**und wählen Sie den gewünschten Dienst aus. Aktivieren Sie im Abschnitt **Einstellungen** das Kontrollkästchen **Client Keep-Alive** .

2. Konfigurieren Sie die erforderlichen HTTP-Parameter für das HTTP-Profil, das an einen oder mehrere Dienste gebunden ist.
3. Navigieren Sie zu **System** > **Profile**, und wählen Sie auf der Registerkarte **HTTP-Profile** das gewünschte Profil aus, und aktualisieren Sie die erforderlichen HTTP-Parameter.

HTTP-Komprimierung

May 11, 2023

Für Websites mit komprimierbarem Inhalt implementiert die HTTP-Komprimierungsfunktion eine verlustfreie Komprimierung, um Latenz, lange Downloadzeiten und andere Probleme mit der Netzwerkleistung zu verringern, indem die von Servern an komprimierungsfähige Browser gesendeten HTTP-Antworten komprimiert werden. Sie können die Serverleistung verbessern, indem Sie die rechenintensive Komprimierungsaufgabe von Ihren Servern auf die NetScaler-Appliance übertragen.

In der folgenden Tabelle werden die Funktionen der HTTP-Komprimierungsfunktion beschrieben:

Funktionalität	Beschreibung
Komprimierungsverhältnis	Das Komprimierungsverhältnis hängt von den Dateitypen in den Antworten ab, ist jedoch immer signifikant, wodurch die über das Netzwerk übertragene Datenmenge spürbar reduziert wird.
Browser-Bewusstsein	NetScaler liefert komprimierte Daten nur an komprimierungsfähige Browser, wodurch die Transaktionszeit zwischen dem Client und dem Server verkürzt wird. Die meisten modernen Webbrowser unterstützen die HTTP-Komprimierung.
Blockierung der Komprimierung	Sie können Inhaltsfilter definieren, um die Komprimierung selektiv zu blockieren, indem Sie integrierte Aktionen anwenden.
Komprimierungs-Caching	Wenn die integrierte Caching-Funktion aktiviert ist, werden nachfolgende Anfragen für denselben Inhalt aus dem lokalen Cache bedient, wodurch die Anzahl der Roundtrips zum Server reduziert und die Transaktionszeiten verbessert werden.
HTTPS-Unterstützung	Die Komprimierung ist bei SSL-Verbindungen nützlich, da sie die Menge an Inhalten reduziert, die entweder auf dem Server oder von der NetScaler-Appliance verschlüsselt und vom Client entschlüsselt werden müssen.

Funktionalität	Beschreibung
Intelligente Response-Filterung	Die NetScaler-Komprimierungsengine filtert Serverantworten intelligent basierend auf definierten Komprimierungsparametern. Zum Beispiel erkennt die Komprimierungs-Engine Antworten und komprimierte Antworten ohne Inhaltslänge und komprimiert sie nicht. Die Erkennung komprimierter Antworten ermöglicht es Original-Sites, serverbasierte Komprimierung mit der NetScaler-Komprimierungsfunktion zu verwenden.
Kompressions-	Die NetScaler-Appliance leitet Anfragen von komprimierungsfähigen Clients transparent an komprimierungsfähige Server weiter, sodass Antworten auf diese Clients komprimiert werden und Antworten auf andere Clients nicht durch die Komprimierungsverarbeitung verzögert werden.

So funktioniert die HTTP-Komprimierung

Ein NetScaler kann sowohl statische als auch dynamisch generierte Daten komprimieren. Es wendet den GZIP- oder den DEFLATE-Komprimierungsalgorithmus an, um fremde und sich wiederholende Informationen aus den Serverantworten zu entfernen und die ursprünglichen Informationen in einem kompakteren und effizienteren Format darzustellen. Diese komprimierten Daten werden an den Browser des Clients gesendet und gemäß dem unterstützten Algorithmus oder den unterstützten Algorithmen des Browsers (GZIP oder DEFLATE) unkomprimiert.

Die NetScaler-Komprimierung behandelt statische und dynamische Inhalte unterschiedlich.

- Statische Dateien werden nur einmal komprimiert und eine komprimierte Kopie wird im lokalen Speicher gespeichert. Nachfolgende Clientanforderungen für zwischengespeicherte Dateien werden von diesem Speicher aus bedient.
- Dynamische Seiten werden jedes Mal dynamisch erstellt, wenn ein Kunde sie anfordert.

Wenn ein Client eine Anfrage an den Server sendet:

1. Die Clientanforderung kommt beim NetScaler an. Der ADC untersucht die Header und speichert Informationen darüber, welche Art von Komprimierung der Browser gegebenenfalls un-

terstützt.

2. Der ADC leitet die Anfrage an den Server weiter und erhält die Antwort.
3. Die NetScaler-Komprimierungsengine untersucht die Serverantwort auf Komprimierbarkeit, indem sie mit Richtlinien verglichen wird.
4. Wenn die Antwort mit einer Richtlinie übereinstimmt, die mit einer Komprimierungsaktion verknüpft ist, und der Clientbrowser einen durch die Aktion angegebenen Komprimierungsalgorithmus unterstützt, wendet NetScaler den Algorithmus an und sendet die komprimierte Antwort an den Clientbrowser.
5. Der Client wendet den unterstützten Komprimierungsalgorithmus an, um die Antwort zu dekomprimieren.

Konfiguration der HTTP-Komprimierung

Standardmäßig ist die Komprimierung auf dem NetScaler deaktiviert. Sie müssen die Funktion aktivieren, bevor Sie sie konfigurieren. Wenn die Funktion aktiviert ist, komprimiert der ADC Serveranforderungen, die durch Komprimierungsrichtlinien festgelegt wurden.

So aktivieren Sie die HTTP-Komprimierung über die CLI

Die Komprimierung kann nur für HTTP- und SSL-Dienste aktiviert werden. Sie können es global aktivieren, sodass es für alle HTTP- und SSL-Dienste gilt, oder Sie können es nur für bestimmte Dienste aktivieren.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die Komprimierung global oder für einen bestimmten Dienst zu aktivieren:

- `enable ns feature cmp`
  ODER
- `set service \<name\> -CMP YES`

So konfigurieren Sie die Komprimierung über die GUI

Führen Sie einen der folgenden Schritte aus:

Um die Komprimierung global zu aktivieren, navigieren Sie zu System > Einstellungen, klicken Sie auf **Grundfunktionen konfigurieren**und wählen Sie HTTP-Komprimierung aus.

Um die Komprimierung für einen bestimmten Dienst zu aktivieren, navigieren Sie zu **Traffic Management > Load Balancing > Services**, wählen Sie den Dienst aus und klicken Sie auf Bearbeiten. Klicken Sie in der Gruppe Einstellungen auf das Stiftsymbol und aktivieren Sie Komprimierung.

Konfigurieren einer Komprimierungsaktion

Eine Komprimierungsaktion gibt die Aktion an, die ausgeführt werden muss, wenn eine Anforderung oder Antwort mit der Regel (Ausdruck) in der Richtlinie übereinstimmt, mit der die Aktion verknüpft

ist. Sie können beispielsweise eine Komprimierungsrichtlinie konfigurieren, die Anforderungen identifiziert, die an einen bestimmten Server gesendet werden, und die Richtlinie mit einer Aktion verknüpfen, die die Antwort des Servers komprimiert.

Es gibt vier eingebaute Komprimierungsaktionen:

- COMPRESS: Verwendet den GZIP-Algorithmus, um Daten von Browsern zu komprimieren, die entweder GZIP oder sowohl GZIP als auch DEFLATE unterstützen. Verwendet den DEFLATE-Algorithmus, um Daten von Browsern zu komprimieren, die nur den DEFLATE-Algorithmus unterstützen. Wenn der Browser keinen der beiden Algorithmen unterstützt, wird die Antwort des Browsers nicht komprimiert.
- NOCOMPRESS: Komprimiert keine Daten.
- GZIP: Verwendet den GZIP-Algorithmus, um Daten für Browser zu komprimieren, die GZIP-Komprimierung unterstützen. Wenn der Browser den GZIP-Algorithmus nicht unterstützt, wird die Antwort des Browsers nicht komprimiert.
- DEFLATE: Verwendet den DEFLATE-Algorithmus, um Daten für Browser zu komprimieren, die den DEFLATE-Algorithmus unterstützen. Wenn der Browser den DEFLATE-Algorithmus nicht unterstützt, wird die Antwort des Browsers nicht komprimiert. Nachdem Sie eine Aktion erstellt haben, ordnen Sie die Aktion einer oder mehreren Komprimierungsrichtlinien zu.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Komprimierungsaktion zu erstellen:

```
add cmp action <name> <cmpType> [-addVaryHeader <addVaryHeader> -varyHeaderValue
<string>]
```

So konfigurieren Sie eine Komprimierungsrichtlinie über die CLI

Eine Komprimierungsrichtlinie enthält eine Regel, bei der es sich um einen logischen Ausdruck handelt, mit dem die NetScaler-Appliance den Datenverkehr identifizieren kann, der komprimiert werden soll.

Wenn NetScaler eine HTTP-Antwort von einem Server empfängt, werden die integrierten Komprimierungsrichtlinien und alle benutzerdefinierten Komprimierungsrichtlinien ausgewertet, um zu bestimmen, ob die Antwort komprimiert werden soll, und falls ja, der anzuwendende Komprimierungstyp. Die den Richtlinien zugewiesenen Prioritäten bestimmen die Reihenfolge, in der die Richtlinien mit den Anforderungen abgeglichen werden.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Komprimierungsrichtlinie zu erstellen:

```
add cmp policy <name> -rule <expression> -resAction <string>
```

So erstellen Sie eine Komprimierungsaktion über die GUI

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Aktionen**, klicken Sie auf **Hinzufügen**, und erstellen Sie eine Komprimierungsaktion, um die Art der Komprimierung anzugeben, die für die

HTTP-Antwort ausgeführt werden soll.

Konfigurieren einer Komprimierungsrichtlinie

Eine Komprimierungsrichtlinie enthält eine Regel, bei der es sich um einen logischen Ausdruck handelt, mit dem die NetScaler-Appliance den Datenverkehr identifizieren kann, der komprimiert werden soll.

Wenn NetScaler eine HTTP-Antwort von einem Server empfängt, werden die integrierten Komprimierungsrichtlinien und alle benutzerdefinierten Komprimierungsrichtlinien ausgewertet, um zu bestimmen, ob die Antwort komprimiert werden soll, und falls ja, der anzuwendende Komprimierungstyp. Die den Richtlinien zugewiesenen Prioritäten bestimmen die Reihenfolge, in der die Richtlinien mit den Anforderungen abgeglichen werden.

In der folgenden Tabelle sind die integrierten HTTP-Komprimierungsrichtlinien aufgeführt. Diese Richtlinien werden global aktiviert, wenn Sie die Komprimierung aktivieren.

Eingebaute klassische oder erweiterte Richtlinie	Beschreibung
ns_nocmp_mozilla_47, ns_adv_nocmp_mozilla_47	Verhindert die Komprimierung von CSS-Dateien, wenn eine Anfrage von einem Mozilla 4.7-Browser gesendet wird.
ns_cmp_mscss, ns_adv_cmp_mscss	Komprimiert CSS-Dateien, wenn die Anforderung von einem Microsoft Internet Explorer-Browser gesendet wird.
ns_cmp_msapp, ns_adv_cmp_msapp	Komprimiert Dateien, die von den folgenden Anwendungen generiert werden: Microsoft Office Word, Microsoft Office Excel, Microsoft Office PowerPoint.
ns_cmp_content_type, ns_adv_cmp_content_type	Komprimiert Daten, wenn die Antwort Header vom Typ Content-Typ enthält und Text enthält.
ns_nocmp_xml_de, ns_adv_nocmp_xml_de	Verhindert die Komprimierung, wenn eine Anfrage von einem Microsoft Internet Explorer-Browser gesendet wird und die Antwort einen Content-Type-Header enthält und Text oder XML enthält.

Bindung einer Komprimierungsrichtlinie

Um eine Komprimierungsrichtlinie in Kraft zu setzen, müssen Sie sie entweder global binden, damit sie für den gesamten Datenverkehr gilt, der durch den NetScaler fließt, oder an einen bestimmten virtuellen Server, sodass die Richtlinie nur für Anforderungen gilt, deren Ziel die VIP-Adresse dieses virtuellen Servers ist.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf jede positive Ganzzahl festlegen.

So binden Sie eine Komprimierungsrichtlinie über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Komprimierungsrichtlinie global oder an einen bestimmten virtuellen Server zu binden:

- `bind cmp global <policyName> [-priority <positive_integer>] [-state ( ENABLED|DISABLED)]...`
- `bind lb vserver <vserverName> -policyName <policyName> -type (Request| Response)-priority <positive_integer> )`

Wiederholen Sie diesen Befehl für jeden virtuellen Server, an den Sie die Komprimierungsrichtlinie binden möchten.

So binden Sie eine Komprimierungsrichtlinie über die GUI

Führen Sie einen der folgenden Schritte aus:

Navigieren Sie auf globaler Ebene zu **Optimierung** > **HTTP-Komprimierung** > **Richtlinien**, klicken Sie auf **Richtlinien-Manager** und binden Sie die erforderlichen Richtlinien, indem Sie den entsprechenden Bindepunkt und Verbindungstyp (Anforderung/Antwort) angeben.

Auf virtueller Serverebene

Navigieren Sie für den virtuellen Lastausgleichsserver zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie den erforderlichen virtuellen Server aus, klicken Sie auf **Richtlinien**und binden Sie die entsprechende Richtlinie.

Navigieren Sie für den virtuellen Content Switching-Server zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie den erforderlichen virtuellen Server aus, klicken Sie auf **Richtlinien**und binden Sie die entsprechende Richtlinie.

Festlegen der globalen Komprimierungsparameter für optimale Leistung

Viele Benutzer akzeptieren die Standardwerte für die globalen Komprimierungsparameter, aber Sie können möglicherweise eine effektivere Komprimierung bereitstellen, indem Sie diese Einstellungen anpassen.

> **Hinweis**
> Nachdem Sie die globalen Komprimierungsparameter konfiguriert haben, müssen Sie Ihre Appliance nicht neu starten. Sie werden sofort auf die neuen Flows angewendet.

In der folgenden Tabelle werden die Komprimierungsparameter beschrieben, die Sie auf dem NetScaler festlegen können.

Komprimierungs-Parameter	Beschreibung
Quantengröße	Größe des Puffers in KB für das Sammeln von Serverantworten beibehalten. Die Antworten werden komprimiert, wenn die Puffergröße diesen Wert überschreitet. Wenn Sie beispielsweise die Quantengröße auf 50 KB festlegen, komprimiert der NetScaler den Inhalt des Puffers, wenn seine Größe größer als 50 KB wird. Mindestwert: 1. Maximaler Wert: 63488 Standardwert: 57344.
Stufe der Kompression	Auf Serverantworten anzuwendende Komprimierungsgrad. Mögliche Werte: Beste Geschwindigkeit, beste Kompression, optimal.
Minimale Größe der HTTP-Antwort	Mindestgröße einer komprimierten HTTP-Antwort in Byte. Antworten, die kleiner als der durch diesen Parameter angegebene Wert sind, werden gesendet, ohne komprimiert zu werden.
Umgehung der Komprimierung bei der CPU-Auslastung	NetScaler CPU-Auslastung in Prozent, bei oder über der keine Komprimierung erfolgt. Standardwert: 100.
Richtlinientyp*	Art der für die Komprimierung verwendeten Richtlinien. Mögliche Werte: Classic, Advanced policy. Standard: Klassisch.
Serverseitige Komprimierung zulassen	Erlauben Sie Servern, komprimierte Daten an den NetScaler zu senden.
Push-Paket komprimieren	Komprimieren Sie nach Erhalt eines Pakets mit einem TCP-PUSH-Flag die akkumulierten Pakete sofort, ohne darauf zu warten, dass der Quantenpuffer gefüllt wird.

Komprimierungs-Parameter	Beschreibung
Externer Cache	Geben Sie eine private Antwortrichtlinie aus, die angibt, dass die Antwortnachricht für einen einzelnen Benutzer bestimmt ist und nicht von einem gemeinsam genutzten oder Proxy-Cache zwischengespeichert werden darf.

So konfigurieren Sie die HTTP-Komprimierung über die GUI

Führen Sie einen der folgenden Schritte aus:

- Um die Komprimierung global zu aktivieren, navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Grundfunktionen konfigurieren**und wählen Sie **HTTP-Komprimierung**aus.
- Um die Komprimierung für einen bestimmten Dienst zu aktivieren, navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, wählen Sie den Dienst aus und klicken Sie auf **Bearbeiten**.
- Klicken Sie in der Gruppe **Einstellungen** auf das Stiftsymbol und aktivieren Sie **Komprimierung**.

So erstellen Sie eine Komprimierungsaktion über die GUI

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Aktionen**, klicken Sie auf **Hinzufügen** und erstellen Sie eine Komprimierungsaktion, um den Komprimierungstyp anzugeben, der für die HTTP-Antwort ausgeführt werden soll

So erstellen Sie über die GUI eine Komprimierungsrichtlinie

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Richtlinien**, klicken Sie auf **Hinzufügen**und erstellen Sie eine Komprimierungsrichtlinie, indem Sie die Bedingung und die entsprechende Aktion angeben, die ausgeführt werden soll.

Bewertung der Komprimierungskonfiguration

Sie können die Komprimierungsstatistiken im Dashboard-Dienstprogramm oder in einem SNMP-Monitor anzeigen. Das Dashboard-Dienstprogramm zeigt zusammenfassende und detaillierte Statistiken in einem Tabellen- und Grafikformat an.

Optional können Sie auch Statistiken für eine Komprimierungsrichtlinie anzeigen, einschließlich der Anzahl der Anforderungen, die der Richtlinienzähler während der richtlinienbasierten Komprimierung erhöht.

> **Hinweis**
>
> - Weitere Informationen zu den Statistiken und Diagrammen finden Sie in der Dashboard-Hilfe zur NetScaler-Appliance.
> - Weitere Informationen zu SNMP finden Sie unter dem Thema SNMP .

So zeigen Sie Komprimierungsstatistiken mit der CLI an

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Komprimierungsstatistiken anzuzeigen:

1. Zum Anzeigen einer Zusammenfassung der Komprimierungsstatistiken.

```
stat cmp
```

> **Hinweis**
> Der Befehl stat cmp policy zeigt nur Statistiken für erweiterte Richtlinien zur Komprimierungsrichtlinie an.

2. Um Treffer und Details der Komprimierungsrichtlinie anzuzeigen

```
show cmp policy \<name\>
```

3. Um detaillierte Kompressionsstatistiken anzuzeigen

```
stat cmp -detail
```

So zeigen Sie Komprimierungsstatistiken mithilfe des Dashboards an:

Im Dashboard-Dienstprogramm können Sie die folgenden Arten von Komprimierungsstatistiken anzeigen:

- Wählen Sie Komprimierung aus, um eine Zusammenfassung der Komprimierungsstatistiken anzuzeigen.
- Um detaillierte Komprimierungsstatistiken nach Protokolltyp anzuzeigen, klicken Sie auf Details
- Um die Rate der von der Komprimierungsfunktion verarbeiteten Anforderungen anzuzeigen, klicken Sie auf die Registerkarte Grafische Ansicht.

So zeigen Sie Komprimierungsstatistiken mithilfe von SNMP an

Sie können die folgenden Komprimierungsstatistiken mithilfe der SNMP-Netzwerkverwaltungsanwendung anzeigen.

- Anzahl der Komprimierungsanforderungen (OID: 1.3.6.1.4.1.5951.4.1.1.50.1)
- Anzahl der übertragenen komprimierten Byte (OID: 1.3.6.1.4.1.5951.4.1.1.50.2)
- Anzahl empfangener komprimierbarer Byte (OID: 1.3.6.1.4.1.5951.4.1.1.50.3)
- Anzahl der übertragenen komprimierbaren Pakete (OID: 1.3.6.1.4.1.5951.4.1.1.50.4)
- Anzahl der empfangenen komprimierbaren Pakete (OID: 1.3.6.1.4.1.5951.4.1.1.50.5)
- Verhältnis der empfangenen komprimierbaren und übertragenen komprimierten Daten (OID: 1.3.6.1.4.1.5951.4.1.1.50.6)

- Verhältnis der insgesamt empfangenen Daten zu insgesamt übertragenen Daten (OID: 1.3.6.1.4.1.5951.4.1.1.50.7)

So zeigen Sie über die GUI weitere Komprimierungsstatistiken an

1. So zeigen Sie HTTP Komprimierungsstatistiken an:

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** und klicken Sie auf **Statistik**.

1. Zum Anzeigen von Statistiken einer Komprimierungsrichtlinie.

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Richtlinien** > wählen Sie die Richtlinie aus und klicken Sie auf **Statistik**.

1. So zeigen Sie Statistiken einer Bezeichnung für Komprimierungsrichtlinien an
2. Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Richtlinien** > wählen Sie ein Richtlinienlabel aus und klicken Sie auf **Statistik**.

Entladen der HTTP-Komprimierung

Die Durchführung einer Komprimierung auf einem Server kann die Leistung des Servers beeinträchtigen. Ein NetScaler, der vor Ihren Webservern platziert und für die HTTP-Komprimierung konfiguriert ist, entlastet die Komprimierung sowohl statischer als auch dynamischer Inhalte, wodurch Server-CPU-Zyklen und -Ressourcen eingespart werden.

Sie können die Komprimierung auf zwei Arten von den Webservern abladen:

Deaktivieren Sie die Komprimierung auf den Webservern, aktivieren Sie die NetScaler-Komprimierungsfunktion auf globaler Ebene und konfigurieren Sie Dienste für die Komprimierung.

Lassen Sie die Komprimierungsfunktion auf den Webservern aktiviert und konfigurieren Sie die NetScaler-Appliance so, dass der Header “Verschlüsselung akzeptieren” von allen HTTP-Clientanforderungen entfernt wird. Die Server senden dann unkomprimierte Antworten. Der NetScaler komprimiert die Serverantworten, bevor er sie an die Clients sendet.

> **Hinweis**
> Die zweite Option funktioniert nicht, wenn die Server automatisch alle Antworten komprimieren. Der NetScaler versucht nicht, eine bereits komprimierte Antwort zu komprimieren.

Der Parameter Servercmp ermöglicht es der NetScaler-Appliance, die Offload-HTTP-Komprimierung zu verarbeiten. Standardmäßig ist dieser Parameter eingeschaltet, damit der Server komprimierte Daten an die NetScaler-Appliance sendet. Um die HTTP-Komprimierung auszuladen, müssen Sie den Parameter servercmp auf OFF setzen. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
set service <service name> -CMP YES
```

Wiederholen Sie diesen Befehl für jeden Dienst, für den Sie die Komprimierung aktivieren möchten.


```
show service <service name>
```

Wiederholen Sie diesen Befehl für jeden Dienst, um zu überprüfen, ob die Komprimierung aktiviert ist.

```
Save config
```

```
set cmp parameter -serverCmp OFF
```

> **Hinweis:**
>
> Wenn der `Servercmp` Parameter eingeschaltet ist und die Appliance eine komprimierte Antwort vom Server erhält, komprimiert die Appliance die Daten nicht weiter. Stattdessen leitet es die komprimierte Antwort an den Client weiter.

Integriertes Caching

May 11, 2023

Der integrierte Cache bietet In-Memory-Speicher auf der NetScaler-Appliance und stellt Webinhalte für Benutzer bereit, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist. Für statische Inhalte erfordert der integrierte Cache wenig Ersteinrichtung. Nachdem Sie die integrierte Cache-Funktion aktiviert und eine grundlegende Einrichtung durchgeführt haben (z. B. die Menge an NetScaler-Appliance-Speicher bestimmt haben, die der Cache verwenden darf), verwendet der integrierte Cache integrierte Richtlinien, um bestimmte Arten von statischem Inhalt zu speichern und bereitzustellen, einschließlich einfacher Webseiten und Bilddateien. Sie können den integrierten Cache auch so konfigurieren, dass dynamische Inhalte gespeichert und bereitgestellt werden, die von Web- und Anwendungsservern als nicht zwischenspeicherbar gekennzeichnet sind (z. B. Datenbankdatensätze und Aktienkurse).

> **Hinweis:**
>
> Der Begriff Integrated Cache kann austauschbar mit AppCache verwendet werden; beachten Sie, dass beide Begriffe aus funktionaler Sicht dasselbe bedeuten.

Wenn eine Anfrage oder Antwort der Regel (logischer Ausdruck) entspricht, die in einer integrierten Richtlinie oder einer von Ihnen erstellten Richtlinie angegeben ist. Die NetScaler-Appliance führt die mit der Richtlinie verknüpfte Aktion aus. Standardmäßig speichern alle Richtlinien zwischengespeicherte Objekte in der Standardinhaltsgruppe und rufen sie aus der Standardinhaltsgruppe ab. Sie können Ihre eigenen Inhaltsgruppen für verschiedene Arten von Inhalten erstellen.

Damit die Appliance zwischengespeicherte Objekte in einer Inhaltsgruppe finden kann, können Sie Selektoren konfigurieren. Die Selektoren gleichen zwischengespeicherte Objekte mit Ausdrücken ab,

oder Sie können Parameter für die Suche nach Objekten in der Inhaltsgruppe angeben. Wenn Sie Selektoren wie von Citrix empfohlen verwenden, konfigurieren Sie sie zuerst, sodass Sie bei der Konfiguration von Inhaltsgruppen Selektoren angeben können. Richten Sie als Nächstes alle Inhaltsgruppen ein, die Sie hinzufügen möchten, damit sie verfügbar sind, wenn Sie die Richtlinien konfigurieren. Um die Erstkonfiguration abzuschließen, erstellen Sie Richtlinienbanken, indem Sie jede Richtlinie an einen globalen Bindungspunkt oder einen virtuellen Server binden. Oder Sie können ein Label binden, das von anderen Policenbanken aus aufgerufen werden kann.

Das integrierte Caching kann verbessert werden, indem die Methode für zwischengespeicherte Objekte vorab geladen wird, bevor sie ablaufen. Um den Umgang mit zwischengespeicherten Daten zu verwalten, können Sie zwischengespeicherte Header konfigurieren, die in die Antworten eingefügt werden. Der integrierte Cache kann auch als Forward-Proxy für andere Cache-Server fungieren.

> **Hinweis:**
>
> Integriertes Caching erfordert eine gewisse Vertrautheit mit HTTP-Anfragen und -Antworten. Informationen zur Struktur von HTTP-Daten finden Sie unter *Live-HTTP-Headers* unter "<http://livehttpheaders.mozdev.org/>."

So funktioniert der Integrationscache

Der integrierte Cache überwacht HTTP- und SQL-Anfragen, die durch die NetScaler-Appliance fließen, und vergleicht die Anfragen mit gespeicherten Richtlinien. Je nach Ergebnis durchsucht die integrierte Cache-Funktion entweder den Cache nach der Antwort oder leitet die Anfrage an den Ursprungsserver weiter. Bei HTTP-Anfragen dient das integrierte Caching als Teilinhalt aus dem Cache als Antwort auf einzelne Bytebereichsanfragen und mehrteilige Bytebereichsanforderungen.

Zwischengespeicherte Daten werden komprimiert, wenn der Client komprimierte Inhalte akzeptiert. Sie können Ablaufzeiten für eine Inhaltsgruppe konfigurieren und Einträge in einer Inhaltsgruppe selektiv ablaufen lassen.

Daten, die aus dem integrierten Cache bereitgestellt werden, sind ein Treffer, und vom Ursprung bereitgestellte Daten sind ein Cache-Fehler, wie in der folgenden Tabelle beschrieben.

Art der Transaktion	Spezifikation
Treffer im Cache	Antworten, die die NetScaler-Appliance aus dem Cache bereitstellt, darunter: Statische Objekte, z. B. Bilddateien und statische Webseiten, 200 OK-Seiten, 203 Seiten mit nicht autoritativen Antworten, 300 Multiple-Choices-Seiten, 301 dauerhaft verschobene Seiten, 302 gefundene Seiten, 304 nicht geänderte Seiten. Diese Antworten werden als positive Antworten bezeichnet. Die NetScaler-Appliance speichert auch die folgenden negativen Antworten im Cache: 307 Temporäre Umleitungsseiten, 403 verbotene Seiten, 404 Seiten nicht gefunden, 410 Gone Pages. Um die Leistung weiter zu verbessern, können Sie die NetScaler-Appliance so konfigurieren, dass mehr Inhaltstypen zwischengespeichert werden.
Speicherbarer Cache-Fehler	Bei einem Speichercachefehler ruft die NetScaler-Appliance die Antwort vom Ursprungsserver ab und speichert die Antwort im Cache, bevor sie an den Client weitergeleitet wird.
Nicht speicherbarer Cache-Fehler	Ein nicht speicherbarer Cache-Fehler ist für das Caching ungeeignet. Standardmäßig ist jede Antwort, die die folgenden Statuscodes enthält, ein nicht speicherbarer Cache-Fehler: 201, 202, 204, 205, 206 Statuscodes, Alle 4xx-Codes, außer 403, 404 und 410, 5xx-Statuscodes

> **Hinweis:**
>
> Verwenden Sie die NITRO-API, um dynamisches Caching in Ihre Anwendungsinfrastruktur zu integrieren, um Cache-Befehle aus der Ferne auszuführen. Sie können beispielsweise Trigger konfigurieren, die zwischengespeicherte Antworten ablaufen lassen, wenn eine Datenbanktabelle aktualisiert wird.

Um die Synchronisation der zwischengespeicherten Antworten mit den Daten auf dem Origi-

nalserver sicherzustellen, konfigurieren Sie Ablaufmethoden. Wenn die NetScaler-Appliance eine Anfrage erhält, die mit einer abgelaufenen Antwort übereinstimmt, aktualisiert sie die Antwort vom Ursprungsserver.

> **Hinweis:**
>
> Citrix empfiehlt, dass Sie die Uhrzeiten auf der NetScaler-Appliance und einem oder mehreren Backend-Servern synchronisieren.

So funktioniert der dynamische Cache

Dynamisches Caching wertet HTTP-Anfragen und -Antworten auf der Grundlage von Parameter-Wert-Paaren, Zeichenketten, Zeichenkettenmustern oder anderen Daten aus. Nehmen wir zum Beispiel an, dass ein Benutzer in einer Anwendung zur Fehlerberichterstattung nach Bug 31231 sucht. Der Browser sendet im Namen des Benutzers die folgende Anfrage:

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
         Template=view&TableId=1000
2
3     Host: mycompany.net
4
5     User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
          Gecko/2008052906 Firefox/3.0
6
7     Accept: text/html,application/xhtml+xml,application/xml;q
         =0.9,\*/\*;q=0.8
8
9     Accept-Language: en-us,en;q=0.5
10 <!--NeedCopy-->
```

In diesem Beispiel enthalten GET-Anfragen für diese Anwendung zur Fehlerberichterstattung immer die folgenden Parameter:

- IssuePage
- RecordID
- Vorlage
- TableId

GET-Anforderungen aktualisieren oder ändern die Daten nicht, sodass Sie diese Parameter in den Caching-Richtlinien und -Selektoren wie folgt konfigurieren können:

- Sie konfigurieren eine Caching-Richtlinie, die in HTTP-Anfragen nach der Zeichenfolge mybugreportingsystem und der GET-Methode sucht. Diese Richtlinie leitet passende Anfragen für Bugs an eine Inhaltsgruppe weiter.

- In der Inhaltsgruppe für Bugs konfigurieren Sie einen `hit`-Selektor, der verschiedenen Parameter-Wert-Paaren entspricht, einschließlich IssuePage, RecordID usw.

> **Hinweis**
>
> Ein Browser kann mehrere GET-Anfragen basierend auf einer Benutzeraktion senden. Im Folgenden finden Sie eine Reihe von drei separaten GET-Anfragen, die ein Browser ausgibt, wenn ein Benutzer nach einem Fehler basierend auf einer Fehler-ID sucht.

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbtns&RecordId=31231&TableId=1000
4
5     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbody&RecordId=31231&tableid=1000
6 <!--NeedCopy-->
```

Um diese Anfragen zu erfüllen, werden mehrere Antworten an den Browser des Benutzers gesendet, und die Webseite, die der Benutzer sieht, ist eine Zusammenstellung der Antworten.

Wenn ein Benutzer einen Fehlerbericht aktualisiert, müssen die entsprechenden Antworten im Cache mit Daten vom Originalserver aktualisiert werden. Die Anwendung zur Fehlerberichterstattung gibt HTTP-POST-Anfragen aus, wenn ein Benutzer einen Fehlerbericht aktualisiert. In diesem Beispiel konfigurieren Sie Folgendes, um sicherzustellen, dass POST-Anfragen eine Invalidierung im Cache auslösen:

- Eine Richtlinie zur Invalidierung von Anfragen, die nach der Zeichenfolge mybugreportingsystem und der POST-HTTP-Anforderungsmethode sucht und passende Anfragen für Fehlerberichte an die Inhaltsgruppe weiterleitet.
- Ein Invalidierungsselektor für die Inhaltsgruppe für Fehlerberichte, bei dem zwischengespeicherte Inhalte basierend auf dem Parameter recordId ablaufen. Dieser Parameter erscheint in allen Antworten, sodass der Invalidierungsselektor alle relevanten Elemente im Cache ablaufen lassen kann.

Der folgende Auszug zeigt eine POST-Anforderung, die den Beispielfehlerbericht aktualisiert.

```
1     POST /mybugreportingsystem/mybugreport.dll?TransitionForm HTTP/1.1\
          r\n
2
3     User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
          Opera 7.23 [en]\r\n
4
5     Host: mybugreportingsystem\r\n
6
```



```
7      Cookie:ttSearch.134=%23options%3Afalse%23active%23owner%3Afalse%23
          unowned%3Afalse%23submitter%3Afalse%23incsub%3Atrue;
8
9      Cookie2: $Version=1\r\n
10
11     . . .
12
13     \r\n
14
15     ProjectId=2&RecordId=31231&TableId=1000&TransitionId=1&Action=
          Update&CopyProjectId=0&ReloadForm=0&State=&RecordLockId=49873+
          issues+in+HTTP&F43. . .
16 <!--NeedCopy-->
```

Wenn die NetScaler-Appliance diese Anfrage empfängt, macht sie Folgendes:

- Ordnet der Anfrage eine Ungültigkeitsrichtlinie zu.
- Findet die Inhaltsgruppe, die in der Richtlinie benannt ist.
- Wendet den Invalidierungsselektor für diese Inhaltsgruppe an und verfällt alle Antworten, die mit recordID=31231 übereinstimmen.

Wenn ein Benutzer eine neue Anfrage für diesen Fehlerbericht ausgibt, geht die NetScaler-Appliance zum Ursprungsserver, um aktualisierte Kopien aller Antworten zu erhalten, die der Berichtsinstanz zugeordnet sind. Es speichert die Antworten in der Inhaltsgruppe und stellt sie dem Browser des Benutzers zur Verfügung, der den Bericht neu zusammenstellt und anzeigt.

Integrierten Cache konfigurieren

Um den integrierten Cache verwenden zu können, müssen Sie die Lizenz installieren und die Funktion aktivieren. Nachdem Sie den integrierten Cache aktiviert haben, zwischenspeichert die NetScaler® Appliance automatisch statische Objekte gemäß den integrierten Richtlinien und generiert Statistiken zum Cacheverhalten. (Integrierte Richtlinien haben einen Unterstrich in der Anfangsposition des Richtliniennamens.)

Auch wenn die integrierten Richtlinien für Ihre Situation ausreichend sind, möchten Sie möglicherweise die globalen Attribute ändern. Beispielsweise können Sie die Größe des Speichers der NetScaler-Appliance ändern, der dem integrierten Cache zugewiesen ist.

Wenn Sie den Cache-Betrieb beobachten möchten, bevor Sie die Einstellungen ändern, lesen Sie “Zwischengespeicherte Objekte und Cache-Statistiken anzeigen. “

> **Hinweis:**

> Der NetScaler Cache ist ein speicherinterner Speicher, der beim Neustart der Appliance gelöscht wird.

Um die integrierte Cache-Lizenz zu installieren

- Eine integrierte Cache-Lizenz ist erforderlich.
- Rufen Sie einen Lizenzcode von Citrix ab, gehen Sie zur Befehlszeilenschnittstelle und melden Sie sich an.

Kopieren Sie die Lizenzdatei an der Befehlszeilenschnittstelle in den Ordner `/nsconfig/license`.

- Starten Sie die NetScaler-Appliance neu, indem Sie den folgenden Befehl verwenden:

```
reboot
```

So aktivieren Sie das integrierte Caching:
Wenn Sie das integrierte Caching aktivieren, beginnt die NetScaler-Appliance, Serverantworten zwischenzuspeichern. Wenn Sie keine Richtlinien oder Inhaltsgruppen konfiguriert haben, speichern die integrierten Richtlinien zwischengespeicherte Objekte in der Standardinhaltsgruppe.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um das integrierte Caching zu aktivieren oder zu deaktivieren:

```
enable ns feature IC
```

Konfigurieren globaler Attribute für das Caching

Globale Attribute gelten für alle zwischengespeicherten Daten. Sie können die Menge an NetScaler-Speicher angeben, die dem integrierten Cache zugewiesen ist, indem Sie den Header einfügen. Ein Kriterium für die Überprüfung, ob ein zwischengespeichertes Objekt bereitgestellt werden muss. Die maximale Länge eines POST-Textes, die im Cache zulässig ist, ob die Richtlinienauswertung für HTTP-GET-Anforderungen Bypass werden soll, und eine Aktion, die ergriffen werden muss, wenn eine Richtlinie nicht ausgewertet werden kann.

Die Cache-Speicherkapazität ist nur durch den Speicher der Hardware-Appliance begrenzt. Außerdem ist sich jede Paket-Engine (zentraler Distributions-Hub aller eingehenden TCP-Anforderungen) in der nCore NetScaler-Appliance der Objekte bewusst, die von anderen Paket-Engines in der nCore NetScaler-Appliance zwischengespeichert wurden.

> **Hinweis:**
>
> Wenn das globale Standardspeicherlimit auf 0 festgelegt ist und die Funktion Integriertes Caching (IC) aktiviert ist, zwischengespeichert die Appliance keine Objekte. Zum Zwischenspeichern müssen Sie explizit das globale Speicherlimit konfigurieren. Wenn Sie jedoch die Option “set authentication, authorization and auditing parameter enableStaticPageCaching” aktivieren, wird in der Appliance ein Teil des Standardspeichers konfiguriert. Dieser Speicher

> reicht nicht aus, um große Objekte zwischenzuspeichern, weshalb IC ein höheres Speicherlimit zugewiesen werden muss. Sie können dies tun, indem Sie den Befehl “set cache parameter —MemLimit” konfigurieren. Die neue Einstellung wird erst angewendet, nachdem Sie die Konfiguration gespeichert und die Appliance neu gestartet haben.

Sie können das globale Speicherlimit ändern, das für das Zwischenspeichern von Objekten konfiguriert ist. Wenn Sie das globale Speicherlimit jedoch auf einen Wert aktualisieren, der unter dem vorhandenen Wert liegt (z. B. von 10 GB auf 4 GB), verwendet die Appliance weiterhin das Speicherlimit.

Das bedeutet, dass das integrierte Caching-Limit zwar auf einen bestimmten Wert konfiguriert ist, das tatsächlich verwendete Limit jedoch höher sein kann. Dieser überschüssige Speicher wird jedoch freigegeben, wenn die Objekte aus dem Cache entfernt werden.

Die Ausgabe des Befehls show cache parameter gibt den konfigurierten Wert (Speicherauslastungslimit) und den tatsächlich verwendeten Wert (Speicherauslastungslimit (aktiver Wert)) an.

Geben Sie in der Befehlszeile Folgendes ein:

```
1     set cache parameter [-memLimit <MBytes>] [-via <string>] [-
         verifyUsing <criterion>] [-maxPostLen <positiveInteger>] [-
         prefetchMaxPending <positiveInteger>] [-enableBypass(YES|NO)] [-
         undefAction (NOCACHE|RESET)]
2 <!--NeedCopy-->
```

Integriertes Caching durch NetScaler-GUI aktivieren

Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Basisfunktionen konfigurieren**, und wählen Sie **Integriertes Caching** aus.

Konfigurieren Sie globale Einstellungen für das Caching mit der NetScaler-GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Einstellungen ändern**, und konfigurieren Sie die globalen Einstellungen für das Caching.

Richten Sie eine integrierte Content-Gruppe, ein Musterset und Richtlinien für Integrated Cache ein

Die NetScaler-Appliance verfügt über eine integrierte Caching-Konfiguration, die Sie zum Caching von Inhalten verwenden können. Die Konfiguration besteht aus einer Inhaltsgruppe namens ctx_cg_poc, einem Mustersatz namens ctx_file_extensions und einer Reihe integrierter Cache-Richtlinien. In der Inhaltsgruppe ctx_cg_poc werden nur Objekte zwischengespeichert, die 500 KB oder weniger groß

sind. Der Inhalt wird für 86000 Sekunden zwischengespeichert, und das Speicherlimit für die Inhaltsgruppe beträgt 512 MB. Das Musterset ist ein indiziertes Array gängiger Erweiterungen für den Dateitypabgleich.

In der folgenden Tabelle sind die integrierten Richtlinien für das integrierte Caching aufgeführt. Standardmäßig sind die Richtlinien an keinen Bindungspunkt gebunden. Sie müssen die Richtlinien an einen Bindungspunkt binden, wenn die NetScaler-Appliance den Datenverkehr anhand der Richtlinien auswerten soll. Die Richtlinien speichern Objekte in der Inhaltsgruppe ctx_cg_poc im Cache.

Name der integrierten Caching-Richtlinie	Richtlinienregel
_cacheVPNStaticObjects	HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS_IN
_cacheTCPVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(“.css”)
_cacheOCVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(“.pdf”)
_cacheWFStaticObjects	HTTP.REQ.URL.ENDSWITH(“.js”)
_mayNoCacheReq	HTTP.RES.HEADER(“Content-Type”).CONTAINS(“application/x-javascript”)
_noCacheRest	TRUE

Cache-Konfiguration leeren

Sie können eine Cache-Gruppe, Cache-Gruppen oder einen Cache-Objekt-Locator leeren. Im Folgenden finden Sie die Befehle zum Leeren von Cache-Objekten.

Geben Sie in der Befehlszeile Folgendes ein:

```
flush cache contentgroup all
```

Beispiel

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
3
4          Flush cache contentGroup all
5          done
6
7  `flush cache contentgroup <content group name>`
8  <!--NeedCopy-->
```


Beispiel:

```
        0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
           html?name=hello
        0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
           html?name=hi

        Flush cache ob -| 0x00000089bae000000004
        done

`flush cache object (-locator <positive_integer> | (-url <URL> (-host <
   string> [-port <port>] [-groupName <string>] [-httpMethod ( GET |
   POST )]))))`
<!--NeedCopy-->
```

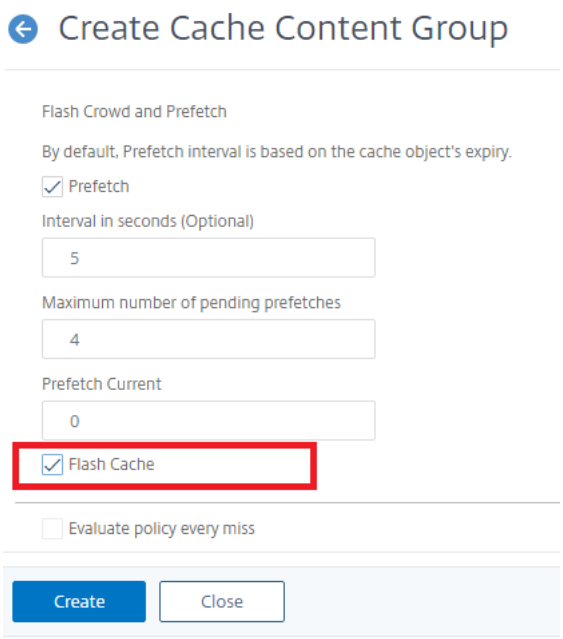
Beispiel:

```
        0x00000089bae000000006 DEFAULT GET //1.1.1.1:80/html/index.html

        flush cache ob -URL /html/index.html -host 1.1.1.1 -groupName
           DEFAULT
        done
<!--NeedCopy-->
```

Leeren der Cachekonfiguration mit der NetScaler-GUI

Führen Sie die Schritte zur Konfiguration des Cache-Leerens mithilfe der NetScaler-GUI aus

1. Navigieren Sie zu **Optimierung** > **Inhaltsgruppen**.
2. Klicken Sie im Detailbereich **Inhaltsgruppen** auf **Hinzufügen**.
3. Stellen Sie auf der Seite “ **Cache-Inhaltsgruppen erstellen** “ auf der Registerkarte “ **Andere** “ den folgenden Parameter ein:
   a) Cache leeren. Aktivieren Sie das Kontrollkästchen, um das Cache-Objekt zu leeren.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Integriertes Caching für verschiedene Szenarien konfigurieren

Im folgenden Abschnitt wird die Konfiguration von integriertem Caching auf der NetScaler Appliance für verschiedene Szenarien beschrieben.

Ab der NetScaler-Version 9.2 verfügt das integrierte Caching über mehr Speicher für das Caching. Der integrierte Caching-Speicher ist nur durch den auf der Hardware-Appliance verfügbaren Speicher begrenzt. Sie können der integrierten Caching-Funktion bis zu 50 Prozent des verfügbaren Speichers zuweisen.

So legen Sie die Speicherzuweisung für den Cache über die CLI fest

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache parameter -memlimit <value>
```

> **Hinweis:**
>
> Das standardmäßige globale Speicherlimit für integriertes Caching ist Null. Selbst wenn Sie die integrierte Caching-Funktion aktivieren, speichert die NetScaler Appliance daher keine Objekte im Cache, bis das globale Speicherlimit explizit festgelegt ist.

Im folgenden Abschnitt werden Sie angewiesen, integriertes Caching für verschiedene Szenarien zu konfigurieren.

> **Hinweis:**
>
> Das Speicherlimit der NetScaler Appliance wird beim Start der Appliance identifiziert. Daher

> müssen Sie bei jeder Änderung des Speicherlimits die Appliance neu starten, damit die Änderungen für alle Packet Engines gelten.

Das integrierte Caching ist aktiviert und das Cache-Speicherlimit ist auf einen Wert ungleich Null gesetzt

Stellen Sie sich ein Szenario vor, in dem Sie die Appliance starten, die integrierte Caching-Funktion aktiviert ist und das globale Speicherlimit auf eine positive Zahl gesetzt ist. Der Speicher, den Sie zuvor eingestellt hatten, wird während des Startvorgangs der integrierten Caching-Funktion zugewiesen. Möglicherweise möchten Sie das Speicherlimit je nach verfügbarem Speicher auf der Appliance auf einen anderen Wert ändern.

Konfiguration mit der CLI

1. Anzeigen des Cache-Parameters

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 MBytes
4                  Memory usage limit (active value): 500 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

1. Festlegen eines Speicherlimits ungleich Null

```
set cache parameter -memlimit 600
```

> **Hinweis:**
>
> Der vorangehende Befehl zeigt die folgende Warnmeldung an: **Warnung: Um ein neues Limit für den integrierten Cache zu verwenden, speichern Sie die Konfiguration und starten Sie die NetScaler Appliance neu.**

1. Speichern Sie die Konfiguration

```
save config
```

1. Führen Sie an der Shell-Eingabeaufforderung den folgenden Befehl aus, um dies in der Konfigurationsdatei zu überprüfen.


```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Starten Sie die Appliance neu

```
root@ns## reboot
```

1. Überprüfen Sie den neuen Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 MBytes
4                  Memory usage limit (active value): 600 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

Nachdem alle Paketmodule erfolgreich gestartet wurden, verhandelt die integrierte Caching-Funktion den von Ihnen konfigurierten Speicher. Wenn die Appliance den konfigurierten Speicher nicht verwenden kann, wird der Speicher entsprechend zugewiesen. Wenn der verfügbare Speicher geringer ist als der, den Sie zugewiesen haben, empfiehlt die Appliance eine geringere Anzahl. Die integrierte Caching-Funktion verwendet denselben Wert wie den aktiven Wert.

Das integrierte Caching ist deaktiviert und das Cache-Speicherlimit ist auf einen Wert ungleich Null gesetzt

In diesem Szenario wird beim Starten der Appliance die integrierte Caching-Funktion deaktiviert und das globale Speicherlimit auf eine positive Zahl gesetzt. Daher wird dem integrierten Caching während des Startvorgangs kein Speicher zugewiesen.

Konfiguration mit der CLI

1. Anzeigen des Cache-Parameters

```
1          > show cache parameter
2                  Integrated cache global configuration:
```



```
3                   Memory usage limit: 600 MBytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```

1. Legen Sie ein neues Speicherlimit fest

```
set cache parameter -memlimit 500
```

> **Hinweis:**
>
> Der vorherige Befehl zeigt die folgende Warnmeldung an: **Warnung: Funktion nicht aktiviert [IC]**.

1. Speichern Sie die Konfiguration

```
save config
```

1. Führen Sie an der Shell-Eingabeaufforderung den folgenden Befehl aus, um dies in der Konfigurationsdatei zu überprüfen

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Überprüfen Sie den neuen Wert für das Speicherlimit

```
1           > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 500 MBytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```


1. Aktivieren Sie die integrierte Caching-Funktion

```
enable ns feature IC
```

1. Überprüfen Sie den neuen Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 Mbytes
4                  Memory usage limit (active value): 500 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

> **Hinweis:**
>
> 500 MB Speicher werden der integrierten Caching-Funktion zugewiesen.

1. Speichern Sie die Konfiguration, um sicherzustellen, dass der Speicher der Funktion automatisch zugewiesen wird, wenn die Appliance neu gestartet wird.

Integriertes Caching ist aktiviert und der Cache-Speicher ist auf Null gesetzt

In diesem Szenario ist beim Starten der Appliance die integrierte Caching-Funktion aktiviert und das globale Speicherlimit wird auf Null gesetzt. Daher wird dem integrierten Caching während des Startvorgangs kein Speicher zugewiesen.

Konfiguration mit der CLI

1. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Überprüfen Sie den Wert für das Speicherlimit


```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 0 Mbytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

> **Hinweis:**
>
> Das Speicherlimit ist auf 0 MB festgelegt und der integrierten Caching-Funktion wird kein Speicher zugewiesen.

1. Legen Sie die Speicherlimits fest, um sicherzustellen, dass die integrierte Caching-Funktion Objekte zwischenspeichert

```
set cache parameter -memLimit 600
```

Sobald Sie den vorhergehenden Befehl ausführen, handelt die Appliance Speicher für die integrierte Caching-Funktion aus, und der verfügbare Speicher wird der Funktion zugewiesen. Dies führt dazu, dass die Appliance Objekte zwischenspeichert, ohne die Appliance neu zu starten.

1. Überprüfen Sie den Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 Mbytes
4                  Memory usage limit (active value): 600 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3:
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```


> **Hinweis:**
>
> 600 MB Arbeitsspeicher werden der integrierten Caching-Funktion zugewiesen.

1. Speichern Sie die Konfiguration. Stellen Sie sicher, dass der Speicher der Funktion automatisch zugewiesen wird, wenn die Appliance neu gestartet wird.
2. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

Integriertes Caching ist deaktiviert und der Cache-Speicher ist auf Null gesetzt

In diesem Szenario wird beim Starten der Appliance die integrierte Caching-Funktion deaktiviert und das globale Speicherlimit auf Null gesetzt. Daher wird dem integrierten Caching während des Startvorgangs kein Speicher zugewiesen.

Konfiguration mit der CLI

1. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Überprüfen Sie den Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 0 Mbytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
```



```
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das Speicherlimit ist auf 0 MB festgelegt und der integrierten Caching-Funktion wird kein Speicher zugewiesen. Wenn Sie einen Cache-Konfigurationsbefehl ausführen, wird außerdem die folgende Warnmeldung angezeigt: **Warnung: Funktion nicht aktiviert [IC]**.

1. Aktivieren Sie die integrierte Caching-Funktion

```
enable ns feature IC
```

> **Hinweis:**
>
> In diesem Stadium, wenn Sie die integrierte Caching-Funktion aktivieren, weist die Appliance der Funktion keinen Speicher zu. Daher wird kein Objekt im Speicher zwischengespeichert. Wenn Sie einen Cache-Konfigurationsbefehl ausführen, wird außerdem die folgende Warnmeldung angezeigt: Für IC ist **kein Speicher konfiguriert. Verwenden Sie den Befehl set cache parameter, um das Speicherlimit festzulegen.**

1. Legen Sie die Speicherlimits fest, um sicherzustellen, dass die integrierte Caching-Funktion Objekte zwischenspeichert

```
set cache parameter -memLimit 500
```

Sobald Sie den vorhergehenden Befehl ausführen, handelt die Appliance Speicher für die integrierte Caching-Funktion aus, und der verfügbare Speicher wird der Funktion zugewiesen. Dies führt dazu, dass die Appliance Objekte zwischenspeichert, ohne die Appliance neu zu starten.

> **Hinweis:**
>
> Die Reihenfolge, in der Sie die Funktion aktivieren und die Speichergrenzen festlegen, ist wichtig. Wenn Sie die Speicherlimits festlegen, bevor Sie die Funktion aktivieren, wird die folgende Warnmeldung angezeigt: **Warnung: Funktion nicht aktiviert [IC]**.

1. Überprüfen Sie den Wert für das Speicherlimit

```
        > show cache parameter
                Integrated cache global configuration:
                Memory usage limit: 500 Mbytes
                Memory usage limit (active value): 500 Mbytes
                Maximum value for Memory usage limit: 843 MBytes
                Via header: NS-CACHE-9.3:
                Verify cached object using: HOSTNAME_AND_IP
                Max POST body size to accumulate: 0 bytes
                Current outstanding prefetches: 0
                Max outstanding prefetches: 4294967295
                Treat NOCACHE policies as BYPASS policies: YES
```



```
12                  Global Undef Action: NOCACHE
13  <!--NeedCopy-->
```

> **Hinweis:**
>
> 500 MB Speicher werden der integrierten Caching-Funktion zugewiesen.

1. Speichern Sie die Konfiguration

```
save config
```

1. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

Selektoren und grundlegenden Content-Gruppen konfigurieren

May 11, 2023

Sie können Selektoren konfigurieren und sie auf Inhaltsgruppen anwenden. Wenn Sie einer oder mehreren Inhaltsgruppen einen Selektor hinzufügen, geben Sie an, ob der Selektor zur Identifizierung von Cache-Anfragen oder zur Identifizierung zwischengespeicherter Objekte verwendet werden soll, die ungültig gemacht werden sollen (abgelaufen). Selektoren sind optional. Alternativ können Sie Inhaltsgruppen so konfigurieren, dass sie `hit` Parameter und Invalidierungsparameter verwenden. Citrix empfiehlt jedoch, dass Sie Selektoren konfigurieren.

Nachdem Sie die Selektoren konfiguriert oder sich dafür entschieden haben, stattdessen Parameter zu verwenden, können Sie eine grundlegende Inhaltsgruppe einrichten. Nachdem Sie die grundlegende Content-Gruppe erstellt haben, müssen Sie entscheiden, wie Objekte aus dem Cache abgelaufen werden sollen, und den Cache-Ablauf konfigurieren. Sie können den Cache weiter ändern, wie unter Verbesserung der Cache-Leistung und Konfigurieren von Cookies, Headern und Pollingbeschrieben, aber Sie möchten möglicherweise zuerst Caching-Richtlinien konfigurieren.

> **Hinweis**
>
> Parameter und Selektoren für Inhaltsgruppen werden nur bei Anfragen verwendet, und Sie verknüpfen sie in der Regel mit Richtlinien, die MAY_CACHE- oder MAY_NOCACHE-Aktionen verwenden.

Vorteile von Selektoren

Ein Selektor ist ein Filter, der bestimmte Objekte in einer Inhaltsgruppe lokalisiert. Wenn Sie keinen Selektor konfigurieren, sucht die Citrix® ADC Appliance nach einer exakten Übereinstimmung in der Inhaltsgruppe. Dies kann dazu führen, dass sich mehrere Kopien desselben Objekts in einer Inhaltsgruppe befinden. Beispielsweise muss eine Inhaltsgruppe, die keinen Selektor hat, möglicherweise URLs für host1.domain.com\ mypage.htm, host2.domain.com\ mypage.htm und host3.domain.com\ mypage.htm speichern. Im Gegensatz dazu kann ein Selektor nur die URL (mypage.html, verwendet den Ausdruck http.req.url) und die Domain (.com, verwendet den Ausdruck http.req.hostname.domain) finden, sodass die Anfragen über dieselbe URL erfüllt werden können.

Selektorausdrücke können einen einfachen Abgleich von Parametern durchführen (z. B. um Objekte zu finden, die einigen Abfragezeichenfolgenparametern und ihren Werten entsprechen). Ein Selektorausdruck kann boolesche Logik, arithmetische Operationen und Kombinationen von Attributen verwenden, um Objekte zu identifizieren (z. B. Segmente eines URL-Stammes, eine Abfragezeichenfolge, eine Zeichenfolge in einem POST-Anforderungstext, eine Zeichenfolge in einem HTTP-Header, ein Cookie). Selektoren können auch programmatische Funktionen ausführen, um Informationen in einer Anfrage zu analysieren. Beispielsweise kann ein Selektor Text in einem POST-Text extrahieren, den Text in eine Liste konvertieren und ein bestimmtes Element aus der Liste extrahieren.

Weitere Informationen zu Ausdrücken und was Sie in einem Ausdruck angeben können, finden Sie unter Richtlinien und Ausdrücke.

Parameter anstelle von Selektoren verwenden

Citrix empfiehlt zwar die Verwendung von Selektoren für eine Inhaltsgruppe, Sie können jedoch stattdessen `hit` Parameter und Invalidierungsparameter konfigurieren. Angenommen, Sie konfigurieren in einer Inhaltsgruppe drei `hit` Parameter für Fehlerberichte: BugID, Issuer und Beauftragter. Wenn eine Anfrage BugID=456 mit issuer=rohiTV und Assignee=Robert enthält, kann die NetScaler-Appliance Antworten bereitstellen, die diesen Parameterwert-Paaren entsprechen.

Bei Invalidierungsparametern in einer Inhaltsgruppe laufen zwischengespeicherte Einträge ab. Nehmen wir zum Beispiel an, dass BugID ein Invalidierungsparameter ist und ein Benutzer eine POST-Anfrage sendet, um einen Fehlerbericht zu aktualisieren. Eine Invalidierungsrichtlinie leitet die Anfrage an diese Inhaltsgruppe weiter, und der Invalidierungsparameter für die Inhaltsgruppe lässt alle zwischengespeicherten Antworten ablaufen, die dem BugID-Wert entsprechen. (Wenn ein Benutzer das nächste Mal eine GET-Anfrage für diesen Bericht ausgibt, kann eine Caching-Richtlinie es der NetScaler-Appliance ermöglichen, den zwischengespeicherten Eintrag für den Bericht vom Originalserver zu aktualisieren.)

Beachten Sie, dass derselbe Parameter als Parameter oder als `hit` Invalidierungsparameter verwendet werden kann.

Inhaltsgruppen extrahieren Anforderungsparameter in der folgenden Reihenfolge:

- URL-Abfrage
- POST-Körper
- Cookie-Kopfzeile

Nach dem ersten Vorkommen eines Parameters, unabhängig davon, wo er in der Anfrage aufgetreten ist, werden alle nachfolgenden Vorkommen ignoriert. Wenn beispielsweise ein Parameter sowohl in der URL-Abfrage als auch im POST-Text vorhanden ist, wird nur der Parameter in der URL-Abfrage berücksichtigt.

Wenn Sie sich entscheiden, Treffer- und Invalidierungsparameter für eine Inhaltsgruppe zu verwenden, konfigurieren Sie die Parameter bei der Konfiguration der Inhaltsgruppe.

Hinweis: Citrix empfiehlt, Selektoren anstelle von parametrisierten Inhaltsgruppen zu verwenden, da Selektoren flexibler sind und an mehr Datentypen angepasst werden können.

Konfigurieren eines Selektors

Eine Inhaltsgruppe kann einen Trefferselektor verwenden, um Cache-Treffer abzurufen, oder einen Invalidierungs-Selektor verwenden, um abgelaufene zwischengespeicherte Objekte abzurufen und neue vom Originalserver abzurufen.

Ein Selektor enthält einen Namen und einen logischen Ausdruck, der als *erweiterte Ausdruck* bezeichnet wird.

Weitere Informationen zu erweiterten Ausdrücken finden Sie unter Richtlinien und Ausdrücke.

Um einen Selektor zu konfigurieren, weisen Sie ihm einen Namen zu und geben einen oder mehrere Ausdrücke ein. Als bewährte Methode sollte ein Selektorausdruck den URL-Stamm und den Host enthalten, es sei denn, es gibt triftige Gründe, sie wegzulassen.

So konfigurieren Sie einen Selektor mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add cache selector \<selectorName\> ( \<rule\> ... )
```

Informationen zum Konfigurieren des Ausdrucks oder der Ausdrücke finden Sie unter So konfigurieren Sie einen Selektorausdruck mithilfe der Befehlszeilenschnittstelle.

```
1 >add cache selector product_selector "http.req.url.query.value("
     ProductId")" "http.req.url.query.value("BatchNum")" "http.req.url.
     query.value("depotLocation")"
2
3 > add cache selector batch_selector "http.req.url.query.value("
     ProductId")" "http.req.url.query.value("BatchId")" "http.req.url.
     query.value("depotLocation")"
4
```



```
5  > add cache selector product_id_selector "http.req.url.query.value("
       ProductId")"
6
7  > add cache selector batchnum_selector "http.req.url.query.value("
       BatchNum")" "http.req.url.query.value("depotLocation")"
8
9  > add cache selector batchid_selector "http.req.url.query.value("
       depotLocation")" "http.req.url.query.value("BatchId")"
10
11 <!--NeedCopy-->
```

So konfigurieren Sie einen Selektor mit der GUI

Navigieren Sie zu **Optimierung > Integriertes Caching > Cache-Selektoren**und fügen Sie den Cache-Selektor hinzu.

Content-Gruppen

Eine Inhaltsgruppe ist ein Container für zwischengespeicherte Objekte, die als Antwort bereitgestellt werden können. Wenn Sie den integrierten Cache zum ersten Mal aktivieren, werden zwischenspeicherbare Objekte in einer Inhaltsgruppe namens Default gespeichert. Sie können Inhaltsgruppen mit einzigartigen Eigenschaften erstellen. Sie können beispielsweise separate Inhaltsgruppen für Bilddaten, Fehlerberichte und Aktienkurse definieren und die Inhaltsgruppe Aktienkurse so konfigurieren, dass sie häufiger aktualisiert wird als die anderen Gruppen.

Sie können den Ablauf einer gesamten Inhaltsgruppe oder ausgewählter Einträge in einer Inhaltsgruppe konfigurieren.

Die Daten in einer Inhaltsgruppe können wie folgt statisch oder dynamisch sein:

- **Statische Inhaltsgruppen**. Findet eine genaue Übereinstimmung zwischen dem URL-Stamm und dem Hostnamen auf der Anfrage und dem URL-Stamm und dem Hostnamen der Antwort.
- **Dynamische Inhaltsgruppen**. Sucht nach Objekten, die bestimmte Parameterwertpaare, beliebige Zeichenketten oder Zeichenkettenmuster enthalten. Dynamische Inhaltsgruppen sind nützlich, wenn Daten zwischengespeichert werden, die häufig aktualisiert werden (z. B. ein Bugreport oder ein Aktienkurs).

Eine Anfrage von einer Inhaltsgruppe bearbeiten

1. Ein Benutzer gibt Suchkriterien für ein Element ein, z. B. einen Fehlerbericht, und klickt in einem HTML-Formular auf die Schaltfläche Suchen.
2. Der Browser gibt eine oder mehrere HTTP-GET-Anfragen aus. Diese Anfragen enthalten Parameter (z. B. den Bug-Besitzer, die Bug-ID usw.).

3. Wenn die NetScaler-Appliance die Anfragen empfängt, sucht sie nach einer passenden Richtlinie, und wenn sie eine Caching-Richtlinie findet, die diesen Anfragen entspricht, leitet sie die Anfragen an eine Inhaltsgruppe weiter.
4. Die Inhaltsgruppe sucht anhand von Kriterien, die Sie in einem Selektor konfigurieren, nach geeigneten Objekten in der Inhaltsgruppe.

Beispielsweise kann die Inhaltsgruppe passende Antworten abrufen `NameField=username and BugID=ID`.

1. Wenn sie passende Objekte findet, kann die NetScaler-Appliance sie dem Browser des Benutzers zur Verfügung stellen, wo sie zu einer vollständigen Antwort (z. B. einem Fehlerbericht) zusammengefügt werden.

Ein Objekt in einer Inhaltsgruppe für ungültig erklären

1. Ein Benutzer ändert Daten (z. B. ändert der Benutzer den Fehlerbericht und klickt auf die Schaltfläche Senden).
2. Der Browser sendet diese Daten in Form einer oder mehrerer HTTP-Anfragen. Beispielsweise kann es einen Fehlerbericht in Form mehrerer HTTP-POST-Anfragen senden, die Informationen über den Bug-Besitzer und die Bug-ID enthalten.
3. Die NetScaler-Appliance gleicht die Anfragen mit den Invalidierungsrichtlinien ab. In der Regel sind diese Richtlinien so konfiguriert, dass sie die HTTP-POST-Methode erkennen.
4. Wenn die Anfrage einer Invalidierungsrichtlinie entspricht, durchsucht die NetScaler-Appliance die Inhaltsgruppe, die dieser Richtlinie zugeordnet ist, und verfällt Antworten, die den konfigurierten Kriterien für die Invalidierung entsprechen.

Beispielsweise kann ein Invalidierungsselektor passende Antworten finden. `NameField=username and BugID=ID`

1. Wenn die NetScaler-Appliance das nächste Mal eine GET-Anfrage für diese Antworten erhält, ruft sie aktualisierte Versionen vom Originalserver ab, speichert die aktualisierten Antworten und sendet diese Antworten an den Browser des Benutzers, wo sie zu einem vollständigen Fehlerbericht zusammengefasst werden.

Richten Sie eine grundlegende Inhaltsgruppe ein

Standardmäßig werden alle zwischengespeicherten Daten in der Standardinhaltsgruppe gespeichert. Sie können weitere Inhaltsgruppen konfigurieren und diese Inhaltsgruppen in einer oder mehreren Richtlinien angeben.

Sie können Inhaltsgruppen für statische Inhalte konfigurieren, und Sie müssen Inhaltsgruppen für dynamische Inhalte konfigurieren. Sie können die Konfiguration jeder Inhaltsgruppe ändern, einschließlich der Standardgruppe.

So richten Sie mithilfe der Befehlszeilenschnittstelle eine grundlegende Inhaltsgruppe ein

Geben Sie in der Befehlszeile Folgendes ein:

```
add cache contentgroup <name> (-hitSelector <hitSelectorName> -invalSelector
 <invalidationSelectorName> | -hitParams <hitParamName> -invalParams<
invalidationParamName>)-type <type> [-relExpiry <sec> | -relExpiryMilliSec
<msec>] [-heurExpiryParam <positiveInteger>]

add cache contentgroup Products_Details -hitSelector product_selector -
invalSelector id_selector

add cache contentgroup bugrep -hitParams IssuePage RecordID Template
TableId -invalParams RecordID -relExpiry 864000
```

So richten Sie mithilfe der GUI eine grundlegende Inhaltsgruppe ein

Navigieren Sie zu **Optimierung > Integriertes Caching > Inhaltsgruppen**und erstellen Sie die Inhaltsgruppe.

Zwischengespeicherte Objekte ablaufen lassen oder leeren

Wenn eine Antwort keinen Expires-Header oder keinen Cache-Control-Header mit einer Ablaufzeit (Max-Age oder Smax-Age) hat, müssen Sie Objekte in einer Inhaltsgruppe ablaufen lassen, indem Sie eine der folgenden Methoden verwenden:

- Konfigurieren Sie die Ablaufeinstellungen für Inhaltsgruppen, um zu bestimmen, ob und wie lange das Objekt aufbewahrt werden soll.
- Konfigurieren Sie eine Invalidierungsrichtlinie und -aktion für die Inhaltsgruppe. Weitere Informationen finden Sie unter Konfigurieren von Richtlinien für Caching und Invalidierung.
- Führen Sie die Content-Gruppe oder die darin enthaltenen Objekte manuell aus.

Nachdem eine zwischengespeicherte Antwort abgelaufen ist, aktualisiert die NetScaler-Appliance sie, wenn der Client das nächste Mal eine Antwortanfrage stellt. Wenn der Cache voll ist, ersetzt die NetScaler-Appliance standardmäßig zuerst die am wenigsten verwendete Antwort.

In der folgenden Liste werden Methoden zum Ablaufen zwischengespeicherter Antworten mithilfe von Einstellungen für eine Inhaltsgruppe beschrieben. In der Regel werden diese Methoden als Prozent oder in Sekunden angegeben:

- **Manuell**. Automatisieren Sie manuell alle Antworten in einer Inhaltsgruppe oder alle Antworten im Cache.
- **Antwortbasiert.** Spezifische Verfallsintervalle für positive und negative Reaktionen. Ein auf der Antwort basierendes Verfallsdatum wird nur berücksichtigt, wenn der Last-Modified-Header in der Antwort fehlt.
- **Heuristischer Ablauf.** Bei Antworten mit einem Last-Modified-Header gibt das heuristische Verfallsdatum die Zeit an, die seit der Änderung der Antwort verstrichen ist (berechnet als ak-

tuelle Zeit abzüglich der Zeit der letzten Änderung, multipliziert mit dem heuristischen Verfallswert). Wenn beispielsweise ein Last-Modified-Header angibt, dass eine Antwort vor 2 Stunden aktualisiert wurde, und die heuristische Ablaufeinstellung 10% beträgt, laufen zwischengespeicherte Objekte nach 0,2 Stunden ab. Bei dieser Methode wird davon ausgegangen, dass häufig aktualisierte Antworten häufiger abgelaufen sein müssen.

- **Absolut oder relativ**. Geben Sie eine genaue (absolute) Uhrzeit an, zu der die Antwort jeden Tag abläuft, im Format HH:MM, Ortszeit oder GMT. Die Ortszeit funktioniert möglicherweise nicht in allen Zeitzonen.

Der relative Ablauf gibt einige Sekunden oder Millisekunden von dem Zeitpunkt an, an dem ein Cachefehler eine Reise zum Ursprungsserver verursacht, bis zum Ablauf der Antwort an. Wenn Sie den relativen Ablauf in Millisekunden angeben, geben Sie ein Vielfaches von 10 ein. Diese Form der Expiration funktioniert für alle positiven Reaktionen. Die Header Last-Modified, Expires und Cache-Control in der Antwort werden ignoriert.

Absoluter und relativer Ablauf haben Vorrang vor allen Ablaufinformationen in der Antwort selbst.

- **Beim Herunterladen**. Die Option Nach Erhalt der vollständigen Antwort ablaufen lässt eine Antwort ablaufen, wenn sie heruntergeladen wird. Dies ist nützlich für häufig aktualisierte Antworten, z. B. Aktienkurse. Standardmäßig ist diese Option deaktiviert.

Die Aktivierung von Flash Cache und Expire After Complete Response Received beschleunigt die Leistung dynamischer Anwendungen. Wenn Sie beide Optionen aktivieren, ruft die NetScaler-Appliance nur eine Antwort für einen Block gleichzeitiger Anfragen ab.

- **Festgeheftet.** Wenn der Cache voll ist, ersetzt die NetScaler-Appliance standardmäßig zuerst die am wenigsten verwendete Antwort. Die NetScaler-Appliance wendet dieses Verhalten nicht auf Inhaltsgruppen an, die als angeheftet markiert sind.

Wenn Sie keine Ablaufeinstellungen für eine Inhaltsgruppe konfigurieren, finden Sie im Folgenden weitere Optionen für ablaufende Objekte in der Gruppe:

- Konfigurieren Sie eine Richtlinie mit einer INVAL-Aktion, die für die Inhaltsgruppe gilt.
- Geben Sie die Namen der Inhaltsgruppen ein, wenn Sie eine Richtlinie konfigurieren, die eine INVAL-Aktion verwendet.

Wie werden die Verfallsmethoden angewendet

Die Expiration funktioniert bei positiven und negativen Reaktionen unterschiedlich. Positive und negative Antworten werden in der unten aufgeführten Tabelle „*Ablauf positiver und negativer Antworten* “ beschrieben.

Im Folgenden finden Sie Faustregeln zum Verständnis der Ablaufmethode, die auf eine Inhaltsgruppe angewendet wird:

- Sie können steuern, ob die NetScaler-Appliance Antwortheader auswertet, wenn sie entscheidet, ob ein Objekt ablaufen soll.
- Absoluter und relativer Ablauf führen dazu, dass die NetScaler-Appliance die Antwort-Header ignoriert (sie überschreiben alle Ablaufinformationen in der Antwort).
- Heuristische Ablaufeinstellungen und „schwach positiv“ und „schwach negativ“ (im Konfigurationsprogramm als **Standardwerte** bezeichnet) veranlassen die NetScaler-Appliance, die Antwort-Header zu überprüfen. Diese Einstellungen wirken wie folgt zusammen:
  - Der Wert in einem Expires- oder Cache-Control-Header überschreibt diese Inhaltsgruppeneinstellungen.
  - Bei positiven Antworten, denen ein Expires- oder Cache-Control-Header fehlt, die aber über einen Last-Modified-Header verfügen, vergleicht die NetScaler-Appliance die heuristischen Ablaufeinstellungen mit dem Header-Wert.
  - Für positive Antworten, denen ein Expires-, Cache-Control- oder Last-Modified-Header fehlt, verwendet die NetScaler-Appliance den Wert „schwach positiv“.
  - Für negative Antworten, denen ein Expires- oder Cache-Control-Header fehlt, verwendet die NetScaler-Appliance den Wert „schwach negativ“.

In der folgenden Tabelle wird beschrieben, wie diese Methoden angewendet werden.

Art der Antwort	Header-Typ für Ablaufdatum	Einstellung der Inhaltsgruppe	Zeitraum, in dem das Objekt im Cache verbleibt
Positiv	Beliebiger Header	Inhalt danach ablaufen lassen (RelExpiry) ohne weitere Einstellungen	Verwenden Sie den Wert der Einstellung **Expire Content After** .
Positiv	Beliebiger Header	Inhalt ablaufen unter (absExpiry) ohne weitere Einstellungen	Subtrahieren Sie das aktuelle Datum vom Wert der Einstellung „ **Inhalt ablaufen bei**“.
Positiv	Beliebiger Header	Inhalt nach (RelExpiry) ablaufen lassen und Inhalt ablaufen bei (absExpiry)	Verwenden Sie den kleineren der beiden Werte für die Inhaltsgruppeneinstellungen. Sehen Sie sich die vorherigen Zeilen in dieser Tabelle an.

Art der Antwort	Header-Typ für Ablaufdatum	Einstellung der Inhaltsgruppe	Zeitraum, in dem das Objekt im Cache verbleibt
Positiv	Zuletzt geändert (mit allen anderen Headern)	Heuristik (Heurexpiry Param) mit jeder anderen Einstellung	Subtrahieren Sie das Datum der letzten Änderung vom aktuellen Datum, multiplizieren Sie das Ergebnis mit dem Wert der heuristischen Ablaufeinstellung und dividieren Sie es dann durch 100.
Positiv	Zuletzt geändert (mit allen anderen Headern)	Standard (positiv) (WeakPosRel Expiry) und keine andere Einstellung	Verwenden Sie den Wert der Standardeinstellung (positiv) für das Ablaufdatum.
Positiv	Läuft ab oder Cache-Control: Max-Age-Header ist vorhanden	Der Header „Zuletzt geändert“ fehlt, Heuristik (Heurexpiry Param), Default (positiv) (WeakPosRel Expiry) oder beides	Subtrahieren Sie das aktuelle Datum vom Gültigkeitsdatum oder dem `Cache-Control:Max-Age` Datum.
Positiv	keine Caching-Header	Standard (positiv) (WeakPosRel Expiration) und jede andere Ablaufeinstellung	Verwenden Sie den Wert der Standardeinstellung (positiv).

Art der Antwort	Header-Typ für Ablaufdatum	Einstellung der Inhaltsgruppe	Zeitraum, in dem das Objekt im Cache verbleibt
Positiv	keine Caching-Header	Heuristik (Heurexpiry Param) ist vorhanden, die Standardeinstellung (positiv) (WeakPosRel Expiry) fehlt.	Wenn der Header Last-Modified nicht vorhanden ist, wird die Antwort nicht zwischengespeichert oder sie wird mit dem Status Bereits abgelaufen zwischengespeichert. Wenn der Last-Modified-Header vorhanden ist, verwenden Sie den heuristischen Verfallswert.
Negativ	Läuft ab oder `Cache-Control:Max-Age`	Inhalt ablaufen nach (RelExpiry), Inhalt ablaufen bei (absExpiry) oder beide Einstellungen	Subtrahieren Sie das aktuelle Datum vom Wert des Expires-Headers oder verwenden Sie den Wert des Cache-Control:Max-Age-Headers.
Negativ	Läuft ab oder Cache-Control-Header fehlen	Inhalt ablaufen nach (RelExpiry), Inhalt ablaufen bei (absExpiry) oder beide Einstellungen	Die Antwort wird nicht zwischengespeichert oder hat den Status „Bereits abgelaufen“.
Negativ	Läuft ab oder `Cache-Control:Max-Age`	Beliebige Einstellung	Subtrahieren Sie das aktuelle Datum vom `Cache-Control:Max-Age` Gültigkeitsdatum oder Datum.

Art der Antwort	Header-Typ für Ablaufdatum	Einstellung der Inhaltsgruppe	Zeitraum, in dem das Objekt im Cache verbleibt
Negativ	Expires und Cache-Control:Max-Age-Header fehlen	Standard (negativ) (WeakNegrel Expiry)	Verwenden Sie den Wert der Standardeinstellung (negativ).
Negativ	Expires und Cache-Control:Max-Age-Header fehlen	Jede andere Einstellung als Standard (negativ) (WeakNegrel Expiry)	Das Objekt ist nicht zwischengespeichert oder hat den Status Bereits abgelaufen.

Manuelles Ablaufen einer Inhaltsgruppe

Sie können alle Einträge in einer Inhaltsgruppe manuell ablaufen lassen.

Um alle Antworten in einer Inhaltsgruppe mithilfe der Befehlszeilenschnittstelle manuell ablaufen zu lassen

Geben Sie in der Befehlszeile Folgendes ein:

```
expire cache contentGroup <name>
```

Um alle Antworten in einer Inhaltsgruppe mithilfe der GUI manuell ablaufen zu lassen

Navigieren Sie zu **Optimierung > Integriertes Caching > Inhaltsgruppen**, wählen Sie die Inhaltsgruppe aus und klicken Sie auf Ungültig machen, um alle Antworten in einer Inhaltsgruppe ablaufen zu lassen.

Um alle Antworten im Cache mithilfe der GUI manuell ablaufen zu lassen

Navigieren Sie zu **Optimierung > Integriertes Caching > Inhaltsgruppen**und klicken Sie auf Alle ungültig machen, um alle Antworten im Cache ablaufen zu lassen.

Den regelmäßigen Ablauf einer Inhaltsgruppe konfigurieren

Sie können eine Inhaltsgruppe so konfigurieren, dass sie ihre Einträge selektiv oder vollständig ablaufen lässt. Das Ablaufintervall kann fest oder relativ sein.

So konfigurieren Sie das Ablaufdatum von Inhaltsgruppen mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
set cache contentgroup \<name> (-relExpiry|-relExpiryMilliSec|-absExpiry
|-absExpiryGMT| -heurExpiryParam|-weakPosRelExpiry|-weakNegRelExpiry| -
expireAtLastBye)\<expirationValue>
```

So konfigurieren Sie das Ablaufdatum von Inhaltsgruppen mithilfe der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**, wählen Sie die Inhaltsgruppe aus und geben Sie die Ablaufmethode an.

Einzelne Antworten ablaufen lassen

Wenn eine Antwort abläuft, wird die NetScaler-Appliance gezwungen, eine aktualisierte Kopie vom Originalserver abzurufen. Antworten, die beispielsweise keine Validatoren `ETag` oder Last-Modified-Header haben, können nicht erneut validiert werden. Daher hat das Löschen dieser Antworten den gleichen Effekt wie das Ablaufen dieser Antworten.

Um eine zwischengespeicherte Antwort in einer Inhaltsgruppe für statische Daten ablaufen zu lassen, können Sie eine URL angeben, die mit der gespeicherten URL übereinstimmen muss. Wenn die zwischengespeicherte Antwort Teil einer parametrisierten Inhaltsgruppe ist, müssen Sie den Gruppennamen und den genauen URL-Stamm angeben. Der Hostname und die Portnummer müssen mit denen im Host-HTTP-Anforderungsheader der zwischengespeicherten Antwort übereinstimmen. Wenn der Port nicht angegeben ist, wird Port 80 angenommen.

So lassen Sie einzelne Antworten in einer Inhaltsgruppe mithilfe der Befehlszeilenschnittstelle ablaufen

Geben Sie in der Befehlszeile Folgendes ein:

```
expire cache object -url <URL> -host <hostName> [-port <port>] [-groupName<
contentGroupName>] [-httpMethod GET|POST]
```

So lassen Sie einzelne Antworten in einer Inhaltsgruppe mithilfe der CLI ablaufen

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
expire cache object -locator <positiveInteger>
```

Um eine zwischengespeicherte Antwort mithilfe der GUI ablaufen zu lassen

Navigieren Sie zu **Optimierung** > **Integriertes Caching > ZwischengespeicherteObjekte, wählen Sie die zwischengespeicherte**Antwort aus und laufen Sie ab.

Um eine Antwort mithilfe der GUI ablaufen zu lassen

Navigieren Sie zu **Optimierung** > **Integriertes Caching > ZwischengespeicherteObjekte**, klicken Sie auf**Suchen** und legen Sie die Suchkriterien fest, um die erforderliche zwischengespeicherte Antwort zu finden und ablaufen zu lassen.

Antworten in einer Inhaltsgruppe löschen

Sie können alle Antworten in einer Inhaltsgruppe, einige Antworten in einer Gruppe oder alle Antworten im Cache entfernen oder löschen. Das Leeren einer zwischengespeicherten Antwort gibt Speicherplatz für neue zwischengespeicherte Antworten frei.

> **Hinweis:**
>
> Verwenden Sie die Methode des Konfigurationsprogramms, um Antworten für mehrere Objekte gleichzeitig zu löschen. Die Befehlszeilenschnittstelle bietet diese Option nicht.

So löschen Sie Antworten aus einer Inhaltsgruppe mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
flush cache contentGroup <name> [-query <queryString> | [-selectorValue <
selectorExpressionIDList> -host <hostName>]]
```

So löschen Sie Antworten aus einer Inhaltsgruppe mithilfe der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**.
2. Spülen Sie die Antworten im Detailbereich wie folgt:
   - Um alle Antworten in allen Inhaltsgruppen zu löschen, klicken Sie auf Alle ungültig machen und löschen Sie alle Antworten.
   - Um Antworten in einer bestimmten Inhaltsgruppe zu löschen, wählen Sie die Inhaltsgruppe aus, klicken Sie auf **Ungültig machen**und löschen Sie alle Antworten.

> **Hinweis**:
> Wenn diese Inhaltsgruppe einen Selektor verwendet, können Sie Antworten selektiv löschen, indem Sie eine Zeichenfolge in das Textfeld Selektorwert eingeben und in das Textfeld Host einen Hostnamen eingeben. Klicken Sie dann auf **Flush und OK.** Der Selectorwert kann eine Abfragezeichenfolge mit bis zu 2319 Zeichen sein, die für die parametrisierte Invalidierung verwendet wird.

Wenn die Inhaltsgruppe einen Invalidierungsparameter verwendet, können Sie die Antworten selektiv löschen, indem Sie eine Zeichenfolge in das Abfragefeld eingeben.

Wenn die Inhaltsgruppe einen Invalidierungsparameter verwendet und die zum Zielhost gehörenden Objekte ungültig machen konfiguriert sind, geben Sie Zeichenfolgen in die Felder **Query und Host** ein.

So leeren Sie eine zwischengespeicherte Antwort mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
flush cache object -locator <positiveInteger> | -url <URL> -host <hostName>
 [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET|POST]
```

Um eine zwischengespeicherte Antwort mithilfe der GUI zu leeren

Navigieren Sie zu **Optimierung** > **Integriertes Caching > ZwischengespeicherteObjekte, wählen Sie das zwischengespeicherte**Objekt aus und leeren Sie es.

Löschen einer Inhaltsgruppe

Sie können eine Inhaltsgruppe entfernen, wenn sie von keiner Richtlinie verwendet wird, die Antworten im Cache speichert. Wenn die Inhaltsgruppe an eine Richtlinie gebunden ist, müssen Sie die Richtlinie zuerst entfernen. Durch das Entfernen der Inhaltsgruppe werden alle in dieser Gruppe gespeicherten Antworten entfernt.

Sie können die Gruppen Default, BASEFILE oder Deltas nicht entfernen. In der Standardgruppe werden zwischengespeicherte Antworten gespeichert, die zu keiner anderen Inhaltsgruppe gehören.

So löschen Sie eine Inhaltsgruppe mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
rm cache contentgroup <name>
```

So löschen Sie eine Inhaltsgruppe mithilfe der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen,** wählen Sie die Content-Gruppe aus, und löschen Sie sie.

Richtlinien für Caching und Invalidierung konfigurieren

May 11, 2023

Mithilfe von Richtlinien kann der integrierte Cache bestimmen, ob versucht werden soll, eine Antwort vom Cache oder vom Ursprung aus bereitzustellen. Die NetScaler-Appliance bietet integrierte Richtlinien für integriertes Caching, und Sie können weitere Richtlinien konfigurieren. Wenn Sie eine Richtlinie konfigurieren, verknüpfen Sie sie mit einer Aktion. Eine Aktion speichert entweder die Objekte, für die die Richtlinie gilt, oder macht die Objekte ungültig (läuft ab). In der Regel haben Sie die Caching-Richtlinien auf Informationen in GET- und POST-Anfragen gestützt. In der Regel stützen Sie Invalidierungsrichtlinien auf das Vorhandensein der POST-Methode in Anfragen sowie auf andere Informationen. Sie können alle Informationen in einer GET- oder POST-Anforderung in einer Caching- oder Invalidierungsrichtlinie verwenden.

Sie können einige der integrierten Richtlinien im Knoten Richtlinien des integrierten Caches im Konfigurationsprogramm einsehen. Die Namen der integrierten Richtlinien beginnen mit einem Unterstrich (_).

Aktionen bestimmen, was die NetScaler-Appliance tut, wenn der Datenverkehr einer Richtlinie entspricht. Folgende Aktionen sind verfügbar:

- **Aktionen zwischenspeichern.** Richtlinien, die Sie der CACHE-Aktion zuordnen, speichern Antworten im Cache und stellen sie aus dem Cache bereit.
- **Maßnahmen zur Ungültigerklärung.** Richtlinien, die Sie der INVAL-Aktion zuordnen, laufen zwischengespeicherte Antworten sofort ab und aktualisieren sie vom Originalserver. Bei webbasierten Anwendungen werden POST-Anfragen häufig anhand von Invalidierungsrichtlinien bewertet.
- **Aktionen „Nicht zwischenspeichern“**. Richtlinien, die Sie einer NOCACHE-Aktion zuordnen, speichern niemals Objekte im Cache.
- **Aktionen vorläufig zwischenspeichern**. Richtlinien, die Sie mit einer MAYCACHE- oder MAYNOCACHE-Aktion verknüpfen, hängen vom Ergebnis weiterer Richtlinienbewertungen ab.

Obwohl der integrierte Cache keine durch die LOCK-Methode angegebenen Objekte speichert, können Sie zwischengespeicherte Objekte nach Erhalt einer `LOCK` Anforderung ungültig machen. Nur für Invalidierungsrichtlinien können Sie mithilfe des Ausdrucks `LOCK` als Methode angeben `http.req.method.eq( “lock” )`. Im Gegensatz zu Richtlinien für `GET` und `POST` Anfragen müssen Sie die LOCK-Methode in Anführungszeichen einschließen, da die NetScaler Appliance diesen Methodennamen nur als Zeichenfolge erkennt.

Nachdem Sie eine Richtlinie erstellt haben, binden Sie sie an einen bestimmten Punkt in der Gesamtverarbeitung von Anforderungen und Antworten. Obwohl Sie eine Richtlinie erstellen, bevor Sie sie binden, müssen Sie verstehen, wie sich die Bindepunkte auf die Reihenfolge der Verarbeitung auswirken, bevor Sie Ihre Richtlinien erstellen.

Die an einen bestimmten Bindepunkt gebundenen Richtlinien stellen eine Richtlinienbank dar. Sie können goto-Ausdrücke verwenden, um die Ausführungsreihenfolge in einer Policybank zu ändern. Sie können Richtlinien auch in anderen Policy-Banks aufrufen. Darüber hinaus können Sie Labels erstellen und Richtlinien an diese binden. Ein solches Label ist keinem Verarbeitungspunkt zugeordnet, aber die daran gebundenen Richtlinien können von anderen Policy-Datenbanken abgerufen werden.

Maßnahmen zur Verknüpfung mit integrierten Caching-Richtlinien

In der folgenden Tabelle werden Aktionen für integrierte Caching-Richtlinien beschrieben.

Aktion	Spezifikation
CACHE	Stellt eine Antwort aus dem Cache bereit, falls die Antwort noch nicht abgelaufen ist. Wenn die Antwort vom Originalserver abgerufen werden muss, speichert die NetScaler-Appliance die Antwort im Cache, bevor sie bereitgestellt wird. Sogar Daten, die häufig aktualisiert werden und auf die häufig zugegriffen wird, können zwischengespeichert werden. Aktienkurse werden beispielsweise häufig aktualisiert, können jedoch zwischengespeichert werden, sodass sie schnell mehreren Benutzern zur Verfügung gestellt werden können. Bei Bedarf können zwischengespeicherte Daten sofort nach dem Herunterladen aktualisiert werden. Eine CACHE-Aktion kann durch integrierte Richtlinien außer Kraft gesetzt werden.
KEIN CACHE	Ruft immer die Antwort vom Ursprungsserver ab und markiert die Antwort als nicht speicherbar. In der Regel konfigurieren Sie NOCACHE-Richtlinien für sensible oder personalisierte Daten.

Aktion	Spezifikation
MAY_CACHE	Diese Einstellung wird in einer Richtlinie zur Anforderungszeit verwendet und ermöglicht vorläufig, dass eine Antwort in einer Inhaltsgruppe gespeichert wird, bis die Richtlinien für die Reaktionszeit ausgewertet wurden. Folgendes ist möglich: 1. Wenn eine entsprechende Richtlinie zur Reaktionszeit eine CACHE-Aktion enthält, aber keine Inhaltsgruppe angibt, wird die Antwort in der Standardgruppe gespeichert, sofern keine integrierten Richtlinien diese Richtlinie außer Kraft setzen. 2. Wenn eine entsprechende Richtlinie für die Reaktionszeit über eine CACHE-Aktion verfügt und dieselbe Inhaltsgruppe wie die Inhaltsgruppe in der Anforderungszeitrichtlinie angibt, wird die Antwort in der benannten Inhaltsgruppe gespeichert, sofern keine integrierten Richtlinien diese Richtlinie außer Kraft setzen. 3. Wenn eine entsprechende Antwortzeitrichtlinie eine CACHE-Aktion enthält, aber eine andere Inhaltsgruppe als die Inhaltsgruppe in der Anforderungszeitrichtlinie angibt, wird eine NOCACHE-Aktion angewendet. 4. Wenn eine entsprechende Antwortzeitrichtlinie eine NOCACHE-Aktion enthält, führen Sie eine NOCACHE-Aktion aus. 5. Wenn es keine entsprechende Richtlinie für die Reaktionszeit gibt, wird eine CACHE-Aktion angewendet, es sei denn, eine integrierte Richtlinie überschreibt diese Richtlinie.

Aktion	Spezifikation
MAY_NOCACHE	Bei einer Richtlinie zur Anforderungszeit verhindert diese Einstellung vorläufig, dass die Antwort zwischengespeichert wird. Zur Antwortzeit wird eine der folgenden Aktionen ausgeführt: - Wenn keine Richtlinie zur Reaktionszeit der Anfrage entspricht, ist die letzte Aktion NOCACHE. — Wenn eine entsprechende Richtlinie zur Reaktionszeit eine CACHE-Aktion enthält, ist die letzte Aktion CACHE, sofern keine integrierten Richtlinien diese Richtlinie außer Kraft setzen. — Wenn eine entsprechende Richtlinie zur Reaktionszeit eine NOCACHE-Aktion enthält, ist die letzte Aktion NOCACHE. -Wenn eine entsprechende Richtlinie zur Reaktionszeit eine CACHE-Aktion enthält, aber keine Inhaltsgruppe angibt, besteht die letzte Aktion darin, die Antwort in der Standardinhaltsgruppe zwischenzuspeichern, es sei denn, integrierte Richtlinien haben Vorrang vor dieser Richtlinie.
EINFALLEN	Läuft zwischengespeicherte Antworten ab. Je nachdem, wie die Richtlinie und die Inhaltsgruppe konfiguriert sind, sind alle Antworten in einer oder mehreren Inhaltsgruppen abgelaufen, oder ausgewählte Objekte in der Inhaltsgruppe sind abgelaufen. Hinweis: Sie können INVAL-Aktionen nur in Richtlinien zur Anforderungszeit angeben.

Bindungspunkte für eine Richtlinie

Sie können die Richtlinie an einen der folgenden Bindungspunkte binden:

- **Eine globale Richtlinienbank**. Dies sind die Standardeinstellung für die Anforderungszeit, die Überschreibung der Anforderungszeit, der Ausfall der Reaktionszeit und die Policy-Banken zur Überschreibung der Antwortzeit, wie unter “Reihenfolge der Richtlinienbewer-

tungbeschrieben. “

- **Ein virtueller Server**. Richtlinien, die Sie an einen virtuellen Server binden, werden nach den globalen Überschreibungsrichtlinien und vor den globalen Standardrichtlinien verarbeitet, wie unter “Reihenfolge der Richtlinienbewertungbeschrieben. “ Wenn Sie eine Richtlinie an einen virtuellen Server binden, binden Sie sie entweder an die Anforderungszeit- oder Antwortzeitverarbeitung.
- **Ein Ad-hoc-Richtlinienlabel**. Ein Policy-Label ist ein Name, der einer Policenbank zugewiesen wird. Zusätzlich zu den globalen Bezeichnungen verfügt der integrierte Cache über zwei integrierte benutzerdefinierte Richtlinienlabels:
  - _reqBuiltInStandardwerte. Dieses Richtlinienlabel wird standardmäßig von der Standardrichtlinienbank zur Anforderungszeit aufgerufen.
  - _resBuiltInStandardwerte. Dieses Richtlinienlabel wird standardmäßig von der standardmäßigen Richtlinienbank für die Reaktionszeit aufgerufen.

Sie können auch neue Richtlinienbezeichnungen definieren. Richtlinien, die an ein benutzerdefiniertes Richtlinienlabel gebunden sind, müssen innerhalb einer Richtlinienbank für einen der integrierten Bindungspunkte aufgerufen werden.

> **Wichtig:**
> Sie müssen eine Richtlinie mit einer INVAL-Aktion an einen Bindungspunkt zur Überschreibung der Anforderungszeit oder einen Override-Bindpunkt zur Reaktionszeit binden. Um eine Richtlinie zu löschen, müssen Sie sie zunächst entbinden.

Reihenfolge der politischen Bewertung

Damit eine erweiterte Richtlinie wirksam wird, müssen Sie sicherstellen, dass die Richtlinie zu einem bestimmten Zeitpunkt während der Verarbeitung des Datenverkehrs durch die NetScaler-Appliance aufgerufen wird. Um den Zeitpunkt des Aufrufs festzulegen, verknüpfen Sie die Richtlinie mit einem Bindungspunkt. Im Folgenden sind die Verbindungspunkte in der Reihenfolge ihrer Bewertung aufgeführt:

- Außerkraftsetzung der**Anforderungszeit.** Wenn eine Anfrage mit einer Richtlinie zur Außerkraftsetzung von Anfragen übereinstimmt, endet standardmäßig die Bewertung der Richtlinie zur Anforderungszeit und die NetScaler-Appliance speichert die Aktion, die mit der passenden Richtlinie verknüpft ist.
- **Virtueller Lastausgleichsserver zur Anforderungszeit**. Wenn die Richtlinienauswertung nicht abgeschlossen werden kann, nachdem alle Richtlinien für die Außerkraftsetzung von Anfragen ausgewertet wurden, verarbeitet die NetScaler-Appliance Richtlinien für die Anforderungszeit, die an virtuelle Server mit Lastausgleich gebunden sind. Wenn die Anfrage mit einer dieser Richtlinien übereinstimmt, wird die Evaluierung beendet und die NetScaler-Appliance speichert die Aktion, die der entsprechenden Richtlinie zugeordnet ist.

- **Virtueller Server für Content Switching zur Anforderungszeit**. Richtlinien, die an diesen Bindungspunkt gebunden sind, werden nach den Richtlinien zur Anforderungszeit ausgewertet, die an virtuelle Server für den Lastenausgleich gebunden sind.
- Standardeinstellung für die**Anforderungszeit.** Wenn die Richtlinienbewertung nach der gesamten Anforderungszeit nicht abgeschlossen werden kann, werden die spezifischen Richtlinien für virtuelle Server ausgewertet, verarbeitet die NetScaler-Appliance die Standardrichtlinien für die Anforderungszeit. Wenn die Anfrage einer Standardrichtlinie für die Anforderungszeit entspricht, endet standardmäßig die Bewertung der Richtlinie zur Anforderungszeit und die NetScaler-Appliance speichert die Aktion, die mit der passenden Richtlinie verknüpft ist.
- **Außerkraftsetzung der Reaktionszeit.** Ähnlich wie bei der Bewertung der Richtlinie zur Außerkraftsetzung von Anfragen.
- **Virtueller Lastausgleichsserver mit Reaktionszeit**. Ähnlich wie bei der Bewertung der Richtlinien für virtuelle Server zur Anforderungszeit.
- **Virtueller Server für Content Switching in Reaktionszeit**. Ähnlich wie bei der Bewertung der Richtlinien für virtuelle Server zur Anforderungszeit.
- **Standardeinstellung für Reaktionszeit.** Ähnlich der Bewertung der Standardrichtlinie zur Anforderungszeit.

Sie können jedem Bindpunkt mehrere Richtlinien zuordnen. Um die Reihenfolge der Evaluierung der mit dem Bindpunkt verknüpften Richtlinien zu steuern, konfigurieren Sie eine Prioritätsstufe. In Ermangelung anderer Flusssteuerungsinformationen werden Richtlinien entsprechend der Prioritätsstufe ausgewertet, beginnend mit dem niedrigsten numerischen Prioritätswert.

> **Hinweis:**
> Richtlinien zur Anforderungszeit für POST-Daten oder Cookie-Header müssen während der Auswertung zur Überschreibung der Anforderungszeit aufgerufen werden, da die integrierten Richtlinien zur Anforderungszeit im integrierten Cache eine `NOCACHE` Aktion für POST-Anfragen und eine `MAY_NOCACHE` Aktion für Anfragen mit Cookies zurückgeben. Sie verknüpfen `MAY_CACHE` oder `MAY_NOCACHE` Aktionen mit einer Richtlinie zur Anforderungszeit, die auf eine parametrisierte Content-Gruppe verweist. Die Antwortzeitrichtlinie bestimmt, ob die Transaktion im Cache gespeichert wird.

Konfigurieren einer Richtlinie für integriertes Caching

Sie konfigurieren neue Richtlinien, um Daten zu verarbeiten, die von den integrierten Richtlinien nicht verarbeitet werden können. Sie konfigurieren separate Richtlinien für das Zwischenspeichern, um das Zwischenspeichern zu verhindern und zwischengespeicherte Daten ungültig zu machen. Im Folgenden sind die Hauptbestandteile einer Richtlinie für integriertes Caching aufgeführt:

- Regel: Ein logischer Ausdruck, der eine HTTP-Anfrage oder -Antwort auswertet.

- Aktion: Sie verknüpfen eine Richtlinie mit einer Aktion, um zu bestimmen, was mit einer Anfrage oder Antwort geschehen soll, die der Richtlinienregel entspricht.

Inhaltsgruppen: Sie verknüpfen die Richtlinie mit einer oder mehreren Inhaltsgruppen, um zu ermitteln, wo die Aktion ausgeführt werden soll.

So konfigurieren Sie eine Richtlinie für das Caching mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add cache policy <policyName> -rule <expression> -actionCACHE|MAY_CACHE
|NOCACHE|MAY_NOCACHE [-storeInGroup <contentGroupName>] [-undefAction
NOCACHE|RESET]
> add cache policy image_cache -rule "http.req.url.contains(\"jpg\")|| http
.req.url.contains(\"jpeg\")"-action CACHE -storeingroup myImages_group -
undefaction NOCACHE

> add cache policy bugReportPolicy -rule "http.req.url.query.contains(\"
IssuePage\")"-action CACHE -storeInGroup bugReportGroup

> add cache policy my_form_policy -rule "http.req.header(\"Host\")contains
(\"my.company.com\")&& http.req.method.eq(\"GET\")&& http.req.url.query.
contains(\"v=7\")"-action CACHE -storeInGroup my_form_event

> add cache policy viewproducts_policy -rule "http.req.url.contains(\"
viewproducts.aspx\")"-action CACHE -storeInGroup Product_Details
```

So konfigurieren Sie eine Richtlinie für die Invalidierung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add cache policy <policyName> -rule <expression> -action INVAL [-
    invalObjects "<contentGroupName1>[,<selectorName1>"]. . .]] | [-
    invalGroup <contentGroupName1>[, <contentGroupName2>. . .]] [-
    undefAction NOCACHE|RESET]
<!--NeedCopy-->
```

```
> add cache policy invalidation_events_policy -rule "http.req.header("
    Host")contains("my.company.com") && http.req.method.eq("GET") &&
    http.req.url.query.contains("v=8") -action INVAL -invalObjects
    my_form_event -undefaction NOCACHE
<!--NeedCopy-->
```

```
> add cache policy inval_all -rule "http.req.method.eq("POST") && http.
    req.url.contains("jpeg")" -action INVAL -invalGroups myImages_group
    myApps_group PDF_group
<!--NeedCopy-->
```



```
> add cache policy bugReportInvalidationPolicy -rule "http.req.url.
    query.contains("TransitionForm")" -action INVAL -invalObjects
    bugReport`
`> add cache policy editproducts_policy  - rule "http.req.url.contains("
    editproducts.aspx")"  - action INVAL -invalObjects "Product_Details,
    batchnum_sel" "Products_In_Depots,batchid_sel"
<!--NeedCopy-->
```

So konfigurieren Sie eine Richtlinie für das Caching oder die Invalidierung mithilfe der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Richtlinien**und erstellen Sie die neue Richtlinie.

Eine weltweit verbindliche integrierte Caching-Richtlinie

Wenn Sie eine Richtlinie global binden, steht sie allen virtuellen Servern auf der NetScaler Appliance zur Verfügung.

So binden Sie eine integrierte Caching-Richtlinie global über die Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

```
bind cache global <policy> -priority <positiveInteger> [-
    typeREQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT] [-
    gotoPriorityExpression <expression>] [-invoke <labelType> <labelName
    >]
<!--NeedCopy-->
```

```
> bind cache global myCachePolicy -priority 100 -type req_default
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das Argument type ist optional für global gebundene Richtlinien, um die Abwärtskompatibilität mit Richtlinien aufrechtzuerhalten, die Sie mit früheren Versionen der NetScaler Appliance definiert haben. Wenn Sie den Typ weglassen, ist die Richtlinie an REQ_DEFAULT oder RES_DEFAULT gebunden, je nachdem, ob es sich bei der Richtlinienregel um einen Ausdruck zur Antwortzeit oder um einen Ausdruck zur Anforderungszeit handelt. Wenn die Regel sowohl Parameter für die Anforderungszeit als auch für die Antwortzeit enthält, ist sie an RES_DEFAULT gebunden. Es folgt ein Beispiel für eine Bindung, die den Typ weglässt

Es folgt ein Beispiel für eine Bindung, bei der der Typ weggelassen wird.

```
> bind cache global myCache Policy 200
```


So binden Sie mithilfe des Konfigurationsdienstprogramms eine integrierte Caching-Richtlinie global

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache Policy Manager** und binden Sie Richtlinien, indem Sie den entsprechenden Bindungspunkt und den Verbindungstyp (Request/Response) angeben.

Binden Sie eine integrierte Caching-Richtlinie an einen virtuellen Server

Wenn Sie eine Richtlinie an einen virtuellen Server binden, ist sie nur für Anforderungen und Antworten verfügbar, die mit der Richtlinie übereinstimmen und die über den relevanten virtuellen Server fließen.

Wenn Sie die GUI verwenden, können Sie die Richtlinie über das Konfigurationsdialogfeld für den virtuellen Server binden. Auf diese Weise können Sie alle Richtlinien aller NetScaler-Module anzeigen, die an diesen virtuellen Server gebunden sind. Sie können auch das **Richtlinien-Manager-Konfigurationsdialogfeld** für den integrierten Cache verwenden. Auf diese Weise können Sie nur die integrierten Caching-Richtlinien anzeigen, die an den virtuellen Server gebunden sind.

So binden Sie eine integrierte Caching-Richtlinie über die Befehlszeilenschnittstelle an einen virtuellen Server:

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name>@ -policyName <policyName> -priority <
   positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

```
bind cs vserver <name>@ -policyName <policyName> -priority <
   positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

So binden Sie eine integrierte Caching-Richtlinie mithilfe des Konfigurationsdienstprogramms an einen virtuellen Server (virtuelle Servermethode)

- CS Virtual Server — Navigieren Sie zu Traffic **Management > Content Switching > Virtuelle Server**, wählen Sie den virtuellen Server aus und binden Sie die entsprechenden Cache-Richtlinien ein.
- LB Virtual Server - Navigieren Sie toTraffic **Management > Load Balancing > Virtuelle Server**, wählen Sie den virtuellen Server aus und binden Sie relevante Cache-Richtlinien.

So binden Sie eine integrierte Caching-Richtlinie mit der GUI (Policy Manager-Methode) an einen virtuellen Server.

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**, und binden Sie Cache-Richtlinien, indem Sie den relevanten Bindepunkt und den Verbindungstyp angeben.

> **Hinweis:**
> Sie können Cache-Richtlinien sowohl an den virtuellen Lastausgleichsserver als auch an den virtuellen Server mit Content Switching binden, indem Sie den entsprechenden Bindepunkt auswählen.

Wie man komprimierte und unkomprimierte Versionen einer Datei zwischenspeichert

Standardmäßig können einem Client, der mit der Komprimierung umgehen kann, unkomprimierte Antworten oder komprimierte Antworten in den Formaten gzip, deflate, compress und pack200-gzip bereitgestellt werden. Wenn der Client die Komprimierung übernimmt, wird in der Anfrage ein `Accept-Encoding:compression` Format-Header gesendet. Der vom Client akzeptierte Komprimierungstyp muss mit dem Komprimierungstyp des zwischengespeicherten Objekts übereinstimmen. Beispielsweise kann eine `cached.gzip` Datei nicht als Antwort auf eine Anfrage mit einem `Accept-Encoding:deflate` Header bereitgestellt werden.

Einem Client, der die Komprimierung nicht verarbeiten kann, wird ein Cachefehler zugestellt, wenn die zwischengespeicherte Antwort komprimiert wird.

Für das dynamische Caching müssen Sie zwei Inhaltsgruppen konfigurieren, eine für komprimierte Daten und eine für unkomprimierte Versionen derselben Daten. Im Folgenden finden Sie ein Beispiel für die Konfiguration der Selektoren, Inhaltsgruppen und Richtlinien für die Bereitstellung unkomprimierter Dateien aus dem Cache an Clients, die die Komprimierung nicht verarbeiten können, und komprimierte Versionen derselben Dateien an den Client bereitzustellen, der mit der Komprimierung umgehen kann.

```
add cache selector uncompressed_response_selector http.req.url "http.req.
header(\"Host\")"

add cache contentGroup uncompressed_group -hitSelector uncompressed_responst_selector
 -invalSelector uncomp_resp_sel

add cache policy cache_uncompressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 !HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
uncompressed_group

bind cache global cache_uncompressed -priority 100 -gotoPriorityExpression
END -type REQ_OVERRIDE

add cache selector compressed_response_selector HTTP.REQ.URL "HTTP.REQ.
HEADER(\"Host\")""HTTP.REQ.HEADER(\"Accept-Encoding\")"

add cache contentGroup compressed_group -hitSelector compressed_response_selector
```



```
add cache policy cache_compressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
compressed_group

bind cache global cache_compressed -priority 200 -gotoPriorityExpression
END -type REQ_OVERRIDE
```

Konfigurieren einer Richtlinienbank für das Caching

Alle Policen, die mit einem bestimmten Verbindungspunkt verknüpft sind, werden zusammenfassend als Policenbank bezeichnet. Sie können nicht nur Prioritätsstufen für Policen in einer Bank konfigurieren, sondern auch die Reihenfolge der Auswertung in einer Bank ändern, indem Sie Goto-Ausdrücke konfigurieren. Sie können die Bewertungsreihenfolge weiter ändern, indem Sie eine externe Policybank von der aktuellen Policybank aus aufrufen. Sie können auch neue Policy-Banks konfigurieren, denen Sie Ihre eigenen Labels zuweisen. Da solche Policy-Banks an keinen Punkt im Verarbeitungszyklus gebunden sind, können sie nur innerhalb anderer Policenbanken aufgerufen werden. Der Einfachheit halber werden Richtlinienbanken, deren Labels keinem integrierten Bindepunkt entsprechen, als Richtlinienlabels bezeichnet.

Zusätzlich zur Steuerung der Reihenfolge der Richtlinienbewertung durch Bindung der Richtlinie und Zuweisen einer Prioritätsstufe, wie unter “Binding Policys“beschrieben, können Sie den Ablauf innerhalb einer Bank von Richtlinien festlegen, indem Sie einen Goto-Ausdruck konfigurieren. Ein Goto-Ausdruck überschreibt den durch die Prioritätsstufen bestimmten Fluss. Sie können den Bewertungsablauf auch steuern, indem Sie nach der Auswertung eines Eintrags in der aktuellen Bank eine externe Policy-Bank aufrufen. Die Bewertung wird immer an die aktuelle Bank zurückgesendet, nachdem die Bewertung abgeschlossen ist.

In der folgenden Tabelle sind die Einträge zur Kontrollbewertung in einer Policy-Bank zusammengefasst.

Attribut	Spezifiziert
Name	Der Name einer Richtlinie oder, um eine andere Richtlinienbank aufzurufen, ohne die Richtlinie zu bewerten, das Schlüsselwort NOPOLICY. Sie können NOPOLICY mehr als einmal in einer Policenbank angeben, aber Sie können eine benannte Policy nur einmal angeben.
Priorität	Eine ganze Zahl. Je niedriger die Ganzzahl ist, desto höher ist die Priorität.

Attribut	Spezifiziert
Gehe zu Expression	Legt die nächste Richtlinie oder Policy-Bank fest, die bewertet werden soll. Sie können einen der folgenden Werte angeben: 1. WEITER: Gehen Sie zu der Richtlinie mit der nächsthöheren Priorität. 2. ENDE: Beenden Sie die Bewertung. 3. USE_INVOCATION_RESULT: Gilt, wenn dieser Eintrag eine andere Policybank aufruft. Wenn das letzte Goto in der aufgerufenen Bank den Wert END hat, wird die Auswertung beendet. Wenn das letzte Goto etwas anderes als END ist, führt die aktuelle Policy-Bank einen NEXT-Befehl durch. 4. Positive Zahl: Prioritätsnummer der nächsten zu bewertenden Richtlinie. 5. Numerischer Ausdruck: Ausdruck, der die Prioritätsnummer der nächsten auszuwertenden Richtlinie erzeugt. Goto kann nur in einer Richtlinienbank durchgeführt werden. Das Auslassen des Goto-Ausdrucks entspricht der Angabe von END.
Aufruftstyp	Bezeichnet einen Policenbanktyp. Der Wert kann einer der folgenden sein: 1. Virtuellen Server anfordern: Ruft Richtlinien zur Anforderungszeit auf, die einem virtuellen Server zugeordnet sind. 2. Virtueller Antwortserver: Ruft Richtlinien für die Reaktionszeit auf, die einem virtuellen Server zugeordnet sind. 3. Policy Label: Ruft eine andere Richtlinienbank auf, die durch das Richtlinienlabel der Bank gekennzeichnet ist.
Name des Aufrufs	Name eines virtuellen Servers oder Richtlinienbezeichnung, abhängig von dem Wert, den Sie für den Aufruftyp angegeben haben.

Der integrierte Cache verfügt über zwei integrierte Richtlinienbeschriftungen, und Sie können weitere Richtlinienlabels konfigurieren:

`_reqBuiltInDefaults`: Diese Policy Label wird vom Standardbindepunkt für die Anforderungszeit aus aufgerufen.
`_resBuiltInDefaults`: Diese Policy Label wird vom Standardbindepunkt für die Antwortzeit aus aufgerufen.

So rufen Sie eine Richtlinienbezeichnung in einer Caching-Richtlinienbank mit der Befehlszeilenschnittstelle auf

Geben Sie in der Befehlszeile Folgendes ein:

```
bind cache policylabel <labelName> -policname<policyName> -priority<
    priority> [-gotoPriorityExpression <gotopriorityExpression>] [-
    invoke <labelType> <labelName>]
<!--NeedCopy-->
```

So rufen Sie ein Policy Label in einer Caching-Policy-Bank mit der GUI auf:

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**, und geben Sie den relevanten Bindpunkt (Override Global oder Standard Global) und den Verbindungstyp an, um die Liste der an diesen Bindungspunkt gebundenen Richtlinien anzuzeigen.
2. Wenn Sie ein Richtlinienlabel aufrufen möchten, ohne eine Richtlinie auszuwerten, klicken Sie auf **NOPOLICY**.

> **Hinweis:**
>
> Um eine externe Policybank aufzurufen, klicken Sie auf das Feld in der Spalte Aufruftyp und wählen Sie in der Policybank den Typ der Policybank aus, den Sie an dieser Stelle aufrufen möchten. Dies kann ein globales Label oder eine virtuelle Serverbank sein. Geben Sie im Feld Invoke Name die Bezeichnung oder den Namen des virtuellen Servers ein.

So rufen Sie ein Caching-Richtlinienlabel in einer Richtlinienbank für virtuelle Server mithilfe der Befehlszeilenschnittstelle auf

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name>@ -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```

```
bind cs vserver <name> -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```


So rufen Sie mithilfe der GUI ein Caching-Richtlinienlabel in einer Richtlinienbank für virtuelle Server auf

1. **Navigieren Sie zu**Traffic Management**>**Load Balancing/Content Switching**>**Virtuelle Server**, wählen Sie den virtuellen Server aus und klicken Sie auf Richtlinien.**
2. Wenn Sie einen vorhandenen Eintrag in dieser Bank konfigurieren, überspringen Sie diesen Schritt. Wenn Sie dieser Richtlinienbank eine neue Richtlinie hinzufügen oder den Eintrag Dummy NOPOLICY verwenden möchten, klicken Sie auf **Hinzufügen** und führen Sie einen der folgenden Schritte aus:
   - Um eine neue Richtlinie zu konfigurieren, klicken Sie auf Cache und konfigurieren Sie die neue Richtlinie wie unter Richtlinie konfigurieren im integrierten Cachebeschrieben.
   - Um eine Richtlinienbank aufzurufen, ohne eine Richtlinie in einer Regel zu verarbeiten, wählen Sie die `NOPOLICY-CACHE` Option aus.

> **Hinweis:**
>
> Um eine externe Policybank aufzurufen, klicken Sie auf das Feld in der Spalte Aufruftyp und wählen Sie in der Policybank den Typ der Policybank aus, den Sie an dieser Stelle aufrufen möchten. Dies kann ein globales Label oder eine virtuelle Serverbank sein. Geben Sie im Feld Invoke Name die Bezeichnung oder den Namen des virtuellen Servers ein.

Konfigurieren Sie ein Richtlinienlabel in einem integrierten Cache

Zusätzlich zum Konfigurieren von Richtlinien in einer Richtlinienbank für einen der integrierten Bindpunkte oder einen virtuellen Server können Sie Caching-Richtlinienlabels erstellen und Richtlinienbänke für diese neuen Labels konfigurieren.

Eine Policy Label für den integrierten Cache kann nur von einem der Bindepunkte aus aufgerufen werden, die Sie im Richtlinien-Manager im Detailbereich für **integrierte Caching-Details** (Anforderungsüberschreibung, Anforderungsstandard, Antwortüberschreibung oder Antwortstandard) oder den integrierten Richtlinienbeschriftungen `\\_reqBuiltinDefaults` und `\\_resBuiltinDefaults` anzeigen können. Sie können eine Richtlinienbezeichnung beliebig oft aufrufen, anders als eine Richtlinie, die nur einmal aufgerufen werden kann.

Die NetScaler-GUI bietet eine Option zum Umbenennen eines Richtlinienlabels. Die Umbenennung eines Richtlinienlabels hat keinen Einfluss auf den Bewertungsprozess der an das Label gebundenen Richtlinien.

> **Hinweis**:
>
> Sie können die Richtlinie `NOPOLICY` “Dummy” verwenden, um jedes Policy Label von einer anderen Richtlinienbank aufzurufen. Der `NOPOLICY` Eintrag ist ein Platzhalter, der keine Regel verarbeitet.

So konfigurieren Sie eine Richtlinienbezeichnung für das Caching mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile den folgenden Befehl ein, um ein Richtlinienlabel zu erstellen und die Konfiguration zu überprüfen:

- `add cache policylabel <labelName> -evaluates (REQ|RES)`
- `show cache policylabel <labelName>`

Rufen Sie dieses Richtlinienlabel von einer Richtlinienbank auf.

So konfigurieren Sie eine Policy Label für das Caching mit der GUI:

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Richtlinienlabels**, fügen Sie eine Richtlinienbezeichnung hinzu, und binden Sie die zwischengespeicherten Richtlinien.

> **Hinweis:**
> Um sicherzustellen, dass der NetScaler das Policy Label zum richtigen Zeitpunkt verarbeitet, konfigurieren Sie einen Aufruf dieses Labels in einer der Richtlinienbanken, die mit den integrierten Bindepunkten verknüpft sind.

So benennen Sie ein Policy Label mit der GUI um:

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Richtlinienbezeichnungen**, wählen Sie die Richtlinienbezeichnung aus, und benennen Sie sie um.

Entbinden und löschen Sie eine integrierte Caching-Richtlinie und ein Richtlinienlabel

Sie können die Bindung einer Richtlinie an eine Policenbank aufheben und sie löschen. Um die Richtlinie zu löschen, müssen Sie sie zunächst aufheben. Sie können auch den Aufruf eines Richtlinienlabels entfernen und ein Richtlinienlabel löschen. Um das Policy-Label zu löschen, müssen Sie zunächst alle Aufrufe entfernen, die Sie für das Label konfiguriert haben.

Sie können die Labels für die integrierten Bindungspunkte nicht aufheben oder löschen (Anforderungsstandard, Anforderungsüberschreibung, Antwortstandard und Antwortüberschreibung).

So heben Sie die Bindung einer globalen Caching-Richtlinie mithilfe der Befehlszeilenschnittstelle auf

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind cache global <policy>
```

So heben Sie die Bindung einer für virtuelle Server spezifischen Caching-Richtlinie mithilfe der Befehlszeilenschnittstelle auf

Geben Sie in der Befehlszeile Folgendes ein:

```
(unbind lb vserver|unbind cs vserver)<vserverName> -policyName <policyName>
 -type(REQUEST|RESPONSE)
```

So löschen Sie eine Caching-Richtlinie mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
rm cache policy <policyName>
```

So heben Sie die Bindung einer Caching-Richtlinie mit der GUI auf:

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**, und heben Sie die Bindung von Richtlinien auf, indem Sie den relevanten Bindepunkt und den Verbindungstyp (Anforderung/Antwort) angeben.

So löschen Sie einen Richtlinienbeschriftungsaufruf mit der GUI:

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**und geben Sie den entsprechenden Verbindungspunkt (virtueller Lastausgleichsserver oder virtueller Content Switching-Server) und den Verbindungstyp an, um die Liste der an diesen virtuellen Server gebundenen Cache-Richtlinien anzuzeigen.
2. Deaktivieren Sie in der Spalte Invoke den Eintrag.

Cache-Unterstützung für Datenbankprotokolle

May 11, 2023

Die integrierte Cache-Funktion überwacht und speichert Datenbankanfragen, wie in den Cache-Richtlinien festgelegt. Benutzer müssen die Cache-Richtlinien für die Protokolle MYSQL und MSSQL konfigurieren, da die NetScaler-Appliance keine Standardrichtlinien bereitstellt. Denken Sie bei der Konfiguration der Standardprotokolle daran, dass die anforderungsbasierten Richtlinien nur CACHE- und INVAL-Aktionen unterstützen, während die antwortbasierten Richtlinien nur „NOCACHE“ -Aktionen unterstützen. Nachdem Sie die Richtlinien konfiguriert haben, müssen Sie sie an virtuelle Server binden. MYSQL- und MSSQL-Richtlinien, sowohl Anfrage- als auch Antwortrichtlinien, sind nur an virtuelle Server gebunden.

Bevor Sie eine Cache-Richtlinie erstellen, müssen Sie eine Cache-Inhaltsgruppe vom Typ MYSQL oder MSSQL erstellen. Wenn Sie eine Cache-Content-Gruppe erstellen, verknüpfen Sie mindestens einen Auswahlselektor mit ihr. Weitere Informationen finden Sie unter Einrichten einer Basis-Content-Gruppe zum Einrichten einer Cache-Inhaltsgruppe.

Im folgenden Beispiel wird erläutert, wie Sie die Cache-Unterstützung für SQL-Protokolle konfigurieren und überprüfen.

```
1 > enable feature IC
2 > set cache parameter -memlimit 100
3 > add cache selector sel1 mssql.req.query.text
4
5 > add cache contentgroup cg1  -type "MSSQL" -hitselector "sel1" -
     invalselector "inval_sel" -relExpiry "500" -maxResSize
6  "100"
```



```
> add cache policy cp1  -rule "mssql.req.query.command.contains("select")" -action "CACHE" -storeInGroup "cg1"
> add cache policy cp2  -invalObjects "cg1" -rule "mssql.req.query.text.contains("insert")" -action "INVAL"
> add db user user1  -password "Pass1"
> add service svc_sql_1 10.102.147.70 mssql 64834 -healthMonitor "NO" -downstateflush "ENABLED"
> add lb vserver lb_mssql1 mssql 10.102.147.77 1433  -lbmethod "roundrobin"
> bind lb vserver lb_mssql1 svc_sql_1
> bind lb vserver lb_mssql1 -policyName cp1  -type "REQUEST" -priority "2"
> bind lb vserver lb_mssql1 -policyName cp2  -type "REQUEST" -priority "1"

> show cache selector sel1
     Name:sel1
                    Expressions:
                    1)mssql.req.query.text
> show cache policy cp1
                    Name:cp1
     Rule:mssql.req.query.command.contains("select")
                    CacheAction:CACHE
                    Stored in group: cg1
                    UndefAction:Use Global
                Hits:2
                    Undef Hits:0
                    Policy is bound to following entities
                    1) Bound to:
                                REQ VSERVER lb_mssql1
                                Priority:2
                                GotoPriorityExpression: END
<!--NeedCopy-->
```

Hinweis:

Die Methoden zur Reduzierung von Flash-Crowds, wie in Flash Crowds reduzierenerklärt, werden für MYSQL- und MSSQL-Protokolle nicht unterstützt.

Ausdrücke für Caching-Richtlinien und Selektoren konfigurieren

May 11, 2023

Ein Anforderungszeitausdruck untersucht Daten in der Anforderungszeit-Transaktion, und ein Reaktionszeitausdruck untersucht Daten in einer Response-Time-Transaktion. In einer Richtlinie für das Caching führt die NetScaler-Appliance die mit der Richtlinie verknüpfte Aktion aus, wenn ein Ausdruck mit Daten in einer Anfrage oder Antwort übereinstimmt. In einem Selektor werden Anforderungszeitausdrücke verwendet, um übereinstimmende Antworten zu finden, die in einer Content-Gruppe gespeichert sind.

Bevor Sie Richtlinien und Selektoren für den integrierten Cache konfigurieren, müssen Sie mindestens die Hostnamen, Pfade und IP-Adressen kennen, die in HTTP-Anforderungs- und Antwort-URLs angezeigt werden. Und Sie müssen wahrscheinlich das Format ganzer HTTP-Anfragen und -Antworten kennen. Programme wie Live HTTP-Header http://livehttpheaders.mozdev.org/)or HTTPFox https://addons.mozilla.org/en-US/firefox/addon/6647 können Ihnen helfen, die Struktur der HTTP-Daten zu untersuchen, mit denen Ihre Organisation zusammenarbeitet.

Es folgt ein Beispiel für eine HTTP-GET-Anfrage für ein Aktienkursprogramm:

```
GET /quote.dll?page=dynamic&mode=data&mode=stock&symbol=CTXS&page=multi
    &selected=CTXS&random=0.00792039478975548 HTTP/1.1

Host: quotes.mystockquotes.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
    Gecko/2008052906 Firefox/3.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q
    =0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate,compress,pack200-gzip

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

Referer: http://quotes.mystockquotes.com/quote.dll?mode=stock&symbol=
    CTXS&page=multi&selected=CTXS

Cookie: __qca=1210021679-72161677-10297606
<!--NeedCopy-->
```

Beachten Sie beim Konfigurieren eines Ausdrucks die folgenden Einschränkungen:

Ausdruck-Typ	Einschränkungen
Anfrage	Konfigurieren Sie keine Anforderungszeitausdrücke in einer Richtlinie mit einer CACHE- oder NOCACHE-Aktion. Verwenden Sie stattdessen MAY_CACHE oder MAY_NOCACHE.
Antwort	Konfigurieren Sie Ausdrücke zur Reaktionszeit nur in Caching-Richtlinien. Selektoren können nur Anforderungszeitausdrücke verwenden. Konfigurieren Sie keine Reaktionszeitausdrücke in einer Richtlinie mit einer INVAL-Aktion. Hinweis: Konfigurieren Sie keine Reaktionszeitausdrücke in einer Richtlinie mit einer CACHE-Aktion und einer parametrisierten Content-Gruppe. Verwenden Sie die MAY_CACHE -Aktion.

> **Hinweis:**
> Eine umfassende Diskussion erweiterter Ausdrücke finden Sie unter Richtlinien und Ausdruck.

Ausdruckssyntax

Im Folgenden sind die grundlegenden Komponenten der Syntax:

- Trennen Sie Schlüsselwörter wie folgt mit Punkten (.):

```
http.req.url
```

- Schließen Sie String-Werte wie folgt in Klammern und Anführungszeichen ein:

```
http.req.url.query.contains("this")
```

- Wenn Sie einen Ausdruck von der Befehlszeile aus konfigurieren, müssen Sie interne Anführungszeichen (die Anführungszeichen, die die Werte im Ausdruck begrenzen, im Gegensatz zu den Anführungszeichen, die den Ausdruck begrenzen) umgehen. Eine Methode besteht darin, einen Schrägstrich wie folgt zu verwenden:

```
\"abc\"
```

Selektorausdrücke werden in der Reihenfolge ihres Aussehens ausgewertet, und mehrere Ausdrücke in einer Selektordefinition werden durch ein logisches UND verbunden. Im Gegensatz zu Selektorausdrücken können Sie boolesche Operatoren angeben und die Priorität in einem erweiterten Ausdruck für eine Richtlinienregel ändern.

Konfigurieren eines Ausdrucks in einer Caching-Richtlinie oder einem Selektor

> **Hinweis:**
> Die Syntax für einen Richtlinienausdruck unterscheidet sich von einem Selektorausdruck. Eine umfassende Diskussion fortgeschrittener Ausdrücke finden Sie unter “Richtlinien und Ausdrücke. “

So konfigurieren Sie einen Richtlinienausdruck mit der Befehlszeilenschnittstelle

1. Starten Sie die Richtliniendefinition wie unter “Global Binden einer integrierten Caching-Richtlinie beschrieben. “
2. Um die Richtlinienregel zu konfigurieren, begrenzen Sie die gesamte Regel in Anführungszeichen und begrenzen Sie Zeichenfolgenwerte innerhalb der Regel in Escape-Anführungszeichen.

Ein Beispiel:

“http.req.url.contains(“jpg”)”

1. Um boolesche Werte hinzuzufügen, fügen Sie &&, || oder! Betreiber.

Die folgenden Beispiele sind:

```
"http.req.url.contains(\"jpg\")|| http.req.url.contains(\"jpeg\")"
```

```
"http.req.url.query.contains(\"IssuePage\")"
```

```
"http.req.header(\"Host\")contains(\"my.company.com\")&& http.req.method.eq
(\"GET\")&& http.req.url.query.contains(\"v=7\")"
```

1. So konfigurieren Sie eine Evaluierungsreihenfolge für die Bestandteile einer Verbindung

```
"http.req.url.contains(\"jpg\")|| (http.req.url.contains(\"jpeg\")&& http.
req.method.eq(\"GET\"))"
```

So konfigurieren Sie einen Selektorausdruck mit der Befehlszeilenschnittstelle:

1. Starten Sie die Selektordefinition wie unter Info zu Inhaltsgruppen beschrieben.
2. Um den Selektorausdruck zu konfigurieren, begrenzen Sie die gesamte Regel in Anführungszeichen und begrenzen Sie Zeichenfolgenwerte innerhalb der Regel in Escape-Anführungszeichen.

Ein Beispiel:

```
"http.req.url.contains(\"jpg\")"
```

1. Sie können keine booleschen Werte hinzufügen, &&, || oder! Betreiber. Geben Sie jedes in Anführungszeichen getrennte Ausdruckselement ein. Mehrere Ausdrücke in der Definition werden als zusammengesetzter Ausdruck behandelt, der durch logische ANDs verbunden ist.

Die folgenden Beispiele sind:


```
"http.req.url.query.value("ProductId")" "http.req.url.query.value("
    BatchNum")" "http.req.url.query.value("depotLocation")"
<!--NeedCopy-->
```

So konfigurieren Sie einen Richtlinien- oder Selektorausdruck mit der GUI

1. Starten Sie die Richtlinie- oder Auswahldefinition wie unter “So konfigurieren Sie eine Richtlinie zum Caching oder Invalidierung mithilfe des Konfigurationsdienstprogramms” oder “So konfigurieren Sie einen Selektor mit dem Konfigurationsdienstprogramm. “
2. Im Feld **Ausdruck** können Sie die Richtlinie “Erweitert” entweder manuell eingeben, indem Sie auf Zur klassischen Syntax wechseln klicken, oder mithilfe des **Ausdruckseditors einen neuen Ausdruck**erstellen.
3. Um einen Operator zwischen zwei Teilen eines zusammengesetzten Ausdrucks einzufügen, klicken Sie auf die Schaltfläche Operatoren und wählen Sie den Operatortyp aus. Das Folgende ist ein Beispiel für einen konfigurierten Ausdruck mit einem booleschen ODER (signalisiert durch doppelte vertikale Balken, ||):
4. Klicken Sie auf die Dropdownliste **Häufig verwendete Ausdrücke**, um die häufig verwendeten Ausdrücke einzufügen.
5. Um den Ausdruck zu testen, klicken Sie auf **Auswerten**. Wählen Sie im Dialogfeld **Ausdrucks-Evaluator** den Flow-Typ aus, der dem Ausdruck entspricht. Fügen Sie in das Datenfeld die HTTP-Anfrage oder -Antwort ein, die Sie mit dem Ausdruck analysieren möchten, und klicken Sie auf **Auswerten**.

Zwischengespeicherte Objekte und Cache-Statistiken anzeigen

Sie können bestimmte zwischengespeicherte Objekte anzeigen und Zusammenfassungsstatistiken über Cache-Anfragen, Fehlschläge und Speicherauslastung anzeigen. Die Statistiken geben einen Einblick in die Datenmenge, die aus dem Cache bereitgestellt wird, welche Elemente für den größten Leistungsvorteil verantwortlich sind und was Sie optimieren können, um die Cache-Leistung zu verbessern.

Dieser Abschnitt enthält die folgenden Details:

- Zwischengespeicherte Objekte anzeigen
- Bestimmte gecachte Antworten finden
- Cache-Statistiken anzeigen

Zwischengespeicherte Objekte anzeigen

Nachdem Sie das Caching aktiviert haben, können Sie Details für zwischengespeicherte Objekte anzeigen. Sie können beispielsweise die folgenden Elemente anzeigen:

- Antwortgrößen und Header-Größen
- Statuscodes
- Content-Gruppen
- ETag, Letzte Änderung und Cache-Control-Header
- URLs anfordern
- Treffer-Parameter
- Ziel-IP-Adressen
- Anfragen- und Reaktionszeiten

So zeigen Sie eine Liste der zwischengespeicherten Objekte über die Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

```
show cache object
```

Eigenschaften	Beschreibung
Antwortgröße (Byte)	Die Größe des Antwortheaders und des Textkörpers.
Größe des Antwortheaders (Byte)	Die Größe des Header-Teils der Antwort.
Antwortstatuscode	Der Statuscode, der mit der Antwort gesendet wurde.
eTag	Der eTag-Header, der in die Antwort eingefügt wurde. In der Regel gibt dieser Header an, ob sich die Antwort kürzlich geändert hat.
Zuletzt geändert	Der Header “Letzte Änderung”, der in die Antwort eingefügt wurde. Dieser Header gibt das Datum an, an dem die Antwort zuletzt geändert wurde.
Cache-Steuerung	Der Cache-Control-Header, der in die Antwort eingefügt wurde.
Datum	Der Date-Header, der angibt, wann die Antwort gesendet wurde.
Contentgroup	Die Content-Gruppe, in der die Antwort gespeichert wird.
Komplexes Spiel	Wenn dieses Objekt basierend auf parametrisierten Werten zwischengespeichert wurde, lautet dieser Feldwert JA.
Host	Der Host, der in der URL angegeben wurde, die diese Antwort angefordert hat.

Eigenschaften	Beschreibung
Hostport	Der Listenport für den Host, der in der URL angegeben ist, die diese Antwort angefordert hat
URL	Die für die gespeicherte Antwort ausgegebene URL.
Ziel-IP	Die IP-Adresse des Servers, von dem diese Antwort abgerufen wurde.
Destination port	Der Listenport für den Zielserver.
Treffer-Parameter	Wenn die Inhaltsgruppe, die die Antwort speichert, Trefferparameter verwendet, werden sie in diesem Feld aufgeführt.
Auswahl treffen	Wenn diese Content-Gruppe einen Trefferauswahl verwendet, wird sie in diesem Feld aufgeführt.
Inval-Selektor	Wenn diese Content-Gruppe einen Selektor für die Invalidierung verwendet, wird sie in diesem Feld aufgeführt.
Selektor-Ausdrücke	Wenn diese Content-Gruppe einen Selektor verwendet, zeigt dieses Feld den Ausdruck an, der die Auswahlregel definiert.
Request time	Die Zeit in Millisekunden seit der Ausgabe der Anfrage.
Reaktionszeit	Die Zeit in Millisekunden, seit der Cache begonnen hat, die Antwort zu erhalten.
Alter	Zeitspanne, in der sich das Objekt im Cache befindet.
Ablauf	Zeitspanne, nach der das Objekt als abgelaufen markiert wird.
Gespült	Ob die Antwort nach Ablauf gespült wurde.

Eigenschaften	Beschreibung
Prefetch	Wenn Prefetch für diese Content-Gruppe konfiguriert wurde, ist die Zeit vor Ablauf, während der das Objekt vom Ursprung abgerufen wird. Prefetch gilt nicht für negative Objekte (z. B. 404 “Objekt nicht gefunden” -Antworten).
Aktuelle Leser	Ungefähr die aktuelle Anzahl der Anfragen, die bearbeitet werden. Wenn eine Antwort mit einem Header-Objekt in Content-Length heruntergeladen wird, sind die aktuellen Fehlschläge und die aktuellen Leserwerte in der Regel jeweils 1. Wenn ein Chunked Response-Objekt heruntergeladen wird, ist der aktuelle Fehlschlagwert in der Regel 1, aber der aktuelle Leserwert ist normalerweise 0, da die Chunked Response, die an den Client bereitgestellt wird, nicht aus den integrierten Caching-Puffern stammt.
Aktuelle Fehlschläge	Die aktuelle Anzahl von Anfragen, die zu einem Cache-Verpassen und Abrufen vom Ursprungsserver geführt haben. Dieser Wert ist normalerweise 0 oder 1. Wenn Poll Every Time für eine Content-Gruppe aktiviert ist, kann die Anzahl größer als 1 sein.
Treffer	Die Anzahl der Cache-Treffer für dieses Objekt.
Fehlschläge	Die Anzahl der Cache-Fehlschläge für dieses Objekt
Komprimierungsformat	Die Art der Komprimierung, die auf dieses Objekt angewendet wird. Zu den Komprimierungsformaten gehören gzip, deflate, compress und pack200-gzip.
HTTP-Version als Antwort	Die Version von HTTP, die zum Senden der Antwort verwendet wurde.

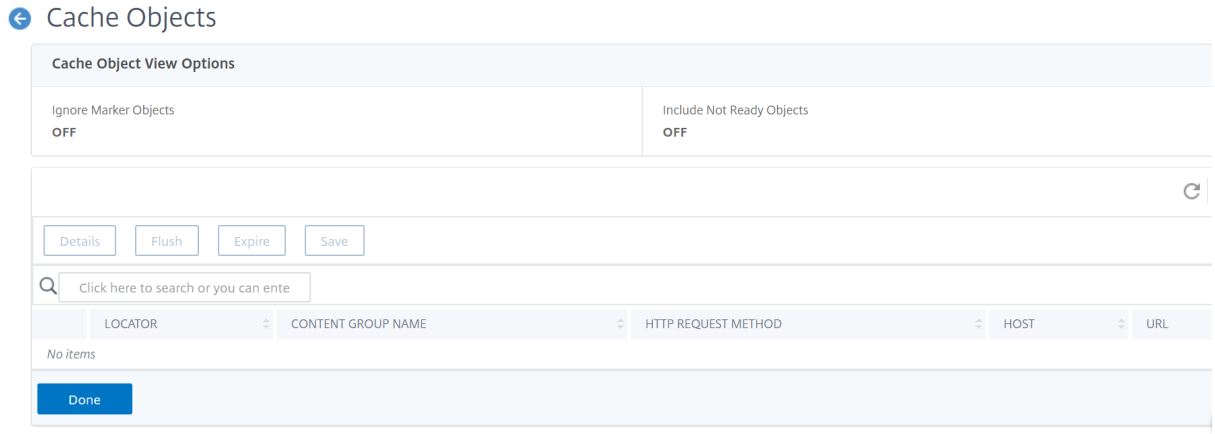
Eigenschaften	Beschreibung
Schwaches Etag als Antwort vorhanden	Starke Etag-Header ändern sich, wenn sich die Bits einer Entität ändern. Starke Header basieren auf den Oktettwerten eines Objekts. Schwache Etag-Header ändern sich, wenn sich die Bedeutung einer Entität ändert. Schwache Etag-Werte basieren auf semantischer Identität. Schwache Etags Werte beginnen mit einem “W.”
Negative Marker-Zelle	Ein Marker-Objekt ist zwischengespeichert, erfüllt aber noch nicht alle Kriterien für das Cache. Beispielsweise kann das Objekt die maximale Antwortgröße für die Content-Gruppe überschreiten. Für Objekte dieses Typs wird eine Markenzelle erstellt. Wenn ein Benutzer das nächste Mal eine Anfrage für dieses Objekt sendet, wird ein Cache-Fehler bereitgestellt.
Reason Marker erstellt	Der Grund, warum eine Marker-Zelle erstellt wurde (z. B. “Warten auf Minhit”, “Antwortdaten für Inhaltslänge sind nicht im Gruppengrößenlimit”).
Jedes Mal automatische Umfrage	Wenn der integrierte Cache eine bereits abgelaufene 200-OK-Antwort mit Validatoren (entweder die letzte Änderung oder die eTag-Antwortheader) erhält, speichert er die Antwort und markiert sie als Auto-PET (jedes Mal automatisch abfragen).
NetScaler Etag wurde als Antwort eingefügt	Eine Variante des ETag-Headers, der von der NetScaler-Appliance generiert wird. Der Wert YES wird angezeigt, wenn der NetScaler ein Etag in die Antwort einfügt.
Vollständige Antwort im Cache vorhanden	Zeigt an, ob dies eine vollständige Antwort ist.
Ziel-IP von DNS verifiziert	Gibt an, ob beim Speichern des Objekts eine DNS-Auflösung durchgeführt wurde.

Eigenschaften	Beschreibung
Objekt wird durch einen Cache-Forward-Proxy gespeichert	Gibt an, ob diese Antwort aufgrund eines Forward-Proxys gespeichert wurde, der im integrierten Cache konfiguriert ist.
Objekt ist ein Delta-Basisdatei	Eine Antwort, die delta-komprimiert ist.
Warten auf Minhits	Gibt an, ob diese Content-Gruppe eine Mindestanzahl von Original-Servern benötigt, die vor dem Zwischenspeichern einer Antwort getroffen werden.
Minhit zählen	Wenn diese Content-Gruppe vor dem Zwischenspeichern eines Objekts eine Mindestanzahl von Ursprungsserveranforderungen erfordert, wird in diesem Feld die Anzahl der bisher empfangenen Anforderungen angezeigt.
HTTP-Anforderungsmethode	Die Methode GET oder POST, die in der Anforderung verwendet wird, die dieses Objekt erhalten hat.
Gespeichert nach Richtlinie	Der Name der Caching-Richtlinie, die dazu geführt hat, dass dieses Objekt gespeichert wurde. Der Wert NICHT VERFÜGBAR gibt an, dass die Richtlinie deaktiviert oder gelöscht wurde. Der Wert NONE gibt an, dass das Objekt nicht mit einer sichtbaren Richtlinie übereinstimmte, sondern nach internen Kriterien für das Caching gespeichert wurde.
Metadaten der Anwendungs-Firewall vorhanden	Dieser Parameter wird verwendet, wenn die Anwendungs-Firewall und der integrierte Cache beide aktiviert sind. Die Anwendungs-Firewall analysiert den Inhalt einer Antwortseite, speichert ihre Metadaten (z. B. URLs und Formulare auf der Seite) und exportiert die Metadaten mit der Antwort in den Cache. Der Cache speichert die Seite und die Metadaten, und wenn der Cache die Seite bedient, sendet er die Metadaten zurück an die Sitzung der Anforderung.

Eigenschaften	Beschreibung
HTTP-Callout-Objekt, Name, Typ, Antwort	Diese Zellen geben an, ob diese Daten als Ergebnis eines HTTP-Callout-Ausdrucks gespeichert wurden, und liefern Informationen über verschiedene Aspekte des Callouts und die entsprechende Antwort. Weitere Informationen zu HTTP-Callouts finden Sie unter “HTTP-Callouts”.

So zeigen Sie zwischengespeicherte Objekte mit der GUI an

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Cache-Objekte**. Sie können alle zwischengespeicherten Objekte anzeigen und entsprechend nach Ihren Anforderungen sortieren.



Finde bestimmte zwischengespeicherte Antworten

Sie können einzelne Elemente im Cache basierend auf Suchkriterien finden. Es gibt verschiedene Methoden, um zwischengespeicherte Elemente zu finden, je nachdem, ob die Content-Gruppe, die die Daten enthält, Treffer- und Invalidierungsselektoren verwendet, wie folgt:

- Wenn die Content-Gruppe Selektoren verwendet, können Sie die Suche nur mit der Locator-ID für das zwischengespeicherte Element durchführen.
- Wenn die Content-Gruppe keine Selektoren verwendet, führen Sie die Suche mit Kriterien wie URL, Host, Name der Inhaltsgruppe durch.

Wenn Sie nach einer zwischengespeicherten Antwort suchen, können Sie einige Elemente nach URL und Host suchen. Wenn sich die Antwort in einer Content-Gruppe befindet, die einen Selektor verwendet, können Sie sie nur mit einer Locator-Nummer (z. B. 0x00000000ad7af00000050) finden. Um eine Locator-Nummer zur späteren Verwendung zu speichern, klicken Sie mit der rechten Maustaste auf

den Eintrag und wählen Sie **Kopieren**. Weitere Informationen zu Selektoren finden Sie unter “Konfigurieren von Selektoren und grundlegenden Inhaltsgruppen. “

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen an, die keinen Selektor haben, über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus <positive integer>] | -group <contentGroupName> |
 -ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen mit einem Selektor über die Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:

```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen an, die keinen Selektor haben, mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Optimierung > Integriertes Caching > Cache-Objekte**, klicken Sie auf Suchen und legen Sie die Suchkriterien fest, um die erforderliche zwischengespeicherte Antwort anzuzeigen.

Wenn Sie noch keine Inhaltsgruppen konfiguriert haben, befinden sich alle Objekte in der Gruppe Standard.

Cache-Statistiken anzeigen

In der folgenden Tabelle werden die detaillierten Cache-Statistiken zusammengefasst, die Sie anzeigen können.

Zähler	Beschreibung
—	—
Treffer	Antworten, die im integrierten Cache gefunden und aus diesem bereitgestellt werden. Umfasst statische Objekte wie Bilddateien, Seiten mit den Statuscodes 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 und Antworten, die einer benutzerdefinierten Richtlinie mit einer CACHE-Aktion entsprechen.
Fehlschläge	Es wurden HTTP-Anfragen abgefangen, bei denen die Antwort letztendlich vom Ursprungsserver abgerufen wurde.
Anfragen	Gesamtzahl der Cache-Anfragen plus Gesamtzahl der Cache-Fehler
Nicht-304 Treffer	Wenn der Benutzer ein Element mehrmals anfordert und das Element im Cache seit dem letzten Servieren der NetScaler-Appliance unverändert ist, gibt die NetScaler-Appliance

anstelle des zwischengespeicherten Objekts eine 304-Antwort an.
This statistic indicates how many items the NetScaler-Appliance served from the cache, excluding 304 responses.|
304 hits	Number of 304 (object not modified) responses the NetScaler-Appliance served from the cache.
304 hit ratio (%)	Percentage of 304 responses that the NetScaler-Appliance served, relative to other responses.
Hit ratio (%)	Percentage of responses that the NetScaler-Appliance served from the cache (cache requests) relative to responses that could not be served from the cache.
Origin bandwidth saved (%)	An estimate of the processing capacity that the NetScaler-Appliance saved on the origin server due to serving responses from the cache.
Bytes served by the NetScaler	Total number of bytes that the NetScaler-Appliance served from the origin server and the cache.
Bytes served by cache	Total number of bytes that the NetScaler-Appliance served from the cache.
Byte hit ratio(%)	Percentage of data that the NetScaler-Appliance served from the cache, relative to all of the data in all served responses.
Compressed bytes from cache	Amount of data, in bytes, that the NetScaler-Appliance served in compressed form.
Storable misses	If the NetScaler-Appliance does not find a requested object in the cache, it fetches the object from the origin server. Dies wird als Cache-Miss bezeichnet. A storable cache miss can be stored in the cache.
Non-storable misses	A non-storable cache miss cannot be stored in the cache.
Misses	All cache misses.
Revalidations	Max-Age setting in a Cache-Control header determines, in number of seconds, when an intervening cache must revalidate the content with the integrated cache before serving it to the user.
For more information, see “Inserting a Cache-Control Header.”
Successful revalidations	Number of revalidations that have been performed.
For more information, see “Inserting a Cache-Control Header.”
Conversions to conditional req	A user-agent request for a cached PET object is always converted to a conditional request and sent to the origin server.
For more information, see “Polling the Origin Server Every Time a Request Is Received.”
Storable miss ratio (%)	Storable cache misses as a percentage of non-storable cache misses.
Successful reval ratio (%)	Successful revalidations as a percentage of all revalidation attempts.
For more information, see “Inserting a Cache-Control Header.”
Expire at last byte	Number of times that the cache expired content immediately after receiving the last body byte. Gilt nur für positive Antworten, wie in der Tabelle “Cache-Hits and Misses beschrieben. “
For more information, see “Example of Performance Optimization.”

|Flashcache misses|If you enable Flash Cache, the cache allows only one request to reach the server, eliminating flash crowds. Diese Statistik gibt die Anzahl der Flash Cache-Anfragen an, die Cache-Fehler waren.
For more information, “Queuing Requests to the Cache.”|
|Flashcache hits|Number of Flash Cache requests that were cache hits.
For more information, see “Queuing Requests to the Cache.”|
Parameterized inval requests	Requests that match a policy with an invalidation (INVAL) action and a content group that uses an invalidation selector or parameters to selectively expire cached objects in the group.
Full inval requests	Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.
Inval requests	Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.
Parameterized requests	Number of cache requests that were processed using a policy with a parameterized content group.
Parameterized non-304 hits	Number of cache requests that were processed using a policy with a parameterized content group, where full cached response was found, and the response was not a 304 (object not updated) response.
Parameterized 304 hits	Number of cache requests that were processed using a policy with a parameterized content group, where the cached object was found, and the object was a 304 (object not updated) response.
Total parameterized hits	Number of cache requests that were processed using a policy with a parameterized content group, where the cached object was found.
Parameterized 304 hit ratio (%)	Percentage of 304 (object not updated) responses that were found using a parameterized policy, relative to all cache hits.
Poll every time requests	If Poll Every Time is enabled, the NetScaler-Appliance always consults the origin server before serving a stored object.
For more information, see “Polling the Origin Server Every Time a Request Is Received.”
Poll every time hits	Number of times a cache hit was found using the Poll Every Time method.
For more information, see “Polling the Origin Server Every Time a Request Is Received.”
Poll every time hit ratio (%)	Percentage of cache hits using the Poll Every Time method, relative to all searches for cached objects using Poll Every Time. For more information, see “Polling the Origin Server Every Time a Request Is Received.”
Maximum memory (KB)	Maximum amount of memory in the NetScaler-Appliance that is allocated to the cache. For more information, see “Configuring Global Attributes for Caching.”
Maximum memory active value (KB)	Maximum amount of memory (active value) that will be set after the memory is allocated to the cache. For more information, see “How to Configure the Integrated Caching Feature of a NetScaler-Appliance for various Scenarios.”
Utilized memory (KB)	Amount of memory that is actually being used.

Memory allocation failures	Number of failed attempts to utilize memory for the purpose of storing a response in the cache.
Largest response so far	Largest response in bytes found in either the cache or the origin server and sent to the client.
Cached objects	Number of objects in the cache, including responses that have not yet been fully downloaded and responses that have been expired but not yet flushed.
Marker objects	Marker objects are created when a response exceeds the maximum or minimum response size for the content group, or has not yet received the minimum number of hits for the content group.
Hits being served	Number of hits that have been served from the cache.
Misses being handled	Responses that were fetched from the origin server, stored in the cache, and then served. Sollte die Zahl für speicherbare Fehlschläge annähern. Beinhaltet keine nicht speicherbaren Fehlschläge.

So zeigen Sie Zusammenfassungs-Cache-Statistiken über die Befehlszeilenschnittstelle an:

Geben Sie in der Befehlszeile Folgendes ein:

```
stat cache
```

So zeigen Sie bestimmte Cache-Statistiken über die Befehlszeilenschnittstelle an:

Geben Sie in der Befehlszeile Folgendes ein:

```
stat cache -detail
```

```
1  > stat cache -detail
2
3  Integrated Cache Statistics - Detail
4  Integrated Cache Statistics - Summary
5                                          Rate (/s)
                                              Total
6
7
8  Hits                                           0
                        0
9
10 Misses                                         0
                        0
11
12 Requests                                       0
                        0
13
14 Hit ratio(%)                                  --
                        0
15
```



```
16 Origin bandwidth saved(%)                          --
                         0
17 Cached objects                                     --
                         0
18
19 Marker objects                                     --
                         0
20                                          Rate (/s)
                                               Total
21
22 Requests                                            0
                         0
23
24
25 Hit Statistics
26
27                                          Rate (/s)
                                               Total
28
29
30 Non-304 hits                                        0
                         0
31
32 304 hits                                            0
                         0
33
34
35 Sql hits                                            0
                         0
36
37
38 Hits                                                0
                         0
39
40 304 hit ratio(%)                                   --
                         0
41
42 Hit ratio(%)                                       --
                         0
43
44 Origin bandwidth saved(%)                          --
                         0
45 Byte Statistics
46                                          Rate (/s)
                                               Total
```



```
47
48
49 Bytes served by NetScaler                          648
       55379204
50
51 Bytes served by cache                              0
                          0
52 Byte hit ratio(%)                                 --
                          0
53 Compressed bytes from cache                        0
                          0
54
55 Miss Statistics
56
57                                                Rate (/s)
                                                     Total
58
59
60 Storable misses                                    0
                          0
61
62 Non-storable misses                                0
                          0
63
64 Misses                                             0
                          0
65
66 Revalidations                                      0
                          0
67
68 Successful revalidations                           0
                          0
69
70 Conversions to conditional req                     0
                          0
71
72
73 Storable miss ratio(%)                            --
                          0
74 Successful reval ratio(%)                         --
                          0
75
76 Flashcache Statistics
77                                                Rate (/s)
                                                     Total
```



```
78
79
80  Expire at last byte                                  0
                          0
81
82  Flashcache misses                                    0
                          0
83  Flashcache hits                                      0
                          0
84
85  Invalidation Statistics
86
87                                                 Rate (/s)
                                                      Total
88
89  Parameterized inval requests                         0
                          0
90
91
92  Full inval requests                                  0
                          0
93
94
95
96  Inval requests                                       0
                          0
97
98  Parameterized Caching Statistics
99
100                                                Rate (/s)
                                                      Total
101
102
103 Parameterized requests                               0
                          0
104
105 Parameterized non-304 hits                           0
                          0
106
107 Parameterized 304 hits                               0
                          0
108
109
110 Total parameterized hits                             0
                          0
```



```
111
112 Parameterized 304 hit ratio(%)                    --
                         0
113
114 Poll Every Time (PET) Statistics
115
116                                                Rate (/s)
                                                      Total
117
118
119 Poll every time requests                            0
                         0
120
121 Poll every time hits                               0
                         0
122
123 Poll every time hit ratio(%)                       --
                         0
124
125 Memory Usage Statistics
126                                                  Total
127
128 Maximum memory(KB)                                 0
129
130 Maximum memory active value(KB)                    0
131
132 Utilized memory(KB)                                0
133
134 Memory allocation failures                         0
135
136 Largest response so far(B)                         0
137
138 Cached objects                                     0
139
140 Marker objects                                     0
141
142 Hits being served                                  0
143 Misses being handled                               0
144  Done
145 <!--NeedCopy-->
```

So zeigen Sie Zusammenfassungs-Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte **Dashboard**.
2. Scrollen Sie nach unten zum Abschnitt **Integriertes Caching** des Fensters.

3. Um detaillierte Statistiken anzuzeigen, klicken Sie unten in der Tabelle auf den Link Mehr…

So zeigen Sie bestimmte Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte **Reporting** .
2. Erweitern Sie unter Integrierte Berichte den Eintrag **Integrierter Cache**, und klicken Sie dann auf den Bericht mit den Statistiken, die Sie anzeigen möchten.
3. Um den Bericht als Vorlage zu speichern, klicken Sie auf **Speichern unter** und benennen Sie den Bericht. Der gespeicherte Bericht wird unter **Benutzerdefinierte** Berichte angezeigt.

Zwischengespeicherte Objekte und Cache-Statistiken anzeigen

May 11, 2023

Sie können bestimmte zwischengespeicherte Objekte und zusammenfassende Statistiken zu Cache-Treffern, Fehlschlägen und Speichernutzung einsehen. Die Statistiken geben einen Einblick in die Datenmenge, die aus dem Cache bereitgestellt wird, welche Elemente für den größten Leistungsvorteil verantwortlich sind und was Sie optimieren können, um die Cache-Leistung zu verbessern.

Dieser Abschnitt enthält die folgenden Details:

- Zwischengespeicherte Objekte anzeigen
- Bestimmte gecachte Antworten finden
- Cache-Statistiken anzeigen

Zwischengespeicherte Objekte anzeigen

Nachdem Sie das Caching aktiviert haben, können Sie Details für zwischengespeicherte Objekte anzeigen. Sie können beispielsweise die folgenden Elemente anzeigen:

- Antwortgrößen und Header-Größen
- Statuscodes
- Content-Gruppen
- ETag, Letzte Änderung und Cache-Control-Header
- URLs anfordern
- Treffer-Parameter
- Ziel-IP-Adressen
- Anfragen- und Reaktionszeiten

So zeigen Sie eine Liste der zwischengespeicherten Objekte über die Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

`show cache object`

Eigenschaften	Spezifikation
Antwortgröße (Byte)	Die Größe des Antwortheaders und des Textkörpers.
Größe des Antwortheaders (Byte)	Die Größe des Header-Teils der Antwort.
Antwortstatuscode	Der Statuscode, der mit der Antwort gesendet wurde.
`ETag`	Der in die Antwort eingefügte `ETag` Header. In der Regel gibt dieser Header an, ob sich die Antwort kürzlich geändert hat.
Zuletzt geändert	Der Header “Letzte Änderung”, der in die Antwort eingefügt wurde. Dieser Header gibt das Datum an, an dem die Antwort zuletzt geändert wurde.
`Cache-Control`	Der Cache-Control-Header, der in die Antwort eingefügt wurde.
Datum	Der Date-Header, der angibt, wann die Antwort gesendet wurde.
`Contentgroup`	Die Content-Gruppe, in der die Antwort gespeichert wird.
Komplexes Spiel	Wenn dieses Objekt basierend auf parametrisierten Werten zwischengespeichert wurde, lautet dieser Feldwert JA.
Host	Der Host, der in der URL angegeben wurde, die diese Antwort angefordert hat.
Hostport	Der Listenport für den Host, der in der URL angegeben ist, die diese Antwort angefordert hat
URL	Die für die gespeicherte Antwort ausgegebene URL.
Ziel-IP	Die IP-Adresse des Servers, von dem diese Antwort abgerufen wurde.
Destination port	Der Listenport für den Zielserver.

Eigenschaften	Spezifikation
Treffer-Parameter	Wenn die Inhaltsgruppe, die die Antwort speichert, Trefferparameter verwendet, werden sie in diesem Feld aufgeführt.
Auswahl treffen	Wenn diese Content-Gruppe einen Trefferauswahl verwendet, wird sie in diesem Feld aufgeführt.
Inval-Selektor	Wenn diese Content-Gruppe einen Selektor für die Invalidierung verwendet, wird sie in diesem Feld aufgeführt.
Selektor-Ausdrücke	Wenn diese Content-Gruppe einen Selektor verwendet, zeigt dieses Feld den Ausdruck an, der die Auswahlregel definiert.
Request time	Die Zeit in Millisekunden seit der Ausgabe der Anfrage.
Reaktionszeit	Die Zeit in Millisekunden, seit der Cache begonnen hat, die Antwort zu erhalten.
Alter	Zeitspanne, in der sich das Objekt im Cache befindet.
Ablauf	Zeitspanne, nach der das Objekt als abgelaufen markiert wird.
Gespült	Ob die Antwort nach Ablauf gespült wurde.
Prefetch	Wenn Prefetch für diese Content-Gruppe konfiguriert wurde, ist die Zeit vor Ablauf, während der das Objekt vom Ursprung abgerufen wird. Prefetch gilt nicht für negative Objekte (z. B. 404 “Objekt nicht gefunden” -Antworten).

Eigenschaften	Spezifikation
Aktuelle Leser	Ungefähr die aktuelle Anzahl der ausgelesenen Treffer. Wenn eine Antwort mit einem Header-Objekt in Content-Length heruntergeladen wird, sind die aktuellen Fehlschläge und die aktuellen Leserwerte in der Regel jeweils 1. Wenn ein Chunked Response-Objekt heruntergeladen wird, ist der aktuelle Fehlschlagwert in der Regel 1, aber der aktuelle Leserwert ist normalerweise 0, da die Chunked Response, die an den Client bereitgestellt wird, nicht aus den integrierten Caching-Puffern stammt.
Aktuelle Fehlschläge	Die aktuelle Anzahl von Anfragen, die zu einem Cache-Verpassen und Abrufen vom Ursprungsserver geführt haben. Dieser Wert ist normalerweise 0 oder 1. Wenn Poll Every Time für eine Content-Gruppe aktiviert ist, kann die Anzahl größer als 1 sein.
Treffer	Die Anzahl der Cache-Treffer für dieses Objekt.
Fehlschläge	Die Anzahl der Cache-Fehler für dieses Objekt.
Komprimierungsformat	Die Art der Komprimierung, die auf dieses Objekt angewendet wird. Zu den Komprimierungsformaten gehören gzip, deflate, compress und pack200-gzip.
HTTP-Version als Antwort	Die Version von HTTP, die zum Senden der Antwort verwendet wurde.
Als Reaktion schwach `etag` anwesend	Starke `etag` Header ändern sich, wenn sich die Teile einer Entität ändern. Starke Header basieren auf den Oktettwerten eines Objekts. Schwache `etag` Header ändern sich, wenn sich die Bedeutung einer Entität ändert. Schwache `etag` Werte basieren auf semantischer Identität. Schwache `etags`-Werte beginnen mit einem “W”.

Eigenschaften	Spezifikation
Negative Marker-Zelle	Ein Marker-Objekt ist zwischengespeichert, erfüllt aber noch nicht alle Kriterien für das Cache. Beispielsweise kann das Objekt die maximale Antwortgröße für die Content-Gruppe überschreiten. Für Objekte dieses Typs wird eine Markenzelle erstellt. Wenn ein Benutzer das nächste Mal eine Anfrage für dieses Objekt sendet, wird ein Cache-Fehler bereitgestellt.
Reason Marker erstellt	Der Grund, warum eine Marker-Zelle erstellt wurde (z. B. “Warten auf Minhit”, “Antwortdaten für Inhaltslänge sind nicht im Gruppengrößenlimit”).
Jedes Mal automatische Umfrage	Wenn der integrierte Cache eine bereits abgelaufene 200-OK-Antwort mit Validatoren (entweder die Last-Modified- oder die `ETag` Antwort-Header) empfängt, speichert er die Antwort und markiert sie als Auto-PET (automatische Abfrage jedes Mal).
NetScaler Etag wurde als Antwort eingefügt	Eine Variante des `ETag` Headers, der von der NetScaler-Appliance generiert wird. Der Wert YES wird angezeigt, wenn der NetScaler eine `Etag` in die Antwort einfügt.
Vollständige Antwort im Cache vorhanden	Zeigt an, ob dies eine vollständige Antwort ist.
Ziel-IP von DNS verifiziert	Gibt an, ob beim Speichern des Objekts eine DNS-Auflösung durchgeführt wurde.
Objekt wird durch einen Cache-Forward-Proxy gespeichert	Gibt an, ob diese Antwort aufgrund eines Forward-Proxys gespeichert wurde, der im integrierten Cache konfiguriert ist.
Objekt ist ein Delta-Basisdatei	Eine Antwort, die delta-komprimiert ist.
Warten auf Minhits	Gibt an, ob diese Content-Gruppe eine Mindestanzahl von Original-Servern benötigt, die vor dem Zwischenspeichern einer Antwort getroffen werden.

Eigenschaften	Spezifikation
Minhit zählen	Wenn für diese Inhaltsgruppe eine Mindestanzahl von Treffern auf den Ursprungsserver erforderlich ist, bevor ein Objekt zwischengespeichert wird, wird in diesem Feld die Anzahl der bisher empfangenen Treffer angezeigt.
HTTP-Anforderungsmethode	Die Methode GET oder POST, die in der Anforderung verwendet wird, die dieses Objekt erhalten hat.
Gespeichert nach Richtlinie	Der Name der Caching-Richtlinie, die dazu geführt hat, dass dieses Objekt gespeichert wurde. Der Wert NICHT VERFÜGBAR gibt an, dass die Richtlinie deaktiviert oder gelöscht wurde. Der Wert NONE gibt an, dass das Objekt nicht mit einer sichtbaren Richtlinie übereinstimmte, sondern nach internen Kriterien für das Caching gespeichert wurde.
Metadaten der Anwendungs-Firewall vorhanden	Dieser Parameter wird verwendet, wenn die Anwendungs-Firewall und der integrierte Cache beide aktiviert sind. Die Anwendungs-Firewall analysiert den Inhalt einer Antwortseite, speichert ihre Metadaten (z. B. URLs und Formulare auf der Seite) und exportiert die Metadaten mit der Antwort in den Cache. Der Cache speichert die Seite und die Metadaten, und wenn der Cache die Seite bedient, sendet er die Metadaten zurück an die Sitzung der Anforderung.
HTTP-Callout-Objekt, Name, Typ, Antwort	Diese Zellen geben an, ob diese Daten als Ergebnis eines HTTP-Callout-Ausdrucks gespeichert wurden, und liefern Informationen über verschiedene Aspekte des Callouts und die entsprechende Antwort. Weitere Informationen zu HTTP-Callouts finden Sie unter “HTTP-Callouts”.

Finde bestimmte zwischengespeicherte Antworten

Sie können einzelne Elemente im Cache basierend auf Suchkriterien finden. Es gibt verschiedene Methoden, um zwischengespeicherte Elemente zu finden, je nachdem, ob die Content-Gruppe, die die Daten enthält, Treffer- und Invalidierungsselektoren verwendet, wie folgt:

Wenn die Content-Gruppe Selektoren verwendet, können Sie die Suche nur mit der Locator-ID für das zwischengespeicherte Element durchführen.

Wenn die Content-Gruppe keine Selektoren verwendet, führen Sie die Suche mit Kriterien wie URL, Host, Name der Inhaltsgruppe durch.

Wenn Sie nach einer zwischengespeicherten Antwort suchen, können Sie einige Elemente nach URL und Host suchen. Wenn sich die Antwort in einer Content-Gruppe befindet, die einen Selektor verwendet, können Sie sie nur mit einer Locator-Nummer (z. B. 0x00000000ad7af00000050) finden. Um eine Locator-Nummer zur späteren Verwendung zu speichern, klicken Sie mit der rechten Maustaste auf den Eintrag und wählen Sie Kopieren. Weitere Informationen zu Selektoren finden Sie unter “Konfigurieren von Selektoren und grundlegenden Inhaltsgruppen. “

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen an, die keinen Selektor haben, über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus<positive integer>] | -group <contentGroupName> |
-ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen mit einem Selektor über die Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:

```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

Um zwischengespeicherte Antworten in Inhaltsgruppen anzuzeigen, die keinen Selektor haben, mithilfe der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Cache-Objekte**, klicken Sie auf **Suchen**und legen Sie die Suchkriterien fest, um die erforderliche zwischengespeicherte Antwort anzuzeigen.

Wenn Sie noch keine Inhaltsgruppen konfiguriert haben, befinden sich alle Objekte in der Gruppe Standard.

Um zwischengespeicherte Antworten in Inhaltsgruppen anzuzeigen, die über einen Selektor verfügen, mithilfe der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Cache-Objekte**, klicken Sie auf **Suchen**und legen Sie die Auswahlkriterien fest, um die erforderliche zwischengespeicherte Antwort anzuzeigen.

Cache-Statistiken anzeigen

In der folgenden Tabelle sind die Cache-Statistiken zusammengefasst.

Zähler

Spezifikation

Cache-Statistiken anzeigen

Aktualisiert: 28.10.2013

In der folgenden Tabelle werden die detaillierten Cache-Statistiken zusammengefasst, die Sie anzeigen können.

Zähler	Spezifiziert
Treffer	Antworten, die im integrierten Cache gefunden und aus diesem bereitgestellt werden. Umfasst statische Objekte wie Bilddateien, Seiten mit den Statuscodes 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 und Antworten, die einer benutzerdefinierten Richtlinie mit einer CACHE-Aktion entsprechen.
Fehlschläge	Es wurden HTTP-Anfragen abgefangen, bei denen die Antwort letztendlich vom Ursprungsserver abgerufen wurde.
Anfragen	Gesamtzahl der Cache-Treffer plus Gesamtzahl der Cache-Fehler.
Nicht-304 Treffer	Wenn der Benutzer ein Element mehrmals anfordert und das Element im Cache seit dem letzten Servieren der NetScaler-Appliance unverändert ist, gibt die NetScaler-Appliance anstelle des zwischengespeicherten Objekts eine 304-Antwort an. Diese Statistik gibt an, wie viele Elemente die NetScaler-Appliance aus dem Cache bereitgestellt hat, mit Ausnahme von 304 Antworten.

Zähler	Spezifiziert
304 Treffer	Anzahl der 304 (Objekt nicht geändert) Antworten, die die NetScaler-Appliance aus dem Cache bereitgestellt hat.
304 Trefferquote (%)	Prozentsatz der 304 Antworten, die die NetScaler-Appliance beantwortet hat, im Vergleich zu anderen Antworten.
Trefferquote (%)	Prozentsatz der Antworten, die die NetScaler-Appliance aus dem Cache bereitgestellt hat (Cache-Treffer), im Verhältnis zu Antworten, die nicht aus dem Cache bereitgestellt werden konnten.
Eingesparte Origin-Bandbreite (%)	Eine Schätzung der Verarbeitungskapazität, die die NetScaler-Appliance aufgrund der Bereitstellung von Antworten aus dem Cache auf dem Originalserver gespeichert hat.
Vom NetScaler bereitgestellte Bytes	Gesamtzahl der Byte, die die NetScaler-Appliance vom Ursprungsserver und dem Cache bereitgestellt hat.
Vom Cache bereitgestellte Byte	Gesamtzahl der Byte, die die NetScaler-Appliance aus dem Cache bereitgestellt hat.
Byte-Treffrate (%)	Prozentsatz der Daten, die die NetScaler-Appliance aus dem Cache bereitgestellt hat, im Verhältnis zu allen Daten in allen bereitgestellten Antworten.
Komprimierte Bytes aus dem Cache	Datenmenge in Byte, die die NetScaler-Appliance in komprimierter Form bereitgestellt hat.
Speicherbare Fehlschläge	Wenn die NetScaler-Appliance ein angefordertes Objekt im Cache nicht findet, ruft sie das Objekt vom Originalserver ab. Dies wird als Cache-Miss bezeichnet. Ein speicherbarer Cachefehler kann im Cache gespeichert werden.

Zähler	Spezifiziert
Fehlschläge, die nicht gespeichert werden können	Ein nicht speicherbarer Cachefehler kann nicht im Cache gespeichert werden.
Fehlschläge	Alle Cache-Fehler.
Revalidierungen	Die Max-Age-Einstellung in einem Cache-Control-Header bestimmt in Sekunden, wann ein dazwischenliegender Cache den Inhalt mit dem integrierten Cache erneut validieren muss, bevor er dem Benutzer zur Verfügung gestellt wird. Weitere Informationen findest du unter „Einen Cache-Control-Header einfügen. „
Erfolgreiche Revalidierungen	Anzahl der durchgeführten Revalidierungen. Weitere Informationen findest du unter „Einen Cache-Control-Header einfügen. „
Konvertierungen in bedingte Req	Eine User-Agent-Anfrage für ein zwischengespeichertes PET-Objekt wird immer in eine bedingte Anfrage umgewandelt und an den Ursprungsserver gesendet. Weitere Informationen findest du unter „Jedes Mal, wenn eine Anfrage eingeht, den Origin Server abfragen. „
Speicherbare Fehlquote (%)	Fehler im speicherbaren Cache als Prozentsatz der nicht speicherbaren Cachefehler.
Erfolgsquote (%)	Erfolgreiche Revalidierungen als Prozentsatz aller Revalidierungsversuche. Weitere Informationen findest du unter „Einen Cache-Control-Header einfügen. „
Läuft beim letzten Byte ab	Häufigkeit, mit der der Inhalt des Caches unmittelbar nach dem Empfang des letzten Body-Bytes abgelaufen ist. Gilt nur für positive Antworten, wie in der Tabelle „Cache Hits and Misses“ beschrieben. „Weitere Informationen finden Sie unter „Beispiel für Leistungsoptimierung. „

Zähler	Spezifiziert
Flash-Cache fehlt	Wenn Sie Flash Cache aktivieren, erlaubt der Cache nur einer Anfrage, den Server zu erreichen, wodurch Flash-Gedränge vermieden werden. Diese Statistik gibt die Anzahl der Flash Cache-Anfragen an, die Cache-Fehler waren. Weitere Informationen finden Sie unter „Anfragen an den Cache einreihen. „
`Flashcache` Hits	Anzahl der Flash-Cache-Anfragen, bei denen es sich um Cache-Treffer handelte. Weitere Informationen findest du unter „Anfragen in den Cache einreihen“. „
Parametrisierte ungültige Anfragen	Anfragen, die einer Richtlinie mit einer Invalidierungsaktion (INVAL) und einer Inhaltsgruppe entsprechen, die einen Invalidierungsselektor oder Parameter verwendet, um zwischengespeicherte Objekte in der Gruppe selektiv ablaufen zu lassen.
Vollständige ungültige Anfragen	Anfragen, die einer Invalidierungsrichtlinie entsprechen, bei der der Parameter InvalGroups konfiguriert ist, und die eine oder mehrere Inhaltsgruppen ablaufen lassen.
Ungültige Anfragen	Anfragen, die einer Invalidierungsrichtlinie entsprechen und zum Ablauf bestimmter zwischengespeicherter Antworten oder ganzer Inhaltsgruppen führen.
Parametrisierte Anfragen	Anzahl der Cache-Anfragen, die mithilfe einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden.
Parametrisierte Treffer (ohne 304)	Anzahl der Cache-Anfragen, die mithilfe einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden, wobei eine vollständige zwischengespeicherte Antwort gefunden wurde und die Antwort keine 304-Antwort (Objekt nicht aktualisiert) war.

Zähler	Spezifiziert
304 Treffer parametrisiert	Anzahl der Cache-Anfragen, die mithilfe einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden, wobei das zwischengespeicherte Objekt gefunden wurde und das Objekt eine 304-Antwort (Objekt nicht aktualisiert) war.
Gesamtzahl der parametrisierten Treffer	Anzahl der Cache-Anfragen, die mithilfe einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden, in der das zwischengespeicherte Objekt gefunden wurde.
Parametrisierte 304-Trefferquote (%)	Prozentsatz der 304 Antworten (Objekt nicht aktualisiert), die mithilfe einer parametrisierten Richtlinie gefunden wurden, im Verhältnis zu allen Cache-Treffern.
Umfrage bei jeder Anfrage	Wenn Poll Every Time aktiviert ist, konsultiert die NetScaler-Appliance immer den Originalserver, bevor sie ein gespeichertes Objekt bereitstellt. Weitere Informationen findest du unter „Jedes Mal, wenn eine Anfrage eingeht, den Origin Server abfragen. „
Umfrage bei jedem Treffer	Häufigkeit, mit der ein Cache-Treffer mithilfe der Methode Poll Every Time gefunden wurde. Weitere Informationen findest du unter „Jedes Mal, wenn eine Anfrage eingeht, den Origin Server abfragen. „
Trefferquote bei jeder Umfrage (%)	Prozentsatz der Cache-Treffer, die die Methode „Jedes Mal abfragen“ verwendet haben, im Verhältnis zu allen Suchen nach zwischengespeicherten Objekten, bei denen „Jedes Mal abfragen“ verwendet wurde. Weitere Informationen findest du unter „Jedes Mal, wenn eine Anfrage eingeht, den Origin Server abfragen. „

Zähler	Spezifiziert
Maximaler Speicher (KB)	Maximale Speichermenge in der NetScaler-Appliance, die dem Cache zugewiesen ist. Weitere Informationen finden Sie unter “Globale Attribute für das Caching konfigurieren.”
Maximaler aktiver Speicherwert (KB)	Maximale Speichermenge (aktiver Wert), die festgelegt wird, nachdem der Speicher dem Cache tatsächlich zugewiesen wurde. Weitere Informationen finden Sie unter „So konfigurieren Sie die integrierte Caching-Funktion einer NetScaler Appliance für verschiedene Szenarien. „
Belegter Speicher (KB)	Menge an Speicher, der tatsächlich verwendet wird.
Fehler bei der Speicherzuweisung	Anzahl der fehlgeschlagenen Versuche, Speicher zu nutzen, um eine Antwort im Cache zu speichern.
Bisher größte Resonanz	Größte Antwort in Byte, die entweder im Cache oder auf dem Ursprungsserver gefunden und an den Client gesendet wurde.
Zwischengespeicherte Objekte	Anzahl der Objekte im Cache, einschließlich Antworten, die noch nicht vollständig heruntergeladen wurden, und Antworten, die abgelaufen, aber noch nicht geleert wurden.
Objekte markieren	Markierungsobjekte werden erstellt, wenn eine Antwort die maximale oder minimale Antwortgröße für die Inhaltsgruppe überschreitet oder noch nicht die Mindestanzahl von Treffern für die Inhaltsgruppe erhalten hat.
Treffer werden serviert	Anzahl der Treffer, die aus dem Cache bereitgestellt wurden.

Zähler	Spezifiziert
Fehlschläge werden behandelt	Antworten, die vom Ursprungsserver abgerufen, im Cache gespeichert und dann bereitgestellt wurden. Sollte die Zahl für speicherbare Fehlschläge annähern. Nicht speicherbare Fehlschläge sind nicht enthalten.

So können Sie sich mithilfe der Befehlszeilenschnittstelle zusammenfassende Cache-Statistiken anzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat cache
```

Um bestimmte Cache-Statistiken mithilfe der Befehlszeilenschnittstelle anzuzeigen

Geben Sie in der Befehlszeile Folgendes ein:

```
stat cache -detail

    > stat cache -detail
    Integrated Cache Statistics - Detail
    Integrated Cache Statistics - Summary
                                                Rate (/s)
                                                   Total
    Hits                                              0
                           0
    Misses                                            0
                           0
    Requests                                          0
                           0
    Hit ratio(%)                                     --
                           0
    Origin bandwidth saved(%)                        --
                           0
    Cached objects                                   --
                           0
    Marker objects                                   --
                           0
                                                Rate (/s)
                                                   Total
    Requests                                          0
                           0
    Hit Statistics
```



```
17                                                  Rate (/s)
                                                       Total
18      Non-304 hits                                        0
                             0
19      304 hits                                            0
                             0
20      Sql hits                                            0
                             0
21      Hits                                                0
                             0
22      304 hit ratio(%)                                   --
                             0
23      Hit ratio(%)                                       --
                             0
24      Origin bandwidth saved(%)                          --
                             0
25
26      Byte Statistics
27                                                  Rate (/s)
                                                       Total
28      Bytes served by NetScaler                         648
           55379204
29      Bytes served by cache                               0
                             0
30      Byte hit ratio(%)                                  --
                             0
31      Compressed bytes from cache                         0
                             0
32      Miss Statistics
33                                                  Rate (/s)
                                                       Total
34      Storable misses                                     0
                             0
35      Non-storable misses                                 0
                             0
36      Misses                                              0
                             0
37      Revalidations                                       0
                             0
38      Successful revalidations                            0
                             0
39      Conversions to conditional req                      0
                             0
40      Storable miss ratio(%)                             --
                             0
```



```
41      Successful reval ratio(%)                                --
                            0
42      Flashcache Statistics
43                                                  Rate (/s)
                                                       Total
44      Expire at last byte                                   0
                            0
45      Flashcache misses                                     0
                            0
46      Flashcache hits                                       0
                            0
47
48      Invalidation Statistics
49                                                  Rate (/s)
                                                       Total
50      Parameterized inval requests                          0
                            0
51      Full inval requests                                   0
                            0
52      Inval requests                                        0
                            0
53
54      Parameterized Caching Statistics
55                                                  Rate (/s)
                                                       Total
56      Parameterized requests                                0
                            0
57      Parameterized non-304 hits                            0
                            0
58      Parameterized 304 hits                                0
                            0
59      Total parameterized hits                              0
                            0
60      Parameterized 304 hit ratio(%)                        --
                            0
61
62      Poll Every Time (PET) Statistics
63                                                  Rate (/s)
                                                       Total
64      Poll every time requests                              0
                            0
65      Poll every time hits                                  0
                            0
66      Poll every time hit ratio(%)                          --
                            0
```



```
67      Memory Usage Statistics
68                                                      Total
69      Maximum memory(KB)                                   0
70      Maximum memory active value(KB)                      0
71      Utilized memory(KB)                                  0
72      Memory allocation failures                           0
73      Largest response so far(B)                           0
74      Cached objects                                       0
75      Marker objects                                       0
76      Hits being served                                    0
77      Misses being handled                                 0
78       Done
79  <!--NeedCopy-->
```

So zeigen Sie Zusammenfassungs-Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte **Dashboard**.
2. Scrollen Sie nach unten zum Abschnitt Integriertes Caching des Fensters.
3. Um detaillierte Statistiken anzuzeigen, klicken Sie unten in der Tabelle auf den Link Mehr…

So zeigen Sie bestimmte Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte Reporting .
2. Erweitern Sie unter Integrierte Berichte den Eintrag Integrierter Cache, und klicken Sie dann auf den Bericht mit den Statistiken, die Sie anzeigen möchten.
3. Um den Bericht als Vorlage zu speichern, klicken Sie auf Speichern unter und benennen Sie den Bericht. Der gespeicherte Bericht wird unter Benutzerdefinierte Berichte angezeigt.

Verbesserung der Cache-Leistung

May 11, 2023

Sie können die Leistung des integrierten Caches verbessern, indem Sie unter anderem gleichzeitige Anfragen für dieselben zwischengespeicherten Daten verarbeiten, Verzögerungen vermeiden, die mit der Aktualisierung zwischengespeicherter Antworten vom Ursprungsserver verbunden sind, und sicherstellen, dass eine Antwort oft genug angefordert wird, dass es sich lohnt, zwischengespeichert zu werden.

Reduzieren Sie Besucherandrang

Flash-Crowds entstehen, wenn viele Benutzer gleichzeitig dieselben Daten anfordern. Die Anfragen in einer Flash-Crowd können zu Cache-Fehlschlägen werden, wenn Sie den Cache so konfiguriert haben, dass Treffer erst dann bereitgestellt werden, wenn das gesamte Objekt heruntergeladen wurde.

Mit den folgenden Techniken können Sie Menschenansammlungen reduzieren oder verhindern:

- **PREFETCH**: Aktualisiert eine positive Antwort, bevor sie abläuft, um sicherzustellen, dass sie niemals veraltet oder inaktiv wird. Weitere Informationen finden Sie im Abschnitt „Eine Antwort vor Ablauf aktualisieren“.
- **Cache-Pufferung**: Beginnt mit der Bereitstellung einer Antwort an mehrere Clients, wenn der Response-Header vom Originalserver empfangen wird, anstatt darauf zu warten, dass die gesamte Antwort heruntergeladen wird. Die einzige Grenze für die Anzahl der Clients, die eine Antwort gleichzeitig herunterladen können, sind die verfügbaren Systemressourcen. Die NetScaler-Appliance lädt herunter und liefert Antworten, auch wenn der Client, der den Download initiiert hat, angehalten wird, bevor der Download abgeschlossen ist. Wenn die Antwort die Cachegröße überschreitet oder wenn die Antwort aufgeteilt wird, speichert der Cache die Antwort nicht mehr, der Service für die Clients wird jedoch nicht unterbrochen.
- **Flash-Cache:** Flash Cache stellt Anfragen an den Cache in die Warteschlange und lässt zu, dass jeweils nur eine Anfrage den Server erreicht.

Weitere Informationen finden Sie im Abschnitt „Anfragen in den Cache einreihen“.

Eine Antwort vor Ablauf aktualisieren

Um sicherzustellen, dass eine zwischengespeicherte Antwort immer dann aktuell ist, wenn sie benötigt wird, aktualisiert die PREFETCH-Option eine Antwort vor ihrer berechneten Ablaufzeit. Das Prefetch-Intervall wird nach Empfang der ersten Client-Anfrage berechnet. Ab diesem Zeitpunkt aktualisiert die NetScaler-Appliance die zwischengespeicherte Antwort in einem Zeitintervall, das Sie im PREFETCH-Parameter konfigurieren.

Diese Einstellung ist nützlich für Daten, die zwischen Anfragen häufig aktualisiert werden. Sie gilt nicht für negative Antworten (z. B. 404-Nachrichten).

So konfigurieren Sie Prefetch für eine Inhaltsgruppe mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <name> -prefetch YES [-prefetchPeriod <seconds> | -
prefetchPeriodMilliSec <milliseconds>] [-prefetchMaxPending <positiveInteger
>]
```

*Um Prefetch für eine Inhaltsgruppe mithilfe der GUI zu konfigurieren

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**und wählen Sie die **Inhaltsgruppe**aus.

Wählen Sie auf der Registerkarte **Andere** in der Gruppe Flash Crowd und Prefetch die Option **Prefetch** aus und geben Sie die Werte in den Textfeldern Intervall und Maximale Anzahl ausstehender Prefetches an.

Anfragen in den Cache einreihen

Die Flash-Cache-Option stellt gleichzeitig eingehende Anfragen in die Warteschlange (eine Flash-Crowd), ruft die Antwort ab und verteilt sie an alle Clients, deren Anfragen sich in der Warteschlange befinden. Wenn die Antwort während dieses Vorgangs nicht mehr zwischenspeicherbar ist, stellt die NetScaler-Appliance die Antwort aus dem Cache ein und übermittelt stattdessen die Antwort des Originalservers an die Clients in der Warteschlange. Wenn die Antwort nicht verfügbar ist, erhalten die Clients eine Fehlermeldung.

Flash Cache ist standardmäßig deaktiviert. Sie können Poll Every Time (PET) und Flash Cache nicht für dieselbe Inhaltsgruppe aktivieren.

Ein Nachteil von Flash Cache besteht darin, dass, wenn der Server mit einem Fehler antwortet (z. B. ein 404, der schnell behoben wird), der Fehler an die wartenden Clients weitergeleitet wird.

> **Hinweis**:
> Wenn Flash Cache aktiviert ist, kann die NetScaler-Appliance in einigen Situationen den Accept-Encoding-Header in der Client-Anfrage nicht korrekt mit dem Content-Encoding-Header in der Antwort abgleichen. Die NetScaler-Appliance kann davon ausgehen, dass diese Header übereinstimmen und fälschlicherweise einen Treffer ausliefern. Um dieses Problem zu umgehen, können Sie integrierte Caching-Richtlinien so konfigurieren, dass Zugriffe nicht an Clients weitergeleitet werden, die nicht über einen geeigneten Accept-Encoding-Header verfügen.

So aktivieren Sie Flash Cache mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <contentGroupName> -flashcache yes
```

So aktivieren Sie Flash Cache mithilfe der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**und wählen Sie die Inhaltsgruppe aus.

Wählen Sie auf der Registerkarte **Andere** in der Gruppe Flash Crowd and Prefetch die Option **Prefetch** aus.

Eine Antwort zwischenspeichern, nachdem ein Client einen Download angehalten hat

Sie können den Quick Abort-Parameter so festlegen, dass eine Antwort weiterhin zwischengespeichert wird, auch wenn der Client eine Anfrage stoppt, bevor sich die Antwort im Cache befindet.

Wenn die Größe der heruntergeladenen Antwort kleiner oder gleich der Quick Abort-Größe ist, stoppt die NetScaler-Appliance das Herunterladen der Antwort. Wenn Sie den Parameter Quick Abort auf 0 setzen, werden alle Downloads angehalten.

So konfigurieren Sie die Größe für einen schnellen Abbruch mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <name> -quickAbortSize <integerInKBytes>
```

So konfigurieren Sie die Größe für einen schnellen Abbruch mithilfe der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**und wählen Sie die Inhaltsgruppe aus.
2. Stellen Sie auf der Registerkarte **Speicher** den entsprechenden Wert im Feld Schnellabbruch: Caching fortsetzen, falls mehr als das Textfeld ist.

Vor dem Caching ist eine Mindestanzahl von Serverzugriffen erforderlich

Sie können konfigurieren, wie oft eine Antwort mindestens auf dem Ursprungsserver gefunden werden muss, bevor sie zwischengespeichert werden kann. Sie müssen erwägen, die Mindestanzahl an Treffern zu erhöhen, wenn der Cache-Speicher schnell voll wird und die Trefferquote niedriger als erwartet ist.

Der Standardwert für die Mindestanzahl von Treffern ist 0. Dieser Wert speichert die Antwort nach der ersten Anfrage im Cache.

So konfigurieren Sie die Mindestanzahl von Treffern, die vor dem Zwischenspeichern erforderlich sind, mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <name> -minhits <positiveInteger>
```

So konfigurieren Sie die Mindestanzahl von Treffern, die vor dem Zwischenspeichern erforderlich sind, mithilfe der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**und wählen Sie die Inhaltsgruppe aus.
2. Stellen Sie auf der Registerkarte **Speicher** den entsprechenden Wert unter Nicht zwischenspeichern ein, wenn die Treffer kleiner als das Textfeld sind.

Beispiel für Leistungsoptimierung

In diesem Beispiel greift ein Kunde auf einen Aktienkurs zu. Aktienkurse sind hochdynamisch. Sie konfigurieren den integrierten Cache so, dass derselbe Aktienkurs für gleichzeitige Kunden bereitgestellt wird, ohne mehrere Anfragen an den Ursprungsserver zu senden. Der Aktienkurs läuft ab, nachdem er auf die Clients heruntergeladen wurde, und die nächste Anfrage wird vom Ursprungsserver abgerufen. Dadurch wird sichergestellt, dass das Angebot immer auf dem neuesten Stand ist.

In der folgenden Aufgabenübersicht werden die Schritte zur Konfiguration des Caches für die Aktienkursanwendung beschrieben.

Caching für eine Aktienkursanwendung konfigurieren

Erstellen Sie eine Inhaltsgruppe für Aktienkurse

Weitere Informationen findest du unter „Über Inhaltsgruppen. „

Konfigurieren Sie für diese Inhaltsgruppe Folgendes:

1. Aktivieren Sie auf der Registerkarte **Ablaufmethode** das Kontrollkästchen Nach Erhalt der vollständigen Antwort ablaufen.
2. Aktivieren Sie auf der Registerkarte **Andere** das Kontrollkästchen **Flash Cache** und klicken Sie auf **Erstellen**.
3. Fügen Sie eine Cache-Richtlinie hinzu, um die Aktienkurse zwischenzuspeichern.

Weitere Informationen finden Sie unter “Konfigurieren einer Richtlinie im integrierten Cache. “

Konfigurieren Sie Folgendes für die Richtlinie

1. Wählen Sie in den **Listen Aktion und In Gruppe speichern**die Option **CACHE** aus und wählen Sie die Gruppe aus, die Sie im vorherigen Schritt definiert haben.
2. Klicken Sie auf **Hinzufügen**und konfigurieren Sie im Dialogfeld **Ausdruck hinzufügen einen Ausdruck**, der Aktienkursanfragen identifiziert, zum Beispiel: http.req.url.contains („cgi-bin/stock-quote.pl“)
3. Aktivieren Sie die Richtlinie.

Weitere Informationen findest du unter „Eine integrierte Caching-Richtlinie weltweit verbindlich. „ In diesem Beispiel binden Sie diese Richtlinie an die Verarbeitung von Anforderungszeitüberschreibungen und legen die Priorität auf einen niedrigen Wert fest.

Cookies, Header und Polling konfigurieren

May 11, 2023

In diesem Thema wird erläutert, wie die Cache-Verwaltung von Cookies, HTTP-Headern und Original-Serverabfragen konfiguriert wird. Dazu gehört das Ändern des Standardverhaltens, das dazu führt, dass der Cache von dokumentierten Standards abweicht, das Überschreiben von HTTP-Headern, die dazu führen könnten, dass cachbarer Inhalt nicht im Cache gespeichert wird, und das Konfigurieren des Caches, dass immer der Ursprung nach aktualisierten Inhalten abgefragt wird.

Abweichung des Cache-Verhaltens von den Standards

Standardmäßig entspricht der integrierte Cache den folgenden RFC-Standards:

- RFC 2616, “HTTP HTTP/1.1”

- Das in RFC 2617, “HTTP-Authentifizierung: Basic and Digest Access Authentication” beschriebene Caching-Verhalten
- Das in RFC 2965, “HTTP State Management Mechanism” beschriebene Caching-Verhalten

Die integrierten Richtlinien und die Attribute der Standard-Inhaltsgruppe gewährleisten die Konformität mit den meisten dieser Standards.

Das standardmäßige integrierte Cache-Verhalten weicht wie folgt von der Spezifikation ab:

- Es gibt eine begrenzte Unterstützung für den Vari-Header. Standardmäßig wird jede Antwort, die einen Vari-Header enthält, als nicht cachbar angesehen, sofern sie nicht komprimiert ist. Eine komprimierte Antwort enthält Inhaltscodierung: gzip, Inhaltscodierung: deflate oder Inhaltscodierung: pack200-gzip und ist auch dann cachbar, wenn sie den Header Vary: Accept-Codierung enthält.
- Der integrierte Cache ignoriert die Werte der Header-Cache-Steuerung: kein Cache und Cache-Kontrolle: privat. Zum Beispiel wird eine Antwort, die Cache-Kontrolle enthält: NO-Cache=”set-Cookie” behandelt, als ob die Antwort Cache-Control: no-cache enthielt. Standardmäßig wird die Antwort nicht zwischengespeichert.
- Ein Bild (Content-Typ = image/*) wird immer als cachbar betrachtet, auch wenn eine Bild-Antwort Set-Cookie- oder set-cookie2-Header enthält oder wenn eine Bildanforderung einen Cookie-Header enthält. Der integrierte Cache entfernt Set-Cookie- und set-cookie2-Header aus einer Antwort, bevor er zwischengespeichert wird. Dies weicht von RFC 2965 ab. Sie können RFC-konformes Verhalten wie folgt konfigurieren:

```
1 add cache policy rfc_compliant_images_policy -rule "http.res.header.set
     -cookie2.exists || http.res.header.set-cookie.exists" -action
     NOCACHE
2
3
4 bind cache global rfc_compliant_images_policy -priority 100 -type
     REQ_OVERRIDE
5 <!--NeedCopy-->
```

- Die folgenden Cache-Control-Header in einer Anforderung erzwingen einen RFC-kompatiblen Cache, eine zwischengespeicherte Antwort vom Original-Server neu zu laden:

```
Cache-control: max-age=0
```

```
Cache-control: no-cache
```

Zum Schutz vor Denial-of-Service-Angriffen ist dieses Verhalten nicht die Standardeinstellung.

- Standardmäßig betrachtet das Caching-Modul eine Antwort als cachbar, sofern nicht anders ein Response-Header-Status vorliegt. Um dieses Verhalten mit RFC 2616 konform zu machen, setzen Sie `-weakPosRelExpiry` und `-weakNegResExpiry` für alle Inhaltsgruppen auf 0.

Cookies aus einer Antwort entfernen

Cookies sind oft für einen Benutzer personalisiert und sollten in der Regel nicht zwischengespeichert werden. Der Parameter `Remove Response Cookies` entfernt die Header `Set-Cookie and Set-Cookie2`, bevor eine Antwort zwischenspeichert wird. Standardmäßig verhindert die Option `Remove Response Cookies` für eine Content-Gruppe das Zwischenspeichern von Antworten mit den Headern `Set-Cookie` oder `Set-Cookie2`.

> **Hinweis:**
> Wenn Bilder zwischengespeichert werden, besteht das integrierte Verhalten darin, die Header `Set-Cookie` und `Set-Cookie2` vor dem Zwischenspeichern zu entfernen, unabhängig davon, wie die Content-Gruppe konfiguriert ist.
>
> Citrix empfiehlt, dass Sie den Standard `Remove Response Cookies` für jede Content-Gruppe akzeptieren, die eingebettete Antworten speichert, z. B. Bilder.

Konfigurieren von `Remove Response Cookies` für eine Content-Gruppe über die Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <name> -removeCookies YES
```

Konfigurieren von Response-Cookies für eine Inhaltsgruppe mithilfe der NetScaler GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**und wählen Sie die Inhaltsgruppe aus.
2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe **Einstellungen** die Option Response-Cookies entfernen aus.

Einfügen von HTTP-Headern zur Reaktionszeit

Der integrierte Cache kann HTTP-Header in Antworten einfügen, die sich aus Cache-Anforderungen ergeben. Die NetScaler Appliance ändert keine Header in Antworten, die aus Cache-Fehlern resultieren.

In der folgenden Tabelle werden Kopfzeilen beschrieben, die Sie in eine Antwort einfügen können.

Header	Spezifikation
Alter	Gibt das Alter der Antwort in Sekunden an, berechnet aus dem Zeitpunkt, zu dem die Antwort auf dem Original-Server generiert wurde. Standardmäßig fügt der Cache einen Age-Header für jede Antwort ein, die aus dem Cache bereitgestellt wird.
via	Listet Protokolle und Empfänger zwischen den Start- und Endpunkten für eine Anfrage oder eine Antwort auf. Die NetScaler Appliance fügt in jede Antwort, die sie aus dem Cache liefert, einen Via-Header ein. Der Standardwert des eingefügten Headers ist `NS-CACHE-10.0`: letztes Oktett der NetScaler IP-Adresse. Weitere Informationen finden Sie unter “Globale Attribute für das Caching konfigurieren.”

Header	Spezifikation
Tag	Der Cache unterstützt die Response-Validierung mit Last-Modified und Tag Headern, um festzustellen, ob eine Antwort veraltet ist. Der Cache fügt nur dann eine Tag in eine Antwort ein, wenn er die Antwort zwischenspeichert und der Original-Server keinen eigenen Tag Header eingefügt hat. Der Tag Wert ist eine beliebige eindeutige Zahl. Der Tag Wert für eine Antwort ändert sich, wenn sie vom Original-Server aktualisiert wird, aber er bleibt unverändert, wenn der Server eine 304-Antwort (Objekt nicht aktualisiert) sendet. Original-Server generieren normalerweise keine Validatoren für dynamischen Inhalt, da dynamischer Inhalt als nicht cachbar angesehen wird. Sie können dieses Verhalten außer Kraft setzen. Beim Einfügen von Tag Header darf der Cache keine vollständigen Antworten liefern. Stattdessen muss der Benutzeragent die dynamische Antwort, die vom integrierten Cache zum ersten Mal gesendet wurde, zwischenspeichern. Um einen Benutzeragenten zum Zwischenspeichern einer Antwort zu zwingen, konfigurieren Sie den integrierten Cache so, dass er einen Tag Header einfügt und den vom Ursprung bereitgestellten Cache-Control-Header ersetzt.

Header	Spezifikation
Cache-Steuerung	Die NetScaler Appliance ändert normalerweise keine Header zur Cachefähigkeit in Antworten, die vom Original-Server aus bereitgestellt werden. Wenn der Original-Server eine Antwort sendet, die als nicht cachbar gekennzeichnet ist, behandelt der Client die Antwort als nicht cachbar, auch wenn die NetScaler Appliance die Antwort im Cache speichert. Um dynamische Antworten in einem Benutzeragenten zwischenzuspeichern, können Sie Cache-Control-Header vom Original-Server ersetzen. Dies gilt nur für Benutzeragenten und andere dazwischenliegende Caches. Sie haben keinen Einfluss auf den integrierten Cache.

Header	Spezifikation
Alter	Gibt das Alter der Antwort in Sekunden an, berechnet aus dem Zeitpunkt, zu dem die Antwort auf dem Original-Server generiert wurde. Standardmäßig fügt der Cache einen Age-Header für jede Antwort ein, die aus dem Cache bereitgestellt wird.
via	Listet Protokolle und Empfänger zwischen den Start- und Endpunkten für eine Anfrage oder eine Antwort auf. Die NetScaler Appliance fügt in jede Antwort, die sie aus dem Cache liefert, einen Via-Header ein. Der Standardwert des eingefügten Headers ist “NS-CACHE-9.2: letztes Oktett der NetScaler-IP-Adresse”. Weitere Informationen finden Sie unter “Globale Attribute für das Caching konfigurieren.”

Header	Spezifikation
Tag	Der Cache unterstützt die Antwortvalidierung mithilfe der Header “Letzte Änderung” und “Tag”, um festzustellen, ob eine Antwort veraltet ist. Der Cache fügt nur dann eine Tag in eine Antwort ein, wenn er die Antwort zwischenspeichert und der Original-Server keinen eigenen Tag Header eingefügt hat. Der Tag Wert ist eine beliebige eindeutige Zahl. Der Tag Wert für eine Antwort ändert sich, wenn sie vom Original-Server aktualisiert wird, aber er bleibt unverändert, wenn der Server eine 304-Antwort (Objekt nicht aktualisiert) sendet. Original-Server generieren normalerweise keine Validatoren für dynamischen Inhalt, da dynamischer Inhalt als nicht cachbar angesehen wird. Sie können dieses Verhalten außer Kraft setzen. Beim Einfügen von Tag Header darf der Cache keine vollständigen Antworten liefern. Stattdessen muss der Benutzeragent die dynamische Antwort, die vom integrierten Cache zum ersten Mal gesendet wurde, zwischenspeichern. Um einen Benutzeragenten zum Zwischenspeichern einer Antwort zu zwingen, konfigurieren Sie den integrierten Cache so, dass er einen Tag Header einfügt und den vom Ursprung bereitgestellten Cache-Control-Header ersetzt.

Header	Spezifikation
Cache-Steuerung	Die NetScaler Appliance ändert normalerweise keine Header zur Cachefähigkeit in Antworten, die vom Original-Server aus bereitgestellt werden. Wenn der Original-Server eine Antwort sendet, die als nicht cachbar gekennzeichnet ist, behandelt der Client die Antwort als nicht cachbar, auch wenn die NetScaler Appliance die Antwort im Cache speichert. Um dynamische Antworten in einem Benutzeragenten zwischenzuspeichern, können Sie Cache-Control-Header vom Original-Server ersetzen. Dies gilt nur für Benutzeragenten und andere dazwischenliegende Caches. Sie haben keinen Einfluss auf den integrierten Cache.

Fügen Sie einen Alter-, via- oder Tag-Header ein

In den folgenden Verfahren wird beschrieben, wie Age-, Via- und ETag-Header eingefügt werden.

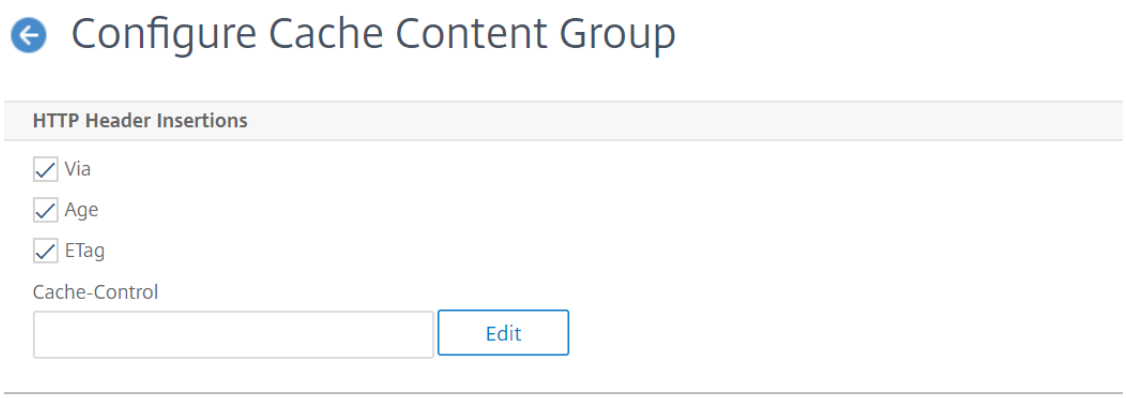
Fügen Sie mithilfe der NetScaler-Befehlsschnittstelle einen Age-, Via- oder ETAG-Headerein:

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <name> -insertVia YES -insertAge YES -insertETag YES
```

Konfigurieren Sie den Age-, Via- oder ETAG-Header mithilfe der NetScaler GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen** und wählen Sie die **Inhaltsgruppe**aus.
2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe HTTP-Header-Einfügungen nach Bedarf die Optionen **Via**, **Age**oder **ETag** aus.
3. Die Werte für die anderen Kopfzeilentypen werden automatisch berechnet. Den Via-Wert konfigurieren Sie in den Haupteinstellungen für den Cache.



Fügen Sie einen Cache-Control-Header ein

Wenn der integrierte Cache einen vom Originalserver eingefügten Cache-Control-Header ersetzt, ersetzt er auch den Expires-Header. Der neue Expires-Header enthält eine Ablaufzeit in der Vergangenheit. Dadurch wird sichergestellt, dass HTTP/1.0-Clients und -Caches (die den Cache-Control-Header nicht verstehen) den Inhalt nicht zwischenspeichern.

Fügen Sie mithilfe der NetScaler Befehlszeilenschnittstelle einen Cache-Control-Header ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <name> -cacheControl <value>
```

Fügen Sie einen Cache-Control-Header mithilfe der NetScaler GUI ein

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Content-Gruppen**und
   a) Klicken Sie auf die Registerkarte **Ablaufmethode**, löschen Sie die Heuristik und die standardmäßigen Ablaufeinstellungen und legen Sie den entsprechenden Wert im Textfeld Inhalt ablaufen nach fest.
   b) Klicken Sie auf die Registerkarte **Andere** und geben Sie den Header, den Sie einfügen möchten, in das Textfeld Cache-Control ein. Klicken Sie alternativ auf Konfigurieren, um die Cache-Control-Direktiven in zwischengespeicherten Antworten festzulegen.

Ignoriere Cache-Kontrolle und Pragma-Header in Anfragen

Standardmäßig verarbeitet das Caching-Modul Cache-Control- und Pragma-Header. Die folgenden Token in den Cache-Control-Headern werden wie in RFC 2616 beschrieben verarbeitet.

- max-age
- max-abgestanden
- nur-wenn-zwischengespeichert

- kein Cache

Ein Pragma: No-Cache-Header in einer Anforderung wird genauso behandelt wie ein Cache-Control: No-Cache-Header.

Wenn Sie das Caching-Modul so konfigurieren, dass es die Header Cache-Control und Pragma ignoriert, veranlasst eine Anforderung, die einen Cache-Control: No-Cache-Header enthält, die NetScaler Appliance, die Antwort vom Original-Server abzurufen, aber die zwischengespeicherte Antwort wird nicht aktualisiert. Wenn das Caching-Modul die Header Cache-Control und Pragma verarbeitet, wird die zwischengespeicherte Antwort aktualisiert.

In der folgenden Tabelle sind die Auswirkungen verschiedener Einstellungen für diese Header und die Einstellung Neuladeanforderung des Browsers ignorieren zusammengefasst.

Einstellung für Ignorieren-Cache-Control und Pragma-Header	**Einstellung für Neuladeanfrage des Browsers ignorieren**	**Ergebnis**
Ja	Ja oder Nein	Ignorieren Sie die Cache-Control- und Pragma-Header des Clients, einschließlich der Cache-Control: no-Cache-Direktive.
Nein	Ja	Der Cache-Control: No-Cache-Header erzeugt einen Cache-Fehlschuss, aber eine Antwort, die sich bereits im Cache befindet, wird nicht aktualisiert.
Nein	Nein	Eine Anforderung, die einen Cache-Control: No-Cache-Header enthält, verursacht einen Cache-Fehlschlag und die gespeicherte Antwort wird aktualisiert.

So ignorieren Sie Cache-Control- und Pragma-Header in einer Anforderung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
set cache contentgroup <name> -ignoreReqCachingHdrs YES
```

So ignorieren Sie Anfragen zum Neuladen von Browsern mithilfe der Befehlszeilenschnittstelle

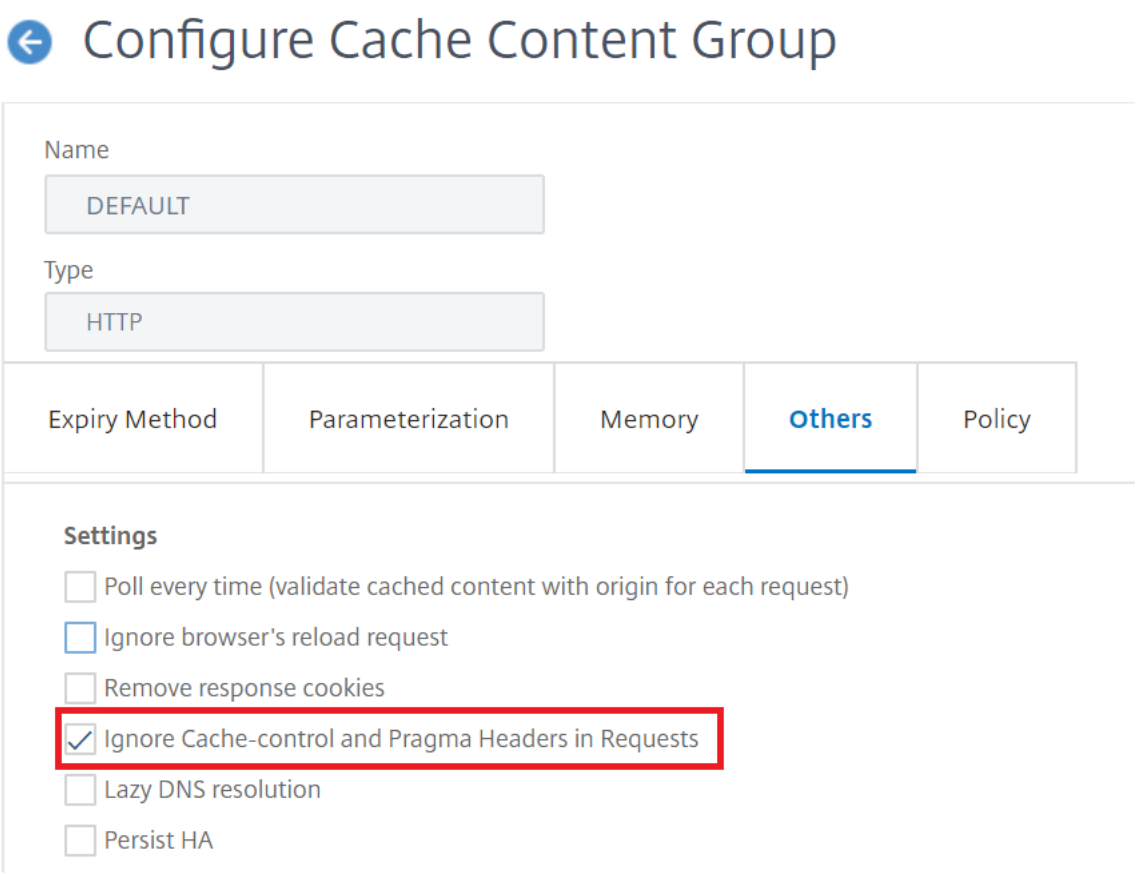
Geben Sie in der Befehlszeile Folgendes ein:

```
set cache contentgroup <name> -ignoreReloadReq NO
```

> **Hinweis:**
> Standardmäßig ist der Parameter -IgnoreReloadReq auf YES festgelegt.

Ignorieren Sie Cache-Control- und Pragma-Header in einer Anfrage mithilfe der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**und wählen Sie die Inhaltsgruppe aus.
2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe **Einstellungen** die Option **Cache-Control und Pragma-Header ignorieren** in der Option **Anfragen** aus.



Beispiel für eine Richtlinie zum Ignorieren von Cache-Control-Headern:

Im folgenden Beispiel konfigurieren Sie eine Richtlinie zum Überschreiben der Anforderungszeit, um Antworten zu cachen, die Content-Typ enthalten: image/* unabhängig vom Cache-Control-Header in der Antwort.

Konfigurieren einer Richtlinie zum Überschreiben der Anforderungszeit, um alle Antworten mit image/* zu cachen

Leeren Sie den Cache mit der Option Alle ungültig machen.

Konfigurieren Sie eine neue Cache-Richtlinie und leiten Sie die Richtlinie an eine bestimmte Content-Gruppe weiter. Weitere Informationen finden Sie unter “Konfigurieren einer Richtlinie im integrierten Cache. “

Stellen Sie sicher, dass die von der Richtlinie verwendete Content-Gruppe so konfiguriert ist, dass sie Cache-Control-Header ignoriert, wie in “Cache-Control und Pragma-Header in Requests ignorieren” beschrieben ist.

Binden Sie die Richtlinie an die Richtlinienbank für die Anforderungszeitüberschreibung.

Weitere Informationen finden Sie unter Global Binden einer integrierten Caching-Richtlinie .

Poll-Original-Server jedes Mal, wenn eine Anfrage empfangen wird

Sie können die NetScaler Appliance so konfigurieren, dass sie immer den Original-Server konsultiert, bevor eine gespeicherte Antwort gesendet wird. Dies ist bekannt als Poll Every Time (PET). Wenn die NetScaler Appliance den Original-Server konsultiert und die PET-Antwort nicht abgelaufen ist, überschreibt eine vollständige Antwort des Original-Servers den zwischengespeicherten Inhalt nicht. Diese Eigenschaft ist nützlich, wenn Sie kundenspezifische Inhalte bereitstellen.

Nachdem eine PET-Antwort abgelaufen ist, aktualisiert die NetScaler Appliance sie, wenn die erste vollständige Antwort vom Original-Server eingeht.

Die Funktion “Poll Every Time” (PET) funktioniert wie folgt:

Bei einer zwischengespeicherten Antwort, die Validatoren in Form eines Tags oder eines Headers für die letzte Änderung enthält, wird die Antwort automatisch als PET gekennzeichnet und zwischengespeichert, wenn sie abläuft.

Sie können PET für eine Content-Gruppe konfigurieren.

Wenn Sie eine Content-Gruppe als PET konfigurieren, wird jede Antwort in der Content-Gruppe als PET gekennzeichnet. Die PET-Inhaltsgruppe kann Antworten speichern, die keine Validatoren haben. Antworten, die automatisch als PET gekennzeichnet sind, sind immer abgelaufen. Antworten, die zu einer PET-Inhaltsgruppe gehören, können nach einer Verzögerung ablaufen, je nachdem, wie Sie die Content-Gruppe konfigurieren.

Zwei Arten von Anfragen sind von Abfragen betroffen:

- Bedingte Anfragen: Ein Kunde stellt eine bedingte Anfrage aus, um sicherzustellen, dass die Antwort, die er hat, die neueste Kopie ist. Eine User-Agent-Anfrage für eine zwischengespeicherte PET-Antwort wird immer in eine bedingte Anforderung umgewandelt und an den

Original-Server gesendet. Eine bedingte Anforderung hat Validatoren in den `If-None-Match` Kopfzeilen `If-Modified-Since` oder. Der `If-Modified-Since` Header enthält die Zeit aus dem `Last-Modified` Header. Ein If-None-Match-Header enthält den Tag-Header-Wert der Antwort. Wenn die Kopie der Antwort des Clients neu ist, antwortet der Original-Server mit 304 Not Modified. Wenn die Kopie veraltet ist, generiert eine bedingte Antwort ein 200 OK, das die gesamte Antwort enthält.

- Unbedingte Anfragen: Eine bedingungslose Anforderung kann nur 200 OK generieren, die die gesamte Antwort enthält.

Antwort des Original-Servers	Aktion
Sende die vollständige Antwort	Der Original-Server sendet die Antwort unverändert an den Client. Wenn die zwischengespeicherte Antwort abgelaufen ist, wird sie aktualisiert.
304 nicht modifiziert	Die folgenden Header-Werte in der 304-Antwort werden mit der zwischengespeicherten Antwort zusammengeführt und die zwischengespeicherte Antwort wird dem Client zugestellt: Date, Expires, Age, Cache-Control-Header Max-Age und S-Maxage-Token
401 nicht autorisiert; 400 schlechte Anfrage; 405 Methode nicht zulässig; 406 nicht akzeptabel; 407 Proxy-Authentifizierung erforderlich	Die Antwort des Ursprungs wird dem Kunden so serviert, wie sie ist. Die zwischengespeicherte Antwort wird nicht geändert.
Jede andere Fehlerantwort, z. B. 404 Not Found	Die Antwort des Ursprungs wird dem Kunden so serviert, wie sie ist. Die zwischengespeicherte Antwort wird entfernt.

> **Hinweis:**
> Der Parameter “Umfrage jedes Mal” behandelt die betroffenen Antworten als nicht speicherbar.

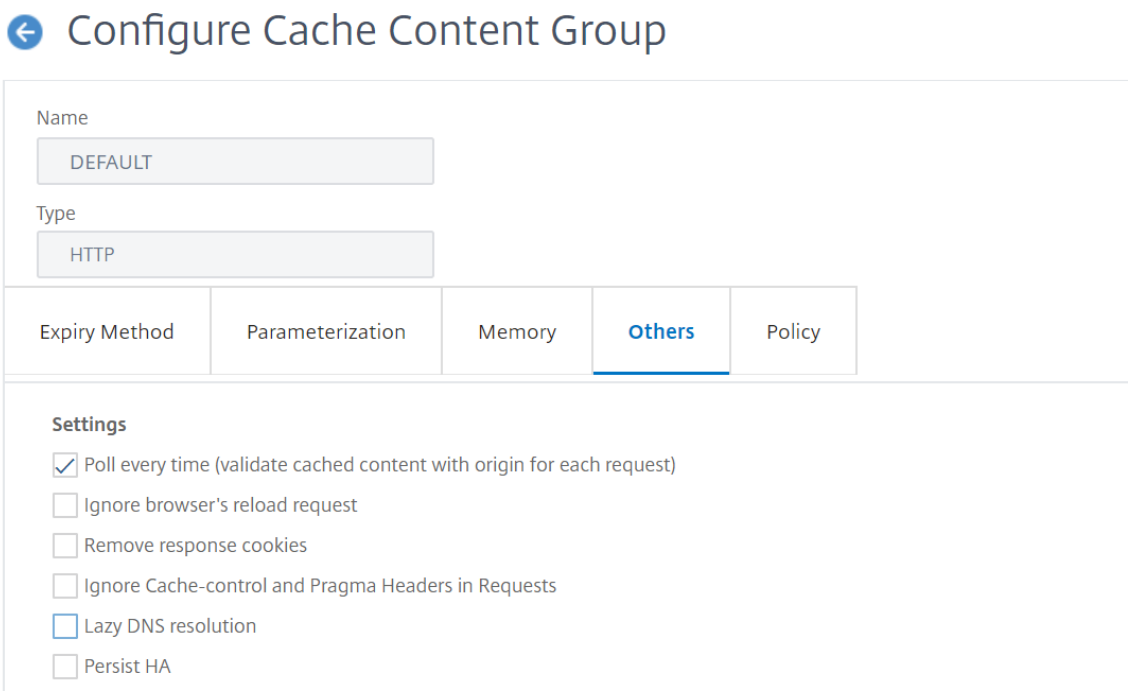
So konfigurieren Sie die Umfrage jedes Mal mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add cache contentgroup <contentGroupName> -pollEveryTime YES
```


Umfrage mit der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**und wählen Sie die Inhaltsgruppe aus.
2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe Einstellungen die Option Jedes Mal abfragen (zwischengespeicherten Inhalt mit Ursprung für jede Anfrage überprüfen).



PET und kundenspezifische Inhalte

Die PET-Funktion kann sicherstellen, dass der Inhalt für einen Kunden angepasst wird. Beispielsweise untersucht eine Website, die Inhalte in mehreren Sprachen bereitstellt, den Accept-Language-Anforderungsheader, um die Sprache für den Inhalt auszuwählen, den sie bereitstellt. Bei einer mehrsprachigen Website, bei der Englisch die vorherrschende Sprache ist, können alle englischsprachigen Inhalte in einer PET-Inhaltsgruppe zwischengespeichert werden. Dadurch wird sichergestellt, dass jede Anfrage an den Original-Server geht, um die Sprache für die Antwort zu bestimmen. Wenn die Antwort englisch ist und sich der Inhalt nicht geändert hat, kann der Original-Server eine 304 Not Modified für den Cache bereitstellen.

Das folgende Beispiel zeigt Befehle zum Zwischenspeichern englischer Antworten in einer PET-Inhaltsgruppe, zum Konfigurieren eines benannten Ausdrucks, der englische Antworten im Cache identifiziert, und zum Konfigurieren einer Richtlinie, die diese Inhaltsgruppe und den benannten Ausdruck verwendet. Fett wird zur Betonung verwendet:

```
1 add cache contentgroup EnglishLanguageGroup -pollEveryTime YES
```



```
2 add expression containsENExpression  - rule "http.res.header(\\"Content-
     Language\\").contains(\\"en\\")"
3 add cache policy englishPolicy -rule containsENExpression -action CACHE
      -storeInGroup englishLanguageGroup
4 bind cache policy englishPolicy -priority 100 -precedeDefRules NO
5 <!--NeedCopy-->
```

PET und Authentifizierung, Autorisierung und Prüfung

Outlook Web Access (OWA) ist ein gutes Beispiel für dynamisch generierte Inhalte, die von PET profitieren. Alle E-Mail-Antworten (*.EML-Objekte) haben einen `ETag` Validator, mit dem sie als PET-Antworten gespeichert werden können.

Jede Anfrage nach einer E-Mail-Antwort wird an den Original-Server weitergegeben, auch wenn die Antwort zwischengespeichert ist. Der Original-Server bestimmt, ob der Anforderer authentifiziert und autorisiert ist. Es überprüft auch, ob die Antwort im Original-Server vorhanden ist. Wenn alle Ergebnisse positiv sind, sendet der Ursprungsserver eine 304 Not Modified Antwort.

Integrierten Cache als Forward-Proxy konfigurieren

May 11, 2023

Der integrierte Cache kann als Forward-Proxygerät dienen, das Anfragen an andere NetScaler-Appliances oder an andere Arten von Cache-Servern weiterleitet. Sie konfigurieren den integrierten Cache als Forward-Proxy, indem Sie die IP-Adressen des oder der Cache-Server identifizieren. Nach der Konfiguration des Forward-Proxys sendet die NetScaler-Appliance Anfragen, die die konfigurierte IP-Adresse enthalten, an den Cache-Server, anstatt den integrierten Cache einzubeziehen.

So konfigurieren Sie den NetScaler mithilfe der Befehlszeilenschnittstelle als Forward-Cache-Proxy

Geben Sie in der Befehlszeile Folgendes ein:

```
add cache forwardProxy <IPAddress> <port>
```

So konfigurieren Sie den NetScaler mithilfe der GUI als Forward-Cache-Proxy

1. Navigieren Sie zu **Optimization** > **Integrated Caching** > **Forward Proxy**und fügen Sie einen Forward-Proxy hinzu, indem Sie die IP-Adresse und die Portnummer angeben.

Standardeinstellungen für den integrierten Cache

May 11, 2023

Die integrierte Cachefunktion von NetScaler bietet integrierte Richtlinien mit Standardeinstellungen und Anfangseinstellungen für die Standard-Inhaltsgruppe. Die Informationen in diesem Abschnitt definieren die Parameter für die integrierten Richtlinien und die Standard-Inhaltsgruppe.

Standard-Caching-Richtlinien

Der integrierte Cache verfügt über integrierte Richtlinien. Die NetScaler-Appliance bewertet die Richtlinien in einer bestimmten Reihenfolge, wie in den folgenden Abschnitten beschrieben.

Sie können diese integrierten Richtlinien durch eine benutzerdefinierte Richtlinie außer Kraft setzen, die an eine Richtlinienbank zur Außerkraftsetzung der Anforderungszeit oder zur Außerkraftsetzung von Antwortzeiten gebunden ist.

> **Hinweis:**
> Wenn Sie Richtlinien vor Version 9.0 konfiguriert und beim Binden der Richtlinien den Parameter -PrecededefRules angegeben haben, werden diese während der Migration automatisch Override-Time-Bindungspunkten zugewiesen.

Standardrichtlinien anzeigen

Die Namen der integrierten Richtlinien beginnen mit einem Unterstrich (_). Sie können die integrierten Richtlinien über die Befehlszeile und die Verwaltungskonsole mit dem Befehl show cache policy einsehen.

Standardanforderungsrichtlinien

Sie können die folgenden integrierten Richtlinien zur Anforderungszeitüberschreitung außer Kraft setzen, indem Sie neue Richtlinien konfigurieren und sie an den Verarbeitungspunkt für die Außerkraftsetzung von Anfragen binden. Beachten Sie in den folgenden Richtlinien, dass die MAY_NOCACHE-Aktion festlegt, dass die Transaktion nur dann zwischengespeichert wird, wenn zur Antwortzeit eine vom Benutzer konfigurierte oder integrierte CACHE-Direktive vorhanden ist.

Die folgenden Richtlinien sind an das Richtlinienlabel _reqBuiltInDefaults gebunden. Sie sind in der Reihenfolge ihrer Priorität aufgeführt.

Zwischenspeichern Sie keine Antwort auf eine Anfrage, die eine andere Methode als GET verwendet.

Der Name der Richtlinie lautet _NongetReq. Die folgende Richtlinienregel ist:

```
!HTTP.REQ.METHOD.eq(GET)
```

Legen Sie eine NOCACHE-Aktion für eine Anfrage mit einem Header-Wert fest, der If-Match oder If-Unmodified-Since enthält.

Der Name der Richtlinie lautet _AdvancedConditionalReq. Die folgende Richtlinienregel ist:


```
HTTP.REQ.HEADER("If-Match").EXISTS || HTTP.REQ.HEADER("If-Unmodified-Since"
).EXISTS
```

Legen Sie eine MAY_NOCACHE-Aktion für eine Anfrage mit den folgenden Header-Werten fest: Cookie, Authorization, Proxy-Authorization oder eine Anfrage, die den NTLM- oder Negotiate-Header enthält.

Der Name der Richtlinie lautet _PersonalizedReq. Die folgende Richtlinienregel ist:

```
HTTP.REQ.HEADER("Cookie").EXISTS || HTTP.REQ.HEADER("Authorization").EXISTS
 || HTTP.REQ.HEADER("Proxy-Authorization").EXISTS || HTTP.REQ.IS_NTLM_OR_NEGOTIATE
```

Standard-Antwortrichtlinien

Sie können die folgenden Standardrichtlinien für Reaktionszeiten außer Kraft setzen, indem Sie neue Richtlinien konfigurieren und sie an den Verarbeitungspunkt für die Außerkraftsetzung der Reaktionszeit binden.

Die folgenden Richtlinien sind an das Richtlinienlabel **_resBuiltInDefaults** gebunden und werden in der Reihenfolge ausgewertet, in der sie aufgeführt sind:

1. Zwischenspeichern Sie keine HTTP-Antworten, es sei denn, sie sind vom Typ 200, 304, 307, 203 oder wenn die Typen zwischen 400 und 499 oder zwischen 300 und 302 liegen.

   Der Name der Richtlinie ist **_uncacheableStatusRes**. Die folgende Richtlinienregel ist:

   ```
   !((HTTP.RES.STATUS.EQ(200))|| (HTTP.RES.STATUS.EQ(304))|| (HTTP.RES.
   STATUS.BETWEEN(400,499))|| (HTTP.RES.STATUS.BETWEEN(300, 302))|| (HTTP.
   RES.STATUS.EQ(307))|| (HTTP.RES.STATUS.EQ(203)))
   ```

2. Zwischenspeichern Sie keine HTTP-Antwort, wenn sie einen Vary-Header mit einem anderen Wert als Accept-Encoding enthält.

   Das Kompressionsmodul fügt den Header Vary: Accept_Encoding ein. Der Name dieses Ausdrucks ist **_uncacheableVaryRes**. Die folgende Richtlinienregel ist:

   ```
   ((HTTP.RES.HEADER("Vary").EXISTS)&& ((HTTP.RES.HEADER("Vary").INSTANCE
   (1).LENGTH > 0)|| (!HTTP.RES.HEADER("Vary").STRIP_END\\_WS.SET_TEXT_MODE
   (IGNORECASE).eq("Accept-Encoding"))))
   ```

3. Zwischenspeichern Sie keine Antwort, wenn ihr Cache-Control-Header-Wert No-Cache, No-Store oder Private ist oder wenn der Cache-Control-Header nicht gültig ist.

   Der Name der Richtlinie lautet **_UncacheableCacheControlRes**. Die folgende Richtlinienregel ist:

   ```
   ((HTTP.RES.CACHE\\_CONTROL.IS\\_PRIVATE)|| (HTTP.RES.CACHE\\_CONTROL.IS
   \\_NO\\_CACHE)|| (HTTP.RES.CACHE\\_CONTROL.IS\\_NO\\_STORE)|| (HTTP.RES
   .CACHE\\_CONTROL.IS\\_INVALID))
   ```


4. Cache-Antworten, wenn der Cache-Control-Header einen der folgenden Werte hat: Public, Must-Revalidate, Proxy-Revalidate, Max-Age, S-Maxage.

   Der Name der Richtlinie lautet **_CacheableCacheControlRes**. Die folgende Richtlinienregel ist:

   ```
   ((HTTP.RES.CACHE_CONTROL.IS_PUBLIC)|| (HTTP.RES.CACHE_CONTROL.IS_MAX_AGE
   )|| (HTTP.RES.CACHE_CONTROL.IS_MUST_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL
   .IS_PROXY_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL.IS_S_MAXAGE))
   ```

5. Zwischenspeichern Sie keine Antworten, die einen Pragma-Header enthalten.

   Der Name der Richtlinie ist **_uncacheablePragmares**. Die folgende Richtlinienregel ist:

   ```
   HTTP.RES.HEADER("Pragma").EXISTS
   ```

6. Zwischenspeichern von Antworten, die einen Expires-Header enthalten.

   Der Name der Richtlinie lautet **_CacheableExpiryRes**. Die folgende Richtlinienregel ist:

   ```
   HTTP.RES.HEADER("Expires").EXISTS
   ```

7. Wenn die Antwort einen Content-Type-Header mit dem Wert Image enthält, entfernen Sie alle Cookies im Header und speichern Sie ihn im Cache.

   Der Name der Richtlinie lautet **_ImageRes**. Die folgende Richtlinienregel ist:

   ```
   HTTP.RES.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).STARTSWITH("
   image/")
   ```

   Sie können die folgende Inhaltsgruppe so konfigurieren, dass sie mit dieser Richtlinie arbeitet:

   ```
   add cache contentgroup nocookie -group -removeCookies YES
   ```

8. Zwischenspeichern Sie keine Antwort, die einen Set-Cookie-Header enthält.

   Der Name der Richtlinie lautet **_ PersonalizedRes**. Die folgende Richtlinienregel ist:

HTTP.RES.HEADER („Cookie setzen“) .EXISTS	HTTP.RES.HEADER(“Set-Cookie2”).EXISTS

Einschränkungen der Standardrichtlinien

Sie können die folgenden integrierten Richtlinien für die Anfragezeit nicht durch benutzerdefinierte Richtlinien überschreiben.

Diese Richtlinien sind in der Reihenfolge ihrer Priorität aufgeführt.

1. Zwischenspeichern Sie keine Antworten, wenn der entsprechenden HTTP-Anfrage eine GET- oder POST-Methode fehlt.

2. Zwischenspeichern Sie keine Antworten auf eine Anfrage, wenn die URL-Länge der HTTP-Anfrage plus Hostname 1744 Byte überschreitet.
3. Zwischenspeichern Sie keine Antwort auf eine Anfrage, die einen If-Match-Header enthält.
4. Zwischenspeichern Sie keine Anfrage, die einen If-Unmodified-Since-Header enthält.

> **Hinweis:**
> Dies unterscheidet sich vom If-Modified-Since-Header.

1. Zwischenspeichern Sie keine Antwort, wenn der Server keinen Ablauf-Header festlegt.

Sie können die folgenden integrierten Richtlinien für die Reaktionszeit nicht außer Kraft setzen. Diese Richtlinien werden in der Reihenfolge bewertet, in der sie aufgeführt sind:

1. Zwischenspeichern Sie keine Antworten, die den HTTP-Antwortstatuscode 201, 202, 204, 205 oder 206 haben.
2. Zwischenspeichern Sie keine Antworten mit dem HTTP-Antwortstatuscode 4xx, mit Ausnahme der Statuscodes 403, 404 und 410.
3. Zwischenspeichern Sie keine Antworten, wenn der Antworttyp FIN-terminiert ist oder die Antwort keines der folgenden Attribute hat: Content-Length oder Transfer-Encoding: Chunked.
4. Zwischenspeichern Sie die Antwort nicht, wenn das Caching-Modul seinen Cache-Control-Header nicht analysieren kann.

Grundeinstellungen für die Standard-Inhaltsgruppe

Wenn Sie das integrierte Caching zum ersten Mal aktivieren, stellt die NetScaler Appliance eine vordefinierte Inhaltsgruppe mit der Bezeichnung Standardinhaltsgruppe zur Verfügung. Ausführliche Informationen finden Sie unter Tabelle mit Standardeinstellungen für Inhaltsgruppen .

Problembehandlung

May 11, 2023

Wenn die integrierte Cache-Funktion nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf NetScaler-Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Fehlerbehebung

Weitere Informationen zu den Ressourcen, die für die Fehlerbehebung und Beispielkonfigurationen verfügbar sind, finden Sie unter Ressource zur Fehlerbehebung bei PDF-Dateien.

Front-End-Optimierung

May 11, 2023

> **Hinweis:** Die Front-End-Optimierung ist verfügbar, wenn Sie über eine Advanced oder Premium NetScaler Lizenz verfügen und NetScaler Version 10.5 oder höher ausführen.

Die HTTP-Protokolle, die Webanwendungen zugrunde liegen, wurden ursprünglich entwickelt, um die Übertragung und das Rendern einfacher Webseiten zu unterstützen. Neue Technologien wie JavaScript und Cascading Stylesheets (CSS) sowie neue Medientypen wie Flash-Videos und grafikreiche Bilder stellen hohe Anforderungen an die Front-End-Performance, also an die Leistung auf Browserebene.

Die NetScaler-Frontend-Optimierungsfunktion (FEO) behebt solche Probleme und reduziert die Lade- und Renderzeit von Webseiten durch:

- Reduzierung der Anzahl der Anfragen.
- Erforderlich für das Rendern jeder Seite.
- Reduzierung der Anzahl von Bytes in Seitenantworten.

Vereinfachung und Optimierung der Inhalte, die dem Client-Browser zur Verfügung gestellt werden.

Sie können Ihre FEO-Konfiguration anpassen, um Ihren Benutzern die besten Ergebnisse zu bieten. NetScaler unterstützen zahlreiche Optimierungen von Webinhalten sowohl für Desktop- als auch für mobile Benutzer. In den folgenden Tabellen werden die Frontend-Optimierungen beschrieben, die durch die FEO-Funktion bereitgestellt werden, und die Operationen, die für verschiedene Dateitypen ausgeführt werden.

Optimierungen, die durch die FEO-Funktion durchgeführt wurden

Web-Optimierung	Problem	Welche Funktion bietet NetScaler FEO	Vorteile
Inlinieren	Clientbrowser senden häufig mehrere Anfragen an Server, um externe CSS, Bilder und JavaScript zu laden, die mit der Webseite verknüpft sind.	CSS Inline, JavaScript Inline, CSS kombinieren	Das Laden von externen CSS, Bildern und JavaScript inline mit den HTML-Dateien verbessert die Seitenrendering-Zeit. Diese Optimierung ist vorteilhaft für Inhalte, die nur einmal angesehen werden, und für Mobilgeräte mit begrenzten Cachegrößen.
Minimierung	Daten, die von Servern abgerufen werden, enthalten unwichtige Zeichen wie Leerzeichen, Kommentare und Zeilenumbrüche. Die Zeit, die Browser für die Verarbeitung solcher Daten aufwenden, führt zu einer Latenz der Website.	CSS-Minimierung, JavaScript-Minimierung, Entfernung von HTML-Kommentaren	Minimierte Dateien verbrauchen weniger Bandbreite und vermeiden die durch spezielle Verarbeitung verursachte Latenz.

Web-Optimierung	Problem	Welche Funktion bietet NetScaler FEO	Vorteile
Bild-Optimierung	Mobile Browser haben oft langsame Verbindungs-geschwindigkeiten und begrenzten Cache-Speicher. Das Herunterladen der Bilder auf mobile Clients verbraucht mehr Bandbreite, Verarbeitungszeit und Cache-Speicherplatz, was zu einer Website-Latenz führt.	JPEG-Optimierung, CSS-Bild-Inlining, **Bildschrumpfung** -Attribute, GIF zu PNG-Konvertierung, HTML-Bild-Inlining, WebP-Bildkonvertierung, JPEG, GIF, PNG zu JPEG-XR-Bildkonvertierung	Reduziert das Bild auf die Größe, die im Image-Tag von NetScaler angegeben wird, sodass Clientbrowser Bilder schneller laden können.
Neupositionierung	Eine ineffiziente Verarbeitung von externem CSS, Bildern und JavaScript erhöht die Ladezeit der Seite.	Bild lazy loading, CSS move to Head, JavaScript move to end	Positioniert HTML-Elemente neu, um die Rendering-Zeit für Webseiten zu reduzieren und es Clientbrowsern zu ermöglichen, die Objekte schneller zu laden.

Web-Optimierung	Problem	Welche Funktion bietet NetScaler FEO	Vorteile
Verbindungsverwaltung	Viele Browser begrenzen die Anzahl gleichzeitiger Verbindungen, die zu einer einzelnen Domain hergestellt werden können. Dies kann dazu führen, dass Browser die Webseitenressourcen nacheinander herunterladen, was zu einer höheren Browserzeit führt.	Domain-Sharding	Überwindet die Verbindungs-beschränkung, wodurch die Seitenrenderzeit verbessert wird, indem Client-Browser mehr Ressourcen parallel herunterladen können.

Weboptimierungen für verschiedene Dateitypen:

NetScaler kann Weboptimierungen für CSS, Bilder, Javascript und HTML durchführen. Weitere Informationen finden Sie unter PDF zur Weboptimierung .

> **Hinweis:**
> Die Front-End-Optimierungsfunktion unterstützt nur ASCII-Zeichen. Der Unicode-Zeichensatz wird nicht unterstützt.

So funktioniert die Frontend-Optimierung

Nachdem der NetScaler die Antwort vom Server erhalten hat:

1. Analysiert den Inhalt der Seite, erstellt einen Eintrag im Cache (wo zutreffend) und wendet die FEO-Richtlinie an.

   Ein NetScaler kann beispielsweise die folgenden Optimierungsregeln anwenden:

   - Entfernen Sie Leerzeichen oder Kommentare in einem CSS oder JavaScript.
   - Kombinieren Sie eine oder mehrere CSS-Dateien zu einer Datei.
   - Konvertiert das GIF-Bildformat in das PNG-Format.

2. Schreibt die eingebetteten Objekte neu und speichert den optimierten Inhalt im Cache mit einer anderen Signatur als der, die für den ersten Cache-Eintrag verwendet wurde.

3. Ruft bei nachfolgenden Anfragen die optimierten Objekte aus dem Cache ab, nicht vom Server, und leitet die Antworten an den Client weiter.

**

Entfernen Sie überflüssige Informationen wie Leerzeichen und Kommentare.

Der Zeitraum, in dem der Browser die zwischengespeicherte Ressource verwenden kann, ohne zu überprüfen, ob neue Inhalte auf dem Server verfügbar sind.

Frontend-Optimierung konfigurieren

Optional können Sie die Werte der globalen Einstellungen für die Frontend-Optimierung ändern. Andernfalls erstellen Sie zunächst Aktionen, die die Optimierungsregeln festlegen, die auf die eingebetteten Objekte angewendet werden sollen.

Nachdem Sie die Aktionen konfiguriert haben, erstellen Sie Richtlinien mit jeweils einer Regel, die einen Anforderungstyp angibt, für den die Antwort optimiert werden soll, und ordnen Sie die Aktionen den Richtlinien zu.

> **Hinweis:** Der NetScaler wertet Richtlinien zur Front-End-Optimierung nur zur Anforderungszeit aus, nicht zur Reaktionszeit.

Um die Richtlinien in Kraft zu setzen, binden Sie sie an Bindungspunkte. Sie können eine Richtlinie global binden, sodass sie für den gesamten Datenverkehr gilt, der über den NetScaler fließt, oder Sie können die Richtlinie an einen virtuellen Load-Balancing- oder Content-Switching-Server vom Typ HTTP oder SSL binden. Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Eine niedrigere Prioritätszahl weist auf einen höheren Wert hin. Der NetScaler wendet die Richtlinien in der Reihenfolge ihrer Prioritäten an.

Voraussetzungen

Für die Frontend-Optimierung muss die integrierte Caching-Funktion von NetScaler aktiviert sein. Außerdem müssen Sie die folgenden integrierten Caching-Konfigurationen durchführen:

- Ordnen Sie Cache-Speicher zu.
- Legen Sie die maximale Antwortgröße und das Speicherlimit für eine Standard-Cache-Content-Gruppe fest.

Weitere Informationen zum Konfigurieren des integrierten Cachings finden Sie unter Integriertes Caching.

Hinweis: Der Begriff Integrated Cache kann austauschbar mit AppCache verwendet werden. Beachten Sie, dass beide Begriffe aus funktionaler Sicht dasselbe bedeuten.

Konfigurieren der Front-End-Optimierung mithilfe der NetScaler Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Aktivieren Sie die Frontend-Optimierungsfunktion.

```
enable ns feature FEO
```

1. Erstellen Sie eine oder mehrere Aktionen zur Frontend-Optimierung.

```
add feo action <name> [-imgShrinkToAttrib] [-imgGifToPng] ...
```

Beispiel: Sofügen Sie eine Front-End-Optimierungsaktion für die Konvertierung von Bildern im GIF-Format in das PNG-Format und die Verlängerung des Ablaufzeitraums des Caches hinzu:

```
add feo action allact -imgGifToPng -pageExtendCache
```

1. [Optional] Geben Sie nicht standardmäßige Werte für die globalen Einstellungen der Frontend-Optimierung an.

```
set feo parameter [-cacheMaxage <integer>] [-JpegQualityPercent <integer>]
[-cssInlineThresSize <integer>] [-inlineJsThresSize <integer> [-inlineImgThresSize
 <integer>]
```

Beispiel: So geben Sie den maximalen Cache-Ablaufzeitraum an:

```
set feo parameter -cacheMaxage 10
```

1. Erstellen Sie eine oder mehrere Frontend-Optimierungsrichtlinien.

```
add feo policy <name> <rule> <action>
```

Beispiel: So fügen Sie eine Front-End-Optimierungsrichtlinie hinzu und verknüpfen sie der oben angegebenen allact-Aktion:

```
>add feo policy pol1 TRUE all act
>add feo policy pol1 "(HTTP.REQ.URL.CONTAINS("testsite"))" allact1
<!--NeedCopy-->
```

1. Binden Sie die Richtlinie an einen virtuellen Load-Balancing- oder Content-Switching-Server oder binden Sie sie global.

```
bind lb vserver <name> -policyName <string> -priority <num>
```

```
bind cs vserver <name> -policyName <string> -priority <num>
```

```
bind feo global <policyName> <priority> -type <type> <gotoPriorityExpression
>
```

Beispiel: Um die Frontend-Optimierungsrichtlinie auf einen virtuellen Server mit dem Namen „abc“ anzuwenden:


```
> bind lb vserver abc -policyName pol1 -priority 1 -type NONE
```

Beispiel: Um die Frontend-Optimierungsrichtlinie auf den gesamten Traffic anzuwenden, der den ADC erreicht, gehen Sie wie folgt vor:

```
> bind feo global pol1 100 -type REQ_DEFAULT
```

1. Speichern Sie die Konfiguration. save ns config

Konfigurieren der Front-End-Optimierung mit der GUI

1. Navigieren Sie zu **Optimierung** > **Front-End-Optimierung** > **Aktionen**, und klicken Sie auf **Hinzufügen** und erstellen Sie eine Front-End-Optimierungsaktion, indem Sie die relevanten Details angeben.
2. [Optional] Geben Sie die globalen Einstellungen für die Frontend-Optimierung an.
3. Navigieren Sie zu **Optimierung** > **Frontend-Optimierung**und klicken Sie im rechten Bereich unter Einstellungen auf **Frontend-Optimierungseinstellungen ändern** und geben Sie die globalen Einstellungen für die Frontend-Optimierung an.
4. Erstellen Sie eine Richtlinie zur Frontend-Optimierung.
5. Navigieren Sie zu **Optimierung** > **Frontend-Optimierung** > **Richtlinien**, klicken Sie auf **Hinzufügen** und erstellen Sie eine Frontend-Optimierungsrichtlinie, indem Sie die entsprechenden Details angeben.
6. Binden Sie die Richtlinie an einen virtuellen Lastausgleichs- oder Content Switching-Server.
   a) Navigieren Sie zu **Optimierung** > **Front-End-Optimierung** > **Richtlinien**.
   b) Wählen Sie eine Front-End-Optimierungsrichtlinie aus, und klicken Sie auf **Richtlinien-Manager**.
   c) Binden Sie unter **Front End Optimization Policy Manager**die Front-End-Optimierungsrichtlinie an einen virtuellen Load Balancing- oder Content Switching-Server.

Überprüfen der Konfiguration der Front-End-Optimierung

Das Dashboard-Dienstprogramm zeigt zusammenfassende und detaillierte Statistiken in tabellarischer und grafischer Form an. Sie können die FEO-Statistiken einsehen, um Ihre FEO-Konfiguration auszuwerten.

Optional können Sie auch Statistiken für eine FEO-Richtlinie anzeigen, einschließlich der Anzahl der Auswahlen, die der Policy-Zähler während des richtlinienbasierten FEO erhöht.

> **Hinweis:**
> Weitere Informationen zu Statistiken und Diagrammen finden Sie in der Dashboard-Hilfe der NetScaler-Appliance.

FEO-Statistiken mithilfe der CLI anzeigen

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Zusammenfassung der FEO-Statistiken, FEO-Richtlinienauswahl und -details sowie detaillierte FEO-Statistiken anzuzeigen:

- `stat feo` Hinweis: Der Befehl stat feo policy zeigt Statistiken nur für erweiterte FEO-Richtlinien an.
- `show feo policy name`
- `stat feo -detail`

FEO-Statistiken auf dem NetScaler-Dashboard anzeigen

In der Dashboard-GUI können Sie:

- Wählen Sie Frontend-Optimierung aus, um eine Zusammenfassung der `FEO` Statistiken anzuzeigen.
- Klicken Sie auf die Registerkarte **Graphische Ansicht**, um die Rate der Anfragen anzuzeigen, die von der FEO-Funktion bearbeitet wurden.

Proben-Optimierung:

In der Beispiel-PDF-Datei finden Sie einige Beispiele für Aktionen zur Inhaltsoptimierung, die auf HTML-Inhalte und die eingebetteten Objekte im HTML-Inhalt angewendet werden.

Klassifizierung der Medien

May 11, 2023

Das Verständnis der Art des Datenverkehrs im Netzwerk hilft Netzwerkadministratoren, den Bandbreitenverbrauch zu verwalten und so eine optimale Netzwerkleistung zu erzielen. Im Medienklassifizierungsmodus werden die Statistiken des Medienverkehrs, der die NetScaler-Appliance durchläuft, überwacht und angezeigt.

Wenn dieser Modus aktiviert ist, kann ein Netzwerkadministrator Statistiken sammeln, aus denen die Menge der abgerufenen Daten und die Gerätetypen hervorgeht, von denen aus auf die Mediendateien zugegriffen wurde. Die NetScaler-Appliance unterstützt in diesem Modus auch Bytebereichsanfragen.

Derzeit kann die NetScaler-Appliance Statistiken für die folgenden Mediendateitypen überwachen und anzeigen:

Medien	Dateityp
Microsoft Reibungsloses Streaming	Video

Medien	Dateityp
Apple Livestreaming	Video
Audiodatentransportstream (ADTS)	Audio
Fortgeschrittene Audiocodierung (AAC)	Audio
Flash-Video (FLV)	Audio und Video
3GP	Audio und Video

Die Appliance kann Statistiken für die folgenden Geräte anzeigen:

Geräteplattform	Gerätetyp
iOS	iPad und iPod
Android	Handys und Tablets
Laptop oder Desktop	Windows-Laptop und Desktop-Computer
Sonstiges	Andere mobile Geräte (Handys und Tablets)

Die Netzwerkadministratoren können die folgenden Statistikindikatoren überprüfen, um die Datenmenge zu ermitteln, auf die über die NetScaler-Appliance für verschiedene Medienverkehrstypen zugegriffen wird.

Name der Mediendatei	Statistik-Zähler
Microsoft Reibungsloses Streaming	mcmssmthstrmvid—Dieser Zähler zeichnet die Gesamtzahl der Microsoft Smooth Streaming-Videos auf, die von der NetScaler-Appliance bereitgestellt werden;Mcmssmthstrvidpl—Dieser Zähler zeichnet die Gesamtzahl der Microsoft Smooth Streaming-Video-Playlisten auf, die von der NetScaler-Appliance bereitgestellt werden;Mcmssmthstrmvidbytes—Dieser Zähler zeichnet die Gesamtzahl der Datenbytes auf, die für den Microsoft Smooth Streaming-Medienverkehr auf der NetScaler-Appliance bereitgestellt werden.Mcmssmthstrmplvidbytespl—Dieser Zähler zeichnet die Gesamtzahl der Microsoft Smooth Streaming-Wiedergabelistenbytes auf, die von der NetScaler-Appliance bereitgestellt werden.
Apple Livestreaming	mccaplelivestrmngvid—Dieser Zähler zeichnet die Gesamtzahl der Apple Live Streaming-Videos auf, die von der NetScaler-Appliance bereitgestellt werden. Mccapplelivestrmngvidpl — Dieser Zähler zeichnet die Gesamtzahl der Apple Live Streaming-Video-Playlisten auf, die von der NetScaler-Appliance bereitgestellt werden.Mcapplelivestreamingvidbytes—Dieser Zähler zeichnet die Gesamtzahl der Datenbytes auf, die für den Apple Live Streaming-Medienverkehr auf der NetScaler-Appliance bereitgestellt wurden.Mcapplelivestreamingplaylistvidbytespl—Dieser Zähler zeichnet die Gesamtzahl der Apple Live Playli-Bytes auf, die von der NetScaler-Appliance bereitgestellt werden.

Name der Mediendatei	Statistik-Zähler
Audiodatentransportstream (ADTS)	`mcadtsaudio`— Dieser Zähler zeichnet die Gesamtzahl der ADTS-Audioclips auf, die von der NetScaler-Appliance bereitgestellt werden.`Mcadtsaudiobytes`— Dieser Zähler zeichnet die Gesamtzahl der Datenbytes auf, die für den ADTS-Medienverkehr auf der NetScaler-Appliance bereitgestellt wurden.
Fortgeschrittene Audiocodierung (AAC)	`Mcaacaudio`— Dieser Zähler zeichnet die Gesamtzahl der AAC-Audioclips auf, die von der NetScaler-Appliance bereitgestellt werden.`Mcaacaudiobytes`— Dieser Zähler zeichnet die Gesamtzahl der Datenbytes auf, die für den AAC-Medienverkehr auf der NetScaler-Appliance bereitgestellt wurden.
Flash-Video (FLV)	`Mcflvvid`— Dieser Zähler zeichnet die Gesamtzahl der Flash-Videos auf, die von der NetScaler-Appliance bereitgestellt werden.`Mcflvvidbytes`— Dieser Zähler zeichnet die Gesamtzahl der Datenbytes auf, die für Flash-Videos auf der NetScaler-Appliance bereitgestellt wurden.
3GP	`mc3gpvidbytes`— Dieser Zähler zeichnet die Gesamtzahl der Datenbytes auf, die für den 3GP-Medienverkehr auf der NetScaler-Appliance bereitgestellt wurden.

Die NetScaler Appliance erkennt Mediendateitypen anhand ihrer Signaturen in den *ersten Textbytes* der Antworten. Beispielsweise haben die ersten Body-Bytes für eine MP4-Datei die folgende Signatur in der Antwort:

```
**....ftypmp42** ....isommp42....moov...lmvhd.....c.\!.c.\!..
```

Die NetScaler Appliance erkennt den Typ des Client-Geräts anhand der *User-Agent-Zeichenfolge*, die das Client-Gerät in der HTTP-GET-Anfrage enthält. Beispielsweise enthält ein Windowphone, das einen UC-Browser verwendet, die folgende User-Agent-Zeichenfolge in der HTTP-GET-Anfrage:

```
User-Agent: **UCWEB**/2.0 (**Windows**; U; wds 8.10; en-US; HTC; 8X by HTC)
U2/1.0.0
```


Medienklassifizierung aktivieren

Standardmäßig ist die Medienklassifizierung auf der NetScaler-Appliance deaktiviert. Sie müssen den Modus aktivieren, bevor Sie ihn verwenden können.

So aktivieren Sie die Medienklassifizierung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns mode Mediaclassification
```

So aktivieren Sie die Medienklassifizierung mithilfe der GUI

Aktivieren Sie die Medienklassifizierung auf der NetScaler-Appliance

Navigieren Sie zu **System** > **Einstellungen** > **Modi konfigurieren** und wählen Sie **Media Classification**aus.

Um Statistiken zum Medienverkehr auf der NetScaler-Appliance anzuzeigen

Navigieren Sie zu **Optimierung** und klicken Sie auf **Medienklassifizierung**, um die Statistiken zum Medienverkehr einzusehen.

Überprüfen Sie die Statistiken zur Medienklassifizierung

Sie können die Statistiken zum Medienverkehr im Dashboard-Dienstprogramm oder über die Befehlszeilenschnittstelle einsehen. Das Dashboard-Dienstprogramm zeigt zusammenfassende und detaillierte Statistiken in einem Tabellen- und Grafikformat an.

> **Hinweis**
> Weitere Informationen zu Statistiken und Diagrammen finden Sie in der Dashboard-Hilfe auf Ihrer NetScaler-Appliance.

So können Sie Statistiken zur Medienklassifizierung mithilfe der Befehlszeilenschnittstelle anzeigen

Geben Sie in der Befehlszeile einen der folgenden Befehle ein, um eine Zusammenfassung der Statistiken zur Medienklassifizierung anzuzeigen, detaillierte Statistiken anzuzeigen oder die Anzeige zu löschen:

```
stat Mediaclassification

stat Mediaclassification -detail

stat Mediaclassification -clearstats
```

Um Statistiken zur Medienklassifizierung im Dashboard einzusehen

Im **Dashboard-Dienstprogramm** können Sie die folgenden Arten von Statistiken zur Medienklassifizierung anzeigen:

1. Wählen Sie **Media Classification** aus, um eine Zusammenfassung der Statistiken zum Medienverkehr anzuzeigen.
2. Um detaillierte Statistiken zum Medienverkehr anzuzeigen, klicken Sie auf die **Details**.
3. Um die Statistiken zum Medienverkehr zu löschen, klicken Sie auf **Löschen**.

Ruf

May 11, 2023

NetScaler bietet auf Reputation basierende Sicherheit. Mithilfe einer Reputationsanalyse können Sie das Risiko der Bearbeitung von Anfragen ermitteln. Sie können Maßnahmen ergreifen, z. B. bestimmte Anfragen blockieren oder löschen, um die Leistung Ihrer Anwendung zu verbessern.

Die NetScaler IP-Reputationsfunktion verwendet IP-Reputationsprüfungen, um Zero-Day-Angriffe zu verhindern und vor bösartigen Quellen zu schützen, die mit Webangriffen, Phishing-Aktivitäten oder Web-Scans verbunden sind.

Weitere Informationen finden Sie unter IP-Reputation.

IP-Reputation

May 11, 2023

IP-Reputation ist ein Tool, das IP-Adressen identifiziert, die unerwünschte Anfragen senden. Mithilfe der IP-Reputationsliste können Sie Anfragen ablehnen, die von einer IP-Adresse mit schlechtem Ruf stammen. Optimieren Sie die Leistung der Web Application Firewall, indem Sie Anfragen filtern, die Sie nicht verarbeiten möchten. Setzen Sie eine Anfrage zurück, löschen Sie sie oder konfigurieren Sie sogar eine Responder Policy, um eine bestimmte Responder Action auszuführen.

Im Folgenden sind einige Angriffe aufgeführt, die Sie mithilfe von IP Reputation verhindern können:

- **Virus Infizierte PCs**. (Heim-PCs) sind die größte Spam-Quelle im Internet. IP Reputation kann die IP-Adresse identifizieren, die unerwünschte Anfragen sendet. Die IP-Reputation kann besonders nützlich sein, um große DDoS-, DoS- oder anomale SYN-Flood-Angriffe von bekannten infizierten Quellen zu blockieren.
- **Zentrales verwaltetes und automatisiertes Botnet**. Angreifer haben aufgrund des Diebstahls von Kennwörtern an Popularität gewonnen, da es nicht lange dauert, bis Hunderte von Computern zusammenarbeiten, um Ihr Kennwort zu knacken. Es ist einfach, Botnet-Angriffe zu starten, um Kennwörter herauszufinden, die häufig verwendete Wörterbuchwörter verwenden.

- **Kompromittierter Webserver**. Angriffe sind nicht so häufig, da das Bewusstsein und die Serversicherheit zugenommen haben, sodass Hacker und Spammer nach einfacheren Zielen suchen. Es gibt immer noch Webserver und Online-Formulare, die Hacker kompromittieren und zum Versenden von Spam verwenden können (wie Viren und Pornos). Solche Aktivitäten sind einfacher zu erkennen und schnell herunterzufahren oder mit einer Reputationsliste wie SpamRats zu blockieren.
- **Windows Exploits**. (wie Active IPs, die Malware, Shell-Code, Rootkits, Würmer oder Viren anbieten oder verbreiten).
- **Bekannte Spammer und Hacker**.
- **Massen-E-Mail-Marketingkampagnen**.
- **Phishing-Proxys** (IP-Adressen, die Phishing-Websites hosten, und andere Betrugsfälle wie Werbeklickbetrug oder Spielbetrug).
- **Anonyme Proxys** (IPs, die Proxy- und Anonymisierungsdienste bereitstellen, einschließlich The Onion Router alias TOR).

Eine NetScaler-Appliance verwendet **Webroot** als Dienstanbieter für eine dynamisch generierte bösartige IP-Datenbank und die Metadaten für diese IP-Adressen. Metadaten können Geolokationsdetails, Bedrohungskategorie, Bedrohungszahl usw. enthalten. Die Webroot Threat Intelligence-Engine erhält Echtzeitdaten von Millionen von Sensoren. Es erfasst, scannt, analysiert und bewertet die Daten automatisch und kontinuierlich mithilfe von fortschrittlichem maschinellem Lernen und Verhaltensanalysen. Die Informationen über eine Bedrohung werden ständig aktualisiert.

Die NetScaler Appliance validiert eine eingehende Anfrage auf ihren schlechten Ruf mithilfe der Webroot verwendet die IP-Reputationsdatenbank. Die Datenbank verfügt über eine riesige Sammlung von IP-Adressen klassifizierten IP-Bedrohungskategorien. Im Folgenden sind die Kategorien von IP-Bedrohungen und deren Beschreibung aufgeführt.

- Spam-Quellen. Spam-Quellen umfassen das Tunneln von Spam-Nachrichten über Proxy, anomale SMTP-Aktivitäten und Forum-Spam-Aktivitäten.
- Windows Exploits. Die Windows-Exploit-Kategorie umfasst aktive IP-Adressen, die Malware, Shellcode, Rootkits, Würmer oder Viren anbieten oder verteilen
- Internet-Angriffe. Die Kategorie der Webangriffe umfasst Cross-Site-Scripting, iFrame-Injection, SQL-Injection, domänenübergreifende Injection oder
- Botnetze. Botnet-Kategorie umfasst Botnet-C&C-Kanäle und infizierte Zombie-Maschinen, die vom Bot-Master gesteuert werden
- Scanner. Die Kategorie Scanner umfasst alle Aufklärungen wie Sonden, Host-Scan, Domain-Scan und Kennwort-Brute-Force-Angriff
- Diensteverweigerung. Die Kategorie "Denial of Services" umfasst DOS, DDOS, anomale Synchronisationsflut und Erkennung von anomalem Datenverkehr
- Ruf. Den Zugriff von IP-Adressen verweigern, von denen derzeit bekannt ist, dass sie mit Malware infiziert sind. Diese Kategorie umfasst auch IPs mit einem durchschnittlich niedrigen Webroot Reputation Index. Die Aktivierung dieser Kategorie verhindert den Zugriff von

identifizierten Quellen, um Malware-Verteilungspunkte zu kontaktieren.
- Phishing. Die Phishing-Kategorie umfasst IP-Adressen, die Phishing-Seiten hosten, andere Betrugsaktivitäten wie Ad-Click-Betrug oder Spielbetrug.
- Proxy. Die Proxykategorie umfasst IP-Adressen, die Proxy- und Def-Dienste bereitstellen.
- Mobile Bedrohungen. Die Kategorie Mobile Threat umfasst IP-Adressen bösartiger und unerwünschter mobiler Anwendungen. Diese Kategorie nutzt Daten des Forschungsteams für mobile Bedrohungen von Webroot.
- Tor-Proxy. Die Tor-Proxykategorie umfasst IP-Adressen, die als Ausgangsknoten für das Tor-Netzwerk fungieren. Ausgangsknoten sind der letzte Punkt entlang der Proxykette und stellen eine direkte Verbindung zum beabsichtigten Ziel des Urhebers her.

Wenn irgendwo im Netzwerk eine Bedrohung erkannt wird, wird die IP-Adresse als bösartig gekennzeichnet und alle mit dem Netzwerk verbundenen Geräte sind sofort geschützt. Die dynamischen Änderungen der IP-Adressen werden mithilfe von fortschrittlichem maschinellem Lernen mit hoher Geschwindigkeit und Genauigkeit verarbeitet.

Wie im Datenblatt von Webroot angegeben, identifiziert das Sensornetzwerk des Webroot viele wichtige IP-Bedrohungsarten, darunter Spam-Quellen, Windows-Exploits, Botnets, Scanner und andere. (Siehe das Flussdiagramm auf dem Datenblatt.)

Die NetScaler-Appliance verwendet einen `iprep` Clientprozess, um die Datenbank von Webroot abzurufen. Der `iprep` Client verwendet die Methode HTTP GET, um zum ersten Mal die absolute IP-Liste von Webroot abzurufen. Später werden alle 5 Minuten Delta-Änderungen überprüft.

> **Wichtig:**
>
> - Stellen Sie sicher, dass die NetScaler Appliance über Internetzugang verfügt und DNS konfiguriert ist, bevor Sie die IP-Reputationsfunktion verwenden.
> - Um auf die Webroot Datenbank zuzugreifen, muss die NetScaler-Appliance in der Lage sein, eine Verbindung zu **api.bcti.brightcloud.com** auf **Port 443**herzustellen. Jeder Knoten in der HA- oder Clusterbereitstellung erhält die Datenbank von Webroot und muss auf diesen vollqualifizierten Domänennamen (FQDN) zugreifen können.
> - Webroot hostet derzeit seine Reputationsdatenbank in AWS. Daher muss NetScaler in der Lage sein, AWS-Domänen für das Herunterladen der Reputationsdatenbank aufzulösen. Außerdem muss die Firewall für AWS-Domains offen sein.
>
> **Hinweis:**
>
> Jede Paket-Engine benötigt mindestens 4 GB, um ordnungsgemäß zu funktionieren, wenn die IP-Reputationsfunktion aktiviert ist.

Erweiterte Richtlinienausdrücke. Konfigurieren Sie die IP-Reputationsfunktion mithilfe erweiterter Richtlinienausdrücke (erweiterte Richtlinienausdrücke) in den Richtlinien, die an unterstützte Module wie Web Application Firewall und Responder gebunden sind. Im Folgenden finden Sie zwei Beispiele,

die Ausdrücke zeigen, mit denen festgestellt werden kann, ob die Client-IP-Adresse bösartig ist.

1. **CLIENT.IP.SRC.IPREP_IS_MALICIOUS**: Dieser Ausdruck wird als TRUE ausgewertet, wenn der Client in die Liste der böswilligen IP-Adressen aufgenommen wurde.
2. **CLIENT.IP.SRC.IPREP_THREAT_CATEGORY (CATEGORY)**: Dieser Ausdruck wird als TRUE ausgewertet, wenn die Client-IP böswillige IP ist und zur angegebenen Bedrohungskategorie gehört.
3. **CLIENT.IPV6.SRC.IPREP_IS_MALICIOUS und CLIENT.IPV6.SRC.IPREP_THREAT_CATEGORY**: Dieser Ausdruck wird als TRUE ausgewertet, wenn die Client-IP vom Typ IPv6 ist und es sich um eine bösartige IP-Adresse in einer angegebenen Bedrohungskategorie handelt.

Im Folgenden sind die möglichen Werte für die Bedrohungskategorie:

SPAM_SOURCES, WINDOWS_EXPLOITS, WEB_ATTACKS, BOTNETS, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, CLOUD_PROVIDERS, MOBILE_THREATS, TOR_PROXY.

> **Hinweis:**
>
> Die IP-Reputationsfunktion prüft sowohl Quell- als auch Ziel-IP-Adressen. Es erkennt böswillige IPs im Header. Wenn der PI-Ausdruck in einer Richtlinie die IP-Adresse identifizieren kann, bestimmt die IP-Reputationsprüfung, ob sie bösartig ist.

iPrep Protokollnachricht. Die `/var/log/iprep.log` Datei enthält nützliche Nachrichten, die Informationen über die Kommunikation mit der Webroot-Datenbank erfassen. Die Informationen können sich auf die während der Webrootkommunikation verwendeten Anmeldeinformationen beziehen, die fehlende Verbindung mit Webroot, Informationen, die in einem Update enthalten sind (z. B. die Anzahl der IP-Adressen in der Datenbank).

Erstellen einer Sperrliste oder einer Allowlist von IPs unter Verwendung eines Richtliniendatensatzes. Sie können eine Positivliste verwalten, um den Zugriff auf bestimmte IP-Adressen zu ermöglichen, die in der Webroot-Datenbank blockiert sind. Sie können auch eine angepasste Sperrliste von IP-Adressen erstellen, um die Reputationsprüfung von Webroot zu ergänzen. Diese Listen können mithilfe eines **Richtliniendatensatzes**erstellt werden. Ein Datensatz ist eine spezielle Form von Mustersatz, der sich ideal für den IPv4- oder IPv6-Adressenabgleich eignet. Um Datensätze zu verwenden, erstellen Sie zuerst den Datensatz und binden Sie IPv4- oder IPv6-Adressen daran. Verwenden Sie beim Konfigurieren einer Richtlinie zum Vergleichen einer Zeichenfolge in einem Paket einen entsprechenden Operator und übergeben Sie den Namen des Mustersatzes oder Datensatzes als Argument.

So erstellen Sie eine Positivliste von Adressen, die während der IP-Reputationsbewertung als Ausnahmen behandelt werden sollen:

- Konfigurieren Sie die Richtlinie so, dass der PI-Ausdruck auf False ausgewertet wird, selbst wenn eine Adresse in der Positivliste von Webroot (oder einem Dienstanbieter) als bösartig aufgeführt wird.

IP-Reputation aktivieren oder deaktivieren. Die IP-Reputation ist Teil der allgemeinen Reputationsfunktion, die lizenzbasiert ist. Wenn Sie die Reputationsfunktion aktivieren oder deaktivieren, wird die IP-Reputation aktiviert oder deaktiviert.

Allgemeines Verfahren. Die Bereitstellung von IP-Reputation umfasst die folgenden Aufgaben:

- Stellen Sie sicher, dass die auf der NetScaler-Appliance installierte Lizenz IP-Reputationsunterstützung bietet. Premium- und Standalone-Anwendungsfirewall-Lizenzen unterstützen die IP-Reputationsfunktion.
- Aktivieren Sie die Funktionen für IP-Reputation und Anwendungsfirewall.
- Fügen Sie ein Anwendungs-Firewall-Profil hinzu.
- Fügen Sie mithilfe der PI-Ausdrücke eine Anwendungsfirewall-Richtlinie hinzu, um die böswilligen IP-Adressen in der IP-Reputation-Datenbank zu identifizieren.
- Binden Sie die Anwendungsfirewall-Richtlinie an einen entsprechenden Bindepunkt.
- Stellen Sie sicher, dass jede Anfrage von einer böswilligen Adresse in der `ns.log` Datei protokolliert wird, um anzuzeigen, dass die Anforderung wie im Profil angegeben verarbeitet wurde.

Konfigurieren Sie die IP-Reputationsfunktion über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

- `enable feature reputation`
- `disable feature reputation`

Die folgenden Beispiele zeigen, wie Sie mithilfe des PI-Ausdrucks eine Anwendungsfirewall-Richtlinie hinzufügen können, um schädliche Adressen zu identifizieren. Sie können die integrierten Profile verwenden, ein Profil hinzufügen oder ein vorhandenes Profil konfigurieren, um die gewünschte Aktion aufzurufen, wenn eine Anforderung mit einer Richtlinienübereinstimmung übereinstimmt.

Beispiele 3 und 4 zeigen, wie ein Richtlinien-Dataset erstellt wird, um eine Sperrliste oder eine Positivliste von IP-Adressen zu generieren.

Beispiel 1:

Der folgende Befehl erstellt eine Richtlinie, die böswillige IP-Adressen identifiziert und die Anforderung blockiert, wenn eine Übereinstimmung ausgelöst wird:

```
add appfw policy pol1 CLIENT.IP.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
add appfw policy pol1 CLIENT.IPv6.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
add appfw policy pol1 "HTTP.REQ.HEADER(\"X-Forwarded-For\").TYPECAST_IPv6_ADDRESS_AT
.IPREP_IS_MALICIOUS"APPFW_RESET
```

Beispiel 2:

Der folgende Befehl erstellt eine Richtlinie, die den Reputationsdienst verwendet, um die Client-IP-Adresse im `X-Forwarded-For` Header zu überprüfen und die Verbindung zurückzusetzen, wenn eine Übereinstimmung ausgelöst wird.


```
> add appfw policy pol1 "HTTP.REQ.HEADER(\"X-Forwarded-For\").TYPECAST_IP_ADDRESS_AT
.IPREP_IS_MALICIOUS"APPFW_RESET**
```

Beispiel 3:

Das folgende Beispiel zeigt, wie eine Liste hinzugefügt wird, um Ausnahmen hinzuzufügen, die bestimmte IP-Adressen zulassen:

```
> add policy dataset Allow_list1 ipv4
> bind policy dataset Allow_list1 10.217.25.17 -index 1
> bind policy dataset Allow_list1 10.217.25.18 -index 2
```

Das folgende Beispiel zeigt, wie eine Liste hinzugefügt wird, um Ausnahmen hinzuzufügen, die angegebene IPv6-Adressen zulassen:

```
add policy dataset Allow_list_ipv6 ipv6
bind policy dataset Allow_list_ipv6 fe80::98c7:d8ff:fe3a:b562 -index 1
bind policy dataset Allow_list_ipv6 fe80::98c7:d8ff:fe3a:b563  -index 2

<!--NeedCopy-->
```

Beispiel 4:

Das folgende Beispiel zeigt, wie die angepasste Liste hinzugefügt wird, um bestimmte IP-Adressen als bösartig zu kennzeichnen:

```
> add policy dataset Block_list1 ipv4
> bind policy dataset Block_list1 10.217.31.48 -index 1
> bind policy dataset Block_list1 10.217.25.19 -index 2
```

Das folgende Beispiel zeigt, wie die angepasste Liste hinzugefügt wird, um angegebene IPv6-Adressen als bösartig zu kennzeichnen.

```
add policy dataset Block_list_ipv6 ipv6
bind policy dataset Block_list_ipv6 fe80::98c7:d8ff:ff3b:b562 -index 1
bind policy dataset Block_list_ipv6 fe80::ffc7:d8ff:fe3a:b562 -index 2
<!--NeedCopy-->
```

Beispiel 5:

Das folgende Beispiel zeigt einen Richtlinienausdruck, um die Client-IP unter den folgenden Bedingungen zu blockieren:

- Es stimmt mit einer in der benutzerdefinierten Block_List1 konfigurierten IP-Adresse überein (Beispiel 4)

- Sie stimmt mit einer in der Webroot-Datenbank aufgelisteten IP-Adresse überein, es sei denn, sie wird durch die Aufnahme in die allow_List1 gelockert (Beispiel 3).

```
> add appfw policy "Ip_Rep_Policy" "((CLIENT.IP.SRC.IPREP_IS_MALICIOUS
    || CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Block_list1")) && ! (
    CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("Allow_list1")))"
    APPFW_BLOCK
<!--NeedCopy-->
```

Das folgende Beispiel zeigt einen Richtlinienausdruck zum Blockieren des Clients IPv6 unter den folgenden Bedingungen:

1. Es stimmt mit einer im angepassten Block_List_IPv6 konfigurierten IPv6-Adresse überein (Beispiel 4)
2. Es stimmt mit einer in der Webroot-Datenbank aufgeführten IPv6-Adresse überein, sofern sie nicht durch die Aufnahme in Allow_List_IPv6 (Beispiel 3) gelockert wurde.

```
add appfw policy "Ip_Rep_v6_Policy" "((CLIENT.IPV6.SRC.
    IPREP_IS_MALICIOUS || CLIENT.IPV6.SRC.TYPECAST_TEXT_T.CONTAINS_ANY("
    Block_list_ipv6")) && ! (CLIENT.IPV6.SRC.TYPECAST_TEXT_T.
    CONTAINS_ANY("Allow_list_ipv6")))" APPFW_BLOCK
<!--NeedCopy-->
```

Verwenden des Proxyservers:

Wenn die NetScaler-Appliance keinen direkten Zugriff auf das Internet hat und mit einem Proxy verbunden ist, konfigurieren Sie den IP-Reputation-Client so, dass er Anfragen an den Proxy sendet.

Konfigurieren Sie einen Proxy-Benutzernamen und ein Passwort auf dem Proxyserver für eine zusätzliche Sicherheitsebene für Ihre Appliance.

Geben Sie in der Befehlszeile Folgendes ein:

```
set reputation settings -proxyServer <proxy server ip> -proxyPort <proxy
server port> -proxyUsername <username> -proxyPassword <password>
```

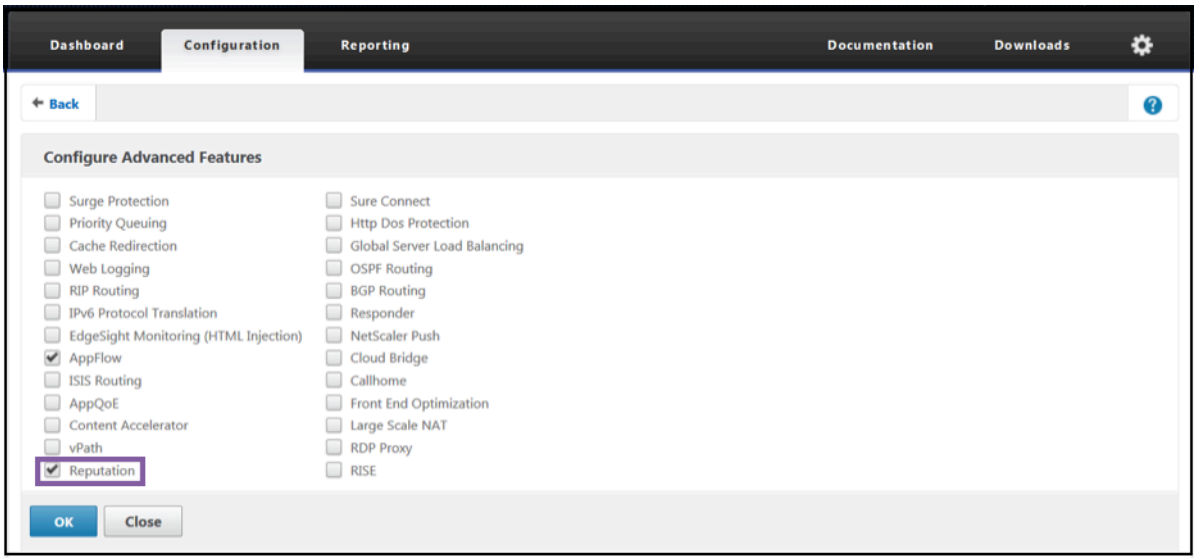
Beispiel:

```
> set reputation settings proxyServer 10.102.30.112 proxyPort 3128 -proxyUsername
 defaultusername -proxyPassword defaultpassword

> set reputation settings -proxyServer testproxy.citrite.net -proxyPort 3128
 -proxyUsername defaultusername -proxyPassword defaultpassword

> unset reputation settings -proxyserver -proxyport -proxyUsername -proxyPassword


> sh reputation settings
```


> **Hinweis:**
>
> Die Proxy-Server-IP kann eine IP-Adresse oder ein vollqualifizierter Domänenname (FQDN) sein.

Konfigurieren Sie die IP-Reputation über die NetScaler-GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie im Abschnitt **Modi und Funktionen** auf den Link, um auf den Bereich **Erweiterte Funktionen konfigurieren** zuzugreifen und das Kontrollkästchen **Reputation** zu aktivieren.
2. Klicken Sie auf **OK**.

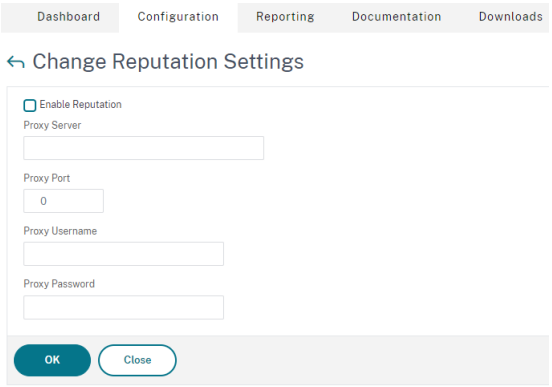


So konfigurieren Sie einen Proxyserver über die NetScaler GUI

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Sicherheit > Reputation**.
2. Klicken Sie unter **Einstellungen**auf **Reputationseinstellungen ändern**, um einen Proxyserver zu konfigurieren.
3. Aktiviere oder deaktiviere die Reputationsfunktion.
4. Geben Sie die folgenden Details ein, um den Proxyserver zu konfigurieren:
   a) **Proxyserver** — Dies kann eine IP-Adresse oder ein vollqualifizierter Domänenname (FQDN) sein.
   b) **Proxy-Port** — Er akzeptiert Werte zwischen [1—65535].
   c) **Proxy-Benutzername** — Geben Sie einen Benutzernamen für die Proxy-Serverauthentifizierung ein.
   d) **Proxykennwort** — Geben Sie ein Passwort für die Proxy-Serverauthentifizierung ein.

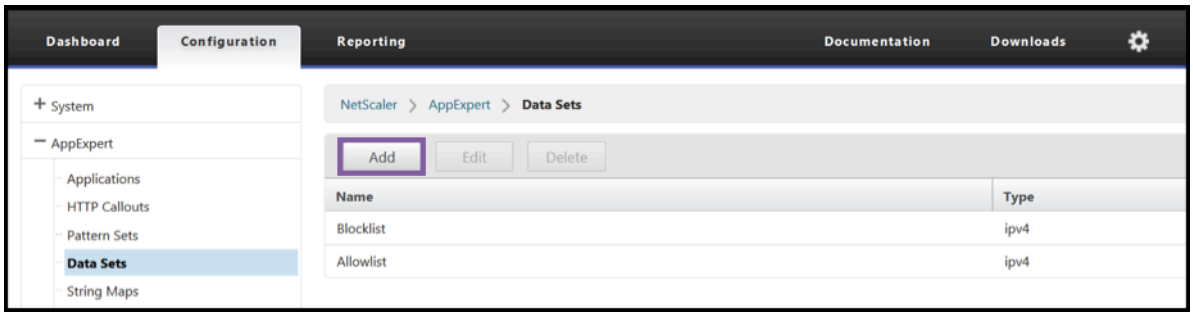
      > **Hinweis:**
      >
      > Die Felder ProxyUserName und ProxyPassword sind aktiviert, wenn die Felder Proxy-

> Server und ProxyPort konfiguriert sind.

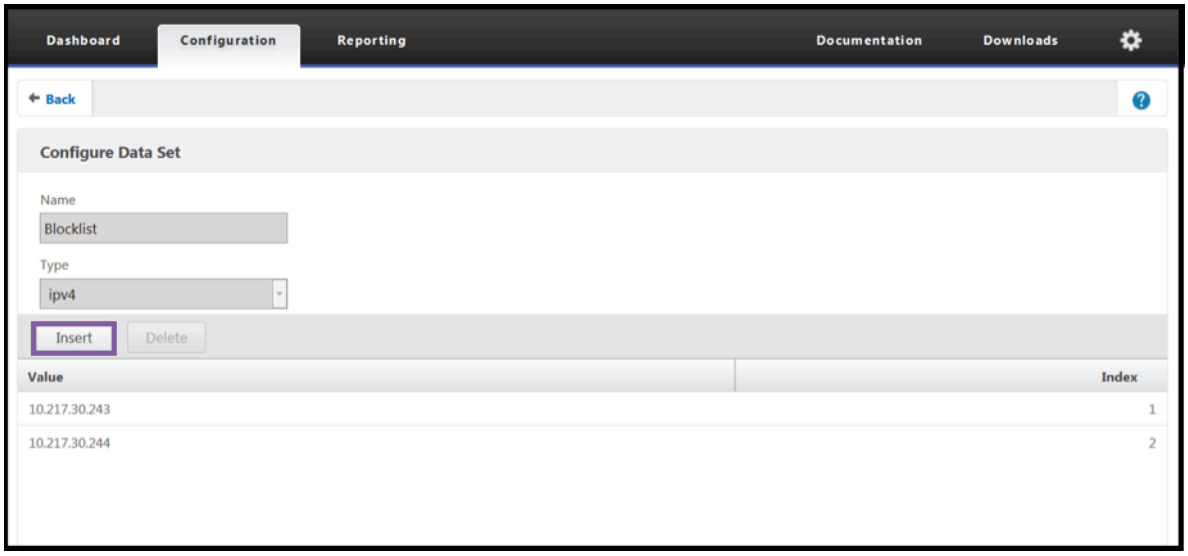


Erstellen Sie über die GUI eine Positivliste und eine Sperrliste von Client-IP-Adressen

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **AppExpert > Datensätze**.
2. Klicken Sie auf **Hinzufügen**.



- Geben **Sie im Bereich Datensatz erstellen** (oder **Datensatz konfigurieren**) einen aussagekräftigen Namen für die Liste der IP-Adressen an. Der Name muss den Zweck der Liste widerspiegeln.
- Wählen Sie **Typ** als **IPv4** oder **IPv6**.
- Klicken Sie auf **Einfügen**, um einen Eintrag hinzuzufügen.



- Fügen **Sie im Bereich Richtlinien-Dataset-Bindung konfigurieren** eine IP-Adresse im IPv4- oder IPv6-Format in das Eingabefeld Wert ein.
- Stellen Sie einen Index bereit.
- Fügen Sie einen Kommentar hinzu, der den Zweck der Liste erklärt. Dieser Schritt ist optional, wird jedoch empfohlen, da ein beschreibender Kommentar bei der Verwaltung der Liste hilfreich ist.

Auf ähnliche Weise können Sie eine Sperrliste erstellen und die IP-Adressen hinzufügen, die als bösartig angesehen werden sollen.

Weitere Informationen zur Verwendung von Datensätzen und zum Konfigurieren erweiterter Richtlinienausdrücke finden Sie unter Mustersätze und Datensätze.

Konfigurieren einer Anwendungs-Firewall-Richtlinie über die NetScaler GUI

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Sicherheit > Anwendungsfirewall > Richtlinien > Firewall**. Klicken Sie auf **Hinzufügen**, um mithilfe der PI-Ausdrücke eine Richtlinie hinzuzufügen, um die IP-Reputation zu verwenden.

Sie können auch den Ausdruckseditor verwenden, um Ihren eigenen Richtlinienausdruck zu erstellen. Die Liste zeigt vorkonfigurierte Optionen, die für die Konfiguration eines Ausdrucks mithilfe der Bedrohungskategorien nützlich sind.

Highlights

- Stoppen Sie schnell und genau schlechten Datenverkehr am Netzwerkrand von bekannten bösartigen IP-Adressen, die verschiedene Arten von Bedrohungen darstellen. Sie können die Anfrage blockieren, ohne den Text zu analysieren.
- Konfigurieren Sie dynamisch die IP-Reputationsfunktion für mehrere Anwendungen.

- Schützen Sie Ihr Netzwerk ohne Leistungseinbußen vor Datenverletzungen und konsolidieren Sie den Schutz mithilfe schneller und einfacher Bereitstellungen auf einer einzigen Services-Fabric.
- Sie können IP-Reputationsprüfungen für Quell- und Ziel-IPs durchführen.
- Sie können die Header auch überprüfen, um schädliche IPs zu erkennen.
- Die IP-Reputationsprüfung wird sowohl bei Forward-Proxy- als auch bei Reverse-Proxy-Bereitstellungen unterstützt.
- Der IP-Reputationsprozess stellt eine Verbindung zu Webroot her und aktualisiert die Datenbank alle 5 Minuten.
- Jeder Knoten in der High Availability (HA) oder Clusterbereitstellung erhält die Datenbank von Webroot.
- Die IP-Reputationsdaten werden von allen Partitionen in Admin-Partitions-Bereitstellungen gemeinsam genutzt.
- Sie können einen AppExpert-Datensatz verwenden, um Listen von IP-Adressen zu erstellen und Ausnahmen für IPs hinzuzufügen, die in der Webroot Datenbank blockiert sind. Sie können auch Ihre eigene angepasste Sperrliste erstellen, um bestimmte IPs als bösartig zu kennzeichnen.
- Die Datei iprep.db wird im `/var/nslog/iprep` Ordner erstellt. Nach der Erstellung wird es nicht gelöscht, auch wenn das Feature deaktiviert ist.
- Wenn die Reputationsfunktion aktiviert ist, wird die NetScaler Webroot Datenbank heruntergeladen. Danach wird es alle 5 Minuten aktualisiert.
- Die Hauptversion der Webroot Datenbank ist Version: 1.
- Die Nebenversion wird jeden Tag aktualisiert. Die Update-Version wird alle 5 Minuten erhöht und auf 1 zurückgesetzt, wenn die Nebenversion erhöht wird.
- PI-Ausdrücke ermöglichen es Ihnen, die IP-Reputation mit anderen Funktionen wie Responder und Rewrite zu verwenden.
- Die IP-Adressen in der Datenbank sind in Dezimalschreibweise.

Tipps zum Debuggen

- Wenn Sie die Reputationsfunktion in der GUI nicht sehen können, überprüfen Sie, ob Sie über die richtige Lizenz verfügen.
- Überwachen Sie die Nachrichten `var/log/iprep.log` zum Debuggen.
- **Webrootkonnektivität**: Wenn die `ns iprep: Not able to connect/resolve WebRoot` Meldung angezeigt wird, stellen Sie sicher, dass die Appliance über einen Internetzugang verfügt und DNS konfiguriert ist.
- **Proxyserver**: Wenn die `ns iprep: iprep_curl_download: 88 curl_easy_perform failed. Error code: 5 Err msg:couldnt resolve proxy name` Meldung angezeigt wird, stellen Sie sicher, dass die Proxy-Serverkonfiguration korrekt ist.
- **IP-Reputationsfunktion funktioniert nicht**: Der IP-Reputationsprozess dauert etwa fünf Minuten, nachdem Sie die Reputationsfunktion aktiviert haben. Die IP-Reputationsfunktion

funktioniert möglicherweise für diese Dauer nicht.

- **Datenbankdownload**: Wenn der Download von IP-DB-Daten nach dem Aktivieren der IP-Reputationsfunktion fehlschlägt, wird der folgende Fehler in den Protokollen angezeigt.

```
iprep: iprep_curl_download:86 curl_easy_perform failed. Error code:7 Err
msg:Couldn't connect to server
```

Lösung: Zulassen Sie den ausgehenden Datenverkehr zu den folgenden URLs, oder konfigurieren Sie einen Proxy, um das Problem zu beheben.

```
localdb-ip-daily.brightcloud.com:443
localdb-ip-rtu.brightcloud.com:443
api.bcti.brightcloud.com:443
<!--NeedCopy-->
```

SSL-Offload und Beschleunigung

May 11, 2023

Eine NetScaler-Appliance, die für die SSL-Beschleunigung konfiguriert ist, beschleunigt SSL-Transaktionen auf transparente Weise, indem sie die SSL-Verarbeitung vom Server auslagert. Um SSL-Offloading zu konfigurieren, konfigurieren Sie einen virtuellen Server, der SSL-Transaktionen abfängt und verarbeitet und den entschlüsselten Datenverkehr an den Server sendet (es sei denn, Sie konfigurieren eine Ende-zu-Ende-Verschlüsselung, in diesem Fall wird der Datenverkehr erneut verschlüsselt). Nach Erhalt der Antwort vom Server schließt die Appliance die sichere Transaktion mit dem Client ab. Aus Sicht des Kunden scheint die Transaktion direkt mit dem Server abzuwickeln. Ein für die SSL-Beschleunigung konfigurierter NetScaler führt auch andere konfigurierte Funktionen aus, z. B. den Lastenausgleich.

Für die Konfiguration von SSL-Offloading sind ein SSL-Zertifikat und ein Schlüsselpaar erforderlich, die Sie erwerben müssen, falls Sie noch kein SSL-Zertifikat besitzen. Zu den weiteren SSL-bezogenen Aufgaben, die Sie möglicherweise ausführen müssen, gehören die Verwaltung von Zertifikaten, die Verwaltung von Zertifikatssperrlisten, die Konfiguration der Clientauthentifizierung und die Verwaltung von SSL-Aktionen und -Richtlinien.

Eine Nicht-FIPS-NetScaler Appliance speichert den privaten Schlüssel des Servers auf der Festplatte. Auf einer FIPS-Appliance wird der Schlüssel in einem kryptografischen Modul gespeichert, das als Hardware-Sicherheitsmodul (HSM) bekannt ist.

Alle NetScaler-Appliances, die keine FIPS-Karte unterstützen (einschließlich virtueller Appliances), unterstützen die externen HSMs Thales nShield® Connect und SafeNet. (MPX 9700/10500/12500/15500-Appliances unterstützen kein externes HSM.)

Hinweis: FIPS-bezogene Optionen für einige der in diesem Dokument beschriebenen SSL-Konfigurationsverfahren sind spezifisch für eine FIPS-fähige NetScaler Appliance.

SSL-Offload-Konfiguration

August 15, 2023

Um das SSL-Offloading zu konfigurieren, müssen Sie die SSL-Verarbeitung auf der NetScaler-Appliance aktivieren und einen SSL-basierten virtuellen Server konfigurieren. Der virtuelle Server fängt SSL-Verkehr ab, entschlüsselt den Datenverkehr und leitet ihn an einen Dienst weiter, der an den virtuellen Server gebunden ist. Um zeitkritischen Datenverkehr wie Medienstreaming zu sichern, können Sie einen virtuellen DTLS-Server konfigurieren. Um das SSL-Offloading zu aktivieren, müssen Sie ein gültiges Zertifikat und einen gültigen Schlüssel importieren und das Paar an den virtuellen Server binden.

> **Hinweis**
>
> Ab Version 13.1 Build 17.x sind Protokolle niedriger als TLSv1.2 in den internen SSL-Diensten deaktiviert. Wenn das (erweiterte) Standardprofil aktiviert ist, ist das Profil `ns_default_ssl_profile_internal_frontend_service` an die internen SSL-Dienste gebunden und die Protokolle SSLv3, TLSv1.0 und TLSv1.1 sind im Profil deaktiviert.

SSL aktivieren

Um SSL-Verkehr zu verarbeiten, müssen Sie die SSL-Verarbeitung aktivieren. Sie können SSL-basierte Entitäten wie virtuelle Server und Dienste konfigurieren, ohne die SSL-Verarbeitung zu aktivieren. Sie funktionieren jedoch erst, wenn die SSL-Verarbeitung aktiviert ist.

SSL-Verarbeitung über die CLI aktivieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature ssl

show ns feature
<!--NeedCopy-->
```

Beispiel:

```
enable ns feature SSL
 Done
show ns feature
```



```
4
5          Feature                        Acronym              Status
6          -------                        -------              ------
7   1)     Web Logging                    WL                   OFF
8   2)     Surge Protection               SP                   ON
9   3)     Load Balancing                 LB                   ON
10  .
11  .
12  .
13  9)     SSL Offloading                 SSL                  ON
14  .
15  .
16  .
17  24)    NetScaler Push                 push                 OFF
18  Done
19 <!--NeedCopy-->
```

SSL-Verarbeitung über die GUI aktivieren

Navigieren Sie zu **System > Einstellungen**, und klicken Sie in der Gruppe **Modi und Funktionen** auf **Grundfunktionen konfigurieren**, und klicken Sie auf **SSL-Offloading**.

Konfigurieren von Diensten

Auf der NetScaler-Appliance stellt ein Dienst einen physischen Server oder eine Anwendung auf einem physischen Server dar. Nach der Konfiguration befinden sich Dienste im deaktivierten Zustand, bis die Appliance den physischen Server im Netzwerk erreichen und seinen Status überwachen kann.

Hinzufügen eines Dienstes über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Dienst hinzuzufügen und die Konfiguration zu überprüfen:

```
1 add service <name> (<IP> | <serverName>) <serviceType> <port>
2 show service <serviceName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add service sslsvc 198.51.100.225 SSL 443
2
3 Done
4
```



```
sh ssl service sslsvc

            Advanced SSL configuration for Back-end SSL Service sslsvc:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Server Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: ???
            DHE Key Exchange With PSK: ???
            Tickets Per Authentication Context: ???

            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT_BACKEND
            Description: Default cipher list for Backend SSL session
     Done
<!--NeedCopy-->
```

Ändern oder entfernen Sie einen Dienst über die CLI

Um einen Dienst zu ändern, verwenden Sie den Befehl set service. Dies entspricht genau dem Befehl add service, außer dass Sie den Namen eines vorhandenen Dienstes eingeben.

Um einen Dienst zu entfernen, verwenden Sie den Befehl rm service, der nur das <name> -Argument akzeptiert.

```
rm service <servicename>
<!--NeedCopy-->
```

Beispiel:

```
rm service sslsvc
```



```
<!--NeedCopy-->
```

Um einen Dienst zu ändern, verwenden Sie den Befehl set service, wählen Sie einen beliebigen Parameter aus und ändern Sie seine Einstellung.

```
set service <name> (<IP> | <serverName>) <serviceType> <port>
<!--NeedCopy-->
```

Beispiel:

```
set service sslsvc 198.51.100.225 SSL 443
<!--NeedCopy-->
```

Konfigurieren Sie einen Dienst über die GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, erstellen Sie einen Service und geben Sie das Protokoll als SSL an.

Virtuelle SSL-Serverkonfiguration

Für sichere Sitzungen muss eine Verbindung zwischen dem Client und einem SSL-basierten virtuellen Server auf der NetScaler-Appliance hergestellt werden. Der virtuelle SSL-Server fängt den SSL-Verkehr ab, entschlüsselt ihn und verarbeitet ihn, bevor er an Dienste gesendet wird, die an den virtuellen Server gebunden sind.

Hinweis: Der virtuelle SSL-Server wird auf der NetScaler-Appliance als heruntergefahren markiert, bis ein gültiges Zertifikat-/Schlüsselpaar und mindestens ein Dienst daran gebunden sind. Ein SSL-basierter virtueller Server ist ein virtueller Lastausgleichsserver vom Protokolltyp SSL oder SSL_TCP. Die Lastausgleichsfunktion muss auf der NetScaler-Appliance aktiviert sein.

Fügen Sie über die CLI einen SSL-basierten virtuellen Server hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen SSL-basierten virtuellen Server zu erstellen und die Konfiguration zu überprüfen:

```
add lb vserver <name> (serviceType) <IPAddress> <port>
show ssl vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver sslvs SSL 192.0.2.240 443
Done
```



```
3
4  sh ssl vserver sslvs
5
6              Advanced SSL configuration for VServer sslvs:
7              DH: DISABLED
8              DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                   RSA: ENABLED          Refresh Count: 0
9              Session Reuse: ENABLED          Timeout: 120 seconds
10             Cipher Redirect: DISABLED
11             SSLv2 Redirect: DISABLED
12             ClearText Port: 0
13             Client Auth: DISABLED
14             SSL Redirect: DISABLED
15             Non FIPS Ciphers: DISABLED
16             SNI: DISABLED
17             OCSP Stapling: DISABLED
18             HSTS: DISABLED
19             HSTS IncludeSubDomains: NO
20             HSTS Max-Age: 0
21             SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                    ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
22             Push Encryption Trigger: Always
23             Send Close-Notify: YES
24             Strict Sig-Digest Check: DISABLED
25             Zero RTT Early Data: DISABLED
26             DHE Key Exchange With PSK: NO
27             Tickets Per Authentication Context: 1
28             ECC Curve: P_256, P_384, P_224, P_521
29
30     1)      Cipher Name: DEFAULT
31             Description: Default cipher list with encryption strength
                   >= 128bit
32      Done
33 <!--NeedCopy-->
```

Ändern oder entfernen Sie einen SSL-basierten virtuellen Server über die CLI

Verwenden Sie den Befehl `set lb vserver` um die Lastausgleichseigenschaften eines virtuellen SSL-Servers zu ändern. Der Befehl set ähnelt dem Befehl `add lb vserver`, außer dass Sie den Namen eines vorhandenen virtuellen Servers eingeben. Um die **SSL-Eigenschaften** eines SSL-basierten virtuellen Servers zu ändern, verwenden Sie den Befehl `set ssl vserver`. Weitere Informationen finden Sie im Abschnitt “Virtuelle SSL-Server-Parameter” weiter unten auf dieser Seite.

Um einen virtuellen SSL-Server zu entfernen, verwenden Sie den Befehl `rm lb vserver`, der nur das

Argument <name> akzeptiert.

Konfigurieren eines SSL-basierten virtuellen Servers über die GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, erstellen Sie einen virtuellen Server und geben Sie das Protokoll als SSL an.

Binden Sie Dienste an den virtuellen SSL-Server

Die ADC-Appliance leitet entschlüsselte SSL-Daten an Server im Netzwerk weiter. Um Daten weiterzuleiten, müssen Dienste, die diese physischen Server darstellen, an den virtuellen Server gebunden sein, der die SSL-Daten empfängt.

In der Regel ist die Verbindung zwischen der ADC-Appliance und dem physischen Server sicher. Daher muss die Datenübertragung zwischen der Appliance und dem physischen Server nicht verschlüsselt werden. Sie können jedoch End-to-Ende-Verschlüsselung bereitstellen, indem Sie die Datenübertragung zwischen der Appliance und dem Server verschlüsseln. Einzelheiten finden Sie unter Konfigurieren von SSL-Offloading mit Ende-zu-Ende-Verschlüsselung.

Hinweis: Aktivieren Sie die Lastenausgleichsfunktion auf der ADC-Appliance, bevor Sie Dienste an den SSL-basierten virtuellen Server binden.

Binden eines Dienstes an einen virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Dienst an den virtuellen Server zu binden und die Konfiguration zu überprüfen:

```
bind lb vserver <name> <serviceName>
show lb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver sslvs sslsvc
     Done

sh lb vserver sslvs

            sslvs (192.0.2.240:443) - SSL       Type: ADDRESS
            State: DOWN[Certkey not bound]
            Last state change was at Wed May  2 11:43:04 2018
            Time since last state change: 0 days, 00:13:21.150
            Effective State: DOWN
            Client Idle Timeout: 180 sec
```



```
12              Down state flush: ENABLED
13              Disable Primary Vserver On Down : DISABLED
14              Appflow logging: ENABLED
15              No. of Bound Services :  1 (Total)       0 (Active)
16              Configured Method: LEASTCONNECTION      BackupMethod:
                   ROUNDROBIN
17              Mode: IP
18              Persistence: NONE
19              Vserver IP and Port insertion: OFF
20              Push: DISABLED  Push VServer:
21              Push Multi Clients: NO
22              Push Label Rule: none
23              L2Conn: OFF
24              Skip Persistency: None
25              Listen Policy: NONE
26              IcmpResponse: PASSIVE
27              RHIstate: PASSIVE
28              New Service Startup Request Rate: 0 PER_SECOND, Increment
                   Interval: 0
29              Mac mode Retain Vlan: DISABLED
30              DBS_LB: DISABLED
31              Process Local: DISABLE
32              Traffic Domain: 0
33              TROFS Persistence honored: ENABLED
34              Retain Connections on Cluster: NO
35      1) sslsvc (198.51.100.225: 443) - SSL State: DOWN       Weight: 1
36       Done
37  <!--NeedCopy-->
```

Trennen Sie einen Dienst über die CLI von einem virtuellen Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1  unbind lb vserver <name> <serviceName>
2  <!--NeedCopy-->
```

Beispiel:

```
1  unbind lb vserver sslvs sslsvc
2       Done
3  <!--NeedCopy-->
```


Binden Sie einen Dienst über die GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und klicken Sie im Abschnitt **Dienste und Dienstgruppen auf die Kachel Load Balancing Virtual Server ServiceBindings** .
3. Klicken Sie auf der Seite **Load Balancing Virtual Server Service Binding** auf die Registerkarte **Bindungen hinzufügen**, **klicken Sie auf Klicken, um** unter **Dienst auswählen**auszuwählen, und aktivieren Sie das Kontrollkästchen neben dem zu bindenden Dienst.
4. Klicken Sie auf **Auswählen** und dann auf **Binden**

Konfigurieren eines virtuellen Servers mit Servernamenangabe (SNI) für das sichere Hosting mehrerer Sites

Virtuelles Hosting wird von Webservern verwendet, um mehr als einen Domainnamen mit derselben IP-Adresse zu hosten. Die Appliance unterstützt das Hosting mehrerer sicherer Domänen, indem sie die SSL-Verarbeitung mithilfe transparenter SSL-Dienste oder virtueller serverbasierter SSL-Offloading von den Webservern auslagert. Wenn jedoch mehrere Sites auf demselben virtuellen Server gehostet werden, ist der SSL-Handshake abgeschlossen, bevor der erwartete Hostname an den virtuellen Server gesendet wird. Daher kann die Appliance nicht ermitteln, welches Zertifikat dem Client nach dem Herstellen einer Verbindung vorgelegt werden soll. Dieses Problem wird gelöst, indem SNI auf dem virtuellen Server aktiviert wird. SNI ist eine Transport Layer Security (TLS) -Erweiterung, die vom Client verwendet wird, um den Hostnamen während der Handshake-Initiierung anzugeben. Die ADC-Appliance vergleicht diesen Hostnamen mit dem allgemeinen Namen und vergleicht ihn, falls er nicht übereinstimmt, mit dem alternativen Antragstellernamen (SAN). Wenn der Name übereinstimmt, legt die Appliance dem Client das entsprechende Zertifikat vor.

Ein Wildcard-SSL-Zertifikat ermöglicht die SSL-Verschlüsselung für mehrere Subdomänen, wenn dieselbe Organisation diese Domänen kontrolliert und der Domainname der zweiten Ebene derselbe ist. Beispielsweise kann ein Wildcard-Zertifikat, das an ein Sportnetzwerk mit dem allgemeinen Namen “*.sports.net” ausgestellt wurde, verwendet werden, um Domänen wie “login.sports.net” und “help.sports.net” zu sichern. Die Domäne “login.ftp.sports.net” kann nicht gesichert werden.

Hinweis:
Auf einer ADC-Appliance werden nur DNS-Einträge für Domänenname, URL und E-Mail-ID im Feld **SAN** verglichen.

Mit der Option -SNICert können Sie mehrere Serverzertifikate an einen einzelnen virtuellen SSL-Server oder transparenten Dienst binden. Der virtuelle Server oder Dienst stellt diese Zertifikate aus, wenn SNI auf dem virtuellen Server oder Dienst aktiviert ist. Sie können SNI jederzeit aktivieren.

Binden Sie mehrere Serverzertifikate über die CLI an einen einzelnen virtuellen SSL-Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um SNI zu konfigurieren und die Konfiguration zu überprüfen:

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )]

bind ssl vserver <vServerName>@ -certkeyName <string> -SNICert

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Um mehrere Serverzertifikate über die CLI an einen transparenten Dienst zu binden, ersetzen Sie `vserver` in den vorhergehenden Befehlen durch den Dienst und `vservername` durch den Dienstnamen.

Hinweis: Erstellen Sie den SSL-Dienst mit der Option `-clearTextPort 80`.

Binden Sie mehrere Serverzertifikate über die GUI an einen einzelnen virtuellen SSL-Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen SSL-Server und wählen Sie unter **CertificatesServerzertifikat**aus.
3. Fügen Sie ein Zertifikat hinzu oder wählen Sie ein Zertifikat aus der Liste aus, und klicken Sie auf **Serverzertifikat für SNI**.
4. Wählen Sie in **den erweiterten EinstellungenSSL-Parameter**aus.
5. Klicken Sie auf **SNI Enable**.

Unterstützung für SNI im Back-End-Dienst

> **Hinweis**: SNI wird in einem DTLS-Back-End-Dienst nicht unterstützt.

Die NetScaler-Appliance unterstützt Server Name Indication (SNI) im Backend. Das heißt, der allgemeine Name wird als Servername im Client-Hallo an den Back-End-Server gesendet, damit der Handshake erfolgreich abgeschlossen werden kann. Diese Unterstützung trägt dazu bei, die Sicherheitsanforderungen von Systemintegratoren des Bundes zu SNI bietet außerdem den Vorteil, dass nur ein Port verwendet wird, anstatt Hunderte verschiedener IP-Adressen und Ports in einer Firewall zu öffnen.

Zu den Sicherheitsanforderungen des föderalen Systemintegrators gehört die Unterstützung von Active Directory Federation Services (ADFS) 3.0 in 2012 R2 und WAP-Servern. Um diese Anforderung zu erfüllen, ist die Unterstützung für SNI im Backend einer NetScaler-Appliance erforderlich.

> **Hinweis:**
>
> Damit SNI funktioniert, muss der Servername im Client-Hello mit dem Hostnamen übereinstimmen, der im Back-End-Dienst konfiguriert ist, der an einen virtuellen SSL-Server gebunden ist. Wenn der Hostname des Backend-Servers beispielsweise www.mail.example.com lautet, muss der SNI-fähige Back-End-Dienst mit dem Servernamen als konfiguriert werden https://www.mail.example.com. Und dieser Hostname muss mit dem Servernamen im Client Hello übereinstimmen.

Unterstützung für dynamisches SNI im Back-End-Dienst

Die NetScaler-Appliance unterstützt dynamisches SNI auf den Back-End-TLS-Verbindungen. Das heißt, die Appliance lernt den SNI in der Clientverbindung und verwendet ihn in der serverseitigen Verbindung. Sie müssen keinen allgemeinen Namen mehr im SSL-Dienst, in der Dienstgruppe oder im Profil angeben. Der in der SNI-Erweiterung der Client-Hello-Nachricht empfangene allgemeine Name wird an die Back-End-SSL-Verbindung weitergeleitet.

Zuvor mussten Sie statisches SNI für SSL-Dienste, Dienstgruppen und SSL-Profile konfigurieren. Daher wurde nur die konfigurierte statische SNI-Erweiterung an den Server gesendet. Wenn ein Client gleichzeitig auf mehrere Domänen zugreifen musste, konnte die ADC-Appliance das vom Client empfangene SNI nicht an den Back-End-Dienst senden. Stattdessen wurde der statische allgemeine Name gesendet, der konfiguriert wurde. Wenn der Back-End-Server jetzt für mehrere Domänen konfiguriert ist, kann der Server mit dem richtigen Zertifikat antworten, das auf dem SNI basiert, das in der Client-Hello-Nachricht von der Appliance empfangen wurde.

Zeigen Sie auf Hinweis:

- SNI muss auf dem Front-End aktiviert sein und das richtige SNI-Zertifikat muss an den virtuellen SSL-Server gebunden sein. Wenn Sie SNI im Front-End nicht aktivieren, werden die SNI-Informationen nicht an das Back-End weitergegeben.
- Wenn die Serverauthentifizierung aktiviert ist, wird das Serverzertifikat durch das CA-Zertifikat überprüft, und die allgemeinen Name/SAN-Einträge im Serverzertifikat werden mit dem SNI abgeglichen. Daher muss das CA-Zertifikat an den Dienst gebunden sein.
- Die Wiederverwendung der Back-End-Verbindung und der SSL-Sitzung basiert auf SNI, wenn dynamisches SNI aktiviert ist.

SSL-Monitore senden kein SNI, wenn dynamisches SNI aktiviert ist. Für SNI-basierte Sondierung fügen Sie ein Back-End-Profil an, auf dem statisches SNI für die SSL-Monitore konfiguriert ist. Der Monitor muss mit demselben benutzerdefinierten Header wie SNI konfiguriert werden.

Konfigurieren von SNI im Back-End-Dienst über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

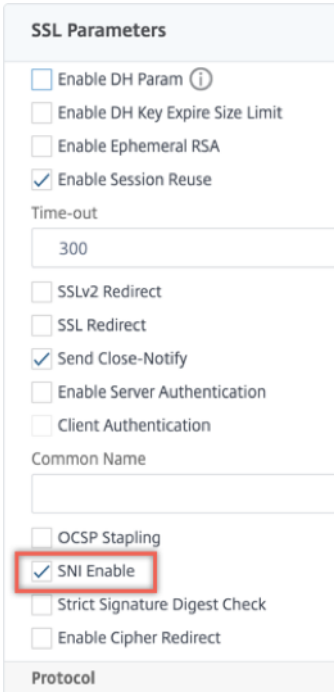
```
add service <name>  <IP>  <serviceType>  <port>

add lb vserver <name>  <IPAddress> <serviceType>  <port>

bind lb vserver <name> <serviceName>

set ssl service <serviceName> -SNIEnable ENABLED -commonName <string>

set ssl profile <name> -SNIEnable ENABLED
<!--NeedCopy-->
```

Beispiel:

```
    add service service_ssl 198.51.100.100 SSL 443

    add lb vserver ssl-vs 203.0.113.200 SSL 443

    bind lb vserver ssl-vs service_ssl

    set ssl service service_ssl -SNIEnable ENABLED  - commonName www.
       example.com

    set ssl profile sslprof -SNIEnable ENABLED
<!--NeedCopy-->
```

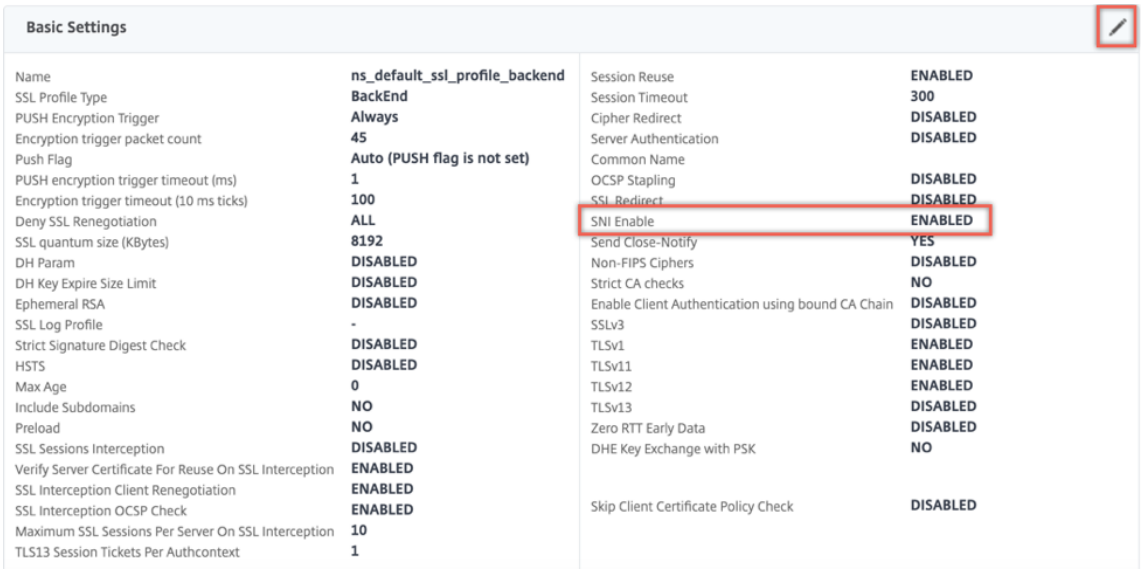
Konfigurieren Sie SNI im Back-End-Dienst über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Wählen Sie einen SSL-Dienst aus und klicken Sie in **Erweiterte Einstellungen**auf **SSL-Parameter**.
3. Klicken Sie auf **SNI Enable**.



Konfigurieren Sie SNI im SSL-Profil über die GUI

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie in **den GrundeinstellungenSNI-Aktivierung**aus.



4. Klicken Sie auf **OK**.

Binden Sie einen sicheren Monitor an einen SNI-fähigen Back-End-Dienst

Sie können sichere Monitore vom Typ HTTP, HTTP-ECV, TCP oder TCP-ECV an die Back-End-Dienste und Dienstgruppen binden, die SNI unterstützen. Die Monitor-Prüfpunkte senden jedoch nicht die SNI-Erweiterung, wenn dynamisches SNI aktiviert ist. Um SNI-Prüfungen zu senden, aktivieren Sie statisches SNI im Back-End-SSL-Profil und binden Sie das Profil an den Monitor. Stellen Sie den benutzerdefinierten Header im Monitor auf den Servernamen ein, der als SNI-Erweiterung im Client-Hello der Monitorprobe gesendet wird.

Konfigurieren und binden Sie einen sicheren Monitor über die CLI an einen SNI-fähigen Back-End-Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

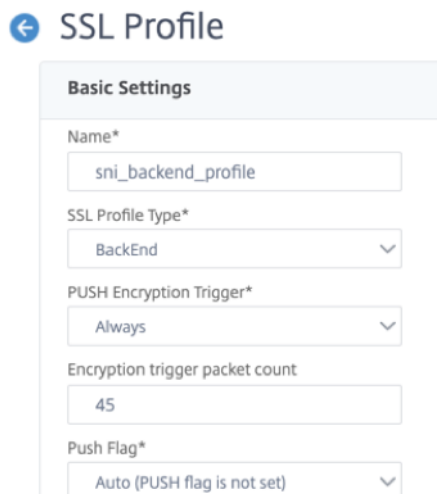
```
add lb monitor <monitorName> <type> -secure YES
add ssl profile <name> -sslProfileType BackEnd
set lb monitor <monitorName> <type> -customHeaders <string> -sslprofile
    <backend ssl profile>
set ssl profile <name> -sniEnable ENABLED -commonName <string>
bind service <name> -monitorName <string>
<!--NeedCopy-->
```

Beispiel:

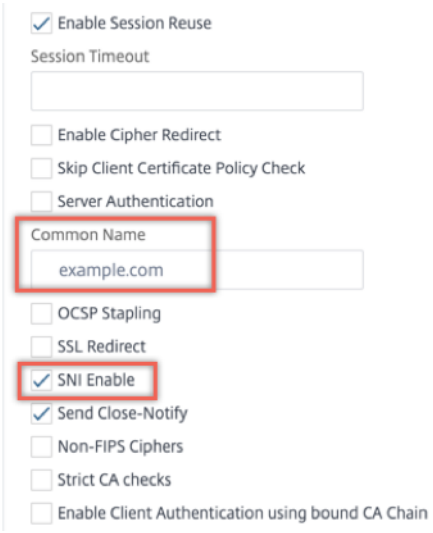
```
add ssl profile sni_backend_profile -sslProfileType BackEnd
set ssl profile sni_backend_profile -sniEnable ENABLED -commonName
   example.com
add lb monitor http-ecv-mon HTTP-ECV -secure YES
set monitor http-ecv-mon HTTP-ECV -customHeaders "Host: example.com\r\n
   " -sslprofile sni_backend_profile
bind service ssl_service  - monitorName http-ecv-mon
<!--NeedCopy-->
```

Konfigurieren und binden Sie einen sicheren Monitor über die GUI an einen SNI-fähigen Back-End-Dienst

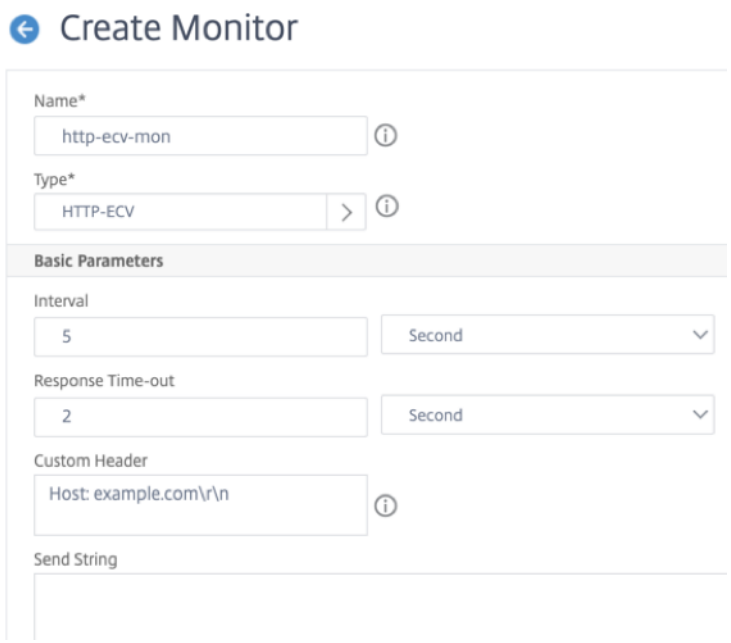
1. Navigieren Sie zu **System > Profile > SSL-Profile**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für das Profil an und wählen Sie **unter SSL-ProfiltypBackend**aus.



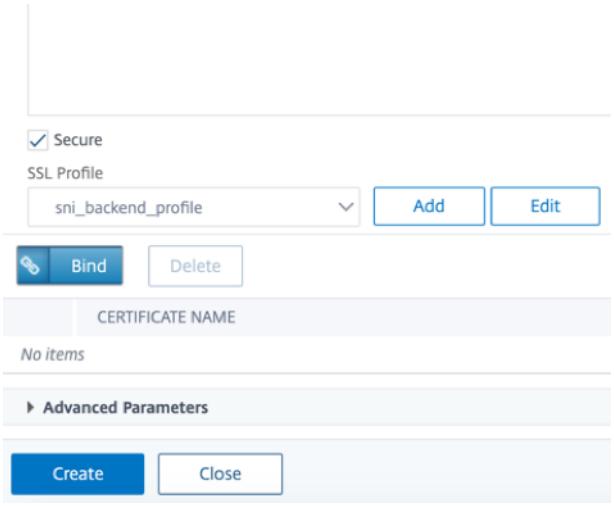
4. Geben Sie den allgemeinen Namen an (wie Host-Header) und wählen Sie **SNI-Aktivieren**.



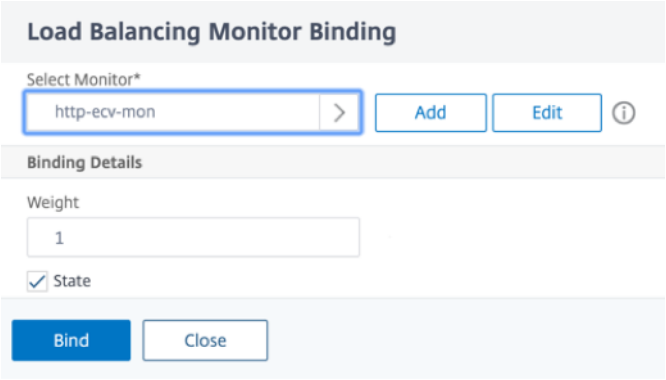
5. Klicken Sie auf **OK**.
6. Navigieren Sie zu **Traffic Management > Load Balancing > Monitor**.
7. Klicken Sie auf **Hinzufügen**.
8. Geben Sie einen Namen für den Monitor an. Wählen Sie unter **Typ**die Option HTTP, HTTP-ECV, TCP oder TCP-ECV aus.
9. Geben Sie einen **benutzerdefinierten Header**an.



10. Wählen Sie **Sicher**aus.
11. Wählen Sie im **SSL-Profil**das Back-End-SSL-Profil aus, das in den vorherigen Schritten erstellt wurde.
12. Klicken Sie auf **Erstellen**.



13. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
14. Wählen Sie einen SSL-Dienst und klicken Sie auf **Bearbeiten**.
15. Klicken Sie **unter Monitore**auf **Bindung hinzufügen**, wählen Sie den in den vorherigen Schritten erstellten Monitor aus und klicken Sie auf **Binden**.



Konfigurieren und binden Sie einen sicheren Monitor über die GUI an einen SNI-fähigen Back-End-Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitor**.
2. Fügen Sie einen Monitor vom Typ **HTTP-ECV** oder **TCP-ECV**hinzu und geben Sie einen **benutzerdefinierten Header**an.
3. Wählen Sie **Create**.
4. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
5. Wählen Sie einen SSL-Dienst und klicken Sie auf **Bearbeiten**.
6. Klicken Sie **unter Monitore**auf **Bindung hinzufügen**, wählen Sie den in Schritt 3 erstellten Monitor aus und klicken Sie auf **Binden**.

Erlaube, dass der Handshake für einen unbekannten Servernamen fortgesetzt wird

> **Hinweis**
>
> Diese Funktion ist in Version 13.1 Build 45.x und höher verfügbar.

Wenn SNI aktiviert ist und die NetScaler-Appliance ein Client-Hello mit einem unbekannten Servernamen empfängt, beendet sie den SSL-Handshake. Ab Version 13.1 Build 45.x ermöglicht die Appliance, dass der SSL-Handshake auch für einen unbekannten Servernamen fortgesetzt wird, und überlässt dem Client die Entscheidung, den Handshake zu beenden oder abzuschließen. Sie können diese Einstellung in einem Front-End-SSL-Profil konfigurieren, wenn SNI mithilfe des **`allowUnknownSNI` Parameters AKTIVIERT** ist.

Lassen Sie diesen Parameter deaktiviert, wenn Sie eine Weiterleitungsaktion für eine SNI-basierte Regel verwenden müssen. Sie haben beispielsweise SNI auf dem virtuellen Server v1 aktiviert und eine Richtlinie konfiguriert, um alle Anfragen für eine bestimmte Domain (www.example.com) an den virtuellen Server v2 weiterzuleiten. Bisher wurden alle Anfragen, die auf Version 1 für diese Domain eingehen, automatisch an Version 2 weitergeleitet. Wenn der `allowunknownSNI` Parameter jedoch aktiviert ist, wird die Anfrage auf v1 verarbeitet. Der Parameter muss deaktiviert sein, damit die Appliance die Anfrage auf v1 verarbeiten kann.

Konfigurieren Sie „Unbekanntes SNI zulassen“ mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

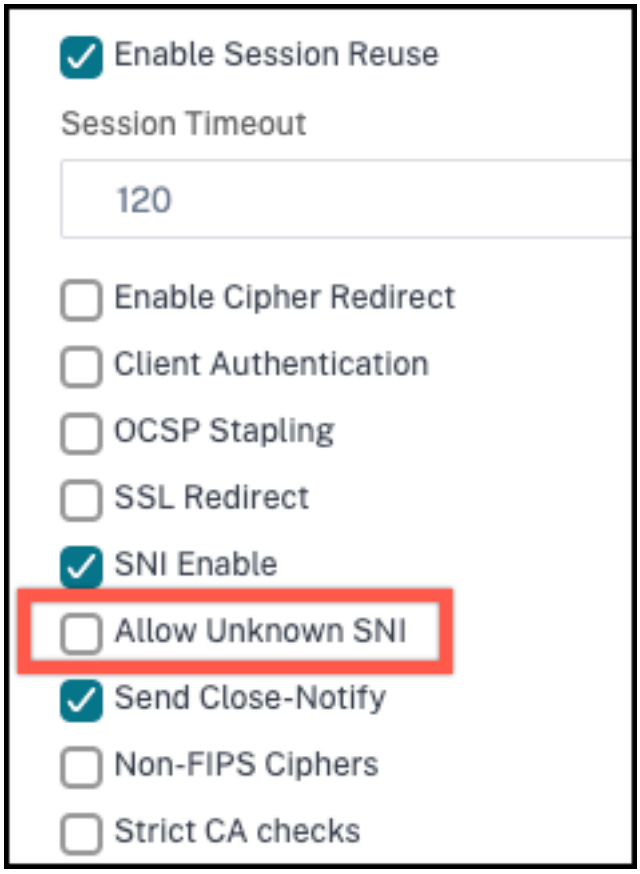
```
set ssl profile default_profile -SNIEnable Enabled -allowUnknownSNI <
DISABLED/ENABLED>
```

Der Parameter ‘allowUnknownsNI ist standardmäßig deaktiviert. Infolgedessen bricht die Appliance den Handshake für einen unbekannten Servernamen ab. Um diese Einstellung zu aktivieren, geben Sie Folgendes ein:

```
set ssl profile default_profile -SNIEnable Enabled -allowUnknownSNI ENABLED
```

Konfigurieren Sie „Unbekanntes SNI zulassen“ mithilfe der GUI

1. Navigieren Sie zu **System** > **Profile** > **SSL-Profil**.
2. Wenn Sie ein Profil hinzufügen, wählen Sie in der Liste **SSL-Profiltyp** die Option **FrontEnd** aus. Andernfalls können Sie ein vorhandenes Frontend-Profil bearbeiten.
3. Wählen Sie **Unbekanntes SNI zulassen**aus.



4. Klicken Sie auf **OK** und dann auf **Fertig**.

Hinzufügen oder Aktualisieren eines Zertifikatsschlüsselpaars

> **Hinweise:**
>
> Wenn Sie kein vorhandenes Zertifikat und keinen vorhandenen Schlüssel haben, lesen Sie ein Zertifikat erstellen.
>
> Um ein ECDSA-Zertifikatschlüsselpaar zu erstellen, klicken Sie auf Ein ECDSA-Zertifikatschlüsselpaarerstellen.
>
> Kennwortgeschützte Zertifikatsschlüsselpaare werden immer erfolgreich hinzugefügt. Wenn in Builds vor 13.0 Build 79.x eine sichere Kennwortoption auf einer NetScaler-Appliance aktiviert war, wurden manchmal die kennwortgeschützten Zertifikatsschlüsselpaare nicht hinzugefügt. Die Zertifikatschlüsselkonfiguration geht jedoch verloren, wenn Sie auf einen früheren Build herunterstufen. In der NITRO-API-Antwort für Zertifikatschlüsselpaare wird die Variable `passplain` anstelle der Variablen `passcrypt` gesendet.

Für jede SSL-Transaktion benötigt der Server ein gültiges Zertifikat und das entsprechende private und öffentliche Schlüsselpaar. Die SSL-Daten werden mit dem öffentlichen Schlüssel des Servers verschlüsselt, der über das Zertifikat des Servers verfügbar ist. Für die Entschlüsselung ist der entsprechende private Schlüssel erforderlich. Das Kennwort des privaten Schlüssels, der beim Hinzufügen eines SSL-Zertifikatsschlüsselpaars verwendet wird, wird mit einem eindeutigen Verschlüsselungsschlüssel für jede NetScaler-Appliance gespeichert.

Die ADC-Appliance lagert SSL-Transaktionen vom Server aus. Daher müssen das Zertifikat und der private Schlüssel des Servers auf der Appliance vorhanden sein, und das Zertifikat muss mit dem entsprechenden privaten Schlüssel gekoppelt werden. Dieses Zertifikatsschlüsselpaar muss an den virtuellen Server gebunden sein, der die SSL-Transaktionen verarbeitet.

Hinweis: Das Standardzertifikat auf einer NetScaler-Appliance ist 2048 Bit. In früheren Builds war das Standardzertifikat 512 Bit oder 1024 Bit. Nach dem Upgrade auf Version 11.0 müssen Sie alle Ihre alten Zertifikatsschlüsselpaare löschen und dann die Appliance neu starten `"ns-"`, um automatisch ein 2048-Bit-Standardzertifikat zu generieren.

Sowohl das Zertifikat als auch der Schlüssel müssen sich im lokalen Speicher der NetScaler-Appliance befinden, bevor sie der Appliance hinzugefügt werden können. Wenn sich Ihr Zertifikat oder Ihre Schlüsseldatei nicht auf der Appliance befindet, laden Sie es auf die Appliance hoch, bevor Sie das Paar erstellen.

Wichtig: Zertifikate und Schlüssel werden standardmäßig im Verzeichnis /nsconfig/ssl gespeichert. Wenn Ihre Zertifikate oder Schlüssel an einem anderen Ort gespeichert sind, müssen Sie den absoluten Pfad zu den Dateien auf der NetScaler-Appliance angeben. Die NetScaler FIPS-Appliances unterstützen keine externen Schlüssel (Nicht-FIPS-Schlüssel). Auf einer FIPS-Appliance können Sie keine Schlüssel von einem lokalen Speichergerät wie einer Festplatte oder einem Flash-Speicher laden. Die FIPS-Schlüssel müssen im Hardware Security Module (HSM) der Appliance vorhanden sein.

Auf NetScaler-Appliances werden nur RSA-Schlüssel unterstützt.

Legen Sie den Benachrichtigungszeitraum fest und ermöglichen Sie dem Ablaufmonitor, vor Ablauf des Zertifikats eine Aufforderung auszustellen.

Die NetScaler-Appliance unterstützt die folgenden Eingabeformate des Zertifikats und der Privatschlüsseldateien:

- PEM — Datenschutz Enhanced Mail
- DER - Distinguished Encoding
- PFX - Austausch personenbezogener Daten

Die Software erkennt das Format automatisch. Daher müssen Sie das Format nicht mehr im inform-Parameter angeben. Wenn Sie das Format angeben (richtig oder falsch), ignoriert die Software es. Das Format des Zertifikats und der Schlüsseldatei müssen identisch sein.

Hinweis: Ein Zertifikat muss mit einem der folgenden Hash-Algorithmen signiert werden:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Eine MPX-Appliance unterstützt Zertifikate mit 512 oder mehr Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server
- 4096-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist)

Eine virtuelle VPX-Appliance unterstützt Zertifikate mit 512 oder mehr Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server
- 4096-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist)

Die folgende Tabelle zeigt die RSASSA-PSS-Parametersätze, die von der NetScaler-Appliance unterstützt werden. RSASSA-PSS-Algorithmen werden bei der X.509-Zertifikatspfadvalidierung unterstützt.

OID für öffentlichen Schlüssel	Maskengenerierungsfunktion (MGF)	MGF-Digest-Funktion	Signature-Digest-Funktion	Salt-Länge
rsaEncryption	MGF1	SHA-256	SHA-256	32 Byte
rsaEncryption	MGF1	SHA-384	SHA-384	48 Byte
rsaEncryption	MGF1	SHA-512	SHA-512	64 Byte

> **Hinweis**
>
> Eine NetScaler SDX-Appliance unterstützt Zertifikate mit 512 oder mehr Bit. Jede NetScaler VPX-Instanz, die auf der Appliance gehostet wird, unterstützt die vorherigen Zertifikatsgrößen für eine virtuelle VPX-Appliance. Wenn jedoch einer Instanz ein SSL-Chip zugewiesen ist, unterstützt diese Instanz die von einer MPX-Appliance unterstützten Zertifikatsgrößen.

Hinzufügen eines Zertifikatschlüsselpaars mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein Zertifikatsschlüsselpaar hinzuzufügen und die Konfiguration zu überprüfen:

```
add ssl certKey <certkeyName> -cert <string>[(-key <string> [-password
    ]) | -fipsKey <string>] [-inform ( DER | PEM )] [<passplain>] [-
    expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]]

show ssl certKey [<certkeyName>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl certKey sslckey -cert server_cert.pem -key server_key.pem -
    password ssl -expiryMonitor ENABLED -notificationPeriod 30
 Done
Note: For FIPS appliances, replace -key with -fipskey

show ssl certKey sslckey
        Name: sslckey           Status: Valid,   Days to expiration
            :8418
        Version: 3
        Serial Number: 01
        Signature Algorithm: md5WithRSAEncryption
        Issuer:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.root.com
        Validity
```



```
                Not Before: Jul 15 02:25:01 2005 GMT
                Not After : Nov 30 02:25:01 2032 GMT
        Subject:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.server.com
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
 Done
<!--NeedCopy-->
```

Aktualisieren oder entfernen Sie ein Zertifikatsschlüsselpaar über die CLI

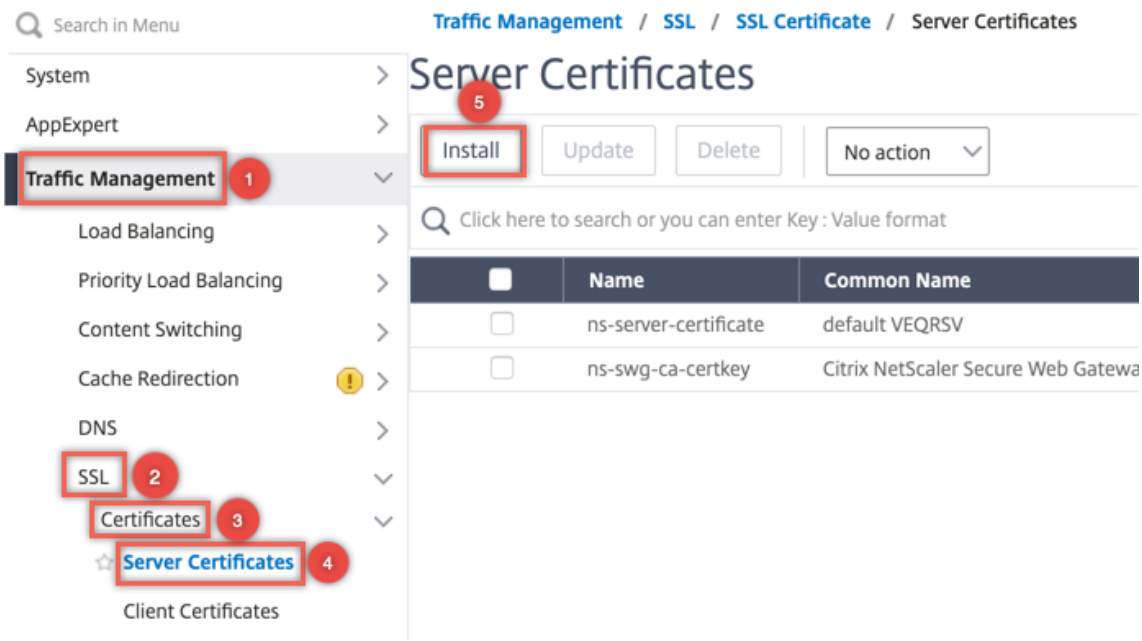
Um die Ablaufüberwachung oder den Benachrichtigungszeitraum in einem Zertifikat-Schlüsselpaar zu ändern, verwenden Sie den Befehl `set ssl certkey`. Um das Zertifikat oder den Schlüssel in einem Zertifikat-Schlüsselpaar zu ersetzen, verwenden Sie den Befehl `update ssl certkey`. Der Befehl `update ssl certkey` hat einen zusätzlichen Parameter zum Überschreiben der Domänenprüfung. Geben Sie für beide Befehle den Namen eines vorhandenen Zertifikat-Schlüssel-Paars ein. Um ein SSL-Zertifikat-Schlüsselpaar zu entfernen, verwenden Sie den Befehl `rm ssl certkey`, der nur das Argument `<certkeyName>` akzeptiert.

Beispiel:

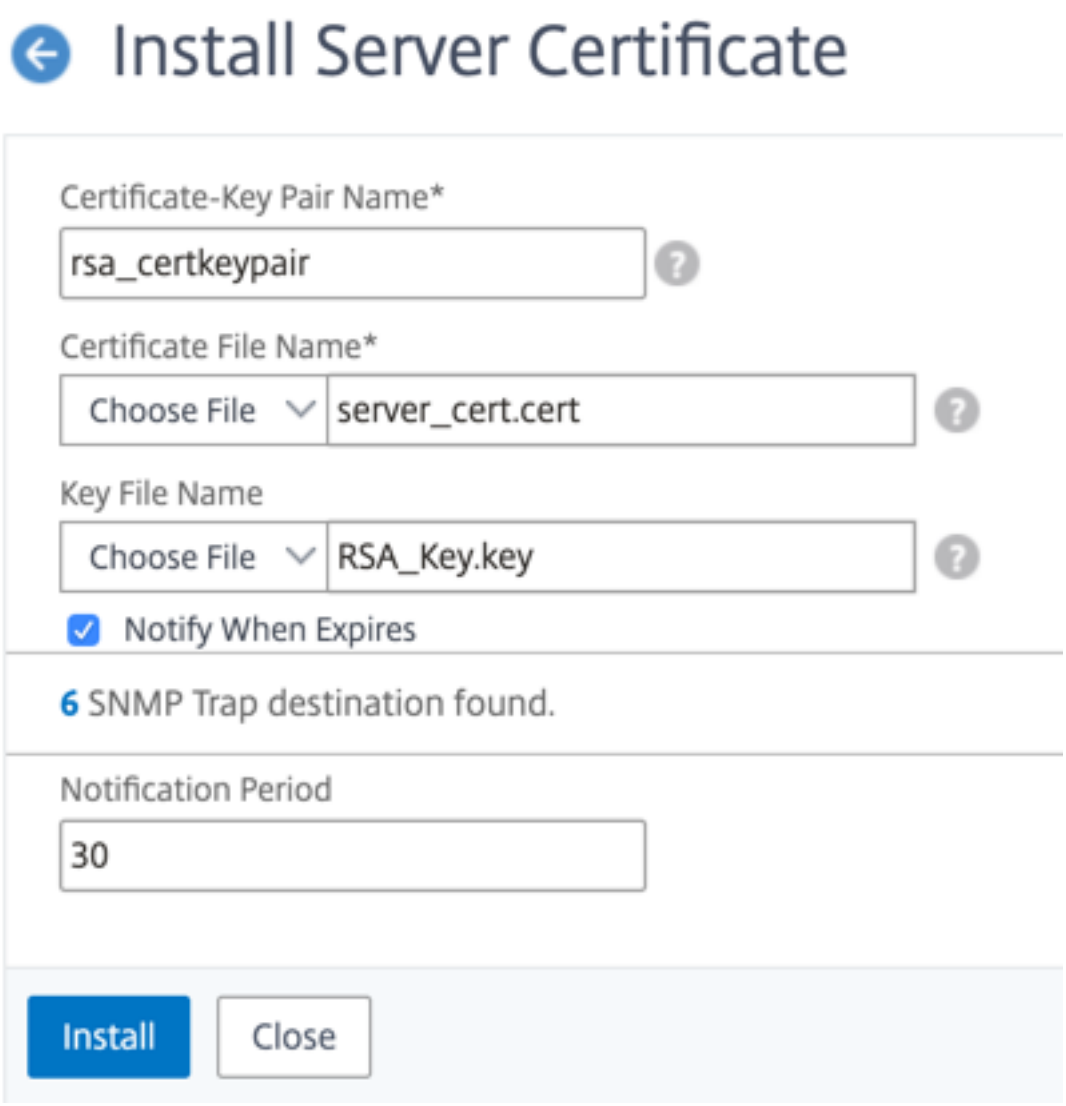
```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED )
       [-notificationPeriod <positive_integer>]]

update ssl certKey <certkeyName> [-cert <string> [-password]] [-key
       <string> | -fipsKey <string>] [-inform <inform>] [-noDomainCheck
          ]
<!--NeedCopy-->
```

Hinzufügen oder Aktualisieren eines Zertifikatsschlüsselpaars über die GUI

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate > Server**.



2. Geben Sie die Werte für die folgenden Parameter ein und klicken Sie auf **Installieren**.
   - Name des Zertifikat-Schlüssel-Paars — Name für das Zertifikat und den privaten Schlüssel.
   - Zertifikatsdateiname — Signiertes Zertifikat, das von der Zertifizierungsstelle erhalten
   - Schlüsseldateiname — Name und optional Pfad der Datei mit privatem Schlüssel, die zum Bilden des Zertifikatsschlüsselpaars verwendet wird.



Binden Sie das Zertifikatschlüsselpaar an den virtuellen SSL-Server

Wichtig: Verknüpfen Sie alle Zwischenzertifikate mit diesem Zertifikat, bevor Sie das Zertifikat an einen virtuellen SSL-Server binden. Informationen zum Verknüpfen von Zertifikaten finden Sie unter Erstellen einer Zertifikatkette.

Das Zertifikat, das für die Verarbeitung von SSL-Transaktionen verwendet wird, muss an den virtuellen Server gebunden sein, der die SSL-Daten empfängt. Wenn Sie über mehrere virtuelle Server verfügen, die SSL-Daten empfangen, muss an jeden von ihnen ein gültiges Zertifikatsschlüsselpaar gebunden sein.

Verwenden Sie ein gültiges, vorhandenes SSL-Zertifikat, das Sie auf die NetScaler-Appliance hochgeladen haben. Erstellen Sie alternativ zu Testzwecken Ihr eigenes SSL-Zertifikat auf der Appliance.

Zwischenzertifikate, die mit einem FIPS-Schlüssel auf der Appliance erstellt wurden, können nicht an einen virtuellen SSL-Server gebunden werden.

Während des SSL-Handshakes listet der Server in der Zertifikatsanforderungsnachricht während der Clientauthentifizierung die Distinguished Names (DN) aller an den Server gebundenen Zertifizierungsstellen (CA) auf. Der Server akzeptiert nur ein Clientzertifikat aus dieser Liste. Wenn Sie nicht möchten, dass der DN-Name eines bestimmten CA-Zertifikats an den SSL-Client gesendet wird, setzen Sie das Flag `skipCA`. Diese Einstellung gibt an, dass der definierte Name des bestimmten Zertifizierungsstellenzertifikats nicht an den SSL-Client gesendet werden darf.

Weitere Informationen zum Erstellen eines eigenen Zertifikats finden Sie unter Zertifikate verwalten.

Hinweis: Citrix empfiehlt, nur gültige SSL-Zertifikate zu verwenden, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurden.

Binden eines SSL-Zertifikatsschlüsselpaars über die CLI an einen virtuellen Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein SSL-Zertifikatsschlüsselpaar an einen virtuellen Server zu binden und die Konfiguration zu überprüfen:

```
1 -  bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName
     > -CA -skipCAName
2 -  show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 bind ssl vs vs1 -certkeyName cert2 -CA -skipCAName
2  Done
3 sh ssl vs vs1
4
5  Advanced SSL configuration for VServer vs1:
6
7  DH: DISABLED
8
9  Ephemeral RSA: ENABLED Refresh Count: 0
10
11  Session Reuse: ENABLED Timeout: 120 seconds
12
13  Cipher Redirect: DISABLED
14
15  SSLv2 Redirect: DISABLED
16
17  ClearText Port: 0
18
```



```
 Client Auth: DISABLED

 SSL Redirect: DISABLED

 Non FIPS Ciphers: DISABLED

 SNI: DISABLED

 OCSP Stapling: DISABLED

 HSTS: DISABLED

 IncludeSubDomains: NO

 HSTS Max-Age: 0

 SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: DISABLED
    TLSv1.2: DISABLED

 Push Encryption Trigger: Always

 Send Close-Notify: YES

 Strict Sig-Digest Check: DISABLED

ECC Curve: P_256, P_384, P_224, P_521

 1) CertKey Name: cert1 CA Certificate OCSPCheck: Optional CA_Name Sent
 2) CertKey Name: cert2 CA Certificate OCSPCheck: Optional CA_Name
    Skipped
 1) Cipher Name: DEFAULT

Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```

Trennen eines SSL-Zertifikatsschlüsselpaars von einem virtuellen Server über die CLI

Wenn Sie versuchen, ein Zertifikatsschlüsselpaar mit dem Befehl `unbind ssl certKey <certkeyName>` von einem virtuellen Server zu trennen, wird eine Fehlermeldung angezeigt. Der Fehler tritt auf, weil sich die Syntax des Befehls geändert hat. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
unbind ssl vserver <vServerName> -certkeyName <string>
```



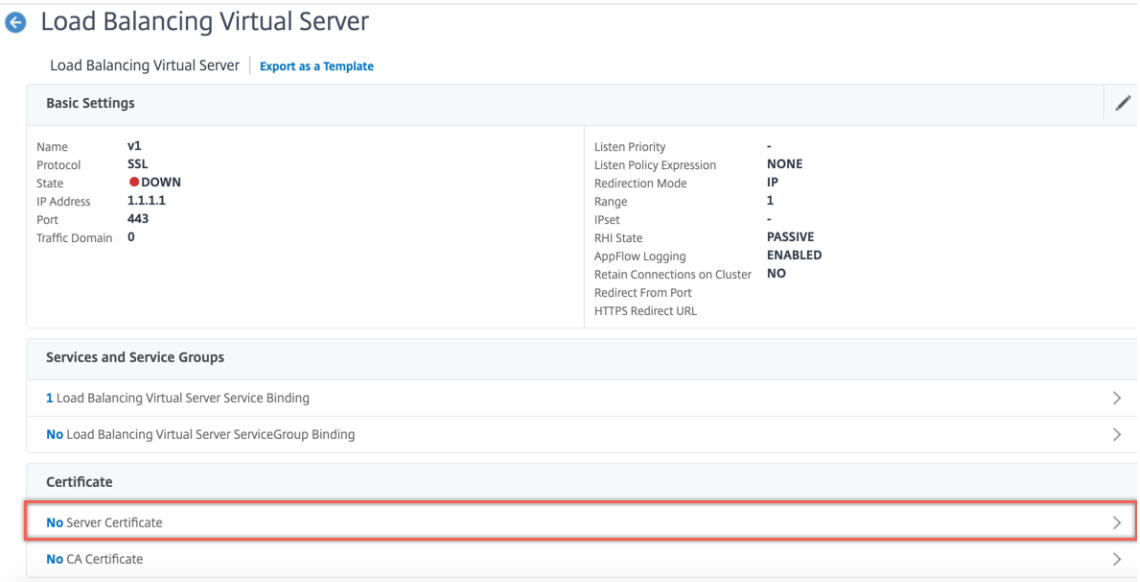
```
<!--NeedCopy-->
```

Beispiel:

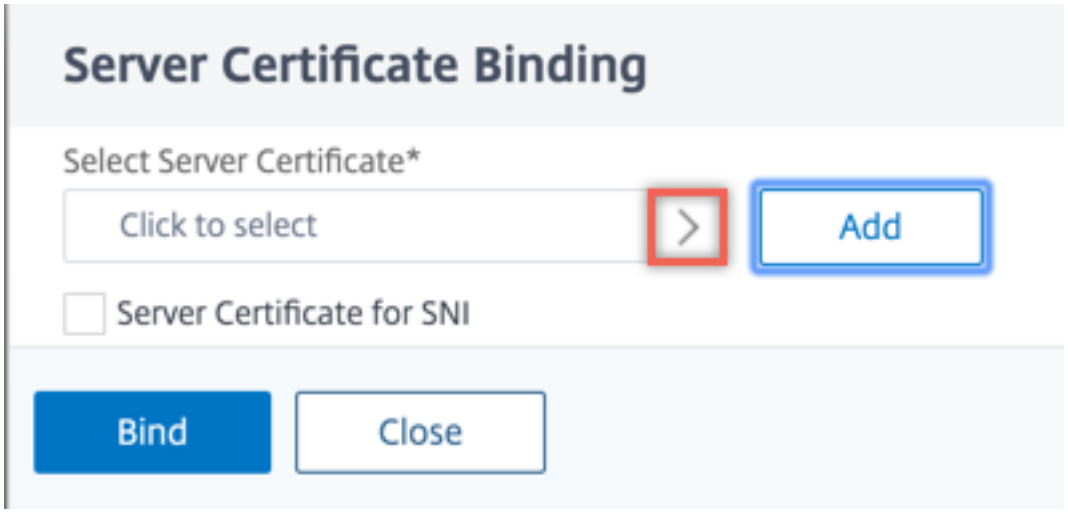
```
unbind ssl vserver vssl -certkeyName sslckey
<!--NeedCopy-->
```

Binden Sie ein SSL-Zertifikat-Schlüsselpaar über die GUI an einen virtuellen Server

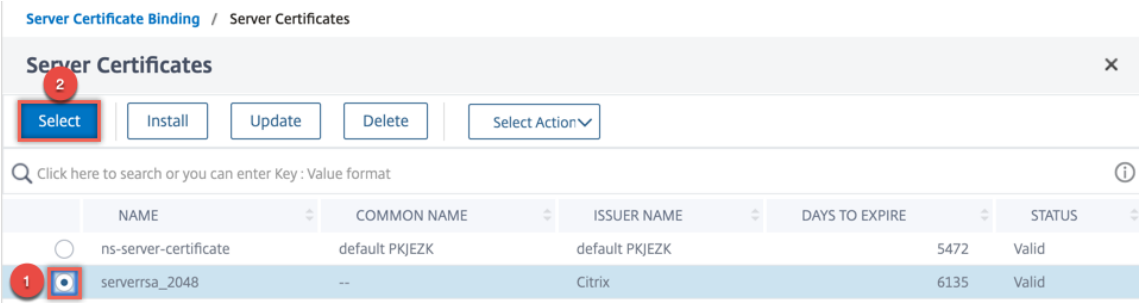
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und öffnen Sie einen virtuellen SSL-Server. Klicken Sie in den Abschnitt **Zertifikat** .



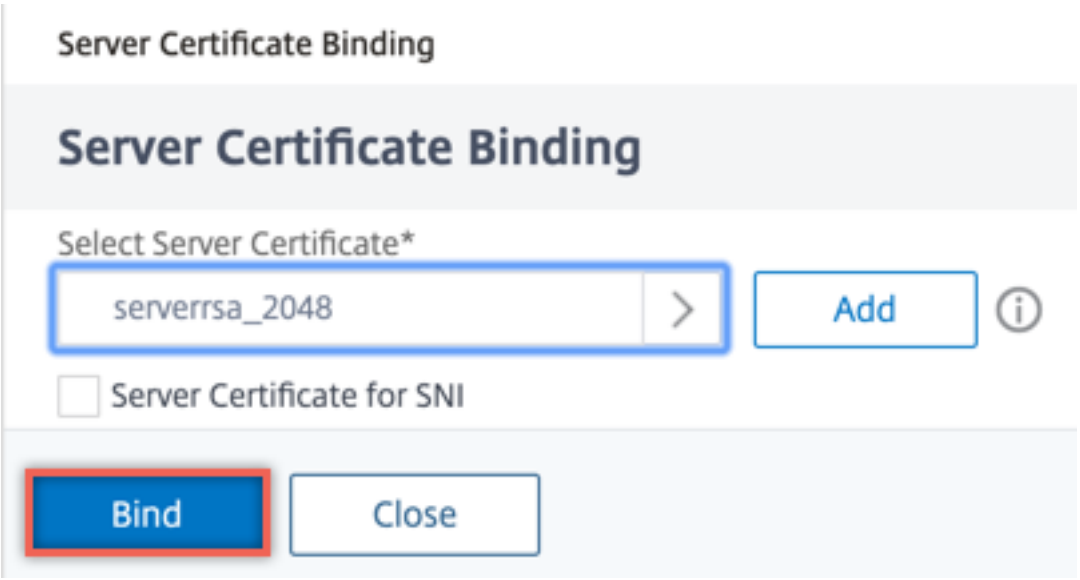
2. Klicken Sie auf den Pfeil, um das Zertifikatsschlüsselpaar auszuwählen.



3. Wählen Sie das Zertifikatsschlüsselpaar aus der Liste aus.



4. Binden Sie das Zertifikatsschlüsselpaar an den virtuellen Server. Um ein Serverzertifikat als SNI-Zertifikat hinzuzufügen, wählen Sie **Serverzertifikat für SNI**aus.



Virtuelle SSL-Serverparameter

Stellen Sie die erweiterte SSL-Konfiguration für einen virtuellen SSL-Server ein. Sie können viele dieser Parameter auch in einem SSL-Profil festlegen. Informationen zu den Parametern, die in einem SSL-Profil festgelegt werden können, finden Sie unter SSL-Profilparameter.

Festlegen von virtuellen SSL-Serverparametern mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServerName>@ [-clearTextPort <port>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )[-sessTimeout <positive_integer>]] [-cipherRedirect (
    ENABLED | DISABLED ) [-cipherURL <URL>]] [-sslv2Redirect ( ENABLED |
     DISABLED )[-sslv2URL <URL>]] [-clientAuth ( ENABLED | DISABLED ) [-
```



```
      clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
      DISABLED )][-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl2 (
      ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 (
      ENABLED | DISABLED )] [-tls11 ( ENABLED | DISABLED )] [-tls12 (
      ENABLED | DISABLED )][-tls13 ( ENABLED | DISABLED )] [-SNIEnable (
      ENABLED | DISABLED )][-ocspStapling ( ENABLED | DISABLED )] [-
      pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES | NO )] [-
      dtlsProfileName <string>] [-sslProfile <string>] [-HSTS ( ENABLED |
      DISABLED )][-maxage <positive_integer>] [-IncludeSubdomains ( YES |
      NO )][-strictSigDigestCheck ( ENABLED | DISABLED )] [-
      zeroRttEarlyData (ENABLED | DISABLED )] [-
      tls13SessionTicketsPerAuthContext <positive_integer>] [-
      dheKeyExchangeWithPsk ( YES | NO )]
2 <!--NeedCopy-->
```

Diffie-Hellman-Parameter (DH)

Um Verschlüsselungen auf der Appliance zu verwenden, die einen DH-Schlüsselaustausch zum Einrichten der SSL-Transaktion erfordern, aktivieren Sie den DH-Schlüsselaustausch auf der Appliance. Konfigurieren Sie andere Einstellungen basierend auf Ihrem Netzwerk.

Um die Verschlüsselungen aufzulisten, für die DH-Parameter über die CLI festgelegt werden müssen, geben Sie Folgendes ein: sh cipher DH.

Um die Chiffre aufzulisten, für die DH-Parameter mithilfe des Konfigurationsdienstprogramms festgelegt werden müssen, navigieren Sie zu **Verkehrsverwaltung > SSL > Verschlüsselungsgruppen**, und doppelklicken Sie auf **DH**.

Weitere Informationen zur Aktivierung des DH-Schlüsselaustauschs finden Sie unter Generieren eines Diffie-Hellman-Schlüssels (DH).

Konfigurieren von DH-Parametern mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um DH-Parameter zu konfigurieren und die Konfiguration zu überprüfen:

```
1 - `set ssl vserver <vserverName> -dh <Option> -dhCount <
    RefreshCountValue> -filepath <string>
2 - show ssl vserver <vServerName>`
3 <!--NeedCopy-->
```

Beispiel:


```
set ssl vserver vs-server -dh ENABLED  -dhFile /nsconfig/ssl/ns-server.cert -dhCount 1000
Done

show ssl vserver vs-server

            Advanced SSL configuration for VServer vs-server:
            DH: ENABLED
            Ephemeral RSA: ENABLED          Refresh Count: 1000
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2: ENABLED  TLSv1.2: ENABLED

    1)      Cipher Name: DEFAULT
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Konfigurieren von DH-Parametern über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **DH Param aktivieren**aus, und geben Sie einen Aktualisierungszähler und einen Dateipfad an.

Vergängliches RSA

Mit kurzlebigen RSA können Exportclients mit dem sicheren Server kommunizieren, auch wenn das Serverzertifikat keine Exportclients unterstützt (1024-Bit-Zertifikat). Wenn Sie verhindern möchten, dass Exportclients auf das sichere Webobjekt oder die sichere Ressource zugreifen, müssen Sie den kurzlebigen RSA-Schlüsselaustausch deaktivieren.

Standardmäßig ist diese Funktion auf der NetScaler-Appliance aktiviert, wobei der Aktualisierungszähler auf Null gesetzt ist (unendliche Verwendung).

Hinweis:

Der kurzlebige RSA-Schlüssel wird automatisch generiert, wenn Sie eine Exportverschlüsselung an einen SSL- oder TCP-basierten virtuellen SSL-Server oder -Dienst binden. Wenn Sie die Exportverschlüsselung entfernen, wird der eRSA-Schlüssel nicht gelöscht. Sie wird später wiederverwendet, wenn eine andere Exportverschlüsselung an einen virtuellen SSL- oder TCP-basierten SSL-Server oder -Dienst gebunden ist. Der eRSA-Schlüssel wird beim Neustart des Systems gelöscht.

Konfigurieren Sie kurzlebigen RSA über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um kurzlebigen RSA zu konfigurieren und die Konfiguration zu überprüfen:

```
set ssl vserver <vServerName> -eRSA (enabled | disabled) -eRSACount <
   positive_integer>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-server -eRSA ENABLED -eRSACount 1000
 Done

show ssl vserver vs-server

        Advanced SSL configuration for VServer vs-server:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
           ENABLED  TLSv1.2: ENABLED
```



```
22
23 1)      Cipher Name: DEFAULT
24         Description: Predefined Cipher Alias
25  Done
26 <!--NeedCopy-->
```

Konfigurieren Sie kurzlebigen RSA über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Ephemere RSA aktivieren**aus, und geben Sie einen Aktualisierungszähler an.

Wiederverwendung der Sitzung

Für SSL-Transaktionen erfordert das Einrichten des ersten SSL-Handshakes CPU-intensive Verschlüsselungsvorgänge mit öffentlichen Schlüsseln. Die meisten Handshake-Vorgänge sind mit dem Austausch des SSL-Sitzungsschlüssels (Clientschlüsselaustauschnachricht) verbunden. Wenn eine Clientsitzung für einige Zeit im Leerlauf ist und dann wieder aufgenommen wird, wird der SSL-Handshake in der Regel erneut durchgeführt. Wenn die Sitzungswiederverwendung aktiviert ist, wird der Austausch von Sitzungsschlüsseln für vom Client empfangene Anfragen zur Sitzungswiederaufnahme vermieden.

Die Wiederverwendung von Sitzungen ist auf der NetScaler-Appliance standardmäßig aktiviert. Durch die Aktivierung dieser Funktion wird die Serverlast reduziert, die Reaktionszeit verbessert und die Anzahl der SSL-Transaktionen pro Sekunde (TPS) erhöht, die der Server unterstützen kann.

Konfigurieren der Wiederverwendung von Sitzungen über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Wiederverwendung der Sitzung zu konfigurieren und die Konfiguration zu überprüfen:

```
1 set ssl vserver <vServerName> -sessReuse ( ENABLED | DISABLED ) -
     sessTimeout <positive_integer>
2 show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 set ssl vserver vs-ssl -sessreuse enabled -sesstimeout 600
2  Done
3
```



```
show ssl vserver vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 600 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
           ENABLED  TLSv1.2: ENABLED

1)      CertKey Name: Auth-Cert-1       Server Certificate

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
<!--NeedCopy-->
```

Konfigurieren der Wiederverwendung von Sitzungen über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Sitzungswiederverwendung aktivieren**aus, und geben Sie eine Zeit an, zu der die Sitzung aktiv bleiben soll.

SSL-Protokolleinstellungen

Die NetScaler-Appliance unterstützt die Protokolle SSLv3, TLSv1, TLSv1.1 und TLSv1.2. Jedes dieser Protokolle kann auf der Appliance festgelegt werden, wie es für Ihre Bereitstellung und die Art der Clients erforderlich ist, die eine Verbindung zur Appliance herstellen.

Die TLS-Protokollversionen 1.0, 1.1 und 1.2 sind sicherer als ältere Versionen des TLS/SSL-Protokolls. Um jedoch Legacy-Systeme zu unterstützen, behalten viele TLS-Implementierungen die Abwärtskompatibilität mit dem SSLv3-Protokoll bei. In einem SSL-Handshake wird die höchste Protokollversion

verwendet, die dem Client und dem auf der NetScaler-Appliance konfigurierten virtuellen SSL-Server gemeinsam ist.

Beim ersten Handshake-Versuch bietet ein TLS-Client die höchste Protokollversion, die er unterstützt. Wenn der Handshake fehlschlägt, bietet der Client eine niedrigere Protokollversion an. Wenn beispielsweise ein Handshake mit TLS-Version 1.1 nicht erfolgreich ist, versucht der Client, neu zu verhandeln, indem er das TLSv1.0-Protokoll anbietet. Wenn dieser Versuch nicht erfolgreich ist, versucht der Client erneut mit dem SSLv3-Protokoll. Ein “Mann in der Mitte” (MITM) -Angreifer kann den anfänglichen Handshake brechen und eine Neuverhandlung mit dem SSLv3-Protokoll auslösen und dann eine Schwachstelle in SSLv3 auszunutzen. Um solche Angriffe zu mildern, können Sie SSLv3 deaktivieren oder Neuverhandlungen mit einem heruntergestuften Protokoll nicht zulassen. Dieser Ansatz ist jedoch möglicherweise nicht praktikabel, wenn Ihre Bereitstellung Legacy-Systeme umfasst. Eine Alternative besteht darin, einen Signalisierungs-Chiffre-Suite-Wert (TLS_FALLBACK_SCSV) in der Clientanforderung zu erkennen.

Ein TLS_FALLBACK_SCSV-Wert in einer Client-Hello-Nachricht zeigt dem virtuellen Server an, dass der Client zuvor versucht hat, eine Verbindung mit einer höheren Protokollversion herzustellen, und dass die aktuelle Anforderung ein Fallback ist. Wenn der virtuelle Server diesen Wert erkennt und eine höhere Version als die vom Client angegebene unterstützt, lehnt er die Verbindung mit einer schwerwiegenden Warnung ab. Der Handshake ist erfolgreich, wenn eine der folgenden Bedingungen erfüllt ist:

- Der TLS_FALLBACK_SCSV-Wert ist nicht in der Hello-Nachricht des Clients enthalten.
- Die Protokollversion im Client Hello ist die höchste Protokollversion, die vom virtuellen Server unterstützt wird.

Konfigurieren der SSL-Protokollunterstützung über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die SSL-Protokollunterstützung zu konfigurieren und die Konfiguration zu überprüfen:

```
set ssl vserver <vServerName> -ssl2 ( ENABLED | DISABLED ) -ssl3 (
    ENABLED | DISABLED ) -tls1 ( ENABLED | DISABLED ) -tls11 ( ENABLED |
     DISABLED ) -tls12 ( ENABLED | DISABLED )

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-ssl -tls11 ENABLED -tls12 ENABLED
Done

sh ssl vs vs-ssl
```



```
5
6          Advanced SSL configuration for VServer vs-ssl:
7              DH: DISABLED
8              Ephemeral RSA: ENABLED                              Refresh
                   Count: 0
9              Session Reuse: ENABLED                                Timeout
                   : 120 seconds
10             Cipher Redirect: DISABLED
11             SSLv2 Redirect: DISABLED
12             ClearText Port: 0
13             Client Auth: DISABLED
14             SSL Redirect: DISABLED
15             Non FIPS Ciphers: DISABLED
16             SNI: DISABLED
17             SSLv2: DISABLED        SSLv3: ENABLED    TLSv1.0: ENABLED
                   TLSv1.1: ENABLED  TLSv1.2: ENABLED
18             Push Encryption Trigger: Always
19             Send Close-Notify: YES
20             1 bound certificate:
21
22     1)      CertKey Name: mycert  Server Certificate
23             1 configured cipher:
24
25     1)      Cipher Name: DEFAULT
26             Description: Predefined Cipher Alias
27
28 Done
29 <!--NeedCopy-->
```

Konfigurieren der SSL-Protokollunterstützung über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** ein zu aktivierendes Protokoll aus.

nah-benachrichtigen

Eine Close-Notify ist eine sichere Nachricht, die das Ende der SSL-Datenübertragung anzeigt. Eine Einstellung für eine nahe Benachrichtigung ist auf globaler Ebene erforderlich. Diese Einstellung gilt für alle virtuellen Server, Dienste und Dienstgruppen. Informationen zur globalen Einstellung finden Sie im Abschnitt “Globale SSL-Parameter” weiter unten auf dieser Seite.

Zusätzlich zur globalen Einstellung können Sie den Close-Notify-Parameter auf der Ebene des

virtuellen Servers, des Dienstes oder der Dienstgruppe festlegen. Sie haben daher die Flexibilität, den Parameter für eine Entität festzulegen und ihn für eine andere Entität aufzuheben. Stellen Sie jedoch sicher, dass Sie diesen Parameter auf globaler Ebene festlegen. Andernfalls gilt die Einstellung auf Entitätsebene nicht.

Konfigurieren von Close-Notify auf Entitätsebene über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die Funktion zum Schließen der Benachrichtigung zu konfigurieren und die Konfiguration zu überprüfen:

1. Um auf der Ebene des virtuellen Servers zu konfigurieren, geben Sie Folgendes ein:

```
set ssl vserver <vServerName> -sendCloseNotify ( YES | NO )
show ssl vserver <vServerName>
<!--NeedCopy-->
```

1. Um auf Service-Ebene zu konfigurieren, geben Sie Folgendes ein:

```
set ssl service <serviceName> -sendCloseNotify ( YES | NO )
show ssl service <serviceName>
<!--NeedCopy-->
```

1. Um auf der Dienstgruppenebene zu konfigurieren, geben Sie Folgendes ein:

```
set ssl serviceGroup <serviceGroupName> -sendCloseNotify ( YES | NO )
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver sslvsvr -sendCloseNotify YES

Done
<!--NeedCopy-->
```

Konfigurieren Sie die Funktion zum Schließen von Benachrichtigungen auf Entitätsebene über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Close-Notify senden**aus.

Globale SSL-Parameter

Die erweiterte Anpassung Ihrer SSL-Konfiguration behebt bestimmte Probleme. Sie können den Befehl `set ssl parameter` oder das Konfigurationsdienstprogramm verwenden, um Folgendes anzugeben:

- Für SSL-Transaktionen zu verwendende Quantengröße.
- CRL-Speichergröße.
- OCSP-Cachegröße.
- Verweigern Sie die SSL-Neuverhandlung.
- Setzen Sie das PUSH-Flag für entschlüsselte, verschlüsselte oder alle Datensätze.
- Löschen Sie Anfragen, wenn der Client den Handshake für eine Domäne initiiert und eine HTTP-Anforderung für eine andere Domäne sendet.
- Stellen Sie die Zeit ein, nach der die Verschlüsselung ausgelöst wird.
  Hinweis: Die von Ihnen angegebene Zeit gilt nur, wenn Sie den `set ssl vserver` Befehl oder das Konfigurationsdienstprogramm verwenden, um die timerbasierte Verschlüsselung festzulegen.
- NDCPP-Konformitätszertifikatprüfung — Gilt, wenn die Appliance als Client fungiert (Back-End-Verbindung). Ignorieren Sie bei der Zertifikatsüberprüfung den allgemeinen Namen, wenn SAN im SSL-Zertifikat vorhanden ist.
- Aktivieren Sie einen heterogenen Cluster von Cavium-Chip-Appliances wie MPX 14000 und Intel Coleto-Chip-Appliances wie MPX 15000-Appliances mit einer unterschiedlichen Anzahl von Paket-Engines.
- Ermöglichen Sie sichere Neuverhandlungen im Backend.
- Adaptive SSL-Verkehrskontrolle.

Konfigurieren globaler SSL-Parameter mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um erweiterte SSL-Einstellungen zu konfigurieren und die Konfiguration zu überprüfen:

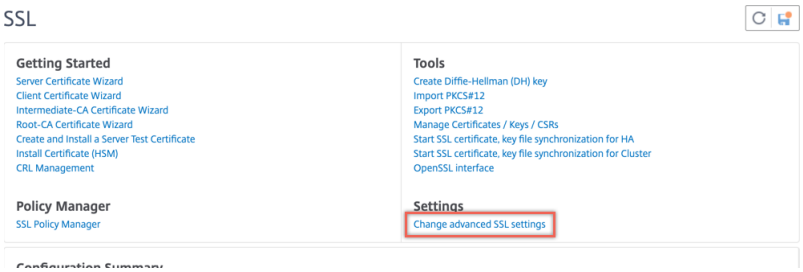
```
1 set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <
    positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout
    <positive_integer>] [-sendCloseNotify (YES | NO)] [-
    encryptTriggerPktCount <positive_integer>] [-denySSLReneg <
    denySSLReneg>] [-insertionEncoding (Unicode|UTF-8)] [-ocspCacheSize
    <positive_integer>][- pushFlag <positive_integer>] [-
    dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <
    positive_integer>] [-ndcppComplianceCertCheck ( YES | NO)] [-
    heterogeneousSSLHW (ENABLED | DISABLED )]
2 show ssl parameter
3 <!--NeedCopy-->
```


Beispiel:

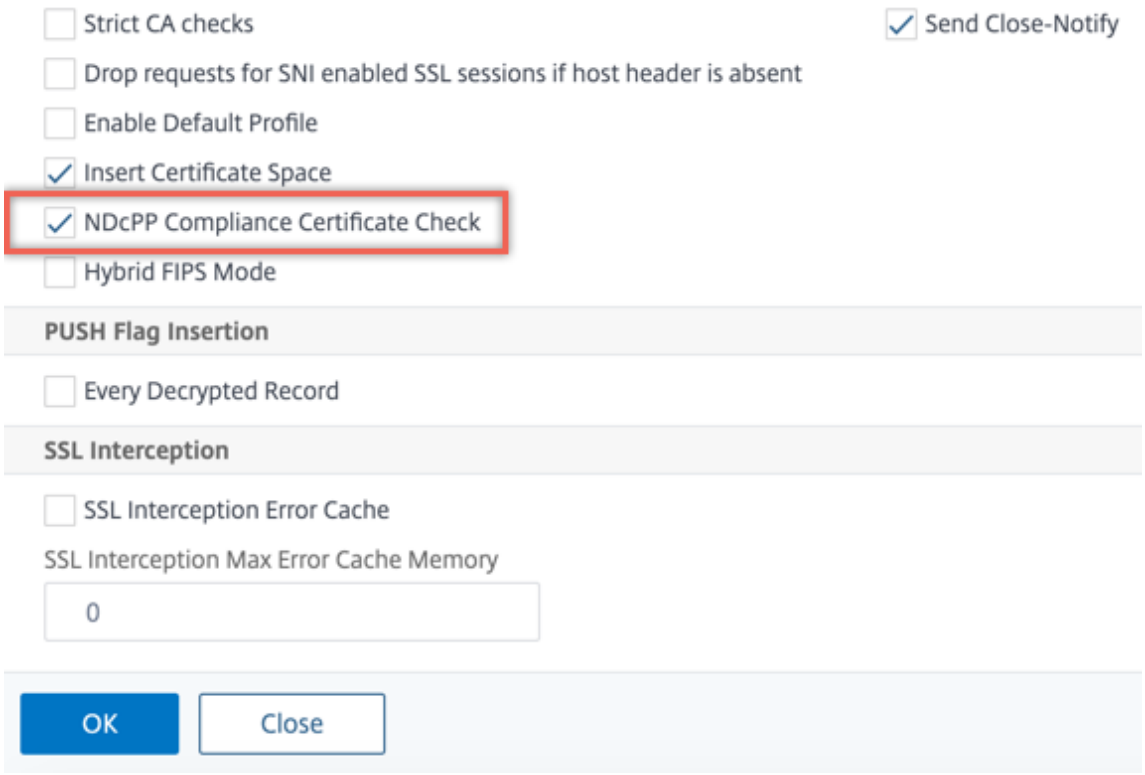
```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks
    no -ssltriggerTimeout 100 -sendClosenotify no -
    encryptTriggerPktCount 45 -denySSLReneg NONSECURE -insertionEncoding
     unicode -ocspCacheSize 10 -pushFlag 3 -dropReqWithNoHostHeader YES
     -pushEncTriggerTimeout 100 ms -ndcppComplianceCertCheck YES
Done

show ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : NO
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x3 (On
       every decrypted and encrypted record)
    Strict Host Header check for SNI enabled SSL sessions : YES
    PUSH encryption trigger timeout                     : 100 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : DISABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
    Software Crypto acceleration CPU Threshold          : 0
    Hybrid FIPS Mode                                    : DISABLED
    Signature and Hash Algorithms supported by TLS1.2   : ALL
    SSL Interception Error Learning and Caching         : DISABLED
    SSL Interception Maximum Error Cache Memory         : 0 Bytes
    NDCPP Compliance Certificate Check                  : YES
    Heterogeneous SSL HW (Cavium and Intel Based)       : ENABLED
 Done
<!--NeedCopy-->
```


Konfigurieren der NDcPP-Konformitätszertifikatprüfung über die GUI

1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe **Einstellungen** die Option **Erweiterte SSL-Einstellungen ändern** aus.



2. Wählen Sie **NDCPP-Konformitätszertifikatprüfung** aus. Klicken Sie auf **OK**.



Unterstützung für sichere Neuverhandlungen am Backend einer NetScaler-Appliance

Hinweis: Diese Funktion wird in Version 13.0 Build 58.x und höher unterstützt. In früheren Versionen und Builds wurde nur unsichere Neuverhandlungen im Backend unterstützt.

Die Funktion wird auf den folgenden Plattformen unterstützt:

- VPX
- MPX-Plattformen mit N2- oder N3-Chips
- Intel Coleto SSL-Chip-basierte Plattformen

Die Funktion wird auf der FIPS-Plattform noch nicht unterstützt.

Sichere Neuverhandlungen werden standardmäßig im Backend einer ADC-Appliance verweigert. Das heißt, der Parameter denySSLReneg ist auf ALL (Standard) festgelegt.

Um eine sichere Neuverhandlung im Backend zu ermöglichen, wählen Sie eine der folgenden Einstellungen für den Parameter denySSLReneg aus:

- NEIN
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NONSECURE

Ermöglichen Sie sichere Neuverhandlungen über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -denySSLReneg <denySSLReneg>
```

Beispiel:

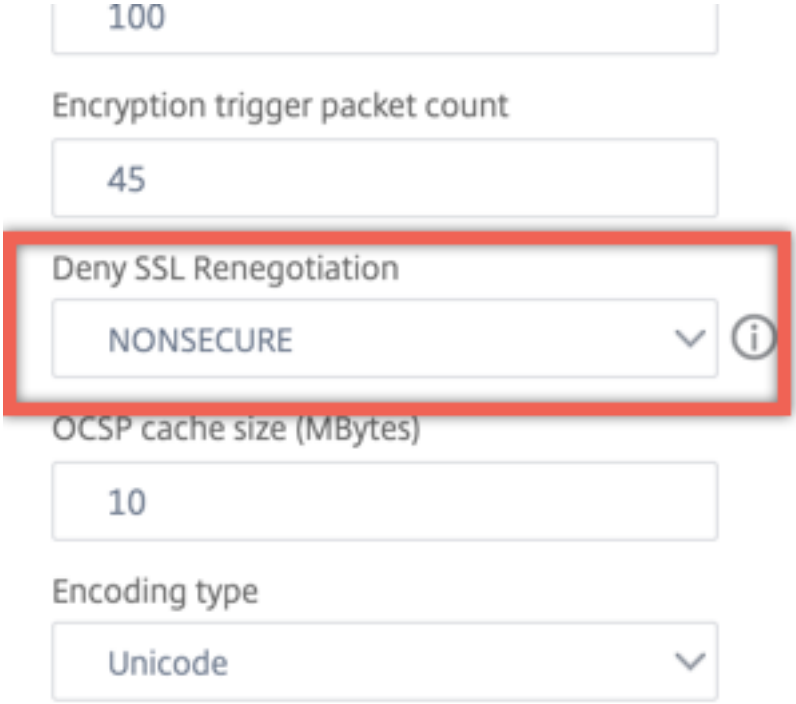
```
set ssl parameter -denySSLReneg NONSECURE
 Done

sh ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : YES
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x0 (Auto)
    Strict Host Header check for SNI enabled SSL sessions : NO
    Match HTTP Host header with SNI                     : CERT
    PUSH encryption trigger timeout                     : 1 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : ENABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
```



```
    Software Crypto acceleration CPU Threshold              : 0
    Hybrid FIPS Mode                                        : DISABLED
    Signature and Hash Algorithms supported by TLS1.2       : ALL
    SSL Interception Error Learning and Caching             : DISABLED
    SSL Interception Maximum Error Cache Memory             : 0 Bytes
    NDCPP Compliance Certificate Check                      : NO
    Heterogeneous SSL HW (Cavium and Intel Based)           : DISABLED
    Crypto Operation Queue Limit                            : 150%
 Done
<!--NeedCopy-->
```

Ermöglichen Sie sichere Neuverhandlungen mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Erweiterte SSL-Einstellungen ändern**.
2. Legen Sie " **SSL-Neuverhandlung verweigern** " auf einen anderen Wert als ALL fest.



Adaptive SSL-Verkehrssteuerung

Hinweis: Diese Funktion wird in Version 13.0 Build 58.x und höher unterstützt.

Wenn viel Verkehr auf der Appliance empfangen wird und die Krypto-Beschleunigungskapazität voll ist, beginnt die Appliance, Verbindungen in die Warteschlange zu stellen, um sie später zu verarbeiten. Derzeit ist die Größe dieser Warteschlange auf 64 K festgelegt und die Appliance beginnt, Verbindungen zu trennen, wenn dieser Wert überschritten wird.

Benutzer können einen Wert konfigurieren, der einen Prozentsatz der tatsächlichen Kapazität darstellt. Infolgedessen löscht die Appliance neue Verbindungen, wenn die Anzahl der Elemente in der Warteschlange den Grenzwert überschreitet, der adaptiv und dynamisch berechnet wird. Dieser Ansatz steuert eingehende SSL-Verbindungen und verhindert übermäßigen Ressourcenverbrauch und andere Ausfälle, wie z. B. einen Ausfall der Lastenausgleichsüberwachung oder eine langsame Reaktion auf sichere Anwendungen auf der Appliance.

Wenn die Warteschlange leer ist, kann die Appliance weiterhin Verbindungen annehmen. Wenn die Warteschlange nicht leer ist, hat das Kryptosystem seine Kapazität erreicht und die Appliance beginnt, Verbindungen in die Warteschlange zu stellen.

Das Limit wird basierend auf folgenden Kriterien berechnet:

- Die tatsächliche Kapazität des Geräts.
- Vom Benutzer konfigurierter Wert als Prozentsatz der tatsächlichen Kapazität. Der Standardwert ist auf 150% festgelegt.

Wenn beispielsweise die tatsächliche Kapazität einer Appliance zu einem bestimmten Zeitpunkt 1000 Operationen/Sekunde beträgt und der Standardprozentsatz konfiguriert ist, beträgt der Grenzwert, nach dem die Appliance Verbindungen trennt, 1500 (150% von 1000).

So konfigurieren Sie das Limit für die Operationswarteschlange über die CLI

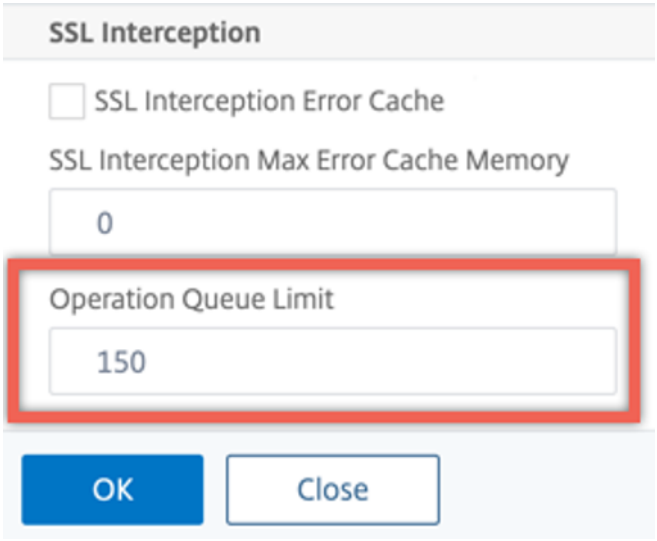
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -operationQueueLimit <positive_integer>
```

Limit der Warteschlange für Vorgänge - Begrenzung des Prozentsatzes der Kapazität der Warteschlange für Kryptovorgänge, ab der neue SSL-Verbindungen erst akzeptiert werden, wenn die Warteschlange reduziert wurde. Standardwert: 150. Mindestwert: 0. Maximaler Wert: 10000.

So konfigurieren Sie das Limit der Operationswarteschlange über die GUI

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie in den **Einstellungen**auf **Erweiterte SSL-Einstellungen ändern**.
3. Geben Sie einen Wert in **Warteschlangenlimit für Vorgänge**ein. Die Standardeinstellung ist 150.
4. Klicken Sie auf **OK**.



Heterogene Clusterbereitstellungen

Sie können eine heterogene Clusterbereitstellung von NetScaler MPX-Appliances mit einer anderen Anzahl von Paket-Engines erstellen, indem Sie den SSL-Parameter “Heterogenous SSL HW” auf ENABLED setzen. Um beispielsweise einen Cluster aus Cavium-Chip-basierten Appliances (MPX 14000 oder ähnlich) und Intel Coleto-Chip-basierten Appliances (MPX 15000 oder ähnlich) zu bilden, aktivieren Sie den SSL-Parameter “Heterogene SSL-HW. “ Um einen Cluster von Plattformen mit demselben Chip zu bilden, behalten Sie den Standardwert (DISABLED) für diesen Parameter bei.

> **Hinweise:**
>
> Die folgenden Funktionen werden in einem heterogenen Cluster nicht unterstützt:
>
> - VPX-Instanzen werden auf NetScaler SDX-Appliances gehostet.
> - SSLv3-Protokoll auf SSL-Entitäten wie virtuellen Servern, Diensten, Dienstgruppen und internen Diensten.
> - CPU-Schwellenwert für Software-Krypto-Beschleunigung (Verwendung von Hardware und Software zur Verbesserung der Verschlüsselungsleistung von ECDSA und ECDHE).

Weitere Informationen zu den Plattformen, die in einem heterogenen Cluster unterstützt werden, finden Sie unter https://docs.citrix.com/en-us/citrix-adc/current-release/clustering/support-for-heterogeneous-cluster.html.

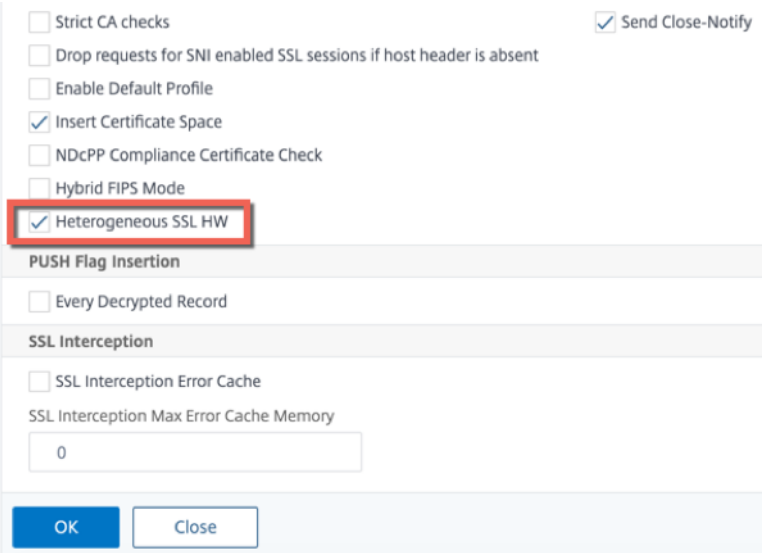
Aktivieren eines heterogenen Clusters mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -heterogeneousSSLHW ENABLED
```


Ermöglichen eines heterogenen Clusters über die GUI

1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe **Einstellungen** die Option **Erweiterte SSL-Einstellungen ändern** aus.
2. Wählen Sie **Heterogene SSL HW**. Klicken Sie auf **OK**.



Push-Flag basierter Verschlüsselungsauslösemechanismus

Mit dem Verschlüsselungsauslösemechanismus, der auf dem PSH-TCP-Flag basiert, können Sie jetzt Folgendes tun:

- Führen Sie aufeinanderfolgende Pakete, in denen das PSH-Flag gesetzt ist, zu einem einzigen SSL-Datensatz zusammen oder ignorieren Sie das PSH-Flag.
- Führen Sie eine timerbasierte Verschlüsselung durch, bei der der Timeoutwert mit dem Befehl `set ssl parameter -pushEncTriggerTimeout <positive_integer>` global festgelegt wird.

Konfigurieren der PUSH-Flag-basierten Verschlüsselung über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Push-Flag-basierte Verschlüsselung zu konfigurieren und die Konfiguration zu überprüfen:

```
set ssl vserver <vServerName> [-pushEncTrigger <pushEncTrigger>]

show ssl vserver
<!--NeedCopy-->
```

Beispiel:


```
set ssl vserver vserver1 -pushEncTrigger always

Done

sh ssl vserver vserver1

            Advanced SSL configuration for VServer vserver1:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: ENABLED

                Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: DISABLED
            DHE Key Exchange With PSK: NO
            Tickets Per Authentication Context: 1
            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT
            Description: Default cipher list with encryption strength
                >= 128bit
Done
<!--NeedCopy-->
```

Konfigurieren der Push-Flag-basierten Verschlüsselung über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und öffnen Sie

einen virtuellen SSL-Server.

2. Wählen Sie im Abschnitt **SSL-Parameter** in der Liste **PUSH-Verschlüsselungsauslöser** einen Wert aus.

Unterstützung für den TLS1.2 Signatur-Hash-Algorithmus

Die NetScaler-Appliance ist vollständig TLS1.2-Signatur-Hash-Erweiterung kompatibel.

In einem SSL-Handshake sendet ein Client eine Liste unterstützter Signatur-Hash-Algorithmen. Der Client teilt dem Server mit der Erweiterung “signature_algorithmus” mit, welche Signatur-Hash-Algorithmus-Paare in den SSL-Handshake-Nachrichten (SKE und CCV) verwendet werden könnten. Das Feld “extension_data” dieser Erweiterung enthält einen Wert “supported_signature_algorithms” in der Client-Hello Nachricht. Der SSL-Handshake wird fortgesetzt, wenn der Server einen dieser Signatur-Hash-Algorithmen unterstützt. Wenn der Server keinen dieser Algorithmen unterstützt, wird die Verbindung getrennt.

Wenn der Server ein Clientzertifikat für die Clientauthentifizierung anfordert, enthält die Zertifikatsanforderungsnachricht einen Wert “supported_signature_algorithms”. Das Clientzertifikat wird basierend auf diesem Signatur-Hash-Algorithmus ausgewählt.

> **Hinweis:**
>
> Die NetScaler-Appliance fungiert als Server für einen Client und als Client für den Backend-Server.

Die Appliance unterstützt nur RSA-SHA1 und RSA-SHA256 im Front-End und RSA-MD5, RSA-SHA1 und RSA-SHA256 im Backend.

Die MPX/SDX/VPX-Appliance unterstützt die folgenden Signatur-Hash-Kombinationen. Wenn auf einer SDX-Appliance ein SSL-Chip einer VPX-Instanz zugewiesen ist, gilt die Verschlüsselungsunterstützung einer MPX-Appliance. Andernfalls gilt die normale Verschlüsselungsunterstützung einer VPX-Instanz.

- Auf einer VPX-Instanz und auf einer MPX/SDX-Appliance ohne N3-Chips:
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224
  - RSA-SHA256
  - RSA-SHA384
  - RSA-SHA512
- Auf einer MPX/SDX-Einheit mit N3-Chips:
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224

- RSA-SHA256
- RSA-SHA384
- RSA-SHA512
- ECDSA-SHA1
- ECDSA-SHA224
- ECDSA-SHA256
- ECDSA-SHA384
- ECDSA-SHA512

Standardmäßig sind alle Signatur-Hash-Algorithmen aktiviert. Sie können jedoch nur einige Signatur-Hash-Algorithmen aktivieren, indem Sie den folgenden Befehl verwenden:

```
set ssl parameter -sigDigestType <sigDigestType>

Parameters

sigDigestType

Signature digest algorithms supported by the appliance. The platform
   determines the list of algorithms supported by default.

              On VPX: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384
                   RSA-

              SHA512

              On MPX with N3 cards: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-

              SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224
                  ECDSA-

              SHA256 ECDSA-SHA384 ECDSA-SHA512

              Other MPX Platforms: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-
                  SHA256 RSA-SHA384 RSA-

              SHA512.

    set ssl parameter -sigDigestType RSA-SHA224 RSA-SHA256 RSA-SHA384
       RSA-SHA512
<!--NeedCopy-->
```

Validierung des Peer-Zertifikats

Gemäß RFC 5246 muss das Peer-Zertifikat mit einem der Signatur-Hash-Algorithmen signiert werden, die in der Client-Hello-Erweiterung enthalten sind. Sie können den Parameter `strictSigDigestCheck` verwenden. Abhängig von der vom Client gesendeten Signatur-Hash-Liste gibt die Appliance bei Aktivierung ein Zertifikat zurück `strictSigDigestCheck`, das von einem der Signatur-Hash-Algorithmen signiert ist, die in der Client-Hello-Erweiterung erwähnt werden. Wenn der Peer kein ordnungsgemäßes Zertifikat besitzt, wird die Verbindung getrennt. Wenn dieser Parameter deaktiviert ist, wird der Signatur-Hash nicht im Peer-Zertifikat geprüft.

Sie können eine strikte Signaturüberprüfung auf einem virtuellen SSL-Server und -Dienst konfigurieren. Wenn Sie diesen Parameter auf einem virtuellen SSL-Server aktivieren, muss das vom Server gesendete Serverzertifikat von einem der Signatur-Hash-Algorithmen signiert sein, die in der Client-Hello-Erweiterung aufgeführt sind. Wenn die Clientauthentifizierung aktiviert ist, muss das vom Server empfangene Clientzertifikat mit einem der Signatur-Hash-Algorithmen signiert werden, die in der vom Server gesendeten Zertifikatsanforderung aufgeführt sind.

Wenn Sie diesen Parameter in einem SSL-Dienst aktivieren, muss das vom Client empfangene Serverzertifikat von einem der Signatur-Hash-Algorithmen signiert sein, die in der Client-Hello-Erweiterung aufgeführt sind. Das Clientzertifikat muss mit einem der Signatur-Hash-Algorithmen signiert werden, die in der Zertifikatsanforderungsnachricht aufgeführt sind.

Wenn das Standardprofil aktiviert ist, können Sie es verwenden, um eine strikte Signaturüberprüfung auf einem virtuellen SSL-Server, einem SSL-Dienst und einem SSL-Profil zu konfigurieren.

Konfigurieren einer strengen Signaturüberprüfung auf einem virtuellen SSL-Server, Dienst oder Profil über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServerName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl service <serviceName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl profile <name>-strictSigDigestCheck ( ENABLED | DISABLED )

Parameters

strictSigDigestCheck

              Check whether peer entity certificate is signed using one
                  of the signature-hash algorithms supported by the
                 NetScaler appliance.

```



```
                Possible values: ENABLED, DISABLED

                Default: DISABLED
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver v1 -strictSigDigestCheck Enabled
set ssl service s1 -strictSigDigestCheck Enabled
set ssl profile p1 -strictSigDigestCheck Enabled
<!--NeedCopy-->
```

> **Wichtig:**
>
> Wenn DH-, ECDHE- oder ECDSA-Verschlüsselungen auf der Appliance konfiguriert sind, muss die SKE-Nachricht mit einem der Signatur-Hashes signiert werden, die in der Clientliste gemeinsam sind, und der auf der Appliance konfigurierten Liste. Wenn kein gemeinsamer Signaturhash vorhanden ist, wird die Verbindung unterbrochen.

SSL für ADC-Admin-UI-Zugriff konfigurieren

Für den HTTPS-Zugriff auf das Konfigurationsdienstprogramm und für sichere Remoteprozeduraufrufe ist ein Zertifikatsschlüsselpaar erforderlich. Auf einer NetScaler MPX-Appliance oder einer virtuellen VPX-Appliance ist ein Zertifikatschlüsselpaar automatisch an die internen Dienste gebunden. Dieses Zertifikat wird jedoch möglicherweise von Browsern nicht als vertrauenswürdig eingestuft. Sie müssen gültige CA-Zertifikate im Browser hochladen, um die Authentifizierung ohne Fehler abzuschließen.

Konfigurieren Sie sicheres HTTPS mithilfe der CLI

Gehen Sie folgendermaßen vor, um sicheres HTTPS mithilfe der CLI zu konfigurieren:

1. Fügen Sie ein Zertifikatsschlüsselpaar hinzu.

```
add certkey server -cert servercert -key serverkey
<!--NeedCopy-->
```

2. Binden Sie dieses Zertifikatschlüsselpaar an die folgenden internen Dienste.

```
bind ssl service nshttps-127.0.0.1-443 -certkeyname server

bind ssl service nshttps-::11-443 -certkeyname server
<!--NeedCopy-->
```


Konfigurieren Sie sicheres HTTPS mithilfe der GUI

Gehen Sie folgendermaßen vor, um sicheres HTTPS mithilfe der GUI zu konfigurieren:

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**.
2. Klicken Sie im Detailbereich auf **Installieren**.
3. Geben **Sie im Dialogfeld Zertifikat installieren** die Zertifikatsdetails ein.
4. Klicken **Sie auf Installieren**und dann auf **Schließen**.
5. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
6. Klicken Sie im Detailbereich auf der Registerkarte **Aktion** auf **Interne Dienste**.
7. Wählen Sie `nshttps-127.0.0.1-443` aus der Liste aus, und klicken Sie dann auf **Öffnen**.
8. Wählen Sie auf der Registerkarte **SSL-Einstellungen** im Bereich **Verfügbar** das in Schritt 4 erstellte Zertifikat aus, klicken Sie auf **Binden**, und klicken Sie dann auf **OK**.
9. Wählen Sie `nshttps-::1-443` aus der Liste aus, und klicken Sie dann auf **Öffnen**.
10. Wählen Sie auf der Registerkarte **SSL-Einstellungen** im Bereich **Verfügbar** das in Schritt 4 erstellte Zertifikat aus, klicken Sie auf **Binden**, und klicken Sie dann auf **OK**.
11. Klicken Sie auf **OK**.

Unterstützung für das TLS 1.3-Protokoll

August 15, 2023

Die NetScaler VPX- und NetScaler MPX-Appliances unterstützen jetzt das in RFC 8446 spezifizierte TLS 1.3-Protokoll.

> **Hinweise:**
>
> - Die TLS 1.3-Hardwarebeschleunigung wird auf den folgenden Plattformen unterstützt:
>   - MPX 5900
>   - MPX/SDX 8900
>   - MPX/SDX 9100
>   - MPX/SDX 15000
>   - MPX/SDX 15000-50G
>   - MPX/SDX 16000
>   - MPX/SDX 26000
>   - MPX/SDX 26000-50S
>   - MPX/SDX 26000-100G
> - Reine Softwareunterstützung für das TLS 1.3-Protokoll ist auf allen anderen NetScaler MPX- und SDX-Appliances außer NetScaler FIPS-Appliances verfügbar.
> - TLS 1.3 wird nur mit dem erweiterten Profil unterstützt. Informationen zum Aktivieren des

> erweiterten Profils finden Sie unter Standardprofil aktivieren. Die Begriffe “Standard” und “erweitert” werden synonym für das SSL-Profil verwendet.
>
> - Um TLS 1.3 verwenden zu können, müssen Sie einen Client verwenden, der der RFC 8446-Spezifikation entspricht.

Unterstützte NetScaler-Funktionen

Die folgenden SSL-Funktionen werden unterstützt:

SSL-Funktionen	Unterstützung am Frontend	Support im Backend
Verschlüsselungssuite TLS 1.3-AES256-GCM-SHA384 (0x1302)	Ja	Ja
Verschlüsselungssuite TLS 1.3_CHACHA20_POLY1305_SHA256 (0x1303)	Ja	Ja
Verschlüsselungssuite TLS 1.3-AES128_GCM-SHA256 (0x1301)	Ja	Ja
ECC-Kurve P_256 für ephemeren DH-Schlüsselaustausch	Ja	Ja
ECC-Kurve P_384 für ephemeren DH-Schlüsselaustausch	Ja	Ja
ECC-Kurve P_521 für ephemeren DH-Schlüsselaustausch	Ja	Ja
Verkürzte Handshakes, wenn die ticket-basierte Sitzungswiederaufnahme aktiviert ist	Ja	Nein
0-RTT frühe Anwendungsdaten	Ja	Nein
Schutz vor Replay-Angriffen für frühe 0-RTT-Anwendungsdaten	Ja	*NA

SSL-Funktionen	Unterstützung am Frontend	Support im Backend
Optionale oder obligatorische zertifikatbasierte Client-Authentifizierung mit Unterstützung für die OCSP- und CRL-Validierung von Peer-Zertifikaten	Ja	Ja
Servernamenerweiterung: Auswahl des Serverzertifikats mithilfe von SNI	Ja	*NA
Anwendungsprotokollaushandlung (ALPN) mithilfe der Erweiterung application_level_protocol_negotiation	Ja	Ja
OCSP-Stapling	Ja	*NA
Protokollnachrichten und AppFlow-Datensätze werden für TLS 1.3-Handshakes erzeugt	Ja	Ja
Optionale Protokollierung von TLS 1.3-Datenverkehrsgeheimnissen durch das Paketerfassungsprogramm `nstrace`	Ja	Ja
Interoperabilität mit TLS-Peers, die RFC 8446 implementieren. Zum Beispiel Mozilla Firefox, Google Chrome und OpenSSL.	Ja	Ja

*NA — nicht zutreffend

Konfiguration

TLS 1.3 ist in einem SSL-Profil standardmäßig deaktiviert. Sie können TLS 1.3 zwar für das Legacy-Profil aktivieren, aber einige Funktionen, wie z. B. abgekürzte Handshakes, wenn die ticketbasierte Sitzungswiederaufnahme aktiviert ist, und 0-RTT-Anwendungsdaten für frühe 0-RTT-Anwendungen werden im Legacy-Profil nicht unterstützt.

Fügen Sie mithilfe der CLI ein Front-End-SSL-Profil hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl profile tls13profile -tls13 ENABLED
<!--NeedCopy-->
```

Beispiel:

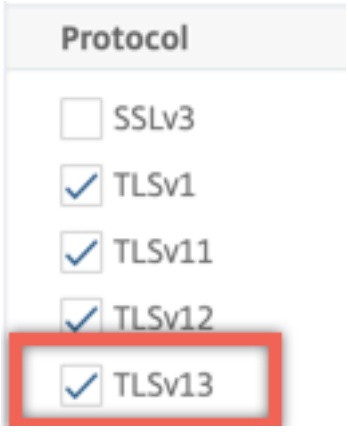
```
sh ssl profile tls13profile
1)  Name: tls13profile           (Front-End)
    SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1.1: ENABLED
       TLSv1.2: ENABLED  TLSv1.3: ENABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED                      Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED                            Refresh Count: 0
    Deny SSL Renegotiation                                ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:             1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions: NO
    Push flag:            0x0 (Auto)
    SSL quantum size:                            8 kB
    Encryption trigger timeout           100 mS
    Encryption trigger packet count:               45
```



```
28      Subject/Issuer Name Insertion Format: Unicode
29
30      SSL Interception: DISABLED
31      SSL Interception OCSP Check: ENABLED
32      SSL Interception End to End Renegotiation: ENABLED
33      SSL Interception Maximum Reuse Sessions per Server:  10
34      Session Ticket: DISABLED
35      HSTS: DISABLED
36      HSTS IncludeSubDomains: NO
37      HSTS Max-Age: 0
38
39      ECC Curve: P_256, P_384, P_224, P_521
40
41  1)  Cipher Name: DEFAULT Priority :1
42      Description: Predefined Cipher Alias
43  Done
44  <!--NeedCopy-->
```

Fügen Sie mithilfe der GUI ein Front-End-SSL-Profil hinzu

1. Navigieren Sie zu **System > Profiles**. Wählen Sie **SSL-Profile**.
2. Klicken Sie auf **Hinzufügen** und geben Sie einen Namen für das Profil an.
3. Wählen Sie **unter ProtokollTLSv13**aus.



4. Klicken Sie auf **OK** und dann auf **Fertig**.

Fügen Sie mithilfe der CLI ein Back-End-SSL-Profil hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  add ssl profile profile1 -sslprofileType BackEnd -tls13 ENABLED
```



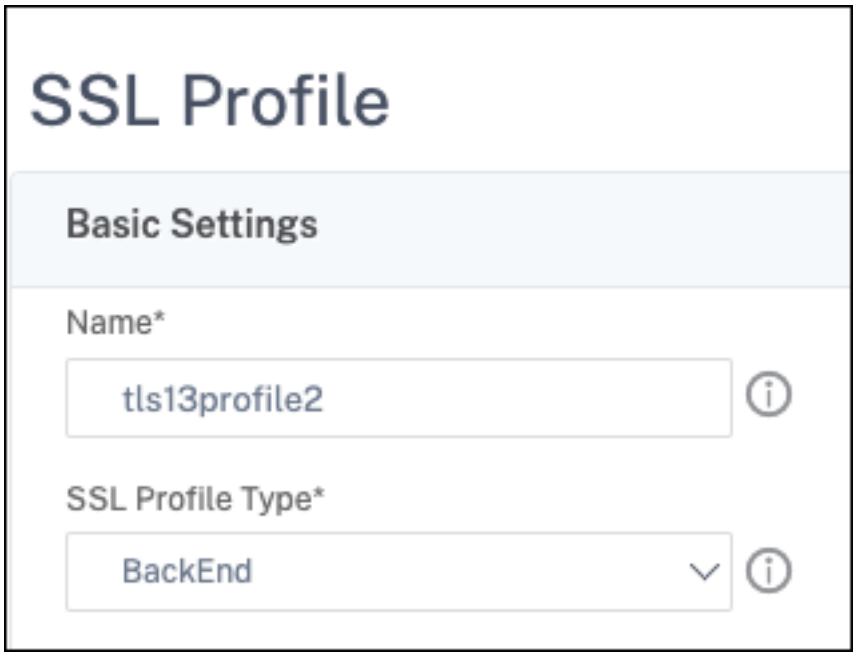
```
<!--NeedCopy-->
```

Beispiel:

```
add ssl profile tls13profile2 -sslprofileType BackEnd

sh ssl profile tls13profile2

1) Name: tls13profile2 (Back-End)

    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: ENABLED
    Server Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks: NO
    Session Reuse: ENABLED Timeout: 300 seconds
    DH: DISABLED
    Ephemeral RSA: DISABLED
    Deny SSL Renegotiation ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout: 1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions: NO
    Push flag: 0x0 (Auto)
    SSL quantum size: 8 kB
    Encryption trigger timeout 100 mS
    Encryption trigger packet count: 45
    Allow Extended Master Secret: NO
    ECC Curve: P_256, P_384, P_224, P_521

1) Cipher Name: DEFAULT_BACKEND Priority :1
    Description: Predefined Cipher Alias

 Done
<!--NeedCopy-->
```


Fügen Sie mithilfe der GUI ein Back-End-SSL-Profil hinzu

1. Navigieren Sie zu **System > Profiles**. Wählen Sie **SSL-Profile**.
2. Klicken Sie auf **Hinzufügen** und geben Sie einen Namen für das Profil an.
3. Wählen Sie unter **SSL-Profiltyp** die Option **BackEnd** aus.



4. Wählen Sie **unter ProtokollTLSv13**aus.
5. Klicken Sie auf **OK** und dann auf **Fertig**.

Binden Sie ein SSL-Profil über die CLI an einen virtuellen SSL-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vserverName> -sslProfile <profile-name>
```

Beispiel:

```
set ssl vserver ssl-vs -sslProfile tls13profile
```

Binden Sie ein SSL-Profil über die GUI an einen virtuellen SSL-Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und wählen Sie einen virtuellen SSL-Server aus.
2. Klicken Sie auf **Edit**.
3. Klicken Sie **unter Erweiterte Einstellungen**auf **SSL-Profil**.
4. Wählen Sie das zuvor erstellte TLS 1.3-Profil aus.
5. Klicken Sie auf **OK** und dann auf **Fertig**.

Binden Sie ein SSL-Profil mithilfe der CLI an einen SSL-Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl service <serviceName> -sslProfile <profile-name>
```

Beispiel:

```
set ssl service ssl-service -sslProfile tls13profile2
```

> Hinweis:
>
> Eine Warnung wird angezeigt, wenn Sie ein Front-End-Profil an einen SSL-Dienst binden.

Binden Sie ein SSL-Profil mithilfe der GUI an einen SSL-Dienst

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und wählen Sie einen SSL-Dienst aus.
2. Klicken Sie auf **Edit**.
3. Klicken Sie **unter Erweiterte Einstellungen**auf **SSL-Profil**.
4. Wählen Sie das zuvor erstellte TLS 1.3-Profil aus.
5. Klicken Sie auf **OK** und dann auf **Fertig**.

SSL-Profilparameter für das TLS 1.3-Protokoll

> Hinweis:
>
> Nur **tls13** gilt für ein Back-End-SSL-Profil.

1. Aktivieren oder deaktivieren Sie TLS 1.3-Parameter in einem SSL-Profil.

   tls13: Status der Unterstützung des TLS 1.3-Protokolls für das SSL-Profil.

   Mögliche Werte: ENABLED, DISABLED

   Standardwert: DISABLED

   ```
   1 set ssl profile tls13profile -tls13 enable
   2 <!--NeedCopy-->
   ```

   ```
   1 set ssl profile tls13profile -tls13 disable
   2 <!--NeedCopy-->
   ```

2. Legen Sie die Anzahl der ausgestellten Sitzungstickets fest.

   tls13SessionTicketsPerAuthContext: Anzahl der Tickets, die der virtuelle SSL-Server ausgibt, wenn TLS 1.3 ausgehandelt wird, die ticketbasierte Wiederaufnahme aktiviert ist und

entweder (1) ein Handshake abgeschlossen wird oder (2) die Client-Authentifizierung nach dem Handshake abgeschlossen wird.

Dieser Wert kann erhöht werden, damit Peers mehrere parallele Verbindungen mit einem neuen Ticket für jede Verbindung öffnen können.

Es werden keine Tickets gesendet, wenn die Wiederaufnahme deaktiviert ist.

Standardwert: 1

Mindestwert: 1

Maximaler Wert: 10

```
set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 1

set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 10
<!--NeedCopy-->
```

3. Stellen Sie den DH-Schlüsselaustausch ein.

   dheKeyExchangeWithPsk: Gibt an, ob ein virtueller SSL-Server einen DHE-Schlüsselaustausch erfordert, wenn ein vorab freigegebener Schlüssel während eines Handshakes zur Wiederaufnahme einer TLS 1.3-Sitzung akzeptiert wird. Ein DHE-Schlüsselaustausch gewährleistet die Vorwärtsgeheimnis, auch wenn Ticketschlüssel kompromittiert sind, auf Kosten zusätzlicher Ressourcen, die für die Durchführung des **DHE-Schlüsselaustauschs** erforderlich sind.

   Die verfügbaren Einstellungen funktionieren wie folgt, wenn das Sitzungsticket aktiviert ist:

   JA: Ein DHE-Schlüsselaustausch ist erforderlich, wenn ein vorab freigegebener Schlüssel akzeptiert wird, unabhängig davon, ob der Kunde den Schlüsselaustausch unterstützt. Der Handshake wird mit einer schwerwiegenden Warnung abgebrochen, wenn der Client den DHE-Schlüsselaustausch nicht unterstützt, wenn er einen vorab freigegebenen Schlüssel anbietet.

   NEIN: Der DHE-Schlüsselaustausch wird durchgeführt, wenn ein vorab freigegebener Schlüssel akzeptiert wird, nur wenn dies vom Kunden angefordert wird.

   Mögliche Werte: JA, NEIN

   Standardwert: NO

   ```
   set ssl profile tls13profile dheKeyExchangeWithPsk yes

   set ssl profile tls13profile dheKeyExchangeWithPsk no
   <!--NeedCopy-->
   ```

4. Aktivieren oder deaktivieren Sie die frühzeitige Datenakzeptanz von 0-RTT.

`zeroRttEarlyData`: Stand der frühen Anwendungsdaten von TLS 1.3. Die zutreffenden Einstellungen funktionieren wie folgt:

ENABLED: Frühe Anwendungsdaten werden möglicherweise verarbeitet, bevor der Handshake abgeschlossen ist.

DISABLED: Frühe Anwendungsdaten werden ignoriert.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

```
set ssl profile tls13profile -zeroRttEarlyData ENABLED

set ssl profile tls13profile -zeroRttEarlyData DISABLED
<!--NeedCopy-->
```

Standard-Verschlüsselungsgruppe

Die Standard-Verschlüsselungsgruppe umfasst TLS 1.3-Chiffren.

```
sh cipher DEFAULT
1) Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035

2)  Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
...
...
27) Cipher Name: TLS 1.3-AES256-GCM-SHA384         Priority : 27
    Description: TLS 1.3 Kx=any      Au=any  Enc=AES-GCM(256) Mac=AEAD
         HexCode=0x1302

28) Cipher Name: TLS 1.3_CHACHA20_POLY1305_SHA256     Priority : 28
    Description: TLS 1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256)
        Mac=AEAD   HexCode=0x1303

29) Cipher Name: TLS 1.3-AES128_GCM-SHA256        Priority : 29
    Description: TLS 1.3 Kx=any      Au=any  Enc=AES-GCM(128) Mac=AEAD
         HexCode=0x1301
Done
<!--NeedCopy-->
```



```
sh cipher DEFAULT_BACKEND
1)  Cipher Name: TLS1-AES-256-CBC-SHA   Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)  Cipher Name: TLS1-AES-128-CBC-SHA   Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
...
...
27) Cipher Name: TLS 1.3-AES256-GCM-SHA384   Priority : 27
    Description: TLS 1.3 Kx=any      Au=any  Enc=AES-GCM(256) Mac=AEAD
         HexCode=0x1302
28) Cipher Name: TLS 1.3-CHACHA20-POLY1305-SHA256    Priority : 28
    Description: TLS 1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256)
        Mac=AEAD   HexCode=0x1303
29) Cipher Name: TLS 1.3-AES128-GCM-SHA256   Priority : 29
    Description: TLS 1.3 Kx=any      Au=any  Enc=AES-GCM(128) Mac=AEAD
         HexCode=0x1301
 Done
<!--NeedCopy-->
```

Einschränkungen

- TLS 1.3 wird auf einer NetScaler FIPS-Appliance nicht unterstützt.
- In einem TLS 1.3-Handshake werden nur RSA-Zertifikate mit 1024-Bit-Schlüsseln und größeren Schlüsseln unterstützt.

Beschränkungen der Sicherheit

TLS 1.3-Serverbetreiber müssen die folgenden Sicherheitseinschränkungen aus Gründen der Abwärtskompatibilität beachten, die in RFC 8446 beschrieben sind. Die Standardkonfiguration auf einer NetScaler-Appliance entspricht diesen Einschränkungen. Eine NetScaler-Appliance setzt diese Regeln jedoch nicht durch.

- Die Sicherheit von RC4-Verschlüsselungssammlungen wird als unzureichend angesehen, wie in RFC7465 beschrieben. Implementierungen dürfen keine RC4-Verschlüsselungssammlungen für irgendeine Version von TLS anbieten oder aushandeln.
- Alte Versionen von TLS ermöglichten die Verwendung von Chiffren mit geringer Stärke. Chiffren mit einer Stärke von weniger als 112 Bit dürfen für keine Version von TLS angeboten oder ausgehandelt werden.

- Die Sicherheit von SSL 3.0 [SSLv3] wird wie in RFC7568 beschrieben als unzureichend angesehen und darf nicht ausgehandelt werden. Deaktivieren Sie SSLv3, wenn TLS 1.3 aktiviert ist (SSLv3 ist standardmäßig deaktiviert).

> **Hinweis:**
>
> Informationen zur Problembehandlung bei Protokollen, die über TLS 1.3 laufen, finden Sie unter Entschlüsseln von TLS 1.3-Verkehr aus der Paketverfolgung.

Anleitungsartikel

May 11, 2023

Bei den Artikeln mit Anleitungen handelt es sich um einfache und benutzerfreundliche Artikel mit Konfigurationsschritten für gängige Bereitstellungen. Klicken Sie auf einen Link, um den Artikel anzusehen.

Erstellen einer Zertifikatsignaturanforderung und Verwenden von SSL-Zertifikaten auf einer NetScaler Appliance

SSL-Aktion konfigurieren, um den Client-Verkehr weiterzuleiten

Konfigurieren Sie die SSL-Aktion, um den Client-Verkehr weiterzuleiten, wenn eine Chiffre auf dem ADC nicht unterstützt wird

Client-Authentifizierung pro Verzeichnis konfigurieren

Konfigurieren der Unterstützung für Outlook Web Access

SSL-basiertes Einfügen von Headern konfigurieren

Konfigurieren Sie SSL-Offloading mit Ende-zu-Ende-Verschlüsselung

Transparente SSL-Beschleunigung konfigurieren

Konfigurieren Sie die SSL-Beschleunigung mit HTTP im Frontend und SSL im Backend

SSL-Offloading mit anderen TCP-Protokollen konfigurieren

SSL-Bridging konfigurieren

Konfigurieren Sie die SSL-Überwachung, wenn die Client-Authentifizierung im Back-End-Dienst aktiviert ist

Konfigurieren Sie einen sicheren Content Switching-Server

Konfigurieren Sie einen virtuellen HTTPS-Server, um HTTP-Verkehr zu akzeptieren

Konfigurieren Sie die anmutige Bereinigung von SSL-Sitzungen

SSL-Zertifikate

May 11, 2023

Ein SSL-Zertifikat, das Teil einer SSL-Transaktion ist, ist ein digitales Datenformular (X509), das ein Unternehmen (Domain) oder eine Einzelperson identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der NetScaler-Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung asymmetrischer Schlüssel (oder öffentlicher Schlüssel) abzuschließen.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

- Von einer autorisierten Zertifizierungsstelle (CA) wie Verisign
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der NetScaler-Appliance

Alternativ können Sie ein vorhandenes SSL-Zertifikat auf der Appliance verwenden.

Zertifikate werden von der NetScaler-Appliance in vier Typen eingeteilt:

- **Serverzertifikate:** Ein Serverzertifikat authentifiziert die Identität des Servers gegenüber dem Client. Im Front-End fungiert die ADC-Appliance als Server. Sie binden ein Serverzertifikat und einen privaten Schlüssel an einen virtuellen SSL-Server auf der ADC-Appliance.
- **Clientzertifikate:** Ein Clientzertifikat authentifiziert die Identität des Clients gegenüber dem Server. Im Back-End fungiert die ADC-Appliance als Client. Sie binden ein Clientzertifikat und einen privaten Schlüssel an den SSL-Dienst oder die Dienstgruppe auf der ADC-Appliance.
- **CA-Zertifikate:** CA-Zertifikate stellen die Endbenutzerzertifikate aus (Client- und Serverzertifikate). Ein CA-Zertifikat kann eine vertrauenswürdige Stammzertifizierungsstelle (von der Zertifizierungsstelle selbst signiert) oder eine zwischengeschaltete CA (signiert von einer vertrauenswürdigen Stammzertifizierungsstelle) sein. Normalerweise benötigen CA-Zertifikate keine privaten Schlüssel.
- **Unbekannte Zertifikate:** Alle anderen Zertifikate fallen in diese Kategorie.

Wichtig: Citrix empfiehlt, dass Sie Zertifikate von autorisierten Zertifizierungsstellen wie Verisign für alle Ihre SSL-Transaktionen verwenden. Verwenden Sie Zertifikate, die auf der NetScaler-Appliance generiert werden, nur zu Testzwecken, nicht in einer Live-Bereitstellung.

- Wenn Sie beim Hinzufügen eines Zertifikatschlüsselpaars eine Zertifikatsdatei mit demselben Namen wie eine vorhandene Zertifikatsdatei hinzufügen, wird die ursprüngliche Zertifikatdatei ohne Warnung überschrieben. Diese Aktion kann nach dem Neustart der Appliance zu Problemen führen, da die ursprüngliche Zertifikatsdatei im `/nsconfig/ssl` Verzeichnis nicht mehr verfügbar ist.
- Das Entfernen von Zertifikaten oder Schlüsseldateien in einer Clusterumgebung schränkt die weitere Konfiguration auf der ADC-Appliance ein. Fügen Sie die Dateien wieder am selben Ort hinzu, um Konfigurationsänderungen vorzunehmen.

Hinweis: Sie können das ADM SSL-Dashboard verwenden, um die SSL-Zertifikatsverwaltung zu vereinfachen und Benachrichtigungen für Zertifikate festzulegen, die nicht verwendet werden oder bald ablaufen. Weitere Informationen finden Sie unter Verwaltung von SSL-Zertifikaten.

Zertifikat erstellen

August 4, 2023

Eine Zertifizierungsstelle (CA) ist eine Stelle, die digitale Zertifikate für die Verwendung in der Kryptografie mit öffentlichen Schlüsseln ausstellt. Anwendungen wie Webbrowser, die SSL-Transaktionen durchführen, vertrauen Zertifikaten, die von einer Zertifizierungsstelle ausgestellt oder signiert wurden. Diese Anwendungen führen eine Liste der Zertifizierungsstellen, denen sie vertrauen. Wenn einer der vertrauenswürdigen Zertifizierungsstellen das für die sichere Transaktion verwendete Zertifikat signiert, setzt die Anwendung die Transaktion fort.

Vorsicht: Citrix empfiehlt, dass Sie für alle Ihre SSL-Transaktionen Zertifikate verwenden, die von autorisierten Zertifizierungsstellen wie Verisign bezogen wurden. Verwenden Sie Zertifikate, die auf der NetScaler-Appliance generiert werden, nur zu Testzwecken, nicht in einer Live-Bereitstellung.

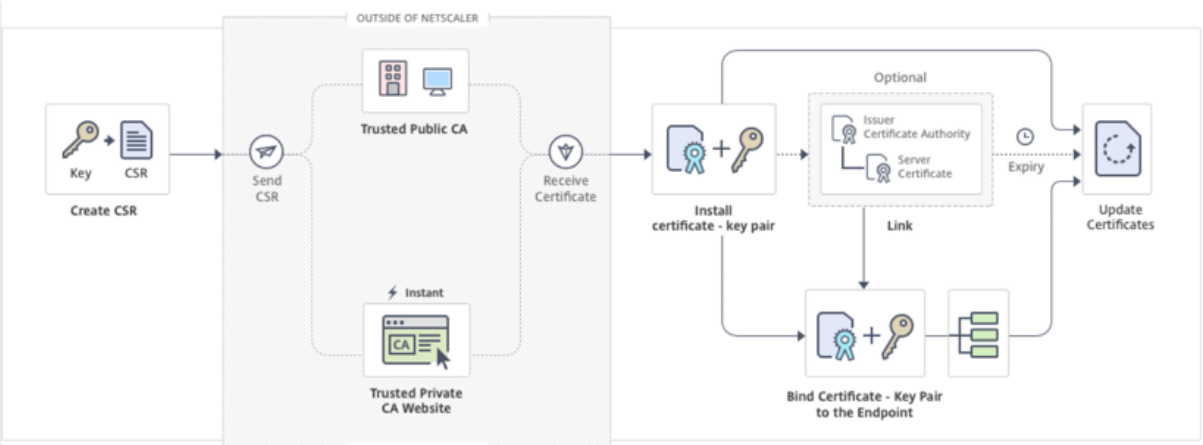
Informationen zum Importieren eines vorhandenen Zertifikats und Schlüssels finden Sie unter Importieren eines Zertifikats.

Führen Sie die folgenden Schritte aus, um ein Zertifikat zu erstellen und es an einen virtuellen SSL-Server zu binden. Die einzigen Sonderzeichen, die in den Dateinamen zulässig sind, sind Unterstrich und Punkt. Sonderzeichen sind als erstes Zeichen im Dateinamen nicht zulässig.

- Erstellen Sie einen privaten Schlüssel.
- Erstellen Sie eine Zertifikatssignieranforderung (CSR).
- Reichen Sie die CSR bei einer Zertifizierungsstelle ein.

- Erstellen Sie ein Zertifikatsschlüsselpaar.
- Binden Sie das Zertifikatsschlüsselpaar an einen virtuellen SSL-Server

Das folgende Diagramm veranschaulicht den Arbeitsablauf.



So erstellen und installieren Sie ein neues Zertifikat

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Erstellen eines privaten Schlüssels

> **Hinweise:**
>
> - Ab Version 12.1 Build 49.x können Sie den AES256-Algorithmus mit dem PEM-Schlüsselformat verwenden, um einen privaten Schlüssel auf der Appliance zu verschlüsseln. AES mit 256-Bit-Schlüssel ist mathematisch effizienter und sicherer als der 56-Bit-Schlüssel des Data Encryption Standard (DES).
> - Ab Version 12.1 Build 50.x können Sie einen RSA-Schlüssel im PKCS #8 -Format erstellen.

Der private Schlüssel ist der wichtigste Teil eines digitalen Zertifikats. Per Definition darf dieser Schlüssel nicht mit irgendjemandem geteilt werden und muss sicher auf der NetScaler Appliance aufbewahrt werden. Alle mit dem öffentlichen Schlüssel verschlüsselten Daten können nur mit dem privaten Schlüssel entschlüsselt werden.

Das Zertifikat, das Sie von der Zertifizierungsstelle erhalten, ist nur mit dem privaten Schlüssel gültig, der zum Erstellen der CSR verwendet wurde. Der Schlüssel ist erforderlich, um das Zertifikat zur NetScaler Appliance hinzuzufügen.

Die Appliance unterstützt nur die RSA-Verschlüsselungsalgorithmen zum Erstellen privater Schlüssel. Sie können beide Arten von privaten Schlüsseln an die Zertifizierungsstelle (CA) senden. Das Zertifikat, das Sie von der Zertifizierungsstelle erhalten, ist nur mit dem privaten Schlüssel gültig, der zum

Erstellen der CSR verwendet wurde. Der Schlüssel ist erforderlich, um das Zertifikat zur NetScaler Appliance hinzuzufügen.

Wichtig:

> - Beschränken Sie unbedingt den Zugriff auf Ihren privaten Schlüssel. Jeder, der Zugriff auf Ihren privaten Schlüssel hat, kann Ihre SSL-Daten entschlüsseln.
> - Die Länge des zulässigen SSL-Schlüsselnamens umfasst die Länge des absoluten Pfadnamens, wenn der Pfad im Schlüsselnamen enthalten ist.

Alle SSL-Zertifikate und Schlüssel werden im Ordner `/nsconfig/ssl` auf der Appliance gespeichert. Für zusätzliche Sicherheit können Sie den DES- oder Triple DES (3DES) -Algorithmus verwenden, um den auf der Appliance gespeicherten privaten Schlüssel zu verschlüsseln.

Erstellen eines privaten RSA-Schlüssels mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

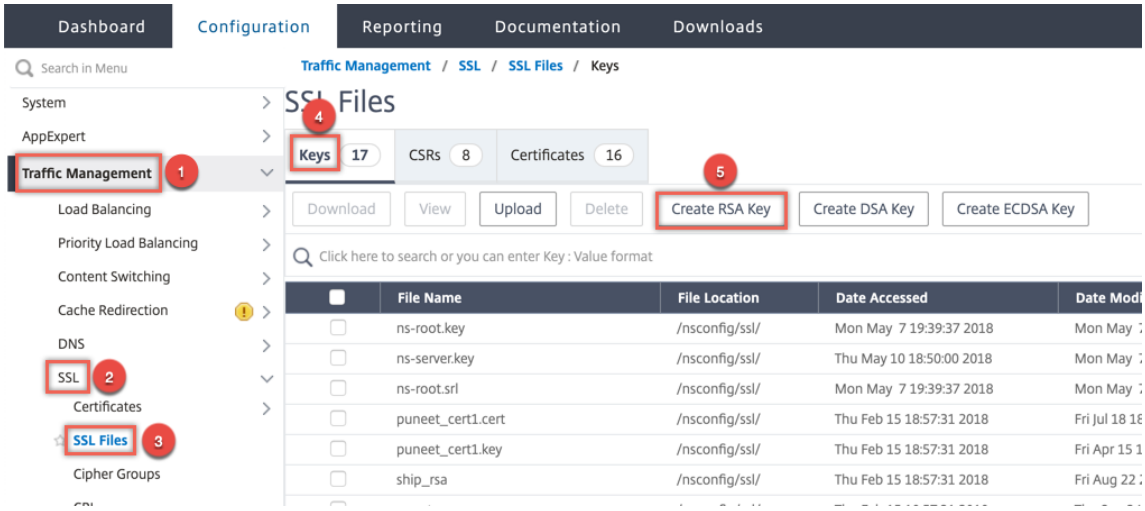
```
create ssl rsakey <keyFile> <bits> [-exponent ( 3 | F4 )] [-keyform (
   DER | PEM )] [-des | -des3 | -aes256] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Beispiel:

```
create rsakey testkey 2048 -aes256 -password 123456 -pkcs8
<!--NeedCopy-->
```

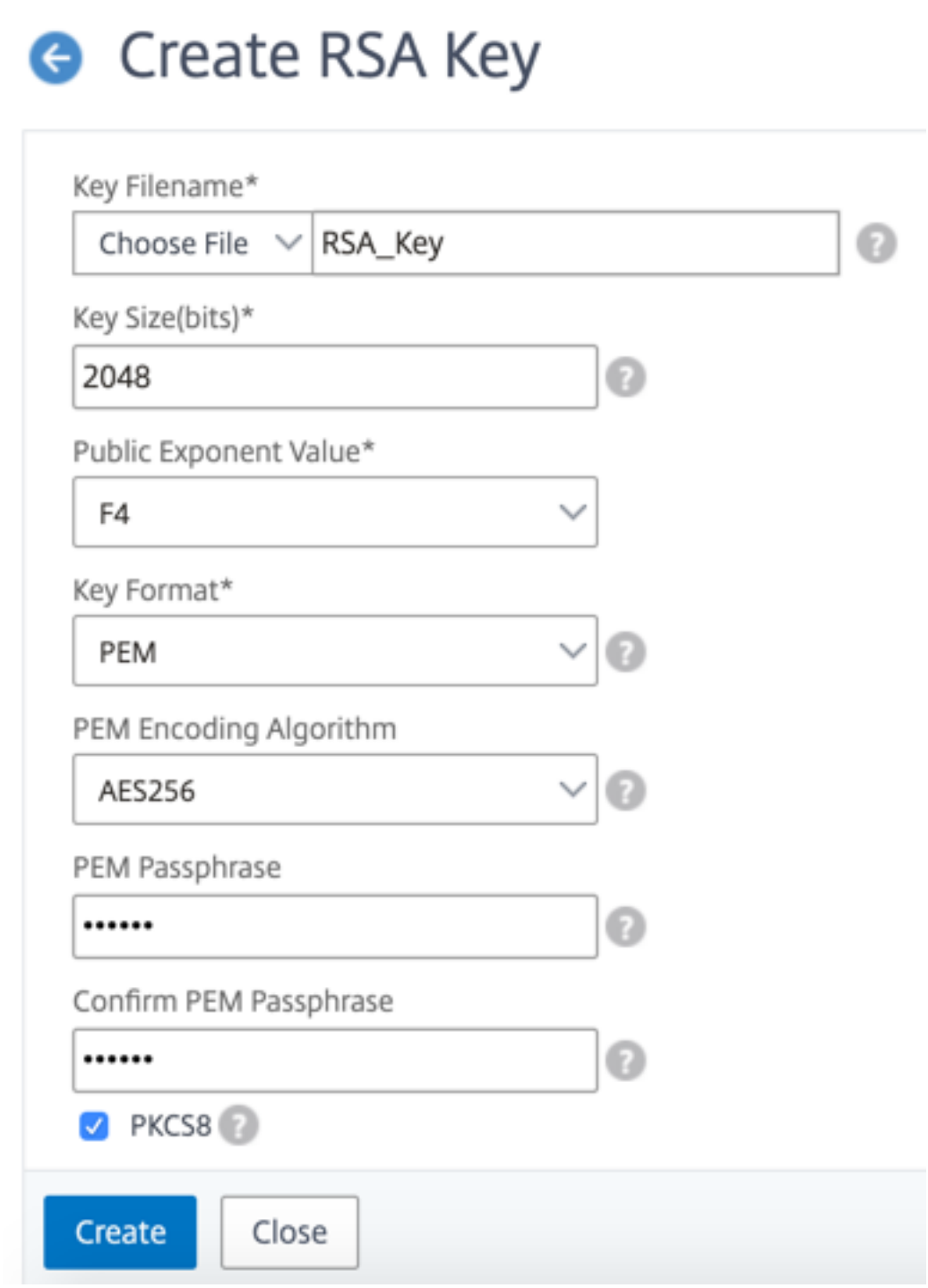
Erstellen eines privaten RSA-Schlüssels mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Dateien**.
2. Wählen Sie auf der Registerkarte **Keys** die Option **RSA-Schlüssel erstellen**aus.



3. Geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

   - **Key Filename** — Name für und optional Pfad zur RSA-Schlüsseldatei. /nsconfig/ssl/ ist der Standardpfad.
   - **Schlüsselgröße** — Größe des RSA-Schlüssels in Bit. Kann von 512 Bit bis 4096 Bit reichen.
   - **Öffentlicher Exponentenwert** — Öffentlicher Exponent für den RSA-Schlüssel. Der Exponent ist Teil des Verschlüsselungsalgorithmus und wird zum Erstellen des RSA-Schlüssels benötigt.
   - **Schlüsselformat** — Das Format, in dem die RSA-Schlüsseldatei auf der Appliance gespeichert ist.
   - **PEM-Codierungsalgorithmus** - Verschlüsseln Sie den generierten RSA-Schlüssel mithilfe des AES 256-, DES- oder Triple-DES (DES3) -Algorithmus. Standardmäßig sind private Schlüssel unverschlüsselt.
   - **PEM-Passphrase — Wenn der private Schlüssel verschlüsselt ist, geben Sie eine Passphrase** für den Schlüssel ein.



Wählen Sie über die grafische Benutzeroberfläche einen AES256-Codierungsalgorithmus in einem RSA-Schlüssel

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Dateien > RSA-Schlüssel erstellen**.

2. Wählen Sie **unter SchlüsselformatPEM**aus.
3. Wählen Sie im **PEM-KodierungsalgorithmusAES256**aus.
4. Wählen Sie **PKCS8**.

Erstellen einer Zertifikatsignaturanforderung mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

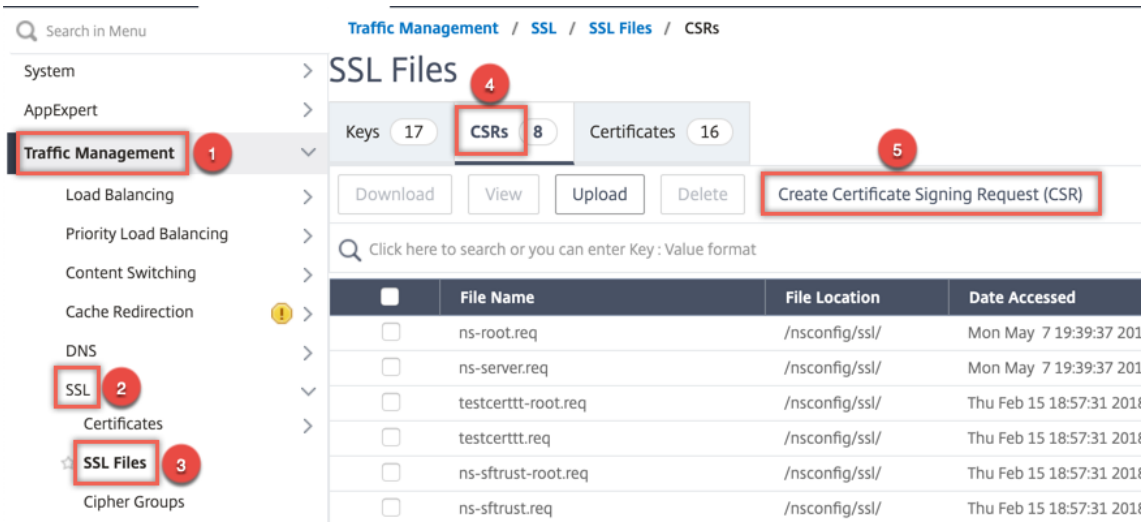
```
create ssl certreq <reqFile> -keyFile <input_filename> | -fipsKeyName <
   string>) [-keyForm (DER | PEM) {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName <string>
     -organizationUnitName <string> -localityName <string> -commonName
    <string> -emailAddress <string> {
 -challengePassword  }
  -companyName <string> -digestMethod ( SHA1 | SHA256 )
<!--NeedCopy-->
```

Beispiel:

```
create ssl certreq priv_csr_sha256 -keyfile priv_2048_2 -keyform PEM -
   countryName IN -stateName Karnataka -localityName Bangalore -
   organizationName Citrix -organizationUnitName NS -digestMethod
   SHA256
<!--NeedCopy-->
```

Erstellen einer Zertifikatssignieranforderung über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie in **SSL-Zertifikat** auf **Certificate Signing Request (CSR) erstellen**



3. Wählen Sie unter **Digest-Methode** die Option **SHA256** aus.

Weitere Informationen finden Sie unter Erstellen einer CSR .

Unterstützung für alternativen Antragstellernamen in einer Zertifikatsignieranforderung

Das Feld “Subject Alternative Name” (SAN) in einem Zertifikat ermöglicht es Ihnen, mehrere Werte, wie Domänennamen und IP-Adressen, einem einzigen Zertifikat zuzuordnen. Mit anderen Worten, Sie können mehrere Domänen wie www.example.com, www.example1.com, www.example2.com, mit einem einzigen Zertifikat sichern.

Einige Browser, wie Google Chrome, unterstützen keinen gebräuchlichen Namen in einer Zertifikatssignieranforderung (CSR) mehr. Sie setzen SAN in allen öffentlich vertrauenswürdigen Zertifikaten durch.

Die NetScaler Appliance unterstützt das Hinzufügen von SAN-Werten beim Erstellen einer CSR. Sie können eine CSR mit einem SAN-Eintrag an eine Zertifizierungsstelle senden, um ein signiertes Zertifikat mit diesem SAN-Eintrag zu erhalten. Wenn die Appliance eine Anforderung erhält, sucht sie in den SAN-Einträgen im Serverzertifikat nach einem übereinstimmenden Domänennamen. Wenn eine Übereinstimmung gefunden wird, sendet es das Zertifikat an den Client und schließt den SSL-Handshake ab. Sie können die CLI oder die GUI verwenden, um eine CSR mit SAN-Werten zu erstellen.

> **Hinweis:** Die NetScaler Appliance verarbeitet nur DNS-basierte SAN-Werte.

Erstellen einer CSR mit dem alternativen Antragstellernamen mithilfe der CLI

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-subjectAltName <string>] [-keyform ( DER | PEM )  {
-PEMPassPhrase  }
```



```
3   ] -countryName <string> -stateName <string> -organizationName <string>
        [-organizationUnitName <string>] [-localityName <string>] [-
       commonName <string>] [-emailAddress <string>] {
4   -challengePassword  }
5    [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
6   <!--NeedCopy-->
```

Parameter:

SubjectAltName: Der alternative Antragstellername (SAN) ist eine Erweiterung von X.509, mit der verschiedene Werte mithilfe eines SubjectAltName-Feldes mit einem Sicherheitszertifikat verknüpft werden können. Diese Werte werden als "Subject Alternative Names" (SAN) bezeichnet. Zu den Namen gehören:

1. IP-Adressen (Präfix mit "IP:" Beispiel: IP:198.51.10.5 IP:192.0.2.100)
2. DNS-Namen (Präfix mit "DNS:" Beispiel: DNS: www.example.com DNS: www.example.org DNS: www.example.net)

Geben Sie in der Befehlszeile Werte in Anführungszeichen ein. Trennen Sie zwei Werte durch ein Leerzeichen. Anführungszeichen sind in der GUI nicht erforderlich.
Maximale Länge: 127

Beispiel:

```
1  create certReq test1.csr -keyFile test1.ky -countryName IN -stateName
       Kar -organizationName citrix -commonName ctx.com -subjectAltName "
       DNS:*.example.com DNS:www.example.org DNS:www.example.net"
2  <!--NeedCopy-->
```

> **Hinweis:**
>
> Auf einer FIPS-Appliance müssen Sie den Schlüsseldateinamen durch den FIPS-Schlüsselnamen ersetzen, wenn Sie den FIPS-Schlüssel direkt auf der Appliance erstellen.
>
> ```
> 1  create certReq <csrname> -fipsKeyName fipskey.ky -countryName IN -
>        stateName Kar -organizationName citrix -commonName ctx.com -
>        subjectAltName "DNS:www.example.com DNS:www.example.org DNS:www.
>        example.net"
> 2  <!--NeedCopy-->
> ```

Erstellen einer CSR mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **SSL-Dateien**.
2. Klicken Sie auf der Registerkarte **CSR** auf **Certificate Signing Request (CSR) erstellen**.
3. Geben Sie die Werte ein und klicken Sie auf **Erstellen**.

Einschränkungen

Um SAN beim Erstellen eines SSL-Zertifikats zu verwenden, müssen Sie die SAN-Werte explizit angeben. Die Werte werden nicht automatisch aus der CSR-Datei gelesen.

Reichen Sie die CSR bei der Zertifizierungsstelle ein

Die meisten Zertifizierungsstellen (CA) akzeptieren die Einreichung von Zertifikaten per E-Mail. Die Zertifizierungsstelle gibt ein gültiges Zertifikat an die E-Mail-Adresse zurück, von der Sie die CSR übermitteln.

Die CSR ist im Ordner `/nsconfig/ssl` gespeichert.

Erstellen eines Testzertifikats

> **Hinweis:**
>
> Informationen zum Generieren eines Servertestzertifikats finden Sie unter Generieren eines Server-Testzertifikats.

Die NetScaler Appliance verfügt über eine integrierte Zertifizierungsstellen-Tools-Suite, mit der Sie selbstsignierte Zertifikate zu Testzwecken erstellen können.

Vorsicht: Da die NetScaler Appliance diese Zertifikate signiert und keine tatsächliche Zertifizierungsstelle, dürfen Sie sie nicht in einer Produktionsumgebung verwenden. Wenn Sie versuchen, ein selbstsigniertes Zertifikat in einer Produktionsumgebung zu verwenden, erhalten Benutzer bei jedem Zugriff auf den virtuellen Server eine Warnung “Zertifikat ungültig”.

Die Appliance unterstützt die Erstellung der folgenden Zertifikattypen:

- Root-CA-Zertifikate
- CA-Zertifikate für Fortgeschrittene
- Endbenutzer-Zertifikate
  - Server-Zertifikate
  - Client-Zertifikate

Erstellen Sie vor dem Generieren eines Zertifikats einen privaten Schlüssel und erstellen Sie damit eine Zertifikatssignierungsanforderung (CSR) auf der Appliance. Anstatt die CSR dann an eine Zertifizierungsstelle zu senden, verwenden Sie die NetScaler CA Tools, um ein Zertifikat zu generieren.

Erstellen eines Zertifikats mithilfe eines Assistenten

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Wählen Sie im Detailbereich unter **Erste Schritte**den Assistenten für den zu erstellenden Zertifikattyp aus.
3. Befolgen Sie die Anweisungen auf dem Bildschirm.

Erstellen eines Root-CA-Zertifikats mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
<!--NeedCopy-->
```

Im folgenden Beispiel ist csreq1 die CSR und rsa1 ist der private Schlüssel, der zuvor erstellt wurde.

Beispiel:

```
create ssl cert cert1 csreq1 ROOT_CERT -keyFile rsa1 -keyForm PEM -days
     365

  Done
<!--NeedCopy-->
```

Erstellen eines zwischengeschalteten CA-Zertifikats mithilfe der CLI

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
     [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
     DER | PEM )] [-CAkey <input_filename>] [-CAkeyForm ( DER | PEM )]
    [-CAserial <output_filename>]
<!--NeedCopy-->
```

Im folgenden Beispiel ist csr1 die zuvor erstellte CSR. Cert1 und rsakey1 sind das Zertifikat und der entsprechende Schlüssel des selbstsignierten Zertifikats (Root-CA), und pvtkey1 ist der private Schlüssel des zwischengeschalteten CA-Zertifikats.

Beispiel:

```
create ssl cert certsy csr1 INTM_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23
Done

create ssl rsakey pvtkey1 2048 -exponent F4 -keyform PEM
Done
<!--NeedCopy-->
```


Erstellen eines Root-CA-Zertifikats mit der GUI

Navigieren Sie zu **Traffic Management > SSL**, und wählen Sie in der Gruppe Erste Schritte den **Assistenten für das Root-CA-Zertifikat**aus, und konfigurieren Sie ein Stammzertifikat der Zertifizierungsstelle.

Erstellen eines zwischengeschalteten CA-Zertifikats über die grafische Benutzeroberfläche

Navigieren Sie zu **Traffic Management > SSL**, und wählen Sie in der Gruppe Erste Schritte den **Assistenten für zwischengeschaltete CA-Zertifikate**aus, und konfigurieren Sie ein zwischengeschaltetes CA-Zertifikat.

Erstellen eines Endbenutzerzertifikats

Ein Endbenutzerzertifikat kann ein Clientzertifikat oder ein Serverzertifikat sein. Um ein Testendbenutzerzertifikat zu erstellen, geben Sie das Zwischenzertifikat der Zertifizierungsstelle oder das selbstsignierte Root-CA-Zertifikat an.

> **Hinweis:** Um ein Endbenutzerzertifikat für die Produktionsverwendung zu erstellen, geben Sie ein vertrauenswürdiges CA-Zertifikat an und senden Sie die CSR an eine Zertifizierungsstelle (CA).

Erstellen eines Test-Endbenutzerzertifikats mithilfe der Befehlszeilenschnittstelle

```
1 create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days<positive_integer>]
    [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
    DER | PEM )] [-CAkey<input_filename>] [-CAkeyForm ( DER | PEM )] [-
    CAserial <output_filename>]
2 <!--NeedCopy-->
```

Wenn kein Zwischenzertifikat vorhanden ist, verwenden Sie die Werte für das Zertifikat (cert1) und den privaten Schlüssel (rsakey1) des Root-CA-Zertifikats in `CAcert` und `CAkey`.

Beispiel:

```
1 create ssl cert cert12 csr1 SRVR_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23
2
3 Done
4 <!--NeedCopy-->
```

Wenn ein Zwischenzertifikat vorhanden ist, verwenden Sie die Werte für das Zertifikat (`certsy`) und den privaten Schlüssel (pvtkey1) des Zwischenzertifikats in `CAcert` und `CAkey`.

Beispiel:

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert certsy -CAkey pvtkey1 -
    CAserial 23

Done
<!--NeedCopy-->
```

Erstellen eines selbstsignierten SAN-Zertifikats mit OpenSSL

Um ein selbstsigniertes SAN-Zertifikat mit mehreren alternativen Antragstellernamen zu erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie eine OpenSSL-Konfigurationsdatei auf Ihrem lokalen Computer, indem Sie die entsprechenden Felder gemäß den Unternehmensanforderungen bearbeiten.

   Hinweis: Im folgenden Beispiel ist die Konfigurationsdatei “req.conf”.

   ```
   [req]
   distinguished_name = req_distinguished_name
   x509_extensions = v3_req
   prompt = no
   [req_distinguished_name]
   C = US
   ST = VA
   L = SomeCity
   O = MyCompany
   OU = MyDivision
   CN = www.company.com
   [v3_req]
   keyUsage = keyEncipherment, dataEncipherment
   extendedKeyUsage = serverAuth
   subjectAltName = @alt_names
   [alt_names]
   DNS.1 = www.company.net
   DNS.2 = company.com
   DNS.3 = company.net
   <!--NeedCopy-->
   ```

2. Laden Sie die Datei in das Verzeichnis /nsconfig/ssl auf der NetScaler Appliance hoch.
3. Melden Sie sich als Benutzer `nsroot` bei der NetScaler CLI an und wechseln Sie zur Shell-Eingabeaufforderung.
4. Führen Sie den folgenden Befehl aus, um das Zertifikat zu erstellen:


```
cd /nsconfig/ssl
openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout cert.
   pem -out cert.pem -config req.conf -extensions 'v3_req'
<!--NeedCopy-->
```

5. Führen Sie den folgenden Befehl aus, um das Zertifikat zu überprüfen:

```
openssl x509 -in cert.pem -noout  - text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
ed:90:c5:f0:61:78:25:ab
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Validity
Not Before: Nov 6 22:21:38 2012 GMT
Not After : Nov 6 22:21:38 2014 GMT
Subject: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
…
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage:
Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Subject Alternative Name:
DNS:www.company.net, DNS:company.com, DNS:company.net
Signature Algorithm: md5WithRSAEncryption …
<!--NeedCopy-->
```

Zertifikate installieren, verknüpfen und aktualisieren

August 15, 2023

Informationen zum Installieren eines Zertifikats finden Sie unter Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaares.

Verknüpfen von Zertifikaten

Viele Serverzertifikate sind von mehreren hierarchischen Zertifizierungsstellen (CA) signiert, was bedeutet, dass die Zertifikate eine Kette wie die folgende bilden:

```
Root CA
|
+---------- Intermediate CA
|
+---------------------- End-Entity (Server) Certificate
```

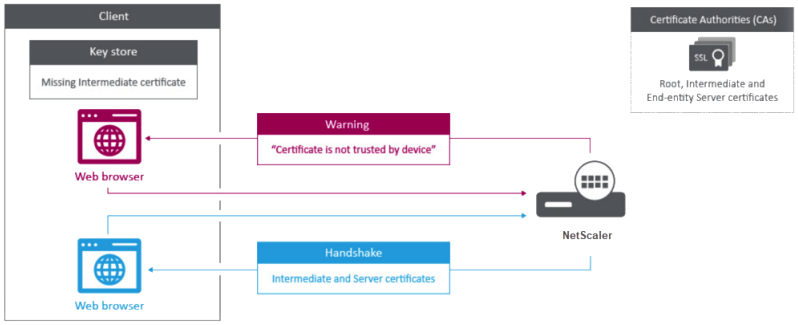
Manchmal wird die Zwischenzertifizierungsstelle in ein primäres und ein sekundäres Zwischenzertifikat der Zertifizierungsstelle aufgeteilt Dann bilden die Zertifikate eine Kette wie folgt:

```
Root CA
|
+------ Primary Intermediate CA
|+-------------- Secondary Intermediate CA
|
+---------------------- End-Entity (Server) Certificate
```

Clientcomputer enthalten normalerweise das Stammzertifizierungsstellenzertifikat in ihrem lokalen Zertifikatsspeicher, aber nicht ein oder mehrere zwischengeschaltete CA-Zertifikate. Die ADC-Appliance muss ein oder mehrere Zwischenzertifikate der Zertifizierungsstelle an die Clients senden.

Hinweis: Die Appliance darf das Stammzertifizierungsstellenzertifikat nicht an den Client senden. Für das Public Key Infrastructure (PKI) -Trust-Relationship-Modell müssen Root-CA-Zertifikate mithilfe einer Out-of-Band-Methode auf Clients installiert werden. Zum Beispiel sind die Zertifikate im Betriebssystem oder Webbrowser enthalten. Der Client ignoriert ein Stammzertifikat der Zertifizierungsstelle, das von der Appliance gesendet wurde.

Manchmal stellt eine zwischengeschaltete Zertifizierungsstelle, die Standardwebbrowser nicht als vertrauenswürdige Zertifizierungsstelle erkennen, das Serverzertifikat aus. In diesem Fall müssen ein oder mehrere CA-Zertifikate mit dem eigenen Zertifikat des Servers an den Client gesendet werden. Andernfalls beendet der Browser die SSL-Sitzung, da er das Serverzertifikat nicht authentifizieren kann.



In den folgenden Abschnitten finden Sie Informationen zum Hinzufügen von Server- und Zwischenzertifikaten:

- Manuelle Zertifikatsverknüpfung
- Automatisiertes Verknüpfen von
- Erstellen Sie eine Kette von Zertifikaten

So verknüpfen Sie ein zwischengeschaltetes Autoritätszertifikat

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Manuelle Zertifikatsverknüpfung

Hinweis: Diese Funktion wird auf der NetScaler FIPS-Plattform und in einem Cluster-Setup nicht unterstützt.

Anstatt einzelne Zertifikate hinzuzufügen und zu verknüpfen, können Sie jetzt ein Serverzertifikat und bis zu neun Zwischenzertifikate in einer einzigen Datei gruppieren. Sie können den Namen der Datei angeben, wenn Sie ein Zertifikat-Schlüsselpaar hinzufügen. Bevor Sie dies tun, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Die Zertifikate in der Datei haben die folgende Reihenfolge:
  - Serverzertifikat (muss das erste Zertifikat in der Datei sein)
  - Optional ein Serverschlüssel
  - Zwischenprodukt Zertifikat 1 (ic1)
  - Zwischenprodukt Zertifikat 2 (ic2)
  - Zwischenzertifikat 3 (ic3) usw.
    Hinweis: Zwischenzertifikatsdateien werden für jedes Zwischenzertifikat mit dem Namen "<certificatebundlename>.pem_ic <
    n>" erstellt, wobei n zwischen 1 und 9 liegt. Beispiel: bundle.pem_ic1, wobei **Bundle** der Name des Zertifikatssatzes und ic1 das erste Zwischenzertifikat im Satz ist.
- Bundle-Option ist ausgewählt.
- Die Datei enthält nicht mehr als neun Zwischenzertifikate.

Die Datei wird analysiert und das Serverzertifikat, die Zwischenzertifikate und der Serverschlüssel (falls vorhanden) werden identifiziert. Zunächst werden das Serverzertifikat und der Schlüssel hinzugefügt. Anschließend werden die Zwischenzertifikate in der Reihenfolge hinzugefügt, in der sie der Datei hinzugefügt wurden, und entsprechend verknüpft.

Ein Fehler wird gemeldet, wenn eine der folgenden Bedingungen zutrifft:

- Eine Zertifikatsdatei für eines der Zwischenzertifikate ist auf der Appliance vorhanden.
- Der Schlüssel wird in der Datei vor dem Serverzertifikat platziert.
- Ein Zwischenzertifikat wird vor das Serverzertifikat gestellt.

- Zwischenzertifikate werden nicht in derselben Reihenfolge in die Datei aufgenommen, in der sie erstellt wurden.
- In der Datei sind keine Zertifikate enthalten.
- Ein Zertifikat hat nicht das richtige PEM-Format.
- Die Anzahl der Zwischenzertifikate in der Datei übersteigt neun.

Hinzufügen eines Zertifikatssatzes mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Zertifikatssatz zu erstellen und die Konfiguration zu überprüfen:

```
add ssl certKey <certkeyName> -cert <string> -key <string> -bundle (YES
    | NO)

show ssl

show ssl certlink
<!--NeedCopy-->
```

Im folgenden Beispiel enthält der Zertifikatssatz (bundle.pem) die folgenden Dateien:

Serverzertifikat (Bundle) ist mit bundle_ic1 verknüpft

Erstes Zwischenzertifikat (bundle_ic1), das mit bundle_ic2 verknüpft ist

Zweites Zwischenzertifikat (bundle_ic2) mit bundle_ic3 verknüpft

Drittes Zwischenzertifikat (bundle_ic3)

```
add ssl certKey bundletest -cert bundle9.pem -key bundle9.pem -bundle
   yes

sh ssl certkey

1)      Name: ns-server-certificate
        Cert Path: ns-server.cert
        Key Path: ns-server.key
        Format: PEM
        Status: Valid,   Days to expiration:5733
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
```



```
        Issuer:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Validity
                Not Before: Apr 21 15:56:16 2016 GMT
                Not After : Mar  3 06:30:56 2032 GMT
        Subject:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

2)      Name: servercert
        Cert Path: complete/server/server_rsa_1024.pem
        Key Path: complete/server/server_rsa_1024.ky
        Format: PEM
        Status: Valid,   Days to expiration:7150
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 1F
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:  C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix
        Validity
                Not Before: Sep  2 09:54:07 2008 GMT
                Not After : Jan 19 09:54:07 2036 GMT
        Subject:  C=IN,ST=KAR,O=Citrix Pvt Ltd,CN=Citrix
        Public Key Algorithm: rsaEncryption
        Public Key size: 1024

3)      Name: bundletest
        Cert Path: bundle9.pem
        Key Path: bundle9.pem
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Validity
                Not Before: Nov 28 06:43:11 2014 GMT
                Not After : Nov 25 06:43:11 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=Server9
```



```
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

4)      Name: bundletest_ic1
        Cert Path: bundle9.pem_ic1
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Validity
                Not Before: Nov 28 06:42:56 2014 GMT
                Not After : Nov 25 06:42:56 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

5)      Name: bundletest_ic2
        Cert Path: bundle9.pem_ic2
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Validity
                Not Before: Nov 28 06:42:55 2014 GMT
                Not After : Nov 25 06:42:55 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

6)      Name: bundletest_ic3
        Cert Path: bundle9.pem_ic3
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
```



```
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Validity
                Not Before: Nov 28 06:42:53 2014 GMT
                Not After : Nov 25 06:42:53 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

7)      Name: bundletest_ic4
        Cert Path: bundle9.pem_ic4
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA5
        Validity
                Not Before: Nov 28 06:42:51 2014 GMT
                Not After : Nov 25 06:42:51 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

8)      Name: bundletest_ic5
        Cert Path: bundle9.pem_ic5
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA4
        Validity
                Not Before: Nov 28 06:42:50 2014 GMT
                Not After : Nov 25 06:42:50 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA5
```



```
149          Public Key Algorithm: rsaEncryption
150          Public Key size: 2048
151
152  9)      Name: bundletest_ic6
153          Cert Path: bundle9.pem_ic6
154          Format: PEM
155          Status: Valid,   Days to expiration:3078
156          Certificate Expiry Monitor: ENABLED
157          Expiry Notification period: 30 days
158          Certificate Type: Intermediate CA
159          Version: 3
160          Serial Number: 01
161          Signature Algorithm: sha256WithRSAEncryption
162          Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA3
163          Validity
164                  Not Before: Nov 28 06:42:48 2014 GMT
165                  Not After : Nov 25 06:42:48 2024 GMT
166          Subject:  C=IN,ST=ka,O=sslteam,CN=ICA4
167          Public Key Algorithm: rsaEncryption
168          Public Key size: 2048
169
170  10)     Name: bundletest_ic7
171          Cert Path: bundle9.pem_ic7
172          Format: PEM
173          Status: Valid,   Days to expiration:3078
174          Certificate Expiry Monitor: ENABLED
175          Expiry Notification period: 30 days
176          Certificate Type: Intermediate CA
177          Version: 3
178          Serial Number: 01
179          Signature Algorithm: sha256WithRSAEncryption
180          Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA2
181          Validity
182                  Not Before: Nov 28 06:42:46 2014 GMT
183                  Not After : Nov 25 06:42:46 2024 GMT
184          Subject:  C=IN,ST=ka,O=sslteam,CN=ICA3
185          Public Key Algorithm: rsaEncryption
186          Public Key size: 2048
187
188  11)     Name: bundletest_ic8
189          Cert Path: bundle9.pem_ic8
190          Format: PEM
191          Status: Valid,   Days to expiration:3078
192          Certificate Expiry Monitor: ENABLED
193          Expiry Notification period: 30 days
```



```
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Validity
                Not Before: Nov 28 06:42:45 2014 GMT
                Not After : Nov 25 06:42:45 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

12)     Name: bundletest_ic9
        Cert Path: bundle9.pem_ic9
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=RootCA4096
        Validity
                Not Before: Nov 28 06:42:43 2014 GMT
                Not After : Nov 25 06:42:43 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
Done

sh ssl certlink

1)      Cert Name: bundletest    CA Cert Name: bundletest_ic1
2)      Cert Name: bundletest_ic1        CA Cert Name: bundletest_ic2
3)      Cert Name: bundletest_ic2        CA Cert Name: bundletest_ic3
4)      Cert Name: bundletest_ic3        CA Cert Name: bundletest_ic4
5)      Cert Name: bundletest_ic4        CA Cert Name: bundletest_ic5
6)      Cert Name: bundletest_ic5        CA Cert Name: bundletest_ic6
7)      Cert Name: bundletest_ic6        CA Cert Name: bundletest_ic7
8)      Cert Name: bundletest_ic7        CA Cert Name: bundletest_ic8
9)      Cert Name: bundletest_ic8        CA Cert Name: bundletest_ic9
Done
<!--NeedCopy-->
```

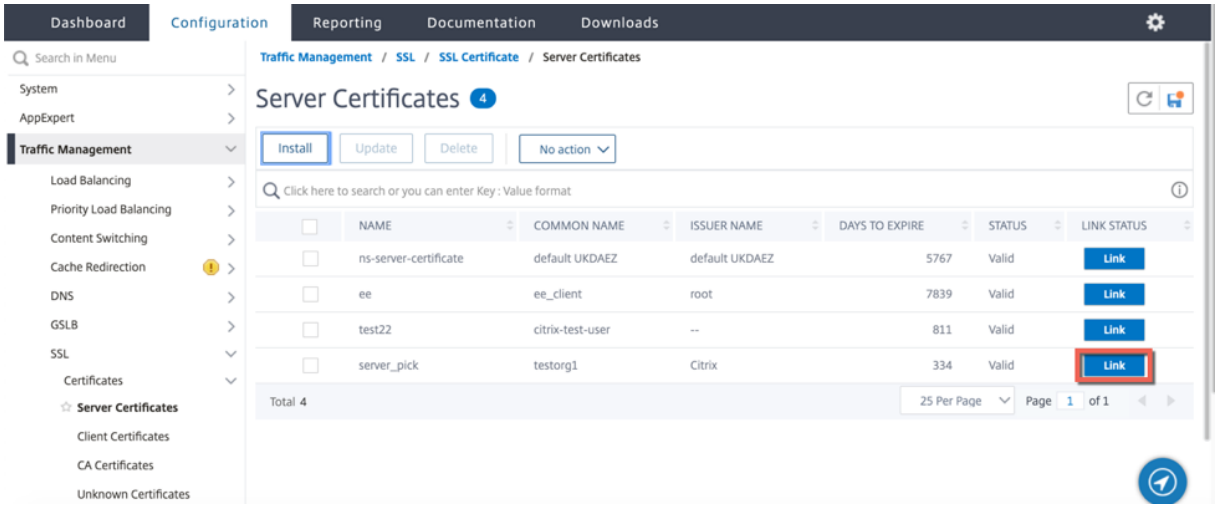

Hinzufügen eines Zertifikatssatzes über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate** > **CA-Zertifikate**.
2. Klicken Sie im Detailbereich auf **Installieren**.
3. Geben **Sie im Dialogfeld Zertifikat installieren** die Details wie das Zertifikat und den Schlüsseldateinamen ein, und wählen Sie dann **Zertifikatpaket**aus.
4. Klicken **Sie auf Installieren**und dann auf **Schließen**.

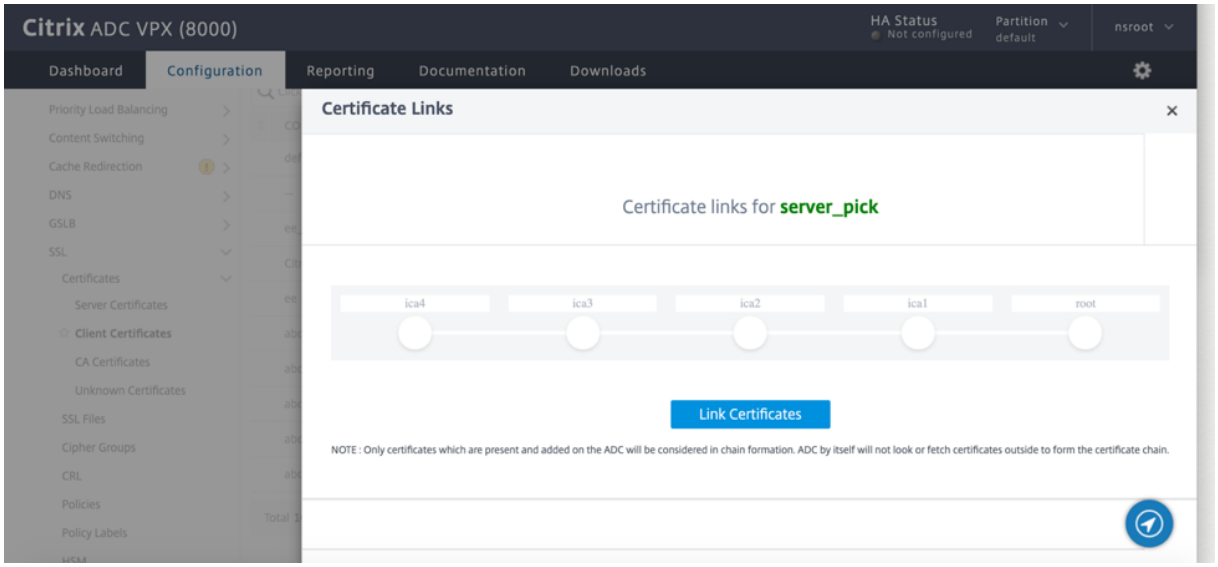
Automatisiertes Verknüpfen von

Hinweis: Diese Funktion ist ab Version 13.0 Build 47.x verfügbar.

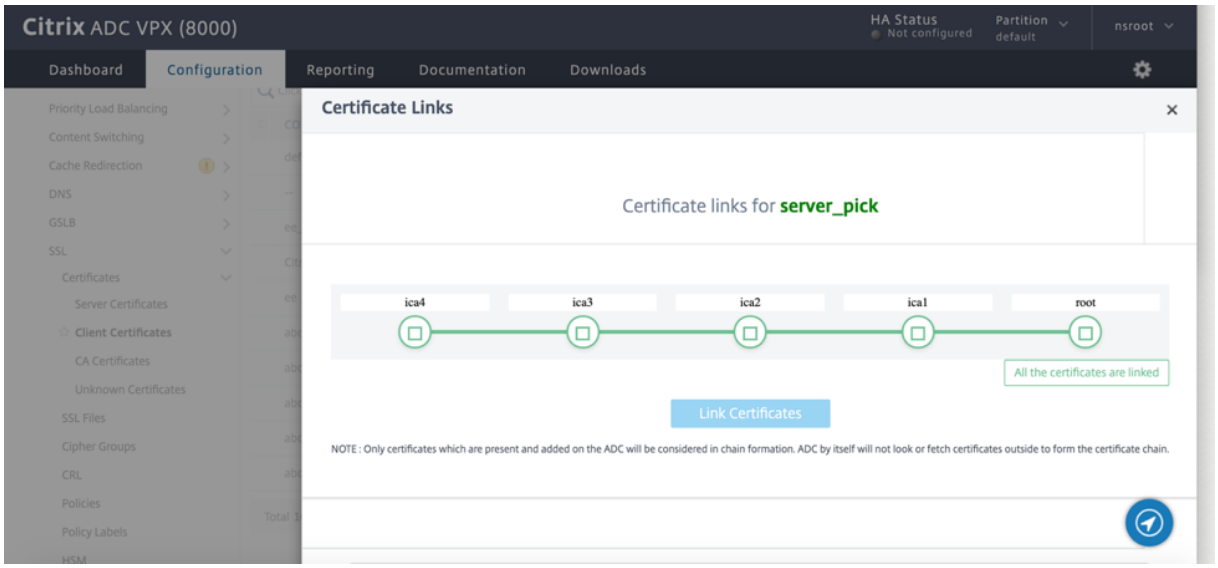
Sie müssen ein Zertifikat nicht mehr manuell mit seinem Aussteller bis zum Stammzertifikat verknüpfen. Wenn die Zwischenzertifikate der Zertifizierungsstelle und das Stammzertifikat auf der Appliance vorhanden sind, können Sie im Endbenutzerzertifikat auf die Schaltfläche **Verknüpfen** klicken.



Die potenzielle Kette erscheint.



Klicken Sie auf **Zertifikat verknüpfen**, um alle Zertifikate zu verknüpfen.



Erstellen Sie eine Kette von Zertifikaten

Anstatt eine Reihe von Zertifikaten (eine einzelne Datei) zu verwenden, können Sie eine Kette von Zertifikaten erstellen. Die Kette verknüpft das Serverzertifikat mit seinem Aussteller (der Zwischenzertifizierungsstelle). Dieser Ansatz erfordert, dass die Zwischenzertifikatsdatei der Zertifizierungsstelle auf der ADC-Appliance installiert ist und die Clientanwendung einem der Zertifikate in der Kette vertrauen muss. Verknüpfen Sie beispielsweise Cert-Intermediate-A mit Cert-Intermediate-B, wobei Cert-Intermediate-B mit Cert-Intermediate-C verknüpft ist, einem Zertifikat, dem die Clientanwendung vertraut.

Hinweis: Die Appliance unterstützt das Senden von maximal 10 Zertifikaten in der Kette der an den

Client gesendeten Zertifikate (ein Serverzertifikat und neun CA-Zertifikate).

Erstellen einer Zertifikatkette mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Zertifikatkette zu erstellen und die Konfiguration zu überprüfen. (Wiederholen Sie den ersten Befehl für jedes neue Glied in der Kette.)

```
link ssl certkey <certKeyName> <linkCertKeyName>
show ssl certlink
<!--NeedCopy-->
```

Beispiel:

```
link ssl certkey siteAcertkey CAcertkey
Done

show ssl certlink

linked certificate:
       1) Cert Name: siteAcertkey CA Cert Name: CAcertkey
Done
<!--NeedCopy-->
```

Erstellen einer Zertifikatkette mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate**.
2. Wählen Sie ein Serverzertifikat aus, und wählen Sie in der Liste **Aktion** die Option **Verknüpfen**aus, und geben Sie einen CA-Zertifikatsnamen an.

Unterstützung für SSL-Zertifikat-Paket

Das aktuelle Design für ein Zertifikatspaket weist folgende Nachteile auf:

- Durch das Hinzufügen eines Zertifikatpakets werden der Konfiguration mehrere Befehle hinzugefügt. Daher können Sie kein weiteres Zertifikatspaket hinzufügen, wenn die beiden Bundles ein gemeinsames Zwischenzertifikat gemeinsam nutzen.
- Das Entfernen eines Zertifikatsbündels ist ein manueller Vorgang. Sie müssen die Dateien in einer bestimmten Reihenfolge manuell entfernen.
- Das Aktualisieren eines Zertifikatpakets wird nicht unterstützt.
- Cluster wird nicht unterstützt.

Das neue Design für ein Zertifikatspaket behebt all diese Probleme. Die neue Entität arbeitet mit einer Zertifikat-Bundle-Datei. Daher müssen nicht für jedes Zwischenzertifikat Dateien erstellt werden. Das Entfernen ist mit dieser neuen Entität ebenfalls einfach.

Zwei Zertifikatspakete können einen Teil der Zwischenzertifikatkette gemeinsam nutzen. Sie können auch ein Zertifikatsschlüsselpaar mit demselben Serverzertifikat und demselben Schlüssel hinzufügen, die auch Teil eines Zertifikatpakets sind.

Im folgenden Beispiel:

1. Das Zertifikatspaket bundle1.pem enthält Serverzertifikat (S1) und Zwischenzertifikate (IC1 und IC2).
2. Das Serverzertifikat ist server_cert.pem (S1).
3. Zwischenzertifikate sind ic1.pem (IC1) und ic2.pem (IC2).

Sie können ein Zertifikatspaket hinzufügen, das S1, IC1 und IC2 enthält.

```
add ssl certkeybundle b1 -bundlefile bundle1.pem
```

Sie können auch ein Zertifikat-Schlüsselpaar mit S1 und IC1 hinzufügen.

```
add ssl certkey server-cert -cert server_cert.pem
```

```
add ssl certkey ic1 -cert ic1.pem
```

Wichtig!

- Die Bundle-Erstellung schlägt fehl, wenn die folgende Reihenfolge nicht erfüllt ist:
  - Serverzertifikat (SC) muss oben in der Bundle-Datei platziert werden.
  - `IC[1-9]` sind Zwischenzertifikate. `IC[i]` wird ausgestellt von `IC[i+1]`. Die Zertifikate müssen in einer Reihenfolge platziert werden, und alle Zwischenzertifikate müssen im Bundle vorhanden sein.
- Zertifikate dürfen nur im PEM-Format vorliegen.
- Der Serverzertifikatschlüssel (SCK) kann an einer beliebigen Stelle im Bundle platziert werden.
- Es werden maximal 9 Zwischenzertifikate unterstützt.

So fügen Sie ein Zertifikatpaket hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl certKeyBundle <bundle_name> -bundlefile <bundle_file_name> -passplain
 <>
```

Beispiel:

```
add ssl certkeyBundle cert_bundle -bundlefile bundle_4096.pem
```


So entfernen Sie ein Zertifikatpaket

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm ssl certKeyBundle <bundle_name>
```

Beispiel:

```
rm ssl certkeybundle cert_bundle
```

So binden Sie ein Zertifikatpaket an einen virtuellen SSL-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vip-name> -certkeybundleName <certkeybundle_name> [ -SNICertkeybundle]
```

Beispiel:

```
bind ssl vserver v_server -certkeyBundleName cert_bundle

show ssl certkeyBundle cert_bundle

1) Name: cert_bundle
        Bundle path: bundle_4096.pem
        Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 83
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=4096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:17:57 2021 GMT
                        Not After : Jul 13 10:17:57 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None


        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 82
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:15:37 2021 GMT
```



```
                        Not After : Jul 13 10:15:37 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 81
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:13:20 2021 GMT
                        Not After : Jul 13 10:13:20 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 00
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:10:23 2021 GMT
                        Not After : Jul 13 10:10:23 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 2048
                SAN ENTRIES: None

1)      Vserver Name: v_server
<!--NeedCopy-->
```

So binden Sie ein Zertifikatpaket als SNI-Zertifikatspaket an einen virtuellen SSL-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vip-name> -certkeybundleName b2 -SNICertkeybundle
```

Beispiel:

```
bind ssl vserver v_server -certkeyBundleName cert_bundle -
    sniCertkeybundle

```



```
sh ssl certkeybundle cert_bundle

1) Name: cert_bundle
        Bundle path: bundle_4096.pem
        Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 83
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=4096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:17:57 2021 GMT
                        Not After : Jul 13 10:17:57 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None


        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 82
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia24096.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:15:37 2021 GMT
                        Not After : Jul 13 10:15:37 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
                Status: Valid,   Days to expiration:278
                Serial Number: 81
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=ia14098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:13:20 2021 GMT
                        Not After : Jul 13 10:13:20 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 4096
                SAN ENTRIES: None

        CA Certificate:
```



```
                Status: Valid,   Days to expiration:278
                Serial Number: 00
                Subject:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Issuer:  C=IN,ST=KAR,O=CITRIX,CN=root4098.com
                Signature Algorithm: sha256WithRSAEncryption
                Validity
                        Not Before: Jul 13 10:10:23 2021 GMT
                        Not After : Jul 13 10:10:23 2022 GMT
                Public Key Algorithm: rsaEncryption
                Public Key size: 2048
                SAN ENTRIES: None

1)    Vserver Name: v_server
2)    Vserver Name: v_server
<!--NeedCopy-->
```

So lösen Sie ein Zertifikatpaket von einem virtuellen SSL-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind ssl vserver <vip-name> -certkeybundleName <certkeybundle_name> [ -SNICertkeybundle]
```

Beispiel:

```
unbind ssl vserver v_server -certkeybundleName cert_bundle
```

Benutzerszenarien für die Bindung von Zertifikatpaketen

In den folgenden Szenarien wird erläutert, wie die ADC-Appliance eine Anforderung in Bezug auf Zertifikatspakete verarbeitet.

Szenario 1: Ein Zertifikat-Schlüsselpaar und ein Zertifikatpaket, das dasselbe Serverzertifikat enthält, sind an denselben virtuellen SSL-Server gebunden

Beim Binden eines Zertifikatsschlüsselpaars und eines Zertifikatpakets, das dasselbe Serverzertifikat enthält, an denselben virtuellen SSL-Server bestimmt die Reihenfolge der Befehle die endgültige Bindung.

Beispiel:

- Das Zertifikatbündel bundle1.pem enthält das Serverzertifikat S1 und die Zwischenzertifikate IC1 und IC2.
- Die Zertifikatsdatei server_cert.pem enthält S1.

Sowohl bundle1.pem als auch server_cert.pem haben dasselbe Serverzertifikat S1.

Wenn die folgenden Befehle in der angegebenen Reihenfolge ausgeführt werden, ersetzt das Serverzertifikat, das an den virtuellen SSL-Server gebunden ist, die Zertifikatspaketbindung an diesen virtuellen Server.

1. `add ssl certkeybundle b1 -bundlefile bundle1.pem`
2. `add ssl certkey server_cert -cert server_cert.pem`
3. `bind ssl vserver v1 -certkeybundle b1`
4. `bind ssl vserver v1 -cert server_cert`

Szenario 2: Zwei Zertifikatspakete enthalten dieselbe Zwischenzertifikatkette

Sie können zwei Zertifikatspakete mit derselben Zwischenzertifikatkette hinzufügen. Die beiden Bündel fungieren als unabhängige Einheiten.

Im folgenden Beispiel enthält das Zertifikatbündel-1 das Serverzertifikat S1 und die Zwischenzertifikate IC1 und IC2 in dieser Reihenfolge. Das Zertifikatbündel-2 enthält das Serverzertifikat S2 und die Zwischenzertifikate IC1 und IC2 in dieser Reihenfolge.

- Zertifikatpaket bundle1.pem (S1, IC1, IC2)
- Zertifikatpaket bundle2.pem (S2, IC1, IC2)

Wenn S1 in Bundle-1 im SSL-Handshake-Prozess ausgewählt wird, wird die Zwischenzertifikatkette von Bundle-1 an den Client gesendet.

```
add ssl certkeybundle bundle-1 -bundlefile bundle1.pem
add ssl certkeybundle bundle-2 -bundlefile bundle2.pem
```

Szenario 2: Zwei Zertifikatspakete enthalten einige gängige Zwischenzertifikate in der Kette

Sie können zwei Zertifikatspakete mit einigen gängigen Zwischenzertifikaten in der Kette hinzufügen.

Im folgenden Beispiel enthält Bundle-1 das Serverzertifikat S1 und die Zwischenzertifikate IC1 und IC2. Das Zertifikatbündel-2 enthält das Serverzertifikat S2 und die Zwischenzertifikate IC1, IC2 und IC3.

Zertifikat-Bundle1.pem (S1, IC1, IC2)
Zertifikat-Bundle2.pem (S2, IC1, IC2, IC3)

```
add ssl certkeybundle bundle-1 -bundlefile bundle1.pem
add ssl certkeybundle bundle-2 -bundlefile bundle2.pem
```

Wenn S1 in Bundle-1 im SSL-Handshake-Prozess ausgewählt wird, wird die Zwischenzertifikatkette von Bundle-1 an den Client gesendet. Das heißt, `(S1→IC1→IC2)` wird an den Kunden gesendet. IC3 wird nicht hinzugefügt.

Wenn S2 in Bundle-2 im SSL-Handshake-Prozess ausgewählt wird, wird die Zwischenzertifikatkette von Bundle-2 nur an den Client gesendet. Das heißt, (S1→IC1→IC2→IC3) wird an den Kunden gesendet.

Einschränkungen des Zertifikatsbündels

- Die Überwachung des Status eines Zertifikats im Zertifikatspaket wird nicht unterstützt.
- Das Aktualisieren eines Zertifikatpakets wird nicht unterstützt.
- Zertifikatpakete können nur an virtuelle SSL-Server gebunden werden.
- Das OCSP-Heften wird nicht unterstützt.

Aktualisieren eines vorhandenen Serverzertifikats

Um ein vorhandenes Serverzertifikat manuell zu ändern, müssen Sie die folgenden Schritte ausführen:

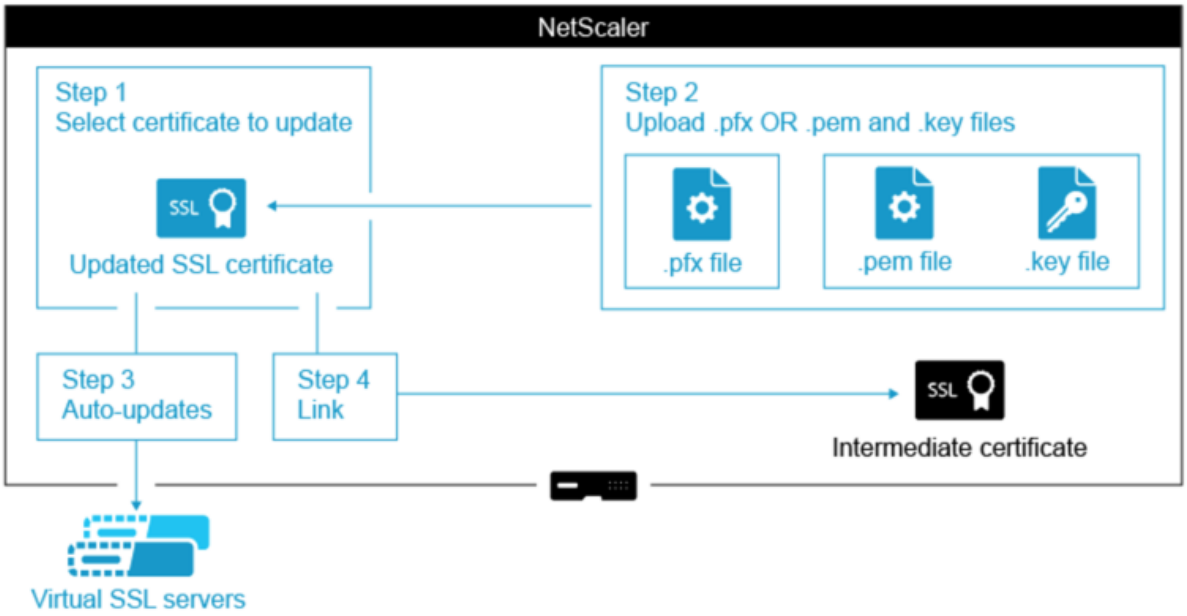
1. Trennen Sie das alte Zertifikat vom virtuellen Server.
2. Entfernen Sie das Zertifikat aus der Appliance.
3. Fügen Sie das neue Zertifikat der Appliance hinzu.
4. Binden Sie das neue Zertifikat an den virtuellen Server.

Um Ausfallzeiten beim Ersetzen eines Zertifikatsschlüsselpaars zu reduzieren, können Sie ein vorhandenes Zertifikat aktualisieren. Wenn Sie ein Zertifikat durch ein Zertifikat ersetzen möchten, das für eine andere Domäne ausgestellt wurde, müssen Sie Domänenprüfungen vor dem Aktualisieren des Zertifikats deaktivieren.

Um Benachrichtigungen über ablaufende Zertifikate zu erhalten, können Sie die Ablaufüberwachung aktivieren.

Wenn Sie ein Zertifikat von einem konfigurierten virtuellen SSL-Server oder -Dienst entfernen oder die Bindung aufheben, wird der virtuelle Server oder Dienst inaktiv. Sie sind aktiv, nachdem ein neues gültiges Zertifikat an sie gebunden wurde. Um Ausfallzeiten zu reduzieren, können Sie die Aktualisierungsfunktion verwenden, um ein Zertifikatsschlüsselpaar zu ersetzen, das an einen virtuellen SSL-Server oder einen SSL-Dienst gebunden ist.

Übersichtsdiagramm zum Aktualisieren eines SSL-Zertifikats auf der NetScaler-Appliance.



So aktualisieren Sie ein vorhandenes Zertifikat

Dies ist ein eingebettetes Video. Klicken Sie auf den Link, um das Video anzusehen

Aktualisieren eines vorhandenen Zertifikatschlüsselpaars mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein vorhandenes Zertifikatsschlüsselpaar zu aktualisieren und die Konfiguration zu überprüfen:

```
update ssl certkey <certkeyName> -cert <string> -key <string>

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Beispiel:

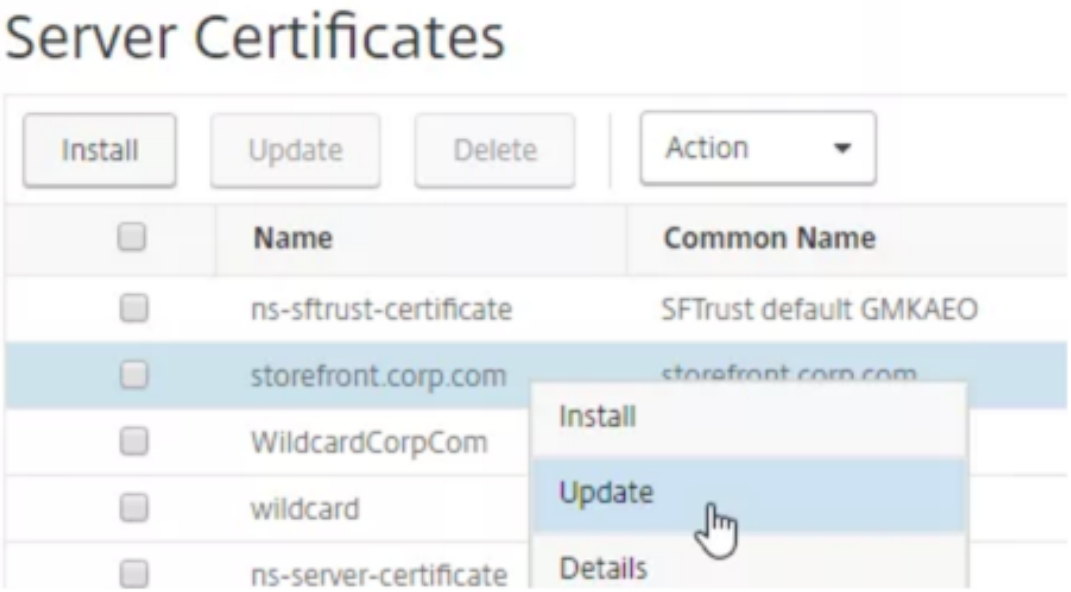
```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem

Done

show ssl certkey siteAcertkey

Name: siteAcertkey       Status: Valid
          Version: 3
          Serial Number: 02
          Signature Algorithm: md5WithRSAEncryption
```



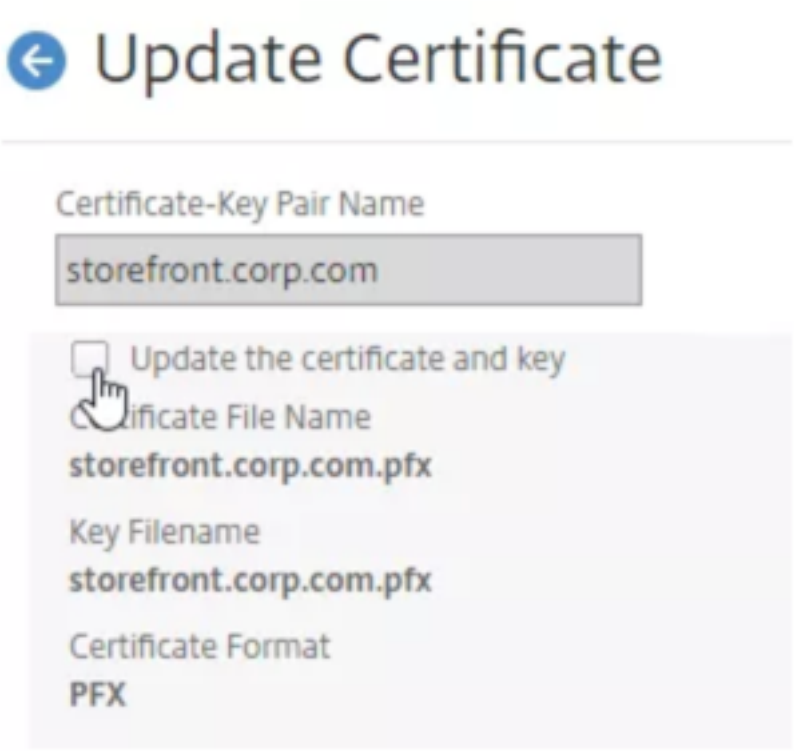
```
            Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech
            Validity
                 Not Before: Nov 11 14:58:18 2001 GMT
                 Not After: Aug 7 14:58:18 2004 GMT
            Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security
            Public Key Algorithm: rsaEncryption
            Public Key size: 2048
Done
<!--NeedCopy-->
```

Aktualisieren eines vorhandenen Zertifikat-Schlüssel-Paars über die grafische Benutzeroberfläche

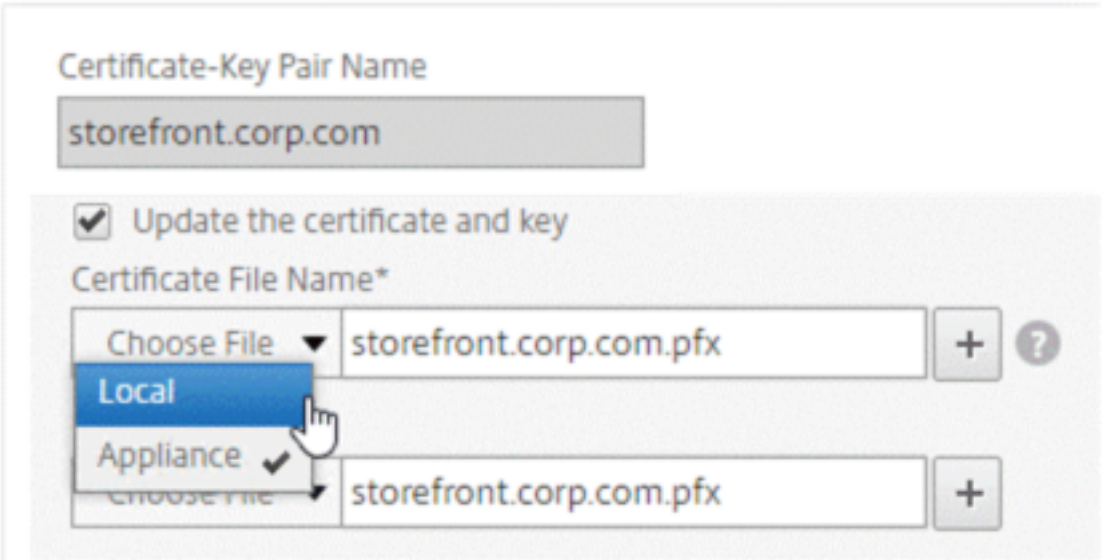
1. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate** > **Serverzertifikate**.
2. Wählen Sie das Zertifikat aus, das Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.



3. Wählen Sie **Zertifikat und Schlüssel aktualisieren**aus.



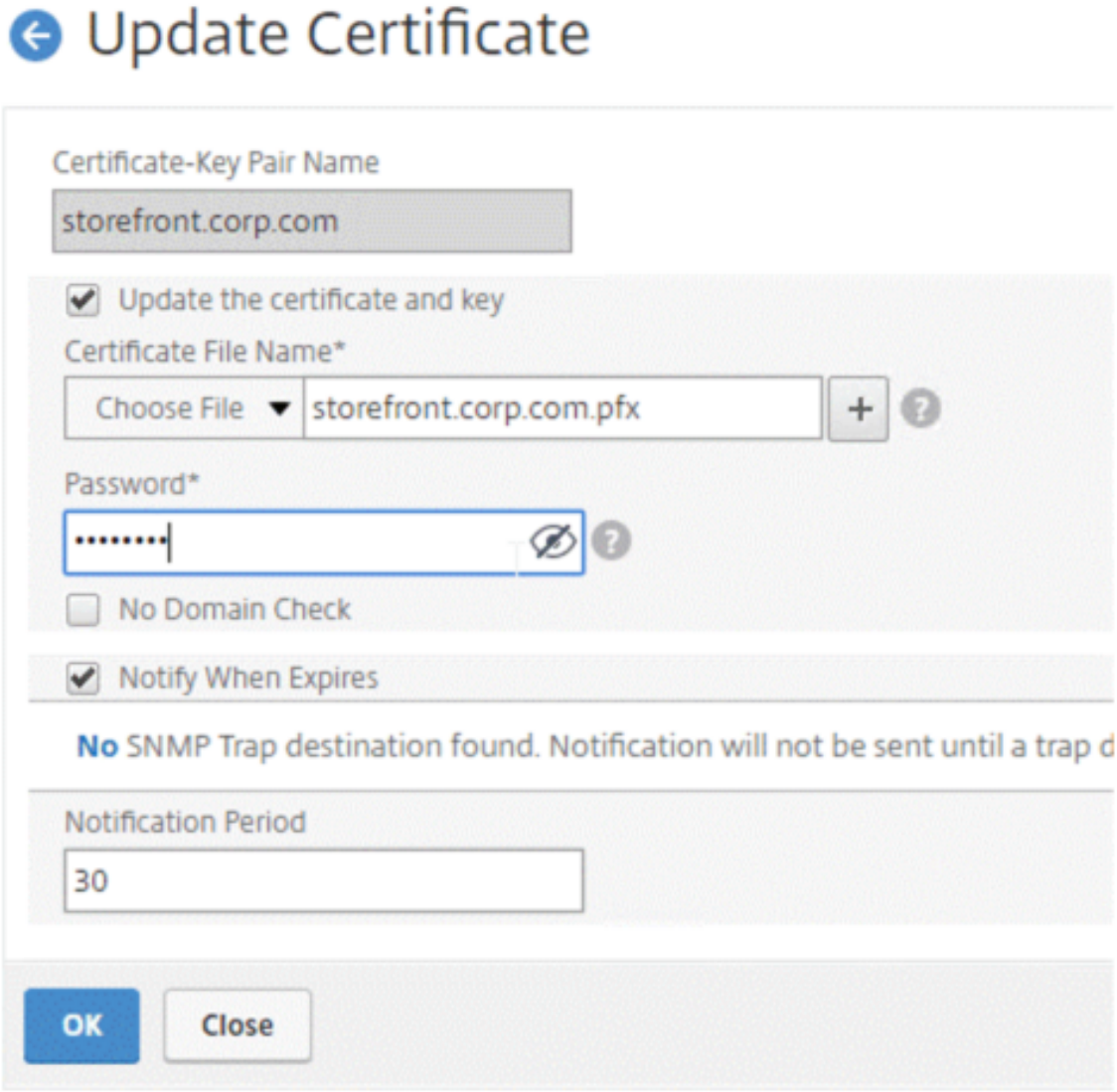
4. Klicken Sie **unter Zertifikatsdateiname**auf **Datei auswählen** > **Lokal**, und navigieren Sie zur aktualisierten PFX-Datei oder Zertifikats-PEM-Datei.



- Wenn Sie eine.pfx-Datei hochladen, werden Sie aufgefordert, das PFX-Dateikennwort anzugeben.
- Wenn Sie eine PEM-Datei für ein Zertifikat hochladen, müssen Sie auch eine Zertifikatsschlüsseldatei hochladen. Wenn der Schlüssel verschlüsselt ist, müssen Sie das Verschlüs-

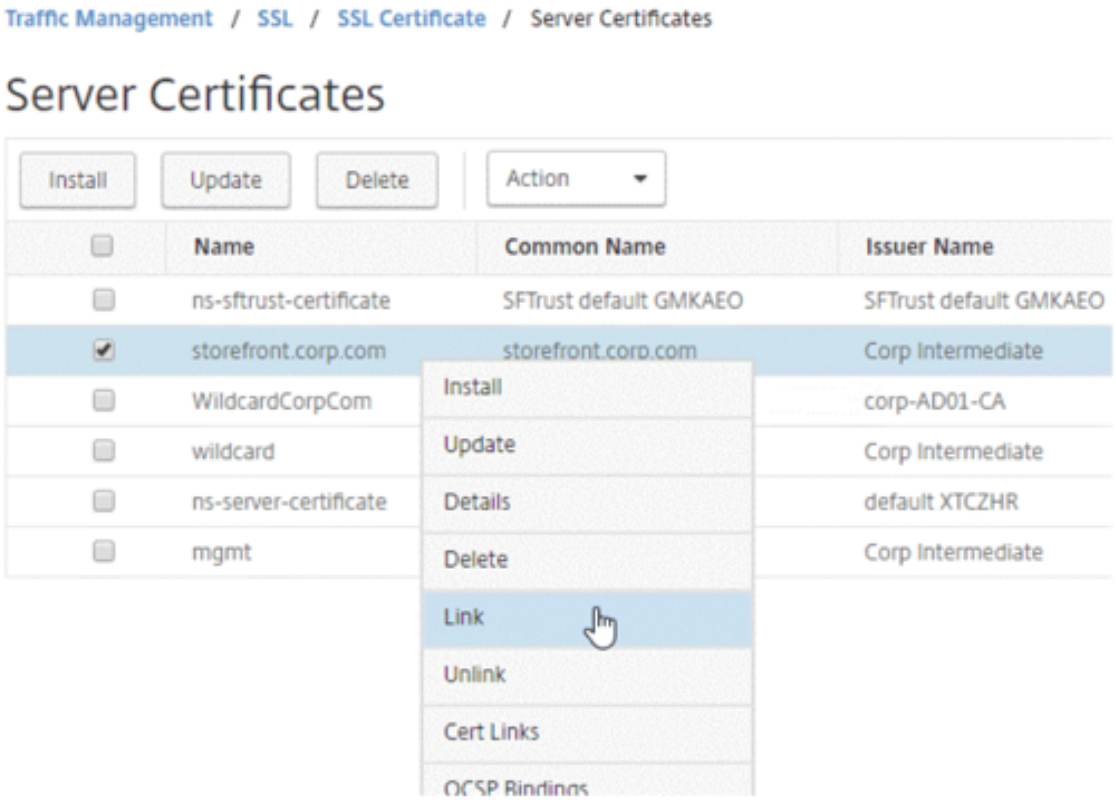
selungskennwort angeben.

5. Wenn der allgemeine Name des neuen Zertifikats nicht mit dem alten Zertifikat übereinstimmt, wählen Sie **Keine Domänenprüfung**aus.
6. Klicken Sie auf **OK**. Alle virtuellen SSL-Server, an die dieses Zertifikat gebunden ist, werden automatisch aktualisiert.



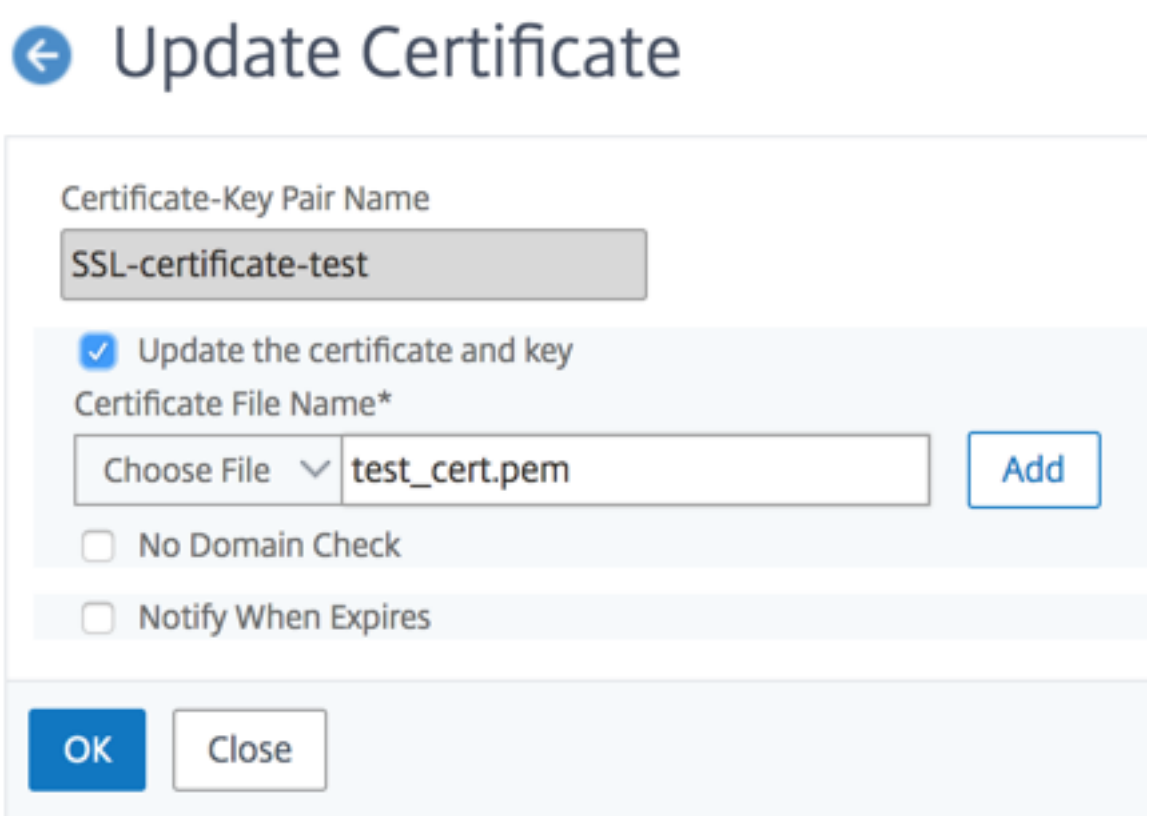
7. Nach dem Ersetzen des Zertifikats müssen Sie möglicherweise die Zertifikatverknüpfung auf ein neues Zwischenzertifikat aktualisieren. Weitere Informationen zum Aktualisieren eines Zwischenzertifikats ohne Unterbrechung der Links finden Sie unter Aktualisieren eines Zwischenzertifikats, ohne die Links zu unterbrechen.
   - Klicken Sie mit der rechten Maustaste auf das aktualisierte Zertifikat, und klicken Sie auf **Zertifikatverknüpfungen**, um festzustellen, ob es mit einem Zwischenzertifikat verknüpft ist.

- Wenn das Zertifikat nicht verknüpft ist, klicken Sie mit der rechten Maustaste auf das aktualisierte Zertifikat, und klicken Sie auf **Link**, um es mit einem Zwischenzertifikat zu verknüpfen. Wenn Sie keine Option zum Verknüpfen sehen, müssen Sie zuerst ein neues Zwischenzertifikat auf der Appliance unter dem Knoten **CA Certificates** installieren.



Aktualisieren eines vorhandenen CA-Zertifikats

Die Schritte zum Aktualisieren eines vorhandenen CA-Zertifikats entsprechen dem Aktualisieren eines vorhandenen Serverzertifikats. Der einzige Unterschied besteht darin, dass Sie bei CA-Zertifikaten keinen Schlüssel benötigen.



Deaktivieren Sie Domainprüfungen

Wenn ein SSL-Zertifikat auf der Appliance ersetzt wird, muss der auf dem neuen Zertifikat angegebene Domänenname mit dem Domänennamen des zu ersetzenden Zertifikats übereinstimmen. Wenn Sie beispielsweise ein Zertifikat für abc.com ausgestellt haben und es mit einem auf def.com ausgestellten Zertifikat aktualisieren, schlägt die Zertifikatsaktualisierung fehl.

Wenn Sie jedoch möchten, dass der Server, der eine bestimmte Domäne gehostet hat, eine neue Domäne hosten soll, deaktivieren Sie die Domänenprüfung, bevor Sie das Zertifikat aktualisieren.

Deaktivieren Sie die Domänenprüfung für ein Zertifikat mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Domänenüberprüfung zu deaktivieren und die Konfiguration zu überprüfen:

```
update ssl certKey <certkeyName> -noDomainCheck

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Beispiel:


```
update ssl certKey sv -noDomainCheck

Done

show ssl certkey sv

Name: sv
Cert Path: /nsconfig/ssl/complete/server/server_rsa_512.pem
Key Path: /nsconfig/ssl/complete/server/server_rsa_512.ky
Format: PEM
Status: Valid,   Days to expiration:9349
Certificate Expiry Monitor: DISABLED
Done
<!--NeedCopy-->
```

Deaktivieren Sie die Domänenprüfung für ein Zertifikat über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**, wählen Sie ein Zertifikat aus und klicken Sie auf **Aktualisieren**.
2. Wählen Sie **Keine Domainprüfung**aus.

Ersetzen Sie das Standardzertifikat einer ADC-Appliance durch ein vertrauenswürdiges CA-Zertifikat, das dem Hostnamen der Appliance entspricht

Das folgende Verfahren setzt voraus, dass das Standardzertifikat (`ns-server-certificate`) an die internen Dienste gebunden ist.

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Zertifikate > Zertifikatsanforderung erstellen**.
2. Geben Sie im allgemeinen Namen ein `test.citrixadc.com`.
3. Reichen Sie die CSR an eine vertrauenswürdige Zertifizierungsstelle ein.
4. Nachdem Sie das Zertifikat von der vertrauenswürdigen Zertifizierungsstelle erhalten haben, kopieren Sie die Datei in das Verzeichnis `/nsconfig/ssl`.
5. Navigieren Sie zu **Traffic Management > SSL > Zertifikate > Serverzertifikate**.
6. Wählen Sie das Standard-Serverzertifikat (`ns-server-certificate`) aus und klicken Sie auf **Aktualisieren**.
7. Navigieren **Sie im Dialogfeld Zertifikat aktualisieren** unter **Certificate File Name zu dem Zertifikat**, das Sie nach dem Signieren von der Zertifizierungsstelle erhalten haben.
8. Geben Sie im Feld **Schlüsseldateiname** den standardmäßigen privaten Schlüsseldateinamen (`ns-server.key`) an.
9. Wählen Sie **Keine Domainprüfung**aus.

10. Klicken Sie auf **OK**.

Ablaufüberwachung aktivieren

Ein SSL-Zertifikat ist für einen bestimmten Zeitraum gültig. Eine typische Bereitstellung umfasst mehrere virtuelle Server, die SSL-Transaktionen verarbeiten, und die an sie gebundenen Zertifikate können zu unterschiedlichen Zeiten ablaufen. Ein auf der Appliance konfigurierter Ablaufmonitor erstellt Einträge in den Syslog- und NS-Überwachungsprotokollen der Appliance, wenn ein konfiguriertes Zertifikat abläuft.

Wenn Sie SNMP-Warnungen für den Ablauf des Zertifikats erstellen möchten, müssen Sie diese separat konfigurieren.

Aktivieren einer Ablaufüberwachung für ein Zertifikat mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Ablaufüberwachung für ein Zertifikat zu aktivieren und die Konfiguration zu überprüfen:

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED ) [-
    notificationPeriod <positive_integer>]]

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl certKey sv -expiryMonitor ENABLED  - notificationPeriod 60
Done
<!--NeedCopy-->
```

Aktivieren einer Ablaufüberwachung für ein Zertifikat über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**, wählen Sie ein Zertifikat aus und klicken Sie auf **Aktualisieren**.
2. Wählen Sie **Bei Ablauf benachrichtigen**aus, und geben Sie optional einen Benachrichtigungszeitraum an.

Aktualisieren Sie ein Zwischenzertifikat, ohne die Links zu unterbrechen

Sie können jetzt ein Zwischenzertifikat aktualisieren, ohne vorhandene Links zu trennen. Die Erweiterung “AuthorityKeyIdentifier” in dem verknüpften Zertifikat, das von dem zu ersetzenden Zertifikat ausgestellt wurde, darf kein Feld mit der Seriennummer des Autoritätszertifikats

(“AuthorityCertSerialNumber”) enthalten. Wenn die Erweiterung ‘AuthorityKeyIdentifier’ ein Seriennummernfeld enthält, müssen die Seriennummern des alten und des neuen Zertifikats identisch sein. Sie können eine beliebige Anzahl von Zertifikaten im Link nacheinander aktualisieren, wenn die vorherige Bedingung erfüllt ist. Zuvor wurden die Links unterbrochen, wenn ein Zwischenzertifikat aktualisiert wurde.

Zum Beispiel gibt es vier Zertifikate: `CertACertB`, `CertC`, und `CertD`. Das Zertifikat `CertA` ist der Aussteller für `CertB`, `CertB` ist der Aussteller für `CertC`und so weiter. Wenn Sie ein Zwischenzertifikat `CertB` durch `CertB_new` ersetzen möchten, ohne die Verbindung zu unterbrechen, muss die folgende Bedingung erfüllt sein:

Die Seriennummer des Zertifikats von `CertB` muss mit der Seriennummer des Zertifikats von `CertB_new` übereinstimmen, wenn beide der folgenden Bedingungen erfüllt sind:

- Die Erweiterung `AuthorityKeyIdentifier` ist in `CertC` vorhanden.
- Diese Erweiterung enthält ein Seriennummernfeld.

Wenn sich der allgemeine Name in einem Zertifikat ändert, geben Sie beim Aktualisieren des Zertifikats an `nodomaincheck`.

Um im vorherigen Beispiel “www.example.com” in `CertD` zu “*.example.com” zu ändern, wählen Sie den Parameter “No Domain Check” aus.

Aktualisieren Sie das Zertifikat mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
update ssl certKey <certkeyName> -cert <string> [-password] -key <
   string>  [-noDomainCheck]
<!--NeedCopy-->
```

Beispiel:

```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem -noDomainCheck
<!--NeedCopy-->
```

Eine Zertifikatkette anzeigen

Ein Zertifikat enthält den Namen der ausstellenden Behörde und den Antragsteller, für den das Zertifikat ausgestellt wurde. Um ein Zertifikat zu validieren, müssen Sie sich den Aussteller dieses Zertifikats ansehen und bestätigen, ob Sie dem Aussteller vertrauen. Wenn Sie dem Aussteller nicht vertrauen, müssen Sie sehen, wer das Ausstellerzertifikat ausgestellt hat. Gehen Sie die Kette hoch, bis Sie das Stammzertifizierungsstellenzertifikat oder einen Aussteller erreichen, dem Sie vertrauen.

Wenn ein Client im Rahmen des SSL-Handshakes ein Zertifikat anfordert, präsentiert die Appliance ein Zertifikat und die Kette der Ausstellerzertifikate, die auf der Appliance vorhanden sind. Ein Administrator kann die Zertifikatkette für die auf der Appliance vorhandenen Zertifikate anzeigen und fehlende Zertifikate installieren.

Zeigen Sie die Zertifikatkette für die auf der Appliance vorhandenen Zertifikate mithilfe der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ssl certchain <cert_name>
<!--NeedCopy-->
```

Beispiele

Es gibt 3 Zertifikate: c1, c2 und c3. Zertifikat c3 ist das Stammzertifikat der Zertifizierungsstelle und signiert c2 und c2-Zeichen c1. Die folgenden Beispiele veranschaulichen die Ausgabe des `show ssl certchain c1` Befehls in verschiedenen Szenarien.

Szenario 1:

Das Zertifikat c2 ist mit c1 verknüpft, und c3 ist mit c2 verknüpft.

Das Zertifikat c3 ist ein Stammzertifikat der Zertifizierungsstelle.

Wenn Sie den folgenden Befehl ausführen, werden die Zertifikatsverknüpfungen zum Stammzertifikat der Zertifizierungsstelle angezeigt.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate name: c2               linked; not a root
       certificate
    2) Certificate name: c3               linked; root certificate
Done
<!--NeedCopy-->
```

Szenario 2:

Das Zertifikat c2 ist mit c1 verknüpft.

Das Zertifikat c2 ist kein Stammzertifikat der Zertifizierungsstelle.

Wenn Sie den folgenden Befehl ausführen, werden die Informationen angezeigt, dass das Zertifikat c3 ein Stammzertifikat der Zertifizierungsstelle ist, aber nicht mit c2 verknüpft ist.


```
show ssl certchain c1

Certificate chain  details of certificate name c1 are:
    1) Certificate Name: c2              linked; not a root
       certificate
    2) Certificate Name: c3              not linked; root certificate
    Done
<!--NeedCopy-->
```

Szenario 3:

Zertifikat c1, c2 und c3 sind nicht verknüpft, aber auf der Appliance vorhanden.

Wenn Sie den folgenden Befehl ausführen, werden Informationen zu allen Zertifikaten angezeigt, die mit dem Aussteller des Zertifikats c1 beginnen. Es wird auch angegeben, dass die Zertifikate nicht verknüpft sind.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: c2              not linked; not a root
       certificate
    2) Certificate Name: c3              not linked; root certificate
    Done
<!--NeedCopy-->
```

Szenario 4:

Das Zertifikat c2 ist mit c1 verknüpft.

Das Zertifikat c3 ist auf der Appliance nicht vorhanden.

Wenn Sie den folgenden Befehl ausführen, werden Informationen über das mit c1 verknüpfte Zertifikat angezeigt. Sie werden aufgefordert, ein Zertifikat mit dem in c2 angegebenen Antragstellernamen hinzuzufügen. In diesem Fall wird der Benutzer aufgefordert, das Stammzertifizierungsstellenzertifikat c3 hinzuzufügen.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: c2              linked; not a root
       certificate
    2) Certificate Name: /C=IN/ST=ka/O=netscaler/CN=test
       Action: Add a certificate with this subject name.
Done
<!--NeedCopy-->
```


Szenario 5:

Ein Zertifikat ist nicht mit dem Zertifikat c1 verknüpft, und das Ausstellerzertifikat von c1 ist auf der Appliance nicht vorhanden.

Wenn Sie den folgenden Befehl ausführen, werden Sie aufgefordert, ein Zertifikat mit dem Antragstellernamen in Zertifikat c1 hinzuzufügen.

```
sh ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: /ST=KA/C=IN
       Action: Add a certificate with this subject name.
<!--NeedCopy-->
```

Servertestzertifikat generieren

May 11, 2023

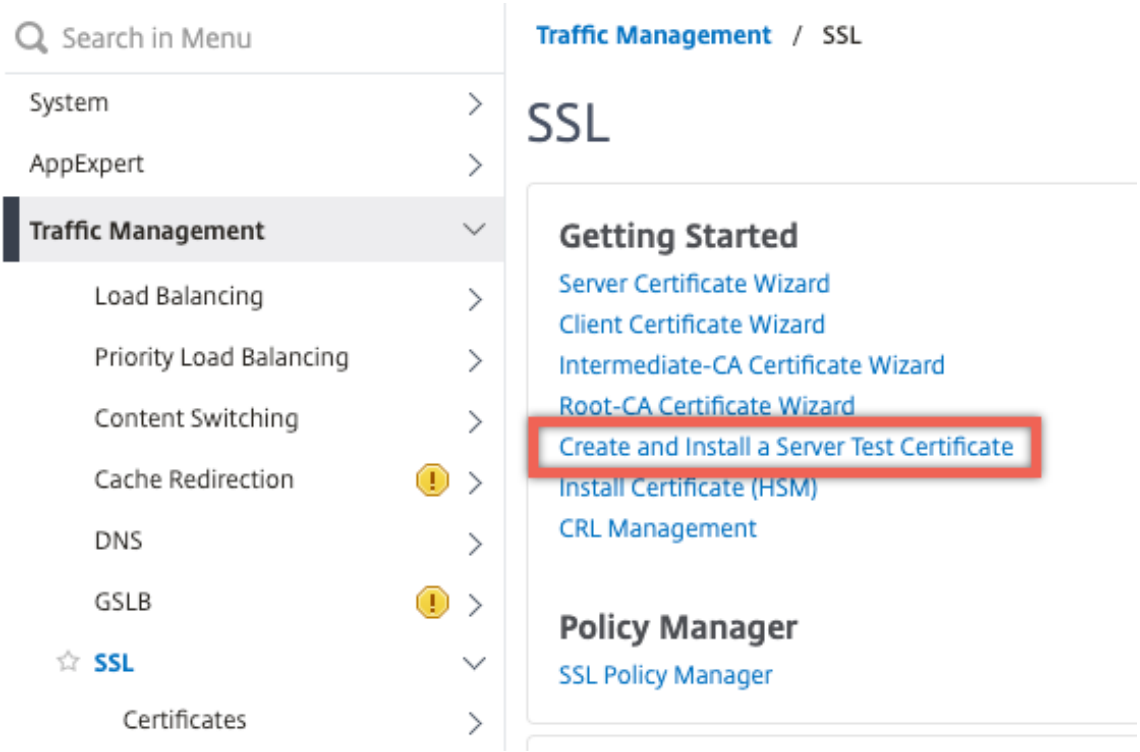
Mit der NetScaler-Appliance können Sie mithilfe eines GUI-Assistenten im Konfigurationsprogramm ein Testzertifikat für die Serverauthentifizierung erstellen. Ein Serverzertifikat wird verwendet, um einen Server in einem SSL-Handshake zu authentifizieren und zu identifizieren. In der Regel stellt eine vertrauenswürdige Zertifizierungsstelle ein Serverzertifikat aus. Der Server sendet das Zertifikat an einen Client, der es zur Authentifizierung des Servers verwendet.

Für die Ausstellung eines Servertestzertifikats fungiert die Appliance als Zertifizierungsstelle. Dieses Zertifikat kann zur Authentifizierung in einem SSL-Handshake mit einem Client an einen virtuellen SSL-Server gebunden werden. Dieses Zertifikat dient nur zu Testzwecken. Nicht in einer Produktionsumgebung verwenden.

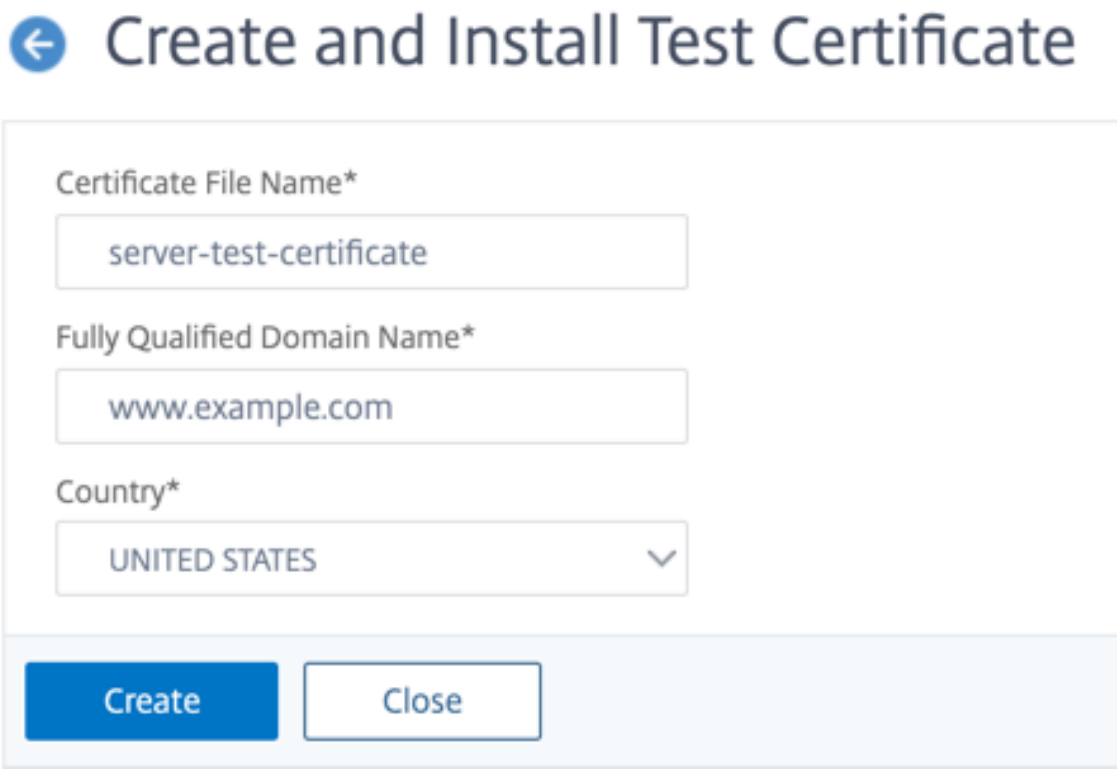
Sie können das Servertestzertifikat auf jedem virtuellen Server installieren, der das SSL- oder das SSL_TCP-Protokoll verwendet.

Generieren Sie ein Servertestzertifikat mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der **Gruppe SSL-Zertifikate**die Option **Servertestzertifikat erstellen und installieren**aus.



2. Geben Sie Details für die Parameter ein und klicken Sie auf **Erstellen**.



SSL-Dateien importieren und konvertieren

May 11, 2023

Sie können jetzt SSL-Ressourcen wie Zertifikate, private Schlüssel, CRLs und DH-Schlüssel von Remote-Hosts importieren, auch wenn kein FTP-Zugriff auf diese Hosts verfügbar ist. Diese Funktion ist besonders in Umgebungen hilfreich, in denen der Shell-Zugriff auf den Remote-Host eingeschränkt ist. Standardordner werden in /nsconfig/ssl wie folgt erstellt:

- Für Zertifikatsdateien: /nsconfig/ssl/certfile
- Für private Schlüssel: die /nsconfig/ssl/keyfile
- Für CRLs: /var/netscaler/ssl/crlfile
- Für DH-Schlüssel: /nsconfig/ssl/dhfile

Importe von HTTP- und HTTPS-Servern werden unterstützt. Der Import schlägt jedoch fehl, wenn sich die Datei auf einem HTTPS-Server befindet, für den Zugriff eine Client-Zertifikatsauthentifizierung erforderlich ist.

> **Hinweis:**
>
> Der Importbefehl ist nicht in der Konfigurationsdatei (ns.conf) gespeichert, da ein erneutes Importieren der Datei nach einem Neustart zu einem Fehler führen kann.

Eine Zertifikatsdatei importieren

Sie können die CLI und die GUI verwenden, um eine Datei (Ressource) von einem Remote-Host zu importieren.

Importieren Sie eine Zertifikatsdatei von einem Remote-Host mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
import ssl certFile [<name>] [<src>]
<!--NeedCopy-->
```

Beispiel:

```
import ssl certfile my-certfile http://www.example.com/file_1
<!--NeedCopy-->
```

```
show ssl certfile
     Name : my-certfile
     URL : http://www.example.com/file_1
<!--NeedCopy-->
```


Um eine Zertifikatsdatei zu entfernen, verwenden Sie den `rm ssl certFile` Befehl, der nur das Argument 'name' akzeptiert.

Importieren Sie eine Schlüsseldatei von einem Remote-Host mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
import ssl keyFile [<name>] [<src>]
<!--NeedCopy-->
```

Beispiel:

```
import ssl keyfile my-keyfile http://www.example.com/key_file
<!--NeedCopy-->
```

```
show ssl keyfile
     Name : my-keyfile
     URL : http://www.example.com/key_file
<!--NeedCopy-->
```

Um eine Schlüsseldatei zu entfernen, verwenden Sie den `rm ssl keyFile` Befehl, der nur das Argument 'name' akzeptiert.

Importieren Sie eine CRL-Datei von einem Remote-Host mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
import ssl crlFile [<name>] [<src>]
<!--NeedCopy-->
```

Um eine CRL-Datei zu entfernen, verwenden Sie den Befehl `rm ssl crlFile`, der nur das Argument <name> akzeptiert.

Beispiel:

```
import ssl crlfile my-crlfile http://www.example.com/crl_file

show ssl crlfile

    Name : my-crlfile
    URL : http://www.example.com/crl_file
<!--NeedCopy-->
```


Importieren Sie eine DH-Datei von einem Remote-Host mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
import ssl dhFile [<name>] [<src>]
<!--NeedCopy-->
```

Beispiel:

```
import ssl dhfile my-dhfile http://www.example.com/dh_file
show ssl dhfile
     Name : my-dhfile
     URL : http://www.example.com/dh_file
<!--NeedCopy-->
```

Um eine DH-Datei zu entfernen, verwenden Sie den Befehl `rm ssl dhFile`, der nur das Argument <name> akzeptiert.

Importieren Sie eine SSL-Ressource mithilfe der GUI

Navigieren Sie zu **Traffic Management > SSL > Importe**und wählen Sie dann die entsprechende Registerkarte aus.

PKCS #8 - und PKCS #12 -Zertifikate importieren

Wenn Sie Zertifikate und Schlüssel verwenden möchten, die Sie bereits auf anderen sicheren Servern oder Anwendungen in Ihrem Netzwerk haben, können Sie sie exportieren und dann in die NetScaler-Appliance importieren. Möglicherweise müssen Sie exportierte Zertifikate und Schlüssel konvertieren, bevor Sie sie in die NetScaler-Appliance importieren können.

Einzelheiten zum Exportieren von Zertifikaten von sicheren Servern oder Anwendungen in Ihrem Netzwerk finden Sie in der Dokumentation des Servers oder der Anwendung, von dem Sie exportieren möchten.

> **Hinweis:**
>
> Bei der Installation auf der NetScaler-Appliance dürfen Schlüssel- und Zertifikatsnamen keine anderen Leerzeichen oder Sonderzeichen als die vom UNIX-Dateisystem unterstützten Zeichen enthalten. Halten Sie sich beim Speichern des exportierten Schlüssels und Zertifikats an die entsprechende Namenskonvention.

Ein Zertifikat und ein privates Schlüsselpaar werden üblicherweise im PKCS #12 -Format gesendet. Die Appliance unterstützt die Formate PEM und DER für Zertifikate und Schlüssel. Informationen zur Konvertierung von PKCS #12 in PEM oder DER oder von PEM oder DER in PKCS #12 finden Sie im Abschnitt „SSL-Zertifikate für den Import oder Export konvertieren“ weiter unten auf dieser Seite.

Die NetScaler-Appliance unterstützt keine PEM-Schlüssel im PKCS #8 -Format. Sie können diese Schlüssel jedoch mithilfe der OpenSSL-Schnittstelle in ein unterstütztes Format konvertieren, auf die Sie über die CLI oder das Konfigurationsprogramm zugreifen können. Bevor Sie den Schlüssel konvertieren, müssen Sie überprüfen, ob der private Schlüssel im PKCS #8 -Format vorliegt. Schlüssel im PKCS #8 -Format beginnen normalerweise mit dem folgenden Text:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----


leuSSZQZKgrgUQ==


-----END ENCRYPTED PRIVATE KEY-----
<!--NeedCopy-->
```

Öffnen Sie die OpenSSL-Schnittstelle über die CLI

1. Öffnen Sie mithilfe eines SSH-Clients wie PuTTY eine SSH-Verbindung zur Appliance.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
3. Geben Sie an der Eingabeaufforderung shell ein.
4. Geben Sie an der Shell-Eingabeaufforderung ein `openssl`.

Öffnen Sie die OpenSSL-Schnittstelle über die GUI

Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe Tools die **OpenSSL-Schnittstelle**aus.

Konvertieren Sie ein nicht unterstütztes PKCS #8 Schlüsselformat mithilfe der OpenSSL-Schnittstelle in ein verschlüsseltes unterstütztes Schlüsselformat

Geben Sie an der OpenSSL-Eingabeaufforderung einen der folgenden Befehle ein, je nachdem, ob das nicht unterstützte Tastenformat vom Typ RSA oder ECDSA ist:

```
OpenSSL>rsa- in <PKCS#8 Key Filename> -des3 -out <encrypted Key
    Filename>

OpenSSL>ec -in <PKCS#8 Key Filename> -des3 -out <encrypted Key Filename
    >
<!--NeedCopy-->
```


Parameter zum Konvertieren eines nicht unterstützten Schlüsselformats in ein unterstütztes Schlüsselformat

- **PKCS #8 -Schlüsseldateiname:** Der Name der Eingabedatei des inkompatiblen privaten PKCS #8 -Schlüssels.
- **verschlüsselter Schlüsseldateiname:** Der Name der Ausgabedatei des kompatiblen verschlüsselten privaten Schlüssels im PEM-Format.
- **unverschlüsselter Schlüsseldateiname:** Der Name der Ausgabedatei des kompatiblen unverschlüsselten privaten Schlüssels im PEM-Format.

SSL-Zertifikate für Import oder Export konvertieren

Eine NetScaler-Appliance unterstützt die Formate PEM und DER für SSL-Zertifikate. Andere Anwendungen, wie Client-Browser und einige externe sichere Server, erfordern verschiedene PKCS-Formate (Public Key Cryptography Standard). Die Appliance kann das PKCS #12 -Format in das PEM- oder DER-Format konvertieren, um ein Zertifikat in die Appliance zu importieren, und kann PEM oder DER in PKCS #12 konvertieren, um ein Zertifikat zu exportieren. Für mehr Sicherheit kann die Konvertierung einer zu importierenden Datei die Verschlüsselung des privaten Schlüssels mit dem DES- oder DES3-Algorithmus beinhalten.

> **Hinweis:**
>
> Wenn Sie die GUI verwenden, um ein PKCS #12 -Zertifikat zu importieren und das Passwort ein Dollarzeichen ($), ein Anführungszeichen (‘) oder ein Escape-Zeichen () enthält, schlägt der Import möglicherweise fehl. Wenn dies der Fall ist, wird die Meldung FEHLER: Ungültiges Passwort angezeigt. Wenn Sie im Passwort ein Sonderzeichen verwenden müssen, stellen Sie sicher, dass Sie diesem ein Escape-Zeichen () voranstellen, sofern nicht alle Importe mit der CLI durchgeführt werden.

Konvertieren Sie das Format eines Zertifikats mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
convert ssl pkcs12 <outfile> [-import [-pkcs12File <inputFilename>] [-
    des | -des3] [-export [-certFile <inputFilename>] [-keyFile <
    inputFilename>]]
<!--NeedCopy-->
```

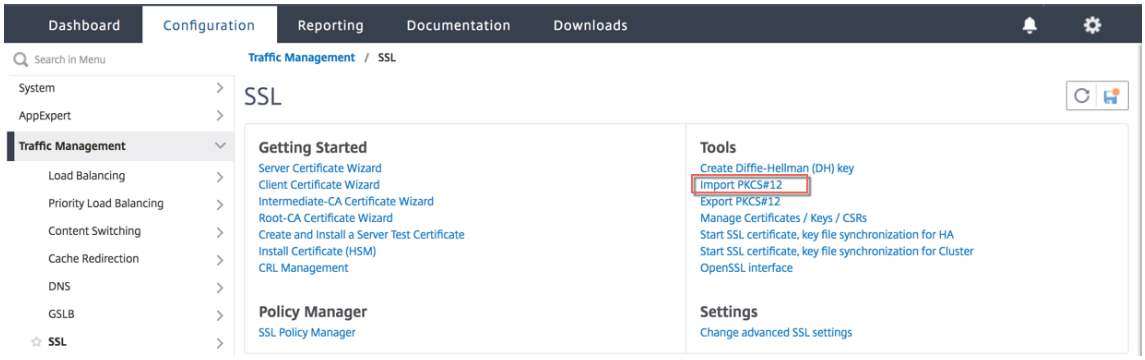
Während des Vorgangs werden Sie aufgefordert, ein Import- oder Exportkennwort einzugeben. Bei einer verschlüsselten Datei werden Sie außerdem aufgefordert, eine Passphrase einzugeben.

Beispiel:

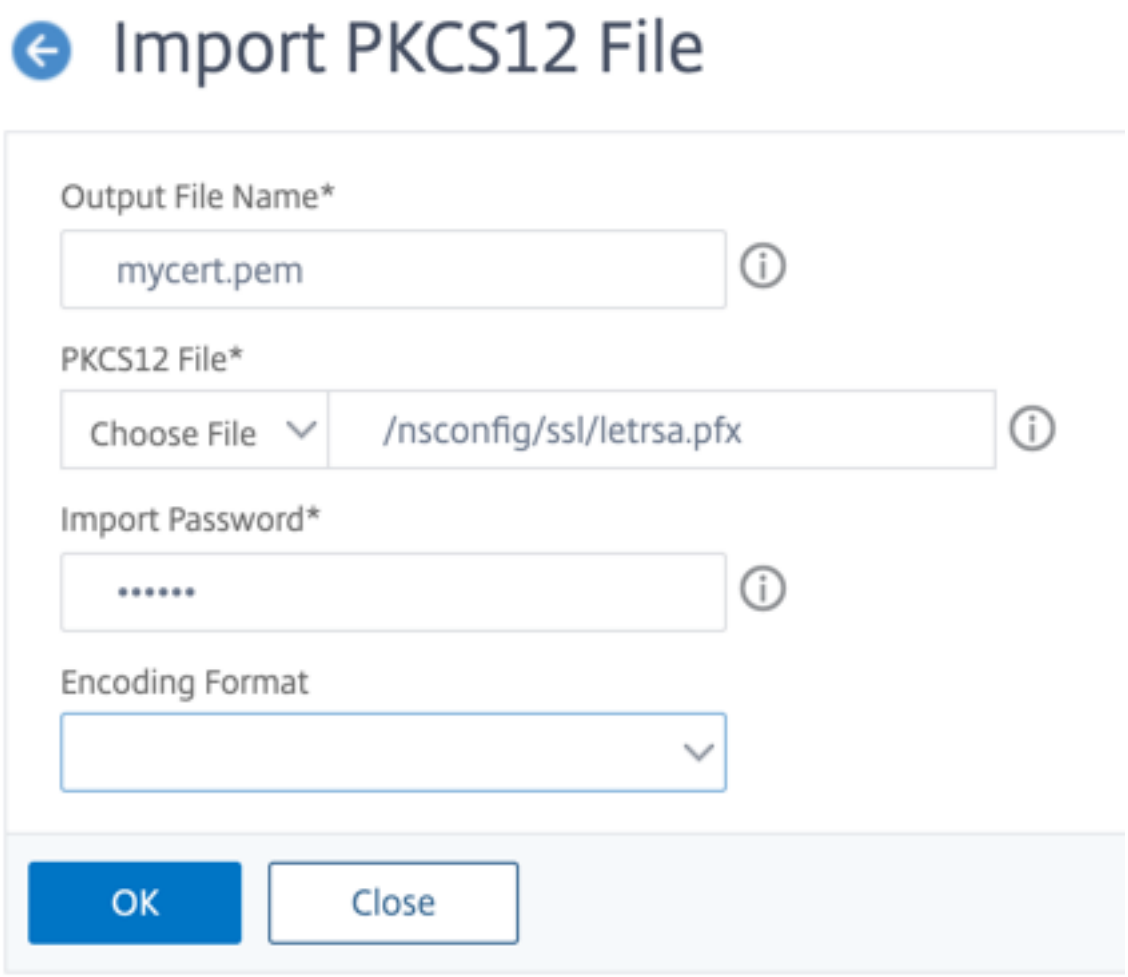

```
convert ssl pkcs12 Cert-Import-1.pem -import -pkcs12File Cert-Import-1.
    pfx -des

convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -
    keyFile Key-Client-1
<!--NeedCopy-->
```

Konvertieren Sie das Format eines Zertifikats mithilfe der GUI

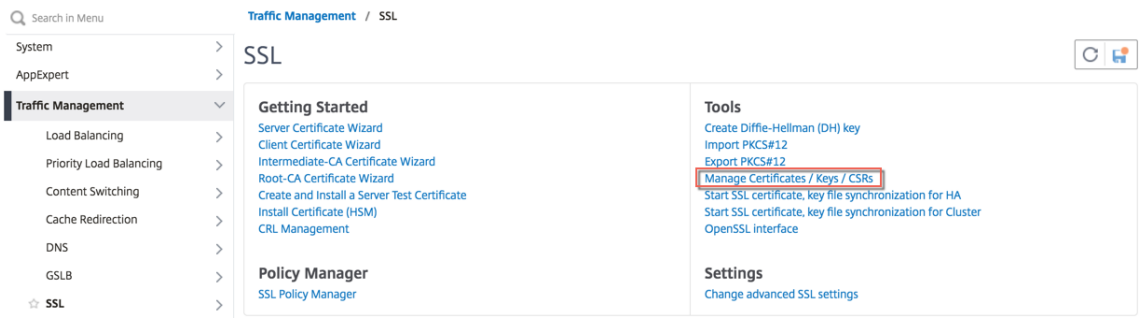
1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe **Tools** die Option **PKCS #12 importieren**aus.



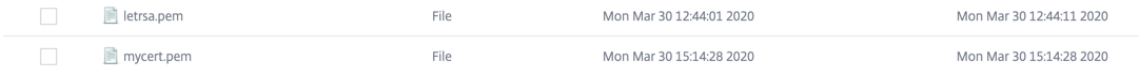
2. Geben Sie den Namen des PEM-Zertifikats im Feld **Name der Ausgabedatei** an.
3. Navigieren Sie auf Ihrem lokalen Computer oder der Appliance zum Speicherort des PFX-Zertifikats.



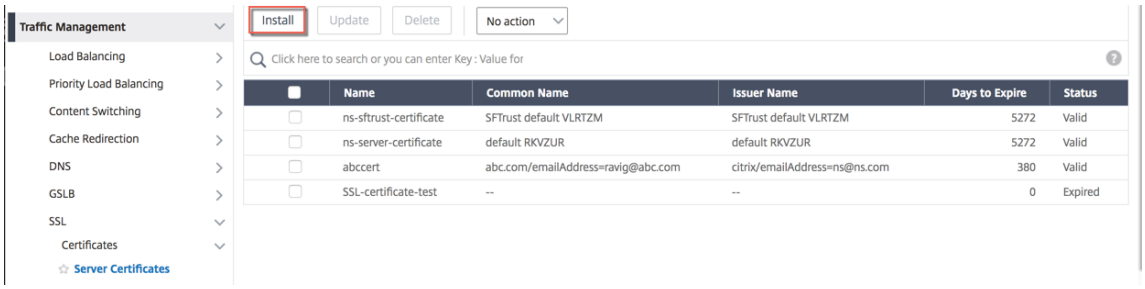
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Zertifikate verwalten /Schlüssel/CSRs**, um die konvertierte PEM-Datei anzuzeigen.



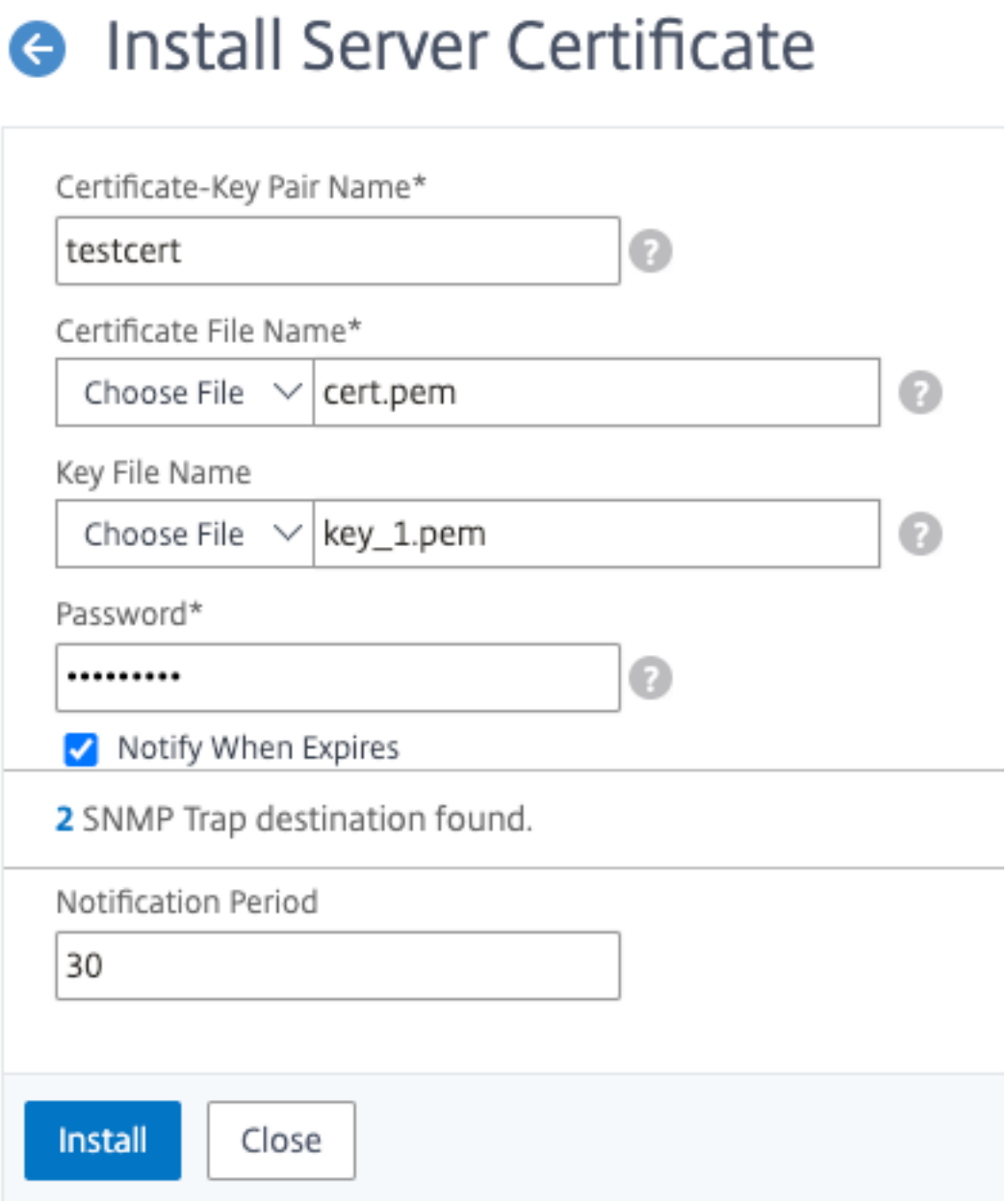
6. Sie können die hochgeladene PFX-Datei und die konvertierte PEM-Datei ansehen.



7. Navigieren Sie zu **SSL** > **Zertifikate** > **Serverzertifikate** und klicken Sie auf **Installieren**.



8. Geben Sie einen Namen für das **Zertifikatsschlüsselpaar**an.
9. Navigieren Sie zum Speicherort der PEM-Datei.
10. Geben Sie das Passwort an, wenn Sie dazu aufgefordert werden.
11. Klicken Sie auf **Installieren**.



12. Binden Sie das Zertifikatschlüsselpaar an einen virtuellen SSL-Server.

SSL-Zertifikat an einen virtuellen Server auf der NetScaler-Appliance binden

June 2, 2023

Ein SSL-Zertifikat ist ein wesentlicher Bestandteil von SSL-Verschlüsselungs- und Entschlüs-

selungsprozessen. Das Zertifikat wird während eines SSL-Handshakes verwendet, um die Identität des SSL-Servers festzustellen, bei dem es sich um die NetScaler-Appliance handelt, da sie als SSL-Terminierungspunkt für die Clients fungiert.

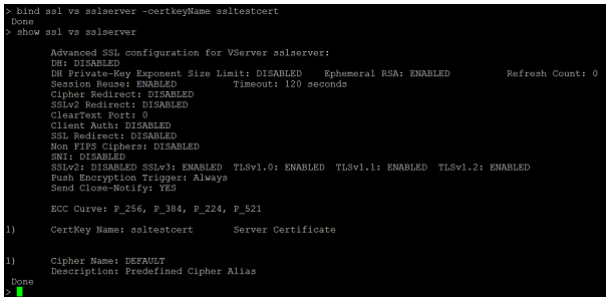
Das zur Verarbeitung der SSL-Transaktionen verwendete Zertifikat muss an den virtuellen Server (SSL) gebunden sein, der die SSL-Daten empfängt.

So binden Sie ein SSL-Zertifikat über die Befehlszeile an einen virtuellen SSL-Server

Geben Sie in der Befehlszeile Folgendes ein:

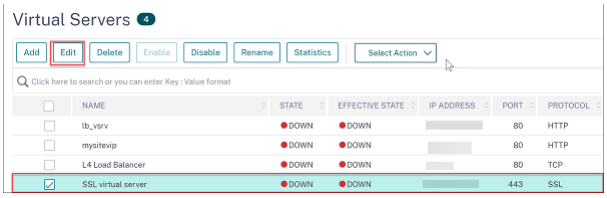
```
bind ssl vs <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vs <vServerName>
<!--NeedCopy-->
```

Beispiel:



So binden Sie ein SSL-Zertifikat über die GUI an einen virtuellen SSL-Server

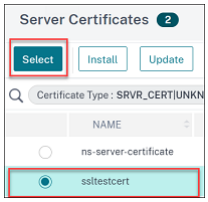
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server vom Typ SSL aus und klicken Sie auf **Bearbeiten**.



3. Klicken Sie auf der Seite **Load Balancing Virtual Server** unter dem Abschnitt **Zertifikate** auf **Kein Serverzertifikat**.

4. Klicken Sie auf der Seite **Serverzertifikat-Bindung** auf **Klicken, um sie auszuwählen**.

5. Wählen Sie das SSL-Zertifikat aus und klicken Sie auf **Auswählen**.



6. Klicken Sie auf **Bind**, um das SSL-Zertifikat an den virtuellen Server zu binden.
7. Klicken Sie auf **Fertig**.

   Sie haben das Binden des SSL-Zertifikats an den virtuellen Server abgeschlossen.

> **Hinweis:**
>
> Wenn Sie versuchen, ein Zertifikatsschlüsselpaar an einen virtuellen Server zu binden, an den bereits ein Zertifikatsschlüsselpaar gebunden ist, entbindet NetScaler den alten Certkey und bindet den neuen. Die folgende Meldung wird angezeigt:
>
> `Warning: Current certificate replaces the previous binding`
>
> Bestehende Verbindungen, bei denen der Handshake abgeschlossen ist, sind nicht betroffen. Die anderen Verbindungen sind beendet.

SSL-Profile

May 11, 2023

Sie können ein SSL-Profil verwenden, um anzugeben, wie eine NetScaler-Appliance SSL-Verkehr verarbeitet. Ein Profil ist eine Sammlung von SSL-Parametereinstellungen für SSL-Entitäten, wie virtuelle Server, Dienste und Dienstgruppen, und bietet einfache Konfiguration und Flexibilität. Sie sind nicht darauf beschränkt, nur einen Satz globaler Parameter zu konfigurieren.

Sie können mehrere Sätze (Profile) globaler Parameter erstellen und verschiedenen SSL-Entitäten unterschiedliche Sätze zuweisen. SSL-Profile werden in zwei Kategorien eingeteilt:

- **Frontend-Profile**: Enthalten Parameter, die für die Frontend-Entität gelten (Entität, die Anfragen von einem Client empfängt).
- **Back-End-Profile**: Enthalten Parameter, die für die Back-End-Entität gelten (Entität, die Client-Anforderungen an einen Server sendet).

Im Gegensatz zu einem TCP- oder HTTP-Profil ist ein SSL-Profil optional. Sobald SSL-Profile aktiviert sind, erben alle SSL-Endpunkte die Standardprofile. Das gleiche Profil kann für mehrere Entitäten wiederverwendet werden. Wenn einer Entität kein Profil zugeordnet ist, gelten die auf globaler Ebene festgelegten Werte. Für dynamisch erlernte Dienste gelten die aktuellen globalen Werte.

Im Vergleich zu der alternativen Methode, bei der SSL-Parameter, Chiffren und ECC-Kurven auf einzelnen SSL-Endpunkten konfiguriert werden müssen, vereinfachen SSL-Profile auf der NetScaler-Appliance das Konfigurationsmanagement, indem sie als zentraler SSL-Konfigurationspunkt für alle zugehörigen Endpunkte fungieren. Mithilfe von SSL-Profilen können Sie Konfigurationsprobleme im Zusammenhang mit der Neuordnung von Verschlüsselungen und Ausfallzeiten bei der Neuordnung von Verschlüsselungen lösen.

SSL-Profile helfen bei der Einstellung der erforderlichen SSL-Parameter und Verschlüsselungsbindungen auf den SSL-Endpunkten, auf denen diese Parameter und Bindungen traditionell nicht festgelegt werden können. SSL-Profile können auch auf sicheren Monitoren eingerichtet werden.

Die SSL-Profilinfrastruktur wurde verbessert, um die neuesten Chiffren und Protokolle zu verwenden. Unterschiede zwischen dem Legacy-Profil (altes Profil) und dem erweiterten SSL-Profil (neues Profil) werden hervorgehoben.

Unterschiede zwischen der alten und der neuen SSL-Profilinfrastruktur

Unterschiede	Altes Profil	Neues Profil
Im Profil enthaltene Chiffren und ECC-Kurven	Nein	Ja
Einfügen einer Chiffre oder einer Verschlüsselungsgruppe in die Mitte einer vorhandenen Liste	Entbinde alle Chiffren und binde erneut in der Reihenfolge der erforderlichen Priorität.	Fügen Sie eine Chiffre hinzu und weisen Sie ihr eine Priorität zu. Wenn keine Priorität angegeben ist, wird der Chiffre die niedrigste Priorität in der Liste zugewiesen.
Alle Chiffren entbinden	`unbind ssl vserver <name> ciphername -ALL`	`unbind ssl profile -cipherName FlushAllCiphers` (Version 12.1 und höher enthalten den Parameter FlushAllCiphers, um die Bindung aller Chiffren oder Verschlüsselungsgruppen von einem Profil aufzuheben, da ALL wie eine Verschlüsselungsgruppe behandelt wird.)

Unterschiede	Altes Profil	Neues Profil
Status von SSLv3	–	Deaktiviert im Standard-Frontend-Profil (ns_default_ssl_profile_frontend). Hinweis: Bevor Sie dieses Profil aktivieren, ist SSLv3 global aktiviert. Nachdem Sie das Profil aktiviert haben, ist SSLv3 im Frontend-Standardprofil deaktiviert.

SSL-Profilinfrastruktur

August 15, 2023

Sicherheitslücken in der SSLv3- und RC4-Implementierung haben die Notwendigkeit unterstrichen, die neuesten Verschlüsselungen und Protokolle zu verwenden, um die Sicherheitseinstellungen für eine Netzwerkverbindung auszuhandeln. Das Implementieren von Änderungen an der Konfiguration, z. B. das Deaktivieren von SSLv3 über Tausende von SSL-Endpunkten hinweg, ist ein umständlicher Prozess. Daher wurden Einstellungen, die Teil der Konfiguration der SSL-Endpunkte waren, zusammen mit den Standardverschlüsselungen in die SSL-Profile verschoben. Um Änderungen in der Konfiguration, einschließlich der Verschlüsselungsunterstützung, zu implementieren, müssen Sie nur das Profil ändern, das an die Entitäten gebunden ist.

Die Standard-Front-End- und Standard-Back-End-SSL-Profile enthalten alle Standard-Verschlüsselungen und ECC-Kurven, zusätzlich zu den Einstellungen, die Teil der alten Profile waren. Beispielausgaben für die Standardprofile finden Sie im Anhang. Der Vorgang “Standardprofil aktivieren” bindet das Standard-Front-End-Profil automatisch an alle Front-End-Entitäten und das Standard-Back-End-Profil an alle Back-End-Entitäten. Sie können ein Standardprofil an Ihre Bereitstellung anpassen. Sie können auch benutzerdefinierte Profile erstellen und sie an SSL-Entitäten binden.

Das Frontend-Profil enthält Parameter, die für eine Frontend-Entität gelten (die Entität, die Anfragen von einem Client empfängt). In der Regel handelt es sich bei dieser Entität um einen virtuellen SSL-Server, einen transparenten SSL-Dienst oder interne Dienste auf der NetScaler-Appliance. Das Back-End-Profil enthält Parameter, die für eine Back-End-Entität gelten (Entität auf der ADC-Appliance, die Clientanfragen an einen Back-End-Server sendet). In der Regel ist diese Entität ein SSL-Dienst oder eine Dienstgruppe auf der NetScaler-Appliance. Wenn Sie versuchen, einen nicht unterstützten Parameter zu konfigurieren, wird der Fehler `ERROR: Specified parameters are`

`not applicable for this type of SSL profile` angezeigt. Einige SSL-Parameter, wie CRL-Speichergröße, OCSP-Cachegröße, UnDeFaction Control und UnDeFaction Data, sind nicht Teil eines Profils, da diese Parameter unabhängig von Entitäten sind. Diese Parameter sind unter **Traffic Management > SSL > Erweiterte SSL-Einstellungen**vorhanden. Informationen zu SSL-Parametern, die auf einem sicheren Monitor unterstützt werden, finden Sie unter Festlegen von SSL-Parametern auf einem sicheren Monitor.

Ein SSL-Profil unterstützt die folgenden Vorgänge:

- **Hinzufügen**: Erstellt ein SSL-Profil auf der NetScaler-Appliance. Geben Sie an, ob das Profil ein Frontend oder ein Backend ist. Standard ist Frontend.
- **Set**: — Ändert die Einstellungen eines vorhandenen Profils.
- **Unset**: Setzt die angegebenen Parameter auf ihre Standardwerte zurück. Wenn Sie keine Parameter angeben, wird eine Fehlermeldung angezeigt. Wenn Sie ein Profil für eine Entität aufheben, ist das Profil nicht an die Entität gebunden.
- **Entfernen**: Löscht ein Profil. Ein Profil, das von einer Entität verwendet wird, kann nicht gelöscht werden. Beim Löschen der Konfiguration werden alle Entitäten gelöscht. Infolgedessen werden die Profile auch gelöscht.
- **Binden**: Bindet ein Profil an eine SSL-Entität.
- **Unbind**: Löst die Bindung eines Profils an eine SSL-Entität.
- Anzeigen:**Zeigt**alle Profile an, die auf der NetScaler-Appliance verfügbar sind. Wenn ein Profilname angegeben ist, werden die Details dieses Profils angezeigt. Wenn eine Entität angegeben ist, werden die mit dieser Entität verknüpften Profile angezeigt.

> **Wichtig:**
>
> - Ein SSL-Profil hat Vorrang vor SSL-Parametern. Das heißt, wenn Sie SSL-Parameter mit dem `set ssl parameter` Befehl konfigurieren und später ein Profil an eine SSL-Entität binden, haben die Einstellungen im Profil Vorrang.
> - Wenn Sie nach dem Upgrade die Standardprofile aktivieren, können Sie die Änderungen nicht rückgängig machen. Das heißt, die Profile können nicht deaktiviert werden. Speichern Sie die Konfiguration und erstellen Sie eine Kopie der Konfigurationsdatei (ns.conf), bevor Sie die Profile aktivieren. Wenn Sie jedoch die Features im Standardprofil nicht verwenden möchten, können Sie weiterhin die alten SSL-Profile verwenden. Weitere Informationen zu diesen Profilen finden Sie unter Legacy-SSL-Profil.
> - In der GUI und CLI wird eine Bestätigungsaufforderung hinzugefügt, wenn Sie das Standardprofil aktivieren, um zu verhindern, dass es versehentlich aktiviert wird.

Protokolle unter TLSv1.2 sind in den internen SSL-Diensten deaktiviert. Wenn das (erweiterte) Standardprofil aktiviert ist, ist das Profil `ns_default_ssl_profile_internal_frontend_service` an die internen SSL-Dienste gebunden und die Protokolle SSLv3, TLSv1.0 und TLSv1.1 sind im Profil deaktiviert.

Befehl:

```
set ssl parameter -defaultProfile ENABLED
    Save your configuration before enabling the Default profile. You
       cannot undo the changes. Are you sure you want to enable the
       Default profile? [Y/N]Y
Done
<!--NeedCopy-->
```

Standardmäßig gelten einige SSL-Parameter, *globale Parameter*genannt, für alle SSL-Endpunkte. Wenn ein Profil jedoch an einen SSL-Endpunkt gebunden ist, gelten die globalen Parameter nicht. Stattdessen gelten die im Profil angegebenen Einstellungen.

Wichtige Hinweise

1. Ein Profil kann an mehrere virtuelle Server gebunden sein, aber an einen virtuellen Server kann nur ein Profil gebunden sein.
2. Um ein Profil zu löschen, das an einen virtuellen Server gebunden ist, trennen Sie das Profil zunächst.
3. Eine Chiffre oder Verschlüsselungsgruppe kann mit unterschiedlichen Prioritäten an mehrere Profile gebunden werden.
4. Ein Profil kann mehrere Verschlüsselungen und Verschlüsselungsgruppen haben, die an unterschiedliche Prioritäten gebunden sind.
5. Änderungen an einer Verschlüsselungsgruppe werden sofort in allen Profilen und auf allen virtuellen Servern widergespiegelt, an die eines der Profile gebunden ist.
6. Wenn eine Verschlüsselungssammlung Teil einer Verschlüsselungsgruppe ist, bearbeiten Sie die Verschlüsselungsgruppe, um diese Verschlüsselungssammlung zu entfernen, bevor Sie die Verschlüsselungssammlung aus dem Profil entfernen.
7. Wenn Sie einer Verschlüsselungssammlung oder Verschlüsselungsgruppe, die an ein Profil angehängt ist, keine Priorität zuweisen, wird ihr die niedrigste Priorität innerhalb des Profils zugewiesen.
8. Sie können eine benutzerdefinierte Verschlüsselungsgruppe (auch als benutzerdefinierte Verschlüsselungsgruppe bezeichnet) aus vorhandenen Verschlüsselungsgruppen und Verschlüsselungssammlungen erstellen. Wenn Sie die Verschlüsselungsgruppe A erstellen und die vorhandenen Verschlüsselungsgruppen X und Y hinzufügen, wird Y in dieser Reihenfolge mit einer niedrigeren Priorität als X zugewiesen. Das heißt, die zuerst hinzugefügte Gruppe hat eine höhere Priorität.
9. Wenn eine Verschlüsselungssammlung Teil von zwei Verschlüsselungsgruppen ist, die an dasselbe Profil angehängt sind, wird die Verschlüsselungssammlung nicht als Teil der zweiten Verschlüsselungsgruppe hinzugefügt. Die Verschlüsselungssammlung mit der höheren Priorität ist wirksam, wenn der Datenverkehr verarbeitet wird.

10. Verschlüsselungsgruppen werden im Profil nicht erweitert. Dadurch wird die Anzahl der Zeilen in der Konfigurationsdatei (ns.conf) stark reduziert. Wenn beispielsweise zwei Verschlüsselungsgruppen mit jeweils 15 Verschlüsselungen an tausend virtuelle SSL-Server gebunden sind, fügt die Erweiterung 30* 1000 verschlüsselungsbezogene Einträge in der Konfigurationsdatei hinzu. Mit dem neuen Profil hätte es nur zwei Einträge: einen für jede Verschlüsselungsgruppe, die an ein Profil gebunden ist.
11. Das Erstellen einer benutzerdefinierten Verschlüsselungsgruppe aus vorhandenen Chiffren und Verschlüsselungsgruppen ist ein Kopier-/Einfügevorgang. Änderungen in der ursprünglichen Gruppe werden nicht in der neuen Gruppe widergespiegelt.
12. Eine benutzerdefinierte Verschlüsselungsgruppe listet alle Profile auf, zu denen sie gehört.
13. Ein Profil listet alle virtuellen SSL-Server, Dienste und Dienstgruppen auf, an die es gebunden ist.
14. Wenn die standardmäßige SSL-Profilfunktion aktiviert ist, verwenden Sie das Profil, um eines der Attribute einer SSL-Entität festzulegen oder zu ändern. Zum Beispiel virtueller Server, Dienst, Dienstgruppe oder ein interner Dienst.

Speichern Sie die Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
save config

shell

root@ns# cd /nsconfig

root@ns# cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber
   >
<!--NeedCopy-->
```

Beispiel:

```
save config
shell
root@ns# cd /nsconfig
root@ns# cp ns.conf ns.conf.NS.11.0.jun.16
<!--NeedCopy-->
```

Das Standardprofil aktivieren

> **Wichtig:**
>
> - Speichern Sie Ihre Konfiguration, bevor Sie die Software aktualisieren, und aktivieren Sie die Standardprofile.
> - Ab Version 11.1 Build 51.x wird in der GUI und CLI eine Bestätigungsaufforderung angezeigt, wenn Sie das Standardprofil aktivieren, um zu verhindern, dass es versehentlich aktiviert wird.

Befehl: Der folgende Befehl aktiviert das Standardprofil und bindet dieses Profil an die SSL-Entitäten, an die ein Profil bereits gebunden ist. Das heißt, wenn ein Profil (zum Beispiel P1) bereits an eine SSL-Entität gebunden ist, ersetzt das Standard-Front-End-Profil oder das Standard-Back-End-Profil P1. Das ältere Profil (P1) wird nicht gelöscht. Es ist jetzt ein erweitertes SSL-Profil und enthält die früheren Einstellungen sowie die Chiffren und ECC-Kurven. Wenn Sie das Standardprofil nicht möchten, können Sie P1 explizit an die SSL-Entität binden.

```
set ssl parameter -defaultProfile ENABLED
    Save your configuration before enabling the Default profile. You
       cannot undo the changes. Are you sure you want to enable the
       Default profile? [Y/N]Y
Done
<!--NeedCopy-->
```

Aktualisieren Sie die Software auf einen Build, der die erweiterte Profilinfrastruktur unterstützt, und aktivieren Sie dann die Standardprofile.

> **Hinweise:**
>
> - Wenn ein Legacy-Profil (P1) bereits an eine SSL-Entität gebunden ist und Sie das Standardprofil aktivieren, überschreibt das Standardprofil die frühere Bindung. Das heißt, das Standardprofil ist an die SSL-Entitäten gebunden. Wenn Sie nicht möchten, dass das Standardprofil gebunden wird, müssen Sie P1 erneut an die SSL-Entität binden.
> - Ein einziger Vorgang (Standardprofil aktivieren oder `set ssl parameter -defaultProfile ENABLED`) aktiviert (bindet) sowohl das Standard-Front-End-Profil als auch das Standard-Back-End-Profil.

Parameter, die Teil der Standardprofile sind

Führen Sie die folgenden Befehle aus, um die Parameter aufzulisten, die Teil der standardmäßigen Front-End- und Back-End-Profile sind.

```
sh ssl profile ns_default_ssl_profile_frontend
sh ssl profile ns_default_ssl_profile_backend
<!--NeedCopy-->
```


Beispiel:

```
> sh ssl profile ns_default_ssl_profile_frontend
1)  Name: ns_default_ssl_profile_frontend   (Front-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED  Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED  Refresh Count: 0
    Deny SSL Renegotiation  ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:  NO
    Match HTTP Host header with SNI:    CERT
    Push flag:  0x0 (Auto)
    SSL quantum size:   8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45
    Subject/Issuer Name Insertion Format:   Unicode

    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server: 10
    Session Ticket: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    Allow Extended Master Secret: NO
    Send ALPN Protocol: NONE
```

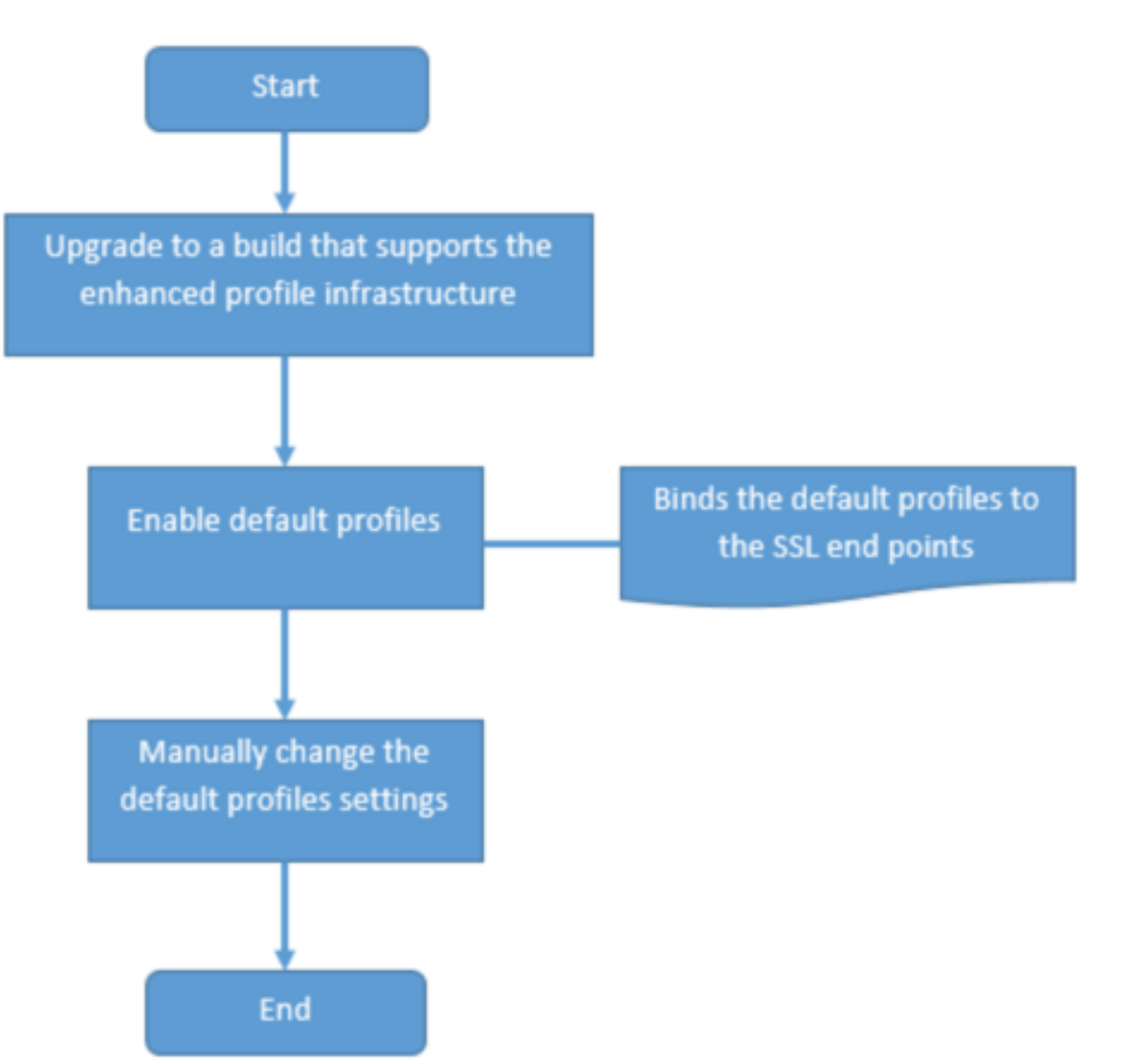


```
42
43
44      ECC Curve: P_256, P_384, P_224, P_521
45
46  1)  Cipher Name: DEFAULT    Priority :1
47      Description: Predefined Cipher Alias
48
49
50  > sh ssl profile ns_default_ssl_profile_backend
51  1)  Name: ns_default_ssl_profile_backend    (Back-End)
52      SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
            ENABLED  TLSv1.3: DISABLED
53      Server Auth: DISABLED
54      Use only bound CA certificates: DISABLED
55      Strict CA checks:   NO
56      Session Reuse: ENABLED  Timeout: 300 seconds
57      DH: DISABLED
58      Ephemeral RSA: DISABLED
59      Deny SSL Renegotiation  ALL
60      Non FIPS Ciphers: DISABLED
61      Cipher Redirect: DISABLED
62      SSL Redirect: DISABLED
63      Send Close-Notify: YES
64      Strict Sig-Digest Check: DISABLED
65      Push Encryption Trigger: Always
66      PUSH encryption trigger timeout:    1 ms
67      SNI: DISABLED
68      OCSP Stapling: DISABLED
69      Strict Host Header check for SNI enabled SSL sessions:  NO
70      Push flag:  0x0 (Auto)
71      SSL quantum size:   8 kB
72      Encryption trigger timeout  100 mS
73      Encryption trigger packet count:    45
74
75      Allow Extended Master Secret: NO
76
77      ECC Curve: P_256, P_384, P_224, P_521
78
79  1)  Cipher Name: DEFAULT_BACKEND    Priority :1
80      Description: Predefined Cipher Alias
81   Done
82   <!--NeedCopy-->
```


Anwendungsfall

Nachdem Sie die Standardprofile aktiviert haben, sind sie an alle SSL-Endpunkte gebunden. Die Standardprofile können bearbeitet werden. Wenn Ihre Bereitstellung die meisten Standardeinstellungen verwendet und nur wenige Parameter ändert, können Sie die Standardprofile bearbeiten. Die Änderungen werden sofort über alle Endpunkte hinweg wiedergegeben. Sie können auch benutzerdefinierte SSL-Profile mit einigen benutzerdefinierten und einigen Standardparametern erstellen und an die SSL-Entitäten binden.

Im folgenden Flussdiagramm werden die Schritte erläutert, die Sie ausführen müssen:



1. Informationen zum Aktualisieren der Software finden Sie unter Aktualisieren der Systemsoftware.
2. Aktivieren Sie die Standardprofile mit der CLI oder GUI.

- Geben Sie in der Befehlszeile Folgendes ein: `set ssl parameter -defaultProfile ENABLED`
- Wenn Sie die GUI bevorzugen, navigieren Sie zu **Traffic Management** > **SSL** > **Erweiterte SSL-Einstellungen ändern**, scrollen Sie nach unten und wählen Sie **Standardprofil aktivieren**aus.

Wenn ein Profil vor dem Upgrade nicht an einen Endpunkt gebunden war, ist ein Standardprofil an den SSL-Endpunkt gebunden. Wenn ein Profil vor dem Upgrade an einen Endpunkt gebunden war, wird dasselbe Profil nach dem Upgrade gebunden, und Standardverschlüsselungen werden dem Profil hinzugefügt.

1. (Optional) Ändern Sie manuell alle Einstellungen im Standardprofil.
   - Geben Sie in der Befehlszeile `set ssl profile <name>` gefolgt von den zu ändernden Parametern ein.
   - Wenn Sie die GUI bevorzugen, navigieren Sie zu **System** > **Profile**. Wählen Sie **unter SSL-Profile**ein Profil aus und klicken Sie auf **Bearbeiten**.

SSL-Profilparameter

Sie können die folgenden SSL-Parameter in einem SSL-Profil festlegen. Sie können einige dieser Parameter in einem virtuellen SSL-Server festlegen. Weitere Informationen zu Parametern für virtuelle SSL-Server finden Sie unter Parameter für virtuelle SSL-Server.

Unterstützung für sichere Neuverhandlungen am Backend einer NetScaler-Appliance

Diese Funktion wird auf den folgenden Plattformen unterstützt:

- VPX
- MPX-Plattformen mit N2- oder N3-Chips
- Intel Coleto SSL-Chip-basierte Plattformen

Diese Funktion wird auf der FIPS-Plattform noch nicht unterstützt.

Sichere Neuverhandlungen werden standardmäßig im Backend einer ADC-Appliance verweigert. Das heißt, der Parameter `denySSLReneg` ist auf ALL (Standard) festgelegt.

Um eine sichere Neuverhandlung im Backend zu ermöglichen, wählen Sie eine der folgenden Einstellungen für den Parameter `denySSLReneg` aus:

- NEIN
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NONSECURE

Ermöglichen Sie sichere Neuverhandlungen über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

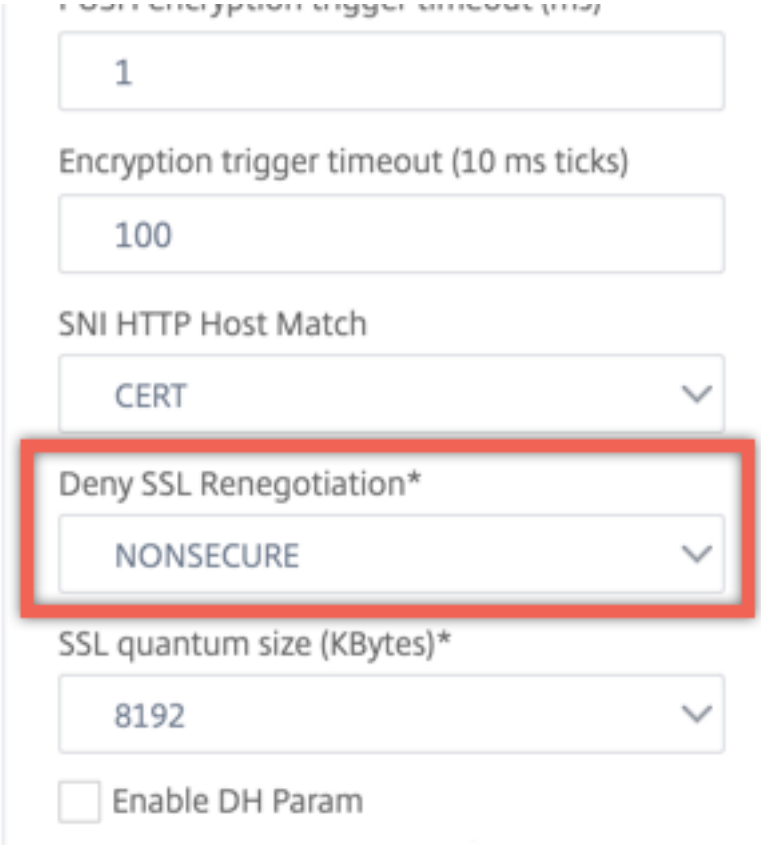
```
set ssl profile <name> -denySSLReneg <denySSLReneg>
```

Beispiel:

```
set ssl profile ns_default_ssl_profile_backend -denySSLReneg NONSECURE
 Done

sh ssl profile ns_default_ssl_profile_backend
1)  Name: ns_default_ssl_profile_backend    (Back-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Server Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:       NO
    Session Reuse: ENABLED      Timeout: 300 seconds
    DH: DISABLED
    Ephemeral RSA: DISABLED
    Deny SSL Renegotiation      NONSECURE
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:      NO
    Push flag:  0x0 (Auto)
    SSL quantum size:       8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45

    ECC Curve: P_256, P_384, P_224, P_521

1)  Cipher Name: DEFAULT_BACKEND        Priority :2
    Description: Predefined Cipher Alias

1)  Service Name: s187
 Done
<!--NeedCopy-->
```


Ermöglichen Sie sichere Neuverhandlungen mit der GUI

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Füge ein Profil hinzu oder bearbeite es.
3. Legen Sie “ **SSL-Neuverhandlung verweigern** “ auf einen anderen Wert als ALL fest.



Host-Header Validierung

Hinweis: Dieser Parameter wurde in Version 13.0 Build 52.x eingeführt.

Mit HTTP/1.1 mussten Clients mehrere Verbindungen verwenden, um mehrere Anfragen zu verarbeiten. Mit HTTP/2 können Clients Verbindungen über Domänen hinweg wiederverwenden, die durch dasselbe Zertifikat abgedeckt sind. Für eine SNI-fähige Sitzung muss die ADC-Appliance steuern können, wie der HTTP-Host-Header validiert wird, um dieser Änderung Rechnung zu tragen. In früheren Builds wurde die Anforderung verworfen, wenn der Parameter aktiviert war (auf “Ja” gesetzt) und die Anforderung den Host-Header für eine SNI-fähige Sitzung nicht enthielt. Wenn der Parameter deaktiviert war (auf “Nein” gesetzt), führte die Appliance die Validierung nicht durch. Ein neuer Parameter `SNIHTTPHostMatch` wird zu einem SSL-Profil und globalen SSL-Parametern hinzugefügt, um diese Validierung besser steuern zu können. Dieser Parameter kann drei Werte annehmen: CERT, STRICT und NONE. Diese Werte funktionieren nur für SNI-fähige Sitzungen wie

folgt. SNI muss auf dem virtuellen SSL-Server oder dem an den virtuellen Server gebundenen Profil aktiviert sein, und die HTTP-Anforderung muss den Host-Header enthalten.

- CERT — Die Verbindung wird weitergeleitet, wenn der Host-Header-Wert in der Anforderung durch das Zertifikat abgedeckt wird, das zum Einrichten dieser SSL-Sitzung verwendet wird.
- STRICT - Die Verbindung wird nur weitergeleitet, wenn der Host-Header-Wert in der Anforderung mit dem Servernamenwert übereinstimmt, der in der Client-Hello-Nachricht der SSL-Verbindung übergeben wurde.
- NEIN - Der Host-Header-Wert wurde nicht überprüft.

Mögliche Werte: NO, CERT, STRICT
Standardwert: CERT

Mit der Einführung des neuen Parameters ändert `SNIHTTPHostMatch` sich das Verhalten des `dropReqWithNoHostHeader` Parameters. Die Einstellung des `dropReqWithNoHostHeader` Parameters wirkt sich nicht mehr darauf aus, wie der Host-Header anhand des SNI-Zertifikats validiert wird.

Festlegen von SSL-Profilparametern über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> [-ssllogProfile <string>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )
[-sessTimeout <positive_integer>]] [-cipherRedirect ( ENABLED |
    DISABLED ) [-cipherURL <URL>]] [-clientAuth ( ENABLED | DISABLED )[-
    clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
DISABLED )] [-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl3 (
    ENABLED | DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-tls11 (
    ENABLED| DISABLED )] [-tls12 ( ENABLED | DISABLED )] [-tls13 (
    ENABLED |DISABLED )] [-SNIEnable ( ENABLED | DISABLED )] [-
    ocspStapling (ENABLED | DISABLED )] [-serverAuth ( ENABLED |
    DISABLED )] [-commonName <string>] [-pushEncTrigger <pushEncTrigger
    >] [-sendCloseNotify ( YES |
NO )] [-clearTextPort <port|*>] [-insertionEncoding ( Unicode | UTF-8)]
     [-denySSLReneg <denySSLReneg>] [-quantumSize <quantumSize>]
[-strictCAChecks ( YES | NO )] [-encryptTriggerPktCount <
    positive_integer>] [-pushFlag <positive_integer>][-
    dropReqWithNoHostHeader ( YES | NO )] [-SNIHTTPHostMatch <
    SNIHTTPHostMatch>] [-pushEncTriggerTimeout <positive_integer>]
[-sslTriggerTimeout <positive_integer>] [-clientAuthUseBoundCAChain (
    ENABLED | DISABLED )] [-sslInterception ( ENABLED | DISABLED )][-
```

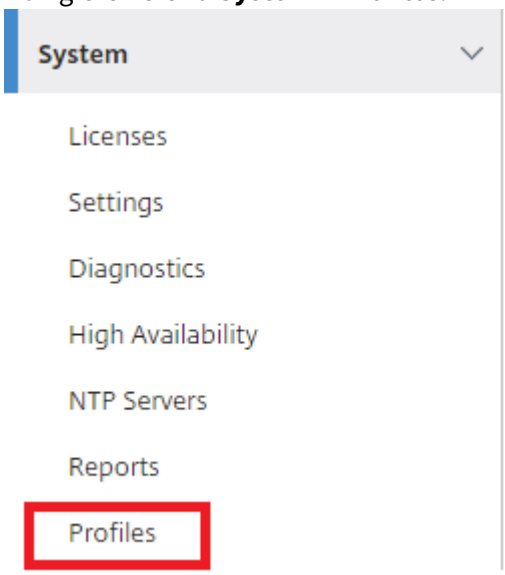


```
      ssliReneg ( ENABLED | DISABLED )] [-ssliOCSPCheck ( ENABLED |
      DISABLED )] [-ssliMaxSessPerServer <positive_integer>] [-HSTS (
      ENABLED| DISABLED )] [-maxage <positive_integer>] [-
      IncludeSubdomains ( YES | NO )] [-preload ( YES | NO )] [-
      sessionTicket ( ENABLED | DISABLED )][-sessionTicketLifeTime <
      positive_integer>] [-sessionTicketKeyRefresh (ENABLED | DISABLED )]
      {
 -sessionTicketKeyData  }
  [-sessionKeyLifeTime <positive_integer>] [-prevSessionKeyLifeTime <
     positive_integer>]
[-cipherName <string> -cipherPriority <positive_integer>][-
    strictSigDigestCheck ( ENABLED | DISABLED )]
[-skipClientCertPolicyCheck ( ENABLED | DISABLED )] [-zeroRttEarlyData
    ( ENABLED | DISABLED )] [-tls13SessionTicketsPerAuthContext
<positive_integer>] [-dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

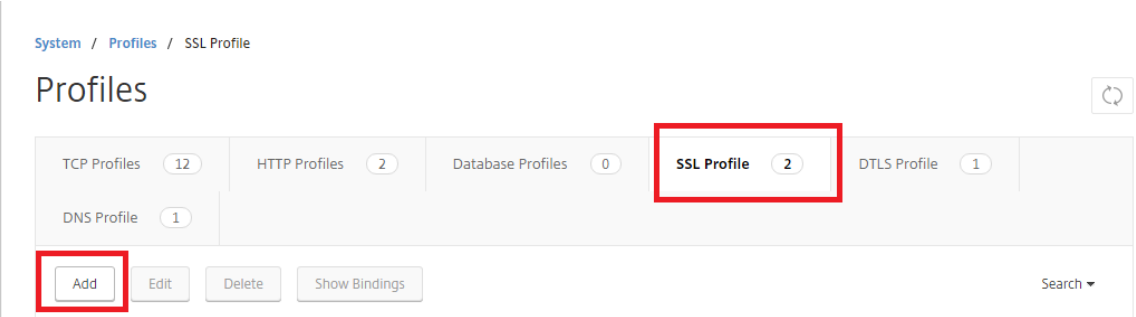
Festlegen von SSL-Profilparametern über die GUI

So fügen Sie ein Profil hinzu:

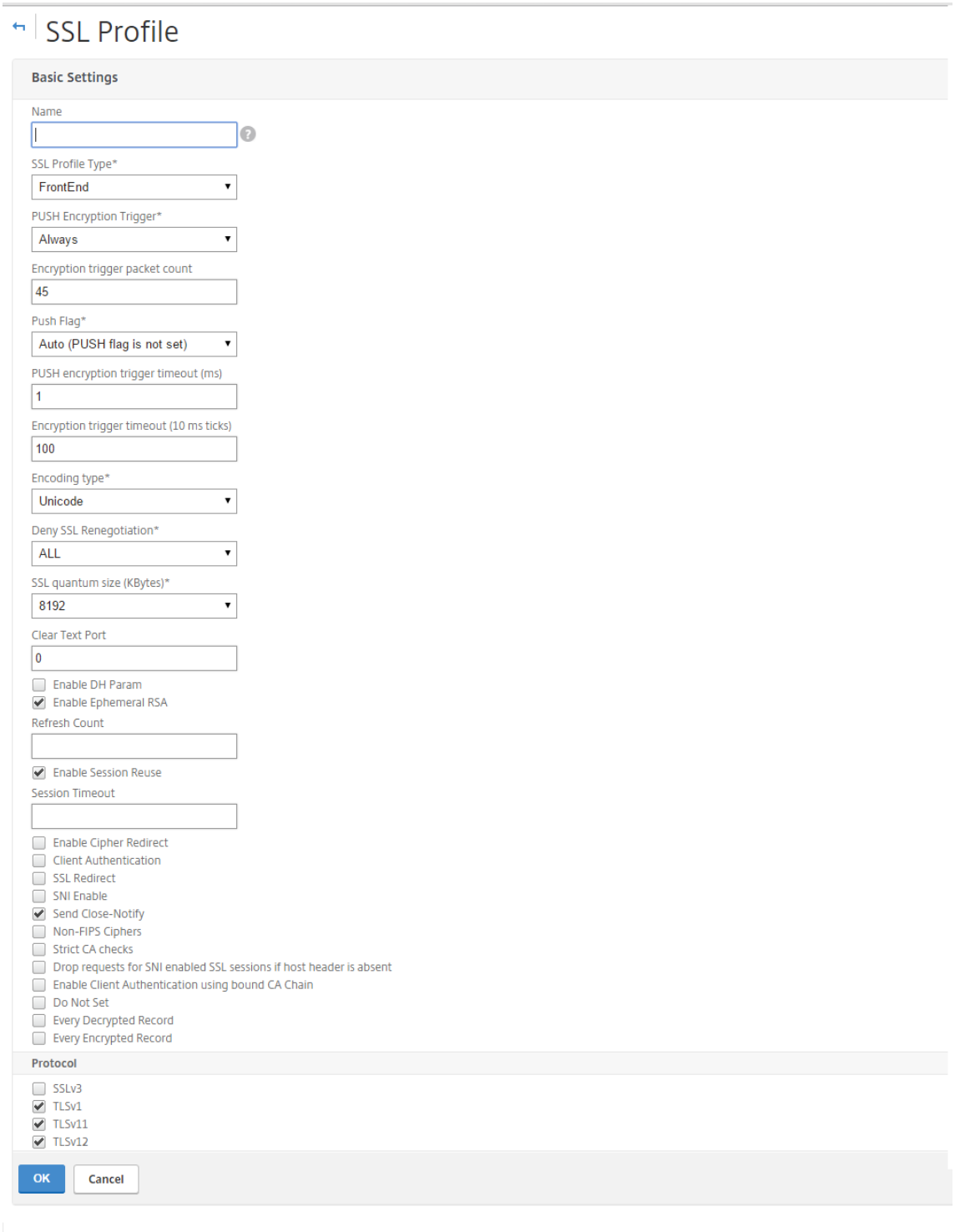
1. Navigieren Sie zu **System > Profiles**.



2. Wählen Sie **SSL-Profile**. Klicken Sie auf **Hinzufügen**.



3. Geben Sie Werte für die verschiedenen Parameter an.



4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig**.

So verwenden Sie ein vorhandenes SSL-Profil wieder:

1. Navigieren Sie zu **System > Profiles**.
2. Wählen Sie ein vorhandenes Profil und klicken Sie auf **Hinzufügen**.

3. Geben Sie einen anderen Namen an, ändern Sie alle Parameter und klicken Sie auf **OK**.
4. Klicken Sie auf **Fertig**.

Erweiterung des TLS-Sitzungstickets

Ein SSL-Handshake ist ein CPU-intensiver Vorgang. Wenn die Wiederverwendung von Sitzungen aktiviert ist, wird der Server-/Clientschlüsselaustausch für vorhandene Clients übersprungen. Sie dürfen ihre Sitzung fortsetzen. Diese Aktion verbessert die Reaktionszeit und erhöht die Anzahl der SSL-Transaktionen pro Sekunde, die ein Server unterstützen kann. Der Server muss jedoch Details zu jedem Sitzungsstatus speichern, der Speicher verbraucht und nur schwer von mehreren Servern gemeinsam genutzt werden kann, wenn Anforderungen über Server verteilt werden.

NetScaler-Appliances unterstützen die TLS-Erweiterung SessionTicket. Die Verwendung dieser Erweiterung zeigt an, dass die Sitzungsdetails auf dem Client und nicht auf dem Server gespeichert werden. Der Client muss angeben, dass er diesen Mechanismus unterstützt, indem er die TLS-Erweiterung des Sitzungstickets in die Hello-Nachricht des Clients einbezieht. Für neue Kunden ist diese Erweiterung leer. Der Server sendet ein neues Sitzungsticket in der NewSessionTicket-Handshake-Nachricht. Das Sitzungsticket wird mithilfe eines Schlüsselpaars verschlüsselt, das nur dem Server bekannt ist. Wenn ein Server jetzt kein neues Ticket ausstellen kann, schließt er einen regulären Handshake ab.

Diese Funktion ist nur in Front-End-SSL-Profilen verfügbar und nur am Front-End der Kommunikation, in dem die Appliance als Server fungiert und Sitzungstickets generiert.

Einschränkungen

- Diese Funktion wird auf einer FIPS-Plattform nicht unterstützt.
- Diese Funktion wird nur mit den TLS-Versionen 1.1 und 1.2 unterstützt.
- Die Beständigkeit der SSL-Sitzungskennung wird mit Sitzungstickets nicht unterstützt.

Aktivieren der TLS-Sitzungsticket-Erweiterung über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -sessionTicket (ENABLED | DISABLED ) [-
   sessionTicketLifeTime <positive_integer>
<!--NeedCopy-->
```

Argumente:

SessionTicket: Erweiterung des TLS-Sitzungstickets im Status. Die Verwendung dieser Erweiterung zeigt an, dass die Sitzungsdetails auf dem Client und nicht auf dem Server gespeichert werden, wie in RFC 5077 definiert.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

SessionTicketLifetime: Geben Sie eine Zeit in Sekunden an, nach der das Sitzungsticket abläuft und ein neuer SSL-Handshake initiiert werden muss.

Standardwert: 300

Mindestwert: 0

Maximaler Wert: 172800

Beispiel:

```
1 add ssl profile profile1 -sessionTicket ENABLED -sessionTicketlifeTime
     300
2 Done
3 <!--NeedCopy-->
```

Aktivieren der TLS-Sitzungsticket-Erweiterung über die GUI

1. Navigieren Sie zu **System** > **Profile**. Wählen Sie **SSL-Profile**.
2. Klicken Sie auf **Hinzufügen** und geben Sie einen Namen für das Profil an.
3. Wählen Sie **Sitzungsticket**.
4. Geben Sie optional die **Lebensdauer des Sitzungstickets (Sekunden)**an.

Sichere Umsetzung von Sitzungstickets

Durch die Verwendung von TLS-Sitzungstickets können Clients abgekürzte Handshakes für eine schnellere Wiederverbindung zu Servern verwenden. Wenn Sitzungstickets jedoch nicht für längere Zeit verschlüsselt oder geändert werden, können sie ein Sicherheitsrisiko darstellen. Sie können Sitzungstickets sichern, indem Sie sie mit einem symmetrischen Schlüssel verschlüsseln. Um eine Weiterleitungsgeheimnis zu erreichen, können Sie ein Zeitintervall angeben, in dem der Schlüssel für das Sitzungsticket aktualisiert wird.

Die Appliance generiert standardmäßig die Schlüssel für das Sitzungsticket. Wenn jedoch mehrere Appliances in einer Bereitstellung die Sitzungstickets des jeweils anderen entschlüsseln müssen, müssen sie alle denselben Sitzungsticketschlüssel verwenden. Daher müssen Sie dieselben Sitzungsticket-Schlüsseldaten manuell auf allen Appliances festlegen (hinzufügen oder laden). Zu den Eckdaten des Sitzungstickets gehören die folgenden Informationen:

- Name des Sitzungstickets.
- Der AES-Schlüssel der Sitzung, der zum Verschlüsseln oder Entschlüsseln des Tickets verwendet wird.

- HMAC-Schlüssel der Sitzung, mit dem der Digest des Tickets berechnet wird.

Sie können jetzt Schlüsseldaten für Sitzungstickets mit einer Länge von 64 Byte für die Unterstützung von 256-Bit-HMAC-Schlüsseln konfigurieren, wie in RFC 5077 empfohlen. Schlüssellängen von 48 Byte werden aus Gründen der Abwärtskompatibilität ebenfalls unterstützt.

> **Hinweis:**
>
> Stellen Sie beim manuellen Eingeben der Sitzungsticket-Schlüsseldaten sicher, dass die Konfiguration über alle NetScaler-Appliances in einem HA-Setup oder in einem Cluster-Setup identisch ist.

Der `sessionTicketKeyLifeTime` Parameter gibt an, wie oft ein Session-Ticket-Schlüssel aktualisiert wird. Sie können den `prevSessionTicketKeyLifeTime` Parameter festlegen, um anzugeben, wie lange der vorherige Session-Ticket-Schlüssel für die Entschlüsselung von Tickets mit diesem Schlüssel beibehalten wird, nachdem ein neuer Schlüssel generiert wurde. Die `prevSessionTicketKeyLifeTime` Einstellung verlängert die Zeit, in der ein Client einen abgekürzten Handshake zum Wiederverbinden verwenden kann. Wenn beispielsweise auf 10 Minuten und `prevSessionTicketKeyLifeTime` auf 5 Minuten festgelegt `sessionTicketKeyLifeTime` ist, wird nach 10 Minuten ein neuer Schlüssel generiert und für alle neuen Sitzungen verwendet. Zuvor verbundene Clients haben jedoch weitere 5 Minuten Zeit, für die zuvor ausgestellte Tickets für einen abgekürzten Handshake honoriert werden.

Konfigurieren von SSL-Sitzungsticket-Daten über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -sessionTicket ENABLED -sessionTicketLifeTime <
    positive_integer> -sessionTicketKeyRefresh ( ENABLED | DISABLED )] -
    sessionTicketKeyLifeTime <positive_integer> [-
    prevSessionTicketKeyLifeTime <positive_integer>]
<!--NeedCopy-->
```

Argumente:

SessionTicket: Verwenden Sie Sitzungstickets wie in RFC 5077 beschrieben. Das Einrichten des ersten Handshakes erfordert CPU-intensive Verschlüsselungsvorgänge mit öffentlichen Schlüsseln. Mit der Einstellung **ENABLED** gibt ein Server ein Sitzungsticket an einen Client aus, mit dem der Client einen abgekürzten Handshake ausführen kann.

Mögliche Werte: ENABLED, DISABLED. Standard: DEAKTIVIERT

SessionTicketLifetime: Lebensdauer des Sitzungstickets in Sekunden. Nach Ablauf dieser Zeit können Kunden dieses Ticket nicht mehr verwenden, um ihre Sitzung fortzusetzen.

Maximalwert: 172800. Mindestwert: 0. Standardeinstellung: 300.

SessionTicketKeyRefresh: Wenn die durch den Parameter für die Lebensdauer des Sitzungsticketschlüssels angegebene Zeit abläuft, generieren Sie den Schlüssel für das Sitzungsticket neu, der zum Verschlüsseln oder Entschlüsseln der Sitzungstickets verwendet wird. Wird automatisch aktiviert, wenn SessionTicket aktiviert ist. Deaktiviert, wenn ein Administrator die Sitzungsticket-Daten eingibt.

Mögliche Werte: ENABLED, DISABLED. Standard: ENABLED

SessionKeyLifetime: Lebensdauer eines symmetrischen Schlüssels in Sekunden, der zum Verschlüsseln der von einer NetScaler-Appliance ausgegebenen Sitzungstickets verwendet wird.

Maximaler Wert: 86400. Minimaler Wert: 600. Standardeinstellung: 3000

prevSessionKeyLifetime: Zeit in Sekunden, für die der vorherige symmetrische Schlüssel, der zum Verschlüsseln von Sitzungstickets verwendet wurde, nach Ablauf der Lebensdauer des Sitzungsticket-Schlüssels für bestehende Clients gültig bleibt. Innerhalb dieser Zeit können bestehende Clients ihre Sitzungen fortsetzen, indem sie den vorherigen Sitzungsticketschlüssel verwenden. Sitzungstickets für neue Clients werden mit dem neuen Schlüssel verschlüsselt.

Maximalwert: 172800. Mindestwert: 0. Standard: 0

Beispiel:

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED
    -sessionTicketlifeTime 120 -sessionTicketKeyRefresh ENABLED -
    sessionTicketKeyLifeTime 100 -prevSessionTicketKeyLifeTime 60

Done

show ssl profile ns_default_ssl_profile_frontend

    Session Ticket: ENABLED
    Session Ticket Lifetime: 120 (secs)
    Session Key Auto Refresh: ENABLED
    Session Key Lifetime: 100 (secs)
    Previous Session Key Lifetime: 60 (secs)
<!--NeedCopy-->
```

Konfigurieren von SSL-Sitzungsticket-Daten über die GUI

1. Navigieren Sie zu **System** > **Profile**und wählen Sie **SSL-Profil**aus.
2. Wählen Sie **ns_default_ssl_profile_frontend aus** und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen** auf das Stiftsymbol und legen Sie die folgenden Parameter fest:

- Sitzungsticket
- Lebensdauer des Sitzungstickets (Sekunden)
- Automatische Aktualisierung des Sitzungsticketschlüssels
- Lebensdauer des Sitzungsticketschlüssels (Sekunden)
- Lebensdauer des Ticketschlüssels für vorherige Sitzung (Sekunden)

4. Klicken Sie auf **OK**.

Geben Sie SSL-Sitzungsticketdaten über die CLI manuell ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -sessionTicket ENABLED

set ssl profile <name> -sessionTicketKeyData

show ssl profile ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

Argumente:

SessionTicket: Verwendung von Sitzungstickets wie in RFC 5077 beschrieben. Das Einrichten des ersten Handshakes erfordert CPU-intensive Verschlüsselungsvorgänge mit öffentlichen Schlüsseln. Mit der Einstellung **ENABLED** gibt ein Server ein Sitzungsticket an einen Client aus, mit dem der Client einen abgekürzten Handshake ausführen kann.

Mögliche Werte: ENABLED, DISABLED. Standard: DEAKTIVIERT

Schlüsseldaten des Sitzungstickets: Contains the session ticket name (0-15 bytes), the session AES key used to encrypt or decrypt the session ticket (16-31 bytes), and the session HMAC key used to compute the digest of the ticket (32-63 bytes). Externally generated by an administrator and added to a NetScaler appliance.

Maximale Länge: 64 Byte

Beispiel:

```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED

Done

set ssl profile ns_default_ssl_profile_frontend -sessionTicketKeyData
    11111111111111111111111111111111111111111111111111

Done
```



```
8
9  show ssl profile ns_default_ssl_profile_frontend
10
11     1) Name: ns_default_ssl_profile_frontend (Front-End)
12     SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1.2: ENABLED
13     Client Auth: DISABLED
14     Use only bound CA certificates: DISABLED
15     Strict CA checks: NO
16     Session Reuse: ENABLED Timeout: 120 seconds
17     DH: DISABLED
18     DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA: ENABLED
           Refresh Count: 0
19     Deny SSL Renegotiation ALL
20     Non FIPS Ciphers: DISABLED
21     Cipher Redirect: DISABLED
22     SSL Redirect: DISABLED
23     Send Close-Notify: YES
24     Push Encryption Trigger: Always
25     PUSH encryption trigger timeout: 1 ms
26     SNI: DISABLED
27     OCSP Stapling: DISABLED
28     Strict Host Header check for SNI enabled SSL sessions: NO
29     Push flag: 0x0 (Auto)
30     SSL quantum size: 8 kB
31     Encryption trigger timeout 100 mS
32     Encryption trigger packet count: 45
33     Subject/Issuer Name Insertion Format: Unicode
34     Session Ticket: ENABLED
35     Session Ticket Lifetime: 300 (secs)
36     Session Key Auto Refresh: DISABLED
37     Session Key Lifetime: 3000 (secs)
38     Previous Session Key Lifetime: 0 (secs)
39     Session Key Data: 84
          dad1afc6d56b0deeb0a7fd7f299a207e8d8c15cdd087a5684a11a329fd732e87a0535d908
40     47
          e8c181ba266f5c8838ae472cb3ab9255b683bf922fad32cee816c329989ef7cdeb278e93a
41
42     ECC Curve: P_256, P_384, P_224, P_521
43
44     1) Cipher Name: DEFAULT Priority :4
45     Description: Predefined Cipher Alias
46
47     1) Internal Service Name (Front-End): nsrnatsip-127.0.0.1-5061
```



```
48      2) Internal Service Name (Front-End): nskrpcs-127.0.0.1-3009
49      3) Internal Service Name (Front-End): nshttps-::1l-443
50      4) Internal Service Name (Front-End): nsrpcs-::1l-3008
51      5) Internal Service Name (Front-End): nshttps-127.0.0.1-443
52      6) Internal Service Name (Front-End): nsrpcs-127.0.0.1-3008
53      7) Vserver Name: v1
54
55  Done
56  <!--NeedCopy-->
```

Geben Sie SSL-Sitzungsticketdaten über die GUI manuell ein

1. Navigieren Sie zu **System > Profile**und wählen Sie **SSL-Profil**aus.
2. Wählen Sie **ns_default_ssl_profile_frontend aus** und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen** auf das Stiftsymbol und legen Sie die folgenden Parameter fest:
   - Sitzungsticket
   - Eckdaten des Sitzungstickets
   - Schlüsseldaten des Sitzungstickets bestätigen
4. Klicken Sie auf **OK**.

Unterstützung für Extended Master Secret in SSL-Handshake auf NetScaler Nicht-FIPS-Plattformen

Extended Master Secret (EMS) ist eine optionale Erweiterung des Transport Layer Security (TLS) -Protokolls. Ein neuer Parameter wird hinzugefügt, der sowohl für Front-End- als auch für Back-End-SSL-Profile gilt, um EMS auf der NetScaler-Appliance zu unterstützen. Wenn der Parameter aktiviert ist und der Peer EMS unterstützt, verwendet die ADC-Appliance die EMS-Berechnung. Wenn der Peer EMS nicht unterstützt, wird die EMS-Berechnung nicht für die Verbindung verwendet, obwohl der Parameter auf der Appliance aktiviert ist. Weitere Informationen zu EMS finden Sie unter RFC 7627.

Hinweis: EMS ist nur für Handshakes anwendbar, die die TLS-Protokollversion 1.0, 1.1 oder 1.2 verwenden.

Plattformunterstützung für EMS

- MPX- und SDX-Plattformen, die entweder Cavium N3-Chips oder Intel Coleto Creek-Kryptokarten enthalten. Die folgenden Plattformen werden mit Intel Coleto-Chips geliefert:
- MPX 5900

- MPX/SDX 8900
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPS/SDX 26000-100 G
- MPX/SDX 15000-50 G

Sie können den `show hardware` Befehl auch verwenden, um festzustellen, ob Ihre Appliance über Coleto (COL) oder N3-Chips verfügt.

- MPX- und SDX-Plattformen ohne Kryptokarten (nur Software).
- Nur-Software-Plattformen: VPX, CPX und BLX.

EMS kann auf den folgenden Plattformen nicht aktiviert werden:

- MPX 9700 FIPS und MPX 14000 FIPS-Plattformen.
- MPX- und SDX-Plattformen mit Cavium N2-Kryptochips.

Wenn der Parameter aktiviert ist, versucht die ADC-Appliance, EMS in TLS 1.2-, TLS 1.1- und TLS 1.0-Verbindungen zu verwenden. Die Einstellung wirkt sich nicht auf TLS 1.3- oder SSLv3-Verbindungen aus.

Damit EMS mit dem Peer ausgehandelt werden kann, aktivieren Sie die Einstellung im SSL-Profil, das an den virtuellen Server (Front-End) oder den Dienst (Backend) gebunden ist.

EMS mit der CLI aktivieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <profile name> [-allowExtendedMasterSecret (YES | NO)]
```

Beispiele

```
1 set ssl profile ns_default_ssl_profile_frontend  -
     allowExtendedMasterSecret YES
2
3 set ssl profile ns_default_ssl_profile_backend  -
     allowExtendedMasterSecret YES
4 <!--NeedCopy-->
```

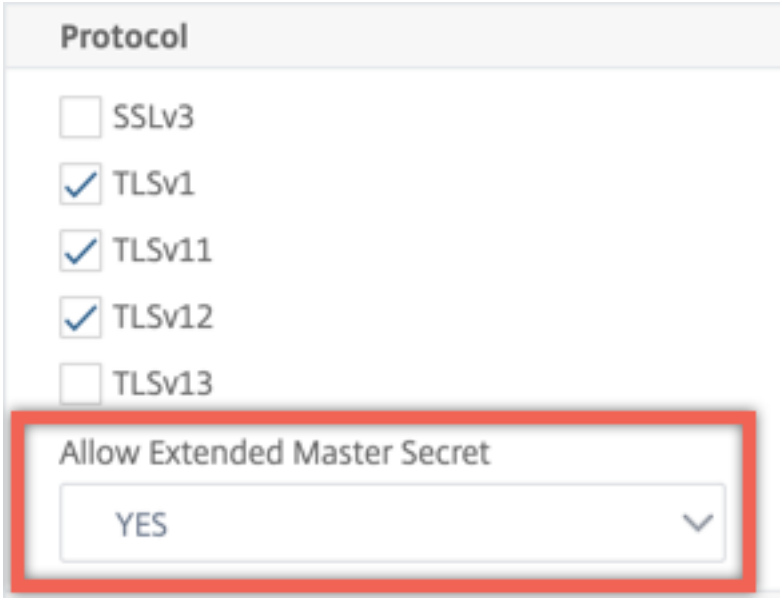
Die folgende Tabelle zeigt den Standardwert des `allowExtendedMasterSecret` Parameters für verschiedene Standard- und benutzerdefinierte Profile.

Profil	Standardeinstellung
Standard-Front-End-Profil	NEIN

Profil	Standardeinstellung
Sicheres Front-End-Standardprofil	JA
Standard-Back-End-Profil	NEIN
Benutzerdefiniertes Profil	NEIN

EMS mit der GUI aktivieren

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Fügen Sie ein Profil hinzu oder bearbeiten Sie ein Profil.
3. Setzen Sie **Extended Master Secret zulassen** auf JA.



Unterstützung für die Verarbeitung der ALPN-Erweiterung in der Client-Hello-Nachricht

Den Front-End-SSL-Profilen `alpnProtocol` wird ein Parameter hinzugefügt, um das Anwendungsprotokoll in der ALPN-Erweiterung für die Verbindungen auszuhandeln, die vom virtuellen SSL_TCP-Server verarbeitet werden. Es wird nur das im SSL-Profil angegebene Protokoll ausgehandelt, wenn dasselbe Protokoll in der ALPN-Erweiterung der Client-Hello-Nachricht empfangen wird.

Hinweis: Der `alpnProtocol` Parameter wird nur für Front-End-SSL-Profile unterstützt und gilt für SSL-Verbindungen, die von virtuellen Servern vom Typ SSL_TCP verarbeitet werden.

Stellen Sie das Protokoll im Front-End-SSL-Profil über die CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile ns_default_ssl_profile_frontend -alpnProtocol <protocol_name
>
```

Der `alpnProtocol` Parameter kann drei Werte annehmen. Maximale Länge: 4096 Byte.

- **KEINE:** Aushandlung des Anwendungsprotokolls findet nicht statt. Dies ist die Standardeinstellung.
- **HTTP1:** HTTP1 kann als Anwendungsprotokoll ausgehandelt werden.
- **HTTP2:** HTTP2 kann als Anwendungsprotokoll ausgehandelt werden.

Beispiel:

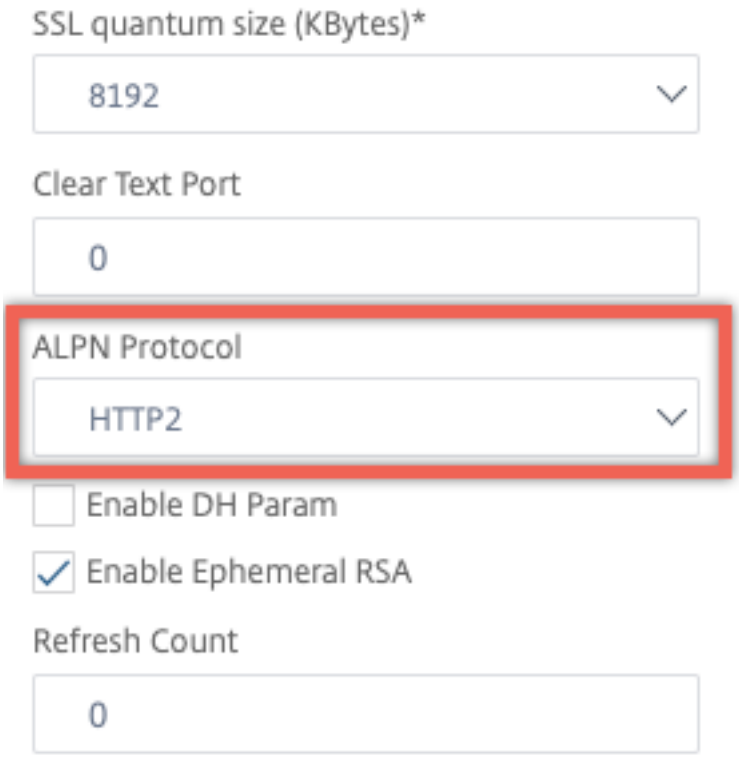
```
set ssl profile ns_default_ssl_profile_frontend -ALPNProtocol HTTP2
> sh ssl profile ns_default_ssl_profile_frontend
1)  Name: ns_default_ssl_profile_frontend   (Front-End)
    SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED  Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED  Refresh Count: 0
    Deny SSL Renegotiation  ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:  NO
    Match HTTP Host header with SNI:    CERT
    Push flag:  0x0 (Auto)
    SSL quantum size:   8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45
```



```
30      Subject/Issuer Name Insertion Format:   Unicode
31
32      SSL Interception: DISABLED
33      SSL Interception OCSP Check: ENABLED
34      SSL Interception End to End Renegotiation: ENABLED
35      SSL Interception Maximum Reuse Sessions per Server: 10
36      Session Ticket: DISABLED
37      HSTS: DISABLED
38      HSTS IncludeSubDomains: NO
39      HSTS Max-Age: 0
40      HSTS Preload: NO
41      Allow Extended Master Secret: NO
42      Send ALPN Protocol: HTTP2
43
44  Done
45  <!--NeedCopy-->
```

Stellen Sie das Protokoll im Front-End-SSL-Profil über die GUI ein

1. Navigieren Sie zu **System > Profile**und wählen Sie **SSL-Profil**aus.
2. Wählen Sie **ns_default_ssl_profile_frontend aus** und klicken Sie auf **Bearbeiten**.
3. Wählen Sie in der Liste **ALPN-Protokoll** die Option **HTTP2**aus.



Laden Sie eine alte Konfiguration

Die Aktivierung der Standardprofile ist nicht umkehrbar. Wenn Sie jedoch entscheiden, dass für Ihre Bereitstellung die Standardprofile nicht erforderlich sind, können Sie eine ältere Konfiguration laden, die Sie gespeichert haben, bevor Sie die Standardprofile aktiviert haben. Die Änderungen werden wirksam, nachdem Sie die Appliance neu gestartet haben.

Laden einer alten Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
shell

root@ns# clear config

root@ns# cd /nsconfig

root@ns# cp ns.conf.NS.11.0.jun.16 ns.conf

root@ns# reboot
<!--NeedCopy-->
```

Ratenbegrenzende SSL-Neuverhandlungen

Wenn die SSL-Neuverhandlung aktiviert ist, gibt es keine Begrenzung für die Anzahl der Neuverhandlungsanfragen. Infolgedessen ist der NetScaler anfällig für DoS-Angriffe, die letztendlich dazu führen können, dass der NetScaler die Verarbeitung des SSL-Datenverkehrs vollständig einstellt. Der Parameter `maxRenegrate` wurde in das SSL-Profil eingeführt, um dieses Problem zu beheben, indem die Anzahl der Neuverhandlungsanfragen begrenzt wird, die innerhalb einer Sekunde auf einer SSL-Entität eingehen.

Dieser Parameter ist nur konfigurierbar, wenn er nicht auf ALL gesetzt `denySSLReneg` ist. Wenn auf Null gesetzt `maxRenegRate` ist, ist die Ratenbegrenzung deaktiviert (Standardeinstellung). Wenn es auf einen Integer-Wert zwischen 1 und 65535 gesetzt ist, ist die Ratenbegrenzung aktiviert und die maximale Anzahl von Neuverhandlungsanfragen pro Sekunde an jede Entität, die an das SSL-Profil gebunden ist, ist auf diesen Integer-Wert begrenzt. Wenn Sie beispielsweise im SSL-Profil `ssl-profile-1` den Parameter `maxRenegRate` auf 100 setzen und dieses Profil an zwei virtuelle Server v1 und v2 gebunden ist, hat v1 ein Limit von 100 und v2 ein Limit von 100 Neuverhandlungsanfragen.

> Hinweis:
>
> Diese Funktion wird vom DTLS-Protokoll nicht unterstützt.

So fügen Sie das Limit hinzu, während Sie ein SSL-Profil mit der CLI erstellen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl profile pf1 -denySSLReneg (NO | FRONTEND_CLIENT | FRONTEND_CLIENTSERVER
 | NONSECURE)-maxRenegRate 100
```

So legen Sie das Limit für ein vorhandenes SSL-Profil mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile pf1 denySSLReneg (NO | FRONTEND_CLIENT | FRONTEND_CLIENTSERVER
 | NONSECURE)-maxRenegRate 100
```

Beispiel In den folgenden Befehlen ist "maxRenegRate" auf 100 gesetzt. Infolgedessen sind maximal 100 Anfragen pro Sekunde an alle Entitäten zulässig, an die das Profil gebunden ist.

```
set ssl profile pf1 denySSLReneg (NO | FRONTEND_CLIENT | FRONTEND_CLIENTSERVER
 | NONSECURE)-maxRenegRate 100

add ssl profile pf1 -denySSLReneg (NO | FRONTEND_CLIENT | FRONTEND_CLIENTSERVER
 | NONSECURE)-maxRenegRate 100
```

So geben Sie das Limit mit der GUI an

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Klicken Sie auf **Hinzufügen**, um ein Profil zu erstellen, oder wählen Sie ein vorhandenes Profil aus.
3. Geben Sie für ein neues Profil einen Namen an.
4. Stellen Sie **Deny SSL Renegotiation** auf einen anderen Wert als **All** ein.
5. Geben Sie die **maximale Neuverhandlungsrate an.**
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Fertig**.

Sicheres Front-End-Profil

February 16, 2021

Neben einem Standard-Front-End und einem Standard-Back-End-Profil ist ab Version 12.1 ein neues sicheres Standard-Front-End-Profil verfügbar. Die Einstellungen, die für eine A+ Bewertung (Stand Mai 2018) von Qualys SSL Labs erforderlich sind, sind in dieses Profil vorinstalliert. Früher mussten Sie jeden Parameter explizit festlegen, der für eine A+-Bewertung auf einem SSL-Front-End-Profil oder einem virtuellen SSL-Server erforderlich ist. Jetzt können Sie das

ns_default_ssl_profile_secure_frontend-Profil an Ihren virtuellen SSL-Server binden und die erforderlichen Parameter werden automatisch auf Ihrem virtuellen SSL-Server festgelegt.

> **Hinweis:**
>
> Das sichere Front-End-Profil kann nicht bearbeitet werden.

Wenn Sie das Standardprofil aktivieren, wird das Standard-Front-End-Profil automatisch an alle virtuellen SSL-Server gebunden. Um eine A+-Bewertung zu erhalten, müssen Sie explizit das ns_default_ssl_profile_secure_frontend-Profil binden und auch ein SHA2/SHA256-Serverzertifikat an Ihren virtuellen SSL-Server binden.

Sichere Front-End-Profilparameter

Die Parameter mit ihren Standardeinstellungen sind hier aufgelistet:

```
SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2: ENABLED
     TLSv1.3: DISABLED

Deny SSL Renegotiation: NONSECURE

HSTS: ENABLED

HSTS IncludeSubDomains: YES

HSTS Max-Age: 15552000

Cipher Name: SECURE    Priority :1
<!--NeedCopy-->
```

Alias für sichere Verschlüsselungsverfahren

Ein neuer gesicherter Chiffrealias wird hinzugefügt und an das sichere Front-End-Profil gebunden. Um die Chiffre aufzulisten, die Teil dieses Alias sind, geben Sie an der Eingabeaufforderung Folgendes ein: show chiffre SECURE

```
show cipher SECURE

    1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc030
    2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02f
```



```
7      3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
          Priority : 3
8             Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)
                 Mac=AEAD   HexCode=0xc02c
9      4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
          Priority : 4
10            Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)
                 Mac=AEAD   HexCode=0xc02b
11 Done
12 <!--NeedCopy-->
```

Konfiguration

Gehen Sie wie folgt vor:

1. Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL hinzu.
2. Binden Sie ein SHA2/SHA256-Zertifikat.
3. Aktivieren Sie das Standardprofil.
4. Binden Sie das sichere Front-End-Profil an den virtuellen SSL-Server.

Abrufen einer A+-Bewertung für einen virtuellen SSL-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> <serviceType> <IPAddress> <port>
2 bind ssl vserver <vServerName> -certkeyName <string>
3 set ssl parameter -defaultProfile ENABLED
4 set ssl vserver <vServerName> -sslProfile
     ns_default_ssl_profile_secure_frontend
5 show ssl vserver [<vServerName>]
6 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver ssl-vsvr SSL 192.0.2.240 443
2
3 bind ssl vserver ssl-vsvr -certkeyName letrsa
4
5 set ssl parameter -defaultProfile ENABLED
6
7 Save your configuration before enabling the Default profile. You cannot
      undo the changes. Are you sure you want to enable the Default
     profile? [Y/N]y
8
```



```
set ssl vserver ssl-vsvr -sslProfile
   ns_default_ssl_profile_secure_frontend
<!--NeedCopy-->
```

```
sh ssl vserver ssl-vsvr

    Advanced SSL configuration for VServer ssl-vsvr:
    Profile Name :ns_default_ssl_profile_secure_frontend
    1) CertKey Name: letrsa     Server Certificate
Done
<!--NeedCopy-->
```

```
sh ssl profile ns_default_ssl_profile_secure_frontend

    1) Name: ns_default_ssl_profile_secure_frontend (Front-End)
    SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:                   NO
    Session Reuse: ENABLED   Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED     Refresh Count: 0
    Deny SSL Renegotiation                NONSECURE
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:  1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:
                           NO
    Push flag:              0x0 (Auto)
    SSL quantum size:                8 kB
    Encryption trigger timeout       100 mS
    Encryption trigger packet count: 45
    Subject/Issuer Name Insertion Format:  Unicode
```



```
    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server:   10
    Session Ticket: DISABLED
    HSTS: ENABLED
    HSTS IncludeSubDomains: YES
    HSTS Max-Age: 15552000
    ECC Curve: P_256, P_384, P_224, P_521
    1) Cipher Name: SECURE    Priority :1
    Description: Predefined Cipher Alias
    1) Vserver Name: v2
Done
<!--NeedCopy-->
```

Abrufen einer A+-Bewertung für einen virtuellen SSL-Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und wählen Sie einen virtuellen SSL-Server aus.
2. Klicken Sie unter Erweiterte Einstellungen auf SSL-Profil.
3. Wählen Sie ns_default_ssl_profile_secure_frontend aus.
4. Klicken Sie auf OK.
5. Klicken Sie auf Fertig.

Anhang A: Beispielmigration der SSL-Konfiguration nach dem Upgrade

January 19, 2021

Hinweis: Dieser Inhalt wurde entfernt, da das SSL-Migrationsskript für das neue Standardprofil nicht mehr unterstützt wird.

Anhang B: Standardeinstellungen für Front-End- und Back-End-SSL-Profile

January 19, 2021

Ein Standard-Front-End-Profil hat die folgenden Einstellungen:

```
sh ssl profile ns_default_ssl_profile_frontend
```



```
2
3  1)Name: ns_default_ssl_profile_frontend
4
5        Configuration for Front-End SSL profile
6        DH: DISABLED
7        Ephemeral RSA: ENABLED          Refresh Count: 0
8        Session Reuse: ENABLED          Timeout: 120 seconds
9        Non FIPS Ciphers: DISABLED
10       Cipher Redirect: ENABLED   Redirect URL: http://10.102.28.212/
             redirect.html
11       Client Auth: DISABLED
12       SSL Redirect: DISABLED
13       SNI: DISABLED
14       SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
             ENABLED
15       Push Encryption Trigger: Always
16       PUSH encryption trigger timeout:     1 ms
17       Send Close-Notify: YES
18       Push flag: 0x0 (Auto)
19       Deny SSL Renegotiation          NO
20       SSL quantum size:          8 kB
21       Strict CA checks:          NO
22       Encryption trigger timeout 100 mS
23       Encryption trigger packet count:     45
24       Use only bound CA certificates: DISABLED
25       Subject/Issuer Name Insertion Format: Unicode
26       Strict Host Header check for SNI enabled SSL sessions:          NO
27
28       ECC Curve: P_256, P_384, P_521
29
30 1)    Cipher Name: AES     Priority :2
31       Description: Predefined Cipher Alias
32
33 1)    Vserver Name: v1
34 2)    Vserver Name: nshttps-::1l-443
35 3)    Vserver Name: nsrpcs-::1l-3008
36 4)    Vserver Name: nskrpcs-127.0.0.1-3009
37 5)    Vserver Name: nshttps-127.0.0.1-443
38 6)    Vserver Name: nsrpcs-127.0.0.1-3008
39 Done
40 <!--NeedCopy-->
```

Ein Standard-Back-End-Profil hat die folgenden Einstellungen:

```
1 sh ssl profile ns_default_ssl_profile_backend
```



```
2
3  1)Name: ns_default_ssl_profile_backend
4
5        Configuration for Back-End SSL profile
6        Session Reuse: ENABLED          Timeout: 300 seconds
7        Non FIPS Ciphers: DISABLED
8        Server Auth: DISABLED
9        SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED  TLSv1.2:
            DISABLED
10       Push Encryption Trigger: Always
11       PUSH encryption trigger timeout:     1 ms
12       Send Close-Notify: YES
13       Push flag: 0x0 (Auto)
14       Deny SSL Renegotiation          ALL
15       SSL quantum size:          8 kB
16       Strict CA checks:          NO
17       Encryption trigger timeout 100 mS
18       Encryption trigger packet count:     45
19       Use only bound CA certificates: DISABLED
20
21       ECC Curve: P_256, P_224, P_521
22
23 1)    Cipher Name: AES     Priority :1
24       Description: Predefined Cipher Alias
25
26 2)    Cipher Name: RC4     Priority :2
27       Description: Predefined Cipher Alias
28
29 1)    Service Name: s2
30 2)    Service Name: s1
31 Done
32 <!--NeedCopy-->
```

Legacy-SSL-Profil

May 11, 2023

> **Hinweis:**
>
> Citrix empfiehlt, die erweiterten Profile anstelle von Legacy-Profilen zu verwenden. Informationen zur erweiterten Profilinfrastruktur finden Sie unter SSL-Profilinfrastruktur.

Wichtig:

> Binden Sie ein SSL-Profil an einen virtuellen SSL-Server. Binden Sie ein DTLS-Profil nicht an einen virtuellen SSL-Server. Informationen zu DTLS-Profilen finden Sie unter DTLS-Profile.

Sie können ein SSL-Profil verwenden, um anzugeben, wie ein NetScaler SSL-Datenverkehr verarbeitet. Das Profil ist eine Sammlung von SSL-Parametereinstellungen für SSL-Entitäten, wie virtuelle Server, Dienste und Dienstgruppen, und bietet eine einfache Konfiguration und Flexibilität. Sie sind nicht darauf beschränkt, nur einen Satz globaler Parameter zu konfigurieren. Sie können mehrere Sätze (Profile) globaler Parameter erstellen und verschiedenen SSL-Entitäten unterschiedliche Sätze zuweisen. SSL-Profile werden in zwei Kategorien eingeteilt:

- Frontend-Profile, die Parameter enthalten, die für die Frontend-Entität gelten. Das heißt, sie gelten für das Unternehmen, das Anfragen von einem Kunden erhält.
- Back-End-Profile, die Parameter enthalten, die für die Back-End-Entität gelten. Das heißt, sie gelten für die Entität, die Clientanfragen an einen Server sendet.

Im Gegensatz zu einem TCP- oder HTTP-Profil ist ein SSL-Profil optional. Daher gibt es kein Standard-SSL-Profil. Das gleiche Profil kann für mehrere Entitäten wiederverwendet werden. Wenn einer Entität kein Profil zugeordnet ist, gelten die auf globaler Ebene festgelegten Werte. Für dynamisch erlernte Dienste gelten die aktuellen globalen Werte.

In der folgenden Tabelle sind die Parameter aufgeführt, die Teil jedes Profils sind.

Frontend-Profil	Backend-Profil
cipherRedirect, cipherURL	denySSLReneg
clearTextPort*	encryptTriggerPktCount
clientAuth, clientCert	nonFipsCiphers
denySSLReneg	pushEncTrigger
dh, dhFile, dhCount	pushEncTriggerTimeout
dropReqWithNoHostHeader	pushFlag
encryptTriggerPktCount	quantumSize
eRSA, eRSACount	serverAuth
insertionEncoding	commonName
nonFipsCiphers	sessReuse, sessTimeout
pushEncTrigger	`SNIEnable`
pushEncTriggerTimeout	ssl3
pushFlag	sslTriggerTimeout
quantumSize	strictCAChecks

Frontend-Profil	Backend-Profil
redirectPortRewrite	tls1
sendCloseNotify	-
sessReuse, sessTimeout	-
SNIEnable	-
ssl3	-
sslRedirect	-
sslTriggerTimeout	-
strictCAChecks	-
tls1, tls11, tls12	-

* Der Parameter clearTextPort gilt nur für einen virtuellen SSL-Server.

Eine Fehlermeldung wird angezeigt, wenn Sie versuchen, einen Parameter festzulegen, der nicht Teil des Profils ist. Zum Beispiel, wenn Sie versuchen, den Parameter clientAuth in einem Back-End-Profil festzulegen.

Einige SSL-Parameter, wie CRL-Speichergröße, OCSP-Cachegröße, UndeFaction-Kontrolle und UndeFaction-Daten, sind in keinem der vorherigen Profile enthalten, da diese Parameter unabhängig von Entitäten sind.

Ein SSL-Profil unterstützt die folgenden Vorgänge:

- Hinzufügen — Erstellt ein SSL-Profil auf dem NetScaler. Geben Sie an, ob das Profil ein Frontend oder ein Backend ist. Frontend ist die Standardeinstellung.
- Festlegen — Ändert die Einstellungen eines vorhandenen Profils.
- Unset (Unset) — Setzt die angegebenen Parameter auf ihre Standardwerte. Wenn Sie keine Parameter angeben, wird eine Fehlermeldung angezeigt. Wenn Sie ein Profil für eine Entität aufheben, ist das Profil nicht an die Entität gebunden.
- Entfernen—Löscht ein Profil. Ein Profil, das von einer Entität verwendet wird, kann nicht gelöscht werden. Beim Löschen der Konfiguration werden alle Entitäten gelöscht. Infolgedessen werden die Profile auch gelöscht.
- Anzeigen — Zeigt alle Profile an, die auf dem NetScaler verfügbar sind. Wenn ein Profilname angegeben ist, werden die Details dieses Profils angezeigt. Wenn eine Entität angegeben ist, werden die mit dieser Entität verknüpften Profile angezeigt.

Erstellen Sie ein SSL-Profil mithilfe der CLI

- Um ein SSL-Profil hinzuzufügen, geben Sie Folgendes ein:

```
add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )]
<!--NeedCopy-->
```

- Um ein vorhandenes Profil zu ändern, geben Sie Folgendes ein:

```
set ssl profile <name>
<!--NeedCopy-->
```

- Um ein vorhandenes Profil zu deaktivieren, geben Sie Folgendes ein:

```
unset ssl profile <name> [-dh] [-dhFile] [-dhCount] [-eRSA] ...
<!--NeedCopy-->
```

- Um ein vorhandenes Profil von einer Entität zu entfernen, geben Sie Folgendes ein:

```
unset ssl vserver <vServerName>  -sslProfile
<!--NeedCopy-->
```

- Um ein vorhandenes Profil zu entfernen, geben Sie Folgendes ein:

```
rm ssl profile <name>
<!--NeedCopy-->
```

- Um ein vorhandenes Profil anzuzeigen, geben Sie Folgendes ein:

```
sh ssl profile <name>
<!--NeedCopy-->
```

Erstellen Sie ein SSL-Profil mithilfe der GUI

Navigieren Sie zu **System** > **Profile**, wählen Sie die Registerkarte SSL-Profile aus und erstellen Sie ein SSL-Profil.

Ermöglichen Sie eine strengere Kontrolle der Validierung von Client-Zertifikaten

Die NetScaler-Appliance akzeptiert gültige Intermediate-CA-Zertifikate, wenn sie von einer einzelnen Root-CA ausgestellt wurden. Das heißt, wenn nur das Root-CA-Zertifikat an den virtuellen Server gebunden ist und diese Root-CA eines der mit dem Client-Zertifikat gesendeten Zwischenzertifikate validiert, vertraut die Appliance der Zertifikatskette und der Handshake ist erfolgreich.

Wenn ein Client jedoch im Handshake eine Kette von Zertifikaten sendet, können die Zwischenzertifikate mithilfe eines CRL- oder OCSP-Responders nur dann validiert werden, wenn das Zertifikat an den virtuellen SSL-Server gebunden ist. Selbst wenn eines der Zwischenzertifikate widerrufen wird, ist der Handshake daher erfolgreich. Im Rahmen des Handshakes sendet der virtuelle SSL-Server die Liste der an ihn gebundenen CA-Zertifikate. Für eine strengere Kontrolle können Sie den virtuellen SSL-Server so konfigurieren, dass er nur ein Zertifikat akzeptiert, das von einem der an diesen virtuellen Server gebundenen CA-Zertifikate signiert wurde. Dazu müssen Sie die `ClientAuthUseBoundCAChain` Einstellung im SSL-Profil aktivieren, das an den virtuellen Server gebunden ist. Der Handshake schlägt fehl, wenn eines der an den virtuellen Server gebundenen CA-Zertifikate das Clientzertifikat nicht signiert hat.

Beispiel: Zwei Clientzertifikate, clientcert1 und clientcert2, werden von den Zwischenzertifikaten Int-CA-A bzw. int-CA-B signiert. Die Zwischenzertifikate sind vom Stammzertifikat Root-CA signiert. Int-CA-A und Root-CA sind an den virtuellen SSL-Server gebunden. Im Standardfall (ClientAuthUseBoundCAChain deaktiviert) werden sowohl clientcert1 als auch clientcert2 akzeptiert. Wenn ClientAuthUseBoundCAChain jedoch aktiviert ist, akzeptiert die NetScaler-Appliance nur clientcert1.

Ermöglichen Sie eine strengere Kontrolle der Clientzertifikatvalidierung über die CLI

Geben Sie in der Befehlszeile Folgendes ein: `set ssl profile <name> -ClientAuthUseBoundCAChain Enabled`

Ermöglichen Sie eine strengere Kontrolle der Validierung von Clientzertifikaten über die GUI

1. Navigieren Sie zu **System** > **Profile**, wählen Sie die Registerkarte **SSL-Profile** und erstellen Sie ein SSL-Profil oder wählen Sie ein vorhandenes Profil aus.
2. Wählen Sie **Client-Authentifizierung mit gebundener Zertifizierungsstellenkette**aktivieren aus.

Migrieren Sie die SSL-Konfiguration auf das erweiterte SSL-Profil

August 15, 2023

> **Hinweis:**
>
> Die Begriffe “Standard” und “erweitert” werden synonym für das erweiterte SSL-Profil verwendet.

In einer typischen Bereitstellung sind Hunderte von virtuellen Servern, Diensten und anderen SSL-Entitäten konfiguriert. Jede Entität kann ihre eigenen SSL-Einstellungen haben. Das Hinzufügen oder Ändern einer Einstellung für alle Entitäten kann ein umständlicher Prozess sein. Um diesem Bedarf

gerecht zu werden und den Konfigurationsprozess zu vereinfachen, können Sie SSL-Profile verwenden und sie an verschiedene Entitäten anhängen.

Ein SSL-Profil ist eine Sammlung von SSL-Parametereinstellungen für SSL-Entitäten wie virtuelle Server, Dienste (einschließlich interner Dienste) und Dienstgruppen. Es bietet einfache Konfiguration und Flexibilität, da Sie nicht darauf beschränkt sind, nur einen Satz globaler Parameter zu konfigurieren. Es gibt zwei Arten von Profilen:

- Frontend-Profil: Gilt für die Entitäten, die Anfragen von einem Client erhalten.
- Back-End-Profil: Gilt für Entitäten, die Client-Anfragen an den Backend-Server senden.

Sie müssen das erweiterte Profil für alle SSL-Endpunkte aktivieren, um die Standardprofile zu erben. Das Standardprofil enthält auch einige neue Parameter, die nur über das Profil konfiguriert werden können. Geben Sie an der NetScaler-CLI Folgendes ein:

```
set ssl parameter -defaultProfile ENABLED
```

Sie können ein Profil nicht deaktivieren. Einige wichtige Punkte im Zusammenhang mit dem erweiterten Profil finden Sie unter Zu beachtende Punkte.

Problemstellung

Wenn Sie das Standardprofil aktivieren, wird das integrierte Standard-SSL-Profil automatisch an alle Front-End-SSL-Entitäten und das `ns_default_ssl_profile_backend` an alle Back-End-SSL-Entitäten gebunden. Das Profil enthält einige Standardeinstellungen. Wenn Sie das Standardprofil aktivieren, gehen Ihre benutzerdefinierten Einstellungen verloren. Das manuelle Reparieren einer großen Konfiguration kann mühsam, zeitaufwändig und fehleranfällig sein. Daher zögern Kunden, zum Standardprofil zu migrieren.

Lösung

Das NetScaler-Team hat ein Skript entwickelt, das Ihre Konfiguration analysiert und benutzerdefinierte Profile auf der Grundlage Ihrer vorhandenen Einstellungen erstellt. Das Skript überprüft die Konfiguration Ihrer SSL-Entitäten und erstellt Profile für dieselben Einstellungen. Dann bindet es das entsprechende Profil an jede SSL-Entität. Das Profil ist als ausführbare Datei verfügbar, die unter Linux-, Windows- und Mac-Betriebssystemen ausgeführt werden kann.

Das Skript ist verfügbar unter https://github.com/netscaler/default-ssl-profile-script#readme.

> Wichtig
>
> Speichern Sie die Konfiguration, bevor Sie das Tool verwenden. Geben Sie in der NetScaler-CLI Folgendes ein: `save config`.

Ergebnis

Nachdem Sie das Skript ausgeführt haben, werden die benutzerdefinierten Profile mit den erforderlichen Einstellungen basierend auf Ihrer Konfiguration erstellt. Das entsprechende Profil ist an die verschiedenen Front-End- und Back-End-SSL-Entitäten gebunden. Ihre SSL-Entitäten haben jetzt dieselben Einstellungen wie vor der Aktivierung des Standardprofils. Der Unterschied besteht darin, dass diese Einstellungen jetzt Teil des SSL-Standardprofils sind. Um die Einstellungen für mehrere SSL-Entitäten zu ändern, müssen Sie nur das zugehörige Profil ändern. Die Einstellungen werden auf alle SSL-Entitäten angewendet, an die das Profil angehängt ist.

Widerrufslisten für Zertifikate

May 11, 2023

Ein von einer CA ausgestelltes Zertifikat bleibt in der Regel bis zu seinem Ablaufdatum gültig. Unter bestimmten Umständen kann die CA das ausgestellte Zertifikat jedoch vor dem Ablaufdatum sperren. Wenn beispielsweise der private Schlüssel eines Eigentümers kompromittiert wird, der Name eines Unternehmens oder einer Einzelperson geändert wird oder sich die Zuordnung zwischen dem Subjekt und der CA ändert.

Eine Zertifikatssperrliste (CRL) identifiziert ungültige Zertifikate anhand der Seriennummer und des Ausstellers.

Zertifizierungsstellen stellen regelmäßig CRLs aus. Sie können die NetScaler-Appliance so konfigurieren, dass sie eine CRL verwendet, um Clientanfragen zu blockieren, die ungültige Zertifikate enthalten.

Wenn Sie bereits eine CRL-Datei von einer CA haben, fügen Sie diese zur NetScaler-Appliance hinzu. Sie können Aktualisierungsoptionen konfigurieren. Sie können den NetScaler auch so konfigurieren, dass die CRL-Datei automatisch in einem bestimmten Intervall synchronisiert wird, entweder von einem Web- oder einem LDAP-Speicherort aus. Die Appliance unterstützt CRLs entweder im PEM- oder im DER-Dateiformat. Stellen Sie sicher, dass Sie das Dateiformat der CRL-Datei angeben, die der NetScaler-Appliance hinzugefügt wird.

Wenn Sie den ADC als CA verwendet haben, um Zertifikate zu erstellen, die in SSL-Bereitstellungen verwendet werden, können Sie auch eine CRL erstellen, um ein bestimmtes Zertifikat zu sperren. Diese Funktion kann beispielsweise verwendet werden, um sicherzustellen, dass selbstsignierte Zertifikate, die auf dem NetScaler erstellt wurden, weder in einer Produktionsumgebung noch nach einem bestimmten Datum verwendet werden.

Hinweis:

Standardmäßig werden CRLs im Verzeichnis /var/netscaler/ssl auf der NetScaler-Appliance gespeichert.

Erstellen Sie eine CRL auf der ADC-Appliance

Da Sie die ADC-Appliance verwenden können, um als CA zu fungieren und selbstsignierte Zertifikate zu erstellen, können Sie auch die folgenden Zertifikate sperren:

- Zertifikate, die Sie erstellt haben.
- Zertifikate, deren CA-Zertifikat Sie besitzen.

Die Appliance muss ungültige Zertifikate sperren, bevor sie eine CRL für diese Zertifikate erstellt. Die Appliance speichert die Seriennummern der gesperrten Zertifikate in einer Indexdatei und aktualisiert die Datei jedes Mal, wenn sie ein Zertifikat sperrt. Die Indexdatei wird automatisch erstellt, wenn ein Zertifikat zum ersten Mal gesperrt wird.

Widerrufen Sie ein Zertifikat oder erstellen Sie eine CRL mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <
    input_filename> | -genCRL <output_filename>)
<!--NeedCopy-->
```

Beispiel:

```
create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -revoke Invalid-1

create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -genCRL CRL-1
<!--NeedCopy-->
```

Widerrufen Sie ein Zertifikat oder erstellen Sie eine CRL mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe Getting Started die Option CRL Management aus.
2. Geben Sie die Zertifikatsdetails ein und **wählen Sie in der Liste „Vorgang** auswählen“ die **Option Zertifikat sperren**oder **CRL generieren**aus.

Fügen Sie dem ADC eine vorhandene CRL hinzu

Bevor Sie die CRL auf der NetScaler-Appliance konfigurieren, stellen Sie sicher, dass die CRL-Datei lokal auf der NetScaler-Appliance gespeichert ist. In einem HA-Setup muss die CRL-Datei auf beiden

ADC-Appliances vorhanden sein, und der Verzeichnispfad zur Datei muss auf beiden Appliances derselbe sein.

Fügen Sie mithilfe der CLI eine CRL auf dem NetScaler hinzu

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine CRL auf dem NetScaler hinzuzufügen und die Konfiguration zu überprüfen:

```
add ssl crl <crlName> <crlPath> [-inform (DER | PEM)]

show ssl crl [<crlName>]
<!--NeedCopy-->
```

Beispiel:

```
> add ssl crl crl-one /var/netscaler/ssl/CRL-one -inform PEM

Done

> show ssl crl crl-one

            Name: crl-one   Status: Valid,  Days to expiration: 29
            CRL Path: /var/netscaler/ssl/CRL-one
            Format: PEM     CAcert: samplecertkey
            Refresh: DISABLED
            Version: 1
            Signature Algorithm: sha1WithRSAEncryption
            Issuer:  C=US,ST=California,L=Santa Clara,O=NetScaler Inc.,
               OU=SSL Acceleration,CN=www.ns.com/emailAddress=
               support@NetScaler appliance.com
            Last_update:Jun 15 10:53:53 2010 GMT
            Next_update:Jul 15 10:53:53 2010 GMT

    1)      Serial Number: 00
            Revocation Date:Jun 15 10:51:16 2010 GMT
     Done
<!--NeedCopy-->
```

Fügen Sie mithilfe der GUI eine CRL auf dem NetScaler hinzu

Navigieren Sie zu **Traffic Management** > **SSL** > **CRL**und fügen Sie eine CRL hinzu.

CRL-Aktualisierungsparameter konfigurieren

Eine CRL wird von einer Zertifizierungsstelle in regelmäßigen Abständen oder manchmal unmittelbar nach dem Widerruf eines bestimmten Zertifikats generiert und veröffentlicht. Citrix empfiehlt, dass Sie die CRLs auf der NetScaler-Appliance regelmäßig aktualisieren, um sich vor Clients zu schützen, die versuchen, eine Verbindung mit ungültigen Zertifikaten herzustellen.

Die NetScaler-Appliance kann CRLs von einem Webstandort oder einem LDAP-Verzeichnis aus aktualisieren. Wenn Sie Aktualisierungsparameter und einen Webspeicherort oder einen LDAP-Server angeben, muss die CRL zum Zeitpunkt der Ausführung des Befehls nicht auf dem lokalen Festplattenlaufwerk vorhanden sein. Bei der ersten Aktualisierung wird eine Kopie auf dem lokalen Festplattenlaufwerk in dem durch den Parameter CRL File angegebenen Pfad gespeichert. Der Standardpfad zum Speichern der CRL lautet /var/netscaler/ssl.

Hinweis: In Version 10.0 und höher ist die Methode zum Aktualisieren einer CRL standardmäßig nicht enthalten. Geben Sie eine HTTP- oder LDAP-Methode an. Wenn Sie ein Upgrade von einer früheren Version auf Version 10.0 oder höher durchführen, müssen Sie eine Methode hinzufügen und den Befehl erneut ausführen.

Konfigurieren Sie die automatische Aktualisierung von CRL mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die automatische Aktualisierung von CRL zu konfigurieren und die Konfiguration zu überprüfen:

```
1 set ssl crl <crlName> [-refresh ( ENABLED | DISABLED )] [-CAcert <
     string>] [-server <ip_addr|ipv6_addr|*> | -url <URL>] [-method (
     HTTP | LDAP )] [-port <port>] [-baseDN <string>] [-scope ( Base |
     One )] [-interval <interval>] [-day <positive_integer>] [-time <HH:
     MM>][-bindDN <string>] {
2  -password  }
3   [-binary ( YES | NO )]
4
5 show ssl crl [<crlName>]
6 <!--NeedCopy-->
```

Beispiel:

```
1     set CRL crl1  -refresh enabled -method ldap -inform DER -CAcert ca1
          -server 10.102.192.192 -port 389 -scope base -baseDN "cn=
         clnt_rsa4_multicert_der,ou=eng,o=ns,c=in" -time 00:01
2
3     set ssl crl crl1 -refresh enabled -method http -cacert ca1 -port 80
          -time 00:10 -url http://10.102.192.192/crl/ca1.crl
4
```



```
5
6       > sh crl
7
8       1)          Name: crl1        Status: Valid,     Days to expiration:
            355
9                    CRL Path: /var/netscaler/ssl/crl1
10                   Format: PEM      CAcert: ca1
11                   Refresh: ENABLED          Method: HTTP
12                   URL: http://10.102.192.192/crl/ca1.crl
                        Port:80
13                   Refresh Time: 00:10
14                   Last Update: Successful, Date:Tue Jul  6 14:38:13 2010
15      Done
16  <!--NeedCopy-->
```

Konfigurieren Sie die automatische Aktualisierung von CRL mithilfe von LDAP oder HTTP mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL > CRL.**
2. Öffnen Sie eine CRL und wählen Sie **Automatische CRL-Aktualisierung aktivieren**aus.

> **Hinweis:**
>
> Wenn die neue CRL im externen Repository vor ihrer tatsächlichen Aktualisierungszeit aktualisiert wurde, wie im Feld **Letzte Aktualisierungszeit** der CRL angegeben, müssen Sie wie folgt vorgehen: Aktualisieren Sie die CRL auf der NetScaler-Appliance
>
> sofort.

Um die Uhrzeit der letzten Aktualisierung anzuzeigen, wählen Sie die CRL aus und klicken Sie auf **Details**.

CRLs synchronisieren

Die NetScaler-Appliance verwendet die zuletzt verteilte CRL, um zu verhindern, dass Clients mit gesperrten Zertifikaten auf sichere Ressourcen zugreifen.

Wenn CRLs häufig aktualisiert werden, benötigt die NetScaler-Appliance einen automatisierten Mechanismus, um die neuesten CRLs aus dem Repository abzurufen. Sie können die Appliance so konfigurieren, dass CRLs in einem bestimmten Aktualisierungsintervall automatisch aktualisiert werden.

Die Appliance verwaltet eine interne Liste von CRLs, die in regelmäßigen Abständen aktualisiert werden müssen. In diesen angegebenen Intervallen durchsucht die Appliance die Liste nach CRLs, die aktualisiert werden müssen. Anschließend stellt es eine Verbindung zum Remote-LDAP-Server oder

HTTP-Server her, ruft die neuesten CRLs ab und aktualisiert dann die lokale CRL-Liste mit den neuen CRLs.

> **Hinweis:**
>
> Wenn die CRL-Prüfung auf obligatorisch gesetzt ist, wenn das CA-Zertifikat an den virtuellen Server gebunden ist und die erste CRL-Aktualisierung fehlschlägt, wird die folgende Aktion für Verbindungen ergriffen:
>
> Alle Client-Authentifizierungsverbindungen mit demselben Aussteller wie die CRL werden als WIDERRUFEN zurückgewiesen, bis die CRL erfolgreich aktualisiert wurde.

Sie können das Intervall angeben, in dem die CRL-Aktualisierung durchgeführt werden muss. Sie können auch die genaue Uhrzeit angeben.

Synchronisieren Sie die automatische Aktualisierung von CRL mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set ssl crl <crlName> [-interval <interval>] [-day <integer>] [-time <
    HH:MM>]
<!--NeedCopy-->
```

Beispiel:

```
set ssl crl CRL-1 -refresh ENABLE -interval MONTHLY -days 10 -time
    12:00
<!--NeedCopy-->
```

Synchronisieren Sie die CRL-Aktualisierung mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL > CRL.**
2. Öffnen Sie eine CRL, wählen Sie **CRL Auto Refresh aktivieren**aus und geben Sie das Intervall an.

Führen Sie die Client-Authentifizierung mithilfe einer Zertifikatssperrliste durch

Wenn auf einer NetScaler-Appliance eine Zertifikatssperrliste (CRL) vorhanden ist, wird eine CRL-Prüfung durchgeführt, unabhängig davon, ob die Durchführung der CRL-Prüfung auf obligatorisch oder optional gesetzt ist.

Der Erfolg oder Misserfolg eines Handschlags hängt von einer Kombination der folgenden Faktoren ab:

- Regel für die CRL-Prüfung

- Regel für die Überprüfung von Client-Zertifikaten
- Status der für das CA-Zertifikat konfigurierten CRL

In der folgenden Tabelle sind die Ergebnisse der möglichen Kombinationen für einen Handshake mit einem gesperrten Zertifikat aufgeführt.

Tabelle 1. Ergebnis eines Handshakes mit einem Client, der ein gesperrtes Zertifikat verwendet

Regel für den CRL-Check	Regel für die Überprüfung von Client-Zertifikaten	Status der für das CA-Zertifikat konfigurierten CRL	Ergebnis eines Handshakes mit einem gesperrten Zertifikat
Optional	Optional	Fehlt	Erfolg
Optional	Erforderlich	Fehlt	Erfolg
Optional	Erforderlich	Gegenwart	Misserfolg
Erforderlich	Optional	Fehlt	Erfolg
Erforderlich	Erforderlich	Fehlt	Misserfolg
Erforderlich	Optional	Gegenwart	Erfolg
Erforderlich	Erforderlich	Gegenwart	Misserfolg
Optional/Obligatorisch	Optional	Abgelaufen	Erfolg
Optional/Obligatorisch	Erforderlich	Abgelaufen	Misserfolg

Hinweis:

- Die CRL-Prüfung ist standardmäßig optional. Um von optional zu obligatorisch oder umgekehrt zu wechseln, müssen Sie das Zertifikat zuerst vom virtuellen SSL-Server trennen und es dann erneut binden, nachdem Sie die Option geändert haben.
- In der Ausgabe des `sh ssl vserver` Befehls bedeutet OCSP-Check: optional, dass eine CRL-Prüfung ebenfalls optional ist. Die CRL-Prüfeinstellungen werden in der `sh ssl vserver` Befehlsausgabe nur angezeigt, wenn die CRL-Prüfung auf obligatorisch gesetzt ist. Wenn die CRL-Prüfung auf optional gesetzt ist, werden die CRL-Prüfdetails nicht angezeigt.

So konfigurieren Sie die CRL-Prüfung mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind ssl vserver <vServerName> -certkeyName <string> [(-CA -crlCheck (
    Mandatory | Optional ))]
```



```
sh ssl vserver
<!--NeedCopy-->
```

Beispiel:

```
bind ssl vs v1 -certkeyName ca -CA -crlCheck mandatory
> sh ssl vs v1

Advanced SSL configuration for VServer v1:

DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1
    .2: ENABLED
Push Encryption Trigger: Always
Send Close-Notify: YES

ECC Curve: P_256, P_384, P_224, P_521

1) CertKey Name: ca CA Certificate CRLCheck: Mandatory CA_Name Sent

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Konfigurieren Sie die CRL-Prüfung mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen SSL-Server.
2. Klicken Sie in den Bereich **Zertifikate** .

3. Wählen Sie ein Zertifikat aus und wählen Sie in der **OCSP- und CRL-Checkliste die Option**CRL**Mandatory aus.

Ergebnis eines Handshakes mit einem gesperrten oder gültigen Zertifikat

Regel für die CRL-Prüfung	Regel für die Überprüfung von Client-Zertifikaten	Status der für das CA-Zertifikat konfigurierten CRL	Ergebnis eines Handschlags mit einem gesperrten Zertifikat	Ergebnis eines Handshakes mit einem gültigen Zertifikat
Erforderlich	Erforderlich	Gegenwart	Misserfolg	Erfolg
Erforderlich	Erforderlich	Abgelaufen	Misserfolg	Misserfolg
Erforderlich	Erforderlich	Fehlt	Misserfolg	Misserfolg
Erforderlich	Erforderlich	Undefiniert	Misserfolg	Misserfolg
Optional	Erforderlich	Gegenwart	Misserfolg	Erfolg
Optional	Erforderlich	Abgelaufen	Erfolg	Erfolg
Optional	Erforderlich	Fehlt	Erfolg	Erfolg
Optional	Erforderlich	Undefiniert	Erfolg	Erfolg
Erforderlich	Optional	Gegenwart	Erfolg	Erfolg
Erforderlich	Optional	Abgelaufen	Erfolg	Erfolg
Erforderlich	Optional	Fehlt	Erfolg	Erfolg
Erforderlich	Optional	Undefiniert	Erfolg	Erfolg
Optional	Optional	Gegenwart	Erfolg	Erfolg
Optional	Optional	Abgelaufen	Erfolg	Erfolg
Optional	Optional	Fehlt	Erfolg	Erfolg
Optional	Optional	Undefiniert	Erfolg	Erfolg

Zertifikatsstatus mit OCSP überwachen

August 15, 2023

Online Certificate Status Protocol (OCSP) ist ein Internetprotokoll, das verwendet wird, um den Status eines Client-SSL-Zertifikats zu ermitteln. NetScaler-Appliances unterstützen OCSP gemäß der Defini-

tion in RFC 2560. OCSP bietet erhebliche Vorteile gegenüber Zertifikatsperrlisten (CRLs) in Bezug auf zeitnahe Informationen. Der aktuelle Widerrufsstatus eines Kundenzertifikats ist besonders nützlich bei Transaktionen mit hohen Geldsummen und hochwertigen Aktiengeschäften. Es verbraucht auch weniger System- und Netzwerkressourcen. Die NetScaler-Implementierung von OCSP umfasst das Batching von Anfragen und das Zwischenspeichern von Antworten.

OCSP-Implementierung

Die OCSP-Validierung auf einer NetScaler-Appliance beginnt, wenn die Appliance während eines SSL-Handshakes ein Client-Zertifikat erhält. Um das Zertifikat zu validieren, erstellt die Appliance eine OCSP-Anforderung und leitet sie an den OCSP-Responder weiter. Dazu verwendet die Appliance eine lokal konfigurierte URL. Die Transaktion befindet sich in einem unterbrochenen Zustand, bis die Appliance die Antwort des Servers auswertet und festlegt, ob die Transaktion zugelassen oder abgelehnt werden soll. Wenn die Antwort des Servers über die konfigurierte Zeit hinaus verzögert wird und keine anderen Responder konfiguriert sind, lässt die Appliance die Transaktion zu oder zeigt einen Fehler an, je nachdem, ob die OCSP-Prüfung auf optional bzw. obligatorisch gesetzt wurde.

Die Appliance unterstützt das Batching von OCSP-Anfragen und das Zwischenspeichern von OCSP-Antworten, um die Belastung des OCSP-Responders zu reduzieren und schnellere Antworten bereitzustellen.

OCSP-Anforderungs-Batching

Jedes Mal, wenn die Appliance ein Client-Zertifikat erhält, sendet sie eine Anfrage an den OCSP-Responder. Um eine Überlastung des OCSP-Responders zu vermeiden, kann die Appliance den Status von mehr als einem Client-Zertifikat in derselben Anfrage abfragen. Damit diese Funktion effizient funktioniert, muss ein Timeout definiert werden, damit die Verarbeitung eines einzelnen Zertifikats nicht übermäßig verzögert wird, während auf die Erstellung eines Batches gewartet wird.

OCSP-Antwort-Caching

Das Zwischenspeichern der vom OCSP-Responder empfangenen Antworten ermöglicht schnellere Antworten an die Clients und reduziert die Belastung des OCSP-Responders. Nach Erhalt des Sperrstatus eines Client-Zertifikats vom OCSP-Responder speichert die Appliance die Antwort lokal für einen vordefinierten Zeitraum. Wenn während eines SSL-Handshakes ein Client-Zertifikat empfangen wird, überprüft die Appliance zunächst ihren lokalen Cache auf einen Eintrag für dieses Zertifikat. Wenn ein Eintrag gefunden wird, der noch gültig ist (innerhalb des Cache-Timeout-Limits), wird er ausgewertet und das Client-Zertifikat wird akzeptiert oder abgelehnt. Wenn kein Zertifikat gefunden wird, sendet die Appliance eine Anfrage an den OCSP-Responder und speichert die Antwort für einen konfigurierten Zeitraum in ihrem lokalen Cache.

> **Hinweis**: Das Cache-Timeout-Limit kann auf maximal 43200 Minuten (30 Tage) festgelegt werden. In Version 12.1 Build 49.x und früher lag das Limit bei 1440 Minuten (ein Tag). Das erhöhte Limit trägt dazu bei, die Suchvorgänge auf dem OCSP-Server zu reduzieren und SSL/TLS-Verbindungsfehler zu vermeiden, falls der OCSP-Server aufgrund von Netzwerk- oder anderen Problemen nicht erreichbar ist.

OCSP-Responderkonfiguration

Die Konfiguration von OCSP umfasst das Hinzufügen eines OCSP-Responders, das Binden des OCSP-Responders an ein Zertifikat der Zertifizierungsstelle (CA) und das Binden des Zertifikats an einen virtuellen SSL-Server. Wenn Sie ein anderes Zertifikat an einen OCSP-Responder binden müssen, der bereits konfiguriert wurde, müssen Sie zuerst die Bindung des Responders aufheben und dann den Responder an ein anderes Zertifikat binden.

Fügen Sie mithilfe der CLI einen OCSP-Responder hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um OCSP zu konfigurieren und die Konfiguration zu überprüfen:

```
add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [ -batchingDepth <
    positive_integer>][-batchingDelay <positive_integer>] [-resptimeout
    <positive_integer>] [-responderCert <string> | -trustResponder] [-
    producedAtTimeSkew <positive_integer>][-signingCert <string>][-
    useNonce ( YES | NO )][ -insertClientCert( YES | NO )]
<!--NeedCopy-->
```

```
bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]
<!--NeedCopy-->
```

```
bind ssl vserver <vServerName>@ (-certkeyName <string> ( CA [-ocspCheck
     ( Mandatory | Optional )]))
<!--NeedCopy-->
```

```
show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Beispiel:


```
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/
    ocsp/" -cache ENABLED -cacheTimeout 30 -batchingDepth 8 -
    batchingDelay 100 -resptimeout 100 -responderCert responder_cert -
    producedAtTimeSkew 300 -signingCert sign_cert  -insertClientCert YES
<!--NeedCopy-->
```

```
bind ssl certKey ca_cert -ocspResponder ocsp_responder1 -priority 1
<!--NeedCopy-->
```

```
bind ssl vserver vs1 -certkeyName ca_cert -CA -ocspCheck Mandatory
<!--NeedCopy-->
```

```
sh ocspResponder ocsp_responder1

    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done
<!--NeedCopy-->
```

```
show certkey ca_cert

    Name: ca_cert     Status: Valid,   Days to expiration:8907
    Version: 3
    …

    1)  VServer name: vs1      CA Certificate
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
Done
<!--NeedCopy-->
```

```
sh ssl vs vs1

    Advanced SSL configuration for VServer vs1:
    DH: DISABLED
    …
```



```
6
7       1) CertKey Name: ca_cert CA Certificate OCSPCheck: Mandatory
8       1) Cipher Name: DEFAULT
9         Description: Predefined Cipher Alias
10      Done
11  <!--NeedCopy-->
```

Ändern Sie einen OCSP-Responder mithilfe der CLI

Sie können den Namen des Responders nicht ändern. Alle anderen Parameter können mit dem `set ssl ocspResponder` Befehl geändert werden.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
1  set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
       ] [-cacheTimeout <positive_integer>] [-batchingDepth <
       positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout
        <positive_integer>] [ -responderCert <string> | -trustResponder][-
       producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
       useNonce ( YES | NO )]
2
3  unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]
4
5  bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
       positive_integer>]
6
7  show ssl ocspResponder [<name>]
8  <!--NeedCopy-->
```

Konfigurieren Sie einen OCSP-Responder mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **OCSP-Responder**, und konfigurieren Sie einen OCSP-Responder.
2. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate**, wählen Sie ein Zertifikat aus, und wählen Sie in der Liste **Aktion** die Option **OCSP-Bindungen**aus. Binden Sie einen OCSP-Responder.
3. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, öffnen Sie einen virtuellen Server, und klicken Sie im Abschnitt Zertifikate auf, um ein CA-Zertifikat zu binden.
4. **Wählen Sie optional OCSP Mandatory**aus.

OCSP-Stapling

August 15, 2023

Die NetScaler-Implementierung von CRL und OCSP meldet nur den Sperrstatus von Clientzertifikaten. Um den Sperrstatus eines Serverzertifikats zu überprüfen, das während eines SSL-Handshakes empfangen wurde, muss ein Client eine Anforderung an eine Zertifizierungsstelle senden.

Bei Websites mit hohem Datenverkehr erhalten viele Clients dasselbe Serverzertifikat. Wenn jeder Client eine Anfrage nach dem Sperrstatus des Serverzertifikats senden würde, würde die Zertifizierungsstelle mit OCSP-Anfragen überschwemmt, um die Gültigkeit des Zertifikats zu überprüfen.

OCSP-Staplinglösung

Um unnötige Überlastung zu vermeiden, unterstützt die NetScaler Appliance jetzt OCSP-Stapling. Das heißt, zum Zeitpunkt des SSL-Handshakes kann die Appliance jetzt den Status eines Serverzertifikats an einen Client senden, nachdem die Antwort von einem OCSP-Responder überprüft wurde. Der Status eines Serverzertifikats wird an das Zertifikat "angeheftet", das die Appliance im Rahmen des SSL-Handshakes an den Client sendet. Um die OCSP-Staplingfunktion verwenden zu können, müssen Sie sie auf einem virtuellen SSL-Server aktivieren und der Appliance einen OCSP-Responder hinzufügen.

> Hinweise
>
> - Alle Zwischenzertifikate enthalten die OCSP-Antworterweiterung, wenn die folgenden Bedingungen erfüllt sind:
>
>   – TLS 1.3 protocol is used
>   – Client sends a status request
>
>   Bisher enthielt nur das Serverzertifikat diese Erweiterung in die Antwort auf die Statusanforderung des Clients.
> - Bei den anderen Protokollen (einschließlich TLS 1.2) sendet der Server die OCSP-Antwort nur für das Serverzertifikat. Das heißt, RFC 6961 wird mit dem TLS 1.2-Protokoll nicht unterstützt.
> - NetScaler Appliances unterstützen OCSP-Stapling, wie in RFC 6066 definiert.
> - OCSP-Stapling wird nur im Front-End von NetScaler Appliances unterstützt.
> - Die ADC-Appliance verhält sich bei Verwendung des TLS 1.3-Protokolls wie folgt: Wenn die zwischengespeicherte OCSP-Antwort ungültig (leer oder abgelaufen) ist, wird eine Anforderung an den OCSP-Responder gesendet, der SSL-Handshake wird jedoch abgeschlossen, ohne auf die Antwort zu warten. Wenn die Antwort empfangen wird, wird sie zwischengespeichert und steht für zukünftige Statusanfragen von Clients zur

> Verfügung.
>
> - Die NetScaler-Unterstützung für OCSP-Stapling ist auf Handshakes mit TLS-Protokollversion 1.0 oder höher beschränkt.

OCSP-Antwort-Caching von Serverzertifikaten

> Hinweis
>
> Wenn das TLS 1.3-Protokoll verwendet wird, wird die OCSP-Antwort für das Serverzertifikat und alle Zwischenzertifikate zwischengespeichert.

Wenn ein Client während des SSL-Handshakes den Sperrstatus des Serverzertifikats anfordert, überprüft die Appliance zunächst ihren lokalen Cache auf einen Eintrag für dieses Zertifikat. Wenn ein gültiger Eintrag gefunden wird, wird dieser ausgewertet und das Serverzertifikat und sein Status werden dem Client angezeigt. Wenn kein Sperrstatuseintrag gefunden wird, sendet die Appliance eine Anforderung für den Sperrstatus des Serverzertifikats an den OCSP-Responder. Wenn es eine Antwort erhält, sendet es das Zertifikat und den Sperrstatus an den Client. Wenn das nächste Aktualisierungsfeld in der OCSP-Antwort vorhanden ist, wird die Antwort für die konfigurierte Zeitdauer zwischengespeichert (Wert wird im Timeout-Feld angegeben).

> **Hinweis**: Sie können die zwischengespeicherte Antwort des Serverzertifikats vom OCSP-Responder löschen, noch bevor das Timeout abläuft. In Version 12.1 Build 49.x und früher war es nicht möglich, den zwischengespeicherten Status im Zertifikatsschlüsselpaar zu verwerfen, bis das konfigurierte Timeout abgelaufen war.

Um den zwischengespeicherten Status über die CLI zu löschen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
clear ssl certKey <certkey name> -ocspstaplingCache
<!--NeedCopy-->
```

Beispiel:

```
clear ssl certKey s1 -ocspstaplingCache
<!--NeedCopy-->
```

So löschen Sie den zwischengespeicherten Status über die GUI

1. Navigieren Sie in der GUI zu **Traffic Management** > **SSL** > **Zertifikate** > **CA-Zertifikate**.
2. Wählen Sie im Detailbereich ein Zertifikat aus.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Löschen**. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Ja**.

OCSP-Staplingkonfiguration

Die Konfiguration des OCSP-Staplings umfasst die Aktivierung der Funktion und die Konfiguration von OCSP. Um OCSP zu konfigurieren, müssen Sie einen OCSP-Responder hinzufügen, den OCSP-Responder an ein CA-Zertifikat binden und das Zertifikat an einen virtuellen SSL-Server binden.

> **Hinweis:**
>
> OCSP-Responder mit nur einer HTTP-basierten URL werden unterstützt.

OCSP-Stapling über die CLI aktivieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <name> -ocspstapling [ENABLED | DISABLED]
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vip1 -ocspStapling ENABLED
Done

sh ssl vserver vip1

     Advanced SSL configuration for VServer vip1:
     DH: DISABLED
     DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA:
        ENABLED Refresh Count: 0
     Session Reuse: ENABLED Timeout: 120 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     ClearText Port: 0
     Client Auth: DISABLED
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: ENABLED
     OCSP Stapling: ENABLED
     SSLv2: DISABLED SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED
          TLSv1.2: ENABLED
     Push Encryption Trigger: Always
     Send Close-Notify: YES

     ECC Curve: P_256, P_384, P_224, P_521

    1) CertKey Name: server_certificate1 Server Certificate

```



```
26      1) Cipher Name: DEFAULT
27       Description: Default cipher list with encryption strength >= 128
            bit
28  Done
29  <!--NeedCopy-->
```

Hinweis: Wenn das Standardprofil (erweitert) aktiviert ist, verwenden Sie den Befehl `set ssl profile <profile name> -ocspStapling [ENABLED | DISABLED]`, um OCSP zu aktivieren oder zu deaktivieren.

OCSP-Stapling über die GUI aktivieren

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Virtueller Server**.
2. Öffnen Sie einen virtuellen Server, und wählen Sie **unter SSL-Parameter**die Option **OCSP Stapling**aus.

OCSP-Konfiguration

Ein OCSP-Responder wird dynamisch oder manuell hinzugefügt, um OCSP-Stapling-Anforderungen zu senden. Ein interner Responder wird dynamisch hinzugefügt, wenn Sie ein Serverzertifikat und dessen Ausstellerzertifikat basierend auf der OCSP-URL im Serverzertifikat hinzufügen. Ein manueller OCSP-Responder wird über die CLI oder GUI hinzugefügt. Um eine OCSP-Anforderung für ein Serverzertifikat zu senden, wählt die NetScaler Appliance einen OCSP-Responder basierend auf der Priorität aus, die ihm beim Binden an ein Ausstellerzertifikat zugewiesen wurde. Wenn ein Responder eine OCSP-Stapling-Anforderung nicht sendet, wird der Responder mit der nächsthöheren Priorität zum Senden der Anforderung ausgewählt. Wenn beispielsweise nur ein Responder manuell konfiguriert wird und dieser fehlschlägt und ein dynamisch gebundener Responder vorhanden ist, wird er zum Senden der OCSP-Anforderung ausgewählt.

Wenn die OCSP-URL nicht HTTP ist, wird kein interner OCSP-Responder erstellt.

> **Hinweis**
>
> Ein manuell hinzugefügter OCSP-Responder hat Vorrang vor einem dynamisch hinzugefügten Responder.

Unterschied zwischen einem manuell erstellten OCSP-Responder und einem intern erstellten OCSP-Responder

Manuell erstellter OCSP-Responder	Intern (dynamisch) erstellter OCSP-Responder
Manuell erstellt und explizit an das Ausstellerzertifikat mit einer Priorität gebunden.	Wird standardmäßig erstellt und gebunden, während ein Serverzertifikat und sein Ausstellerzertifikat (CA-Zertifikat) hinzugefügt werden. Der Name beginnt mit “ns_internal_”.
Eine Priorität zwischen 1 und 127 ist für einen konfigurierten Responder reserviert.	Die Priorität wird ab 128 automatisch zugewiesen.
URL und Batch-Tiefe können geändert werden.	URL und Batch-Tiefe können nicht geändert werden.
Direkt gelöscht.	Wird nur gelöscht, wenn Sie das Serverzertifikat oder das CA-Zertifikat löschen.
Kann an jedes CA-Zertifikat gebunden werden.	Standardmäßig an ein CA-Zertifikat gebunden. Kann nicht an ein anderes CA-Zertifikat gebunden werden.
In der Konfiguration gespeichert (ns.conf).	Befehle zum Hinzufügen werden nicht in der Konfiguration gespeichert. Nur eingestellte Befehle werden gespeichert.
Wenn Sie drei OCSP-Responder mit den Prioritäten 1, 2 und 3 an dasselbe Ausstellerzertifikat binden und später Priorität 2 aufheben, sind die anderen Prioritäten nicht betroffen.	Drei OCSP-Responder sind automatisch an ein Ausstellerzertifikat mit den Prioritäten 128, 129 bzw. 130 gebunden. Wenn Sie das Serverzertifikat entfernen, das zum Erstellen einer Antwortbindung mit Priorität 129 verwendet wurde, wird dieser Responder gelöscht. Außerdem wird die Priorität für den nächsten Responder (Priorität 130) automatisch auf 129 geändert.

Beispiel für die Bearbeitung von Anfragen:

1. Fügen Sie einen virtuellen Server (VIP1) hinzu.
2. Fügen Sie das Ausstellerzertifikat (CA1) hinzu und binden Sie es an VIP1.
3. Fügen Sie drei Zertifikate S1, S2 und S3 hinzu. Die internen Responder resp1, resp2 und resp3 werden standardmäßig erstellt.
4. Binden Sie S3 an VIP1.
5. Eine Anfrage geht an VIP1. Responder resp3 ist ausgewählt.

Um einen internen OCSP-Responder dynamisch zu erstellen, benötigt die Appliance Folgendes:

- Zertifikat des Ausstellers des Serverzertifikats (normalerweise das CA-Zertifikat).
- Zertifikatschlüsselpaar des Serverzertifikats. Dieses Zertifikat muss die von der Zertifizierungsstelle angegebene OCSP-URL enthalten. Die URL wird als Name des dynamisch hinzugefügten internen Responders verwendet.

Ein interner OCSP-Responder hat dieselben Standardwerte wie ein manuell konfigurierter Responder.

> **Hinweis:**
>
> Das Caching ist bei einem internen Responder standardmäßig deaktiviert. Verwenden Sie den Befehl `set ssl ocspResponder`, um das Caching zu aktivieren.

Konfigurieren Sie OCSP mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um OCSP zu konfigurieren und die Konfiguration zu überprüfen:

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
    [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]] [-bundle ( YES | NO )]

add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [-resptimeout <positive_integer
    >] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew
    <positive_integer>][-signingCert <string>][-useNonce ( YES | NO )][
    -insertClientCert ( YES | NO )]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Die Parameter:

httpMethod:

HTTP-Methode zum Senden von OCSP-Anfragen. Für Anforderungen mit einer Länge von weniger als 255 Byte können Sie die HTTP GET-Methode für Abfragen an einen OCSP-Server konfigurieren. Wenn Sie die GET-Methode angeben, die Länge jedoch größer als 255 Byte ist, verwendet die Appliance die Standardmethode (POST).

Mögliche Werte: GET, POST

Standardwert: POST

ocspUrlResolveTimeout:

Zeit in Millisekunden, um auf eine OCSP-URL-Auflösung zu warten. Nach Ablauf dieser Zeit wird der Responder mit der nächsthöheren Priorität ausgewählt. Wenn alle Responder fehlschlagen, wird abhängig von den Einstellungen auf dem virtuellen Server eine Fehlermeldung angezeigt oder die Verbindung wird unterbrochen.

Minimaler Wert: 100

Maximaler Wert: 2000

Beispiel:

```
add ssl certkey root_ca1  - cert root_cacert.pem
add ssl ocspResponder ocsp_responder1 -url "http:// www.myCA.org:80/
    ocsp/" -cache ENABLED -cacheTimeout 30  -resptimeout 100 -
    responderCert responder_cert -producedAtTimeSkew 300 -signingCert
    sign_cert  -insertClientCert YES
bind ssl certKey root_ca1 -ocspResponder ocsp_responder1 -priority 1
sh ocspResponder ocsp_responder1
    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done

show certkey root_ca1
    Name: root_ca1     Status: Valid,   Days to expiration:8907
    Version: 3
    …
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
    Done
<!--NeedCopy-->
```

Ändern Sie OCSP über die CLI

Sie können den Namen eines OCSP-Responders nicht ändern, aber Sie können den Befehl `set ssl ocspResponder` verwenden, um einen der anderen Parameter zu ändern.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>]  [-resptimeout <
    positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]

unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Konfigurieren Sie OCSP über die GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **OCSP-Responder**, und konfigurieren Sie einen OCSP-Responder.
2. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate**, wählen Sie ein Zertifikat aus, und wählen Sie in der Liste **Aktion** die Option **OCSP-Bindungen**aus. **Binden Sie einen OCSP-Responder**.
3. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, öffnen Sie einen virtuellen Server, und klicken Sie im Abschnitt Zertifikate auf, um ein CA-Zertifikat zu binden.
4. Wählen Sie optional **OCSP Mandatory**aus.

> **Hinweis:**
>
> Der Parameter insert client certificate in den Befehlen `add ssl ocspResponder` und `set ssl ocspResponder`ist nicht mehr gültig. Das heißt, der Parameter wird während der Konfiguration ignoriert.

Verfügbare Verschlüsselungen auf NetScaler-Appliances

August 15, 2023

Ihre NetScaler-Appliance wird mit einem vordefinierten Satz von Verschlüsselungsgruppen geliefert. Um Verschlüsselungen zu verwenden, die nicht Teil der DEFAULT-Verschlüsselungsgruppe sind, müssen Sie sie explizit an einen virtuellen SSL-Server binden. Sie können auch eine be-

nutzerdefinierte Verschlüsselungsgruppe erstellen, die an den virtuellen SSL-Server gebunden werden soll. Weitere Informationen zum Erstellen einer benutzerdefinierten Chiffriergruppe finden Sie unter Konfigurieren benutzerdefinierter Chiffriergruppen auf der ADC-Appliance.

Hinweise

- Ab Release 13.0 Build 71.x und höher wird die Hardwarebeschleunigung TLS1.3 auf den folgenden Plattformen unterstützt:
  - MPX 5900
  - MPX/SDX 8900
  - MPX/SDX 9100
  - MPX/SDX 15000
  - MPX/SDX 15000-50G
  - MPX/SDX 16000
  - MPX/SDX 26000
  - MPX/SDX 26000-50S
  - MPX/SDX 26000-100G

  - Nur-Software-Unterstützung für das TLSv1.3-Protokoll ist auf allen anderen NetScaler MPX- und SDX-Appliances mit Ausnahme von NetScaler FIPS-Appliances verfügbar.
- TLSv1.3 wird nur mit dem erweiterten Profil unterstützt. Informationen zum Aktivieren des erweiterten Profils finden Sie unter Aktivieren des erweiterten Profils.
- Um TLS1.3 zu verwenden, müssen Sie einen Client verwenden, der der RFC 8446-Spezifikation entspricht.
- Die RC4-Verschlüsselung ist nicht in der Standard-Verschlüsselungsgruppe der NetScaler-Appliance enthalten. Es wird jedoch in der Software auf den N3-basierten Appliances unterstützt. Die RC4-Verschlüsselung, einschließlich des Handshakes, erfolgt in Software.
- Citrix empfiehlt, diese Verschlüsselung nicht zu verwenden, da sie von RFC 7465 als unsicher und veraltet eingestuft wird.
- Verwenden Sie den Befehl “Hardware anzeigen”, um festzustellen, ob Ihr Gerät über N3-Chips verfügt.

```
sh hardware

Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100

Manufactured on: 8/19/2013

CPU: 2900MHZ

```



```
Host Id: 1006665862

Serial no: ENUK6298FT

Encoded serial no: ENUK6298FT
<!--NeedCopy-->
```

- Um Informationen zu den Verschlüsselungssammlungen anzuzeigen, die standardmäßig am Front-End (an einen virtuellen Server) gebunden sind, geben Sie Folgendes ein: `sh cipher DEFAULT`
- Um Informationen zu den Verschlüsselungssammlungen anzuzeigen, die standardmäßig am Back-End (an einen Dienst) gebunden sind, geben Sie Folgendes ein: `sh cipher DEFAULT_BACKEND`
- Um Informationen zu allen auf der Appliance definierten Verschlüsselungsgruppen (Aliase) anzuzeigen, geben Sie Folgendes ein: `sh cipher`
- Um Informationen zu allen Verschlüsselungssammlungen anzuzeigen, die Teil einer bestimmten Verschlüsselungsgruppe sind, geben Sie Folgendes ein: `sh cipher <alias name>`. Zum Beispiel sh chiffre ECDHE.

Unter den folgenden Links sind die Cipher Suites aufgeführt, die auf verschiedenen NetScaler-Plattformen und auf externen Hardware-Sicherheitsmodulen (HSMs) unterstützt werden:

- **NetScaler MPX/SDX Intel Lewisburg Appliance**: Verschlüsselungsunterstützung auf einer NetScaler MPX/SDX Intel Lewisburg SSL-Chip-basierten Appliance
- **NetScaler MPX/SDX (N3) -Appliance**: Verschlüsselungsunterstützung auf einer NetScaler MPX/SDX (N3) -Appliance
- **NetScaler MPX/SDX Intel Coleto Appliance**: Verschlüsselungsunterstützung auf einer NetScaler MPX/SDX Intel Coleto SSL-Chip-basierten Appliance
- **NetScaler VPX-Appliance**: Verschlüsselungsunterstützung auf einer NetScalerVPX-Appliance
- **NetScaler MPX/SDX 14000 FIPS-Appliance**: Verschlüsselungsunterstützung auf einer NetScaler MPX/SDX 14000 FIPS-Appliance
- **Externes HSM (Thales/Safenet)**: Chiffre wird auf einem externen HSM unterstützt (Thales/Safenet)
- **NetScaler VPX FIPS- und MPX FIPS-Appliances: Verschlüsselungsunterstützung auf NetScalerVPX FIPS- und MPX FIPS-Appliances**

> **Hinweis:**
>
> Informationen zur DTLS-Verschlüsselungsunterstützung finden Sie unter DTLS-Verschlüsselungsunterstützung auf NetScalerVPX-, MPX- und SDX-Appliances.

Tabelle1 - Unterstützung für virtuellen Server/Frontend-Service/interner Service:

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.3	Nicht verfügbar	14.1 alle Builds	14.1 alle Builds	Nicht unterstützt	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	Nicht unterstützt	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	Nicht unterstützt	13.0 alle Builds
	12.1—50.x (außer TLS1.3-CHACHA20-POLY1305-SHA256)	12.1—50.x (außer TLS1.3-CHACHA20-POLY1305-SHA256)	12.1–50.x	Nicht unterstützt	12.1–50.x
TLS 1.1/1.2	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
ECDHE/DHE (Beispiel TLS1-ECDHE-RSA-AES128-SHA)	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
AES-GCM (Beispiel TLS1.2-AES128-GCM-SHA256)	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
SHA-2-Chiffren (Beispiel TLS1.2-AES-128-SHA256)	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
ECDSA (Beispiel TLS1-ECDHE-ECDSA-AES256-SHA)	Nicht unterstützt	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	Nicht unterstützt	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	Nicht unterstützt	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
CHACHA20	Nicht unterstützt	14.1 alle Builds	14.1 alle Builds	Nicht unterstützt	14.1 alle Builds
	Nicht unterstützt	13.1 alle Builds	13.1 alle Builds	Nicht unterstützt	13.1 alle Builds
	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	Nicht unterstützt	13.0 alle Builds
	Nicht unterstützt	Nicht unterstützt	12.1 alle Builds	Nicht unterstützt	12,1—49.x (nur auf MPX 5900/8900)

Tabelle 2 — Unterstützung von Backend-Diensten:

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.3	Nicht verfügbar	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
TLS 1.1/1.2	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
ECDHE/DHE (Beispiel TLS1-ECDHE-RSA-AES128-SHA)	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
AES-GCM (Beispiel TLS1.2-AES128-GCM-SHA256)	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
SHA-2-Chiffren (Beispiel TLS1.2-AES-128-SHA256)	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
ECDSA (Beispiel TLS1-ECDHE-ECDSA-AES256-SHA)	Nicht unterstützt	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds	14.1 alle Builds
	Nicht unterstützt	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds	13.1 alle Builds
	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	Nicht unterstützt	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
CHACHA20	Nicht unterstützt	14.1 alle Builds	14.1 alle Builds	Nicht unterstützt	14.1 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000 FIPS**	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	Nicht unterstützt	13.1 alle Builds	13.1 alle Builds	Nicht unterstützt	13.1 alle Builds
	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	Nicht unterstützt	13.0 alle Builds
	Nicht unterstützt	Nicht unterstützt	12.1 alle Builds	Nicht unterstützt	12,1—49,x für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100 G

Eine detaillierte Liste der unterstützten ECDSA-Chiffren finden Sie unter Unterstützung von ECDSA Cipher Suites.

Hinweise

- TLS-Fallback_SCSV Verschlüsselungssammlung wird auf allen Appliances ab Version 10.5 Build 57.x unterstütz
  t
- Die Unterstützung von HTTP Strict Transport Security (HSTS) ist richtlinienbasiert.
- Alle signierten SHA-2-Zertifikate (SHA256, SHA384, SHA512) werden auf dem Front-End aller Appliances unterstützt. In Version 11.1 Build 54.x und höher werden diese Zertifikate auch im Back-End aller Appliances unterstützt. In Version 11.0 und früher werden nur signierte SHA256-Zertifikate im Backend aller Appliances unterstützt.
- In Release 11.1 Build 52.x und früher werden die folgenden Chiffriergeräte nur am Frontend der MPX 9700 und MPX/SDX 14000 FIPS-Appliances unterstützt:
  - TLS1.2-ECDHE-RSA-AES-256-SHA384
  - TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 From release 11.1 build 53.x, and in release 12.0, these ciphers are also supported on the back end.

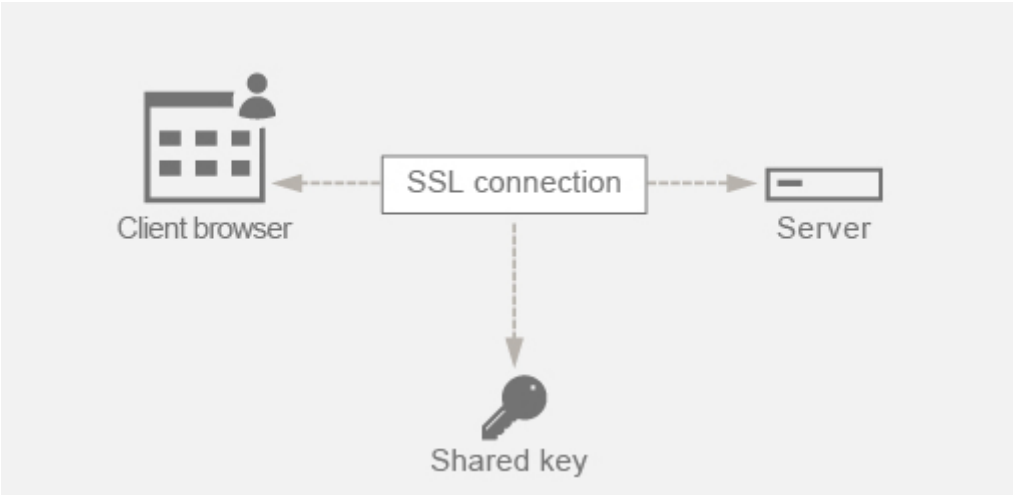
- Alle ChaCha20-Poly1035-Chiffren verwenden eine TLS-Pseudozufallsfunktion (PSF) mit der SHA-256-Hash-Funktion.

Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy gewährleistet den Schutz der aktuellen SSL-Kommunikation, auch wenn der Sitzungsschlüssel eines Webservers zu einem späteren Zeitpunkt kompromittiert wird.

Warum brauchen Sie Perfect Forward Secrecy (PFS)?

Eine SSL-Verbindung wird verwendet, um die Daten zu sichern, die zwischen einem Client und einem Server übergeben werden. Diese Verbindung beginnt mit dem SSL-Handshake, der zwischen dem Browser eines Clients und dem kontaktierten Webserver stattfindet. Während dieses Handshakes tauschen der Browser und der Server bestimmte Informationen aus, um auf einen Sitzungsschlüssel zu gelangen, der als Mittel zur Verschlüsselung der Daten während des restlichen Kommunikationsweges dient.

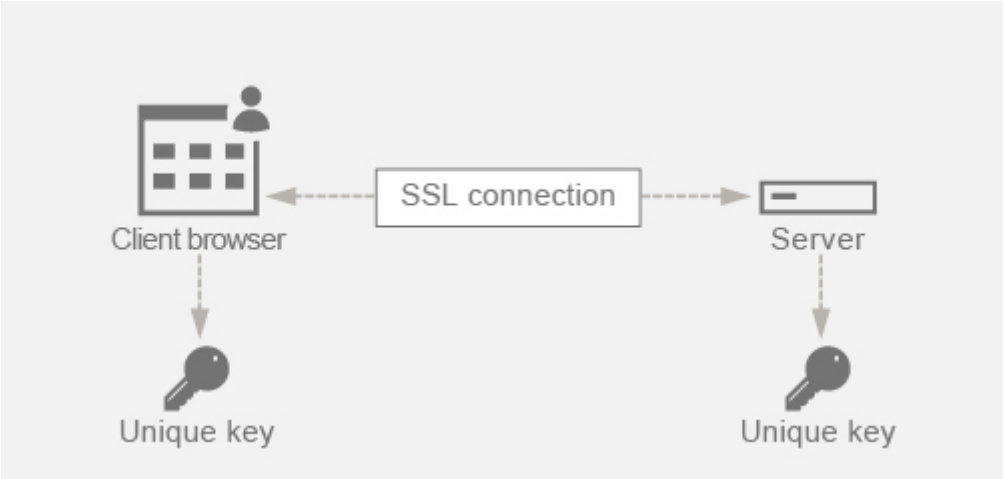


RSA ist der am häufigsten verwendete Algorithmus für den Schlüsselaustausch. Der Browser verwendet den öffentlichen Schlüssel des Servers, um das Pre-Master-Secret zu verschlüsseln und an einen Server zu senden. Dieses Pre-Master-Geheimnis wird verwendet, um zum Sitzungsschlüssel zu gelangen. Das Problem beim RSA-Schlüsselaustausch besteht darin, dass, wenn es einem Angreifer gelingt, den privaten Schlüssel des Servers zu irgendeinem Zeitpunkt in der Zukunft zu erhalten, der Angreifer das Pre-Master-Geheimnis erhält, mit dem der Sitzungsschlüssel abgerufen werden kann. Dieser Sitzungsschlüssel kann jetzt vom Angreifer verwendet werden, um alle SSL-Konversationen zu entschlüsseln. Infolgedessen ist Ihre bisherige SSL-Kommunikation, die zuvor sicher war, nicht mehr sicher, da der gestohlene private Schlüssel des Servers verwendet werden kann, um zum Sitzungsschlüssel zu gelangen und somit auch alle gespeicherten historischen Konversationen zu entschlüsseln.

Die bisherige SSL-Kommunikation muss geschützt werden können, auch wenn der private Schlüssel des Servers kompromittiert wurde. Die Konfiguration von Perfect Forward Secrecy (PFS) hilft bei der Behebung dieses Problems.

Wie hilft PFS?

PFS schützt die bisherige SSL-Kommunikation, indem der Client und der Server sich auf einen neuen Schlüssel für jede Sitzung einigen und die Berechnung dieses Sitzungsschlüssels geheim hält. Es funktioniert auf der Grundlage, dass ein Kompromiss eines Serverschlüssels nicht zu Kompromissen des Sitzungsschlüssels führen darf. Der Sitzungsschlüssel wird an beiden Enden separat abgeleitet und niemals über den Draht übertragen. Die Sitzungsschlüssel werden ebenfalls zerstört, sobald die Kommunikation abgeschlossen ist. Diese Fakten stellen sicher, dass jemand, der Zugriff auf den privaten Schlüssel des Servers erhält, nicht zum Sitzungsschlüssel gelangen kann. Daher könnten sie die vergangenen Daten nicht entschlüsseln.



Erklärung mit Beispiel

Angenommen, wir verwenden DHE, um PFS zu erreichen. Der DH-Algorithmus stellt sicher, dass ein Hacker zwar den privaten Schlüssel des Servers erhält, der Hacker jedoch nicht zum Sitzungsschlüssel gelangen kann. Der Grund dafür ist, dass der Sitzungsschlüssel und die Zufallszahlen (die zum Erreichen des Sitzungsschlüssels verwendet werden) an beiden Enden geheim gehalten werden und niemals über die Leitung ausgetauscht werden.
PFS kann durch Verwendung des ephemeren Diffie-Hellman-Schlüsselaustauschs erreicht werden, der für jede SSL-Sitzung neue temporäre Schlüssel erstellt.

Die Kehrseite beim Erstellen eines Schlüssels für jede Sitzung besteht darin, dass zusätzliche Berechnungen erforderlich sind. Dieses Problem kann jedoch überwunden werden, indem die elliptische Kurve mit kleineren Schlüsselgrößen verwendet wird.

PFS auf der NetScaler-Appliance konfigurieren

PFS kann auf einem NetScaler konfiguriert werden, indem DHE- oder ECDHE-Chiffren konfiguriert werden. Diese Chiffern stellen sicher, dass der erstellte geheime Sitzungsschlüssel nicht auf dem Draht (DH-Algorithmus) geteilt wird und dass der Sitzungsschlüssel nur für kurze Zeit am Leben bleibt (Vergänglich). Beide Konfigurationen werden in den folgenden Abschnitten erläutert.

Hinweis: Die Verwendung von ECDHE-Chiffern anstelle von DHE macht die Kommunikation bei kleineren Schlüsselgrößen sicherer.

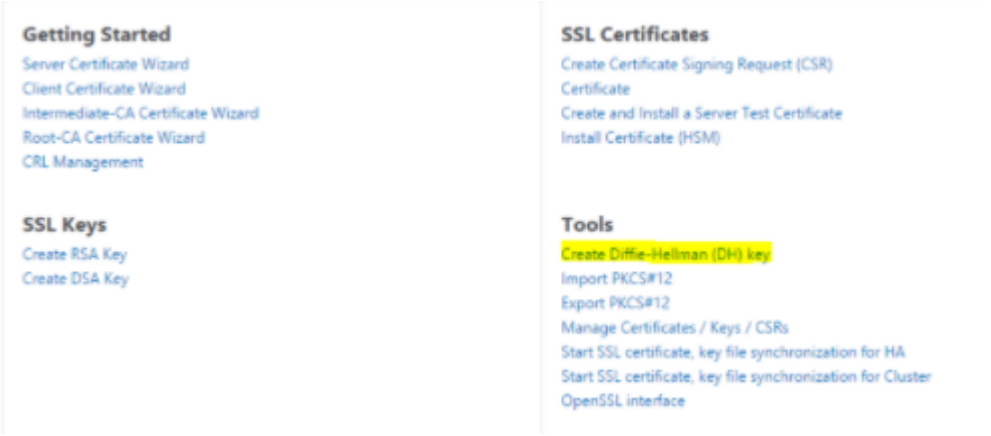
Konfigurieren Sie DHE mit der GUI

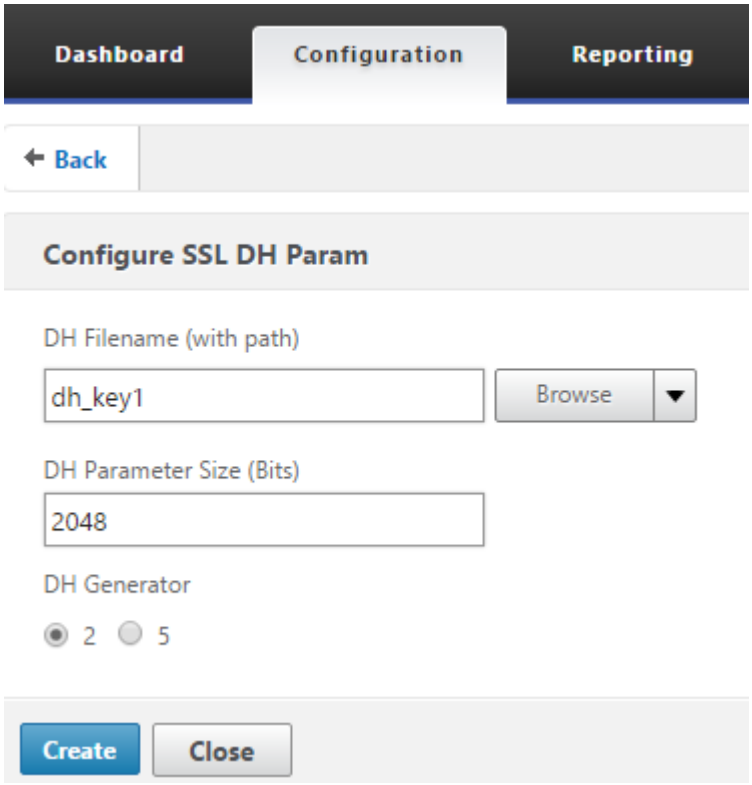
1. Generieren Sie einen DH-Schlüssel.

   a. Navigieren Sie zu **Traffic Management > SSL > Tools**.

   b. Klicken Sie auf **Diffie Helman (DH) Key erstellen**.

   Hinweis: Das Generieren eines 2048-Bit-DH-Schlüssels kann bis zu 30 Minuten dauern.



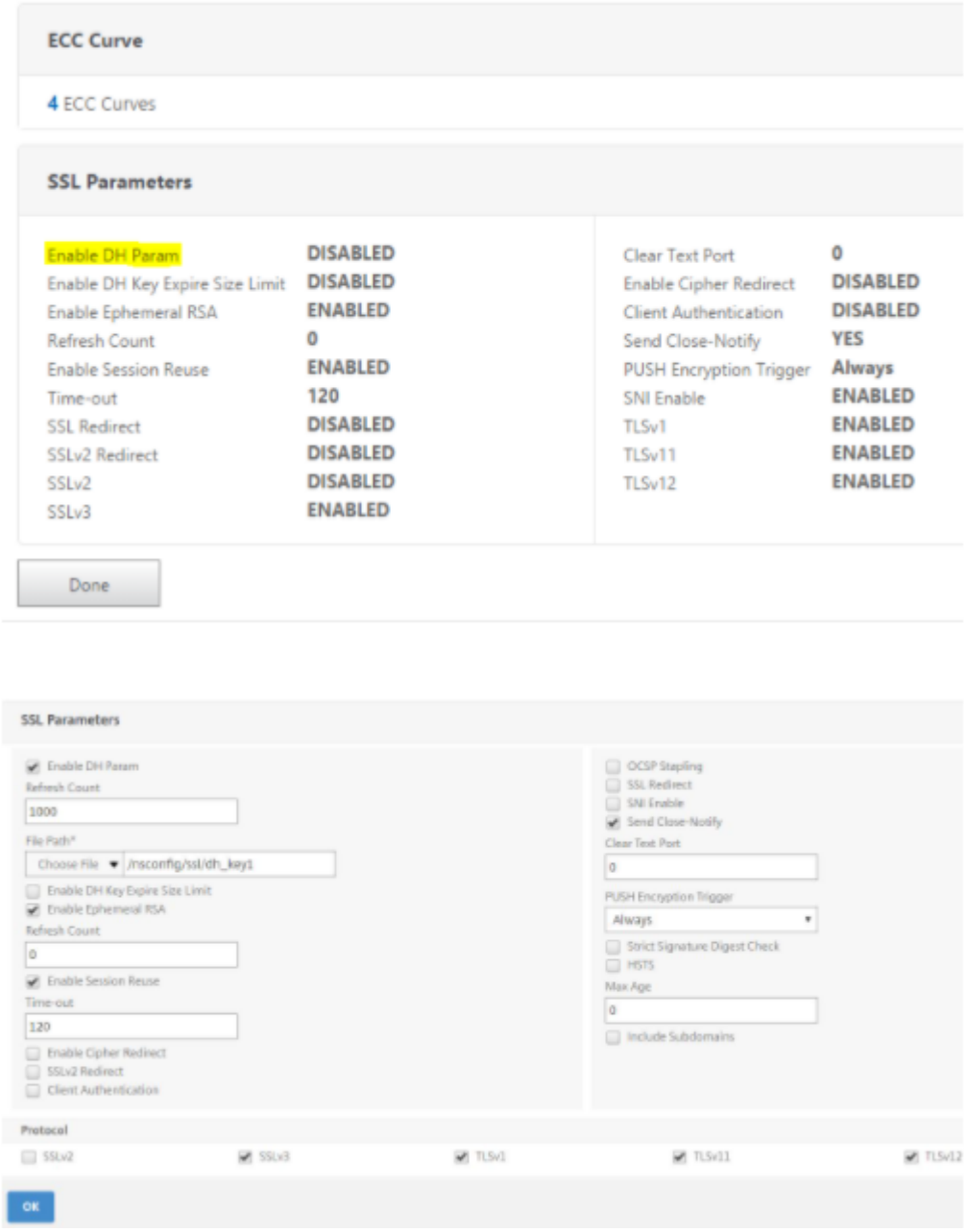


2. Aktivieren Sie DH Param für den virtuellen SSL-Server und fügen Sie den DH-Schlüssel an den virtuellen SSL-Server an.

   a. Navigieren Sie zu **Konfiguration > Traffic Management > Virtuelle Server**.

   b. Wählen Sie den virtuellen Server aus, auf dem Sie DH aktivieren möchten.

   c. Klicken Sie auf **Bearbeiten**, klicken Sie auf **SSL-Parameter**und dann auf **DH Param aktivieren**.



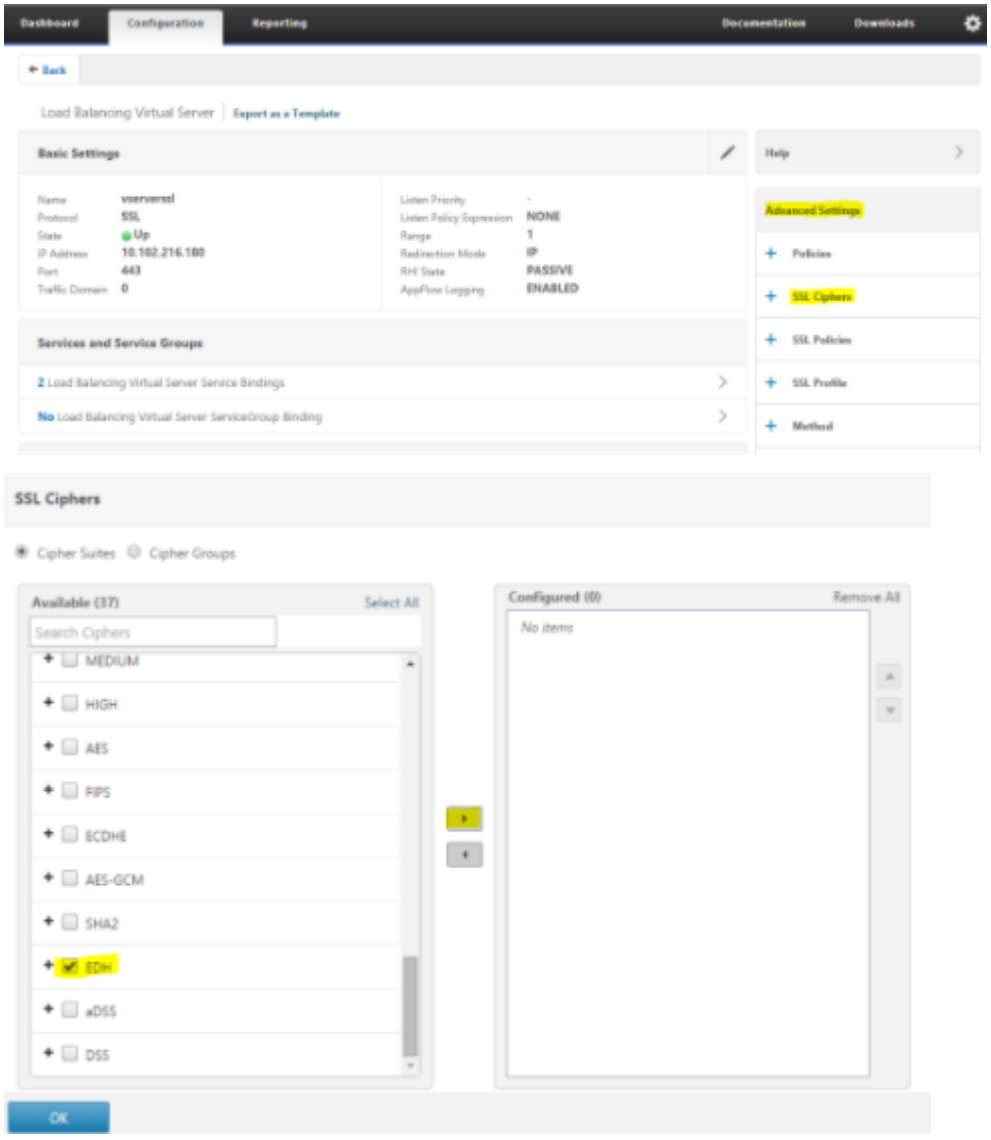
3. Binden Sie die DHE-Chiffern an den virtuellen Server.

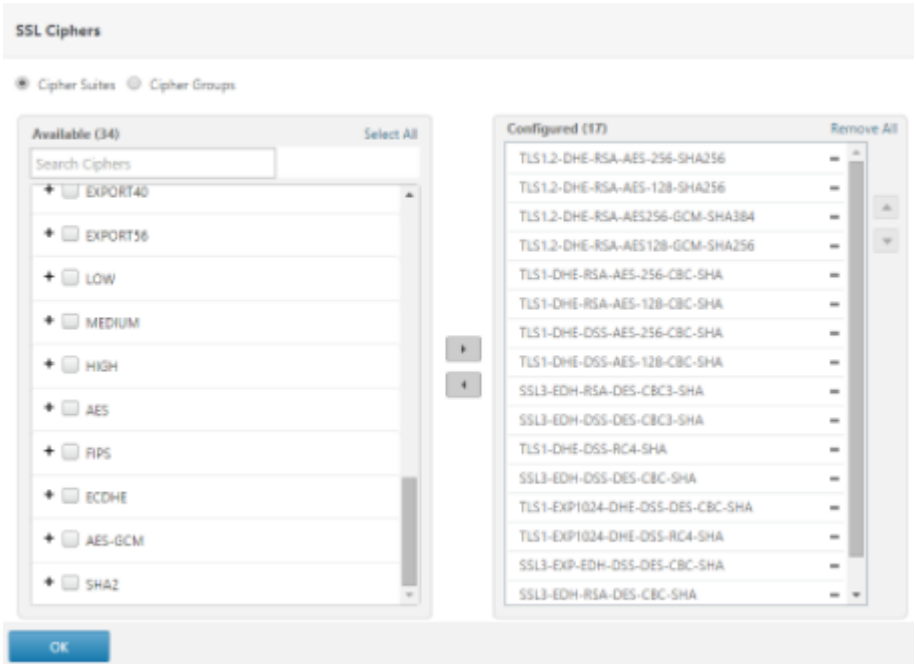
   a. Navigieren Sie zu **Konfiguration > Traffic Management > Virtuelle Server**.

   b. Wählen Sie den virtuellen Server aus, auf dem Sie DH aktivieren möchten, und klicken Sie auf das zu bearbeitende Bleistiftsymbol.

   c. Klicken Sie unter **Erweiterte Einstellungen**auf das Plus-Symbol neben **SSL Ciphers**, wählen Sie die DHE-Verschlüsselungsgruppen aus und klicken Sie zum Binden auf **OK** .

   Hinweis: Stellen Sie sicher, dass die DHE-Chiffren ganz oben in der Chiffrierliste stehen, die an den virtuellen Server gebunden ist.





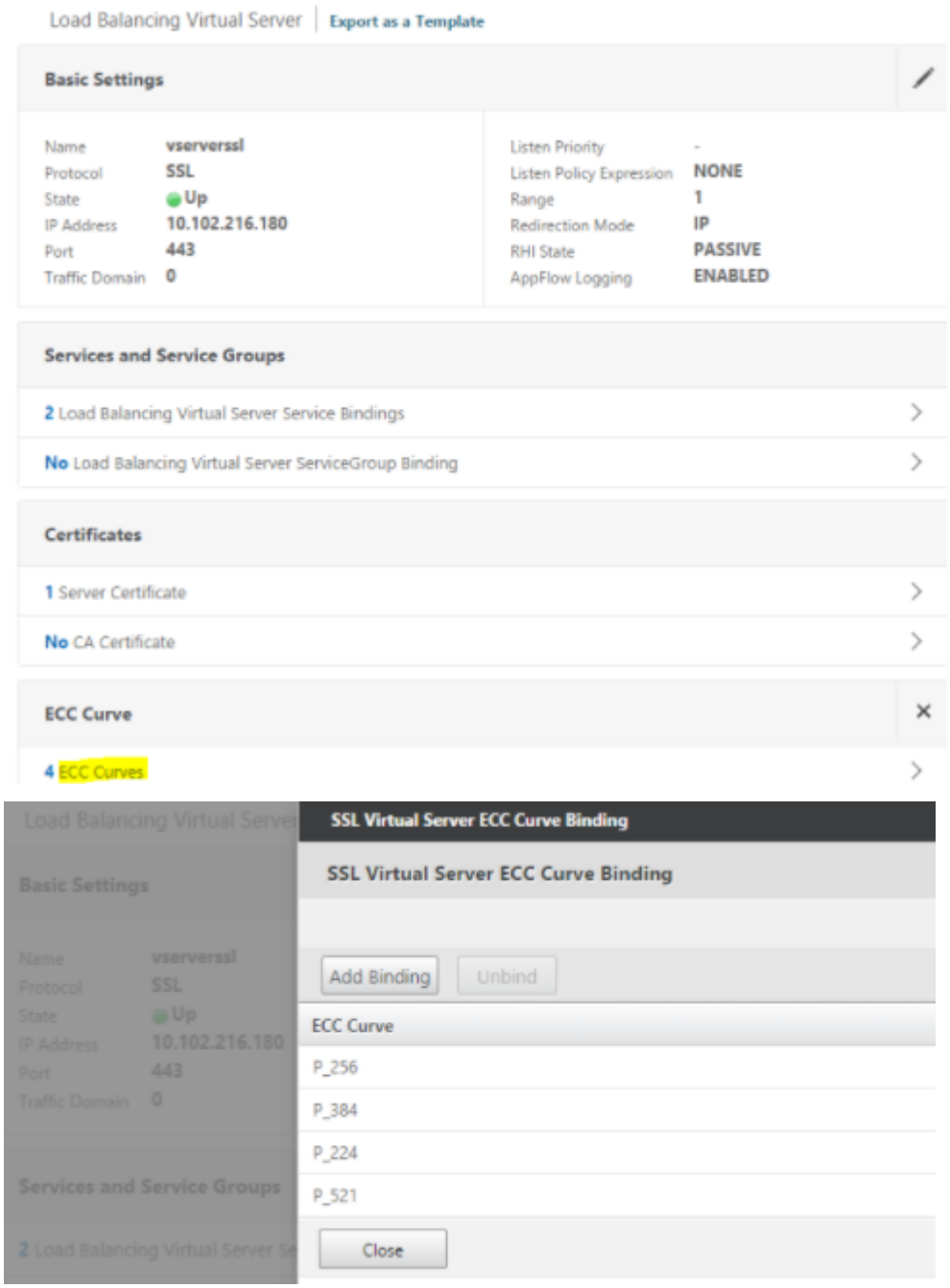
Konfigurieren Sie ECDHE mit der GUI

1. Binden Sie die ECC-Kurven an den virtuellen SSL-Server.

   a. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.

   b. Wählen Sie den virtuellen SSL-Server aus, den Sie bearbeiten möchten, klicken Sie auf **ECC-Kurve** und dann auf **Bindung hinzufügen**.

   c. Binden Sie die erforderliche ECC-Kurve an den virtuellen Server.

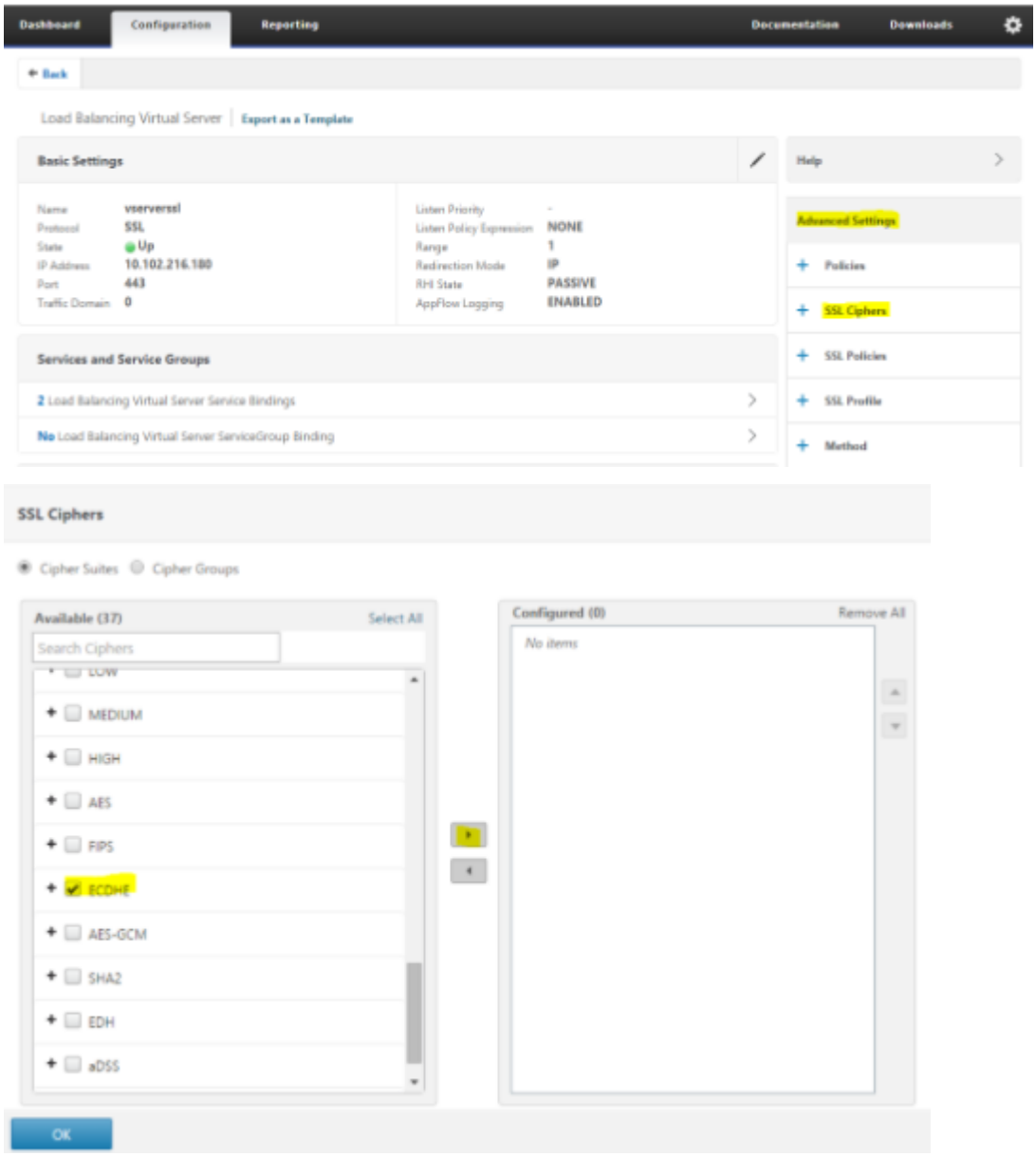


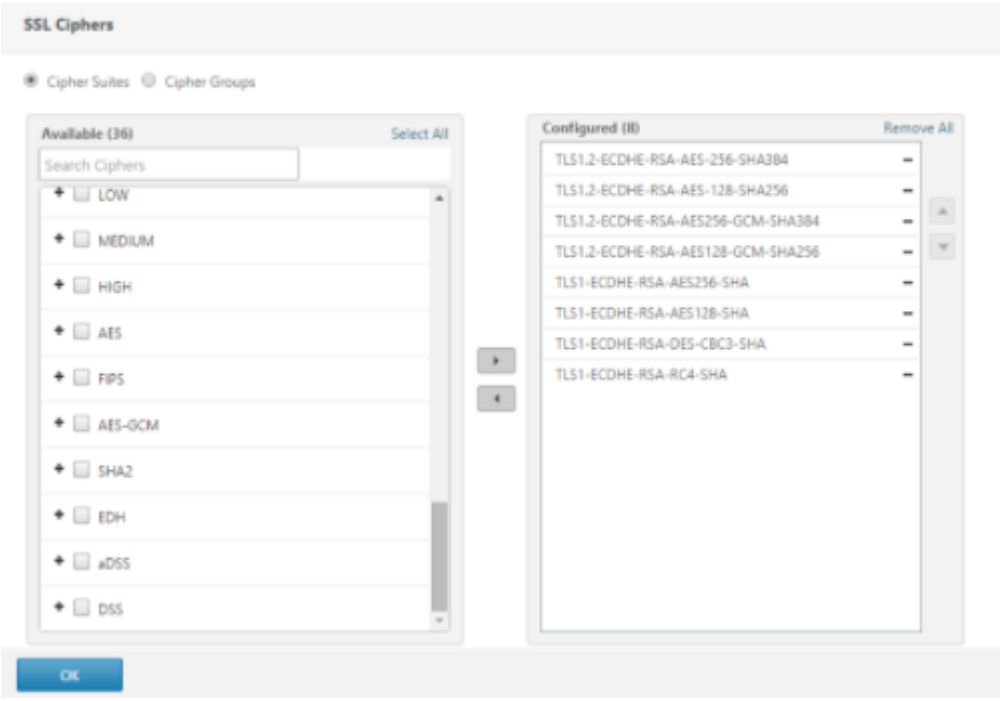
2. Binden Sie die ECDHE-Chiffern an den virtuellen Server.

   a. Navigieren Sie zu **Konfiguration > Traffic Management > Virtuelle Server** und wählen Sie den virtuellen Server aus, auf dem Sie DH aktivieren möchten.

   b. Klicken Sie auf **Edit > SSL Ciphers** und wählen Sie die ECDHE-Verschlüsselungsgruppen aus und klicken Sie auf **Binden**.

   Hinweis: Stellen Sie sicher, dass die ECDHE-Verschlüsselungen in der an den virtuellen Server gebundenen Verschlüsselungsliste ganz oben stehen.





Hinweis: Stellen Sie in jedem Fall sicher, dass die NetScaler-Appliance die Chiffern unterstützt, die Sie für die Kommunikation verwenden möchten.

Konfigurieren Sie PFS mit einem SSL-Profil

Hinweis: Die Option zur Konfiguration von PFS (Cipher oder ECC) mit einem SSL-Profil wird ab Version 11.0 64.x eingeführt. Ignorieren Sie den folgenden Abschnitt bei älteren Versionen.

Um PFS mit einem SSL-Profil zu aktivieren, muss eine ähnliche Konfiguration (wie in früheren Konfigurationsabschnitten beschrieben) durchgeführt werden, jedoch im SSL-Profil, anstatt direkt auf einem virtuellen Server zu konfigurieren.

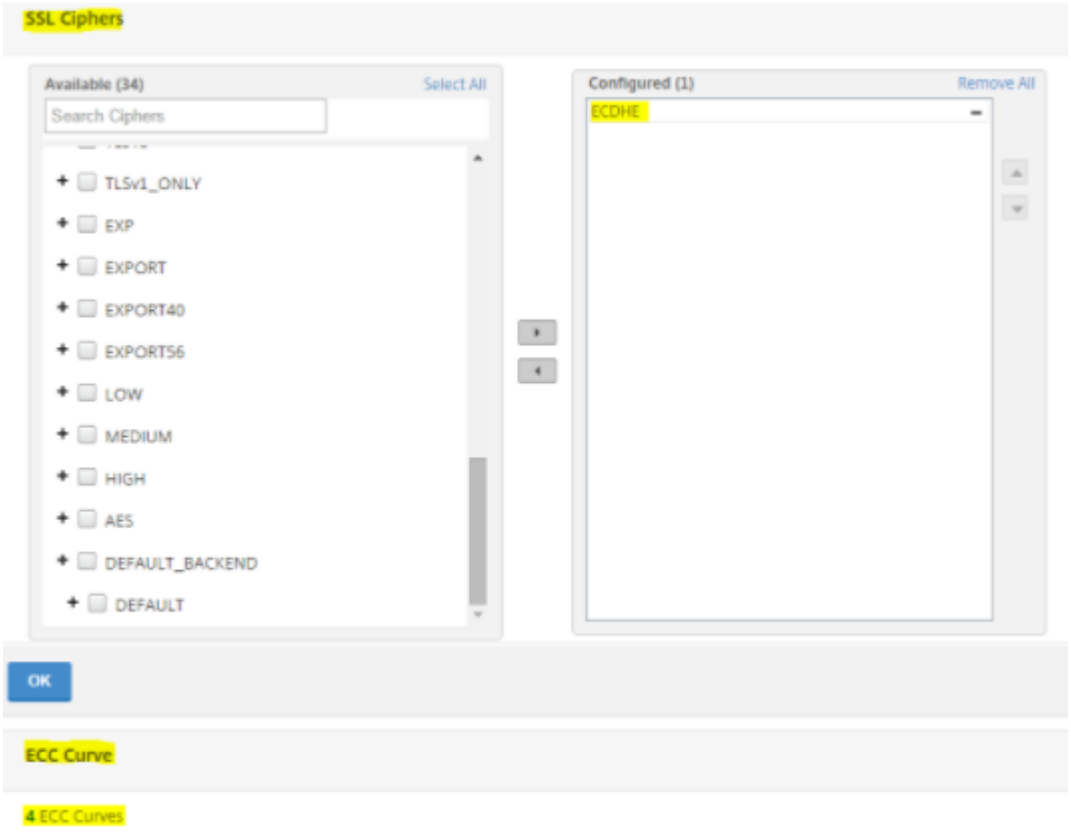
Konfigurieren Sie PFS mit einem SSL-Profil über die grafische Benutzeroberfläche

1. Binden Sie die ECC-Kurven und die ECDHE-Chiffre an das SSL-Profil.

   Hinweis: ECC-Kurven sind bereits standardmäßig an alle SSL-Profile gebunden.

   a. Navigieren Sie zu **System > Profile > SSL-Profile** und wählen Sie das Profil aus, für das Sie PFS aktivieren möchten.

   b. Binden Sie die ECDHE-Chiffern.



2. Binden Sie das SSL-Profil an den virtuellen Server.

   a. Gehen Sie zu **Konfiguration > Traffic Management > Virtuelle Server** und wählen Sie den virtuellen Server aus.

   b. Klicken Sie auf das Stiftsymbol, um das SSL-Profil zu bearbeiten.

   c. Klicken Sie auf **OK** und dann auf **Fertig**.

Konfigurieren Sie PFS mit SSL mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

1. Binden Sie ECC-Kurven an das SSL-Profil.

```
bind sslprofile <SSLProfileName> -eccCurveName <Name_of_curve>
<!--NeedCopy-->
```


2. Binden Sie die ECDHE-Chiffriergruppe.

```
bind sslprofile <SSLProfileName> cipherName <ciphergroupName>
<!--NeedCopy-->
```

3. Legen Sie die Priorität der ECDHE-Chiffre auf 1 fest.

```
set sslprofile <SSLProfileName> cipherName <ciphergroupName>
   cipherPriority <positive_integer>
<!--NeedCopy-->
```

4. Binden Sie das SSL-Profil an den virtuellen Server.

```
set SSL vserver <vservername> sslProfile <SSLProfileName>
<!--NeedCopy-->
```

ECDHE-Verschlüsselungen

May 11, 2023

Alle NetScaler-Appliances unterstützen die ECDHE-Verschlüsselungsgruppe am Frontend und im Backend. Wenn auf einer SDX-Appliance ein SSL-Chip einer VPX-Instanz zugewiesen ist, gilt die Verschlüsselungsunterstützung einer MPX-Appliance. Andernfalls gilt die normale Verschlüsselungsunterstützung einer VPX-Instanz.

Weitere Informationen zu den Builds und Plattformen, die diese Chiffren unterstützen, finden Sie unter Chiffren, die auf den NetScaler Appliances verfügbar sind.

ECDHE-Verschlüsselungssammlungen verwenden elliptische Kurvenkryptographie (ECC). Aufgrund seiner kleineren Schlüsselgröße ist ECC besonders nützlich in einer mobilen (drahtlosen) Umgebung oder einer interaktiven Sprachantwortumgebung, in der jede Millisekunde wichtig ist. Kleinere Schlüsselgrößen sparen Energie, Arbeitsspeicher, Bandbreite und Rechenkosten.

Eine NetScaler-Appliance unterstützt die folgenden ECC-Kurven:

- P_256
- P_384
- P_224
- P_521

Hinweis: Wenn Sie ein Upgrade von einem Build vor Version 10.1 Build 121.10 durchführen, müssen Sie ECC-Kurven explizit an Ihre vorhandenen virtuellen SSL-Server und -Dienste binden. Die Kurven sind standardmäßig an alle virtuellen Server und Dienste gebunden, die Sie nach dem Upgrade erstellen.

Sie können eine ECC-Kurve an SSL-Frontend- und Backend-Entitäten binden. Standardmäßig sind alle vier Kurven gebunden, und zwar in der folgenden Reihenfolge: P_256, P_384, P_224, P_521. Um die Reihenfolge zu ändern, müssen Sie zuerst alle Kurven lösen und sie dann in der gewünschten Reihenfolge binden.

Binden Sie ECC-Kurven mithilfe der CLI an einen virtuellen SSL-Server

Geben Sie in der Befehlszeile Folgendes ein:

```
bind ssl vserver <vServerName > -eccCurveName <eccCurveName >
```

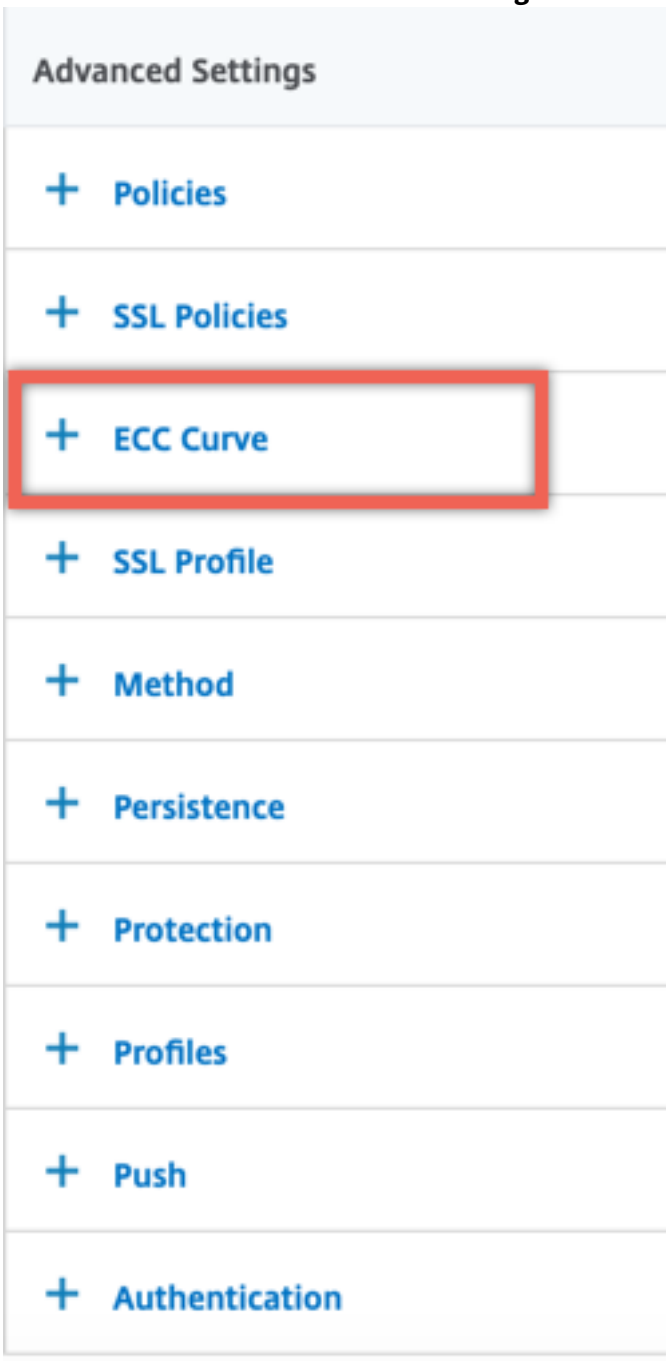
Beispiel:

```
bind ssl vserver  v1 -eccCurveName P_224

sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED
   TLSv1.2: DISABLED
Push Encryption Trigger: Always
Send Close-Notify: YES
ECC Curve: P_224

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

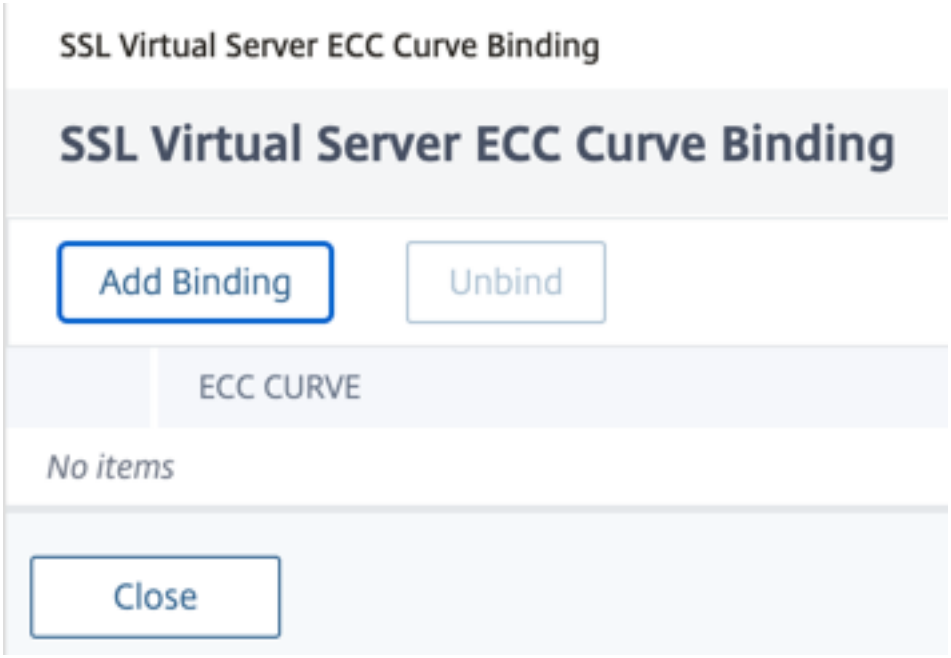
Binden Sie ECC-Kurven mithilfe der GUI an einen virtuellen SSL-Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen SSL-Server aus und klicken Sie auf **Bearbeiten**.

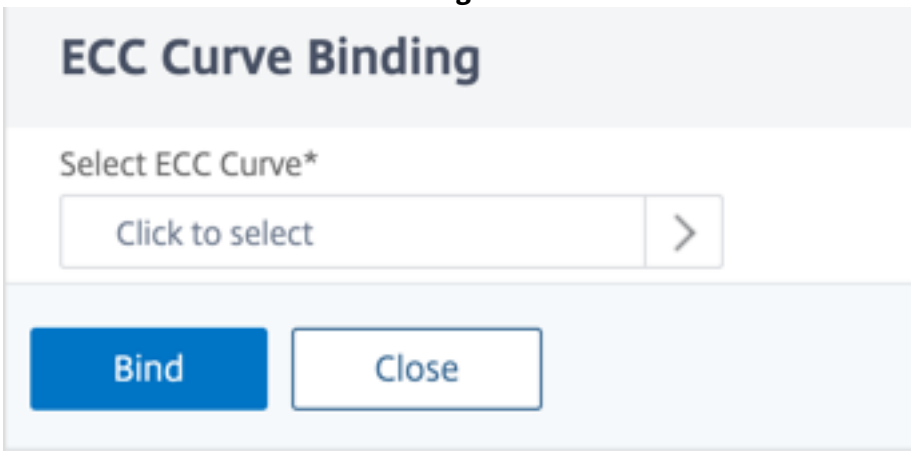
3. Klicken Sie in **den Erweiterten Einstellungen**auf **ECC-Kurve**.



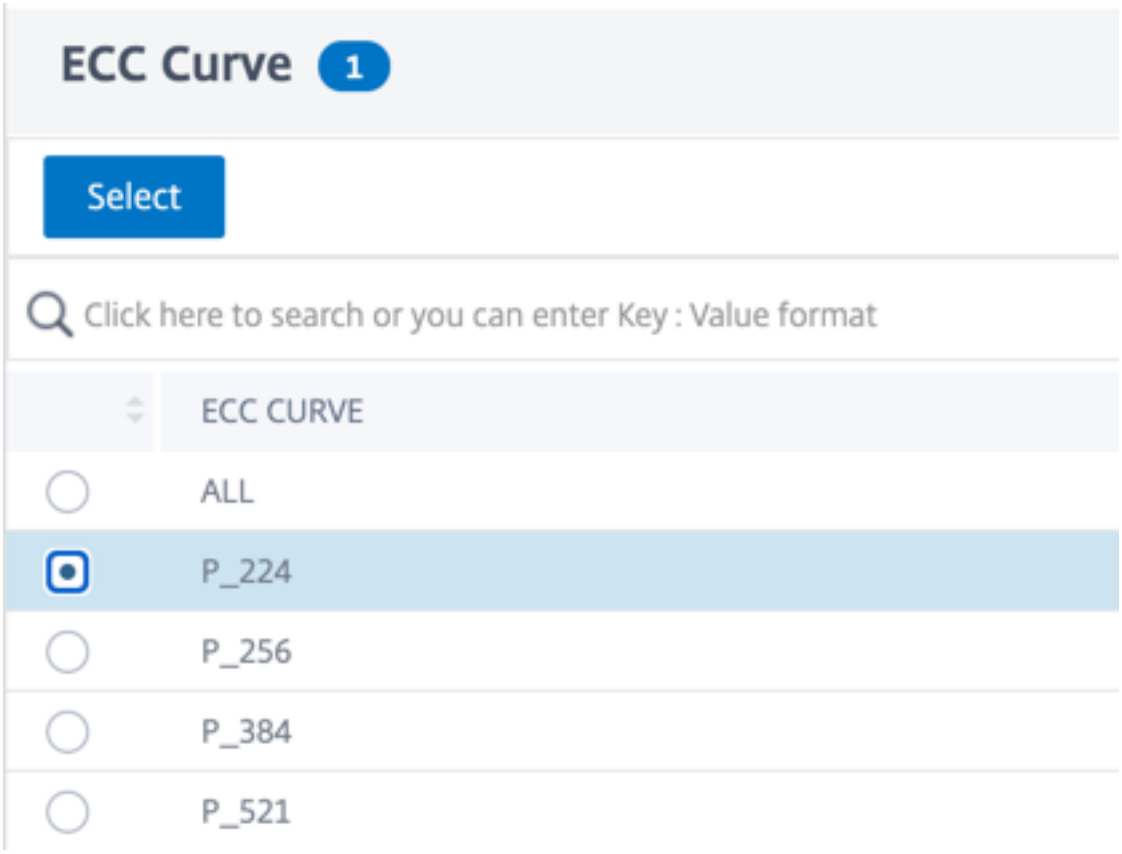
4. Klicken Sie in den ECC-Kurvenabschnitt.
5. Klicken Sie auf der Seite „ **SSL Virtual Server ECC Curve Binding** “ auf **Bindung hinzufügen**.



6. Klicken Sie unter **ECC-Kurvenbindung**auf **ECC-Kurve auswählen**.



7. Wählen Sie einen Wert aus, und klicken Sie dann auf **Auswählen**.



8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Schließen**.
10. Klicken Sie auf **Fertig**.

Binden Sie ECC-Kurven mithilfe der CLI an einen SSL-Service

Geben Sie in der Befehlszeile Folgendes ein:

```
bind ssl service <vServerName > -eccCurveName <eccCurveName >
```

Beispiel:

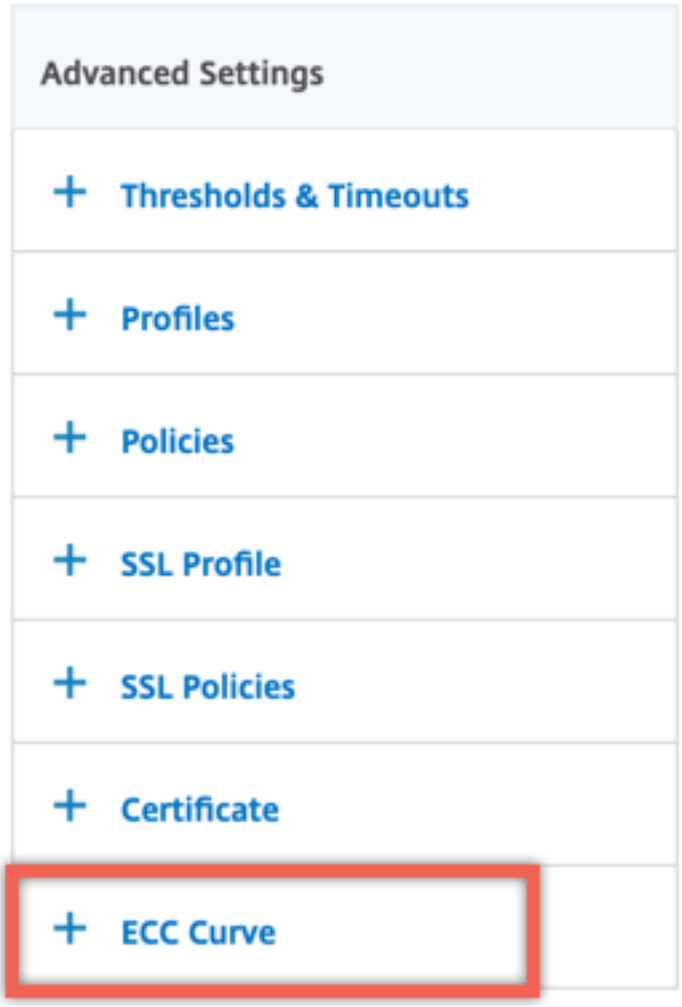
```
> bind ssl service sslsvc -eccCurveName P_224
 Done
> sh ssl service sslsvc

    Advanced SSL configuration for Back-end SSL Service sslsvc:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       DISABLED
    Session Reuse: ENABLED      Timeout: 300 seconds
    Cipher Redirect: DISABLED
    ClearText Port: 0
```



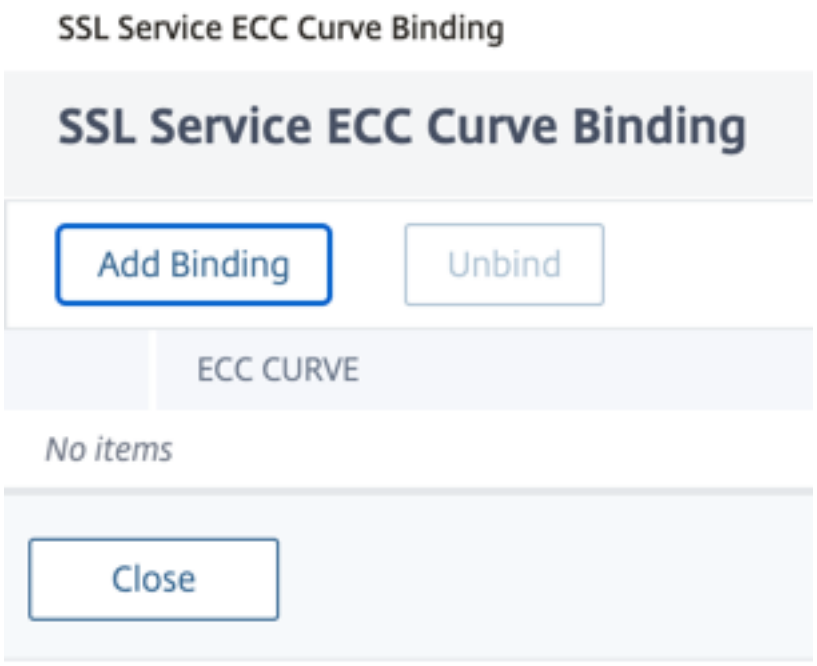
```
    Server Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: ???
    DHE Key Exchange With PSK: ???
    Tickets Per Authentication Context: ???

    ECC Curve: P_224


1)  Cipher Name: DEFAULT_BACKEND
    Description: Default cipher list for Backend SSL session
 Done
<!--NeedCopy-->
```

Binden Sie ECC-Kurven mithilfe der GUI an einen SSL-Service

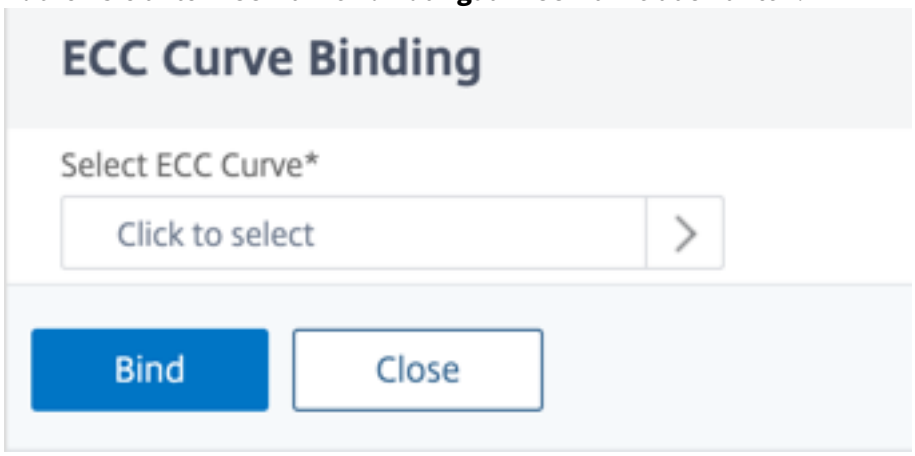
1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Wählen Sie einen SSL-Dienst und klicken Sie auf **Bearbeiten**.
3. Klicken Sie in **den Erweiterten Einstellungen**auf **ECC-Kurve**.



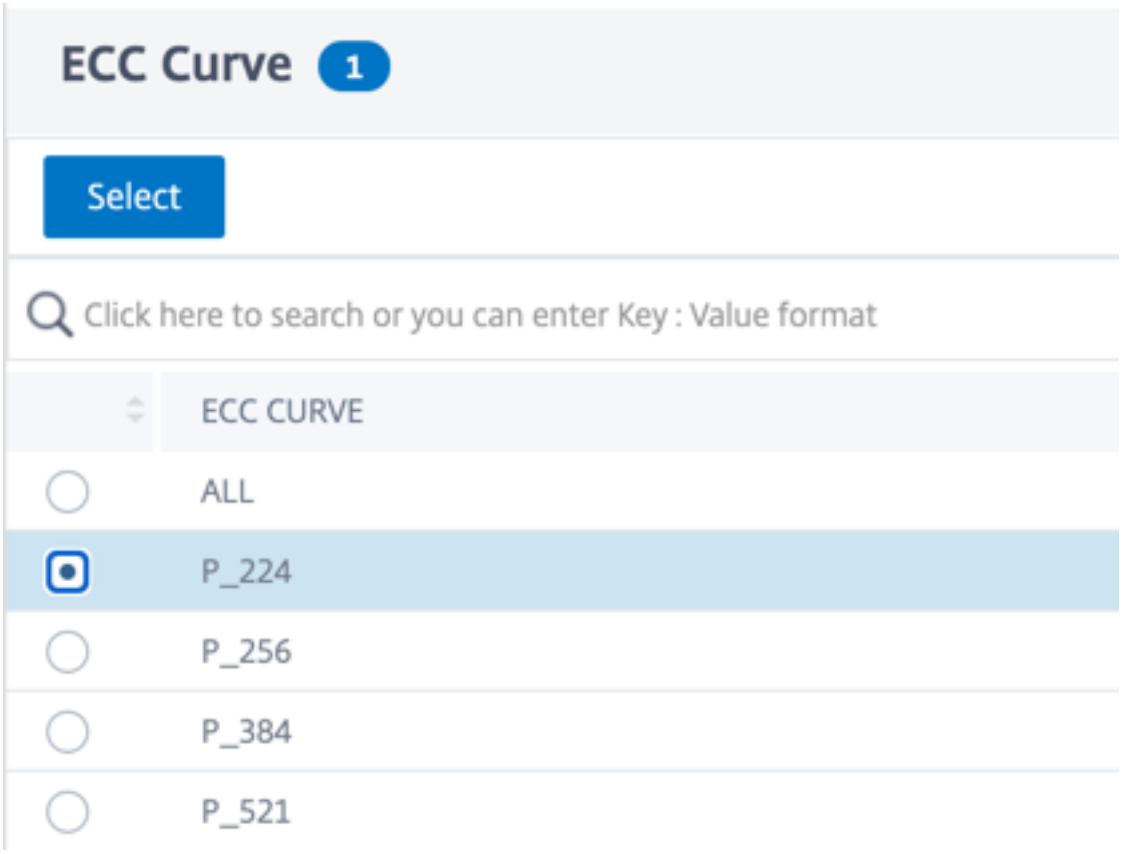
4. Klicken Sie in den ECC-Kurvenabschnitt.
5. Klicken Sie auf der Seite **SSL Service ECC Curve Binding** auf **Add Binding**.



6. Klicken Sie unter **ECC-Kurvenbindung**auf **ECC-Kurve auswählen**.



7. Wählen Sie einen Wert aus, und klicken Sie dann auf **Auswählen**.



8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Schließen**.
10. Klicken Sie auf **Fertig**.

Generierung von Diffie-Hellman-Parametern und Erreichen eines PFS mit DHE

June 19, 2023

Der Diffie-Hellman (DH) -Schlüsselaustausch ist eine Möglichkeit für zwei an einer SSL-Transaktion beteiligte Parteien, sich über einen unsicheren Kanal auf ein gemeinsames Geheimnis zu einigen. Diese Parteien haben keine Vorkenntnisse voneinander. Dieses Geheimnis kann in kryptografisches Schlüsselmaterial für symmetrische Schlüsselverschlüsselungsalgorithmen umgewandelt werden, die einen solchen Schlüsselaustausch erfordern.

Das Feature ist in der Standardeinstellung deaktiviert. Die Funktion wurde so konfiguriert, dass Chiffren unterstützt werden, die DH als Schlüsselaustauschalgorithmus verwenden.

> **Hinweis**:
>
> Das Generieren von 2048-Bit-DH-Parametern kann sehr lange dauern (bis zu 30 Minuten).

Generieren Sie DH-Parameter mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
create ssl dhparam <dhFile> [<bits>] [-gen (2 | 5)]
<!--NeedCopy-->
```

Beispiel:

```
create ssl dhparam Key-DH-1 512 -gen 2
<!--NeedCopy-->
```

Generieren Sie DH-Parameter mithilfe der GUI

Navigieren Sie zu **Traffic Management** > **SSL** und wählen Sie in der Gruppe **Tools** die Option **Diffie-Hellman-Schlüssel (DH) erstellen**und **SSL DH-Parameter konfigurieren**aus.

> **Hinweis:**
>
> Informationen zu DH-Parametern finden Sie unter Diffie-Hellman-Parametern.

Perfektes Vorwärtsgeheimnis mit DHE

Das Generieren von DH-Parametern ist ein CPU-intensiver Vorgang. In früheren Versionen dauerte die Parametergenerierung auf einer VPX-Appliance sehr lange, da sie in der Software erfolgte. Die Parametergenerierung wird durch die Einstellung des `dhKeyExpSizeLimit` Parameters optimiert. Sie können diesen Parameter für einen virtuellen SSL-Server oder ein SSL-Profil festlegen und das Profil dann an einen virtuellen Server binden.

Sie können Perfect Forward Secrecy (PFS) auf NetScaler MPX-Appliances aufrechterhalten, indem Sie die DH-Anzahl auf Null setzen. Daher werden DH-Parameter für jede Transaktion (Minimum `DHcount` ist 0) auf NetScaler MPX-Appliances generiert. Diese Parameter werden ohne nennenswerten Leistungsverlust generiert, da der Betrieb optimiert ist. Zuvor lag die zulässige Mindestanzahl an DH bei 500. Das heißt, Sie können den Schlüssel nicht für bis zu 500 Transaktionen regenerieren.

> **Einschränkung:**
>
> Wenn Sie auf einer NetScaler VPX-Appliance die DH-Anzahl auf Null setzen, werden die

> DH-Parameter nicht regeneriert. Daher müssen Sie den DH-Zähler auf 500 setzen, um PFS aufrechtzuerhalten. Die DH-Parameter werden nach 500 Transaktionen neu generiert.

Optimieren Sie die Generierung von DH-Parametern mithilfe der CLI

Geben Sie in der Befehlszeile die Befehle 1 und 2 ein, oder geben Sie Befehl 3 ein:

```
1. add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )] [-dhCount <positive_integer>] [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED)]
2. set ssl vserver <vServerName> [-sslProfile <string>]
<!--NeedCopy-->
```

```
3. set ssl vserver <vServerName> [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhCount <positive_integer>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Optimieren Sie die Generierung von DH-Parametern mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **DH Key Expire Size Limit aktivieren**aus.

Chiffreumleitung

January 19, 2021

Während des SSL-Handshakes kündigt der SSL-Client (normalerweise ein Webbrowser) die von ihm unterstützte Verschlüsselungssuite in der konfigurierten Reihenfolge an. Aus dieser Liste wählt der SSL-Server dann eine Chiffre aus, die mit seiner eigenen Liste konfigurierter Chiffren übereinstimmt.

Wenn die vom Client angekündigten Chiffre nicht mit den auf dem SSL-Server konfigurierten Chiffrieren übereinstimmen, schlägt der SSL-Handshake fehl. Der Fehler wird durch eine im Browser angezeigte kryptische Fehlermeldung angekündigt. Diese Meldungen erwähnen selten die genaue Ursache des Fehlers.

Mit der Chiffreumleitung können Sie einen virtuellen SSL-Server konfigurieren, um genaue, aussagekräftige Fehlermeldungen zu liefern, wenn ein SSL-Handshake ausfällt. Wenn ein SSL-Handshake fehlschlägt, leitet die ADC-Appliance den Benutzer auf eine zuvor konfigurierte URL um oder zeigt, wenn keine URL konfiguriert ist, eine intern generierte Fehlerseite an.

Konfigurieren der Chiffreumleitung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Verschlüsselungsumleitung zu konfigurieren und die Konfiguration zu überprüfen:

```
- set ssl vserver <vServerName> -cipherRedirect < ENABLED | DISABLED>
   -cipherURL < URL>
- show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-ssl -cipherRedirect ENABLED -cipherURL http://
   redirectURl

Done

show ssl vserver vs-ssl

Advanced SSL configuration for VServer vs-ssl:
DH: DISABLED
Ephemeral RSA: ENABLED          Refresh Count: 1000
Session Reuse: ENABLED          Timeout: 600 seconds
Cipher Redirect: ENABLED        Redirect URL: http://redirectURl
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2: ENABLED
   TLSv1.2: ENABLED
    1)      CertKey Name: Auth-Cert-1       Server Certificate
    1)      Cipher Name: DEFAULT
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```


Konfigurieren der Chiffreumleitung mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Chiffrier-Umleitung aktivieren** aus, und geben Sie eine Umleitungs-URL an.

Verwenden Sie Hardware und Software, um die Leistung der ECDHE- und ECDSA-Verschlüsselung zu verbessern

May 11, 2023

> **Hinweis:**
>
> Diese Verbesserung gilt nur für die folgenden Plattformen:
>
> - MPX/SDX 11000
> - MPX/SDX 14000
> - MPX 22000, MPX 24000 und MPX 25000
> - MPX/SDX 14000 FIPS

Bisher wurden ECDHE- und ECDSA-Berechnungen auf einer NetScaler-Appliance nur auf der Hardware (Cavium-Chips) durchgeführt, wodurch die Anzahl der SSL-Sitzungen zu einem bestimmten Zeitpunkt begrenzt wurde. Mit dieser Erweiterung werden einige Operationen auch in der Software ausgeführt. Das heißt, die Verarbeitung erfolgt sowohl auf den Cavium-Chips als auch auf den CPU-Kernen, um die ECDHE- und ECDSA-Chiffrierleistung zu verbessern.

Die Verarbeitung erfolgt zunächst in Software bis zum konfigurierten Software-Krypto-Schwellenwert. Nachdem dieser Schwellenwert erreicht ist, werden die Operationen auf die Hardware ausgelagert. Daher verwendet dieses Hybridmodell sowohl Hardware als auch Software, um die SSL-Leistung zu verbessern. Sie können das Hybridmodell aktivieren, indem Sie den Parameter „SoftwareCryptoThreshold“ entsprechend Ihren Anforderungen festlegen. Um das Hybridmodell zu deaktivieren, setzen Sie diesen Parameter auf 0.

Die Vorteile sind am größten, wenn die aktuelle CPU-Auslastung nicht zu hoch ist, da der CPU-Schwellenwert nicht ausschließlich für ECDHE- und ECDSA-Berechnungen gilt. Wenn die aktuelle Arbeitslast auf der Appliance beispielsweise 50% der CPU-Zyklen verbraucht und der Schwellenwert auf 80% festgelegt ist, können bei der ECDHE- und ECDSA-Berechnung nur 30% verwendet werden. Nachdem der konfigurierte Software-Krypto-Schwellenwert von 80% erreicht ist, werden weitere ECDHE- und ECDSA-Berechnungen auf die Hardware ausgelagert. In diesem Fall könnte die tatsächliche CPU-Auslastung 80% überschreiten, da die Durchführung von ECDHE- und ECDSA-Berechnungen in der Hardware einige CPU-Zyklen beansprucht.

Aktivieren Sie das Hybridmodell mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set ssl parameter -softwareCryptoThreshold <positive_integer>

Synopsis:

softwareCryptoThreshold:

NetScaler CPU utilization threshold (as a percentage) beyond which
   crypto operations are not done in software. A value of zero implies
   that CPU is not utilized for doing crypto in software.

Default = 0

Min = 0

Max = 100
<!--NeedCopy-->
```

Beispiel:

```
set ssl parameter - softwareCryptoThreshold 80
Done

show ssl parameter
Advanced SSL Parameters

SSL quantum size                  : 8 KB
Max CRL memory size               : 256 MB
Strict CA checks                  : NO
Encryption trigger timeout        : 100 ms
Send Close-Notify                 : YES
Encryption trigger packet c       : 45
Deny SSL Renegotiation            : ALL
Subject/Issuer Name Insertion Format : Unicode
OCSP cache size                   : 10 MB
Push flag                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout   : 1 ms
Crypto Device Disable Limit       : 0
Global undef action for control policies : CLIENTAUTH
Global undef action for data policies : NOOP
Default profile                   : DISABLED
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
```



```
Disable TLS 1.1/1.2 for dynamic and VPN services : NO
Software Crypto acceleration CPU Threshold : 80
Signature and Hash Algorithms supported by TLS1.2 : ALL
<!--NeedCopy-->
```

Aktivieren Sie das Hybridmodell mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Erweiterte SSL-Einstellungen ändern**.
2. Geben Sie einen Wert für den **Software-Krypto-Schwellenwert (%)**ein.

Stellen Sie einen SNMP-Alarm für den ECDHE-Wechselkurs ein

Der ECDHE-basierte Schlüsselaustausch kann dazu führen, dass die Transaktionen pro Sekunde auf der Appliance ausfallen. Ab Version 13.0 Build 52.x können Sie einen SNMP-Alarm für ECDHE-basierte Transaktionen konfigurieren. In diesem Alarm können Sie den Schwellenwert und die normalen Grenzwerte für den ECDHE-Wechselkurs festlegen. Ein neuer Zähler `nsssl_tot_sslInfo_ECDHE_Tx` wird hinzugefügt. Dieser Zähler ist die Summe aller ECDHE-basierten Transaktionszähler im Frontend und Back-End der Appliance. Wenn der ECDHE-basierte Schlüsselaustausch die konfigurierten Grenzwerte überschreitet, wird ein SNMP-Trap gesendet. Ein weiterer Trap wird gesendet, wenn der Wert wieder auf dem konfigurierten Normalwert liegt.

Stellen Sie mit der CLI einen SNMP-Alarm für den ECDHE-Wechselkurs ein

Geben Sie in der Befehlszeile Folgendes ein:

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging ( ENABLED | DISABLED ) -
   severity <severity>
 -state ( ENABLED | DISABLED ) -thresholdValue <positive_integer>  [-
    normalValue <positive_integer>] -time <secs>
<!--NeedCopy-->
```

Beispiel:

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging eNABLED -severity critical
   -state eNABLED -thresholdValue 100 -normalValue 50
<!--NeedCopy-->
```

Unterstützung von ECDSA-Verschlüsselungssammlungen

May 11, 2023

ECDSA-Cipher-Suiten verwenden elliptische Kurvenkryptographie (ECC). Aufgrund seiner kleineren Größe ist es in Umgebungen hilfreich, in denen Verarbeitungsleistung, Speicherplatz, Bandbreite und Stromverbrauch eingeschränkt sind.

Wenn die ECDHE_ECDSA-Verschlüsselungsgruppe verwendet wird, muss das Zertifikat des Servers einen ECDSA-fähigen öffentlichen Schlüssel enthalten.

In der folgenden Tabelle sind die ECDSA-Verschlüsselungen aufgeführt, die von NetScaler MPX- und SDX-Appliances mit N3-Chips, NetScaler VPX Appliances, MPX 5900/26000 und MPX/SDX 8900/15000 unterstützt werden.

Chiffrename	Priorität	Beschreibung	Key Exchange-Algorithmus	Authentifizierungsalgorithmus	Verschlüsselung (Schlüsselgröße)	Algorithmus für Nachrichtenauthentifizierungscode (MAC)	Hex-Code
TLS1-ECDHE-ECDSA-AES128-SHA	1	SSLv3	ECC-DHE	ECDSA	AES(128)	SHA1	0xc009
TLS1-ECDHE-ECDSA-AES256-SHA	2	SSLv3	ECC-DHE	ECDSA	AES(256)	SHA1	0xc00a
TLS1.2-ECDHE-ECDSA-AES128-SHA256	3	TLSv1.2	ECC-DHE	ECDSA	AES(128)	SHA-256	0xc023
TLS1.2-ECDHE-ECDSA-AES256-SHA384	4	TLSv1.2	ECC-DHE	ECDSA	AES(256)	SHA-384	0xc024

Chiffrename	Priorität	Beschreibung	Key Exchange-Algorithmus	Authentifizierungsalgorithmus	Verschlüsselungsalgorithmus (Schlüsselgröße)	Algorithmus für Nachrichtenauthentifizierungscode (MAC)	Hex-Code
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	5	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(128)	SHA-256	0xc02b
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	6	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(256)	SHA-384	0xc02c
TLS1-ECDHE-ECDSA-RC4-SHA	7	SSLv3	ECC-DHE	ECDSA	RC4(128)	SHA1	0xc007
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	8	SSLv3	ECC-DHE	ECDSA	3DES(168)	SHA1	0xc008
TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305	9	TLSv1.2	ECC-DHE	ECDSA	CHACHA20/	AEAD	0xcca9

ECDSA/RSA-Verschlüsselung und Zertifikatauswahl

Sie können sowohl ECDSA- als auch RSA-Serverzertifikate gleichzeitig an einen virtuellen SSL-Server binden. Wenn sowohl ECDSA- als auch RSA-Zertifikate an den virtuellen Server gebunden sind, wählt dieser automatisch das entsprechende Serverzertifikat aus, das dem Client vorgelegt werden soll. Wenn die Client-Verschlüsselungsliste RSA-Chiffren, aber keine ECDSA-Chiffren enthält, präsentiert der virtuelle Server das RSA-Serverzertifikat. Wenn beide Chiffren in der Liste des Clients vorhanden sind, hängt das angezeigte Serverzertifikat von der auf dem virtuellen Server festgelegten Verschlüsselungspriorität ab. Das heißt, wenn RSA eine höhere Priorität hat, wird das RSA-Zertifikat vorgelegt. Wenn ECDSA eine höhere Priorität hat, wird das ECDSA-Zertifikat dem Client vorgelegt.

Client-Authentifizierung mithilfe eines ECDSA- oder RSA-Zertifikats

Für die Client-Authentifizierung kann das an den virtuellen Server gebundene CA-Zertifikat mit ECDSA oder RSA signiert werden. Die Appliance unterstützt eine gemischte Zertifikatskette. Beispielsweise wird die folgende Zertifikatskette unterstützt.

Client-Zertifikat (ECDSA) <-> CA-Zertifikat (RSA) <-> Zwischenzertifikat (RSA) <-> Stammzertifikat (RSA)

Die folgende Tabelle zeigt die elliptischen Kurven, die auf den verschiedenen NetScaler Appliances mit ECDSA-Chiffriergruppen und ECDSA-Zertifikaten unterstützt werden:

Elliptische Kurven	Unterstützte Plattformen
prime256v1	Alle Plattformen, einschließlich FIPS.
secp384r1	Alle Plattformen, einschließlich FIPS.
secp521r1	MPX 5900, MPX/SDX 8900, MPX/SDX 15000, MPX/SDX 26000, VPX
secp224r1	MPX 5900, MPX/SDX 8900. MPX/SDX 15000, MPX/SDX 26000, VPX

Erstellen eines ECDSA-Zertifikatschlüsselpaars

Sie können ein ECDSA-Zertifikatsschlüsselpaar direkt auf einer NetScaler-Appliance erstellen, indem Sie die CLI oder die GUI verwenden. Zuvor konnten Sie ein ECC-Zertifikatsschlüsselpaar auf der Appliance installieren und binden, aber Sie mussten OpenSSL verwenden, um ein Zertifikatsschlüsselpaar zu erstellen.

Nur P_256- und P_384-Kurven werden unterstützt.

> **Hinweis**
>
> Diese Unterstützung ist auf allen Plattformen außer MPX 9700/1050/12500/15500 verfügbar.

Um ein ECDSA-Zertifikatsschlüsselpaar mit der CLI zu erstellen, gehen Sie wie folgt vor:

Geben Sie in der Befehlszeile Folgendes ein:

```
create ssl ecdsaKey <keyFile> -curve ( P_256 | P_384 ) [-keyform ( DER | PEM )] [-des | -des3] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Beispiel:

```
create ecdsaKey ec_p256.ky -curve P_256 -pkcs8
Done
create ecdsaKey ec_p384.ky -curve P_384
Done
<!--NeedCopy-->
```

Um ein ECDSA-Zertifikatsschlüsselpaar mithilfe der GUI zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Dateien > Schlüssel** und klicken Sie auf **ECDSA-Schlüssel erstellen**.
2. Um einen Schlüssel im PKCS #8 Format zu erstellen, wählen Sie **PKCS8**aus.

Konfigurieren benutzerdefinierter Verschlüsselungsgruppen auf der ADC-Appliance

May 11, 2023

Eine Verschlüsselungsgruppe ist eine Reihe von Verschlüsselungssuiten, die Sie an einen virtuellen SSL-Server, -Dienst oder eine Dienstgruppe auf der NetScaler-Appliance binden. Eine Verschlüsselungssuite umfasst ein Protokoll, einen Schlüsselaustauschalgorithmus (Kx), einen Authentifizierungsalgorithmus (Au), einen Verschlüsselungsalgorithmus (Enc) und einen Algorithmus für den Nachrichtenauthentifizierungscode (Mac). Ihre Appliance wird mit einem vordefinierten Satz von Verschlüsselungsgruppen geliefert. Wenn Sie einen SSL-Dienst oder eine SSL-Dienstgruppe erstellen, wird die ALL-Chiffriergruppe automatisch daran gebunden. Wenn Sie jedoch einen virtuellen SSL-Server oder einen transparenten SSL-Dienst erstellen, wird die DEFAULT-Verschlüsselungsgruppe automatisch daran gebunden. Darüber hinaus können Sie eine benutzerdefinierte Verschlüs-

selungsgruppe erstellen und sie an einen virtuellen SSL-Server, -Dienst oder eine Dienstgruppe binden.

Hinweis: Wenn Ihre MPX-Appliance über keine Lizenzen verfügt, ist nur die EXPORT-Chiffre an Ihren virtuellen SSL-Server, -Dienst oder Ihre Dienstgruppe gebunden.

Um eine benutzerdefinierte Verschlüsselungsgruppe zu erstellen, erstellen Sie zunächst eine Verschlüsselungsgruppe und binden dann Chiffren oder Verschlüsselungsgruppen an diese Gruppe. Wenn Sie einen Chiffrieralias oder eine Verschlüsselungsgruppe angeben, werden alle Chiffren in dem Chiffrieralias oder der Verschlüsselungsgruppe zur benutzerdefinierten Verschlüsselungsgruppe hinzugefügt. Sie können einer benutzerdefinierten Gruppe auch einzelne Chiffren (Cipher Suites) hinzufügen. Sie können jedoch eine vordefinierte Verschlüsselungsgruppe nicht ändern. Bevor Sie eine Verschlüsselungsgruppe entfernen, heben Sie die Bindung aller Cipher-Suites in der Gruppe auf.

Beim Binden einer Verschlüsselungsgruppe an einen virtuellen SSL-Server, -Dienst oder eine Dienstgruppe werden die Chiffren an die vorhandenen Verschlüsselungen angehängt, die an die Entität gebunden sind. Um eine bestimmte Verschlüsselungsgruppe an die Entität zu binden, müssen Sie zuerst die Chiffren oder Verschlüsselungsgruppe aufheben, die an die Entität gebunden ist. Binden Sie dann die spezifische Verschlüsselungsgruppe an die Entität. Um beispielsweise nur die AES-Verschlüsselungsgruppe an einen SSL-Dienst zu binden, führen Sie die folgenden Schritte aus:

1. Entbindet die Standard-Verschlüsselungsgruppe ALL, die standardmäßig an den Dienst gebunden ist, wenn der Dienst erstellt wird.

   ```
   unbind ssl service <service name> -cipherName ALL
   <!--NeedCopy-->
   ```

2. Binden Sie die AES-Verschlüsselungsgruppe an den Dienst

   ```
   bind ssl service <Service name> -cipherName AE
   <!--NeedCopy-->
   ```

   Wenn Sie die Verschlüsselungsgruppe DES zusätzlich zu AES binden möchten, geben Sie an der Befehlszeile Folgendes ein:

   ```
   bind ssl service <service name> -cipherName DES
   <!--NeedCopy-->
   ```

Hinweis: Die kostenlose virtuelle NetScaler-Appliance unterstützt nur die DH-Chiffriergruppe.

Konfigurieren Sie eine benutzerdefinierte Verschlüsselungsgruppe mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Verschlüsselungsgruppe hinzuzufügen oder um Verschlüsselungen zu einer zuvor erstellten Gruppe hinzuzufügen, und überprüfen Sie die Einstellungen:


```
add ssl cipher <cipherGroupName>
bind ssl cipher <cipherGroupName> -cipherName <cipherGroup/cipherName>
show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Beispiel:

```
add ssl cipher test

Done

bind ssl cipher test -cipherName ECDHE

Done

sh ssl cipher test

1)      Cipher Name: TLS1-ECDHE-RSA-AES256-SHA  Priority : 1
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1   HexCode
   =0xc014
2)      Cipher Name: TLS1-ECDHE-RSA-AES128-SHA  Priority : 2
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1   HexCode
   =0xc013
3)      Cipher Name: TLS1.2-ECDHE-RSA-AES-256-SHA384    Priority : 3
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA-384
   HexCode=0xc028
4)      Cipher Name: TLS1.2-ECDHE-RSA-AES-128-SHA256    Priority : 4
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA-256
   HexCode=0xc027
5)      Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 5
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc030
6)      Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 6
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02f
7)      Cipher Name: TLS1-ECDHE-ECDSA-AES256-SHA        Priority : 7
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA1
   HexCode=0xc00a
8)      Cipher Name: TLS1-ECDHE-ECDSA-AES128-SHA        Priority : 8
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA1
   HexCode=0xc009
9)      Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-SHA384   Priority : 9
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA-384
   HexCode=0xc024
```



```
10)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-SHA256   Priority : 10
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA-256
   HexCode=0xc023
11)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
   Priority : 11
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc02c
12)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
   Priority : 12
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02b
13)     Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA        Priority : 13
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1   HexCode
   =0xc012
14)     Cipher Name: TLS1-ECDHE-ECDSA-DES-CBC3-SHA      Priority : 14
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=3DES(168) Mac=SHA1
   HexCode=0xc008
15)     Cipher Name: TLS1-ECDHE-RSA-RC4-SHA     Priority : 15
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=RC4(128)  Mac=SHA1   HexCode
   =0xc011
16)     Cipher Name: TLS1-ECDHE-ECDSA-RC4-SHA   Priority : 16
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=RC4(128)  Mac=SHA1
   HexCode=0xc007
17)     Cipher Name: TLS1.2-ECDHE-RSA-CHACHA20-POLY1305 Priority : 17
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=CHACHA20/POLY1305(256) Mac
   =AEAD   HexCode=0xcca8
18)     Cipher Name: TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305
   Priority : 18
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=CHACHA20/POLY1305(256)
   Mac=AEAD   HexCode=0xcca9
Done

bind ssl cipher test -cipherName TLS1-ECDHE-RSA-DES-CBC3-SHA
<!--NeedCopy-->
```

Entbinden von Chiffren aus einer Verschlüsselungsgruppe mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Bindung von Chiffren an eine benutzerdefinierte Verschlüsselungsgruppe aufzuheben, und überprüfen Sie die Einstellungen:

```
show ssl cipher <cipherGroupName>

unbind ssl cipher <cipherGroupName> -cipherName <string>

```



```
show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Entfernen Sie eine Verschlüsselungsgruppe mithilfe der CLI

Hinweis: Sie können eine integrierte Verschlüsselungsgruppe nicht entfernen. Bevor Sie eine benutzerdefinierte Verschlüsselungsgruppe entfernen, stellen Sie sicher, dass die Verschlüsselungsgruppe leer ist.

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine benutzerdefinierte Verschlüsselungsgruppe zu entfernen, und überprüfen Sie die Konfiguration:

```
rm ssl cipher <userDefCipherGroupName> [<cipherName> ...]
show ssl cipher <cipherGroupName>

<!--NeedCopy-->
```

Beispiel:

```
rm ssl cipher test Done

sh ssl cipher test ERROR: No such resource [cipherGroupName, test]
<!--NeedCopy-->
```

Konfigurieren Sie eine benutzerdefinierte Verschlüsselungsgruppe mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Cipher Groups.**
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für die Verschlüsselungsgruppe an.
4. Klicken Sie auf **Hinzufügen**, um die verfügbaren Chiffren und Verschlüsselungsgruppen anzuzeigen.
5. Wählen Sie eine Chiffre oder Verschlüsselungsgruppe aus und klicken Sie auf die Pfeilschaltfläche, um sie hinzuzufügen.
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Schließen**.

So binden Sie eine Verschlüsselungsgruppe mithilfe der CLI an einen virtuellen SSL-Server, -Dienst oder eine Dienstgruppe:

Geben Sie in der Befehlszeile einen der folgenden Befehle ein:

```
bind ssl vserver <vServerName> -cipherName <string>

```



```
bind ssl service <serviceName> -cipherName <string>

bind ssl serviceGroup <serviceGroupName> -cipherName <string>

<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver ssl_vserver_test -cipherName test
Done

bind ssl service  nshttps -cipherName test
Done

bind ssl servicegroup  ssl_svc  -cipherName test
Done
<!--NeedCopy-->
```

So binden Sie eine Verschlüsselungsgruppe mithilfe der GUI an einen virtuellen SSL-Server, Dienst oder Dienstgruppe:

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.

   Ersetzen Sie virtuelle Server für den Service durch Dienste. Ersetzen Sie für Dienstgruppen virtuelle Server durch Dienstgruppen.

   Öffnen Sie den virtuellen Server, Dienst oder Dienstgruppe.

2. Wählen Sie unter **Erweiterte Einstellungen**die Option **SSL-Verschlüsselungen**aus.
3. Binden Sie eine Verschlüsselungsgruppe an den virtuellen Server, Dienst oder Dienstgruppe.

Bindung einzelner Chiffren an einen virtuellen SSL-Server oder -Dienst

Sie können anstelle einer Verschlüsselungsgruppe auch einzelne Chiffren an einen virtuellen Server oder Dienst binden.

Um eine Chiffre mithilfe der CLI zu binden:
Geben Sie in der Befehlszeile Folgendes ein:

```
bind ssl vserver <vServerName> -cipherName <string>
bind ssl service <serviceName> -cipherName <string>
<!--NeedCopy-->
```

Beispiel:


```
bind ssl vserver v1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
Done

bind ssl service sslsvc -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
Done
<!--NeedCopy-->
```

Um eine Chiffre mithilfe der GUI an einen virtuellen SSL-Server zu binden:

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen SSL-Server aus und klicken Sie auf **Bearbeiten**.
3. Wählen Sie unter **Erweiterte Einstellungen**die Option **SSL-Verschlüsselungen**aus.
4. **Wählen Sie in**Cipher Suites**Hinzufügen aus.**
5. Suchen Sie in der verfügbaren Liste nach der Chiffre und klicken Sie auf den Pfeil, um sie der konfigurierten Liste hinzuzufügen.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Fertig**.

Um eine Verschlüsselung an einen SSL-Dienst zu binden, wiederholen Sie die vorherigen Schritte, nachdem Sie den virtuellen Server durch den Dienst ersetzt haben.

Unterstützungsmatrix für Serverzertifikate auf der ADC-Appliance

August 15, 2023

NetScaler unterstützt Serverzertifikatnachrichten, die in mehr als einen Datensatz fragmentiert sind, wenn die Gesamtgröße innerhalb von 32 KB liegt. Zuvor betrug die maximal unterstützte Größe 16 KB und die Fragmentierung wurde nicht unterstützt.

Die NetScaler-Appliance unterstützt die folgenden Serverzertifikate.

Tabelle 1: Unterstützung von Front-End- (FE) und Back-End-Diensten (BE)

Serverzertifikat/Plattform	MPX/SDX (N2 CHIPS) FE	MPX/SDX (N2 CHIPS) BE	MPX/SDX (N3 CHIPS) FE	MPX/SDX (N3 CHIPS) BE	VPX FE	VPX BE
MD5	J	J	J	J	J	J
SHA1	J	J	J	J	J	J
SHA224	J	J	J	J	J	J
SHA256	J	J	J	J	J	J

Serverzertifikat/Plattform	MPX/SDX (N2 CHIPS) FE	MPX/SDX (N2 CHIPS) BE	MPX/SDX (N3 CHIPS) FE	MPX/SDX (N3 CHIPS) BE	VPX FE	VPX BE
SHA384	J	J	J	J	J	J
SHA512	J	J	J	J	J	J
RSA-Schlüssel	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit
DH-Schlüssel	1024 Bit und 2048 Bit	1024 Bit und 2048 Bit	1024 Bit und 2048 Bit	1024 Bit und 2048 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit

Serverzertifikat/Plattform	MPX/SDX 14030/14060/14080 FIPS FE	MPX/SDX 14030/14060/14080 FIPS BE
MD5	J	J
SHA1	J	J
SHA224	J	J
SHA256	J	J
SHA384	J	J
SHA512	J	J
RSA-Schlüssel	2048 Bit und 3072 Bit	2048 Bit und 3072 Bit
DH-Schlüssel	N	N

Serverzertifikat/Plattform	MPX 5900, MPX/SDX 8900, MPX/SDX 9100, MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 16000, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (Front-End)	MPX 5900, MPX/SDX 8900, MPX/SDX 9100 MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 16000, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (Back-End)
MD5	J	J
SHA1	J	J
SHA224	J	J

Serverzertifikat/Plattform	MPX 5900, MPX/SDX 8900, MPX/SDX 9100, MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 16000, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (Front-End)	MPX 5900, MPX/SDX 8900, MPX/SDX 9100 MPX/SDX 15000, MPX/SDX 15000-50G, MPX/SDX 16000, MPX/SDX 26000, MPX/SDX 26000-50G, MPX/SDX 26000-100G (Back-End)
SHA256	J	J
SHA384	J	J
SHA512	J	J
RSA-Schlüssel	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit
DH-Schlüssel	1024 Bit und 2048 Bit	1024 Bit und 2048 Bit

Hinweise

- 4k-Zertifikate erfordern höhere CPU-Zyklen und können die Leistung von Low-End-Appliances beeinträchtigen.
- In Version 11.1 und früher unterstützt eine NetScaler-Appliance die folgenden Erweiterungen für “Signaturalgorithmen” in der Hello-Nachricht des Back-End-Clients: RSA-MD5, RSA-SHA1 und RSA-SHA256.
  Die NetScaler-Appliance unterstützt keine Erweiterungen der Signaturalgorithmen SHA 384 und SHA 512. Daher setzen einige Server, z. B. Windows IIS-Server, die Verbindung zurück.
- Ab Release 12.0 unterstützt eine NetScaler-Appliance alle signature_algorithms Erweiterungen.

Clientauthentifizierung oder Mutual TLS (mTLS)

August 15, 2023

In einer typischen SSL-Transaktion prüft der Client, der über eine sichere Verbindung mit einem Server eine Verbindung herstellt, die Gültigkeit des Servers. Dazu prüft es das Zertifikat des Servers, bevor die SSL-Transaktion initiiert wird. Manchmal möchten Sie den Server jedoch so konfigurieren, dass er den Client authentifiziert, der eine Verbindung zu ihm herstellt.

Wenn die Clientauthentifizierung auf einem virtuellen SSL-Server aktiviert ist, fragt die NetScaler-Appliance während des SSL-Handshakes nach dem Clientzertifikat. Die Appliance prüft das vom Client vorgelegte Zertifikat auf normale Einschränkungen wie die Signatur des Ausstellers und das Ablaufdatum.

Ab Version 13.1 Build 42.x unterstützt die NetScaler Appliance die Validierung signaturübergreifender Zertifikate. Das heißt, wenn ein Zertifikat von mehreren Ausstellern signiert wurde, ist die Überprüfung erfolgreich, wenn mindestens ein gültiger Pfad zum Stammzertifikat vorhanden ist. Wenn eines der Zertifikate in der Zertifikatskette quersigniert war und mehrere Pfade zum Stammzertifikat hatte, suchte die ADC-Appliance früher nur nach einem Pfad. Und wenn dieser Pfad nicht gültig war, schlug die Überprüfung fehl.

> **Hinweis Damit**
>
> die Appliance die Signaturen des Ausstellers überprüfen kann, muss das Zertifikat der Zertifizierungsstelle, die das Clientzertifikat ausgestellt hat, wie folgt lauten:
>
> - Auf dem Gerät installiert.
> - An den virtuellen Server gebunden, mit dem der Client Transaktionen durchführt.

Wenn das Zertifikat gültig ist, ermöglicht die Appliance dem Client den Zugriff auf alle sicheren Ressourcen. Wenn das Zertifikat jedoch ungültig ist, löscht die Appliance die Clientanforderung während des SSL-Handshakes.

Die Appliance überprüft das Clientzertifikat, indem sie zuerst eine Kette von Zertifikaten bildet, beginnend mit dem Clientzertifikat und endend mit dem Stammzertifizierungsstellenzertifikat für den Client (z. B. Verisign). Das Stammzertifizierungsstellenzertifikat kann ein oder mehrere zwischengeschaltete CA-Zertifikate enthalten (wenn die Stammzertifizierungsstelle das Clientzertifikat nicht direkt ausstellt).

Bevor Sie die Clientauthentifizierung auf der NetScaler-Appliance aktivieren, stellen Sie sicher, dass ein gültiges Clientzertifikat auf dem Client installiert ist. Aktivieren Sie dann die Clientauthentifizierung für den virtuellen Server, der die Transaktionen abwickelt. Binden Sie abschließend das Zertifikat der Zertifizierungsstelle, die das Clientzertifikat ausgestellt hat, an den virtuellen Server auf der Appliance.

Hinweis: Eine NetScaler MPX-Appliance unterstützt eine Zertifikatsschlüsselpaargröße von 512 Bit bis 4096 Bit. Das Zertifikat muss mit einem der folgenden Hash-Algorithmen signiert werden:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Wenn auf einer SDX-Appliance ein SSL-Chip einer VPX-Instanz zugewiesen ist, gilt die Unterstützung der Zertifikatsschlüsselpaargröße einer MPX-Appliance. Andernfalls gilt die normale Unterstützung der Zertifikat-Schlüssel-Paargröße einer VPX-Instanz.

Eine virtuelle NetScaler-Appliance (VPX-Instanz) unterstützt Zertifikate mit mindestens 512 Bit bis zu

den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat
- 4096-Bit-Zertifikat auf dem physischen Server

Die folgende Tabelle zeigt die von NetScaler unterstützten RSASSA-PSS-Parametersätze. RSASSA-PSS-Algorithmen werden bei der X.509-Zertifikatspfadvalidierung unterstützt.

OID für öffentlichen Schlüssel	Maskengenerierungsfunktion (MGF)	MGF-Digest-Funktion	Signature-Digest-Funktion	Salt-Länge
rsaEncryption	MGF1	SHA-256	SHA-256	32 Byte
rsaEncryption	MGF1	SHA-384	SHA-384	48 Byte
rsaEncryption	MGF1	SHA-512	SHA-512	64 Byte

Hinweise:

- Informationen zu MPX FIPS-Einschränkungen finden Sie unter Einschränkungen bei MPX FIPS.
- Informationen zu SDX FIPS-Einschränkungen finden Sie unter SDX FIPS-Einschränkungen.

Bereitstellen des Clientzertifikats

Bevor Sie die Clientauthentifizierung konfigurieren, muss ein gültiges Clientzertifikat auf dem Client installiert sein. Ein Clientzertifikat enthält Details zum spezifischen Clientsystem, das sichere Sitzungen mit der NetScaler-Appliance erstellt. Jedes Clientzertifikat ist eindeutig und darf nur von einem Clientsystem verwendet werden.

Unabhängig davon, ob Sie das Clientzertifikat von einer Zertifizierungsstelle erhalten, ein vorhandenes Clientzertifikat verwenden oder ein Clientzertifikat auf der NetScaler-Appliance generieren, müssen Sie das Zertifikat in das richtige Format konvertieren. Auf der NetScaler-Appliance werden Zertifikate entweder im PEM- oder DER-Format gespeichert und müssen in das PKCS #12 -Format konvertiert werden, bevor sie auf dem Clientsystem installiert werden. Nachdem Sie das Zertifikat konvertiert und auf das Clientsystem übertragen haben, stellen Sie sicher, dass es auf diesem System installiert und für die Clientanwendung konfiguriert ist. Die Anwendung, z. B. ein Webbrowser, muss Teil der SSL-Transaktionen sein.

Anweisungen zum Konvertieren eines Zertifikats aus dem PEM- oder DER-Format in das PKCS #12 -Format finden Sie unter Importieren und Konvertieren von SSL-Dateien.

Anweisungen zum Generieren eines Clientzertifikats finden Sie unter Erstellen eines Zertifikats.

Aktivieren der clientzertifikatbasierten Authentifizierung

Standardmäßig ist die Clientauthentifizierung auf der NetScaler-Appliance deaktiviert, und alle SSL-Transaktionen werden ohne Authentifizierung des Clients ausgeführt. Sie können die Clientauthentifizierung so konfigurieren, dass sie im Rahmen des SSL-Handshakes entweder optional oder obligatorisch ist.

Wenn die Clientauthentifizierung optional ist, fordert die Appliance das Clientzertifikat an, fährt jedoch mit der SSL-Transaktion fort, auch wenn der Client ein ungültiges Zertifikat vorlegt. Wenn die Clientauthentifizierung erforderlich ist, beendet die Appliance den SSL-Handshake, wenn der SSL-Client kein gültiges Zertifikat bereitstellt.

Vorsicht: Citrix empfiehlt, dass Sie die richtigen Zugriffssteuerungsrichtlinien definieren, bevor Sie die clientzertifikatbasierte Authentifizierungsprüfung auf optional ändern.

Hinweis: Die Clientauthentifizierung ist für einzelne virtuelle SSL-Server konfiguriert, nicht global.

Clientzertifikatsbasierte Authentifizierung über die CLI aktivieren

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die clientzertifikatbasierte Authentifizierung zu aktivieren und die Konfiguration zu überprüfen:

```
set ssl vserver <vServerName> [-clientAuth (ENABLED | DISABLED)] [-
   clientCert (MANDATORY | OPTIONAL)]
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vssl -clientAuth ENABLED -clientCert Mandatory
Done
show ssl vserver vssl

Advanced SSL configuration for VServer vssl:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
```



```
17          HSTS: DISABLED
18          HSTS IncludeSubDomains: NO
19          HSTS Max-Age: 0
20 SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.2: ENABLED TLSv1
       .2: ENABLED
21
22 1) CertKey Name: sslckey Server Certificate
23
24 1) Policy Name: client_cert_policy Priority: 0
25
26 1) Cipher Name: DEFAULT
27 Description: Predefined Cipher Alias
28 Done
29 <!--NeedCopy-->
```

Clientzertifikatsbasierte Authentifizierung über die GUI aktivieren

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Client-Authentifizierung**und in der Liste des **Client-Zertifikats** die Option **Obligatorisch**aus.

> **Hinweis:**
>
> Wenn die Clientauthentifizierung auf obligatorisch festgelegt ist und das Clientzertifikat Richtlinienerweiterungen enthält, schlägt die Zertifikatsüberprüfung fehl. Stellen Sie im Front-End-SSL-Profil einen Parameter ein, um diese Prüfung zu überspringen. Der Parameter ist standardmäßig deaktiviert. Das heißt, die Prüfung wird standardmäßig durchgeführt.

Überspringen Sie die Überprüfung der Richtlinienerweiterung während der Clientauthentifizierung über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

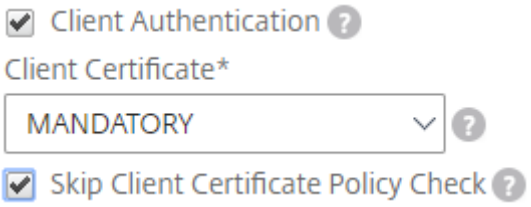
```
1 set ssl profile ns_default_ssl_profile_frontend -clientauth ENABLED -
     skipClientCertPolicyCheck ENABLED
2
3 Parameter
4
5 skipClientCertPolicyCheck
6
7               Control policy extension check, if present inside the
                   X509 certificate chain. Applicable only if client
```



```
                    authentication is enabled and client certificate is
                    set to mandatory. Possible values functions as follows
                    :

- ENABLED: Skip the policy check during client authentication.

- DISABLED: Perform policy check during client authentication.

Possible values: ENABLED, DISABLED

Default: DISABLED
<!--NeedCopy-->
```

Überspringen Sie die Überprüfung der Richtlinienerweiterung während der Clientauthentifizierung über die GUI

1. Navigieren Sie zu **System** > **Profile** > **SSL-Profile**.
2. Erstellen Sie ein neues Front-End-Profil oder bearbeiten Sie ein vorhandenes Front-End-Profil.
3. Stellen Sie sicher, dass die Clientauthentifizierung aktiviert und das Clientzertifikat auf obligatorisch festgelegt ist
4. Wählen Sie **Überprüfung der Clientzertifikatrichtlinie überspringen**.



Binden von CA-Zertifikaten an den virtuellen Server

Eine Zertifizierungsstelle, deren Zertifikat auf der NetScaler-Appliance vorhanden ist, muss das für die Clientauthentifizierung verwendete Clientzertifikat ausstellen. Binden Sie dieses Zertifikat an den virtuellen NetScaler-Server, der die Clientauthentifizierung durchführt.

Binden Sie das CA-Zertifikat so an den virtuellen SSL-Server, dass die Appliance bei der Überprüfung des Clientzertifikats eine vollständige Zertifikatkette bilden kann. Andernfalls schlägt die Bildung der Zertifikatkette fehl und dem Client wird der Zugriff verweigert, auch wenn sein Zertifikat gültig ist.

Sie können CA-Zertifikate in beliebiger Reihenfolge an den virtuellen SSL-Server binden. Die Appliance bildet bei der Überprüfung des Clientzertifikats die richtige Reihenfolge.

Wenn der Client beispielsweise ein von **CA_A**ausgestelltes Zertifikat vorlegt, wobei **CA_A eine**Zwischenzertifizierungsstelle ist, deren Zertifikat von **CA_B**ausgestellt wird, dessen Zerti-

fikat wiederum von einer vertrauenswürdigen Stammzertifizierungsstelle, **Root_CA**, einer Kette von Zertifikaten, die Alle drei Zertifikate müssen an den virtuellen Server der NetScaler-Appliance gebunden sein.

Anweisungen zum Binden eines oder mehrerer Zertifikate an den virtuellen Server finden Sie unter Binden des Zertifikatschlüsselpaars an den virtuellen SSL-Server.

Anweisungen zum Erstellen einer Zertifikatkette finden Sie unter Erstellen einer Zertifikatkette.

Strengere Kontrolle der Validierung von Clientzertifikaten

Die NetScaler-Appliance akzeptiert gültige Zwischen-CA-Zertifikate, wenn sie von einer einzelnen Root-CA ausgestellt werden. Das heißt, wenn nur das Root-CA-Zertifikat an den virtuellen Server gebunden ist und diese Root-CA jedes mit dem Clientzertifikat gesendete Zwischenzertifikat validiert, vertraut die Appliance der Zertifikatkette und der Handshake ist erfolgreich.

Wenn ein Client jedoch eine Kette von Zertifikaten im Handshake sendet, kann keines der Zwischenzertifikate mithilfe eines CRL- oder OCSP-Responders validiert werden, es sei denn, dieses Zertifikat ist an den virtuellen SSL-Server gebunden. Selbst wenn eines der Zwischenzertifikate widerrufen wird, ist der Handshake daher erfolgreich. Im Rahmen des Handshakes sendet der virtuelle SSL-Server die Liste der an ihn gebundenen CA-Zertifikate. Für eine strengere Kontrolle können Sie den virtuellen SSL-Server so konfigurieren, dass er nur ein Zertifikat akzeptiert, das von einem der an diesen virtuellen Server gebundenen CA-Zertifikate signiert ist. Dazu müssen Sie die Einstellung **ClientAuthUseBoundCAChain** im an den virtuellen Server gebundenen SSL-Profil aktivieren. Der Handshake schlägt fehl, wenn eines der an den virtuellen Server gebundenen CA-Zertifikate das Clientzertifikat nicht signiert hat.

Beispiel: Zwei Clientzertifikate, clientcert1 und clientcert2, werden von den Zwischenzertifikaten Int-CA-A bzw. int-CA-B signiert. Die Zwischenzertifikate sind vom Stammzertifikat Root-CA signiert. Int-CA-A und Root-CA sind an den virtuellen SSL-Server gebunden. Im Standardfall (ClientAuthUseBoundCAChain deaktiviert) werden sowohl clientcert1 als auch clientcert2 akzeptiert. Wenn ClientAuthUseBoundCAChain jedoch aktiviert ist, akzeptiert die NetScaler-Appliance nur clientcert1.

Ermöglichen Sie eine strengere Kontrolle der Clientzertifikatvalidierung über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -ClientAuthUseBoundCAChain Enabled
<!--NeedCopy-->
```


Ermöglichen Sie eine strengere Kontrolle der Validierung von Clientzertifikaten über die GUI

1. Navigieren Sie zu **System** > **Profile**, wählen Sie die Registerkarte **SSL-Profile** und erstellen Sie ein SSL-Profil oder wählen Sie ein vorhandenes Profil aus.
2. Wählen Sie **Client-Authentifizierung mit gebundener Zertifizierungsstellenkette**aktivieren aus.

Serverauthentifizierung

August 15, 2023

Da die NetScaler Appliance SSL-Offload und -Beschleunigung im Namen eines Webservers durchführt, authentifiziert die Appliance normalerweise nicht das Zertifikat des Webservers. Sie können den Server jedoch in Bereitstellungen authentifizieren, die eine End-to-End-SSL-Verschlüsselung erfordern.

In einer solchen Situation wird die Appliance zum SSL-Client und führt eine sichere Transaktion mit dem SSL-Server durch. Es überprüft, ob eine CA, deren Zertifikat an den SSL-Dienst gebunden ist, das Serverzertifikat signiert hat, und überprüft die Gültigkeit des Serverzertifikats.

Um den Server zu authentifizieren, aktivieren Sie die Serverauthentifizierung und binden Sie das Zertifikat der Zertifizierungsstelle, die das Serverzertifikat signiert hat, an den SSL-Dienst auf der ADC-Appliance. Beim Binden des Zertifikats müssen Sie die Bindung als CA-Option angeben.

NetScaler unterstützt die Validierung von signierten Zertifikaten. Das heißt, wenn ein Zertifikat von mehreren Ausstellern signiert wurde, ist die Überprüfung erfolgreich, wenn mindestens ein gültiger Pfad zum Stammzertifikat vorhanden ist. Wenn in Version 13.1 Build 42.x und früher eines der Zertifikate in der Zertifikatskette quersigniert war und mehrere Pfade zum Stammzertifikat hatte, suchte die Appliance nur nach einem Pfad. Und wenn dieser Pfad nicht gültig war, schlug die Überprüfung fehl.

Serverzertifikatauthentifizierung aktivieren (oder deaktivieren)

Sie können die CLI und die GUI verwenden, um die Serverzertifikatauthentifizierung zu aktivieren und zu deaktivieren.

Aktivieren (oder deaktivieren) Sie die Serverzertifikatauthentifizierung mit der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Serverzertifikatsauthentifizierung zu aktivieren und die Konfiguration zu überprüfen:


```
set ssl service <serviceName> -serverAuth ( ENABLED | DISABLED )
show ssl service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl service ssl-service-1 -serverAuth ENABLED

show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
                service-1:`
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
    1)      Cipher Name: ALL
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Aktivieren (oder deaktivieren) Sie die Serverzertifikatauthentifizierung mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**und öffnen Sie einen SSL-Dienst.
2. Wählen Sie im Abschnitt SSL-Parameter die Option Serverauthentifizierung aktivieren aus und geben Sie einen allgemeinen Namen an.
3. Wählen Sie unter Erweiterte Einstellungen die Option Zertifikate aus und binden Sie ein CA-Zertifikat an den Dienst.

Binden Sie das CA-Zertifikat mithilfe der CLI an den Dienst

Geben Sie an der Befehlszeile die folgenden Befehle ein, um das CA-Zertifikat an den Dienst zu binden und die Konfiguration zu überprüfen:

```
bind ssl service <serviceName> -certkeyName <string> -CA

```



```
show ssl service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind ssl service ssl-service-1 -certkeyName samplecertkey -CA

show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
               service-1:
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
    1)      CertKey Name: samplecertkey     CA Certificate
       CRLCheck: Optional
    1)      Cipher Name: ALL
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Konfigurieren Sie einen allgemeinen Namen für die Serverzertifikatauthentifizierung

Bei der Ende-zu-Ende-Verschlüsselung mit aktivierter Serverauthentifizierung können Sie einen allgemeinen Namen in die Konfiguration eines SSL-Dienstes oder einer Dienstgruppe aufnehmen. Der von Ihnen angegebene Name wird während eines SSL-Handshakes mit dem allgemeinen Namen im Serverzertifikat verglichen. Stimmen die beiden Namen überein, ist der Handshake erfolgreich.
Wenn die allgemeinen Namen nicht übereinstimmen, wird der für den Dienst oder die Dienstgruppe angegebene allgemeine Name mit den Werten im Feld Subject Alternative Name (SAN) im Zertifikat verglichen. Wenn es mit einem dieser Werte übereinstimmt, ist der Handshake erfolgreich. Diese Konfiguration ist besonders nützlich, wenn sich beispielsweise zwei Server hinter einer Firewall befinden und einer der Server die Identität des anderen vortäuscht. Wenn der allgemeine Name nicht aktiviert ist, wird ein von einem der Server vorgelegten Zertifikate akzeptiert, sofern die IP-Adresse übereinstimmt.

Hinweis: Nur die DNS-Einträge für Domainname, URL und E-Mail-ID im SAN-Feld werden verglichen.

Konfigurieren Sie die Überprüfung allgemeiner Namen für einen SSL-Dienst oder eine Dienstgruppe mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Serverauthentifizierung mit Common-Name-Verifizierung festzulegen und die Konfiguration zu überprüfen:

1. Um einen allgemeinen Namen in einem Dienst zu konfigurieren, geben Sie Folgendes ein:

```
set ssl service <serviceName> -commonName <string> -serverAuth
   ENABLED
show ssl service <serviceName>
<!--NeedCopy-->
```

2. Um einen allgemeinen Namen in einer Dienstgruppe zu konfigurieren, geben Sie Folgendes ein:

```
set ssl serviceGroup <serviceGroupName> -commonName <string> -
   serverAuth ENABLED
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl service svc1 -commonName xyz.com -serverAuth ENABLED

show ssl service svc

     Advanced SSL configuration for Back-end SSL Service svc1:
     DH: DISABLED
     Ephemeral RSA: DISABLED
     Session Reuse: ENABLED Timeout: 300 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     Server Auth: ENABLED Common Name: www.xyz.com
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: DISABLED
     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
    1) CertKey Name: cacert CA Certificate OCSPCheck: Optional
    1) Cipher Name: ALL
     Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```


Konfigurieren Sie die Überprüfung allgemeiner Namen für einen SSL-Dienst oder eine Dienstgruppe mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services** oder navigieren Sie zu **Traffic Management > Load Balancing > Service Groups**und öffnen Sie einen Dienst oder eine Dienstgruppe.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Serverauthentifizierung aktivieren**aus und geben Sie einen allgemeinen Namen an.

SSL-Aktionen und Richtlinien

May 11, 2023

Eine SSL-Richtlinie wertet eingehenden Datenverkehr aus und wendet eine vordefinierte Aktion auf Anforderungen an, die einer Regel entsprechen (Ausdruck). Konfigurieren Sie die Aktionen, bevor Sie die Richtlinien erstellen, damit Sie beim Erstellen einer Richtlinie eine Aktion angeben können. Um eine Richtlinie in Kraft zu setzen, führen Sie einen der folgenden Schritte aus:

- Binden Sie die Richtlinie an einen virtuellen Server auf der Appliance, sodass sie nur für den Datenverkehr gilt, der durch diesen virtuellen Server fließt.
- Binden Sie die Richtlinie global, sodass sie für den gesamten Datenverkehr gilt, der durch die Appliance fließt.

SSL-Aktionen definieren SSL-Einstellungen, die Sie auf die ausgewählten Anforderungen anwenden können. Sie verknüpfen eine Aktion mit einer oder mehreren Richtlinien. Daten in Clientverbindungsanforderungen oder -antworten werden mit einer in der Richtlinie angegebenen Regel verglichen, und die Aktion wird auf Verbindungen angewendet, die der Regel entsprechen (Ausdruck).

Sie können klassische Richtlinien mit klassischen Ausdrücken und erweiterten Richtlinienrichtlinien mit erweiterten Richtlinienausdrücken für SSL konfigurieren.

Hinweis: Benutzer, die keine Erfahrung mit der Konfiguration von Richtlinien an der CLI haben, empfinden es normalerweise als erheblich einfacher, das Konfigurationsdienstprogramm zu verwenden.

Sie können eine benutzerdefinierte Aktion oder eine integrierte Aktion einer erweiterten Richtlinie zuordnen. Klassische Richtlinien erlauben nur benutzerdefinierte Aktionen. In der erweiterten Policy Label können Sie Richtlinien auch unter einer Richtlinienbezeichnung gruppieren. In diesem Fall werden sie nur angewendet, wenn sie von einer anderen Richtlinie aufgerufen werden.

Zu den gängigen Anwendungen von SSL-Aktionen und -Richtlinien gehören Clientauthentifizierung pro Verzeichnis, Unterstützung für Outlook-Webzugriff und SSL-basierte Header-Einfügungen. SSL-

basierte Header-Einfügungen enthalten SSL-Einstellungen, die von einem Server benötigt werden, dessen SSL-Verarbeitung an die NetScaler-Appliance ausgelagert wurde.

SSL-Richtlinien

May 11, 2023

Richtlinien auf der NetScaler-Appliance helfen dabei, bestimmte Verbindungen zu identifizieren, die Sie verarbeiten möchten. Die Verarbeitung basiert auf den Aktionen, die für diese bestimmte Richtlinie konfiguriert sind. Sobald Sie die Richtlinie erstellt und eine Aktion dafür konfiguriert haben, müssen Sie einen der folgenden Schritte ausführen:

- Binden Sie die Richtlinie an einen virtuellen Server auf der Appliance, sodass sie nur für den Datenverkehr gilt, der durch diesen virtuellen Server fließt.
- Binden Sie die Richtlinie global, sodass sie für den gesamten Datenverkehr gilt, der über einen virtuellen Server fließt, der auf der NetScaler-Appliance konfiguriert ist.

Die SSL-Funktion der NetScaler-Appliance unterstützt erweiterte Richtlinien (erweiterte) Richtlinien. Eine vollständige Beschreibung der erweiterten Richtlinienausdrücke, ihrer Funktionsweise und ihrer manuellen Konfiguration finden Sie unter Richtlinien und Ausdrücke. Weitere Informationen zu SSL-Ausdrücken finden Sie unter Erweiterte Richtlinienausdrücke: SSL parsen.

> **Hinweis:**
>
> Benutzer, die keine Erfahrung mit der Konfiguration von Richtlinien an der CLI haben, finden die Verwendung des Konfigurationsdienstprogramms normalerweise erheblich einfacher.

SSL-Richtlinien erfordern, dass Sie vor dem Erstellen einer Richtlinie eine Aktion erstellen, damit Sie die Aktionen beim Erstellen der Richtlinien angeben können.
In erweiterten SSL-Richtlinien können Sie auch die integrierten Aktionen verwenden. Weitere Informationen zu integrierten Aktionen finden Sie unter Integrierte SSL-Aktionen und benutzerdefinierte Aktionen.

Erweiterte SSL-Richtlinien

Eine SSL Advanced-Richtlinie, auch als erweiterte Richtlinie bezeichnet, definiert ein Steuerelement oder eine Datenaktion, die bei Anfragen ausgeführt werden soll. SSL-Richtlinien können daher als Steuerungsrichtlinien und Datenrichtlinien eingestuft werden:

- **Steuerungsrichtlinie**. Eine Steuerungsrichtlinie verwendet eine Steuerungsaktion, z. B. das Erzwingen der Clientauthentifizierung.
  Hinweis: In Version 10.5 oder höher ist SSL-Neuverhandlung verweigern (denySSLReneg)

standardmäßig auf ALL gesetzt. Steuerungsrichtlinien wie CLIENTAUTH lösen jedoch einen Handshake für Neuverhandlungen aus. Wenn Sie solche Richtlinien verwenden, müssen Sie denySSLReneg auf NEIN setzen.

- **Richtlinie zu Daten**. Eine Datenrichtlinie verwendet eine Datenaktion, z. B. das Einfügen einiger Daten in die Anforderung.

Die wesentlichen Bestandteile einer Richtlinie sind ein Ausdruck und eine Handlung. Der Ausdruck identifiziert die Anforderungen, für die die Aktion ausgeführt werden soll.

Sie können eine erweiterte Richtlinie mit einer integrierten Aktion oder einer benutzerdefinierten Aktion konfigurieren. Sie können eine Richtlinie mit einer integrierten Aktion konfigurieren, ohne eine separate Aktion zu erstellen. Um jedoch eine Richtlinie mit einer benutzerdefinierten Aktion zu konfigurieren, konfigurieren Sie zuerst die Aktion und konfigurieren Sie dann die Richtlinie.

Sie können eine zusätzliche Aktion angeben, die als UNDEF-Aktion bezeichnet wird und ausgeführt wird, wenn das Anwenden des Ausdrucks auf eine Anforderung ein undefiniertes Ergebnis hat.

Konfiguration der SSL-Richtlinie

Sie können eine SSL Advanced-Richtlinie über die CLI und der GUI konfigurieren.

Konfigurieren einer SSL-Richtlinie über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add ssl policy <name> -rule <expression> -Action <string> [-undefAction
      <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Konfigurieren einer SSL-Richtlinie über die GUI

Navigieren Sie zu **Traffic Management > SSL > Richtlinien** und klicken Sie auf der Registerkarte **Richtlinien** auf *Hinzufügen*.

Unterstützung für SSL-Richtlinien mit TLS1.3-Protokoll

Ab Version 13.0 Build 71.x und höher wird Unterstützung für SSL-Richtlinien mit dem TLS1.3-Protokoll hinzugefügt. Wenn das TLSv1.3-Protokoll für eine Verbindung ausgehandelt wird, lösen Richtlinienregeln, die vom Client empfangene TLS-Daten überprüfen, jetzt die konfigurierte Aktion aus.

Wenn die folgende Richtlinienregel beispielsweise den Wert „Wahr“ zurückgibt, wird der Datenverkehr an den in der Aktion definierten virtuellen Server weitergeleitet.


```
add ssl action action1 -forward vserver2
add ssl policy pol1 -rule client.ssl.client_hello.sni.contains( “xyz” )
    -action action1
<!--NeedCopy-->
```

Einschränkungen

- Steuerungsrichtlinien werden nicht unterstützt.
- Die folgenden Aktionen werden nicht unterstützt:
  - DOCLIENTAUTH
  - NOCLIENTAUTH
  - caCertGrpName
  - clientCertVerification
  - ssllogProfile

Integrierte SSL-Aktionen und benutzerdefinierte Aktionen

May 11, 2023

Sofern Sie nicht nur die in Ihren Richtlinien integrierten Aktionen benötigen, müssen Sie die Aktionen erstellen, bevor Sie die Richtlinien erstellen. Anschließend können Sie die Aktionen angeben, wenn Sie die Richtlinien erstellen. Es gibt zwei Arten von integrierten Aktionen: Kontrollaktionen und Datenaktionen. Sie verwenden Kontrollaktionen in Kontrollrichtlinien und Datenaktionen in Datenrichtlinien.

Die integrierten Steueraktionen sind:

- doClientAuth — Führt die Authentifizierung des Client-Zertifikats durch. (Nicht unterstützt für TLS1.3)
- noClientAuth — Führen Sie keine Authentifizierung mit dem Client-Zertifikat durch. (Nicht unterstützt für TLS1.3)

Die integrierten Datenaktionen sind:

- ZURÜCKSETZEN — Beenden Sie die Verbindung, indem Sie ein RST-Paket an den Client senden.
- Löschen — Löscht alle Pakete vom Client. Die Verbindung bleibt geöffnet, bis der Client sie schließt.
- NOOP — leitet das Paket weiter, ohne eine Operation daran durchzuführen.

Hinweis: Alle von der Client-Authentifizierung abhängigen Aktionen wie ClientCertVerification und SSLLogProfile werden vom TLS 1.3-Protokoll nicht unterstützt.

Sie können benutzerdefinierte Datenaktionen erstellen. Wenn Sie die Client-Authentifizierung aktivieren, können Sie eine SSL-Aktion erstellen, um Client-Zertifikatsdaten in den Anforderungsheader einzufügen, bevor die Anfrage an den Webserver weitergeleitet wird.

Wenn eine politische Bewertung zu einem undefinierten Zustand führt, wird eine UNDEF-Aktion durchgeführt. Sie können entweder für eine Datenrichtlinie oder eine Kontrollrichtlinie RESET, DROP oder NOOP als UNDEF-Aktion angeben. Für eine Kontrollrichtlinie haben Sie auch die Möglichkeit, DOCLIENTAUTH oder NOCLIENTAUTH anzugeben.

Beispiele für integrierte Aktionen in einer Richtlinie

Wenn der Client im folgenden Beispiel eine andere Chiffre als eine Verschlüsselung der Kategorie EXPORT sendet, fordert die NetScaler-Appliance eine Client-Authentifizierung an. Der Kunde muss ein gültiges Zertifikat für eine erfolgreiche Transaktion vorlegen.

```
1 add ssl policy pol1 -rule CLIENT.SSL.CIPHER_EXPORTABLE.NOT -reqAction
     DOCLIENTAUTH
2 <!--NeedCopy-->
```

In den folgenden Beispielen wird davon ausgegangen, dass die Client-Authentifizierung aktiviert ist.

Wenn die Version im vom Benutzer bereitgestellten Zertifikat mit der Version in der Richtlinie übereinstimmt, wird nichts unternommen und das Paket wird weitergeleitet:

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction NOOP
2 <!--NeedCopy-->
```

Wenn die Version im vom Benutzer bereitgestellten Zertifikat mit der Version in der Richtlinie übereinstimmt, wird die Verbindung unterbrochen:

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction DROP
2 <!--NeedCopy-->
```

Wenn die Version im vom Benutzer bereitgestellten Zertifikat mit der Version in der Richtlinie übereinstimmt, wird die Verbindung zurückgesetzt:

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction RESET
2 <!--NeedCopy-->
```


Überprüfung von Client-Zertifikaten mit richtlinienbasierter Client-Authentifizierung

Sie können die Überprüfung des Client-Zertifikats auf „Obligatorisch“ oder „Option“ setzen, wenn Sie die richtlinienbasierte Client-Authentifizierung konfiguriert haben. Die Standardeinstellung ist obligatorisch.

Stellen Sie die Überprüfung des Client-Zertifikats mithilfe der CLI auf optional ein

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add ssl action <name> ((-clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) [-
     clientCertVerification ( Mandatory | Optional )]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ssl action sslact -clientauth DOCLIENTAUTH -clientcertverification
     OPTIONAL
2 <!--NeedCopy-->
```

Stellen Sie die Überprüfung des Client-Zertifikats mithilfe der GUI auf optional ein

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.
2. Klicken Sie auf der Registerkarte **SSL-Aktionen** auf **Hinzufügen**.
3. Geben Sie einen Namen an und wählen Sie in der Liste der **Client-Zertifikatsüberprüfung** die Option **Optional**aus.

Benutzerdefinierte SSL-Aktionen

Zusätzlich zu den integrierten Aktionen können Sie je nach Bereitstellung auch andere SSL-Aktionen konfigurieren. Diese Aktionen werden als benutzerdefinierte Aktionen bezeichnet.

Konfigurieren Sie eine benutzerdefinierte SSL-Aktion mithilfe der CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Aktion zu konfigurieren und die Konfiguration zu überprüfen:

```
1 add SSL action <name> -clientAuth(DOCLIENTAUTH | NOCLIENTAUTH) -
     clientCert (ENABLED | DISABLED) certHeader <string> -clientHeader <
     string> -clientCertSerialNumber (ENABLED | DISABLED) -
     certSerialHeader <string> -clientCertSubject (ENABLED | DISABLED) -
     certSubjectHeader <string> -clientCertHash (ENABLED | DISABLED) -
```



```
    certHashHeader <string> -clientCertIssuer (ENABLED | DISABLED) -
    certIssuerHeader <string> -sessionID (ENABLED | DISABLED) -
    sessionIDheader <string> -cipher (ENABLED | DISABLED) -cipherHeader
    <string> -clientCertNotBefore (ENABLED | DISABLED) -
    certNotBeforeHeader <string> -clientCertNotAfter (ENABLED | DISABLED
    ) -certNotAfterHeader <string> -OWASupport (ENABLED | DISABLED)
<!--NeedCopy-->
```

```
show ssl action [<name>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl action Action-SSL-ClientCert -clientCert ENABLED -certHeader "X
    -Client-Cert"
<!--NeedCopy-->
```

```
show ssl action Action-SSL-ClientCert

1)      Name: Action-SSL-ClientCert
        Data Insertion Action:
        Cert Header: ENABLED            Cert Tag: X-Client-Cert
Done
<!--NeedCopy-->
```

Konfigurieren Sie eine benutzerdefinierte SSL-Aktion mithilfe der GUI

Navigieren Sie zu **Traffic Management > SSL > Richtlinien**, und klicken Sie auf der Registerkarte **Aktionen** auf **Hinzufügen**.

Konfigurieren Sie eine SSL-Aktion, um den Client-Verkehr an einen anderen virtuellen Server weiterzuleiten

Administratoren können eine SSL-Aktion konfigurieren, um den auf einem virtuellen SSL-Server empfangenen Client-Datenverkehr an einen anderen virtuellen Server weiterzuleiten, um SSL-Offloading zu vermeiden. Oder zum Beenden der Verbindung auf der ADC-Appliance. Dieser virtuelle Server kann vom Typ SSL, TCP oder SSL_BRIDGE sein. Administratoren können sich beispielsweise dafür entscheiden, die Anfrage zur weiteren Bearbeitung an einen anderen virtuellen Server weiterzuleiten, anstatt die Verbindung zu beenden, wenn einer der folgenden Fälle vorliegt:

- Die Appliance hat kein Zertifikat.
- Die Appliance unterstützt keine bestimmte Chiffre.

Um dies zu erreichen, wird ein neuer Bindpunkt 'CLIENTHELLO_REQ' hinzugefügt, um den Client-Verkehr auszuwerten, wenn ein Client-Hallo empfangen wird. Wenn die Richtlinie, die an den virtuellen Server gebunden ist, der den Client-Verkehr empfängt, nach dem Parsen des Client-Hello als wahr bewertet wird, wird der Datenverkehr an einen anderen virtuellen Server weitergeleitet. Wenn dieser virtuelle Server vom Typ SSL ist, führt er den Handshake durch. Wenn dieser virtuelle Server vom Typ TCP oder SSL_BRIDGE ist, führt der Backend-Server den Handshake durch.

In Version 12.1-49.x werden nur die Vorwärts- und Reset-Aktionen für den CLIENTHELLO_REQ-Bindpunkt unterstützt. Die folgenden Ausdruckspräfixe sind verfügbar:

- CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
- CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION
- CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE
- CLIENT.SSL.CLIENT_HELLO.IS_REUSE
- CLIENT.SSL.CLIENT_HELLO.IS_SCSV
- CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET
- CLIENT.SSL.CLIENT_HELLO.LENGTH
- CLIENT.SSL.CLIENT_HELLO.SNI
- CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPROTOCOL (from release 13.0 build 61.x)

Eine Beschreibung dieser Präfixe finden Sie unter Erweiterte Richtlinienausdrücke: Parsing SSL.

Dem Befehl `add SSL action` wird ein Parameter `forward` hinzugefügt, und dem Befehl `bind ssl vserver` wird ein neuer Bindpunkt `CLIENTHELLO_REQ` hinzugefügt.

Konfiguration mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add ssl action <name> -forward <virtual server name>

add ssl policy <name> -rule <expression> -action <string>

bind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type <type>
<!--NeedCopy-->
```

BEISPIEL:

```
add ssl action act1 -forward v2

add ssl policy pol1 -rule client.ssl.client_hello.ciphers.has_hexcode(0
    x002f) -action act1

bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
```



```
<!--NeedCopy-->
```

Konfiguration mit der GUI

Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.

SSL-Aktion erstellen:

1. Klicken Sie **unter SSL-Aktionen**auf **Hinzufügen**.
2. Geben **Sie unter SSL-Aktion erstellen**einen Namen für die Aktion an.
3. Wählen Sie unter **Forward Action Virtual Server**einen vorhandenen virtuellen Server aus oder fügen Sie einen neuen virtuellen Server hinzu, an den der Datenverkehr weitergeleitet werden soll.
4. Stellen Sie optional weitere Parameter ein.
5. Klicken Sie auf **Erstellen**.

SSL-Richtlinie erstellen:

1. Klicken Sie **unter SSL-Richtlinien**auf **Hinzufügen**.
2. Geben **Sie unter SSL-Richtlinie erstellen**einen Namen für die Richtlinie an.
3. Wählen Sie **unter Aktion**die Aktion aus, die Sie zuvor erstellt haben.
4. Geben Sie im **Ausdruckseditor**die auszuwertende Regel ein.
5. Klicken Sie auf **Erstellen**.

Erstellen oder fügen Sie einen virtuellen Server und eine Bindungsrichtliniehinzu:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Fügen Sie einen virtuellen Server hinzu oder wählen Sie ihn aus.
3. Klicken Sie in **Erweiterte Einstellungen**auf **SSL-Richtlinien**.
4. Klicken Sie in den Abschnitt SSL-Richtlinie.
5. **Wählen Sie unter Richtlinie**auswählen die Richtlinie aus, die Sie zuvor erstellt haben.
6. Geben Sie **unter Richtlinienbindung**eine Priorität für die Richtlinie an.
7. Wählen Sie unter **Typ**die Option **CLIENTHELLO_REQ**aus.
8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Fertig**.

Die End-to-End-Konfiguration für die beliebtesten Anwendungsfälle finden Sie in den folgenden Themen:

- Konfigurieren Sie die SSL-Aktion, um den Clientdatenverkehr weiterzuleiten, wenn die Appliance kein domänenspezifisches (SNI-) Zertifikatbesitzt.
- Konfigurieren Sie eine SSL-Aktion, um den Clientdatenverkehr basierend auf dem Protokoll in der ALPN-Erweiterung der Client-Hallo Nachricht weiterzuleiten.

- Konfigurieren Sie die SSL-Aktion, um den Clientdatenverkehr weiterzuleiten, wenn eine Chiffre auf dem ADC nicht unterstützt wird.

SSL-Aktion zur selektiven Auswahl von Zertifizierungsstellen basierend auf SNI für die Clientauthentifizierung

Sie können in der Client-Zertifikatsanfrage nur die Liste der CAs senden, die auf SNI (Domain) basieren, und nicht die Liste aller CAs, die an einen virtuellen SSL-Server gebunden sind. Wenn beispielsweise ein Client-Hallo empfangen wird, werden nur die CA-Zertifikate gesendet, die auf dem SSL-Richtlinienausdruck basieren (z. B. SNI). Um einen bestimmten Satz von Zertifikaten zu senden, müssen Sie eine CA-Zertifikatsgruppe erstellen. Binden Sie dann diese Gruppe an eine SSL-Aktion und die Aktion an eine SSL-Richtlinie. Wenn die Richtlinie, die an den virtuellen Server gebunden ist, der den Client-Verkehr empfängt, nach dem Parsen des Client-Hello als wahr bewertet wird, wird im Client-Anforderungszertifikat nur eine bestimmte CA-Zertifikatsgruppe gesendet.

Zuvor mussten Sie CA-Zertifikate an einen virtuellen SSL-Server binden. Mit dieser Erweiterung können Sie einfach CA-Zertifikatsgruppen hinzufügen und sie einer SSL-Aktion zuordnen.

Hinweis: Aktivieren Sie die Client-Authentifizierung und SNI auf dem virtuellen SSL-Server. Binden Sie die richtigen SNI-Zertifikate an den virtuellen Server.

Gehen Sie wie folgt vor:

1. Fügen Sie eine CA-Zertifikatsgruppe hinzu.
2. Fügen Sie Zertifikatsschlüsselpaare hinzu.
3. Binden Sie die Zertifikatsschlüsselpaare an diese Gruppe.
4. Fügen Sie eine SSL-Aktion hinzu.
5. Fügen Sie eine SSL-Richtlinie hinzu. Geben Sie die Aktion in der Richtlinie an.
6. Binden Sie die Richtlinie an einen virtuellen SSL-Server. Geben Sie den Bindungspunkt als CLIENTHELLO_REQ an.

Konfiguration mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle nacheinander ein:

```
add ssl caCertGroup <caCertGroupName>
add ssl certkey <certkey_name> -cert <cert> -key <key>
bind ssl caCertGroup <caCertGroupName> <certkey_name>
add ssl action <name> -caCertGrpName <string>
add ssl policy <name> -rule <expression> -action <string>
bind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type CLIENTHELLO_REQ
```



```
<!--NeedCopy-->
```

Beispiel:

```
add ssl cacertGroup ca_cert_group

add ssl certkey ca_certkey1 -cert cacert1 -key cakey1
add ssl certkey ca_certkey2 -cert cacert2 -key cakey2
add ssl certkey snicert -cert snicert -key snikey

bind ssl cacertGroup ca_cert_group ca_certkey1
bind ssl caCertGroup ca_cert_group ca_certkey2
<!--NeedCopy-->
```

```
sh ssl caCertGroup ca_cert_group

CA GROUP NAME:     ca_cert_group
ACTIONS REFERRING: 1

1) CertKey Name: ca_certkey1   CA Certificate   CRLCheck: Optional
   CA_Name Sent
2) CertKey Name: ca_certkey2   CA Certificate   CRLCheck: Optional
   CA_Name Sent
<!--NeedCopy-->
```

```
add ssl action pick_ca_group -cacertGrpName ca_cert_group
<!--NeedCopy-->
```

```
sh ssl action pick_ca_group
1) Name: pick_ca_group
   Type: Data Insertion
   PickCaCertGroup: ca_cert_group
   Hits: 0
   Undef Hits: 0
   Action Reference Count: 1
<!--NeedCopy-->
```

```
add ssl policy snipolicy -rule client.ssl.client_hello.sni.contains("
   abc") -action pick_ca_group
bind ssl vserver v_SSL -policyName snipolicy -type CLIENTHELLO_REQ -
   priority 10
<!--NeedCopy-->
```



```
sh ssl policy snipolicy
    Name: snipolicy
    Rule: client.ssl.client_hello.sni.contains("abc")
    Action: pick_ca_group
    UndefAction: Use Global
    Hits: 0
    Undef Hits: 0


    Policy is bound to following entities
1)  Bound to: CLIENTHELLO_REQ VSERVER v_SSL
    Priority: 10
<!--NeedCopy-->
```

```
set ssl vserver v_SSL -clientauth ENABLED -SNIEnable ENABLED
bind ssl vserver v_SSL -certkeyName snicert -sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v_SSL

    Advanced SSL configuration for VServer v_SSL:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED   Refresh Count: 0
    Session Reuse: ENABLED   Timeout: 120 seconds
    Cipher Redirect: DISABLED
    SSLv2 Redirect: DISABLED
    ClearText Port: 0
    Client Auth: ENABLED   Client Cert Required: Mandatory
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: ENABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED
         TLSv1.2: ENABLED  TLSv1.3: DISABLED
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
```



```
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

1)  CertKey Name: snicert   Server Certificate for SNI


    Data policy
1)  Policy Name: snipolicy  Priority: 10



1)  Cipher Name: DEFAULT
    Description: Default cipher list with encryption strength >= 128bit
<!--NeedCopy-->
```

Konfiguration mit der GUI

Erstellen Sie eine CA-Zertifikatsgruppe und binden Sie Zertifikate an die Gruppe:

1. Navigieren Sie zu **Verkehrsmanagement > SSL > CA Certificates Group**.
2. Klicken Sie auf **Hinzufügen** und geben Sie einen Namen für die Gruppe ein.
3. Klicken Sie auf **Erstellen**.
4. Wählen Sie die **CA-Zertifikatsgruppe** aus und klicken Sie dann auf **Bindungen anzeigen**.
5. Klicken Sie auf **Bind**.
6. Wählen Sie auf der Seite **CA Certificate Binding** ein vorhandenes Zertifikat aus oder klicken Sie auf Hinzufügen, um ein neues Zertifikat hinzuzufügen.
7. Klicken Sie auf **Auswählen** und dann auf **Binden**.
8. Um ein weiteres Zertifikat zu binden, wiederholen Sie die Schritte 5 bis 7.
9. Klicken Sie auf **Schließen**.

Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.

SSL-Aktion erstellen:

1. Klicken Sie **unter SSL-Aktionen**auf **Hinzufügen**.
2. Geben **Sie unter SSL-Aktion erstellen**einen Namen für die Aktion an.
3. Wählen Sie unter **Forward Action Virtual Server**einen vorhandenen virtuellen Server aus oder fügen Sie einen virtuellen Server hinzu, an den der Datenverkehr weitergeleitet werden soll.
4. Stellen Sie optional weitere Parameter ein.
5. Klicken Sie auf **Erstellen**.

SSL-Richtlinie erstellen:

1. Klicken Sie **unter SSL-Richtlinien**auf **Hinzufügen**.

2. Geben **Sie unter SSL-Richtlinie erstellen**einen Namen für die Richtlinie an.
3. Wählen Sie unter **Aktion**die zuvor erstellte Aktion aus.
4. Geben Sie im **Ausdruckseditor**die auszuwertende Regel ein.
5. Klicken Sie auf **Erstellen**.

Erstellen oder fügen Sie einen virtuellen Server und eine Bindungsrichtliniehinzu:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Fügen Sie einen virtuellen Server hinzu oder wählen Sie ihn aus.
3. Klicken Sie in **Erweiterte Einstellungen**auf **SSL-Richtlinien**.
4. Klicken Sie in den Abschnitt SSL-Richtlinie.
5. **Wählen Sie unter Richtlinie**auswählen die Richtlinie aus, die Sie zuvor erstellt haben.
6. Geben Sie **unter Richtlinienbindung**eine Priorität für die Richtlinie an.
7. Wählen Sie unter **Typ**die Option **CLIENTHELLO_REQ**aus.
8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Fertig**.

Entbinden Sie eine CA-Zertifikatsgruppe mithilfe der GUI

1. Navigieren Sie zu **Verkehrsmanagement > SSL > CA Certificates Group**.
2. Wählen Sie eine Zertifikatsgruppe aus und klicken Sie auf **Bindungen anzeigen**.
3. Wählen Sie das Zertifikat aus, das Sie aus der Gruppe entfernen möchten, und klicken Sie auf **Binden aufheben**.
4. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Ja••.
5. Klicken Sie auf **Schließen**.

Entfernen Sie eine CA-Zertifikatsgruppe mithilfe der GUI

1. Navigieren Sie zu **Verkehrsmanagement > SSL > CA Certificates Group**.
2. Wählen Sie eine Zertifikatsgruppe aus und klicken Sie auf **Löschen**.
3. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Ja**.

Bindung von SSL-Richtlinien

May 11, 2023

Sie können SSL-Richtlinien global oder nur an einen virtuellen Server vom Typ SSL binden. Global gebundene Richtlinien werden bewertet, nachdem alle Richtlinien, die an Dienste, virtuelle Server oder andere NetScaler-Bindpunkte gebunden sind, bewertet wurden. Wenn die eingehenden Daten

mit einer der in der SSL-Richtlinie konfigurierten Regeln übereinstimmen, wird die Richtlinie ausgelöst und die damit verbundene Aktion ausgeführt.

Wenn Sie eine SSL-Richtlinie an einen virtuellen Server binden, müssen Sie einen der folgenden Bindungspunkte auswählen:

- ANFRAGE (Standardbindungspunkt). Die Bewertung der Richtlinien erfolgt auf der HTTP-Ebene, nachdem der SSL-Handshake abgeschlossen ist.)
- INTERCEPT_REQ (Diese Option gilt für ein Citrix Secure Web Gateway -Setup. Weitere Informationen finden Sie unter SSL-Richtlinieninfrastruktur für SSL-Abfangen).
- CLIENTHELLO_REQ

In ähnlicher Weise müssen Sie beim Aufheben der Bindung einer Richtlinie von einem virtuellen Server den Bindungspunkt angeben.

Wenn Sie CLIENTHELLO_REQ als Bindungspunkt angeben, wird die Richtlinie ausgewertet, wenn eine Client-Hello-Nachricht empfangen wird. Die erlaubten Aktionen sind RESET, FORWARD und `caCertGrpName`. Die Reset-Aktion beendet die Verbindung. Die Weiterleitungsaktion leitet die Anfrage zur Verarbeitung an einen virtuellen Lastausgleichsserver weiter. Die Aktion wählt `caCertGrpName` selektiv Zertifizierungsstellen basierend auf SNI für die Clientauthentifizierung aus. Weitere Informationen zu SSL-Aktionen finden Sie unter Integrierte SSL-Aktionen und benutzerdefinierte Aktionen.

Hinweis: Die Aktion CacertGrpName wird mit dem TLS 1.3-Protokoll nicht unterstützt.

Binden Sie eine SSL-Richtlinie global mithilfe der CLI

Geben Sie an der Befehlszeile den folgenden Befehl ein, um eine globale SSL-Richtlinie zu binden und die Konfiguration zu überprüfen:

```
bind ssl global - policyName <string> [- priority <positive_integer>]
show ssl global
<!--NeedCopy-->
```

Beispiel:

```
bind ssl global -policyName Policy-SSL-2 -priority 90
Done

sh ssl global

      1) Name: Policy-SSL-2 Priority: 90
      2) Name: Policy-SSL-1 Priority: 100
      Done
```



```
<!--NeedCopy-->
```

Binden Sie eine SSL-Richtlinie global mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**.
3. **Klicken Sie im Dialogfeld**SSL-Richtlinien an Global binden/Unbind auf**Insert Policy.**
4. Wählen Sie in der Liste **Richtlinienname** eine Richtlinie aus.
5. Ziehen Sie den Eintrag optional an eine neue Position in der Policenbank, um die Prioritätsstufe automatisch zu aktualisieren.
6. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich gebunden wurde.

Binden oder entbinden Sie eine SSL-Richtlinie mithilfe der CLI an einen virtuellen Server

Geben Sie an der Befehlszeile den folgenden Befehl ein, um eine SSL-Richtlinie an einen virtuellen Server zu binden und die Konfiguration zu überprüfen:

```
bind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type <type>

unbind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type <type>

<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

```
unbind ssl vserver v1 -policyName pol1 -priority 1 -type
    CLIENTHELLO_REQ
<!--NeedCopy-->
```

```
show ssl vserver vs-server

Advanced SSL configuration for VServer vs-server:

DH: DISABLED

```



```
Ephemeral RSA: ENABLED          Refresh Count: 1000

Session Reuse: ENABLED          Timeout: 120 seconds

Cipher Redirect: DISABLED

SSLv2 Redirect: DISABLED

ClearText Port: 80

Client Auth: DISABLED

SSL Redirect: ENABLED

SSL-REDIRECT Port Rewrite: ENABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Policy Name: ssl-policy-1        Priority: 10

1)      Cipher Name: DEFAULT

            Description: Predefined Cipher Alias

Done
<!--NeedCopy-->
```

Binden Sie mithilfe der GUI eine SSL-Richtlinie an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie einen virtuellen SSL-Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **SSL-Richtlinie**aus. Klicken Sie in den Abschnitt **SSL-Richtlinie**, um eine Richtlinie an den virtuellen Server zu binden.
3. Wählen Sie auf der Seite „ **Richtlinienbindung** “ eine vorhandene Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu.
4. Geben Sie die Priorität und den Typ (Bindungspunkt) für die Richtlinie an.
5. Wählen Sie **Binden**aus.
6. Wählen Sie **Done**.

SSL-Richtlinienbeschriftungen

June 2, 2023

Policy-Labels sind Inhaber von Policen. Ein Richtlinienlabel hilft bei der Verwaltung einer Gruppe von Richtlinien, einer sogenannten Policenbank, die von einer anderen Richtlinie aus aufgerufen werden kann. SSL-Richtlinienlabels können je nach Art der Richtlinien, die im Richtlinienlabel enthalten sind, Kontrolllabels oder Datenlabels sein. Sie können einem Datenrichtlinien-Label nur Datenrichtlinien und einem Kontrollrichtlinien-Label nur Kontrollrichtlinien hinzufügen. Um die Policenbank zu erstellen, binden Sie die Richtlinien an das Label und geben Sie die Reihenfolge an, in der jede Richtlinie im Verhältnis zu anderen Richtlinien in der Policenbank für das Richtlinienlabel bewertet wird. In der CLI geben Sie zwei Befehle ein, um ein Richtlinienlabel zu erstellen und Richtlinien an das Richtlinienlabel zu binden. Im Konfigurationsprogramm wählen Sie Optionen aus einem Dialogfeld aus.

Hinweis: Richtlinienbezeichnungen der Typsteuerung werden vom TLS 1.3-Protokoll nicht unterstützt.

Erstellen Sie ein SSL-Richtlinienlabel und binden Sie Richtlinien mithilfe der CLI an das Label

Geben Sie in der Befehlszeile Folgendes ein:

```
add ssl policylabel <labelName> -type ( CONTROL | DATA )

bind ssl policylabel <labelName> <policyName> <priority> [<
   gotoPriorityExpression>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

Beispiel:

```
add ssl policylabel cpl1 -type CONTROL
add ssl policylabel dpl1 -type DATA

add ssl action act1 -clientauth DOCLIENTAUTH
add ssl policy ctrlpol -rule HTTP.REQ.METHOD.EQ("GET") -action act1

add ssl action act2 -clientCert ENABLED -certHeader "X-Client-Cert"
add ssl policy datapol -rule CLIENT.SSL.CLIENT_CERT.EXISTS -action act2

bind ssl policylabel cpl1 ctrlpol 1
bind ssl policylabel dpl1 datapol 1

> sh ssl policylabel
```



```
Control policylabels
1)    Label Name: cpl1
    Type: CONTROL
    Number of bound policies: 1
    Number of times invoked: 0

Data policylabels
1)  Label Name: dpl1
    Type: DATA
    Number of bound policies: 1
    Number of times invoked: 0
Done
>
<!--NeedCopy-->
```

Konfigurieren Sie ein SSL-Richtlinienlabel und binden Sie Richtlinien mithilfe der GUI an das Label

Navigieren Sie zu **Traffic Management > SSL > Policy Labels** und konfigurieren Sie ein SSL-Policy-Label.

Selektive SSL-Protokollierung

September 28, 2022

In einer großen Bereitstellung mit Tausenden von virtuellen Servern werden alle SSL-bezogenen Informationen protokolliert. Früher war es nicht einfach, die Erfolge und Ausfälle der Clientauthentifizierung und des SSL-Handshakes für einige wichtige virtuelle Server zu filtern. Das Durchsuchen des gesamten Protokolls, um diese Informationen abzurufen, war eine zeitaufwändige und mühsame Aufgabe, da die Infrastruktur nicht die Kontrolle zum Filtern der Protokolle bot. Jetzt können Sie SSL-bezogene Informationen für einen bestimmten virtuellen Server oder für eine Gruppe virtueller Server in der protokollieren `ns.log`. Diese Informationen sind besonders hilfreich beim Debuggen von Fehlern.

Mit der Einstellung DEBUG werden alle SSL-bezogenen Informationen angemeldet `ns.log`. Wenn Sie jedoch ein SSL-Protokollprofil konfigurieren, werden nur Informationen protokolliert, die sich auf die Clientauthentifizierung und den SSL-Handshake beziehen. Führen Sie die folgenden Schritte aus, um diese Informationen zu protokollieren:

1. Setzen Sie DEBUG für Syslog-Parameter.

2. Konfigurieren Sie ein SSL-Protokollprofil. Aktivieren Sie nur die Protokollierung von Client-Authentifizierung und SSL-Handshake-Fehlern/-Erfolg und Fehlern. Alle vier werden protokolliert, wenn Sie das SSL-Protokollprofil an das SSL-Profil anhängen. Nur fehlgeschlagen/erfolgreich bei der Clientauthentifizierung und Fehlschläge werden protokolliert, wenn Sie das SSL-Protokollprofil mit der SSL-Aktion anhängen.
3. Hängen Sie das SSL-Protokollprofil an ein SSL-Profil oder eine SSL-Aktion an.

Eine Beispielausgabe von ns.log für eine erfolgreiche Clientauthentifizierung finden Sie am Ende dieser Seite.

Setze DEBUG-Level

Setzen Sie die Syslog-Protokollebene auf DEBUG. Geben Sie in der Befehlszeile Folgendes ein:

```
set audit syslogParams -logLevel DEBUG
```

Wenn Debug festgelegt ist, sind SSL-Protokolle sowohl für Frontend (virtuelle Server) als auch für Backend (Dienste und Dienstgruppen) enthalten. Die selektive SSL-Protokollierung bietet jedoch nur die Kontrolle über das Frontend.

SSL-Protokollprofil

Ein SSL-Protokollprofil ermöglicht die Protokollierung der folgenden Ereignisse für einen virtuellen Server oder eine Gruppe virtueller Server:

- Erfolgreiche und fehlgeschlagene Clientauthentifizierung oder nur Fehlschläge
- SSL-Handshake erfolgreich und fehlschlägt oder nur Fehlschläge.

Standardmäßig sind alle Parameter deaktiviert.

Ein SSL-Protokollprofil kann in einem SSL-Profil oder in einer SSL-Aktion festgelegt werden. Wenn ein SSL-Profil festgelegt ist, können Sie sowohl die Clientauthentifizierung als auch die Erfolgs- und Fehlerinformationen des SSL-Handshakes protokollieren. Wenn eine SSL-Aktion festgelegt ist, können Sie nur Informationen zum Erfolg und zum Ausfall der Clientauthentifizierung protokollieren, da der Handshake abgeschlossen ist, bevor die Richtlinie ausgewertet wird.

Clientauthentifizierung und Erfolg und Fehler beim SSL-Handshake werden protokolliert, auch wenn Sie kein SSL-Protokollprofil konfigurieren. Eine selektive Protokollierung ist jedoch nur möglich, wenn ein SSL-Protokollprofil verwendet wird.

> **Hinweis:**
>
> Das SSL-Protokollprofil wird in Hochverfügbarkeits- und Cluster-Setups unterstützt.

Hinzufügen eines SSL-Protokollprofils über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )] [-
     ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
     DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

Parameter:

Name:

Name für das SSL-Protokollprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem das Profil erstellt wurde.

Name ist ein zwingendes Argument. Maximale Länge: 127

`sslLogClAuth`:

Protokolliert alle Clientauthentifizierungsereignisse Umfasst sowohl Erfolgs- als auch Misserfolgsereignisse

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

`ssllogClAuthFailures`:

Protokolliert alle Ereignisse bei der Clientauthentifizierung

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

`sslLogHS`:

Protokolliert alle SSL-Handshake-bezogenen Ereignisse. Umfasst sowohl Erfolgs- als auch Misserfolgsereignisse

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

`sslLogHSfailures`:

Protokollieren Sie alle SSL-Handshake-bezogenen Fehler.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

Beispiel:


```
> add ssl logprofile ssllog10 -sslLogClAuth ENABLED -sslLogHS ENABLED

 Done

sh ssllogprofile ssllog10

1)      Name: ssllog10

        SSL log ClientAuth [Success/Failures] : ENABLED

        SSL log ClientAuth [Failures] : DISABLED

        SSL log Handshake [Success/Failures] : ENABLED

        SSL log Handshake [Failures] : DISABLED

 Done
<!--NeedCopy-->
```

Hinzufügen eines SSL-Protokollprofils über die grafische Benutzeroberfläche

Navigieren Sie zu **System > Profile > SSL-Protokollprofil** und fügen Sie ein Profil hinzu.

Ändern eines SSL-Protokollprofils über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )][-
   ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
   DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Beispiel:

```
set ssllogprofile ssllog10 -ssllogClAuth en -ssllogClAuthFailures en -
   ssllogHS en -ssllogHSfailures en

Done

sh ssllogprofile ssllog10

    1)            Name: ssllog10

```



```
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
     Done
<!--NeedCopy-->
```

Ändern eines SSL-Protokollprofils über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Profile > SSL-Protokollprofil**, wählen Sie ein Profil aus und klicken Sie auf **Bearbeiten**.
2. Nehmen Sie Änderungen vor und klicken Sie auf **OK**.

Zeigen Sie alle SSL-Protokollprofile über die CLI an

Geben Sie in der Befehlszeile Folgendes ein:

```
sh ssl logprofile
<!--NeedCopy-->
```

Beispiel:

```
sh ssl logprofile

    1)            Name: ssllogp1
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : ENABLED

    2)            Name: ssllogp2
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    3)            Name: ssllogp3
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    4)            Name: ssllog10
```



```
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
Done
<!--NeedCopy-->
```

Zeigen Sie alle SSL-Protokollprofile über die grafische Benutzeroberfläche an

Navigieren Sie zu **System > Profile > SSL-Protokollprofil**. Alle Profile sind aufgeführt.

Hängen Sie ein SSL-Protokollprofil an ein SSL-Profil an

Sie können ein SSL-Protokollprofil an ein SSL-Profil anhängen (festlegen), wenn Sie ein SSL-Profil erstellen, oder später, indem Sie das SSL-Profil bearbeiten. Sie können sowohl Clientauthentifizierung als auch Handshake-Erfolge und -Fehler protokollieren.

> **Wichtig:**
>
> Das standardmäßige SSL-Profil muss aktiviert sein, bevor Sie ein SSL-Protokollprofil anhängen können. Weitere Informationen zum Aktivieren des Standard-SSL-Profils finden Sie unter Standardprofil aktivieren.

Anhängen eines SSL-Protokollprofils an ein SSL-Profil über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set ssl profile <name> [-ssllogProfile <string>]
<!--NeedCopy-->
```

Beispiel:

```
set ssl profile fron_1 -ssllogProfile ssllog10
<!--NeedCopy-->
```

Anhängen eines SSL-Protokollprofils an ein SSL-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Klicken Sie auf **Bearbeiten** und geben Sie im **SSL-Protokollprofil**ein Profil an.

Anhängen eines SSL-Protokollprofils an eine SSL-Aktion

Sie können ein SSL-Protokollprofil nur beim Erstellen einer SSL-Aktion festlegen. Sie können eine SSL-Aktion nicht ändern, um das Protokollprofil festzulegen. Ordnen Sie die Aktion einer Richtlinie zu. Sie können nur Erfolge und Fehler der Clientauthentifizierung protokollieren.

Anhängen eines SSL-Protokollprofils an eine SSL-Aktion über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add ssl action <name> -clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) -
   ssllogProfile <string>
<!--NeedCopy-->
```

Beispiel:

```
> add ssl action act1 -clientAuth DoCLIENTAUTH -ssllogProfile ssllog10

Done

> sh ssl action act1

    1)            Name: act1
                    Type: Client Authentication (DOCLIENTAUTH)
                    Hits: 0
                    Undef Hits: 0
                    Action Reference Count: 0
                    SSLlogProfile: ssllog10
Done
<!--NeedCopy-->
```

Anhängen eines SSL-Protokollprofils an eine SSL-Aktion über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien** und klicken Sie auf **SSL-Aktionen**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie unter Clientauthentifizierung die Option **AKTIVIERT**
4. Wählen Sie im SSL-Protokollprofil ein Profil aus der Liste aus, oder klicken Sie auf “+”, um ein Profil zu erstellen.
5. Klicken Sie auf **Erstellen**.

Beispielausgabe aus der Protokolldatei

Im Folgenden finden Sie eine Beispielprotokollausgabe von`ns.log` für eine erfolgreiche Clientauthentifizierung.

```
1 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 158 0 :  SPCBId 671 -
    ClientIP 10.102.1.98 - ClientPort 49451 - VserverServiceIP
    10.102.57.82 - VserverServicePort 443 - ClientVersion TLSv1.2 -
    CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" - Session
    New - CLIENT_AUTHENTICATED -SerialNumber "2A" - SignatureAlgorithm "
    sha1WithRSAEncryption" - ValidFrom "Sep 22 09:15:20 2008 GMT" -
    ValidTo "Feb  8 09:15:20 2036 GMT" - HandshakeTime 10 ms
2 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 159 0 :  SPCBId 671
    - IssuerName " C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix"
3 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 160 0 :  SPCBId 671
     - SubjectName " C=IN,ST=KAR,O=Citrix Pvt Ltd,OU=A,CN=B"
4 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 161 0 :  Backend SPCBId
     674 - ServerIP 10.102.57.85 - ServerPort 443 - ProtocolVersion
    TLSv1.2 - CipherSuite "AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit" -
     Session Reuse - SERVER_AUTHENTICATED -SerialNumber "3E" -
    SignatureAlgorithm "sha1WithRSAEncryption" - ValidFrom "Sep 24
    06:40:37 2008 GMT" - ValidTo "Feb 10 06:40:37 2036 GMT" -
    HandshakeTime 1 ms
5 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 162 0 :  SPCBId 674
    - IssuerName " C=IN,ST=KAR,O=Citrix Pvt Ltd"
6 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 163 0 :  SPCBId 674
     - SubjectName " C=IN,ST=P,L=Q,O=R"
7 <!--NeedCopy-->
```

Unterstützung des DTLS-Protokolls

August 15, 2023

> **Hinweise**
>
> - Das DTLS 1.2-Protokoll wird auf den folgenden Appliances unterstützt:

  - NetScaler MPX/SDX (N2 and N3 based) and VPX appliances. It is not supported on external HSMs.
  - NetScaler appliances containing Intel Coleto and Intel Lewisburg SSL chips.
  - Front-end of NetScaler VPX appliances.
  - Front-end of NetScaler appliances containing Intel Coleto SSL chips. For more information about the platforms containing Intel Coleto SSL chips, see Support for Intel Coleto SSL chip-based platforms.
  - Front-end of NetScaler MPX (N3 based) appliances except the MPX 14000 FIPS appliances.
- Dienstgruppen vom Typ DTLS werden nicht unterstützt.
- Informationen zur Unterstützung von Enlightened Data Transport (EDT) für NetScaler Gateway finden Sie unter Unterstützung von HDX Enlightened Data Transport.
- Informationen zu den unterstützten Plattformen und Builds finden Sie unter NetScaler MPX-Hardware-Software-Kompatibilitätsmatrix.

Die SSL- und TLS-Protokolle wurden traditionell verwendet, um Streaming-Datenverkehr zu sichern. Beide Protokolle basieren auf TCP, das langsam ist. Außerdem kann TLS keine verlorenen oder neu geordneten Pakete verarbeiten.

UDP ist das bevorzugte Protokoll für Audio- und Videoanwendungen wie Lync, Skype, iTunes, YouTube, Schulungsvideos und Flash. UDP ist jedoch nicht sicher oder zuverlässig. Das DTLS-Protokoll wurde entwickelt, um Daten über UDP zu sichern, und wird für Anwendungen wie Medienstreaming, VOIP und Online-Gaming für die Kommunikation verwendet. In DTLS wird jeder Handshake-Nachricht innerhalb dieses Handshakes eine bestimmte Sequenznummer zugewiesen. Wenn ein Peer eine Handshake-Nachricht erhält, kann er schnell feststellen, ob diese Nachricht die nächste erwartete ist. Wenn dies der Fall ist, verarbeitet der Peer die Nachricht. Wenn nicht, wird die Nachricht zur Bearbeitung in die Warteschlange gestellt, nachdem alle vorherigen Nachrichten empfangen wurden.

Erstellen Sie einen virtuellen DTLS-Server und einen Dienst vom Typ UDP. Standardmäßig ist ein DTLS-Profil (nsdtls_default_profile) an den virtuellen Server gebunden. Optional können Sie ein benutzerdefiniertes DTLS-Profil erstellen und an den virtuellen Server binden.

Hinweis: RC4-Chiffren werden auf einem virtuellen DTLS-Server nicht unterstützt.

DTLS-Konfiguration

Sie können die Befehlszeile (CLI) oder das Konfigurationsdienstprogramm (GUI) verwenden, um DTLS auf Ihrer ADC-Appliance zu konfigurieren.

Hinweis: Das DTLS 1.2-Protokoll wird im Front-End einer NetScaler VPX-Appliance unterstützt. Geben Sie bei der Konfiguration eines virtuellen DTLSv1.2-Servers DTLS12 an. Die Standardeinstellung ist

DTLS1.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver DTLS [-dtls1 ( ENABLED | DISABLED )] [-dtls12 ( ENABLED |
DISABLED )]
```

Erstellen einer DTLS-Konfiguration über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <vserver_name> DTLS <IPAddress>  <port>
2 add service  <service_name>  <IPAddress> UDP 443
3 bind lb vserver  <vserver_name>  <udp_service_name>
4 <!--NeedCopy-->
```

Die folgenden Schritte sind optional:

```
1 add dtlsProfile dtls-profile -maxretryTime <positive_integer>
2 set ssl vserver <vserver_name> -dtlsProfileName <dtls_profile_name>
3 <!--NeedCopy-->
```

Erstellen einer DTLS-Konfiguration über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Erstellen Sie einen virtuellen Server vom Typ DTLS und binden Sie einen UDP-Dienst an den virtuellen Server.
3. Ein Standard-DTLS-Profil ist an den virtuellen DTLS-Server gebunden. Um ein anderes Profil zu binden, wählen Sie in SSL-Parametern ein anderes DTLS-Profil aus. Um ein Profil zu erstellen, klicken Sie auf das Plus (+) neben DTLS-Profil.

Unterstützung für SNI auf einem virtuellen DTLS-Server

Informationen zu SNI finden Sie unter Konfigurieren eines virtuellen SNI-Servers für das sichere Hosting mehrerer Websites.

Konfigurieren von SNI auf einem virtuellen DTLS-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set ssl vserver <vServerName> -SNIEnable ENABLED
2 bind ssl vserver <vServerName> -certkeyName <string> -SNICert
3 show ssl vserver <vServerName>
```



```
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver v1 -sniEnable ENABLED
bind ssl vserver  v1 -certkeyName san2 -sniCert
bind ssl vserver  v1 -certkeyName san13  - sniCert
bind ssl vserver  v1 -certkeyName san17  - sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED
Refresh Count: 0
Session Reuse: ENABLED
Timeout: 1800 seconds
Cipher Redirect: DISABLED

ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: ENABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
DTLSv1: ENABLED
Send Close-Notify: YES
Strict Sig-Digest Check: DISABLED
Zero RTT Early Data: DISABLED
DHE Key Exchange With PSK: NO
Tickets Per Authentication Context: 1

DTLS profile name: nsdtls_default_profile

ECC Curve: P_256, P_384, P_224, P_521

1) CertKey Name: ca
CA Certificate  OCSPCheck: OptionalCA_Name Sent
2) CertKey Name: san2 Server Certificate for SNI
3) CertKey Name: san17 Server Certificate for SNI
```



```
4) CertKey Name: san13 Server Certificate for SNI


1) Cipher Name: DEFAULT
Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```

Konfigurieren von SNI auf einem virtuellen DTLS-Server über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen DTLS-Server und klicken Sie unter Zertifikate auf **Serverzertifikat**.
3. Fügen Sie ein Zertifikat hinzu oder wählen Sie ein Zertifikat aus der Liste aus und wählen Sie **Serverzertifikat für SNI**aus.
4. Klicken Sie in **Erweiterte Einstellungen**auf **SSL-Parameter**.
5. Wählen Sie **SNI Enable**.

Funktionen, die von einem virtuellen DTLS-Server nicht unterstützt werden

Die folgenden Optionen können auf einem virtuellen DTLS-Server nicht aktiviert werden:

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Push verschlüsseln Trigger
- SSLv2Redirect
- SSLv2URL

Parameter, die nicht von einem virtuellen DTLS-Server verwendet werden

Ein virtueller DTLS-Server ignoriert die folgenden SSL-Parameter, auch wenn diese gesetzt sind:

- Verschlüsselung löst Paketanzahl aus
- PUSH-Verschlüsselung Trigger
- SSL-Quantengröße
- Verschlüsselung löst Timeout
- Format für das Einfügen von Betreff-/Ausstellernamen

Konfigurieren Sie Neuverhandlungen für einen DTLS-Dienst

Nicht sichere Neuverhandlungen werden auf einem DTLS-Dienst unterstützt. Sie können die CLI oder die GUI verwenden, um diese Einstellung zu konfigurieren.

Konfigurieren Sie die Neuverhandlung auf einem DTLS-Dienst über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -denysslreneg NONSECURE
<!--NeedCopy-->
```

Beispiel:

```
set ssl parameter -denysslreneg NONSECURE


sh ssl parameter
Advanced SSL Parameters
-----------------------
SSL quantum size                                    : 8 KB
Max CRL memory size                                 : 256 MB
Strict CA checks                                    : NO
Encryption trigger timeout                          : 100 ms
Send Close-Notify                                   : YES
Encryption trigger packet count                     : 45
Deny SSL Renegotiation                              : NONSECURE
Subject/Issuer Name Insertion Format                : Unicode
OCSP cache size                                     : 10 MB
Push flag                                           : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout                     : 1 ms
Crypto Device Disable Limit                         : 0
Global undef action for control policies            : CLIENTAUTH
Global undef action for data policies               : NOOP
Default profile                                     : DISABLED
SSL Insert Space in Certificate Header              : YES
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors  : NO
Disable TLS 1.1/1.2 for dynamic and VPN services    : NO
Software Crypto acceleration CPU Threshold          : 0
Hybrid FIPS Mode                                    : DISABLED
Signature and Hash Algorithms supported by TLS1.2   : ALL
SSL Interception Error Learning and Caching         : DISABLED
SSL Interception Maximum Error Cache Memory         : 0 Bytes
Done
```



```
<!--NeedCopy-->
```

Konfigurieren Sie die Neuverhandlung auf einem DTLS-Dienst über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Wählen Sie einen DTLS-Dienst aus und klicken Sie auf **Bearbeiten**.
3. Navigieren Sie zu **SSL** > **Erweiterte Einstellungen**.
4. Wählen Sie **SSL-Neuverhandlung verweigern**.

Funktionen, die von einem DTLS-Dienst nicht unterstützt werden

Die folgenden Optionen können für einen DTLS-Dienst nicht aktiviert werden:

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Push verschlüsseln Trigger
- SSLv2Redirect
- SSLv2URL
- SNI
- Sichere Neuverhandlung

Parameter, die nicht von einem DTLS-Dienst verwendet werden

Ein DTLS-Dienst ignoriert die folgenden SSL-Parameter, auch wenn diese gesetzt sind:

- Verschlüsselung löst Paketanzahl aus
- PUSH-Verschlüsselung Trigger
- SSL-Quantengröße
- Verschlüsselung löst Timeout
- Format für das Einfügen von Betreff-/Ausstellernamen

> **Hinweis:**
>
> Der Handshake zur Wiederverwendung von SSL-Sitzungen schlägt bei einem DTLS-Dienst fehl, da die Wiederverwendung von Sitzungen derzeit auf DTLS-Diensten nicht unterstützt wird.
>
> **Problemumgehung:** Deaktivieren Sie manuell die Wiederverwendung von Sitzungen für einen

> DTLS-Dienst. Geben Sie bei der CLI Folgendes ein:
>
> ```
> set ssl service <dtls-service-name> -sessReuse DISABLED
> ```

DTLS-Profil

Ein DTLS-Profil mit den Standardeinstellungen wird automatisch an einen virtuellen DTLS-Server gebunden. Sie können jedoch ein DTLS-Profil mit bestimmten Einstellungen erstellen, die Ihren Anforderungen entsprechen.

Verwenden Sie ein DTLS-Profil mit einem virtuellen DTLS-Server oder einem virtuellen VPN-DTLS-Server. Sie können kein SSL-Profil mit einem virtuellen DTLS-Server verwenden.

> **Hinweis:**
>
> Ändern Sie die Einstellung für die maximale Datensatzgröße im DTLS-Profil basierend auf den Änderungen der MTU und der Paketgröße. Beispielsweise wird die standardmäßige maximale Datensatzgröße von 1459 Byte basierend auf einer IPv4-Adresskopfgröße berechnet. Bei IPv6-Datensätzen ist die Header-Größe größer und daher muss die maximale Datensatzgröße reduziert werden, um die folgenden Kriterien zu erfüllen.

```
max record size + UDP header(8bytes)+ IP header size < MTU
```

Beispiel:

```
Default DTLS profile
    1) Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes

Custom DTLS profile
    1) Name: ns_dtls_profile_ipv6_1
    PMTU Discovery: DISABLED
    Max Record Size: 1450 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes
<!--NeedCopy-->
```

Erstellen eines DTLS-Profils mit der CLI

Hinweise:

- Der Parameter `helloverifyrequest` ist standardmäßig aktiviert. Die Aktivierung dieses Parameters hilft, das Risiko zu mindern, dass ein Angreifer oder Bots den Netzwerkdurchsatz überfordert, was möglicherweise zu einer Erschöpfung der ausgehenden Bandbreite führt. Das heißt, es hilft, den DTLS DDoS-Verstärkungsangriff zu mildern.
- Der Parameter `maxHoldQlen` wird hinzugefügt. Dieser Parameter definiert die Anzahl der Datagramme, die auf der DTLS-Schicht zur Verarbeitung in die Warteschlange gestellt werden können. Ein hoher Wert des Parameters `maxHoldQlen` kann zu Speicheransammlungen auf der DTLS-Schicht führen, wenn das UDP-Multiplexing hohen UDP-Datenverkehr überträgt. Daher wird empfohlen, einen niedrigeren Wert zu konfigurieren. Der Mindestwert ist 32, der Maximalwert beträgt 65535 und der Standardwert 32.

Im DTLS-Profil wird ein neuer Parameter `maxBadmacIgnorecount` eingeführt, um fehlerhafte MAC-Datensätze zu ignorieren, die in einer DTLS-Sitzung empfangen wurden. Mit diesem Parameter werden fehlerhafte Datensätze bis zu dem im Parameter festgelegten Wert ignoriert. Die Appliance beendet die Sitzung erst, nachdem das Limit erreicht ist, und sendet eine Warnung.

Diese Parametereinstellung ist nur wirksam, wenn der Parameter `terminateSession` aktiviert ist.

```
ssl dtlsProfile <name> -maxRetryTime <positive_integer> -
    helloVerifyRequest ( ENABLED | DISABLED ) -terminateSession (ENABLED
     | DISABLED ) -maxHoldQLen <positive_integer> -maxBadmacIgnorecount
    <positive_integer>

helloVerifyRequest
               Send a Hello Verify request to validate the client.
               Possible values: ENABLED, DISABLED
               Default value: ENABLED

terminateSession
               Terminate the session if the message authentication code
                   (MAC)
               of the client and server do not match.
               Possible values: ENABLED, DISABLED
               Default value: DISABLED

maxHoldQLen
               Maximum number of datagrams that can be queued at DTLS
                   layer for
               processing
               Default value: 32
               Minimum value: 32
               Maximum value: 65535
```



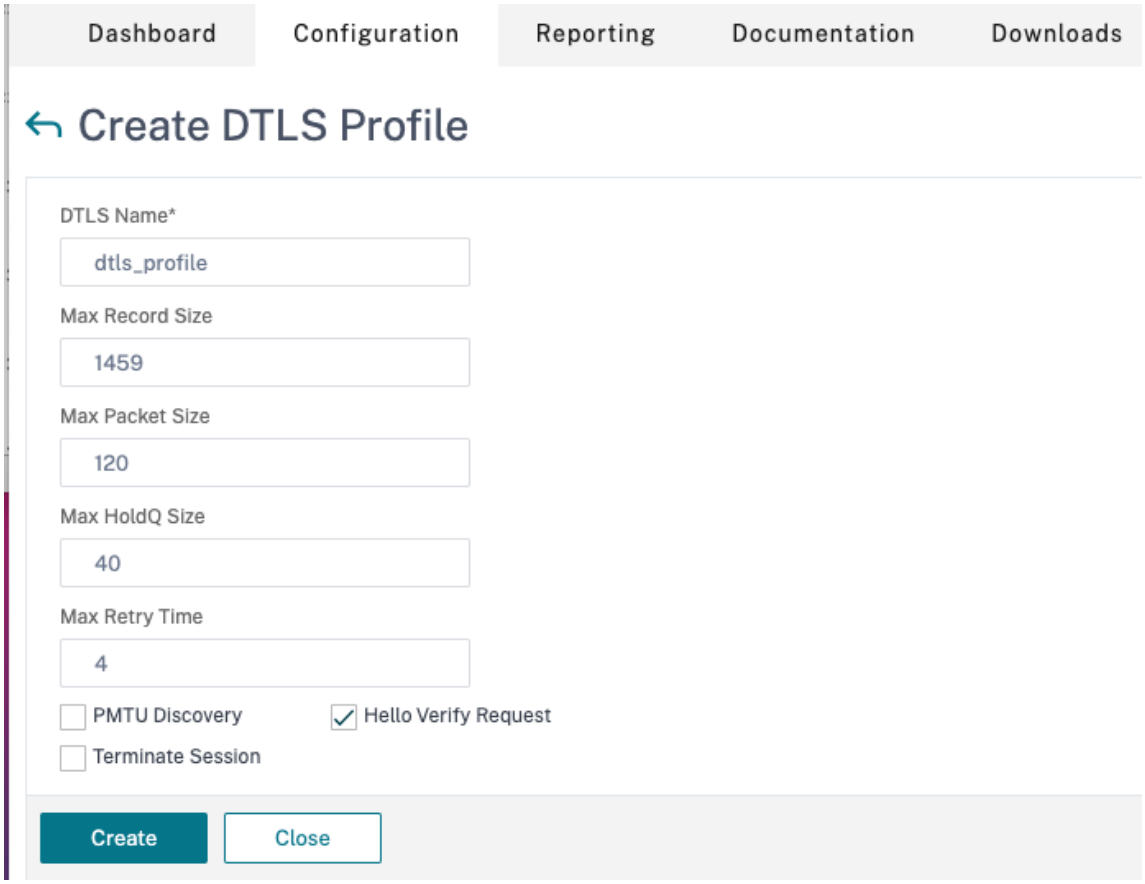
```
20
21 maxBadmacIgnorecount
22                Maximum number of bad MAC errors to ignore for a
                      connection prior disconnect. Disabling parameter
                      terminateSession
23 terminates session immediately when bad MAC is detected in the
      connection.
24                Default value: 100
25                Minimum value: 1
26                Maximum value: 65535
27 <!--NeedCopy-->
```

Beispiel:

```
1  > add ssl dtlsprofile dtls_profile -maxRetryTime 4 -helloVerifyRequest
      ENABLED -terminateSession ENABLED -maxHoldQLen 40 -
      maxBadmacIgnorecount 150
2   Done
3  > sh dtlsprofile dtls_profile
4  1)  Name: dtls_profile
5      PMTU Discovery: DISABLED
6      Max Record Size: 1459 bytes
7      Max Retry Time: 4 sec
8      Hello Verify Request: ENABLED
9      Terminate Session: ENABLED
10     Max Packet Count: 120 bytes
11     Max HoldQ Size: 40 datagrams
12     Max bad-MAC Ignore Count: 150
13
14  Done
15 <!--NeedCopy-->
```

Erstellen eines DTLS-Profils mit der GUI

1. Navigieren Sie zu **System > Profile > DTLS-Profile** und klicken Sie auf **Hinzufügen**.
2. Geben **Sie auf der Seite DTLS-Profil erstellen** Werte für die verschiedenen Parameter ein.



3. Klicken Sie auf **Erstellen**.

Beispiel für eine End-to-End-DTLS-Konfiguration

```
enable ns feature SSL LB

add server s1 198.51.100.2

en ns mode usnip

add service svc_dtls s1 DTLS 443

add lb vserver v1 DTLS 10.102.59.244 443

bind ssl vserver v1 -ciphername ALL

add ssl certkey servercert -cert servercert_aia_valid.pem -key
   serverkey_aia.pem

bind ssl vserver v1 -certkeyname servercert

```



```
17 bind lb vserver lb1 svc_dtls
18
19 sh lb vserver v1
20
21                     v1 (10.102.59.244:4433) - DTLS     Type: ADDRESS
22                     State: UP
23                     Last state change was at Fri Apr 27 07:00:27 2018
24                     Time since last state change: 0 days, 00:00:04.810
25                     Effective State: UP
26                     Client Idle Timeout: 120 sec
27                     Down state flush: ENABLED
28                     Disable Primary Vserver On Down : DISABLED
29                     Appflow logging: ENABLED
30                     No. of Bound Services :  1 (Total) 0 (Active)
31                     Configured Method: LEASTCONNECTION
32                     Current Method: Round Robin, Reason: A new service
                          is bound         BackupMethod: ROUNDROBIN
33                     Mode: IP
34                     Persistence: NONE
35                     L2Conn: OFF
36                     Skip Persistency: None
37                     Listen Policy: NONE
38                     IcmpResponse: PASSIVE
39                     RHIstate: PASSIVE
40                     New Service Startup Request Rate: 0 PER_SECOND,
                          Increment Interval: 0
41                     Mac mode Retain Vlan: DISABLED
42                     DBS_LB: DISABLED
43                     Process Local: DISABLED
44                     Traffic Domain: 0
45                     TROFS Persistence honored: ENABLED
46                     Retain Connections on Cluster: NO
47
48     1) svc_dtls (10.102.59.190: 4433) - DTLS State: UP  Weight: 1
49 Done
50
51
52 sh ssl vserver v1
53
54                     Advanced SSL configuration for VServer v1:
55                     DH: DISABLED
56                     DH Private-Key Exponent Size Limit: DISABLED
                                    Ephemeral RSA: ENABLED
                                                          Refresh Count: 0
57                     Session Reuse: ENABLED                 Timeout:
```



```
                          1800 seconds
                      Cipher Redirect: DISABLED
                      ClearText Port: 0
                      Client Auth: DISABLED
                      SSL Redirect: DISABLED
                      Non FIPS Ciphers: DISABLED
                      SNI: DISABLED
                      OCSP Stapling: DISABLED
                      HSTS: DISABLED
                      HSTS IncludeSubDomains: NO
                      HSTS Max-Age: 0
                      DTLSv1: ENABLED
                      Send Close-Notify: YES
                      Strict Sig-Digest Check: DISABLED
                      Zero RTT Early Data: DISABLED
                      DHE Key Exchange With PSK: NO
                      Tickets Per Authentication Context: 1
                      DTLS profile name: nsdtls_default_profile

                      ECC Curve: P_256, P_384, P_224, P_521

    1)            CertKey Name: servercert               Server
       Certificate

    1)            Cipher Name: DEFAULT
                    Description: Default cipher list with encryption
                       strength >= 128bit

    2)            Cipher Name: ALL
                    Description: All ciphers supported by NetScaler,
                       excluding NULL ciphers
     Done

sh service svc_dtls

                      svc_dtls (10.102.59.190:4433) - DTLS
                      State: UP
                      Last state change was at Fri Apr 27 07:00:26 2018
                      Time since last state change: 0 days, 00:00:22.790
                      Server Name: s1
                      Server ID : None                Monitor Threshold
                       : 0
                      Max Conn: 0        Max Req: 0           Max
                       Bandwidth: 0 kbits
                      Use Source IP: NO
```



```
                        Client Keepalive(CKA): NO
                        Access Down Service: NO
                        TCP Buffering(TCPB): NO
                        HTTP Compression(CMP): NO
                        Idle timeout: Client: 120 sec           Server: 120
                            sec
                        Client IP: DISABLED
                        Cacheable: NO
                        SC: OFF
                        SP: OFF
                        Down state flush: ENABLED
                        Monitor Connection Close : NONE
                        Appflow logging: ENABLED
                        Process Local: DISABLED
                        Traffic Domain: 0

     1)             Monitor Name: ping-default
                                      State: UP               Weight: 1
                                                          Passive: 0
                                    Probes: 5              Failed [Total
                                       : 0 Current: 0]
                                     Last response: Success - ICMP echo
                                        reply received.
                           Response Time: 2.77 millisec
      Done

sh ssl service svc_dtls

                        Advanced SSL configuration for Back-end SSL Service
                            svc_dtls:
                        DH: DISABLED
                        DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: DISABLED
                        Session Reuse: ENABLED                 Timeout:
                           1800 seconds
                        Cipher Redirect: DISABLED
                        ClearText Port: 0
                        Server Auth: DISABLED
                        SSL Redirect: DISABLED
                        Non FIPS Ciphers: DISABLED
                        SNI: DISABLED
                        OCSP Stapling: DISABLED
                        DTLSv1: ENABLED
                        Send Close-Notify: YES
                        Strict Sig-Digest Check: DISABLED
```



```
                      Zero RTT Early Data: ???
                      DHE Key Exchange With PSK: ???
                      Tickets Per Authentication Context: ???
                      DTLS profile name: nsdtls_default_profile
                      ECC Curve: P_256, P_384, P_224, P_521
    1)              Cipher Name: DEFAULT_BACKEND
                      Description: Default cipher list for Backend SSL
                         session
     Done


> sh dtlsProfile nsdtls_default_profile
1)  Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: DISABLED
    Terminate Session: ENABLED
    Max Packet Count: 120 bytes
    Max HoldQ Size: 32 datagrams
    Max bad-MAC Ignore Count: 10

 Done
<!--NeedCopy-->
```

DTLS-Unterstützung für IPv6-Adresse

DTLS wird auch mit IPv6-Adressen unterstützt. Um jedoch DTLS mit IPv6-Adressen zu verwenden, muss die maximale Datensatzgröße im DTLS-Profil angepasst werden.

Wenn der Standardwert für die maximale Datensatzgröße verwendet wird, schlägt die anfängliche DTLS-Verbindung möglicherweise fehl. Passen Sie die maximale Datensatzgröße über ein DTLS-Profil an.

DTLS cipher support

Standardmäßig ist eine DTLS-Verschlüsselungsgruppe gebunden, wenn Sie einen virtuellen DTLS-Server oder -Dienst erstellen. DEFAULT_DTLS enthält die Chiffren, die eine Front-End-DTLS-Entität unterstützt. Diese Gruppe ist standardmäßig gebunden, wenn Sie einen virtuellen DTLS-Server erstellen. DEFAULT_DTLS_BACKEND enthält die Chiffren, die für eine Back-End-DTLS-Entität unterstützt werden. Diese Gruppe ist standardmäßig an einen DTLS-Back-End-Dienst gebunden. DTLS_FIPS enthält die Chiffren, die auf der NetScaler FIPS-Plattform unterstützt werden. Diese

Gruppe ist standardmäßig an einen virtuellen DTLS-Server oder -Dienst gebunden, der auf einer FIPS-Plattform erstellt wurde.

Unterstützung von DTLS-Verschlüsselungen auf NetScaler VPX-, MPX/SDX- (N2- und N3-basierten) Appliances

Wie liest man die Tabellen:

Sofern keine Build-Nummer angegeben wird, wird eine Verschlüsselungssammlung für alle Builds in einer Version unterstützt.

Beispiel:

- **11.1, 12.1, 13.0, 13.1, 14.1**: Alle Builds der Releases 11.1, 12.1, 13.0, 13.1,14.1.
- **-NA-**: nicht zutreffend.

DTLS-Verschlüsselungsunterstützung auf NetScaler VPX-, MPX/SDX (N2-, N3- und Coleto-basierten) Appliances

Name der Verschlüs-selungssuite	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.1, 12.1, 13.0, 13.1, 14.1	12.1, 13.0, 13.1, 14.1
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.1, 12.1, 13.0, 13.1, 14.1	12.1, 13.0, 13.1, 14.1
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_D	11.1, 12.1, 13.0, 13.1, 14.1	Nicht zutreffend
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.1, 13.0, 13.1, 14.1	12.1, 13.0, 13.1, 14.1
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.1, 12.1, 13.0, 13.1, 14.1	Nicht zutreffend
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.1, 12.1, 13.0, 13.1, 14.1	Nicht zutreffend
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1, 13.0, 13.1, 14.1	12.1, 13.0, 13.1, 14.1
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	11.1, 12.1, 13.0, 13.1, 14.1	12.1, 13.0, 13.1, 14.1

Name der Verschlüs-selungssuite	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1, 13.0, 13.1, 14.1	Nicht zutreffend
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0, 13.1, 14.1	12.1, 13.0, 13.1, 14.1
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1, 13.0, 13.1, 14.1	12.1, 13.0, 13.1, 14.1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	13.1–21.x, 14.1	13.1–21.x, 14.1
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDS	13.1–21.x, 14.1	13.1–21.x, 14.1
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	0xc008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	13.1–21.x, 14.1	13.1–21.x, 14.1

Um die Liste der im Front-End unterstützten Standardchiffren anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ssl cipher DEFAULT_DTLS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
```



```
11      Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
           HexCode=0x0039
12  6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
13      Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
           HexCode=0x0033
14  7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
15      Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
           HexCode=0xc012
16  8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
17      Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
           HexCode=0x000a
18  <!--NeedCopy-->
```

Um die Liste der im Back-End unterstützten Standardchiffren anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1   show ssl cipher DEFAULT_DTLS_BACKEND
2   1)  Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
3       Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
           HexCode=0x0035
4   2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
5       Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
           HexCode=0x002f
6   3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
7       Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
           HexCode=0xc014
8   4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
9       Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
           HexCode=0xc013
10  5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
11      Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
           HexCode=0x0039
12  6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
13      Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
           HexCode=0x0033
14  7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
15      Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
           HexCode=0xc012
16  8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
17      Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
           HexCode=0x000a
18  <!--NeedCopy-->
```


Unterstützung von DTLS-Verschlüsselungen auf der NetScaler MPX 14000 FIPS-Plattform

Hinweis: Enlightened Data Support (EDT) wird auf der FIPS-Plattform unterstützt, wenn die folgenden Bedingungen erfüllt sind:

- Der in StoreFront festgelegte UDT-MSS-Wert beträgt 900.
- Die Windows-Clientversion ist 4.12 oder höher.
- DTLS-fähige VDA-Version ist 7.17 oder höher.
- Nicht-DTLS-VDA-Version ist 7.15 LTSR CU3 oder höher.

Wie liest man die Tabellen:

Sofern keine Build-Nummer angegeben wird, wird eine Verschlüsselungssammlung für alle Builds in einer Version unterstützt.

Beispiel:

- **11.1, 12.1, 13.0, 13.1, 14.1**: Alle Builds der Releases 11.1, 12.1, 13.0, 13.1, 14.1.
- **-NA-**: nicht zutreffend.

Name der Verschlüsselungssammlung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.1, 12.1–49.x, 13.0, 13.1, 14.1	12.1–49.x, 13.0, 13.1, 14.1
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES_128_CBC_SHA	11.1, 12.1–49.x, 13.0, 13.1, 14.1	12.1–49.x, 13.0, 13.1, 14.1
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_DI	11.1, 12.1–49.x, 13.0, 13.1, 14.1	Nicht zutreffend
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11.1, 12.1–49.x, 13.0, 13.1, 14.1	12.1–49.x, 13.0, 13.1, 14.1
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11.1, 12.1–49.x, 13.0, 13.1, 14.1	Nicht zutreffend
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	11.1, 12.1–49.x, 13.0, 13.1, 14.1	Nicht zutreffend
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1–49.x, 13.0, 13.1, 14.1	12.1–49.x, 13.0, 13.1, 14.1

Name der Verschlüs-selungssamm-lung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	12.1–49.x, 13.0, 13.1, 14.1	12.1–49.x, 13.0, 13.1, 14.1
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1–49.x, 13.0, 13.1, 14.1	Nicht zutreffend
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1–49.x, 13.0, 13.1, 14.1	12.1–49.x, 13.0, 13.1, 14.1
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1–49.x, 13.0, 13.1, 14.1	12.1–49.x, 13.0, 13.1, 14.1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	13.1–21.x, 14.1	13.1–21.x, 14.1
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDS	13.1–21.x, 14.1	13.1–21.x, 14.1
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	0xc008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	13.1–21.x, 14.1	13.1–21.x, 14.1

Um die Liste der auf einer NetScaler FIPS-Appliance unterstützten Standardverschlüsse anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ssl cipher DTLS_FIPS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
```



```
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA  Priority : 5
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
6)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 6
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

DTLSv1.2-Verschlüsselungsunterstützung auf den Front-End-VPX-Appliances, MPX/SDX-Appliances (Coleto und N3-basiert)

In der folgenden Tabelle sind die zusätzlichen Verschlüsselungen aufgeführt, die für das DTLSv1.2-Protokoll unterstützt werden.

Name der Verschlüsselungssammlung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (VPX-Frontend)	Unterstützte Builds (Coleto-basiert)	Unterstützte Builds (N3-basiert)
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RS	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-DHE-RSA-AES256-GCM-SHA384	0x009f	TLS_DHE_RSA_	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1

Name der Verschlüsselungssammlung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (VPX-Frontend)	Unterstützte Builds (Coleto-basiert)	Unterstützte Builds (N3-basiert)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	0x009e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RS	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-DHE-RSA-AES-256-SHA256	0x006b	TLS_DHE_RSA_	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1.2-DHE-RSA-AES-128-SHA256	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	13.0–47.x, 13.1, 14.1	13.0–52.x, 13.1, 14.1	13.0–58.x, 13.1, 14.1
TLS1-ECDHE-ECDSA-AES128-SHA	0xc009	TLS_ECDHE_EC	13.1–21.x, 14.1	13.1-21.x, 14.1	13.1-21.x, 14.1
TLS1-ECDHE-ECDSA-AES256-SHA	0xc00a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	13.1–21.x, 14.1	13.1-21.x, 14.1	13.1-21.x, 14.1
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	0xc008	TLS_ECDHE_EC	13.1–21.x, 14.1	13.1-21.x, 14.1	13.1-21.x, 14.1

Name der Verschlüsselungssammlung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (VPX-Frontend)	Unterstützte Builds (Coleto-basiert)	Unterstützte Builds (N3-basiert)
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	0xc02b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	13.1–21.x, 14.1	13.1-21.x, 14.1	13.1-21.x, 14.1
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	0xc02c	TLS_ECDHE_EC	13.1–21.x, 14.1	13.1-21.x, 14.1	13.1-21.x, 14.1
TLS1.2-ECDHE-ECDSA-AES128-SHA256	0xc023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	13.1–21.x, 14.1	13.1-21.x, 14.1	13.1-21.x, 14.1
TLS1.2-ECDHE-ECDSA-AES256-SHA384	0xc024	TLS_ECDHE_EC	13.1–21.x, 14.1	13.1-21.x, 14.1	13.1-21.x, 14.1

Unterstützung für Intel Coleto und Intel Lewisburg SSL-Chip-basierte Plattformen

August 15, 2023

Die folgenden Appliances werden mit Intel Coleto-Chips geliefert:

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 15000
- MPX/SDX 15000-50 G
- MPX/SDX 26000

- MPX/SDX 26000-50S
- MPX/SDX 26000-100G

Das folgende Gerät wird mit Intel Lewisburg Chips geliefert:

- MPX/SDX 9100
- MPX/SDX 16000

Verwenden Sie den Befehl “Hardware anzeigen”, um festzustellen, ob Ihre Appliance über Coleto- (COL) - oder Lewisburg (LBG) -Chips verfügt.

```
> sh hardware

    Platform: NSMPX-8900 8\*CPU+4\*F1X+6\*E1K+1\*E1K+1*COL 8955 30010
    Manufactured on: 10/18/2016
    CPU: 2100MHZ
    Host Id: 0
    Serial no: CRAC5CR8UA
    Encoded serial no: CRAC5CR8UA
 Done
<!--NeedCopy-->
```

```
> sh hardware
        Platform: NSMPX-9100 10\*CPU+64GB+8\*F2X+E1K+1*LBG C627 35000
        Manufactured on: 10/1/2021
        CPU: 2300MHZ
        Host Id: 161644678
        Serial no: N2Z3ZD9S21
        Encoded serial no: N2Z3ZD9S21
        Netscaler UUID: 41a26261-227e-11ec-b4db-3cecef56f86b
        BMC Revision: 1.00
Done
<!--NeedCopy-->
```

Einschränkungen

Die folgenden Verschlüsselungen, Protokolle und Funktionen werden nicht unterstützt:

- DH 512-Verschlüsselung
- SSLv3-Protokoll
- Azure Key Vault
- GnuTLS
- ECDSA-Zertifikate mit ECC-Kurven P_224 und P521
- DNSSEC-Offload

> Hinweis: Die
>
> Unterstützung für das Thales Luna Network Hardware Security Module (HSM) ist ab Version 13.1 Build 33.x verfügbar.

Sehen Sie sich die softwarebasierte SSL-Chip-Auslastung auf NetScaler MPX- und SDX-Plattformen an

Weitere Informationen zur softwarebasierten SSL-Chip-Nutzung finden Sie auf den folgenden Plattformen:

- MPX- und SDX-Plattformen, die mit Intel Coleto-Chips geliefert werden.
- MPX-Plattformen, die mit Intel Lewisburg-Chips geliefert werden.

> **Hinweis**
>
> Diese Funktion wird auf den folgenden Plattformen nicht unterstützt:
>
> - SDX 9100
> - MPX/SDX 16000

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> stat ssl

SSL Summary

1.  SSL cards present 4
2.  SSL cards UP 4
    SSL engine status 1
    SSL sessions (Rate) 19849
    SSL Crypto Utilization Asym (%) 88
    SSL Crypto Utilization Symm (%) 1

Crypto Utilization(%)
Asymmetric Crypto Utilization 86.30
Symmetric Crypto Utilization 0.97

System
Transactions Rate (/s) Total
SSL transactions 19849 45900312
SSLv2 transactions 0 0
SSLv3 transactions 0 0
TLSv1 transactions 0 0
TLSv1.1 transactions 0 0
TLSv1.2 transactions 19849 45900312
```



```
TLSv1.3 transactions 0 0
DTLSv1 transactions 0 0
DTLSv1.2 transactions 0 0

Front End
Sessions Rate (/s) Total
SSL sessions 19849 45937019
SSLv2 sessions 0 0
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 19849 45937019
TLSv1.3 sessions 0 0
DTLSv1 sessions 0 0
DTLSv1.2 sessions 0 0
New SSL sessions 19881 50722628
SSL session misses 0 0
SSL session hits 0 0

Back End
Sessions Rate (/s) Total
SSL sessions 0 137
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 0 137
DTLSv1 sessions 0 0
Session multiplex attempts 0 0
Session multiplex successes 0 0
Session multiplex failures 0 0

Encryption/Decryption statistics
Crypto Operation Rate (bytes/s) Total Bytes
Bytes encrypted 24338213 27705995030
Bytes decrypted 24664169 27942280990
Done
<!--NeedCopy-->
```

Werte für die folgenden Zähler werden durch Abfrage der Hardware erreicht:

```
-  SSL Crypto Utilization Asym (%) 88
-  SSL Crypto Utilization Symm (%) 1
<!--NeedCopy-->
```

Werte für die folgenden Zähler werden mit der Software erreicht. Die Werte können geringfügig von

den von der Hardware abgefragten Werten abweichen.

- Crypto Utilization(%)
- Asymmetric Crypto Utilization 85.92
- RSA Crypto Utilization 11.43
  RSA_4K 0.00
  RSA_2K 11.43
  RSA_1K 0.00
  RSA_Others 0.00
- DH Crypto Utilization 74.50
  ECDH Crypto Utilization 0.00
  ECDH_P224 0.00
  ECDH_P256 0.00
  ECDH_P384 0.00
  ECDH_P521 0.00
- ECDSA Crypto Utilization 0.00
  ECDSA_P224 0.00
  ECDSA_P256 0.00
  ECDSA_P384 0.00
  ECDSA_P521 0.00
- Symmetric Crypto Utilization 0.72

Führen Sie für eine granulare Nutzung pro Verschlüsselung den folgenden Befehl aus.

```
> stat ssl -detail

SSL Offloading

1.  SSL cards present 4
2.  SSL cards UP 4
    SSL engine status 1
    SSL sessions (Rate) 19862
    SSL Crypto Utilization Asym (%) 88
    SSL Crypto Utilization Symm (%) 1

Crypto Utilization(%)

Asymmetric Crypto Utilization 85.92

RSA Crypto Utilization 11.43
RSA_4K 0.00
RSA_2K 11.43
RSA_1K 0.00
RSA_Others 0.00
```



```
21
22 DH Crypto Utilization 74.50
23
24 ECDH Crypto Utilization 0.00
25 ECDH_P224 0.00
26 ECDH_P256 0.00
27 ECDH_P384 0.00
28 ECDH_P521 0.00
29
30 ECDSA Crypto Utilization 0.00
31 ECDSA_P224 0.00
32 ECDSA_P256 0.00
33 ECDSA_P384 0.00
34 ECDSA_P521 0.00
35
36 Symmetric Crypto Utilization 0.72
37 System
38 Transactions Rate (/s) Total
39 SSL transactions 19861 46039342
40 SSLv2 transactions 0 0
41 SSLv3 transactions 0 0
42 TLSv1 transactions 0 0
43 TLSv1.1 transactions 0 0
44 TLSv1.2 transactions 19861 46039342
45 TLSv1.3 transactions 0 0
46 DTLSv1 transactions 0 0
47 DTLSv1.2 transactions 0 0
48 Server in record 117437 277622634
49 Front End
50 Sessions Rate (/s) Total
51 SSL sessions 19862 46076050
52 SSLv2 sessions 0 0
53 SSLv3 sessions 0 0
54 TLSv1 sessions 0 0
55 TLSv1.1 sessions 0 0
56 TLSv1.2 sessions 19862 46076050
57 TLSv1.3 sessions 0 0
58 DTLSv1 sessions 0 0
59 DTLSv1.2 sessions 0 0
60 New SSL sessions 19801 50861234
61 SSL session misses 0 0
62 SSL session hits 0 0
63 Session Renegotiation
64 SSL session renegotiations 0 0
65 SSLv3 session renegotiations 0 0
```



```
TLSv1 session renegotiations 0 0
TLSv1.1 session renegotiations 0 0
TLSv1.2 session renegotiations 0 0
DTLSv1 session renegotiations 0 0
DTLSv1.2 session renegotiations 0 0
Key Exchanges
RSA 512-bit key exchanges 0 0
RSA 1024-bit key exchanges 0 2032658
RSA 2048-bit key exchanges 0 143
RSA 3072-bit key exchanges 0 7757028
RSA 4096-bit key exchanges 0 2238698
DH 512-bit key exchanges 0 0
DH 1024-bit key exchanges 0 0
DH 2048-bit key exchanges 19862 5477702
DH 4096-bit key exchanges 0 0
ECDHE 521 curve key exchanges 0 0
ECDHE 384 curve key exchanges 0 0
ECDHE 256 curve key exchanges 0 28569821
ECDHE 224 curve key exchanges 0 0
Total ECDHE key exchanges 0 28569821
Ciphers Negotiated
RC4 40-bit encryptions 0 0
RC4 56-bit encryptions 0 0
RC4 64-bit encryptions 0 0
RC4 128-bit encryptions 0 0
DES 40-bit encryptions 0 0
DES 56-bit encryptions 0 0
3DES 168-bit encryptions 0 0
AES 128-bit encryptions 0 0
AES 256-bit encryptions 19862 17506229
RC2 40-bit encryptions 0 0
RC2 56-bit encryptions 0 0
RC2 128-bit encryptions 0 0
AES-GCM 128-bit encryptions 0 0
AES-GCM 256-bit encryptions 0 28569821
Null cipher encryptions 0 0
Hashes
MD5 hashes 0 0
SHA hashes 0 12028527
SHA256 hashes 19862 5477702
SHA384 hashes 0 0
Handshakes
SSLv2 SSL handshakes 0 0
SSLv3 SSL handshakes 0 0
TLSv1 SSL handshakes 0 0
```



```
TLSv1.1 SSL handshakes 0 0
TLSv1.2 SSL handshakes 19862 46076050
TLSv1.3 SSL handshakes 0 0
DTLSv1 SSL handshakes 0 0
DTLSv1.2 SSL handshakes 0 0
Client Authentications
SSLv2 client authentications 0 0
SSLv3 client authentications 0 0
TLSv1 client authentications 0 0
TLSv1.1 client authentications 0 0
TLSv1.2 client authentications 0 0
TLSv1.3 client authentications 0 0
DTLSv1 client authentications 0 0
DTLSv1.2 client authentications 0 0
Authentications
RSA authentications 19862 17506229
DH authentications 0 0
DSS (DSA) authentications 0 0
ECDSA authentications 0 28569821
Null authentications 0 0
Back End
Sessions Rate (/s) Total
SSL sessions 0 137
SSLv3 sessions 0 0
TLSv1 sessions 0 0
TLSv1.1 sessions 0 0
TLSv1.2 sessions 0 137
DTLSv1 sessions 0 0
Session multiplex attempts 0 0
Session multiplex successes 0 0
Session multiplex failures 0 0
Session Renegotiation
SSL session renegotiations 0 0
SSLv3 session renegotiations 0 0
TLSv1 session renegotiations 0 0
TLSv1.1 back-end session renegot 0 0
TLSv1.2 back-end session renegot 0 0
DTLSv1 session renegotiations 0 0
Key Exchanges
RSA 512-bit key exchanges 0 0
RSA 1024-bit key exchanges 0 0
RSA 2048-bit key exchanges 0 137
RSA 3072-bit key exchanges 0 0
RSA 4096-bit key exchanges 0 0
DH 512-bit key exchanges 0 0
```



```
DH 1024-bit key exchanges 0 0
DH 2048-bit key exchanges 0 0
DH 4096-bit key exchanges 0 0
ECDHE 521 curve key exchanges 0 0
ECDHE 384 curve key exchanges 0 0
ECDHE 256 curve key exchanges 0 0
ECDHE 224 curve key exchanges 0 0
Ciphers Negotiated
RC4 40-bit encryptions 0 0
RC4 56-bit encryptions 0 0
RC4 64-bit encryptions 0 0
RC4 128-bit encryptions 0 0
DES 40-bit encryptions 0 0
DES 56-bit encryptions 0 0
3DES 168-bit encryptions 0 0
AES 128-bit encryptions 0 0
AES 256-bit encryptions 0 137
RC2 40-bit encryptions 0 0
RC2 56-bit encryptions 0 0
RC2 128-bit encryptions 0 0
AES-GCM 128-bit encryptions 0 0
AES-GCM 256-bit encryptions 0 0
Null encryptions 0 0
Hashes
MD5 hashes 0 0
SHA hashes 0 137
SHA256 hashes 0 0
SHA384 hashes 0 0
Handshakes
SSLv3 handshakes 0 0
TLSv1 handshakes 0 0
TLSv1.1 handshakes 0 0
TLSv1.2 handshakes 0 137
DTLSv1 handshakes 0 0
Client Authentications
SSLv3 client authentications 0 0
TLSv1 client authentications 0 0
TLSv1.1 client authentications 0 0
TLSv1.2 client authentications 0 0
DTLSv1 client authentications 0 0
Authentications
RSA authentications 0 137
DH authentications 0 0
DSS authentications 0 0
ECDSA authentications 0 0
```



```
Null authentications 0 0
System Total
RSA key exchanges offloaded 0 0
RSA sign operations offloaded 0 0
DH key exchanges offloaded 19841 5481037
RC4 encryptions offloaded 0 0
DES encryptions offloaded 0 0
AES encryptions offloaded 0 0
AES-GCM 128-bit encryptions offl 0 0
AES-GCM 256-bit encryptions offl 0 0
Encryption/Decryption statistics
Crypto Operation Rate (bytes/s) Total Bytes
Bytes encrypted 12129801 27790903638
Bytes encrypted in hardware 12129801 27790903638
Bytes encrypted in software 0 0
Bytes encrypted on the front-end 5450907 13430410630
Bytes encrypted in hardware on t 5450907 13430410630
Bytes encrypted in software on t 0 0
Bytes encrypted on the back-end 6678894 14360493008
Bytes encrypted in hardware on t 6678894 14360493008
Bytes encrypted in software on t 0 0
Bytes decrypted 12449504 28029427518
Bytes decrypted in hardware 12449504 28029427518
Bytes decrypted in software 0 0
Bytes decrypted on the front-end 8190208 19876552670
Bytes decrypted in hardware on t 8190208 19876552670
Bytes decrypted in software on t 0 0
Bytes decrypted on the back-end 4259296 8152874848
Bytes decrypted in hardware on t 4259296 8152874848
Bytes decrypted in software on t 0 0
SSL
Rate (/s) Total
Total SPCB in use -87 84656
Active SSL sessions -30309 5615559
Current queue size -1 4153
CardQ
Rate (/s) Total
In Q count for current card -1 4153
In BulkQ count for current card 0 0
In KeyQ count for current card -1 4153
Done
<!--NeedCopy-->
```


Hinweise

- Admin-Partition wird unterstützt, aber die Nutzung für alle Partitionen wird in der Standardpartition angezeigt. Auf nicht standardmäßigen Partitionen werden diese Werte als 0 angezeigt.
- In einem Cluster-Setup zeigt die CLIP-Adresse die durchschnittliche Auslastung für alle Knoten im Cluster an. Führen Sie zur knotenspezifischen Nutzung den Befehl auf der CLI jedes Knotens aus. Diese Daten sind möglicherweise für eine SDX-Plattform falsch, wenn die Knoten des Clusters auf derselben Hardware gehostet werden.
- Für VPX-Instanzen auf der SDX-Plattform wird die Auslastung jeder VPX-Instanz angezeigt.

MPX 14000 FIPS-Geräte

August 15, 2023

Wichtig:

- Die FIPS-Plattform MPX 9700/10500/12500/15500 hat das Lebensende erreicht.
- Die Konfigurationsschritte für NetScaler MPX 14000 FIPS und NetScaler MPX 9700/10500/12500/15500 FIPS-Appliances sind unterschiedlich. MPX 14000 FIPS-Appliances verwenden keine Firmware v2.2. Ein FIPS-Schlüssel, der auf dem Hardware Security Module (HSM) der MPX 9700-Plattform erstellt wurde, kann nicht an das HSM der MPX 14000-Plattform übertragen werden. Umgekehrt wird auch nicht unterstützt. Wenn Sie jedoch einen RSA-Schlüssel als FIPS-Schlüssel importiert haben, können Sie den RSA-Schlüssel auf die MPX 14000-Plattform kopieren. Importiere es dann als FIPS-Schlüssel. Es werden nur 2048-Bit- und 3072-Bit-Schlüssel unterstützt.
- Die Firmware-Versionen, die auf der NetScaler-Downloadseite unter “NetScaler Release 12.1-FIPS” und “NetScaler Release 12.1-ndcpp” aufgeführt sind, werden auf den MPX 14000 FIPS- oder SDX 14000 FIPS-Plattformen nicht unterstützt. Diese Plattformen können andere neueste NetScaler-Firmware-Versionen verwenden, die auf der Downloadseite verfügbar sind.

Eine FIPS-Appliance ist mit einem manipulationssicheren (manipulationssicheren) kryptografischen Modul — einem Cavium CNN3560-NFBE-G — ausgestattet, das den FIPS 140-2 Level-3-Spezifikationen entspricht. Die kritischen Sicherheitsparameter (CSPs), hauptsächlich der private Schlüssel des Servers, werden sicher gespeichert und innerhalb des kryptografischen Moduls, auch HSM genannt, gespeichert und generiert. Auf die CSPs wird niemals außerhalb der Grenzen des HSM zugegriffen. Nur der Superuser (`nsroot`) kann Operationen an den im HSM gespeicherten Schlüsseln ausführen.

Bevor Sie eine FIPS-Appliance konfigurieren, müssen Sie den Status der FIPS-Karte überprüfen und

dann die Karte initialisieren. Erstellen Sie einen FIPS-Schlüssel und ein Serverzertifikat, und fügen Sie zusätzliche SSL-Konfiguration hinzu.

Informationen zu den unterstützten FIPS-Chiffern finden Sie unter FIPS-zugelassene Algorithmen und Chiffern.

Informationen zum Konfigurieren von FIPS-Appliances in einem HA-Setup finden Sie unter Konfigurieren von FIPS auf Appliances in einem HA-Setup.

Einschränkungen

1. SSL-Neuverhandlungen mit dem SSLv3-Protokoll werden im Backend einer MPX-FIPS-Appliance nicht unterstützt.
2. 1024-Bit- und 4096-Bit-Schlüssel und der Exponentwert von 3 werden nicht unterstützt.
3. Das 4096-Bit-Serverzertifikat wird nicht unterstützt.
4. Das 4096-Bit-Clientzertifikat wird nicht unterstützt (wenn die Clientauthentifizierung auf dem Back-End-Server aktiviert ist).

Konfigurieren des HSM

Bevor Sie das HSM auf einer MPX 14000 FIPS-Appliance konfigurieren, überprüfen Sie den Status Ihrer FIPS-Karte, um sicherzustellen, dass der Treiber korrekt geladen wurde. Initialisieren Sie dann die Karte.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show fips

FIPS Card is not configured
<!--NeedCopy-->
```

Die Meldung “FEHLER: Betrieb nicht zulässig - keine FIPS-Karte im System vorhanden” wird angezeigt, wenn der Treiber nicht korrekt geladen wurde.

Initialisieren der FIPS-Karte

Die Appliance muss dreimal neu gestartet werden, um die FIPS-Karte ordnungsgemäß zu initialisieren.

> **Wichtig**
>
> - Stellen Sie sicher, dass das Verzeichnis `/nsconfig/fips` erfolgreich auf der Appliance er-

> stellt wurde.
> - Speichern Sie die Konfiguration nicht, bevor Sie die Appliance zum dritten Mal neu starten.

Führen Sie die folgenden Schritte aus, um die FIPS-Karte zu initialisieren:

1. Setzen Sie die FIPS-Karte zurück (`reset fips`).
2. Starten Sie das Gerät neu (`reboot`).
3. Legen Sie das Kennwort für den Sicherheitsbeauftragten für die Partitionen 0 und 1 und das Benutzerkennwort für die Partition (`set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS`) fest.

   Hinweis: Die Ausführung des Befehls set oder reset dauert mehr als 60 Sekunden.
4. Speichern Sie die Konfiguration (`saveconfig`).
5. Stellen Sie sicher, dass der kennwortverschlüsselte Schlüssel für die Hauptpartition (master_pek.key) im Verzeichnis `/nsconfig/fips/` erstellt wurde.
6. Starten Sie das Gerät neu (`reboot`).
7. Stellen Sie sicher, dass der kennwortverschlüsselte Schlüssel für die Standardpartition (default_pek.key) im Verzeichnis `/nsconfig/fips/` erstellt wurde.
8. Starten Sie das Gerät neu (`reboot`).
9. Stellen Sie sicher, dass die FIPS-Karte UP (`show fips`) ist.

Initialisieren Sie die FIPS-Karte über die CLI

Der Befehl `set fips` initialisiert das Hardware Security Module (HSM) auf der FIPS-Karte und legt ein neues Kennwort und ein neues Benutzerkennwort für den Sicherheitsbeauftragten fest.

Vorsicht: Dieser Befehl löscht alle Daten auf der FIPS-Karte. Sie werden aufgefordert, bevor Sie mit der Befehlsausführung fortfahren. Vor und nach dem Ausführen dieses Befehls ist ein Neustart erforderlich, damit die Änderungen übernommen werden. Speichern Sie die Konfiguration, nachdem Sie diesen Befehl ausgeführt haben und bevor Sie die Appliance neu starten.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
reset fips

reboot

set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. Do you want
    to continue?(Y/N)y
```



```
8
9 <!--NeedCopy-->
```

Hinweis: Die folgende Meldung wird angezeigt, wenn Sie den `set fips` Befehl ausführen:

```
1 This command will erase all data on the FIPS card. You must save the
     configuration (saveconfig) after executing this command. [Note: On
     MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
     default, and the -initHSM Level-2 option is internally converted to
     Level-3]  Do you want to continue?(Y/N)y
2
3 saveconfig
4
5 reboot
6
7 reboot
8
9 show fips
10
11         FIPS HSM Info:
12                  HSM Label               : NetScaler FIPS
13                  Initialization          : FIPS-140-2 Level-3
14                  HSM Serial Number       : 3.1G1836-ICM000136
15                  HSM State               : 2
16                  HSM Model               : NITROX-III CNN35XX-NFBE
17                  Hardware Version        : 0.0-G
18                  Firmware Version        : 1.0
19                  Firmware Build          : NFBE-FW-1.0-48
20                  Max FIPS Key Memory     : 102235
21                  Free FIPS Key Memory    : 102231
22                  Total SRAM Memory       : 557396
23                  Free SRAM Memory        : 262780
24                  Total Crypto Cores      : 63
25                  Enabled Crypto Cores    : 63
26
27 <!--NeedCopy-->
```

Erstellen eines FIPS-Schlüssels

Sie können einen FIPS-Schlüssel auf Ihrer MPX 14000 FIPS-Einheit erstellen oder einen vorhandenen FIPS-Schlüssel in die Appliance importieren. Die MPX 14000 FIPS-Appliance unterstützt nur 2048-Bit- und 3072-Bit-Schlüssel und einen Exponentenwert von F4 (dessen Wert 65537 ist). Für PEM-Schlüssel ist kein Exponent erforderlich. Stellen Sie sicher, dass der FIPS-Schlüssel korrekt erstellt wurde. Er-

stellen Sie eine Zertifikatsignieranforderung und ein Serverzertifikat. Fügen Sie abschließend das Zertifikatschlüsselpaar zu Ihrer Appliance hinzu.

Geben Sie den Schlüsseltyp an (RSA oder ECDSA). Geben Sie für ECDSA-Schlüssel nur die Kurve an. Die ECDSA-Schlüsselerstellung mit Kurve P_256 und P_384 wird unterstützt.

> **Hinweis:**
>
> 1024-Bit- und 4096-Bit-Schlüssel und ein Exponentenwert von 3 werden nicht unterstützt.

Erstellen Sie über die CLI einen FIPS-Schlüssel

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent ( 3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Example1:

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4


show ssl fipskey f1

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (Hex: 0x10001)

<!--NeedCopy-->
```

Example2:

```
> create fipskey f2 -keytype ECDSA -curve P_256


> sh fipskey f2
    FIPS Key Name: f2   Key Type: ECDSA Curve: P_256

<!--NeedCopy-->
```

Erstellen eines FIPS-Schlüssels mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Hinzufügen**.

3. Geben Sie im Dialogfeld FIPS-Schlüssel erstellen Werte für die folgenden Parameter an:
   - FIPS-Schlüsselname*—FIPSKeyname
   - Modul*—Modul
   - Exponent*—Exponent

   * Ein erforderlicher Parameter
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
5. Vergewissern Sie sich auf der Registerkarte FIPS-Tasten, dass die für den von Ihnen erstellten FIPS-Schlüssel angezeigten Einstellungen korrekt sind.

Importieren eines FIPS-Schlüssels

Um einen vorhandenen FIPS-Schlüssel mit Ihrer FIPS-Appliance zu verwenden, müssen Sie den FIPS-Schlüssel von der Festplatte der Appliance in das HSM übertragen.

Hinweis: Um Fehler beim Importieren eines FIPS-Schlüssels zu vermeiden, stellen Sie sicher, dass der Name des importierten Schlüssels mit dem ursprünglichen Schlüsselnamen übereinstimmt, als er erstellt wurde.

Importieren eines FIPS-Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-
   wrapKeyName <string>] [-iv<string>] -exponent  F4 ]
<!--NeedCopy-->
```

Beispiel:

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4


import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM

<!--NeedCopy-->
```

Stellen Sie sicher, dass der FIPS-Schlüssel korrekt erstellt oder importiert wurde, indem Sie den`show fipskey` Befehl ausführen.

```
show fipskey
1)      FIPS Key Name: Key-FIPS-2

<!--NeedCopy-->
```


Importieren eines FIPS-Schlüssels mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Importieren**.
3. Wählen Sie im Dialogfeld Als FIPS-Schlüssel importieren die FIPS-Schlüsseldatei aus und legen Sie Werte für die folgenden Parameter fest:
   - FIPS-Schlüsselname*
   - Schlüsseldateiname* — Um die Datei an einem anderen Speicherort als dem Standardwert zu platzieren, geben Sie den vollständigen Pfad an oder klicken Sie auf **Durchsuchen** und navigieren Sie zu einem Speicherort.
   - Exponent*

   * Ein erforderlicher Parameter
4. Klicken Sie auf **Importieren**und dann auf **Schließen**.
5. Vergewissern Sie sich auf der Registerkarte FIPS-Tasten, dass die für den importierten FIPS-Schlüssel angezeigten Einstellungen korrekt sind.

Exportieren eines FIPS-Schlüssels

Citrix empfiehlt, ein Backup eines Schlüssels zu erstellen, der im FIPS HSM erstellt wurde. Wenn ein Schlüssel im HSM gelöscht wird, können Sie den gleichen Schlüssel nicht erneut erstellen, und alle damit verbundenen Zertifikate werden nutzlos gemacht.

Zusätzlich zum Exportieren eines Schlüssels als Backup müssen Sie möglicherweise einen Schlüssel für die Übertragung auf eine andere Appliance exportieren.

Das folgende Verfahren enthält Anweisungen zum Exportieren eines FIPS-Schlüssels in den Ordner `/nsconfig/ssl` auf dem CompactFlash der Appliance und zum Sichern des exportierten Schlüssels mithilfe einer starken asymmetrischen Schlüsselverschlüsselungsmethode.

Exportieren Sie einen FIPS-Schlüssel über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
export ssl fipsKey <fipsKeyName> -key <string>
<!--NeedCopy-->
```

Beispiel:

```
export fipskey Key-FIPS-1 -key Key-FIPS-1.key
<!--NeedCopy-->
```


Exportieren Sie einen FIPS-Schlüssel über die GUI

1. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Exportieren**.
3. Geben Sie im Dialogfeld FIPS-Schlüssel in eine Datei exportieren Werte für die folgenden Parameter an:
   - FIPS-Schlüsselname*—FIPSKeyname
   - Dateiname* — Schlüssel (Um die Datei an einem anderen als dem Standardspeicherort abzulegen, können Sie entweder den vollständigen Pfad angeben oder auf die Schaltfläche Durchsuchen klicken und zu einem Speicherort navigieren.)

   * Ein erforderlicher Parameter
4. Klicken Sie auf **Exportieren**und dann auf **Schließen**.

Importieren eines externen Schlüssels

Sie können FIPS-Schlüssel übertragen, die im HSM der NetScaler-Appliance erstellt wurden. Sie können auch externe private Schlüssel (wie Schlüssel, die mit einem Standard-NetScaler, Apache oder IIS erstellt wurden) auf eine NetScaler FIPS-Appliance übertragen. Externe Schlüssel werden außerhalb des HSM mithilfe eines Tools wie OpenSSL erstellt. Bevor Sie einen externen Schlüssel in das HSM importieren, kopieren Sie ihn auf das Flash-Laufwerk der Appliance unter `/nsconfig/ssl`.

Auf den MPX 14000 FIPS-Appliances ist der Parameter -exponent im Befehl **`import`** `ssl fipskey` beim Importieren eines externen Schlüssels nicht erforderlich. Der richtige öffentliche Exponent wird automatisch erkannt, wenn der Schlüssel importiert wird, und der Wert des -exponent-Parameters wird ignoriert.

Die NetScaler FIPS-Appliance unterstützt keine externen Schlüssel mit einem anderen öffentlichen Exponenten als 3 oder F4.

Sie benötigen keinen Wrap Key auf den MPX 14000 FIPS-Appliances.

Sie können einen externen, verschlüsselten FIPS-Schlüssel nicht direkt in eine MPX 14000 FIPS-Appliance importieren. Um den Schlüssel zu importieren, müssen Sie zuerst den Schlüssel entschlüsseln und dann importieren. Um den Schlüssel zu entschlüsseln, geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
openssl rsa -in <EncryptedKey.key> > <DecryptedKey.out>
<!--NeedCopy-->
```

Hinweis: Wenn Sie einen RSA-Schlüssel als FIPS-Schlüssel importieren, empfiehlt Citrix, den RSA-Schlüssel aus Sicherheitsgründen aus der Appliance zu löschen.

Importieren Sie einen externen Schlüssel als FIPS-Schlüssel über die Befehlszeilenschnittstelle

1. Kopieren Sie den externen Schlüssel auf das Flash-Laufwerk der Appliance.
2. Wenn der Schlüssel im PFX-Format ist, müssen Sie ihn zuerst in das PEM-Format konvertieren. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
convert ssl pkcs12 <output file> -import -pkcs12File <input .pfx
   file name> -password <password>
<!--NeedCopy-->
```

3. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den externen Schlüssel als FIPS-Schlüssel zu importieren und die Einstellungen zu überprüfen:

```
import ssl fipsKey <fipsKeyName> -key <string> -informPEM
show ssl fipskey<fipsKeyName>
<!--NeedCopy-->
```

Beispiel:

```
convert ssl pkcs12 iis.pem -password 123456 -import -pkcs12File iis.pfx

import fipskey Key-FIPS-2 -key iis.pem -inform PEM

show ssl fipskey key-FIPS-2

FIPS Key Name: Key-FIPS-2 Modulus: 0   Public Exponent: F4 (Hex value 0
   x10001)
<!--NeedCopy-->
```

Importieren Sie einen externen Schlüssel als FIPS-Schlüssel über die grafische Benutzeroberfläche

1. Wenn der Schlüssel im PFX-Format ist, müssen Sie ihn zuerst in das PEM-Format konvertieren.
   a) Navigieren Sie zu **Traffic Management > SSL**.
   b) Klicken Sie im Detailbereich unter Tools auf **PKCS importieren #12**.
   c) Stellen Sie im Dialogfeld PKCS12-Datei importieren die folgenden Parameter ein:
      - Name der Ausgabedatei*
      - PKCS12-Dateiname* — Geben Sie den Pfx-Dateinamen an.
      - Kennwort importieren*
      - Kodierungsformat

      *Ein erforderlicher Parameter

2. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
3. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Importieren**.
4. Wählen Sie im Dialogfeld Als FIPS-Schlüssel importieren die PEM-Datei aus und legen Sie Werte für die folgenden Parameter fest:
   - FIPS-Schlüsselname*
   - Schlüsseldateiname* — Um die Datei an einem anderen als dem Standardspeicherort abzulegen, können Sie entweder den vollständigen Pfad angeben oder auf Durchsuchen klicken und zu einem Speicherort navigieren.

   * Ein erforderlicher Parameter
5. Klicken Sie auf **Importieren**und dann auf **Schließen**.
6. Vergewissern Sie sich auf der Registerkarte FIPS-Tasten, dass die für den importierten FIPS-Schlüssel angezeigten Einstellungen korrekt sind.

Konfigurieren von FIPS auf Appliances in einem HA-Setup

Sie können zwei Appliances in einem HA-Paar als FIPS-Appliances konfigurieren.

Voraussetzungen

- Das Hardware Security Module (HSM) muss auf beiden Appliances konfiguriert sein. Weitere Informationen finden Sie unter Konfigurieren des HSM.
- Stellen Sie bei Verwendung der GUI sicher, dass sich die Appliances bereits in einem HA-Setup befinden. Weitere Informationen zum Konfigurieren eines HA-Setups finden Sie unter Hochverfügbarkeit.

> **Hinweis:**
>
> Citrix empfiehlt, das Konfigurationsdienstprogramm (GUI) für dieses Verfahren zu verwenden. Wenn Sie die Befehlszeile (CLI) verwenden, stellen Sie sicher, dass Sie die im Verfahren aufgeführten Schritte sorgfältig ausführen. Das Ändern der Reihenfolge der Schritte oder das Angeben einer falschen Eingabedatei kann zu Inkonsistenzen führen, die einen Neustart der Appliance erfordert. Wenn Sie die CLI verwenden, wird der Befehl `create ssl fipskey` außerdem nicht an den sekundären Knoten weitergegeben. Wenn Sie den Befehl mit denselben Eingabewerten für Modulgröße und Exponent auf zwei verschiedenen FIPS-Appliances ausführen, sind die generierten Schlüssel nicht dieselben. Erstellen Sie den FIPS-Schlüssel auf einem der Knoten und übertragen Sie ihn dann auf den anderen Knoten. Wenn Sie jedoch das Konfigurationsdienstprogramm verwenden, um FIPS-Appliances in einem HA-Setup zu konfigurieren, wird der von Ihnen erstellte FIPS-Schlüssel automatisch an den sekundären Knoten übertragen. Das Verwalten und

> Übertragen der FIPS-Schlüssel wird als sicheres Informationsmanagement (SIM) bezeichnet.

Wichtig: Das HA-Setup muss innerhalb von sechs Minuten abgeschlossen sein. Wenn das Verfahren bei irgendeinem Schritt fehlschlägt, gehen Sie wie folgt vor:

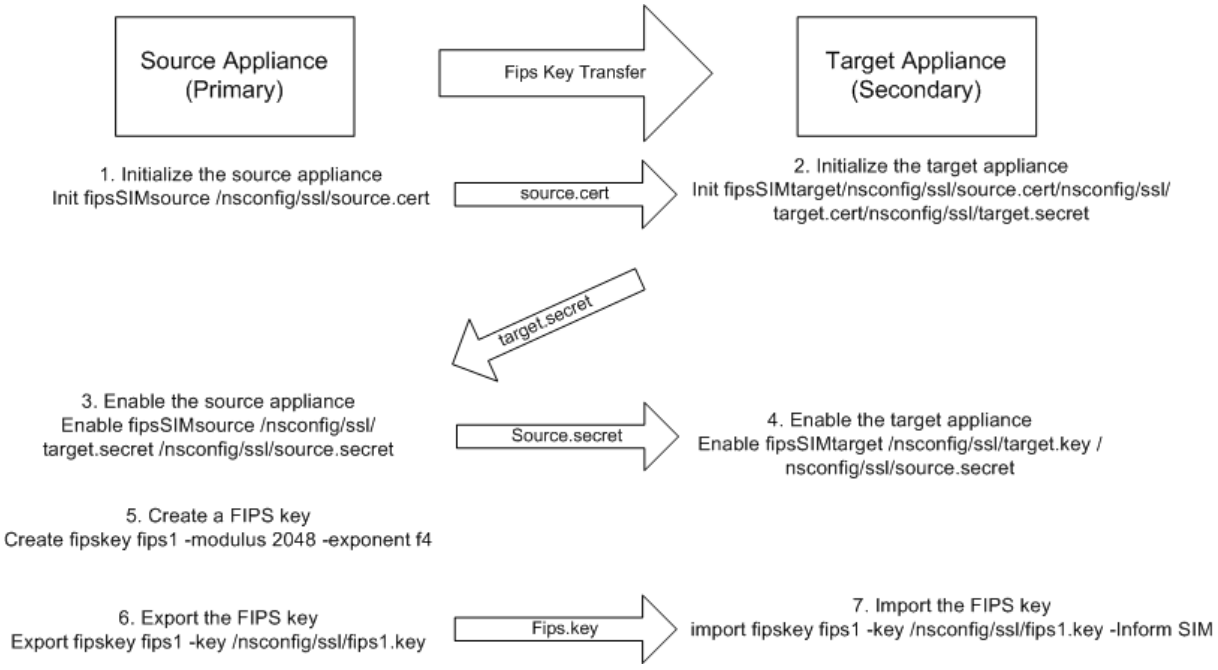
> 1. Starten Sie das Gerät neu oder warten Sie 10 Minuten.
> 2. Entfernen Sie alle durch das Verfahren erstellten Dateien.
> 3. Wiederholen Sie den HA-Setup-Vorgang.
>
> Verwenden Sie keine vorhandenen Dateinamen wieder.

Im folgenden Verfahren ist Appliance A der primäre Knoten und Appliance B der sekundäre Knoten.

Konfigurieren Sie FIPS auf Appliances in einem HA-Setup über die Befehlszeilenschnittstelle

Das folgende Diagramm fasst den Übertragungsprozess auf der CLI zusammen.

Abbildung 1. Übertragen Sie die FIPS-Schlüsselzusammenfassung



1. Öffnen Sie auf **Appliance A** eine SSH-Verbindung zur Appliance mithilfe eines SSH-Clients, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
3. Initialisieren Sie Appliance A als Quell-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 init ssl fipsSIMsource <certFile>
2 <!--NeedCopy-->
```


Beispiel:

```
init fipsSIMsource /nsconfig/ssl/nodeA.cert
```

4. Kopieren Sie diese Datei <certFile> auf Appliance B im Ordner /nconfig/ssl.

   Beispiel:

   ```
   scp /nsconfig/ssl/nodeA.cert nsroot@198.51.100.10:/nsconfig/ssl
   ```

5. Öffnen Sie**auf Appliance B**mithilfe eines SSH-Clients wie PuTTY eine SSH-Verbindung zur Appliance.
6. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
7. Initialisieren Sie Appliance B als Ziel-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   1 init ssl fipsSIMtarget <certFile> <keyVector> <targetSecret>
   2 <!--NeedCopy-->
   ```

   Beispiel:

   ```
   init fipsSIMtarget /nsconfig/ssl/nodeA.cert /nsconfig/ssl/nodeB.key /
   nsconfig/ssl/nodeB.secret
   ```

8. Kopieren Sie diese Datei <targetSecret> auf Appliance A.

   Beispiel:

   ```
   scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.20:/nsconfig/
   ssl
   ```

9. Aktivieren Sie**auf Appliance**A Appliance A als Quell-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   1 enable ssl fipsSIMSource <targetSecret> <sourceSecret>
   2 <!--NeedCopy-->
   ```

   Beispiel:

   ```
   enable fipsSIMsource /nsconfig/ssl/nodeB.secret /nsconfig/ssl/nodeA.
   secret
   ```

10. Kopieren Sie diese Datei <sourceSecret> auf Appliance B.

    Beispiel:

    ```
    scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.10:/nsconfig/
    ssl
    ```

11. Aktivieren Sie**auf Einheit B**Einheit B als Ziel-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:


```
enable ssl fipsSIMtarget <keyVector> <sourceSecret>
<!--NeedCopy-->
```

Beispiel:

```
enable fipsSIMtarget /nsconfig/ssl/nodeB.key /nsconfig/ssl/nodeA.secret
```

12. Erstellen Sie**auf Appliance A**einen FIPS-Schlüssel, wie unter Erstellen eines FIPS-Schlüsselsbeschrieben.
13. Exportieren Sie den FIPS-Schlüssel auf die Festplatte der Appliance, wie unter Einen FIPS-Schlüssel exportierenbeschrieben.
14. Kopieren Sie den FIPS-Schlüssel auf die Festplatte der sekundären Appliance mithilfe eines sicheren Dateiübertragungsdienstprogramms, z. B. SCP.
15. Importieren Sie**auf Appliance B**den FIPS-Schlüssel von der Festplatte in das HSM der Appliance, wie unter Einen FIPS-Schlüssel importierenbeschrieben.

Konfigurieren Sie FIPS auf Appliances in einem HA-Setup über die grafische Benutzeroberfläche

1. Navigieren Sie auf der Appliance, die als primäre Quell-Appliance konfiguriert werden soll, zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Info auf **SIM aktivieren**.
3. Geben **Sie im Dialogfeld SIM für HA-Paar aktivieren** im Textfeld **Zertifikatsdateiname** den Dateinamen ein. Der Dateiname muss den Pfad zu dem Speicherort enthalten, an dem das FIPS-Zertifikat auf der Quell-Appliance gespeichert werden muss.
4. Geben Sie im Textfeld **Key Vector Dateiname** den Dateinamen ein. Der Dateiname muss den Pfad zu dem Speicherort enthalten, an dem der FIPS-Schlüsselvektor auf der Quell-Appliance gespeichert werden muss.
5. Geben Sie im Textfeld **Target Secret File Name** den Speicherort für die Speicherung der geheimen Daten auf der Ziel-Appliance ein.
6. Geben Sie im Textfeld **Source Secret File Name** den Speicherort für die Speicherung der geheimen Daten auf der Quell-Appliance ein.
7. Geben Sie unter **Secondary System Login Credential**die Werte für **Benutzername** und **Kennwort ein**.
8. Klicken Sie auf **OK**. Die FIPS-Appliances sind jetzt im HA-Modus konfiguriert.

Hinweis: Erstellen Sie nach der Konfiguration der Appliances in HA einen FIPS-Schlüssel, wie unter Erstellen eines FIPS-Schlüsselsbeschrieben. Der FIPS-Schlüssel wird automatisch von der primären auf die sekundäre Appliance übertragen.

Erstellen einer Zertifikatsignaturanforderung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
   <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
    [-organizationUnitName <string>] [-localityName <string>] [-
    commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
<!--NeedCopy-->
```

Beispiel:

```
>create certreq f1.req  - fipsKeyName  f1 -countryName US  -stateName CA
    -organizationName Citrix -companyName Citrix -commonName ctx -
   emailAddress test@example.com
Done
<!--NeedCopy-->
```

Erstellen eines Serverzertifikats über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
   input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
    input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
    input_filename>][-CAkeyForm ( DER | PEM )] [-CAserial <
    output_filename>]
<!--NeedCopy-->
```

Beispiel:

```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
   root.key -CAserial ns-root.srl -days 1000
Done
<!--NeedCopy-->
```

Im vorangegangenen Beispiel wird ein Serverzertifikat mithilfe einer lokalen Stammzertifizierungsstelle auf der Appliance erstellt.

Hinzufügen eines Zertifikatschlüsselpaars mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>][-
    expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Beispiel:

```
add certkey cert1 -cert f1.cert -fipsKey f1

<!--NeedCopy-->
```

Nachdem Sie den FIPS-Schlüssel und das Serverzertifikat erstellt haben, können Sie die generische SSL-Konfiguration hinzufügen. Aktivieren Sie die Funktionen, die für Ihre Bereitstellung erforderlich sind. Fügen Sie Server, Dienste und virtuelle SSL-Server hinzu. Binden Sie das Zertifikatschlüsselpaar und den Dienst an den virtuellen SSL-Server. Speichern Sie die Konfiguration.

```
enable ns feature SSL LB

add server s1 10.217.2.5

add service sr1 s1 HTTP 80

add lb vserver v1 SSL 10.217.2.172 443

bind ssl vserver v1  -certkeyName cert1

bind lb vserver v1 sr1

saveconfig

<!--NeedCopy-->
```

Die Grundkonfiguration Ihrer MPX 14000 FIPS Appliance ist nun abgeschlossen.

Weitere Informationen zum Konfigurieren von sicherem HTTPS erhalten Sie, indem Sie auf FIPS konfigurierenklicken.

Weitere Informationen zum Konfigurieren von sicherem RPC erhalten Sie, wenn Sie zum ersten Mal auf FIPS konfigurierenklicken.

Aktualisieren der Lizenz auf einer MPX 14000 FIPS-Appliance

Jedes Update der Lizenz auf dieser Plattform erfordert zwei Neustarts.

1. Aktualisieren Sie die Lizenz im Ordner `/nsconfig/license`.
2. Starten Sie die Appliance neu.
3. Melden Sie sich bei der Einheit an.
4. Starten Sie das Gerät erneut neu.
   Hinweis: Fügen Sie vor dem zweiten Neustart keine neuen Befehle hinzu, speichern Sie die Konfiguration oder überprüfen Sie den Systemstatus.
5. Melden Sie sich bei der Appliance an und stellen Sie sicher, dass FIPS durch Ausführen des Befehls `show ssl fips` initialisiert wird.

Unterstützung für den Hybrid-FIPS-Modus auf den Plattformen MPX 14000 FIPS und SDX 14000 FIPS

> **Hinweis:**
>
> Diese Funktion wird nur auf der neuen MPX/SDX 14000 FIPS-Plattform unterstützt, die eine primäre FIPS-Karte und eine oder mehrere Sekundärkarten enthält. Es wird nicht auf einer VPX-Plattform oder einer Plattform unterstützt, die nur einen Hardwarekartentyp enthält.

Auf einer FIPS-Plattform erfolgt die asymmetrische und symmetrische Verschlüsselung und Entschlüsselung aus Sicherheitsgründen auf der FIPS-Karte. Sie können jedoch einen Teil dieser Aktivität (asymmetrisch) auf einer FIPS-Karte ausführen und die Massenverschlüsselung und -entschlüsselung (symmetrisch) auf eine andere Karte übertragen, ohne die Sicherheit Ihrer Schlüssel zu beeinträchtigen.

Die neue MPX/SDX 14000 FIPS-Plattform enthält eine Primärkarte und eine oder mehrere Sekundärkarten. Wenn Sie den Hybrid-FIPS-Modus aktivieren, werden die geheimen Entschlüsselungsbefehle vor dem Master auf der Primärkarte ausgeführt, da der private Schlüssel auf dieser Karte gespeichert ist. Die Massenverschlüsselung und -entschlüsselung wird jedoch auf die Sekundärkarte abgeladen. Dieser Offload erhöht den Massenverschlüsselungsdurchsatz auf einer MPX/SDX 14000 FIPS-Plattform im Vergleich zum Nicht-Hybrid-FIPS-Modus und der vorhandenen MPX 9700/10500/12500/15000 FIPS-Plattform erheblich. Durch die Aktivierung des Hybrid-FIPS-Modus wird auch die SSL-Transaktion pro Sekunde auf dieser Plattform verbessert.

> **Hinweise:**
>
> - Der hybride FIPS-Modus ist standardmäßig deaktiviert, um die strengen Zertifizierungsanforderungen zu erfüllen, bei denen die gesamte Kryptoberechnungen in einem FIPS-zertifizierten Modul durchgeführt werden müssen. Aktivieren Sie den Hybridmodus, um die Massenverschlüsselung und -entschlüsselung auf die sekundäre Karte zu übertragen.
> - Auf einer SDX 14000 FIPS-Plattform müssen Sie zuerst der VPX-Instanz einen SSL-Chip

> zuweisen, bevor Sie den Hybridmodus aktivieren.

Aktivieren Sie den Hybrid-FIPS-Modus über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set SSL parameter -hybridFIPSMode {
 ENABLED|DISABLED }


Arguments

hybridFIPSMode

When this mode is enabled, system will use additional crypto hardware
   to accelerate symmetric crypto operations.

Possible values: ENABLED, DISABLED

Default value: DISABLED
<!--NeedCopy-->
```

Beispiel:

```
    set SSL parameter -hybridFIPSMode ENABLED
    show SSL parameter
    Advanced SSL Parameters
    ----------------------
    . . . . . .
    Hybrid FIPS Mode    : ENABLED
    . . . . . .

<!--NeedCopy-->
```

Aktivieren Sie den Hybrid-FIPS-Modus über die GUI

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Erweiterte SSL-Einstellungen ändern**.
3. Wählen **Sie im Dialogfeld Erweiterte SSL-Einstellungen ändern** die Option **Hybrid FIPS-Modus**aus.

Einschränkungen:

1. Neuverhandlungen werden nicht unterstützt.

2. Der Befehl `stat ssl parameter` auf einer SDX 14000-Plattform zeigt nicht den korrekten Prozentsatz der sekundären Kartenauslastung an. Es zeigt immer 0,00% Auslastung an.

```
stat ssl

SSL Summary
# SSL cards present 1
# SSL cards UP  1
# Secondary SSL cards present   4
# Secondary SSL cards UP    4
SSL engine status      1
SSL sessions (Rate)     963
Secondary card utilization (%)     0.00
<!--NeedCopy-->
```

SDX 14000 FIPS-Appliances

August 15, 2023

> **Hinweis**
>
> Die Firmware-Versionen, die auf der NetScaler-Downloadseite unter “NetScaler Release 12.1-FIPS” und “NetScaler Release 12.1-NdCPP” aufgeführt sind, werden auf den MPX 14000 FIPS- oder SDX 14000 FIPS-Plattformen nicht unterstützt. Diese Plattformen können andere neueste NetScaler-Firmware-Versionen verwenden, die auf der Downloadseite verfügbar sind.

Eine NetScaler SDX-Appliance ist eine Multitenant-Plattform, auf der Sie mehrere virtuelle NetScaler-Instanzen bereitstellen und verwalten können. Die SDX-Appliance erfüllt Cloud-Computing- und Multitenancy-Anforderungen, indem sie es einem einzelnen Administrator ermöglicht, die Appliance zu konfigurieren und zu verwalten und die Verwaltung jeder gehosteten Instanz an Mandanten zu delegieren.

Eine NetScaler SDX 14030/14060/14080 FIPS-Appliance bietet die Funktionen einer SDX-Appliance mit FIPS-Funktionalität. Es ist mit einem manipulationssicheren (manipulationssicheren) kryptografischen Modul — einem Cavium CNN3560-NFBE-G — ausgestattet, das den FIPS 140-2 Level-3-Spezifikationen entspricht. Die Critical Security Parameters (CSPs), hauptsächlich der private Schlüssel des Servers, werden sicher gespeichert und innerhalb des kryptographischen Moduls generiert. Dieses Modul wird auch als das Hardware Security Module (HSM) bezeichnet. Auf die CSPs wird niemals außerhalb der Grenzen des HSM zugegriffen. Nur der Superuser (`nsroot`) kann Operationen an den im HSM gespeicherten Schlüsseln ausführen.

Eine NetScaler SDX 14030/14060/14080 FIPS-Appliance enthält ein FIPS HSM-Modul mit 63 Ker-

nen. Das FIPS HSM-Modul kann auf bis zu maximal 32 Partitionen partitioniert werden. Der SDX-Administrator kann jeder Partition dedizierten Schlüsselspeicher, kryptografische Ressourcen und die Anzahl der Krypto-SSL-FIPS-Kerne zuweisen. Schlüssel und Ressourcen, die einer Partition zugewiesen sind, sind dediziert und sicher, und jede andere Partition kann nicht auf sie zugreifen oder sie gemeinsam nutzen.

Die von Ihnen erstellte FIPS-HSM-Partition kann zum Zeitpunkt der Bereitstellung der Instanz oder später durch Bearbeiten der Instanz einer VPX-Instanz zugewiesen oder angehängt werden. Die erstellte und an eine Instanz angehängte FIPS-Partition verhält sich für diese Instanz wie ein virtuelles HSM-Modul.

Den VPX-Instanzen auf einer SDX 14030/14060/14080 FIPS-Einheit wird eine Partition für virtuelle FIPS-Funktionen (VF) zugewiesen, die als isolierte virtuelle FIPS-Karte oder HSM behandelt wird. Daher ähneln die Schritte zum Konfigurieren einer FIPS-Partition innerhalb einer VPX-Instanz den Schritten zum Konfigurieren einer MPX-FIPS-Appliance. Einzelheiten zur Einhaltung der Vorschriften finden Sie in den Sicherheitsrichtlinien auf der Website des U.S. National Institute of Standards and Technology (NIST).

Informationen zur Konfiguration von FIPS-Appliances in einem Hochverfügbarkeits-Setup finden Sie unter Konfiguration von FIPS-Appliances in einem HA-Setup.

> **Wichtig**
>
> Jeder Schlüssel enthält einen privaten und einen öffentlichen Schlüssel. Infolgedessen nimmt es zwei Schlüsselbereiche ein. Daher ist die maximale Anzahl von Schlüsseln auf einen unter der halben Schlüsselspeichergröße begrenzt.

Die SDX 14000 FIPS-Plattform unterstützt einen hybriden FIPS-Modus. In diesem Modus können Sie einen Teil der Verschlüsselungs- und Entschlüsselungsaktivität auf eine Nicht-FIPS-Karte auslagern. Weitere Informationen finden Sie unter Hybrid-FIPS-Modus.

Einschränkungen

January 19, 2021

1. SSL-Neuverhandlungen mit dem SSLv3-Protokoll werden im Backend einer SDX FIPS-Appliance nicht unterstützt.
2. 1024-Bit- und 4096-Bit-Schlüssel und ein Exponentenwert von 3 werden nicht unterstützt.
3. Backup und Wiederherstellung werden nicht unterstützt.
4. Cluster- und Verwaltungsdomänen werden nicht unterstützt.
5. Sie können nur eine FIPS-Partition an eine Instanz anhängen.
6. Einer Instanz mit einer FIPS-Partition kann nur ein CPU-Kern zugewiesen werden.

7. Sie können einer Instanz entweder eine FIPS-Partition oder einen SSL-Kern zuweisen, aber nicht beides.
8. Das 4096-Bit-Serverzertifikat wird nicht unterstützt.
9. Das 4096-Bit-Clientzertifikat wird nicht unterstützt (wenn die Clientauthentifizierung auf dem Back-End-Server aktiviert ist).

Terminologie

May 11, 2023

Zeroize: Setztdas HSM zurück. Alle Daten auf dem HSM werden gelöscht. Dieser Schritt ist obligatorisch, bevor das HSM initialisiert wird.

Initialisieren: Stellen Sie die HSM-Funktionen ein. Die NetScaler SDX FIPS-Appliance entspricht FIPS-140-2 Level 2. Sie können Partitionen erstellen, nachdem Sie den Chip initialisiert haben.

Schlüsselspeichergröße: Anzahl der Schlüssel, die auf einer Partition gespeichert werden können. Es können maximal 102235 Schlüssel angegeben werden. Die maximale Anzahl von Schlüsseln, die gespeichert werden können, ist um eins weniger als die Hälfte der angegebenen Anzahl. Wenn Sie beispielsweise 100 angeben, können Sie nur 49 Schlüssel erstellen, da einer der Schlüssel das RSA-Schlüsselpaar ist, das 2 Schlüsselspeicher verbraucht.

Crypto-Core-Kapazität: Anzahl der Krypto-Cores, die einer Partition zugewiesen sind. Maximal 63 Kerne sind verfügbar.

SSL-Kontext: Anzahl gleichzeitiger SSL-Verbindungen, die auf einer Partition erstellt werden können.

HSM initialisieren

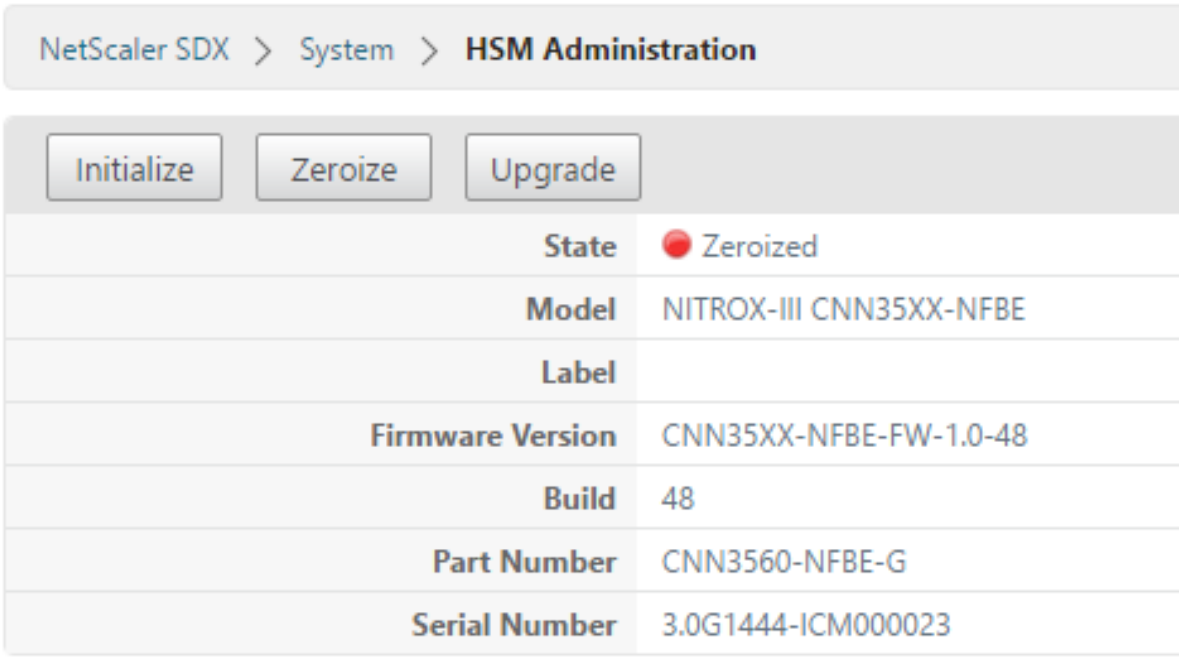
January 19, 2021

Bevor Sie das HSM initialisieren, müssen Sie es zunächst auf Null setzen.

Nullstellen des HSM mithilfe des Verwaltungsdienstes

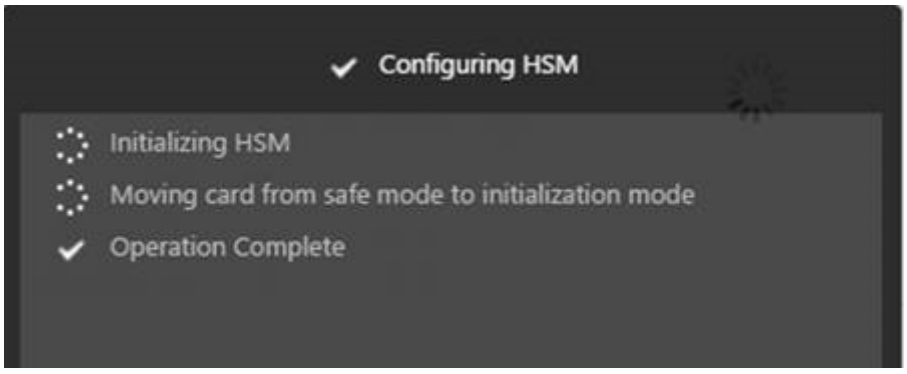
1. Öffnen Sie einen Browser, und melden Sie sich bei der Appliance an.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System > HSM-Administration**, und klicken Sie in der Detailebene auf **Zeroize**.

Alle Daten werden vom FIPS-Chip gelöscht und der Status wird als “Zeroized” angezeigt. Alle zuvor erstellten HSM-Partitionen werden gelöscht.

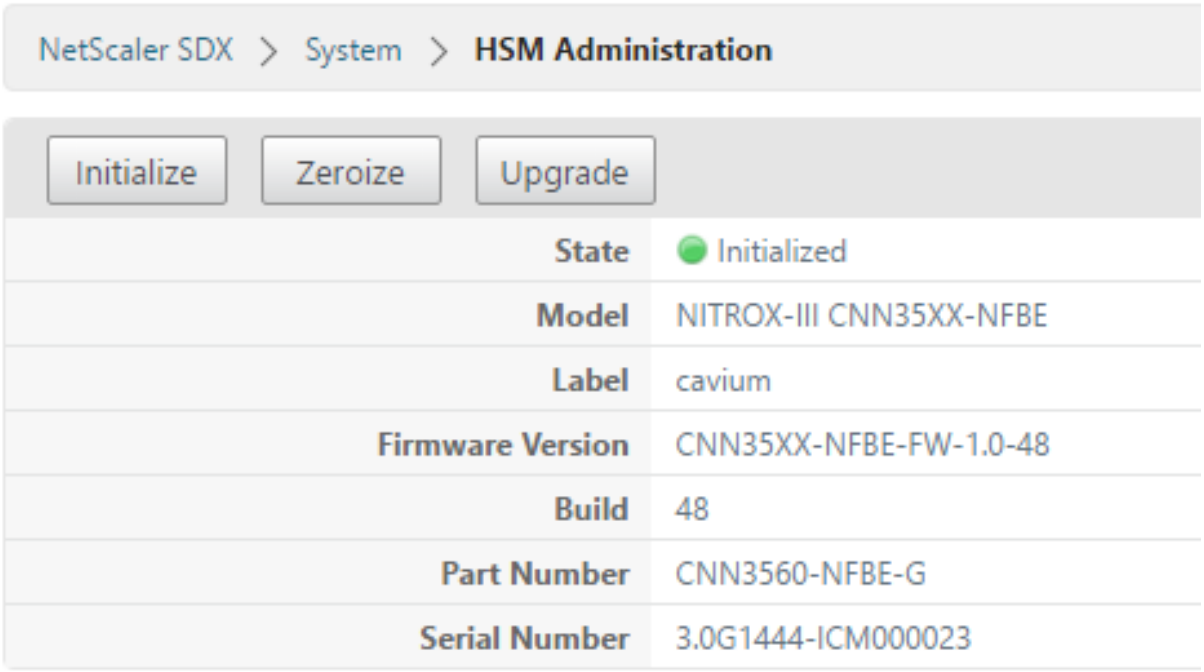


Initialisieren des HSM mit dem Verwaltungsdienst

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System > HSM-Administration**, und klicken Sie in der Detailebene auf **Initialisieren**.
2. Geben Sie einen neuen Benutzernamen ein, geben Sie ein Kennwort an, und klicken Sie auf **OK**.



Der Kartenstatus wird als Initialisiert angezeigt.



Partitionen erstellen

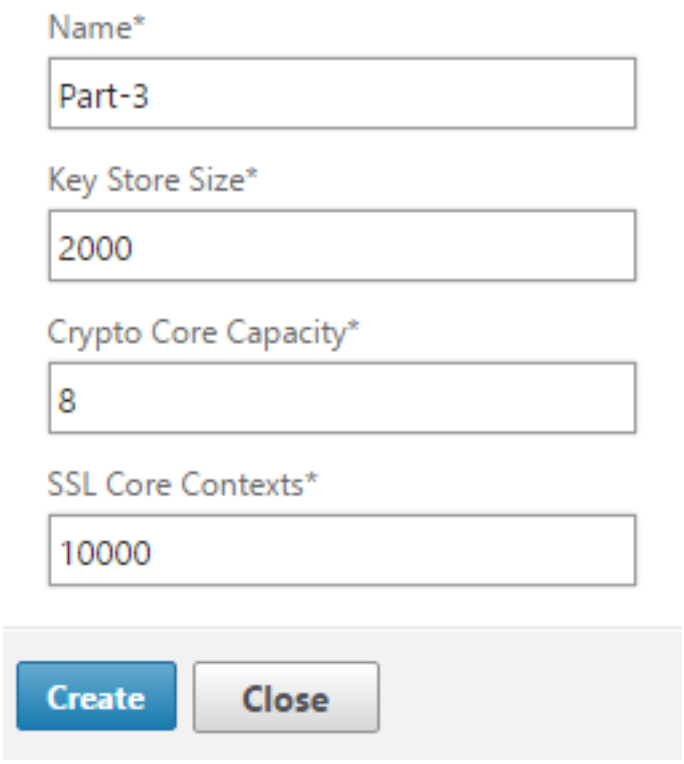
May 11, 2023

Erstellen Sie Partitionen für verschiedene Mandanten und geben Sie die kryptografischen Ressourcen für jede Partition an. Jeder Instanz wird eine Partition zugewiesen, und eine Partition kann nur einer Instanz zugewiesen werden. Durch das Löschen einer Instanz wird die der Instanz zugewiesene Partition gelöscht. Dadurch werden auch die Partitionsdaten gelöscht und sie bleiben nicht ungesichert oder sind später zugänglich. Die Anzahl der Schlüssel und die SSL-Kontextzuweisung hängen von Ihrer Anwendung ab. Informationen zur Anzahl der zuzuweisenden Kerne finden Sie im NetScaler-Datenblatt.

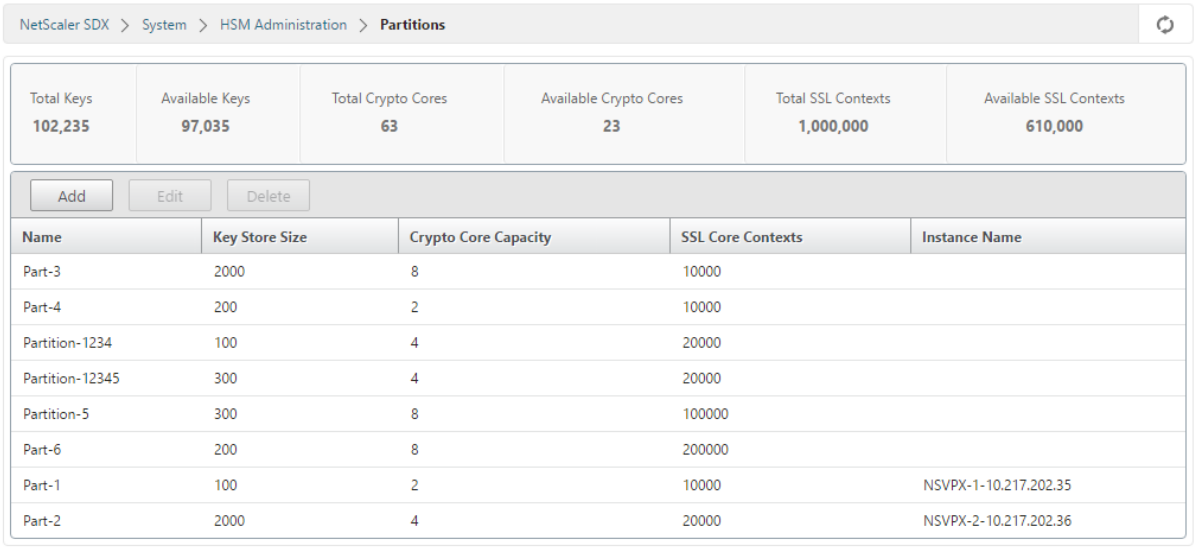
> **Wichtig**
>
> Nachdem Sie einer HSM-Partition eine Schlüsselspeichergröße und Kerne zugewiesen haben, können Sie diese zur Laufzeit nicht mehr ändern. Trennen Sie zuerst die Partition von der Instanz.

Erstellen Sie eine Partition mithilfe des Management Service

1. **Navigieren Sie auf der Registerkarte Konfiguration zu**System**>**HSM Administration**>**Partitionen**und klicken Sie in der Detailebene auf Hinzufügen.**
2. Geben Sie einen Namen für die Partition und die Ressourcen an, die dieser Partition zugewiesen werden sollen.
3. Klicken Sie auf **OK**.



Auf der Übersichtsseite werden alle Partitionen angezeigt, die erstellt wurden. Einigen Partitionen wird eine Instanz zugewiesen, während es sich bei anderen um freie Partitionen handelt.



Bereitstellen einer neuen Instanz oder Ändern eine vorhandene Instanz und Zuweisen einer Partition

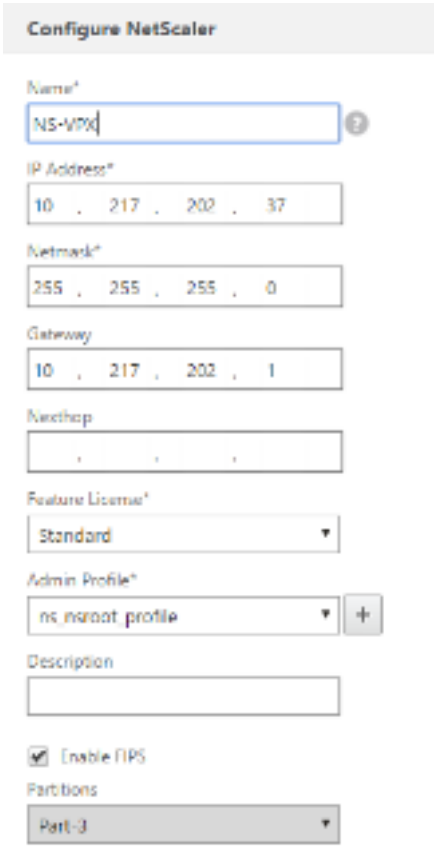
August 11, 2022

Nachdem Sie die Partitionen erstellt haben, müssen Sie sie Instanzen zuweisen.

> **Wichtig:**
>
> - Sie können nur eine FIPS-Partition an eine Instanz anhängen.
> - Einer Instanz mit einer FIPS-Partition kann nur ein CPU-Kern zugewiesen werden.

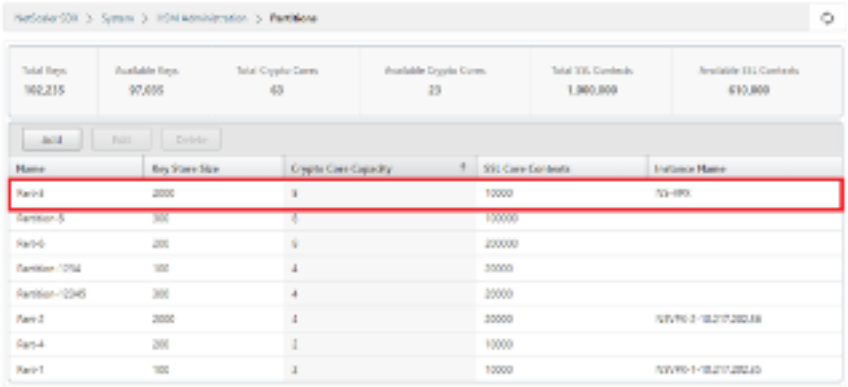
Bereitstellen einer neuen Instanz oder Ändern einer vorhandenen Instanz

1. Navigieren Sie auf der Registerkarte Konfiguration zu **NetScaler** > **Instances**, und fügen Sie eine Instanz hinzu oder ändern Sie sie.
2. Wählen Sie **FIPS aktivieren** und wählen Sie in der Liste **Partitionen** eine Partition aus, die an diese Instanz angehängt werden soll.



Sie können überprüfen, ob die Partition an eine Instanz angehängt ist, indem Sie entweder die GUI oder die CLI verwenden.

Navigieren Sie in der GUI zu **System** > **HSM-Administration** > **Partitionen**. Der an die Partition angehängte Instanzname wird angezeigt.



Um die Zuweisung einer FIPS-Partition aufzuheben, navigieren Sie zu **NetScaler** > **Instances**. Bearbeiten Sie die Instanz, und deaktivieren Sie das Kontrollkästchen **FIPS aktivieren** .

Geben Sie in der CLI an der Eingabeaufforderung die folgenden Befehle ein:

```
1 show fips
```



```
2
3 FIPS Card is not configured
4  Done
5 <!--NeedCopy-->
```

Wenn Sie die folgende Ausgabe sehen, lesen Sie den Abschnitt zur Fehlerbehebung zum Debuggen.

FEHLER: Betrieb nicht erlaubt - keine FIPS-Karte im System vorhanden

> Hinweis:
>
> Wenn eine Partition von einer der vorhandenen VPX-Instanzen getrennt wird, werden die Daten auf der Partition gelöscht. Infolgedessen geht jede aktuelle Konfiguration (z. B. FIPS-Schlüssel) verloren. Nachdem eine Partition getrennt oder erneut an eine neue oder zuvor gebundene VPX-Instanz angehängt wurde, muss sie gemäß den Anweisungen unter Konfigurieren des HSM initialisiert werden, bevor Sie die Partition für sichere Verbindungen verwenden können.
>
> Während dieser Zeit (nachdem die Partition getrennt oder neu angehängt wurde) kann auf die entsprechende VPX-Instanz über die GUI mit HTTP und über die CLI mit SSH zugegriffen werden.

Konfigurieren von HSM für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Appliance

December 3, 2021

Überprüfen Sie zunächst den Status Ihrer FIPS-Karte, um sicherzustellen, dass der Treiber korrekt geladen wurde, und initialisieren Sie dann die Karte.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 show fips
2
3 FIPS Card is not configured
4
5 Done
6 <!--NeedCopy-->
```

Wenn der Treiber nicht korrekt geladen wurde, erscheint die Meldung “FEHLER: Betrieb nicht zulässig - keine FIPS-Karte im System vorhanden”.

Initialisieren der FIPS-Karte

> **Wichtig:**
>
> Stellen Sie sicher, dass das /nsconfig/fips Verzeichnis erfolgreich auf der Appliance erstellt wurde.

Speichern Sie die Konfiguration nicht, bevor Sie die Appliance zum dritten Mal neu starten.

Führen Sie die folgenden Schritte aus, um die FIPS-Karte zu initialisieren:

1. Setzen Sie die FIPS-Karte zurück (reset fips).
2. Starten Sie das Gerät neu (reboot).
3. Legen Sie das Kennwort für den Sicherheitsbeauftragten für die Partitionen 0 und 1 und das Benutzerkennwort für die Partition (set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS) fest.

   Hinweis: Die Ausführung des Befehls set oder reset dauert mehr als 60 Sekunden.
4. Speichern Sie die Konfiguration (saveconfig).
5. Stellen Sie sicher, dass der kennwortverschlüsselte Schlüssel für die Hauptpartition (master_pek.key) im Verzeichnis /nsconfig/fips/ erstellt wurde.
6. Starten Sie das Gerät neu (reboot).
7. Stellen Sie sicher, dass die FIPS-Karte UP (show fips) ist.

Initialisieren Sie die FIPS-Karte über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
reset fips

reboot

set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -
   hsmLabel <string>
<!--NeedCopy-->
```

> **Hinweis**: Die folgende Meldung wird angezeigt, wenn Sie den Befehl **set fips** ausführen:

```
This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. [Note: On
   MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
   default, and the -initHSM Level-2 option is internally converted to
   Level-3]  Do you want to continue?(Y/N)y

saveconfig
```



```
4
5 reboot
6
7 show fips
8 <!--NeedCopy-->
```

Beispiel:

```
1 reset fips
2
3 Done
4
5 reboot
6
7 set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS
8
9 This command will erase all data on the FIPS card. You must save the
     configuration (saveconfig) after executing this command. [Note: On
     MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
     default, and the -initHSM Level-2 option is internally converted to
     Level-3]  Do you want to continue?(Y/N)y
10
11 Done
12
13 saveconfig
14
15 Done
16
17 reboot
18
19 show fips
20
21     FIPS HSM Info:
22     HSM Label : NSFIPS
23     Initialization : FIPS-140-2 Level-2
24     HSM Serial Number : 3.0G1532-ICM000228
25     HSM State : 2
26     HSM Model : NITROX-III CNN35XX-NFBE
27     Hardware Version : 0.0-G
28     Firmware Version : 1.0
29     Firmware Build : NFBE-FW-1.0-48
30     Max FIPS Key Memory : 1000
31     Free FIPS Key Memory : 1000
32     Total SRAM Memory : 557396
33     Free SRAM Memory : 238088
```



```
    Total Crypto Cores : 4
    Enabled Crypto Cores : 4
Done
<!--NeedCopy-->
```

Erstellen eines FIPS-Schlüssels für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Einheit

August 19, 2021

Sie können einen FIPS-Schlüssel auf Ihrer Instanz erstellen oder einen vorhandenen FIPS-Schlüssel in die Instanz importieren. Eine SDX 14030/14060/14080 FIPS-Einheit unterstützt nur 2048-Bit- und 3072-Bit-Schlüssel und einen Exponentenwert von F4. Für PEM-Schlüssel ist kein Exponent erforderlich. Stellen Sie sicher, dass der FIPS-Schlüssel korrekt erstellt wurde. Erstellen Sie eine Zertifikatsignaturanforderung und ein Serverzertifikat. Fügen Sie schließlich der Instanz das Zertifikatschlüsselpaar hinzu.

> **Hinweis:**
>
> 1024-Bit- und 4096-Bit-Schlüssel und ein Exponentenwert von 3 werden nicht unterstützt.

Erstellen eines FIPS-Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent (3
    | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Beispiel:

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4

Done

show ssl fipskey ddvws

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (
   Hex: 0x10001)

Done
<!--NeedCopy-->
```


Importieren eines FIPS-Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-
   wrapKeyName <string>] [-iv<string>] [-exponent F4 ]
<!--NeedCopy-->
```

Beispiel:

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4
Done
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM
Done
<!--NeedCopy-->
```

Überprüfen Sie, ob der FIPS-Schlüssel korrekt erstellt oder importiert wurde, indem Sie den Befehl **show fipskey** ausführen.

```
show fipskey
1)      FIPS Key Name: Key-FIPS-2
Done
<!--NeedCopy-->
```

Erstellen einer Zertifikatsignaturanforderung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
   <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
    [-organizationUnitName <string>] [-localityName <string>] [-
    commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
<!--NeedCopy-->
```

Beispiel:

```
create certreq f1.req  - fipsKeyName f1 -countryName US -stateName CA -
   organizationName Citrix -companyName Citrix -commonName ctx -
   emailAddress test@example.com`
`Done
<!--NeedCopy-->
```


Erstellen eines Serverzertifikats mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
   input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
    input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
    input_filename>] [-CAkeyForm ( DER | PEM )] [-CAserial <
    output_filename>]
<!--NeedCopy-->
```

Beispiel:

```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
   root.key -CAserial ns-root.srl -days 1000
Done
<!--NeedCopy-->
```

Im vorangegangenen Beispiel wird ein Serverzertifikat mit einer lokalen Stammzertifizierungsstelle auf der Appliance erstellt.

Hinzufügen eines Zertifikatschlüsselpaars mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
   string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
   [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod   <
   positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Beispiel:

```
add certkey cert1 -cert f1.cert -fipsKey f1
Done
<!--NeedCopy-->
```

Nach dem Erstellen des FIPS-Schlüssels und des Serverzertifikats können Sie die generische SSL-Konfiguration hinzufügen. Aktivieren Sie die Funktionen, die für Ihre Bereitstellung erforderlich sind. Fügen Sie Server, Dienste und virtuelle SSL-Server hinzu. Binden Sie das Zertifikatschlüsselpaar und den Dienst an den virtuellen SSL-Server, und speichern Sie die Konfiguration.

```
enable ns feature SSL LB
```



```
Done
add server s1 10.217.2.5
Done
add service sr1 s1 HTTP 80
Done
add lb vserver v1 SSL 10.217.2.172 443
Done
bind ssl vserver v1  -certkeyName cert1
Done
bind lb vserver v1 sr1
Done
saveconfig
Done
<!--NeedCopy-->
```

Weitere Informationen zum Konfigurieren von sicherem HTTPS und sicherem RPC finden Sie hier.

Aktualisieren Sie die FIPS HSM-Firmware auf einer VPX-Instanz

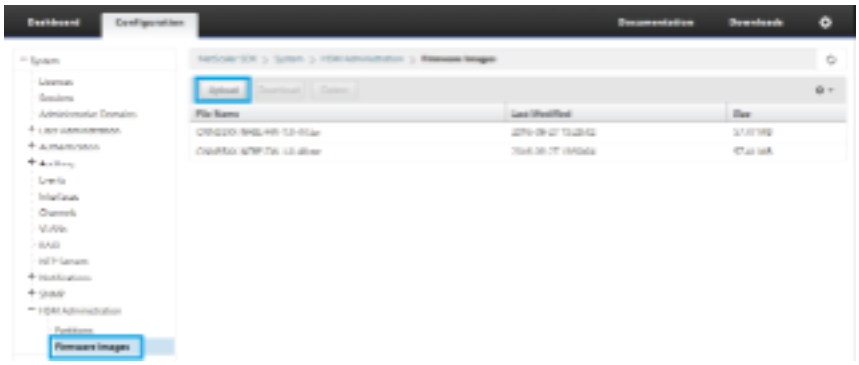
June 2, 2023

> **Hinweis:**
>
> Dieses Upgrade gilt für die FIPS-Karte auf der SDX 14000-Appliance.

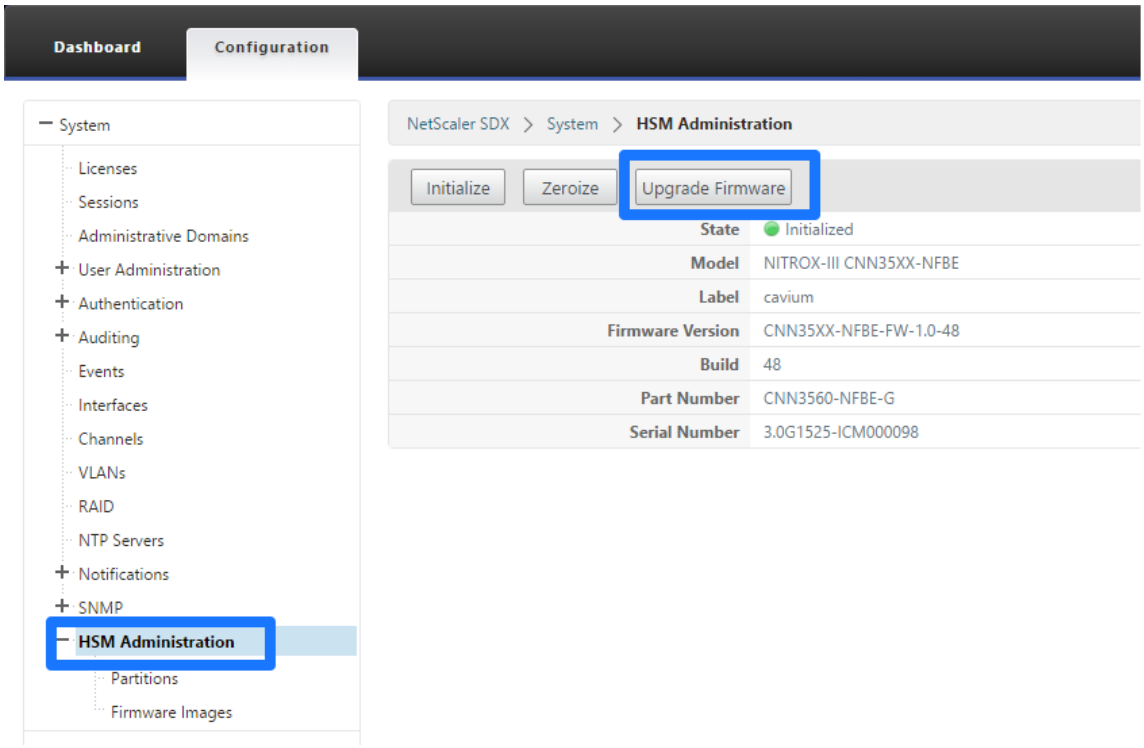
FIPS HSM-Firmware-Updates werden von Zeit zu Zeit veröffentlicht. Laden Sie die neueste Firmware von der NetScaler-Downloadseite herunter und laden Sie sie auf die Appliance hoch. Der Upgrade-Vorgang kann bis zu 10 Minuten dauern. Die Instanz wird nach dem Upgrade neu gestartet.

Aktualisieren Sie die FIPS HSM-Firmware

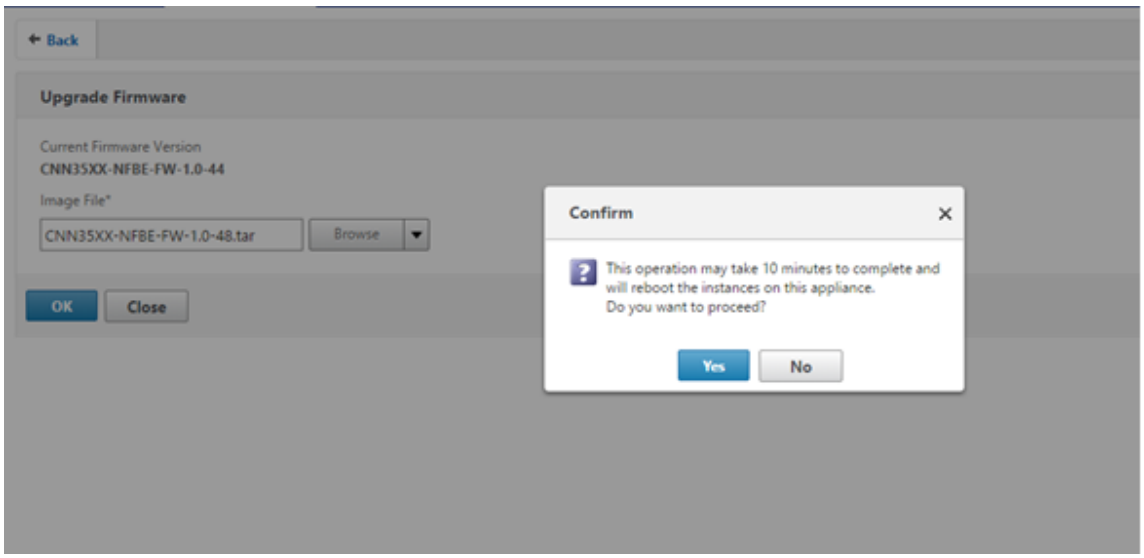
1. Navigieren Sie zu **System > HSM Administration > Firmware-Images**.
2. Wählen Sie **Hochladen**.

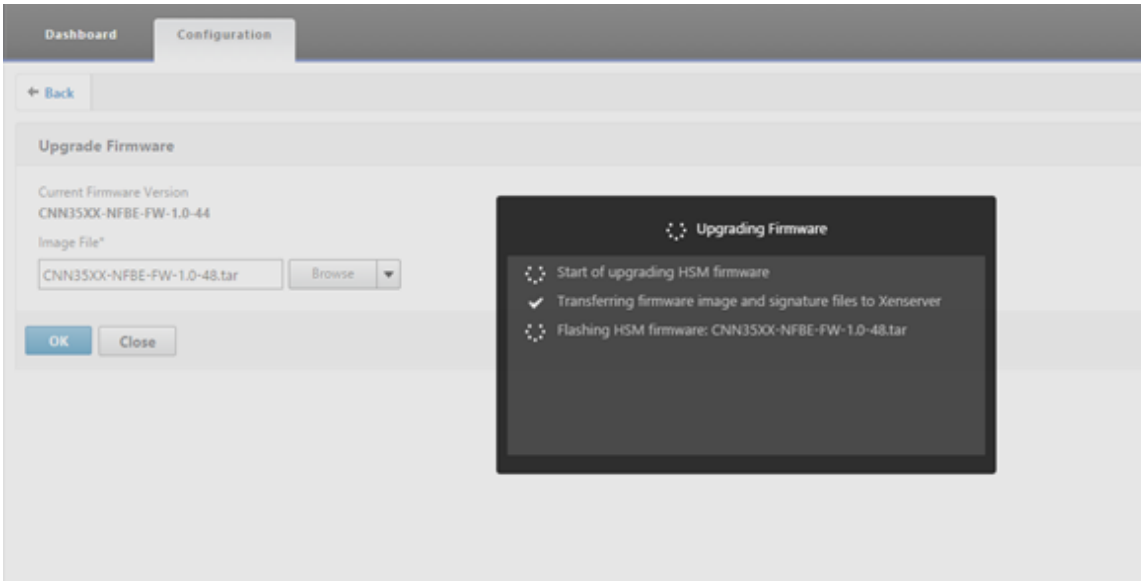


3. Navigieren Sie zu dem Ordner, der das Firmware-Image enthält, und wählen Sie die Datei aus.
4. Navigieren Sie zu **System > HSM Administration**und wählen Sie **Firmware aktualisieren**aus.



5. Wählen Sie das Firmware-Image aus, auf das Sie aktualisieren möchten, und klicken Sie auf **OK**.





Unterstützung für Thales Luna Network Hardwaresicherheitsmodul

May 11, 2023

Eine NetScaler-Appliance ohne FIPS speichert den privaten Schlüssel des Servers auf der Festplatte. Auf einer FIPS-Appliance wird der Schlüssel in einem kryptografischen Modul gespeichert, das als Hardware-Sicherheitsmodul (HSM) bekannt ist. Das Speichern eines Schlüssels im HSM schützt ihn vor physischen und Software-Angriffen. Darüber hinaus sind die Schlüssel mit speziellen FIPS-zugelassenen Verschlüsselungen verschlüsselt.

Nur die NetScaler MPX/SDX 14000 FIPS-Appliances unterstützen eine FIPS-Karte. Unterstützung für FIPS ist nicht auf anderen MPX/SDX-Appliances oder auf NetScaler VPX Appliances verfügbar. Diese Einschränkung wird durch die Unterstützung eines Thales Luna-Netzwerk-HSM auf allen NetScaler MPX-, SDX- und VPX-Appliances mit Ausnahme der MPX/SDX 14000 FIPS-Appliances behoben.

> **Hinweis:**
>
> Support für die Appliances, die unter Support für Intel Coleto und Intel Lewisburg SSL-Chip-basierte Plattformen aufgeführt sind, ist ab Version 13.1 Build 33.x verfügbar.

Ein Thales Luna-Netzwerk HSM wurde entwickelt, um kritische kryptografische Schlüssel zu schützen und sensible kryptografische Operationen in einer Vielzahl von Sicherheitsanwendungen zu beschleunigen.

Unterstützte Versionen Matrix

NetScaler-Version	Version der Software-Appliance	Firmware-Version	Clientversion
11.1, 12.0, 12.1	5.2.3-1	6.2.1	6.0.0
11.1, 12.0, 12.1	6.2.2-5	6.10.9	6.2.2
13.0	7.2.0-220	7.0.3	7.2.2 (7.2.0-220)
13.1	7.2.0-220	7.0.3	10.3.0

Voraussetzungen

May 11, 2023

Bevor Sie ein Thales Luna-Netzwerk HSM mit einem NetScaler verwenden können, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Ein HSM des Thales Luna-Netzwerks ist im Netzwerk installiert, einsatzbereit und für den NetScaler zugänglich. Das heißt, die NSIP-Adresse oder die SNIP-Adresse wird als autorisierter Kunde auf dem HSM hinzugefügt.
- Es stehen Lizenzen zur Unterstützung der erforderlichen Anzahl von Partitionen auf dem HSM zur Verfügung.
- Das Thales Luna-Netzwerk HSM und der NetScaler können Verbindungen untereinander über Port 1792 initiieren.
- Sie verwenden NetScaler Version 11.1 oder höher.
- Die NetScaler Appliance enthält keine FIPS Cavium-Karte.

> **Wichtig**
>
> HSMs des Thales Luna-Netzwerks werden auf den MPX 9700/10500/12500/15500 FIPS-Appliances nicht unterstützt.

Thales Luna-Clients auf ADC konfigurieren

August 15, 2023

Nachdem Sie das Thales Luna HSM konfiguriert und die erforderlichen Partitionen erstellt haben, müssen Sie Clients erstellen und sie Partitionen zuweisen. Konfigurieren Sie zunächst die Thales Luna-Clients auf dem NetScaler und richten Sie die Netzwerkvertrauensverbindungen (NTLs) zwischen den Thales Luna-Clients und dem Thales Luna HSM ein. Eine Beispielkonfiguration ist im Anhangangegeben.

> **Hinweis:**
>
> Wenn Sie auf Softwareversion 14.1 aktualisieren, müssen Sie die Thales Luna-Client-Version 10.3.0 installieren und die folgenden Schritte ausführen.

1. Wechseln Sie das Verzeichnis in /var/safenet und installieren Sie den Thales Luna Client. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cd /var/safenet
<!--NeedCopy-->
```

Um den Thales Luna-Client Version 6.0.0 zu installieren, geben Sie Folgendes ein:

```
install_client.sh -v 600
<!--NeedCopy-->
```

Um den Thales Luna Client Version 6.2.2 zu installieren, geben Sie Folgendes ein:

```
install_client.sh -v 622
<!--NeedCopy-->
```

Um den Thales Luna Client Version 7.2.2 zu installieren, geben Sie Folgendes ein:

```
install_client.sh -v 722
<!--NeedCopy-->
```

Um den Thales Luna Client Version 10.3.0 zu installieren, geben Sie Folgendes ein:

```
install_client.sh -v 1030
<!--NeedCopy-->
```

2. Konfigurieren Sie die NTLs zwischen Thales Luna Client (ADC) und HSM.

Nachdem das Verzeichnis '/var/safenet/' erstellt wurde, führen Sie die folgenden Aufgaben auf dem ADC aus.

a) Ändern Sie das Verzeichnis in '/var/safenet/config/' und führen Sie das 'safenet_config'-Skript aus. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cd /var/safenet/config

sh safenet_config
<!--NeedCopy-->
```

Dieses Skript kopiert die Datei "Chrystoki.conf" in das Verzeichnis /etc/. Es erzeugt auch einen symbolischen Link 'libCryptoki2_64.so' im Verzeichnis '/usr/lib/'.

b) Erstellen und übertragen Sie ein Zertifikat und einen Schlüssel zwischen dem ADC und dem Thales Luna HSM.

Um sicher kommunizieren zu können, müssen der ADC und HSM Zertifikate austauschen. Erstellen Sie ein Zertifikat und einen Schlüssel auf dem ADC und übertragen Sie es dann an das HSM. Kopieren Sie das HSM-Zertifikat in den ADC.

i) Wechseln Sie in das Verzeichnis /var/safenet/safenet/lunaclient/bin.

ii) Erstellen Sie ein Zertifikat auf dem ADC. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
1 ./vtl createCert -n <ip address of NetScaler>
2 <!--NeedCopy-->
```

Dieser Befehl fügt auch das Zertifikat und den Schlüsselpfad zur Datei "/etc/Chrystoki.conf" hinzu.

iii) Kopieren Sie dieses Zertifikat in das HSM. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
1 scp /var/safenet/safenet/lunaclient/cert/client/<ip address of NS
     >.pem <LunaSA_HSM account>@<IP address of Luna SA>
2 <!--NeedCopy-->
```

iv) Kopieren Sie das HSM-Zertifikat in den NetScaler. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
1 scp <HSM account>@<HSM IP>:server.pem  /var/safenet/safenet/
     lunaclient/server_<HSM ip>.pem
2 <!--NeedCopy-->
```

3. Registrieren Sie den NetScaler als Client und weisen Sie ihm eine Partition auf dem Thales Luna HSM zu.

   Melden Sie sich beim HSM an und erstellen Sie einen Client. Geben Sie das NSIP als Client-IP ein. Diese Adresse muss die IP-Adresse des ADC sein, von dem Sie das Zertifikat an das HSM übertragen haben. Nachdem der Client erfolgreich registriert wurde, weisen Sie ihm eine Partition zu. Führen Sie die folgenden Befehle auf dem HSM aus.

   a) Verwenden Sie SSH, um eine Verbindung zum Thales Luna HSM herzustellen und geben Sie das Kennwort ein.

   b) Registrieren Sie den NetScaler im Thales Luna HSM. Der Client wird auf dem HSM angelegt. Die IP-Adresse ist die IP-Adresse des Clients. Das heißt, die NSIP-Adresse.

   Geben Sie an der Eingabeaufforderung Folgendes ein:


```
client register  -client <client name> -ip <NetScaler ip>
<!--NeedCopy-->
```

c) Weisen Sie dem Client eine Partition aus der Partitionsliste zu. Geben Sie Folgendes ein, um die verfügbaren Partitionen anzuzeigen:

```
<luna_sh> partition list
<!--NeedCopy-->
```

Weisen Sie eine Partition aus dieser Liste zu. Typ:

```
<lunash:> client assignPartition -client <Client Name> -par <
   Partition Name>
<!--NeedCopy-->
```

4. Registrieren Sie das HSM mit seinem Zertifikat auf dem NetScaler.

   Ändern Sie auf dem ADC das Verzeichnis in "/var/safenet/safenet/lunaclient/bin" und geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   ```
   ./vtl addserver -n <IP addr of HSM> -c /var/safenet/safenet/
      lunaclient/server_<HSM_IP>.pem
   <!--NeedCopy-->
   ```

   Geben Sie Folgendes ein, um das HSM zu entfernen, das am ADC registriert ist:

   ```
   ./vtl deleteServer -n <HSM IP> -c <cert path>
   <!--NeedCopy-->
   ```

   Geben Sie Folgendes ein, um die auf dem ADC konfigurierten HSM-Server aufzulisten:

   ```
   ./vtl listServer
   <!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > Stellen Sie vor dem Entfernen des HSM mit `vtl` sicher, dass alle Schlüssel für dieses HSM manuell von der Appliance entfernt wurden. HSM-Schlüssel können nicht gelöscht werden, nachdem der HSM-Server entfernt wurde.

5. Überprüfen Sie die Netzwerk-Trustlinks (NTLs) -Konnektivität zwischen ADC und HSM. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   ```
   ./vtl verify
   <!--NeedCopy-->
   ```


Wenn die Überprüfung fehlschlägt, überprüfen Sie alle Schritte. Fehler sind auf eine falsche IP-Adresse in den Client-Zertifikaten zurückzuführen.

6. Speichern Sie die Konfiguration.

   Die vorherigen Schritte aktualisieren die "/etc/Chrystoki.conf" -Konfigurationsdatei. Diese Datei wird gelöscht, wenn der ADC gestartet wird. Kopieren Sie die Konfiguration in die Standardkonfigurationsdatei, die beim Neustart eines ADC verwendet wird.

   Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   ```
   root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
   <!--NeedCopy-->
   ```

   Es wird empfohlen, diesen Befehl jedes Mal auszuführen, wenn die Konfiguration im Zusammenhang mit Thales Luna geändert wird.

7. Starten Sie den Thales Luna Gateway-Prozess.

   Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   ```
   sh /var/safenet/gateway/start_safenet_gw
   <!--NeedCopy-->
   ```

8. Konfigurieren Sie den automatischen Start des Gateway Daemons beim Booten.

   Erstellen Sie die Datei "safenet_is_enrolled", die angibt, dass Thales Luna HSM auf diesem ADC konfiguriert ist. Wenn der ADC neu gestartet wird und diese Datei gefunden wird, wird das Gateway automatisch gestartet.

   Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   ```
   touch /var/safenet/safenet_is_enrolled
   <!--NeedCopy-->
   ```

9. Starten Sie die NetScaler-Appliance neu. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   reboot
   <!--NeedCopy-->
   ```

Thales Luna HSMs in einem Hochverfügbarkeitssetup auf ADC konfigurieren

May 11, 2023

Die Konfiguration von Thales Luna HSMs in einer Hochverfügbarkeit (HA) gewährleistet einen unterbrechungsfreien Service, auch wenn alle, außer eines der Geräte, nicht verfügbar sind. In einem HA-Setup schließt sich jeder HSM im Aktiv-Aktiv-Modus einer HA-Gruppe an. Thales Luna HSMs in einem HA-Setup bieten einen Lastenausgleich aller Gruppenmitglieder, um die Leistung und Reaktionszeit zu erhöhen und gleichzeitig die Gewährleistung eines Hochverfügbarkeitsdienstes zu gewährleisten. Für weitere Informationen wenden Sie sich an den Verkauf und Support von Thales Luna.

Voraussetzungen:

- Mindestens zwei Thales Luna HSM-Geräte. Alle Geräte in einer HA-Gruppe müssen entweder eine PED-Authentifizierung (vertrauenswürdiger Pfad) oder eine Kennwortauthentifizierung aufweisen. Eine Kombination aus Trusted Path Authentication und Passwortauthentifizierung in einer HA-Gruppe wird nicht unterstützt.
- Partitionen auf jedem HSM-Gerät müssen dasselbe Passwort haben, auch wenn die Bezeichnung (Name) unterschiedlich ist.
- Alle Partitionen in HA müssen dem Client zugewiesen werden (NetScaler Appliance).

Nachdem Sie einen Thales Luna-Client auf dem ADC konfiguriert haben, wie unter Konfigurieren eines Thales Luna-Clients auf dem ADCbeschrieben, führen Sie die folgenden Schritte aus, um Thales Luna HSMs in HA zu konfigurieren:

1. Starten Sie an der NetScaler Shell-Eingabeaufforderung `lunacm` (/usr/safenet/lunaclient/bin)

   Beispiel:

   ```
   root@ns# cd /var/safenet/safenet/lunaclient/bin/

   root@ns# ./lunacm
   <!--NeedCopy-->
   ```

2. Identifizieren Sie die Slot-IDs der Partitionen. Um die verfügbaren Steckplätze (Partitionen) aufzulisten, geben Sie Folgendes ein:

   ```
   lunacm:> slot list
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
      Slot Id ->              0
      HSM Label ->            trinity-p1
      HSM Serial Number ->    481681014
      HSM Model ->            LunaSA 6.2.1
      HSM Firmware Version -> 6.10.9
      HSM Configuration ->    Luna SA Slot (PED) Signing With
          Cloning Mode
      HSM Status ->           OK
   ```



```
8
9       Slot Id ->              1
10      HSM Label ->            trinity-p2
11      HSM Serial Number ->    481681018
12      HSM Model ->            LunaSA 6.2.1
13      HSM Firmware Version -> 6.10.9
14      HSM Configuration ->    Luna SA Slot (PED) Signing With
           Cloning Mode
15      HSM Status ->           OK
16
17       Slot Id ->              2
18       HSM Label ->            neo-p1
19       HSM Serial Number ->    487298014
20       HSM Model ->            LunaSA 6.2.1
21       HSM Firmware Version -> 6.10.9
22       HSM Configuration ->    Luna SA Slot (PED) Signing With
            Cloning Mode
23      HSM Status ->           OK
24
25      Slot Id ->              3
26      HSM Label ->            neo-p2
27      HSM Serial Number ->    487298018
28      HSM Model ->            LunaSA 6.2.1
29      HSM Firmware Version -> 6.10.9
30      HSM Configuration ->    Luna SA Slot (PED) Signing With
           Cloning Mode
31      HSM Status ->           OK
32
33      Slot Id ->              7
34      HSM Label ->            hsmha
35      HSM Serial Number ->    1481681014
36      HSM Model ->            LunaVirtual
37      HSM Firmware Version -> 6.10.9
38      HSM Configuration ->    Luna Virtual HSM (PED) Signing With
           Cloning Mode
39      HSM Status ->           N/A - HA Group
40
41      Slot Id ->              8
42      HSM Label ->            newha
43      HSM Serial Number ->    1481681018
44      HSM Model ->            LunaVirtual
45      HSM Firmware Version -> 6.10.9
46      HSM Configuration ->    Luna Virtual HSM (PED) Signing With
           Cloning Mode
47      HSM Status ->           N/A - HA Group
```



```
48
49     Current Slot Id: 0
50 <!--NeedCopy-->
```

3. Erstellen Sie die HA-Gruppe. Die erste Partition wird als primäre Partition bezeichnet. Sie können mehr als eine sekundäre Partition hinzufügen.

```
1 lunacm:> hagroup createGroup -slot <slot number of primary
     partition> -label <group name> -password <partition password >
2
3 lunacm:> hagroup createGroup -slot 1 -label gp12 -password ******
4 <!--NeedCopy-->
```

4. Fügen Sie die sekundären Mitglieder (HSM-Partitionen) hinzu. Wiederholen Sie diesen Schritt für alle Partitionen, die der HA-Gruppe hinzugefügt werden sollen.

```
1 lunacm:> hagroup addMember -slot <slot number of secondary
     partition to be added> -group <group name> -password <partition
      password>
2 <!--NeedCopy-->
```

Code:

```
1 lunacm:> hagroup addMember -slot 2 -group gp12 -password ******
2 <!--NeedCopy-->
```

5. Aktivieren Sie den Modus „Nur HA“.

```
1 lunacm:> hagroup HAOnly  - enable
2 <!--NeedCopy-->
```

6. Aktivieren Sie den aktiven Wiederherstellungsmodus.

```
1 lunacm:.>hagroup recoveryMode  - mode active
2 <!--NeedCopy-->
```

7. Stellen Sie das Intervall für die automatische Wiederherstellung ein (in Sekunden). Die Standardeinstellung ist 60 Sekunden.

```
1 lunacm:.>hagroup interval  - interval <value in seconds>
2 <!--NeedCopy-->
```

Beispiel:

```
1 lunacm:.>hagroup interval  - interval 120
```



```
<!--NeedCopy-->
```

8. Stellen Sie die Anzahl der Wiederholungsversuche für die Wiederherstellung ein. Ein Wert von -1 ermöglicht eine unendliche Anzahl von Wiederholungen.

```
lunacm:> hagroup retry -count <xxx>
<!--NeedCopy-->
```

Beispiel:

```
lunacm:> hagroup retry -count 2
<!--NeedCopy-->
```

9. Kopieren Sie die Konfiguration aus `Chrystoki.conf` dem SafeNet-Konfigurationsverzeichnis.

```
cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

10. Starten Sie die ADC-Appliance neu.

```
reboot
<!--NeedCopy-->
```

Nach der Konfiguration von Thales Luna HSM in HA finden Sie unter Andere ADC-Konfiguration für weitere Konfiguration auf dem ADC.

Andere ADC-Konfiguration

August 19, 2021

1. Generieren Sie einen Schlüssel auf dem HSM.

   Verwenden Sie Tools von Drittanbietern, um Schlüssel auf dem HSM zu erstellen.

2. Fügen Sie einen HSM-Schlüssel auf dem ADC hinzu.

   Wichtig! Das #-Zeichen wird in einem Schlüsselnamen nicht unterstützt. Wenn der Schlüsselname dieses Zeichen enthält, schlägt der Ladeschlüsselvorgang fehl.

   So fügen Sie mit der CLI einen Thales Luna HSM-Schlüssel hinzu:

   Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl hsmkey <KeyName> -hsmType SAFENET -serialNum <serial #> -
   password
<!--NeedCopy-->
```


Wobei:

-keyName ist der Schlüssel, der auf dem HSM mithilfe von Tools von Drittanbietern erstellt wird.

-serialNum ist die Seriennummer der Partition auf dem HSM, auf der die Schlüssel generiert werden.

Hinweis: Verwenden Sie für HSM in einem Hochverfügbarkeitssetup die Seriennummer der Hochverfügbarkeitsgruppe.

-password ist das Kennwort der Partition, auf der die Schlüssel vorhanden sind.

So fügen Sie mit der GUI einen Thales Luna HSM-Schlüssel hinzu:

Navigieren Sie zu **Traffic Management** > **SSL** > **HSM**, und fügen Sie einen HSM-Schlüssel hinzu. Sie müssen den HSM Typ als **SAFENET**angeben.

3. Fügen Sie dem ADC ein Zertifikatschlüsselpaar hinzu. Verwenden Sie zuerst ein Drittanbieter-Tool, um ein mit dem Schlüssel verknüpftes Zertifikat zu generieren. Kopieren Sie dann das Zertifikat in das Verzeichnis /nsconfig/ssl/ auf dem ADC.

   Hinweis: Der Schlüssel muss ein HSM-Schlüssel sein.

   So fügen Sie dem ADC mit der CLI ein Certkey-Paar hinzu:

   Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
   <!--NeedCopy-->
   ```

   So fügen Sie ein Certkey-Paar auf dem ADC mit der GUI hinzu:

   a) Navigieren Sie zu **Traffic Management** > **SSL**.
   b) Wählen Sie unter **Erste Schritte**die Option **Zertifikat (HSM) installieren**aus, und erstellen Sie ein Zertifikatschlüsselpaar mit einem HSM-Schlüssel.

4. Erstellen Sie einen virtuellen Server, und binden Sie das Zertifikatschlüsselpaar an diesen virtuellen Server.

Weitere Informationen zum Erstellen eines virtuellen Servers erhalten Sie, indem Sie auf Konfiguration des virtuellen SSL-Serversklicken.

Um Informationen zum Hinzufügen eines Zertifikatschlüsselpaars zu erhalten, klicken Sie auf Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars.

Informationen zum Binden eines Zertifikatschlüsselpaars an einen virtuellen SSL-Server erhalten Sie, um Informationen zum Binden eines Zertifikatschlüsselpaars an den virtuellen SSL-Serverzu erhalten.

NetScaler-Appliances in einem Hochverfügbarkeitssetup

May 11, 2023

Sie können ein Hochverfügbarkeits-Setup (HA) auf den NetScaler Appliances mit einer Thales Luna HSM-Konfiguration auf eine der folgenden zwei Arten konfigurieren:

- Konfigurieren Sie zunächst ein Thales Luna HSM auf den beiden Knoten mit demselben HSM und derselben Partition. Erstellen Sie dann ein HA-Paar. Fügen Sie schließlich die NetScaler Konfiguration wie Schlüssel, Zertifikatschlüsselpaare und virtuelle Server auf dem primären Knoten hinzu.
- Wenn ein Thales Luna HSM bereits auf einem Knoten mit der NetScaler-Konfiguration konfiguriert ist, fügen Sie eine ähnliche Konfiguration auf dem anderen Knoten hinzu. Kopieren Sie /var/safenet/sfgw_ident_file vom ersten Knoten auf den anderen und starten Sie die safenet_gw-Binärdatei neu. Nachdem das Gateway gestartet ist und ausgeführt wurde, fügen Sie die Knoten in einem HA-Setup hinzu.

Einschränkungen

May 11, 2023

1. Für Änderungen an der HSM-bezogenen Konfiguration in einem vorhandenen Setup, wie das Hinzufügen oder Entfernen eines HSM oder das Erstellen eines HA-Setups, kopieren Sie '/etc/chrystoki.conf' nach '/var/safenet/config'.
2. Nachdem Sie ein HSM hinzugefügt, entfernt oder neu gestartet haben, müssen Sie die Binärdatei '/var/safenet/gateway/safenet_gw' neu starten. Wenn Sie die Gateway-Binärdatei nicht neu starten, stellt das HSM keinen Datenverkehr bereit, nachdem es wieder hinzugefügt wurde oder nachdem es neu gestartet wurde.
3. Um die aktuelle '/var/safenet/gateway/safenet_gw' -Binärdatei neu zu starten oder zu stoppen, verwenden Sie

   ```
   kill -SIGTERM <PID>
   kill -SIGINT <PID>
   <!--NeedCopy-->
   ```

   Es ist wichtig! Verwenden Sie nicht `kill -9 <PID>` oder `kill -6 <PID>`
4. Bevor Sie ein vorhandenes HSM aus dem ADC entfernen, entfernen Sie alle Schlüssel und Zertifikatschlüsselpaare, die diesem HSM zugeordnet sind, aus dem ADC. Sie können diese Dateien nicht aus dem ADC löschen, nachdem Sie das HSM entfernt haben.

5. Auf einer eigenständigen NetScaler-Appliance werden Thales Luna HSMs in HA für Luna Version 6.2 und höher unterstützt.
6. EXPORT-Chiffren werden nicht unterstützt.
7. Die Aktualisierung des Zertifikatschlüsselpaars wird nicht unterstützt.
8. Wenn Sie einen HSM-Schlüssel für ein Drittanbieter-Tool generieren, müssen die Namen des privaten und des öffentlichen Schlüssels identisch sein. Wenn Sie den HSM-Schlüssel auf der Appliance hinzufügen, geben Sie diesen Namen als Schlüsselnamen an.
9. Das ## Zeichen wird in einem Schlüsselnamen und einem Partitionskennwort nicht unterstützt.
10. Cluster- und Adminpartitionen werden nicht unterstützt.

Anhang

May 11, 2023

Beispielbefehle mit ihren Ausgaben:

Führen Sie das Skript aus

```
1       root@ns# pwd
2      /var/safenet/config
3      root@ns# sh safenet_config
4  <!--NeedCopy-->
```

Zertifikat erstellen

```
1      root@ns# cd /var/safenet/safenet/lunaclient/bin
2      root@ns# ./vtl createcert -n 10.102.59.175
3      Private Key created and written to: /var/safenet/safenet/lunaclient
          /cert/client/10.102.59.175Key.pem
4      Certificate created and written to: /var/safenet/safenet/lunaclient
          /cert/client/10.102.59.175.pem
5  <!--NeedCopy-->
```

Kopieren Sie das Zertifikat auf das HSM


```
1     root@ns# scp /var/safenet/safenet/lunaclient/cert/client
         /10.102.59.175.pem admin@10.217.2.7:
2     admin@10.217.2.7's password:
3
4     10.102.59.175.pem          100%  818     0.8KB/s   00:00
5  <!--NeedCopy-->
```

Kopieren des Zertifikats und des Schlüssels aus dem HSM in die NetScaler Appliance

```
1     root@ns# scp admin@10.217.2.7:server.pem /var/Thales Luna/safenet/
         lunaclient/server.2.7.pem
2     admin@10.217.2.7's password:
3
4     server.pem            100% 1164     1.1KB/s   00:01
5  <!--NeedCopy-->
```

Verwenden Sie SSH, um eine Verbindung zum Thales Luna HSM herzustellen

```
1     ssh admin@10.217.2.7
2     Connecting to 10.217.2.7:22...
3     Connection established.
4     To escape to local shell, press 'Ctrl+Alt+]'.
5
6     Last login: Thu Jun 23 02:20:29 2016 from 10.252.243.11
7
8     Luna SA 5.2.3-1 Command Line Shell - Copyright (c) 2001-2014
         SafeNet, Inc. All rights reserved.
9
10    [Safenet1] lunash:>hsm login
11
12
13      Please enter the HSM Administrators' password:
14      > *******
15
16    'hsm login' successful.
17
18
19    Command Result : 0 (Success)
20    [Safenet1] lunash:>
21 <!--NeedCopy-->
```


Registrieren Sie den NetScaler im Thales Luna HSM

```
    [Safenet1] lunash:>client register -client ns175 -ip 10.102.59.175

    'client register' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Weisen Sie dem Client eine Partition aus der Partitionsliste zu

```
    [Safenet1] lunash:>client assignPartition -client ns175 -partition
       p2

    'client assignPartition' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Registrieren Sie das HSM mit seinem Zertifikat auf dem NetScaler

```
    root@ns# ./vtl addserver -n 10.217.2.7 -c /var/safenet/safenet/
       lunaclient/server.2.7.pem

    New server 10.217.2.7 successfully added to server list.
<!--NeedCopy-->
```

Überprüfen Sie die Network Trust Links (NTLs) -Konnektivität zwischen ADC und HSM

```
    root@ns# ./vtl verify

    The following Luna SA Slots/Partitions were found:

    Slot        Serial #                  Label
    ====      ================          =====
       0              477877010          p2
<!--NeedCopy-->
```


Speichern Sie die Konfiguration

```
    root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

Konfigurieren Sie den automatischen Start des Gateway-Daemons beim Booten

```
    touch /var/safenet/safenet_is_enrolled
<!--NeedCopy-->
```

Häufig gestellte Fragen

May 11, 2023

- **Wie überprüfe ich, ob der Thales Luna-Prozess läuft?**

  Geben Sie an der NetScaler -Shell Eingabeaufforderung Folgendes ein:

  ```
  ps - aux | grep safenet_gw
  <!--NeedCopy-->
  ```

- **Wie kann ich die Netzwerkvertrauens-Links (Network Trust Links, NTLs) -Konnektivität zwischen ADC und HSM überprüfen?**

  Ändern Sie nach der Konfiguration von Thales Luna das Verzeichnis in “/var/safenet/safenet/lunaclient/bin” und geben Sie ein:

  ```
  ./vtl verify
  <!--NeedCopy-->
  ```

Unterstützung für Azure Key Vault

August 15, 2023

Die NetScaler Appliance lässt sich in externe HSMs (SafeNet und Thales) für on-premises Bereitstellungen integrieren. Bei Cloud-Bereitstellungen lässt sich die ADC-Appliance in Azure Key Vault integrieren. Die Appliance speichert ihre privaten Schlüssel im Schlüsseltresor, um die Verwaltung und Sicherheit des privaten Schlüssels in der Public Cloud-Domäne zu vereinfachen. Sie müssen keine

Schlüssel mehr an verschiedenen Orten für ADC-Appliances speichern und verwalten, die in mehreren Rechenzentren und Cloud-Anbietern bereitgestellt werden.

Die Verwendung von ADC mit der Preisstufe Azure Key Vault Premium, die HSM-gestützte Schlüssel bereitstellte, bietet FIPS 140-2 Level 2-Konformität.

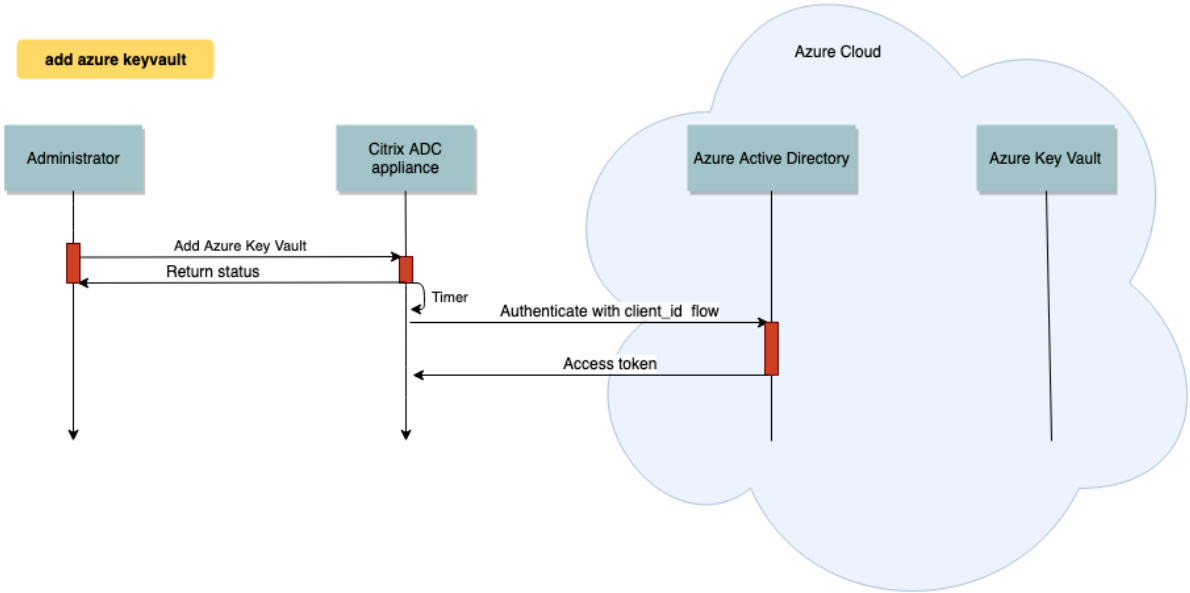
Azure Key Vault ist ein Standardangebot von Microsoft. Weitere Informationen zu Azure Key Vault finden Sie in der Microsoft Azure-Dokumentation.

> **Hinweis:**
>
> Die NetScaler-Integration mit Azure Key Vault wird mit dem TLS 1.3-Protokoll unterstützt.

Architektur im Überblick

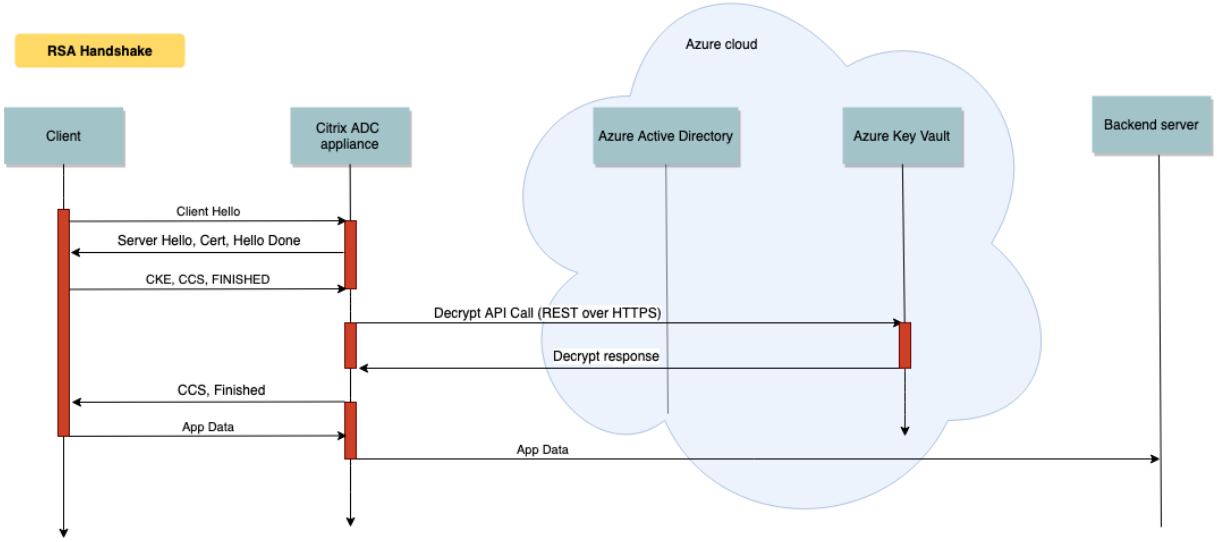
Azure Key Vault ist ein Dienst zum sicheren Speichern von Geheimnissen in der Azure Cloud. Indem Sie Ihre Schlüssel im Azure Key Vault aufbewahren, verringern Sie die Wahrscheinlichkeit, dass Schlüssel gestohlen werden. Sobald der Schlüsseltresor eingerichtet ist, können Sie Ihre Schlüssel darin aufbewahren. Konfigurieren Sie virtuelle Server auf der ADC-Appliance für private Schlüsselvorgänge im Schlüsseltresor. Die ADC-Appliance greift für jeden SSL-Handshake auf den Schlüssel zu.

Das folgende Diagramm veranschaulicht den Vorgang zum Abrufen eines Zugriffstokens aus Azure Active Directory nach der Authentifizierung. Dieses Token wird mit REST-API-Aufrufen für Kryptooperationen mit privaten Schlüsseln verwendet.



Das folgende Diagramm zeigt einen typischen RSA-Handshake. Die Clientschlüsselungsnachricht (CKE), die mit dem öffentlichen Schlüssel verschlüsselt wird, wird mit dem im Schlüsselspeicher

gespeicherten privaten Schlüssel entschlüsselt.



In einem ECDHE-Handshake wird die von der NetScaler Appliance gesendete Serverschlüsselaustauschnachricht (SKE) mithilfe des im Schlüsseltresor gespeicherten privaten Schlüssels signiert.

Voraussetzungen

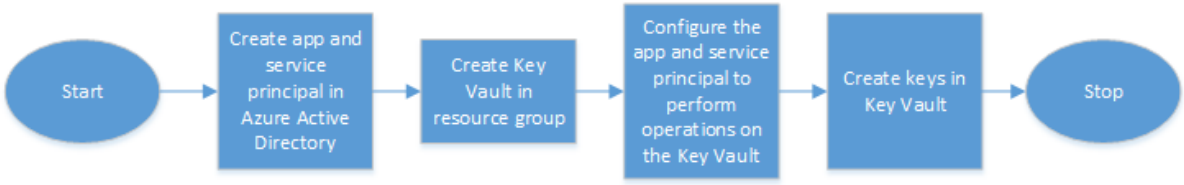
1. Sie müssen ein Azure-Abonnement haben.
2. (Optional) Installieren Sie Azure CLI auf einem Linux-Computer. Anweisungen finden Sie in der Azure-Dokumentation https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-apt?view=azure-cli-latest.
3. Schließen Sie die Konfiguration auf dem Azure-Portal ab, bevor Sie Entitäten auf der ADC Appliance

Konfigurieren der ADC Azure Key Vault-Integration

Führen Sie zuerst die Konfiguration im Azure-Portal durch, gefolgt von der Konfiguration auf der ADC-Appliance.

Führen Sie die folgenden Schritte im Azure-Portal aus

Das folgende Flussdiagramm zeigt den übergeordneten Fluss für die Konfiguration, die für das Azure-Portal erforderlich ist.

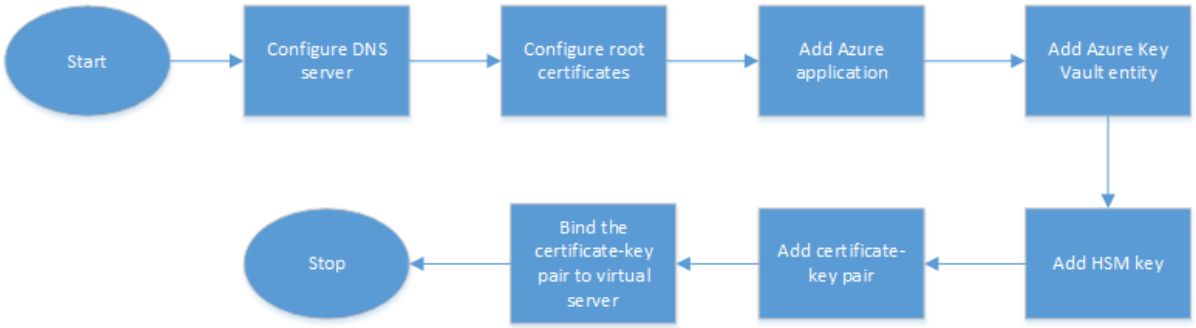


1. Erstellen Sie App und Service Principal in Azure Active Directory.
2. Erstellen Sie einen Schlüsseltresor in einer Ressourcengruppe.
3. Konfigurieren Sie die App und den Service Principal für Signierungs- und Entschlüsselungsvorgänge im Schlüsseltresor.
4. Erstellen Sie Schlüssel im Schlüsseltresor auf eine der folgenden Arten:
    a) Indem Sie eine Schlüsseldatei importieren.
    b) Durch Generieren eines Zertifikats.

Informationen zu den Befehlen zum Konfigurieren der vorangegangenen Schritte finden Sie in der Azure-Dokumentation unter https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals.

Führen Sie die folgenden Schritte auf der ADC-Appliance aus

Das folgende Flussdiagramm zeigt den High-Level-Fluss für die Konfiguration, die auf der ADC-Appliance erforderlich ist.



1. Konfigurieren Sie einen DNS-Server.
2. Konfigurieren Sie Stammzertifikate zur Überprüfung der von Azure präsentierten Zertifikate.
3. Erstellen Sie eine Azure-Anwendung.
4. Erstellen Sie eine Azure Key Vault-Entität.
5. Erstellen Sie einen HSM-Schlüssel.
6. Erstellen Sie ein Zertifikatsschlüsselpaar.
7. Binden Sie das Zertifikatsschlüsselpaar an einen virtuellen Server.

Konfigurieren Sie einen DNS-Server

Für die Namensauflösung des Key Vault-Hosts und des Azure Active Directory-Endpunkts ist ein DNS-Server erforderlich.

So konfigurieren Sie einen DNS-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

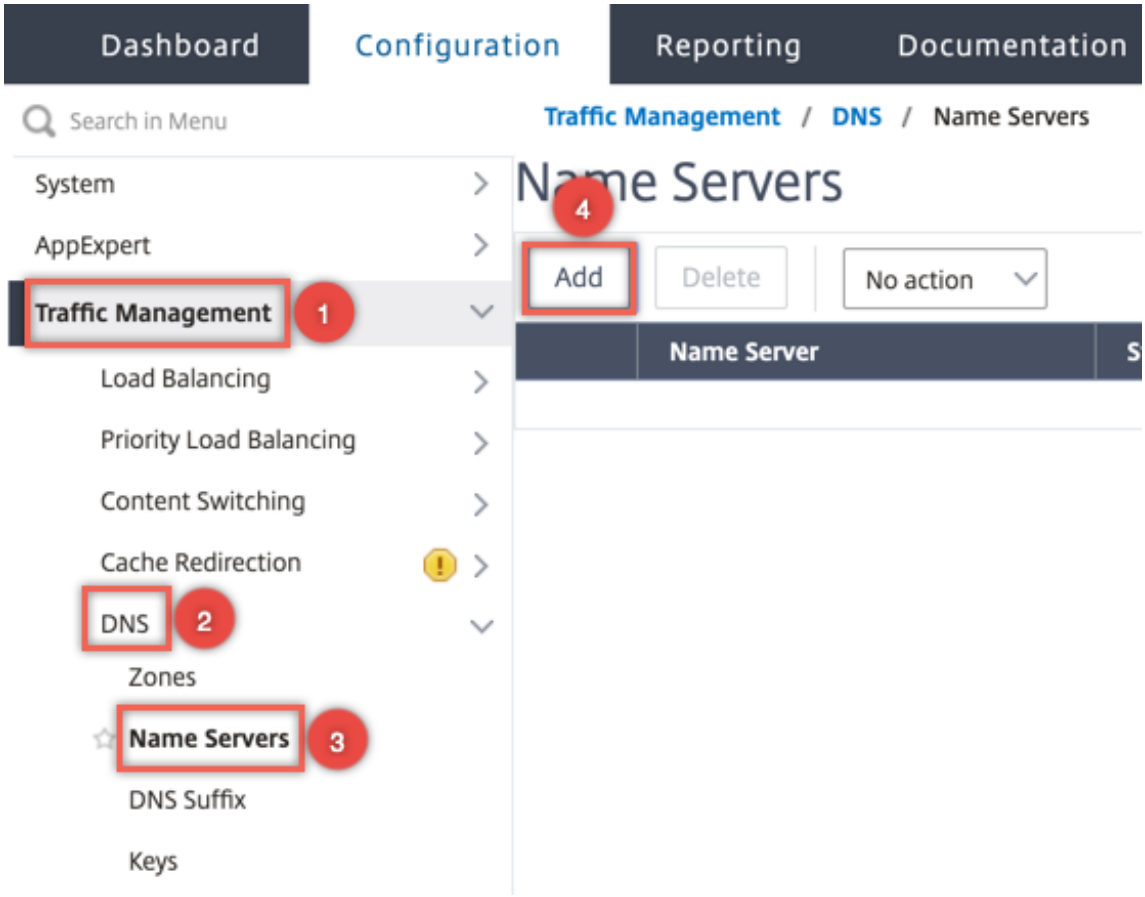
```
add dns nameserver <IP address>
<!--NeedCopy-->
```

Beispiel:

```
add dns nameserver 192.0.2.150
<!--NeedCopy-->
```

So konfigurieren Sie einen DNS-Server mit der GUI

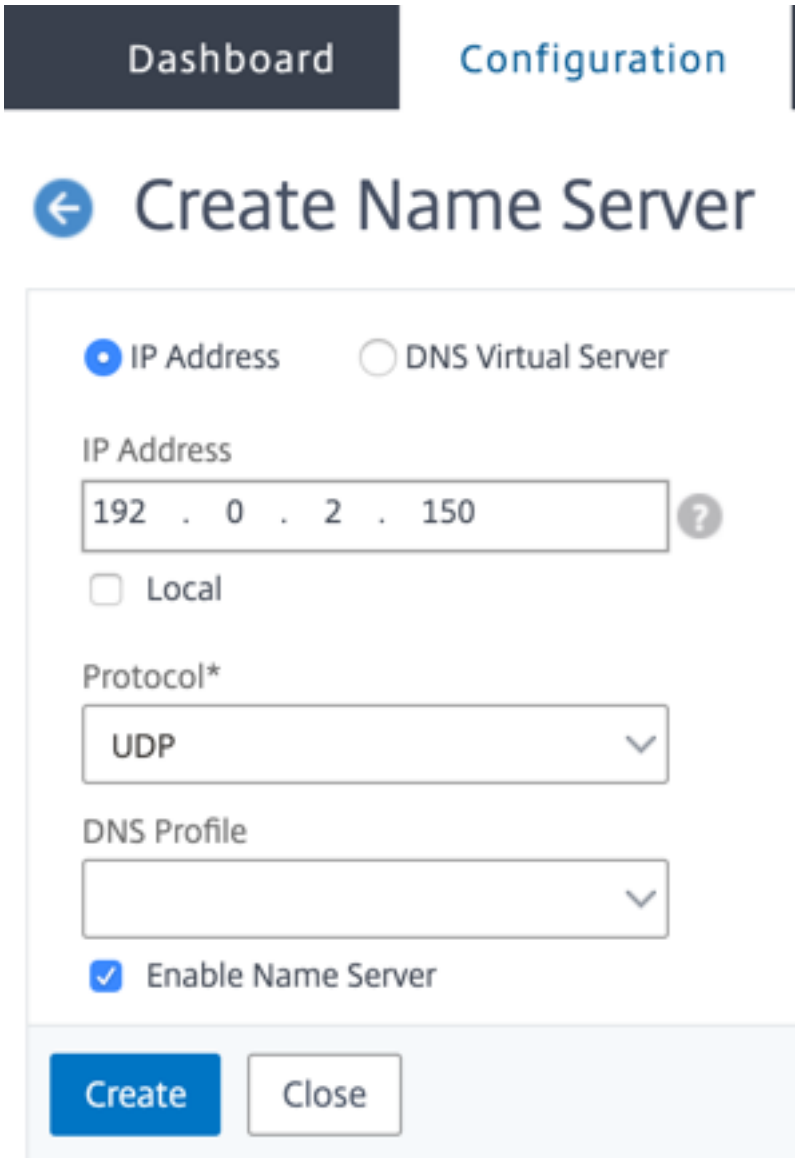
1. Navigieren Sie zu **Traffic Management > DNS > Nameserver**. Klicken Sie auf **Hinzufügen**.



2. Geben Sie Werte für die folgenden Parameter ein:

   - IP-Adresse — Die IP-Adresse eines externen Nameservers oder, falls der lokale Parameter festgelegt ist, die IP-Adresse eines lokalen DNS-Servers (LDNS).

- Protokoll — vom Nameserver verwendetes Protokoll. UDP_TCP ist nicht gültig, wenn der Nameserver ein virtueller DNS-Server ist, der auf der Appliance konfiguriert ist.



3. Klicken Sie auf **Erstellen**.

Hinzufügen und Binden eines Stammzertifikats

Laden Sie die Stammzertifikate des von Azure Key Vault `https://<vault_name>.vault.azure.net` und Azure Active Directory (AAD) vorgestellten Zertifikats herunter https://login.microsoftonline.com und laden Sie es auf die ADC Appliance. Diese Zertifikate sind erforderlich, um das von Azure Key Vault und AAD vorgelegte Zertifikat zu validieren. Binden Sie ein oder mehrere Zertifikate an die CA-Zertifikatsgruppe `ns_callout_certs`.

So fügen Sie mithilfe der CLI ein Stammzertifikat hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

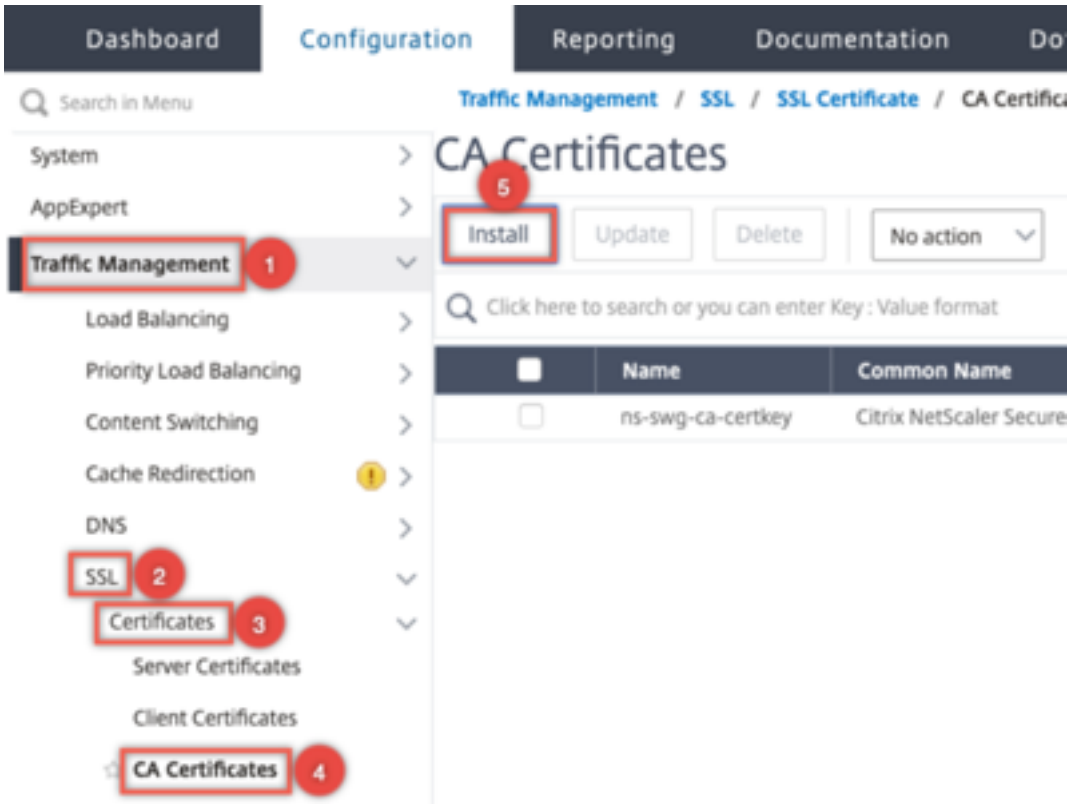
```
add ssl certkey <certkeyname> -cert <certname>
bind ssl caCertGroup <caCertGroupName> <certkeyName>
<!--NeedCopy-->
```

Beispiel:
Im folgenden Beispiel ist das von Azure Key Vault und AAD präsentierte Stammzertifikat dasselbe.

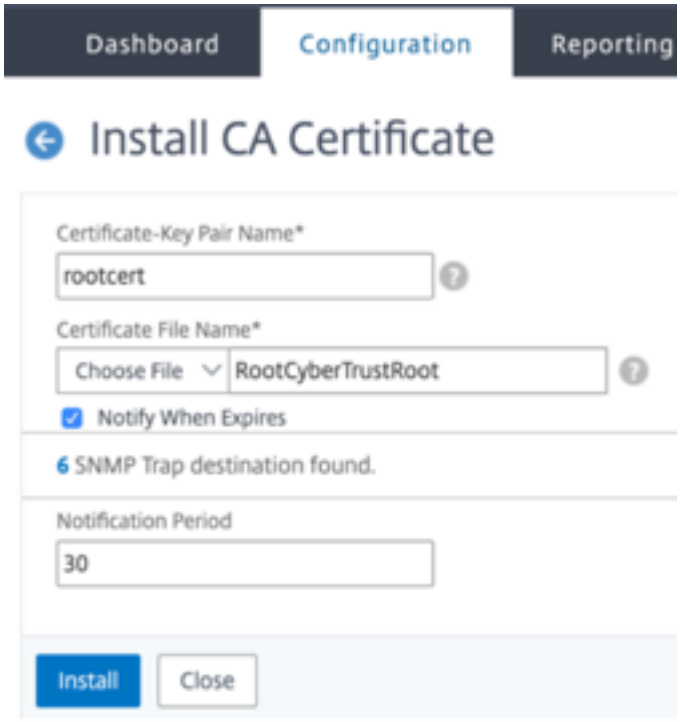
```
add ssl certKey rootcert -cert RootCyberTrustRoot.crt
bind ssl cacertGroup ns_callout_certs  rootcert
<!--NeedCopy-->
```

So fügen Sie mithilfe der GUI ein Stammzertifikat hinzu

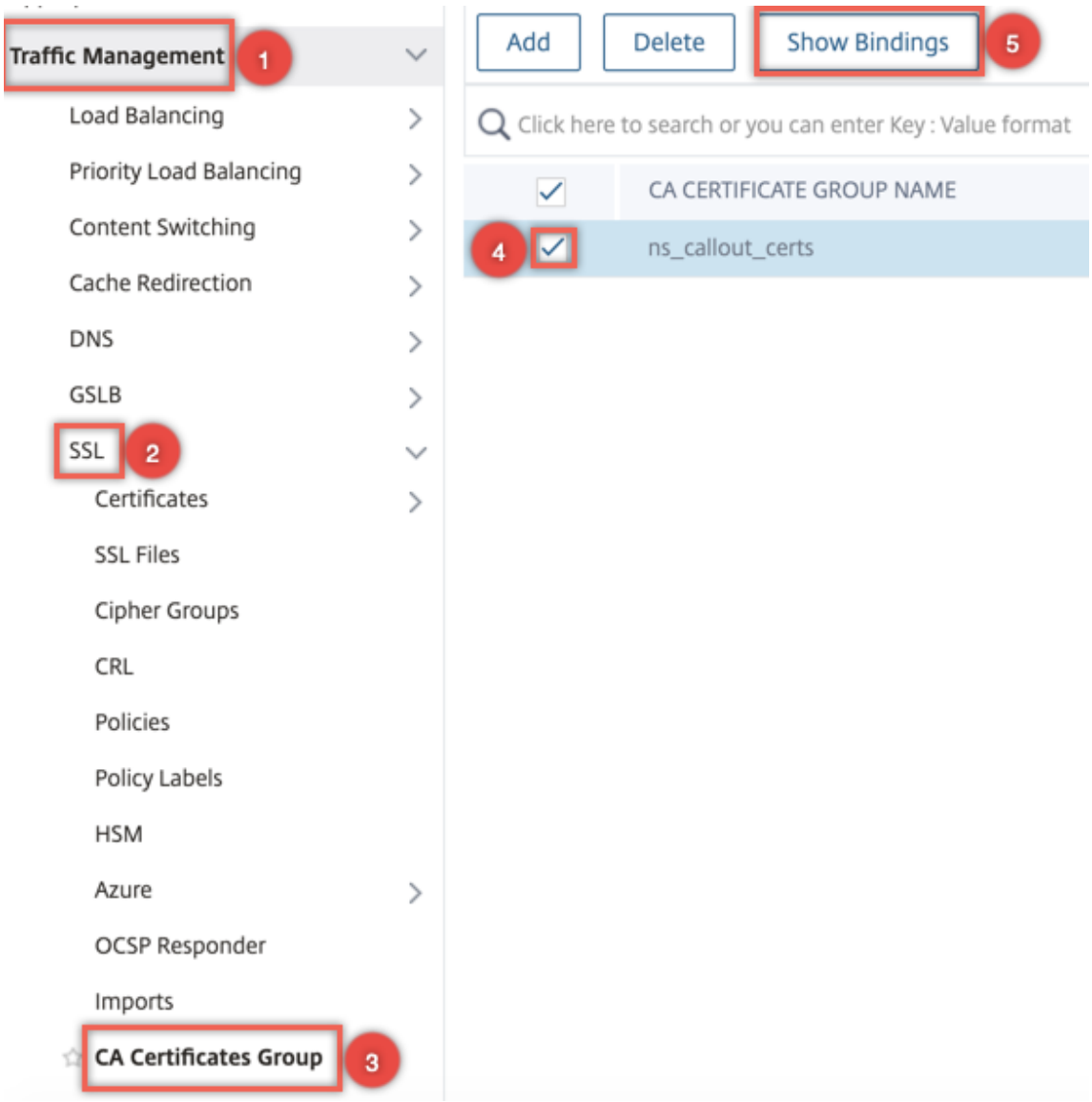
1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate > CA-Zertifikate**.



2. Geben Sie Werte für die folgenden Parameter ein:
   - Name des Zertifikatsschlüssel-Paars
   - Name der Zertifikatsdatei



3. Klicken Sie auf **Installieren**.
4. Navigieren Sie zu **Verkehrsmanagement > SSL > CA Certificates Group**.
5. Wählen Sie **ns_callout_certs** aus und klicken Sie auf **Bindungen anzeigen**.



6. Klicken Sie auf **Bind**.
7. Wählen Sie das zuvor erstellte CA Zertifikat aus und klicken Sie auf **Auswählen**
8. Klicken Sie auf **Binden**, und klicken Sie dann auf **Schließen**.

Konfigurieren einer Azure-Anwendung

Die Azure-Anwendungsentität enthält die erforderlichen Anmeldeinformationen, um sich bei Azure Active Directory zu authentifizieren und das Zugriffstoken abzurufen. Das heißt, um Autorisierungszugriff auf Key Vault-Ressourcen und APIs zu erhalten, fügen Sie die Azure Application ID, das geheime (Kennwort) und die Mandanten-ID auf der ADC-Appliance hinzu.
Wenn Sie die Azure Application Entity mithilfe der CLI konfigurieren, müssen Sie das Kennwort eingeben. Wenn Sie die GUI verwenden, enthält die Azure-Anwendungseinheit die erforderlichen

Anmeldeinformationen, um sich bei Azure Active Directory zu authentifizieren und das Zugriffstoken abzurufen.

So konfigurieren Sie eine Azure-Anwendung mithilfe der CLI

Verwenden Sie den Parameter VaultResource im `add azure application` Befehl, um die Domäne der Ressourcengruppe abzurufen, bevor der Anwendung das Zugriffstoken gewährt wird. Dieser Parameter wird hinzugefügt, da der Domainname für verschiedene Regionen unterschiedlich sein kann. Zum Beispiel könnte die Domäne `vault.azure.net` oder sein `vault.usgov.net`.

Geben Sie an der Eingabeaufforderung Folgendes ein:

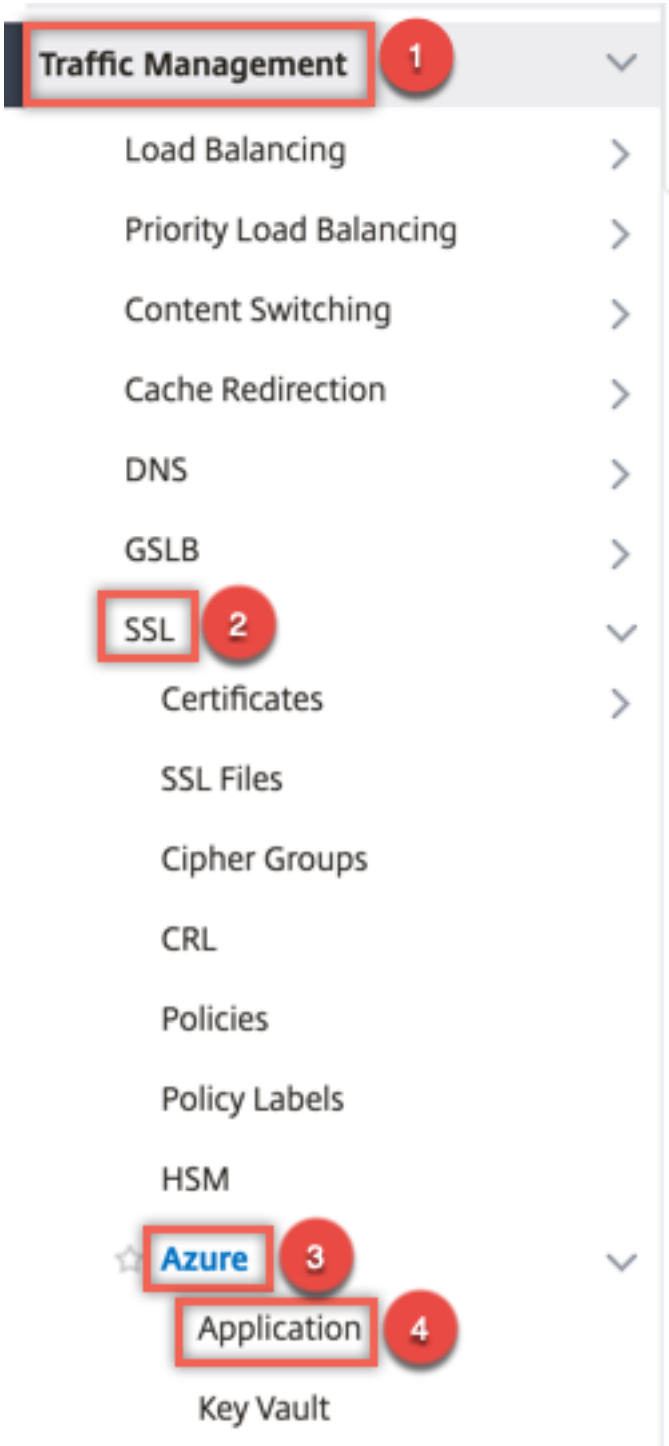
```
add azure application <name> -clientID <string> -clientSecret -tenantID
    <string> -vaultResource <string> [-tokenEndpoint <URL>]
show azure application
<!--NeedCopy-->
```

Beispiel:

```
add azure application app10 -clientiD 12345t23aaa5 -clientsecret
   csHzOoEzmuY= -vaultResource example.vault.azure.net -tenantID 33583
   ee9ca5b
 Done
> sh azure application app10
1)  Name:  app10            ClientID:  12345t23aaa5
    TokenEndpoint:  "https://login.microsoftonline.com/33583ee9ca5b/"
    TenantID:  33583ee9ca5b  VaultResource:  example.vault.azure.net
 Done

<!--NeedCopy-->
```

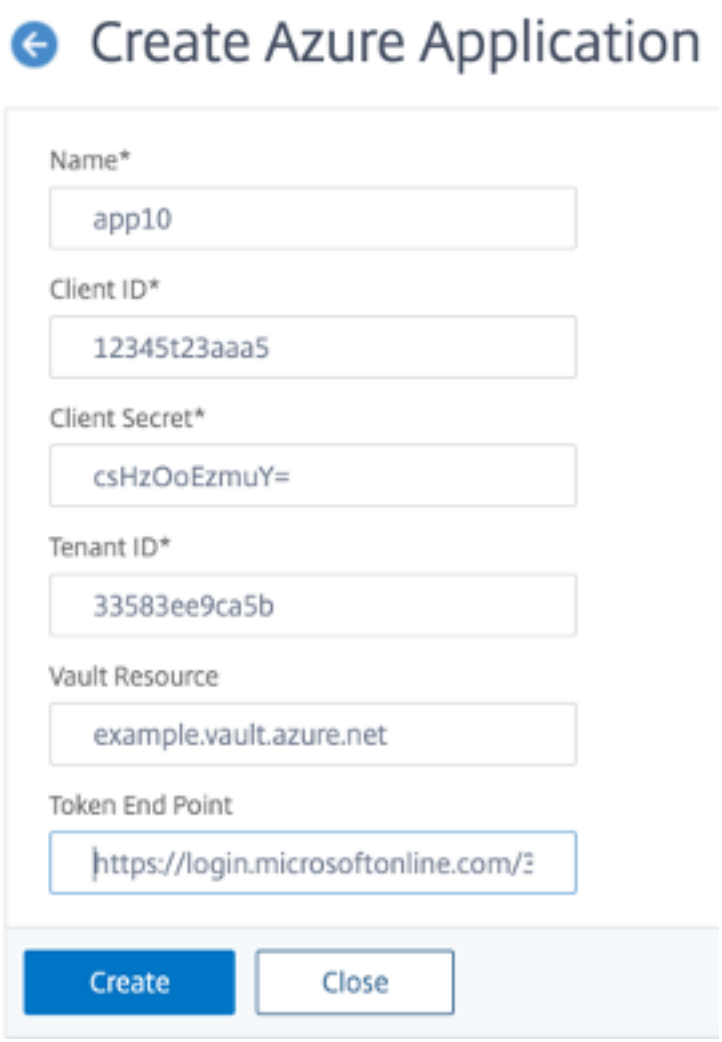
So konfigurieren Sie eine Azure-Anwendung mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Azure > Anwendung**.



2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie Werte für die folgenden Parameter ein:
   - Name — Name für das Anwendungsobjekt auf der NetScaler Appliance.
   - Client-ID — Anwendungs-ID, die generiert wird, wenn eine Anwendung in Azure Active Directory mithilfe der Azure CLI oder des Azure-Portals (GUI) erstellt wird.

- Clientgeheimnis — Kennwort für die in Azure Active Directory konfigurierte Anwendung. Das Kennwort wird in der Azure CLI angegeben oder im Azure-Portal (GUI) generiert.
- Mandanten-ID — ID des Verzeichnisses in Azure Active Directory, in dem die Anwendung erstellt wurde.
- Tresorressource — Tresorresorressource, für die Zugriffstoken gewährt wird Beispiel `vault.azure.net`.
- Token-Endpunkt — URL, von der aus das Zugriffstoken abgerufen werden kann. Wenn der Token-Endpunkt nicht angegeben ist, ist der Standardwert `https://login.microsoftonline.com/<tenant id>`.



Konfigurieren von Azure Key Vault

Erstellen Sie ein Azure Key Vault-Objekt auf der ADC-Appliance.

So konfigurieren Sie Azure Key Vault mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add azure keyVault <name> -azureVaultName <string> -azureApplication
       <string>
show azure keyvault
<!--NeedCopy-->
```

Beispiel:

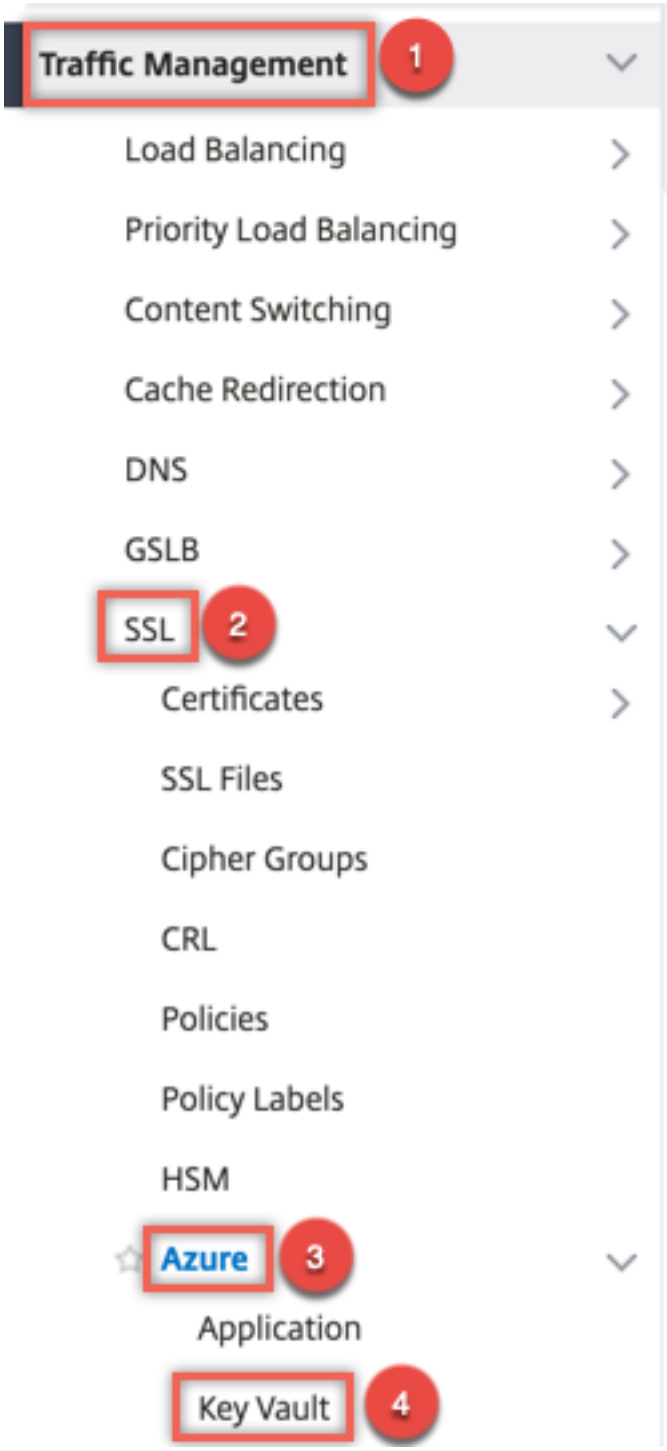
```
add azure keyvault kv1 -azureapplication app10 -azurevaultName pctest.
   vault.azure.net
> sh azure keyVault
1)  Name:  kv1              AzureVaultName:  pctest.vault.azure.net
  AzureApplication:  app10  State:  "Access token obtained"
 Done
<!--NeedCopy-->
```

In der folgenden Tabelle sind die verschiedenen Werte aufgeführt, die der Status des Azure Key Vault annehmen kann, zusammen mit einer kurzen Beschreibung der einzelnen Status.

Status	Beschreibung
`Created`	Anfangszustand des Key Vault-Objekts. Die Authentifizierung wurde nicht versucht.
`Could not reach token end point`	Weist auf einen der folgenden Punkte hin: DNS-Server nicht konfiguriert, Ausstellerzertifikat, das nicht an eine CA-Zertifikatsgruppe gebunden ist, oder Netzwerkprobleme.
`Authorization failed`	Falsche Anmeldeinformationen für die Anwendung.
`Token parse error`	Die Antwort von Azure Active Directory hat nicht das erwartete Format.
`Access token obtained`	Erfolgreich von Azure Active Directory authentifiziert.

So konfigurieren Sie den Azure Key Vault mithilfe der GUI

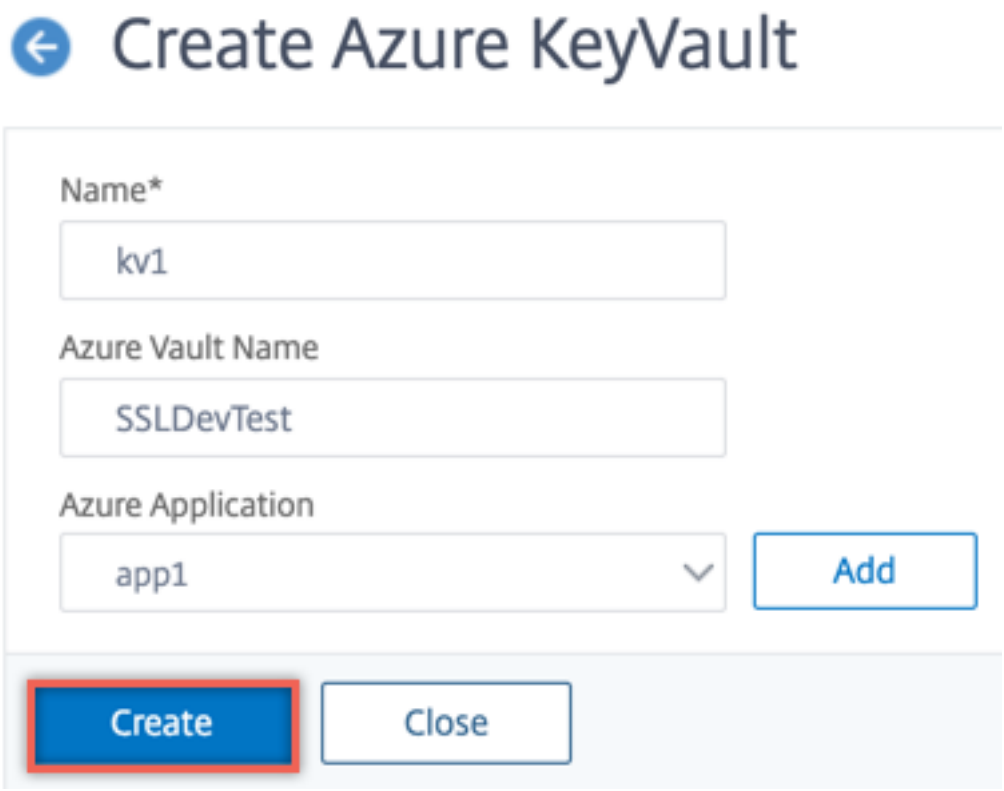
1. Navigieren Sie zu **Traffic Management > SSL > Azure > Schlüsseltresor**.



2. Geben Sie Werte für die folgenden Parameter ein:

   - Name — Name für den Schlüsseltresor.
   - Azure Key Vault Name — Name des Schlüsseltresors, der in Azure Cloud mithilfe der Azure CLI oder des Azure-Portals (GUI) mit Domänennamen konfiguriert wurde.
   - Azure Application Name — Name des Azure Application-Objekts, das auf der ADC Appli-

ance erstellt wurde. Das Azure Application-Objekt mit diesem Namen wird für die Authentifizierung mit Azure Active Directory verwendet.



HSM-Schlüssel hinzufügen

Das Speichern Ihres privaten Schlüssels im HSM gewährleistet die Konformität mit FIPS 140-2 Level 2.

So fügen Sie einen HSM-Schlüssel mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl hsmKey <hsmKeyName> [-hsmType <hsmType>] [-key <string> |
       -serialNum <string>] {
 -password  }
  [-keystore <string>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl hsmKey h1 -keystore kv1 -key san15key -hsmType KEYVAULT


> sh ssl hsmKey h1
```



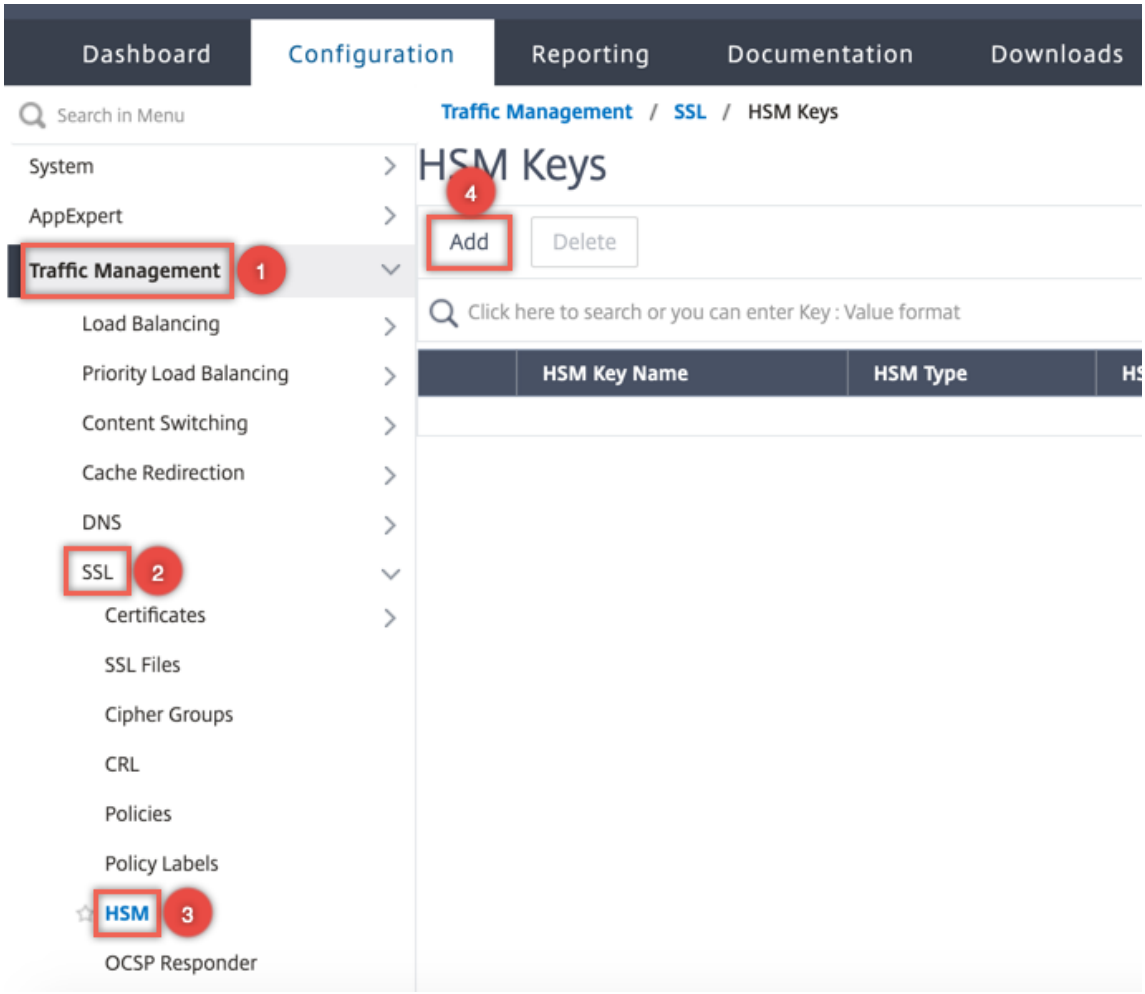
```
5      HSM Key Name: h1        Type: KEYVAULT
6      Key: san15key
7      Key store: kv1
8      State:  “Created”
9   Done
10 <!--NeedCopy-->
```

In der folgenden Tabelle sind die verschiedenen Werte aufgeführt, die der Status eines HSM-Schlüssels annehmen kann, zusammen mit einer kurzen Beschreibung der einzelnen Status.

Status	Beschreibung
Created	Der HSM-Schlüssel wird auf der ADC-Appliance hinzugefügt. Eine Schlüsseloperation wird noch nicht versucht.
Zugriffstoken nicht verfügbar	Zugriffstoken ist nicht verfügbar, als eine Schlüsseloperation versucht wurde.
Nicht autorisiert	Die konfigurierte Azure-Anwendung ist nicht berechtigt, den Schlüsselvorgang auszuführen.
Existiert nicht	Der Schlüssel ist im Azure Key Vault nicht vorhanden.
Unerreichbar	Der Key Vault-Host ist im Netzwerk nicht erreichbar.
Markiert	Die HSM-Taste ist auf der ADC-Appliance aufgrund von Schwellenwertfehlern während des Schlüsselbetriebs mit DOWN gekennzeichnet.
Wichtige Vorgänge waren erfolgreich	Antwort auf Erfolg vom Schlüsseltresor für den Schlüsselbetrieb erhalten.
Wichtige Operationen sind fehlgeschlagen	Fehlerantwort von Key Vault für den Schlüsselbetrieb erhalten.
Tastenbetrieb gedrosselt	Die Anforderung der Schlüsseloperation wird durch den Schlüsseltresor gedrosselt.

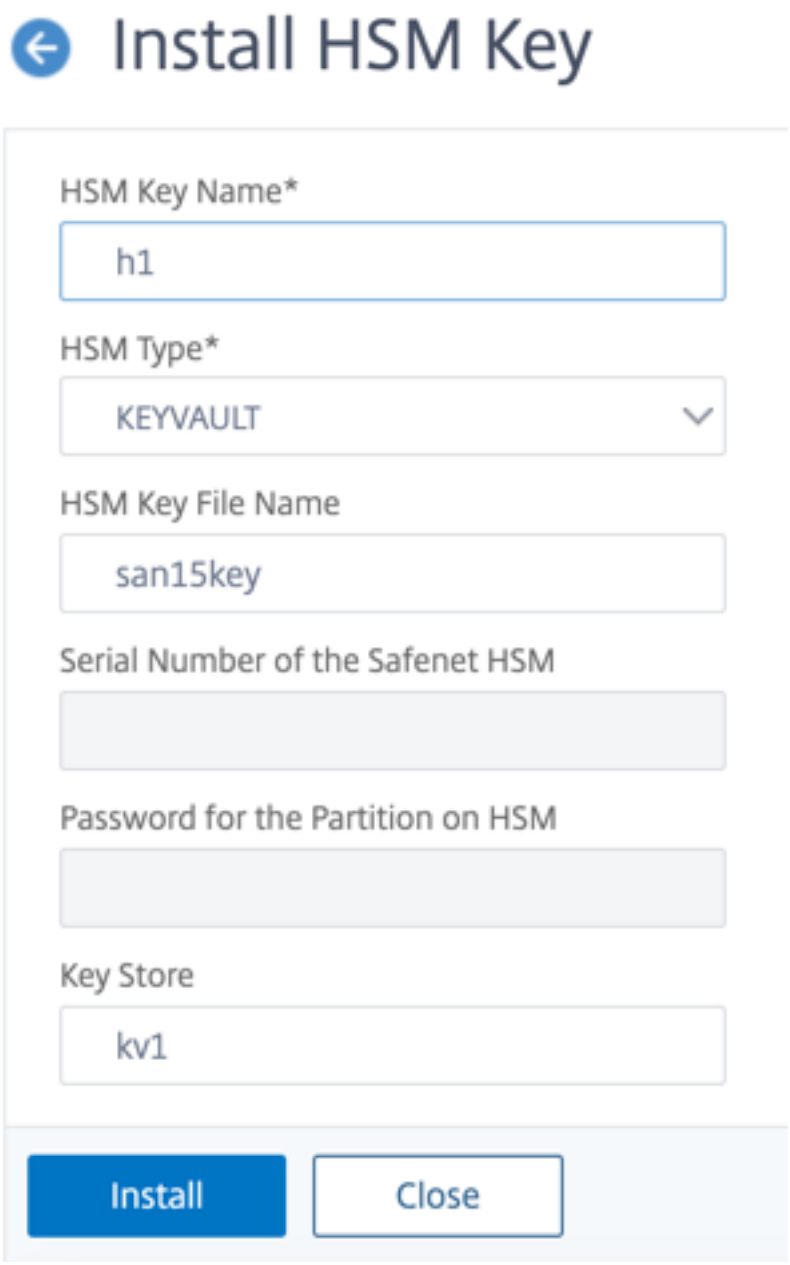
So fügen Sie einen HSM-Schlüssel mithilfe der GUI hinzu

1. Navigieren Sie zu **Traffic Management > SSL > HSM**.



2. Geben Sie Werte für die folgenden Parameter ein.

   - HSM-Schlüsselname — Name des Schlüssels.
   - HSM-Typ — Typ des HSM.
   - Schlüsselspeicher — Name des Schlüsselspeicherobjekts, das HSM darstellt, in dem der Schlüssel gespeichert ist. Beispiel: Name des Key Vault-Objekts oder Azure Key Vault-Authentifizierungsobjekts. Gilt nur für den KEYVAULT Typ HSM.



3. Klicken Sie auf **Hinzufügen**.

Fügen Sie ein Zertifikatschlüsselpaar hinzu

Fügen Sie ein Zertifikatsschlüsselpaar mit dem zuvor erstellten HSM-Schlüssel hinzu.

So fügen Sie ein Zertifikatsschlüsselpaar mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

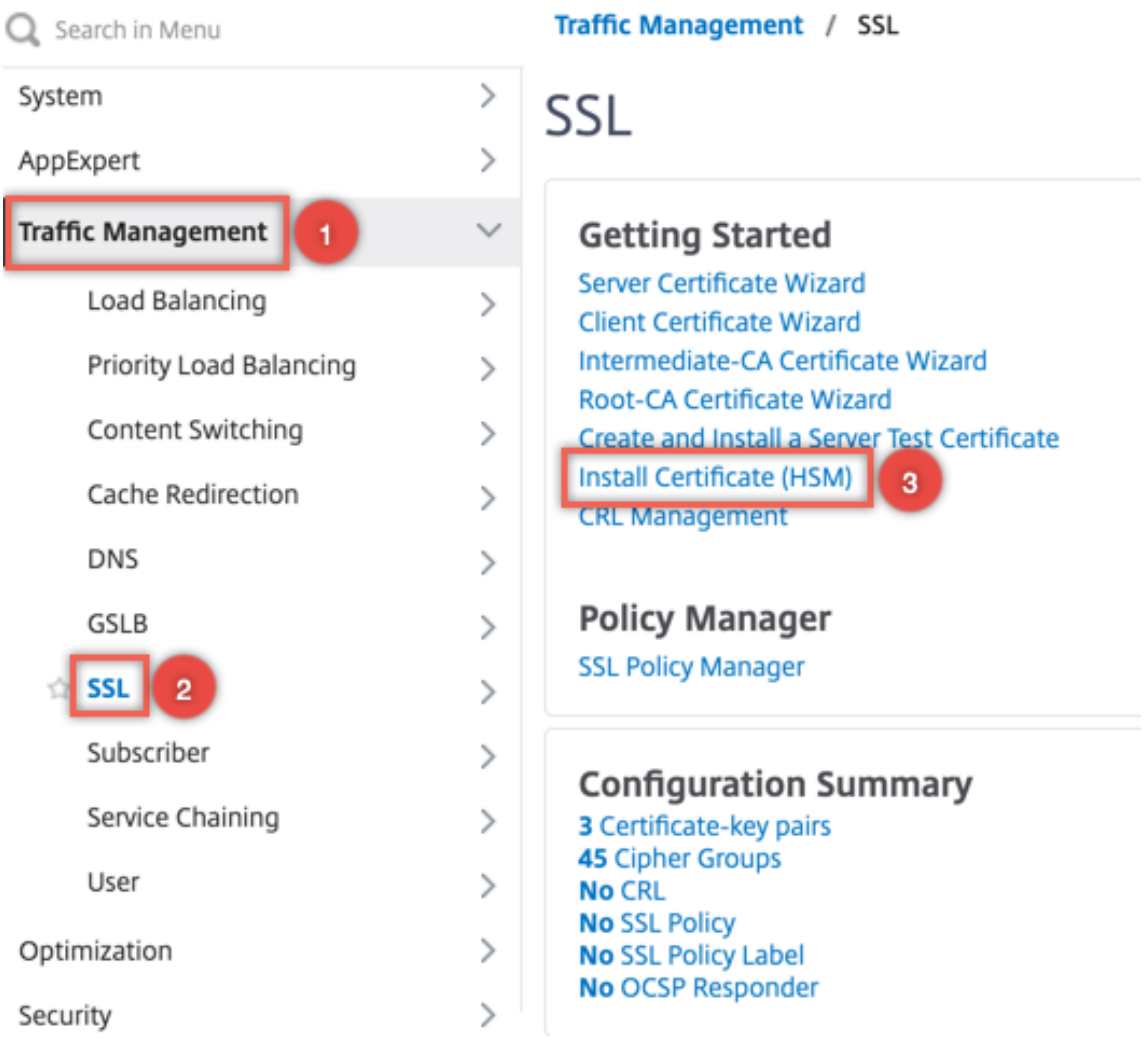

```
add ssl certKey <certkeyName> (-cert <string> [-password]) -hsmKey <
    string>]
show ssl certkey
<!--NeedCopy-->
```

Beispiel:

```
add ssl certKey serverrsa_2048 -cert /nsconfig/ssl/san_certs/san15.pem
    -hsmKey h1
> sh ssl certkey serverrsa_2048
    Name: serverrsa_2048        Status: Valid,   Days to expiration
        :9483
    Version: 3
    Serial Number: F5CFF9EF1E246022
    Signature Algorithm: sha256WithRSAEncryption
    Issuer:  C=in,O=citrix,CN=ca
    Validity
        Not Before: Mar 20 05:42:57 2015 GMT
        Not After : Mar 12 05:42:57 2045 GMT
    Certificate Type:   "Server Certificate"
    Subject:  C=in,O=citrix
    Public Key Algorithm: rsaEncryption
    Public Key size: 2048
    Ocsp Response Status: NONE
 Done
<!--NeedCopy-->
```

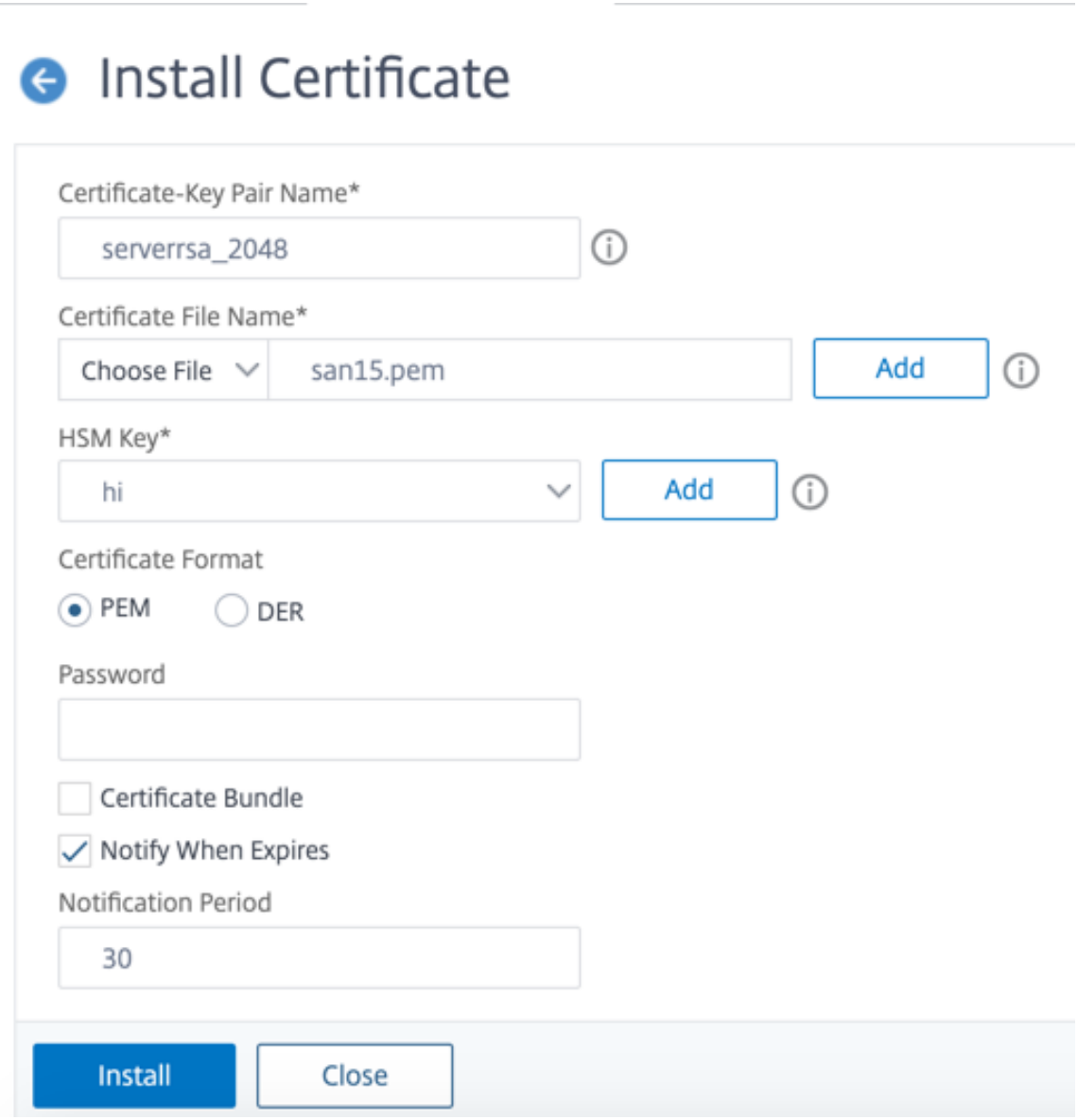
So fügen Sie ein Zertifikatsschlüsselpaar mithilfe der GUI hinzu

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikat (HSM) installieren**.



2. Geben Sie Werte für die folgenden Parameter ein:

   - Name des Zertifikatschlüssel-Paars
   - Name der Zertifikatsdatei
   - HSM-Schlüssel



3. Klicken Sie auf **Installieren**.

Binden Sie das Zertifikatsschlüsselpaar an einen virtuellen Server

Das für die Verarbeitung von SSL-Transaktionen verwendete Zertifikat muss an den virtuellen Server gebunden sein, der die SSL-Daten empfängt.

So binden Sie das SSL-Zertifikatsschlüsselpaar mithilfe der CLI an einen virtuellen Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

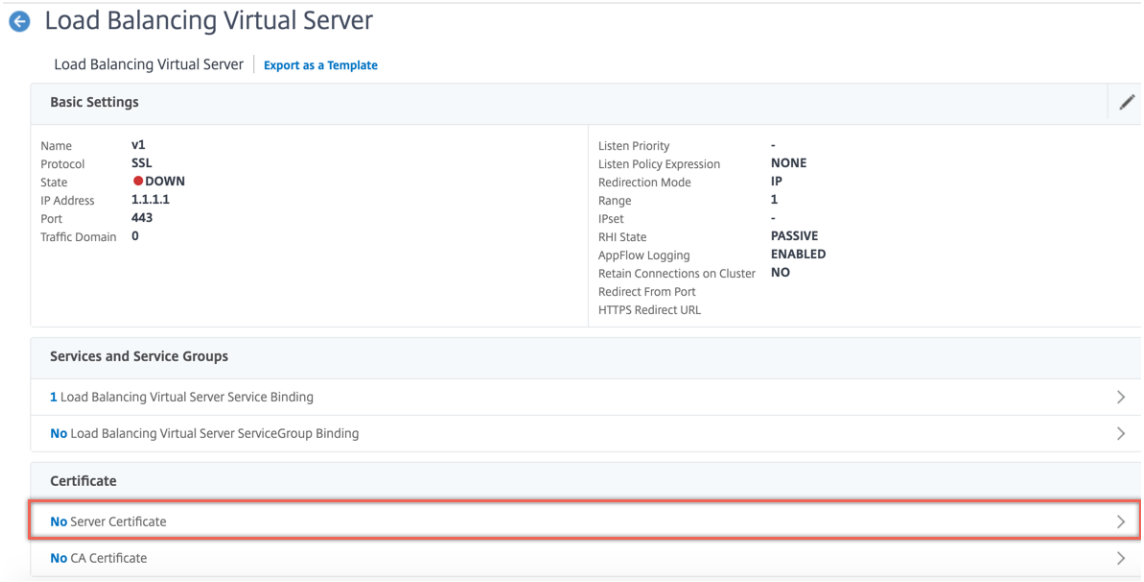

Beispiel:

```
bind ssl vserver v1 -certkeyName serverrsa_2048

sh ssl vserver v1

    Advanced SSL configuration for VServer v1:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED      Refresh Count: 0
    Session Reuse: ENABLED      Timeout: 120 seconds
    Cipher Redirect: DISABLED
    ClearText Port: 0
    Client Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

1)  CertKey Name: serverrsa_2048    Server Certificate



1)  Cipher Name: DEFAULT
    Description: Default cipher list with encryption strength >= 128bit
 Done
<!--NeedCopy-->
```

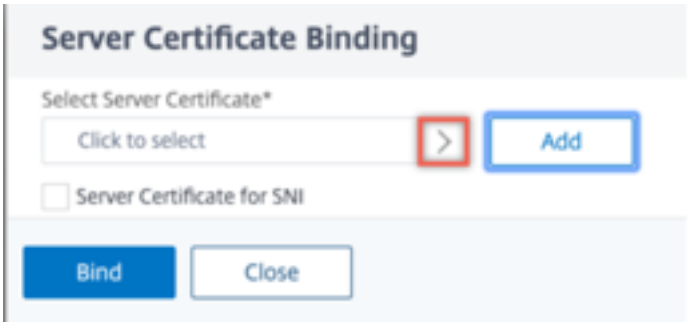
So binden Sie ein SSL-Zertifikatsschlüsselpaar mithilfe der GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und öffnen Sie

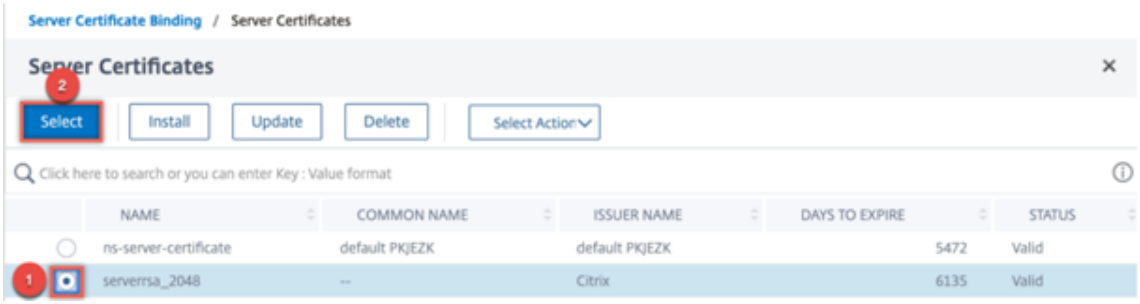
einen virtuellen SSL-Server. Klicken Sie in den Abschnitt Zertifikat .



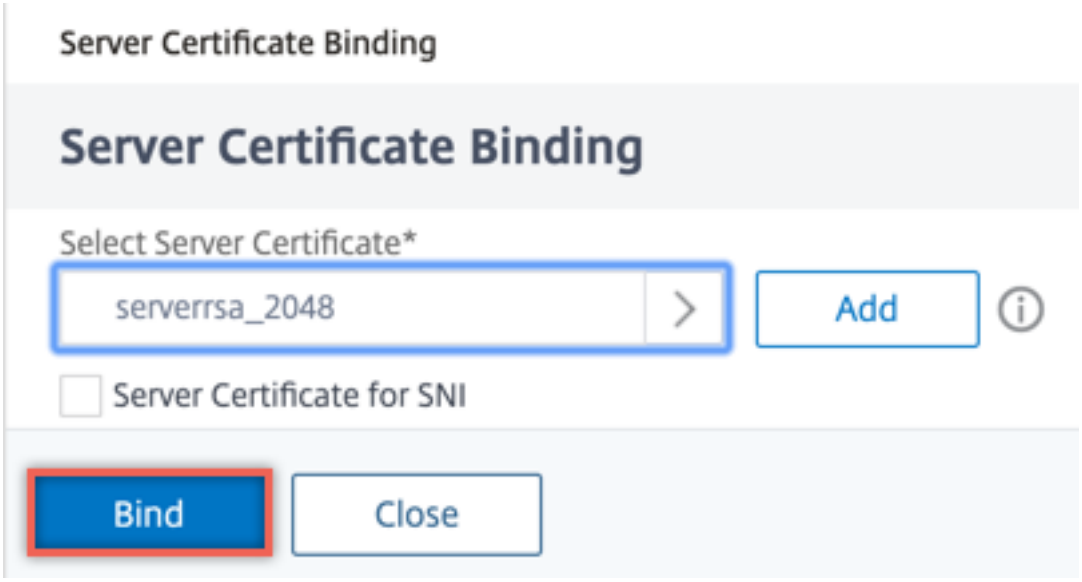
2. Klicken Sie auf den Pfeil, um das Zertifikatsschlüsselpaar auszuwählen.



3. Wählen Sie das Zertifikatsschlüsselpaar aus der Liste aus.



4. Binden Sie das Zertifikatsschlüsselpaar an den virtuellen Server.



Einschränkungen

- Die Anzahl der gleichzeitigen Aufrufe des Azure Key Vault für wichtige Vorgänge ist begrenzt. Die Leistung der ADC-Appliance hängt von den Grenzwerten für Key Vault ab. Weitere Informationen finden Sie unter Microsoft Azure Key Vault-Dokumentation.
- EC-Schlüssel werden nicht unterstützt.
- EDT- und DTLS-Protokolle werden nicht unterstützt.
- ADC-Geräte mit Intel Coleto SSL-Chips werden nicht unterstützt.
- Clustering und Adminpartitionen werden nicht unterstützt.
- Sie können die Azure Application Entity, das Azure Key Vault-Objekt und das HSM-Zertifikatsschlüsselpaar nicht aktualisieren, nachdem Sie sie der ADC-Appliance hinzugefügt haben.
- Ein Zertifikatspaket mit HSM-Schlüsseln wird nicht unterstützt.
- Ein Fehler tritt nicht auf, wenn der HSM-Schlüssel und das Zertifikat nicht übereinstimmen. Stellen Sie beim Hinzufügen eines Zertifikatsschlüsselpaars sicher, dass der HSM-Schlüssel und das Zertifikat übereinstimmen.
- Sie können keinen HSM-Schlüssel an einen virtuellen DTLS-Server binden.
- Sie können OCSP-Anfragen nicht mit einem Zertifikatsschlüsselpaar signieren, das mit einem HSM-Schlüssel erstellt wurde.
- Sie können kein Zertifikatsschlüsselpaar an einen SSL-Dienst binden, wenn das Zertifikatsschlüsselpaar mit einem HSM-Schlüssel erstellt wird.

Häufig gestellte Fragen

Werden bei der Integration in Azure Key Vault private Schlüssel im Speicher der ADC Appliance gespeichert?

Nein, private Schlüssel werden nicht im Speicher der ADC Appliance gespeichert. Für jede SSL-Transaktion sendet die Appliance eine Anfrage an Key Vault.

Ist die Integration FIPS 140-2 Level 2 konform?

Ja, die integrierte Lösung bietet FIPS 140-2 Level 2-Unterstützung.

Welche Schlüsseltypen werden unterstützt?

Es werden nur RSA-Schlüsseltypen unterstützt.

Welche Schlüsselgrößen werden unterstützt?

1024-Bit-, 2048-Bit- und 4096-Bit-RSA-Schlüssel werden unterstützt.

Welche Chiffern werden unterstützt?

Alle auf der ADC-Appliance unterstützten Verschlüsselungen, einschließlich TLSv1.3-Verschlüsselungen mit ECDHE und SHA256, werden unterstützt.

Werden Transaktionen protokolliert?

Die ADC-Appliance protokolliert jede Transaktion, die sie mit dem Schlüsseltresor tätigt. Details wie Uhrzeit, Tresor-IP-Adresse, Port, Erfolg oder Misserfolg der Verbindung und Fehler werden protokolliert.
Im Folgenden finden Sie eine SSL-Protokollausgabe.

```
1 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 896 0 :
    Backend SPCBId 30894 - ServerIP 104.211.224.186 - ServerPort 443
     - ProtocolVersion TLSv1.2 - CipherSuite "ECDHE-RSA-AES256-GCM-
    SHA384 TLSv1.2 Non-Export 256-bit" - Session New -
    SERVER_AUTHENTICATED -SerialNumber "200005
    A75B04365827852D630000000005A75B" - SignatureAlgorithm "
    sha256WithRSAEncryption" - ValidFrom "Mar 17 03:28:42 2019 GMT"
    - ValidTo "Mar 17 03:28:42 2021 GMT" - HandshakeTime 40 ms
2 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
```



```
        0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 897 0 :
      SPCBId 30894 - IssuerName " C=US,ST=Washington,L=Redmond,O=
      Microsoft Corporation,OU=Microsoft IT,CN=Microsoft IT TLS CA 2"
3 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
        0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 898 0 :
      SPCBId 30894 - SubjectName " CN=vault.azure.net"
4 <!--NeedCopy-->
```

Problembehandlung

September 18, 2023

Wenn die SSL-Funktion nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf NetScaler-Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Fehlerbehebung

Die besten Ergebnisse erzielen Sie, wenn Sie die folgenden Ressourcen verwenden, um ein SSL-Problem auf einer NetScaler-Appliance zu beheben:

- Die entsprechende Datei ns.log
- Die neueste ns.conf-Datei
- Die Nachrichtendatei
- Die entsprechende `newnslog` Datei
- Trace-Dateien
- Eine Kopie der Zertifikatsdateien, wenn möglich
- Eine Kopie der Schlüsseldatei, wenn möglich
- Die Fehlermeldung, falls vorhanden

Zusätzlich zu diesen Ressourcen können Sie die Wireshark-Anwendung verwenden, die auf die NetScaler-Trace-Dateien zugeschnitten ist, um die Fehlerbehebung zu beschleunigen.

Behebung von SSL-Problemen

Gehen Sie wie folgt vor, um ein SSL-Problem zu beheben:

- Stellen Sie sicher, dass die NetScaler-Appliance für SSL-Offloading und Load Balancing lizenziert ist.
- Stellen Sie sicher, dass die Funktionen SSL-Offloading und Load Balancing auf der Appliance aktiviert sind.

- Stellen Sie sicher, dass der Status des virtuellen SSL-Servers nicht als DOWN angezeigt wird.
- Stellen Sie sicher, dass der Status des an den virtuellen Server gebundenen Dienstes nicht als DOWN angezeigt wird.
- Stellen Sie sicher, dass ein gültiges Zertifikat an den virtuellen Server gebunden ist.
- Stellen Sie sicher, dass der Dienst einen geeigneten Port verwendet, vorzugsweise Port 443.

Entschlüsselung des TLS1.3-Datenverkehrs aus der Paketverfolgung

Zur Fehlerbehebung bei Protokollen, die über TLS1.3 laufen, müssen Sie zuerst den TLS1.3-Verkehr entschlüsseln. Um TLS 1.3 in Wireshark zu entschlüsseln, müssen die Geheimnisse im NSS Schlüsselprotokollformat exportiert werden. Weitere Informationen zum Schlüsselprotokollformat finden Sie unter NSS Key Log Format.

Informationen zum Erfassen einer Paketverfolgung finden Sie unter Erfassen von SSL-Sitzungsschlüsseln während einer Ablaufverfolgung.

Hinweis: NetScaler protokolliert automatisch die Geheimnisse jeder Verbindung im entsprechenden Format für die verwendete TLS/SSL-Protokollversion.

In einem HA-Setup findet keine CRL-Aktualisierung auf dem sekundären Knoten statt

Die Aktualisierung findet nicht statt, da der CRL-Server nur für den primären Knoten über ein privates Netzwerk zugänglich ist.

Problemumgehung: Fügen Sie auf dem primären Knoten einen Dienst mit der IP-Adresse des CRL-Servers hinzu. Dieser Dienst fungiert als Proxy für den CRL-Server. Wenn die Konfiguration zwischen den Knoten synchronisiert wird, funktioniert die CRL-Aktualisierung sowohl für primäre als auch für sekundäre Knoten über den Dienst, der auf dem primären Knoten konfiguriert ist.

Häufig gestellte Fragen zu SSL

August 15, 2023

Grundlegende Fragen

Der HTTPS-Zugriff auf die GUI schlägt auf einer VPX-Instanz fehl. Wie erhalte ich Zugang?

Für den HTTPS-Zugriff auf die GUI ist ein Zertifikatschlüsselpaar erforderlich. Auf einer NetScaler-Appliance wird ein Zertifikatschlüsselpaar automatisch an die internen Dienste gebunden. Auf einer MPX- oder SDX-Appliance beträgt die Standardschlüsselgröße 1024 Byte, und bei einer VPX-Instanz beträgt die Standardschlüsselgröße 512 Byte. Die meisten Browser akzeptieren heute

jedoch keinen Schlüssel mit weniger als 1024 Bytes. Infolgedessen wird der HTTPS-Zugriff auf das VPX-Konfigurationsdienstprogramm blockiert.

Citrix empfiehlt, ein Zertifikatschlüsselpaar von mindestens 1024 Byte zu installieren und es an den internen Dienst für den HTTPS-Zugriff auf das Konfigurationsdienstprogramm zu binden. Aktualisieren Sie alternativ den `ns-server-certificate` auf 1024 Bytes. Sie können den HTTP-Zugriff auf das Konfigurationsdienstprogramm oder die CLI verwenden, um das Zertifikat zu installieren.

Wenn ich einer MPX-Appliance eine Lizenz hinzufüge, geht die Bindung des Zertifikatschlüsselpaars verloren. Wie löse ich dieses Problem?

Wenn beim Start keine Lizenz auf einer MPX-Appliance vorhanden ist und Sie später eine Lizenz hinzufügen und die Appliance neu starten, verlieren Sie möglicherweise die Zertifikatbindung. Installieren Sie das Zertifikat neu und binden Sie es an den internen Dienst

Citrix empfiehlt, vor dem Starten der Appliance eine entsprechende Lizenz zu installieren.

Was sind die verschiedenen Schritte beim Einrichten eines sicheren Kanals für eine SSL-Transaktion?

Das Einrichten eines sicheren Kanals für eine SSL-Transaktion umfasst die folgenden Schritte:

1. Der Client sendet eine HTTPS-Anfrage für einen sicheren Kanal an den Server.
2. Nach Auswahl des Protokolls und der Verschlüsselung sendet der Server sein Zertifikat an den Client.
3. Der Client überprüft die Authentizität des Serverzertifikats.
4. Wenn eine der Prüfungen fehlschlägt, zeigt der Client das entsprechende Feedback an.
5. Wenn die Schecks bestehen oder der Kunde sich entscheidet, fortzufahren, auch wenn eine Überprüfung fehlschlägt, erstellt der Kunde einen temporären, wegwerfbaren Schlüssel. Dieser Schlüssel wird als *Pre-Master-Geheimnis* bezeichnet und der Client verschlüsselt diesen Schlüssel mithilfe des öffentlichen Schlüssels des Serverzertifikats.
6. Der Server entschlüsselt es nach Erhalt des Pre-Master-Geheimnisses mit dem privaten Schlüssel des Servers und generiert die Sitzungsschlüssel. Der Client generiert auch die Sitzungsschlüssel aus dem Pre-Master-Geheimnis. Daher haben sowohl Client als auch Server jetzt einen gemeinsamen Sitzungsschlüssel, der zur Verschlüsselung und Entschlüsselung von Anwendungsdaten verwendet wird.

Ich verstehe, dass SSL ein CPU-intensiver Prozess ist. Wie hoch sind die CPU-Kosten im Zusammenhang mit dem SSL-Prozess?

Die folgenden beiden Phasen sind mit dem SSL-Prozess verbunden:

- Der erste Handshake und die sichere Kanaleinrichtung unter Verwendung der öffentlichen und privaten Schlüsseltechnologie.
- Massendatenverschlüsselung unter Verwendung der symmetrischen Schlüsseltechnologie.

Beide vorangegangenen Phasen können sich auf die Serverleistung auswirken und erfordern aus folgenden Gründen eine intensive CPU-Verarbeitung:

1. Der erste Handshake beinhaltet Kryptographie mit öffentlich-privaten Schlüsseln, die aufgrund großer Schlüsselgrößen (1024 Bit, 2048 Bit, 4096 Bit) sehr CPU-intensiv ist.
2. Die Verschlüsselung/Entschlüsselung von Daten ist ebenfalls rechnerisch teuer, abhängig von der Datenmenge, die verschlüsselt oder entschlüsselt werden muss.

Was sind die verschiedenen Entitäten einer SSL-Konfiguration?

Eine SSL-Konfiguration hat die folgenden Entitäten:

- Serverzertifikat
- Zertifikat der Zertifizierungsstelle (CA)
- Cipher Suite, die die Protokolle für die folgenden Aufgaben angibt:
  - Anfänglicher Schlüsselaustausch
  - Server- und Clientauthentifizierung
  - Algorithmus zur Massenverschlüsselung
  - Nachrichten-Authentifizierung
- Clientauthentifizierung
- CRL
- SSL Certificate Key Generierung Tool, mit dem Sie die folgenden Dateien erstellen können:
  - Anforderung des Zertifikats
  - Selbstsigniertes Zertifikat
  - RSA-Schlüssel
  - DH-Parameter

Ich möchte die SSL-Entladungsfunktion der NetScaler-Appliance verwenden. Welche Möglichkeiten gibt es, ein SSL-Zertifikat zu erhalten?

Sie müssen ein SSL-Zertifikat erhalten, bevor Sie das SSL-Setup auf der NetScaler-Appliance konfigurieren können. Sie können eine der folgenden Methoden verwenden, um ein SSL-Zertifikat zu erhalten:

- Fordern Sie ein Zertifikat von einer autorisierten Zertifizierungsstelle (CA) an.
- Verwenden Sie das vorhandene Serverzertifikat.
- Erstellen Sie ein Zertifikatschlüsselpaar auf der NetScaler-Appliance.

Hinweis: Dieses Zertifikat ist ein Testzertifikat, das von der NetScaler-Appliance generiert wurde, signiert von der Test-Root-CA. Von der Test-Root-CA signierte Testzertifikate werden von Browsern nicht akzeptiert. Der Browser löst eine Warnmeldung aus, die besagt, dass das Zertifikat des Servers nicht authentifiziert werden kann.

- Für andere Zwecke als Testzwecke müssen Sie ein gültiges CA-Zertifikat und einen CA-Schlüssel angeben, um das Serverzertifikat zu signieren.

Was sind die Mindestanforderungen für ein SSL-Setup?

Die Mindestanforderungen für die Konfiguration eines SSL-Setups lauten wie folgt:

- Besorgen Sie sich die Zertifikate und Schlüssel.
- Erstellen Sie einen virtuellen Lastenausgleich SSL-Server.
- Binden Sie HTTP- oder SSL-Dienste an den virtuellen SSL-Server.
- Binden Sie ein Zertifikatschlüsselpaar an den virtuellen SSL-Server.

Was sind die Grenzen für die verschiedenen Komponenten von SSL?

SSL-Komponenten haben folgende Grenzwerte:

- Bitgröße von SSL-Zertifikaten: 4096
- Anzahl der SSL-Zertifikate: Hängt vom verfügbaren Speicher auf der Appliance ab.
- Maximal verknüpfte Zwischenzertifikate CA SSL: 9 pro Kette.
- CRL-Widerrufe: Hängt vom verfügbaren Speicher auf der Appliance ab.

Was sind die verschiedenen Schritte bei der End-to-End-Datenverschlüsselung auf einer NetScaler-Appliance?

Der serverseitige Verschlüsselungsprozess auf einer NetScaler-Appliance umfasst die folgenden Schritte:

1. Der Client stellt eine Verbindung mit dem SSL-VIP her, der auf der NetScaler-Appliance am sicheren Standort konfiguriert ist.
2. Nach Erhalt der sicheren Anforderung entschlüsselt die Appliance die Anforderung und wendet Content Switching-Techniken der Layer 4 bis 7 und Load Balancing-Richtlinien an. Anschließend wählt es den besten verfügbaren Back-End-Webserver für die Anforderung aus.
3. Die NetScaler-Appliance erstellt eine SSL-Sitzung mit dem ausgewählten Server.
4. Nach dem Einrichten der SSL-Sitzung verschlüsselt die Appliance die Clientanforderung und sendet sie mithilfe der sicheren SSL-Sitzung an den Webserver.

5. Wenn die Appliance die verschlüsselte Antwort vom Server erhält, entschlüsselt und verschlüsselt sie die Daten erneut. Anschließend sendet es die Daten über die CLIentseitigen SSL-Sitzung an den Client.

Die Multiplexing-Technik der NetScaler-Appliance ermöglicht es der Appliance, SSL-Sitzungen wiederzuverwenden, die mit den Webservern eingerichtet wurden. Daher vermeidet die Appliance den CPU-intensiven Schlüsselaustausch, der als *Full Handshake*bezeichnet wird. Dieser Prozess reduziert die Gesamtzahl der SSL-Sitzungen auf dem Server und gewährleistet die End-to-End-Sicherheit.

Zertifikate und Schlüssel

Kann ich das Zertifikat und die Schlüsseldateien an einem beliebigen Ort ablegen? Gibt es einen empfohlenen Speicherort zum Speichern dieser Dateien?

Sie können das Zertifikat und die Schlüsseldateien auf der NetScaler-Appliance oder einem lokalen Computer speichern. Citrix empfiehlt jedoch, das Zertifikat und die Schlüsseldateien im Verzeichnis `/nsconfig/ssl` der NetScaler-Appliance zu speichern. Das Verzeichnis `/etc` ist im Flash-Speicher der NetScaler-Appliance. Diese Aktion bietet Portabilität und erleichtert die Backup und Wiederherstellung der Zertifikatsdateien auf der Appliance.

Hinweis: Stellen Sie sicher, dass das Zertifikat und die Schlüsseldateien im selben Verzeichnis gespeichert sind.

Wie groß ist die maximale Größe des Zertifikatsschlüssels, der auf der NetScaler-Appliance unterstützt wird?

Eine NetScaler-Appliance, auf der eine Softwareversion vor Version 9.0 ausgeführt wird, unterstützt eine maximale Zertifikatschlüsselgröße von 2048 Bit. Version 9.0 und höher unterstützt eine maximale Zertifikatschlüsselgröße von 4096 Bit. Diese Grenze gilt für RSA-Zertifikate.

Eine MPX-Appliance unterstützt Zertifikate von 512 Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server
- 4096-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist)

Eine virtuelle Appliance unterstützt Zertifikate von 512 Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server

- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server
- 2048-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist)

Wie groß ist die maximale Größe des DH-Parameters, der auf der NetScaler-Appliance unterstützt wird?

Die NetScaler-Appliance unterstützt einen DH-Parameter von maximal 2048 Bit.

Wie hoch ist die maximale Länge der Zertifikatkette, d. h. die maximale Anzahl von Zertifikaten in einer Kette, die auf einer NetScaler-Appliance unterstützt wird?

Eine NetScaler-Appliance kann beim Senden einer Serverzertifikatnachricht maximal 10 Zertifikate in einer Kette senden. Eine Kette mit maximaler Länge umfasst das Serverzertifikat und neun Zwischenzertifikate der Zertifizierungsstelle.

Welche Zertifikate und Schlüsselformate werden auf der NetScaler-Appliance unterstützt?

Die NetScaler-Appliance unterstützt die folgenden Zertifikat- und Schlüsselformate:

- Datenschutz Verbesserte E-Mails (PEM)
- Distinguished Coding Regel (DER)

Gibt es ein Limit für die Anzahl der Zertifikate und Schlüssel, die ich auf der NetScaler-Appliance installieren kann?

Nein. Die Anzahl der Zertifikate und Schlüssel, die installiert werden können, ist nur durch den verfügbaren Speicher auf der NetScaler-Appliance begrenzt.

Ich habe das Zertifikat und die Schlüsseldateien auf dem lokalen Computer gespeichert. Ich möchte diese Dateien mithilfe des FTP-Protokolls auf die NetScaler-Appliance übertragen. Gibt es einen bevorzugten Modus für die Übertragung dieser Dateien auf die NetScaler-Appliance?

Ja. Wenn Sie das FTP-Protokoll verwenden, müssen Sie das Zertifikat und die Schlüsseldateien im Binärmodus an die NetScaler-Appliance übertragen.

Hinweis: Standardmäßig ist FTP deaktiviert. Citrix empfiehlt, das SCP-Protokoll für die Übertragung von Zertifikats- und Schlüsseldateien zu verwenden. Das Konfigurationsdienstprogramm verwendet implizit SCP, um eine Verbindung mit der Appliance herzustellen.

Was ist der Standardverzeichnispfad für das Zertifikat und den Schlüssel?

Der Standardverzeichnispfad für das Zertifikat und den Schlüssel ist '/nsconfig/ssl'.

Was passiert beim Hinzufügen eines Zertifikats und eines Schlüsselpaars, wenn ich keinen absoluten Pfad zu den Zertifikats- und Schlüsseldateien angebe?

Geben Sie beim Hinzufügen eines Zertifikatschlüsselpaars einen absoluten Pfad zu den Zertifikats- und Schlüsseldateien an. Wenn Sie dies nicht angeben, durchsucht die ADC-Appliance das Standardverzeichnis nach diesen Dateien und versucht, sie in den Kernel zu laden. Das Standardverzeichnis ist `/nsconfig/ssl`. Wenn beispielsweise die cert1024.pem- und rsa1024.pem-Dateien im Verzeichnis `/nsconfig/ssl` der Appliance verfügbar sind, sind beide der folgenden Befehle erfolgreich:

```
1 add ssl certKey cert1 -cert cert1204.pem -key rsa1024.pem
2 <!--NeedCopy-->
```

```
1 add ssl certKey cert1 -cert /nsconfig/ssl/cert1204.pem -key /nsconfig/
     ssl/rsa1024.pem
2 <!--NeedCopy-->
```

Ich habe ein Hochverfügbarkeits-Setup konfiguriert. Ich möchte die SSL-Funktion im Setup implementieren. Wie muss ich mit dem Zertifikat und den Schlüsseldateien in einem Hochverfügbarkeits-Setup umgehen?

In einem Hochverfügbarkeits-Setup müssen Sie das Zertifikat und die Schlüsseldateien sowohl auf der primären als auch auf der sekundären NetScaler-Appliance speichern. Der Verzeichnispfad für das Zertifikat und die Schlüsseldateien muss auf beiden Appliances identisch sein, bevor Sie ein SSL-Zertifikatschlüsselpaar auf der primären Appliance hinzufügen.

nCipher nShield® HSM

Müssen wir bei der Integration mit nCipher nShield® HSM eine bestimmte Konfiguration berücksichtigen, wenn wir die NetScaler-Appliance zu HA hinzufügen?

Konfigurieren Sie dieselben nCipher-Geräte auf beiden Knoten in HA. nCipher Konfigurationsbefehle werden nicht in HA synchronisiert. Informationen zu den Voraussetzungen für nCipher nShield® HSM finden Sie unter Voraussetzungen.

Müssen wir beide Appliances individuell mit nCipher nShield® HSM und RFS integrieren? Müssen wir diese Aktion vor oder nach dem HA-Setup abschließen?

Sie können die Integration vor oder nach dem HA-Setup abschließen. Wenn die Integration nach dem HA-Setup erfolgt, werden die Schlüssel, die vor der Konfiguration des sekundären Knotens auf den primären Knoten importiert wurden, nicht mit dem sekundären Knoten synchronisiert. Daher empfiehlt Citrix die nCipher Integration vor dem HA-Setup.

Müssen wir den Schlüssel sowohl in die primäre als auch in die sekundären NetScaler-Appliances importieren oder werden die Schlüssel vom primären Knoten mit dem sekundären Knoten synchronisiert?

Wenn nCipher vor der Bildung des HA auf beiden Geräten integriert ist, werden die Schlüssel während der Integration automatisch von RFS synchronisiert.

Angesichts der Tatsache, dass sich das HSM nicht auf der NetScaler-Appliance, sondern auf nCipher befindet, was passiert mit den Schlüsseln und Zertifikaten, wenn ein Knoten ausfällt und ersetzt wird?

Wenn ein Knoten ausfällt, können Sie die Schlüssel und Zertifikate mit dem neuen Knoten synchronisieren, indem Sie nCipher auf den neuen Knoten integrieren. Führen Sie dann die folgenden Befehle aus:

```
1 sync ha files ssl
2 force ha sync
3 <!--NeedCopy-->
```

Die Zertifikate werden synchronisiert und hinzugefügt, wenn die Schlüssel bei der Integration von nCipher synchronisiert werden.

Chiffern

Was ist eine Null-Chiffre?

Chiffern ohne Verschlüsselung werden als Null-Chiffers bezeichnet. Zum Beispiel ist NULL-MD5 eine Null-Chiffre.

Sind die Null-Chiffern standardmäßig für einen SSL-VIP oder einen SSL-Dienst aktiviert?

Nein. Null-Chiffern sind für einen SSL-VIP oder einen SSL-Dienst standardmäßig nicht aktiviert.

Wie ist das Verfahren zum Entfernen von Null-Chiffern?

Um die Null-Chiffern aus einem SSL-VIP zu entfernen, führen Sie den folgenden Befehl aus:

```
bind ssl cipher <SSL_VIP> REM NULL
<!--NeedCopy-->
```

Um die Null-Chiffern aus einem SSL-Dienst zu entfernen, führen Sie den folgenden Befehl aus:

```
bind ssl cipher <SSL_Service> REM NULL -service
<!--NeedCopy-->
```

Welche verschiedenen Chiffrieraliase werden auf der NetScaler-Appliance unterstützt?

Um die auf der Appliance unterstützten Verschlüsselungsaliase aufzulisten, geben Sie an der Eingabeaufforderung Folgendes ein:

```
sh cipher
<!--NeedCopy-->
```

Wie lautet der Befehl zum Anzeigen aller vordefinierten Chiffuren der NetScaler-Appliance?

Um alle vordefinierten Chiffuren der NetScaler-Appliance anzuzeigen, geben Sie an der CLI Folgendes ein:

```
show ssl cipher
<!--NeedCopy-->
```

Wie lautet der Befehl, um die Details einer einzelnen Chiffre der NetScaler-Appliance anzuzeigen?

Um die Details einer einzelnen Chiffre der NetScaler-Appliance anzuzeigen, geben Sie an der CLI Folgendes ein:

```
show ssl cipher <Cipher_Name/Cipher_Alias_Name/Cipher_Group_Name>
<!--NeedCopy-->
```

Beispiel:

```
show cipher SSL3-RC4-SHA
     1) Cipher Name: SSL3-RC4-SHA
     Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128)
    Mac=SHA1
```



```
5        Done
6  <!--NeedCopy-->
```

Welche Bedeutung hat das Hinzufügen der vordefinierten Chiffuren der NetScaler-Appliance?

Durch das Hinzufügen der vordefinierten Verschlüsselungen der NetScaler-Appliance werden die NULL-Ciphers zu einem SSL-VIP oder einem SSL-Dienst hinzugefügt.

Ist es möglich, die Reihenfolge der Chiffre zu ändern, ohne sie von einer Chiffriergruppe auf einer NetScaler-Appliance abzubinden?

Ja. Es ist möglich, die Reihenfolge der Chiffre zu ändern, ohne die Chiffren von einer benutzerdefinierten Chiffriergruppe aufzuheben. Sie können die Priorität in eingebauten Chiffriergruppen jedoch nicht ändern. Um die Priorität einer an eine SSL-Entität gebundenen Chiffre zu ändern, heben Sie zuerst die Bindung des virtuellen Servers, des Dienstes oder der Servicegruppe auf.

Hinweis: Wenn die an eine SSL-Entität gebundene Chiffriergruppe leer ist, schlägt der SSL-Handshake fehl, da keine ausgehandelte Chiffre vorhanden ist. Die Chiffriergruppe muss mindestens eine Chiffre enthalten.

Wird ECDSA auf der NetScaler-Appliance unterstützt?

ECDSA wird auf den folgenden NetScaler Plattformen unterstützt. Weitere Informationen zu unterstützten Builds finden Sie in Tabelle 1 und Tabelle 2 in Chiffren, die auf den NetScaler-Appliances verfügbar sind.

- NetScaler MPX- und SDX-Appliances mit N3-Chips
- NetScaler MPX 5900/8900/15000/26000
- NetScaler SDX 8900/15000
- NetScaler VPX Appliances

Unterstützt die NetScaler VPX Appliance AES-GCM/SHA2-Chiffern im Front-End?

Ja, AES-GCM/SHA2-Chiffre werden auf der NetScaler VPX Appliance unterstützt. Weitere Informationen zu den unterstützten Builds finden Sie unter Chiffren, die auf den NetScaler-Appliances verfügbar sind.

Zertifikate

Ist der Distinguished Name in einem Clientzertifikat für die Dauer der Benutzersitzung verfügbar?

Ja. Während der Dauer der Benutzersitzung können Sie in nachfolgenden Anfragen auf den Distinguished Name des Clientzertifikats zugreifen. Das heißt, selbst nachdem der SSL-Handshake abgeschlossen ist und das Zertifikat vom Browser nicht erneut gesendet wird. Verwenden Sie eine Variable und eine Zuweisung, wie in der folgenden Beispielkonfiguration beschrieben:

Beispiel:

```
add ns variable v2 -type "text(100)"

add ns assignment a1 -variable "$v2" -set       "CLIENT.SSL.CLIENT_CERT
    .SUBJECT.TYPECAST_NVLIST_T('=','/').VALUE("CN")"

add rewrite action act1 insert_http_header subject "$v2"  // example:
    to insert the distinguished name in the header

add rewrite policy pol1 true a1

add rewrite policy pol2 true act1

bind rewrite global pol1 1 next -type RES_DEFAULT

bind rewrite global pol2 2 next -type RES_DEFAULT

set rewrite param -undefAction RESET
<!--NeedCopy-->
```

Warum muss ich das Serverzertifikat binden?

Die Bindung der Serverzertifikate ist die Grundvoraussetzung dafür, dass die SSL-Konfiguration SSL-Transaktionen verarbeiten kann.

Um das Serverzertifikat an einen SSL-VIP zu binden, geben Sie an der CLI Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Um das Serverzertifikat an einen SSL-Dienst zu binden, geben Sie an der CLI Folgendes ein:

```
bind ssl service <serviceName> -certkeyName <cert_name>
<!--NeedCopy-->
```


Wie viele Zertifikate kann ich an einen SSL-VIP oder einen SSL-Dienst binden?

Auf einer NetScaler VPX-, MPX/SDX (N3)- und MPX/SDX 14000 FIPS-Appliance können Sie zwei Zertifikate an einen virtuellen SSL-Server oder einen SSL-Dienst binden, wenn SNI deaktiviert ist. Die Zertifikate müssen jeweils eins vom Typ RSA und ECDSA sein. Wenn SNI aktiviert ist, können Sie mehrere Serverzertifikate vom Typ RSA oder ECDSA binden. Wenn SNI deaktiviert ist, können Sie auf einer NetScaler MPX (N2) oder MPX 9700 FIPS-Appliance nur ein Zertifikat vom Typ RSA binden. Wenn SNI aktiviert ist, können Sie nur mehrere Serverzertifikate vom Typ RSA binden.

Was passiert, wenn ich ein Serverzertifikat aufhebe oder überschreibe?

Wenn Sie das Binden oder Überschreiben eines Serverzertifikats aufheben oder überschreiben, werden alle Verbindungen und SSL-Sitzungen beendet, die mit dem vorhandenen Zertifikat erstellt wurden. Wenn Sie ein vorhandenes Zertifikat überschreiben, wird die folgende Meldung angezeigt:

```
ERROR:

Warning: Current certificate replaces the previous binding.
<!--NeedCopy-->
```

Wie installiere ich ein Zwischenzertifikat auf einer NetScaler-Appliance und verbinde mich mit einem Serverzertifikat?

Weitere Informationen zur Installation eines Zwischenzertifikats finden Sie im Artikel unter http://support.citrix.com/article/ctx114146.

Warum erhalte ich einen Fehler “Ressource existiert bereits”, wenn ich versuche, ein Zertifikat auf dem NetScaler zu installieren?

Anweisungen zum Beheben des Fehlers “Ressource existiert bereits” finden Sie im Artikel unter http://support.citrix.com/article/CTX117284.

Ich möchte ein Serverzertifikat auf einer NetScaler-Appliance erstellen, um das Produkt zu testen und auszuwerten. Wie ist das Verfahren zum Erstellen eines Serverzertifikats?

Führen Sie das folgende Verfahren aus, um ein Testzertifikat zu erstellen.

Hinweis: Ein mit diesem Verfahren erstelltes Zertifikat kann nicht zur Authentifizierung aller Benutzer und Browser verwendet werden. Nachdem Sie das Zertifikat zum Testen verwendet haben, müssen Sie ein Serverzertifikat erhalten, das von einer autorisierten Root-Zertifizierungsstelle signiert wurde.

So erstellen Sie ein selbstsigniertes Serverzertifikat:

1. Um ein Root-CA-Zertifikat zu erstellen, geben Sie an der CLI Folgendes ein:

```
create ssl rsakey /nsconfig/ssl/test-ca.key 1024

create ssl certreq /nsconfig/ssl/test-ca.csr -keyfile /nsconfig/
   ssl/test-ca.key

Enter the required information when prompted, and then type the
   following command:

create ssl cert /nsconfig/ssl/test-ca.cer /nsconfig/ssl/test-ca.
   csr ROOT_CERT -keyfile /nsconfig/ssl/test-ca.key
<!--NeedCopy-->
```

2. Führen Sie das folgende Verfahren aus, um ein Serverzertifikat zu erstellen und es mit dem soeben erstellten Stammzertifikat zu signieren

   a) Um die Anforderung und den Schlüssel zu erstellen, geben Sie an der CLI Folgendes ein:

```
create ssl rsakey /nsconfig/ssl/test-server.key 1024

    create ssl certreq /nsconfig/ssl/test-server.csr -keyfile
       /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

   b) Geben Sie bei Aufforderung die erforderlichen Informationen ein.

   c) Um eine Seriennummerndatei zu erstellen, geben Sie an der CLI Folgendes ein:

```
shell
 # echo '01' >
/nsconfig/ssl/serial.txt
 # exit
<!--NeedCopy-->
```

   d) Um ein Serverzertifikat zu erstellen, das von dem in Schritt 1 erstellten Stammzertifikat signiert wurde, geben Sie an der CLI Folgendes ein:

```
create ssl cert /nsconfig/ssl/test-server.cer /nsconfig/ssl/
   test-server.csr SRVR_CERT -CAcert /nsconfig/ssl/test-ca.cer
    -CAkey /nsconfig/ssl/test-ca.key -CAserial /nsconfig/ssl/
   serial.txt
<!--NeedCopy-->
```

   e) Um ein NetScaler Cert-Schlüsselpaar, das das In-Memory-Objekt ist, das die Serverzertifikatsinformationen für SSL-Handshakes und Massenverschlüsselung enthält, an der CLI

zu erstellen, geben Sie Folgendes ein:

```
add ssl certkey test-certkey -cert /nsconfig/ssl/test-server.
    cer -key /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

f) Um das Cert-Schlüsselpaar an den virtuellen SSL-Server zu binden, geben Sie an der CLI Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Ich habe eine NetScaler-Appliance erhalten, auf der NetScaler Software-Release 9.0 installiert ist. Mir ist eine zusätzliche Lizenzdatei auf der Appliance aufgefallen. Gibt es eine Änderung der Lizenzrichtlinie, beginnend mit NetScaler Software Release 9.0?

Ja. Ab der NetScaler-Softwareversion 9.0 verfügt die Appliance möglicherweise über keine einzige Lizenzdatei. Die Anzahl der Lizenzdateien hängt von der NetScaler Software Release-Edition ab. Wenn Sie beispielsweise die Advanced Edition installiert haben, benötigen Sie möglicherweise zusätzliche Lizenzdateien, um die verschiedenen Funktionen voll funktionsfähig zu machen. Wenn Sie jedoch die Premium Edition installiert haben, verfügt die Appliance über nur eine Lizenzdatei.

Wie exportiere ich das Zertifikat aus dem Internetinformationsdienst (IIS)?

Es gibt viele Möglichkeiten, aber mit der folgenden Methode werden das entsprechende Zertifikat und der private Schlüssel für die Website exportiert. Dieser Vorgang muss auf dem eigentlichen IIS-Server durchgeführt werden.

1. Öffnen Sie das Verwaltungstool für Internetinformationsdienste (IIS) Manager.
2. Erweitern Sie den Website-Knoten und suchen Sie die SSL-fähige Website, die Sie über die NetScaler-Appliance bereitstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf diese Website und klicken Sie
4. Klicken Sie auf die Registerkarte Verzeichnissicherheit, und wählen Sie im Abschnitt Sichere Kommunikation des Fensters das Feld Zertifikat anzeigen aus.
5. Klicken Sie auf die Registerkarte Details und dann auf In Datei kopieren.
6. Klicken Sie auf der Seite Willkommen beim Zertifikatexport-Assistenten auf Weiter.
7. Wählen Sie Ja aus, exportieren Sie den privaten Schlüssel und klicken Sie auf Weiter.

   Hinweis: Der private Schlüssel MUSS exportiert werden, damit SSL Offload am NetScaler arbeitet.

8. Stellen Sie sicher, dass das Optionsfeld Persönlicher Informationsaustausch -PKCS #12 aktiviert ist, und aktivieren Sie nach Möglichkeit *nur* das Kontrollkästchen Alle Zertifikate in den Zertifizierungspfad einbeziehen. Klicken Sie auf Weiter.
9. Geben Sie ein Kennwort ein und klicken Sie auf Weiter.
10. Geben Sie einen Dateinamen und einen Speicherort ein, und klicken Sie dann auf Weiter. Geben Sie der Datei eine Erweiterung von .PFX.
11. Klicken Sie auf Fertig stellen.

Wie konvertiere ich das PKCS #12 -Zertifikat und installiere es auf dem NetScaler?

1. Verschieben Sie die exportierte PFX-Zertifikatdatei an einen Speicherort, von dem aus sie auf die NetScaler-Appliance kopiert werden kann. Das heißt, auf einen Computer, der SSH-Zugriff auf die Verwaltungsschnittstelle einer NetScaler-Appliance ermöglicht. Kopieren Sie das Zertifikat mithilfe eines sicheren Kopierdienstprogramms wie SCP auf die Appliance.
2. Greifen Sie auf die BSD-Shell zu und konvertieren Sie das Zertifikat (z. B. Cert.PFX) in das PEM-Format:

```
root@ns# openssl pkcs12 -in cert.PFX -out cert.PEM
<!--NeedCopy-->
```

3. Um sicherzustellen, dass das konvertierte Zertifikat das richtige x509-Format hat, stellen Sie sicher, dass der folgende Befehl keinen Fehler verursacht:

```
root@ns# openssl x509 -in cert.PEM -text
<!--NeedCopy-->
```

4. Stellen Sie sicher, dass die Zertifikatsdatei einen privaten Schlüssel enthält. Geben Sie zunächst den folgenden Befehl aus:

```
root@ns# cat cert.PEM

Verify that the output file includes an RSA PRIVATE KEY section.

-----BEGIN RSA PRIVATE KEY-----
Mkm^s9KMs9023pz/s...
-----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

   Im Folgenden finden Sie ein weiteres Beispiel für einen Abschnitt mit RSA PRIVATE KEY:

```
    Bag Attributes
    1.3.6.1.4.1.311.17.2: <No Values>
```



```
    localKeyID: 01 00 00 00
    Microsoft CSP Name: Microsoft RSA SChannel Cryptographic
    Provider
    friendlyName:
    4b9cef4cc8c9b849ff5c662fd3e0ef7e_76267e3e-6183-4d45-886e-6
       e067297b38f

    Key Attributes
    X509v3 Key Usage: 10
    -----BEGIN RSA PRIVATE KEY-----
    Proc-Type: 4,ENCRYPTED
    DEK-Info: DES-EDE3-CBC,43E7ACA5F4423968
    pZJ2SfsSVqMbRRf6ug37Clua5gY0Wld4frPIxFXyJquUHr31dilW5ta3hbIaQ+
       Rg

    ... (more random characters)
    v8dMugeRplkaH2Uwt/mWBk4t71Yv7GeHmcmjafK8H8iW80ooPO3D/ENV8X4U/
       tlh

    5eU6ky3WYZ1BTy6thxxLlwAullynVXZEflNLxq1oX+ZYl6djgjE3qg==
    -----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

Im Folgenden finden Sie einen Abschnitt SERVERZERTIFIKAT

```
    Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: AG Certificate
    subject=/C=AU/ST=NSW/L=Wanniassa/O=Dave Mother
    Asiapacific/OU=Support/CN=davemother.food.lan
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIFiTCCBHGgAwIBAgIKCGryDgAAAAAHzANBgkqhkiG9w0BAQUFADA8MRMwEQYK


    ... (more random characters) 5
       pLDWYVHhLkA1pSxvFjNJHRSIydWHc5ltGyKqIUcBezVaXyel94pNSUYx07NpPV
       /

    MY2ovQyQZM8gGe3+lGFum0VHbv/y/gB9HhFesog=
    -----END CERTIFICATE-----
<!--NeedCopy-->
```

Im Folgenden finden Sie einen Abschnitt INTERMEDIATE CA CERTIFICATE:


```
    Bag Attributes: <Empty Attributes>
    subject=/DC=lan/DC=food/CN=hotdog
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIESDCCAzCgAwIBAgIQah20fCRYTY9LRXYMIRaKGjANBgkqhkiG9w0BAQUFADA8


    ... (more random characters)
       Nt0nksawDnbKo86rQcNnY5xUs7c7pj2zxj/IOsgNHUp5W6dDI9pQoqFFaDk
       =

    -----END CERTIFICATE-----
<!--NeedCopy-->
```

Je nach Zertifizierungspfad des exportierten Zertifikats können weitere Zwischenzertifikate folgen.

5. Öffnen Sie die PEM-Datei in einem Texteditor
6. Suchen Sie die erste Zeile der PEM-Datei und die erste Instanz der folgenden Zeile und kopieren Sie diese beiden Zeilen und alle Zeilen dazwischen:

```
-----END CERTIFICATE-----

Note: Make sure that last copied line is the first
-----END CERTIFICATE----- line in the .PEM file.

<!--NeedCopy-->
```

7. Fügen Sie die kopierten Zeilen in eine neue Datei ein. Nennen Sie die neue Datei etwas Intuitives wie cert-key.pem. Dieses Zertifikatschlüsselpaar ist für den Server, der den HTTPS-Dienst hostet. Diese Datei muss sowohl den Abschnitt mit der Bezeichnung RSA PRIVATE KEY als auch den Abschnitt mit der Bezeichnung SERVERZERTIFIKAT im vorherigen Beispiel enthalten.

   Hinweis: Die Zertifikatschlüsselpaardatei enthält den privaten Schlüssel und muss sicher aufbewahrt werden.

8. Suchen Sie alle nachfolgenden Abschnitte, die mit —BEGIN CERTIFICATE— beginnen und mit —END CERTIFICATE— enden, und kopieren Sie jeden dieser Abschnitt in eine separate neue Datei.

   Diese Abschnitte entsprechen Zertifikaten vertrauenswürdiger Zertifizierungsstellen, die in den Zertifizierungspfad aufgenommen wurden. Diese Abschnitte müssen kopiert und in neue einzelne Dateien für diese Zertifikate eingefügt werden. Beispielsweise muss der Abschnitt INTERMEDIATE CA CERTIFICATE des vorherigen Beispiels kopiert und in eine neue Datei eingefügt werden).

Erstellen Sie für mehrere Zwischenzertifizierungsstellenzertifikate in der Originaldatei Dateien für jedes Zwischenzertifikat in der Reihenfolge, in der sie in der Datei erscheinen. Behalten Sie (unter Verwendung entsprechender Dateinamen) die Reihenfolge, in der die Zertifikate erscheinen, im Auge, da sie in einem späteren Schritt in der richtigen Reihenfolge miteinander verknüpft werden müssen.

9. Kopieren Sie die Zertifikatschlüsseldatei (cert-key.pem) und alle zusätzlichen Zertifizierungsstellen-Zertifikatdateien in das Verzeichnis /nsconfig/ssl auf der NetScaler-Appliance.
10. Beenden Sie die BSD-Shell und greifen Sie auf die NetScaler-Eingabeaufforderung zu.
11. Folgen Sie den Schritten unter "Installieren Sie die Zertifikatschlüsseldateien auf der Appliance", um den Schlüssel/das Zertifikat nach dem Hochladen auf das Gerät zu installieren.

Wie konvertiere ich das PKCS #7 -Zertifikat und installiere es auf der NetScaler-Appliance?

Sie können OpenSSL verwenden, um ein PKCS #7 -Zertifikat in ein Format zu konvertieren, das von der NetScaler-Appliance erkennbar ist. Die Prozedur ist identisch mit der Prozedur für PKCS #12 -Zertifikate, außer dass Sie OpenSSL mit verschiedenen Parametern aufrufen. Die Schritte zum Konvertieren von PKCS #7 -Zertifikaten lauten wie folgt:

1. Kopieren Sie das Zertifikat mithilfe eines sicheren Kopierdienstprogramms wie SCP auf die Appliance.
2. Konvertieren Sie das Zertifikat (z. B. cert.P7B) in das PEM-Format:

```
1 openssl pkcs7 -inform DER -in cert.p7b -print_certs -text -out
     cert.pem
2 <!--NeedCopy-->
```

3. Folgen Sie den Schritten 3 bis 7, wie in der Antwort für PKCS #12 -Zertifikate beschrieben.
   Hinweis: Bevor Sie das konvertierte PKCS #7 -Zertifikat auf die Appliance laden, überprüfen Sie, ob es einen privaten Schlüssel enthält, genau wie in Schritt 3 für die PKCS #12 -Prozedur beschrieben. PKCS #7 -Zertifikate, insbesondere die aus IIS exportierten Zertifikate, enthalten normalerweise keinen privaten Schlüssel.

Wenn ich eine Chiffre mithilfe des Befehls bind cipher an einen virtuellen Server oder Dienst binde, sehe ich die Fehlermeldung "Befehl veraltet. "?

Der Befehl zum Binden einer Chiffre an einen virtuellen Server oder Dienst hat sich geändert.

Binden Sie eine SSL-Chiffre mit dem Befehl `bind ssl vserver <vsername> -ciphername <ciphername>` an einen virtuellen SSL-Server.

Verwenden Sie den Befehl `bind ssl service <serviceName> -ciphername <ciphername>`, um eine SSL-Chiffre an einen SSL-Dienst zu binden.

Hinweis: Neue Chiffren und Chiffriergruppen werden zur vorhandenen Liste hinzugefügt und nicht ersetzt.

Warum kann ich keine Chiffriergruppe erstellen und Chiffren mithilfe des Befehls add cipher daran binden?

Die Funktionalität des Befehls "chiffre hinzufügen" hat sich in Release 10 geändert. Der Befehl erstellt nur eine Chiffriergruppe. Um der Gruppe Chiffren hinzuzufügen, verwenden Sie den Befehl bind cipher.

OpenSSL

Wie verwende ich OpenSSL, um Zertifikate zwischen PEM und DER zu konvertieren?

Um OpenSSL verwenden zu können, müssen Sie eine funktionierende Installation der OpenSSL-Software haben und OpenSSL von der Befehlszeile aus ausführen können.

x509-Zertifikate und RSA-Schlüssel können in verschiedenen Formaten gespeichert werden.

Zwei gängige Formate sind:

- DER (ein Binärformat, das hauptsächlich von Java- und Macintosh-Plattformen verwendet wird)
- PEM (eine base64-Darstellung von DER mit Kopf- und Fußzeileninformationen, die hauptsächlich von UNIX- und Linux-Plattformen verwendet wird).

Ein Schlüssel und das entsprechende Zertifikat können zusätzlich zum Root- und Zwischenzertifikaten auch in einer einzigen PKCS #12 (.P12, .PFX) -Datei gespeichert werden.

Prozedur

Verwenden Sie den **OpenSSL-Befehl**, um wie folgt zwischen Formaten zu konvertieren:

1. So konvertieren Sie ein Zertifikat von PEM in DER:

```
x509 -in input.crt -inform PEM -out output.crt -outform DER
<!--NeedCopy-->
```

2. So konvertieren Sie ein Zertifikat von DER in PEM:

```
x509 -in input.crt -inform DER -out output.crt -outform PEM
<!--NeedCopy-->
```

3. So konvertieren Sie einen Schlüssel von PEM in DER:


```
rsa -in input.key -inform PEM -out output.key -outform DER
<!--NeedCopy-->
```

4. So konvertieren Sie einen Schlüssel von DER in PEM:

```
rsa -in input.key -inform DER -out output.key -outform PEM
<!--NeedCopy-->
```

Hinweis: Wenn der Schlüssel, den Sie importieren, mit einer unterstützten symmetrischen Verschlüsselung verschlüsselt ist, werden Sie aufgefordert, die Passphrase einzugeben.

Hinweis: Um einen Schlüssel in oder aus dem veralteten NET-Format (Netscape-Server) zu konvertieren, ersetzen Sie NET gegebenenfalls durch PEM oder DER. Der gespeicherte Schlüssel ist in einer schwachen, ungesalzenen symmetrischen RC4-Verschlüsselung verschlüsselt, sodass eine Passphrase angefordert wird. Eine leere Passphrase ist zulässig.

Grenzwerte des Systems

Welche wichtigen Zahlen sollten Sie sich merken?

1. Zertifikatanforderung erstellen:
   - Dateiname anfordern: Maximal 63 Zeichen
   - Name der Schlüsseldatei: Maximal 63 Zeichen
   - PEM-Passphrase (für verschlüsselten Schlüssel): Maximal 31 Zeichen
   - Allgemeiner Name: Maximal 63 Zeichen
   - Stadt: Maximal 127 Zeichen
   - Name der Organisation: Maximal 63 Zeichen
   - Bundesland/Provinz Name: Maximal 63 Zeichen
   - E-Mail-Adresse: Maximal 255 Zeichen
   - Organisationseinheit: Maximal 63 Zeichen
   - Challenge Password: Maximal 20 Zeichen
   - Firmenname: Maximal 127 Zeichen
2. Zertifikat erstellen:
   - Dateiname des Zertifikats: Maximal 63 Zeichen
   - Dateiname der Zertifikatanforderung: Maximal 63 Zeichen
   - Name der Schlüsseldatei: Maximal 63 Zeichen
   - PEM-Passphrase: Maximal 31 Zeichen
   - Gültigkeitszeitraum: Maximal 3650 Tage
   - Dateiname des CA-Zertifikats: Maximal 63 Zeichen
   - Name der CA-Schlüsseldatei: Maximal 63 Zeichen

- PEM-Passphrase: Maximal 31 Zeichen
- CA-Seriennummerndatei: Maximal 63 Zeichen

3. Erstellen und installieren Sie ein Server-Testzertifikat:
   - Dateiname des Zertifikats: Maximal 31 Zeichen
   - Vollqualifizierter Domainname: Maximal 63 Zeichen
4. Erstellen Sie Diffie-Hellman (DH) Schlüssel:
   - DH-Dateiname (mit Pfad): Maximal 63 Zeichen
   - DH-Parametergröße: Maximal 2048 Bit
5. PKCS12-Schlüssel importieren:
   - Ausgabedateiname: Maximal 63 Zeichen
   - PKCS12 Dateiname: Maximal 63 Zeichen
   - Kennwort importieren: Maximal 31 Zeichen
   - PEM-Passphrase: Maximal 31 Zeichen
   - Überprüfen der PEM-Passphrase: Maximal 31 Zeichen
6. Exportieren PKCS12
   - PKCS12 Dateiname: Maximal 63 Zeichen
   - Dateiname des Zertifikats: Maximal 63 Zeichen
   - Name der Schlüsseldatei: Maximal 63 Zeichen
   - Kennwort exportieren: Maximal 31 Zeichen
   - PEM-Passphrase: Maximal 31 Zeichen
7. CRL-Verwaltung:
   - Dateiname des CA-Zertifikats: Maximal 63 Zeichen
   - Name der CA-Schlüsseldatei: Maximal 63 Zeichen
   - CA-Schlüsseldatei-Kennwort: Maximal 31 Zeichen
   - Indexdateiname: Maximal 63 Zeichen
   - Dateiname des Zertifikats: Maximal 63 Zeichen
8. RSA-Schlüssel erstellen:
   - Name der Schlüsseldatei: Maximal 63 Zeichen
   - Schlüsselgröße: Maximal 4096 Bit
   - PEM-Passphrase: Maximal 31 Zeichen
   - Passphrase überprüfen: Maximal 31 Zeichen
9. Ändern Sie erweiterte SSL-Einstellungen:
   - Maximale CRL-Speichergröße: Maximal 1024 Mbyte
   - Timeout für Verschlüsselungsauslöser (10 mS-Ticks): Maximal 200
   - Paketanzahl der Verschlüsselung: Maximal 50

- OCSP-Cachegröße: Maximal 512 Mbyte

10. Zertifikat installieren:
    - Name des Zertifikatschlüsselpaars: Maximal 31 Zeichen
    - Dateiname des Zertifikats: Maximal 63 Zeichen
    - Dateiname des privaten Schlüssels: Maximal 63 Zeichen
    - Kennwort: Maximal 31 Zeichen
    - Benachrichtigungszeitraum: Maximal 100
11. Chiffriergruppe erstellen:
    - Name der Chiffriergruppe: Maximal 39 Zeichen
12. CRL erstellen:
    - CRL-Name: Maximal 31 Zeichen
    - CRL-Datei: Maximal 63 Zeichen
    - URL: Maximal 127 Zeichen
    - Basis-DN: Maximal 127 Zeichen
    - Bind DN: Maximal 127 Zeichen
    - Kennwort: Maximal 31 Zeichen
    - Tage: Maximal 31
13. Erstellen Sie SSL-Richtlinie:
    - Name: Maximal 127 Zeichen
14. SSL-Aktion erstellen:
    - Name: Maximal 127 Zeichen
15. Erstellen Sie OCSP-Responder:
    - Name: Maximal 32 Zeichen
    - URL: Maximal 128 Zeichen
    - Batchtiefe: Maximal 8
    - Batching-Verzögerung: Maximal 10000
    - Produziert bei Time Skew: Maximal 86400
    - Timeout anfordern: Maximum120000
16. Virtuellen Server erstellen:
    - Name: Maximal 127 Zeichen
    - Umleitungs-URL: Maximal 127 Zeichen
    - Client-Timeout: Maximal 31536000 Sekunden
17. Service erstellen:
    - Name: Maximal 127 Zeichen

- Timeout im Leerlauf (Sekunden):
  Client: Maximal 31536000
  Server: Maximal 31536000

18. Dienstgruppe erstellen:
    - Dienstgruppenname: Maximal 127 Zeichen
    - Server-ID: Maximal 4294967295
    - Timeout im Leerlauf (Sekunden):
      Client: Maximalwert 31536000
      Server: Maximal 31536000
19. Monitor erstellen:
    - Name: Maximal 31 Zeichen
20. Server erstellen:
    - Servername: Maximal 127 Zeichen
    - Domainname: Maximal 255 Zeichen
    - Wiederholung auflösen: Maximal 20939 Sekunden

Prüfung des Inhalts

May 11, 2023

In jüngster Zeit wurden die Gerätetypen erweitert, um verschiedene Multimediainhalte anzuzeigen. Bei den Gerätetypen kann es sich um Mobiltelefone, Tablets und Desktops handeln. Anbieter von Zwischeninfrastrukturen müssen den Originalinhalt von einem Webserver in ein Format umwandeln, das für das Gerät geeignet ist, das den Inhalt anfordert. Die externen Geräte überprüfen den Inhalt, der transkodiert wird, und senden ihn an den Client zurück. Das häufig verwendete Protokoll, um dies zu erreichen, ist ICAP. ICAP ermöglicht den Einsatz der NetScaler-Appliance in verschiedenen Bereitstellungen. ICAP verwendet die Technik zur Inhaltsinspektion, bei der Daten auf Malware und Sicherheitsprobleme untersucht werden.

> **Hinweis**
>
> HTTP/2 ist nicht mit der Inhaltsüberprüfung kompatibel. Die Anwendungen, die HTTP/2 verwenden, funktionieren möglicherweise nicht richtig, wenn der Datenverkehr der Inhaltsüberprüfung unterzogen wird.

ICAP für Remote-Content-Inspektion

May 11, 2023

Das Internet Content Adaptation Protocol (ICAP) ist ein einfaches, schlankes Protokoll für die Ausführung des Value Added Transformation Service für HTTP-Nachrichten. In einem typischen Szenario leitet ein ICAP-Client HTTP-Anfragen und -Antworten zur Verarbeitung an einen oder mehrere ICAP-Server weiter. Die ICAP-Server führen eine Inhaltstransformation für die Anfragen durch und senden Antworten mit entsprechenden Maßnahmen zurück, um die Anfrage oder Antwort zu bearbeiten.

ICAP auf einer NetScaler-Appliance

In einem NetScaler-Setup fungiert die Appliance als ICAP-Client, der mit ICAP-Servern von Drittanbietern (wie Antimalware und Data Loss Protection (DLP)) interagiert. Wenn die Appliance einen eingehenden Web-Traffic empfängt, fängt die Appliance den Datenverkehr ab und bewertet anhand einer Content Inspection-Richtlinie, ob die HTTP-Anfrage eine ICAP-Verarbeitung benötigt. Falls ja, entschlüsselt die Appliance die Nachricht und sendet sie als Klartext an die ICAP-Server. Die ICAP-Server führen den Content Transformation Service für die Anforderungsnachricht aus und senden eine Antwort an die Appliance zurück. Die angepassten Nachrichten können entweder eine HTTP-Anfrage oder eine HTTP-Antwort sein. Wenn die Appliance mit mehreren ICAP-Servern zusammenarbeitet, führt die Appliance einen Lastenausgleich der ICAP-Server durch. Dieses Szenario tritt auf, wenn ein ICAP-Server nicht ausreicht, um die gesamte Verkehrslast zu bewältigen. Sobald die ICAP-Server eine geänderte Nachricht zurückgeben, leitet die Appliance die geänderte Nachricht an den Back-End-Ursprungsserver weiter.

Die NetScaler-Appliance bietet auch einen sicheren ICAP-Dienst, wenn es sich bei dem eingehenden Datenverkehr um einen HTTPS-Typ handelt. Die Appliance verwendet einen SSL-basierten TCP-Dienst, um eine sichere Verbindung zwischen der Appliance und den ICAP-Servern herzustellen.

So funktioniert die ICAP-Anforderungsänderung (REQMOD)

Im Modus zur Anforderungsänderung (REQMOD) leitet die NetScaler-Appliance die vom Client empfangene HTTP-Anfrage an den ICAP-Server weiter. Der ICAP-Server führt dann einen der folgenden Schritte aus:

1. Sendet eine modifizierte Version der Anfrage zurück und die Appliance wiederum sendet die geänderte Anfrage an den Back-End-Ursprungsserver oder leitet die geänderte Anfrage an einen anderen ICAP-Server weiter.
2. Antwortet mit einer Meldung, dass keine Anpassung erforderlich ist.
3. Gibt einen Fehler zurück und die Appliance sendet die Fehlermeldung wiederum an den Benutzer zurück.

So funktioniert die ICAP-Antwortmodifikation (RESPMOD)

Im Antwortmodifikationsmodus (RESPMOD) sendet die NetScaler-Appliance eine HTTP-Antwort an den ICAP-Server (die von der Appliance gesendete Antwort ist in der Regel die vom Originalserver gesendete Antwort). Der ICAP-Server führt dann einen der folgenden Schritte aus:

1. Sendet eine modifizierte Version der Antwort und die Appliance wiederum sendet die Antwort an den Benutzer oder leitet die Antwort an einen anderen ICAP-Server weiter.
2. Antwortet mit einer Meldung, dass keine Anpassung erforderlich ist.
3. Gibt einen Fehler zurück und die Appliance sendet wiederum die Fehlermeldung an den Benutzer.

ICAP-Lizenz

Die ICAP-Funktion funktioniert in einem eigenständigen NetScaler-Setup oder einem Hochverfügbarkeits-Setup mit NetScaler Premium- oder Advanced-Lizenzedition.

ICAP für den Content Transformation Service konfigurieren

Um ICAP für den Content Transformation Service verwenden zu können, müssen Sie zunächst die Funktionen Inhaltsinspektion und Load Balancing aktivieren. Sobald Sie die Funktionen aktiviert haben, können Sie die folgenden Aufgaben ausführen

Um die Inhaltsinspektion zu aktivieren

Wenn Sie möchten, dass die NetScaler-Appliance als ICAP-Client fungiert, müssen Sie zunächst die Funktionen Content Inspection und Load Balancing aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature contentInspection LoadBalancing
<!--NeedCopy-->
```

ICAP-Profil hinzufügen

ICAP-Konfigurationen für eine NetScaler-Appliance werden in einer Entität spezifiziert, die als ICAP-Profil bezeichnet wird. Das Profil enthält eine Sammlung der ICAP-Einstellungen. Zu den Einstellungen gehören Parameter zum dynamischen Generieren einer ICAP-Anfrage, zum Empfangen der ICAP-Antwort und zur Protokollierung von Inhaltsinspektionsdaten.

Um eine ICAP-Anfrage an den ICAP-Server dynamisch zu generieren, wird dem ICAP-Profil ein neuer Parameter “insertHttpRequest” hinzugefügt. Wenn dieser Parameter konfiguriert ist, verwendet

die Appliance den konfigurierten Wert als Richtlinienausdruck und wertet den Ausdruck aus und schließt das Ergebnis als gekapselte HTTP-Anfrage oder -Antwort ein und sendet es dann an den ICAP-Server. Außerdem ist ein neuer Parameter “insertiCapHeaders” konfigurierbar, um die ICAP-Header dynamisch auszuwerten und einzubeziehen.

Wenn die Appliance eine ICAP-Anforderung sendet und keine Antwort vom ICAP-Server erhält, reagiert die Verbindung nicht mehr. Dies geschieht so lange, bis der ICAP-Server eine Antwort sendet oder eine Sitzung freigegeben wird. Das Verhalten kann behandelt werden, indem die ICAP-Antwort-Timeout-Option konfiguriert wird. Sie können einen Parameter für das Anforderungs-Timeout festlegen, damit bei einer verzögerten ICAP-Antwort eine Aktion ausgeführt werden kann. Wenn die NetScaler-Appliance innerhalb des konfigurierten Anforderungs-Timeouts keine Antwort erhält, wird die Anforderungs-Timeout-Aktion ausgeführt.

reqTimeoutAction: Mögliche Werte sind BYPASS, RESET, DROP.
BYPASS: Dadurch wird die Antwort des Remote-ICAP-Servers ignoriert und die Anforderung/Antwort an den Client/Server gesendet.
RESET (Standard): Setzt die Client-Verbindung zurück, indem Sie sie schließen.
DROP: Löscht die Anfrage, ohne dem Benutzer eine Antwort zu senden

Um eine ICAP-Antwort auszuwerten, wird ein neuer Richtlinienausdruck `ICAP.RES` im Callout-Rückgabeausdruck für die Inhaltsüberprüfung verwendet. Dieser Ausdruck wertet die ICAP-Antwort ähnlich dem Ausdruck `HTTP.RES` in `HTTP_CALLOUT`.

Wenn eine NetScaler-Appliance beispielsweise eine HTTP-Anfrage für einen Dienst empfängt, der hinter der virtuellen NetScaler-IP-Adresse gehostet wird, muss die Appliance möglicherweise die Authentifizierung des Clients bei einem externen Server überprüfen und eine Aktion ergreifen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns icapProfile <name> [-preview ( ENABLED | DISABLED )][-previewLength
 <positive_integer>] -uri <string> [-hostHeader <string>] [-userAgent <
string>] -Mode ( REQMOD | RESPMOD )[-queryParams <string>] [-connectionKeepAlive
 ( ENABLED | DISABLED )][-allow204 ( ENABLED | DISABLED )] [-insertICAPHeaders
 <string>][-insertHTTPRequest <string>] [-reqTimeout <positive_integer>][-
reqTimeoutAction <reqTimeoutAction>] [-logAction <string>]
```

Beispiel:

```
add icapprofile reqmod-profile -mode RESPMOD -uri  “/req_scan”  -hostHeader
 “Webroot.reqsca”  -useragent  “NS_SWG-Proxy”
```

```
add ns icapProfile icap_prof1 -uri "/example"-Mode REQMOD -reqtimeout 4 -
reqtimeoutaction BYPASS
```

```
> add icapProfile reqmode-profile -uri '/example'-mode REQMOD -insertHTTPRequest
 q{ HTTP.REQ.METHOD + ""+ HTTP.REQ.URL + "HTTP/1.1\r\n"+ "Host: "+ HTTP.REQ
```



```
.HOSTNAME + "\r\n\r\n"}
```

Aktion zur ICAP-Inhaltsinspektion protokollieren

Um dynamisch Log-Stream-Datensätze für die Inhaltsinspektion oder SYSLOG-Logs zu generieren, können Sie den auf ICAP.RES basierenden Richtlinienausdruck für die ICAP-Antwort verwenden. Dieser Parameter kann im ICAP-Profil konfiguriert werden, um den Richtlinienausdruck für die Generierung der dynamischen Protokolldatensätze zu konfigurieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add audit messageaction icap_log_expr INFORMATIONAL icap.res.full_header

set icapProfile reqmode-profile -logAction messageaction
```

ICAP-Dienst als TCP- oder SSL_TCP-Dienst hinzufügen

Nachdem Sie die Content Inspection-Funktion aktiviert haben, müssen Sie einen ICAP-Dienst für die ICAP-Server hinzufügen, der Teil des Load-Balancing-Setups sein wird. Der Dienst, den Sie hinzufügen, stellt die ICAP-Verbindung zwischen der NetScaler-Appliance und virtuellen Lastausgleichsservern bereit.

Hinweis: Als Administrator können Sie in der Aktion Content Inspection einen ICAP-Dienst hinzufügen und die IP-Adresse des ICAP-Servers direkt konfigurieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add service <name> <IP> <serviceType> <port>
2 <!--NeedCopy-->
```

Beispiel:

```
add service icapsv1 10.10.10.10 SSL_TCP 1345

add service icapsv2 10.10.10.11 SSL_TCP 1345
```

Fügen Sie einen auf TCP oder SSL_TCP basierenden virtuellen Lastausgleichsserver hinzu

Nachdem Sie einen ICAP-Dienst erstellt haben, müssen Sie einen virtuellen Server erstellen, der ICAP-Verkehr akzeptiert und die ICAP-Server lastenausgleicht.

> **Hinweis:**
>
> Sie können auch einen SSL-basierten TCP-Dienst über einen gesicherten Kanal verwenden. Sie verwenden einen SSL_TCP-Dienst und binden sich an die Content Inspection-Aktion.

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add lb vserver <name> <serviceType> <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vicap TCP 0.0.0.0 - persistenceType NONE -cltTimeout
    9000

add lb vserver vicap SSL_TCP 0.0.0.0 0 - persistenceType NONE -
    cltTimeout 9000
<!--NeedCopy-->
```

Binden Sie den ICAP-Dienst an den virtuellen Load-Balancing-Server

Nachdem Sie einen ICAP-Dienst und einen virtuellen Server erstellt haben, müssen Sie den ICAP-Dienst an den virtuellen Server binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver vicap icapsv1
<!--NeedCopy-->
```

Aktion zur Inhaltsinspektion hinzufügen

Nachdem Sie die Funktion zur Inhaltsinspektion aktiviert haben, müssen Sie eine ICAP-Aktion für die Verarbeitung der ICAP-Anforderungsinformationen hinzufügen. Das ICAP-Profil und die Dienste oder der virtuelle Lastausgleichsserver, die erstellt werden, sind an die ICAP-Aktion gebunden. Wenn der ICAP-Server ausgefallen ist, können Sie den Parameter `ifserverdown` für die Appliance so konfigurieren, dass er eine der folgenden Aktionen ausführt.

CONTINUE: Wenn der Benutzer die Inhaltsüberprüfung Bypass möchte, wenn der Remoteserver ausgefallen ist, können Sie standardmäßig die Aktion “WEITER” wählen.
RESET (Standard): Diese Aktion reagiert auf den Client, indem sie die Verbindung mit RST schließt.
DROP: Diese Aktion löscht die Pakete im Hintergrund, ohne eine Antwort an den Benutzer zu senden.

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add contentInspection action <name> -type ICAP -serverName <string> -
    icapProfileName <string>

add ContentInspection action <name> -type ICAP -serverip <ip> -
    serverport <port> -icapProfileName <string>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie den ICAP-Dienst anstelle eines virtuellen Lastausgleichsservers konfigurieren können, können Sie den Dienstnamen in der Option \<-serverip> angeben. Beim Hinzufügen der Content Inspection-Aktion wird der TCP-Dienst automatisch für die angegebene IP-Adresse mit Port 1344 erstellt und für die ICAP-Kommunikation verwendet.

Beispiel:

```
add ContentInspection action ci_act_lb -type ICAP -serverName vicap -
    icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverName icapsv1
    -icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverip 1.1.1.1 -
    serverport 1344 -icapProfileName icap_reqmod
<!--NeedCopy-->
```

Richtlinien zur Inhaltsinspektion hinzufügen

Nachdem Sie eine Aktion zur Inhaltsinspektion erstellt haben, müssen Sie Richtlinien zur Inhaltsinspektion erstellen, um Anfragen zur ICAP-Verarbeitung und Prüfprotokollierung zu bewerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Regel ist mit der Aktion zur Inhaltsinspektion verknüpft, die verknüpft wird, wenn eine Anforderung der Regel entspricht.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Beispiel:

```
add ContentInspection policy ci_pol_basic  - rule true  - action
    ci_act_svc

```



```
3 add ContentInspection policy ci_pol_HTTP  -rule HTTP.REQ.URL.CONTAINS(
      "html" )  -action ci_act_svc
4 <!--NeedCopy-->
```

Binden Sie Richtlinien zur Inhaltsinspektion an den virtuellen Content Switching- oder Load-Balancing-Server

Um eine ICAP-Richtlinie in Kraft zu setzen, müssen Sie sie global binden oder sie an einen virtuellen Content Switching- oder Load Balancing-Server binden, der die Anwendung als Frontend nutzt. Wenn Sie die Richtlinie binden, müssen Sie ihr eine Priorität zuweisen. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden.

> **Hinweis:**
>
> Der virtuelle Anwendungsserver muss vom Typ HTTP/SSL/CS-PROXY sein.

Informationen zum Konfigurieren eines Load Balancing-Setups für die Weiterleitung des Datenverkehrs an den Back-End-Ursprungsserver nach der Inhaltstransformation finden Sie unter Load Balancing.

Konfigurieren des sicheren ICAP-Dienstes

Um eine sichere Verbindung zwischen der NetScaler-Appliance und den ICAP-Webservern herzustellen, verwendet die Appliance einen SSL-basierten TCP-Dienst oder einen virtuellen Lastausgleichsserver, der an eine ICAP-Aktion gebunden ist.

Gehen Sie wie folgt vor, um eine sichere ICAP-Verbindung herzustellen:

1. Fügen Sie einen SSL-basierten TCP-Dienst hinzu.
2. Binden Sie den SSL-basierten TCP-Dienst an einen virtuellen Load-Balancing-Server vom Typ TCP oder SSL_TCP.
3. Binden Sie den SSL-basierten TCP-Dienst oder den virtuellen Lastausgleichsserver an die Content Inspection-Aktion.

Fügen Sie dem virtuellen Load-Balancing-Server einen SSL-basierten TCP-Dienst hinzu

Um eine sichere Verbindung zwischen der NetScaler-Appliance und den ICAP-Webservern herzustellen, verwendet die Appliance einen SSL-basierten TCP-Dienst oder einen virtuellen Lastausgleichsserver, der an eine ICAP-Aktion gebunden ist.

Gehen Sie wie folgt vor, um eine sichere ICAP-Verbindung herzustellen:

1. Fügen Sie einen SSL-basierten TCP-Dienst hinzu.

2. Binden Sie den SSL-basierten TCP-Dienst an einen virtuellen Load-Balancing-Server vom Typ TCP oder SSL_TCP.

Binden Sie den SSL-basierten TCP-Dienst oder den virtuellen Lastausgleichsserver an die Content Inspection-Aktion

Fügen Sie dem virtuellen Load-Balancing-Server einen SSL-basierten TCP-Dienst hinzu

Nachdem Sie die Content Inspection-Funktion aktiviert haben, müssen Sie einen sicheren ICAP-Dienst hinzufügen, der Teil des Load-Balancing-Setups sein wird. Der Dienst, den Sie hinzufügen, stellt eine sichere ICAP-Verbindung zwischen der NetScaler-Appliance und virtuellen Lastausgleichsservern bereit.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add service <name> <IP> <serviceType> <port>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add service icapsv2 10.102.29.200 SSL_TCP 1344 -gslb NONE -maxclient
     0 -maxReq 0 -cip DISABLED -usip NO -useproxport YES -sp ON -
     cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
2 <!--NeedCopy-->
```

Binden Sie den SSL-basierten TCP-Dienst an den virtuellen SSL_TCP- oder TCP-Load-Balancing-Server

Nachdem Sie einen sicheren ICAP-Dienst erstellt haben, müssen Sie den Dienst an den virtuellen Load-Balancing-Server binden. Es ist erforderlich, wenn Sie einen virtuellen Lastausgleichsserver verwenden, um den Lastenausgleich der ICAP-Server durchzuführen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name> <serviceName>
2 <!--NeedCopy-->
```

Beispiel:

```
1 bind lb vserver vicap icapsv2
2 <!--NeedCopy-->
```


Binden Sie einen SSL-basierten TCP-Dienst oder einen virtuellen Load-Balancing-Server an die Content Inspection-Aktion

Sie fügen eine ICAP-Aktion für die Verarbeitung der ICAP-Anforderungsinformationen hinzu und binden auch den SSL-basierten TCP-Dienst an die Aktion.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection action <name> -type ICAP -serverName <string> -
    icapProfileName <string>
<!--NeedCopy-->
```

Beispiel:

```
add ContentInspection action ci_act_svc -type ICAP -serverName icapsv2
    -icapProfileName icap_reqmod

add ContentInspection action ci_act_svc -type ICAP -serverName vicap -
    icapProfileName icap_reqmod
<!--NeedCopy-->
```

Konfigurieren Sie das ICAP-Protokoll mithilfe der GUI

1. Navigieren Sie zu **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Dienste** die Servicedetails ein.
3. Navigieren Sie zu **Load Balancing** > **Virtuelle Server**. Fügen Sie einen virtuellen Load-Balancing-Server vom Typ HTTP/SSL hinzu. Sie können auch einen virtuellen Server auswählen und auf **Bearbeiten**klicken.
4. Nachdem Sie die grundlegenden Serverdetails eingegeben haben, klicken Sie auf **Weiter**.
5. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf **Richtlinien**.
6. Gehen Sie zum Abschnitt **Richtlinien** und klicken Sie auf das **Stiftsymbol**, um die Richtlinie zur Inhaltsinspektion zu konfigurieren.
7. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
8. Klicken Sie im Abschnitt **Richtlinienbindung** auf **+**, um eine Richtlinie zur Inhaltsinspektion hinzuzufügen.
9. Geben Sie auf der Seite „ **ICAP-Richtlinie erstellen** “ einen Namen für die Richtlinie ein.
10. Klicken Sie im Feld **Aktion** auf das “+” -Zeichen, um eine ICAP-Aktion hinzuzufügen.
11. Geben Sie auf der Seite „ **ICAP-Aktion erstellen** “ einen Namen für die Aktion ein.
12. Geben Sie einen Namen für die Aktion ein.
13. Geben Sie im Feld **Servername** den Namen des bereits erstellten TCP-Dienstes ein.
14. Klicken Sie im Feld **ICAP-Profil** auf das “+” -Zeichen, um ein ICAP-Profil hinzuzufügen.

15. Geben Sie auf der Seite „ **ICAP-Profil erstellen** “ einen Profilnamen, URI und MODE ein.
16. Klicken Sie auf **Erstellen**.
17. Klicken **Sie auf der Seite „ICAP-Aktion** erstellen“ auf **Erstellen**.
18. Geben **Sie auf der Seite ICAP-Richtlinie erstellen** im **Ausdrucks-Editor** “true” ein und klicken Sie dann auf **Erstellen**.
19. Klicken Sie auf **Bind**.
20. Wenn Sie aufgefordert werden, die Funktion zur Inhaltsinspektion zu aktivieren, klicken Sie auf **Ja**.
21. Klicken Sie auf **Fertig**.

Informationen zur NetScaler GUI-Konfiguration für den Lastenausgleich und das Weiterleiten des Datenverkehrs nach der Inhaltstransformation an den Back-End-Ursprungsserver finden Sie unter Load Balancing.

Konfigurieren des gesicherten ICAP-Protokolls mit der GUI

1. Navigieren Sie zu **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Dienste** die Servicedetails ein.
3. Navigieren Sie zu **Load Balancing** > **Virtuelle Server**. Fügen Sie einen virtuellen Server vom Typ HTTP/SSL hinzu. Sie können auch einen virtuellen Server auswählen und auf **Bearbeiten**klicken.
4. Nachdem Sie die grundlegenden Serverdetails eingegeben haben, klicken Sie auf **Weiter**.
5. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf **Richtlinien**.
6. Gehen Sie zum Abschnitt **Richtlinien** und klicken Sie auf das **Stiftsymbol**, um die Richtlinie zur Inhaltsinspektion zu konfigurieren.
7. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
8. Klicken Sie im Abschnitt **Richtlinienbindung** auf **+**, um eine Richtlinie zur Inhaltsinspektion hinzuzufügen.
9. Geben Sie auf der Seite „ **ICAP-Richtlinie erstellen** “ einen Namen für die Richtlinie ein.
10. Klicken Sie im Feld **Aktion** auf das “+” -Zeichen, um eine ICAP-Aktion hinzuzufügen.
11. Geben Sie auf der Seite „ **ICAP-Aktion erstellen** “ einen Namen für die Aktion ein.
12. Geben Sie einen Namen für die Aktion ein.
13. Geben Sie im Feld **Servername** den Namen des bereits erstellten TCP_SSL-Dienstes ein.
14. Klicken Sie im Feld **ICAP-Profil** auf das “+” -Zeichen, um ein ICAP-Profil hinzuzufügen.
15. Geben Sie auf der Seite „ **ICAP-Profil erstellen** “ einen Profilnamen, URI und MODE ein.
16. Klicken Sie auf **Erstellen**.
17. Klicken **Sie auf der Seite „ICAP-Aktion** erstellen“ auf **Erstellen**.
18. Geben **Sie auf der Seite ICAP-Richtlinie erstellen** im **Ausdrucks-Editor** “true” ein und klicken Sie dann auf **Erstellen**.

19. Klicken Sie auf **Bind**.
20. Wenn Sie aufgefordert werden, die Funktion zur Inhaltsinspektion zu aktivieren, klicken Sie auf **Ja**.
21. Klicken Sie auf **Fertig**.

Unterstützung von Auditprotokollen für die Ferninspektion von Inhalten

Wenn eine eingehende Anfrage oder ausgehende Antwort inhaltlich überprüft wird, protokolliert die NetScaler-Appliance die ICAP-Details. Die Appliance speichert die Details als Protokollmeldung in der Datei ns.log.

Jede Protokollnachricht enthält in der Regel die folgenden Details:

```
<Source IP> <Destination IP> <Domain> <ICAP server IP><ICAP Mode> <
   Service URI> <ICAP response> <Policy action>
<!--NeedCopy-->
```

Einschränkung: Der Streaming-Modus der App Firewall wird mit der Funktion zur Inhaltsinspektion nicht unterstützt.

Beispiel für eine Protokollnachricht für eine inhaltsgeprüfte Anforderung:

```
Apr 18 14:45:41 <local0.info> 10.106.97.104 04/18/2018:14:45:41 GMT 0-
   PPE-0 : default CI ICAP_LOG 788 0 : Source 10.102.1.98:39048 -
   Destination 10.106.97.89:8011 - Domain 10.106.97.89 - Content-Type
   application/x-www-form-urlencoded - ICAP Server 10.106.97.99:1344 -
   Mode REQMOD - Service /example - Response 204 - Action FORWARD
<!--NeedCopy-->
```

Beispiel für Content-inspizierte Antwortprotokollmeldung:

```
Apr 18 12:34:08 <local0.info> 10.106.97.104 04/18/2018:12:34:08 GMT 0-
   PPE-0 : default CI ICAP_LOG 71 0 : Source 10.106.97.105:18552 -
   Destination 10.106.97.99:80 - Domain NA - Content-Type NA - ICAP
   Server 10.106.97.99:1344 - Mode RESPMOD - Service /example -
   Response 400 - Action Internal Error
<!--NeedCopy-->
```

Integrierte Geräteintegration mit NetScaler

May 11, 2023

Sicherheitsgeräte wie das Intrusion Prevention System (IPS) und die Next Generation Firewall (NGFW) schützen Server vor Netzwerkangriffen. Diese Geräte werden im Layer-2-Inline-Modus eingesetzt und ihre Hauptfunktion besteht darin, Server vor Netzwerkangriffen zu schützen und Sicherheitsbedrohungen im Netzwerk zu melden.

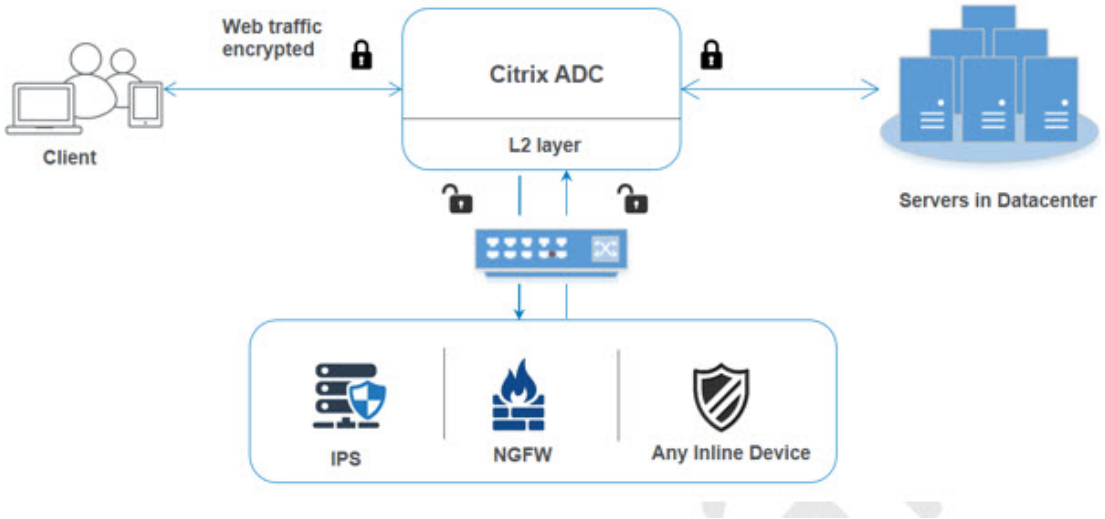
Um anfällige Bedrohungen zu verhindern und erweiterten Sicherheitsschutz zu bieten, ist eine NetScaler-Appliance in ein oder mehrere Inline-Geräte integriert. Bei den Inline-Geräten kann es sich um jedes Sicherheitsgerät wie IPS, NGFW handeln.

Im Folgenden sind einige der Anwendungsfälle aufgeführt, die von der Verwendung der Inline-Geräteintegration mit der NetScaler-Appliance profitieren:

- **Überprüfung des verschlüsselten Datenverkehrs**. Die meisten IPS- und NGFW-Appliances Bypass verschlüsselten Datenverkehr und machen Server dadurch anfällig für Angriffe. Eine NetScaler-Appliance kann den Datenverkehr entschlüsseln und ihn zur Überprüfung an Inline-Geräte senden. Es verbessert die Netzwerksicherheit des Kunden.
- **Entladen von Inline-Geräten von der TLS/SSL-Verarbeitung**. Die TLS/SSL-Verarbeitung ist teuer und das Problem kann zu einer hohen System-CPU in IPS- oder NGFW-Appliances führen, wenn sie den Datenverkehr entschlüsseln. Da der verschlüsselte Datenverkehr schnell zunimmt, können diese Systeme den verschlüsselten Datenverkehr nicht entschlüsseln und überprüfen. NetScaler hilft dabei, Inline-Geräte von der TLS/SSL-Verarbeitung zu trennen. Dies führt dazu, dass das Inline-Gerät ein hohes Volumen an Verkehrsinspektionen unterstützt.
- **Inline-Balancing-Geräte werden geladen**. Die NetScaler-Appliance verteilt den Lastenausgleich mehrerer Inline-Geräte bei hohem Datenverkehrsvolumen.
- **Intelligente Auswahl des Verkehrs**. Jedes Paket, das in die Appliance fließt, kann inhaltlich überprüft werden, z. B. das Herunterladen von Textdateien. Der Benutzer kann die NetScaler-Appliance so konfigurieren, dass sie bestimmten Datenverkehr (z. B. EXE-Dateien) zur Überprüfung auswählt und den Datenverkehr zur Verarbeitung der Daten an Inline-Geräte sendet

Wie der NetScaler in Inline-Geräte integriert ist

Das folgende Diagramm zeigt, wie ein NetScaler in Inline-Sicherheitsgeräte integriert ist.



Wenn Sie Inline-Geräte in die NetScaler-Appliance integrieren, interagiert die Komponente wie folgt:

1. Ein Client sendet eine Anfrage an die NetScaler-Appliance.
2. Die Appliance empfängt die Anfrage und sendet sie auf der Grundlage einer Richtlinienbewertung an ein Inline-Gerät.
   Hinweis: Wenn zwei oder mehr Inline-Geräte vorhanden sind, verteilt die Appliance die Last der Geräte und sendet den Datenverkehr.
   Handelt es sich bei dem eingehenden Datenverkehr um einen verschlüsselten Datenverkehr, entschlüsselt die Appliance die Daten und sendet sie zur Inhaltsüberprüfung als Klartext an das Inline-Gerät.
3. Das Inline-Gerät überprüft die Daten auf Bedrohungen und entscheidet, ob die Daten gelöscht, zurückgesetzt oder an die Appliance zurückgesendet werden sollen.
4. Wenn Sicherheitsbedrohungen bestehen, ändert das Gerät die Daten und sendet sie an die Appliance.
5. Der NetScaler wiederum verschlüsselt die Daten erneut und leitet die Anfrage an den Backend-Server weiter.
6. Der Backend-Server sendet die Antwort an die NetScaler-Appliance.
7. Die Appliance entschlüsselt die Daten erneut und sendet sie zur Überprüfung an das Inline-Gerät.
8. Die Appliance verschlüsselt die Daten erneut und sendet die Antwort an den Client

Softwarelizenzierung

Um die Inline-Gerätintegration bereitzustellen, muss Ihre NetScaler-Appliance mit einer der folgenden Lizenzen ausgestattet sein:

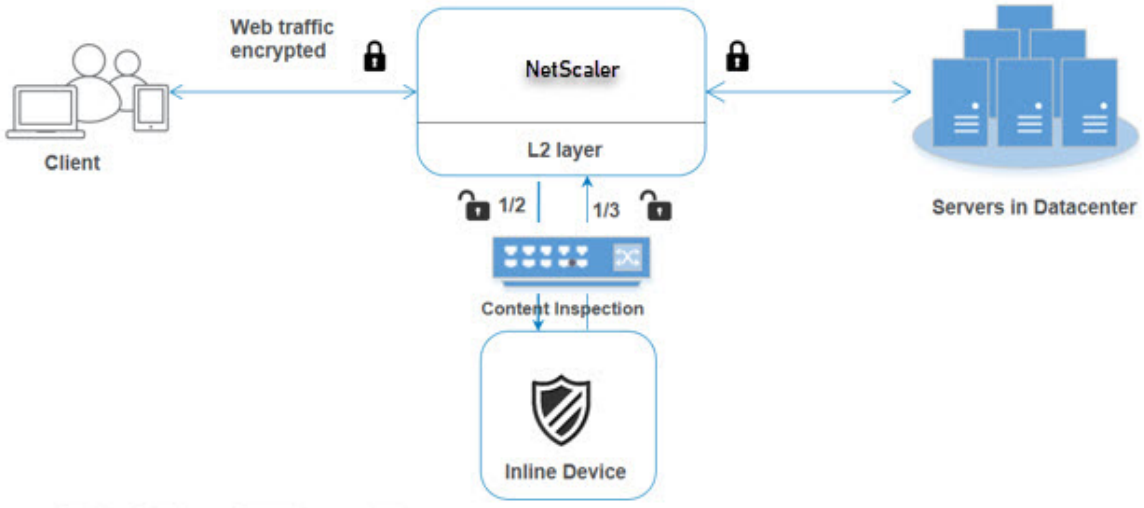
1. ADC Premium
2. ADC Advanced
3. Telco Fortgeschrittene
4. Telco Premium
5. SWG-Lizenz

Konfiguration der integrierten Geräteintegration

Sie können eine NetScaler-Appliance mit einem Inline-Gerät auf drei verschiedene Arten konfigurieren. Die Konfigurationsszenarien lauten wie folgt.

Szenario 1 für die Verwendung eines einzelnen Inline-Geräts

Wenn Sie ein Sicherheitsgerät (IPS oder NGFW) im Inline-Modus integrieren möchten, müssen Sie zunächst die Content Inspection-Funktion aktivieren und den NetScaler in MBF (MAC-basierte Weiterleitung) im globalen Modus aktivieren. Nachdem Sie die Funktionen aktiviert haben, müssen Sie das Content Inspection-Profil und die Aktion Content Inspection für Inline-Geräte hinzufügen, um den Datenverkehr auf der Grundlage der Inspektion zurückzusetzen, zu blockieren oder zu löschen. Fügen Sie dann die Content Inspection-Richtlinie für die Appliance hinzu, um zu entscheiden, welche Teilmenge des Datenverkehrs an die Inline-Geräte gesendet werden soll. Konfigurieren Sie dann den virtuellen Lastausgleichsserver mit aktivierter Layer-2-Verbindung auf dem Server. Binden Sie abschließend die Richtlinie zur Inhaltsinspektion an den virtuellen Load-Balancing-Server.



Aktivieren Sie den MBF-Modus (MAC-basierte Weiterleitung)

Wenn Sie möchten, dass die NetScaler-Appliance in Inline-Geräte wie IPS oder Firewalls integriert wird, müssen Sie diesen Modus aktivieren. Weitere Informationen zu MBF finden Sie im Thema Konfiguration der MAC-basierten Weiterleitung.

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns mode mbf
```

Inhaltsüberprüfung aktivieren

Wenn Sie möchten, dass die NetScaler-Appliance den Inhalt entschlüsselt und dann zur Überprüfung an die Inline-Geräte sendet, müssen Sie die Funktionen Content Inspection und Load Balancing aktivieren.

```
enable ns feature contentInspection LoadBalancing
```

Layer-2-Verbindungsmethode hinzufügen

Um die von Inline-Geräten generierten Antworten zu verarbeiten, verwendet die Appliance den VLAN-Kanal als Layer-2-Methode (L2Conn-Methode) für die Kommunikation mit Inline-Geräten.

Geben Sie in der Befehlszeile Folgendes ein:

```
set l4param -l2ConnMethod <l2ConnMethod>
```

Beispiel

```
set l4param -l2ConnMethod VlanChannel
```

Content Inspection-Profil für Service hinzufügen

Die Inline-Gerätekonfiguration für eine NetScaler-Appliance kann in einer Entität angegeben werden, die als Content Inspection-Profil bezeichnet wird. Das Profil enthält eine Sammlung von Einstellungen, in denen erklärt wird, wie die Integration in ein Inline-Gerät erfolgt.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3”
```


IPS-TCP-Monitor hinzufügen

Wenn Sie Monitore konfigurieren möchten, fügen Sie einen benutzerdefinierten Monitor hinzu.
Hinweis: Wenn Sie Monitore konfigurieren möchten, müssen Sie einen benutzerdefinierten Monitor verwenden. Wenn Sie einen Monitor hinzufügen, müssen Sie den transparenten Parameter aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr>] [-destPort
 <port>] [-transparent ( YES | NO )]
```

Beispiel:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Dienst hinzufügen

Fügen Sie einen Dienst hinzu. Geben Sie eine Schein-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Stellen Sie `use source IP address` (USIP) auf JA ein. Stellen Sie `useproxyport` auf NEIN ein. Standardmäßig ist die Systemüberwachung aktiviert, binden Sie den Dienst an einen Integritätsmonitor und setzen Sie außerdem die Option TRANSPARENT im Monitor auf ON. Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip ON -useproxyport OFF
```

Beispiel:

```
add service ips_service 192.168.10.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

Fügen Sie einen Gesundheitsmonitor hinzu

Standardmäßig ist der Gesundheitsmonitor aktiviert und Sie haben auch die Möglichkeit, ihn bei Bedarf zu deaktivieren. Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent <
YES, NO>
```

Beispiel:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```


Binden Sie den Dienst an den Gesundheitsmonitor

Nach der Konfiguration des Health Monitors müssen Sie den Dienst an den Health Monitor binden. Geben Sie in der Befehlszeile Folgendes ein:

```
bind service <name> -monitorName <name>
```

Beispiel:

```
bind service ips_svc -monitorName ips_tcp
```

Aktion zur Inhaltsinspektion für den Service hinzufügen

Nachdem Sie die Funktion zur Inhaltsinspektion aktiviert und anschließend das Inline-Profil und den Dienst hinzugefügt haben, müssen Sie die Inhaltsinspektionsaktion für die Bearbeitung der Anfrage hinzufügen. Basierend auf der Aktion zur Inhaltsinspektion kann das Inline-Gerät die Aktion beenden, zurücksetzen oder blockieren, nachdem es die Daten überprüft hat.

Wenn der Inline-Server oder -Dienst ausgefallen ist, können Sie den `ifserverdown` Parameter in der Appliance so konfigurieren, dass er eine der folgenden Aktionen ausführt.

CONTINUE: Wenn der Benutzer die Inhaltsüberprüfung Bypass möchte, wenn der Remoteserver ausgefallen ist, können Sie standardmäßig die Aktion “WEITER” wählen.
RESET (Standard): Diese Aktion reagiert auf den Client, indem sie die Verbindung mit RST schließt.
DROP: Diese Aktion löscht die Pakete im Hintergrund, ohne eine Antwort an den Benutzer zu senden.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action <action_name> -type InlineINSPECTION -serverName
 Service_name/Vserver_name>
```

Beispiel:

```
add ContentInspection action <Inline_action> -type InlineSPECTION -serverName
 Inline_service1
```

Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen

Nachdem Sie eine Inhaltsüberprüfungsaktion erstellt haben, müssen Sie Richtlinien für die Inhaltsüberprüfung hinzufügen, um Überprüfungsanfragen zu bewerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Richtlinie bewertet und wählt den zu überprüfenden Verkehr basierend auf der Regel aus.

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL

Um den Webverkehr zu empfangen, müssen Sie einen virtuellen Lastausgleichsserver hinzufügen. Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Beispiel:

```
add lb vserver HTTP_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Binden der Richtlinie zur Inhaltsüberprüfung an den virtuellen Server mit Content Switching oder den virtuellen Lastausgleichsserver vom Typ

Sie binden den virtuellen Load-Balancing-Server oder den virtuellen Content Switching-Server vom Typ HTTP/SSL an die Content Inspection-Richtlinie.
Geben Sie an der Eingabeaufforderung Folgendes ein:

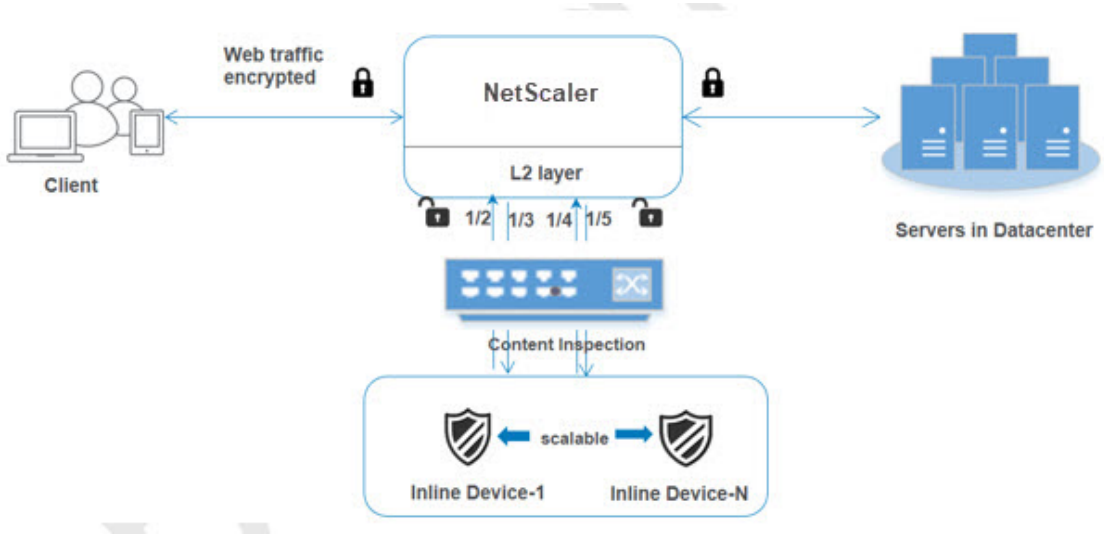
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Beispiel:

```
bind lb vserver HTTP_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Szenario 2: Lastausgleich mehrerer Inline-Geräte mithilfe dedizierter Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, müssen Sie den Lastenausgleich für die Geräte mithilfe verschiedener Inhaltsinspektionsdienste in einem speziellen VLAN-Setup durchführen. In diesem Fall verteilt die NetScaler-Appliance die Geräte und sendet zusätzlich eine Teilmenge des Datenverkehrs über eine dedizierte Schnittstelle an jedes Gerät.
Grundlegende Konfigurationsschritte finden Sie in Szenario 1.



Fügen Sie das Inhaltsprüfprofil1 für Service1 hinzu

Inline-Konfigurationen für eine NetScaler-Appliance können in einer Entität angegeben werden, die als Content Inspection-Profil bezeichnet wird. Das Profil hat eine Sammlung von Geräteeinstellungen. Das Content Inspection Profil1 wurde für Inline-Dienst 1 erstellt und die Kommunikation erfolgt über 1/2 und 1/3 dedizierte Schnittstellen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3”
```

Fügen Sie das Inhaltsprüfprofil2 für Service2 hinzu

Das Content Inspection Profil2 wurde für service2 hinzugefügt und das Inline-Gerät kommuniziert über dedizierte Schnittstellen 1/4 und 1/5 mit der Appliance.
Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface “1/4” -egressInterface “1/5”
```


Dienst 1 für Inline-Gerät 1 hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 1 für das Inline-Gerät 1 hinzufügen, um Teil des Lastausgleichs-Setups zu sein. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_1> -healthmonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service Inline_service1 10.102.29.200 TCP 80 -contentInspectionProfileName
 Inline_profile1 -healthmonitor OFF -usip ON -useproxyport OFF
```

Dienst 2 für Inline-Gerät 2 hinzufügen

Nachdem Sie die Inhaltsinspektionsfunktion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 2 für das Inline-Gerät 2 hinzufügen. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service Inline_service1 10.29.20.205 TCP 80 -contentInspectionProfileName
 Inline_profile2 -healthmonitor OFF -usip ON -useproxyport OFF
```

Virtuellen Lastausgleichsserver hinzufügen

Nachdem Sie das Inline-Profil und die Dienste hinzugefügt haben, müssen Sie einen virtuellen Lastausgleichsserver für den Lastenausgleich der Dienste hinzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <vserver_name> TCP <Pvt_IP3> <port>
```

Beispiel:

```
add lb vserver lb-Inline_vserver TCP *
```

Binden Sie Dienst 1 an den virtuellen Load Balancing-Server

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie nun den virtuellen Lastausgleichsserver an den ersten Dienst.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-Inline_vserver Inline_service1
```

Binden Sie Dienst 2 an den virtuellen Load Balancing-Server

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie den Server nun an den zweiten Dienst.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-Inline_vserver Inline_service2
```

Aktion zur Inhaltsinspektion für den Dienst hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert haben, müssen Sie die Aktion Inhaltsüberprüfung für die Verarbeitung der Inline-Anforderungsinformationen hinzufügen. Basierend auf der ausgewählten Aktion wird das Inline-Gerät gelöscht, zurückgesetzt oder blockiert, nachdem es die angegebene Teilmenge des Datenverkehrs untersucht hat.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action < action_name > -type InlineINSPECTION -
serverName Service_name/Vserver_name>
```

Beispiel:

```
add ContentInspection action Inline_action -type InlineINSPECTION -serverName
 lb-Inline_vserver
```

Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen

Nachdem Sie eine Inhaltsinspektionsaktion erstellt haben, müssen Sie die Inhaltsinspektionsrichtlinie hinzufügen, um Serviceanfragen zu bewerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Regel ist mit der Inhaltsinspektionsaktion verknüpft, die verknüpft wird, wenn eine Anforderung der Regel entspricht.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL

Fügen Sie einen virtuellen Content Switching- oder Lastausgleichsserver hinzu, um Webverkehr zu akzeptieren Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren. Weitere Informationen zum Lastenausgleich finden Sie unter Funktionsweise des Lastenausgleichs .

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Beispiel:

```
add lb vserver http_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Richtlinie zur Inhaltsüberprüfung an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL binden

Sie müssen den virtuellen Content Switching- oder Load Balancing-Server vom Typ HTTP/SSL an die Richtlinie zur Inhaltsüberprüfung binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

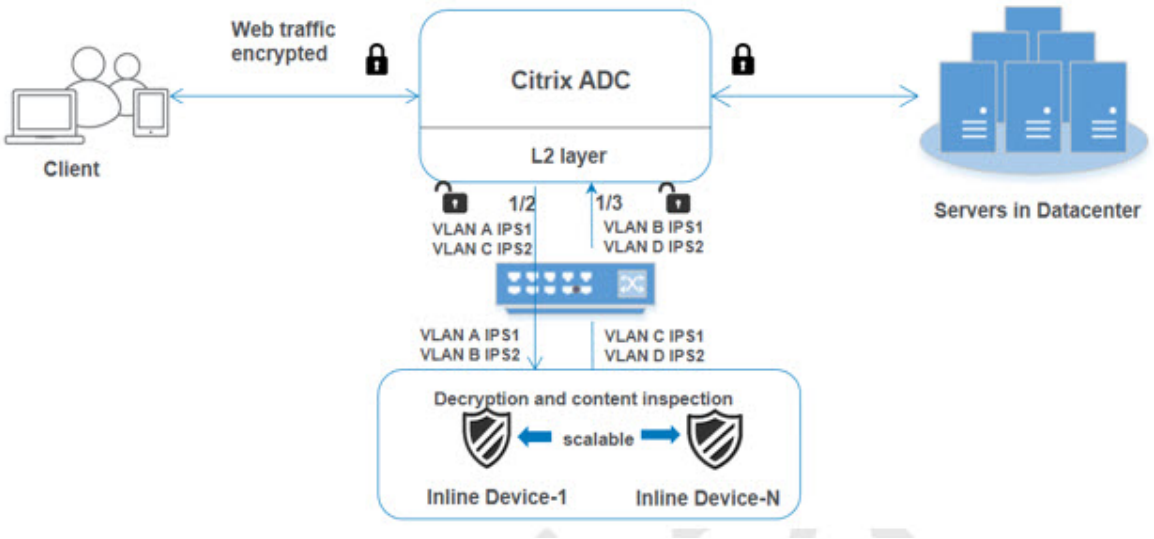
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <L7InlineREQUEST | L4Inline-REQUEST>
```

Beispiel:

```
bind lb vserver http_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```

Szenario 3: Lastausgleich mehrerer Inline-Geräte mithilfe gemeinsam genutzter Schnittstellen

Sie können diese Konfiguration verwenden, wenn Sie mehrere Inline-Geräte verwenden und wenn Sie den Lastenausgleich der Geräte mithilfe verschiedener Dienste in einer gemeinsam genutzten VLAN-Schnittstelle durchführen möchten. Diese Konfiguration mit gemeinsam genutzten VLAN-Schnittstellen ähnelt Anwendungsfall 2. Informationen zur grundlegenden Konfiguration finden Sie in Szenario 2.



Binden Sie VLAN A mit aktivierter Sharing-Option

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 100 -ifnum 1/2 tagged
```

Binden Sie VLAN B mit aktivierter Sharing-Option

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 200 -ifnum 1/3 tagged
```

Binden Sie VLAN C mit aktivierter Sharing-Option

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 300 -ifnum 1/2 tagged
```


Binden Sie VLAN D mit aktivierter Sharing-Option

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 400 -ifnum 1/3 tagged
```

Fügen Sie das Inhaltsprüfprofil1 für Service1 hinzu

Inline-Konfigurationen für eine NetScaler-Appliance können in einer Entität angegeben werden, die als Content Inspection-Profil bezeichnet wird. Das Profil hat eine Sammlung von Geräteeinstellungen. Das Content Inspection-Profil wird für Inline-Dienst 1 erstellt und die Kommunikation erfolgt über 1/2 und 1/3 dedizierte Schnittstellen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3" -egressVlan 100 -ingressVlan
 300
```

Fügen Sie das Inhaltsprüfprofil2 für Service2 hinzu

Das Content Inspection Profil2 wurde für service2 hinzugefügt und das Inline-Gerät kommuniziert über dedizierte Schnittstellen `1/2` und `1/3` mit der Appliance.

Geben Sie in der Befehlszeile Folgendes ein:

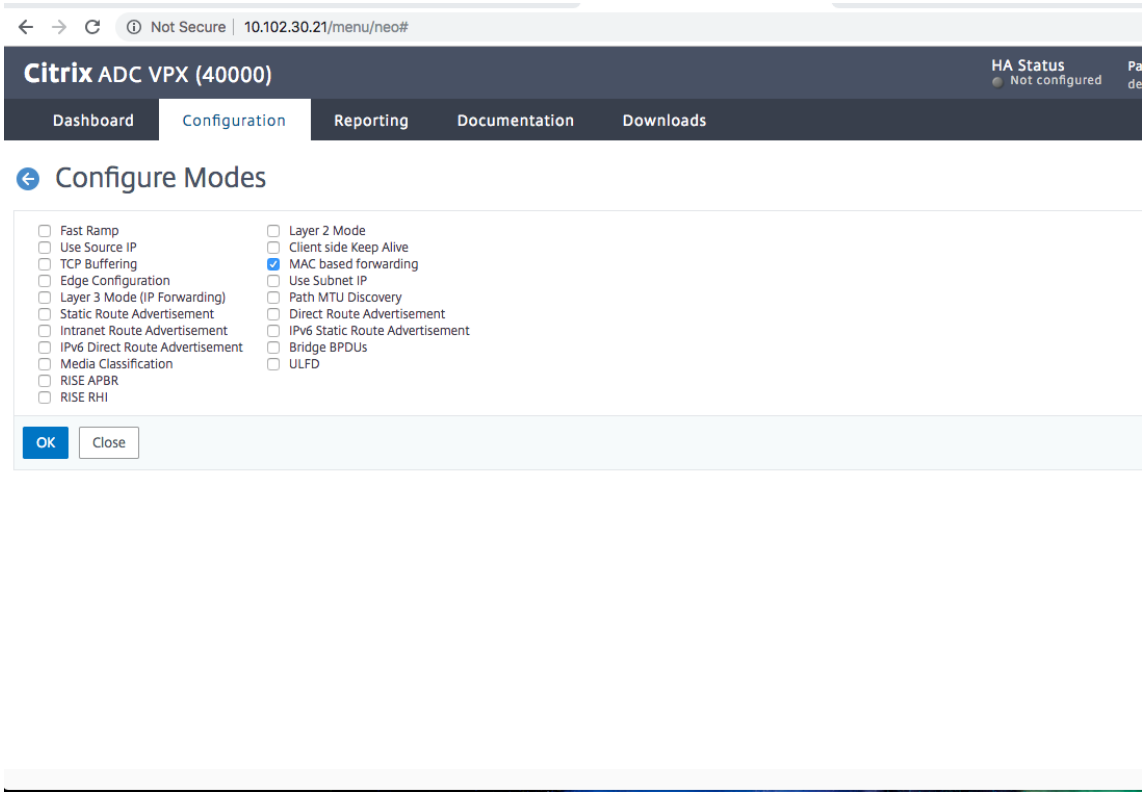
```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

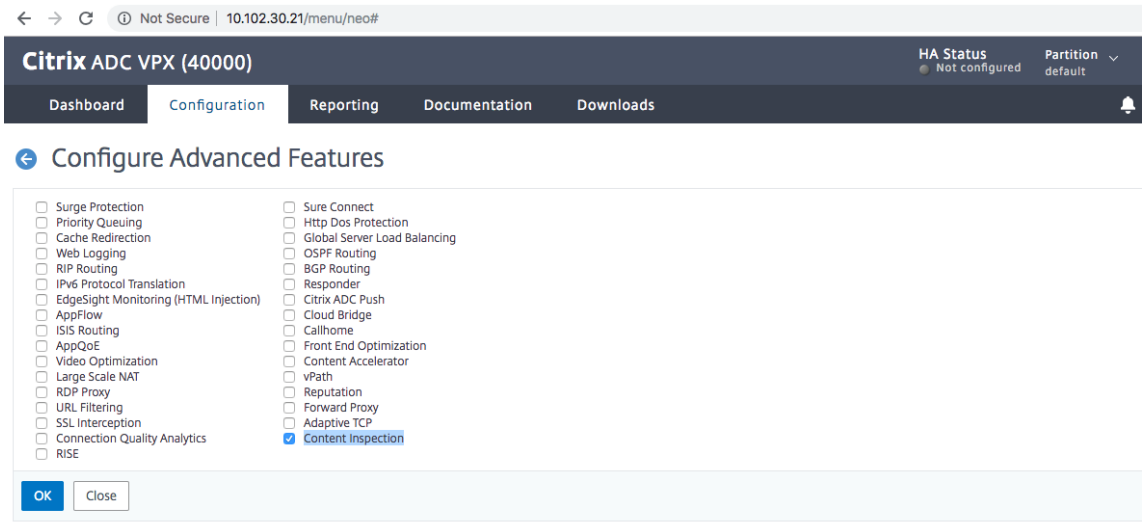
```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3" -egressVlan 200 -ingressVlan
 400
```


Konfigurieren der Inline-Serviceintegration mithilfe der NetScaler GUI

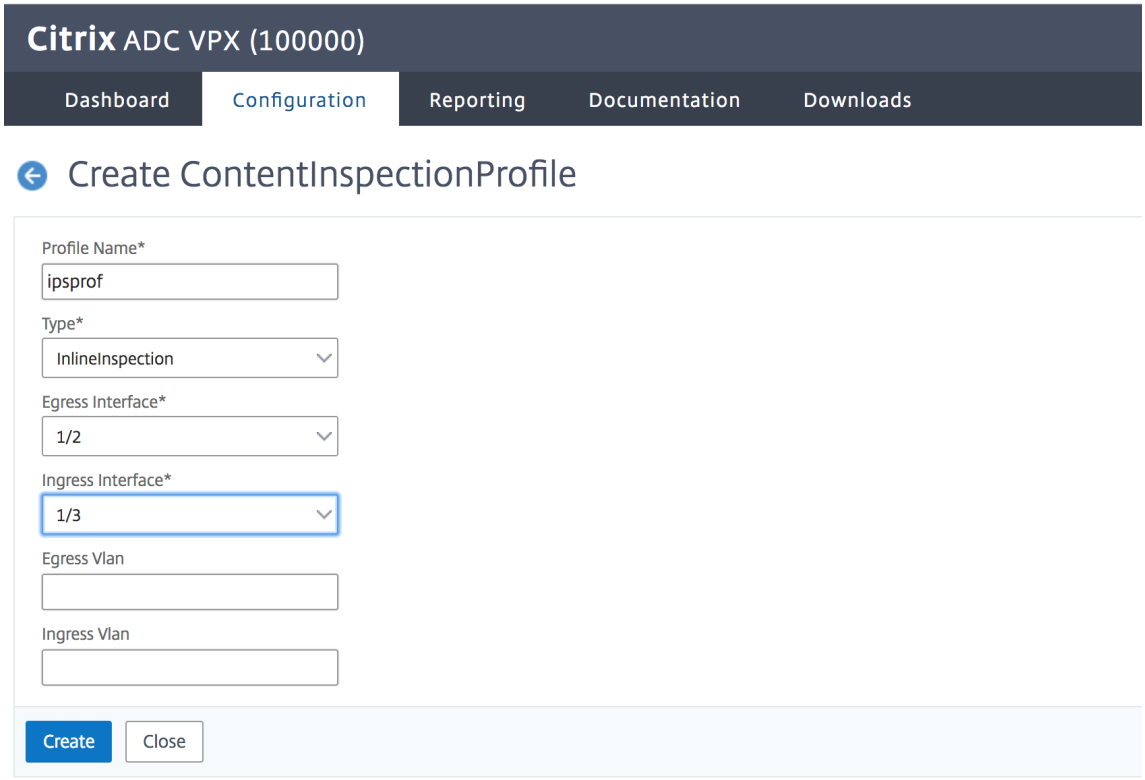
1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zur Registerkarte **Konfiguration** .
2. Navigieren Sie zu **System** > **Einstellungen** > **Modi konfigurieren**.
3. Wählen Sie auf der Seite „ **Modi konfigurieren** “ die Option **Mac Based Forwarding**aus.
4. Klicken Sie auf **OK** und auf **Schließen**.



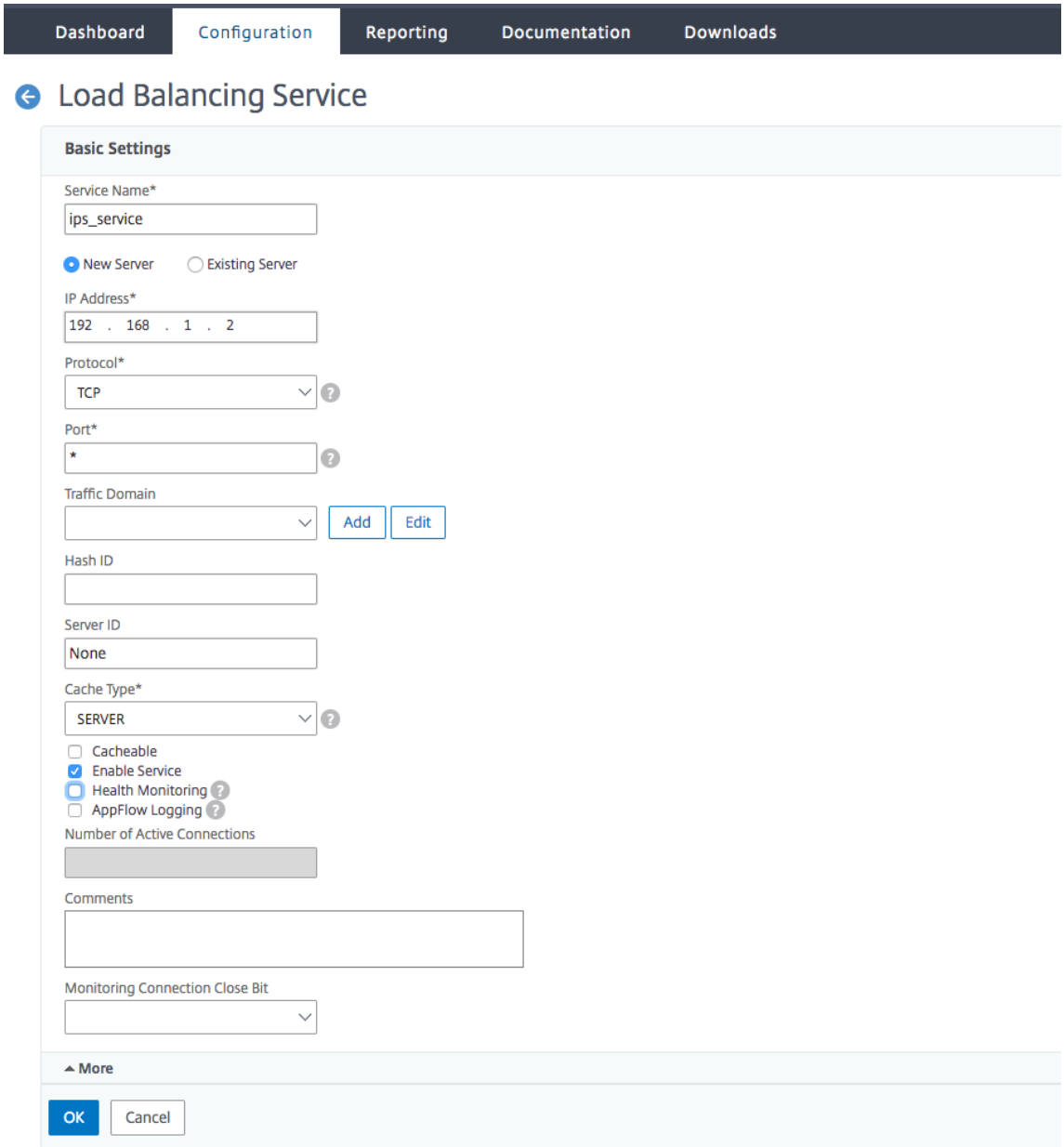
5. Navigieren Sie zu **System** > **Einstellungen** > **Erweiterte Funktionen konfigurieren**.
6. Wählen Sie auf der Seite „ **Erweiterte Funktionen konfigurieren** “ die Option **Inhaltsinspektion**aus.
7. Klicken Sie auf **OK** und auf **Schließen**.



8. Navigieren Sie zu **Sicherheit** > **Inhaltsinspektion** > **ContentInspection-Profile**.
9. Klicken Sie auf der Seite mit den **ContentInspection-Profilen** auf **Hinzufügen**.
10. Stellen Sie auf der Seite „ **ContentInspection-Profile erstellen** “ die folgenden Parameter ein.
    a) Name des Profils. Name des Inhaltsprüfprofils.
    b) Typ. Wählen Sie als Profiltyp InlineInspection aus.
    c) Ausgangsschnittstelle. Schnittstelle, über die die Appliance Datenverkehr vom NetScaler zum Inline-Gerät sendet.
    d) Eingangsschnittstelle. Schnittstelle, über die die Appliance Datenverkehr vom Inline-Gerät zum NetScaler empfängt.
    e) Ausgangs-VLAN. Schnittstellen-VLAN-ID, über die der Datenverkehr an das Inline-Gerät gesendet wird.
    f) VLAN eingeben. Schnittstellen-VLAN-ID, über die die Appliance Datenverkehr von Inline zu NetScaler empfängt (sofern konfiguriert).

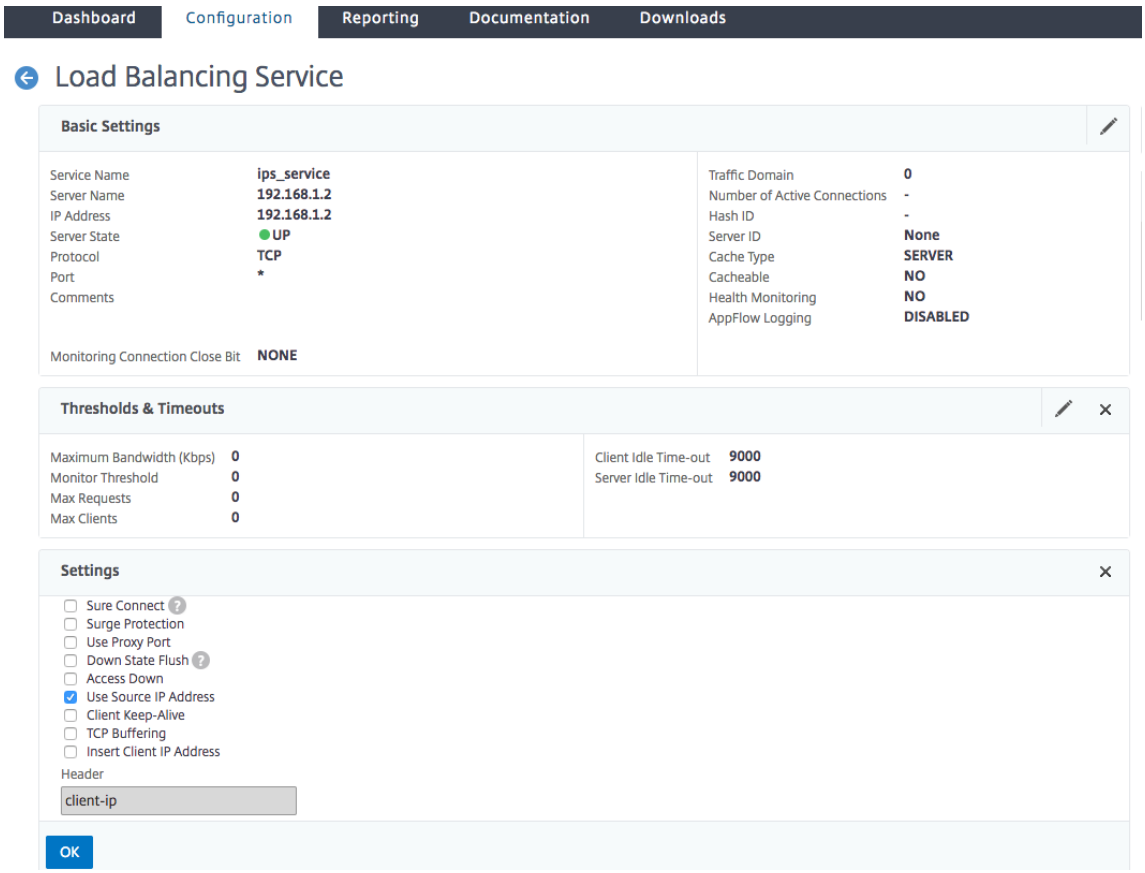


11. Klicken Sie auf **Erstellen** und **Schließen**.
12. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**
13. Stellen Sie auf der Seite **Dienste** die folgenden Parameter ein:
    a) Name des Dienstes. Name des Load Balancing-Dienstes.
    b) IP-Adresse. Verwenden Sie eine Schein-IP-Adresse. Hinweis: Kein Gerät darf die IP-Adresse besitzen.
    c) Protokoll. Wählen Sie den Protokolltyp als TCP aus.
    d) Port. Geben Sie ein *
    e) Gesundheitsüberwachung. Deaktivieren Sie diese Option und aktivieren Sie sie nur, wenn Sie den Dienst an den TCP-Monitor binden möchten. Wenn Sie einen Monitor an einen Dienst binden möchten, muss die Option TRANSPARENT im Monitor aktiviert sein. In Schritt 14 erfahren Sie, wie Sie einen Monitor hinzufügen und ihn an den Dienst binden.
    f) Klicken Sie auf **OK**.

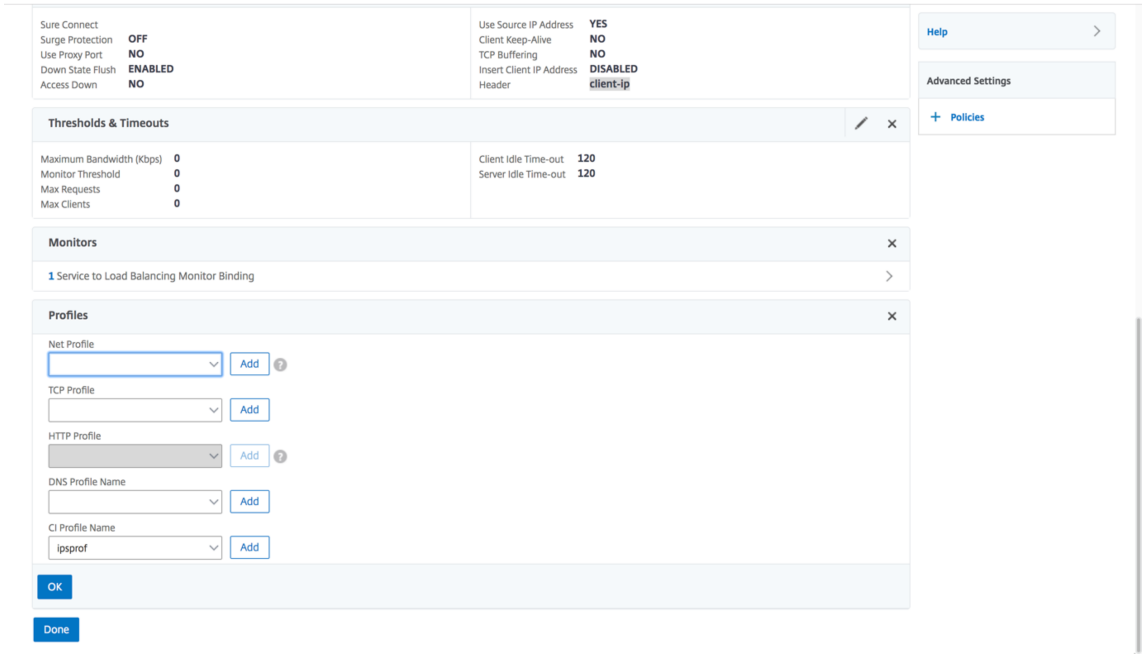


14. Bearbeiten **Sie im Abschnitt Einstellungen** Folgendes und klicken Sie auf **OK**.

    a) Proxyport verwenden: Schalten Sie ihn aus
    b) Quell-IP-Adresse verwenden: Schalten Sie sie ein



15. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf “ **Profile**”.
16. Gehen Sie zum Abschnitt **Profile**, fügen Sie das Inline-Inhaltsprüfprofil hinzu und klicken Sie auf **OK.**

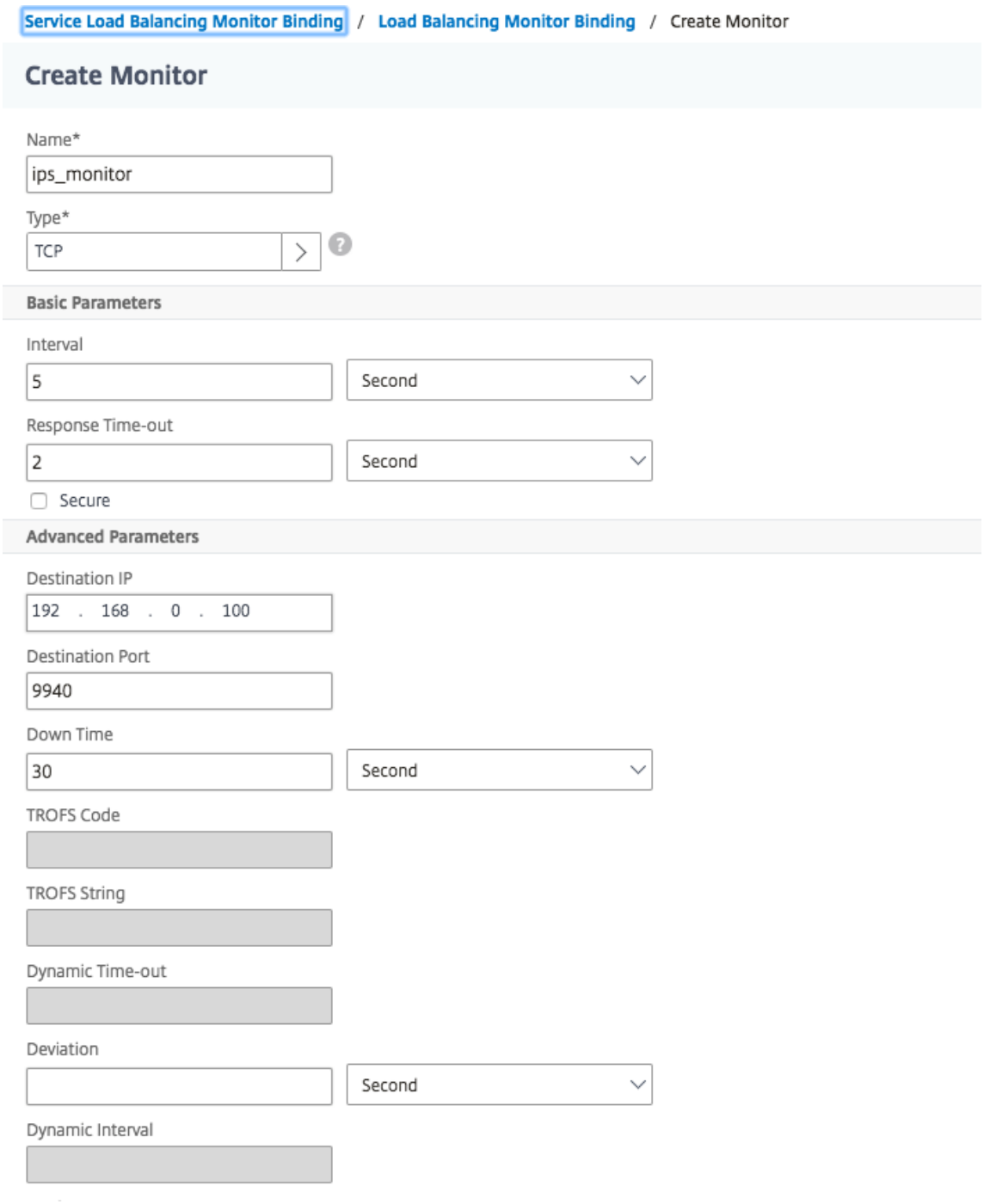


17. Gehen Sie zum Abschnitt „ **Monitore**“, „ **Bindungen hinzufügen** “ > **„Monitor“** > „ **Hinzufügen**“.

    a) Name: Name des Monitors
    b) Typ: Wählen Sie den TCP-Typ
    c) Ziel-IP, PORT: Ziel-IP-Adresse und Port.
    d) Transparent: EINSCHALTEN

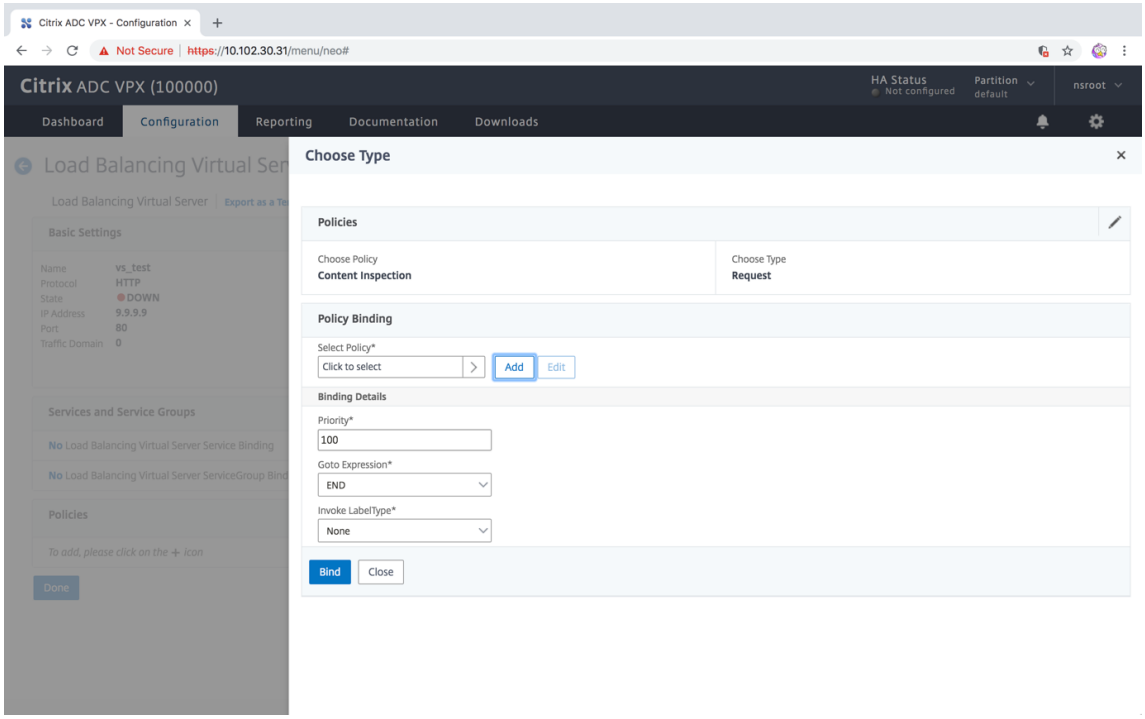
    Hinweis: Monitor-Pakete müssen durch das Inline-Gerät fließen, um den Status des Inline-Geräts zu überwachen.

18. Klicken Sie auf **Erstellen**.



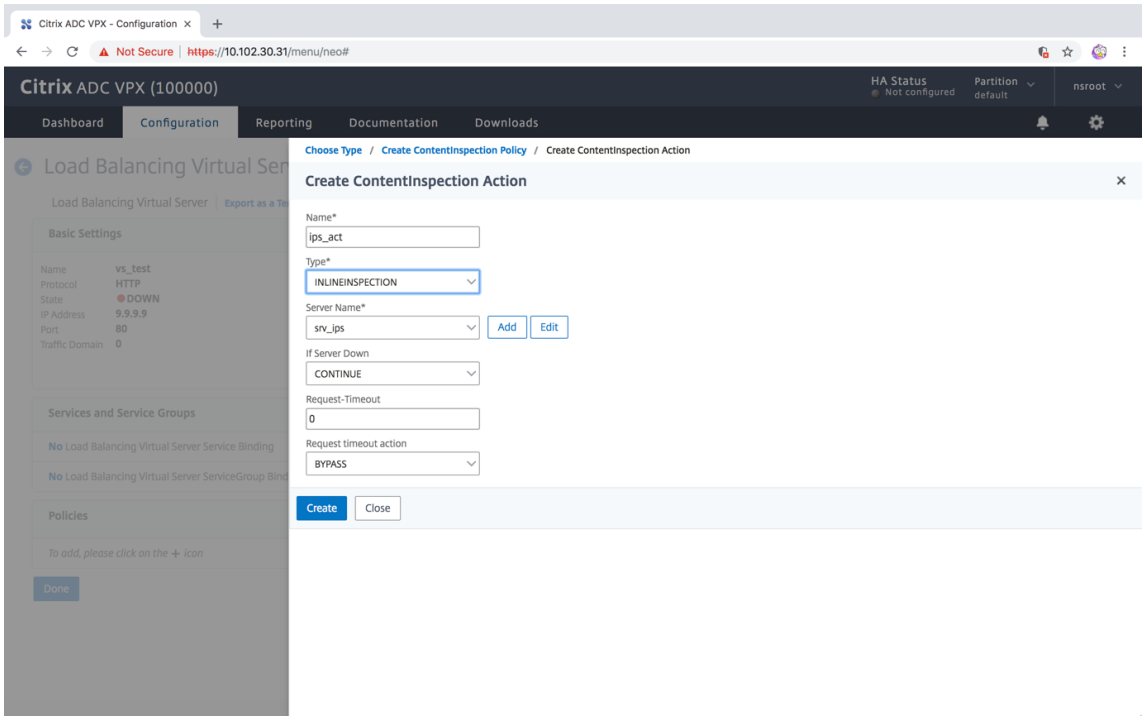
19. Klicken Sie auf **Fertig**.
20. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**. Fügen Sie einen virtuellen Server vom Typ HTTP oder SSL hinzu.
21. Nachdem Sie die Serverdetails eingegeben haben, klicken Sie auf **OK** und erneut auf **OK**.
22. Schalten Sie im Abschnitt **Traffic Settings** des Load Balancing Virtual Servers die Layer-2-Parameter ein.

23. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf **Richtlinien**.
24. Gehen Sie zum Abschnitt **Richtlinien** und klicken Sie auf das Symbol „+“, um die Richtlinie zur Inhaltsinspektion zu konfigurieren.
25. Wählen Sie auf der Seite **„Richtlinie auswählen** “ die Option Inhaltsinspektion aus. Klicken Sie auf **Weiter**.
26. Klicken Sie im Abschnitt **Richtlinienbindung** auf **Hinzufügen**, um eine Richtlinie zur Inhaltsinspektion hinzuzufügen.



27. Geben Sie auf der Seite „ **ContentInspection-Richtlinie erstellen** “ einen Namen für die Richtlinie zur Inline-Inhaltsinspektion ein.
28. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Aktion zur Inline-Inhaltsinspektion zu erstellen.
29. Stellen Sie auf der Seite „ **CI-Aktion erstellen** “ die folgenden Parameter ein:
    a) Name. Name der Inline-Richtlinie zur Inhaltsüberprüfung.
    b) Typ. Wählen Sie den Typ als InlineInspection aus.
    c) Server. Wählen Sie den Server/Dienst als Inline-Geräte aus.
    d) Wenn Server ausgefallen ist. Wählen Sie einen Vorgang aus, wenn der Server ausfällt.
    e) Zeitüberschreitung anfragen. Wählen Sie einen Timeoutwert aus. Sie können Standardwerte verwenden.
    f) Timeout-Aktion anfordern. Wählen Sie eine Zeitüberschreitungsaktion aus. Sie können Standardwerte verwenden.

30. Klicken Sie auf **Erstellen**.



31. Klicken Sie auf **Erstellen**.
32. Geben Sie auf der Seite „ **CI-Richtlinie erstellen** “ weitere Details ein:
33. Klicken Sie auf **OK** und auf **Schließen**.

Integration mit IPS oder NGFW als Inline-Geräte mit SSL-Forward-Proxy

August 19, 2021

Sicherheitsgeräte wie Intrusion Prevention System (IPS) und Next Generation Firewall (NGFW) schützen Server vor Netzwerkangriffen. Diese Geräte können den Live-Datenverkehr überprüfen und werden in der Regel im Layer 2-Inline-Modus bereitgestellt. Die SSL-Forward-Proxy-Appliance bietet Sicherheit für Benutzer und das Unternehmensnetzwerk beim Zugriff auf Ressourcen im Internet.

Eine SSL-Forward-Proxy-Appliance kann mit einem oder mehreren Inline-Geräten integriert werden, um Bedrohungen zu verhindern und erweiterten Sicherheitsschutz zu bieten. Bei den Inline-Geräten kann es sich um ein beliebiges Sicherheitsgerät wie IPS und NGFW handeln.

Einige Anwendungsfälle, in denen Sie von der SSL-Forward-Proxy-Appliance und der Inline-Geräteintegration profitieren können, sind:

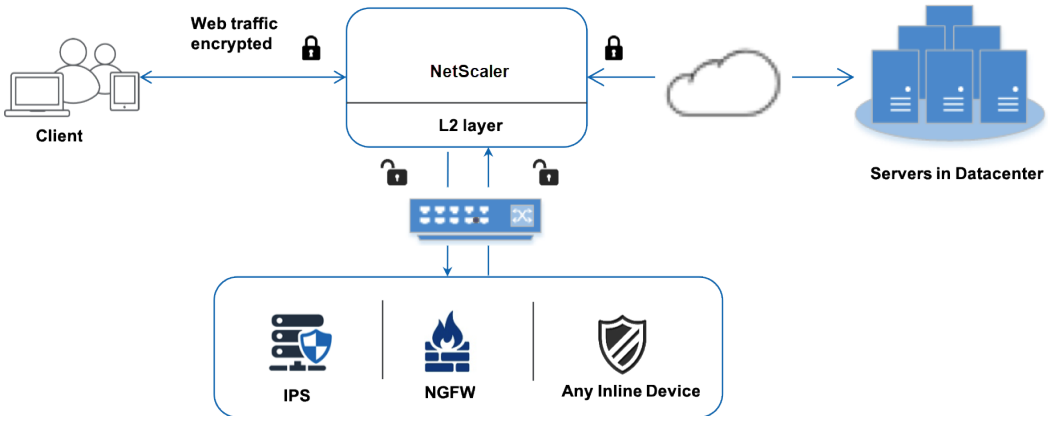
- **Überprüfen des verschlüsselten Datenverkehrs:** Die meisten IPS- und NGFW-Appliances umgehen verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe werden können.

Eine SSL-Forward-Proxy-Appliance kann den Datenverkehr entschlüsseln und ihn zur Überprüfung an die Inline-Geräte senden. Diese Integration erhöht die Netzwerksicherheit des Kunden.

- **Entladen von Inline-Geräten aus der TLS/SSL -Verarbeitung:** Die TLS/SSL -Verarbeitung ist teuer, was zu einer hohen CPU-Auslastung in IPS- oder NGFW-Appliances führen kann, wenn sie auch den Datenverkehr entschlüsseln. Eine SSL-Forward-Proxy-Appliance hilft beim Auslagern von TLS/SSL-Verarbeitung von Inline-Geräten. Inline-Geräte können daher ein höheres Verkehrsaufkommen untersuchen.
- **Inline-Geräte für den Ladeausgleich:** Wenn Sie mehrere Inline-Geräte für die Verwaltung des hohen Datenverkehrs konfiguriert haben, kann eine SSL-Forward-Proxy-Appliance einen Lastausgleich durchführen und den Datenverkehr gleichmäßig auf diese Geräte verteilen.
- **Intelligente Auswahl des Datenverkehrs:** Statt den gesamten Datenverkehr zur Inspektion an das Inline-Gerät zu senden, führt die Appliance eine intelligente Auswahl des Datenverkehrs durch. Beispielsweise wird das Senden von Textdateien zur Überprüfung an die Inline-Geräte übersprungen.

SSL-Forward-Proxy-Integration mit Inline-Geräten

Das folgende Diagramm zeigt, wie ein SSL-Forward-Proxy in Inline-Sicherheitsgeräte integriert ist.



Wenn Sie Inline-Geräte mit der SSL Forward-Proxy-Appliance integrieren, interagieren die Komponenten wie folgt:

1. Ein Client sendet eine Anforderung an eine SSL-Forward-Proxy-Appliance.
2. Die Appliance sendet die Daten an das Inline-Gerät zur Inhaltsüberprüfung basierend auf der Richtlinienbewertung. Bei HTTPS-Datenverkehr entschlüsselt die Appliance die Daten und sendet sie zur Inhaltsüberprüfung im Klartext an das Inline-Gerät.

> **Hinweis:**
>
> Wenn zwei oder mehr Inline-Geräte vorhanden sind, gleicht die Appliance die Geräte aus und sendet den Datenverkehr.

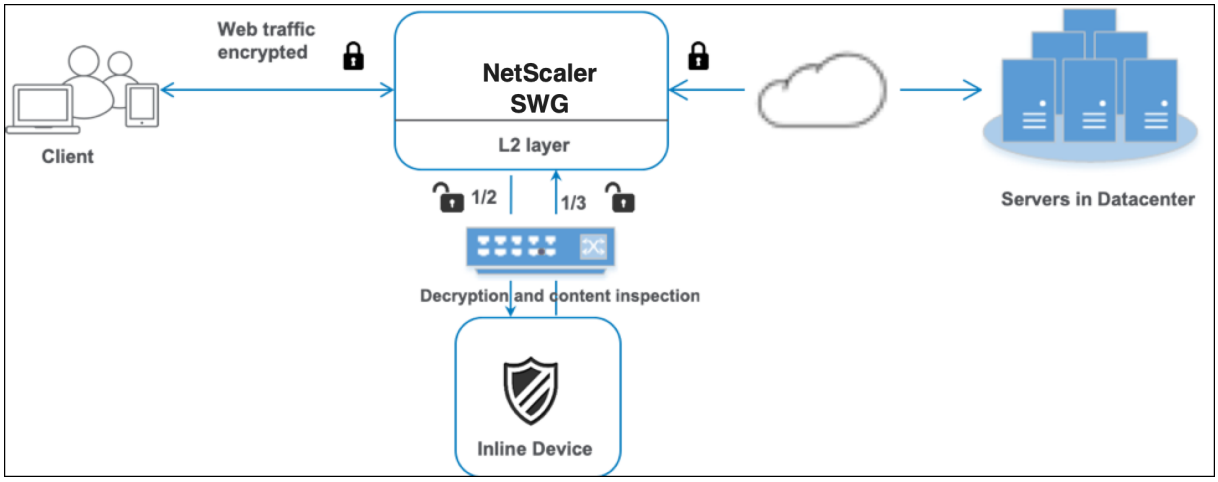
3. Fügen Sie einen virtuellen Content Switching- oder HTTP/HTTPS-Load Balancing-Server hinzu.
4. Das Inline-Gerät prüft die Daten auf Bedrohungen und entscheidet, ob die Daten gelöscht, zurückgesetzt oder an die Appliance gesendet werden sollen.
5. Wenn Sicherheitsbedrohungen vorliegen, ändert das Gerät die Daten und sendet sie an die Appliance.
6. Bei HTTPS-Datenverkehr verschlüsselt die Appliance die Daten erneut und leitet die Anforderung an den Back-End-Server weiter.
7. Der Back-End-Server sendet die Antwort an die Appliance.
8. Die Appliance entschlüsselt die Daten erneut und sendet sie zur Überprüfung an das Inline-Gerät.
9. Das Inline-Gerät prüft die Daten. Wenn Sicherheitsbedrohungen vorliegen, ändert das Gerät die Daten und sendet sie an die Appliance.
10. Die Appliance verschlüsselt die Daten erneut und sendet die Antwort an den Client.

Konfigurieren der Inline-Geräteintegration

Sie können eine SSL-Forward-Proxy-Appliance mit einem Inline-Gerät auf drei verschiedene Arten konfigurieren:

Szenario 1: Verwenden eines einzelnen Inline-Geräts

Um ein Sicherheitsgerät (IPS oder NGFW) in den Inline-Modus zu integrieren, müssen Sie die Inhaltsinspektion und die MAC-basierte Weiterleitung (MBF) im globalen Modus auf der SSL-Forward-Proxy-Appliance aktivieren. Fügen Sie anschließend ein Inhaltsinspektionsprofil, einen TCP-Dienst, eine Inhaltsüberprüfungsaktion für Inline-Geräte hinzu, um den Datenverkehr basierend auf der Inspektion zurückzusetzen, zu blockieren oder zu löschen. Fügen Sie außerdem eine Richtlinie zur Inhaltsüberprüfung hinzu, die von der Appliance verwendet wird, um die Teilmenge des Datenverkehrs zu bestimmen, die an die Inline-Geräte gesendet werden soll. Konfigurieren Sie schließlich den virtuellen Proxyserver mit aktivierter Layer-2-Verbindung auf dem Server und binden Sie die Inhaltsüberprüfungsrichtlinie an diesen virtuellen Proxyserver.



Gehen Sie wie folgt vor:

1. Aktivieren Sie den MAC-basierten Weiterleitungsmodus (MPF).
2. Aktivieren Sie die Funktion zur Inhaltsüberprüfung.
3. Fügen Sie ein Inhaltsinspektionsprofil für den Service hinzu. Das Content-Inspektionsprofil enthält die Inline-Geräteeinstellungen, die die SSL-Forward-Proxy-Appliance mit einem Inline-Gerät integrieren.
4. (Optional) Fügen Sie einen TCP-Monitor hinzu.

   > **Hinweis:**
   >
   > Transparente Geräte haben keine IP-Adresse. Um Integritätsprüfungen durchzuführen, müssen Sie daher einen Monitor explizit binden.

5. Fügen Sie einen Dienst hinzu. Ein Dienst stellt ein Inline-Gerät dar.
6. (Optional) Binden Sie den Dienst an den TCP-Monitor.
7. Fügen Sie eine Inhaltsinspektionsaktion für den Service hinzu.
8. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu, und geben Sie die Aktion an.
9. Fügen Sie einen virtuellen HTTP- oder HTTPS-Proxyserver (Content Switching) hinzu.
10. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

Konfiguration mit der CLI

Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach den meisten Befehlen angegeben.

1. MBF aktivieren.

```
enable ns mode mbf
```


1. Aktivieren Sie das Feature.

```
enable ns feature contentInspection
```

1. Fügen Sie ein Inhaltsinspektionsprofil hinzu.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof -type InlineInspection -ingressinterface
 “1/2” -egressInterface “1/3”
```

1. Fügen Sie einen Dienst hinzu. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Standardmäßig ist die Systemüberwachung ON, binden Sie den Dienst an einen Integritätsmonitor und legen Sie auch die Option TRANSPARENT im Monitor ON fest.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service 198.51.100.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

1. Fügen Sie einen Integritätsmonitor hinzu. Standardmäßig ist der Integritätsmonitor aktiviert und Sie haben auch die Möglichkeit, ihn bei Bedarf zu deaktivieren. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent
    <YES, NO>
   ```

Beispiel:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

1. Binden Sie den Dienst an den Integritätsmonitor

Nachdem Sie den Integritätsmonitor konfiguriert haben, müssen Sie den Dienst an den Integritätsmonitor binden. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind service <name> -monitorName <name>
```

Beispiel:

```
bind service ips_svc -monitorName ips_tcp
```


1. Fügen Sie eine Inhaltsüberprüfungsaktion hinzu.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Beispiel:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
ips_service
```

1. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Fügen Sie einen virtuellen Proxyserver hinzu.

```
add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs> -Listenpolicy
 <expression> -authn401 ( ON | OFF )-authnVsName <string> -l2Conn ON
```

> **Hinweis:**
>
> Der Lastausgleich virtueller Server vom Typ HTTP/SSL wird ebenfalls unterstützt.

Beispiel:

```
add cs vserver transparentcs PROXY * * -cltTimeout 180 -Listenpolicy exp1 -
authn401 on -authnVsName swg-auth-vs-trans-http -l2Conn ON
```

1. Binden Sie die Richtlinie an den virtuellen Server.

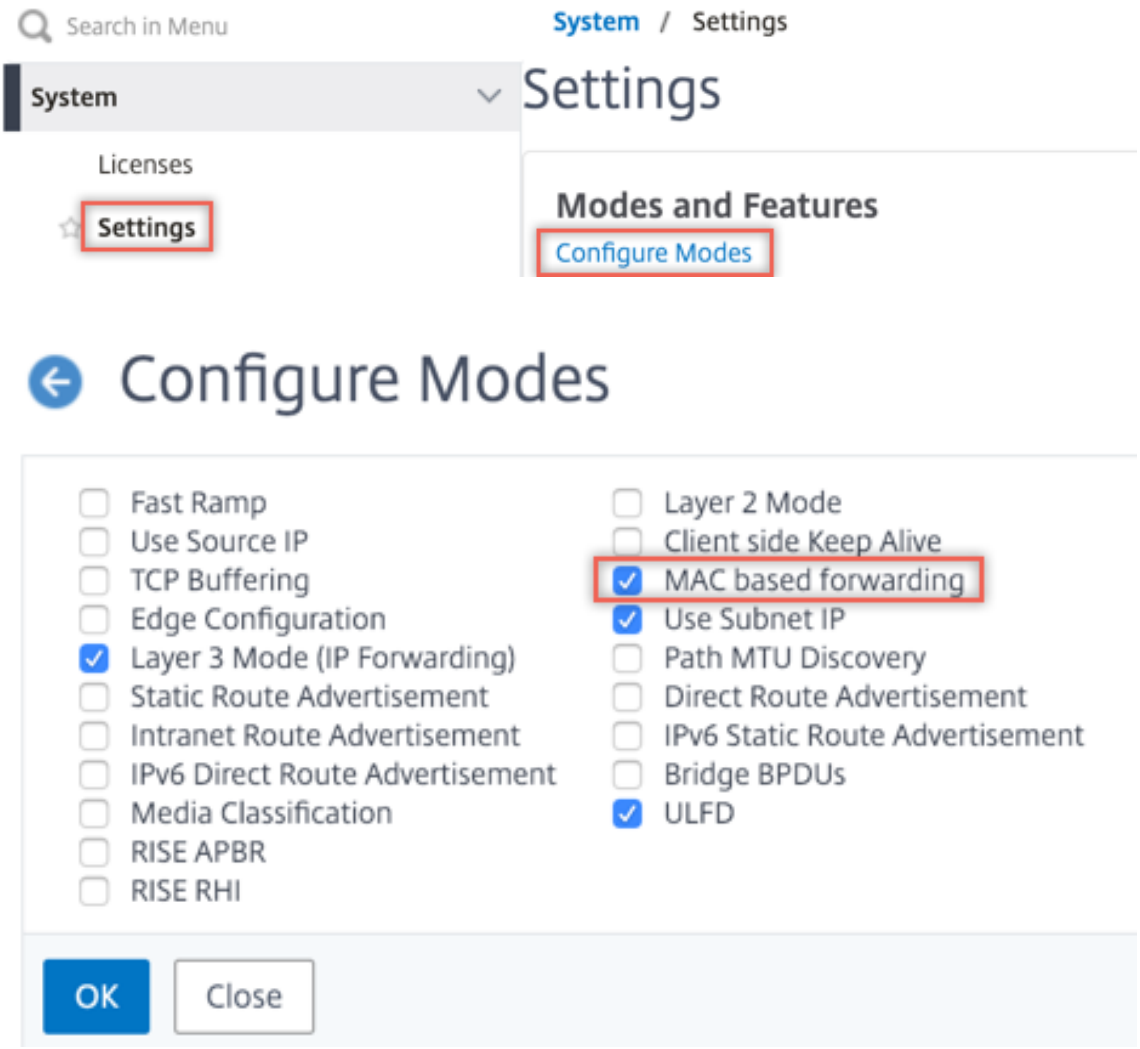
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Beispiel:

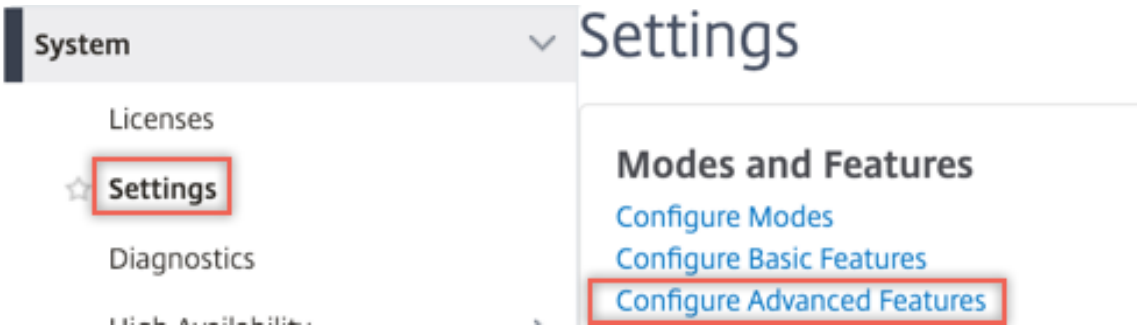
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

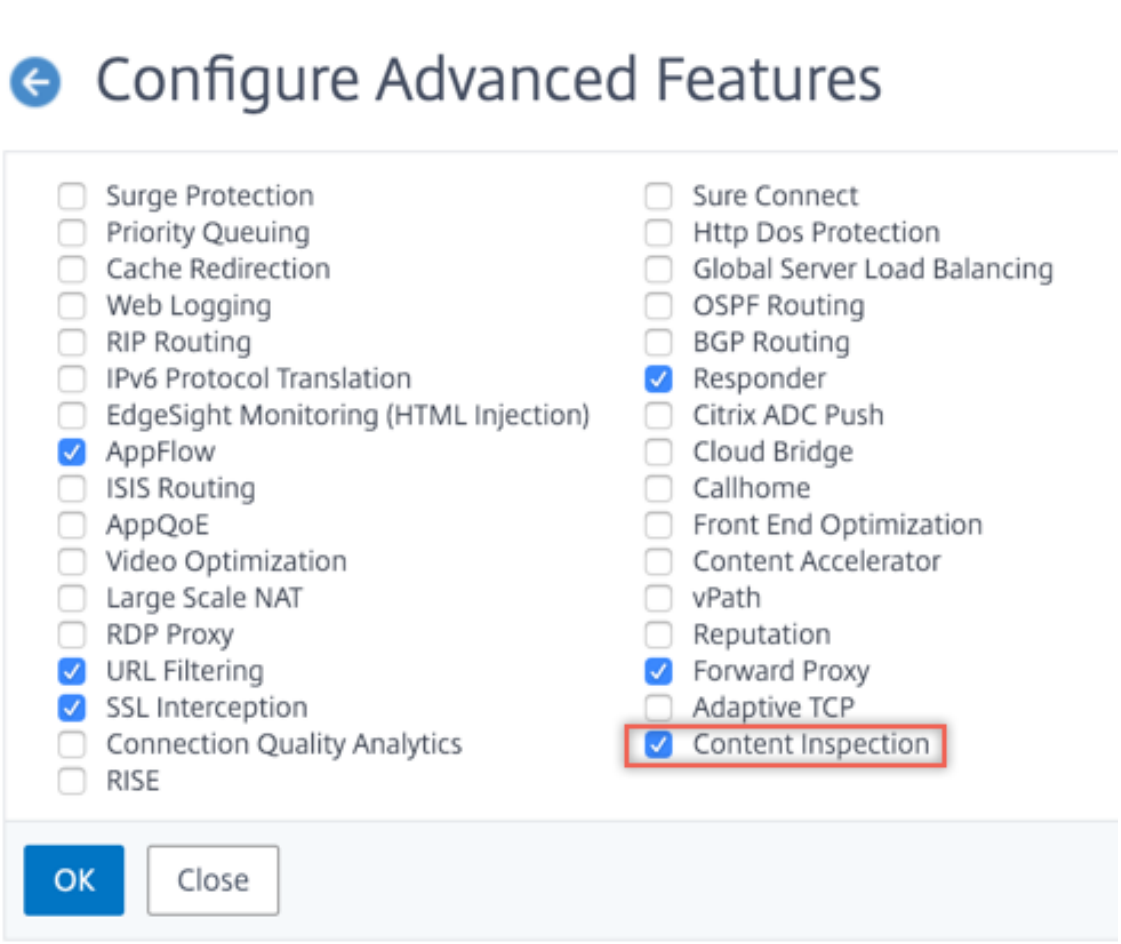
Konfigurieren Sie mit der GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.

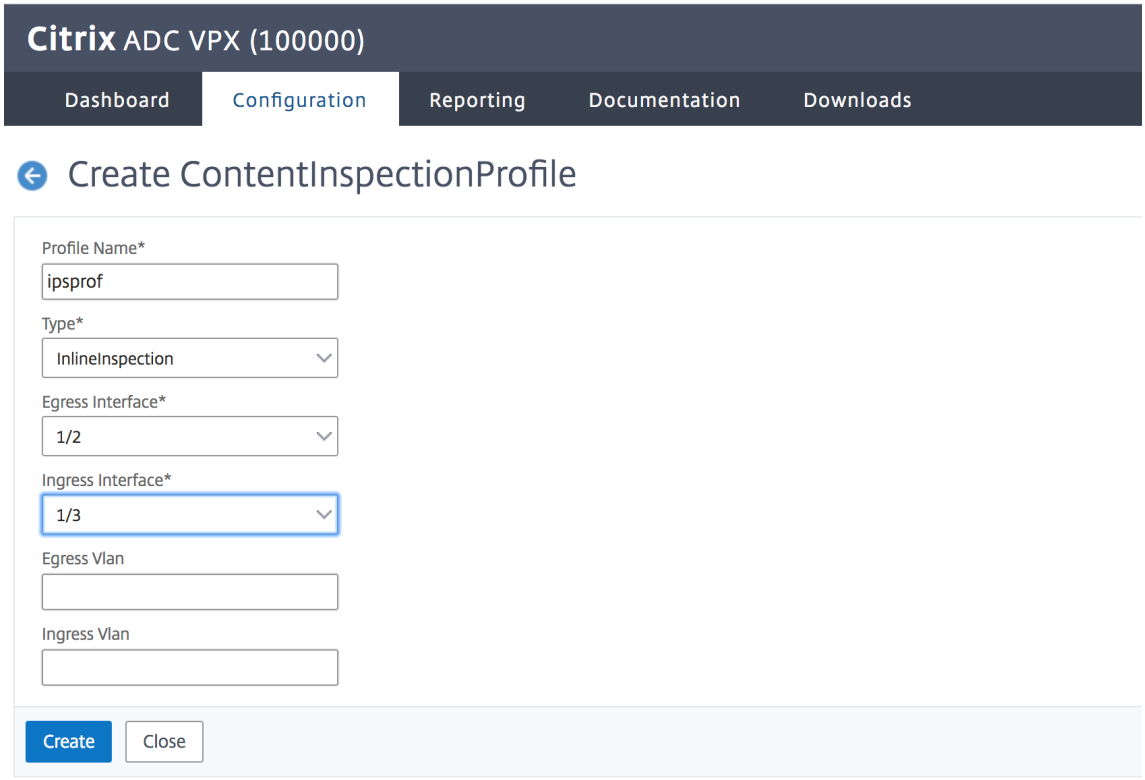


2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

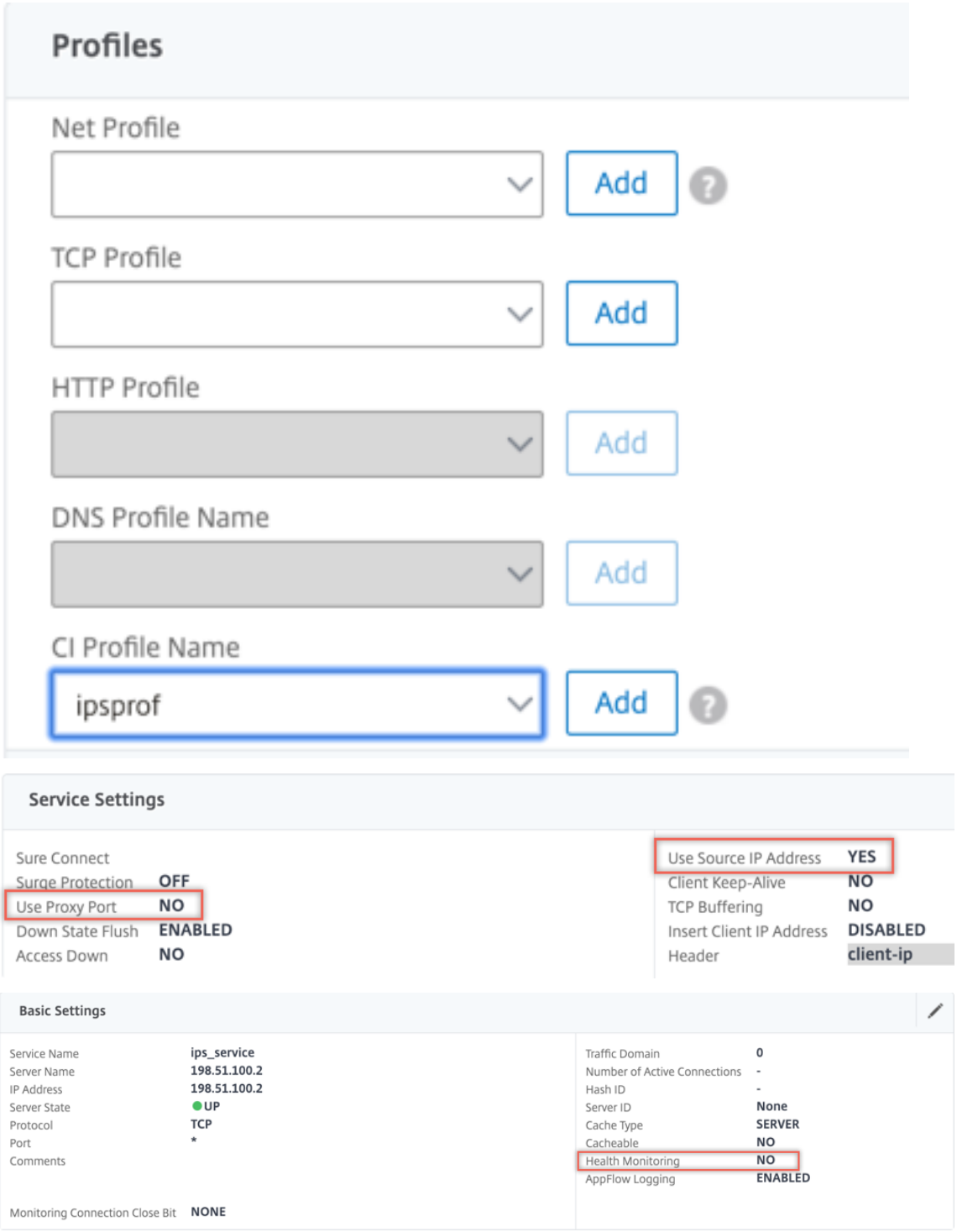




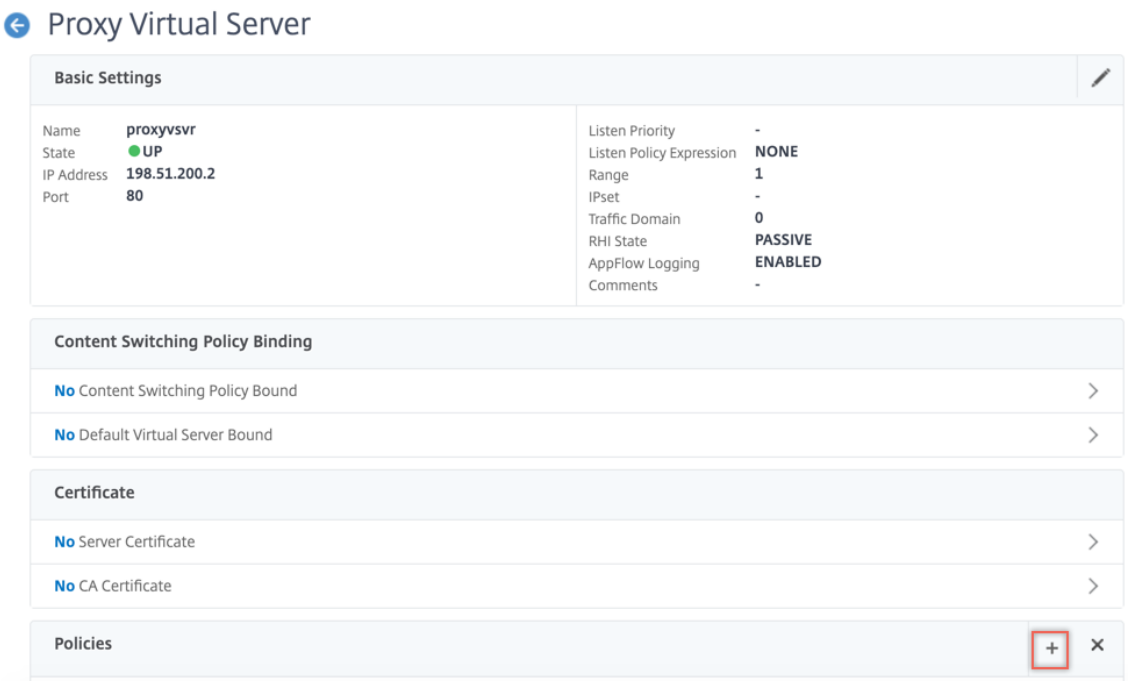
3. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.



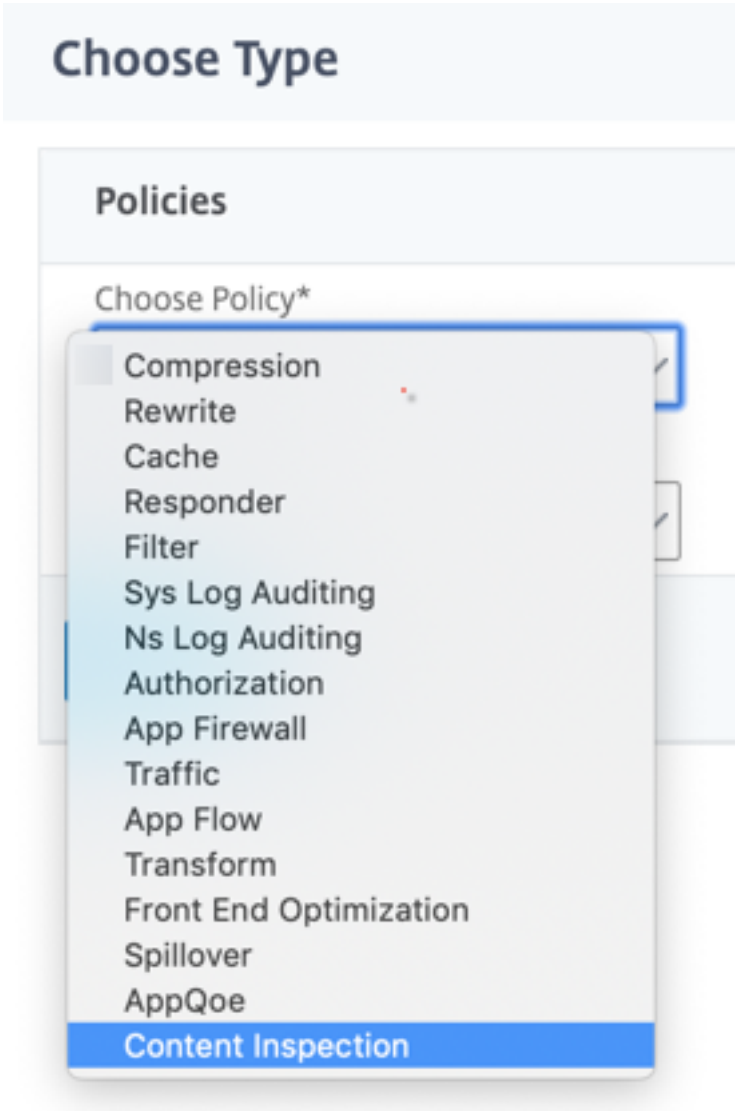
4. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.



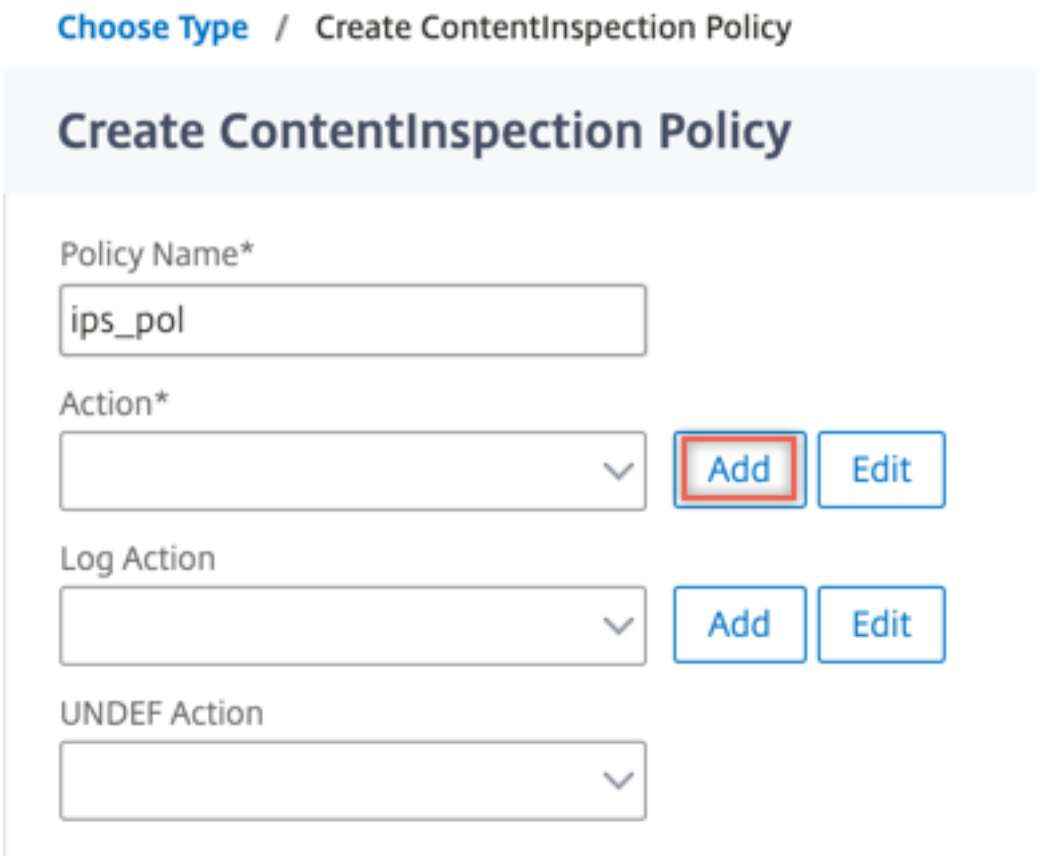
5. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



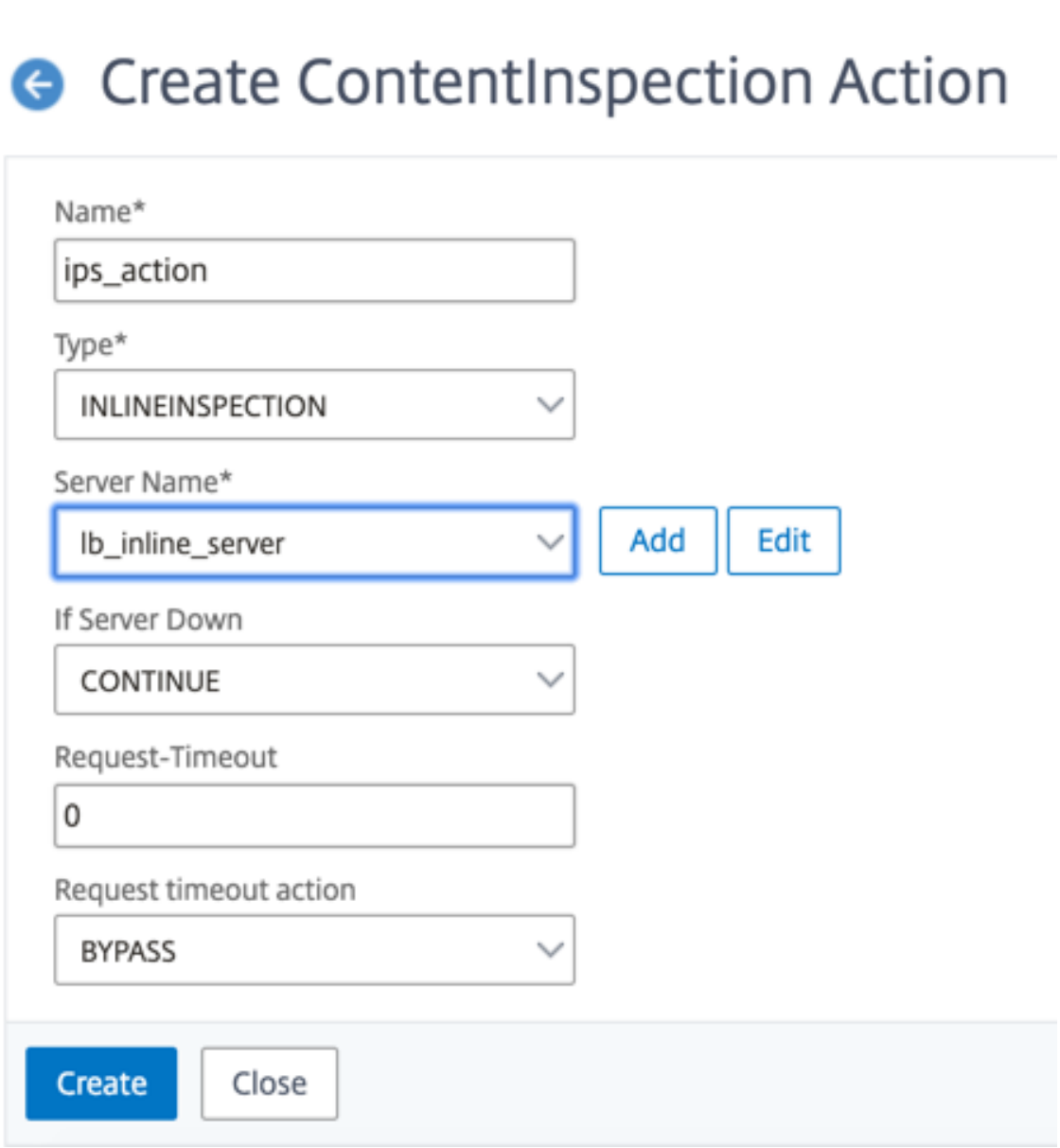
6. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



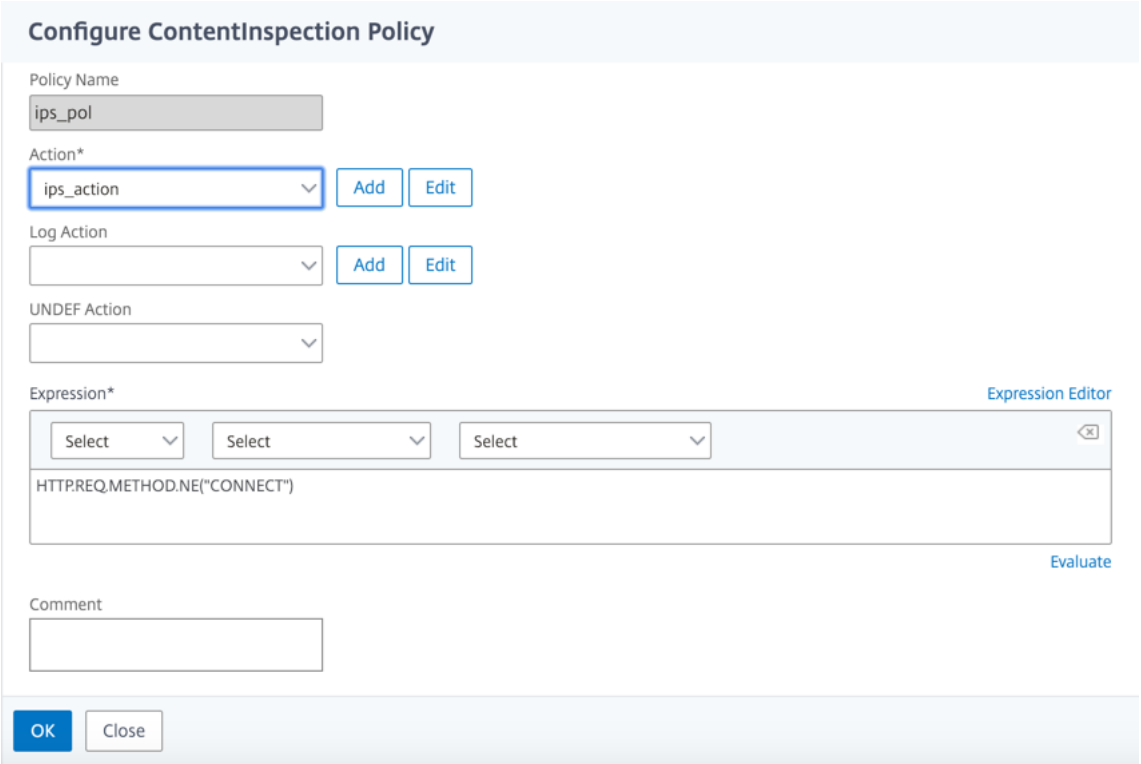
7. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



8. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie **unter Servername**den zuvor erstellten TCP-Dienst aus.



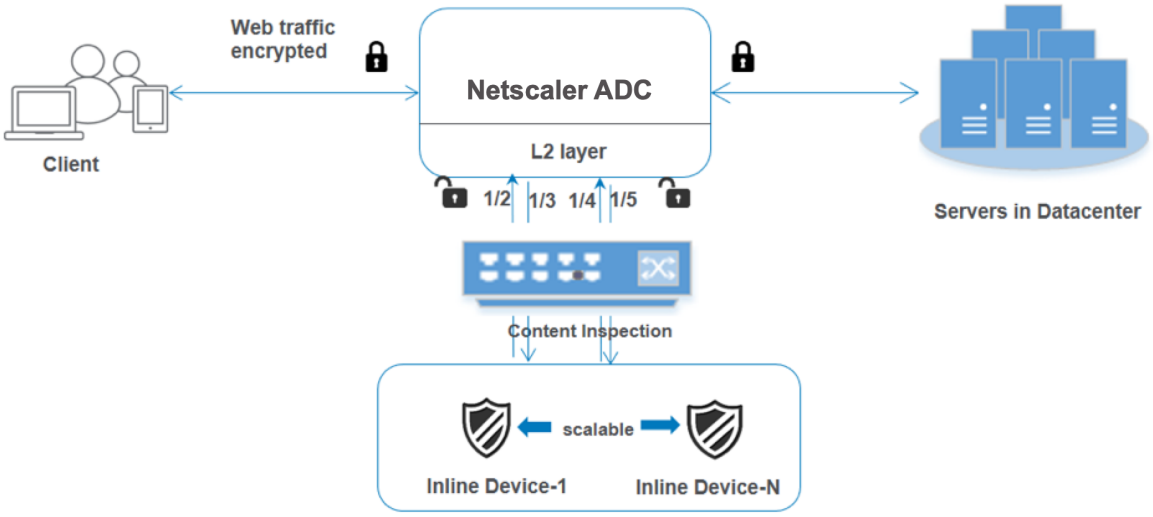
9. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



10. Klicken Sie auf **Bind**.
11. Klicken Sie auf **Fertig**.

Szenario 2: Lastausgleich mehrerer Inline-Geräte mit dedizierten Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, können Sie die Geräte mit verschiedenen Contentinspektionsdiensten mit dedizierten Schnittstellen ausgleichen. In diesem Fall gleicht die SSL-Forward-Proxy-Appliance die Teilmenge des Datenverkehrs aus, der über eine dedizierte Schnittstelle an jedes Gerät gesendet wird. Die Teilmenge wird basierend auf den konfigurierten Richtlinien festgelegt. Beispielsweise werden TXT- oder Bilddateien möglicherweise nicht zur Überprüfung an die Inline-Geräte gesendet.



Die Basiskonfiguration bleibt dieselbe wie in Szenario 1. Sie müssen jedoch für jedes Inline-Gerät ein Inhaltsinspektionsprofil erstellen und die Eingangs- und Ausgangsschnittstelle in jedem Profil angeben. Fügen Sie einen Dienst für jedes Inline-Gerät hinzu. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, und geben Sie ihn in der Inhaltsüberprüfungsaktion an. Führen Sie die folgenden zusätzlichen Schritte aus:

1. Fügen Sie Content-Inspektionsprofile für jeden Service hinzu.
2. Fügen Sie einen Dienst für jedes Gerät hinzu.
3. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.
4. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

Konfiguration mit der CLI

Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach jedem Befehl angegeben.

1. MBF aktivieren.

```
enable ns mode mbf
```

1. Aktivieren Sie das Feature.

```
enable ns feature contentInspection
```

1. Profil 1 für Service 1 hinzufügen.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:


```
add contentInspection profile ipsprof1 -type InlineInspection -ingressInterface
 "1/2"-egressInterface "1/3"
```

1. Profil 2 für Service 2 hinzufügen.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof2 -type InlineInspection -ingressInterface
 "1/4"-egressInterface "1/5"
```

1. Service 1 hinzufügen. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Schalten Sie die Zustandsüberwachung mit dem TCP-Monitor mit der Option TRANSPARENT ein.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Service 2 hinzufügen. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Schalten Sie die Zustandsüberwachung mit der Option TRANSPARENT ein.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Beispiel:

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Binden Sie die Dienste an den virtuellen Lastenausgleichsserver.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Beispiel:

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Beispiel:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu. Geben Sie die Inhaltsinspektionsaktion in der Richtlinie an.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Fügen Sie einen virtuellen Proxyserver hinzu.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Beispiel:

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

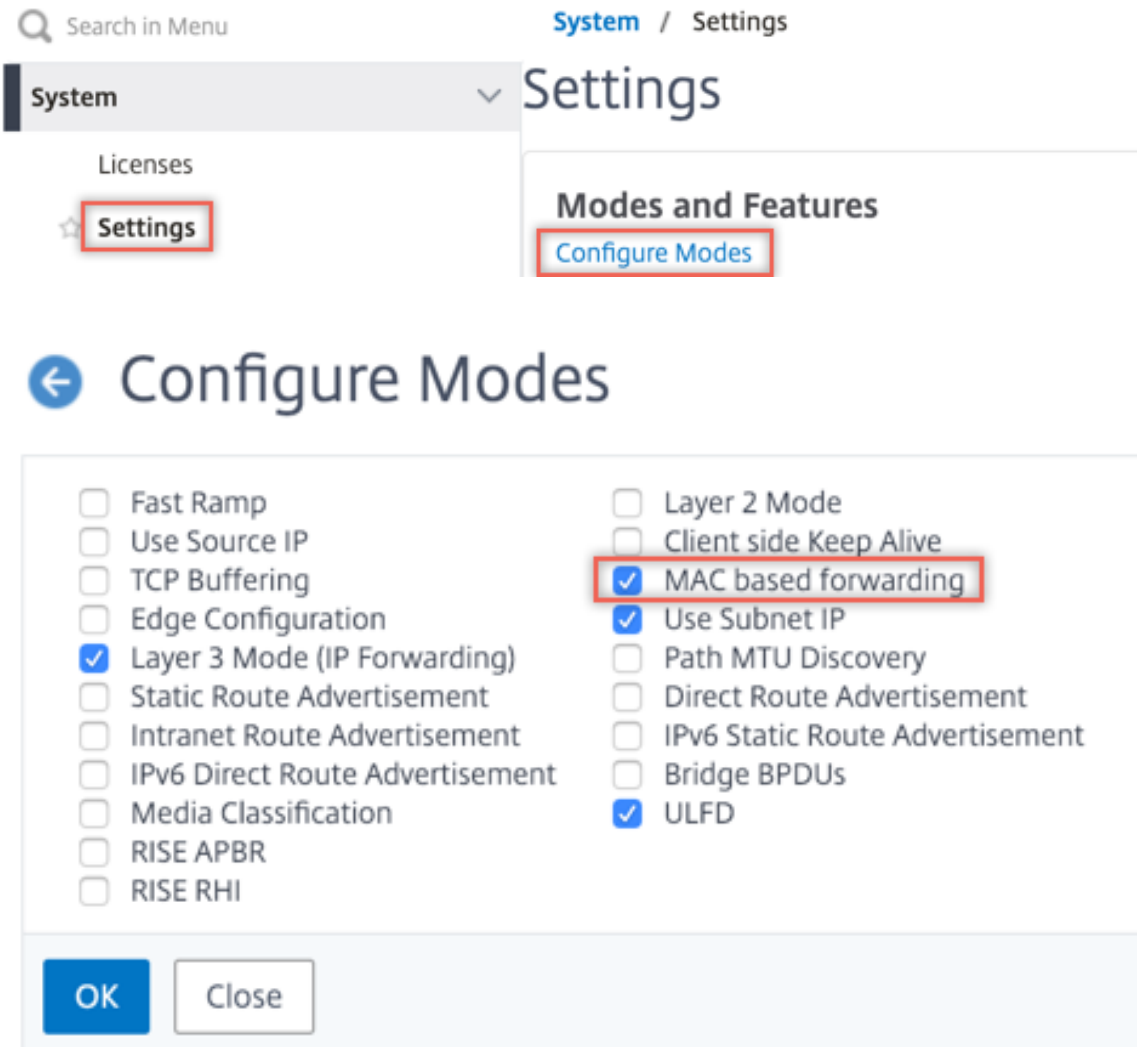
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Beispiel:

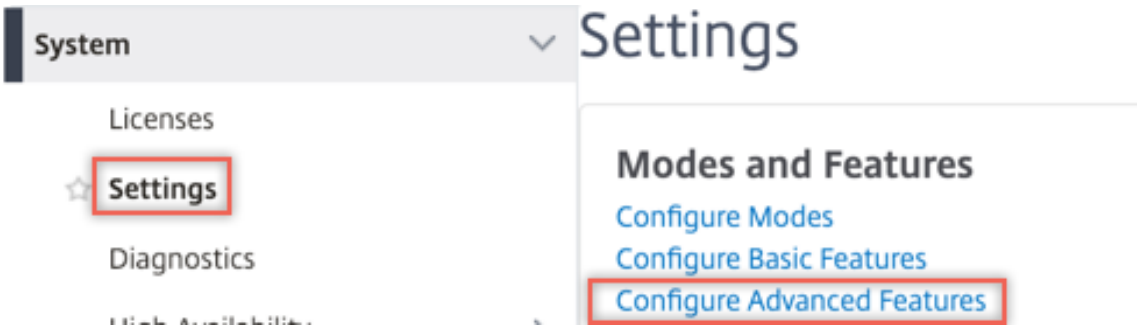
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

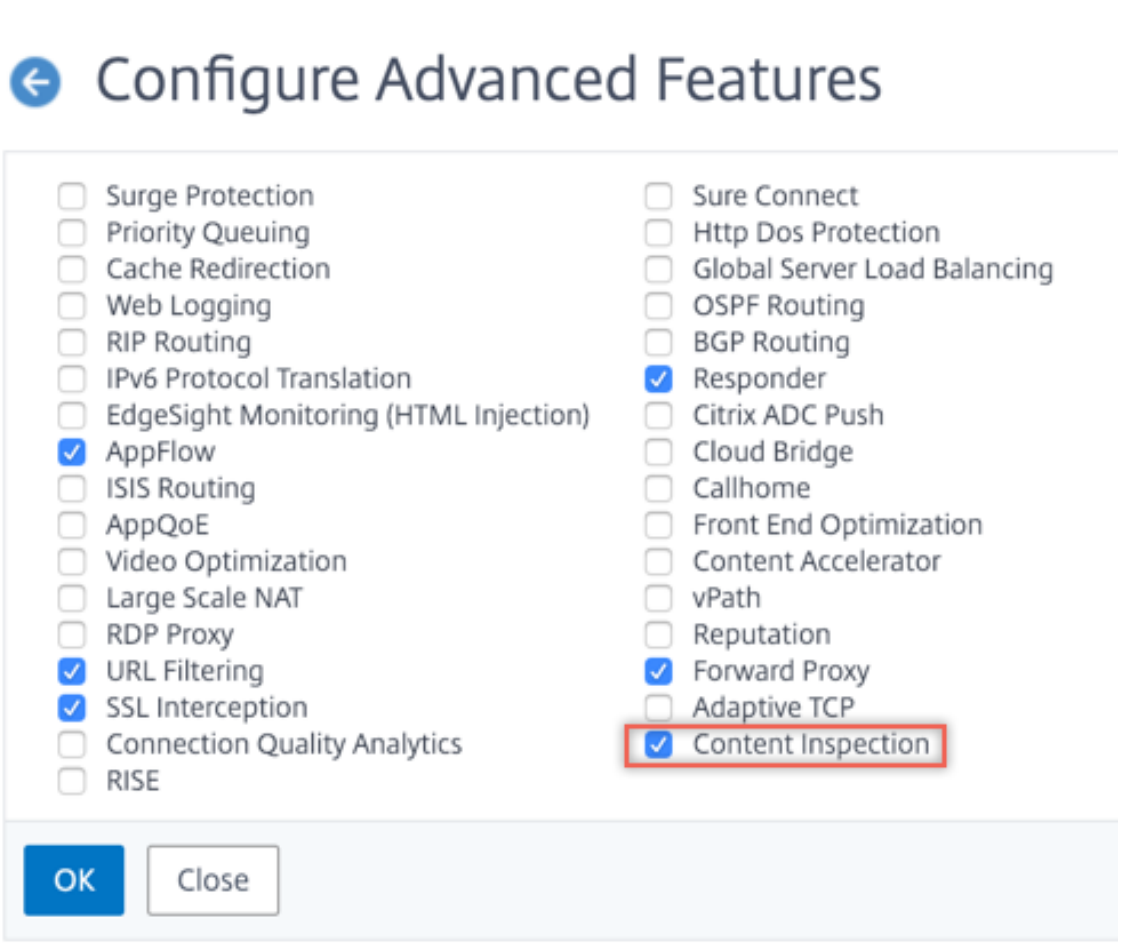
Konfiguration über die GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.

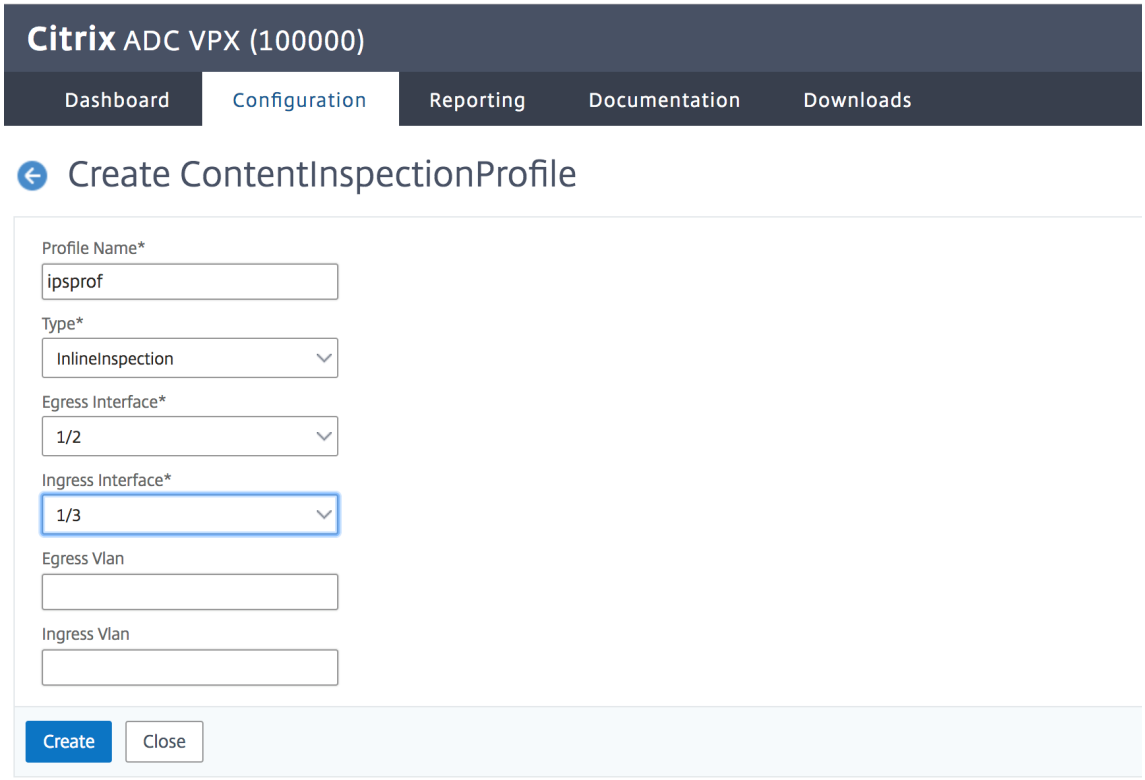


2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

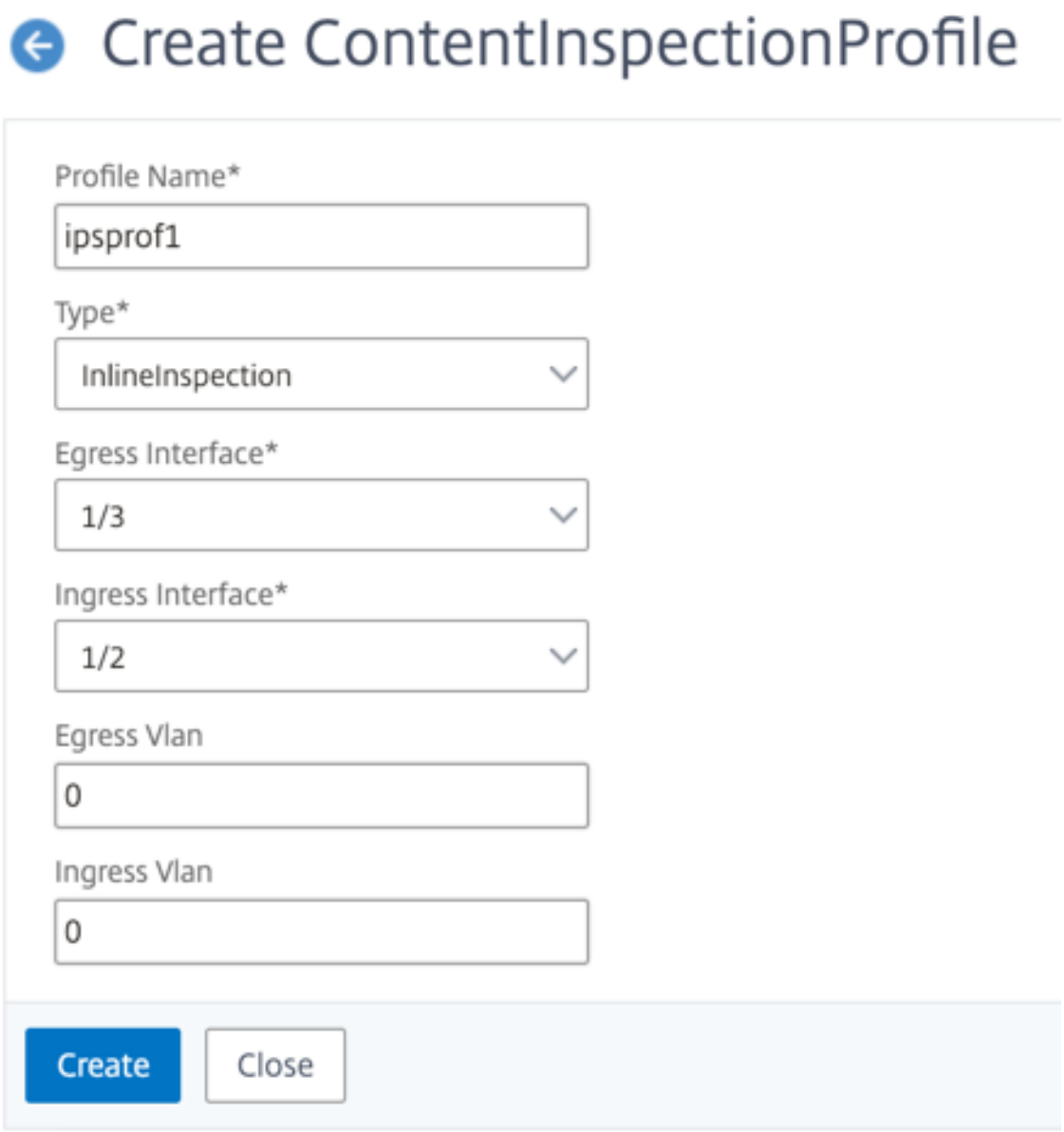




3. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.

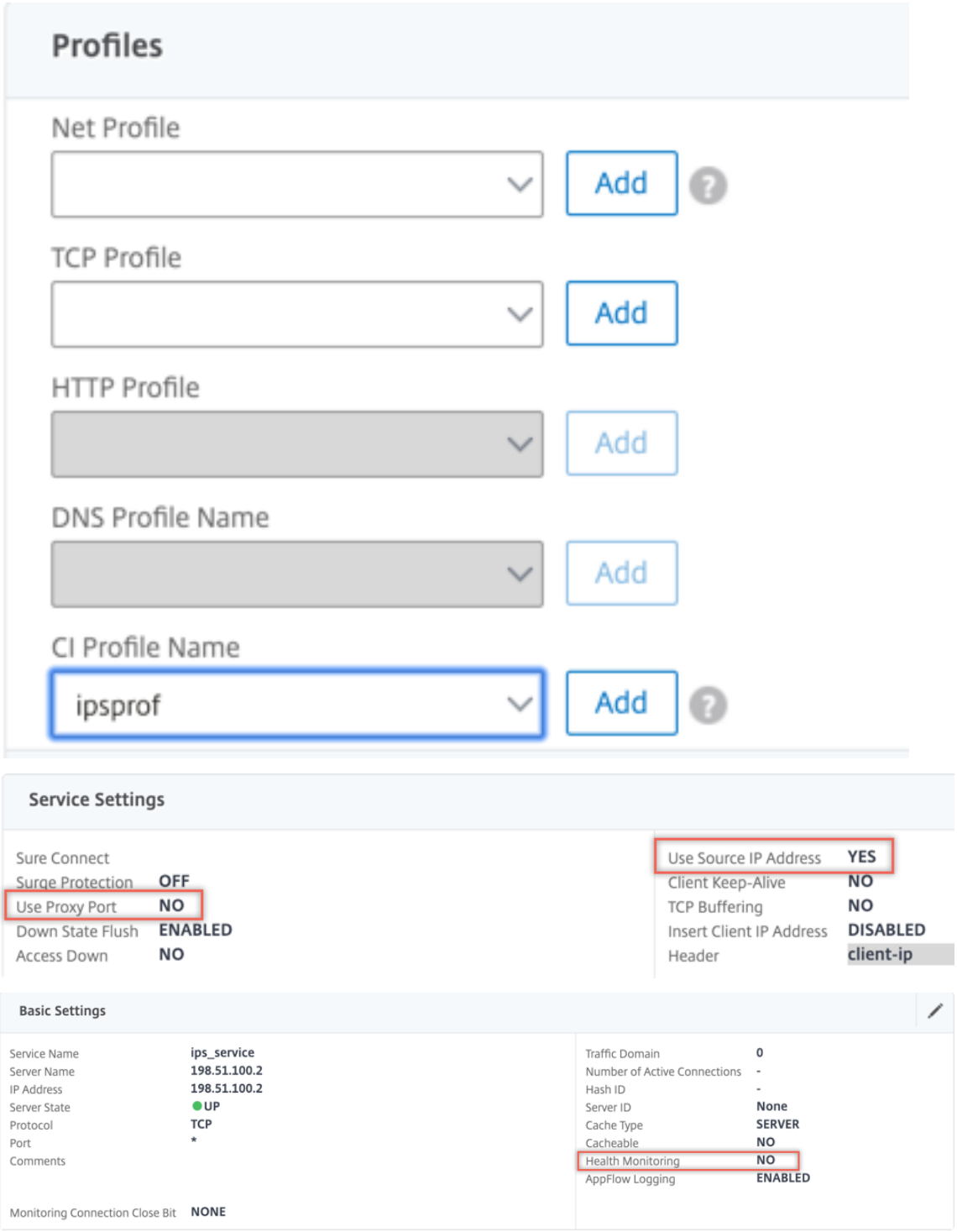


Geben Sie die Eingangs- und Ausgangsschnittstellen an.



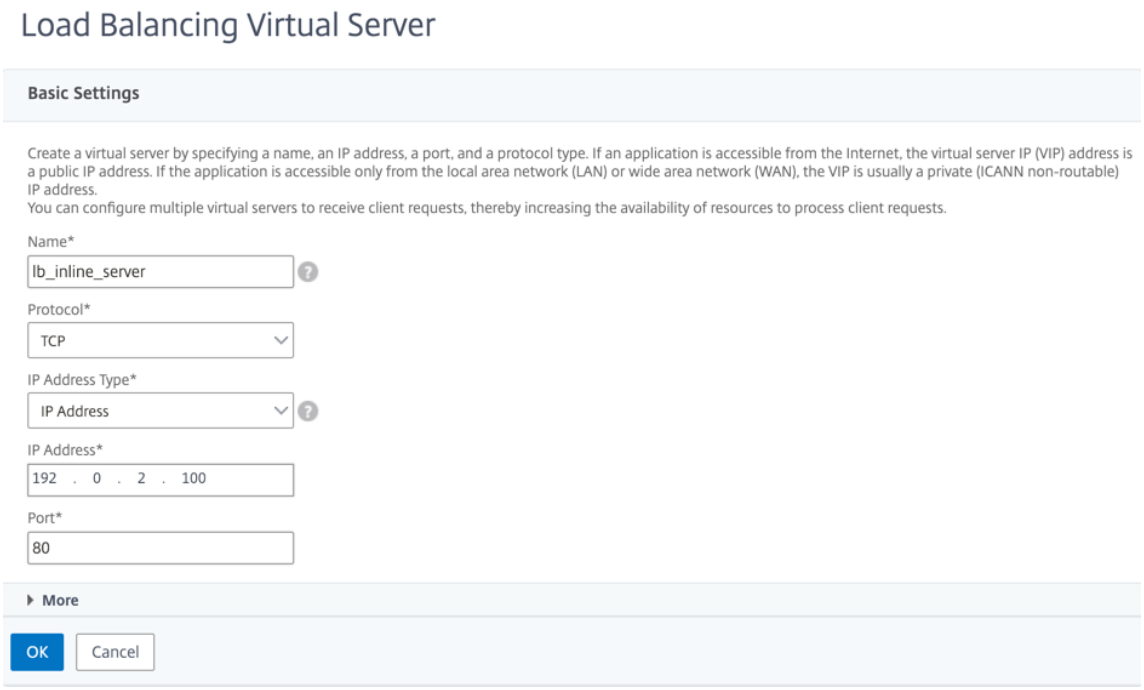
Erstellen Sie zwei Profile. Geben Sie im zweiten Profil eine andere Eingangs- und Ausgangsschnittstelle an.

4. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.



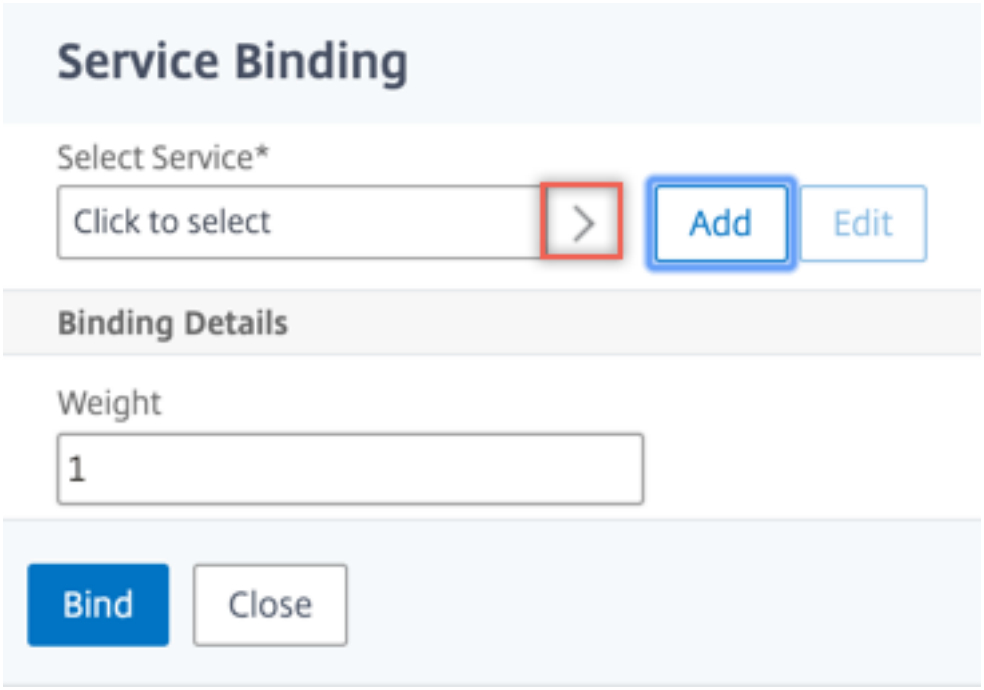
Erstellen Sie zwei Dienste. Geben Sie Dummy-IP-Adressen an, die keinem der Geräte gehören, einschließlich der Inline-Geräte.

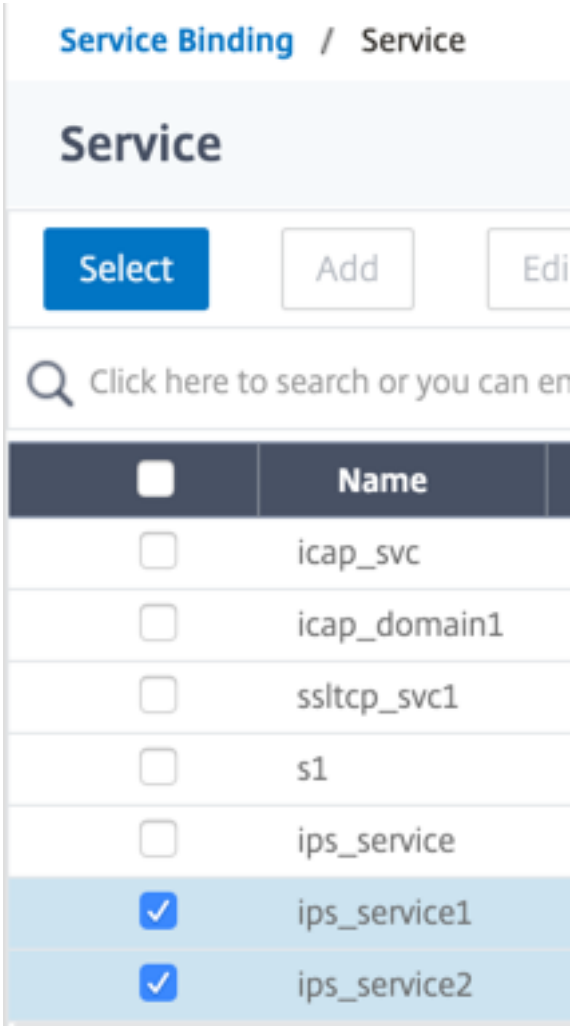
5. Navigieren Sie zu **Lastenausgleich > Virtuelle Server > Hinzufügen**. Erstellen Sie einen virtuellen TCP-Load Balancing Server.

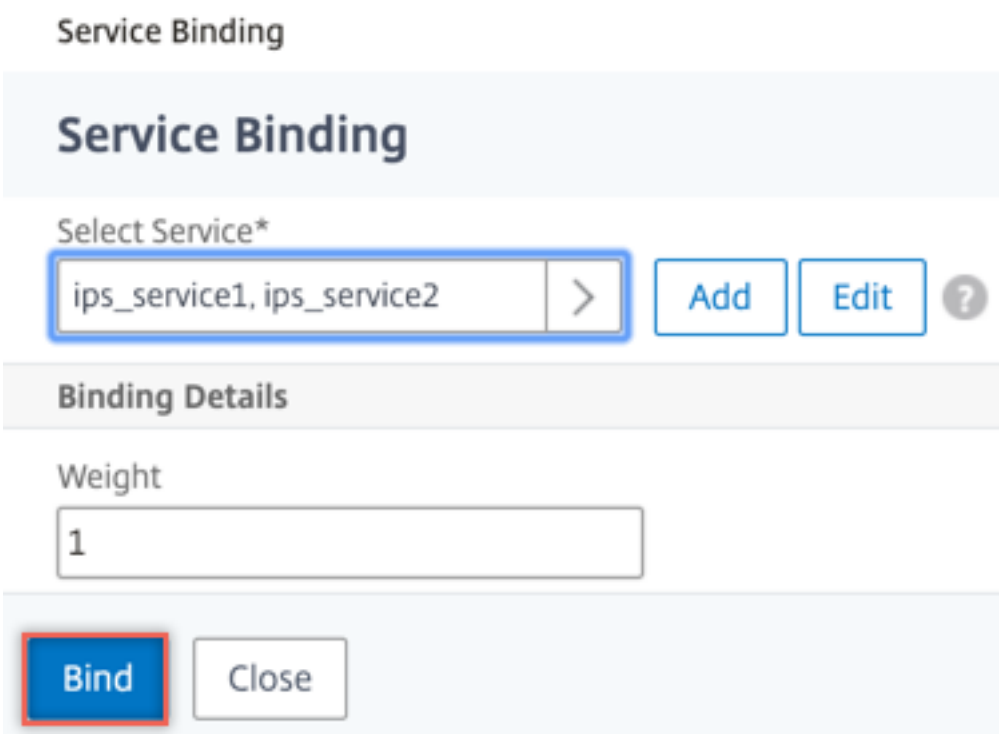


Klicken Sie auf **OK**.

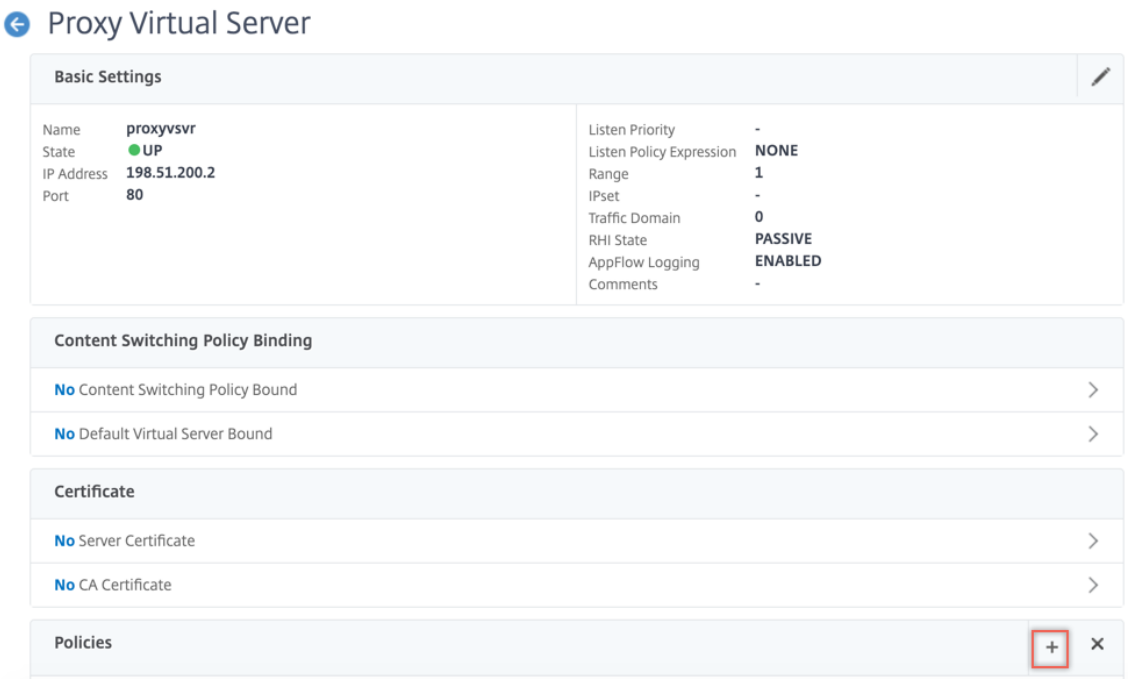
6. Klicken Sie in den Abschnitt **Load Balancing Virtual Server Service Binding**. Klicken Sie unter **Dienstbindung** auf den Pfeil unter **Dienst auswählen**. Wählen Sie die beiden zuvor erstellten Dienste aus, und klicken Sie auf **Auswählen**. Klicken Sie auf **Bind**.



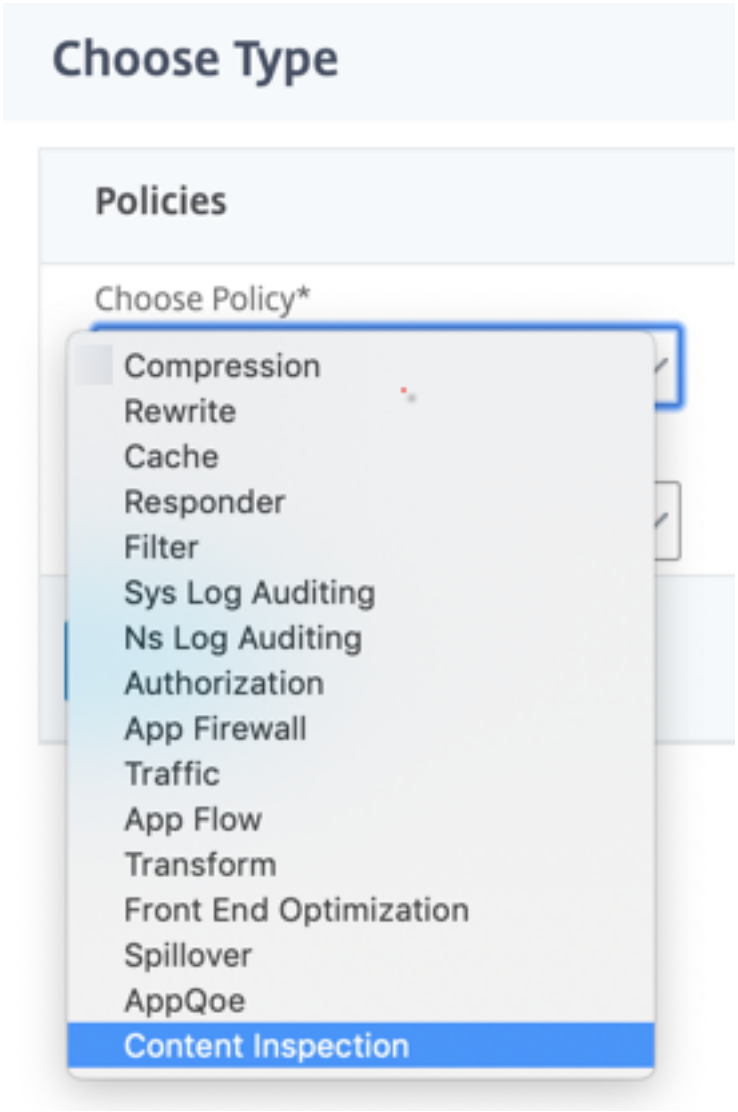




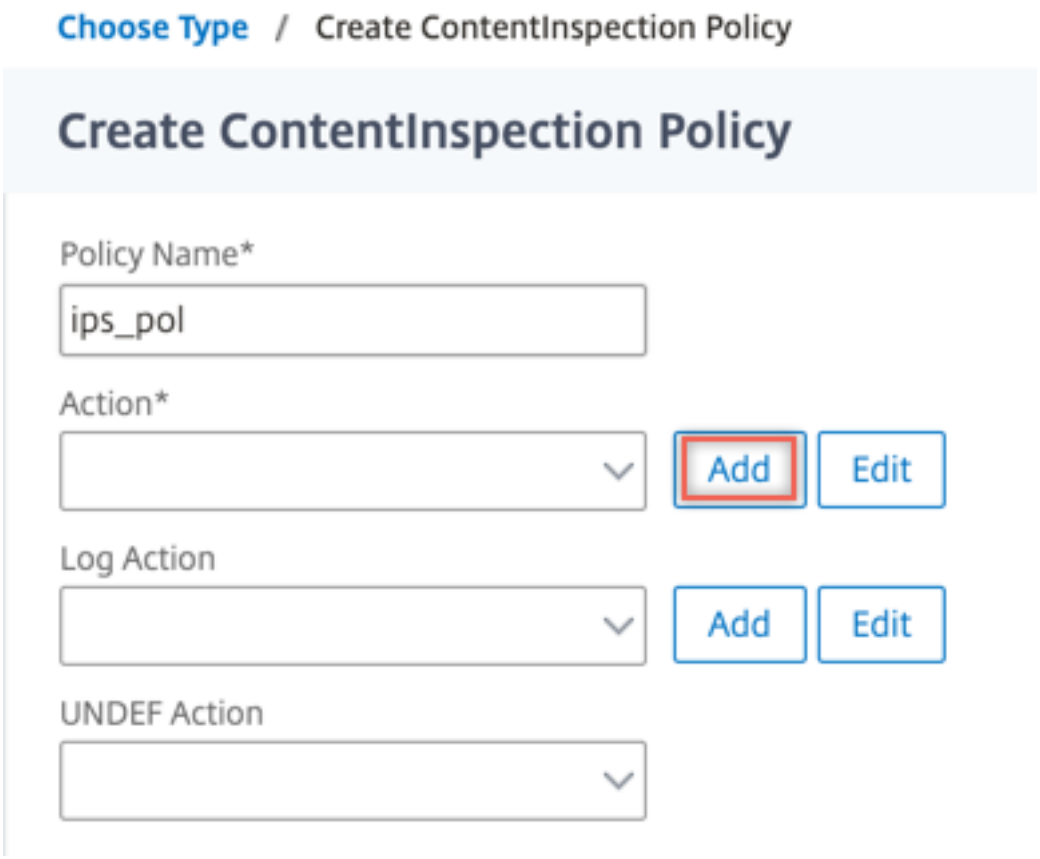
7. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



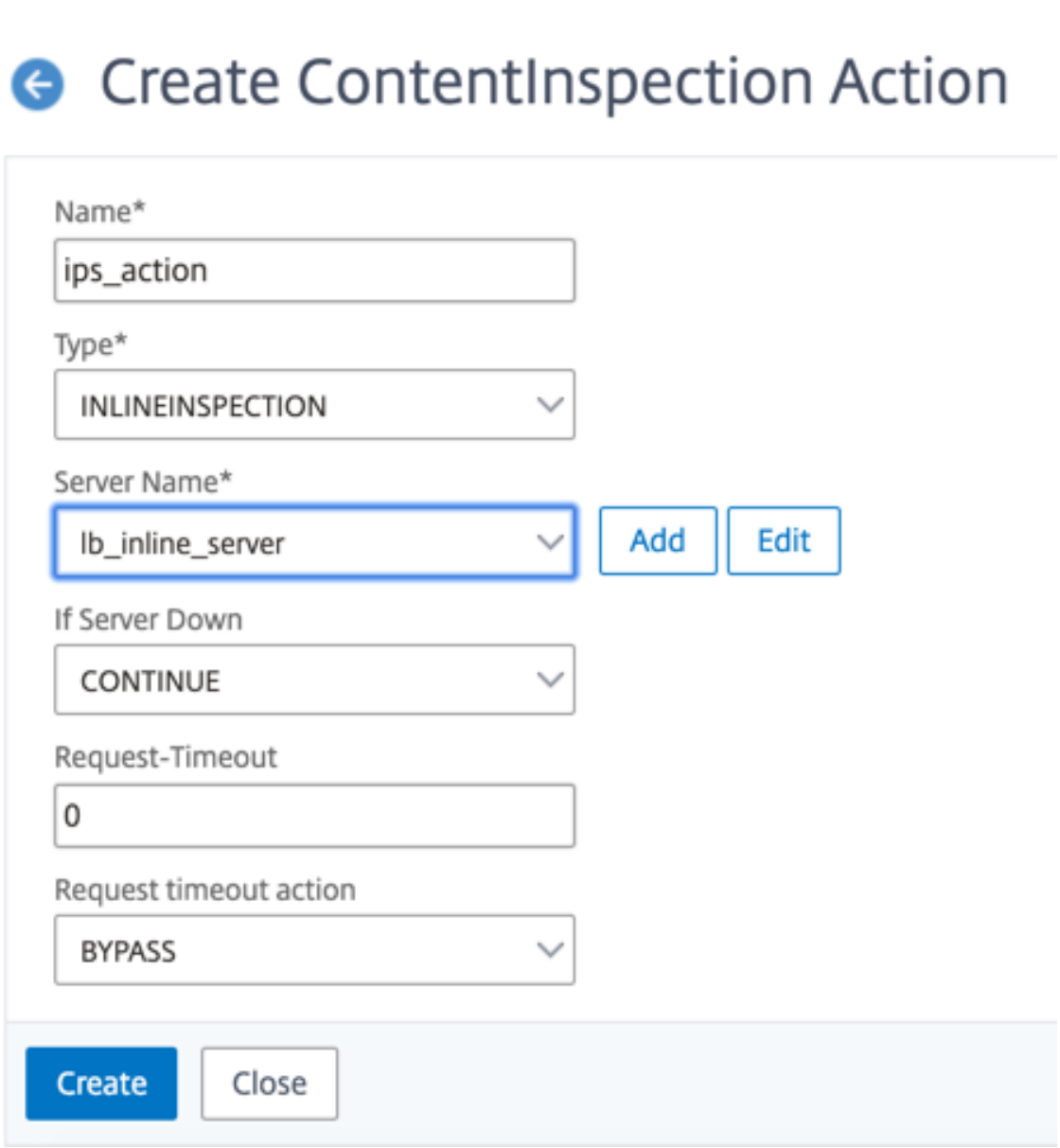
8. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



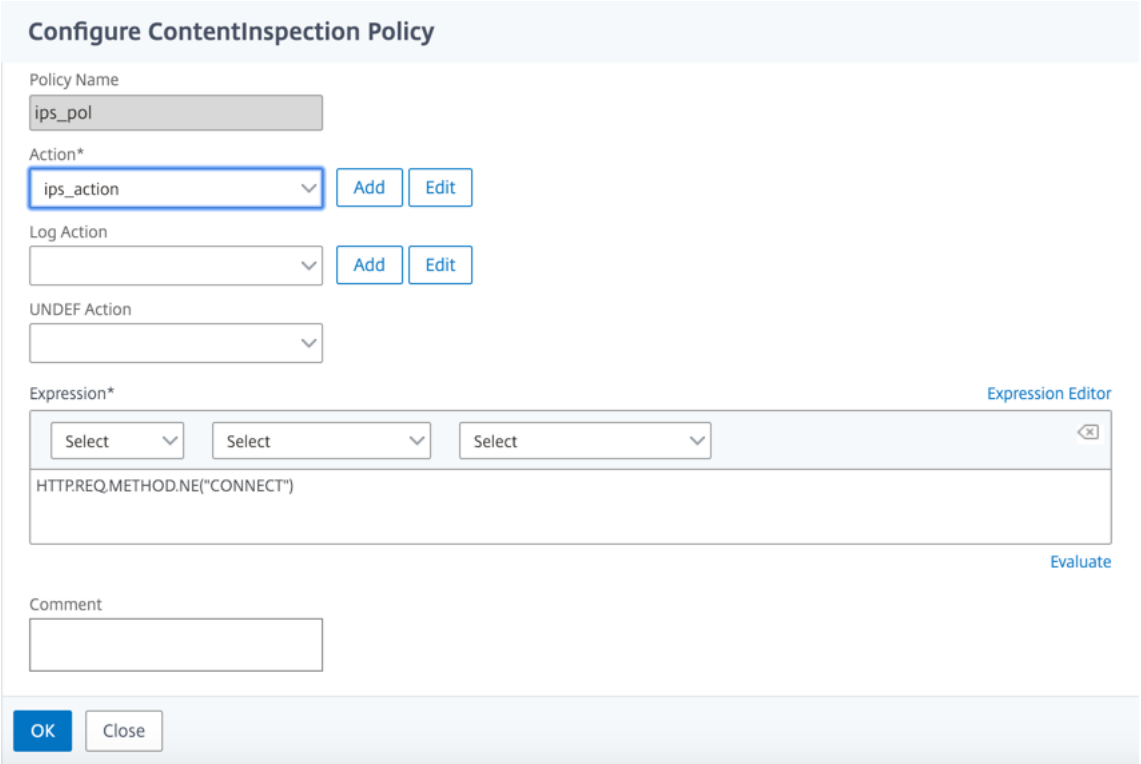
9. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



10. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie unter **Servername** den zuvor erstellten virtuellen Lastenausgleichsserver aus.



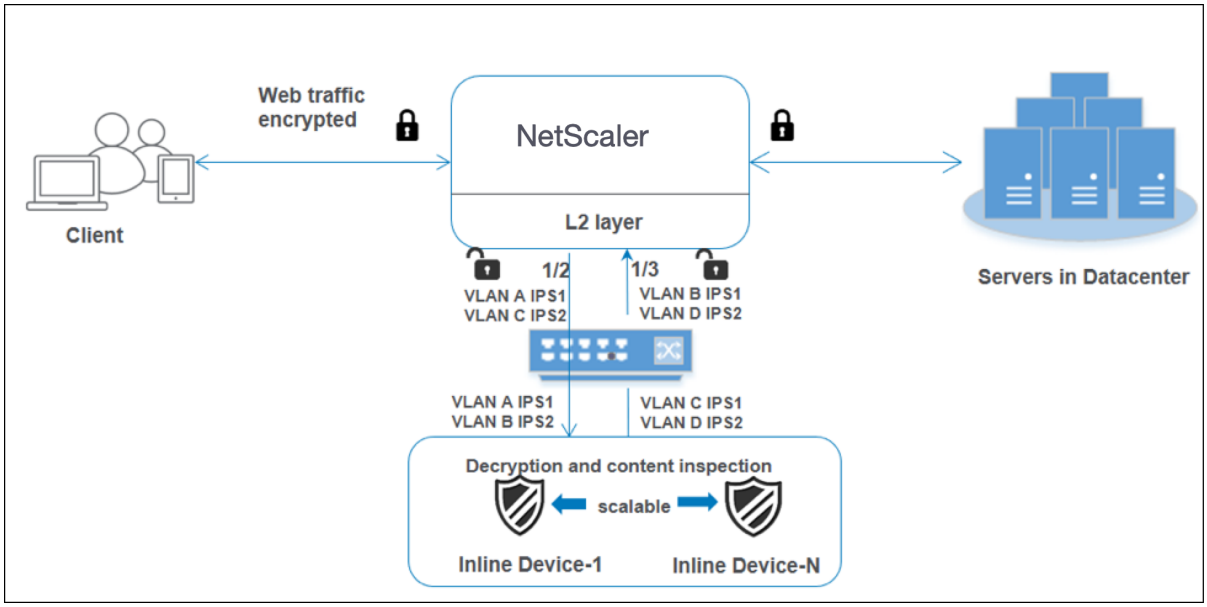
11. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



12. Klicken Sie auf **Bind**.
13. Klicken Sie auf **Fertig**.

Szenario 3: Lastausgleich mehrerer Inline-Geräte mit gemeinsamen Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, können Sie die Geräte mit verschiedenen Contentinspektionsdiensten mit gemeinsam genutzten Schnittstellen ausgleichen. In diesem Fall gleicht die SSL-Forward-Proxy-Appliance die Teilmenge des Datenverkehrs aus, der über eine gemeinsame Schnittstelle an jedes Gerät gesendet wird. Die Teilmenge wird basierend auf den konfigurierten Richtlinien festgelegt. Beispielsweise werden TXT- oder Bilddateien möglicherweise nicht zur Überprüfung an die Inline-Geräte gesendet.



Die Basiskonfiguration bleibt dieselbe wie in Szenario 2. Binden Sie für dieses Szenario die Schnittstellen an verschiedene VLANs, um den Datenverkehr für jedes Inline-Gerät zu trennen. Geben Sie die VLANs in den Content-Inspektionsprofilen an. Führen Sie die folgenden zusätzlichen Schritte aus:

1. Binden Sie die freigegebenen Schnittstellen an verschiedene VLANs.
2. Geben Sie die Ein- und Ausgangs-VLANs in den Content-Inspektionsprofilen an.

Konfiguration über die CLI

Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach jedem Befehl angegeben.

1. MBF aktivieren.

```
enable ns mode mbf
```

1. Aktivieren Sie das Feature.

```
enable ns feature contentInspection
```

1. Binden Sie die freigegebenen Schnittstellen an verschiedene VLANs.

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 100  - ifnum 1/2 tagged
bind vlan 200  - ifnum 1/3 tagged
bind vlan 300  - ifnum 1/2 tagged
bind vlan 400  - ifnum 1/3 tagged
```



```
<!--NeedCopy-->
```

1. Profil 1 für Service 1 hinzufügen. Geben Sie die Ein- und Aus-VLANs im Profil an.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof1 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 100 -ingressVlan 300
```

1. Profil 2 für Service 2 hinzufügen. Geben Sie die Ein- und Aus-VLANs im Profil an.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof2 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 200 -ingressVlan 400
```

1. Service 1 hinzufügen.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Service 2 hinzufügen.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Beispiel:

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Binden Sie die Dienste an den virtuellen Lastenausgleichsserver.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Beispiel:

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Beispiel:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu. Geben Sie die Inhaltsinspektionsaktion in der Richtlinie an.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Fügen Sie einen virtuellen Proxyserver hinzu.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Beispiel:

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

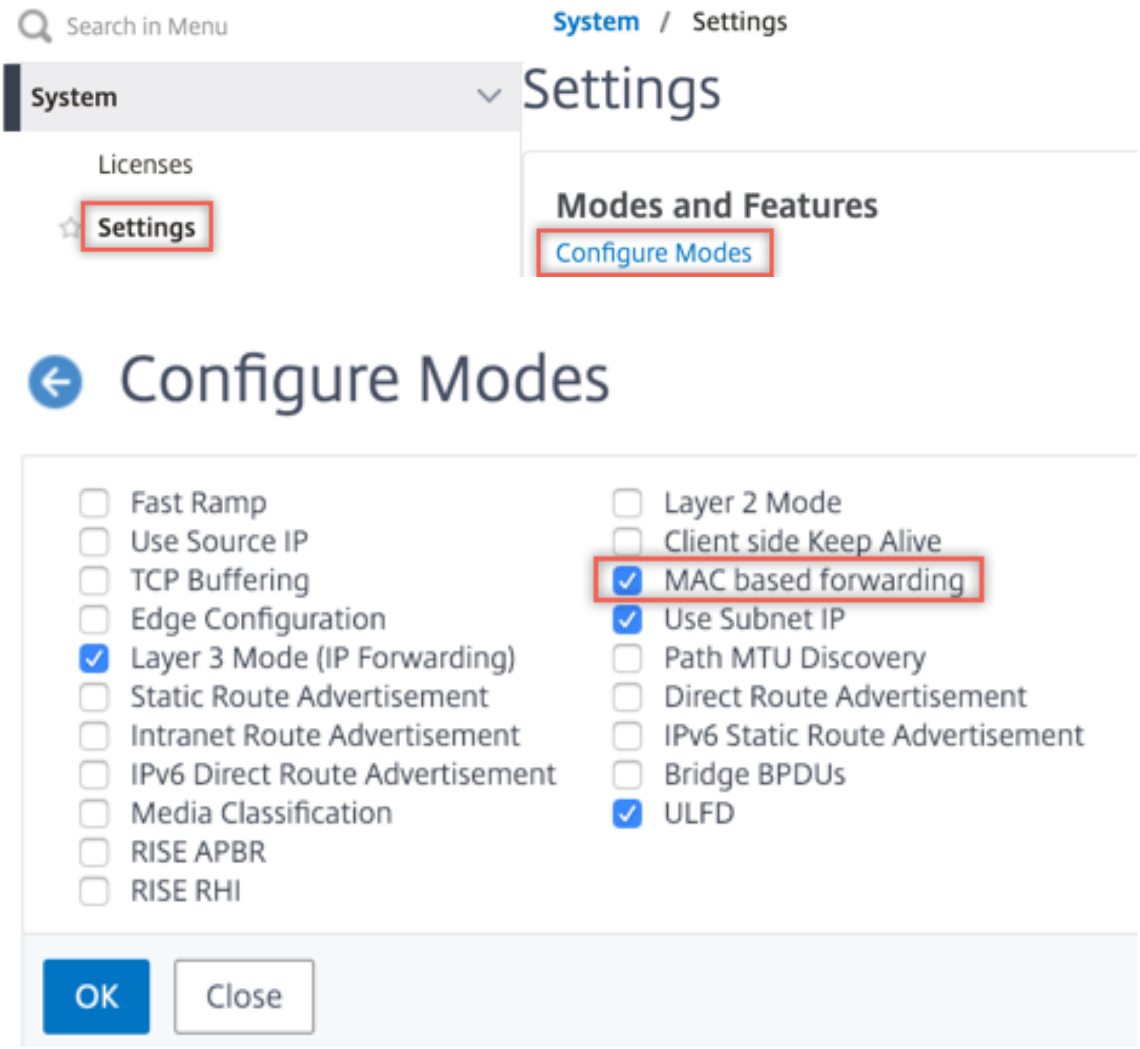
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Beispiel:

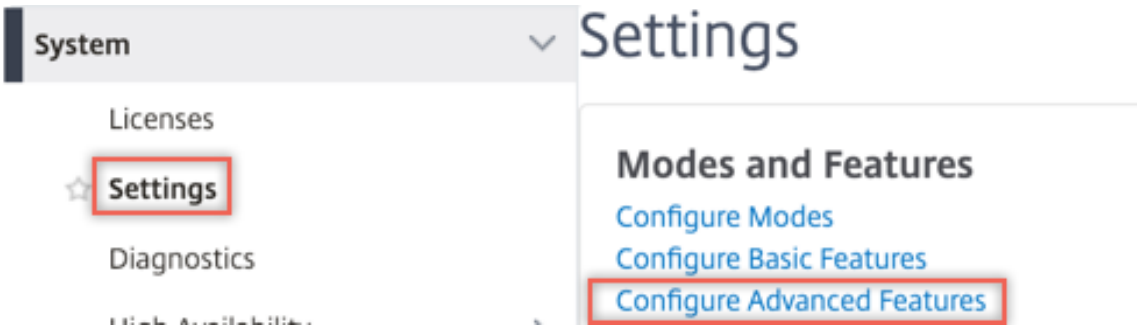
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

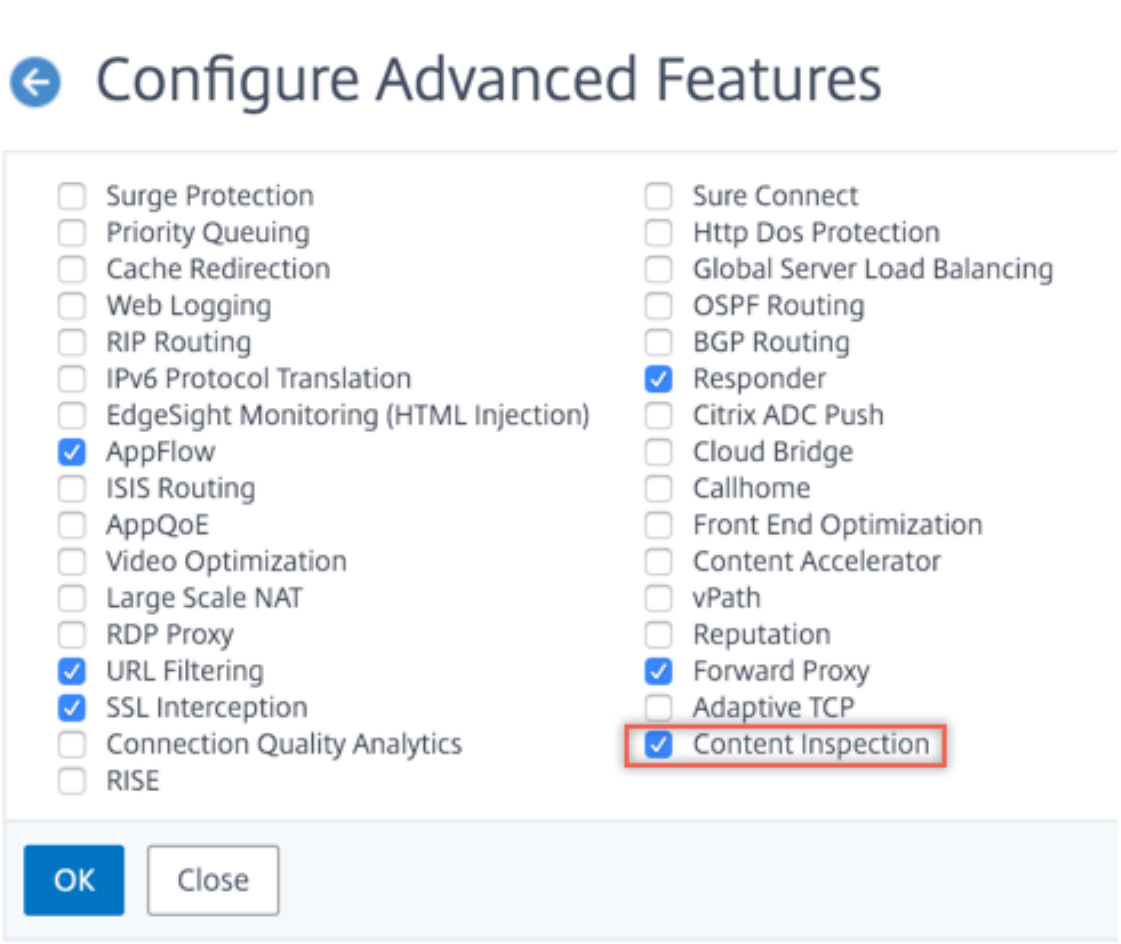
Konfiguration über die GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.

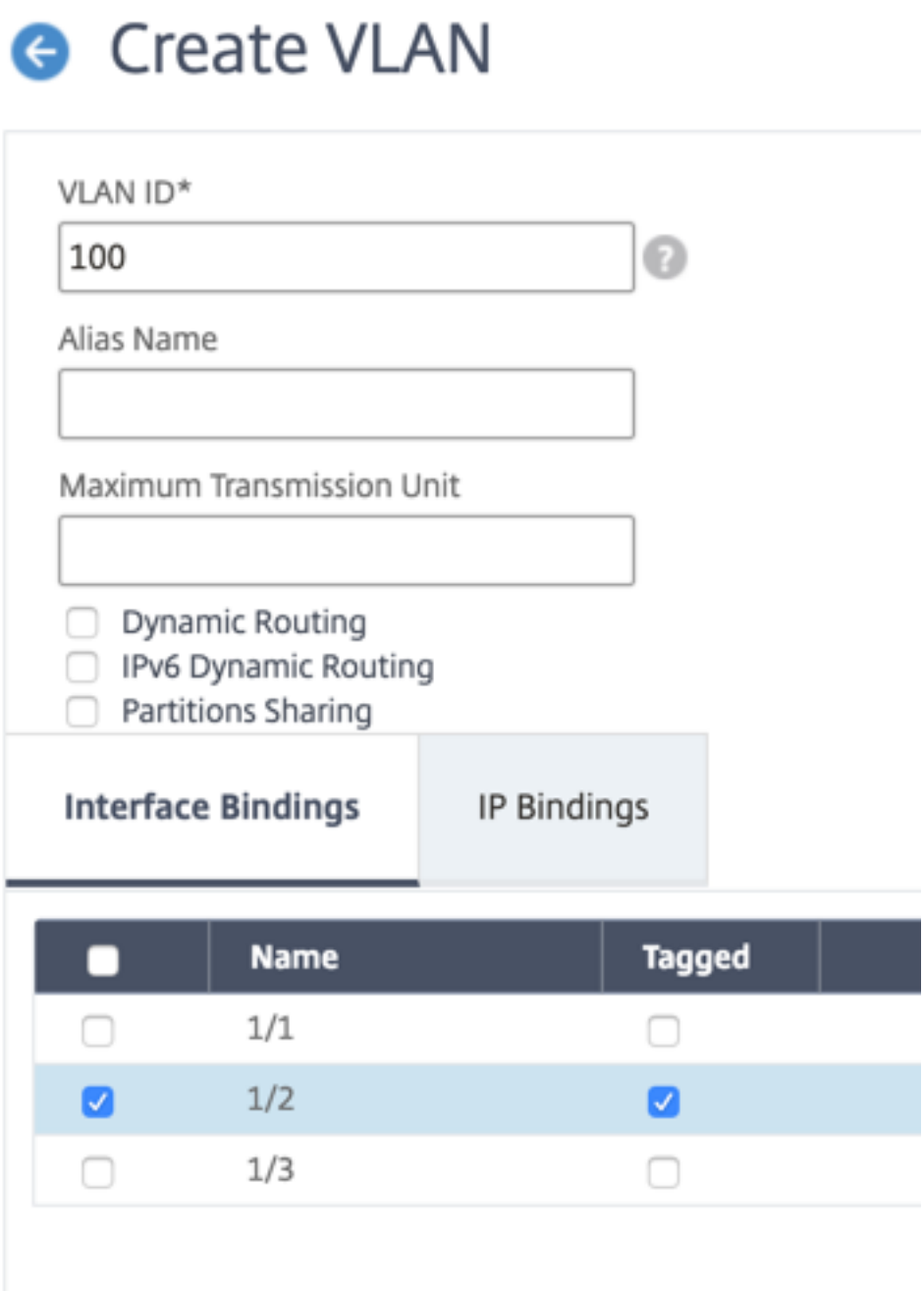


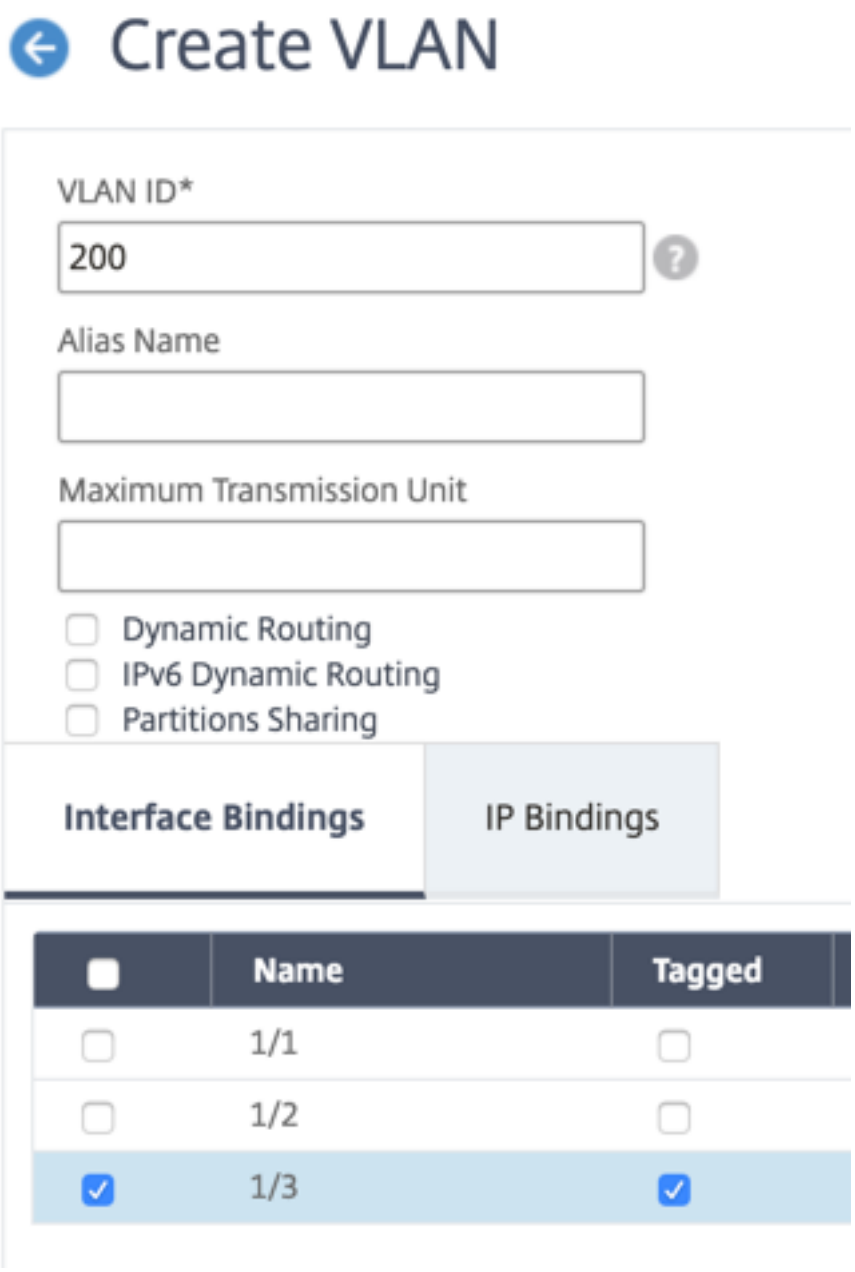
2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

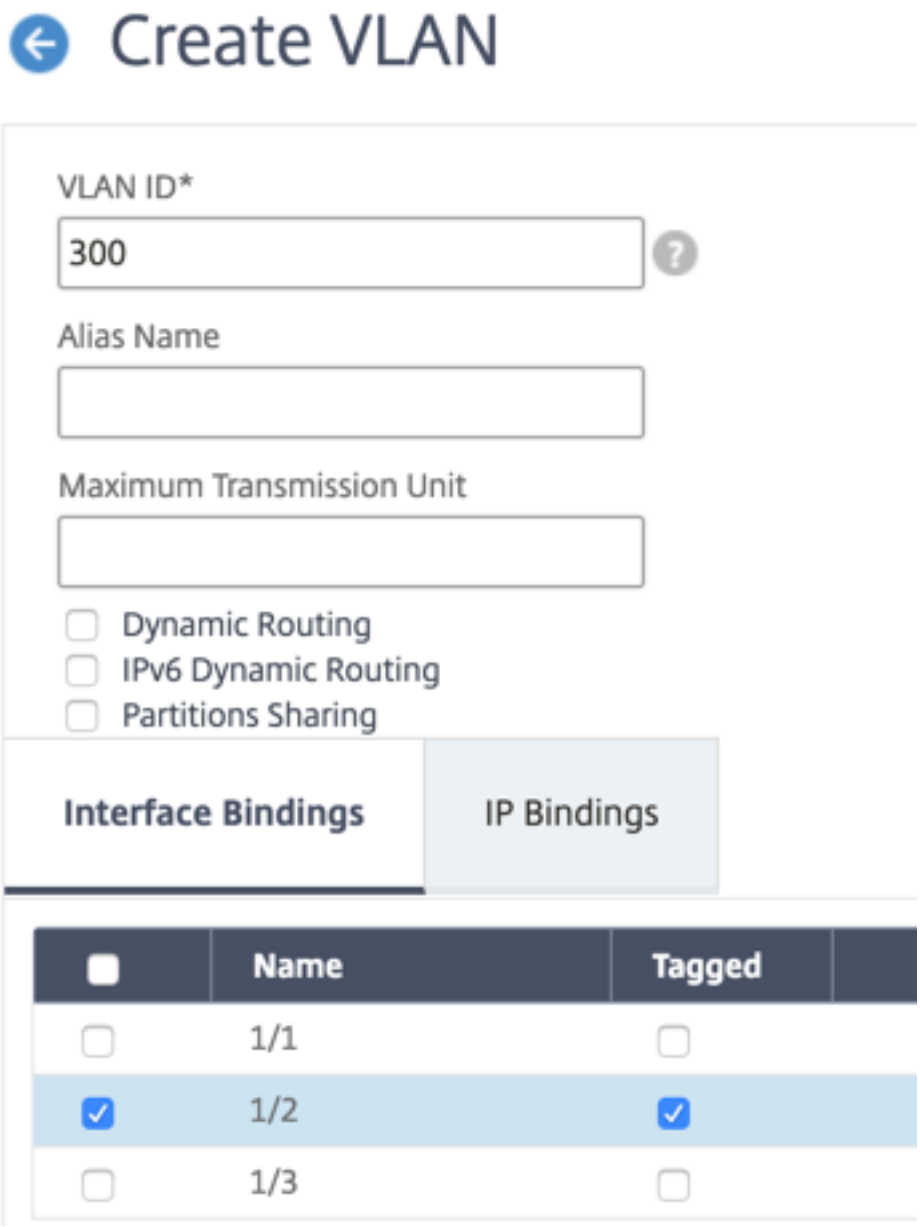


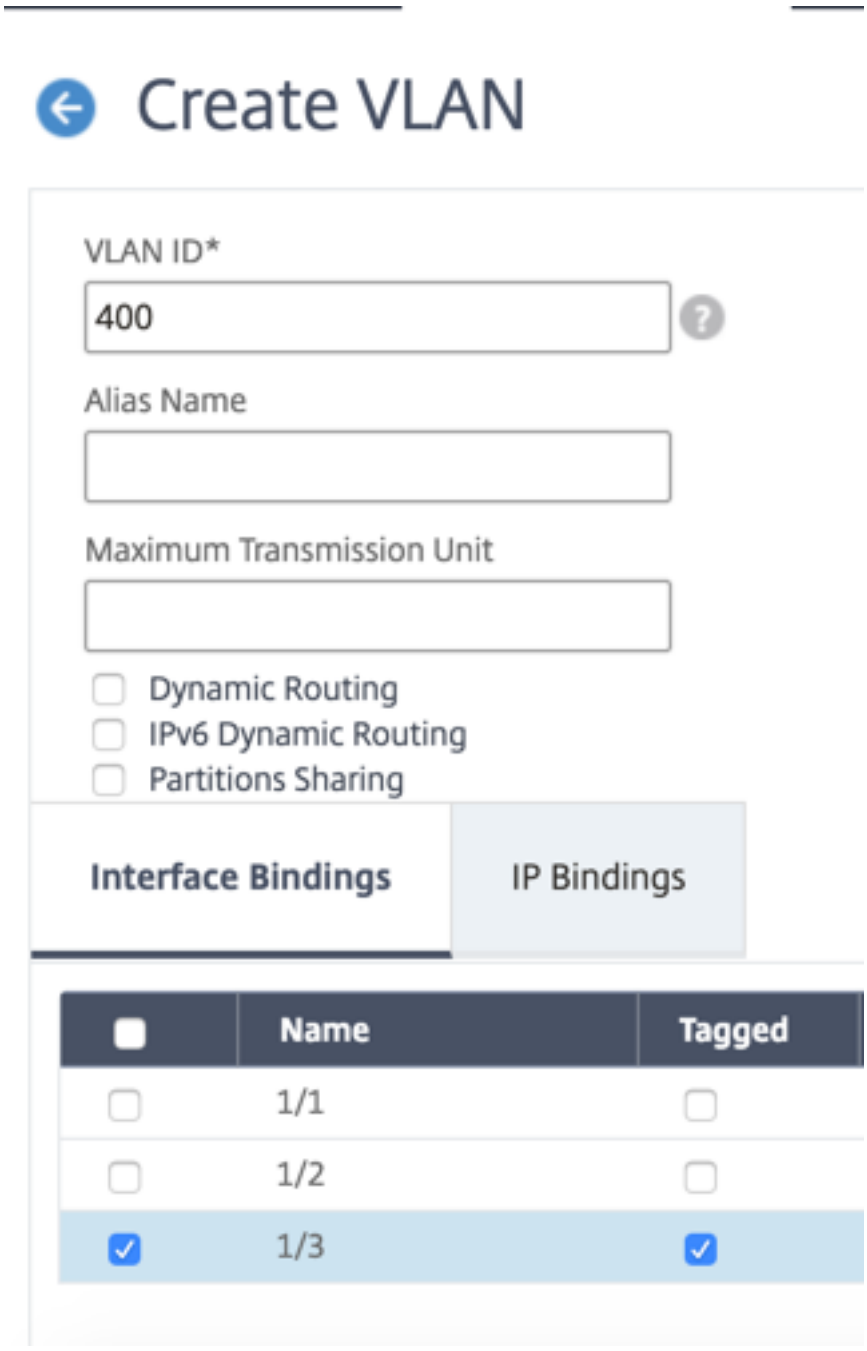


3. Navigieren Sie zu **System > Netzwerk > VLANs > Hinzufügen**. Fügen Sie vier VLANs hinzu und markieren Sie sie den Schnittstellen.

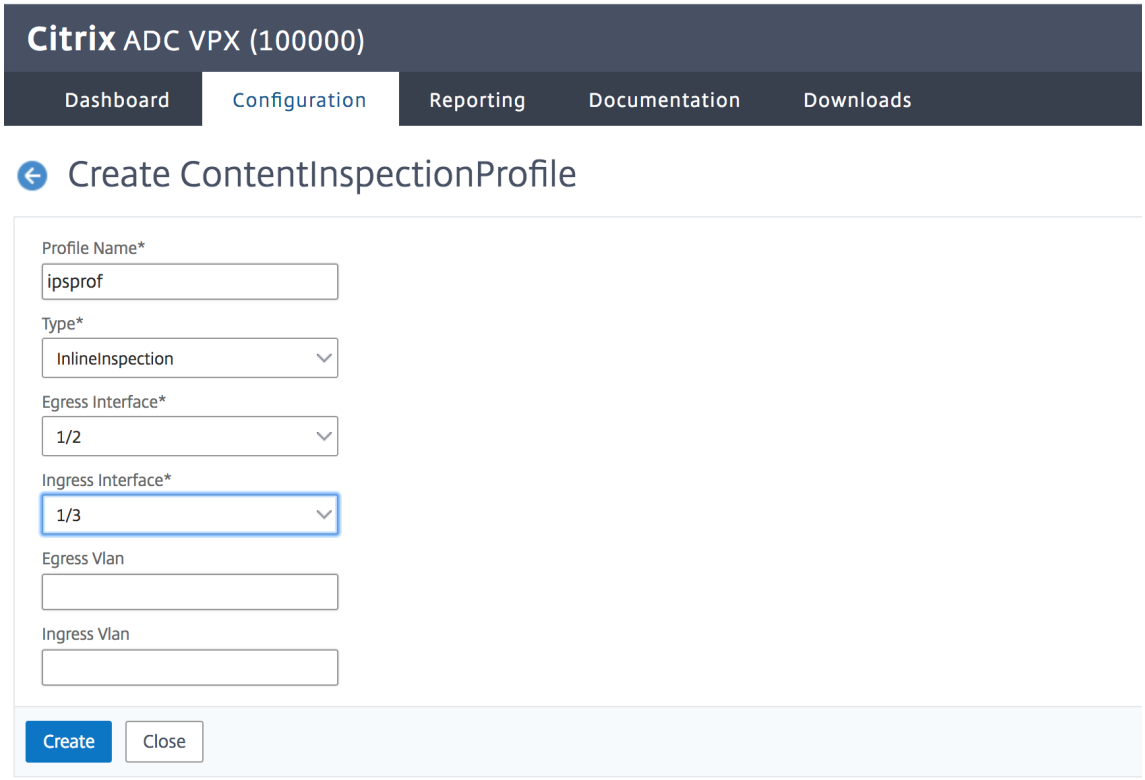




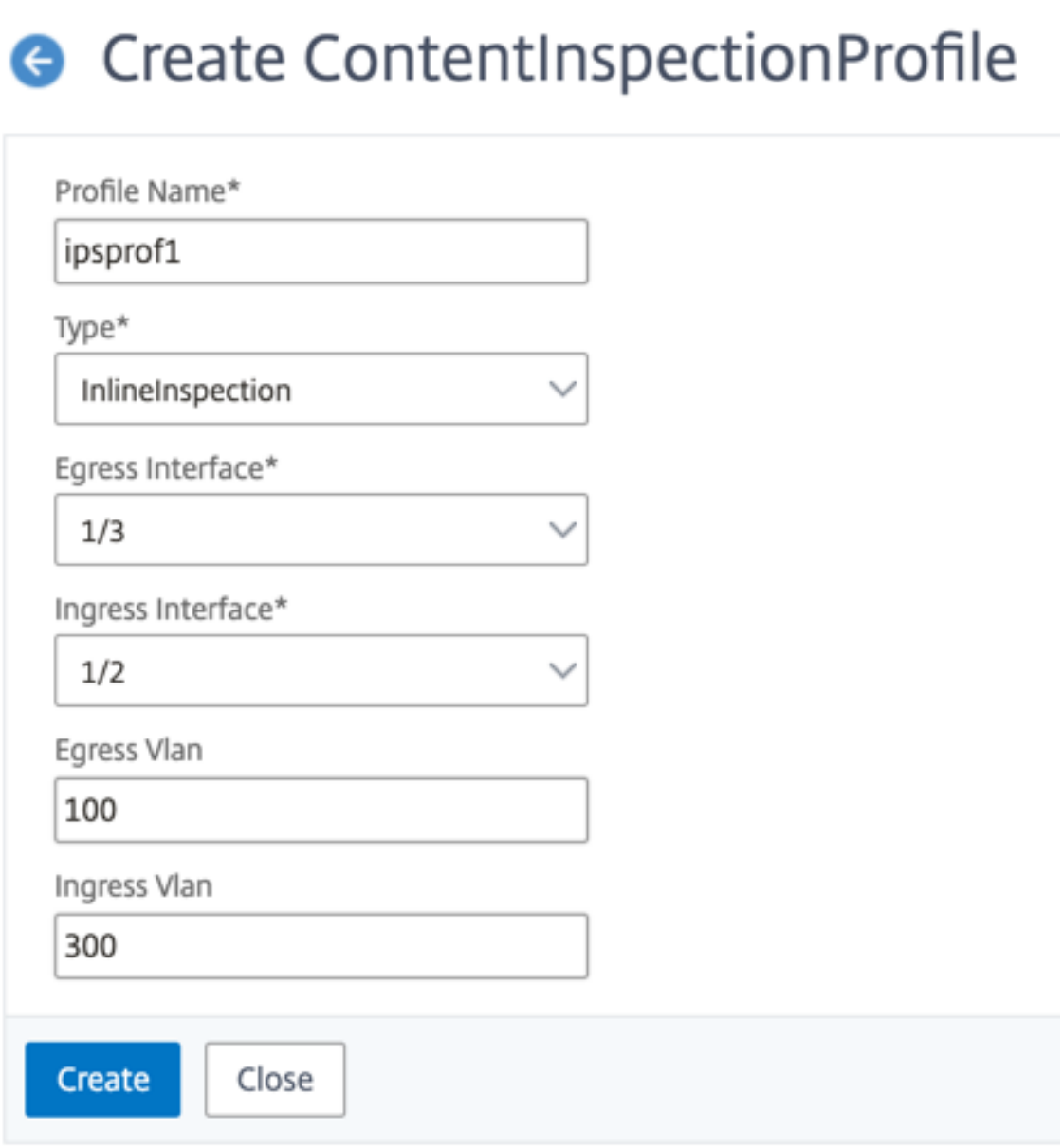




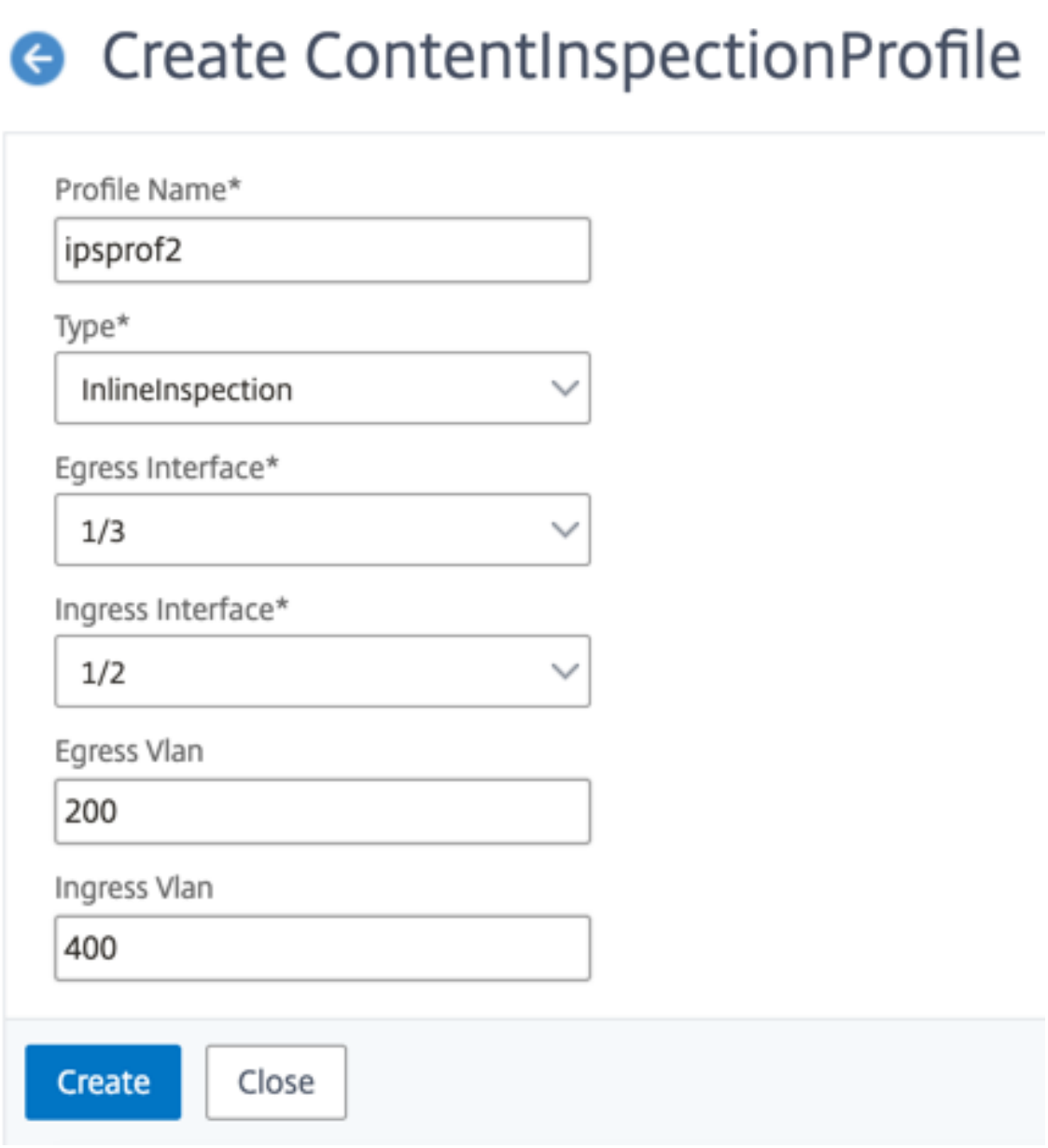
4. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.



Geben Sie die Ein- und Aus-VLANs an.

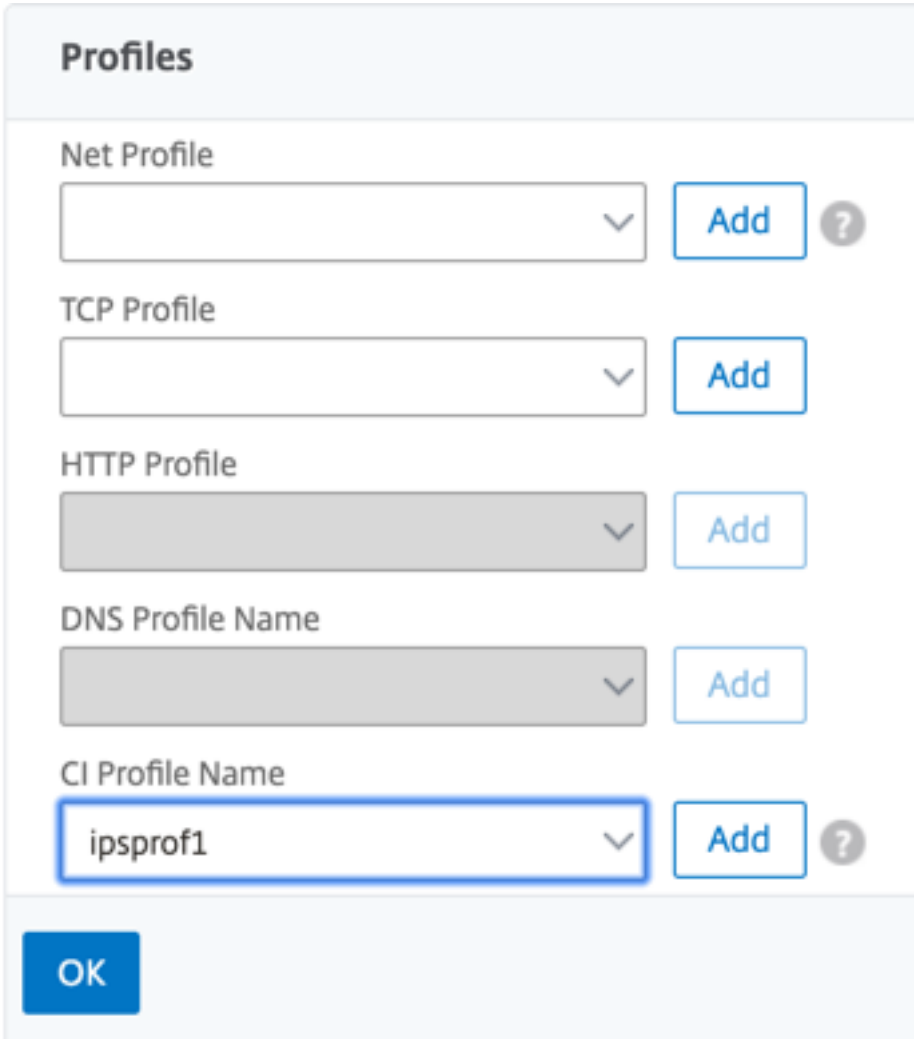


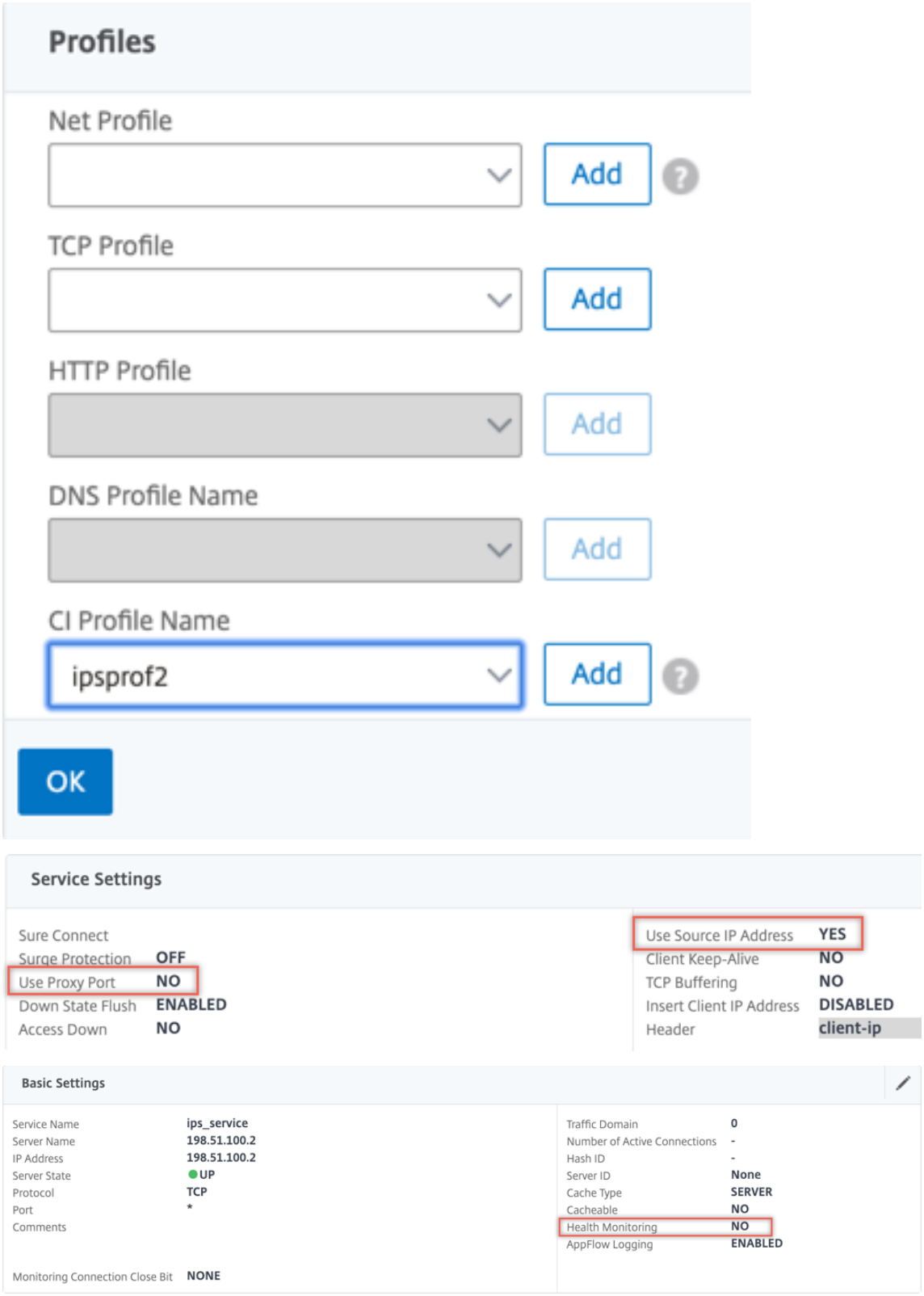
Erstellen Sie weitere Profile. Geben Sie im zweiten Profil ein anderes Ingress- und Egress-VLAN an.



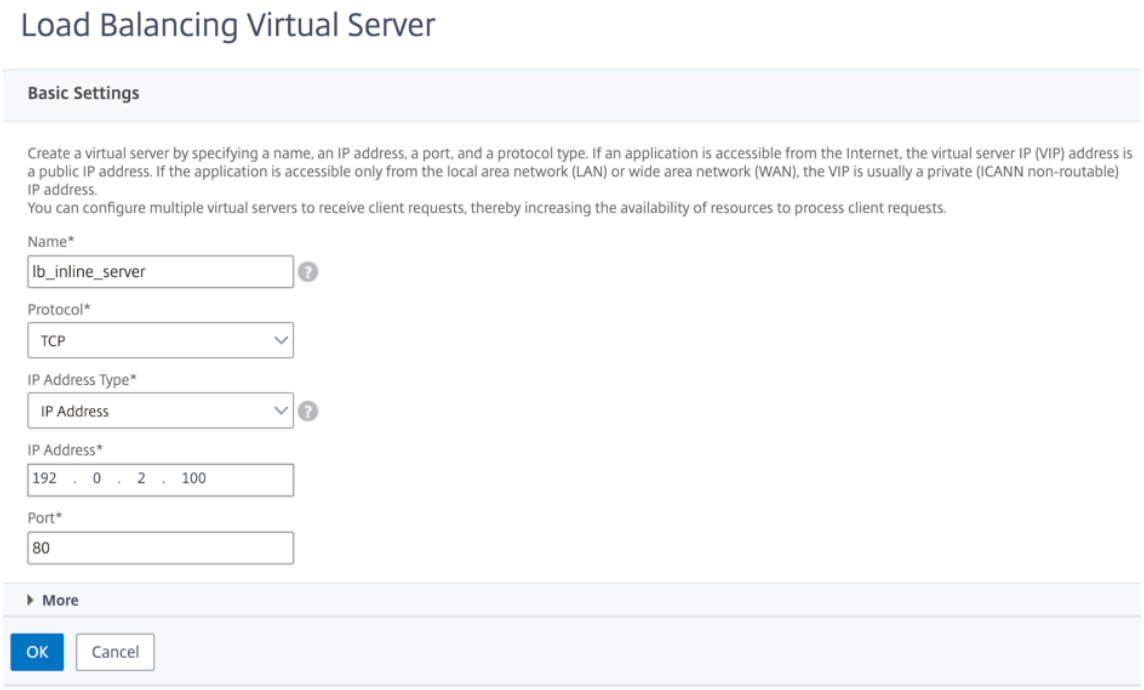
5. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest.

   Erstellen Sie zwei Dienste. Geben Sie Dummy-IP-Adressen an, die keinem der Geräte gehören, einschließlich der Inline-Geräte. Geben Sie Profil 1 in Dienst 1 und Profil 2 in Dienst 2 an.

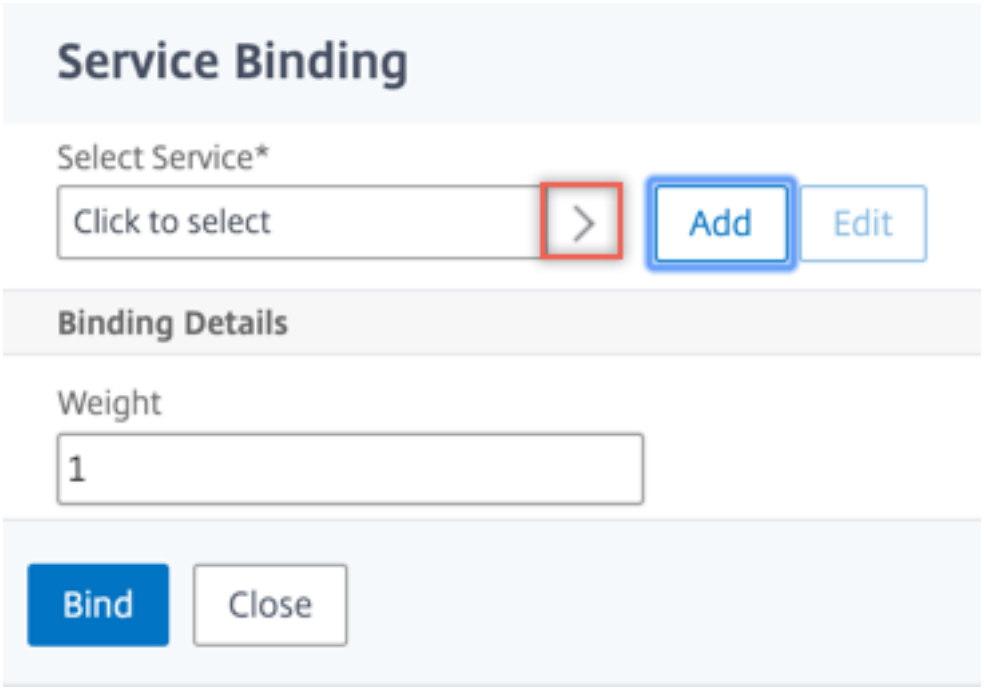


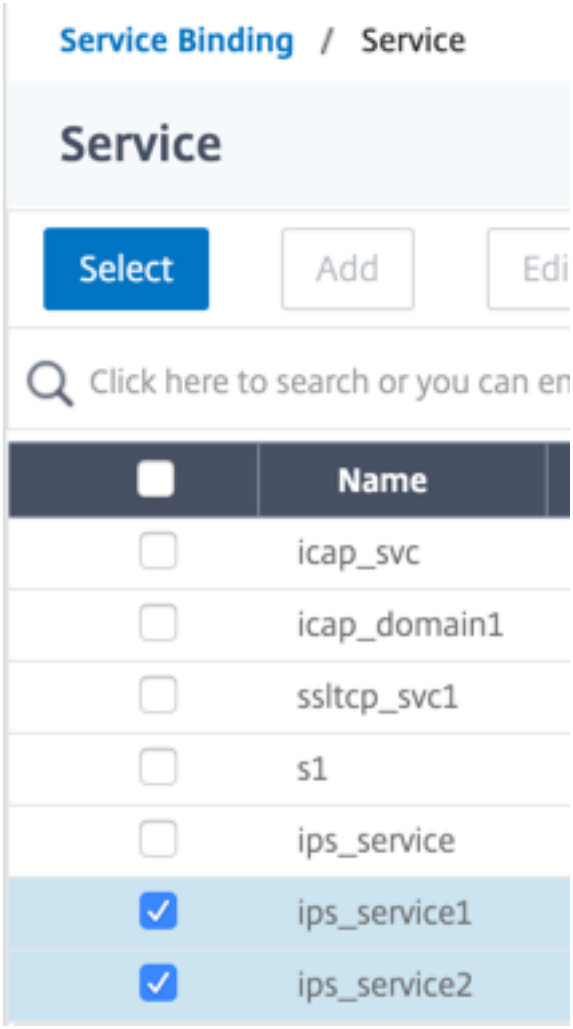


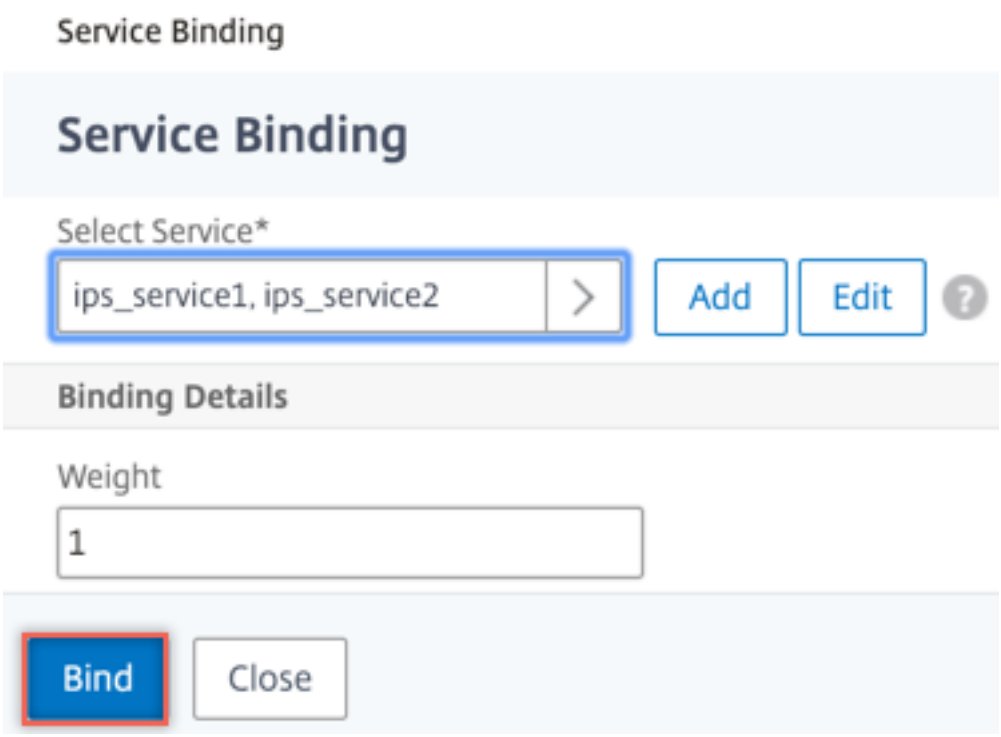
6. Navigieren Sie zu **Lastenausgleich > Virtuelle Server > Hinzufügen**. Erstellen Sie einen virtuellen TCP-Load Balancing Server.



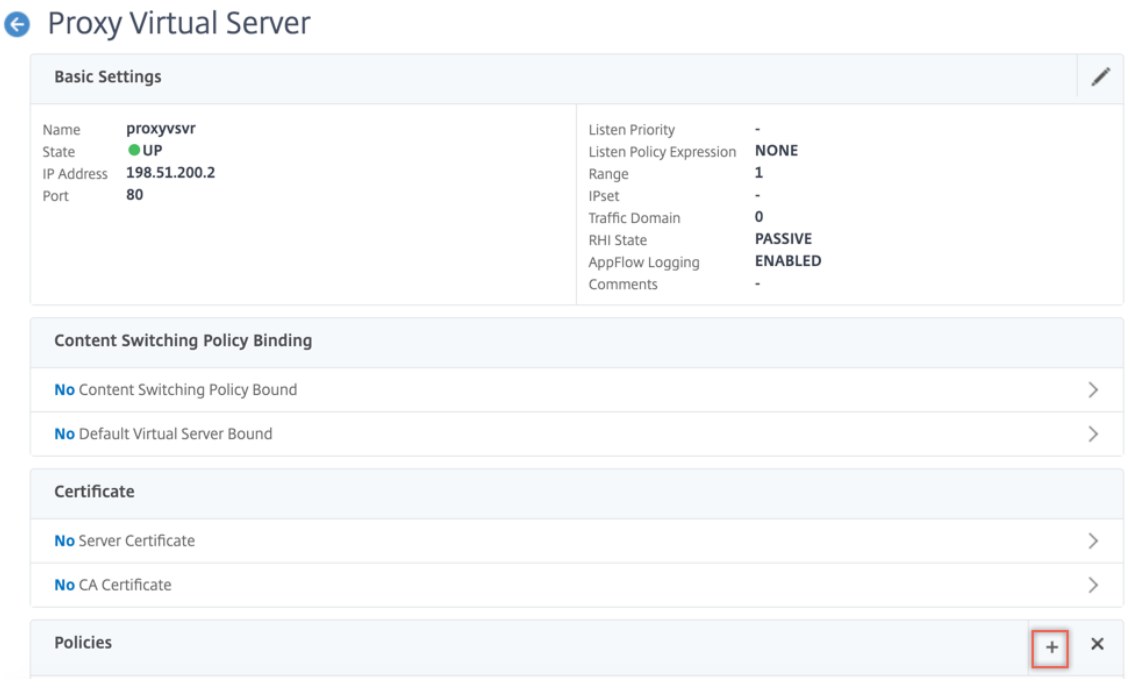
7. Klicken Sie auf **OK**.
8. Klicken Sie in den Abschnitt **Load Balancing Virtual Server Service Binding**. Klicken Sie unter **Dienstbindung** auf den Pfeil unter **Dienst auswählen**. Wählen Sie die beiden zuvor erstellten Dienste aus, und klicken Sie auf **Auswählen**. Klicken Sie auf **Bind**.



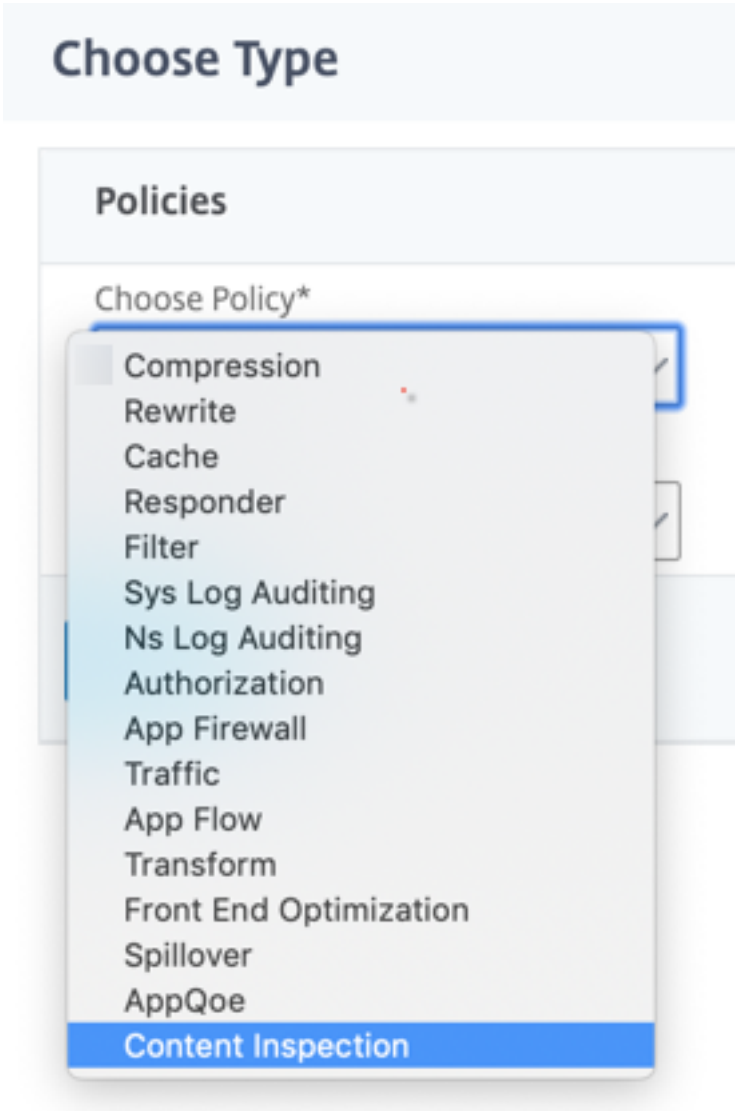




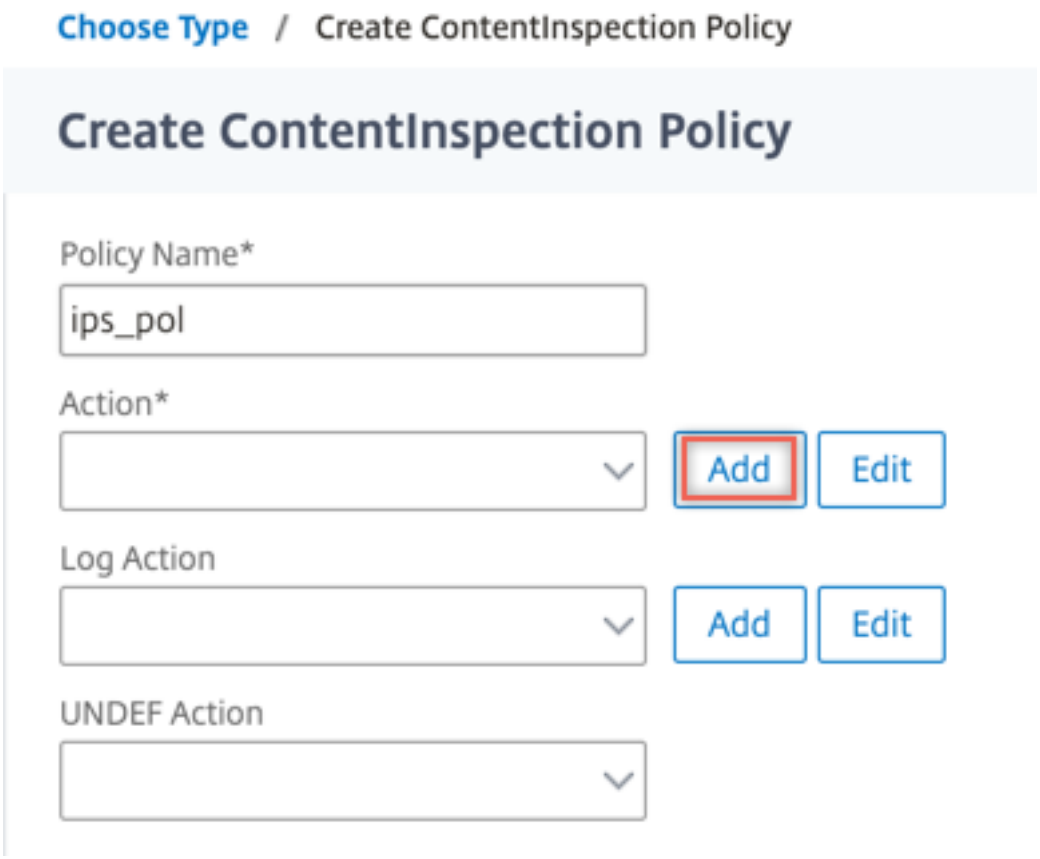
9. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



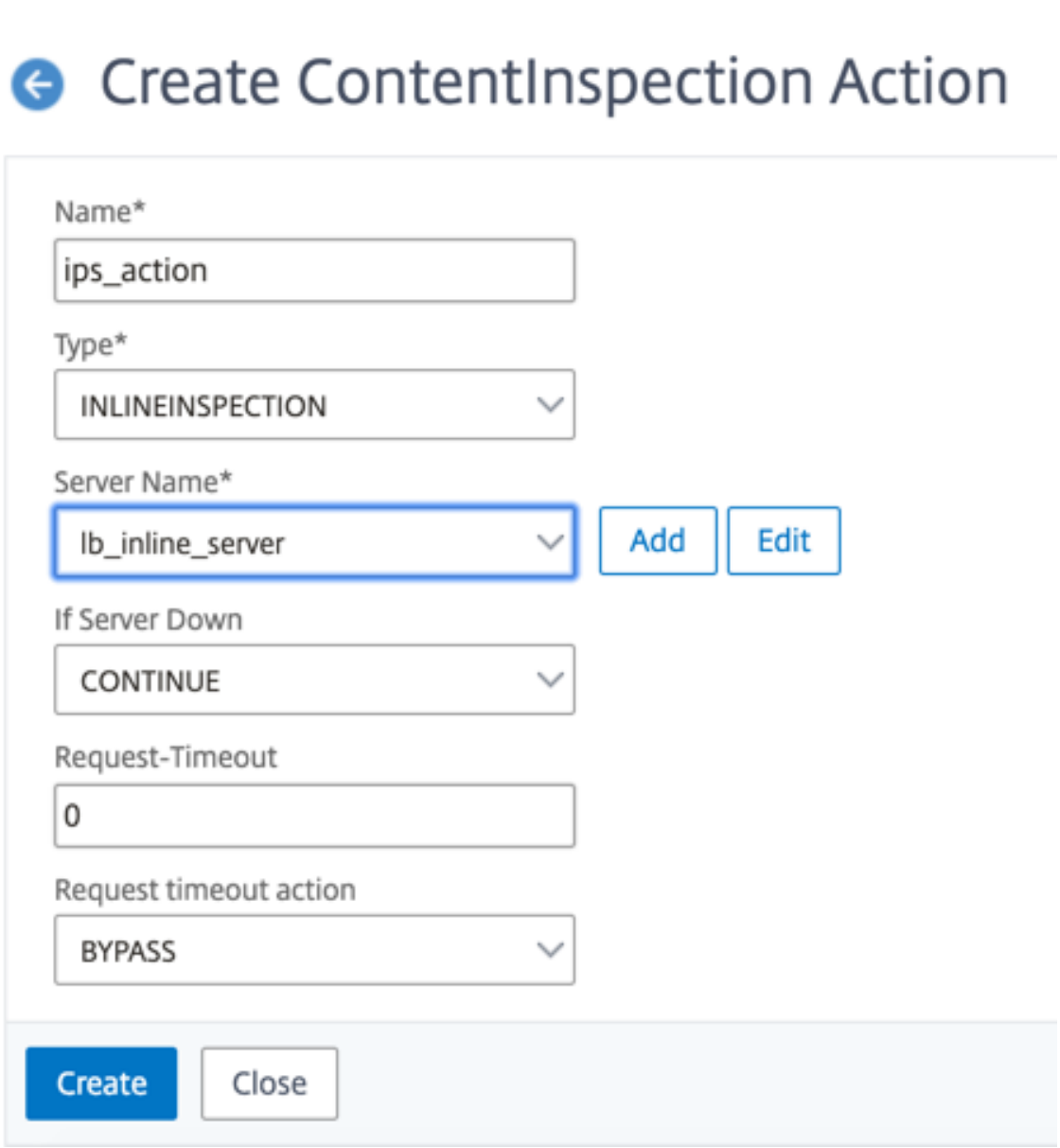
10. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



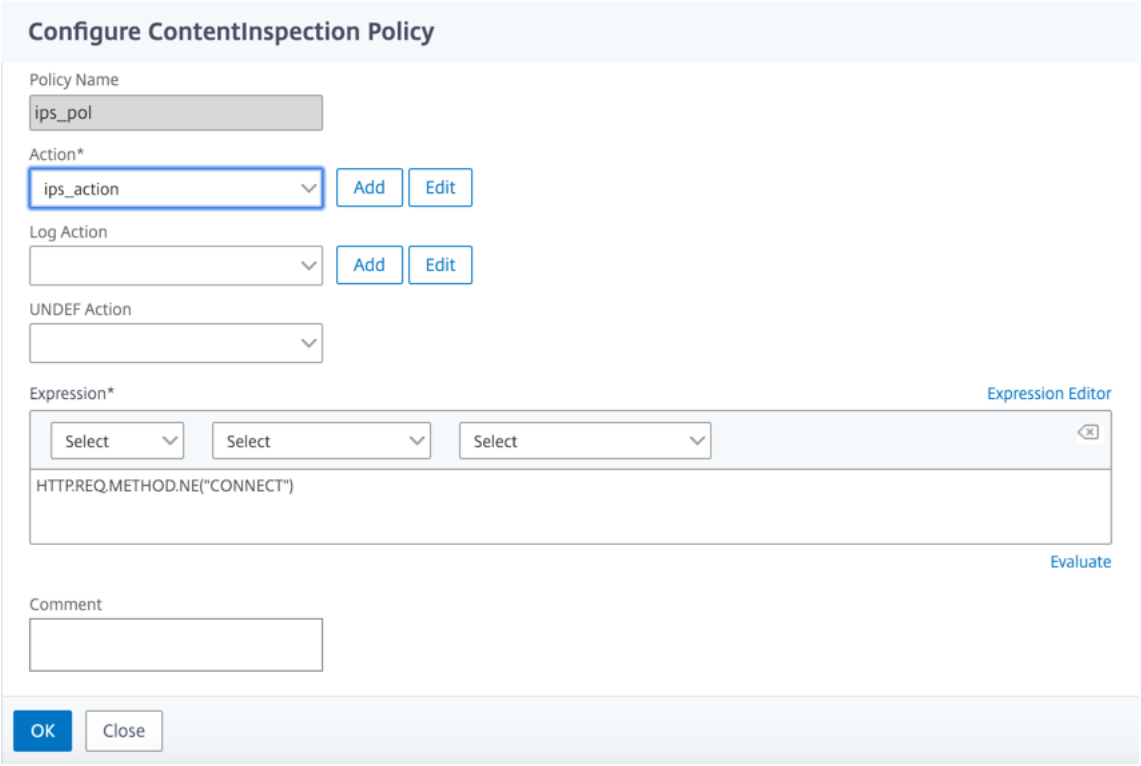
11. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



12. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie unter **Servername** den zuvor erstellten virtuellen Lastenausgleichsserver aus.



13. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



14. Klicken Sie auf **Bind**.
15. Klicken Sie auf **Fertig**.

Integrieren von NetScaler mit passiven Sicherheitsgeräten (Intrusion Detection System)

May 11, 2023

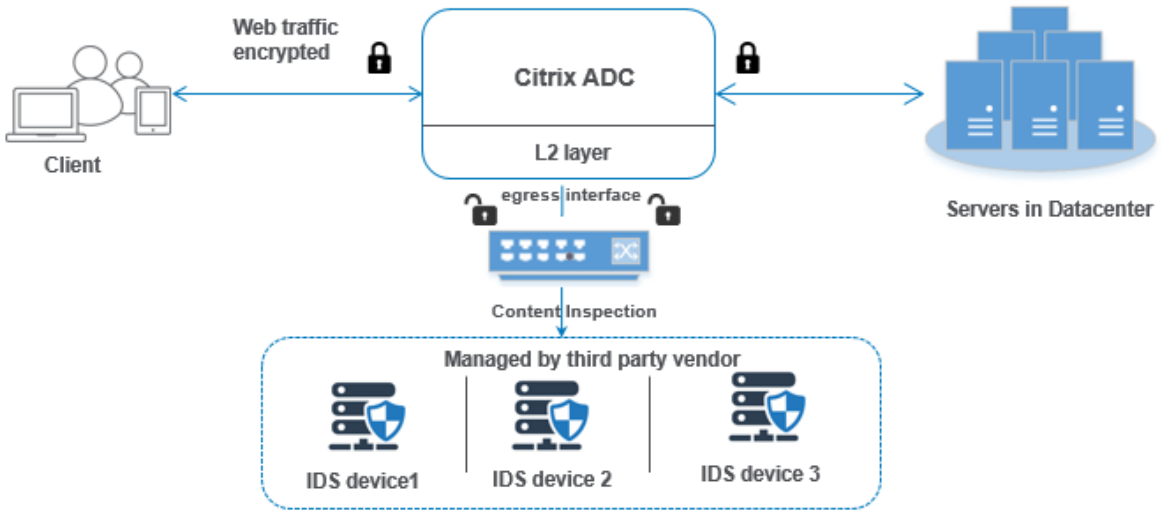
Eine NetScaler-Appliance ist jetzt in passive Sicherheitsgeräte wie das Intrusion Detection System (IDS) integriert. Diese passiven Geräte speichern Protokolle und lösen Warnungen aus, wenn sie einen schlechten oder nicht konformen Datenverkehr erkennen. Es generiert auch Berichte für den Compliance-Zweck. Wenn die NetScaler-Appliance in zwei oder mehr IDS-Geräte integriert ist und wenn ein hohes Verkehrsaufkommen vorhanden ist, kann die Appliance die Geräte ausgleichen, indem der Datenverkehr auf virtueller Serverebene geklont wird.

Für erweiterten Sicherheitsschutz ist eine NetScaler-Appliance in passive Sicherheitsgeräte wie IDS integriert, die im Nur-Erkennungsmodus bereitgestellt werden. Diese Geräte speichern Protokolle und lösen Warnungen aus, wenn ein schlechter oder nicht konformer Datenverkehr festgestellt wird. Es generiert auch Berichte für den Compliance-Zweck. Im Folgenden sind einige der Vorteile der Integration des NetScaler in ein IDS-Gerät aufgeführt.

- **Überprüfung des verschlüsselten Datenverkehrs**. Die meisten Sicherheitsgeräte Bypass den verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe sind. Eine NetScaler-Appliance kann den Datenverkehr entschlüsseln und an IDS-Geräte senden, um die Netzwerksicherheit des Kunden zu verbessern.
- **Entladen von Inline-Geräten von der TLS/SSL-Verarbeitung**. Die TLS/SSL-Verarbeitung ist teuer und führt zu einer hohen System-CPU in Intrusion-Detection-Geräten, wenn sie den Datenverkehr entschlüsseln. Da der verschlüsselte Datenverkehr schnell zunimmt, können diese Systeme den verschlüsselten Datenverkehr nicht entschlüsseln und überprüfen. NetScaler hilft beim Auslagern des Datenverkehrs von der TLS/SSL-Verarbeitung auf IDS-Geräte. Diese Art der Datenauslagerung führt dazu, dass ein IDS-Gerät ein hohes Verkehrsaufkommen unterstützt.
- **Laden ausgleichender IDS-Geräte**. Die NetScaler-Appliance gleicht mehrere IDS-Geräte aus, wenn ein hohes Verkehrsaufkommen besteht, indem der Datenverkehr auf virtueller Serverebene geklont wird.
- **Replikation des Datenverkehrs auf passive Geräte**. Der in die Appliance fließende Datenverkehr kann auf andere passive Geräte repliziert werden, um Konformitätsberichte zu erstellen. Zum Beispiel schreiben nur wenige Regierungsbehörden vor, dass jede Transaktion in einigen passiven Geräten protokolliert wird.
- **Fächern des Datenverkehrs zu mehreren passiven Geräten**. Einige Kunden ziehen es vor, eingehenden Datenverkehr auf mehrere passive Geräte aufzufächern oder zu replizieren.
- **Intelligente Auswahl des Verkehrs**. Jedes Paket, das in die Appliance fließt, muss möglicherweise nicht inhaltlich geprüft werden, z. B. Der Benutzer kann die NetScaler-Appliance so konfigurieren, dass ein bestimmter Datenverkehr (z. B. EXE-Dateien) zur Überprüfung ausgewählt und der Datenverkehr zur Datenverarbeitung an IDS-Geräte gesendet wird.

Wie NetScaler in ein IDS-Gerät mit L2-Konnektivität integriert ist

Das folgende Diagramm zeigt, wie IDS in eine NetScaler-Appliance integriert ist.



Die Wechselwirkung der Komponenten ist wie folgt gegeben:

1. Ein Client sendet eine HTTP/HTTPS-Anforderung an die NetScaler-Appliance.
2. Die Appliance fängt den Datenverkehr ab und repliziert ihn auf ein IDS-Gerät basierend auf der Bewertung der Inhaltsüberprüfungsrichtlinie.
3. Wenn der Datenverkehr verschlüsselt ist, entschlüsselt die Appliance die Daten und sendet sie als Nur-Text.
4. Basierend auf der Bewertung der Richtlinien wendet die Appliance eine Inhaltsinspektionsaktion vom Typ “MIRROR” an
5. In der Aktion ist der IDS-Dienst oder der Lastausgleichsdienst (für mehrere IDS-Geräteintegrationen) konfiguriert.
6. Das IDS-Gerät ist auf der Appliance als Content-Inspection-Diensttyp “Beliebig” konfiguriert. Der Inhaltsinspektionsdienst wird dann dem Inhaltsinspektionsprofil vom Typ “MIRROR” zugeordnet, das die Ausgangsschnittstelle angibt, über die die Daten an das IDS-Gerät weitergeleitet werden müssen. Optional können Sie auch ein VLAN-Tag im Inhaltsüberprüfungsprofil konfigurieren.

   > **Hinweis:**
   >
   > - Die für den IDS-Dienst oder -Server verwendete IP-Adresse ist eine Dummy-Adresse.
   > - Die NetScaler-Appliance unterstützt keinen LA-Kanal für die Ausgangsschnittstelle.

7. Die Appliance repliziert dann die Daten über die Ausgangsschnittstelle auf ein oder mehrere IDS-Geräte.
8. Wenn der Back-End-Server eine Antwort an den NetScaler sendet, repliziert die Appliance die Daten und leitet sie an das IDS-Gerät weiter.

9. Wenn Ihre Appliance in ein oder mehrere IDS-Geräte integriert ist und Sie den Lastausgleich der Geräte bevorzugen, können Sie den virtuellen Lastausgleichsserver verwenden.

Softwarelizenzierung

Um die Inline-Gerätintegration bereitzustellen, muss Ihre NetScaler-Appliance mit einer der folgenden Lizenzen ausgestattet sein:

1. ADC Premium
2. ADC Advanced
3. Telco Fortgeschrittene
4. Telco Premium

Konfigurieren der Einbruchmelde-Systemintegration

Sie können das IDS-Gerät auf zwei verschiedene Arten in den NetScaler integrieren.

Szenario 1: Integration mit einem einzigen IDS-Gerät

Im Folgenden sind die Schritte aufgeführt, die Sie mithilfe der Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsüberprüfung aktivieren
2. Inhaltsüberprüfungsprofil vom Typ MIRROR für den Dienst, der das IDS-Gerät
3. IDS-Dienst vom Typ “ANY” hinzufügen
4. Inhaltsüberprüfungsaktion vom Typ “MIRROR” hinzugefügt
5. Inhaltsüberprüfungsrichtlinie für die IDS-Überprüfung hinzufügen
6. Binden Sie die Inhaltsüberprüfungsrichtlinie an den virtuellen Content Switching- oder Lastausgleichsdienst des Typs HTTP/SSL

Inhaltsüberprüfung aktivieren

Wenn Sie möchten, dass die NetScaler-Appliance den Inhalt zur Überprüfung an die IDS-Geräte sendet, müssen Sie die Funktionen Inhaltsüberprüfung und den Lastausgleich unabhängig von der Entschlüsselung aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature contentInspection LoadBalancing
```

Inhaltsinspektionsprofil vom Typ “MIRROR”

Das Inhaltsinspektionsprofil vom Typ “MIRROR” erklärt, wie Sie eine Verbindung zum IDS-Gerät herstellen können.
Geben Sie an der Eingabeaufforderung ein.

```
add contentInspection profile <name> -type MIRROR -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 10
```

IDS-Dienst hinzufügen

Sie müssen einen Dienst vom Typ “ANY” für jedes IDS-Gerät konfigurieren, das in die Appliance integriert ist. Der Dienst hat die IDS-Gerätekonfigurationsdetails. Der Dienst stellt das IDS-Gerät dar.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Inhaltsüberprüfungsaktion vom Typ MIRROR für IDS-Dienst hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert und anschließend das IDS-Profil und den Dienst hinzugefügt haben, müssen Sie die Aktion Inhaltsüberprüfung für die Bearbeitung der Anforderung hinzufügen. Basierend auf der Inhaltsüberprüfungsaktion kann die Appliance Daten löschen, zurücksetzen, blockieren oder an das IDS-Gerät senden.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Inhaltsüberprüfungsrichtlinie für die IDS-Überprüfung hinzufügen

Nachdem Sie eine Inhaltsüberprüfungsaktion erstellt haben, müssen Sie Richtlinien für die Inhaltsüberprüfung hinzufügen, um Überprüfungsanfragen zu bewerten. Die Richtlinie basiert auf einer

Regel, die aus einem oder mehreren Ausdrücken besteht. Die Richtlinie bewertet und wählt den zu überprüfenden Verkehr basierend auf der Regel aus.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Binden Sie die Inhaltsüberprüfungsrichtlinie an den virtuellen Content Switching- oder Lastausgleichsdienst des Typs HTTP/SSL

Um den Webverkehr zu empfangen, müssen Sie einen virtuellen Lastausgleichsserver hinzufügen. Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Binden der Richtlinie zur Inhaltsüberprüfung an den virtuellen Server mit Content Switching oder den virtuellen Lastausgleichsserver vom Typ

Sie müssen den virtuellen Load Balancing-Server oder den virtuellen Content Switching-Server vom Typ HTTP/SSL an die Inhaltsüberprüfungsrichtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

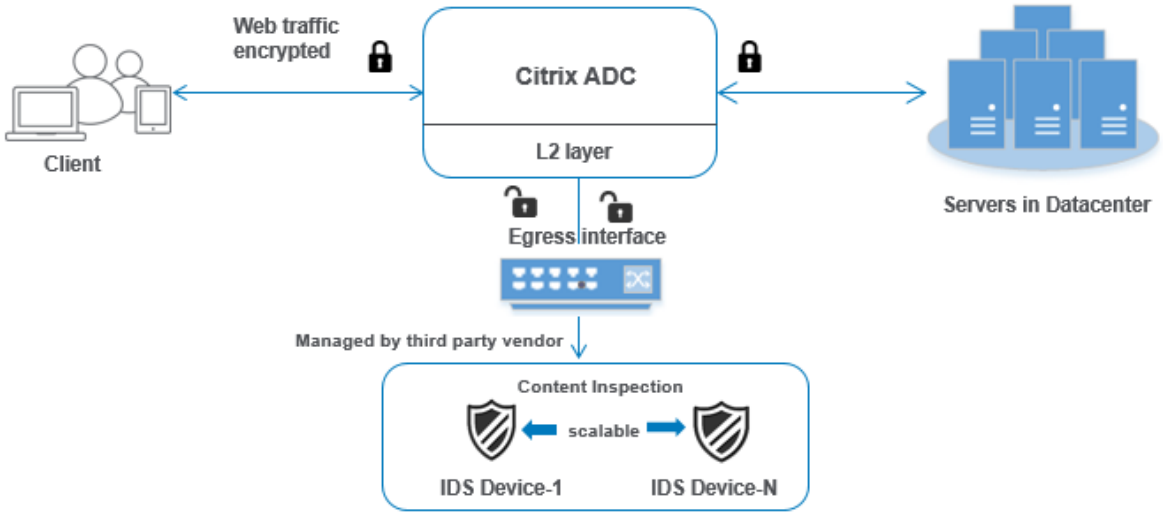
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Beispiel:

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Szenario 2: Lastenausgleich für mehrere IDS-Geräte

Wenn Sie zwei oder mehr IDS-Geräte verwenden, müssen Sie die Last der Geräte mithilfe verschiedener Inhaltsüberprüfungsdienste ausgleichen. In diesem Fall gleicht die NetScaler-Appliance die Geräte aus, zusätzlich zum Senden einer Teilmenge des Datenverkehrs an jedes Gerät. Grundlegende Konfigurationsschritte finden Sie in Szenario 1.



Im Folgenden sind die Schritte aufgeführt, die Sie mithilfe der Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsüberprüfungsprofil 1 vom Typ MIRROR für IDS-Dienst 1 hinzufügen
2. Inhaltsüberprüfungsprofil 2 vom Typ MIRROR für IDS-Dienst 2 hinzufügen
3. IDS-Dienst 1 vom Typ ANY für IDS-Gerät 1 hinzufügen
4. IDS-Dienst 2 vom Typ ANY für IDS-Gerät 2 hinzufügen
5. Hinzufügen eines virtuellen Lastausgleichsservers vom Typ ANY
6. IDS-Dienst 1 an den virtuellen Lastausgleichsserver binden
7. IDS-Dienst 2 an den virtuellen Lastausgleichsserver binden
8. Fügen Sie eine Inhaltsüberprüfungsaktion für den Lastausgleich von IDS-Geräten hinzu.
9. Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen
10. Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL
11. Richtlinie zur Inhaltsüberprüfung an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL binden

Inhaltsüberprüfungsprofil 1 vom Typ MIRROR für IDS-Dienst 1 hinzufügen

Die IDS-Konfiguration kann in einer Entität angegeben werden, die als Inhaltsprüfprofil bezeichnet wird. Das Profil hat eine Sammlung von Geräteeinstellungen. Das Inhaltsüberprüfungsprofil1 wird für den IDS-Dienst 1 erstellt.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection profile <name> -type ANY -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Beispiel:


```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Inhaltsüberprüfungsprofil 2 für den Typ MIRROR für IDS-Dienst 2

Das Inhaltsinspektionsprofil 2 wird für Dienst 2 hinzugefügt, und das Inline-Gerät kommuniziert mit der Appliance über die Ausgangsschnittstelle 1/1.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection profile <name> -type MIRROR -egressInterface -egressVlan
 <positive_integer>]
```

Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

IDS-Dienst 1 vom Typ ANY für IDS-Gerät 1 hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 1 für das Inline-Gerät 1 hinzufügen, um Teil des Lastausgleichs-Setups zu sein. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Hinweis**
>
> Bei der im Beispiel genannten IP-Adresse handelt es sich um eine Scheinadresse.

IDS-Dienst 2 vom Typ ANY für IDS-Gerät 2 hinzufügen

Nachdem Sie die Inhaltsinspektionsfunktion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 2 für das Inline-Gerät 2 hinzufügen. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```


Beispiel:

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Hinweis**
>
> Bei der im Beispiel genannten IP-Adresse handelt es sich um eine Scheinadresse.

Virtuellen Lastausgleichsserver hinzufügen

Nachdem Sie das Inline-Profil und die Dienste hinzugefügt haben, müssen Sie einen virtuellen Lastausgleichsserver für den Lastenausgleich der Dienste hinzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Beispiel:

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

IDS-Dienst 1 an den virtuellen Lastausgleichsserver binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie nun den virtuellen Lastausgleichsserver an den ersten Dienst.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service1
```

IDS-Dienst 2 an den virtuellen Lastausgleichsserver binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie den Server nun an den zweiten Dienst.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Inhaltsüberprüfungsaktion für den IDS-Dienst hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert haben, müssen Sie die Aktion Inhaltsüberprüfung für die Verarbeitung der Inline-Anforderungsinformationen hinzufügen. Basierend auf der ausgewählten Aktion verwirft, setzt die Appliance den Datenverkehr zurück, blockiert oder sendet ihn an das IDS-Gerät.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen

Nachdem Sie eine Inhaltsüberprüfungsaktion erstellt haben, müssen Sie eine Inhaltsüberprüfungsrichtlinie hinzufügen, um Serviceanfragen zu bewerten.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL

Fügen Sie einen virtuellen Content Switching- oder Lastausgleichsserver hinzu, um Webverkehr zu akzeptieren Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren.

Weitere Informationen zum Lastenausgleich finden Sie unter **Funktionsweise des Lastenausgleichs** .

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Richtlinie zur Inhaltsüberprüfung an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL binden

Sie müssen den virtuellen Content Switching- oder Load Balancing-Server vom Typ HTTP/SSL an die Richtlinie zur Inhaltsüberprüfung binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

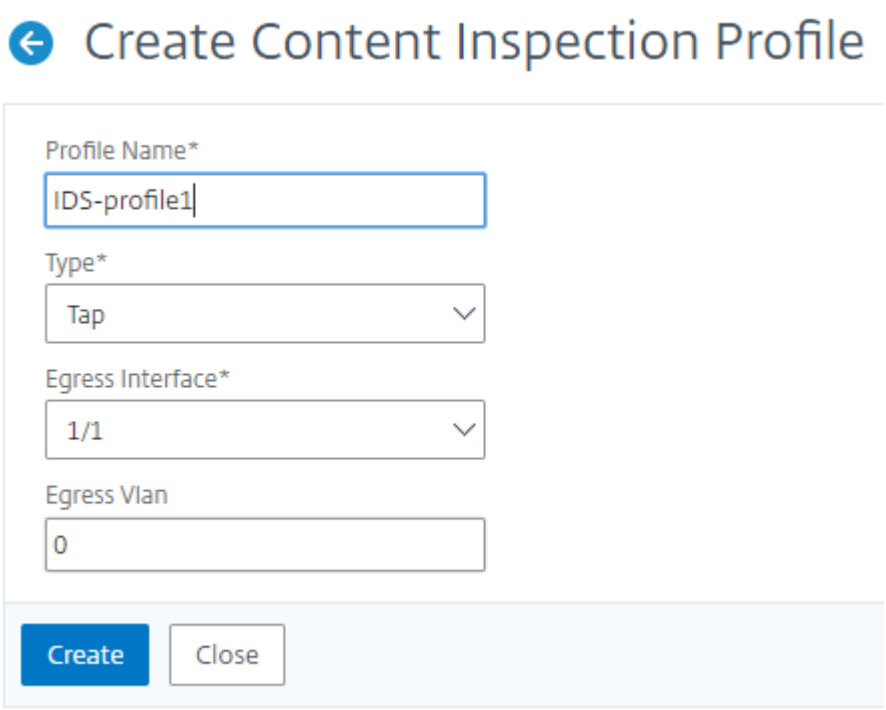
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -type <REQUEST>
```

Beispiel:

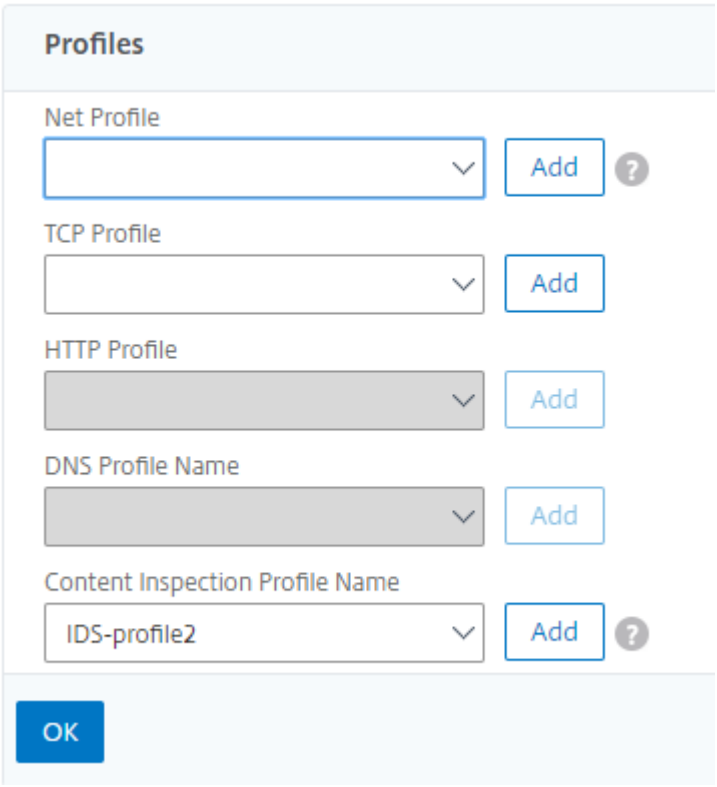
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type REQUEST
```

Konfigurieren der Inline-Serviceintegration mithilfe der NetScaler GUI

1. Navigieren Sie zu **Sicherheit** > **Inhaltsüberprüfung** > **Inhaltsüberprüfungsprofile**.
2. Klicken Sie auf der **Seite Inhaltsüberprüfungsprofil** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Inhaltsüberprüfungsprofil erstellen** die folgenden Parameter fest.
   a) Name des Profils. Name des Inhaltsinspektionsprofils für IDS.
   b) Typ. Wählen Sie die Profiltypen als MIRROR aus.
   c) Ausgangsschnittstelle. Die Schnittstelle, über die der Datenverkehr vom NetScaler zum IDS-Gerät gesendet wird.
   d) Ausgang-VLAN (optional). Die Schnittstellen-VLAN-ID, über die der Datenverkehr an das IDS-Gerät gesendet wird.
4. Klicken Sie auf **Erstellen**.



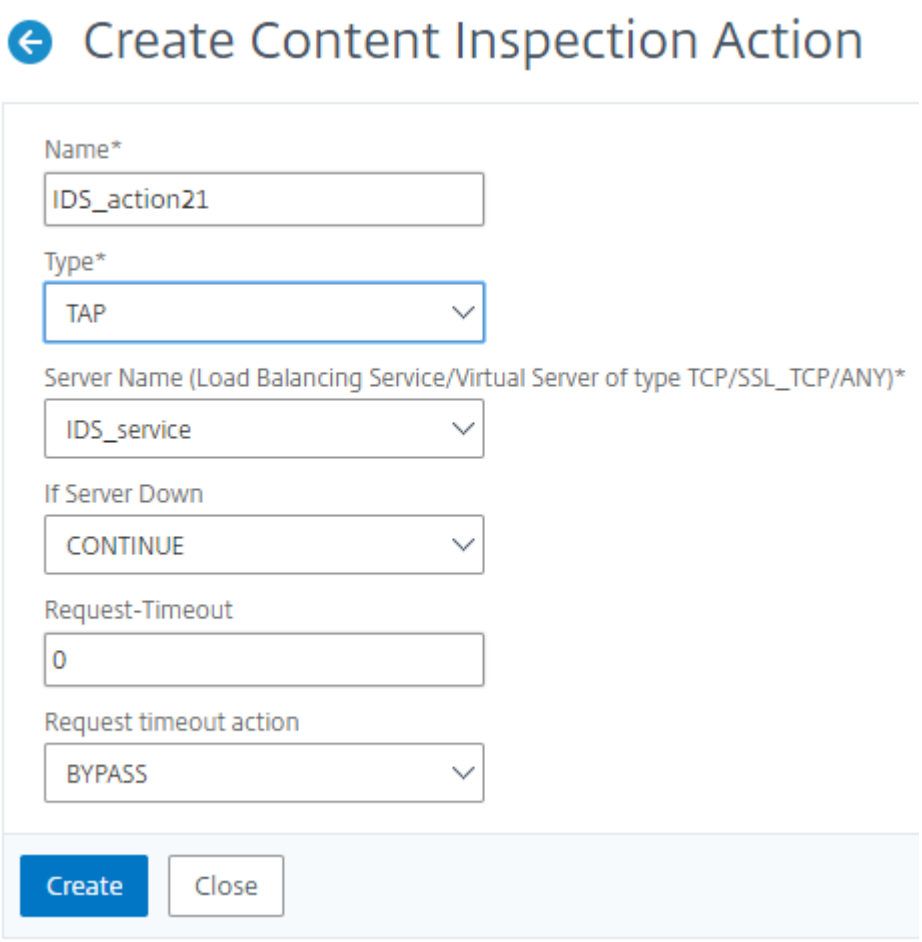
5. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**
6. Geben Sie auf der Seite **Load Balancing Service** die Details des Inhaltsüberprüfungsdienstes ein.
7. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf “ **Profile**”.
8. Gehen Sie zum Abschnitt **Profile** und klicken Sie auf das **Bleistiftsymbol**, um das Inhaltsüberprüfungsprofil hinzuzufügen.
9. Klicken Sie auf **OK**.



10. Navigieren Sie zu **Load Balancing** > **Server**. Fügen Sie einen virtuellen Server vom Typ HTTP oder SSL hinzu.
11. Nachdem Sie die Serverdetails eingegeben haben, klicken Sie auf **OK** und erneut auf **OK**.
12. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf **Richtlinien**.
13. Gehen Sie zum Abschnitt **Richtlinien** und klicken Sie auf das **Stiftsymbol**, um die Inhaltsüberprüfungsrichtlinie zu konfigurieren.
14. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
15. Klicken Sie im Abschnitt **Richtlinienbindung** auf “+”, um eine Richtlinie zur Inhaltsüberprüfung hinzuzufügen.
16. Geben Sie auf der Seite **CI-Richtlinie erstellen** einen Namen für die Richtlinie zur Inline-Inhaltsüberprüfung ein.
17. Klicken Sie im Feld **Aktion** auf das “+” -Zeichen, um eine IDS-Inhaltsüberprüfungsaktion vom Typ MIRROR zu erstellen.
18. Stellen Sie auf der Seite **CI-Aktion erstellen** die folgenden Parameter ein.
    a) Name. Name der Inline-Richtlinie zur Inhaltsüberprüfung.
    b) Typ. Wählen Sie den Typ als MIRROR.

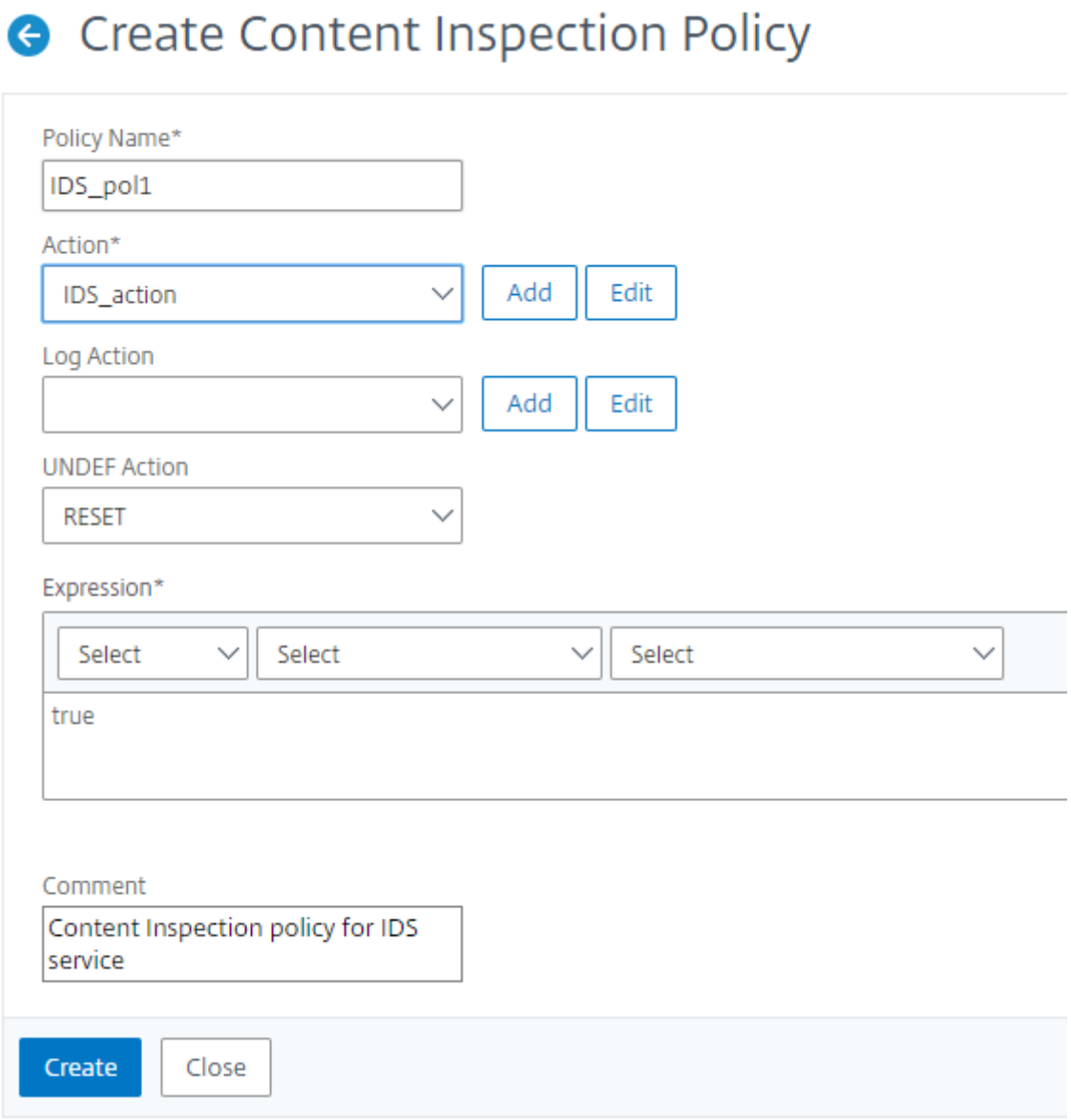
c) Servername. Wählen Sie den Server-/Dienstnamen als Inline-Geräte aus.
d) Wenn Server ausgefallen ist. Wählen Sie einen Vorgang aus, wenn der Server ausfällt.
e) Zeitüberschreitung anfragen. Wählen Sie einen Timeoutwert aus. Standardwerte können verwendet werden.
f) Timeout-Aktion anfordern. Wählen Sie eine Zeitüberschreitungsaktion aus. Standardwerte können verwendet werden.

19. Klicken Sie auf **Erstellen**.



20. Geben **Sie auf der Seite CI-Richtlinie erstellen** weitere Details ein.
21. Klicken Sie auf **OK** und auf **Schließen**.

Informationen zur NetScaler GUI-Konfiguration für den Lastenausgleich und das Replizieren des Datenverkehrs auf IDS-Geräte finden Sie unter Load Balancing.



Informationen zur NetScaler GUI-Konfiguration für den Lastenausgleich und das Weiterleiten des Datenverkehrs nach der Inhaltstransformation an den Back-End-Ursprungsserver finden Sie unter Thema Load Balancing .

Integration von NetScaler Layer 3 mit passiven Sicherheitsgeräten (Intrusion Detection System)

May 11, 2023

Eine NetScaler-Appliance ist jetzt in passive Sicherheitsgeräte wie das Intrusion Detection System

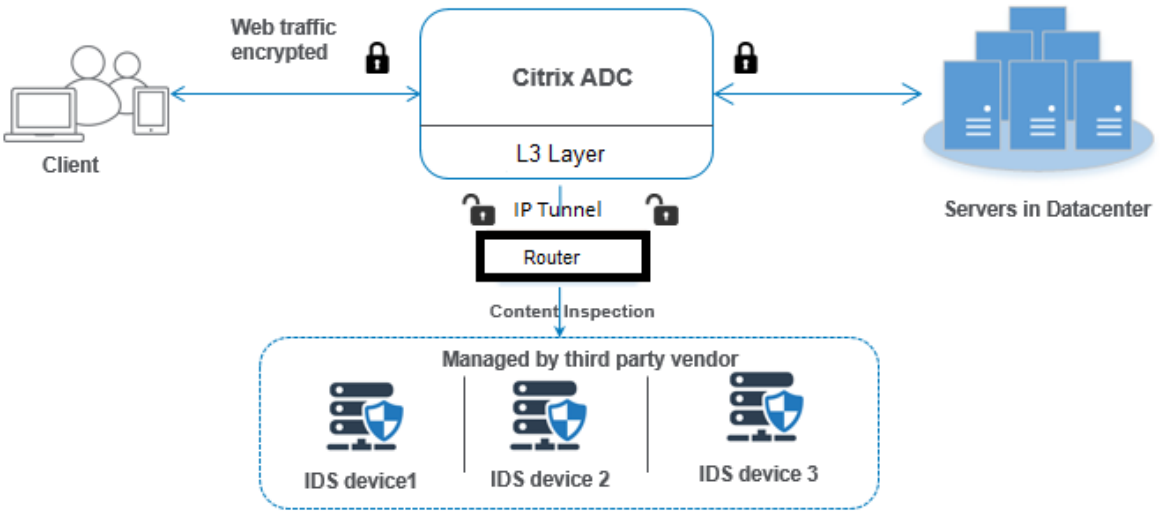
(IDS) integriert. In diesem Setup sendet die Appliance eine Kopie des ursprünglichen Datenverkehrs sicher an Remote-IDS-Geräte. Diese passiven Geräte speichern Protokolle und lösen Warnungen aus, wenn sie einen schlechten oder nicht konformen Datenverkehr erkennen. Es generiert auch Berichte für den Compliance-Zweck. Wenn eine NetScaler Appliance in zwei oder mehr IDS-Geräte integriert ist und ein hohes Verkehrsaufkommen besteht, kann die Appliance den Lastenausgleich der Geräte durchführen, indem der Datenverkehr auf virtueller Serverebene geklont wird.

Für erweiterten Sicherheitsschutz ist eine NetScaler-Appliance in passive Sicherheitsgeräte wie IDS integriert, die im Nur-Erkennungsmodus bereitgestellt werden. Diese Geräte speichern Protokolle und lösen Warnungen aus, wenn ein schlechter oder nicht konformer Datenverkehr festgestellt wird. Es generiert auch Berichte für den Compliance-Zweck. Im Folgenden sind einige der Vorteile der Integration des NetScaler in ein IDS-Gerät aufgeführt.

- **Überprüfung des verschlüsselten Datenverkehrs**. Die meisten Sicherheitsgeräte Bypass den verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe sind. Eine NetScaler-Appliance kann den Datenverkehr entschlüsseln und an IDS-Geräte senden, um die Netzwerksicherheit des Kunden zu verbessern.
- **Entladen von Inline-Geräten von der TLS/SSL-Verarbeitung**. Die TLS/SSL-Verarbeitung ist teuer und führt zu einer hohen System-CPU in Intrusion-Detection-Geräten, wenn sie den Datenverkehr entschlüsseln. Da der verschlüsselte Datenverkehr schnell zunimmt, können diese Systeme den verschlüsselten Datenverkehr nicht entschlüsseln und überprüfen. NetScaler hilft beim Auslagern des Datenverkehrs von der TLS/SSL-Verarbeitung auf IDS-Geräte. Diese Art der Datenauslagerung führt dazu, dass ein IDS-Gerät ein hohes Verkehrsaufkommen unterstützt.
- **Laden ausgleichender IDS-Geräte**. Die NetScaler-Appliance gleicht mehrere IDS-Geräte aus, wenn ein hohes Verkehrsaufkommen besteht, indem der Datenverkehr auf virtueller Serverebene geklont wird.
- **Replikation des Datenverkehrs auf passive Geräte**. Der in die Appliance fließende Datenverkehr kann auf andere passive Geräte repliziert werden, um Konformitätsberichte zu erstellen. Zum Beispiel schreiben nur wenige Regierungsbehörden vor, dass jede Transaktion in einigen passiven Geräten protokolliert wird.
- **Fächern des Datenverkehrs zu mehreren passiven Geräten**. Einige Kunden ziehen es vor, eingehenden Datenverkehr auf mehrere passive Geräte aufzufächern oder zu replizieren.
- **Intelligente Auswahl des Verkehrs**. Jedes Paket, das in die Appliance fließt, muss möglicherweise nicht inhaltlich geprüft werden, z. B. Der Benutzer kann die NetScaler-Appliance so konfigurieren, dass ein bestimmter Datenverkehr (z. B. EXE-Dateien) zur Überprüfung ausgewählt und der Datenverkehr zur Datenverarbeitung an IDS-Geräte gesendet wird.

Wie NetScaler in ein IDS-Gerät mit L3-Konnektivität integriert ist

Das folgende Diagramm zeigt, wie das IDS in eine NetScaler Appliance integriert ist.



Die Wechselwirkung der Komponenten ist wie folgt gegeben:

1. Ein Client sendet eine HTTP/HTTPS-Anforderung an die NetScaler-Appliance.
2. Die Appliance fängt den Datenverkehr ab und sendet die Daten an entfernte IDS-Geräte in verschiedenen Rechenzentren oder sogar in einer Cloud. Diese Integration erfolgt über die IP-Tunnellayer 3. Weitere Informationen zum IP-Tunneling in einer NetScaler-Appliance finden Sie unter IP-Tunneln.
3. Wenn der Datenverkehr verschlüsselt ist, entschlüsselt die Appliance die Daten und sendet sie als Nur-Text.
4. Basierend auf der Bewertung der Richtlinien wendet die Appliance eine Inhaltsinspektionsaktion vom Typ “MIRROR” an
5. Für die Aktion ist ein IDS-Dienst oder ein Load-Balancing-Dienst (für mehrere IDS-Geräteintegrationen) konfiguriert.
6. Das IDS-Gerät ist auf der Appliance als Content-Inspection-Diensttyp “Beliebig” konfiguriert. Der Inhaltsinspektionsdienst wird dann dem Inhaltsprüfungsprofil vom Typ „MIRROR“ und dem Tunnelparameter zugeordnet, der die getunnelte IP-Layer-3-Schnittstelle angibt, über die die Daten an das IDS-Gerät weitergeleitet werden.

   > **Hinweis:**
   >
   > Optional können Sie auch ein VLAN-Tag im Inhaltsprüfungsprofil konfigurieren.

7. Wenn der Back-End-Server eine Antwort an den NetScaler sendet, repliziert die Appliance die Daten und leitet sie an das IDS-Gerät weiter.
8. Wenn Ihre Appliance in ein oder mehrere IDS-Geräte integriert ist und Sie den Lastausgleich der Geräte bevorzugen, können Sie den virtuellen Lastausgleichsserver verwenden.

Softwarelizenzierung

Um die IDS-Integration bereitzustellen, muss Ihre NetScaler Appliance mit einer der folgenden Lizenzen ausgestattet sein:

1. ADC Premium
2. ADC Advanced

Konfigurieren der Einbruchmelde-Systemintegration

Sie können das IDS-Gerät auf zwei verschiedene Arten in einen NetScaler integrieren.

Szenario 1: Integration mit einem einzigen IDS-Gerät

Im Folgenden sind die Schritte aufgeführt, die Sie mithilfe der Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsüberprüfung aktivieren
2. Inhaltsüberprüfungsprofil vom Typ MIRROR für den Dienst, der das IDS-Gerät
3. IDS-Dienst vom Typ “ANY” hinzufügen
4. Inhaltsüberprüfungsaktion vom Typ “MIRROR” hinzugefügt
5. Inhaltsüberprüfungsrichtlinie für die IDS-Überprüfung hinzufügen
6. Binden Sie die Inhaltsüberprüfungsrichtlinie an den virtuellen Content Switching- oder Lastausgleichsdienst des Typs HTTP/SSL

Inhaltsüberprüfung aktivieren

Wenn Sie möchten, dass die NetScaler-Appliance den Inhalt zur Überprüfung an die IDS-Geräte sendet, müssen Sie die Funktionen Inhaltsüberprüfung und den Lastausgleich unabhängig von der Entschlüsselung aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature contentInspection LoadBalancing
```

Fügen Sie ein Inhaltsinspektionsprofil vom Typ „MIRROR“ hinzu

Das Inhaltsüberprüfungsprofil vom Typ “MIRROR” erklärt, wie Sie eine Verbindung zum IDS-Gerät herstellen können.
Geben Sie an der Eingabeaufforderung ein.

> **Hinweis:**
>
> Der IP-Tunnelparameter darf nur für die Layer-3-IDS-Topologie verwendet werden. Andernfalls

> müssen Sie die Ausgangsschnittstelle mit der Ausgangs-VLAN-Option verwenden. GRE/IPIP-Tunneltypen werden mit der Layer-3-IDS-Topologie unterstützt.

```
add contentInspection profile <name> -type MIRROR -ipTunnel <iptunnel_name>
```

Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR -ipTunnel ipsect-
tunnel1
```

IDS-Dienst hinzufügen

Sie müssen einen Dienst vom Typ “ANY” für jedes IDS-Gerät konfigurieren, das in die Appliance integriert ist. Der Dienst hat die IDS-Gerätekonfigurationsdetails. Der Dienst stellt das IDS-Gerät dar.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Inhaltsüberprüfungsaktion vom Typ MIRROR für IDS-Dienst hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert und anschließend das IDS-Profil und den Dienst hinzugefügt haben, müssen Sie die Aktion Inhaltsüberprüfung für die Bearbeitung der Anforderung hinzufügen. Basierend auf der Inhaltsüberprüfungsaktion kann die Appliance Daten löschen, zurücksetzen, blockieren oder an das IDS-Gerät senden.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Inhaltsüberprüfungsrichtlinie für die IDS-Überprüfung hinzufügen

Nachdem Sie eine Inhaltsüberprüfungsaktion erstellt haben, müssen Sie Richtlinien für die Inhaltsüberprüfung hinzufügen, um Überprüfungsanfragen zu bewerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Richtlinie bewertet und wählt den zu überprüfenden Verkehr basierend auf der Regel aus.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Binden Sie die Inhaltsüberprüfungsrichtlinie an den virtuellen Content Switching- oder Lastausgleichsdienst des Typs HTTP/SSL

Um den Webverkehr zu empfangen, müssen Sie einen virtuellen Lastausgleichsserver hinzufügen. Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Binden der Richtlinie zur Inhaltsüberprüfung an den virtuellen Server mit Content Switching oder den virtuellen Lastausgleichsserver vom Typ

Sie müssen den virtuellen Load Balancing-Server oder den virtuellen Content Switching-Server vom Typ HTTP/SSL an die Inhaltsüberprüfungsrichtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

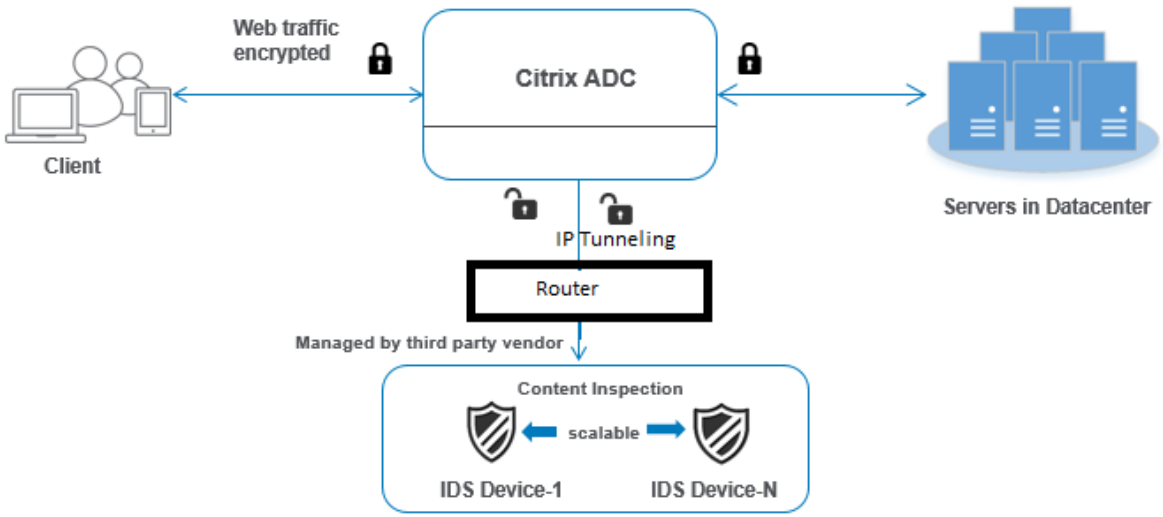
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Beispiel:

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Szenario 2: Lastenausgleich für mehrere IDS-Geräte

Wenn Sie zwei oder mehr IDS-Geräte verwenden, müssen Sie den Lastenausgleich zwischen den IDS-Geräten mithilfe verschiedener Content Inspection Services durchführen. In diesem Fall gleicht die NetScaler-Appliance die Geräte aus, zusätzlich zum Senden einer Teilmenge des Datenverkehrs an jedes Gerät.
Grundlegende Konfigurationsschritte finden Sie in Szenario 1.



Im Folgenden sind die Schritte aufgeführt, die Sie mithilfe der Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsüberprüfungsprofil 1 vom Typ MIRROR für IDS-Dienst 1 hinzufügen
2. Inhaltsüberprüfungsprofil 2 vom Typ MIRROR für IDS-Dienst 2 hinzufügen
3. IDS-Dienst 1 vom Typ ANY für IDS-Gerät 1 hinzufügen
4. IDS-Dienst 2 vom Typ ANY für IDS-Gerät 2 hinzufügen
5. Hinzufügen eines virtuellen Lastausgleichsservers vom Typ ANY
6. IDS-Dienst 1 an den virtuellen Lastausgleichsserver binden
7. IDS-Dienst 2 an den virtuellen Lastausgleichsserver binden
8. Fügen Sie eine Inhaltsüberprüfungsaktion für den Lastausgleich von IDS-Geräten hinzu.
9. Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen
10. Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL
11. Richtlinie zur Inhaltsüberprüfung an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL binden

Inhaltsüberprüfungsprofil 1 vom Typ MIRROR für IDS-Dienst 1 hinzufügen

Die IDS-Konfiguration kann in einer Entität angegeben werden, die als Inhaltsprüfprofil bezeichnet wird. Das Profil hat eine Sammlung von Geräteeinstellungen. Das Inhaltsüberprüfungsprofil1 wird für den IDS-Dienst 1 erstellt.

> **Hinweis**: Der IP-Tunnelparameter darf nur für die Layer-3-IDS-Topologie verwendet werden. Andernfalls müssen Sie die Ausgangsschnittstelle mit der Ausgangs-VLAN-Option verwenden. GRE/IPIP-Tunneltypen werden mit der Layer-3-IDS-Topologie unterstützt.

Geben Sie in der Befehlszeile Folgendes ein:


```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```

Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR - ipTunnel ipsect_tunnel1
```

Inhaltsüberprüfungsprofil 2 für den Typ MIRROR für IDS-Dienst 2

Das Inhaltsinspektionsprofil 2 wird für Dienst 2 hinzugefügt, und das Inline-Gerät kommuniziert mit der Appliance über die Ausgangsschnittstelle 1/1.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```

Beispiel:

```
add contentInspection profile IDS_profile2 -type ANY - ipTunnel ipsect_tunnel2
```

IDS-Dienst 1 vom Typ ANY für IDS-Gerät 1 hinzufügen

Nachdem Sie die Inhaltsinspektionsfunktion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 1 für das Inline-Gerät 1 hinzufügen, um Teil des Load-Balancing-Setups zu sein. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Hinweis**:
>
> Bei der im Beispiel genannten IP-Adresse handelt es sich um eine Scheinadresse.

IDS-Dienst 2 vom Typ ANY für IDS-Gerät 2 hinzufügen

Nachdem Sie die Inhaltsinspektionsfunktion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 2 für das Inline-Gerät 2 hinzufügen. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie in der Befehlszeile Folgendes ein:


```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Hinweis**:
>
> Bei der im Beispiel genannten IP-Adresse handelt es sich um eine Scheinadresse.

Virtuellen Lastausgleichsserver hinzufügen

Nachdem Sie das Inline-Profil und die Dienste hinzugefügt haben, müssen Sie einen virtuellen Lastausgleichsserver für den Lastenausgleich der Dienste hinzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Beispiel:

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

IDS-Dienst 1 an den virtuellen Lastausgleichsserver binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie nun den virtuellen Lastausgleichsserver an den ersten Dienst.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service1
```

IDS-Dienst 2 an den virtuellen Lastausgleichsserver binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie den Server nun an den zweiten Dienst.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Inhaltsüberprüfungsaktion für den IDS-Dienst hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert haben, müssen Sie die Aktion Inhaltsüberprüfung für die Verarbeitung der Inline-Anforderungsinformationen hinzufügen. Basierend auf der ausgewählten Aktion verwirft, setzt die Appliance den Datenverkehr zurück, blockiert oder sendet ihn an das IDS-Gerät.

Geben Sie in der Befehlszeile Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen

Nachdem Sie eine Inhaltsinspektionsaktion erstellt haben, müssen Sie die Inhaltsinspektionsrichtlinie hinzufügen, um Serviceanfragen zu bewerten.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL

Fügen Sie einen virtuellen Content Switching- oder Lastausgleichsserver hinzu, um Webverkehr zu akzeptieren Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren.

Weitere Informationen zum Lastenausgleich finden Sie unter Funktionsweise des Lastenausgleichs .

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Richtlinie zur Inhaltsüberprüfung an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL binden

Sie müssen den virtuellen Content Switching- oder Load Balancing-Server vom Typ HTTP/SSL an die Richtlinie zur Inhaltsüberprüfung binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

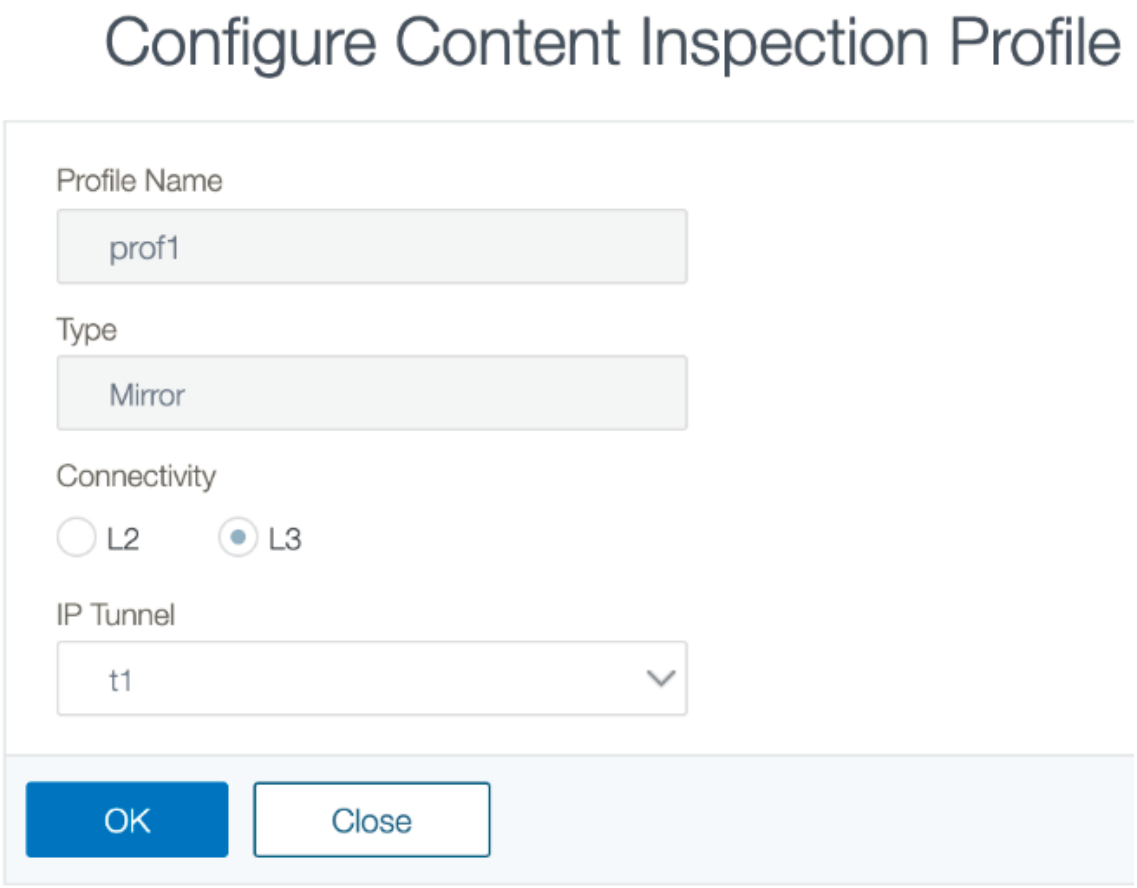
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

Beispiel:

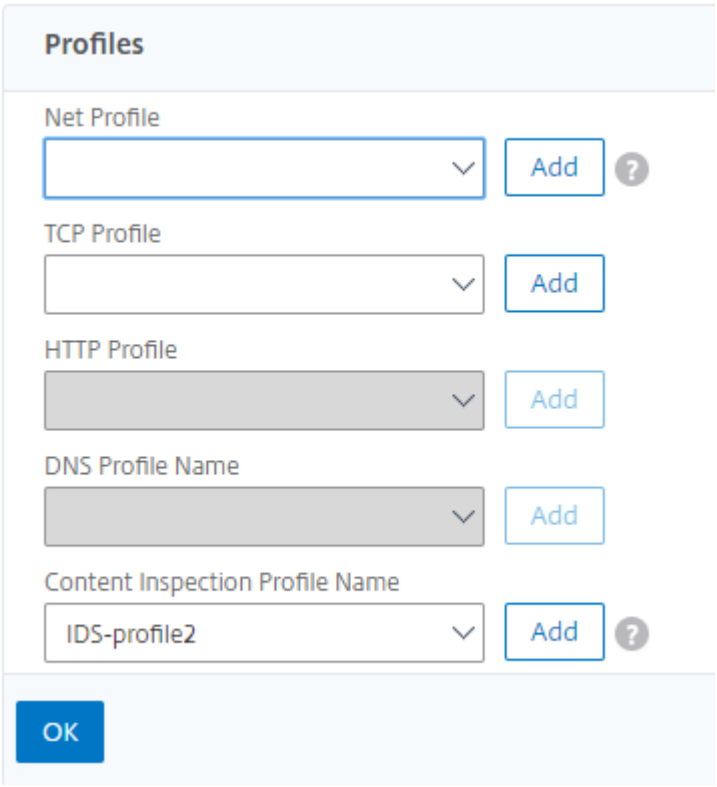
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Konfigurieren der Inline-Serviceintegration mithilfe der NetScaler GUI

1. Navigieren Sie zu **Sicherheit** > **Inhaltsinspektion** > **ContentInspection-Profile**.
2. Klicken Sie auf der **ContentInspection-Profilseite** auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **ContentInspectionProfile erstellen** “ die folgenden Parameter ein.
    a) Name des Profils. Name des Inhaltsinspektionsprofils für IDS.
    b) Typ. Wählen Sie die Profiltypen als MIRROR aus.
    c) Konnektivität. Layer-2- oder Layer-3-Schnittstelle.
    d) IP-Tunnel. Wählen Sie den Netzwerkkommunikationskanal zwischen den beiden Netzwerken aus.
4. Klicken Sie auf **Erstellen**.



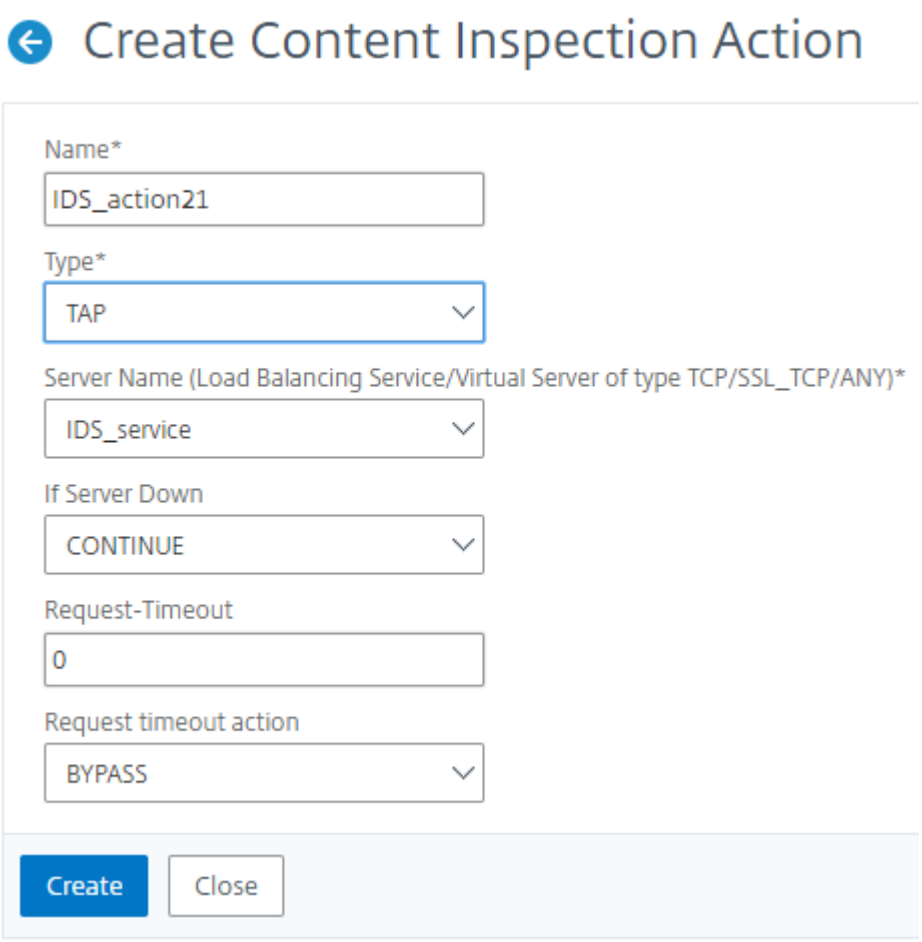
5. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**
6. Geben Sie auf der Seite **Load Balancing Service** die Details des Inhaltsüberprüfungsdienstes ein.
7. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf “ **Profile**”.
8. Gehen Sie zum Abschnitt **Profile** und klicken Sie auf das **Bleistiftsymbol**, um das Inhaltsüberprüfungsprofil hinzuzufügen.
9. Klicken Sie auf **OK**.



10. Navigieren Sie zu **Load Balancing** > **Server**. Fügen Sie einen virtuellen Server vom Typ HTTP oder SSL hinzu.
11. Nachdem Sie die Serverdetails eingegeben haben, klicken Sie auf **OK** und erneut auf **OK**.
12. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf **Richtlinien**.
13. Gehen Sie zum Abschnitt **Richtlinien** und klicken Sie auf das **Stiftsymbol**, um die Inhaltsüberprüfungsrichtlinie zu konfigurieren.
14. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
15. Klicken Sie im Abschnitt **Richtlinienbindung** auf “+”, um eine Richtlinie zur Inhaltsüberprüfung hinzuzufügen.
16. Geben Sie auf der Seite **CI-Richtlinie erstellen** einen Namen für die Richtlinie zur Inline-Inhaltsüberprüfung ein.
17. Klicken Sie im Feld **Aktion** auf das “+” -Zeichen, um eine IDS-Inhaltsüberprüfungsaktion vom Typ MIRROR zu erstellen.
18. Stellen Sie auf der Seite **CI-Aktion erstellen** die folgenden Parameter ein.
    a) Name. Name der Inline-Richtlinie zur Inhaltsüberprüfung.
    b) Typ. Wählen Sie den Typ als MIRROR.

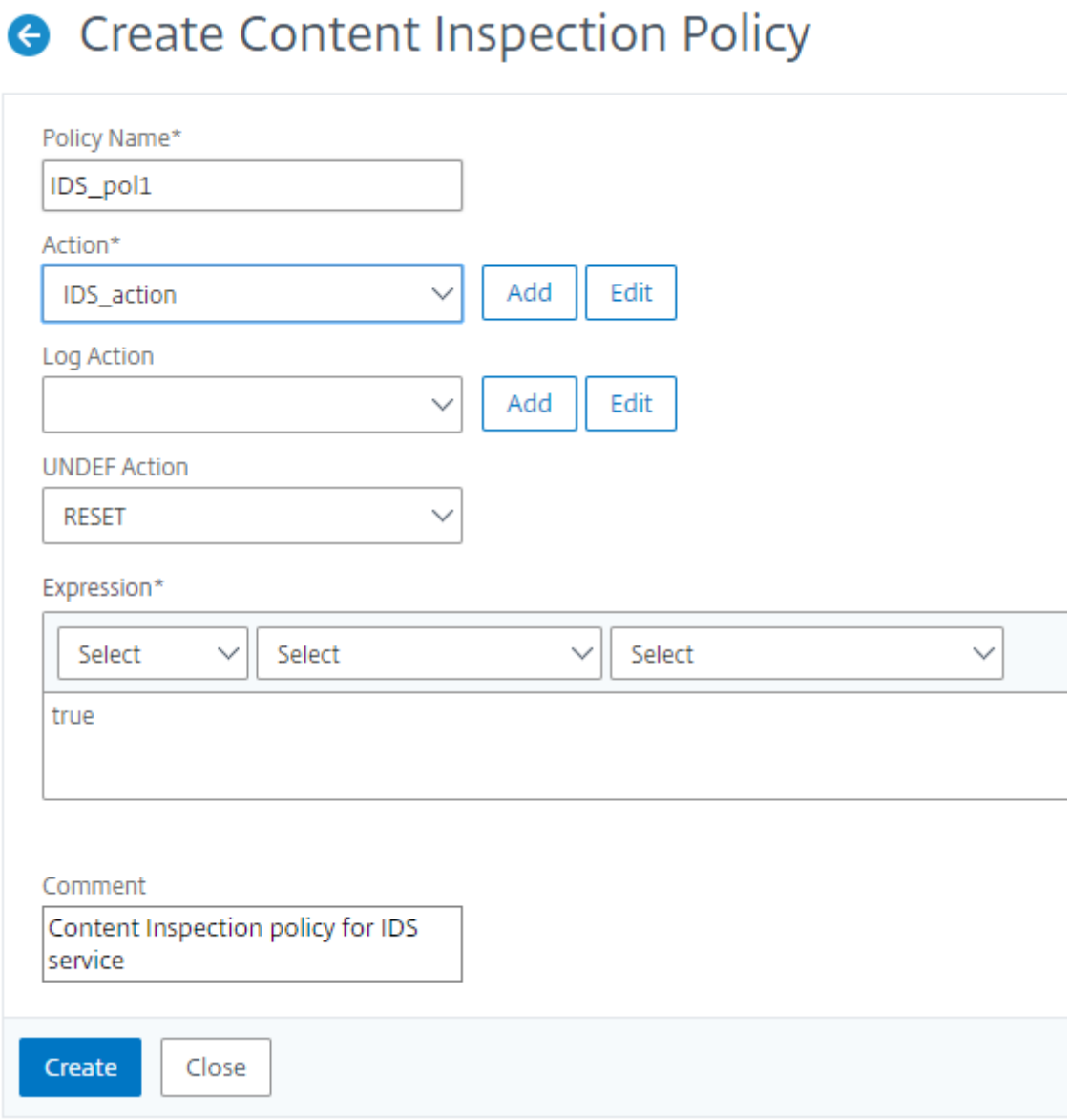
c) Servername. Wählen Sie den Server-/Dienstnamen als Inline-Geräte aus.
d) Wenn Server ausgefallen ist. Wählen Sie einen Vorgang aus, wenn der Server ausfällt.
e) Zeitüberschreitung anfragen. Wählen Sie einen Timeoutwert aus. Standardwerte können verwendet werden.
f) Timeout-Aktion anfordern. Wählen Sie eine Zeitüberschreitungsaktion aus. Standardwerte können verwendet werden.

19. Klicken Sie auf **Erstellen**.



20. Geben **Sie auf der Seite CI-Richtlinie erstellen** weitere Details ein.
21. Klicken Sie auf **OK** und auf **Schließen**.

Informationen zur NetScaler GUI-Konfiguration für den Lastenausgleich und das Replizieren des Datenverkehrs auf IDS-Geräte finden Sie unter Load Balancing.



Informationen zur NetScaler GUI-Konfiguration für den Lastenausgleich und das Weiterleiten des Datenverkehrs nach der Inhaltstransformation an den Back-End-Ursprungsserver finden Sie unter Load Balancing.

Statistiken zur Inhaltsprüfung für ICAP, IPS und IDS

February 16, 2021

Die Statistiken zur Inhaltsinspektion für ICAP, Inline-Geräteintegration (IDS) und Intrusion Prevention System (IPS) sind eine detaillierte Ausgabe (Zusammenfassung) der Details zu Anfragen, Antworten und Serveraktionen.

Die Statistiken zur Inhaltsinspektion sind eine Sammlung statistischer Daten, die die zur Inhaltsüberprüfung gesendete HTTP/HTTPS-Anfrage enthält. HTTP-/HTTPS-Antwort von IPS-, IDS- und ICAP-Geräten sowie Back-End-Serveraktionen.

So zeigen Sie Statistiken zur Inhaltsüberwachung mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat contentInspection
```

```
ContentInspection Stats

Inline Statistics
                                  Total
Requests                           10
Responses                           6
Request Bytes Sent                 3235
Request Bytes Received             2977
Response Bytes Sent                17302
Response Bytes Received            19681
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      0
Inline device Generated Response    3

Mirror Statistics
                                  Total
Requests                           4
Responses                          4
Requests Bytes Sent               2763
Responses Bytes Sent              16732
Serverdown Reset Action taken      0
Serverdown Drop Action taken       0
Serverdown BYPASS Action taken     1

ICAP Statistics
                                  Total
REQMOD requests Sent                6
RESPMOD requests Sent               4
Preview requests                    1
204 Responses Received              6
100 Continue Responses Received     1
204 NO content Received             5
Adaptive Requests                   0
Adaptive Responses                  4
Callout requests Initiated          1
```



```
Callout requests completed          1
ICAP Req/Resp Errors handled        1
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      1

Done
<!--NeedCopy-->
```

SSL-Forward-Proxy

May 11, 2023

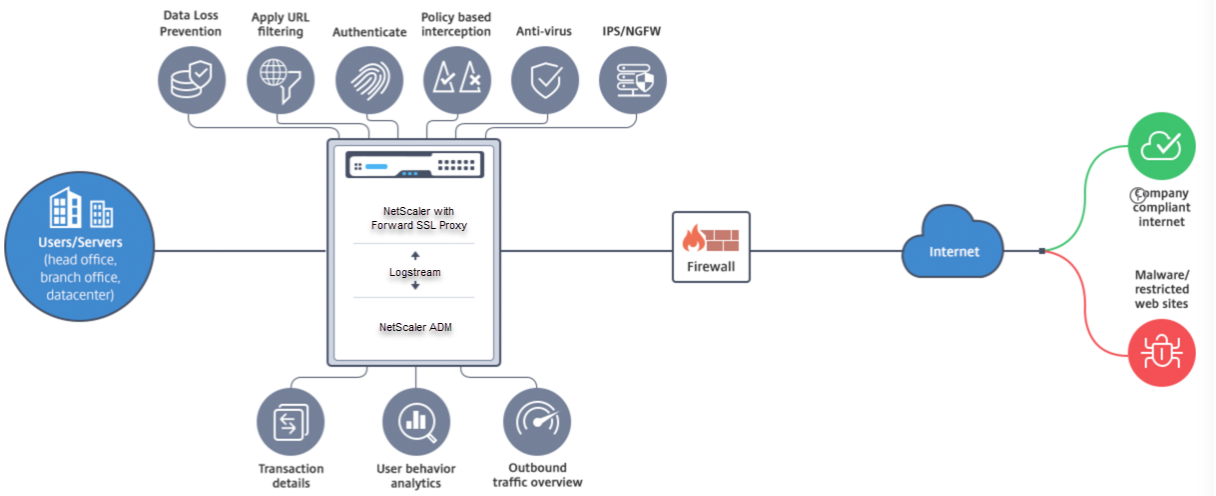
Hinweis: Die SSL-Forward-Proxy-Funktion ist mit der ADC Premium-Lizenz verfügbar.

Der Webverkehr hat in den letzten Jahren exponentiell zugenommen, und Unternehmen verlassen sich zunehmend auf das Internet für ihren täglichen Betrieb. In Kombination mit dem Aufkommen vielfältigerer Endgeräte, Mobilität und BYOD sowie einer wachsenden Anzahl von Angreifern macht dies Benutzer zu leichten Zielen moderner Malware. Sie sind zunehmend anfällig für Identitätsdiebstahl und die Kompromittierung ihrer Daten. Traditionell haben Unternehmen den HTTP-Verkehr auf Malware und Viren untersucht. Sie haben den HTTPS/TLS-Verkehr umgangen, weil er nicht so auffällig war. Es wurde sparsam für Inhalte verwendet, die sensibel und vertrauenswürdig waren. Das hat sich jedoch schnell geändert, da die meisten öffentlichen Internet-Websites heute HTTPS bevorzugen, um die Privatsphäre der Benutzer zu schützen. Die Unfähigkeit, verschlüsselte Pakete zu überprüfen, führt daher zu Malware oder Eindringlingen in das Unternehmensnetzwerk. Die SSL-Forward-Proxy-Lösung bietet Tools, mit denen Unternehmen sich vor Internetbedrohungen schützen können.

Ein Proxy ist ein Server, der den gesamten Datenverkehr zwischen Benutzern und dem Internet oder SaaS-Anwendungen steuert. Da der gesamte Datenverkehr diesen Proxy durchläuft, führt er sicherheitsbezogene Funktionen wie Benutzerauthentifizierung und URL-Kategorisierung aus.

Die folgende Abbildung gibt einen Überblick über die Implementierung des SSL-Forward-Proxys. Der Datenverkehr fließt über das Unternehmensnetzwerk von der Zentrale, Zweigstellen, Rechenzentren und Remote-Mitarbeitern aus. Eine NetScaler-Appliance am Rand des Netzwerks fungiert als Proxy. Die Appliance kann im transparenten Proxy-Modus oder im expliziten Proxymodus betrieben werden und bietet Steuerelemente zum Abfangen des Internetverkehrs, einschließlich HTTPS. Die auf der Appliance konfigurierten Richtlinien bestimmen, ob eine bestimmte Anfrage abgefangen, umgangen oder blockiert wird. Der Zugriff auf eingeschränkte Websites kann mithilfe von URL-Filtern blockiert werden. Ein Benutzer wird authentifiziert, bevor er sich am Unternehmensnetzwerk anmeldet. Alle Anfragen und Antworten werden markiert, um den Benutzer zu identifizieren, und der Zugriff auf die Website wird kategorisiert. Die Benutzeraktivität wird protokolliert und zur Erstellung von Berichten

verwendet. Wenn ein Verstoß auftritt, können Administratoren das infizierte System isolieren, feststellen, ob die Geräte anderer Benutzer, die diese Website besucht haben, gefährdet sind, und geeignete Maßnahmen ergreifen. Wenn Sie NetScaler Application Delivery Management (ADM) in den SSL-Forward-Proxy integrieren, werden die protokollierte Benutzeraktivität und die nachfolgenden Datensätze in der Appliance mithilfe von NetScaler ADM exportiert. `logstream` NetScaler ADM stellt Informationen über die Aktivitäten der Nutzer zusammen, von besuchten Websites bis hin zu der online verbrachten Zeit. Es enthält auch Informationen zur Bandbreitennutzung und zu erkannten Bedrohungen wie Malware und Phishing-Websites. Sie können diese wichtigen Metriken verwenden, um Ihr Netzwerk zu überwachen und die SSL-Forward-Proxy-Funktion verwenden, um Korrekturmaßnahmen zu ergreifen.



Mit dem SSL-Forward-Proxy können IT-Direktoren Folgendes tun:

- Verschaffen Sie sich einen Überblick über den ansonsten umgangenen sicheren Verkehr.
- Blockieren Sie den Zugriff auf bösartige oder unbekannte Websites und verhindern Sie, dass Benutzer innerhalb des Unternehmens infiziert werden.
- Steuern Sie den Zugriff auf einige Websites, z. B. persönliche E-Mails, soziale Netzwerke und Websites zur Jobsuche, vom Unternehmensnetzwerk aus.
- Wenden Sie intelligente Content-Control-Richtlinien an, um maximale Benutzerproduktivität zu gewährleisten.

Erste Schritte mit SSL-Forward-Proxy

May 11, 2023

Wichtig:

- Die OCSP-Prüfung erfordert eine Internetverbindung, um die Gültigkeit von Zertifikaten zu überprüfen. Wenn Ihre Appliance nicht über das Internet über die NSIP-Adresse erreichbar ist, fügen

Sie Zugriffssteuerungslisten (ACLs) hinzu, um NAT von der NSIP-Adresse zur Subnetz-IP-Adresse (SNIP) durchzuführen. Das SNIP muss auf das Internet zugreifen können. Zum Beispiel

```
add ns acl a1 ALLOW -srcIP = <NSIP> -destIP  “!=”
    10.0.0.0-10.255.255.255

add rnat RNAT-1 a1

bind rnat RNAT-1 <SNIP>

apply acls
<!--NeedCopy-->
```

- Geben Sie einen DNS-Namensserver zum Auflösen von Domainnamen an.
- Stellen Sie sicher, dass das Datum auf der Appliance mit den NTP-Servern synchronisiert ist. Wenn das Datum nicht synchronisiert ist, kann die Appliance nicht effektiv überprüfen, ob ein Ursprungsserverzertifikat abgelaufen ist.

Um die SSL-Forward-Proxy-Funktion zu verwenden, müssen Sie die folgenden Aufgaben ausführen:

- Fügen Sie einen Proxyserver im expliziten oder transparenten Modus hinzu.
- Aktivieren Sie SSL-Interception.
  - Konfigurieren Sie ein SSL-Profil.
  - Fügen Sie SSL-Richtlinien hinzu und binden Sie sie an den Proxyserver.
  - Fügen Sie ein CA-Zertifikatschlüsselpaar für SSL-Interception hinzu und binden Sie es.

Hinweis:

Eine im transparenten Proxymodus konfigurierte ADC-Appliance kann nur HTTP- und HTTPS-Protokolle abfangen. Um ein anderes Protokoll wie Telnet zu Bypass, müssen Sie die folgende Listenrichtlinie auf dem virtuellen Proxyserver hinzufügen.

Der virtuelle Server akzeptiert jetzt nur eingehenden HTTP- und HTTPS-Datenverkehr.

```
set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy
    "CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)"`
<!--NeedCopy-->
```

Abhängig von Ihrer Bereitstellung müssen Sie möglicherweise die folgenden Funktionen konfigurieren:

- Authentifizierungsdienst (empfohlen) — um Benutzer zu authentifizieren. Ohne den Authentifizierungsdienst basiert die Benutzeraktivität auf der IP-Adresse des Clients.
- URL-Filterung — um URLs nach Kategorien, Reputationsbewertung und URL-Listen zu filtern.

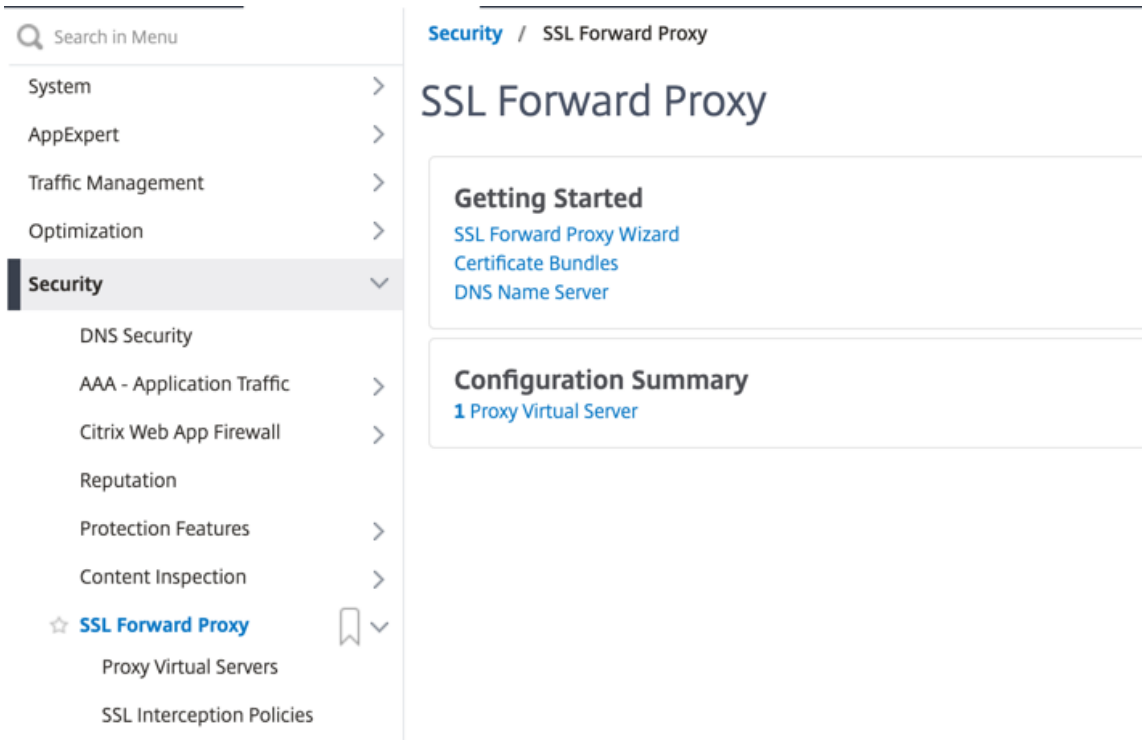
- Analysen — zur Anzeige von Benutzeraktivitäten, Benutzerrisikoindikatoren, Bandbreitenverbrauch und Transaktionsaufschlüsselungen in NetScaler Application Delivery Management (ADM).

Hinweis: SSL Forward Proxy implementiert die meisten typischen HTTP- und HTTPS-Standards, gefolgt von ähnlichen Produkten. Diese Implementierung erfolgt ohne Berücksichtigung eines bestimmten Browsers und ist mit den meisten gängigen Browsern kompatibel. SSL Forward Proxy wurde mit gängigen Browsern und aktuellen Versionen von Google Chrome, Internet Explorer und Mozilla Firefox getestet.

Assistent für die SSL-Weiterleitung

Der SSL-Forward-Proxy-Assistent bietet Administratoren ein Tool zur Verwaltung der gesamten SSL-Forward-Proxy-Bereitstellung mithilfe eines Webbrowsers. Es hilft den Kunden, einen SSL-Forward-Proxy-Dienst schnell aufzurufen, und vereinfacht die Konfiguration, indem eine Reihe genau definierter Schritte ausgeführt wird.

1. Navigieren Sie zu **Sicherheit > SSL-Weiterleitungsproxy**. Klicken Sie unter **Erste Schritte** auf **SSL-Forward-Proxy-Assistent**.



2. Folgen Sie den Schritten im Assistenten, um Ihre Bereitstellung zu konfigurieren.

Hinzufügen einer Listenrichtlinie zum transparenten Proxyserver

1. Navigieren Sie zu **Sicherheit > SSL-Weiterleitungsproxy** > **Virtuelle Proxyserver**. Wählen Sie den transparenten Proxyserver und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie die **Grundeinstellungen**und klicken Sie auf **Mehr**.
3. Geben Sie im Feld **Listeningpriorität** den Wert 1
4. Geben Sie im Feld **Listeningrichtlinienausdruck** den folgenden Ausdruck ein:

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

   Dieser Ausdruck setzt Standardports für HTTP- und HTTPS-Datenverkehr voraus. Wenn Sie verschiedene Ports konfiguriert haben, z. B. 8080 für HTTP oder 8443 für HTTPS, ändern Sie den Ausdruck so, dass er diese Ports widerspiegelt.

Einschränkungen

SSL-Forwardproxy wird in einem Cluster-Setup, in Adminpartitionen und auf einer NetScaler FIPS-Appliance nicht unterstützt.

Proxy-Modi

May 11, 2023

Die NetScaler-Appliance fungiert als Client-Proxy, um eine Verbindung zum Internet und zu SaaS-Anwendungen herzustellen. Als Proxy akzeptiert es den gesamten Datenverkehr und bestimmt das Protokoll des Datenverkehrs. Sofern es sich bei dem Datenverkehr nicht um HTTP oder SSL handelt, wird er unverändert an das Ziel weitergeleitet. Wenn die Appliance eine Anfrage von einem Client empfängt, fängt sie die Anfrage ab und führt einige Aktionen aus, wie z. B. Benutzerauthentifizierung, Standortkategorisierung und Umleitung. Es verwendet Richtlinien, um zu bestimmen, welcher Verkehr zugelassen und welcher blockiert werden soll.

Die Appliance unterhält zwei verschiedene Sitzungen, eine zwischen dem Client und dem Proxy und die andere zwischen dem Proxy und dem Ursprungsserver. Der Proxy stützt sich auf kundendefinierte Richtlinien, um HTTP- und HTTPS-Verkehr zuzulassen oder zu blockieren. Daher ist es wichtig, dass Sie Richtlinien definieren, um sensible Daten wie Finanzinformationen zu Bypass. Die Appliance bietet eine Vielzahl von Layer-4- bis Layer-7-Datenverkehrsattributen und Benutzeridentitätsattributen zur Erstellung von Verkehrsmanagement-Richtlinien.

Bei SSL-Verkehr überprüft der Proxy das Zertifikat des Ursprungsservers und stellt eine legitime Verbindung mit dem Server her. Anschließend emuliert es das Serverzertifikat, signiert es mit einem

auf NetScaler installierten CA-Zertifikat und präsentiert dem Client das erstellte Serverzertifikat. Sie müssen das CA-Zertifikat als vertrauenswürdiges Zertifikat zum Browser des Clients hinzufügen, damit die SSL-Sitzung erfolgreich eingerichtet werden kann.

Die Appliance unterstützt transparente und explizite Proxymodi. Im expliziten Proxymodus muss der Client in seinem Browser eine IP-Adresse angeben, es sei denn, die Organisation überträgt die Einstellung auf das Gerät des Kunden. Diese Adresse ist die IP-Adresse eines Proxyservers, der auf der ADC-Appliance konfiguriert ist. Alle Client-Anfragen werden an diese IP-Adresse gesendet. Für einen expliziten Proxy müssen Sie einen virtuellen Content Switching-Server vom Typ PROXY konfigurieren und eine IP-Adresse und eine gültige Portnummer angeben.

Ein transparenter Proxy ist, wie der Name schon sagt, für den Client transparent. Das heißt, die Clients wissen möglicherweise nicht, dass ein Proxyserver ihre Anfragen vermittelt. Die ADC-Appliance ist in einer Inline-Bereitstellung konfiguriert und akzeptiert transparent den gesamten HTTP- und HTTPS-Verkehr. Für einen transparenten Proxy müssen Sie einen virtuellen Content Switching-Server vom Typ PROXY mit Sternchen (* *) als IP-Adresse und Port konfigurieren. Wenn Sie den **SSL Forward Proxy Wizard** in der GUI verwenden, müssen Sie keine IP-Adresse und keinen Port angeben.

> **Hinweis**
>
> Um andere Protokolle als HTTP und HTTPS im transparenten Proxymodus abzufangen, müssen Sie eine Listen-Policy hinzufügen und sie an den Proxyserver binden.

Konfigurieren Sie den SSL-Forward-Proxy mithilfe der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add cs vserver <name> PROXY <ipaddress> <port>
<!--NeedCopy-->
```

Argumente:

Name:

Name für den Proxyserver. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der virtuelle CS-Server erstellt wurde.

Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „mein Server“ oder „mein Server“).

Dieses Argument ist obligatorisch. Maximale Länge: 127

IP-Adresse:

Die IP-Adresse des Proxyservers.

Hafen:

Portnummer für den Proxyserver. Mindestwert: 1

Beispiel für einen expliziten Proxy:

```
add cs vserver swgVS PROXY 192.0.2.100 80
<!--NeedCopy-->
```

Beispiel für einen transparenten Proxy:

```
add cs vserver swgVS PROXY * *
<!--NeedCopy-->
```

Fügen Sie dem transparenten Proxyserver mithilfe der GUI eine Listenrichtlinie hinzu

1. Navigieren Sie zu **Sicherheit** > **SSL Forward Proxy** > **Proxy Virtual Servers**. Wählen Sie den transparenten Proxyserver und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie die **Grundeinstellungen**und klicken Sie auf **Mehr**.
3. Geben Sie im Feld **Listeningpriorität** den Wert 1
4. Geben Sie im Feld **Listeningrichtlinienausdruck** den folgenden Ausdruck ein:

   ```
   (CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
   <!--NeedCopy-->
   ```

> **Hinweis**
>
> Dieser Ausdruck setzt Standardports für HTTP- und HTTPS-Datenverkehr voraus. Wenn Sie verschiedene Ports konfiguriert haben, zum Beispiel 8080 für HTTP oder 8443 für HTTPS, ändern Sie den vorherigen Ausdruck, um diese Ports anzugeben.

SSL-Interception

May 11, 2023

Eine NetScaler-Appliance, die für SSL-Abfangen konfiguriert ist, fungiert als Proxy. Es kann SSL/TLS-Verkehr abfangen und entschlüsseln, die unverschlüsselte Anfrage überprüfen und es einem Administrator ermöglichen, Compliance-Regeln und Sicherheitsprüfungen durchzusetzen. Beim SSL-Abfangen wird eine Richtlinie verwendet, die festlegt, welcher Datenverkehr abgefangen, blockiert

oder zugelassen werden soll. Beispielsweise darf der Verkehr zu und von Finanzwebsites wie Banken nicht abgefangen werden, aber anderer Datenverkehr kann abgefangen werden, und Websites auf der schwarzen Liste können identifiziert und blockiert werden. Citrix empfiehlt, dass Sie eine generische Richtlinie zum Abfangen des Datenverkehrs und spezifischere Richtlinien konfigurieren, um einen Teil des Datenverkehrs zu Bypass.

Der Client und der Proxy richten einen HTTPS/TLS-Handshake ein. Der Proxy richtet einen weiteren HTTPS/TLS-Handshake mit dem Server ein und empfängt das Serverzertifikat. Der Proxy überprüft das Serverzertifikat im Namen des Clients und überprüft außerdem die Gültigkeit des Serverzertifikats mithilfe des Online Certificate Status Protocol (OCSP). Es regeneriert das Serverzertifikat, signiert es mit dem Schlüssel des auf der Appliance installierten CA-Zertifikats und präsentiert es dem Client. Daher wird ein Zertifikat zwischen dem Client und der NetScaler-Appliance und ein anderes Zertifikat zwischen der Appliance und dem Back-End-Server verwendet.

> **Wichtig**
>
> Das CA-Zertifikat, das zum Signieren des Serverzertifikats verwendet wird, muss auf allen Client-Geräten vorinstalliert sein, damit der Client dem neu generierten Serverzertifikat vertraut.

Bei abgefangenem HTTPS-Verkehr entschlüsselt der Proxyserver den ausgehenden Datenverkehr, greift auf die Klartext-HTTP-Anfrage zu und kann jede Layer-7-Anwendung zur Verarbeitung des Datenverkehrs verwenden, indem er beispielsweise die Klartext-URL untersucht und den Zugriff auf der Grundlage der Unternehmensrichtlinie und der URL-Reputation zulässt oder blockiert. Wenn die Richtlinienentscheidung darin besteht, den Zugriff auf den Originalserver zuzulassen, leitet der Proxyserver die erneut verschlüsselte Anfrage an den Zieldienst (auf dem Ursprungsserver) weiter. Der Proxy entschlüsselt die Antwort vom Ursprungsserver, greift auf die Klartext-HTTP-Antwort zu und wendet optional alle Richtlinien auf die Antwort an. Der Proxy verschlüsselt die Antwort dann erneut und leitet sie an den Client weiter. Wenn die Richtlinienentscheidung darin besteht, die Anfrage an den Ursprungsserver zu blockieren, kann der Proxy eine Fehlerantwort, z. B. HTTP 403, an den Client senden.

Um SSL-Interception durchzuführen, müssen Sie zusätzlich zu dem zuvor konfigurierten Proxyserver Folgendes auf der ADC-Appliance konfigurieren:

- SSL-Profil
- SSL-Richtlinie
- CA-Zertifikatsspeicher
- SSL-Fehler beim automatischen Lernen und Caching

> **Hinweis:**
>
> HTTP/2-Verkehr wird von der SSL-Interception-Funktion nicht abgefangen.

Speicher für SSL-Abhörzertifikate

Ein SSL-Zertifikat, das Teil einer SSL-Transaktion ist, ist ein digitales Datenformular (X509), das ein Unternehmen (Domain) oder eine Einzelperson identifiziert. Ein SSL-Zertifikat wird von einer Zertifizierungsstelle (CA) ausgestellt. Eine CA kann privat oder öffentlich sein. Von öffentlichen Zertifizierungsstellen wie Verisign ausgestellte Zertifikate werden von Anwendungen, die SSL-Transaktionen durchführen, als vertrauenswürdig eingestuft. Diese Anwendungen führen eine Liste von Zertifizierungsstellen, denen sie vertrauen.

Als Forward-Proxy führt die ADC-Appliance die Verschlüsselung und Entschlüsselung des Datenverkehrs zwischen einem Client und einem Server durch. Es fungiert als Server für den Client (Benutzer) und als Client für den Server. Bevor eine Appliance HTTPS-Verkehr verarbeiten kann, muss sie die Identität eines Servers überprüfen, um betrügerische Transaktionen zu verhindern. Daher muss die Appliance als Client für den Ursprungsserver das Ursprungsserverzertifikat überprüfen, bevor sie es akzeptiert. Um ein Serverzertifikat zu überprüfen, müssen alle Zertifikate (z. B. Root- und Zwischenzertifikate), die zum Signieren und Ausstellen des Serverzertifikats verwendet werden, auf der Appliance vorhanden sein. Ein Standardsatz von Zertifizierungsstellenzertifikaten ist auf einer Appliance vorinstalliert. Die Appliance kann diese Zertifikate verwenden, um fast alle gängigen Ursprungs-Serverzertifikate zu überprüfen. Dieser Standardsatz kann nicht geändert werden. Wenn für Ihre Bereitstellung jedoch mehr CA-Zertifikate erforderlich sind, können Sie ein Paket solcher Zertifikate erstellen und das Paket in die Appliance importieren. Ein Paket kann auch ein einzelnes Zertifikat enthalten.

Wenn Sie ein Zertifikatspaket in die Appliance importieren, lädt die Appliance das Paket vom Remote-Standort herunter und installiert es auf der Appliance, nachdem überprüft wurde, dass das Paket nur Zertifikate enthält. Sie müssen ein Zertifikatspaket anwenden, bevor Sie es zur Validierung eines Serverzertifikats verwenden können. Sie können ein Zertifikatspaket auch exportieren, um es zu bearbeiten oder als Backup an einem Offline-Ort zu speichern.

Importieren Sie ein CA-Zertifikatspaket und wenden Sie es mithilfe der CLI auf der Appliance an

Geben Sie in der Befehlszeile Folgendes ein:

```
import ssl certBundle <name> <src>
apply ssl certBundle <name>
<!--NeedCopy-->
```

```
show ssl certBundle
<!--NeedCopy-->
```

ARGUMENTE:

Name:

Name, der dem importierten Zertifikatspaket zugewiesen werden soll. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „meine Datei“ oder „meine Datei“).

Maximale Länge: 31

src:

URL, die das Protokoll, den Host und den Pfad einschließlich des Dateinamens zum Zertifikatspaket angibt, das importiert oder exportiert werden soll. Zum Beispiel `http://www.example.com/cert_bundle_file`.

HINWEIS: Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, für den Zugriff eine Client-Zertifikatsauthentifizierung erforderlich ist.

Maximale Länge: 2047

Beispiel:

```
import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
apply ssl certBundle swg-certbundle
<!--NeedCopy-->
```

```
show ssl certbundle

            Name : swg-certbundle(Inuse)

            URL : http://www.example.com/cert_bundle

    Done
<!--NeedCopy-->
```

Importieren Sie mithilfe der GUI ein CA-Zertifikatspaket und wenden Sie es auf der Appliance an

1. Navigieren Sie zu **Sicherheit > SSL Forward Proxy > Erste Schritte > Zertifikatpakete**.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie ein Zertifikatspaket aus der Liste aus.
   - Um ein Zertifikatpaket hinzuzufügen, klicken Sie auf “+” und geben Sie einen Namen und eine Quell-URL an. Klicken Sie auf **OK**.

3. Klicken Sie auf **OK**.

Entfernen Sie mithilfe der CLI ein CA-Zertifikatspaket von der Appliance

Geben Sie in der Befehlszeile Folgendes ein:

```
remove certBundle <cert bundle name>
<!--NeedCopy-->
```

Beispiel:

```
remove certBundle mytest-cacert
<!--NeedCopy-->
```

Exportieren Sie mithilfe der CLI ein CA-Zertifikatspaket aus der Appliance

Geben Sie in der Befehlszeile Folgendes ein:

```
export certBundle <cert bundle name> <Path to export>
<!--NeedCopy-->
```

ARGUMENTE:

Name:

Name, der dem importierten Zertifikatspaket zugewiesen werden soll. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleich (=) und Bindestrich (-) enthalten. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen (z. B. „meine Datei“ oder „meine Datei“).

Maximale Länge: 31

src:

URL, die das Protokoll, den Host und den Pfad einschließlich des Dateinamens zum Zertifikatspaket angibt, das importiert oder exportiert werden soll. Zum Beispiel `http://www.example.com/cert_bundle_file`.

HINWEIS: Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, für den Zugriff eine Client-Zertifikatsauthentifizierung erforderlich ist.

Maximale Länge: 2047

Beispiel:


```
export certBundle mytest-cacert http://192.0.2.20/
<!--NeedCopy-->
```

Ein CA-Zertifikatspaket aus dem Mozilla CA-Zertifikatsspeicher importieren, anwenden und verifizieren

Geben Sie in der Befehlszeile Folgendes ein:

```
> import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.
   pem
Done
<!--NeedCopy-->
```

Um das Paket anzuwenden, geben Sie Folgendes ein:

```
> apply certbundle mozilla_public_ca
Done
<!--NeedCopy-->
```

Um zu überprüfen, welches Zertifikatspaket verwendet wird, geben Sie Folgendes ein:

```
> sh certbundle | grep mozilla
                Name : mozilla_public_ca (Inuse)
<!--NeedCopy-->
```

Einschränkungen

- Zertifikatpakete werden in einem Cluster-Setup oder auf einer partitionierten Appliance nicht unterstützt.
- Das TLSv1.3-Protokoll wird mit SSL Forward Proxy nicht unterstützt.

SSL-Richtlinieninfrastruktur für SSL-Abfangen

Eine Richtlinie wirkt wie ein Filter für eingehenden Verkehr. Richtlinien auf der ADC-Appliance helfen dabei, zu definieren, wie Proxyverbindungen und Anfragen verwaltet werden. Die Verarbeitung basiert auf den Aktionen, die für diese Richtlinie konfiguriert sind. Das heißt, Daten in Verbindungsanfragen werden mit einer in der Richtlinie angegebenen Regel verglichen, und die Aktion wird auf Verbindungen angewendet, die der Regel (Ausdruck) entsprechen. Nachdem Sie eine Aktion definiert haben, die der Richtlinie zugewiesen werden soll, und die Richtlinie erstellt haben, müssen Sie sie an einen Proxyserver binden, damit sie für den Datenverkehr gilt, der über diesen Proxyserver fließt.

Eine SSL-Richtlinie für das SSL-Interception wertet eingehenden Datenverkehr aus und wendet eine vordefinierte Aktion auf Anforderungen an, die einer Regel (Ausdruck) entsprechen. Die Entscheidung, eine Verbindung abzufangen, zu Bypass oder zurückzusetzen, wird auf der Grundlage der definierten SSL-Richtlinie getroffen. Sie können eine von drei Aktionen für eine Richtlinie konfigurieren: ABFANGEN, BYPASS oder RESET. Sie müssen eine Aktion angeben, wenn Sie eine Richtlinie erstellen. Um eine Richtlinie in Kraft zu setzen, müssen Sie sie an einen Proxyserver auf der Appliance binden. Um anzugeben, dass eine Richtlinie für das SSL-Abfangen vorgesehen ist, müssen Sie den Typ (Bindungspunkt) als INTERCEPT_REQ angeben, wenn Sie die Richtlinie an einen Proxyserver binden. Wenn Sie die Bindung einer Richtlinie aufheben, müssen Sie den Typ als INTERCEPT_REQ angeben.

> **Hinweis**:
>
> Der Proxyserver kann keine Entscheidung zum Abfangen treffen, es sei denn, Sie geben eine Richtlinie an.

Das Abfangen des Datenverkehrs kann auf einem beliebigen SSL-Handshake-Attribut basieren. Die am häufigsten verwendete ist die SSL-Domain. Die SSL-Domain wird normalerweise durch die Attribute des SSL-Handshakes angezeigt. Hierbei kann es sich um den Wert Server Name Indicator handeln, der aus der SSL-Client-Hallo (falls vorhanden) extrahiert wurde, oder um den aus dem Ursprungsserverzertifikat extrahierten Wert (Server Alternate Name, SAN) handeln. Die SSL-Abhörrichtlinie enthält ein spezielles Attribut, DETECTED_DOMAIN. Dieses Attribut erleichtert es den Kunden, Abhörrichtlinien basierend auf der SSL-Domäne aus dem Ursprungsserverzertifikat zu erstellen. Der Kunde kann den Domänennamen mit einer Zeichenfolge, einer URL-Liste (URL-Gruppe oder`patset`) oder einer von der Domäne abgeleiteten URL-Kategorie abgleichen.

Erstellen einer SSL-Richtlinie über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add ssl policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Beispiele:

Die folgenden Beispiele beziehen sich auf Richtlinien mit Ausdrücken, die das Attribut `detected_domain` verwenden, um nach einem Domänennamen zu suchen.

Fangen Sie keinen Datenverkehr zu einem Finanzinstitut wie der XYZBANK ab

```
add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK"
    ) -action BYPASS
<!--NeedCopy-->
```


Erlaube einem Nutzer nicht, vom Unternehmensnetzwerk aus eine Verbindung zu YouTube herzustellen

```
add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.
   url_categorize(0,0).category.eq ("YouTube") -action RESET
<!--NeedCopy-->
```

Den gesamten Benutzerverkehr abfangen

```
add ssl policy pol3  - rule true  - action INTERCEPT
<!--NeedCopy-->
```

Wenn der Kunde die detected_domain nicht verwenden möchte, kann er jedes der SSL-Handshake-Attribute verwenden, um die Domain zu extrahieren und abzuleiten.

Beispielsweise wird in der SNI-Erweiterung der Client-Hello-Nachricht kein Domainname gefunden. Der Domainname muss dem Original-Serverzertifikat entnommen werden. Die folgenden Beispiele beziehen sich auf Richtlinien mit Ausdrücken, die nach einem Domainnamen im Betreffnamen des Originalserverzertifikats suchen.

Den gesamten Benutzerverkehr zu jeder Yahoo-Domain abfangen

```
add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.
   contains("yahoo")  - action INTERCEPT
<!--NeedCopy-->
```

Den gesamten Benutzerverkehr für die Kategorie „Einkaufen/Einzelhandel“ abfangen

```
add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
   subject.URL_CATEGORIZE(0,0).CATEGORY.eq("Shopping/Retail") -action
   INTERCEPT
<!--NeedCopy-->
```

Den gesamten Benutzerverkehr auf eine nicht kategorisierte URL abfangen

```
add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
   subject.url_categorize(0,0).category.eq("Uncategorized") -action
   INTERCEPT
<!--NeedCopy-->
```

Die folgenden Beispiele beziehen sich auf Richtlinien, die die Domain mit einem Eintrag in einem URL-Satz abgleichen.

Fangen Sie den gesamten Benutzerverkehr ab, wenn der Domainname in SNI mit einem Eintrag im URL-Satz „top100“ übereinstimmt


```
add ssl policy pol_url_set  -rule client.ssl.client_hello.SNI.
    URLSET_MATCHES_ANY("top100") -action INTERCEPT
<!--NeedCopy-->
```

Abfangen des gesamten Benutzerdatenverkehrs des Domänennamens, wenn das Ursprungsserverzertifikat mit einem Eintrag im URL-Satz top100 übereinstimmt

```
add ssl policy pol_url_set  -rule client.ssl.origin_server_cert.subject
    .URLSET_MATCHES_ANY("top100") -action INTERCEPT
<!--NeedCopy-->
```

Erstellen einer SSL-Richtlinie für einen Proxyserver mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.
2. Klicken Sie auf der Registerkarte **SSL-Richtlinien** auf **Hinzufügen** und geben Sie die folgenden Parameter an:
   - Richtlinienname
   - Richtlinienaktion — Wählen Sie zwischen Abfangen, Bypass oder Zurücksetzen.
   - Ausdruck
3. Klicken Sie auf **Erstellen**.

Binden Sie eine SSL-Richtlinie mithilfe der CLI an einen Proxyserver

Geben Sie in der Befehlszeile Folgendes ein:

```
bind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type  INTERCEPT_REQ
<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver <name> -policyName pol1 -priority 10 -type
    INTERCEPT_REQ
<!--NeedCopy-->
```

Binden Sie mithilfe der GUI eine SSL-Richtlinie an einen Proxyserver

1. Navigieren Sie zu **Sicherheit > SSL Forward Proxy > Proxy Virtual Servers**.
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie in **Erweiterte Einstellungen**auf **SSL-Richtlinien**.
4. Klicken Sie in das Feld **SSL-Richtlinie** .

5. **Wählen Sie unter Richtlinie**auswählen eine Richtlinie aus, die gebunden werden soll.
6. Wählen Sie unter **Typ**die Option **INTERCEPT_REQ**aus.
7. Klicken Sie auf **Bin** den und dann auf **OK** .

Aufheben der Bindung einer SSL-Richtlinie an einen Proxyserver über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
unbind ssl vserver <vServerName> -policyName <string> -type
   INTERCEPT_REQ
<!--NeedCopy-->
```

In SSL-Richtlinien verwendete SSL-Ausdrücke

Ausdruck	Beschreibung
`CLIENT.SSL.CLIENT_HELLO.SNI.*`	Gibt die SNI-Erweiterung in einem Zeichenkettenformat zurück. Wertet die Zeichenfolge aus, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.client_hello.sni.contains () “xyz.com”
`CLIENT.SSL.ORIGIN_SERVER_CERT.*`	Gibt ein Zertifikat, das von einem Back-End-Server empfangen wurde, in einem Zeichenfolgenformat zurück. Wertet die Zeichenfolge aus, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.origin_server_cert.subject.contains () “xyz.com”
`CLIENT.SSL.DETECTED_DOMAIN.*`	Gibt eine Domain, entweder aus der SNI-Erweiterung oder aus dem Originalserverzertifikat, in einem Zeichenfolgenformat zurück. Wertet die Zeichenfolge aus, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.detected_domain.contains () “xyz.com”

SSL-Fehler beim automatischen Lernen

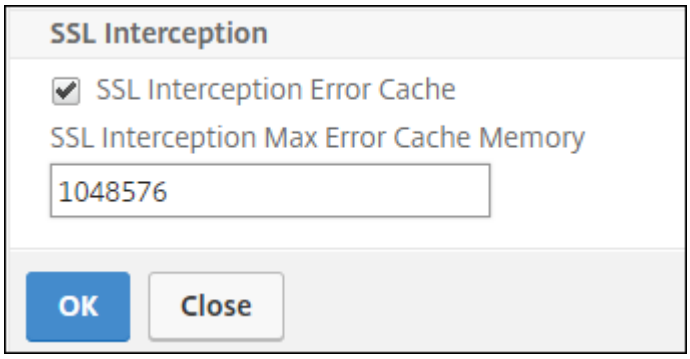
Die Appliance fügt der SSL-Bypass-Liste eine Domain hinzu, wenn der Lernmodus aktiviert ist. Der Lernmodus basiert auf der SSL-Warnmeldung, die entweder von einem Client oder einem Originalserver empfangen wurde. Das heißt, das Lernen hängt davon ab, dass der Client oder Server eine Warnmeldung sendet. Es erfolgt kein Lernen, wenn keine Warnmeldung gesendet wird. Das Gerät erkennt, ob eine der folgenden Bedingungen erfüllt ist:

1. Eine Anfrage für ein Client-Zertifikat wird vom Server empfangen.
2. Im Rahmen des Handshakes wird eine der folgenden Warnungen empfangen:
    - SCHLECHTES ZERTIFIKAT
    - NICHT UNTERSTÜTZTES ZERTIFIKAT
    - ZERTIFIKAT_GESPERRT
    - ZERTIFIKAT_ABGELAUFEN
    - ZERTIFIKAT_UNBEKANNT
    - UNKNOWN_CA (Wenn ein Client das Anpinnen verwendet, sendet er diese Warnmeldung, wenn er ein Serverzertifikat erhält.)
    - HANDSHAKE_FEHLER

Um das Lernen zu aktivieren, müssen Sie den Fehlercache aktivieren und den für das Lernen reservierten Speicher angeben.

Ermöglichen Sie das Lernen mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie in den **Einstellungen**auf **Erweiterte SSL-Einstellungen ändern**.
3. Wählen Sie unter **SSL Interception**die Option **SSL Interception Error Cache**aus.
4. Geben Sie unter **SSL Interception Max Error Cache Memory**den Speicher (in Byte) an, der reserviert werden soll.



5. Klicken Sie auf **OK**.

Ermöglichen Sie das Lernen mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED ) -
   ssliMaxErrorCacheMem <positive_integer>
<!--NeedCopy-->
```

Argumente:

SSLI-Fehlercache:

Aktivieren oder deaktivieren Sie dynamisches Lernen und speichern Sie die erlernten Informationen im Cache, um spätere Entscheidungen zum Abfangen oder Bypass von Anfragen zu treffen. Wenn diese Option aktiviert ist, führt die Appliance eine Cache-Suche durch, um zu entscheiden, ob die Anfrage Bypass werden soll.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

ssliMaxErrorCachemem:

Geben Sie den maximalen Speicher in Byte an, mit dem die gelernten Daten zwischengespeichert werden können. Dieser Speicher wird als LRU-Cache verwendet, sodass die alten Einträge durch neue Einträge ersetzt werden, nachdem das eingestellte Speicherlimit ausgeschöpft ist. Ein Wert von 0 bestimmt automatisch das Limit.

Standardwert: 0

Mindestwert: 0

maximaler Wert: 4294967294

SSL-Profil

Ein SSL-Profil ist eine Sammlung von SSL-Einstellungen wie Verschlüsselungen und Protokollen. Ein Profil ist hilfreich, wenn Sie gemeinsame Einstellungen für verschiedene Server haben. Anstatt für jeden Server dieselben Einstellungen anzugeben, können Sie ein Profil erstellen, die Einstellungen im Profil angeben und das Profil dann an verschiedene Server binden. Wenn kein benutzerdefiniertes Frontend-SSL-Profil erstellt wird, ist das Standard-Frontend-Profil an clientseitige Entitäten gebunden. Mit diesem Profil können Sie Einstellungen für die Verwaltung der clientseitigen Verbindungen konfigurieren.

Für das SSL-Abfangen müssen Sie ein SSL-Profil erstellen und das SSL-Abfangen im Profil aktivieren. Eine Standard-Verschlüsselungsgruppe ist an dieses Profil gebunden, Sie können jedoch weitere Verschlüsselungen konfigurieren, die zu Ihrem Einsatz passen. Binden Sie ein SSL-Interception-CA-Zertifikat an dieses Profil und binden Sie das Profil dann an einen Proxyserver. Für das Abfangen

von SSL sind die wesentlichen Parameter in einem Profil diejenigen, die für die folgenden Aktionen verwendet werden:

- Überprüfen Sie den OCSP-Status des Original-Serverzertifikats.
- Löse eine Neuverhandlung des Clients aus, wenn der Ursprungsserver eine Neuverhandlung anfordert.
- Überprüfen Sie das Originalserverzertifikat, bevor Sie die Front-End-SSL-Sitzung wiederverwenden.

Verwenden Sie das Standard-Back-End-Profil, wenn Sie mit den Originalservern kommunizieren. Stellen Sie alle serverseitigen Parameter, wie z. B. Cipher Suites, im Standard-Back-End-Profil ein. Ein benutzerdefiniertes Backend-Profil wird nicht unterstützt.

Beispiele für die am häufigsten verwendeten SSL-Einstellungen finden Sie unter „Beispielprofil“ am Ende dieses Abschnitts.

Die Verschlüsselungs-/Protokollunterstützung unterscheidet sich je nach internem und externem Netzwerk. In den folgenden Tabellen ist die Verbindung zwischen den Benutzern und einer ADC-Appliance das interne Netzwerk. Das externe Netzwerk befindet sich zwischen der Appliance und dem Internet.

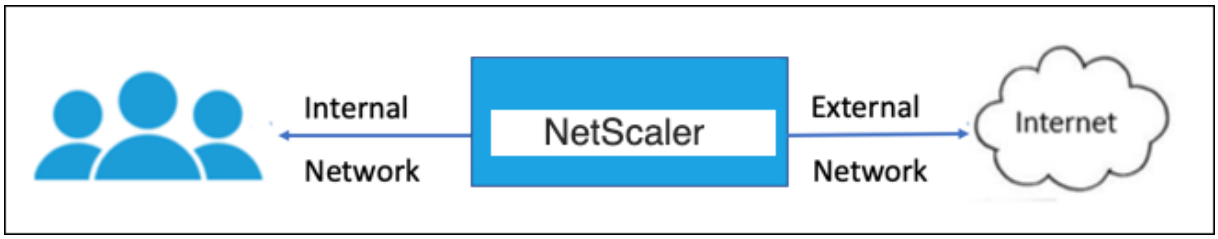


Tabelle 1: Verschlüsselungs-/Protokoll -Unterstützungsmatrix für das interne Netzwerk

Siehe Tabelle 1-Support für virtuelle Server/Frontend-Service/internen Dienst in Ciphers, die auf den NetScaler Appliances verfügbar sind.

Tabelle 2: Verschlüsselung/Protokoll-Unterstützungsmatrix für das externe Netzwerk

Siehe Tabelle 2-Unterstützung für Back-End-Dienste in Ciphers, die auf den NetScaler Appliances verfügbar sind.

Hinzufügen eines SSL-Profils und Aktivieren der SSL-Interception mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED |
 DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer <
positive_integer>
```

Argumente:

SSL-Abfangen:

Aktiviert oder deaktiviert das Abfangen von SSL-Sitzungen.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

SSLI Rene sagt:

Aktiviert oder deaktiviert das Auslösen einer Neuverhandlung durch den Client, wenn eine Neuverhandlungsanfrage vom Originalserver eingeht.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

SSLIOCSP-Prüfung:

Aktiviere oder deaktiviere die OCSP-Prüfung für ein Originalserverzertifikat.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

SSLIMax SSESpro Server:

Maximale Anzahl von SSL-Sitzungen, die pro dynamischem Ursprungsserver zwischengespeichert werden sollen. Für jede SNI-Erweiterung, die vom Client in einer Client-Hello-Nachricht empfangen wird, wird eine eindeutige SSL-Sitzung erstellt. Die passende Sitzung wird für die Wiederverwendung von Serversitzungen verwendet.

Standardwert: 10

Mindestwert: 1

Maximalwert: 1000

Beispiel:

```
add ssl profile swg_ssl_profile  -sslinterception ENABLED

Done

sh ssl profile swg_ssl_profile

1)    Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED
```



```
12
13                  Use only bound CA certificates: DISABLED
14
15                  Strict CA checks:                                   NO
16
17                  Session Reuse: ENABLED
                        Timeout: 120 seconds
18
19                  DH: DISABLED
20
21                  DH Private-Key Exponent Size Limit: DISABLED
                        Ephemeral RSA: ENABLED
                        Refresh Count: 0
22
23                  Deny SSL Renegotiation
                        ALL
24
25                  Non FIPS Ciphers: DISABLED
26
27                  Cipher Redirect: DISABLED
28
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:              1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                          NO
44
45                  Push flag:             0x0 (Auto)
46
47                  SSL quantum size:                               8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:                45
```



```
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                        Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                        Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75 1)             Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79 Done
80 <!--NeedCopy-->
```

Binden Sie ein SSL-Interception-CA-Zertifikat mithilfe der CLI an ein SSL-Profil

Geben Sie in der Befehlszeile Folgendes ein:

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert>
```

Beispiel:

```
1 bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
2
3 Done
4
5 sh ssl profile swg_ssl_profile
```



```
6
7  1)            Name: swg_ssl_profile (Front-End)
8
9                  SSLv3: DISABLED              TLSv1.0: ENABLED  TLSv1
                       .1: ENABLED  TLSv1.2: ENABLED
10
11                 Client Auth: DISABLED
12
13                 Use only bound CA certificates: DISABLED
14
15                 Strict CA checks:                                NO
16
17                 Session Reuse: ENABLED
                       Timeout: 120 seconds
18
19                 DH: DISABLED
20
21                 DH Private-Key Exponent Size Limit: DISABLED
                       Ephemeral RSA: ENABLED
                       Refresh Count: 0
22
23                 Deny SSL Renegotiation
                       ALL
24
25                 Non FIPS Ciphers: DISABLED
26
27                 Cipher Redirect: DISABLED
28
29                 SSL Redirect: DISABLED
30
31                 Send Close-Notify: YES
32
33                 Strict Sig-Digest Check: DISABLED
34
35                 Push Encryption Trigger: Always
36
37                 PUSH encryption trigger timeout:             1 ms
38
39                 SNI: DISABLED
40
41                 OCSP Stapling: DISABLED
42
43                 Strict Host Header check for SNI enabled SSL sessions:
                                           NO
44
```



```
                  Push flag:            0x0 (Auto)

                  SSL quantum size:                              8 kB

                  Encryption trigger timeout           100 mS

                  Encryption trigger packet count:                45

                  Subject/Issuer Name Insertion Format: Unicode

                  SSL Interception: ENABLED

                  SSL Interception OCSP Check: ENABLED

                  SSL Interception End to End Renegotiation: ENABLED

                  SSL Interception Server Cert Verification for Client
                     Reuse: ENABLED

                  SSL Interception Maximum Reuse Sessions per Server:  10

                  Session Ticket: DISABLED              Session Ticket
                     Lifetime: 300 (secs)

                  HSTS: DISABLED

                  HSTS IncludeSubDomains: NO

                  HSTS Max-Age: 0

                  ECC Curve: P_256, P_384, P_224, P_521

1)             Cipher Name: DEFAULT Priority :1

                  Description: Predefined Cipher Alias

1)             SSL Interception CA CertKey Name: swg_ca_cert

Done
<!--NeedCopy-->
```

Binden Sie ein SSL-Interception-CA-Zertifikat mithilfe der GUI an ein SSL-Profil

1. Navigieren Sie zu **System** > **Profile** > **SSL-Profil**.

2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für das Profil an.
4. Aktivieren Sie das **Abfangen von SSL-Sitzungen**.
5. Klicken Sie auf **OK**.
6. Klicken Sie in **den Erweiterten Einstellungen**auf **Zertifikatsschlüssel**.
7. Geben Sie einen SSL-Interception-CA-Zertifikatsschlüssel an, der an das Profil gebunden werden soll.
8. Klicken Sie auf **Auswählen** und dann auf **Binden**.
9. Konfigurieren Sie optional Verschlüsselungen, die zu Ihrem Einsatz passen.
   - Klicken Sie auf das Bearbeitungssymbol und dann auf **Hinzufügen**.
   - Wählen Sie eine oder mehrere Verschlüsselungsgruppen aus und klicken Sie auf den Rechtspfeil.
   - Klicken Sie auf **OK**.
10. Klicken Sie auf **Fertig**.

Binden Sie ein SSL-Profil mithilfe der GUI an einen Proxyserver

1. Navigieren Sie zu **Security** >**SSL Forward Proxy** > **Proxy Virtual Servers**und fügen Sie einen Server hinzu oder wählen Sie einen Server aus, den Sie ändern möchten.
2. Klicken Sie im **SSL-Profil**auf das Bearbeitungssymbol.
3. Wählen Sie in der **SSL-Profilliste** das SSL-Profil aus, das Sie zuvor erstellt haben.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig**.

Beispielprofil:

```
Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED              TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

                Strict CA checks:                                NO

                Session Reuse: ENABLED
                   Timeout: 120 seconds
```



```
12
13                  DH: DISABLED
14
15                  DH Private-Key Exponent Size Limit: DISABLED
                        Ephemeral RSA: ENABLED
                        Refresh Count: 0
16
17                  Deny SSL Renegotiation
                        ALL
18
19                  Non FIPS Ciphers: DISABLED
20
21                  Cipher Redirect: DISABLED
22
23                  SSL Redirect: DISABLED
24
25                  Send Close-Notify: YES
26
27                  Strict Sig-Digest Check: DISABLED
28
29                  Push Encryption Trigger: Always
30
31                  PUSH encryption trigger timeout:              1 ms
32
33                  SNI: DISABLED
34
35                  OCSP Stapling: DISABLED
36
37                  Strict Host Header check for SNI enabled SSL sessions:
                                          NO
38
39                  Push flag:             0x0 (Auto)
40
41                  SSL quantum size:                               8 kB
42
43                  Encryption trigger timeout           100 mS
44
45                  Encryption trigger packet count:                 45
46
47                  Subject/Issuer Name Insertion Format: Unicode
48
49                  SSL Interception: ENABLED
50
51                  SSL Interception OCSP Check: ENABLED
52
```



```
53                  SSL Interception End to End Renegotiation: ENABLED
54
55                  SSL Interception Maximum Reuse Sessions per Server:  10
56
57                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
58
59                  HSTS: DISABLED
60
61                  HSTS IncludeSubDomains: NO
62
63                  HSTS Max-Age: 0
64
65                  ECC Curve: P_256, P_384, P_224, P_521
66
67 1)             Cipher Name: DEFAULT Priority :1
68
69                  Description: Predefined Cipher Alias
70
71 1)             SSL Interception CA CertKey Name: swg_ca_cert
72 <!--NeedCopy-->
```

Verwaltung der Benutzeridentität

May 11, 2023

Eine zunehmende Anzahl von Sicherheitsverletzungen und die wachsende Beliebtheit mobiler Geräte haben die Notwendigkeit unterstrichen, sicherzustellen, dass die Nutzung des externen Internets den Unternehmensrichtlinien entspricht. Nur autorisierte Benutzer dürfen Zugriff auf externe Ressourcen erhalten, die vom Unternehmenspersonal bereitgestellt werden. Identity Management macht es möglich, indem die Identität einer Person oder eines Geräts überprüft wird. Es wird nicht festgelegt, welche Aufgaben die Person übernehmen kann oder welche Dateien die Person sehen kann.

Eine SSL-Forward-Proxy-Bereitstellung identifiziert den Benutzer, bevor der Zugriff auf das Internet gewährt wird. Alle Anfragen und Antworten des Benutzers werden geprüft. Benutzeraktivitäten werden protokolliert und Datensätze werden zur Berichterstattung in das NetScaler Application Delivery Management (ADM) exportiert. In NetScaler ADM können Sie die Statistiken zu Benutzeraktivitäten, Transaktionen und Bandbreitenverbrauch anzeigen.

Standardmäßig wird nur die IP-Adresse des Benutzers gespeichert, aber Sie können die Funktion so konfigurieren, dass weitere Details über den Benutzer aufgezeichnet werden. Sie können diese Identitätsinformationen verwenden, um umfangreichere Richtlinien zur Internetnutzung für bestimmte

Benutzer zu erstellen.

Die NetScaler-Appliance unterstützt die folgenden Authentifizierungsmodi für eine Konfiguration mit expliziten Proxys.

- **Leichtes Directory-Zugriffsprotokoll (LDAP)**. Authentifiziert den Benutzer über einen externen LDAP-Authentifizierungsserver. Weitere Informationen finden Sie unter LDAP-Authentifizierungsrichtlinien.
- **RADIUS**. Authentifiziert den Benutzer über einen externen RADIUS-Server. Weitere Informationen finden Sie unter RADIUS-Authentifizierung.
- **TACACS +**. Authentifiziert den Benutzer über einen externen TACACS-Authentifizierungsserver (Terminal Access Controller Access-Control System). Weitere Informationen finden Sie unter TACACS-Authentifizierungsrichtlinien.
- **Verhandeln**. Authentifiziert den Benutzer über einen Kerberos-Authentifizierungsserver. Wenn bei der Kerberos-Authentifizierung ein Fehler auftritt, verwendet die Appliance die NTLM-Authentifizierung. Weitere Informationen finden Sie unter Authentifizierungsrichtlinien aushandeln.

Bei transparentem Proxy wird nur IP-basierte LDAP-Authentifizierung unterstützt. Wenn eine Clientanforderung empfangen wird, authentifiziert der Proxy den Benutzer, indem er einen Eintrag für die Client-IP-Adresse im Active Directory überprüft. Anschließend wird eine Sitzung basierend auf der Benutzer-IP-Adresse erstellt. Wenn Sie jedoch das SSONameAttribute in einer LDAP-Aktion konfigurieren, wird eine Sitzung mithilfe des Benutzernamens anstelle der IP-Adresse erstellt. Klassische Richtlinien werden für die Authentifizierung in einem transparenten Proxy-Setup nicht unterstützt.

> **Hinweis**
>
> Für einen expliziten Proxy müssen Sie den LDAP-Anmeldenamen auf **saAccountName**festlegen. Für einen transparenten Proxy müssen Sie den LDAP-Anmeldenamen auf **NetworkAddress** und attribute1 auf **sAMAccountName**festlegen.

Beispiel für einen expliziten Proxy:

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
      10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
      CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
      freebsd123$ -ldapLoginName sAMAccountName
2 <!--NeedCopy-->
```

Beispiel für einen transparenten Proxy:

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
      10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
      CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
      freebsd123$ -ldapLoginName networkAddress -authentication disable -
      Attribute1 sAMAccountName
```



```
<!--NeedCopy-->
```

Richten Sie die Benutzerauthentifizierung über die CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication vserver <vserver name> SSL

bind ssl vserver <vserver name> -certkeyName <certkey name>

add authentication ldapAction <action name> -serverIP <ip_addr> -
    ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
    ldapLoginName <string>

add authentication Policy <policy name> -rule <expression> -action <
    string>

bind authentication vserver <vserver name> -policy <string> -priority <
    positive_integer>

set cs vserver <name> -authn401 ON -authnVsName <string>
<!--NeedCopy-->
```

Argumente:

Vservername:

Name des virtuellen Authentifizierungsservers, an den die Richtlinie gebunden werden soll.

Maximale Länge: 127

serviceType:

Protokolltyp des virtuellen Authentifizierungsservers. Immer SSL.

Mögliche Werte: SSL

Standardwert: SSL

Name der Aktion:

Name für die neue LDAP-Aktion. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem die LDAP-Aktion hinzugefügt wurde. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Authentifizierungsaktion” oder “meine Authentifizierungsaktion”).

Maximale Länge: 127

serverIP:

Dem LDAP-Server zugewiesene IP-Adresse.

ldapBase:

Basis (Knoten), von der aus die LDAP-Suche gestartet werden soll. Wenn der LDAP-Server lokal läuft, ist der Standardwert von base dc=netscaler, dc=com. Maximale Länge: 127

ldapBindDn:

Vollständiger Distinguished Name (DN), der zur Bindung an den LDAP-Server verwendet wird.

Standard: CN=Manager,dc=netscaler,dc=com

Maximale Länge: 127

ldapBindDnPassword:

Kennwort zur Bindung an den LDAP-Server.

Maximale Länge: 127

ldapLoginName:

LDAP-Anmeldenamen-Attribut. Die NetScaler-Appliance verwendet den LDAP-Anmeldenamen, um externe LDAP-Server oder Active Directories abzufragen. Maximale Länge: 127

Name der Richtlinie:

Name für die erweiterte AUTHENTIFIZIERUNGSRICHTLINIE. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen ( ), Leerzeichen ( ), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem eine AUTHENTIFIZIERUNGSRICHTLINIE erstellt wurde. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Authentifizierungsrichtlinie” oder “meine Authentifizierungsrichtlinie”).

Maximale Länge: 127

rule:

Name der Regel oder ein erweiterter Richtlinienausdruck, den die Richtlinie verwendet, um zu bestimmen, ob versucht wird, den Benutzer beim AUTHENTICATION-Server zu authentifizieren.

Maximale Länge: 1499

action:

Name der Authentifizierungsaktion, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt.

Maximale Länge: 127

priority:

Positive Ganzzahl, die die Priorität der Richtlinie angibt. Eine niedrigere Zahl gibt eine höhere Priorität an. Richtlinien werden in der Reihenfolge ihrer Prioritäten bewertet, und die erste Richtlinie, die der Anforderung entspricht, wird angewendet. Muss in der Liste der an den virtuellen Authentifizierungsserver gebundenen Richtlinien eindeutig sein.

Mindestwert: 0

Maximaler Wert: 4294967295

Beispiel:

```
add authentication vserver swg-auth-vs SSL

Done

bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey

Done

add authentication ldapAction swg-auth-action-explicit -serverIP
    192.0.2.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "CN=
    Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword zzzzz
     -ldapLoginName sAMAccountName

Done

add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
    action-explicit
Done

bind authentication vserver swg-auth-vs -policy swg-auth-policy -
    priority 1

Done

set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs

Done
<!--NeedCopy-->
```


Aktivieren Sie die Benutzernamenprotokollierung über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

Argumente:

AAAUserName

Aktivieren Sie die AppFlow-Authentifizierung, Autorisierung und Überwachung der Benutzernamenprotokollierung.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

Beispiel:

```
set appflow param -AAAUserName ENABLED
<!--NeedCopy-->
```

URL-Filterung

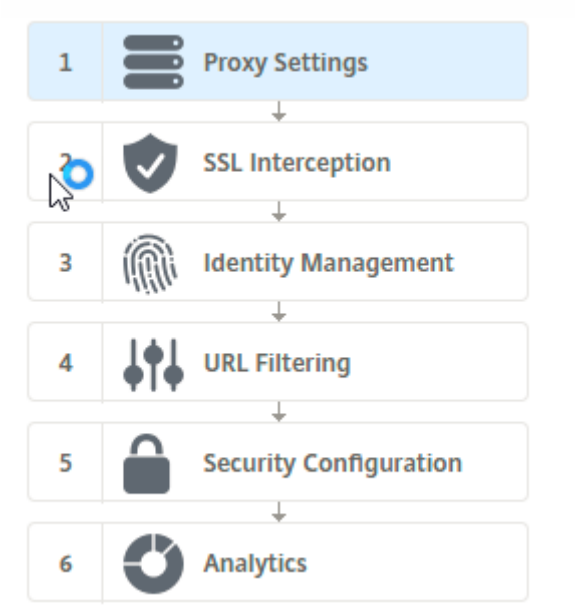
August 15, 2023

> **Hinweis:**
>
> Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

Die URL-Filterung ermöglicht die richtlinienbasierte Steuerung von Websites mithilfe der in URLs enthaltenen Informationen. Mit dieser Funktion können Netzwerkadministratoren den Benutzerzugriff auf bösartige Websites im Netzwerk überwachen und kontrollieren.

Erste Schritte

Wenn Sie ein neuer Benutzer sind und die URL-Filterung konfigurieren möchten, müssen Sie das anfängliche SSL-Forward-Proxy-Setup abschließen. Um mit der URL-Filterung zu beginnen, müssen Sie sich zuerst beim SSL-Forward-Proxyassistenten anmelden. Der Assistent führt Sie durch eine Reihe von Konfigurationsschritten, bevor Sie die URL-Filterrichtlinien anwenden.



> **Hinweis**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie eine gültige URL Threat Intelligence-Feature-Lizenz auf Ihrer Appliance installiert haben. Wenn Sie eine Testversion verwenden, stellen Sie sicher, dass Sie eine gültige Lizenz erwerben, um diese Funktion auf der ADC-Appliance weiterhin nutzen zu können.

Melden Sie sich beim SSL-Forward-Proxyassistenten an

Der SSL-Forward-Proxyassistent führt Sie durch eine Reihe vereinfachter Konfigurationsaufgaben. Im rechten Bereich wird die entsprechende Flow-Sequenz angezeigt. Mit diesem Assistenten können Sie URL-Filterrichtlinien auf eine URL-Liste oder eine vordefinierte Liste von Kategorien anwenden.

Schritt 1: Proxy-Einstellungen konfigurieren

Konfigurieren Sie zunächst einen Proxyserver, über den der Client auf das Gateway zugreift. Dieser Server ist vom Typ SSL und arbeitet im expliziten oder transparenten Modus. Weitere Informationen zur Proxy-Serverkonfiguration finden Sie unter Proxy-Modi.

Schritt 2: Konfigurieren von SSL-Interception

Nach der Konfiguration des Proxyservers müssen Sie den SSL-Abfang-Proxy konfigurieren, um verschlüsselten Datenverkehr auf der NetScaler-Appliance abzufangen. Im Falle der URL-Filterung fängt der SSL-Proxy den Datenverkehr ab und lässt keine blockierten URLs zu, während der gesamte andere Datenverkehr umgangen werden kann. Weitere Informationen zum Konfigurieren von SSL-Interception finden Sie unter SSL-Interception.

Schritt 3: Konfigurieren der Identitätsverwaltung

Ein Benutzer wird authentifiziert, bevor er sich am Unternehmensnetzwerk anmelden darf. Die Authentifizierung bietet die Flexibilität, spezifische Richtlinien für einen Benutzer oder eine Gruppe von Benutzern basierend auf ihren Rollen zu definieren. Weitere Informationen zur Benutzerauthentifizierung finden Sie unter Verwaltung der Benutzeridentifizierung.

Schritt 4: URL-Filterung konfigurieren

Der Administrator kann eine URL-Filterrichtlinie entweder mit der URL-Kategorisierungsfunktion oder mit der URL-Listenfunktion anwenden.

URL-Kategorisierung. Steuert den Zugriff auf Websites und Webseiten, indem der Datenverkehr basierend auf einer vordefinierten Liste von Kategorien gefiltert wird.

URL-Liste. Steuert den Zugriff auf Websites und Webseiten auf der Sperrliste, indem der Zugriff auf URLs verweigert wird, die in einen in die Appliance importierten URLs enthalten sind.

Schritt 5: Konfiguration der Sicherheitskonfiguration

In diesem Schritt können Sie einen Reputationswert konfigurieren und Benutzern ermöglichen, den Zugriff auf die Websites zu kontrollieren, indem sie den Zugriff verweigern, wenn die Bewertung zu niedrig ist. Ihr Reputationswert kann zwischen eins und vier liegen, und Sie können den Schwellenwert konfigurieren, ab dem die Bewertung inakzeptabel wird. Bei Bewertungen, die den Schwellenwert überschreiten, können Sie eine Richtlinienaktion auswählen, um Datenverkehr zuzulassen, zu blockieren oder umzuleiten. Weitere Informationen finden Sie unter URL Reputation Score.

Schritt 6: Konfigurieren der SSL-Forward-Proxyanalyse

Mit diesem Schritt können Sie SSL-Proxyanalysen für die Kategorisierung des Webverkehrs aktivieren, URL-Kategorie in den Benutzertransaktionsprotokollen protokollieren und Datenverkehrsanalysen anzeigen. Weitere Informationen zu SSL-Forward-Proxy-Analysen finden Sie unter Analytics.

Schritt 7: Klicken Sie auf "Fertig", um die Erstkonfiguration abzuschließen und die URL-Filterkonfiguration fortzusetzen

URL-Liste

August 15, 2023

Mit der URL-Listenfunktion können Unternehmenskunden den Zugriff auf bestimmte Websites und Webseitenkategorien kontrollieren. Die Funktion filtert Websites, indem eine Responder-Richtlinie

angewendet wird, die an einen URL-Abgleichsalgorythmus gebunden ist. Der Algorithmus gleicht die eingehende URL mit einem URL-Satz ab, der aus bis zu einer Million (1.000.000) Einträgen besteht. Wenn die eingehende URL-Anfrage mit einem Eintrag im Set übereinstimmt, verwendet die Appliance die Responder-Richtlinie, um die Anfrage auszuwerten (HTTP/HTTPS) und den Zugriff darauf zu steuern.

Typen von URL-Sets

Jeder Eintrag in einem URL-Satz kann eine URL und optional die zugehörigen Metadaten (URL-Kategorie, Kategoriegruppen oder andere verwandte Daten) enthalten. Bei URLs mit Metadaten verwendet die Appliance einen Richtlinienausdruck, der die Metadaten auswertet. Weitere Informationen finden Sie unter URL-Set.

SSL Forward-Proxy unterstützt benutzerdefinierte URL-Sets. Sie können auch Mustersätze verwenden, um URLs zu filtern.

Benutzerdefinierter URL-Satz. Sie können ein benutzerdefiniertes URL-Set mit bis zu 1.000.000 URL-Einträgen erstellen und es als Textdatei in Ihre Appliance importieren.

Musterset Eine ADC-Appliance kann Mustersätze verwenden, um URLs zu filtern, bevor Zugriff auf Websites gewährt wird. Ein Mustersatz ist ein Zeichenfolge-Matching-Algorithmus, der nach einer genauen Übereinstimmung zwischen einer eingehenden URL und bis zu 5000 Einträgen sucht. Weitere Informationen finden Sie unter Musterset.

Jede URL in einem importierten URL-Satz kann eine benutzerdefinierte Kategorie in Form von URL-Metadaten aufweisen. Ihre Organisation kann das Set hosten und die ADC-Appliance so konfigurieren, dass sie das Set regelmäßig aktualisiert, ohne dass ein manuelles Eingreifen erforderlich ist.

Nachdem das Set aktualisiert wurde, erkennt die NetScaler Appliance die Metadaten automatisch. Die Kategorie ist jetzt als Richtlinienausdruck verfügbar, um die URL auszuwerten und Aktionen wie Zulassen, Blockieren, Weiterleiten oder Benachrichtigung des Benutzers anzuwenden.

Erweiterte Richtlinienausdrücke, die mit URL-Sätzen verwendet werden

In der folgenden Tabelle werden die grundlegenden Ausdrücke beschrieben, die Sie zur Bewertung des eingehenden Datenverkehrs verwenden können.

1. .URLSET_MATCHES_ANY — Wird mit TRUE ausgewertet, wenn die URL genau mit einem Eintrag im URL-Satz übereinstimmt.
2. .GET_URLSET_METADATA () — Der Ausdruck GET_URLSET_METADATA () gibt die zugehörigen Metadaten zurück, wenn die URL genau mit einem Muster innerhalb des URL-Sets übereinstimmt. Eine leere Zeichenfolge wird zurückgegeben, wenn es keine Übereinstimmung gibt.

3. .GET_ URLSET_METADATA().EQ(<METADATA)- .GET_ URLSET_METADATA().EQ(<METADATA)
4. .GET_URLSET_METADATA () .TYPECAST_LIST_T (‘,’) .GET (0) .EQ () — Wird als TRUE ausgewertet, wenn sich die übereinstimmenden Metadaten am Anfang der Kategorie befinden. Dieses Muster kann verwendet werden, um separate Felder innerhalb von Metadaten zu kodieren, aber nur für das erste Feld.
5. HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) — Verbindet die Host- und URL-Parameter, die dann für den Abgleich verwendet werden können.

Typen von Responder-Aktionen

> **Hinweis:** In der Tabelle wird HTTP.REQ.URL als verallgemeinert. <URL expression>

In der folgenden Tabelle werden die Aktionen beschrieben, die auf eingehenden Internetverkehr angewendet werden können.

Responder-Aktion	Beschreibung
Allow	Erlauben Sie der Anfrage, auf die Ziel-URL zuzugreifen.
Umleiten	Leitet die Anfrage an die als Ziel angegebene URL weiter.
Blockieren	Lehnen Sie die Anfrage ab.

Voraussetzungen

Konfigurieren Sie einen DNS-Server, wenn Sie einen URL-Satz aus einer Hostnamen-URL importieren. Diese Konfiguration ist nicht erforderlich, wenn Sie eine IP-Adresse verwenden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns nameServer ((<IP> [-local])| <dnsVserverName>)[-state (ENABLED |
DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

Beispiel:

```
add dns nameServer 10.140.50.5
```

Eine URL-Liste konfigurieren

Um eine URL-Liste zu konfigurieren, können Sie den Citrix SSL Forward Proxy Wizard oder die NetScaler-Befehlszeilenschnittstelle (CLI) verwenden. Auf der NetScaler-Appliance müssen Sie zuerst die Responder-Richtlinie konfigurieren und dann die Richtlinie an einen URL-Satz binden.

Citrix empfiehlt, den Citrix SSL Forward Proxy Wizard als bevorzugte Option für die Konfiguration einer URL-Liste zu verwenden. Verwenden Sie den Assistenten, um eine Responder-Richtlinie an einen URL-Satz zu binden. Alternativ können Sie die Richtlinie an einen Mustersatz binden.

Konfigurieren Sie eine URL-Liste mithilfe des SSL-Forward-Proxyassistenten

So konfigurieren Sie die URL-Liste für HTTPS-Verkehr mithilfe der GUI:

1. Navigieren Sie zur Seite **Sicherheit** > **SSL Forward Proxy** .
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   a) Klicken Sie auf **SSL Forward Proxy Wizard**.
   b) Wählen Sie eine vorhandene Konfiguration aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt " **URL-Filter** " auf **Bearbeiten**.
4. Markieren Sie das Kontrollkästchen **URL-Liste**, um die Funktion zu aktivieren.
5. Wählen Sie eine **URL-Listenrichtlinie** aus und klicken Sie auf **Binden**.
6. Klicken Sie auf **Weiter** und dann **Fertig**.

Weitere Informationen finden Sie unter Erstellen einer URL-Listenrichtlinie.

Konfigurieren einer URL-Liste mit der CLI

Gehen Sie wie folgt vor, um eine URL-Liste zu konfigurieren.

1. Konfigurieren Sie einen virtuellen Proxyserver für HTTP- und HTTPS-Verkehr.
2. Konfigurieren Sie die SSL-Interception zum Abfangen von HTTPS-Verkehr.
3. Konfigurieren Sie eine URL-Liste, die einen URL-Satz für HTTP-Verkehr enthält.
4. Konfigurieren Sie die URL-Liste, die URLs enthält, die für den HTTPS-Verkehr festgelegt wurden.
5. Konfigurieren Sie einen privaten URL-Satz.

> **Hinweis**
>
> Wenn Sie bereits eine ADC-Appliance konfiguriert haben, können Sie die Schritte 1 und 2 überspringen und mit Schritt 3 konfigurieren.

Konfiguration eines virtuellen Proxyservers für den Internetverkehr

Die NetScaler-Appliance unterstützt transparente und explizite virtuelle Proxyserver. Gehen Sie wie folgt vor, um einen virtuellen Proxyserver für den Internetverkehr im expliziten Modus zu konfigurieren:

1. Fügen Sie einen virtuellen Proxyserver für SSL hinzu.
2. Binden Sie eine Responder-Richtlinie an den virtuellen Proxyserver.

So fügen Sie mithilfe der CLI einen virtuellen Proxyserver hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
<!--NeedCopy-->
```

So binden Sie eine Responder-Richtlinie mithilfe der CLI an einen virtuellen Proxyserver:

```
bind ssl vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn Sie den SSL-Interceptor bereits als Teil der NetScaler-Konfiguration konfiguriert haben, können Sie das folgende Verfahren überspringen.

SSL-Abfangen für HTTPS-Verkehr konfigurieren

Gehen Sie wie folgt vor, um das SSL-Abfangen für den HTTPS-Verkehr zu konfigurieren:

1. Binden Sie ein CA-Zertifikatsschlüsselpaar an den virtuellen Proxyserver.
2. Aktivieren Sie das Standard-SSL-Profil.
3. Erstellen Sie ein Front-End-SSL-Profil, binden Sie es an den virtuellen Proxyserver und aktivieren Sie das SSL-Abfangen im Front-End-SSL-Profil.

So binden Sie ein Zertifizierungsstellen-Schlüsselpaar mit der Befehlszeilenschnittstelle an den virtuellen Proxyserver:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
<!--NeedCopy-->
```

So konfigurieren Sie ein Front-End-SSL-Profil mithilfe der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -defaultProfile ENABLED

add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
    positive_integer>
<!--NeedCopy-->
```


So binden Sie ein Front-End-SSL-Profil mithilfe der CLI an einen virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServer name>  -sslProfile <name>
<!--NeedCopy-->
```

Konfigurieren einer URL-Liste durch Importieren eines URL-Sets für HTTP-Datenverkehr

Informationen zum Konfigurieren eines URL-Sets für HTTP-Datenverkehr finden Sie unter URL-Set.

Explizite Subdomain-Übereinstimmung durchführen

Sie können jetzt eine explizite Subdomain-Übereinstimmung für einen importierten URL-Satz durchführen. Ein neuer Parameter, “subdomainExactMatch”, wird dem Befehl **import** policy URLset hinzugefügt.

Wenn Sie den Parameter aktivieren, führt der URL-Filter-Algorithmus eine explizite Subdomain-Übereinstimmung durch. Wenn die eingehende URL beispielsweise lautet news.example.com und wenn der Eintrag im URL-Satz lautet example.com, stimmt der Algorithmus nicht mit den URLs überein.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```

Beispiel

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet -
subdomainExactMatch -interval 900
```

Konfigurieren Sie einen URL-Satz für HTTPS-Verkehr

So konfigurieren Sie ein URL-Set für HTTPS-Verkehr mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl policy <name> -rule <expression> -action <string> [-undefAction
     <string>] [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
   URLSET_MATCHES_ANY("top1m") -action INTERCEPT
```



```
<!--NeedCopy-->
```

So konfigurieren Sie einen URL-Satz für HTTPS-Verkehr mithilfe des SSL-Forward-Proxyassistenten

Citrix empfiehlt, den SSL-Forward-Proxyassistenten als bevorzugte Option für die Konfiguration einer URL-Liste zu verwenden. Verwenden Sie den Assistenten, um einen benutzerdefinierten URL-Satz zu importieren und an eine Responder-Richtlinie zu binden.

1. Navigieren Sie zu **Sicherheit > SSL-Forward-Proxy > URL-Filterung > URL-Listen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie auf der Seite “ **Richtlinie für URL-Liste** “ den Richtliniennamen an.
4. Wählen Sie eine Option aus, um einen URL-Satz zu importieren.
5. Aktivieren Sie auf der Registerkarte **URL-Listenrichtlinie** das Kontrollkästchen **URL-Satz importieren** und geben Sie die folgenden URL-Set-Parameter an.
   a) URL-Set-Name — Name des benutzerdefinierten URL-Sets.
   b) URL: Die Webadresse des Standorts, an dem auf den URL-Satz zugegriffen werden soll.
   c) Überschreiben — Überschreibt einen zuvor importierten URL-Satz.
   d) Trennzeichen: Eine Zeichenfolge, die einen CSV-Dateidatensatz begrenzt.
   e) Zeilentrenner — In der CSV-Datei verwendetes Zeilentrenner.
   f) Intervall — Intervall in Sekunden, abgerundet auf die nächste Anzahl von Sekunden, die 15 Minuten entspricht, in der der URL-Satz aktualisiert wird.
   g) Private Set: Option, um das Exportieren des URL-Sets zu verhindern.
   h) Canary URL — Interne URL, mit der getestet wird, ob der Inhalt des URL-Sets vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen.
6. Wählen Sie eine Responder Action aus der Dropdownliste aus.
7. Klicken Sie auf **Erstellen** und **Schließen**.

Einen privaten URL-Satz konfigurieren

Wenn Sie einen privaten URL-Satz konfigurieren und den Inhalt vertraulich behandeln, kennt der Netzwerkadministrator möglicherweise die in der Sperrliste enthaltenen URLs nicht. In solchen Fällen kannst du eine Canary-URL konfigurieren und sie dem URL-Set hinzufügen. Mithilfe der Canary-URL kann der Administrator das private URL-Set anfordern, das für jede Suchanfrage verwendet werden soll. Eine Beschreibung der einzelnen Parameter finden Sie im Abschnitt Wizard.

Um einen URL-Satz mit der CLI zu importieren:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
    rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
    ] [-canaryUrl <URL>]
```



```
2 <!--NeedCopy-->
```

Beispiel:

```
1 import policy urlset test1 -url http://10.78.79.80/alytra/top-1k.csv -
     private -canaryUrl http://www.in.gr
2 <!--NeedCopy-->
```

Importierten URL-Satz anzeigen

Sie können jetzt zusätzlich zu hinzugefügten URL-Sets importierte URL-Sets anzeigen. Ein neuer Parameter “imported” wird dem Befehl `show urlset` hinzugefügt. Wenn Sie diese Option aktivieren, zeigt die Appliance alle importierten URL-Sets an und unterscheidet die importierten URL-Sets von den hinzugefügten URL-Sätzen.

Geben Sie an der Eingabeaufforderung Folgendes ein:
`show policy urlset [<name>] [-imported]`

Beispiel
`show policy urlset -imported`

Konfigurieren des Überwachungsprotokolls

Mithilfe der Prüfprotokollierung können Sie eine Bedingung oder Situation in jeder Phase eines URL-Listenprozesses überprüfen. Wenn eine NetScaler-Appliance eine eingehende URL empfängt und die Responder-Richtlinie einen erweiterten Richtlinienausdruck für URL-Sets enthält, sammelt die Audit-Log-Funktion URL-Set-Informationen in der URL. Es speichert die Details als Protokollnachricht für jedes Ziel, das durch die Audit-Protokollierung zulässig ist.

Die Lognachricht enthält die folgenden Informationen:

1. Zeitstempel.
2. Nachrichtentyp protokollieren.
3. Die vordefinierten Protokollebenen (Kritisch, Fehler, Hinweis, Warnung, Information, Debug, Warnung und Notfall).
4. Loggen Sie Nachrichteninformationen ein, z. B. Name des URL-Sets, Richtlinienaktion, URL.

Um die Überwachungsprotokollierung für die URL-Liste zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Überwachungsprotokollmeldung erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

URL-Muster-Semantik

August 15, 2023

Die folgende Tabelle zeigt die URL-Muster, die zum Angeben der Liste der Seiten verwendet werden sollen, die gefiltert werden sollen. Zum Beispiel `www.example.com/bar` entspricht das Muster nur einer Seite bei `www.example.com/bar`. Um alle Seiten abzugleichen, deren URL mit `www.example.com/bar` beginnt, fügen Sie am Ende der URL ein Sternchen (*) hinzu.

Semantik für URL-Muster zur Übereinstimmung mit der Metadatenzuordnung

Die Musterübereinstimmende Semantik ist in einem Tabellenformat verfügbar. Weitere Informationen finden Sie auf der PDF-Seite Pattern Semantik .

URL-Kategorien zuordnen

August 15, 2023

> **Hinweis:**
>
> Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

Eine Liste von Drittanbieterkategorien und Kategoriegruppen. Weitere Informationen finden Sie auf der Seite URL-Kategorie-Zuordnung .

Anwendungsfall: URL-Filterung mithilfe eines benutzerdefinierten URL-Sets

August 15, 2023

Wenn Sie ein Unternehmenskunde sind, der den Zugriff auf bestimmte Websites und Website-Kategorien steuern möchte, verwenden Sie einen benutzerdefinierten URL-Satz, der an eine Responder-Richtlinie gebunden ist. Die Netzwerkinfrastruktur Ihres Unternehmens kann einen URL-Filter verwenden, um den Zugriff auf schädliche oder gefährliche Websites zu blockieren. Zum Beispiel Websites mit Erwachsenen-, Gewalt-, Spiel-, Drogen-, Politik- oder Jobportalen. Sie können nicht nur die URLs filtern, sondern auch eine benutzerdefinierte Liste von URLs erstellen und in die ADC-Appliance importieren. Die Richtlinien Ihres Unternehmens könnten beispielsweise die Sperrung des Zugriffs auf bestimmte Websites wie soziale Netzwerke, Einkaufsportale und Jobportale vorsehen.

Jede URL in der Liste kann eine benutzerdefinierte Kategorie in Form von Metadaten haben. Die Organisation kann die Liste der URLs als URL hosten, die auf der NetScaler Appliance festgelegt ist. Konfigurieren Sie das Gerät so, dass das Gerät regelmäßig aktualisiert wird, ohne dass ein manueller Eingriff

Nachdem das Set aktualisiert wurde, erkennt die NetScaler Appliance die Metadaten automatisch. Die Responder-Richtlinie verwendet die URL-Metadaten (Kategoriedetails), um die eingehende URL auszuwerten und eine Aktion wie Zulassen, Blockieren, Umleiten oder Benachrichtigen des Benutzers anzuwenden.

Konfigurieren Sie dazu in Ihrem Netzwerk die folgenden Aufgaben:

1. Importieren eines benutzerdefinierten URL-Sets
2. Fügen Sie einen benutzerdefinierten URL-Satz hinzu
3. Konfigurieren Sie eine benutzerdefinierte URL-Liste im SSL-Forward-Proxy-Assistenten.

Importieren einer benutzerdefinierten URL, die über die CLI festgelegt wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
   rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
   ] [-canaryUrl <URL>]

import policy urlset test1  -url http://10.78.79.80/alytra/top-1k.csv
<!--NeedCopy-->
```

Fügen Sie eine benutzerdefinierte URL hinzu, die über die CLI festgelegt wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add urlset <urlset_name>
```

Beispiel:

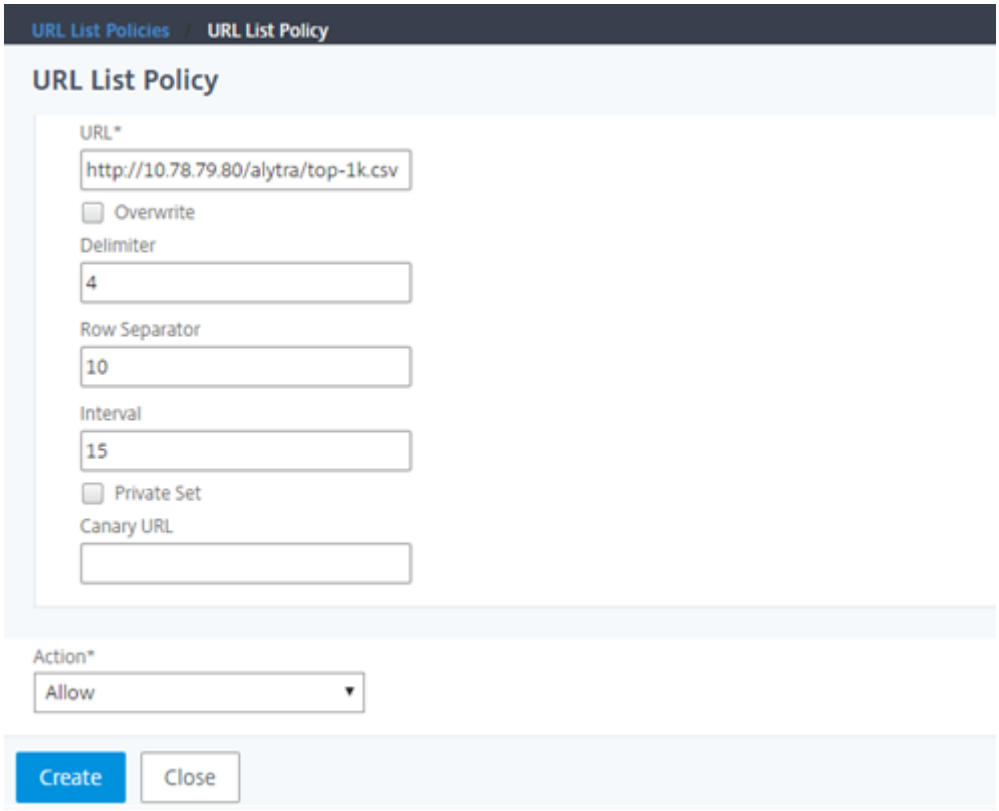
```
add urlset test1
```

Konfigurieren einer URL-Liste mithilfe des SSL-Forward-Proxy-Assistenten

Citrix empfiehlt, den SSL-Forward-Proxy-Assistenten als bevorzugte Option zum Konfigurieren einer URL-Liste zu verwenden. Verwenden Sie den Assistenten, um einen benutzerdefinierten URL-Satz zu importieren und ihn an eine Responder-Richtlinie zu binden.

1. Navigieren Sie zu **Sicherheit > SSL-Weiterleitungsproxy > URL-Filter > URL-Listen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.

3. Geben Sie auf der Seite “ **Richtlinie für URL-Liste** “ den Richtliniennamen an.
4. Wählen Sie eine Option aus, um entweder einen URL-Satz zu importieren.
5. Aktivieren Sie auf der Registerkarte “ **URL-Listenrichtlinie** “ das Kontrollkästchen **URL-Satz importieren** und geben Sie die folgenden URL-Set-Parameter an.
   a) URL-Set-Name — Name des benutzerdefinierten URL-Sets.
   b) URL: Die Webadresse des Standorts, an dem auf den URL-Satz zugegriffen werden soll.
   c) Überschreiben — Überschreibt einen zuvor importierten URL-Satz.
   d) Trennzeichen: Eine Zeichenfolge, die einen CSV-Dateidatensatz begrenzt.
   e) Zeilentrenner — In der CSV-Datei verwendetes Zeilentrenner.
   f) Intervall— Intervall in Sekunden, abgerundet auf die nächsten 15 Minuten, in dem der URL-Satz aktualisiert wird.
   g) Private Set: Option, um das Exportieren des URL-Sets zu verhindern.
   h) Canary URL— Interne URL zum Testen, ob der Inhalt des URL-Sets vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen.
6. Wählen Sie eine Responder Action aus der Dropdownliste aus.
7. Klicken Sie auf **Erstellen** und **Schließen**.



Metadaten-Semantik für benutzerdefinierte URL-Sets

Um einen benutzerdefinierten URL-Satz zu importieren, fügen Sie die URLs zu einer Textdatei hinzu und binden Sie sie an eine Responder-Richtlinie, um URLs für soziale Netzwerke zu blockieren.

Im Folgenden finden Sie Beispiele für URLs, die Sie der Textdatei hinzufügen könnten:

cnn.com, Nachrichten

bbc.com, Nachrichten

google.com, Suchmaschine

yahoo.com, Suchmaschine

facebook.com, Soziale Netzwerke

twitter.com, Soziale Netzwerke

Konfigurieren einer Responder-Richtlinie zum Blockieren von Social-Media-URLs mit der CLI

```
add responder action act_url_unauthorized respondwith '"HTTP/1.1 451
    Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\n"'

add responder policy pol_url_meta_match 'HTTP.REQ.HOSTNAME.APPEND(HTTP.
    REQ.URL).GET_URLSET_METADATA("u1").EQ("Social Media")'
    act_url_unauthorized
<!--NeedCopy-->
```

URL-Kategorisierung

August 15, 2023

> **Hinweis:**
>
> Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

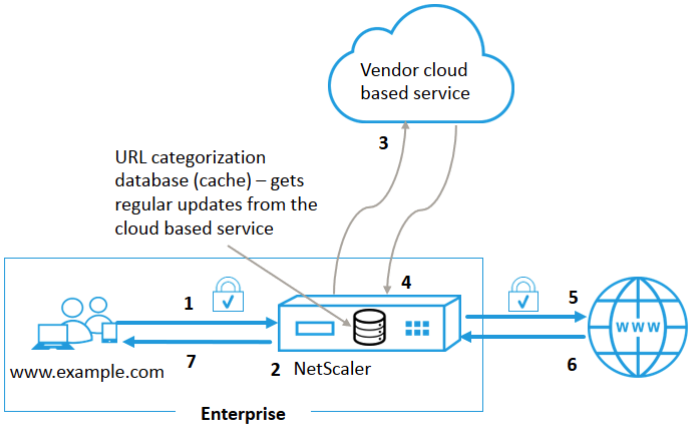
Die URL-Kategorisierung beschränkt den Benutzerzugriff auf bestimmte Websites und Website-Kategorien. Als abonnierter Dienst in Zusammenarbeit mit ermöglicht die Funktion Unternehmen-skunden `NetSTAR`, den Webverkehr mithilfe einer kommerziellen Kategorisierungsdatenbank zu filtern. Die `NetSTAR`-Datenbank enthält eine große Anzahl (Milliarden) von URLs, die in verschiedene Kategorien eingeteilt sind, z. B. soziale Netzwerke, Glücksspiele, Inhalte für Erwachsene, neue Medien und Shopping. Zusätzlich zur Kategorisierung hat jede URL eine Reputationsbewertung, die basierend auf dem historischen Risikoprofil der Website auf dem neuesten Stand gehalten wird. Wir können `NetSTAR`-Daten verwenden, um den Datenverkehr zu filtern, indem wir erweiterte Richtlinien basierend auf Kategorien, Kategoriegruppen (wie Terrorismus, illegale Drogen) oder Reputationsbewertungen für Websites konfigurieren.

Sie könnten beispielsweise den Zugriff auf gefährliche Websites blockieren, z. B. Websites, von denen bekannt ist, dass sie mit Malware infiziert sind. Sie können auch selektiv den Zugriff auf Inhalte wie Inhalte für Erwachsene oder Unterhaltungsstreaming-Medien für Unternehmensbenutzer einschränken. Sie können auch die Transaktionsdetails des Benutzers und die Details des ausgehenden Datenverkehrs erfassen, um die Analyse des Webverkehrs auf dem NetScaler ADM-Server zu überwachen.

NetScaler lädt Daten vom vorkonfigurierten `NetSTAR` Gerät hoch oder lädt sie herunter `nsv10.netstar-inc.com` und `incompasshybridpc.netstar-inc.com` wird standardmäßig als Cloud-Host für Cloud-Kategorisierungsanfragen verwendet. Diese URLs müssen über die Firewall zugänglich sein, damit die URL-Filterung ordnungsgemäß funktioniert. Die Appliance verwendet ihre NSIP-Adresse als Quell-IP-Adresse und 443 als Zielport für die Kommunikation.

Funktionsweise der URL-Kategorisierung

Die folgende Abbildung zeigt, wie ein NetScaler URL-Kategorisierungsdienst in eine kommerzielle URL-Kategorisierungsdatenbank und Cloud-Dienste für häufige Updates integriert ist.



Die Komponenten interagieren wie folgt:

1. Ein Client sendet eine internetgebundene URL-Anfrage.
2. Der SSL-Forward-Proxy wendet eine Richtliniendurchsetzung auf die Anforderung an, die auf den Kategoriedetails wie Kategorie, Kategoriegruppe und Site-Reputationsbewertung basiert. Die Kategoriedetails werden aus der Datenbank zur URL-Kategorisierung abgerufen. Wenn die Datenbank die Kategoriedetails zurückgibt, springt der Prozess zu Schritt 5.
3. Wenn in der Datenbank die Kategorisierungsdetails fehlen, wird die Anforderung an einen Cloud-basierten Suchdienst gesendet, der von einem Anbieter der URL-Kategorisierung verwaltet wird. Die Appliance wartet jedoch nicht auf eine Antwort, stattdessen wird die URL als nicht kategorisiert gekennzeichnet und eine Richtliniendurchsetzung wird durchgeführt (weiter zu

Schritt 5). Die Appliance überwacht weiterhin das Feedback der Cloud-Abfrage und aktualisiert den Cache, sodass zukünftige Anfragen vom Cloud-Lookup profitieren können.

4. Die ADC-Appliance erhält die URL-Kategoriedetails (Kategorie, Kategoriegruppe und Reputationsbewertung) vom Cloud-basierten Dienst und speichert sie in der Kategorisierungsdatenbank.
5. Die Richtlinie erlaubt die URL und die Anfrage wird an den Original-Server gesendet. Andernfalls verwirft die Appliance, leitet sie um oder antwortet mit einer benutzerdefinierten HTML-Seite.
6. Der Original-Server antwortet mit den angeforderten Daten an die ADC-Appliance.
7. Die Appliance sendet die Antwort an den Client.

Anwendungsfall: Internetnutzung unter Einhaltung von Unternehmensrichtlinien für Unternehmen

Sie können die URL-Filter-Funktion verwenden, um Compliance-Richtlinien zu erkennen und zu implementieren, um Websites zu blockieren, die gegen die Unternehmenskonformität verstoßen. Zum Beispiel Websites wie Erwachsene, Streaming-Medien und soziale Netzwerke, die als nicht produktiv angesehen werden können oder in einem Unternehmensnetzwerk überschüssige Internetbandbreite verbrauchen. Die Sperrung des Zugriffs auf diese Websites kann die Produktivität der Mitarbeiter verbessern, die Betriebskosten für die Bandbreitennutzung senken und den Gemeinkosten des Netzwerkverbrauchs reduzieren.

Voraussetzungen

Die Funktion zur URL-Kategorisierung funktioniert auf einer NetScaler-Plattform nur, wenn sie über einen optionalen Abonnementdienst mit URL-Filterfunktionen und Bedrohungsinformationen für SSL-Forward-Proxy verfügt Mit dem Abonnement können Kunden die neuesten Bedrohungskategorisierungen für Websites herunterladen und diese Kategorien dann für den SSL-Forward-Proxy durchsetzen. Bevor Sie die Funktion aktivieren und konfigurieren, müssen Sie die folgenden Lizenzen installieren:

- `CNS_WEBF_SSERVER_Retail.lic`
- `CNS_XXXX_SERVER_PLT_Retail.lic`

Wobei XXXXX der Plattformtyp ist, zum Beispiel: V25000

Richtlinienausdrücke für Resp

In der folgenden Tabelle sind die verschiedenen Richtlinienausdrücke aufgeführt, mit denen Sie überprüfen können, ob eine eingehende URL zulässig, umgeleitet oder gesperrt sein muss.

1. <text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>) - Gibt ein URL_CATEGORY-Objekt zurück. Wenn <min_reputation> größer als 0 ist, enthält das zurückgegebene Objekt keine Kategorie mit einer niedrigeren Reputation als <min_reputation>. Wenn <max_reputation> größer als 0 ist, enthält das zurückgegebene Objekt keine Kategorie mit einer höheren Reputation als <max_reputation>. Wenn die Kategorie nicht rechtzeitig aufgelöst wird, wird der undef-Wert zurückgegeben.
2. <url_category>. CATEGORY() - Gibt die Kategorie für dieses Objekt zurück. Wenn die URL keine Kategorie hat oder wenn die URL fehlerhaft ist, ist der zurückgegebene Wert "Unbekannt".
3. <url_category>. CATEGORY_GROUP() - Gibt eine Zeichenfolge zurück, die die Kategoriegruppe des Objekts identifiziert. Bei dieser Gruppierung handelt es sich um eine übergeordnete Gruppierung von Kategorien, die bei Vorgängen nützlich ist, die weniger detaillierte Informationen über die URL-Kategorie benötigen. Wenn die URL keine Kategorie hat oder wenn die URL fehlerhaft ist, ist der zurückgegebene Wert "Unbekannt".
4. <url_category>. REPUTATION() - Gibt den Reputationswert als Zahl von 0 bis 5 zurück, wobei 5 den riskantesten Ruf angibt. Wenn es die Kategorie "Unbekannt" gibt, ist der Reputationswert 1.

Policy-Typen:

1. Richtlinie zum Auswählen von Anfragen für URLs, die in der Suchmaschinenkategorie enthalten sind - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ( "Search Engine" )`
2. Richtlinie zur Auswahl von Anfragen für URLs, die in der Kategorie "Erwachsene" enthalten sind - `add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY_GROUP().EQ( "Adult" )'`
3. Richtlinie zur Auswahl von Anfragen für Suchmaschinen-URLs mit einem Reputationswert von weniger als 4 — `add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY( "Search Engine" )`
4. Richtlinie zur Auswahl von Anfragen für Suchmaschinen und Einkaufs-URLs - `add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ( "good_categories" )`
5. Richtlinie zur Auswahl von Anfragen für Suchmaschinen-URLs mit einer Reputationsbewertung von mindestens 4 - `add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY().EQ( "Search Engines" )`
6. Richtlinie, um Anfragen für URLs auszuwählen, die sich in der Suchmaschinenkategorie befinden, und diese mit einem URL-Satz zu vergleichen - `'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ( "Search Engine" )&& HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY( "u1" )'`

Responder-Richtlinientypen

In einer Funktion zur URL-Kategorisierung werden zwei Arten von Richtlinien verwendet, und jeder dieser Richtlinientypen wird in der folgenden Tabelle erläutert:

Richtlinientyp	Beschreibung
URL-Kategorie	Kategorisieren Sie den Webverkehr und blockieren, erlauben oder leiten Sie den Datenverkehr basierend auf den Bewertungsergebnissen
URL-Reputationsbewertung	Bestimmt den Reputationswert der Website und ermöglicht Ihnen, den Zugriff basierend auf dem vom Administrator festgelegten Schwellenwert für die Reputationsbewertung zu steuern.

Konfigurieren der URL Kategorisierung

Gehen Sie wie folgt vor, um die URL-Kategorisierung auf einer NetScaler-Appliance zu konfigurieren:

1. URL-Filterung aktivieren.
2. Konfigurieren Sie einen Proxyserver für den Webverkehr.
3. Konfigurieren Sie das SSL-Abfangen für den Webverkehr im expliziten Modus.
4. Konfigurieren Sie gemeinsamen Speicher, um den Cache-Speicher zu begrenzen
5. Konfigurieren der URL-Kategorisierungsparameter
6. Konfigurieren der URL-Kategorisierung mithilfe des Citrix SSL-Forward-Proxy-Assistenten.
7. Konfigurieren Sie die URL-Kategorisierungsparameter mithilfe des SSL-Weiterleitungsproxy-Assistenten
8. Konfigurieren des Seeddatenbankpfads und des Cloud-Servernamens

Schritt 1: URL-Filterung aktivieren

Um die URL-Kategorisierung zu aktivieren, aktivieren Sie die URL-Filterfunktion und Modi für die URL-Kategorisierung.

So aktivieren Sie die URL-Kategorisierung mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature URLFiltering

disable ns feature URLFiltering
```


Schritt 2: Konfigurieren eines Proxyservers für den Webverkehr im expliziten Modus

Die NetScaler-Appliance unterstützt transparente und explizite virtuelle Proxyserver. Gehen Sie wie folgt vor, um einen virtuellen Proxyserver für SSL-Datenverkehr im expliziten Modus zu konfigurieren:

1. Fügen Sie einen Proxyserver hinzu.
2. Binden einer SSL-Richtlinie an den Proxyserver.

So fügen Sie einen Proxyserver mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> [-td <positive_integer>] <serviceType> [-cltTimeout <
secs>]
```

Beispiel:

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
```

Binden einer SSL-Richtlinie mithilfe der CLI an einen virtuellen Proxyserver

```
bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer
>]
```

Schritt 3: SSL-Abfangen für den HTTPS-Verkehr konfigurieren

Gehen Sie wie folgt vor, um das SSL-Abfangen für den HTTPS-Verkehr zu konfigurieren:

1. Binden Sie ein CA-Zertifikatsschlüsselpaar an den virtuellen Proxyserver.
2. Konfigurieren Sie das standardmäßige SSL-Profil mit SSL-Parametern.
3. Binden Sie ein Front-End-SSL-Profil an den virtuellen Proxyserver und aktivieren Sie das SSL-Abfangen im Front-End-SSL-Profil.

So binden Sie ein CA-Zertifikatsschlüsselpaar mithilfe der CLI an den virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -CA -
skipCAName
```

So konfigurieren Sie das Standard-SSL-Profil mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
ENABLED | DISABLED)-ssliMaxSessPerServer positive_integer>
```


Binden Sie ein Front-End-SSL-Profil mithilfe der CLI an einen virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServer name> -sslProfile ssl_profile_interception
```

Schritt 4: Konfigurieren Sie Shared Memory, um den Cache-Speicher

So konfigurieren Sie Shared Memory zur Begrenzung des Cache-Speichers mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache parameter [-memLimit <megaBytes>]
```

Wobei das für das Caching konfigurierte Speicherlimit auf 10 MB festgelegt ist.

Schritt 5: Konfigurieren der URL-Kategorisierungsparameter

So konfigurieren Sie die URL-Kategorisierungsparameter mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>]
```

Beispiel:

```
set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20
```

Schritt 6: Konfigurieren der URL-Kategorisierung mithilfe des Citrix SSL-Forward-Proxy-Assistenten

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zur Seite **Sicherheit** > **SSL Forward Proxy** .
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   a) Klicken Sie auf **SSL Forward Proxy Wizard**, um eine neue Konfiguration
   b) Wählen Sie eine vorhandene Konfiguration aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt “ **URL-Filter** “ auf **Bearbeiten**.
4. Wählen Sie das Kontrollkästchen **URL-Kategorisierung**, um die Funktion zu aktivieren
5. Wählen Sie eine **URL-Kategorisierungsrichtlinie** aus und **klicken**Sie auf
6. Klicken Sie auf **Weiter** und dann **Fertig**.

Weitere Informationen zur URL-Kategorisierungsrichtlinie finden Sie unter Erstellen einer URL-Kategorisierungsrichtlinie.

Schritt 7: Konfigurieren von URL-Kategorisierungsparametern mit einem SSL-Forward-Proxy-Assistenten

1. Melden Sie sich bei der **NetScaler-Appliance** an und navigieren Sie zu **Sicherheit > URL-Filter**.
2. Klicken Sie auf der Seite " **URL-Filter** " auf den Link **URL-Filtereinstellungen ändern** .
3. Geben **Sie auf der Seite Konfigurieren von URL-Filterparametern** die folgenden Parameter an.
   a) Stunden zwischen DB-Aktualisierungen. Stunden des URL-Filters zwischen Datenbankaktualisierungen Minimalwert: 0 und Maximalwert: 720.
   b) Tageszeit zur Aktualisierung der DB. Uhrzeit des URL-Filters zum Aktualisieren der Datenbank.
   c) Cloud-Host. Der URL-Pfad des Cloud-Servers.
   d) Seed-DB-Pfad. Der URL-Pfad des Seed-Datenbank-Suchservers.
4. Klicken Sie auf **OK** und **schließen**.

Beispielkonfiguration:

```
enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering

enable ns mode FR L3 Edge USNIP PMTUD

set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
    -sslInterception ENABLED -ssliMaxSessPerServer 100

add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key

set cache parameter -memLimit 100

add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180

add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
    .req.url.url_categorize(0,0).reputation + "\n""

add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
    Search Engines & Portals

")" act1

bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
    gotoPriorityExpression END -type REQUEST

add dns nameServer 10.140.50.5

```



```
set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
    sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
    SHA512 -ssliErrorCache ENABLED

-ssliMaxErrorCacheMem 100000000

add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
    URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")"" -
    action INTERCEPT

add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
    citrix")" -action INTERCEPT

add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
    URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT

set urlfiltering parameter -HoursBetweenDBUpdates 3 -
    TimeOfDayToUpdateDB 03:00
<!--NeedCopy-->
```

Konfigurieren des Seeddatenbankpfads und des Cloud-Servernamens

Sie können jetzt den Seed-Datenbankpfad und den Namen des Cloud-Lookup-Servers für die manuelle Einstellung des Cloud-Lookup-Servernamens und des Seed-Datenbankpfads konfigurieren. Zu diesem Zweck werden zwei neue Parameter, “CloudHost” und “SeedDBPath”, zum URL-Filterparameter hinzugefügt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer>] [-
CloudHost <string>] [-SeedDBPath <string>]
```

Beispiel:

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00 -CloudHost localhost -SeedDBPath /mypath
```

Die Kommunikation zwischen einer NetScaler Appliance und erfordert `NetSTAR` möglicherweise einen Domänennamenserver. Sie können mit einer einfachen Konsolen- oder Telnet-Verbindung von der Appliance aus testen.

Beispiel:

```
root@ns# telnet nsv10.netstar-inc.com 443
Trying 1.1.1.1...
```



```
Connected to nsv10.netstar-inc.com.
Escape character is '^]'.

root@ns# telnet incompasshybridpc.netstar-inc.com 443
Trying 10.10.10.10...
Connected to incompasshybridpc.netstar-inc.com.
Escape character is '^]'.
<!--NeedCopy-->
```

Konfigurieren des Überwachungsprotokolls

Mit der Überwachungsprotokollierung können Sie einen Zustand oder eine Situation in jeder Phase des URL-Kategorisierungsprozesses überprüfen. Wenn eine NetScaler-Appliance eine eingehende URL empfängt und die Responder Policy über einen URL-Filterausdruck verfügt, sammelt die Überwachungsprotokollfunktion URL-Set-Informationen in der URL. Es speichert die Informationen als Protokollmeldungen für jedes Ziel, das von der Überwachungsprotokollierung zugelassen ist.

- Quell-IP-Adresse (die IP-Adresse des Clients, der die Anfrage gestellt hat).
- Ziel-IP-Adresse (die IP-Adresse des angeforderten Servers).
- Angeforderte URL mit dem Schema, dem Host und dem Domainnamen (http://www.example.com).
- URL-Kategorie, die das URL-Filterframework zurückgibt.
- URL-Kategoriegruppe, die vom URL-Filterframework zurückgegeben wurde
- Die vom URL-Filter-Framework zurückgegebene URL-Reputationsnummer
- Von der Richtlinie durchgeführte Auditprotokollaktion.

Um die Überwachungsprotokollierung für eine Funktion der URL-Liste zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Überwachungsprotokollmeldung erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

Speichern von Fehler mit SYSLOG-Messaging

In jeder Phase des URL-Filtervorgangs verwendet die ADC-Appliance bei einem Fehler auf Systemebene den Überwachungsprotokollmechanismus, um Protokolle in der Datei ns.log zu speichern. Die Fehler werden als Textnachrichten im SYSLOG-Format gespeichert, sodass ein Administrator sie später in einer chronologischen Reihenfolge des Ereignisses anzeigen kann. Diese Protokolle werden

auch zur Archivierung an einen externen SYSLOG-Server gesendet. Weitere Informationen finden Sie im Artikel CTX229399.

Wenn beispielsweise ein Fehler auftritt, wenn Sie das URL-Filter-SDK initialisieren, wird die Fehlermeldung im folgenden Nachrichtenformat gespeichert.

```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing
NetStar SDK (SDK error=-1). (status=1).
```

Die NetScaler-Appliance speichert die Fehlermeldungen in vier verschiedenen Fehlerkategorien:

- **Fehler beim Herunterladen**. Wenn beim Versuch, die Kategorisierungsdatenbank herunterzuladen, ein Fehler auftritt.
- **Scheitern der Integration**. Wenn ein Fehler auftritt, wenn Sie ein Update in die vorhandene Kategorisierungsdatenbank integrieren.
- **Fehler bei der Initialisierung**. Wenn bei der Initialisierung der Funktion zur URL-Kategorisierung ein Fehler auftritt, legen Sie Kategorisierungsparameter fest oder beenden Sie einen Kategorisierungsdienst.
- **Fehler beim Abrufen**. Wenn ein Fehler auftritt, wenn die Appliance die Kategorisierungsdetails der Anforderung abruft.

Konfigurieren von SNMP-Traps für NetStar-Ereignisse

Die Funktion “URL-Filter” generiert SNMP-Traps, wenn die folgenden Bedingungen eintreten:

- NetStar-Datenbank-Update schlägt fehl oder ist erfolgreich.
- Die NetStar SDK-Initialisierung schlägt fehl oder ist erfolgreich.

Die Appliance verfügt über eine Reihe von bedingten Einheiten, die als SNMP-Alarme bezeichnet werden Wenn eine Bedingung im SNMP-Alarm erfüllt ist, generiert die Appliance Traps und sendet sie an ein bestimmtes Trap-Ziel. Wenn beispielsweise die NetStar SDK-Initialisierung fehlschlägt, wird eine SNMP-OID 1.3.6.1.4.1.5951.1.1.0.183 generiert und an das Trap-Ziel gesendet.

Damit die Appliance Traps generiert, müssen Sie zunächst SNMP-Alarme aktivieren und konfigurieren. Anschließend geben Sie das Trap-Ziel an, an das die Appliance die generierten Trap-Nachrichten sendet.

Aktivieren eines SNMP-Alarms

Die NetScaler-Appliance generiert Traps nur für aktivierte SNMP-Alarme. Einige Alarme sind standardmäßig aktiviert, aber Sie können sie deaktivieren.

Wenn Sie einen SNMP-Alarm aktivieren, generiert die URL-Filterfunktion Trap-Meldungen, wenn ein Erfolgs- oder Miserfolgsereignis eintritt. Einige Alarme sind standardmäßig aktiviert.

So aktivieren Sie einen SNMP-Alarm mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
enable snmp alarm <trapName>
show snmp alarm <trapName>
```

So aktivieren Sie einen SNMP-Alarm mithilfe der NetScaler GUI

1. Navigieren Sie zu **System** > **SNMP** > **Alarme**und wählen Sie den Alarm aus.
2. Klicken Sie auf **Aktionen** und wählen Sie **Aktivieren**

Konfigurieren des SNMP-Alarms mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue
 <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Beispiel:

```
set snmp alarm URL-FIL-DB-UPDATE-STATUS -state ENABLED
set snmp alarm URL-FIL-INIT-SDK -state ENABLED
```

Konfigurieren von SNMP-Alarmen mit der GUI

Navigieren Sie zu **System** > **SNMP** > **Alarms**, wählen Sie einen Alarm aus und konfigurieren Sie die Alarmparameter.

Weitere Informationen zu SNMP-Traps finden Sie unter SNMP

URL-Reputationsbewertung

August 15, 2023

> **Hinweis:**
>
> Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

Die Funktion zur URL-Kategorisierung bietet eine richtlinienbasierte Steuerung zur Einschränkung von URLs auf der Sperrliste. Sie können den Zugriff auf Websites basierend auf der URL-Kategorie, dem Reputationswert oder der URL-Kategorie und dem Reputationswert steuern. Wenn Netzwerkadministratoren einen Benutzer überwachen, der auf hochriskante Websites zugreift, können sie eine Responder Policy verwenden, die an den URL-Reputationswert gebunden ist, um solche riskanten Websites zu blockieren.

Nach Erhalt einer eingehenden URL-Anforderung ruft die Appliance die Kategorie und den Reputationswert aus der URL-Kategorisierungsdatenbank ab. Basierend auf dem von der Datenbank zurückgegebenen Reputationswert weist die Appliance Websites eine Reputationsbewertung zu. Der Wert kann zwischen 1 und 4 liegen, wobei 4 die riskanteste Art von Websites ist, wie in der folgenden Tabelle gezeigt.

URL Reputation Bewertung	Reputation Kommentar
1	Saubere Seite
2	Unbekannte Seite
3	Potenziell gefährlich oder mit einer gefährlichen Website verbunden
4	Schädliche Seite

Anwendungsfall: Filtern nach URL-Reputationswert

Stellen Sie sich eine Unternehmensorganisation mit einem Netzwerkadministrator vor, der Benutzertransaktionen und den Netzwerkbandbreitenverbrauch überwacht. Wenn Malware in das Netzwerk gelangen kann, muss der Administrator die Datensicherheit erhöhen und den Zugriff auf böswillige und gefährliche Websites kontrollieren, die auf das Netzwerk zugreifen. Um das Netzwerk vor solchen Bedrohungen zu schützen, kann der Administrator die URL-Filterfunktion so konfigurieren, dass der Zugriff nach URL-Reputationsbewertung zugelassen oder verweigert wird.

Weitere Informationen zur Überwachung des ausgehenden Datenverkehrs und der Benutzeraktivitäten im Netzwerk finden Sie unter Analytics.

Wenn ein Mitarbeiter der Organisation versucht, auf eine Social-Networking-Website zuzugreifen, erhält die ADC-Appliance eine URL-Anfrage. Es fragt die URL-Kategorisierungsdatenbank ab, um die URL-Kategorie als soziales Netzwerk und einen Reputationswert 3 abzurufen, was auf eine potenziell gefährliche Website hinweist. Die Appliance überprüft dann die vom Administrator konfigurierte Sicherheitsrichtlinie, z. B. den Blockzugriff auf Websites mit einer Reputationsbewertung von 3 oder mehr. Es wendet dann die politischen Maßnahmen an, um den Zugriff auf die Website zu kontrollieren.

Um diese Funktion zu implementieren, müssen Sie den URL-Reputationswert und die Sicherheitsschwellenwerte mithilfe des SSL-Forward-Proxy-Assistenten konfigurieren.

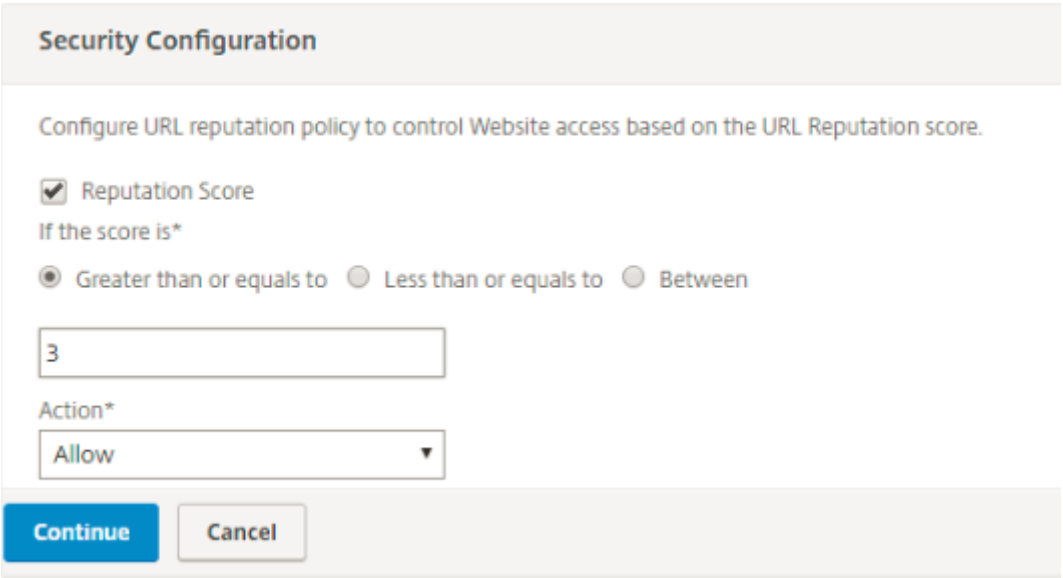
Konfigurieren Sie den Reputation-Score über die GUI

Citrix empfiehlt, den SSL-Forward-Proxy-Assistenten zu verwenden, um den Reputationswert und die Sicherheitsstufen zu konfigurieren. Basierend auf dem konfigurierten Schwellenwert können Sie eine

Richtlinienaktion auswählen, um Datenverkehr zuzulassen, zu blockieren oder umzuleiten.

1. Navigieren Sie zu **Sicherheit** > **SSL Forward Proxy**.
2. Klicken Sie im Detailbereich auf **SSL-Forward-Proxy-Assistent**.
3. Geben Sie auf der Detailseite die Proxy-Servereinstellungen an.
4. Klicken Sie auf **Weiter**, um andere Einstellungen wie SSL-Abfangen und Identifizierungsmanagement festzulegen.
5. Klicken Sie auf **Weiter**, um auf den Abschnitt **Sicherheitskonfiguration** zuzugreifen.
6. Aktivieren Sie im Abschnitt **Sicherheitskonfiguration** das Kontrollkästchen **Reputationswert**, um den Zugriff basierend auf dem URL-Reputationswert zu steuern.
7. Wählen Sie die Sicherheitsstufe und geben Sie den Schwellenwert für den Reputation-Score an:
   a) Größer oder gleich: Zulassen oder Blockieren einer Website, wenn der Schwellenwert größer oder gleich N ist, wobei N zwischen eins und vier reicht.
   b) Kleiner oder gleich— Erlauben oder blockieren Sie eine Website, wenn der Schwellenwert kleiner oder gleich N ist, wobei N von eins bis vier reicht.
   c) Dazwischen - Erlauben oder blockieren Sie eine Website, wenn der Schwellenwert zwischen N1 und N2 liegt und der Bereich zwischen eins und vier liegt.
8. Wählen Sie eine Responder Action aus der Dropdownliste aus.
9. Klicken Sie auf **Fortfahren** und **schließen**.

Die folgende Abbildung zeigt den Abschnitt **Sicherheitskonfiguration** des SSL-Forward-Proxy-Assistenten. Aktivieren Sie die Option URL Reputation Score, um die Richtlinieneinstellungen zu konfigurieren



Analytics

May 11, 2023

In der NetScaler-Appliance werden alle Benutzerdatensätze und nachfolgenden Datensätze protokolliert. Wenn Sie NetScaler Application Delivery Management (ADM) in die NetScaler-Appliance integrieren, werden die protokollierte Benutzeraktivität und die nachfolgenden Datensätze in der Appliance mithilfe der Funktion `logstream` nach NetScaler ADM exportiert.

NetScaler ADM stellt Informationen über die Aktivitäten der Nutzer zusammen, z. B. besuchte Websites und die verbrauchte Bandbreite. Es meldet auch die Bandbreitennutzung und erkannte Bedrohungen wie Malware und Phishing-Sites. Mit diesen Schlüsselmetriken können Sie Ihr Netzwerk überwachen und Korrekturmaßnahmen mit der Citrix SWG-Appliance durchführen. Weitere Informationen finden Sie unter Citrix SSL Forward Proxy Analytics.

So integrieren Sie die NetScaler-Appliance in NetScaler ADM:

1. Aktivieren Sie in der NetScaler-Appliance beim Konfigurieren der SSL-Forward-Proxy-Funktion Analytics und geben Sie die Details der NetScaler ADM-Instanz an, die Sie für Analysen verwenden möchten.
2. Fügen Sie in NetScaler ADM die NetScaler-Appliance als Instanz zu NetScaler ADM hinzu. Weitere Informationen finden Sie unter Instanzen zu NetScaler ADM hinzufügen.

Anwendungsfall: Sicherstellung der Sicherheit eines Unternehmensnetzwerks mithilfe von ICAP zur Malware-Inspektion per Fernzugriff

May 11, 2023

Die NetScaler-Appliance fungiert als Proxy und fängt den gesamten Client-Verkehr ab. Die Appliance verwendet Richtlinien, um den Datenverkehr auszuwerten, und leitet Clientanfragen an den Ursprungsserver weiter, auf dem sich die Ressource befindet. Die Appliance entschlüsselt die Antwort vom Ursprungsserver und leitet den Klartextinhalt zur Malware-Prüfung an den ICAP-Server weiter. Der ICAP-Server antwortet mit der Meldung „Keine Anpassung erforderlich“, einem Fehler oder einer geänderten Anfrage. Abhängig von der Antwort des ICAP-Servers wird der angeforderte Inhalt entweder an den Client weitergeleitet oder es wird eine entsprechende Nachricht gesendet.

Für diesen Anwendungsfall müssen Sie einige allgemeine Konfigurationen, Proxy- und SSL-Interception-Konfigurationen sowie eine ICAP-Konfiguration auf der NetScaler-Appliance durchführen.

Allgemeine Konfiguration

Konfigurieren Sie die folgenden Entitäten:

- NSIP-Adresse
- Subnetz-IP-Adresse (SNIP)
- DNS-Nameserver
- CA-Zertifikatsschlüsselpaar zum Signieren des Serverzertifikats für SSL-Abfangen

Konfiguration des Proxyservers und des SSL-Abhörens

Konfigurieren Sie die folgenden Entitäten:

- Proxy-Server im expliziten Modus, um den gesamten ausgehenden HTTP- und HTTPS-Verkehr abzufangen.
- SSL-Profil zur Definition von SSL-Einstellungen wie Chiffrieren und Parametern für Verbindungen.
- SSL-Richtlinie zur Definition von Regeln für das Abfangen von Datenverkehr. Auf true setzen, um alle Client-Anfragen abzufangen.

Weitere Informationen finden Sie in den folgenden Themen:

- Proxy-Modi
- SSL-Interception

In der folgenden Beispielkonfiguration befindet sich der Antimalware-Erkennungsdienst unter. `www.example.com`

Beispiel für eine allgemeine Konfiguration:

```
add dns nameServer 203.0.113.2

add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.key
<!--NeedCopy-->
```

Beispiel für eine Proxyserver- und SSL-Abfangkonfiguration:

```
add cs vserver explicitswg PROXY 192.0.2.100 80 -Authn401 ENABLED -authnVsName explicit-auth-vs

set ssl parameter -defaultProfile ENABLED

add ssl profile swg_profile -sslInterception ENABLED

bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey

```



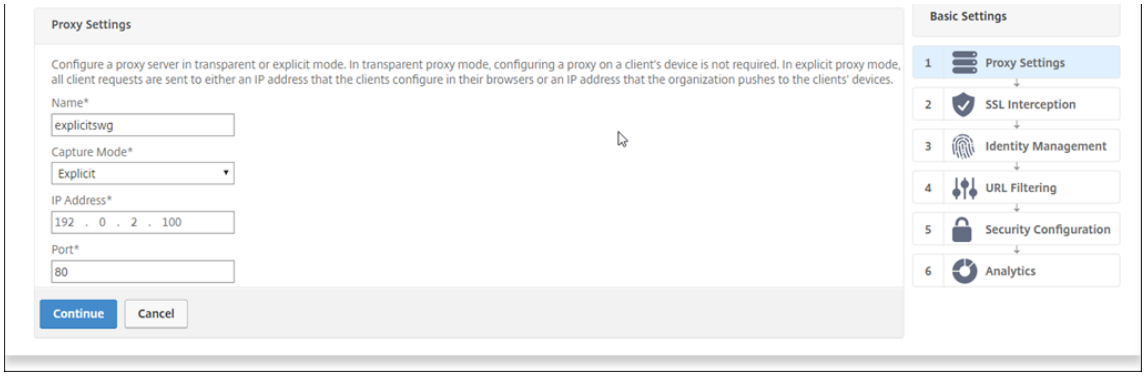
```
set ssl vserver explicitswg -sslProfile swg_profile

add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -type INTERCEPT_REQ
<!--NeedCopy-->
```

Beispiel für eine ICAP-Konfiguration:

```
add service icap_svc 203.0.113.225 TCP 1344

enable ns feature contentinspection

add icapprofile icapprofile1 -uri /example.com -Mode RESMOD

add contentInspection action CiRemoteAction -type ICAP -serverName icap_svc -icapProfileName icapprofile1

add contentInspection policy CiPolicy -rule "HTTP.REQ.METHOD.NE("CONNECT")" -action CiRemoteAction

bind cs vserver explicitswg -policyName  CiPolicy -priority 200 -type response
<!--NeedCopy-->
```

Konfigurieren Sie die Proxy-Einstellungen

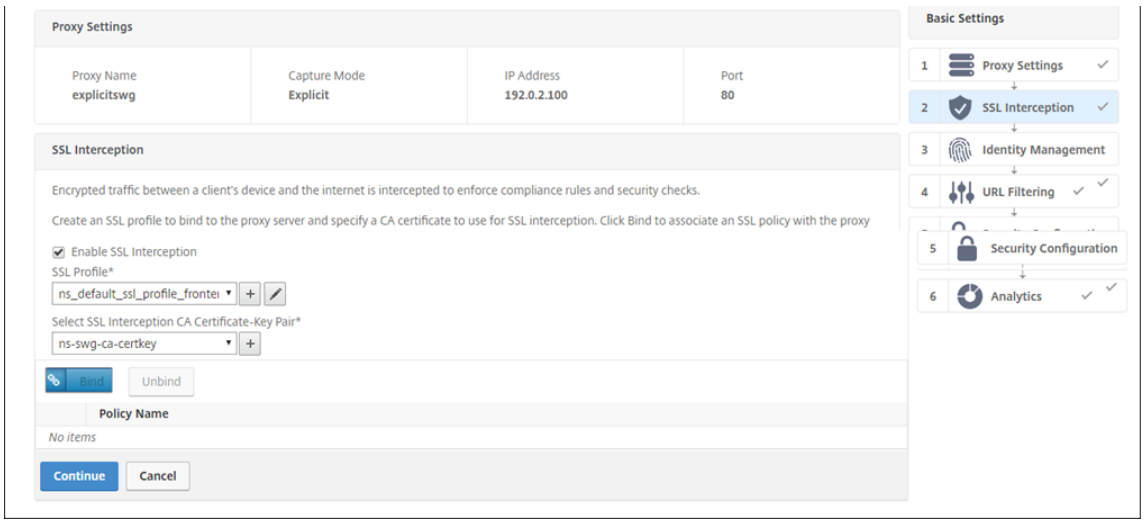
1. Navigieren Sie zu **Sicherheit** > **SSL Forward Proxy** > **SSL Forward Proxy Wizard**.
2. Klicken **Sie auf Erste Schritte** und dann auf **Weiter**.
3. Geben Sie im Dialogfeld **Proxy-Einstellungen** einen Namen für den expliziten Proxyserver ein.
4. Wählen Sie für **den Aufnahmemodus die** Option **Explizit**aus.
5. Geben Sie eine IP-Adresse und eine Portnummer ein.



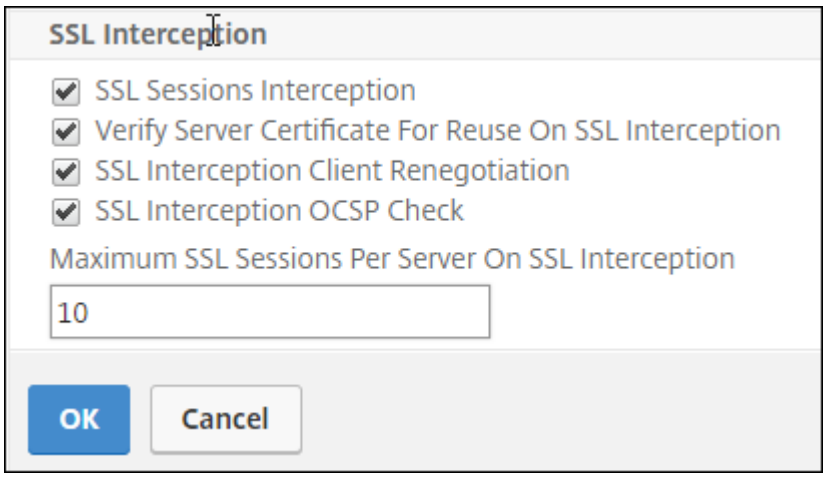
6. Klicken Sie auf **Weiter**.

Konfigurieren Sie die SSL-Abfangeinstellungen

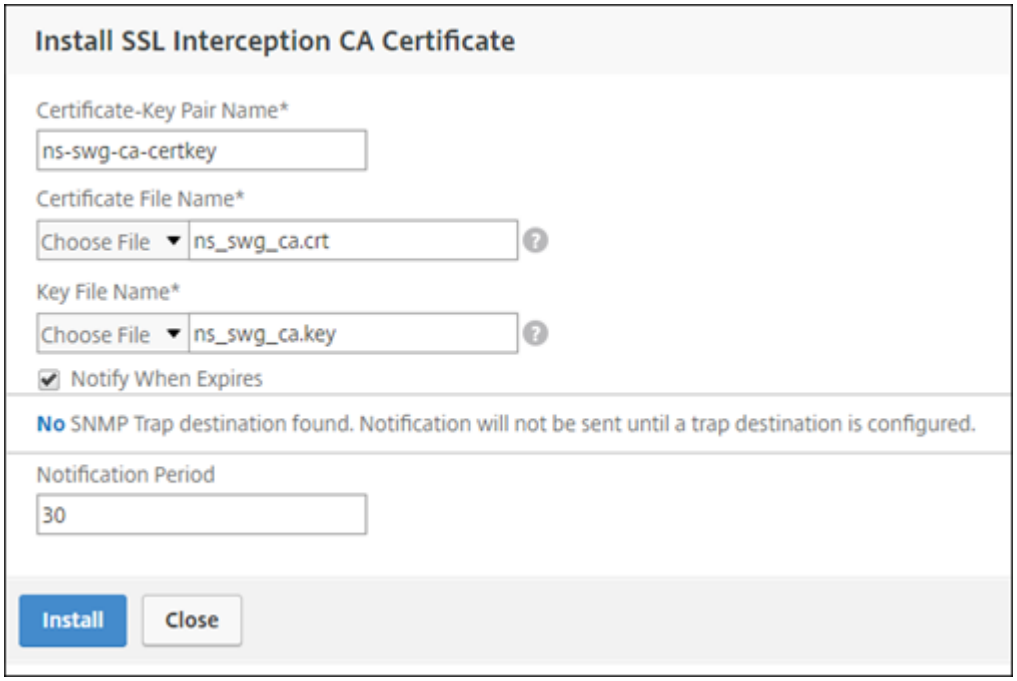
1. Wählen Sie **SSL-Abfangen aktivieren**aus.



2. Wählen Sie unter **SSL-Profil**ein vorhandenes Profil aus oder klicken Sie auf „+“, um ein neues Front-End-SSL-Profil hinzuzufügen. Aktivieren Sie das **Abfangen von SSL-Sitzungen** in diesem Profil. Wenn Sie ein vorhandenes Profil auswählen, überspringen Sie den nächsten Schritt.

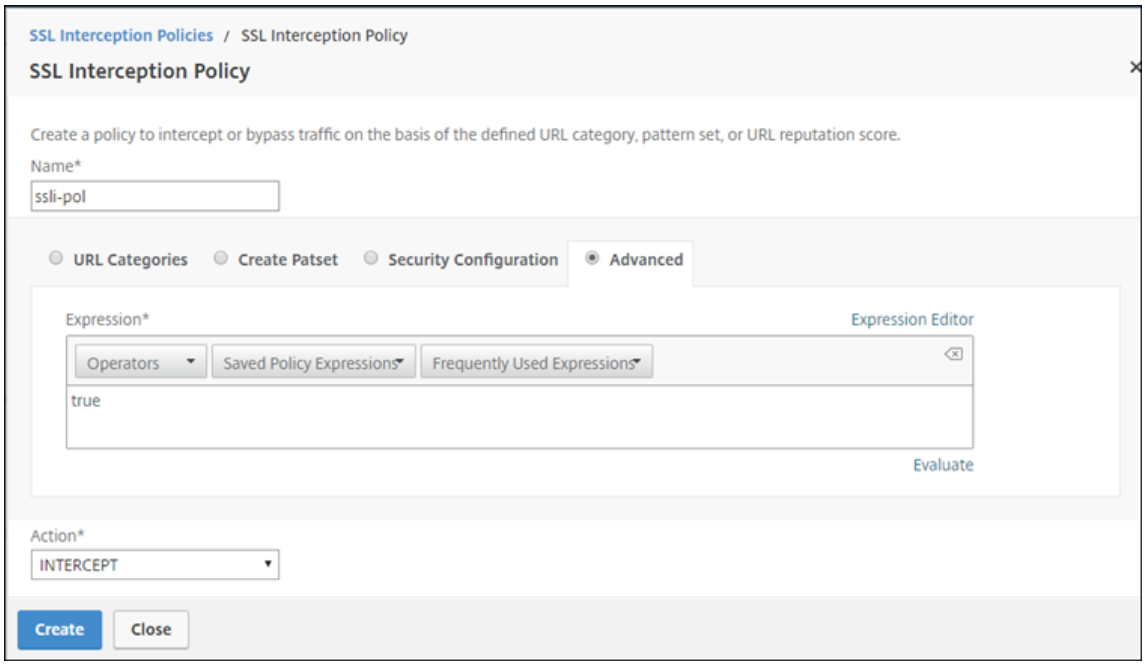


3. Klicken Sie auf **OK** und dann auf **Fertig**.
4. **Wählen Sie unter Select SSL Interception CA Certificate-Key Pair**ein vorhandenes Zertifikat aus oder klicken Sie auf „+“, um ein CA-Zertifikatsschlüsselpaar für die SSL-Interception zu installieren. Wenn Sie ein vorhandenes Zertifikat auswählen, überspringen Sie den nächsten Schritt.



5. Klicken Sie auf **Installieren** und dann auf **Schließen**.
6. Fügen Sie eine Richtlinie hinzu, um den gesamten Verkehr abzufangen. Klicken Sie auf **Bind**. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen, oder wählen Sie eine vorhandene Richtlinie aus. Wenn Sie eine vorhandene Richtlinie auswählen, klicken Sie auf **Einfügen**und überspringen Sie die nächsten drei Schritte.

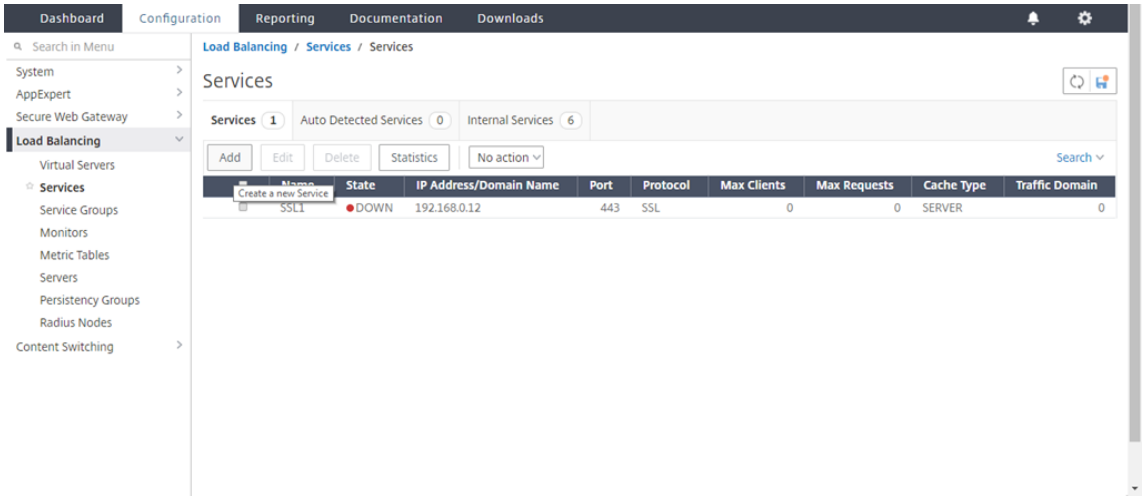
7. Geben Sie einen Namen für die Richtlinie ein und wählen Sie **Erweitert**. Geben Sie im Ausdruckseditor true ein.
8. Wählen Sie für **AktionABFANGEN**aus.



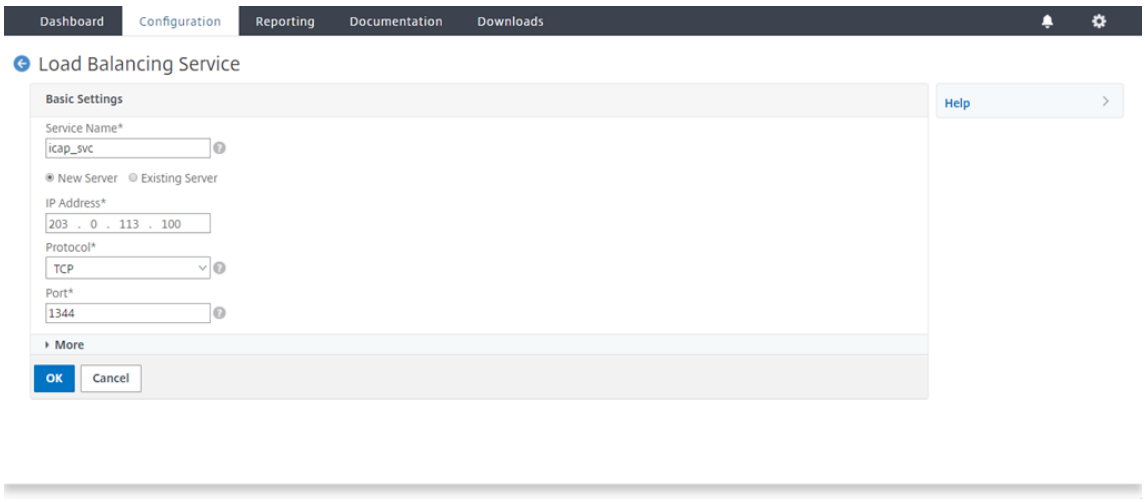
9. Klicken Sie auf **Erstellen**.
10. Klicken Sie viermal auf **Weiter** und dann auf **Fertig**.

Konfigurieren Sie die ICAP-Einstellungen

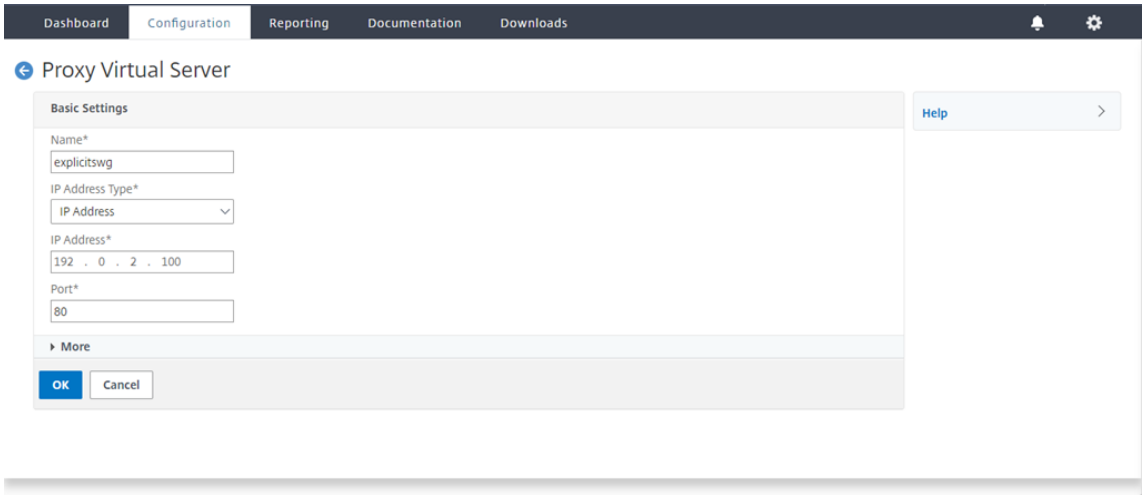
1. Navigieren Sie zu **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**.



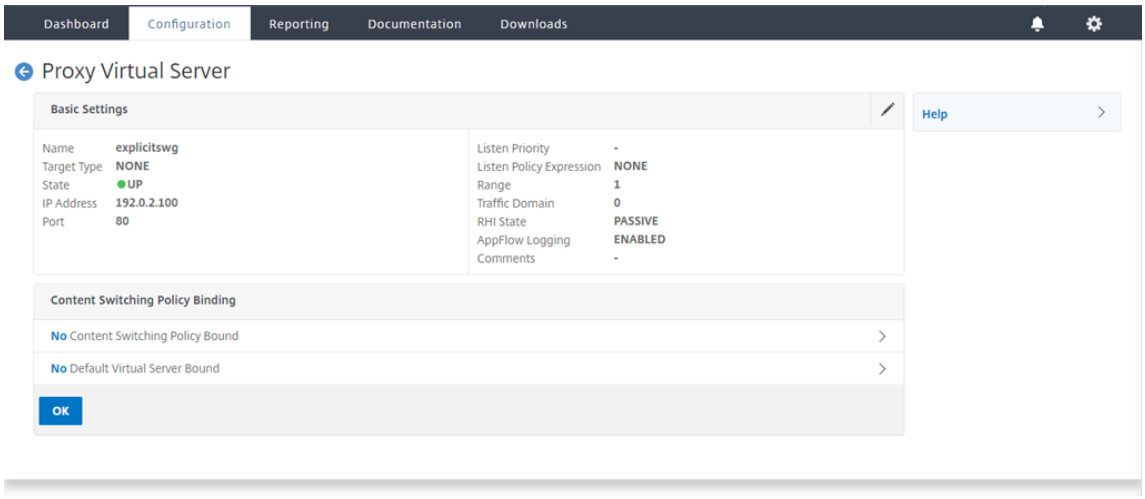
2. Geben Sie einen Namen und eine IP-Adresse ein. Wählen Sie **unter Protokoll**die Option **TCP**aus. Geben Sie im **Feld Port**den Wert **1344**ein. Klicken Sie auf **OK**.



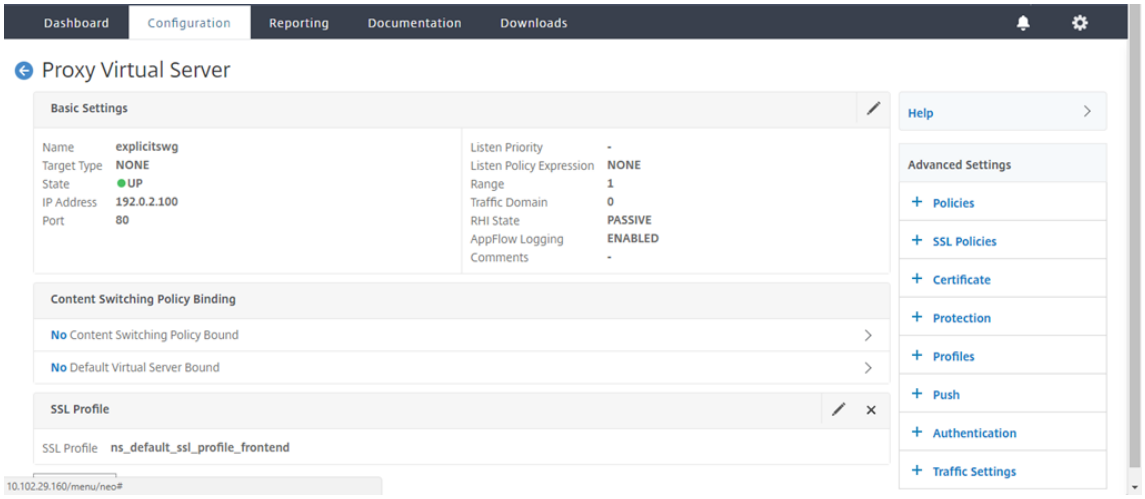
3. Navigieren Sie zu **SSL Forward Proxy** > **Proxy Virtual Servers**. Fügen Sie einen virtuellen Proxyserver hinzu oder wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**. Nachdem Sie die Details eingegeben haben, klicken Sie auf **OK**.



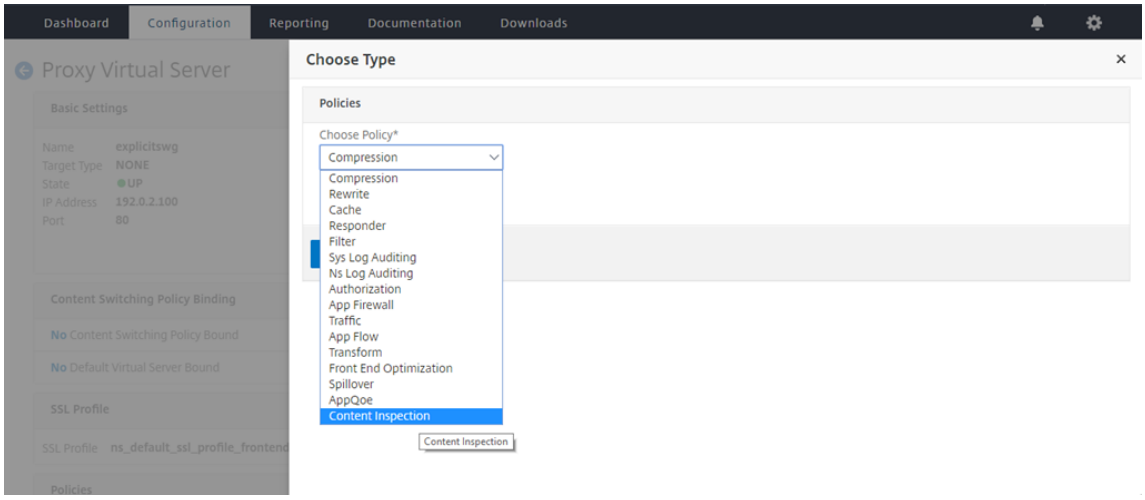
Klicken Sie erneut auf **OK** .



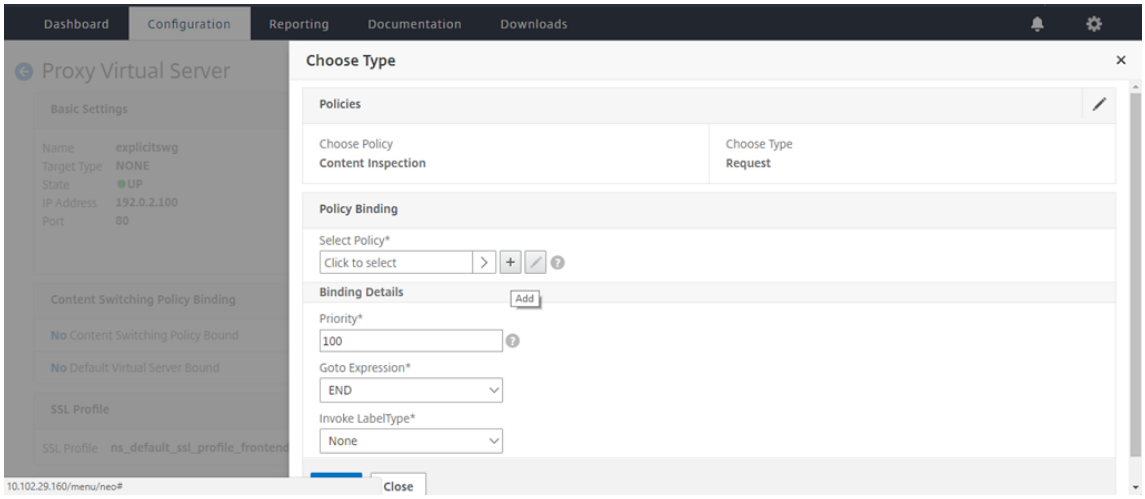
4. Klicken Sie in **den Erweiterten Einstellungen**auf **Richtlinien**.



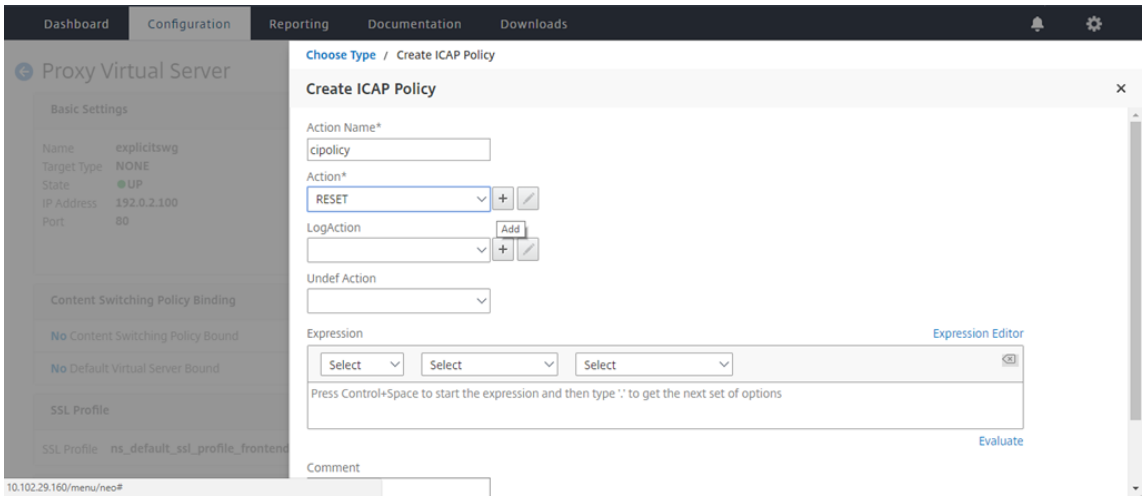
5. **Wählen Sie unter Choose Policy die**Option **Content Inspection**aus. Klicken Sie auf **Weiter**.



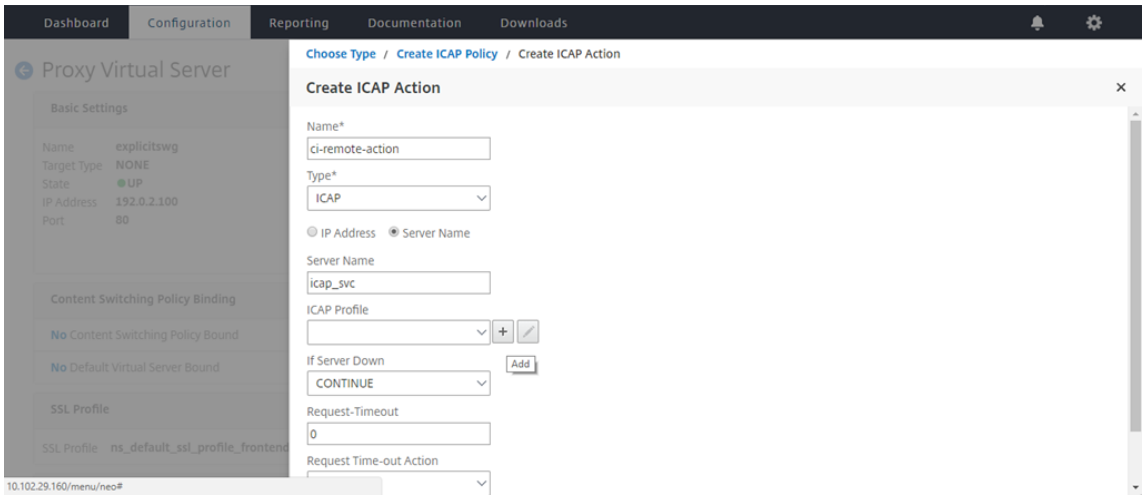
6. Klicken Sie unter „ **Richtlinie auswählen**“ auf das „+“ -Zeichen, um eine Richtlinie hinzuzufügen.



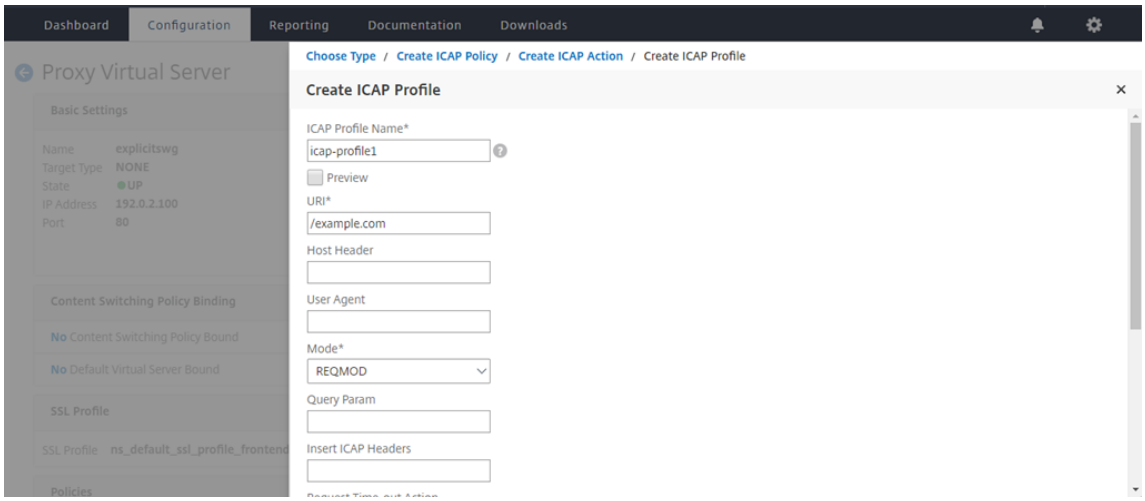
7. Geben Sie einen Namen für die Richtlinie ein. Klicken Sie unter **Aktion**auf das „+“ -Zeichen, um eine Aktion hinzuzufügen.



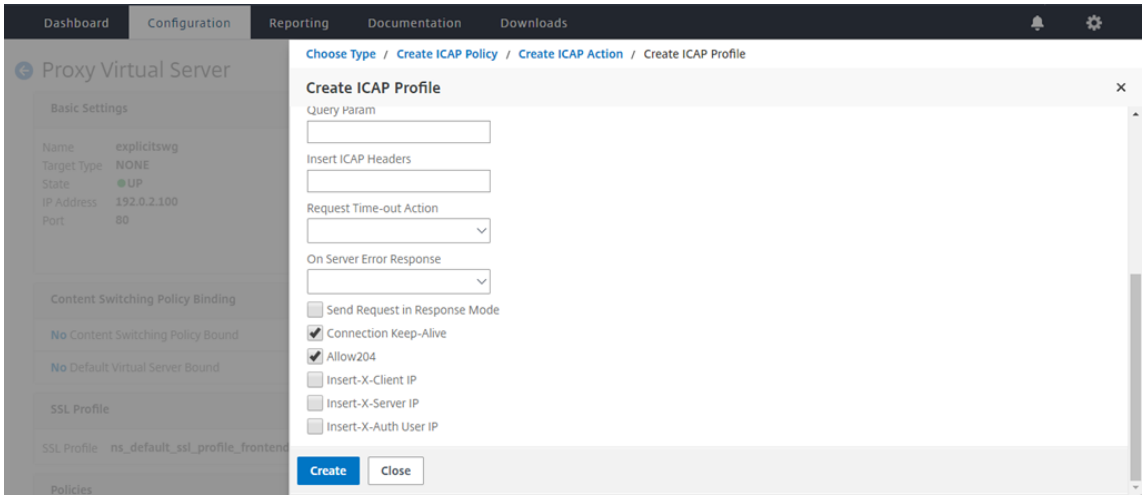
8. Geben Sie einen Namen für die Aktion ein. Geben Sie im Feld **Servername**den Namen des zuvor erstellten TCP-Dienstes ein. Klicken Sie im **ICAP-Profil**auf das „+“ -Zeichen, um ein ICAP-Profil hinzuzufügen.



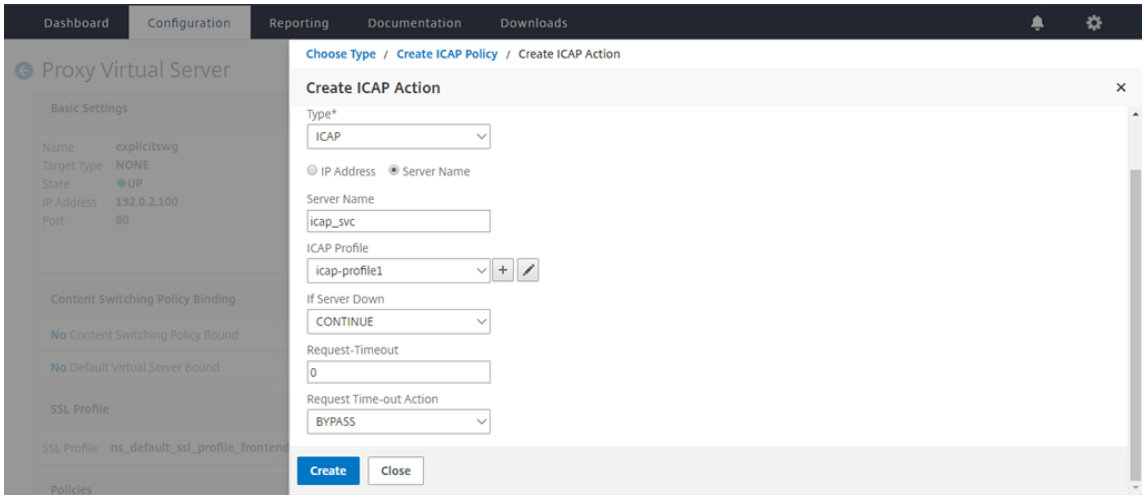
9. Geben Sie einen Profilnamen ein, URI. Wählen Sie unter **Modus**die Option **REQMOD**aus.



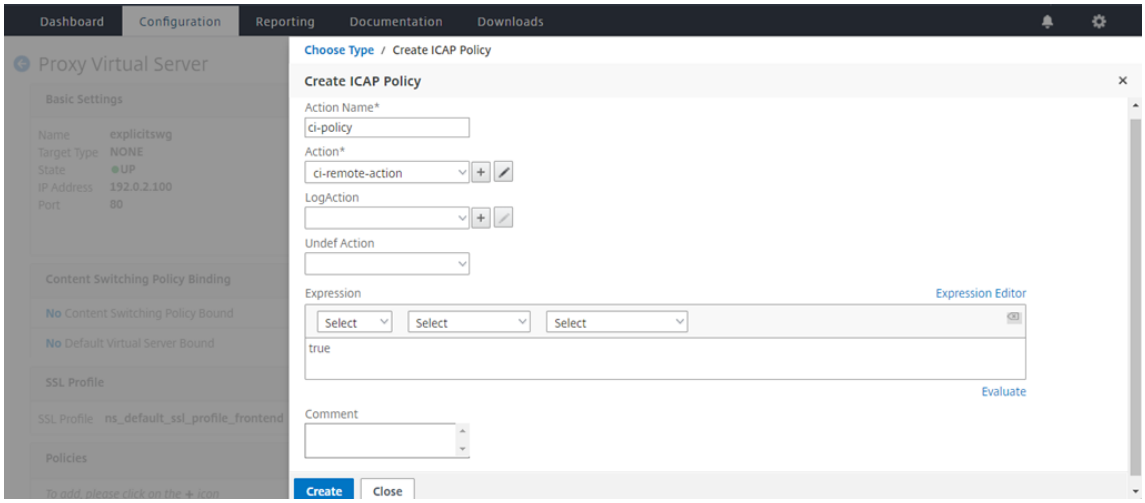
10. Klicken Sie auf **Erstellen**.



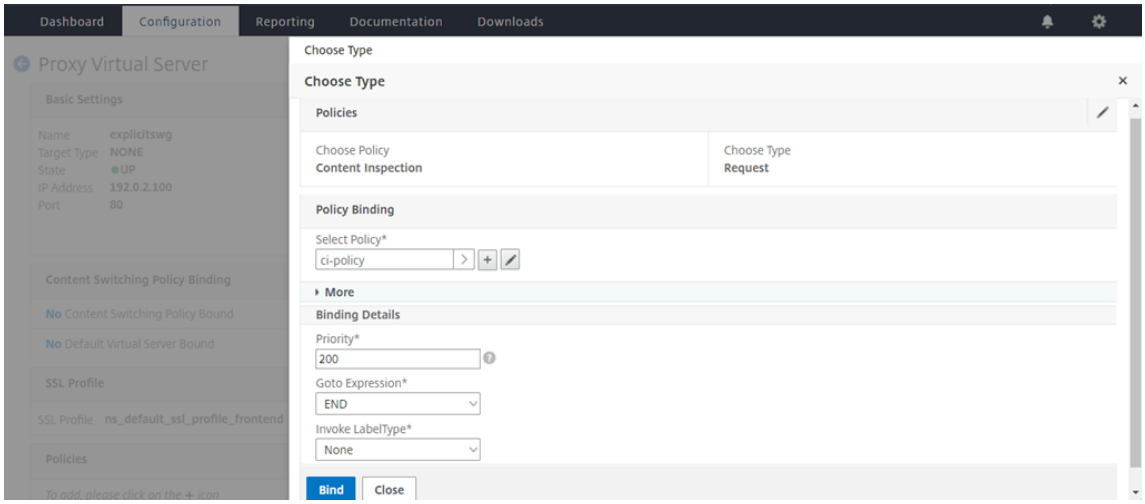
11. Klicken **Sie auf der Seite „ICAP-Aktion** erstellen“ auf **Erstellen**.



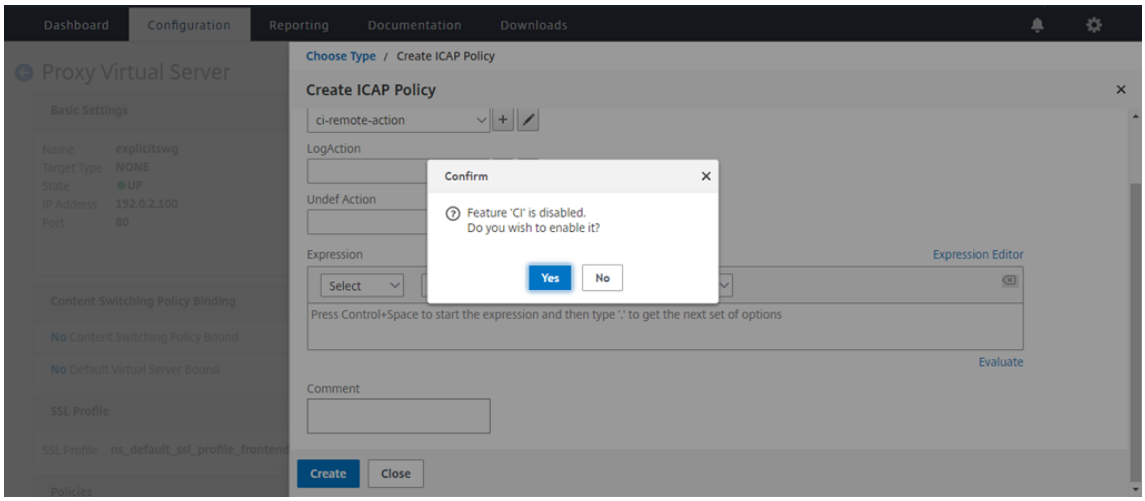
12. Geben Sie auf der Seite „ **ICAP-Richtlinie erstellen** “ im **Ausdruckseditor**den Wert true ein. Klicken Sie dann auf **Erstellen**.



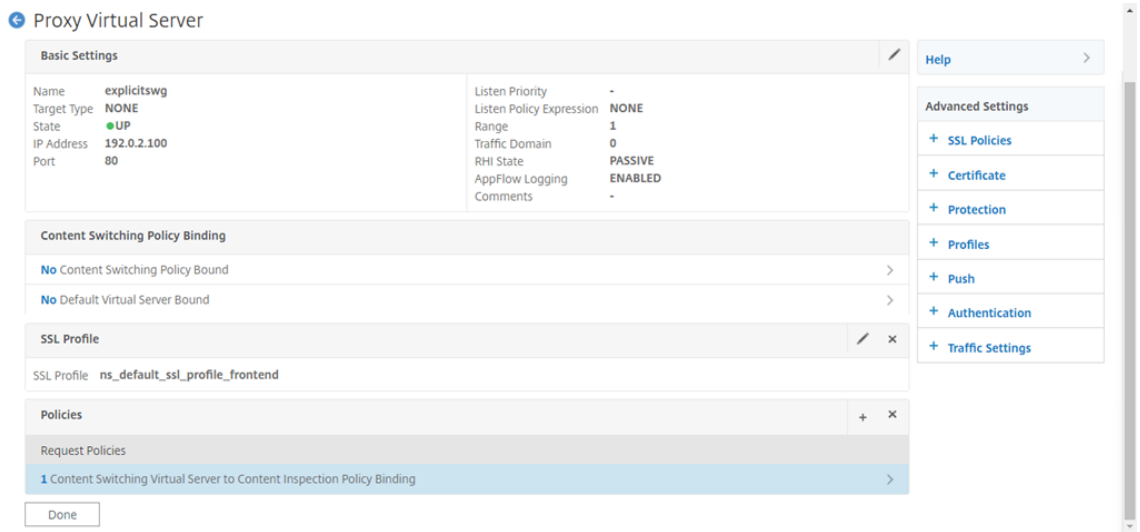
13. Klicken Sie auf **Bind**.



14. Wenn Sie aufgefordert werden, die Funktion zur Inhaltsüberprüfung zu aktivieren, wählen Sie **Ja**aus.



15. Klicken Sie auf **Fertig**.



Beispiel für ICAP-Transaktionen zwischen der NetScaler-Appliance und dem ICAP-Server in RESPMOD

Anfrage von der NetScaler-Appliance an den ICAP-Server:

```
RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0

Host: 10.106.137.15

Connection: Keep-Alive

Encapsulated: res-hdr=0, res-body=282

HTTP/1.1 200 OK

Date: Fri, 01 Dec 2017 11:55:18 GMT

Server: Apache/2.2.21 (Fedora)

Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT

ETag: "20169-45-55f457f42aee4"

Accept-Ranges: bytes

Content-Length: 69

Keep-Alive: timeout=15, max=100

```



```
Content-Type: text/plain; charset=UTF-8

X5O!P%@AP[4PZX54(P^)7CC)7 }
 $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
<!--NeedCopy-->
```

Antwort vom ICAP-Server auf die NetScaler Appliance:

```
ICAP/1.0 200 OK

Connection: keep-alive

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Encapsulated: res-hdr=0, res-body=224

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

ISTag: "9.8-13.815.00-3.100.1027-1.0"

X-Virus-ID: Eicar_test_file

X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;

HTTP/1.1 403 Forbidden

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Cache-Control: no-cache

Content-Type: text/html; charset=UTF-8

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

Content-Length: 5688

<html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset
   =UTF-8"/>

…

…

</body></html>
<!--NeedCopy-->
```


Anleitungsartikel

August 15, 2023

> **Hinweis:**
>
> Die URL-Kategorisierung in der URL-Filterfunktion ist in dieser Version veraltet.

Im Folgenden finden Sie einige Konfigurationsanweisungen oder funktionale Anwendungsfälle, die als How to -Artikel verfügbar sind, mit denen Sie Ihre SSL-Forward-Proxybereitstellung verwalten können.

URL-Filterung

So erstellen Sie eine URL-Kategorisierungsrichtlinie

So erstellen Sie eine URL-Listenrichtlinie

So lassen Sie eine außergewöhnliche URL zu

So blockieren Sie Websites für Erwachsene

Sicherheit

May 11, 2023

Die folgenden Themen behandeln Konfigurations- und Installationsinformationen für NetScaler-Sicherheitsfunktionen. Die meisten dieser Funktionen basieren auf Richtlinien.

Inhaltsfilterung	Sperrt unangemessene HTML-Anfragen und verhindert, dass die Anfragen die Webserver erreichen.
Überlastungsschutz	Erkennt einen schnellen Anstieg der Verbindungsversuche und passt die Geschwindigkeit an, mit der Verbindungen zum Server weitergeleitet werden dürfen, um eine Serverüberlastung zu verhindern.
DNS-Sicherheitsoptionen	Vereinfachter UI-Assistent zur Erstellung von Richtlinien zum Schutz vor DNS-Angriffen.

Überlastungsschutz

May 11, 2023

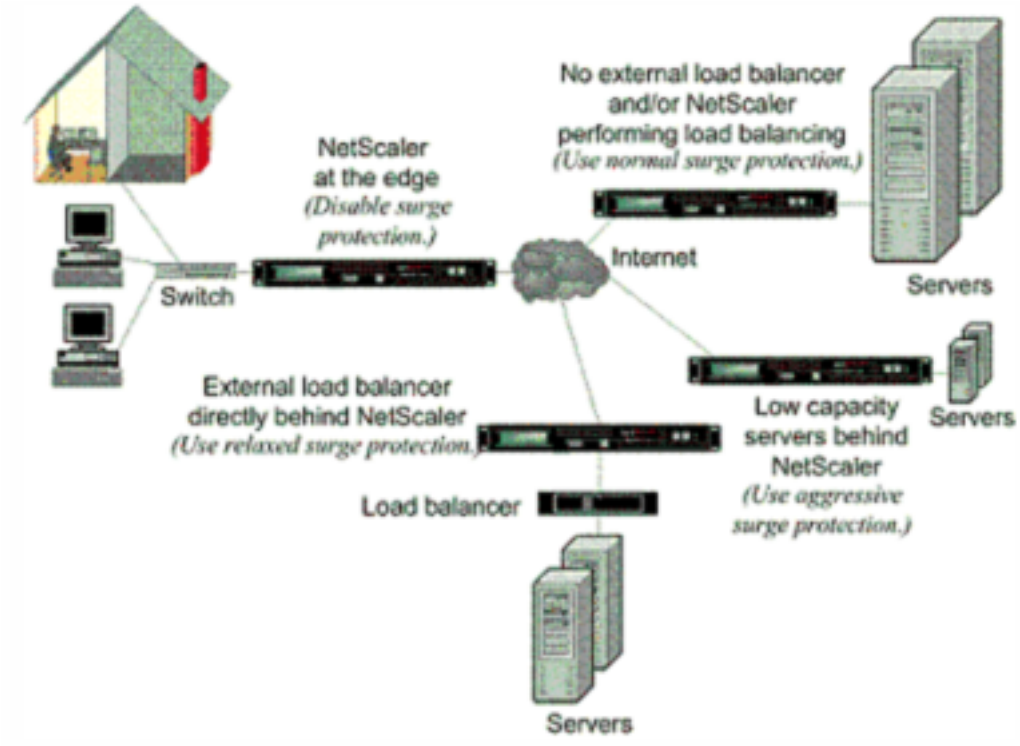
Wenn ein Anstieg der Clientanforderungen einen Server überlastet, wird die Serverantwort langsam und der Server kann nicht auf neue Anfragen reagieren. Die Überlastungsschutzfunktion stellt sicher, dass Verbindungen zum Server mit einer Geschwindigkeit hergestellt werden, die der Server verarbeiten kann. Die Rücklaufquote hängt davon ab, wie der Überlastungsschutz konfiguriert ist. Die NetScaler-Appliance verfolgt auch die Anzahl der Verbindungen zum Server und verwendet diese Informationen, um die Geschwindigkeit anzupassen, mit der neue Serververbindungen geöffnet werden.

Der Überlastungsschutz ist standardmäßig aktiviert. Wenn Sie keinen Überlastungsschutz verwenden möchten, wie es bei einigen speziellen Konfigurationen der Fall ist, müssen Sie ihn deaktivieren.

Die Standardeinstellungen für den Überlastungsschutz sind für die meisten Anwendungen ausreichend. Sie können den Überlastungsschutz jedoch so konfigurieren, dass er Ihren Anforderungen entspricht. Zuerst können Sie den Drosselungswert festlegen, um ihm mitzuteilen, wie aggressiv Verbindungsversuche verwaltet werden sollen. Zweitens können Sie den Basisschwellenwert festlegen, um die maximale Anzahl gleichzeitiger Verbindungen zu steuern, die die NetScaler-Appliance zulässt, bevor der Überspannungsschutz ausgelöst wird. (Der Standard-Basisschwellenwert wird durch den Drosselungswert festgelegt, aber nachdem Sie den Drosselungswert festgelegt haben, können Sie ihn in eine beliebige Zahl ändern.)

Die folgende Abbildung zeigt, wie der Überlastungsschutz so konfiguriert ist, dass der Datenverkehr auf eine Website verarbeitet wird.

Abbildung 1. Eine funktionale Illustration des NetScaler Überlastungsschutzes



> **Hinweis**
>
> Wenn die NetScaler-Appliance am Rand des Netzwerks installiert ist und dort mit Netzwerkgeräten auf der Client-Seite des Internets interagiert, muss die Überspannungsschutzfunktion deaktiviert werden. Überlastungsschutz muss auch deaktiviert werden, wenn Sie den USIP-Modus (Using Source IP) auf Ihrer Appliance aktivieren.

Wenn der Überlastungsschutz deaktiviert ist und ein Anstieg der Anforderungen auftritt, akzeptiert der Server so viele Anforderungen, wie er gleichzeitig verarbeiten kann, und beginnt dann, Anforderungen zu verwerfen. Wenn der Server mehr überlastet wird, sinkt er und die Antwortrate wird auf Null reduziert. Wenn sich der Server einige Minuten später vom Absturz erholt, sendet er Resets für alle ausstehenden Anfragen, bei denen es sich um ein abnormales Verhalten handelt, und reagiert auch auf neue Anfragen mit Resets. Der Prozess wiederholt sich für jede Überspannung in Anforderungen. Daher kann ein Server, der unter DDoS-Angriff steht und mehrere Anfragen erhält, für legitime Benutzer nicht verfügbar sein.

Wenn der Überlastungsschutz aktiviert ist und ein Anstieg der Anforderungen auftritt, verwaltet der Überlastungsschutz die Rate der Anfragen an den Server und sendet Anfragen nur so schnell an den Server, wie der Server diese Anforderungen verarbeiten kann. Auf diese Weise kann der Server auf jede Anfrage korrekt in der Reihenfolge antworten, in der sie empfangen wurde. Wenn der Anstieg vorbei ist, werden die rückgestellten Anforderungen so schnell gelöscht, wie der Server sie verarbeiten kann, bis die Anforderungsrate mit der Rücklaufquote übereinstimmt.

Überlastungsschutz deaktivieren und wieder aktivieren

May 11, 2023

Die Überspannungsschutzfunktion ist standardmäßig aktiviert. Wenn der Überspannungsschutz aktiviert ist, ist er für jeden Dienst aktiv, den Sie hinzufügen.

Deaktivieren oder aktivieren Sie den Überspannungsschutz über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlsätze ein, um den Überspannungsschutz zu deaktivieren oder wieder zu aktivieren und die Konfiguration zu überprüfen:

```
- disable ns feature SurgeProtection
- show ns feature
- enable ns feature SurgeProtection
- show ns feature
<!--NeedCopy-->
```

Beispiel:

```
disable ns feature SurgeProtection
 Done show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   OFF
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

```
 enable ns feature SurgeProtection
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   ON
 .
```



```
 .
 .

 24)    NetScaler Push                  push                  OFF
 Done
>
<!--NeedCopy-->
```

Deaktivieren oder aktivieren Sie den Überspannungsschutz über die GUI

1. Erweitern Sie im Navigationsbereich **System**und wählen Sie dann **Einstellungen**aus.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen ändern**.
3. Deaktivieren **Sie im Dialogfeld Erweiterte Funktionen konfigurieren** die Auswahl aus dem Kontrollkästchen **Überspannungsschutz**, um die Überspannungsschutzfunktion zu deaktivieren, oder aktivieren Sie das Kontrollkästchen, um das Feature zu aktivieren.
4. Klicken Sie auf **OK**.
5. Klicken Sie im Dialogfeld Features aktivieren/deaktivieren auf Ja. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert oder deaktiviert wurde.

Deaktivieren oder aktivieren Sie den Überspannungsschutz für einen bestimmten Dienst über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**. Die Liste der konfigurierten Dienste wird im Detailbereich angezeigt.
2. Wählen Sie im Detailbereich den Dienst aus, für den Sie die Überspannungsschutzfunktion deaktivieren oder wieder aktivieren möchten, und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Dienst konfigurieren** auf die **Registerkarte Erweitert**und scrollen Sie nach unten.
4. Deaktivieren Sie im Rahmen Andere die Auswahl des Kontrollkästchens **Überspannungsschutz**, um die Überspannungsschutzfunktion zu deaktivieren, oder aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren.
5. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert oder deaktiviert wurde.

   Hinweis: Der Überspannungsschutz funktioniert nur, wenn sowohl das Feature als auch die Service-Einstellung aktiviert sind.

Festlegen von Schwellenwerten für den Überlastungsschutz

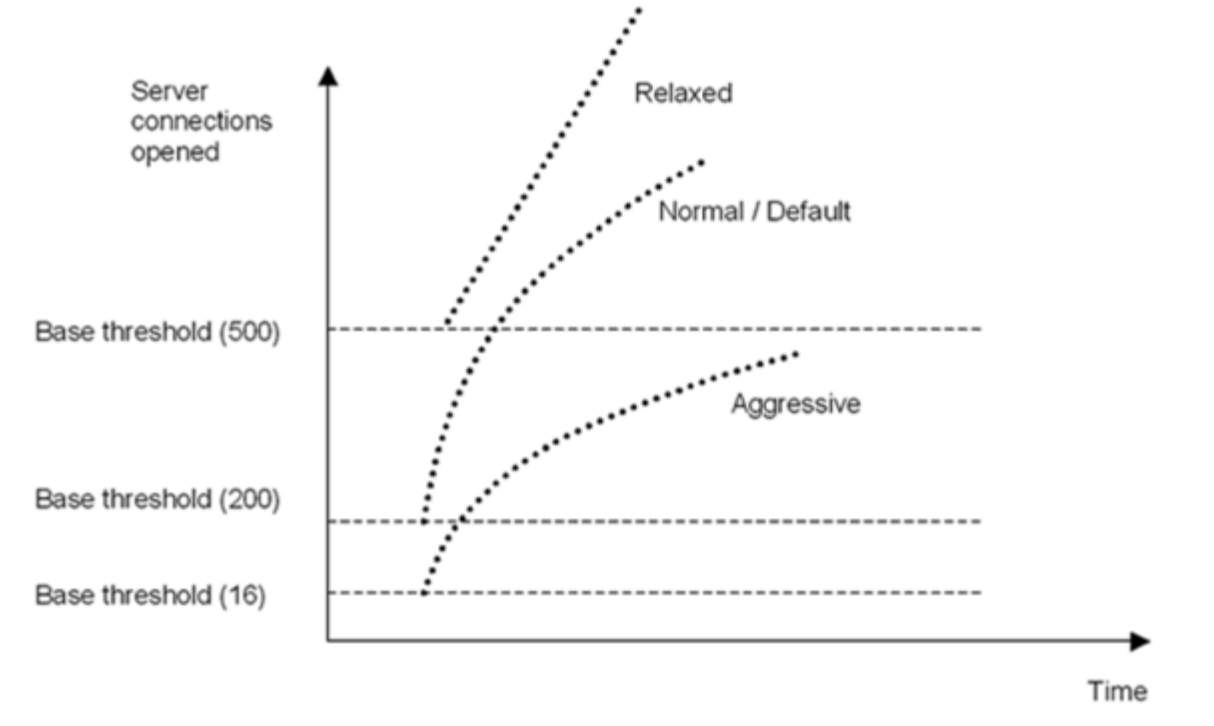
May 11, 2023

Um die Rate festzulegen, mit der die NetScaler Appliance Verbindungen zum Server öffnet, müssen Sie den Schwellenwert und die Drosselwerte für den Überlastungsschutz konfigurieren.

> **Hinweis**
>
> Schwellenwerte werden global konfiguriert, aber sie werden pro einzelnen Server mit Lastausgleich oder pro Dienst durchgesetzt.

Die folgende Abbildung zeigt die Überlastungsschutzkurven, die sich aus der Einstellung der Drosselklappenrate auf entspannt, normal oder aggressiv ergeben. Abhängig von der Konfiguration der Serverkapazität können Sie Basisschwellenwerte festlegen, um geeignete Überlastungsschutzkurven zu generieren.

Abbildung 1. Kurven zum Überlastungsschutz



Ihre Konfigurationseinstellungen wirken sich wie folgt auf das Verhalten des Überlastungsschutzes aus:

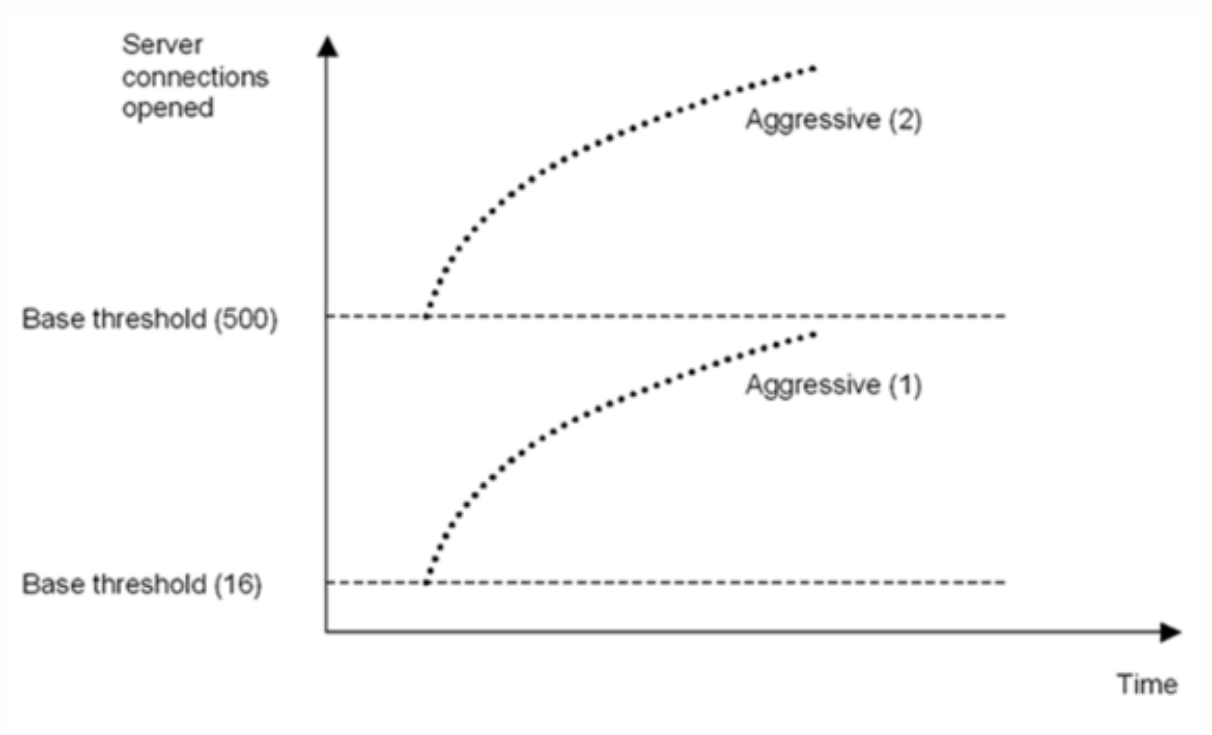
- Wenn Sie keine Drosselrate angeben, wird sie auf Normal (Standardwert) und der Basisschwellenwert auf 200 eingestellt, wie in der vorherigen Abbildung dargestellt.
- Wenn Sie eine Drosselrate (aggressiv, normal oder entspannt) angeben, ohne einen Basisschwellenwert anzugeben, spiegelt die Kurve die Standardwerte des Basisschwellenwerts für

diese Drosselrate wider. Wenn Sie beispielsweise die Drosselrate auf entspannt einstellen, hat die resultierende Kurve den Basisschwellenwert von 500.

- Wenn Sie nur den Basisschwellenwert angeben, verschiebt sich die gesamte Überlastungsschutzkurve abhängig vom angegebenen Wert nach oben oder unten, wie in der folgenden Abbildung dargestellt.
- Wenn Sie sowohl einen Basisschwellenwert als auch eine Drosselrate angeben, basiert die resultierende Überlastungsschutzkurve auf der eingestellten Drosselrate und wird entsprechend dem für den Basisschwellenwert festgelegten Wert angepasst.

In der folgenden Abbildung ergibt sich die untere Kurve (Aggressiv 1), wenn die Drosselrate auf aggressiv eingestellt ist, der Basisschwellenwert jedoch nicht eingestellt ist. Die obere Kurve (Aggressiv 2) ergibt sich, wenn der Basisschwellenwert auf 500 eingestellt ist, die Drosselrate jedoch nicht eingestellt ist. Die zweite obere Kurve (Aggressiv 2) ergibt sich auch, wenn der Basisschwellenwert auf 500 eingestellt ist und die Drosselrate auf aggressiv eingestellt ist.

Abbildung 2. Aggressive Rate mit dem Standard- oder einem festgelegten Basisschwellenwert



Legen Sie den Schwellenwert für den Überlastungsschutz über die GUI fest

1. Erweitern Sie im Navigationsbereich System, und wählen Sie dann Einstellungen aus.
2. Klicken Sie im Detailbereich auf Globale Systemeinstellungen.
3. Wenn Sie einen anderen Basisschwellenwert als den Standardschwellenwert für die Drosselrate festlegen möchten, geben Sie im Dialogfeld Globale Einstellungen konfigurieren im

Textfeld Basisschwellenwert die maximal zulässige Anzahl gleichzeitiger Serververbindungen ein, bevor der Überlastungsschutz ausgelöst wird. Der Basisschwellenwert ist die maximale Anzahl von Serververbindungen, die geöffnet werden können, bevor der Überlastungsschutz aktiviert wird. Der Höchstwert für diese Einstellung beträgt 32.767 Serververbindungen. Die Standardeinstellung für diesen Wert wird durch die im nächsten Schritt gewählte Drosselrate gesteuert.

Hinweis: Wenn Sie hier keinen expliziten Wert festlegen, wird der Standardwert verwendet.

4. Wählen Sie in der Dropdownliste Drosselung eine Drosselrate aus. Die Drosselung ist die Rate, mit der die NetScaler Appliance das Öffnen von Verbindungen zum Server zulässt. Die Drosselklappe kann auf folgende Werte eingestellt werden:
   - **Aggressiv:** Wählen Sie diese Option, wenn die Verbindungs- und Überspannungskapazität des Servers niedrig ist und die Verbindung sorgfältig verwaltet werden muss. Wenn Sie die Drosselung auf aggressiv einstellen, wird der Basisschwellenwert auf einen Standardwert von 16 festgelegt. Dies bedeutet, dass der Überlastungsschutz immer dann ausgelöst wird, wenn 17 oder mehr gleichzeitige Verbindungen zum Server bestehen.
   - **Normal:** Wählen Sie diese Option, wenn sich hinter der NetScaler Appliance oder Downstream kein externer Load Balancer befindet. Der Basisschwellenwert ist auf einen Wert von 200 eingestellt, was bedeutet, dass der Überlastungsschutz immer dann ausgelöst wird, wenn 201 oder mehr gleichzeitige Verbindungen zum Server bestehen. Normal ist die standardmäßige Gasoption.
   - **Entspannt:** Wählen Sie diese Option, wenn die NetScaler Appliance einen Lastausgleich zwischen einer großen Anzahl von Webservern durchführt und daher eine hohe Anzahl gleichzeitiger Verbindungen verarbeiten kann. Der Basisschwellenwert ist auf einen Wert von 500 eingestellt, was bedeutet, dass der Überlastungsschutz nur ausgelöst wird, wenn 501 oder mehr gleichzeitige Verbindungen zum Server bestehen.
5. Klicken Sie auf OK. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die globalen Einstellungen konfiguriert sind.

Surgewarteschlange leeren

May 11, 2023

Wenn ein physischer Server eine Flut von Anfragen erhält, reagiert er nur langsam auf die Clients, die gerade mit ihm verbunden sind, was die Benutzer unzufrieden und verärgert macht. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Um solche Überlastungen zu vermeiden, bietet die NetScaler-Appliance Funktionen wie einen Überspannungsschutz, der die Geschwindigkeit steuert, mit der neue Verbindungen zu einem Dienst hergestellt werden können.

Die Appliance verbindet Multiplexing zwischen Clients und physischen Servern. Wenn die Appliance eine Client-Anfrage für den Zugriff auf einen Dienst auf einem Server empfängt, sucht sie nach einer bereits bestehenden Verbindung zum Server, die frei ist. Wenn eine freie Verbindung gefunden wird, wird diese Verbindung verwendet, um eine virtuelle Verbindung zwischen dem Client und dem Server herzustellen. Wenn keine vorhandene freie Verbindung gefunden wird, stellt die Appliance eine neue Verbindung mit dem Server her und stellt eine virtuelle Verbindung zwischen einem Client und dem Server her. Wenn die Appliance jedoch keine neue Verbindung mit dem Server herstellen kann, sendet sie die Clientanforderung an eine Überspannungswarteschlange. Wenn alle physischen Server, die an den virtuellen Load Balancing- oder Content-Switching-Server gebunden sind, die Obergrenze für Client-Verbindungen erreichen (maximaler Client-Wert, Überspannungsschutzschwelle oder maximale Kapazität des Dienstes), kann die Appliance keine Verbindung zu einem Server herstellen. Die Überspannungsschutzfunktion verwendet die Überspannungswarteschlange, um die Geschwindigkeit zu regulieren, mit der Verbindungen zu den physischen Servern geöffnet werden. Die Appliance verwaltet eine andere Überspannungswarteschlange für jeden Dienst, der an den virtuellen Server gebunden ist.

Die Länge einer Überspannungswarteschlange nimmt zu, wenn eine Anfrage eingeht, für die die Appliance keine Verbindung herstellen kann, und die Länge verringert sich, wenn eine Anfrage in der Warteschlange an den Server gesendet wird oder eine Anfrage ein Timeout erhält und aus der Warteschlange entfernt wird.

Wenn die Warteschlange für einen Dienst oder eine Dienstgruppe zu lang wird, sollten Sie sie möglicherweise leeren. Sie können die Überspannungswarteschlange eines bestimmten Dienstes oder einer bestimmten Dienstgruppe oder aller Dienste und Dienstgruppen, die an einen virtuellen Lastausgleichsserver gebunden sind, leeren. Das Leeren einer Überspannungswarteschlange wirkt sich nicht auf die bestehenden Verbindungen aus. Nur die Anfragen in der Überspannungswarteschlange werden gelöscht. Für diese Anfragen muss der Kunde eine neue Anfrage stellen.

Sie können auch die Surge-Queue eines virtuellen Content Switching-Servers leeren. Wenn ein virtueller Content Switching-Server einige Anfragen an einen bestimmten virtuellen Lastausgleichsserver weiterleitet und der virtuelle Lastausgleichsserver auch einige andere Anfragen empfängt, werden beim Leeren der Überspannungswarteschlange des virtuellen Content Switching-Servers nur die von diesem virtuellen Content Switching-Server empfangenen Anforderungen geleert. Die anderen Anforderungen in der Überspannungswarteschlange des virtuellen Lastausgleichsservers werden nicht geleert.

Hinweis:

- Sie können die Anstiegswarteschlangen von Cache-Umleitungen, Authentifizierung, VPN oder virtuellen GSLB-Servern oder GSLB-Diensten nicht leeren.
- Verwenden Sie die Überspannungsschutzfunktion nicht, wenn die Option “Quell-IP (USIP)

> verwenden” aktiviert ist.

Leeren Sie eine Surge-Queue mithilfe der CLI

Der Befehl flush ns SurgeQ funktioniert auf folgende Weise:

- Sie können den Namen eines Dienstes, einer Dienstgruppe oder eines virtuellen Servers angeben, dessen Überspannungswarteschlange geleert werden muss.
- Wenn Sie während der Ausführung des Befehls einen Namen angeben, wird die Überspannungswarteschlange der angegebenen Entität geleert. Wenn mehrere Entitäten denselben Namen haben, leert die Appliance Überspannungswarteschlangen aller dieser Entitäten.
- Wenn Sie den Namen einer Dienstgruppe und einen Servernamen und einen Port angeben, während der Befehl ausgeführt wird, löscht die Appliance die Überspannungswarteschlange nur des angegebenen Dienstgruppenmitglieds.
- Sie können ein Dienstgruppenmitglied `<serverName> and <port>` nicht direkt angeben, ohne den Namen der Dienstgruppe anzugeben,`<name>` und Sie können nicht `<port>` ohne `<serverName>` angeben Geben Sie `<serverName>` und `<port>` an, wenn Sie die Überspannungswarteschlange für ein bestimmtes Dienstgruppenmitglied leeren möchten.
- Wenn Sie den Befehl ausführen, ohne Namen anzugeben, legt die Appliance die Überspannungswarteschlangen aller auf der Appliance vorhandenen Entitäten.
- Wenn ein Dienstgruppenmitglied mit einem Servernamen identifiziert wird, müssen Sie den Servernamen in diesem Befehl angeben. Sie können seine IP-Adresse nicht angeben.

Geben Sie in der Befehlszeile Folgendes ein:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
```

Beispiele

1. `flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80`

   Der vorhergehende Befehl spült die Überspannungswarteschlange des Dienstes oder virtuellen Servers, der SVC1ANZGB genannt wird und die IP-Adresse als 10.10.10 hat

2. `flush ns surgeQ`

   Der vorhergehende Befehl spült alle Überspannungswarteschlangen auf der Appliance.

Leere eine Überspannungswarteschlange über die GUI

Navigieren Sie zu Traffic Management > Content Switching > Virtuelle Server, wählen Sie einen virtuellen Server aus und wählen Sie in der Aktionsliste die Option Flush Surge Queueaus.

DNS-Sicherheitsoptionen

May 11, 2023

Sie können die DNS-Sicherheitsoptionen jetzt auf der Seite DNS-Sicherheitsprofil hinzufügen in der NetScaler-GUI konfigurieren. Verwenden Sie die AppExpert-Komponenten, um die DNS-Sicherheitsoptionen über die NetScaler-CLI oder die NITRO-API zu konfigurieren. Anweisungen finden Sie in der NITRO API-Dokumentation und im NetScaler Command Reference Guide.

Eine Option, der Schutz vor Cache-Poisoning, ist standardmäßig aktiviert und kann nicht deaktiviert werden. Sie können die anderen Optionen auf alle DNS-Endpunkte oder auf bestimmte virtuelle DNS-Server in Ihrer Bereitstellung anwenden, wie in der folgenden Tabelle dargestellt:

Sicherheitsoption	Kann auf alle DNS-Endpunkte angewendet werden?	Kann auf bestimmte virtuelle DNS-Server angewendet werden?
DNS-DDoS-Schutz	Ja	Ja
Ausnahmen verwalten — Server auf der Whitelist/Blacklist	Ja	Ja
Verhindern Sie zufällige Subdomain-Angriffe	Ja	Ja
Umgehen Sie den Cache	Ja	Nein
DNS-Transaktionen über TCP erzwingen	Ja	Ja
Geben Sie Stammdetails in der DNS-Antwort an	Ja	Nein

Schutz vor Cache-Vergiftungen

Ein Cache-Poison-Angriff leitet Benutzer von legitimen Websites auf bösartige Websites weiter.

Beispielsweise ersetzt der Angreifer eine echte IP-Adresse im DNS-Cache durch eine gefälschte IP-Adresse, die er kontrolliert. Wenn der Server auf Anfragen von diesen IP-Adressen reagiert, wird der Cache vergiftet. Nachfolgende Anfragen nach den Adressen der Domain werden an die Website des Angreifers weitergeleitet.

Die Option Cache-Vergiftungsschutz verhindert das Einfügen von beschädigten Daten in die Datenbank, die DNS-Server-Anforderungen und -Antworten zwischenspeichert. Diese Funktion ist in die

NetScaler Appliances integriert und ist immer aktiviert.

DNS-DDoS-Schutz

Sie können die Option DNS-DDoS-Schutz für jeden Anforderungstyp konfigurieren, der bei einem DDoS-Angriff verwendet wird. Für jeden Typ lässt die Appliance alle Anfragen fallen, die empfangen werden, nachdem ein Schwellenwert für die Anzahl der Anfragen, die in einem bestimmten Zeitraum (Zeitscheibe) empfangen wurden, überschritten wurde. Sie können diese Option auch so konfigurieren, dass eine Warnung auf dem SYSLOG-Server protokolliert wird. Zum Beispiel:

- **DROP:** - Wählen Sie diese Option aus, um Anfragen ohne Protokollierung abzulegen. Angenommen, Sie haben einen Datensatzschutz mit Schwellenwert 15, Zeitscheibe als 1 Sekunde aktiviert und DROP gewählt. Wenn die eingehenden Anfragen 15 Abfragen in 1 Sekunde überschreiten, werden die Pakete gelöscht.
- **WARN:** - Wählen Sie diese Option aus, um Anfragen zu PROTOKOLLIEREN und ABZULEGEN. Angenommen, Sie haben einen Datensatzschutz mit Schwellenwert 15, Zeitscheibe als 1 Sekunde aktiviert und WARN gewählt. Wenn die eingehenden Anfragen 15 Abfragen in einer Sekunde überschreiten, wird eine Warnmeldung protokolliert, die auf eine Bedrohung hinweist, und dann werden die Pakete gelöscht. Citrix empfiehlt Ihnen, Schwellenwerte für WARN festzulegen, die kleiner als den Schwellenwert von DROP für einen Datensatztyp sind. Eine solche Einstellung hilft Administratoren, einen Angriff zu identifizieren, indem sie eine Warnmeldung protokollieren, bevor der eigentliche Angriff stattfindet und NetScaler eingehende Anfragen fallen lässt.

Legen Sie über die grafische Benutzeroberfläche einen Schwellenwert für eingehenden Datenverkehr fest

1. Navigieren Sie zu **Konfiguration** > **Sicherheit** > **DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofil** auf **Hinzufügen**.
3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** wie folgt vor:
4. Erweitern Sie den **DNS-DDoS-Schutz**.
    a) Wählen Sie den Datensatztyp aus und geben Sie den Schwellenwert und den Zeitscheibenwert ein.
    b) Wählen Sie **DROP** oder **WARN**aus.
    c) Wiederholen Sie die Schritte a und b für jeden der anderen Datensatztypen, vor denen Sie schützen möchten.
5. Klicken Sie auf **Submit**.

Ausnahmen verwalten — allowlist/blocklist-Server

Ausnahmen verwalten ermöglicht es Ihnen, Ausnahmen hinzuzufügen, um die Liste zu blockieren oder Listendomänennamen und IP-Adressen zuzulassen. Zum Beispiel:

- Wenn eine bestimmte IP-Adresse beim Posten eines Angriffs identifiziert wird, kann eine solche IP-Adresse zur Sperrliste hinzugefügt werden.
- Wenn Administratoren feststellen, dass eine unerwartet hohe Anzahl von Anfragen für einen bestimmten Domänennamen vorliegt, kann dieser Domänenname zur Sperrliste hinzugefügt werden.
- `NXDomains` und einige der vorhandenen Domänen, die die Serverressourcen verbrauchen können, können auf die Sperrliste gesetzt werden.
- Wenn Administratoren Listendomänennamen oder IP-Adressen zulassen, werden Anfragen oder Anfragen nur von diesen Domänen oder IP-Adressen beantwortet und alle anderen werden gelöscht.

Erstellen Sie eine Zulassungsliste oder eine Sperrliste mit der GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** wie folgt vor:
   a) Erweitern **Sie Ausnahmen verwalten — Whitelist-/Blacklist-Server**.
   b) Wählen Sie **Blockieren** aus, um Abfragen von Domains/Adressen auf der schwarzen Liste zu blockieren, oder wählen Sie Nur **zulassen**, um Abfragen von Domains/Adressen auf der weißen Liste zuzulassen.
   c) Geben Sie in das Feld **Domainname/IP-Adresse** die Domainnamen, IP-Adressen oder IP-Adressbereiche ein. Trennen Sie die Einträge durch Kommas.
   Hinweis: Wenn Sie **Erweiterte Option**auswählen, können Sie die Optionen “Start mit”, “enthält” und “endet mit” verwenden, um die Kriterien festzulegen.
   Sie können beispielsweise Kriterien festlegen, um eine DNS-Abfrage zu blockieren, die mit “image” beginnt oder mit “.co.ru” endet oder “mobile Websites enthält. “
4. Klicken Sie auf **Submit**.

Verhindern Sie zufällige Subdomain-Angriffe

Bei zufälligen Subdomain-Angriffen werden Abfragen an zufällige, nicht vorhandene Subdomänen legitimer Domänen gesendet. Diese Aktion erhöht die Belastung der DNS-Resolver und Server. Infolgedessen können sie überlastet werden und sich verlangsamen.

Die Option „Zufällige Subdomain-Angriffe verhindern“ weist den DNS-Responder an, DNS-Abfragen zu löschen, die eine bestimmte Länge überschreiten.

Gehen Sie davon aus, dass example.com ein Domainname ist, der Ihnen gehört und daher die Lösungsanfrage an Ihren DNS-Server gesendet wird. Der Angreifer kann eine zufällige Subdomain an example.com anhängen und eine Anfrage senden. Basierend auf der angegebenen Abfragelänge und des FQDN werden die Zufallsabfragen gelöscht.

Wenn die Abfrage beispielsweise www.image987trending.example.com lautet, wird sie gelöscht, wenn die Abfragelänge auf 20 festgelegt ist.

Angeben einer DNS-Abfragelänge über die GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** wie folgt vor:
   a) Erweitern Sie **Zufällige Subdomain-Angriffe verhindern**.
   b) Geben Sie den numerischen Wert für die Abfragelänge ein.
4. Klicken Sie auf **Submit**.

Den Cache umgehen

Während eines Angriffs müssen die Daten, die bereits zwischengespeichert sind, geschützt werden. Um den Cache zu schützen, können neue Anfragen für bestimmte Domänen oder Datensatztypen oder Antwortcodes an die Ursprungsserver gesendet und nicht zwischengespeichert werden.

Die Option Bypassing the Cache weist die NetScaler Appliance an, den Cache für bestimmte Domänen, Datensatztypen oder Antwortcodes zu Bypass, wenn ein Angriff erkannt wird.

Umgehen Sie den Cache für bestimmte Domänen oder Datensatztypen oder Antworttypen mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Erweitern Sie auf der Seite **DNS-Sicherheitsprofil hinzufügenden Cache umgehen** und geben Sie die Domainnamen ein. Wählen Sie optional die Datensatztypen oder die Antworttypen aus, für die der Cache umgangen werden muss.
   - Klicken Sie auf **Domänen**, und geben Sie die Domänennamen ein. Trennen Sie die Einträge durch Kommas.
   - Klicken Sie auf **Datensatztypen** und wählen Sie die Datensatztypen aus.
   - Klicken Sie auf **Antworttypen** und wählen Sie den Antworttyp aus.
4. Klicken Sie auf **Submit**.

DNS-Transaktionen über TCP erzwingen

Einige DNS-Angriffe können verhindert werden, wenn die Transaktionen gezwungen werden, TCP anstelle von UDP zu verwenden. Während eines Bot-Angriffs sendet der Client beispielsweise eine Flut von Anfragen, kann aber keine Antworten verarbeiten. Wenn die Verwendung von TCP für diese Transaktionen erzwungen wird, können die Bots die Antworten nicht verstehen und können daher keine Anfragen über TCP senden.

Erzwingen Sie mithilfe der GUI, dass Domänen oder Datensatztypen auf TCP-Ebene ausgeführt werden

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Erweitern Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** die Option **DNS-Transaktionen über TCP erzwingen** und geben Sie die Domainnamen und/oder/ein oder wählen Sie die Datensatztypen aus, für die die DNS-Transaktionen über TCP erzwungen werden müssen.
    - Klicken Sie auf **Domänen**, und geben Sie die Domänennamen ein. Trennen Sie die Einträge durch Kommas.
    - Klicken Sie auf ****Datensatztypen**** und wählen Sie die Datensatztypen aus.
4. Klicken Sie auf **Submit**.

Geben Sie Stammdetails in der DNS-Antwort an

Bei einigen Angriffen sendet der Angreifer eine Flut von Abfragen für nicht verwandte Domänen, die nicht auf der NetScaler Appliance konfiguriert oder zwischengespeichert sind. Wenn der `dnsRootReferral` Parameter ENABLED ist, werden alle Root-Server verfügbar.

Die Option Stammdetails in der DNS-Antwort bereitstellen weist die NetScaler Appliance an, den Zugriff auf Stammverweise für eine Abfrage zu beschränken, die nicht konfiguriert oder zwischengespeichert ist. Die Appliance sendet eine leere Antwort.

Die Option Stammdetails in der DNS-Antwort bereitstellen kann auch Amplifikationsangriffe mildern oder blockieren. Wenn der DnsRootReferral-Parameter DEAKTIVIERT ist, gibt es keine Root-Verweise in den NetScaler-Antworten und werden daher nicht verstärkt.

Aktivieren oder Deaktivieren des Zugriffs auf den Stammserver über die GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** wie folgt vor:
    a) Erweitern **Sie die Option Root-Details angeben in der DNS-Antwort**.

b) Klicken Sie **auf ON** oder **OFF**, um den Zugriff auf den Root-Server zuzulassen oder einzuschränken.

4. Klicken Sie auf **Submit**.

System

May 11, 2023

Dieser Abschnitt enthält Informationen zum NetScaler auf Systemebene. Dazu gehören eine ausführliche Erläuterung der Funktionen auf Systemebene, die Szenarien, in denen die Funktionen verwendet werden können, die Konfigurationsschritte und Beispiele, die Ihnen helfen, die Funktionen besser zu verstehen.

- Grundlegende Operationen
- Authentifizierung und Autorisierung
- TCP-Konfigurationen
- HTTP-Konfigurationen
- SNMP
- Auditprotokollierung
- Webserver-Protokollierung
- Call Home
- Reporting-Tool
- CloudBridge-Connector
- Hohe Verfügbarkeit
- TCP-Optimierung

Systembasisbetrieb

May 11, 2023

Mit den folgenden Konfigurationen können Sie Systembasisvorgänge auf einer NetScaler-Appliance ausführen.

So zeigen Sie die NetScaler-Konfiguration an, speichern und löschen

NetScaler-Konfigurationen werden in der gespeichert `/nsconfig/ns.conf directory`. Damit Konfigurationen sitzungsübergreifend verfügbar sind, müssen Sie die Konfiguration nach jeder Konfigurationsänderung speichern.

Anzeigen der laufenden Konfiguration mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
show ns runningConfig
<!--NeedCopy-->
```

Zeigen Sie die laufende Konfiguration über die GUI an

1. Navigieren Sie zu **System** > **Diagnose**, und klicken Sie in der Gruppe **Konfiguration anzeigen** auf **Konfiguration ausführen**.

Zeigen Sie den Unterschied zwischen den beiden Konfigurationsdateien über die Befehlszeilenschnittstelle an

Geben Sie in der Befehlszeile Folgendes ein:

```
diff ns config <configfile> <configfile2>
<!--NeedCopy-->
```

Zeigen Sie den Unterschied zwischen den beiden Konfigurationsdateien über die GUI an

1. Navigieren Sie zu **System** > **Diagnose**, und klicken Sie in der **Gruppe Konfiguration anzeigen** auf **Konfigurationsdifferenz** .

Speichern von NetScaler Konfigurationen mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
save ns config
<!--NeedCopy-->
```

Speichern Sie NetScaler-Konfigurationen über die GUI

1. Klicken Sie auf der Registerkarte **Konfiguration** in der oberen rechten Ecke auf das Symbol **Speichern** .

Anzeigen gespeicherter Konfigurationen mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
show ns ns.conf
<!--NeedCopy-->
```

Gespeicherte Konfigurationen über die GUI anzeigen

Navigieren Sie zu **System** > **Diagnose** und klicken Sie in der Gruppe **Konfiguration anzeigen** auf **Gespeicherte Konfiguration**.

Löschen der NetScaler Konfiguration mit der Befehlszeilenschnittstelle

Sie haben die folgenden drei Möglichkeiten, die NetScaler-Konfiguration zu löschen.

Grundstufe. Wenn Sie Ihre Konfiguration auf der Basis-Ebene löschen, werden alle Einstellungen außer den folgenden gelöscht:

- `Nsroot` password
- Zeitzone
- NTP-Server
- ADM-Server verbinden
- Lizenz-Fie-Informationen
- NSIP, MIP (s) und SNIP (s)
- Netzwerkeinstellungen (Standardeinstellungen für Gateway, VLAN, RHI, NTP und DNS-Einstellungen)
- Definitionen von HA-Knoten
- Feature- und Moduseinstellungen
- Standardadministratorkennwort (`nsroot`)

Erweiterte Ebene. Wenn Sie Ihre Konfiguration auf der erweiterten Ebene löschen, werden alle Einstellungen außer den folgenden gelöscht:

- NSIP und SNIP (s)
- Netzwerkeinstellungen (Standardeinstellungen für Gateway, VLAN, RHI, NTP und DNS-Einstellungen)
- Definitionen von HA-Knoten

Feature- und Moduseinstellungen werden auf ihre Standardwerte zurückgesetzt.

Volles Level. Wenn Sie Ihre Konfiguration auf der vollen Ebene löschen, werden alle Einstellungen auf die werkseitigen Standardwerte zurückgesetzt. Das NSIP und das Standard-Gateway werden jedoch nicht geändert, da eine Änderung dazu führen kann, dass die Appliance die Netzwerkkonnektivität verliert.

Geben Sie in der Befehlszeile Folgendes ein:


```
clear ns config -force
<!--NeedCopy-->
```

Beispiel: Um die Grundkonfigurationen auf einer Appliance zwangsweise zu löschen.

```
clear ns config -force basic
<!--NeedCopy-->
```

Löschen Sie die NetScaler-Konfiguration über die GUI

Navigieren Sie zu **System** > **Diagnose**, klicken Sie in der Gruppe Wartung auf **Konfiguration löschen, und wählen Sie die Konfigurationsebene** aus, die von der Appliance gelöscht werden soll.

So starten oder fahren Sie die Appliance für nicht gespeicherte NetScaler-Konfigurationen neu

Die NetScaler-Appliance kann von den verfügbaren Benutzeroberflächen aus der Ferne neu gestartet oder heruntergefahren werden. Wenn Sie eine eigenständige NetScaler-Appliance neu starten oder herunterfahren, gehen die nicht gespeicherten Konfigurationen (Konfigurationen, die seit der letzten Ausgabe des Befehls
save ns config ausgeführt wurden) verloren.

In einem Hochverfügbarkeitssetup, wenn die primäre Appliance neu gestartet oder heruntergefahren wird, übernimmt die sekundäre Appliance die Kontrolle und wird zur primären Appliance. Die ungespeicherten Konfigurationen aus dem alten Primärgerät sind auf dem neuen primären Gerät verfügbar.

Sie können die Appliance auch neu starten, indem Sie nur die NetScaler-Software neu starten und das zugrunde liegende Betriebssystem nicht neu starten. Dies wird als warmer Neustart bezeichnet. Wenn Sie beispielsweise eine neue Lizenz hinzufügen oder die IP-Adresse ändern, können Sie die NetScaler-Appliance neu starten, damit diese Änderungen vorgenommen werden.

> **Hinweis:**
>
> Sie können einen Warm-Neustart nur auf einer eigenständigen NetScaler-Appliance durchführen.

Starten Sie die Appliance über die Befehlszeile neu

Geben Sie in der Befehlszeile Folgendes ein:

```
reboot [-warm]
<!--NeedCopy-->
```


Starten Sie eine NetScaler-Appliance über die GUI neu

1. Klicken Sie auf der Konfigurationsseite auf **Reboot**.
2. Wenn Sie zum Neustart aufgefordert werden, wählen Sie **Konfiguration speichern** aus, um sicherzustellen, dass Sie keine Konfigurationen verlieren.

> **Hinweis:**
>
> Sie können einen warmen Neustart durchführen, indem Sie Warm reboot wählen.

Fahren Sie eine Appliance mit der Befehlszeilenschnittstelle herunter

Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

- `shutdown -p now`: Schaltet die Software herunter und schaltet den NetScaler aus. Um NetScaler MPX neu zu starten, drücken Sie den Wechselstromschalter. Um NetScaler VPX neu zu starten, starten Sie die VPX-Instanz neu.
- `shutdown -h now`: Schaltet die Software herunter und lässt den NetScaler eingeschaltet. Drücken Sie eine beliebige Taste, um NetScaler neu zu starten. Dieser Befehl schaltet den NetScaler nicht aus. Schalten Sie daher die Wechselstromversorgung nicht aus oder entfernen Sie die Wechselstromkabel.

> **Hinweis:**
>
> Sie können eine Appliance nicht über die NetScaler GUI herunterfahren.

So synchronisieren Sie die Systemuhr mit Servern im Netzwerk

Sie können Ihre NetScaler-Appliance so konfigurieren, dass ihre lokale Uhr mit einem Network Time Protocol (NTP) -Server synchronisiert wird. Dadurch wird sichergestellt, dass die Uhr dieselben Datums- und Uhrzeiteinstellungen hat wie die anderen Server in Ihrem Netzwerk.

Sie können die Uhrsynchronisierung auf Ihrer Appliance konfigurieren, indem Sie NTP-Servereinträge entweder über die GUI oder die Befehlszeilenschnittstelle zur Datei ntp.conf hinzufügen oder die Datei ntp.conf manuell ändern und dann den NTP-Daemon (NTPD) starten. Die Konfiguration der Uhrsynchronisierung ändert sich nicht, wenn die Appliance neu gestartet, aktualisiert oder heruntergestuft wird. Die Konfiguration wird jedoch in einem Hochverfügbarkeitssetup nicht an den sekundären NetScaler weitergegeben.

Mit der NetScaler GUI können Sie die Zeitzone und die IP-Adresse des NTP-Servers konfigurieren, die für die Uhrsynchronisierung auf dem Bildschirm für den Erstbenutzer (FTU) erforderlich sind.

> **Hinweis:**
>
> Wenn Sie keinen lokalen NTP-Server haben, finden Sie eine Liste öffentlicher Open-Access-NTP-

> Server auf der offiziellen NTP-Site unter Public Time Server List. <http://www.ntp.org> Bevor Sie Ihren NetScaler für die Verwendung eines öffentlichen NTP-Servers konfigurieren, lesen Sie unbedingt die Seite Rules of Engagement (Link finden Sie auf allen Public Time Server-Seiten).
>
> In NetScaler Version 11 wurde die NTP-Version von 4.2.6p3 auf 4.2.8p2 aktualisiert.

Voraussetzung

Um die Uhrsynchronisierung zu konfigurieren, müssen Sie die folgenden Entitäten konfigurieren:

1. NTP-Server
2. NTP-Synchronisierung.

Fügen Sie einen NTP-Server mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen NTP-Server hinzuzufügen und die Konfiguration zu überprüfen:

- `add ntp server (<serverIP> | <serverName>)[-minpoll <positive_integer>] [-maxpoll <positive_integer>]`
- `show ntp server`

Beispiel:

```
add ntp server 10.102.29.30 -minpoll 6 -maxpoll 11
<!--NeedCopy-->
```

Hinzufügen eines NTP-Servers über die GUI

Navigieren Sie zu **System** > **NTP-Server**, und erstellen Sie den NTP-Server.

Aktivieren der NTP-Synchronisierung mit der Befehlszeilenschnittstelle

Wenn Sie die NTP-Synchronisierung aktivieren, startet NetScaler den NTP-Daemon und verwendet die NTP-Servereinträge in der Datei ntp.conf, um seine Ortszeit zu synchronisieren. Wenn Sie die Appliance-Zeit nicht mit den anderen Servern im Netzwerk synchronisieren möchten, können Sie die NTP-Synchronisierung deaktivieren, wodurch der NTP-Daemon (NTPD) gestoppt wird.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
enable ntp sync
<!--NeedCopy-->
```


Aktivieren Sie die NTP-Synchronisierung über die GUI

Navigieren Sie zu **System** > **NTP-Server**, klicken Sie auf **Aktion** und wählen Sie **NTP-Synchronisierung**aus.

Konfigurieren Sie die Uhrsynchronisierung, um eine ntp.conf-Datei über die GUI zu bearbeiten

1. Melden Sie sich an der Befehlszeilenoberfläche an.
2. Wechselt zur Shell-Eingabeaufforderung
3. Kopieren Sie die Datei `/etc/ntp.conf` nach `/nsconfig/ntp.conf`, es sei denn, `/nsconfig directory` enthält bereits eine Datei `ntp.conf`.
4. Für jeden NTP-Server, den Sie hinzufügen möchten, müssen Sie der`/nsconfig/ntp.conf` Datei die folgenden zwei Zeilen hinzufügen:

```
server <IP address for NTP server> iburst

restrict <IP address for NTP server> mask <netmask> nomodify
   notrap nopeer noquery
<!--NeedCopy-->
```

> **Hinweis:**
>
> Aus Sicherheitsgründen sollte es für jeden Servereintrag einen entsprechenden Restrict-Eintrag geben.

Beispiel

Im folgenden Beispiel hat ein Administrator # -Zeichen eingefügt, um einen vorhandenen NTP-Eintrag auszukommentieren, und dann einen Eintrag hinzugefügt:

```
#server 1.2.3.4 iburst

#restrict 1.2.3.4 mask 55.255.255.255 nomodify notrap nopeer
   noquery

server 10.102.29.160 iburst

restrict 10.102.29.160 mask 255.255.255.255 nomodify notrap nopeer
    noquery
<!--NeedCopy-->
```

5. Wenn das Verzeichnis `/nsconfig` keine Datei mit dem Namen `rc.netscaler` enthält, erstellen Sie die Datei.
6. Fügen Sie den folgenden Eintrag hinzu `/nsconfig/rc.netscaler: /bin/sh /etc/ntpd_ctl full_start`

Dieser Eintrag startet den Dienst ntpd, prüft die Datei ntp.conf und protokolliert Meldungen im Verzeichnis /var/log.

Dieser Prozess wird jedes Mal ausgeführt, wenn der NetScaler neu gestartet wird.

7. Starten Sie die NetScaler-Appliance neu, um die Uhrsynchronisierung zu aktivieren. Oder geben Sie an der Shell-Eingabeaufforderung die folgenden Befehle ein, um die Uhrzeitsynchronisierung zu starten, ohne die Appliance neu zu starten:

```
rm /etc/ntp.conf
ln -s /nsconfig/ntp.conf /etc/ntp.conf
/bin/sh /etc/ntpd_ctl full_start
<!--NeedCopy-->
```

So konfigurieren Sie das Sitzungstimeout für Clientverbindungen im Leerlauf

Ein Sitzungstimeout-Intervall wird bereitgestellt, um die Zeitdauer einzuschränken, für die eine Sitzung (GUI, CLI oder API) aktiv bleibt, wenn sie nicht verwendet wird. Für den NetScaler kann das Systemsitzungs-Timeout auf den folgenden Ebenen konfiguriert werden:

- **Timeout auf Benutzerebene.** Gilt für den jeweiligen Benutzer.

Interface-Typ	Time-out-Konfiguration
Grafische Benutzeroberfläche (GUI)	Navigieren Sie zu **System > Benutzerverwaltung > Benutzer**, wählen Sie einen Benutzer aus und bearbeiten Sie die Timeout-Einstellung des Benutzers.
CLI	Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: `set system user <name> -timeout <secs>`

- **Timeout auf Benutzergruppenebene.** Gilt für alle Benutzer in der Gruppe.

Interface-Typ	Time-out-Konfiguration
Grafische Benutzeroberfläche (GUI)	Navigieren Sie zu **System > Benutzerverwaltung > Gruppen**, wählen Sie eine Gruppe aus und bearbeiten Sie die Timeout-Einstellung der Gruppe.

Interface-Typ	Time-out-Konfiguration
CLI	Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:`set system group <groupName> -timeout <secs>`

- **Globales System-Timeout.** Gilt für alle Benutzer und Benutzer aus Gruppen, für die kein Timeout konfiguriert ist.

Interface-Typ	Time-out-Konfiguration
Grafische Benutzeroberfläche (GUI)	Navigieren Sie zu **System > Einstellungen**, klicken Sie auf **Globale Systemeinstellungen ändern**, und aktualisieren Sie den Timeoutwert nach Bedarf.
CLI	Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: `set system parameter -timeout <secs>`

Der für einen Benutzer angegebene Timeoutwert hat die höchste Priorität. Wenn für den Benutzer kein Timeout konfiguriert ist, wird das für eine Mitgliedsgruppe konfigurierte Zeitlimit berücksichtigt. Wenn für eine Gruppe kein Timeout angegeben ist (oder der Benutzer keiner Gruppe angehört), wird der global konfigurierte Timeoutwert berücksichtigt. Wenn Timeout auf keiner Ebene konfiguriert ist, wird der Standardwert von 900 Sekunden als Zeitlimit für die Systemsitzung festgelegt.

Darüber hinaus können Sie für jede der Schnittstellen, auf die Sie zugreifen, Timeout-Dauer angeben. Der für eine bestimmte Schnittstelle angegebene Timeoutwert ist jedoch auf den Timeoutwert beschränkt, der für den Benutzer konfiguriert ist, der auf die Schnittstelle zugreift. Betrachten wir zum Beispiel einen Benutzer “publicadmin”, der einen Timeoutwert von 20 Minuten hat. Beim Zugriff auf eine Schnittstelle muss der Benutzer jetzt einen Timeoutwert angeben, der innerhalb von 20 Minuten liegt.

> **Hinweis:**
>
> Sie können die minimalen und maximalen Timeoutwerte überprüfen, indem Sie den Timeout als eingeschränkt angeben (in der CLI durch Angabe des Parameters *restrictedTimeout*). Dieser Parameter wird bereitgestellt, um frühere NetScaler-Versionen zu berücksichtigen, bei denen der Timeoutwert nicht eingeschränkt wurde.

- Wenn diese Option aktiviert ist, beträgt der minimale konfigurierbare Timeoutwert 5 Minuten

(300 Sekunden) und der maximale Wert 1 Tag (86400 Sekunden). Wenn der Timeoutwert bereits auf einen Wert von mehr als 1 Tag konfiguriert ist und dieser Parameter aktiviert ist, werden Sie aufgefordert, ihn zu ändern. Wenn Sie den Wert nicht ändern, wird der Timeoutwert beim nächsten Neustart automatisch auf die Standard-Timeout-Dauer von 15 Minuten (900 Sekunden) neu konfiguriert. Das Gleiche passiert, wenn der konfigurierte Timeoutwert weniger als 5 Minuten beträgt.

- Wenn diese Option deaktiviert ist, werden die konfigurierten Timeout-Dauern berücksichtigt.
- **Timeout-Dauer an jeder Schnittstelle:**

Interface-Typ	Time-out-Konfiguration
CLI	Geben Sie den Timeoutwert an der Eingabeaufforderung mithilfe des folgenden Befehls an: `set cli mode -timeout <secs>`
API	Geben Sie den Timeoutwert in der Login-Nutzlast an.

So stellen Sie Datum und Uhrzeit des Systems ein, um die Uhr mit einem Zeitserver zu synchronisieren

Um das Systemdatum und die Uhrzeit zu ändern, müssen Sie die Shell-Schnittstelle zum zugrunde liegenden FreeBSD-Betriebssystem verwenden. Um jedoch Datum und Uhrzeit des Systems anzuzeigen, können Sie die Befehlszeilenschnittstelle oder die GUI verwenden.

Zeigen Sie Systemdatum und -zeit über die Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

```
1 show ns config
2 <!--NeedCopy-->
```

Anzeigen von Systemdatum und -uhrzeit über die GUI

Navigieren Sie zu **System** und wählen Sie die Registerkarte **Systeminformationen** aus, um das Systemdatum anzuzeigen.

So konfigurieren Sie HTTP- und HTTPS-Management-Ports für interne Dienste

In einer Bereitstellung im Single-IP-Modus einer NetScaler-Appliance wird eine einzelne IP-Adresse als NSIP-, SNIP- und VIP-Adressen verwendet. Diese einzelne IP-Adresse verwendet unterschiedliche Portnummern, um als NSIP-, SNIP- und VIP-Adressen zu fungieren.

Die Portnummern 80 und 443 sind bekannte Ports für HTTP- und HTTPS-Dienste. Früher waren Port 80 und 443 der NetScaler IP-Adresse (NSIP) dedizierte Ports für interne HTTP- und HTTPS-Verwaltungsdienste. Da diese Ports für interne Dienste reserviert waren, können Sie diese bekannten Ports nicht für die Bereitstellung von HTTP- und HTTPS-Datendiensten von einer VIP-Adresse aus verwenden, die dieselbe Adresse wie die NSIP-Adresse in einer Bereitstellung im Einzel-IP-Modus hat.

Um diese Anforderung zu erfüllen, können Sie jetzt Ports für interne HTTP- und HTTPS-Verwaltungsdienste (der NSIP-Adresse) außer Port 80 und 443 konfigurieren.

Im Folgenden sind die Standardportnummern für interne HTTP- und HTTPS-Verwaltungsdienste in NetScaler MPX-, VPX- und CPX-Appliances aufgeführt:

- NetScaler MPX- und VPX-Appliances: 80 (HTTP) und 443 (HTTPS)
- NetScaler CPX-Appliances: 9080 (HTTP) und 9443 (HTTPS)

Konfigurieren von HTTP- und HTTPS-Verwaltungs-Ports mithilfe der Befehlsschnittstelle

Sie können einen HTTP- und einen HTTPS-Port auf einen beliebigen Wert auf der NetScaler-Appliance konfigurieren, um den HTTP- und HTTPS-Verwaltungsdienst zu unterstützen. Standardmäßig verwendet die NetScaler-Appliance jedoch 80 und 443 Ports für die HTTP- und HTTPS-Verbindung.

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns param  - mgmtHttpPort<port>
<!--NeedCopy-->
```

Beispiel:

```
set ns param -mgmtHttpPort 2000
<!--NeedCopy-->
```

So konfigurieren Sie einen HTTPS-Port mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns param  - mgmtHttpsPort<port>
<!--NeedCopy-->
```

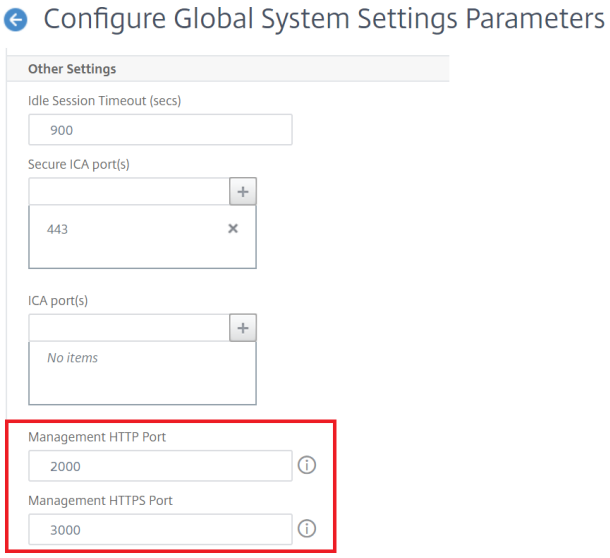
Beispiel:


```
set ns param -mgmtHttpsPort 3000
<!--NeedCopy-->
```

Konfigurieren von HTTP- und HTTPS-Management-Ports über die GUI

Befolgen Sie die unten angegebenen Schritte, um HTTP- und HTTPS-Portwerte zu konfigurieren:

1. Navigieren Sie zu **System** > **Einstellungen** > **Globale Systemeinstellungen ändern**.
2. Legen Sie auf der Seite **Globale Systemeinstellungen konfigurieren** im Abschnitt **Andere** Einstellungen die folgenden Parameter fest.
    a) Management-HTTP-Port. Setzen Sie den Portwert auf 2000. Standardwert = 80, Min = 1, Max = 65534.
    b) Verwaltung HTTPS-Port. Setzen Sie den Portwert auf 3000. Standardwert = 443, Min = 1, Max = 65534.



Konfigurieren Sie den internen HTTP-GUI-Dienst über die NetScaler GUI oder NetScaler CLI oder NetScaler NITRO APIs

Auf einer NetScaler-Appliance ist `/etc/httpd.conf` die Konfigurationsdatei für den internen HTTP-GUI-Dienst, der Verbindungen zur NetScaler GUI verwaltet.

Anstatt die `httpd.conf` Datei für die Konfiguration des internen HTTP-GUI-Dienstes zu verwenden, können Sie jetzt NetScaler GUI, NetScaler CLI oder NetScaler NITRO APIs verwenden. Sie können beispielsweise die NetScaler CLI verwenden, um die maximale Anzahl von Clients zu ändern, die sich gleichzeitig mit dem internen HTTP-GUI-Dienst verbinden können.

Der interne HTTP-GUI-Dienst hat das folgende Namensformat: **nshttpd-gui- -80**<loop back IP address>

Verwenden Sie die NetScaler-Dienstbefehlsoperationen, um den internen HTTP-GUI-Dienst zu konfigurieren.

So ändern Sie den internen HTTP-GUI-Dienst über die CLI:

- Verwenden Sie den Befehl `set service`. Weitere Informationen finden Sie unter Dienst festlegen.
- Verwenden Sie den Befehl `show service`, um die Konfiguration zu überprüfen. Weitere Informationen finden Sie unter Dienst anzeigen.

Beispielkonfiguration:

In der folgenden Beispielkonfiguration ist der Parameter `maxClient` für den internen HTTP-GUI-Dienst auf 300 festgelegt.

```
> sh service nshttpd-gui-127.0.0.1-80
                nshttpd-gui-127.0.0.1-80 (127.0.0.1:80) - HTTP
                State: UP
                Last state change was at Wed Mar 16 20:16:16 2022
                Time since last state change: 0 days, 22:31:00.970
                Server Name: #ns-internal-127.0.0.1#
                Server ID : None                Monitor Threshold : 0
                Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                   kbits
                Use Source IP: NO
                Client Keepalive(CKA): NO
                Monitoring Owner: 0
                Access Down Service: NO
                TCP Buffering(TCPB): NO
                HTTP Compression(CMP): NO
                Idle timeout: Client: 180 sec        Server: 360 sec
                Client IP: ENABLED cip-header
                Cacheable: NO
                SC: ???
                SP: OFF
                Down state flush: DISABLED
                Monitor Connection Close : NONE
                Appflow logging: DISABLED
                TCP profile name: nstcp_internal_apps
                HTTP profile name: nshttp_default_internal_apps
                Process Local: DISABLED
                Traffic Domain: 0

Done
```



```
29
30 > set service nshttpd-gui-127.0.0.1-80 -maxclient 300
31 Done
32
33 > sh service nshttpd-gui-127.0.0.1-80
34                 nshttpd-gui-127.0.0.1-80 (127.0.0.1:80) - HTTP
35                 State: UP
36
37                 ...
38
39                 Max Conn: 300  Max Req: 0          Max Bandwidth: 0
                       kbits
40
41                 ...
42
43 Done
44
45 <!--NeedCopy-->
```

Auslösen der Speicherwiederherstellung mithilfe der Befehlsschnittstelle

Sie können die Speicherwiederherstellung über die Befehlszeilenschnittstelle auslösen.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
start ns memrecovery [-percentage <positive_integer>]
```

Beispiel:

```
start nsmemrecovery -percentage 30
```

Verwenden Sie den folgenden Befehl an der Eingabeaufforderung, um die tatsächlich wiederhergestellte Speichermenge zu überprüfen:

```
stat system memory
```

So weisen Sie zusätzliche Management-CPU für die Datenverarbeitung und -überwachung zu

Wenn Sie eine bessere Leistung für die Konfiguration und Überwachung einer NetScaler MPX-Appliance benötigen, können Sie eine zusätzliche Verwaltungs-CPU aus dem Paket-Engine-Pool der Appliance zuweisen. Diese Funktion wird bei bestimmten NetScaler MPX-Modellen und allen VPX-Modellen mit Ausnahme der VPX-Instanzen unterstützt, die auf NetScaler SDX-Appliances ausgeführt werden. Dies wirkt sich auf die Ausgabe der CPU- und Stat-Systembefehle des Statistiksystems aus.

Unterstützte NetScaler MPX-Modelle:

- 25xxx
- 22xxx
- 14xxx
- 115xx
- 15xxx
- 26xxx

> **Hinweis:**
>
> Für NetScaler MPX 26xxx Modelle mit mehr als 20 Kernen ist die obligatorische zusätzliche Management-CPU-Funktion standardmäßig aktiviert. Für NetScaler VPX-Modelle ist eine Lizenz erforderlich, die mindestens 12 vCPUs unterstützt, um diese Funktion zu aktivieren.

Weisen Sie eine zusätzliche Verwaltungs-CPU mit der Befehlszeilenschnittstelle zu

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `enable extramgmtcpu`
- `disable extramgmtcpu`

> **Hinweis:**
>
> Nachdem Sie diese Funktion aktiviert und deaktiviert haben, zeigt die NetScaler-Appliance eine Warnung an, um die Appliance neu zu starten, damit die Änderungen wirksam werden.

Um den konfigurierten und effektiven Status einer zusätzlichen Management-CPU anzuzeigen.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 show extramgmtcpu
2 <!--NeedCopy-->
```

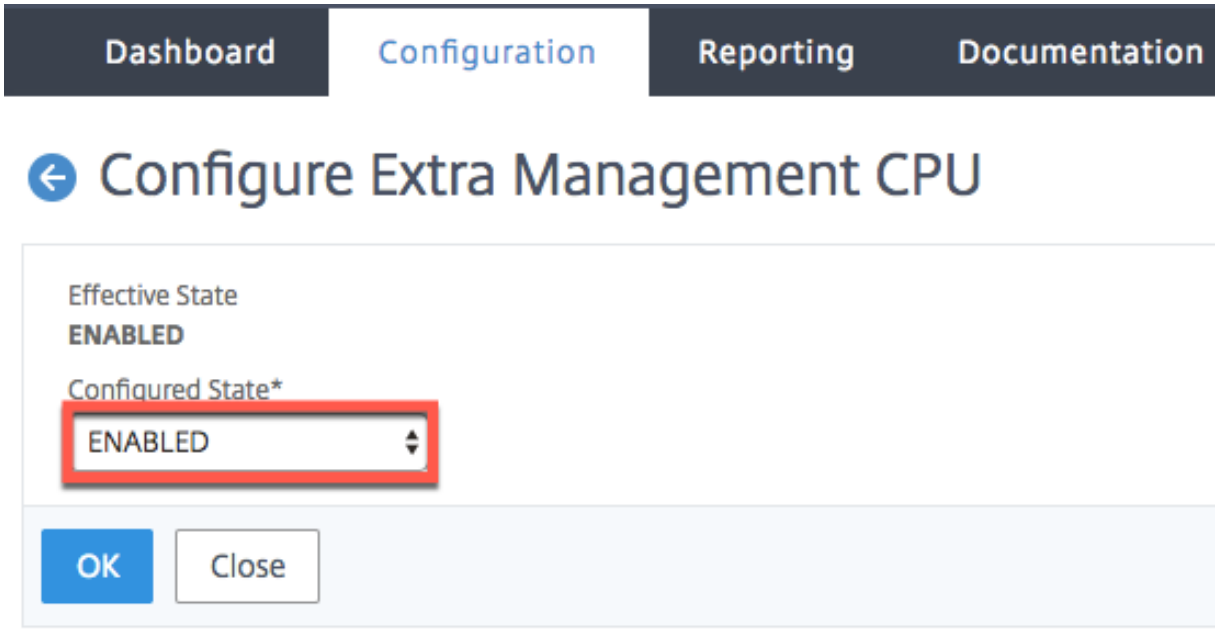
Beispiel:

```
1 > show extramgmtcpu
2 ConfiguredState:  ENABLED EffectiveState:  ENABLED
3 <!--NeedCopy-->
```

> **Hinweis:**
>
> In diesem Beispiel wird der Befehl show vor dem Neustart der Appliance eingegeben.

Weisen Sie über die GUI eine zusätzliche Management-CPU zu

Um über die GUI eine zusätzliche Management-CPU zuzuweisen, navigieren Sie zu **System** > **Einstellungen** und klicken Sie auf **Zusätzliche Management-CPU konfigurieren**. Wählen Sie im Dropdown-Menü **Konfigurierter Status** die Option **Aktiviert** aus und wählen Sie dann **OK**aus.



Um die CPU-Auslastung zu überprüfen, gehen Sie zu **System** > **Einstellungen** > **Dashboard**.

Konfigurieren Sie eine zusätzliche Management-CPU mithilfe der NITRO-API

Verwenden Sie die folgenden NITRO-Methoden und -Formate, um eine zusätzliche Verwaltungs-CPU zu aktivieren, zu deaktivieren und anzuzeigen.

So aktivieren Sie eine zusätzliche Management-CPU:

```
HTTP Method: POST

URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=enable

Payload: {
 "systemextramgmtcpu":{
  }
  }


curl -v -X POST -H "Content-Type: application/json" -u nsroot:nsroot
    http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=
    enable -d '{
 "systemextramgmtcpu":{
  }
  }
 '
<!--NeedCopy-->
```


Deaktivieren einer zusätzlichen Management-CPU

```
HTTP Method: POST
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=disable
Payload: {
 "systemextramgmtcpu":{
  }
  }

curl -v -X POST -H "Content-Type: application/json" -u nsroot:nsroot
   http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=
   disable -d '{
 "systemextramgmtcpu":{
  }
  }
 '
<!--NeedCopy-->
```

So zeigen Sie eine zusätzliche Verwaltungs-CPU an

```
HTTP Method: GET
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu
<!--NeedCopy-->
```

Beispiel:

```
curl -v -X GET -H "Content-Type: application/json" -u nsroot:nsroot
   http://10.102.201.92/nitro/v1/config/systemextramgmtcpu
<!--NeedCopy-->
```

Statistik und Überwachung vor und nach dem Hinzufügen zusätzlicher Management-CPU

Die folgenden Beispiele zeigen die Unterschiede in der Ausgabe der CPU- und Stat-Systembefehle des Statistiksystems vor und nach dem Hinzufügen einer zusätzlichen Management-CPU.

```
stat system cpu
<!--NeedCopy-->
```

Dieser Befehl zeigt Statistiken von CPUs an.

Hier ist eine Beispielausgabe, bevor eine zusätzliche Management-CPU für eines der unterstützten Modelle hinzugefügt wird.

Beispiel


```
> stat system cpu

    CPU statistics

    ID         Usage

    8              1

    7              1

    11             2

    1              1

    6              1

    9              1

    3              1

    5              1

    4              1

    10             1

    2              1
<!--NeedCopy-->
```

Hier ist die Ausgabe nach dem Hinzufügen einer zusätzlichen Verwaltungs-CPU auf derselben MPX-Appliance.

```
    > stat system cpu

    CPU statistics

    ID         Usage

    9              1

    7              1

    5              1

```



```
13      8               1
14
15      11              2
16
17      10              1
18
19      6               1
20
21      4               1
22
23      3               1
24
25      2               1
26  <!--NeedCopy-->
```

```
1  stat system
2  <!--NeedCopy-->
```

Dieser Befehl zeigt die CPU-Nutzung an. Im folgenden Beispiel lautet die Ausgabe vor dem Hinzufügen einer zusätzlichen Verwaltungs-CPU für eines der unterstützten Modelle:

Mgmt zusätzliche CPU-Auslastung (%) 0.00

Beispiel

```
1       > stat system
2
3       NetScaler Executive View
4
5       System Information:
6
7       Up since         Wed Oct 11 11:17:54 2017
8
9       /flash Used (%)                          0
10
11      Packet CPU usage (%)                 1.30
12
13      Management CPU usage (%)             4.00
14
15      Mgmt CPU0 usage (%)                  4.00
16
17      Mgmt Additional-CPU  usage (%)       0.00
18
19      Memory usage (MB)                    2167
20
```



```
    InUse Memory (%)                       5.76

    /var Used (%)                             0
<!--NeedCopy-->
```

Im folgenden Beispiel lautet die Ausgabe nach dem Hinzufügen einer zusätzlichen Verwaltungs-CPU auf derselben MPX-Appliance:

Mgmt zusätzliche CPU-Auslastung (%) 0.80

```
> stat system


NetScaler Executive View

System Information:

Up since        Wed Oct 11 11:55:56 2017

/flash Used (%)                           0

Packet CPU usage (%)                   1.20

Management CPU usage (%)               5.70

Mgmt CPU0 usage (%)                   10.60

Mgmt Additional-CPU  usage (%)         0.80

Memory usage (MB)                      1970

InUse Memory (%)                       5.75

/var Used (%)                             0

<!--NeedCopy-->
```

Backup und Wiederherstellen der Appliance, um verlorene Konfigurationen wiederherzustellen

Wenn Ihre Appliance beschädigt wird oder ein Upgrade benötigt, können Sie Ihre Systemkonfiguration sichern. Das Backup-Verfahren wird entweder über die CLI- oder die GUI-Schnittstelle durchgeführt. Mit der Appliance können Sie auch die Backupdatei von einer externen Quelle importieren. Sie

können dies jedoch nur über die GUI-Schnittstelle tun und es gibt keine Unterstützung über die CLI-Schnittstelle.

Wichtige Punkte

Sie müssen sich an die folgenden Punkte erinnern, wenn Sie Ihre Appliance Backup und wiederherstellen.

- Es muss eine Unterstützung für die Netzwerkkonfiguration auf einer neuen Plattform geben.
- Der neue Plattform-Build muss mit der Backupdatei oder einer späteren Version identisch sein.

Sichern einer NetScaler-Appliance

Abhängig von den Daten- und Sicherungsanforderungen können Sie ein “einfaches” Backup oder ein “vollständiges” Backup erstellen.

- **Grundlegende Backup.** Sie können diese Art der Backup durchführen, wenn Sie Dateien sichern möchten, die sich ständig ändern. Die Dateien, die Sie sichern können, finden Sie in der folgenden Tabelle.

Informationen zu den grundlegenden Backup-Details finden Sie im Thema Tabelle .

- **Vollständiges Backup.** Zusätzlich zu den Dateien, die durch eine Basissicherung gesichert werden, enthält eine vollständige Backup seltener aktualisierte Dateien. Die Dateien, die gesichert werden, wenn Sie die “vollständige” Backupoption verwenden, sind:

Verzeichnis	Unterverzeichnis oder Dateien
nsconfig	ssl*, license*, fips*
/var/	netscaler/ssl/*, wi/java_home/jre/lib/security/cacerts/*, wi/java_home/lib/security/cacerts/*

Die Backupdaten werden als komprimierte TAR-Datei im Verzeichnis `/var/ns_sys_backup/` gespeichert. Um Probleme aufgrund der Nichtverfügbarkeit von Speicherplatz zu vermeiden, können Sie bis zu 50 Backupdateien in diesem Verzeichnis speichern. Mit dem Befehl `rm system backup` können Sie vorhandene Backupdateien löschen und weitere Backups erstellen.

> **Hinweis:**
>
> Führen Sie bei laufendem Backupvorgang keine Befehle aus, die sich auf die Konfiguration auswirken.

> Wenn eine Datei, die gesichert werden muss, nicht verfügbar ist, überspringt der Vorgang diese Datei.

Sichern einer NetScaler-Appliance über die Befehlszeilenschnittstelle

Befolgen Sie die nachstehenden Schritte, um eine NetScaler-Appliance mithilfe der NetScaler-Befehlszeilenschnittstelle zu sichern.

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Speichern Sie die NetScaler-Konfigurationen.

```
save ns config
<!--NeedCopy-->
```

1. Erstellen Sie die Backupdatei.

```
create system backup [<fileName>] -level <basic | full> -comment <
   string>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn der Dateiname nicht angegeben wird, erstellt die Appliance eine TAR-Datei mit der folgenden Namenskonvention:`backup_<level>_<nsip_address>_<date-timestamp>.tgz`.

Beispiel: Sichern der vollständigen Appliance mithilfe der Standardbenennungskonvention für die Backupdatei.

```
> create system backup -level full
<!--NeedCopy-->
```

1. Stellen Sie sicher, dass die Backupdatei erstellt wurde.

```
show system backup
<!--NeedCopy-->
```

Mithilfe des Parameters `fileName` können Sie die Eigenschaften einer bestimmten Backupdatei anzeigen.

Wiederherstellen einer NetScaler-Appliance mit der Befehlszeilenschnittstelle

> **Wichtig:**

> Sie können Ihre Appliance nicht erfolgreich wiederherstellen, wenn Sie Ihre Backupdatei umbenennen oder ändern.

Wenn Sie Ihre Appliance wiederherstellen, entfernt der Wiederherstellungsvorgang die Backupdatei aus dem Verzeichnis `/var/ns_sys_backup/`. Sobald die Dateien entkomprimiert sind, werden die Dateien in die jeweiligen Verzeichnisse kopiert.

Stellen Sie den NetScaler aus einer lokalen Backupdatei über die Befehlszeile wieder her

> **Hinweis:**
>
> Citrix empfiehlt Ihnen, die aktuelle Konfiguration zu sichern, bevor Sie eine vorherige Konfiguration wiederherstellen. Wenn Sie jedoch nicht möchten, dass der Wiederherstellungsbefehl automatisch ein Backup der aktuellen Konfiguration erstellt, verwenden Sie den Parameter `-skipBackup`.

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Rufen Sie eine Liste der auf der Appliance verfügbaren Backupdateien ab.

```
1 show system backup
2 <!--NeedCopy-->
```

2. Stellen Sie die Appliance wieder her, indem Sie eine der Backupdateien angeben.

   `restore system backup <filename> [-skipBackup]`

   Beispiel: Wiederherstellen mit einem vollständigen Backup einer Appliance

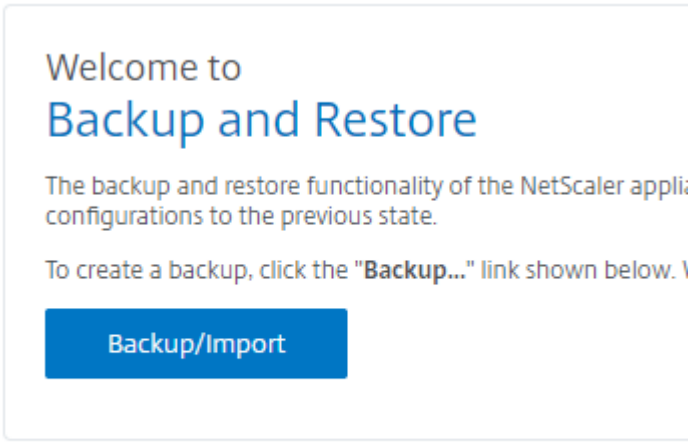
   `> restore system backup backup_full_<nsip_address>_<date-timestamp>.tgz`

3. Starten Sie die Appliance neu.

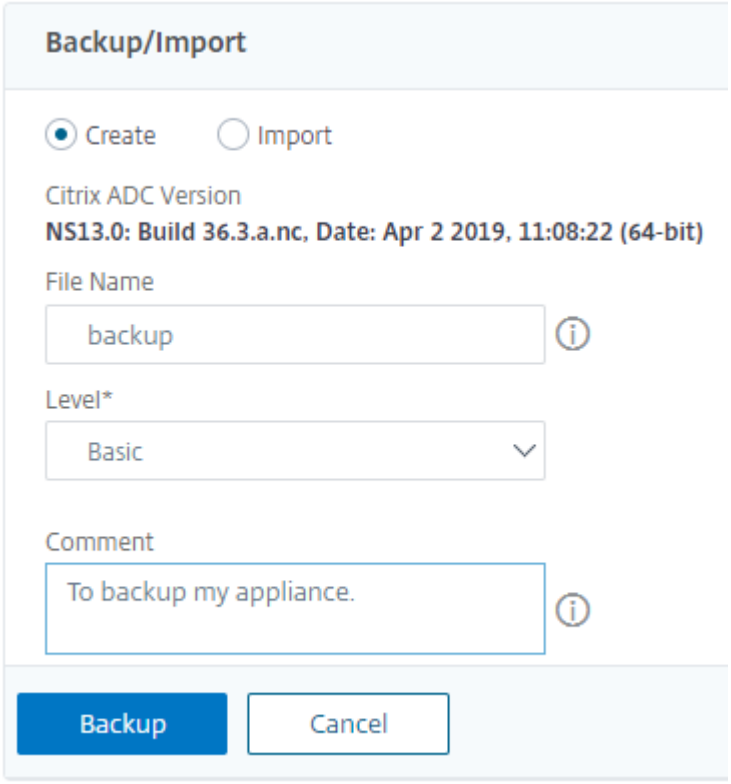
   `reboot`

Backup und Wiederherstellen einer NetScaler-Appliance über die GUI

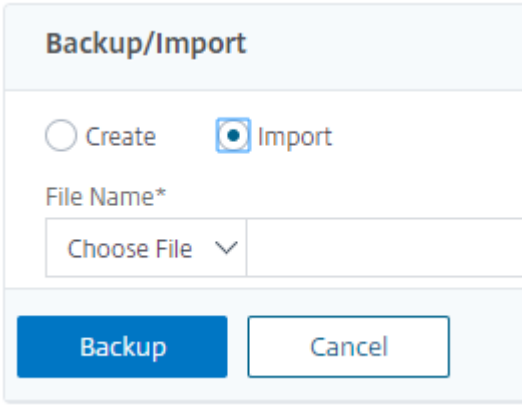
1. Navigieren Sie zu **System** > **Sichern und Wiederherstellen**.



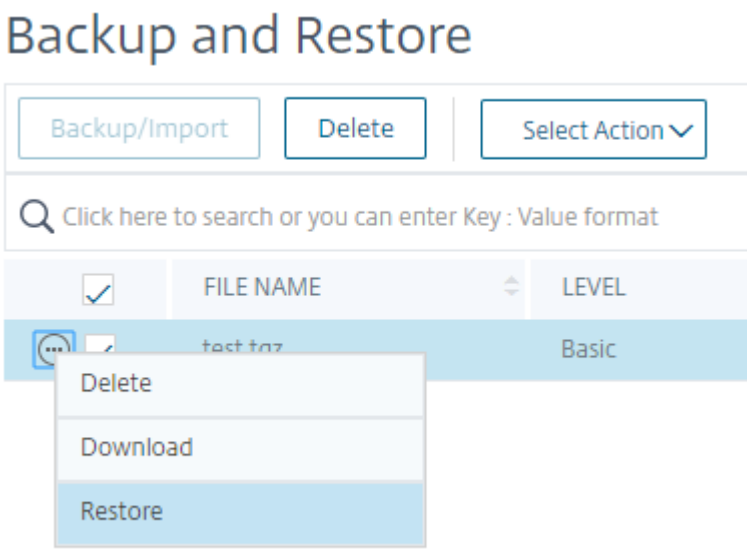
2. Klicken Sie auf **Backup/Import**, um den Vorgang zu starten.
3. Wählen Sie auf der Seite **Backup/Import** die Option **Erstellen** aus und legen Sie die folgenden Parameter fest.
    a) Dateiname. Name der Appliance-Backup-Datei.
    b) Niveau. Wählen Sie ein Backup-Level als Basic oder Full.
    c) Kommentar. Geben Sie eine kurze Beschreibung für das Backup an.
4. Klicken Sie auf **Backup**.



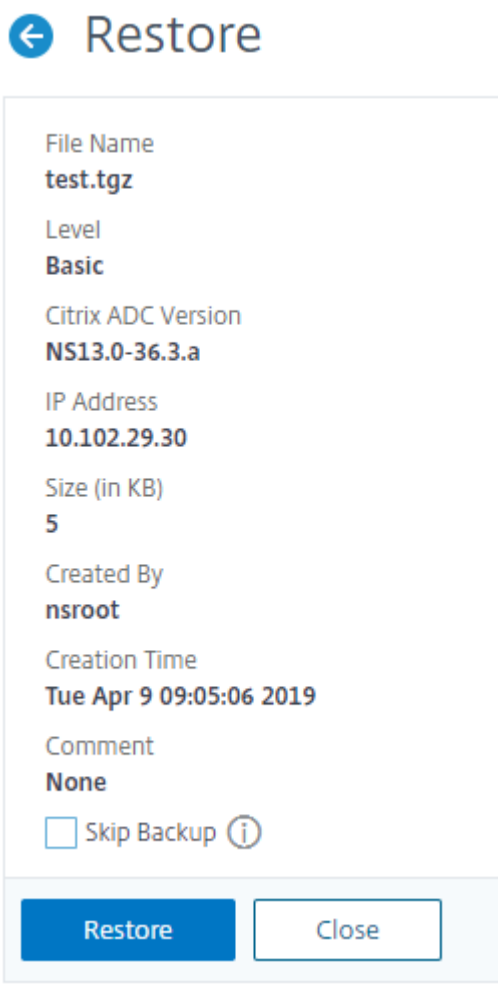
5. Wenn Sie ein Backup importieren möchten, müssen Sie **Importieren** auswählen.



6. Sobald die Backup abgeschlossen ist, können Sie die Datei auswählen und auf **Herunterladen** klicken.
7. Zum Wiederherstellen wählen Sie die Backupdatei aus und klicken Sie auf **Wiederherstellen**.



8. Überprüfen Sie auf der Seite **Wiederherstellen** die Details der Backupdatei und klicken Sie auf **Wiederherstellen**.



9. Nach dem Wiederherstellen müssen Sie die Appliance neu starten.

Weitere Informationen zum Backup und Wiederherstellen von NetScaler-Instanzen finden Sie unter Backup und Wiederherstellen mit NetScaler ADM.

Weitere Informationen zum Backup und Wiederherstellen einer SDX-Appliance finden Sie unter Sichern und Wiederherstellen der SDX-Appliance

Informationen zu Vorgängen, die bei dem Systembackup ausgeführt werden, finden Sie unter Systembackup.

So erstellen Sie ein Paket für den technischen Support zur Lösung von Appliance-Problemen

Wenn Sie Hilfe bei der Analyse und Lösung von Problemen mit einer NetScaler-Appliance benötigen, können Sie auf der Appliance ein Paket für technischen Support erstellen und das Paket an den technischen Support von Citrix senden. Das Paket für den technischen Support von NetScaler ist

ein gezipptes TAR-Archiv mit Systemkonfigurationsdaten und -statistiken. Es sammelt die folgenden Daten von der NetScaler-Appliance, auf der Sie das Bundle generieren:

- **Konfigurationsdateien**. Alle Dateien im Verzeichnis /flash/nsconfig.
- **Newslog-Dateien**. Der aktuell laufende newnslog und einige vorherige Dateien. Um die Größe der Archivdatei zu minimieren, ist die Sammlung `newnslog` auf 500 MB, 6 Dateien oder 7 Tage beschränkt, je nachdem, was zuerst eintritt. Wenn ältere Daten benötigt werden, ist möglicherweise eine manuelle Erfassung erforderlich.
- **Protokolldateien**. Dateien in /var/log/messages , */var/log/ns.log* und anderen Dateien unter /var/log und /var/nslog.
- **Anwendungs-Kerndateien**. Dateien, die in der letzten Woche im Verzeichnis /var/core erstellt wurden, falls vorhanden.
- **Ausgabe einiger CLI-Show-Befehle**.
- **Ausgabe einiger CLI-Statbefehle**.
- **Ausgabe von BSD-Shell-Befehlen**.

Sie können einen einzigen Befehl verwenden, um das Paket für den technischen Support zu generieren und es sicher auf den Server für den technischen Support von Citrix hochzuladen. Zum Hochladen müssen Sie Ihre Citrix Anmeldeinformationen angeben. Wenn Sie das Paket generieren, können Sie die Fall- oder Serviceanforderungsnummer angeben, die Ihnen vom technischen Support von Citrix zugewiesen wurde. Wenn Sie bereits ein Paket für technischen Support generiert haben, können Sie die vorhandene Archivdatei auf den Citrix Technical Support Server hochladen, indem Sie den Dateinamen mit dem vollständigen Pfad angeben.

Das technische Support-Paket wird auf der NetScaler-Appliance in einem Archiv an folgendem Speicherort gespeichert:

```
/var/tmp/support/support.tgz
<!--NeedCopy-->
```

Der Pfad ist ein Symlink zum neuesten Collector für einfachen Zugriff. Der vollständige Dateiname variiert je nach Bereitstellungstopologie, folgt jedoch im Allgemeinen einem ähnlichen Format wie:

```
collector_<P/S>\_<NS IP>\_<DateTime>.tgz.
<!--NeedCopy-->
```

Wenn Ihre NetScaler-Appliance keine direkte Internetverbindung hat, können Sie einen Proxyserver verwenden, um das technische Supportpaket direkt auf den Citrix Technical Support Server hochzuladen. Das Grundformat der Proxy-Zeichenfolge lautet:

```
proxy_IP:<proxy_port>
<!--NeedCopy-->
```

Wenn der Proxyserver eine Authentifizierung erfordert, lautet das Format:


```
username:password@proxsy_IP:<proxy_port>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für NetScaler-Appliances in einem Hochverfügbarkeitspaar müssen Sie das technische Support-Paket auf jedem der beiden Knoten generieren.
>
> Für NetScaler-Appliances in einem Clustersetup können Sie das technische Support-Paket auf jedem Knoten einzeln generieren oder mithilfe der Cluster-IP-Adresse kleinere abgekürzte Archive für alle Knoten generieren.
>
> Für NetScaler-Administratorpartitionen müssen Sie das technische Support-Paket aus der Standard-Admin-Partition generieren. Um das technische Support-Paket für eine bestimmte Partition zu erhalten, müssen Sie den Namen der Partition angeben, für die Sie das technische Support-Paket generieren möchten. Wenn Sie den Namen der Partition nicht angeben, werden Daten aus allen Adminpartitionen gesammelt.

Generieren Sie das Paket für technischen Support von NetScaler über die Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
show techsupport [-scope <scope> <partitionName>] [-upload [-proxy <
    string>] [-casenumber <string>] [-file <string>] [-description <
    string>] [-userName <string> -password ]]
<!--NeedCopy-->
```

Sr. Nein	Aufgabe	Befehl
1	Generieren Sie das Paket für technischen Support und laden Sie es auf den Citrix Server für technischen Support hoch.	show techsupport –upload –userName account1 –password xxxxxxx
2	Generieren Sie das Paket für technischen Support und laden Sie es über einen Proxyserver auf den Citrix Server für technischen Support hoch	show techsupport –upload –proxy 1.1.1.1:80 –userName account1 –password xxxxxxx

Sr. Nein	Aufgabe	Befehl
3	Laden Sie ein vorhandenes Paket für technischen Support auf den Citrix Server für technischen Support hoch.	show techsupport –upload -file,/var/tmp/support/collector_P_10.102.29. –userName account1 –password xxxxxxx
4	Generieren Sie kleine, abgekürzte Archive für alle Knoten in einem Clustersetup. Führen Sie diesen Befehl mit der Cluster-IP-Adresse aus	show techsupport –scope CLUSTER
5	Generieren Sie ein technisches Support-Paket für eine Admin-Partition. Führen Sie diesen Befehl auf der Standard-Admin-Partition aus.	show techsupport –scope PARTITION partition1

So sammeln Sie das technische Support-Paket von SDX- und VPX-Appliances für die Insight-Analyse

Eine NetScaler-Appliance verfügt über einen integrierten Mechanismus zum Sammeln von Protokolldateien. Die Protokolldateien werden wiederum zur Analyse an Citrix Insight Services gesendet.

> **Hinweis:**
>
> Alle Verfahren gelten für die Softwareversion 9.2 oder höher.

Laden Sie das technische Support-Paket von NetScaler MPX- und VPX-Appliances herunter

Um eine Collector-Datei über die NetScaler GUI auszuführen, müssen Sie das folgende Verfahren ausführen:

> **Hinweis:**
>
> Das Verfahren ist für Softwareversion 9.2 oder höher anwendbar.

1. Navigieren Sie zu **System** > **Diagnose**.
2. Klicken Sie im Abschnitt **Tools für den Technischen Support** auf den Link **Support-Datei generieren** .

3. Stellen Sie auf der Seite **Tech Support** die folgenden Parameter ein:
   a) Scope. Um Daten von einem oder mehreren Knoten zu sammeln.
   b) Partition. Name der Partition.
   c) Ladeoptionen für den technischen Support von Citrix. Stellen Sie alle Optionen wie Proxyserver, Servicefallnummer, Collector-Archivdateiname und eine kurze Beschreibung der Archivdatei zum Hochladen des technischen Support-Pakets ein.
   d) Citrix Konto. Geben Sie Ihre Citrix Anmeldeinformationen ein.
4. Klicken Sie auf **Ausführen**.
5. Das technische Support-Paket wird generiert.
6. Klicken Sie auf **Ja**, um das Technical Support Bundle auf Ihren lokalen Desktop herunterzuladen.

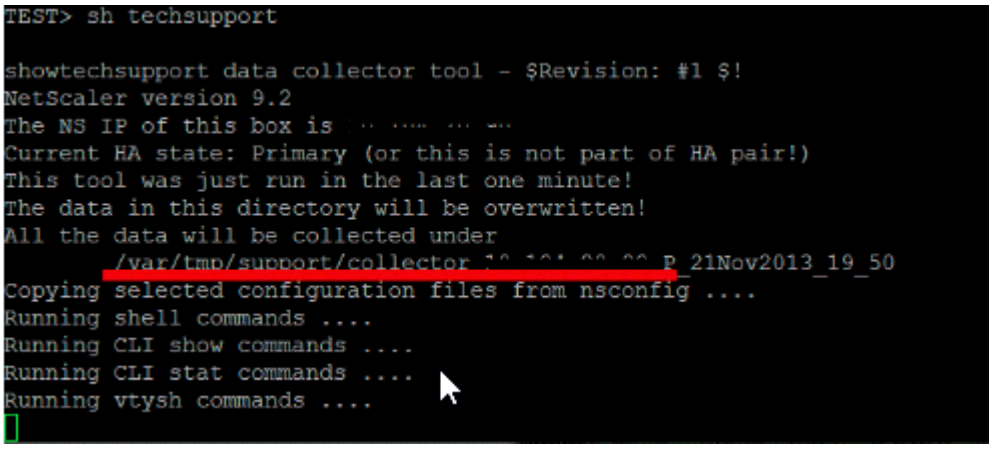
Beziehen Sie das technische Support-Paket über die Befehlszeilenschnittstelle

1. Laden Sie die Datei mit einem Dienstprogramm Secure FTP (SFTP) oder Secure Copy (SCP) von der Appliance herunter, z. B. `WinSCP`, und laden Sie sie zur Analyse in Citrix Insight Services hoch.

> **Hinweis:**
>
> In der NetScaler-Softwareversion vor 9.0 muss das Collector-Skript separat heruntergeladen und ausgeführt werden.

```
1 > show techsupport -scope CLUSTER
2 <!--NeedCopy-->
```

1. Dadurch werden Informationen zum technischen Support von allen Knoten im Cluster gesammelt und die Dateien in einem einzigen Archiv komprimiert.
2. Nachdem die Appliance das Collector-Archiv generiert hat, wird der Speicherort der Datei angezeigt, wie im folgenden Screenshot gezeigt.



Die Datei wird in `/var/tmp/support` gespeichert und Sie können sie überprüfen, indem Sie sich bei einer NetScaler-Appliance anmelden und den folgenden Befehl über eine Shell-Eingabeaufforderung ausführen.

```
root@NS# cd /var/tmp/support/
root@NS# ls -l
<!--NeedCopy-->
```

Beziehen Sie das Diagnose-Paket von NetScaler SDX über die GUI

1. Öffnen Sie die NetScaler SDX-GUI.
2. Erweitern Sie den Knoten **Diagnose** .
3. Wählen Sie den Knoten **Technischer Support** .
4. Klicken Sie auf Technical Support Datei generieren.
5. Wählen Sie im Dropdown-Menü **Appliance** (einschließlich Instanzen) aus.
6. Klicken Sie auf **Hinzufügen**.
7. Wählen Sie eine oder mehrere Instanzen aus, die hinzugefügt werden sollen.
8. Klicken Sie auf **OK**. Warten Sie, bis der Vorgang abgeschlossen ist.
9. Wählen Sie den generierten Bundlenamen aus, und klicken Sie dann auf **Herunterladen**.
10. Laden Sie die Paketdatei in Citrix Insight Serviceshoch.

Weitere Ressourcen

Sehen Sie sich ein Video an

Lies ein anderes Thema

Befehlsreferenzdokument

Vereinheitlichte Konfigurationsdatei für die NetScaler Appliance

September 1, 2023

Die NetScaler Appliance unterstützt eine einheitliche Konfigurationsdatei (`unified.conf`), die die NetScaler-Konfigurationen (`ns.conf`), dynamischen Routing-Konfigurationen (`zebos.conf`) und die Hardware Security Module (HSM) -Konfigurationen () enthält.`chrystoki.conf`

Die vereinheitlichte Konfigurationsdatei bietet eine einzige Ansicht verschiedener Konfigurationstypen. Diese vereinheitlichte Konfigurationsdatei dient nur zu Anzeigezwecken und kann nicht zum Anwenden der Konfigurationen in einer anderen NetScaler-Appliance verwendet werden.

Der vollständige Pfad der einheitlichen Konfigurationsdatei in der NetScaler Appliance lautet:.

/nsconfig/unified.conf Sie können über die Shell-Befehlszeile auf die vereinheitlichte Konfigurationsdatei zugreifen. Die vereinheitlichte Konfigurationsdatei wird nur für eigenständige NetScaler-Appliances und Hochverfügbarkeits-Setups unterstützt.

Beim Speichern einer NetScaler-Konfiguration oder einer dynamischen Routing-Konfiguration wird die Konfiguration zusammen mit dem Speichern in der NetScaler-Konfigurationsdatei (ns.conf) oder der dynamischen Routing-Konfigurationsdatei () auch automatisch in der einheitlichen Konfigurationsdatei gespeichert. zebos.conf

Beim Speichern einer HSM-Konfiguration (Hardware Security Module) wird die Konfiguration nicht automatisch in der einheitlichen Konfigurationsdatei gespeichert. Sie müssen den saveconfig Vorgang ausführen, der die HSM-Konfigurationsdatei (chrystoki.conf) mit der einheitlichen Konfigurationsdatei synchronisiert.

Beispielausgabe

Im folgenden Auszug einer einheitlichen Beispielkonfigurationsdatei (unified.conf) werden zuerst die NetScaler-Konfigurationen aufgeführt, gefolgt von den dynamischen Konfigurationen in der Überschrift **»> VTYSH START CONFIG »**, gefolgt von den Hardware Security Module (HSM) -Konfigurationen, die in der Überschrift **»> START OF HSM CONFIG »**aufgeführt sind.

```
#NS14.1 Build 4.42

enable ns feature WL LB OSPF BGP IPv6PT RESPONDER
enable ns mode FR L3 Edge USNIP PMTUD
...
...
...


>>> VTYSH START CONFIG >>>

!
log syslog
log record-priority
!
interface lo0

...
...
...

!
router bgp 100
```



```
neighbor 4000::1 remote-as 100
no neighbor 4000::1 activate
!
address-family ipv6
redistribute kernel
neighbor 4000::1 activate
exit-address-family
!
end
>>> VTYSH END CONFIG >>>

>>> START OF HSM CONFIG >>>

Chrystoki2 = {

LibUNIX64 = /var/safenet/safenet/lunaclient/lib/libCryptoki2_64.so;
 }


...
...
...

CardReader = {

RemoteCommand = 1;
 }

Misc = {

PE1746Enabled = 0;
ToolsDir = /var/safenet/safenet/lunaclient/bin;
 }

...
...
...

<!--NeedCopy-->
```


Authentifizierung und Autorisierung von Systembenutzern

May 11, 2023

Um die NetScaler-Benutzerauthentifizierung und -Autorisierung zu konfigurieren, müssen Sie zunächst die Benutzer definieren, die Zugriff auf die NetScaler-Appliance haben, und dann können Sie diese Benutzer in Gruppen organisieren. Nach der Konfiguration von Benutzern und Gruppen müssen Sie Befehlsrichtlinien konfigurieren, um Zugriffstypen zu definieren, und die Richtlinien Benutzern und/oder Gruppen zuweisen.

Sie müssen sich als Administrator anmelden, um Benutzer, Gruppen und Befehlsrichtlinien zu konfigurieren. *Der standardmäßige NetScaler-Administratorbenutzername lautet nsroot.* Nachdem Sie sich als Standardadministrator angemeldet haben, sollten Sie das Passwort für das nsroot-Konto ändern. Sobald Sie das Passwort geändert haben, kann kein Benutzer auf die NetScaler-Appliance zugreifen, bis Sie ein Konto für diesen Benutzer erstellt haben. Wenn Sie das Administratorkennwort vergessen, nachdem Sie es von der Standardeinstellung geändert haben, können Sie es auf nsroot zurücksetzen.

> **Hinweis:**
>
> - Lokale Benutzer können sich beim NetScaler authentifizieren, auch wenn externe Authentifizierungsserver konfiguriert sind. Sie können dies einschränken, indem Sie den LocalAuth-Parameter des Befehls set system parameter deaktivieren.
> - Zur Erhöhung der Sicherheit empfiehlt Citrix, das nsroot-Passwort zu ändern. Häufig ist es ratsam, das Kennwort zu ändern. Informationen zum Ändern des nsroot-Kennworts finden Sie unter Zurücksetzen des Kennworts des Standardadministrators (nsroot) .

Benutzer-, Benutzergruppen- und Befehlsrichtlinien

May 11, 2023

Sie müssen zuerst einen Benutzer mit einem Konto definieren und dann alle Benutzer in Gruppen organisieren. Sie können Befehlsrichtlinien erstellen oder integrierte Befehlsrichtlinien verwenden, um den Benutzerzugriff auf Befehle zu regulieren.

> **Hinweis:**
>
> Wenn Sie mehr über das Konfigurieren von Benutzer- und Benutzergruppen im Rahmen des NetScaler-Authentifizierungs- und Autorisierungs-Setups für das Verkehrsmanagement erfahren möchten, lesen Sie Konfigurieren von Benutzern und Gruppen.

Sie können auch die Eingabeaufforderung für einen Benutzer anpassen. Eingabeaufforderungen können in der Konfiguration eines Benutzers, in einer Benutzergruppenkonfiguration und in den globalen

Systemkonfigurationseinstellungen definiert werden. Die für einen Benutzer angezeigte Eingabeaufforderung hat die folgende Rangfolge:

1. Zeigt die Eingabeaufforderung an, wie sie in der Benutzerkonfiguration definiert ist.
2. Zeigt die Eingabeaufforderung an, wie sie in der Gruppenkonfiguration für die Benutzergruppe definiert ist.
3. Zeigt die Eingabeaufforderung an, wie sie in den globalen Systemkonfigurationseinstellungen definiert ist.

Sie können jetzt einen Timeout-Wert für inaktive CLI-Sitzungen für einen Systembenutzer angeben. Wenn die CLI-Sitzung eines Benutzers für eine Zeit inaktiv ist, die den Timeout-Wert überschreitet, beendet die NetScaler-Appliance die Verbindung. Das Timeout kann in einer Benutzerkonfiguration, in einer Benutzergruppenkonfiguration oder in den globalen Systemkonfigurationseinstellungen definiert werden. Das Timeout für inaktive CLI-Sitzungen für einen Benutzer wird in der folgenden Rangfolge festgelegt:

1. Benutzerkonfiguration:
2. Gruppenkonfiguration für die Benutzergruppe.
3. Globale Systemkonfigurationseinstellungen.

Ein NetScaler-Root-Administrator kann das maximale Limit für gleichzeitige Sitzungen für Systembenutzer konfigurieren. Indem Sie das Limit einschränken, können Sie die Anzahl der offenen Verbindungen reduzieren und die Serverleistung verbessern. Solange die CLI-Anzahl innerhalb des konfigurierten Grenzwerts liegt, können sich gleichzeitige Benutzer beliebig oft an der GUI anmelden. Wenn die Anzahl der CLI-Sitzungen jedoch das konfigurierte Limit erreicht, können sich Benutzer nicht mehr an der GUI anmelden. Wenn die Anzahl der gleichzeitigen Sitzungen beispielsweise auf 20 konfiguriert ist, können sich gleichzeitige Benutzer an 19 CLI-Sitzungen anmelden. Wenn der Benutzer jedoch an der `20<sup>th</sup>` CLI-Sitzung angemeldet ist, führt jeder Versuch, sich an der GUI, CLI oder NITRO anzumelden, zu einer Fehlermeldung ((FEHLER: Verbindungslimit zu CFE überschritten).

> **Hinweis:**
>
> In der Standardeinstellung ist die Anzahl der gleichzeitigen Sitzungen auf 20 und die maximale Anzahl gleichzeitiger Sitzungen auf 40 konfiguriert.

Konfigurieren von Benutzerkonten

Um Benutzerkonten zu konfigurieren, geben Sie einfach Benutzernamen und Kennwörter an. Sie können Kennwörter jederzeit ändern und Benutzerkonten entfernen.

> **Hinweis:**
>
> Alle Zeichen in einem Kennwort werden nicht akzeptiert. Es funktioniert jedoch, wenn Sie die Zeichen in Anführungszeichen eingeben.

> Außerdem darf die Zeichenfolge eine maximale Länge von 127 Zeichen nicht überschreiten.

So erstellen Sie ein Benutzerkonto über die Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Benutzerkonto zu erstellen und die Konfiguration zu überprüfen:

- `add system user <username> [-externalAuth ( ENABLED | DISABLED )] [-promptString <string>] [-timeout \<secs>] [-logging ( ENABLED | DISABLED )] [-maxsession <positive_integer>]`
- `show system user <userName>`

Externe Benutzer können den Parameter “Logging” so konfigurieren, dass externe Protokolle mithilfe des Weblogging- oder Audit-Logging-Mechanismus erfasst werden. Wenn der Parameter aktiviert ist, authentifiziert sich der Audit-Client bei der NetScaler-Appliance, um Protokolle zu sammeln.

Beispiel:

```
> add system user johnd -promptString user-%u-at-%T
```

```
1 Enter password:
2 Confirm password:
3 > show system user johnd
4 user name: john
5      Timeout:900 Timeout Inherited From: Global
6      External Authentication: ENABLED
7      Logging: DISABLED
8      Maximum Client Sessions: 20
9 <!--NeedCopy-->
```

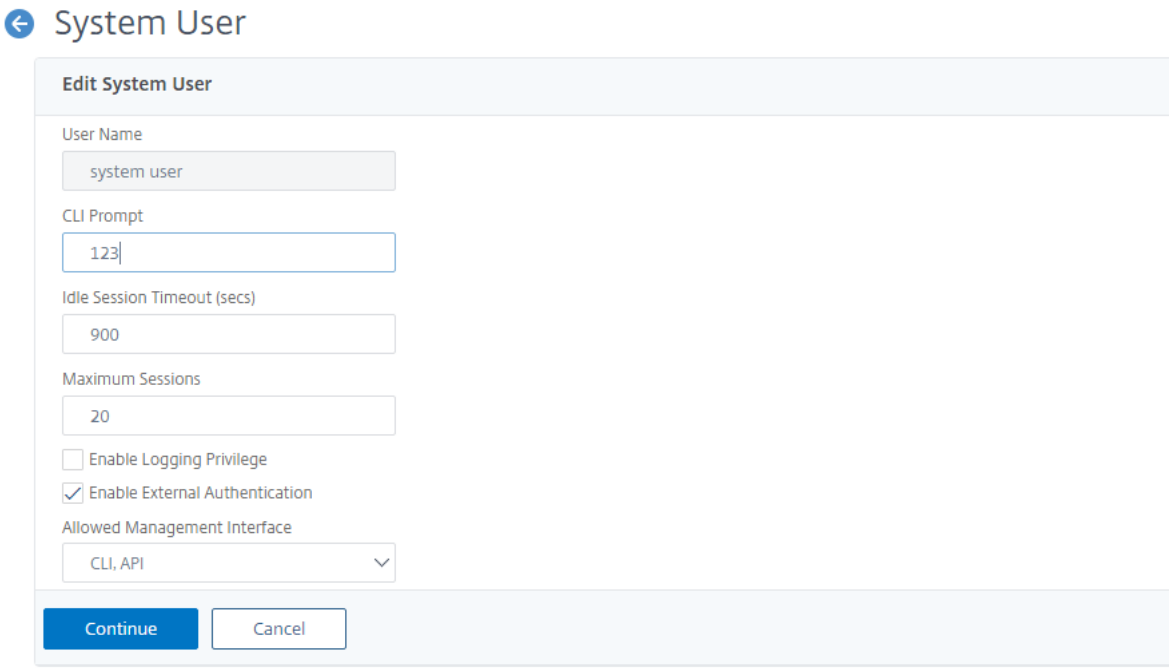
Informationen zur Parameterbeschreibung finden Sie unter Referenz zu Authentifizierung und Autorisierung für Benutzerbefehle .

Konfigurieren eines Benutzerkontos mit der NetScaler GUI

1. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Benutzer**und erstellen Sie den Benutzer.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um einen Systembenutzer zu erstellen.
3. Stellen Sie auf der Seite **Systemgruppe erstellen** die folgenden Parameter ein:
   a) Benutzername. Name der Benutzergruppe.
   b) CLI-Eingabeaufforderung. Die Eingabeaufforderung, die Sie für den CLI-Schnittstellenzugriff festlegen möchten.
   c) Sitzungs-Timeout im Leerlauf (Sekunden). Stellen Sie die Zeit ein, zu der ein Benutzer inaktiv sein kann, bevor die Sitzung abläuft und geschlossen wird.

d) Maximale Anzahl an Sitzungen. Legt die maximale Anzahl von Sitzungen fest, die ein Benutzer ausprobieren kann.
e) Aktivieren Sie das Logging-Privileg. Aktivieren Sie die Protokollierungsberechtigung für den Benutzer.
f) Aktivieren Sie die externe Authentifizierung. Wählen Sie die Option, wenn Sie einen externen Authentifizierungsserver für die Authentifizierung des Benutzers verwenden möchten.
g) Zulässige Verwaltungsschnittstelle. Wählen Sie die NetScaler-Schnittstellen aus, für die die Benutzergruppe Zugriffsrechte erhalten hat.
h) Befehlsrichtlinien. Binden Sie Befehlsrichtlinien an die Benutzergruppe.
i) Partitionen. Binden Sie Partitionen an die Benutzergruppe.

4. Klicken Sie auf **Erstellen** und **Schließen**.



Benutzergruppen konfigurieren

Nachdem Sie eine Benutzergruppe konfiguriert haben, können Sie problemlos allen Mitgliedern der Gruppe dieselben Zugriffsrechte gewähren. Um eine Gruppe zu konfigurieren, erstellen Sie die Gruppe und binden Benutzer an die Gruppe. Sie können jedes Benutzerkonto an mehr als eine Gruppe binden. Das Binden von Benutzerkonten an mehrere Gruppen ermöglicht möglicherweise mehr Flexibilität bei der Anwendung von Befehlsrichtlinien.

So erstellen Sie eine Benutzergruppe über die Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Benutzergruppe zu erstellen und die Konfiguration zu überprüfen:

- `add system group <groupName> [-promptString <string>] [-timeout <secs>]`
- `show system group <groupName>`

Beispiel:

```
> add system group Managers -promptString Group-Managers-at-%h
```

Binden Sie ein Benutzerkonto über die CLI an eine Gruppe

Geben Sie an der Befehlszeile die folgenden Befehle ein, um ein Benutzerkonto an eine Gruppe zu binden und die Konfiguration zu überprüfen:

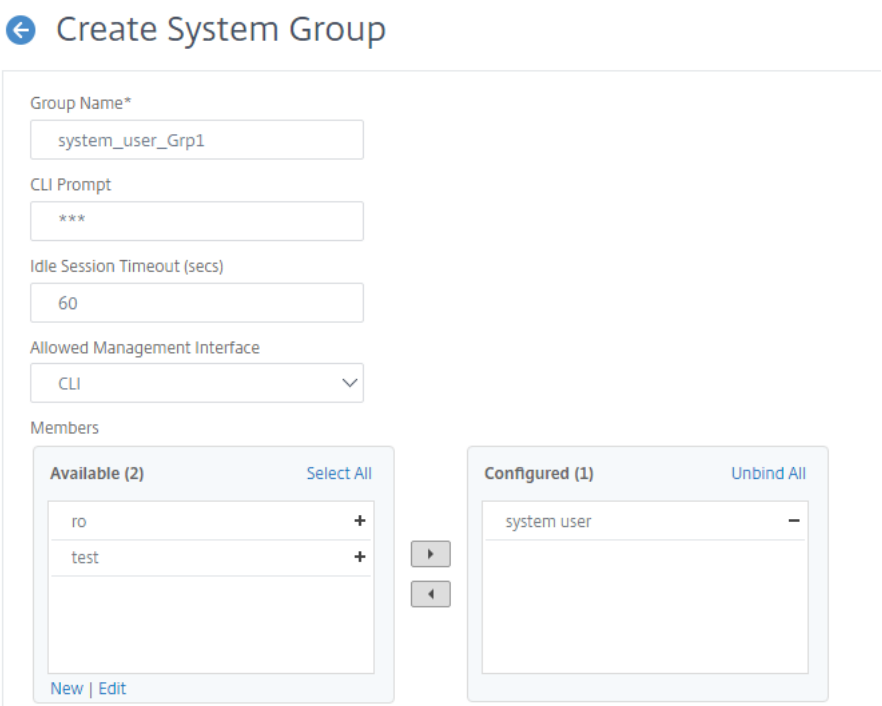
- `bind system group <groupName> -userName <userName>`
- `show system group <groupName>`

Beispiel:

```
> bind system group Managers -userName user1
```

Konfigurieren Sie eine Benutzergruppe über die NetScaler GUI

1. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Gruppen**und erstellen Sie die Benutzergruppe.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Systembenutzergruppe zu erstellen.
3. Stellen Sie auf der Seite **Systemgruppe erstellen** die folgenden Parameter ein:
   a) Gruppenname. Name der Benutzergruppe.
   b) CLI-Eingabeaufforderung. Die Eingabeaufforderung, die Sie für den CLI-Schnittstellenzugriff festlegen möchten.
   c) Sitzungs-Timeout im Leerlauf (Sekunden). Stellen Sie die Zeit ein, zu der ein Benutzer inaktiv sein kann, bevor die Sitzung abläuft und geschlossen wird.
   d) Zulässige Verwaltungsschnittstelle. Wählen Sie die NetScaler-Schnittstellen aus, für die die Benutzergruppe Zugriffsrechte erhalten hat.
   e) Mitglieder. Fügen Sie der Gruppe Benutzerkonten hinzu.
   f) Befehlsrichtlinien. Binden Sie Befehlsrichtlinien an die Benutzergruppe.
   g) Partitionen. Binden Sie Partitionen an die Benutzergruppe.
4. Klicken Sie auf **Erstellen** und **Schließen**.



> **Hinweis:**
>
> Um Mitglieder zur Gruppe hinzuzufügen, klicken Sie im Abschnitt Mitglieder auf **Hinzufügen**. Wählen Sie Benutzer aus der Liste Verfügbar aus und fügen Sie sie der Liste Konfiguriert hinzu.

Befehlsrichtlinien konfigurieren

Befehlsrichtlinien regeln, welche Befehle, Befehlsgruppen, virtuellen Server und andere Entitäten Benutzer und Benutzergruppen verwenden dürfen.

Die Appliance bietet eine Reihe integrierter Befehlsrichtlinien, und Sie können benutzerdefinierte Richtlinien konfigurieren. Um die Richtlinien anzuwenden, binden Sie sie entweder an Benutzer oder an Gruppen.

Hier sind die wichtigsten Punkte, die Sie bei der Definition und Anwendung von Befehlsrichtlinien beachten sollten.

- Sie können keine globalen Befehlsrichtlinien erstellen. Befehlsrichtlinien müssen direkt an die Benutzer und Gruppen auf der Appliance gebunden sein.
- Benutzer oder Gruppen ohne zugeordnete Befehlsrichtlinien unterliegen der Standardbefehlsrichtlinie (DENY-ALL) und können daher keine Konfigurationsbefehle ausführen, bis die richtigen Befehlsrichtlinien an ihre Konten gebunden sind.
- Alle Benutzer erben die Richtlinien der Gruppen, denen sie angehören.
- Sie müssen einer Befehlsrichtlinie eine Priorität zuweisen, wenn Sie sie an ein Benutzer- oder Gruppenkonto binden. Dadurch kann die Appliance bestimmen, welche Richtlinie Priorität

hat, wenn zwei oder mehr widersprüchliche Richtlinien für denselben Benutzer oder dieselbe Gruppe gelten.

- Wenn zwei verschiedene Befehlsrichtlinien mit derselben Priorität an ein Benutzer- oder Gruppenkonto gebunden sind, hat die erste gebundene Richtlinie die höchste Priorität.
- Die folgenden Befehle sind standardmäßig für jeden Benutzer verfügbar und werden von keinem von Ihnen angegebenen Befehl beeinflusst:
- help, CLI-Attribut anzeigen, CLI-Prompt festlegen, CLI-Prompt löschen, CLI-Prompt anzeigen, alias, unalias, history, quit, exit, whoami, config, CLI-Modus festlegen, CLI-Modus aufheben und CLI-Modus anzeigen.

In der folgenden Tabelle werden die integrierten Richtlinien beschrieben.

Richtlinienname	**Erlaubt**
schreibgeschützt	Schreibgeschützter Zugriff auf alle show-Befehle außer show ns RunningConfig, show ns ns.conf und den show-Befehlen für die NetScaler-Befehlsgruppe.
Operator	Schreibgeschützter Zugriff und Zugriff auf Befehle zum Aktivieren und Deaktivieren von Diensten und Servern.
network	Voller Zugriff, mit Ausnahme der SSL-Befehle set und unset, show ns ns.conf, show ns runningConfig und show gslb runningConfig.
sysadmin	[In NetScaler 12.0 und höher enthalten] Ein Sysadmin ist in Bezug auf den zulässigen Zugriff auf die Appliance niedriger als ein Superuser. Ein sysadmin-Benutzer kann alle NetScaler Vorgänge mit folgenden Ausnahmen ausführen: Kein Zugriff auf die NetScaler-Shell, keine Benutzerkonfigurationen ausführen, keine Partitionskonfigurationen ausführen und einige andere Konfigurationen, wie in der Sysadmin-Befehlsrichtlinie angegeben.
Superuser	Vollzugriff. Gleiche Rechte wie der nsroot-Benutzer.

Erstellen Sie benutzerdefinierte Befehlsrichtlinien

Unterstützung für reguläre Ausdrücke wird für Benutzer angeboten, die über die Ressourcen verfügen, um individuellere Ausdrücke zu verwalten, sowie für Bereitstellungen, die die Flexibilität erfordern, die reguläre Ausdrücke bieten. Für die meisten Benutzer sind die integrierten Befehlsrichtlinien ausreichend. Benutzer, die mehr Kontrolle benötigen, aber mit regulären Ausdrücken nicht vertraut sind, möchten möglicherweise nur einfache Ausdrücke verwenden, wie die in den Beispielen in diesem Abschnitt aufgeführten, um die Lesbarkeit der Richtlinien zu gewährleisten.

Beachten Sie Folgendes, wenn Sie einen regulären Ausdruck verwenden, um eine Befehlsrichtlinie zu erstellen.

- Wenn Sie reguläre Ausdrücke verwenden, um Befehle zu definieren, die von einer Befehlsrichtlinie betroffen sind, müssen Sie die Befehle in doppelte Anführungszeichen setzen. Um beispielsweise eine Befehlsrichtlinie zu erstellen, die alle Befehle enthält, die mit **show**beginnen, geben Sie Folgendes ein:
- “^show .*$”
- Geben Sie Folgendes ein, um eine Befehlsrichtlinie zu erstellen, die alle Befehle enthält, die mit rm beginnen:
- “^rm .*$”
- Reguläre Ausdrücke, die in Befehlsrichtlinien verwendet werden, unterscheiden nicht zwischen Groß- und Kleinschreibung.

In der folgenden Tabelle sind Beispiele für reguläre Ausdrücke für Befehlsrichtlinien aufgeführt:

Befehlsspezifikation	Entspricht diesen Befehlen
“^rm\s+.*$”	Alle Aktionen zum Entfernen, da alle Entfernungsobjekte mit der Zeichenfolge rm beginnen, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.
“^show\s+.*$”	Alle Show-Befehle, da alle Show-Aktionen mit der Zeichenfolge show beginnen, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.
“^shell$”	Der Shell-Befehl allein, aber nicht in Kombination mit zusätzlichen Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.

Befehlsspezifikation	Entspricht diesen Befehlen
“^add\s+vserver\s+.*$”	Alle erstellen virtuelle Serveraktionen, die aus dem Befehl zum Hinzufügen eines virtuellen Servers bestehen, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.
“^add\s+(lb\s+vserver)\s+.*”	Alle erstellen virtuelle Serveraktionen von lb, die aus dem Befehl add lb virtual server bestehen, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.

Informationen zu integrierten Befehlsrichtlinien finden Sie in Tabelle Integrierte Befehlsrichtlinientabelle .

So erstellen Sie eine Befehlsrichtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Befehlsrichtlinie zu erstellen und die Konfiguration zu überprüfen:

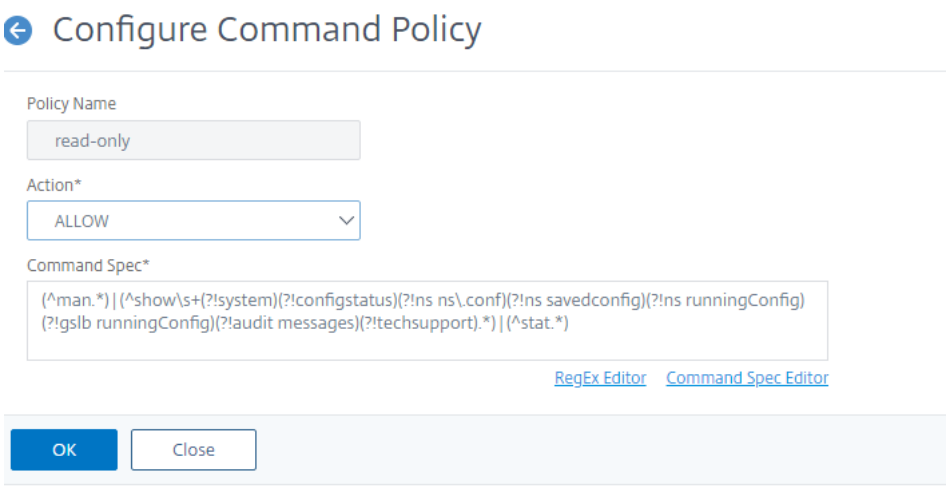
- `add system cmdPolicy <policyname> <action> <cmdspec>`
- `show system cmdPolicy <policyName>`

Beispiel:

```
add system cmdPolicy USER-POLICY ALLOW (\ server\ )|(\ service(Group)*\ )
|(\ vserver\ )|(\ policy\ )|(\ policylabel\ )|(\ limitIdentifier\ )|(^show\
 (?!(system|ns\ (ns.conf|runningConfig)))|(save)|(stat\ .*serv)
```

Konfigurieren Sie eine Befehlsrichtlinie über die NetScaler GUI

1. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Befehlsrichtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Befehlsrichtlinie zu erstellen.
3. Stellen Sie auf der Seite **Befehlsrichtlinie konfigurieren** die folgenden Parameter ein:
   a) Richtlinienname
   b) Aktion
   c) Befehlsspezifikation.
4. Klicken Sie auf **OK**.



Binden Sie Befehlsrichtlinien an Benutzerkonten und Benutzergruppen

Nachdem Sie Ihre Befehlsrichtlinien definiert haben, müssen Sie sie an die entsprechenden Benutzerkonten und Gruppen binden. Wenn Sie eine Richtlinie binden, müssen Sie ihr eine Priorität zuweisen, damit die Appliance bestimmen kann, welche Befehlsrichtlinie zu befolgen ist, wenn zwei oder mehr anwendbare Befehlsrichtlinien in Konflikt stehen.

Befehlsrichtlinien werden in der folgenden Reihenfolge bewertet:

- Befehlsrichtlinien, die direkt an Benutzer und die entsprechenden Gruppen gebunden sind, werden anhand einer Prioritätsnummer bewertet. Eine Befehlsrichtlinie mit einer niedrigeren Prioritätsnummer wird vor einer Befehlsrichtlinie mit einer höheren Prioritätsnummer ausgewertet. Daher werden alle Privilegien, die die Befehlsrichtlinie mit niedrigeren Nummern explizit gewährt oder verweigert, nicht durch eine Befehlsrichtlinie mit höheren Nummern außer Kraft gesetzt.
- Wenn zwei Befehlsrichtlinien, von denen eine an ein Benutzerkonto und die andere an eine Gruppe gebunden ist, dieselbe Prioritätsnummer haben, wird die direkt an das Benutzerkonto gebundene Befehlsrichtlinie zuerst ausgewertet.

So binden Sie Befehlsrichtlinien über die Befehlszeilenschnittstelle an einen Benutzer

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Befehlsrichtlinie an einen Benutzer zu binden und die Konfiguration zu überprüfen:

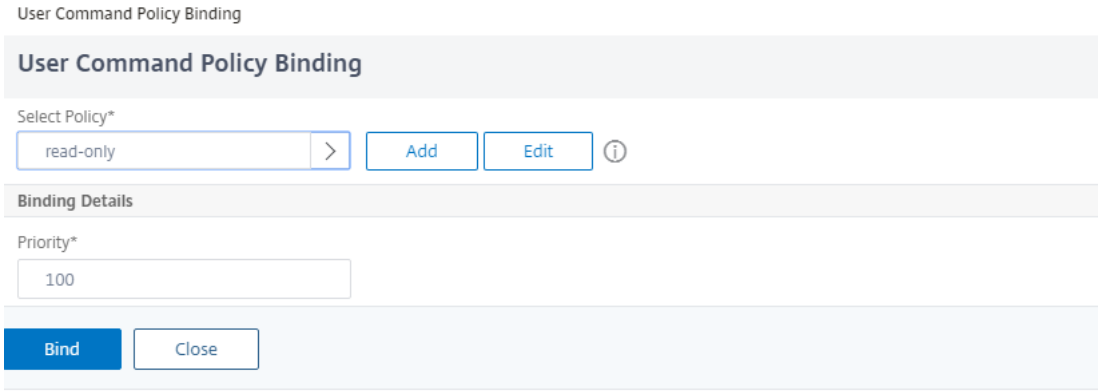
- `bind system user <userName> -policyName <policyName> <priority>`
- `show system user <userName>`

Beispiel:

```
> bind system user user1 -policyName read_all 1
```


Binden Sie Befehlsrichtlinien über die NetScaler GUI an ein Benutzerkonto

Navigieren Sie zu **System** > **Benutzerverwaltung** > **Benutzer**, wählen Sie den Benutzer aus und binden Sie die Befehlsrichtlinien.



Optional können Sie die Standardpriorität ändern, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge bewertet wird.

So binden Sie Befehlsrichtlinien über die Befehlszeilenschnittstelle an eine Gruppe

Geben Sie an der Befehlszeile die folgenden Befehle ein, um eine Befehlsrichtlinie an eine Benutzergruppe zu binden und die Konfiguration zu überprüfen:

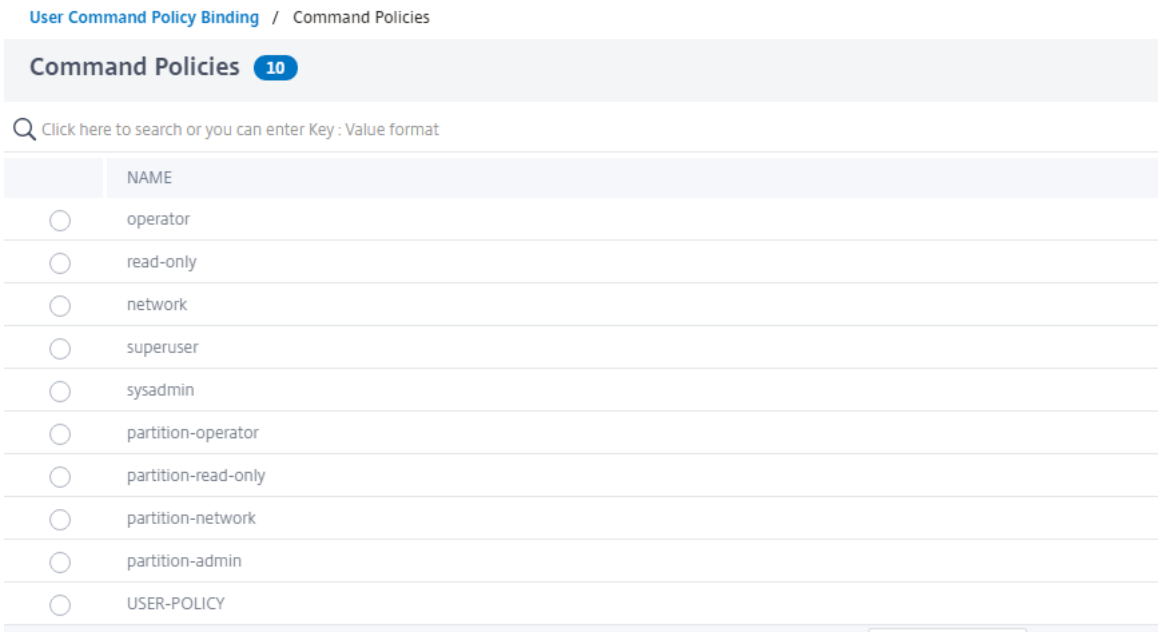
- `bind system group <groupName> -policyName <policyName> <priority>`
- `show system group <groupName>`

Beispiel:

```
> bind system group Managers -policyName read_all 1
```

Binden Sie Befehlsrichtlinien über die NetScaler GUI an eine Benutzergruppe

Navigieren Sie zu **System** > **Benutzerverwaltung** > **Gruppen**, wählen Sie die Gruppen- und Bind-Befehlsrichtlinien aus.



Optional können Sie die Standardpriorität ändern, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge bewertet wird.

Anwendungsbeispiel: Verwaltung von Benutzerkonten, Benutzergruppen und Befehlsrichtlinien in einer Fertigungsorganisation

Das folgende Beispiel zeigt, wie Sie einen vollständigen Satz von Benutzerkonten, Gruppen und Befehlsrichtlinien erstellen und jede Richtlinie an die entsprechenden Gruppen und Benutzer binden. Das Unternehmen Example Manufacturing, Inc., hat drei Benutzer, die auf die NetScaler-Appliance zugreifen können:

- **John Doe.** Der IT-Manager. John muss in der Lage sein, alle Teile der NetScaler-Konfiguration zu sehen, muss aber nichts ändern.
- **Maria Ramiez.** Der leitende IT-Administrator. Maria muss in der Lage sein, alle Teile der NetScaler-Konfiguration mit Ausnahme der NetScaler-Befehle zu sehen und zu ändern (die lokalen Richtlinien schreiben vor, dass sie ausgeführt werden müssen, während sie als nsroot angemeldet sind).
- **Michael Baldrock.** Der für den Lastenausgleich zuständige IT-Administrator. Michael muss in der Lage sein, alle Teile der NetScaler-Konfiguration zu sehen, muss aber nur die Load-Balancing-Funktionen ändern.

Die folgende Tabelle zeigt die Aufschlüsselung der Netzwerkinformationen, Benutzerkontonamen, Gruppennamen und Befehlsrichtlinien für das Beispielunternehmen.

Feld	Wert	Hinweis
NetScaler Hostname	ns01.example.net	–
Benutzerkonten	johnd, mariar und michaelb	John Doe, IT-Manager, Maria Ramirez, IT-Administrator, und Michael Baldrock, IT-Administrator.
Gruppen	Manager und SysOps	Alle Manager und alle IT-Administratoren.
Befehlsrichtlinien	read_all, modify_lb und modify_all	Vollständigen Lesezugriff zulassen, Änderungszugriff auf Loadbalancing zulassen und Vollständigen Änderungszugriff zulassen.

Die folgende Beschreibung führt Sie durch den Prozess der Erstellung eines vollständigen Satzes von Benutzerkonten, Gruppen und Befehlsrichtlinien auf der NetScaler-Appliance mit dem Namen ns01.example.net.

Die Beschreibung enthält Verfahren zum gegenseitigen Binden der entsprechenden Benutzerkonten und Gruppen sowie zum Binden der entsprechenden Befehlsrichtlinien an die Benutzerkonten und Gruppen.

Dieses Beispiel zeigt, wie Sie mithilfe der Priorisierung jedem Benutzer in der IT-Abteilung präzise Zugriffsrechte und Berechtigungen gewähren können.

Das Beispiel geht davon aus, dass die Erstinstallation und Konfiguration bereits auf dem NetScaler durchgeführt wurden.

Konfiguration von Benutzerkonten, Gruppen und Befehlsrichtlinien für eine Beispielorganisation

1. Verwenden Sie das im Abschnitt Konfiguration von Benutzerkonten beschriebene Verfahren, um die Benutzerkonten **johnd**, **mariar**und **michaelb**zu erstellen.
2. Verwenden Sie das unter Konfiguration von Benutzergruppen beschriebene Verfahren, um die Benutzergruppen **Manager** und **SysOps**zu erstellen, und binden Sie dann die Benutzer **mariar** und **michaelb** an die **SysOps-Gruppe** und den Benutzer **johnd an** die **Manager-Gruppe** .
3. Verwenden Sie das unter Erstellen von benutzerdefinierten Befehlsrichtlinien beschriebene Verfahren, um die folgenden Befehlsrichtlinien zu erstellen:

- **read_all** mit der Aktion **Allow** und Befehlsspezifikation `"(^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*)|(^stat.*)"`
- **modify_lb** mit Action als **Allow** und der Befehlsspezifikation `"^set\s+lb\s+.*$"`
- modify_all mit Aktion Zulassen und der Befehlsspezifikation `"^\S+\s+(?!system).*"`

4. Verwenden Sie das unter “Binden von Befehlsrichtlinien an Benutzer und Gruppen” beschriebene Verfahren, um die **read_all-Befehlsrichtlinie** mit dem Prioritätswert **1** an die **SysOps-Gruppe**zu binden.
5. Verwenden Sie das unter “Binden von Befehlsrichtlinien an Benutzer und Gruppen” beschriebene Verfahren, um die **modify_lb-Befehlsrichtlinie** mit dem Prioritätswert **5**an Benutzer **michaelb**zu binden.

Die soeben erstellte Konfiguration führt zu folgendem Ergebnis:

- John Doe, der IT-Manager, hat nur Lesezugriff auf die gesamte NetScaler-Konfiguration, kann jedoch keine Änderungen vornehmen.
- Maria Ramirez, die IT-Leiterin, hat nahezu vollständigen Zugriff auf alle Bereiche der NetScaler-Konfiguration und muss sich nur anmelden, um Befehle auf NetScaler-Ebene auszuführen.
- Michael Baldrock, der für den Lastenausgleich zuständige IT-Administrator, hat nur Lesezugriff auf die NetScaler-Konfiguration und kann die Konfigurationsoptionen für den Lastenausgleich ändern.

Die Befehlsrichtlinien, die für einen bestimmten Benutzer gelten, sind eine Kombination aus Befehlsrichtlinien, die direkt auf das Konto des Benutzers angewendet werden, und Befehlsrichtlinien, die auf eine oder mehrere Gruppen angewendet werden, deren Mitglied der Benutzer ist.

Jedes Mal, wenn ein Benutzer einen Befehl eingibt, durchsucht das Betriebssystem die Befehlsrichtlinien für diesen Benutzer, bis es eine Richtlinie mit einer ALLOW- oder DENY-Aktion findet, die dem Befehl entspricht. Wenn es eine Übereinstimmung findet, stoppt das Betriebssystem die Suche nach Befehlsrichtlinien und erlaubt oder verweigert den Zugriff auf den Befehl.

Wenn das Betriebssystem keine passende Befehlsrichtlinie findet, verweigert es dem Benutzer den Zugriff auf den Befehl gemäß der standardmäßigen Verweigerungsrichtlinie der NetScaler-Appliance.

> **Hinweis:**
>
> Wenn Sie einen Benutzer in mehrere Gruppen einteilen, achten Sie darauf, dass keine unbeabsichtigten Einschränkungen oder Berechtigungen durch Benutzerbefehle entstehen. Beachten Sie bei der Organisation Ihrer Benutzer in Gruppen das Suchverfahren für NetScaler-Befehlsrichtlinien und die Regeln für die Richtlinienreihenfolge, um diese Konflikte zu vermeiden.

Benutzerkonto- und Kennwortverwaltung

June 19, 2023

NetScaler ermöglicht Ihnen die Verwaltung von Benutzerkonten und Kennwortkonfigurationen. Im Folgenden sind einige der Aktivitäten aufgeführt, die Sie für ein Systembenutzerkonto oder ein `nsroot` Administratorkonto auf der Appliance ausführen können.

- Sperrung des Systembenutzerkontos
- Sperren Sie das Systembenutzerkonto für den Verwaltungszugriff
- Entsperren Sie ein gesperrtes Systembenutzerkonto für den Verwaltungszugriff
- Deaktivieren Sie den Verwaltungszugriff für das Systembenutzerkonto
- Kennwortänderung für `nsroot` Administratorbenutzer erzwingen
- Entfernen Sie vertrauliche Dateien in einem Systembenutzerkonto
- Starke Kennwortkonfiguration für Systembenutzer

Sperrung des Systembenutzerkontos

Um Brute-Force-Sicherheitsangriffe zu verhindern, können Sie die Benutzersperrkonfiguration konfigurieren. Die Konfiguration ermöglicht es einem Netzwerkadministrator, einen Systembenutzer daran zu hindern, sich an einer NetScaler-Appliance anzumelden. Und entsperren Sie auch das Benutzerkonto, bevor die Sperrfrist abläuft.

Geben Sie in der Befehlszeile Folgendes ein:

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED)
```

> **Hinweis**
>
> Der Parameter „persistentLoginAttempts“ muss AKTIVIERT sein, um die Details der persistenten Speicherung erfolgloser Benutzeranmeldeversuche bei Neustarts abzurufen.

Beispiel:

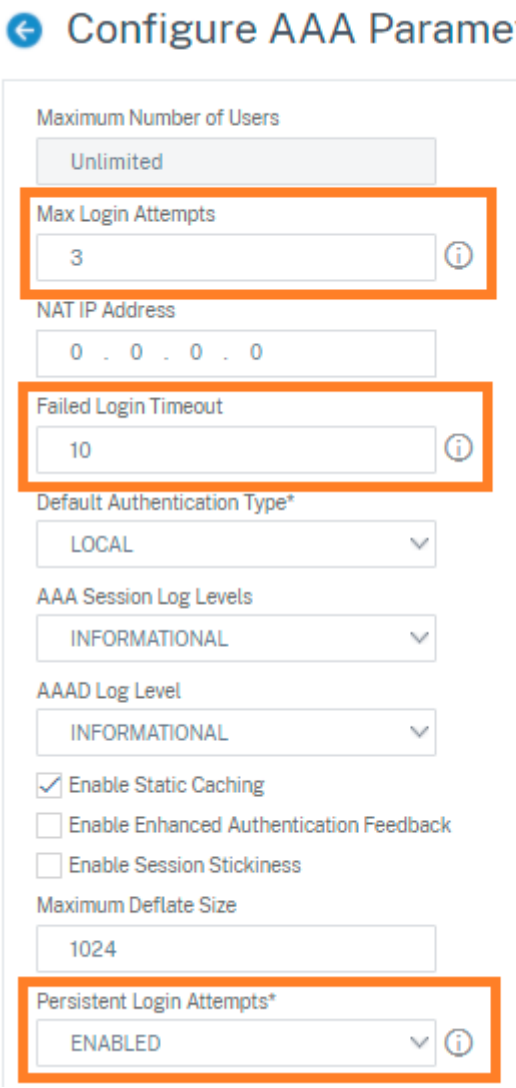
```
set aaa parameter -maxloginAttempts 3 -failedLoginTimeout 10 -persistentLoginAttempts
 ENABLED
```

Konfigurieren Sie die Sperrung von Systembenutzerkonten mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsverkehr > Authentifizierungseinstellungen > AAA-Authentifizierungseinstellungen ändern**.
2. Stellen Sie auf der Seite **„AAA-Parameter konfigurieren** “ die folgenden Parameter ein:

a) Max. Anmeldeversuche. Die maximale Anzahl von Anmeldeversuchen, die der Benutzer versuchen darf.
b) Anmelde-Timeout fehlgeschlagen. Die maximale Anzahl ungültiger Anmeldeversuche des Benutzers.
c) Ständige Anmeldeversuche. Dauerhafte Speicherung erfolgloser Benutzeranmeldeversuche bei Neustarts.

3. Klicken Sie auf **OK**.



Wenn Sie die Parameter festlegen, wird das Benutzerkonto für 10 Minuten für drei oder mehr ungültige Anmeldeversuche gesperrt. Außerdem kann sich der Benutzer selbst mit gültigen Anmeldeinformationen 10 Minuten lang nicht anmelden.

> **Hinweis**
>
> Wenn ein gesperrter Benutzer versucht, sich an der Appliance anzumelden, wird eine Fehler-

> meldung `RBA Authentication Failure: maxlogin attempt reached for test.` angezeigt.

Sperren Sie das Systembenutzerkonto für den Verwaltungszugriff

Mit der NetScaler Appliance können Sie einen Systembenutzer für 24 Stunden sperren und dem Benutzer den Zugriff verweigern.

Die NetScaler-Appliance unterstützt die Konfiguration sowohl für Systembenutzer als auch für externe Benutzer.

> **Hinweis**
>
> Die Funktion wird nur unterstützt, wenn Sie die Option `persistentLoginAttempts` im Parameter `aaa` deaktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

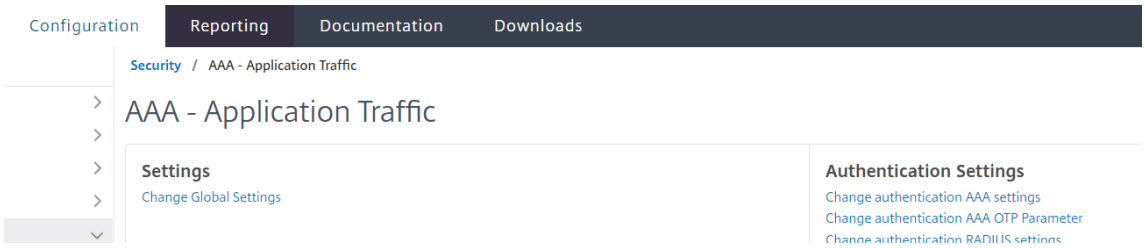
```
set aaa parameter -persistentLoginAttempts DISABLED
```

Um ein Benutzerkonto zu sperren, geben Sie an der Eingabeaufforderung Folgendes ein:

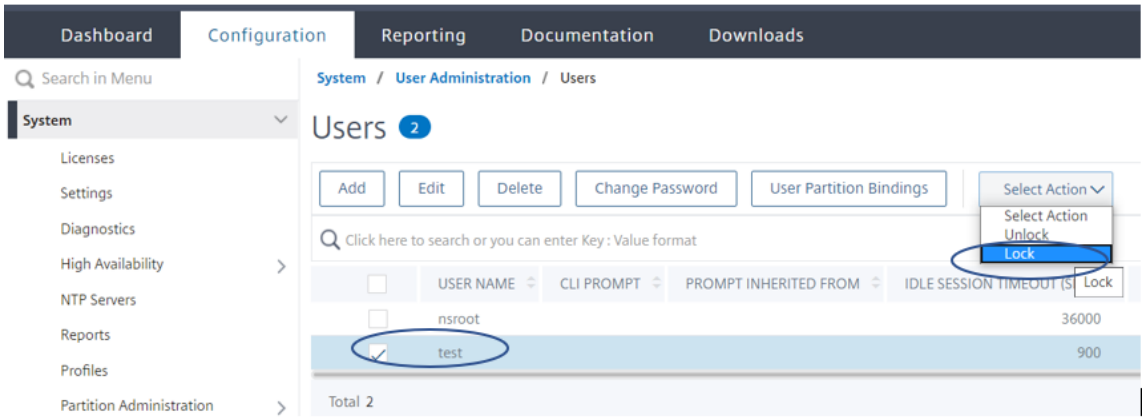
```
lock aaa user test
```

Sperren Sie ein Systembenutzerkonto mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsverkehr > Authentifizierungseinstellungen > AAA-Authentifizierungseinstellungen ändern**.



2. Wählen **Sie unter AAA-Parameter konfigurieren**in der Liste **Persistent Login Attempts** die Option **DISABLED**aus.
3. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
4. Wählen Sie einen Benutzer aus.
5. Wählen Sie in der Liste „Aktion auswählen“ die Option **Sperren**aus.



> **Hinweis**
>
> Die NetScaler-GUI bietet keine Option zum Sperren externer Benutzer. Um einen externen Benutzer zu sperren, muss der ADC-Administrator die CLI verwenden.
> Wenn ein gesperrter Systembenutzer (gesperrt mit Lock-Authentifizierung, Autorisierung und Auditing-Benutzerbefehl) versucht, sich bei NetScaler anzumelden, zeigt die Appliance die Fehlermeldung „RBA-Authentifizierungsfehler: Der Benutzertest ist für 24 Stunden gesperrt“ an.
>
> Wenn ein Benutzer gesperrt ist, um sich am Verwaltungszugriff anzumelden, ist der Konsolenzugriff davon ausgenommen. Der gesperrte Benutzer kann sich an der Konsole anmelden.

Entsperren Sie ein gesperrtes Systembenutzerkonto für den Verwaltungszugriff

Systembenutzer und externe Benutzer können mit dem Befehl lock authentication, authorization und auditing user für 24 Stunden gesperrt werden.

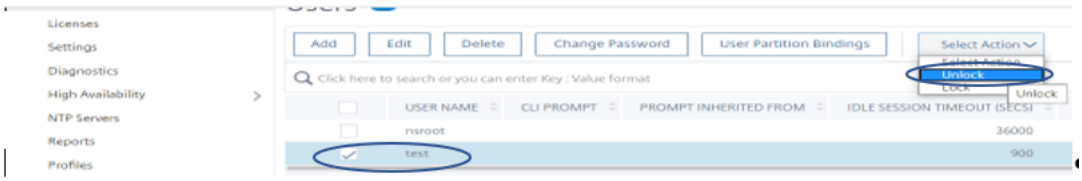
> **Hinweis**
>
> Die ADC-Appliance ermöglicht es Administratoren, den gesperrten Benutzer zu entsperren, und für die Funktion sind keine Einstellungen im Befehl „PersistentLoginAttempts“ erforderlich.

Geben Sie in der Befehlszeile Folgendes ein:

```
unlock aaa user test
```

Konfigurieren Sie die Systembenutzer-Entsperrung mithilfe der GUI

1. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
2. Wählen Sie einen Benutzer aus.
3. Klicken Sie auf **Entsperren**



Die NetScaler-GUI listet nur Systembenutzer auf, die im ADC erstellt wurden, sodass es in der GUI keine Option gibt, externe Benutzer zu entsperren. Um einen externen Benutzer zu entsperren, muss der `nsroot` Administrator die CLI verwenden.

Deaktivieren Sie den Verwaltungszugriff für das Systembenutzerkonto

Wenn die externe Authentifizierung auf der Appliance konfiguriert ist und Sie es als Administrator vorziehen, Systembenutzern den Zugriff zu verweigern, um sich am Verwaltungszugriff anzumelden, müssen Sie die LocalAuth-Option im Systemparameter deaktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

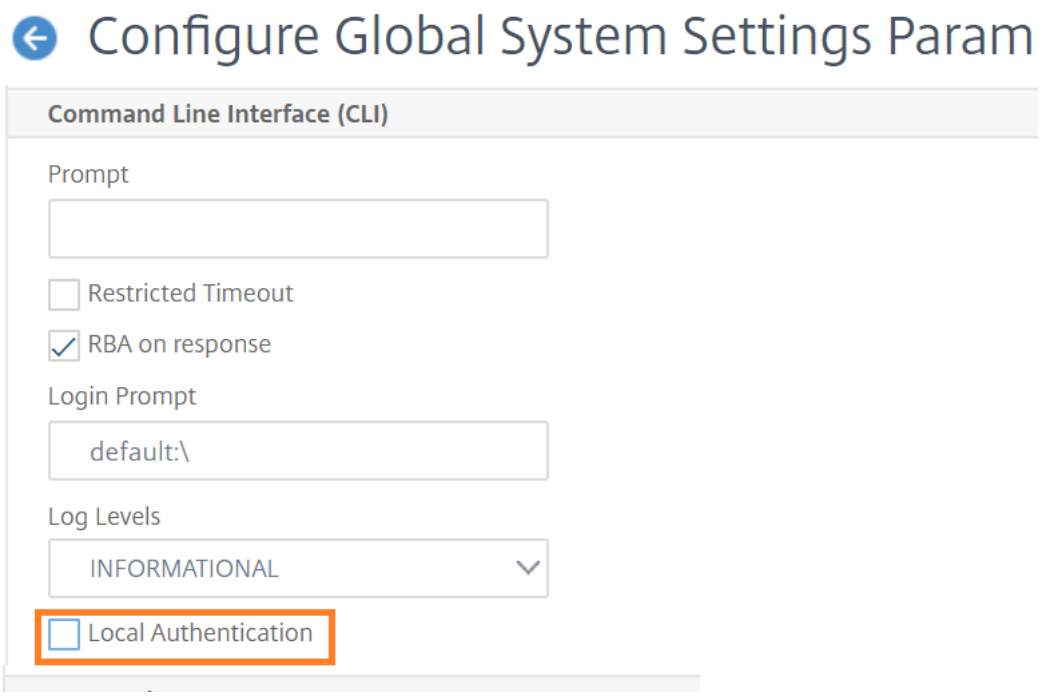
```
set system parameter localAuth <ENABLED|DISABLED>
```

Beispiel:

```
set system parameter localAuth DISABLED
```

Deaktivieren Sie den Verwaltungszugriff für den Systembenutzer mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > System > Einstellungen > Globale Systemeinstellungen ändern**.
2. Deaktivieren **Sie im Abschnitt Befehlszeilenschnittstelle (CLI)** das Kontrollkästchen **Lokale Authentifizierung** .



Wenn Sie die Option deaktivieren, können sich lokale Systembenutzer nicht am ADC-Verwaltungszugriff anmelden.

> **Hinweis**
>
> Der externe Authentifizierungsserver muss konfiguriert und erreichbar sein, um die lokale Systembenutzerauthentifizierung im Systemparameter zu verhindern. Wenn der in ADC für den Verwaltungszugriff konfigurierte externe Server nicht erreichbar ist, können sich lokale Systembenutzer an der Appliance anmelden. Das Verhalten ist für Wiederherstellungszwecke eingerichtet.

Kennwortänderung für Administratorbenutzer erzwingen

Für eine gesicherte `nsroot`-Authentifizierung fordert die NetScaler-Appliance den Benutzer auf, das Standardkennwort in ein neues zu ändern, wenn die Option `forcePasswordChange` im Systemparameter aktiviert ist. Sie können Ihr `nsroot`-Kennwort entweder über die CLI oder die GUI ändern, wenn Sie sich zum ersten Mal mit den Standardanmeldeinformationen anmelden.

Geben Sie in der Befehlszeile Folgendes ein:

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

Beispiel für eine SSH-Sitzung für NSIP:

```
1 ssh nsroot@1.1.1.1
2 Connecting to 1.1.1.1:22...
3 Connection established.
```



```
To escape to local shell, press Ctrl+Alt+].
###############################################################################

WARNING: Access to this system is for authorized users only #
Disconnect IMMEDIATELY if you are not an authorized user! #

###############################################################################

Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
<!--NeedCopy-->
```

Entfernen Sie vertrauliche Dateien in einem Systembenutzerkonto

Um sensible Daten wie autorisierte Schlüssel und öffentliche Schlüssel für ein Systembenutzerkonto zu verwalten, müssen Sie die `removeSensitiveFiles` Option aktivieren. Die Befehle, mit denen vertrauliche Dateien entfernt werden, wenn der Systemparameter aktiviert ist, sind:

- RM-Cluster-Instanz
- RM-Clusterknoten
- RM-Hochverfügbarkeitsknoten
- Konfiguration vollständig löschen
- dem Cluster beitreten
- Clusterinstanz hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
set system parameter removeSensitiveFiles ( ENABLED | DISABLED )
```

Beispiel:

```
set system parameter -removeSensitiveFiles ENABLED
```

Starke Kennwortkonfiguration für Systembenutzer

Für eine sichere Authentifizierung fordert die NetScaler-Appliance Systembenutzer und Administratoren auf, sichere Kennwörter für die Anmeldung an der Appliance festzulegen. Das Kennwort muss lang sein und eine Kombination aus folgenden Elementen sein:

- Ein Kleinbuchstabe
- Ein Großbuchstabe
- Ein numerisches Zeichen

- Ein besonderes Zeichen

Geben Sie in der Befehlszeile Folgendes ein:

```
set system parameter -strongpassword <value> -minpasswordlen <value>
```

Hierbei gilt:

`Strongpassword`. Nach der Aktivierung des starken Kennworts (`enable all` / `enablelocal`) müssen alle Kennwörter oder vertraulichen Informationen Folgendes enthalten:

- Mindestens 1 Kleinbuchstabe
- Mindestens 1 Großbuchstabe
- Mindestens 1 numerisches Zeichen
- Mindestens 1 Sonderzeichen

Exclude the list in `enablelocal` is - `NS_FIPS`, `NS_CRL`, `NS_RSAKEY`, `NS_PKCS12`, NS_PKCS8, NS_LDAP, `NS_TACACS`, `NS_TACACSACTION`, `NS_RADIUS`, `NS_RADIUSACTION`, `NS_ENCRYPTION_PARAMS` . Daher werden für diese ObjectType-Befehle für den Systembenutzer keine starken Kennwortprüfungen durchgeführt.

Mögliche Werte: `enableall`, `enablelocal`, disabled
Standardwert: disabled

`minpasswordlen`. Mindestlänge des Systembenutzerkennworts. Wenn das sichere Kennwort standardmäßig aktiviert ist, beträgt die Mindestlänge 4. Der vom Benutzer eingegebene Wert kann größer oder gleich 4 sein. Der standardmäßige Mindestwert ist 1, wenn das sichere Kennwort deaktiviert ist. Der Maximalwert ist in beiden Fällen 127.

Mindestwert: 1
Maximalwert: 127

Beispiel:

```
set system parameter -strongpassword enablelocal -minpasswordlen 6
```

Standardbenutzerkonto

Das `nsrecover`-Benutzerkonto kann vom Administrator verwendet werden, um die NetScaler-Appliance wiederherzustellen. Sie können sich bei der ADC-Appliance anmelden, indem `nsrecover` Sie den Standardsystembenutzer (`nsroot`) aufgrund unvorhergesehener Probleme nicht anmelden können. Die `nsrecover`-Anmeldung ist unabhängig von Benutzerkonfigurationen und ermöglicht Ihnen den direkten Zugriff auf den Shell-Prompt. Sie können sich immer über den anmelden, `nsrecover` unabhängig davon, ob das maximale Konfigurationslimit erreicht ist.

So setzen Sie das Rootadministratorkennwort (nsroot) zurück

September 1, 2023

Das NetScaler-Rootadministratorkonto (`nsroot`) bietet vollständigen Zugriff auf alle ADC-Funktionen. Um die Sicherheit zu gewährleisten, darf das Administratorkonto nur bei Bedarf verwendet werden.

Als Admin empfiehlt es sich, Ihr Kennwort zu ändern. Wenn Sie Ihr Kennwort vergessen, müssen Sie zuerst auf das Standardkennwort zurücksetzen und es dann in ein neues Kennwort ändern.

Um Ihr Kennwort zurückzusetzen, müssen Sie sich als `nsroot`-Administrator bei Ihrer Appliance anmelden und das Kennwort ändern. Wenn Sie sich jedoch nicht an das Kennwort erinnern, können Sie die Appliance im Einzelbenutzermodus neu starten. Hängen Sie das Dateisystem im Lese-/Schreibmodus ein und entfernen Sie dann den **NetScaler-Eintrag** aus der Datei ns.conf. Starten Sie als letzten Schritt neu und melden Sie sich mit dem Standardgerät bei Ihrer Appliance an und legen Sie ein neues Kennwort fest.

Führen Sie die folgenden Schritte aus, um Ihr Root-Administratorkennwort zurückzusetzen

1. Verbinden Sie einen Computer mit dem Konsolenport des NetScaler und melden Sie sich an.

   > **Hinweis:**
   >
   > Sie können sich nicht mit SSH anmelden, um dieses Verfahren durchzuführen. Sie müssen sich direkt mit der Appliance verbinden.

2. Starten Sie den NetScaler neu.
3. Drücken Sie STRG+C, wenn die folgende Meldung angezeigt wird:

   ```
   Press [Ctrl-C] for command prompt, or any other key to boot immediately
   .
   Booting [kernel] in ## seconds.
   ```

4. Führen Sie den folgenden Befehl aus, um den NetScaler in einem einzigen Benutzermodus zu starten:

   ```
   boot -s
   ```

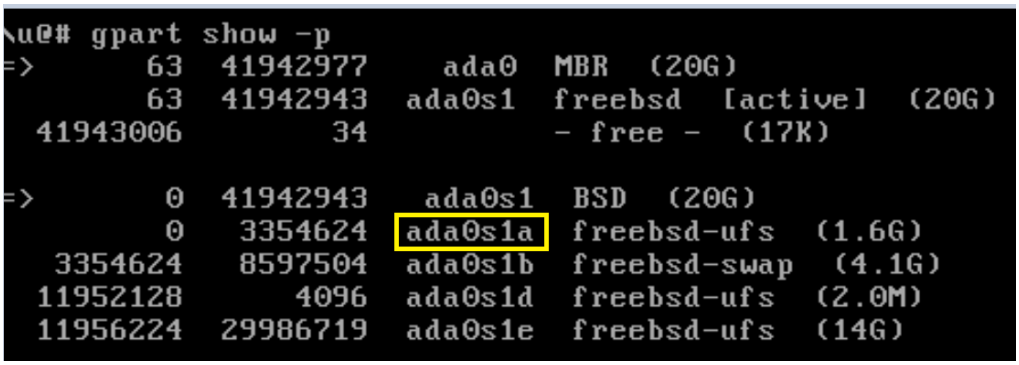
   Nach dem Booten der Appliance wird die folgende Meldung angezeigt:

   Geben Sie den vollständigen Pfadnamen der Shell ein oder `RETURN for /bin/sh:`

5. Drücken Sie die EINGABETASTE, um die Eingabeaufforderung # anzuzeigen, und geben Sie die folgenden Befehle ein, um die Dateisysteme

   a) Führen Sie den folgenden Befehl aus, um die Datenträgerkonsistenz zu überprüfen:

   ```
   fsck_ufs /dev/ada0s1a
   ```


> **Hinweis**
>
> Ihr Flash-Laufwerk hat je nach NetScaler einen bestimmten Gerätenamen. Führen Sie den folgenden Befehl an der ADC-CLI aus und kopieren Sie den Namen mit der Endung “1a”.
>
> ```
> gpart show -p
> ```
>
> Zum Beispiel
>
> 
>

b) Greifen Sie auf das Dev-Verzeichnis zu und geben Sie ‘ls’ ein, um die Laufwerksdetails zu überprüfen.

c) Führen Sie den folgenden Befehl aus, um die bereitgestellten Partitionen anzuzeigen:

```
df
```

> **Hinweis**
>
> Wenn die Flash-Partition nicht aufgeführt ist, müssen Sie sie manuell einhängen.

d) Führen Sie den folgenden Befehl aus, um das Flash-Laufwerk einzubinden:

```
mount /dev/ada0s1a /flash
```

6. Führen Sie den folgenden Befehl aus, um in das Verzeichnis `nsconfig` zu wechseln:

```
cd /flash/nsconfig
```

7. Führen Sie die folgenden Befehle aus, um die Datei ns.conf neu zu schreiben und den Satz von Systembefehlen zu entfernen, die standardmäßig auf den Administrator gesetzt sind:

a) Führen Sie den folgenden Befehl aus, um eine Konfigurationsdatei zu erstellen, die keine Befehle enthält, die standardmäßig vom Administrator verwendet werden:

```
grep -v “set system user nsroot” ns.conf > new.conf
```

b) Führen Sie den folgenden Befehl aus, um eine Backup der vorhandenen Konfigurationsdatei zu erstellen:

```
mv ns.conf old.ns.conf
```


c) Führen Sie den folgenden Befehl aus, um die neue.conf-Datei in ns.conf umzubenennen:

```
mv new.conf ns.conf
```

8. Führen Sie den folgenden Befehl aus, um den NetScaler neu zu starten:

```
reboot
```

9. Melden Sie sich mit den Standard-Administratoranmeldeinformationen an.
10. Führen Sie den folgenden Befehl aus, um das Administratorkennwort zurückzusetzen:

```
set system user nsroot <New_Password>
```

> **Hinweis**
>
> Um das "?"-Zeichen in einer Kennwortzeichenfolge zu benutzen, stellen Sie diesem Zeichen ein \-Zeichen voraus.

Zum Beispiel wird `yourexamplepasswd?` für das Administratorkonto festgelegt, nachdem Sie den folgenden Vorgang ausgeführt haben:

```
> set system user nsroot yourexamplepasswd\?
```

> **Hinweis**
>
> Um ein vergessenes (`nsroot`) Kennwort in einem Hochverfügbarkeits-Setup zurückzusetzen, wird empfohlen, den Peer-Knoten herunterzufahren. Wenn der Peer-Knoten aktiv ist, wird das Kennwort überschrieben, da die Konfigurationssynchronisierung ausgelöst wird, wenn der Knoten nach dem Neustart hochfährt.

Lesen Sie auch den Artikel CTX224027, um zu erfahren, wie der sichere SSH-Zugriff auf die NetScaler-Appliance funktioniert.

Externe Benutzerauthentifizierung

May 11, 2023

Der Authentifizierungsdienst in einer NetScaler-Appliance kann lokal oder extern sein. Bei der externen Benutzerauthentifizierung verwendet die Appliance einen externen Server wie LDAP, RADIUS oder TACACS+, um den Benutzer zu authentifizieren. Um einen externen Benutzer zu authentifizieren und dem Benutzer Zugriff auf die Appliance zu gewähren, müssen Sie eine Authentifizierungsrichtlinie anwenden. Die NetScaler-Systemauthentifizierung verwendet erweiterte Authentifizierungsrichtlinien mit erweiterten Richtlinienausdrücken. Die erweiterten Authentifizierungsrichtlinien werden auch für die Systembenutzerverwaltung in einer partitionierten NetScaler-Appliance verwendet.

> **Hinweis**
>
> Wenn Ihre Appliance weiterhin Classic-Richtlinien und ihre Ausdrücke verwendet, müssen Sie sie nicht mehr verwenden und die Verwendung der Classic-Richtlinie in die Advanced-Richtlinieninfrastruktur migrieren.

Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, müssen Sie sie an die globale Entität des Systems binden. Sie können einen externen Authentifizierungsserver (z. B. TACACS) konfigurieren, indem Sie eine einzelne Authentifizierungsrichtlinie an die globale Entität des Systems binden. Sie können auch eine Kaskade von Authentifizierungsservern konfigurieren, indem Sie mehrere Richtlinien an die globale Entität des Systems binden.

> **Hinweis**
>
> Wenn sich ein externer Benutzer bei der Appliance anmeldet, generiert das System eine Fehlermeldung “Benutzer existiert nicht” in der Datei `ns.log`. Der Grund dafür ist, dass das System den Befehl systemuser_systemcmdpolicy_binding ausführt, um die GUI für den Benutzer zu initialisieren.

LDAP-Authentifizierung (mit externen LDAP-Servern)

Sie können die NetScaler-Appliance so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren LDAP-Servern authentifiziert wird. Für die LDAP-Autorisierung sind identische Gruppennamen im Active Directory, auf dem LDAP-Server und auf der Appliance erforderlich. Die Zeichen und die Groß- und Kleinschreibung müssen ebenfalls identisch sein.

Weitere Informationen zu LDAP-Authentifizierungsrichtlinien finden Sie unter Thema LDAP-Authentifizierungsrichtlinien .

Standardmäßig ist die LDAP-Authentifizierung durch das SSL/TLS-Protokoll gesichert. Es gibt zwei Arten von sicheren LDAP-Verbindungen. Beim ersten Typ akzeptiert der LDAP-Server die SSL/TLS-Verbindung auf einem Port, der von dem Port getrennt ist, der zum Akzeptieren von leeren LDAP-Verbindungen verwendet wird. Nachdem Benutzer die SSL/TLS-Verbindung hergestellt haben, kann LDAP-Datenverkehr über die Verbindung gesendet werden. Der zweite Typ erlaubt sowohl unsichere als auch sichere LDAP-Verbindungen, und der einzelne Port verarbeitet es auf dem Server. In diesem Szenario erstellt der Client zunächst eine klare LDAP-Verbindung, um eine sichere Verbindung zu erstellen. Dann wird der **LDAP-Befehl** StartTLS über die Verbindung an den Server gesendet. Wenn der LDAP-Server StartTLS unterstützt, wird die Verbindung mithilfe von TLS in eine sichere LDAP-Verbindung konvertiert.

Die Portnummern für LDAP-Verbindungen lauten:

- 389 für ungesicherte LDAP-Verbindungen
- 636 für sichere LDAP-Verbindungen

- 3268 für Microsoft unsichere LDAP-Verbindungen
- 3269 für sichere LDAP-Verbindungen von Microsoft

LDAP-Verbindungen, die den Befehl StartTLS verwenden, verwenden die Portnummer 389. Wenn die Portnummern 389 oder 3268 auf der Appliance konfiguriert sind, versucht sie, StartTLS zum Herstellen der Verbindung zu verwenden. Wenn eine andere Portnummer verwendet wird, verwenden Verbindungsversuche SSL/TLS. Wenn StartTLS oder SSL/TLS nicht verwendet werden können, schlägt die Verbindung fehl.

Bei der Konfiguration des LDAP-Servers muss die Groß- und Kleinschreibung der Buchstaben auf dem Server und auf der Appliance übereinstimmen. Wenn das Stammverzeichnis des LDAP-Servers angegeben wird, werden auch alle Unterverzeichnisse durchsucht, um das Benutzerattribut zu finden. In großen Verzeichnissen kann dies die Leistung beeinträchtigen. Aus diesem Grund empfiehlt Citrix, eine bestimmte Organisationseinheit (OU) zu verwenden.

In der folgenden Tabelle sind Beispiele für den definierten Basisnamen (DN) aufgeführt.

LDAP-Server	Basis-DN
Microsoft Active Directory	DC=Citrix, DC=local
Novell eDirectory	dc=Citrix, dc=net
IBM Verzeichnisserver	cn=users
Lotus-Domino	OU=City, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	ou=People, dc=Citrix, dc=com

In der folgenden Tabelle sind Beispiele für den Bind Distinguished Name (DN) aufgeführt.

LDAP-Server	Bind DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=Citrix, DC=local
Novell eDirectory	cn=admin, dc=Citrix, dc=net
IBM Verzeichnisserver	LDAP_dn
Lotus-Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

LDAP-Server	Bind DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=Citrix, DC=local
Novell eDirectory	cn=admin, dc=Citrix, dc=net
IBM Verzeichnisserver	LDAP_dn
Lotus-Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

Konfigurieren Sie die LDAP-Benutzerauthentifizierung mithilfe der CLI

Führen Sie die folgenden Schritte aus, um die LDAP-Authentifizierung für externe Benutzer zu konfigurieren

LDAP-Richtlinie konfigurieren

Führen Sie an der Eingabeaufforderung Folgendes aus:

Schritt 1: Erstellen Sie eine LDAP-Aktion.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> } } >] [-authTimeout <positive_integer>] [-ldapBase
<string>] [-ldapBindDn <string>] { -ldapBindDnPassword } [-ldapLoginName <
string>] [-groupAttrName <string>] [-subAttributeName <string>]
```

Beispiel:

```
add authentication ldapAction ldap_act -serverIP <IP> -authTimeout 30 -
ldapBase "CN=xxxxx,DC=xxxx,DC=xxx"-ldapBindDn "CN=xxxxx,CN=xxxxx,DC=xxxx,DC
=xxx"-ldapBindDnPassword abcd -ldapLoginName sAMAccountName -groupattrName
memberOf -subAttributeName CN
```

Informationen zur Parameterbeschreibung finden Sie unter Referenz zu Authentifizierungs- und Berechtigungsbefehlen .

Schritt 2: Erstellen einer klassischen LDAP-Richtlinie.

```
add authentication ldapPolicy <name> <rule> [<reqAction>]
```

Beispiel:

```
add authentication ldappolicy ldap_pol_classic ns_true ldap_act
```


> **Hinweis**
>
> Sie können mit einer klassischen oder einer erweiterten LDAP-Richtlinie konfigurieren. Citrix empfiehlt jedoch die Verwendung einer erweiterten Authentifizierungsrichtlinie, da klassische Richtlinien ab der Version NetScaler 13.0 veraltet sind.

Schritt 3: Erstellen einer erweiterten LDAP-Richtlinie

```
add authentication Policy <name> <rule> [<reqAction>]
```

Beispiel:

```
add authentication policy ldap_pol_advance -rule true -action ldap_act
```

Schritt 4: Binden der LDAP-Richtlinie an das globale System

Gehen Sie in der Befehlszeile wie folgt vor:

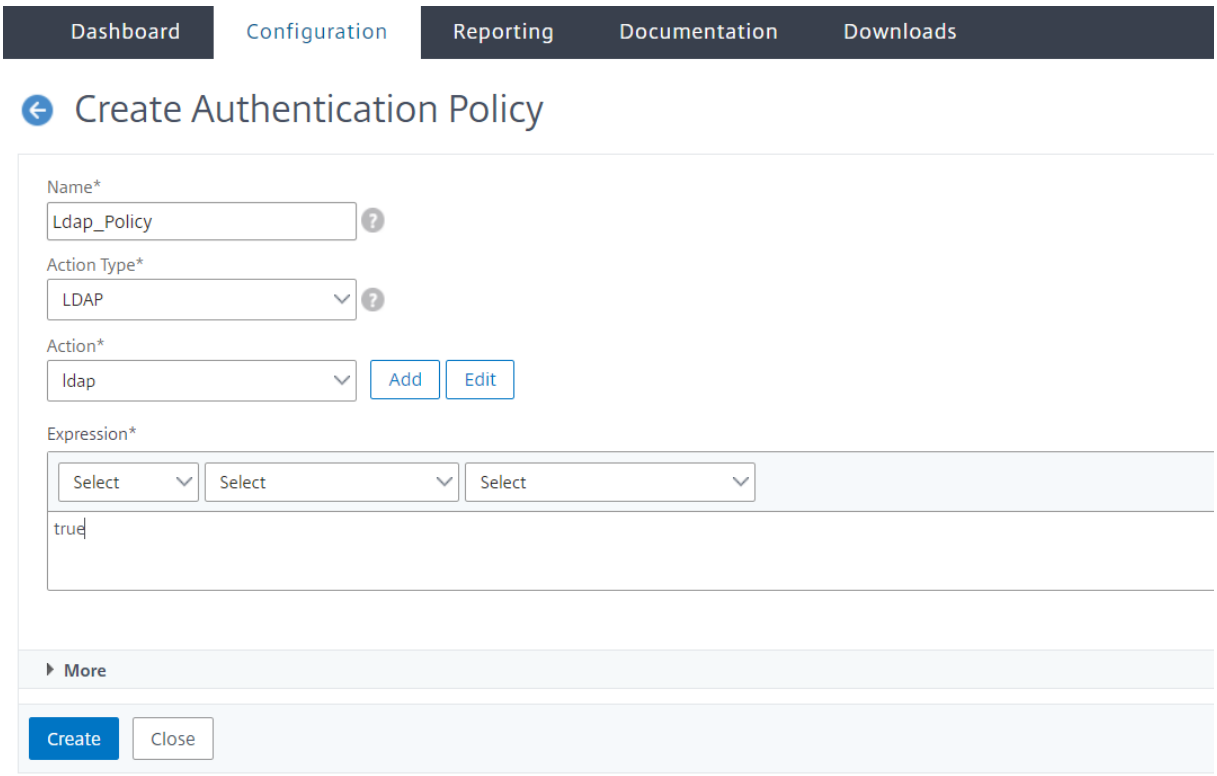
```
bind system global <policyName> [-priority <positive_integer]
```

Beispiel:

```
bind system global ldap_pol_advanced -priority 10
```

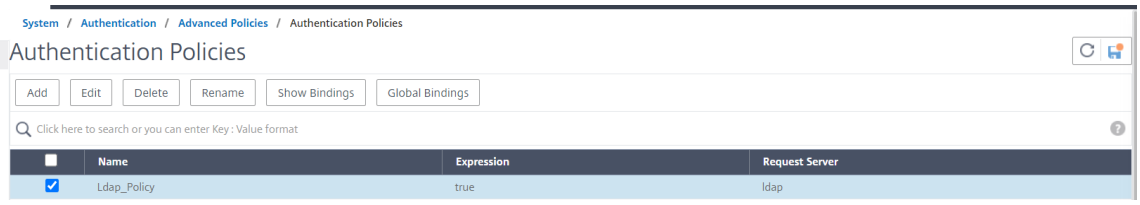
Konfigurieren Sie die LDAP-Benutzerauthentifizierung mithilfe der NetScaler GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie vom Typ LDAP zu erstellen.
3. Klicken Sie auf **Erstellen** und **Schließen**.

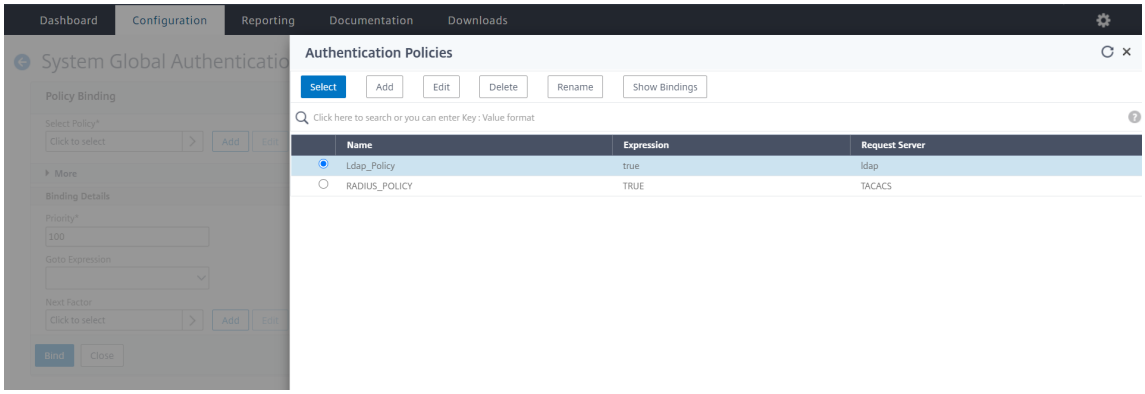


Binden Sie eine Authentifizierungsrichtlinie für die LDAP-Authentifizierung mithilfe der NetScaler GUI an das globale System

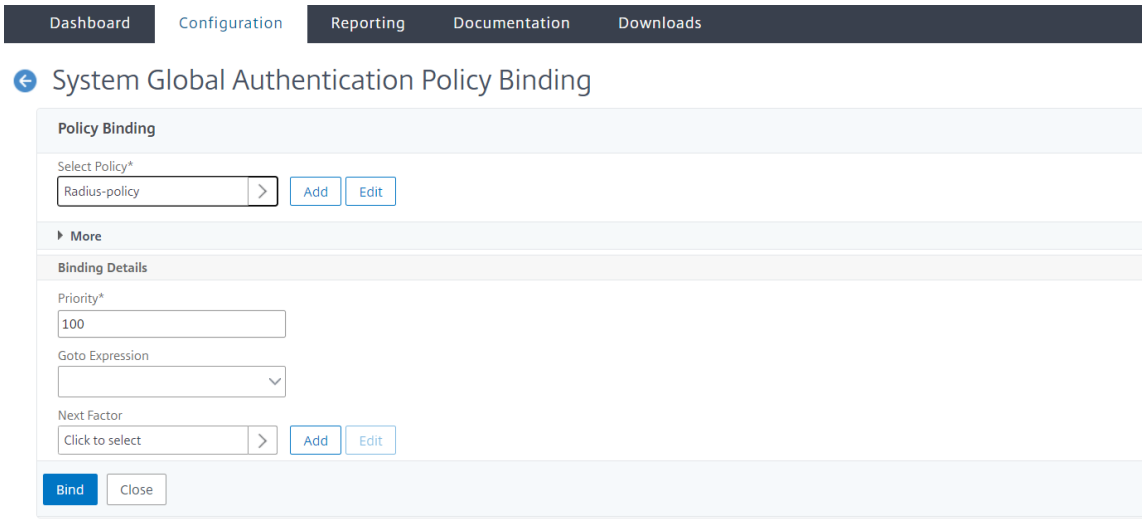
1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > Richtlinie für **Authentifizierungsrichtlinien**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**, um eine globale Systemauthentifizierungsrichtlinienbindung zu erstellen.
3. Klicken Sie auf **Globale Bindungen**.



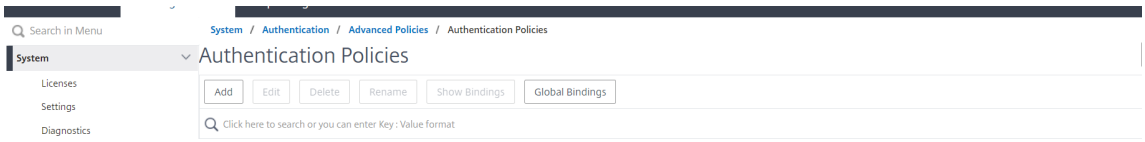
4. Wählen Sie ein Authentifizierungsprofil aus.



5. Wählen Sie die LDAP-Richtlinie aus.
6. Legen Sie auf der Seite **Bindung von System Global Authentication Policy** die folgenden Parameter fest:
   a) Wählen Sie Richtlinie aus .
   b) Verbindliche Angaben



7. Klicken Sie auf **Binden** und **Fertig**.
8. Klicken Sie auf **Globale Bindungen**, um zu bestätigen, dass die Richtlinie auf das globale System beschränkt ist.



Festlegen von Attributen im LDAP-Verzeichnis

Wenn Sie Hilfe bei der Ermittlung Ihrer LDAP-Verzeichnisattribute benötigen, können Sie diese einfach mit dem kostenlosen LDAP-Browser von Softerra nachschlagen.

Sie können den LDAP-Browser von der Softerra LDAP Administrator-Website unter herunterladen < http://www.ldapbrowser.com>. Legen Sie nach der Installation des Browsers die folgenden Attribute fest:

- Der Hostname oder die IP-Adresse Ihres LDAP-Servers.
- Der Port Ihres LDAP-Servers. Die Standardeinstellung ist 389.
- Das Basis-DN-Feld kann leer gelassen werden.
- Mithilfe der vom LDAP-Browser bereitgestellten Informationen können Sie den Basis-DN ermitteln, der für die Registerkarte Authentifizierung benötigt wird.
- Die Prüfung Anonyme Bindung bestimmt, ob der LDAP-Server Benutzeranmeldeinformationen benötigt, damit der Browser eine Verbindung zu ihm herstellen kann. Wenn der LDAP-Server Anmeldeinformationen benötigt, lassen Sie das Kontrollkästchen deaktiviert.

Nach Abschluss der Einstellungen zeigt der LDAP-Browser den Profilnamen im linken Fensterbereich an und stellt eine Verbindung zum LDAP-Server her.

Weitere Informationen finden Sie unter LDAP-Thema .

Schlüsselbasierte Authentifizierungsunterstützung für LDAP-Benutzer

Mit der schlüsselbasierten Authentifizierung können Sie jetzt die Liste der öffentlichen Schlüssel abrufen, die auf dem Benutzerobjekt im LDAP-Server über SSH gespeichert sind. Die NetScaler-Appliance muss während des rollenbasierten Authentifizierungsprozesses (RBA) öffentliche SSH-Schlüssel vom LDAP-Server extrahieren. Der abgerufene öffentliche Schlüssel, der mit SSH kompatibel ist, muss es Ihnen ermöglichen, sich über die RBA-Methode anzumelden.

Ein neues Attribut “sshPublicKey” wird in den Befehlen “add authentication ldapAction” und “set authentication ldapAction” eingeführt. Wenn Sie dieses Attribut verwenden, können Sie die folgenden Vorteile erhalten:

- Kann den abgerufenen öffentlichen Schlüssel speichern, und die LDAP-Aktion verwendet dieses Attribut, um SSH-Schlüsselinformationen vom LDAP-Server abzurufen.
- Kann Attributnamen von bis zu 24 KB extrahieren.

> **Hinweis**
>
> Der externe Authentifizierungsserver wie LDAP wird nur zum Abrufen von SSH-Schlüsselinformationen verwendet. Es wird nicht für den Authentifizierungszweck verwendet.

Es folgt ein Beispiel für den Ablauf von Ereignissen durch SSH:

- Der SSH-Daemon sendet eine AAA_AUTHENTICATE-Anforderung mit leerem Kennwortfeld an den Authentifizierungs-, Autorisierungs- und Überwachungs-Daemonport
- Wenn LDAP zum Speichern des öffentlichen SSH-Schlüssels konfiguriert ist, antworten Authentifizierung, Autorisierung und Überwachung mit dem Attribut `sshPublicKey` zusammen mit anderen Attributen.
- Der SSH-Daemon überprüft diese Schlüssel mit den Clientschlüsseln.
- Der SSH-Daemon übergibt den Benutzernamen in der Anforderungsnutzlast, und Authentifizierung, Autorisierung und Überwachung gibt die für diesen Benutzer spezifischen Schlüssel zusammen mit generischen Schlüsseln zurück.

Um das sshPublicKey -Attribut zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- Mit der Operation add können Sie das Attribut “sshPublicKey” hinzufügen, während Sie den Befehl `ldapAction` konfigurieren.

  ```
  add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr
  |*> | { -serverName <string> } } [-serverPort <port>] … [-Attribute1 <
  string>] … [-Attribute16 <string>][-sshPublicKey <string>][-authentication
   off]<!--NeedCopy-->
  ```

- Mit set operation können Sie das Attribut “sshPublicKey” zu einem bereits hinzugefügten ldapAction-Befehl konfigurieren.

  ```
  set authentication ldapAction <name> [-sshPublicKey <string>][-authentication
   off]<!--NeedCopy-->
  ```

RADIUS-Authentifizierung (mit externen RADIUS-Servern)

Sie können die NetScaler-Appliance so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren RADIUS-Servern authentifiziert wird. Wenn Sie RSA SecurID-, SafeWord- oder Gemalto Protiva-Produkte verwenden, verwenden Sie einen RADIUS-Server.

Weitere Informationen zu RADIUS-Authentifizierungsrichtlinien finden Sie unter RADIUS-Authentifizierung.

Ihre Konfiguration erfordert möglicherweise die Verwendung einer Netzwerkzugriffsserver-IP-Adresse (NAS-IP) oder einer Netzwerkzugriffsserver-ID (NAS-ID). Beachten Sie beim Konfigurieren der Appliance für die Verwendung eines RADIUS-Authentifizierungsservers die folgenden Richtlinien:

- Wenn Sie die Verwendung der NAS-IP aktivieren, sendet die Appliance ihre konfigurierte IP-Adresse an den RADIUS-Server und nicht an die Quell-IP-Adresse, die für den Aufbau der RADIUS-Verbindung verwendet wurde.
- Wenn Sie die NAS-ID konfigurieren, sendet die Appliance den Bezeichner an den RADIUS-Server. Wenn Sie die NAS-ID nicht konfigurieren, sendet die Appliance ihren Hostnamen an den RADIUS-Server.

- Wenn die NAS-IP-Adresse aktiviert ist, ignoriert die Appliance jede NAS-ID, die sie für die Kommunikation mit dem RADIUS-Server verwendet hat.

Konfigurieren Sie die RADIUS-Benutzerauthentifizierung mithilfe der CLI

Führen Sie an der Eingabeaufforderung Folgendes aus:

Schritt 1: Erstellen einer RADIUS-Aktion

```
add authentication radiusaction <name> -serverip <ip> -radkey <key> -
radVendorID <id> -radattributetype <value>
```

Wobei das
`radVendorID` RADIUS-Hersteller-ID-Attribut, das für die Extraktion von RADIUS-Gruppen
`radAttributeType` RADIUS-Attributtyp, der für die Extraktion von RADIUS-Gruppen

Beispiel:

```
add authentication radiusaction RADserver531 rad_action -serverip 1.1.1.1 -
radkey key123 -radVendorID 66 -radattributetype 6
```

Schritt 2: Erstellen Sie eine klassische RADIUS-Richtlinie.

```
add authentication radiusPolicy <name> <rule> [<reqAction>]
```

Beispiel:

```
add authentication radiuspolicy radius_pol_classic ns_true radius_act
```

> **Hinweis**
>
> Sie können mit einer klassischen oder einer erweiterten RADIUS-Richtlinie konfigurieren. Citrix empfiehlt Ihnen, die erweiterte Authentifizierungsrichtlinie zu verwenden, da klassische Richtlinien ab dem Release NetScaler 13.0 veraltet sind.

Schritt 3: Erstellen Sie eine erweiterte RADIUS-Richtlinie

```
add authentication policy <policyname> -rule true -action <radius action
name>
```

Beispiel:

```
add authentication policy rad_pol_advanced -rule true -action radserver531rad_action
```

Schritt 4: Binden Sie die RADIUS-Richtlinie an das globale System.

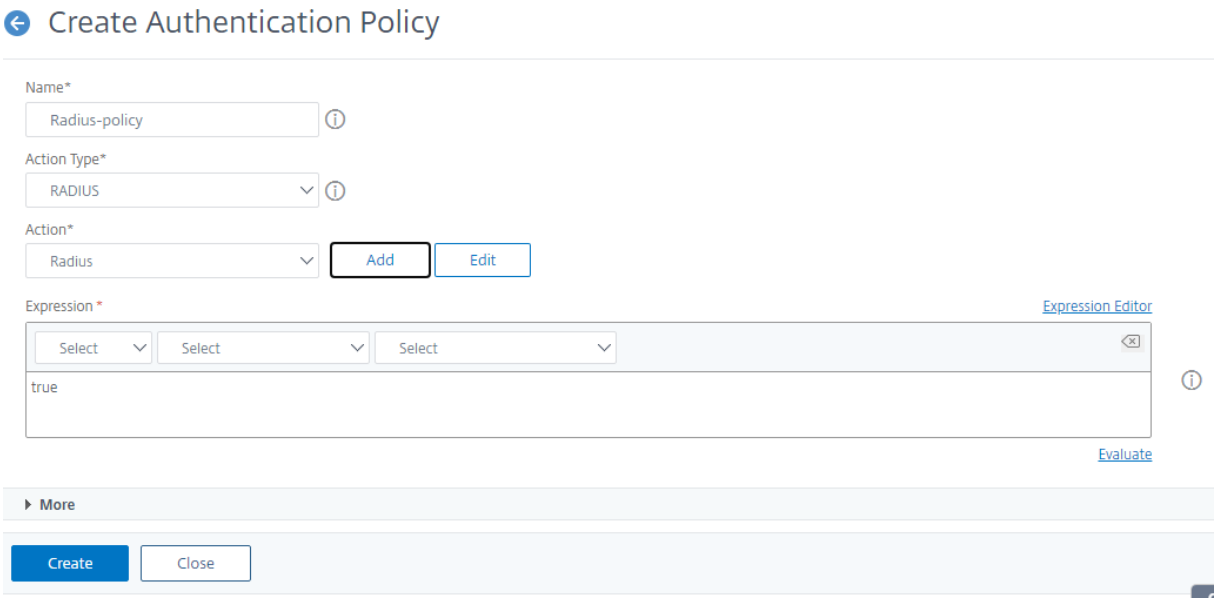
```
bind system global <policyName> -priority <positive_integer
```

Beispiel:

```
bind system global radius_pol_advanced -priority 10
```

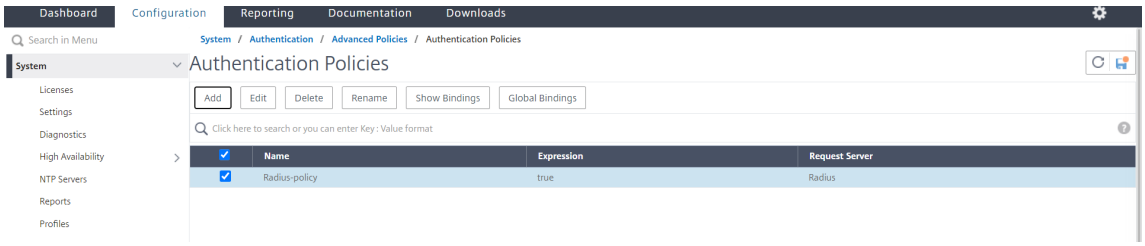

Konfigurieren Sie die RADIUS-Benutzerauthentifizierung über die GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie vom Typ RADIUS zu erstellen.
3. Klicken Sie auf **Erstellen** und **Schließen**.



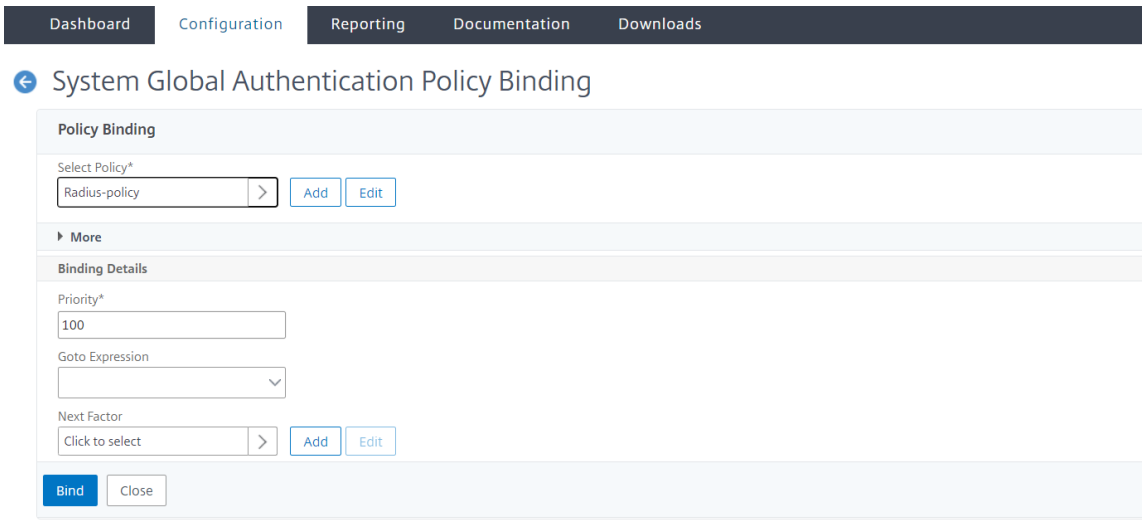
Binden Sie die Authentifizierungsrichtlinie für die RADIUS-Authentifizierung über die GUI an das globale System

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**, um eine globale Systemauthentifizierungsrichtlinienbindung zu erstellen.
3. Klicken Sie auf **Globale Bindungen**.

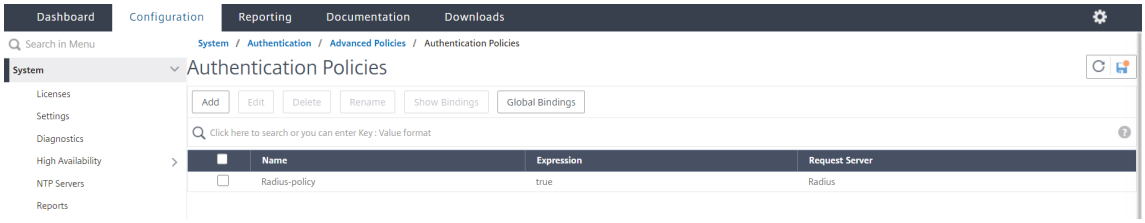


4. Wählen Sie RADIUS.
5. Legen Sie auf der Seite **Bindung von System Global Authentication Policy** die folgenden Parameter fest:

   a) Wählen Sie eine Richtlinie.
   b) Verbindliche Angaben.



6. Klicken Sie auf **Binden** und **Schließen**.
7. Klicken Sie auf **Globale Bindungen**, um zu bestätigen, dass die Richtlinie an das globale System gebunden ist.



RADIUS-Benutzerauthentifizierungsprotokolle wählen

Die NetScaler-Appliance unterstützt Implementierungen von RADIUS, die für die Verwendung mehrerer Protokolle für die Benutzerauthentifizierung konfiguriert sind, darunter:

- Password Authentication Protocol
- Challenge-Handshake-Authentifizierungsprotokoll (CHAP)
- Microsoft Challenge-Handshake-Authentifizierungsprotokoll (MS-CHAP Version 1 und Version 2)

Wenn Ihre Bereitstellung für die Verwendung der RADIUS-Authentifizierung konfiguriert ist und Ihr RADIUS-Server mit einem Kennwortauthentifizierungsprotokoll konfiguriert ist. Sie können die Benutzerauthentifizierung verstärken, indem Sie dem RADIUS-Server ein starkes gemeinsames Geheimnis zuweisen. Starke gemeinsame Geheimnisse von RADIUS bestehen aus zufälligen Sequenzen von Groß- und Kleinbuchstaben, Zahlen und Satzzeichen und sind mindestens 22 Zeichen lang. Verwenden Sie nach Möglichkeit ein Programm zur zufälligen Zeichengenerierung, um gemeinsam genutzte RADIUS-Geheimnisse zu ermitteln.

Um den RADIUS-Datenverkehr weiter zu schützen, weisen Sie jeder Appliance oder jedem virtuellen Server einen anderen gemeinsamen Schlüssel zu. Wenn Sie Clients auf dem RADIUS-Server definieren, können Sie jedem Client auch ein separates Shared Secret zuweisen. Außerdem müssen Sie jede Richtlinie, die die RADIUS-Authentifizierung verwendet, separat konfigurieren.

IP-Adressextraktion konfigurieren

Sie können die Appliance so konfigurieren, dass sie die IP-Adresse von einem RADIUS-Server extrahiert. Wenn sich ein Benutzer beim RADIUS-Server authentifiziert, gibt der Server eine gerahmte IP-Adresse zurück, die dem Benutzer zugewiesen ist. Die folgenden Attribute sind für die Extraktion von IP-Adressen aufgeführt:

- Ermöglicht einem Remote-RADIUS-Server, eine IP-Adresse aus dem internen Netzwerk für einen an der Appliance angemeldeten Benutzer bereitzustellen.
- Ermöglicht die Konfiguration für jedes RADIUS-Attribut mit dem Typ IP-Adresse, einschließlich der Anbieter codiert.

Wenn Sie den RADIUS-Server für die IP-Adressenextraktion konfigurieren, konfigurieren Sie die Hersteller-ID und den Attributtyp.

Die Hersteller-ID ermöglicht es dem RADIUS-Server, dem Client eine IP-Adresse aus einem Pool von IP-Adressen zuzuweisen, die auf dem RADIUS-Server konfiguriert sind. Die Hersteller-ID und die Attribute werden verwendet, um die Zuordnung zwischen dem RADIUS-Client und dem RADIUS-Server herzustellen. Die Hersteller-ID ist das Attribut in der RADIUS-Antwort, das die IP-Adresse des internen Netzwerks bereitstellt. Ein Wert von Null gibt an, dass das Attribut nicht herstellercodiert ist. Der Attributtyp ist das Remote-IP-Adressattribut in einer RADIUS-Antwort. Der Mindestwert ist eins und der Höchstwert ist 255.

Eine übliche Konfiguration ist das Extrahieren der *gerahmten IP-Adresse* des **RADIUS-Attributs** Die Lieferanten-ID ist auf Null gesetzt oder nicht angegeben. Der Attributtyp ist auf acht festgelegt.

Gruppen-Extraktion für RADIUS über die GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Radius**, und wählen Sie eine Richtlinie aus.
2. Wählen oder erstellen Sie eine RADIUS-Richtlinie.
3. Legen Sie auf der Seite **“Authentifizierungs-RADIUS-Server konfigurieren** “ die folgenden Parameter fest.
    a) **Lieferanten-ID der**
    b) **Gruppen-Attributtyp**
4. Klicken Sie auf **OK** und auf **Schließen**.

TACACS+-Authentifizierung (unter Verwendung externer TACACS+-Server)

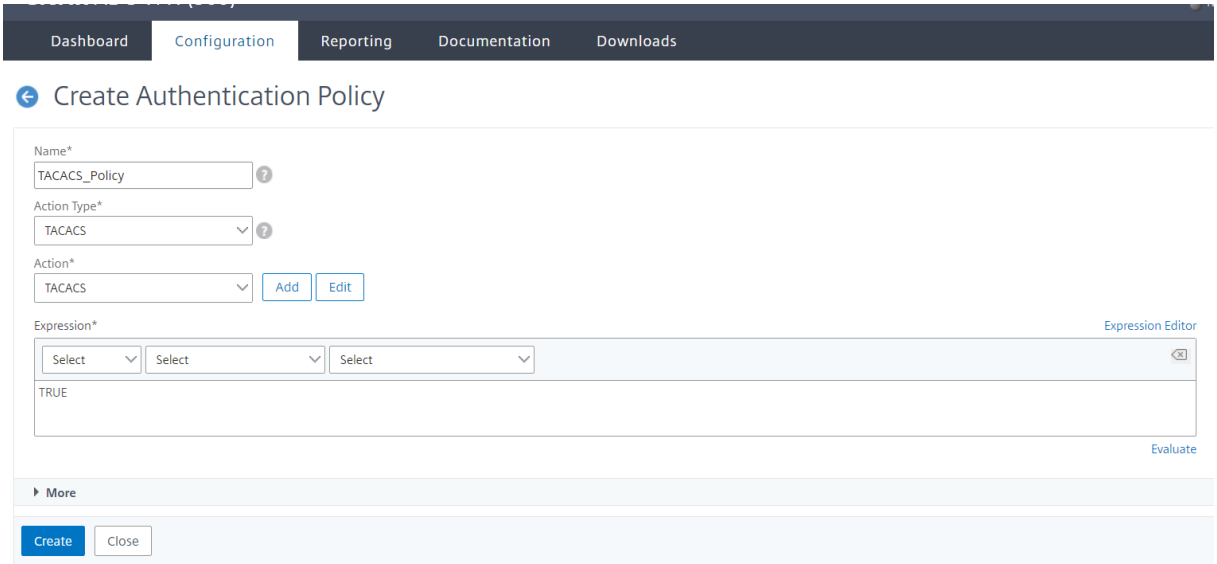
> **Wichtig**
>
> - Citrix empfiehlt, keine TACACS-bezogenen Konfigurationen zu ändern, wenn Sie einen Befehl “clear ns config” ausführen.
> - Die TACACS-bezogene Konfiguration im Zusammenhang mit erweiterten Richtlinien wird gelöscht und erneut angewendet, wenn der Parameter `RBAconfig` im Befehl “clear ns config” für erweiterte Richtlinien auf NO gesetzt ist.
> - Wenn der Parameter `RBAconfig` im Rahmen des Vorgangs “Konfiguration löschen” auf NEIN gesetzt ist, behält NetScaler zusätzlich zu den RBA-Konfigurationen und TACACS-Richtlinien die Verwaltungszugriffssitzungen bei.

Sie können einen TACACS+-Server für die Authentifizierung konfigurieren. Ähnlich wie bei der RADIUS-Authentifizierung verwendet TACACS+ einen geheimen Schlüssel, eine IP-Adresse und die Portnummer. Die Standardportnummer ist 49. Um die Appliance für die Verwendung eines TACACS+-Servers zu konfigurieren, geben Sie die Server-IP-Adresse und das TACACS+-Geheimnis an. Sie müssen den Port nur angeben, wenn die verwendete Serverportnummer etwas anderes als die Standardportnummer 49 ist.

Weitere Informationen finden Sie unter TACACS-Authentifizierung.

Konfigurieren Sie die TACACS+-Authentifizierung mit der GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie vom Typ TACACS zu erstellen.
3. Klicken Sie auf **Erstellen** und **Schließen**.



Nachdem die TACACS+-Servereinstellungen auf der Appliance konfiguriert wurden, binden Sie die

Richtlinie an die globale Systementität.

Binden Sie Authentifizierungsrichtlinien mithilfe der CLI an die globale Systemeinheit

Wenn die Authentifizierungsrichtlinien konfiguriert sind, binden Sie die Richtlinien an die globale Entität des Systems.

Gehen Sie in der Befehlszeile wie folgt vor:

```
bind system global <policyName> [-priority <positive_integer>]
```

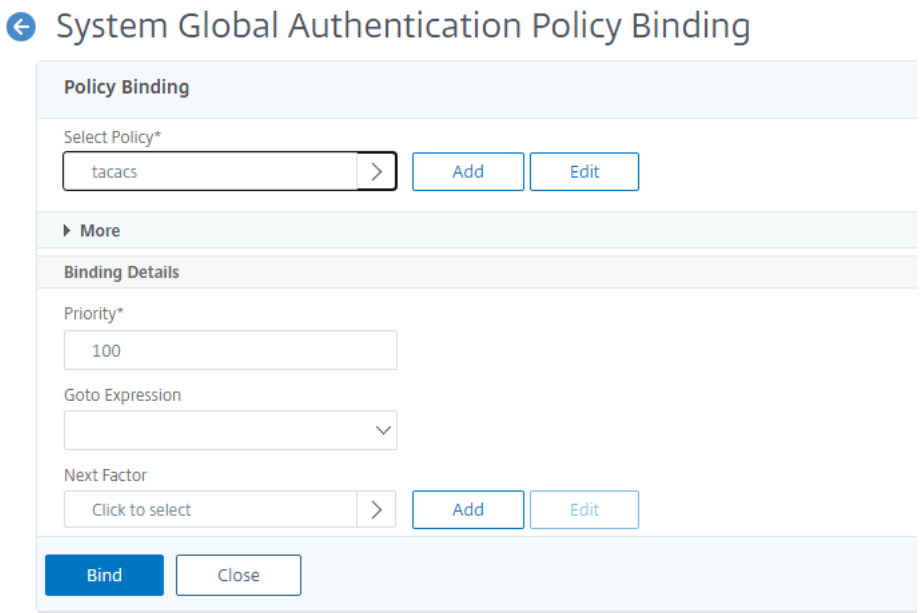
Beispiel:

```
bind system global pol_classic -priority 10
```

Lesen Sie auch den Citrix-Artikel CTX113820, um mehr über externe Authentifizierung mit TACACS zu erfahren.

Binden Sie Authentifizierungsrichtlinien an die globale Systemeinheit über die GUI

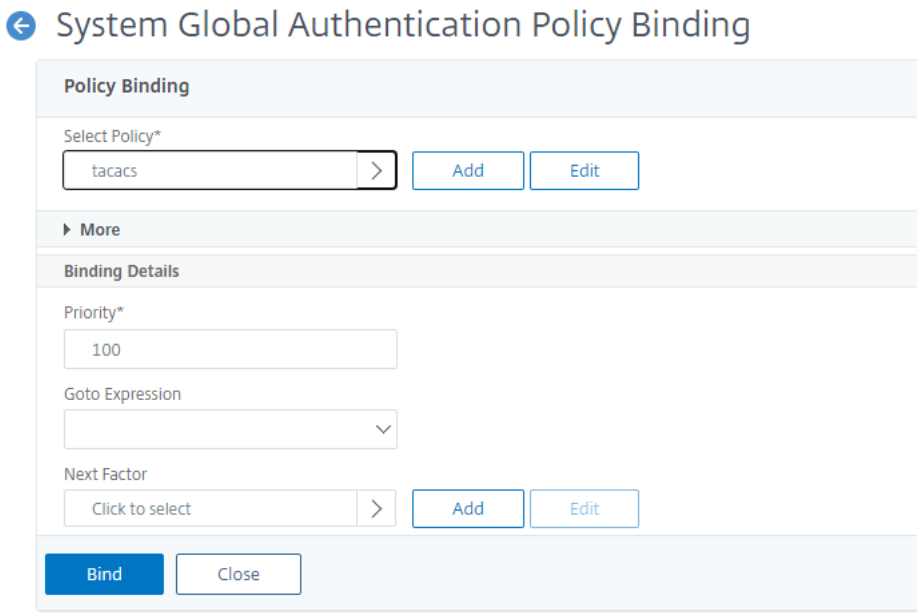
1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Authentifizierungsrichtlinien > Richtlinie**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**, um eine globale Systemauthentifizierungsrichtlinienbindung zu erstellen.
3. Klicken Sie auf **Globale Bindungen**.



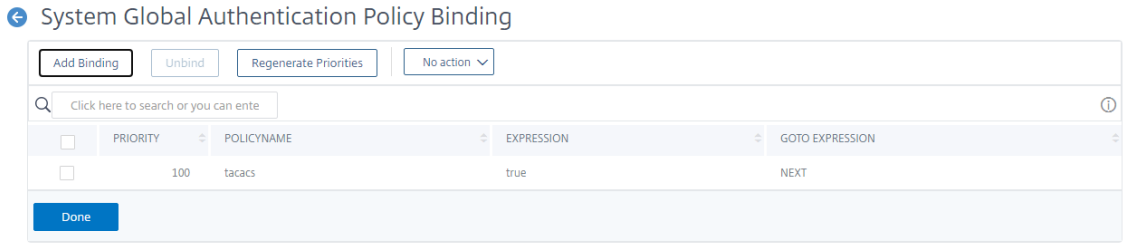
4. Wählen Sie die TACACS-Richtlinie.

5. Legen Sie auf der Seite Bindung von System Global Authentication Policy die folgenden Parameter fest:

   a) Wählen Sie Richtlinie aus .
   b) Verbindliche Angaben



6. Klicken Sie auf **Binden** und **Schließen**.
7. Klicken Sie auf **Globale Bindungen**, um die an das globale System gebundene Richtlinie zu bestätigen.



Weitere Informationen zur Extraktion der TACACS-Gruppe finden Sie im Citrix Artikel CTX220024.

Anzahl der erfolglosen Anmeldeversuche für externe Benutzer anzeigen

Die NetScaler-Appliance zeigt dem externen Benutzer die Anzahl der ungültigen Anmeldeversuche an, wenn Sie mindestens eine nicht erfolgreiche Anmeldung versuchen, bevor Sie sich erfolgreich bei der NetScaler Verwaltungskonsole anmelden.

> **Hinweis**
>
> Derzeit unterstützt NetScaler nur die interaktive Tastaturauthentifizierung für externe Benutzer, bei denen der Parameter „PersistentLoginAttempts“ im Systemparameter aktiviert ist.

Geben Sie in der Befehlszeile Folgendes ein:

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED )]
```

Beispiel:

```
set aaa parameter -maxloginAttempts 5 -failedLoginTimeout 4 -persistentLoginAttempts
 ENABLED
```

```
1  Following msg will be seen to external user when he tries 1 invalid
       login attempt before successfully login to the ADC management access
       .
2
3  Connection established.
4  To escape to local shell, press 'Ctrl+Alt+]'.
5  ##############################################################################

6  #

       #
7  #        WARNING: Access to this system is for authorized users only
              #
8  #         Disconnect IMMEDIATELY if you are not an authorized user!
               #
9  #

       #
10 ##############################################################################


11
12
13 WARNING! The remote SSH server rejected X11 forwarding request.
14 Last login: Mon Aug 24 17:09:00 2020 from 10.10.10.10
15
16 The number of unsuccessful login attempts since the last successful
       login : 1
17 Done
18 >
19 The number of unsuccessful login attempts since the last successful
       login : 1
20 Done
```



```
21 >
22 <!--NeedCopy-->
```

Schlüsselbasierte SSH-Authentifizierung für lokale Systembenutzer

May 11, 2023

Um einen sicheren Benutzerzugriff für die NetScaler-Appliance zu erhalten, können Sie die Public-Key-Authentifizierung des SSH-Servers verwenden. Die schlüsselbasierte SSH-Authentifizierung wird aus den folgenden Gründen der herkömmlichen Authentifizierung auf Basis von Benutzernamen oder Passwort vorgezogen:

- Bietet eine bessere kryptografische Stärke als Benutzerkennwörter.
- Eliminiert die Notwendigkeit, sich an komplizierte Kennwörter zu erinnern, und verhindert Schulter-Surf-Angriffe, die bei Verwendung von Kennwörtern möglich sind.
- Bietet eine passwortlose Anmeldung, um Automatisierungsszenarien sicherer zu machen.

NetScaler unterstützt die schlüsselbasierte SSH-Authentifizierung, indem es das Konzept des öffentlichen und des privaten Schlüssels anwendet. Die schlüsselbasierte SSH-Authentifizierung in NetScaler kann entweder für einen bestimmten Benutzer oder für alle lokalen Benutzer aktiviert werden.

> **Hinweis**
>
> Die Funktion wird nur für lokale NetScaler-Benutzer und nicht für externe Benutzer unterstützt.

Schlüsselbasierte SSH-Authentifizierung für lokale Systembenutzer

In einer NetScaler-Appliance kann ein Administrator eine schlüsselbasierte SSH-Authentifizierung für einen sicheren Systemzugriff einrichten. Wenn sich ein Benutzer mit einem privaten Schlüssel bei NetScaler anmeldet, authentifiziert das System den Benutzer mit dem auf der Appliance konfigurierten öffentlichen Schlüssel.

Konfigurieren Sie die schlüsselbasierte SSH-Authentifizierung für die lokalen NetScaler-Systembenutzer mithilfe der CLI

Die folgende Konfiguration hilft Ihnen bei der Konfiguration der schlüsselbasierten Authentifizierung für lokale NetScaler-Systembenutzer.

1. Melden Sie sich mit Administratoranmeldeinformationen bei einer NetScaler-Appliance an.
2. Standardmäßig greift Ihre `sshd_config` Datei auf diesen Pfad zu: **authorizedKeysFile /nsconfig/ssh/authorized_keys**.

3. **Hängen Sie den öffentlichen Schlüssel an die Datei authorized_keys an: /nsconfig/ssh/authorized_keys.** Der Dateipfad für `sshd_config` ist `/etc/sshd_config`.
4. Kopieren Sie die `sshd_config` Datei in, `/nsconfig` um sicherzustellen, dass die Änderungen auch nach dem Neustart der Appliance erhalten bleiben.
5. Sie können den folgenden Befehl verwenden, um Ihren `sshd` Prozess neu zu starten.

```
    kill -HUP `cat /var/run/sshd.pid`
<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn die Datei authorized_keys nicht verfügbar ist, müssen Sie zuerst eine erstellen und dann den öffentlichen Schlüssel anhängen. **Stellen Sie sicher, dass die Datei über die folgenden Berechtigungen für die authorized_keys**verfügt.
>
> `root@NetScaler## chmod 0644 authorized_keys`

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /nsconfig/ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file
<!--NeedCopy-->
```

Benutzerspezifische, schlüsselbasierte SSH-Authentifizierung für lokale Systembenutzer

In einer NetScaler-Appliance kann ein Administrator jetzt eine benutzerspezifische, schlüsselbasierte SSH-Authentifizierung für einen sicheren Systemzugriff einrichten. Der Administrator muss zuerst die Option `Authorizedkeysfile` in der Datei `sshd_config` konfigurieren und dann den öffentlichen Schlüssel für einen Systembenutzer in die Datei `authorized_keys` einfügen.

> **Hinweis**
>
> Wenn die Datei authorized_keys für einen Benutzer nicht verfügbar ist, muss der Administrator zuerst eine erstellen und ihr dann den öffentlichen Schlüssel hinzufügen.

Konfigurieren Sie die benutzerspezifische schlüsselbasierte SSH-Authentifizierung mithilfe der CLI

Das folgende Verfahren hilft Ihnen bei der Konfiguration der benutzerspezifischen schlüsselbasierten SSH-Authentifizierung für lokale NetScaler-Systembenutzer.

1. Melden Sie sich mit Administratoranmeldeinformationen bei einer NetScaler-Appliance an.
2. Greifen Sie an der Shell-Eingabeaufforderung auf die `sshd_config` Datei zu und fügen Sie die folgende Konfigurationszeile hinzu:

   `AuthorizedKeysFile ~/.ssh/authorized_keys`

   > **Hinweis**
   >
   > Das ~ ist das Home-Verzeichnis und unterscheidet sich für verschiedene Benutzer. Es erweitert sich auf das andere Home-Verzeichnis.

3. Ändern Sie das Verzeichnis in den Systembenutzerordner und fügen Sie die öffentlichen Schlüssel in der `authorized_keys` Datei hinzu.

   `/var/pubkey/<username>/.ssh/authorized_keys`

Nachdem Sie die vorherigen Schritte abgeschlossen haben, starten Sie den `sshd` Vorgang auf Ihrer Appliance mit dem folgenden Befehl neu:

```
    kill -HUP `cat /var/run/sshd.pid`

<!--NeedCopy-->
```

> **Hinweis**
>
> Wenn die Datei authorized_keys nicht verfügbar ist, müssen Sie zuerst eine erstellen und dann den öffentlichen Schlüssel hinzufügen.

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /var/pubkey/<username>/
root@ns# ls
.ssh
root@ns# cd .ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file

<!--NeedCopy-->
```


Lesen Sie auch den Citrix Artikel CTX109011, um zu erfahren, wie sicherer SSH-Zugriff auf NetScaler Appliance funktioniert.

Zwei-Faktor-Authentifizierung für Systembenutzer und externe Benutzer

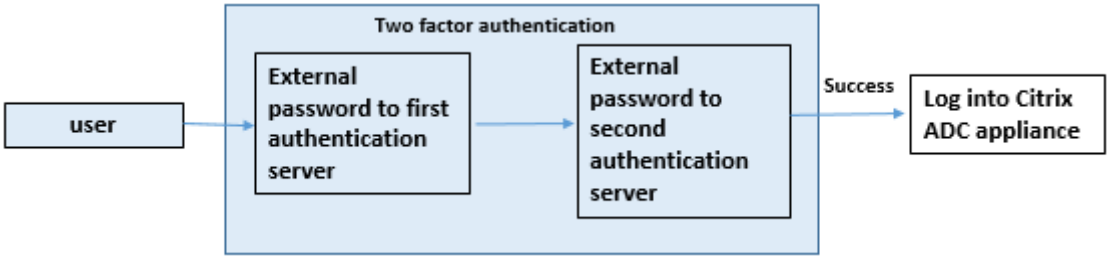
May 11, 2023

Die Zwei-Faktor-Authentifizierung ist ein Sicherheitsmechanismus, bei dem eine NetScaler-Appliance einen Systembenutzer auf zwei Authentifizierungsebenen authentifiziert. Die Appliance gewährt dem Benutzer erst Zugriff, nachdem die Passwörter auf beiden Authentifizierungsebenen erfolgreich validiert wurden. Wenn ein Benutzer lokal authentifiziert ist, muss das Benutzerprofil in der NetScaler-Datenbank erstellt werden. Wenn der Benutzer extern authentifiziert wird, müssen der Benutzername und das Kennwort mit der auf dem externen Authentifizierungsserver registrierten Benutzeridentität übereinstimmen.

> **Hinweis**
>
> Die Zwei-Faktor-Authentifizierungsfunktion funktioniert nur ab NetScaler 12.1 Build 51.16.

So funktioniert die Zwei-Faktor-Authentifizierung

Stellen Sie sich einen Benutzer vor, der versucht, sich bei einer NetScaler-Appliance anzumelden. Der angeforderte Anwendungsserver sendet den Benutzernamen und das Kennwort an den ersten externen Authentifizierungsserver (RADIUS, TACACS, LDAP oder AD). Sobald der Benutzername und das Kennwort validiert sind, wird der Benutzer zu einer zweiten Authentifizierungsebene aufgefordert. Der Benutzer kann jetzt das zweite Kennwort eingeben. Nur wenn beide Passwörter korrekt sind, darf der Benutzer auf die NetScaler-Appliance zugreifen. Das folgende Diagramm veranschaulicht, wie die Zwei-Faktor-Authentifizierung für eine NetScaler-Appliance funktioniert.



Im Folgenden sind die verschiedenen Anwendungsfälle für die Konfiguration der Zwei-Faktor-Authentifizierung für externe Benutzer und Systembenutzer aufgeführt.

Sie können die Zwei-Faktor-Authentifizierung auf einer NetScaler-Appliance auf verschiedene Arten konfigurieren. Im Folgenden sind die verschiedenen Konfigurationsszenarien für die Zwei-Faktor-Authentifizierung auf einer NetScaler-Appliance aufgeführt.

1. Zwei-Faktor-Authentifizierung (2FA) für NetScaler, GUI, CLI, API und SSH.
2. Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer deaktiviert.
3. Die externe Authentifizierung ist mit richtlinienbasierter lokaler Authentifizierung für Systembenutzer aktiviert.
4. Die externe Authentifizierung ist für Systembenutzer mit aktivierter lokaler Authentifizierung deaktiviert.
5. Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer aktiviert.
6. Externe Authentifizierung für ausgewählte LDAP-Benutzer aktiviert

Anwendungsfall 1: Zwei-Faktor-Authentifizierung (2FA) über NetScaler-, GUI-, CLI-, API- und SSH-Schnittstellen

Die Zwei-Faktor-Authentifizierung ist aktiviert und für den gesamten NetScaler-Verwaltungszugriff für GUI, API und SSH verfügbar.

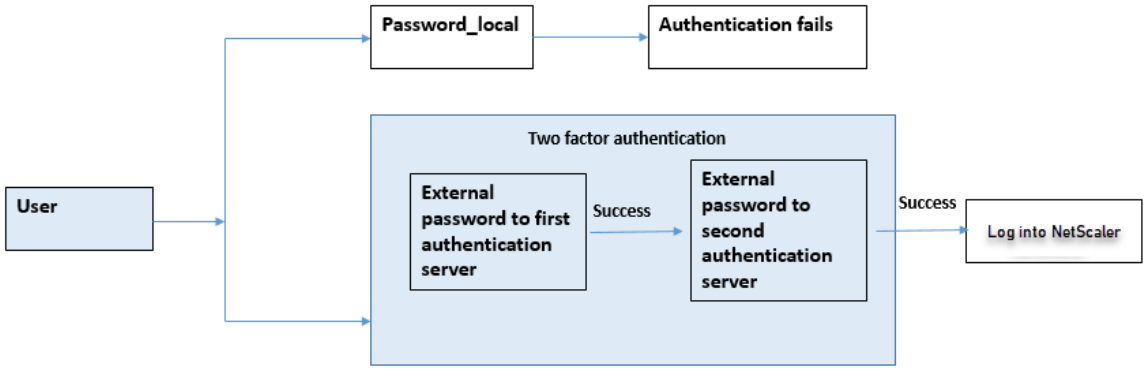
Anwendungsfall 2: Unterstützung der Zwei-Faktor-Authentifizierung auf externen Authentifizierungsservern wie LDAP, RADIUS, Active Directory und TACACS

Sie können die Zwei-Faktor-Authentifizierung auf den folgenden externen Authentifizierungsservern für die Benutzerauthentifizierung der ersten und zweiten Ebene konfigurieren.

- RADIUS
- LDAP
- Active Directory
- TACACS

Anwendungsfall 3: Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer deaktiviert

Sie beginnen den Authentifizierungsprozess, indem Sie die externe Authentifizierungsoption aktivieren und die lokale Authentifizierung für Systembenutzer deaktivieren.



Führen Sie die folgenden Schritte über die Befehlszeilenschnittstelle aus:

1. Authentifizierungsaktion für die LDAP-Richtlinie hinzufügen
2. Authentifizierungsrichtlinie für LDAP-Richtlinie hinzufügen
3. Authentifizierungsaktion für die RADIUS-Richtlinie hinzufügen
4. Fügen Sie eine Authentifizierungsrichtlinie für die RADIUS-Richtlinie hinzu
5. Authentifizierungs-Anmeldeschema hinzufügen
6. Fügen Sie das Label für die Authentifizierungsrichtlinie hinzu und binden Sie es an den RADIUS-Server
7. Globale Authentifizierung des Bind-Systems für die LDAP-Richtlinie
8. Deaktivieren Sie die lokale Authentifizierung im Systemparameter

Authentifizierungsaktion für den LDAP-Server hinzufügen (Authentifizierung der ersten Ebene)

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Authentifizierungsrichtlinie für den LDAP-Server hinzufügen (Authentifizierung der ersten Ebene)

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <ldap policy name> -rule true -action <ldap
```



```
action name>
```

Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Authentifizierungsaktion für RADIUS-Server hinzufügen (Authentifizierung der zweiten Ebene)

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Beispiel:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Authentifizierungsrichtlinie für RADIUS-Server hinzufügen (Authentifizierung der zweiten Ebene)

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <radius policy name> -rule true -action <rad
action name>
```

Beispiel:

```
add authentication policy radpol11 -rule true -action radact1
```

Authentifizierungs-Anmeldeschema hinzufügen

Sie können das Anmeldeschema “SingleAuth.xml” für Systembenutzer verwenden, um das zweite Kennwort für die NetScaler-Appliance anzugeben. Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication loginSchema <login schema name> -authenticationSchema
LoginSchema/SingleAuth.xml
```

Beispiel:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Fügen Sie das Label für die Authentifizierungsrichtlinie hinzu und binden Sie es an den RADIUS-Server

Geben Sie in der Befehlszeile Folgendes ein:


```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

```
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
```

```
bind authentication policylabel label1 -policyName radpol11 -priority 1
```

Binden Sie das Authentifizierungssystem global für die LDAP-Richtlinie

Geben Sie in der Befehlszeile Folgendes ein:

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Beispiel:

```
bind system global pol11 -priority 1 -nextFactor label1
```

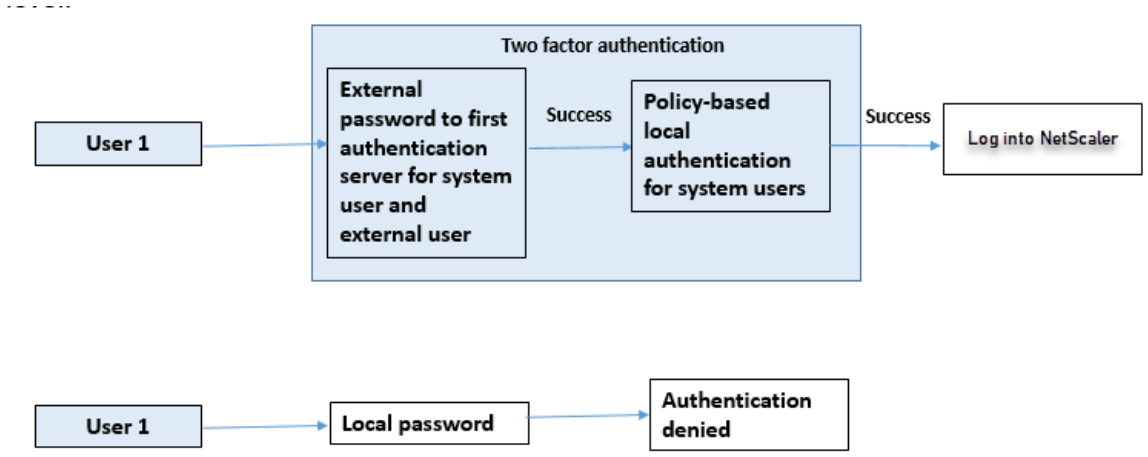
Deaktivieren Sie die lokale Authentifizierung im Systemparameter

Geben Sie in der Befehlszeile Folgendes ein:

```
set system parameter -localauth disabled
```

Anwendungsfall 4: Externe Authentifizierung für Systembenutzer mit angehängter lokaler Authentifizierungsrichtlinie aktiviert

In diesem Szenario darf sich der Benutzer mithilfe der Zwei-Faktor-Authentifizierung bei der Appliance anmelden, wobei die Bewertung der lokalen Authentifizierungsrichtlinien auf der zweiten Ebene der Benutzeridentifikation erfolgt.



Führen Sie die folgenden Schritte über die Befehlszeilenschnittstelle aus.

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Authentifizierungsrichtlinie für LDAP-Richtlinie hinzufügen
3. Lokale Authentifizierungsrichtlinie hinzufügen
4. Bezeichnung für die Authentifizierungsrichtlinie hinzufügen
5. LDAP-Richtlinie als globales System binden
6. Deaktivieren Sie die lokale Authentifizierung im Systemparameter

Authentifizierungsaktion für den LDAP-Server hinzufügen (Authentifizierung der ersten Ebene)

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name -ssoNameAttribute name
```

Authentifizierungsrichtlinie für den LDAP-Server hinzufügen (Authentifizierung der ersten Ebene)

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```


Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Fügen Sie eine lokale Authentifizierungsrichtlinie für Systembenutzer hinzu (Authentifizierung auf zweiter Ebene)

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <policy> -rule <rule> -action <action name>
```

Beispiel:

```
add authentication policy local_policy -rule true -action LOCAL
```

Bezeichnung für die Authentifizierungsrichtlinie hinzufügen und binden

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

> **Hinweis**
>
> Für den Verwaltungszugriff muss der Richtlinientyp RBA_REQ sein.

Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel label1 -policyName radpol11 -priority 1 -
gotoPriorityExpression NEXT
```

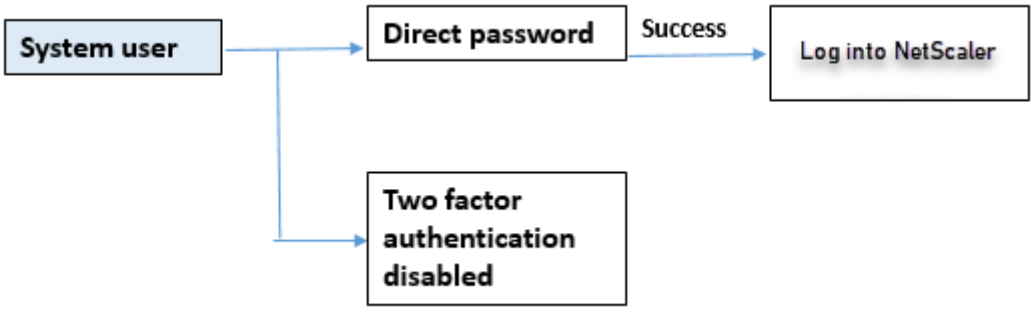
Deaktivieren Sie die lokale Authentifizierung im Systemparameter

Geben Sie in der Befehlszeile Folgendes ein:

```
set system parameter -localauth disabled
```


Anwendungsfall 5: Externe Authentifizierung deaktiviert und lokale Authentifizierung für Systembenutzer aktiviert

Wenn für den Benutzer “ExternalAuth” deaktiviert ist, bedeutet dies, dass der Benutzer auf dem Authentifizierungsserver nicht existiert. Der Benutzer wird beim externen Authentifizierungsserver nicht authentifiziert, auch wenn ein Benutzer mit demselben Benutzernamen auf dem externen authentifizierten Server existiert. Der Benutzer ist lokal authentifiziert.



Um das Systembenutzerkennwort zu aktivieren und die externe Authentifizierung zu deaktivieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

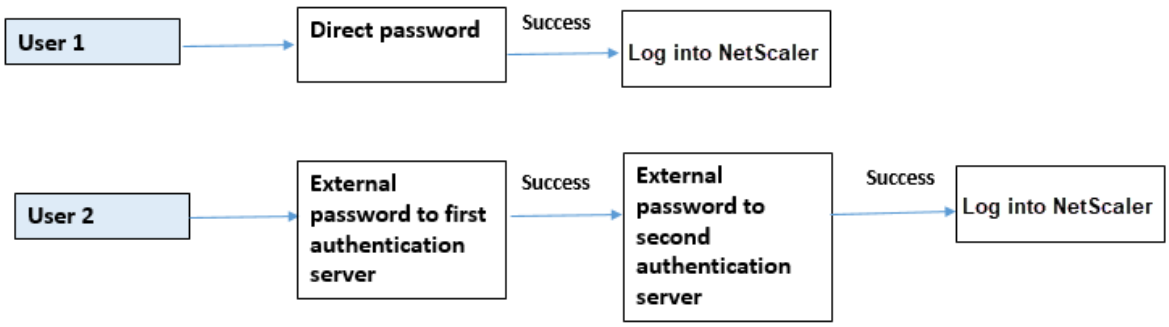
```
add system user <name> <password> -externalAuth DISABLED
```

Beispiel:

```
add system user user1 password1 -externalAuth DISABLED
```

Anwendungsfall 6: Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer aktiviert

Um die Appliance so zu konfigurieren, dass Systembenutzer mithilfe eines lokalen Kennworts authentifiziert werden. Schlägt diese Authentifizierung fehl, wird der Benutzer anschließend mithilfe eines externen Authentifizierungskennworts auf den externen Authentifizierungsservern auf zwei Ebenen authentifiziert.



Konfigurieren Sie die folgenden Schritte über die CLI.

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Authentifizierungsrichtlinie für LDAP-Richtlinie hinzufügen
3. Authentifizierungsaktion für die RADIUS-Richtlinie hinzufügen
4. Fügen Sie eine Authentifizierungsrichtlinie für die RADIUS-Richtlinie hinzu
5. Authentifizierungs-Anmeldeschema hinzufügen
6. Bezeichnung für die Authentifizierungsrichtlinie hinzufügen
7. Bezeichnung der Authentifizierungsrichtlinie für das Anmeldeschema binden
8. Binden Sie das Authentifizierungssystem global für die RADIUS-Richtlinie
9. Binden Sie das Authentifizierungssystem global für die LDAP-Richtlinie

Authentifizierungsaktion für LDAP-Server hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Authentifizierungsrichtlinie für LDAP-Richtlinie hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```


Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Authentifizierungsaktion für RADIUS-Server hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Beispiel:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Fügen Sie eine erweiterte Authentifizierungsrichtlinie für den RADIUS-Server hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Beispiel:

```
add authentication policy radpol11 -rule true -action radact1
```

Authentifizierungs-Anmeldeschema hinzufügen

Sie können das Anmeldeschema SingleAuth.xml verwenden, um die Anmeldeseite anzuzeigen und den Systembenutzer auf der zweiten Authentifizierungsebene zu authentifizieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Beispiel:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Fügen Sie das Label der Authentifizierungsrichtlinie hinzu und binden Sie es an die RADIUS-Authentifizierungsrichtlinie für die Benutzeranmeldung

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```


Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Beispiel:

```
bind authentication policylabel label1 -policyName rad pol11 -priority 1
```

Bind-Authentifizierungsrichtlinie global

Geben Sie in der Befehlszeile Folgendes ein:

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Beispiel:

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Anwendungsfall 7: Die externe Authentifizierung ist nur für ausgewählte externe Benutzer aktiviert

Um selektive externe Benutzer mit der Zwei-Faktor-Authentifizierung gemäß dem in der LDAP-Aktion konfigurierten Suchfilter zu konfigurieren, während andere Systembenutzer mithilfe der Ein-Faktor-Authentifizierung authentifiziert werden.

Konfigurieren Sie die folgenden Schritte über die CLI.

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Authentifizierungsrichtlinie für LDAP-Richtlinie hinzufügen
3. Authentifizierungsaktion für die RADIUS-Richtlinie hinzufügen
4. Fügen Sie eine Authentifizierungsrichtlinie für die RADIUS-Richtlinie hinzu
5. Authentifizierungs-Anmeldeschema hinzufügen
6. Bezeichnung für die Authentifizierungsrichtlinie hinzufügen
7. Bezeichnung der Authentifizierungsrichtlinie für das Anmeldeschema binden
8. Binden Sie das Authentifizierungssystem global für die RADIUS-Richtlinie

Authentifizierungsaktion für LDAP-Server hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:


```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Authentifizierungsrichtlinie für LDAP-Richtlinie hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Authentifizierungsaktion für RADIUS-Server hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Beispiel:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Fügen Sie eine erweiterte Authentifizierungsrichtlinie für den RADIUS-Server hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Beispiel:

```
add authentication policy radpol11 -rule true -action radact1
```


Authentifizierungs-Anmeldeschema hinzufügen

Sie können das Anmeldeschema SingleAuth.xml verwenden, um die Anmeldeseite für die Appliance bereitzustellen, auf der ein Systembenutzer auf einer zweiten Authentifizierungsebene authentifiziert wird.

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Beispiel:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Fügen Sie das Label der Authentifizierungsrichtlinie hinzu und binden Sie es an die RADIUS-Authentifizierungsrichtlinie für die Benutzeranmeldung

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Beispiel:

```
bind authentication policylabel label1 -policyName radpol11 -priority
```

Bind-Authentifizierungsrichtlinie global

Geben Sie in der Befehlszeile Folgendes ein:

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Beispiel:

```
bind system global radpol11 -priority 1 -nextFactor label11
```

So konfigurieren Sie Gruppenbenutzer ohne Zwei-Faktor-Authentifizierung über den Suchfilter:

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Authentifizierungsrichtlinie für LDAP-Server hinzufügen
3. Bind-Authentifizierungssystem global für LDAP-Server

Authentifizierungsaktion für LDAP-Server hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
searchFilter<>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name - searchFilter "memberOf=CN=grp4,CN=Users,DC=
aaatm-test,DC=com"
```

Authentifizierungsrichtlinie für LDAP-Server hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Binden Sie das Authentifizierungssystem global für die LDAP-Richtlinie

Geben Sie in der Befehlszeile Folgendes ein:

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Beispiel:

```
bind system global pol11 -priority 1 -nextFactor label11
```

Anzeige einer benutzerdefinierten Eingabeaufforderung für die Zwei-Faktor-Authentifizierung

Wenn Sie das Zwei-Faktor-Kennwortfeld mit der Datei SingleAuth.xml unter /flash/nsconfig/loginschema/LoginSchema konfigurieren

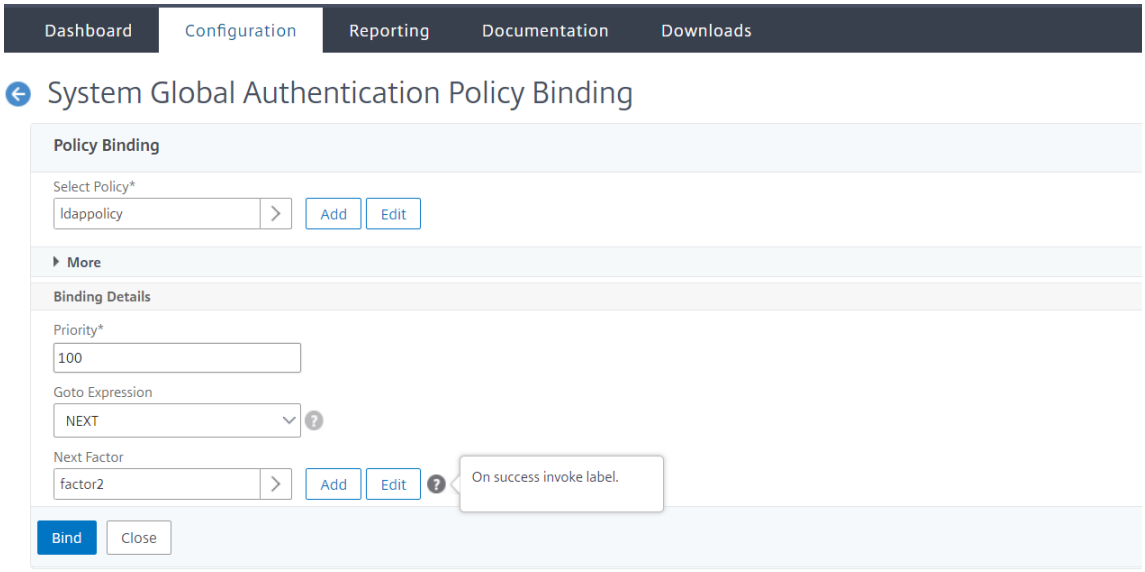
Es folgt der Ausschnitt einer Datei SingleAuth.xml, wobei ‘secondPassword: ‘der zweite Kennwortfeldname ist, der vom Benutzer aufgefordert wird, ein zweites Kennwort einzugeben.


```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
   /1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext/>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</
   SaveID><Type>username</Type></Credential><Label><Text>
   singleauth_user_name</Text><Type>nsg-login-label</Type></Label><
   Input><AssistiveText>singleauth_please_supply_either_domain\
   username_or_user@fully.qualified.domain</AssistiveText><Text><Secret
   >false</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint
   >.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password
   </SaveID><Type>password</Type></Credential><Label><Text>
   SecondPassword:</Text><Type>nsg-login-label</Type></Label><Input><
   Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue/><
   Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>
   singleauth_first_factor</Text><Type>nsg_confirmation</Type></Label><
   Input/></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials
   </Type></Credential><Label><Text>singleauth_remember_my_password</
   Text><Type>nsg-login-label</Type></Label><Input><CheckBox><
   InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential
   ><Label><Type>none</Type></Label><Input><Button>singleauth_log_on</
   Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Konfiguration der Zwei-Faktor-Authentifizierung über die NetScaler GUI

1. Melden Sie sich bei der NetScaler-Appliance an.
2. Gehen Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.

3. Klicken Sie auf Hinzufügen, um die Authentifizierungsrichtlinie der ersten Ebene zu erstellen.
4. Stellen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die folgenden Parameter ein.
    a) Name. Name der Richtlinie
    b) Aktionstyp. Wählen Sie den Aktionstyp als LDAP, Active Directory, RADIUS, TACACS usw.
    c) Aktion. Die Authentifizierungsaktion (Profil), die der Richtlinie zugeordnet werden soll. Sie können eine bestehende Authentifizierungsaktion auswählen oder auf das Plus klicken und eine Aktion des richtigen Typs erstellen.
    d) Expression. Geben Sie einen erweiterten Richtlinienausdruck an.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
    a) Expression. Geben Sie einen erweiterten Richtlinienausdruck an.
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Hinzufügen**, um die Authentifizierungsrichtlinie der zweiten Ebene zu erstellen.
8. Stellen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die folgenden Parameter ein:
    a) Name. Name der Richtlinie
    b) Aktionstyp. Wählen Sie den Aktionstyp als LDAP, Active Directory, RADIUS, TACACS usw.
    c) Aktion. Die Authentifizierungsaktion (Profil), die der Richtlinie zugeordnet werden soll. Sie können eine vorhandene Authentifizierungsaktion auswählen oder auf das Symbol + klicken, um eine Aktion des richtigen Typs zu erstellen.
    d) Expression. Geben Sie einen erweiterten Richtlinienausdruck an
9. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
    a) Expression. Geben Sie einen erweiterten Richtlinienausdruck an.
10. Klicken Sie auf **Erstellen**.
11. Klicken Sie auf der Seite **Authentifizierungsrichtlinien** auf **Global Binding**.
12. Wählen Sie auf der Seite **Globale Authentifizierungsrichtlinienbindung erstellen** die Authentifizierungsrichtlinie der ersten Ebene aus und klicken Sie auf **Bindung hinzufügen**.
13. Wählen Sie auf der Seite **Richtlinienbindung** die Authentifizierungsrichtlinie aus und legen Sie den folgenden Richtlinienbindungsparameter fest.
    a) Nächster Faktor. Wählen Sie das Label für die Authentifizierungsrichtlinie der zweiten Ebene aus.
14. Klicken Sie auf **Binden** und **Schließen**.



15. Klicken Sie auf **Fertig**.
16. Melden Sie sich für die Authentifizierung der zweiten Ebene bei der NetScaler-Appliance an. Der Benutzer kann jetzt das zweite Kennwort eingeben. Nur wenn beide Passwörter korrekt sind, darf der Benutzer auf die NetScaler-Appliance zugreifen.

> **Hinweis:**
>
> Das für eine zweite Faktorauthentifizierung konfigurierte TACACS unterstützt keine Autorisierung und Abrechnung, selbst wenn Sie es mit dem Befehl "TACACSAction" aktivieren. Der zweite Faktor wird nur für den Zweck der Authentifizierung verwendet.

Siehe auch Zwei-Faktor-Authentifizierung in NetScaler nFactor-Authentifizierung .

Eingeschränkte Systembenutzerauthentifizierung für NetScaler-Verwaltungsschnittstellen

May 11, 2023

Sie können den Zugriff der Systembenutzer auf bestimmte NetScaler-Verwaltungsschnittstellen wie CLI oder API einschränken. Der `allowedManagementInterface` Parameter definiert die Liste der zulässigen Verwaltungsschnittstellen. Wenn beispielsweise die Verwaltungsschnittstelle für einen Benutzer oder eine Gruppe auf API eingestellt ist, können alle Benutzer in der Gruppe über die API und nicht über die CLI auf NetScaler zugreifen. Die NetScaler-GUI ist jedoch Teil der API-Schnittstelle, und Benutzer mit API-Berechtigungen können auch auf die GUI-Schnittstelle zugreifen.

> **Hinweis:**
>
> Standardmäßig haben Benutzer und Gruppen Zugriff auf alle Schnittstellen (CLI, API und GUI).

Sie können den Parameter entweder auf Benutzerebene oder auf Benutzergruppenebene konfigurieren. Wenn Sie auf Gruppenebene konfigurieren, wird die Konfiguration auf alle Benutzerkonten in der Gruppe angewendet. Wenn ein Benutzer an mehrere Gruppen gebunden ist, ermöglicht die Appliance den Zugriff auf einen aggregierten Satz von Verwaltungsschnittstellen. Sie können Einstellungen für einen Benutzer in einer Gruppe angeben, indem Sie den Parameter auf Benutzerebene konfigurieren. In diesem Fall ist die Einstellung auf Benutzerebene für eine Gruppe konfiguriert.
In bestimmten Szenarien, in denen der Kunde einen externen Authentifizierungsserver für die Verwaltung von Benutzerkonten verwendet, werden die Serverdetails auf der Appliance konfiguriert. In diesem Fall kann der Administrator eine Benutzergruppe in der NetScaler-Appliance erstellen und der Gruppe alle Benutzer (auf dem externen Server gruppiert) hinzufügen. Beispielsweise werden alle auf dem externen Server verwalteten Benutzer zur Gruppe API_Users hinzugefügt, und der Administrator kann die Gruppe lokal auf der Appliance konfigurieren.

> **Hinweis:**
>
> Die NetScaler-Appliance ermöglicht nur dem `nsroot` Administrator (Superuser) die Konfiguration des Parameters und erlaubt keinem Systembenutzer, die Parametereinstellung zu ändern.

Konfigurieren Sie den Benutzerzugriff auf NetScaler-Verwaltungsschnittstellen mithilfe der CLI

Um Benutzern Zugriff auf eine bestimmte Verwaltungsschnittstelle zu gewähren, müssen Sie den Parameter für die zulässige Verwaltungsschnittstelle festlegen. Geben Sie in der Befehlszeile Folgendes ein:

```
set system group <groupName> [-allowedManagementInterface ( CLI | API )]
```

Beispiel:

```
set system group network_usergroup -allowedManagementInterface CLI
```

Informationen zur Parameterbeschreibung finden Sie unter Referenz zu Authentifizierungs- und Berechtigungsbefehlen .

Informationen zu GUI- und CLI-Schnittstellen finden Sie im Thema Access NetScaler .

TCP-Konfigurationen

August 15, 2023

TCP-Konfigurationen für eine NetScaler-Appliance können in einer Entität angegeben werden, die als TCP-Profil bezeichnet wird, bei der es sich um eine Sammlung von TCP-Einstellungen handelt. Das TCP-Profil kann dann mit Diensten oder virtuellen Servern verknüpft werden, die diese TCP-Konfigurationen verwenden möchten.

Ein Standard-TCP-Profil kann so konfiguriert werden, dass die TCP-Konfigurationen festgelegt werden, die standardmäßig global auf alle Dienste und virtuellen Server angewendet werden.

> **Hinweis:**
>
> Wenn ein TCP-Parameter unterschiedliche Werte für den Dienst, den virtuellen Server und global aufweist, erhält der Wert der am meisten spezifischen Entität (den Dienst) die höchste Priorität. Die NetScaler-Appliance bietet auch andere Ansätze zur Konfiguration von TCP.

Unterstützte TCP-Konfiguration

Die NetScaler-Appliance unterstützt die folgenden TCP-Funktionen:

Verteidigung von TCP gegen Spoofing-Angriffe gemäß RFC 5961

NetScaler unterstützt RST-Fensterdämpfung und SYN-Spoof-Schutzmethoden, um TCP vor Spoofing-Angriffen zu schützen, und ist mit RFC 4953 konform.

Ab der Version NetScaler 14.1-4.x entspricht NetScaler RFC 5961, was einen verbesserten Schutz vor TCP-Spoofing-Angriffen bietet. Mit der RFC 5961-Konformität bietet NetScaler zusätzlich zur RST-Fensterdämpfung und dem SYN-Spoof-Schutz die folgenden Funktionen:

- Reduziert die Wahrscheinlichkeit einer ungültigen Dateneinspeisung.
- Ermöglicht die Begrenzung der Anzahl der vom NetScaler gesendeten Challenge-ACK-Antworten pro Sekunde.

Standardmäßig ist die RFC 5961-Konformität deaktiviert. Sie können es mithilfe der CLI oder der GUI aktivieren. Weitere Informationen finden Sie unter Verteidigung von TCP gegen Spoofing-Angriffe.

Explicit Congestion Notification (ECN)

Die Appliance sendet eine Benachrichtigung über den Netzwerküberlastungsstatus an den Absender der Daten und ergreift Korrekturmaßnahmen für Datenüberlastung oder Datenbeschädigung. Die NetScaler-Implementierung von ECN ist RFC 3168-konform.

Roundtrip-Zeitmessung (RTTM) mit der Zeitstempeloption

Damit die TimeStamp-Option funktioniert, muss sie mindestens eine Seite der Verbindung (Client oder Server) unterstützen. Die NetScaler-Implementierung der Option `TimeStamp` ist RFC 1323-

konform.

Erkennung von unvorsichtigen Wiederübertragungen

Diese Erkennung kann mithilfe von TCP Duplicate Selective Acknowledgment (D-SACK) und Forward RTO-Recovery (F-RTO) erfolgen. Wenn es unechte Wiederübertragungen gibt, werden die Konfigurationen der Überlastungssteuerung in ihren ursprünglichen Zustand versetzt. Die NetScaler Implementierung von D-SACK ist RFC 2883-konform und F-RTO ist RFC 5682-konform.

Überlastungskontrolle

Diese Funktionalität verwendet New-Reno-, BIC-, CUBIC-, Nile- und TCP-Westwood-Algorithmen.

Skalierung von Fenstern

Dies erhöht die Größe des **TCP-Empfangsfensters** über den Maximalwert von 65.535 Byte hinaus.

Punkte, die Sie beachten sollten, bevor Sie die Fensterskalierung konfigurieren

- Sie legen keinen hohen Wert für den Skalierungsfaktor fest, da dies negative Auswirkungen auf die Appliance und das Netzwerk haben kann.
- Sie konfigurieren keine Fensterskalierung, es sei denn, Sie wissen genau, warum Sie die Fenstergröße ändern möchten.
- Beide Hosts in der TCP-Verbindung senden beim Verbindungsaufbau eine Fensterskalierungsoption. Wenn nur eine Seite einer Verbindung diese Option setzt, wird für die Verbindung keine Fensterskalierung verwendet.
- Jede Verbindung für dieselbe Sitzung ist eine unabhängige Fensterskalierungssitzung. Wenn beispielsweise die Anforderung eines Clients und die Antwort des Servers durch die Appliance fließt, kann eine Fensterskalierung zwischen dem Client und der Appliance ohne Fensterskalierung zwischen der Appliance und dem Server erfolgen.

Fenster mit maximaler Überlastung von TCP

Die Fenstergröße ist vom Benutzer konfigurierbar. Der Standardwert ist 8190 Byte.

Selektive Bestätigung (SACK)

Dies verwendet den Datenempfänger (entweder eine NetScaler-Appliance oder ein Client), der den Absender über alle Segmente informiert, die erfolgreich empfangen wurden.

Bestätigung vorwärts (FACK)

Diese Funktion vermeidet TCP-Überlastung, indem sie die Gesamtzahl der im Netzwerk ausstehenden Datenbytes explizit misst und dem Absender (entweder einem NetScaler oder einem Client) hilft, die Menge der Daten zu kontrollieren, die während der Zeitüberschreitung der erneuten Übertragung in das Netzwerk injiziert werden.

TCP-Verbindungs-Multiplexen

Diese Funktion ermöglicht die Wiederverwendung bestehender TCP-Verbindungen. Die NetScaler-Appliance speichert etablierte TCP-Verbindungen zum Wiederverwendungspool. Wenn eine Clientanforderung empfangen wird, sucht die Appliance nach einer verfügbaren Verbindung im Wiederverwendungspool und bedient den neuen Client, wenn die Verbindung verfügbar ist. Wenn sie nicht verfügbar ist, erstellt die Appliance eine Verbindung für die Client-Anfrage und speichert die Verbindung zum Wiederverwendungspool. Der NetScaler unterstützt das Verbindungsmultiplexing für HTTP-, SSL- und DataStream-Verbindungstypen.

Dynamische Empfangspufferung

Auf diese Weise kann der Empfangspuffer basierend auf Speicher- und Netzwerkbedingungen dynamisch angepasst werden.

MPTCP-Verbindung

MPTCP-Verbindungen zwischen dem Client und dem NetScaler. MPTCP-Verbindungen werden zwischen dem NetScaler und dem Back-End-Server nicht unterstützt. Die NetScaler Implementierung von MPTCP ist RFC 6824-konform.

Über die Befehlszeilenschnittstelle können Sie MPTCP-Statistiken wie aktive MPTCP-Verbindungen und aktive Subflow-Verbindungen anzeigen.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Zusammenfassung oder detaillierte Zusammenfassung der MPTCP-Statistiken anzuzeigen oder die Statistikanzeige zu löschen:

1. `Stat MPTCP`
2. `Stat mptcp -detail`
3. `Clearstats basic`

> **Hinweis:**
>
> Um eine MPTCP-Verbindung herzustellen, müssen sowohl der Client als auch die NetScaler-Appliance dieselbe MPTCP-Version unterstützen. Wenn Sie die NetScaler-Appliance als

> MPTCP-Gateway für Ihre Server verwenden, müssen die Server MPTCP nicht unterstützen. Wenn der Client eine neue MPTCP-Verbindung startet, identifiziert die Appliance die MPTPC-Version des Clients anhand der MP_CAPABALE-Option im SYN-Paket. Wenn die Version des Clients höher ist als die auf der Appliance unterstützte Version, gibt die Appliance ihre höchste Version in der MP_CAPABALE-Option des SYN-ACK-Pakets an. Der Client greift dann auf eine niedrigere Version zurück und sendet die Versionsnummer in der MP_CAPABALE-Option des ACK-Pakets. Wenn diese Version unterstützbar ist, setzt die Appliance die MPTCP-Verbindung fort. Andernfalls fällt die Appliance auf einen normalen TCP zurück. Die NetScaler-Appliance initiiert keine Subflows (MP_JOINs). Die Appliance erwartet, dass der Client Subflows initiiert.

Unterstützung für zusätzliche Adressenwerbung (ADD_ADDR) in MPTCP

Wenn Sie in einer MPTCP-Bereitstellung einen virtuellen Server haben, der an einen IP-Satz gebunden ist, der zusätzliche IP-Adressen des virtuellen Servers enthält, gibt die Funktion für zusätzliche Adressenankündigung (ADD_ADDR) die IP-Adresse der virtuellen Server an, die an den IP-Satz gebunden sind. Clients können zusätzliche `MP-JOIN`-Unterflüsse zu den beworbenen IP-Adressen initiieren.

Punkte, die Sie über die MPTCP ADD_ADDR-Funktionalität erinnern

- Sie können im Rahmen der Option `ADD_ADDR` maximal 10 IP-Adressen senden. Wenn mehr als 10 IP-Adressen mit aktiviertem Parameter `mptcpAdvertise` vorhanden sind, ignoriert die Appliance nach der Werbung für die 10-IP-Adresse den Rest der IP-Adressen.
- Wenn der MP-FÄHIGE Subflow an eine der IP-Adressen im IP-Satz anstelle der IP-Adresse des primären virtuellen Servers übertragen wird, wird die IP-Adresse des virtuellen Servers angekündigt, wenn der Parameter `mptcpAdvertise` für die IP-Adresse des virtuellen Servers aktiviert ist

Konfigurieren Sie die Funktion für weitere Adressenwerbung (ADD_ADDR), um über die Befehlszeilenschnittstelle zusätzliche VIP-Adresse anzukündigen

Sie können die Funktionalität `MPTCP ADD_ADDR` sowohl für IPv4- als auch für IPv6-Adresstypen konfigurieren. Im Allgemeinen können mehrere IPv4- und IPv6-IPs an einen einzelnen IP-Satz angeschlossen werden, und der Parameter kann für jede Teilmenge von IP-Adressen aktiviert werden. In der ADD_ADDR-Funktion werden nur die IP-Adressen angekündigt, bei denen die Option “mptcpAdvertise” aktiviert ist, und die verbleibenden IP-Adressen aus dem IP-Satz werden ignoriert. Führen Sie die folgenden Schritte aus, um das Feature `ADD_ADDR` zu konfigurieren:

1. Fügen Sie einen IP-Satz hinzu.
2. Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu, wobei MPTCP Advertise aktiviert ist.
3. Binden Sie die IP-Adresse an die IP gesetzt.

4. Konfigurieren Sie die IP-Satz mit dem virtuellen Lastenausgleichsserver.

Fügen Sie einen IP-Satz hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ipset <name> [-td <positive_integer>]
<!--NeedCopy-->
```

Beispiel:

```
add ipset ipset_1
<!--NeedCopy-->
```

Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu, wobei MPTCP Advertise aktiviert ist

Geben Sie beim Befehl ein:

```
add ns ip <IPAddress>@ <netmask> [-mptcpAdvertise ( YES | NO )] -type <
   type>
<!--NeedCopy-->
```

Beispiel:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
```

Binden Sie IP-Adressen an den IP-Satz

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Beispiel:

```
bind ipset ipset_1 10.10.10.10
```

Konfigurieren der IP, die auf den virtuellen Lastenausgleich eingestellt ist

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Beispielkonfiguration:

```
Add ipset ipset_1
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Konfigurieren Sie die externe IP-Adresse der Werbung mithilfe der ADD_ADDR-Funktionalität

Wenn die angekündigte IP-Adresse im Besitz der externen Entität ist und die NetScaler-Appliance die IP-Adresse bekannt geben muss, muss der Parameter “MPTCPAdvertise” aktiviert sein, wobei Status- und ARP-Parameter deaktiviert sind.

Führen Sie die folgenden Schritte aus, um `ADD_ADDR` für die Ankündigung der externe IP-Adresse zu konfigurieren.

1. Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu, wobei MPTCP Advertise aktiviert ist.
2. Binden Sie die IP-Adresse an die IP gesetzt.
3. Binden Sie IP mit dem virtuellen Lastenausgleichsserver

Fügen Sie eine externe IP-Adresse vom Typ Virtual Server IP (VIP) mit aktivierter MPTCP-Werbung hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip <IPAddress>@ <External-IP-mask -type VIP> [-mptcpAdvertise (
    YES | NO )] -type <type> -state DISABLED -arp DISABLED
<!--NeedCopy-->
```

Beispiel:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP -state
DISABLED -arp DISABLED
```

Binden Sie IP-Adressen an den IP-Satz

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Beispiel:

```
bind ipset ipset_1 10.10.10.10
```

Konfigurieren der IP, die auf den virtuellen Lastenausgleich eingestellt ist

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver lb1 -ipset ipset_1
```

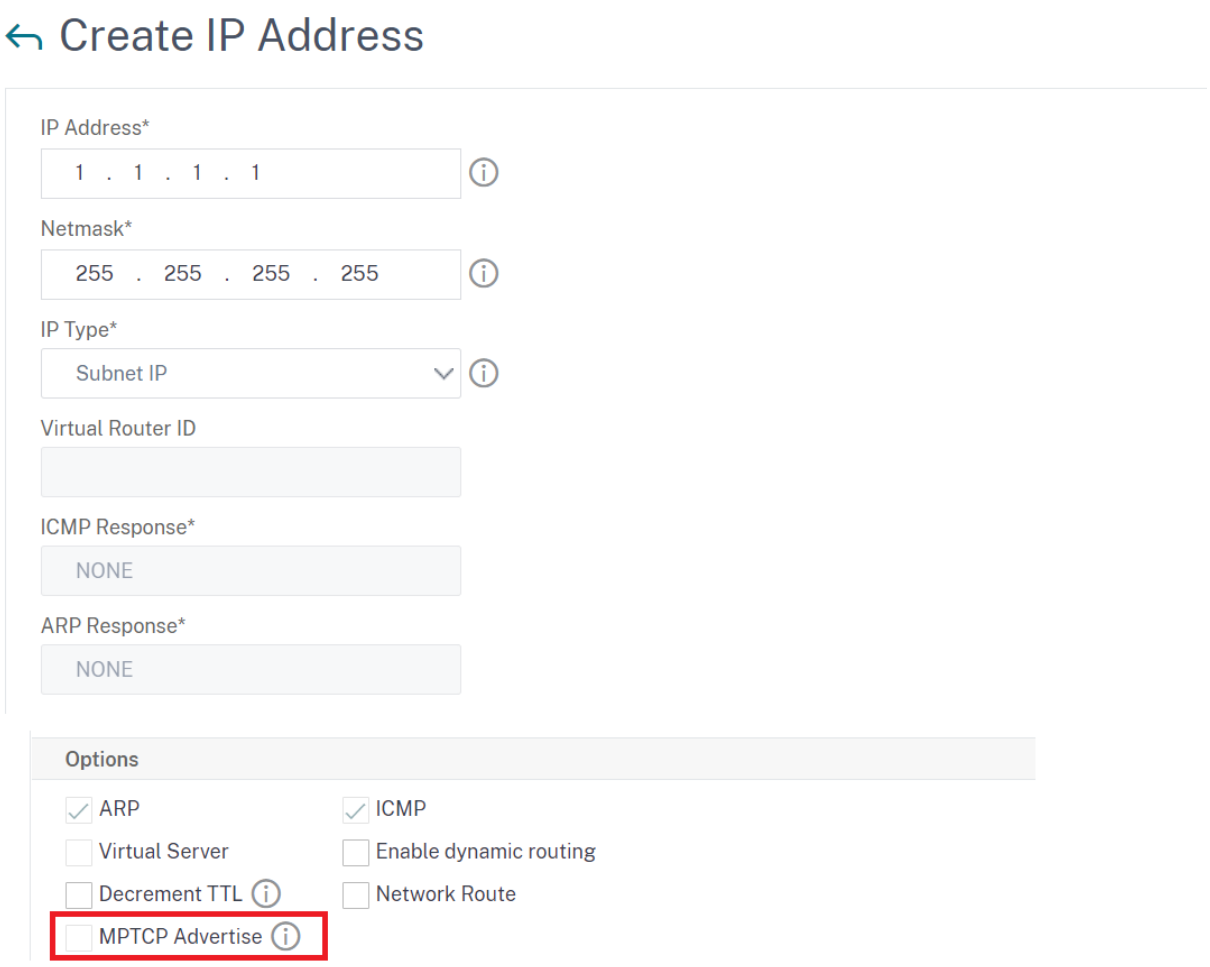
Beispielkonfiguration:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
   state DISABLED -arp DISABLED
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Geben Sie MPTCP-fähigen Clients mithilfe der NetScaler GUI eine IP-Adresse bekannt

Führen Sie den folgenden Schritt aus, um die IP-Adresse an die MPTCP-fähigen Clients anzukündigen:

1. Navigieren Sie zu **System > Netzwerk > IPs**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Aktivieren Sie auf der Seite **IP-Adresse erstellen** das Kontrollkästchen **MPTCP Advertise**, um den Parameter festzulegen. Standardmäßig ist es deaktiviert.



Extrahieren der TCP/IP-Pfad-Overlay-Option und Einfügen des Client-IP-HTTP-Headers

Extrahieren von TCP/IP-Pfadüberlagerung und Einfügen von HTTP-Header von Client-IP. Der Datentransport durch Overlay-Netzwerke verwendet häufig Verbindungsabbruch oder Network Address Translation (NAT), bei der die IP-Adresse des Quell-Clients verloren geht. Um dies zu vermeiden, extrahiert die NetScaler-Appliance die TCP/IP-Pfad-Overlay Option und fügt die IP-Adresse des Quell-Clients in den HTTP-Header ein. Mit der IP-Adresse im Header kann der Webserver den Quellclient identifizieren, der die Verbindung hergestellt hat. Die extrahierten Daten sind für eine Lebensdauer der TCP-Verbindung gültig und dies verhindert daher, dass der nächste Hop-Host die Option erneut interpretieren muss. Diese Option ist nur für Webdienste anwendbar, für die die Einfügeoption Client-IP aktiviert ist.

TCP-Segmentierungsabladung

Lädt die TCP-Segmentierung auf die NIC aus. Wenn Sie die Option auf “AUTOMATIC” festlegen, wird die TCP-Segmentierung auf die NIC verlagert, wenn die NIC unterstützt wird.

Cookie für TCP-Handshake mit Clients synchronisieren

Dies wird verwendet, um SYN-Überschwemmungen zu widerstehen. Sie können den `SYNCOOKIE` -Mechanismus für TCP-Handshake mit Clients aktivieren oder deaktivieren. Deaktivieren von `SYNCOOKIE` verhindert den `SYN`-Angriffsschutz auf der NetScaler-Appliance.

MSS lernen, um MSS Learning für alle virtuellen Server zu aktivieren, die auf der Appliance konfiguriert sind

Unterstützte TCP-Parameter

Die folgende Tabelle enthält eine Liste der TCP-Parameter und ihrer Standardwerte:

|Parameter|Standardwert|Beschreibung|
|— |— |— |
|Fenster-Verwaltung|
TCP-Verzögerter Ack Timer	100 Millisec	Timeout für TCP-verzögerte ACK in Millisekunden.
TCP-Mindestzeitlimit für die Weiterübertragung (RTO) in Milli Sek	1000 Milli Sek	Minimale Zeitüberschreitung für die erneute Übertragung in Millisekunden, angegeben in 10-Millisekunden-Schritten (Wert muss eine ganze Zahl ergeben, wenn sie durch 10 geteilt wird)
Leerlaufzeit der Verbindung vor dem Starten von Keep-Alive-Sonden	900 Sekunden	Löschen Sie im Stille TCP-etablierte Verbindungen bei Leerlauf-Timeouts, die Verbindungen im Leerlauf-Timeout hergestellt haben
TCP-Zeitstempeloption	DEAKTIVIERT	Die Zeitstempeloption ermöglicht eine genaue RTT-Messung. Aktivieren oder Deaktivieren Sie die Option TCP-Zeitstempel.
Timeout für Multipath TCP-Session	0 Sekunden	Zeitüberschreitung für die MPTCP Sitzung in Sekunden. Wenn dieser Wert nicht gesetzt ist, Leerlauf. MPTCP-Sitzungen werden nach dem Client-Leerlauf-Timeout des virtuellen Servers geleert.
Stillschweigendes Löschen von Halbgeschlossenen Verbindungen bei Leerlaufzeitüberschreitung	0 Sekunden	Halbgeschlossene TCP-Verbindungen im Leerlauf still fallen lassen.
Etablierte Verbindungen im Leerlauf-Timeout still fallen lassen	DEAKTIVIERT	Lassen Sie TCP-etablierte Verbindungen im Leerlauf-Timeout still fallen
Speicherverwaltung
TCP-Puffergröße	131072 Bytes	Die Größe des TCP-Puffers ist die Größe des Empfangspuffers im NetScaler. Diese Puffergröße wird Clients und Servern von NetScaler angekündigt und steuert deren Fähigkeit, Daten an NetScaler zu senden. Die Standardpuffergröße beträgt 8K, und normalerweise

ist es sicher, dies zu erhöhen, wenn Sie mit internen Serverfarmen sprechen. Die Puffergröße wirkt sich auch auf die tatsächliche Anwendungslayer in NetScaler aus, wie bei SSL-Endpunktfällen ist sie auf 40 K festgelegt und für die Komprimierung auf 96 K festgelegt. **Hinweis:** Das Argument für die Puffergröße muss festgelegt werden, damit dynamische Anpassungen stattfinden können.|
TCP-Sendpuffergröße	8190 Bytes	TCP-Sendpuffergröße
Dynamische Empfangspufferung von TCP	DEAKTIVIERT	Aktivieren oder deaktivieren Sie die dynamische Empfangspufferung. Wenn diese Option aktiviert ist, kann der Empfangspuffer basierend auf Speicher- und Netzwerkbedingungen dynamisch angepasst werden. **Hinweis:** Das Argument Puffergröße muss festgelegt werden, damit dynamische Anpassungen stattfinden können
TCP-Max-Überlastungsfenster (CWND)	524288 Bytes	Fenster “Maximale Überlastung” von TCP
Status der Fensterskalierung	ENALBED	Aktivieren oder deaktivieren Sie die Fensterskalierung.
Skalierungsfaktor für Fenster	8	Faktor, der zur Berechnung der neuen Fenstergröße verwendet wird. Dieses Argument ist nur erforderlich, wenn die Fensterskalierung aktiviert ist.
Verbindungs-Setup
Keep-Alive-Sonden	DEAKTIVIERT	Senden Sie periodische TCP-Keep-Alive-Sonden (KA), um zu überprüfen, ob der Peer noch aktiv ist.
Leerlaufzeit der Verbindung vor dem Starten von Keep-Alive-Sonden	900 Sekunden	Dauer in Sekunden, damit die Verbindung im Leerlauf ist, bevor eine Keep-Alive-Sonde (KA) gesendet wird.
Keep-Alive-Sondenintervall	75 Sekunden	Zeitintervall in Sekunden vor der nächsten Keep-Alive-Sonde (KA), wenn der Peer nicht reagiert.
Maximale Keep-Alive-Sonden, die verpasst werden müssen, bevor die Verbindung unterbrochen wird.	3	Anzahl der Keep-Alive-Sonden (KA), die gesendet werden sollen, wenn sie nicht bestätigt werden, bevor angenommen wird, dass der Peer ausgefallen ist.
RFC 5961-Konformität	DEAKTIVIERT	Aktivieren Sie die RFC 5961-Konformität, um sich vor Spoofing zu schützen. Wenn diese Option aktiviert ist, werden sowohl RST-Fensterdämpfung als auch SYN-Spoof-Schutz bereitgestellt. Außerdem können Sie die Anzahl der vom NetScaler gesendeten Challenge-ACKS steuern. Beachten Sie, dass Sie sowohl die RST-Fensterdämpfung als auch den SYN-Spoof-Schutz deaktivieren müssen, damit die RFC 5961-Konformitätsfunktion funktioniert.
RST-Fensterdämpfung (Spoofschutz)	DEAKTIVIERT	Aktivieren oder deaktivieren Sie RST-Fensterdämpfung, um vor Spoofing zu schützen. Wenn diese Option aktiviert ist, erfolgt die Antwort mit korrigierendem ACK, wenn eine Sequenznummer ungültig ist.
Akzeptieren Sie RST mit der letzten quittierten Sequenznummer.	AKTIVIERT
Datenübertragung
Sofortiges ACK auf PUSH-Paket	AKTIVIERT	Senden Sie sofort eine positive Bestätigung (ACK) nach Erhalt von TCP-Paketen mit PUSH-Flag.
Maximale Pakete pro MSS	0	Maximale Anzahl von Oktetten, die in einem TCP-Datensegment zugelassen werden sollen
Nagles Algorithmus	DEAKTIVIERT	Nagles Algorithmus kämpft mit dem Problem kleiner Pakete bei der TCP-Übertragung. Anwendungen wie Telnet und andere Echtzeit-Engines, bei denen jeder

Tastendruck an die andere Seite weitergegeben werden muss, erzeugen oft kleine Pakete. Mit Nagle's Algorithmus kann NetScaler solche kleinen Pakete puffern und sendet sie zusammen, um die Verbindungseffizienz zu erhöhen. Dieser Algorithmus muss mit anderen TCP-Optimierungstechniken im NetScaler zusammenarbeiten.|
|Maximale zulässige TCP-Segmente in einem Burst|10 MSS|Maximale Anzahl von TCP-Segmenten in einem Burst zulässig|
|Maximale Pakete, die in die Warteschlange gestellt werden sollen|300|Maximale Größe der Warteschlange außerhalb der Ordnung Pakete. Ein Wert von 0 bedeutet kein Limit|
|Überlastungskontrolle|
TCP Flavor	CUBIC
Einstellung des ersten Überlastungsfensters (cwnd)	4 MSS	Anfängliche maximale Obergrenze für die Anzahl der TCP-Pakete, die bei der TCP-Verbindung zum Server ausstehen können
Explizite TCP-Überlastungsbenachrichtigung (ECN)	DEAKTIVIERT	Die explizite Congestion Notification (ECN) ermöglicht eine End-zu-End-Benachrichtigung über Netzwerküberlastung, ohne Pakete zu verwerfen.
TCP-Max-Überlastungsfenster (CWND)	524288 Bytes	TCP unterhält ein Überlastungsfenster (CWND), das die Gesamtzahl der nicht bestätigten Pakete begrenzt, die möglicherweise End-to-End übertragen werden. In TCP ist das Überlastungsfenster einer der Faktoren, die die Anzahl der Bytes bestimmen, die jederzeit ausstehen können. Das Überlastungsfenster verhindert, dass eine Verbindung zwischen dem Absender und dem Empfänger mit zu viel Verkehr überlastet wird. Es wird berechnet, indem geschätzt wird, wie viel Staus auf der Verbindung vorhanden ist.
TCP-Hybrid-Start (HyStart)	8 Byte
TCP-Mindestzeitlimit für die Weiterübertragung (RTO) in Milli Sek	1000	Minimales Zeitlimit für die Weiterübertragung in Millisekunden, angegeben in Schritten von 10 Millisekunden (der Wert muss eine ganze Zahl ergeben, wenn er durch 10 geteilt wird).
TCP-Dupack-Schwellenwert	DEAKTIVIERT
Burst-Rate Steuerung	3	TCP-Burst-Rate Control DISABLED/FIXED/DYNAMIC. FIXED erfordert, dass eine TCP-Rate festgelegt wird
TCP-Rate	DEAKTIVIERT	Senderate der TCP-Verbindung Payload in KB/s
Höchstwarteschlange für TCP-Rate	0	Maximale Größe der Verbindungswarteschlange in Byte, wenn BurstRateControl verwendet wird.
MPTCP
Mehrweg-TCP	DISABLED	Multipath TCP (MPTCP) ist eine Reihe von Erweiterungen für reguläres TCP, um einen Multipath-TCP-Dienst bereitzustellen, der es ermöglicht, dass eine Transportverbindung über mehrere Pfade gleichzeitig funktioniert.
Multipath-TCP-Drop-Daten für vorab festgelegten Subflow	DISABLED	Aktivieren oder deaktivieren Sie das stillschweigende Löschen der Daten im vorab etablierten Subflow. Wenn diese Option aktiviert ist, werden DSS-Datenpakete im Hintergrund gelöscht, anstatt die Verbindung zu löschen, wenn Daten im vorab festgelegten Subflow empfangen werden.

|Multipath-TCP-fastopen|DISABLED|Aktivieren oder deaktivieren Sie Multipath TCP fastopen. Wenn diese Option aktiviert ist, werden DSS-Datenpakete akzeptiert, bevor die dritte Packung SYN-Handshake empfangen wird.|
|Timeout für Multipath TCP-Session|0 Sekunden|Zeitüberschreitung für die MPTCP Sitzung in Sekunden. Wenn dieser Wert nicht festgelegt ist, werden ungenutzte MPTCP-Sitzungen nach dem Client-Leerlauf-Timeout des virtuellen Servers geleert.|
|Sicherheit|
|SYN Spoof Schutz|DEAKTIVIERT|Aktivieren oder deaktivieren Sie das Löschen ungültiger SYN-Pakete zum Schutz vor Spoofing. Wenn diese Option deaktiviert ist, werden die etablierten Verbindungen zurückgesetzt, wenn ein SYN-Paket empfangen wird.|
|TCP Syncookie|DEAKTIVIERT|Dies wird verwendet, um SYN-Überschwemmungen zu widerstehen. Aktivieren oder deaktivieren Sie den SYNCOOKIE-Mechanismus für TCP-Handshake mit Clients. Das Deaktivieren von SYNCOOKIE verhindert den SYN-Angriffsschutz auf der NetScaler-Appliance.|
|Verlusterkennung und Erholung|
Doppelte selektive Bestätigung (DSACK)	AKTIVIERT	Eine NetScaler-Appliance verwendet Duplicate Selective Acknowledgment (DSACK), um festzustellen, ob eine erneute Übertragung fälschlicherweise gesendet wurde.
Forward RTO Erholung (FRTO)	AKTIVIERT	Erkennt unechte Timeouts für die TCP-Weiterübertragung. Nach der erneuten Übertragung des ersten nicht bestätigten Segments, das durch ein Timeout ausgelöst wird, überwacht der Algorithmus des TCP-Absenders die eingehenden Bestätigungen, um festzustellen, ob das Timeout falsch war. Anschließend entscheidet er, ob neue Segmente gesendet oder nicht bestätigte Segmente erneut übertragen werden sollen. Der Algorithmus hilft effektiv, weitere unnötige Neuübertragungen zu vermeiden und verbessert dadurch die TCP-Leistung im Falle eines unechten Timeouts.
TCP-Vorwärtsbestätigung (FACK)	AKTIVIERT	Aktivieren oder deaktivieren Sie FACK (Forward ACK).
Status der selektiven Bestätigung (SACK)	AKTIVIERT	TCP SACK befasst sich mit dem Problem der Mehrfachpaketverluste, wodurch die Gesamtdurchsatzkapazität reduziert wird. Mit selektiver Bestätigung kann der Empfänger den Absender über alle Segmente informieren, die erfolgreich empfangen wurden, sodass der Absender nur die verlorenen Segmente erneut übermitteln kann. Diese Technik hilft NetScaler, den Gesamtdurchsatz zu verbessern und die Verbindungslatenz zu reduzieren.
Maximale Pakete pro Weiterübertragung	1	Ermöglicht NetScaler zu steuern, wie viele Pakete in einem Versuch erneut übertragen werden sollen. Wenn NetScaler ein partielles ACK erhält und eine erneute Übertragung durchführen muss, wird diese Einstellung berücksichtigt. Dies wirkt sich nicht auf die RTO basierten Wiederübertragungen aus.
TCP-Verzögerter Ack Timer	100 Millisec	Timeout für TCP verzögertes ACK in Millisekunden
TCO-Optimierung
TCP-Optimierungsmodus	TRANSPARENT	TCP-Optimierungsmodi TRANSPARENT/ENDPOINT
Wenden Sie adaptive TCP-Optimierungen an	DEAKTIVIERT	Wenden Sie adaptive TCP-Optimierungen

an|
TCP-Segmentierungs Offload	AUTOMATIC	Verlagern Sie die TCP-Segmentierung auf die NIC. Wenn diese Option auf AUTOMATIC eingestellt ist, wird die TCP-Segmentierung auf die NIC ausgelagert, wenn die NIC dies unterstützt.
ACK-Aggregation	DEAKTIVIERT	Aktivieren oder Deaktivieren von ACK Aggregation
TCP-Zeit-Warten (oder Time_Wait)	40 Sekunden	Zeit zu vergehen, bevor eine geschlossene TCP-Verbindung freigegeben wird
Delink Client und Server auf RST	DEAKTIVIERT	Delink-Client- und Server-Verbindung, wenn vorhanden
herausragende Daten, die an die andere Seite gesendet werden sollen.

> **Hinweis:**
>
> Wenn HTTP/2 aktiviert ist, empfiehlt Citrix, den Parameter TCP Dynamic Receive Buffering im TCP-Profil zu deaktivieren.

Einstellen globaler TCP-Parameter

Mit der NetScaler-Appliance können Sie Werte für TCP-Parameter angeben, die für alle NetScaler-Dienste und virtuellen Server gelten. Dies kann geschehen mit:

- Standard-TCP-Profil
- Globaler TCP-Befehl
- TCP-Pufferungsfunktion

> **Hinweise:**
>
> - Der Parameter `recvBuffSize` des Befehls set ns tcpParam ist ab Version 9.2 veraltet. Legen Sie in späteren Versionen die Puffergröße mithilfe des Parameters `bufferSize` des Befehls set ns tcpProfile fest. Wenn Sie auf eine Version aktualisieren, in der der Parameter `recvBuffSize` veraltet ist, wird der Parameter `bufferSize` auf den Standardwert festgelegt.
> - Stellen Sie bei der Konfiguration des TCP-Profils sicher, dass der TCP-Parameter `buffersize` kleiner oder gleich dem Parameter `httppipelinebuffersize` ist.
> Wenn der Parameter `buffersize` im TCP-Profil größer ist als der Parameter `httppipelinebuffersize` im HTTP-Profil, kann sich die TCP-Payload ansammeln und die Größe des HTTP-Pipeline-Puffers überschreiten. Dies führt dazu, dass die NetScaler-Appliance die TCP-Verbindung zurücksetzt.

Standard-TCP-Profil

Ein TCP-Profil mit dem Namen `nstcp_default_profile` wird verwendet, um TCP-Konfigurationen anzugeben, die verwendet werden, wenn auf Service- oder virtuelle Serverebene keine TCP-

Konfigurationen bereitgestellt werden.

> **Hinweise:**
>
> - Nicht alle TCP-Parameter können über das Standard-TCP-Profil konfiguriert werden. Einige Einstellungen müssen mit dem globalen TCP-Befehl vorgenommen werden (siehe Abschnitt unten).
> - Das Standardprofil muss nicht explizit an einen Dienst oder einen virtuellen Server gebunden sein.

So konfigurieren Sie das Standard-TCP-Profil

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:

```
set ns tcpProfile nstcp_default_profile...
<!--NeedCopy-->
```

- Navigieren Sie auf der Benutzeroberfläche zu **System** > **Profile**, klicken Sie auf **TCP-Profile** und aktualisieren Sie nstcp_default_profile.

Globaler TCP-Befehl

Ein anderer Ansatz, mit dem Sie globale TCP-Parameter konfigurieren können, ist der globale TCP-Befehl. Zusätzlich zu einigen eindeutigen Parametern dupliziert dieser Befehl einige Parameter, die mithilfe eines TCP-Profils festgelegt werden können. Jede Aktualisierung dieser doppelten Parameter spiegelt sich im entsprechenden Parameter im Standard-TCP-Profil wider.

Wenn beispielsweise der SACK-Parameter mit diesem Ansatz aktualisiert wird, wird der Wert im SACK-Parameter des Standard-TCP-Profils (nstcp_default_profile) widergespiegelt.

> **Hinweis:**
>
> Citrix empfiehlt, diesen Ansatz nur für TCP-Parameter zu verwenden, die im Standard-TCP-Profil nicht verfügbar sind.

So konfigurieren Sie den globalen TCP-Befehl

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:

```
set ns tcpParam …
<!--NeedCopy-->
```

- Navigieren Sie auf der GUI zu **System > Einstellungen**, klicken Sie auf **TCP-Parameter ändern** und aktualisieren Sie die erforderlichen TCP-Parameter.

TCP-Pufferungsfunktion

NetScaler bietet eine Funktion namens TCP-Pufferung, mit der Sie die TCP-Puffergröße angeben können. Die Funktion kann global oder auf Service-Ebene aktiviert werden.

> **Hinweis:**
>
> Die Puffergröße kann auch im Standard-TCP-Profil konfiguriert werden. Wenn die Puffergröße im TCP-Puffer-Feature und im Standard-TCP-Profil unterschiedliche Werte aufweist, wird der größere Wert angewendet.

Konfigurieren Sie die TCP-Pufferfunktion global

- Geben Sie in der Befehlszeile ein:

  enable ns mode TCPB

  ```
  set ns tcpbufParam -size <positiveInteger> -memLimit <positiveInteger>
  ```

- Navigieren Sie auf der GUI zu **System** > **Einstellungen**, klicken Sie auf **Modi konfigurieren** und wählen Sie **TCP-Pufferung**aus.

  Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **TCP-Parameter ändern**, geben Sie Werte für **Puffergröße** und **Speicherauslastung** an.

Festlegen von Dienst- oder Virtual Server-spezifischen TCP-Parametern

Mithilfe von TCP-Profilen können Sie TCP-Parameter für Dienste und virtuelle Server angeben. Sie müssen ein TCP-Profil definieren (oder ein integriertes TCP-Profil verwenden) und das Profil mit dem entsprechenden Dienst und dem entsprechenden virtuellen Server verknüpfen.

> **Hinweis:**
>
> Sie können auch die TCP-Parameter von Standardprofilen gemäß Ihren Anforderungen ändern.

Sie können die TCP-Puffergröße auf Service-Ebene mit den durch die TCP-Pufferfunktion angegebenen Parametern angeben.

So geben Sie TCP-Konfigurationen auf Service- oder virtuelle Serverebene mit der Befehlszeilenschnittstelle an

Führen Sie an der Eingabeaufforderung folgende Schritte aus:

1. Konfigurieren Sie das TCP-Profil.

   ```
   set ns tcpProfile <profile-name>...
   <!--NeedCopy-->
   ```


2. Binden Sie das TCP-Profil an den Dienst oder den virtuellen Server.

```
    set service <name> ....
    <!--NeedCopy-->
```

Beispiel:

```
> set service service1 -tcpProfileName profile1
```

So binden Sie das TCP-Profil an den virtuellen Server:

```
set lb vserver <name> ....
<!--NeedCopy-->
```

Beispiel:

```
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

So geben Sie TCP-Konfigurationen auf Dienst- oder virtueller Serverebene mit der GUI an

Führen Sie an der GUI Folgendes aus:

1. Konfigurieren Sie das TCP-Profil.

   Navigieren Sie zu **System** > **Profile** > **TCP-Profile**und erstellen Sie das TCP-Profil.

2. Binden Sie das TCP-Profil an den Dienst oder den virtuellen Server.

   Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste/Virtuelle Server**, und erstellen Sie das TCP-Profil, das an den Dienst oder den virtuellen Server gebunden sein sollte.

Integrierte TCP-Profile

Zur einfacheren Konfiguration bietet NetScaler einige integrierte TCP-Profile. Überprüfen Sie die im Folgenden aufgeführten integrierten Profile und wählen Sie ein Profil aus und verwenden Sie es so, wie es ist, oder ändern Sie es so, dass es Ihren Anforderungen entspricht. Sie können diese Profile an Ihre erforderlichen Dienste oder virtuelle Server binden.

Eingebautes Profil	Beschreibung
nstcp_default_profile	Stellt die standardmäßigen globalen TCP-Einstellungen auf der Appliance dar.
nstcp_default_tcp_lan	Nützlich für Back-End-Serververbindungen, bei denen sich diese Server im selben LAN wie die Appliance befinden.

Eingebautes Profil	Beschreibung
nstcp_default_WAN	nützlich für WAN-Bereitstellungen.
nstcp_default_tcp_lan_thin_stream	Ähnlich wie nstcp_default_tcp_lan profile. Die Einstellungen sind jedoch auf Paketflüsse kleiner Größe abgestimmt.
nstcp_default_tcp_interactive_stream	Ähnlich wie nstcp_default_tcp_lan profile. Es hat jedoch einen reduzierten verzögerten ACK-Timer und ACK bei **PUSH-Paketeinstellungen** .
nstcp_default_tcp_lfp	Nützlich für lange Fatpipe-Netzwerke (WAN) auf der Clientseite. Lange Fatpipe-Netzwerke haben lange Verzögerungen, Leitungen mit hoher Bandbreite mit minimalem Paketabfall.
nstcp_default_tcp_lfp_thin_stream	Ähnlich wie nstcp_default_tcp_lfp profile. Die Einstellungen sind jedoch auf Paketflüsse kleiner Größe abgestimmt.
nstcp_default_tcp_lnp	Nützlich für lange schmale Kanalnetze (WAN) auf der Clientseite. Lange schmale Kanalnetze weisen gelegentlich einen erheblichen Paketverlust auf.
nstcp_default_tcp_lnp_thin_stream	Ähnlich wie nstcp_default_tcp_lnp profile. Die Einstellungen sind jedoch auf Paketflüsse kleiner Größe abgestimmt.
nstcp_internal_apps	Nützlich für interne Anwendungen auf der Appliance (z. B. GSLB-Sitesynchronisierung). Dies enthält abgestimmte Fensterskalierung und SACK-Optionen für die gewünschten Anwendungen. Dieses Profil sollte nicht an andere Anwendungen als interne Anwendungen gebunden sein.
nstcp_default_Mobile_profile	Nützlich für mobile Geräte.
nstcp_default_XA_XD_profile	Nützlich für die Bereitstellung von Citrix Virtual Apps and Desktops.

Beispiel für TCP-Konfigurationen

Beispiele für Beispielbeispiele für die Befehlszeilenschnittstelle zum Konfigurieren von folgenden

TCP gegen Spoofing-Angriffe verteidigen

Prior to RFC 5961 compliance support

So aktivieren Sie die RST-Fensterdämpfung und den SYN-Spoof-Schutz mit der CLI:

```
> set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -spoofSynDrop
   ENABLED
    Done
 > set lb vserver lbvserver1 -tcpProfileName profile1
    Done
<!--NeedCopy-->
```

So aktivieren Sie die RST-Fensterdämpfung und den SYN-Spoof-Schutz mit der GUI:

1. Navigieren Sie zu **System > Profile > TCP-Profile**und klicken Sie auf **Hinzufügen**, um ein TCP-Profil zu erstellen.
2. Wählen Sie **RST Window Attenuation** und **SYN-Spoof Protection aus.**
3. Klicken Sie auf **Erstellen**.

Ab NetScaler Version 14.1-4.x mit RFC 5961-Compliance-Unterstützung

So aktivieren Sie die RFC 5961-Konformität mit der CLI:

```
> set ns tcpProfile profile1 -rstWindowAttenuate DISABLED -spoofSynDrop
    DISABLED -rfc5961Compliance ENABLED
    Done
> set lb vserver lbvserver1 -tcpProfileName profile1
    Done
<!--NeedCopy-->
```

Um die Anzahl der pro Sekunde zulässigen Challenge-ACKs zu begrenzen, aktivieren Sie den Parameter `rfc5961ChallengeAckLimit`:

```
> set ns tcpParam -rfc5961ChlgAckLimit 100
 Done
<!--NeedCopy-->
```

So aktivieren Sie die RFC 5961-Konformität mit der GUI:

1. Navigieren Sie zu **System > Profile > TCP-Profile**und klicken Sie auf **Hinzufügen**, um ein TCP-Profil zu erstellen.

2. Klare **RST-Fensterdämpfung** und **SYN-Spoof-Schutz.**
3. Wählen Sie **RFC5961 Compliance** und klicken Sie auf **Erstellen.**
4. Navigieren Sie zu **System > Einstellungen > TCP-Parameter ändern**.
5. Geben Sie einen Wert in **RFC5961 Chlg Ack Limit** ein und klicken Sie auf **OK.**

Explicit Congestion Notification (ECN)

Aktivieren Sie ECN auf dem erforderlichen TCP-Profil.

```
    > set ns tcpProfile profile1 -ECN ENABLED
    Done
    > set lb vserver lbvserver1 -tcpProfileName profile1
    Done
<!--NeedCopy-->
```

Selektive Danksagung (SACK)

Aktivieren Sie SACK für das erforderliche TCP-Profil.

```
    > set ns tcpProfile profile1 -SACK ENABLED
    Done
    > set lb vserver lbvserver1 -tcpProfileName profile1
    Done
<!--NeedCopy-->
```

Bestätigung vorwärts (FACK)

Aktivieren Sie FACK für das erforderliche TCP-Profil.

```
> set ns tcpProfile profile1 -FACK ENABLED
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

Fensterskalierung (WS)

Aktivieren Sie die Fensterskalierung und legen Sie den Skalierungsfaktor für das gewünschte TCP-Profil fest.

```
set ns tcpProfile profile1  - WS ENABLED  - WSVal 9
Done
set lb vserver lbvserver1 -tcpProfileName profile1
Done
```



```
<!--NeedCopy-->
```

Maximale Segmentgröße (MSS)

Aktualisieren Sie die MSS-bezogenen Konfigurationen.

```
> set ns tcpProfile profile1  - mss 1460 - maxPktPerMss 512
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
<!--NeedCopy-->
```

NetScaler lernt das MSS eines virtuellen Servers

Aktivieren Sie NetScaler, um das VSS zu lernen und andere verwandte Konfigurationen zu aktualisieren.

```
> set ns tcpParam -learnVsvrMSS ENABLED  - mssLearnInterval 180 -
    mssLearnDelay 3600
Done
<!--NeedCopy-->
```

TCP Keep-Alive

Aktivieren Sie TCP Keep-Alive und aktualisieren Sie andere verwandte Konfigurationen.

```
> set ns tcpProfile profile1 -KA ENABLED -KaprobeUpdateLastactivity ENABLED
-KAconnIdleTime 900 -KAmaxProbes 3 -KaprobeInterval 75
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Puffergröße - mit TCP-Profil

Geben Sie die Puffergröße an.

```
> set ns tcpProfile profile1 -bufferSize 8190
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```


Puffergröße - Verwenden der TCP-Pufferfunktion

Aktivieren Sie die TCP-Pufferfunktion (global oder für einen Dienst) und geben Sie dann die Puffergröße und das Speicherlimit an.

```
> enable ns feature TCPB
Done
> set ns tcpbufParam -size 64 -memLimit 64
Done
```

MPTCP

Aktivieren Sie MPTCP und legen Sie dann die optionalen MPTCP-Konfigurationen fest.

```
> set ns tcpProfile profile1 -mptcp ENABLED
Done
> set ns tcpProfile profile1 -mptcpDropDataOnPreEstSF ENABLED -mptcpFastOpen
 ENABLED -mptcpSessionTimeout 7200
Done
> set ns tcpparam -mptcpConCloseOnPassiveSF ENABLED -mptcpChecksum ENABLED
-mptcpSFtimeout 0 -mptcpSFReplaceTimeout 10
-mptcpMaxSF 4 -mptcpMaxPendingSF 4 -mptcpPendingJoinThreshold 0 -mptcpRTOsToSwitchSF
 2 -mptcpUseBackupOnDSS ENABLED
Done
```

Überlastungskontrolle

Stellen Sie den erforderlichen Algorithmus zur TCP-Überlastungssteuerung ein.

```
set ns tcpProfile profile1 -flavor Westwood
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Dynamische Empfangspufferung

Aktivieren Sie die dynamische Empfangspufferung für das erforderliche TCP-Profil.

```
> set ns tcpProfile profile1 -dynamicReceiveBuffering ENABLED
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```


Unterstützung für TCP Fast Open (TFO) in Multipath TCP (MPTCP)

Eine NetScaler-Appliance unterstützt jetzt den TCP Fast Open (TFO) -Mechanismus zum Herstellen von Multipath-TCP-Verbindungen (MPTCP) und zur Beschleunigung von Datenübertragungen. Der Mechanismus ermöglicht die Übertragung von Subflow-Daten während des anfänglichen MPTCP-Verbindungshandshake in SYN- und SYN-ACK-Paketen und ermöglicht auch die Verwendung von Daten durch den empfangenden Knoten während des Verbindungsaufbaus der MPTCP-Verbindung.

Weitere Informationen finden Sie unter Thema TCP Fast Open .

Unterstützung für variable TFO-Cookiegröße für MPTCP

Mit einer NetScaler-Appliance können Sie jetzt ein TCP-Fast Open (TFO) Cookie mit einer Mindestgröße von 4 Byte und einer maximalen Größe von 16 Byte in einem TCP-Profil konfigurieren. Auf diese Weise kann die Appliance mit der konfigurierten TFO-Cookie-Größe im SYN-ACK-Paket auf den Client reagieren.

So konfigurieren Sie das TCP-Fast Open (TFO) Cookie in einem TCP-Profil über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize <positive_integer
>
```

Beispiel

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize 8
```

So konfigurieren Sie das TCP-Fast Open (TFO) Cookie in einem TCP-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Konfiguration** > **System** > Profile.
2. Wechseln Sie im Detailbereich zur Registerkarte **TCP-Profile** und wählen Sie ein TCP-Profil aus.
3. Legen Sie auf der Seite **TCP-Profil konfigurieren** die Größe des **TCP-Fast Open-Cookies** fest.
4. Klicken Sie auf **OK** und **Fertig**.

Syn-Cookie-Zeitüberschreitungsintervall

Der Parameter `TCPSyncookie` ist in TCP-Profilen standardmäßig aktiviert, um einen robusten (RFC 4987) basierten Schutz vor SYN-Angriffen zu bieten. Wenn Sie benutzerdefinierte TCP-Clients aufnehmen müssen, die mit diesem Schutz nicht kompatibel sind, aber dennoch einen Fallback im Falle eines Angriffs sicherstellen möchten, `synAttackDetection` bewältigt dies für Sie, indem Sie das `SYNCookie`-Verhalten automatisch intern für einen Zeitraum aktivieren, der durch den Parameter `autosyncookietimeout` bestimmt wird.

So konfigurieren Sie den maximalen Schwellenwert für SYN ACK-Neuübertragungen über die Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1     set ns tcpparam [-maxSynAckRetx <positive_integer>]
2
3     Set ns tcpparam [-maxSynAckRetx 150]
4 <!--NeedCopy-->
```

So konfigurieren Sie das Timeout-Intervall des automatischen SYN-Cookies über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns tcpparam [-autosyncookietimeout <positive_integer>]
```

```
Set ns tcpparam [-autosyncookietimeout 90]
```

Delink Client- und Serververbindung

Wenn diese Option aktiviert ist, löscht der Parameter die Client- und Serververbindung, wenn noch ausstehende Daten an die andere Seite gesendet werden sollen. In der Standardeinstellung ist der Parameter deaktiviert.

```
1 set ns tcpparam -delinkClientServerOnRST ENABLED
2 Done
3
4 <!--NeedCopy-->
```

Konfigurieren Sie den Schwellenwertparameter für langsamen Start

Sie können den Schwellenwertparameter `slowStartthreshold` für langsamen Start verwenden, um den Wert `tcp-slowstartthreshold` für die Variante `Nile` des Algorithmus zur Überlastungskontrolle zu konfigurieren. Die akzeptablen Werte für den Parameter sind `min = 8190` und `max = 524288`. Der Standardwert ist `524288`. Die TCP-Variante `Nile` unter dem TCP-Profil ist nicht mehr vom Parameter `maxcwnd` abhängig. Sie müssen den Parameter `slowStartthreshold` für die Variante `Nile` konfigurieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set tcpprofile nstcp_default_profile -slowstartthreshold 8190
2 Done
3
4 <!--NeedCopy-->
```


HTTP-Konfigurationen

May 11, 2023

> **Wichtig:**
>
> Ab NetScaler Release 13.0 Build 71.x kann eine NetScaler-Appliance HTTP-Anfragen mit großen Header-Größen verarbeiten, um die L7-Anwendungsanforderungen zu erfüllen. Die Header-Größe kann bis zu 128 KB konfigurierbar sein.

HTTP-Konfigurationen für eine NetScaler-Appliance können in einer Entität angegeben werden, die als HTTP-Profil bezeichnet wird, bei der es sich um eine Sammlung von HTTP-Einstellungen handelt. Das HTTP-Profil kann dann mit Diensten oder virtuellen Servern verknüpft werden, die diese HTTP-Konfigurationen verwenden möchten.

Ein Standard-HTTP-Profil kann konfiguriert werden, um die HTTP-Konfigurationen festzulegen, die standardmäßig global auf alle Dienste und virtuellen Server angewendet werden.

> **Hinweis:**
>
> Wenn ein HTTP-Parameter unterschiedliche Werte für Service, virtuellen Server und global aufweist, erhält der Wert der spezifischsten Entität (des Dienstes) die höchste Priorität.

Die NetScaler-Appliance bietet auch andere Ansätze zur Konfiguration von HTTP. Lesen Sie weiter für weitere Informationen.

Der NetScaler unterstützt ein WebSocket-Protokoll, das es Browsern und anderen Clients ermöglicht, eine bidirektionale Vollduplex-TCP-Verbindung zu den Servern herzustellen. Die NetScaler-Implementierung von WebSocket ist RFC 6455 konform.

> **Hinweis:**
>
> Eine NetScaler-Appliance unterstützt die Konfiguration der User Source IP (USIP) -Adresse für die Protokolle HTTP/1.1 und HTTP/2.

Einstellen globaler HTTP-Parameter

Mit der NetScaler-Appliance können Sie Werte für HTTP-Parameter angeben, die für alle NetScaler-Dienste und virtuellen Server gelten. Dies kann geschehen mit:

- Standard-HTTP-Profil
- Globaler HTTP-Befehl

Standard-HTTP-Profil

Ein HTTP-Profil mit dem Namen nshttp_default_profile wird verwendet, um HTTP-Konfigurationen anzugeben, die verwendet werden, wenn auf Dienst- oder virtueller Serverebene keine HTTP-Konfigurationen bereitgestellt werden.

> **Hinweise:**
>
> - Nicht alle HTTP-Parameter können über das Standard-HTTP-Profil konfiguriert werden. Einige Einstellungen werden mit dem globalen HTTP-Befehl vorgenommen (siehe folgenden Abschnitt).
> - Das Standardprofil muss nicht explizit an einen Dienst oder einen virtuellen Server gebunden sein.

So konfigurieren Sie das Standard-HTTP-Profil

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:

  ```
  set ns httpProfile nshttp_default_profile ...
  ```

- Navigieren Sie auf der GUI zu **System** > **Profile**, klicken Sie auf **HTTP-Profile** und aktualisieren Sie nshttp_default_profile.

Globaler HTTP-Befehl

Ein anderer Ansatz, mit dem Sie globale HTTP-Parameter konfigurieren können, ist der globale HTTP-Befehl. Zusätzlich zu einigen eindeutigen Parametern dupliziert dieser Befehl einige Parameter, die mithilfe eines HTTP-Profils festgelegt werden können. Jede Aktualisierung dieser doppelten Parameter spiegelt sich im entsprechenden Parameter im Standard-HTTP-Profil wider.

Wenn beispielsweise der maxReusePool-Parameter mit diesem Ansatz aktualisiert wird, wird der Wert im maxReusePool-Parameter des Standard-HTTP-Profils (nshttp_default_profile) widergespiegelt.

> **Hinweis:**
>
> Wir empfehlen Ihnen, diesen Ansatz nur für HTTP-Parameter zu verwenden, die im Standard-HTTP-Profil nicht verfügbar sind.

So konfigurieren Sie den globalen HTTP-Befehl

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:

  ```
  set ns httpParam ...
  ```

- Navigieren Sie auf der GUI zu **System > Einstellungen**, klicken Sie auf **HTTP-Parameter ändern** und aktualisieren Sie die erforderlichen HTTP-Parameter.

So konfigurieren Sie ein Ignorieren-Codierungsschema für Connect-Anfrage

Um HTTP/2 zu aktivieren und HTTP/2-Parameter so festzulegen, dass das Codierungsschema in der Verbindungsanforderung ignoriert wird, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpParam [-ignoreConnectCodingScheme ( ENABLED | DISABLED )]
```

Beispiel:

```
set ns httpParam -ignoreConnectCodingScheme ENABLED
```

So binden Sie das HTTP-Profil über die NetScaler-Befehlszeile an einen virtuellen Server

Konfigurieren Sie das HTTP-Profil zum Löschen von ungültigen TRACE- oder TRACK-Anfragen

Sie können den markTraceReqInval-Parameter aktivieren, um TRACK- und TRACK-Anfragen als ungültig zu markieren. Wenn Sie diese Option zusammen mit der Option dropInvalidReqs für die virtuelle IP-Adresse aktivieren, können Sie einen Client zurücksetzen, der TRACE- oder TRACK-Anfragen an eine NetScaler-Appliance sendet.

So konfigurieren Sie das HTTP-Profil mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns httpProfile <profile name> [-markTraceReqInval ENABLED | DISABLED ]
```

Beispiel:

```
set ns httpProfile profile1 -markTraceReqInval ENABLED
```

Konfigurieren des HTTP-Profils für eine Dienstgruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add serviceGroup <serviceGroupName>@ <serviceType> [-cacheType <
    cacheType>] [-td <positive_integer>] [-maxClient <positive_integer>]
     [-maxReq <positive_integer>] [-cacheable ( YES | NO )] [-cip (
    ENABLED | DISABLED ) [<cipHeader>]] [-usip ( YES | NO )] [-
    pathMonitor ( YES | NO )] [-pathMonitorIndv ( YES | NO )] [-
    useproxyport ( YES | NO )] [-healthMonitor ( YES | NO )] [-sp ( ON |
     OFF )] [-rtspSessionidRemap ( ON | OFF )] [-cltTimeout <secs>] [-
    svrTimeout <secs>] [-CKA ( YES | NO )] [-TCPB ( YES | NO )] [-CMP (
    YES | NO )] [-maxBandwidth
2 <positive_integer>] [-monThreshold <positive_integer>] [-state ENABLED
    DISABLED )][-downStateFlush ( ENABLED | DISABLED )] [-tcpProfileName
     <string>] [-httpProfileName <string>] [-comment <string>] [-
    appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-
    autoScale <autoScale> -memberPort <port> [-autoDisablegraceful ( YES
```



```
        | NO )] [-autoDisabledelay <secs>] ] [-monConnectionClose ( RESET |
        FIN )]
3
4 <!--NeedCopy-->
```

Beispiel:

```
add serviceGroup Service-Group-1 HTTP -maxClient 0 -maxReq 0 -cip ENABLED -
usip NO -useproxyport YES -cltTimeout 200 -svrTimeout 300 -CKA NO -TCPB NO
-CMP NO -httpProfileName profile1
```

Konfigurieren Sie das HTTP-Profil mit der NetScaler GUI

Führen Sie das folgende Verfahren aus, um TRACE oder TRACK ungültige Anfragen zu markieren.

1. Melden Sie sich bei der NetScaler-Appliance an und navigieren Sie zu **Konfiguration** > **System** > **Profile**.
2. Klicken Sie auf der Registerkarte **HTTP-Profile** auf **Hinzufügen**.
3. Wählen Sie auf der Seite **HTTP-Profil erstellen** die Option **TRACE-Anfragen als ungültig markieren** aus.
4. Klicken Sie auf **Erstellen**.

Festlegen von dienst- oder virtuellen serverspezifischen HTTP-Parametern

Mithilfe von HTTP-Profilen können Sie HTTP-Parameter für Dienste und virtuelle Server angeben. Sie müssen ein HTTP-Profil definieren (oder ein integriertes HTTP-Profil verwenden) und das Profil mit dem entsprechenden Dienst und dem entsprechenden virtuellen Server verknüpfen.

> **Hinweis:**
>
> Sie können auch die HTTP-Parameter von Standardprofilen gemäß Ihren Anforderungen ändern.

So geben Sie HTTP-Konfigurationen auf Service- oder virtuelle Serverebene mit der Befehlszeilenschnittstelle an

Führen Sie an der Eingabeaufforderung folgende Schritte aus:

1. Konfigurieren Sie das HTTP-Profil.

   ```
   set ns httpProfile <profile-name>...
   ```

2. Binden Sie das HTTP-Profil an den Dienst oder den virtuellen Server.

   So binden Sie das HTTP-Profil an den Dienst:


```
set service <name> .....
```

Beispiel:

```
1 > set service service1 -httpProfileName profile1
2 <!--NeedCopy-->
```

So binden Sie das HTTP-Profil an den virtuellen Server:

```
set lb vserver <name> .....
```

Beispiel:

```
1 > set lb vserver lbvserver1 -httpProfileName profile1
2 <!--NeedCopy-->
```

So geben Sie HTTP-Konfigurationen auf Dienstebene oder virtuelle Serverebene mit der GUI an

Führen Sie an der GUI Folgendes aus:

1. Konfigurieren Sie das HTTP-Profil.

   Navigieren Sie zu **System** > **Profile** > **HTTP-Profile** und erstellen Sie das HTTP-Profil.

2. Binden Sie das HTTP-Profil an den Dienst oder den virtuellen Server.

   Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste/Virtuelle Server** und erstellen Sie das HTTP-Profil, das an den Service/virtuellen Server gebunden sein muss.

Integrierte HTTP-Profile

Zur Vereinfachung der Konfiguration bietet der NetScaler einige integrierte HTTP-Profile. Überprüfen Sie die aufgelisteten Profile und verwenden Sie sie so, wie es ist, oder ändern Sie sie an Ihre Anforderungen. Sie können diese Profile an die erforderlichen Dienste oder virtuellen Server binden.

Eingebautes Profil	Beschreibung
nshttp_default_profile	Stellt die standardmäßigen globalen HTTP-Einstellungen auf der Appliance dar.
nshttp_default_strict_validation	Einstellungen für Bereitstellungen, die eine strikte Validierung von HTTP-Anfragen und -Antworten erfordern.

Beispiel für HTTP-Konfigurationen

Beispiele für Beispiele für eine Befehlszeilenschnittstelle, um Folgendes zu konfigurieren:

- HTTP-Band-Statistiken
- WebSocket-Verbindungen

HTTP-Band-Statistiken

Geben Sie die Bandgröße für HTTP-Anfragen und -Antworten an.

```
> set protocol httpBand reqBandSize 300 respBandSize 2048
Done
> show protocol httpband -type REQUEST
<!--NeedCopy-->
```

WebSocket-Verbindungen

Aktivieren Sie WebSocket für das erforderliche HTTP-Profil.

```
> set ns httpProfile http_profile1 -webSocket ENABLED
Done
> set lb vserver lbvserver1 -httpProfileName profile1
Done
<!--NeedCopy-->
```

Konfigurieren Sie die NetScaler-Appliance so, dass der Upgrade-Header gelöscht oder an den Backend-Server übergeben wird

Der Parameter PassProtocolUpgrade im HTTP-Profil verhindert Angriffe auf die Backend-Server. Abhängig vom Status dieses Parameters wird der Upgrade-Header in der an den Back-End-Server gesendeten Anfrage übergeben oder vor dem Senden der Anfrage gelöscht.

- Wenn der Parameter PassProtocolUpgrade aktiviert ist, wird der Upgrade-Header an den Back-End-Server übergeben. Der Server akzeptiert die Upgrade-Anfrage und benachrichtigt sie in seiner Antwort.
- Wenn der Parameter deaktiviert ist, wird der Upgrade-Header gelöscht und die verbleibende Anfrage wird an den Backend-Server gesendet.

Der Parameter passProtocolUpgrade wird den folgenden Profilen hinzugefügt:

- nshttp_default_profile - standardmäßig aktiviert
- nshttp_default_strict_validation - standardmäßig deaktiviert
- nshttp_default_internal_apps - standardmäßig deaktiviert

- nshttp_default_http_quic_profile — standardmäßig aktiviert

Wir empfehlen Ihnen, den Parameter PassProtocolUpgrade standardmäßig auf disabled zu setzen.

Stellen Sie den PassProtocolUpgrade-Parameter über die CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpProfile <name> [-passProtocolUpgrade ( ENABLED | DISABLED )]
```

Beispiel:

```
set ns httpProfile profile1 -passProtocolUpgrade ENABLED
```

Stellen Sie den PassProtocolUpgrade-Parameter mithilfe der GUI ein

1. Navigieren Sie zu **System > Profile > HTTP-Profile**.
2. Erstellen oder bearbeiten Sie ein HTTP-Profil.
3. Wählen Sie **Pass Protocol Upgrade**aus.

HTTP/2-Konfiguration

May 11, 2023

> **Hinweis:**
> Die HTTP/2-Funktionalität wird von den NetScaler MPX-, VPX- und SDX-Modellen unterstützt. In einer NetScaler VPX-Appliance wird die HTTP/2-Funktionalität ab NetScaler Version 11.0 unterstützt.

Das Problem mit der Leistung von Webanwendungen hängt direkt mit dem Trend zur Erhöhung der Seitengröße und der Anzahl der Objekte auf den Webseiten zusammen. HTTP/1.1 wurde entwickelt, um kleinere Webseiten, langsamere Internetverbindungen und eingeschränktere Serverhardware als heute üblich zu unterstützen. Es ist nicht für neue Technologien wie JavaScript und Cascading Stylesheets (CSS) oder neue Medientypen wie Flash-Videos und grafikreiche Bilder geeignet. Dies liegt daran, dass nur eine Ressource pro Verbindung zum Server angefordert werden kann. Die Einschränkung erhöht die Anzahl der Roundtrips erheblich, was zu einem längeren Seitenrendern und einer verringerten Netzwerkleistung führt.

Das HTTP/2-Protokoll behebt diese Einschränkungen, indem es die Kommunikation mit weniger über das Netzwerk übertragenen Daten ermöglicht und die Möglichkeit bietet, mehrere Anfragen und Antworten über eine einzige Verbindung zu senden. Im Kern behebt HTTP/2 die wichtigsten Einschränkungen von HTTP/1.1, indem die zugrunde liegenden Netzwerkverbindungen effizienter

genutzt werden. Es verändert die Art und Weise, wie Anfragen und Antworten über das Netzwerk übertragen werden.

HTTP/2 ist ein binäres Protokoll. Es ist effizienter zu analysieren, kompakter auf dem Kabel und vor allem weniger fehleranfällig im Vergleich zu Textprotokollen wie HTTP/1.1. Das HTTP/2-Protokoll verwendet eine binäre Framing-Schicht, die den Frame-Typ und die Art und Weise definiert, wie HTTP-Nachrichten eingekapselt und zwischen Client und Server übertragen werden. Die HTTP/2-Funktionalität unterstützt die Verwendung der CONNECT-Methode zum Herstellen einer Tunnelverbindung über einen einzelnen HTTP/2-Stream zu einem Remote-Host.

Das HTTP/2-Protokoll enthält viele leistungssteigernde Änderungen, die die Leistung erheblich verbessern, insbesondere für Clients, die sich über ein Mobilfunknetz verbinden.

In der folgenden Tabelle sind die wichtigsten Verbesserungen in HTTP/2 gegenüber HTTP/1.1 aufgeführt:

HTTP/2-Funktionen	Beschreibung
Kopfzeilenkomprimierung	HTTP-Header haben viele sich wiederholende Informationen und verbrauchen daher unnötige Bandbreite während der Datenübertragung. HTTP/2 reduziert die Bandbreitenanforderungen, indem der Header komprimiert und die Anforderung minimiert wird, HTTP-Header mit jeder Anforderung und Antwort zu transportieren.
Verbindungs-Multiplexing	Die Latenz kann einen enormen Einfluss auf die Ladezeiten der Seite und die Benutzererfahrung haben. Das Verbindungsmultiplexing überwindet dieses Problem, indem mehrere Anfragen und Antworten über eine einzige Verbindung gesendet werden.
Server-Push	Server-Push ermöglicht es dem Server, Inhalte proaktiv an den Client-Browser zu übertragen, wodurch Roundtrip-Verzögerungen vermieden werden. Diese Funktion speichert die Antworten, die der Kunde benötigt, im Cache, reduziert die Anzahl von Roundtrips und verbessert die Seitenrendering-Zeit. Wichtig: Die NetScaler-Appliance unterstützt die Server-Push-Funktionalität nicht.

HTTP/2-Funktionen	Beschreibung
Keine Kopf-of-Line-Blockierung	Unter HTTP 1.1 können Browser pro Verbindung jeweils eine Ressource herunterladen. Wenn ein Browser eine große Ressource herunterladen muss, blockiert er alle anderen Ressourcen, bis der erste Download abgeschlossen ist. HTTP/2 überwindet dieses Problem mit einem Multiplexing-Ansatz. Es ermöglicht dem Client-Browser, andere Webkomponenten parallel über dieselbe Verbindung herunterzuladen und anzuzeigen, sobald sie verfügbar sind.
Priorisierung anfordern	Nicht alle Ressourcen haben die gleiche Priorität, wenn der Browser eine Webseite rendert. Um die Ladezeit zu beschleunigen, priorisieren alle modernen Browser Anfragen nach Art des Assets, ihrem Standort auf der Seite und sogar nach erlernter Priorität aus früheren Besuchen. Mit HTTP/1.1 kann der Browser die Prioritätsdaten nur eingeschränkt verwenden, da dieses Protokoll kein Multiplexing unterstützt und es keine Möglichkeit gibt, die Anforderungspriorisierung durch den Server zu kommunizieren. Das Ergebnis ist eine unnötige Netzwerklatenz. HTTP/2 überwindet dieses Problem, indem es dem Browser erlaubt, alle Anfragen zu versenden. Der Browser kann seine Präferenz für die Stream-Priorisierung über Stream-Abhängigkeiten und Gewichte kommunizieren, wodurch die Server die Antwortbereitstellung optimieren können. Wichtig: Die NetScaler-Appliance unterstützt die Funktion zur Anforderungspriorisierung nicht.

So funktioniert HTTP/2

Eine NetScaler-Appliance unterstützt HTTP/2 sowohl clientseitig als auch serverseitig. Auf der Clientseite fungiert die NetScaler-Appliance als Server, der einen virtuellen HTTP/HTTPS-Server für HTTP/2 hostet. Auf der Back-End-Seite fungiert der NetScaler als Client für die Server, die an den virtuellen Server gebunden sind.

Daher unterhält die NetScaler-Appliance separate Verbindungen sowohl auf der Clientseite als auch auf der Serverseite. Die NetScaler-Appliance verfügt über separate HTTP/2-Konfigurationen für die Client- und Serverseite.

HTTP/2 für HTTPS (SSL) -Lastausgleichskonfiguration

Für eine HTTPS-Lastausgleichskonfiguration verwendet die NetScaler-Appliance die TLS ALPN-Erweiterung (RFC 7301), um festzustellen, ob der Client/Server HTTP/2 unterstützt. Wenn dies der Fall ist, wählt die Appliance HTTP/2 als Protokoll der Anwendungsschicht, um Daten (wie in RFC 7540 - Abschnitt 3.3 beschrieben) auf der Client-/Serverseite zu übertragen.
Die Appliance verwendet bei der Auswahl des Anwendungsschicht-Protokolls über die TLS-ALPN-Erweiterung die folgende Präferenzreihenfolge:

- HTTP/2 (falls im HTTP-Profil aktiviert)
- HTTP/1.1

HTTP/2 für die Konfiguration des HTTP-Lastausgleichs

Für eine HTTP-Lastausgleichskonfiguration verwendet die NetScaler-Appliance eine der folgenden Methoden, um mit dem Client/Server über HTTP/2 zu kommunizieren.

> **Hinweis**
>
> In den folgenden Methodenbeschreibungen sind Client und Server allgemeine Begriffe für eine HTTP/2-Verbindung. Beispielsweise fungiert die NetScaler-Appliance für ein Lastausgleichs-Setup einer NetScaler-Appliance mit HTTP/2 als Server auf der Clientseite und fungiert als Client für die Serverseite.

- **HTTP/2-Upgrade**. Ein Client sendet eine HTTP/1.1-Anfrage an einen Server. Die Anforderung enthält einen Upgrade-Header, der den Server auffordert, die Verbindung auf HTTP/2 zu aktualisieren. Wenn der Server HTTP/2 unterstützt, akzeptiert der Server die Upgrade-Anforderung und benachrichtigt ihn in seiner Antwort. Der Client und der Server beginnen mit der Kommunikation über HTTP/2, nachdem der Client die Upgrade-Bestätigungsantwort erhalten hat.
- **Direkt HTTP/2**. Ein Client beginnt direkt mit einem Server in HTTP/2 zu kommunizieren, anstatt die HTTP/2-Upgrade-Methode zu verwenden. Wenn der Server HTTP/2 nicht unterstützt oder nicht für die direkte Annahme von HTTP/2-Anfragen konfiguriert ist, löscht er die HTTP/2-Pakete

vom Client. Diese Methode ist hilfreich, wenn der Administrator des Clientgeräts bereits weiß, dass der Server HTTP/2 unterstützt.

- **Direkte HTTP/2 mithilfe des alternativen Dienstes (ALT-SVC).** Ein Server kündigt an, dass er HTTP/2 für einen Client unterstützt, indem er ein Feld für den alternativen Dienst (ALT-SVC) in seine HTTP/1.1-Antwort einschließt. Wenn der Client so konfiguriert ist, dass er das Feld ALT-SVC versteht, beginnen der Client und der Server direkt über HTTP/2 zu kommunizieren, nachdem der Client die Antwort erhalten hat.

Die NetScaler-Appliance bietet konfigurierbare Optionen in einem HTTP-Profil für die HTTP/2-Methoden. Diese HTTP/2-Optionen können sowohl auf die Clientseite als auch auf die Serverseite eines HTTPS- oder HTTP-Lastausgleichs angewendet werden. Weitere Informationen zu HTTP/2-Methoden und Optionen finden Sie im PDF-Format HTTP/2-Optionen .

Bevor Sie beginnen

Beachten Sie die folgenden Punkte, bevor Sie mit der Konfiguration von HTTP/2 auf einer NetScaler-Appliance beginnen:

- Die NetScaler-Appliance unterstützt HTTP/2 sowohl clientseitig als auch serverseitig.
- Die NetScaler-Appliance unterstützt die HTTP/2-Server-Push-Funktionalität nicht.
- Die NetScaler-Appliance unterstützt die HTTP/2-Anforderungspriorisierungsfunktion nicht.
- Die NetScaler-Appliance unterstützt keine HTTP/2-SSL-Neuverhandlung für HTTPS-Lastausgleichseinrichtun
- Die NetScaler-Appliance unterstützt keine HTTP/2-NTLM-Authentifizierung.
- Wenn HTTP/2 aktiviert ist, Verbindungsmultiplexing deaktiviert (wie USIP aktiviert) und Eins-zu-Eins-Zuordnung von Client- und Server-TCP-Verbindungen werden Close-Ereignisse wie FIN, Reset (RST) von der Client- oder Serververbindung zur verknüpften Peer-Verbindung weitergeleitet.

Konfigurieren von HTTP/2

Die Konfiguration von HTTP/2 für ein Lastausgleichs-Setup (HTTPS oder HTTP) umfasst die folgenden Aufgaben:

- **Aktivieren Sie HTTP/2 und setzen Sie optionale HTTP/2-Parameter in einem HTTP-Profil**. Aktivieren Sie HTTP/2 in einem HTTP-Profil. Wenn Sie nur HTTP/2 in einem HTTP-Profil aktivieren, verwendet die NetScaler-Appliance nur die Upgrade-Methode (für HTTP) oder die TLS-ALPN-Methode (für HTTPS) für die Kommunikation in HTTP/2.

  Damit die NetScaler-Appliance die direkte HTTP/2-Methode verwenden kann, muss die Option **Direct HTTP/2** im HTTP-Profil aktiviert sein. Damit die NetScaler-Appliance das direkte HTTP/2 mit der alternativen Dienstmethode verwenden kann, muss die Option **Alternativer Dienst (altsvc)** im HTTP-Profil aktiviert sein.

- **Binden Sie das HTTP-Profil an einen virtuellen Server oder einen Dienst**. Binden Sie das HTTP-Profil an einen virtuellen Server, um HTTP/2 für die Clientseite des Lastausgleichs-Setups zu konfigurieren. Binden Sie das HTTP-Profil an einen Dienst, um HTTP2 für die Serverseite des Lastausgleichs-Setups zu konfigurieren.

> **Hinweis**
>
> Citrix empfiehlt, separate HTTP-Profile für die Client- und Serverseite zu binden.

- **Aktivieren Sie den globalen Parameter für die serverseitige Unterstützung von HTTP/2**. Aktivieren Sie den globalen **HTTP-Parameter HTTP/2 Service Side**(**HTTP2Serverside**), um die HTTP/2-Unterstützung auf der Serverseite aller Lastausgleichseinrichtungen zu aktivieren, die HTTP/2 konfiguriert haben.

  HTTP/2 funktioniert auf der Serverseite von Lastausgleichseinrichtungen nicht, wenn **HTTP/2 Service Side** deaktiviert ist, selbst wenn **HTTP/2 im HTTP-Profil** aktiviert ist, das an die zugehörigen Lastausgleichsdienste gebunden ist.

NetScaler-Befehlszeilenprozeduren:

So aktivieren Sie HTTP/2 und legen HTTP/2-Parameter über die NetScaler-Befehlszeile fest

- Um HTTP/2 zu aktivieren und HTTP/2-Parameter beim Hinzufügen eines HTTP-Profils festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )] [-altsvc ( ENABLED | DISABLED )]
show ns httpProfile <name>
```

- Um HTTP/2 zu aktivieren und HTTP/2-Parameter festzulegen, während Sie ein HTTP-Profil ändern, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED)] [-altsvc (ENABLED | DISABLED )]
show ns httpProfile <name>
```

So binden Sie das HTTP-Profil über die NetScaler-Befehlszeile an einen virtuellen Server

Geben Sie in der Befehlszeile Folgendes ein:

```
set lb vserver <name> - httpProfileName <string>
show lb vserver <name>
```

So binden Sie das HTTP-Profil über die NetScaler-Befehlszeile an einen Lastausgleichsdienst

Geben Sie in der Befehlszeile Folgendes ein:

```
set service <name> -httpProfileName <string>
show service <name>
```


So aktivieren Sie die HTTP/2-Unterstützung global auf der Serverseite über die NetScaler-Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns httpParam -HTTP2Serverside( ENABLED | DISABLED )
show ns httpParam
```

So aktivieren Sie HTTP/2 und legen Sie HTTP/2-Parameter über die NetScaler GUI fest

1. Navigieren Sie zu **System** > **Profile**und klicken Sie auf die Registerkarte **HTTP-Profile** .
2. Aktivieren Sie **HTTP/2**, während Sie ein HTTP-Profil hinzufügen oder ein vorhandenes HTTP-Profil ändern.

So binden Sie das HTTP-Profil über die NetScaler GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**und öffnen Sie den virtuellen Server.
2. Klicken Sie in den **Erweiterten Einstellungen**auf **+ HTTP-Profil**, um das erstellte HTTP-Profil an den virtuellen Server zu binden.

So binden Sie das HTTP-Profil über die NetScaler GUI an einen Lastausgleichsdienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service**, und öffnen Sie den Dienst.
2. Klicken Sie in den **Erweiterten Einstellungen**auf **+ HTTP-Profil**, um das erstellte HTTP-Profil an den Dienst zu binden.

So aktivieren Sie die HTTP/2-Unterstützung global auf der Serverseite über die GUI

Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **HTTP-Parameter ändern** und aktivieren Sie **HTTP/2 Serverseite**.

Beispielkonfigurationen

In der folgenden Beispielkonfiguration ist HTTP/2 und direktes HTTP/2 im HTTP-Profil HTTP-PROFILE-HTTP2-CLIENT-SIDE aktiviert. Das Profil ist an den virtuellen Server LB-VS-1 gebunden.

```
1 set ns httpProfile HTTP-PROFILE-HTTP2-CLIENT-SIDE -http2 enabled -
     http2Direct enabled
2 Done
3
4 set lb vserver LB-VS-1 -httpProfileName HTTP-PROFILE-HTTP2-CLIENT-SIDE
5
6 Done
7 <!--NeedCopy-->
```

In der folgenden Beispielkonfiguration ist HTTP/2 und alternativer Dienst (ALT-SVC) im HTTP-Profil HTTP-PROFILE-HTTP2-SERVER-SIDE aktiviert. Das Profil ist an Service LB-SERVICE-1 gebunden.


```
set ns httpparam -HTTP2Serverside ENABLED
Done

set ns httpProfile HTTP-PROFILE-HTTP2-SERVER-SIDE -http2 ENABLED -
   altsvc ENABLED
Done

set service LB-SERVICE-1 -httpProfileName HTTP-PROFILE-HTTP2-SERVER-
   SIDE
Done
<!--NeedCopy-->
```

Konfigurieren Sie die Fenstergröße der HTTP/2-Erstverbindung

Gemäß RFC 7540 muss das Flusssteuerungsfenster für den HTTP2-Stream und die Verbindung auf 64 K (65535) Oktette eingestellt sein, und jede Änderung an diesem Wert muss dem Peer mitgeteilt werden. Die ADC-Appliance kommuniziert die Änderung der Fenstergröße der Durchflusssteuerung wie folgt:

- Verwenden des Frames `SETTINGS` für den Stream.
- Verwenden des Frames `WINDOW_UPDATE` für die Verbindung.

In einem HTTP-Profil müssen Sie den Parameter `http2InitialWindowSize` so konfigurieren, dass die anfängliche Fenstergröße auf Streamebene festgelegt wird. Aufgrund eines internen Systemfehlers initialisiert die ADC-Appliance auch das Flusssteuerungsfenster für die Verbindung. Wenn sich das konfigurierte Flusssteuerungsfenster für den Stream ändert, kommuniziert die ADC-Appliance über den Frame SETTINGS mit dem Peer. Die ADC-Appliance kommuniziert jedoch die Änderung des Flusssteuerungsfensters für die Verbindung über den Frame `WINDOW_UPDATE` nicht. Dies führt zu einem Einfrieren der Verbindung.

Um das Problem zu beheben, wird nun der Parameter `http2InitialConnWindowSize` (in Byte) hinzugefügt, um das Flusssteuerungsfenster für die Verbindung zu steuern. Mithilfe separater konfigurierbarer Parameter können Sie der Appliance jetzt ermöglichen, Updates für die geänderte Fenstergröße sowohl auf Stream- als auch auf Verbindungsebene zu senden.

Konfigurieren Sie den Größenparameter für das erste Verbindungsfenster HTTP/2 mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set http profile p1 -http2InitialConnWindowSize 8290
Initial window size for stream level flow control, in bytes.
Default value: 65535
Minimum value: 8192
Maximum value: 20971520
```



```
<!--NeedCopy-->
```

> **Hinweis:**
> Wenn HTTP/2 aktiviert ist, empfiehlt Citrix, den Parameter TCP Dynamic Receive Buffering im TCP-Profil zu deaktivieren.

Konfiguration von WebSocket über HTTP/2

Die NetScaler-Appliance unterstützt WebSocket-Verbindungen über HTTP/2. Sie können die WebSocket-Verbindungen über die CLI- oder GUI-Schnittstelle aktivieren. Die WebSocket-HTTP/2-Verbindung kann gemultiplext werden.

WebSocket-Verbindungen über HTTP/2 in der CLI konfigurieren

Standardmäßig ist der Parameter **WebSocket Connections** deaktiviert. Sie können die WebSocket-Verbindungen über die CLI-Schnittstelle aktivieren.

Frontend-HTTP/2-WebSocket-Verbindungen aktivieren:

Geben Sie in der Befehlszeile Folgendes ein:

Für die SSL-Konfiguration:

```
add httpprofile <http_profile_name> -http2 enabled -websocket enabled

<!--NeedCopy-->
```

Für die Konfiguration im Klartext:

```
add httpprofile <http_profile_name> -http2 enabled -http2direct enabled
    -websocket enabled

<!--NeedCopy-->
```

Aktivieren Sie Backend-HTTP/2-WebSocket-Verbindungen:

Geben Sie in der Befehlszeile Folgendes ein:

Für die SSL-Konfiguration:

```
add httpprofile <http_profile_name> -http2 enabled
set httpparam -http2serverside ON
<!--NeedCopy-->
```

Für die Konfiguration im Klartext:


```
add httpprofile <http_profile_name> -http2 enabled -http2direct enabled
set httpparam -http2serverside ON
<!--NeedCopy-->
```

WebSocket-Verbindungen über HTTP/2 in der GUI konfigurieren

Sie können das folgende Verfahren verwenden, um die WebSocket-Verbindungen über die GUI-Schnittstelle zu aktivieren.

Bearbeiten Sie die vorhandenen Profile:

1. Navigieren Sie zu **System>Profile>HTTP-Profile**.
2. Wählen Sie das gewünschte Profil aus den **Profilen** aus und klicken Sie auf **Bearbeiten**.
3. Aktivieren Sie im Feld **HTTP-Profil konfigurieren** die Kontrollkästchen **HTTP2** oder **DirectHTTP2**.
4. Aktivieren Sie die WebSocket-Verbindungen, indem Sie das Kontrollkästchen **WebSocket-Verbindungen aktivieren** aktivieren.

Neue Profile hinzufügen:

1. Navigieren Sie zu **System>Profile>HTTP-Profile**.
2. Sie können ein neues HTTP2-Profil hinzufügen, indem Sie auf **Hinzufügen**klicken.
3. Aktivieren Sie im Feld **HTTP-Profil erstellen** die Kontrollkästchen **HTTP2** oder **DirectHTTP2**.
4. Aktivieren Sie das Kontrollkästchen **WebSocket-Verbindungen aktivieren**.

In der folgenden Tabelle wird das WebSocket-Verbindungsverhalten beschrieben, wenn das Backend-Multiplexing deaktiviert ist:

HTTP-Paketversion	WebSocket im HTTP-Profil	Aktion anfordern	HTTP/1.1 Backend	HTTP/2-Backend
HTTP/1.1	Deaktiviert	fallen gelassen	Nicht verfügbar	Nicht verfügbar
HTTP/1.1	Aktiviert	HTTP/1.1	Jede HTTP/1.1-Verbindung ist einer dedizierten HTTP/1.1-Verbindung im Backend zugeordnet	Dedizierte HTTP/2-Verbindung im Backend für jede HTTP/1.1-Verbindung

HTTP-Paketversion	WebSocket im HTTP-Profil	Aktion anfordern	HTTP/1.1 Backend	HTTP/2-Backend
HTTP/2	Aktiviert	HTTP/2	Jeder Stream im Frontend ist einer dedizierten HTTP/1.1-Verbindung zugeordnet	Alle Frontend-Streams können einer einzelnen HTTP/2-Verbindung oder maximal drei HTTP/2-Verbindungen im Backend zugeordnet werden.
HTTP/2	Deaktiviert	fallen gelassen	Nicht verfügbar	Nicht verfügbar

In der folgenden Tabelle wird das WebSocket-Verbindungsverhalten beschrieben, wenn das Backend-Multiplexing aktiviert ist:

HTTP-Paketversion	WebSocket im HTTP-Profil	Aktion anfordern	HTTP/1.1 Backend	HTTP/2-Backend
HTTP/1.1	Deaktiviert	fallen gelassen	Nicht verfügbar	Nicht verfügbar
HTTP/1.1	Aktiviert	HTTP/1.1	Jede HTTP/1.1-Verbindung ist einer dedizierten HTTP/1.1-Verbindung im Backend zugeordnet	Mehrere Http/1.1-Clients können zu einer einzelnen HTTP/2-Verbindung oder zu mehreren HTTP/2-Verbindungen gemultiplext werden

HTTP-Paketversion	WebSocket im HTTP-Profil	Aktion anfordern	HTTP/1.1 Backend	HTTP/2-Backend
HTTP/2	Aktiviert	HTTP/2	Jeder Stream im Frontend ist einer dedizierten HTTP/1.1-Verbindung zugeordnet	Alle Frontend-Streams können einer einzelnen HTTP/2-Verbindung oder mehreren HTTP/2-Verbindungen im Backend zugeordnet werden
HTTP/2	Deaktiviert	fallen gelassen	Nicht verfügbar	Nicht verfügbar

Minderung von HTTP/2 DoS

May 11, 2023

Die Http/2-Denial-of-Service (DoS) -Angriffe haben keine Auswirkungen mehr auf eine NetScaler-Appliance. Wenn die Appliance mehr Frames als das maximale Limit empfängt, schließt die Appliance die Verbindung im Hintergrund.

Um Angriffe zu mildern, können Sie mithilfe des HTTP-Profils die Standardkonfiguration von Frames ändern, die in einer HTTP/2-Verbindung empfangen werden.

Die Tabelle der HTTP/2 DoS-Abschwächung zeigt die Liste der HTTP/2-DoS-Angriffe und deren Abschwächung.

Konfigurieren der Maximalgrenze für HTTP/2-Frames zur Minderung von DoS-Angriffen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpprofile <profile_name> - http2MaxEmptyFramesPerMin <positive_integer
> -http2MaxPingFramesPerMin <positive_integer> -http2MaxSettingsFramesPerMin
 <positive_integer> -http2MaxResetFramesPerMin <positive_integer>
```

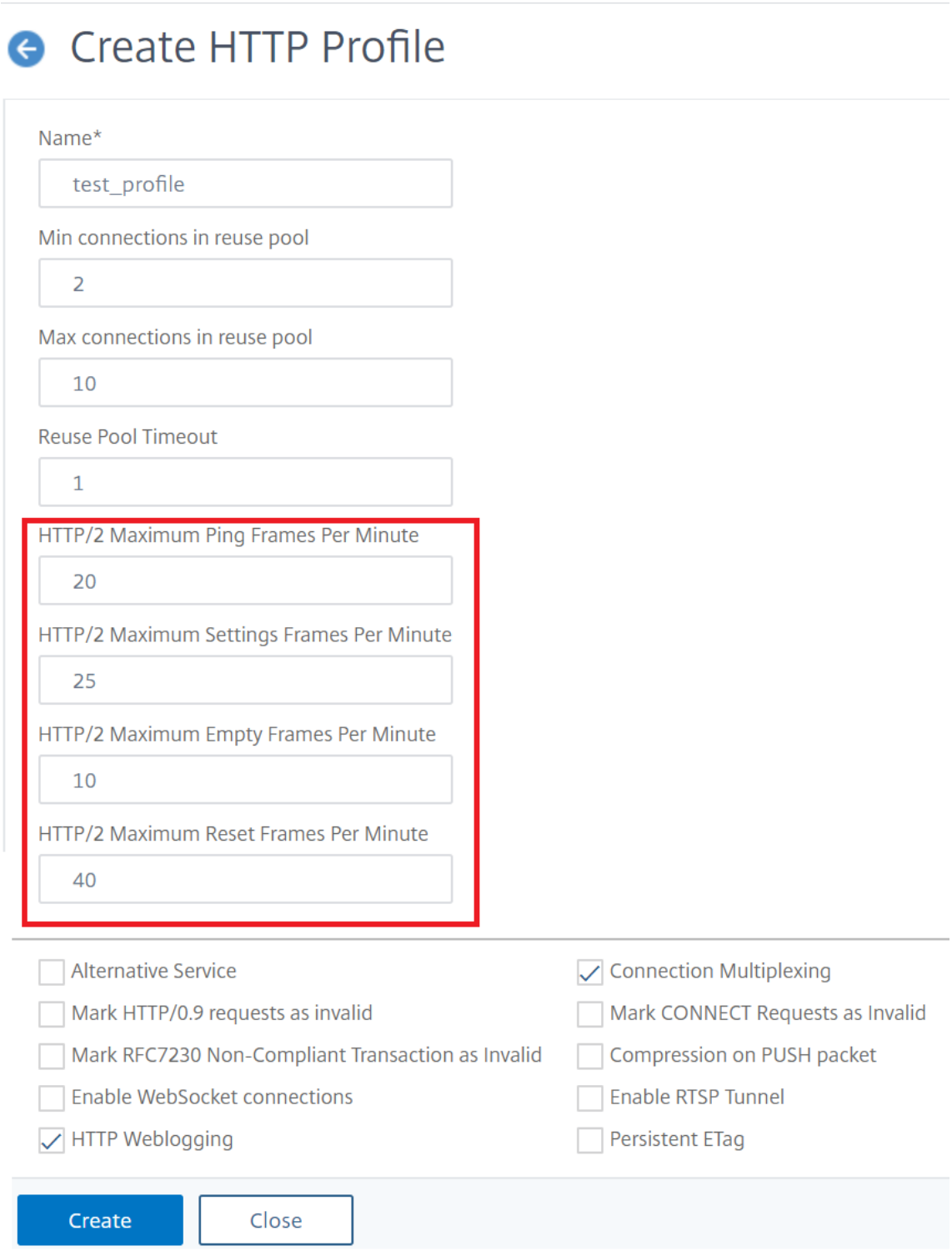
Beispiel:


```
set ns httpprofile profile1 -http2MaxEmptyFramesPerMin 20 -http2MaxPingFramesPerMin
 20 -http2MaxSettingsFramesPerMin 20 -http2MaxResetFramesPerMin 20
```

Konfigurieren Sie das maximale Limit für Frames, die in einer HTTP/2-Verbindung empfangen werden, mithilfe der NetScaler-GUI

Gehen Sie wie folgt vor, um das maximale Limit für Frames zu konfigurieren, die über eine HTTP/2-Verbindung empfangen werden:

1. Erweitern Sie im Navigationsbereich **System** und klicken Sie dann auf **Profile**.
2. Wählen Sie auf der **Profilseite** die Registerkarte **HTTP-Profile** aus.
3. Klicken Sie auf der Registerkarte **HTTP-Profile** auf **Hinzufügen**.
4. Stellen Sie auf der Seite „ **HTTP-Profil konfigurieren** “ den folgenden Parameter ein.
    a) http2MaxPingFramesPerMin. Stellen Sie die maximale Anzahl der pro Verbindung empfangenen PING-Frames in einer Minute ein. Wenn die Anzahl der PING-Frames die Konfigurationsgrenze überschreitet, verwirft die Appliance unbemerkt Pakete über die Verbindung.
    b) http2MaxSettingsFramesPerMin. Stellen Sie die maximale Anzahl von SETTINGS-Frames ein, die pro Verbindung in einer Minute empfangen werden. Wenn die Anzahl der SETTINGS-Frames die Konfigurationsgrenze überschreitet, verwirft ADC unbemerkt Pakete über die Verbindung.
    c) http2MaxResetFramesPerMin. Stellen Sie die maximale Anzahl von RESET-Frames ein, die pro Verbindung in einer Minute gesendet werden. Wenn die Anzahl der RESET-Frames die Konfigurationsgrenze überschreitet, verwirft ADC unbemerkt Pakete über die Verbindung.
    d) http2MaxEmptyFramesPerMin. Stellen Sie die maximale Anzahl leerer Frames ein, die pro Verbindung in einer Minute gesendet werden. Wenn die Anzahl der leeren Frames die Konfigurationsgrenze überschreitet, verwirft ADC unbemerkt Pakete über die Verbindung.
5. Klicken Sie auf **OK** und auf **Schließen**.



HTTP3 über QUIC-Protokoll

May 11, 2023

HTTP/2 über TCP ist der bevorzugte Standard für das Senden mehrerer Streams von HTTP-Anfragen über eine einzige Verbindung. Im TCP-Transportmechanismus gibt es jedoch gewisse Einschränkungen und Latenzprobleme beim Zugriff auf Websites und Webanwendungen. Wenn Sie mehrere Anfragen über dieselbe Verbindung multiplexieren, unterliegen sie der Zuverlässigkeit derselben Verbindung. Wenn das Paket für eine Anforderung verloren geht, verzögern sich alle anderen multiplexierten Anfragen, bis das verlorene Paket erkannt und erneut übertragen wird. Dies führt zu Verzögerungen beim Blockieren von Head-of-Line-Blockierungen und Latenzproblemen.

Für Verbindungs- und Transportverzögerungen verwendet HTTP/3 QUIC anstelle des TCP-Protokolls. Das QUIC ist ein aufkommendes Protokoll, das UDP anstelle von TCP als Basistransport verwendet. In HTTP-over-Quic können Sie mehrere unabhängige Anfragen multiplexen, ohne von einer einzigen TCP-Verbindung abhängig zu sein. QUIC implementiert eine zuverlässige Verbindung, auf der Sie mehrere HTTP-Anfragen streamen können. QUIC enthält auch TLS als integrierte Komponente und nicht als zusätzliche Layer wie in HTTP/1.1 oder HTTP/2.

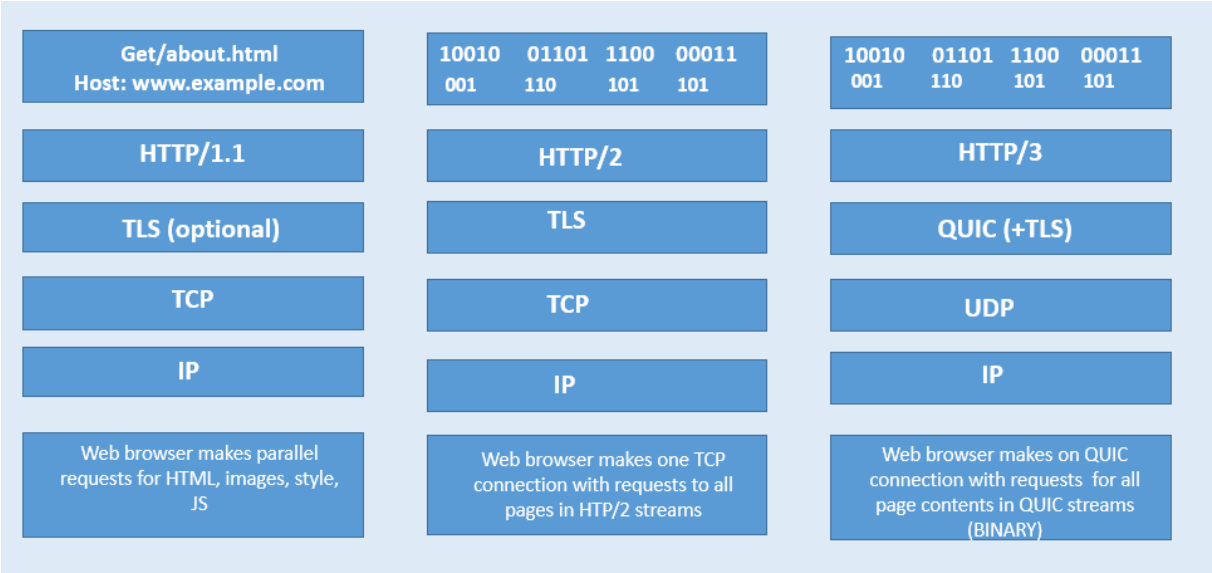
Vorteil der Verwendung des HTTP/3-Protokolls

Einige der wichtigen Vorteile der Verwendung des QUIC-Protokolls für den HTTP/3-Datentransport sind nachstehend aufgeführt:

- Stream-Multiplexen
- Strömungssteuerung auf Stream- und Verbindungsebene
- Verbindungsaufbau mit niedriger Latenz
- Verbindungsmigration und Widerstandsfähigkeit zur NAT-Wiederbindung
- Authentifizierter und verschlüsselter Header und Payload

Transportstapel in HTTP-Protokollen

Die folgende Abbildung zeigt den Transportstapel in den Protokollen HTTP/1.1, HTTP/2 und HTTP/3.



Wie QUIC- und HTTP/3-Verbindungsmanagement in NetScaler funktioniert

Die folgende Abbildung zeigt, wie QUIC- und HTTP/3-Verbindungsmanagement in einer NetScaler Appliance und wie die Komponenten miteinander interagieren.

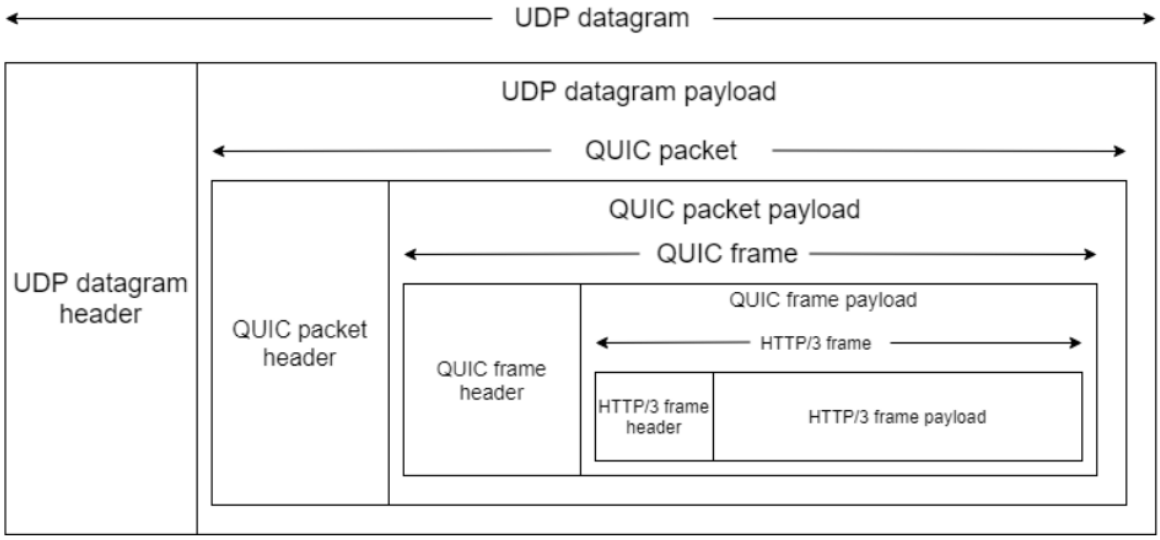
Schritt 1: Clientseitige HTTP/3-Anfrage über das QUIC-Protokoll an die NetScaler Appliance.
Schritt 2: Anforderung, die von NetScaler AS HTTP/1.1 oder HTTP/2 weitergeleitet wird, abhängig von der Unterstützung des Back-End-Servers.
Schritt 3: Antwort über HTTP/2 oder HTTP/1.1 vom Back-End-Server zu NetScaler.
Schritt 4: ADC leitet die Antwort als HTTP/3-Antwort an den Client weiter.

So funktioniert das HTTP/3-Protokoll

Wenn ein Client in HTTP/3 weiß, dass ein HTTP/3-Server an einem bestimmten Endpunkt vorhanden ist, öffnet er eine QUIC-Verbindung. Das QUIC-Protokoll bietet Multiplexing und Flusskontrolle. Innerhalb jedes Streams ist die Basiseinheit der HTTP/3-Kommunikation ein Frame. Jeder Frame-Typ di-

ent einem anderen Zweck. Zum Beispiel bilden HEADER und DATENRAHMEN die Grundlage für HTTP-Anfragen und -Antworten.

Das Multiplexen von Anfragen wird mit der QUIC-Stream-Abstraktion durchgeführt. Jedes Request-Response-Paar verbraucht einen einzelnen QUIC-Stream. Streams sind unabhängig voneinander, daher verhindert ein Stream, der blockiert ist oder einen Paketverlust erleidet, den Fortschritt in anderen Streams nicht. Server-Push ist ein in HTTP/2 eingeführter Interaktionsmodus, der es einem Server ermöglicht, einen Request-Response-Austausch an einen Client zu senden, in Erwartung, dass der Client die angegebene Anfrage stellt. Dies wird von der Netzauslastung gegen einen möglichen Latenzgewinn gehandelt. Zum Verwalten von Server-Push werden mehrere HTTP/3-Frames verwendet, wie PUSH_PROMISE, MAX_PUSH_ID und CANCEL_PUSH. Wie in HTTP/2 werden Anforderungs- und Antwortfelder zur Übertragung komprimiert. Da HPACK auf die orderweise Übertragung komprimierter Feldabschnitte angewiesen ist (eine Garantie, die nicht von QUIC bereitgestellt wird), ersetzt HTTP/3 HPACK durch QPACK. QPACK verwendet separate unidirektionale Streams, um den Status der Feldtabellen zu ändern und zu verfolgen, während codierte Feldabschnitte auf den Status der Tabelle verweisen, ohne ihn zu ändern.



HTTP/3-Konfiguration und Statistikzusammenfassung

May 11, 2023

Um ein HTTP/3-Protokoll für das Senden mehrerer HTTP/3-Datenströme mit QUIC zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie SSL- und Load Balancing-Funktionen.

2. Fügen Sie Lastenausgleich und Content Switching (optional) virtuelle Server vom Typ HTTP_QUIC hinzu.
3. Verknüpfen Sie QUIC-Protokollparameter mit dem virtuellen HTTP_QUIC-Server.
4. Aktivieren Sie HTTP/3 auf dem virtuellen HTTP_QUIC-Server.
5. Binden Sie ein SSL-Zertifikatschlüsselpaar mit dem virtuellen HTTP_QUIC-Server.
6. Verknüpfen Sie SSL/TLS-Protokollparameter mit dem virtuellen HTTP_QUIC-Server.

SSL und Load Balancing aktivieren

Bevor Sie beginnen, stellen Sie sicher, dass die SSL- und Load Balancing-Funktionen auf der Appliance aktiviert sind. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature ssl lb
<!--NeedCopy-->
```

Fügen Sie Lastenausgleich und Content Switching (optional) virtuelle Server vom Typ HTTP_QUIC für den HTTP/3-Dienst hinzu

Sie fügen einen virtuellen Lastausgleichsserver hinzu, um HTTP/3-Datenverkehr über QUIC zu akzeptieren.
Hinweis: Der virtuelle Lastausgleichsserver vom Typ HTTP_QUIC verfügt über integrierte QUIC-, SSL- und HTTP3-Profile. Wenn Sie es vorziehen, benutzerdefinierte Profile zu erstellen, können Sie neue Profile hinzufügen und an den virtuellen Lastenausgleichsserver binden.

```
add lb vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
    port>

add cs vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
    port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver lb-http3 HTTP_QUIC 1.1.1.1 443
add cs vserver cs-http3 HTTP_QUIC 10.10.10.10 443
```

Verknüpfen Sie QUIC-Protokollparameter mit dem virtuellen HTTP_QUIC-Server

Sie können ein QUIC-Profil erstellen und QUIC-Parameter für den QUIC-Dienst angeben und es dem virtuellen Lastenausgleichsserver zuordnen. Sie müssen entweder ein benutzerdefiniertes Profil erstellen oder das integrierte QUIC-Profil verwenden und das Profil an den virtuellen Load Balancing-Server binden.

Schritt 1: Konfigurieren Sie ein benutzerdefiniertes QUIC-Profil
an der Eingabeaufforderung:

```
set quic profile <profile_name> -transport_param <value>
<!--NeedCopy-->
```

Beispiel:

```
set quic profile quic_http3 -ackDelayExponent 10 -activeConnectionIDlimit 4
```

Die verschiedenen QUIC-Transportparameter lauten wie folgt:

-ackDelayExponent. Ein ganzzahliger Wert, der vom NetScaler an den Remote-QUIC-Endpunkt gemeldet wird und einen Exponenten angibt, den der Remote-QUIC-Endpunkt verwenden sollte, um das Feld ACK Delay in den vom NetScaler gesendeten QUIC-ACK-Frames zu dekodieren.

-activeConnectionIDlimit. Ein ganzzahliger Wert, der vom NetScaler dem Remote-QUIC-Endpunkt mitgeteilt wird. Es gibt die maximale Anzahl von QUIC-Verbindungs-IDs vom Remote-QUIC-Endpunkt an, die der NetScaler zu speichern bereit ist.

-activeConnectionMigration. Geben Sie an, ob der NetScaler dem Remote-QUIC-Endpunkt die Durchführung einer aktiven QUIC-Verbindungsmigration ermöglichen muss.

-congestionCtrlAlgorithm. Geben Sie den Algorithmus zur Überlastungssteuerung an, der für QUIC-Verbindungen verwendet werden soll.

-initialMaxData. Ein ganzzahliger Wert, der vom NetScaler an den Remote-QUIC-Endpunkt angekündigt wird und den Anfangswert in Byte für die maximale Datenmenge angibt, die über eine QUIC-Verbindung gesendet werden kann.

-initialMaxStreamDataBidiLocal. Ein ganzzahliger Wert, der vom NetScaler an den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche Flusssteuerungsgrenze in Byte für bidirektionale QUIC-Streams angibt, die vom NetScaler initiiert wurden.

-initialMaxStreamDataBidiRemote. Ein ganzzahliger Wert, der vom NetScaler für den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche Flusssteuerungsgrenze in Byte für bidirektionale QUIC-Streams angibt, die vom Remote-QUIC-Endpunkt initiiert werden.

-initialMaxStreamDataUni. Ein ganzzahliger Wert, der vom NetScaler an den Remote-QUIC-Endpunkt angegeben wird und die anfängliche Flusssteuerungsgrenze in Byte für unidirektionale Streams angibt, die vom Remote-QUIC-Endpunkt initiiert werden.

-initialMaxStreamsBidi. Ein ganzzahliger Wert, der vom NetScaler an den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche maximale Anzahl von bidirektionalen Streams angibt, die der Remote-QUIC-Endpunkt initiieren muss.

-initialMaxStreamsUni. Ein ganzzahliger Wert, der vom NetScaler an den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche maximale Anzahl von unidirektionalen Streams angibt, die der Remote-QUIC-Endpunkt initiieren muss.

-maxAckDelay. Ein ganzzahliger Wert, der vom NetScaler für den Remote-QUIC-Endpunkt angekündigt wird und die maximale Zeitspanne in Millisekunden angibt, um die der NetScaler das Senden von Bestätigungen verzögert.

-maxIdleTimeout. Ein ganzzahliger Wert, der vom NetScaler an den Remote-QUIC-Endpunkt ausgegeben wird und das maximale Leerlauf-Timeout für eine QUIC-Verbindung in Sekunden angibt. Eine QUIC-Verbindung, die länger inaktiv bleibt als das Minimum der vom NetScaler und dem Remote-QUIC-Endpunkt angegebenen Leerlauf-Timeout-Werte und das Dreifache des aktuellen Probe Timeout (PTO), wird vom NetScaler stillschweigend verworfen.

-maxUDPPayloadSize. Ein ganzzahliger Wert, der vom NetScaler für den Remote-QUIC-Endpunkt angekündigt wird und die Größe der größten UDP-Datagramm-Nutzlast in Byte angibt, die der NetScaler bereit ist, bei einer QUIC-Verbindung zu empfangen.

-newTokenValidityPeriod. Ein ganzzahliger Wert, der den Gültigkeitszeitraum der vom NetScaler gesendeten QUIC NEW_TOKEN-Frames in Sekunden angibt.

-retryTokenValidityPeriod. Ein ganzzahliger Wert, der die Gültigkeitsdauer von Adressvalidierungstoken in Sekunden angibt, die über vom NetScaler gesendete QUIC-Retry-Pakete ausgegeben wurden.

-statelessAddressValidation. Geben Sie an, ob der NetScaler eine zustandslose Adressvalidierung für QUIC-Clients durchführen muss, indem er Token in QUIC-Wiederholungspaketen während des Aufbaus der QUIC-Verbindung sendet und Token in QUIC NEW_TOKEN-Frames nach dem Aufbau der QUIC-Verbindung sendet.

Schritt 2: Ordnen Sie das benutzerdefinierte QUIC-Profil einem virtuellen Lastausgleichsserver vom Typ http_quic zu

Geben Sie in der Befehlszeile Folgendes ein:

```
1 set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
     serviceName>@] [-persistenceType <persistenceType>] [-
     quicProfileName <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
set lb vserver lb-http3 -quicProfileName quic_http3
```

Aktivieren und binden Sie HTTP/3 auf einem virtuellen HTTP_QUIC Server

Um HTTP/3 auf einem virtuellen HTTP_QUIC-Server zu aktivieren, wird der HTTP-Profilkonfiguration eine Reihe von Konfigurationsparametern hinzugefügt. Um die Konfiguration zu erleichtern, ist beim Hinzufügen eines virtuellen HTTP_QUIC-Servers ein neues Standard/integriertes HTTP-Profil auf der Appliance verfügbar. Für das Profil sind die Unterstützungsparameter des HTTP/3-Protokolls auf ENABLED festgelegt und auch an die virtuellen HTTP_QUIC-Server begrenzt (anwendbar, wenn Sie den

virtuellen HTTP_QUIC-Server nicht mit einem vom Benutzer hinzugefügten HTTP-Profil verknüpfen möchten). Der Wert der HTTP/3-Parameter im HTTP-Profil entscheidet, ob das HTTP/3-Protokoll ausgewählt und bei der Verarbeitung der Erweiterung TLS ALPN (Application Layer Protocol Negotiation) während des QUIC-Protokoll-Handshake angekündigt werden soll.

Sie können ein HTTP/3-Profil erstellen und HTTP-Parameter für den HTTP/3-Dienst und den virtuellen Lastausgleichsserver angeben. Sie müssen entweder ein benutzerdefiniertes Profil erstellen oder das integrierte HTTP/3-Profil verwenden und das Profil an den virtuellen Lastenausgleichsserver binden.

Schritt 1: Konfigurieren Sie ein benutzerdefiniertes HTTP/3-Profil
an der Eingabeaufforderung:

```
Add ns httpProfile <profile_name> -http3 ENABLED
<!--NeedCopy-->
```

Beispiel:

```
add ns httpProfile http3_quic -http3 ENABLED
```

Schritt 2: Binden Sie das benutzerdefinierte HTTP/3-Profil an einen virtuellen Lastausgleichsserver vom Typ http_quic Geben Sie
an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
    serviceName>@] [-persistenceType <persistenceType>] [-
    httpProfileName <string>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver lb-http3 -httpProfileName http3_quic
```

Binden Sie SSL-Zertifikatschlüsselpaar mit dem virtuellen HTTP_QUIC Server

Um verschlüsselten Datenverkehr zu verarbeiten, müssen Sie ein SSL-Zertifikatschlüsselpaar hinzufügen und es an den virtuellen HTTP_QUIC-Server binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>

<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver lb-http3 -certkeyName rsa_certkeypair
```

Weitere Informationen finden Sie unter Thema Bind SSL-Zertifikat .

Binden Sie SSL/TLS-Protokollparameter mit einem virtuellen HTTP_QUIC-Server

Virtuelle Server vom Typ HTTP_QUIC verfügen über eine integrierte TLS 1.3-Serverfunktionalität, da das QUIC-Protokoll TLS 1.3 als obligatorische Sicherheitskomponente verwendet. Um die Konfiguration beim Hinzufügen eines virtuellen HTTP_QUIC-Servers zu erleichtern, wird ein neues Standard- oder integriertes SSL-Profil vom Typ QUIC-FrontEnd hinzugefügt. Das SSL-Profil hat TLS 1.3-Version aktiviert, die mit TLS 1.3-Chiffrier-Suiten (und elliptischen Kurven) konfiguriert ist. Das SSL-Profil muss dann an die neu hinzugefügten virtuellen HTTP_QUIC-Server gebunden sein.
Sie können ein SSL-Profil erstellen und SSL-Verschlüsselungsparameter für den TLP 1.1-Dienst und den virtuellen Lastausgleichsserver angeben. Sie müssen entweder ein benutzerdefiniertes Profil erstellen oder das integrierte SSL-Profil verwenden und das Profil an den virtuellen Lastenausgleichsserver binden.

Schritt 1: Konfigurieren Sie ein benutzerdefiniertes SSL-Profil
an der Eingabeaufforderung:

```
add ssl profile <name> -sslprofileType QUIC-FrontEnd
<!--NeedCopy-->
```

Beispiel:

```
add ssl profile ssl_profile1 -sslprofileType QUIC-FrontEnd -tls13 ENABLED -
tls12 DISABLED -tls11 DISABLED -tls1 DISABLED
```

Schritt 2: Binden Sie das benutzerdefinierte SSL-Profil an einen virtuellen Lastausgleichsserver vom Typ HTTP_QUIC Geben Sie
an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <name>@ [-sslProfile <string>]
<!--NeedCopy-->
```

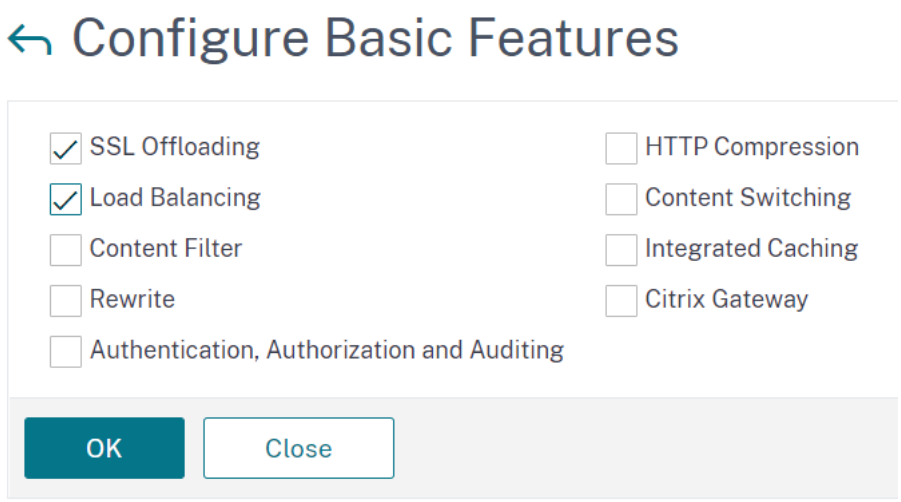
Beispiel:

```
set ssl vserver lb-http3 -sslprofile ssl_profile1
```

Aktivieren Sie SSL- und Load Balancing-Funktionen über die grafische Benutzeroberfläche

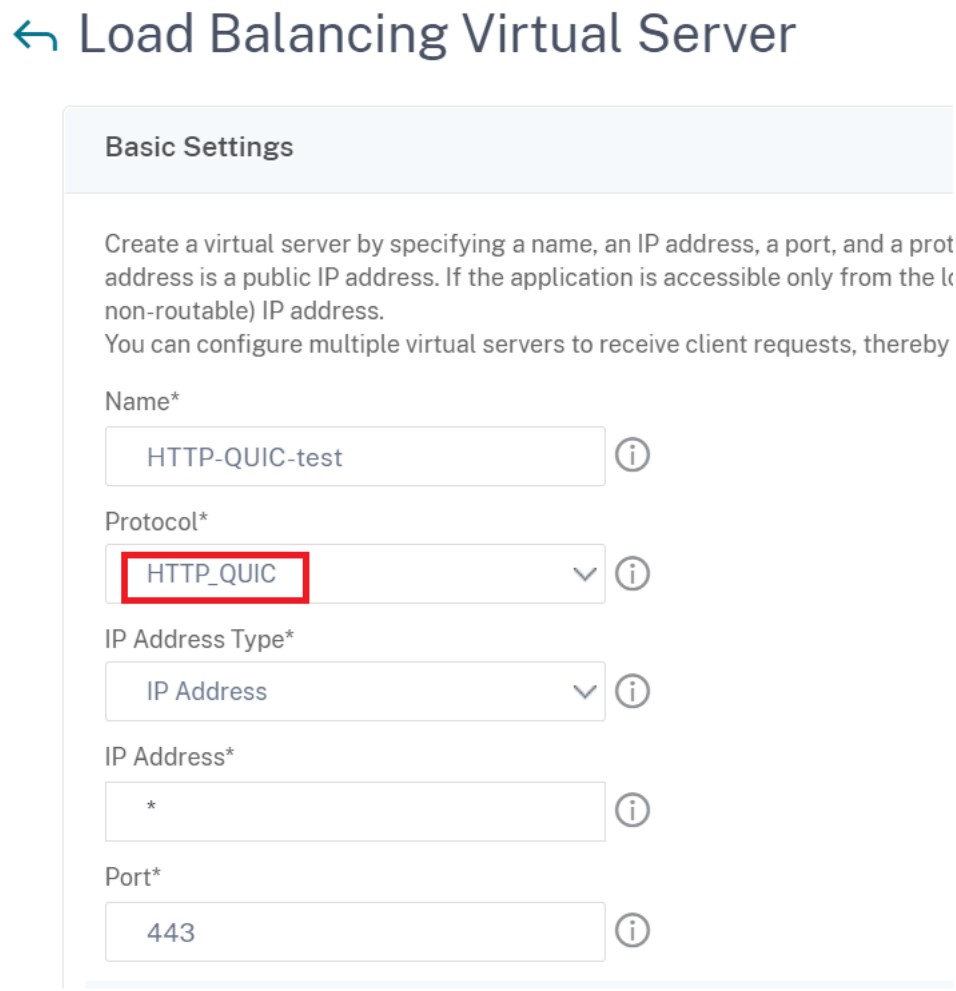
Führen Sie die folgenden Schritte aus, um SSL- und Load Balancing-Funktionen zu aktivieren:

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Wählen Sie auf der Seite **Basisfunktionen konfigurieren** den **SSL** und den **Load Balancing**aus.
3. Klicken Sie auf **OK**und dann auf **Schließen**.



Fügen Sie Lastenausgleich und Content Switching (optional) virtuelle Server vom Typ HTTP_QUIC mit der GUI hinzu

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastenausgleichsserver vom Typ HTTP_QUIC zu erstellen.
3. Klicken Sie auf der Seite **Virtueller Server für Lastenausgleich** auf **Profile**.
4. Wählen Sie im Abschnitt **Profile** den Profiltyp als QUIC aus. Hinweis: QUIC-, HTTP/3- und SSL-Profile sind integrierte Profile.
5. Klicke auf **OK** und dann auf **Fertig**.

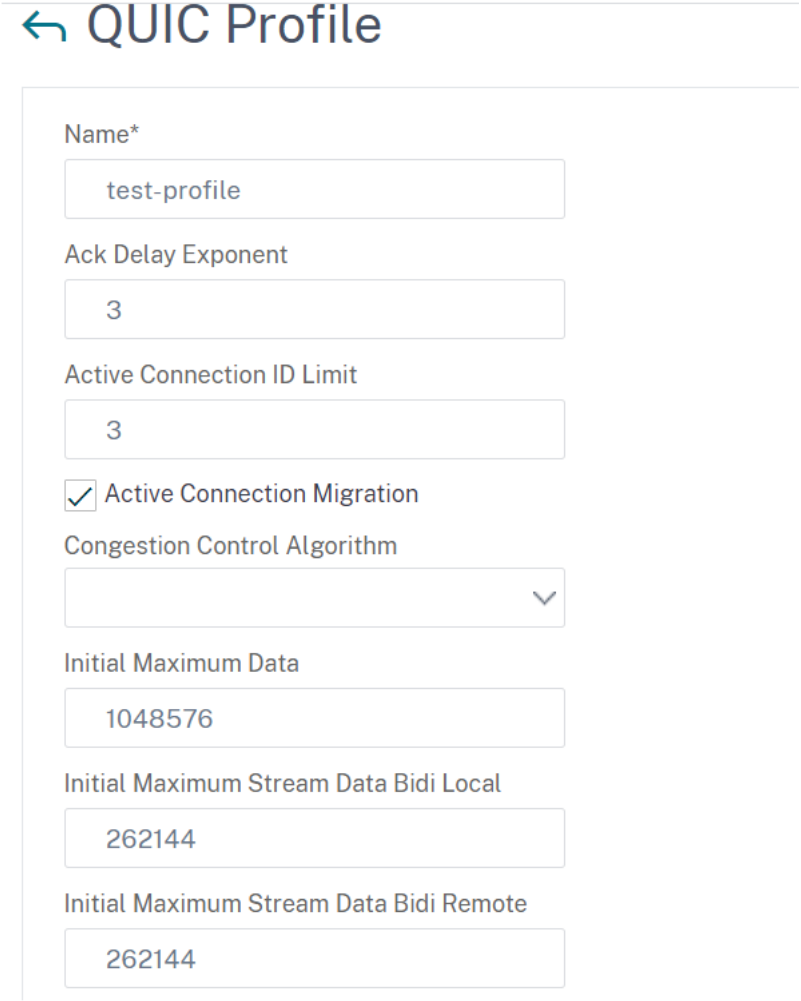


Verknüpfen Sie QUIC-Protokollparameter mit dem virtuellen HTTP_QUIC-Server über die grafische Benutzeroberfläche

Schritt 1: QUIC-Profil hinzufügen

1. Navigieren Sie zu **System > Profile > QUIC-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Legen Sie auf der Seite QUIC-Profil die folgenden Parameter fest. Eine ausführliche Beschreibung der einzelnen Parameter finden Sie im Abschnitt “Assoziiertes QUIC-Protokoll CLI”.
   a) `Ack Delay` Exponent
   b) Limit der aktiven Verbindungs-ID
   c) Aktive Verbindungsmigration
   d) Algorithmus zur Überlastungssteuerung
   e) Anfängliche maximale Daten

f) Anfängliche maximale Stream-Daten Bidi Local
g) Anfängliche maximale Stream-Daten Bidi Remote
h) Anfängliche maximale Stream-Dateneinheit
i) Initialer maximaler Stream-Bidi
j) Initialer maximaler Stream-Uni
k) Maximale Verzögerung bei der Bestätigung
l) Maximaler Leerlauf-Timeout
m) Maximale UDP-Daten GramsperBurst
n) Gültigkeitszeitraum des neuen Tokens
o) Gültigkeitszeitraum des Tokens wiederholen
p) Stateless Adressvalidierung

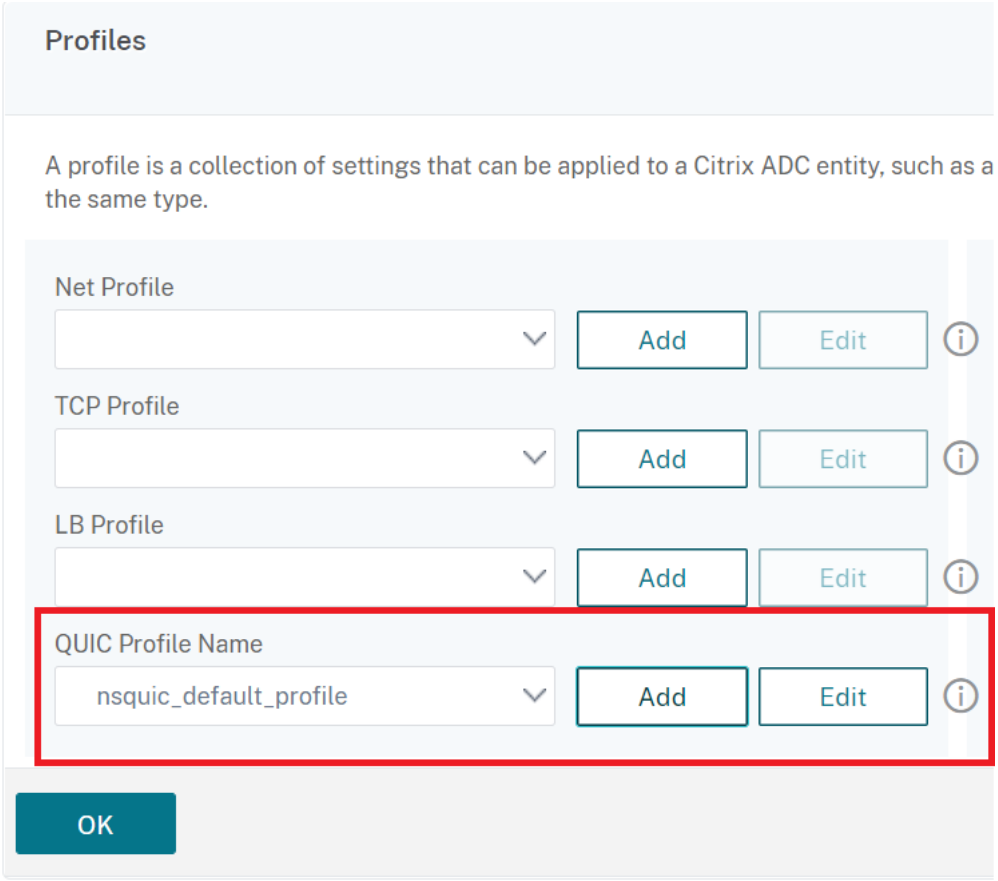


Schritt 2: Verknüpfen Sie QUIC-Profil mit einem virtuellen Lastenausgleichsserver vom Typ HTTP_QUIC

1. Wählen Sie im Abschnitt **Profile** das QUIC-Profil aus. Hinweis: QUIC-, HTTP/3- und SSL-Profile

sind integrierte Profile.

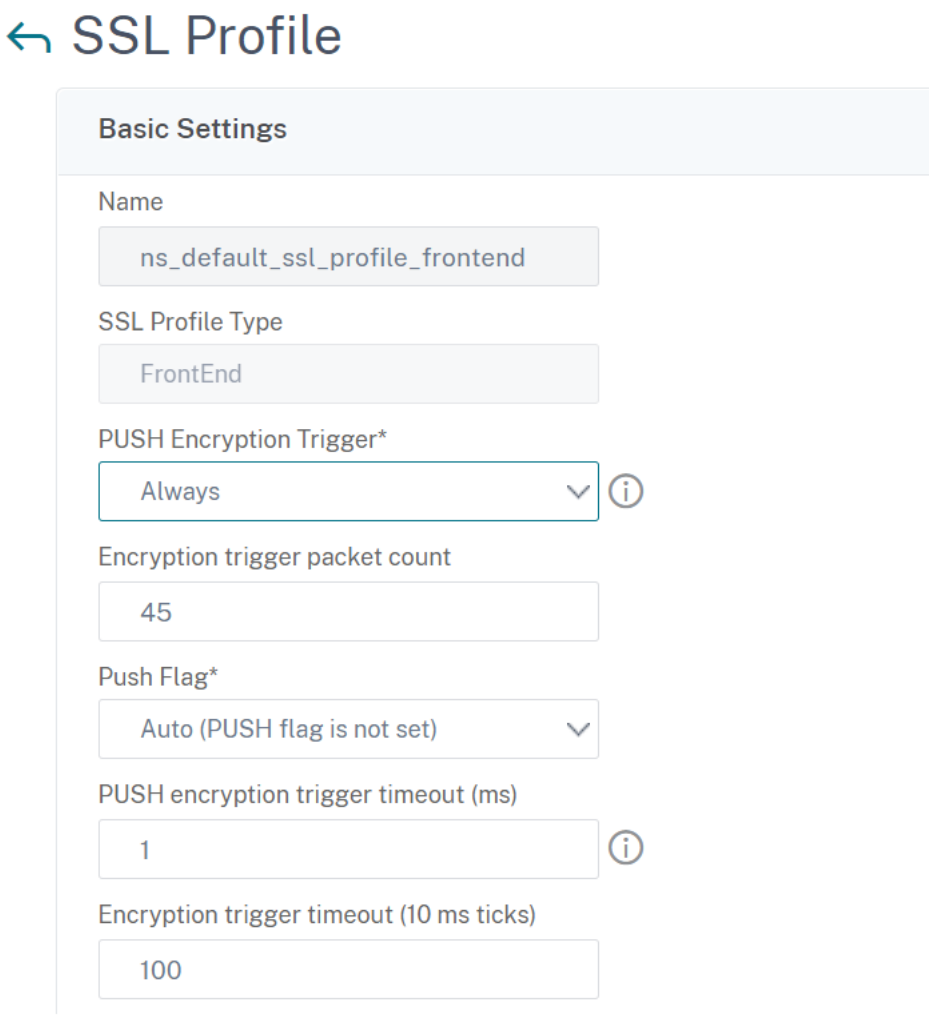
2. Klicke auf **OK** und dann auf **Fertig**.



Verknüpfen Sie SSL/TLS-Protokollparameter mit dem virtuellen Server vom Typ SSL über die grafische Benutzeroberfläche

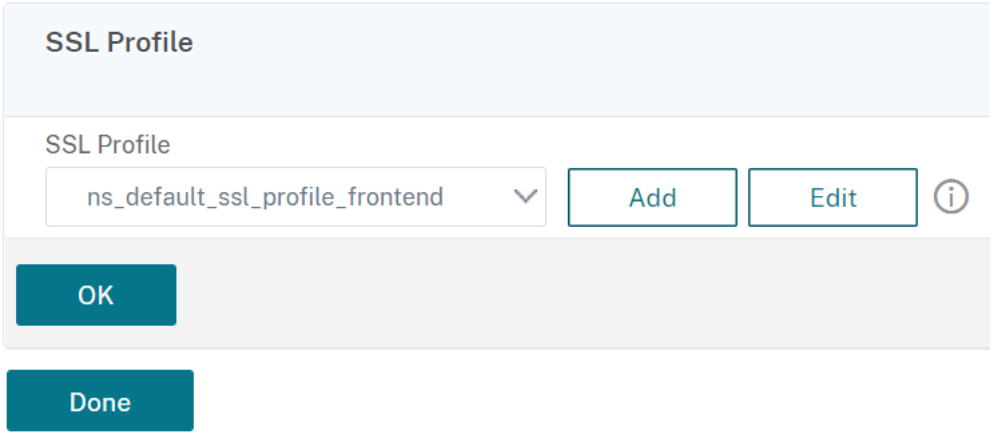
Schritt 1: SSL-Profil hinzufügen

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Legen Sie auf der Seite **QUIC-Profil** die SSL-Parameter fest. Eine ausführliche Beschreibung finden Sie unter Thema zur SSL-Profilkonfiguration.
4. Klicken Sie auf **OK** und auf **Schließen**.



Schritt 2: Verknüpfen Sie das SSL-Profil mit einem virtuellen Lastenausgleichsserver vom Typ SSL.

1. Wählen Sie im Abschnitt **Profile** das SSL-Profil aus.
2. Klicke auf **OK** und dann auf **Fertig**.



Quic- und HTTP/3-Statistiken anzeigen

Die folgenden Befehle zeigen eine detaillierte Zusammenfassung der QUIC- und HTTP3-Statistiken. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 > stat quic
2 > stat quic  - detail
3 <!--NeedCopy-->
```

Um die Statistikanzeige zu löschen, geben Sie eine der folgenden Optionen ein:

```
1 > stat quic -clearstats basic
2 > stat quic -clearstats full
3
4 <!--NeedCopy-->
```

So zeigen Sie eine detaillierte Zusammenfassung der HTTP/3-Statistiken an:

```
1 > stat http3
2 > stat http3  - detail
3 <!--NeedCopy-->
```

Um die Statistikanzeige zu löschen, geben Sie eine der folgenden Optionen ein:

```
1 > stat http3 -clearstats basic
2 > stat http3 -clearstats full
3 <!--NeedCopy-->
```

Richtlinienkonfiguration für HTTP/3-Datenverkehr

May 11, 2023

HTTP/3 verwendet den QUIC-Transport, der auf UDP basiert. Wenn Sie einen Richtlinienausdruck für den virtuellen HTTP- oder SSL-Server definiert hatten, der TCP-Richtlinienausdrücke enthält, kann er nicht mehr mit einem virtuellen HTTP_QUIC-Server verwendet werden. Alle anderen Richtlinien, die keinen TCP- oder klassischen Ausdrücke haben, können an einen virtuellen HTTP_QUIC-Server gebunden werden. Damit die Richtlinien wirksam werden, müssen Sie sicherstellen, dass die Feature-Richtlinien gemäß den folgenden, an die neu hinzugefügten globalen Bindepunkte gebunden sind.

- HTTPQUIC_REQ_DEFAULT
- HTTPQUIC_REQ_OVERRIDE
- HTTPQUIC_RES_DEFAULT

- HTTPQUIC_RES_OVERRIDE

Oder die Richtlinien können an bestimmte Bindepunkte für virtuelle Server gebunden werden:

- REQUEST
- RESPONSE

Weitere Informationen finden Sie unter Thema Binden von Richtlinien mit erweiterter Richtlinieninfrastruktur .

Im Folgenden finden Sie die Richtlinien, die für die HTTP over QUIC-Konfiguration unterstützt werden:

- Responder
- Rewrite
- HTTP-Komprimierung
- Integriertes Caching
- Firewall für Webanwendungen
- URL-Transformation
- SSL
- Frontend-Optimierung (FEO)
- AppQoE

Konfiguration der Responder-Richtlinie für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC haben Unterstützung für Responder Policy. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.

Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC globale Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Responder Action zum Umleiten von URLs hinzufügen

Um eine Responder Action hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder action <name> <type> (<target> | <htmlpage>) [-comment <
     string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
     expression>] [-headers <name(value)> ...]
2 <!--NeedCopy-->
```

Beispiel:

```
add responder action redirectURL redirect "\"https://www.citrix.com/\""
```


Responder-Richtlinie hinzufügen

Um eine Responder Policy hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
     string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add responder policy res-pol "CLIENT.IP.SRC.IN_SUBNET(10.10.10.10/32)"
redirectURL
```

Hinzufügen von Responder-Richtlinienbasierten UDP-Ausdruck

Um einen auf der Responder Policy basierten UDP-Ausdruck hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
     string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add responder policy redirectCitrixUdp "CLIENT.UDP.DSTPORT.EQ(443)"redirectURL
```

Binden Responder Policy richtlinienbasierten UDP-Ausdruck mit einem HTTP/3 QUIC-basierten Lastausgleichsserver

Um einen auf Responder Policy basierenden UDP-Ausdruck an einen virtuellen Lastausgleichsserver zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
      ) | <serviceGroupName>@ |         (-policyName <string>@  [-
     priority <positive_integer>]  [-gotoPriorityExpression <expression>]
       [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
     analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 9 -gotoPriorityExpres
 END -type REQUEST
```


Binden Sie die Responder Policy mit einem HTTP/3 QUIC-basierten Lastenausgleichsserver

Um eine Responder Policy an einen virtuellen Lastausgleichsserver zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 10 -
gotoPriorityExpression END -type REQUEST
```

Binden Sie die Responder Policy an den globalen HTTP/3-Bindepunkt

Um eine Responder Policy an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind responder global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ] bind
    responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```

Beispiel:

```
bind responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
```

> **Hinweis:**
>
> Weitere Informationen finden Sie unter Dokumentation zu Responder-Richtlinien.

Rewriterichtlinienkonfiguration für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC verfügen über Rewriterichtlinienunterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.

Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Im Folgenden sind die Konfigurationsschritte zum Konfigurieren der Rewriterichtlinie für HTTP3 über QUIC aufgeführt.

Neuschreibaktion für HTTP over QUIC hinzufügen

Um eine Rewrite-Aktion hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
    search <expression>] [-refineSearch <expression>] [-comment <string
    >]
2 <!--NeedCopy-->
```

Beispiel:

```
add rewrite action http3-altsvc-action insert_http_header Alt-Svc q/"h3
-29=\":443\"; ma=3600; persist=1"/
```

Rewriterichtlinie für HTTP over QUIC hinzufügen

Um eine Schreibaktion hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add rewrite policy <name> <rule> <action> [<undefAction>] [-comment  <
    string>] [-logAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add rewrite policy http3-altsvc-policy true http3-altsvc-action
```

Binden Sie die Rewriterichtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die Rewriterichtlinie an den virtuellen Load Balancing-Server zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )
     | <serviceGroupName>@ | (-policyName <string>@ [-priority <
    positive_integer>] [-gotoPriorityExpression <expression>] [-type <
    type>] [-invoke (<labelType> <labelName>) ] ) | -analyticsProfile  <
    string>@)
2 <!--NeedCopy-->
```

Beispiel:


```
bind lb vserver lb-http3 -policyName http3-altsvc-policy -priority 10 -type
 RESPONSE
```

Rewriterichtlinie an den globalen HTTP/3-Bindepunkt binden

```
1 To bind a responder policy with HTTP/3 global bind point, at the
     command prompt, type:
2 bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
      [-type <type>] [-invoke (<labelType> <labelName>)]
3 <!--NeedCopy-->
```

Beispiel:

```
bind rewrite global http3-altsvc-policy 3 -type HTTPQUIC_RES_DEFAULT
```

> **Hinweis:**
>
> Weitere Informationen finden Sie unter Rewrite der Richtlinien - Dokumentation.

Konfiguration der Komprimierungsrichtlinie für HTTP/3-Datenverkehr

Wenn NetScaler eine HTTP-Antwort von einem Server empfängt, werden die integrierten Komprimierungsrichtlinien und alle benutzerdefinierten Komprimierungsrichtlinien ausgewertet, um zu bestimmen, ob die Antwort komprimiert werden soll, und falls ja, der anzuwendende Komprimierungstyp. Die den Richtlinien zugewiesenen Prioritäten bestimmen die Reihenfolge, in der die Richtlinien mit den Anforderungen abgeglichen werden.
Virtuelle Server vom Typ HTTP über QUIC haben Unterstützung für Komprimierungsrichtlinien. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Komprimierungsrichtlinie hinzufügen

Um eine Komprimierungsrichtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cmp policy <name> -rule <expression> -resAction <string>
2 <!--NeedCopy-->
```

Beispiel:


```
add cmp policy udp_port_cmp_policy -rule "CLIENT.UDP.DSTPORT.EQ(443)"-
resAction COMPRESS
```

Binden Sie die Komprimierungsrichtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die URL-Transformationsrichtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
      ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
      positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
       REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
      -analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName udp_port_cmp_policy -priority 10 -type
 RESPONSE
```

Binden Sie die Komprimierung global an den globalen HTTP/3-Bindepunkt

Um eine Komprimierungsrichtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind compression global <policyName> <priority>  [<
      gotoPriorityExpression>] [-type <type>] [-invoke (<labelType>  <
      labelName>) ] bind responder global redirectCitrixUdp 3 -type
      HTTPQUIC_REQ_DEFAULT
2 <!--NeedCopy-->
```

Beispiel:

```
bind cmp global udp_port_cmp_policy -priority 100 -type HTTPQUIC_RES_DEFAULT
 Global built-in compression policies
```

Nachdem Sie Ihre Appliance auf NetScaler Release 13.0 Build 82.x aktualisiert haben, werden die folgenden Komprimierungsrichtlinien automatisch an den Standardbindepunkt HTTP/3 gebunden.

```
1 > sho cmp global -type HTTPQUIC_RES_DEFAULT
2         Policy Name: ns_adv_nocmp_xml_ie
3         Priority: 8700
4         GotoPriorityExpression: END
5         Type: HTTPQUIC_RES_DEFAULT
```



```
6
7           Policy Name: ns_adv_nocmp_mozilla_47
8           Priority: 8800
9           GotoPriorityExpression: END
10          Type: HTTPQUIC_RES_DEFAULT
11
12          Policy Name: ns_adv_cmp_mscss
13          Priority: 8900
14          GotoPriorityExpression: END
15          Type: HTTPQUIC_RES_DEFAULT
16
17          Policy Name: ns_adv_cmp_msapp
18          Priority: 9000
19          GotoPriorityExpression: END
20          Type: HTTPQUIC_RES_DEFAULT
21
22          Policy Name: ns_adv_cmp_content_type
23          Priority: 10000
24          GotoPriorityExpression: END
25          Type: HTTPQUIC_RES_DEFAULT
26  <!--NeedCopy-->
```

Wenn nicht gebunden, können die folgenden Befehle über die Eingabeaufforderung konfiguriert werden und Sie können auf Ihrer Appliance konfigurieren.

```
bind cmp global ns_adv_nocmp_xml_ie -priority 8700 -gotoPriorityExpression
END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_nocmp_mozilla_47 -priority 8800 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_mscss -priority 8900 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_msapp -priority 9000 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_content_type -priority 10000 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT
```

Weitere Informationen finden Sie unter Konfiguration von Komprimierungsrichtlinien.

Caching-Richtlinienkonfiguration für HTTP/3-Datenverkehr

Der integrierte Cache bietet In-Memory-Speicher auf der NetScaler-Appliance und stellt Webinhalte für Benutzer bereit, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist. Für statis-

che Inhalte erfordert der integrierte Cache wenig Ersteinrichtung. Nachdem Sie die integrierte Cache-Funktion aktiviert und eine grundlegende Einrichtung durchgeführt haben (z. B. die Menge an NetScaler-Appliance-Speicher bestimmt haben, die der Cache verwenden darf), verwendet der integrierte Cache integrierte Richtlinien, um bestimmte Arten von statischem Inhalt zu speichern und bereitzustellen, einschließlich einfacher Webseiten und Bilddateien. Sie können den integrierten Cache auch so konfigurieren, dass dynamische Inhalte gespeichert und bereitgestellt werden, die von Web- und Anwendungsservern als nicht zwischenspeicherbar gekennzeichnet sind (z. B. Datenbankdatensätze und Aktienkurse).
Virtuelle Server vom Typ HTTP über QUIC haben Cache-Policy-Unterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.

Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Cache-Inhaltsgruppe hinzufügen

Um die Cache-Inhaltsgruppe hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <
    secs> | -relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -
    absExpiryGMT <HH:MM> ...] [-heurExpiryParam <positive_integer>] [-
    weakNegRelExpiry <secs>] [-maxResSize <KBytes>] [-memLimit <MBytes>]
    ...
2 <!--NeedCopy-->
```

Beispiel:

```
add cache contentGroup DEFAULT -maxResSize 500
```

Cache-Richtlinie hinzufügen

Um Cache-Richtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cache policy <policyName> -rule <expression> -action <action>  [-
    storeInGroup <string>] [-invalGroups <string> ...] [-invalObjects <
    string> ...] [-undefAction ( NOCACHE | RESET )] add cache policy <
    name> <rule> <profileName> [-comment <string>]  [-logAction <string
    >]
2 <!--NeedCopy-->
```


Beispiel:

```
add cache policy ctx_doc_pdf -rule "HTTP.REQ.URL.ENDSWITH(\".pdf\")"-action
 CACHE -storeInGroup DEFAULT
```

Binden Sie die Cache-Richtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die Cache-Richtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
     ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
     positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
      REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
     -analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName ctx_doc_pdf -priority 100 -type
REQUEST
```

Binden Sie die Cacherichtlinie global an den globalen HTTP/3-Bindepunkt

So binden Sie eine Cache-Richtlinie für den globalen HTTP/3-Bindepunkt:

```
1 bind cache global <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
2 <!--NeedCopy-->
```

Beispiel:

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Weitere Informationen finden Sie unter Integrierte Cache-Richtlinienkonfiguration.

Global integrierte Cache-Richtlinien

Nach dem Upgrade Ihrer Appliance auf NetScaler Release 13.0 Build 82.x werden die folgenden Cacherichtlinien automatisch an den HTTP/3-Standardbindepunkt gebunden.

Bei einem Upgrade auf das Release 13.0 82.x werden die folgenden Cacherichtlinien automatisch an den Standardbindepunkt HTTP/3 gebunden.


```
> sho cache global -type HTTPQUIC_REQ_DEFAULT
1)      Policy Name: NOPOLICY
        Priority: 185883
        GotoPriorityExpression: USE_INVOCATION_RESULT
        Invoke type: policylabel        Invoke name:
            _httpquicReqBuiltinDefaults
        Global bindpoint: HTTPQUIC_REQ_DEFAULT

 Done
> sho cache global -type HTTPQUIC_RES_DEFAULT
1)      Policy Name: NOPOLICY
        Priority: 185883
        GotoPriorityExpression: USE_INVOCATION_RESULT
        Invoke type: policylabel        Invoke name:
            _httpquicResBuiltinDefaults
        Global bindpoint: HTTPQUIC_RES_DEFAULT

<!--NeedCopy-->
```

Wenn die Richtlinien nach einem Upgrade nicht gebunden sind, können Sie die folgenden Befehle verwenden, um die Konfiguration manuell zu binden und zu speichern.

```
add cache policylabel _httpquicReqBuiltinDefaults -evaluates
    HTTPQUIC_REQ

add cache policylabel _httpquicResBuiltinDefaults -evaluates
    HTTPQUIC_RES

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _nonGetReq -priority 100

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _advancedConditionalReq -priority 200

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _personalizedReq -priority 300

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableStatusRes -priority 100

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableVaryRes -priority 200

bind cache policylabel _httpquicResBuiltinDefaults -policyName
```



```
    _uncacheableCacheControlRes -priority 300
16
17 bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _cacheableCacheControlRes -priority 400
18
19 bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheablePragmaRes -priority 500
20
21 bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _cacheableExpiryRes -priority 600
22
23 bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _imageRes -priority 700
24
25 bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _personalizedRes -priority 800
26
27 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
    USE_INVOCATION_RESULT -type HTTPQUIC_REQ_DEFAULT -invoke policylabel
     _httpquicReqBuiltinDefaults
28
29 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
    USE_INVOCATION_RESULT -type HTTPQUIC_RES_DEFAULT -invoke policylabel
     _httpquicResBuiltinDefaults
30
31 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die ersten beiden Befehle in der Befehlsliste und die letzten beiden Befehle in derselben Liste sind der Vollständigkeit halber enthalten. Beim Ausführen der vier Befehle tritt möglicherweise ein Fehler auf, da die Befehle bereits zum Zeitpunkt des Neustarts der Appliance ausgeführt werden. Aber Sie können diese Fehler ignorieren.

Konfiguration der URL-Transformationsrichtlinie für HTTP/3-Datenverkehr

Die URL-Transformation ändert alle URLs in bestimmten Anfragen von einer externen Version, die von externen Benutzern gesehen wird, an eine interne URL, die nur von Ihren Webservern und Administratoren angezeigt wird. Sie können Benutzeranforderungen nahtlos umleiten, ohne dass die Netzwerkstruktur Benutzern zugänglich gemacht wird. Sie können auch komplexe interne URLs, die sich Benutzer möglicherweise schwer merken können, in einfachere, leichter zu merkende externe URLs ändern.

Virtuelle Server vom Typ HTTP über QUIC haben Cache-Policy-Unterstützung. Da QUIC jedoch

UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

URL-Transformationsprofil hinzufügen

Um ein URL-Transformationsprofil hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add transform profile <name> [-type URL]
2 <!--NeedCopy-->
```

Beispiel:

```
add transform profile msapps
```

URL-Transformationsaktion hinzufügen

Um eine URL-Transformation hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Beispiel:

```
add transform action docx2doc msapps 2
```

URL-Transformationsaktion hinzufügen

Um URL-Transformationsaktion zum Ersetzen der URL hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Beispiel:

```
add transform action docx2doc msapps 1
```


URL-Transformationsrichtlinie hinzufügen

Um eine URL-Transformationsrichtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add transform policy <name> <rule> <profileName> [-comment <string>]
     [-logAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add transform policy urltrans_udp "CLIENT.UDP.DSTPORT.EQ(443)"msapps
```

Binden Sie URL-Transformationsrichtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die URL-Transformationsrichtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
     ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
     positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
      REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
     -analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vs lb-http3 -policyName urltrans_udp -type REQUEST -priority 8
```

Binden Sie URL-Transformationsrichtlinie global mit einem HTTP/3 QUIC-basierten virtuellen Lastenausgleichsserver

Um eine URL-Transformationsrichtlinie zu binden HTTP/3 globaler Bindepunkt, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind transform global <policyName> <priority>  [<gotoPriorityExpression
     >] [-type <type>] [-invoke (<labelType>  <labelName>) ]
2 <!--NeedCopy-->
```

Beispiel:

```
bind transform global urltrans_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Weitere Informationen finden Sie unter Konfiguration von URL-Transformationsrichtlinien.

Konfiguration der Frontend-Optimierung (FEO) für HTTP/3-Datenverkehr

Die HTTP-Protokolle, die Webanwendungen zugrunde liegen, wurden ursprünglich entwickelt, um die Übertragung und das Rendern einfacher Webseiten zu unterstützen. Neue Technologien wie JavaScript und Cascading Stylesheets (CSS) sowie neue Medientypen wie Flash-Videos und grafikreiche Bilder stellen hohe Anforderungen an die Front-End-Performance, also an die Leistung auf Browserebene. Die Funktion der NetScaler Front-End-Optimierung (FEO) behebt solche Probleme und verkürzt die Ladezeit und die Renderzeit von Webseiten.

> **Hinweis:**
>
> `HTTP_QUIC _Override/Default_Request` Der Typ wird für globale Bindung von FEO-Richtlinien nicht unterstützt.

Aktion zur Frontend-Optimierung (FEO) hinzufügen

Um eine FEO-Aktion hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add feo action <name> [-pageExtendCache] [<cacheMaxage>][-
      imgShrinkToAttrib] [-imgGifToPng] [-imgToWebp] [-imgToJpegXR] [-
      imgInline] [-cssImgInline] [-jpgOptimize] [-imgLazyLoad] [-cssMinify
      ] [-cssInline] [-cssCombine] [-convertImportToLink] [-jsMinify] [-
      jsInline] [-htmlMinify] [-cssMoveToHead] [-jsMoveToEND][-
      domainSharding <string> <dnsShards> ...] [-clientSideMeasurements]
2
3 <!--NeedCopy-->
```

Beispiel:

```
add feo action feoact -imgGifToPng -pageExtendCache
```

Richtlinie zur Frontend-Optimierung (FEO) hinzufügen

Um eine FEO-Richtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add feo policy <name> <rule> <action>
```

Beispiel:

```
add feo policy udp_feo_img "CLIENT.UDP.DSTPORT.EQ(443)"IMG_OPTIMIZE
```

Binden Sie FEO-Richtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die FEO-Richtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName udp_feo_img -priority 4 -gotoPriorityExpression
 END -type REQUEST
```

Binden Sie die FEO-Richtlinie an den globalen HTTP/3-Bindepunkt

Um eine Cache-Richtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Beispiel:

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Weitere Informationen finden Sie unter Konfiguration von Front-End-Optimierungsrichtlinien.

SSL-Richtlinienkonfiguration für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC verfügen über SSL-Richtlinienunterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.
SSL-Richtlinien mit Aktionen, die für TLSV1.3 unterstützt werden, gelten nur für HTTP/3-Bind-Punkte oder virtuelle Server.

SSL-Richtlinie hinzufügen

Um eine FEO-Richtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:


```
add ssl policy <name> -rule <expression> [-action <string>] [-
    undefAction <string>] [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl policy ssl-pol -rule CLIENT.SSL.IS_SSL -action NOOP
```

Binden Sie SSL-Richtlinie an den virtuellen HTTP/3-Server

So binden Sie eine SSL-Richtlinie an den virtuellen HTTP/3-Server an der Eingabeaufforderung:

```
bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver lb-http3 -policyName ssl-pol -priority 4 -type REQUEST
```

Fügen Sie SSL-Richtlinie mit UDP-Ausdruck für SSL-Richtlinie hinzu

So fügen Sie an der Eingabeaufforderung eine SSL-Richtlinie mit UDP-Ausdruck hinzu:

```
add ssl policy <name> -rule <expression> [-action <string>] [-
    undefAction <string>] [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl policy ssl_udp_clnt -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action NOOP
```

Binden Sie SSL-Richtlinie mit UDP-Ausdruck an den virtuellen HTTP/3-Server

Um eine SSL-Richtlinie mit UDP-Ausdruck an den virtuellen HTTP/3-Server zu binden, geben Sie an der Eingabeaufforderung ein

```
bind ssl policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Beispiel:

```
bind ssl vs lb-http3 -policyName ssl_udp_clnt -priority 8 -type REQUEST
```


SSL-Richtlinie für den CLIENTHELLO Bindepunkt für HTTP/3-Datenverkehr hinzufügen

Um die SSL-Richtlinie für den CLIENTHELLO Bindepunkt für HTTP/3-Datenverkehr zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
add ssl policy ssl-pol-ch -rule "CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
(0x1301)"-action RESET
```

Binden Sie SSL-Richtlinie an den CLIENTHELLO Bindepunkt

Um eine SSL-Richtlinie an den CLIENTHELLO Bindepunkt zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
bind ssl vs lb-http3 -policyName ssl-pol-ch -type CLIENTHELLO_REQ -priority
 100
```

Binden Sie SSL-Richtlinie an den globalen HTTP/3-Bindepunkt

Um eine SSL-Richtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cache global <policy> -priority <positive_integer> [-gotoPriorityExpression
 <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]
```

Beispiel:

Es folgt ein Beispiel dafür, dass eine DATA-Richtlinie an einen globalen HTTP/3-Bindepunkt gebunden ist:

```
Bind ssl global -policyName ssl-pol-ch -priority 7 -type HTTPQUIC_DATA_DEFAULT
```


> **Hinweis:**
>
> Weiterleitungsaktion, die für den CLIENTHELLO Bindepunkt für virtuelle SSL-Server festgelegt werden kann, wird derzeit für virtuelle Server vom Typ HTTP_QUIC nicht unterstützt.

Konfiguration der Anwendungs-Firewall-Richtlinie für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC verfügen über Unterstützung der Firewall-Richtlinien für Webanwendungen. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Fügen Sie Web Application Firewall-Richtlinie mit UDP-Ausdruck hinzu

So fügen Sie an der Eingabeaufforderung die Web Application Firewall-Richtlinie mit UDP-Ausdruck hinzu:

```
1 add appfw policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw policy appfw_udp "CLIENT.UDP.DSTPORT.EQ(443)"APPFW_BYPASS
```

Binden von Protokollausdrücken mit UDP-basierten Ausdruck für das Web Application Firewall-Profil

So binden Sie Protokollausdrücke an das UDP for Web Application Firewall-Profil an der Eingabeaufforderung:

Beispiel:

```
bind appfw profile APPFW_BLOCK -logExpression logexp-1 "CLIENT.UDP.DSTPORT.
EQ(443)"
```

Binden Sie die Richtlinie der Anwendungs-Firewall mit dem virtuellen HTTP/3-Server

So binden Sie die Richtlinie der Web Application Firewall an den virtuellen HTTP/3-Server an der Eingabeaufforderung:


```
bind appfw policylabel <labelName> <policyName> <priority> [<
    gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vs lb-http3 -policyName appfw_udp -priority 3 -type REQUEST
```

Binden Sie die Richtlinie der Webanwendungs-Firewall an den globalen HTTP/3-Bindepunkt

Um eine Web Application Firewall-Richtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind appfw global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Beispiel:

```
bind appfw global appfw_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

AppQoE-Richtlinienkonfiguration für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC verfügen über AppQoE-Richtlinienunterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

AppQoE-Richtlinie mit UDP-basiertem Ausdruck hinzufügen

So fügen Sie an der Eingabeaufforderung eine AppQoE-Richtlinie mit UDP-Ausdruck hinzu:

```
add AppQoE policy <name> <rule> <profileName> [-comment <string>] [-
    logAction <string>]
<!--NeedCopy-->
```

Beispiel:

```
add appqoe policy appqoe-pol-udp -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action
appqoe-act-basic-prhigh
```


Binden Sie die AppQoE-Richtlinie mit dem virtuellen HTTP/3-Server

Um die AppQoE-Richtlinie an den virtuellen HTTP/3-Server zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind appqoe policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vs lb-http3 -policyName appqoe-pol-udp -type REQUEST -priority 3
```

Binden Sie die AppQoE-Richtlinie an den virtuellen HTTP_QUIC Server

Um die AppQoE-Richtlinie an den `HTTP_QUIC` virtuellen Server zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind appqoe <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vs lb-http3 -policyName appqoe-pol-primd -priority 8 -type REQUEST
```

HTTP/3-Dienstermittlung

May 11, 2023

Das HTTP-Protokoll basiert auf der Verwendung von HTTP-Alternativdiensten für den Ursprungsserver, um die Verfügbarkeit eines gleichwertigen Dienstes bekannt zu geben. Die HTTP/3-Diensterkennung verwendet ebenfalls das gleiche Prinzip. Ein alternativer HTTP/3-Endpunkt kann mit einer der folgenden Methoden beworben werden:

- HTTP Alt-Svc-Antwortheader
- HTTP/2 Alt-Svc Frame in der Antwort
- Application Layer Protocol Negotiation (ALPN)

Der alternative Dienst gibt die Verwendung eines HTTP-Alt-Svc-Antwortheaders und des HTTP/2 Alt-Svc-Frames als HTTP/3-Endpunkt an. Server können HTTP/3 an jedem UDP-Port bereitstellen. Eine alternative Dienstankündigung enthält einen expliziten Port, und URLs enthalten entweder einen expliziten Port oder einen Standardport, der mit dem Schema verknüpft ist.

Clients, die alternative Service-Header oder Frames erhalten, sind nicht verpflichtet, sie zu verwenden. Der Kunde sollte, wenn er auf einen alternativen Dienst aufmerksam gemacht wird und wenn er den alternativen Dienstmechanismus unterstützt, den entsprechenden alternativen Dienst verwenden, der beworben wird. Mit anderen Worten, ein HTTP/1.1-Dienst oder ein HTTP/2-Dienst kann einen äquivalenten Endpunkt ankündigen, der das HTTP/3-Protokoll unterstützt. Der Client, der diese alternativen Dienstinformationen erhält, kann wählen, ob er eine QUIC-Verbindung mit dem angegebenen alternativen Dienst herstellen möchte, und sobald diese Verbindung verfügbar ist, kann diese Verbindung für alle nachfolgenden Anfragen verwendet werden. Wenn der Aufbau der Verbindung mit dem ausgewählten alternativen Dienst fehlschlägt, kann der Client auf den ursprünglichen Endpunkt zurückgreifen. Wenn der Client den beworbenen alternativen Dienst verwendet, wird dies durch Einbeziehung eines Alt-Used-Headers angegeben.

NetScaler unterstützt werbeäquivalente HTTP/3-Endpunkte auf virtuellen Servern vom Typ HTTP und SSL.

Konfigurieren der HTTP/3-Diensterkennung

Führen Sie die folgenden Schritte aus, um die HTTP/3-Diensterkennung zu konfigurieren:

1. Konfigurieren des alternativen HTTP/3-Dienstendpunkts mit einem HTTP-Alt-Svc-Header
2. Konfigurieren Sie den alternativen HTTP/3-Dienstendpunkt mithilfe eines HTTP/2 Alt-Svc-Frames
   Konfigurieren Sie den alternativen HTTP/3-Dienstendpunkt mithilfe eines HTTP-Alt-Svc-Headers
   So kündigen Sie einen HTTP/3-Endpunkt mithilfe eines HTTP-Alt-Svc-Headers an, geben Sie den folgenden Befehl ein:

Hinweis: Der Hauptzweck der Werbung für alternative Dienste besteht darin, den Benutzer wissen zu lassen, dass die HTTP/3-Fähigkeit auch über den HTTP/1.1- oder HTTP/2-Dienst unter einem.b.d:443 zugegriffen werden kann.

```
1 add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ns httpProfile http-profile -altsvc ENABLED -altSvcValue  "h3-29="
      :443"; ma=3600; persist=1"
2 <!--NeedCopy-->
```

oder

```
1 set ns httpProfile http-custom -altsvc ENABLED -altSvcValue  "h3-29="
      :443"; ma=3600; persist=1"
```



```
<!--NeedCopy-->
```

Konfigurieren Sie den alternativen HTTP/3-Dienstendpunkt mithilfe eines HTTP/2 Alt-Svc-Frames

Um einen HTTP/3-Endpunkt mithilfe eines HTTP/2 Alt-SVC-Frames anzukündigen, geben Sie den folgenden Befehl ein:

```
add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ] -
    http2AltSvcFrame [ ENABLED | DISABLED ]
<!--NeedCopy-->
```

Beispiel:

```
add ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue "h3-29=\":443\"; ma=3600; persist=1"
```

oder

```
set ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue "h3-29=\":443\"; ma=3600; persist=1"
```

Konfigurieren Sie den HTTP/3-Alternativdienst mit HTTP-Alt-Svc-Header-Wert über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Profile > HTTP-Profile**.
2. Klicken Sie auf **Hinzufügen**.
3. Wechseln Sie auf der Seite “ **HTTP-Profil erstellen** “ zum Abschnitt HTTP/3 und aktivieren Sie das Kontrollkästchen **Alternativer Dienst** .
4. Das System zeigt das Textfeld **Alternativer Dienstwert** im Abschnitt http2 an.
5. Geben Sie den alternativen Dienstwert als “h3-29=” :443” ein; ma=3600; persist=1”
6. Klicken Sie auf **OK** und auf **Schließen**.

gRPC

May 11, 2023

gRPC in einer NetScaler-Appliance ist ein leichtes, leistungsstarkes und universelles Open-Source-RPC-Framework (Remote Procedure Call). Das Framework ist optimal, um in mehreren Sprachen zu arbeiten, die auf jedem Betriebssystem ausgeführt werden. Auch im Vergleich zu anderen Protokollen bietet gRPC eine bessere Leistung und Sicherheit.

gRPC für NetScaler wird aus den folgenden Gründen bevorzugt:

- Entwickeln Sie verteilte Anwendungen für Rechenzentren und öffentliche/private Cloud-Infrastrukturen.
- Stellen Sie die Kommunikation zwischen Client und Server für Mobilgeräte, das Internet oder die Cloud bereit.
- Greifen Sie auf Cloud-Dienste und Anwendungen zu
- Microservice-Bereitstellungen

Warum gRPC in NetScaler

gRPC in NetScaler wird über HTTP/2 implementiert, um leistungsstarke und skalierbare APIs zu unterstützen. Die Verwendung von Binär statt Text sorgt dafür, dass die Payload kompakt und effizient bleibt. In NetScaler werden die HTTP/2-Anfragen über eine einzige TCP-Verbindung gemultiplext, sodass mehrere Nachrichten gleichzeitig übertragen werden können, ohne die Auslastung der Netzwerkressourcen zu beeinträchtigen. Es verwendet auch Header-Komprimierung, um die Größe von Anfragen und Antworten zu reduzieren.

gRPC unterstützt die folgenden Arten von Servicemethoden, mit denen ein Client Parameter und Rückgabetypen aus der Ferne aufrufen kann.

1. **Unärer RPC**. Der Client sendet eine einzelne Anfrage an den gRPC-Server und erhält eine einzige Antwort zurück.

   Beispiel:
   ```
   rpc SayHello(HelloRequest)returns (HelloResponse);
   ```

2. **RPC-Streaming-Server**. Der Client sendet eine einzelne Anfrage an den gRPC-Server und erhält eine Stream-Antwort.

   Beispiel:
   ```
   rpc StreamingResponse(HelloRequest)returns (HelloResponse);
   ```

3. **Client-Streaming-RPC.** Der Client sendet eine Folge von Nachrichten und wartet darauf, dass der Server seine Antwort liest und zurückgibt.

Beispiel:

```
rpc IntroduceYourself(stream HelloRequest)returns (HelloResponse)
```

4. **Bidirektionales Streaming-RPC**. Sowohl der Client als auch der Server von beiden Seiten senden einen Nachrichtenstrom mithilfe des Lese-Schreib-Streams. Die beiden Streams funktionieren unabhängig voneinander.

   Beispiel:

   ```
   rpc ChatSession (stream HelloRequest)returns (stream HelloResponse)
   ```

NetScaler unterstützt die folgenden Funktionen für seine Dienste mit gRPC-Endpunkten:

- Lastausgleich
- Content Switching
- Sichere Endpunktdienste wie Web Application Firewall, Authentifizierung.
- Konfiguration der Richtlinie
- Statistiken und Protokollierung
- Umschreiben von Inhalten, Filtern von Inhalten
- Layer-4- und Layer-7-Optimierungen, TLS-Angebot
- Gateway-Lösungen für Protokollübersetzungen

gRPC-Komplett-Konfiguration

May 11, 2023

Die gRPC-Ende-zu-Ende-Konfiguration funktioniert, indem eine gRPC-Anfrage von einem Client über das HTTP/2-Protokoll gesendet und erneut gRPC-Nachrichten weitergeleitet werden, die vom gRPC-Server beantwortet wurden.

So funktioniert die durchgängige gRPC-Konfiguration

Das folgende Diagramm zeigt, dass eine gRPC-Konfiguration in einer NetScaler-Appliance funktioniert.

1. Um die gRPC-Konfiguration bereitzustellen, müssen Sie zunächst HTTP/2 im HTTP-Profil aktivieren und außerdem die HTTP/2-Unterstützung global auf der Serverseite aktivieren.
2. Wenn ein Client eine gRPC-Anfrage sendet, wertet der virtuelle Load-Balancing-Server den gRPC-Verkehr mithilfe von Richtlinien aus.
3. Basierend auf der Bewertung der Richtlinien beendet der virtuelle Lastausgleichsserver (mit dem daran gebundenen gRPC-Dienst) die Anfrage und leitet sie als gRPC-Anfrage an den Back-End-gRPC-Server weiter.
4. In ähnlicher Weise beendet die Appliance die Antwort und leitet sie als gRPC-Antwort an den Client weiter, wenn der gRPC-Server auf den Client reagiert.

Beispiel für eine gRPC-Anfrage, die an den gRPC-Server gesendet wurde

Der Anforderungsheader wird als HTTP/2-Header in HEADERS+CONTINUATION Frames gesendet.

```
1  ```
2  HEADERS (flags = END_HEADERS)
3  : method = POST
4  : scheme = http
5  : path = /helloworld.citrix-adc/SayHello
6  : authority = 10.10.10.10.:80
7  grpc-timeout = 15
8  content-type = application/grpc+proto
9  grpc-encoding = gzip
10 DATA (flags = END_STREAM)
11 <Length-Prefixed Message>
12 <!--NeedCopy--> ```
```

Beispiel für gRPC-Antwortheader vom gRPC-Server zur NetScaler Appliance

Response-Header und Trailers-Only werden in einem einzigen HTTP/2-HEADERS-Frameblock bereitgestellt. Es wird erwartet, dass die meisten Antworten sowohl Kopfzeilen als auch Trailer enthalten,

aber für Aufrufe, die sofort einen Fehler auslösen, ist der Befehl „Nur Trailer“ zulässig. Der Status muss in Trailers gesendet werden, auch wenn der HTTP-Statuscode in Ordnung ist.

```
```
HEADERS (flags = END_HEADERS)
: status = 200
Grpc-encoding= gzip
Content-type = application/grpc+proto
DATA
<Length-Prefixed Message>
HEADERS (flags = END_STREAM, END_HEADERS)
grpc-status = 0 # OK

<!--NeedCopy--> ```
```

## Konfigurieren von GRPC über die CLI

Um eine lückenlose gRPC-Bereitstellung zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Fügen Sie ein HTTP-Profil hinzu, bei dem HTTP/2 und HTTP/2 Direct aktiviert sind.
- Aktivieren Sie die globale Backend-HTTP/2-Unterstützung im HTTP-Parameter
- Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest
- Dienst für gRPC-Endpunkt hinzufügen und HTTP-Profil festlegen
- Binden Sie den gRPC-Endpunktdienst an den virtuellen Lastausgleichsserver

### Fügen Sie ein HTTP-Profil hinzu, bei dem HTTP/2 Direct und HTTP/2 Direct aktiviert sind

Sie müssen die direkten HTTP/2- und HTTP/2-Parameter im HTTP-Profil aktivieren. Außerdem müssen Sie den HTTP/2-Direktparameter aktivieren, wenn gRPC über HTTP/2-Klartext erforderlich ist.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Aktivieren Sie die globale Backend-HTTP/2-Unterstützung über den HTTP-Parameter

Um die HTTP/2-Unterstützung global auf der Serverseite mithilfe der NetScaler-Befehlszeile zu aktivieren.


```

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns httpParam -http2ServerSide(ON | OFF)
```

Beispiel:

```
set ns httpParam -http2ServerSide ON
```

Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

So fügen Sie einen virtuellen Lastenausgleichsserver mit der **NetScaler** Befehlszeilenschnittstelle hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Beispiel:

```
add lb vserver lb-grpc HTTP 10.10.10.11 80 -httpProfileName http2gRPC
```

> **Hinweis:**
>
> Wenn Sie einen virtuellen Lastausgleichsserver vom Typ SSL verwenden, müssen Sie das Serverzertifikat binden. Weitere Informationen finden Sie unter Thema Serverzertifikat binden .

Dienst für gRPC-Endpunkt hinzufügen und HTTP-Profil festlegen

So fügen Sie mithilfe der **NetScaler** Befehlszeilenschnittstelle einen gRPC-Dienst mit HTTP-Profil hinzu: Geben Sie
an der Eingabeaufforderung Folgendes ein:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Beispiel:

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Binden Sie den gRPC-Endpunktdienst an den virtuellen Lastausgleichsserver

So binden Sie einen gRPC-Dienst mithilfe der **NetScaler** Befehlszeilenschnittstelle an den virtuellen Lastenausgleichsserver:

Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
bind lb vserver <name> <serviceName>
```


Beispiel:

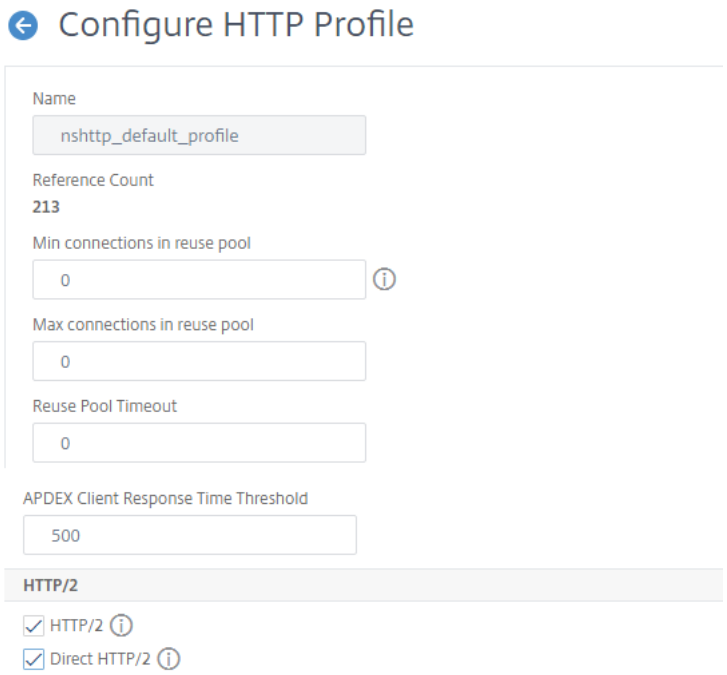
```
bind lb vserver lb-grpc svc-grpc
```

Konfigurieren Sie die komplette gRPC-Bereitstellung mithilfe der GUI

Gehen Sie wie folgt vor, um gRPC mithilfe der GUI zu konfigurieren.

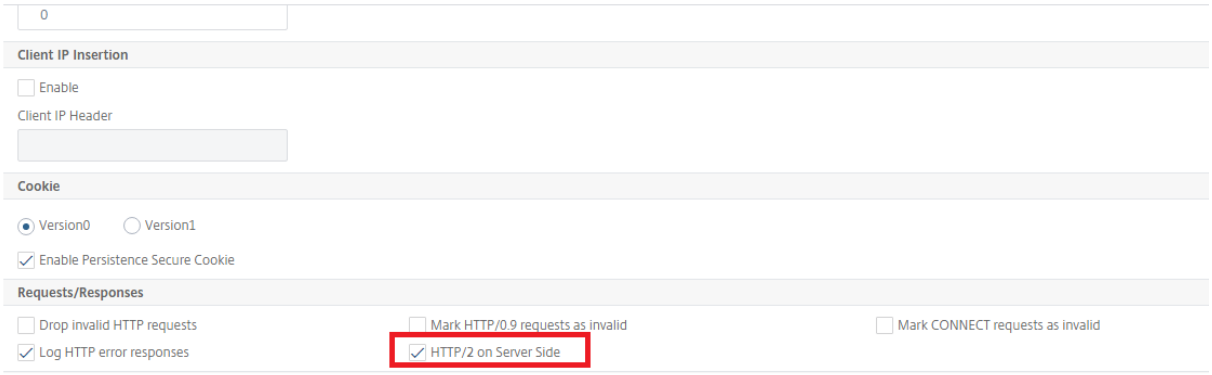
Fügen Sie ein HTTP-Profil hinzu, bei dem HTTP/2 Direct und HTTP/2 Direct aktiviert sind

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Aktivieren Sie die HTTP/2-Option in einem neuen HTTP-Profil oder einem vorhandenen HTTP-Profil



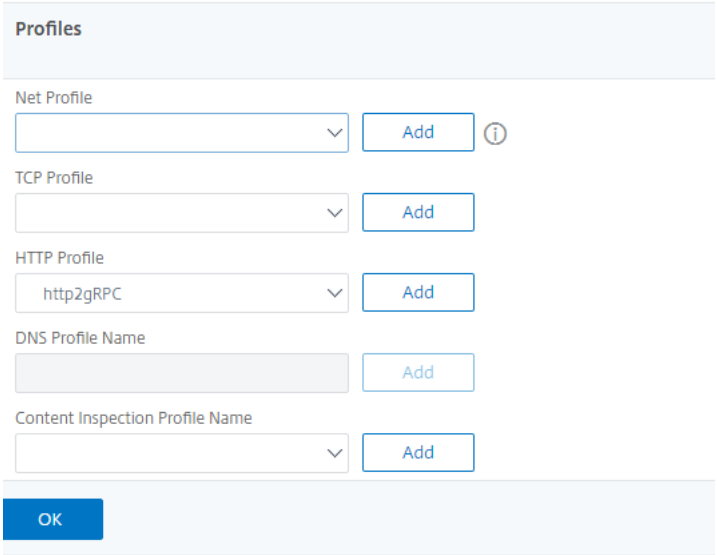
Aktivieren Sie die globale Backend-HTTP/2-Unterstützung im HTTP-Parameter

1. Navigieren Sie zu **System > Einstellungen > HTTP-Parameter**.
2. Wählen Sie auf der Seite „HTTP-Parameter konfigurieren“ die Option HTTP/2 auf der Serverseite aus.
3. Klicken Sie auf **OK**.



Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

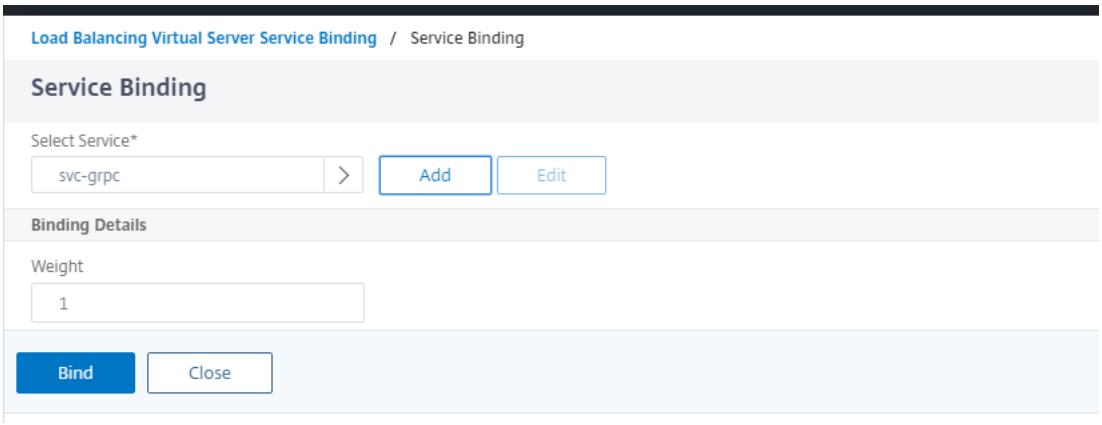
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf Hinzufügen, um einen virtuellen Lastausgleichsserver für gRPC-Verkehr zu erstellen.
3. Klicken Sie auf der Seite Virtueller Server für Lastenausgleich auf Profile.
4. Wählen Sie im Abschnitt Profile den Profiltyp als HTTP aus.
5. Klicke auf OK und dann auf Fertig.



Dienst für gRPC-Endpunkt hinzufügen und HTTP-Profil festlegen

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie auf Hinzufügen, um einen Anwendungsserver für gRPC-Verkehr zu erstellen.
3. Gehen Sie auf der Seite Load Balancing Service zum Abschnitt Profil .
4. Fügen Sie unter Profile das HTTP-Profil für den gRPC-Endpunkt hinzu.

5. Klicke auf OK und dann auf Fertig.



Ausführliche GUI-Prozeduren im Zusammenhang mit dem Lastenausgleich finden Sie unter Thema Load Balancing .

gRPC-Brücke

May 11, 2023

Wenn ein Client eine Anfrage über das HTTP/1.1-Protokoll sendet, unterstützt die NetScaler-Appliance das Bridging der gRPC-Anfragen über das HTTP/1.1-Protokoll, das dem gRPC-Server über das HTTP/2-Protokoll entspricht. In ähnlicher Weise empfängt die Appliance beim Reverse-Bridging die Client-gRPC-Anfrage über das HTTP/2-Protokoll und führt Reverse-Bridging für die gRPC-Anfragen gemäß dem gRPC-Server des HTTP/1.1-Protokolls durch.

So funktioniert gRPC-Bridging

In diesem Szenario überbrückt die NetScaler-Appliance gRPC-Inhalte, die über eine HTTP/1.1-Verbindung empfangen wurden, nahtlos und leitet sie über HTTP/2 an den Back-End-gRPC-Server weiter.

Das folgende Diagramm zeigt, wie Komponenten in einer gRPC-Bridging-Konfiguration miteinander interagieren.

1. Wenn eine gRPC-Anfrage gesendet wird, überprüft die NetScaler-Appliance, ob die Verbindung HTTP/1.1 und der Inhaltstyp application/grpc ist. Die HTTP/1.1-Anfragen werden in die folgenden Pseudo-Header übersetzt.
2. Beim Empfang einer gRPC-Anfrage über eine HTTP/1.1-Verbindung, wie im Content-Type-Header angegeben, wandelt die ADC-Appliance die Anfrage wie unten angegeben über HTTP/2 in gRPC um:

```
    :method: Method-name in HTTP/1.1 request
    :path: Path is HTTP/1.1 request
    content-type: application/grpc
<!--NeedCopy-->
```

1. Basierend auf der Bewertung der Richtlinien beendet der virtuelle Lastausgleichsserver (an den der gRPC-Dienst gebunden ist) die Anfrage oder leitet sie über HTTP/2-Frames an den Back-End-gRPC-Server weiter.
2. Beim Empfang der Antwort über eine HTTP/2-Verbindung vom gRPC-Server puffert die Appliance, bis sie den HTTP/2-Trailer empfängt, und sucht dann nach dem gRPC-Statuscode. Wenn der gRPC-Fehlerstatus ungleich Null ist, sucht die Appliance nach dem zuordnenden HTTP-Statuscode und sendet eine geeignete HTTP/1.1-Fehlerantwort.

Konfigurieren Sie das gRPC-Bridging mithilfe der CLI

Um gRPC-Bridging zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie ein HTTP-Profil hinzu, bei dem HTTP/2 Direct und HTTP/2 Direct aktiviert sind
2. Aktivieren Sie die globale Back-End-HTTP/2-Unterstützung im HTTP-Parameter
3. Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest
4. Fügen Sie den Dienst für den GrPC-Endpunkt hinzu und legen Sie das HTTP-Profil fest
5. Binden Sie den gRPC-Endpunktdienst an den virtuellen Lastausgleichsserver
6. Ordnen Sie den gRPC-Statuscode der HTTP-Antwort zu, wenn der gRPC-Status ungleich Null ist
7. Konfigurieren Sie die gRPC-Pufferung nach Zeit und/oder Größe

Fügen Sie ein HTTP-Profil hinzu, bei dem die Direkten HTTP/2 und HTTP/2 aktiviert sind

Um mit der Konfiguration zu beginnen, müssen Sie die HTTP/2-Funktion im HTTP-Profil aktivieren. Wenn der Client die HTTP 1.1-Anfragen sendet, überbrückt die Appliance die Anfrage und leitet sie an den Backend-Server weiter.

Geben Sie in der Befehlszeile Folgendes ein:


```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Aktivieren Sie die globale Backend-HTTP/2-Unterstützung im HTTP-Parameter

Um die HTTP/2-Unterstützung global auf der Serverseite mithilfe der NetScaler-Befehlszeile zu aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Beispiel:

```
set ns httpParam -http2ServerSide ON
```

Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

So fügen Sie einen virtuellen Lastenausgleichsserver mit der **NetScaler** Befehlszeilenschnittstelle hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Beispiel:

```
add lb vserver lb-grpc HTTP 10.10.10.10 80 -httpProfileName http2gRPC
```

> **Hinweis:**
>
> Wenn Sie einen virtuellen Lastausgleichsserver vom Typ SSL verwenden, müssen Sie das Serverzertifikat binden. Weitere Informationen finden Sie unter Thema Serverzertifikat binden .

Fügen Sie den Dienst für den GrPC-Endpunkt hinzu und legen Sie das HTTP-Profil fest

So fügen Sie mithilfe der **NetScaler** Befehlszeilenschnittstelle einen gRPC-Dienst mit dem HTTP-Profil hinzu.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```


Beispiel:

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Binden Sie den gRPC-Endpunktdienst an den virtuellen Lastausgleichsserver

Um einen gRPC-Endpunktdienst mithilfe der CLI an den virtuellen Load-Balancing-Server zu binden.

Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
bind lb vserver <name> <serviceName>
```

Beispiel:

```
bind lb vserver lb-grpc svc-grpc
```

Ordnen Sie den gRPC-Statuscode dem HTTP-Statuscode in der HTTP/1.1-Antwort zu

Im gRPC-Bridging-Szenario reagiert der gRPC-Dienst auf die Anfrage mit einem gRPC-Statuscode. Die Appliance ordnet den gRPC-Statuscode einem entsprechenden HTTP-Antwortcode und einer Begründung zu. Die Zuordnung erfolgt auf der Grundlage der unten angegebenen Tabelle. Wenn die NetScaler-Appliance die HTTP/1.1-Antwort an den Client sendet, sendet sie den HTTP-Statuscode und die Begründung.

gRPC-Statuscode	Statuscode der HTTP-Antwort	Grundphrase für die HTTP-Antwort
OK = 0	200	OK
STORNIERT = 1	499	*
UNBEKANNT = 2	500	Interner Serverfehler
UNGÜLTIGE_ARGUMENT = 3	400	Ungültige Anforderung
DEADLINE_ÜBERSCHRITTEN = 4	504	Gateway-Timeout
NICHT_GEFUNDEN = 5	404	*
EXISTIERT_BEREITS = 6	409	Konflikt
ERLAUBNIS_VERWEIGERT = 7	403	Verboten
NICHT AUTHENTIFIZIERT = 16	401	Nicht autorisiert
RESSOURCE_EXHAUSTED = 8	429	*
FEHLGESCHLAGENE VORBEDINGUNG = 9	400	Ungültige Anforderung
ABGEBROCHEN = 10	409	Konflikt

gRPC-Statuscode	Statuscode der HTTP-Antwort	Grundphrase für die HTTP-Antwort
AUSSERHALB DES ZULÄSSIGEN BEREICHS = 11	400	Ungültige Anforderung
NICHT IMPLEMENTIERT = 12	501	Nicht implementiert
INTERN = 13	500	Interner Serverfehler
NICHT VERFÜGBAR = 14	503	Dienst nicht verfügbar
DATENVERLUST = 15	500	Interner Serverfehler

Konfigurieren Sie die gRPC-Pufferung nach Zeit und/oder Größe

Die NetScaler-Appliance puffert die gRPC-Antwort vom Back-End-Server, bis der Antwort-Trailer empfangen wird. Dadurch werden bidirektionale gRPC-Aufrufe unterbrochen. Wenn die gRPC-Antwort sehr groß ist, verbraucht sie außerdem eine erhebliche Menge an Speicher, um die Antwort vollständig zu puffern. Um das Problem zu lösen, wurde die gRPC-Bridging-Konfiguration erweitert, um die Pufferung zeitlich und/oder größenmäßig zu begrenzen. Wenn die Puffergröße oder das Zeitlimit den Schwellenwert überschreitet, stoppt die Appliance die Pufferung und leitet die Antwort an den Client weiter, auch wenn eine der Einschränkungen ausgelöst wird (entweder wird der Trailer nicht innerhalb der konfigurierten Puffergröße empfangen oder wenn das konfigurierte Timeout eintritt). Daher funktionieren die konfigurierten Richtlinien und ihre Ausdrücke (basierend auf dem GRPC-Statuscode) nicht wie erwartet.

Um die gRPC-Pufferung durch die CLI nach Zeit und/oder Größe zu begrenzen, können Sie konfigurieren, wann Sie ein neues HTTP-Profil hinzufügen, oder konfigurieren, wenn Sie ein vorhandenes Profil ändern.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Oder

```
set ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Hierbei gilt:

`grpcholdlimit`. Maximale Größe in Byte, die zum Puffern von gRPC-Paketen zulässig ist, bis der Trailer empfangen wird. Sie können sowohl die Parameter als auch einen beliebigen Parameter konfigurieren.

Standardwert: 131072
Mindestwert: 0
Maximalwert: 33554432

`grpcholdtimeout`. Maximal zulässige Zeit in Millisekunden, um gRPC-Pakete zwischenzuspeichern, bis der Trailer empfangen wird. Der Wert sollte ein Vielfaches von 100 sein.
Standardwert: 1000
Mindestwert: 0
Maximalwert: 180000

Beispiel:

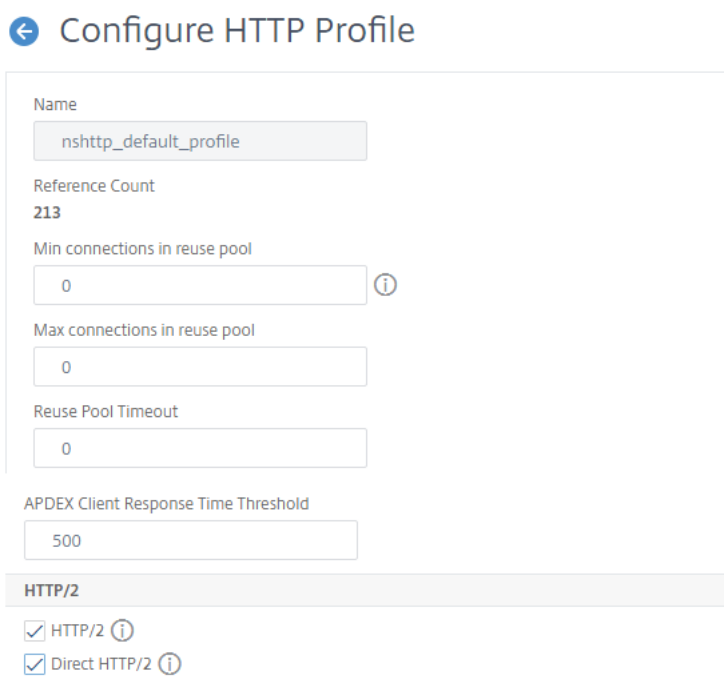
```
add httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
set httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
```

Konfigurieren Sie gRPC-Bridging mithilfe der GUI

Gehen Sie wie folgt vor, um gRPC-Bridging mithilfe der NetScaler-GUI zu konfigurieren.

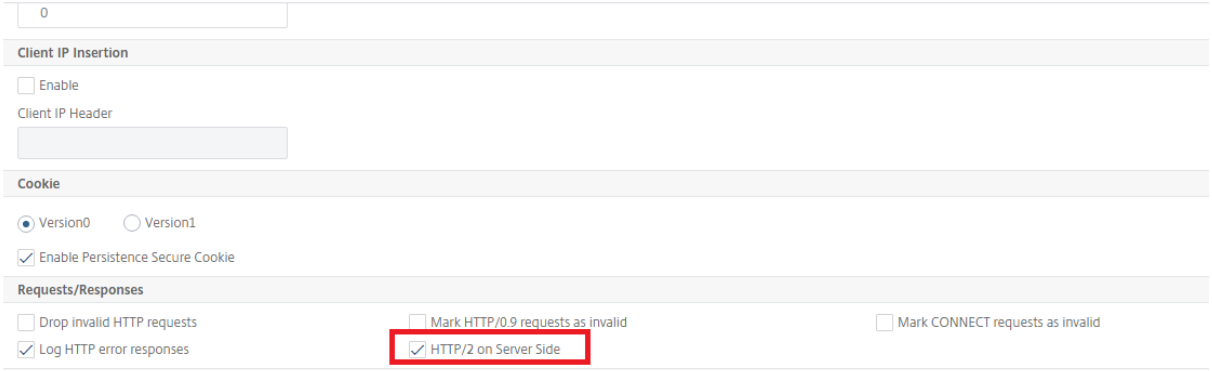
Fügen Sie ein HTTP-Profil hinzu, bei dem HTTP/2 Direct und HTTP/2 Direct aktiviert sind

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Wählen Sie **HTTP/2** im HTTP-Profil aus.



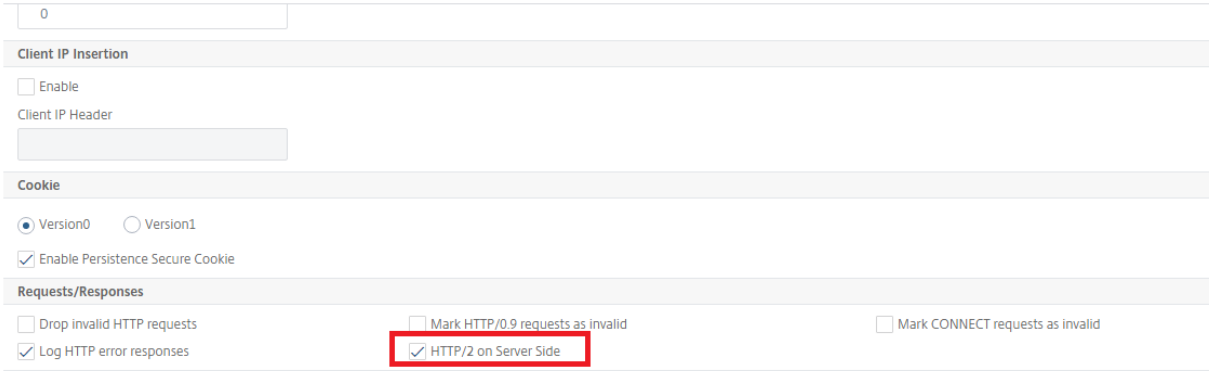
Aktivieren Sie die globale Back-End-HTTP/2-Unterstützung im HTTP-Parameter

1. Navigieren Sie zu **System > Einstellungen > HTTP-Parameter**.
2. Wählen Sie auf der Seite „ **HTTP-Parameter konfigurieren** “ die Option **HTTP/2 auf Serverseite** aus.
3. Klicken Sie auf **OK**.



Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

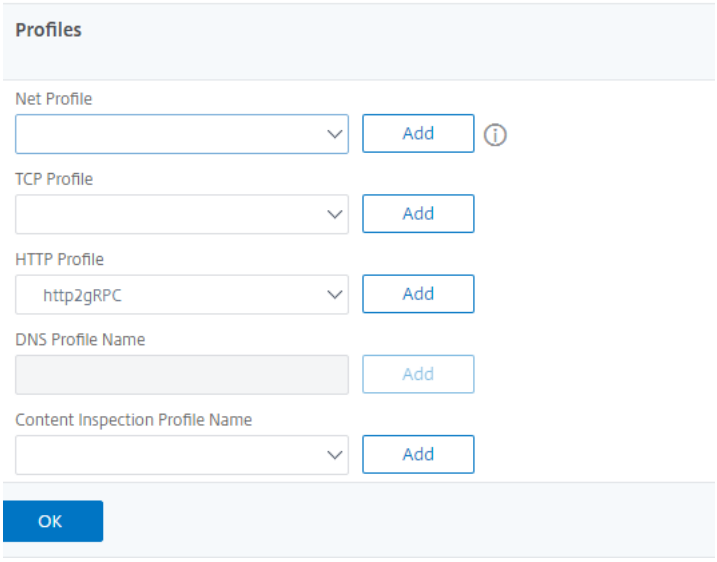
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Verkehr zu erstellen.
3. Klicken Sie auf der Seite **Virtueller Server für Lastenausgleich** auf **Profile**.
4. Wählen Sie im Abschnitt **Profile** den Profiltyp als HTTP aus.
5. Klicke auf **OK** und dann auf **Fertig**.



Dienst für gRPC-Endpunkt hinzufügen und HTTP-Profil festlegen

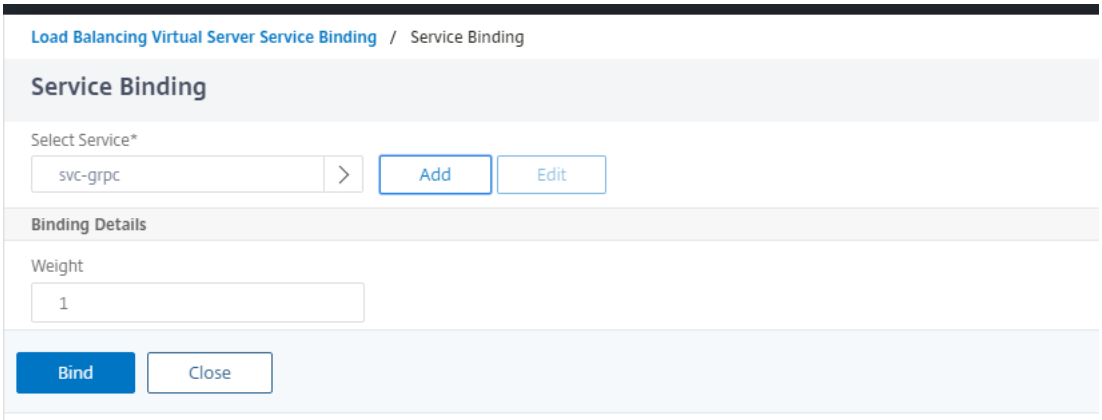
1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie auf **Hinzufügen**, um einen Anwendungsserver für gRPC-Verkehr zu erstellen.
3. Gehen Sie auf der Seite **Load Balancing Service** zum Abschnitt **Profil** .

4. Fügen Sie unter **Profile**das **HTTP-Profil** für den gRPC-Endpunkt hinzu.
5. Klicke auf **OK** und dann auf **Fertig**.



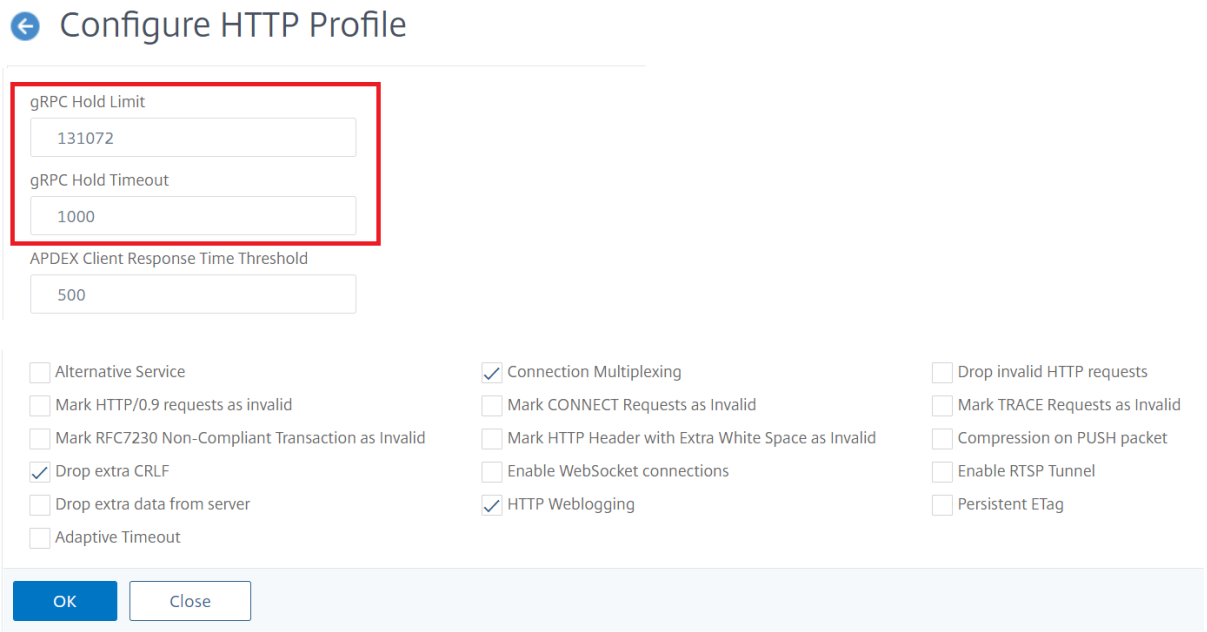
Binden Sie den Dienst für den gRPC-Endpunkt an den virtuellen Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Verkehr zu erstellen.
3. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf den Abschnitt **Dienst- und Dienstgruppen** .
4. Wählen Sie auf der Seite **Load Balancing Virtual Server Service Binding** den gRPC-Dienst aus, den Sie binden möchten.
5. Klicken Sie auf **Schließen** und dann auf **Fertig**.



Konfigurieren Sie die gRPC-Pufferung nach Zeit und Größe mithilfe der GUI

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Wählen Sie **HTTP/2** im HTTP-Profil aus.
3. Stellen Sie auf der Seite „ **HTTP-Profil konfigurieren** “ die folgenden Parameter ein:
   a) GRPCHoldTimeout. Geben Sie die Zeit in Millisekunden ein, um gRPC-Pakete zwischenzuspeichern, bis der Trailer empfangen wird.
   b) GRP-Obergrenze. Geben Sie die maximale Größe in Byte ein, um gRPC-Pakete zwischenzuspeichern, bis der Trailer empfangen wird.
4. Klicken Sie auf **OK** und auf **Schließen**.



Ausführliche GUI-Prozeduren für das Binden von Service und Lastenausgleich virtueller Server finden Sie unter Thema Load Balancing .

gRPC-Reverse-Bridging

May 11, 2023

In diesem Szenario überbrückt die NetScaler-Appliance gRPC-Inhalte, die über eine HTTP/2-Verbindung empfangen wurden, nahtlos und leitet sie über HTTP/1.1 an den Back-End-gRPC-Server weiter.

So funktioniert Reverse Bridging

Das folgende Diagramm zeigt, wie Komponenten in einer gRPC-Bridging-Konfiguration miteinander interagieren.

1. Der Client sendet eine gRPC-Anfrage über eine HTTP/2-Verbindung mit gRPC-Headern in HTTP/2-Frames und Proto-Buf-Nutzlast.
2. Basierend auf der Bewertung der Richtlinien übersetzt der virtuelle Load-Balancing-Server (mit dem daran gebundenen gRPC-Dienst) die Anfrage und leitet sie über eine HTTP/1.1-Verbindung an den Backend-Server weiter.
3. Wenn die Antwort auf HTTP/1.1 empfangen wird und die Antwort keinen GRPC-Statuscode enthält, leitet ADC aus dem HTTP-Antwortcode einen GRPC-Statusfall ab.
4. Die Appliance fügt dann die gRPC-Header in den HTTP/2-Trailer ein, bevor sie die Antwort an den Client weiterleitet.

Konfigurieren Sie gRPC Reverse Bridging mithilfe der CLI

Um gRPC Reverse Bridging zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Fügen Sie das HTTP-Profil 1 hinzu, wobei HTTP/2 und HTTP/2 Direct für den virtuellen Lastausgleichsserver aktiviert sind
- Fügen Sie HTTP-Profil 2 hinzu, wobei HTTP/2 für den Backend-Server deaktiviert ist
- Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und stellen Sie ihn auf HTTP-Profil 1 ein
- Dienst für den gRPC-Endpunkt hinzufügen und auf HTTP-Profil 2 setzen
- Binden Sie den Dienst für den gRPC-Endpunkt an den virtuellen Lastausgleichsserver
- Ordnen Sie den HTTP-Statuscode dem gRPC-Statuscode zu, wenn die Antwort keinen GRPC-Statuscode hat

Fügen Sie das HTTP-Profil 1 hinzu, wobei HTTP/2 und HTTP/2 Direct für den virtuellen Lastausgleichsserver aktiviert sind

Um mit der Reverse-Bridging-Konfiguration zu beginnen, müssen Sie zwei HTTP-Profile hinzufügen. Ein Profil zum Aktivieren von HTTP/2 für gRPC-Clientanfragen und ein anderes Profil zum Deaktivieren

von HTTP/2 für Serverantworten ohne gRPC.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

füge ns hinzu HttpProfile profile1 —http2 ENABLED -Http2Direct AKTIVIERT

Fügen Sie HTTP-Profil 2 hinzu, wobei HTTP/2 für Back-End-Server deaktiviert ist

Um die HTTP/2-Unterstützung im HTTP-Profil für die Antwort des Back-End-Servers zu deaktivieren, verwenden Sie die NetScaler-Befehlszeile.

Geben Sie in der Befehlszeile Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

füge ns hinzu HttpProfile profile2 —http2 DEAKTIVIERT http2Direct DEAKTIVIERT

Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und stellen Sie ihn auf HTTP-Profil 1 ein

So fügen Sie einen virtuellen Lastenausgleichsserver mithilfe der NetScaler Befehlszeilenschnittstelle hinzu.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Beispiel:

füge lb vserver lb-grpc HTTP 10.10.10.10 80 -HttpProfilname profile1 hinzu

> **Hinweis:**
>
> Wenn Sie einen virtuellen Lastausgleichsserver vom Typ SSL verwenden, müssen Sie das Serverzertifikat binden. Weitere Informationen finden Sie unter Thema Serverzertifikat binden .

Dienst für den gRPC-Endpunkt hinzufügen und auf HTTP-Profil 2 setzen

So fügen Sie einen Dienst mit dem GrPC-Endpunkt hinzu und legen das HTTP-Profil 2 mithilfe der NetScaler Befehlszeilenschnittstelle fest.

Geben Sie in der Befehlszeile Folgendes ein:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Beispiel:

```
add service svc-grpc 10.10.10.11 HTTP 80 -httpProfileName profile2
```

Binden Sie den Dienst für den gRPC-Endpunkt an den virtuellen Lastausgleichsserver

So binden Sie einen gRPC-Dienst mithilfe der NetScaler Befehlszeilenschnittstelle an den virtuellen Lastenausgleichsserver.

Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
bind lb vserver <name> <serviceName>
```

Beispiel:

```
bind lb vserver lb-grpc svc-grpc
```

Ordnen Sie den HTTP-Antwortcode dem gRPC-Statuscode zu

Wenn der Server keinen gRPC-Statuscode generiert, generiert die NetScaler-Appliance auf der Grundlage der empfangenen HTTP-Antwort einen geeigneten gRPC-Statuscode. Die Statuscodes sind in der folgenden Zuordnungstabelle aufgeführt.

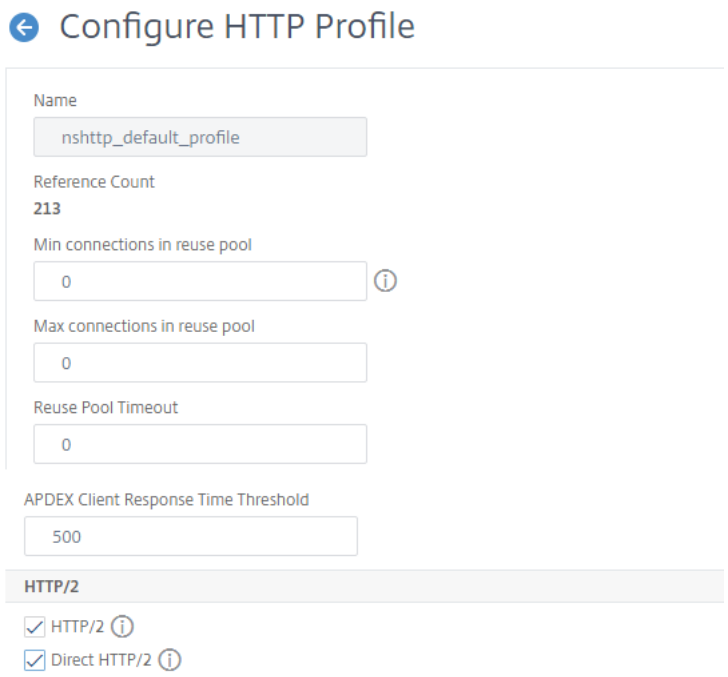
Statuscode der HTTP-Antwort	gRPC-Statuscode
200	OK
400	INTERN = 13
403	ERLAUBNIS_VERWEIGERT = 7
401	NICHT AUTHENTIFIZIERT = 16
429, 502, 503, 504	NICHT VERFÜGBAR = 14
404	NICHT IMPLEMENTIERT = 12

Konfigurieren Sie gRPC Reverse Bridging mithilfe der GUI

Fügen Sie das HTTP-Profil 1 hinzu, wobei HTTP/2 und HTTP/2 Direct für den virtuellen Lastausgleichsserver aktiviert sind

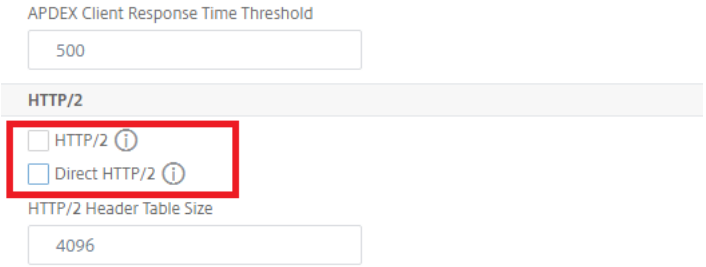
1. Navigieren Sie zu System > Profile und klicken Sie auf HTTP-Profile.

2. Aktivieren Sie die HTTP/2-Option in einem HTTP-Profil 1.



Fügen Sie HTTP-Profil 2 hinzu, wobei HTTP/2 für Back-End-Server deaktiviert ist

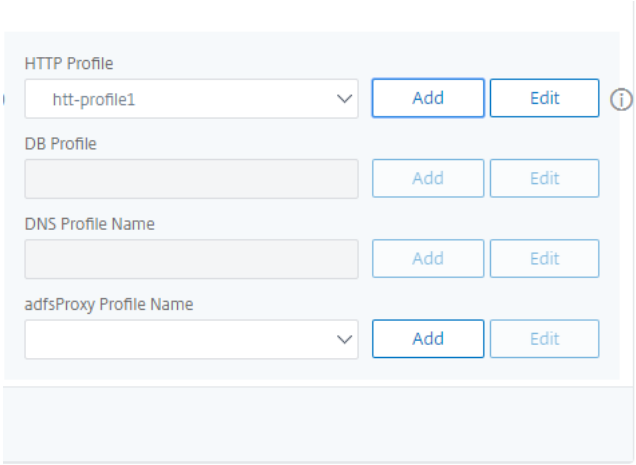
1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Aktivieren Sie die **HTTP/2-Option** in einem HTTP-Profil 2.
3. Klicken Sie auf **OK**.



Fügen Sie einen virtuellen Load-Balancing-Server vom Typ SSL/HTTP hinzu und stellen Sie ihn auf HTTP-Profil 1 ein

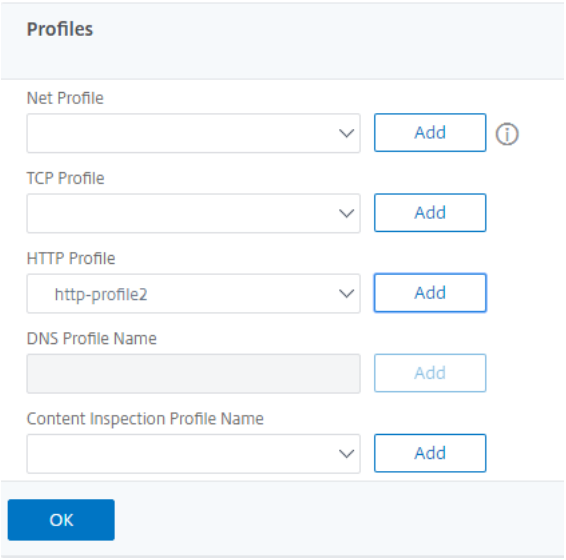
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Verkehr zu erstellen.
3. Klicken Sie auf der Seite **Virtueller Server für Lastenausgleich** auf **Profile**.
4. Wählen Sie im Abschnitt **Profile** den Profiltyp als HTTP aus.

5. Klicke auf **OK** und dann auf **Fertig**.



Dienst mit gRPC-Endpunkt hinzufügen und auf HTTP-Profil 2 setzen

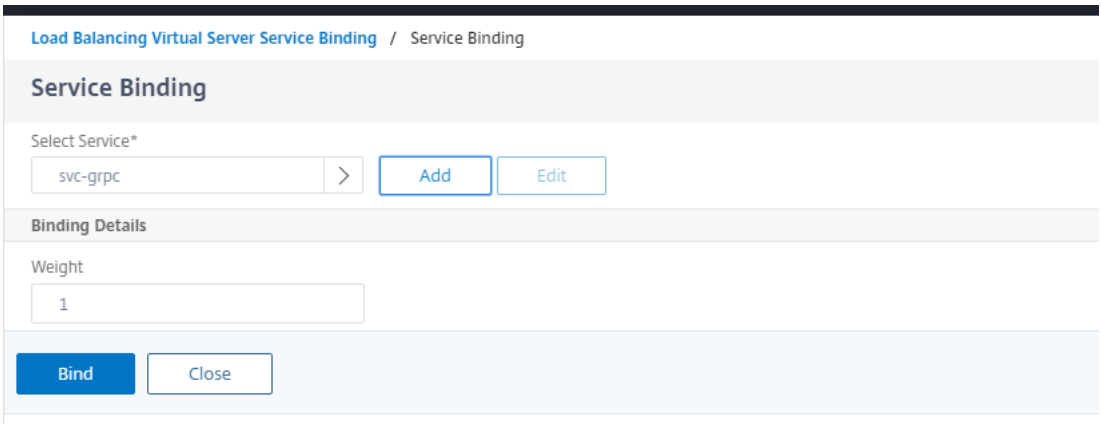
1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie auf **Hinzufügen**, um einen Anwendungsserver für gRPC-Verkehr zu erstellen.
3. Gehen Sie auf der Seite **Load Balancing Service** zum Abschnitt **Profil** .
4. Fügen Sie unter **Profile**das **HTTP-Profil** für den gRPC-Endpunkt hinzu.
5. Klicke auf **OK** und dann auf **Fertig**.



Binden Sie den Dienst für den gRPC-Endpunkt an den virtuellen Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.

2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Verkehr zu erstellen.
3. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf den Abschnitt **Serviceand Service Groups** .
4. Wählen Sie auf der Seite **Load Balancing Virtual Server Service Binding** den gRPC-Dienst aus, den Sie binden möchten.
5. Klicken Sie auf **Schließen** und dann auf **Fertig**.



Ausführliche GUI-Prozeduren finden Sie unter Thema Load Balancing .

Beendigung des gRPC-Anrufs

May 11, 2023

Wenn für eine NetScaler-Appliance Richtlinien wie die Ratenbegrenzung und die Web App Firewall-Sicherheit konfiguriert sind und wenn eine Richtlinie als wahr bewertet wird, kann die Appliance den Anruf beenden und mit einer berechenbaren gRPC-Fehlermeldung an den Client antworten.

gRPC mit Rewrite-Richtlinie

May 11, 2023

Der Anwendungsfall gRPC with Rewrite Policy erklärt, wie die NetScaler-Appliance einige Informationen in den gRPC-Anfragen oder -Antworten umschreibt. Das folgende Diagramm zeigt, wie die Komponenten interagieren.

Das folgende Diagramm zeigt, wie Komponenten in einer gRPC mit Rewrite-Richtlinienkonfiguration miteinander interagieren.

1. Aktivieren Sie die Rewrite-Funktion auf der Appliance.
2. Konfigurieren Sie die Rewrite-Aktion, um gRPC-Header zu ändern, hinzuzufügen oder zu löschen.
3. Konfigurieren Sie die Rewrite-Richtlinie zur Bestimmung der gRPC-Anfragen (Verkehr), bei denen eine Aktion ausgeführt werden muss.
4. Binden Sie die Rewrite-Richtlinie an den virtuellen Load-Balancing-Server, um zu überprüfen, ob der Datenverkehr mit dem Richtlinienausdruck übereinstimmt.
5. Mithilfe einer Rewrite-Richtlinie können Sie auf der Grundlage des gRPC-Statuscodes Folgendes ausführen.
   a) Ändern Sie die Antworten vom gRPC-Webserver.
   b) Ändern, fügen Sie gRPC-Header hinzu oder löschen Sie sie.
   c) Ändern Sie die URL der Anfrage an den gRRC-Server.

Konfigurieren Sie die gRPC-Anrufbeendigung mit der Rewrite-Richtlinie

Um die gRPC-Anrufbeendigung mit der Rewrite-Richtlinie zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Funktion zum Umschreiben aktivieren
2. Hinzufügen einer Rewrite-Richtlinie
3. Binden Sie die Rewrite-Richtlinie an den virtuellen Lastausgleichsserver

Funktion zum Umschreiben aktivieren

Um die Rewrite-Funktion verwenden zu können, müssen Sie sie zuerst aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns rewrite
```


Hinzufügen einer Rewrite-Richtlinie

Nachdem Sie eine Rewrite-Aktion konfiguriert haben, müssen Sie als Nächstes eine Rewrite-Richtlinie konfigurieren, um die gRPC-Anfragen auszuwählen, auf die die NetScaler-Appliance umschreiben muss.

Geben Sie in der Befehlszeile Folgendes ein:

```
add rewrite policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Beispiel:

```
add rewrite policy grpc-rewr_pol1 "http.res.header(\"grpc-status\").NE
(\"0\")"RESET
```

Binden Sie die Rewrite-Richtlinie an den virtuellen Lastausgleichsserver

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie mit dem gRPC-Dienst an den virtuellen Lastausgleichsserver binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Beispiel:

```
bind lb vserver lb-grpc -policyName grpc-rewr_pol1 -priority 100
```

gRPC mit der Responder Policy

May 11, 2023

Die Konfiguration der GrPC mit Responder Policy erklärt, wie eine NetScaler Appliance unterschiedliche Antworten auf GrPC-Anfragen über das HTTP/2-Protokoll liefert. Wenn Benutzer eine Website-Homepage anfordern, möchten Sie möglicherweise eine andere Homepage angeben, je nachdem, wo sich jeder Benutzer befindet oder welcher Browser der Benutzer verwendet.

Das folgende Diagramm zeigt die Komponenten, die interagieren.

1. Aktivieren Sie die Responder-Funktion auf der Appliance.
2. Konfigurieren Sie die Responder-Aktion, um eine benutzerdefinierte Antwort zu generieren, eine Anfrage an eine andere Webseite umzuleiten oder eine Verbindung zurückzusetzen.
3. Konfigurieren Sie die Responder-Richtlinie zur Bestimmung der gRPC-Anfragen (Verkehr), bei denen eine Aktion ausgeführt werden muss.
4. Binden Sie die Responder-Richtlinie an den virtuellen Lastausgleichsserver, um zu prüfen, ob der Datenverkehr mit dem Richtlinienausdruck übereinstimmt.
5. Mithilfe einer Responder Policy können Sie basierend auf dem gPC-Statuscode Folgendes ausführen.

Konfigurieren Sie die GrPC-Anrufbeendigung mit der Responder Policy über die Befehlszeilenschnittstelle

Um die GrPC-Anrufbeendigung mit der Responder-Richtlinie zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie die Responder-Funktion
2. Eine Responder Action hinzufügen
3. Fügen Sie eine Responder Policy hinzu und verknüpfen Sie die Responder Action
4. Binden Sie die Responder Policy an den virtuellen Lastenausgleichsserver

Aktivieren Sie die Responder-Funktion

Um die Responder-Funktion verwenden zu können, müssen Sie sie zuerst aktivieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns responder
```

Fügen Sie die Responder Action hinzu

Nachdem Sie die Funktion aktiviert haben, müssen Sie die Responder-Aktion für die Verarbeitung der gRPC-Antwort basierend auf dem vom Back-End-Server zurückgegebenen Statuscode konfigurieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add responder action <name> <type>
```

Beispiel:

```
add responder action grpc-act respondwith "HTTP/1.1 200 OK\r\nServer: NS
-Responder\r\nContent-Type:application/grpc\r\ngrpc-status: 12\r\ngrpc
-message: Not Implemented\r\n\r\n"+ "Method: "+ HTTP.REQ.URL+ "is not
implemented."
```

Responder-Richtlinie hinzufügen

Nachdem Sie eine Responder-Aktion konfiguriert haben, müssen Sie als Nächstes eine Responder-Richtlinie konfigurieren, um die gRPC-Anfrage auszuwählen, auf die die NetScaler-Appliance antworten muss.

Geben Sie in der Befehlszeile Folgendes ein:

```
add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Beispiel:

```
add responder policy grpc-resp-pol1 HTTP.REQ.URL.NE( “/helloworld.Greeter/
SayHello” )grpc-act
```

Binden Sie die Responder-Richtlinie an den virtuellen Load-Balancing-Server

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie mit dem gRPC-Dienst an den virtuellen Lastausgleichsserver binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind responder global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Beispiel:

```
bind lb vserver lb-grpc svc-grpc -policyName grpc-resp-pol1 -priority 100
```

Weitere Informationen zur Responder Policy finden Sie unter Thema Responder-Richtlinie .

Richtlinienausdrücke zum Abgleichen von GrPC-Protokollpufferfeldern

Die NetScaler Appliance unterstützt die folgenden Richtlinienausdrücke in der grPC-Konfiguration:

- **Zugriff auf den GrPC-Protokollpuffer.** Der willkürliche gRPC-API-Aufruf stimmt mit der Nummer des Nachrichtenfelds mit den neuen Richtlinienausdrücken überein. In einer PI-Konfiguration werden die Übereinstimmungen nur mit den “Feldnummern” und “API-Pfad” durchgeführt.
- **GrPC-Header-Filterung.** Die “HttpProfile” -Parameter für grPC werden verwendet, um das Standardverhalten des GrPC-Parsens (einschließlich GrPC-Richtlinienausdrücken) anzupassen. Die folgenden Parameter gelten für GrPC-Richtlinienausdrücke:
  - **gRPCLengthDelimitation.** Es ist standardmäßig aktiviert und erwartet, dass die Protokollpuffer mit einer längengetrennten Nachricht angezeigt werden.
  - **gRPCHoldLimit.** Der Standardwert ist 131072. Es ist die maximale Größe der Protokollpuffernachricht in Byte. Es ist auch die maximale Stringlänge und die maximale “Byte” -Feldlänge.

Konfigurieren Sie GrPC Advance Policy Ausdrücke mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED ) -
    gRPCLengthDelimitation ( ENABLED | DISABLED ) -gRPCHoldLimit <int>
```

Beispiel:

```
set ns httpProfile http2gRPC -http2 ENABLED -gRPCLengthDelimitation
    ENABLED -gRPCHoldLimit 131072
```

Konfigurieren Sie GrPC-Header-Filterparameter mit der GUI

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Scrollen Sie auf der Seite “ **HTTP-Profil erstellen** “ nach unten zum Abschnitt **HTTP/3** und wählen Sie **GrPC Length Delimitation**aus.

Das folgende Beispiel für einen Richtlinienausdruck zeigt einen Wert in Nachricht 5, Unternachricht 4 und Feld 3. Es ist ein 32-Bit-Int gleich 2.

```
http.req.body(1000).grpc.message(5).message(4).int32(3).eq(2)
```

Die folgenden Richtlinienausdrücke werden hinzugefügt, um die Nachrichtenfelder des GRPC-Protokollpuffers nach Zahlen abzugleichen:

- message
- double

- float
- int32
- int64
- uint32
- uint64
- sint64
- sint32
- fixed32
- fixed64
- sfixed32
- sfixed64
- bool
- string
- enum
- Bytes

API-Pfadabgleich

Der API-Pfadabgleich wird verwendet, um dem korrekten gRPC-API-Aufruf zu entsprechen, wenn mehr als eine API verwendet wird. Stimmen Sie dem API-Pfad überein, der im Pseudo-Header ': path' in der HTTP-Anfrage zu finden ist.

Beispiel:

```
http.req.header(":path").eq("acme.inventory.v1/ListBooks")
```

GrPC Health Check Monitor

June 19, 2023

Der gRPC Integritätsmonitor prüft die gRPC Server auf ihren Integritätsstatus. Der gRPC Integritätsmonitor überprüft den allgemeinen Zustand des gRPC Dienstes oder den Zustand eines bestimmten Dienstes. Derzeit unterstützt die NetScaler Appliance nur die Prüfmethode.

In der NetScaler Appliance wird der Integritätsprüfmonitor konfiguriert, indem die gRPC-Parameter wie gRPCHealthCheck gRPCStatusCode, gRPCServiceName und httprequest in der HTTP2-Monitorkonfiguration festgelegt werden. Ein Client, der das Protokoll implementiert, fragt den Server nach seinem Status ab (fehlerfrei, unbekannt oder Dienst nicht implementiert) und erwartet die Statusantwort vom Dienst.

Die folgende Tabelle enthält Einzelheiten zu den neuen gRPC Parametern und ihrer Beschreibung:

grPC-Parameter	Wert	Beschreibung
gRPCHealthCheck	ja/nein	Aktivieren oder Deaktivieren der gRPC-Integritätsprüfung.
gRPCStatusCode	int ohne Vorzeichen (0-65535), Standardwert: 12	Konfigurieren Sie bis zu 16 grPC-Statuscode. Die Appliance sucht in der Statusantwort nach dem Statuscode 0. Wenn er 0 nicht empfängt, kann der Dienst einrichten, ob einer der 16 Codes mit dem Dienststatus übereinstimmt.
gRPCServiceName	Dienstname in doppelten Anführungszeichen, Default = “” (leere Zeichenfolge)	Prüfen Sie den Zustand des jeweiligen Dienstes.

Konfigurieren Sie den grPC-Integritätsmonitor in HTTP/2 mithilfe der Befehlsschnittstelle

Um eine gRPC Integritätsprüfung durchzuführen, müssen Sie den Zustandsprüfdienst aktivieren, den gRPC Statuscode konfigurieren und den gRPC Dienstnamen angeben, für den die gRPC Integritätsprüfung durchgeführt werden muss. Geben Sie in der Befehlszeile Folgendes ein:

```
add lb monitor <monitor_name> HTTP2 -httpRequest <string> -grpcHealthCheck
( YES | NO )- grpcStatusCode <positive_integer> - grpcServiceName string>]
```

Beispiel:

```
add lb monitor http2 HTTP2 -httprequest  “POST /grpc.health.v1.Health/Check”
 - gRPCHealthCheck Yes -gRPCStatusCode 0 -grpcServiceName "ECHO"
```

Konfigurieren des gRPC-Integritätsmonitors in HTTP/2 mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Klicken Sie auf **Hinzufügen**.
3. Legen Sie auf der Seite **Monitor erstellen** die folgenden Parameter fest:
   a) Name. Name des gRPC Gesundheitsmonitors.
   b) Typ. Wählen Sie den Diensttyp als HTTP/2 aus.

c) GrPC HealthCheck. Prüfung der gRPC Integritätsprüfung aktivieren.
d) gRPC Statuscode. Der gRPC Dienststatus ist nur dann “UP”, wenn der gRPC Statuscode Null oder der konfigurierte Wert ist. Der Status geht “runter”, wenn der Statuscode ein anderer Wert als Null oder der konfigurierte Wert ist.
e) gRPC Name des Dienstes. Dienst, für den der Gesundheitscheck durchgeführt wird.

4. Erstellen **Erstellen**.

QUIC

May 11, 2023

Quick UDP Internet Protocol (QUIC) ist eine Kombination aus (TCP+TLS+HTTP/2) Protokollen, die auf UDP implementiert sind. Das QUIC-Transportprotokoll führt Multiplexing für die Verbindungen zwischen zwei Endpunkten mit UDP aus. Auch im Vergleich zu anderen Protokollen bietet QUIC eine hohe Leistung in Bezug auf Sicherheit, schnelle Bereitstellung des Datenverkehrs und geringere Latenz.

Eine QUIC-Brücke ist in einer NetScaler Appliance zum Lastenausgleich des QUIC-Datenverkehrs zwischen einem QUIC-Client und einem QUIC-Back-End-Server konfiguriert. Die QUIC-Brücke ermöglicht es Ihnen, dauerhafte QUIC-Verbindungen zwischen Client und Server zu haben, wenn eine NAT-Neubindung oder eine Verbindungsmigration vorliegt. Diese Konfiguration verarbeitet jedoch keine Daten. Es wird nur für den Lastenausgleich des QUIC-Datenverkehrs über die NetScaler Appliance verwendet.

QUIC-Pakete enthalten eine Verbindungs-ID, damit Endpoints die Pakete mit einer anderen Adresse oder 4-Tupel derselben Verbindung verknüpfen können. Die Verbindungs-ID enthält die Details der Server-ID, die für die NetScaler Appliance und die Back-End-Server freigegeben werden. Die NetScaler Appliance extrahiert die Verbindungs-ID-Details der Server-ID und sendet den Datenverkehr zurück an den Back-End-Server. Die Verbindungs-IDs befinden sich in geschützten Paketen, die die Verbindungen im Falle einer Verbindungsmigration robust machen.

> **Wichtig**
>
> Die Back-End-Server müssen Unterstützung haben, um die Server-ID in QUIC-Verbindungs-ID zu codieren.

Vorteile der QUIC-Brücke

Die QUIC-Brücke für die NetScaler Appliance wird aus folgenden Gründen bevorzugt:

- Keine teuren Kryptooperationen.
- Zustandsloses Routing ist möglich (kein 4-Tupel-basierter Lastenausgleich).

Crypto-Offload-Unterstützung für QUIC

Wenn eine NetScaler Appliance mit den SSL-Hardwarechips ausgestattet ist, führt sie die Kryptobeschleunigung transparent durch und beschleunigt QUIC-Transaktionen. Diese Beschleunigung erfolgt durch die Verlagerung der Kryptoverarbeitung von der Software auf die Hardware. Für diese Unterstützung ist keine explizite Konfiguration erforderlich. Die Beschleunigung von QUIC-Transaktionen wird in den NetScaler Appliances mit `Intel Coleto`-Hardware unterstützt.

QUIC-Bridge-Konfiguration

June 19, 2023

Um die QUIC-Brücke zu konfigurieren, müssen Sie Folgendes ausfüllen:

- QUIC-Bridge-Profil hinzufügen
- QUIC-Backend-Server hinzufügen
- QUIC-Dienst auf der Appliance hinzufügen
- Fügen Sie einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge hinzu
- Binden Sie QUIC-Brücke an einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge

> **Wichtig**
>
> Bevor Sie die QUIC-Brücke konfigurieren, stellen Sie sicher, dass Sie zuerst die Lastenausgleichsfunktion auf der Appliance aktivieren. Weitere Informationen finden Sie unter Einrichten des einfachen Lastenausgleichs.

Konfigurieren Sie die QUIC-Brücke mit der CLI

Die folgenden Abschnitte müssen über die Befehlszeilenschnittstelle konfiguriert werden.

Fügen Sie ein QUIC-Bridge-Profil hinzu

Fügen Sie ein QUIC-Brückenprofil hinzu.

Geben Sie in der Befehlszeile Folgendes ein:

```
add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
    serveridlen <value>
```

Beispiel:

```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```


> **Hinweis**
>
> Der im Beispiel konfigurierte `serveridlen` Parameter ist die Länge einer benutzerdefinierten Server-ID, die die Hexadezimalzeichenfolge von IP und PORT ist.

QUIC-Back-End-Anwendungsserver hinzufügen

Fügen Sie QUIC-Back-End-Anwendungsserver hinzu.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 -  add server <name> (<IPAddress>)
2 -  add server <name> (<IPAddress>)
```

Beispiel:

```
1 -  add server s1 192.0.2.20
2 -  add server s2 192.0.2.30
```

QUIC Bridge-Dienst hinzufügen

Sie müssen den Anwendungsservern den QUIC-Bridge-Dienst hinzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 -  add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
     CustomServerID <string>]
2
3 -  add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
     CustomServerID <string>]
```

Beispiel:

```
1 -  add service src1 s1 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A8026401BB
2
3 -  add service src2 s2 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A802C801BB
```

> **Hinweis**
>
> Die im vorhergehenden Beispiel konfigurierten `CustomServerID` Parameter sind die Hexadezimalzeichenfolge einer entsprechenden IP und der PORT des Servers (s1 und s2). Für das QUIC-Bridge-Feature empfiehlt Citrix, den `CustomServerID` Parameter nur im Hex-String-Format zu konfigurieren.

Fügen Sie einen virtuellen Load Balancing-Server vom Typ QUIC Bridge hinzu

Sie müssen einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge hinzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
add lb vserver <name> [<IPAddress>@ <port>] [-persistenceType <
    persistenceType >] [-lbMethod < lbMethod >] [-rule <rule>] [-
    cltTimeout <secs>] [-quickBridgeProfilename <name>]
```

Beispiel:

```
add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
    persistenceType CUSTOMSERVERID -lbMethod TOKEN -rule QUIC.
    CONNECTIONID -cltTimeout 120 -quicBridgeProfilename q1
```

> **Hinweis**
>
> Während der Konfiguration des virtuellen QUIC-Bridge-Servers müssen Sie den Parameter `persistenceType` als `CUSTOMSERVERID`, den Parameter `rule` als `QUIC.CONNECTIONID` und den Parameter `LbMethod` als `TOKEN` konfigurieren.

Binden Sie den QUIC Bridge-Dienst an den virtuellen Load Balancing-Server vom Typ QUIC Bridge

Sie müssen den QUIC-Bridge-Dienst an den virtuellen Load Balancing-Server vom Typ QUIC Bridge binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
-  bind lb vserver <name> (<serviceName>)

-  bind lb vserver <name> (<serviceName>)
```

Beispiel:

```
-  bind lb vserver quic_bridge_vip src1

-  bind lb vserver quic_bridge_vip src2
```

Konfigurieren der QUIC-Brücke für Dienstgruppen

Sie können QUIC-Bridge-Funktionen auch für Dienstgruppen konfigurieren. In den folgenden Schritten können Sie die QUIC-Brücke für Dienstgruppen konfigurieren.

Um QUIC Bridge für Dienstgruppen zu konfigurieren, müssen Sie Folgendes ausführen:

QUIC-Bridge-Profil hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
    serveridlen <value>
```

Beispiel:

```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

Server vom Typ QUIC hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
-  add server <name> (<IPAddress>)
-  add server <name> (<IPAddress>)
```

Beispiel:

```
-  add server s1 192.0.2.20
-  add server s2 192.0.2.30
```

QUIC Bridge-Servicegruppe hinzufügen

Geben Sie in der Befehlszeile Folgendes ein:

```
add serviceGroup <serviceGroupName> (<IP> | <serverName>) <serviceType>
```

Beispiel:

```
add serviceGroup svg1 QUIC_BRIDGE
```

Binden Sie die QUIC-Server an die Servicegruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
-  bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
-  bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
```

Beispiel:


```
1 -  bind serviceGroup svg1 s1 443 -customServerID C0A8026401BB
2 -  bind serviceGroup svg1 s2 443 -customServerID C0A802C801BB
```

Fügen Sie einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
      persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
      quickBridgeProfilename <name>]
```

Beispiel:

```
1 add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
      persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
      quicBridgeProfilename q1
```

Binden Sie den virtuellen Load Balancing-Server vom Typ QUIC Bridge an die Dienstgruppe

Geben Sie in der Befehlszeile Folgendes ein:

```
1 bind lb vserver <name>@ (<serviceName>@ <serviceGroupName>
```

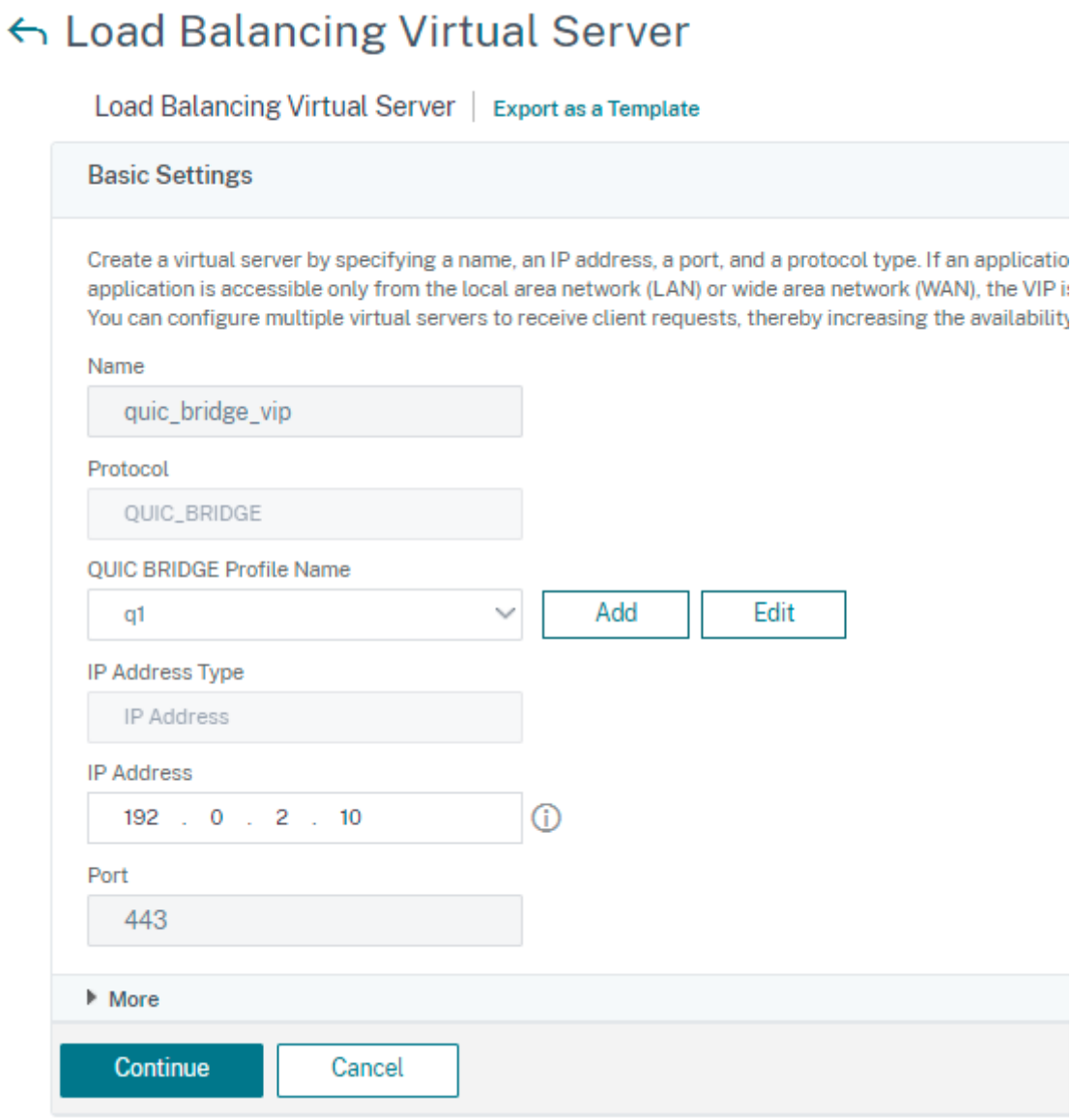
Beispiel:

```
1 bind lb vserver quic_bridge_vip svg1
```

Konfigurieren Sie die QUIC-Brücke mit der GUI

Führen Sie die folgenden Schritte aus, um die QUIC-Brücke über die grafische Benutzeroberfläche zu konfigurieren.

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf der Seite **Virtuelle Server** auf **Hinzufügen**.
3. Wählen Sie auf der Seite **Load Balancing Virtual Server** das Protokoll als QUIC_BRIDGE aus und geben Sie die Details ein. Klicken Sie auf **OK**.

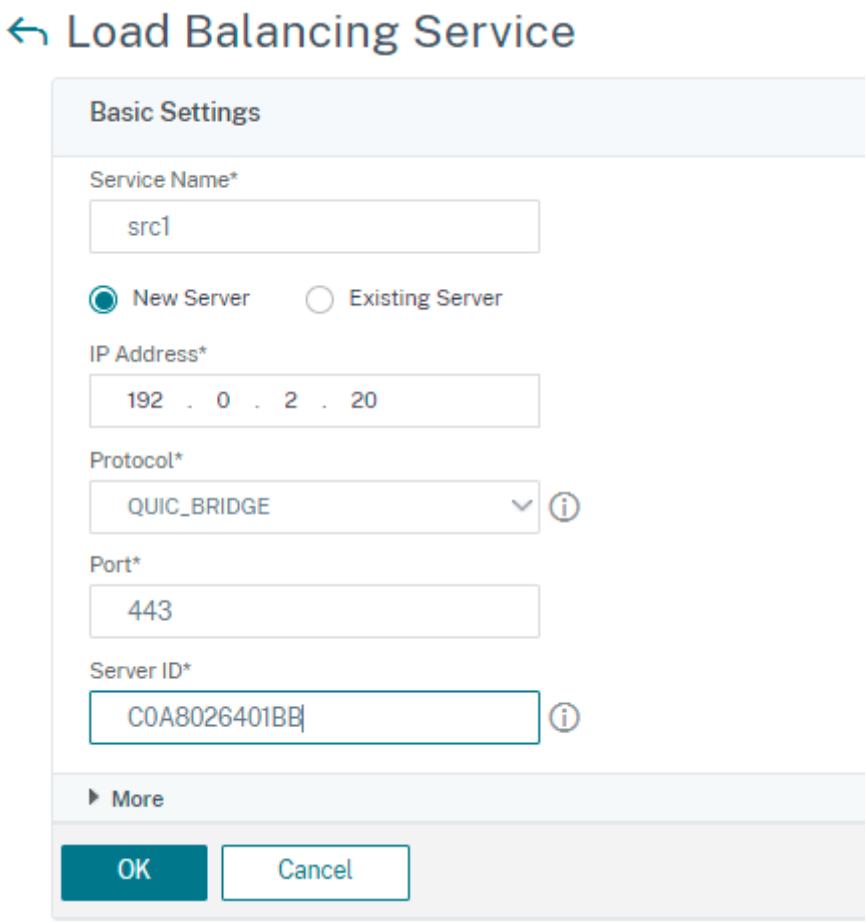


4. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf **Weiter** und **Fertig**.

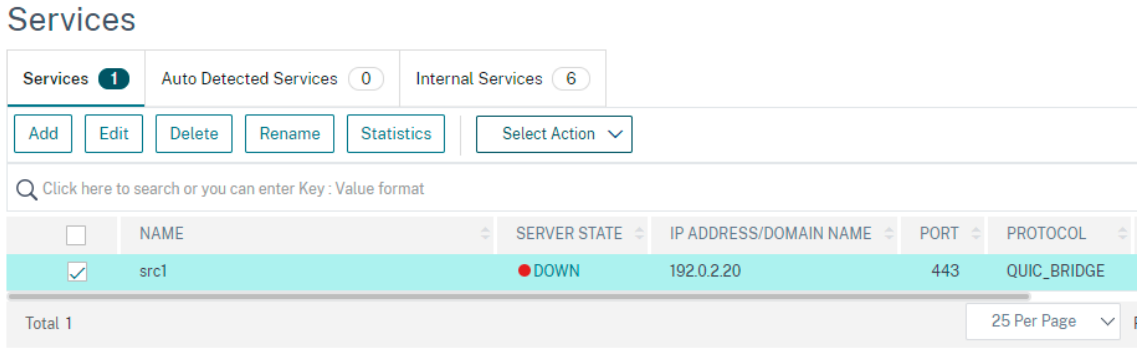
Konfigurieren Sie den Lastenausgleich für die Dienste über die grafische Benutzeroberfläche

Führen Sie die folgenden Schritte aus, um den Lastenausgleich für die Dienste über die grafische Benutzeroberfläche zu konfigurieren.

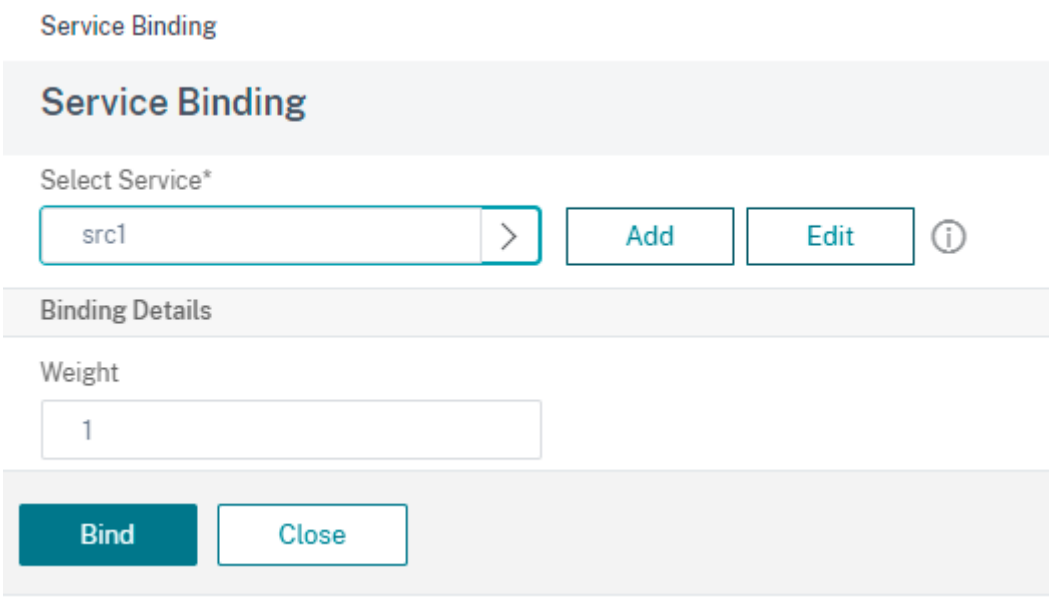
1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**. Klicken Sie auf der Seite **Dienste** auf **Hinzufügen**.
2. Geben Sie auf der Seite **Load Balancing Service** die Details ein und klicken Sie auf **OK**.



3. Wählen Sie auf der Seite **Virtuelle Server** den erstellten virtuellen Server aus, um den Dienst zu binden.
4. Scrollen Sie auf der Seite **Load Balancing Virtual Server** nach unten und wählen Sie die **Dienste und Dienstgruppen**aus.
5. Klicken Sie im Bildschirm **Dienstbindung** auf Feld **Service auswählen** .
6. Wählen Sie im Bildschirm **Dienst den Dienst** aus, der an den virtuellen Lastenausgleichsserver gebunden werden soll, und klicken Sie auf **Auswählen**.



7. Der src1-Dienst ist ausgewählt und klicken Sie im Bildschirm **Dienstbindung** auf **Binden**.



8. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf **Fertig**.

Statistiken für QUIC bridge anzeigen

QUIC-Brücke unterstützt Statistikbefehle, um eine detaillierte Zusammenfassung der QUIC-Brückenstatistiken anzuzeigen.

Die folgenden Befehle zeigen eine ausführliche Zusammenfassung der QUIC-Bridge-Statistiken. Geben Sie an der Eingabeaufforderung Folgendes ein:

- `stat quicbridge`
- `stat quicbridge -detail`

Um die Statistikanzeige zu löschen, geben Sie eine der folgenden Optionen ein:

- `stat quicbridge -clearstats basic`
- `stat quicbridge -clearstats full`

Zeigen Sie QUIC-Bridge-Statistiken über die GUI an

Führen Sie die folgenden Schritte aus, um QUIC Bridge-Statistiken anzuzeigen.

1. Bewegen Sie auf der Registerkarte **Dashboard** die Maus auf den Abschnitt **Systemübersicht** .
2. Klicken Sie auf **Systemübersicht** und wählen Sie QUIC BRIDGE aus der Dropdownliste aus.

Proxyprotokoll

July 4, 2023

Das Proxyprotokoll transportiert Clientdetails sicher von Client zu Server über NetScaler-Appliances. Die Appliance fügt einen Proxyprotokoll-Header mit Clientdetails hinzu und leitet ihn an den Back-End-Server weiter. Im Folgenden sind einige Anwendungsszenarien für das Proxyprotokoll in einer NetScaler-Appliance aufgeführt.

- Ursprüngliche Client-IP-Adresse ermitteln
- Auswählen einer Sprache für eine Website
- Blockieren der Auflistung ausgewählter
- Protokollieren und Sammeln von Statistiken.

Im Folgenden sind die drei Betriebsmodi aufgeführt:

- Einfügen. Die Appliance fügt die Clientdetails ein und sendet sie an den Back-End-Server.
- Vorwärts. Die Appliance leitet die Clientdetails an den Backend-Server weiter.
- Stripped. Die Appliance speichert die Clientdetails zu Protokollzwecken. Wenn das Proxyprotokoll auf dem Back-End-Server nicht unterstützt wird, sendet die Clientdetails mithilfe der Konfiguration der Rewriterichtlinie an den Server

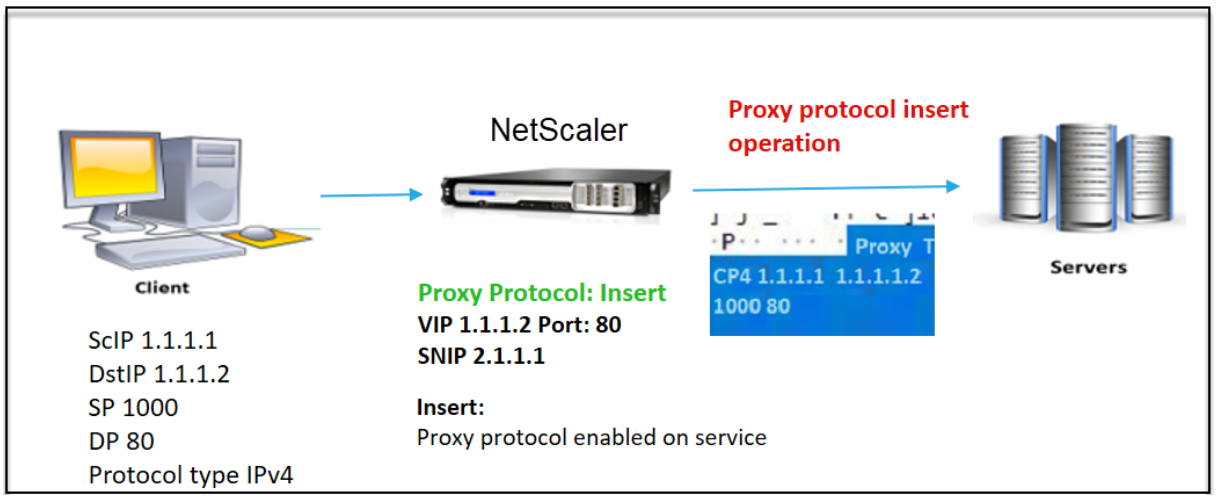
Einschränkungen

Das Proxyprotokoll wird für die TCP Fast Open (TFO) und MultiPath TCP-Funktionen nicht unterstützt. Die Funktion wird nur für Dienste unterstützt, für die die NetScaler-Appliance die TCP-Verbindungsbeendigung vornimmt. Es ist keine Unterstützung für andere Dienste, zum Beispiel “ANY”.

So funktioniert das Proxyprotokoll in einer NetScaler-Appliance

Die folgenden Flussdiagramme zeigen, wie Sie das Proxyprotokoll für NetScaler-Appliances für den Insert-, Forwards- und Stripping-Vorgang konfigurieren können:

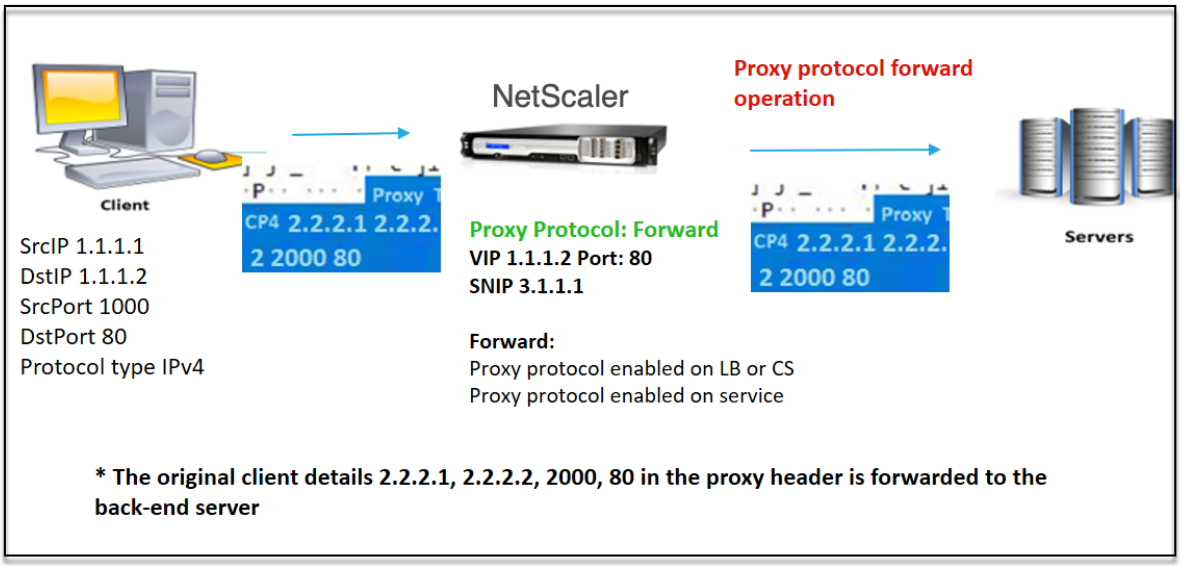
Insert-Vorgang



Die Interaktion der Komponente ist wie folgt:

- Bei der NetScaler-Instanz müssen Sie das Proxyprotokoll im Netzprofil aktivieren und an den Dienst binden.
- Beim Insert-Vorgang fügt NetScaler einen Proxyheader mit Clientverbindungsdetails hinzu und leitet ihn an den Backend-Server weiter.
- Auf der sendenden Seite entscheidet die Appliance die Proxyprotokollversion basierend auf der CLI-Konfiguration.

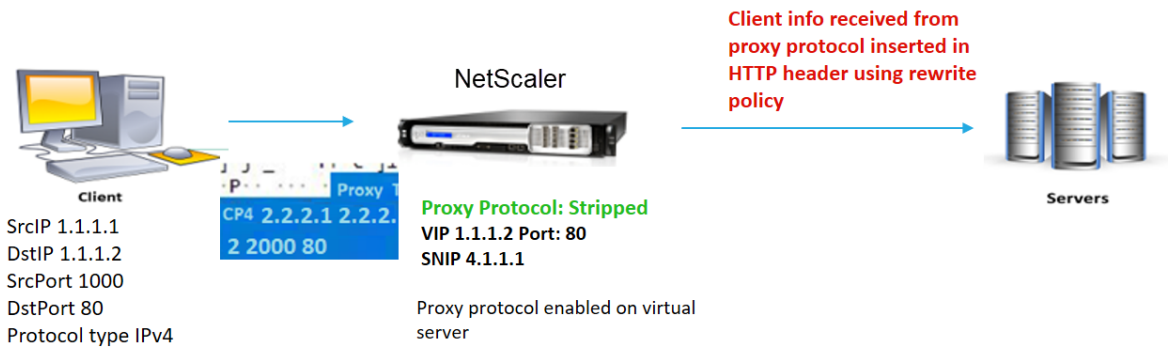
Forward-Vorgang



Die Interaktion der Komponente ist wie folgt:

- Ein Client sendet eine Anfrage zusammen mit dem Proxyheader an den NetScaler. Die Appliance identifiziert die Version dynamisch.
- In der NetScaler-Appliance handelt es sich um einen Forward-Vorgang. Das Proxyprotokoll ist auf dem virtuellen Lastausgleichsserver oder dem virtuellen Content Switching-Server aktiviert und für den Dienst aktiviert. Die Appliance empfängt den Proxyheader und leitet die Header-Details an den Backend-Server weiter.
- Wenn die Details des Proxyheaders ungültig sind, setzt die Appliance die Verbindung zurück.
- Auf der sendenden Seite entscheidet die Appliance die Proxyprotokollversion basierend auf der CLI-Konfiguration.

Stripped-Vorgang



Die Interaktion der Komponente ist wie folgt:

- Ein Client sendet eine Anfrage zusammen mit einem Proxyheader an die NetScaler-Appliance.
- Wenn es sich in der NetScaler-Appliance um einen Stripped-Vorgang handelt, leitet die Appliance die vom Proxyprotokoll erhaltenen Clientinformationen weiter und fügt sie mithilfe von Rewriterichtlinienausdrücken in den HTTP-Header ein.
- Die Clientdetails wie Quell-IP-Adresse, Ziel-IP-Adresse, Quellport und Zielport werden mit Rewriterichtlinienausdrücken in einem HTTP-Header hinzugefügt. Die Rewriterichtlinie wertet den Ausdruck aus und wenn “wahr”, wird die entsprechende Aktion der Rewriterichtlinie ausgelöst. Und die Clientdetails werden in einem HTTP-Header an den Back-End-Server weitergeleitet.
- Wenn die Details des Proxyheaders ungültig sind, setzt die Appliance die Verbindung zurück.

Proxyprotokoll-Versionsformate

Die Proxyprotokollversion ist in zwei Formaten verfügbar. Die Appliance entscheidet, ein Format basierend auf der Länge der eingehenden Daten zu verwenden. Ausführliche Informationen finden Sie unter Proxyprotokoll-RFP .

1. Proxyprotokoll-Version-1-Format

   ```
   PROXY TCP4/TCP6/UNKNOWN <SRC IP> <DST IP> <SRC PORT> <DST PORT>
   ```

   - PROXY -> Eindeutiges Zeichenfolgenformat für Proxyheader-Version -1.
   - Unterstützt Protokolle TCP über IPv4 und TCP über IPv6. Für die verbleibenden Protokolle ist dies UNBEKANNT.
   - SRC-IP — Quell-IP (Ursprüngliche Client-IP) -Adresse eines Pakets.
   - DST IP — Ziel-IP-Adresse eines Pakets.
   - SRC-Port — Quellport eines Pakets.
   - DST-Port — Zielport eines Pakets.

2. Proxyprotokoll-Version-2-Format

   ```
   0D 0A 0D 0A 00 0D 0A 51 55 49 54 0A <13th byte> <14th byte> <15-16th byte> <17th byte onwards>
   ```

   - D 0A 0D 0A 00 0D 0A 51 55 49 54 0A -> Eindeutige binäre Zeichenfolge für Proxyheader-Version -2.
   - Unterstützt Protokolle TCP über IPv4 und TCP über IPv6. Für die verbleibenden Protokolle ist dies UNBEKANNT.
   - Dreizehntes Byte — Protokollversion und Befehl.
   - Vierzehntes Byte — Adresse und Protokollfamilie.
   - 15-16. Byte — Adresslänge in Netzwerkreihenfolge.
   - Siebzehntes Byte ab — Adressiert Informationen, die in der Netzwerkreihenfolge vorhanden sind - src IP, dst IP, src-Port, dst-Port.

Unterstützung von Ausdrücken für Responder-Richtlinien in der Infrastruktur

Das Proxyprotokoll unterstützt die folgenden Infrastrukturausdrücke für Responder-Richtlinien für virtuelle Server vom Typ TCP und HTTP:

1. CLIENT.PROXY.SRCIP_STR
2. CLIENT.PROXY.DSTIP_STR
3. CLIENT.PROXY.SRCPORT
4. CLIENT.PROXY.DSTPORT
5. CLIENT.PROXY.ETHERTYPE

> **Hinweis**
>
> NetScaler unterstützt den Responderrichtlinien-Infrastrukturausdruck für das Proxyprotokoll auf einem virtuellen Server vom Typ TCP ab NetScaler Version 13.1-48.x.

Konfigurieren Sie das Proxyprotokoll in NetScaler-Appliance

Führen Sie die folgenden Schritte aus, um das Proxyprotokoll in Ihrer NetScaler-Appliance zu konfigurieren.

1. Aktivieren Sie das Proxyprotokoll als global.
2. Konfigurieren Sie das Proxyprotokoll für den Insert-Vorgang.
3. Konfigurieren Sie das Proxyprotokoll für den Forward-Vorgang.
4. Konfigurieren Sie das Proxy-Protokoll für den Strip-Betrieb.

Aktivieren Sie das Proxyprotokoll als global

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns param -proxyProtocol ENABLED
```

Konfigurieren Sie das Proxyprotokoll für Insert-

Um das Proxyprotokoll für den Insert-Vorgang zu konfigurieren, müssen Sie das Protokoll auf dem virtuellen Lastausgleichsserver deaktivieren und das Protokoll im Dienst aktivieren.

Hinzufügen eines Netzprofils mit deaktiviertem Proxyprotokoll für den Lastausgleich des virtuellen Servers

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Beispiel:

```
Add netprofile proxyprofile-1 -proxyProtocol DISABLED -proxyprotocoltxversion
 V1
```

> **Hinweis:**
>
> Wenn Sie das Proxyprotokoll auf Ihrer Appliance deaktivieren, müssen Sie den Protokollversion-sparameter nicht festlegen.

Fügen Sie ein Netzprofil mit einem für den Dienst aktivierten Proxyprotokoll hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```


Beispiel:

```
add netprofile proxyprofile-2 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Fügen Sie einen virtuellen Lastausgleichsserver für NetScaler-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Beispiel:

```
add lb vserver lbvserver-1 http 1.1.1.1 80
```

Fügen Sie den HTTP-Dienst für NetScaler-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Beispiel:

```
Add service http-service-1 2.2.2.1 http 80
```

Festlegen des Netzwerkprofils mit dem virtuellen Lastausgleichsserver in der NetScaler-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vserver name> -netprofile <name>
```

Beispiel:

```
set lb vserver lbvserver-1 -netprofile proxyProfile-1
```

Festlegen des Netzwerkprofils mit dem HTTP-Dienst in der NetScaler-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <service name> -netprofile <name>
```

Beispiel:

```
set service http-service-1 -netprofile proxyProfile-2
```


Binden Sie den virtuellen Lastausgleichsserver an den Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <vserver name> <service name>
```

Beispiel:

```
bind lb vserver lbvserver-1 http-service-1
```

Proxyprotokoll für Forward-Vorgang konfigurieren

Um das Proxyprotokoll für den Forward-Betrieb für die nächste NetScaler-Instanz in der Proxyschicht zu konfigurieren, müssen Sie das Protokoll aktivieren und eine Bindung an den virtuellen Server oder Dienst herstellen.

> **Hinweis:**
>
> Das für den virtuellen Lastausgleichsserver erstellte Netzprofil kann auch für den Dienst verwendet werden.

Hinzufügen eines Netzprofils mit aktiviertem Proxyprotokoll für den Lastausgleich des virtuellen Servers

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Beispiel:

```
add netprofile proxyprofile-3 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Netzprofil mit aktiviertem Proxyprotokoll für den Dienst hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Beispiel:

```
add netprofile proxyprofile-4 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```


Fügen Sie einen virtuellen Lastausgleichsserver für NetScaler-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Beispiel:

```
add lb vserver lbvserver-2 http 2.2.2.2 80
```

Fügen Sie den HTTP-Dienst für NetScaler-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Beispiel:

```
Add service http-service-2 3.3.3.1 http 80
```

Festlegen des Netzwerkprofils mit dem virtuellen Lastausgleichsserver in der NetScaler-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vserver name> -netprofile <name>
```

Beispiel:

```
set lb vserver lbvserver-2 -netprofile proxyProfile-3
```

Festlegen des Netzwerkprofils mit dem HTTP-Dienst in der NetScaler-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <service name> -netprofile <name>
```

Beispiel:

```
set service http-service-2 -netprofile proxyProfile-4
```

Binden Sie den virtuellen Lastausgleichsserver an den Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <vserver name> <service name>
```

Beispiel:

```
bind lb vserver lbvserver-2 http-service-2
```


Konfigurieren Sie das Proxyprotokoll für Strip-Betrieb

Um das Proxyprotokoll für den Strip-Betrieb zu konfigurieren, müssen Sie das Proxyprotokoll auf dem virtuellen Lastausgleichsserver aktivieren und das Proxyprotokoll für den Dienst deaktivieren.

Netzprofil mit aktiviertem Proxyprotokoll für virtuellen Server hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED> -proxyprotocoltxversion <V1/
V2>
```

Beispiel:

```
add netprofile proxyprofile-5 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Fügen Sie einen virtuellen Server für Lastenausgleich oder Content Switching für NetScaler-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Beispiel:

```
add lb vserver lbvserver-3 http 2.2.2.2 80
```

Fügen Sie den HTTP-Dienst für NetScaler-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Beispiel:

```
Add service http-service-3 3.3.3.1 http 80
```

Festlegen des Netzprofils mit Lastausgleich oder virtuellem Content Switching-Server in NetScaler-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vserver name> -netprofile <name>
```

Beispiel:

```
set lb vserver lbvserver-3 -netprofile proxyProfile-5
```


Binden Sie den virtuellen Lastausgleichsserver an den Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <vserver name> <service name>
```

Beispiel:

```
bind lb vserver lbvserver-3 http-service-3
```

Konfigurieren Sie den Infrastrukturausdruck der Responderrichtlinie für das Proxyprotokoll mithilfe der CLI

Um eine Responder-Richtlinie zu konfigurieren, geben Sie an der Befehlszeile Folgendes ein:

```
add responder policy <name> <expression> <action>
```

Beispiel:

```
> add responder policy resppol_proxy_srcip "CLIENT.PROXY.SRCIP_STR.EQ("
    10.106.26.83")" RESET
Done
<!--NeedCopy-->
```

Um die Responder-Richtlinie an den virtuellen Load Balancing-Server zu binden, geben Sie an der Befehlszeile Folgendes ein:

```
bind lb vserver <name> -policyname <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type <type>
```

Beispiel:

```
> bind lb vserver lb_tcp1 -policyName resppol_proxy_srcip -priority 10
    -gotoPriorityExpression END -type REQUEST
Done
<!--NeedCopy-->
```

Beispiel für eine End-to-End-Konfiguration

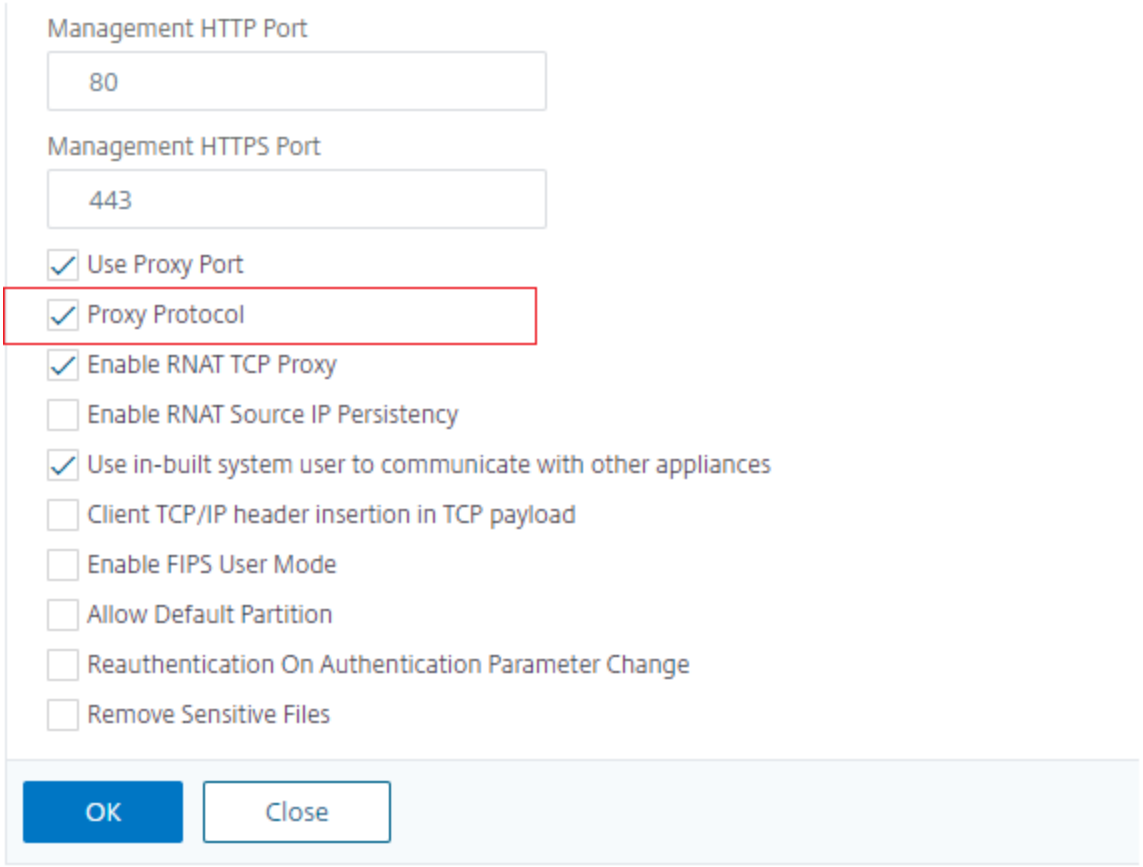
```
> add ns tcpProfile tcp-proxy-profile -tcpmode ENDPOINT

> add netprofile net_proxyv1 -MBF DISABLED -proxyProtocol
ENABLED

> enable ns mode l2

> enable ns mode l3 usnip
```



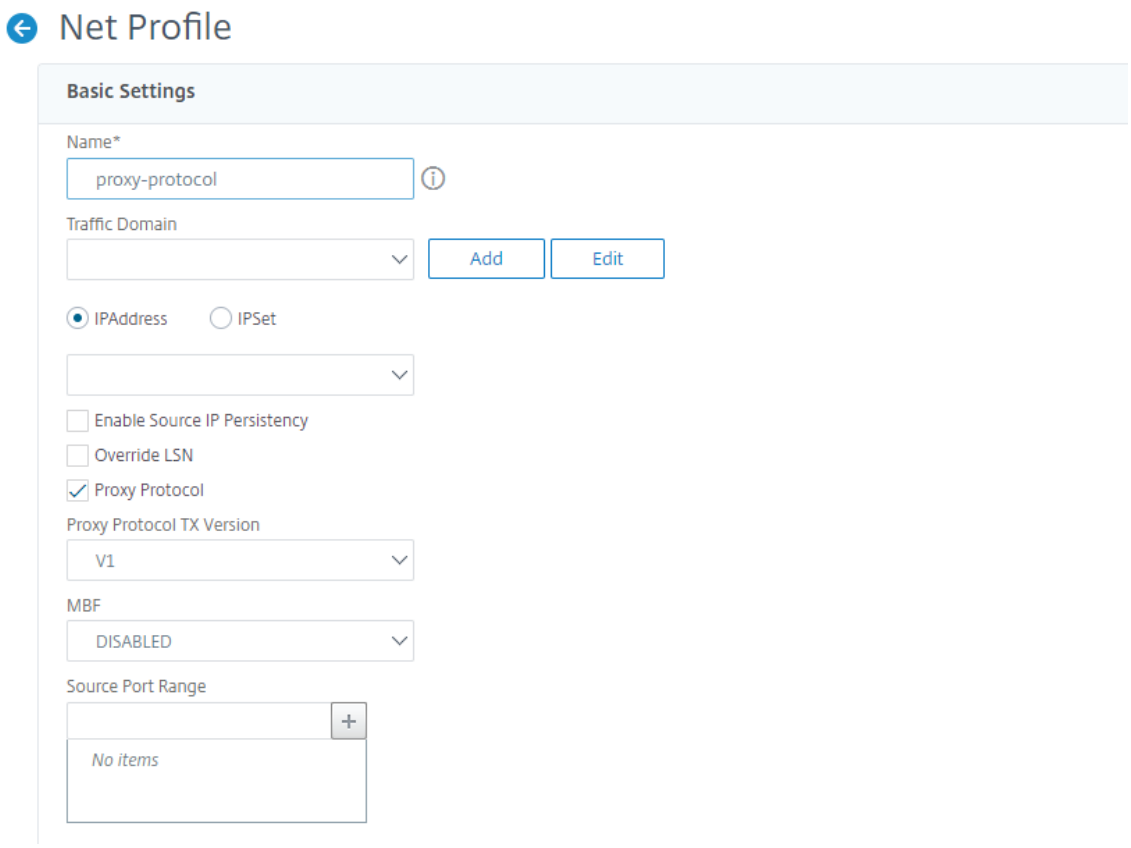
```
9
10 > add ns ip 10.106.26.146 255.255.255.0 -type SNIP
11 Done
12 > add ns ip 10.106.26.144 255.255.255.0 -type SNIP
13 Done
14
15 > add lb vserver lb_tcp1 TCP 10.106.26.141 80
16 > add service s1 10.106.26.82 TCP 8080
17
18 > bind lb vserver lb_tcp1 s1
19
20 > set lb vserver lb_tcp1 -tcpProfileName tcp_proxy -netProfile
      net_proxyv1
21
22 > set ns param -proxyProtocol ENABLED
23
24 > add responder policy resppol_proxy_srcip "CLIENT.PROXY.SRCIP_STR.EQ("
      10.106.26.83")" RESET
25
26 > bind lb vserver lb_tcp1 -policyName resppol_proxy_srcip -priority 10
      -gotoPriorityExpression END -type REQUEST
27 Done
28 <!--NeedCopy-->
```

Konfigurieren des Proxyprotokolls über die NetScaler GUI

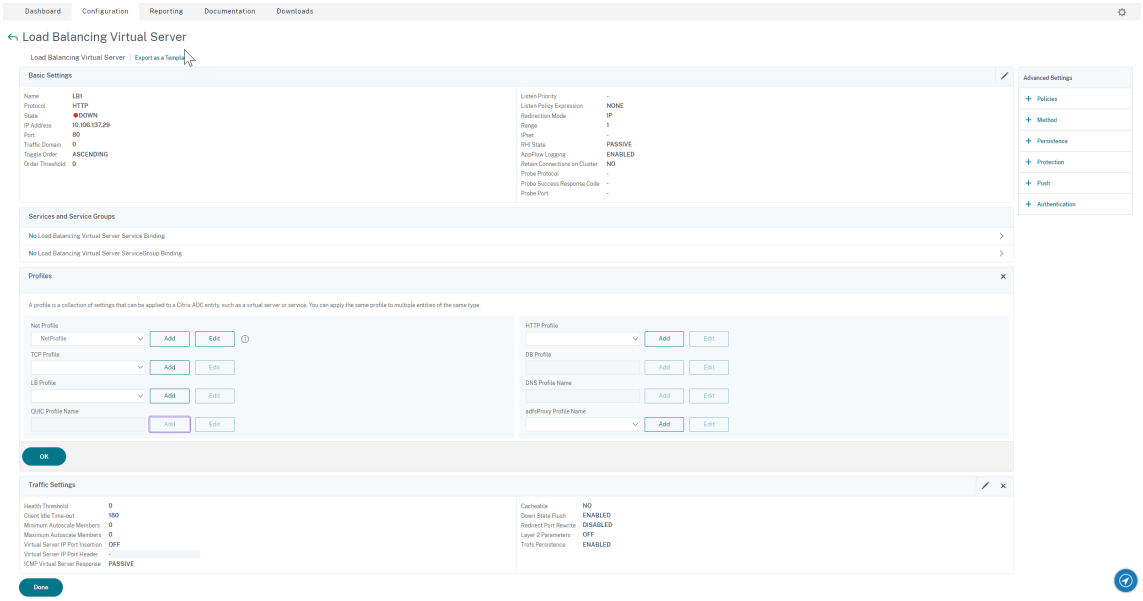
1. Navigieren Sie zu **System** > **Einstellungen** > **Globale Systemeinstellungen ändern**.
2. **Aktivieren Sie auf der Seite “Parameter für globale Systemeinstellungen konfigurieren** “ das Kontrollkästchen **Proxyprotokoll** .
3. Klicken Sie auf **OK** und auf **Schließen**.



4. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile**.
5. Klicken Sie im Detailbereich auf **Hinzufügen**, um ein Netzprofil für den virtuellen Lastausgleichsserver zu erstellen.
6. Legen Sie auf der Seite **Net Profile** die folgenden Parameter fest:
   a) **Name** : Name des Netzprofils.
   b) **Proxy-Protokoll**: Aktivieren oder deaktivieren Sie das Proxy-Protokoll für den virtuellen Lastausgleichsserver.
   c) **Proxy-Protokoll-TX-Version**: Stellen Sie die Proxy-Protokollversion auf V1 oder V2 ein, basierend auf dem Format der eingehenden Daten.
7. Klicken Sie auf **OK**.

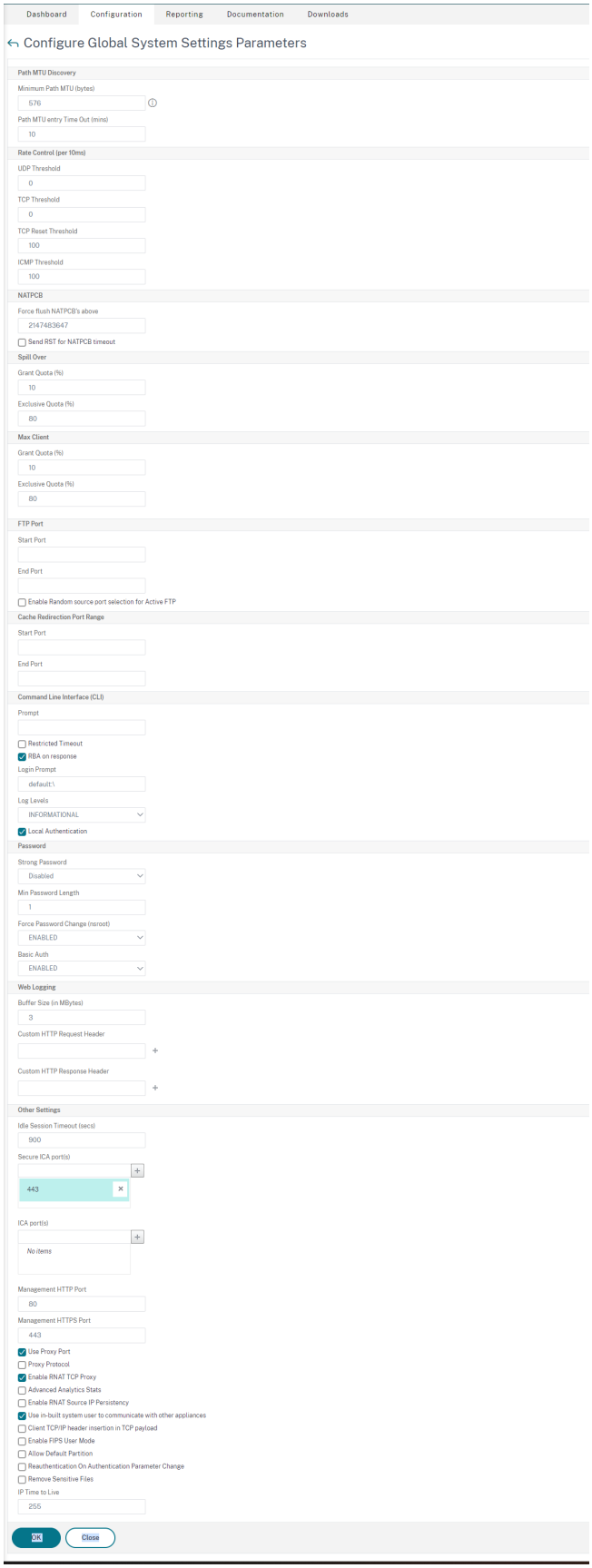


8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
9. Klicken Sie im Detailbereich auf **Hinzufügen**.
10. Legen Sie auf der Seite **Load Balancing Virtual Server** die grundlegenden Parameter fest.
11. Wählen Sie im Abschnitt **Erweiterte Einstellungen** die Option **Profile**aus.
12. Klicken Sie im Abschnitt **Profile** auf das Stiftsymbol.
13. Wählen Sie ein Netzprofil aus und klicken Sie auf **OK**.
14. Klicken Sie auf **Fertig**.



15. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
16. Klicken Sie im Detailbereich auf **Hinzufügen**.
17. Legen Sie auf der Seite **Load Balancing Service** die grundlegenden Parameter fest.
18. Wählen Sie im Abschnitt **Erweiterte Einstellungen** die Option **Profile**aus.
19. Klicken Sie im Abschnitt **Profile** auf das Stiftsymbol.
20. Wählen Sie ein Netzprofil aus und klicken Sie auf **OK**.
21. Klicken Sie auf **Fertig**.

> **Hinweis:**
>
> Wenn Sie mehr als eine NetScaler-Appliance als Teil der Proxy-Schicht haben, müssen Sie die Proxyprotokollkonfiguration auf jeder Appliance für den Forward-Vorgang festlegen.



Client-IP-Adresse in TCP-Option

May 11, 2023

Die NetScaler Appliance verwendet viele Möglichkeiten, um die Clientinformationen an den Back-End-Server zu senden. Eine solche Methode besteht darin, die Client-IP-Adresse in der TCP-Option zu senden. Die Appliance verwendet die TCP-Optionsnummer im TCP-Profil, wenn der Back-End-Server die TCP-Option zum Lesen der Client-IP-Adresse verwendet.

Die NetScaler Appliance sendet die Client-IP-Adresse im TCP-Optionsheader nur in den folgenden Paketen:

- endgültiges ACK-Paket des Dreiwege-Handshakes
- ein erstes Datenpaket.

Im Folgenden sind einige der Nutzungsszenarien für die TCP-Optionskonfiguration in einer NetScaler Appliance aufgeführt.

- Ursprüngliche Client-IP-Adresse ermitteln
- Auswählen einer Sprache für eine Website
- Blockieren der Auflistung der ausgewählten IP-Adressen

Im Folgenden sind die beiden Betriebsmodi zum Senden der Client-IP-Adresse in der TCP-Option aufgeführt:

- **Einfügen**. Im Einfügemodus fügt die Appliance die Clientdetails im Feld TCP-Option 28 (konfigurierbar, aber der bevorzugte Wert ist 28) hinzu und sendet sie an den Back-End-Server.
- **Vorwärts**. Im Vorwärtsmodus empfängt der virtuelle Server die Client-IP-Details in der TCP-Option von einem Proxygerät. Für den virtuellen Server müssen Sie dieselbe TCP-Option konfigurieren, mit der das Proxygerät die Client-IP-Details gesendet hat.

  Die Appliance sendet dann die Clientdetails im TCP-Optionsfeld an den Back-End-Server. Für den Dienst, der den Back-End-Server darstellt, können Sie jede TCP-Option festlegen, aber der bevorzugte Wert ist 28.

Die NetScaler Appliance unterstützt auch das Senden des Clientports in der TCP-Option für die Konfiguration des Einfügemodus.

> **Hinweise:**
>
> - Multiplexing wird für den empfangenen Datenverkehr auf einem virtuellen Server nicht unterstützt, wenn die Client-IP-TCP-Option für das gebundene TCP-Profil aktiviert ist.
> - Für einen virtuellen TCP- oder HTTP-Server wird die TCP-Optionsnummer mit oder ohne aktivierte Funktion im transparenten Modus weitergeleitet.

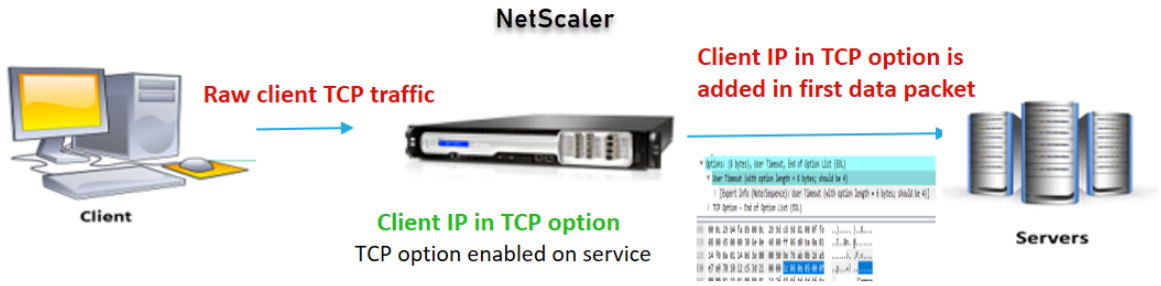
Einschränkungen

Die TCP-Optionskonfigurationsfunktion wird in TFO-, MultiPath-TCP- und HTTP2-Funktionen nicht unterstützt.

Wie die TCP-Optionskonfiguration in einer NetScaler Appliance

Die folgenden Flussdiagramme zeigen, wie Sie die TCP-Option in den NetScaler Appliances für Einfüge- und Weiterleitungsvorgänge konfigurieren können.

Vorgang einsetzen:

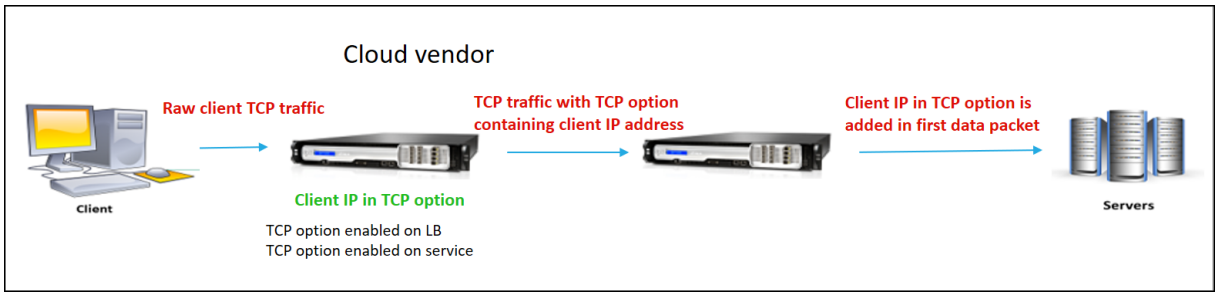


Die Interaktion der Komponente ist wie folgt:

- Ein Client sendet eine Anfrage an NetScaler.
- Im Einfügevorgang fügt die NetScaler Appliance die Client-IP-Adresse und den Port in die konfigurierte TCP-Option der folgenden Pakete in den Back-End-Server ein.
  - endgültiges ACK-Paket des Dreiwege-Handshakes
  - erstes Datenpaket

> **Hinweis:**
>
> Wenn der eingehende Datenverkehr HTTPS ist, werden die Client-IP-Adresse und der Client-Port in der TCP-Option in der SSL-Client-Hello-Nachricht gesendet, bei der es sich um das erste Datenpaket auf TCP-Ebene handelt.

Vorwärtsbetrieb:



Die Interaktion der Komponente ist wie folgt:

- Ein Client sendet eine HTTP/HTTPS-Anforderung an die NetScaler Appliance.
- Für den Weiterleitungsvorgang ist die TCP-Option auf einem virtuellen Lastausgleichsserver oder einem virtuellen Content Switching-Server aktiviert und auch im Dienst aktiviert. Die Appliance erhält die Clientdetails in der TCP-Optionsnummer, die im virtuellen Server angegeben ist.
- Die NetScaler Appliance fügt dann die Client-IP-Adresse und den Port in die konfigurierte TCP-Option (für den Dienst) der folgenden Pakete in den Back-End-Server ein.
  - endgültiges ACK-Paket des Dreiwege-Handshakes
  - erstes Datenpaket

Konfigurieren der TCP-Option für den Insert-Vorgang

Das Konfigurieren der TCP-Option für den Insert-Vorgang umfasst die folgenden Schritte:

1. Konfigurieren Sie ein TCP-Profil. Aktivieren Sie die Client-IP-TCP-Option (`clientIpTcpOption`), und geben Sie die TCP-Optionsnummer (`clientIpTcpOptionNumber`) an. Aktivieren Sie optional `sendClientPortInTcpOption`, um den Client-Port im TCP-Optionsheader zu senden.

   > **Hinweis:**
   >
   > Citrix empfiehlt, die TCP-Optionsnummer im TCP-Profil auf 28 zu konfigurieren.

2. Binden Sie das TCP-Profil an einen Dienst

So konfigurieren Sie ein TCP-Profil mit CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- `add tcpprofile <name> -clientIpTcpOption (ENABLED | DISABLED)-clientIpTcpOptionNu <positive_integer> -sendClientPortInTcpOption (ENABLED | DISABLED)`
- `show tcpprofile <name>`

So binden Sie das TCP-Profil über die CLI an den Dienst:

Geben Sie in der Befehlszeile Folgendes ein:

- `set service <name> -tcpprofileName <name>`
- `show service <name>`

Beispiel-Konfiguration

```
1 add tcpprofile TCP-PROFILE-1 -clientIpTcpOption ENABLED -
     clientIpTcpOptionNumber 28 -sendClientPortInTcpOption ENABLED
2 set service SERVICE-1  - tcpprofileName TCP-PROFILE-1
```



```
<!--NeedCopy-->
```

Konfigurieren der TCP-Option für den Vorwärtsbetrieb

Die Konfiguration der TCP-Option für den Vorwärtsbetrieb umfasst die folgenden Schritte:

1. Konfigurieren Sie ein TCP-Profil. Aktivieren Sie die Client-IP-TCP-Option (`clientIpTcpOption`), und geben Sie die TCP-Optionsnummer (`clientIpTcpOptionNumber`) an.
2. Binden des TCP-Profils an einen virtuellen Load Balancing- oder Content Switching Server
3. Binden Sie das TCP-Profil an die Dienste.

So konfigurieren Sie ein TCP-Profil mit CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- `add tcpprofile <name> -clientIpTcpOption (ENABLED | DISABLED)-clientIpTcpOptionNu <positive_integer>`
- `show tcpprofile <name>`

So binden Sie das TCP-Profil über die CLI an einen virtuellen Lastausgleichs- oder Content Switching-Server:

Geben Sie in der Befehlszeile Folgendes ein:

- `set lb vserver <name> -tcpprofileName <name>`
- `show lb vserver <name>`

So binden Sie das TCP-Profil über die CLI an den Dienst:

Geben Sie in der Befehlszeile Folgendes ein:

- `set service <name> -tcpprofileName p1`
- `show service <name>`

Beispiel-Konfiguration

```
add tcpprofile TCP-PROFILE-2 -clientIpTcpOption ENABLED -
    clientIpTcpOptionNumber 29
set lb vserver LBVS-2  - tcpprofileName TCP-PROFILE-2
set service SERVICE-2 -tcpprofileName TCP-PROFILE-2
<!--NeedCopy-->
```

Konfigurieren der TCP-Option mithilfe der NetScaler GUI

1. Navigieren Sie zu **System** > **Profile**.

2. Klicken Sie auf der Registerkarte **TCP-Profil** auf **Hinzufügen**.
3. Konfigurieren Sie auf der Seite **TCP-Profil konfigurieren** die folgenden Parameter:
    - **clientIptcpoption**. Ermöglicht der TCP-Option, Client-IP-Adressen zu senden oder zu empfangen.
    - **clientiptcpoptionnumber**. Legt die TCP-Optionsnummer fest.
    - **sendClientPortInTcpOption** Sendet den Client-Port in der TCP-Option für die Konfiguration des Einfügemodus.
4. Klicken Sie auf **OK** und auf **Schließen**.

SNMP

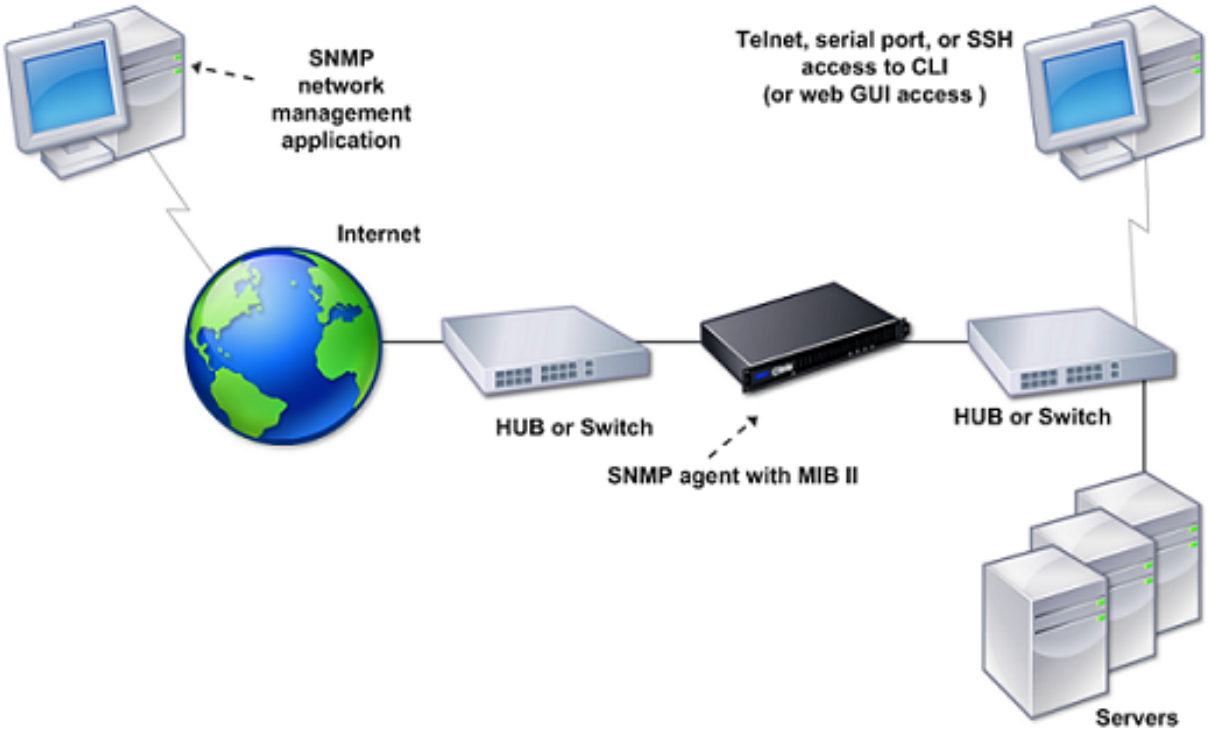
May 11, 2023

Sie können das Simple Network Management Protocol (SNMP) verwenden, um den SNMP-Agenten auf der NetScaler-Appliance so zu konfigurieren, dass er asynchrone Ereignisse generiert, die als Traps bezeichnet werden. Die Traps werden immer dann generiert, wenn auf dem NetScaler ungewöhnliche Bedingungen herrschen. Die Traps werden dann an ein Remote-Gerät gesendet, das als *Trap-Listener* bezeichnet wird, das den anormalen Zustand der NetScaler Appliance signalisiert. *Sie können den SNMP-Agenten auch über ein Remote-Gerät, das als SNMP-Manager bezeichnet wird, nach systemspezifischen Informationen fragen.* Der Agent durchsucht dann die Management Information Base (MIB) nach den angeforderten Daten und sendet die Daten an den SNMP-Manager.

Der SNMP-Agent auf dem NetScaler kann Traps generieren, die mit SNMPv1, SNMPv2 und SNMPv3 kompatibel sind. Für die Abfrage unterstützt der SNMP-Agent SNMP Version 1 (SNMPv1), SNMP Version 2 (SNMPv2) und SNMP Version 3 (SNMPv3).

Informationen zu SNMP-Parametern, Traps und deren Beschreibungen finden Sie unter NetScaler SNMP OID Reference.

Die folgende Abbildung zeigt ein Netzwerk mit einem NetScaler, für das SNMP aktiviert und konfiguriert ist. In der Abbildung verwendet jede SNMP-Netzwerkverwaltungsanwendung SNMP, um mit dem SNMP-Agenten auf dem NetScaler zu kommunizieren. Der SNMP-Agent durchsucht seine Management Information Base (MIB), um die vom SNMP-Manager angeforderten Daten zu sammeln und der Anwendung die Informationen zur Verfügung zu stellen.



> **Wichtig**
>
> Das SNMP-Modul in einer NetScaler Appliance unterstützt eine maximale Länge von 128 Byte (gemäß RFC 3416) für eine SNMP-OID. Ein langer Indexvariablenname für ein Objekt kann dazu führen, dass eine SNMP-OID größer als 128 Byte ist.
>
> Um dieses Problem zu beheben, unterstützt das NetScaler SNMP-Modul eine maximale Länge von 31 Zeichen für einen Indexvariablennamen. Wenn ein Indexvariablenname 31 Zeichen lang ist, konvertiert das SNMP-Modul, das einen Hash-Algorithmus verwendet, den Namen in einen Hashwert von 31 Zeichen. Dieser Hash-Wert wird in der SNMP-OID für diese Variable verwendet.
>
> Der ursprüngliche Name der Indexvariablen wird in einer anderen Variablen gespeichert, die das folgende Namensformat hat: `<variable type>FullName`. Wenn beispielsweise der Name eines virtuellen Lastausgleichsservers mehr als 31 Zeichen enthält, enthält `vserverName` SNMP OID den Hash-Wert und die `vsvrFullName` SNMP-OID enthält den vollständigen (ursprünglichen) Namen des virtuellen Servers.
>
> In ähnlicher Weise zeigt die Indexvariable für SNMP-Traps einen Hash-Wert an. `<variable type>FullName`, der den vollständigen Namen des ursprünglichen Indexvariablennamens speichert, ist ebenfalls Teil der Fallenmeldungen.

Importieren von MIB-Dateien in den SNMP-Manager und Trap-Listener

Um eine NetScaler Appliance zu überwachen, müssen Sie die MIB-Objektdefinitionsdateien herunterladen. Die NetScaler Appliance unterstützt die folgenden unternehmensspezifischen MIBs:

- **Eine Teilmenge von Standard-MIB-2-Gruppen**. Stellt die MIB-2-Gruppen SYSTEM, IF, ICMP, UDP und SNMP bereit.
- **Ein Systemunternehmen MIB**. Bietet systemspezifische Konfiguration und Statistiken.

Sie können die MIB-Objektdefinitionsdateien aus dem Verzeichnis /netscaler/snmp oder über die Registerkarte Downloads der GUI beziehen.

NetScaler zum Generieren von SNMP-Traps konfigurieren

May 11, 2023

Sie können die NetScaler-Appliance konfigurieren, um asynchrone Ereignisse zu generieren, die als *Traps* bezeichnet werden. Die Traps werden immer dann generiert, wenn ungewöhnliche Bedingungen auf der Appliance vorliegen. Die Traps werden an ein Remote-Gerät gesendet, das als *Trap-Listener* bezeichnet wird. Es hilft Administratoren, die Appliance zu überwachen und umgehend auf Probleme zu reagieren.

Die NetScaler Appliance stellt eine Reihe von Zustandsobjekten namens *SNMP-Alarme* bereit. Wenn die Bedingung in einem SNMP-Alarm erfüllt ist, generiert die Appliance SNMP-Trap-Meldungen, die an die konfigurierten Trap-Listener gesendet werden. Wenn beispielsweise der LOGIN-FAILURE-Alarm aktiviert ist, wird bei jedem Anmeldefehler auf der Appliance eine Trap-Meldung generiert und an den Trap-Listener gesendet.

Um die NetScaler Appliance zum Generieren von Traps zu konfigurieren, müssen Sie Alarme aktivieren und konfigurieren. Anschließend geben Sie die Trap-Listener an, an die die Appliance die generierten Trap-Nachrichten sendet.

Aktivieren eines SNMP-Alarms

Die NetScaler-Appliance generiert Traps nur für aktivierte SNMP-Alarme. Einige Alarme sind standardmäßig aktiviert, aber Sie können sie deaktivieren.

Wenn Sie einen SNMP-Alarm aktivieren, generiert die Appliance entsprechende Trap-Meldungen, wenn einige Ereignisse eintreten. Einige Alarme sind standardmäßig aktiviert.

So aktivieren Sie einen SNMP-Alarm mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `enable snmp alarm <trapName>`
- `show snmp alarm <trapName>`

So aktivieren Sie einen SNMP-Alarm mithilfe der GUI

1. Navigieren Sie zu **System > SNMP > Alarme**und wählen Sie den Alarm aus.
2. Klicken Sie auf **Aktionen** und wählen Sie **Aktivieren**

Konfiguration von Alarmen

Die NetScaler Appliance stellt eine Reihe von Zustandsobjekten namens *SNMP-Alarme* bereit. Wenn die für einen SNMP-Alarm festgelegte Bedingung erfüllt ist, generiert die Appliance SNMP-Trap-Meldungen, die an die konfigurierten Trap-Listener gesendet werden. Wenn beispielsweise der LOGIN-FAILURE-Alarm aktiviert ist, wird bei jedem Anmeldefehler auf der Appliance eine Trap-Meldung generiert und an den Trap-Listener gesendet.

Sie können einem SNMP-Alarm einen Schweregrad zuweisen. Wenn Sie dies tun, wird den entsprechenden Trap-Meldungen dieser Schweregrad zugewiesen.

Im Folgenden sind die auf der Appliance definierten Schweregrade in absteigender Reihenfolge des Schweregrads aufgeführt.

- Kritisch
- Hauptfach
- Minor
- Warnung
- Zur Information

Wenn Sie beispielsweise einen Schweregrad der Warnung für den SNMP-Alarm mit dem Namen LOGIN-FAILURE festlegen, werden die Trap-Meldungen, die bei einem Anmeldefehler generiert werden, mit dem Schweregrad der Warnung zugewiesen.

> **Hinweis**
>
> NetScaler unterstützt verschiedene SNMP-Alarme. Weitere Informationen finden Sie unter SNMP-Alarme.

Sie können auch einen SNMP-Alarm konfigurieren, um die entsprechenden Trap-Meldungen zu protokollieren, die generiert werden, wenn die Bedingung für diesen Alarm erfüllt ist.

So konfigurieren Sie einen SNMP-Alarm mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen SNMP-Alarm zu konfigurieren und die Konfiguration zu überprüfen:

- `set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`

- `show snmp alarm <trapName>`

Hierbei gilt:

ThresholdValue: Wert für den hohen Schwellenwert. Die NetScaler Appliance generiert eine SNMP-Trap-Nachricht, wenn der Wert des dem Alarm zugeordneten Attributs größer oder gleich dem angegebenen hohen Schwellenwert ist.

NormalValue: Wert für den normalen Schwellenwert. Eine Trap-Meldung wird generiert, wenn der Wert des jeweiligen Attributs nach Überschreiten des hohen Schwellenwerts auf oder unter diesen Wert fällt.

So konfigurieren Sie SNMP-Alarme mit der GUI

Navigieren Sie zu **System > SNMP > Alarme**, wählen Sie einen Alarm aus und konfigurieren Sie die Alarmparameter.

Konfigurieren von SNMPv1- oder SNMPv2-Traps

Nach der Konfiguration der Alarme müssen Sie den Trap-Listener angeben, an den die Appliance die Trap-Meldungen sendet. Neben der Angabe von Parametern wie IP- oder IPv6-Adresse und dem Zielport des Trap-Listeners können Sie den Trap-Typ (entweder generisch oder spezifisch) und die SNMP-Version angeben.

Sie können maximal 20 Trap-Listener für den Empfang von generischen oder spezifischen Traps konfigurieren.

Sie können die Appliance auch so konfigurieren, dass sie SNMP-Trap-Nachrichten mit einer anderen Quell-IP-Adresse als der NetScaler IP-Adresse (NSIP oder NSIP6) an einen bestimmten Trap-Listener sendet. Für einen Trap-Listener mit einer IPv4-Adresse können Sie die Quell-IP entweder auf eine zugeordnete IP-Adresse (MIP) oder eine auf der Appliance konfigurierte Subnetz-IP-Adresse (SNIP) festlegen. Für einen Trap-Listener mit einer IPv6-Adresse können Sie die Quell-IP auf eine auf der Appliance konfigurierte Subnetz-IPv6 (SNIP6) -Adresse setzen.

Sie können die Appliance auch so konfigurieren, dass Trap-Nachrichten basierend auf einem Schweregrad an einen Trap-Listener gesendet werden. Wenn Sie beispielsweise den Schweregrad für einen Trap-Listener als Minor festlegen, werden alle Trap-Meldungen des Schweregrads kleiner oder größer als Minor (Minor, Major und Critical) an den Trap-Listener gesendet.

Wenn Sie einen Community-String für den Trap-Listener definiert haben, müssen Sie auch einen Community-String für jeden Trap angeben, der an den Listener gesendet werden soll. Ein Trap-Listener, für den eine Community-Zeichenfolge definiert wurde, akzeptiert nur Trap-Nachrichten, die eine Community-Zeichenfolge enthalten, die mit der im Trap-Listener definierten Community-Zeichenfolge übereinstimmt. Andere Trap-Nachrichten werden gelöscht.

So fügen Sie eine SNMP-Trap mit der CLI hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 )-destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>`
- `show snmp trap`

Beispiel:

```
> `add snmp trap specific 192.0.2.10 -version V2 -destPort 162 -communityName com1 -severity Major`
<!--NeedCopy-->
```

So konfigurieren Sie SNMP-Traps mithilfe der GUI

Navigieren Sie zu **System > SNMP > Traps**und erstellen Sie die SNMP-Trap.

Konfiguration von SNMPv3-Traps

SNMPv3 bietet Sicherheitsfunktionen wie Authentifizierung und Verschlüsselung unter Verwendung der Anmeldeinformationen von SNMP-Benutzern. Ein SNMP-Manager kann SNMPv3-Trapmeldungen nur empfangen, wenn seine Konfiguration das dem SNMP-Benutzer zugewiesene Kennwort enthält.

Das Trap-Ziel kann nun SNMPv1-, SNMPv2- und SNMPv3-Trapmeldungen empfangen.

So konfigurieren Sie eine SnmPv3-Trap mit der CLI

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Fügen Sie eine SNMPv3-Trap hinzu.

   `add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 | V3) -destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>`

   > **Hinweis**
   >
   > Nach der Einstellung kann die SNMP-Trap-Version nicht geändert werden.

   Beispiel

   ```
   > add snmp trap specific 192.0.2.10 -version V3 -destPort 162 -communityName com1 -severity Major
   ```



```
2 <!--NeedCopy-->
```

2. Fügen Sie einen SNMP-Benutzer hinzu.

   ```
   add snmp user <name> -group <string> [ -authType ( MD5 | SHA ){ -
   authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]
   ```

   Beispiel

   ```
   1 > add snmp user edocs_user -group edocs_group
   2 <!--NeedCopy-->
   ```

3. Binden Sie den SNMPv3-Trap an den SNMP-Benutzer.

```
bind snmp trap <trapClass> <trapDestination> [-version <version>] (-userName
 <string> [-securityLevel <securityLevel>])
```

Beispiel

```
1     > bind snmp trap specific 192.0.2.10 -version V3 -userName
         edocs_user -securityLevel authPriv
2 <!--NeedCopy-->
```

So konfigurieren Sie einen SNMPv3-Trap mit der GUI

1. Fügen Sie eine SNMPv3-Trap hinzu.

   Navigieren Sie zu **System > SNMP > Traps**, und erstellen Sie die SNMP-Trap, indem Sie V3 als SNMP-Version auswählen.

2. Fügen Sie einen SNMP-Benutzer hinzu.

   Navigieren Sie zu **System > SNMP > Benutzer** und erstellen Sie den SNMP-Benutzer.

3. Binden Sie den SNMPv3-Trap an den SNMP-Benutzer.

   - Navigieren Sie zu **System > SNMP > Traps**und wählen Sie die Trap der SNMP Version 3 aus.
   - Wählen Sie den Benutzer aus, an den der Trap gebunden werden soll, und definieren Sie die entsprechende Sicherheitsstufe.

SNMP-Trap-Logging

Eine NetScaler Appliance kann SNMP-Trap-Meldungen protokollieren (für SNMP-Alarme, bei denen die Protokollierungsfunktion aktiviert ist), wenn Sie die Option SNMP-Trap-Logging aktivieren und mindestens ein Trap-Listener auf der Appliance konfiguriert ist. Jetzt können Sie die Audit-Log-Ebene

von Trap-Meldungen angeben, die an einen externen Log-Server gesendet werden. Die Standardprotokollebene ist Informativ. Mögliche Werte sind Emergency, Alert, Critical, Error, Warning, Debug und Notice.

Beispielsweise können Sie die Audit-Log-Ebene für eine SNMP-Trap-Meldung, die durch einen Anmeldefehler generiert wurde, auf Kritisch setzen. Diese Informationen stehen dann auf dem NSLOG- oder SYSLOG-Server zur Fehlerbehebung zur Verfügung.

So aktivieren Sie die SNMP-Trap-Protokollierung und konfigurieren Trap Log Level mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die SNMP-Trap-Protokollierung zu konfigurieren und die Konfiguration zu überprüfen:

- `set snmp option [-snmpTrapLogging (ENABLED | DISABLED)][-snmpTrapLoggingLevel <snmpTrapLoggingLevel>]`
- `show snmp option`

So aktivieren Sie die SNMP-Trapprotokollierung und konfigurieren die SNMP-Trap-Log-Ebene mit der GUI

Navigieren Sie zu **System > SNMP**, klicken Sie auf SNMP-Optionen ändern und legen Sie die folgenden Parameter fest:

1. SNMP-Trapprotokollierung — Aktivieren Sie dieses Kontrollkästchen, um die SNMP-Trapprotokollierung zu aktivieren, wenn mindestens ein Trap-Listener auf der Appliance konfiguriert ist.
2. SNMP-Trap-Protokollierungsebene — Wählen Sie eine Überwachungsprotokollstufe für das SNMP-Trap aus. Standardmäßig ist die Auditstufe für eine SNMP-Trap auf “Informational” festgelegt.

Konfiguration von NetScaler für SNMP v1- und v2-Abfragen

May 11, 2023

Sie können den NetScaler SNMP-Agenten von einem Remote-Gerät aus, den sogenannten SNMP-Managern, nach systemspezifischen Informationen fragen. Der Agent durchsucht dann die Management Information Base (MIB) nach den angeforderten Daten und sendet die Daten an den SNMP-Manager.

Die folgenden Typen von SNMP v1- und v2-Abfragen werden vom SNMP-Agenten unterstützt:

- GET

- KOMM ALS NÄCHSTES
- ALL
- BULK HOLEN

Sie können Zeichenketten, sogenannte Community-Strings, erstellen und jede dieser Zeichenketten Abfragetypen zuordnen. Sie können jedem Abfragetyp eine oder mehrere Community-Zeichenketten zuordnen. Community-Strings sind Passwörter, die zur Authentifizierung von SNMP-Abfragen von SNMP-Managern verwendet werden.

Wenn Sie beispielsweise dem Abfragetyp GET NEXT zwei Community-Zeichenketten wieabc**und**bcd**zuordnen, betrachtet der SNMP-Agent auf der NetScaler-Appliance nur die GET NEXT SNMP-Abfragepakete, die**abc**oder bcd als Community-Zeichenfolge enthalten.**

Einen SNMP-Manager angeben

Sie müssen die NetScaler-Appliance so konfigurieren, dass die entsprechenden SNMP-Manager sie abfragen können. Sie müssen dem SNMP-Manager auch die erforderlichen NetScaler-spezifischen Informationen zur Verfügung stellen. Sie können bis zu 100 SNMP-Manager oder Netzwerke hinzufügen.

Für einen IPv4-SNMP-Manager können Sie anstelle der IP-Adresse des Managers einen Hostnamen angeben. In diesem Fall müssen Sie einen DNS-Nameserver hinzufügen, der den Hostnamen des SNMP-Managers in seine IP-Adresse auflöst. Sie können bis zu fünf auf Hostnamen basierende SNMP-Manager hinzufügen.

> **Hinweis**:
> Die Appliance unterstützt nicht die Verwendung von Hostnamen für SNMP-Manager mit IPv6-Adressen. Sie müssen die IPv6-Adresse angeben.

Wenn Sie nicht mindestens einen SNMP-Manager konfigurieren, akzeptiert und beantwortet die Appliance SNMP-Abfragen von allen IP-Adressen im Netzwerk. Wenn Sie einen oder mehrere SNMP-Manager konfigurieren, akzeptiert die Appliance und antwortet nur auf SNMP-Abfragen von diesen spezifischen IP-Adressen.

Wenn Sie einen SNMP-Manager aus der Konfiguration entfernen, kann dieser Manager die Appliance nicht mehr abfragen.

So fügen Sie SNMP-Manager hinzu, indem Sie IP-Adressen mithilfe der Befehlszeilenschnittstelle angeben

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `add snmp manager <IPAddress> ... [-netmask <netmask>]`
- `show snmp manager`

Beispiel

```
> add snmp manager 10.102.29.10 10.102.29.15 10.102.29.30
```

Um einen SNMP-Manager hinzuzufügen, indem Sie seinen Hostnamen mithilfe der Befehlszeilenschnittstelle angeben

Wichtig: Wenn Sie anstelle der IP-Adresse den Hostnamen des SNMP-Managers angeben, müssen Sie einen DNS-Nameserver konfigurieren, um den Hostnamen in die IP-Adresse des SNMP-Managers aufzulösen. Weitere Informationen finden Sie unter "Hinzufügen eines Nameservers. "

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `add snmp manager <IPAddress> [-domainResolveRetry ****<integer>]`
- `show snmp manager`

Beispiel

```
add nameserver 10.103.128.15
add snmp manager engwiki.eng.example.net -domainResolveRetry 10
```

So fügen Sie mithilfe der GUI einen SNMP-Manager hinzu

1. Navigieren Sie zu **System** > **SNMP** > **Manager**und erstellen Sie den SNMP-Manager.

   > **Wichtig**:
   >
   > Wenn Sie den Hostnamen des SNMP-Managers anstelle seiner IPv4-Adresse angeben, müssen Sie einen DNS-Nameserver konfigurieren, um den Hostnamen mit der IP-Adresse des SNMP-Managers aufzulösen.

> **Hinweis**:
> Die Appliance unterstützt keine Hostnamen für SNMP-Manager mit IPv6-Adressen.

Eine SNMP-Community angeben

Sie können Zeichenketten, sogenannte Community-Strings, erstellen und sie den folgenden SNMP-Abfragetypen auf der Appliance zuordnen:

- GET
- KOMM ALS NÄCHSTES
- ALL
- BULK HOLEN

Sie können jedem Abfragetyp eine oder mehrere Community-Zeichenketten zuordnen. Wenn Sie beispielsweise zwei Community-Zeichenketten wie **abc** und **bcd**dem Abfragetyp GET NEXT zuordnen, betrachtet der SNMP-Agent auf der Appliance nur die GET NEXT SNMP-Abfragepakete, die **abc** oder **bcd** als Community-Zeichenfolge enthalten.

Wenn Sie einem Abfragetyp keine Community-Zeichenfolge zuordnen, beantwortet der SNMP-Agent alle SNMP-Abfragen dieses Typs.

So spezifizieren Sie eine SNMP-Community mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `add snmp community <communityName> <permissions>`
- `show snmp community`

Beispiel

```
> add snmp community com all
```

So konfigurieren Sie einen SNMP-Community-String mithilfe der GUI

Navigieren Sie zu **System** > **SNMP** > **Community**und erstellen Sie die SNMP-Community.

Konfiguration von NetScaler für SNMPv3-Abfragen

May 11, 2023

Simple Network Management Protocol Version 3 (SNMPv3) basiert auf der Grundstruktur und Architektur von SNMPv1 und SNMPv2. SNMPv3 erweitert jedoch die Basisarchitektur, um Verwaltungs- und Sicherheitsfunktionen wie Authentifizierung, Zugriffskontrolle, Datenintegritätsprüfung, Überprüfung des Datenursprungs, Überprüfung der Aktualität von Nachrichten und Datenvertraulichkeit zu integrieren.

Zur Implementierung von Sicherheit und Zugriffskontrolle auf Nachrichtenebene führt SNMPv3 das benutzerbasierte Sicherheitsmodell (USM) und das View-based Access Control Model (VACM) ein.

- **Benutzerbasiertes Sicherheitsmodell.** Das benutzerbasierte Sicherheitsmodell (USM) bietet Sicherheit auf Nachrichtenebene. Es ermöglicht Ihnen, Benutzer und Sicherheitsparameter für den SNMP-Agenten und den SNMP-Manager zu konfigurieren. USM bietet die folgenden Funktionen:

  - **Datenintegrität:** Zum Schutz von Nachrichten vor Änderungen während der Übertragung über das Netzwerk.
  - **Überprüfung der Datenherkunft:** Um den Benutzer zu authentifizieren, der die Nachrichtenanfrage gesendet hat.
  - **Aktualität von Nachrichten:** Zum Schutz vor Verzögerungen oder Wiederholungen von Nachrichten.
  - **Vertraulichkeit der Daten:** Um den Inhalt von Nachrichten vor der Offenlegung an unbefugte Stellen oder Einzelpersonen zu schützen.
- **Modell der ansichtsbasierten Zugriffskontrolle.** Mit dem View-based Access Control Model (VACM) können Sie Zugriffsrechte für einen bestimmten Unterbaum der MIB auf der Grundlage verschiedener Parameter wie Sicherheitsstufe, Sicherheitsmodell, Benutzername und Ansichtstyp konfigurieren. Es ermöglicht Ihnen, Agenten so zu konfigurieren, dass sie verschiedenen Managern unterschiedliche Zugriffsebenen auf die MIB gewähren.

NetScaler unterstützt die folgenden Entitäten, mit denen Sie die Sicherheitsfunktionen von SNMPv3 implementieren können:

- SNMP-Engines
- SNMP-Ansichten
- SNMP-Gruppen
- SNMP-Benutzer

Diese Entitäten arbeiten zusammen, um die SNMPv3-Sicherheitsfunktionen zu implementieren. Views werden erstellt, um den Zugriff auf Teilbäume der MIB zu ermöglichen. Anschließend werden Gruppen mit der erforderlichen Sicherheitsstufe und dem Zugriff auf die definierten Ansichten erstellt. Schließlich werden Benutzer erstellt und den Gruppen zugewiesen.

> **Hinweis**:
>
> Die Ansicht-, Gruppen- und Benutzerkonfiguration werden synchronisiert und in einem Hochverfügbarkeitspaar (HA) an den sekundären Knoten weitergegeben. Die Engine-ID wird jedoch weder weitergegeben noch synchronisiert, da sie für jede NetScaler-Appliance eindeutig ist.

Um die Nachrichtenauthentifizierung und Zugriffskontrolle zu implementieren, müssen Sie Folgendes tun:

Einstellung der Engine-ID

SNMP-Engines sind Dienstanbieter, die sich im SNMP-Agenten befinden. Sie bieten Dienste wie das Senden, Empfangen und Authentifizieren von Nachrichten. SNMP-Engines werden anhand von Engine-IDs eindeutig identifiziert.

Die NetScaler-Appliance verfügt über eine eindeutige EngineID, die auf der MAC-Adresse einer ihrer

Schnittstellen basiert. Es ist nicht erforderlich, die EngineID zu überschreiben. Wenn Sie die Engine-ID jedoch ändern möchten, können Sie sie zurücksetzen.

So legen Sie die Engine-ID mithilfe der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `set snmp engineId <engineID>`
- `show snmp engineId`

Beispiel

```
> set snmp engineId 8000173f0300c095f80c68
```

So legen Sie die Engine-ID mithilfe der GUI fest

Navigieren Sie zu **System** > **SNMP** > **Benutzer**, klicken Sie auf **Engine-ID konfigurieren** und geben Sie eine Engine-ID ein.

Eine Ansicht konfigurieren

SNMP-Ansichten beschränken den Benutzerzugriff auf bestimmte Teile der MIB. SNMP-Ansichten werden verwendet, um die Zugriffssteuerung zu implementieren.

So fügen Sie mithilfe der Befehlszeilenschnittstelle eine SNMP-Ansicht hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `add snmp view <name> <subtree> -type ( included | excluded )`
- `show snmp view <name>`
- `rm snmp view <name> <subtree>`

Hierbei gilt:

Name. Name für die SNMPv3-Ansicht. Es kann aus 1 bis 31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und die Zeichen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), At-Zeichen (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstriche (_) enthalten. Sie sollten einen Namen wählen, der hilft, die SNMPv3-Ansicht zu identifizieren.

Teilbaum. Ein bestimmter Zweig (Unterbaum) des MIB-Baums, den Sie dieser SNMPv3-Ansicht zuordnen möchten. Sie müssen den Teilbaum als SNMP-OID angeben. Dies ist ein Argument mit einer maximalen Länge: 99.

Typ. Schließt den durch den Teilbaumparameter angegebenen Teilbaum in oder aus dieser Ansicht ein. Diese Einstellung kann nützlich sein, wenn Sie einen Teilbaum wie A in eine SNMPv3-Ansicht aufgenommen haben und einen bestimmten Teilbaum von A, z. B. B, aus der SNMPv3-Ansicht ausschließen möchten. Dies ist ein zwingendes Argument. Mögliche Werte: enthalten, ausgeschlossen.

Beispiele

add snmp view SNMPv3test 1.1.1.1 -type included
sh snmp view SNMPv3test
rm snmp view SNMPv3test 1.1.1.1

So konfigurieren Sie eine SNMP-Ansicht mithilfe der GUI

Navigieren Sie zu **System** > **SNMP** > **Views**und erstellen Sie die SNMP-Ansicht.

Eine Gruppe konfigurieren

SNMP-Gruppen sind logische Aggregationen von SNMP-Benutzern. Sie werden verwendet, um die Zugriffskontrolle zu implementieren und die Sicherheitsstufen zu definieren. Sie können eine SNMP-Gruppe konfigurieren, um Zugriffsrechte für Benutzer festzulegen, die dieser Gruppe zugewiesen sind, wodurch die Benutzer auf bestimmte Ansichten beschränkt werden.

Sie müssen eine SNMP-Gruppe konfigurieren, um Zugriffsrechte für Benutzer festzulegen, die dieser Gruppe zugewiesen sind.

So fügen Sie eine SNMP-Gruppe mithilfe der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `add snmp group <name> <securityLevel> -readViewName <string>`
- `show snmp group <name> <securityLevel>`

Hierbei gilt:

Name. Name für die SNMPv3-Gruppe. Kann aus 1 bis 31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und die Zeichen Bindestrich (-), Punkt (.), Pfund (#), Leerzeichen (), At-Zeichen (@), Gleichheitszeichen (=), Doppelpunkt (:) und Unterstriche (_) enthalten. Sie sollten einen Namen wählen, anhand dessen die SNMPv3-Gruppe identifiziert werden kann.

Sicherheitsstufe. Sicherheitsstufe, die für die Kommunikation zwischen der NetScaler-Appliance und den SNMPv3-Benutzern, die der Gruppe angehören, erforderlich ist. Geben Sie eine der folgenden Optionen an:

Nein,**Autor, Nopriv**. Erfordert weder Authentifizierung noch Verschlüsselung.

VerfasserNopriv. Authentifizierung erforderlich, aber keine Verschlüsselung.

VerfasserPriv. Authentifizierung und Verschlüsselung erforderlich. Hinweis: Wenn Sie die Authentifizierung angeben, müssen Sie einen Verschlüsselungsalgorithmus angeben, wenn Sie der Gruppe einen SNMPv3-Benutzer zuweisen. Wenn Sie auch Verschlüsselung angeben, müssen Sie jedem Gruppenmitglied sowohl einen Authentifizierungs- als auch einen Verschlüsselungsalgorithmus zuweisen. Dies ist ein zwingendes Argument. Mögliche Werte: noAuthNoPriv, authNoPriv, authPriv.

Lesen Sie den Namen der Ansicht. Name der konfigurierten SNMPv3-Ansicht, die Sie an diese SNMPv3-Gruppe binden möchten. Ein an diese Gruppe gebundener SNMPv3-Benutzer kann auf die Teilbäume zugreifen, die an diese SNMPv3-Ansicht als Typ INCLUDED gebunden sind, aber nicht auf die, die vom Typ EXCLUDED sind. Wenn die NetScaler-Appliance mehrere SNMPv3-View-Einträge mit demselben Namen hat, sind alle diese Einträge der SNMPv3-Gruppe zugeordnet. Dies ist ein zwingendes Argument. Maximale Länge: 31

So konfigurieren Sie eine SNMP-Gruppe mithilfe der GUI

Navigieren Sie zu **System** > **SNMP** > **Gruppen**und erstellen Sie die SNMP-Gruppe.

Einen Benutzer konfigurieren

SNMP-Benutzer sind die SNMP-Manager, denen die Agenten den Zugriff auf die MIBs ermöglichen. Jeder SNMP-Benutzer ist einer SNMP-Gruppe zugewiesen.

Sie müssen Benutzer am Agenten konfigurieren und jeden Benutzer einer Gruppe zuweisen.

So konfigurieren Sie einen Benutzer mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

- `add snmp user <name> -group <string> [-authType ( MD5 | SHA ){ -authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]`
- `show snmp user <name>`

Hierbei gilt:

AuthType ist die Authentifizierungsoption, die bei der Konfiguration eines Benutzers verfügbar ist. Es gibt zwei Authentifizierungstypen wie MD5 und SHA.

PrivType ist die Verschlüsselungsoption, die bei der Konfiguration eines Benutzers verfügbar ist. Es gibt zwei Arten der Verschlüsselung, z. B. DES mit einer Schlüsselgröße von 128 Bit und AES mit einer Schlüsselgröße von 128 Bit.

Beispiel

```
> add snmp user edocs_user -group edocs_group
<!--NeedCopy-->
```

So konfigurieren Sie einen SNMP-Benutzer mithilfe der GUI

Navigieren Sie zu **System** > **SNMP** > **Benutzer**und erstellen Sie den SNMP-Benutzer.

Konfiguration von SNMP-Alarmen für die Ratenbegrenzung

May 11, 2023

NetScaler-Appliances sind ratenbegrenzt. Informationen zu den verschiedenen Modellen, die für jede Plattform verfügbar sind, finden Sie im Datenblatt. Das Datenblatt ist auf www.citrix.comverfügbar. Klicken Sie auf **Produkte**. Klicken Sie unter **App Delivery and Security**auf **NetScaler**. Klicken Sie auf **Plattformen > Physikalische Appliances** und dann auf **NetScaler MPX/SDX-Datenblatt**.

Der maximale Durchsatz (Mbit/s) und die Pakete pro Sekunde (PPS) werden durch die für die Appliance erworbene Lizenz bestimmt. Für Plattformen mit begrenzter Geschwindigkeit können Sie SNMP-Traps so konfigurieren, dass Benachrichtigungen gesendet werden, wenn der Durchsatz und die PPS ihre Grenzwerte erreichen und wenn sie wieder normal sind.

Durchsatz und PPS werden alle sieben Sekunden überwacht. Sie können Traps mit hohen und normalen Schwellenwerten konfigurieren, die als Prozentsatz der lizenzierten Grenzwerte ausgedrückt werden. Die Appliance generiert dann einen Trap, wenn der Durchsatz oder die PPS den hohen Schwellenwert überschreiten, und einen zweiten Trap, wenn der überwachte Parameter auf den normalen Schwellenwert fällt. Die NetScaler-Appliance sendet nicht nur die Traps an das konfigurierte Zielgerät, sondern protokolliert auch die den Traps zugeordneten Ereignisse in der Datei /var/log/ns.log als EVENT ALERTSTARTED und EVENT ALERTENDED.

Eine Überschreitung des Durchsatzlimits kann zu Paketverlusten führen. Sie können SNMP-Alarme konfigurieren, um Paketverlust zu melden.

Weitere Informationen zu SNMP-Alarmen und Traps finden Sie unter “Konfigurieren des NetScaler zum Generieren von SNMP v1- und v2-Traps. “

Dieses Dokument enthält die folgenden Details:

- Konfiguration eines SNMP-Alarms für Throughput oder PPS
- Konfiguration eines SNMP-Alarms für verworfene Pakete

Konfiguration eines SNMP-Alarms für Throughput oder PPS

Um sowohl Durchgänge als auch PPS zu überwachen, müssen Sie separate Alarme konfigurieren und den PPS-Schwellenwert in Mbit/s festlegen.

So konfigurieren Sie einen SNMP-Alarm für die Durchsatzrate über die CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den SNMP-Alarm zu konfigurieren, den Schwellenwert in Mbit/s festzulegen und die Konfiguration zu überprüfen:

- `set snmp alarm PF-RL-RATE-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm PF-RL-RATE-THRESHOLD`

Beispiel

```
1 > set snmp alarm PF-RL-RATE-THRESHOLD -thresholdValue 70 -normalValue
     50
2 <!--NeedCopy-->
```

So konfigurieren Sie einen SNMP-Alarm für PPS über die CLI

Geben Sie an der Befehlszeile die folgenden Befehle ein, um den SNMP-Alarm für PPS zu konfigurieren und die Konfiguration zu überprüfen:

- `set snmp alarm PF-RL-PPS-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm PF-RL-PPS-THRESHOLD`

Beispiel

```
1 > set snmp alarm PF-RL-PPS-THRESHOLD -thresholdValue 70 -normalValue 50
2 <!--NeedCopy-->
```

So konfigurieren Sie einen SNMP-Alarm für Throughput oder PPS über die GUI

1. Navigieren Sie zu **System > SNMP > Alarme**und wählen Sie **PF-RL-RATE-THRESHOLD** (für die Durchsatzrate) oder **PF-RL-PPS-THRESHOLD** (für Pakete pro Sekunde).
2. Stellen Sie die Alarmparameter ein und aktivieren Sie den ausgewählten SNMP-Alarm.

Konfiguration des SNMP-Alarms für verworfene Pakete

Sie können einen Alarm für Pakete konfigurieren, die aufgrund einer Überschreitung des Durchsatzlimits verworfen wurden, und einen Alarm für Pakete, die aufgrund der Überschreitung des PPS-Grenzwerts verworfen wurden.

So konfigurieren Sie einen SNMP-Alarm für Pakete, die aufgrund eines zu hohen Durchsatzes verworfen wurden, über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set snmp alarm PF-RL-RATE-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

So konfigurieren Sie über die CLI einen SNMP-Alarm für Pakete, die aufgrund übermäßiger PPS-Werte verworfen wurden

Geben Sie in der Befehlszeile Folgendes ein:

```
set snmp alarm PF-RL-PPS-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

So konfigurieren Sie einen SNMP-Alarm für verworfene Pakete über die GUI

1. Navigieren Sie zu **System > SNMP > Alarms**und wählen Sie **PF-RL-RATE-PKTS-DROPED** (für Pakete, die aufgrund eines zu hohen Durchsatzes verworfen wurden) oder **PF-RL-PPS-PKS-PKTS-DROPED** (für Pakete, die aufgrund übermäßigen PPS verworfen wurden).
2. Stellen Sie die Alarmparameter ein und aktivieren Sie den ausgewählten SNMP-Alarm.

Konfiguration von SNMP im FIPS-Modus

May 11, 2023

Der FIPS-Modus erfordert Simple Network Management Protocol Version 3 (SNMPv3) mit der Option Authentifizierung und Datenschutz (AuthPriv). SNMP Version 1 und Version 2 verwenden einen Community-String-Mechanismus, um einen sicheren Zugriff auf Verwaltungsdaten zu ermöglichen. Die Community-Zeichenfolge wird als Klartext zwischen einem SNMP-Manager und einem SNMP-Agenten gesendet. Diese Art der Kommunikation ist unsicher und ermöglicht es Eindringlingen, auf SNMP-Informationen im Netzwerk zuzugreifen.

Das SNMPv3-Protokoll verwendet das User-Based Security Model (USM) und das View-Based Access Control Model (VACM), um den Verwaltungszugriff auf SNMP-Messaging-Daten zu authentifizieren und

zu kontrollieren. SNMPv3 hat drei Sicherheitsstufen: keine Authentifizierung, kein Datenschutz (noAuthNoPriv), Authentifizierung und kein Datenschutz (AuthNoPriv) sowie Authentifizierung und Datenschutz (AuthPriv).

Wenn Sie den FIPS-Modus aktivieren und die NetScaler-Appliance neu starten, werden die folgenden SNMP-Konfigurationen von der Appliance entfernt:

1. Community-Konfiguration für die Protokolle SNMPv1 und SNMPv2.
2. SNMPv3-Gruppen, die mit der Sicherheitsleveloption NoAuthNoPriv oder AuthNoPriv konfiguriert wurden.
3. Traps, die für SNMPv1 oder SNMPv2 oder SNMPv3 mit der Sicherheitsstufenoption NoAuthNoPriv konfiguriert wurden.

Nach dem Neustart der Appliance konfigurieren Sie SNMPv3 mit der Option AuthPriv. Weitere Informationen zum Konfigurieren der AuthPriv-Option in SMNP v3 finden Sie im Thema SNMPV3

> **Hinweis**:
>
> Durch Aktivieren des FIPS-Modus und Neustart der Appliance wird die Ausführung der folgenden SNMP-Trap- und Gruppenbefehle blockiert:

```
1.  add snmp community <communityName> <permissions>

2.  add snmp trap <trapClass> <trapDestination> ... [-version: v1/
   v2]   [-td <positive_integer>] [-destPort <port>] [-
   communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity
   <severity>] [-allPartitions ( ENABLED | DISABLED )]

3.  add snmp group <name> <securityLevel : noAuthNoPriv/ authNoPriv
    > -readViewName <string>

4.  bind snmp trap specific <TrapIp>-userName <v3 user name> -
   securityLevel <noAuthNoPriv/ authNoPriv>
<!--NeedCopy-->
```

Audit-Protokollierung

May 11, 2023

> **Wichtig**
>
> Citrix empfiehlt, eine SYSLOG- oder NSLOG-Konfiguration nur während Wartungs- oder Ausfallzeiten zu aktualisieren. Wenn Sie eine Konfiguration aktualisieren, nachdem Sie eine Sitzung

> erstellt haben, werden die Änderungen nicht auf die vorhandenen Sitzungsprotokolle angewendet.

Auditing ist eine methodische Untersuchung oder Überprüfung eines Zustands oder einer Situation. Mit der Audit-Logging-Funktion können Sie die NetScaler-Status- und Statusinformationen protokollieren, die von verschiedenen Modulen gesammelt wurden. Die Protokollinformationen können sich im Kernel und in den Daemons auf Benutzerebene befinden. Für die Auditprotokollierung können Sie das SYSLOG-Protokoll, das native NSLOG-Protokoll oder beides verwenden.

SYSLOG ist ein Standardprotokoll für die Protokollierung. Es besteht aus zwei Komponenten:

- **SYSLOG-Auditmodul.** Läuft auf der NetScaler-Appliance.
- **SYSLOG-Server.** Läuft auf dem zugrunde liegenden FreeBSD-Betriebssystem (OS) der NetScaler-Appliance oder auf einem Remote-System.

SYSLOG verwendet ein Benutzerdatenprotokoll (UDP) für die Datenübertragung.

In ähnlicher Weise besteht das native NSLOG-Protokoll aus zwei Komponenten:

- **NSLOG-Auditmodul.** Läuft auf der NetScaler-Appliance.
- **NSLOG-Server.** Läuft auf dem zugrunde liegenden FreeBSD-Betriebssystem der NetScaler-Appliance oder auf einem Remote-System.

NSLOG verwendet TCP für die Datenübertragung.

Wenn Sie einen SYSLOG- oder NSLOG-Server ausführen, stellt er eine Verbindung zur NetScaler-Appliance her. Die NetScaler-Appliance beginnt dann, alle Protokollinformationen an den SYSLOG- oder NSLOG-Server zu senden. Und der Server filtert die Logeinträge, bevor er sie in einer Protokolldatei speichert. Ein NSLOG- oder SYSLOG-Server empfängt Protokollinformationen von mehr als einer NetScaler-Appliance. Die NetScaler-Appliance sendet Protokollinformationen an mehr als einen SYSLOG-Server oder NSLOG-Server.

Wenn mehrere SYSLOG-Server konfiguriert sind, sendet die NetScaler-Appliance ihre SYSLOG-Ereignisse und -Meldungen an alle konfigurierten externen Protokollserver. Dies führt zum Speichern redundanter Nachrichten und erschwert Systemadministratoren die Überwachung. Um dieses Problem zu beheben, bietet die NetScaler-Appliance Algorithmen für den Lastausgleich. Die Appliance kann die SYSLOG-Nachrichten auf die externen Protokollserver ausgleichen, um die Wartung und Leistung zu verbessern. Zu den unterstützten Load-Balancing-Algorithmen gehören RoundRobin, LeastBandwidth, CustomLoad, LeastPackets und AuditlogHash.

> **Hinweis**
>
> Die NetScaler-Appliance kann Audit-Logmeldungen mit bis zu 16 KB an einen externen SYSLOG-Server senden.

Die Protokollinformationen, die ein SYSLOG- oder NSLOG-Server von einer NetScaler-Appliance sammelt, werden in Form von Nachrichten in einer Protokolldatei gespeichert. Diese Meldungen enthalten normalerweise die folgenden Informationen:

- Die IP-Adresse einer NetScaler-Appliance, die die Protokollnachricht generiert hat.
- Zeitstempel
- Meldungstyp
- Die vordefinierten Protokollebenen (Kritisch, Fehler, Hinweis, Warnung, Information, Debug, Warnung und Notfall)
- Meldungstext

Um die Auditprotokollierung zu konfigurieren, konfigurieren Sie zunächst die Auditmodule auf der NetScaler-Appliance. Die Appliance umfasst die Erstellung von Audit-Richtlinien und die Angabe der NSLOG-Server- oder SYSLOG-Serverinformationen. Anschließend installieren und konfigurieren Sie den SYSLOG- oder NSLOG-Server auf dem zugrunde liegenden FreeBSD-Betriebssystem der NetScaler-Appliance oder auf einem Remote-System.

> **Hinweis**
>
> SYSLOG ist ein Industriestandard für die Protokollierung von Programmmeldungen, und verschiedene Anbieter bieten Unterstützung. Die Dokumentation enthält keine Informationen zur SYSLOG-Serverkonfiguration.

Der NSLOG-Server hat eine eigene Konfigurationsdatei (auditlog.conf). Sie können die Protokollierung auf dem NSLOG-Serversystem anpassen, indem Sie zusätzliche Änderungen an der Konfigurationsdatei (auditlog.conf) vornehmen.

> **Hinweis**
>
> Der ICMP-Zugriff auf den Syslog-Server ist erforderlich, wenn der Syslog-Server als FQDN unter Syslog-Aktion im Netzwerk verwendet wird. Wenn der ICMP-Zugriff in der Umgebung blockiert ist, konfigurieren Sie ihn als Syslog-Server mit Lastausgleich und setzen Sie den Wert des healthMonitor-Parameters im Befehl set service auf NO.
> Informationen zur Konfiguration von ICMP finden Sie unter SYSLOG-Server für den Lastausgleich

Konfigurieren der NetScaler-Appliance für die Überwachungsprotokollierung

May 11, 2023

> **Warnung:**
>
> Klassische Richtlinienausdrücke und ihre Verwendung sind ab NetScaler 12.0 Build 56.20 veraltet (von der Verwendung abgeraten, werden aber weiterhin unterstützt). Als Alternative empfiehlt Citrix, erweiterte Richtlinien zu verwenden. Weitere Informationen finden Sie unter Erweiterte Richtlinien.

In der Auditprotokollierung werden Statusinformationen aus verschiedenen Modulen angezeigt, sodass ein Administrator den Ereignisverlauf in chronologischer Reihenfolge einsehen kann. Hauptbestandteile eines Prüfungsrahmens sind “Prüfungsaktion”, “Audit-Richtlinie”. “Audit-Aktion” beschreibt Konfigurationsinformationen des Überwachungsservers, während “Audit-Richtlinie” eine Bindungseinheit mit einer “Audit-Aktion” verknüpft. Die Prüfungsrichtlinien verwenden das Framework “Classic Policy Engine” (CPE) oder das Progress Integration (PI) -Framework, um “Prüfungsmaßnahmen” mit “globalen Systembindungsgesellschaften” zu verknüpfen.

Die Richtlinienrahmen unterscheiden sich jedoch voneinander darin, dass die Audit-Log-Richtlinien für globale Unternehmen verbindlich sind. Bisher unterstützte das Audit-Modul nur klassische und erweiterte Richtlinienausdrücke. Derzeit können Sie mit dem erweiterten Ausdruck Audit-Log-Richtlinien nur an globale Systementitäten binden.

> **Hinweis**
>
> Wenn Sie eine Richtlinie an globale Entitäten binden, müssen Sie sie an eine globale Systementität desselben Ausdrucks binden. Beispielsweise können Sie eine klassische Richtlinie nicht an eine erweiterte globale Entität binden oder eine erweiterte Richtlinie an eine klassische globale Entität binden.
>
> Außerdem können Sie nicht sowohl die klassische Überwachungsprotokollrichtlinie als auch die erweiterte Überwachungsprotokollrichtlinie an einen virtuellen Lastausgleichsserver binden.

Konfiguration von Audit-Log-Richtlinien in einem klassischen Richtlinienausdruck

Die Konfiguration der Auditprotokollierung in der klassischen Richtlinie besteht aus den folgenden Schritten:

1. **Konfiguration einer Audit-Log-Aktion**. Sie können eine Überwachungsaktion für verschiedene Server und für verschiedene Protokollierungsstufen konfigurieren. “Audit-Aktion” beschreibt Konfigurationsinformationen des Überwachungsservers, während “Audit-Richtlinie” eine Bindungseinheit mit einer “Audit-Aktion” verknüpft. Standardmäßig verwenden SYSLOG und NSLOG nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist für die Übertragung vollständiger Daten zuverlässiger als UDP. Wenn Sie TCP für SYSLOG verwenden, können Sie das Pufferlimit auf der NetScaler-Appliance festlegen, um die Protokolle zu speichern. Danach werden die Protokolle an den SYSLOG-Server gesendet.
2. **Konfiguration der Audit-Log-Richtlinie**. Sie können entweder SYSLOG-Richtlinien konfigurieren, um Nachrichten auf einem SYSLOG-Server zu protokollieren, oder eine NSLOG-Richtlinie, um Nachrichten auf einem NSLOG-Server zu protokollieren. Jede Richtlinie enthält eine Regel, die auf **`true`** oder `ns_true` für die zu protokollierenden Nachrichten festgelegt ist, sowie eine SYSLOG- oder NSLOG-Aktion.

3. **Verbindliche Audit-Log-Richtlinien für globale Unternehmen**. Sie müssen die Überwachungsprotokollrichtlinien global an globale Entitäten wie SYSTEM, VPN, NetScaler AAA usw. binden. Sie können dies tun, um die Protokollierung aller NetScaler-Systemereignisse zu aktivieren. Durch Definieren der Prioritätsstufe können Sie die Auswertungsreihenfolge für die Protokollierung des Audit-Servers festlegen. Priorität 0 ist die höchste und wird zuerst ausgewertet. Je höher die Prioritätszahl, desto niedriger ist die Priorität der Bewertung.

Jeder dieser Schritte wird in den folgenden Abschnitten erläutert.

Konfiguration der Audit-Log-Aktion

Um die SYSLOG-Aktion in einer erweiterten Richtlinieninfrastruktur über die CLI zu konfigurieren.

> **Hinweis**
>
> Mit der NetScaler-Appliance können Sie nur eine SYSLOG-Aktion für die IP-Adresse und den Port des SYSLOG-Servers konfigurieren. Die Appliance erlaubt es Ihnen nicht, mehrere SYSLOG-Aktionen für dieselbe Server-IP-Adresse und denselben Port zu konfigurieren.

Eine Syslog-Aktion enthält einen Verweis auf einen Syslog-Server. Es gibt an, welche Informationen protokolliert werden sollen, und erwähnt, wie diese Informationen protokolliert werden sollen.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
1 -  add audit syslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
     transport ( TCP | UDP )]`
2 -  show audit syslogAction [<name>]
3
4 <!--NeedCopy-->
```

Um die NSLOG-Aktion in einer erweiterten Richtlinieninfrastruktur über die CLI zu konfigurieren.

Eine ns-Protokollaktion enthält einen Verweis auf einen nslog-Server. Es gibt an, welche Informationen protokolliert werden sollen, und erwähnt, wie diese Informationen protokolliert werden sollen.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
1 -  add audit nslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
2 -  show audit nslogAction [<name>]
3 <!--NeedCopy-->
```


Auditprotokollrichtlinien konfigurieren

Konfigurieren Sie die Audit-Log-Richtlinien in der klassischen Policy-Infrastruktur über die CLI.

Geben Sie in der Befehlszeile Folgendes ein:

```
1 -  add audit syslogpolicy <name> <-rule> <action>
2 -  add audit nslogpolicy <name> <-rule> <action>
3 <!--NeedCopy-->
```

Verbindliche Audit-Syslog-Richtlinien zur Prüfung von syslog global

Binden Sie die Audit-Log-Richtlinie im Advanced Policy Framework über die CLI.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType]
```

```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

Binden Sie die Audit-Log-Richtlinie im klassischen Policy-Framework über die CLI.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind systemglobal <policy Name> <Priority>
```

```
unbind systemglobal <policy Name> <Priority>
```

Audit-Log-Richtlinien mit Advanced Policy Expression konfigurieren

Die Konfiguration der Auditprotokollierung in Advanced Policy besteht aus den folgenden Schritten:

1. **Konfiguration einer Audit-Log-Aktion**. Sie können eine Überwachungsaktion für verschiedene Server und für verschiedene Protokollierungsstufen konfigurieren. “Audit-Aktion” beschreibt Konfigurationsinformationen des Überwachungsservers, während “Audit-Richtlinie” eine Bindungseinheit mit einer “Audit-Aktion” verknüpft. Standardmäßig verwenden SYSLOG und NSLOG nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist für die Übertragung vollständiger Daten zuverlässiger als UDP. Wenn Sie TCP für SYSLOG verwenden, können Sie das Pufferlimit auf der NetScaler-Appliance festlegen, um die Protokolle zu speichern. Danach werden die Protokolle an den SYSLOG-Server gesendet.
2. **Konfiguration der Audit-Log-Richtlinie**. Sie können entweder SYSLOG-Richtlinien konfigurieren, um Nachrichten auf einem SYSLOG-Server zu protokollieren, oder eine NSLOG-Richtlinie, um Nachrichten auf einem NSLOG-Server zu protokollieren. Jede Richtlinie enthält eine Regel, die auf **`true`** oder `ns_true` für die zu protokollierenden Nachrichten festgelegt ist, sowie eine SYSLOG- oder NSLOG-Aktion.

3. **Verbindliche Audit-Log-Richtlinien für globale Unternehmen**. Sie müssen die Überwachungsprotokollrichtlinien global an die globale System-Entität binden, um die Protokollierung aller NetScaler-Systemereignisse zu ermöglichen. Durch Definieren der Prioritätsstufe können Sie die Auswertungsreihenfolge für die Protokollierung des Audit-Servers festlegen. Priorität 0 ist die höchste und wird zuerst ausgewertet. Je höher die Prioritätszahl, desto niedriger ist die Priorität der Bewertung.

> **Hinweis**
>
> Die NetScaler-Appliance wertet alle Richtlinien aus, die an true gebunden sind.

Konfiguration der Audit-Log-Aktion

Um die Syslog-Aktion in einer erweiterten Richtlinieninfrastruktur über die CLI zu konfigurieren.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
1 -  add audit syslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
     transport ( TCP | UDP )]
2 -  show audit syslogAction [<name>]
3 <!--NeedCopy-->
```

Konfigurieren Sie die NSLOG-Aktion in der erweiterten Richtlinieninfrastruktur über die CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Parameter festzulegen und die Konfiguration zu überprüfen:

```
1 -  add audit nslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
2 -  show audit nslogAction [<name>]
3 <!--NeedCopy-->
```

Auditprotokollrichtlinien konfigurieren

Um eine Syslog-Audit-Aktion über die CLI hinzuzufügen.

Geben Sie in der Befehlszeile Folgendes ein:

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
          domainResolveRetry <integer>])
2     | -lbVserverName <string>))[-serverPort <port>] -logLevel <logLevel
          >[-dateFormat <dateFormat>]
```



```
3       [-logFacility <logFacility>][-tcp ( NONE | ALL )] [-acl ( ENABLED
            | DISABLED )]
4      [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog ( YES |
           NO )]
5       [-appflowExport ( ENABLED | DISABLED )] [-lsn ( ENABLED | DISABLED
            )][-alg ( ENABLED | DISABLED )]
6      [-subscriberLog ( ENABLED | DISABLED )][-transport ( TCP | UDP )]
           [-tcpProfileName <string>][-maxLogDataSizeToHold
7  <!--NeedCopy-->
```

Beispiel

```
1      > add audit syslogaction audit-action1 10.102.1.1 -loglevel
           INFORMATIONAL -dateformat MMDDYYYY
2      > add audit nslogAction nslog-action1 10.102.1.3 -serverport 520 -
           loglevel INFORMATIONAL -dateFormat MMDDYYYY
3      > add audit syslogpolicy syslog-pol1 TRUE audit-action1
4      > add audit nslogPolicy nslog-pol1 TRUE nslog-action1
5      > bind system global nslog-pol1 -priority 20
6  <!--NeedCopy-->
```

Fügen Sie über die CLI eine nslog-Audit-Aktion hinzu.

Geben Sie in der Befehlszeile Folgendes ein:

```
1      add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
           domainResolveRetry <integer>])) [-serverPort <port>]       -
           logLevel <logLevel> ... [-dateFormat <dateFormat>][-logFacility
           <logFacility>] [-tcp ( NONE | ALL )][-acl ( ENABLED | DISABLED )
           ] [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog (
           YES | NO )][-appflowExport ( ENABLED | DISABLED )] [-lsn (
           ENABLED | DISABLED )][-alg ( ENABLED | DISABLED )] [-
           subscriberLog ( ENABLED | DISABLED )]`
2  <!--NeedCopy-->
```

Verbindliche Audit-Log-Richtlinien für globale Unternehmen

Binden Sie die Syslog-Audit-Log-Richtlinie im Advanced Policy Framework über die CLI.

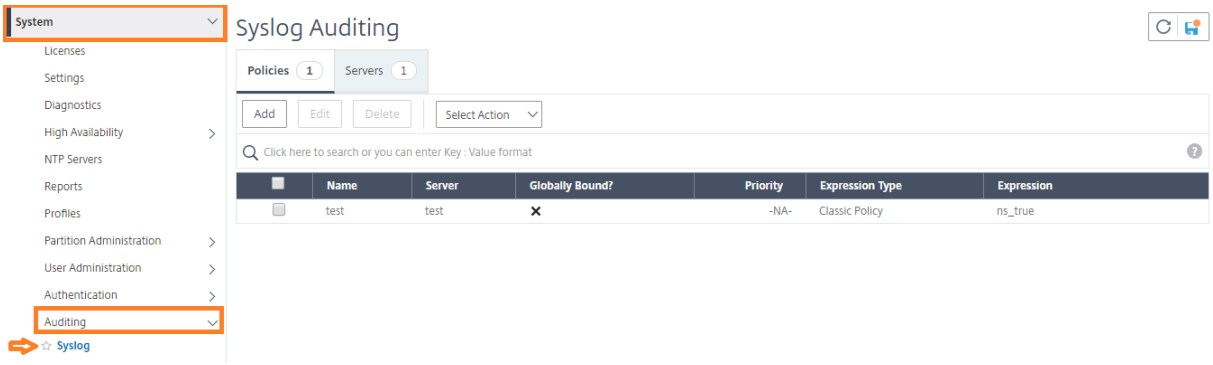
Geben Sie in der Befehlszeile Folgendes ein:

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
```

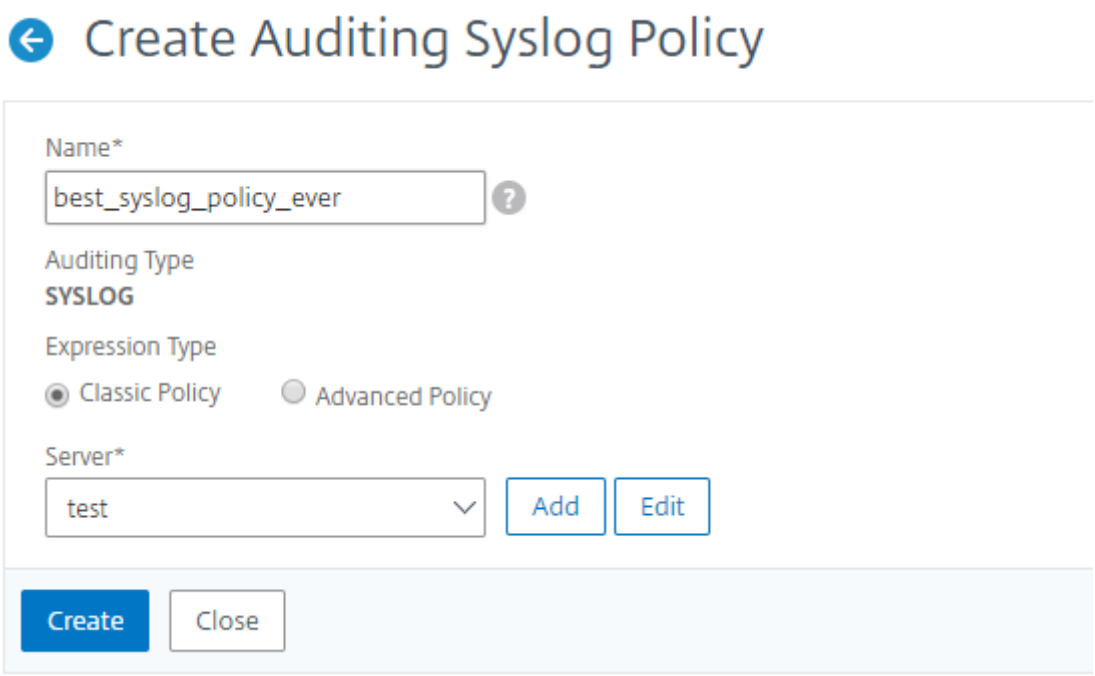
```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```


Konfiguration der Audit-Log-Richtlinie über die GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Auditing** > **Syslog**.



1. Wählen Sie **die Registerkarte Server** .
2. Klicken Sie auf **Hinzufügen**.
3. Füllen Sie auf der Seite **“Auditing Server erstellen** “ die entsprechenden Felder aus und klicken Sie auf **Erstellen**.
4. Um die Richtlinie hinzuzufügen, wählen Sie die Registerkarte **Richtlinien** aus und klicken Sie auf **Hinzufügen**.
5. Füllen **Sie auf der Seite “Auditing Syslog-Richtlinie** erstellen” die entsprechenden Felder aus und klicken Sie auf **Erstellen**.



6. Um die Richtlinie global zu binden, wählen Sie **Advanced Policy Globale Bindings** aus der Drop-downliste aus. Wählen Sie die Richtlinie **best_syslog_policy_ever** aus. Klicken Sie auf **Select**.

7. Wählen Sie in der Dropdownliste den Bindepunkt als **SYSTEM_GLOBAL** aus, klicken Sie auf **Binden**, und klicken Sie dann auf **Fertig**.

Konfigurieren der richtlinienbasierten Protokollierung

Sie können richtlinienbasierte Protokollierung für Rewrite- und Responder-Richtlinien konfigurieren. Überwachungsmeldungen werden dann in einem definierten Format protokolliert, wenn die Regel in einer Richtlinie auf TRUE ausgewertet wird. Um die richtlinienbasierte Protokollierung zu konfigurieren, konfigurieren Sie eine Auditmeldungsaktion, die erweiterte Richtlinienausdrücke verwendet, um das Format der Auditmeldungen anzugeben. Und verknüpfen Sie die Aktion mit einer Richtlinie. Die Richtlinie kann entweder global oder an einen virtuellen Lastausgleich- oder Content Switching-Server gebunden sein. Sie können Audit-Message-Aktionen verwenden, um Nachrichten auf verschiedenen Protokollierungsebenen zu protokollieren, entweder nur im Syslog-Format oder sowohl im Syslog- als auch im neuen nslog-Format.

Voraussetzungen

- Die Option Konfigurierbare Protokollmeldungen (userDefinedAuditlog) ist für die Konfiguration des Überwachungsaktionsservers aktiviert, an den Sie die Protokolle in einem definierten Format senden möchten.
- Die zugehörige Prüfungsrichtlinie ist an das globale System gebunden.

Konfigurieren einer Aktion für Überwachungsnachrichten

Sie können Aktionen für Überwachungsnachrichten konfigurieren, um Nachrichten auf verschiedenen Protokollierungsebenen zu protokollieren, entweder nur im Syslog-Format oder sowohl im Syslog- als auch in neuen ns-Protokollformaten. Auditmeldungsaktionen verwenden Ausdrücke, um das Format der Auditmeldungen anzugeben.

Erstellen Sie eine Audit-Nachrichtenaktion über die CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
add audit messageaction <name> <logLevel> <stringBuilderExpr> [-
   logtoNewnslog (YES|NO)]
<!--NeedCopy-->
```

```
add audit messageaction log-act1 CRITICAL '"Client:"+CLIENT.IP.SRC+"
   accessed "+HTTP.REQ.URL'
<!--NeedCopy-->
```


Konfigurieren Sie eine Audit-Nachrichtenaktion über die GUI

Navigieren Sie zu **System > Auditing > Nachrichtenaktionen**, und erstellen Sie die Aktion "Überwachungsnachricht".

Aktion für Audit-Nachrichten an eine Richtlinie binden

Nachdem Sie eine Überwachungsnachrichtenaktion erstellt haben, müssen Sie sie an eine Rewrite- oder Responderrichtlinie binden. Weitere Informationen zum Binden von Protokollnachrichtenaktionen an eine Rewrite- oder Responder Policy finden Sie unter Rewrite oder Responder.

Installation und Konfiguration des NSLOG-Servers

May 11, 2023

Während der Installation wird die ausführbare Datei des NSLOG-Servers (Auditserver) zusammen mit anderen Dateien installiert. Die ausführbare Auditserver-Datei enthält Optionen zum Ausführen verschiedener Aktionen auf dem NSLOG-Server, einschließlich des Ausführens und Stoppens des NSLOG-Servers. Darüber hinaus verwenden Sie die ausführbare Datei auditserver, um den NSLOG-Server mit den IP-Adressen der NetScaler-Appliances zu konfigurieren, von denen aus der NSLOG-Server mit dem Sammeln von Protokollen beginnt. Die Konfigurationseinstellungen werden in der NSLOG-Serverkonfigurationsdatei (auditlog.conf) angewendet.

Anschließend starten Sie den NSLOG-Server, indem Sie die ausführbare Auditserver-Datei ausführen. Die NSLOG-Serverkonfiguration basiert auf den Einstellungen in der Konfigurationsdatei. Sie können die Protokollierung auf dem NSLOG-Serversystem weiter anpassen, indem Sie zusätzliche Änderungen an der NSLOG-Serverkonfigurationsdatei (auditlog.conf) vornehmen.

> **Achtung**:
>
> Die Version des NSLOG-Serverpakets muss mit der des NetScaler. Wenn die Version des NetScaler beispielsweise 10.1 Build 125.9 ist, muss auch der NSLOG-Server dieselbe Version haben.

In der folgenden Tabelle sind die Betriebssysteme aufgeführt, auf denen der NSLOG-Server unterstützt wird.

Betriebssystem	Softwareanforderungen	Bemerkungen
Windows	Windows XP Professional, Windows Server 2003, Windows 2000/NT, Windows Server 2008, Windows Server 2008 R2	
Linux	RedHat Linux 4 oder höher, SUSE Linux Enterprise 9.3 oder höher	
FreeBSD	FreeBSD 6.3 oder später	Verwenden Sie für NetScaler 10.5 nur FreeBSD 8.4.
Mac-Betriebssystem	Mac OS 8.6 oder neuer	Wird in NetScaler 10.1 und späteren Versionen nicht unterstützt.

Die minimalen Hardwarespezifikationen für die Plattform, auf der der NSLOG-Server ausgeführt wird, lauten wie folgt:

- Prozessor: Intel x86 ~501 Megahertz (MHz)
- RAM - 512 Megabyte (MB)
- Steuerung — SCSI

Installation des NSLOG-Servers auf dem Linux-Betriebssystem

Melden Sie sich als Administrator am Linux-System an. Gehen Sie wie folgt vor, um die ausführbaren Dateien des NSLOG-Servers auf dem System zu installieren.

Um das NSLOG-Serverpaket auf einem Linux-Betriebssystem zu installieren

1. Geben Sie an der Linux-Befehlszeile den folgenden Befehl ein, um die Datei NSauditserver.rpm in ein temporäres Verzeichnis zu kopieren:

   ```
   cp <path_to_cd>/Utilities/auditserver/Linux/NSauditserver.rpm /tmp
   ```

2. Geben Sie den folgenden Befehl ein, um die Datei NSauditserver.rpm zu installieren.

   rpm -i NSauditserver.rpm

   Mit diesem Befehl werden die Dateien extrahiert und in den folgenden Verzeichnissen installiert:

   - /usr/local/netscaler/etc

- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

So deinstallieren Sie das NSLOG-Serverpaket auf einem Linux-Betriebssystem

1. Geben Sie in der Befehlszeile den folgenden Befehl ein, um die Audit-Serverprotokollierungsfunktion zu deinstallieren:

   ```
   rpm -e NSauditserver
   ```

2. Verwenden Sie den folgenden Befehl, um weitere Informationen zur NSAditServer-RPM-Datei zu erhalten:

   ```
   rpm -qpi \*.rpm
   ```

3. Verwenden Sie den folgenden Befehl, um die installierten Audit-Serverdateien anzuzeigen:

   ```
   rpm -qpl *.rpm
   ```

   `*.rpm`: Gibt den Dateinamen an.

Installieren des NSLOG-Servers auf dem FreeBSD-Betriebssystem

Bevor Sie den NSLOG-Server installieren können, müssen Sie das NSLOG-Paket von der NetScaler Produkt-CD kopieren oder von www.citrix.comherunterladen. Das NSLOG-Paket hat das folgende Namensformat:

`AuditServer_<release number>-<build number>.zip`

Beispiel: `AuditServer_10.5-58.11.zip`

Dieses Paket enthält Dateien für alle unterstützten Plattformen: Linux, Windows und FreeBSD. Installieren Sie auf einem FreeBSD-Betriebssystem das NSLOG-Paket, das das folgende Namensformat hat:

`audserver_bsd-<release number>-<build number>.tgz`

Beispiel: `audserver_bsd-10.5-58.11.tgz`

So laden Sie das NSLOG-Paket von www.citrix.com herunter:

1. Gehen Sie in einem Webbrowser zu www.citrix.com.
2. Klicken Sie in der Menüleiste auf **Anmelden**.
3. Geben Sie Ihre Anmeldeinformationen ein und klicken Sie dann auf **Anmelden**.
4. Klicken Sie in der Menüleiste auf **Downloads**.
5. **Wählen Sie in der Liste „Produkt auswählen“** die Option **NetScaler**aus.
6. **Wählen Sie auf der**NetScaler-Seite**die Version aus, für die Sie das NSLOG-Paket herunterladen möchten (z. B. Version 10.5), und wählen Sie dann Firmware aus.**

7. Wählen Sie unter **Firmware**die NetScaler-Firmware für die Build-Nummer aus, für die Sie das NSLOG-Paket herunterladen möchten.
8. Scrollen Sie auf der angezeigten Seite nach unten, wählen Sie **Audit-Server**aus und klicken Sie neben dem Paket, das Sie herunterladen möchten, auf **Datei** herunterladen.

Um das NSLOG-Serverpaket auf einem FreeBSD-Betriebssystem zu installieren

1. Auf dem System, auf das Sie das NSLOG-Paket `AuditServer_<release number>-<build number>.zip` heruntergeladen haben (z. B. `AuditServer_9.3-51.5.zip`) extrahieren Sie `FreeBSD NSLOG server package audserver_bsd-<release number>-<build number>.tgz` aus dem Paket (z. B. `audserver_bsd-9.3-51.5.tgz`).
2. Kopieren Sie das FreeBSD-NSLOG-Serverpaket `audserver_bsd-<release number>-<build number>.tgz` (zum Beispiel `audserver_bsd-9.3-51.5.tgz`) in ein Verzeichnis auf einem System, auf dem FreeBSD OS läuft.
3. Führen Sie in der Befehlszeile für das Verzeichnis, in das das FreeBSD-NSLOG-Serverpaket kopiert wurde, den folgenden Befehl aus, um das Paket zu installieren:

   `pkg_add audserver_bsd-<release number>-<build number>.tgz`

   Beispiel:

   ```
   pkg_add audserver_bsd-9.3-51.5.tgz
   <!--NeedCopy-->
   ```

   Die folgenden Verzeichnisse werden extrahiert:

   - `<root directory extracted from the FreeBSD NSLOG server package tgz file>NetScalerbin` (zum Beispiel `/var/auditserver/netscaler/bin`)
   - `<root directory extracted from the FreeBSD NSLOG server package tgz file>netscaler/etc` (zum Beispiel `/var/auditserver/netscaler/etc`)
   - `<root directory extracted from the FreeBSD NSLOG server package tgz file>\netscaler\samples` (zum Beispiel `/var/auditserver/samples`)
4. Geben Sie in der Befehlszeile den folgenden Befehl ein, um zu überprüfen, ob das Paket installiert ist:

   `pkg_info | grep NSaudserver`

Um das NSLOG-Serverpaket auf einem FreeBSD-Betriebssystem zu deinstallieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

`pkg_delete NSaudserver`

Installieren von NSLOG-Serverdateien auf dem Windows-Betriebssystem

Bevor Sie den NSLOG-Server installieren können, müssen Sie das NSLOG-Paket von der NetScaler Produkt-CD kopieren oder von www.citrix.comherunterladen. Das NSLOG-Paket hat das folgende Namensformat `AuditServer _<release number>-<build number>.zip` (z. B. `AuditServer_9.3-51.5.zip`). Dieses Paket enthält NSLOG-Installationspakete für alle unterstützten Plattformen.

So laden Sie das NSLOG-Paket von www.citrix.com herunter

1. Gehen Sie in einem Webbrowser zu www.citrix.com.
2. Klicken Sie in der Menüleiste auf Anmelden.
3. Geben Sie Ihre Anmeldeinformationen ein und klicken Sie dann auf Anmelden.
4. Klicken Sie in der Menüleiste auf Downloads.
5. Suchen Sie nach der Seite, die die entsprechende Versionsnummer und den entsprechenden Build enthält.
6. Klicken Sie auf dieser Seite unter Audit-Server auf Herunterladen, um das NSLOG-Paket mit dem Format `AuditServer_<release number>-<build number>.zip` auf Ihr lokales System herunterzuladen (z. B. `AuditServer_9.3-51.5.zip`).

So installieren Sie den NSLOG-Server auf einem Windows-Betriebssystem

1. Auf dem System, auf das Sie das NSLOG-Paket `AuditServer_<release number>-<build number>.zip` heruntergeladen haben (z. B. `AuditServer_9.3-51.5.zip`) extrahieren Sie `audserver_win-<release number>-<build number>.zip` aus dem Paket (z. B. `audserver_win-9.3-51.5.zip`).
2. Kopieren Sie die extrahierte Datei `audserver_<release number>-<build number>.zip` (z. B. `audserver_win-9.3-51.5.zip`) in ein Windows-System, auf dem Sie den NSLOG-Server installieren möchten.
3. Entpacken Sie die `audserver_<release number>-<build number>.zip` Datei (z. B. `audserver_win-9.3-51.5.zip`).
4. Die folgenden Verzeichnisse werden extrahiert:
   a) `<root directory extracted from the Windows NSLOG server package zip file>\bin`(zum Beispiel `C:\audserver_win-9.3-51.5\bin`)
   b) `<root directory extracted from the Windows NSLOG server package zip file>\etc` (zum Beispiel `C:\audserver_win-9.3-51.5\etc`)
   c) `<root directory extracted from the Windows NSLOG server package zip file>\samples` (zum Beispiel `C:\audserver_win-9.3-51.5\samples`)
5. Führen Sie in der Befehlszeile den folgenden Befehl von der `<root directory extracted from the Windows NSLOG server package zip file>\bin path`


```
audserver -install -f <directorypath>\auditlog.conf
```

<directorypath>: Gibt den Pfad zur Konfigurationsdatei (auditlog.conf) an. log.conf ist standardmäßig im Verzeichnis \<root directory extracted from Windows NSLOG server package zip file\>\samples. Sie können auditlog.conf jedoch in das gewünschte Verzeichnis kopieren.

So deinstallieren Sie den NSLOG-Server auf einem Windows-Betriebssystem

Führen Sie in der Befehlszeile aus dem <root directory extracted from Windows NSLOG server package zip file>\bin Pfad den folgenden Befehl aus:

```
audserver -remove
```

NSLOG-Server-Befehlsoptionen

Informationen zu NSLOG-Serverbefehlen finden Sie unter Audit-Server-Optionen.

Führen Sie den Befehl audserver aus dem Verzeichnis aus, in dem die ausführbare Datei des Auditservers vorhanden ist:

- Unter Windows: \ns\bin
- Unter Solaris und Linux:\usr\local\netscaler\bin

Die Konfigurationsdateien des Auditservers befinden sich in den folgenden Verzeichnissen:

- Unter Windows: \ns\etc
- Unter Linux: \usr\local\netscaler\etc

Die ausführbare Datei des Auditservers wird wie ./auditserver in Linux und FreeBSD gestartet.

Hinzufügen der NetScaler Appliance-IP-Adressen auf dem NSLOG-Server

Fügen Sie in der Konfigurationsdatei (auditlog.conf) die IP-Adressen der NetScaler-Appliances hinzu, deren Ereignisse protokolliert werden müssen.

So fügen Sie die IP-Adressen der NetScaler-Appliance hinzu

Geben Sie in der Befehlszeile den folgenden Befehl ein:

```
audserver -addns -f <directorypath\>\auditlog.conf
```

<directorypath>: Gibt den Pfad zur Konfigurationsdatei an (auditlog.conf).

Sie werden aufgefordert, die Informationen für die folgenden Parameter einzugeben:

NSIP: Gibt die IP-Adresse der NetScaler-Appliance an, z. B. 10.102.29.1.

Benutzer-ID: Gibt den Benutzernamen an, z. B. nsroot.

Passwort: Gibt das Passwort an, zum Beispiel nsroot.

Wenn Sie mehrere NetScaler-IP-Adressen (NSIP) hinzufügen und später nicht alle NetScaler-Appliance-Ereignisdetails protokollieren möchten, können Sie die NSIPs manuell löschen, indem Sie die NSIP-Anweisung am Ende der Datei auditlog.conf entfernen. Für ein Hochverfügbarkeits-Setup (HA) müssen Sie mithilfe des Befehls audserver sowohl primäre als auch sekundäre NetScaler-IP-Adressen zu auditlog.conf hinzufügen. Stellen Sie vor dem Hinzufügen der IP-Adresse sicher, dass der Benutzername und das Passwort auf dem System vorhanden sind.

Überprüfen der NSLOG-Serverkonfigurationsdatei

Überprüfen Sie die Konfigurationsdatei (`audit log.conf`) auf Syntaxkorrektheit, damit die Protokollierung starten und ordnungsgemäß funktionieren kann.

Um die Konfiguration zu überprüfen, geben Sie an der Befehlszeile den folgenden Befehl ein:

```
audserver -verify -f <directorypath>\auditlog.conf
```

`<directorypath>: Specifies the path to the configuration file (audit log.conf).`

Ausführen des NSLOG-Servers

January 19, 2021

So starten Sie die Protokollierung des Überwachungsservers

Geben Sie den folgenden Befehl an einer Eingabeaufforderung ein:

Audserver -start -f<directorypath>\auditlog.conf

<directorypath>: Gibt den Pfad zur Konfigurationsdatei an (audit log.conf).

So beenden Sie die Protokollierung von Überwachungs-Servern, die als Hintergrundprozess in FreeBSD oder Linux gestartet werden

Geben Sie den folgenden Befehl ein:

```
audserver -stop
```


So beenden Sie die Überwachungsserverprotokollierung, die als Dienst in Windows gestartet wird

Geben Sie den folgenden Befehl ein:

```
audserver -stopservice
```

Anpassen der Protokollierung auf dem NSLOG-Server

May 11, 2023

Sie können die Protokollierung auf dem NSLOG-Server anpassen, indem Sie zusätzliche Änderungen an der NSLOG-Serverkonfigurationsdatei (log.conf) vornehmen. Verwenden Sie einen Texteditor, um die log.conf-Konfigurationsdatei auf dem Serversystem zu ändern.

Um die Protokollierung anzupassen, verwenden Sie die Konfigurationsdatei, um Filter und Protokolleigenschaften zu definieren.

- **Filter protokollieren.** Filtern Sie Protokollinformationen von einer NetScaler-Appliance oder einer Reihe von NetScaler-Appliances.
- **Eigenschaften protokollieren.** Jeder Filter hat einen zugehörigen Satz von Protokolleigenschaften. Protokolleigenschaften definieren, wie die gefilterten Protokollinformationen gespeichert werden.

Dieses Dokument enthält die folgenden Details:

- Filter erstellen
- Protokolleigenschaften angeben

Erstellen von Filtern

Sie können die Standardfilterdefinition verwenden, die sich in der Konfigurationsdatei (audit log.conf) befindet, oder Sie können den Filter ändern oder einen neuen Filter erstellen. Sie können mehrere Protokollfilter erstellen.

> Hinweis: Wenn
> für die konsolidierte Protokollierung eine Protokolltransaktion stattfindet, für die es keine Filterdefinition gibt, wird der Standardfilter verwendet (sofern er aktiviert ist). Die einzige Möglichkeit, die konsolidierte Protokollierung aller NetScaler-Appliances zu konfigurieren, besteht darin, den Standardfilter zu definieren.

So erstellen Sie einen Filter

Geben Sie in der Befehlszeile den folgenden Befehl in die Konfigurationsdatei (auditlog.conf) ein:


```
filter <filterName> [IP <ip>] [NETMASK <mask>] ON | OFF]
<!--NeedCopy-->
```

Filtername: Geben Sie den Namen des Filters an (maximal 64 alphanumerische Zeichen).

ip: Geben Sie die IP-Adressen an.

Maske: Geben Sie die Subnetzmaske an, die in einem Subnetz verwendet werden soll.

Geben Sie ON an, damit der Filter Transaktionen protokollieren kann, oder geben Sie OFF an, um den Filter zu deaktivieren. Wenn kein Argument angegeben ist, ist der Filter aktiviert.

Beispiele:

```
filter F1 IP 192.168.100.151 ON
<!--NeedCopy-->
```

Um den Filter F2 auf die IP-Adressen 192.250.100.1 bis 192.250.100.254 anzuwenden:

```
filter F2 IP 192.250.100.0 NETMASK 255.255.255.0 ON
<!--NeedCopy-->
```

FilterName ist ein erforderlicher Parameter, wenn Sie einen Filter mit anderen optionalen Parametern wie der IP-Adresse oder der Kombination aus IP-Adresse und Netzmaske definieren.

Festlegen von Protokolleigenschaften

Die mit dem Filter verknüpften Protokolleigenschaften werden auf alle im Filter vorhandenen Protokolleinträge angewendet. Die Definition der Protokolleigenschaft beginnt mit dem Schlüsselwort BEGIN und endet mit END, wie im folgenden Beispiel dargestellt:

```
BEGIN <filtername>
    logFilenameFormat ...
    logDirectory ...
    logInterval ...
    logFileSizeLimit ....
END
<!--NeedCopy-->
```

Einträge in der Definition können Folgendes enthalten:

- **LogFileNameFormat** gibt das Format des Dateinamens der Protokolldatei an. Der Name der Datei kann aus folgenden Typen bestehen:
  - Statisch: Eine konstante Zeichenfolge, die den absoluten Pfad und den Dateinamen angibt.

- Dynamisch: Ein Ausdruck, der die folgenden Formatbezeichner enthält:
  - Datum (% {format} t)
  - erstellt einen Dateinamen mit NSIP

Beispiel:

```
LogFileNameFormat Ex%`{
`%m%d%y }
t.log
<!--NeedCopy-->
```

Dadurch wird der erste Dateiname als Exmmddyy.log erstellt. Neue Dateien haben die Namen: exMMDDYY.Log.0, exMMDDYY.Log.1 usw. Im folgenden Beispiel werden die neuen Dateien erstellt, wenn die Dateigröße 100 MB erreicht.

Beispiel:

```
LogInterval size
LogFileSize 100
LogFileNameFormat Ex%`{
`%m%d%y }
t
<!--NeedCopy-->
```

> **Achtung**
>
> Das im Parameter LogFileNameFormat angegebene Datumsformat %t überschreibt die Protokollintervalleigenschaft für diesen Filter. Um zu verhindern, dass jeden Tag eine neue Datei erstellt wird und nicht erst, wenn die angegebene Größe der Protokolldatei erreicht ist, verwenden Sie %t nicht im Parameter LogFileNameFormat.

- **LogDirectory** gibt das Verzeichnisnamenformat der Protokolldatei an. Der Name der Datei kann einer der folgenden sein:
  - Statisch: Ist eine konstante Zeichenfolge, die den absoluten Pfad und Dateinamen angibt.
  - Dynamisch: Ist ein Ausdruck, der die folgenden Formatbezeichner enthält:
    - Datum (% {format} t)
    - erstellt ein Verzeichnis mit NSIP

  Das Verzeichnistrennzeichen hängt vom Betriebssystem ab. Verwenden Sie in Windows das Verzeichnistrennzeichen.

  Beispiel:

```
LogDirectory dir1\dir2\dir3
<!--NeedCopy-->
```


Verwenden Sie in den anderen Betriebssystemen (Linux, FreeBSD usw.) das Verzeichnistrennzeichen.

- **LogInterval** gibt das Intervall an, in dem neue Logdateien erstellt werden. Verwenden Sie einen der folgenden Werte:
  - Stündlich: Jede Stunde wird eine Datei erstellt. Standardwert.
  - Täglich: Jeden Tag um Mitternacht wird eine Datei erstellt.
  - Wöchentlich: Jeden Sonntag um Mitternacht wird eine Datei erstellt.
  - Monatlich: Eine Datei wird am ersten Tag des Monats um Mitternacht erstellt.
  - Keine: Eine Datei wird nur einmal erstellt, wenn die Protokollierung des Auditservers beginnt.
  - Größe: Eine Datei wird nur erstellt, wenn die maximale Größe der Protokolldatei erreicht ist.

  Beispiel:

  ```
  LogInterval Hourly
  <!--NeedCopy-->
  ```

  - **LogFileSizeLimit** gibt die maximale Größe (in MB) der Protokolldatei an. Eine neue Datei wird erstellt, wenn das Limit erreicht ist.

  > **Hinweis**
  >
  > Sie können die Eigenschaft loginterval überschreiben, indem Sie Größe als Wert zuweisen.

  Die Standardeinstellung LogFileSizeLimit ist 10 MB.

  Beispiel:

  ```
  LogFileSizeLimit 35
  <!--NeedCopy-->
  ```

SYSLOG Über TCP

May 11, 2023

Syslog ist ein Standard für das Senden von Ereignisbenachrichtigungen. Diese Nachrichten können lokal oder auf einem externen Logserver gespeichert werden. Syslog ermöglicht es Netzwerkadministratoren, Protokollmeldungen zu konsolidieren und Erkenntnisse aus den gesammelten Daten abzuleiten.

Syslog wurde ursprünglich für die Verwendung über UDP entwickelt, wodurch eine große Datenmenge innerhalb desselben Netzwerks mit minimalem Paketverlust übertragen werden kann.

Telekommunikationsbetreiber bevorzugen jedoch die Übertragung von Syslog-Daten über TCP, da sie eine zuverlässige, geordnete Datenübertragung zwischen Netzwerken benötigen. Beispielsweise verfolgt das Telekommunikationsunternehmen die Benutzeraktivitäten, und TCP sorgt für eine erneute Übertragung im Falle eines Netzwerkausfalls.

So funktioniert Syslog over TCP

Um zu verstehen, wie Syslog über TCP funktioniert, sollten Sie zwei hypothetische Fälle betrachten:

Sam, ein Netzwerkadministrator, möchte wichtige Ereignisse auf einem externen Syslog-Server protokollieren.

XYZ Telecom, ein ISP, muss eine erhebliche Menge an Daten auf Syslog-Servern übertragen und speichern, um die gesetzlichen Vorschriften einzuhalten.

In beiden Fällen müssen die Protokollmeldungen über einen zuverlässigen Kanal übertragen und sicher auf einem externen Syslog-Server gespeichert werden. Im Gegensatz zu UDP stellt TCP eine Verbindung her, überträgt Nachrichten sicher und überträgt alle Daten, die aufgrund eines Netzwerkausfalls beschädigt sind oder verloren gehen, erneut (vom Absender zum Empfänger).

Die NetScaler-Appliance sendet Protokollnachrichten über UDP an den lokalen Syslog-Daemon und sendet Protokollnachrichten über TCP oder UDP an externe Syslog-Server.

SNIP-Unterstützung für Syslog

Wenn das Audit-Log-Modul Syslog-Meldungen generiert, verwendet es eine NetScaler-IP-Adresse (NSIP) als Quelladresse für das Senden der Nachrichten an einen externen Syslog-Server. Um ein SNIP als Quelladresse zu konfigurieren, müssen Sie es zu einem Teil der NetProfile-Option machen und das NetProfile an die Syslog-Aktion binden.

> **Hinweis**
>
> TCP verwendet SNIP zum Senden von Überwachungstests, um die Konnektivität zu überprüfen, und sendet dann die Protokolle über NSIP. Daher muss der Syslog-Server über SNIP erreichbar sein. Netzprofile können verwendet werden, um den gesamten TCP-Syslog-Verkehr vollständig über SNIP umzuleiten.

Die Verwendung einer SNIP-Adresse wird in der internen Protokollierung nicht unterstützt.

Vollqualifizierter Domainnamen-Support für Audit-Log

Bisher wurde das Audit-Log-Modul mit der Ziel-IP-Adresse des externen Syslog-Servers konfiguriert, an den die Protokollmeldungen gesendet werden. Jetzt verwendet der Audit-Log-Server einen vollqualifizierten Domänennamen (FQDN) anstelle der Ziel-IP-Adresse. Die FQDN-Konfiguration löst den

konfigurierten Domänennamen des Syslog-Servers auf die entsprechende Ziel-IP-Adresse auf, um die Protokollmeldungen vom Audit-Log-Modul zu senden. Der Nameserver muss ordnungsgemäß konfiguriert sein, um den Domainnamen zu lösen und Probleme mit domänenbasierten Diensten zu vermeiden.

> **Hinweis**
>
> Bei der Konfiguration eines FQDN wird die Konfiguration des Serverdomänennamens derselben NetScaler-Appliance in der Syslog-Aktion oder der NSlog-Aktion nicht unterstützt.

Konfiguration von Syslog über TCP über die Befehlszeilenschnittstelle

So konfigurieren Sie eine NetScaler Appliance für das Senden von Syslog-Nachrichten über TCP über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
          domainResolveRetry <integer>]) | -lbVserverName<string>))[-
          serverPort <port>] -logLevel <logLevel>[-dateFormat <dateFormat
          >] [-logFacility <logFacility>]   [-tcp ( NONE | ALL )] [-acl (
          ENABLED | DISABLED )][-timeZone ( GMT_TIME | LOCAL_TIME )][-
          userDefinedAuditlog ( YES | NO )][-appflowExport ( ENABLED |
          DISABLED )] [-lsn ( ENABLED | DISABLED )][-alg ( ENABLED |
          DISABLED )] [-subscriberLog ( ENABLED | DISABLED )][-transport (
           TCP | UDP )] [-tcpProfileName <string>][-maxLogDataSizeToHold <
          positive_integer>][-dns ( ENABLED | DISABLED )] [-netProfile <
          string>]
2 <!--NeedCopy-->
```

```
1     add audit syslogaction audit-action1 10.102.1.1 -loglevel
          INFORMATIONAL -dateformat MMDDYYYY -transport TCP
2 <!--NeedCopy-->
```

Hinzufügen der SNIP-IP-Adresse zur Netzprofiloption über die Befehlszeilenschnittstelle

So fügen Sie dem Netzwerkprofil über die Befehlszeilenschnittstelle eine SNIP-IP-Adresse hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
1     add netProfile <name> [-td <positive_integer>] [-srcIP <string>][-
          srcippersistency ( ENABLED | DISABLED )][-overrideLsn ( ENABLED
          | DISABLED )]add syslogaction <name> <serverIP>  - loglevel all
           - netprofile net1
2 <!--NeedCopy-->
```



```
1     add netprofile net1  -srcip 10.102.147.204`
2 <!--NeedCopy-->
```

Wobei, srCip ist das SNIP.

Hinzufügen von Netzprofilen in einer Syslog-Aktion über die Befehlszeilenschnittstelle

So fügen Sie eine NetProfile-Option in einer Syslog-Aktion über die Befehlszeilenschnittstelle hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
1      add audit syslogaction <name> (<serverIP> | -lbVserverName <string
           >)  -logLevel <logLevel>
2     -netProfile <string> …
3
4 <!--NeedCopy-->
```

```
1     add syslogaction sys_act1 10.102.147.36  -loglevel all  -netprofile
          net1
2 <!--NeedCopy-->
```

Wobei -netprofile den Namen des konfigurierten Netzprofils angibt. Die SNIP-Adresse ist als Teil des NetProfile konfiguriert und diese NetProfile-Option ist an die Syslog-Aktion gebunden.

> **Hinweis:**
>
> Sie müssen das NetProfile immer an die SYSLOGUDP- oder SYSLOGTCP-Dienste binden, die an den virtuellen Lastausgleichsserver SYSLOGUDP oder SYSLOGTCP gebunden sind.

Konfiguration der FQDN-Unterstützung über die Befehlszeilenschnittstelle

So fügen Sie einer Syslog-Aktion über die Befehlszeilenschnittstelle einen Serverdomänennamen hinzu

Geben Sie in der Befehlszeile Folgendes ein:

```
1 add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
     domainResolveRetry <integer>]) | -lbVserverName <string>)) -logLevel
      <logLevel> ...
2     set audit syslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>]-
        serverDomainName <string>] [-lbVserverName <string>]-
        domainResolveRetry <integer>] [-domainResolveNow]
3 <!--NeedCopy-->
```


So fügen Sie einer NSlog-Aktion über die Befehlszeilenschnittstelle einen Serverdomänennamen hinzu.

Geben Sie in der Befehlszeile Folgendes ein:

```
1     add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
          domainResolveRetry <integer>]))  -logLevel <logLevel> ...
2     set audit nslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
          serverDomainName <string>] [-domainResolveRetry <integer>][-
          domainResolveNow]
3 <!--NeedCopy-->
```

Wobei serverDomainName. Domänenname des Logservers. Schließt sich gegenseitig mit serverIP / lbVserverName aus.

DomainResolveRetry - Ganzzahl. Zeit (in Sekunden), die die NetScaler-Appliance wartet, nachdem eine DNS-Auflösung ausgefallen ist, bevor sie die nächste DNS-Abfrage zur Auflösung des Domainnamens sendet.

DomainJetzt lösen. Inbegriffen, wenn die DNS-Abfrage sofort gesendet werden muss, um den Domainnamen des Servers aufzulösen.

Konfiguration von Syslog über TCP mithilfe der GUI

So konfigurieren Sie die NetScaler-Appliance so, dass sie Syslog-Nachrichten über TCP mithilfe der GUI sendet

1. **Navigieren Sie zu**System**>**Auditing**>**Syslog**und wählen Sie die Registerkarte Server aus.**
2. Klicken Sie auf **Hinzufügen** und wählen Sie als Transporttyp **TCP**aus.

Konfiguration eines Netzprofils für die SNIP-Unterstützung mithilfe der GUI

So konfigurieren Sie das Netzprofil für die SNIP-Unterstützung mithilfe der GUI

1. Navigieren Sie zu **System > Auditing > Syslog** und wählen Sie die Registerkarte **Server** aus.
2. Klicken Sie auf **Hinzufügen** und wählen Sie ein Netzprofil aus der Liste aus.

Konfiguration von FQDN mithilfe der GUI

So konfigurieren Sie FQDN mithilfe der GUI

1. **Navigieren Sie zu**System**>**Auditing**>**Syslog**und wählen Sie die Registerkarte Server aus.**
2. Klicken Sie auf **Hinzufügen** und wählen Sie einen Servertyp und einen Serverdomänennamen aus der Liste aus.

SYSLOG-Server mit Lastenausgleich

May 11, 2023

Die NetScaler Appliance sendet ihre SYSLOG-Ereignisse und -Meldungen an alle konfigurierten externen Protokollserver. Dies führt zur Speicherung redundanter Nachrichten und erschwert die Überwachung für Systemadministratoren. Um dieses Problem zu beheben, bietet die NetScaler-Appliance Lastausgleichsalgorithmen, mit denen die SYSLOG-Meldungen für eine bessere Wartung und Leistung zwischen den externen Protokollservern ausgeglichen werden können. Zu den unterstützten Lastausgleichsalgorithmen gehören RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets und AuditlogHash.

Load-Balancing von SYSLOG-Servern über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

1. Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   ```
   add service <name>(<IP> | <serverName>)<serviceType (SYSLOGTCP |
   SYSLOGUDP)> <port>
   ```

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP und die Lastausgleichsmethode als AUDITLOGHASH an.

   ```
   add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
   <AUDITLOGHASH>]
   ```

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.

   ```
   Bind lb vserver <name> <serviceName>
   ```

4. Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

   ```
   add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
   ```

5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

   ```
   add syslogpolicy <name> <rule> <action>
   ```

6. Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

   ```
   bind system global <policyName>
   ```

Load-Balancing von SYSLOG-Servern über die GUI

1. Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   Navigieren Sie zu **Traffic Management** > **Services**, klicken Sie auf **Hinzufügen** und wählen Sie **SYLOGTCP** oder **SYSLOGUDP** als Protokoll aus.

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP und die Lastausgleichsmethode als AUDITLOGHASH an.

   Navigieren Sie zu **Traffic Management** > **Virtuelle Server**, klicken Sie auf **Hinzufügen** und wählen Sie **SYLOGTCP oder**SYSLOGUDP** als Protokoll aus.

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.

   Navigieren Sie zu **Traffic Management** > **Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie dann **AUDITLOGHASH in der LoadBalancing-Methode**

4. Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

   Navigieren Sie zu **System** > **Überwachung**, klicken Sie auf **Server** und fügen Sie einen Server hinzu, indem Sie unter **Server** die Option **LB Vserver** auswählen.

5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

   Navigieren Sie zu **System** > **Syslog**, klicken Sie auf **Richtlinien**, und fügen Sie eine SYSLOG-Richtlinie hinzu.

6. Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

   Navigieren Sie zu **System** > **Syslog**, wählen Sie eine SYSLOG-Richtlinie aus, und klicken Sie auf **Aktion**. Klicken Sie dann auf **Globale Bindungen**, und binden Sie die Richtlinie an System Global.

Beispiel:

Die folgende Konfiguration legt den Lastausgleich von SYSLOG-Meldungen zwischen den externen Protokollservern fest, wobei AUDITLOGHASH als Load-Balancing-Methode verwendet wird. Die Last der AUDITLOGHASH-Methode gleicht den Datenverkehr basierend auf dem Eingabe-Hashwert der Audit-Agents aus. Die Agents sind die Module, die Auditlog in einer NetScaler-Appliance generieren. Wenn beispielsweise ein Agent-LSN Auditlogs basierend auf der Client-IP-Adresse ausbalancieren möchte, generiert das LSN-Modul den Hashwert basierend auf ClientIP und übergibt den Hashwert an das auditlog-Modul. Das auditlog-Modul sendet die Auditlog-Meldungen, die denselben Hashwert haben, an den externen Syslog-Server.

Die NetScaler-Appliance generiert SYSLOG-Ereignisse und -Meldungen, die einen Lastausgleich zwischen den Diensten Service1, Service2 und Dienst 3 aufweisen.

```
add service service1 192.0.2.10 SYSLOGUDP 514
add service service2 192.0.2.11 SYSLOGUDP 514
add service service3 192.0.2.11 SYSLOGUDP 514
add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
bind lb vserver lbvserver1 service1
bind lb vserver lbvserver1 service2
bind lb vserver lbvserver1 service3
```



```
add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
add syslogpolicy syspol1 ns_true sysaction1
bind system global syspol1
<!--NeedCopy-->
```

Verwenden Sie den folgenden Befehl, um SYSLOG unter Verwendung eines LB-Servers mit FQDN zu konfigurieren, wenn das ICMP-Paket blockiert ist:

```
set service service1 -healthMonitor NO
```

Einschränkungen:

- Die NetScaler-Appliance unterstützt keinen externen Lastenausgleich des virtuellen Servers, der die SYSLOG-Nachrichten zwischen den Protokollservern ausgleicht.

Standardeinstellungen für die Protokolleigenschaften

January 19, 2021

Im Folgenden finden Sie ein Beispiel für den Standardfilter mit Standardeinstellungen für die Protokolleigenschaften:

```
begin default
 logInterval Hourly
 logFileSizeLimit 10
 logFilenameFormat  auditlog%`{
 `%y%m%d }
 t.log
 end default
<!--NeedCopy-->
```

Im Folgenden finden Sie zwei Beispiele für die Definition der Standardfilter:

Beispiel 1:

```
Filter f1 IP 192.168.10.1
<!--NeedCopy-->
```

Dadurch wird eine Protokolldatei für NSI 192.168.10.1 mit den Standardwerten des Protokolls erstellt.

Beispiel 2:

```
Filter f1 IP 192.168.10.1
begin f1
    logFilenameFormat logfiles.log
end f1
```



```
<!--NeedCopy-->
```

Dadurch wird eine Protokolldatei für NSIP 192.168.10.1 erstellt. Da das Format des Protokolldateinamens angegeben wird, sind die Standardwerte der anderen Protokolleigenschaften wirksam.

Beispielkonfigurationsdatei (audit.conf)

May 17, 2023

Es folgt ein Beispiel für eine Konfigurationsdatei:

```
##############################
# This is the Auditserver configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##############################
MYIP <NSAuditserverIP>
MYPORT 3023
#   Filter filter_nsip  IP <Specify the NetScaler IP address to filter
    on > ON
#   begin filter_nsip
#       logInterval         Hourly
#       logFileSizeLimit    10
#       logDirectory         logdir\%A\
#       logFilenameFormat   nsip%\\{
 \\%d%m%Y }
 t.log
#   end filter_nsip
Filter default
begin default
    logInterval      Hourly
    logFileSizeLimit    10
    logFilenameFormat   auditlog%\{
 \%y%m%d }
 t.log
end default
<!--NeedCopy-->
```


Webserver-Protokollierung

May 11, 2023

Sie können die Webserver-Protokollierungsfunktion verwenden, um Protokolle von HTTP- und HTTPS-Anfragen zum Speichern und Abrufen an ein Clientsystem zu senden. Diese Funktion besteht aus zwei Komponenten:

- Der Web-Log-Server, der auf dem NetScaler läuft.
- Der NetScaler Web Logging (NSWL) -Client, der auf dem Clientsystem ausgeführt wird.

Wenn Sie den NetScaler Web Logging (NSWL) -Client ausführen:

1. Es stellt eine Verbindung zum NetScaler her.
2. Der NetScaler puffert die HTTP- und HTTPS-Anforderungsprotokolleinträge, bevor er sie an den Client sendet.
3. Der Client kann die Einträge filtern, bevor er sie speichert.

Um die Webserver-Protokollierung zu konfigurieren, aktivieren Sie zunächst die Weblogging-Funktion auf dem NetScaler und konfigurieren die Größe des Puffers für das temporäre Speichern der Protokolleinträge. Anschließend installieren Sie NSWL auf dem Clientsystem. Anschließend fügen Sie die NetScaler-IP-Adresse (NSIP) zur NSWL-Konfigurationsdatei hinzu. Sie können jetzt den NSWL-Client starten, um mit der Protokollierung zu beginnen. Sie können die Webserverprotokollierung anpassen, indem Sie zusätzliche Änderungen an der NSWL-Konfigurationsdatei (log.conf) vornehmen.

Konfiguration des NetScaler für die Webserver-Protokollierung

May 11, 2023

Um den NetScaler für die Webserverprotokollierung zu konfigurieren, müssen Sie nur die Webserver-Protokollierungsfunktion aktivieren. Optional können Sie die folgenden Konfigurationen durchführen:

- Ändern Sie die Größe des Puffers (Standardgröße ist 16 MB), in dem die protokollierten Informationen gespeichert werden, bevor sie an den NetScaler Web Logging (NSWL) -Client gesendet werden.
- Geben Sie die benutzerdefinierten HTTP-Header an, die Sie an den NSWL-Client exportieren möchten. Sie können maximal zwei HTTP-Request- und zwei HTTP-Response-Header-Namen konfigurieren.

So konfigurieren Sie die Webserver-Protokollierung mithilfe der Befehlszeilenschnittstelle

Führen Sie in der Befehlszeile die folgenden Operationen aus:

- Aktivieren Sie die Webserver-Protokollierungsfunktion.

  ```
  enable ns feature WL
  ```

- [Optional] Ändern Sie die Puffergröße zum Speichern der protokollierten Informationen.

  ```
  set ns weblogparam -bufferSizeMB <size>
  ```

  > **Hinweis**:
  >
  > Um Ihre Änderung zu aktivieren, müssen Sie die Webserver-Protokollierungsfunktion deaktivieren und dann erneut aktivieren.

- [Optional] Geben Sie die benutzerdefinierten HTTP-Header-Namen an, die Sie exportieren möchten.

  ```
  set ns weblogparam [-customReqHdrs <string> ...] [-customRspHdrs <
  string> ...]
  ```

```
    > enable ns feature WL
    Done
    > set ns weblogparam -bufferSizeMB 60
    Done
    > show ns weblogparam
        Web Logging parameters:
        Log buffer size:  60MB
        Custom HTTP request headers: (none)
        Custom HTTP response headers: (none)
    Done
    > set ns weblogparam -customReqHdrs req1 req2 -customRspHdrs res1
       res2
    Done
    > show ns weblogparam
        Web Logging parameters:
        Log buffer size:  60MB
        Custom HTTP request headers: req1, req2
        Custom HTTP response headers: res1, res2
    Done
<!--NeedCopy-->
```

So konfigurieren Sie die Webserver-Protokollierung mithilfe der GUI

1. Navigieren Sie zu **System** > **Einstellungen** und führen Sie die folgenden Operationen aus:

a) Um die Webserver-Logging-Funktion zu aktivieren, klicken Sie auf **Erweiterte Funktionen ändern** und wählen Sie **Webloggingaus**.
b) Um die Puffergröße zu ändern, klicken Sie auf **Globale Systemeinstellungen ändern** und geben Sie unter **Webloggingdie** Puffergröße ein.
c) Um die benutzerdefinierten HTTP-Header anzugeben, die exportiert werden sollen, klicken Sie auf **Globale Systemeinstellungen ändern** und geben Sie unter **Webprotokollierung** die Header-Werte an.

Installation des NetScaler Web Logging (NSWL) -Clients

May 11, 2023

Wenn Sie NSWL installieren, wird die ausführbare Clientdatei (NSWL) zusammen mit anderen Dateien installiert. Die ausführbare NSWL-Datei enthält eine Liste der Optionen, die Sie verwenden können. Weitere Informationen finden Sie unter Konfigurieren des NSWL-Clients.

> **Achtung**
>
> Die Version des NSWL-Clients muss mit der von NetScaler übereinstimmen. Wenn die Version von NetScaler beispielsweise 10.1 Build 125.9 ist, muss der NSWL-Client ebenfalls dieselbe Version haben. Außerdem funktioniert der Weblogging-Client (NSWL) sowohl auf 32-Bit- als auch auf 64-Bit-Servercomputern. Die Download-Seite hat nur einen 32-Bit-Weblog-Client. Der 64-Bit-Weblog-Client ist auf Anfrage erhältlich und empfiehlt Ihnen, sich für weitere Informationen an den NetScaler-Support zu wenden.

In der folgenden Tabelle sind die Betriebssysteme aufgeführt, auf denen der NSWL-Client installiert werden kann.

Betriebssystem	**Version**	**Hardwareanforderungen**	**Bemerkungen**
—	—	—	—
Windows	Windows Server 2016 oder höher	Prozessor — x86/amd64-CPU (1 GHz oder höher), RAM - 4 GB (oder höher)
macOS	macOS 8.6 oder höher	Wird auf NetScaler 10.1 und späteren Versionen nicht unterstützt.
Linux	Ubuntu, SUSE Linux, CentOS, Red Hat Enterprise Linux, 2016 oder später veröffentlicht	Prozessor — x86/amd64-CPU (1 GHz oder höher), RAM — 4 GB (oder höher)
Solaris	Solaris Sun OS 5.6 oder höher	Prozessor — UltraSparc-III 400 MHz, RAM - 512 MB, Controller — SCSI	Wird auf NetScaler 10.5 und späteren Versionen nicht unterstützt.
FreeBSD|FreeBSD 6.3 oder höher|Prozessor — x86/amd64-CPU (1 GHz oder höher), RAM - 4 GB (oder höher) |Verwenden Sie für NetScaler 10.5 nur FreeBSD 8.4.| |AIX|AIX 6.1|-|Wird von NetScaler 10.5 und späteren Versionen nicht unterstützt.

Wenn das NSWL-Clientsystem die Protokolltransaktion aufgrund einer CPU-Beschränkung nicht verarbeiten kann, läuft der Web-Log-Puffer über und der Protokollierungsprozess wird erneut initiiert.

> **Achtung**
>
> Eine erneute Initiierung der Protokollierung kann zum Verlust von Protokolltransaktionen führen.

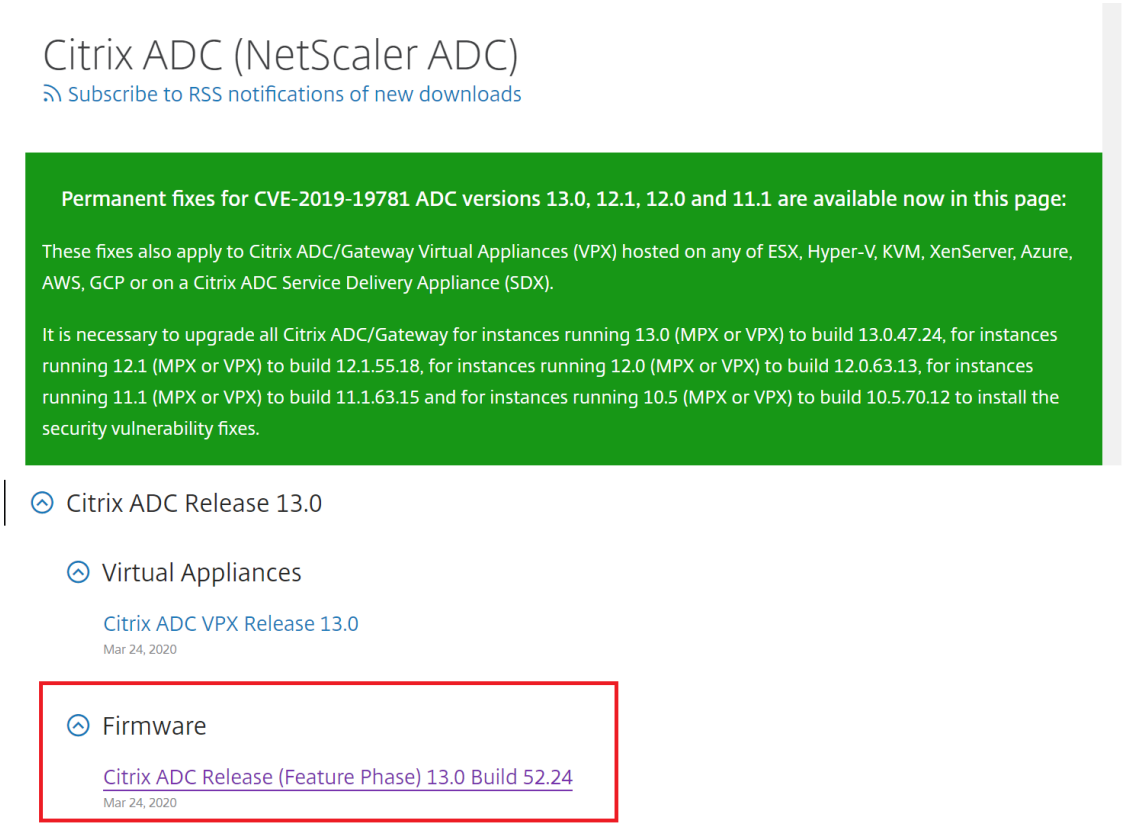
Um einen durch eine CPU-Beschränkung verursachten Engpass im NSWL-Clientsystem vorübergehend zu beheben, können Sie die Größe des Webserver-Logging-Puffers auf der NetScaler-Appliance anpassen. Um das Problem zu lösen, benötigen Sie ein Clientsystem, das den Durchsatz der Site bewältigen kann.

Laden Sie den NSWL-Client herunter

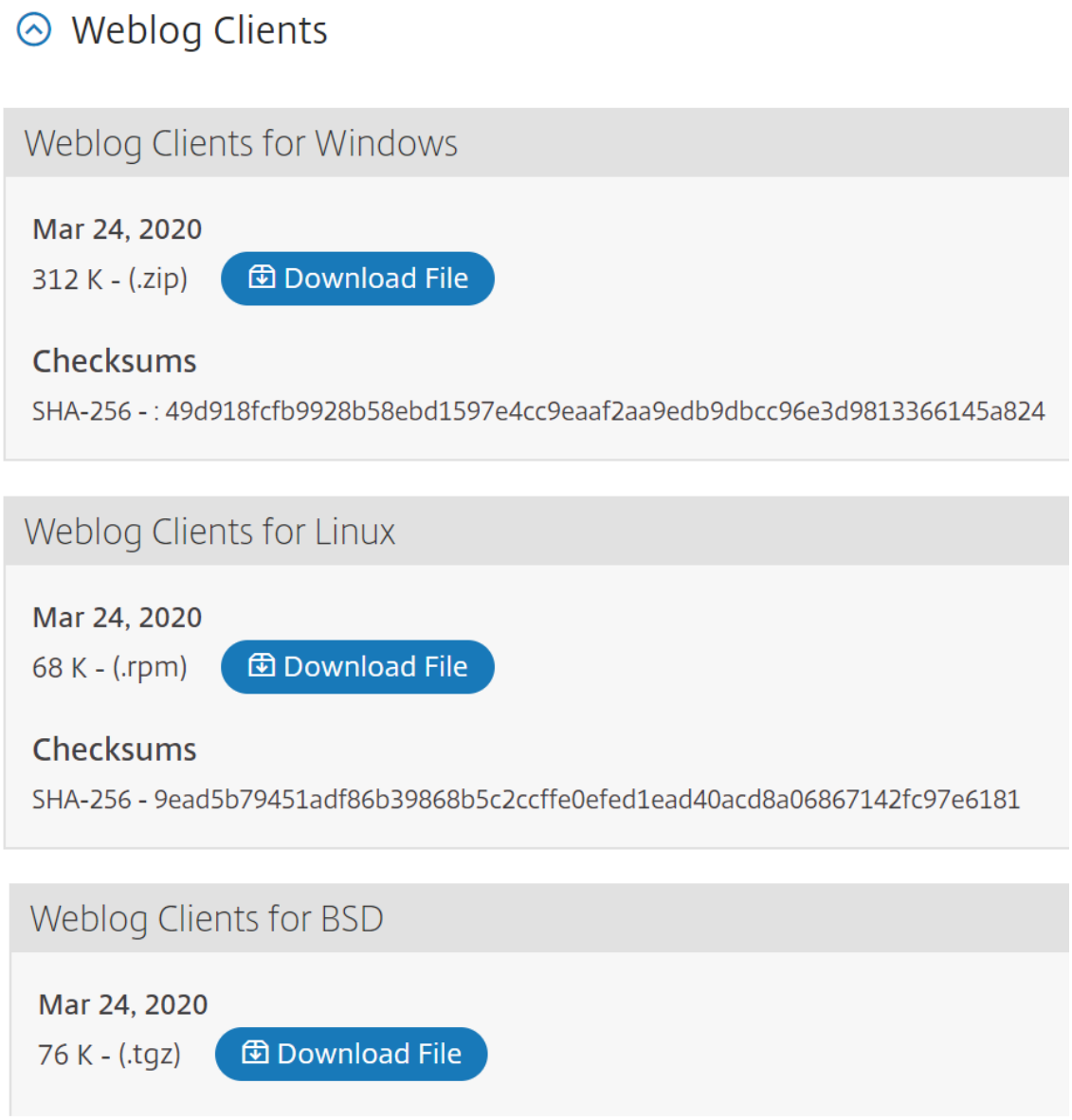
Sie können das NSWL-Clientpaket entweder von der NetScaler-Produkt-CD oder von der NetScaler-Downloadseite herunterladen. Innerhalb des Pakets gibt es separate Installationspakete für jede unterstützte Plattform.

So laden Sie den NSWL-Client von der Citrix-Website herunter

1. Melden Sie sich bei Citrix an, indem Sie auf die URL zugreifen `https://www.citrix.com/downloads/citrix-adc/`.
2. Navigieren Sie zu einer bestimmten NetScaler-Release-Version und suchen Sie nach der zugehörigen Firmware.
3. Klicken Sie auf **Firmware** (z. B. NetScaler Release (Feature Phase) 13.0 Build 52.24).



4. Gehen Sie auf der **Build-Seite für NetScaler Release (Feature Phase)** zum Abschnitt **Weblog-Clients** .
5. In diesem Abschnitt können Sie Weblog-Clients für Windows, Linux und BSD herunterladen.



Installieren Sie den NSWL-Client auf Solaris

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren Sie die `nswl_solaris-<release number>-<build number>.tar file` aus dem Paket.
2. Kopieren Sie die entpackte Datei auf ein Solaris-System, auf dem Sie den NSWL-Client installieren möchten.
3. Extrahieren Sie die Dateien aus der TAR-Datei mit dem folgenden Befehl:


```
tar xvf nswl_solaris-9.3-51.5.tar
```

Im temporären Verzeichnis wird ein Verzeichnis Weblog erstellt, und die Dateien werden in das Weblog-Verzeichnis extrahiert.

- Installieren Sie das Paket mit dem folgenden Befehl:

  ```
  pkgadd -d
  ```

- Die Liste der verfügbaren Pakete wird angezeigt. Im folgenden Beispiel wird ein Weblog-Paket gezeigt:

  ```
  1 NSweblog NetScaler Weblogging (SunOS,sparc)7.0
  ```

Sie werden aufgefordert, die Pakete auszuwählen. Wählen Sie die Paketnummer des Weblogs aus, das installiert werden soll.

Nachdem Sie die Paketnummer ausgewählt und die **Eingabetaste gedrückt**haben, werden die Dateien extrahiert und in den folgenden Verzeichnissen installiert:

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das NSWL-Paket installiert ist:

   ```
   pkginfo | grep NSweblog
   ```

2. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   pkgrm NSweblog
   ```

Installieren Sie den NSWL-Client unter Linux

> **Wichtig**
>
> Die Installation eines NSWL-Clients unter Linux ersetzt die Konfigurationsdatei. Sie müssen ein Backup erstellen, bevor Sie es installieren.

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren Sie die Datei `nswl_linux-<release number>-<build number>.rpm` aus dem Paket.
2. Kopieren Sie die entpackte Datei auf ein System mit Linux OS, auf dem Sie den NSWL-Client installieren möchten.
3. Führen Sie den folgenden Befehl aus, um das NSWL-Paket zu installieren:

   ```
   rpm -i nswl_linux-9.3-51.5.rpm
   ```


Mit diesem Befehl werden die Dateien extrahiert und in den folgenden Verzeichnissen installiert.

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   rpm -e NSweblog
   ```

2. Führen Sie den folgenden Befehl aus, um weitere Informationen zur Weblog-RPM-Datei zu erhalten:

   ```
   rpm -qpi *.rpm
   ```

3. Führen Sie den folgenden Befehl aus, um die installierten Webserver-Logging-Dateien anzuzeigen:

   ```
   rpm -qpl *.rpm
   ```

Installieren Sie den NSWL-Client auf FreeBSD

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren Sie die Datei nswl_bsd-<release number>-<build number>.tgz aus dem Paket.
2. Kopieren Sie die entpackte Datei auf ein System, auf dem FreeBSD OS läuft und auf dem Sie den NSWL-Client installieren möchten.
3. Führen Sie den folgenden Befehl aus, um das NSWL-Paket zu installieren:

   ```
   pkg_add nswl_bsd-9.3-51.5.tgz
   ```

Mit diesem Befehl werden die Dateien extrahiert und in den folgenden Verzeichnissen installiert.

```
1 -  /usr/local/netscaler/etc
2 -  /usr/local/netscaler/bin
3 -  /usr/local/netscaler/samples
```

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   pkg_delete NSweblog
   ```

2. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Paket installiert ist:

   ```
   pkg_info | grep NSweblog
   ```


Installieren Sie den NSWL-Client auf dem Mac

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren Sie die Datei `nswl_macos-<release number>-<build number>.tgz` aus dem Paket.
2. Kopieren Sie die entpackte Datei auf ein System, auf dem macOS ausgeführt wird und auf dem Sie den NSWL-Client installieren möchten.
3. Führen Sie den folgenden Befehl aus, um das NSWL-Paket zu installieren:

   ```
   pkg_add nswl_macos-9.3-51.5.tgz
   ```

Mit diesem Befehl werden die Dateien extrahiert und in den folgenden Verzeichnissen installiert:

- /usr/local/netscaler/usw
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   pkg_delete NSweblog
   ```

2. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Paket installiert ist:

   ```
   pkg_info | grep NSweblog
   ```

Installieren Sie den NSWL-Client unter Windows

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren Sie die Datei `nswl_win-<release number>-<build number>.zip` aus dem Paket.
2. Kopieren Sie die entpackte Datei auf ein Windows-System, auf dem Sie den NSWL-Client installieren möchten.
3. Entpacken Sie auf dem Windows-System die Datei in ein Verzeichnis (bezeichnet als `<NSWL-HOME>`). Die folgenden Verzeichnisse werden extrahiert: `/bin`, `/etc` und `/samples`.
4. Führen Sie in der Befehlszeile den folgenden Befehl aus `<NSWL-HOME>\bin directory`:

   ```
   nswl -install -f <directorypath>\log.conf
   ```

Hierbei gilt:

Der Verzeichnispfad bezieht sich auf den Pfad der Konfigurationsdatei (log.conf). Die Datei befindet sich standardmäßig im Verzeichnis `<NSWL-HOME>` und `/etc`. Sie können die Konfigurationsdatei in ein beliebiges anderes Verzeichnis kopieren.

> **Hinweis**
>
> Um den NSWL-Client zu deinstallieren, führen Sie an der Eingabeaufforderung den folgenden Befehl aus <NSWL-HOME>\bin directory:

```
1 > nswl -remove
```

Installieren Sie den NSWL-Client auf dem AIX-System

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren Sie die Datei nswl_aix-<release number>-<build number>.rpm aus dem Paket.
2. Kopieren Sie die entpackte Datei auf ein System, auf dem AIX OS ausgeführt wird und auf dem Sie den NSWL-Client installieren möchten.
3. Führen Sie den folgenden Befehl aus, um das NSWL-Paket zu installieren:

   ```
   rpm -i nswl_aix-9.3-51.5.rpm
   ```

Mit diesem Befehl werden die Dateien extrahiert und in den folgenden Verzeichnissen installiert.

- /usr/local/netscaler/etc
- /usr/local/netscaler/
- usr/local/netscaler/samples

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   rpm -e NSweblog
   ```

2. Führen Sie den folgenden Befehl aus, um weitere Informationen zur Weblog-RPM-Datei zu erhalten:

   ```
   rpm -qpi *.rpm
   ```

3. Führen Sie den folgenden Befehl aus, um die installierten Webserver-Logging-Dateien anzuzeigen:

   ```
   rpm -qpl *.rpm
   ```

Konfigurieren des NSWL-Clients

May 11, 2023

Nachdem Sie den NSWL-Client installiert haben, können Sie den NSWL-Client mithilfe der ausführbaren Datei nswl konfigurieren. Diese Konfigurationen werden in der NSWL-Client-Konfigurationsdatei (log.conf) gespeichert.

> **Hinweis:**
>
> Sie können die Protokollierung auf dem NSWL-Client weiter anpassen, indem Sie weitere Änderungen an der NSWL-Konfigurationsdatei (log.conf) vornehmen. Weitere Informationen finden Sie unter Anpassen der Protokollierung auf dem NSWL-Clientsystem.

In der folgenden Tabelle werden die Befehle beschrieben, mit denen Sie den NSWL-Client konfigurieren können.

NSWL-Befehl	Spezifiziert
nswl -help	Die verfügbaren NSWL-Hilfeoptionen.
nswl -addns -f <path-to-configuration-file>	Das System, das die Protokoll-Transaktionsdaten sammelt. Sie werden aufgefordert, die IP-Adresse der NetScaler-Appliance einzugeben. Geben Sie einen gültigen Benutzernamen und ein Kennwort ein.
nswl -verify -f <path-to-configuration-file>	Prüfen Sie die Konfigurationsdatei auf Syntax- oder Semantikfehler.
nswl -start -f <path-to-configuration-file>	Starten Sie den NSWL-Client basierend auf den Einstellungen in der Konfigurationsdatei. Hinweis: Für Solaris und Linux: Um die Web-Server-Protokollierung als Hintergrundprozess zu starten, geben Sie am Ende des Befehls das kaufmännische Und-Zeichen (&) ein.
nswl -stop (nur Solaris und Linux)	Stoppen Sie den NSWL-Client, falls er als Hintergrundprozess gestartet wurde. Andernfalls verwenden Sie STRG+C, um die Web-Server-Protokollierung zu beenden.
nswl -install -f <path-to-configuration-file> (nur Windows)	Installieren Sie den NSWL-Client als Dienst in Windows.

NSWL-Befehl	Spezifiziert
nswl -startservice (nur Windows)	Starten Sie den NSWL-Client, indem Sie die Einstellungen in der Konfigurationsdatei verwenden, die in der Installationsoption nswl angegeben ist. Sie können den NSWL-Client auch über **Start > Systemsteuerung > Dienste**starten. Hinweis: Die NSWL-Protokolldateien werden in C:\Windows\SysWOW64. erstellt
nswl -stopservice (nur Windows)	Beendet den NSWL-Client.
nswl -remove	Entfernen Sie den NSWL-Clientdienst aus der Registrierung.

Führen Sie die folgenden Befehle aus dem Verzeichnis aus, in dem sich die ausführbare NSWL-Datei befindet:

- `Windows: \ns\bin`
- `Solaris and Linux: \usr\local\netscaler\bin`

Die Konfigurationsdateien für die Web-Server-Protokollierung befinden sich im folgenden Verzeichnispfad:

- `Windows: \ns\etc`
- `Solaris and Linux: \usr\local\netscaler\etc`

Die ausführbare NSWL-Datei wird als gestartet. \ nswl unter Linux und Solaris.

Fügen Sie die IP-Adressen der NetScaler-Appliance hinzu

Fügen Sie in der NSWL-Client-Konfigurationsdatei (log.conf) die NetScaler IP-Adresse (NSIP) hinzu, von der der NSWL-Client mit dem Sammeln von Protokollen beginnt.

So fügen Sie die NSIP-Adresse der NetScaler-Appliance hinzu

1. Geben Sie an der Eingabeaufforderung des Clientsystems Folgendes ein:

   ```
   nswl -addns -f < directorypath > \log.conf
   < directorypath >: Specifies the path to the configuration file (log.
   conf).
   ```

2. Geben Sie bei der nächsten Eingabeaufforderung die folgenden Informationen ein:

   - **NSIP**: Geben Sie die IP-Adresse der NetScaler-Appliance an.

- Benutzername und Kennwort: Geben Sie die nsroot-Benutzeranmeldeinformationen der NetScaler-Appliance an.

  > **Hinweis:**
  >
  > Jeder Systembenutzer mit aktivierter Protokollierungsberechtigung unterstützt diese Funktionalität.

> **Hinweis:**
>
> Wenn Sie mehrere NetScaler IP-Adressen (NSIP) hinzufügen und später nicht alle Details des NetScaler-Systemprotokolls protokollieren möchten, können Sie die NSIPs manuell löschen, indem Sie die NSIP-Anweisung am Ende der Datei log.conf entfernen. Während eines Failover-Setups müssen Sie der log.conf sowohl primäre als auch sekundäre NetScaler-IP-Adressen hinzufügen, indem Sie den Befehl verwenden. Stellen Sie vor dem Hinzufügen der IP-Adresse sicher, dass der Benutzername und das Kennwort auf den NetScaler-Appliances vorhanden sind.

Überprüfen Sie die NSWL-Konfigurationsdatei

Um sicherzustellen, dass die Protokollierung korrekt funktioniert, überprüfen Sie die NSWL-Konfigurationsdatei (log.conf) auf dem Clientsystem auf Syntaxfehler.

So überprüfen Sie die Konfiguration in der NSWL-Konfigurationsdatei

Geben Sie an der Eingabeaufforderung des Clientsystems Folgendes ein:

```
nswl -verify -f <directorypath>\log.conf
```

< directorypath>: Gibt den Pfad zur Konfigurationsdatei (log.conf) an.

NSWL-Client ausführen

Starten der Webserver-Protokolle

Geben Sie an der Eingabeaufforderung des Clientsystems Folgendes ein:

```
nswl -start -f <directorypath>\log.conf
```

<directorypath>: Gibt den Pfad zur Konfigurationsdatei (log.conf) an.

Beenden der Web-Server-Protokollierung, die als Hintergrundprozess auf den Betriebssystemen Solaris oder Linux gestartet wurde

Geben Sie in der Befehlszeile Folgendes ein:

```
nswl -stop
```


So beenden Sie die Web-Server-Protokollierung, die als Dienst auf dem Windows-Betriebssystem gestartet wurde

Geben Sie in der Befehlszeile Folgendes ein:

```
nswl -stopservice
```

Anpassen der Protokollierung auf dem NSWL-Clientsystem

May 11, 2023

Sie können die Anmeldung am NetScaler Web Logging (NSWL) -Clientsystem anpassen, indem Sie weitere Änderungen an der NSWL-Clientkonfigurationsdatei (log.conf) vornehmen. Verwenden Sie einen Texteditor, um die Konfigurationsdatei log.conf auf dem Clientsystem zu ändern.

Um die Protokollierung anzupassen, verwenden Sie die Konfigurationsdatei, um Filter und Protokolleigenschaften zu definieren.

- **Filter protokollieren.** Filtern Sie Protokollinformationen basierend auf der Host-IP-Adresse, dem Domänennamen und dem Hostnamen der Webserver.
- **Eigenschaften protokollieren.** Jeder Filter hat einen zugehörigen Satz von Protokolleigenschaften. Protokolleigenschaften definieren, wie die gefilterten Protokollinformationen gespeichert werden.

Beispiel für eine Konfigurationsdatei

Es folgt ein Beispiel für eine Konfigurationsdatei:

```
1  ##########
2  # This is the NSWL configuration file
3  # Only the default filter is active
4  # Remove leading # to activate other filters
5  ##########
6  ##########
7  # Default filter (default on)
8  # W3C Format logging, new file is created every hour or on reaching 10
      MB file size,
9  # and the file name is Exyymmdd.log
10 ##########
11 Filter default
12 begin default
13         logFormat               W3C
14         logInterval             Hourly
15         logFileSizeLimit        10
```



```
        logFilenameFormat       Ex%`{
 `%y%m%d }
 t.log
end default
##########
# NetScaler caches example
# CACHE_F filter covers all the transaction with HOST name www.
   netscaler.com and the listed server ip's
##########
#Filter CACHE_F HOST www.netscaler.com IP 192.168.100.89 192.168.100.95
    192.168.100.52 192.168.100.53 ON
##########
# netscaler origin server example
# Not interested in Origin server to Cache traffic transaction logging
##########
#Filter ORIGIN_SERVERS IP 192.168.100.64 192.168.100.65 192.168.100.66
   192.168.100.67 192.168.100.225 192.168.100.226 192.168.
100.227 192.168.100.228 OFF
##########
# netscaler image server example
# all the image server logging.
##########
#Filter IMAGE_SERVER HOST www.netscaler.images.com IP 192.168.100.71
   192.168.100.72 192.168.100.169 192.168.100.170 192.168.10
0.171 ON
##########
# NCSA Format logging, new file is created every day midnight or on
   reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.
   log.
# Exclude objects that ends with .png .jpg .jar.
##########
#begin ORIGIN_SERVERS
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        40
#       logFilenameFormat       /datadisk5/ORGIN/log/%v/NS%`{
 `%m%d%y }
 t.log
#       logExclude              .png .jpg .jar
#end ORIGIN_SERVERS

##########
# NCSA Format logging, new file is created every day midnight or on
   reaching 20MB file size,
```



```
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log with log record timestamp as GMT.
##########
#begin CACHE_F
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk5/netscaler/log/%v/NS%`{ `%m%d%y }t.log
#       logtime                 GMT
#end CACHE_F

##########
# W3C Format logging, new file on reaching 20MB and the log file path name is
# atadisk6/netscaler/log/server's ip/Exmmyydd.log with log record timestamp as LOCAL.
##########
#begin IMAGE_SERVER
#       logFormat               W3C
#       logInterval             Size
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk6/netscaler/log/%AEx%`{ `%m%d%y }t
#       logtime                 LOCAL
#end IMAGE_SERVER

##########
# Virtual Host by Name firm, can filter out the logging based on the host name by,
##########

#Filter VHOST_F IP 10.101.2.151 NETMASK 255.255.255.0
#begin VHOST_F
#       logFormat               W3C
#       logInterval             Daily
#       logFileSizeLimit        10
logFilenameFormat /ns/prod/vhost/%v/Ex%`{ `%m%d%y }t
#end VHOST_F

########## END FILTER CONFIGURATION ##########
```



```
<!--NeedCopy-->
```

Erstellen von Filtern

Sie können die Standardfilterdefinition in der Konfigurationsdatei (log.conf) verwenden oder den Filter ändern oder einen Filter erstellen. Sie können mehrere Protokollfilter erstellen.

> **Hinweis:**
>
> Die konsolidierte Protokollierung, die Transaktionen protokolliert, für die kein Filter definiert ist, verwendet den Standardfilter, wenn er aktiviert ist. Die konsolidierte Protokollierung aller Server kann nur durch Definition des Standardfilters erfolgen.

Wenn der Server mehrere Websites hostet und jede Website einen eigenen Domänennamen hat und jede Domäne einem virtuellen Server zugeordnet ist, können Sie die Webserver-Protokollierung so konfigurieren, dass für jede Website ein separates Protokollverzeichnis erstellt wird. In der folgenden Tabelle werden die Parameter zum Erstellen eines Filters angezeigt.

Tabelle 1. Parameter für die Erstellung eines Filters

Parameter	Spezifiziert
Filtername	Name des Filters. Der Filtername kann alphanumerische Zeichen enthalten und darf nicht länger als 59 Zeichen sein. Filternamen, die länger als 59 Zeichen sind, werden auf 59 Zeichen abgeschnitten.
Hostname	Hostname des Servers, für den die Transaktionen protokolliert werden.
IP `ip`	IP-Adresse des Servers, für den Transaktionen protokolliert werden sollen (z. B. wenn der Server mehrere Domänen mit einer IP-Adresse hat).
IP `ip 2...ip` n:	Mehrere IP-Adressen (z. B. wenn die Serverdomäne über mehrere IP-Adressen verfügt).
ip6 IP	IPv6-Adresse des Servers, für den Transaktionen protokolliert werden sollen.
IP-IP-NETMASK-Maske	In einem Subnetz zu verwendende Kombination aus IP-Adressen und Netzwerkmasken.

Parameter	Spezifiziert
ON | OFF	Aktivieren oder Deaktivieren des Filters zur Protokollierung von Transaktionen Wenn kein Argument ausgewählt ist, ist der Filter aktiviert (EIN).

Um einen Filter zu erstellen, geben Sie in der Datei log.conf den folgenden Befehl ein:

- `filter <filterName> <HOST name> | [IP<ip> ] | [IP<ip 2...ip n> ] | <IP ip NETMASK mask> [ON | OFF]`
- `filter <filterName> <HOST name> | [IP6 ip/<prefix length>] [ON | OFF]`

Erstellen Sie einen Filter für einen virtuellen Server

Um einen Filter für einen virtuellen Server zu erstellen, geben Sie in der Datei log.conf den folgenden Befehl ein:

```
filter <filterName> <VirtualServer IP address>
```

Beispiel

Im folgenden Beispiel geben Sie eine IP-Adresse von 192.168.100.0 und eine Netzmaske von 255.255.255.0 an. Der Filter gilt für die IP-Adressen 192.168.100.1 bis 192.168.100.254.

```
1  Filter F1 HOST www.netscaler.com ON
2  Filter F2 HOST www.netscaler.com IP 192.168.100.151 ON
3  Filter F3 HOST www.netscaler.com IP 192.168.100.151 192.165.100.152 ON
4  Filter F4 IP 192.168.100.151
5  Filter F5 IP 192.168.100.151 HOST www.netscaler.com OFF
6  Filter F6 HOST www.netscaler.com HOST www.xyz.com HOST www.abcxyz.com
       IP 192.168.100.200 ON
7  Filter F7 IP 192.250.100.0 NETMASK 255.255.255.0
8  Filter F8 HOST www.xyz.com IP 192.250.100.0 NETMASK 255.255.255.0 OFF
9  For creating filters for servers having IPv6 addresses.
10 Filter F9 2002::8/112 ON
11 Filter F10 HOST www.abcd.com IP6 2002::8 ON
12
13 <!--NeedCopy-->
```


Geben Sie die Protokolleigenschaften an

Protokolleigenschaften werden auf alle Protokolleinträge angewendet, die mit dem Filter verknüpft sind. Die Definition der Protokolleigenschaft beginnt mit dem Schlüsselwort `BEGIN` und endet mit `END`, wie im folgenden Beispiel dargestellt:

```
BEGIN <filtername>
 logFormat ...
 logFilenameFormat ...
 logInterval ...
 logFileSize ....
 logExclude ....
 logTime ….
 END
<!--NeedCopy-->
```

Einträge in der Definition können Folgendes enthalten:

- **LogFormat** gibt die Webserverprotokollierungsfunktion an, die NCSA, W3C Extended und benutzerdefinierte Protokolldateiformate unterstützt.

Standardmäßig ist die Eigenschaft `logformat` w3c. Geben Sie zum Überschreiben custom oder NCSA in die Konfigurationsdatei ein, z. B.:

```
LogFormat NCSA
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für die NCSA- und benutzerdefinierten Protokollformate wird die Ortszeit verwendet, um Transaktionen zu zeitstempeln und für die Dateirotation.

- **LogInterval** gibt die Intervalle an, in denen neue Protokolldateien erstellt werden. Verwenden Sie einen der folgenden Werte:
  - Stündlich: Jede Stunde wird eine Datei erstellt.
  - Täglich: Jeden Tag um Mitternacht wird eine Datei erstellt. Standardwert.
  - Wöchentlich: Jeden Sonntag um Mitternacht wird eine Datei erstellt.
  - Monatlich: Eine Datei wird am ersten Tag des Monats um Mitternacht erstellt.
  - Keine: Eine Datei wird nur einmal erstellt, wenn die Web-Server-Protokollierung gestartet wird.

Beispiel:

```
LogInterval Daily
<!--NeedCopy-->
```


LogFileSizeLimit gibt die maximale Größe der Protokolldatei in MB an. Es kann mit jedem Protokollintervall (wöchentlich, monatlich usw.) verwendet werden. Eine Datei wird erstellt, wenn die maximale Dateigröße erreicht ist oder wenn die definierte Protokollintervall-Zeit verstrichen ist.

Um dieses Verhalten zu überschreiben, geben Sie die Größe als Eigenschaft `loginterval` an, damit eine Datei nur erstellt wird, wenn die Größenbeschränkung der Protokolldatei erreicht ist.

Die Standardeinstellung für `LogFileSizeLimit` ist 10 MB.

Beispiel:

```
LogFileSizeLimit 35
<!--NeedCopy-->
```

- **LogFileNameFormat** gibt das Format des Dateinamens der Protokolldatei an. Der Name der Datei kann aus folgenden Typen bestehen:
  - Statisch: Gibt eine konstante Zeichenfolge an, die den absoluten Pfad und den Dateinamen enthält.

    Dynamisch: Gibt einen Ausdruck an, der das folgende Format enthält:

    * Server-IP-Adresse
    * Datum (% {format} t)
    * URL-Suffix (%x)
    * Hostname (%v)

Beispiel:

```
LogFileNameFormat Ex%`{
 `%m%d%y }
 t.log
<!--NeedCopy-->
```

Dieser Befehl erstellt den ersten Dateinamen als Exmmddyy.log und erstellt dann jede Stunde eine Datei mit einem Dateinamen: ExmmDdyy.log.0, ExmmDdyy.Log.1,…, Exmmddyy.log.n.

Beispiel:

```
      LogInterval size
      LogFileSize 100
      LogFileNameFormat Ex%`{
 `%m%d%y }
 t
<!--NeedCopy-->
```


> **Achtung:**
>
> Das im Befehl LogFileNameFormat angegebene Datumsformat%t überschreibt die Protokollintervall-Eigenschaft für diesen Filter. Um zu verhindern, dass täglich eine neue Datei erstellt wird, anstatt wenn die angegebene Protokolldateigröße erreicht ist, verwenden Sie nicht %t im LogFileName-Format.

- **LogexClude** verhindert das Protokollieren von Transaktionen mit den angegebenen Dateinamenerweiterungen.

Beispiel:

```
LogExclude.html
<!--NeedCopy-->
```

Mit diesem Befehl wird eine Protokolldatei erstellt, die Protokolltransaktionen für *.html-Dateien ausschließt.

LogTime gibt die Protokollzeit entweder als GMT oder LOCAL an.

Die Standardeinstellungen sind:

- NCSA-Protokolldateiformat: LOCAL
- W3C-Protokolldateiformat: GMT.

Verstehen Sie die NCSA- und W3C-Protokollformate

Der NetScaler unterstützt die folgenden Standardprotokolldateiformate:

- Allgemeines NCSA-Protokollformat
- Erweitertes W3C-Protokollformat

NCSA: Allgemeines Protokollformat

Wenn das Protokolldateiformat NCSA ist, zeigt die Protokolldatei Protokollinformationen im folgenden Format an:

```
Client_IP_address -User_Name [Date:Time -TimeZone] "Method Object
    HTTP_version" HTTP_StatusCode BytesSent
<!--NeedCopy-->
```

Um das NCSA Common Protokollformat zu verwenden, geben Sie **NCSA** in das Argument LogFormat in der Datei `log.conf` ein.

In der folgenden Tabelle wird das Protokollformat von NCSA Common beschrieben.

Argument	Spezifiziert
Client_IP_Adresse	Die IP-Adresse des Clientcomputers.
Benutzername	Der Benutzername.
Datum	Das Datum der Transaktion.
Zeit	Der Zeitpunkt, zu dem die Transaktion abgeschlossen wurde.
Zeitzone	Die Zeitzone (Greenwich Mean Time oder Ortszeit).
Methode	Die Anforderungsmethode (z. B. GET, POST).
Objekt	Die URL.
HTTP_version	Die vom Client verwendete HTTP-Version.
HTTP_StatusCode	Der Statuscode in der Antwort.
Byte gesendet	Die Anzahl der vom Server gesendeten Byte.

W3C erweitertes Protokollformat

Eine erweiterte Protokolldatei enthält eine Folge von Zeilen mit ASCII-Zeichen, die entweder durch einen Line Feed (LF) oder die Sequenz Carriage Return Line Feed (CRLF) abgeschlossen sind. Protokolldateigeneratoren müssen die Konvention für die Leitungsbeendigung für die Plattform einhalten, auf der sie ausgeführt werden.

Protokollanalysatoren müssen entweder LF- oder CRLF-Formular akzeptieren. Jede Zeile kann entweder eine Direktive oder einen Eintrag enthalten. Wenn Sie das W3C Extended Logformat verwenden möchten, geben Sie W3C als Log-Format Argument in der Datei log.conf ein.

Standardmäßig ist das Standard-W3C-Protokollformat intern als benutzerdefiniertes Protokollformat definiert, wie folgt dargestellt:

```
%`{
 `%Y-%m-%d%H:%M:%S }
 t %a %u %S %A %p %m %U %q %s %j %J %T %H %+{
 user-agent }
 i %+{
 cookie }
  i%+{
 referer }
 i
<!--NeedCopy-->
```


Sie können auch die Reihenfolge ändern oder einige Felder in diesem W3C-Protokollformat entfernen. Zum Beispiel:

```
logFormat W3C %`{
 `%Y-%m-%d%H:%M:%S }
 t %m %U
<!--NeedCopy-->
```

W3C-Protokolleinträge werden mit dem folgenden Format erstellt:

```
#Version: 1.0
#Fields: date time cs-method cs-uri
#Date: 12-Jun-2001 12:34
2001-06-12 12:34:23 GET /sports/football.html 2001-06-12 12:34:30
GET /sports/football.html
<!--NeedCopy-->
```

Einträge

Einträge bestehen aus einer Folge von Feldern, die sich auf eine einzelne HTTP-Transaktion beziehen. Felder sind durch Leerzeichen getrennt. Citrix empfiehlt die Verwendung von Tabulatorzeichen. Wenn ein Feld in einem bestimmten Eintrag nicht verwendet wird, markiert ein Bindestrich (-) das ausgelassen Feld.

Richtlinien

Informationen zum Protokollierungsprozess finden Sie in der Tabelle Richtlinien . Zeilen, die mit dem Pfundzeichen (#) beginnen, enthalten Anweisungen.

Beispiel:

Die folgende Beispielprotokolldatei zeigt die Protokolleinträge im W3C-Extended-Protokollformat:

```
#Version: 1.0
#Fields: time cs-method cs-uri
#Date: 12-Jan-1996 00:00:00
00:34:23 GET /sports/football.html
12:21:16 GET /sports/football.html
12:45:52 GET /sports/football.html
12:57:34 GET /sports/football.html
<!--NeedCopy-->
```


Felder

Die Fields Direktive listet eine Sequenz von Feldbezeichnern auf, die die in jedem Eintrag aufgezeichneten Informationen angeben. Feldbezeichner haben möglicherweise eine der folgenden Formen:

- **Bezeichner:** Bezieht sich auf die Transaktion als Ganzes.
- **prefix-identifier: Bezieht** sich auf Informationsübertragung zwischen Parteien, die durch das Wertpräfix definiert sind.
- **Präfix (Header):** Gibt den Wert des HTTP-Header-Feld-Headers für die Übertragung zwischen Parteien an, die durch das Wertpräfix definiert Auf diese Weise angegebene Felder haben immer den Typ.

In der folgenden Tabelle werden definierte Präfixe beschrieben.

Präfix	Spezifiziert
c	Client
s	Server
r	Remote
cs	Client zum Server
Sc	Server zum Client
sr	Server zum Remoteserver (von Proxys verwendetes Präfix)
rs	Remote-Server zum Server (von Proxys verwendetes Präfix)
x	Anwendungsspezifischer Bezeichner

Beispiele:

Die folgenden Beispiele sind definierte Bezeichner, die Präfixe verwenden:

cs-method: Die Methode in der Anforderung, die vom Client an den Server gesendet wird.

sc(Referer): Das Feld `Referer` in der Antwort.

c-ip: Die IP-Adresse des Clients.

Identifikatoren

In der folgenden Tabelle werden die Bezeichner des erweiterten W3C-Protokollformats beschrieben, die kein Präfix benötigen.

Identifier	Beschreibung
Datum	Das Datum, an dem die Transaktion abgeschlossen wurde.
Zeit	Der Zeitpunkt, zu dem die Transaktion abgeschlossen ist.
Zeit in Anspruch genommen	Die für den Abschluss der Transaktion benötigte Zeit (in Sekunden).
Bytes	Die Anzahl der übertragenen Byte.
zwischengespeichert	Zeichnet auf, ob ein Cache-Treffer aufgetreten ist. Eine Null gibt an, dass ein Cache fehlschlägt.

In der folgenden Tabelle werden die Bezeichner des erweiterten W3C-Protokollformats beschrieben, die ein Präfix erfordern.

Identifier	Beschreibung
IP	Die IP-Adresse und die Portnummer.
DNS	Der DNS-Name.
Status	Der Statuscode.
comment	Der Kommentar wurde mit einem Statuscode zurückgegeben.
method	Die Methode.
url	Die URL.
url-Stamm	Der Stammteil der URL.
url-Abfrage	Der Abfrageteil der URL.

Mit dem Dateiformat W3C Extended Log können Sie Protokollfelder auswählen. Diese Felder sind in der folgenden Tabelle aufgeführt.

Feld	Beschreibung
Datum	Das Datum, an dem die Transaktion abgeschlossen ist.

Feld	Beschreibung
Zeit	Der Zeitpunkt, zu dem die Transaktion abgeschlossen ist.
Client-IP	Die IP-Adresse des Clients.
Benutzername	Der Benutzername.
Dienstname	Der Dienstname, der immer HTTP ist.
Server-IP	Die Server-IP-Adresse.
Serverport	Die Server-Portnummer
Methode	Die Anforderungsmethode (z. B. GET, POST).
Url-Stamm	Der URL-Stamm.
URL-Abfrage	Der Abfrageteil der URL.
HTTP-Status	Der Statuscode in der Antwort.
Byte gesendet	Die Anzahl der an den Server gesendeten Byte (Anforderungsgröße, einschließlich HTTP-Header).
Bytes empfangen	Die Anzahl der vom Server empfangenen Byte (Größe der Antwort, einschließlich HTTP-Header).
Zeitaufwand	Die Zeit, die für den Abschluss einer Transaktion in Sekunden gebraucht wird.
Protokollversion	Die Versionsnummer von HTTP, die vom Client verwendet wird.
Benutzeragent	Das Feld **User-Agent** im HTTP-Protokoll.
Cookie	Das **Cookie-Feld** des HTTP-Protokolls.
`Referer`	Das Feld `Referer` des HTTP-Protokolls.

Erstellen Sie ein benutzerdefiniertes Protokollformat

Sie können das Anzeigeformat der Protokolldateidaten manuell oder mithilfe der NSWL-Bibliothek anpassen. Mithilfe des benutzerdefinierten Protokollformats können Sie die meisten Protokollformate ableiten, die Apache derzeit unterstützt.

Erstellen Sie ein benutzerdefiniertes Protokollformat mithilfe der NSWL-Bibliothek

Verwenden Sie eine der folgenden NSWL-Bibliotheken, je nachdem, ob die ausführbare NSWL-Datei auf einem Windows- oder Solaris-Hostcomputer installiert wurde:

- **Windows:** Die nswl.lib-Bibliothek im Verzeichnis `\ns\bin` auf dem Hostcomputer des Systemmanagers.
- **Solaris:** Die Bibliothek `libnswl.a` in `usr/local/netscaler/bin`.

1. Fügen Sie die folgenden zwei vom System definierten C-Funktionen in einer C-Quelldatei hinzu:

   ns_userdeffieldName (): Diese Funktion gibt die Zeichenfolge zurück, die als benutzerdefinierter Feldname im Protokolldatensatz hinzugefügt werden muss.

   ns_userdeffieldVal (): Diese Funktion implementiert den Wert des benutzerdefinierten Feldes und gibt ihn dann als String zurück, der am Ende des Protokolldatensatzes hinzugefügt werden muss.

2. Kompilieren Sie die Datei in eine Objektdatei.
3. Verknüpfen Sie die Objektdatei mit der NSWL-Bibliothek (und optional mit Bibliotheken von Drittanbietern), um eine neue ausführbare NSWL-Bibliothek zu bilden.
4. Fügen Sie am Ende der LogFormat-Zeichenfolge in der Konfigurationsdatei (log.conf) eine %d Zeichenfolge hinzu.

Beispiel:

```
##########
# A new file is created every midnight or on reaching 20MB file size,
# and the file name is
/datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log and create
digital
#signature field for each record.
BEGIN CACHE_F
    logFormat custom "%a - "%{
 user-agent }
 i" [%d/%B/%Y %T -%g] "%x"
%s %b%{
 referrer }
 i "%{
 user-agent }
 i" "%{
 cookie }
 i" %d "
    logInterval Daily
    logFileSizeLimit 20
    logFilenameFormat
```



```
/datadisk5/netscaler/log/%v/NS%`{
 `%m%d%y }
 t.log
END CACHE_F
<!--NeedCopy-->
```

Manuelles Erstellen eines benutzerdefinierten Protokollformats

Um das Format anzupassen, in dem Protokolldateidaten angezeigt werden müssen, geben Sie eine Zeichenfolge als Argument der **LogFormat-Protokolleigenschaftsdefinition** an. Im Folgenden finden Sie ein Beispiel, in dem Zeichenfolgen verwendet werden, um ein Protokollformat zu erstellen:

```
LogFormat Custom ""%a - "%{
 user-agent }
 i" %[%d/%m/%Y]t %U %s %b %T"
<!--NeedCopy-->
```

- Die Zeichenfolge kann die Steuerzeichen vom Typ “c”\ n und\ t enthalten, um neue Zeilen und Registerkarten darzustellen.
- Verwenden Sie die Esc-Taste mit literalen Anführungszeichen und umgekehrten Schrägstrichen.

Die Merkmale der Anforderung werden protokolliert, indem %-Direktiven in die Formatzeichenfolge eingefügt werden, die in der Protokolldatei durch die Werte ersetzt werden.

Wenn der Formatbezeichner %v (Hostname) oder %x (URL-Suffix) in einer Protokolldateinamenformatzeichenfolge vorhanden ist, werden die folgenden Zeichen im Dateinamen durch einen Unterstreichungsstrich im Namen der Protokollkonfigurationsdatei ersetzt:

```
" *. /: < > ? \ |
```

Zeichen, deren ASCII-Werte im Bereich von 0-31 liegen, werden wie folgt ersetzt:

```
%<ASCII value of character in hexadecimal>.
```

Beispielsweise wird das Zeichen mit dem ASCII-Wert 22 durch %16 ersetzt.

> **Achtung:**
>
> Wenn der Formatbezeichner%v in einer Protokolldateinamen-Formatzeichenfolge vorhanden ist, wird für jeden virtuellen Host eine separate Datei geöffnet. Um eine kontinuierliche Protokollierung sicherzustellen, muss die maximale Anzahl von Dateien, die ein Prozess geöffnet haben kann, ausreichend groß sein. Eine Vorgehensweise zum Ändern der Anzahl der Dateien, die geöffnet werden können, finden Sie in der Dokumentation des Betriebssystems.

Erstellen Sie Apache-Protokollformate

Sie können aus den benutzerdefinierten Protokollen die meisten Protokollformate ableiten, die Apache derzeit unterstützt. Die benutzerdefinierten Protokollformate, die den Apache-Protokollformaten entsprechen, sind:

NCSA/Combined: LogFormat custom%h%l%u [%t] “%r” %s%b “% {referer} i” “% {useragent} i”

NCSA/Common: LogFormat custom %h %l %u [%t] “%r” %s %B

Referer Log: LogFormat benutzerdefiniert “% {referer} i” ->%U

Benutzeragent: LogFormat custom% {user-agent} i

Ebenso können Sie die anderen Serverprotokollformate aus den benutzerdefinierten Formaten ableiten.

Argumente zum Definieren eines benutzerdefinierten Protokollformats

In der folgenden Tabelle wird das benutzerdefinierte Protokollformat beschrieben.

Argument	Spezifiziert
%a	Remote-IPv4-Adresse.
%A	Lokale IPv4-Adresse.
%a6	Remote-IPv6-Adresse.
%A6	Lokale IPv6-Adresse.
%B	Gesendete Byte, mit Ausnahme der HTTP-Header (Antwortgröße).
%b	Empfangene Byte, ohne die HTTP-Header (Anforderungsgröße).
%d	Benutzerdefiniertes Feld.
%K	Informationen zum Client-Port.
%e1	Wert des ersten benutzerdefinierten HTTP-Anforderungsheaders.
%e2	Wert des zweiten benutzerdefinierten HTTP-Anforderungsheaders.
%E1	Wert des ersten benutzerdefinierten HTTP-Antwortheaders.

Argument	Spezifiziert
%E2	Wert des zweiten benutzerdefinierten HTTP-Antwortheaders. Hinweis: Anweisungen zum Exportieren benutzerdefinierter HTTP-Header finden Sie unter Konfiguration des NetScaler für die Webserverprotokollierung
%g	Greenwich Mean Time Offset (z. B. -0800 für Pacific Standard Time).
%h	IPv4-Adresse eines Remote-Hosts.
%h6	IPv6-Adresse eines Remote-Hosts.
H	Protokoll anfordern.
% {Foobar}	Inhalt der Foobar: Kopfzeile (n) in der an den Server gesendeten Anfrage. Das System unterstützt die Header User -Agent, Referer und Cookie. Das + nach dem% in diesem Format informiert den Logging-Client, das + als Worttrennzeichen zu verwenden.
%j	Empfangene Byte, einschließlich Header (Anforderungsgröße).
%J	Gesendete Byte, einschließlich Header (Antwortgröße).
%l	Name des Remote-Logs (von identd, falls angegeben).
%m	Methode anfordern.
%M	Zeit, die für die Bearbeitung der Anfrage benötigt wurde (in Mikrosekunden).
% {Foobar}	Inhalt von Foobar: Kopfzeile (n) in der Antwort. USER -AGENT-, Referrer- und Cookie-Header (einschließlich gesetzter Cookie-Header) werden unterstützt.
%p	Kanonischer Port des Servers, der die Anfrage bedient.
%P	Die Admin-Partition.

Argument	Spezifiziert
%q	Abfragezeichenfolge (vorangestellt mit einem Fragezeichen (?) wenn eine Abfragezeichenfolge existiert).
%r	Erste Zeile der Anfrage.
%s	Anfragen, die intern umgeleitet wurden, dies ist der Status der ursprünglichen Anfrage.
%t	Uhrzeit im gängigen Protokollformat (englisches Standardzeitformat).
% {format} t	Zeit muss in der vom Format angegebenen Form im Format strftime (3) vorliegen. Formatbeschreibungen finden Sie unter Definition des Zeitformats.
%T	Zeit, die für die Bearbeitung der Anfrage benötigt wurde, in Sekunden.
%u	Remote-Benutzer (von Auth; möglicherweise falsch, wenn der Rückgabewert (%s) 401 ist).
%U	URL-Pfad angefordert.
%v	Kanonischer Name des Servers, der die Anfrage bedient.
%V6	IPv6-Adresse des virtuellen Servers im System, wenn Load Balancing, Content Switching und/oder Cache-Umleitung verwendet werden.
%D	Druckt die HTTP-Transaktions-ID.
%L	Transaktionszeit in Millisekunden.
%R	HTTP-Reason-Zeichenfolge, die dem Statuscode zugeordnet ist.
%f	Protokollierung des Quellports.
%V	IPv4-Adresse des virtuellen Servers.

> **Hinweis**
>
> Anweisungen zum Exportieren benutzerdefinierter HTTP-Header finden Sie unter Konfigurieren

> des NetScaler für die Webserver-Protokollierung

Wenn Sie beispielsweise das Protokollformat als `%+{ user-agent } i`definieren und wenn der Benutzeragentwert NetScaler System Web Client ist, werden die Informationen als NetScaler System+Web+Client protokolliert. Eine Alternative besteht darin, doppelte Anführungszeichen zu verwenden. Zum Beispiel protokolliert "%{user-agent}i" es als "NetScaler System Web Client. " Verwenden Sie den Schlüssel `\<Esc\>` nicht für Zeichenfolgen von %.. .r,%. .i und %. .o. Es entspricht den Anforderungen des Common Log Formats. Clients können Steuerzeichen in das Protokoll einfügen. Daher müssen Sie vorsichtig sein, wenn Sie mit rohen Logfiles arbeiten.

Zeitformatdefinition

In der folgenden Tabelle wird die Zeitformatdefinition beschrieben, um Informationen zum Formatteil der Zeichenfolge `%{ format } t` zu erhalten, die in der Tabelle "Benutzerdefiniertes Protokollformat" beschrieben wird. Werte in Klammern ([]) zeigen den Wertebereich an, der angezeigt wird. Beispielsweise zeigt [1,31] in der %d-Beschreibung in der folgenden Tabelle, dass %d zwischen 1 und 31 liegt.

Argument	Spezifiziert
———	———-
%%	Das Gleiche wie%.
%a	Der abgekürzte Name des Wochentags für das Gebietsschema.
%A	Der vollständige Name des Wochentags für das Gebietsschema
%b	Der abgekürzte Name des Monats für das Gebietsschema.
%B	Der vollständige Name des Monats für das Gebietsschema.
%C	Die Jahrhundertzahl (das Jahr geteilt durch 100 und als Dezimalzahl auf eine Ganzzahl gekürzt `[1,99]`); einzelnen Ziffern geht eine 0 voraus.
%d	Benutzerdefiniertes Feld.
%K	Die Jahrhundertzahl (das Jahr geteilt durch 100 und als Dezimalzahl auf eine Ganzzahl gekürzt `[1,99]`); einzelnen Ziffern geht eine 0 voraus.
%e	Der Tag des Monats `[1,31]`; einzelnen Ziffern steht ein Leerzeichen vorangestellt.
%h	Der abgekürzte Name des Monats für das Gebietsschema.
%H	Die Stunde (24-Stunden-Uhr) `[0,23]`; einzelnen Ziffern geht eine 0 voraus.
%I	Die Stunde (12-Stunden-Uhr) `[1,12]`; einzelnen Ziffern geht eine 0 voraus.
%j	Die Zahl des Tages im Jahr `[1,366]`; einstelligen Ziffern wird 0 vorangestellt.
%k	Die Stunde (24-Stunden-Uhr) `[0,23]`; einzelnen Ziffern ist ein Leerzeichen vorangestellt.
%l	Die Stunde (12-Stunden-Uhr) `[1,12]`; einzelnen Ziffern geht ein Leerzeichen voraus.
%m	Die Zahl des Monats im Jahr `[1,12]`; einstelligen Ziffern geht eine 0 voraus.
%M	Die Minute `[00,59]`; eine 0 führende Zahl ist zulässig, aber nicht erforderlich.
%n	Fügt eine neue Zeile ein.
%p	Entspricht entweder morgens oder nachmittags für das Gebietsschema.

%r	Die entsprechende Zeitdarstellung im 12-Stunden-Uhrformat mit %p
%S	Die Sekunden `[00,61]`; der Wertebereich ist `[00,61]` eher als `[00,59]`, um die gelegentliche Schaltsekunde und die doppelte Schaltsekunde zuzulassen.
%3	Die Millisekunden `[000,999]`; der Wertebereich ist. `[000,999]`
%6	Die Mikrosekunden `[000000,999999]`; der Wertebereich ist `[000000,999999]`.
%9	Die Nanosekunden `[000000000,999999999]`; der Wertebereich ist `[000000000,999999999]` .
%t	Fügt eine Registerkarte ein.
%u	Der Wochentag als Dezimalzahl `[1,7]`. 1 steht
Sonntag, 2 steht für Dienstag und so weiter.
%U	Die Zahl der Woche im Jahr als Dezimalzahl `[00,53]`, wobei Sonntag der erste Tag der Woche 1 ist.

> **Hinweis:**
>
> Wenn Sie eine Konvertierung angeben, die keiner der in der vorhergehenden Tabelle beschriebenen Konvertierungsspezifikationen entspricht, oder einer der im nächsten Absatz aufgeführten geänderten Konvertierungsspezifikationen entspricht, ist das Verhalten nicht definiert und gibt 0 zurück.

Der Unterschied zwischen `%U` und `%W` (und auch zwischen modifizierten Konvertierungen `%OU` und `%OW`) ist der Tag, der als erster Wochentag angesehen wird. Woche Nummer 1 ist die erste Januarwoche (beginnend mit einem Sonntag für `%U` oder einem Montag für `%W`). Die Wochennummer 0 enthält die Tage vor dem ersten Sonntag oder Montag im Januar für `%U` und `%W`.

Serverprotokolle anzeigen

Sie können eine NSWL-Funktion so konfigurieren, dass Serverprotokolle auf der Konsole angezeigt werden oder Serverprotokolle in ein Verzeichnis auf der NetScaler-Appliance umleiten.

Es gibt zwei Möglichkeiten, Protokolle auf der Konsole anzuzeigen (Standardausgabe):
Option 1: Alle Protokolle auf der Konsole anzeigen.
Option 2: Zeigen Sie nur ausgewählte Protokolle auf der Konsole mit Filtern mit `logfilenameformat` als `STDOUT` an.

Call Home

May 11, 2023

Appliances funktionieren manchmal aufgrund von Software- oder Hardwareproblemen nicht gut. In solchen Fällen muss NetScaler Daten sammeln und Probleme lösen, bevor mögliche Auswirkungen

beim Kunden auftreten können. Indem Sie Call Home auf Ihrer NetScaler Appliance aktivieren, können Sie den Fehlerbenachrichtigungsprozess automatisieren. Sie vermeiden es nicht nur, den NetScaler-Support anzurufen, eine Serviceanfrage zu stellen und Systemdaten hochzuladen, bevor das Support-Team das Problem beheben kann, sondern der Support kann ein Problem identifizieren und beheben, bevor es auftritt. Call Home überwacht die Appliance regelmäßig und lädt automatisch Daten auf den Server des technischen Supports von Citrix hoch. Darüber hinaus bieten die eingehenden Call Home-Daten Einblicke in die Verwendung von NetScaler. Mehrere Teams innerhalb von Citrix können diese Daten verwenden, um NetScaler besser zu entwerfen, zu unterstützen und zu implementieren.

Standardmäßig ist Call Home auf allen Plattformen und allen Varianten von NetScaler (MPX, VPX, SDX) aktiviert. Wenn diese Funktion aktiviert ist, ermöglichen Sie Citrix, NetScaler-Bereitstellungs- und Telemetriedaten für eine bessere Implementierung und einen besseren Support-Service zu sammeln.

> **Hinweis**
>
> Informationen zu Call Home finden Sie auch auf der Seite "Häufig gestellte Fragen zu Call Home".

Vorteile

Call Home bietet die folgenden Vorteile.

- Überwachen Sie Hardware- und Softwarefehler. Weitere Informationen finden Sie im Abschnitt Überwachen kritischer Fehlerbedingungen.
- Informieren Sie wichtige Ereignisse, die sich auf Ihr Netzwerk auswirken.
- Senden Sie Leistungsdaten und Details zur Systemnutzung an Citrix an:
  - Analysieren und verbessern Sie die Produktqualität.
  - Bereitstellung von Informationen zur Fehlerbehebung in Echtzeit zur proaktiven Problemerkennung und schnelleren Problemlösung.

Plattform-Unterstützung

Die Call Home-Funktion wird auf allen NetScaler-Plattformen und allen Appliance-Modellen (MPX, VPX und SDX) unterstützt.

- NetScaler MPX: Alle MPX-Modelle.
- NetScaler VPX: Alle VPX-Modelle, einschließlich VPX-Appliances, die ihre Lizenz aus externen oder zentralen Lizenzierungspools beziehen.
- NetScaler SDX: Überwacht das Laufwerk und die zugewiesenen SSL-Chips auf Fehler oder Fehler. Die VPX-Instanzen haben jedoch keinen Zugriff auf die Power Supply Unit (PSU) und daher wird ihr Status nicht überwacht. In einer SDX-Plattform können Sie Call Home entweder direkt auf einer einzelnen Instanz oder über die SVM konfigurieren.

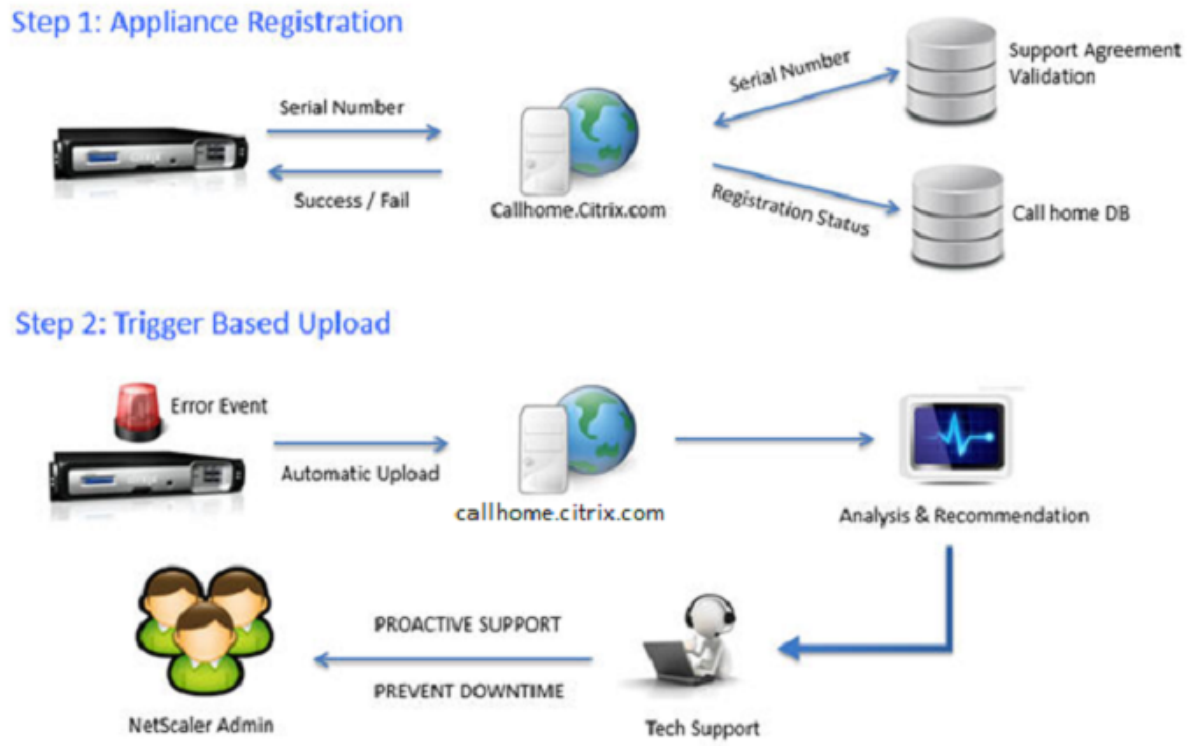
Voraussetzungen

Um Call Home verwenden zu können, muss die NetScaler Appliance über Folgendes verfügen:

- **Internetverbindung.** Call Home benötigt eine Internetverbindung, damit der NetScaler eine Verbindung zum NetScaler-Supportserver herstellen kann, um ein Datenarchiv hochzuladen.
- **URL.** Call Home tauscht Datenverkehr mit dem `callhome.citrix.com` über SSL/TLS-Protokoll über Port 443 für bidirektionalen Verkehr aus.

So funktioniert Call Home

Die folgende Abbildung zeigt einen grundlegenden Workflow von Call Home in einer NetScaler Appliance, die an einem Kundenstandort bereitgestellt wird.



Im Folgenden ist der Workflow eines Call Home:

1. Richten Sie die Internetverbindung ein. Damit Call Home Systemdaten hochladen kann, muss Ihr Gerät über eine Internetverbindung verfügen. Wenn dies nicht der Fall ist, können Sie eine Proxy-Serverkonfiguration konfigurieren, um eine Internetverbindung bereitzustellen. Weitere Informationen finden Sie im Abschnitt Call Home konfigurieren.

2. Aktivieren Sie Call Home. Wenn Sie Ihre Appliance über die NetScaler Befehlszeilenschnittstelle oder GUI auf die neueste Software aktualisieren, ist Call Home standardmäßig aktiviert, und das Sys-

tem verzögert den Registrierungsvorgang um 24 Stunden. Während dieser Zeit können Sie die Funktion manuell deaktivieren, aber Citrix empfiehlt, sie zu aktivieren.

> **Hinweis**
>
> Wenn Sie Ihre Appliance von einer älteren Version aktualisieren, für die Call Home explizit deaktiviert ist, aktiviert das System die Funktion weiterhin standardmäßig und zeigt bei Ihrer ersten Anmeldung eine Benachrichtigung an.

Wenn Sie Änderungen an der Konfiguration für eine Internetverbindung vornehmen, müssen Sie außerdem Call Home deaktivieren und aktivieren. Es ermöglicht Call Home, sich ohne Fehlerfehler beim Citrix Insight Services (CIS) -Server zu registrieren.

3. Registrieren Sie die NetScaler-Appliance auf dem NetScaler Support Server. Wenn Call Home die Appliance beim NetScaler-Supportserver registriert, überprüft der Server die Datenbank auf die Gültigkeit der Seriennummer der Appliance. Wenn die Seriennummer gültig ist, registriert der Server das Gerät für den Call Home-Dienst und sendet eine erfolgreiche Antwort auf die Registrierung. Andernfalls sendet der Server eine Meldung über einen Fehler bei der Registrierung zurück. Die grundlegenden Systeminformationen werden als separate Nachricht gesendet. Zu den Daten gehören Angaben zur Speicher- und CPU-Auslastung sowie die Durchsatzzahlen. Die Daten werden standardmäßig alle 7 Tage als Teil der Heartbeat-Nachricht gesendet. Ein Wert von weniger als 5 Tagen wird jedoch nicht empfohlen, da häufige Uploads nicht sinnvoll sind.

4. Überwachen Sie kritische Fehlerbedingungen. Nach der Registrierung beginnt Call Home mit der Überwachung des Geräts. In der folgenden Tabelle sind die Bedingungen aufgeführt, die Call Home auf dem Gerät überwachen kann.

Kritische Fehlerbedingung	Beschreibung	Call Home Überwachungsintervall	Entsprechender SNMP-Alarmname
Fehler beim Compact Flash-Laufwerk	Beim Compact-Flash-Laufwerk der Appliance traten Lese- oder Schreibfehler auf.	24 Stunden	COMPACT-FLASH-ERRORS
Fehler beim Festplattenlaufwerk	Bei den Festplatten der Appliance traten Lese- oder Schreibfehler auf.	24 Stunden	HARD-DISK-DRIVE-ERRORS

Kritische Fehlerbedingung	Beschreibung	Call Home Überwachungsinter-vall	Entsprechender SNMP-Alarmname
Ausfall des Netzteils	Eines der Netzteile der NetScaler Appliance ist ausgefallen.	7 Sekunden	POWER-SUPPLY-FAILURE
Ausfall der SSL-Karte	Eine der SSL-Karten auf der NetScaler Appliance ist ausgefallen.	7 Sekunden	SSL-CARD-FAILED
Warmer Neustart	Die Appliance wurde aufgrund eines Ausfalls eines Systemprozesses warm neu gestartet.	Nach jedem Neustart der NetScaler Appliance.	WARM-RESTART-EVENT
Speicheranomalie-Fehler	Die Speicherauslastung steigt zunehmend über den normalen Grenzwert hinaus und überschreitet den Schwellenwert.	1 Tag	Kein SNMP-Alarm
Ratenbegrenzung Paket Drop	Die Durchsatzgrenzen oder die Grenzwerte für Pakete pro Sekunde (pps) wurden erreicht.	7 Sekunden	PF-RL-PPS-PKTS-DROPPED, PF-RL-RATE-PKTS-DROPPED

5. Laden Sie Call Home-Daten hoch. Wenn eine der vorherigen kritischen Bedingungen auf der Appliance festgestellt wird, benachrichtigt die Call Home-Funktion automatisch den NetScaler-Support. Die Support-Archive werden auf den NetScaler-Supportserver hochgeladen. Sie können den SNMP-Alarm CALLHOME-UPLOAD-EVENT auch so konfigurieren, dass bei jedem Call Home-Upload eine SNMP-Warnung generiert wird. Die SNMP-Warnung informiert den lokalen Administrator über das kritische Ereignis.

> **Hinweis**
>
> Call Home erstellt die Call Home-TAR-Datei und lädt sie nur für das erste Auftreten einer bestimmten Fehlerbedingung seit dem letzten Neustart auf den Citrix Tech-Support-Server hoch. Wenn Sie möchten, dass die Appliance jedes Mal Warnungen sendet, wenn ein bestimmter Fehlerzustand auftritt, konfigurieren Sie den entsprechenden SNMP-Alarm für den Fehlerzustand.

6. Erstellen einer Serviceanfrage. Call Home erstellt automatisch eine Serviceanfrage für alle kritischen hardwarebezogenen Ereignisse. Die Ereignisse werden wie folgt klassifiziert: Ausfall der Stromversorgung, Ausfall der SSL-Karte, Festplattenlaufwerksfehler und Compact-Flash-Fehler. Bei anderen Fehlern können Sie sich nach Überprüfung der Systemprotokolle an das NetScaler-Supportteam wenden, um eine Serviceanfrage zur Untersuchung zu stellen.

Konfigurieren von Call Home

Um Call Home zu konfigurieren, überprüfen Sie die Internetverbindung auf der Appliance und stellen Sie sicher, dass ein DNS-Nameserver konfiguriert ist. Wenn keine Internetverbindung besteht, konfigurieren Sie einen Proxy-Server oder -Dienst. Aktivieren Sie dann Call Home auf der Appliance und überprüfen Sie den Registrierungsstatus der Appliance mit dem NetScaler-Supportserver. Nach der Registrierung kann Call Home Daten überwachen und hochladen. Darüber hinaus können Sie SNMP-Alarme konfigurieren, um den Administrator am Kundenstandort zu benachrichtigen.

Um Call Home zu konfigurieren, können Sie entweder die NetScaler -Befehlszeilenschnittstelle oder die GUI verwenden, um die folgenden Aufgaben auszuführen:

- Aktivieren Sie Call Home.
- Konfigurieren Sie Call Home für optionale Proxy-Server-Parameter.
- Überprüfen Sie den Call Home-Registrierungsstatus.
- Zeigen Sie Fehler und Zeitstempeldetails an.
- Konfigurieren Sie SNMP-Alarme.

So konfigurieren Sie Call Home mit der NetScaler Befehlszeilenschnittstelle

Mit der NetScaler Befehlszeilenschnittstelle können Sie Folgendes tun:

`Enabling Call Home`

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature callhome
```

Konfigurieren von Call Home für optionale Proxy-Server-Parameter

Call Home ermöglicht die Konfiguration des optionalen Proxyservers für die Internetverbindung. Sie können entweder einen Proxy-Server mit IP-Adresse und Port oder einen Proxy-Authentifizierungsdienst mit Ein- oder Zweiwege-Authentifizierung konfigurieren.

To configure optional proxy server with IP address and port

Geben Sie in der Befehlszeile Folgendes ein:

```
set callhome -proxyMode ( YES | NO )[-IPAddress <ip_addr|ipv6_addr|*>] [-port <port |*>]
```

```
1 set callhome -proxyMode YES -IPAddress 10.102.167.33 -port 80
2 <!--NeedCopy-->
```

> **Hinweis**
>
> Call Home verwendet den Proxy-Server nur, wenn Sie den Proxy-Modus-Parameter auf JA setzen. Wenn Sie es auf NEIN setzen, funktioniert die Proxy-Funktionalität nicht, auch wenn die IP-Adresse und der Port konfiguriert sind. Die Portnummer muss für einen HTTP-Dienst und nicht für einen HTTPS-Dienst gelten.

Konfigurieren des optionalen Proxy-Authentifizierungsdienstes

Dieser Modus bietet zwei Arten der Sicherheitsauthentifizierung: Einweg- und Zweiwege-Authentifizierung. Um beide Typen einzurichten, müssen Sie einen SSL-Dienst konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines SSL-Dienstes .

Bei der unidirektionalen Authentifizierung authentifiziert nur die NetScaler Appliance den Proxyserver. Bei der Zweiwege-Authentifizierung authentifiziert die NetScaler Appliance den Proxyserver und der Proxyserver authentifiziert wiederum die Appliance.

Konfigurieren des Proxy-Authentifizierungsdienstes

Geben Sie in der Befehlszeile Folgendes ein:

```
set callhome -proxyMode ( YES | NO )[-proxyAuthService <string>]
```

```
1 set callhome -proxyMode YES -proxyAuthService callhome_proxy
2 <!--NeedCopy-->
```

Konfigurieren der Einweg-Proxy-Serverauthentifizierung

Führen Sie die folgenden Aufgaben aus, um die Einweg-Proxy-Serverauthentifizierung

1. Erstellen Sie einen SSL-Dienst.
2. Binden Sie ein CA-Zertifikat an den Dienst.
3. Binden Sie einen HTTPS-Monitor an den Dienst.
4. Konfigurieren Sie Call Home für die Verwendung des SSL-Dienstes.

Konfigurieren der Zweiwege-Proxy-Serverauthentifizierung

Führen Sie die folgenden Aufgaben aus, um die Zweiwege-Proxy-Server-Authentifizierung

1. Erstellen Sie einen SSL-Dienst
2. Binden Sie ein CA-Zertifikat an den Dienst.
3. Binden Sie ein Clientzertifikat.
4. Binden Sie einen HTTPS-Monitor an den Dienst.
5. Konfigurieren Sie Call Home für die Verwendung des SSL-Dienstes.

Überprüfen des Status der Call Home-Registrierung

Geben Sie in der Befehlszeile Folgendes ein:

```
show callhome

    show callhome

     Registration with Citrix upload server SUCCESSFUL

     Mode: Default

     Contact email address: exampleadmin@example.com

     Heartbeat Custom Interval (days): 7

     Proxy Mode: Yes

        Proxy IP Address:10.102.29.200

        Proxy Authentication Service:

        Proxy Port: 80

    Trigger event                  State   First occurrence
                      Latest occurrence

     -------------                  -----   ----------------
                     -----------------

     1) Warm boot                   Enabled N/A
                                    ..

     2) Compact flash errors        Enabled ..
                                      ..

```



```
29       3) Hard disk drive errors      Enabled ..
                                          ..
30
31       4) SSL card failure            N/A     N/A
                                        N/A
32
33       5) Power supply unit failure   N/A     N/A
                                        N/A
34
35       6) Rate limit packet drops     Enabled ..
                                          ..
36
37       7) Memory anomaly              Enabled ..
                                          ..
38
39       Done
40 <!--NeedCopy-->
```

> **Hinweis**
>
> Wenn sich das Call Home nicht bei CIS registriert, zeigt die Appliance eine Fehlermeldung an.

SNMP-Alarme aktivieren

Die NetScaler Appliance bietet eine Reihe von Fehlerbedingungseinheiten, die als *SNMP-Alarme*bezeichnet werden. Wenn eine Fehlerbedingung in einem SNMP-Alarm erfüllt ist, generiert die Appliance SNMP-Trap-Nachrichten, die an die konfigurierten Trap-Listener gesendet werden. Wenn beispielsweise der Alarm SSL-CARD-FAILED aktiviert ist, wird eine Trap-Nachricht generiert und an den Trap-Listener gesendet. Die Trap-Nachricht wird bei jedem Ausfall der SSL-Karte auf der Appliance gesendet. Weitere Informationen finden Sie unter SNMP.

Geben Sie in der Befehlszeile Folgendes ein:

```
enable snmp alarm <trapName>

show snmp alarm <trapName>
```

So konfigurieren Sie Call Home mithilfe der GUI

So überprüfen Sie, ob die Call Home-Funktion standardmäßig in der GUI aktiviert ist

1. Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen**.
2. Klicken Sie im **Detailbereich** auf den Link **Erweiterte Funktionen konfigurieren** .
3. Auf der Seite **Erweiterte Funktionen konfigurieren** muss die Option **Call Home** als aktiviert angezeigt werden.

So aktivieren Sie Call Home mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen**.
2. Klicken Sie im **Detailbereich** auf den Link **Erweiterte Funktionen konfigurieren** und wählen Sie die Option **Callhome** aus.

So konfigurieren Sie Call Home für die optionale Authentifizierung im Proxymodus mithilfe der GUI

1. Sie können eine der beiden Möglichkeiten verwenden, um auf die Call Home Page zuzugreifen:
   a) Navigieren Sie zu **System** > **Systeminformationen**.
   b) Navigieren Sie zu **System** > **Diagnose**.
      i. Wählen Sie im Detailbereich unter **Tools für den technischen Support**die Option **Call Home**aus.
2. Stellen Sie auf der Seite **Call Home konfigurieren** die folgenden Parameter ein.
   a) **Modus**. Call Home-Betriebsmodus. Mögliche Typen: Standardbereitstellung von Citrix Service Provider (CSP).

      > **Hinweis**
      > Diese Option ist nicht vom Benutzer konfigurierbar. Der Modus wird automatisch bestimmt und basierend auf dem Typ der NetScaler-Bereitstellung festgelegt.

   b) **E-Mail Adresse**. E-Mail-Adresse des Administrators am Kundenstandort kontaktieren.
   c) **CallHome Heartbeats-Intervall (Tage).** Überwachungsintervall (in Tagen) zwischen Call Home-Heartbeats. Minimalwert=1 und Maximalwert=30.
   d) **Aktivieren Sie Call Home**. Aktivieren oder deaktivieren Sie die Call Home-Funktion, um den Status der Appliance-Registrierung auf dem NetScaler-Supportserver einzusehen.
   e) **Proxy-Modus**. Wenn Sie keine Internetverbindung haben, aktivieren Sie den Proxy-Modus und legen Sie die optionalen Proxy-Parameter fest.
   f) **Proxyserver**. Wenn Sie den Proxymodus mithilfe eines Proxyservers festlegen, geben Sie die Server-IP-Adresse an.
      i. **Proxy-Dienst**. Wenn Sie den Proxymodus mithilfe eines Proxy-Dienstes festlegen, geben Sie den Dienstnamen an.
      ii. **IP-Adresse**. Die IP-Adresse des Proxyservers.
      iii. **Hafen**. Portnummer des Proxyservers.
      iv. **SSL-Dienst für Proxy-Authentifizierung**. Der Name des Proxy-Dienstes, der die Authentifizierung im Proxymodus bereitstellt.
3. Klicken Sie auf **OK** und **Fertig**.

So konfigurieren Sie den SSL-Dienst für die Proxyserver-Authentifizierung mit der GUI

Informationen zum Konfigurieren des SSL-Dienstes über die grafische Benutzeroberfläche finden Sie unter Konfigurieren eines SSL-Dienstes .

So überprüfen Sie den Registrierungsstatus von Call Home über die GUI

1. Sie können eine der beiden Möglichkeiten verwenden, um auf die **Call Home** Page zuzugreifen:
   a) Navigieren Sie zu **System** > **Systeminformationen**.

b) Navigieren Sie zu **System** > **Diagnose**.
   i. Wählen Sie im Detailbereich unter **Tools für den technischen Support**die Option **Call Home**aus.
2. Auf der Seite **Call Home konfigurieren** zeigt das Feld **Registrierung beim Citrix Upload-Server** den Registrierungsstatus an.

So konfigurieren Sie einen SNMP-Alarm

1. Navigieren Sie zu **System** > **SNMP** > **Alarme**.
2. Wählen Sie im Detailbereich einen Alarm aus und konfigurieren Sie seine Parameter.
3. Klicken Sie auf **OK** und auf **Schließen**.

Unterstützung der Bereitstellung von Citrix Service Provider (CSP)

In einer Citrix Service Provider (CSP) -Umgebung, in der NetScaler-Dienste auf VPX-Instanzen bereitgestellt werden, kann Call Home die lizenzspezifischen Informationen überwachen und verfolgen und die Informationen sicher an Citrix Insight Services (CIS) senden. CIS wiederum sendet die Informationen zu Buchhaltungszwecken und für CSP-Kunden zur Überprüfung ihrer Lizenznutzung an das Portal License Usage Insights (LUI). Derzeit unterstützen CSP-Umgebungen NetScaler-Dienste nur auf VPX-Instanzen, nicht auf MPX- oder SDX-Appliances. Die VPX-Instanzen können entweder im Standalone- oder im Hochverfügbarkeitsmodus bereitgestellt werden.

Reporting-Tool

May 11, 2023

Verwenden Sie das Citrix® NetScaler® Reporting Tool, um NetScaler Performance-Statistiken als Berichte anzuzeigen. Statistikdaten werden vom Dienstprogramm `nscollect` gesammelt und in einer Datenbank gespeichert. Wenn Sie bestimmte Leistungsdaten über einen Zeitraum hinweg anzeigen möchten, zieht das Reporting Tool bestimmte Daten aus der Datenbank heraus und zeigt sie in Diagrammen an.

Berichte sind eine Sammlung von Diagrammen. Das Reporting-Tool bietet integrierte Berichte und die Option zum Erstellen benutzerdefinierter Berichte. In einem Bericht können Sie die Diagramme ändern und neue Diagramme hinzufügen. Sie können auch den Betrieb des Datenerfassungsdienstprogramms ändern und seinen Betrieb beenden oder starten. `nscollect`

Verwenden des Berichtswerkzeugs

Das Reporting Tool ist eine webbasierte Schnittstelle, auf die von der Citrix® NetScaler® Appliance aus zugegriffen wird. Verwenden Sie das Tool Berichterstellung, um die Performance-Statistikdaten

als Berichte anzuzeigen, die Grafiken enthalten. Zusätzlich zur Verwendung der integrierten Berichte können Sie benutzerdefinierte Berichte erstellen, die Sie jederzeit ändern können. Berichte können zwischen einem und vier Diagrammen enthalten. Sie können bis zu 256 benutzerdefinierte Berichte erstellen. Sie können einen benutzerdefinierten Bericht für eine beliebige Anzahl von Entitäten erstellen.

Rufen Sie das Reporting-Tool auf

1. Verwenden Sie den Webbrowser Ihrer Wahl, um eine Verbindung zur IP-Adresse des NetScaler herzustellen (z. B. `http://10.102.29.170/`). Das Fenster Webanmeldung wird angezeigt.
2. Geben Sie im Textfeld Benutzername den Benutzernamen ein, der dem NetScaler zugewiesen ist.
3. Geben Sie im Textfeld Kennwort das Kennwort ein.
4. Wählen Sie im Dropdownlistenfeld Start in die Option Reporting.Klicken Sie auf Anmelden.

Die folgenden Screenshots zeigen die Berichtssymbolleiste und die Diagrammsymbolleiste, auf die in dieser Dokumentation häufig verwiesen wird.

Abbildung 1. *Bericht-Symbolleiste*

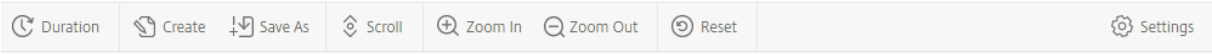
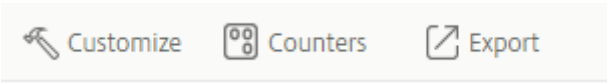


Abbildung 2. *Diagramm-Symbolleiste*



Arbeiten mit Berichten

Sie können Statistiken für die verschiedenen Funktionsgruppen, die auf dem NetScaler konfiguriert sind, über ein bestimmtes Zeitintervall zeichnen und überwachen. Mithilfe von Berichten können Sie das Verhalten Ihrer Appliance beheben oder analysieren. Es gibt zwei Arten von Berichten: integrierte Berichte und benutzerdefinierte Berichte. Berichtsinhalte für integrierte oder benutzerdefinierte Berichte können in einem grafischen oder tabellarischen Format angezeigt werden. Die grafische Ansicht besteht aus Linien-, Flächen- und Balkendiagrammen, in denen bis zu 32 Datensätze (Zähler) angezeigt werden können. In der tabellarischen Ansicht werden die Daten in Spalten und Zeilen angezeigt. Diese Ansicht ist nützlich für das Debuggen von Fehlerzählern.

Der Standardbericht, der im Berichtstool angezeigt wird, lautet CPU versus Speicherauslastung und HTTP-Anforderungsrate. Sie können die Standardberichtansicht ändern, indem Sie den gewünschten Bericht als Standardansicht anzeigen und dann auf **Standardbericht**klicken.

Berichte können für die letzte Stunde, den letzten Tag, die letzte Woche, den letzten Monat, das letzte Jahr erstellt werden, oder Sie können die Dauer anpassen.

Mit Berichten können Sie Folgendes tun:

- Umschalten zwischen einer tabellarischen Ansicht der Daten und einer grafischen Datenansicht.
- Ändern Sie den grafischen Darstellungstyp, z. B. Balkendiagramm oder Liniendiagramm.
- Passen Sie Diagramme eines Berichts an.
- Exportieren Sie das Diagramm als CSV-Datei (Comma Separated Value) von Excel.
- Zeigen Sie die Diagramme im Detail an, indem Sie hineinzoomen, verkleinern oder einen Drag-Vorgang verwenden (Scrollen).
- Legen Sie einen Bericht als Standardbericht für die Anzeige bei jeder Anmeldung fest.
- Zähler hinzufügen oder entfernen.
- Berichte drucken.
- Aktualisieren Sie Berichte, um die neuesten Leistungsdaten anzuzeigen.

Integrierte Berichte verwenden

Das Reporting-Tool bietet integrierte Berichte für häufig angezeigte Daten. Integrierte Berichte sind für die folgenden Funktionsgruppen verfügbar: System, Netzwerk, SSL, Komprimierung, Integrierter Cache, NetScaler Gateway und NetScaler Application Firewall. Standardmäßig werden die integrierten Berichte für den letzten Tag angezeigt. Sie können jedoch die Berichte für die letzte Stunde, die letzte Woche, den letzten Monat oder das letzte Jahr anzeigen.

> **Hinweis**:
>
> Sie können Änderungen an integrierten Berichten nicht speichern, aber Sie können einen geänderten integrierten Bericht als benutzerdefinierten Bericht speichern.

Integrierten Bericht anzeigen

1. Erweitern Sie im linken Bereich des Reporting-Tools unter Integrierte Berichte eine Gruppe (z. B. SSL).
2. Klicken Sie auf einen Bericht (z. B. **SSL > Alle Backend-Ciphers)**.

Berichte erstellen und löschen

Sie können Ihre eigenen benutzerdefinierten Berichte erstellen und sie mit benutzerdefinierten Namen zur Wiederverwendung speichern. Sie können je nach Ihren Anforderungen verschiedene Zähler für verschiedene Gruppen darstellen. Sie können bis zu 256 benutzerdefinierte Berichte erstellen.

Sie können entweder einen Bericht erstellen oder einen integrierten Bericht als benutzerdefinierten Bericht speichern. Standardmäßig enthält ein neu erstellter benutzerdefinierter Bericht ein Diagramm mit dem Namen Systemübersicht, in dem der CPU-Auslastungszähler für den letzten Tag

angezeigt wird. Sie können das Intervall anpassen und die Datenquelle und Zeitzone über die Berichtssymbolleiste festlegen.

Erstellen Sie einen benutzerdefinierten Bericht

1. Klicken Sie im **Berichtstool auf der Berichtssymbolleiste** auf **Erstellen**. Wenn Sie einen benutzerdefinierten Bericht basierend auf einem vorhandenen Bericht erstellen möchten, öffnen Sie den vorhandenen Bericht, und klicken Sie dann auf **Speichern unter**.
2. Geben Sie im Feld **Berichtsname** einen Namen für den benutzerdefinierten Bericht ein.
3. Führen Sie einen der folgenden Schritte aus:
   - Um den Bericht einem vorhandenen Ordner hinzuzufügen, klicken Sie unter Erstellen in oder Speichern in auf den Abwärtspfeil, um einen vorhandenen Ordner auszuwählen, und klicken Sie dann auf **OK**.
   - Um einen neuen Ordner zum Speichern des Berichts zu erstellen, klicken Sie auf das Symbol Zum Hinzufügen eines Ordners klicken, geben Sie unter Ordnername den Namen des Ordners ein, geben Sie unter Erstellen in an, wo der neue Ordner in der Hierarchie gespeichert werden soll, und klicken Sie dann auf **OK**.

> **Hinweis**:
> Sie können bis zu 128 Ordner erstellen.

Löschen eines benutzerdefinierten Berichts

1. Klicken Sie im linken Bereich des Berichtstools neben Benutzerdefinierte Berichte auf das Symbol Klicken, um das Symbol für benutzerdefinierte Berichte zu verwalten.
2. Aktivieren Sie das Kontrollkästchen, das dem Bericht entspricht, den Sie löschen möchten, und klicken Sie dann auf Löschen.

   > **Hinweis**:
   >
   > Wenn Sie einen Ordner löschen, wird der gesamte Inhalt dieses Ordners gelöscht.

Ändern des Zeitintervalls

Standardmäßig zeigen integrierte Berichte Daten für den letzten Tag an. Wenn Sie jedoch das Zeitintervall für einen integrierten Bericht ändern möchten, können Sie den Bericht als benutzerdefinierten Bericht speichern. Das neue Intervall gilt für alle Diagramme im Bericht. In der folgenden Tabelle werden die Zeitintervalloptionen beschrieben.

Ändern Sie das Zeitintervall

1. Klicken Sie im linken Bereich des Reporting-Tools auf einen Bericht.

2. Klicken Sie auf der Berichtssymbolleiste auf **Dauer**und dann auf ein Zeitintervall.

Einstellen der Datenquelle und Zeitzone

Sie können Daten aus verschiedenen Datenquellen abrufen, um sie in den Berichten anzuzeigen. Sie können auch die Zeitzone für die Berichte definieren und die Zeitauswahl des aktuell angezeigten Berichts auf alle Berichte anwenden, einschließlich der integrierten Berichte.

Legen Sie die Datenquelle und die Zeitzone fest

1. Klicken Sie im **Berichtstool**auf der Berichtssymbolleiste auf **Einstellungen**.
2. Wählen **Sie im Dialogfeld Einstellungen unter** Datenquelle die Datenquelle aus, aus der Sie die Leistungsindikatoreninformationen abrufen möchten.
3. Führen Sie einen oder beide der folgenden Schritte aus:
   - Wenn sich das Werkzeug an den Zeitraum erinnern soll, für den ein Diagramm dargestellt wird, aktivieren Sie das Kontrollkästchen **Zeitauswahl für Diagramme** speichern.
   - Wenn die Berichte die Zeiteinstellungen Ihrer NetScaler-Appliance verwenden sollen, aktivieren Sie das Kontrollkästchen **Zeitzone der Appliance verwenden** .

Exportieren und Importieren von benutzerdefinierten Berichten

Sie können Berichte mit anderen NetScaler-Administratoren teilen, indem Sie Berichte exportieren. Sie können auch Berichte importieren.

Exportieren oder importieren Sie benutzerdefinierte Berichte

1. Klicken Sie im linken Bereich des Reporting-Tools neben Benutzerdefinierte Berichte auf das Symbol **Klicken, um benutzerdefinierte Berichte zu verwalten** .
2. Aktivieren Sie das Kontrollkästchen, das dem Bericht entspricht, den Sie exportieren oder importieren möchten, und klicken Sie dann auf **Exportieren** oder **Importieren**.

   > **Hinweis**:
   >
   > Wenn Sie die Datei exportieren, wird sie in ein .gz-Dateiformat exportiert.

Mit Diagrammen arbeiten

Verwenden Sie Diagramme, um Zähler oder Gruppen von Leistungsindikatoren darzustellen und zu überwachen. Sie können bis zu vier Diagramme in einen Bericht aufnehmen. In jedem Diagramm können Sie bis zu 32 Zähler darstellen. Die Diagramme können verschiedene grafische Formate verwenden (z. B. Fläche und Balken). Sie können die Diagramme innerhalb des Berichts nach oben oder un-

ten verschieben, die Farben und die visuelle Anzeige für jeden Leistungsindikator in einem Diagramm anpassen und ein Diagramm löschen, wenn Sie es nicht überwachen möchten.

In allen Berichtsdiagrammen steht die horizontale Achse für die Zeit und die vertikale Achse für den Wert des Zählers.

Hinzufügen eines Diagramms

Wenn Sie einem Bericht ein Diagramm hinzufügen, wird das Diagramm Systemübersicht mit dem Zähler der CPU-Auslastung für den letzten Tag angezeigt.

> **Hinweis**:
>
> Wenn Sie einem integrierten Bericht Diagramme hinzufügen und den Bericht beibehalten möchten, müssen Sie den Bericht als benutzerdefinierten Bericht speichern.

Gehen Sie wie folgt vor, um einem Bericht ein Diagramm hinzuzufügen.

Hinzufügen eines Diagramms zu einem Bericht

1. Klicken Sie im linken Bereich des Reporting-Tools auf einen Bericht.
2. Klicken Sie unter dem Diagramm, in dem Sie das neue Diagramm hinzufügen möchten, auf das Symbol Hinzufügen.

Ändern eines Diagramms

Sie können ein Diagramm ändern, indem Sie die Funktionsgruppe ändern, für die die Statistiken angezeigt werden, und indem Sie verschiedene Leistungsindikatoren auswählen.

Ein Diagramm ändern

1. Klicken Sie im linken Bereich des Reporting-Tools auf einen Bericht.
2. Klicken Sie unter dem Diagramm, das Sie ändern möchten, auf Leistungsindikatoren.
3. Geben Sie im angezeigten Dialogfeld im Feld Titel einen Namen für das Diagramm ein.
4. Führen Sie neben dem Plotdiagramm für einen der folgenden Schritte aus:
   - Klicken Sie auf Globale Systemstatistiken, um Leistungsindikatoren für globale Leistungsindikatoren wie Integrierter Cache und Komprimierung zu plotten.
   - Um Entitätsindikatoren für Entitätstypen wie Lastenausgleich und GSLB zu plotten, klicken Sie auf Systementitätsstatistik.
5. Klicken Sie in der Gruppe Auswählen auf die gewünschte Entität.
6. Klicken Sie unter Zähler unter Verfügbar auf einen oder mehrere Zählernamen, die Sie plotten möchten, und klicken Sie dann auf die Schaltfläche >.

7. Wenn Sie in Schritt 4 System-Entitätsstatistiken ausgewählt haben, klicken Sie auf der Registerkarte Entitäten unter Verfügbar auf einen oder mehrere Entitätsinstanznamen, die Sie plotten möchten, und klicken Sie dann auf die Schaltfläche >.
8. Klicken Sie auf OK.

Ein Diagramm anzeigen

Sie können die grafischen Formate der gezeichneten Zähler in einem Diagramm angeben. Diagramme können als Liniendiagramme, Spline-Diagramme, Schrittliniendiagramme, Streudiagramme, Flächendiagramme, Balkendiagramme, gestapelte Flächendiagramme und gestapelte Balkendiagramme angezeigt werden. Sie können auch den Zeichnungsbereich eines Diagramms vergrößern, verkleinern oder einen Bildlauf innerhalb des Zeichnungsbereichs durchführen. Sie können die Ansicht für alle Datenquellen für 1 Stunde, 1 Tag, 1 Woche, 1 Monat, 1 Jahr und 3 Jahre vergrößern oder verkleinern.

Weitere Optionen zum Anpassen der Ansicht eines Diagramms sind das Anpassen der Diagrammachsen, das Ändern der Hintergrund- und Kantenfarbe der Zeichnungsfläche, das Anpassen der Farbe und Größe der Raster und das Anpassen der Anzeige jedes Datensatzes (Zählers) in einem Diagramm.

Datensatznummern, z. B. Datensatz 1, entsprechen der Reihenfolge, in der die Zähler in Ihrem Diagramm am unteren Rand des Diagramms angezeigt werden. Wenn beispielsweise die CPU-Auslastung und die Speicherauslastung in erster und zweiter Reihenfolge am unteren Rand des Diagramms angezeigt werden, entspricht die CPU-Auslastung dem Datensatz 1 und die Speicherauslastung entspricht dem Datensatz 2.

Wenn Sie einen integrierten Bericht ändern, müssen Sie den Bericht als benutzerdefinierten Bericht speichern, um Ihre Änderungen beizubehalten.

Ändern des Diagrammtyps eines Diagramms

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Bereich unter dem Diagramm, das Sie anzeigen möchten, auf der Diagrammsymbolleiste auf **Anpassen**.
3. Klicken Sie auf der Registerkarte **Diagramm** unter **Kategorie**auf **Plottyp**, und klicken Sie dann auf den Diagrammtyp, den Sie für das Diagramm anzeigen möchten. Wenn Sie das Diagramm in 3D anzeigen möchten, aktivieren Sie das Kontrollkästchen 3D verwenden.

Richten Sie ein Diagramm mit detaillierten Daten neu aus

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich auf der Berichtssymbolleiste auf **Vergrößern**, und führen Sie eine oder beide der folgenden Aktionen aus:

- Um das Diagramm neu zu fokussieren, um Daten für ein bestimmtes Zeitfenster anzuzeigen, ziehen Sie den Cursor von der Startzeit zur Endzeit. Beispielsweise können Sie Daten für einen Zeitraum von einer Stunde an einem bestimmten Tag anzeigen.
- Um das Diagramm neu zu fokussieren, um Daten für einen Datenpunkt anzuzeigen, klicken Sie einfach einmal auf das Diagramm, in dem Sie vergrößern möchten, und erhalten Sie detailliertere Informationen.

3. Wenn Sie über den gewünschten Zeitraum verfügen, für den Sie detaillierte Daten anzeigen möchten, klicken Sie auf der Berichtssymbolleiste auf Tabellarische Ansicht. In der tabellarischen Ansicht werden die Daten in numerischer Form in Zeilen und Spalten angezeigt.

Numerische Daten für ein Diagramm anzeigen

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Bereich auf der Berichtssymbolleiste auf Tabellarische Ansicht. Um zur grafischen Ansicht zurückzukehren, klicken Sie auf **Grafische Ansicht**.

> **Hinweis**: Sie können die numerischen Daten auch in der grafischen Ansicht anzeigen, indem Sie den Mauszeiger über die Kerben in den Gitternetzlinien bewegen.

Scrollen Sie in einem Diagramm durch die Zeit

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich auf der Berichtssymbolleiste auf **Bildlauf**, und klicken Sie dann in das Diagramm, und ziehen Sie den Cursor in die Richtung, für die Sie Daten für einen neuen Zeitraum anzeigen möchten. Wenn Sie beispielsweise Daten in der Vergangenheit anzeigen möchten, ziehen Sie nach links.

Ändern der Hintergrund- und Textfarbe eines Diagramms

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Bereich unter dem Diagramm, für das Sie die Achsen anpassen möchten, auf **Anpassen**.
3. Klicken Sie auf der Registerkarte **Diagramm** unter **Kategorie**auf eine oder mehrere der folgenden Optionen:
   - Um die Hintergrundfarbe zu ändern, klicken Sie auf **Hintergrundfarbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.
   - Um die Textfarbe zu ändern, klicken Sie auf **Textfarbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.

Passen Sie die Achsen eines Diagramms an

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Bereich unter dem Diagramm, für das Sie die Achsen anpassen möchten, auf **Anpassen**.
3. Klicken Sie auf der Registerkarte **Diagramm** unter Kategorie auf eine oder mehrere der folgenden Optionen:
   - Um den Maßstab der linken Y-Achse zu ändern, klicken Sie auf **Linke Y-Achse**, und wählen Sie dann den gewünschten Maßstab aus.
   - Um den Maßstab der rechten Y-Achse zu ändern, klicken Sie auf Y-Achse rechts, wählen Sie im zu plottenen Datensatz den Datumssatz aus, und wählen Sie dann den gewünschten Maßstab aus.

     > Hinweis:
     > Die Datensatznummern, z. B. Datensatz 1, entsprechen der Reihenfolge, in der die Zähler im Diagramm am unteren Rand des Diagramms angezeigt werden. Wenn beispielsweise die CPU-Auslastung und die Speicherauslastung in erster und zweiter Reihenfolge am unteren Rand des Diagramms angezeigt werden, entspricht die CPU-Auslastung dem Datensatz 1 und die Speicherauslastung entspricht dem Datensatz 2.
   - Um jeden Datensatz in einer eigenen verdeckten Y-Achse zu plotten, klicken Sie auf Mehrere Achsen und dann auf Aktivieren.

Ändern der Hintergrundfarbe, Kantenfarbe und Gitternetzlinien für eine Zeichnungsfläche eines Diagramms

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Bereich unter dem Diagramm, für das Sie die Zeichnungsfläche anpassen möchten, auf **Anpassen**.
3. Klicken Sie auf der Registerkarte **Zeichnungsfläche** unter Kategorie auf eine oder mehrere der folgenden Optionen:
   - Um die Hintergrundfarbe und Kantenfarbe des Diagramms zu ändern, klicken Sie auf **Hintergrundfarbe und Kantenfarbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.
   - Um die horizontalen oder vertikalen Raster des Diagramms zu ändern, klicken Sie auf **Horizontale Raster** oder **Vertikale Raster**, und wählen Sie dann die Optionen für die Anzeige der Raster, Rasterbreite, Rasterfarbe, Transparenz und Effekte aus.

Ändern der Farbe und des Diagrammtyps eines Datensatzes

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.

2. Klicken Sie im rechten Bereich unter dem Diagramm, für das Sie die Anzeige des Datensatzes (Leistungsindikatoren) anpassen möchten, auf **Anpassen**.
3. Wählen Sie auf der Registerkarte **Datensatz** unter Datensatz auswählen den Datensatz (Zähler) aus, für den Sie die grafische Anzeige anpassen möchten.
   Hinweis: Die Datensatznummern, z. B. Datensatz 1, entsprechen der Reihenfolge, in der die Zähler in Ihrem Diagramm am unteren Rand des Diagramms angezeigt werden. Wenn beispielsweise die
   CPU-Auslastung und die
   Speicherauslastung in erster und zweiter Reihenfolge am unteren Rand des Diagramms angezeigt werden, entspricht die
   CPU-Auslastung dem
   Datensatz 1 und die
   Speicherauslastung entspricht dem
   Datensatz 2.
4. Führen Sie unter Kategorie eine oder mehrere der folgenden Aktionen aus:
   - Um die Hintergrundfarbe zu ändern, klicken Sie auf **Farbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.
   - Um den Diagrammtyp zu ändern, klicken Sie auf **Plottyp**, und wählen Sie dann den Diagrammtyp aus, der für den Datensatz angezeigt werden soll. Wenn Sie das Diagramm als 3D anzeigen möchten, aktivieren Sie das Kontrollkästchen 3D verwenden.

Exportieren von Diagrammdaten nach Excel

Zur weiteren Datenanalyse können Sie Diagramme in einem kommagetrennten Format (CSV) nach Excel exportieren.

So exportieren Sie Diagrammdaten nach Excel

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Bereich unter dem Diagramm mit den Daten, die Sie nach Excel exportieren möchten, auf **Exportieren**.

Löschen eines Diagramms

Wenn Sie ein Diagramm nicht verwenden möchten, können Sie es aus dem Bericht entfernen. Sie können Diagramme nur aus benutzerdefinierten Berichten dauerhaft entfernen. Wenn Sie ein Diagramm aus einem integrierten Bericht löschen und die Änderungen beibehalten möchten, müssen Sie den Bericht als benutzerdefinierten Bericht speichern.

Ein Diagramm löschen

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.

2. Klicken Sie im rechten Bereich unter dem Diagramm, das Sie löschen möchten, auf das Symbol **Löschen** .

Beispiele

Trendbericht zur CPU-Auslastung und Speicherauslastung der letzten Woche anzeigen

1. Erweitern Sie im linken Bereich des Reporting-Tools unter Integrierte Berichte die Option System.
2. Klicken Sie auf den Bericht CPU versus Speichernutzung und HTTP-Anforderungsrate.
3. Klicken Sie im rechten Bereich auf der Berichtssymbolleiste auf **Dauer**, und klicken Sie dann auf **Letzte Woche**.

Vergleichen Sie die Byte-Empfangsrate und die Byte-Übertragungsrate zwischen den beiden Schnittstellen für die letzte Woche

1. Klicken Sie im rechten Fensterbereich auf der Berichtssymbolleiste auf Erstellen.
2. Geben Sie im Feld **Berichtsname** einen Namen für den benutzerdefinierten Bericht ein (z. B. Custom_Interfaces), und klicken Sie dann auf **OK**. Der Bericht wird mit dem Standarddiagramm “Systemübersicht” erstellt, in dem der CPU-Auslastungszähler für die letzte Stunde dargestellt wird.
3. Klicken Sie unter Systemübersicht auf der Diagrammsymbolleiste auf Zähler.
4. Geben Sie im Zählerauswahlbereich unter Titel einen Namen für das Diagramm ein (z. B. Interfaces bytes data).
5. Klicken Sie im Diagramm für auf Systementitätsstatistik, und wählen Sie dann unter Gruppe auswählen die Option Schnittstelle aus.
6. Klicken Sie auf der Registerkarte **Entitäten** auf einen oder mehrere Schnittstellennamen, die Sie plotten möchten (z. B. 1/1 und 1/2), und klicken Sie dann auf die Schaltfläche >.
7. Klicken Sie auf der Registerkarte Leistungsindikatoren auf empfangene Bytes (Rate) und übertragene Bytes (Rate), und klicken Sie dann auf die Schaltfläche >.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf der Berichtssymbolleiste auf **Dauer**und dann auf **Letzte Woche**.

Stoppen und Starten des Datenerfassungsdienstprogramms

Das Dienstprogramm zur Datenerfassung wird automatisch ausgeführt `nscollect`, wenn Sie den NetScaler starten. Dieses Dienstprogramm ruft die Anwendungsleistungsdaten ab und speichert sie in Form von Datenquellen auf dem ADC. Sie können bis zu 32 Datenquellen erstellen. Die Standarddatenquelle ist `/var/log/db/default`.

Das Datenerfassungsdienstprogramm erstellt Datenbanken für globale Leistungsindikatoren und entitätsspezifische Leistungsindikatoren und verwendet diese Daten zum Generieren von Berichten. Global-Counter-Datenbanken werden unter erstellt `/var/log/db/<DataSourceName>`. Die entity-spezifischen Datenbanken werden basierend auf den Entitäten erstellt, die auf dem NetScaler konfiguriert sind, und für jeden Entitätstyp in `/var/log/db/<DataSourceName/EntityNameDB>` wird ein separater Ordner erstellt.

`nscollect` ruft alle 5 Minuten Daten ab. Es speichert Daten in 5-Minuten-Granularität für einen Tag, stündlich für die letzten 30 Tage und täglich für drei Jahre.

Möglicherweise müssen Sie das Datenerfassungsdienstprogramm anhalten und neu starten, wenn die Daten nicht korrekt aktualisiert werden oder die Berichte beschädigte Daten anzeigen.

Stopp `nscollect`

Geben Sie in der Befehlszeile Folgendes ein:

```
/netscaler/nscollect stop
```

Starten Sie nscollect in der aktuellen SSH-Sitzung mit dem NetScaler:

Geben Sie in der Befehlszeile Folgendes ein:

```
/netscaler/nscollect start
```

Starten Sie nscollect auf dem lokalen System:

Geben Sie in der Befehlszeile Folgendes ein:

```
/netscaler/nscollect start &
```

CloudBridge-Connector

May 11, 2023

Hinweis: Die aktuelle NetScaler 1000V-Version unterstützt diese Funktion nicht.

Die CloudBridge Connector-Funktion der NetScaler Appliance verbindet Unternehmensrechenzentren mit externen Clouds und Hosting-Umgebungen und macht die Cloud so zu einer sicheren Erweiterung Ihres Unternehmensnetzwerks. Cloud-gehostete Anwendungen werden so angezeigt, als ob sie in einem zusammenhängenden Unternehmensnetzwerk ausgeführt würden. Mit Citrix CloudBridge Connector können Sie Ihre Rechenzentren um die Kapazität und Effizienz erweitern, die von Cloud-Anbietern verfügbar sind.

Mit dem CloudBridge Connector können Sie Ihre Anwendungen in die Cloud verlagern, um Kosten zu senken und die Zuverlässigkeit zu erhöhen.

Sie können den CloudBridge Connector nicht nur zwischen einem Rechenzentrum und einer Cloud verwenden, sondern auch zwei Rechenzentren verbinden, um eine sichere und beschleunigte Verbindung mit hoher Kapazität zu gewährleisten.

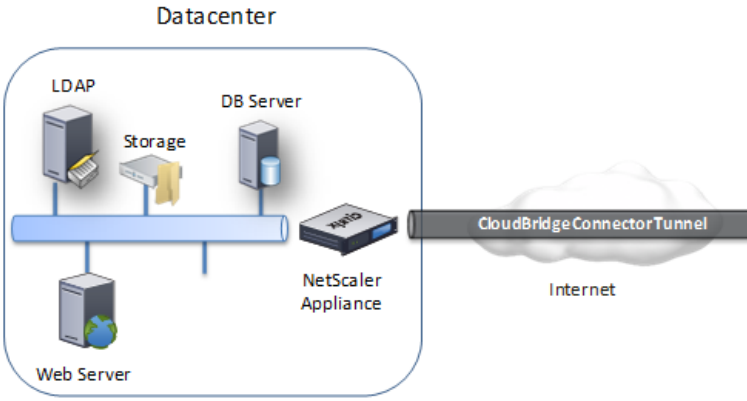
CloudBridge Connector verstehen

Um die Citrix CloudBridge Connector-Lösung zu implementieren, verbinden Sie ein Rechenzentrum mit einem anderen Rechenzentrum oder einer externen Cloud, indem Sie einen Tunnel einrichten, der als CloudBridge Connector-Tunnel bezeichnet wird.

Um ein Rechenzentrum mit einem anderen Rechenzentrum zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen zwei NetScaler-Appliances ein, eine in jedem Rechenzentrum.

Um ein Rechenzentrum mit einer externen Cloud (z. B. Amazon AWS-Cloud) zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler Appliance im Rechenzentrum und einer virtuellen Appliance (VPX) ein, die sich in der Cloud befindet. Der Remote-Endpunkt kann ein CloudBridge Connector oder ein NetScaler VPX mit Premium-Lizenz sein.

Die folgende Abbildung zeigt einen CloudBridge Connector-Tunnel, der zwischen einem Rechenzentrum und einer externen Cloud eingerichtet wurde.



Die Appliances, zwischen denen ein CloudBridge Connector-Tunnel eingerichtet ist, werden als *Endpunkte* oder *Peers* des CloudBridge Connector-Tunnels bezeichnet.

Ein CloudBridge Connector-Tunnel verwendet die folgenden Protokolle:

- Generisches Routing Encapsulation (GRE) -Protokoll
- IPSec-Protokollsuite mit offenem Standard im Transportmodus

Das GRE-Protokoll bietet einen Mechanismus zur Kapselung von Paketen aus einer Vielzahl von Netzwerkprotokollen, die über ein anderes Protokoll weitergeleitet werden. GRE wird verwendet, um:

- Verbinden Sie Netzwerke, auf denen Nicht-IP- und nicht routbare Protokolle ausgeführt werden.
- Brücke über ein Wide Area Network (WAN).
- Erstellen Sie einen Transporttunnel für jede Art von Verkehr, der unverändert über ein anderes Netzwerk gesendet werden muss.

Das GRE-Protokoll kapselt Pakete, indem es den Paketen einen GRE-Header und einen GRE-IP-Header hinzufügt.

Die Internet Protocol Security (IPSec) -Protokollsuite sichert die Kommunikation zwischen Peers im CloudBridge Connector-Tunnel.

In einem CloudBridge Connector-Tunnel stellt IPSec Folgendes sicher:

- Integrität der Daten
- Authentifizierung des Datenursprungs
- Vertraulichkeit der Daten (Verschlüsselung)
- Schutz vor Replay-Angriffen

IPSec verwendet den Transportmodus, in dem das GRE-gekapselte Paket verschlüsselt wird. Die Verschlüsselung erfolgt über das Encapsulating Security Payload (ESP) -Protokoll. Das ESP-Protokoll gewährleistet die Integrität des Pakets mithilfe einer HMAC-Hash-Funktion und gewährleistet die Vertraulichkeit durch die Verwendung eines Verschlüsselungsalgorithmus. Nachdem das Paket verschlüsselt und der HMAC berechnet wurde, wird ein ESP-Header generiert. Der ESP-Header wird nach dem GRE-IP-Header eingefügt, und am Ende der verschlüsselten Payload wird ein ESP-Trailer eingefügt.

Peers im CloudBridge Connector-Tunnel verwenden das Internet Key Exchange Version (IKE) -Protokoll (Teil der IPSec-Protokollsuite), um eine sichere Kommunikation wie folgt auszuhandeln:

- Die beiden Peers authentifizieren sich gegenseitig, indem sie eine der folgenden Authentifizierungsmethoden verwenden:
  - **Authentifizierung mit vorab gemeinsam genutzten Schlüsseln**. Eine Textzeichenfolge, die als Pre-Shared Key bezeichnet wird, wird auf jedem Peer manuell konfiguriert. Die Pre-Shared-Schlüssel der Peers werden zur Authentifizierung miteinander abgeglichen. Damit die Authentifizierung erfolgreich ist, müssen Sie daher auf jedem Peer denselben Pre-Shared-Schlüssel konfigurieren.
  - **Authentifizierung digitaler Zertifikate**. Der Initiator-Peer (Absender) signiert Nachrichtenaustauschdaten mit seinem privaten Schlüssel, und der andere Empfänger-Peer verwendet den öffentlichen Schlüssel des Absenders, um die Signatur zu überprüfen. In der Regel wird der öffentliche Schlüssel in Nachrichten ausgetauscht, die ein X.509v3-Zertifikat enthalten. Dieses Zertifikat bietet ein gewisses Maß an Sicherheit, dass die im Zertifikat dargestellte Identität eines Peers mit einem bestimmten öffentlichen Schlüssel verknüpft ist.
- Die Fachkollegen verhandeln dann, um eine Einigung über Folgendes zu erzielen:
  - Ein Verschlüsselungsalgorithmus.

- Kryptografische Schlüssel zum Verschlüsseln von Daten in einem Peer und zum Entschlüsseln der Daten in dem anderen.

Diese Vereinbarung über das Sicherheitsprotokoll, den Verschlüsselungsalgorithmus und die kryptografischen Schlüssel wird als Security Association (SA) bezeichnet. SAs sind Einwegsysteme (Simplex). Wenn beispielsweise zwei Peers, CB1 und CB2, über einen Connector-Tunnel kommunizieren, hat CB1 zwei Sicherheitszuordnungen. Ein SA wird für die Verarbeitung ausgehender Pakete verwendet, und der andere SA wird für die Verarbeitung eingehender Pakete verwendet.

SAs laufen nach einer bestimmten Zeit ab, die als *Lebensdauer*bezeichnet wird. Die beiden Peers verwenden das Internet Key Exchange (IKE) -Protokoll (Teil der IPSec-Protokollsuite), um neue kryptografische Schlüssel auszuhandeln und neue SAs einzurichten. Der Zweck der begrenzten Lebensdauer ist es, Angreifer daran zu hindern, einen Schlüssel zu knacken.

In der folgenden Tabelle sind einige IPSec-Eigenschaften aufgeführt, die von einer NetScaler-Appliance unterstützt werden:

IPsec-Eigenschaften	Unterstützte Typen
IKE-Versionen	V1, V2
IKE DH-Gruppe	Eine NetScaler Appliance unterstützt nur die DH-Gruppe 2 (1024-Bit-MODP-Algorithmus) sowohl für iKEV1 als auch für iKEv2.
IKE-Authentifizierungsmethoden	Authentifizierung mit vorab gemeinsam genutzten Schlüsseln, Authentifizierung mit digitalen Zertifikaten
Verschlüsselungsalgorithmus	AES (128 Bit), AES 256 (256 Bit), 3DES
Hash-Algorithmus	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5

Überwachung von CloudBridge Connector-Tunneln

May 11, 2023

Sie können die Statistiken zur Überwachung der Leistung eines CloudBridge Connector-Tunnels anzeigen. Verwenden Sie die GUI oder die NetScaler-Befehlszeile, um die CloudBridge Connector-Tunnelstatistiken auf einer NetScaler-Appliance anzuzeigen.

In der folgenden Tabelle sind die statistischen Zähler aufgeführt, die für die Überwachung von CloudBridge Connector-Tunneln auf einer NetScaler-Appliance verfügbar sind.

Statistischer Zähler	Spezifiziert
Bytes empfangen	Gesamtzahl der Byte, die die NetScaler-Appliance seit dem letzten Start der Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen hat.
Byte gesendet	Gesamtzahl der Byte, die von der NetScaler-Appliance seit dem letzten Start der Appliance über alle konfigurierten CloudBridge Connector-Tunnel gesendet wurden.
Empfangene Pakete	Gesamtzahl der Pakete, die die NetScaler-Appliance seit dem letzten Start der Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen hat.
Gesendete Pakete	Gesamtzahl der Pakete, die seit dem letzten Start der Appliance von der NetScaler-Appliance über alle konfigurierten CloudBridge Connector-Tunnel gesendet wurden.
Empfangsrate in Byte	Anzahl der Byte pro Sekunde, die von der NetScaler-Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen wurden.
Übertragungsrate in Byte	Anzahl der Byte pro Sekunde, die von der NetScaler-Appliance über alle konfigurierten CloudBridge Connector-Tunnel gesendet werden
Rate empfangener Pakete	Anzahl der Byte pro Sekunde, die von der NetScaler-Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen wurden
Geschwindigkeit gesendeter Pakete	Anzahl der Byte pro Sekunde, die von der NetScaler-Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen wurden

Alle diese Zähler werden auf 0 zurückgesetzt, wenn die NetScaler-Appliance neu gestartet wird. Sie

steigen in den folgenden Phasen nicht an:

- Phase der Internet Key Exchange (IKE) -Authentifizierung (Pre-Shared Key) auf jedem konfigurierten CloudBridge Connector-Tunnel.
- Einrichtungsphase der IKE Security Association (SA) auf jedem konfigurierten CloudBridge Connector-Tunnel.

So zeigen Sie CloudBridge Connector-Tunnelstatistiken mithilfe der NetScaler-Befehlszeile an

Geben Sie in der Befehlszeile Folgendes ein:

- **Stat-IPSec-Zähler**

So zeigen Sie CloudBridge Connector-Tunnelstatistiken mithilfe der GUI an

1. Greifen Sie auf die GUI zu, indem Sie einen Webbrowser verwenden, um eine Verbindung zur IP-Adresse der NetScaler-Appliance herzustellen.
2. Navigieren Sie auf der **Registerkarte Konfiguration** zu **System** > **CloudBridge**Connector.
3. Klicken Sie auf der CloudBridge Connector-Seite auf CloudBridge Connector **erstellen/überwachen**. Die Diagramme **IPSec-Bytes** und **IPSec-Pakete** zeigen die empfangene Byte-Rate, die gesendete Byte-Rate, die empfangene Paketrate und die gesendete Paketrate aller CloudBridge Connector-Tunnel, die auf der NetScaler-Appliance konfiguriert sind.

```
    > stat ipsec counters
    Secure tunnel(s) summary
                        Rate (/s)        Total
    Bytes Received    0    2811248
    Bytes Sent            0    157460630
    Packets Received    0    56787
    Packets Sent        0    200910
    Done
    >
<!--NeedCopy-->
```

Konfiguration eines CloudBridge Connector-Tunnels zwischen zwei Rechenzentren

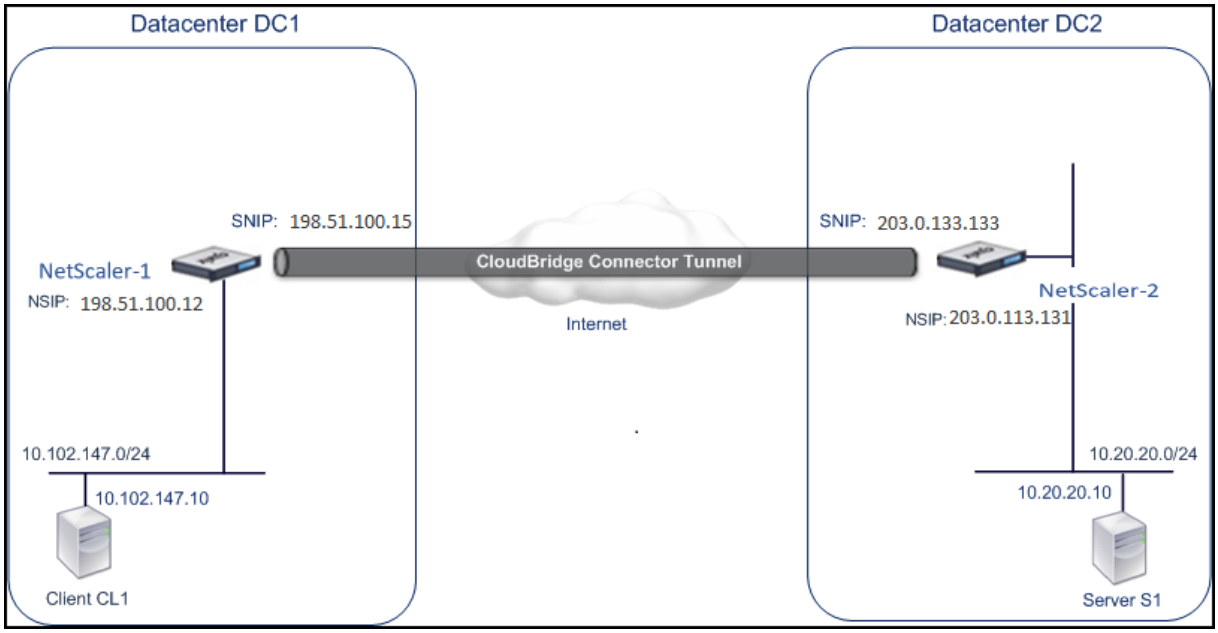
May 11, 2023

Sie können einen CloudBridge Connector-Tunnel zwischen zwei verschiedenen Rechenzentren konfigurieren, um Ihr Netzwerk zu erweitern, ohne es neu konfigurieren zu müssen, und die Funktionen der beiden Rechenzentren nutzen. Ein CloudBridge Connector-Tunnel zwischen den beiden geografisch getrennten Rechenzentren ermöglicht es Ihnen, Redundanz zu implementieren und Ihr

Setup vor Ausfällen zu schützen. Der CloudBridge Connector-Tunnel trägt dazu bei, die Infrastruktur und Ressourcen in den Rechenzentren optimal zu nutzen. Die Anwendungen, die in den beiden Rechenzentren verfügbar sind, werden für den Benutzer als lokal angezeigt.

Um ein Rechenzentrum mit einem anderen Rechenzentrum zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance in einem Rechenzentrum und einer NetScaler-Appliance im anderen Rechenzentrum ein.

Betrachten Sie zur Veranschaulichung des CloudBridge Connector-Tunnels zwischen Rechenzentren ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen der NetScaler-Appliance NS_Appliance-1 im Rechenzentrum DC1 und der NetScaler-Appliance NS_Appliance-2 im Rechenzentrum DC2 eingerichtet wird.



Sowohl NS_Appliance-1 als auch NS_Appliance-2 funktionieren im L2- und L3-Modus. Sie ermöglichen die Kommunikation zwischen privaten Netzwerken in Rechenzentren DC1 und DC2. Im L3-Modus ermöglichen NS_Appliance-1 und NS_Appliance-2 die Kommunikation zwischen dem Client CL1 im Rechenzentrum DC1 und dem Server S1 im Rechenzentrum DC2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Da sich Client CL1 und Server S1 in unterschiedlichen privaten Netzwerken befinden, ist der L3-Modus auf NS_Appliance-1 und NS_Appliance-2 aktiviert, und die Routen werden wie folgt aktualisiert:

- CL1 hat eine Route zu NS_Appliance-1, um S1 zu erreichen.
- NS_Appliance-1 hat eine Route zu NS_Appliance-2, um S1 zu erreichen.
- S1 hat eine Route zu NS_Appliance-2, um CL1 zu erreichen.
- NS_Appliance-2 hat eine Route zu NS_Appliance-1, um CL1 zu erreichen.

In der folgenden Tabelle sind die Einstellungen der NetScaler-Appliance NS_Appliance-1 im Rechenzentrum DC1 aufgeführt.

In der folgenden Tabelle sind die Einstellungen der NetScaler-Appliance NS_Appliance-2 im Rechenzentrum DC2 aufgeführt.

Entität	Name	Details
Die NSIP-Adresse		198.51.100.12
SNIP-Adresse		198.51.100.15
CloudBridge Connector-Tunnel	Cloud_Connector_DC1-DC2	1. Lokale Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 198.51.100.15, 2. IP-Adresse des Remote-Endpunkts des CloudBridge Connector-Tunnels: 203.0.113.133. Name der GRE-Tunneldetails = Cloud_Connector_DC1-DC2, Name der IPSec-Profildetails = Cloud_Connector_DC1-DC2, Verschlüsselungsalgorithmus = AES, Hash-Algorithmus = HMAC SHA1

Punkte, die bei der Konfiguration des CloudBridge Connector-Tunnels zu beachten sind

Stellen Sie vor der Einrichtung eines CloudBridge Connector-Tunnels sicher, dass die folgenden Aufgaben abgeschlossen wurden:

1. Stellen Sie in jedem der beiden Rechenzentren eine NetScaler-Appliance bereit und richten Sie sie ein.
2. Stellen Sie sicher, dass die IP-Adressen der CloudBridge Connector-Tunnelendpunkte für einander zugänglich sind.

Konfigurationsprozedur

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance, die sich in einem Rechenzentrum befindet, und einer anderen NetScaler-Appliance, die sich im anderen Rechenzen-

trum befindet, einzurichten, verwenden Sie die GUI oder die Befehlszeilenschnittstelle einer der NetScaler-Appliances.

Wenn Sie die GUI verwenden, wird die auf der ersten NetScaler-Appliance erstellte CloudBridge Connector-Tunnelkonfiguration automatisch auf den anderen Endpunkt (die andere NetScaler-Appliance) des CloudBridge Connector-Tunnels übertragen. Daher müssen Sie nicht auf die GUI der anderen NetScaler-Appliance zugreifen, um die entsprechende CloudBridge Connector-Tunnelkonfiguration darauf zu erstellen.

Die CloudBridge Connector-Tunnelkonfiguration auf jeder der NetScaler-Appliances besteht aus den folgenden Entitäten:

- **IPSec-Profil**— Eine IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **GRE-Tunnel**— Ein IP-Tunnel gibt die lokale IP-Adresse (eine öffentliche SNIP-Adresse, die auf der lokalen NetScaler-Appliance konfiguriert ist), die Remote-IP-Adresse (eine öffentliche SNIP-Adresse, die auf der Remote-NetScaler-Appliance konfiguriert ist), das für die Einrichtung des CloudBridge Connector-Tunnels verwendete Protokoll (GRE) und eine IPSec-Profilentität an.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie den IP-Tunnel damit**— Eine PBR-Entität spezifiziert eine Reihe von Bedingungen und eine IP-Tunnelentität. Der Quell-IP-Adressbereich und der Ziel-IP-Bereich sind die Bedingungen für die PBR-Entität. Sie müssen den Quell-IP-Adressbereich und den Ziel-IP-Adressbereich festlegen, um das Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Stellen Sie sich beispielsweise ein Anforderungspaket vor, das von einem Client im Subnetz im ersten Rechenzentrum stammt und für einen Server im Subnetz im zweiten Rechenzentrum bestimmt ist. Wenn dieses Paket mit dem Quell- und Ziel-IP-Adressbereich der PBR-Entität auf der NetScaler-Appliance im ersten Rechenzentrum übereinstimmt, wird es über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

So erstellen Sie ein IPSEC-Profil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipsec profile <name> [-ikeVersion (V1 | V2)] [-encAlgo (AES | 3 DES)...] [-hashAlgo <hashAlgo\> ...] [-lifetime <positive_integer>] (-psk | (-publickey<string> -privatekey <string>-peerPublicKey <string >))[-livenessCheckInterval <positive_intege>][-replayWindowSize \< positive_integer>] [-ikeRetryInterval <positive_integer>] [-retransmissiontime <positive_integer>]`
- `show ipsec profile <name>`

Um einen IP-Tunnel zu erstellen und das IPSEC-Profil mithilfe der Befehlszeilenschnittstelle daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol <protocol>] [-ipsecProfileName <string>]`
- `show ipTunnel <name>`

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der Befehlszeilenschnittstelle daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = <remote_subnet_range> -ipTunnel <tunnel_name>`
- `apply ns pbrs`
- `show ns pbr <pbr_name>`

Beispiel

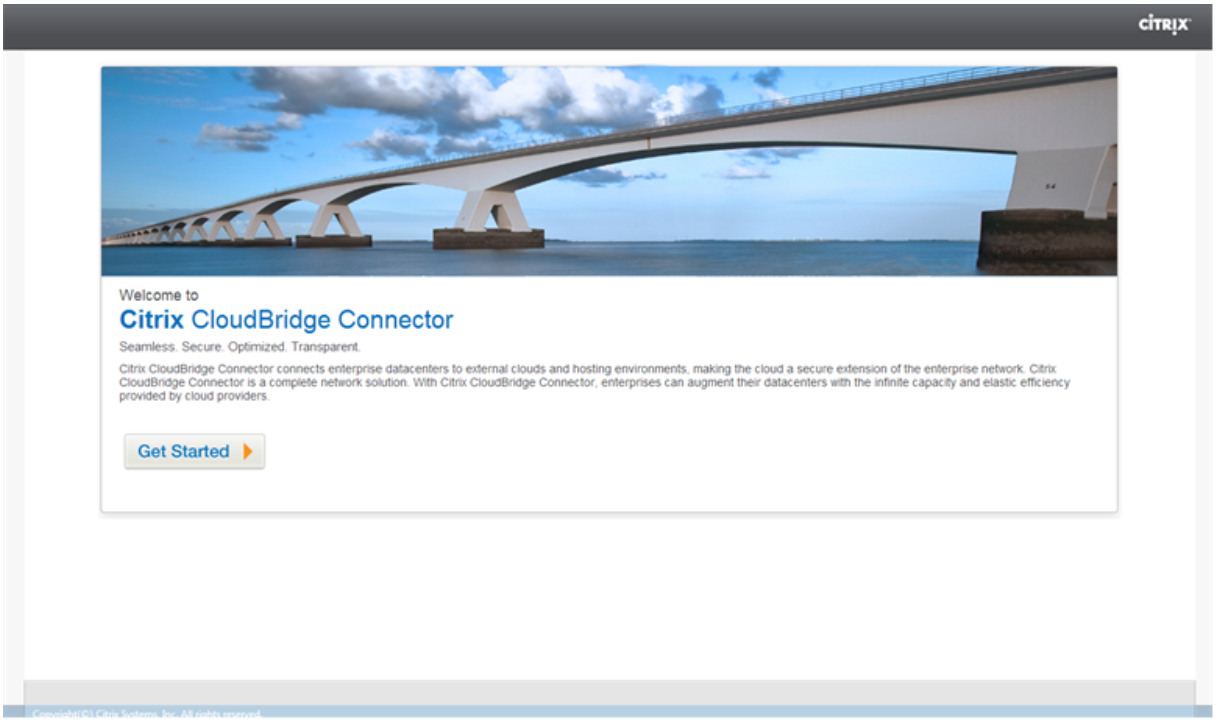
```
1  add ipsec profile Cloud_Connector_DC1-DC2  -encAlgo AES -hashAlgo
       HMAC_SHA1
2      Done
3      > add ipTunnel Cloud_Connector_DC1-DC2 203.0.113.133
           255.255.255.255 198.51.100.15 -protocol GRE -ipsecProfileName
           Cloud_Connector_DC1-DC2
4
5      Done
6      > add ns pbr PBR-DC1-DC2 ALLOW -srcIP 198.51.100.15 -destIP
           203.0.113.133 ipTunnel Cloud_Connector_DC1-DC2
7
8      Done
9      > apply ns pbrs
10
11     Done
12 <!--NeedCopy-->
```

So konfigurieren Sie einen CloudBridge Connector-Tunnel in einer NetScaler-Appliance mithilfe der GUI

1. Geben Sie die NSIP-Adresse einer NetScaler-Appliance in die Adresszeile eines Webbrowsers ein.
2. Melden Sie sich an der GUI der NetScaler-Appliance an, indem Sie Ihre Kontoanmeldeinformationen für die Appliance verwenden.
3. Navigieren Sie zu **System** > **CloudBridge Connector**.
4. Klicken Sie im rechten Bereich unter **Erste Schritte**auf CloudBridge **erstellen/überwachen**.

Wenn Sie zum ersten Mal einen CloudBridge Connector-Tunnel auf der Appliance konfigurieren, wird ein **Willkommensbildschirm** angezeigt.

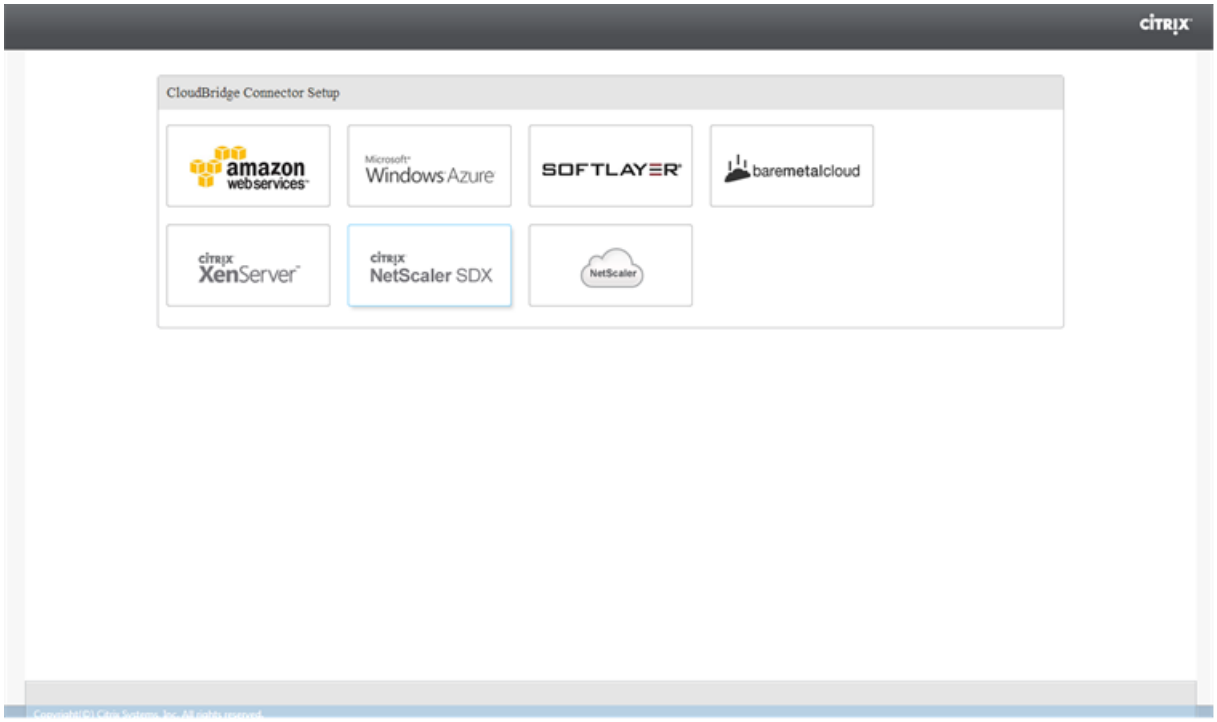
5. Klicken Sie auf dem **Willkommensbildschirm** auf **Get Started**.



Hinweis:

Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der NetScaler-Appliance konfiguriert haben, wird der Willkommensbildschirm nicht angezeigt, sodass Sie nicht auf Get Started klicken.

1. Klicken Sie im Bereich **CloudBridge Connector Setup** auf **NetScaler**.



1. Geben Sie im NetScaler-Bereich Ihre Kontoanmeldeinformationen für die Remote-NetScaler-Appliance ein. Klicken Sie auf **Weiter**.
2. Stellen Sie im Bereich **CloudBridge Connector-Einstellungen** den folgenden Parameter ein:
   - **CloudBridge Connector-Name**— Name für die CloudBridge Connector-Konfiguration auf der lokalen Appliance. Muss mit einem ASCII-Zeichen oder einem Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die CloudBridge Connector-Konfiguration erstellt wurde.
3. Stellen Sie unter **Lokale Einstellung**den folgenden Parameter ein:
   - **Subnetz-IP — IP-Adresse**des lokalen Endpunkts des CloudBridge Connector-Tunnels.
4. Stellen Sie unter **Remote Setting**den folgenden Parameter ein:
   - **Subnetz-IP — IP-Adresse**des Peer-Endpunkts des CloudBridge Connector-Tunnels.
5. Stellen Sie unter **PBR-Einstellung** die folgenden Parameter ein:
   - **Operation**— Entweder ist gleich (=) oder ist nicht gleich (! =) logischer Operator.
   - **Source IP Low — Niedrigste**Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden kann.
   - **Source IP High**— Die höchste Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden soll.
   - **Operation**— Entweder ist gleich (=) oder ist nicht gleich (! =) logischer Operator.

- Ziel-IP Low* — Niedrigste Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden kann.
- **Ziel-IP High**— Die höchste Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden soll.

6. (Optional) Stellen Sie unter **Sicherheitseinstellungen**die folgenden IPSec-Protokollparameter für den CloudBridge Connector-Tunnel ein:

   - **Verschlüsselungsalgorithmus**— Verschlüsselungsalgorithmus, der vom IPSec-Protokoll im CloudBridge-Tunnel verwendet wird.
   - **Hash-Algorithmus**— Hash-Algorithmus, der vom IPSec-Protokoll im CloudBridge-Tunnel verwendet wird.
   - **Schlüssel**— Wählen Sie eine der folgenden IPSec-Authentifizierungsmethoden aus, die von den beiden Peers verwendet werden sollen, um sich gegenseitig zu authentifizieren.
     - **Automatisch generierter Schlüssel**— Die Authentifizierung basiert auf einer Textzeichenfolge, einem sogenannten Pre-Shared Key (PSK), der automatisch von der lokalen Appliance generiert wird. Die PSK-Schlüssel der Peers werden zur Authentifizierung miteinander abgeglichen.
     - **Spezifischer Schlüssel**— Authentifizierung auf der Grundlage einer manuell eingegebenen PSK. Die PSKs der Peers werden zur Authentifizierung miteinander verglichen.
       * Pre Shared Security Key — Die Textzeichenfolge, die für die auf Pre-Shared Keys basierende Authentifizierung eingegeben wurde.
     - **Zertifikate hochladen**— Authentifizierung auf der Grundlage digitaler Zertifikate.
       * **Öffentlicher Schlüssel**— Ein lokales digitales Zertifikat, das verwendet wird, um die lokale NetScaler-Appliance gegenüber dem Peer zu authentifizieren, bevor IPSec-Sicherheitszuordnungen eingerichtet werden. Dasselbe Zertifikat sollte vorhanden und für den Peer Public Key-Parameter im Peer festgelegt sein.
       * **Privater Schlüssel**— Privater Schlüssel des lokalen digitalen Zertifikats.
       * **Peer Public Key**— Digitales Zertifikat des Peers. Wird verwendet, um den Peer zum lokalen Endpunkt zu authentifizieren, bevor IPSec-Sicherheitszuordnungen eingerichtet werden. Dasselbe Zertifikat sollte vorhanden und für den Public-Key-Parameter im Peer festgelegt sein.

7. Klicken Sie auf **Fertig**.

Die neue CloudBridge Connector-Tunnelkonfiguration auf beiden NetScaler-Appliances wird auf der Registerkarte Home der jeweiligen GUI angezeigt. Der aktuelle Status des CloudBridge Connector-Tunnels wird im Bereich Configured CloudBridge Connectors angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

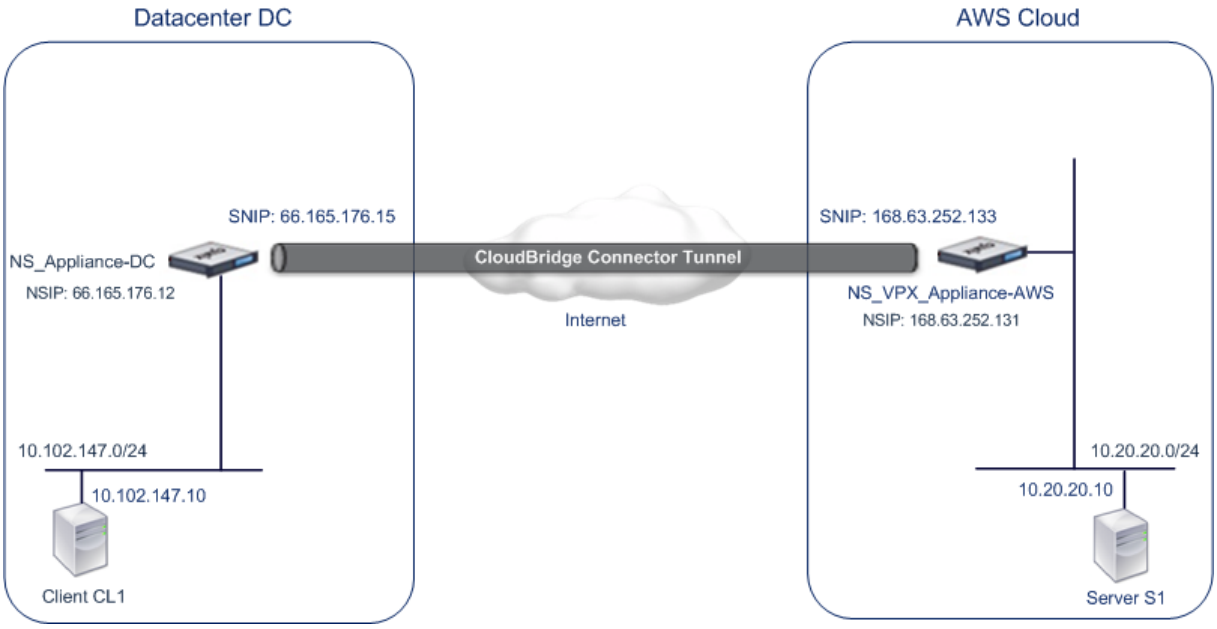
Konfiguration des CloudBridge Connector zwischen Rechenzentrum und AWS-Cloud

May 11, 2023

Sie können einen CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und der AWS-Cloud konfigurieren, um die Infrastruktur und die Rechenkapazitäten des Rechenzentrums und der AWS-Cloud zu nutzen. Mit AWS können Sie Ihr Netzwerk ohne Anfangsinvestitionen oder die Kosten für die Wartung der erweiterten Netzwerkinfrastruktur erweitern. Sie können Ihre Infrastruktur nach Bedarf nach oben oder unten skalieren. Sie können beispielsweise mehr Serverkapazitäten leasen, wenn die Nachfrage steigt.

Um ein Rechenzentrum mit der AWS-Cloud zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance, die sich im Rechenzentrum befindet, und einer virtuellen NetScaler-Appliance (VPX) in der AWS-Cloud ein.

Stellen Sie sich zur Veranschaulichung eines CloudBridge Connector-Tunnels zwischen einem Rechenzentrum und der Amazon AWS-Cloud ein Beispiel vor, in dem ein CloudBridge Connector-Tunnel zwischen der NetScaler-Appliance NS_Appliance-DC im Rechenzentrums-DC und der virtuellen NetScaler-Appliance (VPX) NS_VPX_Appliance-AWS eingerichtet wird.



Sowohl NS_Appliance-DC als auch NS_VPX_Appliance-AWS funktionieren im L3-Modus. Sie ermöglichen die Kommunikation zwischen privaten Netzwerken im Rechenzentrum DC und der AWS-Cloud. NS_Appliance-DC und NS_VPX_Appliance-AWS ermöglichen die Kommunikation zwischen Client CL1 im Rechenzentrum und Server S1 in der AWS-Cloud über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

> **Hinweis**:
>
> AWS unterstützt den L2-Modus nicht, daher muss auf beiden Endpunkten nur der L3-Modus aktiviert sein.

Für eine korrekte Kommunikation zwischen CL1 und S1 ist der L3-Modus auf NS_Appliance-DC und NS_VPX_Appliance-AWS aktiviert und die Routen werden wie folgt aktualisiert:

- CL1 hat eine Route zu NS_Appliance-DC, um S1 zu erreichen.
- NS_Appliance-DC haben eine Route zu NS_VPX_Appliance-AWS, um S1 zu erreichen.
- S1 sollte eine Route zu NS_VPX_Appliance-AWS haben, um CL1 zu erreichen.
- NS_VPX_Appliance-AWS haben eine Route zu NS_Appliance-DC, um CL1 zu erreichen.

In der folgenden Tabelle sind die Einstellungen der NetScaler-Appliance NS_Appliance-DC im Rechenzentrums-DC aufgeführt.

Entität	Name	Details
Die NSIP-Adresse		66.165.176.12
SNIP-Adresse		66.165.176.15

Entität	Name	Details
CloudBridge Connector-Tunnel	CC_Tunnel_DC-AWS	Lokale Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 66.165.176.15, Remote-Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 168.63.252.133, GRE-Tunneldetails — Name= cc_Tunnel_DC-AWS

In der folgenden Tabelle sind die Einstellungen für NetScaler VPX NS_VPX_Appliance-AWS in der AWS-Cloud aufgeführt.

Entität	Name	Details
NSIP-Adresse		10.102.25.30
Öffentliche EIP-Adresse, die der NSIP-Adresse zugeordnet ist		168.63.252.131
SNIP-Adresse		10.102.29.30
Öffentliche EIP-Adresse, die der SNIP-Adresse zugeordnet ist		168.63.252.133

Entität	Name	Details
CloudBridge Connector-Tunnel	CC_Tunnel_DC-AWS	Lokale Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 168.63.252.133, Remote-Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 66.165.176.15; **GRE-Tunneldetails Name= cc_Tunnel_DC-AWS, IPSec-Profildetails, Name= cc_Tunnel_DC-AWS, Verschlüsselungsalgorithm= AES, Hash-Algorithmus** = HMAC SHA1

Voraussetzungen

Stellen Sie vor der Einrichtung eines CloudBridge Connector-Tunnels sicher, dass die folgenden Aufgaben abgeschlossen wurden:

1. Installieren, konfigurieren und starten Sie eine Instanz der NetScaler Virtual Appliance (VPX) in der AWS-Cloud. Anweisungen zur Installation von NetScaler VPX in AWS finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf AWS.
2. Provisioning und Konfigurieren einer physischen NetScaler Appliance oder Bereitstellen und Konfigurieren einer virtuellen NetScaler Appliance (VPX) auf einer Virtualisierungsplattform im Rechenzentrum.
3. Stellen Sie sicher, dass die IP-Adressen der CloudBridge Connector-Tunnelendpunkte für einander zugänglich sind.

NetScaler VPX-Lizenz

Nach dem erstmaligen Instanzstart benötigt NetScaler VPX for AWS eine Lizenz. Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, lesen Sie den VPX Licensing Guide unter: http://support.citrix.com/article/CTX122426.

Sie müssen:

1. Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.

2. Laden Sie die Lizenz auf die Instanz hoch.

Wenn es sich um eine **kostenpflichtige** Marketplace-Instanz handelt, müssen Sie keine Lizenz installieren. Der richtige Funktionsumfang und die richtige Leistung werden automatisch aktiviert.

Konfigurationsschritte

Verwenden Sie die GUI der NetScaler-Appliance, um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance, die sich in einem Rechenzentrum befindet, und einer virtuellen NetScaler-Appliance (VPX) in der AWS-Cloud einzurichten.

Wenn Sie die GUI verwenden, wird die auf der NetScaler-Appliance erstellte CloudBridge Connector-Tunnelkonfiguration automatisch an den anderen Endpunkt oder Peer (den NetScaler VPX auf AWS) des CloudBridge Connector-Tunnels übertragen. Daher müssen Sie nicht auf die GUI (GUI) des NetScaler VPX auf AWS zugreifen, um die entsprechende CloudBridge Connector-Tunnelkonfiguration darauf zu erstellen.

Die CloudBridge Connector-Tunnelkonfiguration auf beiden Peers (die NetScaler-Appliance, die sich im Rechenzentrum befindet, und die virtuelle NetScaler-Appliance (VPX), die sich in der AWS-Cloud befindet) besteht aus den folgenden Entitäten:

- **IPSec-Profil**— Eine IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK an, die vom IPSec-Protokoll in beiden Peers des CloudBridge Connector-Tunnels verwendet werden sollen.
- **GRE-Tunnel**— Ein IP-Tunnel spezifiziert eine lokale IP-Adresse (eine öffentliche SNIP-Adresse, die auf dem lokalen Peer konfiguriert ist), eine Remote-IP-Adresse (eine auf dem Remote-Peer konfigurierte öffentliche SNIP-Adresse), ein Protokoll (GRE), das zur Einrichtung des CloudBridge Connector-Tunnels verwendet wird, und eine IPSec-Profilentität.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie den IP-Tunnel damit**— Eine PBR-Entität spezifiziert eine Reihe von Bedingungen und eine IP-Tunnelentität. Der Quell-IP-Adressbereich und der Ziel-IP-Bereich sind die Bedingungen für die PBR-Entität. Sie müssen den Quell-IP-Adressbereich und den Ziel-IP-Adressbereich festlegen, um das Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Betrachten Sie beispielsweise ein Anforderungspaket, das von einem Client im Subnetz im Rechenzentrum stammt und für einen Server im Subnetz in der AWS-Cloud bestimmt ist. Wenn dieses Paket mit dem Quell- und Ziel-IP-Adressbereich der PBR-Entität auf der NetScaler-Appliance im Rechenzentrum übereinstimmt, wird es über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

So erstellen Sie ein IPSEC-Profil mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- add ipsec profile <name> [-**ikeVersion** (V1 | V2)] [-**encAlgo** (AES | 3DES)...] [-**hashAlgo** <hashAlgo> ...] [-**lifetime** <positive_integer>] (-**psk** | (-**publickey** <string> -**privatekey** <string> -**peerPublicKey** <string>))[-**livenessCheckInterval** <positive_integer>] [-**replayWindowSize** <positive_integer>] [-**ikeRetryInterval** <positive_integer>] [-**retransmissiontime** <positive_integer>]
- **show ipsec profile** <name>

Um einen IP-Tunnel zu erstellen und das IPSEC-Profil mithilfe der Befehlszeilenschnittstelle daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol <protocol>] [-ipsecProfileName <string>]
- show ipTunnel <name>

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der Befehlszeilenschnittstelle daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

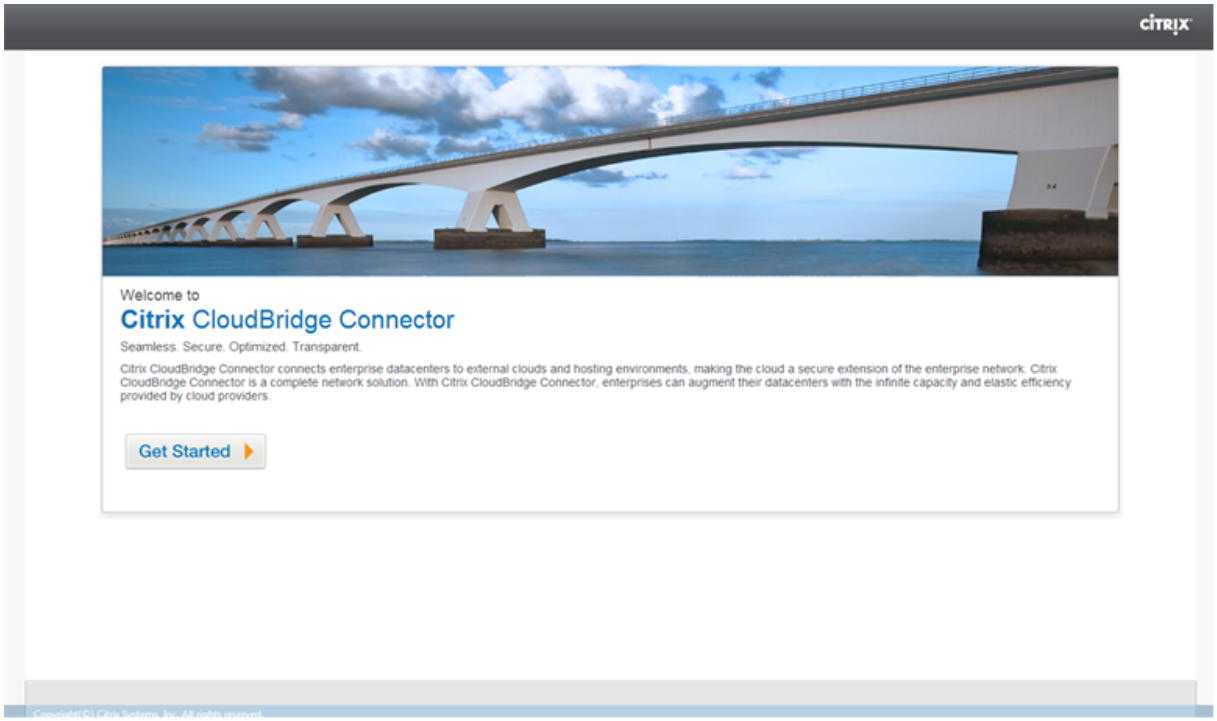
- add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = <remote_subnet_range> -ipTunnel <tunnel_name>
- apply ns pbrs
- show ns pbr <pbr_name>

Beispiel

```
1     > add ipsec profile CC_Tunnel_DC-AWS -encAlgo AES -hashAlgo
          HMAC_SHA1
2
3     Done
4     > add ipTunnel CC_Tunnel_DC-AWS 168.63.252.133 255.255.255.0
          66.165.176.15 - protocol GRE -ipsecProfileName CC_Tunnel_DC-AWS
5
6     Done
7     > add ns pbr PBR-DC-AWS ALLOW - srcIP 66.165.176.15 - destIP
          168.63.252.133 ipTunnel CC_Tunnel_DC-AWS
8
9     Done
10    > apply ns pbrs
11
12    Done
13 <!--NeedCopy-->
```

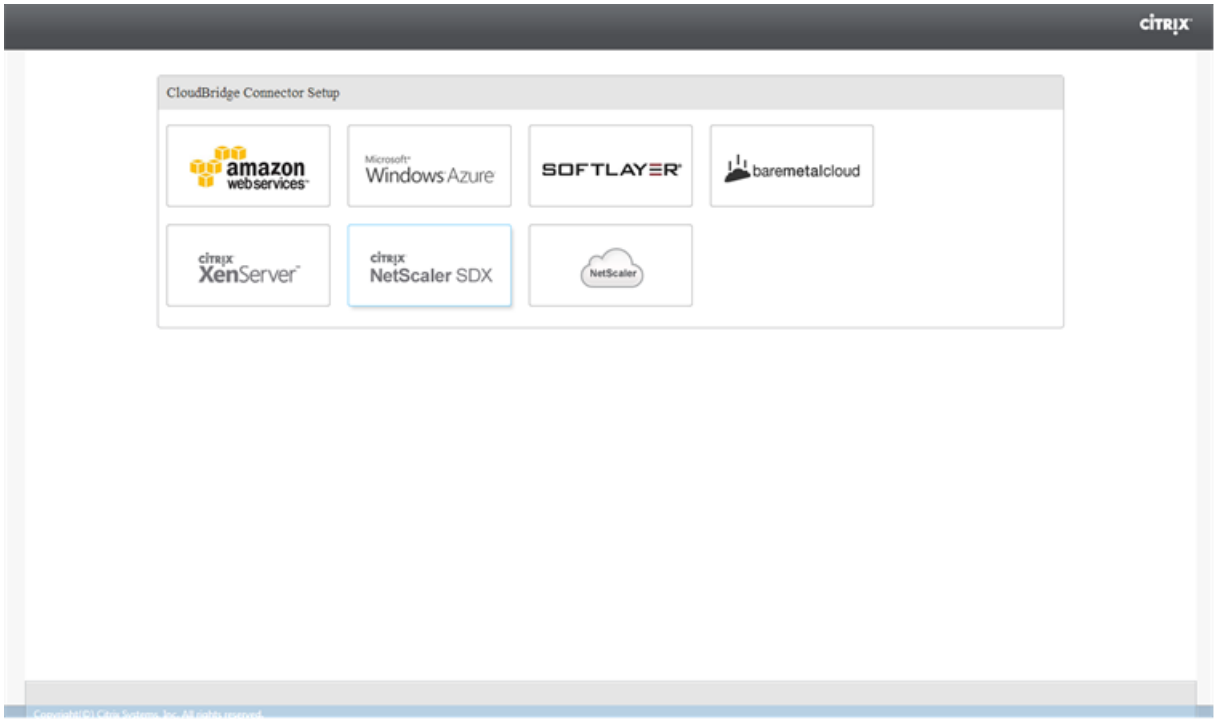

So konfigurieren Sie einen CloudBridge Connector-Tunnel in einer NetScaler-Appliance mithilfe der GUI

1. Geben Sie die NSIP-Adresse einer NetScaler-Appliance in die Adresszeile eines Webbrowsers ein.
2. Melden Sie sich an der GUI der NetScaler-Appliance an, indem Sie Ihre Kontoanmeldeinformationen für die Appliance verwenden.
3. Navigieren Sie zu **System** > **CloudBridge Connector**.
4. Klicken Sie im rechten Bereich unter **Erste Schritte**auf CloudBridge **erstellen/überwachen**.
5. Wenn Sie zum ersten Mal einen CloudBridge Connector-Tunnel auf der Appliance konfigurieren, wird ein **Willkommensbildschirm** angezeigt.
6. Klicken Sie auf dem **Willkommensbildschirm** auf **Get Started**.



> **Hinweis**:
>
> Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der NetScaler-Appliance konfiguriert haben, wird der Willkommensbildschirm nicht angezeigt, sodass Sie nicht auf Get Started klicken.

1. Klicken Sie im Bereich **CloudBridge Connector Setup** auf **Amazon Web Services**



1. Geben Sie im **Amazon-Bereich** Ihre AWS-Kontoanmeldeinformationen ein: AWS Access Key ID und AWS Secret Access Key. Sie können diese Zugriffsschlüssel von der AWS-GUI-Konsole abrufen. Klicken Sie auf **Weiter**.

> **Hinweis**
>
> Bisher stellte der Setup-Assistent immer eine Verbindung zu derselben AWS-Region her, auch wenn eine andere Region ausgewählt wurde. Infolgedessen schlug die Konfiguration des CloudBridge Connector-Tunnels zu einem NetScaler VPX, der in der ausgewählten AWS-Region ausgeführt wurde, früher fehl. Dieses Problem wurde jetzt behoben.

1. Wählen Sie im **NetScaler-Bereich** die NSIP-Adresse der virtuellen NetScaler-Appliance aus, die auf AWS ausgeführt wird. Geben Sie dann Ihre Kontoanmeldeinformationen für die virtuelle NetScaler-Appliance ein. Klicken Sie auf **Weiter**.
2. Stellen Sie im Bereich **CloudBridge Connector-Einstellungen** den folgenden Parameter ein:
   - **CloudBridge Connector-Name**— Name für die CloudBridge Connector-Konfiguration auf der lokalen Appliance. Muss mit einem ASCII-Zeichen oder einem Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), gleich (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die CloudBridge Connector-Konfiguration erstellt wurde.
3. Stellen Sie unter **Lokale Einstellung**den folgenden Parameter ein:
   - **Subnetz-IP — IP-Adresse**des lokalen Endpunkts des CloudBridge Connector-Tunnels. Muss eine öffentliche IP-Adresse vom Typ SNIP sein.

4. Stellen Sie unter **Remote Setting**den folgenden Parameter ein:

    - **Subnetz-IP — IP-Adresse**des CloudBridge Connector-Tunnelendpunkts auf der AWS-Seite. Muss eine IP-Adresse vom Typ SNIP auf der NetScaler VPX-Instance auf AWS sein.
    - **NAT**— Öffentliche IP-Adresse (EIP) in AWS, die dem auf der NetScaler VPX-Instance in AWS konfigurierten SNIP zugeordnet ist.

5. Stellen Sie unter **PBR-Einstellung**die folgenden Parameter ein:

    - **Operation**— Entweder ist gleich (=) oder ist nicht gleich (! =) logischer Operator.
    - **Source IP Low — Niedrigste**Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden kann.
    - **Source IP High**— Die höchste Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden soll.
    - **Operation**— Entweder ist gleich (=) oder ist nicht gleich (! =) logischer Operator.
    - **Ziel-IP Low — Niedrigste**Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden kann.
    - **Ziel-IP High**— Die höchste Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets verglichen werden soll.

6. (Optional) Stellen Sie unter **Sicherheitseinstellungen**die folgenden IPSec-Protokollparameter für den CloudBridge Connector-Tunnel ein:

    - **Verschlüsselungsalgorithmus**— Verschlüsselungsalgorithmus, der vom IPSec-Protokoll im CloudBridge-Tunnel verwendet wird.
    - **Hash-Algorithmus**— Hash-Algorithmus, der vom IPSec-Protokoll im CloudBridge-Tunnel verwendet wird.
    - **Schlüssel**— Wählen Sie eine der folgenden IPSec-Authentifizierungsmethoden aus, die von den beiden Peers verwendet werden sollen, um sich gegenseitig zu authentifizieren.
        - **Automatisch generierter Schlüssel**— Die Authentifizierung basiert auf einer Textzeichenfolge, einem sogenannten Pre-Shared Key (PSK), der automatisch von der lokalen Appliance generiert wird. Die PSK-Schlüssel der Peers werden zur Authentifizierung miteinander abgeglichen.
        - **Spezifischer Schlüssel**— Authentifizierung auf der Grundlage einer manuell eingegebenen PSK. Die PSKs der Peers werden zur Authentifizierung miteinander verglichen.
            * **Pre Shared Security Key**— Die Textzeichenfolge, die für die auf Pre-Shared Keys basierende Authentifizierung eingegeben wurde.
        - **Zertifikate hochladen**— Authentifizierung auf der Grundlage digitaler Zertifikate.
            * **Öffentlicher Schlüssel**— Ein lokales digitales Zertifikat, das verwendet wird, um den lokalen Peer gegenüber dem Remote-Peer zu authentifizieren, bevor IPSec-

Sicherheitszuordnungen eingerichtet werden. Dasselbe Zertifikat sollte vorhanden und für den Peer Public Key-Parameter im Peer festgelegt sein.

* **Privater Schlüssel**— Privater Schlüssel des lokalen digitalen Zertifikats.
* **Peer Public Key**— Digitales Zertifikat des Peers. Wird verwendet, um den Peer zum lokalen Endpunkt zu authentifizieren, bevor IPSec-Sicherheitszuordnungen eingerichtet werden. Dasselbe Zertifikat sollte vorhanden und für den Public-Key-Parameter im Peer festgelegt sein.

7. Klicken Sie auf **Fertig**.

Die neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance im Rechenzentrum wird auf der Registerkarte Home der GUI angezeigt. Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler VPX-Appliance in der AWS-Cloud wird auf der GUI angezeigt. Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Configured CloudBridge angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Konfiguration eines CloudBridge Connector-Tunnels zwischen einer NetScaler-Appliance und einem Virtual Private Gateway auf AWS

May 11, 2023

Um ein Rechenzentrum mit Amazon Web Services (AWS) zu verbinden, können Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance im Rechenzentrum und einem Virtual Private Gateway auf AWS konfigurieren. Die NetScaler-Appliance und das Virtual Private Gateway bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

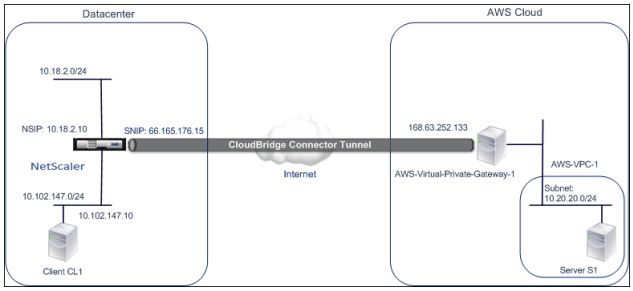
> **Hinweis:**
>
> Sie können auch einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance in einem Rechenzentrum und einer NetScaler VPX-Instanz (anstelle eines virtuellen privaten Gateway) in AWS einrichten. Weitere Informationen finden Sie unter Konfigurieren von CloudBridge Connector zwischen Datacenter und AWS Cloud.

Virtuelle private Gateways in AWS unterstützen die folgenden IPsec-Einstellungen für einen Cloud-Bridge Connector-Tunnel. Daher müssen Sie dieselben IPSec-Einstellungen angeben, wenn Sie die NetScaler-Appliance für den CloudBridge Connector-Tunnel konfigurieren.

IPsec-Eigenschaften	Einstellung
IPSec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE-Authentifizierungsmethode	Vorab gemeinsam genutzter Schlüssel
Verschlüsselungsalgorithmus	AES
Hash-Algorithmus	HMAC SHA1

Beispiel für CloudBridge Connector-Tunnelkonfiguration und Datenfluss

Betrachten Sie zur Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen der NetScaler-Appliance NS_Appliance-1 in einem Rechenzentrum und dem virtuellen privaten Gateway-Gateway AWS-Virtual-Private-Gateway-1 in der AWS-Cloud eingerichtet wird.



NS_Appliance-1 fungiert auch als L3-Router, der es einem privaten Netzwerk im Rechenzentrum ermöglicht, über den CloudBridge Connector-Tunnel ein privates Netzwerk in der AWS-Cloud zu erreichen. Als Router ermöglicht NS_Appliance-1 die Kommunikation zwischen Client CL1 im Rechenzentrum und Server S1 in der AWS-Cloud über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Auf NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration eine IPSec-Profilentität mit dem Namen NS_AWS_IPSec_Profile, eine CloudBridge Connector-Tunnelentität mit dem Namen NS_AWS_Tunnel und eine Policy-Based Routing (PBR) -Entität mit dem Namen NS_AWS_PBR.

Die IPSec-Profilentität NS_AWS_IPSec_Profile gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus und Hash-Algorithmus an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen. NS_AWS_IPSec_Profile ist an die IP-Tunnelentität NS_AWS_Tunnel gebunden.

Die CloudBridge Connector-Tunnelentität NS_AWS_Tunnel gibt die lokale IP-Adresse (eine öffentliche IP-Adresse, die auf der NetScaler-Appliance konfiguriert ist), die Remote-IP-Adresse (die IP-Adresse des AWS-Virtual-Private-Gateway-1) und das Protokoll (IPSec) an, das zur Einrichtung des Cloud-Bridge Connector-Tunnels verwendet wird. NS_AWS_Tunnel ist an die Policy-Based Routing (PBR) -Entität NS_AWS_PBR gebunden.

Die PBR-Entität NS_AWS_PBR spezifiziert eine Reihe von Bedingungen und eine CloudBridge Connector-Tunnelentität (NS_AWS_Tunnel). Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für NS_AWS_PBR. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich werden jeweils als Subnetz im Rechenzentrum und als Subnetz in der AWS-Cloud angegeben. Jedes Anforderungspaket, das von einem Client im Subnetz des Rechenzentrums stammt und an einen Server im Subnetz in der AWS-Cloud gerichtet ist, entspricht den Bedingungen in NS_AWS_PBR. Dieses Paket wird dann für die CloudBridge Connector-Verarbeitung berücksichtigt und über den CloudBridge Connector-Tunnel (NS_AWS_Tunnel) gesendet, der an die PBR-Entität gebunden ist.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

IP-Adresse des CloudBridge Connector-Tunnelendpunkts (NS_Appliance-1) auf der Rechenzentrumsseite	66.165.176.15
IP-Adresse des CloudBridge Connector-Tunnelendpunkts (AWS-Virtual-Private-Gateway-1) in AWS	168.63.252.133
Rechenzentrumssubnetz, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll	10.102.147.0/24
AWS-Subnetz, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll	10.20.20.0/24

Einstellungen auf Amazon AWS

		Routing = Statisch, IP-Adresse = IP-Adresse des über das Internet routbaren CloudBridge Connector-Tunnelendpunktes auf der NetScaler-Seite = 66.165.176.15
Kunden-Gateway	AWS-Customer-Gateway-1	
Virtuelles privates Gateway	AWS-Virtual-Private-Gateway-1	Zugehöriger VPC = AWS-VPC-1
VPN-Verbindung	AWS-VPN-Connection-1	Kunden-Gateway = AWS-Customer-Gateway-1, Virtual Private Gateway= Virtual-Private-Gateway-1, Routing-Optionen: Typ = Statisch, Statische IP-Präfixe = Subnetze auf der NetScaler-Seite = 10.102.147.0/24

Einstellungen auf der NetScaler-Appliance NS_Appliance-1in Datacenter-1:

Gerät	Einstellungen
–	–
SNIP1 (nur zu Referenzzwecken)	66.165.176.15
IPSec-Profil	NS_AWS_IPsec_Profile	IKE-Version = v1, Verschlüsselungsalgorithmus = AES, Hash-Algorithmus = HMAC SHA1
CloudBridge Connector Tunnel|NS_AWS_Tunnel|Remote-IP = 168.63.252.133, Lokale IP= 66.165.176.15, Tunnelprotokoll = IPSec, IPSec-Profil= NS_AWS_IPsec_Profile| |Richtlinienbasierte Route|NS_AWS_PBR|Quell-IP-Bereich = Subnetz im Rechenzentrum =10.102.147.0-10.102.147.255, Ziel-IP-Bereich =Subnetz in AWS =10.20.20.0-10.20.20.255, IP-Tunnel = NS_AWS_Tunnel

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einem AWS-Gateway konfigurieren, sollten Sie die folgenden Punkte berücksichtigen:

1. AWS unterstützt die folgenden IPSec-Einstellungen für einen CloudBridge Connector-Tunnel. Daher müssen Sie dieselben IPSec-Einstellungen angeben, wenn Sie die NetScaler-Appliance für den CloudBridge Connector-Tunnel konfigurieren.

- IKE-Version = v1
- Verschlüsselungsalgorithmus = AES
- Hash-Algorithmus = HMAC SHA1

2. Sie müssen die Firewall am NetScaler-Ende so konfigurieren, dass sie Folgendes zulässt.
   - Alle UDP-Pakete für Port 500
   - Alle UDP-Pakete für Port 4500
   - Alle ESP-Pakete (IP-Protokollnummer 50)
3. Sie müssen Amazon AWS konfigurieren, bevor Sie die Tunnelkonfiguration auf dem NetScaler angeben, da die öffentliche IP-Adresse des AWS-Endes (Gateway) des Tunnels und der PSK automatisch generiert werden, wenn Sie die Tunnelkonfiguration in AWS einrichten. Sie benötigen diese Informationen, um die Tunnelkonfiguration auf der NetScaler-Appliance zu spezifizieren.
4. Das AWS-Gateway unterstützt statische Routen und das BGP-Protokoll für Routenaktualisierungen. Die NetScaler-Appliance unterstützt das BGP-Protokoll in einem CloudBridge Connector-Tunnel zum AWS-Gateway nicht. Daher müssen auf beiden Seiten des CloudBridge Connector-Tunnels geeignete statische Routen verwendet werden, um den Verkehr ordnungsgemäß durch den Tunnel zu leiten.

Konfiguration von Amazon AWS für den CloudBridge Connector-Tunnel

Um eine CloudBridge Connector-Tunnelkonfiguration auf Amazon AWS zu erstellen, verwenden Sie die Amazon AWS Management Console, eine webbasierte grafische Oberfläche für die Erstellung und Verwaltung von Ressourcen auf Amazon AWS.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration in der AWS-Cloud beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto für die Amazon AWS-Cloud.
- Sie haben eine virtuelle private Cloud, deren Netzwerke Sie über den CloudBridge Connector-Tunnel mit den Netzwerken auf der NetScaler-Seite verbinden möchten.
- Sie sind mit der Amazon AWS Management Console vertraut.

> **Hinweis**:
>
> Die Verfahren zur Konfiguration von Amazon AWS für einen CloudBridge Connector-Tunnel können sich je nach Amazon AWS-Veröffentlichungszyklus im Laufe der Zeit ändern. Citrix empfiehlt, dass Sie die Amazon AWS-Dokumentation für die neuesten Verfahren nachlesen.

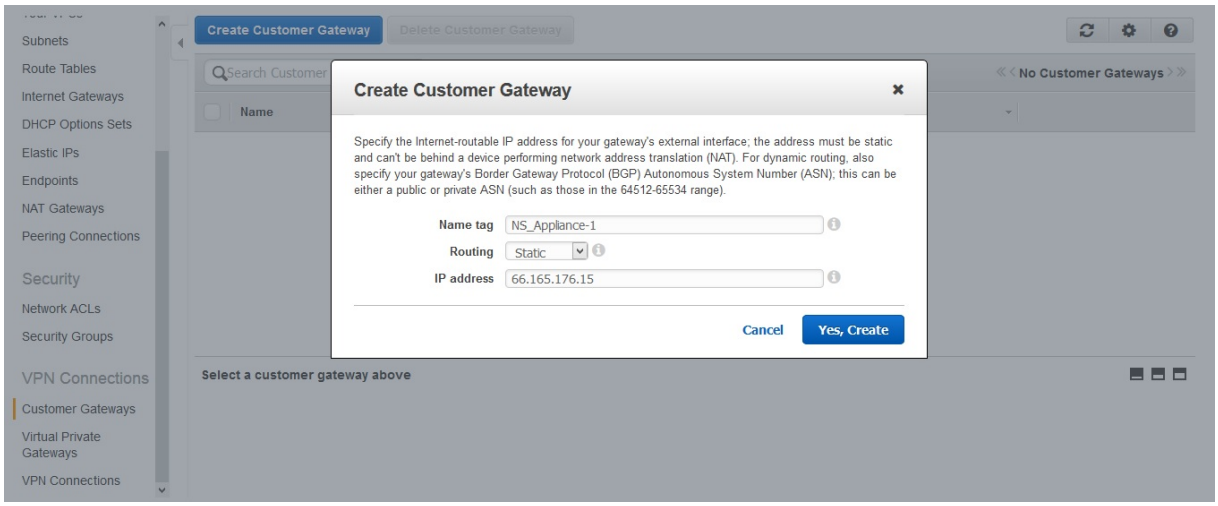
So konfigurieren Sie einen CloudBridge-Connector-Tunnel zwischen einem NetScaler und AWS-Gateway, führen Sie die folgenden Aufgaben in der AWS Management Console aus:

- **Erstellen Sie ein Kunden-Gateway**. Ein Kunden-Gateway ist eine AWS-Entität, die einen CloudBridge Connector-Tunnelendpunkt darstellt. Bei einem CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einem AWS-Gateway stellt das Kunden-Gateway die NetScaler-Appliance in AWS dar. Das Kunden-Gateway gibt einen Namen, die Art des im Tunnel verwendeten Routings (statisch oder BGP) und die IP-Adresse des CloudBridge Connector-Tunnelendpunkts auf der NetScaler-Seite an. Bei der IP-Adresse kann es sich um eine über das Internet routbare, NetScaler-eigene Subnetz-IP-Adresse (SNIP) handeln oder, wenn sich die NetScaler-Appliance hinter einem NAT-Gerät befindet, um eine über das Internet routbare NAT-IP-Adresse, die die SNIP-Adresse darstellt.
- **Erstellen Sie ein Virtual Private Gateway und hängen Sie es an eine VPC**an. Ein virtuelles privates Gateway ist ein CloudBridge Connector-Tunnelendpunkt auf der AWS-Seite. Wenn Sie ein virtuelles privates Gateway erstellen, haben Sie ihm einen Namen zugewiesen oder AWS erlaubt, den Namen zuzuweisen. Anschließend verknüpfen Sie das Virtual Private Gateway mit einer VPC. Diese Zuordnung ermöglicht es den Subnetzen der VPC, über den CloudBridge Connector-Tunnel eine Verbindung zu den Subnetzen auf der NetScaler-Seite herzustellen.
- **Erstellen Sie eine VPN-Verbindung**. Eine VPN-Verbindung spezifiziert ein Kunden-Gateway und ein virtuelles privates Gateway, zwischen denen ein CloudBridge Connector-Tunnel erstellt werden soll. Es gibt auch ein IP-Präfix für die Netzwerke auf der NetScaler-Seite an. Nur IP-Präfixe, die dem Virtual Private Gateway (durch einen statischen Routeneintrag) bekannt sind, können Datenverkehr von der VPC durch den Tunnel empfangen. Außerdem leitet das Virtual Private Gateway keinen Datenverkehr, der nicht an die angegebenen IP-Präfixe gerichtet ist, durch den Tunnel. Nachdem Sie eine VPN-Verbindung konfiguriert haben, müssen Sie möglicherweise einige Minuten warten, bis sie erstellt wird.
- **Konfigurieren Sie die Routing-Optionen**. Damit das Netzwerk der VPC die Netzwerke auf der NetScaler-Seite über den CloudBridge Connector-Tunnel erreicht, müssen Sie die Routingtabelle der VPC so konfigurieren, dass sie Routen für die Netzwerke auf der NetScaler-Seite enthält, und diese Routen an das Virtual Private Gateway weiterleiten. Sie können Routen auf eine der folgenden Arten in die Routingtabelle einer VPC aufnehmen:
  - **Aktivieren Sie die Route-Propagation.** Sie können die Routenpropagierung für Ihre Routing-Tabelle aktivieren, sodass Routen automatisch an die Tabelle weitergegeben werden. Die statischen IP-Präfixe, die Sie für die VPN-Konfiguration angeben, werden an die Routingtabelle weitergegeben, nachdem Sie die VPN-Verbindung erstellt haben.
  - **Geben Sie statische Routen manuell**ein. Wenn Sie die Routenpropagation nicht aktivieren, müssen Sie die statischen Routen für die Netzwerke auf der NetScaler-Seite manuell eingeben.
- **Konfiguration herunterladen**. Nachdem die Konfiguration des CloudBridge Connector-Tunnels (VPN-Verbindung) auf AWS erstellt wurde, laden Sie die Konfigurationsdatei der VPN-Verbindung auf Ihr lokales System herunter. Möglicherweise benötigen Sie die Informationen in der Konfigurationsdatei, um den CloudBridge Connector-Tunnel auf der

NetScaler-Appliance zu konfigurieren.

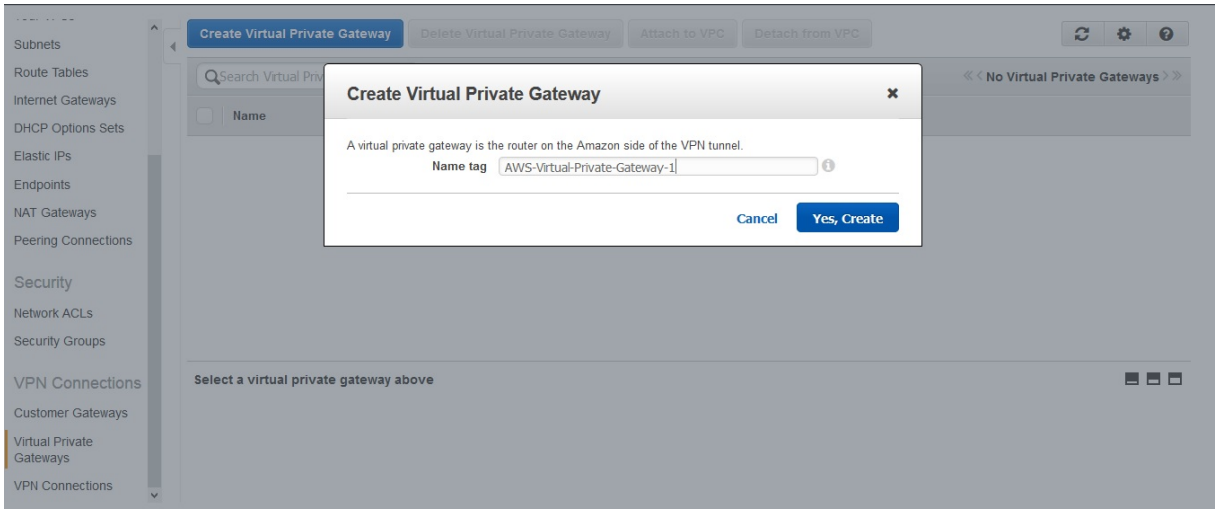
Um ein Kunden-Gateway zu erstellen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Navigieren Sie zu **VPN-Verbindungen** > **Kunden-Gateways** und klicken Sie auf **Kunden-Gateways erstellen**.
3. Stellen **Sie im Dialogfeld „Kunden-Gateway erstellen** “ die folgenden Parameter ein und klicken Sie dann auf **Ja, Erstellen**:
   - **Namensschild**. Ein Name für das Kunden-Gateway.
   - **Routing-Liste**. Art des Routings zwischen NetScaler-Appliance und AWS Virtual Private Gateway für Werberouten untereinander über den CloudBridge Connector-Tunnel. Wählen Sie **Statisches Routing** aus der **Routing-Liste** aus. **Hinweis**: Die NetScaler-Appliance unterstützt das BGP-Protokoll in einem CloudBridge Connector-Tunnel zum AWS-Gateway nicht. Daher müssen auf beiden Seiten des CloudBridge Connector-Tunnels geeignete statische Routen verwendet werden, um den Verkehr ordnungsgemäß durch den Tunnel zu leiten.
   - **IP-Adresse**. Über das Internet routingbare CloudBridge Connector-Tunnel-IP-Adresse auf der NetScaler-Seite. Bei der IP-Adresse kann es sich um eine über das Internet routbare, NetScaler-eigene Subnetz-IP-Adresse (SNIP) handeln oder, wenn sich die NetScaler-Appliance hinter einem NAT-Gerät befindet, um eine über das Internet routbare NAT-IP-Adresse, die die SNIP-Adresse darstellt.

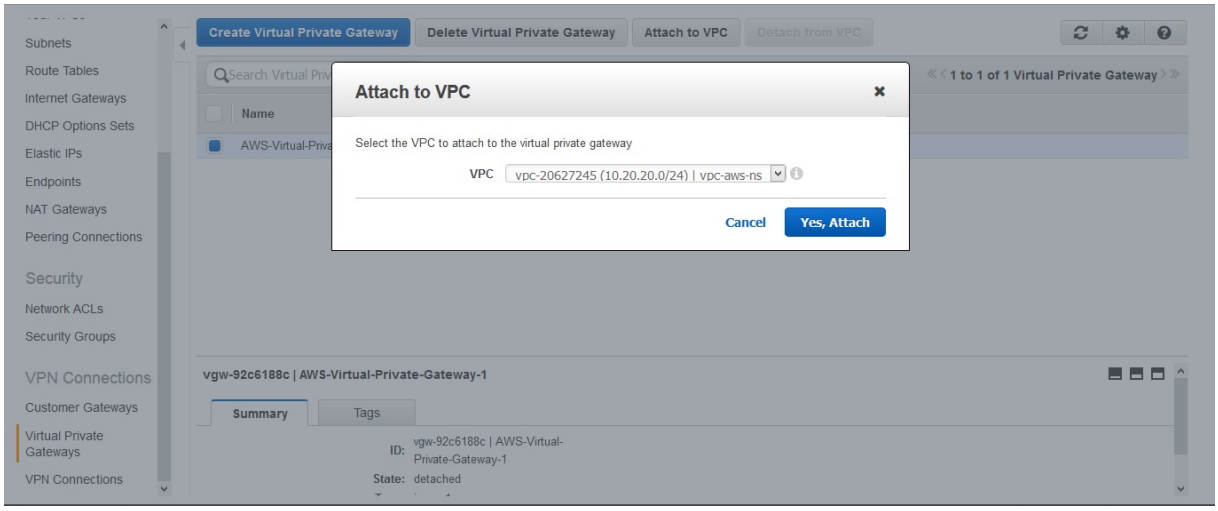


Um ein virtuelles privates Gateway zu erstellen und es an eine VPC anzuhängen

1. Navigieren Sie zu **VPN-Verbindungen** > **Virtual Private Gateways**und klicken Sie dann auf Create Virtual Private Gateway.
2. Geben Sie einen Namen für das Virtual Private Gateway ein und klicken Sie dann auf Ja, Erstellen.



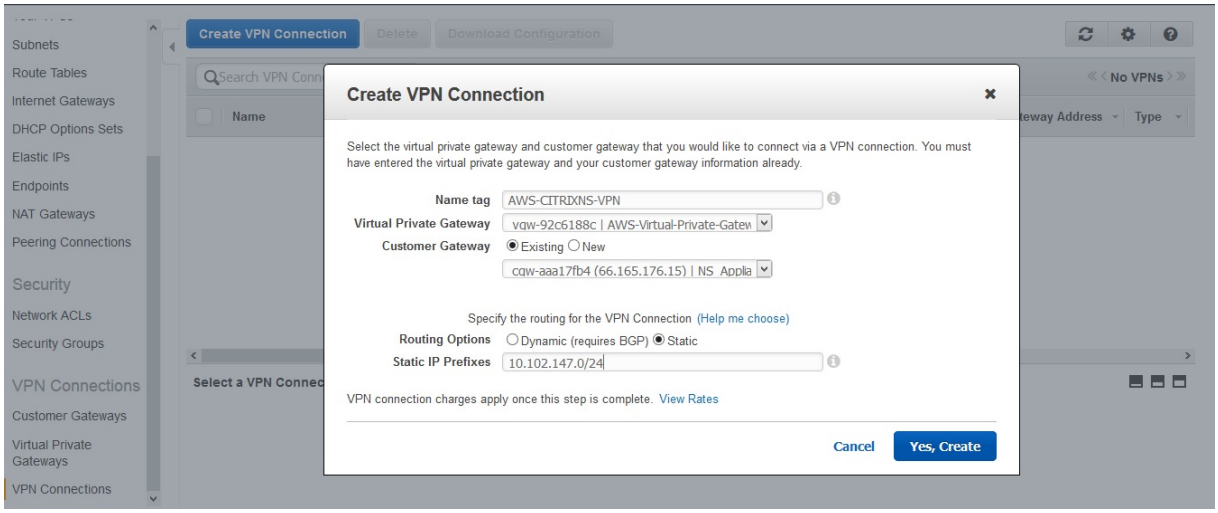
1. Wählen Sie das virtuelle private Gateway aus, das Sie erstellt haben, und klicken Sie dann auf An VPC anhängen.
2. Wählen Sie im Dialogfeld An VPC anhängen Ihre VPC aus der Liste aus und wählen Sie dann Ja, Anhängen.



So erstellen Sie eine VPN-Verbindung:

1. Navigieren Sie zu VPN-Verbindungen > VPN-Verbindungen und klicken Sie dann auf VPN-Verbindung erstellen.
2. Stellen Sie im Dialogfeld „VPN-Verbindung erstellen“ die folgenden Parameter ein und wählen Sie dann Ja, Erstellen aus:
   - **Namensschild**. Ein Name für die VPN-Verbindung.
   - **Virtuelles privates Gateway**. Wählen Sie das Virtual Private Gateway aus, das Sie zuvor erstellt haben.
   - **Kunden-Gateway**. Wählen Sie Bestehend aus. Wählen Sie dann aus der Dropdown-Liste das Kunden-Gateway aus, das Sie zuvor erstellt haben.

- **Routing-Optionen**. Art des Routings zwischen dem Virtual Private Gateway und dem Kunden-Gateway (NetScaler-Appliance). Wählen Sie Statisch aus. Geben Sie im Feld Statische IP-Präfixe die IP-Präfixe für das Subnetz auf der NetScaler-Seite an, getrennt durch Kommas.



Um die Routenpropagierung zu aktivieren:

1. Navigieren Sie zu **Route Tables** und wählen Sie die Routingtabelle aus, die dem Subnetz zugeordnet ist, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll.

> **Hinweis**
>
> Standardmäßig ist dies die Haupt-Routing-Tabelle für die VPC.

1. Wählen Sie im Detailbereich auf der Registerkarte **Route Propagation** die Option **Bearbeiten**, wählen Sie das Virtual Private Gateway aus und klicken Sie dann auf **Speichern**.

Um statische Routen manuell einzugeben:

1. Navigieren Sie zu **Routing-Tabellen** und wählen Sie Ihre Routing-Tabelle aus.
2. Klicken Sie auf der Registerkarte **Routen** auf **Bearbeiten**.
3. Geben Sie im Feld **Ziel** die statische Route ein, die von Ihrem CloudBridge Connector-Tunnel (VPN-Verbindung) verwendet wird.
4. Wählen Sie die Virtual Private Gateway-ID aus der **Zielliste** aus, und klicken Sie dann auf **Speichern**.

Um die Konfigurationsdatei herunterzuladen:

1. Navigieren Sie zu **VPN-Verbindung**, wählen Sie eine VPN-Verbindung aus und klicken Sie dann auf **Konfiguration herunterladen**.
2. Stellen **Sie im Dialogfeld „Download-Konfiguration** “ die folgenden Parameter ein und klicken Sie dann auf **Ja, Herunterladen**.
   - **Verkäufer**. Wählen Sie **Generisch**aus.

- **Plattform**. Wählen Sie **Generisch**aus.
- **Software**. Wählen Sie **Vendor Agnostic**aus.

Konfigurieren der NetScaler Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einem Virtual Private Gateway in der AWS-Cloud zu konfigurieren, führen Sie die folgenden Aufgaben auf der NetScaler-Appliance aus.
Sie können entweder die NetScaler-Befehlszeile oder die GUI verwenden.

- **Erstellen Sie ein IPSec-Profil.** Eine IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel, der das IPSec-Protokoll verwendet, und verknüpfen Sie das IPSec-Profil damit**. Ein IP-Tunnel gibt die lokale IP-Adresse (eine auf der NetScaler-Appliance konfigurierte SNIP-Adresse), die Remote-IP-Adresse (die öffentliche IP-Adresse des Virtual Private Gateway in AWS), das Protokoll (IPSec), das zur Einrichtung des CloudBridge Connector-Tunnels verwendet wird, und eine IPSec-Profilentität an. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität spezifiziert eine Reihe von Regeln und eine IP-Tunnelentität (CloudBridge Connector-Tunnel). Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das NetScaler-seitige Subnetz anzugeben, dessen Datenverkehr den Tunnel durchqueren soll, und legen Sie den IP-Zieladressbereich fest, um das AWS VPC-Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Jedes Anforderungspaket, das von einem Client im Subnetz auf der NetScaler-Seite stammt und für einen Server im AWS-Cloud-Subnetz bestimmt ist und dem Quell- und Ziel-IP-Bereich der PBR-Entität entspricht, wird über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

So erstellen Sie ein IPSEC-Profil über die NetScaler Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> -psk <string> -**ikeVersion** v1`
- `show ipsec profile** <name>`

Um einen IPSEC-Tunnel zu erstellen und das IPSEC-Profil mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`

- show ipTunnel <name>

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP** <subnet-range> -*ipTunnel <tunnelName>
- apply pbrs
- show pbr <pbrName>

Mit den folgenden Befehlen werden alle Einstellungen der NetScaler-Appliance NS_Appliance-1 erstellt, die in „Beispiel für CloudBridge Connector-Konfiguration und Datenfluss“ verwendet werden.

”

```
1      > add ipsec profile NS_AWS_IPSec_Profile -psk
           DkiMgMdcbqvYREEuIvxsbKkW0Foyabcd -ikeVersion v1  - lifetime
           31536000
2      Done
3      > add iptunnel NS_AWS_Tunnel 168.63.252.133 255.255.255.255
           66.165.176.15  - protocol IPSEC  - ipsecProfileName
           NS_AWS_IPSec_Profile
4
5      Done
6      > add pbr NS_AWS_Pbr -srcIP 10.102.147.0-10.102.147.255  - destIP
           10.20.0.0-10.20.255.255  - ipTunnel NS_AWS_Tunnel
7      Done
8
9      > apply pbrs
10
11     Done
12 <!--NeedCopy-->
```

So erstellen Sie ein IPSEC-Profil mithilfe der GUI

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen **Sie im Dialogfeld IPSec-Profil hinzufügen** die folgenden Parameter ein:
    - Name
    - Verschlüsselungsalgorithmus
    - Hash-Algorithmus
    - IKE-Protokollversion (wählen Sie V1)

4. Wählen Sie die Methode **Pre-Shared Key Authentication** und legen Sie den Parameter **Pre-Shared Key Exists** fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um einen IP-Tunnel zu erstellen und das IPSEC-Profil mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf Hinzufügen.
3. Stellen **Sie im Dialogfeld IP-Tunnel hinzufügen** die folgenden Parameter ein:
    - Name
    - Remote-IP
    - Maske aus der Ferne
    - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option Subnetz-IP aus).
    - Lokale IP (Alle konfigurierten IPs des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
    - Protokoll
    - IPSec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Stellen **Sie im Dialogfeld PBR erstellen** die folgenden Parameter ein:
    - Name
    - Aktion
    - Nächster Hop-Typ (IP-Tunnelauswählen)
    - Name des IP-Tunnels
    - Quell-IP Low
    - Quell-IP High
    - Ziel-IP Niedrig
    - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance wird in der GUI angezeigt.

Der aktuelle Status des CloudBridge Connector-Tunnels wird im Bereich Configured CloudBridge Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen.
Weitere Informationen zur Anzeige von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler-Appliance finden Sie unter Überwachung von CloudBridgeConnector-Tunneln.

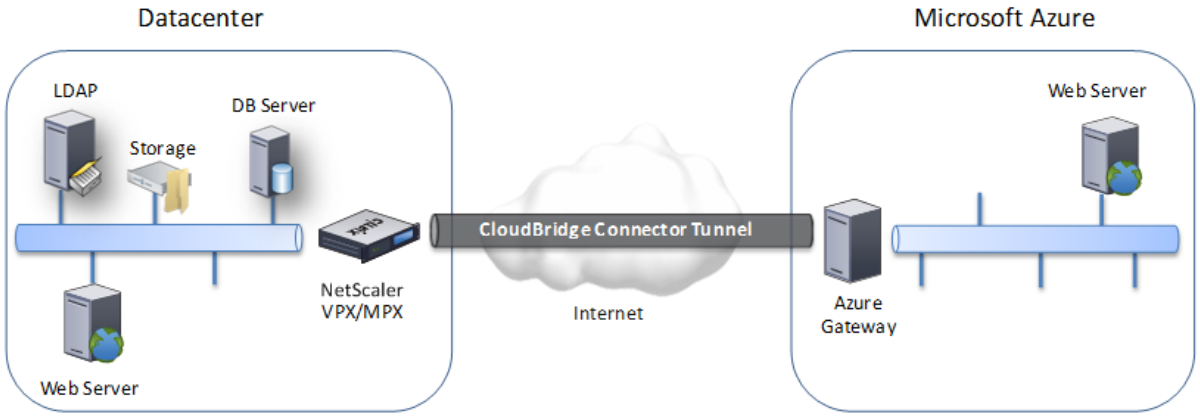
Konfiguration eines CloudBridge Connector-Tunnels zwischen einem Rechenzentrum und der Azure-Cloud

May 11, 2023

Die NetScaler-Appliance bietet Konnektivität zwischen Ihren Unternehmensrechenzentren und dem Microsoft-Cloud-Hosting-Anbieter Azure und macht Azure zu einer nahtlosen Erweiterung des Unternehmensnetzwerks. NetScaler verschlüsselt die Verbindung zwischen dem Unternehmensrechenzentrum und der Azure-Cloud, sodass alle zwischen den beiden übertragenen Daten sicher sind.

So funktioniert der CloudBridge Connector-Tunnel

Um ein Rechenzentrum mit der Azure-Cloud zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance, die sich im Rechenzentrum befindet, und einem Gateway in der Azure-Cloud ein. Die NetScaler-Appliance im Rechenzentrum und das Gateway in der Azure-Cloud sind die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers des CloudBridge Connector-Tunnels bezeichnet.



Ein CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und der Azure-Cloud verwendet im Tunnelmodus die auf offenen Standards basierende Internet Protocol Security (IPSec) -Protokollsuite, um die Kommunikation zwischen Peers im CloudBridge Connector-Tunnel zu sichern. In einem CloudBridge Connector-Tunnel stellt IPSec Folgendes sicher:

- Integrität der Daten
- Authentifizierung des Datenursprungs
- Vertraulichkeit der Daten (Verschlüsselung)
- Schutz vor Replay-Angriffen

IPSec verwendet den Tunnelmodus, in dem das komplette IP-Paket verschlüsselt und dann gekapselt wird. Die Verschlüsselung verwendet das ESP-Protokoll (Encapsulating Security Payload), das die Integrität des Pakets mithilfe einer HMAC-Hashfunktion sicherstellt und die Vertraulichkeit mithilfe eines Verschlüsselungsalgorithmus gewährleistet. Das ESP-Protokoll generiert nach der Verschlüsselung der Payload und der Berechnung des HMAC einen ESP-Header und fügt ihn vor das verschlüsselte IP-Paket ein. Das ESP-Protokoll generiert auch einen ESP-Trailer und fügt ihn am Ende des Pakets ein.

Das IPSec-Protokoll kapselt dann das resultierende Paket, indem es vor dem ESP-Header einen IP-Header hinzufügt. Im IP-Header wird die Ziel-IP-Adresse auf die IP-Adresse des CloudBridge Connecter-Peers gesetzt.

Peers im CloudBridge Connector-Tunnel verwenden das Internet Key Exchange Version 1 (IKEv1) -Protokoll (Teil der IPSec-Protokollsuite), um eine sichere Kommunikation wie folgt auszuhandeln:

1. Die beiden Peers authentifizieren sich gegenseitig mithilfe der Pre-Shared-Key-Authentifizierung, bei der die Peers eine Textzeichenfolge austauschen, die als Pre-Shared Key (PSK) bezeichnet wird. Die Pre-Shared-Schlüssel werden zur Authentifizierung miteinander abgeglichen. Damit die Authentifizierung erfolgreich ist, müssen Sie daher auf jedem Peer denselben Pre-Shared-Schlüssel konfigurieren.
2. Die Fachkollegen verhandeln dann, um eine Einigung über Folgendes zu erzielen:
   - Ein Verschlüsselungsalgorithmus
   - Kryptografische Schlüssel zum Verschlüsseln von Daten auf einem Peer und zum Entschlüsseln von Daten auf dem anderen.

   Diese Vereinbarung über das Sicherheitsprotokoll, den Verschlüsselungsalgorithmus und die kryptografischen Schlüssel wird als Security Association (SA) bezeichnet. SAs sind Einwegsysteme (Simplex). Wenn beispielsweise ein CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance in einem Rechenzentrum und einem Gateway in einer Azure-Cloud eingerichtet wird, verfügen sowohl die Rechenzentrums-Appliance als auch das Azure-Gateway über zwei SAs. Ein SA wird für die Verarbeitung ausgehender Pakete verwendet, und der andere SA wird für die Verarbeitung eingehender Pakete verwendet. SAs laufen nach einem bestimmten Zeitintervall ab, das als Lebensdauer bezeichnet wird.

Beispiel für CloudBridge Connector-Tunnelkonfiguration und Datenfluss

Betrachten Sie zur Veranschaulichung des CloudBridge Connector Tunnels ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen der NetScaler-Appliance CB_Appliance-1 in einem Rechenzentrum und dem Gateway Azure_Gateway-1 in der Azure-Cloud eingerichtet wird.

CB_Appliance-1 fungiert auch als L3-Router, der es einem privaten Netzwerk im Rechenzentrum ermöglicht, über den CloudBridge Connector-Tunnel ein privates Netzwerk in der Azure-Cloud zu erreichen. Als Router ermöglicht CB_Appliance-1 die Kommunikation zwischen dem Client CL1 im Rechenzentrum und dem Server S1 in der Azure-Cloud über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Auf CB_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration eine IPSec-Profilentität mit dem Namen CB_Azure_IPSec_Profile, eine CloudBridge Connector-Tunnelentität mit dem Namen CB_Azure_Tunnel und eine Policy Based Routing (PBR) -Entität mit dem Namen CB_Azure_PBR.

Die IPSec-Profilentität CB_Azure_IPSec_Profile gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus und Hash-Algorithmus an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen. cb_Azure_IPSec_Profile ist an die IP-Tunnelentität CB_Azure_Tunnel gebunden.

Die CloudBridge Connector-Tunnelentität CB_Azure_Tunnel gibt die lokale IP-Adresse (eine öffentliche IP-Adresse (SNIP) an, die auf der NetScaler-Appliance konfiguriert ist), die Remote-IP-Adresse (die IP-Adresse des Azure_Gateway-1) und das Protokoll (IPSec), das zur Einrichtung des CloudBridge Connector-Tunnels verwendet wird. CB_Azure_Tunnel ist an die PBR-Entität CB_Azure_PBR gebunden.

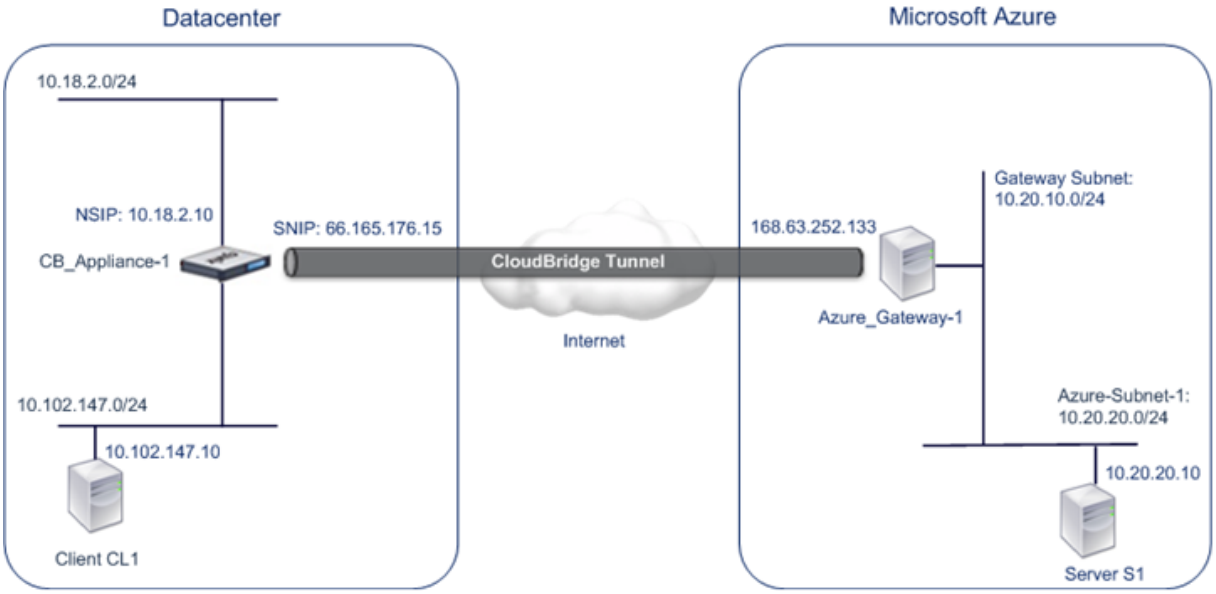
Die PBR-Entität CB_Azure_PBR spezifiziert eine Reihe von Bedingungen und eine CloudBridge Connector-Tunnelentität (CB_Azure_Tunnel). Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für cb_Azure_PBR. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich werden jeweils als Subnetz im Rechenzentrum und als Subnetz in der Azure-Cloud angegeben. Jedes Anforderungspaket, das von einem Client im Subnetz des Rechenzentrums stammt und an einen Server im Subnetz in der Azure-Cloud gerichtet ist, entspricht den Bedingungen in cb_Azure_PBR. Dieses Paket wird dann für die CloudBridge-Verarbeitung berücksichtigt und über den CloudBridge Connector-Tunnel (CB_Azure_Tunnel) gesendet, der an die PBR-Entität gebunden ist.

In Microsoft Azure umfasst die CloudBridge Connector-Tunnelkonfiguration eine lokale Netzwerkentität namens My-Datacenter-Network, eine virtuelle Netzwerkentität mit dem Namen Azure-Network-for-CloudBridge-Tunnel und ein Gateway mit dem Namen Azure_Gateway-1.

Die lokale (lokale Netzwerkeinheit für Azure) My-Datacenter-Network gibt die IP-Adresse der NetScaler-Appliance auf der Rechenzentrumsseite und das Rechenzentrumssubnetz an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Die virtuelle Netzwerkentität Azure-Network-for-CloudBridge-Tunnel definiert ein privates Subnetz namens Azure-Subnet-1 in

Azure. Der Verkehr des Subnetzes durchquert den CloudBridge Connector-Tunnel. Der Server S1 wird in diesem Subnetz bereitgestellt.

Die lokale Netzwerkentität My-Datacenter-Network ist der virtuellen Netzwerkentität Azure-Network-for-CloudBridge-Tunnel zugeordnet. Diese Zuordnung definiert die Details des Remote-Netzwerks und des lokalen Netzwerks der CloudBridge Connector-Tunnelkonfiguration in Azure. Gateway Azure_Gateway-1 wurde für diese Zuordnung erstellt, um zum CloudBridge-Endpunkt am Azure-Ende des CloudBridge Connector-Tunnels zu werden.



Weitere Informationen zu den Einstellungen finden Sie im PDF-Dokument CloudBridge Connector Tunnel Settings .

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance im Rechenzentrum und Microsoft Azure konfigurieren, sollten Sie die folgenden Punkte berücksichtigen:

1. Die NetScaler-Appliance muss über eine öffentlich zugängliche IPv4-Adresse (Typ SNIP) verfügen, um sie als Tunnelendpunktadresse für den CloudBridge Connector-Tunnel verwenden zu können. Außerdem sollte sich die NetScaler-Appliance nicht hinter einem NAT-Gerät befinden.
2. Azure unterstützt die folgenden IPSec-Einstellungen für einen CloudBridge Connector-Tunnel. Daher müssen Sie bei der Konfiguration des NetScaler für den CloudBridge Connector-Tunnel dieselben IPSec-Einstellungen angeben.
   - IKE-Version = v1
   - Verschlüsselungsalgorithmus = AES
   - Hash-Algorithmus = HMAC SHA1
3. Sie müssen die Firewall im Rechenzentrums-Edge so konfigurieren, dass sie Folgendes zulässt.

- Alle UDP-Pakete für Port 500
- Alle UDP-Pakete für Port 4500
- Alle ESP-Pakete (IP-Protokollnummer 50)

4. IKE-Re-Keying, bei dem neue kryptografische Schlüssel zwischen den CloudBridge Connector-Tunnelendpunkten neu ausgehandelt werden, um neue SAs einzurichten, wird nicht unterstützt. Wenn die Security Associations (SAs) ablaufen, wechselt der Tunnel in den Status DOWN. Daher müssen Sie einen sehr hohen Wert für die Lebensdauer von SAs festlegen.
5. Sie müssen Microsoft Azure konfigurieren, bevor Sie die Tunnelkonfiguration auf dem NetScaler angeben, da die öffentliche IP-Adresse des Azure-Endes (Gateway) des Tunnels und der PSK automatisch generiert werden, wenn Sie die Tunnelkonfiguration in Azure einrichten. Sie benötigen diese Informationen, um die Tunnelkonfiguration auf dem NetScaler zu spezifizieren.

Konfiguration des CloudBridge Connector-Tunnels

Um einen CloudBridge Connector-Tunnel zwischen Ihrem Rechenzentrum und Azure einzurichten, müssen Sie CloudBridge VPX/MPX in Ihrem Rechenzentrum installieren, Microsoft Azure für den CloudBridge Connector-Tunnel konfigurieren und dann die NetScaler-Appliance im Rechenzentrum für den CloudBridge Connector-Tunnel konfigurieren.

Die Konfiguration eines CloudBridge Connector-Tunnels zwischen einer NetScaler-Appliance im Rechenzentrum und Microsoft Azure umfasst die folgenden Aufgaben:

1. **Einrichtung der NetScaler-Appliance im Rechenzentrum**. Diese Aufgabe umfasst die Bereitstellung und Konfiguration einer physischen NetScaler-Appliance (MPX) oder die Bereitstellung und Konfiguration einer virtuellen NetScaler-Appliance (VPX) auf einer Virtualisierungsplattform im Rechenzentrum.
2. **Konfiguration von Microsoft Azure für den CloudBridge Connector-Tunnel**. Diese Aufgabe umfasst die Erstellung von lokalen Netzwerk-, virtuellen Netzwerk- und Gateway-Entitäten in Azure. Die lokale Netzwerkentität gibt die IP-Adresse des CloudBridge Connector-Tunnelendpunkts (der NetScaler-Appliance) auf der Rechenzentrumsseite und das Rechenzentrumssubnetz an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Das virtuelle Netzwerk definiert ein Netzwerk in Azure. Zum Erstellen des virtuellen Netzwerks gehört die Definition eines Subnetzes, dessen Datenverkehr den zu bildenden CloudBridge Connector-Tunnel durchqueren soll. Anschließend verknüpfen Sie das lokale Netzwerk mit dem virtuellen Netzwerk. Schließlich erstellen Sie ein Gateway, das zum Endpunkt am Azure-Ende des CloudBridge Connector-Tunnels wird.
3. **Konfiguration der NetScaler-Appliance im Rechenzentrum für den CloudBridge Connector-Tunnel**. Diese Aufgabe umfasst das Erstellen eines IPSec-Profils, einer IP-Tunnelentität und einer PBR-Entität in der NetScaler-Appliance im Rechenzentrum. Die IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK an, die im CloudBridge Connector-Tunnel verwendet werden

sollen. Der IP-Tunnel gibt die IP-Adresse der beiden CloudBridge Connector-Tunnelendpunkte (der NetScaler-Appliance im Rechenzentrum und des Gateway in Azure) als auch das Protokoll an, das im CloudBridge Connector-Tunnel verwendet werden soll. Anschließend verknüpfen Sie die IPSec-Profilentität mit der IP-Tunnelentität. Die PBR-Entität spezifiziert die beiden Subnetze im Rechenzentrum und in der Azure-Cloud, die über den CloudBridge Connector-Tunnel miteinander kommunizieren sollen. Anschließend verknüpfen Sie die IP-Tunnelentität mit der PBR-Entität.

Konfiguration von Microsoft Azure für den CloudBridge Connector-Tunnel

Um eine CloudBridge Connector-Tunnelkonfiguration auf Microsoft Azure zu erstellen, verwenden Sie das Microsoft Windows Azure Management Portal, eine webbasierte grafische Oberfläche für die Erstellung und Verwaltung von Ressourcen in Microsoft Azure.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration in der Azure-Cloud beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto für Microsoft Azure.
- Sie haben ein konzeptionelles Verständnis von Microsoft Azure.
- Sie sind mit dem Microsoft Windows Azure Management Portal vertraut.

Um einen CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und einer Azure-Cloud zu konfigurieren, führen Sie die folgenden Aufgaben in Microsoft Azure mithilfe des Microsoft Windows Azure-Verwaltungsportals aus:

- **Erstellen Sie eine lokale Netzwerkentität**. Erstellen Sie eine lokale Netzwerkentität in Windows Azure, um die Netzwerkdetails des Rechenzentrums anzugeben. Eine lokale Netzwerkentität gibt die IP-Adresse des CloudBridge Connector-Tunnelendpunkts (NetScaler) auf der Rechenzentrumsseite und das Rechenzentrumssubnetz an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll.
- **Erstellen Sie ein virtuelles Netzwerk**. Erstellen Sie eine virtuelle Netzwerkentität, die ein Netzwerk in Azure definiert. Diese Aufgabe beinhaltet die Definition eines privaten Adressraums, in dem Sie einen Bereich von privaten Adressen und Subnetzen angeben, die zu dem im Adressraum angegebenen Bereich gehören. Der Verkehr der Subnetze durchquert den CloudBridge Connector-Tunnel. Anschließend ordnen Sie der virtuellen Netzwerkentität eine lokale Netzwerkentität zu. Diese Zuordnung ermöglicht es Azure, eine Konfiguration für einen CloudBridge Connector-Tunnel zwischen dem virtuellen Netzwerk und dem Rechenzentrumsnetzwerk zu erstellen. Ein (zu erstellendes) Gateway in Azure für dieses virtuelle Netzwerk wird der CloudBridge-Endpunkt am Azure-Ende des CloudBridge Connector-Tunnels sein. Anschließend definieren Sie ein privates Subnetz für das zu erstellende Gateway. Dieses Subnetz gehört zu dem Bereich, der im Adressraum der virtuellen Netzwerkentität angegeben ist.

- **Erstellen Sie ein Gateway in Windows Azure**. Erstellen Sie ein Gateway, das zum Endpunkt am Azure-Ende des CloudBridge Connector-Tunnels wird. Azure weist dem erstellten Gateway aus seinem Pool an öffentlichen IP-Adressen eine IP-Adresse zu.
- **Erfassen Sie die öffentliche IP-Adresse des Gateway und den Pre-Shared-Schlüssel.** Bei einer CloudBridge Connector-Tunnelkonfiguration in Azure werden die öffentliche IP-Adresse des Gateway und der Pre-Shared Key (PSK) automatisch von Azure generiert. Notieren Sie sich diese Informationen. Sie benötigen es für die Konfiguration des CloudBridge Connector-Tunnels auf dem NetScaler im Rechenzentrum.

> **Hinweis:**
>
> Die Verfahren zum Konfigurieren von Microsoft Azure für einen CloudBridge Connector-Tunnel können sich je nach Microsoft Azure-Release-Zyklus im Laufe der Zeit ändern. Die neuesten Verfahren finden Sie in der Microsoft Azure-Dokumentation.

Konfigurieren der NetScaler Appliance im Rechenzentrum für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und einer Azure-Cloud zu konfigurieren, führen Sie die folgenden Aufgaben auf dem NetScaler im Rechenzentrum aus. Sie können entweder die NetScaler-Befehlszeile oder die GUI verwenden:

- **Erstellen Sie ein IPSec-Profil.** Eine IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel mit dem IPSec-Protokoll und ordnen Sie ihm das IPSec-Profil zu**. Ein IP-Tunnel gibt die lokale IP-Adresse (eine öffentliche SNIP-Adresse, die auf der NetScaler-Appliance konfiguriert ist), die Remote-IP-Adresse (die öffentliche IP-Adresse des Gateway in Azure), das Protokoll (IPSec), das zur Einrichtung des CloudBridge Connector-Tunnels verwendet wird, und eine IPSec-Profilentität an. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel und ordnen Sie ihr den IP-Tunnel zu**. Eine PBR-Entität spezifiziert eine Reihe von Bedingungen und eine IP-Tunnelentität (CloudBridge Connector-Tunnel). Der Quell-IP-Adressbereich und der Ziel-IP-Bereich sind die Bedingungen für die PBR-Entität. Sie müssen den Quell-IP-Adressbereich festlegen, um das Rechenzentrumssubnetz anzugeben, dessen Datenverkehr den Tunnel durchqueren soll, und den Ziel-IP-Adressbereich, um das Azure-Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Jedes Anforderungspaket, das von einem Client im Subnetz des Rechenzentrums stammt und an einen Server im Subnetz in der Azure-Cloud gerichtet ist, entspricht dem Quell- und Ziel-IP-Bereich der PBR-Entität. Dieses Paket wird dann für die CloudBridge Connector-Tunnelverarbeitung berücksichtigt und über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

Die GUI kombiniert all diese Aufgaben in einem einzigen Assistenten, dem CloudBridge Connector-Assistenten.
So erstellen Sie ein IPSEC-Profil mithilfe der NetScaler-Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ipsec profile <name> -psk <string> -ikeVersion v1
```

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mithilfe der NetScaler-Befehlszeile daran:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -
ipsecProfileName <string>
```

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der NetScaler-Befehlszeile daran zu binden

```
add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> ipTunnel
 <tunnelName> apply pbrs
```

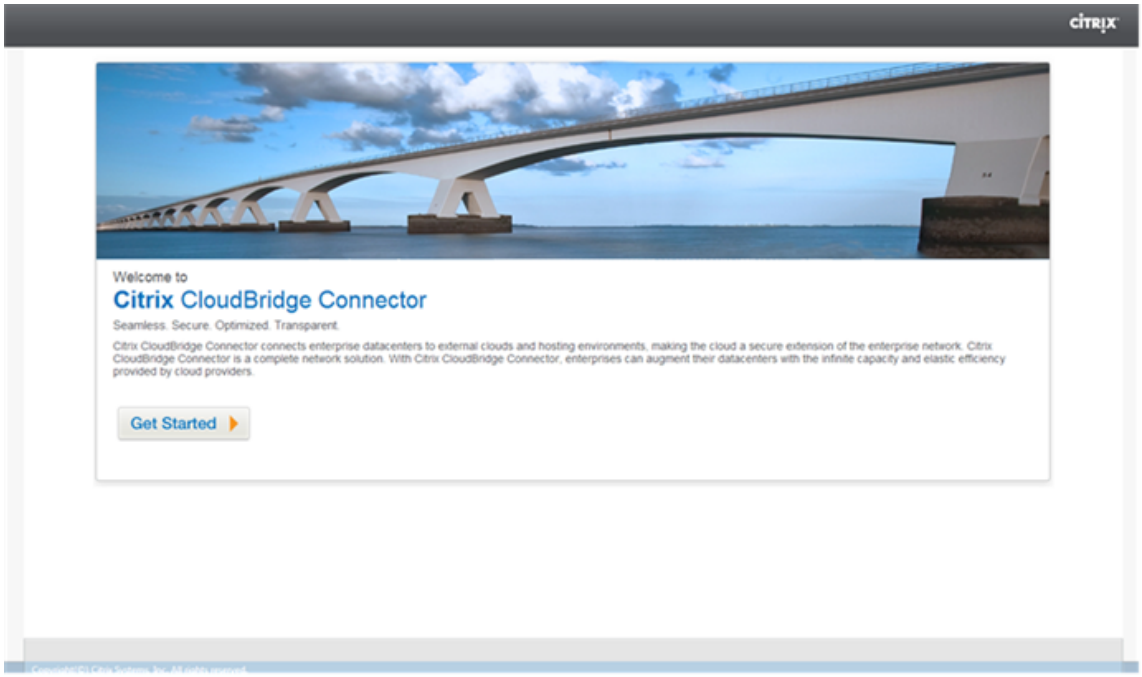
Beispielkonfiguration

Mit den folgenden Befehlen werden alle Einstellungen der NetScaler-Appliance cb_Appliance-1 erstellt, die im „Beispiel für die CloudBridge Connector-Konfiguration und den Datenfluss“ verwendet werden.

```
1  > add ipsec profile CB_Azure_IPSec_Profile -psk
       DkiMgMdcbqvYREEuIvxsbKkW0FOyDiLM  -ikeVersion v1  - lifetime 31536000
2  Done
3
4  >  add iptunnel CB_Azure_Tunnel 168.63.252.133 255.255.255.255
       66.165.176.15  - protocol IPSEC  - ipsecProfileName
       CB_Azure_IPSec_Profile
5  Done
6
7  > add pbr CB_Azure_Pbr -srcIP 10.102.147.0-10.102.147.255  - destIP
       10.20.0.0-10.20.255.255  - ipTunnelCB_Azure_Tunnel
8  Done
9
10 > apply pbrs
11 Done
12 <!--NeedCopy-->
```

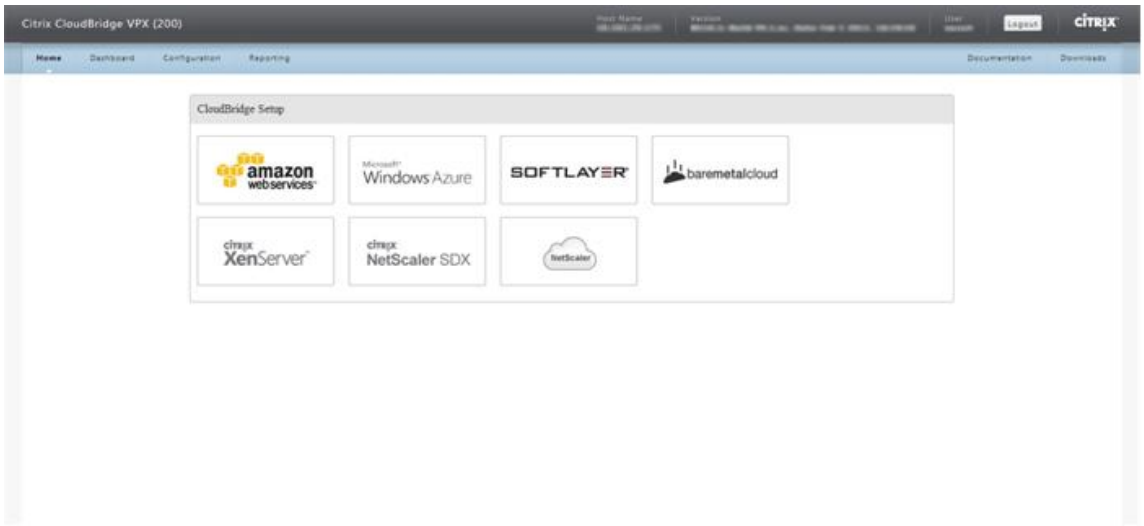
So konfigurieren Sie einen CloudBridge Connector-Tunnel in einer NetScaler-Appliance mithilfe der GUI

1. Greifen Sie auf die GUI zu, indem Sie einen Webbrowser verwenden, um eine Verbindung zur IP-Adresse der NetScaler-Appliance im Rechenzentrum herzustellen.
2. Navigieren Sie zu **System** > **CloudBridge Connector**.
3. Klicken Sie im rechten Bereich unter **Erste Schritte**auf CloudBridge **erstellen/überwachen**.
4. Klicken Sie auf **Erste Schritte**.

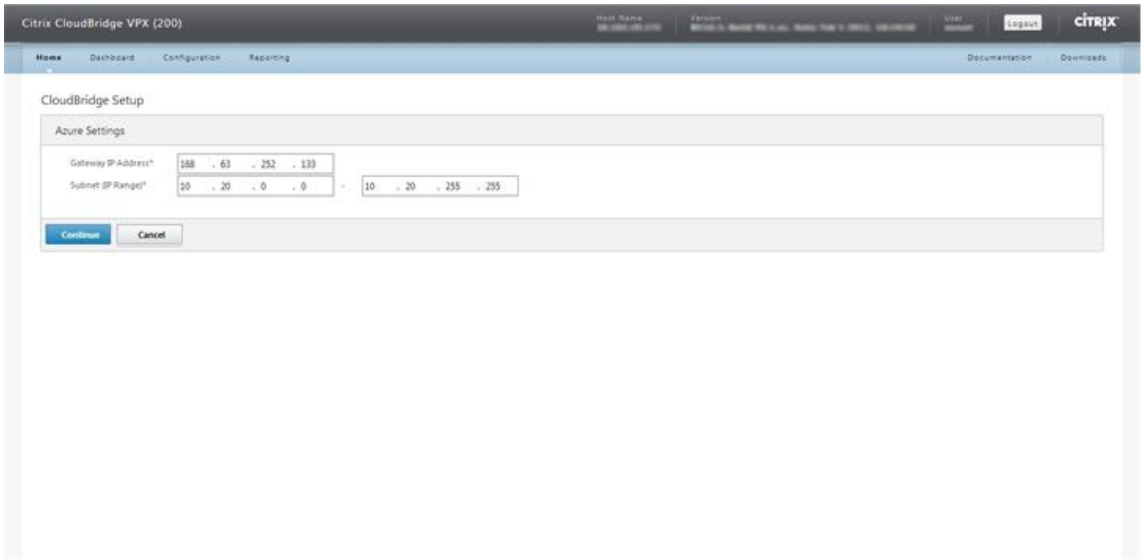


> **Hinweis**: Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der NetScaler-Appliance konfiguriert haben, wird dieser Bildschirm nicht angezeigt, und Sie werden zum CloudBridge Connector-Setup-Bereich weitergeleitet.

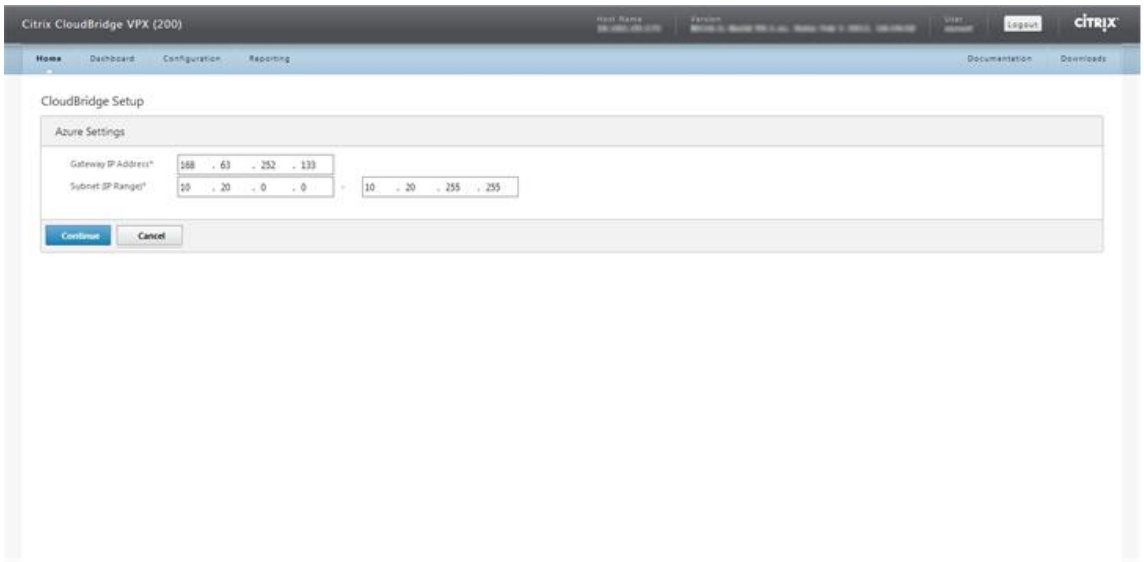
5. Klicken Sie im Bereich CloudBridge-Setup auf **Microsoft Windows Azure**.



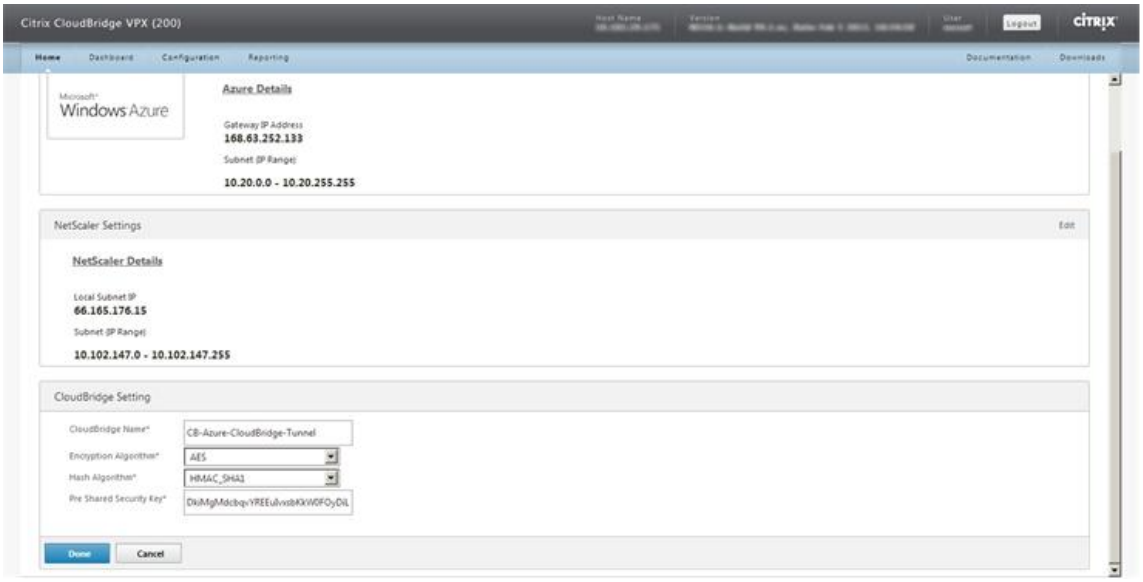
6. Geben Sie im Bereich Azure-Einstellungen in das Feld **Gateway-IP-Adresse** die IP-Adresse des Azure-Gateways ein. Der CloudBridge Connector-Tunnel wird dann zwischen der NetScaler-Appliance und dem Gateway eingerichtet. Geben Sie in den Textfeldern **Subnetz (IP-Bereich)** einen Subnetzbereich (in der Azure-Cloud) an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Klicken Sie auf **Weiter**.



7. Wählen Sie im Bereich NetScaler-Einstellungen aus der Dropdownliste **Lokale Subnetz-IP** eine öffentlich zugängliche SNIP-Adresse aus, die auf der NetScaler Appliance konfiguriert ist. Geben Sie in den Textfeldern **Subnetz (IP-Bereich)** einen lokalen Subnetzbereich an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Klicken Sie auf **Weiter**.



8. Geben Sie im Bereich **CloudBridge-Einstellungen** in das Textfeld CloudBridge-Name einen Namen für die CloudBridge ein, die Sie erstellen möchten.



9. Wählen Sie aus den Dropdownlisten Verschlüsselungsalgorithmus und Hash-Algorithmus die Algorithmen AES bzw. HMAC_SHA1 aus. Geben Sie in das Textfeld Pre Shared Security Key den Sicherheitsschlüssel ein.
10. Klicken Sie auf **Fertig**.

Überwachung des CloudBridge Connector-Tunnels

Sie können Statistiken zur Überwachung der Leistung eines CloudBridge Connector-Tunnels zwischen der NetScaler-Appliance im Rechenzentrum und Microsoft Azure einsehen. Verwenden Sie die GUI oder die NetScaler-Befehlszeile, um die CloudBridge Connector-Tunnelstatistiken auf der NetScaler-Appliance anzuzeigen. Verwenden Sie das Microsoft Windows Azure Management Portal, um die CloudBridge Connector-Tunnelstatistiken in Microsoft Azure anzuzeigen.

Anzeigen von CloudBridge Connector-Tunnelstatistiken in der NetScaler Appliance

Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

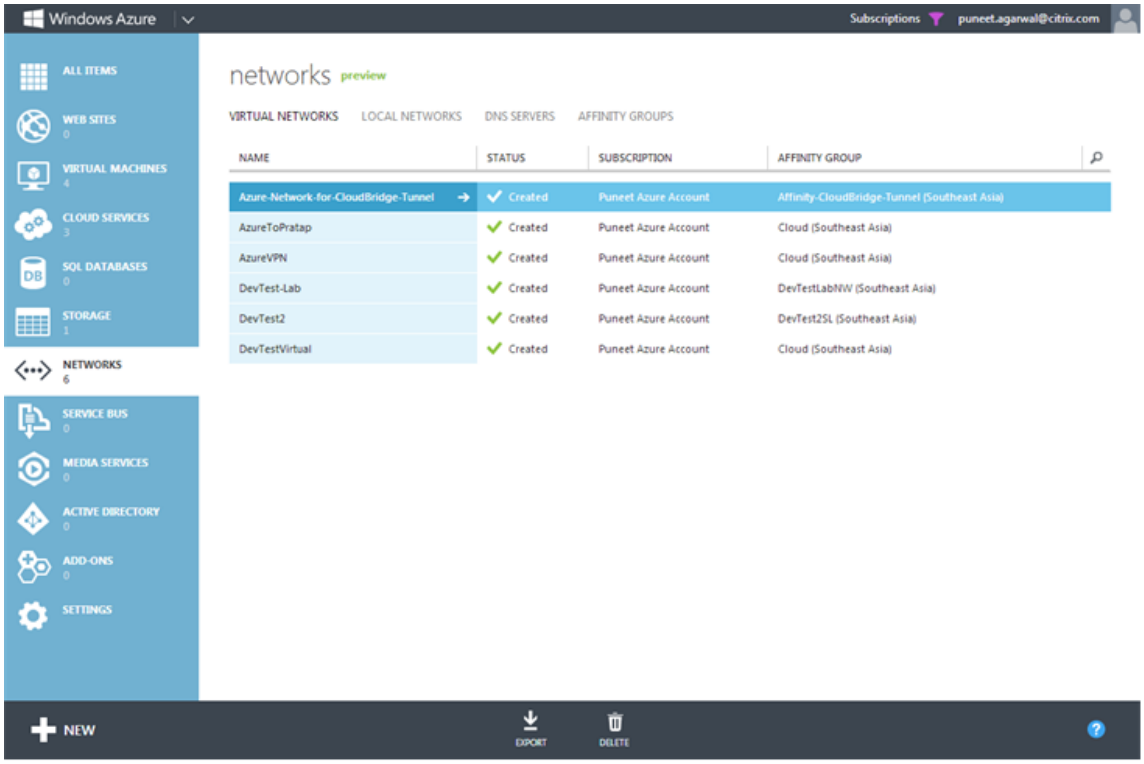
Anzeigen von CloudBridge Connector-Tunnelstatistiken in Microsoft Azure

In der folgenden Tabelle sind die statistischen Zähler aufgeführt, die für die Überwachung von CloudBridge Connector-Tunneln in Microsoft Azure verfügbar sind.

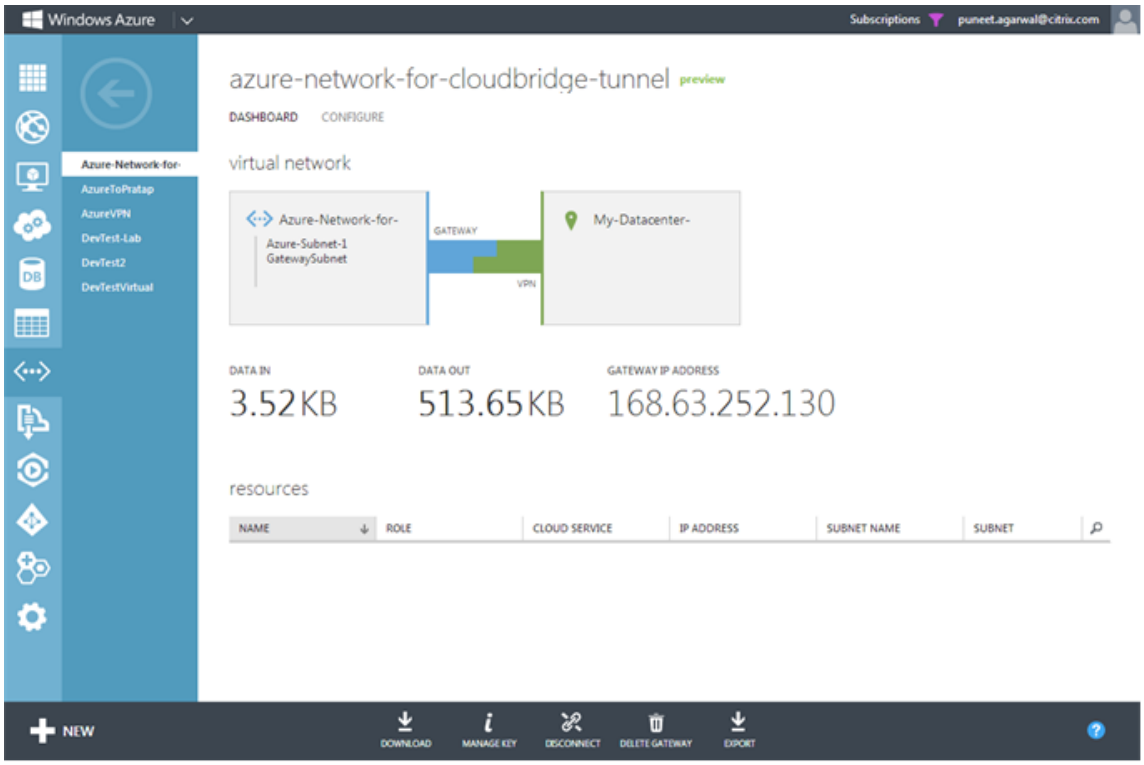
Statistischer Zähler	Spezifiziert
DATEN IN	Gesamtzahl der Kilobyte, die das Azure-Gateway seit der Erstellung des Gateways über den CloudBridge Connector-Tunnel empfangen hat.
DATEN RAUS	Gesamtzahl der Kilobyte, die das Azure-Gateway seit der Erstellung des Gateways über den CloudBridge Connector-Tunnel gesendet hat.

So zeigen Sie CloudBridge Connector-Tunnelstatistiken mithilfe des Microsoft Windows Azure-Verwaltungsportal an

1. Melden Sie sich mit den Anmeldeinformationen Ihres Microsoft Azure-Kontos am Windows Azure Management Portal an.
2. Klicken Sie im linken Bereich auf **NETWORKS**.
3. Wählen Sie auf der Registerkarte **Virtuelles Netzwerk** in der Spalte Name die virtuelle Netzwerkentität aus, die einem CloudBridge Connector-Tunnel zugeordnet ist, dessen Statistiken Sie anzeigen möchten.



4. Sehen Sie sich auf der **DASHBOARD-Seite** des virtuellen Netzwerks die DATA IN- und DATA OUT-Zähler für den CloudBridge Connector-Tunnel an.



Konfiguration des CloudBridge Connector-Tunnels zwischen Rechenzentrum und Softlayer-Unternehmens-Cloud

May 11, 2023

Die GUI enthält einen Assistenten, mit dem Sie auf einfache Weise einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance in einem Rechenzentrum und NetScaler VPX-Instanzen in der SoftLayer-Unternehmens-Cloud konfigurieren können.

Wenn Sie den Assistenten der NetScaler-Appliance im Rechenzentrum verwenden, wird die auf der NetScaler-Appliance erstellte CloudBridge Connector-Tunnelkonfiguration automatisch an den anderen Endpunkt oder Peer (den NetScaler VPX auf SoftLayer) des CloudBridge Connector-Tunnels übertragen.

Mithilfe des Assistenten der NetScaler-Appliance im Rechenzentrum führen Sie die folgenden Schritte aus, um einen CloudBridge Connector-Tunnel zu konfigurieren.

1. Stellen Sie eine Verbindung zur Softlayer Enterprise Cloud her, indem Sie die Anmeldeinformationen des Benutzers angeben.

2. Wählen Sie den Citrix XenServer aus, auf dem die NetScaler VPX-Appliance ausgeführt wird.
3. Wählen Sie die NetScaler VPX-Appliance aus.
4. Stellen Sie die CloudBridge Connector-Tunnelparameter bereit für:
    - Konfigurieren Sie einen GRE-Tunnel.
    - Konfigurieren Sie IPSec im GRE-Tunnel.
    - Erstellen Sie eine Netbridge, die eine logische Darstellung des CloudBridge-Connectors darstellt, indem Sie einen Namen angeben.
    - Binden Sie den GRE-Tunnel an die Netbridge.

So konfigurieren Sie einen CloudBridge Connector-Tunnel mithilfe der GUI

1. Melden Sie sich an der GUI der NetScaler-Appliance im Rechenzentrum an, indem Sie Ihre Kontoanmeldeinformationen für die Appliance verwenden.
2. Navigieren Sie zu **System** > **CloudBridge Connector** .
3. Klicken Sie im rechten Bereich unter **Erste Schritte**auf **CloudBridge Connector erstellen/überwachen**.
4. Klicken Sie auf **Erste Schritte**.

> **Hinweis**:
>
> Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der NetScaler-Appliance konfiguriert haben, wird dieser Bildschirm nicht angezeigt, und Sie werden zum CloudBridge Connector-Setup-Bereich weitergeleitet.

1. Klicken Sie im Bereich CloudBridge Connector Setup auf Softlayer und folgen Sie dann den Anweisungen des Assistenten.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Konfiguration eines CloudBridge Connector-Tunnels zwischen einer NetScaler-Appliance und einem Cisco IOS-Gerät

May 11, 2023

Sie können einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einem Cisco-Gerät konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk auf einen Cloud-Anbieter auszudehnen. Die NetScaler-Appliance und das Cisco IOS-Gerät bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

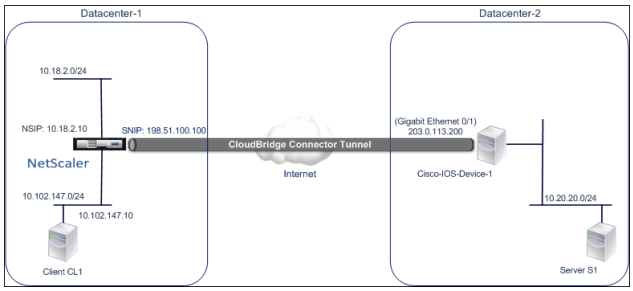
Beispiel für CloudBridge Connector-Tunnelkonfiguration und Datenfluss

Betrachten Sie zur Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet wird:

- NetScaler Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- Cisco IOS-Gerät Cisco-IOS-Device-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und Cisco-iOS-Device-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und Cisco-iOS-Device-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Auf NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPSec-Profilentität NS_Cisco_IPSec_Profile, die CloudBridge Connector-Tunnelentität NS_Cisco_Tunnel und die Policy-Based Routing (PBR) -Entität NS_Cisco_PBR.



Weitere Informationen finden Sie im CloudBridge Connector-Tunnel zwischen einer NetScaler Appliance und den Cisco IOS-Geräteeinstellungen pdf.

Zu berücksichtigende Punkte für eine CloudBridge Connector-Tunnelkonfiguration

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einem Cisco IOS-Gerät konfigurieren, sollten Sie die folgenden Punkte berücksichtigen:

- Die folgenden IPSec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einem Cisco IOS-Gerät unterstützt.

IPsec-Eigenschaften	Einstellung
IPSec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE DH-Gruppe	DH-Gruppe 2 (MODP-Algorithmus mit 1024 Bit)
IKE-Authentifizierungsmethode	Vorab gemeinsam genutzter Schlüssel
IKE-Verschlüsselungsalgorithmus	ARSCH, 3DS
IKE-Hash-Algorithmus	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5
ESP-Verschlüsselungsalgorithmus	ARSCH, 3DS
ESP-Hash-Algorithmus	HMAC SHA1, HMAC SHA256, HMAC SHA256, HMAC SHA256, HMAC MD5

- Sie müssen dieselben IPSec-Einstellungen auf der NetScaler-Appliance und dem Cisco IOS-Gerät an den beiden Enden des CloudBridge Connector angeben.
- NetScaler stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren und gemeinsamen Parameter für die Spezifizierung eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie auf dem Cisco-Gerät denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus für IKE (beim Erstellen der IKE-Richtlinie) und ESP (beim Erstellen des IPSec-Transformationssatzes) angeben.
- Sie müssen die Firewall am NetScaler-Ende und am Cisco-Gerätesende konfigurieren, um Folgendes zu ermöglichen.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

Konfigurieren des Cisco IOS-Geräts für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel auf einem Cisco IOS-Gerät zu konfigurieren, verwenden Sie die Cisco IOS-Befehlszeilenschnittstelle, die die primäre Benutzeroberfläche für die Konfiguration, Überwachung und Wartung von Cisco-Geräten darstellt.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration auf einem Cisco IOS-Gerät beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto mit Administratoranmeldeinformationen auf dem Cisco IOS-Gerät.

- Sie sind mit der Cisco IOS-Befehlszeilenschnittstelle vertraut.
- Das Cisco IOS-Gerät ist in Betrieb, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.

> **Hinweis**:
>
> Die Verfahren zum Konfigurieren des CloudBridge Connector-Tunnels auf einem Cisco IOS-Gerät können sich je nach Cisco Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle Cisco-Produktdokumention zu befolgen, um weitere Informationen zu erhalten, siehe Thema Konfigurieren von IPSec-VPN-Tunneln .

Um einen CloudBridge-Connector-Tunnel zwischen einer NetScaler Appliance und einem Cisco IOS-Gerät zu konfigurieren, führen Sie die folgenden Aufgaben in der IOS-Befehlszeile des Cisco-Gerätsaus:

- Erstellen Sie eine IKE-Richtlinie.
- Konfigurieren Sie einen vorab freigegebenen Schlüssel für die IKE-Authentifizierung.
- Definieren Sie einen Transformationssatz und konfigurieren Sie IPsec im Tunnelmodus.
- Erstellen Sie eine Krypto-Zugriffsliste
- Erstellen Sie eine Krypto-Karte
- Wenden Sie die Krypto-Map auf eine Schnittstelle an

Die Beispiele in den folgenden Prozeduren erstellen Einstellungen `Cisco IOS device Cisco-IOS-Device-1` im Abschnitt “Beispiel für CloudBridge Connector-Konfiguration und Datenfluss. “

Informationen**zum Erstellen einer IKE-Richtlinie**finden Sie im PDF-Format der IKE-Richtlinie .

So konfigurieren Sie einen Pre-Shared-Key mithilfe der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:

Befehl	Beispiel	Beschreibung des Befehls
krypto-isakmp-Identitätsadresse	Cisco-iOS-Device-1 (Konfiguration) # Crypto-ISAKMP-Identitätsadresse	Geben Sie die ISAKMP-Identität (Adresse) für das Cisco IOS-Gerät an, das bei der Kommunikation mit dem Peer (NetScaler-Appliance) während IKE-Verhandlungen verwendet werden soll. In diesem Beispiel wird das Schlüsselwort address angegeben, das die IP-Adresse 203.0.113.200 (Gigabit-Ethernet-Schnittstelle 0/1 von Cisco-iOS-Device-1) als Identität für das Gerät verwendet.
Krypto ist ein KMP-Schlüssel, Schlüsselzeichenfolge, Adresse, Peer-Adresse	Cisco-iOS-Device-1 (Config) # crypto isakmp key example presharedkey address 198.51.100.100	Geben Sie einen Pre-Shared-Schlüssel für die IKE-Authentifizierung an. In diesem Beispiel wird der gemeinsame Schlüssel examplepresharedkey für die Verwendung mit der NetScaler-Appliance NS_Appliance-1 (198.51.100.100) konfiguriert. Der gleiche vorab freigegebene Schlüssel muss auf der NetScaler Appliance konfiguriert werden, damit die IKE-Authentifizierung zwischen dem Cisco IOS-Gerät und der NetScaler-Appliance erfolgreich ist.

So erstellen Sie eine Krypto-Zugriffsliste mit der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts den folgenden Befehl im globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
Zugriffsliste Zugriffslistennummer zulassen IP-Quelle Wildcard Ziel Wildcard	Cisco-iOS-Device-1 (Config) # Zugriffsliste 111 erlaubt IP 10.20.20.0 0.0.0.255 10.102.147.0 0.0.0.255	Geben Sie Bedingungen an, um die Subnetze zu bestimmen, deren IP-Verkehr über den CloudBridge Connector-Tunnel geschützt werden soll. In diesem Beispiel wird die Zugriffsliste 111 so konfiguriert, dass der Datenverkehr vor Subnetzen 10.20.20.0/24 (auf der Seite Cisco-iOS-Device-1) und 10.102.147.0/24 (auf der Seite NS_Appliance-1) geschützt wird.

So definieren Sie eine Transformation und konfigurieren den IPSec-Tunnelmodus mithilfe der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:
Befehl	Beispiel	Beschreibung des Befehls
–	–	–
crypto ipsec transform-Setname ESP_Authentication_Transform ESP_Encryption_Transform Hinweis: ESP_Authentication_Transform kann die folgenden Werte annehmen: esp-sha-hmac, esp-sha256-hmac, esp-sha384-hmac, esp-sha512-hmac, esp-md5-hmac. ESP_Encryption_Transform kann die folgenden Werte annehmen: esp-aes oder esp-3des	Cisco-ios-device-1(config)# crypto ipsec transform-set NS-CISCO-TS esp-sha256-hmac esp-3des	Definieren Sie einen Transformationssatz und geben Sie den ESP-Hash-Algorithmus (für die Authentifizierung) und den ESP-Verschlüsselungsalgorithmus an, die beim Datenaustausch zwischen den CloudBridge Connector-Tunnel-Peers verwendet werden sollen. In diesem Beispiel wird der Transformationssatz NS-CISCO-TS definiert und der ESP-Authentifizierungsalgorithmus als esp-sha256-hmac und der ESP-Verschlüsselungsalgorithmus als esp-3des angegeben.
Mode-Tunnel	Cisco-IOS-Gerät-1 (config-Crypto-Trans) # Modus-Tunnel	Stellen Sie IPSec im Tunnelmodus ein.

|exit|Cisco-IOS-Device-1 (config-Crypto-Trans) # exit, Cisco-IOS-Device-1 (config) #|Beenden Sie den globalen Konfigurationsmodus.|

So erstellen Sie eine Krypto-Map mit der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
—	–	–
Crypto Mapmap-Name seq-num ipsec-isakmp	Cisco-iOS-Device-1 (Konfiguration) # Krypto-Map NS-CISCO-CM 2 ipsec-isakmp	Rufen Sie den Crypto-Map-Konfigurationsmodus auf, geben Sie eine Sequenznummer für die Crypto-Map an und konfigurieren Sie die Crypto-Map so, dass IKE zur Einrichtung von Sicherheitszuordnungen (SAs) verwendet wird. In diesem Beispiel werden Sequenznummer 2 und IKE für die Crypto-Map NS-CISCO-CM konfiguriert.
Peer-IP-Adresse festlegen	Cisco-iOS-Device-1 (config-crypto-map) # auf Peer 172.23.2.7 setzen	Geben Sie den Peer (NetScaler Appliance) anhand seiner IP-Adresse an. In diesem Beispiel wird 198.51.100.100 angegeben, was die CloudBridge Connector-Endpunkt-IP-Adresse auf der NetScaler-Appliance ist.
übereinstimmen/adresse/zugriffslist-id	Cisco-iOS-Device-1 (config-crypto-map) # entspricht der Adresse 111	Geben Sie eine erweiterte Zugriffsliste an. Diese Zugriffsliste legt die Bedingungen fest, um die Subnetze zu bestimmen, deren IP-Verkehr über den CloudBridge Connector-Tunnel geschützt werden soll. In diesem Beispiel wird die Zugriffsliste 111 spezifiziert.
Transformationssatz Transformationssatzname setzen	Cisco-iOS-Device-1 (Config-Crypto-Map) # Transformationssatz NS-CISCO-TS festlegen	Geben Sie an, welche Transformationssätze für diesen Crypto-Map-Eintrag zulässig sind. In diesem Beispiel wird der Transformationssatz NS-CISCO-TS spezifiziert.
Exit	cisco-iOS-Device-1 (config-crypto-map) # exit
cisco-iOS-Device-1 (config) #	Zurück in den globalen Konfigurationsmodus.	

So wenden Sie eine Krypto-Map über die Cisco IOS-Befehlszeile auf eine Schnittstelle an:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
Schnittstellen-Schnittstellen-ID	Cisco-iOS-Device-1 (Konfiguration) # Schnittstelle GigabitEthernet 0/1	Geben Sie eine physische Schnittstelle an, auf die die Crypto-Map angewendet werden soll, und wechseln Sie in den Schnittstellenkonfigurationsmodus. Dieses Beispiel spezifiziert die Gigabit-Ethernet-Schnittstelle 0/1 des Cisco-iOS-Device-1 von Cisco. Die IP-Adresse 203.0.113.200 ist bereits für diese Schnittstelle festgelegt.
Krypto-Mapmap-Name	Cisco-iOS-Device-1 (config-if) # Krypto-Map NS-CISCO-CM	Wenden Sie die Crypto-Map auf die physische Schnittstelle an. In diesem Beispiel wird die Krypto-Map NS-CISCO-CM angewendet.
exit	Cisco-iOS-Device-1 (config-if) # beenden, Cisco-IOS-Device-1 (config) #	Beenden Sie den globalen Konfigurationsmodus.

Konfigurieren der NetScaler Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einem Cisco IOS-Gerät zu konfigurieren, führen Sie die folgenden Aufgaben auf der NetScaler-Appliance aus. Sie können entweder die NetScaler-Befehlszeile oder die grafische Benutzeroberfläche (GUI) von NetScaler verwenden:

- Erstellen Sie ein IPSec-Profil.
- Erstellen Sie einen IP-Tunnel, der das IPSec-Protokoll verwendet, und verknüpfen Sie das IPSec-Profil damit.
- Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel.

So erstellen Sie ein IPSEC-Profil mit der NetScaler-Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1`
- `show ipsec profile <name>`

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mithilfe der NetScaler-Befehlszeile daran:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `add ipTunnel <name>`

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mithilfe der NetScaler-Befehlszeile daran:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbrs <pbrName>`

Die folgenden Befehle erstellen Einstellungen im `NetScaler appliance NS_Appliance-1` Abschnitt **Beispiel für CloudBridge Connector-Konfiguration und Datenfluss**.

```
1      > add ipsec profile NS_Cisco_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 - lifetime 315360 - encAlgo 3
          DES
2      Done
3      > add iptunnel NS_Cisco_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 - protocol IPSEC - ipsecProfileName
          NS_Cisco_IPSec_Profile
4
5      Done
6      > add pbr NS_Cisco_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
          10.20.0.0-10.20.255.255 - ipTunnel NS_Cisco_Tunnel
7
8      Done
9      > apply pbrs
10
11     Done
12 <!--NeedCopy-->
```

So erstellen Sie ein IPSEC-Profil mit der GUI:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen **Sie im Dialogfeld IPSec-Profil hinzufügen** die folgenden Parameter ein:
   - Name
   - Verschlüsselungsalgorithmus

- Hash-Algorithmus
- IKE-Protokollversion

4. Konfigurieren Sie die **IPSec-Authentifizierungsmethode**, die von den beiden CloudBridge Connector-Tunnel-Peers zur gegenseitigen Authentifizierung verwendet wird: Wählen Sie die **Pre-Shared Key Authentifizierungsmethode** aus, und legen Sie den Parameter **Pre-Shared Key Exists** fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil über die grafische Benutzeroberfläche daran:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Stellen **Sie im Dialogfeld IP-Tunnel hinzufügen** die folgenden Parameter ein:
   - Name
   - Remote-IP
   - Maske aus der Ferne
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option Subnetz-IP aus).
   - Lokale IP (Alle konfigurierten IPs des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPSec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Stellen **Sie im Dialogfeld PBR erstellen** die folgenden Parameter ein:
   - Name
   - Aktion
   - Nächster Hop-Typ (IP-Tunnelauswählen)
   - Name des IP-Tunnels
   - Quell-IP Low
   - Quell-IP High
   - Ziel-IP Niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So wenden Sie eine PBR mit der GUIan:

1. Navigieren Sie zu **System** > **Netzwerk** > **PBRs**.
2. **Wählen Sie auf der Registerkarte**PBRs**die**PBR**aus und wählen Sie in der**Aktionsliste**die Option Anwenden aus.**

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge Connector-Tunnels wird im Bereich Configured CloudBridge Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Konfiguration eines CloudBridge Connector-Tunnels zwischen einer NetScaler-Appliance und einer Fortinet FortiGate-Appliance

May 11, 2023

Sie können einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer Fortinet FortiGate-Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk auf einen Cloud-Anbieter auszudehnen. Die NetScaler-Appliance und die FortiGate-Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

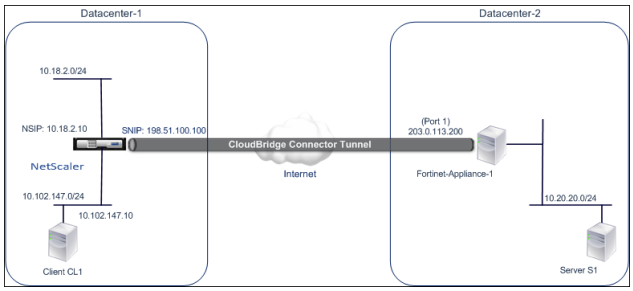
Beispiel für eine CloudBridge Connector-Tunnelkonfiguration

Betrachten Sie zur Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet wird:

- NetScaler Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- FortiGate-Appliance FortiGate-Appliance-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und FortiGate-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und FortiGate-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Auf NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPSec-Profilentität NS_Fortinet_IPSec_Profile, die CloudBridge Connector-Tunnelentität NS_Fortinet_Tunnel und die Policy-Based Routing (PBR) -Entität NS_Fortinet_PBR.



Weitere Informationen finden Sie unter CloudBridge Connector-Tunnelkonfigurationstabelle pdf.

Informationen zu Einstellungen für Fortinet Fortigate-Appliance-1 in Rechenzentrum-2 finden Sie in der Tabelle.

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer NetScaler Appliance und einer FortiGate-Appliance konfigurieren, sollten Sie die folgenden Punkte beachten:

- Die folgenden IPsec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer NetScaler Appliance und einer FortiGate-Appliance unterstützt.

IPsec-Eigenschaften	Einstellungen
IPSec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE DH-Gruppe	DH-Gruppe 2 (MODP-Algorithmus mit 1024 Bit)
IKE-Authentifizierungsmethode	Vorab gemeinsam genutzter Schlüssel
IKE-Verschlüsselungsalgorithmus	AES
IKE-Hash-Algorithmus	HMAC SHA1
ESP-Verschlüsselungsalgorithmus	AES
ESP-Hash-Algorithmus	HMAC SHA1

- Sie müssen dieselben IPSec-Einstellungen auf der NetScaler-Appliance und der FortiGate-Appliance an den beiden Enden des CloudBridge Connector angeben.
- NetScaler stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemein-

samen Parameter für die Spezifizierung eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie in der FortiGate-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in IKE (Phase-1-Konfiguration) und ESP (Phase-2-Konfiguration) angeben.

- Sie müssen die Firewall am NetScaler-Ende und am FortiGate-Ende so konfigurieren, dass Folgendes möglich ist.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)
- Die FortiGate-Appliance unterstützt zwei Arten von VPN-Tunneln: richtlinienbasierte und routenbasierte. Zwischen einer FortiGate-Appliance und einer NetScaler-Appliance wird nur ein richtlinienbasierter VPN-Tunnel unterstützt.

Konfiguration der FortiGate-Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel auf einer FortiGate-Appliance zu konfigurieren, verwenden Sie den Fortinet Web-based Manager, die primäre Benutzeroberfläche für die Konfiguration, Überwachung und Wartung von FortiGate-Appliances.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration auf einer FortiGate-Appliance beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto mit Administratoranmeldeinformationen auf der FortiGate-Appliance.
- Sie kennen den Fortinet Web-based Manager.
- Die FortiGate-Appliance ist in Betrieb und läuft, ist mit dem Internet verbunden und außerdem mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.

> **Hinweis**
>
> Die Verfahren zum Konfigurieren des CloudBridge Connector-Tunnels auf einer FortiGate Appliance können sich je nach Fortinet-Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle Fortinet-Produktdokumentation zum Konfigurieren von IPSec-VPN-Tunnelnzu befolgen.

Um einen CloudBridge-Connector-Tunnel zwischen einer NetScaler Appliance und einer FortiGate-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der FortiGate-Appliance mithilfe des webbasierten Fortinet-Managers aus:

- **Aktivieren Sie die richtlinienbasierte IPSec-VPN-Funktion**. Aktivieren Sie diese Funktion, um richtlinienbasierte VPN-Tunnel auf der FortiGate-Appliance zu erstellen. Zwischen

einer FortiGate-Appliance und einer NetScaler-Appliance wird nur ein richtlinienbasierter VPN-Tunneltyp unterstützt. Eine richtlinienbasierte VPN-Tunnelkonfiguration auf einer FortiGate-Appliance umfasst Phase-1-Einstellungen, Phase-2-Einstellungen und eine IPSec-Sicherheitsrichtlinie.

- **Definieren Sie Phase-1-Parameter.** Phase-1-Parameter werden von der FortiGate-Appliance für die IKE-Authentifizierung verwendet, bevor ein sicherer Tunnel zur NetScaler-Appliance gebildet wird.
- **Definieren Sie Phase-2-Parameter**. Phase-2-Parameter werden von der FortiGate-Appliance verwendet, um einen sicheren Tunnel zur NetScaler-Appliance zu bilden, indem IKE-Sicherheitszuordnungen (SA) eingerichtet werden.
- **Geben Sie private Subnetze**an. Definieren Sie die FortiGate-seitigen und die Netscaler-seitigen privaten Subnetze, deren IP-Verkehr durch den Tunnel transportiert werden soll.
- **Definieren Sie eine IPSec-Sicherheitsrichtlinie für den Tunnel**. Eine Sicherheitsrichtlinie ermöglicht den IP-Verkehr zwischen Schnittstellen auf einer FortiGate-Appliance. Eine IPSec-Sicherheitsrichtlinie spezifiziert die Schnittstelle zum privaten Subnetz und die Schnittstelle, die die NetScaler-Appliance über den Tunnel verbindet.

So aktivieren Sie die richtlinienbasierte IPSec-VPN-Funktion mithilfe des Fortinet Web-based Managers

1. Navigieren Sie zu **System** > **Konfiguration** > **Funktionen**.
2. Wählen Sie auf der Seite **mit den Funktionseinstellungen** die Option **Mehr anzeigen** aus und aktivieren Sie das **richtlinienbasierte IPSec-VPN**.

So definieren Sie Phase-1-Parameter mithilfe des Fortinet Web-based Managers

1. Navigieren Sie zu **VPN** > **IPSec** > **Auto Key (IKE)** und klicken Sie auf **Create Phase1**.
2. Stellen Sie auf der Seite **Neue Phase 1** die folgenden Parameter ein:
    - Name: Geben Sie einen Namen für diese Phase-1-Konfiguration ein.
    - Remote Gateway: Wählen Sie *Statische IP-Adresse aus.*
    - Modus: Wählen Sie *Main (ID-Schutz)*.
    - Authentifizierungsmethode: Wählen Sie *Preshared Key*aus.
    - Pre-Shared Key: Geben Sie einen Pre-Shared-Schlüssel ein. Derselbe Pre-Shared-Schlüssel muss auf der NetScaler-Appliance konfiguriert werden.
    - Peer-Optionen: Stellen Sie die folgenden IKE-Parameter für die Authentifizierung einer NetScaler-Appliance ein.
        - IKE-Version: Wählen Sie *1.*
        - Modus-Konfiguration: Deaktivieren Sie diese Option, falls sie ausgewählt ist.
        - Lokale Gateway-IP: Wählen Sie *Main Interface IP*aus.
        - P1-Vorschlag: Wählen Sie die Verschlüsselungs- und Authentifizierungsalgorithmen für die IKE-Authentifizierung aus, bevor Sie einen sicheren Tunnel zur NetScaler-Appliance bilden.

        * 1 — Verschlüsselung: Wählen Sie *AES128*.
        * Authentifizierung: Wählen Sie *SHA1*aus.
        * Schlüssellebensdauer: Geben Sie eine Zeitspanne (in Sekunden) für die Lebensdauer des Phase-1-Schlüssels ein.
        * DH-Gruppe: Wählen Sie 2aus.
      - *X-Auth: Wählen Sie Deaktivieren.*
      - Deed Peer Detection: Wählen Sie diese Option.
3. Klicken Sie auf **OK**.

So spezifizieren Sie private Subnetze mithilfe des Fortinet Web-based Managers

1. Navigieren Sie zu **Firewall-Objekte** > **Adresse** > **Adressen** und wählen Sie **Neu erstellen**aus.
2. Stellen Sie auf der Seite **Neue Adresse** die folgenden Parameter ein:
   - Name: Geben Sie einen Namen für das FortiGate-seitige Subnetz ein.
   - Typ: Wählen Sie *Subnetz*aus.
   - Subnetz/IP-Bereich: Geben Sie die Adresse des FortiGate-seitigen Subnetzes ein.
   - Schnittstelle: Wählen Sie die lokale Schnittstelle zu diesem Subnetz aus.
3. Klicken Sie auf **OK**.
4. Wiederholen Sie die Schritte 1 bis 3, um das Netscaler-seitige Subnetz anzugeben.

So definieren Sie Phase-2-Parameter mithilfe des Fortinet Web-based Managers

1. Navigieren Sie zu **VPN** > **IPSec** > **Auto Key (IKE)** und klicken Sie auf **Create Phase 2.**
2. Stellen Sie auf der Seite **Neue Phase 2** die folgenden Parameter ein:
   - Name: Geben Sie einen Namen für diese Phase-2-Konfiguration ein.
   - Phase 1: Wählen Sie die Phase-1-Konfiguration aus der Drop-down-Liste aus.
3. Klicken Sie auf **Erweitert** und stellen Sie die folgenden Parameter ein:
   - P2-Vorschlag: Wählen Sie die Verschlüsselungs- und Authentifizierungsalgorithmen für die Bildung eines sicheren Tunnels zur NetScaler-Appliance aus.
     - 1 — Verschlüsselung: Wählen Sie *AES128*.
     - Authentifizierung: Wählen Sie *SHA1*aus.
     - Wiedergabe-Erkennung aktivieren: Wählen Sie diese Option.
     - Perfect Forward Secrecy (PFS) aktivieren: Wählen Sie diese Option.
     - DH-Gruppe: Wählen Sie *2*aus.
   - Schlüssellebensdauer: Geben Sie eine Zeitspanne (in Sekunden) für die Lebensdauer des Phase-2-Schlüssels ein.
   - Autokey Keep Alive: Wählen Sie diese Option.
   - Automatisch verhandeln: Wählen Sie diese Option.
   - Quick Mode Selector: Geben Sie die FortiGate-seitigen und die Netscaler-seitigen privaten Subnetze an, deren Datenverkehr durch den Tunnel geleitet werden soll.
     - Quelladresse: Wählen Sie das FortiGate-seitige Subnetz aus der Dropdownliste aus.
     - Quellport: Geben Sie *0*ein.

- Zieladresse: Wählen Sie das Netscaler-seitige Subnetz aus der Dropdownliste aus.
- Zielport: Geben Sie *0*ein.
- Protokoll: Geben Sie *0*ein.

4. Klicken Sie auf **OK**.

So definieren Sie eine IPSec-Sicherheitsrichtlinie mithilfe des Fortinet Web-based Managers

1. Navigieren Sie zu **Richtlinie** > **Richtlinie** > **Richtlinie** und klicken Sie auf **Neu erstellen**.
2. Stellen Sie auf der Seite **„Richtlinie bearbeiten** “ die folgenden Parameter ein:
   - Richtlinientyp: Wählen Sie *VPN*aus.
   - Richtlinienuntertyp: Wählen Sie *IPSec*aus.
   - Lokale Schnittstelle: Wählen Sie die lokale Schnittstelle zum internen (privaten) Netzwerk aus.
   - Lokales geschütztes Subnetz: Wählen Sie das FortiGate-seitige Subnetz aus der Dropdownliste aus, dessen Datenverkehr durch den Tunnel durchlaufen werden soll.
   - Ausgehende VPN-Schnittstelle: Wählen Sie die lokale Schnittstelle zum externen (öffentlichen) Netzwerk aus.
   - Remotegeschütztes Subnetz: Wählen Sie das NetScaler-seitige Subnetz aus der Dropdownliste aus, dessen Datenverkehr durch den Tunnel durchlaufen werden soll.
   - Zeitplan: Behalten Sie die Standardeinstellung (*immer*) bei, sofern keine Änderungen erforderlich sind, um bestimmte Anforderungen zu erfüllen.
   - Service: Behalten Sie die Standardeinstellung (*ANY) bei*, sofern keine Änderungen erforderlich sind, um Ihre spezifischen Anforderungen zu erfüllen.
   - VPN-Tunnel: Wählen Sie *Vorhandene verwenden* und wählen Sie den Tunnel aus der Dropdownliste aus.
   - Die Initiierung des Datenverkehrs vom Remotestandort zulassen: Wählen Sie aus, ob der Datenverkehr aus dem Remotenetzwerk den Tunnel initiieren darf.
3. Klicken Sie auf **OK**.

Konfigurieren der NetScaler Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer FortiGate-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der NetScaler-Appliance aus. Sie können entweder die NetScaler-Befehlszeile oder die grafische Benutzeroberfläche (GUI) von NetScaler verwenden:

- **Erstellen Sie ein IPSec-Profil.** Eine IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und Authentifizierungsmethode an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel, der das IPSec-Protokoll verwendet, und verknüpfen Sie das IPSec-Profil damit**. Ein IP-Tunnel gibt die lokale IP-Adresse (auf der NetScaler-Appliance konfigurierte IP-Adresse des CloudBridge Connector-Tunnelendpunkts (vom Typ

SNIP), die Remote-IP-Adresse (auf der FortiGate-Appliance konfigurierte IP-Adresse des CloudBridge Connector-Tunnelendpunkts), das Protokoll (IPSec), das zur Einrichtung des CloudBridge Connector-Tunnels verwendet wird, und eine IPSec-Profilentität an. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.

- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität spezifiziert eine Reihe von Regeln und eine IP-Tunnelentität (CloudBridge Connector-Tunnel). Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das Netscaler-seitige Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll, und legen Sie den Ziel-IP-Adressbereich fest, um das FortiGate-Appliance-seitige Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll.

So erstellen Sie ein IPSEC-Profil über die NetScaler Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Um einen IPSEC-Tunnel zu erstellen und das IPSEC-Profil mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName** <string>`
- `show ipTunnel <name>`

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

So erstellen Sie ein IPSEC-Profil mithilfe der GUI

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **IPSec-Profil hinzufügen** “ die folgenden Parameter ein:
    - Name
    - Verschlüsselungsalgorithmus
    - Hash-Algorithmus

- IKE-Protokollversion
- Perfect Forward Secrecy (diesen Parameter aktivieren)

4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers zur gegenseitigen Authentifizierung verwendet wird: Wählen Sie die Pre-Shared Key Authentifizierungsmethode aus, und legen Sie den Parameter Pre-Shared Key Exists fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um einen IP-Tunnel zu erstellen und das IPSEC-Profil mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Stellen Sie auf der Seite **IP-Tunnel hinzufügen** die folgenden Parameter ein:
    - Name
    - Remote-IP
    - Maske aus der Ferne
    - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option *Subnetz-IP*aus).
    - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
    - Protokoll
    - IPSec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **PBR erstellen** “ die folgenden Parameter ein:
    - Name
    - Aktion
    - Nächster Hop-Typ (*IP-Tunnel*auswählen)
    - Name des IP-Tunnels
    - Quell-IP Low
    - Quell-IP High
    - Ziel-IP Niedrig
    - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance wird in der GUI angezeigt.

Der aktuelle Status des CloudBridge Connector-Tunnels wird im Bereich Configured CloudBridge Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Mit den folgenden Befehlen werden die Einstellungen der NetScaler-Appliance NS_Appliance-1 in „Beispiel für eine CloudBridge Connector-Konfiguration“ erstellt. „

```
1      >  add ipsec profile NS_Fortinet_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1  - encAlgo AES  - hashalgo
          HMAC_SHA1  - lifetime 315360 -perfectForwardSecrecy ENABLE
2
3       Done
4      >  add iptunnel NS_Fortinet_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100  - protocol IPSEC  - ipsecProfileName
          NS_Fortinet_IPSec_Profile
5
6       Done
7      > add pbr NS_Fortinet_Pbr -srcIP 10.102.147.0-10.102.147.255  -
          destIP 10.20.0.0-10.20.255.255  - ipTunnel NS_Fortinet_Tunnel
8
9       Done
10     > apply pbrs
11
12      Done
13 <!--NeedCopy-->
```

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

CloudBridge Connector-Tunneldiagnose und -Fehlerbehebung

May 11, 2023

Wenn Sie Probleme mit einer CloudBridge Connector-Tunnelkonfiguration haben, stellen Sie sicher, dass alle Voraussetzungen erfüllt wurden, bevor der Tunnel eingerichtet wurde. Wenn dies der Fall wäre, könnte das Problem an den IP-Adressen der Tunnelendpunkte, einer NAT-Konfiguration, der Art und Weise, wie der Tunnel eingerichtet wurde, oder am Datenverkehr liegen.

Fehlerbehebung bei einem CloudBridge Connector-Tunnel

Wenn Ihr CloudBridge Connector-Tunnel nicht ordnungsgemäß funktioniert, liegt das Problem möglicherweise an der Einrichtung des Tunnels oder am Datenverkehr. Wenn Sie sich nicht sicher sind, welche Art von Problem Sie haben, suchen Sie in der Protokolldatei nach einer Fehlermeldung und prüfen Sie, ob die Fehlermeldung in der Liste der Probleme beim Tunnelaufbau enthalten ist. Wenn Sie Ihre Fehlermeldung nicht finden, überprüfen Sie die Liste möglicher Probleme im Zusammenhang mit dem Datenverkehr.

Probleme im Zusammenhang mit der Einrichtung von Tunneln

Wenn die Anforderungen für die Konfiguration des IPSec-Tunnels erfüllt und der CloudBridge Connector-Tunnel konfiguriert ist und der Status des Tunnels nicht AKTIV ist, suchen Sie in der Datei iked.log nach Debugging-Informationen auf einer oder beiden NetScaler-Appliances, die als Tunnelendpunkte konfiguriert sind.

Geben Sie auf beiden Appliances den folgenden Befehl an der NetScaler -Shell Eingabeaufforderung ein:

```
cat /tmp/iked.debug | tee /var/iked.log
```

Das PDF zur Fehlerbehebung listet einige häufige Fehler und ihre Lösungen auf.

Probleme im Zusammenhang mit dem Datenverkehr

Wenn die Daten im CloudBridge Connector-Tunnel nicht ordnungsgemäß zwischen den Tunnelendpunkten ausgetauscht werden, gehen Sie wie folgt vor.

- Für einen CloudBridge Connector-Tunnel, der die GRE- und IPSec-Protokolle verwendet:
  - Stellen Sie sicher, dass der L2-Modus auf beiden CloudBridge Connector-Tunnelendpunkten aktiviert ist. Um den L2-Modus zu aktivieren, geben Sie den folgenden Befehl an der NetScaler-Befehlszeilenschnittstelle ein:

    ```
    enable mode L2
    ```

    * Wenn einer der CloudBridge Connector-Tunnelendpunkte eine virtuelle CloudBridge-Appliance (VPX) ist und auf einem VMware ESXi-Hypervisor bereitgestellt wird, stellen Sie sicher, dass der Promiscuous-Modus für den mit der CloudBridge VPX-Appliance verknüpften vSwitch auf Accept gesetzt ist.
  - Wenn ein VLAN durch einen CloudBridge Connector-Tunnel erweitert wird, überprüfen Sie die Eins-zu-Eins-Zuordnung auf der erweiterten VLAN-Entität an jedem der Tunnelendpunkte
  - Stellen Sie sicher, dass die IP-Tunnelentität an die richtige Netbridge-Entität in jedem der Tunnelendpunkte gebunden ist.

- Stellen Sie sicher, dass der ARP-Eintrag für den Peer-CloudBridge Connector-Tunnelendpunkt auf dem lokalen Tunnelendpunkt vorhanden ist, indem Sie den folgenden Befehl an der NetScaler-Befehlszeilenschnittstelle eingeben:
  ```
  show arp
  ```
- Wenn die Ausgabe einen unvollständigen ARP-Eintrag anzeigt, fließt kein bidirektionaler Verkehr durch den Tunnel. Wenn bidirektionaler Verkehr fließt, zeigt der ARP-Eintrag den Namen der Tunnelschnittstelle für die Geräte auf der anderen Seite des Tunnels an.
- Entfernen Sie die IP-Tunnelentitäten von beiden Tunnelendpunkten und fügen Sie sie erneut mit denselben Parametern hinzu, wobei das IPSec-Profil jedoch auf NONE gesetzt ist, sodass der Tunnel nur das GRE-Protokoll verwendet.
  Nachdem Sie im IP-Tunnel (der das GRE-Protokoll verwendet) Folgendes überprüft haben, konfigurieren Sie den Tunnel mit IPSec-Parametern, indem Sie ein gültiges IPSec-Profil für die jeweiligen IP-Tunnelentitäten an jedem der Tunnelendpunkte angeben.
  Der richtige PING- oder TCP-Fluss durch den Tunnel.
  Richtiger Fluss des Datenverkehrs durch den Tunnel.
  Nachdem sich der konfigurierte Tunnel (der die GRE- und IPSec-Protokolle verwendet) im Status UP befindet und der Datenverkehr nicht ordnungsgemäß durch den Tunnel fließt und wenn ein NAT-Gerät vor einem oder beiden Tunnelendpunkten bereitgestellt wurde, analysieren Sie die eingehenden und ausgehenden Pakete auf den NAT-Geräten.

- Wenn eine NetScaler-Appliance als Router oder Gateway verwendet wird.
  - Stellen Sie sicher, dass der L3-Modus auf der NetScaler-Appliance aktiviert ist. Um den L3-Modus zu aktivieren, führen Sie den folgenden Befehl in der CloudBridge-Befehlszeile aus.
  - aktiviere den Modus L3
  - Wenn Subnetze an eine Netbridge-Entität gebunden sind, stellen Sie sicher, dass die richtige IP-Tunnelentität auch an die Netbridge gebunden ist.
  - Führen Sie den folgenden Befehl in der NetScaler-Befehlszeile aus, um zu sehen, wo die Pakete (Eingabe und Ausgabe) verworfen werden:
    ```
    stat ipsec counters
    ```
  - Stellen Sie sicher, dass die richtigen Routen an beiden Tunnelendpunkten konfiguriert sind.
  - Wenn kein NAT-Gerät vor der NetScaler-Appliance bereitgestellt wird, stellen Sie sicher, dass die Firewalls so konfiguriert sind, dass sie alle ESP-Pakete (IP-Protokollnummer 50) und alle UDP-Pakete für Port 4500 zulassen.

Wenn keine der oben genannten Maßnahmen zu einem erfolgreichen Datenaustausch zwischen den Tunnelendpunkten führt, wenden Sie sich an den technischen Support von Citrix.

Checkliste, bevor Sie sich an den technischen Support von Citrix wenden

Stellen Sie für eine schnelle Lösung sicher, dass Sie die folgenden Artikel bereit haben, bevor Sie sich an den technischen Support von Citrix wenden.

- Einzelheiten zur Bereitstellung und Netzwerktopologie.
- Die Protokolldatei wurde gesammelt, indem Sie den folgenden Befehl an der NetScaler-Shell-Eingabeaufforderung eingeben.
  ```
  cat /tmp/iked.debug | tee /var/log/iked.log
  ```
- Das Paket für den technischen Support wurde erfasst, indem Sie den folgenden Befehl in der NetScaler-Befehlszeile eingeben.
  ```
  show techsupport
  ```
- Paketspuren wurden an beiden CloudBridge Connector-Tunnelendpunkten erfasst. Um eine Paketverfolgung zu starten, geben Sie den folgenden Befehl in der NetScaler-Befehlszeile ein.
  ```
  start nstrace -size 0
  ```
  Um die Paketverfolgung zu beenden, geben Sie den folgenden Befehl in der NetScaler-Befehlszeile ein.
  ```
  stop nstrace
  ```
- Ausgabe des folgenden Befehls, der an der NetScaler Eingabeaufforderung eingegeben wurde.
  ```
  show arp
  ```

Interoperabilität des CloudBridge Connector — strongSwan

May 11, 2023

strongSwan ist eine Open-Source-IPSec-Implementierung für Linux-Plattformen. Sie können einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer strongSwan-Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk auf einen Cloud-Anbieter auszudehnen. Die NetScaler-Appliance und die strongSwan-Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

Beispiel für eine CloudBridge Connector-Tunnelkonfiguration

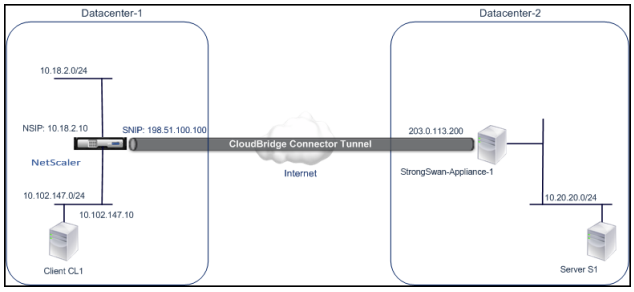
Betrachten Sie zur Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet wird:

- NetScaler Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird

- strongSWAN-Appliance strongWAN-Appliance-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und strongSwan-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und strongSwan-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Auf NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPSec-Profilentität NS_StrongSwan_IPSec_Profile, die CloudBridge Connector-Tunnelentität NS_StrongSwan_Tunnel und die Policy-Based Routing (PBR) -Entität NS_strongswan_PBR.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Haupteinstellungen des CloudBridge Connector-Tunnel-Setups

Entität	Details
IP-Adresse des CloudBridge Connector-Tunnelendpunkts (NS_Appliance-1) in Datacenter-1	198.51.100.100
IP-Adresse des CloudBridge Connector-Tunnelendpunkts (strongSwan-Appliance-1) im Rechenzentrum-2	203.0.113.200
Rechenzentrum — Subnetz 1, dessen Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll	10.102.147.0/24
Rechenzentrum — Subnetz 2, dessen Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll	10.20.20.0/24

Einstellungen auf der NetScaler-Appliance NS_Appliance-1 in Datacenter-1

|SNIP1 (nur zu Referenzzwecken)|198.51.100.100|
|–|–|–|
|IPSec Profile|NS_Strongswan_IPSec_Profile|IKE-Version: v1, Verschlüsselungsalgorithmus: AES, Hash-Algorithmus:
HMAC_SHA1 psk = examplepresharedkey (Hinweis: Dies ist zur Veranschaulichung ein Beispiel für einen Pre-Share-Schlüssel. NetScaler empfiehlt nicht, diese Zeichenfolge in Ihrer CloudBridge Connector-Konfiguration zu verwenden.) | CloudBridge
Connector-Tunnel|NS_Strongswan_Tunnel|Remote-IP = 203.0.113.200, Local IP= 198.51.100.100, Tunnelprotokoll = IPSEC, IPSec profile= NS_strongswan_IPsec_Profile| |Richtlinienbasierte Route|NS_Strongswan_PBR|Quell-IP-Bereich = Subnetz im Rechenzentrum-1=10.102.147.0-10.102.147.255, Ziel-IP-Bereich =Subnetz im Rechenzentrum-2=10.20.20.0-10.20.20.255, IP-Tunnel = NS_StrongSwan_Tunnel|

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie mit der Konfiguration des CloudBridge-Connector-Tunnels beginnen, stellen Sie sicher, dass:

- Sie haben Grundkenntnisse über Linux-Konfigurationen.
- Sie haben Grundkenntnisse über die IPSec-Protokollsuite.
- Die strongSwan-Appliance ist in Betrieb, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.
- Die NetScaler-Appliance ist in Betrieb und läuft, ist mit dem Internet verbunden und außerdem mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.
- Die folgenden IPSec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer strongSwan-Appliance unterstützt.
  - IPSec-Modus: Tunnelmodus
  - IKE-Version: Version 1
  - IKE-Authentifizierungsmethode: Pre-Shared Key
  - IKE-Verschlüsselungsalgorithmus: AES
  - IKE-Hash-Algorithmus: HMAC SHA1
  - ESP-Verschlüsselungsalgorithmus: AES
  - ESP-Hash-Algorithmus: HMAC SHA1
- Sie müssen dieselben IPSec-Einstellungen auf der NetScaler-Appliance und der strongSwan-Appliance an den beiden Enden des CloudBridge Connector-Tunnels angeben.
- NetScaler stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemeinsamen Parameter für die Spezifizierung eines IKE-Verschlüsselungsalgorithmus und eines ESP-

Verschlüsselungsalgorithmus. Daher müssen Sie in der strongSwan-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in den IKE- und ESP-Parametern in der Datei IPsec.conf angeben.

- Sie müssen die Firewall am NetScaler-Ende und am strongSwan-Ende so konfigurieren, dass Folgendes möglich ist.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

StrongSwan für den CloudBridge Connector-Tunnel konfigurieren

Um einen CloudBridge-Connector-Tunnel zwischen einer NetScaler-Appliance und einer strongSwan-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der strongSwan-Appliance aus:

- **Geben Sie die IPSec-Verbindungsinformationen in der Datei ipsec.conf an. Die Datei ipsec.conf**definiert alle Steuerungs- und Konfigurationsinformationen für IPSec-Verbindungen in der strongSwan-Appliance.
- **Geben Sie den Pre-Shared-Schlüssel in der Datei ipsec.secrets an. Die Datei ipsec.secrets**definiert Geheimnisse für die IKE/IPSec-Authentifizierung für IPSec-Verbindungen in der strongSwan-Appliance.

Die Verfahren zum Konfigurieren von IPsec VPN (CloudBridge Connector Tunnel) auf einer StrongSwan Appliance können sich je nach StrongSwan Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle StrongSwan-Dokumentation zum Konfigurieren von IPSec-VPN-Tunnelnzu befolgen.

Im Anschluss an einen Beispielauszug aus der Datei ipsec.conf werden IPsec-Informationen zum Einrichten des IPsec-VPN-Tunnels angegeben, die unter Beispiel einer CloudBridge-Connector-Konfiguration beschrieben werden. Weitere Informationen finden Sie unter CloudBridge Connector-Konfiguration pdf.

Im Anschluss an einen Beispielauszug aus der Datei ipsec.secrets wird der vorab freigegebene IKE-Authentifizierungsschlüssel zum Einrichten des IPsec-VPN-Tunnels angegeben, der unter Beispiel einer CloudBridge Connector-Konfiguration beschrieben wird.

`/etc/ipsec.secrets` PSK ‘beispielpresharedkey’ #pre -sharedkey für IPSec IKE-Authentifizierung

Konfigurieren der NetScaler Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer strongSwan-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der NetScaler-Appliance aus. Sie können entweder die NetScaler-Befehlszeile oder die grafische Benutzeroberfläche (GUI) von NetScaler verwenden:

- **Erstellen Sie ein IPSec-Profil.** Eine IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und Authentifizierungsmethode an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel, der das IPSec-Protokoll verwendet, und verknüpfen Sie das IPSec-Profil damit**. Ein IP-Tunnel gibt die lokale IP-Adresse (IP-Adresse des CloudBridge Connector-Tunnelendpunkts (vom Typ SNIP), die auf der NetScaler-Appliance konfiguriert ist), die Remote-IP-Adresse (auf der strongSwan-Appliance konfigurierte IP-Adresse des CloudBridge Connector-Tunnelendpunkts), das zum Einrichten des CloudBridge Connector-Tunnels verwendete Protokoll (IPSec) und eine IPSec-Profilentität an. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität spezifiziert eine Reihe von Regeln und eine IP-Tunnelentität (CloudBridge Connector-Tunnel). Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das Netscaler-seitige Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll, und legen Sie den Ziel-IP-Adressbereich fest, um das strongSwan-Seitensubnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll.

So erstellen Sie ein IPSEC-Profil über die NetScaler Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1`
- `show ipsec profile <name>`

Um einen IPSEC-Tunnel zu erstellen und das IPSEC-Profil mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

So erstellen Sie ein IPSEC-Profil mithilfe der GUI

1. **Navigieren Sie zu**System**>**CloudBridge****Connector**>**IPSec-Profil.****
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **IPSec-Profil hinzufügen** “ die folgenden Parameter ein:
   - Name
   - Verschlüsselungsalgorithmus
   - Hash-Algorithmus
   - IKE-Protokollversion
4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers verwendet wird, um sich gegenseitig zu authentifizieren: Wählen Sie die **Authentifizierungsmethode Pre-Shared Key** aus und legen Sie den Parameter **Pre-Shared** Key Exists fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um einen IP-Tunnel zu erstellen und das IPSEC-Profil mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Stellen Sie auf der Seite IP-Tunnel hinzufügen die folgenden Parameter ein:
   - Name
   - Remote-IP
   - Maske aus der Ferne
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option *Subnetz-IP*aus).
   - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPSec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **PBR erstellen** “ die folgenden Parameter ein:
   - Name
   - Aktion
   - Nächster Hop-Typ (*IP-Tunnel*auswählen)
   - Name des IP-Tunnels
   - Quell-IP Low
   - Quell-IP High
   - Ziel-IP Niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge Connector-Tunnels wird im Bereich Configured CloudBridge Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.
Mit den folgenden Befehlen werden die Einstellungen der NetScaler-Appliance NS_Appliance-1 in „Beispiel für eine CloudBridge Connector-Konfiguration“ erstellt:

```
1      > add ipsec profile NS_StrongSwan_IPSec_Profile -psk
           examplepresharedkey -ikeVersion v1 - encAlgo AES - hashalgo
           HMAC_SHA1
2
3
4      Done
5
6      > add iptunnel NS_StrongSwan_Tunnel 203.0.113.200 255.255.255.255
           198.51.100.100 - protocol IPSEC - ipsecProfileName
           NS_StrongSwan_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_StrongSwan_Pbr -srcIP 10.102.147.0-10.102.147.255 -
           destIP 10.20.0.0-10.20.255.255 - ipTunnel NS_StrongSwan_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Interoperabilität des CloudBridge Connector — F5 BIG-IP

May 11, 2023

Sie können einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer F5 BIG-IP-Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk auf einen Cloud-Anbieter auszudehnen. Die NetScaler-Appliance und die F5 BIG-IP-Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

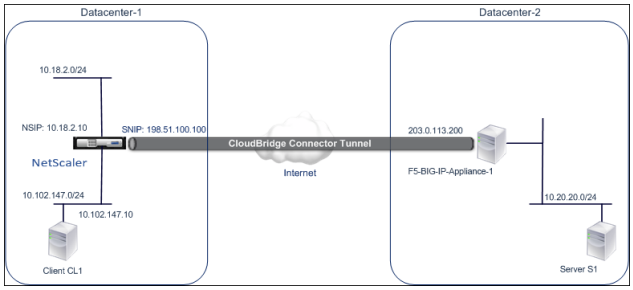
Beispiel für eine CloudBridge Connector-Tunnelkonfiguration

Betrachten Sie zur Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet wird:

- NetScaler Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- F5 BIG-IP-Appliance F5-Big-IP-Appliance-1 in einem Rechenzentrum, das als Rechenzentrum-2 ausgewiesen ist

NS_Appliance-1 und F5-Big-IP-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und F5-Big-IP-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Auf NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPSec-Profilentität NS_F5-big-IP_IPsec_Profile, die CloudBridge Connector-Tunnelentität NS_F5-big-IP_Tunnel und die Policy-Based Routing (PBR) -Entität NS_F5-big-IP_PBR.



Weitere Informationen finden Sie unter F5 big IP pdf.

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

- Die NetScaler-Appliance ist in Betrieb und läuft, ist mit dem Internet verbunden und außerdem mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-

Tunnel geschützt werden soll.

- Die F5 BIG-IP-Appliance ist in Betrieb, ist mit dem Internet verbunden und außerdem mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.
- Die folgenden IPSec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer F5 BIG-IP-Appliance unterstützt.
  - IPSec-Modus: Tunnelmodus
  - IKE-Version: Version 1
  - IKE-Authentifizierungsmethode: Pre-Shared Key
  - IKE-Verschlüsselungsalgorithmus: AES
  - IKE-Hash-Algorithmus: HMAC SHA1
  - ESP-Verschlüsselungsalgorithmus: AES
  - ESP-Hash-Algorithmus: HMAC SHA1
- Sie müssen dieselben IPSec-Einstellungen auf der NetScaler-Appliance und der F5 BIG-IP-Appliance an den beiden Enden des CloudBridge Connector-Tunnels angeben.
- NetScaler stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemeinsamen Parameter für die Spezifizierung eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie in der F5 BIG-IP-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in IKE (Phase-1-Konfiguration) und ESP (Phase-2-Konfiguration) angeben.
- Sie müssen die Firewall am NetScaler-Ende und am F5-BIG-IP-Ende so konfigurieren, dass Folgendes möglich ist.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

Konfiguration von F5 BIG-IP für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer F5 BIG-IP-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der F5 BIG-IP-Appliance aus:

- **Erstellen Sie einen virtuellen Weiterleitungsserver für IPSec.** Ein virtueller Weiterleitungsserver fängt den IP-Verkehr für den IPSec-Tunnel ab.
- **Erstellen Sie einen IKE-Peer.** Ein IKE-Peer spezifiziert die lokalen und externen IPSec-Tunnelendpunkte. Es spezifiziert auch Algorithmen und Anmeldeinformationen, die für IPSec IKE Phase 1 verwendet werden sollen.
- **Erstellen Sie eine benutzerdefinierte IPSec-Richtlinie.** Eine Richtlinie legt das IPSec-Protokoll (ESP) und den Modus (Tunnel) fest, die für die Bildung des IPSec-Tunnels verwendet werden sollen. Es spezifiziert auch die Algorithmen und Sicherheitsparameter, die für IKE IPSec

Phase 2 verwendet werden sollen.

- **Erstellen Sie einen bidirektionalen IPSec-Verkehrsselektor.** Ein Traffic Selector gibt die F5-BIG-IP-Seiten-und NetScaler-seitigen Subnetze an, deren IP-Verkehr durch den IPSec-Tunnel geleitet werden soll.

Die Verfahren zur Konfiguration von IPSec-VPN (CloudBridge Connector-Tunnel) auf einer F5 BIG-IP-Appliance können sich je nach F5-Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, dass Sie die offizielle F5 BIG-IP-Dokumentation zur Konfiguration von IPSec-VPN-Tunneln befolgen, und zwar unter:

https://f5.com

So erstellen Sie einen virtuellen Weiterleitungsserver für IPSec mithilfe der F5 BIG-IP-GUI

1. Klicken Sie auf der Registerkarte **Main** auf **Lokaler Verkehr** > **Virtuelle Server**und dann auf **Erstellen**.
2. Stellen Sie auf dem Bildschirm **Neue virtuelle Serverliste** die folgenden Parameter ein:
   - **Name**. Geben Sie einen eindeutigen Namen für den virtuellen Server ein.
   - **Typ**. Wählen Sie **Forwarding (IP)**aus.
   - **Zieladresse**. Geben Sie eine Wildcard-Netzwerkadresse im CIDR-Format ein, z. B. 0.0.0.0/0 für IPv4, um jeglichen Datenverkehr zu akzeptieren.
   - **Service-Anschluss**. Wählen Sie **Alle Ports** aus der Liste aus.
   - **Protokollliste**. Wählen Sie **Alle Protokolle** aus der Liste aus.
   - **VLAN- und Tunnelverkehr**. Behalten Sie die Standardauswahl bei, **Alle VLANs und Tunnel**.
3. Klicken Sie auf **Fertig**.

So erstellen Sie eine benutzerdefinierte IPSec-Richtlinie mithilfe der F5 BIG-IP-GUI

1. **Klicken Sie auf der Registerkarte**Main**auf**Netzwerk**>**IPSec > **IPSec-Richtlinienund klicken Sie dann auf Erstellen.**
2. Stellen Sie auf dem Bildschirm **Neue Richtlinie** die folgenden Parameter ein:
   - **Name**. Geben Sie einen eindeutigen Namen für die Richtlinie ein.
   - **IPSec-Protokoll.** Behalten Sie die Standardauswahl bei, ESP.
   - **Modus**. Wählen Sie Tunnel aus. Der Bildschirm wird aktualisiert und zeigt weitere zugehörige Einstellungen an.
   - **Lokale Tunneladresse**. Geben Sie die IP-Adresse des lokalen IPSec-Tunnelendpunkts ein (konfiguriert auf der F5 BIG-IP-Appliance).
   - **Tunnel-Remoteadresse**. Geben Sie die IP-Adresse des Remote-IPSec-Tunnelendpunkts ein (auf der NetScaler-Appliance konfiguriert).
3. Behalten Sie für die IKE-Phase-2-Parameter die Standardwerte bei, oder wählen Sie die Optionen aus, die für Ihre Bereitstellung geeignet sind.
4. Klicken Sie auf **Fertig**.

So erstellen Sie mit der F5 BIG-IP-GUI einen bidirektionalen IPSec-Verkehrsselektor

1. **Klicken Sie auf der Registerkarte**Main**auf**Netzwerk**>**IPSec**>**Traffic Selectors**und klicken Sie dann auf Erstellen.**
2. Stellen Sie auf dem Bildschirm **New Traffic Selector** die folgenden Parameter ein:
   - **Name**. Geben Sie einen eindeutigen Namen für den Traffic Selector ein.
   - **Bestellen**. Behalten Sie den Standardwert **(First)**bei. Diese Einstellung legt die Reihenfolge fest, in der der Traffic Selector List auf dem Bildschirm mit der Verkehrsauswahlliste angezeigt wird.
3. Wählen Sie in der **Konfigurationsliste** die Option **Erweitert**aus und legen Sie die folgenden Parameter fest:
   - **Quell-IP-Adresse**. Klicken Sie auf **Host** oder **Netzwerk**und geben Sie im Feld **Adresse** die Adresse des F5-BIG-IP-Seitensubnetzes ein, dessen Datenverkehr über den IPSec-Tunnel geschützt werden soll.
   - **Quellport**. Wählen Sie *** Alle Anschlüsse**aus.
   - **Ziel-IP-Adresse**. Klicken Sie auf **Host**und geben Sie im Feld **Adresse die Adresse** des NetScaler-seitigen Subnetzes ein, dessen Datenverkehr über den IPSec-Tunnel geschützt werden soll.
   - **Zielport**. Wählen Sie *** Alle Anschlüsse**aus.
   - **Protokoll**. Wählen Sie *** Alle Protokolle**aus.
   - **Richtung**. Wählen Sie **Beides**aus.
   - **Aktion**. Wählen Sie **Schützen**aus. Die Einstellung **IPSec-Richtlinienname** wird angezeigt.
   - **Name der IPSec-Richtlinie**. Wählen Sie den Namen der benutzerdefinierten IPSec-Richtlinie aus, die Sie erstellt haben.
4. Klicken Sie auf **Fertig**.

Konfigurieren der NetScaler Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer F5 BIG-IP-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der NetScaler-Appliance aus. Sie können entweder die NetScaler-Befehlszeile oder die grafische Benutzeroberfläche (GUI) von NetScaler verwenden:

- **Erstellen Sie ein IPSec-Profil.** Eine IPSec-Profilentität gibt die IPSec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und Authentifizierungsmethode an, die vom IPSec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel, der das IPSec-Protokoll verwendet, und verknüpfen Sie das IPSec-Profil damit**. Ein IP-Tunnel gibt die lokale IP-Adresse (die auf der NetScaler-Appliance konfigurierte IP-Adresse des CloudBridge Connector-Tunnelendpunkts (vom Typ SNIP), die Remote-IP-Adresse (auf der F5 BIG-IP-Appliance konfigurierte IP-Adresse des

CloudBridge Connector-Tunnelendpunkts), das Protokoll (IPSec), das zur Einrichtung des CloudBridge Connector-Tunnels verwendet wird, und eine IPSec-Profilentität an. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.

- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität spezifiziert eine Reihe von Regeln und eine IP-Tunnelentität (CloudBridge Connector-Tunnel). Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das Netscaler-seitige Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll, und legen Sie den Ziel-IP-Adressbereich fest, um das F5-BIG-IP-Seitensubnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll.

So erstellen Sie ein IPSEC-Profil über die NetScaler Befehlszeile

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecyENABLE`
- `show ipsec profile** <name>`

Um einen IPSEC-Tunnel zu erstellen und das IPSEC-Profil mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der NetScaler-Befehlszeile daran zu binden

Geben Sie in der Befehlszeile Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

So erstellen Sie ein IPSEC-Profil mithilfe der GUI

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSecProfile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **IPSec-Profil hinzufügen** “ die folgenden Parameter ein:
    - Name
    - Verschlüsselungsalgorithmus
    - Hash-Algorithmus
    - IKE-Protokollversion

4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers verwendet wird, um sich gegenseitig zu authentifizieren: Wählen Sie die **Authentifizierungsmethode Pre-Shared Key** aus und legen Sie den Parameter **Pre-Shared** Key Exists fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um einen IP-Tunnel zu erstellen und das IPSEC-Profil mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Stellen Sie auf der Seite **IP-Tunnel hinzufügen** die folgenden Parameter ein:
    - Name
    - Remote-IP
    - Maske aus der Ferne
    - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option *Subnetz-IP*aus).
    - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
    - Protokoll
    - IPSec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der GUI daran zu binden

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **PBR erstellen** “ die folgenden Parameter ein:
    - Name
    - Aktion
    - Nächster Hop-Typ (*IP-Tunnel*auswählen)
    - Name des IP-Tunnels
    - Quell-IP Low
    - Quell-IP High
    - Ziel-IP Niedrig
    - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge Connector-Tunnels wird im Bereich Configured CloudBridge Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Mit den folgenden Befehlen werden die Einstellungen der NetScaler-Appliance NS_Appliance-1 in „Beispiel für eine CloudBridge Connector-Konfiguration“ erstellt. :


```
1      > add ipsec profile NS_F5-BIG-IP_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
          HMAC_SHA1 -lifetime 315360 -perfectForwardSecrecy ENABLE
2
3
4      Done
5
6      > add iptunnel NS_F5-BIG-IP_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 -protocol IPSEC -ipsecProfileName NS_F5-BIG-
          IP_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_F5-BIG-IP_Pbr -srcIP 10.102.147.0-10.102.147.255 -
          destIP 10.20.0.0-10.20.255.255 -ipTunnel NS_F5-BIG-IP_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Interoperabilität des CloudBridge Connector — Cisco ASA

May 11, 2023

Sie können einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer Cisco ASA-Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk auf einen Cloud-Anbieter auszudehnen. Die NetScaler-Appliance und die Cisco ASA-Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

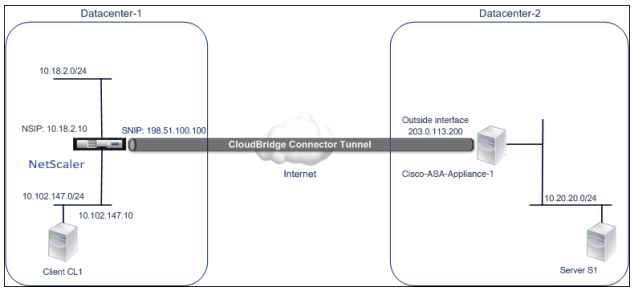
Beispiel für eine CloudBridge Connector-Tunnelkonfiguration

Betrachten Sie zur Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Appliances eingerichtet wird:

- NetScaler Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- Cisco ASA-Appliance Cisco-ASA-Appliance-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und Cisco-ASA-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und Cisco-ASA-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Auf NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPSec-Profilentität NS_Cisco-ASA_IPsec_Profile, die CloudBridge Connector-Tunnelentität NS_Cisco-ASA_Tunnel und die Policy-Based Routing (PBR) -Entität NS_Cisco-ASA_PBR.



Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie mit der Konfiguration des CloudBridge-Connector-Tunnels beginnen, stellen Sie sicher, dass:

- Die folgenden IPSec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer Cisco ASA-Appliance unterstützt.

IPsec-Eigenschaften	Einstellungen
IPSec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE-Authentifizierungsmethode	Vorab gemeinsam genutzter Schlüssel
IKE-Verschlüsselungsalgorithmus	ARSCH, 3DS

IPsec-Eigenschaften	Einstellungen
IKE-Hash-Algorithmus	HMAC SHA1, HMAC MD5
ESP-Verschlüsselungsalgorithmus	ARSCH, 3DS
ESP-Hash-Algorithmus	HMAC SHA1, HMAC MD5

- Sie müssen dieselben IPSec-Einstellungen auf der NetScaler-Appliance und der Cisco ASA-Appliance an den beiden Enden des CloudBridge Connector-Tunnels angeben.
- NetScaler stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemeinsamen Parameter für die Spezifizierung eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie in der Cisco ASA-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in IKE (Phase-1-Konfiguration) und ESP (Phase-2-Konfiguration) angeben.
- Sie müssen die Firewall am NetScaler-Ende und am Cisco ASA-Ende konfigurieren, um Folgendes zu ermöglichen.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

Konfiguration von Cisco ASA für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel auf einer Cisco ASA-Appliance zu konfigurieren, verwenden Sie die Cisco ASA-Befehlszeilenschnittstelle, die die primäre Benutzeroberfläche für die Konfiguration, Überwachung und Wartung von Cisco ASA-Appliances ist.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration auf einer Cisco ASA-Appliance beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto mit Administratoranmeldeinformationen auf der Cisco ASA-Appliance.
- Sie sind mit der Cisco ASA-Befehlszeilenschnittstelle vertraut.
- Die Cisco ASA-Appliance ist in Betrieb, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.

> **Hinweis**
>
> Die Verfahren zur Konfiguration des CloudBridge Connector-Tunnels auf einer Cisco ASA-Appliance können sich je nach Cisco-Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle Cisco ASA-Produktdokumentation zur Konfiguration von IPSec-VPN-Tunneln unter

> folgender Adresse zu befolgen:
>
> - http://www.cisco.com

Um einen CloudBridge-Connector-Tunnel zwischen einer NetScaler-Appliance und einer Cisco ASA-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben in der Befehlszeile der Cisco ASA-Appliance aus:

- **Erstellen Sie eine IKE-Richtlinie**. Eine IKE-Richtlinie definiert eine Kombination von Sicherheitsparametern, die während der IKE-Verhandlung (Phase 1) verwendet werden. In dieser Aufgabe werden beispielsweise Parameter wie Hash-Algorithmus, Verschlüsselungsalgorithmus und Authentifizierungsmethode festgelegt, die bei der IKE-Verhandlung verwendet werden sollen.
- **Aktivieren Sie IKE auf der externen Schnittstelle**. Aktivieren Sie IKE auf der externen Schnittstelle, über die der Tunnelverkehr zum Tunnel-Peer fließt.
- **Erstellen Sie eine Tunnelgruppe**. Eine Tunnelgruppe gibt den Tunneltyp und den Pre-Shared-Schlüssel an. Der Tunneltyp muss auf ipsec-l2l gesetzt sein, was für IPSec LAN to LAN steht. Ein Pre-Shared Key ist eine Textzeichenfolge, die die Peers eines CloudBridge Connector-Tunnels verwenden, um sich gegenseitig zu authentifizieren. Die Pre-Shared-Schlüssel werden für die IKE-Authentifizierung miteinander abgeglichen. Damit die Authentifizierung erfolgreich ist, müssen Sie daher denselben Pre-Shared-Schlüssel auf der Cisco ASA-Appliance und der NetScaler-Appliance konfigurieren.
- **Definieren Sie einen Transformationssatz**. Ein Transformationssatz definiert eine Kombination von Sicherheitsparametern (Phase 2), die nach erfolgreicher IKE-Verhandlung beim Datenaustausch über den CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie eine Zugriffsliste**. Krypto-Zugriffslisten werden verwendet, um die Subnetze zu definieren, deren IP-Verkehr über den CloudBridge-Tunnel geschützt wird. Die Quell- und Zielparameter in der Zugriffsliste geben die Subnetze der Cisco Appliance-Seite und der NetScaler-Seite an, die über den CloudBridge Connector-Tunnel geschützt werden sollen. Die Zugriffsliste muss auf „Zulassen“ gesetzt sein. Jedes Anforderungspaket, das von einer Appliance im Cisco-Appliance-seitigen Subnetz stammt und an eine Appliance im NetScaler-Seitensubnetz gerichtet ist und mit den Quell- und Zielparametern der Zugriffsliste übereinstimmt, wird über den CloudBridge Connector-Tunnel gesendet.
- **Erstellen Sie eine Krypto-Map**. Crypto Maps definieren die IPSec-Parameter für Sicherheitsassoziationen (SAs). Dazu gehören: Crypto-Zugriffsliste zur Identifizierung der Subnetze, deren Datenverkehr über den CloudBridge-Tunnel geschützt werden soll, Peer-Identifizierung (NetScaler) anhand der IP-Adresse und Transformationssatz, der den Peer-Sicherheitseinstellungen entspricht.
- **Wenden Sie die Crypto Map auf die externe Schnittstelle**an. In dieser Aufgabe wenden Sie die Crypto-Map auf die externe Schnittstelle an, über die der Tunnelverkehr zum Tunnel-Peer fließt. Wenn die Crypto-Map auf eine Schnittstelle angewendet wird, wird die Cisco ASA-Appliance angewiesen, den gesamten Schnittstellenverkehr anhand des Crypto-Map-Sets

auszuwerten und bei Verhandlungen über Verbindungs- oder Sicherheitszuordnungen die angegebene Richtlinie zu verwenden.

Mit den Beispielen in den folgenden Verfahren werden Einstellungen der Cisco ASA-Appliance Cisco-ASA-Appliance-1 erstellt, die im Beispiel für die Konfiguration und den Datenfluss von CloudBridge Connector verwendet werden.

So erstellen Sie eine IKE-Richtlinie mithilfe der Cisco ASA-Befehlszeile

Geben Sie an der Befehlszeile der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:

Befehl	Beispiel	Beschreibung des Befehls
Priorität der Crypto-IKEV1-Richtlinie	Cisco-ASA-Appliance-1 (Konfiguration) # Crypto IKEV1-Richtlinie 1	Rufen Sie den IKE-Richtlinienkonfigurationsmodus auf und identifizieren Sie die zu erstellende Richtlinie. (Jede Richtlinie wird anhand der von Ihnen zugewiesenen Prioritätsnummer eindeutig identifiziert.) In diesem Beispiel wird Richtlinie 1 konfiguriert.
Verschlüsselung (3des | aes)	Cisco-ASA-Appliance-1 (config-ikev1-policy) # Verschlüsselung 3des	Geben Sie den Verschlüsselungsalgorithmus an. In diesem Beispiel wird der 3DES-Algorithmus konfiguriert.
Hash (sha | md5)	Cisco-ASA-Appliance-1 (config-ikev1-policy) # hash sha	Geben Sie den Hash-Algorithmus an. In diesem Beispiel wird SHA konfiguriert.
AuthentifizierungPre-Sharing	Cisco-ASA-Appliance-1 (config- ikev1-policy) # Authentifizierung vor der Freigabe	Geben Sie die Pre-Share-Authentifizierungsmethode an.
gruppe 2	Cisco-ASA-Appliance-1 (config-ikev1-policy) # Gruppe 2	Geben Sie den 1024-Bit-Diffie-Hellman-Gruppenbezeichner (2) an.

Befehl	Beispiel	Beschreibung des Befehls
Lebenszeit Sekunden	Cisco-ASA-Appliance-1 (config-ikev1-policy) # lifetime 28800	Geben Sie die Lebensdauer der Sicherheitszuordnung in Sekunden an. In diesem Beispiel werden 28800 Sekunden konfiguriert. Dies ist der Standardwert für die Lebensdauer in einer NetScaler-Appliance.

So aktivieren Sie IKE auf der externen Schnittstelle mithilfe der Cisco ASA-Befehlszeile

Geben Sie an der Befehlszeile der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:

Befehl	Beispiel	Beschreibung des Befehls
crypto ikev1 draußen aktivieren	Cisco-ASA-Appliance-1 (config) # crypto ikev1 draußen aktivieren	Aktivieren Sie IKEv1 auf der Schnittstelle, über die der Tunnelverkehr zum Tunnel-Peer fließt. In diesem Beispiel wird IKEv1 auf der nach außen benannten Schnittstelle aktiviert.

So erstellen Sie eine Tunnelgruppe über die Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, wie in der angeschlossenen pdf Tunnel Group über die Cisco ASA-Befehlszeilegezeigt:

So erstellen Sie eine Krypto-Zugriffsliste über die Cisco ASA-Befehlszeile

Geben Sie an der Befehlszeile der Cisco ASA-Appliance den folgenden Befehl im globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
Zugriffsliste Zugriffslistennummer zulassen IP-Quelle Wildcard Ziel Wildcard	Cisco-ASA-Appliance-1 (Config) # Zugriffsliste 111 erlaubt IP 10.20.20.0 0.0.0.255 10.102.147.0 0.0.0.255	Geben Sie Bedingungen an, um die Subnetze zu bestimmen, deren IP-Verkehr über den CloudBridge Connector-Tunnel geschützt werden soll. In diesem Beispiel wird die Zugriffsliste 111 konfiguriert, um den Datenverkehr aus den Subnetzen 10.20.20.0/24 (auf der Cisco-ASA-Appliance-1-Seite) und 10.102.147.0/24 (auf der NS_Appliance-1-Seite) zu schützen.

So definieren Sie einen Transformationssatz mithilfe der Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus. Siehe Transformieren Set mit ASA-Befehlszeilentabelle pdf.

So erstellen Sie eine Kryptozuordnung über die Cisco ASA-Befehlszeile

Geben Sie an der Befehlszeile der Cisco ASA-Appliance die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
Krypto-Kartenname seq-num entspricht Adresse Zugriffslistenname	Cisco-ASA-Appliance-1 (config) # Krypto-Map NS-CISCO-CM 1 entspricht der Adresse 111	Erstellen Sie eine Krypto-Map und geben Sie eine Zugriffsliste dafür an. In diesem Beispiel wird die Crypto-Map NS-CISCO-CM mit der Sequenznummer 1 konfiguriert und NS-CISCO-CM die Zugriffsliste 111 zugewiesen.

Befehl	Beispiel	Beschreibung des Befehls
Crypto Map Kartenname seq-num setzt die Peer-IP-Adresse	Cisco-ASA-Appliance-1 (Konfiguration) # Krypto-Map NS-CISCO-CM 1 Satz Peer 198.51.100.100	Geben Sie den Peer (NetScaler Appliance) anhand seiner IP-Adresse an. In diesem Beispiel wird 198.51.100.100 angegeben, was die IP-Adresse des Tunnelendpunkts auf der NetScaler-Appliance ist.
Crypto Map Kartenname seq-num set ikev1 transform-set transform-set-name	Cisco-ASA-Appliance-1 (Konfiguration) # Krypto-Map NS-CISCO-CM 1 Satz ikev1-Transformationssatz NS-CISCO-TS	Geben Sie an, welcher Transformationssatz für diesen Crypto-Map-Eintrag zulässig ist. In diesem Beispiel wird der Transformationssatz NS-CISCO-TS spezifiziert.

So wenden Sie mithilfe der Cisco ASA-Befehlszeile eine Crypto-Map auf eine Schnittstelle an

Geben Sie an der Befehlszeile der Cisco ASA-Appliance die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
Crypto Map-Name Schnittstellenname	Cisco-ASA-Appliance-1 (config) # Crypto Map NS-CISCO-CM-Schnittstelle draußen	Wenden Sie die Crypto-Map auf die Schnittstelle an, über die der CloudBridge Connector-Tunnelverkehr fließen wird. In diesem Beispiel wird die Crypto-Map NS-CISCO-CM auf die externe Schnittstelle angewendet.

Konfigurieren der NetScaler Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer NetScaler-Appliance und einer Cisco ASA-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der NetScaler-Appliance aus. Sie können entweder die NetScaler-Befehlszeile oder die grafische Benutzeroberfläche (GUI) von

NetScaler verwenden:

- Erstellen Sie ein IPSec-Profil.
- Erstellen Sie einen IP-Tunnel, der das IPSec-Protokoll verwendet, und verknüpfen Sie das IPSec-Profil damit.
- Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel.

So erstellen Sie ein IPSEC-Profil mithilfe der NetScaler-Befehlszeile:

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

Gehen Sie wie folgt vor, um einen IPSEC-Tunnel zu erstellen und das IPSEC-Profil mithilfe der NetScaler-Befehlszeile daran zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

Gehen Sie wie folgt vor, um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der NetScaler-Befehlszeile daran zu binden:

Geben Sie in der Befehlszeile Folgendes ein:

- `**add pbr** <pbrName> **ALLOW** -**srcIP** <subnet-range> -**destIP** <subnet-range>`
- `**ipTunnel** <tunnelName>`
- `**apply pbrs**`
- `**show pbr** <pbrName>`

Um ein IPSEC-Profil mithilfe der GUI zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **IPSec-Profil hinzufügen** “ die folgenden Parameter ein:
    - Name
    - Verschlüsselungsalgorithmus
    - Hash-Algorithmus
    - IKE-Protokollversion
    - Perfect Forward Secrecy (Aktivieren Sie diesen Parameter)
4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers verwendet wird, um sich gegenseitig zu authentifizieren: Wählen

Sie die **Authentifizierungsmethode Pre-Shared Key** aus und legen Sie den Parameter **Pre-Shared** Key Exists fest.

5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um einen IP-Tunnel zu erstellen und das IPSEC-Profil mithilfe der GUI daran zu binden, gehen Sie wie folgt vor:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der **Registerkarte IPv4-Tunnel**auf **Hinzufügen**.
3. Stellen Sie auf der Seite **IP-Tunnel hinzufügen** die folgenden Parameter ein:
   - Name
   - Remote-IP
   - Maske aus der Ferne
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option Subnetz-IPaus).
   - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPSec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Um eine PBR-Regel zu erstellen und den IPSEC-Tunnel mithilfe der GUI daran zu binden, gehen Sie wie folgt vor:

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Legen Sie auf der Seite **PBRerstellen** die folgenden Parameter fest:
   - Name
   - Aktion
   - Nächster Hop-Typ (IP-Tunnelauswählen)
   - Name des IP-Tunnels
   - Quell-IP Low
   - Quell-IP High
   - Ziel-IP Niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der NetScaler-Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge Connector-Tunnels wird im Bereich Configured CloudBridge Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Mit den folgenden Befehlen werden die Einstellungen der NetScaler-Appliance NS_Appliance-1 in „Beispiel für eine CloudBridge Connector-Konfiguration“ erstellt. „:


```
> add ipsec profile NS_Cisco-ASA_IPSec_Profile -psk
   examplepresharedkey -ikeVersion v1 -encAlgo AES -hashalgo
   HMAC_SHA1 -lifetime 315360 -perfectForwardSecrecy ENABLE

Done

> add iptunnel NS_Cisco-ASA_Tunnel 203.0.113.200 255.255.255.255
   198.51.100.100 -protocol IPSEC -ipsecProfileName NS_Cisco-
   ASA_IPSec_Profile


Done

> add pbr NS_Cisco-ASA_Pbr -srcIP 10.102.147.0-10.102.147.255 -destIP
   10.20.0.0-10.20.255.255 -ipTunnel NS_Cisco-ASA_Tunnel


Done

> apply pbrs

Done

<!--NeedCopy-->
```

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer NetScaler Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer NetScaler Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Hohe Verfügbarkeit

May 11, 2023

Eine Hochverfügbarkeitsbereitstellung (HA) von zwei NetScaler-Appliances kann einen unterbrechungsfreien Betrieb bei jeder Transaktion gewährleisten. Wenn eine Appliance als primärer Knoten und die andere als sekundärer Knoten konfiguriert ist, akzeptiert der primäre Knoten Verbindungen und verwaltet Server, während der sekundäre Knoten den primären Knoten

überwacht. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Kontrolle.

Der sekundäre Knoten überwacht den primären Knoten, indem er regelmäßige Nachrichten (oft als Heartbeat-Nachrichten oder Zustandsprüfungen bezeichnet) sendet, um festzustellen, ob der primäre Knoten Verbindungen akzeptiert. Wenn eine Integritätsüberprüfung fehlschlägt, versucht der sekundäre Knoten die Verbindung für einen bestimmten Zeitraum erneut, woraufhin festgestellt wird, dass der primäre Knoten nicht normal funktioniert. Der sekundäre Knoten übernimmt dann die primäre (ein Prozess, der als Failover bezeichnet wird).

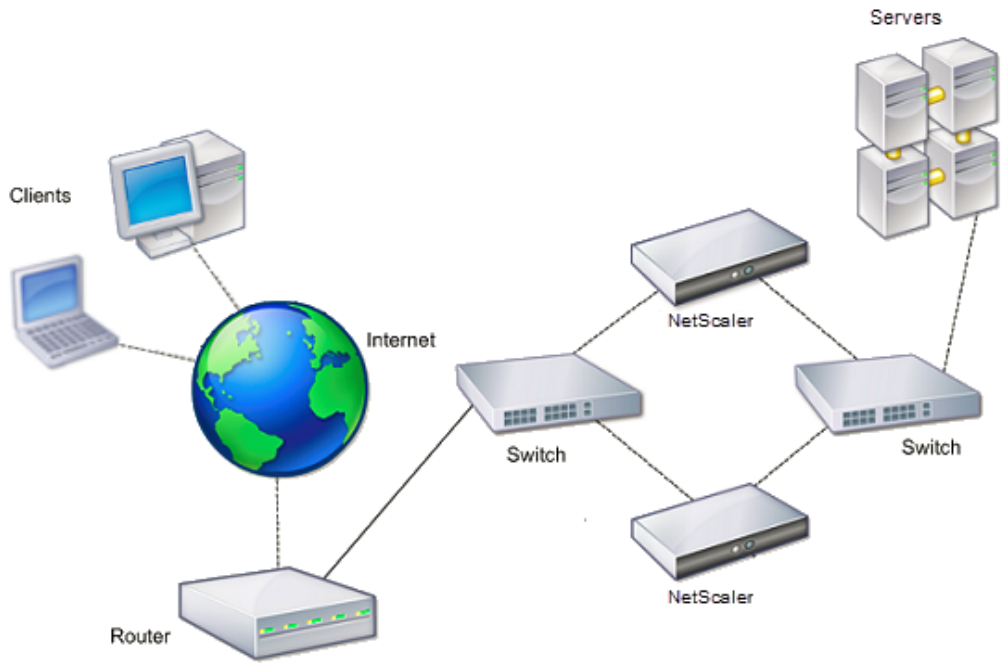
Nach einem Failover müssen alle Clients ihre Verbindungen zu den verwalteten Servern wiederherstellen, aber die Regeln für die Sitzungspersistenz werden wie vor dem Failover beibehalten.

Wenn die Webserver-Protokollierungspersistenz aktiviert ist, gehen aufgrund des Failovers keine Protokolldaten verloren. Damit die Protokollierungspersistenz aktiviert wird, muss die Konfiguration des Protokollservers Einträge für beide Systeme in der Datei log.conf enthalten.

> **Hinweis:**
>
> In einigen Fällen wird der primäre Knoten als Proxy für den sekundären Knoten verwendet.

Die folgende Abbildung zeigt eine Netzwerkkonfiguration mit einem HA-Paar.

Abbildung 1. NetScaler-Appliances in einer Hochverfügbarkeitskonfiguration



Um HA zu konfigurieren, sollten Sie zunächst ein Basis-Setup erstellen, bei dem sich beide Knoten im

selben Subnetz befinden. Anschließend können Sie die Intervalle, in denen die Knoten Informationen zur Integritätsprüfung übermitteln, den Prozess, mit dem Knoten die Synchronisation aufrechterhalten, und die Weitergabe von Befehlen vom primären zum sekundären Knoten anpassen. Sie können den Failsafe-Modus konfigurieren, um zu verhindern, dass keiner der Knoten primär ist. Wenn Ihre Umgebung Geräte enthält, die keine kostenlosen ARP-Nachrichten von NetScaler akzeptieren, sollten Sie virtuelle MAC-Adressen konfigurieren. Wenn Sie für eine komplexere Konfiguration bereit sind, können Sie HA-Knoten in verschiedenen Subnetzen konfigurieren.

Um die Zuverlässigkeit Ihres HA-Setups zu verbessern, können Sie Routenmonitore konfigurieren und redundante Links erstellen. In einigen Situationen, z. B. bei der Fehlerbehebung oder Durchführung von Wartungsaufgaben, möchten Sie möglicherweise einen Knoten zum Failover zwingen (dem anderen Knoten den Primärstatus zuweisen), oder Sie möchten den sekundären Knoten zwingen, sekundär zu bleiben oder der primäre Knoten primär zu bleiben.

Punkte, die bei einem Hochverfügbarkeits-Setup zu beachten sind

June 19, 2023

> **Hinweis**
>
> Die folgenden Anforderungen für die Konfiguration von Systemen in einem HA-Setup:

- In einer HA-Konfiguration müssen die primären und sekundären NetScaler-Appliances vom gleichen Modell sein. Verschiedene NetScaler Modelle werden in einem HA-Paar nicht unterstützt. Außerdem werden NetScaler-VPXs, die auf verschiedenen -Modellen bereitgestellt werden, in einem HA-Paar nicht unterstützt. Nur NetScaler VPXs, die auf demselben -Modell bereitgestellt werden, können ein HA-Paar bilden.
- In einem HA-Setup müssen beide Knoten dieselbe Version von NetScaler ausführen.
- Einträge in der Konfigurationsdatei (ns.conf) auf dem primären und dem sekundären System müssen übereinstimmen, mit den folgenden Ausnahmen:
  - Das primäre und das sekundäre System müssen jeweils mit ihren eigenen eindeutigen IP-Adressen (NSIPs) konfiguriert werden.
  - In einem HA-Paar müssen die Knoten-ID und die zugehörige IP-Adresse eines Knotens auf den anderen Knoten verweisen. Wenn Sie beispielsweise die Knoten NS1 und NS2 haben, müssen Sie NS1 mit einer eindeutigen Knoten-ID und der IP-Adresse von NS2 konfigurieren, und Sie müssen NS2 mit einer eindeutigen Knoten-ID und der IP-Adresse von NS1 konfigurieren.
- Wenn Sie eine Konfigurationsdatei auf einem der Knoten mithilfe einer Methode erstellen, die nicht direkt über die GUI oder die CLI erfolgt (z. B. SSL-Zertifikate importieren oder zu Start-

skripten wechseln), müssen Sie die Konfigurationsdatei auf den anderen Knoten kopieren oder eine identische Datei auf diesem Knoten erstellen.

- Anfänglich werden alle NetScaler-Appliances mit demselben RPC-Knotenkennwort konfiguriert. RPC-Knoten sind interne Systementitäten, die für die System-zu-System-Kommunikation von Konfigurations- und Sitzungsinformationen verwendet werden. Aus Sicherheitsgründen sollten Sie die Standard-RPC-Knotenkennwörter ändern.

  Auf jedem NetScaler ist ein RPC-Knoten vorhanden. Dieser Knoten speichert das Kennwort, das mit dem vom Kontaktsystem bereitgestellten Kennwort verglichen wird. Um mit anderen Systemen kommunizieren zu können, benötigt jeder NetScaler Kenntnisse über diese Systeme, einschließlich der Authentifizierung auf diesen Systemen. RPC-Knoten verwalten diese Informationen, einschließlich der IP-Adressen der anderen Systeme und der Kennwörter, die sie für die Authentifizierung benötigen.

  RPC-Knoten werden implizit erstellt, wenn ein Knoten hinzugefügt oder eine Global Server Load Balancing (GSLB) -Site hinzugefügt wird. Sie können RPC-Knoten nicht manuell erstellen oder löschen.

  > **Hinweis**:
  >
  > Wenn die NetScaler-Appliances in einem Hochverfügbarkeits-Setup im einarmigen Modus konfiguriert sind, müssen Sie alle Systemschnittstellen außer der mit dem Switch oder Hub verbundenen deaktivieren.

  Für eine IPv6-HA-Konfiguration gelten die folgenden Überlegungen:

  - Sie müssen die IPv6PT-Lizenz auf beiden NetScaler-Appliances installieren.
  - Nach der Installation der IPv6PT-Lizenz aktivieren Sie die IPv6-Funktion mithilfe der GUI oder der Befehlszeilenschnittstelle.
  - Beide NetScaler-Appliances benötigen eine globale NSIP-IPv6-Adresse. Darüber hinaus müssen Netzwerkentitäten (z. B. Switches und Router) zwischen den beiden Knoten IPv6 unterstützen.

Konfiguration der Hochverfügbarkeit

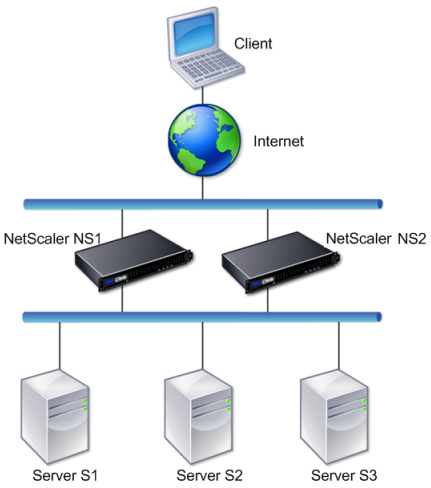
May 11, 2023

Um eine Hochverfügbarkeitskonfiguration einzurichten, erstellen Sie zwei Knoten, von denen jeder die NetScaler IP (NSIP) -Adresse des anderen als Remoteknoten definiert. Melden Sie sich zunächst bei einer der beiden NetScaler Appliances an, die Sie für Hochverfügbarkeit konfigurieren möchten, und fügen Sie einen Knoten hinzu. Geben Sie die NetScaler IP (NSIP) -Adresse der anderen Appliance als Adresse des neuen Knotens an. Melden Sie sich dann bei der anderen Appliance an und fügen Sie

einen Knoten hinzu, der die NSIP-Adresse der ersten Appliance enthält. Ein Algorithmus bestimmt, welcher Knoten primär und welcher sekundär wird.

Die folgende Abbildung zeigt ein einfaches HA-Setup, bei dem sich beide Knoten im selben Subnetz befinden.

Abbildung 1. Zwei NetScaler Appliances in einer Hochverfügbarkeitskonfiguration angeschlossen



Schritte zur Konfiguration der Hochverfügbarkeit

Das Einrichten eines Hochverfügbarkeitspaars aus zwei NetScaler-Appliances besteht aus den folgenden Aufgaben auf beiden Appliances:

- **Fügen Sie einen Knoten hinzu**. Fügen Sie auf einer Appliance, sagen wir N1, die andere Appliance hinzu, sagen wir N2, indem Sie eine eindeutige Knoten-ID und die NSIP-Adresse der Appliance (N2) angeben. Sie können eine beliebige Ganzzahl im Bereich von 1 bis 64 für die Peer-Knoten-ID angeben.

  Die auf dem Selbstknoten angegebene Peer-Knoten-ID gilt nur für den Eigenknoten und hat keine Relevanz für den Peer-Knoten. Sie haben beispielsweise N2 als Peer-Knoten auf N1 hinzugefügt und die Knoten-ID als 33 für N2 angegeben. Die Node-ID-Einstellung von N2 auf 33 gilt nur für N1 und hat keine Auswirkung auf die Konfiguration von N2.

  Die auf beiden Knoten angegebene Peer-Knoten-ID muss nicht denselben Wert haben und kann geändert werden. Auf beiden Knoten ist die Eigenknoten-ID fest auf Null codiert und kann nicht geändert werden.

- **Deaktivieren Sie den HA-Monitor für ungenutzte Schnittstellen**. Auf dem Selbstknoten müssen Sie den HA-Monitor für jede Schnittstelle deaktivieren, die nicht verbunden ist oder

nicht für den Datenverkehr verwendet wird. Durch das Deaktivieren des HA-Monitors für unbenutzte Schnittstellen werden HA-Failover verhindert, die verursacht werden, wenn der Status einer dieser ungenutzten Schnittstellen DOWN wird.

> **Hinweis**:
>
> Um sicherzustellen, dass jeder Knoten in der Hochverfügbarkeitskonfiguration dieselben Einstellungen hat, müssen Sie Ihre SSL-Zertifikate, Startskripts und andere Konfigurationsdateien mit denen auf dem primären Knoten synchronisieren.

CLI-Verfahren

Um ein Hochverfügbarkeitspaar aus zwei NetScaler-Appliances mithilfe der CLI einzurichten, führen Sie die folgenden Aufgaben auf jeder der beiden Appliances aus:

So fügen Sie einen Knoten mithilfe der CLI hinzu:

Geben Sie in der Befehlszeile Folgendes ein:

- `add ha node <id> <IPAddress>`
- `show ha node`

So deaktivieren Sie den HA-Monitor für eine unbenutzte Schnittstelle mithilfe der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- `set interface <ifNum> [-haMonitor ( ON | OFF )]`
- `show interface <ifNum>`

Beispiel:

```
> add ha node 33 203.0.113.33

> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

GUI-Prozedur

Die NetScaler GUI bietet einen Bildschirm, der die Aufgaben des Hinzufügens eines Peer-Knotens sowie des Deaktivierens des HA-Monitors an ungenutzten Schnittstellen auf dem Selbstknoten kombiniert. Der Bildschirm bietet auch eine Option zur automatischen Konfiguration des Peer-Knotens für das HA-Setup, sodass der Peer-Knoten nicht manuell konfiguriert werden muss.

So richten Sie ein hochverfügbares Paar aus zwei NetScaler-Appliances mithilfe der GUI ein:

1. Melden Sie sich an der GUI einer der Appliances an.

2. Navigieren Sie zu **System** > **Hohe Verfügbarkeit** > **Knoten** und geben Sie die NSIP-Adresse des Peer-Knotens in das Feld **Remote Node IP Address** ein.
3. Wählen Sie die Option **Turn Off HA Monitor interface/channels that are down**.
4. Wählen Sie **Configure remote system to participate High Availability setup**, und geben Sie die Anmeldeinformationen des Peer-Knotens ein.
5. Klicken Sie auf **Erstellen**.

Deaktivieren oder Aktivieren eines Nodes

Sie können nur einen sekundären Knoten deaktivieren oder aktivieren. Wenn Sie einen sekundären Knoten deaktivieren, sendet er keine Heartbeat-Nachrichten mehr an den primären Knoten, sodass der primäre Knoten den Status des sekundären Knotens nicht mehr überprüfen kann. Wenn Sie einen Knoten aktivieren, nimmt der Knoten an der Hochverfügbarkeitskonfiguration teil.

So deaktivieren oder aktivieren Sie einen Knoten mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set ha node -hastatus DISABLED`
- `set ha node -hastatus ENABLED`

So deaktivieren oder aktivieren Sie einen Knoten mithilfe der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Wählen Sie in der Liste **Hochverfügbarkeitsstatus** die **Option AKTIVIERT (aktiv an HA teilnehmen)** oder **DEAKTIVIERT (Nicht an HA teilnehmen)**aus.

Konfiguration der Kommunikationsintervalle

March 10, 2023

Das Hallo-Intervall ist das Intervall, in dem die Heartbeat-Nachrichten an den Peer-Knoten gesendet werden. Das tote Intervall ist das Zeitintervall, nach dem der Peer-Knoten als DOWN markiert wird, wenn Heartbeat-Pakete nicht empfangen werden. Die Heartbeat-Nachrichten sind UDP-Pakete, die an Port 3003 des anderen Knotens in einem HA-Paar gesendet werden. Das Totintervall muss als Vielfaches des Hello-Intervalls festgelegt werden. Standardmäßig ist das Hello-Intervall auf 200 Millisekunden und das Tot-Intervall auf 3 Sekunden festgelegt.

So legen Sie die Hello- und Dead-Intervalle mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

- `set HA node [-helloInterval <msecs>] [-deadInterval <secs>]`
- `show HA node <id>`

So legen Sie die Hallo- und Dead-Intervalle mit der GUI fest

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Legen Sie die folgenden Parameter fest:
   - Hello Interval (ms)
   - Dead Interval (Sekunden)

Synchronisation konfigurieren

September 18, 2023

Bei der Synchronisation wird die Konfiguration des primären Knotens auf dem sekundären Knoten dupliziert. Der Zweck der Synchronisation besteht darin, sicherzustellen, dass unabhängig von der Anzahl der auftretenden Failovers keine Konfigurationsinformationen zwischen dem primären und dem sekundären Knoten verloren gehen. Die Synchronisation verwendet den UDP-Port 3010.

Die Synchronisation wird durch einen der folgenden Umstände ausgelöst:

- Der sekundäre Knoten in einem HA-Setup wird nach einem Neustart aktiviert.
- Der primäre Knoten wird nach einem Failover sekundär.

Die automatische Synchronisation ist standardmäßig aktiviert. Sie können auch die Synchronisierung erzwingen.

> **Hinweis:**
>
> - Die Befehlsweiterleitung ist während der HA-Synchronisierung deaktiviert, um widersprüchliche Befehlseinstellungen zu verhindern, die zu einem Ausfall der Befehlsweiterleitung führen können.
> - Während einer HA-Synchronisierung führt der sekundäre Knoten den `clear ns config` Befehl aus, um die bestehende Konfiguration zu löschen und die neue Konfiguration zu laden, die vom primären Knoten abgerufen wurde. Die klare Konfiguration entfernt jedoch nicht die statische Standardroute, die im sekundären Knoten konfiguriert ist. Wenn diese

> statische Standardroute auf ein falsches Gateway verweist, kann dies zu Ausfallzeiten der Dienste führen.

Synchronisation deaktivieren oder aktivieren

Die automatische HA-Synchronisierung ist standardmäßig auf jedem Knoten in einem HA-Paar aktiviert. Sie können es auf jedem Knoten aktivieren oder deaktivieren.

So deaktivieren oder aktivieren Sie die automatische Synchronisation mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile Folgendes ein:

- `set HA node -haSync DISABLED`
- `set HA node -haSync ENABLED`

So deaktivieren oder aktivieren Sie die Synchronisation mithilfe der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Deaktivieren oder wählen Sie unter HA-Synchronisierung die Option Sekundärer Knoten, um die Konfiguration von der Option Primär abzurufen.

Erzwingen der Synchronisation des sekundären Knotens mit dem primären Knoten

Zusätzlich zur automatischen Synchronisation unterstützt der NetScaler die erzwungene Synchronisation. Sie können die Synchronisation entweder vom primären oder vom sekundären Knoten aus erzwingen. Wenn Sie die Synchronisation vom sekundären Knoten aus erzwingen, beginnt dieser, seine Konfiguration mit dem primären Knoten zu synchronisieren.

Wenn die Synchronisation jedoch bereits läuft, schlägt die erzwungene Synchronisation fehl und das System zeigt eine Warnung an. Die erzwungene Synchronisation schlägt auch unter den folgenden Umständen fehl:

- Sie erzwingen die Synchronisierung auf einem eigenständigen System.
- Der sekundäre Knoten ist deaktiviert.
- Die HA-Synchronisierung ist auf dem sekundären Knoten deaktiviert.

So erzwingen Sie die Synchronisation mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile Folgendes ein:

```
force HA sync
```


Um die Synchronisation mithilfe der GUI zu erzwingen

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Klicken Sie auf der Registerkarte **Knoten** in der Aktionsliste auf **Synchronisation erzwingen**.

Synchronisieren von Konfigurationsdateien in einer Hochverfügbarkeitseinrichtung

October 8, 2021

In einem Hochverfügbarkeits-Setup werden alle Konfigurationsdateien im Abstand von einer Minute automatisch vom primären Knoten zum sekundären Knoten synchronisiert. Die Synchronisierung von Konfigurationsdateien kann manuell über die Befehlszeile oder der GUI am primären oder sekundären Knoten durchgeführt werden.

Dateien auf der Sekundärseite, die sekundär spezifisch sind (nicht auf der Primärseite vorhanden), werden während der Synchronisierung nicht gelöscht.

So synchronisieren Sie Dateien in einem Hochverfügbarkeits-Setup über die Befehlszeile

Geben Sie an der Eingabeaufforderung ein:

```
sync HA files <mode>
```

Beispiel

```
1 > sync HA files all
2  Done
3 <!--NeedCopy-->
```

```
1 > sync HA files ssl
2  Done
3 <!--NeedCopy-->
```

Parameterbeschreibungen (des in der CLI-Prozedur aufgeführten Befehls)

```
sync ha files <mode>
```

```
mode
```

Geben Sie einen der folgenden Synchronisationsmodi an.

- **all** - Synchronisieren Sie Dateien im Zusammenhang mit der Systemkonfiguration, Access Gateway-Lesezeichen, SSL-Zertifikaten, SSL-CRL-Listen und Anwendungsfirewall-XML-Objekten.
- **Lesezeichen** - Synchronisiert alle Access Gateway-Lesezeichen.
- **ssl** - Synchronisiert alle Zertifikate, Schlüssel und CRLs für die SSL-Funktion.
- **Importe** - Synchronisieren Sie alle für die Anwendungsfirewall konfigurierten XML-Objekte (z. B. WSDLs, Schemas, Fehlerseiten).
- **misc** - Synchronisiert alle Lizenzdateien und die Datei rc.conf.
- **all_plus_misc** - Synchronisiert Dateien im Zusammenhang mit der Systemkonfiguration, Access Gateway-Lesezeichen, SSL-Zertifikaten, SSL-CRL-Listen, XML-Objekten der Anwendungsfirewall, Lizenzen und der Datei rc.conf.

So synchronisieren Sie Dateien in einem Hochverfügbarkeits-Setup über die GUI

Navigieren Sie zu **System** > **Diagnose** und klicken Sie in der Gruppe **Dienstprogramme** auf **HA-Dateisynchronisierung starten**.

Konfigurieren der Befehlsausbreitung

August 4, 2023

In einem HA-Setup wird jeder Befehl, der auf dem primären Knoten ausgegeben wird, automatisch an den sekundären Knoten weitergegeben und dort ausgeführt, bevor er auf dem primären Knoten ausgeführt wird. Wenn die Befehlsweiterleitung fehlschlägt oder die Befehlsausführung auf dem sekundären Knoten fehlschlägt, führt der primäre Knoten den Befehl aus und protokolliert einen Fehler. Die Befehlsausbreitung verwendet Port 3010.

In einer HA-Paarkonfiguration ist die Befehlsweiterleitung standardmäßig sowohl auf dem primären als auch auf dem sekundären Knoten aktiviert. Sie können die Befehlsweiterleitung auf jedem Knoten in einem HA-Paar aktivieren oder deaktivieren. Wenn Sie die Befehlsübertragung auf dem primären Knoten deaktivieren, werden Befehle nicht an den sekundären Knoten weitergegeben. Wenn Sie die Befehlsweiterleitung auf dem sekundären Knoten deaktivieren, werden Befehle, die vom primären Knoten weitergegeben werden, nicht auf dem sekundären Knoten ausgeführt.

> **Hinweis**
>
> Denken Sie nach dem erneuten Aktivieren der Propagierung daran, die Synchronisation zu erzwingen.

Wenn die Synchronisation stattfindet, während Sie die Propagierung deaktivieren, werden alle konfigurationsbezogenen Änderungen, die Sie vornehmen, bevor die Deaktivierung der Propagierung wirk-

sam wird, mit dem sekundären Knoten synchronisiert. Dies gilt auch für Fälle, in denen die Weitergabe deaktiviert ist, während die Synchronisation läuft.

So deaktivieren oder aktivieren Sie die Befehlsweiterleitung mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- setze den HA-Knoten -HAProp DISABLED
- setze den HA-Knoten -HAProp AKTIVIERT

So deaktivieren oder aktivieren Sie die Befehlsweiterleitung mit der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Deaktivieren oder wählen Sie den Primärknoten, der die Konfiguration an die Option Sekundär weitergibt.

> **Hinweis:**
>
> Die Befehlsweiterleitung ist während der HA-Synchronisierung deaktiviert, um widersprüchliche Befehlseinstellungen zu verhindern, die zu einem Ausfall der Befehlsweiterleitung führen können.

Beschränkung des Synchronisationsverkehrs mit hoher Verfügbarkeit auf ein VLAN

May 11, 2023

Bei einer Bereitstellung mit hoher Verfügbarkeit (HA) fließt der Datenverkehr im Zusammenhang mit der Aufrechterhaltung der HA-Konfiguration zwischen den beiden HA-Knoten. Dieser Verkehr ist von den folgenden Typen:

- Config-Synchronisierung
- Weitergabe der Konfiguration
- Spiegelung von Verbindungen
- Load Balancing-Persistenz, Konfigurationssynchronisierung
- Persistente Sitzungssynchronisierung
- Synchronisation des Sitzungsstatus

Ein ordnungsgemäßer Fluss dieses HA-bezogenen Datenverkehrs zwischen den beiden Knoten ist für das Funktionieren der HA-Bereitstellung von entscheidender Bedeutung. In der Regel ist das Volumen des HA-bezogenen Datenverkehrs gering, kann aber bei einem Failover sehr hoch werden. Sie wird sehr hoch, wenn das Failover für Stateful-Verbindungen aktiviert ist und der Knoten, der vor dem Failover primär war, eine große Anzahl von Verbindungen verarbeitet hat.

Standardmäßig fließt der HA-bezogene Datenverkehr durch die VLANs, an die die NSIP-Adresse gebunden ist. Um einem möglichen Anstieg dieses Datenverkehrs Rechnung zu tragen, können Sie den HA-bezogenen Datenverkehr vom Verwaltungsdatenverkehr trennen und seinen Fluss auf ein separates VLAN beschränken. Dieses VLAN wird als HA SYNC-VLAN bezeichnet.

Punkte, die vor der Konfiguration eines HA SYNC-VLAN zu beachten sind

- Die Konfiguration eines HA SYNC VLAN wird weder propagiert noch synchronisiert. Mit anderen Worten, das HA SYNC VLAN ist knotenspezifisch und wird unabhängig auf jedem Knoten konfiguriert.
- HA SYNC VLAN-Konfiguration wird entfernt, wenn Sie die Konfiguration nur im FULL-Modus löschen.
- HA MON muss für Schnittstellen, die Teil des HA SYNC-VLAN sind, auf OFF gesetzt werden, um eine Situation zu vermeiden, in der beide Knoten als primärer Knoten fungieren.
- Verwaltungsschnittstellen (z. B. 0/1 und 0/2) dürfen nicht Teil des HA SYNC-VLAN sein, damit HA-bezogener Datenverkehr nicht über die Verwaltungsschnittstellen fließt.
- Citrix empfiehlt, Heartbeat-Meldungen mit hoher Verfügbarkeit auf Verwaltungsschnittstellen zu deaktivieren und auf HA SYNC-VLAN-Schnittstellen zu aktivieren. Nachdem diese Empfehlungen erfüllt wurden, können Hochverfügbarkeits-Heartbeat-Meldungen auch auf Datenschnittstellen aktiviert werden.

  Weitere Informationen zum Deaktivieren von Heartbeat-Nachrichten mit hoher Verfügbarkeit auf Schnittstellen finden Sie unter Verwalten von Heartbeat-Nachrichten mit hoher Verfügbarkeit auf einer NetScaler Appliance.

Um ein HA-SYNC-VLAN auf einem NetScaler Knoten zu konfigurieren, geben Sie ein konfiguriertes VLAN mit dem HA SYNC-VLAN-Parameter der lokalen Knotenentität an.

So konfigurieren Sie ein HA SYNC-VLAN auf einem lokalen Knoten über die Befehlszeile:

Geben Sie in der Befehlszeile Folgendes ein:

- `set ha node -syncvlan <VLANID>`
- `show node`

Beschreibung des Parameters:

syncvlan (Sync VLAN) - VLAN, auf das HA-bezogener Datenverkehr gesendet wird. Dies umfasst Datenverkehr für Synchronisation, Propagierung, Verbindungsspiegelung, Load Balancing-Persistenz, Konfigurationssynchronisation, persistente Sitzungssynchronisation und Synchronisation des Sitzungsstatus. HA Heartbeats können jedoch jede Schnittstelle verwenden.

So konfigurieren Sie ein HA SYNC-VLAN auf einem Knoten mit der GUI:

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Legen Sie den **Sync-VLAN-Parameter** fest, während Sie den lokalen Knoten ändern.

Konfigurieren des ausfallsicheren Modus

January 19, 2021

In einer HA-Konfiguration stellt der ausfallsichere Modus sicher, dass ein Knoten immer primär ist, wenn beide Knoten die Zustandsprüfung fehlschlagen. Damit soll sichergestellt werden, dass, wenn ein Knoten nur teilweise verfügbar ist, Backupmethoden aktiviert sind, um den Datenverkehr so gut wie möglich zu verarbeiten. Der HA-Ausfallsicheremodus wird unabhängig auf jedem Knoten konfiguriert.

Die folgende Tabelle zeigt einige der ausfallsicheren Fälle. Der Status NOT_UP bedeutet, dass der Knoten die Zustandsprüfung fehlgeschlagen ist, aber er ist teilweise verfügbar. Der UP Status bedeutet, dass der Knoten die Integritätsprüfung bestanden hat.

Knoten A (primärer) Integritätsstatus	Knoten B (sekundärer) Integritätsstatus	Standard-HA-Verhalten	Fail-Safe aktiviertes HA-Verhalten	Beschreibung
NOT_UP (zuletzt fehlgeschlagen)	NOT_UP (zuerst fehlgeschlagen)	A (Sekundär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn beide Knoten fehlschlagen, bleibt der Knoten, der der letzte primäre Knoten war, primär.

Knoten A (primärer) Integritätsstatus	Knoten B (sekundärer) Integritätsstatus	Standard-HA-Verhalten	Fail-Safe aktiviertes HA-Verhalten	Beschreibung
NOT_UP (zuerst fehlgeschlagen)	NOT_UP (zuletzt fehlgeschlagen)	A (Sekundär), B (Sekundär)	A (Sekundär), B (Primär)	Wenn beide Knoten fehlschlagen, bleibt der Knoten, der der letzte primäre Knoten war, primär.
BEREIT	BEREIT	A (Primär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn beide Knoten die Integritätsprüfung bestehen, keine Änderung des Verhaltens mit aktivierter Fail-Safe.
BEREIT	NOT_UP	A (Primär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn nur der sekundäre Knoten ausfällt, ändert sich das Verhalten bei aktivierter Fail-Safe nicht.
NOT_UP	BEREIT	A (Sekundär), B (Primär)	A (Sekundär), B (Primär)	Wenn nur der primäre Fehler auftritt, keine Änderung des Verhaltens mit aktivierter Fail-Safe.

Knoten A (primärer) Integritätsstatus	Knoten B (sekundärer) Integritätsstatus	Standard-HA-Verhalten	Fail-Safe aktiviertes HA-Verhalten	Beschreibung
NOT_UP	UP (STAYSEC-ONDARY)	A (Sekundär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn der sekundäre als STAYSEC-ONDARY konfiguriert ist, bleibt der primäre Primärserver auch dann primär, wenn er fehlschlägt.

So aktivieren Sie den ausfallsicheren Modus mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set HA node [-failSafe ( **ON** | **OFF** )]
```

Beispiel

```
1 set ha node -failsafe ON
2 <!--NeedCopy-->
```

So aktivieren Sie den ausfallsicheren Modus mit der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Wählen Sie unter **Fehlerabgesicherter Modus**die Option **Einen primären Knoten pflegen**, auch wenn beide Knoten fehlerhaft sind.

Virtueller MAC-Adressen konfigurieren

May 11, 2023

Eine virtuelle MAC-Adresse ist eine Floating-Entität, die von den primären und sekundären Knoten in einem HA-Setup gemeinsam genutzt wird.

In einem HA-Setup besitzt der primäre Knoten alle Floating-IP, wie MIPs, SNIPs und VIPs. Der primäre Knoten reagiert auf Anfragen des Address Resolution Protocol (ARP) für diese IP-Adressen mit einer eigenen MAC-Adresse. Infolgedessen wird die ARP-Tabelle eines externen Geräts (z. B. eines Upstream-Routers) mit der Floating-IP und der MAC-Adresse des primären Knotens aktualisiert.

Wenn ein Failover auftritt, übernimmt der sekundäre Knoten den neuen primären Knoten. Anschließend verwendet es Gratuitous ARP (GARP), um die Floating-IP anzukündigen, die es vom primären System erworben hat. Die MAC-Adresse, die der neue Primärserver ankündigt, ist jedoch die MAC-Adresse seiner eigenen Schnittstelle.

Einige Geräte (insbesondere einige Router) akzeptieren die von der NetScaler-Appliance generierten GARP-Nachrichten nicht. Daher behalten einige externe Geräte die alte Zuordnung von IP zu MAC bei, die vom alten primären Knoten angekündigt wurde. Dies kann dazu führen, dass eine Website ausfällt.

Sie können dieses Problem lösen, indem Sie einen virtuellen MAC auf beiden Knoten eines HA-Paares konfigurieren. Beide Knoten besitzen dann identische MAC-Adressen. Daher bleibt die MAC-Adresse des sekundären Knotens bei einem Failover unverändert, und die ARP-Tabellen auf den externen Geräten müssen nicht aktualisiert werden.

Um einen virtuellen MAC zu erstellen, müssen Sie zunächst eine Virtual Router ID (VRID) erstellen und sie an eine Schnittstelle binden. (In einem HA-Setup müssen Sie die VRID an die Schnittstellen auf beiden Knoten binden.) Sobald die VRID an eine Schnittstelle gebunden ist, generiert das System einen virtuellen MAC mit der VRID als letztes Oktett.

Dieser Abschnitt enthält die folgenden Details:

- Konfiguration virtueller IPv4-MACs
- Konfiguration virtueller IPv6-MAC6s

Konfiguration virtueller IPv4-MACs

Wenn Sie eine virtuelle IPv4-MAC-Adresse erstellen und an eine Schnittstelle binden, verwendet jedes IPv4-Paket, das von der Schnittstelle gesendet wird, die virtuelle MAC-Adresse, die an die Schnittstelle gebunden ist. Wenn kein virtueller IPv4-MAC an eine Schnittstelle gebunden ist, wird die physische MAC-Adresse der Schnittstelle verwendet.

Der generische virtuelle MAC hat das Formular `00:00:5e:00:01:<VRID>`. Wenn Sie beispielsweise eine VRID mit einem Wert von 60 erstellen und sie an eine Schnittstelle binden, ist der resultierende virtuelle MAC 00:00:5 e: 00:01:3 c, wobei 3c die Hex-Darstellung der VRID ist. Sie können 255 VRIDs mit Werten von 1 bis 255 erstellen.

Einen virtuellen IPv4-MAC erstellen oder ändern

Sie erstellen einen virtuellen IPv4-MAC, indem Sie ihm eine virtuelle Router-ID zuweisen. Anschließend können Sie den virtuellen MAC an eine Schnittstelle binden. Sie können nicht mehrere

VRIDs an dieselbe Schnittstelle binden. Um die virtuelle MAC-Konfiguration zu überprüfen, sollten Sie die virtuellen MACs und die an die virtuellen MACs gebundenen Schnittstellen anzeigen und untersuchen.

So fügen Sie mithilfe der Befehlszeilenschnittstelle einen virtuellen MAC hinzu

Geben Sie in der Befehlszeile Folgendes ein:

- `add vrID`
- `bind vrid <id> -ifnum <interface_name>`
- `show vrID`

Beispiel

```
> add vrID 100
 Done
> bind vrid 100 -ifnum 1/1 1/2 1/3
 Done
<!--NeedCopy-->
```

So lösen Sie die Bindung von Schnittstellen zu einem virtuellen MAC mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `unbind vrid <id> -ifnum <interface_name>`
- `show vrID`

So konfigurieren Sie einen virtuellen MAC mithilfe der GUI

Navigieren Sie zu **System** > **Netzwerk** > **VMAC** und fügen Sie auf der Registerkarte **VMAC** einen neuen virtuellen MAC hinzu oder bearbeiten Sie einen vorhandenen virtuellen MAC.

Entfernen eines virtuellen IPv4-MAC

Um einen virtuellen IPv4-MAC zu entfernen, löschen Sie seine virtuelle Router-ID.

So entfernen Sie einen virtuellen IPv4-MAC mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

`rm vrid <id>`

Beispiel


```
rm vrid 100s
<!--NeedCopy-->
```

So entfernen Sie einen virtuellen IPv4-MAC mithilfe der GUI

Navigieren Sie zu **System** > **Netzwerk** > **VMAC** und löschen Sie auf der Registerkarte **VMAC** den virtuellen IPv4-MAC.

Konfiguration virtueller IPv6-MAC6s

Der NetScaler unterstützt virtuelles MAC6 für IPv6-Pakete. Sie können jede Schnittstelle an einen virtuellen MAC6 binden, auch wenn ein virtueller IPv4-MAC an die Schnittstelle gebunden ist. Jedes IPv6-Paket, das von der Schnittstelle gesendet wird, verwendet den virtuellen MAC6, der an diese Schnittstelle gebunden ist. Wenn kein virtuelles MAC6 an eine Schnittstelle gebunden ist, verwendet ein IPv6-Paket den physischen MAC.

Einen virtuellen MAC6 erstellen oder ändern

Sie erstellen einen virtuellen IPv6-MAC, indem Sie ihm eine virtuelle IPv6-Router-ID zuweisen. Anschließend können Sie den virtuellen MAC an eine Schnittstelle binden. Sie können nicht mehrere IPv6-VRIDs an eine Schnittstelle binden. Um die virtuelle MAC6-Konfiguration zu überprüfen, sollten Sie die virtuellen MAC6s und die an die virtuellen MAC6s gebundenen Schnittstellen anzeigen und untersuchen.

So fügen Sie mithilfe der Befehlszeilenschnittstelle einen virtuellen MAC6 hinzu

Geben Sie in der Befehlszeile Folgendes ein:

- `add vrID6 <id>`
- `bind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Beispiel

```
> add vrID6 100
Done
> bind vrID6 100 -ifnum 1/1 1/2 1/3
 Done
<!--NeedCopy-->
```


So heben Sie die Bindung von Schnittstellen von einem virtuellen MAC6 mithilfe der Befehlszeilenschnittstelle auf

Geben Sie in der Befehlszeile Folgendes ein:

- `unbind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

So konfigurieren Sie einen virtuellen MAC6 mithilfe der GUI

Navigieren Sie zu **System** > **Netzwerk** > **VMAC** und fügen Sie auf der Registerkarte **VMAC6** einen neuen virtuellen MAC6 hinzu oder bearbeiten Sie einen vorhandenen virtuellen MAC6.

Entfernen eines virtuellen MAC6

Um einen virtuellen IPv4-MAC zu entfernen, löschen Sie seine virtuelle Router-ID.

So entfernen Sie einen virtuellen MAC6 mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
rm vrid6 <id>
```

Beispiel

```
1 rm vrid6 100s
2 <!--NeedCopy-->
```

So entfernen Sie einen virtuellen MAC6 mithilfe der GUI

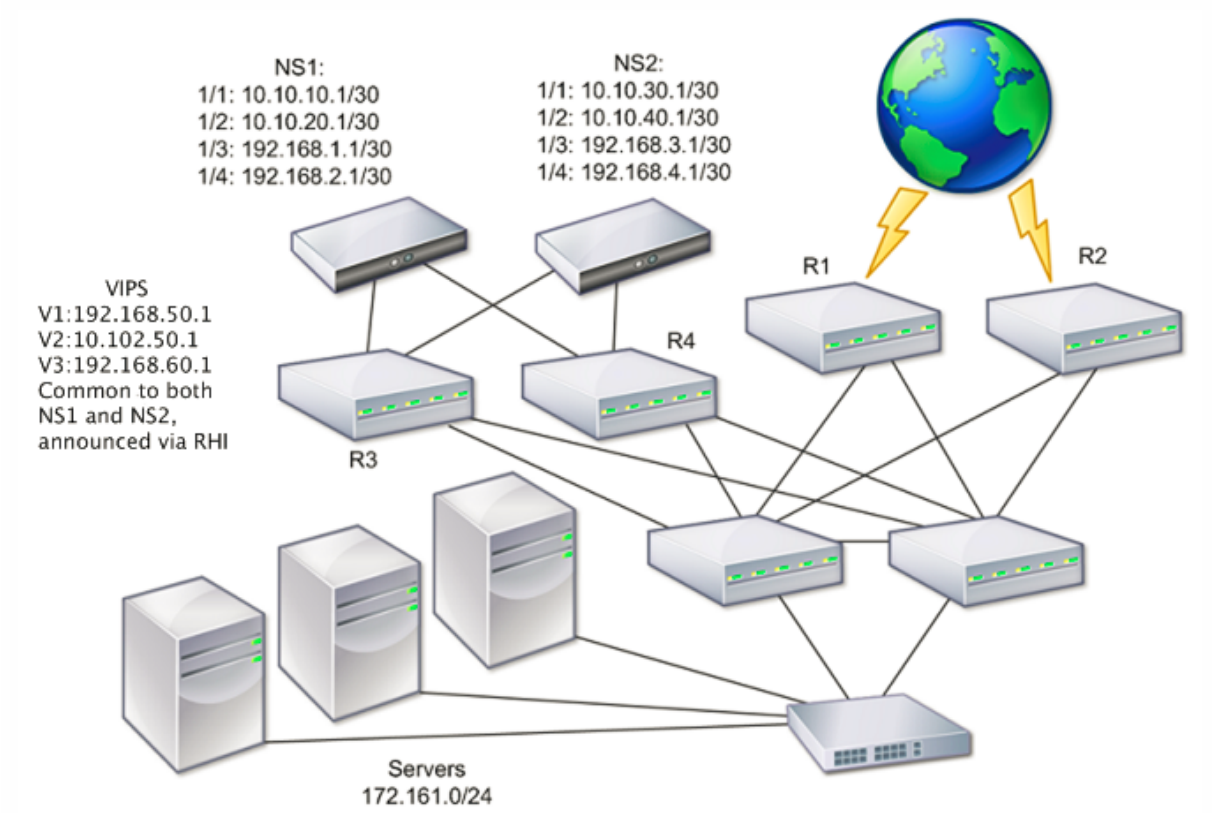
Navigieren Sie zu **System** > **Netzwerk** > **VMAC** und löschen Sie auf der Registerkarte **VMAC6** die virtuelle Router-ID.

Konfigurieren von Knoten mit hoher Verfügbarkeit in verschiedenen Subnetzen

May 11, 2023

Die folgende Abbildung zeigt eine HA-Bereitstellung mit den beiden Systemen, die sich in unterschiedlichen Subnetzen befinden:

Abbildung 1. Hohe Verfügbarkeit über ein geroutetes Netzwerk



In der Abbildung sind die Systeme NS1 und NS2 mit zwei separaten Routern, R3 und R4, in zwei verschiedenen Subnetzen verbunden. Die NetScaler-Appliances tauschen Heartbeat-Pakete über die Router aus. Diese Konfiguration könnte erweitert werden, um Bereitstellungen mit einer beliebigen Anzahl von Schnittstellen zu ermöglichen.

> **Hinweis**:
>
> Wenn Sie in Ihrem Netzwerk statisches Routing verwenden, müssen Sie statische Routen zwischen allen Systemen hinzufügen, um sicherzustellen, dass Heartbeat-Pakete erfolgreich gesendet und empfangen werden. (Wenn Sie dynamisches Routing auf Ihren Systemen verwenden, sind statische Routen nicht erforderlich.)

Wenn sich die Knoten in einem HA-Paar in zwei separaten Netzwerken befinden, müssen der primäre und der sekundäre Knoten über unabhängige Netzwerkkonfigurationen verfügen. Dies bedeutet, dass Knoten in verschiedenen Netzwerken Entitäten wie SNIP-Adressen, VLANs und Routen nicht gemeinsam nutzen können. Diese Art der Konfiguration, bei der die Knoten in einem HA-Paar unterschiedliche konfigurierbare Parameter haben, wird als Independent Network Configuration (INC) oder Symmetric Network Configuration (SNC) bezeichnet.

Die folgende Tabelle fasst die konfigurierbaren Entitäten und Optionen für eine INC zusammen und zeigt, wie sie auf jedem Knoten festgelegt werden müssen.

NetScaler-Entitäten	Optionen
IPs (NSIP/SNIPs)	Knotenspezifisch. Nur auf diesem Knoten aktiv.
VIPs	Floating.
VLANs	Knotenspezifisch. Nur auf diesem Knoten aktiv.
Routen	Knotenspezifisch. Nur auf diesem Knoten aktiv. Die Routen für den Link-Load-Balancing sind variabel.
ACLs	Schwimmend (üblich). Aktiv auf beiden Knoten.
Dynamisches Routing	Knotenspezifisch. Nur auf diesem Knoten aktiv. Der sekundäre Knoten sollte auch die Routing-Protokolle ausführen und sich mit Upstream-Routern verbinden.
L2-Modus	Schwimmend (üblich). Aktiv auf beiden Knoten.
L3-Modus	Schwimmend (üblich). Aktiv auf beiden Knoten.
Umgekehrte NAT (RNAT)	RNAT-Konfiguration mit der NAT-IP-Adresse, die auf eine virtuelle Server-IP-Adresse (VIP) eingestellt ist, da die VIP-Adresse floatend (häufig) ist.

Wie bei der Konfiguration von HA-Knoten im selben Subnetz melden Sie sich zum Konfigurieren von HA-Knoten in verschiedenen Subnetzen bei jeder der beiden NetScaler Appliances an und fügen einen Remote-Knoten hinzu, der die andere Appliance darstellt.

Remoteknoten hinzufügen

Wenn sich zwei Knoten eines HA-Paares in unterschiedlichen Subnetzen befinden, muss jeder Knoten eine andere Netzwerkkonfiguration haben. Um zwei unabhängige Systeme so zu konfigurieren, dass sie als HA-Paar funktionieren, müssen Sie daher während des Konfigurationsprozesses den INC-Modus angeben.

Wenn Sie einen HA-Knoten hinzufügen, müssen Sie den HA-Monitor für jede Schnittstelle deaktivieren, die nicht angeschlossen ist oder nicht für Datenverkehr verwendet wird. Für CLI-Benutzer ist dies ein separates Verfahren.

So fügen Sie einen Knoten mithilfe der Befehlszeilenschnittstelle hinzu

Geben Sie in der Befehlszeile Folgendes ein:

- `add ha node <id> <IPAddress> -inc ENABLED`
- `show ha node`

Beispiel

```
1 > add ha node 3 10.102.29.170 -inc ENABLED
2  Done
3 > add ha node 3 1000:0000:0000:0000:0005:0600:700a:888b
4   Done
5 <!--NeedCopy-->
```

Deaktivieren eines HA-Monitors mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set interface <ifNum> [-haMonitor ( **ON** | **OFF** )]`
- `show interface <ifNum>`

Beispiel

```
1 > set interface 1/3 -haMonitor OFF
2  Done
3 <!--NeedCopy-->
```

So fügen Sie einen Remote-Knoten mithilfe der GUI hinzu

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** und fügen Sie auf der Registerkarte **Knoten** einen neuen Remote-Knoten hinzu.
2. Stellen Sie sicher, dass Sie die Optionen HA-Monitor bei ausgeschlagenen Schnittstellen/Kanälen ausschalten und den INC-Modus (Independent Network Configuration) im Selbstmodus aktivieren aktiviert haben.

Knoten entfernen

Wenn Sie einen Knoten entfernen, befinden sich die Knoten nicht mehr in Hochverfügbarkeitskonfiguration.

So entfernen Sie einen Knoten mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:


```
rm ha node <id>
```

Beispiel

```
> rm ha node 2
  Done
<!--NeedCopy-->
```

So entfernen Sie einen Knoten mithilfe der GUI

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und löschen Sie den **Knoten** auf der Registerkarte Knoten.

> **Hinweis**:
>
> Mit dem Network Visualizer können Sie die NetScaler Appliances anzeigen, die als Hochverfügbarkeits-Paar (High Availability, HA-Paar) konfiguriert sind, und Hochverfügbarkeits-Konfigurationsaufgaben ausführen.

Konfigurieren von Routenmonitoren

September 18, 2023

Sie können Routenmonitore verwenden, um den HA-Status von der internen Routingtabelle abhängig zu machen, unabhängig davon, ob die Tabelle dynamisch gelernte oder statische Routen enthält. In einer HA-Konfiguration überwacht ein Routenmonitor auf jedem Knoten die interne Routingtabelle, um sicherzustellen, dass immer ein Routeneintrag für das Erreichen eines bestimmten Netzwerks vorhanden ist. Wenn der Routeneintrag nicht vorhanden ist, ändert sich der Status des Routenmonitors auf DOWN.

Wenn eine NetScaler-Appliance nur statische Routen hat, um ein Netzwerk zu erreichen, und Sie einen Routenmonitor für das Netzwerk erstellen möchten, müssen Sie überwachte statische Routen (MSR) für die statischen Routen aktivieren. MSR entfernt nicht erreichbare statische Routen aus der internen Routingtabelle. Wenn MSR auf statischen Routen deaktiviert ist, kann eine nicht erreichbare statische Route in der internen Routingtabelle verbleiben, was den Zweck der Routenüberwachung zunichte macht.

Routenmonitore werden sowohl im Nicht-INC-Modus als auch im INC-Modus unterstützt.

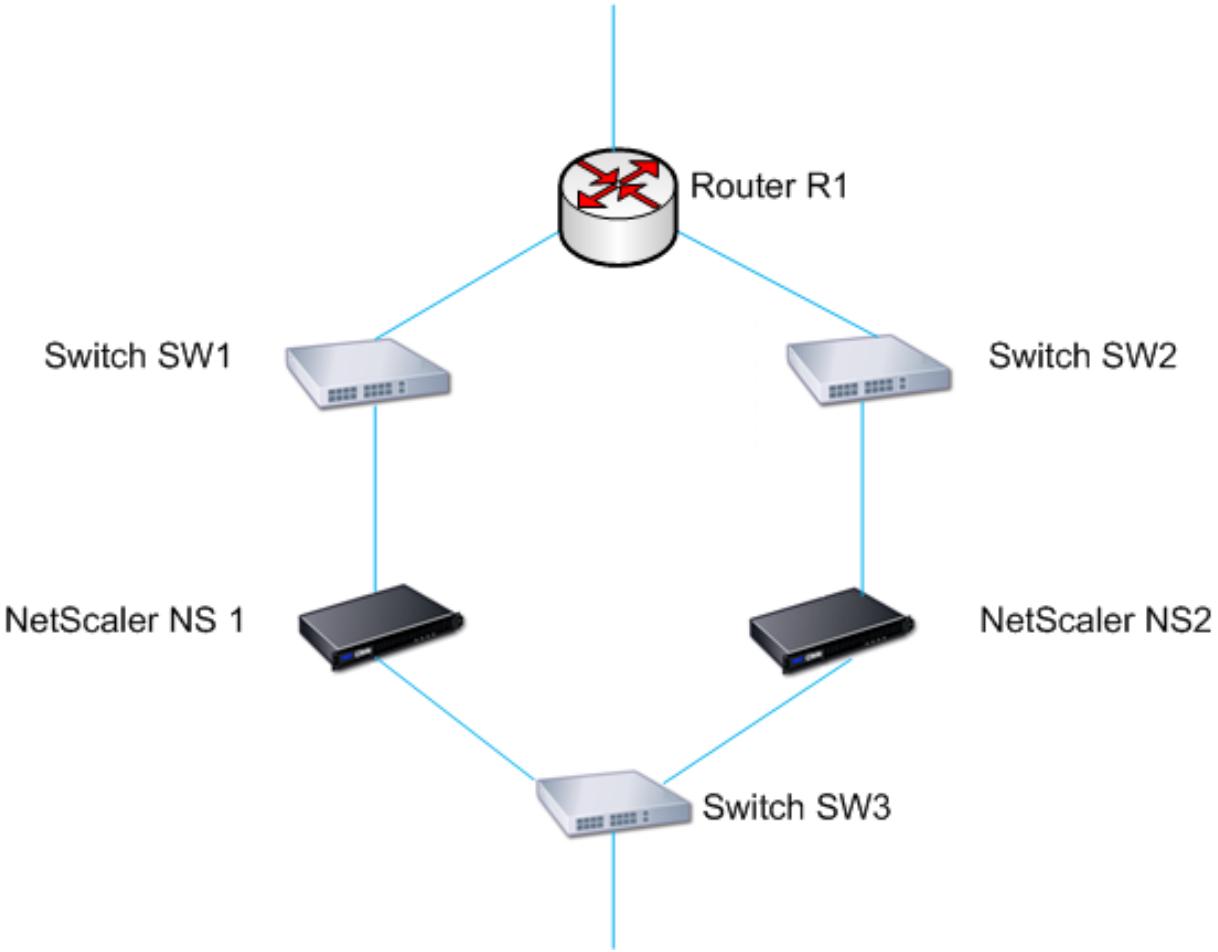
Routing Monitore in HA im Nicht-INC-Modus	Routing Monitore in HA im INC-Modus
Routenmonitore werden von Knoten weitergegeben und während der Synchronisierung ausgetauscht.	Routenmonitore werden während der Synchronisation weder von Knoten weitergegeben noch ausgetauscht.
Routenmonitore sind nur im aktuellen primären Knoten aktiv.	Routenmonitore sind sowohl auf dem primären als auch auf dem sekundären Knoten aktiv.
Die NetScaler Appliance zeigt den Status eines Routenmonitors immer als UP an, unabhängig davon, ob der Routeneintrag in der internen Routingtabelle vorhanden ist oder nicht.	Die NetScaler Appliance zeigt den Status des Routenmonitors als DOWN an, wenn der entsprechende Routeneintrag in der internen Routingtabelle nicht vorhanden ist.
Ein Routenmonitor beginnt in den folgenden Fällen nach 180 Sekunden mit der Überwachung seiner Route [Dies geschieht, damit dynamische Routen gelernt werden können, was 180 Sekunden dauern kann]: Neustart, Failover, Befehl set route6 für v6-Routen, set route msr enable/disable Befehl für v4-Routen, Hinzufügen eines neuen Routenmonitors.	-

Routenmonitore sind in einer HA-Konfiguration ohne INC-Modus nützlich, bei der die Nichterreichbarkeit eines Gateway von einem primären Knoten aus eine der Bedingungen für ein HA-Failover sein soll.

Stellen Sie sich ein Beispiel für ein HA-Setup ohne INC-Modus in einer zweiarmigen Topologie vor, die die NetScaler-Appliances NS1 und NS2 im selben Subnetz mit dem Router R1 und den Switches SW1, SW2 und SW3 hat.

Da R1 der einzige Router in diesem Setup ist, möchten Sie, dass das HA-Setup immer dann ausfällt, wenn R1 vom aktuellen primären Knoten aus nicht erreichbar ist. Sie können einen Routenmonitor (z. B. RM1 bzw. RM2) auf jedem der Knoten konfigurieren, um die Erreichbarkeit von R1 von diesem Knoten aus zu überwachen.

Abbildung 1.



Mit NS1 als aktuellem primären Knoten sieht der Ausführungsablauf wie folgt aus:

1. Der Routenmonitor RM1 auf NS1 überwacht die interne Routingtabelle von NS1 auf das Vorhandensein eines Routeneintrags für Router R1. NS1 und NS2 tauschen in regelmäßigen Abständen Heartbeat-Nachrichten über den Switch SW1 oder SW3 aus.
2. Wenn Switch SW1 ausfällt, erkennt das Routing-Protokoll auf NS1, dass R1 nicht erreichbar ist, und entfernt daher den Routeneintrag für R1 aus der internen Routing-Tabelle. NS1 und NS2 tauschen in regelmäßigen Abständen Heartbeat-Nachrichten über den Switch SW3 aus.
3. RM1 erkennt, dass der Routeneintrag für R1 in der internen Routingtabelle nicht vorhanden ist, und leitet ein Failover ein Failover ein. Wenn die Route zu R1 sowohl von NS1 als auch von NS2 unterbrochen ist, erfolgt ein Failover alle 180 Sekunden, bis eine der Appliances R1 erreichen und die Konnektivität wiederherstellen kann.

Hinzufügen eines Routenmonitors zu einem Hochverfügbarkeitsknoten

Eine einzige Prozedur erstellt einen Routenmonitor und bindet ihn an einen HA-Knoten.

> Hinweis:
>
> Wenn Sie Admin-Partitionen konfiguriert haben, stellen Sie sicher, dass Sie Routenmonitore von der Standardpartition hinzufügen.

So fügen Sie mithilfe der Befehlszeilenschnittstelle einen Routenmonitor hinzu

Geben Sie an der Befehlszeile Folgendes ein:

- `bind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- `show HA node`

Beispiel

```
> bind HA node 0 -routeMonitor 10.102.71.0 255.255.255.0
 Done
> bind HA node 0 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
 Done
<!--NeedCopy-->
```

So fügen Sie mithilfe der GUI einen Routenmonitor hinzu

Navigieren Sie zu **System** > **Hochverfügbarkeit** und klicken Sie auf der Registerkarte **Route Monitors** auf **Configure**.

Routenmonitore entfernen

So entfernen Sie einen Routenmonitor mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile Folgendes ein:

- `unbind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- ha-Knoten anzeigen

Beispiel

```
unbind HA node 3 -routeMonitor 10.102.71.0 255.255.255.0
unbind HA node 3 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
<!--NeedCopy-->
```

So entfernen Sie einen Routenmonitor mithilfe der GUI

Navigieren Sie zu **System** > **Hohe Verfügbarkeit** und löschen Sie auf der Registerkarte **Route Monitore** den Routenmonitor.

Begrenzung von Failovers, die durch Routenmonitore im Nicht-INC-Modus verursacht werden

May 11, 2023

Wenn in einer HA-Konfiguration ohne INC-Modus Routenmonitore auf beiden Knoten ausfallen, erfolgt alle 180 Sekunden ein Failover, bis einer der Knoten alle von den jeweiligen Routenmonitoren überwachten Routen erreichen kann.

Für einen Knoten können Sie jedoch die Anzahl der Failovers für ein bestimmtes Intervall einschränken, indem Sie die Parameter Maximale Anzahl von Flips und Maximale Flip-Zeit auf den Knoten festlegen. Wenn eines der Grenzwerte erreicht ist, finden keine Failovers mehr statt und der Knoten wird als primärer Knoten zugewiesen (aber der Knotenstatus ist NICHT IN BETRIEB), selbst wenn ein Routenmonitor auf diesem Knoten ausfällt. Diese Kombination aus HA-Status als Primary und Node State als NOT UP wird als Stick Primary State bezeichnet.

Wenn der Knoten dann in der Lage ist, alle überwachten Routen zu erreichen, werden beim nächsten Monitorausfall die Parameter Maximum Number of Flips und Maximum Flip Time auf dem Knoten zurückgesetzt und die im Parameter Maximale Flipzeit angegebene Zeit gestartet.

Diese Parameter werden auf jedem Knoten unabhängig festgelegt und daher weder propagiert noch synchronisiert.

Parameter zur Begrenzung der Anzahl der Failovers

- **Maximale Anzahl von Flips (MaxFlips)**

  Maximale Anzahl von Failovers, die innerhalb des maximalen Flip-Time-Intervalls für den Knoten in HA im Nicht-INC-Modus zulässig sind, wenn die Failover durch einen Ausfall des Route-Monitors verursacht werden.

- **Maximale Flipzeit (MaxFlipTime)**

  Zeitraum in Sekunden, in dem Failover aufgrund eines Route-Monitor-Fehlers für den Knoten in HA im Nicht-INC-Modus zulässig sind.

So begrenzen Sie die Anzahl der Failovers mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set HA node [-maxFlips < positive_integer>] [-maxFlipTime <positive_integer >]`
- `show HA node [< id>]`

Um die Anzahl der Failovers mithilfe der GUI zu begrenzen

1. Navigieren Sie zu **System** > **Hohe Verfügbarkeit** und öffnen Sie auf der Registerkarte **Knoten** den lokalen Knoten.

2. Legen Sie die folgenden Parameter fest:

- Maximale Anzahl von Flips
- Maximale Umdrehzeit

```
> set ha node -maxFlips 30 -maxFlipTime 60
Done
> sh ha node
1) Node ID: 0
IP: 10.102.169.82 (NS)
Node State: UP
Master State: Primary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: ENABLED
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen :None
Interfaces causing Partial Failure:None
SSL Card Status: NOT PRESENT
Hello Interval: 200 msecs
Dead Interval: 3 secs
Node in this Master State for: 0:4:24:1 (days:hrs:min:sec)

2) Node ID: 1
IP: 10.102.169.81
Node State: UP
Master State: Secondary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: SUCCESS
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen : None
Interfaces causing Partial Failure: None
SSL Card Status: NOT PRESENT

Local node information:
Configured/Completed Flips: 30/0
Configured Flip Time: 60
Critical Interfaces: 1/1
```



```
41
42      Done
43 <!--NeedCopy-->
```

SNMP-Alarm für „Sticky Primary State“

Aktivieren Sie den HA-STICKY-PRIMARY SNMP-Alarm in einem Knoten mit einer Hochverfügbarkeitseinrichtung, wenn Sie eine Warnung erhalten möchten, wenn der Knoten zu einem festen Primärknoten wird. Wenn der Knoten zu klebrigen primären Knoten wird, warnt er durch Generieren einer Trap-Nachricht (StickyPrimary (1.3.6.1.4.1.5951.1.1.0.138)) und sendet ihn an alle konfigurierten SNMP-Trap-Ziele. Weitere Informationen zum Konfigurieren von SNMP-Alarmen und Trap-Zielen finden Sie unter Onfiguring des NetScaler zum Generieren von SNMPv1- und SNMPv2-Traps.

Häufig gestellte Fragen

Stellen Sie sich ein Beispiel für ein Hochverfügbarkeits-Setup zweier NetScaler-Appliances NS-1 und NS-2 im Nicht-INC-Modus vor. Die maximale Anzahl von Flips und die maximale Umdrehzeit in beiden Knoten wurden mit denselben Werten festgelegt.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt:

Entität	Detail
IP-Adresse von NS-1	10.102.173.211
IP-Adresse von NS-2	10.102.173.212
Maximale Anzahl von Flips	2
Maximale Umdrehungszeit	200

Informationen über die maximale Anzahl von Flips und die maximale Drehzeiteinstellungenfinden Sie in der PDF-Datei.

Konfiguration des Failover-Schnittstellensatzes

May 11, 2023

Ein Failover Interface Set (FIS) ist eine logische Gruppe von Schnittstellen. In einer HA-Konfiguration ist die Verwendung eines FIS eine Möglichkeit, ein Failover zu verhindern, indem Schnittstellen gruppiert werden, sodass, wenn eine Schnittstelle ausfällt, weiterhin andere funktionierende

Schnittstellen verfügbar sind. Ein FIS kann auch für die Knoten eines NetScaler-Clusters konfiguriert werden.

HA-MON-Schnittstellen, die nicht an ein FIS gebunden sind, werden als kritische Schnittstellen (CI) bezeichnet, da, wenn eine von ihnen ausfällt, ein Failover ausgelöst wird.

> **Hinweis**:
>
> Ein FIS erstellt keine aktive Konfiguration und keine Standby-Konfiguration. Es verhindert auch nicht, dass Schleifen überbrückt werden, wenn Verbindungen mit demselben VLAN verbunden werden.

FIS erstellen oder ändern

Um ein FIS hinzuzufügen und Schnittstellen daran zu binden, verwenden Sie die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `add fis <name>`
- `bind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Beispiel

```
> add fis fis1
 Done
> bind fis fis1 1/3 1/5
 Done
<!--NeedCopy-->
```

Eine ungebundene Schnittstelle wird zu einer kritischen Schnittstelle (CI), wenn sie aktiviert ist und HA MON aktiviert ist.

So trennen Sie die Bindung einer Schnittstelle von einem FIS mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `unbind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Beispiel

```
> unbind fis fis1 1/3
 Done
<!--NeedCopy-->
```


So konfigurieren Sie ein FIS mithilfe der GUI

Navigieren Sie zu System > Hochverfügbarkeit und fügen Sie auf der Registerkarte Failover-Schnittstellensatz ein neues FIS hinzu oder bearbeiten Sie ein vorhandenes FIS.

FIS entfernen

Wenn das FIS entfernt wird, werden seine Schnittstellen als kritische Schnittstellen gekennzeichnet.

So entfernen Sie ein FIS mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
rm fis <name>
```

Beispiel

```
1 > rm fis fis1
2   Done
3 <!--NeedCopy-->
```

So entfernen Sie ein FIS mithilfe der GUI

Navigieren Sie zu **System** > **High Availability** und löschen Sie auf der Registerkarte **Failover Interface Set** das FIS.

Die Ursachen von Failover verstehen

September 8, 2021

Die folgenden Ereignisse können zu Failover in einer Hochverfügbarkeitskonfiguration führen:

1. Wenn der sekundäre Knoten für einen Zeitraum kein Heartbeat-Paket vom Primär erhält, der das tote Intervall überschreitet, das auf der Sekundarstufe festgelegt ist. (Siehe Anmerkung 1.)
2. Der primäre Knoten erlebt einen Hardwarefehler seiner SSL-Karte.
3. Der primäre Knoten erhält drei Sekunden lang keine Heartbeat-Pakete auf seinen Netzwerkschnittstellen.
4. Auf dem primären Knoten schlägt eine Netzwerkschnittstelle fehl, die nicht Teil eines Failover Interface Sets (FIS) oder eines Link Aggregation (LA) -Kanals ist und der HA-Monitor (HAMON) aktiviert ist. (Siehe Anmerkung 2.)
5. Auf dem primären Knoten schlagen alle Schnittstellen in einem FIS fehl. (Siehe Anmerkung 2.)

6. Auf dem primären Knoten schlägt ein LA-Kanal mit aktiviertem HAMON fehl. (Siehe Anmerkung 2.)
7. Auf dem primären Knoten schlagen alle Schnittstellen fehl (siehe Anmerkung 2). In diesem Fall tritt ein Failover unabhängig von der HAMON-Konfiguration auf.
8. Auf dem primären Knoten sind alle Schnittstellen manuell deaktiviert. In diesem Fall tritt ein Failover unabhängig von der HAMON-Konfiguration auf.
9. Sie erzwingen ein Failover, indem Sie den Befehl Force Failover auf beiden Knoten ausgeben.
10. Ein Routenmonitor, der an den primären Knoten gebunden ist, geht DOWN.

> **Hinweis 1:**
>
> Weitere Informationen zum Einstellen des Totintervalls finden Sie unter Konfigurieren der Kommunikationsintervalle. Mögliche Ursachen für einen Knoten, der keine Heartbeat-Pakete von einem Peer-Knoten empfängt, sind:
>
> - Ein Netzwerkkonfigurationsproblem verhindert, dass Heartbeats das Netzwerk zwischen den HA-Knoten durchqueren.
> - Der Peer-Knoten kommt es zu einem Hardware- oder Softwarefehler, der dazu führt, dass er einfriert (hängt), neu startet oder anderweitig die Verarbeitung und Weiterleitung von Heartbeat-Paketen stoppt.
>
> **Hinweis 2:**
>
> In diesem Fall bedeutet Fail, dass die Schnittstelle aktiviert wurde, aber in den DOWN-Status wechselt, wie aus dem Befehl show interface oder aus der GUI hervorgeht. Mögliche Ursachen für eine aktivierte Schnittstelle im Zustand DOWN sind LINK DOWN und TXSTALL.

Einen Knoten zum Failover zwingen

May 11, 2023

Möglicherweise möchten Sie ein Failover erzwingen, wenn Sie beispielsweise den primären Knoten ersetzen oder aktualisieren müssen. Sie können ein Failover entweder vom primären oder vom sekundären Knoten erzwingen. Ein erzwungenes Failover wird nicht weitergegeben oder synchronisiert. Um den Synchronisationsstatus nach einem erzwungenen Failover anzuzeigen, können Sie den Status des Knotens anzeigen.

Ein erzwungenes Failover schlägt unter den folgenden Umständen fehl:

- Sie erzwingen ein Failover auf einem eigenständigen System.
- Der sekundäre Knoten ist deaktiviert.
- Der Sekundärknoten ist so konfiguriert, dass er sekundär bleibt.

Die NetScaler-Appliance zeigt eine Warnmeldung an, wenn sie ein potenzielles Problem erkennt,

wenn Sie den Befehl Force Failover ausführen. Die Nachricht enthält die Informationen, die die Warnung ausgelöst haben, und fordert eine Bestätigung an, bevor Sie fortfahren.

Sie können ein Failover auf einem primären Knoten, einem sekundären Knoten und wenn sich die Knoten im Listenmodus befinden, erzwingen.

- **Failover auf dem primären Knoten erzwingen**.

  Wenn Sie ein Failover auf dem primären Knoten erzwingen, wird der primäre Knoten zum sekundären und der sekundäre Knoten zum primären Knoten. Erzwungenes Failover ist nur möglich, wenn der primäre Knoten feststellen kann, dass der sekundäre Knoten UP ist.

  Wenn der sekundäre Knoten DOWN ist, gibt der Befehl Force Failover die folgende Fehlermeldung zurück: “Der Betrieb ist aufgrund eines ungültigen Peer-Status nicht möglich. Behebung und Wiederholen.”

  Wenn sich das sekundäre System im Anspruchs-Status befindet oder inaktiv ist, wird die folgende Fehlermeldung zurückgegeben:

  ```
  Operation not possible now. Please wait for the system to stabilize
  before retrying.
  ```

- **Erzwingen eines Failovers auf dem sekundären Knoten**.

  Wenn Sie den Befehl Failover erzwingen vom sekundären Knoten ausführen, wird der sekundäre Knoten primär und der primäre Knoten wird sekundär. Ein Force-Failover kann nur auftreten, wenn der Zustand des sekundären Knotens gut ist und nicht so konfiguriert ist, dass er sekundär bleibt.

  Wenn der sekundäre Knoten nicht zum primären Knoten werden kann oder wenn der sekundäre Knoten so konfiguriert wurde, dass er sekundär bleibt (mit der Option STAYSECONDARY), zeigt der Knoten die folgende Fehlermeldung an:

  ```
  Operation not possible as my state is invalid. View the node for more
  information.
  ```

- **Failover erzwingen, wenn sich Knoten im Listenmodus befinden**.

  Wenn auf den beiden Knoten eines HA-Paares unterschiedliche Versionen der Systemsoftware ausgeführt werden, wechselt der Knoten, auf dem die höhere Version ausgeführt wird, in den Listenmodus. In diesem Modus funktioniert weder die Befehlsausbreitung noch die Synchronisierung.

  Bevor Sie die Systemsoftware auf beiden Knoten aktualisieren, testen Sie die neue Version auf einem der Knoten. Um dies zu tun, müssen Sie ein Failover auf dem System erzwingen, das bereits aktualisiert wurde. Das aktualisierte System übernimmt dann als primärer Knoten, aber weder die Befehlsausbreitung noch die Synchronisierung erfolgt. Außerdem müssen alle Verbindungen wiederhergestellt werden.

> **Wichtig!**
>
> Wenn Sie ein Failover erzwingen, wenn ein HA-Synchronisationsvorgang ausgeführt wird, gehen möglicherweise einige aktive Datensitzungen im HA-Setup verloren. Warten Sie also, bis der HA-Synchronisationsvorgang abgeschlossen ist, bevor Sie den Force-Failover-Vorgang ausführen.

So erzwingen Sie Failover auf einem Knoten mithilfe der Befehlszeilenschnittstelle:

Geben Sie in der Befehlszeile Folgendes ein:

```
force HA failover
```

So erzwingen Sie Failover auf einem Knoten über die grafische Benutzeroberfläche:

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und wählen Sie auf der Registerkarte **Knoten** den Knoten aus, wählen Sie in der Liste Aktion die Option **Failover erzwingen** aus.

Erzwingen des sekundären Knotens, sekundär zu bleiben

August 19, 2021

In einem HA-Setup kann der sekundäre Knoten gezwungen werden, unabhängig vom Status des primären Knotens sekundär zu bleiben.

Angenommen, der primäre Knoten muss aktualisiert werden und der Prozess dauert einige Sekunden. Während des Upgrades wird der primäre Knoten möglicherweise einige Sekunden lang heruntergefahren, aber Sie möchten nicht, dass der sekundäre Knoten übernommen wird. Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er auch dann sekundär, wenn der primäre Knoten ausfällt. Wenn Sie erzwingen, dass der Status eines Knotens in einem HA-Paar sekundär bleibt, nimmt er nicht an Übergängen des HA-Zustands der Maschine teil. Der Status des Knotens wird als STAYSECONDARY angezeigt.

Das Erzwingen des Knotens, sekundär zu bleiben, funktioniert sowohl auf eigenständigen als auch auf sekundären Knoten. Auf einem eigenständigen Knoten müssen Sie diese Option verwenden, bevor Sie einen Knoten zum Erstellen eines HA-Paares hinzufügen können. Wenn Sie den neuen Knoten hinzufügen, stoppt der vorhandene Knoten die Verarbeitung von Datenverkehr und wird zum sekundären Knoten. Der neue Knoten wird zum primären Knoten.

> **Hinweis**:
>
> Wenn Sie ein System zwingen, sekundär zu bleiben, wird der erzwungene Prozess weder propagiert noch synchronisiert. Es betrifft nur den Knoten, auf dem Sie den Befehl ausführen.

So zwingen Sie, dass der sekundäre Knoten mit der Befehlszeilenschnittstelle sekundär bleibt

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ha node -hastatus STAYSECONDARY
```

So zwingen Sie, dass der sekundäre Knoten mit der GUI sekundär bleibt

Navigieren Sie zu **System** > **Hochverfügbarkeit**, öffnen Sie auf der Registerkarte **Knoten** den lokalen Knoten, und wählen Sie **STAY SECONDARY**.

Erzwingen des primären Knotens, primär zu bleiben

August 19, 2021

In einem HA-Setup können Sie erzwingen, dass ein gesunder Primärknoten auch nach einem Failover primär bleibt. Sie können diese Option entweder auf einem primären Knoten in einem HA-Paar aktivieren. Mit dieser Option kann sich der primäre Knoten im Primärzustand befinden, solange er gesund ist.

Auf einem eigenständigen Knoten müssen Sie diese Option verwenden, bevor Sie einen Knoten zum Erstellen eines HA-Paares hinzufügen können. Wenn Sie den neuen Knoten hinzufügen, funktioniert der vorhandene Knoten weiterhin als primärer Knoten, und der neue Knoten wird zum sekundären Knoten.

So zwingen Sie, dass der primäre Knoten mit der Befehlszeilenschnittstelle primär bleibt

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ha node -hastatus STAYPRIMARY
```

So zwingen Sie, dass der primäre Knoten mit der GUI primär bleibt

Navigieren Sie zu **System** > **Hochverfügbarkeit**, öffnen Sie auf der Registerkarte **Knoten** den lokalen Knoten, und wählen Sie **STAY PRIMARY** .

Häufig gestellte Fragen zu hoher Verfügbarkeit

May 11, 2023

1. Welche Ports werden verwendet, um die HA-bezogenen Informationen zwischen den Knoten in einer HA-Konfiguration auszutauschen?

   In einer HA-Konfiguration verwenden beide Knoten die folgenden Ports, um Informationen für HA auszutauschen:

   - UDP-Port 3003, um Heartbeat-Pakete auszutauschen.
   - Port 3010 für Synchronisation und Befehlsübertragung.

2. Was sind die Bedingungen, die die Synchronisation auslösen?

   Die Synchronisation wird durch eine der folgenden Bedingungen ausgelöst:

   - Die vom sekundären Knoten empfangene Inkarnationsnummer des primären Knotens stimmt nicht mit der des sekundären Knotens überein.
     Hinweis: Beide Knoten in einer HA-Konfiguration verwalten einen Zähler namens *Inkarnationszahl*, der die Anzahl der Konfigurationen in der Konfigurationsdatei des Knotens zählt. Jeder Knoten sendet seine Inkarnationsnummer in den Heartbeat-Nachrichten an jeden anderen Knoten. Die Inkarnationsnummer wird für die folgenden Befehle nicht erhöht:
     a) Alle HA-Konfigurationsbefehle. Fügen Sie beispielsweise einen HA-Knoten hinzu, legen Sie einen HA-Knoten fest und binden Sie einen HA-Knoten.
     b) Alle Interface-bezogenen Befehle. Beispiel: Schnittstelle festlegen und Schnittstelle deaktivieren.
     c) Alle kanalbezogenen Befehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.
   - Der sekundäre Knoten wird nach einem Neustart aktiviert.
   - Der primäre Knoten wird nach einem Failover sekundär.

3. Welche Konfigurationen werden in einer HA-Konfiguration im INC- oder Nicht-INC-Modus nicht synchronisiert oder weitergegeben?

   Die folgenden Befehle werden weder weitergegeben noch mit dem sekundären Knoten synchronisiert:

   - Alle knotenspezifischen HA-Konfigurationsbefehle. Fügen Sie beispielsweise einen HA-Knoten hinzu, legen Sie einen HA-Knoten fest und binden Sie einen HA-Knoten.
   - Alle Interface-bezogenen Konfigurationsbefehle. Beispiel: Schnittstelle festlegen und Schnittstelle deaktivieren.
   - Alle kanalbezogenen Konfigurationsbefehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.

> **Hinweis:**
>
> Die folgenden Konfigurationen werden weder synchronisiert noch nur in HA im INC-Modus weitergegeben. Jeder Knoten hat seinen eigenen:
>
> - SNIPs
> - VLANs
> - Strecken (außer LLB-Strecken)
> - Routenmonitore
> - RNAT-Regeln (außer jeder RNAT-Regel mit VIP als NAT-IP)
> - Dynamische Routing-Konfigurationen
> - Netzprofile

4. Wird eine dem sekundären Knoten hinzugefügte Konfiguration auf dem primären Knoten synchronisiert?

   Nein, eine dem sekundären Knoten hinzugefügte Konfiguration wird nicht mit dem primären Knoten synchronisiert.

5. Was könnte der Grund dafür sein, dass beide Knoten behaupten, der primäre Knoten in einer HA-Konfiguration zu sein?

   Der wahrscheinlichste Grund ist, dass der primäre und sekundäre Knoten beide fehlerfrei sind, aber der sekundäre nicht die Heartbeat-Pakete vom primären erhalten. Das Problem könnte im Netzwerk zwischen den Knoten liegen.

6. Steht bei einer HA-Konfiguration Probleme auf, wenn Sie die beiden Knoten mit unterschiedlichen Systemtakteinstellungen bereitstellen?

   Verschiedene Einstellungen der Systemuhr auf den beiden Knoten können zu folgenden Problemen führen:

   - Die Zeitstempel in den Logdateieinträgen stimmen nicht überein. Diese Situation macht es schwierig, die Protokolleinträge auf Probleme zu analysieren.
   - Nach einem Failover können Probleme mit jeder Art von Cookie-basierter Persistenz für den Lastenausgleich auftreten. Ein erheblicher Unterschied zwischen den Zeiten kann dazu führen, dass ein Cookie früher als erwartet abläuft, was zur Beendigung der Persistenzsitzung führt.
   - Ähnliche Überlegungen gelten für alle zeitbezogenen Entscheidungen auf den Knoten.

7. Was sind die Bedingungen für einen Fehlschlag des *Force-HA-Sync-Befehls* ?

   Die erzwungene Synchronisation schlägt unter den folgenden Umständen fehl:

   - Sie erzwingen die Synchronisation, wenn die Synchronisation bereits läuft.
   - Sie erzwingen die Synchronisation auf einer eigenständigen NetScaler-Appliance.
   - Der sekundäre Knoten ist deaktiviert.

- Die HA-Synchronisierung ist auf dem aktuellen sekundären Knoten deaktiviert.
- Die HA-Propagierung ist auf dem aktuellen primären Knoten deaktiviert und Sie erzwingen die Synchronisation vom primären Knoten aus.

8. Was sind die Bedingungen für das Scheitern des Befehls „ *HA-Dateien synchronisieren* “?

   Das Synchronisieren von Konfigurationsdateien schlägt unter einem der folgenden Umstände fehl:

   - Auf einem eigenständigen System.
   - Wenn der sekundäre Knoten deaktiviert ist.

9. Wechselt in einer HA-Konfiguration der sekundäre Knoten, wenn er die Funktion des primären Knotens übernimmt, wieder in den sekundären Status, wenn der ursprüngliche primäre Knoten wieder online ist?

   Nein. Nachdem der sekundäre Knoten die Position des primären Knotens übernommen hat, bleibt er auch dann als primärer Knoten aktiv, wenn der ursprüngliche primäre Knoten wieder online ist. Führen Sie den Befehl *force failover* aus, um den primären und den sekundären Status der Knoten auszutauschen.

10. Was sind die Bedingungen, unter denen der Befehl Force Failover fehlschlägt?

    Ein erzwungenes Failover schlägt unter den folgenden Umständen fehl:

    - Sie erzwingen ein Failover auf einem eigenständigen System.
    - Der sekundäre Knoten ist deaktiviert.
    - Der Sekundärknoten ist so konfiguriert, dass er sekundär bleibt.
    - Der primäre Knoten ist so konfiguriert, dass er primär bleibt.
    - Der Status des Peer-Knotens ist unbekannt.

Behebung von Problemen mit hoher Verfügbarkeit

May 11, 2023

Die häufigsten Probleme mit hoher Verfügbarkeit sind, dass die Hochverfügbarkeitsfunktion überhaupt nicht oder nur zeitweise funktioniert. Im Folgenden werden häufig auftretende Probleme mit hoher Verfügbarkeit sowie mögliche Ursachen und Lösungen aufgeführt.

- **Problem**
  Die Unfähigkeit der NetScaler-Appliances, die NetScaler-Appliances in einem Hochverfügbarkeits-Setup zu koppeln.
  - **Ursache**
    Netzwerkkonnektivität

Auflösung

Stellen Sie sicher, dass beide Appliances an den Switch angeschlossen sind und die Schnittstellen aktiviert sind.

- **Ursache**

  Das Passwort für das Standard-Administratorkonto stimmt nicht überein

  Auflösung

  Stellen Sie sicher, dass das Passwort auf beiden Appliances identisch ist.
- **Ursache**

  IP-Konflikt

  Auflösung

  Stellen Sie sicher, dass beide Appliances über eine eindeutige NetScaler-IP-Adresse (NSIP) verfügen. Die Appliances sollten nicht dieselbe NSIP-Adresse haben.
- **Ursache**

  Nichtübereinstimmung der Knoten-ID

  Auflösung

  Stellen Sie sicher, dass die Node-ID-Konfiguration auf beiden Appliances eindeutig ist. Die Appliances sollten nicht dieselbe Node-ID-Konfiguration haben. Darüber hinaus müssen Sie einer Knoten-ID einen Wert zwischen 1 und 64 zuweisen.
- **Ursache**

  Das Passwort des RPC-Knotens stimmt nicht überein

  Auflösung

  Stellen Sie sicher, dass beide Knoten dasselbe RPC-Knotenkennwort haben.
- **Ursache**

  Ein Administrator hat den Remote-Knoten deaktiviert

  Auflösung

  Aktivieren Sie den Remote-Knoten.
- **Ursache**

  Die Firewall-Anwendung hat die Heartbeat-Pakete blockiert

  Auflösung

Stellen Sie sicher, dass der UDP-Port 3003 zulässig ist.

- **Problem**

  Beide Geräte geben an, das primäre Gerät zu sein.
  - **Ursache**

    Fehlende Heartbeat-Pakete zwischen den Geräten

    Auflösung

    Stellen Sie sicher, dass der UDP-Port 3003 nicht für die Kommunikation zwischen den Appliances blockiert ist.
- **Problem**

  Die NetScaler-Appliance kann die Konfiguration nicht synchronisieren.

- **Ursache**
  Eine Firewall-Anwendung blockiert den erforderlichen Port.
  Auflösung
  Stellen Sie sicher, dass der UDP-Port 3010 (oder UDP-Port 3008 mit sicherer Synchronisation) nicht für die Kommunikation zwischen den Appliances blockiert ist.
- **Ursache**
  Ein Administrator hat die Synchronisation deaktiviert.
  Auflösung
  Aktivieren Sie die Synchronisation auf der Appliance, bei der das Problem auftritt.
- **Ursache**
  Verschiedene NetScaler-Versionen oder -Builds sind auf Appliances installiert.
  Auflösung
  Führen Sie ein Upgrade der Appliances auf dieselbe NetScaler-Version oder denselben NetScaler-Build durch.

- **Problem**
  Die Befehlsübertragung zwischen den Appliances schlägt fehl.
  - **Ursache**
    Eine Firewall-Anwendung blockiert den Port.
    Auflösung
    Stellen Sie sicher, dass der UDP-Port 3011 (oder UDP-Port 3009 mit sicherer Propagation) nicht für die Kommunikation zwischen den Appliances blockiert ist.
  - **Ursache**
    Ein Administrator hat die Befehlsweitergabe deaktiviert.
    Auflösung
    Aktivieren Sie die Befehlsweitergabe auf der Appliance, bei der das Problem auftritt.
  - **Ursache**
    Verschiedene NetScaler-Versionen oder -Builds sind auf Appliances installiert.
    Auflösung
    Führen Sie ein Upgrade der Appliances auf dieselbe NetScaler-Version oder denselben NetScaler-Build durch.
- **Problem**
  Die NetScaler-Appliances im Hochverfügbarkeitspaar können den erzwungenen Failover-Prozess nicht ausführen.
  - **Ursache**
    Der sekundäre Knoten ist deaktiviert.
    Auflösung
    Aktivieren Sie den sekundären Knoten.
  - **Ursache**
    Der sekundäre Knoten ist so konfiguriert, dass er sekundär bleibt.

Auflösung
Stellen Sie den sekundären Hochverfügbarkeitsstatus des sekundären Knotens auf Enable from Stay Secondary ein.

- **Problem**
  Die sekundäre Appliance empfängt nach dem Failover-Vorgang keinen Datenverkehr.
  - **Ursache**
    Der Upstream-Router versteht die GARP-Nachrichten der NetScaler-Appliance nicht.
    Auflösung
    Konfigurieren Sie die virtuelle MAC-Adresse auf der sekundären Appliance.

Verwalten von Heartbeat-Meldungen mit hoher Verfügbarkeit auf einer NetScaler Appliance

May 11, 2023

Die beiden Knoten in einer Hochverfügbarkeitskonfiguration senden und empfangen auf allen aktivierten Schnittstellen Heartbeat-Meldungen zueinander und voneinander. Die Heartbeat-Meldungen fließen unabhängig von der HA MON-Einstellung auf diesen Schnittstellen. Wenn NSVLAN oder beide (NSVLAN und SYNC) auf einer Appliance konfiguriert sind, fließen die Heartbeat-Nachrichten nur über die aktivierten Schnittstellen, die Teil von NSVLAN und SYNCVLAN sind.

Wenn ein Knoten die Heartbeat-Meldungen auf einer aktivierten Schnittstelle nicht empfängt, sendet er kritische Warnungen an die angegebenen SNMP-Manager. Diese kritischen Warnungen geben Fehlalarme aus und ziehen unnötige Aufmerksamkeit der Administratoren auf Schnittstellen, die nicht als Teil der Verbindungen zum Peer-Knoten konfiguriert sind.

Um dieses Problem zu beheben, wird die HAHeartbeat-Option für Schnittstellen und Kanäle verwendet, um den HA-Heartbeat-Nachrichtenfluss auf diesen zu aktivieren oder zu deaktivieren.

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen auf einer Schnittstelle mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set interface <ID> [-HAHeartBeat ( ON | OFF )]`
- `show interface <ID>`

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen auf einem Kanal mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set channel <ID> [-HAHeartBeat ( ON | OFF )]`
- `show channel <ID>`

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen für eine Schnittstelle über die GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **Schnittstellen**.
2. Aktivieren oder deaktivieren Sie den **HA-Heart-Beat-Parameter** .

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen auf einem Kanal über die GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **Kanäle**.
2. Aktivieren oder deaktivieren Sie den **HA-Heart-Beat-Parameter** .

NetScaler in einem Hochverfügbarkeitssetup entfernen und ersetzen

May 11, 2023

Dieses Thema hilft Ihnen dabei, sich mit dem Austausch von RMA zu befassen. Dieses Thema enthält außerdem Anweisungen zum Backup von Konfigurationen, zum Upgrade oder Downgrade der mitgelieferten Softwareversion und zum Einrichten des RPC-Passworts auf dem ADC.

Zu berücksichtigende Punkte

Die folgenden Konfigurationen werden in einer Hochverfügbarkeitskonfiguration im INC-Modus (Independent Network Configuration) oder Nicht-INC-Modus nicht synchronisiert oder propagiert:

- Alle knotenspezifischen HA-Konfigurationsbefehle. Fügen Sie beispielsweise einen HA-Knoten hinzu, legen Sie einen HA-Knoten fest und binden Sie einen HA-Knoten.
- Alle Interface-bezogenen Konfigurationsbefehle. Beispiel: Schnittstelle festlegen und Schnittstelle deaktivieren.
- Alle kanalbezogenen Konfigurationsbefehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.
- Alle Konfigurationsbefehle von Interface HA Monitoring.

Die folgenden Konfigurationen werden in einer HA-Konfiguration im INC-Modus (Independent Network Configuration) weder synchronisiert noch weitergegeben:

- SNIPs
- VLANs
- Strecken (außer LLB-Strecken)
- Routenmonitore
- RNAT-Regeln (außer jeder RNAT-Regel mit VIP als NAT-IP)
- Dynamische Routing-Konfigurationen

Anweisungen

Gehen Sie wie folgt vor, um einen NetScaler im Hochverfügbarkeits-Setup zu ersetzen:

- Entfernen Sie einen aktiven sekundären NetScaler-Knoten
- Sekundären Ersatzknoten konfigurieren
- Überprüfen und aktualisieren Sie den Software-Build-on-Ersatz-ADC
- Stellen Sie das Passwort für Neue Sekundarstufe so ein, dass es dem primären entspricht
- Lizenzen zum Ersatz-ADC hinzufügen
- HA-Paar zwischen primärem und neuem sekundären Knoten erstellen

Entfernen Sie einen aktiven sekundären Knoten

1. Melden Sie sich an beiden ADCs an und führen Sie den folgenden Befehl aus, um zu bestätigen, welcher Knoten primär und welcher Knoten sekundär ist:

   ```
   show ha node
   <!--NeedCopy-->
   ```

2. Melden Sie sich am primären ADC an, Backup Sie die Konfigurationen auf dem primären Knoten und kopieren Sie die Dateien vor den Änderungen vom ADC. Diese Dateien befinden sich im Verzeichnis „/var /ns_sys_backup/“.

   Führen Sie die folgenden Schritte aus:

   a) Speichern Sie die ADC-Laufkonfigurationen im Speicher:

   ```
   save ns config
   <!--NeedCopy-->
   ```

   b) Erstellen Sie das vollständige Backup-Dateipaket:

   ```
   create system backup -level full
   <!--NeedCopy-->
   ```

   c) Erstellen Sie das grundlegende Backup-Dateipaket:

   ```
   create system backup -level basic
   <!--NeedCopy-->
   ```

3. Nachdem alle Sicherungsdateien generiert wurden, sollten Sie sie unbedingt vom Gerät kopieren, bevor Sie fortfahren.

   Öffnen Sie von einem Windows-Terminal aus eine Befehlszeile und kopieren Sie die Sicherungsdateien vom ADC auf Ihre lokale Festplatte. Dies kann mit dem folgenden Befehl erfolgen:


```
pscp <username>@<NSIP>:<Target file source>  <Target file
   destination>
<!--NeedCopy-->
```

Beispiel:

```
pscp nsroot@10.125.245.78:/var/ns_sys_backup/backup_basic_10
   .125.245.78_2016_09_14_15_08.tgz c:\nsbackup\backup_basic_10
   .125.245.78_2016_09_14_15_08.tgz
<!--NeedCopy-->
```

Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für das angegebene Administratorkonto ein und drücken Sie dann die Eingabetaste. Wiederholen Sie diese Schritte, bis alle Backup-Pakete auf den lokalen PC kopiert sind, bevor Sie fortfahren.

4. Stellen Sie eine SSH-Verbindung zum sekundären ADC her und setzen Sie das Gerät auf den Status „STAYSECONDARY“. Dadurch wird die Einheit gezwungen, nicht zu versuchen, die Hauptrolle zu übernehmen, falls während des Austauschs ein Fehler festgestellt wird. Vergewissern Sie sich, dass Sie mit dem sekundären ADC verbunden sind, bevor Sie diesen Schritt ausführen

```
set ha node  -haStatus <state>
set ha node  -haStatus STAYSECONDARY
<!--NeedCopy-->
```

5. Sobald der **Knotenstatus** des sekundären ADC erfolgreich STAYSECONDARY anzeigt, wechseln Sie zum primären ADC, löschen Sie den sekundären Knoten und führen Sie den folgenden Befehl aus:

```
save ns config
<!--NeedCopy-->
```

Führen Sie die folgenden Befehle aus, während Sie am primären ADC angemeldet sind

a) Führen Sie den folgenden Befehl aus, um zu ermitteln, welcher numerische Wert den sekundären HA-Knoten darstellt:

```
show ha node
<!--NeedCopy-->
```

b) Führen Sie den folgenden Befehl aus, um den sekundären ADC aus dem primären HA-Paar zu entfernen:

```
rm ha node <node ID>
<!--NeedCopy-->
```


c) Führen Sie den folgenden Befehl aus, um die Konfiguration zu speichern:

```
save ns config
<!--NeedCopy-->
```

d) Wenn der sekundäre ADC jetzt entfernt ist, fahren Sie ihn herunter, trennen Sie ihn und entfernen Sie ihn aus dem Netzwerk.

Hinweis. Achten Sie darauf, alle Verbindungen zu kennzeichnen, bevor Sie die Verbindung trennen.

Sekundären Ersatzknoten konfigurieren

1. Schalten Sie das neue Gerät ein, während der Ersatz-ADC installiert ist. VERBINDEN Sie die Netzwerkverbindungen zu diesem Zeitpunkt NICHT.
2. Wenn der Startvorgang abgeschlossen ist, verwenden Sie den Konsolenport, um eine Verbindung zum ADC herzustellen, und konfigurieren Sie das NSIP, das Sie für die Verbindung mit dem Gerät verwenden werden.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **4.**

   Hinweis. In diesem Beispiel verwenden wir ein anderes NSIP für den Ersatz-ADC. Wenn Sie die IP der ursprünglichen Sekundäreinheit verwenden möchten, können Sie sie beim Austausch ändern, bevor Sie den neuen ADC an die primäre HA-Einheit binden.
4. Der ADC sollte jetzt gebootet sein. Verbinden Sie nun die Netzwerkschnittstelle, die für den Verwaltungsverkehr verwendet wird, und stellen Sie sicher, dass die IP-Adresse von Ihrem Netzwerk aus erreichbar ist.

Überprüfen und aktualisieren Sie den Software-Build-on-Ersatz-ADC

Bevor wir die neue Einheit mit dem primären ADC synchronisieren, müssen wir sicherstellen, dass auf beiden ADCs derselbe Build ausgeführt wird.

1. Führen Sie den folgenden Befehl aus, um die Version auf ADC zu überprüfen:

   ```
   show version
   <!--NeedCopy-->
   ```

2. Erstellen Sie während des neuen sekundären ADC einen Unterordner in **/var**, der für das Upgrade verwendet werden soll.
3. Gehen Sie zu NetScaler-Downloads und laden Sie das entsprechende Paket herunter, das der Build-Version entspricht, die auf dem primären ADC ausgeführt wird.

4. Laden Sie die TGZ-Datei herunter und extrahieren Sie sie:

```
tar -xvzf "file.tgz"
<!--NeedCopy-->
```

5. Kopieren Sie die extrahierten Dateien auf den sekundären ADC. Öffnen Sie auf Ihrem Windows-Terminal eine „Befehlszeile“ und navigieren Sie zu dem Verzeichnis, das das entpackte .tgz-Build-Paket enthält, und führen Sie den folgenden pscp-Befehl aus:

```
pscp <Target file source>  <username>@<NSIP>:<Target file
   destination>
<!--NeedCopy-->
```

   Beispiel:

```
C:\inetpub>pscp c:\inetpub\build-12.1-47.14_nc.tgz nsroot@10
   .20.245.80:/var/NS_upg_12.1_47.14/build-12.1-47.14_nc.tgz
<!--NeedCopy-->
```

6. Nachdem die Datei übertragen wurde, kehren Sie zum sekundären ADC zurück und aktualisieren Sie das Upgrade. Ausführliche Anweisungen finden Sie unter Upgrade einer Citrix ADX Standalone Appliance.
7. Sobald der neue sekundäre neu gestartet wurde, wird SSH wieder in das Gerät aufgenommen und bestätigt, dass das Upgrade erfolgreich ist und der Build dem des primären entspricht.

Stellen Sie das Passwort auf dem sekundären Ersatzknoten so ein, dass es dem primären entspricht

Hinweis: Wenn Sie zu diesem Zeitpunkt die Management-IP-Adresse (NSIP) des neuen sekundären ADC ändern möchten, können Sie dies tun, bevor Sie fortfahren.

Ändern Sie das Passwort auf dem neuen sekundären ADC so, dass es mit dem Passwort übereinstimmt, das sich derzeit auf dem primären ADC befindet.

1. Stellen Sie sicher, dass das Standardpasswort für das Administratorkonto (nsroot) mit dem des primären ADC übereinstimmt. Dies wird mit dem folgenden Befehl erreicht, während Sie über SSH bei der neuen sekundären Einheit angemeldet sind:

```
set system user <user> <password>
<!--NeedCopy-->
```

   Mit diesem Befehl wird das Passwort für den angegebenen Benutzer festgelegt/zurückgesetzt.

2. SSH in den primären und neuen sekundären ADC und bestätigen, dass Kennwörter übereinstimmen.

Lizenzen zum sekundären Ersatzknoten hinzufügen

Nachdem der neue ADC aktualisiert und bereit für die Kopplung ist, laden Sie die entsprechende Lizenzierung für den Ersatzknoten herunter und installieren Sie sie.

1. Navigieren Sie https://www.citrix.com zu, um Lizenzen für das neue Ersatzgerät anzufordern und herunterzuladen.
2. Sobald Sie alle entsprechenden Lizenzen heruntergeladen haben, stellen Sie eine SSH-Verbindung zum neuen sekundären ADC her und geben Sie den folgenden Befehl ein, um den aktuellen Status der Lizenzierung einzusehen:

```
show license
<!--NeedCopy-->
```

3. Von der Windows-Terminal-Befehlszeile aus müssen Sie nun die Lizenzdateien mit dem folgenden Befehl auf den neuen sekundären ADC hochladen:

   Hinweis. Wenn Sie mehrere Lizenzen haben, wiederholen Sie diesen Schritt, bis alle Lizenzen hochgeladen sind.

```
pscp <Target file source>  <username>@<NSIP>:<Target file
   destination>
<!--NeedCopy-->
```

   Beispiel:

```
C:\inetpub>pscp c:\inetpub\NS-VPX-3K-LIC-020030ad0024.lic
   nsroot@10.125.245.80:/nsconfig/license/NS-VPX-3K-LIC-020030
   ad0024.lic
<!--NeedCopy-->
```

4. Stellen Sie eine SSH-Verbindung zum neuen sekundären ADC her und führen Sie einen Warmneustart mit dem folgenden Befehl durch:

```
reboot  -w
<!--NeedCopy-->
```

   Nachdem das Gerät neu gestartet wurde, verbinden Sie sich per SSH mit dem Gerät und führen Sie den Befehl show license erneut aus. Zu diesem Zeitpunkt sollten die Lizenzen beantragt werden.

Hochverfügbarkeit zwischen primärem und neuem sekundären Knoten einrichten

Zu diesem Zeitpunkt sind wir bereit, die NetScaler Einheiten zu einem Hochverfügbarkeitspaar zu verbinden. Weitere Informationen finden Sie unter Konfigurieren von Hochverfügbarkeit.

Wiederholungsversuche anfordern

May 11, 2023

Wenn eine NetScaler Appliance eine HTTP-Anforderung erhält, aber einen Verbindungsfehler mit einem Back-End-Server aufweist, verwendet die Appliance eine Wiederholungsanweisung. Die erneute Anfrage behebt Szenarien mit Verbindungsfehlern und ermöglicht es der Appliance, den nächsten verfügbaren Dienst auszuwählen und die Anforderung weiterzuleiten. Durch eine Neu-Anfrage kann der Client Roundtrip-Zeit (RTT) sparen.

Die Funktion “Wiederholung anfordern” ist für die folgenden Szenarien mit Verbindungsfehlern anwendbar:

- Wenn ein Backend-Server eine TCP-Verbindung zurücksetzt, wenn eine HTTP-Anfrage empfangen wird. Weitere Informationen finden Sie unter Wiederholungsversuche beantragen.
- Wenn ein Backend-Server während des Verbindungsaufbaus eine TCP-Verbindung zurücksetzt. Weitere Informationen finden Sie unter Wiederholungsversuche beantragen.
- Wenn eine Antwort von einem Back-End eine Zeitüberschreitung (basierend auf dem konfigurierten Timeoutwert), wenn eine Appliance eine HTTP-Anfrage sendet. Weitere Informationen finden Sie unter Wiederholungsversuche beantragen.

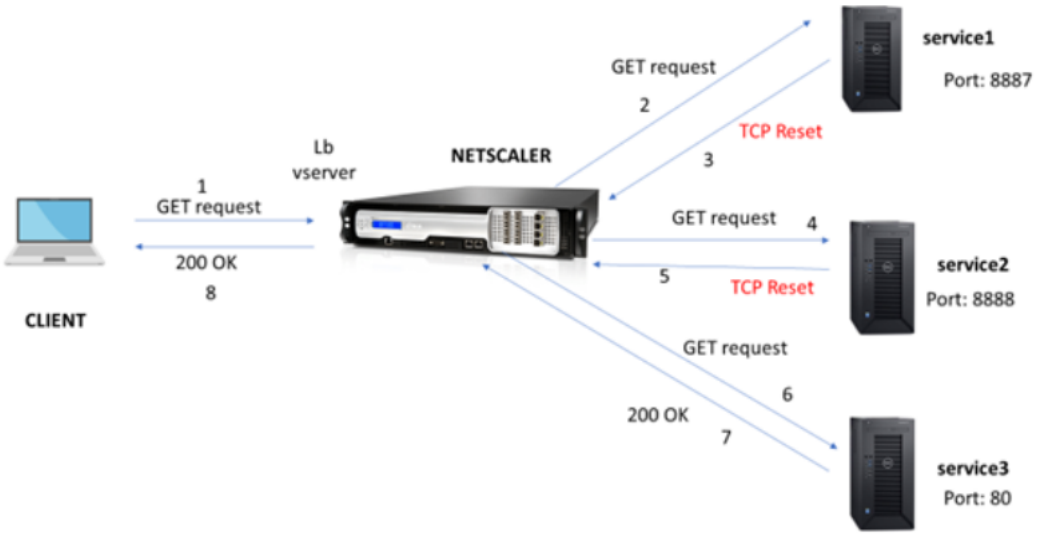
Wiederholung anfordern, wenn der Backend-Server die TCP-Verbindung zurücksetzt

May 11, 2023

Wenn ein Back-End-Server eine TCP-Verbindung zurücksetzt, leitet die Funktion zur Wiederholung der Anforderung die Anfrage an den nächsten verfügbaren Server weiter, anstatt den Reset an den Client zu senden. Durch das Reload-Balancing speichert der Client RTT, wenn die Appliance dieselbe Anfrage an den nächsten verfügbaren Dienst initiiert.

So funktioniert die Wiederholung von Anfragen, wenn der Backend-Server eine TCP-Verbindung zurücksetzt

Das folgende Diagramm zeigt, wie Komponenten miteinander interagieren.



1. Der Vorgang beginnt mit der Aktivierung der Appqoe-Funktion auf Ihrer Appliance.
2. Wenn der Client eine HTTP- oder HTTPS-Anfrage sendet, sendet der virtuelle Lastausgleichsserver die Anfrage an den Back-End-Server.
3. Wenn der angeforderte Dienst nicht verfügbar ist, setzt der Back-End-Server die TCP-Verbindung zurück.
4. Wenn in der Appqoe-Konfiguration „Wiederholung“ aktiviert ist und die gewünschte Anzahl von Wiederholungsversuchen angegeben ist, verwendet der virtuelle Lastausgleichsserver den konfigurierten Load-Balancing-Algorithmus, um die Anfrage an den nächsten verfügbaren Anwendungsserver weiterzuleiten.
5. Nachdem der virtuelle Lastausgleichsserver die Antwort erhalten hat, leitet die Appliance die Antwort an den Client weiter.
6. Wenn die verfügbaren Backend-Server gleich oder kleiner als die Anzahl der Wiederholungsversuche sind und wenn alle Server einen Reset senden, würde die Appliance einen internen Serverfehler von 500 melden. Betrachten Sie ein Szenario mit fünf verfügbaren Servern und der Wiederholungsanzahl, die auf sechs festgelegt ist. Wenn alle fünf Server die Verbindung zurücksetzen, gibt die Appliance einen internen Serverfehler von 500 an den Client zurück.
7. In ähnlicher Weise leitet die Appliance den Reset an den Client weiter, wenn die Anzahl der Backend-Server die Anzahl der Wiederholungsversuche übersteigt und wenn die Backend-Server die Verbindung zurücksetzen. Stellen Sie sich ein Szenario mit drei Back-End-Servern und der Wiederholungsanzahl vor, die auf zwei festgelegt ist. Wenn die drei Server die Verbindung zurücksetzen, sendet die Appliance eine Reset-Antwort an den Client.

Konfigurieren der Wiederholung der Anfrage für die GET-Methode

Um die Wiederholungsfunktion für die GET-Methode zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

1. Aktivieren Sie AppQoE
2. Add AppQoE action
3. Add AppQoE policy
4. Binden Sie die AppQoE-Richtlinie an den virtuellen Lastausgleichsserver

Aktivieren Sie AppQoE

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature appqoe
```

Add AppQoE action

Sie müssen eine AppQoE-Aktion konfigurieren, um anzugeben, ob die Appliance es nach einem TCP-Reset erneut versuchen soll, und um die Anzahl der Wiederholungsversuche anzugeben.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Beispiel:

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Wobei
retryOnReset. Aktivieren Sie “Wiederholen”, wenn der Back-End-Server eine TCP-Verbindung zurücksetzt.
Zahlen. Wiederholte Anzahl.

Add AppQoE policy

Um AppQoE zu implementieren, müssen Sie die AppQoE-Richtlinie so konfigurieren, dass eingehende HTTP- oder SSL-Anfragen in einer bestimmten Warteschlange priorisiert werden.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add appqoe policy reset_policy -rule http.req.method.eq(get)-action reset_action
```


Binden Sie die Appqoe-Richtlinie an den virtuellen Lastenausgleich

Wenn ein Backend-Server eine TCP-Paketanforderung zurücksetzt und der virtuelle Lastausgleichsserver die Anforderung an den nächsten verfügbaren Dienst weiterleiten soll, müssen Sie den virtuellen Lastausgleichsserver an die AppQoE-Richtlinie binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Beispiel:

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

Konfigurieren Sie den Wiederholungsversuch für POST-Anfragen

Sie müssen immer vorsichtig sein, wenn Sie Balancing-Anfragen neu laden, die Daten in den Backend-Server schreiben. Stellen Sie bei solchen Anfragen sicher, dass die Inhaltslänge kurz ist. Wenn die Inhaltslänge lang ist, kann dies zu einem Ressourcenverbrauch führen. Folgen Sie den unten angegebenen Schritten, um den Reload-Balancing für POST-Anfragen zu konfigurieren.

1. Aktivieren Sie AppQoE
2. Add AppQoE action
3. Add AppQoE policy
4. Binden Sie die AppQoE-Richtlinie an den virtuellen Lastausgleichsserver

Aktivieren Sie AppQoE

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature appqoe
```

Appqoe-Aktion hinzufügen

Sie müssen eine AppQoE-Aktion hinzufügen, die Sie nach einem TCP-Reset und der Anzahl der Wiederholungsversuche erneut versuchen können.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Beispiel:

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```


Appqoe-Richtlinie hinzufügen

Um AppQoE zu implementieren, müssen Sie die AppQoE-Richtlinie konfigurieren, um zu definieren, wie die Verbindungen in einer bestimmten Warteschlange in die Warteschlange gestellt werden.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add appqoe policy reset_policy -rule HTTP.REQ.CONTENT_LENGTH.le(2000)-
action reset_action
```

> **Hinweis:**
>
> Sie können diese Konfiguration verwenden, wenn Sie es vorziehen, die Funktion zur erneuten Anforderung von Anfragen für Inhalte mit einer Länge von weniger als 2000 einzuschränken.

Binden von virtuellen Lastenausgleichsserver an AppQoE-Richtlinie

Wenn ein Backend-Server eine TCP-Paketanforderung zurücksetzt und Sie möchten, dass der virtuelle Lastausgleichsserver die Anfrage über eine bestimmte Warteschlange an den nächsten verfügbaren Dienst weiterleitet, müssen Sie den virtuellen Lastausgleichsserver an die AppQOE-Richtlinie binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

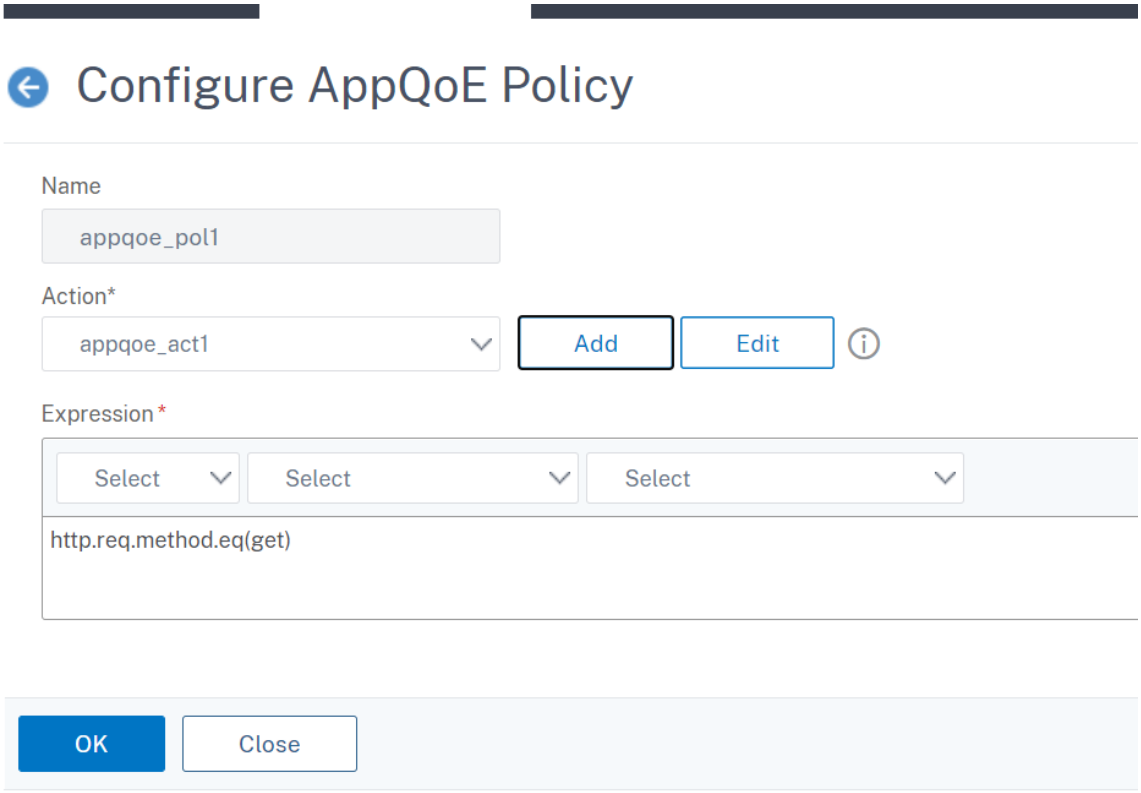
Beispiel:

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

Konfigurieren Sie die AppQoE-Richtlinie für den erneuten Versuch von Anfragen mithilfe der NetScaler GUI

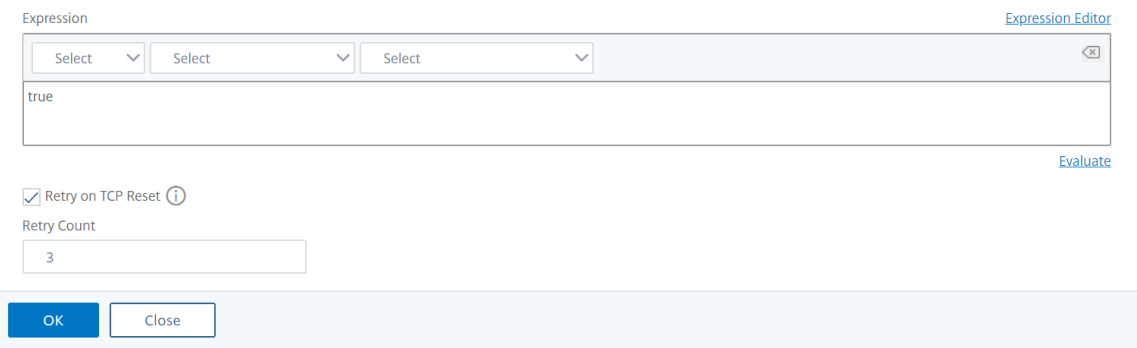
1. **Navigieren Sie zu**AppExpert**>**AppQoE**> Policies.**
2. Klicken Sie auf der Seite **AppQoE-Richtlinien** auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **AppQoE-Richtlinie erstellen“ die folgenden Parameter ein** : a. Name. AppQoE-Richtlinienname
   b. Aktion. Fügen Sie eine Aktion hinzu oder bearbeiten Sie sie. Informationen zum Erstellen einer Aktion finden Sie im Abschnitt .
   c. Ausdruck. Wählen oder geben Sie den Richtlinienausdruck `HTTP.REQ.CONTENT_LENGTH.le (2000)` ein.

4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren Sie die AppQoE-Aktion für den erneuten Anforderungsausgleich mithilfe der NetScaler GUI

1. **Navigieren Sie zu**AppExpert**>**AppQoE**> Action.**
2. Klicken Sie auf der Seite **AppQoE-Aktionen** auf **Hinzufügen**.
3. Stellen Sie auf der Seite **AppQoE-Aktion erstellen** die folgenden Parameter für den erneuten Versuch beim TCP-Reset ein:
   a. Versuchen Sie es erneut beim TCP-Reset. Aktivieren Sie das Kontrollkästchen, um die Wiederholungsaktion für den TCP-Reset zu aktivieren.
   b. Anzahl der Wiederholungsversuche. Geben Sie die Anzahl der Wiederholungsversuche ein.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren der Wiederholung der Anfrage für die GET-Methode beim Zurücksetzen des Backend-Servers bei TCP-SYN-Einrichtung

Die CLI- und GUI-Konfiguration ähnelt den Schritten, die für die GET-Methode verfolgt werden. Weitere Informationen finden Sie unter Abschnitt Konfigurieren von Anforderungstversuchen für GET-Methode. wenn der Back-End-Server einen Verbindungsabschnitt zurücksetzt.

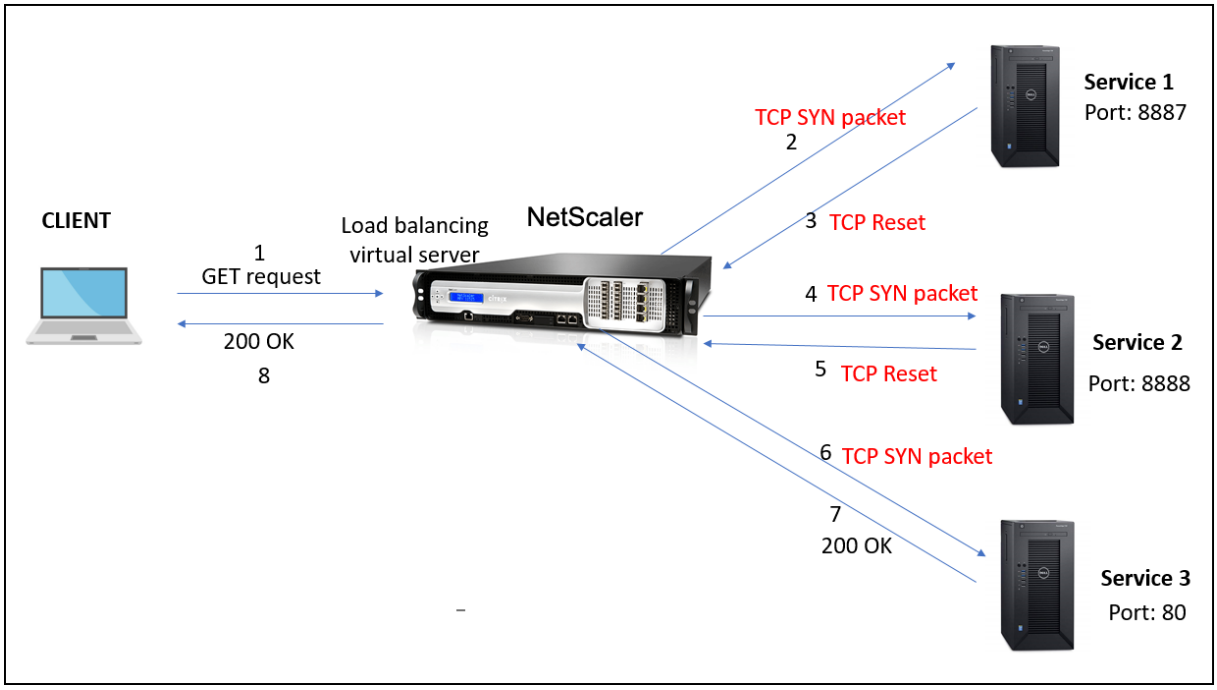
Wiederholungsversuche anfordern, wenn der Backend-Server während der Verbindungseinrichtung die TCP-Verbindung zurücksetzt

August 19, 2021

Wenn ein Back-End-Server eine TCP-Verbindung während des Verbindungsaufbaus zurücksetzt, leitet die Funktion zur Wiederholung der Anforderung die Anfrage an den nächsten verfügbaren Server weiter, anstatt den Reset an den Client zu senden. Durch den Reload-Balancing speichert der Client RTT, wenn die Appliance dieselbe Anfrage an den nächsten verfügbaren Dienst initiiert.

So funktioniert die Wiederholung der Anfrage, wenn der Back-End-Server eine TCP-Verbindung bei der SYN-Einrichtung zurücksetzt

Das folgende Diagramm zeigt, dass die Komponenten miteinander interagieren:



1. Der Prozess beginnt mit der Aktivierung der Appqoe-Funktion auf Ihrer Appliance.
2. Wenn der Client eine HTTP- oder HTTPS-Anfrage sendet, initiiert der virtuelle Lastausgleichsserver eine Verbindung zum Backend-Server.
3. Wenn der angeforderte Dienst bei TCP-SYN-Einrichtung nicht verfügbar ist, setzt der Backend-Server die TCP-Verbindung zurück.
4. Wenn in der Appqoe-Konfiguration “Wiederholung” mit der gewünschten Anzahl von Wiederholungsversuchen aktiviert ist, verwendet der virtuelle Lastausgleichsserver den konfigurierten Load Balancing-Algorithmus, um die Anforderung an den nächsten verfügbaren Anwendungsserver weiterzuleiten.
5. Nachdem der virtuelle Lastausgleichsserver die Antwort erhalten hat, leitet die Appliance die Antwort an den Client weiter.
6. Wenn die verfügbaren Back-End-Server gleich oder kleiner als die Wiederholungsanzahl sind und wenn alle Server einen Reset senden, würde die Appliance einen internen 500-Serverfehler beantworten. Betrachten Sie ein Szenario mit fünf verfügbaren Servern und der Wiederholungsanzahl, die auf sechs festgelegt ist. Wenn alle fünf Server die Verbindung zurücksetzen, gibt die Appliance einen internen 500-Serverfehler an den Client zurück.
7. Wenn die Anzahl der Back-End-Server höher ist als die Wiederholungsanzahl und wenn die Back-End-Server die Verbindung bei TCP-SYN-Einrichtung zurücksetzen, leitet die Appliance den Reset an den Client weiter. Stellen Sie sich ein Szenario mit drei Back-End-Servern und der Wiederholungsanzahl vor, die auf zwei festgelegt ist. Wenn die drei Server die Verbindung zurücksetzen, sendet die Appliance ein Reset-Paket an den Client.

Konfigurieren der Wiederholung der Anforderung (GET und POST-Methode), wenn der Back-End-Server bei TCP-SYN-Einrichtung zurückgesetzt wird

Die CLI- und GUI-Konfiguration ähnelt den Schritten, die für die GET- und POST-Methode befolgt werden. Weitere Informationen finden Sie unter Konfigurieren der Wiederholung der Anforderung für die GET-Methode, Konfigurieren der Wiederholung der Anforderung für die POST-Methode, wenn der Back-End-Server einen Verbindungsabschnitt zurücksetzt.

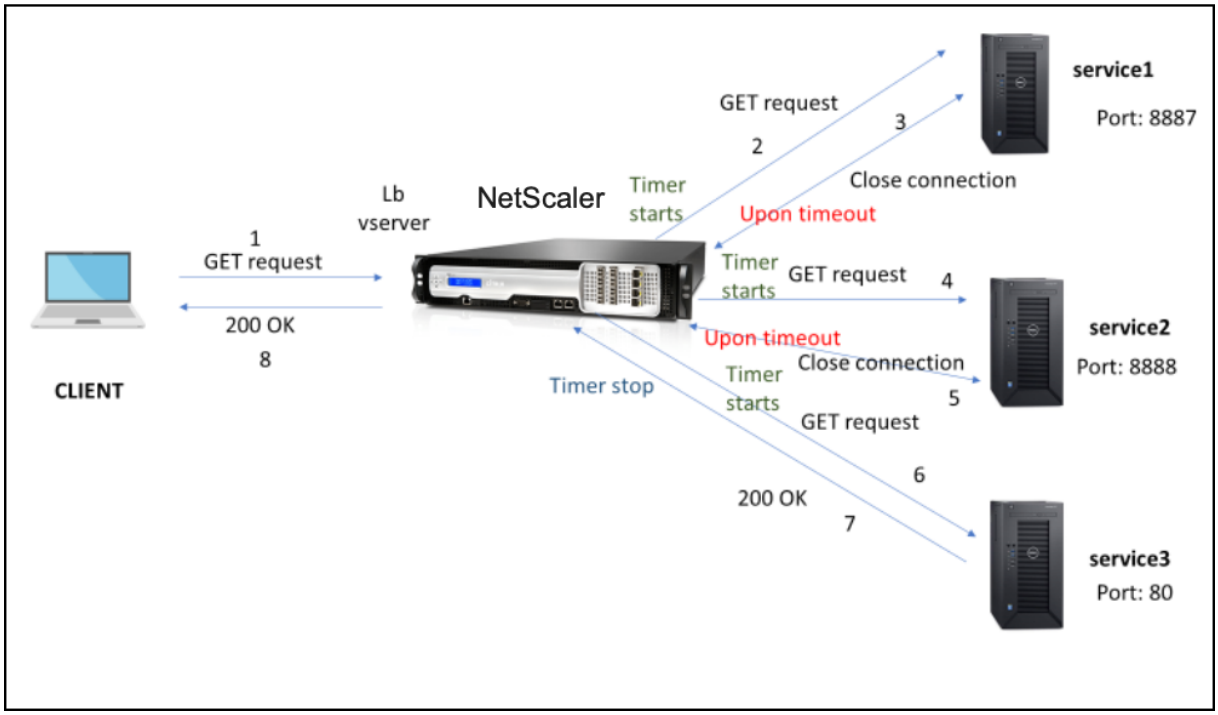
Wiederholungsversuch anfordern, wenn die Antwort des Backend-Servers abgelaufen ist

May 11, 2023

Eine Wiederholung der Anforderung ist für ein weiteres Szenario verfügbar. Wenn ein Backend-Server mehr Zeit benötigt, um auf Anfragen zu antworten, führt die Appliance bei Timeout einen erneuten Lastausgleich durch und leitet die Anfrage an den nächsten verfügbaren Server weiter.

So funktioniert die Wiederholung von Anfragen, wenn die Antwort des Backend-Servers zu einem Timeout kommt

Das folgende Diagramm zeigt, wie die Komponenten miteinander interagieren:



1. Der Vorgang beginnt mit der Aktivierung der Appqoe-Funktion auf Ihrer Appliance.

2. Die Appqoe-Konfiguration hat den Parameter „RetryOnTimeout“ in Millisekunden.
3. Wenn die Appliance eine Anfrage sendet und der Server mehr Zeit benötigt, um zu antworten, führt die Appliance einen Neulastausgleich auf der Grundlage des konfigurierten Timeout-Werts durch. Die Appliance setzt die Verbindung zurück, wählt einen anderen Dienst und leitet die Anfrage weiter, anstatt auf die Serverantwort zu warten.
4. Nachdem der virtuelle Lastausgleichsserver die Antwort erhalten hat, leitet die Appliance die Antwort an den Client weiter. Die Verwendung eines Timeout-Parameters verhindert, dass die Appliance weiter auf eine Serverantwort wartet, was zu einem erhöhten RTT führt.
5. Wenn die verfügbaren Backend-Server gleich oder kleiner als die Anzahl der Wiederholungsversuche sind und wenn bei allen Servern ein Timeout für die Anfrage auftritt, würde die Appliance einen internen Serverfehler von 500 melden. Betrachten Sie ein Szenario mit fünf verfügbaren Servern und der Wiederholungsanzahl, die auf sechs festgelegt ist. Wenn bei allen fünf Servern ein Timeout für die Anfrage auftritt, gibt die Appliance einen internen Serverfehler von 500 an den Client zurück.
6. In ähnlicher Weise wartet die Appliance auf den letzten Dienst, wenn die Anzahl der Backend-Server die Anzahl der Wiederholungsversuche übersteigt und wenn der Backend-Server bei einer Anfrage ein Timeout durchführt, bis der Server eine Antwort sendet oder die Client-Leerlaufverbindung abläuft. Stellen Sie sich ein Szenario mit drei Back-End-Servern und der Wiederholungsanzahl vor, die auf zwei festgelegt ist. Wenn alle drei Server auf die Anfrage hin ein Timeout haben, wartet die Appliance weiter auf den dritten Dienst, bis der Server eine Antwort sendet oder die inaktive Client-Verbindung abläuft.

Konfigurieren Sie den Wiederholungsversuch (GET- und POST-Methode), wenn die Antwort des Backend-Servers zu einem Timeout führt

Um die Wiederholungsanfrage für die GET-Methode bei Timeout zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

1. Appqoe aktivieren
2. Appqoe-Aktion konfigurieren
3. Appqoe-Richtlinie hinzufügen
4. Binden Sie die Appqoe-Richtlinie an den virtuellen Lastenausgleich

> **Hinweis:**
>
> Das Szenario „Wiederholungsversuch bei Timeout anfordern“ gilt auch für die POST-Methode.

Appqoe aktivieren

Geben Sie in der Befehlszeile Folgendes ein:

```
enable ns feature appqoe
```


Appqoe-Aktion für Timeout hinzufügen

Sie müssen die appqoe-Aktion so konfigurieren, dass sie es bei Timeout erneut versucht, und die Anzahl der Wiederholungsversuche definieren.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appqoe action <name> -retryOnTimeout <msecs> -numRetries <positive_integer
>
```

Beispiel:

```
add appqoe action appact1 -retryOnTimeout 35 -numRetries 5
```

Appqoe-Richtlinie hinzufügen

Um appqoe zu implementieren, müssen Sie die Appqoe-Richtlinie konfigurieren, um zu definieren, wie die Verbindungen in die Warteschlange gestellt werden.

Geben Sie in der Befehlszeile Folgendes ein:

```
add appqoe policy <name> -rule <rule> -action <name>
```

Beispiel:

```
add appqoe policy timeout_policy -rule http.req.method.eq(get)-action
appact1
```

Binden Sie die Appqoe-Richtlinie an den virtuellen Lastenausgleich

Wenn ein Backend-Server lange braucht, um zu antworten, und wenn Sie möchten, dass der virtuelle Lastausgleichsserver die Anfrage an den nächsten verfügbaren Dienst weiterleitet, müssen Sie die Appqoe-Richtlinie an den virtuellen Balancing-Server binden.

Geben Sie in der Befehlszeile Folgendes ein:

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Beispiel:

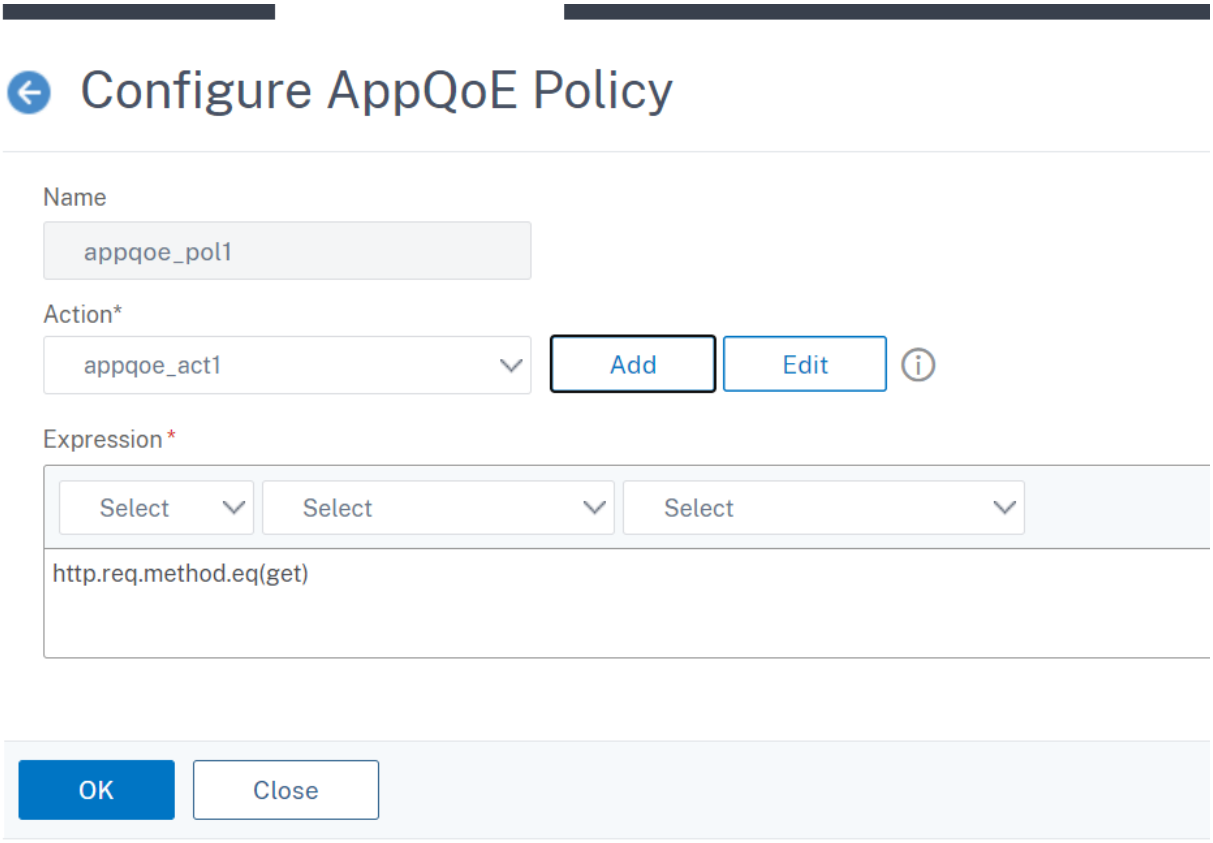
```
bind lb vserver v1 -policyName timeout_policy -type REQUEST -priority 1
```

Konfigurieren Sie die AppQoE-Richtlinie für das Re-Loadbalancing bei Timeout mithilfe der NetScaler-GUI

1. Navigieren Sie zu **AppExpert > AppQoE**> Policies.

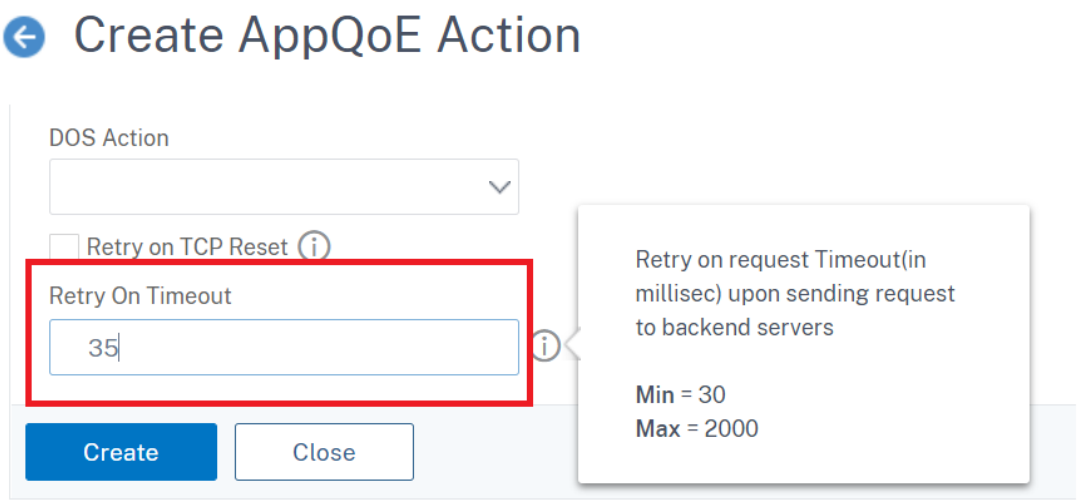
2. Klicken Sie auf der Seite **AppQoE-Richtlinien** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Create an AppQoE Policy** die folgenden Parameter fest:

   a. Name. AppQoE-Richtlinienname
   b. Aktion. Fügen Sie eine Aktion hinzu oder bearbeiten Sie sie. Informationen zum Erstellen einer neuen Aktion finden Sie im Abschnitt AppQoE-Aktion erstellen.
   c. Ausdruck. Wählen Sie den Richtlinienausdruck „http.req.method.eq (get)“ aus oder geben Sie ihn ein.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren Sie die AppQoE-Aktion für die Wiederholung von Anfragen mithilfe der NetScaler-GUI

1. Navigieren Sie zu **AppExpert > AppQoE**> Action.
2. Klicken Sie auf der Seite **AppQoE-Aktionen** auf **Hinzufügen**.
3. Stellen Sie auf der Seite „ **AppQoE-Aktion erstellen** “ den folgenden Parameter für den Wiederholungsversuch beim Antworttimeout des Backend-Servers ein: a.
   Versuchen Sie es erneut bei Timeout. Versuchen Sie es erneut, wenn das Anforderungs-Timeout (in Millisekunden) abgelaufen ist, wenn eine Anfrage an Backend-Server gesendet wird.
4. Klicken Sie auf **Erstellen** und **Schließen**.



TCP-Optimierung

July 24, 2023

TCP verwendet die folgenden Optimierungstechniken und Strategien (oder Algorithmen) zur Überlastungskontrolle, um Netzwerkengpässe bei der Datenübertragung zu vermeiden.

Strategien zur Staukontrolle

TCP wird seit langem verwendet, um Internetverbindungen herzustellen und zu verwalten, Übertragungsfehler zu behandeln und Webanwendungen reibungslos mit Client-Geräten zu verbinden. Der Netzwerkverkehr ist jedoch schwieriger zu kontrollieren, da der Paketverlust nicht nur von der Überlastung des Netzwerks abhängt und eine Überlastung nicht unbedingt zu Paketverlusten führt. Um die Überlastung zu messen, sollte sich ein TCP-Algorithmus daher sowohl auf den Paketverlust als auch auf die Bandbreite konzentrieren.

PRR-Algorithmus (Proportional Rate Recovery)

TCP-Schnellwiederherstellungsmechanismen reduzieren die durch Paketverluste verursachte Weblatenz. Der neue PRR-Algorithmus (Proportional Rate Recovery) ist ein schneller Wiederherstellungsalgorithmus, der TCP-Daten während einer Loss Recovery auswertet. Das Muster ist dem Rate-Halving nachempfunden, indem der Bruchteil verwendet wird, der für das vom Staukontrollalgorithmus gewählte Zielfenster geeignet ist. Dadurch wird die Fensteranpassung minimiert, und die tatsächliche Fenstergröße am Ende der Wiederherstellung liegt nahe am Schwellenwert für langsamen Start (ssthresh).

Schnelles TCP-Öffnen (TFO)

TCP Fast Open (TFO) ist ein TCP-Mechanismus, der einen schnellen und sicheren Datenaustausch zwischen einem Client und einem Server während des ersten TCP-Handshakes ermöglicht. Diese Funktion ist als TCP-Option im TCP-Profil verfügbar, das an einen virtuellen Server einer NetScaler-Appliance gebunden ist. TFO verwendet ein TCP-Fast-Open-Cookie (ein Sicherheitscookie), das die NetScaler-Appliance generiert, um den Client zu validieren und zu authentifizieren, der eine TFO-Verbindung zum virtuellen Server initiiert. Mithilfe dieses TFO-Mechanismus können Sie die Netzwerklatenz einer Anwendung um die Zeit reduzieren, die für einen vollständigen Roundtrip erforderlich ist, wodurch die Verzögerung bei kurzen TCP-Übertragungen erheblich reduziert wird.

So funktioniert TFO

Wenn ein Client versucht, eine TFO-Verbindung herzustellen, enthält er ein TCP-Fast-Open-Cookie mit dem anfänglichen SYN-Segment, um sich zu authentifizieren. Wenn die Authentifizierung erfolgreich ist, kann der virtuelle Server auf der NetScaler-Appliance Daten in das SYN-ACK-Segment aufnehmen, obwohl er das letzte ACK-Segment des Drei-Wege-Handshakes nicht empfangen hat. Dadurch wird im Vergleich zu einer normalen TCP-Verbindung, für die ein dreifacher Handshake erforderlich ist, bevor Daten ausgetauscht werden können, bis zu einem kompletten Round-Trip eingespart.

Ein Client und ein Backend-Server führen die folgenden Schritte durch, um eine TFO-Verbindung herzustellen und Daten während des ersten TCP-Handshakes sicher auszutauschen.

1. Wenn der Client kein TCP-Fast-Open-Cookie hat, um sich zu authentifizieren, sendet er eine Fast Open Cookie-Anfrage im SYN-Paket an den virtuellen Server auf der NetScaler-Appliance.
2. Wenn die TFO-Option in dem an den virtuellen Server gebundenen TCP-Profil aktiviert ist, generiert die Appliance ein Cookie (indem die IP-Adresse des Clients mit einem geheimen Schlüssel verschlüsselt wird) und antwortet dem Client mit einem SYN-ACK, das das generierte Fast Open Cookie in einem TCP-Optionsfeld enthält.
3. Der Client speichert das Cookie für zukünftige TFO-Verbindungen zu demselben virtuellen Server auf der Appliance.
4. Wenn der Client versucht, eine TFO-Verbindung zu demselben virtuellen Server herzustellen, sendet er SYN, das das zwischengespeicherte Fast Open Cookie (als TCP-Option) zusammen mit HTTP-Daten enthält.
5. Die NetScaler-Appliance validiert das Cookie, und wenn die Authentifizierung erfolgreich ist, akzeptiert der Server die Daten im SYN-Paket und bestätigt das Ereignis mit einem SYN-ACK, einem TFO-Cookie und einer HTTP-Antwort.

> **Hinweis:**
>
> Schlägt die Client-Authentifizierung fehl, löscht der Server die Daten und bestätigt das Ereignis nur mit einem SYN, das auf ein Sitzungs-Timeout hinweist.

1. Wenn auf der Serverseite die TFO-Option in einem an einen Dienst gebundenen TCP-Profil aktiviert ist, bestimmt die NetScaler-Appliance, ob das TCP Fast Open Cookie in dem Dienst vorhanden ist, zu dem sie versucht, eine Verbindung herzustellen.
2. Wenn das TCP Fast Open Cookie nicht vorhanden ist, sendet die Appliance eine Cookie-Anfrage im SYN-Paket.
3. Wenn der Backend-Server das Cookie sendet, speichert die Appliance das Cookie im Serverinformationscache.
4. Wenn die Appliance bereits über ein Cookie für das angegebene Ziel-IP-Paar verfügt, ersetzt sie das alte Cookie durch das neue.
5. Wenn das Cookie im Serverinformationscache verfügbar ist, wenn der virtuelle Server versucht, mithilfe derselben SNIP-Adresse erneut eine Verbindung zu demselben Backend-Server herzustellen, kombiniert die Appliance die Daten im SYN-Paket mit dem Cookie und sendet sie an den Backend-Server.
6. Der Backend-Server bestätigt das Ereignis sowohl mit Daten als auch mit einem SYN.

Hinweis: Wenn der Server das Ereignis nur mit einem SYN-Segment bestätigt, sendet die NetScaler-Appliance das Datenpaket sofort erneut, nachdem das SYN-Segment und die TCP-Optionen aus dem ursprünglichen Paket entfernt wurden.

Konfiguration von TCP fast open

Um die Funktion TCP Fast Open (TFO) zu verwenden, aktivieren Sie die Option TCP Fast Open im entsprechenden TCP-Profil und setzen Sie den Parameter TFO Cookie Timeout auf einen Wert, der den Sicherheitsanforderungen für dieses Profil entspricht.

Aktivieren oder deaktivieren Sie TFO mithilfe der CLI

Geben Sie in der Befehlszeile einen der folgenden Befehle ein, um TFO in einem neuen oder vorhandenen Profil zu aktivieren oder zu deaktivieren.

Hinweis: Der Standardwert ist DISABLED.

```
1     add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
2     set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
3     unset tcpprofile <TCP Profile Name> - tcpFastOpen
4     Examples
5     add tcpprofile Profile1 - tcpFastOpen
6     Set tcpprofile Profile1 - tcpFastOpen Enabled
7     unset tcpprofile Profile1 - tcpFastOpen
8 <!--NeedCopy-->
```


So legen Sie den Timeout-Wert für das TCP-FastOpen-Cookie mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
1     set tcpparam  - tcpfastOpenCookieTimeout <Timeout Value>
2     Example
3     set tcpprofile  - tcpfastOpenCookieTimeout 30secs
4 <!--NeedCopy-->
```

So konfigurieren Sie das TCP Fast Open mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Markieren Sie auf der Seite „ **TCP-Profil konfigurieren** “ das Kontrollkästchen **TCP Fast Open** .
3. Klicke auf **OK** und dann auf **Fertig**.

So konfigurieren Sie den TCP-Fast-Cookie-Timeout-Wert mithilfe der GUI

Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen** > **TCP-Parameter ändern** und dann zur Seite „ **TCP-Parameter konfigurieren**“, um den Timeout-Wert für das TCP-Fast-Open-Cookie festzulegen.

TCP-HyStart

Ein neuer TCP-Profilparameter, HyStart, aktiviert den HyStart-Algorithmus, bei dem es sich um einen langsamen Start-Algorithmus handelt, der dynamisch einen sicheren Punkt für die Beendigung bestimmt (ssthresh). Es ermöglicht einen Übergang zur Vermeidung von Engpässen ohne starke Paketverluste. Dieser neue Parameter ist standardmäßig deaktiviert.

Wenn ein Stau erkannt wird, geht HyStart in eine Phase zur Vermeidung von Staus über. Wenn Sie es aktivieren, erhalten Sie einen besseren Durchsatz in Hochgeschwindigkeitsnetzwerken mit hohem Paketverlust. Dieser Algorithmus trägt dazu bei, bei der Verarbeitung von Transaktionen eine nahezu maximale Bandbreite aufrechtzuerhalten. Es kann daher den Durchsatz verbessern.

Konfiguration von TCP HyStart

Um die HyStart-Funktion zu verwenden, aktivieren Sie die Cubic HyStart-Option im entsprechenden TCP-Profil.

So konfigurieren Sie HyStart mithilfe der Befehlszeilenschnittstelle (CLI)

Geben Sie an der Befehlszeile einen der folgenden Befehle ein, um HyStart in einem neuen oder vorhandenen TCP-Profil zu aktivieren oder zu deaktivieren.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Beispiele:

```
    add tcpprofile profile1 -hystart ENABLED
    set tcpprofile profile1 -hystart ENABLED
    unset tcprofile profile1 -hystart
<!--NeedCopy-->
```

So konfigurieren Sie die HyStart-Unterstützung mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite „ **TCP-Profil konfigurieren** “ das Kontrollkästchen **Cubic Hystart** .
3. Klicke auf **OK** und dann auf **Fertig**.

Steuerung der TCP-Burstrate

Es wird beobachtet, dass TCP-Steuerungsmechanismen zu einem sprunghaften Verkehrsfluss in Hochgeschwindigkeits-Mobilfunknetzen führen können, was sich negativ auf die Gesamteffizienz des Netzwerks auswirkt. Aufgrund von Mobilfunkbedingungen wie Überlastung oder Layer-2-Übertragung von Daten kommen TCP-Bestätigungen verklumpt beim Absender an, was einen Übertragungsschub auslöst. Diese Gruppen aufeinanderfolgender Pakete, die mit einer kurzen Lücke zwischen den Paketen gesendet werden, wird als TCP-Paket-Burst bezeichnet. Zur Vermeidung von Datenausbrüchen verwendet die NetScaler-Appliance eine TCP-Burst-Rate-Control-Technik. Bei dieser Technik werden die Daten für eine gesamte Roundtrip-Zeit gleichmäßig im Netzwerk verteilt, sodass die Daten nicht in einem Burst-Modus gesendet werden. Durch die Verwendung dieser Technik zur Burst-Rate-Steuerung können Sie einen besseren Durchsatz und niedrigere Paketabwurfraten erzielen.

So funktioniert die TCP-Burst-Rate-Steuerung

In einer NetScaler-Appliance verteilt diese Technik die Übertragung eines Pakets gleichmäßig über die gesamte Dauer der Roundtrip-Time (RTT). Dies wird durch die Verwendung eines TCP-Stacks und

eines Netzwerkpaketplaners erreicht, der die verschiedenen Netzwerkbedingungen identifiziert, um Pakete für laufende TCP-Sitzungen auszugeben und so die Bursts zu reduzieren.

Beim Absender kann der Sender die Übertragung von Paketen verzögern, anstatt Pakete sofort nach Erhalt einer Bestätigung zu übertragen, um sie mit der Geschwindigkeit zu verteilen, die vom Scheduler (dynamische Konfiguration) oder vom TCP-Profil (feste Konfiguration) definiert ist.

Konfiguration der TCP-Burst-Rate-Steuerung

Um die Option TCP-Burst Rate Control im entsprechenden TCP-Profil zu verwenden und die Burst-Rate-Control-Parameter festzulegen.

So stellen Sie die TCP-Burstratensteuerung mithilfe der Befehlszeile ein

Stellen Sie in der Befehlszeile einen der folgenden TCP-Burst Rate Control-Befehle ein, die in einem neuen oder vorhandenen Profil konfiguriert sind.

Hinweis: Der Standardwert ist DISABLED.

```
add tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
    | Fixed

set tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
    | Fixed

unset tcpprofile <TCP Profile Name> -burstRateControl Disabled |
    Dynamic | Fixed
<!--NeedCopy-->
```

Hierbei gilt:

Deaktiviert — Wenn die Burst-Rate-Steuerung deaktiviert ist, führt eine NetScaler-Appliance außer der MaxBurst-Einstellung kein Burst-Management durch.

Behoben — Wenn die TCP-Burst-Rate-Steuerung auf Fest gesetzt ist, verwendet die Appliance den im TCP-Profil angegebenen Wert für die Senderate der TCP-Verbindungsnutzlast.

Dynamisch — Wenn die Burst Rate Control „Dynamisch“ ist, wird die Verbindung auf der Grundlage verschiedener Netzwerkbedingungen reguliert, um TCP-Bursts zu reduzieren. Dieser Modus funktioniert nur, wenn sich die TCP-Verbindung im ENDPOINT-Modus befindet. Wenn die dynamische Burst-Rate-Steuerung aktiviert ist, ist der MaxBurst-Parameter des TCP-Profils nicht wirksam.

```
add tcpProfile  profile1 -burstRateControl Disabled

set tcpProfile profile1 -burstRateControl Dynamic
```



```
4
5 unset tcpProfile profile1 -burstRateControl Fixed
6 <!--NeedCopy-->
```

So legen Sie die TCP-Burst-Rate-Control-Parameter mithilfe der Befehlszeilenschnittstelle fest

Geben Sie in der Befehlszeile Folgendes ein:

```
1     set ns tcpprofile nstcp_default_profile  -burstRateControl <type of
          burst rate control>  -tcprate <TCP rate> -rateqmax <maximum
         bytes in queue>
2
3     T1300-10-2> show ns tcpprofile nstcp_default_profile
4             Name: nstcp_default_profile
5             Window Scaling status:  ENABLED
6             Window Scaling factor: 8
7             SACK status: ENABLED
8             MSS: 1460
9             MaxBurst setting: 30 MSS
10            Initial cwnd setting: 16 MSS
11            TCP Delayed-ACK Timer: 100 millisec
12            Nagle's Algorithm: DISABLED
13            Maximum out-of-order packets to queue: 15000
14            Immediate ACK on PUSH packet: ENABLED
15            Maximum packets per MSS: 0
16            Maximum packets per retransmission: 1
17            TCP minimum RTO in millisec: 1000
18            TCP Slow start increment: 1
19            TCP Buffer Size: 8000000 bytes
20            TCP Send Buffer Size: 8000000 bytes
21            TCP Syncookie: ENABLED
22            Update Last activity on KA Probes: ENABLED
23            TCP flavor: BIC
24            TCP Dynamic Receive Buffering: DISABLED
25            Keep-alive probes: ENABLED
26            Connection idle time before starting keep-alive probes: 900
                  seconds
27            Keep-alive probe interval: 75 seconds
28            Maximum keep-alive probes to be missed before dropping
                 connection: 3
29            Establishing Client Connection: AUTOMATIC
30            TCP Segmentation Offload: AUTOMATIC
31            TCP Timestamp Option: DISABLED
```



```
32              RST window attenuation (spoof protection): ENABLED
33              Accept RST with last acknowledged sequence number: ENABLED
34              SYN spoof protection: ENABLED
35              TCP Explicit Congestion Notification: DISABLED
36              Multipath TCP: DISABLED
37              Multipath TCP drop data on pre-established subflow:
                    DISABLED
38              Multipath TCP fastopen: DISABLED
39              Multipath TCP session timeout: 0 seconds
40              DSACK: ENABLED
41              ACK Aggregation: DISABLED
42              FRTO: ENABLED
43              TCP Max CWND : 4000000 bytes
44              FACK: ENABLED
45              TCP Optimization mode: ENDPOINT
46              TCP Fastopen: DISABLED
47              HYSTART: DISABLED
48              TCP dupack threshold: 3
49              Burst Rate Control: Dynamic
50              TCP Rate: 0
51              TCP Rate Maximum Queue: 0
52  <!--NeedCopy-->
```

So konfigurieren Sie die TCP-Burst Rate Control mithilfe der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Wählen Sie auf der Seite „ **TCP-Profil konfigurieren** “ in der Dropdownliste die Option **TCP Burst Control** aus:
   a) BurstRateCntrl
   b) CreditBytePrms
   c) RateBytePerms
   d) RateSchedulerQ
3. Klicke auf **OK** und dann auf **Fertig**.

PAWS-Algorithmus (Schutz vor Wrapped Sequence)

Wenn Sie die TCP-Zeitstempeloption im Standard-TCP-Profil aktivieren, verwendet die NetScaler-Appliance den PAWS-Algorithmus (Protection Against Wrapped Sequence), um alte Pakete zu identifizieren und abzulehnen, deren Sequenznummern sich im Empfangsfenster der aktuellen TCP-Verbindung befinden, weil die Sequenz „eingeschlossen“ wurde (ihren Maximalwert erreicht und bei 0 neu gestartet).

Wenn eine Netzwerküberlastung ein Nicht-SYN-Datenpaket verzögert und Sie eine neue Verbindung öffnen, bevor das Paket eintrifft, kann das Umwickeln von Sequenznummern dazu führen, dass die neue Verbindung das Paket als gültig akzeptiert, was zu Datenbeschädigungen führt. Wenn jedoch die TCP-Zeitstempeloption aktiviert ist, wird das Paket verworfen.

Die TCP-Zeitstempeloption ist standardmäßig deaktiviert. Wenn Sie es aktivieren, vergleicht die Appliance den TCP-Zeitstempel (seg.TSVal) im Header eines Pakets mit dem aktuellen Zeitstempelwert (ts.Recent). Wenn seg.tsVal gleich oder größer als ts.Recent ist, wird das Paket verarbeitet. Andernfalls verwirft die Appliance das Paket und sendet eine Korrekturbestätigung.

So funktioniert PAWS

Der PAWS-Algorithmus verarbeitet alle eingehenden TCP-Pakete einer synchronisierten Verbindung wie folgt:

1. Wenn `SEG.TSval` < `Ts.recent`: Das eingehende Paket ist nicht akzeptabel. PAWS sendet eine Bestätigung (wie in RFC-793 angegeben) und verwirft das Paket. Hinweis: Das Senden eines ACK-Segments ist erforderlich, um die TCP-Mechanismen zur Erkennung und Wiederherstellung von halboffenen Verbindungen beizubehalten.
2. Wenn sich das Paket außerhalb des Fensters befindet: PAWS lehnt das Paket ab, wie bei der normalen TCP-Verarbeitung.
3. If `SEG.TSval` > `Ts.recent`: `PAWS` akzeptiert das Paket und verarbeitet es.
4. Wenn `SEG.TSval` <= `Last.ACK.sent`(das ankommende Segment erfüllt): PAWS kopiert den Wert `SEG.TSval` nach `Ts.recent`.
5. Wenn das Paket in der richtigen Reihenfolge ist: PAWS akzeptiert das Paket.
6. Wenn das Paket nicht in der richtigen Reihenfolge ist: Das Paket wird wie ein normales TCP-Segment innerhalb des Fensters behandelt, das nicht in der richtigen Reihenfolge ist. Zum Beispiel könnte es für eine spätere Lieferung in die Warteschlange gestellt werden.
7. Wenn der Wert `Ts.recent` länger als 24 Tage inaktiv ist: Die Gültigkeit von `Ts.recent` wird überprüft, wenn die PAWS-Zeitstempelprüfung fehlschlägt. Wenn sich herausstellt, dass der Ts.recent-Wert ungültig ist, wird das Segment akzeptiert und `PAWS rule` aktualisiert `Ts.recent` mit dem TSval-Wert aus dem neuen Segment.

So aktivieren oder deaktivieren Sie den TCP-Zeitstempel mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
`set nstcpprofile nstcp_default_profile -TimeStamp (ENABLED | DISABLED)
    `
```

So aktivieren oder deaktivieren Sie TCP-Zeitstempel mit der GUI

Navigieren Sie zu **System** > **Profil** > **TCP-Profil**, wählen Sie das Standard-TCP-Profil aus, klicken Sie auf **Bearbeiten**und aktivieren oder deaktivieren Sie das Kontrollkästchen **TCP-Zeitstempel** .

Optimierungstechniken

TCP verwendet die folgenden Optimierungstechniken und -methoden für optimierte Flusskontrollen.

Richtlinienbasierte TCP-Profilauswahl

Der Netzwerkverkehr ist heute vielfältiger und bandbreitenintensiver als je zuvor. Angesichts des erhöhten Datenverkehrs ist der Effekt, den Quality of Service (QoS) auf die TCP-Leistung hat, erheblich. Um die QoS zu verbessern, können Sie jetzt AppQoE-Richtlinien mit verschiedenen TCP-Profilen für verschiedene Klassen von Netzwerkverkehr konfigurieren. Die AppQoE-Richtlinie klassifiziert den Datenverkehr eines virtuellen Servers, um ein TCP-Profil zuzuordnen, das für einen bestimmten Verkehrstyp wie 3G, 4G, LAN oder WAN optimiert ist.

Um dieses Feature zu verwenden, erstellen Sie für jedes TCP-Profil eine Richtlinienaktion, ordnen Sie eine Aktion AppQoE-Richtlinien zu und binden Sie die Richtlinien an die virtuellen Server mit Lastenausgleich.

Informationen zur Verwendung von Abonnentenattributen zur TCP-Optimierung finden Sie unter Richtlinienbasiertes TCP-Profil.

Konfigurieren der Richtlinienbasierten TCP-Profilauswahl

Die Konfiguration der richtlinienbasierten TCP-Profilauswahl umfasst die folgenden Aufgaben:

- AppQoE aktivieren. Bevor Sie die TCP-Profilfunktion konfigurieren, müssen Sie die AppQoE-Funktion aktivieren.
- AppQoE-Aktion wird hinzugefügt. Nachdem Sie die AppQoE-Funktion aktiviert haben, konfigurieren Sie eine AppQoE-Aktion mit einem TCP-Profil.
- Konfiguration der AppQoE-basierten TCP-Profilauswahl. Um die TCP-Profilauswahl für verschiedene Verkehrsklassen zu implementieren, müssen Sie AppQoE-Richtlinien konfigurieren, anhand derer Ihr NetScaler die Verbindungen unterscheiden und die richtige AppQoE-Aktion an jede Richtlinie binden kann.
- Bindung der AppQoE-Richtlinie an den virtuellen Server. Nachdem Sie die AppQoE-Richtlinien konfiguriert haben, müssen Sie sie an einen oder mehrere virtuelle Load Balancing-, Content Switching- oder Cache-Umleitungsserver binden.

Konfiguration über die Befehlszeilenschnittstelle

So aktivieren Sie AppQOE mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile die folgenden Befehle ein, um die Funktion zu aktivieren, und überprüfen Sie, ob sie aktiviert ist:

- `enable ns feature appqoe`
- `show ns feature`

Um ein TCP-Profil zu binden, während Sie eine AppQoE-Aktion mithilfe der Befehlszeilenschnittstelle erstellen

Geben Sie an der Befehlszeile den folgenden AppQoE-Aktionsbefehl mit der `tcpprofiletobind` Option ein.

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS | NS )
[<CustomFile>] [-altContentSvcName <string>] [-altContentPath <string>] [-
maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth <positive_integer
>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-
dosAction ( SimpleResponse |HICResponse )] [-tcpprofiletobind <string>]
show appqoe action
```

So konfigurieren Sie eine AppQoE-Richtlinie mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Um eine AppQoE-Richtlinie mithilfe der Befehlszeilenschnittstelle an virtuelle Server für Load Balancing, Cache-Umleitung oder Content Switching zu binden

Geben Sie in der Befehlszeile Folgendes ein:

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <priority
>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <priority
>
```

Beispiel


```
1     add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
         ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500
          -slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
         sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
         ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack
         ENABLED -tcpmode ENDPOINT
2     add appqoe action appact1 -priority HIGH -tcpprofile tcp1
3     add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
         action appact1
4     bind lb vserver lb2 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
5     bind cs vserver cs1 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
6  <!--NeedCopy-->
```

Konfiguration der richtlinienbasierten TCP-Profilerstellung mit der GUI

Um AppQOE mithilfe der GUI zu aktivieren

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.
3. Aktivieren Sie im Dialogfeld **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **AppQoE**.
4. Klicken Sie auf **OK**.

So konfigurieren Sie die AppQoE-Richtlinie mithilfe der GUI

1. Navigieren Sie zu **App-Expert** > **AppQoE** > **Actions.**
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
3. Um eine Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
4. Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
5. Geben Sie im Bildschirm **AppQoE-Aktion erstellen** oder **AppQoE-Aktion konfigurieren** Werte für die Parameter ein, oder wählen Sie sie aus. Der Inhalt des Dialogfelds entspricht den unter ““Parameter für die Konfiguration der AppQoE-Aktion” beschriebenen Parametern wie folgt (ein Sternchen gibt einen erforderlichen Parameter an):
   a) Name—Name
   b) Action type—respondWith
   c) Priorität — Priorität
   d) Policy Queue Depth—polqDepth
   e) Queue Depth—priqDepth

f) DOS Action—dosAction

6. Klicken Sie auf **Erstellen**.

So binden Sie die AppQoE-Richtlinie mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen Server aus und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie im Abschnitt **Richtlinien** auf (+), um eine AppQoE-Richtlinie zu binden.
3. Gehen Sie im Schieberegler **Richtlinien** wie folgt vor:
   a) Wählen Sie in der Dropdownliste einen Richtlinientyp als AppQoE aus.
   b) Wählen Sie einen Verkehrstyp aus der Dropdownliste aus.
4. Gehen Sie im Abschnitt **Richtlinienbindung** wie folgt vor:
   a) Klicken Sie auf **Neu**, um eine AppQoE-Richtlinie zu erstellen.
   b) Klicken Sie auf **Existing Policy**, um eine AppQoE-Richtlinie aus der Dropdownliste auszuwählen.
5. Legen Sie die Bindungspriorität fest und klicken Sie auf An die Richtlinie an den virtuellen Server **binden** .
6. Klicken Sie auf **Fertig**.

SACK-Blockgenerierung

Die TCP-Leistung verlangsamt sich, wenn mehrere Pakete in einem Datenfenster verloren gehen. In einem solchen Szenario überwindet ein SACK-Mechanismus (Selective Acknowledgment) in Kombination mit einer selektiven Wiederholungsrichtlinie diese Einschränkung. Für jedes eingehende Paket, das nicht in der richtigen Reihenfolge ist, müssen Sie einen SACK-Block generieren.

Wenn das Paket, das nicht in der Reihenfolge ist, in den Queue-Block für die Reassemblierung passt, fügen Sie die Paketinformationen in den Block ein und legen Sie die vollständigen Blockinformationen auf SACK-0 fest. Wenn ein Paket nicht in der richtigen Reihenfolge in den Zusammenbaublock passt, senden Sie das Paket als SACK-0 und wiederholen Sie die früheren SACK-Blöcke. Wenn ein Paket nicht in der richtigen Reihenfolge ein Duplikat ist und die Paketinformation auf SACK-0 gesetzt ist, dann D-Sack den Block.

Hinweis: Ein Paket wird als D-SACK betrachtet, wenn es sich um ein bestätigtes Paket oder um ein fehlerhaftes Paket handelt, das bereits empfangen wurde.

Kunde verbietet

Eine NetScaler-Appliance kann Client-Renegings während einer SACK-basierten Wiederherstellung verarbeiten.

Speicherprüfungen zur Markierung des Endpunkts auf der Leiterplatte berücksichtigen nicht den gesamten verfügbaren Speicher

Wenn in einer NetScaler-Appliance der Schwellenwert für die Speichernutzung auf 75 Prozent gesetzt wird, anstatt den gesamten verfügbaren Speicher zu nutzen, führt dies dazu, dass neue TCP-Verbindungen die TCP-Optimierung Bypass.

Unnötige Neuübertragungen aufgrund fehlender SACK-Blöcke

Wenn Sie in einem Modus ohne Endpunkt DUPACKS senden und SACK-Blöcke für einige Pakete fehlen, die nicht in der richtigen Reihenfolge sind, werden weitere Übertragungen vom Server ausgelöst.

SNMP für Verbindungen hat die Optimierung aufgrund von Überlastung umgangen

Die folgenden SNMP-IDs wurden einer NetScaler-Appliance hinzugefügt, um die Anzahl der Verbindungen zu verfolgen, bei denen TCP-Optimierungen aufgrund von Überlastung umgangen wurden.

1. 1.3.6.1.4.1.5951.4.1.1.46.131 (tcpOptimizationEnabled). Um die Gesamtzahl der mit der TCP-Optimierung aktivierten Verbindungen zu verfolgen.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (tcpOptimizationBypassed). Um die Gesamtzahl der Verbindungen zu verfolgen, wurde die TCP-Optimierung umgangen.

Dynamischer Empfangspuffer

Um die TCP-Leistung zu maximieren, kann eine NetScaler Appliance nun die Größe des TCP-Empfangspuffers dynamisch anpassen.

Tail Loss Sonde-Algorithmus

Ein Wiederübertragungs-Timeout (RTO) ist ein Verlust von Segmenten am Ende einer Transaktion. Ein RTO tritt auf, wenn Probleme mit der Anwendungslatenz auftreten, insbesondere bei kurzen Webtransaktionen. Um den Verlust von Segmenten am Ende einer Transaktion auszugleichen, verwendet TCP den TLP-Algorithmus (Tail Loss Probe).
TLP ist ein Algorithmus, der nur für Absender bestimmt ist. Wenn eine TCP-Verbindung für einen bestimmten Zeitraum keine Bestätigung erhält, überträgt TLP das letzte unbestätigte Paket (Loss Probe). Im Falle eines Endausfalls bei der ursprünglichen Übertragung löst die Bestätigung der Verlustsonde eine SACK- oder FACK-Wiederherstellung aus.

Konfiguration der Tail Loss Probe

Um den Tail Loss Probe (TLP) -Algorithmus zu verwenden, müssen Sie die TLP-Option im TCP-Profil aktivieren und den Parameter auf einen Wert setzen, der den Sicherheitsanforderungen für dieses

Profil entspricht.

Aktivieren Sie TLP über die Befehlszeile

Geben Sie in der Befehlszeile einen der folgenden Befehle ein, um TLP in einem neuen oder vorhandenen Profil zu aktivieren oder zu deaktivieren.

> **Hinweis**:
>
> Der Standardwert ist DISABLED.

```
add tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

set tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

unset tcpprofile <TCP Profile Name> - taillossprobe
```

Beispiele:

```
add tcpprofile nstcp_default_profile - taillossprobe

set tcpprofile nstcp_default_profile -taillossprobe Enabled

unset tcpprofile nstcp_default_profile -taillossprobe
```

Konfigurieren Sie den Tail Loss Probe-Algorithmus mithilfe der NetScaler-GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite „ **TCP-Profil konfigurieren** “ das Kontrollkästchen **Tail Loss Probe** .
3. Klicke auf **OK** und dann auf **Fertig**.

Lösungen zur Fehlerbehebung für NetScaler

May 11, 2023

In diesem Thema finden Sie einige grundlegende Lösungen zur Fehlerbehebung, die zur Behebung von Problemen in Ihrer Appliance erforderlich sind. Sie erhalten einen Überblick über die NetScaler Appliance, die Integration in das Netzwerk und die Probleme, die Sie bei grundlegenden Systemfunktionen erwarten können.

Pakettracings in NetScaler aufzeichnen

May 11, 2023

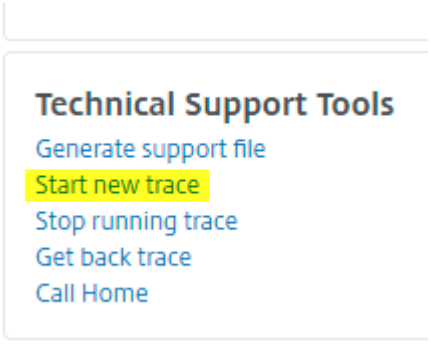
In diesem Artikel zur Fehlerbehebung wird erläutert, wie ein Administrator mithilfe der NetScaler GUI eine Netzwerkpaketverfolgung aufzeichnen kann.

Wichtige Punkte

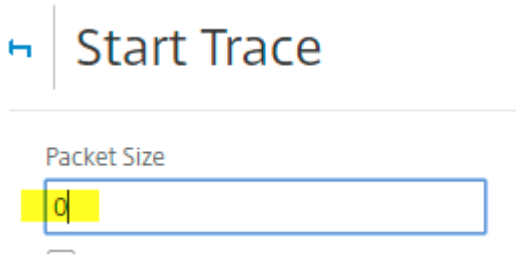
- Citrix empfiehlt die Verwendung der aktuellen Wireshark-Version aus dem “Abschnitt zum automatisierten Erstellen”, der auf der folgenden Webseite verfügbar ist: http://www.wireshark.org/download/automated.
- In NetScaler Version 11.1 oder höher, um die Erfassung zu entschlüsseln und sicherzustellen, dass ECC (Elliptic Curve Cryptography), Sitzungswiederverwendung und DH-Parameter auf dem virtuellen Server deaktiviert sind. Sie müssen dies tun, bevor Sie eine Spur aufnehmen.

Packet-Trace auf NetScaler Version 11.1 aufzeichnen

1. Navigieren Sie zur Seite **System** > **Diagnose** .
2. klicken Sie auf der **Diagnoseseite** auf den Link **Neue Ablaufverfolgung starten**, wie im folgenden Screenshot gezeigt.

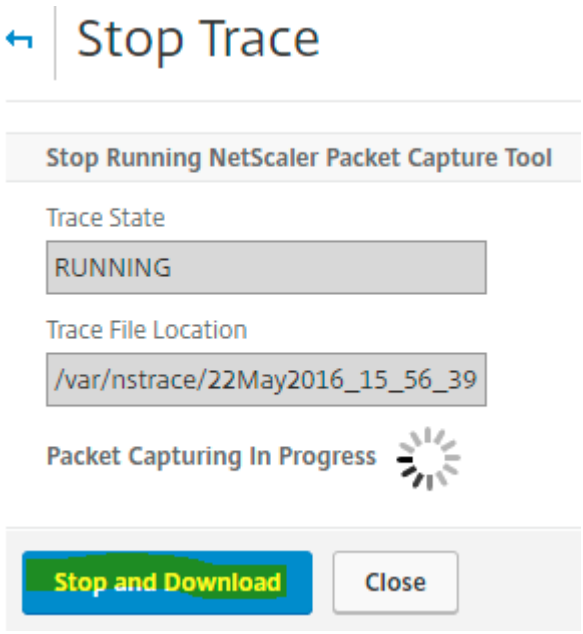


3. Aktualisieren Sie die Paketgröße im Feld **Paketgröße** auf 0.

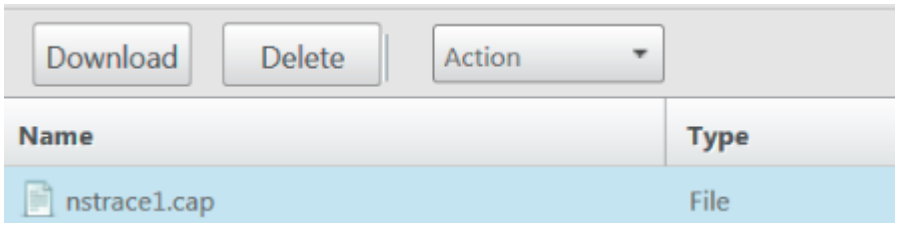


4. Klicken Sie auf **Start**, um die Aufzeichnung des Netzwerk-Paket-Trace

5. Klicken Sie auf **Beenden und herunterladen**, um die Aufzeichnung des Netzwerk-Paket-Trace nach Abschluss des Tests zu beenden.

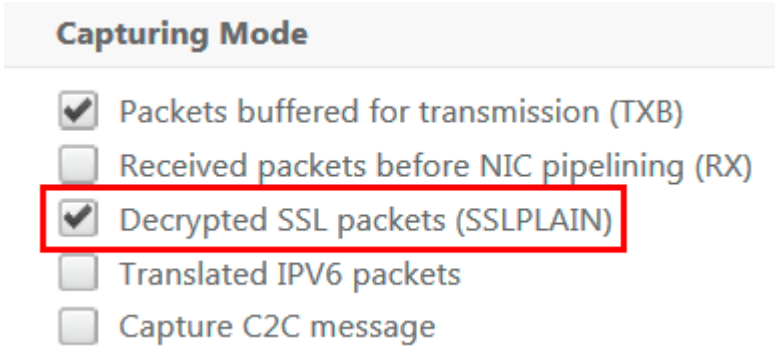


6. Wählen Sie die gewünschte Datei aus, klicken Sie auf **Auswählen** und dann auf **Herunterladen**.



7. Öffnen Sie die Netzwerk-Paket-Trace-Datei mit dem Wireshark-Dienstprogramm, um den Inhalt der Datei anzuzeigen.

> **Hinweis**: Wählen Sie Entschlüsselte SSL-Pakete (SSLPLAIN) aus, um die Paketverfolgung ohne den privaten Schlüssel zu entschlüsseln.



SSL-Masterschlüssel erfassen

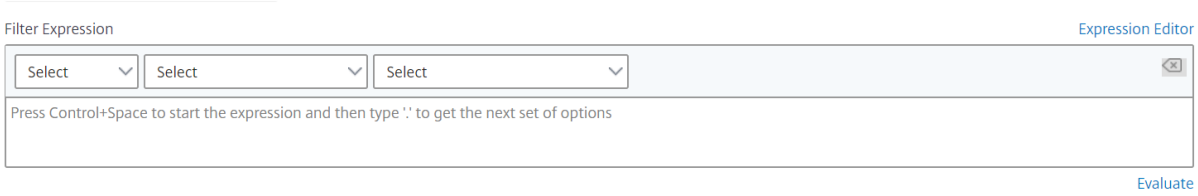
In der Version 11.0, 11.1 und höher gibt es eine Option zum Erfassen der Sitzungsschlüssel, die nur für diese bestimmte Sitzung/nstrace gültig ist. Diese Option kann verwendet werden, wenn Sie den privaten Schlüssel nicht teilen oder den SSLPLAIN-Modus verwenden möchten. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX135889.

Exportieren von Sitzungsschlüsseln ohne privaten Schlüssel zu teilen

In den meisten Szenarien ist der private Schlüssel nicht verfügbar oder wird nicht freigegeben. In solchen Szenarien können wir vorschlagen, die **SSL-Sitzungsschlüssel** anstelle des privaten Schlüssels zu exportieren. Lesen Sie,
[Exportieren und Verwenden von SSL-Sitzungsschlüsseln zum Entschlüsseln von SSL-Traces ohne gemeinsame Nutzung des privaten SSL-Keys, siehe https://support.citrix.com/article/CTX135889.

Filter

Außerdem wird immer empfohlen, IP-basierte Filter hinzuzufügen, während Spuren aufgezeichnet werden. Der Prozess stellt sicher, dass Sie nur interessierten Datenverkehr erfassen, was Ihre Fehlerbehebung erleichtert. Das Hinzufügen von Filtern verringert auch die Belastung des Geräts beim Aufnehmen von Spuren.



Einfache IP-basierte Filter reichen aus, um die richtigen Aufnahmen zu erhalten. Weitere Informationen zu `nstrace` Filtern und Beispielen finden Sie auf der NetScaler-Dokumentationsseite .

Anwendungsfall zur Erfassung einer Paketverfolgung mit IP-Filter des virtuellen Servers (sowohl Front-End als auch Back-End)

Wenn Sie einen Filter der IP-Adresse des virtuellen Servers verwenden und die Option “—link” in der CLI aktivieren oder die Option “Gefilterten Verbindungs-Peer-Verkehr verfolgen” in der GUI (verfügbar ab Version 10.1) auswählen, können Sie sowohl den Front-End- als auch den Back-End-Verkehr für die IP-Adresse erfassen.

```
start nstrace -size 0 -filter "CONNECTION.IP.EQ(1.1.1.1)" -link ENABLED

show nstrace
```



```
4          State:  RUNNING          Scope:  LOCAL            TraceLocation
               :  "/var/nstrace/24Mar2017_16_00_19/..." Nf:  24
                              Time:  3600             Size:  0
                             Mode:  TXB NEW_RX
5          Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  24
               Mar2017_16_00_19 Filter:  "CONNECTION.IP.EQ(1.1.1.1)" Link:
                ENABLED           Merge:  ONSTOP           Doruntimecleanup
               :  ENABLED
6          TraceBuffers:  5000      SkipRPC:  DISABLED       Capsslkeys:
               DISABLED    InMemoryTrace:  DISABLED
7  <!--NeedCopy-->
```

Erfassung zyklischer Spuren

Es ist immer schwierig, ein zeitweiliges Problem zu beheben. Die zyklische Ablaufverfolgung eignet sich am besten für intermittierende Probleme. Die Traces können über einen Zeitraum von wenigen Stunden oder Tagen ausgeführt werden, bevor das Problem auftritt. Sie können auch einen bestimmten Filter verwenden und die Größe der generierten Ablaufverfolgungsdateien auswerten, bevor Sie sie für eine längere Zeit ausführen.

Führen Sie den folgenden Befehl in der CLI aus:

```
1  start nstrace -nf 60 -time 30 -size 0
2  This particular trace will create 60 files each of them for 30 sec.
       This means the files will start getting overwritten after 60 trace
       files or 30 mins
3  Show nstrace à To check the status of the nstrace
4  Stop nstrace à To stop the nstrace.
5
6  <!--NeedCopy-->
```

Bewährte Methoden

Auf einer Einheit, die GB Verkehr pro Sekunde verarbeitet, ist das Erfassen von Datenverkehr ein sehr ressourcenintensiver Prozess. Die Auswirkungen auf Ressourcen beziehen sich hauptsächlich auf die CPU und den Speicherplatz. Die Auswirkungen auf den Speicherplatz können durch die Verwendung

von Filterausdrücken reduziert werden. Die Auswirkungen auf die CPU bleiben jedoch bestehen und führen manchmal zu einem leichten Anstieg, da die Appliance nun Pakete gemäß dem Filter verarbeiten muss, bevor sie erfasst werden.

Die beste Vorgehensweise bei der Rückverfolgung ist:

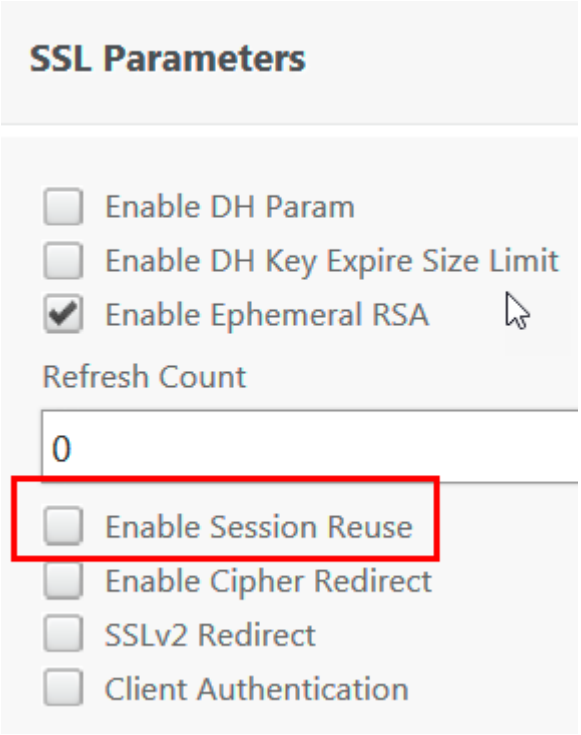
1. Die Dauer, für die die Ablaufverfolgung ausgeführt wird, muss so begrenzt wie möglich sein, wenn Sie dennoch sicherstellen, dass die Pakete von Interesse erfasst werden.
2. Planen Sie die Verfolgungsaktivität so ein, dass sie zu einem Zeitpunkt stattfindet, an dem die Anzahl der Benutzer (und damit der Verkehr) stark reduziert wird, z. B. außerhalb der Geschäftszeiten.

Weitere Ressourcen

Deaktivieren Sie die Wiederverwendung von Sitzungen auf einem virtuellen Server über die

Die Wiederverwendung von Sitzungen ist deaktiviert, wenn Sie einen Trace erfassen, um einen SSL-Handshake im Trace abzuschließen. Wenn es aktiviert ist, können Sie einen teilweisen Handshake in der Ablaufverfolgung erfassen. Stellen Sie sicher, dass Sie die Option nach der Trace-Erfassung aktivieren.
Deaktivieren Sie die Wiederverwendung einer SSL-Sitzung nicht, wenn die Persistenzmethode sslsession ist, da dies die Persistenz für bestehende Verbindungen beeinträchtigt. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX121925.

1. Öffnen Sie den virtuellen Server und navigieren Sie zu SSL-Parameter.
2. Deaktivieren Sie “Sitzungswiederverwendung aktivieren”, falls aktiviert



Deaktivieren Sie die Wiederverwendung von Sitzungen auf einem virtuellen Server über die CLI

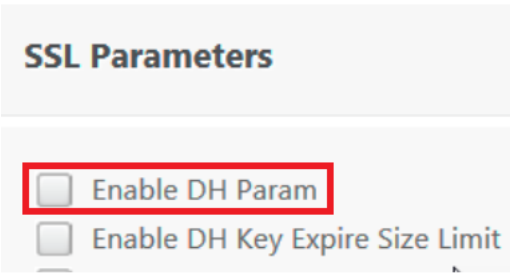
1. SSH an die Appliance-Konsole.
2. Führen Sie den folgenden Befehl aus, um DH Param vom virtuellen Server aus zu deaktivieren:

```
set ssl vserver "vServer_Name"-sessReuse DISABLED
```

DH-Parameter auf virtuellem Server über die GUI deaktivieren

Weitere Informationen zu DH-Parametern finden Sie unter https://support.citrix.com/article/CTX213335.

1. Öffnen Sie den virtuellen Server und navigieren Sie zu SSL-Parameter.
2. Deaktivieren Sie DH Param, falls aktiviert.



Deaktivieren Sie den DH-Parameter auf dem virtuellen Server über die CLI

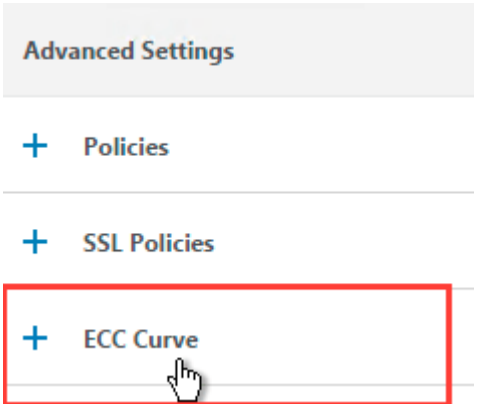
1. SSH an die Appliance-Konsole.
2. Führen Sie den folgenden Befehl aus, um DH Param vom virtuellen Server aus zu deaktivieren:

```
set ssl vserver "vServer_Name"-dh DISABLED
```

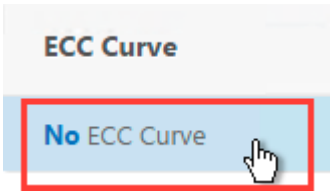
Deaktivieren Sie die ECC-Kurve auf dem virtuellen Server über die GUI

Die ECC-Kurve ist deaktiviert, um den erfassten SSL-Trace mit einem privaten Schlüssel zu entschlüsseln Sie dürfen die Schlüssel nicht deaktivieren, wenn die zugehörigen SSL-Chiffren verwendet werden. Weitere Hinweise zur ECC-Kurve finden Sie unter https://support.citrix.com/article/CTX205289

1. Öffnen Sie den virtuellen Server und navigieren Sie zu ECC Curve.



2. Wenn keine ECC-Kurve an den virtuellen Server gebunden ist, ist keine weitere Aktion erforderlich.



3. Wenn eine ECC-Kurve an den virtuellen Server gebunden ist, klicken Sie auf die ECC-Kurve und lösen Sie sie vom virtuellen Server.

Deaktivieren Sie die ECC-Kurve auf dem virtuellen Server über die CLI

1. SSH an die Appliance-Konsole.
2. Führen Sie den folgenden Befehl für jede an den virtuellen Server gebundene ECC-Kurve aus:

```
unbind ssl vserver "vServer_Name"-eccCurveName "ECC_Curve_Name"
```


So geben Sie Speicherplatz im Verzeichnis /var frei

September 18, 2023

Im folgenden Artikel wird erläutert, wie ein Administrator den Speicherplatz aus dem Verzeichnis `/var` einer NetScaler-Appliance freigeben kann. Sie können den Schritten folgen, wenn die GUI nicht zugänglich ist.

Wenn der Festplattenspeicher im Verzeichnis /var der Appliance knapp ist, können Sie sich möglicherweise nicht bei der GUI anmelden. In diesem Szenario können Sie die alten Protokolldateien entfernen, um freien Speicherplatz im Verzeichnis /var zu erstellen.

Wichtige Punkte

- Stellen Sie sicher, dass Sie die Dateien sichern, bevor Sie die Dateien von der Appliance entfernen.

Führen Sie das folgende Verfahren aus, um Speicherplatz im Verzeichnis `/var` einer NetScaler-Appliance freizugeben:

1. Melden Sie sich mit SSH an der CLI von NetScaler an. Weitere Informationen zum Abschließen dieser Aufgabe finden Sie in der NetScaler Dokumentation.
2. Nachdem Sie sich bei der NetScaler CLI angemeldet haben, wechseln Sie mit dem folgenden Befehl zur Shell-Eingabeaufforderung. `shell`
3. Führen Sie den folgenden Befehl aus, um die Verfügbarkeit von Speicherplatz auf der NetScaler-Appliance anzuzeigen. `df -h`
4. Wenn die Speicherkapazität des Verzeichnisses `/var` bis zu 90 Prozent gefüllt ist, müssen Sie einige Dateien aus diesem Verzeichnis löschen.

   - Führen Sie die folgenden Befehle aus, um den Inhalt des Verzeichnisses /var anzuzeigen:

     ```
     cd /var
     ls -l
     ```

   Die Verzeichnisse, die normalerweise von Interesse sind, sind wie folgt:

   ```
   /var/nstrace - This directory contains trace files.This is the
      most common reason for HDD being filled on the NetScaler
      appliance. This is due to an nstrace being left running for
      indefinite amount of time. All traces that are not of interest
      can and should be deleted. To stop an nstrace, go back to the
      CLI and issue stop nstrace command.

   /var/log - This directory contains system specific log files.
   ```



```
4
5  /var/nslog - This directory contains NetScaler log files.
6
7  /var/tmp/support - This directory contains technical support files
       , also known as, support bundles. All files not of interest
       should be deleted.
8
9  /var/core - Core dumps are stored in this directory. There will be
        directories within this directory and they will be labeled
       with numbers starting with 1. These files can be quite large in
        size. Clear all files unless the core dumps are recent and
       investigation is required.
10
11 /var/crash - Crash files, such as process crashes are stored in
       this directory. Clear all files unless the crashes are recent
       and investigation is required.
12
13 /var/nsinstall -  Firmware is placed in this directory when
       upgrading. Clear all files, except the firmware that is
       currently being used.
```

- Überprüfen Sie, ob eines der Verzeichnisse mehr Speicherplatz belegt:

```
1  du -hs *
2  44k    cache
3  2.0k    clusterd
4  2.0k    configdb
5  6.0k    core
6  989M    crash
7  4.0k    cron
8  2.0k    dev
9  6.0k    download
10 2.0k    gui
11 2.0k    install
12 2.0k    krb
13 2.0k    learnt_data
14 122M    log
15 366M    NetScaler
16 14k    ns_gui
17 86k    ns_sys_backup
18 631M    nsinstall
19 883M    nslog
20 32k    nsproflog
21 2.0k    nssynclog
22 16k    nstemplates
```



```
36k    nstmp
4.5G    nstrace
8.1M    opt
6.0k    pubkey
52k    run
28M    safenet
72M    tmp
2.0k    vmtools
14k    vpn
```

- Löschen Sie die Dateien, die nicht benötigt werden:

```
rm -r nstrace/*
```

Weitere Hilfe zum Löschen von Dateien finden Sie in den FreeBSD-Handbuchseiten.

  - Löschen Sie die Dateien, die nicht benötigt werden.
    `rm -r nstrace/*`
    Weitere Hilfe zum Löschen von Dateien finden Sie in den FreeBSD-Handbuchseiten.
  - Wenn das Protokoll oder das Verzeichnis `nslog` mehr Speicherplatz beansprucht, führen Sie die folgenden Befehle aus, um das Protokollverzeichnis zu öffnen und seinen Inhalt anzuzeigen:

```
cd /var/log
ls -l
cd /var/nslog
ls -l
```

1. Stellen Sie sicher, dass alle Dateien komprimiert sind. Dies wird durch die Dateinamenerweiterung .tar.gz angezeigt.

   Wenn die Datei nicht komprimiert ist, gehen Sie wie folgt vor:

   Um die Datei in das GZ-Format zu komprimieren:

```
cd /var/log
gzip <filename>
```

   Die komprimierte Datei befindet sich unter /var/log

   Um die Datei in das Format .tar.gz zu komprimieren:

```
cd /var/nslog
tar -cz <filename>.tar.gz <filename>
```

   Die komprimierte Datei befindet sich unter /var/nslog

2. Wenn Sie NetScaler ADM verwenden, überprüfen Sie das Verzeichnis /var/ns_system_backup. Stellen Sie sicher, dass NetScaler ADM die Backup Sicherungsdateien löscht.

Weitere Ressourcen

Informationen zu den Befehlen, die im vorherigen Verfahren erwähnt wurden, finden Sie unter http://ss64.com/bash/.

Download von Core- oder abgestürzten Dateien von der NetScaler-Appliance

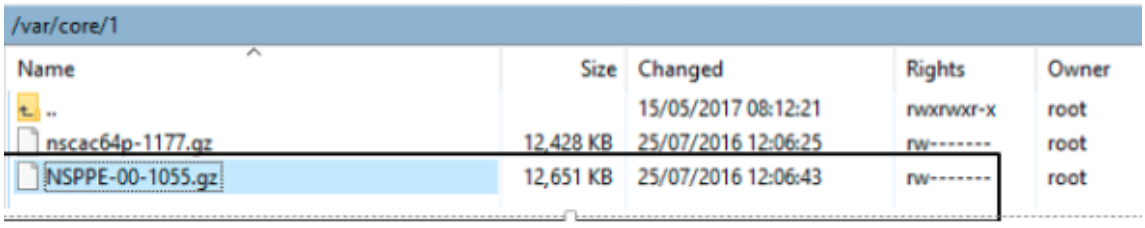
May 11, 2023

In diesem Artikel zur Fehlerbehebung wird erläutert, wie ein Administrator Kern- oder Absturzdateien von der NetScaler-Appliance herunterladen kann.

Laden Sie mithilfe des SFTP-Clients Kern- oder Absturzdateien von der NetScaler-Appliance herunter

Gehen Sie wie folgt vor, um die Kern- oder Absturzdateien von einer NetScaler-Appliance herunterzuladen:

1. Öffnen Sie WinSCP und melden Sie sich an der NetScaler Management-IP-Adresse an.
2. Navigieren Sie zum `/var/core/1`, um die Dateien herunterzuladen.



> **Hinweis:**
>
> Um die neueste Crash- oder Core-Datei herunterzuladen, können Sie das WinSCP-Tool auch über die Befehlszeilenschnittstelle verwenden. Die Dateien können sich entweder im Kern- oder Absturzverzeichnis befinden.

Leistungsstatistiken und Ereignisprotokolle sammeln

May 11, 2023

Sie können Leistungsstatistiken von virtuellen Servern und zugehörigen Diensten aus einer archivierten Datei `newnslog` im Verzeichnis `/var/nslog` sammeln. Die `newnslog`-Dateien werden durch Ausführen von `/netscaler/nsconmsg` interpretiert.

Erfassen Sie Leistungsstatistiken und Ereignisprotokolle mit der CLI

Sie können den Befehl `nsconmsg` von der NetScaler-Shell-Eingabeaufforderung aus ausführen, um Ereignisse zu melden.

Geben Sie in der Befehlszeile Folgendes ein:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d event
```

```
1 Displaying event information
2 NetScaler V20 Performance Data
3 NetScaler NS10.5: Build 57.7.nc, Date: May 14 2015, 07:35:21
4 rtime: Relative time between two records in milliseconds
5 seqno rtime event-message                          event-time
6 11648 16310 PPE-0 MonServiceBinding_10.104.20.110:443_(tcp-default)
7 <!--NeedCopy-->
```

Zeigt die Zeitspanne an, die von einer bestimmten “newnslog”-Datei abgedeckt wird

Geben Sie in der Befehlszeile Folgendes ein:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d setime
```

Die aktuellen Daten werden an die `/var/nslog/newnslog`-Datei angehängt. NetScaler archiviert die `newnslog`-Datei standardmäßig automatisch alle zwei Tage. Um die archivierten Daten zu lesen, müssen Sie das Archiv wie im folgenden Beispiel gezeigt extrahieren:

`cd /var/nslog`: Befehl, um von NetScaler Shell Prompt aus in ein bestimmtes Verzeichnis zu wechseln.

`tar xvfz newnslog.100.tar.gz`: Befehl zum Extrahieren der TAR-Datei.

`/netscaler/nsconmsg -K newnslog.100 -d setime`: Befehl zur Überprüfung der von der jeweiligen Datei abgedeckten Zeitspanne, in diesem Beispiel `newnslog.100`.

`ls -l`: Der Befehl überprüft die gesamte Protokolldatei und den Zeitstempel, die diesen Dateien zugeordnet sind.


```
root@NETSCALER## cd /var/nslog
root@NETSCALER## ls -l
```

```
 wheel    461544 Aug  7  2014 newnslog.1.tar.gz
-rw-r--r--   1 root       wheel    191067 Aug  7  2014 newnslog.10.tar.
   gz
-rw-r--r--   1 root       wheel  11144873 Apr 26 22:04 newnslog.100.tar
   .gz
-rw-r--r--   1 root       wheel  11095053 Apr 28 22:04 newnslog.101.tar
   .gz
-rw-r--r--   1 root       wheel  11114284 Apr 30 22:04 newnslog.102.tar
   .gz
-rw-r--r--   1 root       wheel  11146418 May  2 22:04 newnslog.103.tar
   .gz
-rw-r--r--   1 root       wheel  11104227 May  4 22:04 newnslog.104.tar
   .gz
-rw-r--r--   1 root       wheel  11297419 May  6 22:04 newnslog.105.tar
   .gz
-rw-r--r--   1 root       wheel  11081212 May  8 22:04 newnslog.106.tar
   .gz
-rw-r--r--   1 root       wheel  11048542 May 10 22:04 newnslog.107.tar
   .gz
-rw-r--r--   1 root       wheel  11101869 May 12 22:04 newnslog.108.tar
   .gz
-rw-r--r--   1 root       wheel  11378787 May 14 22:04 newnslog.109.tar
   .gz
-rw-r--r--   1 root       wheel  44989298 Apr 11  2014 newnslog.11.gz
<!--NeedCopy-->
```

Zeigt die Zeitspanne innerhalb einer Datei an

Verwenden Sie den Befehl `nsconmsg`, um nur eine Zeitspanne innerhalb der angegebenen Datei anzuzeigen, wie im folgenden Beispiel gezeigt:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -s time=22Mar2007:20:00 -T 7 -s
ConLb=2 -d oldconmsg
```

Hierbei gilt:

`s` : time=22Mar2007:20:00:00 beginnt am 22. März 2007 genau um 20:00 Uhr.

`T 7` : Zeigt Daten für sieben Sekunden an

`s` : Zeigt den Detaillierungsgrad der Lastausgleichsstatistiken an.

`d` : Zeigt statistische Informationen an.

> **Hinweis:**
>
> Ab ADC-Version 12.1 müssen Sie auch die Sekunden zu “time” hinzufügen, also: 22Mar2007:20:00:00

Die vom Parameter `-d oldconmsg` bereitgestellten statistischen Informationen werden alle sieben Sekunden aufgezeichnet. Das Folgende ist eine Beispielausgabe.

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec) Mbps(1.02)
   Pers(OFF) Err(0)
Pkt(186/sec, 610 bytes) actSvc(4) DefPol(NONE) override(0)
Conn: Clt(253, 1/sec, OE[252]) Svr(3)
S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
   Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
S(10.128.49.39:80:UP) Hits(9731048, 4/sec, P[2929279, 0/sec]) ATr(9)
   Mbps(0.27) BWlmt(0 kbits) RspTime(161.69 ms)
Other: Pkt(41/sec, 756 bytes) Wt(10000) RHits(31555)
Conn: CSvr(32, 0/sec) MCSvr(19) OE(13) RP(4) SQ(0)
S(10.128.49.38:80:UP) Hits(9341366, 5/sec, P[2700778, 0/sec]) ATr(4)
   Mbps(0.27) BWlmt(0 kbits) RspTime(120.50 ms)
Other: Pkt(42/sec, 720 bytes) Wt(10000) RHits(31556)
Conn: CSvr(37, 0/sec) MCSvr(19) OE(13) RP(9) SQ(0)
S(10.128.49.37:80:UP) Hits(9685018, 4/sec, P[2844418, 0/sec]) ATr(3)
   Mbps(0.23) BWlmt(0 kbits) RspTime(125.38 ms)
Other: Pkt(38/sec, 670 bytes) Wt(10000) RHits(31556)
Conn: CSvr(32, 0/sec) MCSvr(20) OE(10) RP(7) SQ(0)
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Anzahl der Client-Verbindungen der einzelnen Dienste entspricht nicht der Anzahl der Client-Verbindungen des virtuellen Servers. Der Grund liegt in der Wiederverwendung von Sitzungen zwischen der NetScaler Appliance und dem Back-End-Dienst.

Virtuelle Serverausgabe

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec) PHits(5)
   Mbps(1.02) Pers(OFF) Err(0) LConn_Best [Idx:SubIdx] 0:0
   PrimVserverDownBackupHits(0)
Pkt(186/sec, 610 bytes) actSvc(4) DefPol(NONE) override(0) newlyUP(0)
Conn: Clt(253, 1/sec, OE[252]) Svr(3) SQ(Total: 0 OnVserver: 0
   OnServices: 0)
slimit_SO: (Sothreshhold: 0 [Ex: 0]  Consumed: [Ex: 0 Borrowed: 0
   TotActiveConn: 0] Available: 0)
```



```
<!--NeedCopy-->
```

In der folgenden Liste werden die Statistiken für virtuelle Server beschrieben:

1. IP (IP address:port:state:Load balancing method): Die IP-Adresse und der Port der virtuellen IP-Adresse wie konfiguriert. Der virtuelle Serverstatus oder die virtuelle IP-Adresse lautet UP, DOWN oder OUT OF SERVICE; die für die virtuelle IP-Adresse konfigurierte Loadbalancing-Methode.
2. Hits (##):Anzahl der Anfragen, die den virtuellen Server erreicht haben.
3. Mbps (##): Das gesamte Verkehrsvolumen auf dem virtuellen Server (Rx + Tx) wurde in Mbit/s umgerechnet.
4. Pers: Die Art der Persistenz ist konfiguriert.
5. Err (##): Häufigkeit, mit der eine Fehlerseite vom virtuellen Server generiert wurde.
6. Pkt (##/sec, ## bytes): Volumen des Netzwerkverkehrs (als Pakete), der durch den virtuellen Server fließt, und durchschnittliche Paketgröße, die durch den virtuellen Server fließt.
7. actSvc(##): Anzahl der aktiven Dienste, die an den virtuellen Server gebunden sind.
8. DefPol (RR): Gibt an, ob die Standard-Load-Balancing-Methode aktiv ist. Die Standard-Load-Balancing-Methode wird für einige erste Anfragen verwendet, um das Verhalten der anderen Methoden zu glätten.
9. Clt (##, ##/sec): Anzahl der aktuellen Client-Verbindungen zur Rate des virtuellen Servers.
10. OE [##]: Anzahl der Serververbindungen vom virtuellen Server im Status Open Established.
11. Svr (##): Anzahl der aktuellen Serververbindungen vom virtuellen Server.
12. PHits (##): Anzahl der Persistenz-Treffer.
13. SO: Häufigkeit, mit der Spillover stattgefunden hat.
14. LConn_Best [Idx:SubIdx] (port:##). Der Index-Sub-Slot des besten Servers, wenn die Methode mit den wenigsten Verbindungen verwendet wird.
15. PrimVserverDownBackupHits (##): Anzahl der Treffer zum Backup des virtuellen Servers, als der Primärserver ausgefallen war.
16. Override (##): Häufigkeit, mit der die nächstbesten Server auf der Grundlage von L2Conn für maxClt ausgewählt wurden.
17. newlyUP (##): Anzahl der aktuellen Dienste, die neu verfügbar sind.
18. SQ(Total:OnVserver:OnServices:): Aktuelle Länge der Überspannungswarteschlange.
19. slimit_SO: (Sothreshhold:Exclusive:Consumed: [Exclusive:Borrowed: TotActiveConn:] Available: (##)): Exklusive und gemeinsam genutzte Informationen zum gemeinsamen Limit für Spillover.

In der vorherigen Ausgabe gibt Svr(3) an, dass der Befehl die statistische Stichprobe sammelt. Es gibt drei aktive Verbindungen für den virtuellen Server zum Backend-Server, obwohl es insgesamt vier Dienste gibt. Wenn ein Client eine Verbindung mit dem virtuellen Server herstellt, ist es nicht erforderlich, dass der Client Datenverkehr sendet oder empfängt, wenn der Befehl die Informationen

sammelt. Daher ist es üblich, dass der Zähler `Svr` niedriger als die Zahl `OE[]` ist. Der Zähler `Svr` steht für die Anzahl der aktiven Verbindungen, die aktiv Daten senden oder empfangen. Die Subnetz-IP-Adresse (SNIP) ist mit dem zugehörigen Backend-Server verbunden. Und der NetScaler verfolgt den virtuellen Server, der mit dem Backend-Server verbunden ist, und berechnet den Zähler.

Ausgabe virtueller Dienste

```
S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
    Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms) Load(0) LConn_Best [Idx
    :SubIdx] (C:0; V:0,I:1, B:0, X:0, SI:0)
Other: Pkt(36/sec, 712 bytes) Wt(10000) Wt(Reverse Polarity)(10000)
    RHits(31555) Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) E(5) RP(11) SQ
    (0)
slimit_maxClient: (MaxClt: 2 [Ex: 0]  Consumed: [Ex: 0 Borrowed: 0
    TotActiveConn: 0] Available: 2)
newlyUP_mode: NO, Pending: 0, update: 0x0, incr_time: 0x0, incr_count:
    0
<!--NeedCopy-->
```

In der folgenden Liste werden die Servicestatistiken beschrieben:

1. `S (IP address:port:state)`: IP-Adresse, Port und Status des Dienstes, z. B. DOWN, UP oder OUT OF SERVICE.
2. `Hits (##, P[##])`: Anzahl der an den Dienst gerichteten Anfragen, Anzahl der Anfragen, die aufgrund der konfigurierten Serverpersistenz an den Dienst gerichtet wurden.
3. `ATr (##)`: Anzahl der aktiven Verbindungen zum Dienst.

   > **Hinweis:**
   >
   > Aktive Verbindungen haben die ausstehende Anfrage an den Dienst oder weisen derzeit Verkehrsaktivitäten auf.

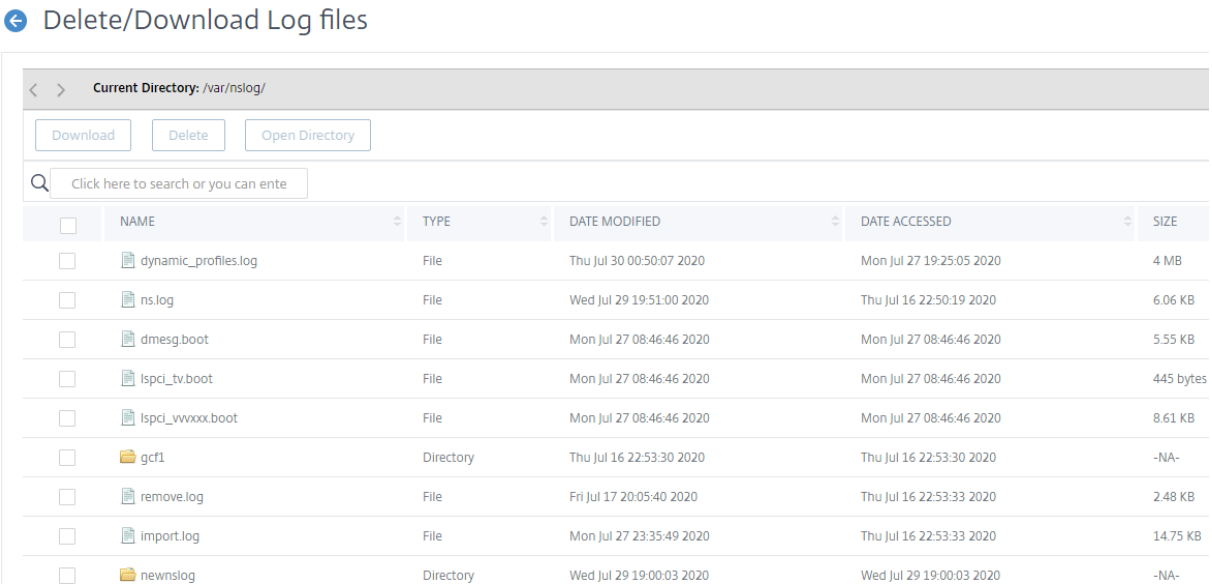
4. `Mbps (##.####)`: Das gesamte Verkehrsvolumen des Dienstes (Rx + Tx) wurde in Mbit/s umgerechnet.
5. `BWlmt (## kbits)`: Definiertes Bandbreitenlimit.
6. `RspTime (## ms)`: Durchschnittliche Antwortzeit des Dienstes in Millisekunden.
7. `Pkt(##/sec, ##bytes)`: Verkehrsvolumen in Form von Paketen pro Sekunde, die an den Dienst gesendet werden; Durchschnittliche Größe der Pakete.
8. `Wt (##)`: Gewichtsindex, der im Loadbalancing-Algorithmus verwendet wird.

> **Hinweis:**
>
> Wenn Sie diesen Wert durch 10.000 dividieren, erhalten Sie das tatsächlich konfigurierte Gewicht des Dienstes.

9. `RHits (##)`: Zähler für laufende Anfragen, der im Round-Robin-Loadbalancing-Algorithmus verwendet wird.
10. `CSvr (##, ##/sec)`: Anzahl der Verbindungen zum Service-Tarif.
11. `MCSvr (##)`: Maximale Anzahl von Verbindungen zum Dienst.
12. `OE (##)`: Anzahl der Verbindungen zum Dienst im Status geöffnet und eingerichtet.
13. `E (##)`: Anzahl der Verbindungen zum Dienst im etablierten Zustand.
14. `RP (##)`: Anzahl der Verbindungen zum Dienst, die sich im Wiederverwendungspool befinden.
15. `SQ (##)`: Anzahl der Verbindungen zum Dienst, die in der Überspannungswarteschlange warten.
16. `Load (##)`: Laden Sie den Dienst ein.
17. `LConn_Idx: (Current index(##); current virtual index(##),I:(##), base virtual slot index(##), transaction (##), Sub slot index(##))`: Index des Servers, wenn die Methode mit der geringsten Verbindung verwendet wird.
18. `Wt(Reverse Polarity)`: Umgekehrter Gewichtungsindex, der im Loadbalancing-Algorithmus verwendet wird.
19. `slimit_maxClient: (MaxClient [Exclusinve] Consumed: [Exclusive:Borrowed :TotActiveConnection:] Available: (##))`: Exklusive und gemeinsam genutzte Informationen zum gemeinsamen Limit für maximale Anzahl von Kunden.
20. `newlyUP_mode: (No, pending (##), update (##*##), incr_time (##*##), incr_count (##))`: Zeigt an, ob der Dienst neu eingerichtet wurde, und seine Statistiken entsprechen der Anzahl der zulässigen Treffer für den neuen Dienst. Auch die Uhrzeit, zu der die Gewichte für diesen Service aktualisiert werden.

Erfassen Sie Leistungsstatistiken und Ereignisprotokolle mit der NetScaler GUI

1. Navigieren Sie zu **System > Diagnose > Wartung > Protokolldateien löschen/herunterladen**.
2. Wählen Sie eine Datei aus und klicken Sie auf **Herunterladen**, um die Datei herunterzuladen.



Protokolldateirotation konfigurieren

May 11, 2023

Die NetScaler-Appliance generiert Protokolle in mehreren Verzeichnissen und in verschiedenen Formaten. Einige dieser Protokolle werden standardmäßig nicht rotiert und können an Größe zunehmen und zu viel Speicherplatz beanspruchen. Mithilfe der mitgelieferten Hilfsprogramme für die Protokollrotation (`newsyslog`) können Sie diese Protokolle konsistent verwalten, indem Sie zur einfacheren Verwaltung und Verwaltung nur relevante Informationen speichern.

Das in der NetScaler-Firmware enthaltene `newsyslog` Dienstprogramm archiviert Protokolldateien und rotiert die Systemprotokolle, sodass das aktuelle Protokoll während der Rotation leer ist. Das System-Crontab führt dieses Dienstprogramm stündlich aus und liest die Konfigurationsdatei, in der die zu rotierenden Dateien und die Bedingungen angegeben sind. Die archivierten Dateien können bei Bedarf komprimiert werden.

Die bestehende Konfiguration befindet sich in `/etc/newsyslog.conf`. Da sich diese Datei jedoch im Speicherdateisystem befindet, muss der Administrator die Änderungen speichern, `/nsconfig/newsyslog.conf` damit die Konfiguration den Neustart des NetScaler übersteht.

Die in dieser Datei enthaltenen Einträge haben das folgende Format:

```
logfilename [owner:group] mode count size when flags [/pid_file] [sig_num]
```

> **Hinweis:**
>
> Felder in eckigen Klammern sind optional und können weggelassen werden.

Jede Zeile in der Datei steht für eine Protokolldatei und die Bedingungen, unter denen die Rotation erfolgen muss.

Im Beispiel gibt das Feld `size` an, dass die Größe von `ns.log` 100 Kilobyte ist. Das Feld `count` gibt an, dass die Anzahl der archivierten `ns.log`-Dateien 25 ist. Eine Größe von 100 K und eine Anzahl von 25 sind die Standardwerte für Größe und Anzahl.

> **Hinweis:**
>
> Wenn das Feld mit einem Sternchen (*) konfiguriert ist, bedeutet dies, dass die Datei ns.log nicht zeitabhängig rotiert wird. Jede Stunde wird durch einen Crontab-Job das `newsyslog` Dienstprogramm ausgeführt, das überprüft, ob die Größe von ns.log größer oder gleich der in dieser Datei konfigurierten Größe ist. In diesem Beispiel wird die Datei gedreht, wenn sie größer oder gleich 100 K ist.

```
root@ns# cat /etc/newsyslog.conf
# Netscaler newsyslog.conf

# This file is present in the memory filesystem by default, and any
    changes
# to this file will be lost following a reboot. If changes to this file
# require persistence between reboots, copy this file to the /nsconfig
# directory and make the required changes to that file.
#
# logfilename [owner:group] mode count size when flags [/pid_file] [
    sig_num]
/var/log/cron 600 3 100 * Z
/var/log/amd.log 644 7 100 * Z
/var/log/auth.log 600 7 100 * Z
/var/log/ns.log 600 25 100 * Z
<!--NeedCopy-->
```

Das Feld `size`kann geändert werden, um die Mindestgröße der Datei `ns.log` zu ändern, oder das Feld kann geändert werden, um die Datei `ns.log` basierend auf einer bestimmten Zeit zu drehen.

Die tägliche, wöchentliche und/oder monatliche Spezifikation wird wie `[Dhh]`folgt angegeben: bzw. `[Dhh [Mdd]]` Die optionalen Tageszeitfelder sind standardmäßig Mitternacht. Die Bereiche und Bedeutungen dieser Spezifikationen sind:

```
Hh hours, range 0 ... 23
w day of week, range 0 ... 6, 0 = Sunday
dd day of month, range 1 ... 31, or the letter L or l to specify the
    last day of the month.
<!--NeedCopy-->
```

Beispiele:

Hier sind einige Beispiele mit Erklärungen für die Protokolle, die standardmäßig rotiert werden:

`/var/log/auth.log 600 7 100 * Z`

Das Authentifizierungsprotokoll wird rotiert, wenn die Datei 100 K erreicht, die letzten 7 Kopien der Datei auth.log werden archiviert und mit gzip (Z-Flag) komprimiert, und den resultierenden Archiven werden die folgenden Berechtigungen zugewiesen: rw——-.

`/var/log/all.log 600 7 * @T00 Z`

Das Catch-All-Log wird jeden Abend um Mitternacht siebenmal rotiert (@T00) und mit gzip komprimiert. Den resultierenden Archiven werden die folgenden Berechtigungen zugewiesen —rw-r—-.

`/var/log/weekly.log 640 5 * $W6D0 Z`

Das wöchentliche Protokoll wird jeden Montag um Mitternacht fünfmal rotiert. Den resultierenden Archiven sind Berechtigungen zugewiesen.

Allgemeine Rotationsmuster:

- `D0`. rotieren jeden Abend um Mitternacht
- `D23`. jeden Tag um 23:00 Uhr rotieren
- `W0D23`. rotieren Sie jede Woche am Sonntag um 23:00 Uhr
- `W5`. rotieren Sie jede Woche am Freitag um Mitternacht
- `MLD6`. rotieren Sie am letzten Tag eines jeden Monats um 6:00 Uhr
- `M5`. rotieren an jedem fünften Tag des Monats um Mitternacht

Wenn sowohl ein Intervall als auch eine Zeitspezifikation angegeben sind, müssen beide Bedingungen erfüllt sein. Das heißt, die Datei muss mindestens so alt wie das angegebene Intervall sein und die aktuelle Uhrzeit muss der Zeitspezifikation entsprechen.

Sie können die minimale Dateigröße festlegen, es gibt jedoch keine Begrenzung der Dateigröße, bevor das `newsyslog`-Dienstprogramm in der nächsten Stunde an die Reihe kommt.

Newsyslog debuggen:

Um das Verhalten des `newsyslog`-Hilfsprogramms zu debuggen, fügen Sie das Verbose-Flag hinzu.

```
root@dj_ns# newsyslog -v
/var/log/cron <3Z>: size (Kb): 31 [100] --> skipping
/var/log/amd.log <7Z>: does not exist, skipped.
/var/log/auth.log <7Z>: size (Kb): 2 [100] --> skipping
/var/log/kerberos.log <7Z>: does not exist, skipped.
/var/log/lpd-errs <7Z>: size (Kb): 0 [100] --> skipping
/var/log/maillog <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/sendmail.st <10>: age (hr): 0 [168] --> skipping
/var/log/messages <5Z>: size (Kb): 7 [100] --> skipping
/var/log/all.log <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/slip.log <3Z>: size (Kb): 0 [100] --> skipping
```



```
/var/log/ppp.log <3Z>: does not exist, skipped.
/var/log/security <10Z>: size (Kb): 0 [100] --> skipping
/var/log/wtmp <3>: --> will trim at Wed Apr 1 04:00:00 2009
/var/log/daily.log <7Z>: does not exist, skipped.
/var/log/weekly.log <5Z>: does not exist, skipped.
/var/log/monthly.log <12Z>: does not exist, skipped.
/var/log/console.log <5Z>: does not exist, skipped.
/var/log/ns.log <5Z>: size (Kb): 18 [100] --> skipping
/var/log/nsvpn.log <5Z>: size (Kb): 0 [100] --> skipping
/var/log/httperror.log <5Z>: size (Kb): 1 [100] --> skipping
/var/log/httpaccess.log <5Z>: size (Kb): 1 [100] --> skipping
root@dj_ns#
<!--NeedCopy-->
```

So geben Sie Speicherplatz in einem /Flash-Verzeichnis in einer NetScaler Appliance frei

May 11, 2023

In diesem Artikel zur Fehlerbehebung wird erläutert, wie ein Administrator Speicherplatz aus dem /flash Verzeichnis einer NetScaler Appliance freigeben kann.

Vorgehensweise zum Freigeben von Speicherplatz im /flash Verzeichnis einer NetScaler Appliance

1. Melden Sie sich mit SSH an der CLI von NetScaler an.
2. Nachdem Sie sich bei der NetScaler CLI angemeldet haben, wechseln Sie mit dem folgenden Befehl zur Shell-Eingabeaufforderung.`shell`.
3. Führen Sie den `df -h` Befehl aus, um die Verfügbarkeit von Speicherplatz auf der NetScaler Appliance anzuzeigen.
4. Wenn die Kapazität des Verzeichnisses /flash mehr als 90 Prozent oder niedrig ist, müssen Sie einige Dateien aus diesem Verzeichnis löschen.
5. Führen Sie die folgenden Befehle aus, um den Inhalt des /flash -Verzeichnisses anzuzeigen:

   ```
   cd /flash
   ls -l
   ```


6. Möglicherweise finden Sie mehrere Dateien verschiedener Versionen des NetScaler Software-Releases. Stellen Sie sicher, dass die an diesem Speicherort vorhandenen Dateien für die aktuelle Version der NetScaler-Software auf Ihrer Appliance gelten. Führen Sie den folgenden Befehl aus, um alle anderen Dateien von der Appliance zu entfernen.

```
rm <filename>
```

> **Hinweis**
>
> Entferne nur die älteren Versionen des Kernels. Das /flash Verzeichnis muss die Dateien enthalten, die die aktuelle Version oder der aktuelle Build der NetScaler-Softwareversion verwendet, und die Datei kernel.gz. Citrix empfiehlt, diese Dateien nicht aus dem /flash Verzeichnis zu entfernen.

Referenzmaterial

May 11, 2023

Verwenden Sie diese Referenzinformationen, um ein vertieftes Verständnis der folgenden NetScaler Komponenten zu erhalten:

NetScaler SNMP OIDs - Details der SNMP-OIDs, mit denen Informationen von einer NetScaler Appliance abgerufen werden können.

NetScaler Syslog Messages - Details zu den Syslog-Nachrichten, die von der NetScaler Appliance bereitgestellt werden.

NetScaler CLI-Befehle - Details zu den Befehlen, mit denen die NetScaler Appliance über die CLI konfiguriert werden kann. Sie können auch die Details jedes Befehls in der CLI anzeigen, indem Sie den <ns-command-name> Befehl man eingeben.

API-Referenz - Details zu allen Vorgängen, die mit der REST-API auf der NetScaler Appliance ausgeführt werden können.

NetScaler Advanced Policy Expressions - Details zu den Ausdrücken, mit denen erweiterte Richtlinien definiert werden können.

